



P2000AE

Security Management System

Software User Manual

P2000AE

Security Management System

Software User Manual

Version 4.1 and higher, December, 2008

24-10235-8 Revision B



Copyright 2008
Johnson Controls, Inc.
All Rights Reserved

No part of this document may be reproduced without the prior permission of Johnson Controls, Inc.

Acknowledgment

Cardkey P2000, BadgeMaster, and Metasys are trademarks of Johnson Controls, Inc.
All other company and product names are trademarks or registered trademarks of their respective owners.

If this document is translated from the original English version by Johnson Controls, Inc., all reasonable endeavors will be used to ensure the accuracy of translation. Johnson Controls, Inc. shall not be liable for any translation errors contained herein or for incidental or consequential damages in connection with the furnishing or use of this translated material.

Due to continuous development of our products, the information in this document is subject to change without notice. Johnson Controls, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with furnishing or use of this material. Contents of this publication may be preliminary and/or may be changed at any time without any obligation to notify anyone of such revision or change, and shall not be regarded as a warranty.



Declaration of Conformity

This product complies with the requirements of the European Council Electromagnetic Compatibility directive 2004/108/EEC and the Low Voltage Directive 2006/95/EEC.

This equipment must not be modified for any reason and it must be installed as stated in the Manufacturer's instruction.

If this shipment (or any part thereof) is supplied as second-hand equipment, equipment for sale outside the European Economic Area or as spare parts for either a single unit or system, it is not covered by the Directives.

UNDERWRITERS LABORATORIES COMPLIANCE VERIFICATION SHEET
P2000AE SYSTEM
Page 1 of 3

This product is listed under Underwriters Laboratories UL 1076 for Proprietary Burglar Alarm Units and Systems. When installed at the site the following requirements must be met to comply with this standard.

1. Transient protection devices that are installed must not be removed or defeated.
2. The computers audible alarm indicator must not be disabled.
3. All system components must be connected to a UL Listed Uninterruptible Power Supply that provides a minimum of 24 hours of AC emergency power.
4. The maximum number of Panels that may be connected to the P2000 system is 1000.
5. The P2000 shall give priority to signals in the order given below and shall annunciate subsequent signals at a rate no less than one every 10 seconds.

Priority 0	Highest Priority	Hold-up or Panic Alarm
Priority 1	Second Highest	Burglar Alarm
Priority 2	Third Highest	Burglar Alarm Supervision
Priority 3	Fourth Highest	Other Supervisory Alarms
Priority 4	Fifth Highest	Guard Tour

6. The "Pop-up" feature for input points must be enabled.
7. At the host computer (Central Station), alarms must not be filtered away from the host using the feature "Message Filtering".
8. Alarms must not be forwarded away from the host computer (Central Station) using the feature "Message Forwarding".
9. The "Panel Poll Interval" must not exceed 90 seconds for CK705, CK720, CK721 and/or CK721-A panels.
10. The "Host Poll Timeout" must not exceed 200 seconds for CK705, CK720, CK721 and/or CK721-A panels.
11. P2000 server must use transient suppression devices on the LAN interfaces at the computers. The table below specifies the devices that must be used for the various types of LAN interfaces.

LAN Interface	Manufacturer of Device	Device Part Number
10Base-2	Black Box	SP350A-R2 (In-line connector)
10Base-2	Black Box	SP501A ("T" connector)
10Base-5 (AUI)	Black Box	SP362
10/100Base-T	Black Box	SP512A-R3

12. Systems requiring the use of a network hub, router and/or serial port server shall have that equipment installed in a temperature controlled environment. The temperature controlled environment must be maintained between 13 - 35°C (55 - 95°F) by the HVAC system. Twenty-four hour standby power shall be provided for the HVAC system.
13. The installer shall incorporate a supply line transient suppression device complying with the Standard for Transient Voltage Surge Suppressors, UL 1449, with a maximum rating of 330 V. Supply line transient suppression device is to be used with the power supply to the network hub, router, serial port server, serial-to-ethernet converter and RS232-to-RS485 converter.
14. The Hewlett Packard ML370 or ML350 serving as the P2000 host computer shall be installed in a temperature controlled environment. The temperature controlled environment must be maintained between 13 - 35°C (55 - 95°F) by the HVAC system. Twenty four hour standby power shall be provided for the HVAC system.
15. The 240 Vac configurations have not been tested by Underwriters Laboratories except for the ML370 G3 and the ML350 G5.

UNDERWRITERS LABORATORIES COMPLIANCE VERIFICATION SHEET

P2000AE SYSTEM

Page 2 of 3

16. The workstation defined as "Server" must have the alarm monitor parameter set to "always active".
17. For P2000 software version 4.1 or later, when configuring "Service Startup" parameters the following services shall not be disabled.

P2000 RTL Route Service
Metasys III Action Queue
P2000 CK720 Download Service
P2000 CK720 Priority Service v2.1
P2000 CK720 Upload Service
P2000 CK722 Interface Service
P2000 Object Engine Service
P2000 Periodic Service
P2000 Smart Download Service

18. For Line Security over the Internet, between the P2000 server and the controllers CK705, CK720, CK721, CK721-A, CK721M, and CK722 the following equipment shall be used.

NetScreen, Model NS-5XT-X0X (where X is any number 0 to 9), 4-Port VPN router

The P2000 server and router shall be configured to use an encryption method including an Authentication Header (AH) and an algorithm capable of Triple-DES (3DES) or better that is NIST certified.

19. For Line Security over the Internet, between the P2000 server and the controller S321, the following equipment shall be used.

NetScreen, Model NS-5XT-X0X (where X is any number 0 to 9), 4-Port VPN router and

Digi International, Model Digi One SP serial-to-ethernet converter or

B&B Electronics Mfg Co., Model 485OT9L RS232-to-RS485 converter

The P2000 server and router shall be configured to use an encryption method including an Authentication Header (AH) and an algorithm capable of Triple-DES (3DES) or better that is NIST certified.

20. The router and serial port server shall be installed within the same room as the controllers CK705, CK720, CK721, CK721-A, CK721M, and/or CK722 and within 20 feet of the controller when employed for encrypted line security.

21. P2000 systems use the Digi International Model Digi One SP converter or B&B Electronics Model 485OT9L converter to communicate to S321-DIN controllers.

22. The B&B Electronics Model 485OT9L converter shall be installed within the same room as the P2000 server and within 20 feet of the server under all conditions of use.

23. The Digi International Model Digi One SP may be mounted at the central supervising station or the protected premise. When used at the central supervising station, a Cylinx Model TSP-4B-E transient suppression device shall be used on the RS485 communication line. When used at the protected premise, a Blackbox Model RS512A-R3 transient suppression device shall be used on the LAN communication line.

24. A spare router, serial port server, serial-to-ethernet converter and RS232-to-RS485 converter shall be available and put in to service within 6 minutes when they are employed for encrypted line security with the controllers CK705, CK720, CK721, CK721-A, CK721M, and/or CK722.

25. P2000 workstations, network hubs, routers, serial port servers, serial-to-ethernet converter and RS232-to-RS485 converters must use signal line transient suppression devices complying with the Standard for Protectors for Data Communications and Fire Alarm Circuits, UL 497B, with a maximum marked rating of 50V.

26. Alarm signals received at a remote P2000 server via the Remote Message Services from a different P2000 server are supplementary.

UNDERWRITERS LABORATORIES COMPLIANCE VERIFICATION SHEET
P2000AE SYSTEM
Page 3 of 3

27. Alarm signals received at a P2000 workstation are supplementary.
28. Alarm signals received at a personal computer or personal digital assistant through the Web Access feature are supplementary.
29. The communication medium between the protected property and communications service provider shall be for the exclusive use of the protected property and is not to be shared with other communications service provider subscriber.
30. From Message Data Configuration, under CK722 Device, for each Alarm Category on the Alarm Options tab, the following parameters must have its Enabled value set to True:
 - Panel Down
 - Hardware Module not Operational
 - Notification Event Dropped
 - Panel Input Point
31. The following features have not been investigated by Underwriters Laboratories
 - BACnet interface to Metasys® products
 - Dial-Up
 - Intrusion
 - Stop and Search
32. The following products have not been investigated by Underwriters Laboratories
 - Aritech®
 - S300-KDM

Table of Contents

Chapter 1: Introduction	1
Getting Started	1
Chapter Summaries	1
Manual Conventions.....	2
Basic System Components	2
Registration Parameters.....	4
Main Menu.....	4
System Overview	4
Basic Configuration	5
Network Communication.....	5
Loop Communication.....	6
Communication Modes	6
Types of Communication.....	6
Access Requests	7
Time and Time Zones.....	7
Access Profiles	7
Valid or Invalid Badges	7
Controlling Special Access.....	7
Overriding Basic Access.....	7
Assigning Access Profiles.....	8
Alarms	8
External Device Alarms	8
Door Alarms	8
Software-Only Alarms.....	8
P2000 Host Alarms	8
Remote Alarms	8
Non-alarm Input Points	8
Output Relays	9
Input/Output Linking.....	9
Activating Outputs by Events.....	9
Activating Outputs Manually	9
Events	9
Database Partitioning.....	9
Logging On to the P2000 System Software	10
Changing the Default Login Values.....	11
Logging Out of the P2000 System Software	12
Navigating through the P2000 System.....	12
Mouse Conventions	12

Instruction Conventions.....	13
Menu Shortcuts.....	13
Verification Passwords.....	13
Context Sensitive Help.....	14
Online Help	14
Viewing the Toolbar	14
Using P2000 SCT.....	14
Starting the P2000 SCT.....	15
Chapter 2: Configuring the System.....	17
System Configuration Overview	17
Using the System Configuration Window.....	17
Set Up Workstations and System Users	19
Workstations	19
Workstation Field Definitions	20
Adding Users to the System	21
User Role Management.....	21
Assigning System Users.....	23
Changing the User Password.....	23
Setting Up User Accounts.....	23
Adding a Login Name and Password for the P2000 System into the Operating System.....	23
Configure System Components	27
Registration Parameters	28
Site Parameters	29
Site Parameters Field Definitions	30
Local Site	42
Local Configuration	43
Time Zones	44
Configuring Time Blocks.....	44
Holiday Types.....	46
Holiday	46
Using the Holiday Calendar	47
Assigning Holiday Types	47
Configure Hardware Components.....	48
Hardware Configuration Sequence.....	48
Create Panels	48
Panel Naming Conventions	48
Loop Configuration	48
Soft Input Points	50
Edit Panel Field Definitions.....	50
Configure Panel Components.....	56
Configure Panel Time Zones	56
Configure Panel Holidays	57
Configure Panel Card Formats.....	58

Configure Additional Panel Components.....	58
Create and Configure Terminals.....	58
Set up Terminals for each Panel	59
Edit Terminal Field Definitions	60
Create Terminal Groups	69
Configure PIN Codes.....	70
PIN Only	71
PIN + Card ID	71
PIN.....	71
Four-Digit PINs	72
PIN Duress	72
PIN Retry Alarm.....	72
Create Input and Output Points and Groups.....	72
Create Output Points and Groups	73
Create Input Points and Groups	74
Create Input Points	74
Input Point Field Definitions	75
Configuring Reader Terminal Hardwired Input Points	80
Using Reader Terminal Door Contact Input Points.....	80
Using the Terminal Down Input Point	81
Create Input Groups	81
Creating Instruction Text.....	82
Create Panel Card Events	83
Panel Card Event Field Definitions.....	84
Configure Soft Alarms.....	86
Soft Alarms Field Definitions.....	86
Configure Elevators and Cabinets.....	87
Elevator Access Control.....	87
General Overview	87
Low Level Interface.....	88
High Level Interface.....	88
Basic Definitions	88
Defining Floor Names	89
Defining Floor Masks	90
Configuring Elevators	91
Elevator Configuration Field Definitions.....	91
Configuring Floors	93
Defining Floor Groups.....	94
Creating Access Groups for Elevator Floors	94
Cabinet Access Control.....	94
Defining Door Names	95
Defining Door Masks	96
Configuring Cabinets	96
Cabinet Configuration Field Definitions	96
Configuring Doors.....	97
Defining Door Groups	98

Creating Access Groups for Cabinet Doors.....	99
Configure Message Filtering and Message Routing	99
Operators and Messages.....	99
Basic Principles and Definitions.....	99
Sequence of Steps.....	100
Message Filtering.....	100
Create Message Filter Groups.....	107
Message Routing	108
Configuring P2000 Remote Servers	108
P2000 Remote Server Field Definitions.....	108
Set Up Message Data Configuration.....	110
Aritech OPC Intrusion Message Configuration	110
CK722 Message Configuration	111
Time and Attendance Interface	112
T&A Terminal Message Configuration.....	112
Time & Attendance Object Message Configuration.....	113
Work Schedule Message Configuration	113
Message Data Configuration Alarm Options.....	114
Set up Access Groups, Entity Options, and Security Roles	117
Create Access Groups.....	117
Entity Options.....	118
Define Organization Elements	118
Define Entity Categories	119
Define Entity Groups.....	121
Create Access Profile Templates	122
Create User Defined Fields	125
Define Identifier Purposes	127
Security Roles.....	127
Security Flags	128
Access Security Roles	129
Privilege Security Roles.....	130
Entering Entities.....	130
Chapter 3: Operating the System	131
Entity Management	131
Entering Entity Information	132
Viewing Entity Information	132
Entity Field Definitions	133
Filtering Entity Data	151
Entity Duplicator.....	151
Entity Bulk Edit.....	152
Auto Badge Management	153
Entity Resync	155
Entity Status Resync in Legacy Panels	155
Entity Status Resync in CK722 Panels.....	156

Image Recall	158
Monitoring Alarms	160
Alarm Configuration	160
Alarm Category	160
Alarm Handling.....	161
Monitoring Remote Alarms.....	162
Alarm Monitor Definitions.....	163
Alarm Response Field Definitions.....	166
Configuring Alarm Colors	167
Creating Predefined Alarm Response Text.....	169
Monitoring Alarms Using the SIA Interface	169
To View Messages from the SIA Device:.....	170
Message Forwarding.....	171
Operator Controls	172
Controlling Doors	172
Controlling Outputs	173
Controlling Panel Relays.....	174
Security Threat Level Control.....	174
Defining Security Levels	174
Applying Security Level	175
Input Point Suppression	176
Using the Control Center.....	177
Controlling Areas and Muster Zones.....	178
Area Control	178
Configuring the Area.....	178
Controlling the Area	181
Defining Area Filters	183
Displaying Area Details.....	183
Area Details Field Definitions	184
Area Layout	185
Mustering	186
Basic Definitions	187
Sequence of Steps	188
Define Risk Areas and Muster Zones	188
Muster Zone Definition Fields.....	188
Defining Zone Terminals.....	192
Defining Muster Terminals.....	192
Defining Sequester Terminals	193
Mustering Events	193
Controlling Muster Zones.....	194
Muster Zone Status and Control Field Definitions	195
Viewing and Printing Muster Transactions in Real Time	198
Muster Reports	198
Intrusion Detection	199
Basic Definitions.....	200
Basic Intrusion Components	200

Intrusion Configuration	201
Intrusion Access Groups	201
Intrusion Management	202
Using the Intrusion Command Center	202
Viewing Intrusion Transactions Using the Real Time List.....	204
Monitoring Intrusion Using the Real Time Map.....	204
Viewing Intrusion Status Using the System Status Display.....	205
Central Station Support.....	205
Intrusion Events	205
OPC Aritech Intrusion Interface	205
Creating Events.....	206
Using Event Configuration Dialog Boxes	206
Creating Triggers	206
Trigger Field Definitions.....	207
Creating Actions.....	208
Event Actions Field Definitions	209
OPC Server Event Actions	209
Counting Events.....	211
Creating Manual Triggers	212
Monitoring the System in Real Time	213
Using the Real Time List.....	213
Monitoring Remote Messages in Real Time.....	213
Viewing Real Time List Transactions.....	214
To Display Color Coded Transactions:.....	216
Printing the Real Time List	216
Viewing History Information	217
Using the Real Time Map	218
Sub Maps and Attachments.....	218
Opening a Door	219
Activating Events from the Real Time Map.....	220
Creating a Real Time Map	220
Adding Map Attachments.....	222
Adding Image Sets.....	223
Chapter 4: System Options	225
Partitions	225
Partition Types	226
Regular Partitions	226
The Super User Partition	226
Creating Partitions	227
Video Imaging	227
Video Imaging Specifications.....	228
Defining a Video Imaging Workstation.....	228
Printing a Badge	229
Capturing the Portrait and Signature Images	229

Viewing and Printing the Badge.....	230
MIS Interface	231
MIS Prerequisites.....	231
Understanding the Input and Output Tables	232
Partitioned Systems	232
Using the MIS Interface.....	232
Metasys Integration (BACnet)	233
Overview	233
Theory of Operation	233
System Setup.....	235
Setting Up External IPs.....	235
Setting Up BACnet Site Options	236
BACnet Site Field Definitions.....	236
Configuring Hardware Components for BACnet Interface.....	237
Setting Up BACnet Action Interlocks	237
Action Interlock Operation	237
M3/M5 Setup.....	238
Troubleshooting	238
Duplicate Object Name Errors	238
Msg Rejected Errors	238
Action Interlock Errors	239
Metasys System Extended Architecture.....	239
Defining MSEA Graphics	239
Registering the P2000 Server with a Site Director.....	240
Guard Tour	242
Basic Principles and Definitions	242
Sequence of Steps.....	243
Defining System Hardware for Guard Tour Operation	243
Assigning Tour Badges	243
Configuring Guard Tours.....	244
Using the Guard Tour Configuration Window	244
Timezones, Start and Abort Times	246
Additional Guard Tour Options	247
Adding Stations to the Guard Tour.....	249
Tour Station Definition Fields	249
Controlling Guard Tours	251
Guard Tour Handling	254
Guard Tour Details	254
Guard Tour Notes	255
Viewing and Printing Transactions in Real Time.....	255
CCTV.....	256
Using P2000 functions with the CCTV Option	257
CCTV Configuration Overview.....	257
Points to Note	258
Using the CCTV/AV Configuration Window	258
Defining System Hardware for the CCTV Option.....	259

Namespace and Database	259
Relationship Between the Namespace and Database	259
CCTV Naming Conventions.....	260
Naming Items for the CCTV Server Namespace.....	260
Defining the Number of Namespace Items.....	261
Number of Default Items Permitted	261
Changing the Number of Namespace Items.....	261
Switch Protocols	262
Tristate Check Boxes.....	262
CCTV Option Components	262
CCTV Server.....	263
Create and Configure the CCTV Server	263
Edit Server Field Definitions	264
Switches.....	265
Create and Configure Switches	265
Edit CCTV Switch Field Definitions.....	265
Alarms, Auxiliaries, Macros and Tours	268
Alarms.....	268
Auxiliaries	268
Macros	268
Tours.....	268
Edit CCTV Alarm, Auxiliary, Macro and Tour Field Definitions.....	269
Monitors	269
Create and Configure Monitors.....	269
Edit CCTV Monitor Tabs.....	270
Sequences	271
Edit CCTV Sequence Field Definitions	272
Cameras	272
Create and Configure Cameras	272
Edit CCTV Camera Tabs	272
Camera Auxiliaries, Patterns and Presets	275
Camera Auxiliaries.....	275
Patterns	275
Presets.....	275
Edit CCTV Named Camera Item Field Definitions	275
CCTV Control.....	276
CCTV Standard Controls	277
Selecting the Item to Control	277
Operating the Controls.....	277
Using Switch Controls.....	277
Selecting a Switch	278
Selecting a Tour, Macro or Switch Auxiliary	278
Using Tour, Macro or Switch Auxiliary Controls	278
Using the Monitor Controls	279
Selecting a Monitor.....	279
Selecting a Sequence.....	279

Using Sequence Controls	279
Using the Camera Controls	279
Selecting a Camera	280
Selecting a Pattern, Preset or Camera Auxiliary	280
Using Pattern, Preset or Camera Auxiliary Controls.....	280
CCTV Option Event Actions.....	281
CCTV Event Action Field Definitions	282
DVR.....	282
Redundancy	283
FDA Part 11.....	283
Intercom	284
Hardware Requirements	284
Intercom System Hardware Verification	285
Intercom Configuration.....	285
Intercom Exchange.....	285
Intercom Stations.....	286
Intercom Control.....	287
Controlling Intercom Stations using the Real Time Map.....	289
Intercom Events	289
OPC Intercom Control.....	289
P2000 Enterprise.....	291
Enterprise Parameters	292
Assign Entities Enterprise Access.....	293
Define Global Access Rights.....	294
Web Access	295
Sequence of Steps.....	296
Creating and Assigning Web Access User Roles	296
Defining Web Access Options.....	299
Web Access Options Field Definitions	299
Defining Request Approvers	300
Submitting Requests using Web Access	303
Web Access Functions.....	304
Employee Services.....	304
Guard Services	305
Management Services	305
Visitor Management.....	306
Work Scheduler	306
Emergency Access Disable	307
Processing Web Access Requests	307
Customizing the Web Access Interface	307
Assigning Styles to Web Access Users	308
Chapter 5: System Maintenance.....	309
Downloading Data to Panels	309
Download Status	311

Smart Download Control	311
Controlling and Monitoring P2000 Services	312
Service Startup Configuration	312
P2000 Services Definitions.....	314
Starting and Stopping Service Control.....	315
Controlling Services using Windows Administrative Tools	316
Controlling Services through the Service Monitor.....	317
Workstation Status	317
System Status	318
Writing the Controller Database to Flash Memory	321
Updating CK705/CK720 Panels	322
Updating CK722 Panels	323
Updating S321 Panels.....	324
Database Maintenance	325
Database Maintenance Actions	326
Database Backup.....	329
Configuring a Backup Device	329
To Perform Manual Backups:	330
Advanced Backups	331
Automatic Backups	331
FDA Part 11 Backups	332
Database Restore	332
System Validation	334
Request Queue View	335
Searching Specific Requests	337
Viewing Request Details	338
Chapter 6: System Reports	339
Using P2000 Standard Reports.....	339
P2000 Standard Report Definitions.....	342
Selected Sample Reports.....	344
Running the Alarm Activity Report.....	344
Running the Entities Report.....	345
Running the Entities without Identifiers Report.....	347
Running the Transaction History Report.....	348
Creating Custom Reports.....	349
Creating a Custom Crystal Report for the P2000 System	349
Database Table Definitions.....	349
Report Interfaces	349
To Import a Custom Crystal Report into the P2000 System:.....	350
Editing a P2000 Standard Report in Crystal	351
To Export an Existing Standard Report from the P2000 System:.....	351
To Edit the P2000 Report in Crystal	351

Appendix A: Event Triggers/Actions	353
Trigger Types	353
Category: Alarm	353
Category: Anti-Loitering Object	354
Category: Anti-Passback Object	354
Category: Area	355
Category: Audit	355
Category: Automatic Payment Machine	356
Category: AV	356
Category: Badge	356
Category: Counter	358
Category: Date / Time	358
Category: External Trigger	358
Category: Input Point	359
Category: Integration Device	359
Category: Integration Server	360
Category: Integration Station	360
Category: Interlock Object	361
Category: Intrusion Annunciator	361
Category: Intrusion Area	361
Category: Intrusion Device	362
Category: Intrusion Keypad	363
Category: Intrusion Zone	363
Category: Jacques Intercom Station	364
Category: Lane Equipment Cabinet Door	364
Category: Multi Command Object	364
Category: Mustering	365
Category: Notification Object	365
Category: Occupancy Object	365
Category: Operator	365
Category: Output Point	366
Category: Panel	366
Category: S300 Hardware	367
Category: Station	367
Category: Stop and Search	367
Category: Terminal	367
Category: Time & Attendance Reader	369
Category: Time Zone	369
Category: Work Schedule	370
Category: XMan Holding Room	370
Category: XMan XRay Machine	370
Category: Zenitel Intercom Station	371
Event Action Types	371
Category: Anti-Passback	371
Category: Audio-Visual	372

Category: BACnet	372
Category: Badge	372
Category: CCTV	373
Category: CK722 BACNet	373
Category: Download - BACNet	373
Category: Download - Legacy	374
Category: Host	374
Category: Inputs	376
Category: Intercom	376
Category: Intrusion Annunciator	376
Category: Intrusion Area	377
Category: Intrusion Zone	377
Category: MCO	377
Category: Metasys Interlock	377
Category: Mustering	377
Category: Occupancy	377
Category: OPC Server	377
Category: Outputs	377
Category: Panel	377
Category: Security Level	378
Category: Terminal	378
Appendix B: Message Types and Sub-Types	381
Appendix C: Panel Comparison Matrix	389
Appendix D: CCTV Switch Protocols	393
Communications	393
Camera Movement Actions	393
Monitor Sequences	394
General ASCII Protocol	395
Commands Supported	395
American Dynamics	397
The American Dynamics Protocol	397
Supported CCTV Controls	397
Supported CCTV Event Actions	397
Supported OPCWrite Event Actions	398
Autorepeat Actions	398
Automatic Status Update Tags	398
Maximum and Default Values	398
BetaTech	399
Switch Configuration	399
Keyboard 16 Commands	399

The BetaTech Protocol	399
Supported CCTV Controls	399
Supported CCTV Event Actions.....	399
Supported OPCWrite Event Actions	400
Autorepeat Actions	400
Automatic Status Update Tags.....	400
Maximum and Default Values	400
Geutebrück - GST Interface	401
The Geutebrück Protocol	401
Supported CCTV Controls	401
Supported CCTV Event Actions.....	402
Supported OPCWrite Event Actions	402
Macros	402
Camera Auxiliaries.....	402
Monitor Sequences.....	403
Autorepeat Actions	403
Automatic Status Update Tags.....	403
Maximum and Default Values	403
Panasonic.....	405
Switch Configuration	405
Panasonic SX850 Protocol	405
Supported CCTV Controls	405
Supported CCTV Event Actions.....	406
Supported OPCWrite Event Actions	406
Camera Movement Commands.....	406
Autorepeat Actions	406
Automatic Status Update Tags.....	406
Maximum and Default Values	407
Pelco	409
The Pelco 9760 Protocol.....	409
Supported CCTV Controls	409
Supported CCTV Event Actions.....	410
Supported OPCWrite Event Actions	410
Autorepeat Actions	410
Automatic Status Update Tags.....	411
Macro Programming.....	411
Recording Patterns	411
Maximum and Default Values	411
Philips Burle (Bosch)	413
Switch Macros.....	413
The Philips Burle Protocol.....	413
Supported CCTV Controls	414
Supported CCTV Event Actions.....	414
Supported OPCWrite Event Actions	414
Autorepeat Actions	414
Automatic Status Update Tags.....	414

Maximum and Default Values	415
Cabling Configuration	415
Ultrak	417
Switch Configuration	417
Keyboard 64 Commands	417
The Ultrak MaxPro-1000 Protocol.....	417
Supported CCTV Controls	417
Supported CCTV Event Actions.....	417
Supported OPCWrite Event Actions	418
Auxiliaries	418
Monitor Sequences.....	418
Autorepeat Actions	418
Automatic Status Update Tags.....	418
Maximum and Default Values	418
Vicon	421
Switch Configuration	421
The Vicon Protocol.....	421
Supported CCTV Controls	421
Momentary and Latched Auxiliaries	422
Camera Lens Speed Control	422
Supported CCTV Event Actions.....	422
Supported OPCWrite Event Actions	422
Autorepeat Actions	423
Automatic Status Update Tags.....	423
Maximum and Default Values	423
Appendix E: CCTV Server Namespace Definitions	425
Flags	425
Notes.....	425
Namespace Tags	426
Switch Namespace Tags	426
Monitor Namespace Tags.....	431
Camera Namespace Tags.....	433
Macro Namespace Tags.....	437
Auxiliary Namespace Tags	437
Tour Namespace Tags	437
Alarm Namespace Tags	437
Sequence Namespace Tags	438
Pattern Namespace Tags	438
Preset Namespace Tags	438
Appendix F: DCOM Configuration.....	439
DCOM Installation.....	439

Appendix G: Using a Keypad Reader on CK721/720/705 Panels

Invoking Access Requests from a Keypad.....	441
To invoke access with a Badge:	441
To invoke access with PIN Only:	441
To invoke access with Card ID:	441
To invoke access with PIN and Card ID:	441
To invoke access using PIN and badge:	442
To invoke access with PIN and badge, allowing PIN after badge:	442
Invoking Access Requests from a Keypad with a Common PIN	442
To invoke access with a Common PIN:	442
Invoking Timed Overrides from a Keypad	442
To invoke Timed Override with Badge:.....	442
To invoke Timed Override with PIN Only:.....	442
To invoke Timed Override with Card ID:.....	443
To invoke Timed Override with PIN and Card ID:.....	443
To invoke Timed Override with PIN and Badge:.....	444
To invoke Timed Override with PIN and Badge, allowing PIN after badge:	444
Invoking Panel Card Events from a Keypad.....	445
To invoke Panel Card Events with Badge:	445
To invoke Panel Card Events with PIN Only:	445
To invoke Panel Card Events with Card ID:	445
To invoke Panel Card Events with PIN and Card ID:	446
To invoke Panel Card Events with PIN and Badge:	446
To invoke Panel Card Events with PIN and Badge, allowing PIN after badge:	447
Quick Guide to Using Keypad Readers.....	447

Appendix H: Troubleshooting

Windows 2003 Authentication	451
SQL Server Authentication	451
P2000AE Authentication.....	452
Testing the Workstation	452
Troubleshooting Workstation Problems	452
P2000AE Login Troubleshooting	453
P2000AE Network Troubleshooting.....	454
CCTV Control Troubleshooting.....	455

Appendix I: Secured Premises Notification Settings

Index

Chapter 1: Introduction

P2000 represents the latest technology in integrated security management systems. Using Microsoft® Windows® 2003 operating system, and CK705, CK720, CK721, and CK722 controllers, the P2000 software is easy to configure and use, and offers the power and speed of network communications.

Through its intuitively laid-out menus, the user can create entity records, define hardware components, and control access through badging, CCTV, area control, mustering, and elevator control to name a few, as well as monitor local and remote transactions and alarm activity in real time.

Note: “P2000AE” is also referred to as “P2000” throughout this manual. In addition, the screen captures shown in this manual may differ slightly, depending on the software version you are using.

Getting Started

Operators familiar with Windows-based programs should easily master the P2000 software. This manual provides complete instructions on configuring and operating the system; and virtually the entire manual content is accessible from P2000’s online Help documentation.

Take a few moments to review the information in this chapter and get familiar with the P2000 system basics.

Chapter Summaries

- **Chapter 1: Introduction.** Presents the conventions used throughout this manual, an overview of basic system components, and menu options available in the system. The system overview will familiarize you with P2000 system capabilities and how to log on, log out, and navigate through the system.

- **Chapter 2: Configuring the System.** Directs you through tasks to properly configure your system for operation. Elements featured in this chapter include: Workstations, Operators, User Roles, Site Parameters, Local Configuration, Time Zones, Holidays, Panels, Terminals, Input and Output definitions, Elevators/Cabinets, Message Filtering and Routing, Access Groups, and Entity Options.

- **Chapter 3: Operating the System.** Describes the primary features used to run the P2000 system. It will familiarize you with system menus, as well as show you how to provide access to entities, monitor alarms, control doors, set outputs and panel relays, control areas and muster zones, control and detect intrusion in a facility, create events, and monitor the system in real time.

- **Chapter 4: System Options.** Describes additional options that can be used in conjunction with the P2000 system package. These include Partitioning, Video Imaging, MIS Interface, Metasys® Integration (BACnet), Metasys System Extended Architecture, Guard Tour, CCTV, DVR, Redundancy,

FDA Part 11, Intercom, P2000 Enterprise, and Web Access.

- **Chapter 5: System Maintenance.** Describes the tools available to maintain your system in optimum operating condition.
- **Chapter 6: System Reports.** Includes a complete list of P2000 Standard Reports, along with a brief description of each and how they might be used.
- **Appendix A: Event Triggers/Actions.** Lists all trigger categories, types, conditions, and event action types available for Event configuration.
- **Appendix B: Message Types and Sub-Types.** Lists all message types and sub-types available for Message Filtering.
- **Appendix C: Panel Comparison Matrix.** Lists the panel types supported by the P2000 system, including their features and capabilities.
- **Appendix D: CCTV Switch Protocols.** Describes the CCTV Switch Protocols that are supported by the CCTV option.
- **Appendix E: CCTV Server Namespace Definitions.** Describes the CCTV Server namespace tags.
- **Appendix F: DCOM Configuration.** Describes changes to the DCOM settings that need to be made to assure proper CCTV configuration.
- **Appendix G: Using a Keypad Reader on CK721/720/705 Panels.** Presents the sequence of actions at a keypad reader.
- **Appendix H: Troubleshooting.** Explains connection problems and how to solve them.
- **Appendix I: Secured Premises Notification Settings.** Describes the sequence of actions needed to notify operators when a panel card event is used to unsuppress alarm signals.

Manual Conventions

The following terms and conventions are used throughout this manual.

Note: Denotes additional or special information relevant to the current topic or procedure.

TIP: The tip box describes time-saving or additional information.



CAUTION

Indicates possible damage to the equipment including software, if the procedures are not performed correctly.



APPLICATION NOTE

Provides essential information relevant to the program.

Basic System Components

The following terms describe the P2000 system, including hardware and software terms, computer equipment, and field equipment. Figure 1-1 displays the P2000 System with Network Panels.

P2000 Server – The main computer in the system. The system Server runs the P2000 system software, stores database information, and communicates with the field panels. The P2000 Server may also be referred to as the Database (DB) and Communications (Comms.) Server.

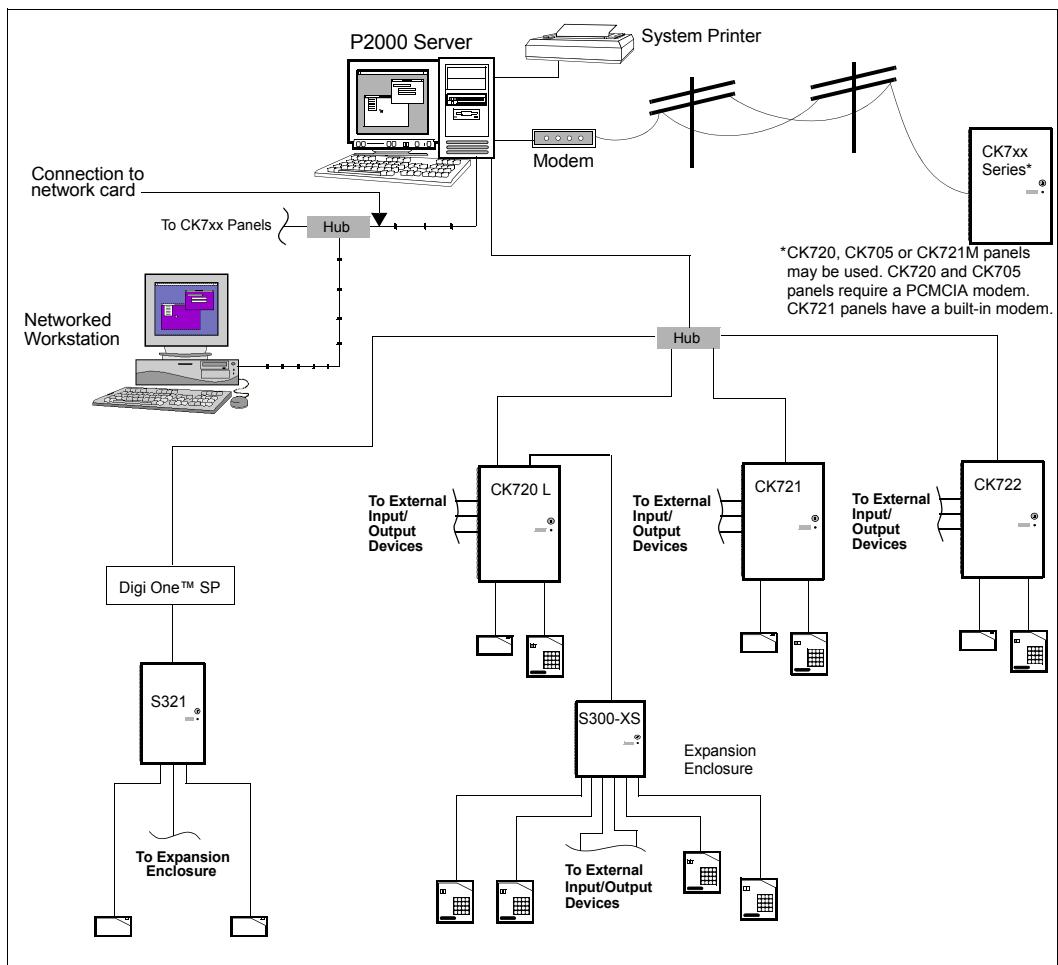


Figure 1-1.P2000 System with Network Panels



We recommend the system Server be used only as a Server and not as an additional day-to-day workstation.

CAUTION *You must protect the Server from physical access by unauthorized users. Use the Server only for those tasks that must be performed from the Server.*

Workstations – Workstations allow additional users to monitor and configure the P2000 system. Workstations communicate with the Server via an Ethernet TCP/IP local area net-

work (LAN). Workstations run the P2000 software on Microsoft Windows 2000, Windows XP or Vista Business operating systems.

P2000 Enterprise – System that consists of one or more P2000 Sites.

P2000 Site – Uniquely identified by its Local Site Name. A P2000 Site can have multiple locations but only one P2000 Server.

P2000 Location - A physical location or place with a P2000 workstation, panel, terminal, input or output point.

System Printer – System printers, connected either to the Server or to workstations, provide real-time transaction printing or report printing capabilities.

Field Panels – This term refers to CK705, CK720, CK721, and CK722 network panels. These connect to terminals and communicate with the Server. CK705, CK720, and CK721 are called “legacy panels.” CK722 is also called BACnet panel. Refer to *Appendix C: Panel Comparison Matrix* for a detailed list of features and capabilities.

Terminals – Terminals provide a point of contact with panels to facilitate a variety of functions. Terminal add-on boards are used to connect readers, input points, and output points. These terminals are circuit boards mounted in the basic panel enclosure or an expansion enclosure, and may include the S300-DIN-RDR2S and RDR2 (dual reader boards), SIO8 (eight outputs and eight 4-state inputs), IO8 (eight outputs and eight 2-state inputs), I16 (sixteen 2-state inputs), and the SI8 (eight 4-state inputs).

External Device – This general term describes any device wired to one of the terminal types, such as readers, motion sensors or other input devices, door strikes, or audible alarm devices.

Registration Parameters

The options included with your system and the maximum badge capacity are enabled via the entry of your valid Registration Key provided by *Johnson Controls*. The Registration Key is associated with your purchase contract.

Main Menu

The Main menu is the backbone of the P2000 system. From here, you select each feature and option available in the system. While logical operation of the system does not follow the Main menu from right-to-left, every menu and option is displayed.

System Overview

This overview section is designed to help P2000 users understand basic operation prior to configuring the system. The following topics are covered:

Basic Configuration – An overview of system configuration.

Communication Modes – An overview of the P2000 system operating modes and communications types.

Access Requests – How the system determines whether an entity is granted or denied access at a door.

Controlling Special Access – Describes features that can override normal system operation.

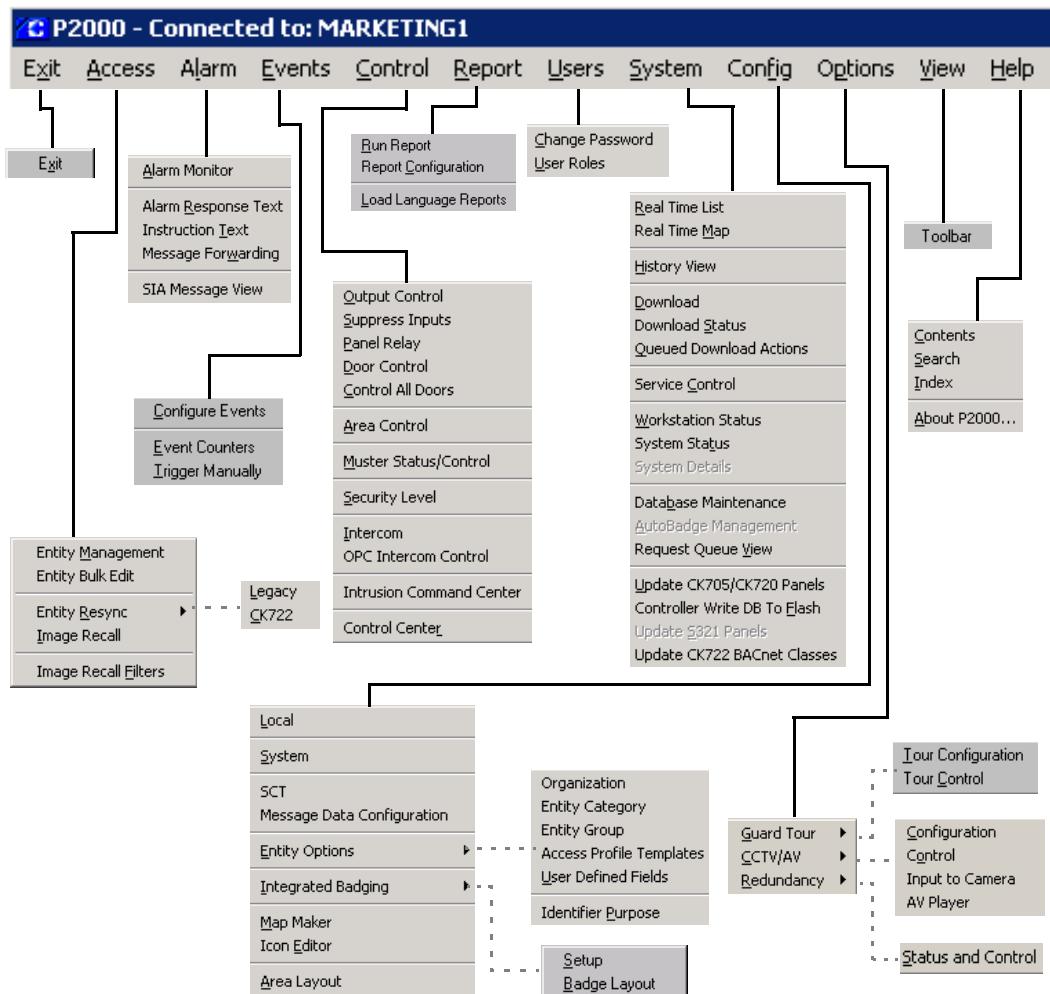
Alarms – Various types of alarms are described.

Non-alarm Input Points – A basic description of input points.

Output Relays – A basic description of output relays.

Events – How input points and output relays can be manipulated automatically or manually in various ways to create events.

Database Partitioning – An overview of how database partitioning is used within the P2000 system.



Basic Configuration

Network Communication

CK7xx panels support terminals, readers, and input/output devices, and connect to the P2000 Server via a network card. Each panel has an embedded 32-bit processor, with 64-reader capability for CK722s, 16-reader capability for CK720s and CK721s, and 4-reader capability for CK705s.

S321 panels can also connect to the P2000 Server through the network using a Digi One™ SP converter box. S321 panels have 2-reader capability.

Note: S321 panels are not available in this release.

A single workstation is shown in Figure 1-1 on page 3; however, a fully configured Server can support multiple workstations. The number of

workstations (including the Server) depends on the type of system you purchased.

If Integrated Video Imaging is part of the configuration, the Video Imaging workstation is attached to the network similarly to the workstations.

Loop Communication

In a combined P2000 system configuration, the Server connects via a current loop configuration to S321 panels using an RS232-to-RS485 converter connected to a built-in serial port. The P2000 loop system can support up to 32 loops, with up to thirty S321 panels per loop.

Communication Modes

The P2000 Server communicates with panels that provide reader interfaces, input points, or output relays. Communication is bi-directional, some messages are sent from the Server to the field panels, other messages are sent from the panels to the Server, and then can be distributed within the system (e.g. workstations). The volume of messages across the communication link depends, in part, on the overall operating mode of the system.

While several factors affect overall system performance (performance is defined as the speed with which communication occurs between the Server, workstations, and field panels), the most significant factor is operating mode, which is defined when configuring the system. The P2000 system provides the following three operating modes:

Local – In this mode, the field panels make all access decisions. This eliminates the need for panels to communicate with the Server every time an access request is presented at a reader. Local mode provides the best overall system capability; however, access will be denied to those badges not stored in the panel memory.

Central – This mode is useful when you want to assign access restrictions on a global scale (throughout the entire system). All access requests are forwarded to the Server for an access grant or deny decision. Central mode has the most impact on system performance (the slowest), and should be used only when necessary.

Shared – Access decisions are made either at the panel level or by the Server. Field panels will first search for a badge in their memory, as in Local mode. If a badge's record is not found at the panel level, the access request is then forwarded to the Server, as in Central mode. Shared mode is useful when a panel's badge capacity is exceeded.

Shared mode is the preferred method of operation. This mode not only gives you the high performance of Local mode for badges stored in the panel memory, but will also give proper access to all badges even if they are not stored in the panel memory.

Types of Communication

The P2000 Server communicates with system field panels via Transactions, Downloads, and Commands.

Transactions – Transactions indicate some form of system activity. They can include such items as access requests and general system messages such as when a panel loses communication with a reader. Typically, transactions represent communication initiated at field panels and sent to the P2000 Server.

