SIEMENS

SiPass integrated MP2.65

User Guide

MP 2.65 SP3

A-100028-1
15.12.2015

Building Technologies

CPS Fire Safety

Copyright

Edition: 15.12.2015

Document ID: A-100028-1

Table of Contents

1 Introduction and Starting Up 15
1.1 System Preferences 15
1.1.1 Customizing System Preferences 15
1.1.1.1 General Tab 16
1.1.1.2 Audit Trail Tab 17
1.1.1.3 Audit Trail Columns Tab 17
1.1.1.4 Notify Email Tab 17
1.1.2 Customizing Views and Toolbars 19
1.1.3 User Definable Menu Items 19
1.1.3.1 Adding a New Button to a Toolbar 19
1.1.3.2 Attaching and Running an Executable Command 20
1.2 Online Help and SiPass integrated License Information 20
1.3 Setting up Printers for SiPass integrated 20
1.3.1 Audit Trail Printing 21
1.3.1.1 Privilege Control for Printer Access 21
1.3.1.2 System Behavior 21
1.3.1.3 Filtering of Audit Trail Columns 21
1.3.2 Configuring an Audit Trail Printer 22
1.3.2.1 Audit Trail Printing Columns 23
1.3.2.2 Viewing the Contents of the Printer Buffer 23
1.3.3 Plan Printing 23
1.3.3.1 Configuring a Site Plan Printer 23
1.3.4 Report Printing 24
1.3.4.1 Configuring a Report Printer 24
2 System Components 25
2.1 The Behavior of Components Offline 25
2.2 Server Properties 26
2.3 Ethernet Comms 26
2.3.1 Setting the Ethernet comms 26
2.4 Adding an ACC 28
2.4.1 ACC configuration Options 29
2.4.2 ACC-Granta 29
2.5 FLN Connections 30
2.6 Devices 30
2.6.1 Default Settings for Devices 32
2.6.2 Discovering Devices 33
2.7 Points 33
2.7.1 Defining Access Points 34
2.7.1.1 Access point general configuration 35
2.7.1.2 Access point Host Verification Configuration 35
2.7.1.3 Access point Additional Access Configuration 36
2.7.1.4 Access Point Dual Custody 36

2.7.1.5 Access point Intrusion Control Configuration 40
2.7.1.6 Access point Programmable Authorization 40
2.7.2 Defining Input and Output Points 40
2.8 Device Firmware Download and Configuration 42
2.8.1 Creating a Custom Card Format 44
2.8.2 Configuring Reader Interface Offline Modes 45
2.8.3 Configuring Siemens OSDP Readers 47
2.9 Initializing Units 48
2.9.1 Initialization Options 48
2.9.2 Creating an Initialization Event Task 49
2.9.3 Creating an Operation Mode Event Task 49
2.10 Dependencies Reports 50
3 Site Management 52
3.1 Time Schedules 52
3.1.1 Creating a Time Schedule 52
3.1.1.1 Time Schedule interval definition 53
3.2 Point Groups 53
3.2.1 Creating a Point Group 54
3.3 Component Groups 55
3.3.1 Creating a Component Group 55
3.4 Operational States and Control States 56
3.4.1 Control State Priorities 56
3.4.2 Using Control States 57
3.5 Creating a Host Event Task 58
3.5.1 Host Event Task Trigger fields 59
3.5.2 Host Event Task Effect fields 59
3.6 Creating a Controller Event Task 60
3.6.1 Controller Event Tasks Trigger Fields 61
3.6.2 Controller Event Task Effect Fields 61
3.6.3 Switching between Controller Event Tasks and Host Event Tasks 61
3.6.3.1 Triggering a Host Event Task from a Controller Event Task 62
3.6.3.2 Triggering a Controller Event Task from a Host Event Task 62
3.7 Creating a Holiday 63
3.8 Log Book 64
3.8.1 Adding a topic to the Log Book subjects 64
3.8.2 Making an Entry into a Log Book 64
3.9 Messaging 64
3.9.1 Messaging a GSM Mobile 64
3.9.1.1 Configuring Modem Hardware Resources 65
3.9.1.2 Event Task Message Forwarding to GSM Mobiles 65
3.9.1.3 Alarm Class Message Forwarding to GSM Mobile(s) 66
3.9.2 Configuring Message Forwarding to a Pager or Email Address 66
3.9.2.1 Step 1 - Configuring Service Providers 67
3.9.2.2 Step 2 - Configuring Cardholder Details 67

3.9.2.3 Step 3 – Creating the Messaging Event Task 68
3.10 Server Messaging 68
3.11 Anti-Passback 70
3.11.1 Creating an Anti-Passback Cluster 72
3.11.2 Creating an Anti-Passback area 72
3.11.2.1 Area Definition Configuration Fields 74
3.11.3 Assigning a sub-area to an Anti-Passback area 74
3.11.4 Viewing Cardholders in an Area 75
3.11.5 Forgiving Anti-Passback Violations 75
3.12 Intrusion Areas 76
3.12.1 Configuring an Intrusion Area 76
3.12.2 Viewing the details of an input point 77
3.13 Door Interlocking 78
3.13.1 Configuring a Door Interlocking Set 78
3.13.2 Configuring the Delay Time for an Interlocked Door 78
3.14 External Alarm Monitoring 78
3.14.1 Configuring an External Alarm Monitoring unit 79
3.14.2 Configuring an External Alarm Monitoring unit using the Auto Wizard 79
3.14.3 Configuring External Alarm Point details 80
4 Personnel Management 82
4.1 Operator Groups 82
4.1.1 Creating an Operator Group 82
4.1.1.1 General Details 84
4.1.2 Report Privileges 85
4.2 Operators 85
4.2.1 Adding Operators 86
4.2.1.1 Operator Details 86
4.2.2 Searching for an Operator 87
4.3 Workgroup 88
4.3.1 Work Group Fields 88
4.3.1.1 Work Group Configuration Tab Fields Description 88
4.3.1.2 Contact Tab Field Description 89
4.3.2 Partition Workgroups 89
4.3.2.1 Creating a Partition Work Group 90
4.3.3 Non-Partition Workgroups 90
4.3.3.1 Creating a Non-Partition Work Group 91
4.3.4 Configuring Workgroup Access Privileges 91
4.3.4.1 Temporarily Disabling Workgroup Access Privileges 92
4.3.4.2 Modifying Workgroup Access Privileges 92
4.3.5 Voiding a Workgroup 92
4.3.6 Deleting a Workgroup 93
4.3.7 Configuring Card Profiles for Workgroups 93
4.3.8 Automatic Bulk Card Creation 93
4.3.9 Configuring Cardholder Workgroup for Anti-Passback Assignment 94
4.4 Credential Profile 94

4.4.1 Adding / Deleting Credential Profiles 95
4.5 Cardholders 95
4.5.1 Cardholder Tabs and Tab Fields 96
4.5.1.1 Definition Tab 96
4.5.1.2 Advanced Tab 98
4.5.1.3 Personal Tab 99
4.5.1.4 Vehicle Tab 100
4.5.1.5 Tracking Tab 100
4.5.1.6 Control Tab 101
4.5.1.7 Imaging Tab 101
4.5.1.8 Custom Tabs 102
4.5.2 Adding Cardholders 103
4.5.2.1 Configuring the DEFINITION Tab 103
4.5.2.2 Configuring the ADVANCED Tab 108
4.5.2.3 Configuring the PERSONAL Tab 110
4.5.2.4 Configuring the VEHICLE Tab 111
4.5.2.5 Configuring the TRACKING Tab 112
4.5.2.6 Configuring the CONTROL Tab 113
4.5.2.7 Configuring the IMAGING Tab 114
4.5.3 Searching for a Cardholder 116
4.5.3.1 Search Based on Details Provided 116
4.5.3.2 Search and Select a Cardholder from the 'Search Cardholder' Dialog 117
4.5.4 Configuring Multiple Cards for a Cardholder 118
4.5.5 Unused Cards 118
4.5.5.1 Tracking Unused Cards using Customized / Predefined Reports 118
4.5.5.2 Configuring a Host Event Task based on the Actionable Report 120
4.6 Visitors 120
4.6.1 Adding a Visitor 121
4.6.2 Issuing and Returning Visitor Cards 122
4.6.3 Adding a Visitor to a list of Expected Visitors 123
5 Access Management 124
5.1 Access Levels 124
5.1.1 Configuring Access Levels 124
5.1.2 Searching for an Access Level 125
5.2 Access Groups 125
5.2.1 Configuring Access Groups 125
5.2.2 Searching for an Access Group 125
5.3 Access Assignment 126
5.3.1 Configuring Access Privileges 126
5.3.1.1 Assigning Cardholder's Private Access Privileges 127
5.3.1.2 Assigning Cardholder's Workgroup Access Privileges 129
5.3.1.3 Assigning Cardholder's Venue Booking Access Privileges 130
5.3.2 Workgroup and Operator Access Privileges 130

5.4 Offline Access 130
5.4.1 Defining Offline Access Groups 130
5.4.2 Defining Offline Access Privileges 131
5.5 Venue Management 131
5.5.1 Creating a New Venue 132
5.5.2 Configuring Access Control for Venue 132
5.5.3 Venue Booking 133
5.5.3.1 Booking a Venue 133
5.5.3.2 Configuring a Recurrent Venue Booking 134
5.5.3.3 Listing Current Bookings 135
5.5.3.4 Single-Screen Display of Single/Multiple Venue Bookings 135
5.5.3.5 Assigning Cardholder's Venue Booking Access Privileges 136
6 Monitoring Your Site 138
6.1 Active Audit Trail Window 138
6.1.1 Multiple Audit Trail Views 138
6.2 SiPass integrated Alarm System 139
6.2.1 Creating an Alarm Class 139
6.2.1.1 Alarm Class Options 140
6.2.2 Creating a Defined State 141
6.3 Handling Alarms 142
6.3.1 Restorable Alarms 142
6.3.2 Non-Restorable Alarms 142
6.3.3 Creating Custom Alarm Responses 143
6.3.4 Actioning an Alarm 143
6.3.4.1 Method 1 - Alarm Display dialog 143
6.3.4.2 Method 2 - Site Plan 144
6.3.4.3 Method 3 - Alarm Queue 144
6.4 Controlling Points 145
6.4.1 Querying a Point 145
6.4.2 Securing and Unsecuring a Point 145
6.4.3 Allowing Access to an Output Point 146
6.4.4 Manual Override 146
6.4.5 Using the Alarm Queue 147
6.5 Overviewing Your Site 148
6.5.1 Database components 148
6.5.2 Viewing the Status screen 148
7 Data Management 149
7.1 Managing the Database 149
7.1.1 Backing up the Database 149
7.1.1.1 Database Backup Components 150
7.1.1.2 Host Event Task-Triggered Database Backup 150
7.1.1.3 Cancelling an Event Task Triggered Backup 150
7.1.2 Restoring the Database 151
7.1.2.1 Database Restore Components 152
7.2 Managing the Audit Trail 152

7.2.1 Archiving the Audit Trail 153
7.2.1.1 Automatic Audit Trail Archiving 153
7.2.1.2 Manual Audit Trail Archiving (Forced Operation) 153
7.2.2 Backing up the Audit Trail 154
7.2.2.1 Audit Trail Backup Operations 154
7.2.3 Restoring the Audit Trail 155
7.2.4 Purging the Audit Trail Archives 155
7.2.5 Host Event Task Triggered Audit Trail Purge 156
7.3 Managing the Log Book 156
7.3.1 Backing up the Log Book 156
7.3.1.1 Log Book Backup Operations 157
7.3.2 Restoring the Log Book 157
7.3.3 Purging the Log Book 157
7.4 Using a Compact Flash Card for Database Management 158
7.4.1 Configuring a Compact Flash Card in SiPass integrated 158
8 Reports 159
8.1 Log Book Reports 159
8.1.1 Log Book Report Filters 160
8.2 Scheduled Reporting 161
9 Smart Card Encoding 162
9.1 Creating a Smart Card Profile 163
9.2 Configuring the Sector / Block Contents 165
9.2.1 Configuring the Sector / Block Contents for Mifare Classic Cards 165
9.2.2 Configuring the Application / File Contents for Mifare DESFire Cards 166
9.2.3 Output Formats 167
9.2.4 Access Control Formats 167
9.2.5 Data Types 168
9.3 Configuring the Sector Keys 168
9.3.1 Configuring the Sector Keys for Mifare Classic Cards 168
9.3.1.1 Access Conditions 169
9.3.2 Configuring the Sector Keys for Mifare DESFire Cards 169
9.4 Configuring a custom access control format 170
9.5 Assigning a Profile 171
9.5.1 Assigning a Profile to a Card Template 171
9.5.2 Assigning a Profile to an Individual Cardholder 171
9.6 Reading a card with the Profile Viewer 172
9.7 Configuring a Smart Card Printer 172
9.8 Configuring a Card Reader (Smart card or Enrollment) 173
9.8.1 Reader Types Supported 174
10 CCTV 175
10.1 CCTV Configuration Summary 175
10.2 Using CCTV Controls 176
10.2.1 CCTV Camera Controls 176
10.3 Programming SiPass integrated for CCTV 178

10.3.1 Configuring the CCTV Bus 178
10.3.2 Configuring the CCTV Controller Unit 179
10.3.3 Programming a Camera 180
10.3.4 Programming a Monitor 181
10.3.5 Programming an Auxiliary Device....182
10.3.6 Programming an Alarm Point....182
10.3.7 Grouping Cameras and Monitors....183
10.4 Configuring CCTV 183
10.4.1 Creating a camera preset 183
10.4.2 Creating a camera pattern 184
10.4.3 Creating a camera sequence....185
10.5 Configuring a Generic CCTV 186
10.5.1 Prerequisites of Generic CCTV Configuration....186
10.5.2 Programming SiPass integrated for Generic CCTV 186
10.5.2.1 CCTV Bus and Parameter Configuration 186
10.5.2.2 Configuring the Generic CCTV Bus 187
10.5.2.3 Configuring the New Command Sets for Generic CCTV 189
10.6 Operating CCTV....190
10.6.1 Viewing images from a camera 190
10.6.2 Viewing preset images from a camera 191
10.6.3 Running a Pattern....191
10.6.4 Running a Sequence 192
10.6.5 Viewing Images through the Live CCTV Dialog 193
10.6.6 Resuming / Restarting CCTV Patterns and Sequences after power loss 193
10.6.7 CCTV Alarm and Event Handling 194
10.6.7.1 Triggering a CCTV Event 194
10.6.7.2 Triggering a SiPass Alarm (Pelco with DT4 only) 195
11 Image Verification....197
11.1 Configuring Image Verification at an Access Point....197
11.2 Operating Image Verification....198
11.2.1 Operating Image Verification from the Audit Trail....199
12 Dial-up....200
12.1 Dial-up Components 200
12.2 Pre-requisites 201
12.3 Dialup Setup Checklist....202
12.4 Creating the Dialup Connection 202
12.4.1 Step 1: Making the Connection....203
12.4.2 Step 2: Assigning a username and password to the SiPass Server Service 204
12.4.3 Step 3: Setting up an ACC for remote communications 204
12.5 Creating the Dial-up Bus Service 205
12.5.1 Defining the Dial-up ACC....206
12.5.1.1 Dialup Properties....206
12.5.2 Defining other Components 207
12.5.3 Alarm Class on Dial-up Controllers....207

12.5.4 Initialization and Downloading 208
12.5.4.1 Initialization Options 208
12.5.4.2 Automatic download of data to a remote ACC 209
12.5.4.3 Uploading data from a remote unit 209
12.6 Redundant Communications 210
12.6.1 Pre-requisites 211
12.6.2 Redundancy Configuration Summary 211
12.6.3 Setting up Dialup Redundancy 211
12.6.3.1 Creating the Dialup Connection 211
12.6.3.2 Setting-up password storage 212
12.6.3.3 Setting up an ACC for remote communications 212
12.6.4 Setting-up redundant dialup on an ACC 213
12.6.4.1 Dialup ACC Options 214
13 Elevators 215
13.1 Elevator Control 216
13.2 Fire Override 216
13.2.1 Fire Override and Wiring 216
13.3 Setting up an Elevator System 217
13.3.1 Low-level System Pre-Configuration 217
13.3.2 Defining the Advanced Central Controller (ACC) 217
13.3.3 Defining the Output Point Modules (OPM) 218
13.3.4 Defining the Card Readers 218
13.3.5 Defining the Banks 219
13.3.6 Defining the Floors 219
13.3.7 Defining the Elevators 221
13.4 Access Control 222
13.4.1 Assigning Floor Access to Cardholders 223
14 Guard Tour 225
14.1 Configuring Guard Tour 225
14.1.1 Adding a Guard to the System 225
14.1.1.1 Creating a Tour 226
14.1.2 Creating a Tour Group 229
14.1.3 Starting and Monitoring Tours 229
14.1.3.1 Registering and starting a Tour 229
14.1.3.2 Monitoring Tours 231
14.1.3.3 Displaying Tour Stop Log 231
14.1.3.4 Printing a Guard Tour Report 232
14.1.3.5 Starting a Tour from the Guard Tour Monitor 232
14.1.3.6 Stopping a Tour 233
14.1.3.7 Skipping a Tour Point 233
14.1.3.8 Acknowledging an Alarm 234
14.1.3.9 Aborting a Tour 234
14.1.3.10 Guard Tour Window 235
14.1.3.11 Right Mouse Button Options 235
15 Biometric Integration 236
15.1 Introduction 236

15.1.1 Prerequisites 236
15.2 Configuring the Bioscrypt Bus 238
15.3 Saving the Custom Card Configuration 238
15.4 Creating a Bioscrypt Credential Profile 239
15.5 Determining the Bioscrypt / Enrollment Reader Configuration 239
15.5.1 Configuring the Bioscrypt reader in SiPass integrated 239
15.5.2 Configuring an Enrollment Reader for the Bioscrypt functionality 241
15.6 Importing the Bioscrypt Reader Configuration 241
15.7 Configuring the Bioscrypt profile to a Work Group 242
15.8 Types of Bioscrypt Configuration in SiPass integrated 243
15.8.1 Configuration Type A: Card Assignment 243
15.8.1.1 Configuring the Bioscrypt Reader for Configuration I ...243
15.8.1.2 Assigning Fingerprints and Cards with the Bioscrypt Reader 244
15.8.2 Configuration Type B: Fingerprint Acquisition 245
15.8.2.1 Configuring an Enrollment Reader for Configuration II 245
15.8.2.2 Card Enrollment with Bioscrypt Details 246
16 Intrusion Arming Terminal (ATI5100 / IAT-010) 248
16.1 IAT-010 Terminal Types 248
16.2 Configuring a New Intrusion Terminal (Standalone) 249
16.2.1 Configure / Discover a New IAT-010 Device 249
16.2.2 Configuring the IAT-010 device on the Components Dialog 250
16.2.3 Assigning an IAT-010 to an Intrusion Area as an Arm/Disarm Point 251
16.2.4 Configuring an Access Level and an Access Group, with the Intrusion Area 251
16.2.5 Configuring a Cardholder's Access Privilege with the Access Group 251
16.2.5.1 Configuring the IAT-010 Terminal to Arm / Part-arm / Disarm the Intrusion Area 251
16.3 Overview of Configuring an Intrusion Terminal with Access Control 252
16.3.1 Discovering the IAT-010 Device 252
16.3.1.1 Creating a new IAT-010 device on the Components dialog 252
16.3.1.2 Discovering the IAT-010 device on the FLN Configuration dialog 253
16.3.2 Linking a Door Reader to the IAT-010 for Intrusion Control 253
16.3.3 Creating an Intrusion Area with Arm / Disarm and Input Points ..253
16.3.4 Access Level Configuration to include Intrusion Area and Input Point, and assigning of an Access Group 254
16.3.5 Configuring a Cardholder's Access Privilege to the Access Group 254
16.3.6 Operating the IAT-010 Terminal to Arm / Part-arm / Disarm the Intrusion Area 254
16.4 Intrusion Control for Multiple Areas 254
16.5 Executing Manual Override commands for the IAT- 010 device 255
16.5.1 Manual Commands for the Standalone Intrusion Terminal 255

16.5.2 Manual Commands for the Intrusion Terminal with Access Control (linked terminal) 255
16.6 Deleting an ATI5100 Device 255
16.6.1 Deleting an Intrusion Terminal (Standalone) 255
16.6.2 Deleting an Intrusion Terminal with Access Control 256
16.7 Partial Arming / Part-Arming 256
16.7.1 Configuring Input Points for Partial / Part Arming 256
16.8 Intrusion Terminal Alerts of Unsealed Inputs 257
16.9 Isolation Privileges for Multiple Unsealed Inputs 257
16.10 Trouble-Shooting 258
17 DVR 259
17.1 Programming SiPass integrated for DVR 259
17.2 Configuring the DVR Comms Channel 260
17.3 Configuring the SISTORE/DVR Client in SiPass integrated 260
17.4 Configuring a DVR unit 261
17.4.1 Configuring Input / Output Points for a DVR Unit 262
17.4.1.1 Field Definitions for Digital Input / Output Points 262
17.4.1.2 Field Definitions for Digital Output Points 263
17.4.1.3 Configuring Host Event Tasks for Digital Input/Output points 263
17.4.1.4 Configuring a Manual Command to Change the State of a DVR Digital Output 263
17.4.1.5 Configuring a DVR Digital Input / Output Point Group .264
17.4.2 Configuring Monitors for a DVR Unit 264
17.4.2.1 Configuring Remote Video Inputs for the DVR Unit 264
17.4.2.2 DVR Unit Functions Available from Site Plans 265
17.4.3 Configuring a DVR Camera 265
17.4.3.1 Discovering configured DVR video alarms (sensors) ... 266
17.4.3.2 Field Definitions for Video Alarms (sensors) 267
17.4.3.3 Setting up a Host Event Task to change the DVR Video Alarm program 267
17.4.3.4 Setting up a HET to create a connection between a DVR camera and monitor 268
17.4.4 Grouping DVR Cameras 268
17.4.5 Configuring an IP Camera 269
17.4.5.1 Viewing IP Camera video on the Live DVR dialog 270
17.4.5.2 Viewing IP Camera video on the Virtual Monitor 270
17.4.5.3 Using an IP Camera as a Remote Video Source 270
17.4.5.4 Using an IP Camera for Cardholder Imaging 271
17.4.5.5 IP Camera Supported Protocols 271
17.5 Configuring a Generic DVR unit 272
17.5.1 Configuring Input / Output Points for a Generic DVR Unit 272
17.5.2 Configuring Monitors/DVR Cameras/IP Cameras for a Generic DVR Unit 273
17.6 Operating DVR from SiPass integrated 273
17.6.1 Viewing Pictures from a DVR Camera 274
17.6.2 Setting up a DVR Recording Event Task 274
17.6.3 Playing Back DVR Recordings from the Audit Trail 275

17.7 Virtual Monitors 275
17.8 Operating the DVR Client 275
17.8.1 Creating a Preset from the DVR Client 276
17.8.2 Recording from the DVR Client 276
17.8.3 Search and Playback of a DVR Recording 277
17.8.3.1 Searching for recorded video clips 277
17.8.3.2 Playback recorded video clips 279
17.9 Operating the SISTORE DVR Client 279
17.9.1 Using the SISTORE AX Client to view live images 279
17.9.2 Using the SISTORE AX Client to record and playback 280
17.10 Creating a DVR Audit Trail Report 281
17.11 Viewing Live Video in SiPass integrated 282
17.11.1 Live DVR 282
17.11.1.1 Live Video 282
17.11.1.2 Recorded Video 282
17.11.2 Virtual Monitors 282
18 Photo-ID and Graphics 283
18.1 Graphics 283
18.2 Drawing toolbar 283
18.2.1 Additional Menus 284
18.2.1.1 Edit Menu 284
18.2.1.2 View Menu 286
18.2.1.3 Drawing Menu 286
18.3 Graphics Tools 287
18.4 Drawings 288
18.5 Symbols 289
18.5.1 Creating a symbol 289
18.5.2 Importing graphics to make your own symbol 289
18.6 Site Plans 290
18.6.1 Creating a site plan 290
18.6.2 Importing graphics into your site plan 290
18.6.3 Adding System Components (Symbols) to Your Site Plan 290
18.6.4 Adding Shortcuts to Your Site Plan 291
18.6.4.1 Shortcut Action Types 291
18.6.4.2 Shortcut Actions 292
18.6.5 Adding Counters and Timers to your Site Plan 292
18.7 Alarm Instructions 293
18.8 Using Site Plans to Monitor your Site 293
18.8.1 Interpreting the Site Plan 293
18.8.2 Securing a Point or Area From a Site Plan 294
18.8.3 Unsecure a Point or Area From a Site Plan 294
18.8.4 Allow Access to an Output Point From a Site Plan 294
18.8.5 Manually Controlling a Point from a Site Plan 295
18.8.6 Querying a Point From a Site Plan 295
18.8.6.1 Point Details 296
18.8.7 Actioning an Alarm from a Site Plan 296

18.9 Card Template Design and Encoding 296
18.9.1 Creating a Card Template 297
18.9.2 Adding a Cardholder Photograph to a Card Template 297
18.9.3 Adding a Bar Code to a Card Template....298
18.9.4 Adding a Magstripe to a Template....299
19 Video Imaging and Card Printing 300
19.1 Configuring the video image settings 300
19.2 Capturing Cardholder Photographs 301
19.2.1 Image Recall 301
19.3 Importing a Cardholder's Photograph or Signature 301
19.4 Card Printing 302
19.4.1 Configuring a Card Printer 303
19.4.2 Printing a Card 304
19.4.2.1 Batch Printing Card Filters 305
19.4.3 Batch Card Printing Monitor....306
Index 307

1 Introduction and Starting Up

Congratulations on choosing SiPass integrated to be your access control software solution. SiPass integrated is the leading access control software on the market. SiPass integrated is an access control and security management system that monitors and controls access to your site, using a personal computer running the latest Windows operating system.

The graphical user interface of SiPass integrated is designed to support the complex and demanding needs of security staff and operators. You can quickly and easily navigate the system and use the many functions provided. SiPass integrated is a complete system that packages all your access control needs into an easy-to-use application.

The SiPass integrated system allows you to effectively and efficiently monitor your building site and the people who access it. The system also allows dial-up communication via modems, meaning that fewer resources are required to monitor a large number of sites.

1.1 System Preferences

System Preferences allow you to customize the SiPass integrated user interface and system operation to your own preferences. There are three tabs for defining System Preferences. If you have installed the optional *Photo ID and Image verification* Module, a fourth tab is present (*Imaging*) on client machines.

The system preferences are operator specific and changes made to the default preferences and will only affect the operator who made those changes.

In addition to the customizable system settings, SiPass integrated will remember the size and position of the *Audit Trail* window from each operator's last session.

1.1.1 Customizing System Preferences

Customizing System Preferences will provide you with an enhanced and personalized Audit Trail view.

1. Select **Preferences** from the **Options** menu to display the *General* tab.
2. Complete the *General* tab system preferences. The section General Tab details the various the fields / options displayed on this tab.
3. To alter the Audit Trail preferences, choose the *Audit Trail* tab and complete the preferences displayed on this tab.
4. To select a location for archiving, choose the **Archive Folder Location** button.
5. To alter the Audit Trail Columns that are displayed, choose the *Audit Trail Columns* tab.
6. Select the columns to appear in the *Active Audit Trail.* Options selected in this dialog do not change the columns that are printed as part of Audit Trail Reports.
   - Select top or bottom section and press the 'Ctrl', 'Shift' and '+' keys to fit all Audit Trail Columns on the screen
   - The Audit Trail information appears in a window on the main screen of SiPass integrated and, due to the limitations of screen size, only a limited amount of information can be viewed at any one time. It may be necessary to scroll across to view events that do not completely fit within the window.
7. To alter Imaging details, select the *Imaging* tab and choose the preferences that are suitable for the viewing of images on screen. These preferences will depend largely on the video capture card installed in your PC.
8. Click **Save**.

1.1.1.1 General Tab

The following table explains the settings available on the *General* Tab.

Setting	Context	Description
Background Image File	User	Specifies the path and file name of the image to appear in the background of the SiPass integrated main screen.
Default Card & Operator Expiry Date	System(Local)	Specifies the date that will appear by default in the Cardholder and Operator definition screens. To disable the expiry date so that the card or operator privileges will never expire, de-select the checkbox.
Visitor default validity time (days)	System	Specifies the default time in days for visitors cards.
Operator Lockout Timeout	Operator	Specifies the time in minutes before workstation lockout is activated. You must re-enter your password to re-activate SiPass integrated, once your workstation has become locked. A value of 0 doesn't lock out the workstation.
Home Plan	User	Specifies the site plan that will automatically open when a user logs on.
Base PIN Code Required	System	If the Yes checkbox is ticked, a PIN code is required for each cardholder to gain access.
Base Pin Digits	System	The exact number of digits in the Base PIN Code.
Accept Unique Pins Only	System	When checked, each PIN Number assigned to a Cardholder in the Cardholder dialog must be unique.
Number of Generated PINs in PIN selection dialog	System	Specifies the number of PINs displayed on the PIN selection dialog. To change the number of PINs displayed select a number from the dropdown list.
PIN Duress Extension	System	Specifies the number of digits added to the cardholders' standard PIN in order to form a Duress PIN. This is formed by increasing or decreasing the last number of the cardholder's standard PIN. For example, if the cardholder's PIN is 1234, by selecting a PIN Duress Extension of 2, the duress PIN becomes 1232 or 1236.
Confirm on Save	Operator	When checked, the Save Confirmation dialog will appear when saving a modified Database record.
Confirm on Delete	Operator	When checked, the Delete Confirmation dialog will appear when deleting a Database record.
Employee Number Enforced	System	When checked, an employee number must be entered when a new cardholder is added in the system.
Display Higher Priority Alarm	System	When checked, allows alarms of a higher priority to be displayed in the Action Alarm dialog, if an alarm is already being actioned by an operator. The operator may select the higher priority alarm and choose to action it instead.
Clear on Save (Cardholder window only)	System	When checked, it will clear the cardholder window once it has been saved.
Save <None> Workgroup by Default (Cardholder window only)	System	When checked, if no Workgroup has been selected for a cardholder, no workgroup, i.e. '<None>' will be allocated to the cardholder by default.
Show on Start-up	Operator	When checked the System Status screen will be displayed upon start-up.
Refresh Rate (sec)	Operator	Specifies how often the data displayed in the Status monitor is updated to reflect the latest changes in status and alarm conditions. Default is 10 seconds. The current refresh rate is shown on the System Status screen.

1.1.1.2 Audit Trail Tab

The following table explains the settings available on the *Audit Trail* tab.

Setting	Description
Disable Detailed AT Logging	Tick this checkbox if you want to disable messages appearing in the audit trail, that relate to details of the changes made to database components by each operator.
Latest Message First	Tick this checkbox if you want to display the latest transaction in the access control system, at the top of the *Audit Trail* Window (instead of the bottom).
Additionally Write to TAB Files	Tick this checkbox if you want to write the audit trail transactions to a TAB File, in addition to the SQL database.
Write to Database	Tick this checkbox if you want Audit Trail Events to be written to a database table. By default, Audit Trail events are written to a tab file only. This option allows your site to maintain greater control over the backup and restoration of the Audit Trail history.
Latest Message First	Tick this checkbox to configure the audit trail to display the last message at the top of the window.
Top Viewer	Specifies the number of lines displayed in the upper section of the *Active Audit Trail* window. When this value is exceeded, the system automatically removes 20% of the Audit Trail events, so those new events can be displayed. The maximum number of lines that can be displayed is 50000.
Bottom Viewer	Specifies the number of lines displayed in the lower section of the Active Audit Trail window. The maximum number of lines displayed is 50000. When the viewer becomes full, the oldest lines are removed as new lines are added.
Default Colors	Specifies the default message color that appears in the Active Audit Trail window. To change colors, choose **Select Colors** button. You can select the background color and text color for the event in an alarm state, and also the colors for the event in a normal state.
Logon/Logoff Colour	Specifies the text color that will display on the in the *Active Audit Trail* window when you logon or logoff SiPass integrated. To change colors, choose the **Select Colors** button. You can select the background color and text color for the event in an alarm state, and also the colors for the event in a normal state.
Comms Actions Colour	Specifies the color of a Comms Actions event that appears in the *Active Audit Trail* window. To change colors, choose the **Select Colors** button. You can select the background color and text color for the event in an alarm state, and also the colors for the event in a normal state.
Alarm Actions Colors	Specifies the color of the Alarm action event that appears in the *Active Audit Trail* window. To change colors, choose the **Select Colors** button. You can select the background color and text color for the event in an alarm state, and also the colors for the event in a normal state.
Database Actions Colors	Specifies the color of the Database action event that appears in the Active Audit Trail window. To change colors, choose the **Select Colors** button. You can select the background color and text color for the event in an alarm state, and also the colors for the event in a normal state.
Event Task Colors	Specifies the color of the Event task that appears in the *Active Audit Trail* window. To change colors, choose the **Select Colors** button. You can select the background color and text color for the event in an alarm state, and also the colors for the event in a normal state.

1.1.1.3 Audit Trail Columns Tab

This tab displays all the field columns that can be displayed for the audit trail. Select the checkboxes of the audit trails you want displayed, and click **Save**.

1.1.1.4 Notify Email Tab

The Options drop down of this tab displays the types of email notifications that can be configured in SiPass integrated. These options and the configuration instructions are as follows:

- **Disabled:** Select this option to disable the email notification feature.
- **Exchange Server:** Select this option to send email notifications to cardholders using the Exchange Server.
- **SMTP:** Select this option to send email notifications to cardholders using the SMTP protocol.

Configuration Fields	Description
Exchange URL	Enter the URL of your Exchange Server web service. e.g., http://192.168.0.10/EWS/ExchangeServer It is recommended that you contact your system administrator for this information.
User Name	Enter the username of the main user.
Password	Enter the password of the main user.
Domain	Enter the domain name.

Recommendations:

1. Use any computer within the same domain with the Outlook 2007 or 2010 Auto Discovery feature.
2. Hold the **Ctrl** button and right click on the **Outlook Icon** in the system tray.
3. Select **Test E-mail Auto Configuration** from the menu.
4. Type in any email address located on the Exchange server.
5. Ensure that only the "Use Auto Discover" checkbox is enabled.
6. Click **Test**.
7. Search the results for the line starting with *Availability Service URL*. This contains the Exchange Web Services (EWS) URL.

The User Name and Password (provided by system administrator) specifies the account to be used as the Organizer of all the meetings created by SiPass. This account should have privileges to create/update/delete meetings in the Exchange server.

Note: This feature is supported by Exchange 2007 SP1, Exchange 2010 and Exchange 2013.

SMTP

Select this option to send email notifications to cardholders using the SMTP protocol.

Option	Description
Organizer Email	Enter the organizer's email address that will remain the standard email address displayed in the From: field of all emails sent from SiPass.
Host	Enter the SMTP Server host IP address.
Port	Enter the port number of the server
User Name	Enter the username of the main user.
Password	Enter the password of the main user.
Enable SSL checkbox	Tick this checkbox if you want to enable the SSL security protocol. **Note:** It is recommended that you contact your system administrator for this information.

1.1.2 Customizing Views and Toolbars

SiPass integrated allows you to customize the position of the toolbars, as well as move the icons across toolbars with a single drag and drop motion.

1. From the **View** menu, select the **Customize** option to display *Customize* dialog
2. Tick on the box next to the toolbar you would like to display.
3. You can also add the toolbars to your SiPass integrated display by selecting the icons. For example, selecting the **Alarm** icon will automatically display the **Alarm** toolbar.
4. Select the *Commands* tab.
5. Select a toolbar from the *Categories* dialog box, all the commands available will display in the *Commands* dialog box.
6. Select the icon you would like to add and drag it to you the toolbar.
7. To further customize the menu's and toolbars select the *Options* tab. To reset the menu and toolbar to the original settings, select **Reset Menu and toolbar usage data**.
8. Select **Close**.

1.1.3 User Definable Menu Items

SiPass integrated allows operators to create and customize their own menu bars and buttons. This functionality is client specific, and is not governed by Operator partitioning.

There are 2 simple stages required to apply this feature:

- **Stage 1**: Adding a new button to a tool bar
- **Stage 2**: Attaching and running an executable command to the new button

These stages have been discussed in the sections that follow.

1.1.3.1 Adding a New Button to a Toolbar

1. From the **View** menu, select **Customize…**
2. On the *Customize* dialog, select the *Commands* tab.
3. Scroll down the list of the **Categories** box, and select **All Commands**.
4. Scroll down list of the **Commands** box, and select **External Command**.

There are 24 External Commands buttons that an operator can use.

5. Click and drag this external command to a selected toolbar on the SiPass integrated user interface.

⇨ The new button will now be displayed on the toolbar.

1.1.3.2 Attaching and Running an Executable Command

1. From the **Options** menu, select **Custom Command Configuration**.
2. Click **Add**.
   ⇨ An external command will appear on the adjacent box.
3. In the **Name** field, enter a name for this External Command button.
4. In the **Path** field, enter a path for the External Command.
5. In the **Icon File** field, enter a file for an icon for the External Command button.
6. Click **Apply**.
7. Click the new menu button on the toolbar. This action runs the executable command attached to the button.

Consider that an executable command to open a Notepad application was attached to the new button. Clicking on the new button on the toolbar will execute this command, and so open the specified Notebook application.

Audit Trails will be generated for actions corresponding to the creation and edit of these User Definable Menu items.

Before backing up the SiPass integrated database, the operator will need to manually copy the XML file corresponding to the defined menu items to the other PC.

1.2 Online Help and SiPass integrated License Information

SiPass integrated provides an interactive Online Help reference manual under the **Help** menu. The menu also provides an **About** box with license information, as well as information about SiPass integrated which you can access on the web under the **SiPass integrated on the WEB** menu option.

You can select any of these options from the **Help** menu at any time.

1.3 Setting up Printers for SiPass integrated

SiPass integrated provides the functionality to configure four unique, task-oriented printing operations. Individual printers can be set up to automatically carry out specific printing tasks according to operator requirements.

The four printing operations are:

- **Audit Trail Printing**
- **Card Printing**
- **Plan Printing**
- **Report Printing**

Each of the above tasks can be configured from the standard *Windows Print Setup* dialog, which is opened by selecting the **New Printer** button under the tabs in the *Setup Global Printers* dialog. The **New Printer** button will only appear if there are no printers installed in Windows.

Printers may be shared across the application, although some limitations are imposed upon the use of each of the printer types. Each task requires a dedicated printer, but there is some allowance for multiple uses.

All printer output is dependent upon the access privileges assigned to the operator.

Actual printers cited in the following section are for the purposes of example only. Consult your local System Administrator and SiPass integrated distributor for details concerning recommended printers and their compatibility with your site.

1.3.1 Audit Trail Printing

Audit Trail printing can be carried out using either standard page or line printers. The SiPass integrated application identifies a line printer through the **Tractor Feed** setting, which is enabled during the configuration process. If this is not set, the system assumes that the printer is a page printer and buffers the page until the printable area is filled. The buffer is then dumped to the printer output file for normal printing.

To avoid potential conflicts, spooling should be selected in all circumstances. Refer to the appropriate *Printer Properties* dialogs when installing your printers. These are located in the **Start** menu of your computer under **Settings > Printers and Faxes,** and display the advanced settings and page setup options available for the selected printer.

1.3.1.1 Privilege Control for Printer Access

Operator Group privileges control access to the *Printer Setup* dialog. If an operator does not have the necessary access privileges, the **Printer Setup** options located under the **File** menu will be disabled, preventing the current settings from being altered. This stops the operator from enabling or disabling the **Print Audit Trail** option from within SiPass integrated.

1.3.1.2 System Behavior

These important issues are related to system behavior and Audit Trail printing:

- It is recommended that a separate default printer be installed and configured for Audit Trail printing from the printer configured for Report printing.
- Where the use of the same line printer for both Audit Trail and Report printing is unavoidable, ensure that the **Enable Audit Trail Printing** checkbox under the *Audit Trail* tab of the *Setup Global Printers* dialog is disabled before you print a Report. This will prevent live audit trail messages conflicting with the current printing job.

To help keep Audit Trail and Report printing separate:

- You can send the Audit Trail to a page printer that does not have a default printer requirement.
- In the case where a line printer is used, you must ensure that Audit Trail and Report printing are not run concurrently. This will require manual intervention.
- A Print Preview of an Audit Trail screen will display a blank page unless the **Enable Audit Trail Printing** checkbox is ticked during setup. In addition, without the necessary access privileges, an operator cannot alter the current settings in order to display the Audit Trail report prior to printing.

1.3.1.3 Filtering of Audit Trail Columns

It is important to understand the distinction between Audit Trail printing and Audit Trail Reports. Audit Trail printing produces a “hard copy” of the events recorded in the Audit Trail and takes place dynamically as the events occur. The columns that are displayed in Audit Trail printing are not configurable. However, Audit Trail reports are the result of retrieving and formatting records from the Audit Trail database. The columns displayed in Audit Trail reports are configurable.

This functionality is totally independent of the display settings used in the *Audit Trail* tab of the *System Preferences* dialog.

Checking the **Print Alarm Messages Only** checkbox in the *Setup Global Printers* dialog initiates the filtering of Audit Trail messages, so that only Alarm messages are printed.

Printer settings are retained for all operators, so that when operators are changed, the **printer enabled** or **print filtering** options will not be altered. However, the *Print Setup* dialog will appear disabled for operators lacking the necessary access privileges to alter these settings.

1.3.2 Configuring an Audit Trail Printer

An audit trail printer can be either a standard laser or a line printer. While a line printer will print a line at a time, a laser printer will buffer the messages until the page buffer is full and then print the contents a single page at a time. Both printer types are configured in a similar way.

Follow the procedure below to configure the audit trail printer.

▷ If you are connecting the printer directly to a SiPass client PC, ensure that you have installed the appropriate printer driver for that printer. Otherwise, the printer cannot be selected from the drop-down list during the configuration process.

1. From the **File** menu, select the **Print Setup** option to display the *Setup Global Printers* dialog.
2. Choose the *Audit Trail Printer* tab. This is the default tab and it displays the current printer, if connected.
3. Check the **Enable Audit Trail Printing** checkbox. This activates the **Audit Trail Options** section of the dialog. If this check box is not ticked, Audit Trail events will not be printed.
4. From the **Audit Trail Print Options** section, select the type of messages to be displayed by highlighting the appropriate radio button.
   - **Print Alarm Messages Only**: This option enables the printing of Alarm messages only from the Audit Trail.
   - **Print All Messages**: This option enables the printing of all messages from the Audit Trail.
5. Tick the **132 Column** checkbox, if required. By default, the font used by the printer will be a standard width font, such as *Courier*.
   - Select this option if your audit trail printer can print 132 or more characters per line. The fields A/N, DATE, TIME, LOCATION, F_NAME, L_NAME, CARDNO, and MESSAGE will be printed with format "%s %-12.12s %-12s %-22.22s %-12.12s %-12.12s %-12.12s %-43.43s". (133 characters).
   - Do not select this option if your audit trail printer can only print 80 characters per line. The fields A/N, DATE, TIME, LOCATION and MESSAGE will be printed with format "%s %-12.12s %-12.12s %-20.20s %-32.32s" (81 chars).
6. Choose the **Select Printer** button to open the *Print Setup* dialog.
7. Select a suitable printer type from the list displayed in the **Name** drop down box.
8. From the (Paper) **Source** drop down box, select the paper source.
9. Select the paper orientation.
   - **Portrait**: Select this option if you are using an 80 column printer.
   - **Landscape**: Select this option if you are using a 132 column printer, and have ticked the **132 Column** check box in the *Setup Global Printers* dialog, or if you are using a laser printer and want a wide audit trail printout.
10. Choose the **OK** button to return to the *Setup Global Printers* dialog.
11. Choose the **Apply** button.

⇨ The columns that will appear in the Audit Trail printout may not be altered. They are as outlined in the section that follows.

⇨ Once the setup for Audit Trail printing has been completed, the system immediately begins to pass the Audit Trail events to the line printer as they occur.

1.3.2.1 Audit Trail Printing Columns

The following table lists the columns available for Audit Trail printing. These columns cannot be modified.

Column	Description
Type (of Message)	Indicates whether the displayed message is a Normal or Alarm message.
Date Occurred	Displays the date of the Audit Trail event
Time Occurred	Displays the time of the Audit Trail event
Location	Displays the location where the Audit Trail event took place.
Message	Displays the contents of the Audit Trail message.

1.3.2.2 Viewing the Contents of the Printer Buffer

You can view the contents of the buffer by using the **Print Preview** option.

- From the **File** menu, choose **Print Preview**.

⇨ The contents of the buffer will now be displayed.

The printed version provides you with an alternative “hard-copy” backup of the Audit Trail.

1.3.3 Plan Printing

Plan Printing is unique in that SiPass integrated supports many different drawing formats, both in physical size and file type, as well as different printer technologies. Sending plans and drawings to the appropriate printer / plotter will produce outputs at the correct size and scale, making them more manageable and their interpretation easier. Sizes range from A4 up to A0.

The supported technologies for plan printers and plotters include the following Windows-compatible technologies:

- Pen Plotters,
- Inkjet Printers
- Bubble jet Printers
- Laser Printers
- Electrostatic Printers

1.3.3.1 Configuring a Site Plan Printer

A site plan printer allows you to generate paper copies of your site plans. These are very useful for introducing new staff to the site, as well as organizing and coordinating Guard Tours.

1. From the **File** menu, select **Print Setup** to display the *Setup Global Printers* dialog.
2. Choose the *Site Plan Printer* tab. If you wish to nominate another Plan printer as the default, choose the **Select Printer** button to open the *Print Setup* dialog.
3. Make the necessary changes to the printer settings. For further information concerning the setup options, refer to the printer manuals.
4. Choose the **OK** button to return to the *Setup Global Printers* dialog.

1.3.4 Report Printing

Report printing is a vital aspect of the SiPass integrated access control system. It can assume one of three general types:

- Audit Trail Reports
- Database Reports
- Log Book Reports

Although their content is different, these reports essentially are created and configured the same way. Therefore, a single printer can be used for all three types of reports, subject to site-specific considerations such as network traffic, and the volume and frequency of reports that are required. Virtually all reports are printed as standard A4 size documents. This means that the installation of printers and the printer drivers are generally straightforward tasks, since most A4 printers now install under the “Plug and Play” scenario.

1.3.4.1 Configuring a Report Printer

▷ If you are connecting directly to a SiPass client, ensure that you have installed the appropriate printer driver.

1. From the **File** menu, select **Print Setup** to show the *Setup Global Printers* dialog.
2. Select the *Reports Printer* tab.
3. If you wish to nominate another Reports printer as the default, choose **Select Printer** button to open the *Print Setup* dialog.
4. Make the necessary changes to the printer settings. For further information, refer to the documentation that came with your printer.
5. Choose the **OK** button to return to the *Setup Global Printers* dialog.

2 System Components

The SiPass integrated system monitors and reports vital information regarding events that occur at your site. Before SiPass integrated can do this, the system must be programmed with details about the layout and the hardware structure of the site.

The components that you will create when commissioning your site will depend on the type of installation you have.

A brief overview of the SiPass ACC Series components is in the following table:

Component	Description
Server	The Server is the foundation to which all other components connect.
Ethernet Comms	This is the communications channel that the Server uses to communicate with an ACC Controller. Communication by Ethernet eliminates the need to install an access bus at installation time.
ACC Controller	The SiPass Central Controller sends and receives messages to and from the Server and the hardware devices that monitor your system.
FLN Connection	Each hardware device in the SiPass integrated system communicates with an ACC by a Field Level Network connection.
Devices	A device is a hardware component that controls the physical operation of the SiPass integrated system. It may, for example, control access to lifts, elevators, and fire exits, or it may be a component for controlling intrusion detection devices.
Points	Points belong to devices. They make up the basic hardware components of the system and can be anything from locks and infra-red sensors to card readers and floors.
Groups	Groups are collections of points. They allow the control of many points that share some commonality, as if they were a single entity. The points in a group do not necessarily need to be in the same part of a building. Groups are especially useful for controlling cardholder access.

2.1 The Behavior of Components Offline

When communications between ACC units and the SiPass Server are disabled, several factors have to be taken into account. It is important that database changes be stored while offline and downloaded quickly to controllers when communications are restored, but it is equally important that commands to components like doors and input points are NOT executed at online time.

For example, in a high-security facility, a set of commands to open doors is sent while ACCs are offline. Two hours later when communications are restored, the delayed open door command is executed, probably at a time that is extremely inappropriate. To prevent this, any manual command, Event Task Effect or site plan command sent to an offline ACC unit will result in a “Command Failed” message immediately being sent to the Audit Trail. This message will be received for each point involved; for example, if a disable command is sent to an offline point group, a Command Failed message will be received for each point in the group.

If a command is sent to both offline and online ACCs, devices or points, the commands to the online components will be executed and a Fail message will be received for each offline point. For example, a point group may contain points connected to different ACC units.

This scenario applies to Host-based commands only. Controller Event Task messages between ACCs are not buffered, so peer-to-peer commands, sent when inter-ACC communications are disabled, will simply fail when no reply is received.

2.2 Server Properties

The Server is the main component in your system. All the components used in the SiPass integrated system are ultimately connected to the Server. Each SiPass integrated system can only have one Server, but may have many Clients (depending upon the license agreement).

By default, the Server name will be the same as the name of the computer on which the Server software has been installed.

To change the Server Name:

1. Choose **Components** from the **System** toolbar or menu.
2. Select the **Server**.
3. Change the name of the Server, by typing a new name into the **Server Name** field.
4. For SiPass integrated to operate correctly, the Server name must match the name of the PC on which the server has been installed.
5. Click **Save**.

2.3 Ethernet Comms

The Ethernet Communications channel connects the Server to the advanced Central Controller (ACC), and allows communication between the Server and defined devices and points.

Communication by Ethernet means that a dedicated Bus does not have to be installed, because both Windows and the ACC understand TCP/IP. TCP/IP is a protocol used to send and receive messages over Ethernet networks.

The number of ACCs that can be connected to a single Ethernet Comms channel is limited only by:

- The number of IP addresses available on the local network on which the ACCs are located
- The connection speed.

In the SiPass integrated component hierarchy, the Ethernet Comms is a “child” item of the Server, and is automatically assigned the name “ACC Controllers”. This name cannot be changed.

2.3.1 Setting the Ethernet comms

Setting the Ethernet communications channel involves allocating a maximum number of cards per ACC and deciding whether a PIN code is required at access points connected to this channel.

1. Choose **Components** from the **System** toolbar or menu.
2. Select the Server in the left hand pane.
3. Underneath the Server you will see the Ethernet communications channel, called “ACC Controllers”. Select this.
4. Set the default port number. The default **Port No.** is 4343. This value may be changed if required; for example, if the port number is already being used by another application.

If the Port No. is changed, you will need to update the Port No. for every ACC connected to this Ethernet Comms, using the ACC configuration software.

A port number is a logical address in a TCP/IP connection and should only be assigned or addressed by an experienced IT administrator. Two additional read-only fields also appear and supply information selected during the SiPass integrated installation

Facility Code: The default facility code for access cards at this site

Card Technology: The default type of card used for access

5. Change the maximum number of facility cards permitted per ACC, if required. The default is 25,000.
6. The **PIN Code Required** and **PIN Code digits** fields are read only fields. These fields are defined in the System Preferences dialog. Please refer the section General Tab of this user manual.

If you are using a SIEMENS RS485 reader, the PIN length can be set to 6 digits.

7. Specify the **ACC Alive Poll Time (s)** that the server will wait between successively polling the ACC to check it is online. Default is 5s.
8. Specify the **ACC Response Time (s)** that the server will wait to receive a response from the ACC before triggering a 'No Response' event, declaring the ACC to be offline. The default time is 5 seconds.
9. Specify the **Bus Delay to send Time (ms)**
10. Configure the **Disable Daylight Saving on all units** checkbox, as required. The operator can change the state of the box to either the ticked, or unticked state only. A highlighted / filled checkbox is only a display state of the ACC units under that particular controller.
    - A ticked checkbox implies that all ACC units under this controller have disabled Daylight Savings.
    - An unchecked box implies that all the ACC units under this controller have enabled Daylight Savings.
    - A highlighted / filled checkbox implies that only some ACC units under this controller have disabled Daylight Savings, while others have left it enabled.
11. Click **Save**.

2.4 Adding an ACC

The Advanced Central Controller manages communication between devices and points in your system and the Server. Adding an ACC involves assigning it a name and Time Zone and entering the unit Serial Number.

1. Choose **Components** from the **System** toolbar or menu.
2. Select the **Server** in the left hand pane.
3. Select the ACC Controllers communications channel.
4. Click the **New Unit** button.
   ⇨ A new ACC will appear connected to the comms channel and a new tab will be available.
5. Enter the name of the ACC unit into the **Unit Name** field. This name must exactly match the name used when configuring your ACC.
6. Select the correct time zone for your ACC's region from the **Time Zone** drop-down box.
   – Select the alarm definition that will apply to this ACC from the **Alarm Definition** drop-down box.
7. Select the type of unit being connected from the **Unit Type** drop-down box. The types of units listed in this drop down box are as follows:
   – ACC
   – ACC-Lite
   – ACC-4
   – ACC-8
   – ACC-16
   – ACC-32
   – ACC-Granta
8. Select a **Backup mode** for ACC database.
   – **None**: No backup mode applied. To ensure database Integrity after power loss, an event task must be configured to auto initialize the ACC for operation.
   – **On-Board Flash**: The ACC database will be backed up locally using the on-board flash.
9. Enter the serial number of the ACC into the **Serial Number** field.
   ⇨ The serial number will have been issued with the ACC unit (should be printed on the sticker on the ACC). The Unit No. will be automatically assigned.
10. Enter a desired description for the ACC into the **Description** field.

An operator can enter an alternate name or number for the device, to the internal name that is already provided for the device. i.e., while the internal name of this device is an ACC, an operator can enter a number or name that helps operators or maintenance personnel identify the device in their site.

This description will be preserved during backup and restore of the system.

Further, this description field can be used as a filter field while generating reports in SiPass Explorer. This assists operators search for reports using this field as a filter.

Once configured and saved, this field can be still be modified. Audit Trails and Reports will reflect changes to Device Descriptions appropriately.

11. Choose the appropriate operation checkbox options, as described in the section ACC Configuration Options [→ 29].
12. Click **Save**.

2.4.1 ACC configuration Options

The options available are explained in the table below.

Option	Description
Disable Power Monitoring	Tick this checkbox to disable reporting of power failures at the ACC.
Disable Communications	Tick this checkbox to disable all communications between the ACC and the Server. The ACC will effectively be offline.
Disable Tamper	Tick this checkbox to disable reporting of any wire tampering detected on supervised wires. This tab also contains read-only fields in the Statistics section:
Disable Telnet	Tick this checkbox to disable the ability to connect a telnet session with the ACC. If you have already done this via the ACC, the checkbox must still be ticked to ensure that the ACC continues to ignore telnet requests.
Disable Daylight Saving Time	Tick this checkbox to disable the Daylight Saving Time feature for this ACC unit only.
IP Address	The IP address of the ACC Controller.
Version	The current version of the firmware loaded onto the ACC.
Status	Status of the comms channel between the ACC and the Server.
Refresh	This button will update the data in the Statistics section.

2.4.2 ACC-Granta

ACC-Granta is the new hardware that is being used along with SiPass integrated.

The following rules apply if the user wants to change the hardware from ACC-Granta to any other type of units:

1. ACC-Granta can be converted to ACC-Unit only if FLN 4 is not configured.
2. ACC-Granta can be converted to ACC-lite only if FLN 1 is configured with the type Access or Entro and FLN count is 1.
3. ACC-Granta can be converted to ACC-4/8/16/32 only if FLN-1 is configured with the type Entro and FLN count is 1.

Other unit types cannot be converted to ACC Granta.

Modem Port Configuration

A modem can be configured on an ACC-Granta unit by selecting the **Enable Communication Redundancy** in the **Dialup/PP**P tab of the *Components dialog* box.

A modem can be configured only on FLN 1 on an ACC-Granta unit. If FLN1 is in use then a modem cannot be configured on the ACC-Granta unit. Also if the modem is configured on FLN1 then, FLN1 cannot be used for any other purpose.

2.5 FLN Connections

Devices are connected to an ACC by a Field Level Network connection, or FLN. There are four FLNs available per ACC. FLNs are numbered 1 through to 4, and FLN number 3 is further divided into FLN 3a and FLN 3b. BLN's and IS are now usable as FLN's. Each FLN is capable of connecting to 16 devices, so now you are able to connect a total of 96 devices per ACC.

Adding an FLN connection involves assigning it a name and number, and setting the baud rate.

1. Choose **Components** from the **System** toolbar or menu.
2. Select the **Server** in the left hand pane.
3. Select the ACC Controllers communications channel.
4. Select the ACC to which you want to configure an FLN connection.
5. Click the **New FLN** button.
   ⇨ A new FLN will appear connected to the unit and a new tab will be available.
6. Enter a name for the FLN into the **Name** field.
7. Select the number of the FLN Connection from the **Number** drop-down box.

If ACC-Granta is the type of ACC used, then FLN 1 to 4 are available for selection.

8. Select which kind of FLN you wish to add from the Type drop down box:
   - **ACC FLN Bus**: Select this to add an ACC device.
   - **Entro FLN Bus**: Select this bus to add SiPass Entro device.
   - **Granta FLN Bus**: Select this bus to add an ACC Granta device. A Granta FLN bus can be used only with FLN 4.
9. Click **Save**.

2.6 Devices

A device is a component that processes and transfers data between points and your SiPass server. Each device is capable of storing information in its own memory.

You can also set default settings for a device, so that when a new device is created it will automatically be configured to the default settings.

1. Choose **Components** from the **System** toolbar or menu.
2. Select the **Server** in the left hand pane.
3. Select the ACC Controllers communications channel.
4. Select the ACC to which you want to add a new device.
5. Select the FLN to which the Device will be connected.
6. Click the **New Device** button. A menu will appear showing a list of device types.

7. If you have selected an ACC FLN the following list of devices will appear:
   - ⇨ **ADD5100:** Dual Reader Interface (DRI)
   - ⇨ **API5100:** Input Point Module (IPM)
   - ⇨ **AFO5100:** Output Point Module (OPM)
   - ⇨ **ADE5300:** Eight Reader Interface (ERI)
   - ⇨ **AFO5200:** 8 Input /Output (8IO)
   - ⇨ **ATI5100:** Intrusion Arming Terminal (ATI5100)
8. If you have selected an Entro FLN the following list will appear:
   - ⇨ **DC12:** Single Door Dual Reader
   - ⇨ **DC22:** Single Door Dual Reader
   - ⇨ **DC800:** Single Door Dual Reader
   - ⇨ **PD30/PD40:** Single Door controller with built in reader
   - ⇨ **IOR6:** 4 Input / 6 Output Module
9. If you have selected a Granta FLN, the following list will appear:
   - ⇨ **4322–Cotag**: 2 Readers/4 Input and 2 Output Module
   - ⇨ **4422-Swipe**: 2 Reader/ 4 Input and 2 Output Module
   - ⇨ **4253-IO**: 16 Input / 8 Output Module
   - ⇨ **Backboard Device**: Zero input/zero Output/Zero reader points
10. Select the device type you want to add. A series of tabs will become available according to the device selected.
11. Enter a meaningful name for the device into the **Name** field.
12. Select the alarm definition that will apply to this device from the **Alarm Definition** drop-down box. A default device number will automatically be assigned in the **Device Number** field. You can change this by entering a new number into the field.

The valid device numbers for Granta FLN are as follows:

13. Tick the **Second Reader** checkbox if you want to enable both card readers on a DRI (DRI devices only).

To enable the second reader, the appropriate configuration must also be made on the *FLN Configuration* dialog. The operator needs to verify that the *Enable Second Reader* checkbox has been ticked on the Configuration tab of the *FLN Configuration* dialog.

14. Further, configure the required Reader Technology for the second reader on the same dialog.
15. Select the **Door Set** configuration for the reader- This will vary according to the reader selected. The table below specifies the different options available for each reader.
16. Click **Save**.

8IO	No selection available: the configuration for this device is pre-determined.
IPM	No selection available: the configuration for this device is pre-determined.
OPM	No selection available: the configuration for this device is pre-determined.
DRI	Dual Reader Door ; 2 Single Reader Doors, Turnstile single door contact, Turnstile dual door contact.

SRI	Single Reader Door ACC installation only.
ERI	8 single reader doors; 6 single reader doors and 1 dual reader door; 4 single reader doors and 2 dual reader doors; 2 single reader doors and 3 dual reader doors; 4 dual reader doors.
DC12	No selection available: the configuration for this device is pre-determined.
DC22	No selection available: the configuration for this device is pre-determined.
DC800	No selection available: the configuration for this device is pre-determined.
PD30/40	No selection available: the configuration for this device is pre-determined.
IOR6	No selection available: the configuration for this device is pre-determined.
4322-Cotag	2 Readers/4 Input and 2 Output Module
4422-Swipe	2 Reader/ 4 Input and 2 Output Module
4253-IO	16 Input / 8 Output Module
Backboard	Zero input/ Zero Output/ Zero reader points

Configuring a DRI reader as a turnstile

1. Repeat steps 1-10 as above (‘To Configure a device’)
2. Select **Turnstile Single door contact** or **Turnstile dual door contact**.
3. When configuring operational modes under the *Door Reader* tab, the **Double/Single Arming** mode will not be supported.
4. Click **Save**.

⇨ The device details will be saved in the system.

!	*NOTICE*
	IMPORTANT The turnstile will only operate under the ‘access control’ (i.e. Card badging) mode. If an operator or cardholder uses manual commands or event task effects on the turnstile, then these commands will override both access points in the turnstile, and they will act as two separate doors. The offline mode is also not supported in the turnstile.

2.6.1 Default Settings for Devices

SiPass integrated allows you to nominate particular settings as the default settings for a new device. You can save one set of default settings for each type of device available.

Setting default device settings from the Components dialog

1. Select **Components** from the **System** menu or toolbar.
2. Open an existing device record or create a new device record in the *Components* dialog.
3. The **Set Default** button will only be enabled after you have saved at least one device in the system
4. The **Default Device** settings only apply to devices created in the *Component* screen.

5. Change the settings according to your preferences. You cannot set defaults for device, reader, and point names.
6. Click the **Set Default** button.
   ⇨ A confirmation dialog will appear asking if you want your current settings for this device to be the default settings.
7. Click **OK**.

⇨ Any new devices of this type that are created will automatically be assigned the default settings.

SiPass integrated also allows you to nominate particular settings as the default settings for a device before you create the device. You can save one set of default settings for each type of device available.

Setting default device settings before creating a device

1. Select **Configure Device Defaults** from the **Options** menu.
2. Select a **Controller** and **Device** from the drop-down lists.
3. Change the settings according to your preferences. You cannot set defaults for device, access, and point names.
4. Click **Save**.

⇨ Any new devices of this type will automatically be assigned the default settings.

2.6.2 Discovering Devices

The FLN Configuration tool allows you to discover new devices.

1. Select **FLN Configuration** from the **System** menu.
2. Right click **Global settings** and select **Search Range**.
3. Click **Yes** to begin the search. The navigation tree will automatically expand and all new devices discovered will be displayed in blue.
4. Select a device to add to SiPass integrated.
5. Enter a meaningful name in the **Name** field.
6. Click **Save New Device**.
   ⇨ If you clicked the **Refresh Display** button to view the latest device information, wait for the operation to complete (till the information is displayed in the respective fields) before clicking the **Save New Device** button.
7. Click **Yes** to confirm.
8. Repeat steps 5-8 for each device you wish to add.
9. Click **Close** when you are finished to exit the FLN Configuration tool.

2.7 Points

When you create a device, any points associated with that device are automatically created and stored in the device's record in the **Components** dialog.

Or, if you create an Input Point Module (IPM) Device, the *Input* tab will contain a table of default inputs and the *Output* tab will contain a list of default outputs.

You then modify the settings for the input and output points that are actually connected to the device, by modifying values in the displayed table.

2.7.1 Defining Access Points

1. Choose **Components** from the **System** toolbar or menu.
2. Select the Server in the left hand pane.
3. Select the ACC Controllers communications channel.
4. Select the ACC and then the FLN connected to the device for which you want to define an access point.
5. Select the device containing the access point.
6. Select each of the *Reader* tabs in turn. These tabs will only be available for reader interface devices.
   - To disable Reader 2 of a DRI de-select the **Second Reader** checkbox on the *Devices* tab.
   - The reader will be given a default name in the Name field, which consists of the Device name appended with the access label (e.g. “Door 1 Reader 1”). You can change this by entering a new name into the field.
7. Select the alarm definition that will apply to this point from the **Alarm Definition** drop-down box.
8. Select how the reader should operate from the **Operation Mode** drop-down box.
   - See SiPass integrated *Reference Manual* for details of the different operation modes.
9. Enter the Facility Codes, separated by commas that this reader will accept into the **Multiple Facility Codes** field.
   ⇨ This field will only be enabled for facilities that have purchased the Card Technology “HID Prox 26-bit Multi-Facility” as part of their license. Tenants at your facility, if any, will also be permitted access at readers if they have a valid card and their card’s Facility Code is permitted at that reader. There is a maximum of 20 different Facility Codes permitted per reader. Also note that multiple Facility Codes are reader-specific; each reader may allow access to different Facility Codes.
10. Complete the following reader specific parameters:
    - The **Reset Reader Tamper** button will allow for a reader device to be manually reset after it has gone into tamper mode (Siemens RS485 readers only).
11. Click **Additional Access Method** Options to set up either a ‘Daily Code’ or ‘PIN as Card’ access.
12. Click **Host Verification** to configure host verification for this reader.
13. Click **Dual Custody** to configure Dual Custody for this reader.
14. Click **Intrusion Control** to configure intrusion controls for this reader.
15. Click **Save**.

A checkbox in the *Cardholder* dialog will record the “3 Wrong PIN” status of a card. A SiPass operator must disable this checkbox and save the record to re-enable to the card for use.

It is also important to note that the incorrect PIN entries do not have to be made at the same reader; three consecutive incorrect entries made at any readers defined for this SiPass Server will void the card.

2.7.1.1 Access point general configuration

The following configuration options are available.

Option	Description
PIN Timeout (sec)	The time in seconds that a cardholder has to enter a PIN on the keypad. The timeout begins once the first digit is entered, or a card is badged and the reader is set to Card and PIN operation mode. This function can also be used in an intrusion area under Double/Single arming mode. Under this mode, the PIN timeout field will specify the length of time in seconds between the double card badge that is necessary to arm an intrusion area. If double badging does not occur within the specified time, then the area will be disarmed.
Buzzer Period (sec)	The time in seconds that can be specified to the pre-alarm or door held state so that the buzzer will sound for a door held open at this allocated time. If a value of 0 is entered, the door state will be 'alarm' and it will buzz until the door is closed.
Void card after 3 wrong PIN entries	Tick this checkbox, if you want any card that enters a wrong PIN number three times at this reader to be temporarily voided. Each incorrect PIN entry is recorded in the Audit Trail, along with a "3 Wrong PIN – Card Voided" message. All subsequent attempts at entry with that card will result in a "3 Wrong PIN Void Card – Entry denied" message.
Remote Arming Terminal	Tick this checkbox if you want a point to be used as a Remote Arming Terminal. This checkbox will only be enabled for CX23 and Siemens RS 485 readers, and only when Double/Single arming is not selected under the Operational Mode drop down box. If Double/Single arming has been selected, then this checkbox will not be displayed.

2.7.1.2 Access point Host Verification Configuration

The following configuration options are available.

Option	Description
***Time out (sec)**	The time in seconds that the *Image Verification* dialog will wait for a response from an operator, before closing and allowing access to be re-tried.
Alarm Class	Select the alarm class that will apply to this point from the **Alarm Class** drop down box.
CCTV Sequence	The configured CCTV sequence to display when the *Image Verification* dialog appears on-screen.
CCTV Monitor	The monitor on to which to display the live image when entry is requested at reader configured for image verification.
Unit	Select the DVR unit from the **Unit** dropdown box.
Camera	Select a camera for the unit from the **Camera** dropdown box.
Preset (PTZ only)	Select the preset numbers for the camera.
Save Image Snapshot	Determines whether a snapshot is saved of the host verification image.
****Snapshot Delay**	The delay in seconds after the host verification event occurs and when the snapshot is taken.

Note:

* If the CCTV is used as a video source for Host Verification and creating a CCTV Camera Sequence; ensure that the Sequence Time specified in the **Delay (s)** field of the *Configuration – Sequences* tab of the *CCTV Configuration* dialog, is the same as **Timeout (sec)** specified in the *Host Verification* tab of the access point door reader in the *Components* dialog. If both these values are not the same, the CCTV Switcher may switch early to another Host Verification request. For more information on configuring a Camera Sequence, refer the section Creating a Camera Sequence [→ 185].

**If the CCTV is used as a video source for Host Verification, the default Snapshot Delay can be left as it is at 0 seconds. However, if the DVR is used as a video source for Host Verification and a longer time is expected to display the video, the default Snapshot Delay should be set to 3 seconds.

2.7.1.3 Access point Additional Access Configuration

The following configuration options are available.

Option	Description
Time Schedule	Select the time during which the additional access, like a Daily Code is valid.
Additional Access Method during Time Schedule	Determines which type of additional access you wish to configure. It will be in effect during the Time Schedule that was configured above.
Additional Access Method outside Time Schedule	Determines what additional access will be available outside the configured Time Schedule.
Current Additional Access Method	The additional access method currently in use on this reader. Click the refresh button to update this display.
***Daily Code**	The daily code for this reader. This may or may not be the same daily code used at other access points.
***Code No. of Digits**	The exact number of digits in the daily code. When specifying the number of digits to be used at the keypad, and you wish to create Controller Base Event Tasks on PIN entry, ensure that the number of digits specified is the same as 'Base PIN digits" under System Preferences.

***Please note that in order for the configuration to be saved successfully, settings in the *Additional Access Method Options* tab have to be saved with a clearly specified Daily Code, and Code No. of Digits. Such configurations cannot be saved with a blank Daily Code, while defining a reader interface module.

2.7.1.4 Access Point Dual Custody

Dual Custody is a way of securing resources so that two people are required before access is granted. This means that two cardholders, who have been configured for the Dual Custody, will need to badge their card at a specific reader for access to be granted.

There are three kinds of Dual Custody modes that can be configured for a door reader:

- **Standard**:
  If set to the Standard mode, any two cardholders with appropriate access will be allowed entry.
- **Supervisory**:
  If set to the Supervisory mode, one of two cardholders must be flagged as a Supervisor. Cardholders are marked as Supervisors by checking the **Supervisor** checkbox on the *Definition* tab of the *Cardholder* dialog.
- **None**:
  If the mode is set to None, it implies that Dual Custody has not been configured for that particular reader.

Using Self-Authorization at a Dual Custody Reader

A single cardholder who has Self-Authorization privileges will be able to gain access to doors configured for Dual Custody. In such a case, a second authorized cardholder is not required, and all dual custody rules are waived.

To configure a cardholder with Self-Authorization privileges, tick the **Self-Authorize** checkbox on the *Definition* tab of the *Cardholder* dialog, and save the cardholder.

The Self-Authorization feature works independent of the Supervisory mode, and can be enabled at any time. Further, both the Supervisory and Self-Authorize privileges can be applied to a card.

Dual Custody Rules for Single Readers

The table below explains the Dual Custody access rules that apply at a Single Reader. It details situations when access is allowed or denied, depending on the

Dual Custody privilege assigned to cardholders, and the Door Reader's configured Dual Custody mode.

With reference to the table,

Cardholder 1 => Refers to the first card to be badged at the Access Point

Cardholder 2 => Refers to the second card to be badged at the Access Point

Employee => Refers to a cardholder with Standard Dual Custody Access Privileges

Self-Authorized Employee => Refers to a cardholder with Standard Dual Custody Access Privileges + Self-Authorize privileges

Supervisor => Refers to a cardholder with Supervisory Dual Custody Privileges

Self-Authorized Supervisor => Refers to a cardholder with Supervisory Dual Custody Privileges + Self-Authorize privileges

Dual Custody Privilege of Cardholder 1	Dual Custody Privilege of Cardholder 2	Access Point	Access Status
Employee	Employee	Standard Dual Custody	Granted
Employee	Supervisor	Standard Dual Custody	Granted
Supervisor	Employee	Standard Dual Custody	Granted
Supervisor	Supervisor	Standard Dual Custody	Granted
Self-Authorized Employee	-	Standard Dual Custody	Granted
Self-Authorized Supervisor	-	Standard Dual Custody	Granted
Employee	Self-Authorized Employee	Standard Dual Custody	Granted
Employee	Self-Authorized Supervisor	Standard Dual Custody	Granted
Supervisor	Self-Authorized Employee	Standard Dual Custody	Granted
Supervisor	Self-Authorized Supervisor	Standard Dual Custody	Granted
Employee	Employee	Supervisory Dual Custody	Denied
Employee	Supervisor	Supervisory Dual Custody	Granted
Supervisor	Employee	Supervisory Dual Custody	Granted
Supervisor	Supervisor	Supervisory Dual Custody	Granted
Self-Authorized Employee	-	Supervisory Dual Custody	Denied
Self-Authorized Employee	Supervisor	Supervisory Dual Custody	Granted
Self-Authorized Supervisor	-	Supervisory Dual Custody	Granted
Employee	Self-Authorized Employee	Supervisory Dual Custody	Denied
Employee	Self-Authorized Supervisor	Supervisory Dual Custody	Granted
Supervisor	Self-Authorized Employee	Supervisory Dual Custody	Granted
Supervisor	Self-Authorized Supervisor	Supervisory Dual Custody	Granted

Rules for Single Reader Dual Custody with Anti-Passback

An Access Point that has Dual Custody enabled, can be assigned as an IN / OUT / Internal Reader to an Anti-Passback area.

The cardholders will be logged into the Anti-Passback area once the 2nd Card badge has occurred at the Dual Custody Access Point.

The Dual Custody reader for the Anti-Passback area will increment (or decrement) the area count by 2 after a successful Dual Custody access.

If an Anti-Passback area has a capacity limit enforced and cannot accept 2 more cardholders, the Dual Custody access may be denied.