Downloads – Downloads refer to the transfer of system configuration information from the P2000 Server to the memory of the field panels. This includes information such as badge records and access rights. Network panels can be downloaded in minutes using the download feature.

Commands – Commands, such as opening a door manually, are initiated at the Server and sent to the appropriate panels.

Access Requests

The basic function of the P2000 system is to grant or deny entities access to areas in and around your facility or facilities.

The P2000 system makes access decisions based on:

- Time and Time Zones
- Access Profiles
- Valid or invalid badges

Time and Time Zones

Almost every P2000 system feature can be controlled by time. This includes basic access where readers and badges can be enabled or disabled. By configuring time zones you can determine the following:

- When any reader-controlled door in your facility can grant access to a valid badge.
- At which times during a 24-hour period an entity can be granted access at a reader-controlled door.
- Reader override.

Access Profiles

Access profiles relate to the time of day, areas, and access groups an entity can be granted access. A badge can be valid in all other

respects, but the entity can be restricted as to the times and days they can enter your facility, or an area within the facility. The P2000 system also provides the means to grant entities special privileges, which is also described as *special access*.

Valid or Invalid Badges

The P2000 system provides many methods for you to determine what constitutes a valid badge in your system. These include the use of the following:

- Facility Codes
- Encoded Badge Number
- Issue Level
- Expiration Date
- Badge Time Zones
- Badge Access Groups

Controlling Special Access

In addition to basic access, operators can control special access for overriding the normal operation of the system. The two main categories for special access are:

- Overriding Basic Access
- Assigning Access Profiles

Overriding Basic Access

In most cases you will want to configure the P2000 system for basic access control and also provide the means for special access. In general, special access may be necessary at predetermined times or may be random occurrences as circumstances warrant. The P2000 system allows you to account for both, with features such as the following:

Timed Override – A door can be automatically unlocked between specified times.

Extended Access – A door can be manually unlocked and propped open as needed.

Auxiliary Access – An external device, such as a push button, can temporarily open a door without the use of a badge or PIN code.

Assigning Access Profiles

The other means of providing special access is through access profiles, which are assigned to badge identifiers. Access profiles allow the entity the following access:

- Gaining access to your facility outside normal operating hours.
- Granting different access times, to satisfy the requirements for assisted access according to ADA (Americans with Disabilities Act).
- Manually executing override features such as Extended Access.

Alarms

Another fundamental principle of P2000 system operation is to report alarm activities. Alarms can be triggered by several methods including the following:

- External Device Alarms
- Door Alarms
- Software-Only Alarms
- P2000 Host Alarms
- Remote Alarms

External Device Alarms

External devices, such as motion or glass break sensors, can be wired to P2000 input points. When these devices become active, as in a motion sensor detecting movement, they trigger the input point, which causes an alarm. You can define how input points respond when acti-

vated, whether or not they trigger output relays, and at which times an alarm can be activated. This offers you the flexibility of automating the alarm operation.

Door Alarms

When a door is unsecured due to unauthorized activities, the door is considered to be in a forced alarm state and is reported to the system. The system can also monitor cases where the door is “propped” open after a valid access grant.

Software-Only Alarms

Software-only alarms are unlike external device alarms in that software alarms are triggered by system activities (such as when a panel loses AC power), rather than by external devices, which are wired to the system panels and terminals.

P2000 Host Alarms

The P2000 system also reports host alarms, such as alarms originated by P2000 event actions, Redundancy Failover alarms or FDA Record Retention alarms.

Remote Alarms

These are external device alarms, door alarms, software-only alarms, and host alarms that are generated at remote sites.

Non-alarm Input Points

The P2000 system allows you to use input points for activities other than alarms. For example, a motion sensor wired to an input might be used to turn on lights.

Output Relays

Where input points are triggered by external devices, output relays allow you to trigger external devices using the P2000 system. These devices might include warning indicators for alarm situations or non-alarm related functions such as lighting or environment control. In general, output relays are activated by one of the following:

- Input/Output Linking
- Events
- Manually

Input/Output Linking

The P2000 system allows you to form individual output relays into groups (as a note, you can also group input points). The primary purpose of linking inputs to output relays is to trigger external devices in the following situations:

- In emergency situations. These might include room lighting or warning indicators such as flashing lights or sirens.
- To automatically activate a building function such as lighting or environment control.

Activating Outputs by Events

As an alternative to input/output linking, output relays can also be activated either manually or automatically by events.

Activating Outputs Manually

Operators can manually activate outputs using the P2000 Output Control application.

Events

Events are sequences of system commands or actions that may be activated at a pre-defined time or on an as-needed basis. You can use the P2000 system to activate and deactivate events either manually or automatically. Examples of events include the following:

Card Events – A badge is assigned event privileges and may execute an event from a reader equipped with a keypad.

Timed Events – Events are assigned specific activation dates and times, and are activated or deactivated automatically by the P2000 system.

System Events – Event triggers can be based on a variety of system activities, such as when an operator attempts to log on with an invalid user name or password.

Database Partitioning

You can divide the P2000 database into smaller sections that can be individually managed. Database partitioning structures define what data is accessible by an individual operator, or by a group of operators. You can create as many partitions as you need, depending on your system requirements. After partitions are created, they can be assigned to all major system components. See *Chapter 4: System Options* for more information.

There are two types of partitions:

Super User – This partition is automatically created by the system and is the main partition in the database. Only one Super User partition can be defined. This partition can be assigned to multiple operators and has access to all partitions of the system.

Regular – Regular partitions are assigned to operators. These partitions allow the operator to add, modify, delete, or view records within their assigned partition.

If you are new to the P2000 system or new to security management in general, it is important you have at least a basic understanding of these principles before configuring the system. What is important to keep in mind is the relationship between the various system features.

As you work through Chapters 2 and 3, these principles will be reinforced as you learn which options relate to which specific system features.

Logging On to the P2000 System Software

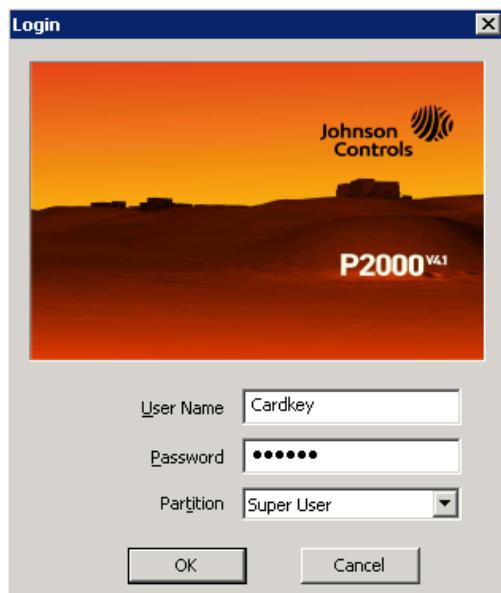
The P2000 system uses a User Name and unique password to establish each authorized user. Passwords are used to protect access within a database or system. A password is a unique combination of alphanumeric characters, such as in a string of letters and/or numbers.

Logging on to the P2000 system is similar for the Server and for a workstation.

1. Double-click the P2000 icon on your Windows desktop,



or, from your Windows desktop, select **Start>Programs>Johnson Controls>P2000 Workstation>Launch P2000**. The P2000 Login window appears.



2. Place the cursor in the User Name field and enter **Cardkey**.
3. Press <Tab> to move to the Password field, or place the cursor in the field. Enter **master** in the Password field.
4. If this is a partitioned system, use the **Super User** default option in the Partition field. Operators that belong to the Super User partition have access to all areas of the P2000 program.
5. Click **OK** or press <Enter> to continue. The P2000 Main menu bar displays. To cancel the login procedure, click **Cancel**.

Note: By default, the Alarm Monitor window is automatically opened when logging on to the Server. For detailed information, see "Monitoring Alarms" on page 160.

Changing the Default Login Values

By using the default User Name and Password, whether at the Server or at a workstation, you are logging on to the system with Super User privileges. This account has, by default, full privileges for viewing and changing system parameters. After initially logging on to the system, you have the option to change the default login User Name and Password to prevent unauthorized users full access to the system.

The default account cannot be removed from the system. Instead, use the following steps to change the default login name and password, thereby restricting access to the Super User account.

To Change the Default User Name and Password:

- From the P2000 Main menu, select **Access>Entity Management**.



- The Entity Management window opens. Select **System Admin** from the list of entities. Click the **User** tab.
- For new systems, the only User Name will be the default, Cardkey. With Cardkey selected, click the **Edit** icon on the menu bar.

The screenshot shows the 'User' edit dialog box with the 'General' tab selected. The 'User Name' field contains 'Cardkey'. The 'User Account Type' dropdown is set to 'P2000'. The 'Password' and 'Confirmed Password' fields both contain masked text. Under 'Account Policy', there are three unchecked checkboxes: 'Account Disabled', 'User must change password at next logon', and 'Always Verify Password'. A checked checkbox for 'Multi-Alarm Handling' is present. On the right, under 'Password Expiration', there are two radio buttons: 'Never' (selected) and 'Based on Password Policy'. At the bottom, 'Message Filter Group' and 'Alarm Processing Group' both show '<none>'.

- Information for the Cardkey User name is displayed. To change the **User Name** and **Password**, place the pointer in each field, and use the <Backspace> or <Delete> keys to erase the default user name and password. Then enter the new User Name and Password.
- Re-enter your password in the **Confirmed Password** field.



Once you have changed the default Login password, you can only use the new User Name and Password to access the Super User account.

For more detailed information on adding a user name and password into the P2000 system, refer to “Adding Users to the System” on page 21.

- Click the **Save** icon to save your settings.

Note: You must log out of the P2000 system for the changes to take effect (see the following section for details).

Logging Out of the P2000 System Software

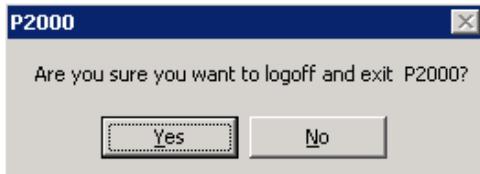
After changing the default User Name and Password, you must log out of the P2000 system; however, this does not require the Server or workstations to be shut down.

To Log Out of the P2000 System:

- From the P2000 Main menu, select **Exit>Exit**.



- The system prompts for logout verification, as shown below.



- Click **Yes** or press <Enter>. The system returns to the Windows desktop.

Navigating through the P2000 System

The P2000 system provides an easy-to-use graphical user interface (GUI) for making selections and entering data.

Mouse Conventions

The standard pointing device for the P2000 Server and workstations is a two-button

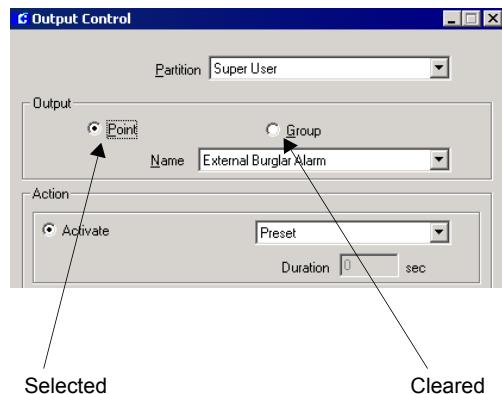
mouse. The left mouse button is the primary mouse button. The following terms are used throughout this manual to describe how you navigate through the P2000 system.

Pointer – The pointer may display differently depending on the action that you are performing. For example, the pointer is normally an arrow, but will change to an hourglass to denote the system is saving, retrieving, or compiling information. When in a text field, the pointer changes to a cursor.

Select – This term directs you to select a menu, submenu, or button option. For example, “select **Control>Output Control**” means to click on the Control option from the Main menu bar, then click on the Output Control submenu. The phrase, “select the Point option” means to click the button next to the option.

Clear – Click again on a selected button to clear the option.

Click – Press and release the left mouse button once. Note that “click” always refers to the left mouse button, unless the right mouse button is specifically called out in the text.



Double-click – Quickly press twice and release the left mouse button.

Click and Drag – Press and hold down the left mouse button to select an item, drag and point

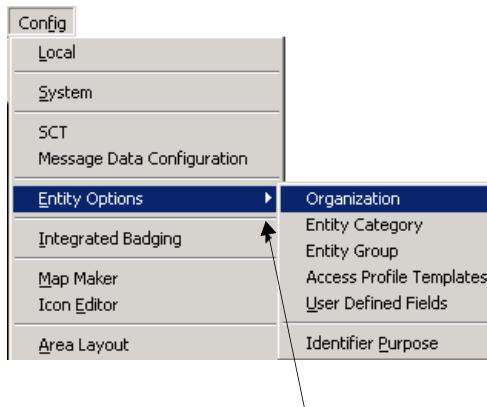
to where you want to place the object; then release the mouse button.

Instruction Conventions

For clarity, the following convention is used throughout the manual for selecting P2000 menus, submenus, and options:

From the P2000 Main menu, select **Config>Entity Options>Organization**.

In this example, you would click the Configuration option from the P2000 Main menu bar, then click the Entity Options menu, and then click the Organization submenu item to display the *Organization* window:



An arrow indicates there are submenus for this menu item.

Menu Shortcuts

In the P2000 system the mouse is normally used, but you may also use key combinations to select the menus on the Main menu bar and submenus, and to open windows.

To Select an Option on the Main Menu and Submenus Using a Menu Shortcut:

1. Select the P2000 Main menu bar as the active window.
2. Press <Alt> + <the underlined letter shown on the Main menu bar>.
3. Once a Main menu is open, simply press the underlined letter of the submenu item you wish to select.

To Tab through Open Windows on the Screen:

1. When you have several windows open on the system, you can press <Alt> + the **Tab** key to bring open windows forward and make them active, including the P2000 window.

To Tab through Fields on a Window:

1. Once an active window is selected, you can use the **Tab** key to tab through fields on the window.

Verification Passwords

The P2000 software offers added security by requiring operators to verify their login password when performing certain system-critical functions. If this option is selected in the User tab (see page 147), when operators access some functions, a password verification dialog box displays for the operators to enter their login password.

The purpose of a verification password is to prevent unauthorized users from performing system-critical functions at unattended PCs.

Context Sensitive Help

Help is available from most P2000 windows or dialog boxes, by pressing <F1>. Once you press <F1>, help text for the selected item displays in a separate window.

Online Help

The P2000 software contains virtually the entire User's Guide in online documentation accessed via the Help option on the Main menu. You can also press F1 for context-sensitive help from most windows in the program and most individual fields.

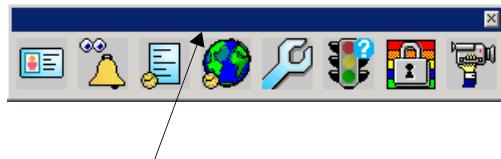
Access information under Introduction, System Configuration, System Operation, System Options, System Maintenance, or System Reports; or use the Index to search for specific topics.

Viewing the Toolbar

The Toolbar gives you easy access to the more commonly used windows in the P2000 system.

To Use the Toolbar:

1. If the toolbar is not visible, from the P2000 Main menu select **View>Toolbar**. The Toolbar displays.



Click and drag to another position

2. Place the mouse over an icon to display the name of the icon.
3. To open a dialog box from the Toolbar, click the desired icon. Choices are: Access Entity, Alarm Monitor, Real Time List,

Real Time Map, System Configuration, System Status, Security Level Control, and Launch AV Player (if the DVR option is available in your facility).

4. To position the toolbar anywhere on the screen, click the title bar and drag it to the desired position.
5. To close the toolbar, click the Close button, or select **View>Toolbar** from the P2000 Main menu.

Using P2000 SCT

The P2000 System Configuration Tool (SCT) is a browser-based application provided as part of the P2000 software package. The P2000 SCT is installed on the P2000 Server and allows you to configure CK722 controllers for use with the P2000 system.

The SCT enables you to create and modify BACnet objects that will be downloaded to one or more CK722 controllers. These objects determine how the CK722 functions. Objects can be created and then assigned directly to a CK722 Device object, or you may use factory supplied templates (or create your own templates) to design common access control or intrusion detection applications.

You can access the P2000 SCT directly from the P2000 software or via a browser on any computer with a LAN/WAN connection to the P2000 Server (if permitted by the Security or IT Administrator). When the P2000 SCT's configuration settings are modified, these changes can be downloaded to the CK722 controller, and the P2000 Server software will automatically be updated to reflect the changes.

For detailed instructions on how to use the P2000 SCT, refer to the *P2000AE System Configuration Tool (SCT) Manual*.

Starting the P2000 SCT

The P2000 SCT is installed on the server as part of the P2000 software installation. For instructions, refer to the *P2000AE Server/Workstation Software Installation Manual*.

The P2000 SCT can be accessed in one of two ways:

- Directly from the P2000 Server or workstation.
- Using any web browser from a computer with a LAN/WAN connection to the P2000 Server (if configured for remote access).

To Launch P2000 SCT Directly from the P2000 Server or Workstation:

1. From the P2000 Main menu, select **Config>SCT**.

If the archive already exists (created upon initial start-up of the P2000 SCT application), the P2000 SCT user interface appears, displaying the archive and its contents. If launching the P2000 SCT for the first time, the Create Site dialog appears. Refer to the *P2000AE System Configuration Tool (SCT) Manual* for details.

To Launch P2000 SCT from a Computer with a LAN/WAN Connection to the P2000 Server:

1. Launch your Web browser.
2. Enter one of the following URLs in your browser and press <Enter>. In Microsoft Internet Explorer, the URL field is called Address.

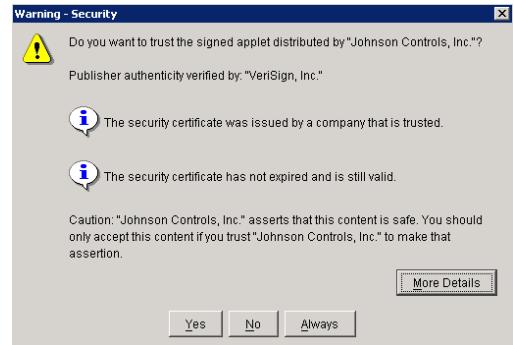
http://IP Address of P2000 Server/sct
Example: *http://122.655.234.411/sct*

OR

http://P2000 Server Name/sct
Example: *http://jsmithpc1.xyz.com/sct*

Note: You may be required to install the Java Runtime Environment to access the P2000 SCT via your browser.

The Security Warning screen appears.



3. Click Always. The P2000 SCT Login screen appears.



Note: To quickly access the P2000 SCT in the future, you can add the URL to your browser Favorites list. Refer to your browser's online help for assistance.

4. Enter your **Username** and **Password**. The Username and Password are the same as those used to access the P2000 software. For information on adding users refer to "Adding Users to the System" on page 21.
5. Click the **Login** button.

If the archive already exists (created upon initial start-up of the P2000 SCT application), the P2000 SCT user interface appears, displaying the archive and its contents. If launching the P2000 SCT for the first time, the Create Site dialog appears. Refer to the *P2000AE System Configuration Tool (SCT) Manual* for details.

Chapter 2: Configuring the System

To operate your *P2000 Security Management System*, the software must be set up and configured to communicate with the system hardware. After all hardware installations are complete, you are ready to configure the P2000 software. Configuration is typically performed by a System Engineer or System Administrator.

System Configuration Overview

Configuration should progress in a logical sequence. For example, you must configure the System parameters before you can assign them to Panels; you must configure Panels before you can assign Terminals to them; and you must configure Terminals before you can create Terminal Groups, Inputs, and Outputs. This chapter will guide you through a logical progression. After the system is configured, you always have the option to return to a component and make changes if necessary.

Note: To configure CK722 panels and associated devices, refer to the *System Configuration Tool (SCT) Manual* and to the *CK722 Commissioning Guide*.

The following elements must be set up to complete system configuration:

- Set up Workstations and System Users
- Configure System Components
- Configure Hardware Components
- Configure Elevators and Cabinets

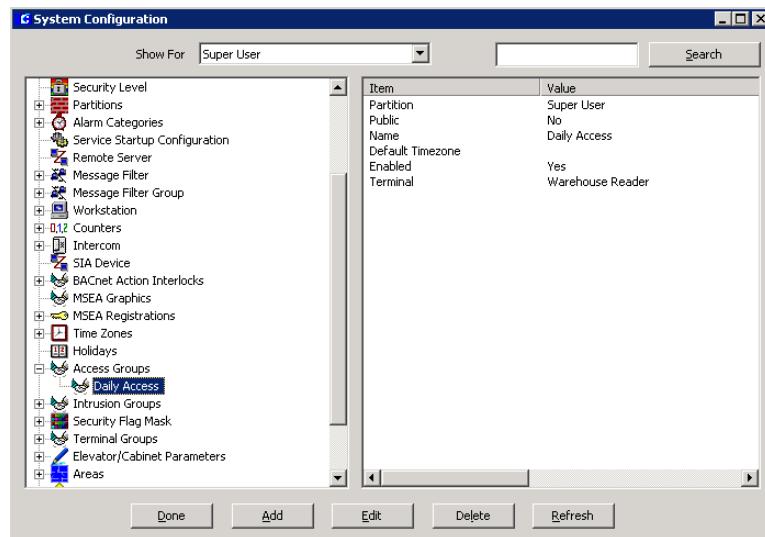
- Configure Message Filtering and Message Routing
- Set up Message Data Configuration
- Set up Security Flags, Access Groups, and Entity Options

After you have configured your system components, these items will be available to you as you work your way through hardware configuration. The parameters set up during hardware configuration will be accessible when you begin creating your database. As soon as the system is completely configured, you are ready to begin system operation.

TIP: It will be helpful to develop a Naming Convention Plan to apply to panels and terminals, inputs and outputs, and various access and terminal groups you will configure in the P2000 software. A fully developed plan can speed the configuration process by creating a quick reference to system component names and get your system running as quickly as possible. (See “Panel Naming Conventions” on page 48 for more information.)

Using the System Configuration Window

The System Configuration window provides quick access to all hardware component configurations. Select **Config>System** from the P2000 Main menu bar and enter your password if prompted. The System Configuration window opens, as shown in the following page. All “root” items in the system configuration “tree” display on the left side of the window



(windowpane). A plus (+) sign next to an item indicates that “branches” exist beneath them. When you select a branch in the tree, the detailed settings and values relating to that selection are listed on the right windowpane.

You can add as many items to the configuration as you need, depending on your Registration Parameters. After items have been added to the system, you can edit them as desired.

To Add an Item to the System Configuration:

1. From the “configuration tree,” click the “root” icon for the item you wish to add.
2. To access configuration dialog boxes, either click the **Add** button at the bottom of the window, or right-click to access a shortcut menu and select **Add**. The appropriate dialog box opens.



3. After you have added the information according to the field definitions, click **OK**

to return to the System Configuration window. When dialog boxes offer several configuration tabs, such as in the Panel or Terminal Edit dialog boxes, continue to the next tab, as applicable. When all settings have been entered, click **OK** to save the settings and return to the System Configuration window. The settings for the new item will be listed on the right windowpane.

4. Continue to add items in this manner until all hardware items and their related controls have been configured in the P2000 system.

To Edit System Configuration Items:

1. From the configuration tree, click the item you wish to edit and click the **Edit** button at the bottom of the window (or right-click the item and select **Edit** from the shortcut menu). The Edit dialog box opens.
2. After you have completed your changes, click **OK** to save the settings and return to the System Configuration window. The changes will be reflected on the right windowpane.

To Search for System Configuration Items:

1. To search for a specific item, enter the name of the item in the search field at the top right corner of the System Configuration window.
- You can enter complete or partial words; no wildcards are needed, and this field is not case sensitive.
2. Click the **Search** button. The System Configuration window will display the match entered in the search field.
3. Continue clicking **Search** until you find the item you are looking for.



APPLICATION NOTE

Refreshing the System Configuration Window: The refresh button is used to update changes made at the Server or other workstations.

Set Up Workstations and System Users

Before configuring system and hardware components, Workstations and Users should be properly set up to communicate with the Server. While Workstations are assigned from the System Configuration window, Users are defined in the Entity Management window. The following sections describe how to:

- Set up Workstations
- Add Users to the System
- Set up User Accounts

Workstations

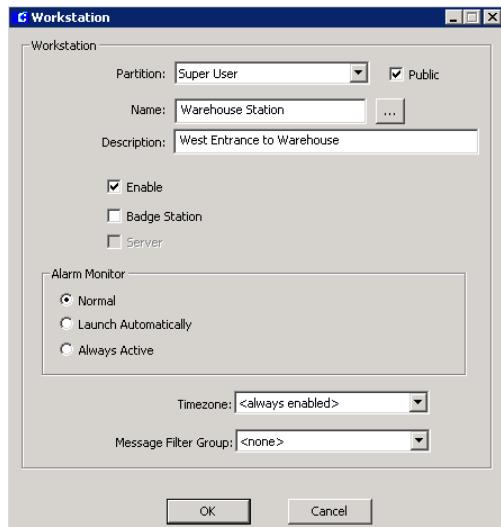
Workstations communicate with the Server via the network. The Server can communicate with a maximum number of Workstations concurrently, based on your registration options.

Workstations are assigned a Partition, a name, a Timezone, and designated as Public to make the workstation visible to all partitions. A workstation must be configured as a Badge Station if it will operate Video Imaging. When you click a Workstation on the System Configuration window, the current settings display on the right windowpane.

Note: To log on from a workstation to the P2000 system, user accounts must be set up in the Windows operating system. Refer to "Setting Up User Accounts" on page 23.

To Add a Workstation:

1. In the System Configuration window, click the **Workstation** root icon.
2. Click the **Add** button to access the Workstation dialog box.



3. Enter the information required. (Refer to "Workstation Field Definitions" for detailed information.)
4. Click **OK** to save your entries and return to the System Configuration window. The new Workstation displays beneath the main Workstation icon.

5. Click the new Workstation icon to display the current settings on the right window-pane. It may be necessary to click the plus (+) sign to display all configured Workstations on the system.

Workstation Field Definitions

Partition – If your system has the Partition option, select the Partition to which the Workstation will have access. Partitions are described in detail on page 225.

Public – (Displays on partitioned systems only.) Select the Public check box to make this Workstation visible to all partitions.

Note: *A workstation must be made **Public** to allow users from different partitions to log on at that workstation.*

Name – Enter the name of the Workstation. This name must be the name of this workstation, as configured in the Windows operating system. You can also click the [...] button to find a workstation on your network (see your system administrator).

Description – Enter a meaningful description or location of the workstation. This field is used by the Web Access option to select the location where a badge will be issued.

Enable – The system will not recognize the Workstation unless the **Enable** check box is selected.

Badge Station – Select this box to define this workstation as a Video Imaging station.

Server – This box is used only to identify the workstations that operate as the system Server.

Alarm Monitor – Defines whether or not the Alarm Monitor window displays at the workstation after logging on. Select one of the following options:

- **Normal** – This is the default option for workstations. Enables an authorized user to open and close the Alarm Monitor window on this workstation.
- **Launch Automatically** – If selected, the Alarm Monitor window is automatically launched after logging on. Users with the appropriate roles can open and close the Alarm Monitor window, if required.
- **Always Active** – This is the default option for Server stations. The Alarm Monitor is automatically launched after logging on and cannot be closed by the user. This is the required option for UL listed sites, where all alarms must always be visible at the Server to meet UL requirements.

Timezone – Assign a Time Zone to the workstation to define the days and hours it will be in use. See “Time Zones” on page 44 for detailed information.

Message Filter Group – Assign a Message Filter Group to define which messages will be transmitted to this workstation. Select <none> if you wish to transmit all messages to this workstation. See “Configure Message Filtering and Message Routing” on page 99 for detailed information.

To Edit a Workstation:

1. Click the plus (+) sign next to the root Workstation icon to display all configured Workstations.
2. Select the Workstation you wish to edit and click **Edit**. The Workstation dialog box opens.
3. Enter the new information.
4. Click **OK** to save your settings and return to the System Configuration window. The new settings display on the right window-pane.

Adding Users to the System

Access to the system is controlled by users that have been assigned system privileges and characteristics that allow them to perform various system functions. Therefore, user records must be created for each person who will operate the Server or a workstation in the P2000 system. The user record consists of the person's login ID, password, user roles, and other features that determine how the user will operate. User roles are assigned by group and must be created before they will be available to assign to users.

User Role Management

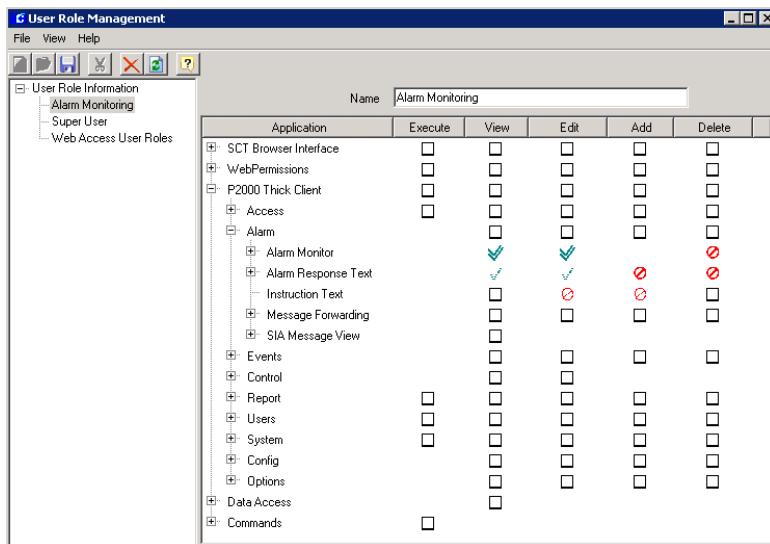
User roles define the system elements to which a user has access. For example, a guard operating a P2000 workstation at the warehouse gate will need to have access to alarm monitoring, but will not need access to Entity Management functions. Some users may need to view system functions, but will not be allowed to edit features, and some users will need full rights and privileges such as a system administrator or designee.

The P2000 software is delivered with a default user that can be used to configure the system, and therefore has all user privileges. You can completely configure the system using only the default user or you can create additional user roles that include various combinations of rights to applications, dialogs, functions, and fields, depending on the responsibilities and access needs of the individual users. Once user roles have been created, they will be accessible from the User tab in the Entity Management window.

Note: In addition to assigning rights to P2000 applications, you can also define dialog components and individual data fields associated with the Entity Management application.

To Create User Roles:

1. From the P2000 Main menu, select **Users>User Roles**. The User Role Management window opens.
2. From the User Role Management window menu bar, select **File>New** or click the **New** icon. The left pane will display



<new> and will show the name of the User Role once the record is saved.

3. Enter the **Name** of the User Role.
4. The User Role Management window opens as a two-pane window. On the left is a list of all currently defined user roles, on the right are the “application resources” which are the applications, dialog components, data fields, and commands. Application resources are organized into the following basic tree structures and allow granting/denying access to entire sub-trees:

SCT Browser Interface – Use to define roles associated with the SCT Browser Interface.

WebPermissions – Use to define roles associated with the Web Access option.

P2000 Thick Client – Use to define roles associated with P2000 applications.

Data Access – Use to define roles associated with certain fields within a record.

Commands – Use to define roles associated with any of the commands that can be performed from the Control Center application, see page 177.

5. In addition, the right pane is divided into the following five columns and indicate the permission levels for the different application resources:

Execute – The user can execute applications.

View – The user can see application resources, but cannot edit, add or delete.

Edit – The user can view and make changes to entries in the application resources, but cannot add or delete.

Add – The user can view, edit, and add records, but cannot delete.

Delete – The user can view, edit, add new, and delete existing application resources.

6. To grant or restrict access to a function, select the application resource line or click

the (+) plus sign to display items under the same tree, then select the desired function.

7. Right-click the check box under the desired permission level and select one of the following options:

Unknown – The application resource will not be included in the User Role.

Grant – Grants access to the application resource.

Grant All – Grants access to the application resource and to all items under the same tree.

Deny – Denies access to the application resource.

Deny All – Denies access to the application resource and to all items under the same tree.

To resolve potential configuration conflicts between multiple user roles, rights are evaluated based on the following order:

Order	If you select...	access is...
1	Deny All/Deny	denied
2	Grant All/Grant	granted
3	Implied Deny	denied
4	Implied Grant	granted
5	Unknown	denied

This order ensures that a configuration conflict will be resolved in favor of NOT granting access to the application resource.

Points to Note:

- Implied Deny/Grant means that the last explicitly set right in the hierarchy order to the root item is to grant/deny all access.
- Explicitly set rights (green) are not modified if a parent privilege is modified to a right that does not explicitly impact the children item.
- If you select Deny All instead of Deny, then explicitly granted items under the parent privilege are modified from Granted (green) to implied deny.

- The implied grants (blue) are modified, as they are only granted because the parent has a “Grant All” privilege.
8. Click the **Save** icon. The User Role will now be accessible from the User tab of the Entity Management window. Refer to the “User Tab” on page 147 for details.
 9. To edit an existing user role, select the user role name on the left pane and click the **Edit** icon. Make the appropriate changes on the right pane then click the **Save** icon.

Note: If you delete or make changes to a User Role, currently logged on users who have been assigned with the deleted/modified User Role, will maintain the same rights/restrictions defined in the User Role until they log out of the system. This does not apply to deletions/changes made to all newly started applications, where users can maintain the same rights/restrictions as long as the application remains opened; new rights will apply when the application is restarted.

Assigning System Users

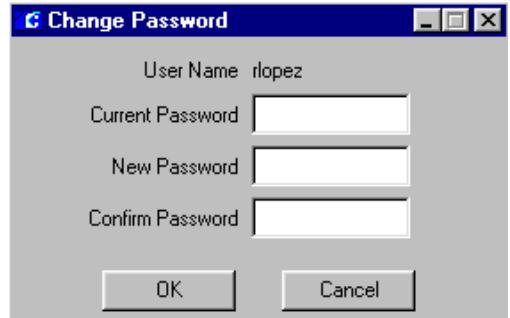
After initial login, the system is ready for user configuration. Every user is assigned a name, which uniquely identifies the user, and is usually the person’s first and last name. The user password and name are used to verify access to the system. User configuration is part of the Entity Management application and is described in detail on page 147.

Changing the User Password

Use the Change Password option to change a user’s password. Depending on the rights assigned using User Role Management, some or all users may be able to change their own password at any time.

To Change a Password:

1. From the P2000 Main menu, select **Users>Change Password**. The Change Password window opens.



2. Enter your current password in the **Current Password** field.
3. Enter your new password in the **New Password** field.
4. Re-enter your new password in the **Confirm Password** field.
5. Click **OK** to save your new password. There is no need to log out of the system. The new password is now valid within the P2000 system.

Setting Up User Accounts

To add users to the P2000 system, accounts must be set up in the operating system. Without proper authorizations, the system will not allow connections to the Server.

Adding a Login Name and Password for the P2000 System into the Operating System

When you add users into the Windows list of valid users on the server, you must assign this user account as a member of the “PEGASYS Users” group to give them rights to connect to the P2000 database. Use the same user name

and password that the user uses to log on to Windows at the workstation.

The user account may be assigned membership of other groups as desired. The commonly used groups are explained below:

PEGASYS Users – Gives rights to log on to the P2000 database.

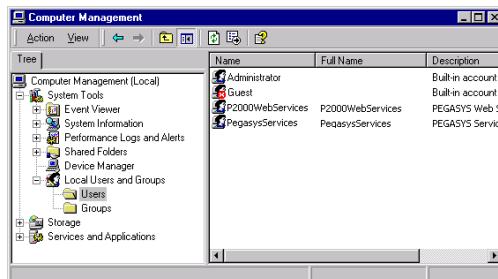
PEGASYS Administrators – Gives rights to administrate the P2000 database (create and drop tables, restore the database, etc.).

Users – Gives rights to log on to the server computer locally.

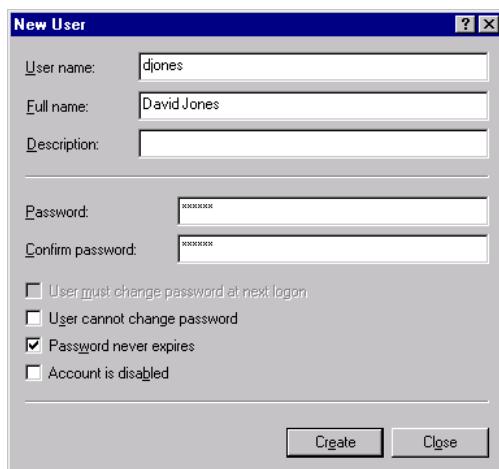
Administrators – Gives rights to administrate the server computer (add users, change hardware configuration, etc.).

Windows 2003 Server Details

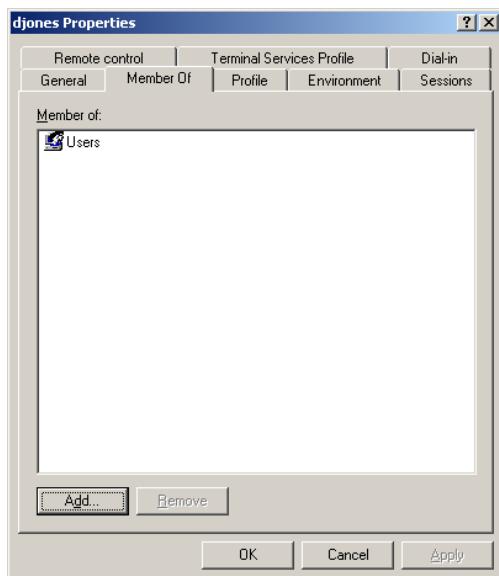
- Run the Computer Management program; select Start>Settings>Control Panel>Administrative Tools. Double-click the Computer Management icon.



- Click on System Tools>Local Users and Groups>Users.
- From the Computer Management menu, select Action>New User. The New User dialog box opens.

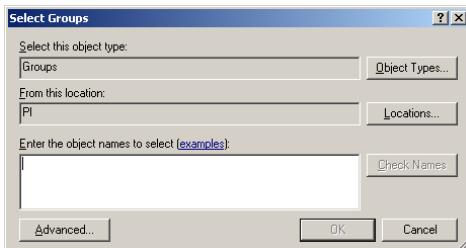


- Enter the data for the new user, then click the Create button. Click Close to return to the Computer Management window.
- Right-click the newly added user on the right pane and select Properties.
- In the user Properties window, click the Member Of tab.

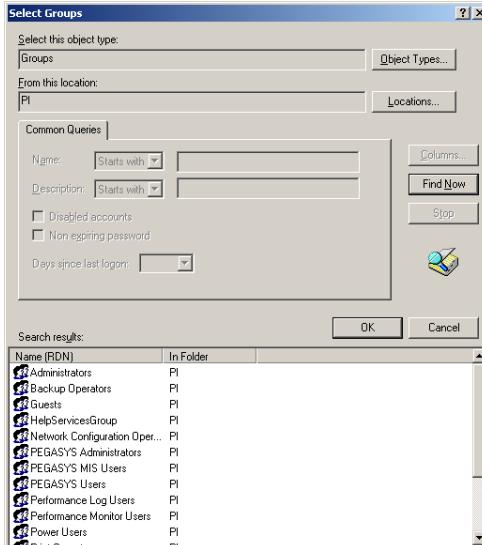


- Click the Add button.

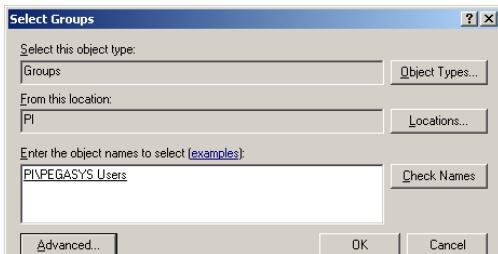
8. In the Select Groups window, click the **Advanced** button.



9. In the expanded Select Groups window, click the **Find Now** button.
10. From the list of groups select the PEGASYS Users group and click **OK**.



11. In the Select Groups window, verify that the correct group is listed and click **OK**.



12. Click **OK** at the confirmation message.



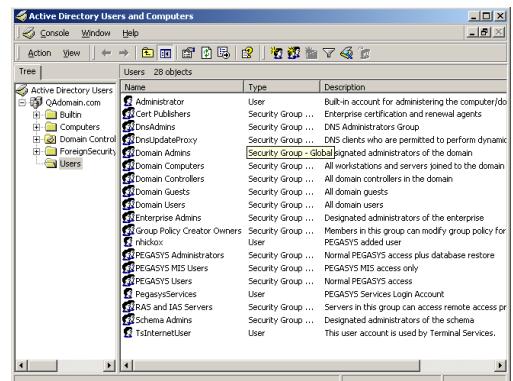
13. Repeat steps 7 - 12 for other groups you want to add, (see page 24 for reference), this time selecting that particular group from the list.

14. Click **OK** to close the user Properties window.

Windows 2003 Server with Active Directory Details

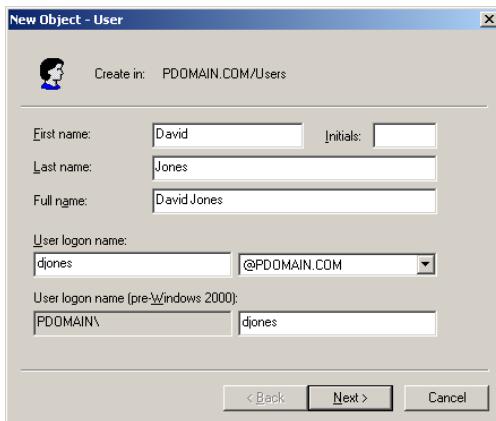
Follow this procedure if you are using Windows 2003 Server or Windows 2003 Server Enterprise Edition and the server is a member of a domain.

1. Run the Computer Management program (select **Start>Programs>Administrative Tools>Active Directory Users and Computers**).



2. Expand the **Active Directory Users** and **Domain Name** entries. Right-click **Users** and select **New>User**.

3. The New User dialog box opens. Enter the data for the new user, then click the **Next** button.



4. Enter the password for the new user, check the password type (if you select the **Password never expires** feature, you will be prompted to click **OK** to confirm it). Click **Next**.



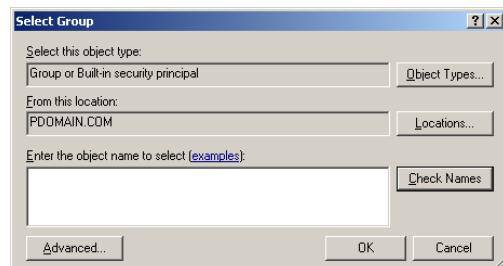
5. Verify the parameters, then click **Finish**.



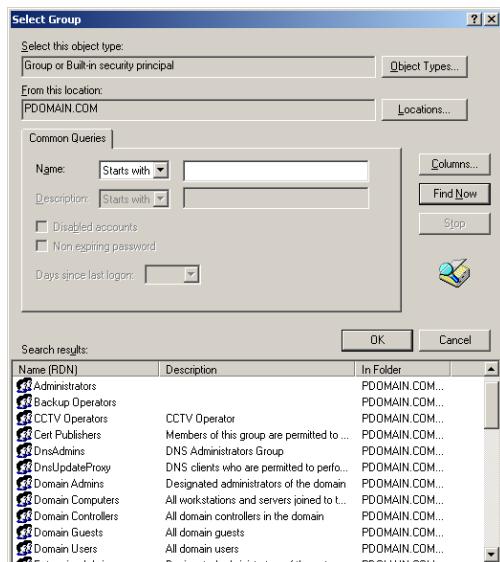
6. To add a member to a user group, from the Active Directory Users and Computers window, select the newly added user on the right pane, right-click and select **Add to a group**.

Note: *The user is already a member of Domain Users.*

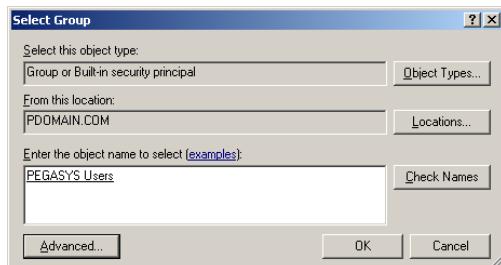
7. In the Select Group window, click the **Advanced** button.



8. In the expanded Select Group window, click the **Find Now** button.
9. From the list of groups select the PEGASYS Users group and click **OK**.



10. In the Select Group window, verify that the correct group is listed and click **OK**.

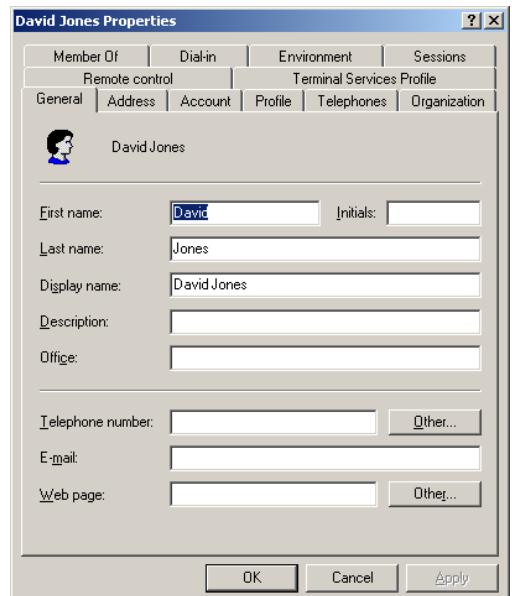


11. Click **OK** at the confirmation message.



12. Repeat steps 6 - 11 for other groups you want to add, (see page 24 for reference), this time selecting that particular group from the list.