Configuring a Door Reader for Dual Custody

1. Select **System > Components** on the menu bar.
2. Navigate to a specific Device on the Server tree hierarchy that you wish to configure for Dual Custody.
3. Select a specific *Door Reader* tab of this device.
4. Select the *Dual Custody* tab.
5. Configure a required **Time Schedule** used for Dual Custody configuration.
6. From the **Dual Custody when Time Schedule On** drop down list, select the Dual Custody mode in effect when the Time Schedule is active.
7. From the **Dual Custody when Time Schedule Off** drop down list, select the Dual Custody mode in effect when the Time Schedule is not active.
8. In the **Dual Custody Timeout (sec)** field, configure the maximum time allowed (in seconds) between the first and second cardholder's card badge. If the second card is presented after this timeout expires, it is treated as a separate card badge. By default, the Dual Custody Timeout is set to 20 seconds.
   ⇨ The **Current Status** field will display as **Standard**, **Supervisory** or **None**, depending on the Dual Custody status of the door reader.
9. Click the **Refresh** button to refresh the present status of the reader.

In order to enable a reader for the Dual Custody mode, the door has to be set to the DOOR CLOSED state. If the door contact is in an Alarm condition, or if the door is open, the reader will be disabled. Further, Dual Custody will not work on a reader that has already been configured for Elevator Control, or an Intrusion Arming Terminal.

10. When the **Always Self-Authorize** checkbox is left un-ticked, the general Dual Custody rules (as explained in previous sections) are applicable. However, when this checkbox is ticked, the following set of rules are applicable:

- **For Access with a Single Card Badge, the Cardholder must have Self-Authorize Enabled**

User Scenario: An employee that has **Self-Authorize** enabled, but **Supervisor** disabled, will be granted access at a reader that is configured for Supervisory Dual Custody.

1st Card Badge	2nd Card Badge	Access Point Configuration	Access Granted/Denied	Always Self-Authorize
Employee*	X	Supervisory Dual Custody	YES	Enabled
Supervisor*	X	Supervisory Dual Custody	YES	Enabled

With reference to the table above;

Employee* refers to a cardholder with Standard Access Privileges with Self-Authorization

Supervisor* refers to a cardholder with Supervisory Dual Custody Privileges with Self-Authorization

X implies that no card has been badged

- **For Supervisory Dual Custody Access, the first card badged must have 'Self-Authorize' disabled**

1st Card Badge	2nd Card Badge	Access Point Configuration	Access Granted/Denied	Always Self-Authorize
Employee	Supervisor	Supervisory Dual Custody	YES	Enabled
Employee	Employee*	Supervisory Dual Custody	NO	Enabled
Supervisor	Employee	Supervisory Dual Custody	YES	Enabled

With reference to the table above;

Employee refers to a cardholder with Standard Access Privileges

Employee* refers to a cardholder with Standard Access Privileges with Self-Authorization

Supervisor refers to a cardholder with Supervisory Dual Custody Privileges

- **Turnstiles that have Supervisory Dual Custody enabled require that the 2nd card badged MUST be a Supervisor**

This rule applies regardless of whether the card badged first was a Supervisor or a Non-supervisor.

1st Card Badge	2nd Card Badge	Access Point Configuration	Access Granted/Denied	Always Self-Authorize
Employee	Supervisor	Supervisory Dual Custody	YES	Enabled
Employee	Employee*	Supervisory Dual Custody	NO	Enabled
Supervisor	Employee	Supervisory Dual Custody	NO	Enabled

With reference to the table above;

Employee refers to a cardholder with Standard Access Privileges

Employee* refers to a cardholder with Standard Access Privileges with Self-Authorization

Supervisor refers to a cardholder with Supervisory Dual Custody Privileges

Dual Custody Rules at a Turnstile

Turnstiles that have the Supervisory Dual Custody feature enabled, require that the 2nd card badged at the reader MUST be a Supervisor. This is regardless of whether the card badged first was a Supervisor or a Non-Supervisor.

As a result, the following rules apply:

- If a Supervisor badges first, and a Non-Supervisor badges next, access will be denied.
- If a Non-Supervisor badges first, and a Supervisor badges next, access will be granted.
- If a Supervisor badges first, and another Supervisor badges next, access will be granted.

Only ONE person will be allowed to enter at a turnstile when access is granted.

- If access is granted (as per the rules explained elbow), only the first cardholder will be allowed to enter. This action will be reported as a **Valid Card** entry in the audit trail. The second cardholder will be reported as **Cardholder did not enter**.

Manual Override Commands for Dual Custody

Manual commands enable various Dual Custody modes for specific access points. When the Dual Custody manual command is submitted, it overrides the current operating mode.

The following are some of the Manual Override commands available for Dual Custody:

- Restore Dual Custody Configuration Mode
- Set mode ‘No Dual Custody’
- Set mode ‘Standard Dual Custody’
- Set mode ‘Supervisory Dual Custody’

These manual commands to enable various Dual Custody modes for a specific point are also available as Access Point ‘Effects’ for both Controller and Host Event Tasks.

2.7.1.5 Access point Intrusion Control Configuration

The following configuration options are available.

Option	Description
Terminal Device	The terminal device used for Intrusion Control
Time Schedule	The Time Schedule controlling when the Intrusion Control is active
Current State	The current state of the Intrusion Control

2.7.1.6 Access point Programmable Authorization

The following configuration options are available.

Option	Description
Timeout (ms)	This field specifies the time-out period set for authorization. The field becomes enabled when the Programmable Authorization operation modes are selected for the reader device. If a card is badged, and authorization takes longer than the timeout period set in this field; the card will be denied access and an appropriate audit trail message will be displayed. The default value of this field is 0.

2.7.2 Defining Input and Output Points

1. Choose **Components** from the **System** toolbar or menu.
2. Select the Server in the left hand pane.
3. Select the ACC Controllers communications channel.
4. Select the ACC and then the FLN connected to the device for which you want to define an input or output point.
5. Select the device containing the point.

6. Select the *Input/Output tab* if you are modifying a card reader device, or either the *Input* tab or the *Output* tab if you are modifying an Input Point Module (IPM).
   - ⇨ Input points and Output points for devices are listed in the table below. You can change the properties of a point by clicking in a cell and either entering a new value or selecting from a drop-down list.
   - ⇨ Latch allows you to configure the length of time that the door lock will remain unsecured after the door has shut.
7. Choose the **Save** button when you have defined all the necessary points.

Input Points

Property	Description
Point Name	The name of the point. This is the name that will be assigned to alarms.
Alarm Definition	The alarm class of the input point.
Time Schedule	The Time Schedule during which the input point is enabled or disabled.
Operation Mode	This specifies how the point should operate as part of the security system (depends on the type of input point associated with the selected device). In case of REX input , the Operation Mode options are: • **Passback** • **Passback No Message** • **Passback No Report** - Lock Not Activated • **Passback Report** - Lock Not Activated • **Input Disabled** **Note:** When the Passback No Message input mode is set, the behavior changes with the associated Time Schedule as described below: • **Time Schedule is ON and Passback input takes place:** The latch is unlocked for the defined access time without any message reported in the audit trail. • **Time Schedule is OFF and Passback input takes place:** The latch is unlocked for the defined access time and a Passback Triggered message is reported in the audit trail. If you do not wish to have any message at all times, set the Time Schedule to *Always* (point unsecure).
Input Delay	This specifies the length of time before an alarm will be reported (exact operation dependant upon mode set).
Shunt Delay	This specifies the length of time that a door monitor will remain disabled after a door has been opened, before a “Door Held” alarm is registered (exact operation dependant upon mode set).
Pre-Alarm Delay	This is an initial delay after an alarm event has occurred, which can trigger a low priority warning instead of a high priority alarm.
Invert Input	This option reverses the input of the point. Alarm events become restore events and so on.

Output Points

Property	Description
Point Name	The name of the point. This is the name that will be assigned to alarms and events and appear in the Audit Trail.
Time Schedule	The Time Schedule during which the output point will be able to be activated.
Alarm Definition	The alarm class of the output point.
Delay 1	If the Delay 1 field is set to zero, the output point will operate in Pulse mode.
Delay 2	This delay is used for special accessibility.

2.8 Device Firmware Download and Configuration

When a new firmware device is added to the system, the initial configuration of the device is essential to ensure that it will work correctly with the SiPass integrated software.

1. Select **FLN configuration** from the **System** menu.
2. Select the *Mifare Smart Card Configuration* tab.
   ⇨ Under the Smart Card Configurations panel, the smart cards that have been added will be displayed.
3. To configure a new smart card, select **Add**.
4. Fill out the following fields:
   - **Configuration Name**: Enter a unique name for the new smart card configuration.
   - **Sector (1-15)**: Enter the sector on the smart card in which access data is stored.
   - **Block (0-2)**: Enter the block containing the sector into which access data is stored.
   - **Encryption Key**: Enter an encryption key for the smart card. It must be 12 characters in length and in Hexadecimal. Hexadecimal numbers use the digits 0-9 and letters A-F.
   - **Confirm Key**: You will need to re-enter the Encryption key to confirm it.
5. When you have entered all the details, select **OK**.
   ⇨ A confirmation dialog will appear asking you if you want to add the configuration to the database.
   ⇨ The Smart Card configuration details will now appear on the **Smart Card Configurations** panel.
6. Click to expand the **Global Settings** option on the left hand side panel of the dialog. A list of all your ACC Controllers will appear. Click on it to expand the tree and view the units connected to each controller.
7. By clicking and highlighting each unit, an ACC Details tab will appear displaying the following fields:
   - **Name**: This will display the name of the selected unit.
   - **IP Address**: This will display the IP address of the selected unit.
   - **Serial No.**: This will display the Serial number of the selected unit.
8. Expand the plus symbol on the tree view for the desired unit to display the FLN Channels connected to that unit.
9. Select the FLN channel from the list that you wish to configure.
   ⇨ The following details will be displayed on the right hand side panel, under the tab *FLN Details*.
10. Set Device Number will display the following tables:
    - **Device S/N**: This will display the device's serial number
    - **New Device Number**: This box will allow you to set a new device number for the selected FLN Channel. Click on the up and down buttons to select the new number you wish to allocate.
11. Once you have entered the new details, click on the **Set Device Number** button which will save your changes.
12. In the **Clear Device Number**, select the **Device number** of the device to be cleared. Click the **Clear Device Number** button.

13. Click on the **+** symbol next to the selected FLN Channel to expand the tree.
    ⇨ The current devices you have installed will be displayed.
14. Select the device you wish to configure.
    ⇨ The tabs **Device Details** and **Configuration** will be displayed on the right hand side panel. The fields of the tabs are explained in the tables below.
15. To check that the information was stored on the device, select **Refresh Display**.
16. Click **Save**.
    ⇨ If you clicked the **Refresh Display** button, wait for the operation to complete (till the information is displayed in the respective fields) before saving.
17. If you have made any errors or to go back to the previous settings, select **Set Display to Last Default** to undo any changes that have been made.

Device Details Fields

Fields	Description
Name	This will display the name of the device.
Device Number	This will display the device number. Use the up and down arrows to select a number and click on Set to save.
Model	This will display the model type of the device.
Revision	This displays the Hardware revision given to the device.
Serial Number	This will display the device Serial number.
Hard Reset	Select this option to perform a complete hardware reset, all values on the device will be reset.
Soft Reset	Select this option to report all input states only, no outputs will be reset.
Drop to BootRom	Use this function to reset the hardware to its original operating system before it begins loading the specified firmware application.
Run Application	Use this function to reverse the drop to BootRom. This will call upon the hardware to run on the current application in the firmware.

The buttons **Hard Reset, Drop to Bootrom, Run Application** and **Download Firmware** are applicable only to Backboard device and are not enabled for the 4322-Cotag, 4422-Swipe and 4253-IO devices.

The DC12, DC22, IOR6 and DC800 devices are not supported for selection at input points. These are available only for Alarm/Normal operation modes.

Configuration Tab Fields

Fields	Description
Reader Technology	From the Reader 1 dropdown box, select the reader type that has been installed. Repeat this step if there's more than one reader, up to 8 readers can be selected.
Inputs	Select from Monitored and Unmonitored inputs for the device.
Local Output follows Local Input	Select this output if you want the output on the device to follow the local input.
Reader LED's	Select from ZAP for Asia Pacific, or ZAM for North America.
Reader Tamper Auto Reset	Select Yes or No whether you would like the device to reset itself after the reader has been tampered (Siemens RS485 readers only).
Mifare Smart Card Configuration	Select the Configuration from the drop down box. This corresponds to the smart card configuration settings. The Sector and Block will display the matching values to the configuration that has been chosen above.

Granta Specific Configuration Tab Fields

Fields	Description
Inputs	Select from Monitored and Unmonitored inputs for the device. This configuration is available on Granta I/O modules.
Enhanced Read	Tick to enable Enhanced read check on Cotag cards. This configuration is available on Granta Baseboard devices.
Parity Check	Tick to enable Parity check on Cotag cards. This configuration is available on Granta Baseboard devices.
Cotag Reader holdoff time	Enter value between 0-255 to set the holdoff time (in tenths of a second) for all Cotag readers. This configuration is available on Granta Baseboard devices.
Repeat transaction delay	Enter a value between 0-255 to set a repeat transaction delay (in seconds) for all Cotag readers. This configuration is available on Granta Baseboard devices.

2.8.1 Creating a Custom Card Format

The following instruction explains how to create a custom card format from the *FLN Configuration* dialog.

1. Select **FLN configuration** from the **System** menu.
2. Select the *Custom Card format* tab.
3. Select **Add**.
4. Complete the following fields:
   - **Name**: By default, the name will match the custom card format stored in the SiPass integrated database. This can be changed to any desired name.
   - **Total Length**: The total number of bits contained in the card. This can be increased by extending the end of the bar and moving it right or left, either to increase or decrease bit length.
   - **Number**: The range of bits that will be used to specify the card number within the card. It can be increased by extending the end of the bar and moving it right or left; the box can also be dragged along to change the range. To change the MSB (Most Important Bit), double-click on the box or right-click with your mouse.

- **Facility**: This represents the facility that is currently selected by the tenant in SiPass integrated, and depicts how the bits of the card are interpreted.
- **Facility Addition**: Check this box to add an additional facility to the card.
- **Revision**: Check this box to incorporate the revision of the card.
- **Even Parity**: Select this function to validate the card where the parity bits are checked for even number of bits.
- **Odd Parity**: Select this function to validate the card where the parity bits are checked for an odd number of bits.

5. To save the changes, select **OK** or to have the changes take effect straight away, select **Apply**.
   ⇨ The *Custom Card* dialog will close down, and the *Custom Card Format* tab will appear.
6. If you have finished adding profiles, select Close. Alternatively, to update or change an existing card format, select it from the list and click on **Update**.

2.8.2 Configuring Reader Interface Offline Modes

Offline modes control how the reader interfaces behave when disconnected from the ACC.

You can define Offline Access Groups by selecting **Program > Offline Access Group**.

If the device firmware does not respond, or support the Offline mode, a message will be shown warning you that this is the case. You will need to upload the latest firmware.

Setting offline modes

1. Select **FLN configuration** from the **System** menu.
2. Click to expand the **Global Settings** option on the left hand side panel of the dialog. A list of all your ACC Controllers will appear. Click on it to expand the tree and view the units connected to each controller.
3. Select the desired reader interface unit to be configured.
4. Select the *Offline Mode* tab.
5. Select a **Door Set** to use when in Offline Mode from the dropdown list.
6. Select the **Offline Mode** for each available door from the dropdown list. You may need to scroll the Offline Door Configuration section to the right to see the dropdown list.
7. Set the time delay in hours, minutes and seconds in **Activation Delay**. Activation Delay is the time after going offline before initiating Offline Mode.
8. Configure your **Offline Mode**.
   - If one of the Card or PIN modes is selected, you can pick a specific **Offline Access Group** by clicking the … button. There is a default group that will be assigned if you do not select one.
   - If “Card and PIN” mode is selected you can set the PIN timeout to control how long a cardholder has to enter a PIN after badging their card.
   - If Facility Access is selected a list of facilities (up to 20) which will be granted access when presented to a door that is running ‘facility access’ mode is visible under Allowed facilities. To enter a facility code , click inside the **Allowed facilities** box and add the codes separated by a comma (Maximum twenty (20) codes allowed). For example: Adding the codes‘7,9’ will allow users whose cards have the facility numbers, 7, and 9 will be able to open the door.
9. Click **Save**.

!	*NOTICE*
	• Entro devices do NOT store audit trail when in Offline Mode. • The SRI / DRI / ERI can store events, so that when the device goes back online the messages will be displayed in the Audit Trail. • The number of doors configured to a device, do not make any difference to the storage requirements for events. • If the door is opened and closed, it will also store a DoorFrame opened and closed message. • The DRI/SRI has a relatively small storage size, and has a limit of 212 Card events + Door open/close events that it can store in the offline mode. • The ERI has a larger memory size, and has a limit of 1668 Card events + Door open/close events that it can store in the offline mode. • If the Passback button is pressed, it is considered a single input event, like a door open/close. In this mode, up to 710 input events (state changes) can be stored in a DRI/SRI; and up to 5630 input events (state changes) can be stored in an ERI.

Offline Mode Table

Mode	Description
Disabled	The device is disabled and there will be no change in state.
Unlocked	The door will unlock when device goes offline.
Facility Access	The door will grant access to any cardholder whose facility matches those specified in ‘Facility Access’.
Locked	The door will remain locked when device goes offline.
Card	The door is locked but pre-programmed cards can still gain access. The Passback on the door also functions.
PIN	The door is locked and card badges are ignored. PIN entry from pre-programmed cardholders with “Card as PIN” enabled will gain access. The Passback on the door also functions.
Card or PIN	The door is locked and card badges or PIN entry from pre-programmed cardholders will gain access. For the PIN entry to work the cardholders must have “Card as PIN” enabled. The Passback on the door also functions.
Card and PIN	The door is locked and in “Card and PIN” mode. Only pre-programmed cardholders can gain access and they must badge their card and enter the correct PIN. The Passback on the door also functions.

2.8.3 Configuring Siemens OSDP Readers

The instructions that follow explain how to configure Siemens OSDP Readers in SiPass integrated. Ensure that the required readers are displayed and configured correctly on the *Reader Firmware & Config* tab of the respective FLN on the *FLN Configuration* dialog.

1. Select **FLN Configuration** from the **System** menu.
2. Select the *Siemens OSDP Reader Configuration* tab.
3. Click **Add** to create a secure OSDP Key. The *OSDP Secure Key Configuration* dialog is displayed. This is where a secure key is created to allow encrypted communication between the controller and the reader. This is supported only for the Dual Reader Interface (DRI), which supports the encrypted mode.
4. In the **Name** field, enter a name for the secure key configuration.
5. In the **Encryption Key** field; enter a unique encryption key for the configuration.
6. In the **Confirm Key** field; re-enter the encryption key as in the previous step.
7. Click **OK**. The secure key configuration will be saved, and you will be returned to the *Siemens OSDP Reader Configuration* tab.
8. From the **Reader Firmware** box; select the reader for which firmware download is required.
9. Click **Add**.
10. The *Device Firmware Selection* dialog is displayed. Navigate to the location where the firmware update files are stored.
11. Select a file and click **Open**.
12. The opened firmware is displayed in the **Reader Firmware** box.
13. From the Global Settings tree on the left panel, select the specific reader device.
14. Tick the checkboxes of the reader and firmware to be downloaded.
15. Click the **Download Firmware** button of this dialog, and return to the *Reader Firmware & Config* tab.
16. Tick the checkbox corresponding to the reader to be selected.
17. Next, click the drop down list of the **Flash Firmware** button. Details of the options on this drop down list are as follow:
    - **New firmware and restart**: This option downloads the firmware, and restarts the OSDP reader immediately after download.
    - **New firmware only**: This option only downloads the firmware. The OSDP reader will not be restarted with this option.
    - **Restart reader**: This option only restarts the OSDP reader. Firmware will not be downloaded with this option.
    - **Note**: The three options listed above can be configured at the ACC, FLN, Device or Reader level. Depending on the level selected, all readers in the level can be chosen for firmware download/restart, or a specific reader/s can be chosen for the same.
18. The firmware image download process will be initiated. When complete, the selected reader and its firmware will be configured in the SiPass integrated system. Audit trails will reflect the configuration that was just performed.

2.9 Initializing Units

When a new ACC unit is added to the system, an initial data set needs to be downloaded to that unit. This is done through the process called initialization. Initialization may also be required when a configured unit is re-connected to the system.

ACC components must be online and communicating before they can be initialized

▷ Before you initialize a unit, you should define both the points that belong to the unit and the access control details for cardholders at those points.

1. Select **Initialize** from the **System** toolbar or menu. The *Initialize System* dialog will appear with list of all the units defined in the system will appear in the **Available** list.
2. Select the unit to be initialized by highlighting its name in the **Available** list.
3. Choose **Add** to add the unit to the **Selected** list.
4. Repeat Steps 2 and 3 until all the units to be initialized have been added to the **Selected** list.
5. Tick the **Initialization Options** checkbox to unlock the data component options corresponding to those elements to be downloaded during initialization.
6. Select each data element to be downloaded to the specified units by ticking the corresponding checkbox.
7. Choose **Full Initialize** to perform a full initialization of the selected units.
8. Choose **Compact Backup** to compact the data stored on an onboard flash backup card, if available, allowing more data to be backed up.
9. Choose **Image Download** to download Firmware to selected units.

2.9.1 Initialization Options

The following table lists the available options:

Option	Description
Memory	When ticked, the selected units will clear their memory on initialization.
Holiday	When ticked, all defined holidays will be downloaded on initialization.
Time Schedule	When ticked, all defined Time Schedules will be downloaded on initialization.
Point	When ticked, all information about the points that belong to the selected units will be downloaded on initialization.
Employee Access	When ticked, all cardholders' access control information will be downloaded on initialization.
Elevator	When ticked, all elevator data will be downloaded on initialization.
Event Task	When ticked, all controller-based event task data will be downloaded on initialization.
Intrusion Area	When ticked, all intrusion area information is downloaded to the unit.
Anti-Passback	When selected, all Anti-Passback area information is downloaded to the unit.
Download Expired Cards	When selected expired cards are also downloaded to the ACC.
Download all cards to all ACCs	When selected all cards are downloaded to all ACCs regardless of access privileges.

2.9.2 Creating an Initialization Event Task

You can create an event task to automatically perform a full initialization on an Advanced Central Controller after a unit has been reset; for example, after a power loss.

1. Select **Program> Event Tasks > Controller toolbar**.
2. Enter a name for the Initialization Event Task into the **Event Name** field.
3. Select the Time Schedule during which the event task will be able to occur.
4. Select **Unit** from the **Type** drop-down menu.
5. Select the ACC you want to be initialized after a unit reset from the **Controller** drop-down menu.
6. Select **Reset**.
7. Select **Unit** from the **Target** drop-down menu.
8. Select **Full Initialization** from the **Command** drop-down menu.
9. Select the ACC you want initialized from the **Location** drop-down menu.
10. Enter the message that will appear in the Audit Trail when the event runs, into the **Message** field.
11. Click **Save**.

2.9.3 Creating an Operation Mode Event Task

Operation mode changes can be triggered by an event task. For example, you may want the operation mode at a certain door to be Card Only during normal business hours, Card & PIN until midnight, and then Host Verification & PIN until the start of the business hours the next day.

1. Select **Host Event Tas**k from the **System** toolbar or menu.
2. Enter an appropriate name for the Event Task into the **Event Name** field.
3. Select the Time Schedule to trigger the mode change.
4. Select **Time Schedule** from the **Source1** drop-down box.
5. Select **Start** from the **State1** drop-down box.
6. Select **Access Point** from the **Target** drop-down box.
7. Select the mode that you want a reader to switch to, from the **Command** drop-down box.
8. Select the reader from the **Location** drop-down box.
9. Enter a message to be displayed in the Audit Trail when the Event Task occurs, into the **Message** field.
10. Click **Save**.

2.10 Dependencies Reports

The dependency report dialog appears while the user presses the ctrl key when attempting to delete any of the ACC, FLN or devices in the Component dialog.

The dependency report displays the various dependencies of ACCs, FLNs and devices in a tree structure.

The Dependency report contains the following newly added objects:

- Credentials
- Credential Schema
- Workgroups
- Guard Tours
- Guard Tour Groups
- Activities
- Flags
- Timers
- Counters

Devices in the *Components* dialog can now be deleted, without having to first remove the dependencies that have been configured to it.

The steps required to delete a device with dependencies, are listed below:

1. Open the *Components* dialog.
2. Navigate to the device to be deleted under the **Servers** tree hierarchy of this dialog.
3. Select the device, and click the **Delete** button.

A dialog box appears with the message, '**Are you sure you want to delete this item?**'

1. Press the **Ctrl** key on the keyboard, and click the **Yes** button of this dialog simultaneously. The *Dependencies Report* dialog appears.
2. Select the device to be deleted on this dialog, and click **OK**.
3. Next, click **Yes** on the subsequent dialog that appears.

You may be requested to wait while deletion is in progress. Do not close the application before this operation is complete.

The device will now be deleted from the *Components* dialog, and dependencies configured to it will be removed.

Devices in the Components dialog can also be Unlinked in the same way as deleting a device. Unlinking, removes the object from the various points that it is dependent on.

1. Open the *Components* dialog.
2. Navigate to the device to be deleted under the **Servers** tree hierarchy of this dialog.
3. Select the device, and click the Delete button.A dialog box appears with the message, '**Are you sure you want to delete this item?**'
4. Press the **Ctrl** key on the keyboard, and click the **Yes** button of this dialog simultaneously. The *Dependencies Report* dialog appears.
5. Select the device to be unlinked on this dialog and click **Unlink.**
6. Next, click **Yes** on the subsequent dialog that appears.

You may be requested to wait while deletion is in progress. Do not close the application before this operation is complete.

The device will now be unlinked from the *Components* dialog, and dependencies configured to it will be removed.

The ASP objects such as Activity, Flag, Timer and Counter do not allow unlinking or deletion if they are currently in use.

The dependency report also supports Operational Partitioning, which means different operators will have assigned rights that allow them to delete, edit or view the object accordingly.

If an operator does not have the assigned rights to edit/ delete/ view an object then SiPass displays an error message saying **"Insufficient Privileges to delete/edit/view the object"** accordingly.

3 Site Management

After you have created all the components at your site using the *Components* dialog, you must then configure the parts of the system that define how and when components operate.

3.1 Time Schedules

Time Schedules define when certain events should occur at your site. For example, cardholders can be denied access after business hours by creating a Time Schedule that gives them access during office hours only. The SiPass integrated system provides you with three pre-defined Time Schedules.

They are indicated in the following table:

Time Schedule	Description
Always (point unsecure)	Access at all times, including weekends and holidays - effectively, no access control.
Never (point always secure)	No Time Schedules defined. Access is never granted.
System Function (non busy intervals)	Access between 2:00 am and 3:00 am everyday including holidays.

3.1.1 Creating a Time Schedule

The SiPass integrated system allows you to created about 65,000 different Time Schedules, with a maximum of 20 independent time intervals defined for each Time Schedule.

1. Choose **Time Schedule** from the **Program** toolbar.
2. Enter a unique name identifying the Time Schedule into the **Time Schedule** field. You can enter up to 40 characters, in any combination of upper and lower case letters, and numbers.
3. Define the time intervals that will make up the Time Schedule.
4. To add the time interval to the **Defined Time Intervals** list, choose **Add**.
   - Time Schedules can also be defined by selecting the **Graph View** button. You may enter more than one time interval for each day. However, the start and stop times on any given day must not overlap
5. Click **Save**.

Creating a Time Schedule for a single day

1. Enter the name for your Time Schedule into the **Time Schedule** field.
2. Select **User Defined** from the **Day Type** drop-down list.
3. Set the **Start Time** to 12:00 am and **Start Day** to Monday.
4. Set the **Stop Time** to 12:00 am and **Stop Day** to Tuesday.
5. Choose **Add**.
6. Click **Save**.

Creating a Time Schedule using Graph View

1. Choose **Time Schedule** from the **Program** toolbar or menu.
2. Enter a unique name identifying the Time Schedule into the **Time Schedule** field. You can enter up to 40 characters, in any combination of upper and lower case letters, and numbers.
3. Select the **Graph View** Button.
4. Double-click to select the start day and time of your time interval and drag the cursor to create the Time Schedule.
5. To define further time intervals for the Time Schedule, repeat Step 4. However, keep in mind that the start and stop times on any given day must not overlap.
6. Choose **OK**.
7. The time interval will be created in the **Defined Time Intervals** list.
8. Choose **Save**.

3.1.1.1 Time Schedule interval definition

The following table explains the options available when defining Time Intervals.

Option	Description
Day Type	Specifies the days that the Time Schedule includes. There is no default day type. To select a day type, choose the drop down arrow and select a new type from the list. The following day types may be selected: • **Weekday**: Allows you to assign a start time and stop time for each weekday (Monday through Friday). • **Weekend**: Allows you to assign a start time and stop time for each day of the weekend (Saturday and Sunday). • **Holiday1**: Allows you to assign a start time and stop time for a single day. • **Holiday2**: Allows you to assign a start time and stop time for a single day. • **User**: Allows you to define a Time Schedule that nominates the start and stop days and the start and stop times for any day.
Start Day	Start day for a particular time interval. To select a start day, choose the drop down arrow and select a new day from the list. The start day is only available when the user day type has been selected.
Stop Day	Stop day for a particular time interval. To select a stop day, choose the drop down arrow and select a new day from the list. The stop day is only available when the user day type has been selected.
Start Time	Start time for a particular time interval. If there is more than one interval being defined, the time interval will start at this time on each day. The start time, by default, is 8:00 am. To change the start time, select the hours, minutes or seconds and use the up-down arrows to set the correct time.
Stop Time	Stop time for a particular time interval. If there is more than one interval being defined, the time interval will stop at this time on each day. The stop time, by default, is 5:00 pm. To change the stop time, select the hours, minutes or seconds and use the up-down arrows to set the correct time.

3.2 Point Groups

Point Groups are collections of points, floors, sub-groups, areas / sub-areas. Point Groups allow you to send a command to several points simultaneously, and ease the burden of assigning access control privileges to multiple points. A Point Group can only consist of points of the same type. A group cannot include a combination of input and output points.

When altering the properties or members of a group, care should be exercised due to the potential impact on the operation of the access control system.

If the changes are to take effect immediately, the system controllers must be re-initialized.

Usually, complex changes to point groups, such as the removal of individual points or changes to cardholder access control privileges are not immediately downloaded to system controllers.

3.2.1 Creating a Point Group

Creating a group involves assigning the group a unique number and specifying the group type, alarm class and members.

▷ Ensure that you have defined all the points, floors, sub-units or areas you will need to include in a group.

1. Select **Component Group** from the **Program** toolbar or menu.
2. Ensure **Point Group** is selected from the list.
3. Enter a unique name that identifies the group into the **Group Name** field. You can enter up to 40 characters, in any combination of upper and lower case letters, and numbers.
4. Click **Add Members**.
5. Select the group type by choosing the drop-down arrow on the **Group Type** field and selecting a type.
6. Select the name of the points you want to include in the group.
7. Click **Add >**.
8. Click **OK**.
9. Select the alarm class that best defines how the system should behave under certain (alarm) conditions. To change the alarm class, choose the drop down arrow and select a new alarm class from the list. To un-assign an alarm class, simply select the existing alarm class and press the **Delete** key on your keyboard. Do NOT click on the SiPass **Delete** button.
10. Configure the group alarm triggers.
    - **Count**:
      Specifies the number of group members that must be in alarm state, or have returned to normal but whose timers have not yet timed out, before the group goes into alarm. If 0 is entered, it prevents an alarm from occurring.
    - **Timer**:
      An internal timer starts counting (in seconds) for each member of the group that was in alarm after it returns to normal. The group goes into alarm if the number of points counting down or currently in alarm reaches the Group Count. If a point times out, the current count is decreased by one (which may cause the group to return to normal state). This means that if a certain number of group members have entered an alarm state simultaneously or within a configurable time interval, the group alarm will be generated.
11. Set the group actions.
    - **Isolate**:
      When checked disables the group alarm and normal messages, however individual member messages will still appear in the Active Audit Trail window.
    - **Clearance Required**:
      When checked, the member(s) that caused the group to enter an alarm state must be restored before the group can return to normal. If this box is checked, a group timer will be started every time a member returns to a normal state after registering an alarm. If this box is not checked, a group timer will be started every time a member enters an alarm state.
12. Choose **Save**.

!	*NOTICE*
	• The Group Type and Group Alarm Status fields indicate the type of members and the group's alarm status respectively. These fields do not appear until a group has been created. • When Point Groups are added to the system, it is essential that you update the Operator Group permissions to include them. Any time that changes are made to Groups, it is necessary to initialize the system after you have saved the changes for them to take effect • Deleting a group does NOT remove the individual points from the Database. Deleting a group may require other changes to the system. Because of this, removal of a group can make the Database inaccessible to other users for long periods and may impact on the performance of the system. • In relation to a Dial-up environment, because of the large number of commands generated by any changes to Groups, it is possible that an event task will be triggered to auto-download those changes to all the controllers in the system. This will depend upon the number of members in the group and the number of commands needed to trigger such an event.

3.3 Component Groups

In addition to Point Groups, you can create other groups to Partition Devices, FLNs, Units and Components in the same way. View, Edit and Create privileges to these groups can be then added to operator groups to control how the items in the group can be viewed and modified by operators. However, unlike Point Groups, these groups are used only for Operator Partitioning and are not functional groups.

By default whenever a new Unit, Device, FLN or Component it is assigned to the default group and the privileges assigned to the operator group that created it. However for greater control you can create your own groups to effectively manage your site.

3.3.1 Creating a Component Group

Creating a group involves assigning the group a unique name and specifying the members.

▷ Ensure that you have defined all the Devices, FLNs Units or Components you will need to include in a group.

1. Select **Component Group** from the **Program** toolbar or menu.
2. Select **Device Group**, **FLN Group**, **Unit Group or Component Group**.
3. Enter a unique name that identifies the group into the **Group Name** field. You can enter up to 40 characters, in any combination of upper and lower case letters, and numbers.
4. Click **Add Members**.
5. Select the name of the Devices, FLNs, Units or Components you want to include in the group.
6. Click **Add >**.
7. Click **OK**.
8. Click **Save**.

3.4 Operational States and Control States

The operational state of a point refers to its current location, or activity. For example, a door latch output point can be locked or unlocked. A PIR input point can be in an alarm or normal state

Points change their operational state in response to a number of things in SiPass integrated:

- Host Event Tasks
- Controller Event Tasks
- Manual Commands
- The normal events that occur at a facility, such as a valid card badge.

Each point in the security system is, at any given time, in a certain Control State i.e. it is under the control of one of the four command types above. For example, a door latch can be simply locked as dictated by the current Time Schedule and waiting for a valid card badge to unlock, or it could be locked by an operator sending a “Latch Lock” command via the Manual Command dialog.

In addition, there are two types of Event Tasks and Manual Commands: Permanent and Interruptible. A Permanent command is used for situations where you want to completely over-ride the current operational state of a point for a duration of time (including indefinitely). The point will not change state (e.g. unlock) until over-ridden by particular commands, which are explained in the next section.

An Interruptible command can be used for situations where you want to temporarily change the operational state of a point, but without interfering with normal access control. A point under Interruptible Command control will only change state in response to normal security and access events, or until another command (permanent or interruptible) is sent.

Differentiating between Permanent and Interruptible commands this way provides greater flexibility to the operator in controlling points at a facility.

3.4.1 Control State Priorities

In order to ensure consistency of operation within SiPass integrated, Control States must be given a priority. For example, it must be made clear that an Event Task with a Permanent Effect will not be overridden by a card-access attempt, but only by another Permanent Event Task. This avoids conflicts between simultaneous commands to points, as well as making access control even tighter.

These Control States and their priority are listed below. “1” indicates the highest priority.

Priority	Control State	Description
1	**Permanent Manual Command or Event Task**	A manual command or event task (Host or Controller) has been sent to a point and the **Permanent** option was selected. A point issued a Permanent Manual Command or Event Task will not change its operational state until: A new Permanent Event Task is sent to the point and the point is under Permanent Event Task control. A new Permanent Manual Command is sent to the point and the point is under Permanent Manual Command control. A “Cancel Permanent Action” command is sent to the point. A “Return to Time Schedule Control” command is sent to the point. The stated duration of the control state expires.
2	**Access/Internal Action**	A normal access or internal event that occurs at a point; for example, a card badge, or a PIR trigger. A point under Access/Internal Action Control Mode may remain in that mode for the defined period of time (e.g. a door is unlocked after a valid badge for the configurable delay period) or until one of the actions below: A Permanent Event Task or Command is sent to the point. A new internal or access event message is sent to the point; for example, a PIR input in alarm is restored by an operator. A “Cancel Permanent Action” command is sent to the point. A “Return to Time Schedule Control” command is sent to the point.
3	**Interruptible Manual Command or Event Task**	A manual command or event task (Host or Controller) has been sent to a point and the Permanent option was not selected. A point issued an Interruptible Manual Command or Event Task will not change its operational state until: A new Permanent Event Task or Command is sent to the point. A new Interruptible Event Task or Command is sent to the point. A new internal or access event message is sent to the point; for example, a PIR input in alarm is restored by an operator. The stated duration of the control state expires. A “Return to Time Schedule Control” command is sent to the point.
4	**Time Schedule Control**	The point remains in the operational state for the current Time Schedule as configured in the *Components* dialog. A point under Time Schedule Control will change its operational state in response to any of the above Control States.

3.4.2 Using Control States

SiPass integrated stores a queue of Control State Commands for each point. This queue contains the last non-executed command of each Control State type. So, there will be four commands, at most, in the control state queue.

When the current control state is terminated, the next control state in the queue will be executed as per the following rules:

- Completion/termination of a Permanent command will restore the effect of:
  - The last Internal command, or
  - The last Interruptible command, or
  - Time Schedule Control
- Completion/termination of an Internal/Access command will restore the effect of
  - The last Interruptible command, or
  - Time Schedule Control
- Completion/termination of an Interruptible command will restore the effect of
  - Time Schedule Control

Exceptions

There are certain exceptions to the above rules. These are:

- Change of Time Schedule State will terminate all current and non-current Interruptible commands.
- Execution of a Permanent Manual command will terminate all current and non-current Interruptible Manual commands.
- Execution of a Permanent Event Task will terminate all current and non-current Interruptible Event Tasks.
- Execution of the “Return to Time Schedule Control” command will terminate all current and non-current commands (Interruptible and Permanent) and return control to Time Schedule Control.

Every unsuccessful change of Control State (for example, if the change is denied due to the above rules) is recorded in the Audit Trail.

3.5 Creating a Host Event Task

A Host Event Task is a system related operation that is performed once certain conditions have been met. When you define a host event task, you define the conditions that must be met (Trigger) for the operation (Effect) to be executed. Host event tasks can be used to perform numerous system activities simultaneously.

For example, a host event task can be used to control certain points in the system when other points change state. This might be useful to automatically secure an area when a security breach is detected at your site. In this case, a host event task could be defined in order to lock all the doors within a specified area when any sensor (intrusion detector) in that area enters an alarm state.

An audit trail message appears when a host event task begins, and another audit trail message appears upon completion.

▷ Ensure that you have configured all the components at your site that will trigger an event or execute a command when an event has been triggered. Also establish the Time Schedules to be used in the host event tasks.

1. Choose **Program > Event Tasks > Host**.
2. Enter a unique name for the host event task into the **Event Name** field. You may enter up to 40 characters, in any combination of upper and lower case letters, and numbers. There are two pre-defined host event tasks in the system. These are as follows:
   - **Check Before Start Date Cards**:
     Checks the Start Date in the cardholder record. The cardholder’s access control privileges are enabled if their Start Date is equal to or greater than the current date.
   - **Check Expired Cards**:
     Checks the Expiry Date in the cardholder record. If the Expiry Date has been reached, the cardholder will be voided.
3. Select the **Time Schedule** in which the host event task is to occur. To select the Time Schedule, choose the drop down arrow and select a time zone from the list.
   - The effect a Time Schedule has on a host event task is detailed in the table at the end of this section.
4. Specify the **Trigger** details.
   ⇨ The fields within the Trigger section of the dialog will depend upon the source type chosen.
   ⇨ Event Tasks based upon “Special Date” may take up to 15 minutes to trigger from the specified time.
5. Complete the **Effect** details.
6. Click **Save**.

Time Schedule	Description
Never (point always secure)	The host event task can never be triggered.
Always (point unsecure)	The host event task can be triggered at any time including holidays and weekends.
System Function (non busy intervals)	The host event task can only be triggered between 2 am and 3 am every day of the year including holidays.

3.5.1 Host Event Task Trigger fields

The following fields are available when defining the trigger of Host Event Task.

Field	Description
Source1	The item that will trigger the specified host event task. To change the first source, choose the drop down arrow and select a new source from the list.
Location1	Specifies the location that will trigger the event. The available locations depend upon the source type selected. For example, if the source was an input event type, then only the input points defined in the system will be available.
State1	The state into which the source must enter in order to trigger the event. The condition is also met when initialization occurs and the source is in the specified state. To change State1, choose the drop down arrow and select a new state from the list. **Note**: If you have entities of 3rd party systems that are integrated with SiPass integrated, the STATES of these entities can be uploaded and downloaded between the two systems. The STATE corresponding to the 3rd party system will contain the term '**External System**' in the STATE 1 drop down list. For example, for the **Access** alarm type, 3rd party systems can have defined statues with the status **Battery Low External System**, **Unlock External System**, **Door Held External System**, **Lock External System**, etc.
Additional Criteria	When checked, additional criteria must be added and exist before an action takes place.
Source2	Secondary source item required to trigger the specified host event task, only if the first condition has been met. The secondary source is Workgroup.
Location2	Specifies the location that will trigger the event. This will be one of the work groups defined in the Database.

3.5.2 Host Event Task Effect fields

The following fields are available when defining the effect of a host event task.

Field	Description
Target	Specifies the type of item that the host event task will affect. To change the target, choose the drop down arrow and select a new target from the list.
Location	Specifies the name of the object that the event will affect. For example, if the specified event is unlocking a door, the target for such an event would be an output point and the actual door to be unlocked will be the location. To change the location, choose the drop down arrow and select a new location from the list.
Command	This is the command that will be performed on the target item when the host event task occurs.
Data	Specifies the data string for the command (if required).
Message	Message to appear on the Audit Trail when the host event task occurs.

3.6 Creating a Controller Event Task

Controller Event Tasks are triggered by internal controller activities, and therefore can occur even when disconnected from the server.

▷ Establish the Time Schedules to be used in the controller event task.

▷ Ensure that your daily code is the same number of digits as the Base PIN length.

1. Choose **Program > Event Tasks > Controller**.
2. Enter a unique name for the Controller Event Task into the **Event Name** field.
3. Select the **Time Schedule** during which the Controller Event Task will be able to activate, from the Time Schedule drop-down box.
4. Specify the **Trigger1** details. The fields within the Trigger section of the dialog will depend upon the Type chosen.
   – When selecting an Input point as the source for a controller based event task, the “Device” tasks will trigger from the actual activity at the point, regardless of the mode applied to that point. The “Logical” tasks will take into account the mode applied, for example if the point is disabled, and only operate based upon these modes, this means if the input point is disabled the event task will not run.
5. Specify two triggers for a controller event task, by selecting from the Logical Operator drop-down box and completing the fields in the **Trigger 2** section. The fields in the Trigger2 section are exactly the same as for Trigger1.
   – The Logical Operator options are detailed in the table at the end of this section.
6. Complete the **Effect** details. The fields within the **Effect** section of the dialog will depend upon the source type chosen.
7. Click **Save**.
8. To create another controller event task with similar details, choose **Copy**. The event task details will be copied into a new controller event task.

In most cases, by selecting zero, the data within the specified range of the event will allow a trigger on any card.

Operator	Effect
None	The fields in the Trigger 2 section will be disabled.
AND	Both Trigger 1 and Trigger 2 must occur before the Effect will be activated. Note that Trigger 1 and Trigger 2 must occur within 2 seconds of each other if the AND operator is used.
NOR	Both Trigger 1 and Trigger 2 must occur, or both return to their original states, before the Effect will be activated.
OR	Either Trigger 1, or Trigger 2, or both must occur before the Effect will be activated.
XOR	Either Trigger 1, or Trigger 2, but not both must occur before the Effect will be activated.

3.6.1 Controller Event Tasks Trigger Fields

The following fields are available when defining the trigger of a controller event task.

Fields	Description
Type	The type of event that must occur.
Controller	The controller connected to the source of the event.
Source	The controller or device that must undergo a change in state to trigger the effect.
State	The state into which the source must enter to trigger the effect.
Data	Any additional data that may need to be entered to identify the trigger.
Credential Profile	If the state being defined requires a Card Number, the Credential Profile field becomes enabled for the required profile to be selected from the field's drop down list.
Logical Operator	This field specifies the state requirement for the effect to occur. The following options can be selected from the field: **NONE**: The configured Effect will occur if neither Trigger 1 or Trigger 2 states are true. **AND**: The configured Effect will occur if both Trigger 1 and Trigger 2 states are true. **NOR**: The configured Effect will occur if neither Trigger 1 or Trigger 2 states are true. **OR**: The configured Effect will occur if either the Trigger 1 or Trigger 2 state is true. **XOR**: The configured Effect will occur if either the Trigger 1 or Trigger 2 state is true, but NOT both.

3.6.2 Controller Event Task Effect Fields

The following fields are available when defining the effect of a Controller Event Task.

Fields	Description
Type	Specifies the type of component that the event task will affect.
Controller	Specifies the controller connected to the target of the effect.
Target	The component that will perform the Command if triggered.
Command	This is the command that will be performed when the event task occurs.
Data	Specifies a data string for the command (if required).
Delay	The delay time in seconds before the Command will be executed.
Message	This is the message displayed in the Audit Trail when the event task occurs.

3.6.3 Switching between Controller Event Tasks and Host Event Tasks

Controller Event Tasks and Host Event Tasks generally correspond to different kinds of events. Controller Event Tasks are usually triggered by hardware related events, and Host Event Tasks are triggered by Global SiPass integrated conditions, like swiping a card or loss of communication to a controller. There is some overlap between the two types of event tasks.

However, it is possible to create a flow-on effect, and cause a Host Event Task to be triggered by Controller Event Task conditions, and vice versa. This is done by creating a host event task and assigning it as a command (Effect) in a Controller Event Task.

3.6.3.1 Triggering a Host Event Task from a Controller Event Task

The various stages and steps required to trigger a Host Event Task from a Controller Event Task are detailed in this section.

Stage 1: Creating the Host Event Task

1. Choose **Program > Event Tasks > Controller**.
2. Enter a unique name or select an existing host event task in the **Event Name** field.
3. Select the **Time Schedule** during which the host event task will be able to occur, from the **Time Schedule** drop-down box.
4. Select “ACC Control” from the **Source1** drop-down box.
5. Select “Activated” from the **State1** drop-down box.
6. Assign an ACC to this Host event task from the **Location** drop-down box.
7. Complete the **Effect** section.
8. Click **Save**.

Stage 2: Creating the Controller Event Task

1. Choose **Program > Event Tasks > Controller**.
2. Enter a unique name or select an existing controller event task in the **Event Name** field.
3. Select the Time Schedule during which the controller event task will be able to occur, from the **Time Schedule** drop-down box.
4. Select “ACC Event Task” from the **Type** drop-down box.
5. Complete the **Trigger** section.
6. Select “Run Host Task” from the **Type** drop-down box in the **Effect** section.
7. Select the Host Event Task, from the **Target** drop-down box.
8. Complete the **Delay** and **Message** fields.
9. Click **Save**.

⇨ When the specified Trigger occurs, the controller event task will execute the Host Event Task that you selected.

3.6.3.2 Triggering a Controller Event Task from a Host Event Task

The stages and steps required to trigger a Controller Event Task from a Host Event Task are detailed in this section:

Stage 1: Creating a Controller Event Task

1. Choose **Program > Event Tasks > Controller**.
2. Enter a new name or select an existing controller event task from the **Event Name** drop-down box.
3. Select the Time Schedule during which the controller event task may be activated, from the **Time Schedule** drop-down box.
4. Select “Host Control” from the **Type** drop-down box.
5. Select the ACC Controller assigned to this controller event task from the **Controller** drop-down box.

6. Select the state of the Host Event Task, which will trigger this controller event task, from the **State** drop-down box. There are two options: **Cleared** and **Set**.
7. Complete the **Effect** section.
8. Click **Save**.

Stage 2: Creating the Host Event Task

1. Select **Program > Event Tasks > Controller**.
2. Enter a new name or select an existing controller event task from the **Event Name** drop-down box.
3. Complete the **Trigger** section.
4. Select “ACC Trigger” from the Target drop-down box in the **Effect** section.
5. Choose either the “Set Trigger” state or the “Clear Trigger” state from the **State** drop-down box.
6. Select the Controller Event task you defined in step 1, from the **Location** drop-down box.
7. Complete the **Message** field.
8. Click **Save**.

⇨ When the specified Trigger occurs, the host event task will execute the Controller Event Task that you selected.

3.7 Creating a Holiday

Holidays allows dates that are exceptional to the normal rules to be defined in the Time Zone records; For example, Christmas Day or New Year’s Day. This allows cardholders access to be controlled without having to change Time Zone definitions every time a holiday occurs.

Only one holiday can be defined for a single date.

▷ Ensure that you have installed the appropriate bus drivers and have configured each bus.

1. Choose **Holidays** from the **Program** toolbar or menu.
2. Enter a unique name for the holiday into the **Holiday Name** field.
   – You may enter up to 40 characters, any combination of upper / lower case letters.
3. Enter a date for the specified holiday into the **Date** field.
   – To change the date, choose the drop down arrow and select a new date from the calendar.
4. Select the type of Holiday from the **Type** drop-down box. SiPass integrated allows you to define two types of Holidays. You can change the effects of a holiday by modifying the relevant Time Schedule(s) in the *Time Schedule* dialog.
5. Select the ACCs that will observe the holiday.
6. Choose **Add >.**
   ⇨ The ACC will appear in the **Selected** list.
7. Click **Save**.

3.8 Log Book

The Log Book allows operators to make a record of a site's activities, using a simple heading-based log system. When certain events at your site occur, the operator can open the log book, select the appropriate topic, and log their observations or the action taken. This creates a permanent record that can be recorded at a later stage.

To configure the Log Book you have to create a set of topics, used to categorize log entries. This section explains how to create these topics and add entries to the Log Book.

3.8.1 Adding a topic to the Log Book subjects

The Look Up Table allows you to create the necessary topics for the Log Book.

Please refer the section Lookup Data of the SiPass Explorer User Manual for detailed information on how this can be done.

3.8.2 Making an Entry into a Log Book

Once you have created topics to be used for the Log Book Entries, operators can use them to log entries regarding activities at your site

1. Choose **Log Entry** from the **Operation** toolbar or menu.
   ⇨ By default, the *Log Book Entry Form* dialog displays the **Operator Name**, **Date** and **Time** fields as non-editable fields. The operator can only select from the **Subject** combo box and only modify the **Description** field.
2. Select a subject from the drop down list in the **Subject** combo box by highlighting it in the displayed list.
3. Your choice of subject will be displayed in the combo box and the **Save** button will be enabled.
4. Complete the appropriate comments in the **Description** field as free text.
5. Click **Save**.

⇨ Each entry will be logged individually.

⇨ A report can be generated that prints all Log Book Entries.

3.9 Messaging

SiPass integrated can automatically send a message to a pager (or a similar paging system, like an intercom system), a GSM mobile phone or e-mail address when certain conditions have been met. This allows important events on the site to be registered, when no one is around to monitor them.

The sections that follow explain the various steps required to configure and send messages to GSM mobiles, pagers and e-mail addresses.

3.9.1 Messaging a GSM Mobile

Configuring and sending a message to a GSM mobile allows selected personnel to be notified via SMS that a certain event / trigger has occurred.

The first step required to configure this feature, is to add and configure Modem Hardware resources in SiPass integrated.

Once the modem hardware is configured, operators can configure message forwarding to a GSM mobile in two ways:

- Event Task Message Forwarding to a GSM Mobile
- Alarm Class Message Forwarding to a GSM Mobile

The sections that follow will take the user through all the steps required to configure SiPass integrated for this feature, and send messages.

3.9.1.1 Configuring Modem Hardware Resources

GSM Modems are mapped as hardware entities in SiPass integrated. These modems will first have to be added and configured to the system.

1. Select **System > Components**.
2. Click the **New Bus** button.
3. Select **Modems**.
4. Click the **New Unit** button.
5. In the **Modem Name** field, add a name for the modem unit.
6. From the **Modem Type** drop down list, select **AT Command** or **Hayes Compatible Modem**.
7. From the **Modem Port** field, select a port.
   ⇨ This list displays all the modem ports that are available on the server.
8. To view the Modem Status and Event History, click the **View Modem Status** button. To pause the scroll of Modem Event History messages, click the **Pause History View** button.
   ⇨ The Overall Modem Status will display one of the following statuses: **Available**, **Malfunctioning** or **Busy**.
9. To return to view Modem Settings, click the **View Modem Settings** button.
10. Click **Save**.

If a GSM Modem is being used for Dialup Redundancy, it cannot be used for Short Messaging Services (SMS).

A Modem unit cannot be deleted if it has an Alarm Class associated with it.

3.9.1.2 Event Task Message Forwarding to GSM Mobiles

An operator can configure a Host Event Task to send messages to selected mobile numbers, when a certain trigger / event has occurred.

The main pre-requisite to this feature is that the mobile number to which the message should be forwarded, must be specified on the *Personal* tab of the *Cardholder* dialog for the selected cardholders.

Once the mobile number for the cardholder(s) has been specified, an event task can be configured in the *Host Event Task* dialog as described below.

1. Select **Program > Event Task > Host**.
2. Enter an **Event Name**.
3. Select the appropriate **Time Schedule**.
4. From the **Source 1** drop-down list, select a required trigger source.
5. From the **State 1** drop-down list, specify a required state.
6. From the **Effect** drop-down list, select **Message Forwarding**.
7. From the **Command** field, select **Forward to GSM Mobile(s)**.
8. All the cardholders, whose mobile number have been entered in the *Cardholder* dialog, will be displayed in the **Cardholder** box field.
9. Select a Cardholder(s).
10. In the **Message** field, type a message that will be forwarded to the cardholder's mobile on event trigger.
11. Click **Save**.

3.9.1.3 Alarm Class Message Forwarding to GSM Mobile(s)

An operator who wishes to setup Alarm Class Message Forwarding will need to perform two main configuration activities:

- Configure an Alarm Class to forward a message on State change
- Assign a point to the Alarm Class

These steps required for these two configurations will be discussed in this section.

The main pre-requisite to this feature is that the mobile number, to which the message should be forwarded, must be specified on the Personal tab of the Cardholder dialog for the selected cardholders.

Configuring an Alarm Class to forward message on State change

1. Select **Program > Alarm Class**.
2. Specify an **Alarm Definition Name**.
3. Specify an **Alarm Type** in the **Type** field.
4. Tick the **Forward to GSM Mobile(s)** checkbox.
5. In the box below this checkbox, specify the cardholders to whom the message should be forwarded.
6. Specify the state change in the **Current Defined States** section.
7. Click **Save**.

Configuring an access point for the alarm class

1. Select **System > Components**.
2. In the tree hierarchy, navigate to the access point configured for the alarm class.
3. In the **Alarm Definitions** field, select the Alarm Class that was configured for message forwarding.
4. Click **Save**.

Once these two configurations have been implemented, a state change will raise an alarm. This in turn, will forward a message to the selected GSM mobile(s).

3.9.2 Configuring Message Forwarding to a Pager or Email Address

Configuring and sending a message to a pager or mobile service is a three-stage process that includes Configuring the Service Provider, Configuring Cardholder information and Creating the Event Task to handle the paging scenario.

Configuring and sending a message to an email address is a two-stage process that includes configuring cardholder information and creating the event task to handle the email forwarding. A connection between SiPass integrated and an Email Server must be present to allow messages to be forwarded to email addresses.

3.9.2.1 Step 1 - Configuring Service Providers

1. From the **System** menu, select **Messaging** and then select **Service Providers**.
2. Enter the Service Provider Information.
   – You may need to contact your chosen service provider for the correct details to complete this section.
3. Enter the Dial-Up Parameters.
4. Enter the Local Parameters.

If a modem on the SiPass server is deleted, you will need to re-configure your service provider details.

Service Provider Configuration Fields

The fields used to configure Service Providers are given below:

Field	Description
Service Provider Name	Enter the name of the service provider.
Service Provider Password	Enter the password for access to the Service Provider. Note that not all Service Providers will require a password. If a password is not required, this field will be ignored.
Maximum Messages per Session	Select the maximum number of messages able to be sent per session using the up and down arrows. This will package multiple messages for the same service provider into a single phone call. That is, you can send the same message to multiple cardholders' pagers with one call.
Disable Service Provider	Tick this checkbox if you wish to disable the Service Provider
Use Dial-up	Un-tick this checkbox if you want to send messages via a method other than dial-up modem. This could be via a paging or similar device that is compliant with the standard automatic TAP protocol.
Port	This field will be enabled only if the Use Dial-Up checkbox has been un-ticked. Select from the list the Com Port on the PC to which the TAP-compliant messaging device is connected
Service Provider Phone No	Enter the phone number for the Service Provider.
Modem	Select the modem to be used for sending the message from the drop-down list. You will need to install and configure an appropriate modem on the SiPass Server before you can select it for messaging. Please consult your System Administrator for more information regarding the installation and configuration of a modem.
Port	Select the port number on the workstation connected to the messaging or paging device. This field will only be enabled if the Use Dial-up checkbox in the Service Provider Information section has been un-ticked. The Service Provider details will be saved

3.9.2.2 Step 2 - Configuring Cardholder Details

To enable SiPass integrated to send a message to a cardholder, the cardholder's pager number, mobile number or email address must be entered as part of their cardholder details.

Do one of the following:

- Ensure that the **Mobile Number** and **Mobile Service Provider** fields are completed if you wish to send messages to the cardholder's mobile phone.
- Ensure that the **Pager Number** and **Pager Service Provider** fields are completed if you wish to send messages to the cardholder's pager.
- Ensure that the **Email Address** and **Use Email in Message Forwarding** fields are completed if you wish to send messages to the cardholder's email address.

3.9.2.3 Step 3 – Creating the Messaging Event Task

The final step in configuring the SiPass integrated messaging component is to create an Event Task. This will allow you to configure the System Components that trigger a message, the recipient of the message and the message itself.

1. Choose **Program > Event Tasks > Host**.
2. Enter a unique name for the event task into the **Event Name** field.
3. Select the **Time Schedule** during which messages can be sent.
4. Specify the **Trigger** details.
5. Select **Message Forwarding** from the **Target** drop-down list.
6. Select **Forward to Pager(s)** from the **Command** drop-down list to send a message to a pager or a mobile phone.
7. Select **Forward to Email(s)** from the **Command** drop-down list to send an email.
8. Select the cardholder to whom the message will be forwarded from the **Location** drop-down list.
   - Only cardholders with a valid service provider (mobile or pager) configured in their database record will be selectable.
9. Enter the text message to be sent to that cardholder's mobile phone and/or pager into the **Message** field.
10. Click **Save**.

Each text message is formatted by SiPass integrated before being sent to the Service Provider for paging, including adding a date and time stamp, and UserID.

Different Service Providers may process the entire message, text plus formatting, in a different manner. For example, characters or strings that have a particular meaning to the Service Provide, can be inserted into the **Message** field. For more information on using the Message string in such a way, consult the documentation for your Service Provider's supported protocol.

Note: Both SMTP and Microsoft Exchange protocols are supported. For Email Messaging setup, see section Notify Email Tab [→ 17] in this document.

3.10 Server Messaging

SiPass integrated can send messages to and from SiPass servers on a network. To do this, you need to define the other servers on the network that will communicate messages to and from your server.

A **message originator** is a SiPass server that is sending a message to your server.

A **message receiver** is a SiPass server that is receiving a message sent from your server.

Configuring and sending a message to a SiPass server is a three-stage process that includes Configuring message receivers, Configuring message originators and Creating the event task to handle the server messaging.

Stage 1 - Configuring Message Receivers

1. From the **System** menu, select **Messaging** and then select **Message Receiver**.
2. Enter a unique name for the SiPass server capable of receiving messages into the **Receiver Name** field.
3. Select the type of address you will use to locate this server when sending messages, from the **Address Type** drop-down box.
4. Enter the address of the Server PC into the Address field, according to the type that you selected in step 3.
5. Tick the **Disable Receiver** checkbox if you want to disable server messaging for this particular server.
6. Click the **Test Connection** button.
   ⇨ The status of the connection will appear in the field below.
7. If the connection is working, choose the **Save** button.

Stage 2 - Configuring Message Originators

1. From the **System** menu, select **Messaging** and then select **Message Originator**.
2. Enter a unique name for the server capable of sending messages into the **Originator Name** field.
3. Select the type of address you will use to locate this server, from the **Address Type** drop-down box.
4. Enter the address of the Server PC into the **Address** field.
5. Tick the **Disable Originator** checkbox if you want to disable server messaging for this particular server.
6. If the connection is working, choose the **Save** button.

Stage 3 - Configuring the Server Messaging Event Task

1. From the **System** menu or toolbar, select **Event Task**.
2. Enter a unique name for the messaging event task into the **Event Name** field.
3. Select the **Time Schedule** during which server messages can be sent from the **Time Schedule** drop-down box.
4. Select **Message Forwarding** from the **Target** drop-down box.
5. Select **Forward to other SiPass server(s)** from the **Command** drop-down box.
6. Highlight the server names in the SiPass Servers list to which the message should be forwarded. Use SHIFT + Right Click to select multiple servers.
7. Enter a message describing the event into the **Message** field.
8. Click **Save**.

⇨ When the trigger occurs, details of the event and the message entered will be displayed on the Messaging Queue window of each selected Server.

3.11 Anti-Passback

The SiPass integrated Anti-Passback functionality allows you to define a set of locations (called „Areas“) that cardholders must enter and exit in a specific sequence. This lets you force entry and exit travel through a site, and monitor exactly the number of cardholders entering a particular location.

The Anti-Passback features in SiPass integrated are flexible enough to suit the environment of any site. The following Anti-Passback alarms can be generated:

- Soft Anti-Passback
- Hard Anti-Passback
- Fail-soft Anti-Passback
- Area Count violations

Soft Anti-Passback

In this mode, cardholders must use their access card to gain entry to and exit from a defined locality. If a valid cardholder has presented their access card to enter a locality and not presented the card when exiting they are in breach of the Anti-Passback rules. The next time the cardholder attempts to enter that same locality a Soft Anti-Passback alarm will be raised. However, the cardholder **will** still be permitted entry into the area.

Hard Anti-Passback

In this mode, cardholders must use their access card to gain entry into and exit from a defined area. If a valid cardholder has presented their access card to enter an area and not presented the card when exiting they are in breach of the Anti-Passback rules. The next time the cardholder attempts to enter that same area a hard Anti-Passback alarm will be raised and that cardholder will not be permitted entry into the area.

Fail-Soft Anti-Passback

Depending on the size of the area governed by Anti-Passback rules, multiple ACCs may be required to share Anti-Passback data.

Fail-soft Anti-Passback mode dictates that if the connection between ACCs in an Anti-Passback Area is broken, then SiPass integrated will default to Soft Anti-Passback mode for that area. That is, access outside of the Anti-Passback rules will be permitted, but the violation will be recorded in the Audit Trail.

Area Count Violations

By applying a limit to the number of cardholders who may enter a specified area, you can:

- Raise an alarm when the area count has been reached.
- Raise an additional alarm when the area count has been exceeded.
- Trigger event tasks such as preventing further cardholders from entering a area that has reached its limit, or turning on an “Area Full” sign.

Timed Re-entry

Timed Re-entry is a feature of Anti-Passback that allows you to limit re-use of a card at certain readers or reader groups within a specified amount of time.

An attempt to re-enter an Area in “Timed Re-entry” mode within the duration will result in access being denied and a “Timed Re-entry Restricted” violation message reported to the Audit Trail.

Internal Readers Anti-Passback

This form of Anti-Passback enforces the use of entry and exit readers, before cardholders can access any other internal readers within that area. Cardholders must badge their card at an Entry Reader (log in to the area) before they can access any internal readers within that area. Soft or hard anti-Passback modes can be set to any of the internal readers within the area. When assigning access points to an area, any internal reader can be assigned as an access point to that area.

Delayed Reporting

Under normal access operation modes, a valid card badge is equivalent to a valid door entry in SiPass integrated. That is, if a valid card has been badged, to SiPass integrated this means that the cardholder has physically passed through the door.

However, it is possible for a cardholder to badge their card, but not actually proceed through the door. If this occurred at an Area configured for Anti-Passback, this would mean the Area Count would be incorrectly incremented or decremented, and the cardholder incorrectly located by the system.

To counteract this, access points used to enter defined Anti-Passback Areas should be assigned to the Operation Modes “Card Only Delayed Reporting” or “Card and PIN Delayed Reporting”. Access points assigned one of these modes will only recognize a valid access attempt if the associated door monitor registers that the door has opened after a valid badge.

Other Anti-Passback Features

Besides the standard access features provided by the Anti-Passback function, a number of other attributes can also be easily configured. These include:

Audit Trail Entries – All area transactions are immediately logged to the SiPass integrated audit trail. An additional area specific column can also be added to your audit trail view using the Operator Preferences feature of SiPass integrated.

Reports – You can generate reports regarding the localities at your site. More specifically you can generate reports on cardholders that are currently inside a specified area.

Distribution of Anti-Passback data across ACCs

It is recommended that, where possible, card readers set up to control access to an Anti-Passback system are not connected to different ACCs.

This will depend on how your site is structured; for reasons of complexity or physical size, it may not be feasible for all readers controlling access to an area or areas to be connected to a single ACC. While the performance of Anti-Passback controllers should not be affected, in these instances you should be aware of the behavior of the Global Anti Passback (GAP) system in case of communications failure.

ACCs communicate to each other the movements of cardholders across shared Anti-Passback areas. This process is completely transparent to the operator. However, if the connection between ACCs is disabled for some reason, cardholder movement data may not be sent. This means that ACCs may hold incorrect information about the whereabouts of a particular cardholder.

In this instance, Areas set to Hard Anti-Passback mode will default to that mode. This stops cardholders from entering and exiting areas until all communications are restored. Areas set to Fail-soft Anti-Passback mode will default to Soft Anti-Passback.

The above applies only to communications losses between ACCs that share Areas. If comms loss occurs between two ACCs with no Anti-Passback areas in common, operation will continue as normal.

3.11.1 Creating an Anti-Passback Cluster

SiPass integrated allows you to create clusters of ACCs in which Anti-Passback can operate. Once setup, a cluster of ACCs communicate among themselves to ensure that Anti-Passback operates across ACCs even when communications with the server are lost.

▷ Ensure that you have configured all ACCs that will form a cluster and have pre-planned your Anti-Passback areas so that you know which ACCs to include in the cluster.

1. Select **Anti-Passback Area** from the **System** Menu.
2. Select the **New Cluster** button.
3. Enter a descriptive name for the Area into the **Cluster Name** field.
4. Click on an ACC from the Available Units List to highlight it and then select **Add** to add the ACC to the **Selected Units** list. Repeat this step until all ACCs to from the cluster have been selected.
5. Click **Save**.

⇨ This newly created cluster will appear in the tree view on the left hand side of the dialog.

3.11.2 Creating an Anti-Passback area

Anti-Passback revolves around the concept of an **Area**. An **Area** in SiPass integrated is defined as a space with at lease one entry and one exit point. An area can consist of two or more sub-areas.

A **Sub-Area** is simply an area that is located within another area. The sub-areas must operate in the same Anti-Passback mode as the area to which they belong.

Creating an area involves assigning the IN and OUT readers which are used to enter and exit the area, the Anti-Passback mode, and also giving the area a Count if required. The count of an area includes all cardholders currently located in an area, including all sub-areas of that area. This means that if a cardholder exits an area and enters a sub-area of that area, the count of the original area will remain the same, and the count of the sub-area will increase by one.

If a cardholder exits the sub-area and re-enters the area, the original area's count will still remain the same, and the sub-area's count will decrease by one.

If Area details are changed, deleted or updated, the ACCs that handle Anti-Passback access to those areas must be re-initialized for the changes to take effect.

To create an Anti-Passback area

▷ Ensure that you have configured in SiPass integrated the Dual Reader Interface (DRI) or SRI devices used to access and exit the area(s).

▷ Ensure that you have configured your ACC cluster(s)

1. Select **Anti-Passback Area** from the **System** Menu.
2. Select the **New Area** button.
   ⇨ The area definition screens will now appear showing the *Definition* Tab.
3. Complete the *Definition* tab details.
4. Select the *Member* tab.
5. Select “IN Reader” from the **Type** drop-down box.
   ⇨ The list of readers you have defined at the facility will be displayed in the **Available** List. Once the list is displayed, select the reader(s) and choose **Add** to move them to the **Selected** List.
6. Select “OUT Reader” from the **Type** drop-down box
   ⇨ The readers you have configured at the facility will appear in the **Available** List, minus those readers that have already been assigned as IN Readers for this area.
7. Select the readers from the **Available** List which permit exit from this area, and choose **Add** to move them to the **Selected** List.
   – If you selected “Timed Re-entry” as the Anti-Passback mode in step 3, it is not compulsory to choose any OUT readers for this area.
8. Select “Internal Reader” from the **Type** drop-down box.
   ⇨ The list of readers you have defined at the facility will be displayed in the **Available** List.
9. Once the list is displayed, select the reader(s) which will be the internal readers in the area, and choose **Add** to move them to the **Selected** List.
   – An internal reader is not an ‘IN’ or ‘OUT’ reader, it is only an internal reader for the area.
10. If you wish to set cardholder limits for each workgroup for your Anti-Passback area, select the *Workgroup* tab.
11. Highlight the workgroup to be added from the available list and click the **Add** button.
    ⇨ The workgroup will now be added to the selected list.
12. Configure the workgroup by setting the limit and enforce attributes.
    – **Capacity**: Sets the maximum number of cardholders that belong to that workgroup which can enter the Anti-Passback area.
    – **Enforce Capacity**: This checkbox forces the maximum count for that workgroup by denying entry to additional cardholders that belong to the workgroup when the capacity is reached, even if the overall Anti-Passback area has not reached its capacity.
13. Click **Save**.

Cardholders that belong to workgroups not specifically assigned a limit to the Anti-Passback area share the remainder of the overall limit.

3.11.2.1 Area Definition Configuration Fields

The fields used to configure the main definition of the Area tab are provided in the table that follows:

Field	Description
Area Name	Enter the name of the Anti-Passback area. This name will be displayed in system messages (e.g.: Audit Trail)
Mode	Select the mode of operation for the Anti-Passback area as described earlier.
Alarm Class	Select the alarm class that will apply to this Anti-Passback area from the Alarm Class drop down box.
Area Number	A read only field that indicates the ID for the Anti-Passback area.
Current Status	Displays the current status for the Anti-Passback area. To refresh the information select Load.
Mustering Anti-Passback Area	Tick this checkbox if the Anti-Passback area is a mustering area and will be used for reporting cardholders logged into the area during an emergency. This area will be included when a “Mustering Report” is generated.
Maximum Cardholders	Enter the maximum number of cardholders permitted to be logged into the area at any one time.
Enforce Maximum Cardholders	Tick this checkbox to enforce the maximum limit on the Anti-Passback area. This means that no further cardholders will be permitted to enter the area until another cardholder has first exited.
Enable Four Eyes Access	Tick this checkbox to enable four eyes access control for the Anti-Passback area. This allows you to set a time period for badging between the first and second badge of the two cardholders which are required in the specified area at any one time.
Four Eyes Timer	Enter the time in seconds, that will delay alarm generation after a first cardholder enters the Anti-Passback area, and before the second cardholder also enters. This entry can range from 1 second to 32767 seconds.
Include Cardholders in Anti-Passback sub-areas	Tick this checkbox if cardholders already logged in to sub-areas are also included in the four eyes count.
Trigger Alarm if no Cardholder	Tick this checkbox to generate an alarm when the Anti-Passback area becomes empty.
Re-entry Timeout	Only enabled when the mode selected is Timed Re-entry. Enter the time in minutes before a cardholder can re-use their access card at the re-entry doors. Please note that if an exit reader is configured in the Timed Re-entry configuration, cardholders badging to exit are automatically allowed to re-enter at any time.

3.11.3 Assigning a sub-area to an Anti-Passback area

You must define the IN and OUT readers for both sub-areas and the areas to which they belong. This means that some readers will be assigned twice.

▷ Ensure that you have configured all of the sub-areas to be assigned.

1. Select **Anti-Passback Area** from the **System** menu or toolbar.
2. Select the Area from the *Name* dialog, or create a new area.
3. Select the *Member* tab.
4. Select **Sub area** from the **Type** drop-down box. The **Available** List will be populated with all defined areas, that have been assigned the same Anti-Passback mode as the current Area.
5. Select the Sub-area(s) you want to assign to this Area, and choose **Add** to move them to the selected list.
6. Click **Save**.

3.11.4 Viewing Cardholders in an Area

SiPass integrated allows you to view a detailed list of cardholder located in an area, in real-time.

1. Select **Anti Passback Area** from the **System** toolbar or menu.
2. Select from the **Area Name** drop-down box the area you want to view.
3. Select the *Area Data* tab.
4. Choose the **Load Cardholders** button to refresh the list with details of cardholders currently in that Area. The table at the end of this section explains each column in the list.
5. To refresh other properties within this dialog use the buttons provided:
   - **Load Current Count**:
     Updates the Current Count field.
   - **Reset Current Count**:
     Resets the Current Count field to zero and removes all cardholders from the area.
   - **Forgive All**:
     Forgives cardholders in all areas. Cardholders may enter/ exit any Anti-Passback area once only without violating Anti-Passback rules.

Forgiving a cardholder only operates for a single card badge. Once the cardholder has entered/exited an area after a forgive command has been granted, normal Anti-Passback rules immediately apply.

Column	Description
Card No.	The card number of the card holder
First Name	Cardholder's first name
Last Name	Cardholder's last name
Date	Date when the cardholder entered the area or sub-area
Time	Time when the cardholder entered the area or sub-area

3.11.5 Forgiving Anti-Passback Violations

To **Forgive** a cardholder is to allow them to enter or exit an area, where normally this would produce an Anti-Passback violation. The Forgive feature permits access for the first use of a card, whether at an Entry or an Exit Reader. Upon power-up, all cards will be in 'forgive mode' when the Anti-Passback mode has been applied.

In addition, single cardholders can be forgiven an Anti-Passback violation from the Audit Trail, manual command or Event Task, and all cardholders in an area can be forgiven simultaneously. Forgiving a cardholder only operates for a single card badge. Once the cardholder has entered or exited an area after a forgive command has been granted, normal Anti-Passback rules immediately apply.

Sending a manual Forgive command

1. Select **Manual Override** from the **Operation** menu.
2. Choose the **APB Area** button.
3. Select **Forgive All Cards** to forgive every active card defined in SiPass integrated.
4. Alternatively, select **Forgive Card** to issue a forgive command to a single cardholder. The **Card Number** field will appear.
5. Choose **Send**.

If you are issuing a forgive command to a primary card number (that is, not a Tenant or 2nd Card Number), enter the card number into the Card Number field. If you are issuing a forgive command to a tenant or 2nd card number, the card number must be entered in the following format:

<number>,<facility>,<technology>

Where **number** = card number, **facility** = facility code, **technology** = card technology code.

For example: 0034,15,10

3.12 Intrusion Areas

Intrusion areas allow cardholders to control whole groups of points (known as areas) through any device in SiPass integrated. Cardholders are able to secure and unsecure intrusion areas with the right access privileges.

3.12.1 Configuring an Intrusion Area

▷ Ensure that the input access points have been configured on the desired components. Please refer the Defining Access Points [➙ 34] section of this manual.

▷ Ensure that arming and disarming of the selected areas has also been performed.

1. Select **Intrusion Area** from the **System** toolbar or menu.
2. When adding a second or subsequent Intrusion Area, you will need to select **New** on the bottom left hand side of the *Intrusion Area* dialog.
3. Enter a unique name for the Intrusion Area into the **Name** field.
4. Enter an abbreviated version of the name above under **Short Name**. This will be used for display on the reader's LCD screen. This option has been included to allow for future development.
5. Select the alarm class that will apply to this intrusion area from the **Alarm Class** drop down box.
6. Select the **Time Schedule** that will be applied to the intrusion area.
   - **Never (Point always Secure)**: The area is secured.
   - **Always (Point always unsecure)**: The area is always unsecure
   - **System Function (Non-busy intervals)**: The area will become unsecure between 2am and 3am everyday of the year including holidays
7. Select the Arming Time Schedule **Off/On** state.
   - **Arm/Disarm**: Area will be armed when the Time Schedule is not active and disarmed when the Time Schedule is on.
   - **Arm/Part Arm**: Area will be armed when the Time Schedule is not active and only Part Armed when it's on.
   - **Part Arm/Disarm**: Area will be Part disarmed when the Time Schedule is off and completely disarmed when it's on.
8. Enter the **Entry Delay** in seconds which will delay the alarm when the cardholder walks into the area. Also enter the **Exit Delay** to specify the time in exiting the area before the input points become enabled and an alarm can be reported.
   - This is only enabled when the **Entry/Exit Delay** operational mode is selected.
   - ⇨ The ID field displays the intrusion area ID in read only mode.

9. Click on the *Intrusion Area Members* Tab
10. Select the Unit from the drop down box which displays all available ACC units.
11. Select the **Type** of member that can be assigned to an Intrusion Area. Selecting a type changes the **Available List** accordingly. The type of members that can be selected are the following:
    - **Input Points**: All available input points that had been set for intrusion operation through the components dialog or whose operation mode is set to Input Disabled.
    - **Entry Lockout Points**: All available access points
    - **Dependent Intrusion Areas**: All available intrusion areas
12. Select the unit and point from the list displayed in the top window by clicking once on that unit/point.
13. Click on the **Intrusion Area** Link to display a drop down box for the intending arming action for that point
    - **Arm**: The area will be completely armed.
    - **Partitial Arm**: Any input points that have been assigned to an intrusion area as Partially armed points will enter an alarm state when Partial Alarm is selected.

Part Arming can only be selected for input point types.

14. The selected unit will appear on the window below. Once you have finished adding units, select **Save**. To remove any units, select the unit and select **Remove**.
15. You will now need to configure cardholder's permissions for the intrusion area. Please refer to the details regarding Isolation in the section Definition Tab [→ 96] in this manual.
    ⇨ Once an area is configured, it will be displayed on a tree on the left hand side panel of the dialog.

The armed state of a native intrusion area is retained only if the area was armed by a Time Schedule. Otherwise the armed state of the native intrusion area is not retained. However this does not affect the armed state of external intrusion areas.

3.12.2 Viewing the details of an input point

1. Once you have set up an Intrusion Area, select it from the tree on the vertical panel on the left hand side of the dialog.
2. Expand the tree until the points are displayed.
3. Select the point to view its details. On the right hand side panel, the Point Details are displayed:
    - **Name**: Displays the point's name
    - **Operation mode**: Displays the point's operation mode.

Once you have configured the Intrusion Area, you will need to give cardholder privileges to the new areas by configuring the cardholder preferences. Refer to the section in this manual under Access level and Cardholder privileges.

3.13 Door Interlocking

Door Interlocking is a mode of operation for multiple doors that lock together with a multiple set of rules. By combining a set of doors into a single interlocking set, you can ensure that only 1 door can unlock at any given point in time. Once this door is unlocked by a cardholder, all other doors configured in the same set will remain locked, even if a valid cardholder presents their access card.

All doors in an interlocked set must be configured on a single ACC.

3.13.1 Configuring a Door Interlocking Set

▷ Ensure that the doors (devices) have been configured for the desired doors.

1. Select **Door Interlocking** from the **System** toolbar or menu.
2. Click the **New** button located at the bottom of the dialog.
3. Enter a new Name for the Door Interlocking Set.
4. Select the alarm class that will apply to this Door Interlocking Set from the **Alarm Class** drop down box.
5. Select the *Members* tab to begin choosing the doors that will become part of the interlocking set.
6. Select the ACC from which the doors will be selected using the **Controller Unit** drop down list.
   ⇨ All doors available for selection will appear in the **Available** list box.
7. Select the doors to be added to the set by clicking on the appropriate names of the readers belonging to that door (holding the CTRL key down will allow you to select multiple doors at the one time.
8. Click the **Add** button to add the doors to the **Selected Doors** list box.
9. Click **Save**.

A door can only be configured to any number of Door Interlocking Sets.

3.13.2 Configuring the Delay Time for an Interlocked Door

1. Select **Door Interlocking** from the **System** toolbar or menu.
2. Click the **+** button to expand the Door Interlocking set your door belongs to.
3. Select the door you wish to modify from the list.
4. Enter the **Delay Time** by typing a value into the field or clicking the up and down buttons.
5. Click **Save**.

3.14 External Alarm Monitoring

The External Alarm Monitoring (EAM) function allows SiPass integrated to communicate with an external alarm monitoring company. To configure this, a set of external alarm monitoring points need to be set up to respond to state changes from input points, as well as intrusion zone points, and any groups of these points.

3.14.1 Configuring an External Alarm Monitoring unit

▷ Ensure that you have configured any necessary input points, and intrusion zone points.

▷ Ensure that a set of external alarm monitoring points has also been configured.

1. Select **External Alarm Monitoring** from the **System** toolbar or menu.
   ⇨ The *Bus Details* tab will appear and the **Bus Name** will be displayed. This is a read only field.
2. Expand the tree under ACC Controllers until the ACC's are displayed. The *ACC Details* tab will display:
   – **Name**: Displays the name of the ACC configured. Read Only field.
   – **IP Address**: Displays the IP address of the ACCC. Read Only field.
   – **Serial Number**: Displays the Serial number of the ACC. Read Only field.
3. To set up a new External Alarm Monitoring unit, select **New EAM Unit**.
4. Complete the following Unit Details:
   – **Name**: Enter a unique name to identify the External Alarm Monitoring unit.
   – **Hard ID**: Enter a unit ID used to initialize the External Alarm Monitoring unit.
   – **FLN Port**: Displays the FLN port that the external alarm monitoring unit can be connected to. Only an ISB port can be used. Read Only display.
   – **Baud Rate**: Select the baud rate at which the unit will transmit data.
   – **Protocol**: Select the list of protocols for the unit, only Securitel is available in this version.
   ⇨ The Auto Creation Wizard link launches a wizard for an automotive creation process.

On **Granta** hardware, external alarm monitoring can be configured on only FLN 1, FLN 2 and FLN 3. Any of these three FLNs can be used to configure Securitel on the Granta unit.

5. Click **Save**.

⇨ A new External Alarm Monitoring unit has been added.

3.14.2 Configuring an External Alarm Monitoring unit using the Auto Wizard

1. Select **External Alarm Monitoring** from the **System** toolbar or menu.
2. Expand the tree under ACC Controllers and select EAM.
3. Select the **Auto Creation Wizard** link.
4. Select **Next** to begin the wizard.
   – You can exit the Auto Creation Wizard at any time by selecting **Cancel** from this point onwards.

5. Complete the following fields on the dialog:
   - **Point Type**: Select the point type for the unit from the dropdown list
   - **Include Tamper Events (Input Points only)** checkbox: This box is only enabled for input points. Ticking this checkbox will create 2 additional points for “Short” and “Open” event types which are two new alarm states that an input point can be in.
   - **Point List**: Select the points to be added to the unit from the list. More than one point can be selected.
   - **Time Schedule**: Select the Time Schedule that will be assigned to the External Alarm Monitoring point.
   - **EAM Type**: Read only. This field specifies the event type for the selected point. If an Input Point or Input Point group is selected only Alarm/Normal even types, will be displayed. If an Intrustion Point or Intrusion Point group is selected, only Secure/Unsecure event types will be displayed.
   - **User ID**: This field is only visible for Intrusion points. Specifies the User ID that triggered the Secure/Unsecure events.
6. Select **Next** when all the necessary fields are complete.
   ⇨ This dialog allows you to configure the External Alarm Monitoring events.
7. Complete the following Fields:
   - **Point Number**: Specify the point number that will be reported to the alarm monitoring company. This is an identifier for the alarm company and it doesn’t match the point number in configuration in SiPass integrated.
   - **Allocated Point Number**: Read Only. This number ranges from 1 to 255 and it is automatically assigned to an allocated number.
   - **Point Description**: Specifies the event name for each event type and point. Automatically generated but can be edited.
   - **Sample Event Name**: Read Only. Specifies the event name for each type and point
   - **Sample Message**: Read Only. Specifies the event message name that will appear in the active audit trail window when the event occurs in the system.
   - **Reset to defaults** button: This button resets all the fields to its default and automated entries.
8. When finished, select **Next**, successively for each point, until they’re all complete. When you reach the last point, select **Finish**.
9. The External Alarm Monitoring points have now been configured.
10. To add subsequent units, you can use the **New** button located on the lower right hand side of the dialog.

3.14.3 Configuring External Alarm Point details

1. Select **External Alarm Monitoring** from the **System** toolbar or menu.
2. Expand the tree under ACC Controllers, until the EAM units are displayed.
3. Select any of the EAM units.
4. To add subsequent units, use the **New** button located on the lower right hand side of the dialog.
5. Click **Save**.

Field	Description
Event Name	Displays the name of the event, automatically generated if point was created using the Auto Wizard.
Time Schedule	Select from the list of available time schedules that can be assigned to the event.
Point Type (Trigger 1 and Trigger 2)	Select a member (input points, input point group, area point, area point group) that can be assigned to this event.
Source (Trigger 1 and Trigger2)	Displays the list of available points, depending on the Point Type selected above.
Event Type (Trigger 1 and Trigger 2)	Displays the list of states that can be assigned to the External Alarm Monitoring point. Select from **Alarm**, **Normal**, **Secure** and **Unsecure.**
Logical Operator:	This specifies if the second trigger (Trigger 2) is enabled. It is only enabled if the Point Type is an Input or Intrusion point. The list of available operators is below. • **NONE**: When selected the second trigger (Trigger 2) is enabled. • **AND**: This enables the second trigger (Trigger 2). When selected, the event will only take effect if the first and second trigger event occur simultaneously. • **OR**: Enables the second trigger (Trigger 2). When selected, the event will only take effect if either the first or second trigger event occurs
Message	Specifies the message that appears in the active Audit Trail window when the event occurs in the system. This is automatically generated if the point was created using the Auto Wizard
Point Number:	This specifies the point number that will be reported to the alarm monitoring company. This is automatically generated if the point was created using the Auto Wizard.
EAM type	This is the notification that is sent to the alarm monitoring company. Select from four alarm types: **Alarm**, **Normal**, **Secure** and **Unsecure**.

4 Personnel Management

SiPass integrated operators and cardholders make up the personnel at a SiPass integrated site. Operators are grouped by **Operator Groups**, and Cardholders are grouped according to **Work Groups**. This information is defined in the SiPass integrated system.

The SiPass integrated system contains information about the personnel who use the site and about the site itself. The system uses this information to accurately monitor events, and to display detailed information about personnel to authorized operators. For these reasons, it is essential to keep the SiPass integrated system up-to-date.

4.1 Operator Groups

To limit the access an operator has to records contained in the SiPass integrated system, each operator must be assigned to an Operator group. Members of an Operator Group are conferred a required level of access / privileges to the system, to carry out their jobs.

The concept of separating the privileges that Operator Groups have is called **Operator Partitioning**.

When an operator is created, that operator must be assigned to an operator group. The operator will then be assigned the privileges defined for that group. An operator can only grant the same or a subset of the privileges belonging to their own operator group

4.1.1 Creating an Operator Group

Creating an Operator group includes assigning an operator group name, establishing the viewable Audit Trail events, System Functions, Access Controls, Password Complexity Rules and available Site Plans.

When creating an operator group, the system administrator will only be able to see and grant access to those functions to which their own operator group has access.

There are 3 key areas to fill out:

- **General**: Determines password restrictions and audit trail viewing
- **Operator Functions**: Determines which system functions and cardholder fields are available
- **Partition Functions**: Determines which objects in the system are available

To create an Operator Group

1. Select **Operator Group** from the **Program** toolbar to display the *Operator Group* dialog.
2. Complete the fields in the *General* section.

If some operator group options are changed, any operator who belongs to that group and is currently using a Client must log off and then log back on before the changes take effect.

3. Select **Cardholder Fields** to assign some or all of the cardholder fields to this operator group. For example, you might not want one operator group to be able to view cardholder PINs.
   - Once a field is selected you can double click it to change the privilege from [**v**] (View) to [**e**] (Edit)

Changing the privileges is not supported for the **Imaging** field. When selected, all the privileges (create, view and edit) are applicable for the field.

4. Select **System Functions** to assign some or all of the system functions to this operator group. For example, you need to add the **Cardholder** System function if you want this operator group to modify cardholder records.
5. Select a function and click **Add** to add just the one, or click **Add All** to add them all at the same time
6. Select the level of privilege, by double-clicking on the system function, to change the privilege level.
   - **c** (Create): Allows members of the group to create, delete and view database records.
   - **v** (View): Allows members of the operator group to view the records only.
   - **e** (Edit): Allows members of the group to view and modify existing Database records.
7. Select **Audit Trail Reports** if your operator group has access to reporting functions.
   - Select the Audit Trail Reports over which the operator has control.
8. Select **Device Group**, to assign device groups to your operator group.
   - These are like a point group but for devices. The operator group requires access to a device via a Device Group to view and modify the device.
9. Select **FLN Group** to assign FLN groups to your operator group. These are like a point group, but for FLNs. The operator group requires access to an FLN via a FLN Group to view and modify it.
10. Select **Holiday** to assign your system defined Holidays to an operator group. Operators can only view and modify holidays that they have privileges to.
11. Select **Site Plan** to assign site plans to your operator group. This defines which site plans they can view and modify.
12. Select **Point Groups** to assign point groups to your operator group. Please note this will affect the points an operator can see.

To be able to view an Access Group, the operators should have view (**v**) privileges for all the Access Levels that belong to that Access Group.

To be able to view an Access Level, the operators should have view (**v**) privileges for all the Point Groups, Points, etc. that belong to that Access Level.

To be able to view/update a Point, the operators should have at least one Point Group containing that Point assigned to their Operator Group.

13. Select **SiPass Explorer Items** to assign appropriate privileges for individual SiPass Explorer items to your operator group.
14. Select **Time Period** to assign specific time periods to your operator group.
15. Select **Unit Group** to assign Unit groups to your operator group. These are like a point group but for Units. The operator group requires access to a Unit via a Unit Group to view and modify it.
16. Select **Work Groups** to assign Work Groups to your operator group.

Only Partition Work Groups will be listed here for Operator Partitioning.

17. Select the work groups over which the operator has control. Please note that only those cardholders that belong to the assigned work groups can be administered by the Operator. Any audit trail entries (including reports) relating to cardholders that do not belong to these assigned work groups will not appear when the Operator is logged on.
    - If no workgroups are assigned to an operator group, that operator group will be unable to create cardholder records. Also, no card accesses will be visible to that operator from the Audit Trail.
18. Select **Component Group** to assign Component Groups to your operator group.
19. Click **Save**.

4.1.1.1 General Details

This table lists the general details that can be changed. These include the group name, lockout status, audit trail viewing and password complexity.

Setting	Description
Operator Group Name	This is a unique Name for the Operator group. You may enter up to 40 characters, in any combination of upper and lower case letters and numbers.
Group Lock Out	When checked, this denies access to the SiPass integrated system to all members of the specified operator group. This check box is only available to administrators and members of an operator group that have privileges within the group displayed. You cannot lock out your own operator group.
Logon/Logoff	When checked, logon and logoff activities will appear in the Active Audit Trail window for the Operator Group currently being configured.
Comms actions	When checked, communications activities will appear in the Active Audit Trail window. Included are comms related activities such as initialization, comms lost, comms restored, dial up activity and other general communications events.
Alarm actions	When checked, information regarding alarms that have been received, actioned or waiting to be actioned, etc. will appear in the Active Audit Trail window. Many of these messages are “free-form” text.
Database actions	When checked, Database events such as Adding, Editing or Deleting records, and Backing up, Restoring or Purging activities will appear in the Active Audit Trail window.
Event Task	When checked, all types of event task related messages, many of which are “free-form” text, will appear in the Active Audit Trail window.
Detailed Logging	When checked, displays detailed Audit Trail information when records are updated.
Min. Password Age (days)	Specifies the minimum number of days after the operator has changed the password before it can be changed again.
Min. Password Length	Specifies the minimum number of characters allowed in the password

Setting	Description
Logon Retries	Specifies the number of allowed logon attempts with the wrong password before the operator account is locked out.
Max. Password Age (days)	Specifies how old the password can be before the operator is forced to change it.
Account Lockout Duration (mins)	Specifies how long an operator account is locked out when the logon retries are exceeded.
Password Complexity Check	Turns the password complexity check on and off. When the complexity check is turned on the password must include three of the following character types: • Number (e.g. 1234) • Special character (e.g. !%$#) • Uppercase character (e.g. A) • Lowercase character (e.g. a)

4.1.2 Report Privileges

The Report privileges are handled like a tree. You can assign privileges to a folder, a specific report or a folder plus reports. The following privileges apply:

Privilege	Folder	Report
View [v]	Report folder will be visible to the operator in SiPass Explorer.	Report will be visible to the operator in SiPass Explorer.
Edit [e]	Report folder can be modified by the operator in SiPass Explorer.	Report can be modified by the operator in SiPass Explorer.
Create [c]	Reports can be created by the operator within this folder in SiPass Explorer. The operator can also delete the folder.	Report can be deleted by the operator in SiPass Explorer.

To give Reports privileges to an Operator Group:

1. Ensure the Report section is opened in the *Operator Group* dialog and the correct Operator Group is selected.
2. Select a report or folder from the Reports tree and click **Add >** or **Add Hierarchy >>**.
   - **Add >** just adds the selected folder or report.
   - **Add Hierarchy >>** adds the selected item and all its child elements in the tree.
3. Right click the folder or report and select **View**, **Edit** or **Create** to modify the privilege assigned.
4. Remove unwanted reports or folders by selecting the item and clicking **Remove >** or **Remove Hierarchy >>**.
   - **Remove >** only removes the selected folder or report.
   - **Remove Hierarchy >>** removes the select item and all its child elements in the tree.
5. Click **Save**.

4.2 Operators

Operators are responsible for maintaining the System Database, and monitoring the site. They must have access to system information, but there may be occasions where you wish to impose limits on what an operator can change.

Operator Privileges determine whether an operator can view, edit or create a wide range of information on the Database. These privileges are assigned to Operator Groups. When you define an Operator Group, you define its privileges, which then apply to all operators in that group.

4.2.1 Adding Operators

Adding an operator to the system includes providing the operator with a user name, assigning them to an appropriate operator group and designating a Time Schedule during which they may log onto the system.

▷ Ensure that all the operator groups have been established, along with the appropriate privileges. Each operator must be assigned to an operator group.

1. Select **Operator** from the **Program** menu.
2. Complete the operator's identification details.
3. (**Optional**) Complete the automatic logon details. Use the Windows logon to log into the SiPass workstation. Tick this checkbox to enable the operator to log straight into the SiPass client from Windows, without having to enter a new username and password.

   ⇨ A *Select User* dialog will appear, prompting you to select a domain and user.
4. Complete the operator's access details.

   – The **Time Schedule** table at the end of this section provides an example of the effect that a Time Schedule has on an operator.
5. By right-clicking anywhere inside the *Operator* dialog, the *General* tab of the *System Preferences* dialog appears. This allows you to change the default operator expiry date.
6. Click **Save**.

Time Schedule	Description
Never	The operator can never log on to the SiPass integrated system.
Always	The operator can always logon.
System Function	The operator can only log on between 2 am and 3 am every day of the year including holidays.

4.2.1.1 Operator Details

The following table lists the operator details that can be set.

Detail	Description
Last Name	Operator's last name. You may enter up to 30 characters, in any combination of upper and lower case letters and numbers.
First Name	Operator's first name. You may enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Password	The operator's password is required when logging on to SiPass integrated. The password is encrypted and appears as asterisks on screen. You may enter up to 128 characters in any combination of upper and lower case letters, numbers and symbols. The password is case sensitive and is required each time the operator logs on to the SiPass integrated system.
User Name	The operator's user name is required when logging on to SiPass integrated. The user name must be unique to the system. You may enter up to 20 characters in any combination of upper and lower case letters and numbers.
Confirm Password	Confirmation of the operator's password. Unless the entry into the Confirm Password field matches the entry into the Password field, the operator's record will not be saved in the system
Operator Group	Specifies the operator group to which the operator will be assigned. The operator group determines the level of access and the privileges the operator has available when using SiPass integrated. To assign an operator group, choose the drop down arrow and select a group from the list.
Time Schedule	Specifies the Time Schedule during which the operator can log on to the SiPass integrated system.

Detail	Description
Expiry Date	The date after which the operator's log on access is denied. To change the date, choose the drop down arrow and select a new date from the displayed calendar. To disable the expiry date (the operator will always have log on privileges), simply de-select the checkbox.
Operator Lock Out	When checked, the operator is denied access when attempting to log on to the SiPass integrated system. If the operator has been locked out, a dialog will appear informing the operator that they have been denied access to the SiPass integrated system. If an operator is locked out, only an operator that belongs to the Administrator operator group or a group with higher privileges can change this setting.
Password Never Expires	When checked the operators password will never expire and will always work on this account.
Can't Change Password	When checked means the operator can not change their password at logon by selecting the Change Password button.
Technician	This checkbox is read-only and will be checked only if the Technician Operator Group has been selected. This group is not available in a default installation.
Require Windows User Authentication	Instead of automatically logging in with the Windows user credentials, the operator must supply their Windows username and password to login. **Note:** When using the integrated Windows login functions with SiPass integrated, a real password must be used. This means that your Windows password cannot be blank. A blank password will fail to connect and the SiPass integrated client will not start.

4.2.2 Searching for an Operator

SiPass integrated allows you to search the Database for a specific operator based on details you supply about that operator. The more details you supply, the narrower the search becomes and there is less chance of more than one matching record being found. The Search function will only reveal those operators who are present in an operator group to which you have privileges.

Searching the Database for an operator's record will be more efficient and quicker if you provide as much information about the operator as possible to narrow the search.

1. Choose **Operator** from the **Operator** toolbar or the **Program** menu to display the *Operator* dialog
2. Enter all or part of the details known about the operator into the respective fields displayed in the Operator dialog. Data may be entered into more than one field to narrow the search.
3. Choose **Search** to begin the Database search.
   - ⇨ The *Operator Records* dialog will appear if more than one operator's record matches the search criteria. If only one record matches the search criteria, then that operator's information will be displayed directly in the *Operator* dialog.
   - ⇨ Only those operator records to which you have access will be displayed. The Search button is only visible when a record is not currently displayed. The Search button changes to a "Reset" button when an operator record is displayed. To clear the dialog fields and perform a search, choose either **Reset** or **Clear**.
4. To select an operator from the *Operator Records* dialog, double-click anywhere on that operator's row, or select the operator and choose **OK**.

⇨ The selected operator's record will be retrieved from the Database and will appear in the *Operator* dialog.

4.3 Workgroup

Workgroups are logical groups to which selected cardholders belong. Generally, cardholders whose jobs are the same or similar will belong to the same Workgroup.

Types of Workgroups:

You may, or may not want to allow operators to have privileges to view/create/edit the partition functions of a workgroup. Based on whether want to confer these Operator Partitioning privileges to an operator, there are two kinds of workgroups that can be created:

- **Partition Workgroups**

Operator Partitioning is possible with Partition Workgroups. The ability to View / Create / Edit the Partition Workgroup depends on the operator privileges conferred to the operator group.

These partition workgroups can be used for assigning Access Control and Anti-Passback control.

A cardholder can be configured to only one partition workgroup.

The level of partition privileges the operator can configure to his/her operator group depends on the operator's own privileges.

For detailed information on these workgroups, refer the section Partition Workgroups [➙ 89].

- **Non-Partition Workgroups**

Operator Partitioning is **not** possible with Non-Partitioned Workgroups.

A cardholder can be a member of multiple Non-Partition Workgroups.

They can be used for assigning Access and Anti-Passback control.

For detailed information on these workgroups, refer the section Non-Partition Workgroups [➙ 90].

4.3.1 Work Group Fields

The sections that follow provide details of fields and other configuration options on the *Work Group* dialog.

4.3.1.1 Work Group Configuration Tab Fields Description

Field	Description
Work Group Name	Specifies a unique name for the work group. You may enter up to 40 characters, in any combination of upper and lower case letters and numbers.
Void Work Group checkbox	When checked, all cardholder cards belonging to this work group will be voided and all cardholders belonging to that work group will be denied access at all access points.
Partition Group checkbox	When checked, the work group created will be considered a Partition Work Group.
Clear Card Number (enabled for visitor only)	Tick this checkbox to clear the card number for a visitor under the visitor dialog.
Department	Indicates that the work group is an internal department.
Contractor	Indicates that the work group is an external contracting company.
Other	Indicates that the work group is a miscellaneous group that does not belong to either a department or contractor.
Visitor	Indicates that the work group is a dedicated group for visitors.

Clear Card Number (enabled for visitor only)	Tick this checkbox to clear the card number for a visitor under the *Visitor* dialog. This checkbox is enabled only when the **Visitor** checkbox is ticked.
Access Control box	Displays the access control details configured for the selected work group.
Disable Access Control checkbox	Tick this checkbox to temporarily disable any inherited access privileges for the selected workgroup. To re-enable the access privileges, un-tick this checkbox.
Access Privileges button	Clicking this button displays the *Access Assignment* dialog, where access privileges for the workgroup can be created or modified.

4.3.1.2 Contact Tab Field Description

Name	Specifies the name of the primary contact for the work group. You can enter up to 40 characters, in any combination of upper and lower case letters and numbers.
Title	Specifies the primary contact's title. You can enter up to 20 characters, in any combination of upper / lower case letters and numbers.
Addr	Specifies the primary contact's home address. You can enter up to 80 characters, in any combination of upper and lower case letters and numbers.
Phone	Specifies the primary contact's home phone number. You can enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Fax	Specifies the primary contact's fax number. You can enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Mob	Specifies the primary contact's mobile phone number. You can enter up to 20 characters, in any combination of upper and lower case letters and numbers.

4.3.2 Partition Workgroups

This section will explain the concept of Partition Workgroups.

Only Partition Workgroups can be used for Operator Partitioning.
Each cardholder can be configured to only ONE partition workgroup.
They can be used for assigning Access and Anti-Passback control.

Creating Partition Workgroups

For details on how to create Partition Workgroups, refer the section Creating Partition Workgroups [→ 90] of this manual.

Searching/Selecting Partition Workgroups

Once configured and saved, Partition Workgroups will be listed in the following dialogs:

- In the **Workgroup Name** dropdown field of the *Work Group* dialog. The ability to View / Create / Edit the Partition Workgroup depends on the operator privileges conferred to the operator group.
- In the **Workgroup Id** dropdown field of the *Cardholder* dialog. Only Partition Workgroups will be listed here. However, the ability to view these workgroups depends on the operator privileges conferred to the operator group.

Searching for a Cardholder belonging to a Partition Group

Operators can use the **Search** button on the *Cardholder* dialog to list or find a cardholder/s that belongs to a Partition Group.

In order for operators in an operator group to view cardholders belonging to Partition Workgroups assigned to them, they must be given operator privileges to **Customized** and **Pre-defined Cardholder reports**. These can be found within the **SiPass Explorer** items under **Partition Functions** displayed in the *Operator Group* dialog.

4.3.2.1 Creating a Partition Work Group

1. Select *Operation* > *Work Group* from the main menu.
   ⇨ The *Work Group* dialog is displayed. This dialog displays a tree view of all the available work groups, on its left panel.
2. Select the *Work Group Configuration* tab.
3. Enter a name for the work group in the **Work Group Name** field. You can search for existing work groups by clicking the **…** button.
   – **Note**: This name should be as descriptive as possible. This will help SiPass operators identify the Work Group easily. Enter up to 40 characters, in any combination of upper and lower case letters and numbers.
4. By default, the **Partition Work Group** checkbox is ticked. This checkbox is enabled only when creating a new work group.
5. Select the **Group Type**. For more information on each option, refer the field descriptions of the **Group Type** in the section Work Group Configuration Tab Fields Description [→ 88].
6. Click **Save**.
   ⇨ This workgroup will be saved as a Partition Work Group.
7. **From the perspective of an operator's privileges:** Partition workgroups can be selected on the *Operator Group* dialog for operator partitioning of the workgroup partition functions. You can view this partition workgroup list by navigating in the following manner from the main menu: *Program* > *Operator Group* > *Partition functions* > *Work Groups*

See also

Automatic Bulk Card Creation [→ 93]

4.3.3 Non-Partition Workgroups

This section will explain the concept of Non-Partition Workgroups.

Non-Partition Workgroups are NOT available for Operator Partitioning.
They can be used for assigning Access and Anti-Passback control.

Creating Non-Partition Workgroups

For details on how to create Non-Partition Workgroups, refer the section Creating a Non-Partition Work Group [→ 91] of this manual.

Searching/Selecting Non-Partition Workgroups

Once configured and saved, Non-Partition Workgroups will be listed in the following dialogs:

- In the **Workgroup Name** dropdown field of the *Work Group* dialog.
- Clicking the **Work Groups** button of the *Advanced* tab in the *Cardholder* dialog will display the *Cardholder's Work Groups* dialog. The operator can view the Non-Partition Workgroups in this dialog, and select a workgroup/s to be configured for the cardholder. The selected Non-Partition workgroups will be listed in the **Work Groups** section of the *Advanced* tab.

4.3.3.1 Creating a Non-Partition Work Group

1. Select *Operation* > *Work Group* from the main menu.
   ⇨ The Work Group dialog is displayed. This dialog displays a navigation tree on its left panel. Here, you can view the hierarchy of all the work groups available in the system.
2. Select the *Work Group Configuration* tab.
3. Enter a name for the work group in the **Work Group Name** field. You can search for existing work groups by clicking the **…** button.
   – This name should be as descriptive as possible. This will help SiPass operators identify the workgroup easily. Enter up to 40 characters, in any combination of upper and lower case letters and numbers.
4. Untick the **Partition Work Group** checkbox. This checkbox is enabled only when creating a new work group.
5. Select the **Group Type**. For more information on each option, refer the Field Descriptions of the Group Type box in the section Work Group Configuration Tab Fields Description [→ 88].
6. Click **Save**.
   ⇨ This workgroup will be saved as a Non-Partition Work Group.
7. **From the perspective of an operator's privileges:** Non-partition workgroups cannot be used for Operator Partitioning, and will not be listed in the *Operator Group* dialog for operator partitioning of the workgroup partition functions.

4.3.4 Configuring Workgroup Access Privileges

1. Select *Workgroup* from the *Operation* menu.
2. Find or create the workgroup record whose access privileges to be changed.
3. Click on the **Access Privileges** button. The *Access Assignment* dialog is displayed.
4. Click the *Access Assignment* tab.
5. From the **Access Type** field drop down list, select the access objects that should be included in the workgroup privileges.
   – If you wish to create new, or modify existing access levels and groups, click the *Access Group Definition* tab, and *Access Level Definition* tab, and configure these tabs as required.
6. The select access type object names will be listed in the adjacent box of the *Access Assignment* tab.
7. Select the access type object and click **Add**, to add them to the workgroup's access privileges.
8. Click **OK**. You will be returned to the *Work Group* dialog.
   ⇨ The selected access privilege is displayed in the **Access Control** section of this dialog.
9. Click **Save**.
10. For instructions on how to assign these workgroup access privileges to a bulk set of card/cardholders, refer the section Automatic Bulk Card Creation [→ 93].
11. For instructions on how to assign these workgroup access privileges to a specific cardholder, refer the section Assigning Cardholder's Workgroup Access Privileges [→ 129].

4.3.4.1 Temporarily Disabling Workgroup Access Privileges

It is possible to temporarily disable inherited access privileges for a specific workgroup. This means that all the cardholders belonging to this workgroup will not be able to use the access privileges of this workgroup, until its access privileges are re-enabled.

1. Select *Workgroup* from the *Operation* menu.
2. Find the workgroup record whose access privileges to be temporarily disabled.
3. Check the **Disable Access Control** checkbox.
4. Click **Save**.

⇨ The access privileges of the selected workgroup are temporarily disabled. To re-enable its access privileges, un-tick the **Disable Access Control** checkbox.

4.3.4.2 Modifying Workgroup Access Privileges

1. Click *Operation* > *Work Group* from SiPass main menu to display the *Work Group* dialog.
2. Enter the name of the work group in the **Work Group Name** field, or click the **…** button to search for a work group. Alternatively, you can also select the work group from the left navigation tree.
3. Click the **Access Privileges** button of this dialog.
   ⇨ This displays the *Access Assignment* dialog.
4. Click the access privilege to be modified, in the **Access Control** box of this dialog.
5. Click the **Remove** button, or double-click the item. This will delete the item from the box.

⇨ You can now add new access privilege/s to the box if required.

4.3.5 Voiding a Workgroup

When a work group is made void, all cardholder cards belonging to this work group will be voided, AND all cardholders belonging to that work group will be denied access at all access points.

1. Click **Operation** > **Work Group** from SiPass main menu to display the *Work Group* dialog.
2. Enter the name of the work group in the **Work Group Name** field, or click the **…** button to search for a work group. Alternatively, you can also select the work group from the left navigation tree.
3. Tick the **Void Work Group** checkbox.
4. Click **Save**.

4.3.6 Deleting a Workgroup

1. Click **Operation > Work Group** from SiPass main menu to display the *Work Group* dialog.
2. Enter the name of the work group in the **Work Group Name** field, or click the **...** button to search for a work group. Alternatively, you can also select the work group from the left navigation tree.
3. Click **Delete**.
4. Click **Yes** to confirm your action.

⇨ This workgroup will be deleted from the system.

4.3.7 Configuring Card Profiles for Workgroups

1. Select the *Card Configuration* tab of the *Work Group* dialog.
2. Click the **Smart Card Profile** drop down list, and select a profile to be assigned to this work group.
3. Click the **Update Cardholders** button.

   ⇨ This action updates this smart card profile to the *Advanced* tab of the *Cardholder* dialog, for every cardholder in the selected work group.
   – **Note**: If the **Profile** field, detailed above, is cleared or left blank, the cardholders in the selected workgroup will no longer be configured with this smart card profile.
4. Click **Save** to save your configuration.

4.3.8 Automatic Bulk Card Creation

Once you have defined a Work Group it is possible to automatically create a set of cards and assign them to it. This way, you can automatically apply the same set of access control privileges to a set of cards.

Note: Bulk cards cannot be created automatically for non-partition workgroups.

▷ Ensure that you have created and saved the Work Group for which you wish to create a bulk set of cards automatically.

1. Choose **Work Group** from the **Operation** toolbar or menu.
2. From the **Work Group Name** drop-down box, select the name of the Work Group in which you wish to create a bulk set of cards.
3. Ensure that the correct Work Group details are complete, including the Work Group's access control privileges (if required).
4. Enter the range of cards to be automatically created in the **Card Range** field. For example "11-15" will create cards 11, 12, 13, 14, and 15.
5. Choose the **Create Cards** button.

   ⇨ SiPass integrated will now begin creating all cards in the range specified. A *Status* dialog will appear indicating the status of the bulk creation of cards.
6. When finished, choose **Close**.

4.3.9 Configuring Cardholder Workgroup for Anti-Passback Assignment

1. Navigate to the *Advanced* tab of the *Cardholder* dialog for the cardholder to be configured for workgroup anti-passback count.
2. In the **Work Groups** section of this tab, tick the **Use for Anti-Passback** checkbox for the Partition / Non-Partition Workgroup that should be configured for the cardholder's anti-passback count.
3. Click **Save**.

⇨ **Note**: Only one workgroup listed in this section can be used to be included in the cardholders anti-passback count.

4.4 Credential Profile

The Credential Profile feature gives collections of workgroups the flexibility to use different card formats for access control and security. Cardholders can be configured with multiple cards of different credential profiles.

Components of the Credential Profile

The Credential Profile is defined by the following components:

- **Name**: This field details the name of the Credential Profile.
- **Card Technology**: This field details the Card Technology assigned to this credential profile.
- **Facility Code**: This field details the Facility Code of the credential profile.
- **Validity Code**: This field details the Validity Code of credential profile.
- **PIN Mode**: This field details the Operation Mode configured for the credential profile.
- **PIN Digits**: This field details the number of digits that can be configured for the card's PIN Number.
- **In Use**: This field details if the card is in use. If ticked, it indicates that this Credential Profile has been applied to at least one card.

Once created, a Credential Profile can be configured to a cardholder's card.

Two valid cards cannot have the same credential profile. When displayed as being '**In Use**', the **Name**, **Card Technology**, **Facility Code** and **Validity Code** of that particular card cannot be modified.

Navigating to the Credential Profile

The *Credential Profile* dialog can be accessed in two ways:

- Select **Program** > **Credential Profile**.

OR

1. Select **Operation** > **Cardholder**.
2. Next, click the *Definition* tab.
3. Click the **Credential Profile** button.

4.4.1 Adding / Deleting Credential Profiles

1. Select **Program > Credential Profile** from the main toolbar to display the *Cardholder's Credential Profile* dialog.
2. To add a credential profile, select **Add**.
   ⇨ A new row will be added to this dialog. Once configured and saved, each row corresponds to an individual Credential Profile.
3. Select a cell under the **Name** column. This field can be edited by typing into it.
4. Select a cell under the **Card Technology** column. This field can be configured by making a selection from the cell's drop-down list.
5. Select a cell under the **Facility Code** column. This field can be edited by typing into it.
6. Select a cell under the **Validity Code** column. This field can be edited by typing into it.
7. Select a cell under the **PIN Mode** column to configure an operation mode for the profile.
8. Select a cell under the **PIN Digits** column. This field can be edited by typing into it.
9. Select a cell under the **In Use** column.
   ⇨ This field will change depending on whether the Credential Profile has been assigned to a card. When assigned, it will display as **Yes**. If not, it will display as **No**.
10. To delete a Credential Profile, select the appropriate profile row and click **Delete**.

Operators can also access the *Cardholder's Credential Profile* dialog from the *Definition* tab on the *Cardholder / Visitor* dialog. Click the **Credential Profile** button on this tab to display the dialog. If more than one card configured to a cardholder has the same Credential Profile, only one of them will be valid.

4.5 Cardholders

SiPass integrated allows authorized personnel and their movements at your site to be identified and tracked. To effectively track cardholder movements, new cardholders' details must be entered into the system and those records updated when their details or access privileges change.

In addition to the default tabs, the *Cardholder* dialog also supports customizable cardholder fields, called pages. These controls provide the functionality and the opportunity to collect a significant amount of additional cardholder information.

Once the information about a cardholder has been entered into the system and access privileges have been established, that cardholder's access to the site can be monitored and controlled. If the *Photo ID and Image verification Module* is installed, photo ID access cards can be created which can incorporate a cardholder's photograph and signature.

4.5.1 Cardholder Tabs and Tab Fields

The sections that follow will detail the fields available on the *Definition*, *Advanced*, *Personal*, *Vehicle*, *Imaging*, *Tracking* and *Control* tabs of the *Cardholder* dialog.

Once a cardholder has been saved, the following four fields will appear at the base of the *Cardholder* dialog, and will remain visible while the operator navigates any of the dialog's tabs:

- **Last Name**: Displays the last name of the cardholder;
- **First Name**: Displays the first name of the cardholder;
- **Card No**: Displays the card number of the cardholder.

If this field is displayed as ***Card No**, it implies that at least one other card has been assigned to this cardholder. The details of the additional card/s can be found on the *Advanced* tab.

- **Updated**: Displays the Date and Time at which this cardholder was last updated.

4.5.1.1 Definition Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Photo Panel	Found under Access Control on this tab, this panel displays the stored photograph of the cardholder, if one already exists.
Last Name	Specify the cardholder's last name. You may enter up to 30 characters, in any combination of upper and lower case letters and numbers.
First Name	Specify the cardholder's first name. You may enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Employee Number	This field must be entered if the Employee Number Enforced option has been enabled in *System Preferences*. You may enter up to 16 characters in any combination of upper and lower case letters and numbers.
Work Group Id	Specify the work group to which the cardholder will be assigned. To change the work group, select a new work group from the drop-down list. If you have not defined any work groups in the SiPass Database, you may select **None** from the list. It is recommended that cardholders be re-assigned to an appropriate work group at a later stage. **Note**: Only partitioned Work Groups will be displayed in this field.
Define Work Group button	This button brings up the *Work Group* dialog.
Search button	This button displays the *Search Cardholder* dialog.
Next button	This button displays the next cardholder in sequential card number order, to the one presently displayed.
Previous button	This button displays the previous cardholder in sequential card number order, to the one presently displayed.
View History button	This button displays the *View History* dialog.
Credentials Window	This box displays the credential details of cards configured to the cardholder.
Card Number	This field should contain a cardholder's number that is unique to the system. The number of digits in the card number, and the maximum number of cardholders, will be dependent on the SiPass card technology that you purchased with your license.
Credential Profile	Displays the Credential Profile of the card
PIN	Indicates the cardholder's Personal Identification Number. To select a PIN for the current cardholder, click on the button on the right next to the field which will display a list of PIN's available for use. This field will be updated immediately when the cardholder's card number is entered. The cardholder may use their PIN if particular readers at your site have been configured for both Card and PIN. This field will be hidden unless the operator has the "See PIN" Operator Privilege assigned.

Item	Description
Void Cardholder	When checked, all cards that are assigned to the cardholder card become void. The cardholder will not have access to any point at your site.
Start Date	Specifies the cardholder's start date. To change the date, click the drop down arrow from the Start Date field below, and select a new date from the displayed calendar. See explanation at the end of the table.
End Date	Specifies the cardholder's end date. To change the date, click the drop down arrow of the End Date field below, and select a new date from the displayed calendar. To disable the end date (the cardholder will always exist in the database), simply un-tick the checkbox. See explanation at the end of the table.
PIN Error Disabled	If this checkbox is ticked, it implies that this card has been made void because the PIN was entered incorrectly 3 times. The operator can un-tick this checkbox, which configures the card to be valid for PIN access again.
Status	Indicates the status of the cardholder's card. The following describes the possible status: • **Valid**. Access will be granted. • **Work Group void**. The workgroup to which the cardholder belongs has been voided and all members belonging to that group will be denied access privileges. • **Void**. The Void Card check box for the cardholder has been selected. Access will be denied. • **Expired**. The end date of the cardholder's card has passed. Access will be denied. • **Before start date**. The start date on the cardholder's card has not yet been reached. Access will be denied.
Add button	This button adds a new row of card credentials in the Credentials box.
Delete button	This button deletes a selected row of card credentials in the Credentials box.
Credential Profile	This button displays the *Cardholder's Credential Profile* dialog.
Void Cardholder	Ticking this checkbox voids all the cards belonging to the cardholder, which will deny him access to the site.
Isolate	When checked, the employee is allowed to secure any area (to which they have been granted access), even if inputs are not sealed.
APB Exclusion	Ticking this checkbox will exclude the cardholder from any Anti-Passback areas that have been created.
Visitor	This checkbox indicates that the cardholder is a visitor to the site rather than a permanent cardholder.
Accessibility	Ticking this checkbox means that when this cardholder badges his card at a reader, the door will unlock for the Extended Latch Time rather than the normal latch time, permitting easier access. The Extended Latch Time is configured in the *Components* dialog.
Supervisor	Ticking this checkbox nominates the cardholder as a "Supervisor" for doors that are configured with the Dual Custody mode of operation. Some doors require a standard cardholder and a Supervisor to present an access card before access will be granted. Ticking this checkbox means that when this cardholder badges his card at a reader, the door will unlock for the Extended Latch Time rather than the normal latch time, permitting easier access. The Extended Latch Time is configured in the *Components* dialog.
Self Authorise	Ticking this checkbox will allow the cardholder to gain access to a door configured with the Dual Custody mode of operation, without needing the accompaniment of a subsequent cardholder before the door is unlocked.
Re-Entry Exclusion	Ticking this checkbox will exempt the cardholder from Timed Re-entry rules for areas that are operating in the Anti-Passback mode "Timed Re-entry".
Access Control Window	Displays the Access Privileges configured for the cardholder.
Access Privileges button	Opens *the Access Assignment* dialog to allow changes to access privileges.
Read	This button allows you to view the encoded cardholder information on a valid card. A dialog will appear containing the information held on the badged card.
Assign	This button allows you to assign a card to a cardholder. This is a toggle-state button.
Read and Search	This button allows you to read the encoded cardholder information on a valid card, and then search for the card number on the system. This is a toggle-state button.

Item	Description
Encode	This button encodes a smart card with the details of the selected cardholder. The number entered in the Card Number field can be encoded onto the smart card if a smart card reader is attached to the PC and Smart Card Encoding has been configured from the System menu.
New button	This button displays a new *Cardholder* dialog with empty fields.
Save	This button saves all the information configured on this dialog.
Delete	This button deletes this cardholder and all his/her assigned cards, from the database.

Operators may need to change the start or end date of cardholders.

When changed:

- Other Cardholder Credentials which have the same start or end date prior to these changes, are updated in addition.
- For Cardholder Credentials which have an earlier start or end date than the one entered; the operator will be prompted with a message notifying them that the new date is greater than the initial date, and asks if the operator would like to continue.
- If cardholder's end date is greater than 50 years in the future, the **End Date** check box will be un-ticked for that cardholder after saving the details.

4.5.1.2 Advanced Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Work Group Name field	Lists the names of the workgroups that the cardholder is assigned to.
Partitioning field	Specifies if the corresponding work group is a Partitioning Work Group.
Use for Anti-Passback field	Specifies the workgroup that should be used for the Anti-Passback area count.
Choose Button	Displays the *Cardholder's Work Groups* dialog.
Fingerprints Window	This box displays details of fingerprints captured by the system.
Index	Specifies which finger was used for the fingerprint capture.
Saved	Specifies whether the captured fingerprint is saved in the system.
Encoded	Specifies whether the fingerprint is encoded to card.
Credential Profile	Specifies the credential profile assigned to the card with this fingerprint
Smart Card Data (Profile)	This field displays the Smart Card Profile configured for the cardholder.
Profile Viewer button	This field dislays the *Profile Viewer* dialog.
General Data	This window can be used to enter general data about the cardholder.

4.5.1.3 Personal Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Title	Cardholder's title. You may enter up to 20 characters, in any combination of upper and lower case letters and numbers.
Date of Birth	Cardholder's date of birth. You may enter the date of birth in any format.
Address	Cardholder's home address. You may enter up to 60 characters, in any combination of upper and lower case letters and numbers.
Payroll Number	Cardholder's payroll number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers.
Phone Number	Cardholder's home phone number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers.
Mobile Number	Cardholder's mobile phone number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers. Note: In order to utilize the Message Forwarding to Mobiles feature of SiPass integrated, the following format is to be used for all mobile phone numbers: • The first part of the number should be the Country Code • The second part should be the local mobile phone number, excluding any leading zero. • The mobile phone number entered should not contain any spaces. For example, a fictitious mobile phone number 0123 123 123, should be entered in the following format: 61123123123, where 61 is the country code and the rest is the local mobile phone number.
Mobile Service Provider	Cardholder's mobile service provider. Select a mobile service provider from the pre-defined list. Service providers are configured in the Service Providers dialog, available from the Messaging option which is available from the System menu.
Pager Number	Cardholder's pager number. You may enter up to 16 characters, in any combination of upper and lower case letters and numbers.
Pager Service Provider	Cardholder's pager service provider. Select a pager service provider from the pre-defined list. Service providers are configured in the Service Providers dialog, available from the Messaging option which is available from the System menu.
E-mail Address	Cardholder's email address. Begin the Email address with SMTP (Simple Mail Transfer Protocol). E.g.: SMTP.username@emailprovider.com
Use Email address in Message Forwarding checkbox	Tick this checkbox if you want the cardholder's details to be available in the Event Task Effect for Message Forwarding – Forward to Email(s).
Username	Enter a unique username for the cardholder in this field. Note: Only cardholders who have a username and password can be configured as Organizers for Venue Bookings.
Password	Enter a unique password for the cardholder in this field. Note: Only cardholders who have a username and password can be configured as Organizers for Venue Bookings.

4.5.1.4 Vehicle Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Car Rego 1	Registration number of the cardholder's first vehicle. You may enter up to 10 characters, in any combination of upper and lower case letters and numbers.
Car Model 1	Model of the cardholder's first vehicle. You may enter up to 20 characters, in any combination of upper / lower case letters and numbers.
Car Colour 1	Color of the cardholder's first vehicle. You may enter up to 15 characters, in any combination of upper / lower case letters and numbers.
Car Rego 2	Registration number of the cardholder's second vehicle. You may enter up to 10 characters, in any combination of upper / lower case letters and numbers.
Car Model 2	Model of the cardholder's second vehicle. You may enter up to 20 characters, in any combination of upper / lower case letters and numbers.
Car Colour 2	Color of the cardholder's second vehicle. You may enter up to 15 characters, in any combination of upper and lower case letters and numbers

4.5.1.5 Tracking Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Card Trace checkbox	When checked, this check box allows all the valid card transactions performed by the cardholder to appear in the Audit Trail as special exception alarms.
DateTime Card Last Used	This field will display Date and Time details about when a card was last used
Card Number Last Used	This field displays the card number that was last used
Point Name	This field displays the access point details where the card was last used
Last Anti-Passback Location	This field displays details about the anti-passback location where the card was last used
Anti-Passback Credential Profile	This dropdown field displays the Card number and Credential Profile of all the cards assigned to the cardholder.
Forgive Card button	This button "forgives" a cardholder and permits them to exit or enter an area, where normally this would produce an Anti-Passback violation. A forgive feature permits access for the first use of a card at either an Entry or Exit reader.
Remove Card from APB button	This button removes the card from the Anti-Passback area.
Add Card to APB button	This button adds the card to the Anti-Passback area.

4.5.1.6 Control Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Card Number / Credential Profile	Drop down list to choose card/s assigned to the cardholder.
Access	Drop down list to choose between Access Points / Access Points Groups that will be displayed directly below this field.
Output	Displays a drop down list to choose between Outpoint Points / Output Point Group / Notification Zones / Notification Zone Groups that will be displayed directly below this field.
Add button	Adds the selections of the Access and Output fields to the Output Control section below.
Remove button	Removes selections from the Output Control section below.
Card field	Details the chosen card.
Access Point / Group field	Details the chosen Access Point / Group
Output Point / Group field	Details the chosen Output Point / Group
Time Schedule	Details the chosen Time Schedule
Filter Against Access Privileges checkbox	This selection filters this particular cardholder against all the access privileges configured for the same cardholder.

4.5.1.7 Imaging Tab

The fields and controls on this tab are explained in the table below.

Item	Description
Front Side tab	This tab will display a preview of the Card Template selected.
Reverse Side tab	This tab will display a preview of the Card Template selected.
Photo radio button	This button is used to display the image configured for the cardholder.
Signature radio button	This button is used to display the signature configured for the cardholder.
Live button	This button will connect the screen on this tab to video capture driver, to display a live image.
Capture button	The button captures the live image.
Import button	This button will bring up the Windows ‘Open’ dialog. The user can select a Graphics Image file from this dialog.
Export button	This button will import export the Graphics Image to a required location.
Contrast scale	This scale can be used to adjust the contrast level of the image displayed on the tab.
Brightness scale	This scale can be used to adjust the brightness level of the image displayed on the tab.
Card Template	This drop-down list displays the available Card Templates that can be selected.
Insert Card	This command is given to the Card Printer to insert a card for printing.
Eject Card	This command is given to the Card Printer to eject a card.
Print	This command is given to the Card Printer to print a card.

4.5.1.8 Custom Tabs

While some sites require minimal information concerning their cardholders, others may require very detailed information.

SiPass integrated allows you to customize cardholder records to suit your requirements in two ways:

- By adding additional pages to the *Cardholder* / *Visitor* dialog. Such additional pages are known as **Custom Pages**. Operators can design Custom Pages using an application within SiPass integrated known as SiPass Explorer.
- By customizing the layout of existing Predefined Pages of the *Cardholder* / *Visitor* dialog.

To access SiPass Explorer, select **SiPass Explorer** from the main menu.

For detailed information on Custom Pages, refer the section Custom Pages of the SiPass Explorer User Manual.

Configuring Custom Tabs on the Cardholder Dialog

An operator can design and create **Custom Tabs** for the *Cardholder* dialog.

These tabs are created by designing **Custom Pages** using the **SiPass Explorer** application. For detailed information on how to create Custom Pages, refer the SiPass Explorer User Manual.

The following steps are only required if Customizable Cardholder Fields have been created for the *Cardholder* dialog.

1. Choose the first customizable tab, in this case.
2. Complete each of the fields in the tab. Some fields can be populated from drop-down lists.

If there are any compulsory fields among the customizable fields, it is essential that they be completed. Failure to complete compulsory controls will generate an error.

3. New categories to the Custom Cardholder Fields can be added under the existing fields. Simply select a blank category from the drop down box in the field you'd like to add the category to and type in the name. When you have finished select Save.
4. When done, choose **OK**, You will be returned to the normal view of the Cardholder Custom Page.
5. Select any additional customizable tabs and complete the controls.
6. Click **Save**.

4.5.2 Adding Cardholders

This section provides simple instructions on how to add a cardholder to SiPass integrated.

▷ **Navigation from Main Menu:** *Operation > Cardholder > Definition* tab

1. Display the *Definition* tab of the *Cardholder* dialog. For descriptions on fields of this tab, refer Definition Tab [→ 96].
2. Complete the Cardholder's Identification details.
   - ⇨ A single row of cardholder credentials appears in the **Credentials** section of this dialog. You can save a cardholder without a card number, by deleting this default row, and then clicking **Save**.
   - ⇨ Once the cardholder has been saved their **Last Name**, **First Name** and **Card Number** is displayed along the bottom of the *Cardholder* dialog, for all the tabs associated with this dialog. This helps you concentrate on the cardholder whose details you are entering or modifying, without the need to constantly refer back to the *Definition* tab.
3. Click **Save**.
   This new cardholder is saved in the SiPass integrated system.
   If you would like to create access privileges for the cardholder, or configure this cardholder record in any other way, proceed to the sections that follow.

4.5.2.1 Configuring the DEFINITION Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Definition* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Definition Tab [→ 96].

Configuring Cardholder Identification Details

This section describes how to add/modify cardholder identification details on the *Definition* tab of the *Cardholder* dialog.

▷ **Navigation from Main Menu:** *Operation > Cardholder > Definition* tab

1. Display the *Definition* tab of the *Cardholder* dialog. For descriptions on fields of this tab, refer Definition Tab [→ 96].
2. Complete the Cardholder's Identification details.
   - ⇨ A single row of cardholder credentials appears in the **Credentials** section of this dialog. You can save a cardholder without a card number, by deleting this default row, and then clicking *Save*.
   - ⇨ Once the cardholder has been saved their **Last Name**, **First Name** and **Card Number** is displayed along the bottom of the *Cardholder* dialog, for all the tabs associated with this dialog. This helps you concentrate on the cardholder whose details you are entering or modifying, without the need to constantly refer back to the *Definition* tab.
3. Click **Save**.
   This new cardholder is saved in the SiPass integrated system.

Assigning Cardholder to Partition Workgroup

Navigation from Main Menu: *Operation* > *Cardholder*.

1. Click the *Definition* tab.
2. Open or Create a new record for the cardholder who is to be assigned a partition workgroup.
3. Select a Work Group from the **Work Group** drop down field. You can also click the … button to select from the list of partition workgroups.
   – **NOTICE! Note:** Only Partition Workgroups are listed in this field. For details on Partition workgroups, refer the section Partition Workgroups [→ 89]
4. Click **Save**.

⇨ The cardholder will be assigned to the selected partition workgroup.

Configuring Cardholders' Card & Card Credentials

The **Credentials** section of this tab is used to configure and display cards and card credentials for a cardholder. An operator can configure multiple cards for a cardholder.
Note: A maximum of 5 cards can be assigned to each cardholder.
On creating a new cardholder, a single row of cardholder credentials appears in the *Credentials* section of this dialog.

To Configure Card Credentials:

1. Navigate to *Operation* > *Cardholder* from the *SiPass* main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who needs to be configured a card.
4. Click **New** to add a new credentials row. Or, you can configure the default row of this section.
5. In the **Card Number** field, enter a card number that is unique to the system. The field can be filled by badging the respective card, and clicking the **Assign Card** button.
6. Select a **Credential Profile** for the card. If you wish to create or edit a credential profile, click the **Credential Profile** button on this tab.
   For details on creating a Credential Profile, refer the section Credential Profile [→ 94].
7. In the **PIN** field, type in a PIN number, or select a PIN from the drop down list. This is the cardholder's Personal Identification Number for this card.
8. If the **Void** checkbox is ticked, the card will be made void. The cardholder will not be able to access the site, using this card.
9. In the **Start Date** field, type or select the date when the card can be used for access by the cardholder.
10. In the **End Date** field, type or select the date after when the cardholder can no longer use this card for access.

11. To disable the end date, simply un-tick the checkbox of the **End DateTime** field below.
12. Save your changes.

⇨ This newly configured card credentials will be saved in the system.

- **Note**:
  - The number of digits in the **Card Number**, and the maximum number of cardholders, will depend on the SiPass card technology purchased with the license.
  - The drop down list of the *PIN field* is updated when a cardholder's card number is entered. The cardholder may use their PIN if particular readers at the site are configured for both *Card* and *PIN*. This field will be hidden if the operator does not have the 'See PIN' operator privilege assigned.

Setting Unlimited End Date & Time for Card

The following action allows configures the cardholder's access for an indefinite Date or Time.
As a result of this action, the **End DateTime** field of the *Cardholder* dialog becomes disabled for the particular cardholder.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder to be configured with this feature.
4. Tick the checkbox of the **End DateTime** field.
5. Click **Save**.

Voiding a Cardholder

The following action voids all the cards assigned to the cardholder, and none of his/her cards can be used to access the site.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be made void.
4. Tick the **Void Cardholder** checkbox.
5. Click **Save**.

Isolating a Cardholder

Isolating a cardholder means that the cardholder will be allowed to secure any area (to which they are granted access), even if input points of the area are not sealed.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be isolated.
4. Tick the **Isolate** checkbox.
5. Click **Save**.

Configuring APB Exclusion

The following action configures the cardholder to be excluded from an Anti-Passback areas that have been created.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be configured APB Exclusion.
4. Tick the **APB Exclusion** checkbox.
5. Click **Save**.

Configuring Extended Latch Time Accessibility

The following action can be configured to allow easier access for the cardholder. When a cardholder badges his/her card at a reader, the door will unlock for the Extended Latch Time, rather than the normal Latch Time. You can configure the Extended Latch Time in the *Components* dialog.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be configured with this feature..
4. Tick the **Accessibility** checkbox.
5. Click **Save**.

Configuring Cardholder as Supervisor

The following action configures the cardholder as a Supervisor for doors that are configured with the Dual Custody mode of operation. For more information, refer **Supervisor** checkbox description in the section Definition Tab [→ 96].

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be configured as a supervisor.
4. Tick the **Supervisor** checkbox.
5. Click **Save**.

Configuring Self-Authorization

This action allows the cardholder to gain access to a door configured with the Dual Custody mode of operation, without needing the accompaniment of a subsequent cardholder before the door is unlocked.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be configured with self-authorization privileges.
4. Tick the **Self Authorize** checkbox.
5. Click **Save**.

Configuring Re-Entry Exclusion

This action exempts the cardholder from Timed Re-entry rules for areas that are operating in the Anti-Passback mode 'Timed Re-entry'.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be configured with Re-entry Exclusion.
4. Tick the **Re-Entry Exclusion** checkbox.
5. Click **Save**.

Configuring Private Access Privileges

The following actions are required to configure Private Access Privileges for the cardholder. For more information on Private Access Privileges, refer the section Assigning Cardholder's Private Access Privileges [→ 127].

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be assigned a partition workgroup.
4. Ensure that cardholder identification and partition workgroup details are defined.
5. Click the **Access Privileges** button. The *Access Assignment* dialog is displayed.
6. Proceed to configure access privileges for the cardholder. For more information on assigning Private Access Privileges for a cardholder, refer the section Assigning Cardholder's Private Access Privileges [→ 127].
7. The private access privileges assigned to a cardholder will be visible in **Private** tree hierarchy of the **Access Control** window of this tab.
8. Click **Save**.

Reading a Card

This action allows the operator to view the encoded cardholder information on a valid card. A dialog will appear containing the information held on the badged card.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open the record for the cardholder whose card is to be read.
4. Click the **Read** drop-down button, and select a required reader.
   The *Read Card* dialog is displayed.
5. Placed the card on the reader.
   The card details will be displayed on your system.

Assigning a Card

This action allows you to assign a card to a cardholder. This is a toggle-state button.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Open or Create a new record for the cardholder who is to be assigned a card.
4. Badge a card at a configured reader, and click the **Assign** button.
   The card number is displayed in the **Card Number** field.
5. Click **Save**.

Reading and Searching Card

This action allows you to read the encoded cardholder information on a valid card, and then search for the card number on the system. This is a toggle-state button.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Click the *Definition* tab.
3. Badge a card at a configured reader, and click the **Read & Search** button.

⇨ The card information will be displayed on the *Definition* tab.

4.5.2.2 Configuring the ADVANCED Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Advanced* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Advanced Tab [→ 98].

Configuring Cardholder's Non-Partition Workgroup/s

The **Work Groups** section of this tab will list the Partition work group that the cardholder is assigned to (from the *Definition* tab). The partition work group will have its corresponding **Partitioning** checkbox ticked. This indicates that this is the Partition work group.

To assign the cardholder to a Non-Partition work group, follow the instructions below.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder who is to be assigned a non-partition workgroup.
3. Click the *Advanced* tab.
4. Click the **Choose** button.
   The Cardholder's *Work Groups* dialog is displayed.
5. Select an object/s from **the Available Non-Partition Work Groups** list, and click **Add**.
   If you want to create a work group, click the **Define Work Group** button, and configuring the dialog that appears.
6. Click **OK**.
   The non-partition work group is listed in the *Advanced* tab.
7. Click **Save**.

Note: You can remove the cardholder from this non-partition work group, by clicking the **Choose** button, and removing the work group from the list of selected work groups.

Configuring Cardholder's Anti-Passback Count Workgroup

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder who is to be configured with this feature.
3. Click the *Advanced* tab.
4. Click the **Choose** button.
   The Cardholder's *Work Groups* dialog is displayed.
5. In the **Work Groups** section of this tab;
   Tick the **Use Anti-Passback** checkbox for the partition / non-partition work group that should include this cardholder in its anti-passback count.
6. Click **Save**.
7. **Note**: Only one work group can be selected for the cardholder's anti-passback count.

Saving Cardholder's Fingerprints

▷ In order to enable the fields of this section, ensure that a Bioscrypt reader is configured and connected to the system. For more details on these fields, refer the section Configuring the Bioscrypt Bus [→ 238].

▷ The **Finger Prints** section of the *Advanced* tab displays details of the cardholder's fingerprints.

▷ A maximum of 2 fingerprints can be saved for each cardholder.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose fingerprints are to be saved.
3. Click the *Advanced* tab.
4. Capture the cardholder's fingerprint using the bioscrypt reader configured to the system.
   Note: You can repeat this step to capture additional fingerprints. However, only 2 of these prints can be saved in the system.
5. The **Finger Prints** section of the *Advanced* tab will display a new row for the captured fingerprint. If you have captured multiple fingerprints, select the rows that you do not require, and click the **Delete** button to remove these rows.
6. In the **Index** field, click to select the finger name that was used for the fingerprint capture.
7. In the **Credential Profile** field, select a credential profile to which this fingerprint should be saved.
8. Click the **Save** button on the *Cardholder* dialog.

⇨ The fingerprint/s will be saved in the SiPass integrated system. This system indicates this by displaying a ticked **Saved** checkbox for the fingerprint that was saved.

Encoding Cardholder's Fingerprint/s to Card

You can select a cardholder's fingerprint/s that is saved in the system, and encode it to a card.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose fingerprints are to be encoded to card.
3. Click the *Advanced* tab.
4. Ensure that you have captured, configured and saved a cardholder's fingerprints in the system. For more information on how to do this, refer the section Configuration Type B: Fingerprint Acquisition [→ 245].
5. Place the card to be encoded on the Enrolment Reader, and click the **Encode** button on the *Cardholder* dialog.
6. The fingerprint/s will be encoded to the card.

⇨ This system indicates this by displaying a ticked **Encoded** checkbox for the fingerprint that was encoded to a card.

Configuring Cardholder's Smart Card Data

You can configure Smart Card profile for a cardholder in the Smart Card Data section of this tab.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder for whom smart card data is to be configured.
3. Click the *Advanced* tab.
4. Cick the **Profile** drop down button, and select a profile from the list.
   If you wish to create/modify an existing smart card profile, click the **Profile Viewer** button.
5. Click **Save**.

Configuring Cardholder's General Data

You can enter any general data for the cardholder that will be stored in the system database.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose general data is to be configured.
3. Click the *Advanced* tab.
4. In the **General Data** field of this tab, type in the information required.
5. Click **Save**.

4.5.2.3 Configuring the PERSONAL Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Personal* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Personal Tab [→ 99].

Configuring Cardholder's Personal Details

You can enter a cardholder's personal details in relevant fields of this tab. The cardholder's personal details are not essential when creating a cardholder record. These fields can be used to narrow a match when attempting to locate a cardholder record in the database or to positively identify the cardholder.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose personal details are to be configured.
3. Click the *Personal* tab.
4. Complete the **Title**, **Date of Birth**, **Address** and **Payroll Number** fields of this tab. For details on each of the field, refer the section Personal Tab [→ 99].
5. Click **Save**.

Configuring Cardholder's Contact Details

You can enter a cardholder's contact details in relevant fields of this tab.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose contact details are to be configured.
3. Click the *Personal* tab.
4. Complete the **Phone Number**, **Mobile Number**, **Mobile Service Provider**, **Pager Number**, **Pager Service Provider**, **Email Address** fields of this tab. For details on each of the field, refer the section Personal Tab [→ 99].
5. Click **Save**.

Configuring Cardholder's User Details

You can enter a cardholder's **Username** and **Password** in the **User Details** section of the *Personal* tab. Cardholders with these details configured can be configured as Organizers of Venue Bookings in the system.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose user details are to be configured.
3. Click the *Personal* tab.
4. Enter a name in the **Username** field.
5. Enter a password in the **Password** field.
6. Click **Save**.

4.5.2.4 Configuring the VEHICLE Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Vehicle* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Vehicle Tab [→ 100].

Configuring Cardholder's Vehicle Details

You can add details about the cardholder’s vehicle into the system through this tab. Note that these details are not essential when creating a cardholder record. However, they can be used to narrow a match when attempting to locate a cardholder in the database.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose vehicle details are to be configured.
3. Click the *Vehicle* tab.
4. Complete the fields under the *Vehicle* tab. For details on the various fields in the *Vehicle* tab, please refer the section Vehicle Tab [→ 100].
5. Click **Save**.

4.5.2.5 Configuring the TRACKING Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Tracking* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Tracking Tab [→ 100].

Configuring a Card to be Traced

You can specify if the cardholder’s card transactions are to appear as special alarms in the system, on this tab.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose card is to be configured for trace.
3. Click the *Tracking* tab.
4. Tick the **Card Trace** checkbox.
5. Click **Save**.

This action allows all valid card transactions performed by the cardholder to appear in the Audit Trail as special exception alarms. Traced cardholder numbers that appear in audit trail will be pre-pended with the hash symbol, ‘#’.

The last Date and Time, Card Number, Point Name and Anti-Passback Location that was used by the cardholder will also be displayed on this tab. For more details on these fields, refer section Tracking Tab [→ 100].

Exempting Cardholder from Anti-Passback Violation

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose card is to be exempted from anti-passback violation.
3. Click the *Tracking* tab.
4. Select the required card from the **Anti-Passback Credential Profile** drop down list.
5. Click **Forgive Card**.
6. Click **Save**.

Adding/Removing Card from Anti-Passback Area

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose card is to be configured.
3. Click the *Tracking* tab.
4. Select the required card from the **Anti-Passback Credential Profile** drop down list.
5. To remove the card from the anti-passback area count, click **Remove Card from APB**.
6. To add a card to the anti-passback area count, click **Add Card to APB**.
7. Click **Save**.

4.5.2.6 Configuring the CONTROL Tab

For a quick-reference guide on the main fields to be configured, refer the section Control Tab [→ 101]. The *Control* tab can be used to configure the system to control a specific card-holder's access to points in the site. At a system-level, this is done by using this tab to link specific readers (Access points) to door latches or output relays (Output points).

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose access is to be configured.
3. Click the *Control* tab.
4. The **Output Control** box of this tab has four fields. For more information on these fields, refer the section Control Tab [→ 101].
5. From the **Card** field, select a card you wish to configure for an output link.
   - **Note**: By selecting the **All Card** option on the **Card Number** drop down menu, the user can configure a specific output link to all the cardholder's cards.
6. From the **Access Point Group** field drop-down box, select one or more Access Points or Access Point Groups you want to link to a notification zone. The available points or point groups will appear in the list of this field. Multiple points can be selected by using CTRL + left click.
7. From the **Output Point / Group** drop-down box, select the output point or output point group you want to be activated. The available points or point groups will appear in the list below. Select one or more points or point groups from the list. Multiple output points can be selected by using CTRL + left click.
8. Select the **Time Schedule** during which the selected output points or groups may be activated.
9. Click **Add**. The linked access points and output points/groups will be added to the **Output Control** list.
10. Repeat the previous steps for every output point or group link you want to assign to this cardholder.
11. Click **Save**.

⇨ When the cardholder badges his or her card at one of the selected access points during the nominated Time Schedule, the output points will be unsecured. If the output points are already unsecured, there will be no effect.

4.5.2.7 Configuring the IMAGING Tab

The sections that follow provide detailed instructions on how to perform specific configurations on the *Imaging* tab of the *Cardholder* dialog.

For a quick-reference guide on the main fields to be configured, refer the section Imaging Tab [→ 101].

Importing Cardholder Images

The *Imaging* tab will only appear if the *Video Imaging and Card Printing Module* is installed. The *Imaging* tab allows you to capture a photograph or signature of a cardholder from a live video image. This photograph or signature can then be printed onto the cardholder's access card or viewed on-screen, together with the cardholder record.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder for whom images are to be imported.
3. Click the *Imaging* tab.
4. Select the **Import** button to display the Windows *Open* dialog.
5. Select the desired image file from those displayed in the list. The image will be displayed in the left-hand panel of the dialog.
6. Suitably crop and position the image in the template.
   – **Note**: Generally used image formats like JPG, BMP, PNG and TIF can be uploaded in SiPass integrated. Graphic Interchange Format (GIF) files are licensed and cannot be used with SiPass integrated.

Capturing Cardholder Photographs

Once you have installed SiPass' *Photo ID and Image Verification Module* and have configured the image preferences, you can begin capturing cardholder images.

▷ Ensure that the video capture card has been installed and configured.

▷ Create an employee record for the employee whose image is to be captured.

▷ Ensure that a card template has been created.

1. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
2. Open or Create a new record for the cardholder whose photograph is to be captured.
3. Click the *Imaging* tab.
4. Click **Live**.
   ⇨ The imaging panel will display a live video image on screen.
5. Position the camera and employee so that the employee's picture is displayed clearly (in focus) on screen. Refer to the video camera's user guide for detailed instructions concerning its operation and settings.
6. Click **Capture**.
7. The live video image will appear on screen as a still image. A cropping tool will appear overlaid on the captured photo, and a contrast and brightness slider will also appear.

8. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle to the desired size.
9. By positioning the cursor anywhere inside the cropping area, you can hold down the left mouse button and drag to move the cropped area. The part of the captured image that appears within the rectangle will appear in the photo field on the card template.
10. Use the **Contrast and Brightness** sliders, to adjust the image quality. The higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
11. Click **Save** when complete.

Capturing Cardholder Signature

Once you have installed SiPass' Photo ID and Image Verification Module and have configured the image preferences, you can begin capturing cardholder signatures.

Ensure that the signature capture pad has been installed and configured.

1. Create an employee record for the employee whose signature is to be captured.
2. Ensure that a card template has been created.
3. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
4. Open or Create the record for the cardholder whose signature is being captured.
5. Click the *Imaging* tab.
6. Enable the **Signature** radio button by clicking on it once.
7. Choose **New Signature**. Sign the capture pad using the pen provided.
8. Use the **Contrast** and **Brightness** sliders to adjust the signature.
9. Click **Save**.

Importing Cardholder's Photograph or Signature

Once you have installed SiPass' *Photo ID Module* and have configured imaging preferences, you can begin importing photographs and signatures of cardholders.

1. Create an employee record for the cardholder whose image will be captured.
2. Ensure that the cardholder photograph or signature exists.
3. Navigate to *Operation* > *Cardholder* from the SiPass main menu.
4. Open or Create the database record for the cardholder whose photograph or signature is being imported.
5. Click the *Imaging* tab. If a previous image of the employee signature exists in the employee's record, it will automatically be recalled when the *Imaging* tab has been selected.
6. Select the **Photo** radio button to import the cardholder's photograph or select the Signature radio button to import a signature.
7. Click the **Import** button.
8. Select the image file to import.
9. Click the **Open** button or double click on the file name.

10. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle.
11. Use the **Contrast** and **Brightness** sliders, to adjust the image quality - the higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
12. Click **Save**.

4.5.3 Searching for a Cardholder

SiPass integrated allows you to search the Database for a specific cardholder.

This can be done in two ways:

- Search based on details provided

– OR –

- Search by selecting a cardholder from the *Search Cardholder* dialog.

Both these methods have been discussed in detail in the two sections that follow.

4.5.3.1 Search Based on Details Provided

1. Choose **Cardholder** from the **Operation** toolbar or menu to display the *Cardholder* dialog.
2. Enter all or part of the details known about the cardholder into the respective fields displayed on the *Definition* tab.
3. To narrow the search as much as possible, enter all the data you can about the cardholder for whom you are searching. The more search criteria you enter, the more effective and quicker the search.
4. You can also use wildcards to search for cardholder details as specified in the table provided below in this section.
5. Click **Search** to begin the **Database** search.
   ⇨ The *Search Cardholder* dialog will appear if more than one cardholder record matches the search criteria. If only one record matches the search criteria, then that cardholder's information will be displayed directly in the *Definition* tab.
6. To skip to the next record, choose **Next**, or to go back a record, choose **Previous**.
7. When more than one cardholder is found as a result of a search, the order in which the cardholder's appear in the *Search Cardholder* dialog can be changed by clicking on the appropriate column header, sorting the order by **Card Number**, **Last Name**, **First Name, Employee Number** and **Card Status**.
8. To select a cardholder from the *Search Cardholder* dialog, double-click anywhere on the listed record or select the cardholder record and choose **OK**.

⇨ The selected cardholder's record will be retrieved from the Database and appear in the *Definition* tab.

Character	Description
%	Matches any string of zero or more characters
-	Matches any one character
[token]	Brackets can enclose a range or a set of numbers or letters, such as [1-9] or [klmnopq]. To format tokens use the following: • A ‘range’ token This token is formed with a start character and stop character. – Start is the beginning of the character range. – “" is a special character indicating a range. – Stop is the end of the character range. • A ‘set’ token: has discrete values in any order and it is inside brackets, it can be in any order, i.e., [ab6bc], and [abcde] are types of token sets.
^ token	The caret (^) before a token indicates that any characters following the caret will not be included in the search. For example: [^c-g] means that the search will not include any character which is a ‘c’ or a ‘g’.

4.5.3.2 Search and Select a Cardholder from the ‘Search Cardholder’ Dialog

The operator can also use the *Search Cardholder* dialog to select a cardholder. This can be done in the following manner:

1. Select the *Definition* tab on the *Cardholder* dialog.
2. Click **Search**. This action will display the **Search Cardholder** dialog and will list all the cardholders.
3. The cardholders can be segregated on the basis on the following field filters:
   - Card Number
   - First Name
   - Last Name
   - Workgroup
   - Workgroup Description
   - Workgroup Status
   - Access Group
   - Start Date
   - End Date
   - Card Status
   - Employee Number
   - Credential Profile
   - Visitor
4. Click under each Field cell. This will bring up a drop-down filter field. You can type specific information related to this field to search for a cardholder/(s). The cardholders filtered according to this data, will be displayed below.
5. Further, you can search for cardholder by making a required selection from the **Report Type** field. This action will display a report of cardholders that are filtered according to the option selected. For example, selecting Valid Cardholders will display all the cardholders whose status is displayed as Valid in the *Cardholder* dialog.
6. Viewing and selecting a cardholder from *Search Cardholder* dialog list can be done in the following ways:
   - Right-click and select **View Cardholder**. This action displays the details of the selected cardholder on the *Definition* tab, while keeping the *Search Cardholder* dialog displayed.

- Right-click and select **View Cardholder and Close Search**. This action displays the details of the selected cardholder on the *Definition* tab, and closes the *Search Cardholder* dialog.
- Double-click on a cardholder in the list. The details of the selected cardholder will be displayed on the *Definition* tab, and the *Search Cardholder* dialog will be closed.

NOTICE! If you click **View Cardholder** without performing a new search, the previous search result is displayed. To ensure that you get an updated cardholder search report every time, it is recommended to run a new search before viewing the result.

4.5.4 Configuring Multiple Cards for a Cardholder

The **Credentials** section of the *Definition* tab lists all the cardholder's cards.

If only one card has been assigned to the cardholder, it will still be displayed on this tab.

For more information, refer the section Configuring Cardholders' Card & Card Credentials [→ 104].

See also

Credential Profile [→ 94]

4.5.5 Unused Cards

SiPass integrated can track cards that have not been used recently.

The operators need to follow these processes to apply this feature:

- **Configure a Report**:

  The operator tracks and views Unused Card(s) by configuring a Customized or Predefined report in SiPass Explorer.
- **Convert the Report into an Actionable Report**:

  The operator converts the Customized or Predefined Report into an Actionable Report, by assigning an action to it. This action can be either to void an Unused Card(s), or Cardholder(s) of these unused cards.
- **Trigger a Host Event Task**:

  In the Host Event Task dialog, the operator selects the created Actionable Report to trigger the action that voids Unused Card(s), or Cardholder(s).

These processes are discussed in detail, in the sections that follow.

4.5.5.1 Tracking Unused Cards using Customized / Predefined Reports

It is possible to configure SiPass integrated to generate reports of cards that are unused for a specific number of days. This feature will allow operators to track and view details of these cards.

This is particularly useful when configuring cardholders with multiple cards. It gives the operator the ability to track, not just the cardholder, but each of his cards also.

Configuring SiPass to generate reports of unused cards is done in SiPass Explorer.

This can be done in two ways:

- By configuring a Customized Report that displays all the inactive cards, filtered using specific parameters.

– OR –

- By using a Pre-defined Report that displays all the inactive cards using a 30-Day Threshold.

The steps required for both these options are provided below.

Tracking Unused Cards using a Customized Report

1. Select **SiPass Explorer** from the main menu bar.
2. In the **Navigation** panel, select and right-click **Customized Reports**.
3. Select **New Report**. This action will display the **Report Wizard** application.
4. Click **Next**.
5. Enter a **Name** for the report, and click **Next**.
6. Select **Cards – Inactive** from the **Record Type** field.
7. From the **Available Fields** section, add all the fields required for this report.
8. Click **Next**.
9. Specify the filter conditions in this dialog.

For more information on how to specify Filter Conditions, refer the section Filter Conditions of the SiPass Explorer User Manual.

10. Click **Finish**.

⇨ This action will display the report on the SiPass Explorer panel.

Tracking Unused Cards using a Predefined Report

On selecting this option, the system generates a report for all the cards that have been unused since the last 30 days.

1. Select **SiPass Explorer** from the main menu.
2. In the **Navigation** panel, select and expand **Predefined Reports**.
3. Select and expand **Cardholder**.
4. Right-click the **Inactive Cards – 30 Day Threshold** report.

The steps required to covert this Predefined Report to an Actionable Report by assigning a **Void Card / Cardholder** action to it, are the same as those described in the section above.

Converting the Report into an Actionable Report

This sub-section explains how an operator can convert this Customized Report to an Actionable Report, by assigning an action to it. This action can be to void unused cardholder(s) / card(s).

1. Select and right-click on this report on the **Navigation** panel.
2. Select **Customize Current View**.
3. In the dialog that appears, select **Available Actions**.
4. Tick the **Void Cardholder** checkbox to void a cardholder of an inactive card(s). Further, click on this option to highlight it.
5. Tick the **Void Card** checkbox to void an inactive card. Further, click on this option to highlight it.
6. Select the **Set as Default** button.
7. Click **Apply**, and **OK**.

⇨ The customized report has been converted to an Actionable Report.

The steps required to covert this Predefined Report to an Actionable Report by assigning a **Void Card / Cardholder** action to it, are the same as those described in the section above.

4.5.5.2 Configuring a Host Event Task based on the Actionable Report

This section explains how an operator can select the Actionable Report as a Target, to void Unused Cards, or Cardholder(s) of these unused cards.

1. Select **Program > Event Tasks > Host**.
2. After entering an **Event Name** and **Time Schedule**, configure all the fields of the **Trigger** section.
3. From the **Target** field, select **Actionable Report**.
4. From the **Report** field, select a specific **Actionable Report**.
5. Enter a required message in the **Message** field.
6. Click **Save**.

⇨ The system has now been configured to void Unused Card(s) or Cardholders(s) of unused cards, based on the Actionable Report selected.

4.6 Visitors

SiPass integrated includes an extensive Visitor Management function. Visitors in SiPass can be regarded as temporary cardholders: the same information needs to be captured as for permanent cardholders, but additional information such as card issue status and length of stay also needs to be recorded.

The Visitor interface is therefore extremely similar in appearance and functionality to the Cardholder dialog. Access privileges and personal data need to be assigned and collected, Visitor facial and signature images can be captured and printed onto a card, and custom visitor fields for additional data can be created. You can also create custom fields specifically for Cardholders, Visitors, or both.

It is not necessary to create a new Visitor record each time the same person visits a facility. Once a record is created, it can be activated (issued) and deactivated (returned) instead of creating multiple records.

A Visitor type is available in the Workgroups dialog, allowing you to create workgroups specifically for the purpose of organizing visitor groups.

All visitor transactions are recorded in the Audit Trail and an extensive Visitor reporting facility is available to produce documentation of visitor histories.

4.6.1 Adding a Visitor

There are pre-defined tabs available when adding a visitor – *Visitor Definition*, *Advanced*, *Personal*, *Tracking*,*Visitor Management*, *Control*, *Imaging* and *Visitor Details*. You can create additional tabs the Custom Fields feature of the SiPass Explorer application. For more information refer to the SiPass Explorer User Manual.

▷ Ensure that all the access points, areas, Time Schedules and site management details have been configured. If you have the optional *Photo ID* and *Card Printing* modules installed and are going to print a visitor card, ensure you have designed a card template first.

▷ Ensure that field entries are not preceded by (white) spaces. This may cause unpredictable behavior in other areas of the application.

1. Select **Visitor** from the **Operation** toolbar or menu.
2. Complete the *Visitor Definition* tab exactly as for a normal cardholder except for the visitor start and end dates, these vary.
   - The **Start Date** will be set to the current date, click on the drop down box to select a new date.
   - The **End Date** will also be set to the current date, unless changed.
   - In order to change the validity days, this can be done via the **System Preferences** option in the **Options** menu. Enter the number of days next to 'Visitor default validity time (days)'.
3. Select the *Advanced* tab and configure the cardholder's details as required (as described for a normal cardholder).
4. Select the *Personal* tab and complete the visitor's personal details (as described for a normal cardholder).
5. Select the *Tracking* tab and tick the **Card Trace** checkbox to enable tracking of the visitor.
6. Select the *Visitor Management* tab and complete the visitor management details:
   - **Select Cardholder**: Allows an existing cardholder with whom the visitor is meeting to be nominated.
   - **Remove Cardholder**: Removes the existing cardholder with whom the visitor is meeting to be nominated..
7. Select the *Control* tab and fill in the information as described for a normal cardholder.
8. Select the *Visitor Details* tab and fill in the required information.
9. Select the *Imaging* tab, if you intend to capture the Visitor's photograph or signature.
   ⇨ The *Imaging* tab will only appear if the *Photo ID and Image Verification* Module is installed. The *Imaging* tab allows you to capture a photograph or signature of a visitor from a live video image. This photograph or signature can then be printed onto the visitor's access card or viewed on-screen.
10. Complete the details in the *Visitor Details* tab as required.
11. If you have created any *Customizable Cardholder* Fields for the *Visitor* dialog, they must be completed.
12. Return to the *Visitor Definition* tab.
13. Click **Save**.

4.6.2 Issuing and Returning Visitor Cards

Once you have created the Visitor record with access privileges and personal details, Visitor cards can be issued or returned as required. Issuing a card requires that you nominate an existing cardholder to be the “sponsor” for the visitor.

Issuing a Visitor card

1. Select **Visitor** from the **Operation** menu or toolbar.
2. Use the **Search** button in the *Visitor Definition* tab to locate the Visitor record for whom you want to issue a card. Otherwise, create the new record as described in the previous procedure.
3. Select the *Visitor Management* tab.
4. Choose *Select Cardholder*.
5. Select an existing cardholder from the list who will “sponsor” the visit.
   – If you press an alphabet key on the keyboard, SiPass integrated will automatically scroll the list to the nearest cardholder surname beginning with that letter.
6. Choose **OK**.
   ⇨ You will be returned to the *Visitor Management* tab of the *Visitor* dialog and the selected cardholder will appear in the **First Name** and **Last Name** fields.
7. Choose **Issue** and **Save**.
   ⇨ The **Card Status** field will update to “Issued” and the **Issue Time** field will contain the current time.
8. Click **Save**.

⇨ The Visitor record will be updated with the Card Issue details.

Returning a Visitor card

1. Select **Visitor** from the **Operation** menu or toolbar.
2. Use the **Search** function in the *Definition* tab to locate the Visitor record for whom you want to return a card.
3. Use the **Next** function to navigate to the next record in the database. Use the **Previous** function to navigate to the preceding record.
4. Select the *Visitor Management* tab.
5. Choose **Return Save**.
   ⇨ The Status field will be updated to “Returned” and the Return Time field will contain the current time.
6. Return to the *Definition* tab.
7. Click **Save**.

⇨ The Visitor record will be updated with the Card Return details.

4.6.3 Adding a Visitor to a list of Expected Visitors

A list of visitors expected to visit the site can be compiled and displayed at any time.

1. Select **Expected Visitors** from the **Operation** menu or toolbar.
2. Choose **Add**.
3. Select a visitor from the list of visitors displayed by highlighting their name.
   ⇨ Only those visitors that are enrolled in the system will be available for selection. Before adding a visitor to the list of expected visitors ensure that you have enrolled the details of that visitor first.
4. Select the date and time the visitor is expected to arrive at the facility.
5. Select the date and time the visitor is expected to depart the facility.
6. Choose **OK**. Choose **Close**.

⇨ The Expected Visitors list will be updated and closed.

5 Access Management

The level of access a cardholder has to various points at your site is determined by the access control privileges that they have been assigned. Cardholder access control is achieved by:

- Creating Time Schedules
- Defining Access Levels
- Defining Access Groups
- Assigning Access Privileges to Cardholders or Workgroups

5.1 Access Levels

An access level is a collection of access points or access point groups mapped to a Time Schedule.

An operator must have access privileges to all of the points in an access level, before they can modify, delete or assign the access level to access groups.

5.1.1 Configuring Access Levels

▷ Ensure that all the access points, point groups, areas/sub-areas and floors to which the cardholder will require access have been defined.

▷ Establish the Time Schedules during which the cardholders will require access.

1. Select **Access Level** from the **Program** toolbar.
   ⇨ The *Access Level Definition* dialog is displayed. Alternatively, you can also access this dialog by clicking the **Access Privileges** button on the *Cardholder* dialog.
2. Enter a name for the Access Level into the **Name** field.
3. Select the **Time Schedule** for which the selected access points will be unsecured, from the **Time Schedule** drop down box. The following table gives an example of the effect a Time Schedule has on an access point.
   – **Never**: The cardholder cannot gain access at any time
   – **Always**: The cardholder can gain access at the points, areas/sub-areas, groups or floors at all times
   – **System Function (non busy intervals)**: The event task can only be triggered between 2 am and 3 am every day of the year including holidays
4. The **Copy** button can be used to create a new Access level based on one that already exists.
5. The **Time Schedule** button allows you to modify the Time Schedules.
6. Select whether you are adding access points or access point groups from the **Type** drop down box.
7. Select the point or point group in the bottom list that you want to add to the Access Level. Click the **Add** button to add it to the adjacent list.
8. To remove an access type from this list, select it, and click the **Remove** button.
9. Repeat for every point or point group that you want to add to the access level.
10. Click **Save**.

5.1.2 Searching for an Access Level

1. Select **Access Level** from the **Program** toolbar.
2. In the **Search** field indicated by **<Search>** enter the name or part of the name of the Access level you are looking for.
3. Click on the Arrow button to begin your search.
   ⇨ A list of all matching access levels will appear in the list box.
4. Click on the **Cross** button to clear the search field and enter a new term for searching.

This search field is dynamic and will automatically begin filtering the list of access levels based upon the letters you type into the field as you type.

5.2 Access Groups

An access group is a collection of access levels. Access groups are assigned to cardholders and workgroups to determine the level of access personnel have to entry points at your site. The following steps describe how an Access Group can be defined.

5.2.1 Configuring Access Groups

▷ Ensure you have defined all of the access levels required for your site.

1. Select **Access Group** from the **Program** menu.
   ⇨ The *Access Group Definition* dialog is displayed. Alternatively, you can also access this dialog by clicking the **Access Privileges** button of the *Cardholder* dialog.
2. Enter a name for the Access Group into the **Access Group Name** field.
   ⇨ A list of Access Levels will appear in the **Available Access Levels** list.
3. Select the access level you want in the Access Group and use the **Add** button to move them to the **Selected Access Levels** list.
4. Repeat for every access level you want to add to the group.
5. To remove an access level, select it from the **Select Access Levels** list, and click the **Remove** button.
6. Click **Save**.

5.2.2 Searching for an Access Group

1. Select **Access Group** from the **Program** toolbar.
2. In the **Search** field indicated by **<Search>** enter the name or part of the name of the Access Group you are looking for.
3. Click on the Arrow button to begin your search.
   ⇨ A list of all matching access groups will appear in the list box.
4. Click on the Cross button to clear the search field and enter a new term for searching.

This search field is dynamic and will automatically begin filtering the list of access groups based upon the letters you type into the field as you type.

5.3 Access Assignment

Operators can assign *single* or *multiple* access rights to cardholders, workgroups or venues, without limitations on the number of access rights per cardholder. This can be done for any of the following access types: *Points*, *Point Groups*, *Access Levels*, *Access Groups*, *Floors*, *Floor Groups*, *Intrusion Areas*, *Intrusion Area Point Groups*.

Any of the above can be assigned either permanently, or temporarily (with a start and end date). Any combination of permanent access rights, or access rights with time constraint is possible. Overlapping access rights are also allowed. It is possible to have expired access rights automatically removed (and archived) from the cardholder definition screen.

When assigning access to workgroups; any modification to the access rights of a workgroup will immediately affect all cardholders belonging to this workgroup. Cardholders with multiple Workgroups assigned to them will inherit all access rights from all workgroups.

5.3.1 Configuring Access Privileges

As an operator, the access privileges you define and assign to a cardholder will determine the points through which they are able to gain entry to the site, and the time-schedules for entry. The SiPass integrated system allows operators to grant **Multiple Access Privileges** to a cardholder.

This means that cardholders can access a site using Multiple Access Privileges, configured by an operator in the following ways:

- Assigning a cardholder's **Private Access Privileges**

The operator can assign Private Access Privileges for individual cardholder. For further details, refer the section Assigning Cardholder's Private Access Privileges [➙ 127].

- Assigning **Work group Access Privileges**

The operator can assign a Work group to a cardholder. The cardholder can then access the site using the access privileges assigned to his/her work group.

If a cardholder has multiple workgroups assigned, he/she will can inherit and use the access privileges of all the workgroups assigned. For further details, refer the section Assigning Cardholder's Workgroup Access Privileges [➙ 129].

- Assigning **Venue Booking Access Privileges**

The operator can assign access privileges to venue bookings for cardholder or entire workgroups. For further details refer the section Assigning Cardholder's Venue Booking Access Privileges [➙ 136].

- The flexibility of SiPass integrated allows operators to grant cardholders **with a combination of Private, Workgroup and Venue Booking Access Privileges**.

See also

Configuring Access Control for Venue [➙ 132]

5.3.1.1 Assigning Cardholder's Private Access Privileges

Ensure that all access types like points, point groups, areas/sub-areas, floors, venue bookings, etc., to which the cardholder will require access have been defined.

1. Select *Operation* > *Cardholder* from the main menu.
   ⇨ The *Cardholder* dialog is displayed.
2. On the *Definition* tab, find an existing cardholder, or create a new cardholder for whom access privileges need to be defined. For more information, refer the section Adding Cardholders [→ 103].
   – **NOTE**: Any existing private access privileges of a cardholder will be displayed in the **Private** tree of the **Access Control** box of this dialog. The steps required to add new access control privileges, or modify existing privileges, are available in the following section.
3. Click the **Access Privileges** button.
4. The *Access Assignment* dialog is displayed. Configure this dialog to assign private access privileges to the cardholder. For more information, refer the section Configuring the Access Assignment dialog [→ 127].

Configuring the Access Assignment dialog

The **Access Assignment** dialog can be used to assign *Private*, as well as *Workgroup* access privileges. Hence, the instructions provided below are applicable to both.

DIALOG DESCRIPTION

This dialog has three tabs:

- **Access Assignment**: You can use this tab to select and configure the Access Type items (points, levels, groups, etc) to be assigned to the cardholder / workgroup, and also specify the Time Schedule for access.
- **Access Group Definition**: You can use this tab to define new Access Groups.
- **Access Level Definition**: You can use this tab to define Access Levels.

1. Click the *Access Assignment* tab.
2. This tab has two main sections: **Configuration** and **Access Control**.
   – The **Configuration** section is where you must first define the access privileges for the cardholder / workgroup. This is then added to the **Access Control** section of this tab.
   – The **Access Control** section will list all the configured access privilege details.
   – **Note** : For cardholder / workgroup with existing access privileges:
   – The **Access Control** box will list the access control item details for cardholder / workgroup that already have access privileges assigned.
3. Select an item from the **Access Type** drop down list.
4. Click on an access object displayed in the adjacent box to highlight it.
5. Select the **Time Schedule** to be configured for the access object.
6. If you want to configure temporary access control privileges for a specific calendar period, continue to the next step.
7. If you want to restrict the access privileges defined for the cardholder / workgroup, to specific calendar period, proceed with the instructions a, b and c below. This means that the cardholder / workgroup will be able to access the site, using the access privileges you define, only during the specified Day/Month/Year period.

- a. Tick the **Use Start Date and End Date** checkbox.
- b. In the **Start** field, specify the Date/Month/Year and Time (Hour/Sec.), to define when the cardholder / work groups' access privileges will begin. You can also click the dropdown arrow of this field, to make a selection.
- c. In the **End** field, specify the Date/Month/Year and Time (Hour/Sec.), to define when the cardholder / workgroups' access privileges will end.
- **Important**: If you define a **Start Time** and **End Time**, which is longer than the time specified in the Time-Schedule, the cardholder will only be able to access the site only during the time specified in the Time Schedule. For example, consider that a Time Schedule configured for a point is 9:00 am – 5:00 pm. Next, the operator configures a cardholder / workgroups' access privileges for the same point with a Start Date and End Date from 1/12/2015 - 2 am to 4/12/2015 – 10 pm. In such a situation, the cardholder will be able to access the site at the assigned point from the 1/12/2015 – 4/12/2015, but only between 9:00 – 5:00 pm.

8. If you selected **Intrusion Area Point** from the **Access Type** drop-down list, you will need to configure two additional fields on this tab: Control Mode and Arming Rights.
9. If you selected **Intrusion Area Point Group** from the **Access Type** drop down list, you will need to configure only the **Control Mode** field.
10. Click the **Add** button, to add the configured access type item to the **Access Control** box of this dialog. You can also double-click the item, or drag-and-drop it into the box below.
11. You can remove an item from the box by selecting it, and clicking the **Remove** button. Or, double-click to remove it from the box.
12. The **Access Control** box contains the following fields: **Name**, **Time-Schedule**, **Start**, **End**, **Control Mode** and **Arming Rights**. These fields display the configuration details you specified for each access privilege in the previous steps.
13. When complete, click **OK**.

    ⇨ All the access privileges you configured will be transferred to the selected cardholder / workgroup.

For Cardholder's Private Access Assignment:

The *Cardholder* dialog will be displayed. Expand the **Private** tree item of the **Access Control** box of this dialog to view the configured private access privileges.

For Workgroup Access Assignment:

The *Work Group* dialog will be displayed. The *Access Control* box of this dialog displays the configured access privileges for the selected workgroup. Click **Save**.

Modifying Private Access Privileges

1. Open the *Access Assignment* dialog.
2. Click the access privilege to be modified, in the **Access Control** box of this dialog.
3. Click the **Remove** button, or double-click the item. This will delete the item from the box.

⇨ You can now add a new, modified private access privilege to the box.

5.3.1.2 Assigning Cardholder's Workgroup Access Privileges

Cardholders can be assigned workgroup access privileges for Partition or Non Partition Workgroups.

The sections that follow provide instructions on how to configure such workgroup access control privileges.

See also

Configuring Workgroup Access Privileges [→ 91]

Assigning Cardholder's Parition Workgroup Privileges

1. Click **Operation** > **Cardholder** > **Definition** tab, and create a new record, or open an existing record for a cardholder to be assigned partition workgroup access.
2. Click the **Workgroup** drop down list. This list displays the available partition workgroups.
3. Select a workgroup from the list and click **Save**.

Assigning Cardholder's Non-Partition Workgroup Privileges

1. Click **Operation** > **Cardholder** > **Advanced** tab, and create a new record, or open an existing record for a cardholder to be assigned partition workgroup access.
2. In the **Work Groups** section of this tab; click the **Choose** button. The *Cardholder's Work Groups* dialog is displayed.
3. Select a workgroup from the **Available Non-Partition Work Groups** section.
4. Click **Add** and **OK**. This workgroup will be added to the *Advanced* tab of the *Cardholder* dialog.
5. Click **Save**.

The cardholder can now use the Access Control privileges configured to the selected Non-Partition Workgroup. The Access Control section of the *Definition* tab will display the assigned workgroup as part of the cardholder's workgroup access privileges.

5.3.1.3 Assigning Cardholder's Venue Booking Access Privileges

Operators can assign cardholders to venue bookings which will allow cardholders to inherit the access privileges of the specific venue they are configured to.

For more information, please refer the sections under the topic Assigning Cardholder's Venue Booking Access Privileges [→ 136].

5.3.2 Workgroup and Operator Access Privileges

It is possible for an operator to assign access groups to a cardholder, where the operator has actually not been granted privileges for those access groups.

For example, an administrator or high-level operator creates a workgroup called “Security” with access privileges for Access Group A. This workgroup is flagged to automatically grant access privileges to cardholders assigned to the workgroup.

Another operator group is created, that does not have access privileges to any Access Groups, but is granted access privileges to the Security workgroup. An operator belonging to this operator group can assign the workgroup “Security” to a new cardholder, effectively transferring access privileges for Access Group A to the cardholder even though their operator group has not been granted privileges for this Access Group.

This kind of scenario can be avoided by:

- Creating a single operator group for the creation of cardholders or
- Ensuring that all operator groups with “create” permissions for workgroups have been granted privileges to exactly the same access groups.

5.4 Offline Access

SiPass integrated allows you to configure cardholders that have access if the reader interface devices stop communicating with the ACC.

5.4.1 Defining Offline Access Groups

Offline Access Groups control who has access to which doors when the reader interfaces are offline.

1. Select **Offline Access Group** from the **Program** menu.
2. Click **New Offline Access Group**.
3. Enter a name for the group and click **Save**.

Your Offline Access Group is now created. You can assign cardholders to this group from the *Cardholder* dialog and add doors to the group from the Offline Mode configuration in the *FLN Configuration* dialog.

5.4.2 Defining Offline Access Privileges

Offline Access Privileges are assigned in a similar way as regular access privileges.

An operator can configure 100 unique card numbers (as configured in SiPass integrated for cardholders) that can be granted access at doors controlled by a RIM device (devices like DRI/SRI/ERIs). When a RIM device is operating in the Offline mode, and a user badges a card, the device will check its internal list of 100 cards to see if the card: (a) Exists in the list of up to 100 cards, (b) Has access to that particular reader device.

If both conditions are met, the device will open the door and store a 'Valid Card' event; or if invalid, an 'Invalid Card' event.

If the door is opened and closed, it will also store a DoorFrame opened and closed message.

The system will warn the operator when the cardholder limit is reached. But please keep this in mind when assigning cardholders to groups.

The steps that follow detail how operators can configure Offline Access Privileges in the SiPass integrated system.

1. Select **Cardholder** from the **Operation** menu.
2. Find or create the cardholder record whose access privileges you want to modify.
3. Click on the **Access Assignment** button.
4. Click **Offline Access Groups**.
5. Tick the checkboxes of the Offline Access Group you wish to add and click **Close** to close the dialog.
6. Select each Offline Access Group and click **Add** to view which doors it includes.
7. Click **OK** to return to the *Cardholder* dialog.
8. Click **Save**.

5.5 Venue Management

SiPass integrated's VENUE MANAGEMENT feature is a highly flexible and versatile tool that allows you create and manage venues in your site.

You can create access controlled venues on your site, which can be booked for the purpose of meetings, conferences, trainings, etc. Operators can configure organizers, participants, the time schedule of the venue bookings, and also control access privileges to cardholders for the venue.

This feature also lets you view various bookings across multiple venues and time periods which can help organizers plan and book venues efficiently.

In functionality, venue bookings allow you to create access privileges, for a special set of access privileges for a cardholders or workgroups, over a temporary period, after which the temporary privileges can be removed, if required.

Dialog Description

- Click *Operation* > *Venue Management* from the main menu.
  ⇨ This displays the *Venue Booking Management* dialog.

Tabs: There are two tabs on this dialog:

- **Venue**: This tab is used to define a venue, and its access control configuration.
- **Venue Booking**: This tab is used to book a venue, and view/edit/delete existing bookings.

Left Panel: There are three expandable boxes in this panel:

- **Venues**: All venues configured in the system are listed here.
- **Calendar**: A monthly calendar, with the current day highlighted, is displayed here.
- **Views**: You can use this box to customize views of venue schedules and bookings for single or multiple venues side-by-side.

5.5.1 Creating a New Venue

1. Click *Operation* > *Venue Management* from the main menu.
   ⇨ The *Venue Booking Management* dialog is displayed.
2. Click the **New Venue** button to define a new venue for your site.
3. Click the *Venue* tab.
4. Enter a name for the venue in the **Name** field.
5. Enter a description of the venue in the **Description** field.
6. Click **Save**.
7. The **Venues** tree panel on the left of this dialog displays all venues avail-able in the system.

Searching for existing venues:

1. Click the **…** button on this dialog.
2. Select a venue from the *Venue Search* dialog that appears.

The filtered text box at the top of this dialog can be used for filtering the venue bookings.

5.5.2 Configuring Access Control for Venue

You can control access to each venue by configuring its Access Assignment. This allows you to define and control all the points of entry and exit to the venue.

1. Open the *Venue Booking Management* dialog.
2. Create a new venue, or open an existing venue by clicking the **…** button. You can also select the desired venue from the venue tree view on the left panel of this dialog.
3. Select the **Define Access Privileges** button.
   ⇨ The *Access Assignment* dialog is displayed.
4. You can now configure and assign access privileges to this venue on this dialog. For further details, refer the section Configuring the Access Assignment dialog [➞ 127].
5. The access privileges you define will be displayed in the **Access** box of this dialog.
6. Click **Save**.

5.5.3 Venue Booking

Venue Booking is a simple configuration that allows you to book a specific venue, configure Organizer/s, Participants, the start & end Date and Time of the booking, and also grant access control privileges to cardholders to access the venue.

5.5.3.1 Booking a Venue

▷ Ensure that the Venue to be booked is configured in the system.

1. Click **Operation > Venue Management** from the SiPass main menu.
   ⇨ The *Venue Booking Management* dialog.
2. Select the venue in the **Venues** tree panel on the left.
3. Next, click the *Venue Booking* tab.
4. The Calendar is displayed on this tab. Select from the **Day**, **Work Week**, **Week** or **Month** buttons to view the Calendar accordingly.
   – **Day**: Displays 24 hours of the present day
   – **Work Week**: Displays all 24 hours from Monday – Friday of the present work week
   – **Week**: Displays all 7 days of the current work week by default. To display a different week, select it from the Calendar box on the adjacent left panel.
   – **Month**: Displays all the days of the month. Use the scroll bar to view days of the previous or following month/s.

Opening the Venue Booking Definition dialog

Option 1:

- You can highlight **Hours/Days/Weeks** on this calendar, and then right-click to display the **New Venue Booking** menu option. Select this option to display the *Venue Booking Definition* dialog.

Option 2:

- Click the **New Venue Booking** button on the *Venue Booking* tab. The *Venue Booking Definition* dialog is displayed.

Configuring the Venue Booking Definition dialog

1. Click the *Venue Booking* tab.
2. Enter a **Name** for the booking. If this booking authentication is required, tick the **Require Authentication** checkbox.
   – **Note**: The **Require Authentication** checkbox is related to the ‘organizers’ configured for this venue booking.

To allow an organizer/s to edit a booking:

1. Tick **the Require Authentication** checkbox
2. Add the cardholder as an organizer for the venue booking.
3. Ensure that this organizer has a Username and Password (configured in the Personal tab of the Cardholder dialog). If checkbox is ticked, and the organizer/s does not have a username and password configured, the booking can still be saved. But, the organizer/s can-not edit the booking until they are given a username and password.
   ⇨ **Only a user logged into the system as an administrator can edit the booking without requiring a username and password.**
4. In the field below, enter a **Description** of the booking.

5. Select the Start Date and Start Time of the booking in the **Start Date** field.
6. Select the End Date and End Time of the booking in the **End Date** field.
7. Select the venue in the **Venue** field. By default, the venue selected on the *Venue Booking Management* dialog will populate this field. Click the **…** button to search and select another venue.
8. Click **Save**.

Adding / Removing Organizers:

1. In the **Organizers** section, click the **Add** button.
2. The *Search Cardholder* dialog will be displayed. Double-click on a cardholder to configure them as an organizer. You can select and configure multiple organizers for the same venue booking.
3. To delete this organizer/s, select the card-holder and click the **Remove** button.
   - For instructions on how to configure Venue Booking access privileges to individual cardholders, refer the section Assigning Venue Booking Privileges to Cardholders [→ 136].
   - For instructions on how to configure Venue Booking access privileges to workgroups, refer the section Assigning Venue Booking Privileges to Workgroups [→ 136].

5.5.3.2 Configuring a Recurrent Venue Booking

1. Open the *Venue Booking Definition* dialog.
2. Click the *Recurrence* tab.
3. Select from the following options available on this tab:

Recurrence pattern	Details	Range of recurrence
One Off	Select this option to configure this booking as a one-off booking that will not recur.	
Daily	• Select **Every__day(s)** to repeat this booking for a selected number of days. Enter the number of days for recurrence in this field. • Select **Every weekday** to configure this booking to recur every weekday	• Select **End after: ___ occurrences** to end the recurrence of the booking after a number of occurrences. Specify a number of occurrences in this field. • Select **End by** and select a date, to end the recurrence of the booking by the selected date
Weekly	• Select **Recur every __ week(s) on**:, and specify the number of weeks you want the booking to recur.	
Monthly	• Select **Day __ of every __ month(s)** to configure recurrence of the booking on a monthly basis. For example, for the fifth day of every month. • The **__ __ of every __ month(s)** to configure it for a specific recurrence. For example, for every third Thursday of every month.	

- Click **Save**.

5.5.3.3 Listing Current Bookings

- Click the Current Bookings button on the Venue Booking tab.
  ⇨ The bookings for all venues will be listed by Name, Start Date, End Date and Venue.

Search and Filter this list:

- You can search and filter this list by typing your search term in the filter box below each column.

Editing venue booking items on this list:

1. Each venue booking item can also be edited or deleted by double-clicking on the item, which will bring up the *Venue Booking Definition* dialog.
2. Or, by right-clicking on the item, and choosing **Edit Venue Booking** or the **Delete Venue Booking**.
3. **Note**: If the item chosen is configured as a recurring venue booking, a dialog will be displayed with the following options:
   – **Open this occurrence**: This option allows you to edit only Venue Booking for the specific date/time
   – **Open this series**: This option allows you to edit the venue booking to affect all the venue bookings in its recurrence series.

5.5.3.4 Single-Screen Display of Single/Multiple Venue Bookings

1. Click the **New Calendar View** button of the **Views** box in the left panel.
2. The *Calendar View* dialog is displayed.
3. Enter a name for the new view you want to create.
4. Select the venues whose bookings you want to view.
5. If you select multiple venues, their booking schedules will be displayed side-by-side.
6. Click *Save* and *Close*.

⇨ The saved view will be displayed in the Views box. Select a view to display it in the Venue Booking tab.

5.5.3.5 Assigning Cardholder's Venue Booking Access Privileges

Operators can assign cardholders to venue bookings which will allow cardholders to inherit the access privileges of the specific venue they are configured to.

This can be done by in the following ways:

- **Assigning Venue Booking access privileges to Individual Cardholders to Venue Bookings** (as Organisers or Participants)
- **Assigning Venue Booking access privileges to Workgroups**

The sections that follow provide detailed instructions on the two options listed above.

Assigning Venue Booking Privileges to Cardholders

▷ Ensure that the Venue to be booked is configured in the system.

1. Click **Operation > Venue Management** from the SiPass main menu.
   ⇨ The *Venue Booking Management* dialog.
2. Select the venue in the **Venues** tree panel on the left.
3. Next, click the *Venue Bookings* tab.
4. Double-click on an existing venue booking on this tab to open it. The *Venue Booking Definitio*n dialog is displayed.
5. In the **Participants** section, select the *Cardholder* tab and click the **Add** button.
   ⇨ The *Search Cardholder* dialog appears.
6. Select a cardholder on this dialog, and click the **Add** button to add individual cardholders.
7. To remove a participant, select the cardholder, and click the **Remove** button.
8. Click **Save**.

⇨ The cardholder will inherit the access privileges of the venue selected for this venue booking.

Assigning Venue Booking Privileges to Workgroups

▷ Ensure that the Venue to be booked is configured in the system.

1. Click **Operation > Venue Management** from the SiPass main menu.
   ⇨ The *Venue Booking Management* dialog.
2. Select the venue in the **Venues** tree panel on the left.
3. Next, click the *Venue Bookings* tab.
4. Double-click on an existing venue booking on this tab to open it. The *Venue Booking Definitio*n dialog is displayed.
5. In the **Participants** section, select the *Work Group* tab and click the **Add** button.
   ⇨ The *Select Work Group …* dialog appears.
6. Select a work group on this dialog, and click the **OK** button to add individual workgroups.
7. To remove a work group, select it, and click the **Remove** button.
8. Click **Save**.

⇨ All the cardholders in the selected workgroups will inherit the access privileges of the venue selected for this venue booking.

Actions triggered by Venue Booking Time

The Advanced Security Programming (ASP) functionality in SiPass integrated includes venue booking as event trigger. After setting up a venue, you can configure an ASP activity to trigger an action, before or after every booking start or stop. This helps in creating different actions for the same venue based on the time the booking is made for that venue.

For example, an action can be configured to turn on the air conditioning 10 minutes before the booking start time, or turn on the lighting 5 minutes before the booking start time, turn off the lighting and air conditioning 2 minutes after the booking stop time.

Note: In case of bookings with overlapping start and end times, care must be taken that an action for the start of next booking is not cancelled by the end time of the previous booking. For example, if the lights-on action is set to 11:00 am for Booking 2 but the lights-off action from Booking 1 is set to 11:02 am, the overlap in start and end trigger times of the two bookings will turn off the lights for booking 2.

More details of the event trigger properties can be found in the *SiPass integrated MP2.65 Reference Manual*.

6 Monitoring Your Site

SiPass integrated allows you to monitor and control your site using a number of powerful and easy-to-use tools. Primarily, you monitor activity at your site with Active Audit Trail or a Site Plan. (To view, edit and operate any of your sites using Site Plans, you must have the optional *Graphics Module* installed.) Your site is constantly monitored in the background using the SiPass integrated alarm system, which immediately informs you of alarm situations.

6.1 Active Audit Trail Window

The *Active Audit Trail* Window (main screen) allow you to monitor events that occur at your site as they happen. You can specify which events, and what specific information each event is displayed in the *Active Audit Trail* Window.

All database changes made by an operator are logged to the SiPass integrated audit trail, including brief information regarding the details for each change made.

The Main Screen is arranged into two separate viewers with a movable horizontal partition inserted between each viewer. The viewing windows operate independently of each other.

The upper viewer of the Active Audit Trail window displays a list of events that have occurred at your site. The most recent event will occur at the bottom of the viewer.

The lower viewer of the Active Audit Trail window displays a list of the most recent events that have occurred at your site. The most recent event will always occur at the bottom of the viewer and, as new events appear, previous events will automatically be scrolled upwards.

You may use the scroll bars located on the right-hand side of the viewers to view events or alarms that do not appear on your screen.

It is recommended that if you wish to view an event that has scrolled above the physical display, you use the upper viewer. This allows you to continually monitor events as they occur in the lower viewer.

The Alarm Queue icon in the status bar displays a list of outstanding alarms waiting to be actioned or restored to normal. The Alarm Queue can be turned on or off without affecting the appearance or operation of the Audit Trail windows.

SiPass integrated allows you to perform the following tasks by right-clicking on an audit trail entry:

- View the details of a point associated with an audit trail entry
- View the details of a cardholder associated with an audit trail entry
- Allow entry to a cardholder that has violated Anti-Passback rules
- View a photograph of the cardholder stored in the database
- View a live image snapshot of the cardholder, if the Image Verification module is installed and the snapshot option enabled.
- View a DVR recording, if the DVR Interface module is installed.
- View details of a visitor associated with an audit trail entry.

An icon representing each event that appears in the Active Audit Trail window is located in the leftmost column.

6.1.1 Multiple Audit Trail Views

SiPass integrated allows operators to customize and view multiple live audit trail views (referred to as **Custom Transaction Logs** in SiPass Explorer) at the same time. This enhanced feature allows operators to filter display fields in each custom transaction log.

Operators can apply from SiPass Explorer.

For information on Custom Transaction Logs, please refer the section Custom Transaction Logs of the SiPass Explorer User Manual.

6.2 SiPass integrated Alarm System

The SiPass integrated alarm system monitors your site via points, groups and units. If one of these elements changes its state, you can configure an alarm to activate. You can also establish the method used to handle this alarm and it's priority level.

6.2.1 Creating an Alarm Class

An Alarm Class allows you to be notified of a change in state at a particular point, or group of points. The Alarm Class allows you to determine how the operator is notified of the door violation, and the way in which they must handle the alarm.

1. Choose **Alarm Class** from the **Program** toolbar or menu.
2. Enter a unique name for the alarm class into the **Alarm Definition Name** field. You may enter up to 40 characters, in any combination of upper and lower case letters and numbers.
3. Select the type of alarm class from the **Type** field. To change the alarm class type, choose the drop down arrow and select a new type from the list.
4. Select the color you want the message text to be when displayed on the **Alarm Queue** screen. Choose the **Alarm Display Color** button, and select a color from the palette.
5. Select the background color you want the message background to display on the Alarm Queue screen. Choose the **Select Alarm Background Color** button and select a color from the palette.
6. Complete the Alarm Handling details.
7. To change the alarm priority, choose the drop down arrow and select a new alarm priority from the list.
8. Specify the **Instruction File Name**. Details the file name of the alarm instruction(s) that may be retrieved by the operator when the alarm is triggered. To change the file name, choose the drop down arrow and select a new file name from the list.
9. Specify the **Sound File Name**. Details the file name of the sound file to be played when the alarm is triggered. To change the sound file, choose the drop down arrow and select a new sound file from the list. If no file is specified, the default alarm sound will be used. A sound file can only be specified if a sound card is installed in the computer. A sound file must be placed in the correct location before it can be incorporated into an alarm class definition typically, "C:\Program Files\SiPass\DataFolder\Drawing\Sound".
10. If the alarm requires acknowledging, tick the **Requires Acknowledging** checkbox.
11. If the Requires Acknowledging checkbox is ticked, the following fields can be configured:
    - **Alarm Priority**: Set the priority of the alarm
    - **Instruction File Name**: Select an Instruction File that will be displayed to operators when the alarm is raised.
    - **Sound File Name**: Select a Sound File to be configured for the alarm
12. Complete the **Alarm Options** details.
    - **Restorable Alarm**: Tick this checkbox if the alarm is configured as a restorable alarm.
    - **Forward via OPC**: Tick this checkbox to forward the alarm via the OPC bus.

- **Forward to GSM Mobile(s) checkbox**: Tick this checkbox to forward this alarm to a GSM Mobile(s). The cardholder's mobile number must be saved in the cardholder dialog for this feature to work.
- Once actioned, re-activate alarm every: Configure the time interval between re-activated alarms.
- **If not actioned, trigger a host event task after**: Configure a time-period after which a host event task will be raised, if the alarm is still not actioned.

13. Define the Current Defined States details. For details on the available states for various Alarm Types, please refer the section **Alarm Class** of the SiPass integrated Reference Manual.
14. Click **Save**.

6.2.1.1 Alarm Class Options

The table below describes the configuration options for Alarm Classes.

Option	Description
Requires Acknowledging	If this checkbox is ticked, the operator must acknowledge an alarm once if it has been triggered.
Edit Alarm Priority	Choose this button if you want to create new alarm priorities, other than the standard SiPass integrated Lowest to Highest. Up to one thousand Alarm priorities in total can be defined.
Alarm Priority	Specifies the priority level for the alarm class. • None: Will be sent to the Audit Trail, but will not appear on the Alarm Queue. • Lowest: Will display an Alarm dialog, but will appear at the bottom of the alarm queue. • Standard 1 to 5: Will display an Alarm dialog, and will appear above lowest priority alarms in the alarm queue. An alarm priority of standard 5 is of a higher priority than an alarm of priority of standard 1. • Highest: Will display an Alarm dialog, and will appear at the head of the alarm queue.
Restorable Alarm	Tick this checkbox to require that an alarm must return to a normal state, and be actioned by an operator, before the alarm will be completely deactivated. A non-restorable alarm is considered normal as soon as it is actioned. When you choose to make an alarm class restorable, you must define both an "alarm" and "restore" state for that alarm class.
Once Actioned, re-activate alarm every	Specifies the Time period before an actioned alarm is re-activated, if it has not already been restored to its normal state.
If not actioned, trigger an event after	Specifies the Time period after an alarm is triggered that a specified event should occur, if the alarm has not been actioned.
Forward Via OPC	If this checkbox is ticked, when this alarm occurs, the point name, alarm state and point status will be forwarded to every OPC point that you have defined in the Components dialog.

6.2.2 Creating a Defined State

The Alarm Class can assume a number of different states. Each possible state must be defined. An alarm is triggered when a point enters into a state defined as an alarm.

1. Choose **Alarm Class** from the **Program** toolbar or menu.
2. From the **Alarm Class Name** field, select the name of the alarm class for which a state is to be defined.
3. Choose **Add**.
   ⇨ A new line will appear in the **Defined States** grid.
4. Select the item in the **Status** column.
5. Specify the status to be defined.
6. To change the status type, choose the drop down arrow and select a new status from the list. To expand the drop down list so that you can view the entire text, you can click on the right hand border of a column and drag to increase the column width.
   - **Alarm State Status for 3rd Party Systems in SiPass integrated:** If you have entities of 3rd party systems that are integrated with SiPass, the status of these entities can be uploaded and downloaded between the two systems. The status corresponding to the 3rd Party system will contain the term '**External System'** in the drop down list. For example, for the **Access** alarm type, 3rd Party systems can have defined states with the status **Door Held External System**, **Lock External System**, etc.
7. Enter the status description (in the **Status Description** column) that will appear in the Audit Trail, alarm queue, and alarm query when this status is reported.
8. Specify the status type. To change the status type, select a new state from the **Alarm/Restore** column.
   - **Alarm**:
     If the status is defined as Alarm, whenever it occurs, the corresponding point, area, group or unit will be considered to be in an alarm state. An audit trail event will be generated, and any other events you have defined for the alarm class will be triggered.
   - **Restore**:
     If the status is defined as Restore, whenever it occurs, the corresponding point, area, group or unit will be considered physically restored to its normal state. You cannot define a status as “Restore” if you have not ticked the Restorable Alarm check box.
   - **Ignore**:
     If the status is defined as Ignore, when it occurs, nothing will be reported in the alarm queue, no changes will be displayed on the site plans, and no event tasks will be triggered.
9. Specify the symbol (in the **Symbol Name** column) to appear on the site plan to indicate the status of the alarm. To change the symbol, choose the drop down arrow and select a new symbol from the list.
10. Select **Yes** in the Dial Back column, if you want a remote component (assigned this alarm class) to initiate a dial back to the SiPass server if an alarm occurs.
11. Click **Save**.

6.3 Handling Alarms

When an alarm is triggered in SiPass integrated, the *Alarm Display* dialog will appear.

Once such an alarm has been triggered, there are a number of tools that you can use to handle the situation. Every alarm shown in the *Alarm Display* dialog requires the alarm event to be actioned. By actioning the alarm, you acknowledge that you know about the alarm condition and are doing something to rectify the situation.

An operator can select from a list of custom responses when actioning an alarm, or enter their own. After the alarm has been actioned, further tasks may need to be carried out in order to return the alarm to its normal state.

There are two types of alarm conditions that can occur:

- Restorable
- Non-restorable

6.3.1 Restorable Alarms

Restorable alarms occur when something has physically changed at your site. For example, if an alarm class for a door-frame existed on your SiPass integrated database, the alarm can be set to restorable. If the door has been forced, and triggered alarm, you can action that alarm. But, that input will not return to normal until the door is physically closed. If it is not returned to its normal state within the Time Period specified in the alarm-class record, the alarm will reactivate. The reactivated alarm will trigger the Alarm Display dialog to appear again, and the count will increment to one.

Sometimes a point, area, group or unit, which is restorable, will return to normal before you action the alarm. For example, an open boom gate might close; in which case, actioning the alarm would be sufficient to clear it.

To restore an alarm you may need to do one or more of the following:

- Physically change the situation at your site. For example, you may need to close a door that is obstructed.
- Unsecure (disable) the input point so that it no longer registers an alarm.
- Manually send a command through the system to restore the point, area, group or unit.
- Find out more about the point, area, group or unit registering an alarm.

6.3.2 Non-Restorable Alarms

Defining a Non-Restorable Alarm generally assumes that you want the operator to acknowledge a specific alarm once only. For example, you may define an alarm class so that a void card is detected at a reader connected to a main door. You want the operator to acknowledge that someone has attempted to gain access using a void card. If the alarm is not restorable, the point in alarm will be considered normal as soon as the alarm is actioned.

The related alarm will be cleared from the alarm queue.

6.3.3 Creating Custom Alarm Responses

SiPass integrated allows you to create pre-defined alarm responses that can be selected from a menu in the *Alarm* dialog. This means that alarm responses can be consistent for similar alarm events. New alarm responses can be added “on the fly” from the *Alarm* dialog.

1. Select **Alarm Responses** from the **Program** menu.
2. Enter your pre-defined response into the **Alarm Response** field.
   ⇨ This message will appear in the Audit Trail when the alarm is actioned by an operator.
3. Choose **Add** to add your response to the **Current Alarm Responses** list. Each item in the list will appear on the **Pre-defined Alarm Response** menu in the *Alarm* Dialog when an alarm is triggered.
4. Repeat steps 2 – 3 for every alarm response you want to be available to operators. Choose **Close** when you have finished.

6.3.4 Actioning an Alarm

When an alarm is triggered and an *Alarm Display* dialog appears, you must action the alarm. By actioning the alarm, you are logging a message to the system, indicating that you have acknowledged the alarm and are doing something about it.

There are three ways you can action an alarm:

- Via the *Alarm Display* dialog
- Via the **Site Plan**
- Via the **Alarm Queue**

6.3.4.1 Method 1 - Alarm Display dialog

When the *Alarm Display* dialog appears the alarm status display appears in the upper left-hand corner of the *Alarm Display* dialog. This display informs you of the number of events currently in the alarm queue, the number of alarms that have been actioned and are waiting to be restored, and the location of the alarm that triggered the dialog and the reason for the alarm.

1. Select an appropriate alarm response from the **Pre-defined Alarm Response** drop-down box, or enter a new response. The text entered should briefly reflect the nature of the alarm and the action taken by the operator/security personnel.
2. Choose **Add Response** to add the response to the **Log of action taken** field. You may select or enter multiple alarm responses, by choosing **Add Response** after each entry. You must enter a response into the dialog before the **Action** button is enabled. You can choose **Edit Response** to open the *Alarm Responses* dialog, which allows you to create, modify and delete pre-defined alarm responses.
3. Choose **Action**. The *Alarm Display* dialog will be removed and an event will appear in the Audit Trail indicating that the alarm has been actioned. The contents of the Log of action taken field will also be displayed in the Audit Trail, to show what action has been taken in response to the alarm.
   – To silence the alarm before actioning it, you can enter the time (in seconds) into the secs field and choose Silence. The Alarm Display dialog will disappear and the alarm will be silenced. If the alarm has not been actioned before the silence time has expired, the alarm will re-trigger.
   – The action of silencing the alarm will appear in the Audit Trail as well as each time that the alarm re-activates.
   – More than one operator may receive the alarm at their Client PC. However, only one operator needs to action the alarm.

6.3.4.2 Method 2 - Site Plan

1. Choose **Plan**, from the *Alarm Display* dialog.
2. Select the point, area, or floor to be actioned by clicking on it.
3. Choose **Action** from the **Alarm** toolbar.
4. Select an appropriate alarm response from the **Pre-defined Alarm Response** drop-down box, or enter a new response.
5. Choose **Add Response** to add the response to the **Log of action taken** field.
   - You may select or enter multiple alarm responses, by choosing Add Response after each entry.
   - You must enter a response into the dialog before the **OK** button is enabled.
   - You can choose **Edit Response** to open the *Alarm Responses* dialog, which allows you to create, modify and delete pre-defined alarm responses.
6. Choose **OK**.

⇨ The alarm event will disappear from the **Alarm Queue** window and an Audit Trail event will be generated, informing the SiPass integrated operator(s) that the alarm has been actioned. The *Alarm Display* dialog will be removed.

⇨ If the alarm is restorable, and has not been restored to its normal state within the specified Time Schedule, the alarm will remain in the **Alarm Queue** window and continue to re-activate until it has been restored.

⇨ An event will appear in the Audit Trail that indicates the alarm has been actioned. The contents of the Log of action taken field will also be displayed in the Audit Trail, to show what action has been taken in response to the alarm.

⇨ More than one operator may receive the alarm at their client PC. However, only one operator needs to action the alarm.

To action alarms from Site Plans, the operator should have the appropriate Operator Privilege for Site Plans, and also privileges to the particular unit or point in concern.

6.3.4.3 Method 3 - Alarm Queue

All alarms that have been triggered and are waiting to be restored to their normal state or to be actioned appear in the *Alarm Queue* window. As well as being displayed in the Alarm Queue, the alarms are also displayed in the Audit Trail.

1. Choose **Queue** from the **Alarm** toolbar or choose **Alarm Queue** from the *Alarm Display* dialog.
   ⇨ A message will appear in the Audit Trail indicating that you have crossed to the *Alarm Queue* Window.
2. Highlight the alarm to be actioned, by clicking on it. More than one alarm can be actioned at once, by using CTRL – Left Click to select multiple rows.
3. Choose **Action**.
4. Select an appropriate alarm response from the **Pre-defined Alarm Response** drop-down box, or enter a new response.
5. Choose **Add Response** to add the response to the Log of action taken field. You may select or enter multiple alarm responses, by choosing **Add Response** after each entry.
6. You must enter a response into the dialog before the **OK** button is enabled.
   - You can choose **Edit Response** to open the *Alarm Responses* dialog, which allows you to create, modify and delete pre-defined alarm responses.

7. Choose **OK**.

⇨ The alarm will disappear from the *Alarm Queue* window and an Audit Trail event will be generated, indicating the alarm has been actioned. The contents of the Log of action taken field will also be displayed in the Audit Trail, to show what action has been taken in response to the alarm.

⇨ If the alarm is restorable, and has not been restored to its normal state within the specified Time Schedule, the alarm will remain in the *Alarm Queue* window and continue to re-activate until it has been restored.

!	*NOTICE*
	The operator privileges (from the System Functions found on the Operator Group dialog) required to configure various aspects of the Alarm Queue are stated below. • Operators with View (v), Edit (e) and Create (c) privileges for the Alarm Queue can action alarms in the Alarm Queue. They can also use the 'Add Reponse' feature to add or delete a response to the Pre-defined Alarm Response. • Only Operators with Edit (e) privileges can edit existing Pre-defined Alarm Responses. • Operators with only View (v) permissions CAN action the alarm, and use an existing alarm response from the Pre-defined Alarm Response options. • An operator without any privileges for the Alarm Queue, will not be able to view the Alarm Queue dialog. ⇨ Further, Alarm Queue Privileges do not affect the privileges for Site Plan Alarms.

6.4 Controlling Points

SiPass integrated allows you to control points using a number of different tools. This flexibility allows you to send commands to individual points, areas and units, view detailed information regarding a individual point, and provides an overview of all the components configured at your site.

6.4.1 Querying a Point

SiPass integrated allows you to view a detailed description of single point, intrusion area, group or unit. This information can often help you to handle an alarm situation, or just keep you up-to-date with the state of your site.

You can only query a point, intrusion area, group or unit using a Site Plan.

6.4.2 Securing and Unsecuring a Point

SiPass integrated allows you to secure or unsecure a single point, area, unit or group. By doing this you are able to override the normal behavior of an individual point, area or group. You can only secure or unsecure an area, point or group using a Site Plan, or the **Manual Override** function.

The following table provides a brief outline of the actions triggered when you secure or unsecure an individual point, area or group:

Point Type	Unsecure	Secure
Input Point	If you unsecure an input point, it will become disabled. A disabled input point cannot register an alarm. You may wish to disable an input that is faulty, and continually enters an alarm state for example.	If you secure an input point, it will become enabled. An enabled input point can register an alarm. You might wish to enable an input point that was previously disabled.
Output Point	If you unsecure an output, it will become unlocked. Unlocking an output is a fast way of allowing access. If the output controls a monitored door, it will stop the alarm for that monitored input.	If you secure an output point, it will be locked. Locking an output is a fast way of stopping an alarm activated due to the point being unlocked.
Groups / Intrusion Areas	If you unsecure a group or Intrusion area, its individual points will be unsecured.	If you secure a group or area, its individual points will become secured.

6.4.3 Allowing Access to an Output Point

SiPass integrated allows you to override the normal behavior of an individual output point, to allow access to a particular location. For example, if a cardholder forgets their access card and needs to gain entry into a secure location, you can allow that cardholder to gain access by sending that point a manual 'allow access' command. This command initiates the same system processes as if they had actually used their card access. You can only allow access to an output point (door) using a Site Plan.

6.4.4 Manual Override

Manual override allows you to manually manipulate an individual point, intrusion area, floor or elevator by sending electronic messages through the system. Manual commands can also be used to perform diagnostic functions. These commands will often be sufficient to restore locations to their normal state, or to check the correct operation of a specific point.

To send a manual command:

1. Choose **Manual Override** from the **Operation** toolbar.
2. Select a point, elevator, area or unit from the **Type** toolbar.
3. The **Commands** available for the type you select will appear inside a list box of commands.
4. Select the unit to which the point, point group, area, elevator or unit is associated (not available for Type = Unit) from the **Unit Name** field. The default selection "All Units" will display all the points, point groups, areas, and elevators available in the system.
5. Select the specific point, point group, intrusion area, elevator or unit to which you wish to send a command from the list box at the bottom of the *Manual Override* dialog.
6. Select the Command to be sent, from the list box of commands.
   - ⇨ Additional fields may need to be completed depending upon the type of command that you select.
   - ⇨ When the *Manual Override* dialog is first opened, the default setting opens with the **Access** button selected and the **Allow Access** command highlighted. An extra field to the right of the **Commands** drop down list (highlighted above) accompanies the following commands.

7. Enter the appropriate details in the additional field (if required). The command you have selected may require a “Duration” option:
   - **Until Time Schedule Change**:
     This command will apply until the next Time Schedule begins, or until the time entered in the **Duration** field expires, whichever occurs first. After this the component will revert to normal Time Schedule control. Entering a value of zero in the Duration field means that the command is effectively permanent; the command will apply until the next manual command is sent.
   - **Permanent**:
     This command will apply until the “Return to Time Schedule Control” command is sent to the component, or until the time entered in the Duration field expires.
8. Choose **Send**. The command will be sent and an event will be generated in the Audit Trail that indicates the type of action the command produced.

6.4.5 Using the Alarm Queue

The Alarm Queue displays a list of alarms with points, waiting to be restored to their normal state, or to be actioned. The Alarm Queue will automatically appear when an operator logs on AND there is an outstanding alarm.

- To display the Alarm Queue, choose **Alarm Queue** from the **Alarm** toolbar.

Once the window is displayed, you can view the information for each current alarm or action alarms that have not been actioned.

The following table describes the information contained in the Alarm Queue.

Column	Description
Priority	The priority of the alarm. Entries will be arranged according to their priority, as specified in their Alarm Class definition. Alarms of highest priority appear first.
Priority Desc	The description of the Alarm Priority, as recorded in the Alarm Priority dialog.
Date	The date the alarm was first triggered.
Time	The time the alarm was first triggered.
Location	The point, area, group or unit that triggered the alarm.
Status	A short message describing the status of the alarm. For example, “Waiting for normal” indicates the point, area, group or unit, which triggered the alarm, has been actioned but is waiting to be returned to its normal state.
Count	Number of times an alarm entered alarm and back to normal without being actioned.
Current State	A message describing the current state of the alarm. For example, “Door has been forced” indicates the door has been forcibly opened. This message is user-defined in the Alarm Class Definition dialog.

6.5 Overviewing Your Site

There are two ways in which you can gain an overall view of your site. The *Overview* window displays a graphical tree of every component in the SiPass integrated database, providing you with a summary of the contents.

The Status screen can be used to monitor the active components of your site, like door latches, clients and alarms, and is constantly updated in real time.

6.5.1 Database components

SiPass integrated allows you to obtain an overall picture of the configured Database components. The Database components appear in a tree-like structure that displays the Server, Cardholders, Workgroups, Point Groups, Points and Alarm Classes that have been configured and saved in the system. Only those objects to which you have privileges will appear.

To overview your site's Database components:

1. Choose **System Overview** from the **Data** toolbar or menu.
2. Double-click on each heading, to expand the tree one branch further.
   - For example, to display all the configured work groups, double-click on **Work Groups**. You can further expand the tree by double clicking on each individual work group to display the cardholders assigned to that work group. Double-clicking those elements that display a "+" will expand the tree by one level, while double-clicking elements that display a "–" will collapse the tree.
3. You may select any object to display brief details regarding that object in the right-hand panel of the window.
   - You may also right-click on any cardholder, work group or point to display a dialog containing information about the selected object. For example, if you right click on a cardholder's name the *Cardholder Maintenance* dialog will appear.

6.5.2 Viewing the Status screen

The SiPass integrated status screen provides a summary of the status of the active components of the system and current alarm conditions. You can choose to automatically have the status screen visible when an operator logs into SiPass integrated.

- Select **System Status** from the **Alarm** menu.

⇨ The *System Status* window will appear. The following table describes the information displayed in each tab:

Tab	Description
System Summary	Displays status information on all connections, alarms and doors.
Physical Points in alarm	Displays the status of all physical point alarms in the system.
Logical Points in alarm	Displays information on the status of all logical point alarms in the system.
Door Status	Graphical display of all system doors.

Automatically displaying the Status Screen on start-up

1. Select **Preferences** from the **Options** menu.
2. In the **System Status Monitor** section, tick the checkbox **Show on Startup**.

⇨ The value in the **Refresh Rate (sec)** field determines how often the data displayed in the Status monitor is updated to reflect the latest changes in status and alarm conditions.

7 Data Management

!	*NOTICE*
	• It is recommended that you use the backup functionality provided by your SiPass integrated system to perform any archiving of database material. • In cases where you are using 3rd party applications to backup data within your SiPass integrated system / folders, it is important to test this operation before implementation. Some backup software may conflict with the SiPass operation depending on the way in which it generates its backup data. • It is not recommended that system backups be performed during peak / busy durations of system functioning.

7.1 Managing the Database

There are three main methods by which an operator can manage the SiPass integrated database:

- Backing up the database
- Restoring the database

Both these methods have been discussed in the immediate sections that follow.

7.1.1 Backing up the Database

SiPass integrated allows you to back up information contained in the Database. All the information contained in the Database can be backed up as individual components (for example, image files) or can be backed up collectively. You may wish to backup the Database as a precaution against data corruption, or to move information contained in the Database to another location.

You can restore any Database records that you have previously backed up, through the following steps:

1. Select **Data > Backup > Database**.
2. Select the Database components that you want to back up by ticking or unticking the appropriate checkbox.

!	*NOTICE*
	The Local and System settings must not be used when restoring a backed up database onto a new PC (a PC other than the original SiPass integrated installation) or when a new build of SiPass integrated has been installed. Restoring these settings under the described circumstances may corrupt your SiPass integrated database.

3. Specify the location and name for the back up file in the **Backup To** field. You can choose **Browse** to graphically select a location for the backup.
4. Choose **OK** to begin the backup procedure.
   - ⇨ The *Backing Up Database* dialog will appear displaying the current status of the backup. When the backup procedure has been completed, a further Backup dialog will appear to inform you of the successful operation.
   - ⇨ When this operation is performed, the original PC Name and original SiPass integrated licence details will be restored to the repository.
5. Choose **OK**.

7.1.1.1 Database Backup Components

The table below explains the available database components when backing up the database.

Component	Description
Database	When ticked, backs up the entire Database including the Multi-site Access Management information, Custom Cardholder Pages, sounds, alarm instructions, look-up tables, operator preferences, and all the database files, themselves.
Graphics Files	When ticked, backs up the graphics information including, site plans, drawings, symbols, card templates, and cardholder images.
Images	When ticked, backs up all the images contained in the Database; for example, cardholder photos and signatures. The image files, themselves are backed up using this option.
Reports	When ticked, backs up all the custom Audit Trail Database report templates currently contained within SiPass integrated.
System Settings	When ticked, backs up the local machine's SiPass integrated-related settings; for example, the Server name, locations of data directories, printer information and registry keys. The locations of database files, graphics files, image files and report files are backed up using this option. In addition, settings related to the following functions are also backed up – Log Book and Guard Tour.
Local Settings	When ticked, backs up the local user (operator) settings; for example, the operator's system preferences

7.1.1.2 Host Event Task-Triggered Database Backup

An operator can configure a Database Backup to be triggered by a Host Event Task.

1. Select **Program > Event Task > Host**.
2. Configure the fields of the *Trigger* section, as required. For information on how to configure an Event Task, refer the Section Creating a Host Event Task [→ 58].
3. In the *Effect* Section, select **Database** in the **Target** field.
4. Select the required type of Database Backup from the options of the *Command drop down list.*

To perform a complete database backup, it is recommended that the **Database Backup – Full** command option be selected.

7.1.1.3 Cancelling an Event Task Triggered Backup

This feature allows the operator to cancel a Backup triggered by an Event Task.

To perform this function, select **Data > Backup > Cancel Automatic Backup**.

Operators should be given privileges to Host Event Task Backup to be able to use the **Cancel Automatic Backup** feature.

A status bar at the bottom of the screen will indicate the progress of the Host Event Task Backup.

7.1.2 Restoring the Database

SiPass integrated allows you to restore a previously backed up Database.

!	*NOTICE*
	Performing a Database restoration will overwrite any records that currently exist in the Database. You cannot cancel the restoration process once it has begun. If possible, make backup copies of the current Database before restoring a previous version of the Database.

1. Select **Data > Restore > Database**.
2. Specify the path and file name of the Database to be restored, in the **Restore From** field. You must choose **Browse** to select the location of the record to be restored. The backed up Database file should include the extension ".bkp".
   - The **OK** button will remain disabled until you have made a valid choice of backup file via the Browse facility. Only those items that were saved in the back up are available to be restored. For example, if the backup file contained only image information, then the only active switch would correspond to Images.
3. Select the components you wish to restore by ticking or un-ticking the appropriate checkboxes. Only those components that were originally backed up will be available to restore.
   - The Local and System settings must not be used when restoring a backed up database onto a new PC (a PC other than the original SiPass integrated installation) or when a new build of SiPass integrated has been installed. Restoring these settings under the described circumstances may corrupt your SiPass database.
   - Some minor settings, such as custom toolbars, will need to be re-configured after this restore process.
4. Choose **OK** to begin the Database restoration process.
   ⇨ When the restoration procedure has completed, a Restore dialog will appear informing you that the process is complete.
5. Remember to shut down both your SiPass Server and Client in order for the restored database to take effect. Remember to restart both your SiPass server and client.

⇨ The SiPass Audit Trail will display a status message that indicates the success of the database restoration. Each time a restoration process is attempted, SiPass integrated will perform an integrity check, to ensure that the database was restored correctly

⇨ If the restoration was not successful, it is recommended that you check the size of the SiPass SQL Transaction log (Asco4_log) and if necessary increase the size of this log.

7.1.2.1 Database Restore Components

The table below explains the available database components when restoring the database.

Component	Description
Database	Restores the entire Database
Graphics Files	Restores the graphics information; for example, site plans and symbols
Images	Restores all the images contained in the Database; for example, cardholder photos and signatures
System Settings	Restores the local machine settings; for example, the Server name, the locations of data directories, and so on.
Local Settings	Restores the local machine (operator) settings; for example, the operator's system preferences

7.2 Managing the Audit Trail

SiPass integrated allows its operators to manage their Audit Trails using three basic processes:

- **ARCHIVE**

Archiving is basically the action of moving Audit Trail entries/logs, kept in the SQL database table, to an external SQL archive files. These SQL archive files are in the SQL Compact format (with the **.sqlarc** file extension). This process allows the operator to maintain a collection of .sqlarc files at a destination referred to as the Archive Location.

- **BACKUP**

The Audit Trail Backup process involves creating copies of the SQL archive (.sqlarc) files, that are stored in the Archive Location, to another External / Backup location. This external location can be a backup server, or another other such backup media. Backups should be created before an upgrade installation of SiPass integrated. In the unexpected event of a hardware failure, operator error or any other such data loss, these copies or Backed up files can be used to update the original .sqlarc files.

- **RESTORE**

Generally performed after upgrading SiPass integrated, the Audit Trail Restore process involves copying all the backed up .sqlarc files from the External / Backup location back to the Archive Location. These files will then become available for Audit Trail Reporting purposes.

Process	Retrieve From	Send To
ARCHIVING	SiPass integrated Audit Trail	Archive Location
BACKUP	Archive Location	External / Backup Location
RESTORE	External / Backup Location	Archive Location

SUMMARY OF BASIC AUDIT TRAIL MANAGEMENT PROCESSES

SiPass integrated allows operators to manage Audit Trails using three basic processes:

- Archiving Audit Trials to an Archive Location
- Manual Backup of Audit Trails from Archive Location to an Backup/External Location
- Restoring Audit Trail files from Backup/External Location to Archive Location

7.2.1 Archiving the Audit Trail

SiPass integrated allows you to make a record of the events that have occurred at your site and that have been logged to the Audit Trail.

Archiving of Audit Trails can be done in two ways:

- Automatic Audit Trail Archiving
- Manual Audit Trail Archiving (Forced Operation)

7.2.1.1 Automatic Audit Trail Archiving

The SiPass integrated audit trail is archived automatically daily. This means that the audit trail is stored in archive files at regular intervals without the need for manual intervention.

As part of the Automatic Audit Trail Archiving process, SiPass Integrated will use a default location. However, the operator has the option of configuring a different archive location, outlined below.

(Optional) Configuring the Audit Trail Archive location

1. Select **Preferences** from the **Options** Menu.
2. Select the **Audit Trail** tab.
3. Click the **Archive Folder Location** button.
4. Enter the path of the folder in which the backups will be stored in the **Current Archive Folder Location** field. Alternatively the **…** button may be clicked and a location can be chosen by browsing for an appropriate folder location.
5. Select **OK**.
6. Click **Save**.

The specified folder must be accessible from the SiPass integrated Server PC with the Windows User Account that is logged on. It is recommended that this location is specified using a UNC path designation.

7.2.1.2 Manual Audit Trail Archiving (Forced Operation)

The operator can choose to perform a forced Audit Trail archive operation. This is particularly useful in instances where the operator may want backup the database in preparation for a SiPass integrated version upgrade. This operation will also archive the current days audit trail.

1. Select **Data > Archive > Audit Trail**.
2. Click **Yes** to start the Manual Audit Trail Archiving operation.

It is recommended that this manual Audit Trail Archiving operation be performed before backing up a database.

7.2.2 Backing up the Audit Trail

In this process, the audit trail files are manually copied to an Archive Location where it is stored.

1. Select **Data > Backup > Audit Trail**.
2. Select the radio button corresponding to the task to be performed – **Backup Only**, **Backup** and **Purge or Purge only**.
3. Choose **List Dates**.
   ⇨ All the Audit Trail records that exist, between the specified start and end dates, will appear in the **Available Dates** list box.
4. Select the specific date to be backed up, by clicking on it.
5. Choose **Add >**.
   ⇨ The selected date will appear in the **Selected Dates** list box.
6. Repeat Steps 4 and 5, until you have selected all the dates to be backed up.
7. Specify the location for the back up file in **the Backup To** field. You may choose **Browse** to select a location for the backup.
8. Choose **Execute** to begin the backup process.

⇨ The **Status** box, located at the bottom of the dialog, will display the status of the backup process

7.2.2.1 Audit Trail Backup Operations

The table below explains the various backup operations and configuration.

Option	Description
Backup only	Allows you to create a backup of Audit Trail records only.
Backup and purge	Allows you to make both a backup of the Audit Trail records in another location and delete them from their current location.
Purge only	Allows you to delete the Audit Trail records. Select the date-range over which the backup will be performed.
From	Specifies the start date for the backup date range. If no records exist for this date, the first archive displayed in the Available Archives list will automatically become the next subsequent file. To change the date, choose the drop down arrow and select a new date from the calendar displayed.
To	Specifies the last date for the backup date range. If no records exist for this date, the last archive displayed in the Available Archives list will automatically become the latest previous file. To change the date, choose the drop down arrow and select a new date from the calendar displayed.

7.2.3 Restoring the Audit Trail

SiPass integrated allows you to restore previously backed up Audit Trail records, according to date. You can restore Audit Trail Archive files, or TAB files.

The following instructions explain how to restore Audit Trail from the TAB files generated by older versions of SiPass integrated.

▷ Ensure that your Archive Folder location has been set to where your archived Audit Trail files are kept.

1. Select **Data > Restore > Audit Trail**.
2. Specify the path of the file(s) to be restored, in the **Restore From** field. You can choose **Browse** to select the location where the TAB files/Archive files are kept.
3. Select each file (in the **Available Files** list) from which the Audit Trail will be restored.
4. Choose **Restore** to restore the Audit Trail records from the selected files.

Please note that on restoring a TAB file, it will be converted to an Archive file automatically.