13. To manage the existing domain user, from the Active Directory Users and Computers window, select the newly added user on the right pane, right-click and select **Properties**. The Properties screen opens.

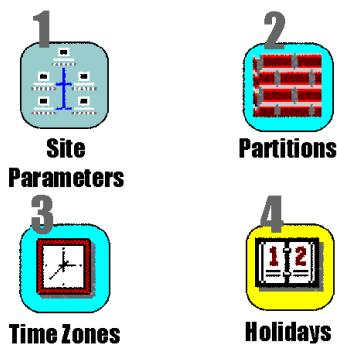


14. Complete each tab according to your needs, then click **OK**.

15. Close all windows.

Configure System Components

System components that operate globally throughout the P2000 system include Site Parameters, Partitions, Time Zones, and Holidays. To speed the configuration process, we recommend that you set up system components in the following order:



Site Parameters – Site Parameters define general system information, real time printing, panel types, facility codes, record retention times, and other parameters that are specific for the entire facility.

Partitions – You can divide the P2000 database into smaller sections that can be individually managed. (This feature is optional.) Partitions allow a system to function as multiple, separate systems. For more information on Partitions, see page 225.

Time Zones – Times Zones are used throughout the system to define Active and Inactive time periods for various system components.

Holidays – Holidays are defined for the entire facility. Holiday start and stop times may be different for different access rights.

Registration Parameters

You can review the maximum number of terminals and workstations, the maximum badges allowed, and other parameters specified for your system. Select **Config>System** from the P2000 Main menu bar, enter your password if prompted, and click the **Registration Parameters** icon at the top of the configuration tree in the System Configuration window. The parameters will display on the right windowpane. These parameters are determined by contract and cannot be edited within the program. For more information see “Registration Parameters” on page 4.

Item	Value
Installation Key	IK25OWEBE8YT
Registration Key	FU55T8PYEOWD
Valid Registration	Yes
System Type	P2000
Serial Number	1
Version	4.1
Partitioning	Yes
MIS Interface	Yes
BACnet Interface	Yes
MSEA Interface	Yes
Guard Tour Interface	Yes
CCTV Interface	Yes
Audio-Visual Interface	Yes
Intercom Interface	Yes
Web Access	Yes
Large Web Access	Yes
Intrusion	Yes
FDA Title 21 CFR Part 11	Yes
Enterprise System	Yes
Redundancy	Double Take
Integrated Badging	Yes
Max Terminals	128
Max Workstations	7
Max Badging Workstations	2

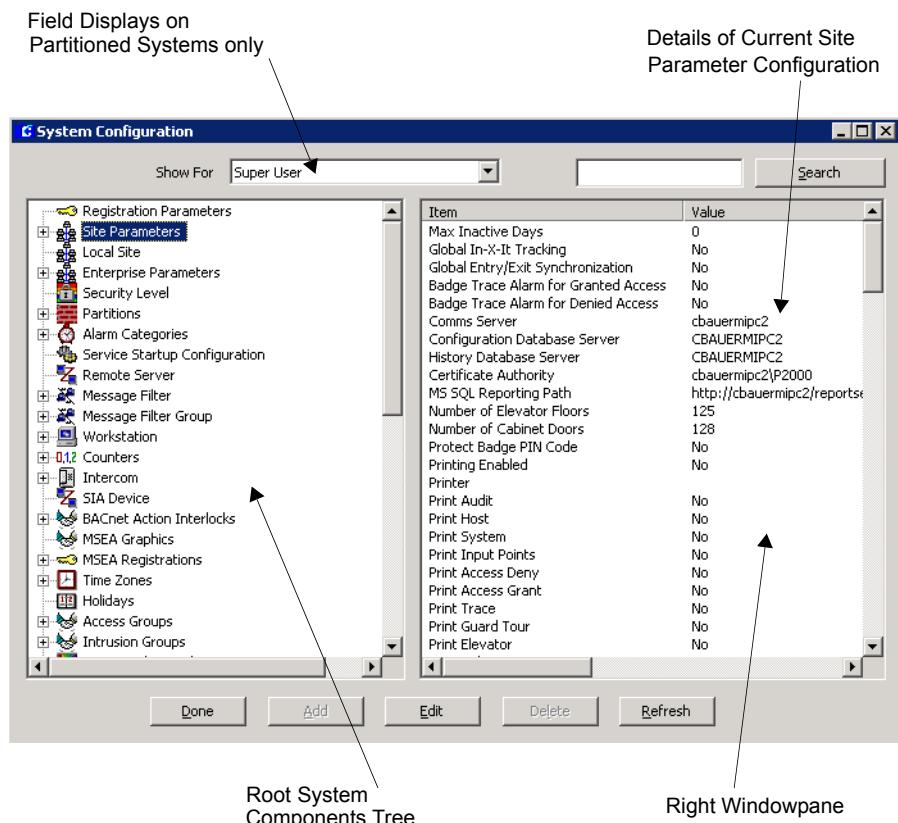
Site Parameters

The elements that define how your access control system will operate are entered in Site Parameters. The P2000 system uses the information in Site Parameters to determine how system and hardware components will be configured. It is important to plan your access requirements by establishing elements such as the server that will handle system communications, real time printing, panel types, facility codes, record retention times, and other parameters that are specific for the entire facility. Additional elements such as BACNet, MIS and Web Access setup information will be available if your facility has purchased these options, and are described in *Chapter 4: System Options*.

When you click Site Parameters in the System Configuration window, the current settings display on the right windowpane. You may edit these settings as desired. The Backup Device, DB Server, and Real Time Printer in Site Parameters can only be set at the Server. On a partitioned system, only users that belong to the Super User partition can edit Site Parameters.

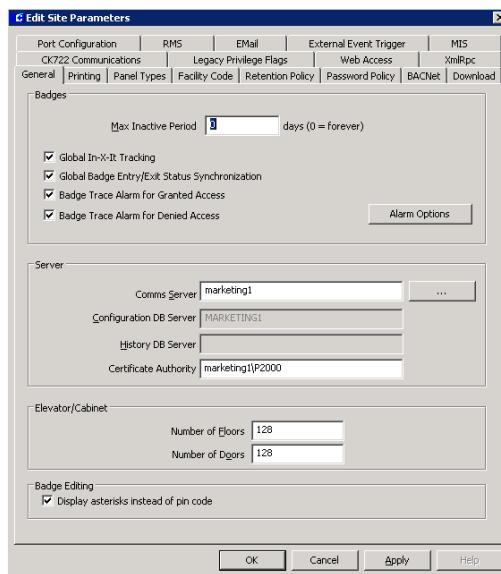


CAUTION
The Server settings in the General tab, are advanced settings that should be changed only at the direction of our Technical Support team. If these settings are changed, the system may not work properly!



To Edit Site Parameters:

- With Site Parameters selected, click **Edit**. The Edit Site Parameters dialog box opens at the General tab.



- Enter the information in each tab according to your system requirements. (See “Site Parameters Field Definitions” for detailed information.)
- As you work through the tabs, you may click **Apply** to save your entries.
- After you have entered all the information, click **OK** to save the settings and return to the System Configuration window. The new values will display on the right windowpane.

Site Parameters Field Definitions

General Tab

Max Inactive Period – Enter the number of days after which a badge will be disabled due to inactivity. The operator will have to manually reactivate the badge when needed.

Global In-X-It Tracking – If selected, messages are sent to the real time list to report global entry/exit violations. A global entry/exit violation occurs when access is granted after presenting a valid badge at, for example an entry reader and then that badge is presented again at another entry reader, despite the requirement to badge at entry and exit readers alternately.

Global Badge Entry/Exit Status Synchronization

– Select this check box to allow synchronization of badge status across multiple panels. This feature is not recommended for medium and large systems, unless using panels CK720/CK705 of version 2.5 or higher.

Badge Trace Alarm for Granted Access – Select this check box to generate an alarm when a badge with the Trace flag set is granted access at any reader in the system.

Badge Trace Alarm for Denied Access – Select this check box to generate an alarm when a badge with the Trace flag set is denied access at any reader in the system.

Alarm Options – Click this button to open the Alarm Categories window and assign alarm options associated with the Badge Trace Alarms. For detailed instructions, see page 160.

Comms Server – Defaults to the server that handles communications.

Configuration DB Server – Displays the name of the server that handles the configuration databases.

History DB Server – Displays the name of the server that handles the history databases.

Certificate Authority – Displays the server name where the Certificate Authority is installed, as well as the name of the Certificate Authority used to enable encryption for communicating with CK722 controllers.

Number of Floors – Enter the maximum number of floors at your facility (up to 128) for ele-

vator access. This is the number of floors that will display in the Floor Name Configuration list.

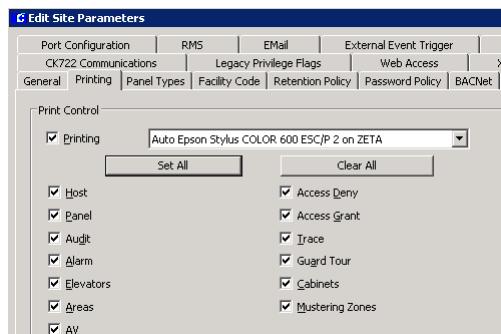
Number of Doors – Enter the maximum number of doors at your facility (up to 128) for cabinet access. This is the number of doors that will display in the Door Name Configuration list.

Display asterisks instead of pin code – If selected, the PIN code entered in the Identifier tab of Entity Management displays as asterisks.

Printing Tab

Real Time printers can be set up only from the system Server, even if the operators have permissions to edit Site Parameters at their workstations. Printers to be used by the P2000 system must first be set up using the Windows printer set up function. If you need assistance adding printers to the system, see your system administrator or refer to your Windows documentation.

Note: While the same options are offered from Real Time Printing, this function operates independently from the Real Time List viewed on screen. It is not connected in any way to a history file. It simply prints the transaction types selected as they occur.



Printing – Select this check box to print any transaction, then choose a printer from the drop-down list. We recommend a dot matrix

printer be used exclusively for printing the following transaction types as they occur.

Set All – Select this box to print all transactions.

Clear All – Select this box to clear the selections. To limit the type of transactions printed, select any of the following options:

Host – Prints triggered and system events.

Panel – Prints reader strikes and status, terminal and panel status changes, and so on.

Audit – Prints operator actions such as add an alarm instruction, edit an event, run a report, and so on.

Alarm – Prints all alarm messages.

Elevators – Prints all elevator messages.

Areas – Prints all area messages.

AV – If your facility has the DVR option, select this box to print all audio-visual messages. DVR is described on page 282.

Access Deny – Prints all Access Deny messages.

Access Grant – Prints all Access Grant messages.

Trace – Prints all transactions associated with a badge identifier. The Trace option must also be enabled on Access Profiles, see page 138.

Guard Tour – If your facility has the Guard Tour option, select this box to print all guard tour messages. Guard Tour is described in detail on page 242.

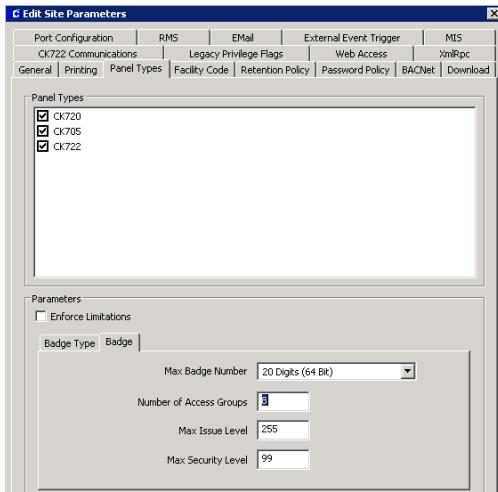
Cabinets – Prints all cabinet messages.

Mustering Zones – Prints all mustering zone messages.

As a reference, see “Using the Real Time List” on page 213.

Panel Types Tab

Use this tab to select the panel types that will be configured for the system. Specific features for the selected panel type will display when configuring the panels and their system and hardware components. Your system can be configured with any combination of panel types. The panel types selected here are the only types that can be selected in the Type field of the Edit Panel dialog box when defining a new panel, with the exception of the CK722 panel, which is configured using the SCT application. Refer to the *System Configuration Tool (SCT) Manual* and the *CK722 Commissioning Guide* for details.



The Parameters box defines various elements for each panel type. Before entering your selections, refer to the following table for the maximum default values for each panel type:

Parameters	Elements	CK720/CK705/ CK721	CK722 (BACNET)	S321
Badge	Max Badge Number	20 Digits	20 Digits	4,294,967,295
	Number of Access Groups	32 (downloads a maximum of 8)	100	2
	Max Issue Level	255	255	7
	Max Security Level	99 (2.2 and higher)	99	99

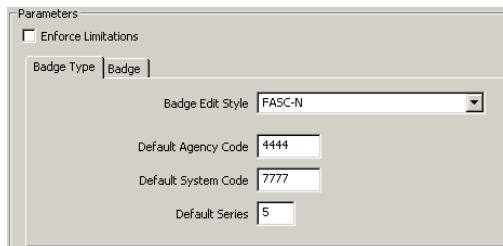
Enforce Limitations – Select this check box to force the system to use the default values listed in the table below. If you select to Enforce Limitations, you will not be required to enter any values in the Parameters box and all tabs will be disabled. There is a combination of options depending on whether or not you select this check box and the type or types of panels selected. Refer to the following rules:

- **If you select one panel type and enable Enforce Limitations**, you will force the system to use the maximum default values for the panel selected.
- **If you select more than one panel type and enable Enforce Limitations**, you will force the system to use the lowest values among the panel types selected.
- **If you select one panel type and do not enable Enforce Limitations**, you will be able to enter any value up to the maximum default values for the panel selected.
- **If you select more than one panel type and do not enable Enforce Limitations**, you will be able to enter any value, but the system will only recognize the maximum values for each panel type selected.

Note: The S321 panel is not available in this release.

Badge Type Tab

Settings in this tab define the badge type to be used at your facility.



Badge Edit Style – Select one of the following options:

- **Normal** – Select Normal if your facility uses any badge type other than FASC-N.
- **FASC-N** – Select FASC-N (Federal Agency Smart Credential Number) if your facility supports the Federal Government smart card encoding protocol. If you select this option, the system will generate a 15-digit badge number using the following default values.

Default Agency Code – Enter the 4-digit default agency code to be used at your facility.

Default System Code – Enter the 4-digit default system code to be used at your facility.

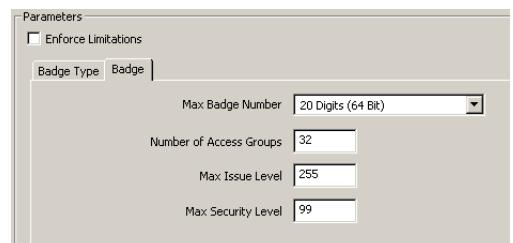
Default Series – Enter a 1-digit default series number to be used at your facility.

For more information, refer to “FASC-N Badges” on page 146.

Badge Tab

Settings entered in this tab govern how badge identifiers will be configured for the entire system. When you create a badge identifier, the system uses this information to determine the maximum allowed values. For more infor-

mation, refer to “Access Profiles Tab” on page 138 and to “Identifier Tab” on page 142.



Max Badge Number – Select from the drop-down list the maximum number of characters allowed to be entered in the Badge Number field. CK705, CK720, and CK722 panels support up to 20 digits, S321 panels support up to badge number 4,294,967,295.

Number of Access Groups – Enter the maximum number of access groups that can be assigned to each badge identifier. This is the number of access groups that will display in the Access/Intrusion Group tab in Access Profiles. You can define up to 100 access groups if using CK722 panels, up to 32 access groups for CK705/CK720 panels (but download only eight); and up to two access groups if using S321 panels.

Max Issue Level – Enter the highest issue level that can be assigned to a badge identifier. The maximum value will display in the badge Issue Level drop-down list. CK705, CK720, and CK722 panels support issue levels 0-255, S321 panels support issue levels 0-7.

Max Security Level – Enter the highest security level that can be assigned to a badge identifier. This is the maximum number that will display in the Security Rights tab in Access Profiles. Refer to “Security Threat Level Control” on page 174.

Facility Code Tab

Some of the codes stored in every badge identifier are known as *facility codes*. These codes are provided by *Johnson Controls* and allow you to identify the badges that belong to your facility. Use this tab to assign facility codes to CK722 panels. This code must match the facility code assigned in SCT when you defined the CK722 panel.

Facility codes for CK720 and CK705 panels are assigned in the Edit Terminal dialog box. To assign facility codes to S321 panels, use the Edit Panel dialog box.

No.	Name	Value
0	Default Facility Code	0
1	Sunny Valley	2648
2		
3		
4		
5		
6		
7		

Add **Delete**

The box displays the *Default Facility Code* with a default value of 0. Double-click these fields to change the default values and enter the name of your site and the code assigned by *Johnson Controls*. If you are using badges with different facility codes, enter the names and corresponding values for each group of badges. You cannot delete facility codes that have been assigned to badges.

Retention Policy Tab

In the Retention Time box, enter the amount of time and select Days, Hours, or Minutes from the drop-down lists. If you enter “1440 Minutes” on any of the fields, the system automatically converts it into “1 Day.” If you enter “1441 Minutes,” the system leaves the value as is. The system converts even values only.

Retention Time	Audit Trail	Days
Transactions	30	Days
Alarms	30	Days
Muster Data	30	Days
Request Queue	30	Days
Tour Note	30	Days

FDA Retention Policy
 Enforce FDA Title 21 CFR Part 11 Record Retention and Validation Policy

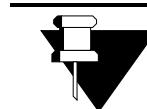
Retention Period (years)
Violation Alert Period (days)
Last FDA Backup

Backup Device Config Device

Audit Trail – Enter the time after which all audit records at the Server, such as logins, logouts, and record changes will be purged.

Transactions – Enter the time after which all system and identifier transactions will be purged.

Alarms – Enter the time after which all alarm records will be purged.



Site Parameters Application:
The number of days history should be stored on the Server hard drive depends on the amount of activity at your site. If you continually fill up the server hard drive, you can reduce the number of days history will be stored.

Muster Data – Enter the time after which all Muster data will be deleted from the system.

Request Queue – Enter the time after which all Request Queue records will be deleted from the system. Refer to “Request Queue View” on page 335.

Tour Note – If your system is registered for the Guard Tour option, enter the time after which all notes will be deleted from the system. Refer to “Guard Tour Notes” on page 255.

FDA Retention Policy

Settings in this box are available if your system is registered for the FDA Part 11 option. Refer to “FDA Part 11” on page 283.

Enforce FDA Title 21 CFR Part 11 Record Retention and Validation Policy – Select this box to enable FDA Part 11 record retention policy, which addresses the protection of records for a specified period.

Retention Period – Enter the number of years to define the amount of time that the system will keep all records in the system.

Violation Alert Period – Enter the number of days to generate a warning message before records are deleted from the system. If the Retention Period is longer than any of the values entered in the Retention Time box above, an alarm message is generated, and repeated on a daily basis, until the operator performs the FDA Backup procedure, see page 332.

Last FDA Backup – This is a displayed field only and shows the date you informed the system that a backup was archived, according to your company policies to comply with FDA Part 11 record retention requirements.



Changes to any of the FDA Record Retention Policy settings will take effect only after all services have stopped and restarted using Service Control. You must also log off and on at the Server computer to see these changes.

Backup Device – Select the name of the device to which database backups will be sent. For detailed information refer to “Configuring a Backup Device” on page 329.

Password Policy Tab

Settings in this tab provide additional security to your system by allowing the system administrator to define a number of parameters to set up strong passwords, passwords that are hard to break.

Password Validation – Enter the number of days during which a changed password remains valid. Users are required to change their password within this period; otherwise, the account will be automatically disabled. The user will be informed of the password expiration at the next login. If you enter “0” in this field, the password remains valid indefinitely, unless you enter a password expiration date on the User tab of Entity Management (see page 147). If complying with FDA Part 11, FDA recommends that the password be changed every 30 days.

Max. consecutive Invalid Logins – If users exceed the maximum number of consecutive invalid login attempts entered in this field, they immediately lose their ability to access P2000 and the account is automatically disabled for one hour. There will be no limitations

if you enter “0.” FDA recommends no more than three invalid attempts.

Minimum Length – Enter the minimum number of characters in a password. FDA recommends the password to be at least 6 characters long.

‘A’ to ‘Z’ or ‘a’ to ‘z’ – Enter the number of letters (uppercase and lowercase) required in a password.

‘0’ to ‘9’ – Enter the number of numerals required in a password.

Other – To use characters not defined as letters or numerals (symbols such as & or !), enter the number of symbols required in a password.

Enforce FDA Title 21 CFR Part 11 Password Policy – This feature is available for selection if your facility has purchased the FDA Part 11 option. Select this box to enable FDA Part 11 password policy. For more information, see “FDA Part 11” on page 283.



CAUTION *Changes to any of the FDA Password Policy settings will take effect only after all services have stopped and restarted using Service Control. You must also log off and on at the Server computer to see these changes.*

Directive Services Password Validation

P2000 user passwords can be authenticated against a directory service such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP). This eliminates user passwords from the P2000 database.

This feature is useful in situations where passwords are periodically changed and therefore, eliminates the need to update passwords in the P2000 system and also passwords that are used to log on to Windows.

To use directory service password validation, the following parameters must be defined:

Directory Services Path – This is the Lightweight Directory Access Protocol (LDAP) path for the directory server. The actual value to use for the Directory Services Path is unique to your specific network configuration and needs to be obtained from your network administrator.

Username Formatting – The formatting of the username passed to Directory Services for authentication. The username will be the string as entered with \$USERNAME replaced by the actual username. For Windows Active Directory the default “\$USERNAME” is recommended. Special formatting may be needed for LDAP systems or when requested by your Directory Services administrator.

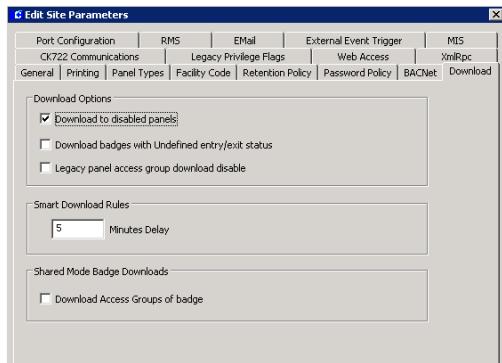
Use Encryption – Forces the connection to the Directory Services to use data encryption for network communications. Not recommended for Windows Active Directory. May be requested by your Directory Services administrator.

Secure Authentication – Requests the connection to the Directory Services to be made using secure communications such as Kerberos. Recommended for Windows Active Directory. May be requested by your Directory Services administrator.

Bind Server – Requests the Directory Services to bind to the server. Not needed for Windows Active Directory. May be needed for LDAP systems if your Directory Services Path includes a server name or when requested by your Directory Services administrator.

Download Tab

Use this tab to define different downloading options.



Download to disabled panels – Select this option to download items to disabled panels. If this option is not selected and the panel is offline, items that are automatically downloaded by the system will not be queued for download until you select this check box again.

Note: *If you do not select this option, when you enable the panel again using the Enabled function in the Edit Panel dialog box, you should queue a complete download for that panel, see “Downloading Data to Panels” on page 309.*

Download badges with Undefined entry/exit status – Select this option to change the entry/exit status of downloaded badges to Undefined.

Legacy panel access group download disable – Select this option to disable downloading badge identifiers to the panel when access groups are changed.

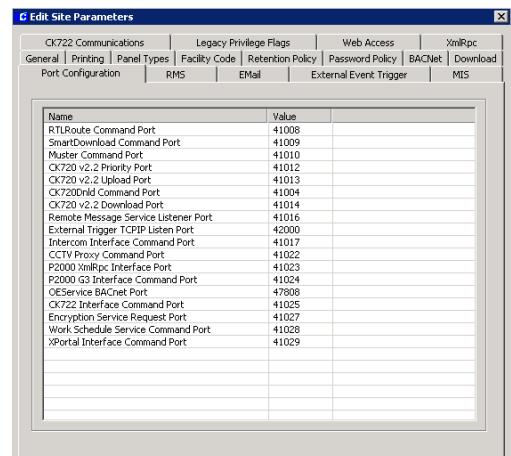
Smart Download Rules – This option defines the time for downloading badge identifiers to panels when changes are made to access groups and terminal groups, as well as defines the time for downloading entity and badge

identifier changes. The download will start automatically whenever the system does not process any access groups, terminal groups, entity or badge identifier changes, during the number of minutes that you enter in this field. The default value is 5 minutes. Enter **0** to download immediately.

Download Access Groups of badge – Select this option to enable downloading of access groups when downloading badges after a Central mode request for a terminal in Shared mode. Changes to this option will only take effect after you restart the P2000 Priority Service, refer to “Starting and Stopping Service Control” on page 315.

Port Configuration Tab

Use the Port Configuration tab to change the default port values that are assigned to the P2000 system applications during software installation. To change a port number, double-click the desired value and enter a number between 1 and 65535, you will be prompted to restart the Server and all workstations.

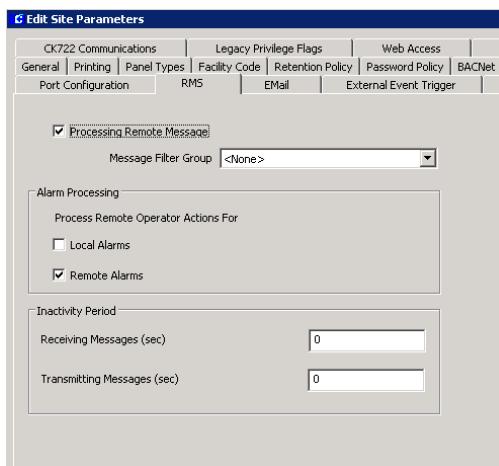


The CK720 Priority Port, CK720 Upload Port, and CK720 Download Port values (firmware version 2.2 and higher) **must** match the values

configured at the panel, and **must** use TCP/IP port numbers above 41000. This version of P2000 does not support CK720 panel versions prior to 2.2. If you use panel those panels, you must upgrade to the latest firmware.

RMS Tab

Settings in the Remote Message Service (RMS) tab determine if your P2000 site will receive messages from remote P2000 sites. In addition, you can define whether remote messages indicating alarm status changes for local and/or remote alarms are to be processed.



Processing Remote Message – Select this check box to receive messages from remote P2000 sites. If you select this option, the P2000 Remote Message Service will process incoming messages and pass them on to RTL-Route for distribution within the local system and, if applicable, to other remote sites.

Message Filter Group – Select from the drop-down list, the Message Filter Group that defines which remote messages your P2000 Remote Message Service will process. If you select <None>, your local P2000 site will be able to receive all remote messages. See “Con-

figure Message Filtering and Message Routing” on page 99 for detailed information.

Local Alarms – Select this check box to allow operators at a remote site to acknowledge, respond, and complete alarms originated at your P2000 site. By default, this option is not selected.

Remote Alarms – Select this check box to allow operators at a remote site to acknowledge, respond, and complete alarms originated at other P2000 sites. By default, this option is not selected.

Note: While the Alarm Status column in the Alarm Monitor window will display a “Responded” status, the alarm response entered at a remote P2000 site will **NOT** be part of the P2000 alarm history in your P2000 site.

Receiving Messages (sec) – Enter the time in seconds after which P2000 will generate an alarm because no messages are received from a remote server. If you enter “0,” an alarm will not be generated.

Transmitting Messages (sec) – Enter the time in seconds after which P2000 will generate an alarm because no messages are transmitted to a remote server. If you enter “0,” an alarm will not be generated.

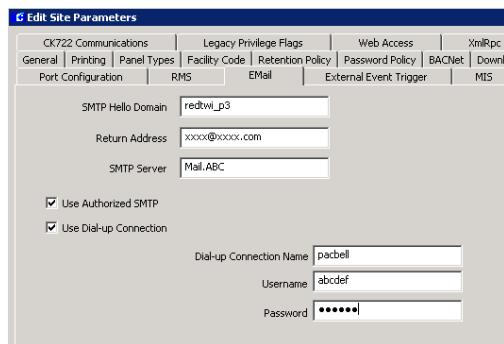
Note: The time configured here is applicable to all remote server connections from/to this computer. Inactivity periods are checked every 30 seconds by the Remote Message Service. These periods should be configured in line with the maximum duration of session configured in the Transmit Session tab in the P2000 Remote Server dialog box of the transmitting system.

All remote message server communication alarms generated by the local system will be

reset to “Secure” when the P2000 Remote Message Service is restarted.

Email Tab

Use this tab to enter a valid e-mail account that will be used to send e-mail messages, and also where automatic error returns could be sent. Before you enter your connection parameters, check with your Internet Service Provider (ISP) or IT department to verify the required connection settings.



SMTP Hello Domain – This value is the domain name sent with the SMTP “Hello” command. Enter the domain of the computer sending the e-mail. The computer name of the P2000 Server is normally acceptable unless your SMTP Administrator requests a specific value.

Return Address – Enter the e-mail address at your P2000 site that will be used to send messages and also be used to receive automatic error returns.

SMTP Server – Enter the name of the SMTP (Simple Mail Transfer Protocol) Server provided by your Internet Service Provider (ISP) or IT department.

Use Authorized SMTP – Select this check box if your ISP requires authenticated e-mail connections that need a username and password to send e-mails. The Dial-up Connection User- name and Password will be used.

Use Dial-up Connection – Select this check box if your P2000 site uses a dial-up connection (via telephone lines).

Dial-up Connection Name – Enter the name of the dial-up connection used at your P2000 site.

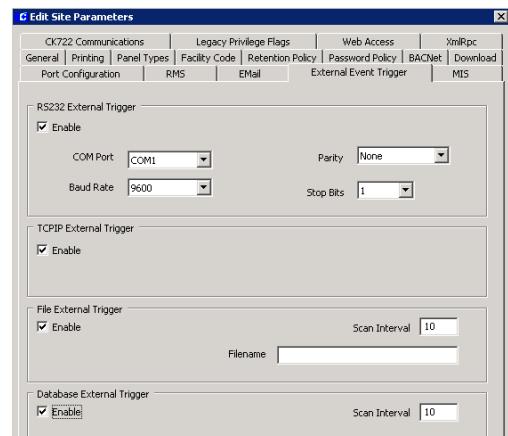
Username – Enter the name to be used to establish the dial-up connection.

Password – Enter the password to be used to establish the dial-up connection.

External Event Trigger Tab

The P2000 software allows external inputs to be used as event trigger conditions. These external inputs can be in the form of an RS232 serial message or a TCP/IP message; an ASCII file or a database write. These inputs allow external software or hardware systems to send a message to the P2000 system, which will trigger a Host event that will in turn generate an alarm or other event action.

Settings in this tab define which of the external inputs will be monitored.



RS232 External Trigger – If you select **Enable**, the P2000 system will open the configured RS232 port and listen for incoming characters. When characters are received, they will be

placed into an input buffer. When a carriage return is received, the current contents of the input buffer will be processed and checked to see if it meets a trigger condition. When the input buffer has been processed, it will be cleared and P2000 will start waiting for the next message. If you select this option, you must specify the **COM Port** to use. The RS232 port will be initialized with the **Baud Rate**, **Parity**, and **Stop Bits** configured for that port.

TCP/IP External Trigger – If you select **Enable**, the P2000 system will create a TCP/IP socket on the configured IP port and listen for incoming characters. When characters are received, they will be placed into an input buffer. When a carriage return is received, the current contents of the input buffer will be processed and checked to see if it meets a trigger condition. When the input buffer has been processed, it will be cleared and the P2000 will start waiting for the next message. The external system may connect to this TCP/IP socket and remain connected or it may disconnect after each message. If the external system remains connected, then only one external system may send messages. If the external system connects, sends the message, and then disconnects, then multiple external systems may send messages. If the P2000 detects a network error or if the external system closes its connection, the P2000 will return to the listen state waiting for new incoming connections.

File External Trigger – If you select **Enable**, the P2000 system will periodically check the configured location to look for the existence of the configured file name. When the specified file is found it will be renamed to <original name>.BAK. After it has been renamed, the lines in the file will be processed. The file must contain only ASCII text. If the file contains multiple lines, each line must be separated by a carriage return. The last line in the file may optionally include the carriage return or not.

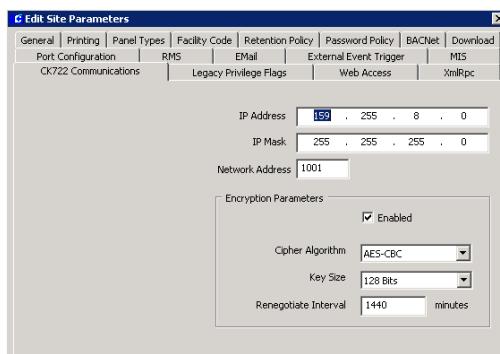
Each line in the file will be processed separately and checked to see if it meets a trigger condition. After the file has been processed, it will be deleted. If you select this option, you must enter the path and **Filename** of the ASCII file to look for, as well as the **Scan Interval** time (1 to 65535 seconds) between scans.

Database External Trigger – If you select **Enable**, the P2000 system will periodically check for any records in the external trigger database table. Each row found in this table will be processed separately and checked to see if it meets a trigger condition. After a row has been processed, it will be deleted. If you select this option, you must enter the **Scan Interval** time (1 to 65535 seconds) between scans.

Note: Since these external inputs do not authenticate the user sending the incoming message, enabling any of these inputs may cause the P2000 to be non-compliant with FDA Title 21 CFR Part 11. When you enable any of these external inputs, Site Parameters checks the Enforce FDA Rules setting. If this setting is on, then a warning message will display to inform that the P2000 may now be non-compliant if the events modify database records. Refer to “FDA Part 11” on page 283.

CK722 Communications Tab

Settings in the CK722 Communications tab are required to connect to the object engine and to communicate with CK722 panels. You must stop and restart the P2000 Object Engine Service for the changes to take effect, see “Starting and Stopping Service Control” on page 315.



IP Address – Enter the IP address of the object engine that is used to communicate with CK722 panels.

IP Mask – Enter the IP mask address of the object engine.

Network Address – This field displays the default value of **1001**. This value must be same throughout the BACnet Devices Network.

Enabled – Select Enabled to allow encryption of all messaging between CK722 panels and the P2000 Server.

Cipher Algorithm – Select from the drop-down list one of the following choices:

- **AES-CBC** – Advanced Encryption Standard. Strong encryption with long expected life. Key sizes: 128, 192, and 256 bits.
- **3DES-CBC** – DES repeated three times. Provides strong protection. Key size: 192.
- **DES-CBC** – Lower level security. Key size: 64.

Note: For more information about encryption standards refer to www.nist.gov.

Key Size – If you select AES, select the Key Size you wish to use. The greater the key number the higher the security, however the panel communications could be slower.

Renegotiate Interval – Enter a Renegotiate Interval. Periodic renegotiation refreshes the keys to limit the time a key is exposed. We recommend you use the default.

Legacy Privilege Flags Tab

In previous versions of P2000 some badge privileges, such as Executive privilege, Override privilege, and three Special Access flags, were assigned to entities on a global level. P2000 introduces the concept of Security Flags, which define the access rights that will be assigned to an entity using Access Profiles, (see page 138). The introduction of Security Flags makes assigning these privileges more granular, as now each door determines which access profile will be granting certain privileges.

The settings on this tab allow you to map badge options used in earlier versions of P2000 with the security flags generated during installation. P2000 automatically generates 100 security flag records during initial installation. The first five security flag records are initially reserved for mapping the badge privileges options.



Executive – Executive privileges allow entities unlimited access to all doors in a facility. Select from the drop-down list the Executive Privilege or any other Security Flag to be assigned as the Executive flag. The Executive privilege flags apply to all panels in the same partition as the badge identifier, and to all pan-

els that are defined as Public. If the badge identifier is in the Super User partition, then the Executive privilege applies to all panels.

Override – Select from the drop-down list the Override or any other Security Flag to be assigned as the Override flag.

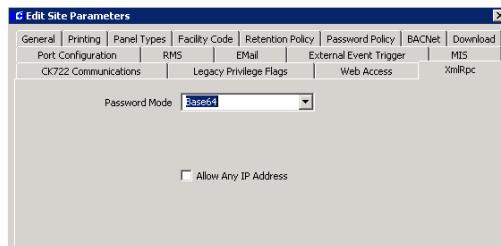
Special Access – Select from the drop-down list the associated Special Access or any other Security Flag to be assigned as the Special Access A, B, or C flag.

Once you define the legacy flags, refer to “Security Roles” on page 127 for instructions on how to manage and associate these flags with security roles.

Note: When modifying these settings, you must perform a full badge identifier download to all legacy panels.

XmRpc Tab

Use this tab to configure communications with an external device using the XmRpc protocol.



Password Mode – Select from the drop-down list one of the following encryption modes to be used for XmRpc communication:

- **Base64** – Password is Base64 encoded.
- **Clear Text** – Password is not encoded.
- **SHA Hash** – Password uses the SHA (Secure Hash Algorithm) standard.

Allow Any IP Address – Select the check box to allow the P2000 system to accept XmRpc commands from any IP address. If this check box is not selected, the P2000 system will only accept XmRpc commands from the IP address defined in the External IPs application, see page 235 for details.

Local Site

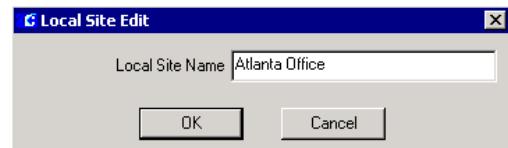
The P2000 Local Site name is assigned during the initial software installation and uniquely identifies the P2000 site within the P2000 Enterprise System.

The Local Site name is a system wide setting and does not require a partition reference. The site name is part of all audit entries, alarms, and transactions originated in your system. Applications such as the Alarm Monitor and Real Time List display the site name to indicate the P2000 site where the message originated.

The system allows changes to the Local Site name, for example to change the name of the facility location, however frequent changes to this setting are not recommended. Changes to the Local Site name can only be performed from the P2000 Server.

To Edit the P2000 Local Site Name:

1. In the System Configuration window, click the **Local Site** root icon.
2. Click the **Edit** button to open the Local Site Edit dialog box.

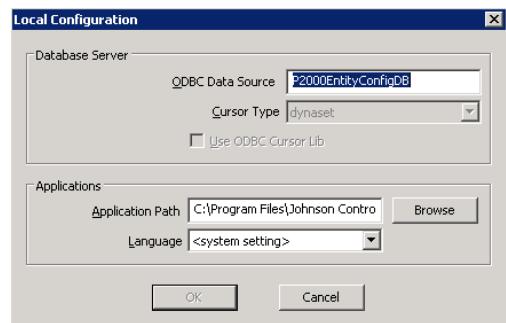


3. Enter a **Local Site Name** (up to 32 characters) that will easily identify your P2000 site.
4. Click **OK** to save the Local Site Name.
5. A message displays, warning that changing the site name requires you to update existing database records that refer to the current site name. Click **Yes** if you want to proceed to change the name.
6. You will be prompted to stop all P2000 services at the Server, refer to “Starting and Stopping Service Control” on page 315, and to log out of all workstations.
7. Click **OK** to proceed with the update of the database tables.
8. After the database tables have been updated, click **Yes** to restart the Server computer.

Local Configuration

Use the Local Configuration window to enter the database server source and application path of your P2000 system, and to select the language in which you wish the P2000 software to run. Incorrect settings in this dialog box will cause the P2000 software not to function properly.

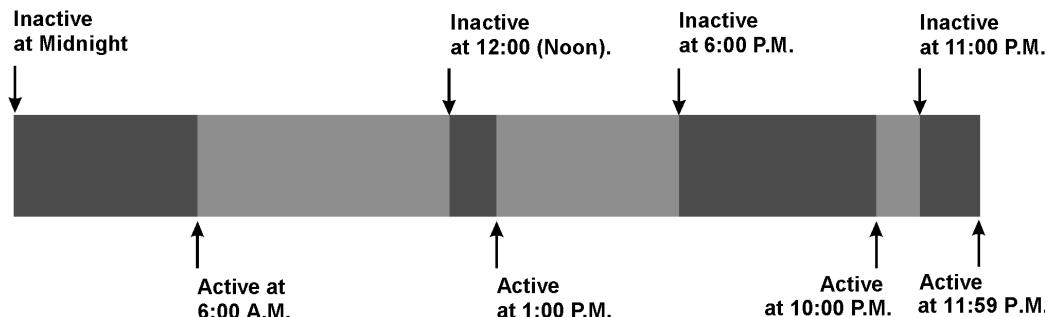
1. From the P2000 Main menu, select **Config>Local**. Enter your password if prompted. The Local Configuration dialog box opens.



2. The **ODBC Data Source** field displays the name of the ODBC data source that communicates with the database server.
3. The **Application Path** field displays the location of the P2000 program. Click **Browse** to find another path, if the location has changed.
4. If you wish to run the P2000 software in a language that is different from the Windows operating system language, select the desired **Language** from the drop-down list, otherwise use the default *<system settings>* option.

Note: Contact your Johnson Controls representative if you wish to run the P2000 software in a different language.

5. Click **OK** to save your settings. If you are switching languages, you will be prompted to close all P2000 programs and restart, in order for the changes to take effect.



Time Zones

Time zones define all the periods during which a reader, identifier, alarm point, or other system component or feature is active or inactive. A time zone is a set of enable and disable times applied to days of the week and holidays. You can set up different time zones and then assign these time zones to readers, inputs, outputs, terminal groups, and other system elements.

At least one time zone must be assigned to each panel. This could be done at the time the panels are created, or at a later time. See “Configure Panel Time Zones” on page 56.

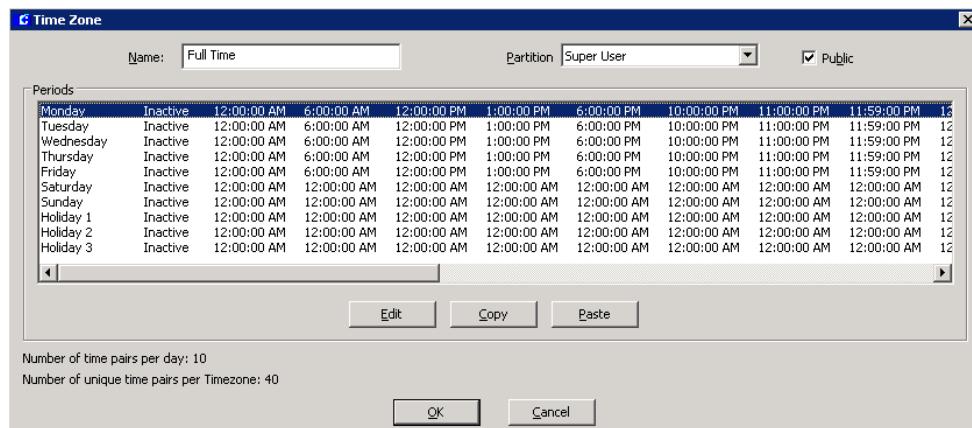
After time zones have been configured, click the plus (+) sign next to the Time Zones icon to display the various time zones configured for the system. When you click on a Time Zones

icon in the System Configuration window, the values for the time zone items display on the right windowpane.

Configuring Time Blocks

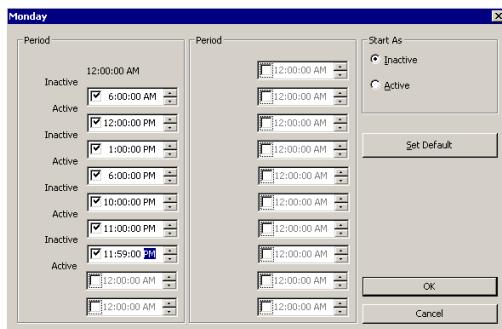
The period between an active and inactive time may be thought of as a time block. With four active and four inactive times (including midnight) you can configure up to eight time blocks per day.

The above example shows eight time blocks representing a “business hours” day, opened at 6:00 A.M., closed one hour for lunch, opened until 6:00 P.M., and opened for cleaning from 10:00 to 11:00 P.M.



To Create a New Time Zone:

1. Select the **Time Zones** icon and click the **Add** button at the bottom of the window. The Time Zone dialog box opens.
2. Select the **day of the week** (or a holiday) you wish to define and click the **Edit** button. A time zone dialog box opens with the name of the day in the title block.



3. In the Start As box, select whether, starting at midnight, this time zone will be Inactive or Active.

If you select “Inactive,” the time period between 12:00 A.M. and the hour entered in the first field in the list will be labeled “Inactive.” (See the Period group box.) If you select “Active” from the Start As box, the time period between 12:00 A.M. and the hour entered in the first field in the list will be labeled “Active.”

4. In the Period group box, define the time at which the period between 12:00 A.M. changes status (from Active to Inactive or vice versa).

Note: The time format displayed throughout the P2000 software is set up in the Windows Control Panel, Regional Options, under the Time tab.

Check the box and select the hour from the spin box. For example, if the time period

starting at midnight is *Inactive*, enter the hour at which the time period will become *Active*. In the next field, select the time at which the period will return to *Inactive*. You can include minutes and seconds, if needed.

Note: You can define a number of Active and Inactive times; however, select only those time check boxes you wish to enable. For example, to create a Time Zone that is active from 6:00 A.M. to 6:00 P.M., select the first check box and set the time to 6:00 A.M.; then select the second check box and set the time to 6:00 P.M.

5. The Set Default button sets all times to 12:00, and either Active or Inactive as defined in the Start As box.
6. Click **OK** to save the settings and return to the Time Zone dialog box.
7. Continue to edit and enter time zones, until all days of the week and any applicable holidays have been defined. Refer to the next section “To Copy a Time Zone.”
8. Enter a descriptive **Name** for the new time zone (Day Shift, Swing, and so on).
9. If this is a partitioned system, select the **Partition** in which this time zone will be active.
10. If this is a partitioned system, select **Public** if you wish this time zone to be visible to all partitions.
11. Click **OK**. To add this time zone to all panels, click **Yes**. Otherwise, you must add the new time zone for each panel separately using the Panel Timezone application, see page 56. To add the time zone to CK722 panels, use the SCT tool.

The new time zone icon and name displays in the list of items beneath the root Time Zones icon. These time zones will now be accessible to other system features such as

panels, workstations, entities, and so on, for the partition selected.

To Copy a Time Zone:

You can copy a time zone from one day to the next, or to all of the days.

1. In the Time Zone dialog box, define one time zone (a day of the week or a holiday).
2. Select the defined **time zone** and click **Copy**.
3. Select the day to which you wish to copy the time zone and click **Paste**.

Holiday Types

When the system reaches midnight prior to a day defined as a holiday it switches to Active and Inactive periods, depending on the Holiday Type specified for that time zone.

You can define three Holiday Types. For example, you may want to define a Type 1 holiday to indicate a full day, such as Christmas Day; and a Type 2 holiday as a half-day, such as Christmas Eve; and a Type 3 that is specific to your company.

You can set different Holiday Types for different Time Zones. For example, Night Shift full-day holiday hours may begin and end at different times than Day Shift full-day holiday hours.

To Create Holiday Types:

1. From the Time Zone window, select **Holiday 1** and click **Edit**.
2. Define the Active and Inactive periods as described for the other days of the week.
3. Define Holiday 2 and 3, if needed.
4. Click **OK** to save your settings and return to the System Configuration window.

These holiday types correspond directly to Type 1, 2, and 3 in the Edit Holiday dialog box.

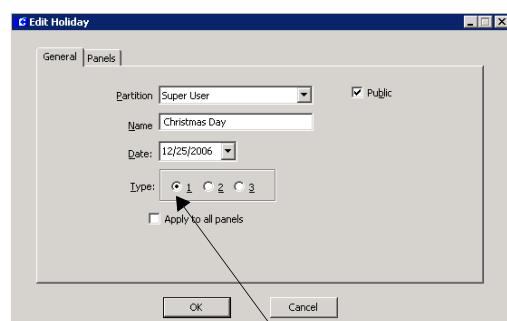
Holiday

Use the Holiday window to define dates when the system will use Holiday 1, 2, or 3 active and inactive periods rather than the usual time zones set for those days of the week. When the system reaches midnight prior to a day defined as a Holiday, it switches to Active and Inactive periods, depending on the Holiday type specified for that time zone.

Each day of a Holiday period must be assigned separately. For example, you may plan to allow two days off for the Christmas holiday. You must define two separate holidays with separate names and dates, such as Christmas 1 for the first date, and Christmas 2 for the second date.

To Add a Holiday:

1. Click the **Holidays** Icon in the System Configuration window.
2. Click the **Add** button. The Edit Holiday dialog box opens at the General tab.



Select a Type as defined on the Time Zone dialog box

3. If this is a partitioned system, select the **Partition** to which the Holiday will apply,

and select **Public** if you wish this Holiday to be visible to all partitions.

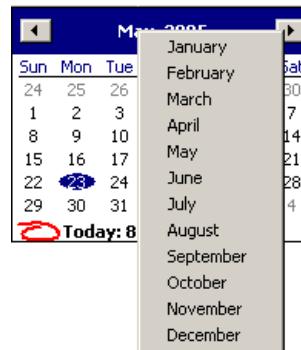
4. Enter the **Name** of the Holiday.
5. Enter the **Date** of the Holiday. (See “Using the Holiday Calendar” for details.)
6. Select the **Type: 1, 2, or 3** depending on the Holiday types set up in the Time Zone dialog box.
7. To add this Holiday to all panels, select the **Apply to all panels** check box.
8. To add this Holiday to specific panels, click the **Panels** tab and move the desired panels in the **Available Panels** list to the **Panels** list on the left side.

Note: This is particularly useful for adding Holidays to CK722 panels (the Holiday Type 1, 2, or 3 must match the Type defined using the SCT tool). For other panel types, you can either use this procedure or you can use the Panel Holiday application, see page 57.

9. Click **OK** to save the new Holiday.

Using the Holiday Calendar

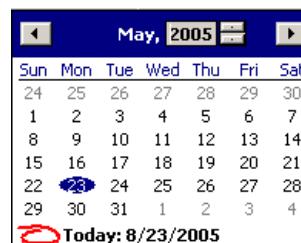
When you click the down arrow of the Date list box, the Holiday calendar displays. You can display any month or year on the calendar.



To Change the Calendar Year:

Do one of the following:

1. Use the left or right arrows in the Calendar header to move forward or backward through the months into the next or last year, or
2. Click the year in the Calendar header. A spin box displays. Use the spin arrows to move forward or backward through the years.



To Change the Calendar Month:

Do one of the following:

1. Use the left or right arrows in the Calendar header to move forward or backward through the months. You can also press Page Up or Page Down to move through the months, or
2. Click the name of the month in the Calendar header and choose a month from the list.

Assigning Holiday Types

Holiday Types correspond directly to Holiday 1, 2, and 3 on the Time Zone dialog box. You can define different hours for each holiday type, depending on your facility’s preferences. For example, in the Time Zone window, you may designate Holiday 1 as a full day and Holiday 2 as a half day. You can then create a holiday in the Holiday dialog box, such as New Year’s Eve, as Type 2, changing the active and

inactive times for that holiday to correspond with a half-day schedule. (See “Time Zones” on page 44 for more information on creating Holiday types.)

Configure Hardware Components

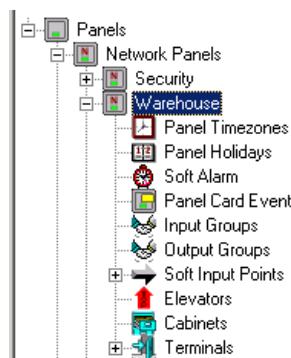
Hardware components are the physical panels, terminals, and other inputs and outputs that make up the security management system.

After the physical panel and terminal hardware is set up at the various system locations, panels and terminals must be created and then configured using the P2000 software program.

Note: To configure CK722 panels and related components, refer to the System Configuration Tool (SCT) Manual and to the CK722 Commissioning Guide.

Hardware Configuration Sequence

When you create panels, the new panel icons and names display under the root Panels icon in the System Configuration window, and placeholders for additional items that need to be configured are listed under each panel.



The logical configuration sequence, however, does not follow the order presented on the System Configuration window. We recommend hardware configuration begin with the following sequence:



Create Panels

Field panels are advanced intelligent controllers that interface between the Server and other hardware in the system. CK705, CK720, and CK721 panels communicate with the Server via 10Base-T and 10/100Base-T (CK721 only) network connections. S321 panels communicate with the Server via a loop configuration.

Panel Naming Conventions

Panels should be named logically, including information such as a panel’s location and what it controls. This will be helpful when configuring other system components and when troubleshooting the system. For example, the panel name *Bldg B SW Corner* will be more meaningful to an operator than *Panel 1B*. Descriptive names cannot only identify the panel name and location; but also, when terminals and time zones associated with this panel use similar names, the components will be listed together (alphabetically) when viewing a list of panels and terminals.

Loop Configuration

Use the Loop Configuration dialog box to configure the software to communicate S321 panel connections (loop number and address) to the

P2000 Server. See “Loop Communication” on page 6 for more information. New loops can only be created at the Server.

Note: Loop Configuration is not available in this release. This feature is not required with CK705, CK720, or CK721 panels, which communicate over a network connection.

To Configure Loop Configuration:

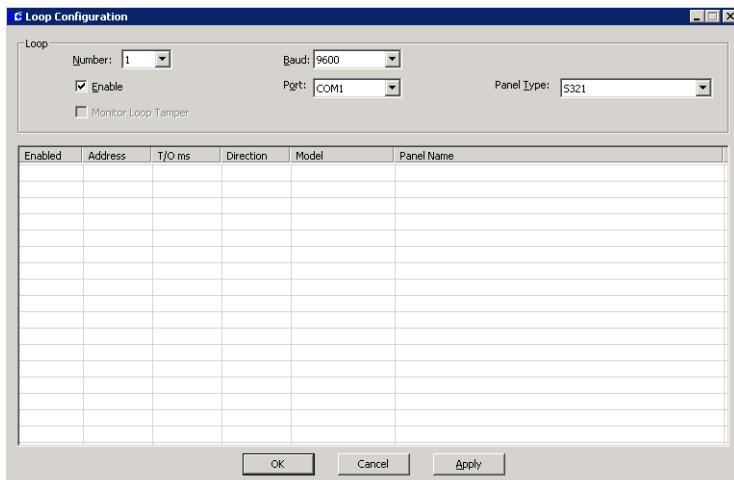
1. From the System Configuration window, click the plus (+) sign next to the root **Connections** icon to display the connecting options.
 2. Select the root **Serial** icon and click **Add**. The Loop Configuration dialog box opens.
 3. In the Loop box, select a loop **Number** (1 - 32) from the drop-down list.
 4. Select **Enable** to establish software communication with the loop. To temporarily disable loop communication, without having to delete the loop, select the check box again to disable it.

5. Select the **Baud** rate from the drop-down list that was programmed at the panel. (The default is 9600.)
 6. Select the **Serial Port** from the drop-down list. This represents the actual port in the AccelePort Serial Adapter.
 7. From the **Panel Type** drop-down list, select S321.
 8. Click **OK** to save your settings.

After panels have been created and configured for loop communication, the bottom box in the Loop Configuration dialog box will display the panel name, model, and others settings. The system will also allow you to enable or temporarily disable the panel from here, and this setting will be reflected in the Edit Panel dialog box for the panel selected.

To Add a New Panel:

1. From the System Configuration window, click the plus (+) sign next to the root **Panels** icon to display the root panel types.
 2. Select one of the following panel types:
Network Panels – To configure CK705, CK720, and CK721 panels.



S321 Panels – To configure S321 panels.
Not available in this release.

3. Click **Add**. The Edit Panel dialog box opens at the General tab.
4. Fill in the information on each tab. (See “Edit Panel Field Definitions” for details.)
5. As you work through the tabs, you may click **Apply** to save your entries.
6. Click **OK** to save your entries. A message box will display asking if you wish to automatically add all time zones to the new panel. If you select **No**, you can add the time zones later, refer to “Configure Panel Time Zones” on page 56.
7. If you select **Yes**, the time zones will be automatically added, and you will return to the System Configuration window, where a new Panel icon bearing the name assigned will be listed under the root Panel icon.

Soft Input Points

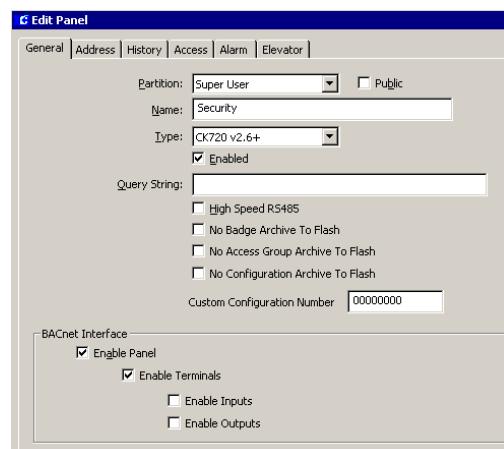
When a panel is created in the system, a Panel Down soft input point is automatically created for input point 25 and displays under the Soft Input Point icon as “Panel Down <panel name>.” If enabled in the Input Point dialog box, this input point will report to the Alarm Queue and Real Time List. If disabled, the alarm will not report to the Alarm Queue, but will continue to report to the Real Time List.

If you rename the panel, you must edit the input point to manually enter the new panel name, as in “Panel Down <panel name>.” Refer to “Create Input Points” on page 74 for detailed information.

Edit Panel Field Definitions

General Tab

This dialog box defines descriptive information of the panel.



Partition – If you use Partitioning, select the Partition that will have access to this panel information.

Public – If you use Partitioning, select the Public check box to allow all partitions to see this panel.

Name – Enter a descriptive name for the panel.

Type – Select a panel type from the drop-down list.

- *If you select a CK7xx panel type*, the Address and Elevator tabs are available.

Note: Throughout this chapter, the term CK7xx refers to CK720, CK721, and CK705 panels.

- *If you select an S321 panel type*, the Loop/Unit and Misc tabs are available.

Note: Certain features will be enabled/disabled depending on the panel version selected. The version selected will be validated when the panel connects. Network panels that do not match will be put into a misconfigured state and will not be allowed to fully communicate until the problem is solved.

Enabled – The system will not recognize the panel unless the **Enabled** check box is selected. To temporarily disable the panel, without having to delete the panel or disconnect the network cable, select the check box again to disable it. When you disable a panel, the readers will continue to grant access, but the panel will not communicate with the Server until you enable the panel again.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 103), and is also used with the P2000-Metasys option (refer to “Configuring Hardware Components for BACnet Interface” on page 237).

High Speed RS485 – Select this box to allow a fast communication rate with RS485 serial connectors to CK7xx add-on terminals. This option requires high-speed add-on terminals. See the CK7xx manual for configurations that support the faster communications rate.

No Badge Archive to Flash – Available for CK7xx panels version 2.5 and higher. If enabled, the Badge database is not saved to Flash during a Write-Flash operation.

No Access Group Archive to Flash – Available for CK7xx panels version 2.5 and higher. If enabled, the Access Group database (including elevator Access Groups) is not saved to Flash during a Write-Flash operation.

No Configuration Archive to Flash – Available for CK7xx panels version 2.5 and higher. If enabled, the Configuration databases such as Panel, Elevator, Terminal, Input, Output, Time

Zones, Holidays, Soft Alarms, and Card Events are not saved to Flash during a Write-Flash operation.

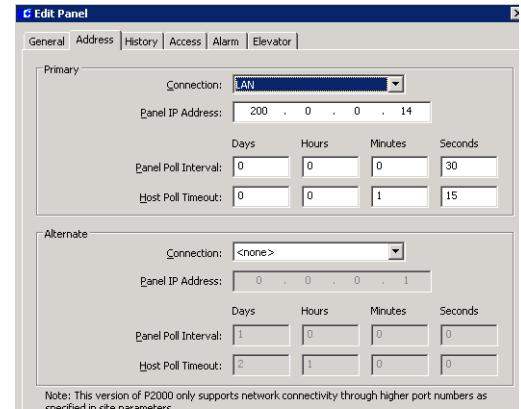
Custom Configuration Number – Available for CK7xx panels version 2.6 and higher. This field allows you to enter a number that is provided by *Johnson Controls*, to enable special custom features.

BACnet Interface – Select the **Enable Panel** check box to define the panel, and if you wish, the associated Terminals, Inputs and Outputs check boxes, as BACnet objects. The number of BACnet objects should not exceed 7200. Keep the number of BACnet objects reasonably low; otherwise, system performance can be adversely affected. Refer to the *Metasys® and P2000AE Integration Manual* for details.

Address Tab

Use this tab when configuring CK7xx panels. This dialog box defines Primary and Alternate IP addresses for the panel. (You cannot complete panel configuration unless you assign an IP address.)

Note: You must first configure the panel at the Server, then proceed to configure the panel using the CK7xx panel user interface.



Primary Connection – The default connection for standard network connected panels is LAN.

Primary Panel IP Address – Enter the IP Address. This entry must match the IP address at the panel.

Primary Panel Poll Interval – Enter the number of days, hours, minutes, and/or seconds to set up the maximum time that the panel should be without contact with the Server. This value is downloaded to the panel.

Primary Host Poll Timeout – Enter the number of days, hours, minutes and/or seconds that the Server will wait without receiving a poll, until it declares the panel down.

Use the **Alternate** box to configure panels (CK720 or CK705 version 2.5 and higher) that have a second network connection through a Dual Ethernet interface. Dual Ethernet allows the alternate connection to take over the communications if the primary connection fails.

Alternate Connection – For panels with two network connections, select the **LAN** option from the drop-down list.

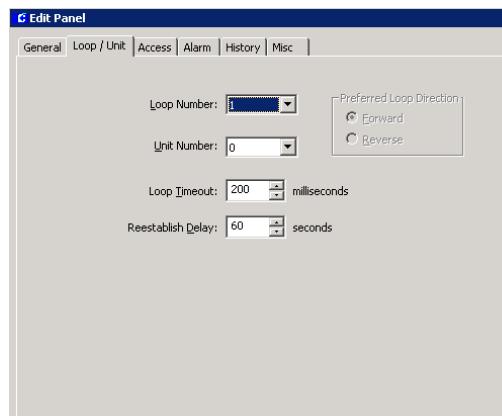
Alternate Panel IP Address – For panels with two network connections, enter the IP address of the alternate connection. This entry should be from a different subnet address and must match the IP address at the panel.

Alternate Panel Poll Interval – Enter the number of days, hours, minutes, and/or seconds to set up the maximum time that the panel should be without contact with the Server. This value is downloaded to the panel.

Alternate Host Poll Timeout – Enter the number of days, hours, minutes and/or seconds that the Server will wait without receiving a poll, until it declares the panel down.

Loop/Unit Tab

Use this tab when configuring S321 panels. (S321 panels are not available in this release.)



Loop Number – Select from the drop-down list a loop number defined in the Loop Configuration dialog box. The P2000 system can support up to 32 loops.

Unit Number – Select from the drop-down list a unit number to be assigned to this panel. The P2000 system supports up to thirty S321 panels per loop.

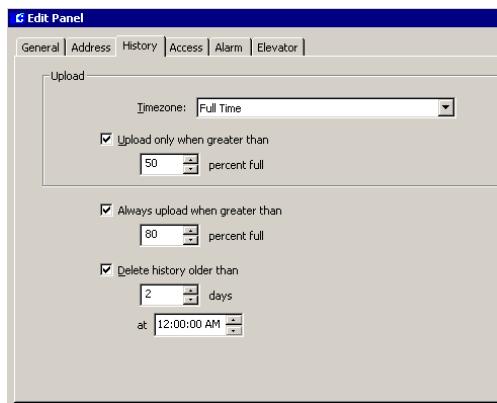
Loop Timeout – Select the time from the spin box (100 to 2000 milliseconds) that the port driver will wait for a response to a message, before going offline.

Reestablish Delay – Select the time from the spin box (5 to 32000 seconds) after which the panel will try to reestablish communication.

Preferred Loop Direction – Not available for S321 panels.

History Tab

History settings govern how the panel uploads data to the Server, and how long the panel retains data in the transaction database before older data is deleted.



Timezone – Select a time zone from the drop-down list during which the panel uploads data to the Server.

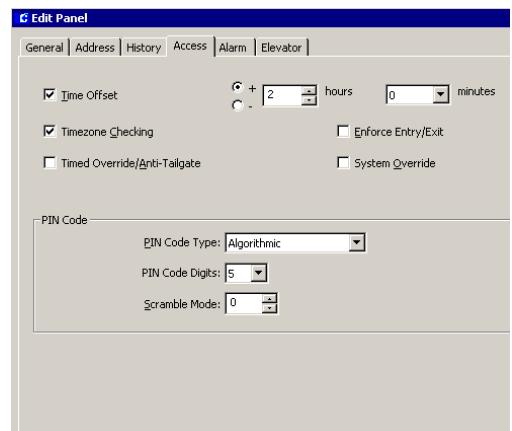
Upload only when greater than – To limit the panel from always uploading data to the Server during the time zone selected, select this box and select a percentage from the spin box only after which data will be uploaded.

Always upload when greater than – Select this box and select a percentage from the spin box after which the panel will always upload data to the Server.

Delete history older than – Select this box and enter the number of days the panel will hold data before deletion. Select a time at which the history will be deleted.

Access Tab

This dialog box defines Time Offsets for communicating with remote panels and other time zone-related information. Here you enable or disable Timed Override/Anti-Tailgate, Entry/Exit, and System Override parameters; and set the PIN Code type used at the panel. (See the *Tip* box on page 54 for more information on PIN types.)



Time Offset – Enable Time Offset if the panel is in a different geographical time zone from the Server. Enter the appropriate hours and minutes for the time offset.

Timezone Checking – Enable Timezone Checking if the panel is to check for valid reader and badge time zones, badge access requests, PIN code suppression, and upload suppression during the assigned time zones. If disabled, badge access decisions will be made on the basis of valid badge and valid access group parameters only.

Enforce Entry/Exit – Enable Enforce Entry/Exit if the panel will operate Entry and Exit terminals. Entry and Exit terminals require entities to badge at Entry and Exit terminals alternately. For example, badging at an Entry terminal and then badging again at another Entry terminal is invalid. If Entry and Exit terminals are installed in the panel, the Enforce Entry/Exit check box must be enabled for the Entry and Exit requirements to operate.

Timed Override/Anti-Tailgate – If enabled, a Reader-controlled door in a state of manual Timed Override will be locked automatically when the door is closed. If disabled, the Reader-controlled door will remain in override mode even when the door is closed.

System Override – If enabled, all doors controlled by the panel are set in the unlocked position. If disabled, all doors are set to their normal position.

PIN Code Type – Select a PIN code type from the drop-down list (**Algorithmic** or **Custom**). An algorithmic PIN is determined by an algorithm programmed in the terminal. A custom PIN code must be entered in the Identifier tab for each individual entity. (See the following *Tip* box for more information on PIN types, and refer to “Configure PIN Codes” on page 70 for instructions.) Algorithmic codes need to be requested from Technical Support.

PIN Code Digits – Select from the drop-down list the number of PIN code digits (**4** or **5**) that will allow access at a keypad terminal.

TIP: *We recommend all panels in the system that use PIN code readers be defined to use the same number of PIN code digits and to have the same PIN type, or access may be denied. Access would be denied because of mismatches in PIN code length and type between the PINs defined here and the PINs defined in the Identifier tab of Entity Management.*

Scramble Mode – Eight algorithms are embedded in the terminal. If **Algorithmic** was selected in the PIN Code Type field, enter a number from 0 through 7 to choose the appropriate algorithm.

Alarm Tab

Panel relay, latch output functionality, and other parameters are set up in the Alarm tab.



Reporting Delay – If enabled, the alarm is delayed by the number of seconds (0 to 60) set in the Reporting Delay field. If the input point returns to the secure state before the delay expires, the panel will not report the alarm to the Server at all. If disabled, the alarm is reported immediately. Open and short conditions for 4-state input points are reported immediately regardless of this setting.

Latch Output – Not available for S321 panels. If enabled, the alarm relay is activated whenever an alarm occurs, and remains latched (activated) until reset by a card activated event, or acknowledged at the panel. If disabled, the panel alarm relay is activated whenever an alarm occurs and deactivated when all alarms are reset (if configured to do so in the Input Point dialog box).

Enable Panel Relay Group Outputs – Not available for S321 panels. If enabled, two output groups are created to represent the two physical output points on the panel CPU board: Relay 1 and Relay 2. These display as icons under the Output Groups icon for the panel selected. These output groups can be controlled as any other output group in the system.

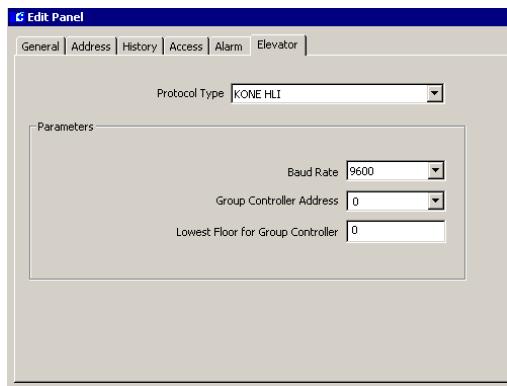
Output Delay – Not available for S321 panels. Enter the number of seconds before the latch in the Latch Output field is to be activated. Use this field only when the Latch Output field is

enabled. You can define a time interval before the panel's alarm relay activates; for example, if an input point has been configured to activate the panel's alarm relay, this would be the selectable delay in seconds (0 to 60), before the relay activates. The delay starts after the input point has activated.

Enable Input Suppression Messages – Available for CK7xx panels version 2.5 and higher. If enabled, input points that enter suppression will be reported as being suppressed. When the input is no longer suppressed, the current input point state is reported.

Elevator Tab

Use this tab to configure the panel to communicate with *High Level Interface* elevator control equipment via a serial protocol. Once the elevator protocol parameters are defined, use the Elevator Configuration dialog box to define the readers and associated outputs/inputs that will operate with your particular elevator controller. For details, refer to “Elevator Access Control” on page 87.



Protocol Type – Select from the drop-down list the KONE HLI option. This is the only type supported in this release. Protocols 1 to 10 are reserved for future use.

Baud Rate – Select the baud rate from the drop-down list, options are 9600 or 1200. This setting must match the baud rate configured at the elevator group controller.

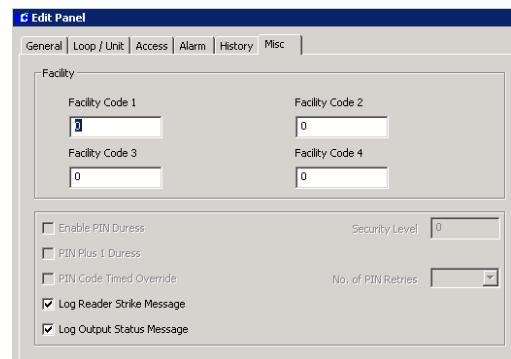
Group Controller Address – Select an address (1 to 8) from the group controller address drop-down list. This setting must match the address of the elevator group controller. An incorrect setting will not permit the integration to be operational.

Lowest Floor for Group Controller – Enter the lowest level (1 to 64) of the building served by any KONE elevator in this KONE group controller. An incorrect setting will secure and unsecure floors other than those intended.

Misc Tab

Use this tab when configuring S321 panels. Enter the facility code provided by *Johnson Controls*.

Note: Facility codes for CK7xx panels are assigned in the Edit Terminal dialog box.

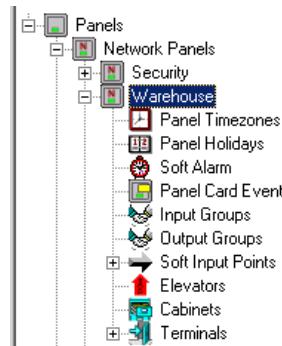


Log Reader Strike Message – If selected, the transaction will display in the Real Time List and on the System Status window.

Log Output Status Message – Select this check box to send output relay messages from the panel to the Server (whether or not access is granted). Must be selected to show as active on the System Status window.

Configure Panel Components

When a new panel is created, the new Panel icon is listed under the root Panels icon in the System Configuration window, and placeholders for all panel components are added under the new panel.



Some components must be configured before they can be applied to other components; however, the System Configuration window does not list them in a logical configuration sequence. For example, you must configure Panel Time Zones before you can complete Terminal configuration, but you must configure Terminals before you can create Soft Alarms, Input and Output Points and Groups, and Panel Card Events. For this reason, it is important to configure Panel Time Zones and Panel Holidays (if used), and then configure Terminals before continuing with other panel components. We recommend the following configuration sequence:

- **Configure Panel Time Zones**
- **Configure Panel Holidays**

- **Configure Panel Card Formats**
- **Configure Additional Panel Components**

Complete instructions are presented in the following sections.

Configure Panel Time Zones

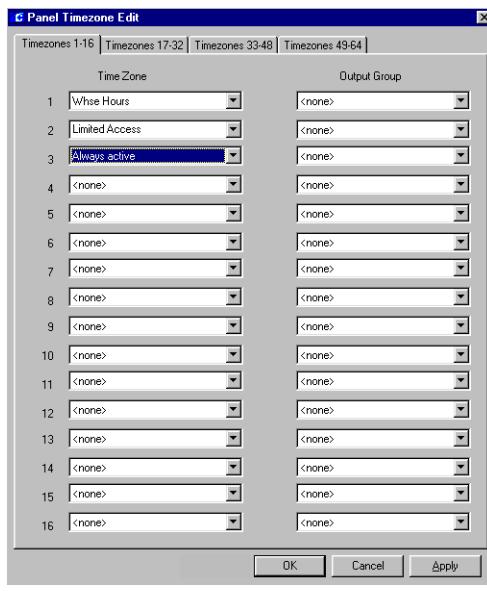
Time Zones (created during System Configuration) can be applied to a specific panel and its associated components. You must apply at least one time zone to each panel in your system. If time zones are applicable to other panel components such as readers, inputs or outputs, these time zones must also be defined.

You can automatically operate outputs such as lights, air conditioning, and so on, by associating Output Groups with Panel Time Zones.

Panel Time Zones must be defined before you can complete Terminal configuration. If you have not yet configured Terminals and Output Groups, you should enter Panel Time Zones now, and return to add the Output Groups and any additional time zones.

To Assign a Panel Time Zone:

1. From the System Configuration window, click the plus (+) sign next to the Panel to which you wish to assign the Time Zone. The panel components are listed below the panel icon.
2. Click the **Panel Timezones** icon and click **Edit**. The Panel Timezone Edit dialog box opens.



3. Use the drop-down lists to select any time zones configured in the system.
4. If you need to assign more than 16 time zones, click the **Timezones 17–32** tab and continue to add time zones as in Step 3. Select additional tabs and enter additional time zones as needed, up to a total of 64.
5. After all time zones (and Output Groups, if applicable) are assigned, click **OK** to save your entries and return to the System Configuration window.

To Assign an Output Group to a Panel Time Zone:

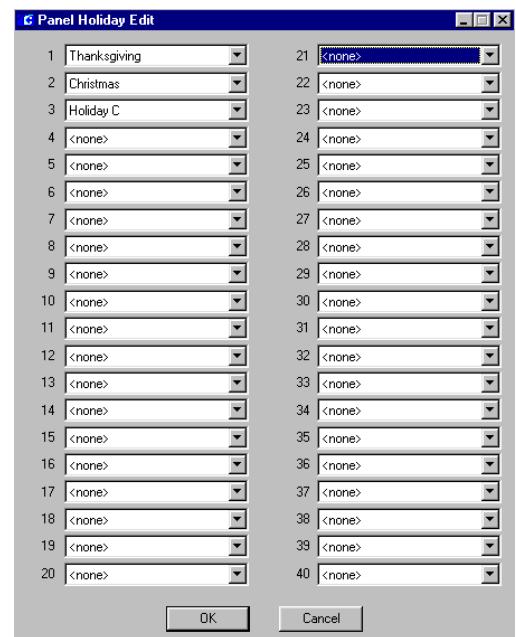
1. In the Panel Timezone Edit dialog box, select the **Time Zone** to which you wish to associate an Output Group.
2. Under the Output Group header next to the selected Time Zone, select an **Output Group** from the drop-down list. Output Groups must be created before they will be accessible from the Panel Time Zone drop-down lists. (See “Create Input and Output Points and Groups” on page 72.)

Configure Panel Holidays

Panel Holidays are not required for system operation; however, they may be useful in certain applications. For example, you may want to allow facility access during a Holiday period, but limit the number of entry doors. You can assign a specific Holiday Time Zone to restrict access at a specific panel. You can define up to 40 Panel Holidays.

To Assign a Panel Holiday:

1. From the System Configuration window, click the plus (+) sign next to the Panel to which you wish to assign a Panel Holiday.
2. Click the **Panel Holidays** icon and click **Edit**. The Panel Holiday Edit dialog box opens.



3. Use the drop-down lists to select the system Holidays that will apply to this panel.

- When all Holidays are defined, click **OK** to save the settings and return to the System Configuration window.

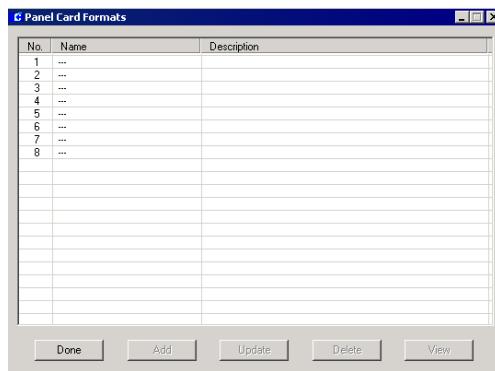
Configure Panel Card Formats

P2000 supports up to eight custom card formats that can be downloaded to all S321 and CK7xx panels of version 2.2 or higher. Upon selection, custom card files will be stored in a separate database table. Once the selected card formats have been compiled, they will be available for selection using the Card Type tab in the Edit Terminal dialog box.

Note: Contact Johnson Controls for instructions in generating Custom Card Format files.

To Add Custom Card Formats:

- In the System Configuration window, click the **Panel Card Formats** icon and click **Edit**. The Panel Card Formats dialog box opens.



- To add a custom card format, click the line item you wish to define and click the **Add** button.
- Navigate to the directory where your card format files are stored and double-click the <name>.txt file you wish to use. The name

and description of the selected card format file displays in the line item selected. You can add up to eight custom card format files.

Note: Do not import card formats that are already available as standard formats in the Card Type tab, see page 68.

- To update or replace an existing file, select the file name from the list and click **Update**. A verification message displays, click **Yes** then proceed to select the replacement file.
- To delete a file format, select the file name from the list and click **Delete**. You will be prompted for verification.
- To view the contents of a file format, select the file from the list and click **View**. A text file will display the format code string of the selected format. When you finish viewing the file, close the window.
- Click **Done** to close the Panel Card Formats dialog box. The new card formats will be available from the Card Type tab in the Edit Terminal dialog box.

Configure Additional Panel Components

Soft Alarms, Input and Output Points and Groups, and Panel Card Events all use Terminal information in their configuration; therefore, you must create and configure terminals before you can configure these components. See “Create and Configure Terminals” for more information.

Create and Configure Terminals

Terminals are add-in boards such as reader boards and Input/Output boards. These are installed into the panels to communicate with

devices such as card readers; input groups such as alarm monitoring devices; and output devices that control other devices such as lights, air conditioning, alarm annunciations, and so forth.

Each terminal installed in your system must be set up and configured in the P2000 software to establish communication and control. Once Terminals are configured, they may be included in Terminal Groups and associated with Input Points and Groups to report alarms and trigger events. We recommend the following setup and configuration sequence:

- **Set up Terminals for Each Panel**
- **Create Terminal Groups**
- **Create Input and Output Points and Groups**

Complete instructions are presented in the following sections. If you have not already developed naming conventions for these program elements, it will be helpful to do so before beginning this procedure. Refer to “Panel Naming Conventions” on page 48 for more information.

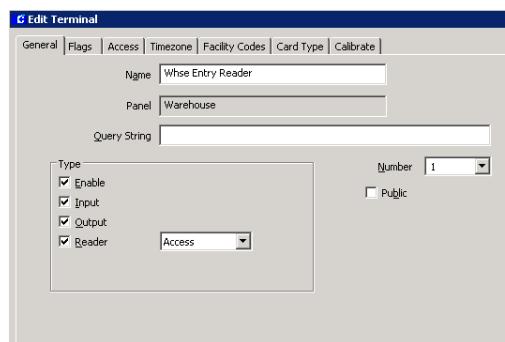
Set up Terminals for each Panel

Terminals can control card readers, input points, output points, or a combination of the three, depending on the type of board installed in the panel. You must set up terminals for each panel configured in the P2000 software. As with all configuration operations, the Edit Terminal dialog box is accessed from the System Configuration window.

Note: Not all terminal options are available to all panel types. Terminal options available are dependent on the type of panel they are connected to.

To Create a New Terminal:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon to display the root panel types.
2. Click the plus (+) sign next to the panel type configured for your system, for example **Network Panels**. The panel names created under this type will display.
3. Click the plus (+) sign next to the panel in which the terminal is installed. All the items that can be configured for the panel are listed under it.
4. Click the **Terminals** icon and click **Add**. The Edit Terminal dialog box opens at the General tab. Enter the information in each tab according to your system requirements and naming conventions. (See “Edit Terminal Field Definitions” for detailed information.) As you work through the tabs, click **Apply** to save your settings.



5. When all entries are complete, click **OK** to save your settings and return to the System Configuration window. Your new terminal icon and name will be listed under the Terminal icon. In the following example, Terminals named Whse Entry Reader, Whse Exit Reader, and Whse I/O8 were created for the Warehouse panel.



- Continue to create terminals for every panel in which they are installed.

Edit Terminal Field Definitions

The Edit Terminal dialog box opens at the General tab. You must enter information in all Edit Terminal tabs to complete configuration. Tabs are dependent on the type of panel.

General Tab

Name – Enter the name of the new Terminal. Remember to use descriptive names according to your Naming Conventions Plan.

Panel – This field will default to the name of the panel you selected from the System Configuration window.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 103), and is also used with the P2000-Metasys option (refer to “Configuring Hardware Components for BACnet Interface” on page 237).

Enable – Select **Enable** so the new terminal will be recognized by the system, then select the terminal types you have installed in this panel:

Input – Indicates an alarm monitor terminal or another terminal that provides input points.

Output – Indicates an output control terminal or another terminal that provides output points.

Reader – Indicates a card reader terminal. If selected as the terminal type, additional tabs

are added. Choose one of the following reader types from the drop-down list:

- **Access** – Normal access reader.
- **Entry** – Entry defined access reader.
- **Exit** – Exit defined access reader.

Note: *For Entry/Exit to work, all Entry and all Exit terminals must either run in Central mode, or they must all be defined on the same panel and run in Local mode.*

Number – Enter a terminal address number. This terminal address number corresponds to the physical address as installed at the panel. (See your specific hardware configuration if you need more information on terminal address assignment.)

Public – (Displays on partitioned systems only.) Select the **Public** check box if you wish this terminal to be visible to all partitions.

Flags Tab

Edit Terminal	
General Flags Access Timezone Facility Codes Card Type Calibrate	
Reader <input type="checkbox"/> Alarm Shunt Only for Auxiliary Access <input type="checkbox"/> Facility Code Only when Offline <input type="checkbox"/> PIN Required when Offline <input type="checkbox"/> Allow PIN after Badge <input type="checkbox"/> Reverse Reading <input checked="" type="checkbox"/> Log Reader Strike Message <input type="checkbox"/> Access Grant Message on Door Open Only <input type="checkbox"/> Re-lock on Door Open <input type="checkbox"/> No Green Light on Aux Access <input type="checkbox"/> Deny If Door Open	
<input type="checkbox"/> Anti Tailgate <input type="checkbox"/> Momentary Auxiliary Access <input type="checkbox"/> Reader Override Timezone Enable <input type="checkbox"/> Soft In-It <input type="checkbox"/> Valid & Unauthorized <input type="checkbox"/> Reverse Swipe Duress <input type="checkbox"/> PIN Plus 1 Duress <input type="checkbox"/> Star Feature <input type="checkbox"/> BQT Reader with LCD	
Input/Output Alarm Debounce Time: <input type="text" value="20"/> 10 ms <input checked="" type="checkbox"/> Log Output Status Message	
Override Reset Threat Level Override is reset when the threat level reaches <input type="text" value="1"/>	

Reader Box

Alarm Shunt Only for Auxiliary Access – If enabled, the Aux-Access Input Point on the terminal will suppress only the Door Open

Alarm. If disabled, the Aux-Access Input Point on the terminal will perform an access grant.

Facility Code Only when Offline – If enabled, the terminal accepts any badge with the correct facility code when the terminal is offline from the panel. Not available for S321 panels.

PIN Required when Offline – If enabled, an algorithmic PIN number is required for badge acceptance if the terminal goes offline. Not available for S321 panels.

Allow PIN after Badge – If enabled, an entity can enter the PIN number after presenting the badge instead of before presenting the badge. Press the <#> key after entering the PIN number (refer to “Configure PIN Codes” on page 70). If disabled, the conditions under Trigger Type in the Options box of the Panel Card Event will apply, see page 84.

Reverse Reading – If enabled, when you turn a badge facing away from you and swipe in the normal direction, the badge will still read. This does not apply to mag stripe, proximity, or barcode cards.

Log Reader Strike Message – Not available for S321 panels. If enabled, the transaction will display in the Real Time List and on the System Status window. This option must be disabled if the reader is to be assigned to an elevator or cabinet.

Access Grant Message on Door Open Only – If enabled, access grant messages are generated when an entity swipes the badge and opens the door. This option is only available for S321 and CK7xx panels version 2.0 and higher. For this feature to work, the terminal must be configured to run in Local mode.

Re-lock on Door Open – This option is only available for S321 and CK7xx panels version 2.2 and higher with RDR2 add-on terminals of model number PS201-E or higher. Normally

the Anti-Tailgate and Timed Override/Anti Tailgate options cancel both access time and shunt time when the door closes. Enabling the Re-lock on Door Open option will modify the anti-tailgate feature to lock the strike when the door opens, for example to avoid excessive wear of the electrical equipment. The shunt time is still cancelled when the door closes.

Note: *The Re-Lock on Door Open mode is only available if the RDR2 is of model number PS201-E or higher. If not, the Re-Lock on Door Open mode will work identically to the existing Anti-Tailgate mode. For specific instructions, refer to the CK7xx release 2.2 and higher documentation.*

No Green Light on Aux Access – Available for CK7xx panels version 2.5 and higher. If enabled, no green light will display on auxiliary access. (Requires S300-DIN-RDR2S, with firmware revision Q or above.)

Deny If Door Open – Available for CK7xx panels version 2.5 and higher. If enabled, an access denied message is generated when an entity swipes the badge at an opened door.

Anti Tailgate – If enabled, the access timer resets and the door immediately locks when the door closes. This prevents reopening the door using one badge access.

Momentary Auxiliary Access – If enabled, the Access Time will begin timing when a switch shorts the terminal’s Aux-Access input point contact. If disabled, the terminal’s Aux-Access input point contact will energize the door relay as long as the contact is shorted.

Reader Override Timezone Enable – If enabled, the reader does not require a badge to open the door during the reader override time zone. (A time zone must be selected in the Override field of the Timezone tab to enable this function.)

Soft In-X-It – If enabled, entities will have access even though the In-X-It status is incorrect. (A soft alarm can be triggered if configured through the Soft Alarms dialog box, see page 86.)

Valid & Unauthorized – If enabled, a green light indicates that badging has taken place, however the system will not grant access to the entity. A security guard must manually unlock the door with a key or push a button to open the door and allow access.

Reverse Swipe Duress – If enabled, you can turn the badge away from you and swipe in the normal direction to report a duress alarm. (Soft alarm must be configured for this reader, refer to “Soft Alarms Field Definitions” on page 86.) This does not apply to mag stripe, proximity, or barcode cards. When you enable Reverse Swipe Duress, the Reverse Reading option is automatically enabled.

PIN Plus 1 Duress – This option is only available for S321 and CK7xx panels version 2.2 and higher. If enabled, a duress alarm is generated when an entity adds 1 to the last digit of the PIN code (e.g. 6 becomes 7, not 61). When this option is enabled, the 9 does not create a duress alarm. If the last digit of the PIN code is a 9, then the user substitutes a 0 for the 9 and this will trigger the duress alarm. This feature only works if the Duress soft alarm is enabled.

Star Feature – This option is only available for S321 and CK7xx panels version 2.2 and higher. If enabled, an entity can press the star (*) key at the keypad plus a feature number, to activate some of the panel’s functions that are normally invoked from keypads that contain the A, B, C or D keys. The (#) key acts as the *Enter* key, it wraps-up the previously entered keys and starts the processing of the key sequence. It also clears the keypad buffer for the next command to be entered. The (*) key starts the feature selection process. Once

pressed, the entity can activate one of the following features:

0 = Local Override, followed by number of minutes

1 = Enable event, followed by event number

2 = Disable event, followed by event number

* = Clear the keypad buffer. This works independently of the Star Feature setting

The entity must enter all PIN and Card ID information before selecting a feature. As an alternative, instead of pressing the (#) key, the entity can swipe the badge to wrap-up the previously entered keys and start the processing of the key sequence, unless the “Allow PIN after badge” option is selected.

For details refer to *Appendix G: Using a Keypad Reader on CK721/720/705 Panels*.

BQT Reader with LCD – Available for CK7xx panels version 2.5 and higher. If selected, the system will enable the LCD display of the following messages (arranged from highest to lowest initial priority):

■ **Reader Offline** – A “reader offline” message will display on the LCD when a terminal cannot communicate with a panel for more than 5 seconds. As soon as a poll message is received, this message will no longer display.

■ **Access Granted** – An “access granted” message will display on the LCD when a reader is not offline. When the granted access timer expires, this message will no longer display. The LCD will display the access granted message when it is in override, it has received an assisted activate message, or it has received a normal access grant.

■ **Access Denied** – An “access denied” message will display on the LCD when a reader is not offline and does not have an active access granted message. When the denied

access timer expires, this message will no longer display. The denied access time is either 1.5 seconds, or the defined assisted access time (see page 66). The LCD will display the access denied message when it has received an invalid assisted activate message, or it has received an invalid access grant.