7.2.4 Purging the Audit Trail Archives

SiPass integrated allows you to delete Audit Trail records that are no longer needed at your site across a range of dates.

Before purging any Audit Trail records, it is highly recommended that you back up Audit Trail records to another location, (for example, a tape or disk), just in case they need to be retrieved at a later date. This can be achieved by selecting the **Backup and Purge** option from the Task section of the dialog.

1. Select **Data > Purge > Audit Trail**.
2. Select the date range over which the purge will be performed.
   - **From**: Specifies the start date, for the purge date range. If no records exist for this date, the first file displayed in the **Available Archives** list will automatically become the next subsequent file. To change the date, choose the drop down arrow and select a new date from the calendar displayed.
   - **To**: Specifies the last date, for the purge date range. If no records exist for this date, the last file displayed in the **Available Archives** list will automatically become the latest previous file. To change the date, choose the drop down arrow and select a new date from the calendar displayed.
3. Choose **List Archives**. All the Audit Trail records that exist, between the specified start and end dates will appear in the **Available Archives** list box. Both the Start and End dates are included.
4. Select the specific files to be purged by clicking on it.
5. Choose **Add >**. The selected files will appear in the **Selected Archives** list box.
6. Repeat steps 4 and 5, until you have selected all the files to be purged.
7. Choose **Execute** to begin the purging process.

⇨ The **Status** box, located at the bottom of the dialog, will display the status of the purge process and a purge event will be recorded in the Audit Trail.

7.2.5 Host Event Task Triggered Audit Trail Purge

An operator can configure a purge of all audit trail archive files to be triggered by a host event task.

1. Select **Program** > **Event Task** < **Host**.
2. Configure the fields of the *Trigger* section as required. For information on how to configure an event task, refer the section Creating a Host Event Task [→ 58].
3. In the *Effects* section, select **Database** for the **Target** field.
4. Select **Purge Audit Trail** in the **Command** drop down list.

7.3 Managing the Log Book

The Log Book can be managed in three main ways:

- Backing up the Log Book
- Restoring the Log Book and
- Purging the Log Book

These three options have been discussed in the immediate sections that follow.

7.3.1 Backing up the Log Book

SiPass integrated allows you to make a record of events or conditions at your site that are significant enough to be reported separately in the Log Book. The operators record these events in the Log Book so that they may inform the relevant persons of the events or conditions independently of the Audit Trail. You may also purge the information simultaneously, creating an archive of Log Book records.

You cannot backup the Log Book for today's date. Only dates that have occurred before the current date can be backed up.

1. Select **Data > Backup > Logbook**.
   ⇨ The *Backup and/or Purge Log Book* dialog will appear with the **Backup Only** radio button is highlighted by default.
2. Select the radio button corresponding to the task to be performed.
3. Select the date range over which the backup is to be performed.
4. Choose **List Dates**.
   ⇨ All the Log Book records that exist, between the specified start and end dates, will appear in the Available Dates list box.
5. Select the specific date to be backed up, by clicking on it.
6. Choose **Add >**.
   ⇨ The selected date will appear in the **Selected Dates** list box.
7. Repeat Steps 4 and 5, until you have selected all the dates to be backed up.
8. Specify the location for the back up file in the **Backup To** field. You may choose **Browse** to graphically select a location for the backup.
9. Choose **Execute** to begin the backup process.

⇨ The **Status** box, located at the bottom of the dialog, will display the status of the backup process.

7.3.1.1 Log Book Backup Operations

The table below explains the various backup operations and configuration.

Option	Description
Backup only	Allows you to create a backup of the Log Book records only.
Backup and purge	Allows you to make both a backup of the Log Book records in another location and delete them from their current location.
Purge only	Allows you to delete the Log Book records.
From	Specifies the start date for the backup date range. If no records exist for this date, the first date displayed in the Available Dates list will automatically become the next subsequent date. To change the date, choose the drop down arrow and select a new date from the calendar displayed.
To	Specifies the last date for the backup date range. If no records exist for this date, the last date displayed in the Available Dates list will automatically become the latest previous date. To change the date, choose the drop down arrow and select a new date from the calendar displayed.

7.3.2 Restoring the Log Book

SiPass integrated allows you to restore a previously backed up Log Book record. You may wish to restore a previously backed up record for the purpose of generating a report.

▷ Back up the current Log Book records before restoring a previous version.

1. Select **Data > Restore > Logbook**.
2. Specify the path and file name of the Log Book record to be restored, in the **Restore From** field. You must choose Browse to graphically select the location of the record to be restored. The backed up Log Book file should include the extension ".dlz".
3. Select the date or dates from the **Available Dates**.
4. Choose the **Select All** button if you wish to restore all the dates listed in the **Available list**.
5. Choose **Restore** to begin the Log Book restoration process.
6. Choose **Close**.
7. Create a Log Book Report, to ensure that the Log Book has been restored.
8. Shut down and re-start both your SiPass Server and Client after the restoration is complete.

7.3.3 Purging the Log Book

SiPass integrated allows you to delete Log Book records that are no longer needed at your site.

Before purging any Log Book records, it is highly recommended that you backup the Log Book records to another location, (for example, a tape or disk), just in case they need to be retrieved at a later date. This can be achieved by selecting the Backup and Purge option in the Task section of the dialog.

1. Select **Data > Purge > Log book**.
   ⇨ The *Backup and/or Purge Log Book* dialog will appear with the Purge Only radio button highlighted.
2. Select the date range over which the purge will be performed.

- **From**: Specifies the start date for the purge date range. If no records exist for this date, the first date displayed in the Available Dates list will automatically become the next subsequent date. To change the date, choose the drop down arrow and select a new date from the calendar displayed.
- **To**: Specifies the last date for the purge date range. If no records exist for this date, the last date displayed in the Available Dates list will automatically become the latest previous date. To change the date, choose the drop down arrow and select a new date from the calendar displayed.

3. Choose **List Dates**. All the Log Book records that exist, between the specified start and end dates will appear in the Available Dates list box.
4. Select the specific date to be purged, by clicking on it.
5. Choose **Add >**. The selected date will appear in the **Selected Dates** list box.
6. Repeat steps 4 and 5, until you have selected all the dates to be purged.
7. Choose **Execute** to begin the purging process. The **Status** box, located at the bottom of the dialog, will display the status of the purge process and a purge event will be recorded in the Audit Trail.

7.4 Using a Compact Flash Card for Database Management

When enabled, the Compact Flash Card features the following benefits:

- Larger database storage for large sites
- Persistent Audit Trail which can be preserved over a power loss

In effect, the Compact Flash Card replaces the functionality of the Onboard Flash for database storage and the volatile RAM used for Audit trail.

The life of a compact flash depends upon the amount of data written and erased from it. Taking this into consideration, it is recommended that an Industrial grade flash, with level 2 wear leveling and a larger size than 64Meg, be opted for use. This type of flash card ensures greater card life, robustness and performance.

7.4.1 Configuring a Compact Flash Card in SiPass integrated

This section specifies how a Compact Flash Card can be configured within SiPass integrated.

Install the card as per instructions provided in the Compact Flash Installation Manual.

After the Compact Flash Card has been inserted, initialize the ACC, choosing **Compact Backup** from the *Initialize System* dialog to compact the data and save to the flash card.

After it has been inserted, the Compact Flash Card becomes active only after the first initialize of the ACC.

8 Reports

The SiPass integrated system contains a powerful reporting package, which allows you to create detailed reports on information contained in the Log Book. You can customize the information that appears in each report to suit your own needs. Any reports you produce will only contain data to which your operator group has privileges.

SiPass Predefined reports are available through SiPass Explorer, to access the whole range of reports available to SiPass integrated. It can be accessed via the **SiPass Explorer** menu or toolbar. For a full description of the SiPass Predefined reports functionality, please refer to the SiPass Explorer User Manual.

8.1 Log Book Reports

The Log Book offers an integrated reporting tool to prepare daily activity reports by operators. At some sites, the preparation and submission of a Log Book report is mandatory, and in some circumstances, may even be a statutory requirement for operators monitoring the activities of a site.

Creating a Log Book Report is very similar to creating Database or Audit Trail reports The process of creating a report is roughly a three-step operation, but the exact number of steps required will depend upon how complex a report you want to create.

Step 1: Ordering Report Records

1. Select **Data > Reports > Log Book Report**.
2. Complete the **Date / Time Range** details.
   - **From**: Contains two fields - **Date** and **Time** - which determine the oldest Time Schedule from which the Log Book information will be selected.
   - **To**: Contains two fields - **Date** and **Time** - which determine the most recent Time Schedule from which the Log Book information will be selected.
3. Select whether the report will be sorted by **Operator Name** or **Subject** by highlighting this field in **Fields Selected** list box.
4. Select the sort function to apply to this field by enabling the corresponding radio button. Choosing either **Ascending** or **Descending** will cause an icon to appear next to the selected field, indicating that records will be sorted in alphabetical or reverse alphabetical order according to your choice of radio button. Please note that the sort function does not have to be used.
   - **None**: When enabled, does not use the selected field to sort the information.
   - **Ascending**: When enabled, sorts the information by the specified field, in ascending order.
   - **Descending**: When enabled, sorts the information by the specified field, in descending order.

Step 2: Creating a Query

By creating a query, you can filter the records that will appear in the report, based on the criteria you select. If you do not wish to filter the records displayed in the report, simply proceed to step 3.

1. Choose the first constraint to be placed on the report information by selecting a field from the list.
2. Select the specific attribute to be used as the constraint. For example, if you chose to create a query based on operators, you may select the specific operator from the **Operator Name** drop-down list.

3. Select the **Query** filter to apply, from the **Filter** list. To change the filter, choose the drop down arrow and select a new filter from the list.
4. Choose **Add**. The specified data query will be added to the **Query** box.
5. If you want to enter more than one query, you can choose the way in which multiple queries are handled, by selecting the correct operand between each.
   - **And**: When selected, the report will display all results that match the combined queries entered, as if they were a single query. Using the AND function to filter between criteria belonging to the same field type (eg: points) will return a blank report).
   - **Or**: When selected, the report will display all results that match each query entered, as if they were separate queries.
6. For more complex reports, you can group queries together, using the ( ) button

⇨ If you select the **Remember Settings** checkbox before exiting the dialog or previewing the report, the current query will load when you next open the *Log Book Report* dialog.

Step 3: Printing, Previewing or Exporting your Report

Once you have selected the information on which to base your report, chosen the order in which records are to be displayed and created your query, you are ready to print, preview, or export your report.

8.1.1 Log Book Report Filters

The table below explains the available Log Book report filters.

Filter	Description
Equals	The report will display only those records that exactly match (except case) the entered criteria.
Not Equals	The report will display all the records that do not exactly match the entered criteria.
Like	Allows you to use a wild card in the query. For example, an entry of “Like %t%” for a cardholder’s First Name, would result in a report displaying all cardholders whose first name contains the letter “t”. You may also use “[]” to find a single character in a specified range (for example, “like [\]” ¬would search for the character \. The standard Windows wild card “*” does not work in this instance.
Less than	This query has two sub-functions. The first applies to numerical data, where the report displays all records that are numerically smaller than the entered data. The second applies to alphabetical data, where the report displays all records that alphabetically precede the entered criteria.
Less than or equal to	A combination of both the Equals and Less than query filters.
Greater than	This query has two sub functions. The first applies to numerical data, where the report displays all records that are numerically larger than the entered data. The second applies to alphabetical data, where the report displays all records that alphabetically follow the entered criteria.
Greater than or equal to	A combination of both the Equals and Greater than query filters.

8.2 Scheduled Reporting

Reports within SiPass Reporting can be automatically generated and exported with an event task. This allows you to perform regular reporting without the ongoing manual effort.

The following actions can be scheduled:

- Printing
- Exporting to a file
- Exporting and emailing

To schedule reporting

▷ Email functionality requires you to configure cardholders for email, and the server for sending mail.

1. Click **Program** and select **Event Tasks > Host**.
2. Enter a name for the event task.
3. Select a valid **Time Schedule** to control when the event will occur.
4. Select a **Source** and **State** for when the event task will trigger
   - If you want to schedule the report for a specific time, set the **Source** to **Time Schedule** and set the **State** to **Start**. This will trigger the event when the Time Schedule selected above begins.
5. Set **Target** to **Reporting** and select a Report to use from the list
6. Select **Print**, **SaveAs** or **Email Forwarding**.
   - If selecting **Print**, click the **…** button to configure the print settings.
   - If selecting **SaveAs**, select the Type of file to export to and click the **...** button to select the file to save to.
   - If selecting **Email Forwarding,** click the **+** button to add a cardholder to the list of recipients. Only cardholders with email forwarding enabled will be shown in this list.
7. Enter a message in the **Message** field, that will print in the audit trail when the event task is run.
8. Click **Save**.

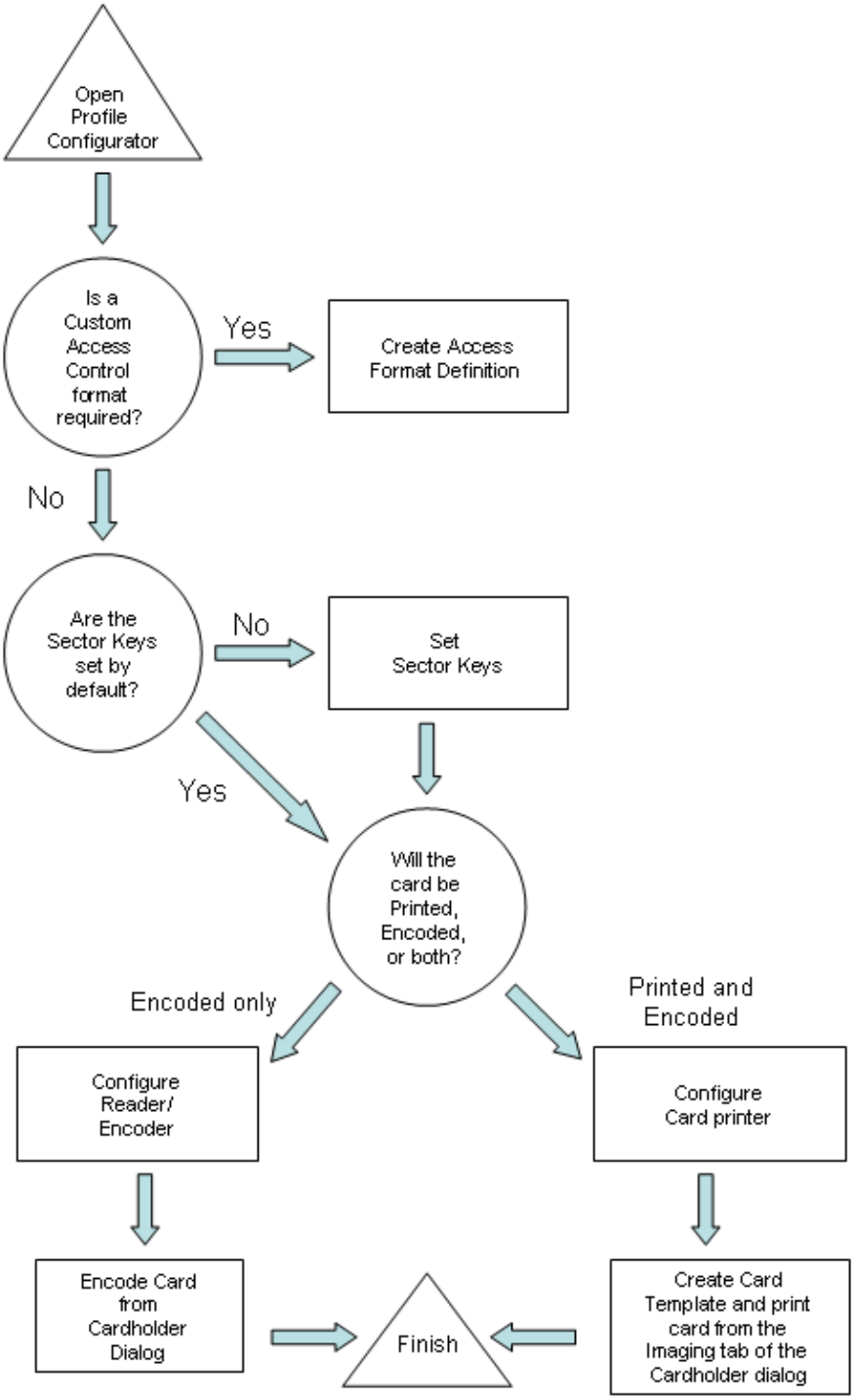
9 Smart Card Encoding

Smart Card Encoding is an option of the SiPass Integrated access control software. It allows SiPass integrated to both encode and read Mifare and DESFire based smart cards. This option supports a wide range of possible smart card formats and shows the user how a smart card will be used in and around their facility.

In addition, SiPass integrated allows individual smart card profiles to be pre-configured within the system, allowing each tenant or even cardholder's belonging to different divisions to have smart cards encoded with information that suits their exact needs.

Finally SiPass integrated also supports the use of card printers with built in smart card encoding mechanisms that allow smart cards to be encoded as they are printed. Of course, a dedicated smart card reader/encoder can also be used for this purpose.

The following diagram displays a rough flow chart for encoding smart cards from start to finish using SiPass integrated.



9.1 Creating a Smart Card Profile

A smart card encoding profile includes the information required to configure each sector and block or application and file on a smart card with the appropriate information, including the appropriate read and write keys.

1. From the **System** menu, select **Profile Configuration**.
2. Enter a name for the Smartcard profile into the **Profile Name** field.
3. Select the appropriate card type.

	NOTICE
	If DESFire is the **Card Type** selected, a checkbox **Format Before Encoding** appears below **the Card Type** drop-down. Check the **Format Before Encoding** checkbox if you want the smart card to be formatted before you encode new data. A Master Key can be set for DESFire cards, allowing operators to configure a higher level of security. This master key is set when the **Card Type** selected is DESFire. A selection can then be made from the **Card Master Key** drop down field.

4. Left-click on the square “blue” node once to configure the sector/block contents. Refer the section Configuring a Sector / Block Detail [→ 165] of this user manual for information on this function.
5. Right-click on the Key corresponding to above node to configure the sectors read and write keys. Refer the section Configuring the Sector Keys [→ 168] of this user manual for further details.
6. Repeat the above steps until all the contents of sector and block that you wish encoded and the appropriate read and write keys have been defined.
7. Click **Save**.

Note:

If the **Format Before Encode** is unchecked, then any one of the following conditions may occur:

1. If the current encoding is using the same profile used in the previous encoding, the data in the DESFire smart card will be updated.
2. If the current profile is different from the profile used in the previous card encoding, and there is no **Application ID** overlap, the new profile configuration will be added to the existing profile in the DESFire smart card.
3. If the current profile is different from the profile used in the previous card encoding, and there is an **Application ID** overlap, the new profile configuration will be updated where the Application ID overlaps. If the overlapping application has a different configuration than the previous one then the encoding may fail.

See also

Configuring the Application / File Contents for Mifare DESFire Cards [→ 166]

9.2 Configuring the Sector / Block Contents

9.2.1 Configuring the Sector / Block Contents for Mifare Classic Cards

A 1k Mifare smart card incorporates 16 unique data sectors, and a 4k card supports up to 40. Each of these data sectors can then be split into three further data blocks. Depending upon the necessary requirements of a particular card, each block can potentially hold different data, such as an access card number, a cardholder's name, address or even an electronic purse amount. Of course, depending upon the size of the information blocks within a sector, it can be combined to hold larger amounts of data.

The following procedure explains how to configure the information to be encoded in a particular sector and block.

1. In the left hand column, left-click on the square "blue" node once, corresponding to the sector for which the data contents are to be specified.
2. Use the table on the right-hand side to specify the details for this sector as outlined in the following steps.
3. Specify the **Sector**. This should match the number of the node that was selected previously. The available sector numbers will differ depending on which card type is selected.
4. Select the **Block** where contents will begin to be written.
   - For Sectors 0-31 information can be written in blocks 0, 1, or 2.
   - For Sectors 32-39 information can be written in blocks 0-14
5. Select the **Offset** used.
6. Select the **Length** of the data to be written (in characters)
7. Select the **Output** format:
8. Select the **Access Control** format to be encoded on the card.
9. Select the **Data Type** to be encoded to the card sector (only for custom format selections)
10. Select or enter the **Data** to be encoded in the sector or block. The data entered will depend upon the format and data type selected in the previous two steps.
11. Repeat the above process until all sectors and all blocks that require encoded information have been completed.

9.2.2 Configuring the Application / File Contents for Mifare DESFire Cards

A DESFire 2k, 4k and 8k smart card incorporates 27 unique applications, each of which has a unique key and is locked by the key. Each of these applications can accommodate 32 files.(although the total length will be limited by the size of the smart card). Each file can have a length of maximum 4096 bytes and minimum of 32 bytes.

The following procedure explains how to configure the information to be encoded in each application:

1. Configure the **Application ID** (AID) by double-clicking above the key icon in the left –hand column.
   - AID number is an hexadecimal number. AID appears by default only for imported Bioscrypt profiles; and for manually created Bioscrypt profiles AID has to be configured manually. (AID, File ID, File size has to be configured manually by the user based on the configuration in the L1 Reader for Bioscrypt system. AID for SALTO system is not editable by the user as it is not a configurable parameter in SALTO)

Application ID cannot be empty and it cannot contain all zeros. The Application ID cannot be a duplicate within a profile. For an external system (SALTO system, Bioscrypt system) the Application ID cannot be configured from SiPass integrated.

2. To set the encryption key, right double-click on the key in the left hand column and set the key on the dialog that opens. To select a key, left-double-click on the key and select the options from the drop-down list.
3. Specify the User-defined Key number, right-click on the small key in the left hand column. The default key number is 1. The key number range is from 0-13.

User defined Key number for an external system (SALTO system and Bioscrypt system) cannot be set in SiPass integrated.

4. In the left-hand column, **Encrypted Communication Mode** can be checked.

SiPass supports the configuration of the communication mode between the ACC and the reader for DESfire EV1 smartcards. This communication mode can be plain or fully encrypted communication mode.

If the checkbox **Encrypted Communication Mode** is checked it will configure this particular application/file to use full encryption when the communication between the ACC and reader takes place. If it is not checked then plain mode will be used.

Some third party systems do not support fully encrypted communication mode.

5. In the left-hand column, left-click on the square “blue” node once, corresponding to the application for which the data contents are to be specified.
6. Use the table on the right-hand side to specify the details for this application as outlined in the following steps.
7. Specify the **Application** number. This should match the number of the blue node that was previously selected.
8. Select the **File** number to where the contents will begin to be written.

Changing the **Application ID** for the **Application** number 0 does not affect **File** number 0, but it affects other files the user may have configured within the **Application** number 0

9. Select the **Length of the data to be written.**
10. Select the **Output** format.
11. Select the **Access Control** format to the encoded on the card.
12. Select the **Data Type** to be encoded to the card application (only for custom format selections).
13. Select the **Data** to be encoded in the application or file. The data entered will depend upon the format and data type selected in the previous two steps.
14. Repeat the above process until all the applications and files that required encoded information have been completed.
15. Click **Verify**. Verify button is used to test encoding of the smartcard with the profile thus ensuring that the profile will fit in the DESFire smartcard. If the test encode is successful then a message is shown at the top of the screen of profile configuration dialog, together with the size of the DESFire card used for verification.

When you click the **Profile Viewer** on the Personal tab of the *Cardholder Dialog*, the verified profile configuration will be compared to the card used for verification. If the card size is less than that used for verification, then an error message will pop-up asking the user to use a larger size smart card.

9.2.3 Output Formats

The following table describes the various output formats.

Format	Description
ASCII	Standard for the code numbers used by computers to represent all the upper and lower-case Latin letters, numbers, punctuation, etc.
BCD	Binary Coded Decimal format
Date/Time	Date and time stamp format
Byte	Set of bits that represent a single character
Word	One complete word
Double Word	Two complete words
BCD Boolean	Binary Coded Decimal Boolean
Binary	Raw Binary data (e.g., data read from an external system). SiPass integrated will not apply any further formatting to the binary data. Will be encoded ‘as-is’.

9.2.4 Access Control Formats

The following table describes the various access control formats.

Format	Description
None	This sector/block may be used to hold custom information that does not relate to the access control system. For example, an electronic purse amount.
Wiegand 26-bit	Read Only field. This is enabled within a MIFARE sector and cannot be read with industry standard 26-bit format
Wiegand 37-bit	Read Only field. This is enabled within a MIFARE sector and cannot be read with industry standard 37-bit format
MIFARE Facility	Siemens own 36-bit encoded facility format
CSN	Card Serial Number. Only available for Sector 0

9.2.5 Data Types

The following table describes the various data types.

Format	Description
Boolean	True or false statement
Integer	Whole number only
String	A linear sequence of symbols (characters or words or phrases)
Custom Database Field	SiPass integrated custom cardholder field information.
External Type	The data that is received from the external system.

9.3 Configuring the Sector Keys

9.3.1 Configuring the Sector Keys for Mifare Classic Cards

To ensure that information within a smart card is always as secure as possible, the MIFARE Classic smart cards allow you to program protection or encryption keys for each sector. Without the knowledge of the 12-digit key, the information held within the sector cannot be interrogated or used.

To configure the security keys for each sector of the smart card:

▷ Ensure that you have the default factory keys handy before attempting to change a sector key on the smart card to a new value.

1. In the left hand column, left click on the “yellow” key corresponding to the sector for which the read and write keys are to be specified.
2. Click the **Keys** button at the bottom of the page.
3. Select **Mifare Key**.
4. Enter a name for the key into the **Key Name** field.
5. Enter the current existing or default key A into the **Key A** field.
   – You may need to consult your smart card dealer or manufacturer to determine what the sector default keys are when the smart cards are shipped.
6. Confirm key A by re-entering it into the **Confirm Key A** field.
7. Enter the current or existing default key B into the **Key B** field.
   – You may need to consult your smart card dealer or manufacturer to determine what the sector default keys are when the smart cards are shipped.
8. Confirm key B by re-entering it into the **Confirm Key B** field.
9. To overwrite the default sector key or existing sector key with a new one, check the **Overwrite the Sector Key** checkbox.
10. Enter the current key A into the **Key A** field. The key must be 12 digits in length, made up of any combination of numbers 0 to 9, and upper case letters A to F.
11. Confirm Key A by re-entering it into the **Confirm Key A** field.
12. Enter the Key B into the **Key B** field. The key must be 12 digits in length, made up of any combination of numbers 0 to 9, lower case letters a to f, and upper case letters A to F.
13. Confirm Key B by re-entering it into the **Confirm Key B** field.
14. Select the access conditions that exist for each block within this sector:
15. Click **Save**.

Please note that once a key is created and saved, it can be configured to multiple sectors.

9.3.1.1 Access Conditions

The table below explains the possible access conditions.

Access Conditions	Description
All functions with KA and KB	The sector and block can be written to, and read using both keys A and Key B.
Read with KA, Write with KB	Reading the contents of the sector and block will be done using key A only. Writing/Encoding information to the sector and block will be done using Key B only.
Read only with KA and KB	The sector cannot be written to, and can only be read using both keys A and Key B.
Read / subtract with KA, Write / add with KB	Reading information or subtracting value from the contents of the sector and block will be done using key A only. Writing information or adding electronic value to the sector and block will be done using Key B only.
Read / subtract with KA or KB	Read information or subtracting electronic value from the sector and block can be performed with Key A or Key B.
Read / Write with KB	Reading the contents or Writing new contents to the sector and block will be done using key B only.
Read Only KB	The sector cannot be written to, and can only be read using Key B.
Blocked	The sector and block cannot be read or overwritten.

9.3.2 Configuring the Sector Keys for Mifare DESFire Cards

The Mifare DESFire cards allow you to program security keys for each application of the card profile. The Mifare DESFire keys can use three types of encryption namely DES(16 digits), 3DES(32 digits), and AES(32 digits). Without the knowledge of the 32-digit key, the information held within the application cannot be interrogated or used.

To configure the security keys for the card profile:

▷ Ensure that you have the default factory keys handy before attempting to change the security key on the smart card to the new value.

1. In the left-hand column, click on the ‘yellow’ key corresponding to the application for which the security key is to be specified.
2. Click the **Keys** button at the bottom of the dialog.
3. Select **Desfire Key**.
4. Enter a name for the key into the **Key Name** field.
5. Select a type of **Encryption** from the drop-down.
6. Enter a unique key into the **Read/Write Key** field.
7. Re-enter the same unique key into the **Confirm Read/Write Key** field.
8. Click **Save**.

To overwrite the default or existing security key:

1. Select the **Key Name** that is to be overwritten.
2. Check the **Overwrite the Application Key** checkbox.
3. Enter the new key into the **Read/Write Key** field.
4. Re-enter this key into the **Confirm Read/Write Key** field.
5. Click **Save**.

Note: To enable read only (not write/encoding) of the security key, repeat the steps above, and enter a new read key into the **Read Key** and **Confirm Read Key** field, and click **Save.**

9.4 Configuring a custom access control format

No two facilities should share exactly the same access details. Of course this opening statement is almost a logical statement. Because of this, many corporations derive their own custom formats to use at facilities in which they originally installed their equipment. SiPass integrated allows you take advantage of this situation and upgrade you base technology in unison, but still use the old custom format.

▷ Ensure that you have the custom format details, before you attempt to replicate such a format using SiPass integrated, this will save a lot of time and effort.

1. Click the **Custom Format** button located at the bottom of the *Profile Configuration* dialog.
2. Enter name for the format into the **Data Format Name** field.
3. Enter the length of the format (number of characters) into the **Wiegand length** field.
4. Enter the **Start** and **End** bits in the custom string that will hold the company (site) information. Use 0,0 if no company bits will be used in the format.
5. Enter the **Start** and **End** bits in the custom string that will hold the facility information. Use 0,0 if no facility bits will be used in the format.
6. Enter the **Start** and **End** bits in the custom string that will hold the card number.
7. Enter the **Start** bit, **End** bit, and Position to be used for an even parity check.
8. Enter the **Start** bit, **End** bit, and Position to be used for an odd parity check.
9. Choose **Save** to save the custom card format.
10. On saving the DESFire profile, a *Test encode dialog* opens. The Test encode dialog allows the user to check if the profile can be encoded within a card. Click Yes to test fir encode. Click No to exit the dialog.

The following provides an example of a custom format called Siemens 10-bit:

Bit	1	2	3	4	5	6	7	8	9	10
Info	P	S	S	F	F	C	C	C	C	P

Where:

P = Parity, S = Company, F = Facility, C = Card Number

Therefore, the format configuration is:

Data Format Name: Siemens 10-bit

Wiegand Length: 10

Company Start Bit: 2

Company End Bit: 3

Facility Start Bit: 4

Facility End Bit: ` 5

Card Number Start Bit: 6

Card Number End Bit: 9

A DESFire card can have only one SALTO application per card for a given SALTO system. Hence every profile created by the SiPass can have only one SALTO binary data. The following points should be considered while configuring a DESFire card with SALTO.

1. The keys used for the application that has SALTO binary data should be provided by the SALTO system.
2. File ID should always be 1.
3. Any application ID can be used for the SALTO binary data. It is recommended that SALTO binary data should be atleast 288 bytes in size.

9.5 Assigning a Profile

Once you have configured your card profiles for different purposes, they must be assigned to a cardholder before a card can be encoded and issued to that cardholder. This assignment can be conducted through two different mechanisms, by either assigning the profile to a card template, or assigning the profile directly to the cardholder themselves.

9.5.1 Assigning a Profile to a Card Template

A profile can be associated with a card template when you create that template in SiPass integrated. This method ensures that all cardholders with the same type of cards will end up with the same smart card configuration and basic setup.

▷ Ensure that you have configured your smart card profiles, including read / write keys, and information that will be written to each sector.

1. Create or edit and existing card template as described in the *Photo ID and Graphics* chapter.
2. Click once on the **Smart Card** icon located on the **Drawing** toolbar.
3. Place the mouse pointer over the card template and click the left mouse button once.
4. Using the selection list available in the *Smart Card Profile Selection* dialog, select the profile that you wish to use for the card template currently being created.
5. Click **OK**. The dialog will now disappear and the smart card icon will appear on the card template.
6. Complete the card template as required by adding further graphics, database fields etc.
7. Ensure that you save the card template will a logical name before exiting the *Card Template design* window.
8. When printing a card using a card template from the *Cardholder* dialog, using the GEMPLUS GCI680 encoding module in a card printer, the profile and appropriate smart card contents will now be written to the smart card itself.

9.5.2 Assigning a Profile to an Individual Cardholder

A profile can be associated with an individual cardholder and this profile can be used to encode the card directly on a one-on-one basis when cardholders are issued a card.

▷ Ensure that you have configured your smart card profiles, including read / write keys, and information that will be written to each sector.

1. Open the *Cardholder* dialog by choosing **Cardholder** from the **Operation** toolbar.
2. Create a new cardholder or open an existing account for the cardholder who will be issued with a smart card.
3. Ensure all the details for that cardholder have been completed.
4. Click once on the *Personal* tab in the *Cardholder* dialog.
5. Select the appropriate smart card profile from the **Profile** drop-down list located at the bottom at the dialog.
6. Click **Save**.

⇨ When issuing a card to a Cardholder, the profile and appropriate smart card contents will now be written to the smart card itself when a card is presented at the smart card encoder connected to the SiPass Client and the **Encode Card** button is pressed.

9.6 Reading a card with the Profile Viewer

With the Profile Viewer you can place a card on your smart card reader, select the appropriate profile and then read back the data on the card.

1. Select **Operation > Profile Viewer**.
2. Select a profile name. Depending on the profile that is selected, the fields displayed in the *Profile Viewer dialog* changes accordingly.
3. Select **Raw Data** or **User Format**.
   - **Raw Data** is just the data on the card, whereas **User Format** presents the data in the profile defined format.
4. Ensure the card is placed on your smart card reader and click **Read Card**.
5. Select different sectors to display the contents of that sector.
6. Click **Close**.

9.7 Configuring a Smart Card Printer

To ensure that you get the best results possible, SiPass integrated allows you to configure the settings for each of the different printer types available. This includes card printers.

▷ Ensure that you have configured your smart card printer and driver correctly.

1. From the **File** menu, select **Print Setup** to show the *Setup Global Printers* dialog.
2. Select the *Card Printer* tab.
3. If you wish to nominate a card printer other than the one displayed as the current printer, choose **Select Printer** to open the *Print Setup* dialog and display a list of appropriate printers.
4. Select the printer type from the **Printer Type** drop-down list.
5. Select the com port to be used to transmit encoding details, by selecting the appropriate port from the **Encoding COM Port** drop-down list.
6. To encode the smart card at the same time as printing ensure that the **Encode Smart card when printing** checkbox has been enabled.
7. Click **OK**.

9.8 Configuring a Card Reader (Smart card or Enrollment)

To extract information from a card, you have to be able to read it. When assigning a card to a new employee, you may need to determine the card number and other important information. The information from the card reader dialog is stored in the local registry so each SiPass integrated client will have its own reader configuration settings.

▷ Ensure that you have installed the drivers required for your readers. The GEMPLUS readers require a driver to be installed which is included with your SiPass integrated CD. You will need to unzip the file and install all drivers before proceeding.

1. From the **Options** menu, select **Enrollment Reader Configuration**.
2. Click the **Add** button to bring up a dialog where you can select a reader to be configured.

DESFire encoding/reading is supported only for OmniKey CardMan 5 ×21 readers.

3. Select a reader and click **OK**.

To delete a selected reader; select the reader from the **Select Type** drop down list, and click **Remove**.

4. The address of the reader appears in the **Reader Address** field by default.
5. If the selected reader is to be used only for Card Reading, tick the **Reading** checkbox.
6. If this reader is to be used for card reading and encoding, tick the **Encoding** checkbox. The **Reading** checkbox will be selected automatically.
7. Select the profile to be used for reading the card from the **Profile Name** drop-down list.
8. If you have connected a smart card reader, enter the sector and block to be read into the **Sector (0-39)** and **Block (0-14)** fields.
9. If the reader is not connected by USB, select the serial port to which the reader has been connected from the **Port Name** drop-down list.
10. If the reader is Wiegand or Clock & Data select the card format to be read using the **Card Format** drop-down list and the reader supply voltage (or source) from the **Voltage** drop-down list.
11. Choose **OK**.

9.8.1 Reader Types Supported

The list below outlines the supported enrolment readers and Smart Card Encoders:

- CERPASS Registration Reader
- Siemens RS485 Reader
- Profile Reader – HID6055B (Smart Card Profile)
- Profile Reader - GEMPLUS GCI680 (Smart Card Profile)
- Profile Reader - GEMPLUS GEX332 (Smart Card Profile)
- Profile Reader – OmniKey CardMan 5X21 (Supporting Mifare Classic and Mifare DESFire smart cards)
- USB Reader Interface – Wiegand (Various Formats)
- USB Reader Interface – Clock and Data (Various Formats)
- Siemens AR6201 – MX (Supports Mifare Classic cards)
- Siemens Proximity Reader (Supporting Mifare Classic and Mifare DESFire smart cards)

10 CCTV

CCTV is a module of the SiPass integrated access control software. It allows SiPass integrated to communicate with CCTV equipment using a high level interface. This interface allows control and manipulation of the equipment connected to the CCTV system, such as cameras, monitors, and auxiliary devices.

The CCTV high level interface allows presets, patterns and sequences to be recorded in SiPass integrated, and viewed and controlled using the SiPass integrated GUI. This provides the access control and security operator with a seamless GUI interface to the CCTV system.

The CCTV HLI (High Level Interface) is compatible with a range of CCTV systems. Refer to the SiPass integrated Release Notes for more information regarding the supported CCTV HLIs.

The SiPass CCTV Module allows you to control your CCTV system using the same GUI that you use to control your access control and security system. This type of integration means that your security operators no longer need to switch between applications to perform their jobs. From SiPass integrated alone an operator has the ability to view an alarm, automatically view the CCTV images at the alarm location, and record his or her comments regarding the alarm all from one workstation.

10.1 CCTV Configuration Summary

The following list provides a summary of the configuration and setup for the SiPass CCTV module.

- Ensure that Windows XP and the corresponding service pack have been installed on all PCs in the SiPass integrated access control and security network.
- If your access control and security network is to be configured using more than one PC, ensure that all machines are connected together using an appropriate communications protocol, such as the internet protocol TCP/IP.
- Ensure that your wiring of the CCTV system does not exceed the recommended distances for the communications taking place (e.g. RS232 comms should not exceed 10m). If you need to introduce communications over longer distances you should include line amplification.
- Install the appropriate SiPass integrated software onto each PC in your access control and security network, ensuring that exactly the same version of SiPass integrated is used for all installed components.
- Ensure that the CCTV system architecture has been planned in advance.
- Ensure that you have programmed the CCTV controller using the CCTV system Administration software and that all CCTV devices have been connected to the appropriate equipment.
- Ensure that the CCTV controller has been connected to the SiPass integrated PC where the CCTV bus service has been installed.
- Program and configure the CCTV Bus and CCTV Controller using SiPass integrated.
- Program the necessary cameras, monitors, auxiliary devices, and groups of these components in SiPass integrated.
- Configure the necessary presets, patterns, and sequences using SiPass integrated.
- Program any CCTV-related event tasks using SiPass integrated.

10.2 Using CCTV Controls

The SiPass CCTV window looks and operates like a standard Windows XP program. The tools provided by SiPass integrated to operate and configure the CCTV equipment have been professionally designed to provide you with access to the functions you need to perform all CCTV related Tasks.

10.2.1 CCTV Camera Controls

SiPass integrated allows you to control and manipulate the PTZ cameras in your CCTV system. This means that without leaving the SiPass integrated environment, you can move a PTZ camera in a horizontal or vertical direction using the on-screen mouse pointer, change the speed of this movement, zoom in and out, change the brightness of the images and control the focus.

Using the on-screen mouse pointer

When using the SiPass CCTV on-screen video display, the mouse pointer can be used to control the movement of a PTZ camera.

You can control the horizontal and vertical movement of the camera by holding down the left mouse button and moving the mouse in the same direction that you want the camera to move. The mouse must be in the active CCTV window.

When the camera reaches the desired position, release the left mouse button and the camera will stop moving. This allows the SiPass CCTV operator to view images in any direction for which the camera is physically able.

Zoom In

The Zoom In control allows you to use the zoom in functionality of a PTZ camera. By placing the mouse pointer over the Zoom In button and holding down the left mouse button, the camera will change its focal length and move in toward the object (enlarge the objects that are farthest from the camera's view). The camera will stop zooming when the mouse button is released.

The "Z" key on your keyboard can be used to Zoom In instead of using the mouse. You may also use this key to simultaneously Zoom In when moving the camera using on-screen mouse pointer.

Zoom Out

The Zoom Out control allows you to use the zoom out functionality of a PTZ camera. By placing the mouse pointer over the Zoom Out button and holding down the left mouse button the camera will change its focal length and move away from the object (providing a wider image from the camera's view). The camera will stop zooming when the mouse button is released.

The "X" key on your keyboard can be used to Zoom Out instead of using the mouse. You may also use this key to simultaneously Zoom Out when moving the camera using on-screen mouse pointer.

Open Iris

The Open Iris control allows you to control the size of the lens aperture and the amount of light passing through the lens. As the iris is opened, the CCTV image appears lighter. By placing the mouse pointer over the Open Iris button and holding down the left mouse button, the camera will begin to open the lens aperture, making the CCTV image brighter. The iris will stop opening when the mouse button is released.

Close Iris

The Close Iris control allows you to control the size of the lens aperture and the amount light passing through the lens. As the iris is closed, the CCTV image appears darker. By placing the mouse pointer over the Close Iris button and holding down the left mouse button, the camera will begin to close the lens aperture, making the CCTV image darker. The iris will stop closing when the mouse button is released.

Focus Near

The Focus Near control allows you to adjust the camera lens so that images close to the camera become more sharply defined. By placing the mouse pointer over the Focus Near button and holding down the left mouse button, the camera will begin to change the lens focal length, making the images closer to camera appear more sharply defined. The re-focusing will stop when the mouse button is released.

Focus Far

The Focus Far control allows you to adjust the camera lens so that images farther away from the camera become more sharply defined. By simply placing the mouse pointer over the Focus Far button and holding down the left mouse button, the camera will begin to change the lens' focal length, making images further away from the camera appear more sharply defined. The re-focusing will stop when the mouse button is released.

Pan / Tilt Speed

The Pan / Tilt Speed control allows you to control the speed at which the camera can be moved. By placing the mouse pointer over the Close Iris button and clicking the left mouse button once, a speed menu will appear, displaying the following options:

- **Variable**

The variable speed control allows you to select the speed of the camera's pan and tilt functionality in relation to the mouse pointer's on-screen position. The closer the CCTV mouse pointer control is to the center of the screen the slower the movement of the camera. The closer to the edge of the on-screen picture the CCTV mouse pointer is, the faster the movement of the camera.

- **Slow**

The slow control fixes the pan and tilt operation of the camera to a slow speed. When using the on-screen mouse pointer to move the position of the camera, the movement will be slow.

- **Medium**

The medium control fixes the pan and tilt operation of the camera to a medium speed. When using the on-screen mouse pointer to move the position of the camera, the movement will be of medium pace.

- **Fast**

The fast control fixes the pan and tilt operation of the camera to a fast speed. When using the on-screen mouse pointer to move the position of the camera, the movement will be quick.

- **Turbo**

The turbo control fixes the pan and tilt operation of the camera to a turbo speed. When using the on-screen mouse pointer to move the position of the camera, the movement will be very quick.

Please note that the camera speeds do not affect the operations of the SIMATRIX CCTV system.

Screen Size

The Screen Size control allows you to enlarge the size of the on-screen CCTV display. By placing the mouse pointer over the Screen Size button and clicking the left mouse button once, the on-screen CCTV display will become enlarged. Once enlarged, you only need to click on the same button again to return to the normal display.

Video Source

The Video Source control allows you to select which video card will be the source of on-screen images. By placing the mouse pointer over the Video Source button and clicking the left mouse button once, a menu will appear allowing you to select the video source which to display. This function can be used when you have connected multiple video cards to your PC.

10.3 Programming SiPass integrated for CCTV

In order for the SiPass CCTV module to function correctly, SiPass integrated must be programmed with the appropriate data. This includes programming a CCTV bus, CCTV Unit, cameras, monitors, auxiliary camera devices, and configuring groups of these CCTV components.

10.3.1 Configuring the CCTV Bus

The communications channel used by SiPass integrated to send and receive messages to and from the CCTV system uses a specialized channel and protocol interpreter called a bus. The following section outlines the procedure used to add and configure this bus using SiPass integrated.

▷ Ensure you have installed the SiPass Server and configured the CCTV Bus Service.

▷ Ensure that you have assigned the correct operator privileges to the operator who will be configuring the CCTV system using SiPass integrated.

▷ Ensure that you have programmed the CCTV controller with the correct information, using the CCTV System Administration software.

1. Choose the **Components** button from the **System** toolbar or menu.
2. Select the Server Name by double clicking on it.
3. Choose the **New Bus** button.
   ⇨ A menu will appear displaying a list of bus options.
4. Choose **CCTV**.
   ⇨ A new unnamed CCTV bus will appear in the Server tree.
5. Enter the name of the Bus Driver Service into the **Bus Name** field. The name you assign to the CCTV bus in this field must match the name you gave this same CCTV bus during installation.
   – SiPass integrated cannot be used to control the CCTV equipment if the Bus name entered in the *Components* dialog is different to the name entered during installation.
6. Select an alarm class, if required, from the **Alarm Class** drop down list. You must assign an alarm class to a unit before it can be represented on a site plan.
7. Select the protocol used by the CCTV controller from the **CCTV Command Set** drop-down list. The supported CCTV protocols include Pacom, Pelco and SIMATRIX. There are other generic CCTV protocols that are supported. For information on how to configure a Generic CCTV Bus, please refer the section Configuring a Generic CCTV [→ 186].

8. Select the communications Baud Rate from the **Baud Rate** drop-down list. This baud rate would normally be 9600.
9. Select the serial communications port to which the CCTV system will connect from the **Port** drop-down list. This port would normally be COM2, depending upon other devices connected to the PC.
10. If necessary, and only in the event that your CCTV system requires you to do so, enter the CCTV Keyboard ID, into the **User ID** field. This will normally be a four-digit ID number.
    – SiPass integrated cannot be used to control the CCTV equipment if the keyboard ID does not match the ID configured using the CCTV System Administration software.
11. Click the *CCTV Bus Parameters* tab.
12. If you wish to log all CCTV bus activity to a permanent data file, select the **Log commands to file** check box. The log file will be stored in the following location – “c:\Temp\BussLog.txt”.
    – Depending upon the amount of CCTV bus activity, the overall system performance may be affected if this log to file option is selected. It is recommended that this option only be selected for diagnostic purposes.
13. Choose **Save** and then stop and restart the CCTV Bus Service.

10.3.2 Configuring the CCTV Controller Unit

The main component of a CCTV system is the CCTV controller or processor unit. This device controls the operation of each camera, monitor and auxiliary device in the system, through the use of a Switch box often referred to as a Matrix. SiPass integrated uses a high level interface to send commands to and receive messages from this CCTV Controller.

However, each type of controller communicates using a different protocol, therefore the controller needs to be programmed in SiPass integrated, so communications can be successfully performed.

▷ Ensure that you have configured the CCTV Bus in SiPass integrated, and met the pre-requisites for configuring this bus.

▷ Ensure that the SiPass Server is running and operational.

▷ For **Generic CCTV Switcher** – Ensure that SiPass CCTV Generic Bus Service is running parallel and operational.

▷ For **default CCTV Switcher** – Ensure that SiPass SimatrixBus service and SiPass PacomBus service are running and operational

1. Choose the **Components** button from the **System** toolbar or menu.
2. Select the **Server Name** by double clicking on it.
3. Select the **CCTV** bus.
4. Choose the **New Unit** button.
   ⇨ A new unit will appear connected to the CCTV bus and a *CCTV Unit* tab will also appear.
5. Enter a name for the CCTV controller into the **Unit Name** field.
6. Select the CCTV Controller from the **Unit Type** drop-down list.
7. Enter a description for the CCTV Controller Unit in the **Description** field.
8. Click **Save**.

10.3.3 Programming a Camera

CCTV cameras are the basis of the CCTV system. SiPass integrated allows you to program either a fixed or a PTZ (Pan/Tilt/Zoom) type camera. The following section outlines the procedure used to program a CCTV camera in SiPass integrated.

1. Choose the **Components** button from the **System** toolbar or menu.
2. Select the Server Name by double clicking on it.
3. Double-click on the name of the CCTV Bus.
   ⇨ A new tree branch will appear displaying the CCTV Unit previously created.
4. Select the CCTV Unit by clicking on it once.
5. Choose the **New Point** button.
   ⇨ A menu will appear displaying a list of CCTV point options.
6. Choose **Camera**. A new camera will appear connected to the CCTV Unit and the *CCTV Point* tab will appear.
7. The **Type** field is populated by default.
8. Enter a unique name for the camera into the **Name** field. You may enter up to 40 characters in any combination of upper and lower case letters, numbers, periods and spaces.
9. Enter the ID number of the camera into the **Description** field. This point number must be exactly the same as the ID number configured in the CCTV system for the camera.
10. Select the *Camera* tab.
11. Select the camera type from the **Sub-Type** drop-down list. The types of cameras that can be configured in SiPass integrated include:
    - **PTZ Camera**:
      A PTZ camera is a camera that can be controlled from a remote location to provide vertical and horizontal movement, focus and zoom capabilities.
    - **Fixed Camera**:
      A fixed camera is a camera that cannot be controlled from a remote location and once mounted is fixed in direction unless manually moved.
12. If you have selected PTZ Camera, select the controls that are associated with the specific camera by selecting the appropriate check boxes in the Camera Controls area.
    - **Pan, Tilt, Zoom**:
      This option indicates that the camera has a motorized mechanism that can be used to remotely control the vertical and horizontal position of the camera and also provides a zoom in and zoom out capability.
    - **Iris Control**:
      This option indicates that the camera has a motorized mechanism that can be used to remotely adjust the lens aperture and therefore, the amount of light passing through the lens.
    - **Focus Control**:
      This option indicates that the camera has a motorized mechanism that remotely allows objects at various distances to be sharply defined.
13. Enter the number of presets that can be stored on the camera into the **Maximum Presets** field (PTZ type cameras only).
14. Select an Alarm Class for this camera from the **Alarm Class** drop-down box.

15. Enter the Alarm Number assigned to this camera by the CCTV Administration Software into the **Logical Alarm No.** field. This will allow SiPass integrated to respond to alarms registered at this camera by the Switcher.

The Alarm section is enabled only for cameras on DT4 Pelco 9760 CCTV units (DT4).

16. Click **Save**.

10.3.4 Programming a Monitor

CCTV monitors allow a security operator to visually observe the pictures captured by the system's cameras. This section outlines the procedure used to program a CCTV monitor in SiPass integrated.

SiPass integrated allows you to control image viewing on both dedicated CCTV monitors and the built-in SiPass CCTV monitor (using the SiPass GUI).

1. Choose the **Components** button from the **System** toolbar or menu.
2. Double-click on the name of the CCTV Bus.
   ⇨ A new tree branch will appear displaying the CCTV Unit previously created.
3. Select the CCTV Unit by clicking on it once.
4. Choose the **New Point** button. A menu will appear displaying a list of CCTV point options.
5. Choose **Monitor**.
   ⇨ A new monitor will appear connected to the CCTV Unit and the CCTV Point tab will also appear.
6. Enter a unique name for the monitor into the **Name** field. You may enter up to 40 characters in any combination of upper and lower case letters, numbers, periods and spaces.
7. Enter a description for the monitor in the **Description** field. This may include the location of the monitor.
8. Enter the ID number of the monitor into the **Point Number** field. This point number must be exactly the same as the ID number configured in the CCTV system for the monitor.
9. Choose **Save**.

10.3.5 Programming an Auxiliary Device

Many optional devices can be fitted to CCTV cameras. For example, heaters, wind screen wipers and other camera enhancement equipment can be fitted to a camera to enhance its usability. The following section outlines the procedure used to program an auxiliary CCTV camera device in SiPass integrated.

1. Choose the **Components** button from the **System** toolbar or menu.
2. Double-click on the name of the CCTV Bus.
   ⇨ A new tree branch will appear displaying the CCTV Unit previously created.
3. Select the CCTV Unit by clicking on it once.
4. Choose the **New Point** button.
   ⇨ A menu will appear displaying a list of CCTV point options.
5. Choose the *Auxiliary* tab.
   ⇨ A new auxiliary CCTV camera device will appear connected to the CCTV Unit, and the CCTV Point tab will appear.
6. Enter a unique name for the auxiliary CCTV camera device into the **Name** field.
7. Enter a description for the monitor in the **Description** field. This may include the location of the monitor.
8. Enter the ID number of the auxiliary device into the **Point Number** field. This point number must be exactly the same as the ID number configured in the CCTV system for the monitor.
9. Select the *Auxiliary* tab.
10. Select the camera to which the auxiliary device is connected from the **Camera** drop-down list.
11. Click **Save**.

10.3.6 Programming an Alarm Point

This section outlines the procedure used to program the CCTV Alarm Point.

1. Choose the Components button from the **System** toolbar or menu.
2. Double-click on the name of the CCTV Bus.
   ⇨ A new tree branch will appear displaying the CCTV Unit previously created.
3. Select the CCTV Unit by clicking on it once.
4. Choose the **New Point** button. A menu will appear displaying a list of CCTV point options.
5. Choose **Alarm Point**.
   ⇨ A new alarm point will appear connected to the CCTV Unit and the CCTV Point tab will also appear.
6. Enter a unique name for the alarm point into the **Name** field. You may enter up to 40 characters in any combination of upper and lower case letters, numbers, periods and spaces.
7. Enter a title for the alarm point in the **Title** field.
8. Enter the ID number of the alarm point into the **Point Number** field. This point number must be exactly the same as the ID number configured in the CCTV system for the alarm point.
9. Enter a description for the alarm point in the **Description** field. This may include the location of the alarm point.
10. Click **Save**.

10.3.7 Grouping Cameras and Monitors

SiPass integrated allows CCTV components to be grouped together. These groups are used during configuration and operation processes.

Grouping components also allows you to partition the control that operators have over CCTV points.

1. Choose the **Point Group** button from the **Program** toolbar or menu.
2. Choose **Add Members**.
3. Select the Group Type from the **Group Type** drop-down list. To create a group of CCTV monitors or CCTV cameras choose either **Monitor Group** or **Camera Group** from the list.
4. Select the name of the monitor or camera to be added to the group from those displayed in the available list.
5. Choose **Add >**.
   ⇨ The selected camera or monitor will be added.
6. Repeat Steps 5 and 6 until all members have been added to the **Selected** list.
7. Choose the **OK** button.
8. Click **Save**.

10.4 Configuring CCTV

Once the CCTV components have been programmed in SiPass integrated, you can start configuring the CCTV system for operation. SiPass integrated allows you to configure Patterns, Presets, Sequences, and to trigger CCTV events. These configuration options allow total control over the CCTV system from within the SiPass GUI itself.

10.4.1 Creating a camera preset

SiPass integrated allows you configure multiple camera-preset definitions. This means that from SiPass integrated you can program a defined, recallable position for any PTZ camera programmed in the system.

A preset allows the SiPass operator to quickly recall a pre-defined view through a motor driven camera and display this on a monitor for observation. A preset can also be the target of an event triggered task, whereby a certain event automatically switches a particular camera view on, and moves the camera to the SiPass programmed preset position. The following procedure outlines the method used to configure presets from SiPass integrated.

▷ Ensure that all the CCTV equipment has been configured in SiPass integrated and that the Matrix Switcher and all CCTV equipment are operational.

▷ Ensure that the SiPass Server and SiPass CCTV Bus services are running.

1. Choose **CCTV** from the **Program** toolbar or menu.
2. Select a specific Monitor Group or the **All Monitors** option from the **Monitor Group** drop-down box.
3. Select the monitor that will be used to display the CCTV images during the configuration process. Then choose the **Preset** button.
4. Select a specific Camera Group or the “**All Cameras**” option from the **Camera Group** drop-down box.
5. Single click or select on the name of the PTZ camera for which the Preset is to be configured from the **Camera** list.

6. Using the CCTV tools provided, move the camera and select the exact position that you wish to configure as a preset.
7. Select the Preset Index position for that camera from the **Preset Name** drop-down box.
8. Remove the existing description and enter a unique name for that preset into the **Preset Name** drop-down box.
9. Click **Save**.

10.4.2 Creating a camera pattern

SiPass integrated allows you configure multiple CCTV camera patterns. This means that from SiPass you can program a defined, moveable single camera routine for any PTZ camera programmed in the system.

A pattern allows the SiPass operator to quickly recall a pre-defined view through a motor driven camera and display this on a monitor for observation. A Pattern can also be the target of an event triggered task, whereby a certain event automatically switches a particular camera view on, and automatically shows the pattern on the configured CCTV monitor.

▷ Ensure that all the CCTV equipment has been configured in SiPass integrated and that the Matrix Switcher and all CCTV equipment is operational.

▷ Ensure that the SiPass Server and SiPass CCTV Bus services are running.

1. Choose **CCTV** from the **Program** toolbar or menu.
2. Select a specific Monitor Group or the “All Monitors” option from **the Monitor Group** drop-down box.
3. Select the monitor that will be used to display the CCTV images during the configuration process, then choose the **Pattern** button.
4. Select a specific Camera Group or the “All Cameras” option from the **Camera Group** drop-down box.
5. Single click on the name of the PTZ camera for which the Pattern is to be configured, from the **Camera** list.
6. Enter a unique name for the Pattern in the **Pattern Name** field, located near the top of the tab.
7. Press the **Record** button to begin recording your pattern. Patterns are a set of commands that govern the movement of a specific camera. For this reason, it is recommended that a Pattern always begin and end with a pre-defined Preset location so that the x-y co-ordinates are always the same each time the pattern starts and finishes. To select a Preset simply double click on the name of this Preset in the **Presets** list.
8. Using the CCTV tools provided, move the camera in the desired fashion for the pattern. This may include any combination of positioning the camera using horizontal or vertical movement, zooming, and focusing.
9. Once completed, choose **Stop**.
10. Click **Save**.

10.4.3 Creating a camera sequence

SiPass integrated allows you configure multiple CCTV camera sequences. This means that from SiPass integrated you can program a defined series of patterns, presets, and dwells (stop or pause times) for multiple cameras in the CCTV system.

This sequence can then be saved and replayed on any one of more monitors in the CCTV system.

▷ Ensure that all the CCTV equipment has been configured in SiPass integrated and that the Matrix Switcher and all CCTV equipment is operational.

▷ Ensure that the SiPass Server and SiPass CCTV Bus services are running.

1. Choose **CCTV** from the **Program** toolbar or menu.
2. Select a specific Monitor Group or the “All Monitors” option from the **Monitor Group** drop-down box.
3. Select the monitor that will be used to display the CCTV images during the configuration process and Then, choose the **Sequence** button.
4. Enter a unique name for the Sequence in the **Sequence Name** field, located near the top of the tab.
5. Select a specific Camera Group or the “All Cameras” option from the **Camera Group** drop-down box.
6. Select a camera from the **Camera** drop-down box.
7. Add the desired components to the sequence, by doing the following:
8. Select a Preset from the **Available Preset** list and then choose the **Add** button to add this preset to the sequence.
9. Select a Pattern from the **Available Patterns** list, and then choose the **Add** button to add this pattern to the sequence.
10. Select a new camera to which the displayed view will switch from the **Switch To Camera** drop-down list. Then choose the **Add** button to add this to the sequence.
11. Repeat the previous step until all sequence components have been added to the **Selected Action** box.
12. Select the exact order in which each action will be performed, by either promoting or demoting its position in the **Selected Action** list. You use the buttons provided to demote or promote the action.
13. To change the delay time in seconds, double-click on the name of the action in the **Selected Actions** list. Then enter a new time into the **Delay (s)** column. This delay time specifies the amount of time before the next action in the list is executed.
14. Once all the actions have been included in the sequence and the delay times for each action configured, do one of the following to save it:
15. Click **Save**.
16. Preview the sequence to ensure that it is correct and accurate.

10.5 Configuring a Generic CCTV

This functionality deals with the ability to install a CCTV generic bus in SiPass integrated.

A prime function that supports this feature is the COMMAND MAPPING functionality. This feature allows the operator to create CCTV command sets in SiPass integrated, which can be communicated to any generic CCTV system to in order to connect to it and control it.

Multiple generic CCTV services are supported within the SiPass integrated server.

One generic CCTV service can connect to more than one CCTV switcher.

This functionality supports the ability to configure Host Based Event Tasks for user defined commands. It also supports user-defined syntax and the input of additional parameters.

The CCTV generic bus also supports event notification (e.g., Camera Video Loss, Unit Communication Loss, Bus Down / up, etc.)

DETAILS OF **COMMAND MAPPING**

This functionality allows the system integrator to configure the command format sent to the CCTV switcher based on the protocol of the switcher.

1. It allows the operator to modify the command format sent to the CCTV switcher based on the protocol of the switcher.
2. It allows the operator to add in new command sets to the CCTV switcher according to requirements.
3. It allows the user to send plain text through the RS232 connection unit, to the switcher. Note: The connection unit does not have to be the switcher. It can be any connection unit that supports the RS232 protocol.

10.5.1 Prerequisites of Generic CCTV Configuration

- The generic CCTV configuration requires that a remote PC should be available, installed with Microsoft Windows XP and the corresponding service pack. The CCTV generic bus service will be installed on this remote PC.
- The procedure to install the same is detailed in the section that follows.

Installing the Generic CCTV Bus Service

- The SiPass integrated software should be installed on this remote PC, with options for the Generic CCTV bus selected during the installation process.

See also

CCTV Configuration Summary [→ 175]

10.5.2 Programming SiPass integrated for Generic CCTV

In order for the SiPass CCTV module to function correctly, SiPass integrated must be programmed with the appropriate data. This includes programming a CCTV bus, CCTV Unit, cameras, monitors, auxiliary camera devices, and configuring groups of these CCTV components.

10.5.2.1 CCTV Bus and Parameter Configuration

The communications channel used by SiPass integrated to send and receive messages to and from the CCTV system uses a specialized channel and protocol interpreter called a bus. The sections that follow will explain how to configure a CCTV bus, and its parameters.

Configuring the Genric CCTV Bus

Operator can configure CCTV bus parameters for default as well as generic CCTV types in SiPass integrated. The following section outlines the procedure used to add and configure a generic CCTV bus.

10.5.2.2 Configuring the Generic CCTV Bus

Operator can configure CCTV bus parameters for default as well as generic CCTV types in SiPass integrated. The following section outlines the procedure used to add and configure a generic CCTV bus.

▷ Ensure you have installed the SiPass Server and configured the CCTV Bus Service.

▷ Ensure that you have assigned the correct operator privileges to the operator who will be configuring the CCTV system using SiPass integrated.

▷ Ensure that you have programmed the CCTV controller with the correct information, using the CCTV System Administration software.

1. Choose the **Components** button from the System toolbar or menu.
2. Select the Server Name by double clicking on it.
3. Choose the **New Bus** button.
   ⇨ A menu will appear displaying a list of bus options.
4. Choose **CCTV**.
   ⇨ A new unnamed CCTV bus will appear in the Server tree.
5. Enter a name of the Generic Bus Diver service into the **Bus Name** field.

The name of the generic CCTV bus does not need to match the name given to the same CCTV bus during installation. However, ensure that the **Generic Bus** installation option is chosen during installation.

6. Select an alarm class, if required, from the **Alarm Class** drop down list. You must assign an alarm class to a unit before it can be represented on a site plan.
7. Select the protocol used by the CCTV controller from the **CCTV Command Set** drop-down list.
   ⇨ This list will display pre-defined CCTV command set names for Pacom, Pelco and SIMATRIX. Operators have the flexibility to create new command sets by copying and modify existing ones. Once created, the new command set names will be displayed in this list. To create a new command set, please refer the section Configuring New Command Sets for Generic CCTV. [➝ 189]
8. Select the communications Baud Rate from the **Baud Rate** drop-down list. This baud rate would normally be 9600.
9. Select the serial communications port to which the CCTV system will connect from the Port drop-down list. This port would normally be COM2, depending upon other devices connected to the PC.
10. Select the serial communications port to which the CCTV system will connect from the Port drop-down list. This port would normally be COM2, depending upon other devices connected to the PC.

	PELCO GENERIC BUS	SMATRIX GENERIC BUS
Port	COM1	COM1
Host Name	Will be Host specific	Will be Host specific
Port Number	8085	8085
Parity	None	Even
Stop Bits	1	2
Data Bits	8	8
User ID	7777	-

1. Enter the **IP Address or Host Name** of the PC to which the CCTV switcher is connected.
2. Enter the **Port Number** to which the generic CCTV service is listening. The Port Number is usually 8085.
3. Make required selections from the **Parity**, **Stop Bits** and **Data Bits** drop down fields.

Note that these selections should match the Parity, Stop Bit and Data Bit settings that have been physically configured on the CCTV switcher.

4. If necessary, and only in the event that your CCTV system requires you to do so, enter the CCTV Keyboard ID, into the **User ID** field. This will normally be a four-digit ID number.
   - SiPass integrated cannot be used to control the CCTV equipment if the keyboard ID does not match the ID configured using the CCTV System Administration software.
5. Click the *CCTV Bus Parameters* tab.
6. If you wish to log all CCTV bus activity to a permanent data file, select the **Log commands to file** check box. The log file will be stored in the following location – “c:\Temp\BussLog.txt”.
   - Depending upon the amount of CCTV bus activity, the overall system performance may be affected if this log to file option is selected. It is recommended that this option only be selected for diagnostic purposes.
7. Choose **Save** and then stop and restart the CCTV Bus Service.

10.5.2.3 Configuring the New Command Sets for Generic CCTV

Click the **Configure Command Set** button on the *CCTV Bus Parameters* tab.

The *Configure CCTV Command* Set dialog will be displayed. The **Command Set** drop down list contains default CCTV protocols for which command sets are pre-configured in the SiPass integrated system. The grid box below displays the commands and its properties.

Column Name	Description
Name	The name of the command should be entered under this field.
Syntax	The syntax for the command should be entered under this field
Description	A description of the command should be entered in this field.
Show in HBET	The drop down list of this field, containing 'Yes' and 'No' options, can be used to specify if the respective command should be displayed in the *Host Event Task* dialog. Please note that this field will be disabled for commands that are not applicable to the Host Event Tasks.

SIMATRIC Generic and PELCO Generic will have default command sets defined that will display the syntax parameters. However, operators who wish to create generic Philips or other PACOM command sets will need to refer the product documentation for the specific CCTV syntax.

1. Click the **Save As** button.
2. Enter a new command set name in the dialog that appears.
3. Click **Save**.
   ⇨ The default set of commands will now be saved under the new command set name, and displayed.
4. To add a new command row to this set, click the **Add Command** button.
5. When entering the Syntax for new commands, the following parameters must be used for respective properties:

Syntax Subject	Syntax Parameter
Camera	<CA>
Monitor	<MO>
Alarm Point	<PO>
Preset	<PR>
Speed	<SP>

In case two or more commands needs to be sent to the switcher, separate them with \t. This is particularly useful when a command has a pre-requisite command to run.

Other free-flowing parameters, up to a length of 4, are also supported (e.g. <para>, <p1>, etc).

1. To delete a particular command row, select it and click the **Delete Command** button.
2. To save your changes, click **Save**.

Please note that none of the properties (Command Set Name / Command Name / Syntax / Description / Show in HET) of the default command sets (Simatrix Generic, Pelco Generic) can be modified and saved. Also note that the Command Name of the default commands (Switch Camera to Monitor, Run Preset, etc) cannot be changed. Also these default commands cannot be deleted.

To delete an entire command set:

1. Select the command set from the **Command Set** drop down list.
2. Click the **Delete** button.

10.6 Operating CCTV

Once the configuration process has been completed you are now ready to use your CCTV system in conjunction with your access control system. The operational components include viewing fixed camera pictures, viewing and manipulating PTZ type cameras, and running presets, patterns and sequences.

SiPass CCTV clients can be prioritized when configuring a CCTV switcher, to prevent clashes occurring when multiple clients try to manipulate a single camera. See the literature provided with your System Administration software for more information.

10.6.1 Viewing images from a camera

SiPass integrated allows you to select both the monitor on which images are to be displayed and the specific camera that will be used to capture those images. Fixed cameras can only display relatively static images, that only change when something within their line of view changes. Images captured using a PTZ camera can not only be viewed, but the line of view from the camera can be manipulated using SiPass integrated.

1. Choose the **CCTV Operation** button from the **Operation** toolbar or menu.
2. Select a specific Monitor Group or the **All Monitors** option from the **Monitor Group** drop-down list.
3. Select the monitor that will be used to display the CCTV images.
4. Select a specific Camera Group or the “All Cameras” option from the **Camera Group** drop-down box.
5. Double click on the name of the camera from which images will be viewed.
   - The display from that camera will appear on-screen if the SiPass integrated monitor has been selected. Otherwise, the CCTV picture from that camera will appear on the monitor selected.
6. You can now view captured images. If the camera is a PTZ type camera, you can use the SiPass CCTV tools to manipulate the displayed image and direction of camera viewing.
7. Choose **Close**.

10.6.2 Viewing preset images from a camera

SiPass integrated allows you to select a specific camera and a pre-configured preset for that camera and display the images from the preset on a selected monitor. Only PTZ cameras can be used to display preset images.

1. Choose **CCTV** from the **Operation** toolbar or menu.
2. Select a specific Monitor Group from the **Monitor Group** drop-down box.
3. Select the monitor that will be used to display the preset, by highlighting the name of the monitor and then choosing the **Preset** button.
   ⇨ The display from that camera will appear on-screen if the SiPass monitor has been selected. Otherwise, the CCTV picture from that camera will appear on the monitor selected.
4. Select a specific Camera Group or the **All Cameras** option from the **Camera Group** drop-down box.
5. Select the camera for which the desired Preset has been configured from the **Camera** list displayed.
6. Select the Preset that you wish to view from the displayed list.
7. Choose **Run**.
   ⇨ The Preset will appear on the selected monitor. If the monitor chosen was the SiPass GUI, you will need to select the *Operator – Cameras* tab to view the CCTV images. By selecting the *Operator – Cameras* tab you can also use the CCTV tools provided to enhance the Preset's image quality or move the camera from the preset location.
8. Choose **Close**.

10.6.3 Running a Pattern

SiPass integrated allows you to select a specific camera and a pre-configured pattern for that camera and display the images on a specific monitor. Only PTZ cameras can be used to display CCTV patterns.

1. Choose **CCTV Operation** from the **Operation** toolbar or menu.
2. Select a specific Monitor Group or the "All Monitors" option from the **Monitor Group** drop-down box.
3. Select the monitor that will be used to display the pattern, by highlighting the name of the monitor. Then choose the operation's *Pattern* tab.
   ⇨ The display from that camera will appear on-screen if the SiPass monitor has been selected. Otherwise, the CCTV picture from that camera will appear on the monitor selected.
4. Select a specific Camera Group or the "All Cameras" option from the **Camera Group** drop-down box.
5. Select the camera for which the desired Pattern has been configured from the **Camera** list displayed.
6. Select whether you want the Pattern to run continuously or specify the exact number of times to run the pattern by choosing the appropriate **Execute** option.
7. Select the Pattern that you wish to view from the displayed list.

8. Choose **Run** or press **ALT + R**.
   ⇨ The Pattern will appear on the selected monitor. If the monitor chosen was the SiPass GUI, you will need to select the *Operator – Cameras* tab to view the CCTV images. By selecting the *Operator – Cameras* tab you can also use the CCTV tools provided to enhance the Pattern's image quality or move the camera manually.
9. Choose **Stop** to stop the Pattern from running
10. Choose **Close**.

10.6.4 Running a Sequence

SiPass integrated allows you to select both the monitor on which a sequence can be displayed and the specific sequence to be run. Both fixed and PTZ cameras can be incorporated as part of a sequence.

1. Choose the **CCTV Operation** from the **Operation** toolbar or menu.
2. Select a specific Monitor Group or the **All Monitors** option from the **Monitor Group** drop-down box.
3. Select the monitor that will be used to display the pattern, by highlighting the name of the monitor. Then choose the **Sequence** button.
   ⇨ The display from that camera will appear on-screen if the SiPass monitor has been selected. Otherwise, the CCTV picture from that camera will appear on the monitor selected.
4. Select whether you want the Sequence to run continuously or a specified number of times by choosing the appropriate **Execute** option.
5. Select the Sequence that you wish to display from the displayed list of Sequences.
6. Choose **Run** or press **ALT + R**. The Sequence will appear on the selected monitor. If the monitor chosen was the SiPass GUI, you will need to select the *Operator – Cameras* tab to view the CCTV images. By selecting the *Operator – Cameras* tab you can also use the CCTV tools provided to enhance the Sequence's image quality or move the camera manually.
7. Choose **Stop** to stop the sequence from running.
8. Choose **Close**.

10.6.5 Viewing Images through the Live CCTV Dialog

SiPass integrated also has a separate dialog available for viewing live images and controlling PTZ cameras while you continue to operate SiPass. The Live CCTV window is designed to be a “floating” window that opens in response to Event Tasks and site plan commands, allowing you to immediately view a specific camera image of the relevant area. You can also open the Live CCTV dialog from the Alarm menu.

The SiPass Client you are using must be selected as the Monitor in the CCTV Operations dialog, before the Live CCTV dialog can be used to manipulate PTZ cameras from SiPass integrated.

1. Choose the **Live CCTV** button from the **Alarm** toolbar or menu.
   ⇨ The image shown will be the view from the last active camera, or the last camera selected from the *CCTV Operations* dialog. To change which camera is shown in the Live CCTV dialog, you must open the *CCTV Operations* dialog and select another camera
2. Use the camera controls located along the top of the dialog to manipulate the camera and image.
3. You can increase the size of the window by left-clicking on one of the corners or edges and dragging the mouse.

Presets, patterns and sequences cannot be controlled, they can only be viewed through the Live CCTV dialog.

10.6.6 Resuming / Restarting CCTV Patterns and Sequences after power loss

Once communications between SiPass integrated and the CCTV Controller are lost or the SiPass integrated system itself loses power, SiPass can no longer control the operation of the cameras or monitors in your CCTV system. This means that any Sequences or Patterns being controlled from SiPass integrated cannot be completed or recovered until communications has been restored.

To overcome this problem you may wish to do the following:

- Create some patterns and macros on the CCTV Controller itself (e.g. via a CCTV keyboard).
- Create Event Tasks in SiPass integrated that automatically configure the desired CCTV settings (e.g. which sequences are run on what monitors). These Event Tasks should be triggered when communications on the CCTV Bus have been restored.