- **Enter PIN Code** – An “enter PIN code” message will display on the LCD when a reader is not offline, it does not have an active access granted message, and it does not have an active access denied message. The LCD will display the enter PIN code message when a PIN code is required after a regular badge swipe; the PIN Only flag is set and the user pressed a key at the reader; the Card ID flag is set and the user pressed a key at the reader; or the PIN + Card ID flag is set at the terminal and the user depressed a key at the reader.
- **Enter Shunt Time** – An “enter shunt time” message will display on the LCD when a reader is not offline, it does not have an active access granted message, it does not have an active access denied message, or it does not have an active PIN code message. The LCD will display the enter shunt time message after a regular badge with override privilege has been swiped. The shunt timer range is from 0 to 9999 minutes.
- **Shunt Time Warning** – A “shunt time warning” message will display on the LCD when a reader is not offline, it does not have an active access granted message, it does not have an active access denied message, it does not have an active PIN code message, or it does not have an active shunt time message. The LCD will display the shunt time warning when the shunt timer value reaches the value defined for the shunt warning time.
- **Present Card** – A “present card” message displays on the LCD by default. Since it has the lowest priority (unless changed by the

customer), this message will not display as long as any of the other messages are active.

Input/Output Box

Alarm Debounce Time – (Inputs only) Enter a delay time in milliseconds that the system will wait to sample this terminal’s Supervised Input Point Circuits. The default is 20 msec. This improves system performance by ignoring a circuit disturbance, such as a door jiggle as it closes, rather than reporting an alarm.

Log Output Status Message – (Outputs only) Not available for legacy or S321 panels. Select this check box to send output relay messages from the panel to the P2000 Server (whether or not access is granted). Must be selected to show as active on the System Status window. This option must be disabled if the output point is to be assigned to an elevator or cabinet.

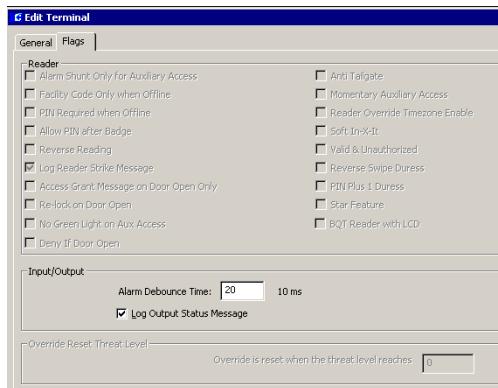
For example:

To Create an I/O Terminal:

1. From the System Configuration window, select the panel to which the I/O terminal will be added.
2. Select the terminal to which you wish to add input points and click **Add**. The Edit Terminal dialog box opens.



3. Enter a descriptive name for the terminal. In the example, we created Whse I/O8 and under Type, selected both **Input** and **Output** to indicate an I/O-8 board.
4. Enter the physical address for this terminal.
5. Click the **Flags** tab.



6. Enter an **Alarm Debounce** time.
7. Select **Log Output Status Message** if you want the status of the outputs to display in the Real Time List and the System Status window.

Override Reset Threat Level Box

Each reader terminal defined for a CK7xx (version 2.4 or higher) or S321 panel can be configured with an Override Reset Threat Level ranging between 0 and 99. A value of 0 disables the “Override Reset” feature; a value between 1 and 99 invokes the following behavior:

Whenever a terminal’s Security Level reaches or exceeds the terminal’s Override Reset Threat Level, all time zone based overrides, host initiated overrides and entity overrides are immediately disabled. Subsequent attempts to invoke host initiated overrides or entity overrides will be denied.

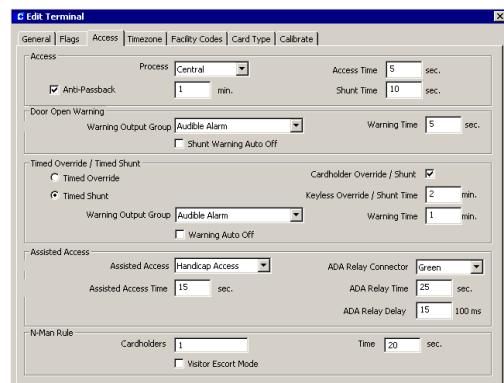
Once a terminal’s Security Level drops below the terminal’s Override Reset Threat Level, the

time zone based override is restored immediately. Host initiated overrides and entity overrides are not automatically restored, but subsequent attempts to invoke host initiated overrides or entity overrides will be granted, provided the configuration allows these overrides.

The System Override feature is not affected by the Override Reset Threat Level, and will remain in effect as long as the panel’s System Override flag is set.

Access Tab

The Access tab defines the terminal’s operating mode, and the access parameters and overrides allowed at the terminal.



Access Box

Process – Select one of three operating modes from the drop-down list.

- **Local** – Access decisions for this terminal are made at the panel level. Must be selected for readers assigned to elevators or cabinets.
- **Central** – Access decisions for this terminal are made at the Server.
- **Shared** – Access decisions are first requested at the panel; if the badge record is not stored at the panel, the access request is passed on to the Server.

For more information on system performance and operating process modes, see “Communication Modes” on page 6.

Anti-Passback – Select Anti-Passback if this reader is an anti-passback reader. Enter a time in minutes that a badge used at the reader is invalid before it can be used at the same or any other anti-passback reader.

Access Time – Enter a time in seconds that the door strike is energized after each valid badge access request. The maximum value is 25 seconds.

Shunt Time – Enter a time in seconds that the door open alarm is suppressed after a valid badge access request. The shunt time should be longer than the access time. The maximum value is 255 seconds.

Note: *After an access grant, the shunt time is cancelled once the door status changes to locked and closed, even if the shunt time has not yet expired.*

Door Open Warning Box

Warning Output Group – Select the output group from the drop-down list that is to be activated when the Warning Time is reached.

Warning Time – Enter the time in seconds (0 to 255) before the Shunt Time expires for the Warning Output Group to be activated if the door remains open.

Shunt Warning Auto Off – If enabled, the Warning Output Group is reset when either the door is closed, access is granted, or the door is overridden. Therefore, the Door Open Warning will be deactivated when there is no Propped Door alarm in the immediate future.

Timed Override/Timed Shunt Box

With S321 and CK7xx panels version 2.2 and higher, the Local Override feature of previous releases can be configured to work in two different modes:

Timed Override – If you select this option, both the access time and the shunt time are extended by the number of minutes entered at a keypad reader. Use the Timed Override mode if you want the door to be unlocked for an extended period of time.

Timed Shunt – Available for S321 and CK7xx panels version 2.2 and higher with RDR2 add-on terminals of model number PS201-E or higher. If you select this option, only the shunt time is extended by the number of minutes entered at a keypad reader. The access time remains at the configured value. Use the Timed Shunt mode if you want the door to be held open for an extended period of time, but do not want the door to be unlocked for that time.

Note: *The Timed Shunt mode is only available if the RDR2 is of model number PS201-E or higher. If not, the Timed Shunt mode will work identically to the existing Timed Override mode. For specific instructions, refer to the CK7xx release 2.2 or higher documentation.*

Timed Overrides/Shunts only work if the following two conditions are met: the presented badge must be associated with an Access Profile that has the Override option enabled, and the Cardholder Override/Shunt option is enabled in this tab.

The Timed Override/Anti-Tailgate option in the Edit Panel dialog box applies equally to Timed Overrides and Timed Shunts.

Cardholder Override/Shunt – If enabled, an authorized entity may temporarily override the

shunt time and/or access time by performing a badging procedure at a keypad reader. The timed override/shunt establishes an extended shunt time and/or access time period from 0 to 1440 minutes (24 hours). The entity's badge must be associated with an Access Profile that has the Override flag set in Privilege Security Roles. Follow these instructions to perform a timed override/shunt access at a keypad:

1. Enter your **PIN code** on the keypad (if PIN codes are part of your system configuration).
2. Press the <*> key (or <*> 0 if the Star Feature is selected in the Flags tab).
3. Enter the number of minutes desired for the override/shunt period.
4. Press the <#> key.
5. Badge into the keypad reader, so that the override/shunt privilege can be checked against the badge record.
6. To terminate the timed override/shunt period (before the number of minutes selected have run out), repeat steps 1 through 5, entering 0 minutes in step 3.

For details refer to *Appendix G: Using a Keypad Reader on CK721/720/705 Panels*.

Keyless Override/Shunt Time – Available for S321 and CK7xx panels version 2.2 and higher. Instead of having to enter the number of minutes for the timed override/shunt at a keypad reader, you can have the system do it for you. Entering a time from 1 to 1440 minutes into this field treats a qualifying badging procedure as if the number of minutes had been entered at the keypad. You can still choose to enter a different number of minutes at the keypad reader, which will take priority over the configured override/shunt time. Entering a 0 into the Keyless Override/Shunt Time field turns this feature off. The rules as to who can invoke a keyless timed override/shunt are

identical to those governing the keypad invoked override.

Warning Output Group – Select the output group from the drop-down list that is to be activated when the timed override/shunt expiration for this terminal falls within the time set in the Warning Time field.

Warning Time – Enter the time (0 to 10 minutes) to activate the Warning Output Group to warn operators that the override/shunt is about to expire. For example, if you have created a temporary door override/shunt for 8 hours, you can create an audible output group that will activate 10 minutes before the override/shunt expires to let operators know the door will shortly begin operating in normal mode.

Warning Auto Off – If enabled, the Warning Output Group is reset when the door closes or when override is extended past the point when the warning should be triggered. Just an access grant alone does not deactivate the Override Warning. This feature is most useful in connection with the Timed Override/Anti-Tailgate option enabled. If Timed Override/Anti-Tailgate is not enabled, it is possible that the Override Warning is deactivated before the override actually expires. If you want to avoid this scenario, disable this option.

Assisted Access Box

Note: *The Assisted Access feature is only available if the RDR2 is of model number PS201-E or higher. If not, the Assisted Access will work identically to the regular Access mode. In addition, this feature only works on terminals that operate in Local mode.*

Enter the information in this box only if you are configuring S321 or CK7xx panels version 2.2 and higher with RDR2 add-on modules of model number PS201-E or higher. The

Assisted Access box allows you to set up a door's access time to be different, to satisfy the requirements for assisted access according to ADA (Americans with Disabilities Act). The system provides three Special Access flags, A, B, and C, which can be renamed according to your facility needs, and then assigned to entities that require special access at a door. For more information, see "Security Roles" on page 127.

Additionally, you may activate an ADA relay in conjunction with the granting of assisted access.

Assisted Access – Select from the drop-down list one of the following options:

- **Never** – Assisted Access is not available at the door, even if the entity's Access Profile has the Special Access "A" flag enabled.
- **Always** – The door will always be opened for the Assisted Access Time, regardless if the entity's Access Profile has the Special Access "A" flag enabled.
- **Special Access A** – The door will be opened for the Assisted Access Time, only if the entity's Access Profile has the Special Access "A" flag enabled. If the Special Access "A" flag has been renamed, that name will display here.

Assisted Access Time – Enter the amount of time in seconds (1 to 120) that the door will remain unlocked to provide access time to entities with special needs. The assisted shunt time will exceed the assisted access time by the same amount that the regular shunt time exceeds the regular access time.

ADA Relay Connector – In case an output on an S300 I/O terminal is not available to drive an ADA relay, you may use either one of the two outputs that are available on an RDR2 module. Select from the drop-down list the RDR2's connector that will be activated for the ADA

Relay time when assisted access is granted. Choices are:

- **Green** – if the ADA relay is connected to the RDR2 connector that normally drives the green light.
- **Shunt** – if the ADA relay is connected to the RDR2 connector that normally indicates the shunt condition.
- **None** – if the ADA relay is not connected to any RDR2 connector.

Note that when connecting the ADA relay to either one of these outputs, its regular function, such as activating the green light or indicating the shunt condition, is no longer available. Also, see the S321 or CK7xx documentation about wiring procedures.

ADA Relay Time – Enter the amount of time in seconds (1 to 120) that needs to elapse after an assisted access grant before the ADA Relay Connector will be deactivated. The ADA Relay time therefore specifies the time the ADA relay is activated minus any ADA Relay Delay.

ADA Relay Delay – Enter the amount of time (0 to 30 units of 100 milliseconds) that needs to elapse after an assisted access grant before the ADA Relay Connector will be activated. This may be necessary to avoid operating the door-opening device before the door is fully unlocked.

N-Man Rule Box

Available for CK7xx and S321 panels. This option provides additional security measures for specific access-controlled readers at your facility. The N-Man Rule is based on a team of entities who must present their badge as a group within a defined period of time to gain access at an N-Man Rule defined reader. For this option to work, the terminals are required to operate in Central mode.

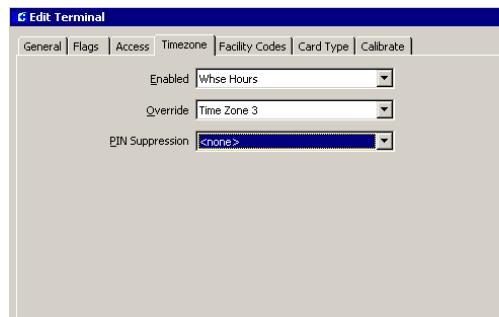
Cardholders – Enter the number of entities who must badge as a unit when entering an N-Man Rule controlled-reader.

Time – Enter the time in seconds during which the number of entities in the team are required to present their badge.

Visitor Escort Mode – If enabled, a visitor can gain access after badging at an N-Man Rule defined reader, as long as the visitor's sponsor presents the badge after the visitor. If this option is selected, the default number in the **Cardholders** field will be 2.

Timezone Tab

The Timezone tab defines the time zones in which this terminal will operate. Panel Time Zones must be set up before they will display in drop-down lists.



Enabled – Select a time zone from the drop-down list that will be in effect for this terminal.

Override – Select a time zone from the drop-down list that can be set as an override for this terminal. This field is available if Reader Override Timezone Enable is selected in the Flags tab.

PIN Suppression – Select a time zone from the drop-down list during which entities do not have to enter a PIN number.

Facility Codes Tab

Available for CK7xx panels. Enter a Facility Code and corresponding card type for each group of cards that will use this terminal. You may enter up to 12 different facility codes. Facility codes must be entered consecutively. When a facility code is 0, the following codes are ignored. See “Misc Tab” on page 55 to assign facility codes to S321 panels.

Edit Terminal					
General	Flags	Access	Timezone	Facility Codes	Card Type
1	468			Wiegand	7
2	468			N-Crypt	8
3	0				9
4	0				10
5	0				11
6	0				12

Card Type Tab

Select the type of card that will be used at this reader. If the reader is disabled, the Card Type should be set to “No Card Allowed.” HID Corporate 1000 works offline (using the *Facility Code Only when Offline* option), as long as the Binary BaFe card type is also selected.

Edit Terminal					
General	Flags	Access	Timezone	Facility Codes	Card Type
<input type="checkbox"/> No Card Allowed	<input type="checkbox"/> BCD BaFe				
<input type="checkbox"/> Standard Wiegand	<input type="checkbox"/> 26-bit Wiegand Inverted				
<input type="checkbox"/> Encrypted Wiegand	<input type="checkbox"/> Eyecam, Prox, Indala				
<input type="checkbox"/> Binary BaFe	<input type="checkbox"/> PIN + Card ID				
<input type="checkbox"/> Mag Stripe	<input type="checkbox"/> 26 bit Sensor Forward				
<input type="checkbox"/> Invert Data	<input type="checkbox"/> 26 bit Sensor Reverse				
<input type="checkbox"/> PIN Only	<input type="checkbox"/> 32 bit Motorola				
<input type="checkbox"/> Card ID	<input type="checkbox"/> Custom				
<input type="checkbox"/> HID Corporate 1000					
Custom Card Formats					
<input type="checkbox"/> 64 bit Wiegand	<input type="checkbox"/> Not Present				
<input type="checkbox"/> 64bit Wiegand Reverse	<input type="checkbox"/> Not Present				
<input type="checkbox"/> Not Present	<input type="checkbox"/> Not Present				
<input type="checkbox"/> Not Present	<input type="checkbox"/> Not Present				

The Custom Card Formats box displays the card formats that were downloaded into the

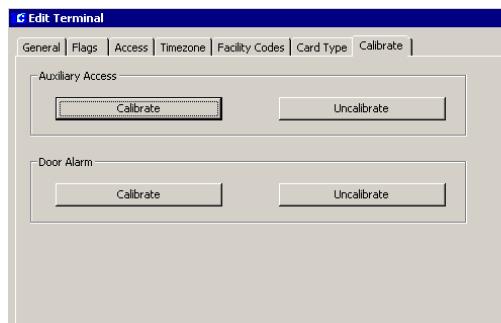
panel, using the Panel Card Formats dialog box, see page 58 for detailed instructions.

Only one type of card should be selected, with two exceptions:

- In addition to a non-PIN based card type you may check the PIN + Card ID check box. This gives people who have forgotten their badge the opportunity to get access by keying-in their badge number and their PIN. See the description of PIN Codes on page 70.
- If you use a two-wire reader with a keypad, you must wire the Data 0 and Data 1 wires so that the keypad produces the correct input to the panel. If this configuration causes the badge data to be reported inversely, you can check the “Invert Data” check box to inverse just the badge data, so that the panel can correctly interpret both the keypad data and the badge data.

Calibrate Tab

Use this tab to calibrate auxiliary access input point contacts on the terminal, as well as door contact input points. Available only on inputs of the S300-DIN-RDR2S module connected to CK7xx panels, version 2.2 and higher.



To calibrate or uncalibrate the auxiliary access, you must define a Propped Door (24) input point. After the calibration command has been

successfully issued, input point 24 can be deleted if it is not being used.



During the entire input calibration procedure, the input's contact must be physically closed. Otherwise, the input's status will be unreliable.

If you click either of the **Calibrate** buttons, the Server will send a calibration command to the panel, the panel then forwards the command to the S300-DIN-RDR2S to initiate the input's calibration. When the S300-DIN-RDR2S completes its calibration, typically within a few seconds, the panel will send a transaction message to the Real Time List indicating the calibration result. After a successful calibration, four-state input statuses will be available for the input point.

If you click either of the **Uncalibrate** buttons, the Server will send a command to the panel to uncalibrate the S300-DIN-RDR2S input. The panel will then send a transaction message to the Real Time List indicating the uncalibration result. After the uncalibration, four-state input statuses will no longer be available for the input, only two-state statuses.

Note: Once you perform a calibration procedure on an input, you should not use this feature again, unless you change the controller hardware or the input point's wiring.

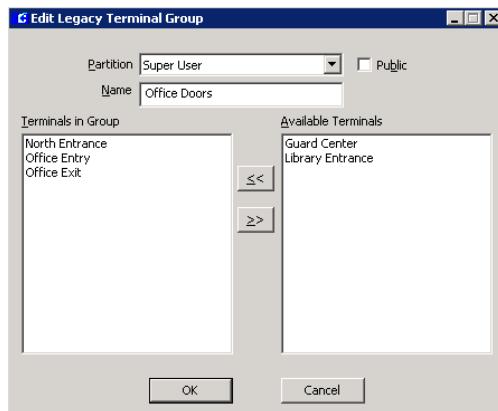
Create Terminal Groups

You can group terminals that have common access throughout your facility and then apply them as a group rather than individually to the various functions. For example, you may have ten terminals (readers) with access to an office area. When grouped together, you can assign entities that should have access to that area to the “Office Doors” group, rather than assigning all ten terminals to the entities individually.

Terminal Groups may also be used to define events. Using the office example, the “Office Doors” group can be associated with an entity and an event to trigger the lights to come on no matter which door the entity uses.

To Create a Terminal Group:

- From the System Configuration window, click the plus (+) sign next to the root **Terminal Groups** icon to display the root terminal group types.
- Select one of the following options:
 - Legacy Terminal Groups** – To group S321, CK720, CK721, and CK705 terminals.
 - ACO Terminal Groups** – To group CK722 Access Control objects (defined using the SCT tool), plus any of the above legacy terminals.
 - DSO Terminal Groups** – To group CK722 Door Sequence objects (defined using the SCT tool), plus any of the above legacy terminals.
- Click **Add**. The corresponding Edit Terminal Group dialog box opens.



- If you use Partitioning, select the **Partition** that will have access to this Terminal Group. All available terminals (for the par-

tition selected) will be listed on the right side of the dialog box.

- If you use Partitioning, select the **Public** check box to allow all partitions to see this Terminal Group.
- Enter a descriptive **Name** for this Terminal Group.
- From the **Available Terminals** list, click the terminal you wish to include in your group.
- Click **<<**. The terminal moves to the left side of the dialog box, to be included in the **Terminals in Group** box.
- To remove a terminal from the **Terminals in Group** box, select the terminal and click **>>**.
- When all terminals you wish to include in the group have been moved to the **Terminals in Group** box, click **OK**. A Terminal Group icon for the new group will be added under the corresponding Terminal Groups icon in the System Configuration window.

In the example, “Office Doors” has been added as a new terminal group.



Configure PIN Codes

Note: This section applies to CK720, CK721, CK705, and S321 panels. To configure CK722 panels and related components, refer to the System Configuration Tool (SCT) Manual and to the CK722 Commissioning Guide.

There are three different ways of using PINs to get access at a reader. These ways are called “PIN Only,” “PIN + Card ID,” and “PIN.” In configurations that require presenting a badge to request access, it is possible to add the mode “PIN + Card ID” as an alternative for people who have forgotten their badge.

Refer to *Appendix G: Using a Keypad Reader on CK721/720/705 Panels* for further instructions.

PIN Only

In “PIN Only” mode all it takes for the system to identify a person is entering a PIN at a reader. Given a fixed scramble mode, an algorithm produces a unique PIN for every badge number between 1 and 32767. When a PIN is entered at the keypad, the algorithm calculates the corresponding badge number and the access decision is made based on that badge’s access rights. This feature works with 5-digit algorithmic PINs only.

For “PIN Only” to work, you need to configure the following parameters:

1. The panel’s **PIN Code Type** must be set to **Algorithmic** (see page 54).
2. The panel’s **PIN Code Digits** must be set to “5” (see page 54).
3. The panel’s **Scramble Mode** must be set to the value used to create the PINs from the badge numbers (see page 54).
4. The terminal’s **PIN Only** card type must be selected in the Card Type tab. All other card types must not be selected (see page 68).
5. The terminal’s **Allow PIN after Badge** in the Flags tab has no effect (see page 61).
6. The terminal’s **PIN Suppression** in the Timezone tab has no effect. For obvious reasons you cannot waive the requirement to enter a PIN in “PIN Only” mode.

To use “PIN Only” mode, simply enter your 5-digit algorithmic PIN at the keypad followed by the # key, and the access decision will be made.

PIN + Card ID

In this mode the badge does not have to be presented at the reader. The numeric keypad is used to enter the PIN and the badge number. This feature works with 4 or 5-digit algorithmic and with 4 or 5-digit custom PINs.

For “PIN + Card ID” to work, you need to configure the following parameters:

1. The terminal’s **PIN + Card ID** must be selected in the Card Type tab. All other card types should not be selected, unless you want to use the “PIN + Card ID” mode only as an alternative for people who have forgotten their badge (see page 68).
2. The terminal’s **Allow PIN after Badge** in the Flags tab has no effect (see page 61).
3. The terminal’s **PIN Suppression** in the Timezone tab has no effect, i.e., you cannot use time zones to waive the requirement to enter a PIN in “PIN + Card ID” mode.

To use “PIN + Card ID” mode, you must enter your PIN followed by your 5-digit badge number followed by the # key. You must enter leading zeros if your badge number has fewer than 5 digits.

PIN

In this mode the PIN needs to be entered in conjunction with a valid badge presented at the reader. This feature works with 4 or 5-digit algorithmic and with 4 or 5-digit custom PINs.

For “PIN” to work, you need to configure the following parameters:

1. Select a card type in the terminal's Card Type tab that matches the reader's technology (see page 68).
2. All other card types should not be selected.
3. The terminal's **PIN Only** card type in the Card Type tab must not be selected.
4. The terminal's **PIN + Card ID** card type in the Card Type tab should not be selected, unless you want to use the "PIN + Card ID" mode as an alternative for people who have forgotten their badge.
5. The terminal's **PIN Suppression** in the Timezone tab must be set to a defined time zone. PINs are only required to be entered when the time zone is inactive.

To use "PIN" mode when the terminal's **Allow PIN after Badge** option in the Flags tab is not set, you must key in the entire PIN before presenting the badge. The PIN does not need to be terminated with a # key.

To use "PIN" mode when the terminal's **Allow PIN after Badge** option in the Flags tab is set, the PIN must be terminated with a # key. You can enter the PIN and the # key before, during, or after the badge is presented.

To use "PIN" mode when you also have the **PIN + Card ID** card type selected, as an alternative for people who have forgotten their badge, the # key must not be entered before the badge is presented.

Four-Digit PINs

A four-digit custom PIN is defined by the first four digits entered in the **PIN Code** field in the Identifier tab (see page 142). Algorithmic codes need to be requested from Technical Support.

PIN Duress

The PIN Duress feature in the Soft Alarm dialog box, creates an access grant and a duress alarm only if all of the following conditions apply:

1. The duress soft alarm is defined at the panel (see page 86).
2. The entity is required to enter a PIN at the terminal.
3. Exactly one digit of the PIN is replaced by the digit 9.
4. All other digits match the badge's PIN.
5. The card type selected in the terminal's Card Type tab is not "PIN Only."

PIN Retry Alarm

A PIN Code Retry alarm is generated when the respective soft alarm is defined at the panel, and three consecutive unsuccessful attempts to enter a PIN were made for the same badge (see page 86). In Local mode, the three consecutive attempts can be made at any terminal of a single panel. In Central mode, the three consecutive attempts can be made at any terminal at any panel.

Create Input and Output Points and Groups

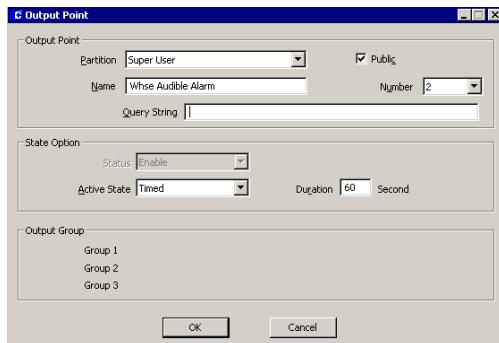
Input and output points and groups work together to control devices connected to the system terminals. For example, an *input* can be configured for a broken window contact and this can generate an *output* to an alarm annunciation. A group of inputs can generate the same output, no matter which input point in the group is activated.

Create Output Points and Groups

Output Points are dry contact relays located on the Terminal boards. These are opened or closed by the system to control devices connected to them such as lights, air conditioning, alarm annunciations, parking barriers, and so on. After output points are created, they can be grouped with other output points that have a common purpose in the system and then used in conjunction with specific inputs.

To Create Output Points:

1. From the System Configuration window, select a Terminal that has been configured for output.
2. Click the **Output Points** icon and click **Add**. The Output Point dialog box opens.



3. If this is a partitioned system, select in the Output Point box the active **Partition** and check **Public** if you wish the output point to be visible to all partitions.
4. Enter a descriptive **Name** for the output point. (In the example, the name is Whse Audible Alarm.)
5. Select an output point **Number** from the drop-down list. This number represents the physical connection to the I/O terminal.
6. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 103), and is also used with

the P2000-Metasys option (refer to “Configuring Hardware Components for BACnet Interface” on page 237).

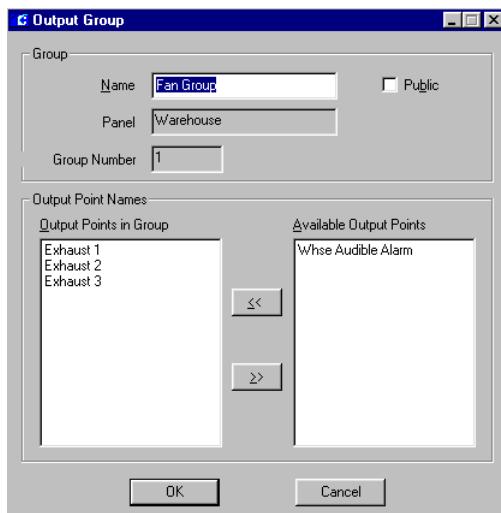
7. If this is an S321 output point, select Disable from the **Status** drop-down list to use the default S321 output point functionalities. Select Enable to define this output point as any general output point.
8. In the **State Option** box, select the **Active State** from the drop-down list. See the following definitions:
 - Reset** – Reserved for diagnostic purposes.
 - Set** – Turns on the output point. This option must be selected for output points assigned to elevators or cabinets.
 - Fast Flash** – Toggles the output point on and off quickly (once per second).
 - Slow Flash** – Toggles the output point on and off slowly (once per two seconds).
 - Timed** – Turns on the output point for a specified time in seconds.
9. If the Active State is **Timed**, you must enter a **Duration** in seconds.
10. The Output Group box is view-only. Each output point can belong to three output groups.
11. Click **OK** to save your settings. The new output point will be listed under the Output Points icon.

To Create Output Groups:

Output Points can be grouped together to perform common functions. For example, an input such as an air sampling device can be configured to activate a group of exhaust fans connected to output points on a terminal.

1. From the System Configuration window, click the Panel in which the terminals for the output group are installed.

- Select the **Output Groups** icon and click **Add**. The Output Group dialog box opens.



- In the Group box, enter a **Name** for the Output Group.
- The Panel field displays the name of the Panel selected.
- The Group Number field displays the number that is automatically assigned when you create an output group.
- If your system is partitioned, select the **Public** box if you wish this group to be visible to all partitions.
- In the Output Point Names box, select an **Output Point** from the list of Available Output Points.
- Click **<<** to move the Output Point to the list of Output Points in Group.
- Continue to move available output points from the "Available" list to the "Group" list until all output points you wish to include are in the Output Points in Group box.
- To remove an output point from the Output Points in Group box, select the output point and click **>>**.

- Click **OK** to save your settings. A new Output Group icon will be listed under the root Output Groups icon for the panel.

Create Input Points and Groups

Input points can be physical connections to monitored devices such as a window or door contact, or a motion detector. They can be software alarms that are reported to the system, and can be connected to alarm popups and instruction text. They can also trigger an event or an output device.

Create Input Points

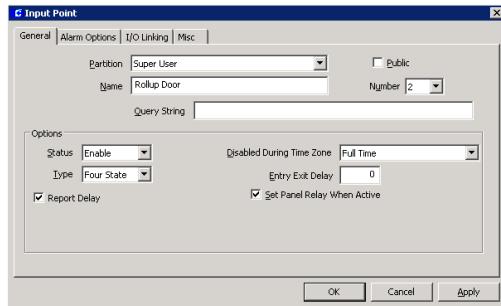
After the terminal is created, the Input Points icon is added under the terminal. From here you create the input points for the terminal. (If you need more information, refer to "Create and Configure Terminals" on page 58.)

To Create Input Points:

- From the System Configuration window, select a Terminal that has been configured for inputs.
- Click the **Input Points** icon (under the Terminal icon) and click **Add**. The Input Point dialog box opens at the General tab.
- Enter the information in each tab, as described in the following "Input Point Field Definitions."
- Click **OK** to save your settings and return to the System Configuration window. A new Input Point icon will be listed under the root Input Points icon. When you click on the new input point, the settings will display on the right windowpane.

Input Point Field Definitions

General Tab



Partition – If you use partitions, select the appropriate Partition that will have access to this input point.

Public – If you use partitions, click the Public check box if you want this input point to be visible to all partitions.

Name – Enter a descriptive Name for the input point.

Number – Select an input point number from the drop-down list.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 103), and is also used with the P2000-Metasys option (refer to “Configuring Hardware Components for BACnet Interface” on page 237).

Status – If you select Enable, all input point changes of state are reported. Select Disable if you do not want these changes reported.

Disabled During Time Zone – Select a Time Zone during which the input point will be disabled. For example, it is impractical to report a door contact alarm during business hours when the door is in constant use.

Type – Choose either Two State or Four State.

Entry Exit Delay – Enter a time (0 to 600 seconds) that the alarm will be suppressed until an event disables the alarm. If a delayed entry/exit value is defined for an input point, the system will delay reporting activation of this input point for the time value specified. If the input point is suppressed within this delay period (that is, by a card event), the alarm will not be reported. For example, an entity can badge at a reader, open the door, and then badge at a second reader to suppress the door alarm before it reports. If the entity does not badge and suppress the alarm (by card event) at the second reader within the specified time, the alarm will be reported.

Report Delay – If enabled, the alarm is delayed by the number of seconds set in the Reporting Delay field in the Alarm tab of the Edit Panel dialog box. If the input point returns to the secure state before the delay expires, the panel will not report the alarm to the Server at all. If disabled, the alarm is reported immediately. Open and short conditions for 4-state input points are reported immediately.

Set Panel Relay When Active – If enabled, the relay on the panel activates when the input point is activated. If disabled, the relay on the panel does not activate. Not available for S321 panels.

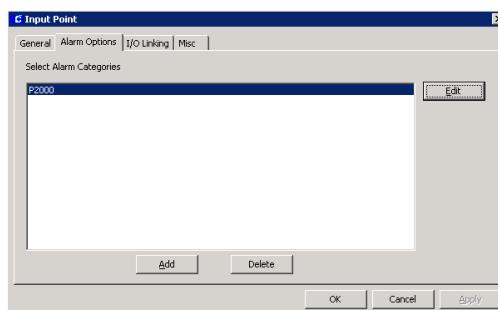
Alarm Options Tab

Use this tab to configure alarm options for P2000 devices that generate alarms, such as input points, cameras, switches, etc. Each alarm must belong to at least one Alarm Category (see “Alarm Configuration” on page 160 for details), but can also be assigned to multiple alarm categories, each with its own set of alarm options.

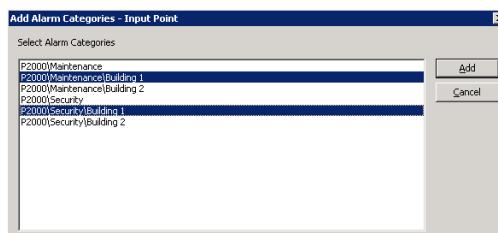
For example, if an input point connected to a glass breakage sensor generates an alarm, the P2000 system may create two separate alarms

for two configured alarm categories: P2000\Maintenance\Building 1 and P2000\Security\Building 1. Typically, a single operator is configured to receive only a single category of alarms, and therefore would only receive a single alarm. However, higher level operators such as supervisors, or an operator at a central alarm monitoring location, may be configured to receive both of these alarms.

1. Click the **Alarm Options** tab. The **P2000** Alarm Category will display by default.



2. To assign this alarm to other alarm categories, click the **Add** button. The Add Alarm Categories dialog box appears displaying all previously created alarm categories (see page 160 for details).

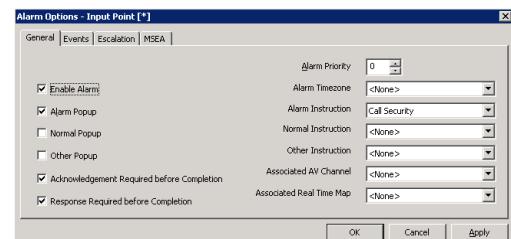


Note: If you use the Enterprise option, the Alarm Categories defined for all P2000 sites within an Enterprise system will be listed.

3. Select one or more categories and click the **Add** button. The list will display all the selected alarm categories.

4. To remove a category from the list, select the alarm category and click **Delete**.
5. Once you have all the alarm categories you want to assign to this alarm, select an alarm category from the list and click **Edit** to edit the alarm options. You can select and edit more than one category at a time. The Alarm Options dialog box opens displaying the General tab. Refer to the following definitions.

General Tab



Alarm Priority – Enter a value from 0 to 255. Zero equals the highest priority. This is the order in which the alarm message will be placed in the alarm queue. If alarm messages have the same alarm priority, the date and time determine which alarm is positioned higher in the queue.

Enable Alarm – If selected, the alarm is added to the alarm queue and displayed in the alarm monitoring window to notify the operator of its activation. Leave this selection disabled if the item is unrelated to alarm monitoring. For example, you can enable an alarm for a “Maintenance” alarm category and disable the same alarm for a “Security” alarm category.

Alarm Timezone – Select from the drop-down list the time zone during which the alarm upon activation will be reported in the Alarm Monitor window. If you select <None>, the alarm will be reported at any time once it is activated.

Alarm Popup – When you enable Alarm Popup for an alarm, the Alarm Monitor window automatically displays in front of all other windows on the screen whenever the alarm is in the alarm state. If disabled, the alarm is simply entered in the alarm queue.

Alarm Instruction – Select from the drop-down list the Instruction Text that will display in the Alarm Response window when the alarm is in the alarm state. The Alarm Response window will display a set of instructions related to that particular alarm.

Note: Before you can assign instruction text to the various popups, you must first create instruction text. See “Creating Instruction Text” on page 82 for more information.

Normal Popup – When you enable Normal Popup for an alarm, the Alarm Monitor window automatically displays in front of all other windows on the screen whenever the alarm enters its normal state.

Normal Instruction – Select from the drop-down list the Instruction Text that will display in the Alarm Response window when the alarm enters its normal state. The Alarm Response window will display a set of instructions related to that particular alarm.

Other Popup – When you enable Other Popup for an alarm, the Alarm Monitor window automatically displays in front of all other windows on the screen whenever the alarm is in a state other than “alarm” or “normal.”

Other Instruction – Select from the drop-down list the Instruction Text that will display in the Alarm Response window when the alarm enters a state other than “alarm” or “normal.”

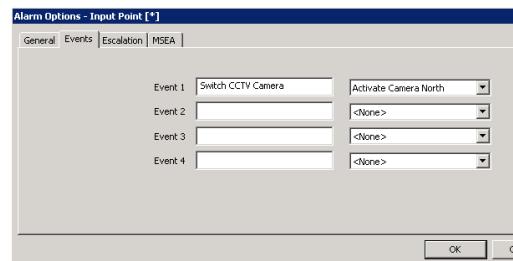
Acknowledgement Required before Completion – Select this check box to require acknowledgement of this alarm before its completion.

Response Required before Completion – Select this check box to require response to this alarm before its completion.

Associated AV Channel – If your facility uses the DVR option, select the camera to be associated with this alarm. If applicable, this selection will override the selection made in the Input to camera mapping window.

Associated Real Time Map – Select the Real Time Map to be associated with this alarm. If applicable, this selection will override the default behavior of the Real Time Map containing the alarm. That is, when you click the Map button in the Alarm Monitor, the associated Real Time Map will display, even if it is different from the Real Time Map containing the alarm.

Events Tab



Event 1-4 – You can define up to four events that can be triggered from the Alarm Monitor window whenever the alarm goes into an alarm condition and is entered into the alarm queue. Enter a descriptive Event name and select a previously configured Event from the associated drop-down list, see “To Activate an Event from the Alarm Monitor:” on page 167.

Escalation Tab

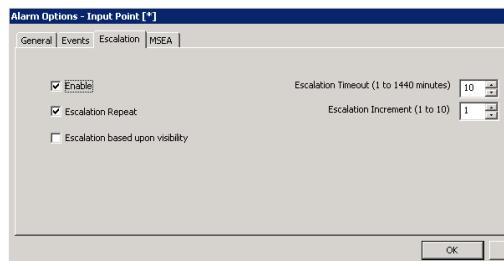
The alarm escalation function constantly monitors all generated alarms that have their escalation options enabled. Escalation level value range is from 0 to 10, where 0 indicates a non-escalated alarm.

The alarm escalation feature provides for two different conditions when an alarm may be escalated:

- If an alarm is generated for a specific alarm category and there are currently no operators logged on to the P2000 system that have privileges to receive alarms for that category.
- If an alarm is generated and remains pending for the configured escalation timeout period.

If either of these conditions occurs, that alarm will be regenerated with an elevated escalation level. The escalation level will be incremented by the configured escalation increment value. This process may be repeated multiple times until a high enough escalation level is reached that matches the privileges of a currently logged on operator. If no operators are logged on to the P2000 system, the alarm will be regenerated until the maximum escalation level is reached, and then no further action will be taken.

After an escalated alarm has been completed, the next occurrence of that alarm is created with no escalation level.



Enable – Select this check box to enable alarm escalation.

Escalation Repeat – Select this check box to allow for escalation to occur more than once for the alarm. For example, if the Escalation Timeout is set to 30 minutes, and the Escalation Increment is set to 2, every half an hour the escalation value for alarms remaining in pending state will go up by 2 until it reaches the maximum value. If this check box is not selected, escalation can occur only once for this alarm.

Escalation based upon visibility – When this check box is selected, the alarm will be immediately escalated by a defined increment if, at the time of occurrence, no operator able to receive alarms from this Alarm Category is logged on.

Escalation Timeout (1 to 1440 minutes) – Enter the time period (in minutes) after which an alarm remaining in pending state will be escalated by the Escalation Increment.

Escalation Increment (1 to 10) – Enter the value by which to escalate an alarm each time the escalation takes place.

MSEA Tab

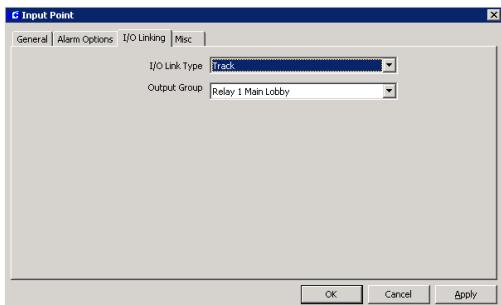
In facilities that use the Metasys System Extended Architecture (MSEA) option, this feature allows an alarm that is forwarded to MSEA to contain an embedded reference to a MSEA Graphic. For more information, see “Defining MSEA Graphics” on page 239.



Select from the drop-down list the **MSEA Graphic** to reference in this alarm. When an alarm is received and displayed by Metasys, the Metasys operator can simply click the alarm to display the graphic item associated with the alarm and the item that caused the alarm.

I/O Linking Tab

Use the I/O Linking tab to link I/O Types to specific output groups. You must define output groups in the Output Group dialog box before you can use this function. See “Create Output Points and Groups” on page 73 for detailed information.



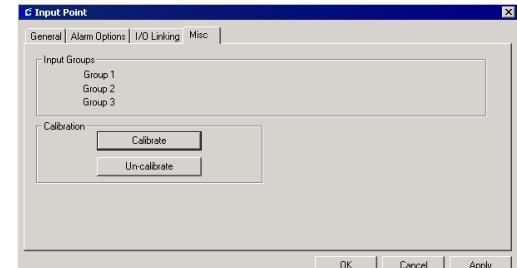
I/O Link Type – Select the appropriate link type from the drop-down list. Select one of the following choices:

- **None** – Default selection, indicating that there is no linkage between the input point and output group.

- **Active-on** – When the input point is activated, the output group activates.
- **Secure-on** – When the input point is secure, the output group activates.
- **Track** – When the input point is activated, the output group activates. When the input point is secure, open, or short, the output group deactivates.
- **Mimic** – When the input point is activated, open, or short, the output group activates. When the input point is secure, the output group deactivates.
- **Active-off** – When the input point is activated, the output group deactivates.
- **Secure-off** – When the input point is secure, the output group deactivates.
- **Reverse Track** – When the input point is activated, open, or short, the output group deactivates. When the input point is secure, the output group activates.

Output Group – Select from the drop-down list the Output Group to which you wish to link.

Misc Tab



Input Groups – If this input point is included in an Input Group, the associated Input Group will display in this box. An input point cannot be included in more than three Input Groups.

Calibration – Available only on inputs of the S321 or S300-DIN-RDR2S module connected to CK7xx panels version 2.2 and higher.



CAUTION
During the entire input calibration procedure, the input's contact must be physically closed. Otherwise, the input's status will be unreliable.

If you click the **Calibrate** button, the Server will send a calibration command to the panel, the panel then forwards the command to the S300-DIN-RDR2S or S321 to initiate the input's calibration. When the S300-DIN-RDR2S or S321 completes its calibration, typically within a few seconds, the panel will send a transaction message to the Real Time List indicating the calibration result. After a successful calibration, four-state input statuses will be available for the input point.

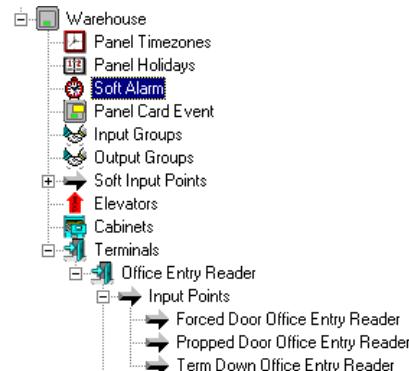
If you click the **Un-calibrate** button, the Server will send a command to the panel to un-calibrate the S300-DIN-RDR2S or S321 input. The panel will then send a transaction message to the Real Time List indicating the un-calibration result. After the un-calibration, four-state input statuses will no longer be available for the input, only two-state statuses.

Note: Once you perform a calibration procedure on an input, you should not use this feature again, unless you change the controller hardware or the input point's wiring.

Configuring Reader Terminal Hardwired Input Points

When a reader terminal is created, three input points are reserved for specific inputs: input points for reader terminal door contact points (these have to be configured in the Soft Alarm window, see “Configure Soft Alarms” on page 86), and an input point for a terminal down input point. In the following example, Input Points “Forced Door Office Entry Reader,” “Proposed Door Office Entry Reader,” and “Term Down Office Entry Reader” were

created for the Office Entry Reader terminal in the Warehouse panel.



Using Reader Terminal Door Contact Input Points

Using the previous example, when the Office Entry Reader was created and “Forced Door, Proposed Door” was enabled in the Edit Soft Alarm window, the system created the Input Points icon with two entries beneath it. The first input point, named “Forced Door Office Entry Reader” in the example, was created for input point 18 (varies, depending on the panel type). The second input point, named “Proposed Door Office Entry Reader” was created for input point 24 (varies, depending on the panel type). You can use these input points as a door contact alarm. If enabled in the Input Point dialog box, these input points will report to the Alarm Queue and Real Time List if the door contact is broken, or if left open longer than the configured alarm suppression for the reader.

To Edit a Reader Terminal Door Contact Input Point:

1. Select the Forced Door or Proposed Door <terminal name> icon under the reader terminal you wish to configure and click **Edit** to open the Input Point dialog box. If Forced Door was selected, input point 18

will display in the Number field. If Propped Door was selected, input point 24 will display in the Number field. These are hardwired to points 18 or 24 on the reader terminal.

2. Enter the information on each tab as you would any other input point.
3. Click **OK** to save your settings and return to the System Configuration window.

Note: *If you rename a terminal that has a Forced Door or Propped Door input point, you must edit the input points to manually enter the new terminal name, as in "Forced Door <terminal name>" or "Propped Door <terminal name>." As an alternative, you could also disable the "Forced Door, Propped Door" in the Soft Alarm window and then enable it again to automatically create the input points under the new terminal name.*

Using the Terminal Down Input Point

When a reader terminal is created in the system, a Terminal Down Input Point is automatically created for input point 25 on the terminal and displays under its input point icon as Term Down <terminal name>. If enabled in the Input Point dialog box, this input point will report to the Alarm Queue and Real Time List. If disabled, the alarm will not report to the Alarm Queue, but will continue to report to the Real Time List.

To Edit a Reader Terminal Down Input Point:

1. Select the Term Down <terminal name> icon under the reader terminal you wish to configure and click **Edit** to open the Input Point dialog box. Input point 25 will display in the Number field. (This is hardwired to point 25 on the reader terminal.)
2. Enter the information on each tab as you would for any other input point.

3. Click **OK** to save your settings and return to the System Configuration window.

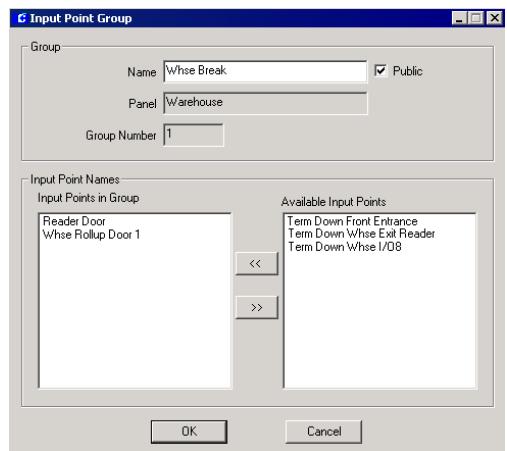
Note: *If you rename a terminal that has a Terminal Down Input Point, you must edit the Terminal Down Input Point to manually enter the new terminal name, as in "Term Down <terminal name>."*

Create Input Groups

Input Points from the same panel can be grouped to perform related functions. For example, motion detectors within a specific area can be grouped together to trigger an alarm or other output when activated. You can create as many input groups as you need; however, an individual input point can be included in no more than three input groups.

To Create an Input Group:

1. In the System Configuration window, select the panel containing the I/O board with the input points you wish to group.
2. From the component icons, click **Input Groups** and click **Add**. The Input Point Group dialog box opens.



3. In the Group box, enter a descriptive **Name** for the Input Group.
4. If your system is partitioned, select **Public** if you wish this group to be visible to all partitions.
5. The **Panel** name will display in the Panel field.
6. The **Group Number** field displays the number that is automatically assigned when you create an input group.
7. In the Input Point Names box, select an Input Point from the **Available Input Points** list (on the right windowpane) and click **<<**. The Input Point is moved to the **Input Points in Group** list (on the left windowpane).
8. Select all the input points you wish to include in the group and move them into the group list until all have been added.
9. To remove an input point from the Input Points in Group box, select the input point and click **>>**.
10. Click **OK** to save your settings and return to the System Configuration window. A new Input Group icon will be listed under the root Input Groups icon for the panel.

Creating Instruction Text

Instruction text can be assigned to input points and other P2000 applications. When any of these elements changes state, an alarm is sent to the Alarm queue and displayed in the Alarm Monitor window. When an operator selects the message for response, the instruction text displays in the Alarm Response dialog box.

You can configure Alarm Instructions with an embedded URL and assign that instruction to an alarm. When the alarm instruction displays in the Alarm Monitor, the user can click the URL and it will launch the Web Browser with

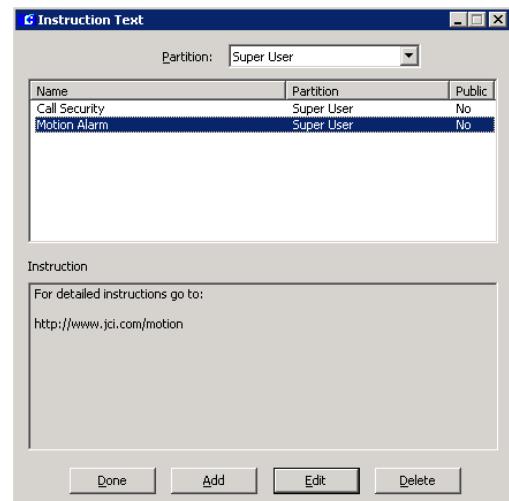
the URL. The alarm instruction detects URLs that begin with the following prefixes:

http:	file:	mailto:
ftp:	https:	gopher:
nntp:	prospero:	telnet:
news:	wais:	

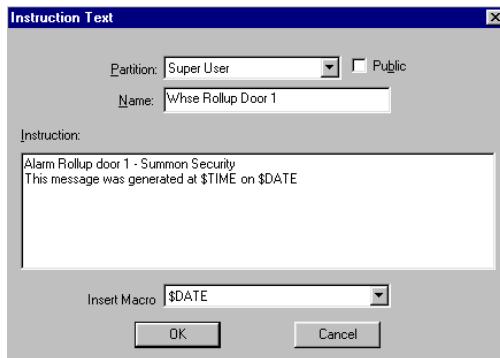
When one of the above URLs are found in the instruction text, Windows will perform its configured default action for the URL. For URLs of “http:” or “https:”, the Web Browser will be launched with that URL. If the URL begins with “mailto:”, Windows will launch your email program. If the URL begins with “file:”, Windows will launch the associated application to view the file.

To Create Instruction Text:

1. From the P2000 Main menu, select **Alarm>Instruction Text**. The Instruction Text dialog box opens.



2. Click **Add**. An instruction entry dialog box opens.



3. If this is a partitioned system, select the appropriate **Partition**, and select **Public** if you want this instruction to be visible to all partitions.
4. Enter the **Name** of the Instruction. This is the name that will display in drop-down lists for selection in P2000 applications that use Instruction Text.
5. Enter the actual instruction text you want to display.
6. If you wish to insert a macro to be part of the instruction text, select a macro from the **Insert Macro** drop-down list. Refer to the following table.

Use Macro....	To Insert...
\$ASCII(xxx)	ASCII Character
\$BADGE_DESCRIPTION	Badge Description
\$BADGE_NUMBER	Badge Number
\$BS	Backspace
\$CARDHOLDER_FIRSTNAME	Entity's First Name
\$CARDHOLDER_LASTNAME	Entity's Last Name
\$CARDHOLDER_NAME	Entity's First <space> Last Name
\$CR	Carriage Return
\$DATE	Today's Date
\$FF	Form Feed
\$INPUT_NAME	Input Name
\$INPUT_NUMBER	Input Number
\$ITEM_NAME	Item Name
\$LF	Line Feed
\$MSG_SUBTYPENO	Message Sub-Type Number

Use Macro....	To Insert...
\$MSG_TYPENO	Message Type Number
\$MSG_XML	P2000 Message in XML format as defined in the P2000 RMS-XML API manual.
\$OPERATOR	Operator Name
\$PANEL_NAME	Panel Name
\$TAB	TAB
\$TERMINAL_NAME	Terminal Name
\$TIME	Current Time
\$UDF_x*	User Defined Field

* The x must be replaced with the UDF order number. This macro is used with Host events, where the triggering message is directly associated with an Entity, such as an Access Grant message.

Note: Do not include macros in Instruction Text that is used in delayed event actions. The information needed for the macros is not available when the action is delayed. See “Creating Actions” on page 208.

7. Click **OK** to save the Instruction Text entry and return to the Instruction Text dialog box. Click **Done**.

Create Panel Card Events

Panel Card Events operate independently from the Server and therefore affect only the Panel for which they are configured. Panel Card Events are particularly useful for panels that operate offline, such as in areas that must remain operable if the network goes down.

Note: Panel Card Events are configured for each panel while “System” events are configured for the Server. For more information on System Events, see “Creating Events” on page 206.

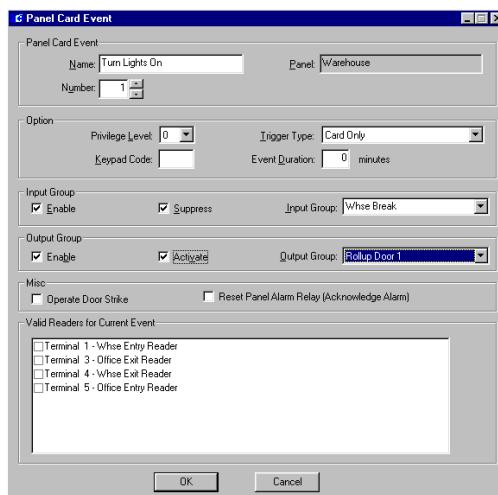
A Panel Card Event is based on badge (trigger) activity and used to suppress or unsuppress an input group, activate or deactivate an output

group, operate a door strike, and/or reset a panel alarm relay.

The following section presents steps to create Panel Card Events. To invoke panel card events using a keypad, refer to *Appendix G: Using a Keypad Reader on CK721/720/705 Panels*.

To Create a Panel Card Event:

- From the System Configuration window, select the panel to which you wish to assign a Panel Card Event.
- Select the **Panel Card Event** icon and click **Add**. The Panel Card Event dialog box opens.



- Enter the information according to the Panel Card Event Field Definitions.
- When all information is added, click **OK** to save your settings and return to the System Configuration window.

Panel Card Event Field Definitions

Panel Card Event

Name – Enter a descriptive event name.

Panel – The Panel name defaults to the panel selected (display only).

Number – Enter an event number from 1 to 20.

Option

Privilege Level – This entry corresponds to the entity's privilege level (from 0 to 7, with 0 being the lowest), assigned through Access Profiles. The entity's privilege level must be equal to or greater than the Privilege Level defined here to initiate the event, see “Access Profiles Tab” on page 138 for more information.

Trigger Type – Indicates the condition that will trigger this card event. Select one of the following:

- **Card Only** – Present badge.
- **Card/PIN Code** – Enter PIN code, then present badge.
- **Card/Keypad Code** – Enter activation or deactivation code, followed by the code specified in the Keypad Code field, then present badge.
- **Card/PIN/Keypad Code** – Enter PIN and activation or deactivation code, followed by the keypad code, then present badge.
- **Any Void Card** – Present any void badge. In this case the card event's privilege level should be set to 0, as void badges do not have any privilege level. For this condition to trigger a card event with a consistent behavior, the terminal should run in local mode. The card event may also be triggered on terminals running on shared or central mode, depending on the generated card message.

- **Special Access Flags** – Select one of the three Special Access flags A, B, or C that will trigger this card event. The system provides three Special Access flags, A, B, and C, which can be renamed according to your facility needs, and then assigned to entities that require special access at a door. For more information, see “Security Roles” on page 127. Special access conditions are set up in the Access tab of the terminal dialog box, see page 66.

Note: If “Allow PIN after Badge” is enabled in the Terminal dialog box, the entity can enter the PIN number after presenting the badge, see page 61 for more information.

Keypad Code – Enter a four-digit keypad code that must be entered to activate or deactivate the event. Deactivating an event can only be accomplished by using a keypad code.

Event Duration – Enter the duration, in minutes that the event will be active (up to 1440 minutes). If the event activates an output group, the output group will be deactivated after this time period. If the event suppresses an input group, the input group will be unsuppressed after this time period. Event duration applies only to event activation, and not to event deactivation. Furthermore, only output group activation and input group suppression may be assigned a duration, but not output group deactivation and input group unsuppression.

Input Group

Enable – Select this box to enable the Input Group Suppression function.

Suppress – Select Suppress to suppress the specific Input Group when this event is activated. Do not select Suppress to unsuppress the specific Input Group when this event is activated. When this event is deactivated, the

selected action is inverted, i.e. an event that suppresses an input group on activation, unsuppresses that input group on deactivation, and an event that unsuppresses an input group on activation, suppresses that input group on deactivation.

Input Group – Select the name of the Input Group that will be suppressed or unsuppressed.

Output Group

Enable – Select this box to enable the Output Group Activate function.

Activate – Select Activate to activate the specific Output Group when this event is activated. Do not select Activate to deactivate the specific Output Group when this event is activated. When this event is deactivated, the selected action is inverted, i.e. an event that activates an output group on activation, deactivates that output group on deactivation, and an event that deactivates an output group on activation, activates that output group on deactivation.

Output Group – Select the name of the Output Group that will be activated or deactivated.

Misc.

Operate Door Strike – If not selected, a valid event invokes the event action only, but does not unlock the door. This setting does not apply to badges with executive privilege. Also, events with trigger type “Any Void Card” never unlock the door.

Reset Panel Alarm Relay (Acknowledge Alarm)

– If selected, the panel alarm relay is reset. Not available for S321 panels.

Note: If a panel card event is created for CK7xx panels and none of the boxes to suppress output points or strike readers are enabled, the panel card event will still show in the Real Time List, as an activated event.

Valid Readers for Current Event

The terminals connected to this panel display in the list. Select those readers that will be used to initiate this card event. If not selected, the terminal will not be affected by the event.

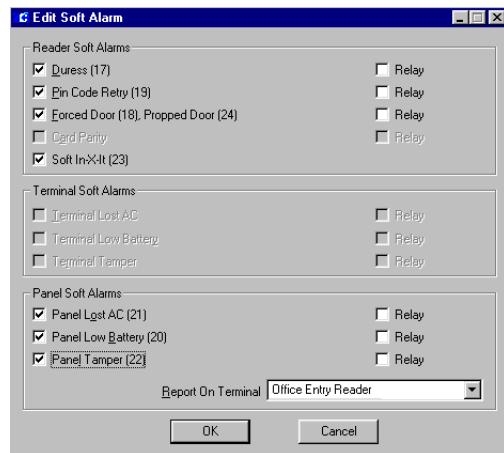
Configure Soft Alarms

Soft alarm points and their addresses are created by the system during installation rather than hardwired to an actual input point. You can enable these soft alarms for Readers, Terminals, or Panels.

The alarm point numbers may be different, depending on the type of panel selected.

To Enable Soft Alarms:

- From the System Configuration window, select the Panel for which you wish to enable soft alarms.
- Select the **Soft Alarm** icon and click **Edit**. The Edit Soft Alarm dialog box opens.
- Select the **Reader**, **Terminal**, or **Panel Soft Alarms** you wish to enable, and select the corresponding **Relay** box to activate the panel relay. See “Soft Alarms Field Definitions” for detailed information.



- Click **OK** to save your settings and return to the System Configuration window.

Soft Alarms Field Definitions

Duress – If enabled, an alarm is generated when an authorized entity reverse-swipes the badge, provided that the terminals’ Reverse Swipe Duress feature is enabled, or substitutes a “9” for one of their PIN code digits. The PIN is used with the badge and grants access to avoid compromising the personal safety of the entity. The panel relay for a duress alarm is only activated when the reader is either in Local mode, or in Shared mode and the panel knows the badge.

PIN Code Retry – When enabled, an alarm is generated when three consecutive invalid PIN codes are entered at a keypad reader.

Note: If you enable the **Relay** box associated with a Duress and/or PIN Code Retry alarm to activate the panel relay, you must also enable the **Latch Output** option on the **Alarm** tab of the **Edit Panel** dialog box, see page 54.

Forced Door/Propped Door – If enabled, a “Forced Door” alarm message will be printed

whenever there is a door open condition without a valid badge read detected first; and a “Propped Door” alarm message will be printed whenever there is a door open condition with a valid badge, but the door is left open past the entry time.

Card Parity – This soft alarm type is not used with CK7xx or S321 panels.

Soft In-X-It – If enabled, the Soft In-X-It overrides the system In-X-It control function for a specified reader and allows entities to gain access at that reader even though they have the wrong In-X-It status. An alarm is generated when a violation occurs.

Terminal Lost AC – This soft alarm type is not used with CK7xx or S321 panels.

Terminal Low Battery – This soft alarm type is not used with CK7xx or S321 panels.

Terminal Tamper – This soft alarm type is not used with CK7xx or S321 panels.

Panel Lost AC – Used with the UPS option, this soft alarm sends an alarm if the panel loses power. Not available for S321 panels.

Panel Low Battery – With UPS equipped panels, an alarm is sent when the battery in the panel is low. Not available for S321 panels.

Panel Tamper – The panel has an internal hardware connection for its own enclosure tamper switch that generates a special message whenever the enclosure is opened or closed. Not available for S321 panels.

Report on Terminal – Select a terminal from the drop-down list. This is the actual terminal connection associated with the Soft Alarm and is used for panel soft alarms only. Not available for S321 panels.

Configure Elevators and Cabinets

The P2000 system supports the elevator and cabinet access control using CK705, CK720, and CK721 panels.

The following sections describe how to configure:

- **Elevator Access Control**
- **Cabinet Access Control**

Elevator Access Control

General Overview

The elevator access control gives you the ability to assign entities access to various elevators and floors in your facility, through their access groups.

Elevator readers cannot be overridden by a Local Cardholder Override or a Timed Override, and do not allow the Auxiliary Access input to grant access to any floors.

Also, panel card events cannot be used on elevator readers.

Elevators are assigned floors and floor groups, then these floors and floor groups are included in access groups which are assigned to entities.

The basic procedures for defining and implementing the elevator access control are:

- Define Floor Names
- Define Floor Masks
- Configure Elevators
- Configure Floors
- Define Floor Groups
- Create Access Groups for Elevator Floors

Steps to perform each procedure are presented in the following sections. To successfully implement the elevator access control, configure these steps in the order presented.

Low Level Interface

Elevators are readers associated with a set of output points and an optional set of input points. The field panel interfaces with the elevator manufacturer's control system using output points to enable car-call buttons, and input points to monitor car-call buttons.

The panel may grant access to a floor by enabling the corresponding car-call button when a badge is presented at a reader installed in the elevator cab.

An elevator cab must be equipped with one reader, and one output needs to be assigned to every floor button in the cab that needs to be enabled by the security system. If floor tracking is desired, one input needs to be assigned to every floor button in the cab that is supposed to create a floor tracking message.

There is no prescribed scheme to associate outputs and inputs by their address to the elevator's floor buttons, but the reader and all outputs and inputs for an elevator must be defined on the same panel. The association of elevators, floors, readers, outputs and inputs is done by defining an Elevator in the P2000 software, and then downloading it into the panel.

When presenting a badge at the elevator cab's reader, the panel searches the badge record for floor access information. This information is then applied to energize the output relays of those floors that the person should have access. It is the elevator control system's responsibility to ensure the elevator does not go to disabled floors. The enabled floors will be disabled after the elevator access time has expired, unless they are still enabled by public access or by direct output control. All buttons, that are

exclusively enabled by the elevator access grant will produce floor tracking messages.

The P2000 system provides a D620 elevator mode that if selected, causes a modification in the badging sequence and in the elevator input and output point's behavior; refer to page 92 for more information.

High Level Interface

The KONE interface is a master slave protocol over RS232 or RS485, according to KONE Elevator EPL HLI Security Protocol specification V=2.3 SO-13.20.10-KAM, with the CK7xx being the master.

Each panel connects to a KONE group controller with up to 8 elevators, with each elevator serving up to 64 floors. To connect to the KONE group controller, you have to remove all modems from the panel and install a serial PCMCIA card.

To define a KONE elevator, the High Level Interface flag has to be checked, and the Protocol and Address fields have to be defined. To define the floors of a KONE elevator, the public access timezone must be defined, but there should be no output or input points associated with the floor. A floor is on public access when the specified timezone is active. A floor is not on public access when the specified timezone is inactive.

The rest of this integration is identical to the low level elevator interface.

Basic Definitions

Valid Badge – A valid badge in this context is defined as a badge that is accepted by the elevator's reader with a green light. The specific rights of this badge are dependent on the badge's access groups' floor masks, so it may be possible that a valid badge gives no access to any of the elevator's floors.

Elevator Access Grant – The valid badge’s access groups’ floor masks determine which of the elevator cab’s call buttons are enabled by an elevator access grant. Relinquishing an elevator access grant does not disable an elevator button that is enabled by public access or by direct output control.

Direct Output Control – Each elevator cab’s floor buttons may be enabled by direct output control from the Server’s or the panel’s user interface. Relinquishing direct output control does not disable an elevator button that is enabled by an elevator access grant or by public access.

Access Grant Message – When a valid badge is presented, the panel sends an elevator access grant message to the Server, which includes the badge’s number and entity name.

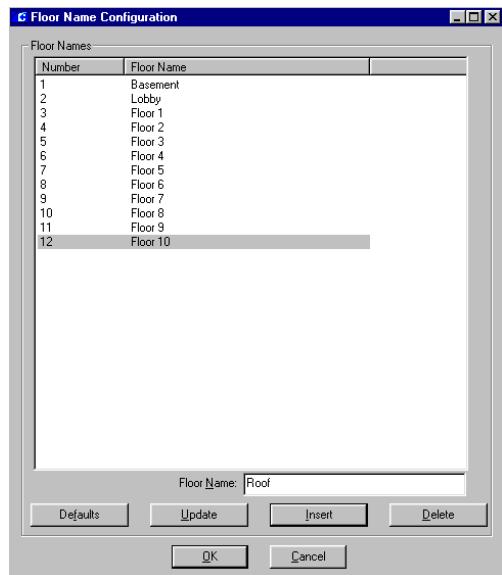
Override – When the reader terminal in the elevator cab is overridden, the public access feature energizes all of the associated output relays. This means, that there will be no floor tracking messages generated. Except for local cardholder override, all modes of reader override are applicable to elevator terminals, i.e. override per timezone, per panel system override and per the “Unlock All Doors” command from the Server.

Executive Privilege – Badges with executive privilege enable all floors of the elevator per elevator access grant.

Defining Floor Names

Use the Floor Name Configuration dialog box to define floor names and associated index number. Floors should be named by physical characteristics such as “Basement” or “Roof Access” to help identify the floor name and location when configuring the actual elevators. The system supports up to 128 floors.

- From the System Configuration window, click the plus (+) sign next to the root **Elevator/Cabinet Parameters** icon to display the elevator parameters.
- Click the **Elevator Floor Names** icon and click **Edit**. The Floor Name Configuration dialog box opens.



The number of floors entered in the Site Parameters dialog box displays. (Refer to “To Edit Site Parameters:” on page 30).

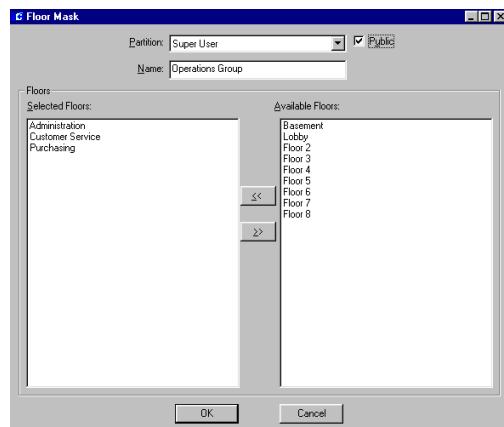
- Click on the floor you wish to rename. The floor name will display in the **Floor Name** field at the bottom of the window.
- Rename the floor accordingly and click **Insert**. The new name will display and the list of floor names will move down one position. For example, if you rename floor 1 and floor 2, Number 3 on the list will become Floor 1.

5. To edit a floor name, click on the floor name, rename it, then click **Update**.
6. If you delete a floor name, using the **Delete** button, the next floor on the list will move up one position.
7. To restore the default floor names, click the **Defaults** button.
8. When you finish configuring floor names, click **OK** to return to the System Configuration window.

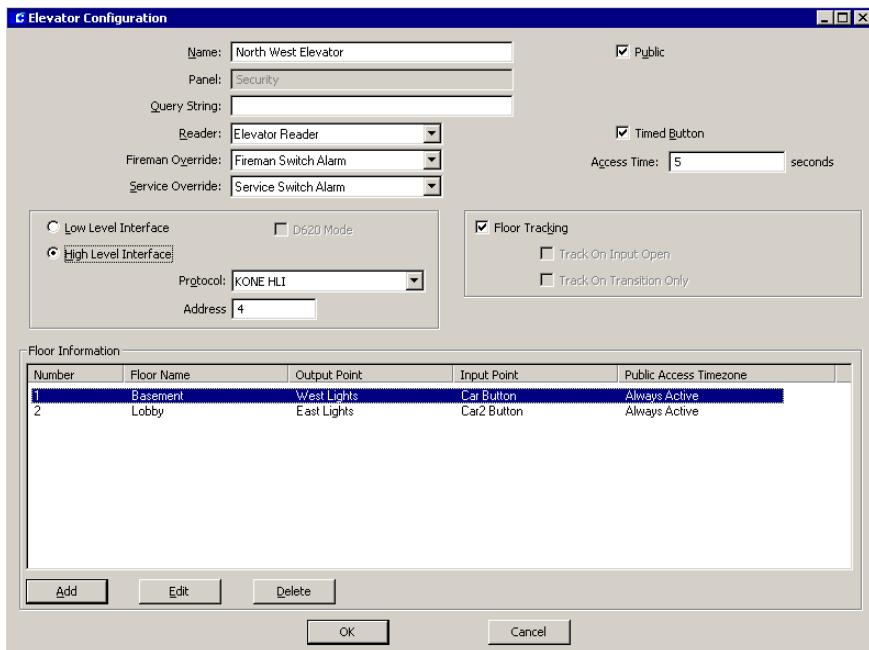
Defining Floor Masks

You can group floors that have common access throughout your facility and then apply them as a group to associate them with physical elevators when configuring Floor Groups. For example, your facility may have three floors that access the Operations department. When floors are grouped, you can assign entities that should have access to the three floors to the “Operations” group, rather than assigning all three floors to the entities individually.

1. From the System Configuration window, click the plus (+) sign next to the root **Elevator/Cabinet Parameters** icon to display the elevator parameters.
2. Click the **Elevator Floor Masks** icon and click **Add**. The Floor Mask dialog box opens.



3. If you use Partitioning, select the **Partition** that will have access to this Floor Mask. All available floors (for the partition selected) will be listed on the right side of the dialog box.
4. If you use Partitioning, select the **Public** check box to allow all partitions to see this Floor Mask.
5. Enter a descriptive **Name** for this Floor Mask. In the example, “Operations Group” will include Administration, Customer Service, and Purchasing floors.
6. From the **Available Floors** list, click the floor you wish to include in your group.
7. Click **<<**. The floor moves to the left side of the dialog box, to be included in the **Selected Floors** box.
8. To remove a floor from the Selected Floors box, select the floor and click **>>**.
9. When all floors you wish to include in the group have been moved to the Selected Floors box, click **OK**. A Floor Mask icon for the new group will be added under the Elevator Floor Masks root icon in the System Configuration window.



Configuring Elevators

Use the Elevator Configuration dialog box to define the reader and associated output and optional input points that will operate with your particular elevator controller type.

1. From the System Configuration window, click the **Panel** to which you wish to assign an elevator.
2. Select the **Elevators** icon and click **Add**. The Elevator Configuration dialog box opens.
3. Enter the required information according to the following Elevator Configuration Field Definitions.
4. After you have entered all the information, click **OK** to save your settings and return to the System Configuration window.

Elevator Configuration Field Definitions

Name – Enter a descriptive **Name** for this elevator.

Public – Select **Public** if you wish the elevator to be visible to all partitions.

Panel – This field defaults to the name of the panel you selected from the System Configuration window.

Query String – This value only applies if you have the P2000-Metasys option. Refer to “Configuring Hardware Components for BACnet Interface” on page 237.

Reader – Select an available reader from the drop-down list that has not yet been assigned to an elevator or cabinet.

Fireman Override – If the elevator has a fireman override switch, select from the drop-down list an available input point that has

not yet been assigned to an elevator or cabinet. The only purpose of this input point is to send messages to the Real Time List; it does not control Fireman Override.

Service Override – If the elevator has a service override switch, select from the drop-down list an available input point that has not yet been assigned to an elevator or cabinet. The only purpose of this input point is to send messages to the Real Time List; it does not control Service Override.

Timed Button – If enabled, the access grant at an elevator remains active for the specified elevator access time, independent of any elevator buttons being pressed. If this option is not enabled, the access grant is cancelled as soon as an enabled elevator button is pressed. It does not matter whether or not that enabled point is on public access. If no button is pressed, the access grant is cancelled at the end of the specified elevator access time.

Access Time – Enter the amount of time in seconds (2 to 600) that entities have to press a car-call button after badging at the elevator.

At the time a valid badge is presented to the elevator reader, the elevator access time starts. The elevator access time starts over with every subsequent presentation of a valid badge. At the beginning of the elevator access time certain floor buttons are enabled by the panel outputs per elevator access grant. Subsequent presentation of other badges therefore may enable more outputs. Only outputs exclusively enabled by elevator access grants will be disabled at the end of the elevator access time.

Low Level Interface – This is the default connection to the elevator control system. The idea behind tying a security system to an elevator control system is to allow people access only to certain floors and to control public access to floors by time zone control. The way this is done through the Low Level Interface is

by tying the security system's electrical outputs to the elevator control equipment, letting it know which of the cab's floor buttons a person is allowed to press. Obviously, a person in the cab could press any button, but only those that are "enabled" by the security system will actually register and take the elevator to those floors. Each pressed button can also be fed back to an electrical input of the security system, so it can track which buttons were pressed at any time.

D620 Mode – This option enables the low level D620 Elevator Mode. If enabled, when a badge is presented at the elevator cab's reader, the panel searches the badge record for floor access information. The floor access information is compared with the floor button selection input point. If the floor button selection input point matches the floor access information, then the output (timed) point for the floor the person should have access to is enabled. It is the elevator control system's responsibility to ensure the elevator does not go to disabled floors.

The cab's floor button selection must be made before the elevator access time has expired, unless the floor call-button is enabled by public access or by direct output control. The floor car-call button that is exclusively enabled by the elevator access grant will produce floor tracking message.

High Level Interface – Select this option to have the system communicate with the elevator control equipment via a serial protocol, exchanging all necessary information in both directions.

Protocol – If using a high level interface, select from the drop-down list the serial protocol used to communicate to the elevator control equipment. The only protocol supported at this time is the **KONE HLI**. To select this option, you must define the protocol parameters in the Elevator tab, see page 55.

Address – Enter the KONE elevator address (from 1 to 8) inside the KONE group controller. This value must match the address of the elevator group controller.

Floor Tracking – If enabled, the panel generates a history message identifying the badge number, entity's name, elevator, and floor selected when the car-call button is pressed.

Floor tracking messages are generated only for floors whose associated output is exclusively enabled by the elevator access grant, and not enabled by public access or by direct output control. A floor tracking message is generated for each elevator input that experiences a transition from the normal into the off-normal state during the elevator access time; or that is in the off-normal state at the time a valid badge is presented.

Track On Input Open – Defines the normal and off-normal states. If enabled, a floor tracking message will be generated when the floor's input is open. If disabled, a floor tracking message will be generated when the floor's input is closed.

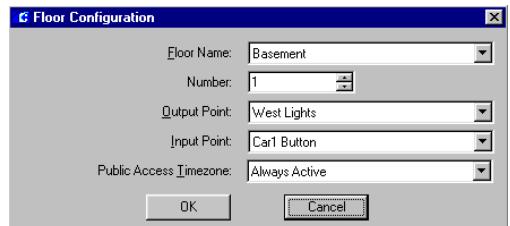
Track On Transition Only – If enabled, a floor tracking message will be generated only when the input transitions from a normal to off-normal state. If disabled, a floor tracking message will be generated when the input transitions from a normal to off-normal state and during the presentation of a valid badge while the input is in the off-normal state.

Note: *The Track On Input Open and Track On Transition Only options apply only to elevators that use input points for floor tracking, and only when the Floor Tracking option is enabled for Low Level Interface connections.*

Configuring Floors

The Floor Information box at the bottom of the Elevator Configuration dialog box displays the associated floors active for access. Follow the next steps to add the individual floors that this particular elevator will service.

1. In the Elevator Configuration dialog box, click the **Add** button at the bottom of the window. The Floor Configuration dialog box opens.

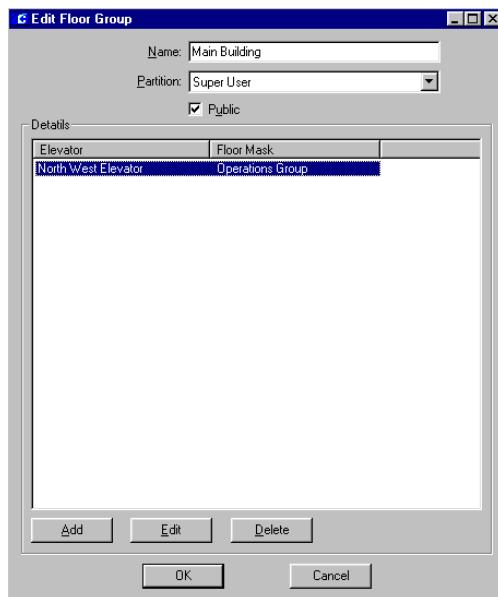


2. Select a **Floor Name** from the drop-down list that has not yet been assigned to this elevator. The list will display the floors names as configured in the Floor Name Configuration dialog box.
3. The floor **Number** index will automatically display in the Number field. You could select the Number first, and the associated floor name will display in the Floor Name field.
4. Select from the **Output Point** drop-down list an available output point that has not yet been assigned to an elevator or cabinet.
5. Select from the **Input Point** drop-down list an available input point that has not yet been assigned to an elevator or cabinet.
6. Select from the **Public Access Timezone** drop-down list the time zone defined to allow entities to use the elevator without presenting their badge at the reader. If no time zone is selected, then this floor is not active for public access.
7. Click **OK** to save your settings and return to the Elevator Configuration dialog box.

Defining Floor Groups

Use the Edit Floor Group dialog box to associate specific groups of floors with physical elevators.

- From the System Configuration window, click the plus (+) sign next to the root **Elevator/Cabinet Parameters** icon to display the elevator parameters.
- Click the **Elevator Floor Groups** icon and click **Add**. The Edit Floor Group dialog box opens.



- Enter a descriptive **Name** for the Floor Group.
- If you use Partitioning, select the **Partition** that will have access to this Floor Group.
- Select the **Public** check box to allow all partitions to see this Floor Group.
- Click the **Add** button at the bottom of the dialog box. The Group Detail dialog box opens.



- Select from the **Elevator** drop-down list an elevator name, previously configured in the Elevator Configuration dialog box.
- Select from the **Floor Mask** drop-down list a floor mask name, previously configured in the Floor Mask dialog box.
- Click **OK** to save your entries and return to the Edit Floor Group dialog box.
- Click **OK** to save the Floor Group and return to the System Configuration window.

Creating Access Groups for Elevator Floors

Access groups are described under “Create Access Groups” on page 117. Refer to this section for detailed information.

Cabinet Access Control

Cabinets are readers associated with a set of output points and an optional set of input points. The field panel interfaces with a bank of cabinets using output points to unlock cabinet doors, and input points to monitor the status of cabinet doors.

The panel may grant access to a cabinet by unlocking the corresponding door when a badge is presented at a reader installed in the cabinet definition.

The cabinet access control gives you the ability to assign entities access to various cabinets and doors in your facility, through their access groups.

Cabinets are assigned doors and door groups, then these doors and door groups are included in access groups which are assigned to entities.

The basic procedures for defining and implementing the cabinet access control are:

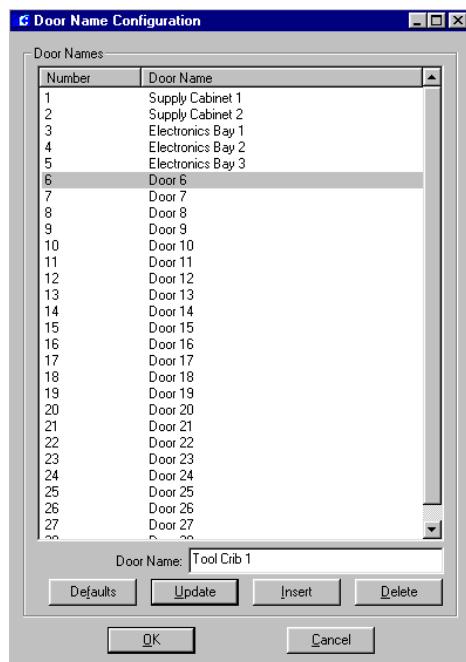
- Define Door Names
- Define Door Masks
- Configure Cabinets
- Configure Doors
- Define Door Groups
- Create Access Groups for Cabinet Doors

Steps to perform each procedure are presented in the following sections. To successfully implement the cabinet access control, configure these steps in the order presented.

Defining Door Names

Use the Door Name Configuration dialog box to define door names and associated index number. Doors should be named by physical characteristics such as “Supply Cabinet 1” or “Electronics Bay 1” to help identify the door name and location when configuring the actual cabinets. The system supports up to 128 doors.

1. From the System Configuration window, click the plus (+) sign next to the root **Elevator/Cabinet Parameters** icon to display the cabinet parameters.
2. Click the **Cabinet Door Names** icon and click **Edit**. The Door Name Configuration dialog box opens.



The number of doors entered in the Site Parameters dialog box displays. (Refer to “To Edit Site Parameters:” on page 30.)

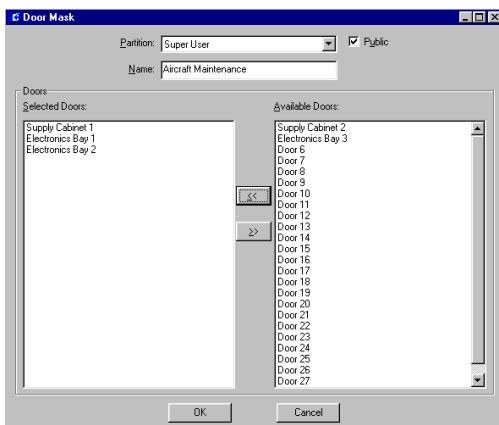
3. Click on the door you wish to rename. The door name will display in the **Door Name** field at the bottom of the window.
4. Rename the door accordingly and click **Insert**. The new name will display and the list of door names will move down one position. For example, if you rename door 1 and door 2, Number 3 on the list will become Door 1.
5. To edit a door name, click on the door name, rename it, then click **Update**.
6. If you delete a door name, using the **Delete** button, the next door on the list will move up one position.
7. To restore the default door names, click the **Defaults** button.

- When you finish configuring door names, click **OK** to return to the System Configuration window.

Defining Door Masks

You can group doors that have common access throughout your facility and then apply them as a group to associate them with physical cabinets when configuring Door Groups.

- From the System Configuration window, click the plus (+) sign next to the root **Elevator/Cabinet Parameters** icon to display the cabinet parameters.
- Click the **Cabinet Door Masks** icon and click **Add**. The Door Mask dialog box opens.



- If you use Partitioning, select the **Partition** that will have access to this Door Mask. All available doors (for the partition selected) will be listed on the right side of the dialog box.
- Select the **Public** check box to allow all partitions to see this Door Mask.
- Enter a descriptive **Name** for the Door Mask. In the example, "Aircraft Maintenance Group" includes Supply Cabinet 1, Electronics Bay 1, and Electronics Bay 2 doors.

- From the **Available Doors** list, click the door you wish to include in your group.
- Click **<<**. The door moves to the left side of the dialog box, to be included in the **Selected Doors** box.
- To remove a door from the Selected Doors box, select the floor and click **>>**.
- When all doors you wish to include in the group have been moved to the Selected Doors box, click **OK**. A Door Mask icon for the new group will be added under the Cabinet Door Masks root icon in the System Configuration window.

Configuring Cabinets

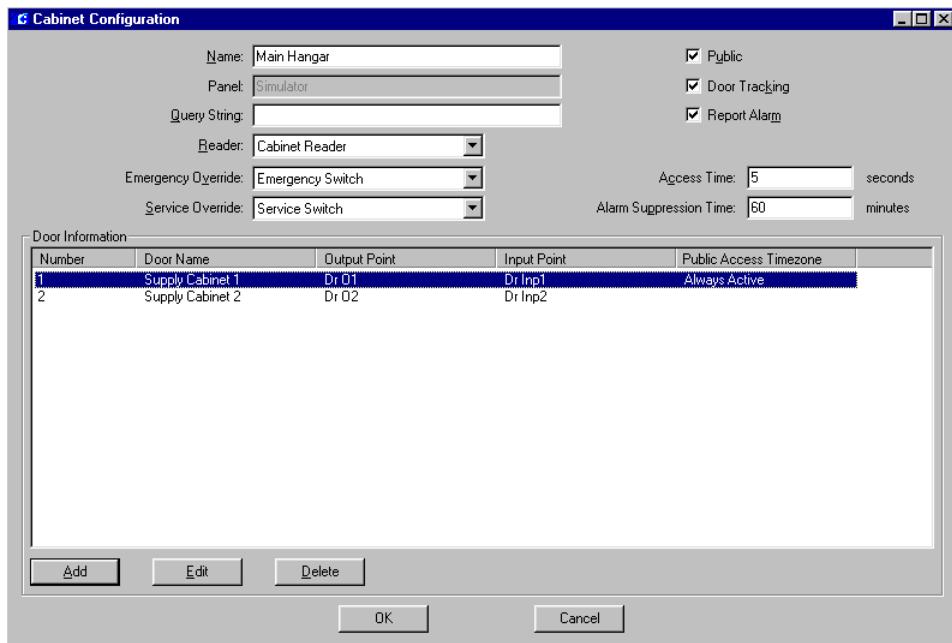
Use the Cabinet Configuration dialog box to define the reader and associated output and optional input points that will operate with your particular cabinet controller type.

- From the System Configuration window, click the **Panel** to which you wish to assign a cabinet.
- Select the **Cabinets** icon and click **Add**. The Cabinet Configuration dialog box opens.
- Enter the required information according to the following Cabinet Configuration Field Definitions.
- After you have entered all the information, click **OK** to save your settings and return to the System Configuration window.

Cabinet Configuration Field Definitions

Name – Enter a descriptive **Name** for this cabinet.

Public – Select **Public** if you wish the cabinet to be visible to all partitions.



Panel – This field defaults to the name of the panel you selected from the System Configuration window.

Query String – This value only applies if you have the P2000-Metasys option. Refer to “Configuring Hardware Components for BACnet Interface” on page 237.

Reader – Select an available reader from the drop-down list that has not yet been assigned to an elevator or cabinet.

Emergency Override – If the cabinet has an emergency override switch, select from the drop-down list an available input point that has not yet been assigned to an elevator or cabinet. The only purpose of this input point is to send messages to the Real Time List; it does not control Emergency Override.

Service Override – If the cabinet has a service override switch, select from the drop-down list an available input point that has not yet been assigned to an elevator or cabinet. The only purpose of this input point is to send messages

to the Real Time List; it does not control Service Override.

Door Tracking – If enabled, the panel generates a history message identifying the badge number, cabinet, and door selected when an enabled door is opened.

Report Alarm – If enabled, an alarm will be reported when a door, that has not been enabled, is opened; or when an enabled door remains opened for longer than the time set in the Alarm Suppression Time.

Access Time – Enter the amount of time in seconds (2 to 600) that entities have to open a door after badging at the cabinet.

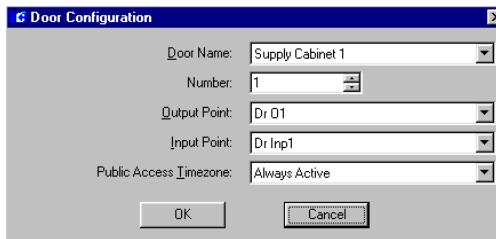
Alarm Suppression Time – Enter the amount of time in minutes (2 to 1440) for a door to remain open.

Configuring Doors

The Door Information box at the bottom of the Cabinet Configuration dialog box displays the

associated doors active for access. Follow the next steps to add individual doors to this cabinet.

1. In the Cabinet Configuration dialog box, click the **Add** button at the bottom of the window. The Door Configuration dialog box opens.

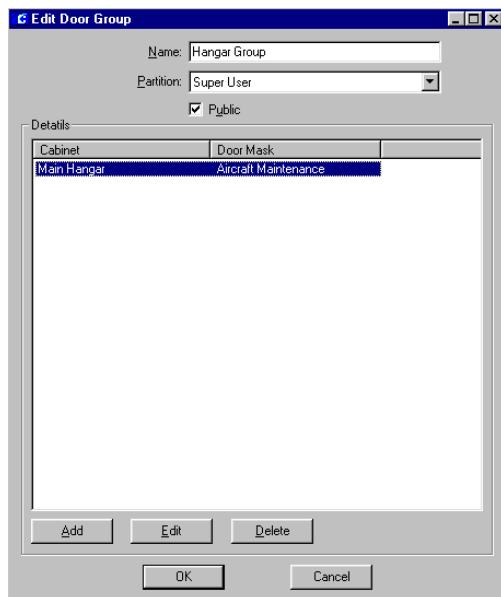


2. Select a **Door Name** from the drop-down list that has not yet been assigned to this cabinet. The list will display the doors names as configured in the Door Name Configuration dialog box.
3. The door **Number** index will automatically display in the Number field. You could select the Number first, and the associated door name will display in the Door Name field.
4. Select from the **Output Point** drop-down list an available output point that has not yet been assigned to an elevator or cabinet.
5. Select from the **Input Point** drop-down list an available input point that has not yet been assigned to an elevator or cabinet.
6. Select from the **Public Access Timezone** drop-down list the time zone defined to allow entities to access the cabinet without presenting their badge at the reader. If no time zone is selected, then this door is not active for public access.
7. Click **OK** to save your settings and return to the Cabinet Configuration dialog box.