10.6.7 CCTV Alarm and Event Handling

CCTV systems often are equipped with their own internal Alarm Handling and Event mechanisms. Presets, sequences, and combinations of events can be programmed as macros using the CCTV Administration software. CCTV Alarm types can also usually be defined for cameras, in order to trigger macros if an alarm occurs.

This Alarm and Event Handling mechanism, internal to CCTV Switchers, can be linked to SiPass' own alarm handling and event task functionality.

This chapter is only relevant for sites using the Pelco 9740/9760 CCTV system.

Linking the CCTV system's Alarm and Event Handling to SiPass integrated has two advantages:

- CCTV alarms can be triggered from SiPass integrated events. For example, a complex CCTV macro can be triggered from an alarm originating from SiPass. If a secure door is forced, a whole series of cameras can automatically switch to a preset or sequence without creating a series of SiPass integrated event tasks.
- SiPass integrated alarms can be triggered from CCTV alarms. For example, if a camera wire to the CCTV Switcher is cut, SiPass can be informed by the switcher of the event and forward an alarm onto operators or security personnel.
- Additionally, the "Video Loss" alarm is a particular CCTV-specific alarm which can be selected in the *SiPass Alarm Class* dialog when defining an alarm class for cameras.

10.6.7.1 Triggering a CCTV Event

Setting up a CCTV Alarm or Macro to trigger from SiPass integrated is a three-step process:

Step 1: Creating the CCTV Event

CCTV Alarms and Macros are configured on a Switcher using the CCTV administration software that came with the system. As each system is configured differently, you must consult your CCTV System's documentation for more information on how to define Alarms and Macros.

Step 2: Creating the Alarm Point

1. Select **Components** from the **System** toolbar or menu.
2. Select from the **Components** tree on the left hand side the CCTV Switcher for which you want to create an alarm point.
3. Choose **New Unit**, and select **Alarm** from the menu.

   ⇨ A new point will appear under the CCTV Unit and a new tab will appear.
4. Enter a name for the alarm point into the **Name** field. For ease of reference, this name should match the name of the Alarm Type configured in the CCTV Administration software.
5. Enter the alarm point number in the **Point No.** field. The point number must match the alarm number for this **Alarm Type** as configured in the Administration software.
6. Click **Save**.

Step 3: Creating the Event Task

You will most likely create two event tasks for each CCTV Alarm; an “alarm trigger” event task and an “alarm restore” event task. The first event task triggers the alarm in response to a SiPass alarm event, and the second restores the CCTV alarm on the Switcher when the SiPass integrated alarm conditions have been restored.

1. Select **Program > Event Task > Host**.
2. Enter a descriptive name for the event task into the **Event Name** field.
3. Select from the **Time Schedule** drop-down box the time during which this event task can be triggered.
4. Complete the fields in the **Trigger** section as for a normal Event Task.
5. Select “CCTV” from the **Target** drop-down box.
6. Select “Activate Alarm” or “Acknowledge Alarm” from the **Command** drop-down box, depending on whether you want to trigger the CCTV alarm or de-activate it respectively.
7. Select from the **Switcher** drop-down box the CCTV Unit on which the alarm is defined.
8. Select the CCTV Alarm from the **Alarm** drop-down box.
9. Click **Save**.

10.6.7.2 Triggering a SiPass Alarm (Pelco with DT4 only)

Setting up a SiPass event to trigger from a CCTV alarm is a three-step process:

Step 1: Creating the CCTV Alarm Type

CCTV Alarm Types are configured on a Switcher using the CCTV administration software that came with the system. As each system is configured differently, you must consult your CCTV System’s documentation for more information on how to create Alarm Types.

Step 2: Creating a Camera Point Alarm Class

1. Select **Alarm Class** from the **Program** menu or toolbar.
2. Enter a new name for the Alarm Class into the **Alarm Definition Name** field.
3. Select “Camera” from the **Type** drop-down box.
4. Complete the fields in the **Alarm Handling** and **Alarm Options** sections as for a normal Alarm Class.
5. The **Current Defined States** table lists all of the possible camera states that are forwarded to SiPass by the CCTV Switcher. At the moment only two states are reported.
6. Select **Add**.
   ⇨ A new row will appear in the table.
7. Click in the **Status** column and select Video “Loss”.
8. Enter a description for the video loss state into the **Status Description** column.
9. Select “Alarm” from the **Alarm/Restore** column.
10. Select an appropriate **Symbol Name**. This is the symbol that will appear in Site Plans when the camera point enters the “Video Loss” state.

11. Choose **Add** again. Another row will appear below the first. Click in the **Status** column and select “Acknowledged”.
12. Enter a description into the **Status Description** column.
13. In the Alarm/Restore column, select “Restore”.
14. Select an appropriate **Symbol Name**.
    ⇨ This is the symbol that will appear in Site Plans when the camera point alarm is restored.
15. Click **Save**.

Step 3: Initializing the CCTV Switcher

Once you have finishing configuring your CCTV Units and Camera points, you must initialize each Switcher with the details.

1. Select **Components** from the **System** toolbar or menu.
2. Select from the **Components** tree the CCTV Switcher you want to initialize.
3. Choose **Initialize Video Loss Alarm**. This process may take a few minutes.

11 Image Verification

SiPass integrated allows you to perform image verification on cardholders. This advanced functionality increases the security of your site, by allowing security operators to visually confirm the identity of personnel attempting access.

Image verification can be configured to be mandatory at particular access points, requiring the guard to manually verify identity before allowing access. It can also be configured to allow access according to cardholder access privileges, but automatically take a snapshot of the cardholder to be displayed on a selected monitor.

11.1 Configuring Image Verification at an Access Point

Before you can use the Image Verification feature of SiPass integrated, you need to configure those access points at which image verification will apply. Image verification is configured through the *Image Verification* tab in the *Components* dialog. The steps required to do this are as follows:

1. Choose **Components** from the **System** toolbar or menu.
   ⇨ The *Components* dialog will appear.
2. Select the Server name in the components hierarchy.
3. Select the **ACC Controllers** ethernet comms.
4. Select the ACC to which the access point is connected.
5. Select the FLN connection to which the device controlling the access point is connected.
6. Select the door controller device connected to the access point.
7. Select each *Reader* tab in turn and configure each individually.
8. Select from the **Operation Mode** drop-down box the image verification mode that you want to apply to this access point. The available modes are detailed in the **Available Modes** table, at the end of this section.
9. Enter a value into the Host Verify Timeout field. This is the length of time, in seconds, that the system will wait for an operator response after a card is badged. If the **Allow Access** check box is not ticked and the response times out, the card reader will reset and access may be attempted again. If the **Allow Access** check box is ticked and the response times out, the access will be granted.
10. Select the *Input/Output* tab and select the time schedule during which image verification will be enabled, for each input and output point, from the **Time Schedule** drop-down box. The Time Schedule table at the end of this section details the effect a time schedule has on image verification.
11. Select the *Image Verification* tab.
12. Select the CCTV sequence to run when a cardholder presents their card at the access point, from the **CCTV Sequence** drop-down box for each reader.
13. Select the monitor on which you want the selected sequence to be shown, from the **Monitor** drop-down box for each reader.
14. Select an Alarm Class for the image verification access point, from the **Alarm Class** drop-down box for each reader.
15. Select the **Save Image Snapshot** checkbox to save live images to disk when an access attempt is made at the point for each reader.
16. Enter the snapshot delay in seconds into the **Snapshot Delay** field for each reader. This number represents the time taken for the camera to move from the start of the selected camera sequence to the ideal position for taking a snapshot of the cardholder.
17. Choose **Save**.

Available Modes

Access Mode	Description
Host Verification – Card only	A card is required for access at this point; if a valid cardholder makes an access attempt, the Image Verification screen will be displayed on the SiPass GUI and a security operator will be prompted to allow or deny access.
Host Verification – Card and PIN	Both a card and a PIN code are required for access at this point; if an access attempt is made by a valid cardholder, the Image Verification screen will be displayed on the SiPass GUI and a security operator will be prompted to allow or deny access.
View Only – Card only	A card is required for access at this point; if a valid cardholder makes an access attempt, access will be determined by normal access privileges, but a CCTV snapshot of the access attempt will be taken and stored in the database.
View Only – Card and PIN	Both a card and a PIN code are required for access at this point; if an access attempt is made by a valid cardholder, access will be determined by normal access privileges, but a CCTV snapshot of the access attempt will be taken and stored in the database.

Time Schedule

Time Schedule	Description
Always (point unsecured)	Image verification mode will always be enabled.
Never (point secure)	Image verification mode will always be disabled
Office Hours (9-5)	Image verification mode will be enabled between 9:00am and 5:00pm.

11.2 Operating Image Verification

Setting an access point's Image Verification mode to "Operator controlled" or "Host Verification" means that when an access card is badged at a reader, the *Image Verification* dialog will appear on the SiPass client. The security operator needs to manually verify that the live CCTV image matches the stored database image of the cardholder, before allowing or denying entry.

A cardholder must have access privileges to a point for the Image Verification screen to be displayed upon an access attempt. For example, if a person does not have privileges during a certain Time Schedule, or is using a void card, access will be denied by the hardware controller, and the Image Verification screen will not be displayed.

If an access point's Image Verification mode has been set to "View Only", the *Image Verification* dialog will still appear on screen. However, the dialog will be for viewing and snapshot purposes only. Access will be determined as normal.

An operator must have the appropriate privileges for both Image Verification and the access point, to be able to use the Image Verification dialog to view live CCTV or DVR images and confirm or deny entry at that point.

Performing Image Verification

1. When an access card is badged at an image verification access point, the *Image Verification* dialog will appear: The stored database photo appears on the left hand side, and the live CCTV snapshot appears on the right.
2. If you are satisfied that the live photo matches the database photo, choose **Allow**. The door will unlock and access will be permitted.
3. Otherwise, select the **Deny** button. The door will remain locked and the door controller will reset and wait for the next access attempt.

The door controller will wait a certain amount of time for a response from an operator. During this time, swiping any other card at the reader will have no affect. If there still has not been a response from an operator after this time, the controller will reset and access can be re-attempted. The timeout period can be configured by entering a value into the Host Verify Timeout field of the *Access* tab of the relevant device. The default is 60 seconds.

If an operator has not allowed or denied entry using Image Verification within 30 seconds, an audible alarm will sound. This can be silenced by choosing Silence. This event is not a SiPass alarm.

11.2.1 Operating Image Verification from the Audit Trail

If you have checked the **Save Image Snapshot** checkbox in the *Image Verification* tab of the *Components* dialog, each time an access attempt is made at an access point configured for image verification, a live snapshot of the cardholder will be saved to the database. Both the cardholder's image from the database and the saved CCTV snapshot can be viewed from the audit trail.

For example, a guard may observe from the audit trail that a cardholder has entered the site, but may not recall seeing that cardholder when he or she completed the last guard tour. The live CCTV snapshot of the access attempt can be recalled from the Audit Trail, to confirm whether that cardholder has indeed entered the site, or someone else has used the card to gain unauthorized access.

Stored snapshots can also be viewed in *Image Verification* reports.

Viewing a stored cardholder image from the Audit Trail

1. Locate the audit trail entry for which you wish to view a stored database image of a cardholder. The entry must be an access attempt by a valid cardholder.
2. Right click on the entry. A menu will appear.
3. Select **View** Image.
4. Choose the *Imaging* tab to see the stored database image of the cardholder.

Viewing a Live CCTV Snapshot from the Audit Trail

1. Locate the audit trail entry for which you wish to view a live CCTV image. The audit trail entry must be an access attempt by a valid cardholder, at a point configured for image verification.
2. Right click on the entry. A menu will appear.
3. Select **View Snapshot**.
   ⇨ The *Image Verification* dialog will appear, displaying only the live CCTV snapshot of the access attempt made at that point.
4. Choose **Close**.

12 Dial-up

Dial-up refers to communications via a modem (as opposed to a direct connection) between a PC running the SiPass integrated software and an ACC controller.

Using SiPass integrated, an operator can achieve the same functionality from a dial-up unit as they can from a unit directly connected to the PC. For example, an operator can lock a door, unlock a door and even change a cardholder's access control privileges at a remote location by using dial up functions. Database changes from the SiPass Server and audit logs from the remote unit are downloaded and uploaded automatically each time a connection is initiated with a remote ACC.

12.1 Dial-up Components

The components involved in a dialup system will depend on the complexity. A single remote connection consists of the following components:

- Dialup Bus
- Modem(s)
- RAS Connection
- Remote ACC (or Remote ACC network)

Dialup Bus

The Dialup Bus represents a connection from the SiPass Server to a remote modem or modem bank. One Dialup Bus has to be configured for each remote ACC or ACC network; essentially, one Dialup Bus per remote "connection point", meaning a remote modem or group of modems.

Modem – Remote side

The remote modem communicates with the ACC via the RS-232 Modem port directly in the case of single remote ACC, or through a remote RAS client in the case of a remote ACC network. Any Hayes-compatible modem, that supports a baud rate of 2400bps or above, may be connected to the ACC.

An RS-232 connector must be used to connect the remote modem to the Modem port on the ACC. Other connections, such as an RJ45 phone line connector cannot be used.

Modem – Server side

The modem should support a minimum Baud rate of 2400bps (Bits per second). The SiPass Server must have at least one serial connection port available for connection to a modem. The local modem(s) may only be defined on the same PC as the SiPass Server.

You should install the latest modem manufacturer's drivers for the modem you are using for Dialup control. The default Windows drivers should not be used.

RAS Connection – Server Side

SiPass integrated uses the Windows RAS protocol to handle communications between the Server and the remote connection. The number of RAS connections you will need to create on the SiPass Server will vary, depending on how your modem or modems are set up. A single RAS connection, regardless of the number of remote ACCs, is able to manage multiple connections at the same time.

RAS Connection – Remote Side

If the remote site has multiple ACCs present, instead of using a single modem for each ACC, a PC may be used as an RAS connection manager on the remote side. This allows you to manage large remote ACC networks without the need for a modem assigned to each ACC.

No SiPass integrated components need to be installed on a remote RAS client at all. The remote client only needs to have Windows installed and the RAS connection to be configured.

Remote ACC or ACC Network

Configuring a remote ACC involves supplying the communications parameters, like RAS Connection and IP address details. Once configured, a remote ACC will operate in the same manner as a local ACC.

A Dialup ACC must be initially configured with dialup communications parameters (using HyperTerminal or similar access program) before it can be configured from the SiPass GUI.

Remote devices do not need to be configured any differently in the SiPass integrated **Components** dialog.

12.2 Pre-requisites

The following lists the recommended pre-requisites for a successful SiPass integrated dialup configuration:

- If there is more than one modem connected to the SiPass Server PC, it is highly recommended that Windows 2003 / 2008 Server be used as the operating system. Windows XP Professional is not recommended unless only a single modem is connected. The appropriate changes to the Server profile configuration also need to be made.
- The modems used on both the Server side and Remote side should preferably be of the same make and model.

Note: The Dial-up configuration instructions, provided in the sections that follow, can be applied for a PC that uses either the Windows 2003 or 2008 Server as the operating system. Although the overall configuration is essentially the same for both operating systems, there may be slight variations in the configuration dialogs when using the Windows 2008 Server.

12.3 Dialup Setup Checklist

The following checklists can be used when configuring your remote ACC network(s) and the SiPass Server for dialup communication:

- **If the remote ACC is connected directly to the modem:**
  - Install a modem on the PC hosting the SiPass Server,
  - Create a dialup connection on the PC hosting the SiPass Server
  - Connect modem(s) to the remote ACC unit(s)
  - Configure the Dialup Bus in SiPass integrated
  - Configure the dialup ACC(s) in SiPass integrated
  - Initialize the dialup ACC(s) with the configuration details
- **If the remote ACC network is connected via remote RAS Client:**
  - Install a modem on the PC hosting the SiPass Server,
  - Create a dialup connection on the PC hosting the SiPass Server
  - Connect modem(s) to the remote RAS client
  - Create a dialup connection on the remote Client
  - Configure the Dialup Bus in SiPass integrated
  - Configure the dialup ACC(s) in SiPass integrated
  - Initialize the dialup ACC(s) with the configuration details

12.4 Creating the Dialup Connection

You must create a dialup connection on the PC hosting the SiPass Server, in order to dial and send data to a remote ACC. The dialup connection uses the Windows RAS protocol to send and receive messages from the remote units. Only one RAS connection has to be configured; this connection is used by all remote ACCs for access.

If your remote ACC network uses a “gateway” PC on the remote side, you must also configure a remote dialup connection on that PC. Steps 2 and 3 below do not apply to the remote PC.

It is recommended that the following procedures be carried out by a Systems Administrator or a similar person who is familiar with setting up dialup and network connections in the Windows operating environment.

Local Administrator privileges are required to set up a dialup connection on a PC in a Windows network.

Whichever user is logged in during the creation of the dialup connection must be assigned to the SiPass Server Service as described in the next procedure. This applies to connections created on the SiPass Server only.

12.4.1 Step 1: Making the Connection

1. Select **Settings > Network and Dial up Connections > Make a new connection** from the Windows **Start** menu.
2. Choose **Next**.
3. Select the **Dial-up to private network** option.
4. Enter the Phone Number of the remote modem you want to dial. If you are dialing a different state or country, tick the **Use Dialing Rules** checkbox to enable those fields.
5. A “0” can be placed in front of the number if necessary, to indicate dialling an outside line. A comma can also be placed before the Phone number to indicate a pause.
6. If you are configuring this connection on the SiPass Server, this number will be the number of the remote ACC or remote gateway PC that you wish to dial.
7. If you are configuring this connection on the remote gateway PC, this number will be the number of the SiPass Server that you wish to dial.
8. Choose **Next**.
9. Leave the **Enable Internet Connection Sharing** for this connection un-ticked. Choose **Next**.
10. Select the **For all users** option. Choose **Next**.
11. Enter a meaningful name for the dialup connection. This is the name that will appear in the **Connection** drop-down box in the SiPass integrated *Components* dialog (SiPass Server only).
12. Enter the Username and Password of the user that you want to assign to this connection. The username/password you assign here must be the same that is assigned to the ACC, as shown in the procedure To configure an ACC for dialup communications.
13. Choose **Properties**. Choose **Configure**.
    - The value selected in the **Maximum Speed (bps)** field should be approximately twice the rated speed of the modem used to dial the remote ACC. For example, for a 28.8k modem, select 57600.
14. Ensure all of the Hardware features options are selected. Choose **OK**.
15. Select the *Security* tab.
16. Select the **Advanced** (custom settings) option. Choose **Settings**.
17. Select the Allow these protocols option, and disable all protocols except for Unencrypted password (PAP). Choose **OK**.
18. Select the *Networking* tab.
19. Un-tick all options except for **Internet Protocol (TCP/IP)**. Select the **Settings** button.
20. Disable all settings in this dialog. Choose **OK**.
21. Choose **OK** to exit the *Connection Properties* dialog.
22. Choose **Dial** to dial and test the connection you have just created, or choose **Cancel** to exit to the desktop.

12.4.2 Step 2: Assigning a username and password to the SiPass Server Service

1. Choose **Settings > Control Panel** from the Windows **Start** menu.
2. Double click on the **Administrative Tools** icon.
3. Double click on the **Services** icon.
4. Scroll down the list until you find the SiPassServer entry. Right click on SipassServer and select Properties from the menu.
5. Select the *Log On* tab.
6. Select the **This Account** option. Choose **Browse** to assign a user to this Service.
7. Select a user from the list. The user you select must be the same user who was logged in while the dialup connection was being created, as described in the previous procedure.
8. Choose **OK**.

12.4.3 Step 3: Setting up an ACC for remote communications

This procedure describes how to assign the address details, username and password you have configured on the SiPass Server to the remote ACC. A program such as Telnet or HyperTerminal is used to connect to the ACC for configuration.

The Firmware Instruction set must be downloaded before the ACC can be configured for Dialup Communications.

▷ Ensure that the ACC is connected and communicating with the SiPass Server, and you have configured HyperTerminal for communications with the ACC.

1. Choose **Start > Programs > Accessories > Communications> > HyperTerminal**.
2. Choose **File > Open** and select the connection to the ACC.
3. Press the <Enter> key on the keyboard until the Username prompt appears.
4. At the Login prompt type “SIEMENS“ and press the <Enter> key on the keyboard. Please note the user name is case sensitive.
5. At the Password prompt type “spirit“ and press the <Enter> key on the keyboard.
6. If you have successfully logged into the ACC the message “User SIEMENS logged In” will appear.
7. Ensure that you are logged into the Application Level of the ACC. If you have successfully downloaded the latest firmware instruction set, you will automatically be logged into the application level when connecting to an ACC via HyperTerminal.
8. Type “get modem” and press the <Enter> key. A list of default dialup settings will appear in the HyperTerminal window, The ‘set modem’ command is used to set the Connection parameters.
9. To set the IP address of the ACC (for PPP communications), type “set modem local address “ACCAddress”” at prompt. Where “ACCAddress“ refers to the IP address of the modem connected to the ACC.

10. To set the IP address of the Host (for PPP communications), type “set modem remote address “HostAddress”” at the prompt. Where “HostAddress“ refers to the IP address of the PPP link on the Server PC which the ACC will be dialing. This will have been configured by you as described in the section *To assign a static IP address to a network connection*.
11. To set the subnet mask (if any), type “set modem subnetmask “SubnetMask”” at the prompt. Where “SubnetMask“ refers to the subnet mask used to access the remote network of ACCs.
12. To set the username property, type “set modem username 'UserName'” at the prompt. Where “UserName“ refers to the Windows user name assigned to the SiPass Server Connection in the procedure *To Create the Connection*.
13. To set the password property, type “set modem password “Password” command at the prompt. Where “Password“ refers to the Windows password assigned to the SiPass Server Connection in the procedure *To Create the Connection*.
14. To set the phone number property, type “set modem number “PhoneNumber”” at the prompt. Where “PhoneNumber“ refers to the phone number of the modem connected to the SiPass Server.
15. Type the command “reboot” at the prompt and press <Enter>

	*NOTICE*
	Important: These parameters, except for “username” and “password”, can also be set from SiPass integrated. Any values entered in the SiPass GUI will over-ride the above settings. This means that you must enter the same values in SiPass integrated as configured above before establishing the first connection, otherwise the dialup parameters will be over-ridden by the default settings and you will have to re-configure the ACC.

12.5 Creating the Dial-up Bus Service

You may have selected to install a dialup bus during your SiPass integrated installation. If this is the case, you can proceed to defining a Dialup Bus.

1. Select **Components** from the *System* dialog or menu.
2. Select the Server name in the left hand pane.
3. Choose **New Bus**. A menu displaying a list of options will appear. Select **Dialup / Remote Network**.
4. Select the RAS connection that you defined in the previous section from the **Connection** drop-down box.
5. Select the Alarm Class that will apply to this dialup bus from the **Bus Alarm** drop-down box.
6. The default Initial Maximum number of cards per ACC is 25,000. If you need to change this value, enter a new number into the field. The actual maximum number of cards per ACC will depend on the license you have purchased.

7. The Number of commands to unit before auto-download field determines how many database commands at the Server can occur, before the SiPass integrated server will automatically dial the remote ACCs and download the list of database changes. The default is 1000.
8. Choose **Connect** to connect to the remote ACCs. The Status field will be updated according to whether the connection was successful or not.

⇨ Once a connection has been made, a remote ACC and any connected devices will operate exactly like a local ACC plus devices.

12.5.1 Defining the Dial-up ACC

The remote ACC must be configured with communications and address parameters. The steps required to define a Dial-up ACC are as follows:

1. Select **Components** from the **System** menu or toolbar.
2. Select the remote Bus that you defined in the previous section from the **Components** tree. Choose **New Unit**.

   ⇨ A new ACC will appear under the remote Bus and two new tabs will become available. The fields in the *ACC Controller* tab are filled in exactly the same as for a local ACC unit.
3. Select the *Dialup/PPP Properties* tab.
4. Tick the *Allow incoming Connections* checkbox if you want the SiPass Server to be able to initiate a connection to the ACC.
5. Enter the number of the first modem connected to the SiPass Server into the first **Server Phone Number** field.
6. If you are only using one modem to dial in to the Server, enter the same number into the second **Server Phone Number** field. If two modems are connected to the SiPass Server, enter the number of the second modem into this field.
7. Complete the fields in the **Other Properties** section:
   – The command list must be terminated with the '^M' character.
8. Click **Save**.

12.5.1.1 Dialup Properties

The following table explains the available properties when configuring dialup ACCs.

Property	Description
ACC PPP Address	The PPP Address of the connection on the remote ACC. Note that this is different to the TCP/IP address configured for the PC during initial installation.
Host PPP Address	The PPP Address of the connection on the SiPass Server. Note that this address is different to the TCP/IP address of the Server PC.
Subnet Mask	The Subnet Mask (if applicable) used to access ACCs on the remote network.
Idle Timeout (min)	The length of time after which, if there has been no communication either from or to the ACC, the ACC will disconnect the Dialup connection to the SiPass Server.

Property	Description
No. of Retries	The number of times the ACC will attempt to dial the first phone number. If there has not been a successful connection, the ACC will attempt the same number of tries on the second phone number, and continue to alternate between the two numbers.
Baud Rate	The baud rate of the serial dialup connection. This should be set to the next fastest speed above the baud rate of the modem connected to the ACC.
Modem Initialization String	The commands that are sent to a modem prior to sending information; for example, to turn off sounds or to disable a certain communications mode. Consult your modem's User Guide for a list of modem commands that are understood.
Dial Server When	The number of Audit Trail messages that accumulate in the ACC Audit Trail buffer before the ACC dials the SiPass Server to upload.

12.5.2 Defining other Components

Once you have defined the dialup bus for the ACC Series platform, all other components, including FLN connections, Devices and Points, are defined earlier in this manual.

12.5.3 Alarm Class on Dial-up Controllers

If you want an alarm on a dial-up unit to be reported immediately to the system, you must define an Alarm Class for each remote ACC, device and point. The Alarm Class assigned must require acknowledgement from an operator, and also have the **Dial Back** checkbox ticked.

Alarm Classes on a dial-up unit are defined in exactly the same manner as Alarm Classes on a local unit.

The Alarm Class you define must include all the appropriate states. For example, each door should have a state for door open, door forced, door held and door closed. This ensures that an alarm will be up-loaded to the Server immediately, if any of these changes of state occurs.

If you do not assign an Alarm Class to a point on the dial-up controller, or do not select the **Dial Back** option, you will not be notified immediately when a change in state occurs. The unit will generate a message (and place it in the Audit Log) stating that the point has changed state, but this will not reach the Server until the unit uploads its Audit Trail buffer to the Server.

Furthermore, the message will never be displayed unless a report is generated.

12.5.4 Initialization and Downloading

Data at your site has to be downloaded to remote Controllers and Devices just like local units. Changes to the SiPass Server database are downloaded to remote units by initialization.

Initialization can be performed manually, or automatically initiated by SiPass integrated depending on your configuration settings in the Components dialog.

Initializing a remote unit

▷ Ensure that you are able to dial a dialup ACC before you intialize a dialup unit.

1. Select **Initialize** from the **System** dialog or menu.
   ⇨ A list of every ACC defined in the Components dialog, and currently online, will appear in the **Available** field.
2. Select the remote unit(s) in the **Available** list that you want to initialize.
3. Choose **Add >**.
   ⇨ The unit will be moved to the **Selected** list.
4. You can select which data is downloaded to units during Initialization by ticking the **Initialization Options** checkbox. This step is optional; you may choose to stick with the default settings.
5. A confirmation dialog will appear asking if you are sure you want to change these settings. Click **Yes** to proceed.
6. Any data component can be downloaded by ticking or un-ticking the appropriate checkbox.
7. Click **Full Initialize**.

⇨ The data you selected will be downloaded to the remote ACC(s). The initialization process will be displayed in the Audit Trail.

12.5.4.1 Initialization Options

The following table explains the available initialization options.

Option	Description
Memory	This option is disabled and is not applicable.
Holiday	All defined holidays will be downloaded on initialization.
Time Schedule	All defined Time Schedules will be downloaded on initialization.
Point	All information about the points that belong to the selected units will be downloaded on initialization.
Employee Access	All cardholders' access control information will be downloaded on initialization.
Anti-Passback	Anti-Passback information, such as areas, points and modes will be downloaded on initialization.
Intrusion Area	All intrusion area information will be downloaded on initialization.
Download expired cards	Expired cardholder cards will be downloaded on intialization.
Download all cards to all ACC's	All cardolder cards will be downloaded to each of the ACC's.
Elevator	All elevator data will be downloaded on initialization.
Event Task	All controller-based event task data will be downloaded on initialization.

12.5.4.2 Automatic download of data to a remote ACC

When creating an ACC dialup bus, the value in the field **No. of commands to unit before auto-download** determines how often the SiPass Server will automatically initiate a connection to remote ACCs to download recent database changes.

It is important to note that this value refers to database commands, not changes. A single database command may generate a relatively high number of commands.

When this value is reached, the Server will dial each remote ACC and download database changes to the following items:

- Cardholders
- Points (input and output)
- Time Schedules
- Holidays
- Point Groups
- Workgroups

The lower the value in the **No. of Commands to unit before auto-download** field, the higher the frequency of automatic downloads. Setting the value too low may have an effect on the speed of your network, depending on network bandwidth and the normal traffic generated by your site.

Initialization messages

During both manual and automatic initialization, messages are displayed in the Audit Trail indicating the progress and status of the dialup connection and database download.

12.5.4.3 Uploading data from a remote unit

There are four scenarios under which data from an ACC may be uploaded to the SiPass Server:

- The ACC Audit Log (buffer) approaches capacity.
- An alarm is generated on a remote unit.
- A manual “Establish Dialup Connection” command is sent to a remote unit.
- A “Establish Dialup Connection” Event Task is triggered.

The ACC Audit Log (buffer) approaches capacity

Each Advanced Central Controller has an Audit Log, called a buffer, used to store Audit Trail events that have occurred. When the ACC buffer reaches a defined value, the remote ACC will automatically initiate a connection back to the SiPass Server and upload the Audit Log to the Server Database.

The value at which an ACC will initiate a connection and upload is defined in the **Dial Server when xxx messages have been accumulated at the controller** field of the *Components* dialog. The default value is 100.

An alarm is generated on a remote unit

Alarms generated at a remote controller are sent immediately to the SiPass Server, if the point or unit in alarm has been assigned an appropriate Alarm Class. The Alarm Class assigned must have the **Dial Back** checkbox ticked.

If the point or unit has not been assigned an Alarm Class, the remote ACC will not automatically initiate a connection if an alarm occurs.

A manual “Establish Dialup Connection” command is sent to a remote unit

It is possible to send a manual “Establish Dialup Connection” command to a unit, which will cause the remote ACC to dial in to the SiPass Server.

An “Establish Dialup Connection” Event Task is triggered on the SiPass Server. The Establish Dialup Connection command may be used as an effect in a SiPass Event Task. For example, you may want to establish a connection at 3 a.m. nightly to upload the ACC audit trail and download the latest database changes.

Creating an Event Task to establish a dialup connection

1. Select **Program > Event Task > Host**.
2. Enter a name for the Event Task into the **Event Name** field.
3. Select the Time Schedule during which this Event Task will be triggered.
4. Select “Time Schedule” from the **Source1** drop-down box.
5. Select “Start” from the **State1** drop-down box.
6. Select “Unit” from the **Target** drop-down box.
7. Select “Establish Dialup Connection” from the **Command** drop-down box.
8. Select the Remote ACC to which you want to initiate a dialup connection, from the **Location** drop-down box.
9. Click **Save**.

⇨ A connection will be established with the remote unit at the start of the Time Schedule selected in step 3. The latest database changes will be downloaded to the ACC and the Audit Trail uploaded.

12.6 Redundant Communications

SiPass integrated contains a number of mechanisms to protect the Server-Controller communications channel in case of failure. These mechanisms use additional, redundant communications channels to automatically switch over if the previous channel is disabled.

There are three levels of communications redundancy that can be configured.

- Ethernet Level Redundancy
- Dialup Backup Redundancy
- Secondary Phone Number Dialup Redundancy

The first level is completely transparent to the user. SiPass integrated will actively reroute data if a node fails in the Ethernet architecture between the Server and the ACC. This requires no configuration or action on the part of the SiPass operator and is not discussed in this User’s Guide.

Dialup Backup Redundancy involves creating a normal dialup connection between the Server and the ACC(s) and designating the connection as redundant. If the Ethernet connection fails altogether, an ACC equipped with redundant dialup will automatically dial in to the SiPass Server.

You can also supply a second phone number with which to dial in. If the ACC encounters a busy signal on the first attempt, it will automatically retry using the backup number. You will need to configure two modems into the SiPass Server PC to use a secondary phone number.

⚠ CAUTION

Redundant Communications will not work in conjunction with Co-stand by server, unless a network modem system such as a Shield modem box is connected.

12.6.1 Pre-requisites

The following lists the recommended pre-requisites for a successful Redundant Communications configuration:

- If there is more than one modem connected to the SiPass Server PC, it is highly recommended that Windows 2003 Server is used as the operating system. Windows XP Professional is not recommended unless only a single modem is connected. The procedures in this section assume you are using Windows 2003 Server as the operating system for setting up dialup communications.
- It is recommended that the SiPass Server is also located on a network domain, controlled by a Windows 2003 server domain controller, instead of a standalone or Workgroup PC. SiPass integrated does not necessarily have to be installed on the domain controller itself, only located on a PC within a domain.
- The modems used on both the Server side and Remote side should preferably be of the same make and model.

12.6.2 Redundancy Configuration Summary

The following is a summary of the dialup redundancy configuration process:

- Enable the storage of passwords using reversible encryption at the Domain Controller (for SiPass Servers within a domain only).
- Create the dialup connection for the redundant ACC dialup.
- Configure the appropriate ACC(s) for redundant dialup communications.
- Define the ACC in SiPass integrated

12.6.3 Setting up Dialup Redundancy

12.6.3.1 Creating the Dialup Connection

1. Select **Settings > Network and Dialup Connections > Make new connection** from the Windows **Start** menu.
2. Choose **Next**.
3. Select **Set up an Advanced connection** and choose **Next**.
4. Select the **Accept incoming connections** option. Choose **Next**.
5. If the SiPass Server PC is located on a domain, you will be prompted to proceed.
6. Choose **Yes**.
7. Right click the name of the PC you are using, from the tree in the left hand pane. Select **Properties** from the menu.
8. In the *General* tab, ensure that the **Remote Access Server** checkbox is ticked.
9. Select the *Security* tab. Choose the **Authentication Methods** button.
10. De-select all options except for **Unencrypted Password (PAP)**.
11. Select the *IP* tab. Choose **Add**.
12. Enter a starting IP address and an End IP address into the field. This address range represents the number of addresses that the Server can allocate to incoming connections. The addresses in this range must be unique; that is, they cannot already have been assigned to existing PCs on the network in which the Server is located. You should allocate a number of addresses no less than the number of ACCs on the remote site.

13. Select the *PPP* tab.
14. Deselect all options in this tab.
15. Choose **Apply**.
16. Choose **OK** to exit the dialog.

⇨ Configuring your SiPass Server PC to accept an incoming call from a remote ACC is now complete.

12.6.3.2 Setting-up password storage

1. Select **Settings > Control Panel** from the Windows **Start** menu.
2. Double click on the Administrative tools icon.
3. Select the **Local Security Policy** icon.
4. Open **Account Policies**, and then **Password Policy** in the tree on the left hand side by clicking on them. A list of options will appear in the right hand pane.
5. Double click on the item **Store password using reversible encryption**.
6. Select the **Enabled** option. Choose **OK**.
7. Exit from the *Local Security Settings* dialog.
8. Reboot the computer for the change to take affect.

12.6.3.3 Setting up an ACC for remote communications

This procedure describes how to assign the address details, username and password you have configured on the SiPass Server to the remote ACC. A program such as Telnet or HyperTerminal is used to connect to the ACC for configuration.

The Firmware Instruction set must be downloaded before the ACC can be configured for Dialup Communications.

▷ Ensure that the ACC is connected and communicating with the SiPass Server, and you have configured HyperTerminal for communications with the ACC.

1. Choose **Start > Programs > Accessories > Communications > HyperTerminal**.
2. Choose **File > Open** and select the connection to the ACC.
3. Press the <Enter> key on the keyboard until the Username prompt appears.
4. At the Login prompt type “SIEMENS” and press the <Enter> key on the keyboard. Please note the user name is case sensitive.
5. A Password prompt will now appear.
6. At the Password prompt type “spirit” and press the <Enter> key. If you have successfully logged into the ACC the message “User SIEMENS logged In” will appear.
7. Ensure that you are logged into the Application Level of the ACC. If you have successfully downloaded the latest firmware instruction set, you will automatically be logged into the application level when connecting to an ACC via HyperTerminal.
8. Type “get modem” at the prompt. A list of default dialup settings will appear in the HyperTerminal window.

9. To set the IP address of the ACC (for PPP communications), type “set modem localaddress “ACCAddress” at the prompt. Where “ACCAddress” refers to the IP address of the modem connected to the ACC.
10. To set the IP address of the Host (for PPP communications), type “set modem remoteaddress “HostAddress”” the following command at the prompt. Where “HostAddress“ refers to the IP address of the PPP link on the Server PC which the ACC will be dialing. This will have been configured by you as described in the section To assign a static IP address to a network connection.
11. To set the subnet mask (if any), type “set modem subnetmask “SubnetMask”” the following command at the prompt. Where “SubnetMask“ refers to the subnet mask used to access the remote network of ACCs.
12. To set the username property, type “set modem username “UserName”” at the prompt. Where “UserName“ refers to the Windows user name assigned to the SiPass Server Connection in the procedure *To Create the Connection*.
13. To set the password property, type “set modem password “Password”” at the prompt. Where “Password“ refers to the Windows password assigned to the SiPass Server Connection in the procedure *To Create the Connection*.
14. To set the phone number property, type “set modem number “PhoneNumber”” the following command at the prompt. Where “PhoneNumber“ refers to the phone number of the modem connected to the SiPass Server.
15. Type the command “reboot” at the prompt and press the <Enter> key.

⇨ The ACC is now configured for Dialup communications.

These parameters, except for “username” and “password”, can also be set from SiPass integrated. Any values entered in the SiPass GUI will over-ride the above settings. This means that you must enter the same values in SiPass integrated as configured above before establishing the first connection, otherwise the dialup parameters will be over-ridden by the default settings and you will have to re-configure the ACC.

12.6.4 Setting-up redundant dialup on an ACC

1. Select **Components** from the **System** menu.
2. Select the ACC from the Components tree for which you are configuring Redundant Dialup.
3. Select the *Dialup/PPP Properties* tab.
4. Tick the **Enable Communications Redundancy** checkbox. The fields in the dialog will be enabled.
5. Tick the **Allow incoming Connections** checkbox if you want the SiPass Server to be able to dial in to the ACC.
6. Enter the number of the first modem connected to the SiPass Server into the first **Server Phone Number** field.
7. If you are only using one modem to dial in to the Server, enter the same number into the second **Server Phone Number** field.
8. If two modems are connected to the SiPass Server, enter the number of the second modem into this field.
9. Complete the fields in the **Other Properties** section:
   – The command list must be terminated with the ‘^M’ character.
10. Select from the drop-down box in the **Unit Connection** section the RAS connection used to connect back to the SiPass Server.
11. Click **Save**.

12.6.4.1 Dialup ACC Options

The following table explains the configuration options for dialup ACCs.

Option	Description
ACC PPP Address	The PPP Address of the connection on the remote ACC. Note that this is different to the TCP/IP address configured for the PC during initial installation.
Host PPP Address	The PPP Address of the connection on the SiPass Server. Note that this address is different to the TCP/IP address of the Server PC.
Subnet Mask	The Subnet Mask (if applicable) used to access ACCs on the remote network.
Idle Timeout (min)	The length of time after which, if there is no communication either from or to the ACC, the ACC will disconnect the Dialup connection to the SiPass Server.
No. of Retries	The number of times the ACC will attempt to dial the first phone number. If there has not been a successful connection, the ACC will attempt the same number of tries on the second phone number, and continue to alternate between the two numbers.
Baud Rate	The baud rate of the serial dialup connection. This should be set to the next fastest speed above the baud rate of the modem connected to the ACC.
Modem Initialization String	The commands that are sent to a modem prior to sending information; for example, to turn off sounds or to disable a certain communications mode. Consult your modem's User Guide for a list of commands
Dial Server When	The number of Audit Trail messages that accumulate in the ACC Audit Trail buffer before the ACC dials the SiPass Server to upload.

13 Elevators

SiPass integrated can control the access of cardholders and the public to particular floors, and the times during which they may access those floors. Floor access control privileges are assigned to cardholders in exactly the same manner as access to doors.

The ACC maintains a database of cardholders and access control privileges. When a cardholder presents his/her card to the card reader located inside an elevator car, the controller reads its database and establishes the floors to which they have access. Only those floors will be made available to the cardholder.

It is also normal for floors to be unsecured during particular times of the day. For example, during office hours where any member of the staff or public can access a company's floors. The Time Schedule downloaded to the controller determines when floors are secured (access privileges are required) or unsecured (anyone can access the floor).

In high-rise residential buildings, visitors generally require access to elevators after being allowed into the building via the tenant's intercom unit.

The following table explains some of the key terms used to describe Elevator and Access Control systems:

Term	Description
Bank	A bank is a group of one or more elevators that service identical floors. A bank can also be known as a "Rise" or a "Group".
Floor	A floor is a level in a building at which an elevator can stop and take on or release passengers. In SiPass integrated, a floor is treated like an access point; it can be assigned a Time Schedule, and a cardholder can be granted permission to access the floor.
Elevator (Car)	This is the physical carriage which carries passengers. A card reader located inside the elevator car allows cardholders to badge their card before selecting a secure floor.
Floor Group	A group of one or more floors. A floor group is treated like a point group in SiPass integrated; actions can be performed on the entire group, and floor groups assigned to access levels.
Crossover Floors	In tall buildings with very many floors, there may not be an elevator or bank that services every floor in the building. A crossover floor is a floor that is common to a set of elevators, some of which service lower floors, some of which service upper floors.
Unserviced Floors	Floors which are not serviced by a particular elevator or bank.
Fire Override (FOR)	Fire Override refers to the ability to modify the access control behaviour of an elevator system in the event of a fire or emergency. The default Fire Override behaviour will depend upon the legal requirements for elevator systems in your location.
Access Control System (ACS)	The application responsible for managing access to floors by cardholders.
Low Level Interface (LLI)	In a Low Level Interface, the ACS is also responsible for energizing and de-energizing the buttons located inside the elevator car. The ACS interfaces with the elevator itself by way of hardware called a Service Interface Module (SIM). In SiPass integrated, the role of a SIM is carried out by the Output Point Module (OPM), which connects to the buttons inside the elevator car.

13.1 Elevator Control

There are two individual systems that control the operation of elevators. The Elevator Management System regulates and controls the mechanical operation of the elevators, while the Access Control System regulates the access of elevators to floors.

This section details how the Access Control system is configured, from both a software and a hardware perspective, to provide correct elevator operation and a level of security.

Floor security is controlled via a hardware (low-level) interface; in this case, an Output Point Module, or OPM. The inputs and outputs of the OPM are connected to the buttons inside the elevator car, and enable or disable them according to whether a cardholder has access permissions to that floor or not.

Low Level Elevator Control incorporates relay-logic. Relays are energized and de-energized to activate and de-activate the security of floors, according to the Time Schedule and cardholder access control privileges.

- Requires an Output Point Module (OPM) for every 16 floors.
- Fire override is accomplished by the OPM.

13.2 Fire Override

This section applies only to setting up Low-Level Elevator Control.

Fire Override (FOR) refers to the override of access control during an emergency by the Elevator Management or Fire systems. FOR is carried out as a result of a trigger, usually a FOR Input like a fire alarm. The trigger may come from SiPass integrated or another application, but SiPass integrated receives and forwards a trigger through the FOR inputs and outputs on the OPM.

When a Fire Override input on an OPM is activated, it de-energizes the outputs on that OPM. This in turn de-energizes the elevator buttons connected to the outputs, making those floors accessible in an emergency. This allows any passengers inside the elevator car to exit safely at any floor, and permits access to the elevators by passengers wishing to leave a floor.

In practice however, fire regulations in your region may require different behavior from the Elevator Management System. For example, in an emergency situation, it may be required that elevators travel to the nearest floor, open the doors and then are disabled until reset by a master control.

For an exact description of how Fire Override must be carried out in your jurisdiction, consult the local fire regulations and the Elevator Management System manufacturer.

13.2.1 Fire Override and Wiring

Whether or not Fire Override is implemented at a facility will affect how OPMs are wired to each elevator. As stated in the previous section, triggering the FOR inputs will de-energize the outputs on an OPM, unsecuring the corresponding floors.

If there is an overlap between OPMs – that is, if the outputs on one OPM are shared between elevators – this means with FOR enabled, both elevators will be affected if the FOR input is triggered. Such a scenario may not be desirable; for example, independent elevator operation may be required in an emergency situation.

This requires therefore that sites with FOR enabled be wired with no overlap.

A third scenario also exists, as the OPM actually has two FOR inputs which can independently control blocks of up to eight outputs. This allows you to keep independent control of elevators for sites with a small number of floors and/or elevators.

13.3 Setting up an Elevator System

Setting up a low-level elevator system in SiPass integrated requires a knowledge of how the SiPass integrated system hardware has been wired to the Elevator system; specifically, the order in which input and output points on the Output Point Module(s) have been wired to the destination floor buttons inside the elevator car.

There are seven major steps in configuring a low-level elevator system in SiPass integrated:

- Pre-configuration
- Configure the ACC Elevator Controllers
- Configure the Output Point Modules used to connect to the Elevator system
- Configure the Reader Interface Modules inside each Elevator Car
- Configure the Banks
- Configure the Floors in each Bank
- Configure the Elevators

13.3.1 Low-level System Pre-Configuration

This section explains how to work out the requirements for your facility's elevator access control system, and how the Fire Override wiring of your system will affect its configuration under SiPass integrated.

The following are the theoretical maximums that may be configured for a single ACC:

Component	Theoretical Maximum
Banks	64 per controller
Elevators	255 per controller
Floors	255 per system
Cardholders	Up to 1 million per controller

In a real scenario however, the actual maximums will be less. Possible reasons for this are as follows:

- One OPM may only connect up to 16 floors
- If FOR is required you may not overlap floors between OPMs.
- One ACC may only connect up to 36 OPM devices (6 per FLN Channel)
- One reader is required for each elevator car that accesses secure floors.

13.3.2 Defining the Advanced Central Controller (ACC)

The Advanced Central Controller stores the cardholder floor access privileges, including floor Time Schedules, and communicates with OPMs and the Elevator Management System.

Defining an Elevator Controller is the same as defining an access controller, as described earlier in the section Adding an ACC [➞ 28].

A High Level Interface can be configured on FLN1/FLN 2/FLN3. Hence any of these three FLN's can be used to configure HLI on the ACC-Granta unit.

13.3.3 Defining the Output Point Modules (OPM)

The OPM is connected to the floor buttons inside the elevator car, and permits access to secure floors if the cardholder has the correct privileges.

1. Select **Components** from the System toolbar or menu.
2. Select the ACC and then the FLN channel to which the OPM will be connected.
3. Choose **New Device**, and select OPM from the menu.
4. Enter a suitable name for the OPM into the **Name** field.
5. Select an Alarm Class for the OPM from the **Alarm Definitions** drop-down menu.
6. Click **Save**.

Input and Output points that are used for elevator access control do not need to be configured from the Components dialog. Any settings in the *Input* and *Output* tabs for these points will be over-ridden by the settings in the *Elevator Configuration* dialog, and these points will be disabled in the Components dialog if assigned to an elevator.

Input and Output points that are used for other purposes, like duress buttons or PIRs, are configured from the *Components* dialog as per System Components.

13.3.4 Defining the Card Readers

A Reader Interface Module (RIM) must be configured inside each elevator car. The RIM allows cardholders to badge their card and attempt to access secure floors. A RIM inside an elevator car can either be a DRI (Dual Reader Interface) or an SRI (Single Reader Interface).

1. Select **Components** from the **System** toolbar or menu.
2. Select the ACC and then the FLN channel to which the RIM will be connected. Choose **New Device**, and select DRI or SRI from the menu. A new device will appear in the **Components** tree and several new tabs will appear. In this example we will choose an SRI.
3. Enter a descriptive name for the SRI into the **Name** field.
4. Select an Alarm Class from the **Alarm Definitions** field.
5. Select the *Reader* tab.
6. Select an Alarm Class for the reader from the **Alarm Definition** drop-down box.
7. Select the correct operation mode from the **Operation Mode** drop-down box. The mode will determine how the SRI should operate.
8. Select the Time Schedule during which the daily code is enabled from the **Daily Code Time Schedule** drop-down box.
9. Complete the following fields, as they apply:
   - **Host Verify Timeout**:
     The time in seconds that the Image Verification dialog will wait for a response from an operator, before closing and allowing access to be re-attempted.
   - **PIN Timeout**:
     The time in seconds that a cardholder has to enter a PIN on the keypad. The timeout begins once the first digit is entered, or a card is badged and the reader is set to Card and PIN operation mode.

- **Daily Code**:
  The daily code for this reader. This may or may not be the same daily code used at other access points.
- **Daily Code No. of Digits**:
  The exact number of digits in the daily code.

10. Tick the **Void Card After 3 Wrong PIN Entries** checkbox, if you want any card that enters a wrong PIN number three times at this reader to be temporarily voided.
    - To re-activate a card that has been temporarily voided after 3 wrong PIN entries: In the *Cardholder* screen uncheck the **3 PIN disabled** box
11. Complete the *Input/Output* and *Image Verification* tabs, as described earlier in this manual.
12. Click **Save**.

13.3.5 Defining the Banks

Banks are groups of one or more elevators that service the same floors. Elevator components including Banks, Floors and Elevators are configured in a separate dialog, called Elevator Configuration.

1. Select **Elevator** from the **System** menu or toolbar.
2. Select the ACC Elevator Controller for which you are defining a Bank, from the **Components** tree. Select the **Bank Wizard** option in the *ACC details* tab, or right-click and select **Create Bank** from the menu. A Bank will appear under the ACC in the **Components** tree and a new tab will appear.
3. Enter a descriptive name for the Bank into the **Bank Name** field.
4. Select “Low” from the **Bank Type** drop-down menu. The options available in the **Bank Type** menu will depend on the options you have chosen in the *Validity Check* dialog during SiPass integrated installation.
5. Click **Save**.

13.3.6 Defining the Floors

You must define which floors that a bank will service. Defining the floors for a single bank may require more than one use of the Bank Floor Wizard. The Wizard is designed to easily “correct” the type and number of floors in a bank. This means you can configure the below-ground floors for a bank first, assigning them a unique label, and then add the above-ground floors later using a different label.

The following terms are used when defining floors:

- Rise Number

Rise Numbers are an internal address used by SiPass integrated as a reference for the floor, to be passed to the Elevator Management System. Each floor in the building is assigned only one Rise Number.

In SiPass integrated, Rise Number 1 normally represents the lowest possible serviceable floor in the building; for example, Rise Number 1 could be Basement Level 3.

- Floor Number

Floor Numbers are user-assigned labels, and are not used in SiPass integrated for anything other than indicating the position of the floor with respect to Ground.

Defining the floors in a bank

1. Select **Elevator** from the **System** menu or toolbar.
2. Select from the **Components** tree the Bank for which you are defining the floors.
3. Select the **Floor Wizard** option, or right-click on the Bank and select **Bank Floor Wizard**.
4. Choose **Next**.
   - The **Floor Name Prefix** field indicates the text that will be used when these floors appear in SiPass integrated dialogs; for example, “Above Ground”. The default is the Bank Name.
   - The **Floor Name Postfix** field indicates the text that appears before the floor number, when these floors appear in SiPass integrated dialogs; for example, “Floor” or “Level”. The default is “Floor”.

Every floor in SiPass integrated must have a unique name.

5. Enter into the **Rise Numbers** field the floors you are defining to be serviced by this bank. Single floor numbers are separated by commas. You can use a dash to represent a range of serviced floors, and use a comma to separate Rise Numbers; for example “1-4, 9-20’.
   ⇨ The **Current Rise Numbers** field indicates the Rise Numbers that you have already defined for this Bank. You can override currently defined floors by re-entering all or some of the current rise numbers into the **Rise Numbers** Field. Entering additional Rise Numbers will add those floors to existing floors for this Bank. Only the **Time Schedule**, **Alarm Class** and **Enabled** fields will be over-ridden if you re-enter defined Rise Numbers. Floor names are only changed through the Floor Name column of the *Bank Floor details* tab.
6. Complete the **Floor Number Suffix** details:
   - **Append Number**:
     Tick this checkbox to append the Floor Number to the Floor as it appears in SiPass integrated dialogs.
   - **Keep Rise Increments**:
     Tick this checkbox if you want to match the increments in Floor Numbers to increments in the Rise Numbers. For example: the numbers “1-3, 5-7, 11-20” are entered into the Rise Numbers field, and the Start Number is 4. The corresponding Floor Numbers for this group of floors would be “4-6, 8-10, 14-23”.
   - **Start Number**:
     Select where to begin numbering floors.
   - **Ascending/Descending**:
     Tick the appropriate option to count upwards or backwards from the Start Number when assigning Floor Numbers.
7. Select a **Time Schedule** that will be applied to every floor selected. Individual floor Time Schedules can be changed later.
8. Select an **Alarm Class** that will be applied to every floor selected. Individual floor Alarm Classes can be changed later.
9. Select from the **Floor Enabled** drop-down box whether all floors will be enabled or disabled by default.

10. Choose **Finish**.

    ⇨ You will be returned to the *Elevator Configuration* dialog. A table of floors will have been created under the selected Bank.

11. You can modify the properties of individual floors by clicking in the appropriate cell and selecting or entering a new value. This allows you to define groups of floors with the same attributes and then alter details for particular floors later.

    – Disabling a floor means that it will not be accessible from any elevator in the bank.

12. Click **Save**.

13.3.7 Defining the Elevators

Defining an elevator requires that you select the OPM inputs and outputs that are connected to the floor buttons in that elevator.

1. Select **Elevator** from the **System** toolbar or menu.
2. Select the **Bank** in the **Components** tree for which you are defining an elevator.
3. Select **Elevator Wizard** from the *Bank Details* tab, or right-click on the Bank and select **Create Elevator**.
4. Choose **Next**. The **Select OPMs** list lists all of the Output Point Modules (OPM) that you have defined through the *Components* dialog. Ticking the checkbox next to an OPM will list all of that OPM's available input and output points in the two columns to the right. Multiple OPMs may be selected. You can re-order the points in the input/output lists by clicking and dragging the OPMs in the Select OPMs list. Points will be listed in order of OPM. Ticking a checkbox next to an Input point or Output point indicates that it should be assigned to a floor. Any surplus inputs or outputs that have been ticked will be ignored.

    – SiPass integrated will assign all ticked Input points and Output points to serviced floors in the order they appear in the *Bank Floor Details* tab.
    – For example, an elevator services from the Ground Floor to Floor number 12, and the OPM wired to this elevator is called "OPM Elevator 1". The first input on this OPM is connected to the button for Ground Floor, the second input is wired to the first floor button, and so forth, until 13 inputs have been assigned.

5. Ticking the **Match IN/OUT** checkbox will match input point selections to outpoint point selections.
6. Un-tick the **Floor Reporting** checkbox to disable Floor Reporting. That is, if OPM input points are not used for floor reporting for this elevator.
7. Ticking the **Invert Input** checkbox will set the default Invert Input for each floor.
8. Choose **Finish**. A new elevator will be created under the selected Bank and a new tab will appear containing the details you entered in the Elevator Wizard.
9. You can enter a new name for the elevator into the **Name** field if required.
10. Select the Reader located in the elevator car from the **Reader** drop-down box.

11. Enter an ID to be assigned to this elevator from the **ID** field. Each Elevator must have a unique ID number. In a Low Level Interface, the Elevator ID is assigned by the Access Control System (SiPass integrated).
    - The value in the **Delay** field represents the time allowed between a valid card badge and being able to select a secure floor. If a floor has not been selected within this Time Schedule (and Floor Reporting is enabled), the floor buttons will be re-secured and the person will have to badge the card again to attempt access.
12. Tick the **Inputs Inverted** checkbox to invert the input received from this elevator's input and point points by SiPass integrated. Only values in the **Input Point** / **Output Point** columns may be changed in the table.
    - Individual floors cannot be added or removed from single Elevators. This is because each elevator in a Bank must service exactly the same floors. If you want to add or remove serviced floors from elevators, you must either create a new Bank for that elevator, or remove the floors from the Bank itself.
13. Click **Save**.

13.4 Access Control

Access to particular floors at a site is determined by the access privileges configured for the cardholder attempting to gain access (including the Time Schedule applied to those privileges).

For example, cleaners may be contracted to clean the first and second floors of a building. These floors have been assigned general public access during 8:00 am and 5:00 pm weekdays (anyone can access the floors during these times). Outside these hours, verification is required before access will be granted. However, the cleaners must clean the floors outside these hours. To prevent them from having access to the floors at all times, they are provided with access privileges to the floors between 9:00 pm and 11:00 pm on weekdays only.

If the cleaners attempt to access the floors between 9:00 and 11:00 pm, they will be granted access upon verification. If the cleaners attempt to access the floors outside these hours (other than the general public access hours), they will be denied access.

13.4.1 Assigning Floor Access to Cardholders

SiPass integrated treats floors like doors. A cardholder must badge their card before attempting “entry” and the floor button will only be enabled if they have the correct access privileges during that time. Floors can also be assigned to floor groups, which are just like point groups. Floor groups can be assigned to access groups in the same manner as access groups.

Creating a Floor Group

1. Select **Point Group** from the **Program** menu.
2. Enter a descriptive name for the floor point group into the **Group Name** field.
3. Choose **Add Members**.
4. Select **Floor Points** from the **Group Type** drop-down box.
   ⇨ The **Available list** will be populated with all of the floors that have been defined.
5. Select from the **Available list** those floors you want to add to the group.
6. Use the **Add** button to shift selected floors to the **Selected** list. The **Add All** button will select all floors.
7. Choose **OK**.
   ⇨ You will be returned to the **Point Group** dialog.
8. Select an Alarm Class for the **Floor Point Group**.
9. Complete the **Alarm Trigger** and **Group Action** fields.
   - **Group**:
     Specifies the number of group members that must be in alarm state, or have returned to normal but whose timers have not yet timed out, before the group goes into alarm. If 0 is entered, it prevents an alarm.
   - **Timer**:
     An internal timer starts counting (in seconds) for each member of the group that was in alarm after it returns to normal. The group goes into alarm if the number of points counting down or currently in alarm reaches the Group Count. If a point times out, the current count is decreased by one. This means that if a certain number of group members have entered an alarm state simultaneously or in a configurable time interval, the group alarm will be generated.
   - **Isolate**:
     When checked, disables the group messages. However, individual member messages will still appear in the Active Audit Trail window.
   - **Clearance Required**:
     When checked, the member(s) that caused the group to enter an alarm state must be restored before the group can return to normal.
10. Click **Save**.

Assigning Floors and Floor Groups to a Cardholder

1. Select **Access Level** from the **Program** menu or toolbar.
2. Enter a descriptive name for the Access Level into the **Name** field.
3. Select the **Time Schedule** during which access to the Selected Points or Point Groups is possible. The **List View** button displays all defined **Access Levels** by **Time Schedule**.
4. Select either Floor Point or Floor Point Group from the **Type** drop-down box. The floors or floor point groups you have defined will appear in the list below.
5. Select those points or groups from the list, and choose **Add** to add them to the **Selected** list above.
6. When you have selected all the items you want to add to the Access Level, choose **Save**.

14 Guard Tour

Guard Tour is used to monitor the movement of security guards throughout your site and ensure that they visit and check their assigned tour points at the required times. An operator can start a guard tour, and add, delete or modify the details of guards and guard tours. Tour groups can be created to assist with the management and choice of tours. Guard Tour monitors a guard's progress around the points of contact or stops that make up a tour. These points or tour stops are configured from those defined in the SiPass integrated database.

14.1 Configuring Guard Tour

In order to operate guard tour on-site, specific components are required to be configured. These include:

- Adding a Guard to the system
- Creating a Tour
- Defining a Group of tours

14.1.1 Adding a Guard to the System

For a cardholder to be configured as a guard, they must already be defined as a cardholder in the SiPass integrated system.

Registering a cardholder as a guard does not affect the cardholder's status in any other part of the SiPass integrated system. Being registered as a guard simply means that the cardholder can be assigned to tours.

From time to time, it may be necessary to view the details of cardholders prior to being configured as guards. It is also a simple way to verify that the person is a defined cardholder within SiPass integrated.

Viewing Cardholder Details

1. Select the **Program > Guard Tour > Guards**.
2. In either the *Members of* SiPass integrated list or the *Members of Guard Tour* list, highlight an Cardholder whose details you wish to view.
3. Select the **Details** button.
4. Select the **Close** button to exit from the *User Details* dialog.

Adding a Guard to the system

1. Select the **Program > Guard Tour > Guards**.
   ⇨ The **Guard Specification** dialog will appear, displaying a list of Cardholders available for configuration as guards.
2. From the *Members of SiPass* integrated list, select the desired Cardholder(s). Hold down the CTRL or SHIFT keys on the keyboard to select multiple records.
3. Select the **Add** button.
   ⇨ The selected member(s) will be added to the *Members of Guard Tour* list.
4. Repeat Steps 2 and 3 until all the required Cardholders have been added to the *Members of Guard Tour* list.
5. Click **Save**.

14.1.1.1 Creating a Tour

A guard's tour is the primary component of Guard Tour and consists of two main elements:

- The guard
- The physical journey through the site

Each tour is assigned a name and is defined by the points that the guard must visit to complete their security check.

There are two types of tours:

- Ordered Tours
- Random Tours

All tours, irrespective of their type, consist of points to be visited and the expected times of arrival at those points. A configurable tolerance either side of the expected time of arrival allows guards to carry out their rounds with some flexibility without jeopardizing security at your site.

Ordered Tours

Since a tour is made up of the points that the guard must visit in order to complete their rounds, the guard must check those points in the sequence specified. The guard will be informed of the stopping pattern via a report that is normally prepared by the operator prior to tour commencement.

This type of tour ensures compliant guard behavior during tours. Guards are compelled to followed pre-defined routes and carry out specified card reader activities during the course of their tour, thereby ensuring that all the points on the tour are visited according to tour parameters.

Random Tours

A Random Tour, sometimes referred to as an Unordered Tour, is one that is created by the system. The points are identical to those in an ordered tour at the same site, except that the visiting pattern is generated randomly.

The visiting pattern for a Random Tour is generated randomly when the tour is registered with the guard. It is not feasible to require the guard to visit any one point of a Random Tour within a certain time frame, simply because there is no effective method to predict the interval required to travel between any two tour points.

However, a time restriction is applied for the completion of the whole tour. This ensures that the tour is completed within the designated time frame.

The greatest advantage to be gained from using random tours is that they prevent the tours from becoming predictable to an outside observer. This enhances the effectiveness of security guards.

Tour Completion Time

Guard Tour allows a guard a certain amount of time to proceed from one point to the next. This time can be specified exactly. However, you can also specify a tolerance either side of the expected time of arrival to allow for unforeseen circumstances, such as bad weather. If the guard arrives early at a designated point outside the specified bandwidth (Tolerance), an Early alarm is raised. If the guard takes more than the maximum allowable time to reach the point (expected time of arrival plus the tolerance), a Late alarm is raised.

This feature is useful for two reasons. Firstly, it will assist in ensuring the personal safety of the guard force by triggering an alarm when a tour point is not reached due to restraint or assault. Secondly, if guard activity is under scrutiny as part of normal management practice, it also provides the operator with more effective control over both the tours and guards.

Each tour created by Guard Tour has several parameters that are required to be set. These parameters apply to both Ordered and Random tours. The parameters are as follows:

- Net Expected Time
- Tolerance

The Net Expected Time refers to the total time to complete the tour.

The Tolerance refers to the allowable time either side of the expected time of arrival at each point. The Tolerance value that appears in the dialog applies to each point and can be adjusted if required.

Assigning these times prevents a guard from taking too long to complete the security check, or from hurrying through the tour so they can rest at their desk.

Grace Period

Normally, a tour is completed when the guard has visited all of the tour stops in the tour.

Examples of these situations are:

- When a guard has missed a tour stop on a tour
- When a guard has quit a tour without visiting all of the tour stops on a tour
- When a guard is running extremely late for the last tour stop on a tour

Under these conditions, the indication of appropriate alarm states in the SiPass audit trail cannot be shown and a “Grace Period” may come into effect.

The “Grace Period” defines a period of time between when the last event was received or expected and when the tour can be completed, and it is unlikely that any further events for that tour are to be received.

By default, the “Grace Period” is set to 30 minutes. The “Grace Period begins when:

- A random tour is marked as running late
- The last tour stop in an ordered tour is late (or visited)

The “Grace Period” is reset if a tour stop is visited after either of the events above has occurred AND before the tour is set to Completed.

Checking a Point

Guards must show that they have visited tour points by performing the points’ defined actions.

Tour points can be one of two types:

- Access - If it is an access point, this will require a card swipe, set with the appropriate mode of operation. (These are indicated in the Tour Definition dialog).
- Input - If it is an input point, the point must change state. The type of sensor attached to the point will determine the action required by the guard. No authentication will take place. The system “assumes” the identity of the guard.

Elevator access points (floors), areas and sub-areas are not supported by Guard Tour.

Creating a Tour

▷ Ensure that you have correctly configured the card readers at your facility.

1. Select **Program** > **Guard Tour** > **Tours**.
   ⇨ The *Tour Definition* dialog will appear, displaying a list of available points.
2. To enter the name of a new tour, select the **New** button.
3. Enter the name of the tour in the **Enter New Tour Name** field. All tour names must be unique.
4. Choose the **OK** button.
5. Check the **Default Start as Ordered Tour** checkbox, if your wish the tour to be an Ordered Tour. Leave this checkbox empty, if you wish the tour to be Random.
6. From the **Available Points** list, highlight the first point that you wish to include in the tour.
   – Points configured for Image Verification can not be included in a guard tour.
7. Select the **Add** button.
   ⇨ The point will be added to the **Tour Order** list.
8. Repeat the previous two steps until all the desired points have been added to the tour.
   ⇨ All points added to a tour are automatically assigned default values. The default values are detailed in the **Default Values** table at the end of this section.
9. Alter the values for each of the tour stops added in the tour to suit this distance and time required between stops
10. Alter the sequence of points, if required.
11. Enter the **Random Tour Details**.
12. Enter the total time to complete the tour in the Net Expected Time field.
13. Enter the allowable tolerance for the whole tour in the **Tolerance** field.
14. Click **Save**.

Aspect	Point Type	Default Value
Time	Access / Input	4 minutes
Tolerance	Access / Input	2 minutes
Card Req	Access Only	Yes
Card Req	Input Only	No
Disabled	Access / Input	No

Table 1: Default Values

14.1.2 Creating a Tour Group

The Tour Groups option is used to define a collection of tours based on those already defined in the system. A Tour Group usually consists of tours that are logically similar. Tour Groups enable an operator to select a random tour for a guard, and still retain some control over the selected tour. Defining a Tour Group consists of adding or removing tours to or from a group.

1. Select **Program > Guard Tour > Tours.**
2. Select the **New** button.
3. Enter the name of the Tour Group in the **Enter New Tour Group Name** field. All Tour Group names must be unique. If you attempt to assign the name of an existing tour group an error dialog will appear.
4. Select the **OK** button in the **New Group Name** dialog.
5. Select the newly created Tour Group from the **Tour Group Name** field. From the **Available Tours** list, highlight the tour that you wish to add to the Tour Group.
6. Select the **Add** button.
   ⇨ The tour will be added to the Tours in **Group** list.
7. Repeat Steps 6 and 7 for each tour that you wish to add to the Tour Group.
8. Click **Save**.

14.1.3 Starting and Monitoring Tours

Once you have successfully logged into SiPass integrated, Guard Tour starts automatically and runs in the background, until required. Guard Tour uses its own window to show guard-related activity, similar to the Active Audit Trail.

The Guard Tour window is displayed by selecting the **Guard Tour** button on the main SiPass integrated toolbar, The **Guard Tour** button has its own associated toolbar that appears directly below the main toolbar.

14.1.3.1 Registering and starting a Tour

Registering a tour consists of selecting tour parameters and starting a tour, effectively creating a guard and tour combination. It is a five-stage process involving both the *Register* dialog and the *Guard Tour Monitor* screen. These stages are as follows:

- Determining the status of the tour (Ordered or Random)
- Selecting a tour
- Selecting a guard for the tour
- Selecting the tour properties
- Starting the tour

Starting a Tour

1. Select **Data > Guard Tour Status**.
2. If you wish to randomly select a tour, tick the **Use Random Tour Selection** checkbox. Guard Tour will then select a tour at random from those available in the database. When you choose to select a tour at random by ticking this checkbox, the **Random Tour from Group**, **Select a Tour Group** and **Select a Tour** fields will be disabled.

3. If you wish to further refine your selection of a tour from a particular Tour Group, Select a Tour Group from the **Select a Tour Group** field and then check the **Random Tour from Group** checkbox. Guard Tour will select a tour at random from the nominated Tour Group. When you choose to select a tour at random from a particular Tour Group, the **Select a Tour** field will be disabled. This will prevent you from selecting a tour yourself from the Tour Group.

The **Checkbox Combination** table at the end of this section, describes the effect of various checkbox combinations.

1. If you wish to select guards at random, tick the **Use Random Guard Selection** checkbox. This will disable the **Select a Guard** field and a guard will be chosen at random from those available. If you wish to manually select a guard, leave the checkbox vacant.
2. If you have chosen to manually select a guard in Step 5, choose a guard from the **Select a Guard** field.
3. Complete the **Tour Properties**.
   - **Radio Controlled**:
     When this checkbox is ticked, it implies that some form of verification process should be in place
   - **Ordered checkbox**:
     This checkbox allows the operator to override the tour type as specified in the *Tour Definition* dialog. The value displayed will default to that of the original configuration for the selected tour.
4. Complete the **Start** Options.
   - **Start Immediately**:
     This indicates that the tour will begin as soon as the SiPass operator has selected the **Register** button. When starting tours in this way, ensure that a time has been allowed for the guard to reach the first tour stop.
   - **Start on First Tour Stop**:
     This indicates that the tour will start as soon as the guard reaches the first tour stop and badges their card. When starting a tours in this way, ensure that the time to reach the first point in the tour has been set to ‘0”.
5. Select the **Register** button. The *Tour Selection* dialog will appear containing details of the Guard / Tour pairing.
6. Select the **Yes** to begin the tour with the selected options.

Option	Checkbox Combination	End Result of Configuration
1	**Use Random Tour Selection**	This combination of checkboxes sets the tour selection process to random and then automatically directs the system to select a tour at random from all those available. However, the options to manually select a specific Tour Group and then to select a tour from within that group will be disabled.
2	**Random Tour From Group**	This combination of checkboxes sets the Tour Group selection process to manual. However, the selection of tours from a Tour Group is disabled.
3	**No Selection**	This combination of checkboxes sets the tour selection process to manual. You may select any valid combination of tour group and guard.

Table 2: Checkbox Combinations

14.1.3.2 Monitoring Tours

Guard Tour allows you to closely monitor guard activity through the *Guard Tour Monitor*. In addition to providing the current status of any given tour, the *Guard Tour Monitor* alerts you to any potential problems, early or late arrivals by guards and reports the progress of each tour under way.

When you start Guard Tour, the *Guard Tour Monitor* screen appears and may or may not contain tour information. This will depend upon whether or not there is any pending or currently running tours at the time of start up. The *Guard Tour Monitor* displays the configured settings, in tabular form, for the tours that are either under way or pending.

To open the Guard Tour Monitor:

- Select **Data > Guard Tour > Status**.

⇨ The **Guard** field (column) displays icons indicating the status of tours. These assist in readily identifying the progress of tours displayed in the *Guard Tour Monitor* screen.

14.1.3.3 Displaying Tour Stop Log

Guard Tour allows you to view the details of a tour as it progresses, from within the *Guard Tour Monitor*. This information can be used to assist with the management of this and any other tours that are scheduled.

1. From the *Guard Tour Monitor*, highlight the tour whose details you wish to view.
2. Double-click the mouse. The *Tour Stop Log* dialog will appear containing current details of the tour points and the guard activity for each. From this dialog, you can view the progress of the tour and identify any points where problems have occurred or are likely to occur. The **Tour Stop Log** fields are described in the **Tour Stop Log Fields** table at the end of this section.
3. Select the Close button to close the *Tour Stop Log* dialog.

Field	Description
Name	This field displays the name of the tour point. The first record in the list is the name of the tour.
Status	This field displays the current status of the points; i.e., the activity logged by the guard at each of the points in the tour. The Status field incorporates an icon to provide a visual reference of the status of the tour.
Occurred	This field displays the time at which the guard activity, if any, has taken place.

Table 3: Tour Stop Log Fields

14.1.3.4 Printing a Guard Tour Report

Guard Tour provides a facility to prepare and print detailed tour reports for use by either the operator or the guards. These tour reports are normally prepared immediately prior to commencing a tour. In addition, you can prepare historical reports on the activity of Guard Tour for review and auditing purposes.

- Mobile / Pager
- Two-way radio

“Self-guided” tours by the guards require that they be given copies of the report, and place the obligation on them to conduct the tour as per the list of tour points and time limits in the report. The following steps explain how a Guard Tour Report can be printed.

1. From the *Guard Tour Monitor*, highlight a tour from which you want to create a report.
2. Select the **Print** button. The report will be created.
3. Select the **Report Preview** button.
4. Select the **OK** button to close the *Print Setup* dialog.
5. Select the print icon at the top of the screen.
6. The standard *Windows Print* dialog will appear.
7. Complete all the required details.
8. Select the **OK** button. The report will be printed.

⇨ When the report is printed it will contain all the necessary information for the guard to complete their tour.

14.1.3.5 Starting a Tour from the Guard Tour Monitor

Once a tour has been created and moved to the Guard Tour Monitor, it can be started immediately or at the discretion of the operator. The physical tour by the guard should commence at or about the same time.

▷ Ensure that the guard is actually available for the tour that you are about to commence.

▷ Ensure that you have printed out the appropriate report for the guard to use on their tour.

▷ Ensure that the guard has received a copy of the tour report and they have familiarized themselves with the tour.

▷ Ensure that you have advised the guard of any unusual circumstances that may affect the progress of the tour, such as Disabled points.