Defining Door Groups

Use the Edit Door Group dialog box to associate specific groups of doors with physical cabinets.

1. From the System Configuration window, click the plus (+) sign next to the root **Elevator/Cabinet Parameters** icon to display the cabinet parameters.
2. Click the **Cabinet Door Groups** icon and click **Add**. The Edit Door Group dialog box opens.



3. Enter a descriptive **Name** for the Door Group.
4. If you use Partitioning, select the **Partition** that will have access to this Door Group.
5. Select the **Public** check box to allow all partitions to see this Door Group.
6. Click the **Add** button at the bottom of the dialog box. The Group Detail dialog box opens.



7. Select from the **Cabinet** drop-down list a cabinet name, previously configured in the Cabinet Configuration dialog box.
8. Select from the **Door Mask** drop-down list a door mask name, previously configured in the Door Mask dialog box.
9. Click **OK** to save your entries and return to the Edit Door Group dialog box.
10. Click **OK** to save the Door Group and return to the System Configuration window.

Creating Access Groups for Cabinet Doors

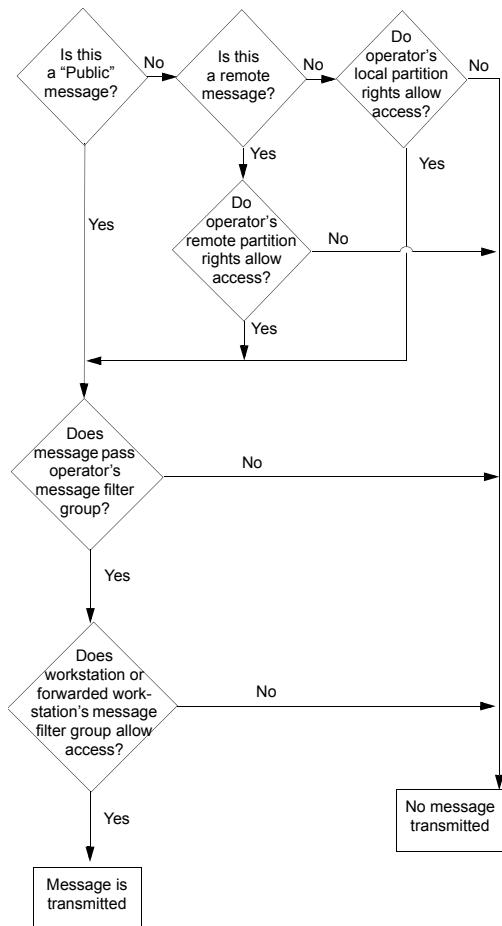
Access groups are described under “Create Access Groups” on page 117. Refer to this section for detailed information.

Configure Message Filtering and Message Routing

Message Filtering and Routing configuration allows you to transmit and receive specific messages to and from specific local or remote P2000 systems, thereby reducing network traffic by transmitting and receiving only messages that pass filter criteria. The Remote Message Server (RMS) maintains central control over all message routing and transmits messages only to P2000 Servers or workstations that the RMS assumes are able and willing to receive the message.

Operators and Messages

The following illustrates the authorization process to allow operators to see messages.



Basic Principles and Definitions

P2000 Site – Uniquely identified by its Local Site name. A P2000 Site can have multiple locations but only one P2000 Server.

P2000 Location – A physical location or place with a P2000 workstation or panel.

P2000 Server – A single server that communicates with the panels for that site. Typically, it

is also the database server for that site, but it is possible for another computer to act as the database server for performance reasons.

P2000 Workstation – A single computer that is connected to one P2000 Server and is used to run the P2000 software.

P2000 System – A P2000 System is defined by what is controlled by the P2000 Server. A P2000 System has no relationship to geography, so a single P2000 system can and often will contain multiple facilities in multiple locations.

Local P2000 Server/Workstations – A P2000 Server and/or P2000 Workstations are local to each other, if they are part of the same P2000 System.

P2000 Remote Server – A P2000 Server that controls a different P2000 System to the one where the transaction was originated. The P2000 Remote Server is the recipient of a forwarded transaction and has no knowledge of the access control hardware and system information related to the originating P2000 System.

Remote Transactions – Remote Transactions are messages received from another P2000 System.

Message Forwarding – Message Forwarding is the ability to temporarily forward messages from one P2000 operator logged on at a local P2000 workstation “A” to another local P2000 workstation “B.” The forwarded messages will only be visible at the P2000 workstation “B,” if the operator at workstation “B” has sufficient rights to view these messages.

Message Filtering – Reduces network traffic by only transmitting a sub-set of P2000 messages that pass a filter criteria.

Message Routing – Allows the system to route a sub-set of messages to a remote P2000 System.

Remote Message Service (RMS) – P2000 service that receives messages from the local RTL Route Service and transmits these messages to the remote P2000 Remote Message Service. When receiving a remote message, the local Remote Message Service will process the message and pass it on to the local RTL Route Service for distribution to the local workstations.

Sequence of Steps

The basic procedures for defining and implementing message filtering and routing are:

- Define message filters
- Create message filter groups
- Configure P2000 Remote Servers
- Assign message filter groups to workstations (page 20), operators (page 148), and remote servers (page 109).
- Define Remote Message Service settings in Site Parameters, see “RMS Tab” on page 38.

Message Filtering

Message filtering allows you to control the types of messages transmitted to local workstations or remote servers, thereby reducing network traffic by only transmitting a sub-set of P2000 messages that pass filter criteria.

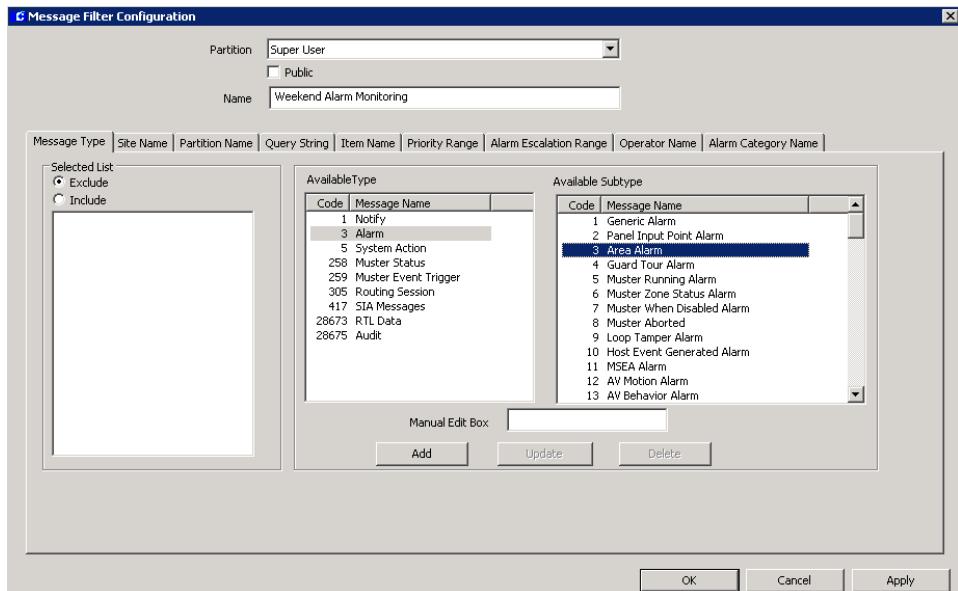
Messages are sent to all workstations by default, provided the message is marked “Public” or the logged on operator has the proper access. Depending on the parameters selected in the Message Filter Configuration dialog box, you can filter which messages are to be transmitted when alarm and transaction messages are generated. The system will only transmit messages that pass the filter criteria

defined. You can, for instance, filter messages to send a specific group to one workstation and a different group to another. By using message filters you may for example, limit the alarm messages sent to workstations located in Building A to only those alarms originating in Building A, and do the same for Building B. For a complete list of all available message types and associated sub-types, see *Appendix B: Message Types and Sub-Types*.

Note: All messages are sent by default to the local Server at all times, therefore this feature cannot be used at the Server.

To Create a Message Filter:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Select the **Message Filter** icon and click **Add**. The Message Filter Configuration dialog box opens.



3. If you use Partitioning, select the **Partition** that will have access to this Message Filter.
4. If you use Partitioning, select the **Public** check box to allow all partitions to see this Message Filter.
5. Enter a descriptive **Name** for this Message Filter.
6. Refer to the following sections to define message types, filters, and ranges.

Note: The length of all filter strings entered in each Selected List is limited to approximately 1000 characters.

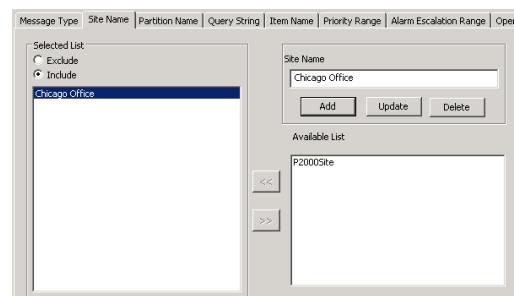
7. As you work through the tabs, you may click **Apply** at any time to save your entries.
8. After you have entered all the information, click **OK** to save the settings and return to the System Configuration window.

Define Message Types

1. Click the **Message Type** tab.
2. In the **Available Type** box, click the message type you wish to define.
3. In the **Available Subtype** box, click the message subtype you wish to define. The selections in this box are dependent on the type selected in the Available Type box.
4. Click the **Add** button. The message type and subtype code will be automatically entered in the Selected List box.
5. To enter messages from third-party software or any currently unknown message, enter the text in the **Manual Edit Box**, then click the **Add** button.
6. To edit your selection, select the message code from the Selected List box, make the change, then click the **Update** button.
7. To delete a message type from the Selected List, select the message code and click the **Delete** button.
8. Once the message types are selected, click the **Include** option in the Selected List box to accept these types of messages.
9. To reject all messages of the type selected, click **Exclude**.

Define Site Name Filters

Messages associated with the Site Name selected in this tab will be either accepted or rejected. For example, you can select to see *Area Alarm* messages originated only at the *Chicago Office*, or you can select to see all *Area Alarm* messages, except the ones originated at the *Chicago Office*, if the **Exclude** option is selected.



1. Click the **Site Name** tab.
2. Select from the **Available List** the Site Name and click **<<** to move it to the Selected List. To remove it from the Selected List, click **>>**.

Note: The Available List displays the Local Site Name only. All other site names need to be entered in the Site Name field. Site Name entries are case sensitive.

3. To add a remote site name to the Selected List, enter the name in the **Site Name** field and click the **Add** button.

If the Site Name changes either at the local site or at the remote site, you must re-select the name from the Available List or re-enter the new name in the Site Name field.

Entries may contain a filter string to specify more than one Site Name, for example enter “New*” to add Site Names such as New York, New Jersey, New Security, etc.

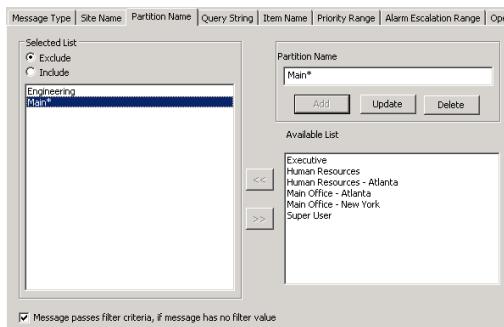
Note: The wildcard character * (asterisk) in a filter string means that all possible selections will be listed. The wildcard character is supported at the end of the filter value only.

4. To edit a remote site name or filter string, select the name, make the change, then click the **Update** button.

5. To delete a remote site name or filter string from the list, select the name and click the **Delete** button.
6. Once the Site Names are selected, click the **Include** option in the Selected List box to accept messages associated with the Site Names.
7. To reject all messages associated with the Site Names selected, click **Exclude**.

Define Partition Name Filters

The system will either accept or reject messages associated with the Partition Names selected in this tab. The Available List displays all partition names within the local system, including any Remote Partitions entered in the User tab of Entity Management.



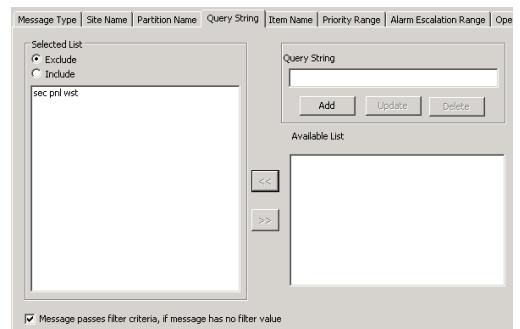
1. Click the **Partition Name** tab.
2. Select from the **Available List** the Partition Name and click **<<** to move it to the **Selected List**. To remove it from the **Selected List**, click **>>**.
3. To add a remote partition name to the **Selected List**, enter the name in the **Partition Name** field and click the **Add** button.
If the Partition Name changes either at the local site or at the remote site, you must re-select the name from the Available List or re-enter the new name in the Partition Name field.

You may enter a filter string to specify more than one Partition Name, for example enter “Main*” to add Partition Names such as “Main Office - Atlanta” and “Main Office - New York.”

4. To edit a remote partition name or filter string, select the name, make the change, then click the **Update** button.
5. To delete a remote partition name or filter string from the list, select the name and click the **Delete** button.
6. Once the Partition Names are selected, click the **Include** option in the Selected List box to accept messages associated with the Partition Names.
7. To reject all messages associated with the Partition Names selected, click **Exclude**.
8. If the **“Message passes filter criteria, if message has no filter value”** check box is enabled, the message will meet the filter criteria even if there is no filter value. Do not select the check box to stop the message from passing the filter criteria if there is no filter value.

Define Query String Filters

Use this tab to filter messages by Query Strings. Query Strings are filled by querying Panels, Terminals, Input Points, and Output Points. The Available List displays all query strings defined within the local system.



1. Click the **Query String** tab.
2. Select from the **Available List** the Query String and click **<<** to move it to the Selected List. To remove it from the Selected List, click **>>**.
3. To add a remote query string to the Selected List, enter the query string in the **Query String** field and click the **Add** button.

If the Query String Name changes either at the local site or at the remote site, you must re-select the name from the Available List or re-enter the new name in the Query String field.

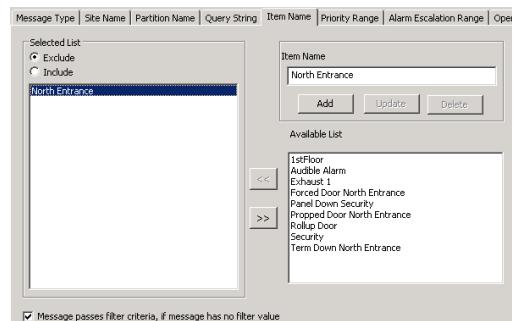
You may enter a filter string to specify more than one Query String, then click the **Add** button.

4. To edit a remote query string name or filter string, select the name, make the change, then click the **Update** button.
5. To delete a remote query string name or filter string from the list, select the name and click the **Delete** button.
6. Once the Query Strings are selected, click the **Include** option in the Selected List box to accept messages associated with the Query Strings.
7. To reject all messages associated with the Query String selected, click **Exclude**.
8. If the “**Message passes filter criteria, if message has no filter value**” check box is enabled, the message will meet the filter criteria even if there is no filter value. Do not select the check box to stop the message from passing the filter criteria if there is no filter value.

Define Item Name Filters

Use this tab to filter messages by Item Names. The Available List displays all Panels, Termi-

nals, Input and Output Points defined within the local system.



1. Click the **Item Name** tab.
2. Select from the **Available List** the Item Name and click **<<** to move it to the Selected List. To remove it from the Selected List, click **>>**.

3. To add an item from a remote site to the Selected List, enter the name in the **Item Name** field and click the **Add** button.

If the Item Name changes either at the local site or at the remote site, you must re-select the name from the Available List or re-enter the new name in the Item Name field.

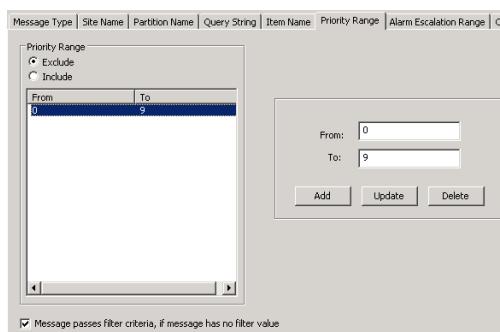
You may enter a filter string to specify more than one Item Name.

4. To edit a remote item name or filter string, select the name, make the change, then click the **Update** button.
5. To delete a remote item name or filter string from the list, select the name and click the **Delete** button.
6. Once the Item Names are selected, click the **Include** option in the Selected List box to accept messages associated with the Item Names.
7. To reject all messages associated with the Item Name selected, click **Exclude**.

- If the “**Message passes filter criteria, if message has no filter value**” check box is enabled, the message will meet the filter criteria even if there is no filter value. Do not select the check box to stop the message from passing the filter criteria if there is no filter value.

Define Priority Ranges

Priorities define the order an alarm message is placed in the alarm queue. You can configure message filtering to accept or reject messages within a priority range. For example, you can assign a security supervisor to monitor high priority alarms only (zero being the highest).



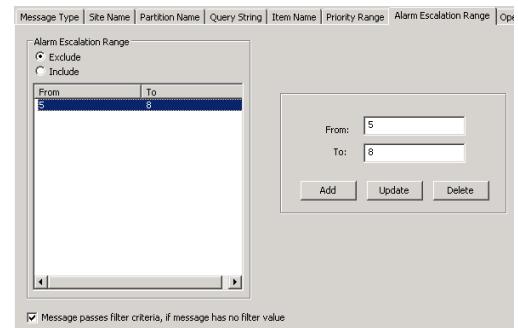
- Click the **Priority Range** tab.
- Enter in the **From** field the start of the priority range.
- Enter in the **To** field the end of the priority range.
- Click the **Add** button. The selected values will display in the **Priority Range** box.
- To edit the priority range, select the value, make the change, then click the **Update** button.
- To delete an entry, select the value and click the **Delete** button.
- Once the Priority Ranges are selected, click the **Include** option in the Priority Range list box to accept messages that

have a priority value within the range selected.

- To reject all messages that have a priority value within the range selected, click **Exclude**.
- If the “**Message passes filter criteria, if message has no priority**” check box is enabled, the message will meet the filter criteria even if there is no priority value. Do not select the check box to stop the message from passing the filter criteria if there is no priority value.

Define Alarm Escalation Ranges

You can configure message filtering to accept or reject messages based on the alarm escalation value. For example, you can assign a security supervisor to monitor only the alarms escalated above level 5 (0 meaning that an alarm has not been escalated, and 10 meaning an alarm has been escalated to the highest possible value).

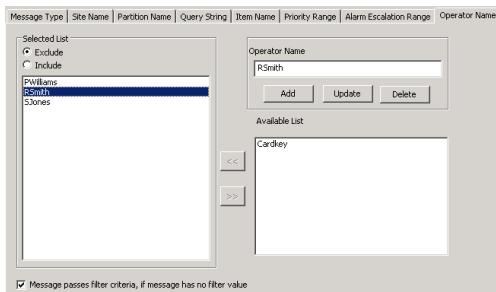


- Click the **Alarm Escalation Range** tab.
- Enter in the **From** field the start of the alarm escalation range.
- Enter in the **To** field the end of the alarm escalation range.
- Click the **Add** button. The selected values will display in the **Alarm Escalation Range** box.

5. To edit the alarm escalation range, select the value, make the change, then click the **Update** button.
6. To delete an entry, select the value and click the **Delete** button.
7. Once the Alarm Escalation Ranges are selected, click the **Include** option in the Alarm Escalation Range list box to accept messages that have an alarm escalation value within the range selected.
8. To reject all messages that have an alarm escalation value within the range selected, click **Exclude**.
9. If the “**Message passes filter criteria, if message has no priority**” check box is enabled, the message will meet the filter criteria even if there is no alarm escalation value. Do not select the check box to stop the message from passing the filter criteria if there is no alarm escalation value.

Define Operator Name Filters

Use this tab to accept or reject messages associated with the operator names selected here. For example, you can limit the number of operators who respond to alarm messages generated at your local site. The Available List displays the names of all the operators within the local system.



1. Click the **Operator Name** tab.

2. Select from the **Available List** the Operator Name and click **<<** to move it to the Selected List. To remove it from the Selected List, click **>>**.

3. To add remote operator names to the Selected List, enter the name in the **Operator Name** field and click the **Add** button.

If the Operator Name changes either at the local site or at the remote site, you must re-select the name from the Available List or re-enter the new name in the Operator Name field.

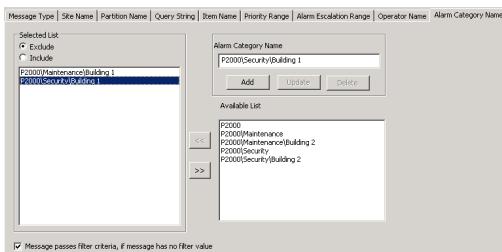
You may enter a filter string to specify more than one Operator Name.

4. To edit a remote operator name or filter string, select the name, make the change, then click the **Update** button.
5. To delete a remote operator name or filter string from the list, select the name and click the **Delete** button.
6. Once the Operator Names are selected, click the **Include** option in the Selected List box to accept messages associated with the Operator Names.
7. To reject all messages associated with the Operator Names selected, click **Exclude**.
8. If the “**Message passes filter criteria, if message has no filter value**” check box is enabled, the message will meet the filter criteria even if there is no filter value. Do not select the check box to stop the message from passing the filter criteria if there is no filter value.

Define Alarm Category Filters

The system will either accept or reject messages associated with the Alarm Category Names selected in this tab. The Available List displays the default “P2000” category and all user-defined categories. If you use the Enterprise option, the Alarm Categories defined for

all P2000 sites within an Enterprise system will be listed.



1. Click the **Alarm Category Name** tab.
2. Select from the **Available List** the Alarm Category Name and click **<<** to move it to the Selected List. To remove it from the Selected List, click **>>**.
3. To add an alarm category name, enter the name in the **Alarm Category Name** field and click the **Add** button.
You may enter a filter string to specify more than one Alarm Category Name.
4. To edit a remote alarm category name or filter string, select the name, make the change, then click the **Update** button.
5. To delete an alarm category name or filter string from the list, select the name and click the **Delete** button.
6. Once the Alarm Category Names are selected, click the **Include** option in the Selected List box to accept messages associated with the Alarm Category Names.
7. To reject all messages associated with the Alarm Category Name selected, click **Exclude**.
8. If the “**Message passes filter criteria, if message has no filter value**” check box is enabled, the message will meet the filter criteria even if there is no filter value. Do not select the check box to stop the message from passing the filter criteria if there is no filter value.

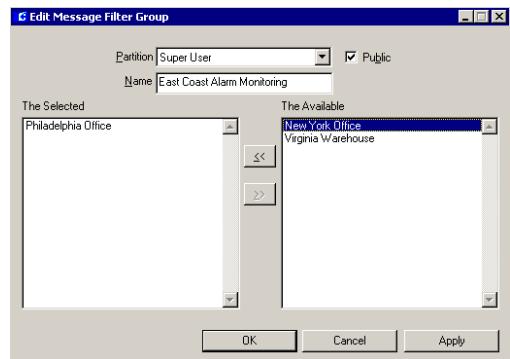
Create Message Filter Groups

Message filters are assigned by groups, therefore you must create Message Filter Groups before they will be available to be assigned to workstations, operators, and remote servers.

A Message Filter Group can contain multiple message filters, but if at least one message filter within the group passes the filter criteria, the message gets transmitted.

To Create a Message Filter Group:

1. From the System Configuration window, select the **Message Filter Group** icon and click **Add**. The Edit Message Filter Group dialog box opens.



2. If you use Partitioning, select the **Partition** that will have access to this Message Filter Group. All available message filters (for the partition selected) will be listed on the right side of the dialog box.
3. If you use Partitioning, select the **Public** check box to allow all partitions to see this Message Filter Group.
4. Enter a descriptive **Name** for this Message Filter Group.
5. From the **Available** list, click the message filter you wish to include in your group.

- Click **<<**. The message filter moves to the left side of the dialog box, to be included in the **Selected** box.

Note: The Selected box will display “auto-added” next to a Message Filter that was automatically added using a Host Event.

- To remove a message filter from the Selected box, select the message filter and click **>>**.
- When all message filters you wish to include in the group have been moved to the Selected box, click **OK**. A Message Filter Group icon for the new group will be added under the Message Filter Groups icon in the System Configuration window.

Message Routing

Message routing allows the transfer of alarm and transaction messages between P2000 Servers located at different P2000 Sites. Message routing is processed by the Alarm Monitor (see “Monitoring Remote Alarms” on page 162) and the Real Time List application (see “Monitoring Remote Messages in Real Time” on page 213).

Configuring P2000 Remote Servers

The P2000 Remote Server application must be properly configured at each remote site that wishes to transmit and receive alarm and transaction messages. The setup must include the name, IP address and Remote Message Service Listener Port number of the remote site; the type of messages that will be forwarded and at what times; and other related parameters.

To Create a P2000 Remote Server:

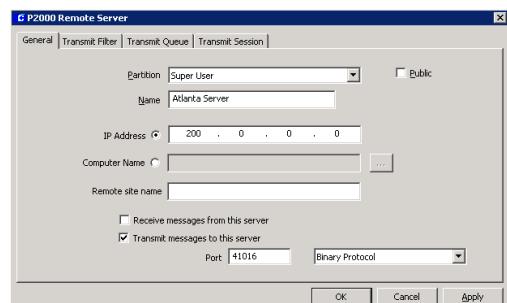
- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Select the **Remote Server** icon and click **Add**. The P2000 Remote Server dialog box opens at the General tab.
- Fill in the information on each tab according to the following “P2000 Remote Server Field Definitions.”
- As you work through the tabs, you may click **Apply** at any time to save your entries.
- After you have entered all the information, click **OK** to save the settings and return to the System Configuration window.

Note: Any change made to the P2000 Remote Server settings will only take effect after you restart the P2000 Remote Message Service, refer to “Starting and Stopping Service Control” on page 315.

P2000 Remote Server Field Definitions

General Tab

Use this tab to define general descriptive information of the P2000 remote servers that will be allowed to receive or transmit messages to other servers.



Partition – If you use Partitioning, select the Partition that will have access to this P2000 Remote Server.

Public – Select this check box to allow all partitions to see this P2000 Remote Server.

Name – Enter a descriptive Name of the P2000 Remote Server.

IP Address – If you select the IP Address option, enter the IP Address of the P2000 Remote Server that will be used to receive or transmit messages.

Computer Name – If you select the Computer Name option, enter the Windows computer name that will be used to receive or transmit messages, or click the [...] button to find a computer by name on your network.

Remote Site Name – Enter the name of the remote site that will be sending messages to your local site. You must enter a name in this field if you select the *Receive messages from this server* option.

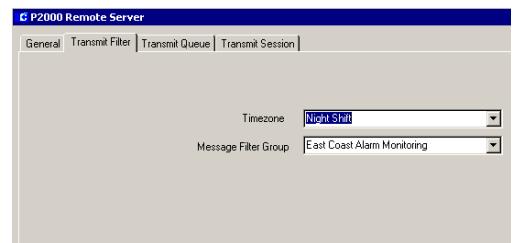
Receive messages from this server – Select this option to receive messages from this remote server.

Transmit messages to this server – Select this option to transmit messages to this remote server.

Port – Enter the Remote Message Service Listener Port number of the remote site, and select from the drop-down list the protocol to be used for transmitting messages to the remote server. Options are: Binary Protocol, HTTP Post XML Protocol, and XML Protocol.

Transmit Filter Tab

This tab defines what type of messages and during which times you want to send messages to a remote server.



Timezone – Select from the drop-down list the time zone during which messages, that pass the Message Filter Group criteria, will be transmitted to the P2000 remote server. Select <Always Enabled> to send messages at all times.

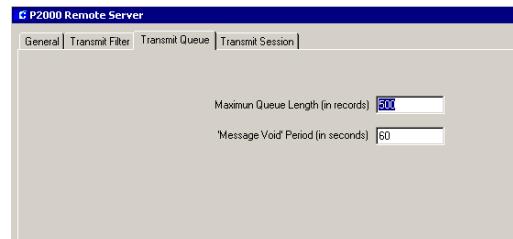


If the P2000 Remote Server is down during an active time zone, messages will not be transmitted and they will not be available for later transmission!

Message Filter Group – Select the Message Filter Group that defines which messages will be transmitted to this P2000 remote server. Select <None> to transmit all messages to this remote server.

Transmit Queue Tab

Use this tab to define message queue parameters for the remote server.

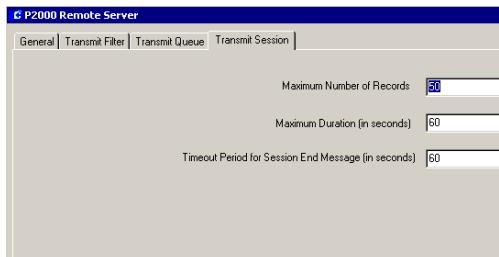


Maximum Queue Length – Enter the maximum number of messages that can be placed in the transmission queue. Messages are transmitted based on the First-In-First-Out (FIFO) principle.

Message Void Period – Enter the time in seconds after which the system will declare messages in the buffer as obsolete.

Transmit Session Tab

Parameters specific to individual transmission sessions are set up in the Transmit Session tab.



Maximum Number of Records – Enter the maximum number of messages than can be transmitted within one session.

Maximum Duration – Enter the maximum duration in seconds that a session will be kept open.

Timeout Period for Session End Message – Enter the number of seconds that the session will wait without receiving a message, until it declares the session closed.

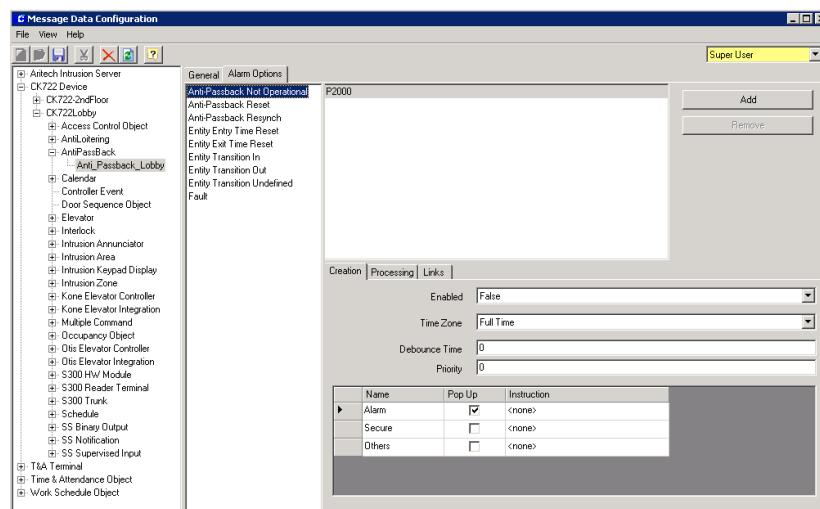
Set Up Message Data Configuration

Use this application to configure additional information for the processing of messages that are not provided by SCT (the configuration tool for the CK722 panel) or by third party configurators (such as the OPC Server Configurator or the Time & Attendance interface).

Aritech OPC Intrusion Message Configuration

Once the OPC intrusion panels and associated areas, zones, and annunciators have been configured using the instructions provided with the OPC Server Configurator, they must be enabled in the Data Message Configuration application to populate the associated data into the P2000 database.

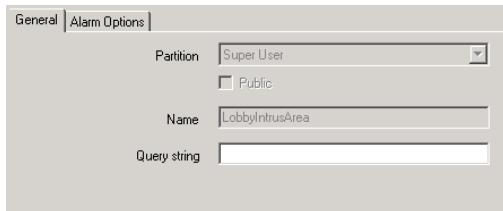
- From the P2000 Main menu, select **Config>Message Data Configuration**. The Message Data Configuration window opens as a two pane window.



2. From the left window pane, select **Aritech Intrusion Server** and click **New**. The Server name displays.
3. In the General tab, on the right side of the window select the **Enable** check box to send a message to OPCProxy server to populate data into the P2000 database.
4. Click the **Save** icon.

Once you enable the intrusion server, the Message Data Configuration window is automatically populated with the intrusion device and associated intrusion areas, zones, and annunciators.

5. To configure the components associated with the intrusion server, click the plus (+) sign to expand items in the tree. A plus (+) sign next to an item indicates that items may exist beneath them. When you select an item in the tree, the values relating to that selection are listed on the right windowpane. Click the **Edit** icon.



6. The General tab displays the **Name** of the intrusion component. Enter the **Partition**, **Public**, and **Query String** settings for each of the intrusion component.
7. Click **Save**.

Note: Item names of the same type (configured using the OPC Server configurator), must be unique, for example two zones cannot have the same name.

8. To configure alarm options for intrusion components, refer to “Message Data Configuration Alarm Options” on page 114.

CK722 Message Configuration

Use Message Data Configuration to set up message processing associated with CK722 components that were defined using SCT.

1. From the P2000 Main menu, select **Config>Message Data Configuration**. The Message Data Configuration window opens as a two pane window.
2. From the left window pane, click the plus (+) sign next to **CK722 Device** to expand items in the tree. The tree will display the CK722 devices that were configured using the SCT tool.
3. Select a CK722 device and click the **Edit** icon.



4. The General tab, on the right side of the window, displays the **Name** defined for the CK722 device using SCT. You only need to enter the **Query String** (if any), associated with the CK722 device.
5. To configure the CK722 device as a BACnet object, click the **BACnet Enabled** check box.
6. If you select an object in the **Enable BACnet Interface** box, by default, every one of those objects defined for the selected CK722 panel will become a BACnet object.
7. Click **Save**.

Note: *Restart the BACnet Service. If you do not restart the BACnet Service on the P2000 BACnet Server after editing, the changes to the Message Data Configuration application will not be applied when viewing P2000 objects from the M3 or M5 workstation.*

8. To configure components associated with a CK722 device, click the plus (+) sign to expand items in the tree. A plus (+) sign next to an item indicates that items may exist beneath them. When you select an item in the tree, the values relating to that selection are listed on the right window-pane. Click the **Edit** icon.
9. The General tab displays the **Name** of the CK722 component, as defined in SCT. You need to enter the **Query String** (if any). Click **Save**.
10. To configure alarm options for each of the CK722 components, refer to “Message Data Configuration Alarm Options” on page 114.

Time and Attendance Interface

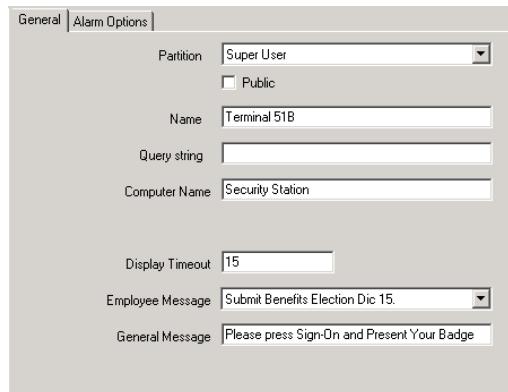
The **Work Scheduler** feature that is part of the *Time and Attendance* system has been designed to record and track an entity’s work schedule and attendance record, and can be integrated with a third party application, such as a payroll system.

The interface is configured using the third party application, and is operated from Web Access, where you can define a particular work schedule for an entity, broadcast a message that displays on the Time and Attendance terminal where the entity signs-on, and monitor the entity’s Time and Attendance status. Refer to the *Web Access Manual* for details. You must, however, use Message Data Configuration to configure additional information for the processing of Time and Attendance messages.

T&A Terminal Message Configuration

Message Data Configuration allows you to configure message processing associated with the Time and Attendance terminal where entities sign-on.

1. From the P2000 Main menu, select **Config>Message Data Configuration**. The Message Data Configuration window opens as a two pane window.
2. From the left window pane, select **T&A Terminal** and from the menu bar, select **File>New** or click the **New** icon. The left pane will display <**new**> and will show the name of the item once the record is saved.



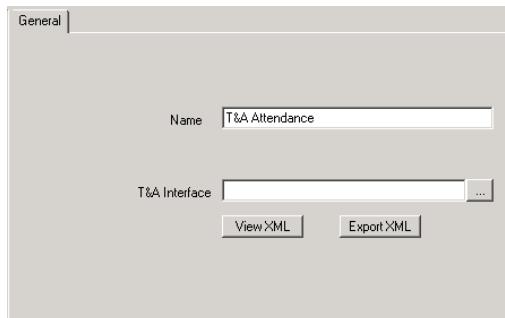
3. In the General tab, on the right side of the window, enter the **Partition** where the Time and Attendance Terminal resides.
4. Select the **Public** check box if you wish to make the Time and Attendance Terminal visible to all partitions.
5. Enter the **Name** of the Time and Attendance Terminal.
6. Enter the **Query String** (if any), associated with the Time and Attendance Terminal.
7. In the **Computer Name** field, enter the name of the station associated with the Time and Attendance Terminal.

8. In the **Display Timeout** field, enter the number of seconds the message will display in the Time and Attendance Terminal.
9. From the **Employee Message** drop-down list, select an employee message that will be broadcasted on the Time and Attendance Terminal. Employee Messages are created using User Defined Fields.
10. In the **General Message** field, enter the general message that will be broadcasted on the Time and Attendance Terminal.
11. Click **Save**.
12. To configure alarm options for each Time and Attendance Terminal, refer to “Message Data Configuration Alarm Options” on page 114.

Time & Attendance Object Message Configuration

Use to configure message processing associated with the Time and Attendance Object.

1. From the P2000 Main menu, select **Config>Message Data Configuration**. The Message Data Configuration window opens as a two pane window.
2. From the left window pane, select **Time & Attendance Object** and from the menu bar, select **File>New** or click the **New** icon. The left pane will display <new> and will show the name of the item once the record is saved.

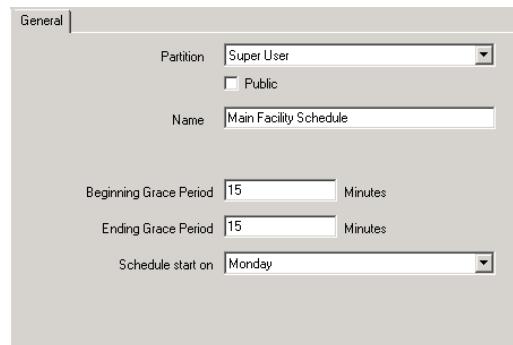


3. In the General tab, on the right side of the window, enter the **Name** of the Time and Attendance Object.
4. To use an optional interface, enter the name of the **T&A Interface** here, or click the browse [...] button to select a specific XML file from the list.
5. To view details associated with the T&A Interface file, click the **View XML** button. The Display XML window opens displaying information in XML format. Close the window.
6. To export the T&A Interface file, click the **Export XML** button.
7. Click **Save**.

Work Schedule Message Configuration

Use to define general rules associated with the Work Schedule.

1. From the P2000 Main menu, select **Config>Message Data Configuration**. The Message Data Configuration window opens as a two pane window.
2. From the left window pane, select **Work Schedule Object** and from the menu bar, select **File>New** or click the **New** icon. The left pane will display <new> and will show the name of the item once the record is saved.

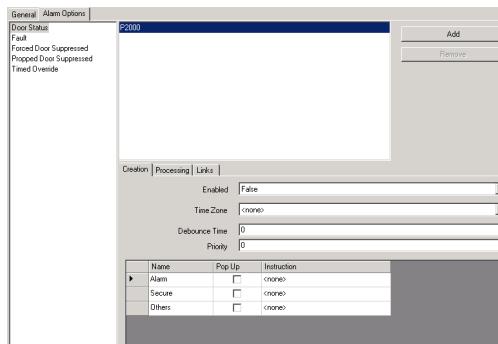


3. In the General tab, on the right side of the window, enter the **Partition** where the Work Schedule resides.
4. Select the **Public** check box if you wish to make the Work Schedule visible to all partitions.
5. Enter the **Name** of the Work Schedule.
6. In the **Beginning Grace Period** field, enter the number of minutes to be provided as the beginning grace period.
7. In the **Ending Grace Period** field, enter the number of minutes to be provided as the ending grace period.
8. Select from the **Schedule start on** drop-down list, the day of the week defined as the schedule start day.
9. Click **Save**.

Message Data Configuration Alarm Options

Please note that the options displayed on the right side of the window, depend on the selected item. For example, the Alarm Options tab will not be available, if the selected item cannot trigger an alarm. Also, the list of applicable alarm states varies depending on the selected alarm type.

Alarm Options Tab



The options listed on the right box depend on the item selected.

Alarm Category

The top right box allows you to assign an Alarm Category to the alarm that is generated by the selected item. Each alarm must belong to at least one Alarm Category (see “Alarm Configuration” on page 155 for details), but can also be assigned to multiple alarm categories, each with its own set of alarm options.

The P2000 Alarm Category will display by default. If you wish to assign this alarm to other alarm categories, click the **Add** button. The Alarm Category Selection dialog box opens displaying all previously created alarm categories (see page 155 for details).

If you use the Enterprise option, the Alarm Categories defined for all P2000 sites within an Enterprise system will be listed.

Select one or more categories and click the **Add** button. The list will display all the selected alarm categories.

To remove a category from the list, select the alarm category and click **Remove**.

Creation Tab

Creation														
Enabled	<input type="checkbox"/> False													
Time Zone	<none>													
Debounce Time	0													
Priority	0													
<table border="1"> <thead> <tr> <th>Name</th> <th>Pop Up</th> <th>Instruction</th> </tr> </thead> <tbody> <tr> <td>Alarm</td> <td><input type="checkbox"/></td> <td><none></td> </tr> <tr> <td>Secure</td> <td><input type="checkbox"/></td> <td><none></td> </tr> <tr> <td>Others</td> <td><input type="checkbox"/></td> <td><none></td> </tr> </tbody> </table>			Name	Pop Up	Instruction	Alarm	<input type="checkbox"/>	<none>	Secure	<input type="checkbox"/>	<none>	Others	<input type="checkbox"/>	<none>
Name	Pop Up	Instruction												
Alarm	<input type="checkbox"/>	<none>												
Secure	<input type="checkbox"/>	<none>												
Others	<input type="checkbox"/>	<none>												

Enabled – Select **True** if the alarm is added to the alarm queue and displayed in the alarm monitoring window to notify the operator of its activation. Select **False** if the item is unrelated

to alarm monitoring. For example, you can enable an alarm for a “Maintenance” alarm category and disable the same alarm for a “Security” alarm category. Select **Device** to use the setup defined at the specific device. This is not a recommended option.

Time Zone – Select from the drop-down list the time zone during which the item upon activation will be reported as an alarm in the Alarm Monitor window. If you select <**none**>, the item will be reported at any time once it is activated.

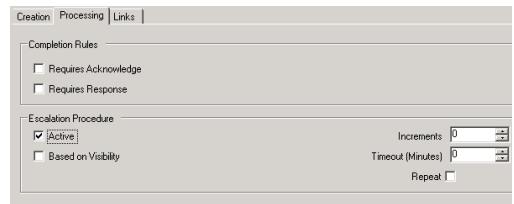
Debounce Time – If available, enter a delay time in milliseconds during which the alarm will not be generated.

Priority – Enter a value from 0 to 255. Zero equals the highest priority. This is the order in which the alarm message will be placed in the alarm queue. If alarm messages have the same alarm priority, the date and time determine which alarm is positioned higher in the queue.

Alarm Popup and Instruction – The list of alarms depends on the item selected. Select the line item you wish to define, and enable the **Popup** check box to allow the Alarm Monitor window to automatically display in front of all other windows on the screen whenever the item is in the alarm state. If Popup is not selected, the item is simply entered in the alarm queue. You should also select from the drop-down list the **Instruction Text** that will be displayed in the Alarm Response window when the item is in the alarm state. The Alarm Response window will display a set of instructions related to that particular alarm.

Before you can assign instruction text to the various popups, you must first create instruction text. See “Creating Instruction Text” on page 87 for more information.

Processing Tab



Completion Rules

Requires Acknowledge – Select this check box to require acknowledgement of this alarm before its completion.

Requires Response – Select this check box to require response to this alarm before its completion.

Escalation Procedure

The alarm escalation function constantly monitors all generated alarms that have their escalation options enabled. Escalation level value range is from 0 to 10, where 0 indicates a non-escalated alarm.

The alarm escalation feature provides for two different conditions when an alarm may be escalated:

- If an alarm is generated for a specific alarm category and there are currently no operators logged on to the P2000 system that have privileges to receive alarms for that category.
- If an alarm is generated and remains pending for the configured escalation timeout period.

If either of these conditions occurs, that alarm will be regenerated with an elevated escalation level. The escalation level will be incremented by the configured escalation increment value. This process may be repeated multiple times until a high enough escalation level is reached that matches the privileges of a currently

logged on operator. If no operators are logged on to the P2000 system, the alarm will be regenerated until the maximum escalation level is reached, and then no further action will be taken.