1. Select **Data > Guard Tour Status**.
2. From the displayed list of pending tours, highlight the tour that you wish to start. Pending tours can be identified by their status. All pending tours have a status of “Ready”.
3. Select the **Start** Button.

⇨ The tour will commence.

14.1.3.6 Stopping a Tour

Guard Tour allows you to stop a tour at any time. Stopping a tour can be done for a number of reasons; for example, a guard may be unable to continue because he has deviated from the tour, or due to other unforeseen circumstances.

1. From the **Guard Tour** menu, select **Monitor**, or select the **Status** button from the **Guard Tour** toolbar. The *Guard Tour Monitor* screen will appear.
2. Highlight the tour that you wish to stop from those that are currently running. All active tours will have a status of “Running”.
3. Choose the **Stop** button. The tour will be stopped.
4. A number of events will then take place:
   - The audible alarm will sound, requiring an appropriate response.
   - The tour icon will change from GREEN to RED.
   - The status of the tour will change to “Completed”.
   - Messages will be passed to the SiPass audit trail indicating which tour stops have been visited.
   - A message will be passed to the SiPass audit trail indicating that the tour has been stopped.
5. Choose the **Alarm** button to acknowledge and silence the alarm.

⇨ By pressing this button, the system is advised that there has been a response to the alarm.

14.1.3.7 Skipping a Tour Point

Guard Tour allows the guard to skip tour points. A tour point can be skipped if, for example, it has been taken out of service to be repaired. The points are generally shown as Disabled in the Tour Report and may be subject to alternate checking procedures by the guard.

- You can only skip the next tour point in the sequence. There is no option to skip a tour point out of sequence.
- You cannot skip points in a tour that is not already running.
- You cannot skip points that have already been visited.
- You cannot skip points in a Random Tour.

1. Select **Data > Guard Tour Status**.
2. From the tours that are currently running, double-click the tour that contains the point you wish to skip.
3. Highlight the tour stop that you wish to skip.
4. Choose the **Skip** button.

⇨ The icon associated with the skipped tour point will change accordingly and the tour point’s Status will change to “Skipped”. This point in the sequence will be ignored by the system and no alarm will be triggered as a result.

⇨ The internal timer for that point will be stopped and re-set. In the case of an Ordered tour, the internal timer will be re-set to show the remaining time to arrive at the next point. In the case of a Random tour, the internal timer will not change.

When a tour point is skipped, a message to that effect is passed to the SiPass integrated audit trail and the status of the point is updated to “Skipped” in the Tour Stop Log dialog.

14.1.3.8 Acknowledging an Alarm

When you stop a tour for any reason or if a guard is early or late when arriving at a tour point, an audible alarm will be triggered by Guard Tour.

1. Select **Data > Guard Tour Status**. The *Guard Tour Monitor* screen will appear. You will notice that the background color of the icon associated with the tour that has gone into an alarm state has changed from GREEN to RED.
   – Guard Tour alarms are not propagated to the SiPass integrated Status Bar Alarm Panel.
2. Select the tour in which the alarm has occurred.
3. Choose the **Alarm** button. The audible alarm will be silenced and the tour record will remain visible in the Guard Tour Monitor for one minute. In the case where an alarm is triggered by a late arrival by a guard at a tour point, or a missed tour stop, the tour will remain displayed on the Guard Tour Monitor until the tour is completed (“Grace Period” timeout) or until stopped by the operator.
4. To find out why the alarm was raised, double click on the selected tour, to display the *Tour Stop Log* dialog. This dialog will show any tour stops that have triggered an alarm due to the late or early arrival of guard, or if the tour has been stopped all together.
5. Carry out any designated response to the alarm.

It is not necessary to halt the tour in order to respond to a raised alarm. All raised alarms will log an entry to the SiPass Audit Trail.

14.1.3.9 Aborting a Tour

Guard Tour allows you to cancel a tour prior to its commencement, or abandon a running tour. Although you can abort a tour that is already running, the Abort option is primarily used to abandon a tour prior to its commencement. It is recommended that, where you wish to abandon a currently running tour, you use the Stop option.

1. Select **Data > Guard Tour Status**.
2. Highlight the tour that you wish to abort from those displayed in the list.
3. Choose the **Abort** button.

⇨ The tour will be aborted.

⇨ The tour record will remain in the *Guard Tour Monitor* for a period of one minute and then be deleted.

No audible alarm will sound. However, a message will be passed to the SiPass audit trail indicating that the tour has been aborted. The principal difference between “Stopping” a tour and “Aborting” a tour lies in the fact that when a tour is stopped prematurely, this causes an alarm condition.

14.1.3.10 Guard Tour Window

The Guard Tour window is used to display the details of currently running tours. The fields in the table are described below.

Column Name	Description
Guard	This column displays the name of the guard assigned to the tour.
Tour	This column displays the name of the tour.
Last Point	This column displays the name of the last tour point visited by the guard.
Next Point	This column displays the name of the next scheduled tour point to be visited.
Time	This column counts down the remaining time to reach the next tour point.If the guard arrives at the tour point ahead of schedule, the countdown values will display as positive (+) values and if they arrive after the scheduled arrival time, the values will display as negative (-). The internal timer will continue to operate until the guard reaches the next point or until re-set by the operator.
Tolerance	A guard may be early or late when visiting the next point. This column displays the time range either side of the scheduled time of arrival that is allowable by Guard Tour. If they arrive at the tour point outside this allowable time range, an alarm will be triggered and displayed in the SiPass audit trail to alert the operator. As the tour progresses, the tolerance value is subject to a cumulative effect in random tours and may display a value as high as the total of the tolerances for all of the configured tour points. In a random tour, it is possible for the guard to catch up over the total tour time, depending upon the circumstances under which the tour is being conducted.

14.1.3.11 Right Mouse Button Options

By right-clicking the mouse button inside the Guard Tour Monitor Window, you can access an alternate series of options:

Option	Description
Print Tour	This option allows you to create and print a tour report for the tour that you have selected.
Acknowledge Alarm	This option is used to silence the audible alarms that occur when guards arrive late or early at tour points.
Start Tour	This option allows you to start a tour.
Stop Tour	This option allows you to stop a tour or to formally shut down a completed tour.
Abort Tour	This option allows you to abort a tour prior to its commencement
Close	This option allows you the close the Guard Tour Monitor.
Report Preview	This option allows you to preview a report.

15 Biometric Integration

15.1 Introduction

The Bioscrypt functionality allows operators to capture fingerprint templates and encode the fingerprint template into the smart card during enrollment.

An optional feature allows operators to capture and store the fingerprint template into the SiPass integrated database. This feature is configurable based on the individual country regulations regarding fingerprint storage.

This functionality allows operators to encode fingerprint templates as cardholder data into the smart card, while enrolling the card at the same simultaneously.

It supports the 1K and 4K Mifare cards, and the 2K, 4K and 8K DESFire Card Technology.

It utilizes the Triple DES (also known as 3DES), mechanism for encryption.

The Bioscrypt reader can be connected to RIM devices (DRI, ERI and SRI) for Access Control.

15.1.1 Prerequisites

Before proceeding to create a Bioscrypt components in SiPass integrated, the operator must ensure that the following prerequisites are available with the SecureAdmin application.

- Install the Server and Client of the **SecureAdmin version 4.1.9**.

After the SecureAdmin application is installed, the documentation for the application should also be available on your PC. Please refer the same for information on how to use the application.

- Register the **BIOSCRYPT V-Station** reader in SecureAdmin. Please refer the Secure Admin documentation for detailed information on how to register.
- Configure the **Wiegand** output for the BIOSCRYPT V-Station reader. This can be done through the following steps:

1. Navigate through **Device Settings** to locate the *Wiegand* tab of the BIOSCRYPT V-Station device.
2. In the *Miscellaneous Settings* section of this tab, check the **Activate Wiegand Output** checkbox.
3. Select **Always Output** in the adjacent dropdown field.
4. Next, operators can choose to configure either a Mifare Classic or Mifare DESFire card template. For details, refer the two sections that follow.
5. Click the **Wiegand Output Settings** button. Set **Verification Output.**
6. Proceed to create a **Site Key** to authenticate the Mifare Smart Card. A detailed guide for the same can be found in the **SecureAdmin** documentation.
   ⇨ While enrolling Mifare cards for a site, set the 'Key B' for Read/Write operations or select the **Use ESI Site Key encryption** option to prevent the default Key A being assigned to all the cards.
7. Set the **Site Key** and **Smartcard Layout** on the BIOSCRYPT V-Station reader. Refer the SecureAdmin documentation to set the Site Key.
8. Open the **SmartCard Device Manager** and ensure that the Use Wiegand String option is ticked for every device integrated into the system. **Overwrite Card Wiegand String** should also be ticked for Mifare DESFire card.

To configure the Mifare Classic card template:

▷ The custom format is used to send the **CSN** number of cards that use the Mifare Classic card technology.

1. Click the **Custom Wiegand Settings** button, and configure the template in the *Weigand Format* dialog displayed.
2. Enter the **Name** of the configuration.
3. Enter **Length** as 40.
4. In the **Weigand ID** settings, Enter **Start Position** as 0, **Length** as 32, **Heart Beat Value** as 0.
5. In the **User fields** settings, specify the following information:
   - Name – Successful code
   - Start Position – 32
   - Length – 8
   - Success Value – 0
   - Failure – 250
6. Click **Apply**.

This configuration is required only if the system is required to configure the Mifare Classic card.

To configure the Mifare DESFire card template:

▷ The Card Type has to be set to DESFire to configure a DESFire card. To select the card type as DESFire, perform the following steps:

1. Click the **Smart Card** tab from **SecureAdmin** to open the *Smart Card Device Manager dialog.*
2. Select **DESFire Smart Card** from the *Smart Card Type pop-up.*

▷ The custom format is used to send the UID number of cards that use the Mifare DESFire card technology.

1. Click the **Custom Wiegand Settings** button, and configure the template in the *Weigand Format* dialog displayed.
2. Enter the **Name** of the configuration.
3. Enter **Length** as 72.
4. In the **Weigand ID** settings, Enter **Start Position** as 0, **Length** as 64, **Heart Beat Value** as 0.
5. In the **User fields** settings, specify the following information:
   - Name
   - Start Position -64
   - Length-8
   - Success Value-0
   - Failure-250
6. Click **Apply.**

This configuration is required only if the system is required to configure the Mifare DESFire Classic card.

In case of L1 readers using Mifare DESFire cards, the Master key should not be modified. If changed, the key will not be read by the L1 reader.

15.2 Configuring the Bioscrypt Bus

This section details the steps required to configure a Bioscrypt bus in SiPass integrated.

1. Select **System > Components** on the SiPass integrated main menu to open the *Components* dialog.
2. Selected the SiPass integrated server required.
3. Click the **New Bus** button, and select **Bioscrypt System**.
4. Enter a name for the bus in the **Name** field.
5. Enter the **Site Key**. The Site Key entered here should match the Site Key configured in SecureAdmin. The Site Key should be of 12 digits.
6. In the Biometric Quality Section, configure the expected quality of the fingerprint. Adjust the **Minimum Quality** and the **Minimum Content** of the finger print.

Note: In order to be accepted by the SiPass integrated system, fingerprints presented through the Bioscrypt reader must meet the minimum standards set in the **Minimum Quality** and **Minimum Content** fields. By default the Minimum Quality and Minimum Content is 50.

7. Click **Save**.

⇨ The Bioscrypt bus will be saved with the configured settings.

⇨ **The ACC should be initialized for changes to take effect.**

See also

Introduction [→ 236]

15.3 Saving the Custom Card Configuration

1. Select **System > FLN Configuration** from the SiPass integrated main menu to open the *FLN Configuration* dialog.
2. Expand the **Global Settings** item in the tree hierarchy on the left hand pane.
3. Select the *Custom Card Format* tab.
4. Click the **Add** button.
   ⇨ The *Custom Card Configuration* dialog appears with a default configuration. Change the default configuration of the Custom Card Configuration according to the below steps.
5. Enter a new **Name** for the custom card to be used for the Bioscrypt functionality.
6. Set the **Total Length** field from **1 to 40** for **Mifare smart card** and **1 to 72** for **DESFire smart card**.
7. Set the **Number** field from **1 to 32** for **Mifare smart card** and **1 to 64** for **DESFire smart card**.
8. Un-tick the **Facility** field checkbox.
9. Tick the **Revision** field checkbox, and set this field from **33 to 40 for Mifare smart card** and **65 to 72 for DESFire Smart Card**.
10. Un-tick the **Even Parity** and **Odd Parity** fields.

11. Click **OK** to save the custom card configuration.
    ⇨ The newly created custom card configuration is added to the *Custom Card Format* list.
12. Navigate to the door reader device being used in the *FLN Configuration* dialog from the tree hierarchy.
13. Click the *Configuration* tab for the device.
14. Ensure that **Custom Card (Wiegand)** is selected in the **Technology** field.
15. In the **Configuration** field, select the newly created custom card (Mifare/DESFire) format from the drop down list.
16. Click the **Save Configuration** button to save the custom card configuration.
17. Click the **Close** button.

15.4 Creating a Bioscrypt Credential Profile

1. Select **Program** > **Credential Profil**e from the SiPass integrated main menu to display the Credential Profile dialog.
2. Select the **Base** card profile.
3. Verify if **Bioscrypt Credential** is checked for this profile.
   – **Note**: The Bioscrypt credential checkbox will appear in the *Credential Profile* dialog only after a bioscrypt system bus is created in the *Components* dialog.
4. Click **OK** to save this profile.

15.5 Determining the Bioscrypt / Enrollment Reader Configuration

The Bioscrypt reader and the Enrollment reader can be configured in SiPass integrated for the Bioscrypt functionality. The operators can decide if they require an enrollment reader, apart from the Bioscrypt reader; in which case, they will need to configure an enrollment reader in the Enrollment Configuration dialog. The enrollment reader has to be configured to import a Bioscrypt Profile.

The steps required to configure a Bioscrypt and Enrollment reader in SiPass integrated are explained in the sections that follow.

15.5.1 Configuring the Bioscrypt reader in SiPass integrated

Please note that the configuration explained in this section is client-specific.

Configuring the Bioscrypt Reader in SiPass integrated

1. Select **Options > Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select **Bioscrypt Reader Configuration**.

Please note that the **Encode** button of the *Cardholder* dialog will be disabled if the Bioscrypt reader configuration is the only card reader added in the **Select Type** field of the *Enrollment Reader Configuration* dialog.

4. Tick the **Reading** checkbox if you wish to use the Bioscrypt Reader only to read the card.
5. Or else, tick the **Encoding** checkbox if you wish to use the Bioscrypt Reader to encode the card. Ticking the **Encoding** checkbox ticks the **Reading** checkbox by default.

The options available in the *Fingerprint Enrollment* section of this dialog, determine the various functionalities that can be configured. The table below explains the options.

Configuration Option	Expected Configuration Action
Prompt to encode the fingerprint on card	When this option is ticked, the Bioscrypt device is used to encode the fingerprint template on the card. When this option is un-ticked, the system saves the acquired fingerprint to be stored in the SiPass database.
Use Card Serial Number as Template Identifier	When this option is ticked, the fingerprint template will be identified by the Card Serial Number (CSN) of the card. When this option is un-ticked, the fingerprint template will be identified by the card number given in the *Definition* tab of the *Cardholder* dialog. If no card number was specified, the user is notified that a card number is required to complete the card assignment operation.
Store the fingerprint for encoding later	When this option is ticked, the fingerprint will be saved to the database as part of the enrollment process.

For **Configuration Type A: Card Assignment** – **Prompt to encode the fingerprint on card** and **Use Card Serial Number as Template Identifier** options should be checked.

For **Configuration Type B: Fingerprint Accquisition** – **Use Card Serial number as Template Identifier** and **Store the fingerprint for encoding later** options should be checked.

1. In the *Communication Settings* section of this dialog, do the following:
2. Enter an appropriate value for the Bioscrypt device in the **Device ID** field. The Device ID value for Bioscrypt reader shall match the Device ID value set in the Communication tab of SecureAdmin.
3. Specify the type of connection to the Bioscrypt reader in the **Connect Using** field.
4. Enter the IP address of the Bioscrypt device in the **IP Address** field.
5. Click **Save** to save this configuration.

15.5.2 Configuring an Enrollment Reader for the Bioscrypt functionality

Configuring the enrollment reader for the Bioscrypt functionality

If you wish to use an enrollment reader as part of the Bioscrypt functionality, the reader needs to be configured in the Enrollment Reader configuration dialog.

The option to use the enrollment reader to read, search and assign cards will be enabled in the *Cardholder* dialog, only when the enrollment reader is configured to the **Reading** mode in the *Enrollment Reader Configuration* dialog. This action ensures that the **Read**, **Assign** and **Read & Search** buttons of the *Cardholder* dialog will be made drop-down buttons, to allow selection of the reader device to be used.

1. Select **Options > Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select the enrollment reader to be used for this functionality.
4. Tick the **Reading** checkbox of the **Operation Mode** field.
5. In the **Profile Name** field, select the Bioscrypt profile from the drop down list.
6. Set the **Sector / Application** in the fields.
7. Select the port to be used for the enrollment reader in the **Port Name** field.
8. Click **Save** to save this configuration.

15.6 Importing the Bioscrypt Reader Configuration

The user can import a Bioscrypt profile into SiPass integrated by using the *Profile Configuration* dialog.

▷ Ensure that the Bioscrypt Reader has been configured in SiPass integrated. Refer Configuring the Bioscrypt reader in SiPass integrated [→ 239] on how to configure a Bioscrypt Reader.

1. Click **System > Profile Configuration** from the SiPass integrated main menu.
2. Enter a new **Profile Name** for the Bioscrypt profile.
3. Select a **Card Type**.
4. Click the **Import** dropdown button, and select **Bioscrypt Reader Configuration** to import the Bioscrypt reader configuration into this dialog.
   ⇨ The reader configuration layout gets automatically imported from the reader into SiPass integrated, and is displayed on this dialog. After importing the Bioscrypt profile, the user can change or add new fields to the profile as needed.

Next, a new Sector Key needs to be configured for this configuration.

1. Click the drop down arrow of the **Keys** button.
2. Select between Mifare Key or DESFire Key.

Each profile created by SiPass integrated can have only one Bioscrypt binary data.

⇨ This action displays the *Keys Configuration* dialog.

3. Enter a new **Key Name**.
4. Enter the transport keys of the Mifare card in the *Smart Card Keys* section of this dialog.
5. Tick the **Overwrite the Sector Key** checkbox if you want to overwrite the sector key.
   - The Site Keys entered here must match the Site Key entered in the Components dialog while creating the Bioscrypt bus.
   - If the length of the Site Key is less than 32 digits, it should be appended with zeroes to fill 32 digits if DESFire key is used.
   - The File ID should be the same that has been configured in the Bioscrypt system. Refer the section Configuring Bioscrypt bus for more information.

Next, each sector of the Bioscrypt Profile needs to be configured with the newly created Site Key.

1. To do this, double-click each Key icon corresponding to a sector of the profile. A drop-down list is displayed.
2. Select the new Site Key for the Bioscrypt profile from this list, and continue to configure this key to all the remaining sectors of this profile.
3. Click the **Save** button to save this configuration.

For detailed information on configuring a card profile, please refer the section Creating a Smart Card Profile [→ 163]

See also

Configuring the Bioscrypt Bus [→ 238]

15.7 Configuring the Bioscrypt profile to a Work Group

This section details the steps required to configure a new workgroup with the Bioscrypt profile.

1. Select **Operation > Work Group** on the SiPass integrated main menu to open the *Work Group* dialog.
2. Configure a New Work Group.
3. Click the drop down arrow of the Profile field, and select the Bioscrypt smart card profile created.
4. Click **Save**.

15.8 Types of Bioscrypt Configuration in SiPass integrated

SiPass integrated can be configured to work with the Bioscrypt reader in two ways, each providing a different functionality. A brief explanation of each configuration type follows.

Card Assignment

This configuration type allows operators to use the SiPass integrated interface to select cardholders for whom fingerprints are required. The Bioscrypt reader is then used to obtain the cardholder's fingerprint, and assign a card with fingerprint details written to it.

In this case, the fingerprint template is not saved to the database. In is only saved to the card assigned.

Fingerprint Acquisition

The functionality of this configuration builds on the result of Configuration Type 1, where a cardholder is assigned a card containing their fingerprint information. However, in this type of configuration, SiPass integrated also saves the fingerprint to the database for future use.

15.8.1 Configuration Type A: Card Assignment

Through this configuration, the operator selects a cardholder in SiPass integrated, whose card will then be assigned and written with their fingerprint data using the Bioscrypt reader device. A summary of the configuration stages required for this scenario is detailed below.

Summary of Configuration Stages for Type I

▷ Ensure that you have installed the SecureAdmin client and server software.

▷ Ensure that you have created a Bioscrypt bus in SiPass integrated.

▷ Ensure that you have saved the custom card configuration in SiPass integrated.

1. Configure the Bioscrypt Enrollment Reader in SiPass integrated through the *Enrollment Reader Configuration* dialog. For further information, refer the section Configuring the Bioscrypt Reader for Configuration I [→ 243].
2. Use the *Cardholder* dialog to begin scanning a fingerprint on the Bioscrypt reader, and assigning a card with the fingerprint. For further information, refer the section Assigning Fingerprints and Cards with the Bioscrypt Reader [→ 244].

The sections that follow explain each of these configuration stages in detail.

15.8.1.1 Configuring the Bioscrypt Reader for Configuration I

The Bioscrypt reader can be configured to read and encode the fingerprint template onto a card in this type of configuration, without saving the card template to the database.

- Follow the steps described in the section Configuring the Bioscrypt reader in SiPass integrated [→ 239].

Ensure that **Prompt to encode the fingerprint on card** option is checked on *Enrollment Reader Configuration* dialog.

15.8.1.2 Assigning Fingerprints and Cards with the Bioscrypt Reader

Once operators have created a Bioscrypt bus, and the enrolled a Bioscrypt reader in SiPass integrated, they can proceed to assign cards with fingerprints using the Bioscrypt reader. This is done on the *Cardholder* dialog. The instructions that follow explain this process.

1. Select **Operation** > **Cardholder** on the main menu to display the *Cardholder* dialog.
2. Click the **Assign** drop down button, and select **Assign fingerprint from Bioscrypt reader**. The drop-down appears only if multiple readers have been connected to SiPass integrated.
   ⇨ *Register Card with Fingerprint* dialog will be displayed.
3. Follow the instructions of the dialog to acquire a fingerprint.
4. When a satisfactory fingerprint has been obtained, the *Cardholder* dialog prompts to register the fingerprint with a card.
5. Place the card on the Bioscrypt reader to assign the fingerprint to the card.
   ⇨ The card number will be displayed on the *Cardholder* dialog. And an icon is displayed on the definition tab of the cardholder indicating that fingerprint is on the card.
6. Configure all other required cardholder details.
7. Click **Access Privileges** button, select the access points for the cardholder and click **OK.**
8. Click **Save**.

⇨ As a result of this configuration, the acquired fingerprint gets physically assigned to a card using the Bioscrypt reader. This is also indicated by an icon.

You can inspect the card after acquiring the fingerprint.

- In the *Cardholder* dialog, click **Read** drop-down and select **Inspect Bioscrypt Card.** *Read Card* dialog shows up**.** Place the card on the Bioscrypt reader.

⇨ The Bioscrypt reader reads the card and shows the biometrics stored on the card.

You can verify the card details by doing the following steps:

1. Badge the card on the Bioscrypt reader; follow the instruction on the reader and present fingerprint.
2. If the card is valid then it is notified to the user by an audit trail message which says **Valid**. If the card is invalid then it is notified to the user through an audit trail message which says **Invalid**.

15.8.2 Configuration Type B: Fingerprint Acquisition

This functionality allows the operator to use SiPass integrated to encode a card that has already been assigned fingerprints through the Bioscrypt reader.

A summary of the configuration stages required for this scenario is detailed below.

Summary of Configuration Stages for Type I

- ▷ Ensure that you have installed the SecureAdmin client and server software.
- ▷ Ensure that you have created a Bioscrypt bus in SiPass integrated.
- ▷ Ensure that the Bioscrypt Reader Configuration has been imported for the purpose of configuring the smart card profile. For more information, refer the section Importing the Bioscrypt Reader Configuration [→ 241].
- ▷ Ensure that a Bioscrypt profile has been configured for a work group. For more information, refer the section Configuring the Bioscrypt profile to a Work Group [→ 242]

Make sure, in the *Enrollment Reader Configuration* dialog, under the **Fingerprint Enrollment** section, the **Use Card Serial Number as Template Identifier** is unchecked and **Store the fingerprint for encoding later** option is checked for this configuration.

1. Configure the Bioscrypt Enrollment Reader in SiPass integrated through the Enrollment Reader Configuration dialog. For further information, refer the section Configuring the Bioscrypt Reader for Configuration II. [→ 245]
2. Use the Cardholder dialog to begin scanning a fingerprint on the Bioscrypt reader, and assigning a card with the fingerprint. For further information, refer the section Card Enrollment with Bioscrypt Details. [→ 241]
3. The sections that follow explain each of these configuration stages in detail.

15.8.2.1 Configuring an Enrollment Reader for Configuration II

The Bioscrypt reader must be configured in SiPass integrated. This section details the steps required to do this.

It is important to note that the configuration explained in this section is client-specific.

1. Select **Options** > **Enrollment Reader Configuration** on the SiPass integrated main menu.
2. Click the **Add** button.
3. From the **Select Type** drop down list, select **Profile Reader – OmniKey CardMan 5×21**. Ensure that the **Bioscrypt Reader Configuration** is also added as part of this drop down list. Ensure that the **Encoding** is checked.

Note that on selecting this reader type, the **Encoding** checkbox gets ticked by default and the **Profile** section of this dialog becomes enabled. The OmniKey CardMan 5×21 reader is used to read both Mifare and DESFire cards.

4. From the **Profile Name** drop down list, select the card profile to be used for the bioscrypt card enrollment.

5. Enter the **Sector/ Application** for the profile selected. (Sector is entered for Mifare card. Application is entered for DESFire card)
6. From the **Port Name** drop down list, specify the port name of the card reader.
7. Click **Save** and **Close**.

⇨ The enrollment reader will be now be enrolled in SiPass integrated.

15.8.2.2 Card Enrollment with Bioscrypt Details

Once operators have created a Bioscrypt bus, enrolled the Bioscrypt reader, and imported a Bioscrypt Profile in SiPass integrated, they can proceed to assign cards with fingerprints using the Bioscrypt reader. This is done on the *Cardholder* dialog. The instructions that follow will explain this process

Ensure that the Bioscrypt smart card profile is selected in the **Profile** field of the *Advanced* tab on the *Cardholder* dialog.

Assigning a fingerprint to the card

1. Select **Operation** > **Cardholder** on the main menu to display the *Cardholder* dialog.
2. To assign a finger print to a card, place the card on the Enrollment Reader.
3. Click **Assign** to get the CSN number. The CSN number is displayed in the **Card Number** field of on the *Cardholder* dialog.
4. Enter the required cardholder details like the First Name, Last Name, Workgroup, etc.
5. Click the **Access Privileges** button, select the access points for the cardholder and click **OK.**
6. Click the **Assign** drop down button, and select **Acquire fingerprint for base card from Bioscrypt reader.**
7. Follow the instructions on the dialog to acquire a fingerprint.
8. You can repeat the previous step to capture additional fingerprints. However, only 2 fingerprints can be saved in the system.
9. The **Finger Prints** section of the *Advanced* tab will display a new row for the captured fingerprint. If you have captured multiple fingerprints, select the rows that you do not require, and click the **Delete** button to remove these rows.
10. In the **Index** field, click to select the finger name that was used for the fingerprint capture.
11. In the **Credential Profile** field, select a credential profile to which this fingerprint should be saved.
12. Click **Save**. The fingerprint/s will be saved in the SiPass integrated system. The system indicates this by displaying a ticked **Saved** checkbox for the fingerprint that was saved.

13. Click **Read & Search** button to read the contents of the card placed on the reader. An icon is displayed on the cardholder dialog which depicts fingerprint is on the card as well as on the disk.
14. Click **Encode**. The fingerprint/s will be encoded to the card. The SiPass system indicates this by displaying a ticked **Encoded** checkbox for the fingerprint that was encoded to a card.

    ⇨ Smart Card encoding successful message is displayed to the user.

⇨ As a result of this configuration, the fingerprint gets encoded to a card using the Bioscrypt reader.

You can inspect the card after acquiring the fingerprint.

- In the *Cardholder* dialog, click **Read** drop-down and select **Read card from Profile Reader – OmniKey CardMan 5×21.** *Read Card* dialog shows up. Place the card on the Bioscrypt reader.

⇨ The Bioscrypt reader reads the card and shows the biometrics stored on the card.

You can verify the card details by applying the following steps:

1. Badge the card on the Bioscrypt reader; follow the instruction on the reader and present fingerprint.
2. If the card is valid then it is notified to the user by an audit trail message which says **Valid**. If the card is invalid then it is notified to the user through an audit trail message which says **Invalid**.

16 Intrusion Arming Terminal (ATI5100 / IAT-010)

The IAT-010 is an Intrusion Arming Terminal, developed to efficiently secure and provide privileged access to high security intrusion areas.

The ATI5100 is referred to as the IAT-010 within the SiPass integrated software.

Utilizing the existing SiPass integrated access control architecture, the IAT-010 device can be easily configured into the system to allow cardholders with access privileges to arm or disarm intrusion areas. Audit Trail messages will appear in SiPass integrated as the arming status of each intrusion area changes.

Partial Arming is another key feature of the IAT-010. This feature allows the cardholder to arm / disarm perimeter points alone, and allow movement to continue in the remaining areas.

All these features have been explained in detail in the sections that follow.

The IAT-010 does not support Sintony Intrusion Areas.

16.1 IAT-010 Terminal Types

An IAT-010 (ATI5100) can be configured to function as either of the following terminal types:

- Intrusion Terminal
- Intrusion Terminal with Access Control

The configurations required for both these terminal types will be explained in detail in the sections that follow.

Intrusion Terminal

- When the Intrusion Terminal is configured to this mode, it may be used only for Intrusion Control.
- In this mode, the cardholder uses the IAT-010 keypad to enter a valid PIN number and thereby change the arming state of the intrusion areas configured to the terminal.

Intrusion Terminal with Access Control

- When the Intrusion Terminal is configured with Access Control, it can be used for Intrusion Control as well as for Access Control.
- When configured with Access Control, the IAT-010 terminal is assigned to a door reader, and is operated by the reader operation mode configured in SiPass integrated. When configured to this mode, the IAT-010 keypad is not represented as an access point in the system.

16.2 Configuring a New Intrusion Terminal (Standalone)

This section explains how the user can create a new IAT-010 (ATI5100) device as an Intrusion Terminal (standalone).

1. Discover a new IAT-010 device on the *FLN Configuration* dialog
2. Configure a new IAT-010 device on the *Components* dialog
3. Assign the IAT-010 to an intrusion area as an arm/disarm point
4. Configure an Access Level with the intrusion area, and assign it to an access group
5. Enter the PIN on the IAT-010 terminal to arm / part-arm / disarm the intrusion area

Each of the steps mentioned above, have been detailed in the sections that follow.

16.2.1 Configure / Discover a New IAT-010 Device

An operator can configure / discover a new IAT-010 device can be done in either of the following ways:

- Discovering the IAT-010 device through the *FLN Configuration* dialog,

OR

- Creating a new IAT-010 device on the *Components* dialog

Although either of these methods can be used to create a new IAT-010 device, it is recommended that the operator utilize the *FLN configuration* dialog. The following sections will explain how to discover and create an IAT-010 device on the *FLN Configuration* dialog.

Discovering the IAT-O10 device on the FLN Configuration dialog

The following steps explain how the IAT-10 device can be discovered from the FLN Configuration dialog:

1. Select **FLN Configuration** from the **System** menu.
2. Right-click the respective ACC and select **Search Exhaustive**.
   ⇨ This action will search for and display devices that have been physically connected to the ACC. The user will notice that the new IAT-010 device appears at the FLN that the device was physically connected to. Further, note that the **Device Number** will also be displayed on this tab.
3. Locate the **Terminal Type** on the **Device Details** tab
4. Select **Intrusion Terminal**.
5. Provide a name for this Intrusion Terminal in the **Name** field.
6. Click **Save New Device**.

Creating a new IAT-O10 device on the Components dialog

The operator also has the option of creating and configuring this device on the *Components* dialog. The following steps can be used for this option:

1. Open the *Components* dialog.
2. Select the appropriate FLN under the respective ACC, to which the ATI5100 device has been physically connected.
3. **Click New Device** and select **IAT**.
4. Enter a name into the **Name** field on the *Device* tab of this new item.
5. Ensure that the **Device Numbe**r is correct. (To retrieve the right device number, run an **Exhaustive Search** as described in the section Discovering Devices [→ 33] of this user manual.
6. From the drop-down list of the **Terminal Type** field, select the type of intrusion terminal you want to configure.
7. Click **Save New Device**.

16.2.2 Configuring the IAT-010 device on the Components Dialog

The following section explains how to configure a new IAT-010 device on the *Components* dialog:

1. Open the *Components* dialog.
2. Expand the given FLN under the respective ACC. The IAT-010 device 'IntrusionTerminal-Standalone' that was saved in the *FLN Configuration* dialog will appear under the given FLN.
3. Verify the **Device Number** of the IAT-010 on this dialog.

If a correct device number has not been entered into this field, the user will not be able to save the device. If saved without the right device number, the device will appear to be offline.

The user will be able to confirm the right device number from the respective device information provided in the *FLN Configuration* dialog. This will be discussed in the following section.

4. Select the *Keypad* tab of this new IAT-010 device.

The *Keypad* tab appears for IAT-010 device only when it is created as an Intrusion Terminal (standalone). It will not appear when the device is created with Access Control.

5. The **Name** field is entered by default. Select the required **Alarm Definitions**.
6. Set the Time Schedule to **Always (point unsecure)**.
7. Enter the timeout for PIN entry in the **Command Timeout (sec**) field. By default, this field is set to 10 seconds.
8. Click **Save**.

⇨ Once these selections have been saved, the **Current State** field is displayed as '**Enabled'**.

Please ensure that the input point to be assigned to the Intrusion Area has been configured to the Intrusion Area Entry / Exit Operation Mode on the *Input / Output* tab of the associated reader.

16.2.3 Assigning an IAT-010 to an Intrusion Area as an Arm/Disarm Point

The operator will now have to create an intrusion area with arm / disarm, entry lockout and input points. Please refer the section Configuring an Intrusion Area [→ 76] this user manual for information on how to configure an intrusion area.

To configure an input point for part-arming, please refer to the sections under Partial Arming / Part- Arming [→ 256] of this user manual.

16.2.4 Configuring an Access Level and an Access Group, with the Intrusion Area

In this step, the operator will have to configure an Access Level to include the Intrusion Area on the *Access Level* dialog.

Next, the operator will need to add this Access Level to an Access Group on the *Access Group* dialog.

16.2.5 Configuring a Cardholder's Access Privilege with the Access Group

As the next step, the operator has to configure a valid cardholder's Access Privilege to include the Access Group. This can be done by using the **Define Access Privileges** button on the *Cardholder* dialog.

The defined privileges should be then saved on the *Cardholder* dialog.

16.2.5.1 Configuring the IAT-010 Terminal to Arm / Part-arm / Disarm the Intrusion Area

Next, the operator needs to configure the IAT-010 Terminal to arm / part-arm / disarm the intrusion area.

1. Tick the **PIN as Card** checkbox and click **Save**.
2. The **Pin Number** field on the *Cardholder* dialog will provide a valid PIN number. Enter this Pin Number on the intrusion terminal keypad. Press the **Enter** key.
3. The terminal will provide options for Arm / part-arm / disarm of the Intrusion Area. Selecting the appropriate options will allow the user to effectively utilize the Intrusion Arming Terminal in the **Standalone** mode.

For information on how to operate the IAT-010, please refer to the *ATI5100 Operations Manual.*

16.3 Overview of Configuring an Intrusion Terminal with Access Control

This section explains how the user can create a new IAT-010 device with Access Control in the *Components* dialog.

1. Discover the IAT-010 device on the *FLN Configuration* dialog
2. Configure the new IAT-010 device on the *Components* dialog
3. Link the IAT-010 device to a door reader
4. Create an Intrusion Area specifying Arm / Disarm, and Input (Aux) points
5. Configure an Access Level with the Intrusion Area, and the Access Point. Assign it to an Access Group.
6. Configure a cardholder's Access Privilege to include the Access Group
7. Operate the IAT-010 according to the configured Operation Mode of the door reader

These steps have been explained in detail in the sections that follow.

16.3.1 Discovering the IAT-010 Device

This section details the steps required to discover the new IAT-010 device on the FLN Configuration dialog.

This can be done in either of the following ways:

- Discovering the IAT-010 device on the *FLN Configuration* dialog
- Creating a new IAT-010 device on the *Components* dialog

Although either of these methods can be used to create a new IAT device, it is recommended that the operator utilize the *FLN configuration* dialog.

16.3.1.1 Creating a new IAT-010 device on the Components dialog

1. Select **Components** from the **System** menu or tool bar.
2. Expand the given FLN under the respective ACC.
   ⇨ The IAT-010 device that was saved in the FLN Configuration tool will appear under the given FLN.
3. Select this new IAT-010 device. Verify its Device Number and ensure that its Status is **Online**.

Please refer section Configure / Discover a new IAT-010 device [→ 249] for information on using the *Components* dialog to create a new IAT-010 device, instead of the *FLN Configuration* dialog.

16.3.1.2 Discovering the IAT-010 device on the FLN Configuration dialog

1. Select *FLN Configuration* dialog from the **System** menu.
2. Right-click the respective ACC and select **Search Exhaustive**.
   ⇨ This action will search for and display the devices that have been configured to the ACC. The user will notice that the new IAT-010 device appears at the FLN it was created under. Further, note that the **Device Number** will also be displayed on this tab.
3. Enter a name for the device in the **Name** field.
4. Locate the **Door Set** on the *Device Details* tab.
5. Select **Intrusion Terminal with Access Control**.
6. Click **Save New Device**.

16.3.2 Linking a Door Reader to the IAT-010 for Intrusion Control

This section details the steps required to link reader to the newly created ATI5100 device for intrusion control.

An IAT-010 can be linked to any RIM device (DRI, SRI, ERI).

1. Select an available DRI from an FLN bus on the ACC.
2. Select either *Door Reader 1 / Door Reader 2* tab of the DRI.
3. Select the *Intrusion Control* tab of this Door Reader.
4. In the **Terminal Device** field, select the created IAT-010 device from the drop down menu.
   ⇨ Once a Terminal Device has been selected, the other reader will not be configurable for the same Intrusion Terminal.
5. From the **Time Schedule** field, specify a required time-schedule.
6. Click **Save**. Once these selections have been saved, the **Current State** field of this tab displays the device as **Enabled**.
7. On viewing the tab of the newly created IAT-010 device, the user will note that the **Linked Reader** field displays the door reader that was configured for intrusion control with this device.

Please ensure that the input point to be assigned to the Intrusion Area has been configured to the **Intrusion Area Entry / Exit** Operation Mode on the *Input / Output* tab of the associated reader.

16.3.3 Creating an Intrusion Area with Arm / Disarm and Input Points

The operator will now have to create an intrusion area with arm / disarm, entry lockout and input points. Please refer the section Configuring an Intrusion Area [→ 76] of this user manual for information on how to configure an intrusion area.

To configure an input point for part-arming, please refer the section Partial Arming / Part-Arming [→ 256] of this manual.

16.3.4 Access Level Configuration to include Intrusion Area and Input Point, and assigning of an Access Group

In this step, the operator has to configure an Access Level to include the Intrusion area and the Input point/s assigned to the IAT-010, using the *Access Level* dialog.

Next, the operator has to assign this Access Level to an Access Group, using the *Access Group* dialog.

16.3.5 Configuring a Cardholder's Access Privilege to the Access Group

In this step, the operator has to configure a valid cardholder's Access Privilege to include the Access Group. This can be done by clicking the **Define Access Privileges** button on the *Cardholder* dialog. This will bring up the *Define Access* dialog, where the user can select the access privileges to the configured to the cardholder.

16.3.6 Operating the IAT-010 Terminal to Arm / Part-arm / Disarm the Intrusion Area

This section describes the steps required to operate the IAT-010 Terminal to arm / part-arm / disarm the intrusion area.

1. Operate the IAT-010 terminal according the **Operation Mode** configured on the *Components* dialog.
2. Use the IAT-010 keypad to control the intrusion area.

16.4 Intrusion Control for Multiple Areas

The IAT-010 terminal can be used to arm / disarm / part-arm multiple areas. The user can then choose to operate on all the areas, or on a specific area alone.

Selection of the areas available to the user will depend on the Intrusion Area configuration, as well as User Privileges.

For example, consider a situation where the IAT-010 terminal is assigned as an arm / disarm point for areas A, B and C. However, a particular user has arming privileges only for areas A, B and D. In such a case, only areas A and B will be available to the user at that particular intrusion terminal.

16.5 Executing Manual Override commands for the IAT- 010 device

Manual commands can be used to override and control existing configurations of the IAT-010 device with SiPass integrated.

16.5.1 Manual Commands for the Standalone Intrusion Terminal

When configured as a standalone device, the user will only be able to send Intrusion Control commands using the IAT-010 device keypad as an Access point. The ACC does not support manual commands to allow access, block / lock door etc., when the standalone keypad is selected as an access point.

When the IAT-010 keypad is selected as the Access Point, only 6 manual commands can be configure for the Standalone IAT-010 device. These commands are as follows:

- Intrusion Control – Disable
- Intrusion Control – Enable
- Intrusion Control – Restore Config
- Reader Buzzer Off
- Reader Buzzer On
- Reset Reader Tamper

16.5.2 Manual Commands for the Intrusion Terminal with Access Control (linked terminal)

When configured as an Intrusion Terminal with Access Control (linked terminal), the ACC will support manual commands that are available for any access point.

16.6 Deleting an ATI5100 Device

In order to delete an IAT-010 device, it is mandatory that the user conform to an essential sequence of deletion.

The user will have to progressively delete every access level/s, Intrusion Areas where the IAT-O10 device exists, before finally deleting it from the *Components* dialog.

16.6.1 Deleting an Intrusion Terminal (Standalone)

In order to delete an Intrusion Terminal (standalone), the operator will need to apply the following steps:

1. Open the *Intrusion Area Configuration* dialog.
2. Select the *Intrusion Area Members* tab and remove the required Intrusion Terminal from the **Selected List**.
3. Click **Save**.
4. Next, open the *Components* dialog.
5. Select the required Intrusion Terminal, and click the **Delete** button.

⇨ The terminal will be deleted.

16.6.2 Deleting an Intrusion Terminal with Access Control

In order to delete an Intrusion Terminal with Access Control, the operator will need to apply the following steps:

1. Open the *Intrusion Area Configuration* dialog.
2. Select the *Intrusion Area Members* tab and remove the access point that the IAT-010 is linked to from the **Selected List**.
3. Next, open the *Components* dialog and select the *Intrusion Control* tab of the access point door reader.
4. Make a blank selection from the **Terminal Device** drop down menu.
5. Click **Save**.
6. This action will de-link this access point from the respective IAT-010 device.
7. Select the IAT-010 device to be deleted from the respective FLN, and click **Delete**.

16.7 Partial Arming / Part-Arming

In addition to Arming and Disarming an intrusion area, a user also has the option to Partially Arm / Part-arm the area. This functionality is called **Partial Arming** or **Part Arming**.

Consider an Intrusion Area where Input Points A, B and C are configured as Part-Arm. These points are called **Perimeter Inputs**.

Further, Input Points D and E of the same Intrusion Area are configured as Full-Arm.

When the area is part-armed, only part-armed (perimeter) inputs A, B and C become enabled.

When the area is armed, all the inputs A, B, C, D and E become enabled.

16.7.1 Configuring Input Points for Partial / Part Arming

In order to enable an input point for part / partial arming, the operator will need to configure the point accordingly, on the Intrusion Area dialog. This section explains how this can be done.

For both Intrusion Terminal types, the steps required to configure input points for part-arm are the same.

1. Select the **Input Point** of the Intrusion Area, on the *Intrusion Area Configuration* dialog.
2. From the **Intrusion Area Link** column, select the cell corresponding to the Input point required.
3. Right-click this cell and select **Part Arm**.
4. Click **Add**.
5. Click **Save** and **Close**.

16.8 Intrusion Terminal Alerts of Unsealed Inputs

- **Situation**: The user has selected an area to be armed / part-armed. However, the area is not ready to arm because of an unsealed input in the area. Further, the cardholder in this case, does not have Isolation Privileges.

  LCD Message:

  Intrusion Area 1

  Not Ready to Arm

  Press ? to list

  unsealed inputs
- **Situation:** If the user presses the **?** key on the IAT-010 terminal;

  LCD Message:

  Unsealed input –

  input 040101
- **Situation:** If there are more than 3 unsealed inputs;

  LCD Message:

  Unsealed inputs –

  Scroll for more –

  Input 040101

  Input 040102

  Input 040103

At this point, the user can use the **Scroll** button to move down and view the displayed list of unsealed points on the LCD screen.

In order to grant the cardholder Isolation Privileges to isolate the unsealed inputs, check the **Isolation** checkbox on the *Cardholder* dialog and save. This will give the cardholder privileges to isolate any unsealed input, and proceed to arm / part arm an intrusion area with unsealed inputs.

16.9 Isolation Privileges for Multiple Unsealed Inputs

- **Situation**: The user wants to arm an area with multiple unsealed points, and has been given Isolation Privileges. They will be offered an extra option to seal / isolate an unsealed input, instead of just viewing the list of unsealed inputs.

  LCD Message:

  Input 040101

  is unsealed

  Press <return key symbol> to seal

  ? for full list

If the user presses the **<Return>** key, the arming process will continue in the usual manner.

If the user presses the **<?>** key, the arming process will be terminated and the IAT-010 will display the list of unsealed inputs, as described in the previous section.

16.10 Trouble-Shooting

The following section provides important user information about how he can fix possible trouble-shooting situations.

The IAT-010 continues to remain offline after Component and FLN configuration

It needs to be mentioned that if the IAT-010 continues to remain offline even after FLN Configuration, the following problems could be considered:

- The ACC needs to be initialized. Please refer the section Initializing Units [→ 48] of this user manual for further details.
- The device has not been configured with the right device number.
- The IAT-010 has not been physically connected to the right FLN on the ACC.

The IAT-010 does not present intelligent characters / numbers on the LCD, on pressing the keys

Please ensure that the latest firmware of the ACC and the IAT-010 has been downloaded. For further information, please refer the section Device Firmware Download and Configuration [→ 42] of this user manual.

17 DVR

The SiPass integrated DVR solution allows SiPass to communicate with DVR equipment using a high level interface. This interface allows control and manipulation of the equipment connected to the DVR system, such as DVR units, cameras and auxiliary devices. The DVR High Level Interface allows you to view and record digital images from a SiPass workstation.

Whilst SiPass integrated supports many DVR systems, Siemens SISTORE DVR system is the recommended system for reliability and performance.

A DVR communicates with SiPass integrated workstations by TCP/IP protocol across an Ethernet network. This allows even greater flexibility when integrating your DVR camera system with the SiPass integrated access control and security system. You only need to connect a DVR to the network on which the desired SiPass DVR workstation is located.

If you only require the use of a single operator and therefore a single PC, the DVR Client files can be installed on the same machine that the SiPass server and Client are installed. If you require a separate SiPass workstation for viewing and recording functionality, the DVR Client files can be installed on a separate PC, along with a SiPass Client.

The SISTORE interface cannot be used to control PTZ type cameras, but can be used to control the recording mechanism on a SISTORE system.

DVR Configuration Summary

The following list provides a summary of the configuration and setup for the SiPass DVR option.

- Ensure that Windows and the same service pack have been installed on all PCs in the SiPass integrated access control and security network.
- If your access control and security network is to be configured using more than one PC, ensure that all machines are connected together using an appropriate communications protocol.
- Install the appropriate SiPass integrated software onto each PC in your access control and security network, ensuring that exactly the same version of SiPass integrated is used for all installed components.
- Ensure that the DVR system architecture has been planned in advance.
- Ensure that you have programmed the DVR unit using the System Administration software and that all DVR devices have been connected.
- Ensure that the DVR unit has been connected to the SiPass PC where the DVR bus service has been installed.
- Install the DVR Client files on the PC(s) where DVR images are to be viewed. Configure the DVR Client with the address and details of the DVR.
- Program and configure the DVR Bus and DVR using SiPass integrated.
- Program the necessary cameras and camera groups in SiPass integrated.

17.1 Programming SiPass integrated for DVR

In order for the SiPass DVR option to function correctly, SiPass integrated must be programmed with the appropriate data. This includes programming DVRs, DVR cameras, and camera groups.

17.2 Configuring the DVR Comms Channel

SiPass integrated sends and receives information to and from the DVR system using TCP/IP across an Ethernet network. As both Windows and the DVR switcher understand the TCP/IP protocol, there is no need to configure any additional components.

▷ Ensure that you have installed the SiPass Server.

▷ Ensure that you have installed the DVR Client on the workstation that you are going to view DVR images.

▷ Ensure that you have assigned the correct operator privileges.

▷ Ensure that you have programmed any DVRs with the correct information.

1. Choose the **Components** button from the **System** toolbar or menu.
   ⇨ The *Components* dialog will appear, displaying a hierarchical tree structure of SiPass integrated components.
2. Select the **Server Name** by double clicking on it.
3. Click the **New Bus** button.
   ⇨ A menu will appear showing a list of buses that your license allows you to create.
4. Select the **DVR** option.
   ⇨ A new bus will appear connected to the Server and a new tab option will become available.
5. Select the **Add** button. A new DVR unit type will appear under the **DVR** Column.
6. Click on the unit to display a drop down menu, and select your desired unit.
7. Enter the location of the folder on the PC's hard disk where you have installed the DVR client software, into the **Install Directory** field.
   – The DVR Client software must be installed in the same directory on each PC.
8. Click **Save**.

17.3 Configuring the SISTORE/DVR Client in SiPass integrated

Before SISTORE/DVR cameras can be manipulated from either SiPass integrated or the DVR Client, you must add the location of the client folder to the Windows Environment Variables path. This section applies to both SISTORE AX and SISTORE -clients.

SISTORE CX / SX Units that are Version 3.1 or later can be controlled directly from SiPass integrated so these steps may not be required.

1. Select **Settings > Control Panel > System** from the Windows **Start** menu. The *System* dialog will appear, and the *General* tab will be open by default.
2. Choose the *Advanced* tab.
3. Choose **Environment Variables**. The *Environment Variables* dialog will appear.
4. Select the "Path" row and choose **Edit**.

5. Place a semicolon after the last entry in the **Variable Value** field. Immediately after the semicolon, type the location of the SISTORE client files. For example: C:\SISTORE AX
6. Choose **OK**.

⇨ The environment variable path has now been configured.

17.4 Configuring a DVR unit

The main component of a DVR system is the DVR unit itself. This device controls the operation of DVR cameras in the system and is responsible for the recording of images. SiPass integrated uses a high level interface to send commands to and receive messages from the DVR. After you have configured a DVR with the System Administrator software, the address, type and security details must be programmed in SiPass integrated.

▷ Ensure that you have configured the DVR comms channel.

▷ Ensure that you have connected the DVR to a SiPass workstation PC, or to the network on which the workstation PC is located.

If the Type is “General SISTORE” and SISTORE CX unit is connected, the Video Port should read “12050” and the PTZ Port should read as “23479” by default.

If the Type is “General SISTORE” and SISTORE MX unit is connected, both Video Port and PTZ Port should read as “12050”.

1. Choose the **Components** button from the **System** toolbar or menu.
2. The *Components* dialog will appear, displaying a hierarchical tree structure of SiPass integrated components. Select the **Server Name** by double clicking on it. The *Operational* tab will appear.
3. Select the DVR bus created and click the **New Unit** button. A new DVR unit will appear connected to the bus and a new tab will become available.
4. Enter a unique name for the DVR into the **Name** field.
5. Select the type of DVR unit from the **Type** drop-down box.
6. Assign an Alarm Class to the DVR from the **Alarm Class** drop-down box.
7. The only alarm states that will apply to DVR Alarm Classes will be “Communications Lost” and “Communications Restored”, which correspond to “Alarm” and “Restore” respectively.
8. Enter a description for the DVR Switcher in the **Description** field.
9. Enter the IP address of the network card installed on the Host PC into the **Host Server IP** field. You only need to supply a Host IP address if there is more than one network card installed on the PC running the SiPass Server. In this case, you must supply the IP address of the network card on the SiPass Server which the DVR uses to communicate.
10. Enter the IP address of the DVR into the **DVR IP** field.
11. Enter the Port number that the switcher will use to communicate with the SiPass PC.
12. Enter the User Name and Password used to configure the DVR by the DVR Administration software.
13. Enter a name for the device in the **Device Name** field.

14. Enter a device version in the **Device Version** field.
15. Enter the **SW Version**.
16. Enter the number of **Video Inputs/Outputs** and **Digital Inputs/Outputs** in the respective fields.
17. The **Refresh** button will update the communications status of the switcher that appears in the read-only field.
18. Click the **Save** button. The DVR unit details will be saved to SiPass integrated.

17.4.1 Configuring Input / Output Points for a DVR Unit

The operator can configure DVR Input / Output Points on the *Components* dialog in two ways:

- Using the **Auto Discover** button to automatically discover Input and Output points that have not yet been configured in the dialog.
- By specifying the maximum number of Input and Output points that he wishes to configure.

Auto-Discovery of Input / Output points

1. Select the *Input/Output points* tab of the new DVR unit that was created.

The *Input/Output points* tab will appear only when the DVR unit has been configured as General SISTORE in the **Type** field. This field appears in the *DVR Switcher* tab.

2. Click the **Auto Discover** button. The **Digital Input** and **Output Points** will be displayed on this tab.
3. The **Auto-Discover** button will be disabled if the Comm Status details of the DVR Unit (as given in the *DVR Switcher* tab) has not been updated. To update these details, click the **Refresh** button on this tab.

Specifying the number of Input / Output points to be configured

1. Select the *Input/Output points* tab.
2. Select the maximum number of inputs required from the **Max inputs** drop-down list. The specified number of input points will be displayed.
3. Select the maximum number of outputs required from the **Max outputs** drop-down list. The specified number of output points will be displayed.
4. Any of these points can be deleted by highlighting it and pressing the **DEL** key.

17.4.1.1 Field Definitions for Digital Input / Output Points

The **Digital Input Points** section defines the Input Points by the following fields on the *Input/Output* tab:

- **Input Name**
- **Enable Input**
- **Invert Input**
- **Status**
- **Alarm Definition**

A DVR Digital Input Point uses **Normal** / **Alarm** as alarm class states.

The operator will need to specify a required Alarm/Restore state. Once configured, the Digital Input Point can be configured with this Alarm Definition.

17.4.1.2 Field Definitions for Digital Output Points

The Digital Output Points section defines the Output Points by the following fields on the *Input/Output* tab:

- **Output Name**
- **Status**
- **Alarm Definition**

A DVR Digital Output Point uses **Lock** / **Unlock** as the alarm class states.

Once configured, the Digital Output Point can be configured with this Alarm Definition.

17.4.1.3 Configuring Host Event Tasks for Digital Input/Output points

The operator can perform the following Host Event Task (HET) configurations:

- Configure a HET triggered by a Digital Input / Output Point
- Define a HET to change the state of a DVR Digital Input / Output Point

  The operator can configure a Host Event Task to change the state of a selected DVR digital output. For example, a HET can be configured to change the state of a **Digital Input / Output** point from the **Trigger State Open** to the **Target State Close**. In this case, the Output Point has to be configured as the target.

17.4.1.4 Configuring a Manual Command to Change the State of a DVR Digital Output

Operators can configure manual commands to change the state of a DVR Digital Output.

1. Select **Operation > Manual Override**.
2. Select the **Output** button from the **Type** box.
3. Select the required DVR unit name from the **Unit Name** field.
4. Choose the required state change from the box above **Unit Name**.
5. The available states for the DVR unit are:
   - **Close**
   - **Open**
   - **Single Pulse**
6. Select the DVR output point for the state change from the *Points* tab.
7. Click **Send** and **Close**.

17.4.1.5 Configuring a DVR Digital Input / Output Point Group

Operators can configure DVR Digital Input / Output Point Groups on the *Component Group* dialog.

1. Select **Program > Component Group**. This will bring up the *Component Group* dialog.
2. Enter a name for the group in the **Group Name** field.
3. From the left panel of groups, select **Point Group**.
4. Click the **Add Members** button. This will bring up the *Create Group* dialog.
5. If you want to configure an Input Point Group, select **Input Points** from the **Group Type** drop-down field. If an Output Point Group is to be configured, select **Output Points** from this field.
6. Select the Input / Output points that you want to add to this group from the **Available** box.
7. Click **Add All >>**. This action will add them to the **Selected** box.
8. Click **OK**.
9. Select an alarm from the **Alarm Class** drop-down field.
10. Click **Save** and **Close**.

17.4.2 Configuring Monitors for a DVR Unit

The operator can configure Monitors for DVR units on the *Monitors* tab of the *Components* dialog in two ways:

- Using the **Auto Discover** button to automatically discover Monitors that have not yet been configured in the dialog
- By specifying the maximum number of Monitors he wishes to configure on the **Max Monitors:** drop-down list.

The Monitors section defines the Monitors by the **#** (Monitor Number), **Monitor Name** and **Video Output Channel** fields.

17.4.2.1 Configuring Remote Video Inputs for the DVR Unit

The operator can configure Remote Video Inputs for DVR units in on the *Remote Video Inputs* tab of the *Components* dialog in two says:

- Using the **Auto Discover** button to automatically discover Remote Video Inputs that have not yet been configured in the dialog
- By specifying the maximum number of Remote Video Inputs he wishes to configure on the **Max Points:** drop-down list.

The Remote Video Inputs section defines the inputs by the **#** (Input Number), **Input Name**, **Alarm Definition, IP Address**, **Port** and **Protocol** fields.

17.4.2.2 DVR Unit Functions Available from Site Plans

Operators can add, modify or remove DVR digital Input or 0utput Points/Groups to or from Site Plans.

Adding DVR input / output points / groups a Site Plan

1. From the tool bar of the **Site Plan**, select the **Add Location / Group** button.
2. Click on a desired location in the Site Plan to apply it. This action will bring up the *Add Location / Group to Site Plan* dialog.
3. Select **Point** or **Group** from the **Type** drop-down field.

Select **Point** to add an Input/Output Point to the plan. Select **Group** to add an Input/Output Point Group to the plan.

4. Only Point/Groups that have Alarm Classes assigned will be displayed on this dialog.
5. Click **OK**.

Deleting DVR input / output points / groups from a Site Plan

To delete any of these points / groups, select the particular point/group, and click **Delete**.

Refer the section Adding System Components (symbols) to Your Site Plan [→ 290] detailed instructions on how to add a system component (like a DVR Point or Group) to a site plan.

17.4.3 Configuring a DVR Camera

SiPass integrated allows you to program either a fixed or a PTZ (Pan/Tilt/Zoom) type DVR camera. Up to 16 cameras can be created for each DVR.

SiPass integrated does not support PTZ Cameras on MX or AX SISTORE units.

▷ Ensure that you have configured the DVR comms channel and at least one DVR unit

▷ Ensure that you have connected the DVR unit to a SiPass workstation PC, or to the network on which the workstation PC is located.

1. Choose the **Components** button from the **System** toolbar or menu.
2. Select the **Server Name** by double clicking on it.
3. Select the DVR comms channel.
4. Select the DVR for which you want to define a camera.
5. Choose the **New Point** button.
   ⇨ A new camera will appear connected to the Switcher and a new tab will become available.
6. Enter a unique name for the camera into the **Name** field.
7. Enter a unique title for the camera into the **Camera Title** field.
8. Select a type of camera from the **Type** drop down box.
9. Assign an Alarm Class to the DVR from the **Alarm Class** drop-down box
10. Enter a unique number for the camera into the **Camera No.** field.
11. Enter the number of preset positions for the camera into the **Max. Preset** field.
12. Enter a value in the **Pre-Recording Interval** field.

An operator can configure a Host Event Task to playback a recorded video. The duration of the recorded video to be played back, is specified in the **Duration** field of the *Host Event Task* dialog (when the Target is set to 'DVR', and the **Command** is set to 'DVR Recording'). Assume that the **Duration** field is configured for 60 seconds, and the **Pre-Recording Interval** (on the *Components* dialog, as described above in this section), is configured for 15 seconds; When the DVR recording playback is triggered using the Host Event Task, it will playback 60 seconds of recorded video (as configured in the Host Event Task), preceded by video recorded 15 seconds before this duration.

13. Enter a description for the camera in the **Description** field.
14. Click **Save**.

17.4.3.1 Discovering configured DVR video alarms (sensors)

Operators can configure DVR video alarms in two ways:

- Using the **Auto Discover** button to automatically discover Video alarm
- By specifying the maximum number of alarms to be configured

Auto-discovery of video alarms

1. Select a defined camera under a DVR unit.
2. Select the *Video Alarm* tab of this camera.
3. Click the **Auto Discover** button.

⇨ This action will display all the alarms configured for this camera in the Video Alarm section of this dialog.

The Input/Output Points, Monitors and Remote Video Inputs will appear only if the **Type** selected for the DVR Switcher is **General SISTORE**.

Specifying the video alarms to be configured

1. Select a defined camera under a DVR unit.
2. Select the *Video Alarm* tab of this camera.
3. Select the maximum number of alarms to be configured from the **Max. Alarm** drop-down field.

⇨ This action will display the configured number of sensors in the **Video Alarms** section of this dialog.

17.4.3.2 Field Definitions for Video Alarms (sensors)

The Video Alarms section defines the sensors by the following fields on the *Video Alarms* tab:

- **#** (Video Alarm Number)
- **Sensor Name**
- **Sensor Type**
- **Time Schedule**

Alarms related to the sensor points of a camera can be controlled using time schedule. Time Schedule field can be set to **Always(point unsecure)**, **Never(point always secure)** or **System Function**.

- **Alarm Definition**

An Alarm Class needs to be defined specifically for the Video Alarms, with the following configuration:

Field	Required Configuration
Type	Input
Status	Alarm / Normal
Alarm / Restore	Ignore / Alarm / Restore

Once configured, the Video Alarms can be configured with this Alarm Definition.

17.4.3.3 Setting up a Host Event Task to change the DVR Video Alarm program

The operator can configure a Host Event Task to change the program of a video alarm sensor.

1. Select **Program > Event Tasks > Host Event Task**.
2. Specify an **Event Name**.
3. Specify a **Time Schedule**.
4. Specify **Source 1** as an **Input Point** or **Output Point**.
5. Select a required **State 1**.
6. Specify a **Location 1**.
7. Select DVR in the Target field, select **DVR**.
8. Select a desired switcher in the **Switcher** field.
9. Select EDS / ODR program switching from the **Command** field.
10. Select a camera in the **Cameras** field.
11. Enter a message for the Host Event Task in the **Message** field.
12. Click **Save**.

17.4.3.4 Setting up a HET to create a connection between a DVR camera and monitor

An operator can configure a Host Event Task to create a connection between a DVR camera and a selected analog monitor.

1. Select **Program > Event Tasks > Host Event Task**.
2. Specify an **Event Name**.
3. Specify a **Time Schedule**.
4. Select **Time Schedule** in the **Source 1** field.
5. Select **Start / Start** and **Stop / Stop** in the **State 1** field.
6. Select **DVR** in the **Target** field.
7. Select **Camera/Monitor Connecting** in the **Command** field.
8. Select a switcher in the **Switcher** field.
9. Select a camera in the **Cameras** field.
10. Select a monitor in the **Monitors** field.
11. Enter a message in the **Message** field.
12. Click **Save**.

⇨ The Host Event Task has now been configured.

17.4.4 Grouping DVR Cameras

SiPass integrated allows DVR components to be grouped together. These groups are used during configuration and operation processes. Grouping components also allows you to partition the control that operators have over DVR points. The following section outlines the procedure used to group DVR components.

1. Choose the **Point Group** button from the **Program** toolbar or menu.
2. Choose **Add Members**.
3. Select “DVR Camera” from the **DVR Points** drop-down list.
   ⇨ The available members for that group will appear in the **Available** list.
4. Select the name of the camera to be added to the group from those displayed in the **Available** list.
5. Choose **Add >**.
   ⇨ The selected camera/monitor will be added to the selected list.
6. Repeat Steps 4 and 5 until all members have been added to the **Selected** list.
7. Choose the **OK** button.
   ⇨ The **Alarm Class**, **Group Alarm Triggers**, **Group Actions** and **Group Alarm** Status components in the *Group* dialog have no effect when defining a camera group.
8. Click **Save**.

17.4.5 Configuring an IP Camera

SiPass integrated allows an operator to configure IP Cameras in the system.

There are four main applications of the IP Camera configuration:

- To view IP Camera video using the DVR Live Monitor
- To view IP Camera video using the Virtual Monitor
- To use an IP Camera as a Remote Video Source
- To use an IP Camera for Cardholder Imaging

To apply any of these features, the camera will first have to be configured in the SiPass integrated system.

The IP Camera is configured as a new bus on the server. The steps required to configure it are as follows:

1. Choose the **Components** button from the **System** toolbar or menu.
2. Select the **Server Name** by double clicking on it.
3. Click the **New Bus** button.
4. Select **IP Cameras** from the drop-down list that appears.
5. Next, select the **New Unit** button.
6. Enter a name for the unit in the **Name** field.
7. Enter a description for the unit in the **Description** field.
8. Click **Save**.
9. Click the **New Point** button.
10. Enter a name for the camera in the **Name** field.
11. Enter a title in the **Title** field.
12. Enter a camera number in the **Number** field.
13. Enter the IP address of the camera in the **IP** field.

Please note that the type of IP Camera being configured must support the RTSP protocol.

14. Enter a port number in the **Port** field. This port number depends on the type of IP Camera being used. Refer relevant manuals of the specific IP Camera for information on the Port number.
15. If the IP Camera being used carries extra URL requirements, enter this URL into the **Extra URL** field.
16. A description for IP Camera can be entered in the **Description** field.
17. If the IP Camera is to be used for Cardholder image capture, tick the check box for **This IP Camera can be used for cardholder's image capture**.
18. Click **Save**.

17.4.5.1 Viewing IP Camera video on the Live DVR dialog

Once an IP Camera has been configured on the *Components* dialog, its video can be viewed on the *Live DVR* dialog in the following manner:

▷ Ensure that the right IP address has been entered for the camera in the *Components* dialog.

1. Select **Alarm** > **Live DVR**. This action displays the *DVR Operation* dialog.
2. From the **Switcher** drop down list, select the name of the switcher configured for the IP Camera bus.
3. From the **Camera** drop down list, select the name of the configured IP Camera.
4. Click **Display**.

⇨ The DVR Main dialog will now display the video from the selected IP camera.

To use record the IP Camera video, the camera must first be configured as a Remote Video Source. For more information on this feature, refer the section Using IP Cameras as Remote Video Sources.

17.4.5.2 Viewing IP Camera video on the Virtual Monitor

Once an IP Camera has been configured on the *Components* dialog, its video can be viewed on the *Virtual Monitor* dialog in the following manner:

▷ Ensure that the right IP address has been entered for the camera in the *Components* dialog.

1. Select **Alarm** > **Virtual Monitors**. This action displays the *Virtual Monitors* dialog.
2. Expand the **IP Cameras** tree hierarchy from the **Cameras** panel.
3. Click and drag the configured IP Camera to any screen on the adjacent screen-grid. Alternatively, you can also right-click on a desired screen and select **Set Camera**. This action will display the *Select Camera Point* dialog from where you can select the IP camera. Click **OK** to display the video on the selected screen.

To use record the IP Camera video, the camera must first be configured as a Remote Video Source. For more information on this feature, refer the section Using IP Cameras as Remote Video Sources.

17.4.5.3 Using an IP Camera as a Remote Video Source

To use IP Cameras as Remote Video Sources, it should first be connected to a DVR Unit.

This functionality requires that the IP Camera be configured as the Remote Video Source on the SISTORE CX tool.

Ensure that the IP address entered in the SISTORE CX tool matches the IP address configured for the IP camera in the *Components* dialog.

17.4.5.4 Using an IP Camera for Cardholder Imaging

Once an IP Camera has been configured on the Components dialog, it can be used for the purpose of Cardholder image capture in the following manner:

Ensure that the right IP address has been entered for the camera in the *Components* dialog.

Ensure that the tick box is ticked for **This IP Camera can be used for cardholder image capture** in the *Components* dialog.

1. Select **Options** > **Preferences**.
2. Click on the **Imaging** tab.
3. Click the **IP Camera** radio button and select the IP Camera device from the *drop down menu*.
4. Click **Save** and **Close** the *Preferences* dialog.
5. Select **Operation** > **Cardholder**.
6. Click on the **Imaging** tab.
7. Live video from the IP Camera will appear when the **Live** button is clicked.
8. After live video appears a photo can be captured by clicking the **Capture** button.

17.4.5.5 IP Camera Supported Protocols

For Live streaming withIP Cameras, SiPass supports the RTSP protocol as a command protocol and RTP for the data stream.

The following Codecs are supported:

- MJPEG
- MPEG4
- H264

The RTSP URL is dependant on the type of IP Camera.
Example: rtsp://user:password@ip:port/axis-media/media.amp
The rtsp://user:password@ip:port part of the URL is the default for the VSS SDK player. The rest is the request string for the camera.
Not all cameras require a user and password so in that case it may be omitted.
E.G. rtsp://ip:port/axis-media/media.amp.
If there is no port defined for the RTSP server E.G rtsp://ip/axis-media/media.asp the 554 is used by the player as it is the default port for the RTSP control channel.

17.5 Configuring a Generic DVR unit

This section explains how operators can configure generic DVR units in the SiPass integrated system.

▷ Ensure that you have configured the DVR comms channel.

▷ Ensure that you have connected the DVR to a SiPass workstation PC, or to the network on which the workstation PC is located.

1. Open the *Components* dialog and configure a DVR bus and a New Unit. Steps 1 to 4 of the section Configuring a DVR unit [→ 261] of this chapter explains how this can be done.
2. Next, select **Generic** from the **Type** drop-down field of this dialog.
3. Assign an Alarm Class to the DVR from the **Alarm Class** drop-down box.
4. The only alarm states that will apply to DVR Alarm Classes will be “Communications Lost” and “Communications Restored”, which correspond to “Alarm” and “Restore” respectively.
5. Enter a description for the DVR Switcher in the **Description** field.
6. Configure the **DVR Server** field.
7. Enter the IP address of the network card installed on the Host PC into the **Host Server IP** field. You only need to supply a Host IP address if there is more than one network card installed on the PC running the SiPass Server. In this case, you must supply the IP address of the network card on the SiPass Server which the DVR uses to communicate.
8. Enter the IP address of the DVR into the **DVR IP** field.
9. Enter the Port number that the switcher will use to communicate with the SiPass PC.
10. Enter the **User Name** and **Password** used to configure the DVR by the DVR Administration software.
11. Enter a name for the device in the **Device Name** field.
12. Enter a device version in the **Device Version** field.
13. Enter the **SW Version**.
14. Enter the number of **Video Inputs/Outputs** and **Digital Inputs/Outputs** in the respective fields.
15. The **Refresh** button will update the communications status of the switcher that appears in the read-only field.
16. Click the **Save** button. The DVR unit details will be saved to SiPass integrated.

17.5.1 Configuring Input / Output Points for a Generic DVR Unit

The operator can configure generic DVR Input / Output Points on the *Components* dialog in exactly the same manner as SISTORE DVR units. This means that the operator can either automatically discover Input and Output points using the **Auto Discover** button; or specify the maximum number of Input and Output points to be configured.

The configuration steps required to do this have been explained in the section Configuring Input / Output Points for a DVR Unit [→ 262].

Other functionalities supported by Input/Output Points of Generic DVR units:

The following functionalities are also supported with the Input/Output points configured for generic DVR units:

- Input / Output points can be used as a Triggers for Host Based Event Tasks
- An alarm configured to the Input Point will be displayed in the Alarm Queue
- Input Point events will be logged in Audit Trails
- Input Points can be monitored from Site Plans
- Alarm Classes can be configured to the unit
- Input / Output points are supported in Input / Output point groups
- Operator Partitioning is possible for these Input / Output points
- Commands can be sent to Output points through Manual Commands and Site Plans
- SiPass integrated Reports support these Input / Output points

Configurable fields for Input / Output Points of a generic DVR unit:

As with other DVR units, the following fields can be configured for Input Points for a generic DVR unit:

- **Input Name** / **Output Name**
- **Alarm Definition**: This field can be used to configure an alarm class to the input / output point of a generic DVR unit.
- **Enable Input** (for Input Points)
- **Invert Input** (for Input Points)
- **Status**

17.5.2 Configuring Monitors/DVR Cameras/IP Cameras for a Generic DVR Unit

The configuration of Monitors, DVR Cameras, IP Cameras for a generic DVR unit can be done in the manner as other DVR units.

To configure a monitor for a generic DVR Unit, please refer the section Configuring Monitors for a DVR Unit [→ 264] of this manual.

To configure a DVR Camera for a generic DVR unit, please refer the section Configuring a DVR Camera [→ 265] of this manual.

To configure an IP Camera for a generic DVR unit, please refer the section Configuring an IP Camera [→ 269] of this manual.

17.6 Operating DVR from SiPass integrated

When the DVR Client is called from a SiPass integrated workstation to play back a recorded image or view a live image, the actual client will depend on the type of DVR System(s) you have installed at your facility. This chapter uses the SiPass DVR GUI as an example when operating a DVR System from within SiPass integrated.

- Ensure that all the DVR equipment has been configured in SiPass integrated.
- Ensure that the DVR unit and camera have been turned on and the System Administration software has been used to configure the DVR Switcher.
- Ensure that the SiPass Server and the network connection between the DVR workstations and any DVRs are running and operational.
- Ensure that the correct operator privileges have been assigned.

17.6.1 Viewing Pictures from a DVR Camera

SiPass integrated allows you to select a camera and display live images from that camera on the DVR GUI screen.

1. Choose **Live DVR** from the **Alarm** toolbar or menu.
2. Select from the **Switcher** drop-down box the DVR unit connected to the desired camera.
3. Select from the **Camera** drop-down box the camera for which you want to view the live image.
4. Choose **Display**.
   ⇨ The *DVR Main* dialog will open, displaying the live image from the selected camera.
5. To view cameras from a different DVR unit, select the new unit from the **DVR Unit** drop-down box. Any cameras defined for that unit will appear in the **Camera** list on the left hand side.
6. To go to a preset for a select camera, simply choose the **Preset name** from the **Preset** list below.

⇨ Now, the selected DVR camera should ideally display images for the operators to view.

17.6.2 Setting up a DVR Recording Event Task

SiPass integrated allows you to set up an event task to trigger recording of up to 600 seconds of live images.

1. Choose **Event Tasks > Host** from the **Program** toolbar or menu.
2. Complete the **Trigger** details as for a normal Event Task. For example, if an access point registers an alarm outside of business hours you may want a camera to record any individuals entering through that point.
3. Select **DVR** from the **Target** drop-down field.
4. Select the desired DVR unit from the **Switcher** drop-down box.
5. Select **DVR Recording** from the **Command** drop-down field.
6. Enter the length of time in seconds that you want the DVR camera to record into the **Duration** field. Acceptable times range between 1 and 600 seconds.
7. Select the camera from which live images should be recorded, from the **Camera** drop-down box.
8. If the camera is a PTZ camera, select the position from which the camera should begin recording, from the **Preset** drop-down box.
9. Enter a message describing the event task into the **Message** field.
10. Click **Save**.

⇨ If the specified trigger occurs, the DVR camera will record a live image for the entered duration. A message will appear in the Audit Trail stating the trigger has occurred. This will be followed by a DVR Recording message giving the date and time, as well as whether the recording was successful or failed.

17.6.3 Playing Back DVR Recordings from the Audit Trail

SiPass integrated features a DVR Playback option from the Audit Trail right-click menu.

1. Right-click on a DVR recording event from the Audit Trail.
2. Select the **Play Back** option.

⇨ The DVR Client will appear, and the recording you selected from the Audit Trail will begin playing in the viewing window.

17.7 Virtual Monitors

The Virtual Monitor feature allows operators to arrange and view a matrix of DVR images simultaneously.

1. Select **Alarm > Virtual Monitors**.
2. The cameras available to provide DVR views can be seen by expanding the tree hierarchy of the **Cameras** panel.
3. The right side panel displays 4 windows where different DVR views can be played.
4. The operator can select the layout of the *Virtual Monitors* dialog.
5. To increase / decrease the number of windows, select **File > Load**.
6. Select from the selections available to alter the number of windows as required.
7. To add a view to individual windows, select a camera from the **Cameras** panel.
8. Click and drag this camera, and drop it onto a selected window on the right. This action will play the live image of that camera on the selected window.

17.8 Operating the DVR Client

SiPass integrated features a fully integrated DVR Client as part of its Graphical User Interface. The Client allows you to view live images, organize your DVR Camera system including sequences and presets, and record and playback live images, which are archived by date and time.

The SiPass DVR Client currently only applies to SISTORE CX / SX units that are Version 3.1 and higher.

The dedicated SiPass DVR GUI is opened by selecting **Live DVR** from the **Alarm** toolbar or menu. The following table show the function of each set of controls:

Control	Function
Camera List	Lists all of the cameras you have defined for DVR operation. The icons indicate the camera type.
Preset List	Lists all of the presets you have defined for the camera selected above.
Playback Controls	Allows you to select and play back a previous DVR recording event. Also allows you to record in real-time from the DVR Client.
PTZ Controls	A series of controls for manipulating PTZ cameras, camera focus, and auxiliary camera devices like wipers and lamps.
DVR Mode	Selects Live Video or Recorded Video mode.
DVR Units	Lists the DVR units that you have defined in the Components dialog.

Using the Camera Controls

The camera controls in the DVR Client allow you to move a PTZ camera using the mouse, and activate auxiliary devices.

Directing the camera using the mouse

As well as the compass on the right hand side of the DVR Client, cameras can also be manipulated using a mouse inside the viewing area.

By clicking and dragging the left mouse button, while the mouse pointer is positioned inside the viewing window, a camera can be moved in the direction of the mouse drag. The closer the mouse pointer is to the edge of the screen, the faster the camera will move.

Changing a camera title

The titles of cameras in the list on the left hand side can be changed from the DVR Client. Any changes will be updated in the *Components* dialog.

1. In the **Camera** list on the right hand side, double right-click on the camera title to be changed. The title will be highlighted and a cursor will appear.
2. Change the camera title by editing the title text.
3. Click on another camera. The highlighting will be removed.
4. Choose **Set** to save the title change.

17.8.1 Creating a Preset from the DVR Client

DVR Camera Presets can also be created from the SiPass DVR Client.

1. Select the camera for which you want to define a preset, from the **Camera** list.
2. In the **Presets** list on the right hand side, select a blank Preset, or an existing Preset if you wish to over-write it.
3. Use the Camera controls to set the camera position and focus to the desired setting.
4. Choose the **Set** button. This will assign the current camera setting to this Preset Slot.
5. You can add or change Preset names by right double-clicking in the **Name** Column, and entering a new name.

17.8.2 Recording from the DVR Client

An operator can record a live video from the DVR Client.

1. Open the *DVR Main* dialog.
2. Select **Live Video** from the drop-down list of the **Mode** field.
3. This action will display the live image from the selected camera. This mode generally appears by default on opening this dialog.
4. Select the DVR Unit connected to the camera you want to record, from the **DVR Unit** list at the top of the dialog. The list of cameras defined for this unit will appear in the **Camera** list.
5. Select the camera from the list from which you want to record a live image.
6. If the camera has PTZ functionality, use the PTZ Controls on the right hand side to move the camera into the desired recording position.
7. Choose **Start** in the **Recording** section.

The operator can add a comment to the video to be recorded by typing in the Comment field.

You can use the PTZ controls to manipulate the camera and also select **Presets** while in recording mode.

When you have finished recording, choose **Stop**. The recording event will be stored in the DVR event calendar and can be replayed from both the DVR Client and the Audit Trail.

17.8.3 Search and Playback of a DVR Recording

The DVR Client can be used to play back video images that you have recorded. This includes video images recorded by generic DVR units.

Further, SiPass integrated allows you to perform a filtered search for specific video images from a DVR unit.

The sections that follow explain how to perform a filtered search for video images, and how to playback these images.

Playing back a DVR recording using the DVR Main dialog

1. On the *DVR Main* dialog, select **Recorded Video** from the drop-down list of the **Mode** field.
2. An operator can use the appropriate buttons in the **Playback** box to **Start**, move to the **Prev Frame**, move to the **Next Frame**, **Pause**, **Resume** and **Stop** a recorded video. The operator can also use the horizontal scroll bar in this box to navigate to different parts of the video.
3. To search for a recorded video by the Time of recording, select the **By Time** radio button in the **Search Criteria** box. You can select from the list available in this drop-down field. Click **Search**.
4. To search for a recorded video by the Comment attached to the recording, select the **By Comment** radio button in the **Search Criteria** box.
5. Click **Search**.
6. The search results of recorded video clips will appear in the **Video Clips** box. Click any clip in the list and use the options in the **Playback** box to view it.

17.8.3.1 Searching for recorded video clips

Searching for recorded video clips

▷ Open the *DVR Main* dialog, and select **Recorded Video** from the **Mode** dropdown field.

1. In the *Play Options* section, click the **Search Video Clips** radio button.
2. Configure the search criteria required. For more information on the search criteria, refer the table provided below.
3. Click the **Search** button.

⇨ The search results of the recorded video clips will be displayed in the Video Clips section.

The table that follows explains the Play Options, Search Criteria, Video clip listings and Playback options available to customize the viewing of recorded video.

Section	Available Options	Description
Play Options	**Search video clips**	This option allows the operator to search recorded video files by the **Camera**, **Time**, **Comment** search criteria on this dialog.
	Play by time	This option allows the operator to search recorded video files by **Camera** and the **Start time** of the video.
Search Criteria	**Camera**	This field lists all the cameras configured to the DVR unit selected in the DVR Unit field of this dialog. The operator can tick the checkbox corresponding to the camera, and the search will return all the video clips that were recorded by that camera.
	By Time	**Start time**: The search will return results of all the video files that were recorded after Start time specified in this field.
		End time: The search will return results of all the video files that end recording before the End time specified in this field.
	By Comment	This option allows operators to search for video clips based on the comment attached to the recorded video clips.
Video Clips	**#**	This field displays the video clip number.
	Camera	This field displays the name of the camera that recorded the video clip.
	Comment	This field displays the comment about the recorded video clip.
	Start Time	This field displays the exact time when the video started recording.
	Stop Time	This field displays the exact time when the video stopped recording.
	ClipStorageId	This filed displays the Clip Storage Identification number.
Playback*	**Speed**	This option allows you to increase or decrease the speed of the video clip being played.
	Start	This button starts playing the selected recorded video clip.
	Stop	This button stops playing the video clip.
	Play Backward	This button allows the operator to play the video clip backwards from its current play position.
	Prev Frame	This button moves the video clip being played to the previous frame.
	Pause	This button pauses the video clip being played.
	Next Frame	This button moves the video clip being played to the next frame.
	Play Forward	This button allows the operator to play the video clip forwards from its current play position.

***Mouse-over on the buttons of this section will display the names of the individual buttons.

17.8.3.2 Playback recorded video clips

This section explains how to select and play recorded video clips that are returned after a search.

Playing a recorded video clip

1. Follow the instructions provided in the section Searching for recorded video clips [→ 277] to perform a filtered search for recorded video clips.
2. The resulting video clips of the search will be listed in the *Video Clips* section of the *DVR Main* dialog.
3. Select a video clip that you want to play.
4. Click the **Play** button in the *Playback* section of this dialog. Alternatively, double-click the required video clip in the *Video Clips* section.

⇨ The video clip that is selected will be played.

Using the Playback options to customize viewing the video

An operator can use the appropriate buttons in the Playback section to Play, move to the Prev Frame, move to the Next Frame, Pause, Resume and Stop a recorded video. For further information on these buttons, please table in the section Searching for recorded video clips [→ 277].

The operator can also use the horizontal scroll bar in this section to navigate to different parts of the video.

17.9 Operating the SISTORE DVR Client

If you have installed the recommended DVR solution, Siemens SISTORE, at your facility, the viewing and recording process will be slightly different. This is because a separate DVR Graphical User Interface is used for SISTORE DVR systems within SiPass integrated.

This chapter gives only a brief description of the most important components of the SISTORE DVR user interfaces, and aims to introduce the operator to the basic functionality of the SISTORE Clients. For more information on configuring and using this DVR Client, it is highly recommended that you consult the User's Guide that came with the DVR software.

17.9.1 Using the SISTORE AX Client to view live images

The following instructions show the basic usage of the SISTORE AX type DVR Client. This Client appears when you have SISTORE AX type DVR units installed at your site, and you trigger viewing from a SISTORE DVR camera through the *DVR Operation* dialog, an *Event Task*, or a *Graphic Map*.

SISTORE AX Client Controls

If you hold the mouse pointer over an icon on the SISTORE AX client GUI, a tool tip will appear giving a brief description of the command.

Control	Description
Select Site	Selects a SISTORE AX DVR unit from which to select and view camera images.
Select Camera	Select the camera to view from the current DVR unit.
Split-pane view	Select how many camera images to display on screen.

Control	Description
Full screen view	Displays the current camera image(s) using the entire screen space. Click anywhere on the screen to return to the client view.
PTZ/Lens Controls	Controls to zoom in/out, focus near/far, and open and close the iris.
Preset Controls	Choose whether to create a new preset from the current camera position (MEM) or go to an existing preset (POS).
Alarm on/off	This controls the reporting of alarm events of up to four types from a DVR unit; for example, Video Loss alarm.

17.9.2 Using the SISTORE AX Client to record and playback

The following instructions show the basic usage of the SISTORE AX type DVR Client to record images, and play back previously recorded images.

The “Search” Client appears when you have SISTORE AX type DVR units installed at your site, and you trigger viewing of a recorded image through the **Play Back** option from the Audit Trail right-click menu.

You may search for DVR Recording events by calendar/time search (Time Lapse search) or by Recording event (Event search); for example, by alarm event or motion detection.

SISTORE AX Search Client Controls (Time Lapse Mode)

If you hold the mouse pointer over an icon on the SISTORE AX client GUI, a tool tip will appear giving a brief description of the command.

Control	Description
Select Site	Selects a SISTORE AX DVR unit from which to select and view camera images.
Select Camera	Select the camera to view from the current DVR unit.
Split-pane view	Select how many camera images to display on screen.
Recording Calendar	Select a day to view images recorded by a camera (if any). Days marked in blue indicate recording events on that day.
Recording Time	Select a time from which to begin viewing by clicking a Time Schedule on the timeline with the mouse.
Reload Image	Reloads the current recorded image.
Go to Time	Opens a dialog from which you can enter an exact time during the selected day to being viewing.
Search Mode	Selects the mode to search for recorded sequences. There are two modes: Time Lapse Search – uses a calendar and timeline to select recordings for playback. Event Search – uses a query dialog to search for specific events by camera, motion detection and alarm response.
Play Controls	Controls to play, stop, forward and rewind the selected DVR recording.

SISTORE AX Search Client Controls (Event Mode)

If you hold the mouse pointer over an icon on the SISTORE AX client GUI, a tool tip will appear giving a brief description of the command.

Control	Description
New Event Query	Opens the Event Search dialog to create a new query to search for DVR Recordings.
Next Event	Cycles to next Recording in the Results list.
Event Query Results	Lists all matching results of the query.

17.10 Creating a DVR Audit Trail Report

The following information relating to DVRs is recorded in the Audit Trail and will appear in Audit Trail reports:

- Start and stop times for DVR recording and playback events activated from an SiPass workstation
- Start and stop times for DVR event tasks that have been triggered
- Configuration, modification and deletion of DVR system components in SiPass integrated
- DVR shortcuts activated from Site plans

The following example shows how to generate an audit trail report from DVR Camera events. You can create other types of DVR audit trail reports, depending on the information you want to appear.

1. Choose **Data > Reports > Audit Trail Report**.
2. You can select either **Detailed Audit Trail Report** or **Concise Report** from the **Report** drop-down box.
3. A Detailed Audit Trail report provides more information about events, including details of operators, cardholders and hardware units. A Concise Report shows only the date and location of audit trail messages.
4. Select **Location** from the **Fields Selected** list box.
5. Select a date and time from the **From** drop-down boxes. This represents the earliest record that will appear in the report.
6. Select a date and time from the **To** drop-down boxes. This represents the most recent record that will appear in the report.
7. Select **Equals** from the **Filter** drop-down box in the **Query** section.
8. Select **DVR Point** from the Filter: **Point Type** drop-down list.
9. Select from the **Location** drop-down box the DVR camera that you want to include in the audit trail report.
10. Click the **Add** button. The DVR camera will be added to the **Query** list at the bottom of the dialog.
11. Repeat steps 6 and 7 for every DVR camera that you want to include in your report.
12. Choose the **Print** button to send the report directly to the default Report Printer, or:
13. Choose the **Print Preview** button. The *Print Preview* window will appear showing details of the Audit Trail events concerning the cameras you selected.
14. You can print or convert the format of your report from the *Print Preview* screen by using the toolbar at the top of the window.
15. The following table shows the different filters you can use to create Audit Trail reports on DVR events:

Filter Selected	Filter Action
Location	Allows you to filter reports by DVR Camera.
Message	Allows you to filter reports by the message that is displayed in the Audit trail. For example, “DVR Recording Event Task successful” or “DVR camera deleted”.
Date Occurred	Allows you to filter by the date that the event occurred. This allows you to create a comprehensive report showing all activity over a certain period of time.
Time Occurred	Allows you to filter by the time that the event occurred.

17.11 Viewing Live Video in SiPass integrated

17.11.1 Live DVR

The Live DVR dialog allows operators to view live video images in SiPass integrated.

1. Select **Alarm** > **Live DVR** from the main menu.
   ⇨ The *DVR Operation* dialog will be displayed.
2. Select the DVR **Switcher** to be used for the video display.
3. Select the **Camera** to be used for the video display.
4. Click **Display**.
   ⇨ The *DVR Main* dialog will be displayed.

17.11.1.1 Live Video

This section explains the various options that are available on the Live Video dialog to view live video.

1. Select **Alarm** > **Live DVR** on the SiPass integrated main menu.
2. Select a **Switcher** and **Camera** for the video display.
   ⇨ This action displays the *DVR Main* dialog.
3. Select **Live Video** from the Mode dropdown list.

⇨ The dialog is now refreshed to support the viewing of live video. The section that follows will provide details on the various options available to view recorded video.

17.11.1.2 Recorded Video

This section explains the various options that are available on the Live Video dialog to view recoded video files.

1. Select **Alarm** > **Live DVR** on the SiPass integrated main menu.
2. Select a **Switcher** and **Camera** for the video display.
   ⇨ This action displays the *DVR Main* dialog.
3. Select **Recorded Video** from the **Mode** dropdown field.

⇨ The dialog is now refreshed to support the viewing of recoded video. The section that follows will provide details on the various options available to view recorded video.

17.11.2 Virtual Monitors

The Virtual Monitor feature allows operators to arrange and view a matrix of DVR images simultaneously.

1. Select **Alarm > Virtual Monitors**.
2. The cameras available to provide DVR views can be seen by expanding the tree hierarchy of the **Cameras** panel.
3. The right side panel displays 4 windows where different DVR views can be played.
4. The operator can select the layout of the *Virtual Monitors* dialog.
5. To increase / decrease the number of windows, select **File > Load**.
6. Select from the selections available to alter the number of windows as required.
7. To add a view to individual windows, select a camera from the **Cameras** panel.
8. Click and drag this camera, and drop it onto a selected window on the right. This action will play the live image of that camera on the selected window.

18 Photo-ID and Graphics

Video imaging and card printing is an optional module of the SiPass integrated access control system. It allows cardholder photographs and signatures to be captured on-screen or imported, card templates to be created and access cards to be printed.

The Photo ID module allows you to connect a video or digital camera to the SiPass integrated system and capture a cardholder's photograph and signature. These images can be saved to the SiPass integrated database along with any other cardholder information. They can then be viewed on-screen as part of the record or imported into a card template and printed onto an access card.

SiPass integrated allows you to create your own customized card templates. These templates can include any combination of text, graphics, images, photographs, signatures, or cardholder database information. Once created a card template is attached to a cardholder's record and then recalled or printed when appropriate.

The additional SiPass Card Encoding module also allows you to include a bar code or magnetic stripe in your card templates, in a range of formats. Once inserted onto a template and attached to a cardholder's record, all you need to do is print the card.

The SiPass Photo ID module also allows you to print your own access cards. You can print a single cardholder's card when their record is opened or a group of cards based on criteria that you supply.

18.1 Graphics

Using the optional SiPass Graphics module, you can view and monitor your secured area or site, create and modify floor plans, card templates and alarm instructions from a graphical perspective. When the Graphics module is configured and an alarm is activated, you can choose to see a graphical representation of the point, area, group or unit in question shown on the surrounding floor plan.

SiPass integrated allows you to draw floor plans, import plans, and insert symbols representing input and output points, as well as any areas, groups and units at your site. These symbols allow you to monitor each of the inputs, areas, groups and units. If the status of a component changes, its symbol automatically changes color.

18.2 Drawing toolbar

The Drawing toolbar enables elements of the graphics package. This enables you to create, modify and view graphics components that allow you to monitor your site.

- Choose **New > Drawing** from the **File** menu.
  - ⇨ After you have selected **New Drawing**, an extended **File** menu then becomes available to add a new or open an existing graphic object. Three **File** Menu commands now provide access to sub-menus – **New**, **Open** and **Import**.

The table below shows the commands that are available in the extended **File** menu.

Command	Description
New	Allows you to open a sub menu, from which you can choose to create a new drawing, symbol, site plan, card template, or alarm instruction.
Open	Allows you to open a sub menu, from which you can choose to open an existing drawing, symbol, site plan, card template, or alarm instruction.
Close	Allows you to close the current graphic. If you have edited the graphic, a dialog appears asking if you wish to save the graphic before closing.

Command	Description
Save	Allows you to save changes to the currently open graphic.
Save As	Allows you to save the currently open file (symbol, site plan, card template or drawing) under a different file name.
Import	Allows you to open a sub menu, from which you can choose to import an image/AVI file, AutoCAD/DXF file, photo, signature, or drawing.
Refresh Imported Drawing	Allows you to return to the original imported graphic. If you have made any modifications to the graphic these will be lost upon refreshing.
Save As Drawing	Allows you to save a drawing created in a card template, symbol or site plan. For example, when creating a site plan, you can save the graphic, minus any symbols, as a drawing. This allows you to import the drawing when creating other graphic types.
Print Setup	Displays a dialog that allows the printer, paper size and page orientation to be selected.
Print Preview	Allows you to view the print job before it is sent to the printer.
Print	Sends the print job to the nominated printer.
Lock Workstation	Allows you to manually lock the workstation. Manually locking and unlocking the workstation generates an event that is recorded in the Active Audit Trail.
Logoff	Allows you to log off from SiPass integrated, without disconnecting from the Server.
Exit	Allows you to log off from SiPass integrated, shut down the SiPass Client and disconnect from the Server.

18.2.1 Additional Menus

Once an existing drawing, symbol, site plan, card template, or alarm instruction has been opened or a new one created, three additional menus become accessible:

- **Edit** (Extended)
- **View** (Extended)
- **Drawing**

18.2.1.1 Edit Menu

The type of graphic determines the available functions in the **Edit** menu. The **Edit** menu allows drawings, site plans, symbols, card templates and alarm instructions to be edited. It also allows the individual components to be modified. The following list outlines the functions contained in the menu.

The following table shows the full range of commands available in the **Edit** menu. Depending upon the graphic object being edited, menu items may vary.

Command	Description
Undo	Allows you to undo your last action.
Redo	Allows you to cancel the last undo action.
Cut	Deletes the selected object and places it in the clipboard.
Copy	Copies the selected object and places it in the clipboard.
Paste	Pastes the last object placed in the clipboard into your alarm instruction or graphic at the cursor position.
Paste Special	Pastes text with extra options.
Clear	Deletes the selected object(s) from the alarm instruction.
Select All	Selects all the text and graphics objects.
Find	Allows you to search the text contained in your alarm instruction for a specific word, phrase or text string.
Find Next	Allows you to search the text contained in your alarm instruction for a second or subsequent occurrence of a text string that was searched for, using the Find command.
Insert Date & Time	Inserts the current date and time in a desired format, into an alarm instruction.

Command	Description
Insert Object	Allows you to insert an object created in another application into an alarm instruction. For example, you can insert a bitmap into your instruction and display the bitmap or an icon that represents that bitmap.
Format Font	Displays the Font dialog that allows you to format text characters in an alarm instruction to match the attributes required.
Format Bullet Style	Allows you to change the selected paragraph(s) from normal text to a bulleted list.
Format Paragraph	Displays the Paragraph dialog that allows you to alter the paragraph attributes of the selected text, such as the text indentation and paragraph alignment.
Format Tabs	Displays the Tabs dialog that allows you to specify the tab stop positions for the selected paragraphs. The tab stop positions are created relative to the ruler displayed at the top of the Alarm Instruction window.
Links	Displays the Link Dialog that lists all the links (to text or graphics, created in another application) that you have inserted into your alarm instruction, and allows you to change the attributes of each link.
Object Properties	Displays the Picture Properties dialog that allows you to view the general details regarding the selected object and change the attributes of that object.
Image Object	Allows you to open the application where the object was created and edit that object.
Edit	Allows you to edit the selected text or drawing object. When chosen, the attributes dialog for the selected text or drawing object will appear.
Group	Allows you to combine two or more selected text or graphic objects into a single object.
Ungroup	Allows you to return a set of selected grouped objects to their original state as single elements.
Move To Front	Allows you to promote the selected text or drawing object to the front of the graphic. All other objects in the graphic will appear in a layer beneath the selected object.
Move to Back	Allows you to demote the selected text or drawing object to the rear of the graphic. All other objects in the graphic will appear in a layer above the selected object.
Align	Allows you to align two or more selected text or drawing objects in a graphic.
Size To Image	Allows you to revert to the imported image's original size.
Rotate Image Clockwise	Allows you to rotate an imported image in a clockwise direction, by the specified amount.
Flip Image	Allows you to flip an imported image about either its vertical or horizontal axis.
Invert Image Colors	Allows you to invert or reverse the colors displayed in an imported image, effectively creating a negative of the original.
Process Image	Displays the Process Image dialog that allows you to change the brightness and contrast of the selected imported image.
Optimize Image	Allows you to optimize the selected imported image.

18.2.1.2 View Menu

The **View** menu enables status bar and also allows you to zoom in or out on a graphic.

The following table shows the full range of commands available in the **View** menu.

Command	Description
Status Toolbar	When selected, the Status Bar is displayed at the bottom of the screen. The Status Bar displays system or other messages that are relevant to the task being performed.
Color Palette	When selected, the Color toolbar is displayed.
Zoom In	Allows you to magnify the graphic being created or modified, with the selected point appearing at the center of the screen.
Zoom Out	Allows you to reduce the size of the graphic being created or modified. This is useful for you to view more text and drawing objects on screen at one time.
Normal Size	Allows you to display the graphic being created or modified at its original size.
Grid	When selected, a grid will appear in the background of the graphic as a static display when you are creating or modifying graphic objects.
Bar Code	When selected, the cursor will change to a Bar Code and the Bar Code Encoder dialog will open to insert a Bar Code into a card template.
Magstripe	When selected, the cursor will change to a Magstripe and the Magstripe Encoder dialog will open to insert a Magnetic Stripe into a card template.
Smart Card	When selected, the cursor will change to a Smart Card chip and the Smart Card Encoding Configuration dialog will open to insert a Smart Card chip into a card template.

18.2.1.3 Drawing Menu

The **Drawing** menu allows the attributes of the selected object in a graphic to be changed.

The following table shows the full range of commands available in the **Drawing** menu.

Command	Description
Select	Displays the Select tool that allows you to select a graphic or text object.
Delete	Allows you to delete the selected text or graphic object.
Duplicate	Allows you to copy and paste the selected object(s).
Line	Displays the Line tool that allows you to draw a straight line.
Ellipse	Displays the Ellipse tool that allows you to draw an ellipse.
Arc	Displays the Arc tool that allows you to draw an arc.
Rectangle	Displays the Rectangle tool that allows you to draw a rectangle.
Polygon	Displays the Polygon tool that allows you to draw a polygon.
Text	Displays the Text tool that allows you to insert text into a graphic.
Insert Database Field	Allows you to insert a Database field box into a card template. **Note**: This option is only available when creating or modifying a card template.
Left Justify	Any selected or new text that you add to the graphic will be left justified.
Center Justify	Any selected or new text that you add to the graphic will be center justified.
Right Justify	Any selected or new text that you add to the graphic will be right justified.
Font	Displays the Font dialog that allows you to format the font characteristics.
Vertical Arcs	When selected, all arcs drawn using the Arc tool will have their start and finish points in the vertical plane.

Command	Description
Line Color	Displays the Color dialog that allows you to modify the color of the line of a selected object or any new drawing object to be created.
Fill Shapes	When selected, all new drawing objects created will be automatically filled.
Fill Color	Displays the Color dialog that allows you to modify the fill color of a selected object or any new drawing object to be created.
Thin Pen	When selected, the lines of all new or selected objects will be set to a thin thickness.
Medium Pen	When selected, the lines of all new or selected objects will be set to a medium thickness.
Thick Pen	When selected, the lines of all new or selected objects will be set to a wide thickness.

18.3 Graphics Tools

When creating or modifying a drawing, symbol, site plan, card template or alarm instruction, a number of drawing and graphics tools become available.

The **Drawing** and **Font** toolbars can be moved by clicking and holding the mouse pointer over the top of the toolbar, and dragging the toolbar to a new location.

Drawing Toolbar

The **Drawing** toolbar allows you to create and modify many drawing symbols (circles, squares, etc.) and text objects. By default, the **Drawing** toolbar will appear on the right-hand side of the screen. The available drawing tools include:

Command	Description
New Drawing	Allows you to create a new drawing, which can be incorporated into a card template, symbol or plan.
Open Drawing	Allows you to open an existing drawing, which can then be either edited or incorporated into a card template, symbol or plan.
Save Graphic	Allows you to save changes to the graphic on which you are currently working.
Print Graphic	Allows you to print the current graphic.
Cut Selection	Deletes the selected text or graphic and places it on the clipboard
Copy Selection	Copies the selected text or graphic and places it on the clipboard
Paste Selection	Inserts a copy of the clipboard contents into the active graphic at the cursor's current position
Select	Allows you to select objects in the active graphic
Straight Line	Draws a straight line
Ellipse	Draws an ellipse
Arc	Draws an arc
Rectangle	Draws a rectangle
Polygon	Draws a polygon
Text	Allows you to place text in the active graphic
Zoom In	Allows you to zoom in closer within the active graphic
Zoom Out	Allows you to zoom out within the active graphic
Left Justify	Left justifies the text within a text box
Center Justify	Center justifies the text within a text box
Right Justify	Right justifies the text within a text box
Font	Displays the Font dialog that allows you to change the font attributes
Align Left	Aligns the left edges of two or more selected objects in the graphic
Align Right	Aligns the right edges of two or more selected objects in the graphic

Command	Description
Align Top	Aligns the top edges of two or more selected objects in the graphic
Align Bottom	Aligns the bottom edges of two or more selected objects in the graphic
Align Center	Aligns the centers of two or more selected objects in the graphic
Import Image/AVI	Allows you to import an image file or AVI
Import Photo	Allows you to insert a cardholder photo field into a card template
Import Signature	Allows you to import cardholder signatures into a card template
Insert Database Field	Allows you to insert a field from the Database into a card template
Add location/Group	Allows you to add a location or group to a site plan
Crosshairs	Displays the drawing crosshairs, which allow for more accurate drawing
Add Action/Shortcut	Adds a shortcut for a manual command to a site plan
Grid	Displays the drawing grid that allows for more accurate drawing and alignment
Bar Code	Allows you to add a Bar Code strip to a card template

Text Toolbar

The Text toolbar allows you to size, justify and style text that is to be added to a graphic. By default, the Text toolbar will appear along the top border of the window. The available text tools include:

Command	Description
Font	Allows you to select the font
Font Size	Allows you to select the font size
Bold	Allows you to apply a Bold style to the text
Italics	Allows you to apply an Italic style to the text
Underline	Allows you to apply an underline style to the text
Colour	Allows you to select a font color from a drop down list. (Only available for an Alarm Instruction)
Left Justify	Left justifies the text in a text box
Center Justify	Center justifies the text in a text box

18.4 Drawings

You may need a graphic that is neither a symbol, plan or card template. In SiPass integrated such graphics, called drawings, can be saved and then later imported into symbols, plans and card templates.

For example, by creating a drawing of a familiar layout that will be used in more than one site plan, you can create the graphic once as a drawing and then import it into every site plan that contains that layout.

Creating a drawing

1. Select **New > Drawing** from the **File** menu.
2. Use the graphics tools provided to create your drawing.
3. When finished, select **Save As** from the **File** menu. You will be prompted to supply a filename and location for the drawing file.
4. Click **Save**.

You may open more than one drawing at any given time. When you have more than one drawing open, you may copy and paste drawing and text objects from one drawing to another.

Importing Graphics into Your Drawing

SiPass allows you to import a wide variety of image formats (for example, AutoCAD/DXF) into your drawing. This allows you to create graphics using other applications, and then use them in SiPass integrated.

	The GIF file format is not supported by SiPass integrated as this is a proprietary image format.

18.5 Symbols

A symbol is a graphic element used to represent the status of a system point, area, group or unit on a site plan. Symbols are drawn using the same graphical tools as those used for creating site plans, card templates, and drawings. The color of the symbol is set by the system to indicate its current state.

SiPass integrated comes bundled with a number of built-in symbols that you can use. If you require symbols that are more representative or relevant to your site, you can create your own symbols.

If a point, area, group or unit status does not have a symbol, the system will represent it with a “?” symbol on the site plan.

SiPass integrated allows you to create a new symbol that can be used to represent the status of a point, area, group or unit in your site plan. You may create symbols using the graphics tools provided or import graphics from an external source or from an existing drawing created in SiPass integrated.

18.5.1 Creating a symbol

1. Select **New**, then **Symbol** from the **File** menu.
2. Use the graphics tools provided to create your symbol.
3. When finished, select **Save As** from the **File** menu.
   ⇨ You will be prompted to supply a filename and location for the drawing file.
4. Click **Save**.

	NOTICE
	If you want the symbol to change color according to the point’s status, it must be filled with the standard RED fill color.

18.5.2 Importing graphics to make your own symbol

SiPass integrated allows you to import a wide variety of graphics when creating symbols. They allow you to create graphics in other applications or by using the drawing functions in SiPass integrated, and then to use them when creating or modifying a symbol.

18.6 Site Plans

A site plan is a graphical representation or drawing of the secured area or site. It includes symbols that represent the current status of points, areas, groups and units. Each site plan is dynamically updated by the system as it monitors changes to points, areas and groups.

The scale of plans is determined by your needs. You may have one plan for each floor of a building, or you may include only one section of the floor in each plan. You may also have an overview plan for the entire site that displays a small-scale version of the site.

18.6.1 Creating a site plan

SiPass integrated allows you create a graphical representation of part or your entire site, which can be used to monitor and control access. You may create drawing objects using the graphics tools provided or import graphics from an external source and then insert symbols to represent the status of various points, areas, groups and units contained at your site.

1. Select **New > Site Plan** from the **File** menu.
2. Use the graphics tools provided to create your site plan.
3. When finished, select **Save As** from the **File** menu.
4. Enter the name of the plan into the **New Name** field.
5. Click **OK**.

Site plans can also be imported. See next section.

18.6.2 Importing graphics into your site plan

SiPass integrated allows you to import images files, AVI files, AutoCAD/DXF images and drawings created in SiPass integrated into a site plan. This allows you to create graphics using other applications and then use them when creating or modifying a plan.

18.6.3 Adding System Components (Symbols) to Your Site Plan

Symbols can be used on a site plan to monitor the status of points, areas, groups and units. You can configure a symbol on a site plan to change, as the component represented by that symbol changes.

▷ Create the graphical symbols that you wish to use on your site plan.

▷ Create an alarm class for the type of point, area, group or unit and specify the symbol to appear for each status in the **Current Defined States** list box.

▷ Assign the alarm class to the points, areas, groups or units that will be represented by a symbol.

1. **Open** or **Create** the site plan where the symbol is to be added.
2. From the **Edit** menu, select **Add Location/Group to Plan**, from the **Edit** menu. A **Paste** icon will appear.
3. Position the cursor over the site plan where you want to place the symbol and click the left mouse button. The *Add Location/Group to Plan* dialog will appear.
4. You can choose the **Point Details** button to display an overview of the points configured at your site.

5. Select the location type from the **Type** drop-down menu. Specify the name of the specific type for which a symbol will be added in the **Name** field. Brief configuration details regarding the selected element will appear at the bottom of the dialog.
   – Only those elements that have been assigned an alarm class will appear in the **Name** list.
6. Choose **OK**
7. To save changes to your site plan, select **Save** from the **File** menu.

18.6.4 Adding Shortcuts to Your Site Plan

Shortcuts can be used on a site plan to perform manual commands quickly.

▷ Create the image (icon) to represent the shortcut on a site plan.

1. **Open** or **Create** the site plan where the shortcut will be added.
2. Select **Add Action Shortcut** from the **File** menu.
3. The **Paste** icon will appear.
4. Position the cursor over the site plan, where you wish to place the shortcut and click the left mouse button.
5. The *Edit Action Shortcut Details* dialog will appear.
6. Select the **Action** type.
7. Complete the **Options** details.
8. Enter a message into the **Message** field.
9. This text will be sent to the Audit Trail when the shortcut is executed, and also displayed as help text when the mouse pointer is held over the shortcut icon on a site plan.
10. Choose **Browse** in the **Button** Icon section of the dialog.
11. Select the image you wish to appear as the trigger for the shortcut.
12. Choose **OK**.

⇨ The shortcut will be created and the image selected will appear as a button on the site plan.

18.6.4.1 Shortcut Action Types

The following table explains the available action types.

Action type	Description
Manual Control	Allows you to create a shortcut to a manual command. Once created, clicking on the icon that represents that shortcut will execute the manual command.
Open Plan	Allows you to create a shortcut that opens another site plan.
Toggle State	Allows you to create a shortcut to a toggle command, which allows you to specify both an on-action and an off-action.
CCTV Action	Allows you to create a shortcut to a CCTV camera command, such as switching a camera on or off, or running a predefined sequence.
DVR Action	Allows you to create a shortcut to a DVR camera command, such as recording a live image or moving the camera to a fixed preset.

18.6.4.2 Shortcut Actions

The following table explains the available actions.

Action	Description
Manual Command	Select the point type by choosing the appropriate button in the Point Type section. • Select the command to be sent to the point, from the Commands drop-down menu. Additional fields may have to be filled in depending on the point type and the command chosen. • Select the Unit Name which controls the point to which you want to send the manual command, from the Unit Name drop-down menu. • Select the point group or single point to which you want to send the command, by selecting the Group Name (group) or Location (single) radio buttons, then selecting from the drop-down menu. • The Time Zone drop-down menu only applies to Unsecure commands. It specifies during which times this shortcut may be used to send an Unsecure (unlock or disable) command to a point or area.
Open Plan	Select from the Options section of the dialog the Plan you want to be opened when the shortcut is activated.
Toggle State	Perform the procedure for setting a Manual Command, described above. Do this for both the On-Action and Off-Action tabs. • The on-action will be executed when the shortcut icon is first clicked. The icon will then appear recessed on the site plan. Clicking on the shortcut again will execute the off-action and return the icon to its original state.
DVR Action	Select from the Command drop-down menu the command to be executed when the shortcut is clicked. • If you chose DVR Recording as the Command, enter the desired recording time into the Duration field. Valid times are between 1 and 600 seconds.
CCTV Action	Select from the Switcher drop-down menu the DVR Switcher connected to the camera that will perform the selected command. • Select from the Camera drop-down menu the Camera that will perform the selected command. • Select from the Presets drop-down menu which Preset will be executed when the shortcut is clicked.

18.6.5 Adding Counters and Timers to your Site Plan

Counters and Timers can be added to your site plan. Many more uses exist for Counter/Timers with the assistance of ASP. Counters can be used on a site plan for monitoring how many people badge at a reader or how many people are in an anti-passback area as just some examples. While timers can be used to time how long someone is in the building or how long before the next badge at a reader as examples.

Before you can add a Timer/Counter to your site plan, it first needs to be configured in ASP. Please refer to the SiPass Explorer User Manual for further information on configuring Counters/Timers in ASP.

To add a Counter/Timer to your site plan:

1. **Open** or **create** the site plan where the Counter/Timer will be added.
2. From the *buttons toolbar* on the right-hand side, click the **Add Counter/Timer Button.**
3. Click the area on the site plan that you want to create the Timer/Counter. The *Add Counter/Timer to site plan* dialog will appear.
4. Choose a Type from the drop down list. This can be (Counter, Timer or APB Area Count.)
5. Choose the Counter/Timer/APB area from the Name drop down list.

If the name for the Timer/Counter is short, the default size of the counter/timer that appears on the site plan will be large enough to display the counter/Timer information. The object can be resized but if it is made too small then it is possible the counter/Timer value may not be displayed in entirety when the site plan is opened for monitoring.

6. Selections for the general text appearance such as Font, text Color, Background Color and Vertical/Horizontal alignment can be configured under Text Edition.
7. If it is a Timer that is being added, a format drop box will appear where you can select whether to display the timer in seconds, minutes and seconds etc.
8. Click **OK** to add the Counter/Timer.

18.7 Alarm Instructions

An alarm instruction is a procedure that outlines the steps to be taken when a particular alarm has been triggered. By creating alarm instructions, you ensure consistency and efficiency when dealing with alarm situations.

SiPass integrated allows you to create an alarm instruction that can be a combination of written procedure and intuitive graphics.

Creating an alarm instruction:

1. Select **New > Alarm Instruction** from the **File** menu.
2. Use the text tools provided to create your alarm instruction.
3. When you have finished, select **Save As** from the **File** menu to save the alarm instruction.

You have created and saved an alarm instruction, it can be incorporated into an alarm class definition that allows the instruction to be viewed when an alarm is activated.

18.8 Using Site Plans to Monitor your Site

Once you have created a site plan and added the appropriate symbols to that plan, it can be used to monitor your site. When an alarm has been triggered, the symbol representing the point, group, area or unit in question on the site plan will change color. It will remain that way until it has been actioned and, if necessary, returned to its normal state. A site plan can also be used to send manual commands to elements, allowing you to control many aspects of your site from the graphical plan.

18.8.1 Interpreting the Site Plan

When you have selected the correct site plan, you will be able to see the current status of each of its points, areas, groups and units. Each element is represented by a symbol that changes color according to its current status.

Important: The part of the symbol that is to change color according to status, must be filled with the standard RED when it is drawn.

Colour	Symbol
RED (SOLID)	Alarm symbol
RED (FLASHING)	Alarm Symbol
MAGENTA	Alarm Symbol
GREEN	Restored symbol
BLUE	Symbol remains as it was when it was unsecured.

By positioning the mouse pointer over a point on a site plan, a brief description of that point will appear, including the name of the point and its current state. By positioning the mouse pointer over a point on a site plan, and right clicking, the Query dialog will appear, displaying detailed information about that point.

18.8.2 Securing a Point or Area From a Site Plan

SiPass integrated allows you to send a manual command to secure a particular point or area using a Site Plan.

1. Choose **Open Site Plan** from the **Alarm** menu, and select the plan that contains the appropriate points or area.
2. Select the point, area, or group to be secured by clicking on it.
3. Choose **Secure Location/ Group** from the **Alarm** toolbar.

⇨ The point, area or group will be secured.

18.8.3 Unsecure a Point or Area From a Site Plan

SiPass integrated allows you to send a manual command to unsecure a particular point or area using a Site Plan.

1. Choose **Site Plan**, and select the plan that contains the appropriate points or area.
2. Select the point, area, or group to be unsecured by clicking on it.
3. Choose **Unsecure** from the **Alarm** toolbar.

⇨ The point, area or group will be unsecured.

18.8.4 Allow Access to an Output Point From a Site Plan

SiPass integrated allows you to override the normal behavior of an individual output point to allow access to a particular location. For example, if a cardholder forgets their access card and needs to gain entry into a secure area, you can allow that cardholder to enter the area by sending the output point a manual “allow” command.

1. Select the icon that represents the output point. The point should now appear highlighted on the site plan.
2. Choose **Allow Access** from the **Alarm** toolbar. The point will temporarily change state. For example, if you selected an output point at a door, the door will temporarily unlock for the configured time and then return to its normal state (locked).
3. Choose **Unsecure Location/ Group** from the **Alarm** toolbar.

18.8.5 Manually Controlling a Point from a Site Plan

You can manually manipulate an individual point, area, floor, or elevator by sending electronic messages through the system. Manual commands can also be used to perform diagnostic functions.

1. Choose the icon that represents the point to be manually controlled.
2. The point should now appear highlighted on the site plan.
3. Choose **Override** from the **Alarm** toolbar.
4. Select which component you wish to manually control by selecting the appropriate button from the **Type** toolbar. The Commands are always available by accessing the **Manual Override** function from the **Operation** menu.
5. Select the unit to which the type is associated from the **Unit Name** field.
6. Select the specific point, point group, area, elevator or unit to which you wish to send a command, from the list box at the bottom of the dialog.
7. Select the **Command** to be sent from the **Commands** list box.
8. Choose **Send**.
   ⇨ The command will be sent to the respective component and an event will be generated in the Audit Trail indicating the resulting action.
9. Choose **Close** to return to the main SiPass integrated screen.

18.8.6 Querying a Point From a Site Plan

SiPass integrated allows you to view a detailed description of a single point, area, group or unit. This information can often help you to handle an alarm situation, or just keep you up-to-date with the state of your site.

1. Select the icon that represents the point, area, group, or unit to be queried.
2. Right click on the selected point, area, group or unit.
   ⇨ The *Query* dialog will appear. View the details regarding the selected point, area, group or unit.
3. Choose **Close** when you have finished viewing the details.

18.8.6.1 Point Details

The following table explains the point details when querying a point.

Detail	Description
Location	The name of the point, area, group or unit that you are querying.
Type	Indicates the specific type of point, area, group or unit that you are querying.
Alarm Class	Specifies the Alarm Class that has been assigned to the point, area, group or unit.
Priority	Indicates the priority level of the Alarm Class assigned to the point, area, group or unit.
Time/Date	Indicates exactly when the selected item first went into alarm.
Alarm Count	Specifies exactly how many times this item has entered an alarm state without being actioned (after being restored).
Status	Brief description of the status of the point, area, group or unit. The status displayed here is defined in the alarm class definition.
Alarm State	The current state of the point, area, group or unit.
Enable	Indicates whether the point, area, group or unit is enabled or disabled. Alarms cannot go off at disabled points.
Last Alarm Comment	Displays the brief message entered by the operator about the last alarm occurring at this point, area, group or unit.

18.8.7 Actioning an Alarm from a Site Plan

SiPass integrated allows you to action an alarm using a site plan, after an alarm has been triggered and is to be acknowledged.

1. Select the alarm to be actioned from the **Alarm Queue** and choose **Site Plan**. A plan appears that displays the point, area, or floor where the alarm was activated. If the plan has been configured correctly, all points or areas currently in an un-actioned alarm state will be flashing red.
2. Select the point area, or floor to be actioned by clicking on it.
3. Choose **Action Alarm** from the **Alarm** toolbar.
4. Enter a message into the **Log of action** taken field. This will indicate that you have acknowledged the alarm and are taking action to investigate. This message is passed to the Audit Trail.
5. Choose **OK**.
   ⇨ The alarm event will disappear from the **Alarm Queue** window (if the point has returned to a normal state) and an Audit Trail event will be generated, informing the SiPass operator(s) that the alarm has been actioned.

18.9 Card Template Design and Encoding

SiPass integrated incorporates an advanced card production suite that allows you to design, print, and issue customized access cards for any aspect of your site. The card design tools provided by SiPass integrated allow you to include watermark images, cardholder photographs, cardholder signatures, database information and text onto a single or double sided card template.

To further enhance the card production capabilities of SiPass integrated an additional module can be added that allows a card to be encoded with a bar code, magnetic stripe or smart card.

18.9.1 Creating a Card Template

A Card Template is a user-created card design. This design is created using the same graphical tools as those used to draw symbols, site plans, and drawings in SiPass integrated. Card templates allow you to create multiple card designs, and use them for different cardholders throughout your site. You may design a template for both the front and reverse of a card.

SiPass integrated allows you to incorporate cardholder photographs, signatures, database information, text, graphics, watermarks, and company logos onto a card template. A card saved to an employee record using a card template will be updated whenever the database field is changed.

You may also insert a bar code or magnetic stripe into the card template that can be used to further enhance the access security at your site. All cards printed using this template will contain either a bar code or a magnetic stripe, and depending upon whether the template is single-sided or duplex may contain both.

1. Select **New > Card Template** from the **File** menu.
2. Configure the card template page setup, by selecting **Card Template Page Setup** from the **File** menu.
3. Ensure that the correct printer is assigned in **Print Setup** for correct template size.
4. Complete the card template page setup details:
   - **Double Sided Card**:
     When checked allows you to create a double-sided card template.
   - **Page 1**:
     Allows you to specify the front side of the employee card.
   - **Page 2**:
     Allows you to specify the reverse side of the card.
5. Use the graphics and drawing tools provided by SiPass integrated to design your card template.
6. When finished, Select **Save As** from the **File** menu.
   ⇨ The *Card Template Name* dialog will appear.
7. Enter the name of the card template into the **Enter Name** field. Card template names cannot exceed 20 characters.
8. Choose **OK**.

18.9.2 Adding a Cardholder Photograph to a Card Template

The SiPass integrated graphics package allows you to create a field that displays the photograph of a cardholder on their access card. The employee's photograph is captured using SiPass' video imaging capabilities.

1. **Open** or **Create** the card template to which cardholder photograph will be added.
2. Select **Import > Photo** from the **File** menu. The cursor will change to a paste icon.
3. Position the cursor over the card template, where you wish to place the photo box and click the left mouse button. A photo box will appear on the card template.
4. Resize the photo box by selecting it and placing the mouse pointer over one of the corner handles.
5. While holding down the left mouse button, drag the corner out until the desired size has been achieved.
6. Click **Save**.

Once you have placed the photo box on the card template, you can move it by placing the mouse pointer over the photo box, holding down the left mouse button, and dragging it to a new location.

18.9.3 Adding a Bar Code to a Card Template

SiPass integrated allows you to add elements to a card template that display a bar code on an access card.

Ensure that you are aware of the bar code format used at your site before adding a bar code to a card template.

1. **Open** or **Create** the card template where the bar code will be added.
2. Select the **Bar Code** icon from the drawing toolbar. The cursor will change from an arrow to a Bar Code.
3. Position the cursor on the area of the template where you wish to place the Bar Code and click the left mouse button. The *Bar Code Encoder* dialog will appear.
4. Select the bar code format to be used from the **Select Format** drop down list. See table below.
5. Choose the **OK** button.
6. Reposition, orient and size the Barcode frame to fit within the card template.
7. Select **Save** from the **File** menu to save the template.

Bar Code Format	Description
3 of 9 - Access	This is an industry standard Bar Code containing automatically selected database fields.
3 of 9 - Generic	This is an industry standard Bar Code. Any cardholder custom field may be selected and encrypted with the standard 3 of 9 algorithm.
Asco Encrypted Bar Code	This is a proprietary Bar Code format and contains automatically selected database fields for encryption. These fields are unknown to the operator.
Asco Facility Bar Code	This is a proprietary Bar Code format that makes use of the site's facility code, together with database fields, for encryption. This format is used on older sites, and may be used when software is upgraded. New installations should use Asco Encrypted Bar Code, which has higher security.

18.9.4 Adding a Magstripe to a Template

A Magnetic Stripe object can be inserted on the reverse of an existing card template, to represent a Magnetic Stripe itself that is physically part of the card.

▷ Ensure that the card printer that you intend using is Magstripe capable.

▷ Ensure that you are aware of the exact magstripe format used at your site.

1. **Open** or **Create** the card template into which the magnetic stripe will be added.
2. From the **Edit** menu select **Card Template Page Set Up** then enable the **Double Sided card** checkbox
3. Select the **Magstripe** icon on the drawing toolbar. Position the cursor over the template where you wish to place the Magnetic Stripe and click the mouse.
4. Select the type of Magnetic Stripe from the **Select Format** drop-down list.
   - **Asco Encrypted Magstripe**:
     This is a proprietary Magnetic Stripe format and contains automatically selected database fields for encryption. These fields are unknown to the operator.
   - **Custom Field**:
     Allows a Custom Field to be selected for printing on a magstripe.

The Magnetic Stripe frame will be placed at the default position on the reverse side of the card template. The Magnetic Stripe's position is fixed.

5. Select the Track to be encoded from the **Track ID** drop down box.
6. Select the custom Field to be used for encoding from the **Field** drop down box.
7. Click **Save**.

19 Video Imaging and Card Printing

SiPass integrated allows you to capture live images using a video or digital camera and store these images with the record or a cardholder. You can also import images from over 32 different file types. Once the Video Imaging and Card Printing Module has been installed, each operator can configure the image settings to their own preferences.

By using SiPass integrated to set the camera or video card properties, the settings will not be permanently recorded and will only be configured for the current session. It is recommended that you configure settings with the video capture card or digital camera's own installation software.

19.1 Configuring the video image settings

▷ Ensure that at least one video capture card, or USB-compatible digital camera, and the appropriate software has been installed.

1. Select **Preferences** from the **Options** menu.
2. Choose the *Imaging* tab.
   ⇨ If your PC does not have a suitable camera or video capture card installed, an error dialog will be displayed. The following steps in the procedure are based upon a Logitech QuickCam digital camera. The screens displayed and the configurable settings contained may vary, depending upon the camera and video capture card installed and the driver being used.
3. Choose the **Video Source** button.
4. Configure the Video capture settings according to your preferences.
   ⇨ The Video Capture settings will normally deal with video capture source, picture quality (resolution, brightness) and the physical settings of the camera, like tilt.
5. Choose the **OK** button. You will be returned to the Imaging tab of the *System Preferences* dialog.
6. Choose the **Video Format** button.
   ⇨ The *Video Format* dialog will appear. The screens displayed and configurable settings contained may vary, depending upon the camera, video capture card installed and the driver being used.
7. Configure the video format settings according to your preferences.

⇨ You will be returned to the *Imaging* tab.

Video Overlay has been added to the GUI in anticipation of future SiPass integrated development. This feature may or may not be supported, and will depend upon your installed video capture card. Currently, the recommended card (Videum VO) does not support Video Overlay. The button will be disabled, indicating that your installed hardware is incompatible with this feature.

The configuration of the video display and capture card is now complete. It may also be necessary to configure these options permananetly using the software installed when the video capture card was installed.

19.2 Capturing Cardholder Photographs

Once you have installed SiPass' Photo ID and Image Verification Module and have configured the image preferences, you can begin capturing cardholder images.

▷ Ensure that the video capture card has been installed and configured.

▷ Create an employee record for the employee whose image is to be captured.

▷ Ensure that a card template has been created.

1. Choose **Cardholder** from the **Operation** toolbar or menu.
2. Open or Create the record for the cardholder whose image is being captured.
3. Choose the *Imaging* tab. Choose **Live**.
   ⇨ The imaging panel will display a live video image on screen.
4. Position the camera and employee so that the employee's picture is displayed clearly (in focus) on screen. Refer to the video camera's user guide for detailed instructions concerning its operation and settings.
5. Choose **Capture**.
   ⇨ The live video image will appear on screen as a still image. A cropping tool will appear overlaid on the captured photo, and a contrast and brightness slider will also appear.
6. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle to the desired size.
7. By positioning the cursor anywhere inside the cropping area, you can hold down the left mouse button and drag to move the cropped area. The part of the captured image that appears within the rectangle will appear in the photo field on the card template.
8. Use the **Contrast** and **Brightness** sliders, to adjust the image quality. The higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
9. Choose the *Definition* tab, when finished.
10. Click **Save**.

19.2.1 Image Recall

Image details - employee photographs and signatures - are saved to each employee record. Any client terminal can access these records merely by opening the desired employee record and choosing the Imaging tab at the top of the dialog. The last saved image will be displayed.

19.3 Importing a Cardholder's Photograph or Signature

Once you have installed SiPass' Photo ID Module and have configured imaging preferences, you can begin importing photographs and signatures of cardholders.

▷ Create an employee record for the cardholder whose image will be captured.

▷ Ensure that the cardholder photograph or signature exists.

1. Choose **Cardholder** from the **Operation** menu or toolbar.
2. **Open** or **Create** the database record for the cardholder whose photograph or signature is being imported.

3. Choose the *Imaging* tab. If a previous image of the employee signature exists in the employee's record, it will automatically be recalled when the Imaging tab has been selected.
4. Select the **Photo** radio button to import the cardholder's photograph or select the **Signature** radio button to import a signature.
5. Choose the **Import** button.
6. Select the image file to import.
7. Choose the **Open** Button or double click on the file name.
8. By positioning the cursor over one of the handles located at the corner of the cropping rectangle, you can change the size of the cropped area by dragging the rectangle.
9. Use the **Contrast** and **Brightness** sliders, to adjust the image quality - the higher up the scale, the greater the Contrast and/or Brightness, and vice versa.
10. Choose the *Definition* tab, when finished.
11. Click **Save**.

19.4 Card Printing

The SiPass integrated Video Imaging and Card Printing module also provides the tools you need to print access cards on-site. SiPass integrated allows you to print a single card from a cardholder's record, or print a group of cards based on selectable criteria. Card Printing is normally carried out as a function of the Video Imaging and Card Printing Module and requires a dedicated printer for the purpose. Card printing cannot be carried out on conventional printers. However, conventional printers can be used to proof card templates.

Depending upon your requirements, cards can be printed as single-sided or double-sided (duplex). Many card printers are capable of duplex printing.

!	*NOTICE*
	You should keep in mind that used printer ribbon contains negative images of data contained on cards. Ensure that you dispose of used printer ribbons according to your policy for handling confidential information.

19.4.1 Configuring a Card Printer

Configuring a card printer is a two-stage process. The printer must first be configured in SiPass integrated, and then through the Windows Printers and Faxes utility.

For the purposes of this procedure, a Magna Class Card Printer has been used. This is currently a preferred type of card printer and is supported by SiPass integrated.

Stage 1: Configuring a Card Printer

▷ Refer to the printer manufacturer's literature and release notes. You may need to upgrade the host PC with a Service Pack to ensure correct printer operation.

1. From the **File** menu, select the **Print Setup** option.
2. Choose the *Card Printer* tab.
3. Select the brand of printer from the **Printer Type** drop-down list
4. If you wish to nominate another card printer as the default, choose the **Select Printer** button to open the *Print Setup* dialog.
5. Select the printer from the **Name** drop-down list.
6. Set the **Orientation** to either **Portrait** or **Landscape**.
   ⇨ The card template used in the design of the cards will determine this setting.
7. Choose the **Properties** button.
8. Select the appropriate printer settings.
9. When you are satisfied with the printer settings, choose the **OK** button.
   ⇨ You will be returned to the *Print Setup* dialog.
10. Choose **OK**.
    ⇨ You will be returned to the *Setup Global Printers* dialog.
11. Choose the **Apply** button.

Stage 2: Configuring a Card Printer

1. Select **Settings > Printers and Faxes** from the Windows **Start** menu.
2. Highlight the card printer icon, right click the mouse and then select the **Properties** option from the menu.
3. Select the *Advanced* tab.
4. Highlight the following options:
   – Highlight the Spool print documents so program finishes printing faster option.
   – Highlight the Start printing immediately option.
   ⇨ These settings are required to ensure that card printing can take place.

Do not use the **Print directly to the printer** option.

5. Select the *Ports* tab.
6. Tick the **Enable bi-directional support** checkbox.
7. Choose the **OK** button.

19.4.2 Printing a Card

SiPass integrated allows you to print an access card for any cardholder in your database. This function would normally be carried when a cardholder is newly enrolled in SiPass integrated or when a new access card needs to be issued.

Printing a single card

▷ Ensure that a card printer has been correctly installed and configured.

▷ Ensure that the appropriate card template has been designed

1. Select **Cardholder** from the **Operation** menu or toolbar.
2. Create a new cardholder record or open the record of an existing cardholder.
3. Choose the *Imaging* tab.
4. Capture the cardholder's photograph
5. Choose **Print**. The card will be sent to the printer.

⇨ The cardholder's details are also automatically saved when cards are printed from the *Cardholder* dialog.

Printing a batch of cards

1. From the **Operation** menu, select **Batch Card Printing**.
2. Select the **Card Filter Options** that best describe the group of cards you wish to print, by selecting the checkbox and entering or choosing the appropriate data.
3. Choose the **Generate** button.
   ⇨ The list of cardholders that match your criteria will appear in the **Generated Card List** field.
4. From the displayed list, select those cardholders to be excluded from the batch print job by double clicking anywhere on their record.
   ⇨ The entry in the **Print** column for that record will now say "No", indicating that a card will not be printed.
5. Select the required **Print Configuration**.
   - **Start Immediately**:
     Allows the SiPass Operator to choose whether to start the Batch Print job immediately or wait and start the print job manually from the *Batch Card Printing Monitor* window.
   - **Apply Request to Proceed Message After**:
     If selected, this option allows you to specify whether a confirmation to proceed with the batch print job appears. You can also specify the exact number of cards that are printed before the confirmation dialog next appears.
   - **Apply Card Template if none defined**:
     Allows you to specify a default card template for each cardholder in the SiPass integrated system that has not been assigned a template. This option will not be enabled if the **Card Template filter** option has been selected.

– **Always Encode upon Question:**
Allows you to encode and print all the cards configured for Batch Card Encoding / Printing. Leaving this checkbox un-ticked means that SiPass integrated will not encode any cards that require an operator decision. For example, an operator may have configured this dialog to encode and print a card with a card number that already exists in the system. Normally, this would bring up a dialog asking the operator to verify (Yes or No) if the card number should be used for the new card. There are other situations that may arise, requiring an operator decision. Such cards will not be encoded if this checkbox is left un-ticked. However, SiPass integrated will proceed with the batch card encoding and printing process for the remaining cards.

6. Choose **Proceed** to send the job to the batch print queue. A confirmation window will appear.
7. Select **Yes**.
   ⇨ The cards will begin printing automatically if the **Start Immediately** option has been selected. If this option has not been selected the print job will be paused and can be started from the *Batch Card Printing Monitor* window.
8. Choose **Close**.

⇨ If you have entered a value into the **Apply Request to Proceed Message After** field, a dialog will appear each time the specified number of cards have been printed.

19.4.2.1 Batch Printing Card Filters

The following table explains the available card filters for batch printing

Filter	Description
Card Range	This option allows you to select a range of cards based on specified card numbers. For example “12 - 56”, 10, 100 – 145”.
Only These Workgroups	This option allows you to select one or more workgroups to which cardholders belong. Simply select a single workgroup by clicking on it. To choose multiple workgroups hold down the CTRL key while selecting each workgroup.
Card Template	This option allows you to select a card template. All cardholders with the template associated with their database record will be included.
Custom Field	This allows you to select a custom field from a list of all defined custom fields in the system. Once selected, you will then be able to select a specific value associated with that custom field. All cardholders with a record that matches the selected custom field value will be included.
Cards Last Printed	This allows you to select cardholders based on the date and time their card was last printed, from the following conditions: –Before, On or before, After, or On or after Any cardholder whose card was printed in the selected range will be included, dependant upon the other criteria you have chosen.
Filter on Card Printed State	Allows you to select all cardholders that have or have not had their access card previously printed based on your selection.
Cardholder Modified	This allows you to select cardholders whose database record was changed based on the following conditions: –Before, On or before, After, or On or after Any cardholder whose record was changed within the selected range will be included, dependant upon the other criteria you have chosen.
Filter on Employee Modified State Since Last Printed	Allows you to select all cardholders whose database record has either been changed or remained unchanged since their card was last printed.
Filter Out Void Cards	Allows you to ignore all cardholders with a void status.

19.4.3 Batch Card Printing Monitor

This section shows how to open and use the *Batch Card Printing Monitor* window. This window allows you to monitor the progress of print jobs, and to pause, start, abort, or resume a batch card print job.

1. From the **Data** menu, select **Batch Card Printing Monitor**. The *Batch Card Printing Monitor* window will appear displaying the status of each batch card print job that has been generated. The following describe each column in the window:
   - **Batch**: Batch card printer number – auto generated based on date and time.
   - **Status**: paused, queuing (another currently printing in a queue of batch jobs), printing, aborted.
   - **Progress**: The number of cards that have been printed out of the total number.
   - **Current**: Card number that is currently being printed.
   - **Printer**: Printer to which the job will be sent.
2. To start, pause, abort or resume card batch print jobs, right-click on the job you want to action. A menu will appear showing a list of options: **Start**, **Pause**, **Resume**, **Abort**. Select the action you want to perform on the print job.
3. Close the *Batch Card Printing Monitor* window when you have finished.

Index

A

ACC 25
ACC series, Devices 30
ACC Series, Points 33
ACC, configuring 28
ACC, configuring for remote access 204
Access Control 215
  to floors 222
Access Groups, configuring 125
Access Levels, configuring 124
Access Points, configuring 34
ACCs
  remote 201
Action Shortcut 291
Actioning an Alarm 296
  Log of action taken 296
Add
  Action 288
  Group 288
  Host Event Task 58
  Location 288
  Shortcut 288
Adding
  Bar Code 298
  Photo Boxes 297
Adding a DVR Camera 265
Adding a Guard to the System 225
Address Range, IP 211
Alarm
  Count 147
  Current State 147
  Instruction 139
  Location 147
  Status 141, 147
  Symbols 141
Alarm Class for dialup components 207
Alarm Date 147
Alarm Instruction 293
  Close 283
  Creating 293
  New 283
  Open 283
  Save 284
Alarm Priority 147
Alarms, CCTV 194
Align 285
  Bottom 288
  Centre 288
  Left 287
  Top 288
Align Right 287
Allowing
  Output Point 294
And 160
Anti-Passback area violations 70
Anti-passback violations, forgiving 100
Anti-Passback, multiple ACCs 71
Apply Card Template 304
Apply Request 304
Arc 287
Arc Tool 286
Area, viewing cardholders 75
Areas
  Intrusion 76
Areas, configuration 72
Audit Trail
  Backup 153
  Columns 15
  Purge 155
  Restore 155
AutoCAD DXF File
  Import 284
Auxiliary Device 182

B

Backup
  Audit Trail 153
  Database 149
  Location 149
Backup - Log Book 156
Bar Code 288, 298
Baud Rate 200
Bold 288
Bus 178, 186

C

Camera 180, 190, 274, 275
  Groups 183
  Movement 176
Capture Card
  Installation 197
Capturing
  Photograph 301
Card List 304

Card Template
- Bar Codes 298
- Close 283
- Design 296, 297
- New 283
- Open 283
- Page Setup 297
- Photo Box 297
- Save 284

Cardholder
- Return card 122

CCTV
- Auxiliary Device 182
- Camera 180
- Component Groups 183
- Configuring Operation 183
- Controller 179
- Controls 176
- Groups 183
- Monitor 181
- Operation 190
- Protocol 178
- Unit 179

CCTV Bus 178, 186
Centre Justify 286, 287
Checklist 175
Clear 284
Clearance Reqd 54
Close 283
Close Iris 177
Colour 288
Colour Palette 286
Commands 146
Component Groups 183
Configuration Checklist 259
Configuring
- Patterns 184
- Presets 183
- Sequences 185

Configuring a SISTORE Client 260
Configuring Operation 183
Controller 179
Controller Event Task
- configuring 63

Controls 176
Copy 284, 287
Count 54
Crosshairs 288
Customisable Cardholder Fields 102
Customisable Tab 102
Cut 284, 287

D

Database 215
- Backup 149
- Field 288
- Restore 151

Default Settings, Devices 33
Defining the Dialup ACC 206
Delayed Reporting, Timed Re-entry 71
Delete 286
Design
- Card Template 296

Device, configuring 30
Devices 25
Dial-up
- ACC 202
- bus service 205
- Defining Other components 207
- Definition 200

Dial-up Bus 200
Dialup components overview 200
Dialup configuration checklist 202
Dialup redundancy configuration 211
Dialup/PPP Properties 206
Disabled Cardholders 75
Door Interlocking 78
Double Sided Card 297
Download
- Server to ACC 209

Download, automatic 209
Drawing
- Close 283
- Import 284
- New 283, 287
- Open 283, 287
- Save 284, 287

Drawing Toolbar 283, 287
Drawings 288
Dual Custody 36
Duplicate 286
DVR Bus 260
DVR Camera Groups 268
DVR Comms Channel 260
DVR IP Address 261, 272
DVR Recording 274, 275

E

Edit 285

Elevator Control 216
Elevator Controller
low level 217
Ellipse 287
Ellipse Tool 286
Encoding 162
Ethernet Comms 25
Event Name 58, 68
Event Task 274, 275
Event Task, establish connection 210
Events, CCTV 194
Exit 284

F

Fail-soft Anti-Passback 70
Fill Colour 287
Fill Shapes 287
Find 284
Find Next 284
Fire Over-ride
overview 216
wiring 216
Fixed Camera 180
Flip Image 285
FLN 25
FLN, configuring 30
Focus Control 180
Focus Far 177
Focus Near 177
Font 286, 287, 288
Size 288
Forgive 100
Format Bullet Style 285
Format Font 285
Format Paragraph 285
Format Tabs 285

G

Generate 304
Graphics 283
Graphics Module 283
Graphics Tools 287
Grid 286, 288
Group 285
Type 54
Grouping
Cameras 183
Monitors 183
Groups 183, 268
Work 84
Guard Tour
Starting 229
Guard Tour Window 235
Guard 235
Last Point 235
Next Point 235
Time 235
Tolerance 235
Tour 235
Guards 225
Adding a Guard to the System 225
Viewing Employee Details 225

H

Hard Anti-Passback 70
Holiday
Date 63
Name 63
Host Event Task
Add 58
Create 58
New 58
Time Zone 58
Host IP Address 261, 272
HyperTerminal, commands 204
HyperTerminal, using 204

I

Icons 231
Image Recall 301
Imaging Preferences 300
Import 284
Photo 288
Raster Image 288
Signature 288
Import a photograph 301
Import a signature 301
Importing
Photograph 301
Signature 301
Importing Graphics 289, 290
Initialization
Dialup 208
Input point 41
Insert Database Field 286
Insert Date & Time 284
Insert Object 285
Interruptible Commands 56
Introduction 175, 283
Intrusion Area 76

Intrusion Area Name 76
Invert Image Colours 285
Iris Control 180
Italics 288

J
Justify
Centre 286, 288
Left 286, 288
Right 286

L
Left Justify 286, 287
Line Colour 287
Line Tool 286
Links 285
Lock Workstation 284
Log Book
Backup 156
Purge 157
Report 159
Restore 157
Log Commands 179
Log Off 284
Logical Operators, Controller Event Task 60
Low level
Banks 219
Card Readers 218
Elevators 221
Floors 219
OPMs 218

M
Macros, CCTV 194
Manual Control 295
Maximum cards per ACC 205
Medium Pen 287
Menus
Additional 284
Message Forwarding, configuring 69
Message originator 68
Message Originator, configuring 69
Message receiver 68
MIFARE 162
Modems
Remote 200
Server 200
Monitor 181
Groups 183
Monitoring Tours 231
Monitoring Your Site 293
Mouse Pointer 176
Move to Back 285
Move to Front 285
Multiple Facility Codes 34

N
Net Expected Time 227
New 283, 287
Normal Size 286
Number of commands before auto-download 206

O
Object Properties 285
Open 283, 287
Open Iris 176
Operating CCTV 190
Operator Group Privileges
Audit Trail Reports 83
OPM as interface module 216
Optimising an Image 285
Or 160
Output point 41
Output Point
Allowing Access 294

P
Pan 177, 180
Paste 284, 287
Pattern 184, 191
Permanent Commands 56
Phone Number, Server 206
Photo
Import 284
Photo Boxes 297
Photograph
Capturing 301
Importing 301
Plan
Close 283
New 283
Open 283
Save 284
Playback 280
Point
Securing 294
Unsecuring 294
Points 25
Points, Configuring 34
Polygon 287

Polygon Tool 286
Port 179
Port number 261, 272
Preferences
Imaging 300
Preset 191
Presets 183
Print 284, 287
Print Preview 284
Print Setup 284
Printing a card 304
Printing a Guard Tour Report 232
Privilege Level 83
Proceed 305
Process Image 285
Profile 162, 163, 165
Programming
Auxiliary Device 182
Camera 180
CCTV Bus 178, 186
CCTV Controller 179
CCTV Equipment 178, 186
CCTV Unit 179
Monitor 181
Protocol 178
PTZ Camera 180
Pulse Mode, output points 41
Purge Audit Trail 155
Purge Log Book 157

Q

Query Filter 160
Querying a Point 295

R

Random Tour 226
RAS connection
remote 201
Server 200
Raster Image
Import 284
Rectangle 287
Rectangle Tool 286
Redo 284
Redundant comms, pre-requisites 211
Redundant communications overview 210
Refresh Imported Drawing 284
Registering a Tour 229
Report Filters 281
Reports 159, 207
Reset Menu and Toolbar 19
Restore
Audit Trail 155
Database 151
Restore Log Book 157
REX input
Operation Mode 41
Right Justify 286, 287
Right Mouse Button Options 235
Rotate an Image
Clockwise 285
Running
Patterns 191
Sequences 192

S

Save 284, 287
Save As 284
Save As Drawing 284
Scheduled Reporting 161
Screen Size 178
Secured 215
Securing a Point 294
Securing groups and areas 146
Securing input points 146
Securing output points 146
Select 287
Select All 284
Select Tool 286
Sequence 185, 192
Server
Name 26
Server Messaging Event Task 69
Signature
Import 284
Importing 301
SiPass Server Service 204
Sistore Client GUI Controls 279, 280
Sistore Client, Operation 279
Sistore Client, playback 280
Sistore Client, record and playback 280
Site Plans 290
Actioning an Alarm 296
Adding Shortcuts 291
Adding Symbols 290
Importing Graphics 290
Manually Controlling Points 295
Querying a Point 295
Using (to Monitor Your Site) 293

Size of Screen 178
Smart Card 162, 163, 165
Soft Anti-Passback 70
Speed Pan/Tilt 177
Start Immediately 304
Starting a Tour
From the Guard Tour Monitor 232
Status 141
Status Screen
Refresh rate 148
Status Toolbar 286
Straight Line 287
Summary 175, 259
Symbol 141, 289
Close 283
Importing Graphics 289
New 283
Open 283
Save 284
Symbol Colour
Blue 294
Green 294
Magenta 294
Red (Flashing) 294
Red (Solid) 294
System Architecture 259
System Components
Groups 25
Server 25

T

Text
Bold 288
Centre Justify 288
Colour 288
Italics 288
Left Justify 288
Underline 288
Text Tool 286, 287
Text Toolbar 288
Thick Pen 287
Thin Pen 287
Tilt 177, 180
Time Schedule Control 57
Time Schedules 52
Timed Re-entry 70
Timer 54
Tolerance 227
Tool
Add Action 288
Add Group 288
Add Location 288
Add Shortcut 288
Align Bottom 288
Align Centre 288
Align Left 287
Align Right 287
Align Top 288
Arc 287
Bar Code 288
Centre Justify 287
Crosshairs 288
Database Field 288
Ellipse 287
Font 287
Grid 288
Import Photo 288
Import Raster Image 288
Import Signature 288
Left Justify 287
Polygon 287
Rectangle 287
Right Justify 287
Straight Line 287
Text 287
Zoom In 287
Zoom Out 287
Tool Menu 286
Tool Select 287
Toolbar
Drawing 287
Text 288
Tools
Graphics 287
Tour Groups 229
Tour Points
Access 227
Input 227
Tour Stop Log 231
Name 231
Occurred 231
Status 231
Tours 226

U

Underline 288
Undo 284
Ungroup 285

Unit 179
unsealed input 257
Unsecured 215
Unsecuring a Point 294
Unsecuring groups and Intrusion areas 146
Unsecuring input points 146
Unsecuring output points 146
Upload
ACC to Server 209

V

Verification 304
Vertical Arcs 286
Video Capture Card 197
Video Card
Installation 197
Video Source 178
View Menu 286
Viewing
Presets 191
Viewing Employee Details 225
Viewing Pictures 190, 274

W

wild card 116
Windows, password storage 212
Work Groups 84

Z

Zoom 180
Zoom In 176, 286, 287
Zoom Out 176, 286, 287

Issued by
Siemens Switzerland Ltd
Building Technologies Division
International Headquarters
Gubelstrasse 22
CH-6301 Zug
+41 41-724 24 24
www.siemens.com/buildingtechnologies