After an escalated alarm has been completed, the next occurrence of that alarm is created with no escalation level.

Active – Select this check box to enable alarm escalation.

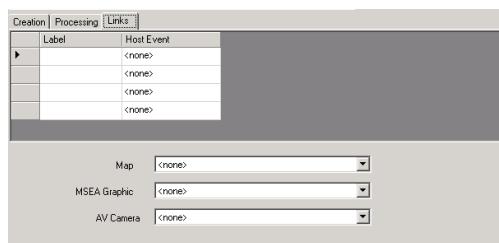
Based on Visibility – When this check box is selected, the alarm will be immediately escalated by a defined increment if, at the time of occurrence, no operator able to receive alarms from this Alarm Category is logged on.

Increments – Enter the value by which to escalate an alarm each time the escalation takes place.

Timeout (Minutes) – Enter the time period (in minutes) after which an alarm remaining in pending state will be escalated by the Escalation Increment.

Repeat – Select this check box to allow for escalation to occur more than once for the alarm. For example, if the Escalation Timeout is set to 30 minutes, and the Escalation Increment is set to 2, every half an hour the escalation value for alarms remaining in pending state will go up by 2 until it reaches the maximum value. If this check box is not selected, escalation can occur only once for this alarm.

Links Tab



Host Event 1-4 – You can define up to four events that can be triggered from the Alarm Monitor window whenever the items goes into an alarm condition and is entered into the alarm queue. Enter a descriptive event name in the **Label** box and select a previously configured Event from the associated drop-down list, see “To Activate an Event from the Alarm Monitor.” on page 162.

Map – Select the Real Time Map to be associated with this alarm. If applicable, this selection will override the default behavior of the Real Time Map containing the item. That is, when you click the Map button in the Alarm Monitor, the associated Real Time Map will be displayed, even if it is different from the Real Time Map containing the item.

MSEA Graphic – In facilities that use the Metasys System Extended Architecture (MSEA) option, this feature allows an alarm that is forwarded to MSEA to contain an embedded reference to a MSEA Graphic. For more information, see “Defining MSEA Graphics” on page 227. Select from the drop-down list the MSEA Graphic to reference in this alarm. When an alarm is received and displayed by Metasys, the Metasys operator can simply click the alarm to display the graphic item associated with the alarm and the item that caused the alarm.

AV Camera – If your facility uses the DVR option, select the camera to be associated with this alarm. If applicable, this selection will override the selection made in the Input to camera mapping window.

Set up Access Groups, Entity Options, and Security Roles

After you have configured your panels, terminals, terminal groups and various input and outputs, you are ready to complete system configuration by adding Access Groups, Entity Options, and Security Roles. While Access Groups and Security Roles are assigned from the System Configuration window, Entity Options are assigned via the P2000 Main menu. We recommend these elements be assigned in the following sequence:

- Access Groups
- Entity Options
- Security Roles

After these final elements are added, you are ready to move on to operating the system.

Create Access Groups

After terminals and terminal groups have been configured, you can group them together to create common access groups. For example, you can assign two terminals that control the doors into a common area, such as a ware-

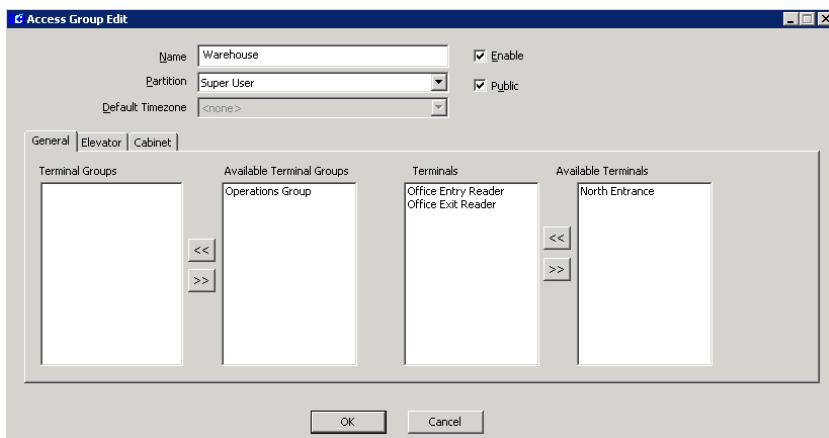
house, to an access group. When you assign an entity's access profile to that access group, the entity will be granted access to both doors in the group. This is a quick way to assign access to a large number of doors and areas.

If your system is configured to operate elevators and cabinets, elevator floors and cabinet doors can also be assigned to control which floors and doors an entity can access.

Once access groups are created, they will be accessible from the Access Profiles tab in Entity Management.

To Create an Access Group:

1. From the System Configuration window, select the **Access Groups** icon from the root system icons.
2. Click **Add**. The Access Group Edit dialog box opens at the General tab.
3. Enter a descriptive **Name** for the Access Group.
4. Select the **Enable** check box for the system to recognize this access group. If at any time you wish to temporarily disable access to any of the items in this group, without having to delete the access group, leave this box unchecked.



5. If this is a partitioned system, select the **Partition** name in which the items for this access group reside.
6. Select **Public** if you wish this Access Group to be visible to other partitions.
7. From the list of **Available Terminals** list at the far right of the dialog box, select the terminal you wish to include in the Access Group. This list includes all legacy readers and CK722 access control objects (ACOs) and door sequence objects (DSOs) defined in the system.
8. Click **<<** to move the terminal into the **Terminals** box.
9. From the **Available Terminal Groups** list, select the Terminal Group you wish to include in the Access Group. This list includes all legacy terminal groups, ACO terminal groups, and DSO terminal groups defined in the system.
10. Click **<<** to move it into the **Terminals Groups** box.
11. To add elevator floors to the Access Group, click the **Elevator** tab and select from the **Available Floor Groups** list, the Floor Group you wish to include in the Access Group.
12. To add cabinet doors to the Access Group, click the **Cabinet** tab and select from the **Available Door Groups** list, the Door Group you wish to include in the Access Group.
13. Click **OK**. The new Access Group will display under the root Access Groups icon. When you click the new Access Group icon, the parameters display on the right windowpane of the System Configuration window.

Entity Options

At a minimum, a first and last name must be entered into the Entity database for each person who will have access to your facility. Entity data entry is typically performed as part of system operation, which is described in detail in *Chapter 3: Operating the System*.

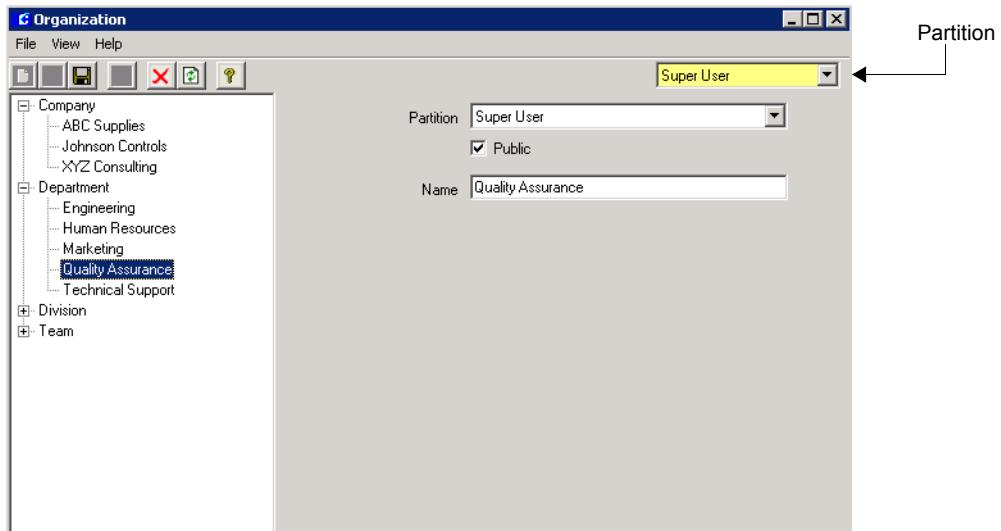
However, if your facility will take advantage of additional entity information, such as company and department definition, and any other information specific to each facility (defined in User Defined fields), these must be configured prior to adding entities, to make this information accessible from the Entity Management window.

You can also create access profile templates to speed entity data entry, as well as define identifier purposes to specify the identifier's intention. Complete instructions are presented in the following sections:

- **Define Organization**
- **Define Entity Categories**
- **Define Entity Groups**
- **Create Access Profile Templates**
- **Create User Defined Fields**
- **Define Identifier Purposes**

Define Organization Elements

The Organization feature allows you to define up to four organizational units labeled Company, Department, Division, and Team. These organizational units can be linked to entities, and can be used for sorting records or reporting entity activity. If your facility will include any of these organizational items as part of entity information, you must first configure these elements to make them available for assignment in the Entity Management window.



To Define Organization Elements:

1. From the P2000 Main menu, select **Config>Entity Options>Organization**. The Organization window opens.
2. The Organization window opens as a two-pane window. The left side displays the following four organizational units:
 - Company
 - Department
 - Division
 - Team
3. Select the unit you wish to define, and from the Organization menu bar, select **File>New** or click the **New** icon. The left pane will display <**new**> and will show the name of the item once the record is saved.
4. If this is a partitioned system, select from the **Partition** drop-down list, the partition to which the organizational item belongs.
5. If this is a partitioned system, select the **Public** check box to allow other partitions to see this record.
6. Enter the **Name** of the organization item.

7. Click the **Save** icon. The item will now be accessible from the Organization tab of the Entity Management window. Refer to the “Organization Tab” on page 136 for more information.

Note: The Partition drop-down list at the top right side of the window allows you to display and edit items that belong to the selected partition. In addition, you can also view other items that are marked as **Public** items, however the information is not accessible for modification.

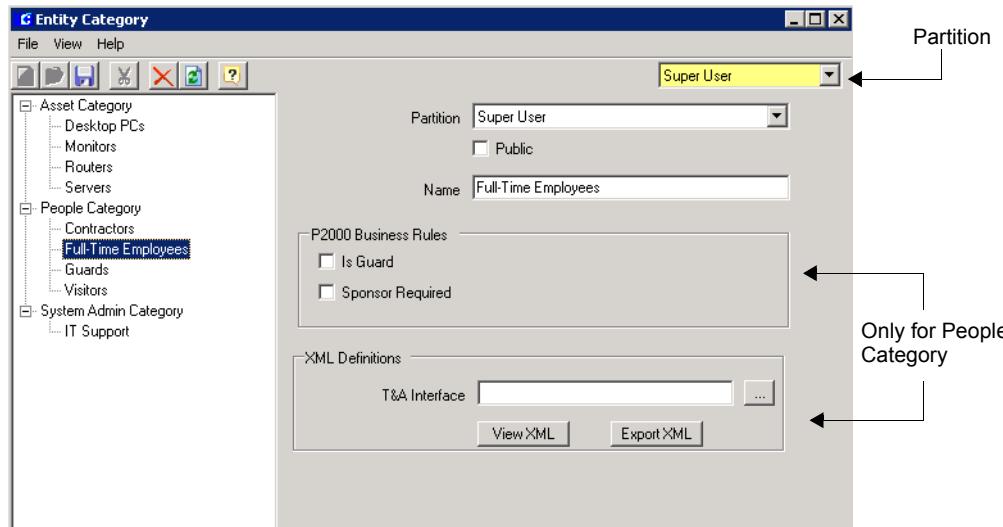
Define Entity Categories

You can define multiple entity categories for each of the three entity types: Asset, People, and System Admin. Once the categories are defined, you can assign them to entities in the Entity Management window for filtering and reporting purposes.

To Define Entity Categories:

- From the P2000 Main menu, select **Config>Entity Options>Entity Category**. The Entity Category window opens.
- The Entity Category window opens as a two-pane window. The left side displays the three entity types:
 - Asset
 - People
 - System Administrator
- Select the type of entity category you wish to define, and from the Entity Category menu bar, select **File>New** or click the **New** icon. The left pane will display <**new**> and will show the name of the item once the record is saved.
- If this is a partitioned system, select from the **Partition** drop-down list, the partition to which the entity category belongs.
- If this is a partitioned system, select the **Public** check box to allow other partitions to see this entity category.
- Enter the **Name** of the entity category.
- If your facility uses the Guard Tour option, you must enable **Is Guard** in the P2000 Business Rules box for entity categories that will be assigned to entities who participate in guard tour operations. Refer to “Guard Tour” on page 242.
- Enable **Sponsor Required** in the P2000 Business Rules box for entity categories that will be assigned to entities that are given temporary or limited access to the facility and that require a sponsor to take responsibility for them.
- Enter the name of the **T&A Interface**, or click the browse [...] button to select a specific XML file from the list.
- To view details associated with the T&A Interface file, click the **View XML** button. The Display Xml window opens displaying information in XML format. Close the window.
- To export the T&A Interface file, click the **Export XML** button.

Note: P2000 Business Rules and XML Definitions are only available for People Category.



12. Click the **Save** icon. The item will now be accessible from the General tab of the Entity Management window. Refer to the “General Tab” on page 133 for more information.

Note: The Partition drop-down list at the top right side of the window allows you to display and edit items that belong to the selected partition. In addition, you can also view other items that are marked as **Public** items, however the information is not accessible for modification.

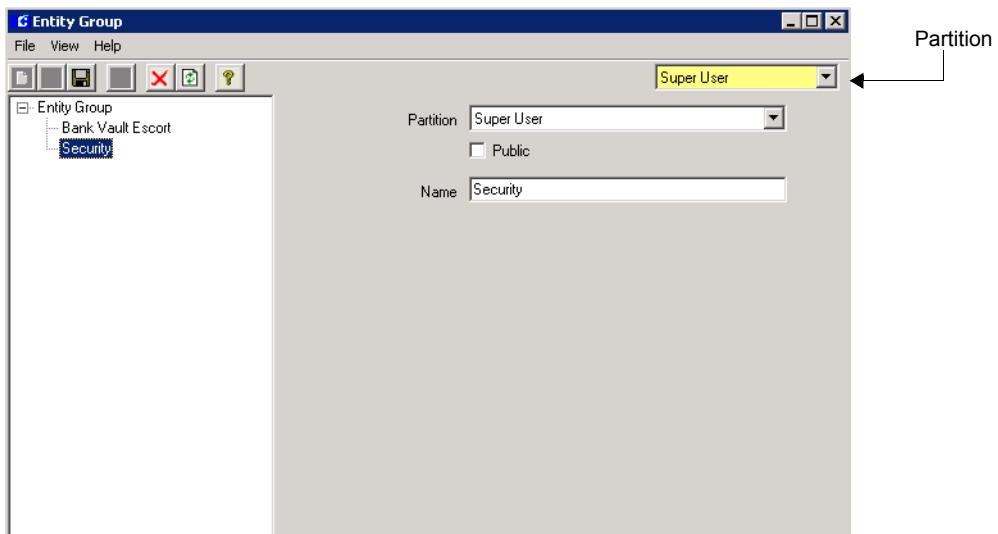
Define Entity Groups

Entity Groups ensure that a single person or asset is not left alone in a high security area. This feature allows persons and/or assets with similar access control requirements to be grouped together, requiring them to present their identifiers concurrently before being granted access to an area. In accordance to escort requirements (available only with CK722 panels), entities that are members of an Entity Group can only be granted access when the required members of the Entity Group are present at the door. To add or remove members

to/from the entity group, refer to “Entity Group Tab” on page 135.

To Define Entity Groups:

1. From the P2000 Main menu, select **Config>Entity Options>Entity Group**. The Entity Group window opens.
2. The Entity Group window opens as a two-pane window. The left side displays the root Entity Group entry.
3. Click the root Entity Group entry, and from the Entity Group menu bar, select **File>New** or click the **New** icon. The left pane will display <**new**> and will show the name of the item once the record is saved.
4. If this is a partitioned system, select from the **Partition** drop-down list, the partition to which the entity group belongs.
5. If this is a partitioned system, select the **Public** check box to allow other partitions to see this record.
6. Enter the **Name** of the entity group.
7. Click the **Save** icon. The entity group will now be accessible from the Entity Group tab of the Entity Management window.



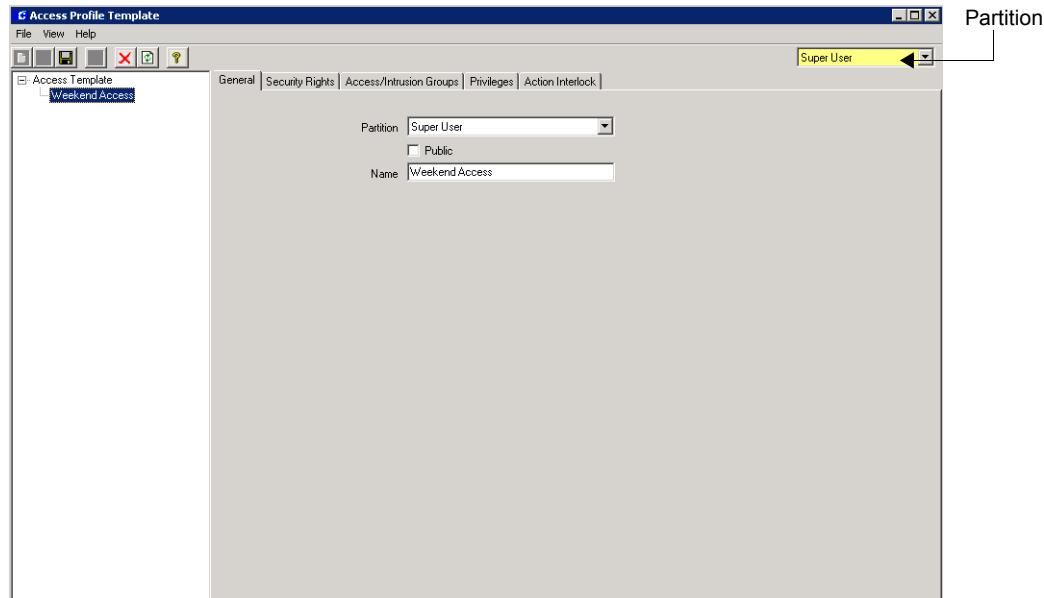
Note: The Partition drop-down list at the top right side of the window allows you to display and edit items that belong to the selected partition. In addition, you can also view other items that are marked as **Public** items, however the information is not accessible for modification.

Create Access Profile Templates

Access Profile Templates are an excellent tool for speeding the entry of entities into your system. You may have a large group of entities that need the same access privileges. For example, your entire Day Shift Shipping Department may need access to the same group of doors, time zones, and other access options. An Access Profile Template can be created to apply access groups and time zones to an identifier, simply by selecting the template from the Access Profiles tab in the Entity Management window, and then applying the Access Profile to the identifier. You can create a number of Access Profile Templates to speed entity data entry.

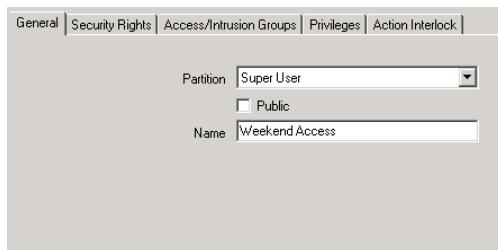
To Create an Access Profile Template:

1. From the P2000 Main menu, select **Config>Entity Options>Access Profile Templates**. The Access Profile Template window opens as a two-pane window. The left side displays the root Access Template icon.
2. Click the root Access Template icon, and from the Access Profile Template menu bar, select **File>New** or click the **New** icon. The left pane will display <**new**> and will show the name of the item once the record is saved.
3. The right side will display the tabs to complete the access template configuration. For details, refer to the definitions at the end of this section.
4. When you complete the access template configuration, click the **Save** icon. The Access Profile Template will now be accessible from the Access Profiles tab of the Entity Management window, see page 138 for details.



Note: The Partition drop-down list at the top right side of the window allows you to display and edit items that belong to the selected partition. In addition, you can also view other items that are marked as **Public** items, however the information is not accessible for modification.

General Tab

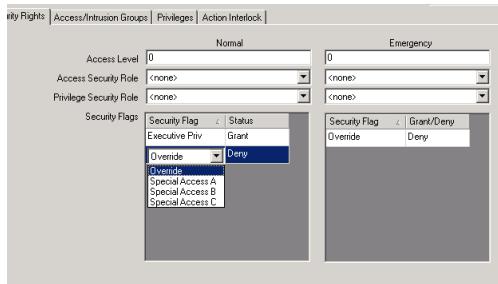


Partition – If this is a partitioned system, select the Partition in which this access profile template will be active.

Public – If this is a partitioned system, select Public if you wish this access profile template to be visible to all partitions.

Name – Enter a descriptive Name for the access profile template.

Security Rights Tab



Security rights determine whether or not an access request made by the entity will be granted or denied. The panels will make the access decision based on the rights assigned to

the entity. This tab allows you to define the access rights of an entity under normal and under emergency circumstances. In emergency situations, the system will switch the entity's normal access privilege to a set of alternative privileges without having to change the entity's rights, which may be time consuming during an emergency.

Access is granted or denied based on access levels and/or security roles.

Access Levels

Normal Access Level – Enter a normal access level from 0 (lowest) to 99. To obtain access at a door, this number must be equal to or greater than the Security Level set up for the terminal. If the Security Level at the terminal is raised, entities will be denied access, unless the access profile has the Executive privilege defined. Normal Access Level is considered an alternative access mode and is available only for CK722 panels.

Emergency Access Level – Enter an emergency access level from 0 (lowest) to 99. To obtain access at a door, this number must be equal to or greater than the Security Level set up for the terminal. If the Security Level at the terminal is raised, entities will be denied access, unless the access profile has the Executive privilege defined. Emergency Access Level control provides a rapid method of restricting access in case of an emergency and is available only for legacy (CK720, CK721, and CK705) panels.

Security Roles

Security roles are only available with CK722 panels. Entities can be assigned through their access profiles, two sets of security roles, one set for standard (**Normal**) operation and one set for elevated security (**Emergency**) operation.

Normal security roles are defined for normal daily access. **Emergency** security roles are

defined for temporary emergency situations. When an emergency is declared, the selected **Emergency** security roles become active and are used instead of the **Normal** roles.

To assign Security Roles through this access profile, select from the associated drop-down lists any of the previously defined Access or Privilege Security Role, refer to “Security Roles” on page 127 for detailed information.

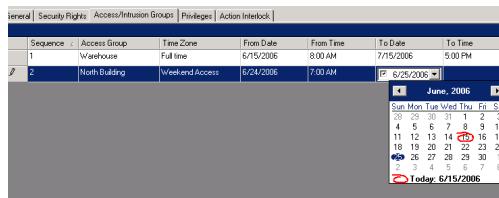
Access Security Role – Select from the drop-down list a previously defined Access Security Role. Select one for Normal and if you wish one for Emergency operation.

Privilege Security Role – Select from the drop-down list a previously defined Privilege Security Role. Select one for Normal and if you wish one for Emergency operation.

Security Flags – You can define security flags that override roles defined in the Access and Privilege security roles.

1. Right-click anywhere on the list box and select **Add**.
2. From the **Security Flag** drop-down list select the flag you wish to override.
3. From the **Status** drop-down list, select whether you wish to **Deny** or **Grant** the access based on the flag selected.

Access/Intrusion Groups Tab



Use this tab to define the Access/Intrusion Groups and corresponding Time Zones that will be assigned to this access profile template.

You can define an unlimited number of access/intrusion groups, but will only download up to 100 groups if using CK722 panels; up to eight access groups if using CK720/CK721/CK705 panels; and up to two access groups if using S321 panels.

1. In the Access/Intrusion Group tab, right-click anywhere on the list box and select **Add**. The **Sequence** column automatically assigns a number to the entry. This number indicates the sequence order in which the access/intrusion group will be downloaded to the panel.

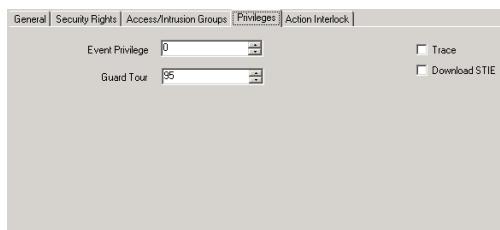
Note: To insert a group between two existing groups, you would select **Insert** instead of **Add**. You can also use “drag and drop” to change the position of a group within the list.

2. Select from the drop-down list, the **Access Group** you wish to assign to this access profile template.
3. Select from the drop-down list, the **Time Zone** that will be assigned to the selected access/intrusion group.
4. To define a temporary access period for the selected group, click the **From Date** field, select the check box and click the down arrow to select a start date from the system calendar when permission for access will be granted. If the check box is not selected, access will be allowed immediately.
5. Click the **From Time** field and click the spin box buttons to select the time when permission for access will be granted.

Note: For example, if the reader doors included in the Access Group normally grant access from 8:00 A.M. to 5:00 P.M., you can set up temporary access on a selected date and time period that will grant the entity permission for limited access within the normal time zone. This feature is performed by the Smart Download service and therefore, you can use it only when Smart Download is running, see “P2000 Services Definitions” on page 314. This feature only works on terminals running in Local mode.

6. Select from the **To Date** and **To Time** fields the date and time when permission for access will expire.
7. To remove an entry, select the line item, right-click and select **Delete**.

Privileges Tab



Event Privilege – Every access badge identifier has an event privilege level, ranging from 0 to 7, with zero as the lowest level. If an entity’s badge is to initiate a card event, his/her event privilege level must be equal to or greater than the privilege level defined in the Panel Card Event dialog box.

Guard Tour – This field is used if you have purchased the Guard Tour option. Select from the drop-down list a priority number from 1 (lowest) to 99. This number determines which tours the selected guard can perform. Only tour badges with equal to or greater than this priority can perform a tour.

Trace – If enabled, all identifier transactions associated with the entity’s access profile will

be traced and printed, as they occur, on any printer configured to print trace transactions, as long as the Badge Trace and Print options are selected in the Real Time List window.

Download to STIE – This option applies only to panels using STI-E terminal interfaces. If selected, the badge identifier is downloaded to the STI-E terminal. The STI-E terminal can save up to 1,000 badges in a resident database for use if the panel becomes inactive.

Action Interlock Tab

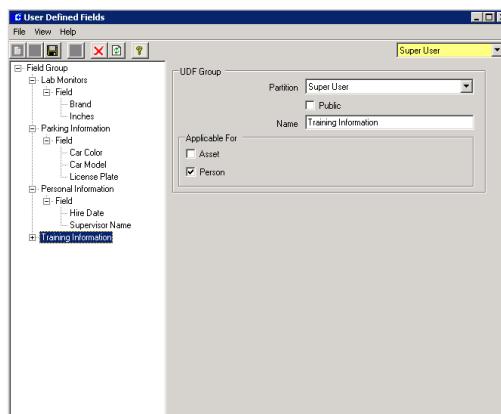
If your facility has purchased the BACnet option, the Action Interlock tab will display. Use this tab to allow badges that use this Access Profile Template to activate up to two action interlocks that will be triggered when the badge is granted access. For more information, refer to “Action Interlock Operation” on page 237.

Create User Defined Fields

With User Defined Fields (UDF) you can create data entry fields that will be available for entering a variety of optional information in the Entity Management window. User Defined Fields are created in groups, separately for Persons and for Assets. Each User Defined Field group can contain a set of fields that can store date, integers, strings, or boolean fields.

To Create User Defined Fields:

1. From the P2000 Main menu, select **Config>Entity Options>User Defined Fields**. The User Defined Fields window opens.

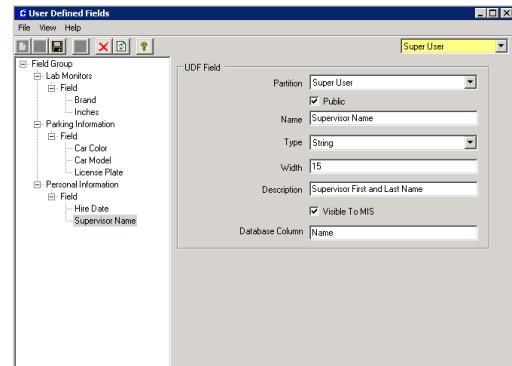


2. The User Defined Fields window opens as a two-pane window. The left side displays the root Field Group icon. Click the root **Field Group** icon, and from the User Defined Fields menu bar, select **File>New** or click the **New** icon.

The left pane will display <**new**> and will show the name of the group once the record is saved. The right pane will display the fields to create the UDF Group.

3. If this is a partitioned system, select from the **Partition** drop-down list, the partition to which the UDF Group belongs.
4. If this is a partitioned system, select the **Public** check box to allow other partitions to see this UDF Group.
5. Enter the **Name** of the UDF Group.
6. Select the associated check box to indicate whether this UDF Group will be applicable for **Assets** or **Persons**.
7. Click the **Save** icon. Continue creating the necessary UDF Groups.
8. Once the UDF Groups are created, click the plus (+) sign next to the root UDF Group wish to define. The **Field** icon will display.
9. Click the **Field** icon and from the User Defined Fields menu bar, select **File>New** or click the **New** icon.

10. The left pane will display <**new**> and will show the name of the field once the record is saved. The right pane will display the fields to create the user defined field.



11. If this is a partitioned system, select from the **Partition** drop-down list, the partition to which the user defined field belongs.
12. If this is a partitioned system, select the **Public** check box to allow other partitions to see this user defined field.
13. Enter the **Name** of the User Defined Field you wish to display as the field title when UDF is selected from the Entity Management window. Names must only contain alphanumeric characters, spaces or underscores, other characters are now allowed.
14. Enter the **Type** of format in which the information is to be displayed. Select either String, Integer (numeric), Boolean (toggle field), or Date from the drop-down list.
15. In the **Width** field, enter the maximum number of characters to be allowed in this field. If you selected the String format, you can enter up to 255 characters; for the Integer format, you can enter up to 9 characters.

Note: The **Type** and **Width** fields cannot be modified after the entry is saved.

16. Enter a **Description** of this field.

17. By default, all UDF fields become automatically part of the MIS tables. If you do not wish to display this field in the MIS Interface tables, clear the **Visible To MIS** check box.
18. Enter the name of **Database Column** to which the user defined field belongs. This field is used to supply your own column name to the UDF. If you leave it blank, the UDF name is the column name.
19. Click the **Save** icon. The new user defined field will be added under the corresponding UDF Group and will now be accessible from the Miscellaneous tab of the Entity Management window, see page 138.

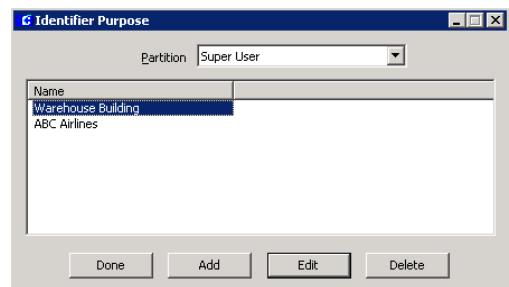
Note: The Partition drop-down list at the top right side of the window allows you to display and edit items that belong to the selected partition. In addition, you can also view other items that are marked as **Public** items, however the information is not accessible for modification.

Define Identifier Purposes

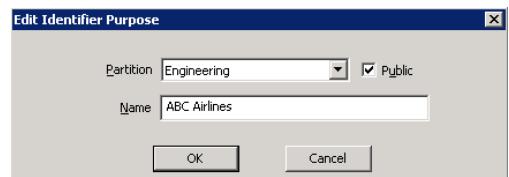
Users can assign a purpose to an identifier, for example to specify the identifier's intention. The Purpose field can be used for different applications. For example, an airport employee may have multiple identifiers, one for each airline terminal he is allowed to access. The Purpose field for each identifier could be used to identify the airline where the identifier is valid. Use the Identifier Purpose tool to create the different Purpose field values that will be available for assignment in the Identifier tab of the Entity Management window.

To Define Identifier Purpose Fields:

1. From the P2000 Main menu, select **Config>Entity Options>Identifier Purpose**. The Identifier Purpose dialog box opens.



2. Click **Add**. The Edit Identifier Purpose dialog box opens.



3. If this is a partitioned system, select the **Partition** to which this identifier purpose field belongs and select **Public** if you wish this purpose field to be visible to all partitions.
4. Enter the **Name** of the identifier purpose.
5. Click **OK** to save the record.
6. Click **Done**. This purpose field will be available from the Identifier tab of the Entity Management window.

Security Roles

Security roles are used with CK722 panels and are assigned to each entity (through Access Profiles). These roles can determine whether or not an access request made by the entity will be granted or denied. The P2000 system allows you to define different set of roles for different situations. You can for example, give certain people override privileges at certain doors, while giving other override privileges at other doors. In addition, in the event of an emergency, you can quickly change the normal

privileges assigned to the entity to an alternative set of emergency privileges.

Security roles consists of 100 security flag records, which are automatically generated during initial installation. The first five security flag records are reserved for mapping badge privileges options used in previous versions of P2000, refer to “Legacy Privilege Flags Tab” on page 41 for details.

The following sections describe how to define the Security Flags that will be used throughout the system, as well as the Access Roles and Privilege Roles that will be assigned to the entities through Access Profiles.

Security Flags

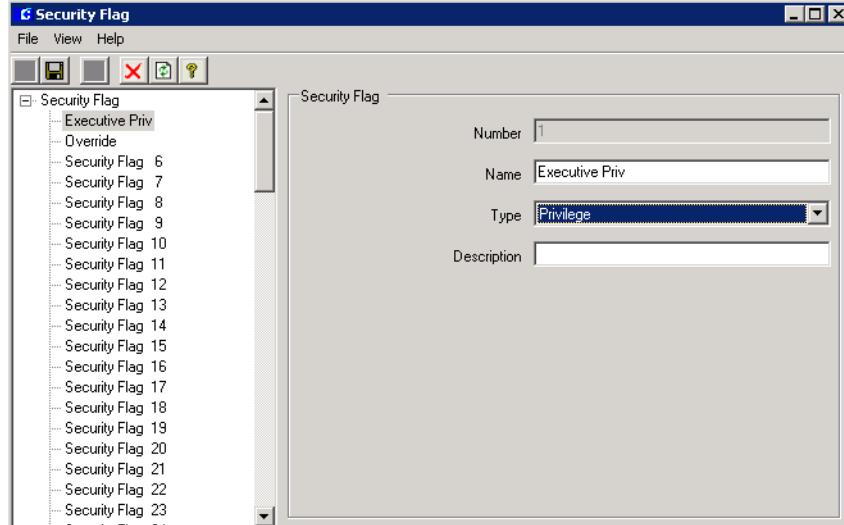
This application allows you to define the security flags that will be used throughout the system. The CK722 panel allows 100 flags, while CK705, CK720, and CK721 panels allow flags 1 to 5. You can modify the name of each security flag according to your system needs, define each security flag as an Access or Privilege role, and then associate these roles with multiple access profiles, which are then

assigned to entities with the purpose of granting or denying access requests.

Security Flags apply to all P2000 sites within an Enterprise system.

To Define Security Flags:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the plus (+) sign next to the root **Security Flag Mask** to display the security items.
3. Click the **Security Flags** icon, then click **Edit**. The Security Flag dialog box opens.
4. Click the Security Flag you wish to define, and from the Security Flag menu bar, select **File>Edit** or click the **Edit** icon.
5. The **Number** field displays the number that is automatically assigned to the selected Security Flag.
6. The **Name** field displays the default name of the selected Security flag. You can modify the name according to your configurations.



- From the **Type** drop-down list, select whether this security flag will be used as a **Privilege** or as an **Access** role.

Once the entry is saved, and you modify the defined Type ...

from	to	then the security flags will be removed from
Access	Privilege	Access Roles
Access	Unknown	Access Roles, Access Profiles, Access Templates
Privilege	Access	Privilege Roles
Privilege	Unknown	Privilege Roles, Access Profiles, Access Templates.

- Enter a **Description** of the Security Flag.
- Click the **Save** icon. The security flag will be available for selection in the Privilege or Access role list. Refer to the following section.

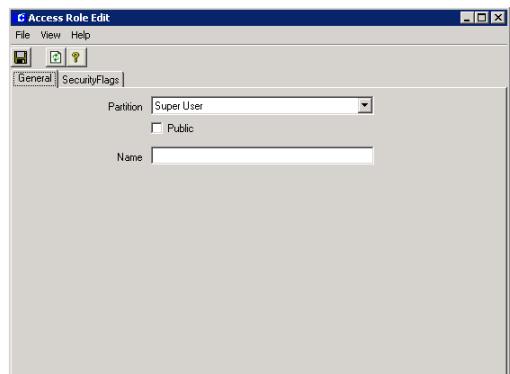
Access Security Roles

This application allows you to define the access security roles that will be available for assignment using Access Profiles.

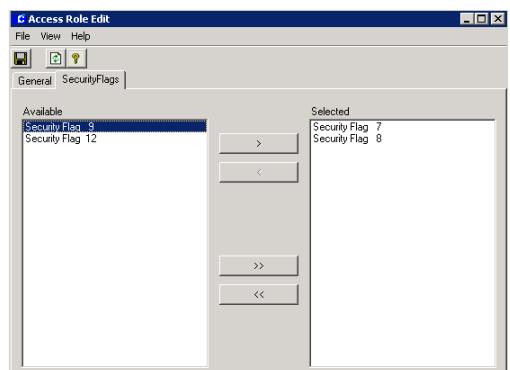
An access role consists of any combination of the predefined access security flags. You can create an unlimited number of access roles, which can be used multiple times throughout the system.

To Define Access Security Roles

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the plus (+) sign next to the root **Security Flag Mask** to display the security items.
- Click the **Access Security Role** icon, then click **Add**. The Access Role Edit dialog box opens at the General tab.



- If this is a partitioned system, select the **Partition** in which this access security role will be active.
- If this is a partitioned system, select **Public** if you wish this access security role to be visible to all partitions.
- Enter a descriptive **Name** for the access security role.
- Click the **Security Flags** tab.



- The list displays the security flags that were defined as Access roles using the Security Flags application, see page 128. Select the role to be included in the Access Role and move it to the Selected box.
- Click the **Save** icon. The access security role will be available for assignment using Access Profiles.

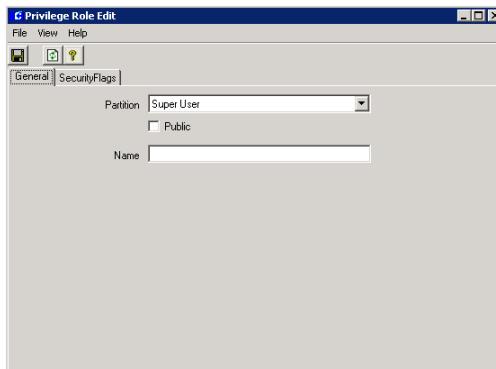
Privilege Security Roles

This application allows you to define the privilege security roles that will be available for assignment using Access Profiles.

A privilege role consists of any combination of the predefined privilege security flags. You can create an unlimited number of privilege roles, which can be used multiple times throughout the system.

To Define Privilege Security Roles

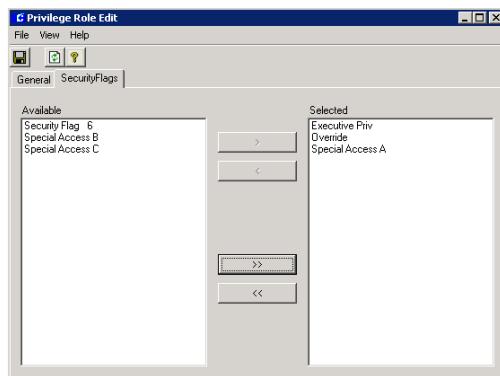
- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the plus (+) sign next to the root **Security Flag Mask** to display the security items.
- Click the **Privilege Security Role** icon, then click **Add**. The Privilege Role Edit dialog box opens at the General tab.



- If this is a partitioned system, select the **Partition** in which this privilege security role will be active.
- If this is a partitioned system, select **Public** if you wish this privilege security role to be visible to all partitions.

- Enter a descriptive **Name** for the privilege security role.

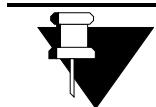
- Click the **Security Flags** tab.



- The list displays the security flags that were defined as Privilege roles using the Security Flags application, see page 128. Select the role to be included in the Privilege Role and move it to the Selected box.
- Click the **Save** icon. The privilege security role will be available for assignment using Access Profiles.

Entering Entities

After all configuration elements have been defined; along with companies, departments, and user defined fields, if applicable; you are ready to enter entities into the database. See “Entering Entity Information” on page 132 for more detailed information.



APPLICATION NOTE

Commissioning the System: When commissioning the system, we recommend you create at least one or two entity records, including access profiles and badge identifiers; then swipe these badges to ensure door controls are working properly.

Chapter 3: Operating the System

This chapter describes procedures typically performed by operators of the *P2000 Security Management System*, assuming all system configuration has been completed. (System Configuration is described in Chapter 2; if it has not been completed, some of the functions described in this chapter will not be ready to operate.)

Operations typically performed as part of system maintenance; such as downloading data, updating software and panels, starting and stopping service control, and reviewing system and workstation status; are typically performed by a system administrator and are described in *Chapter 5: System Maintenance*.

The following sections describe how to:

- **Create entities and identifiers**
- **Monitor alarms**
- **Manually control doors, outputs, panel relays, security threat levels, and suppress inputs**
- **Control areas and muster zones**
- **Detect and control intrusion in a facility**
- **Create events**
- **Monitor the system in Real Time**



All configuration steps outlined in Chapter 2: Configuring the System, must be completed before you can program and use the essential functions described in this chapter AND some system features require specific configuration settings before others can be enabled. These are described in the appropriate sections that follow.

Entity Management

An entity is a Person, Asset or System Administrator entered in the P2000 system to define their existence in a facility. You can monitor the location of Persons and Assets, and provide or deny them access to defined areas of the facility based on their access profiles. Persons and System Administrators can be provided with “user” access to operate the P2000 software or Web interface; and in the case of System Administrators, interface with another system (e.g. MIS interface). These entity types serve to categorize entities at a high level.

Access privileges define which entities may enter a specific area of the facility, and at what time they may enter. Access privileges are assigned to individual reader terminals and/or group of reader terminals, including ACO and DSO objects within CK722 panels; these devices are assigned to specific access groups, and then when entity records are added to the Entity database, the entities are assigned to the access groups using access profiles.

The Entity Management application provides flexible tools to create entities and assign identifiers with which to grant or deny facility access. At a minimum, a first and last name must be entered into the Entity database for each person who will have access to your facility. Additional entity information can include personal information such as address and phone; organization information such as a company name and department; a Photo ID; and any additional information such as eye color, height, weight, or other information you can define in User Defined Fields.



APPLICATION NOTE

MIS Interface: Entity information of type Person or Asset can be added, deleted, or updated from a database outside the P2000 software using the optional MIS Interface. See "MIS Interface" on page 231 for more information. This option requires programming and should be performed only by trained IS personnel.

Entering Entity Information

Every person or asset who needs access to the facility must have an Entity, Access Profile, and Identifier record entered into the P2000 system. Entities can be entered all at once at system startup, and then added, edited, or removed as necessary thereafter.

If you use database partitioning, an entity can belong to one partition and the associated identifiers can belong to multiple partitions with different access parameters.

An entity may have a number of different identifiers; however, if your facility uses legacy panels, each access badge identifier must have a unique number.

Viewing Entity Information

1. Select **Access>Entity Management** from the P2000 Main menu to display the Entity Management window.
2. To view the entities in a specific order, click the desired column header in the list box. The list will be sorted by the selected column.

Note: The system displays up to 20,000 entities at a time, for the partition and/or Enterprise Site selected. If the number of entities in your system exceeds 20,000, you must use the Filter feature, described in "Filtering Entity Data" on page 151.

The screenshot shows the Entity Management window with the following details:

- Enterprise Site:** Set to "Enterprise".
- Partition:** Set to "Super User".
- Table Headers:** Name, First Name, Middle Name, Description, Entity Type, Entity Categ., Partition, Public, Company, Division, Departm.
- Table Data:**

Engineering			Test Equipment	Asset	Laptop	Super User	<input type="checkbox"/>	XYZ Inc.	South Region	Engineer
Evans	Jeff	T.		Person	Guard	Super User	<input type="checkbox"/>	XYZ Inc.	West Region	Security
Jackson	Peter	B.		Person	Tenant	Super User	<input type="checkbox"/>	ABC Industrie	West Region	Engineer
Jasper	Jeannette	A.		Person	Tenant	Super User	<input checked="" type="checkbox"/>	DHL Inc.	South Region	Sales
Jones	Tom	R.		Person	Tenant	Super User	<input type="checkbox"/>	ABC Industrie	South Region	Sales
- Detail View:** Shows Jasper's information with fields: Partition (Super User), Entity Type (Person), Entity Category (Tenant). It also shows a thumbnail image of Jeannette, her first name (Jeannette), middle initial (A), last name (Jasper), Date/Time Created (3/3/2006 9:57:08 AM), and ID (375).
- Right Panel:** A tree view labeled "P2000Site" showing the hierarchy of sites.

Entity Types

When adding an entity to the P2000 database, you must select an entity type before any other data can be entered. Once the entity record is saved, the entity type cannot be changed. A P2000 entity may be one of the following types:

Person – This is any person who is granted access to the facility and can be configured as a P2000 User to perform system functions.

Asset – This entity type allows you to track the location of physical assets in the facility and who these assets are currently assigned to.

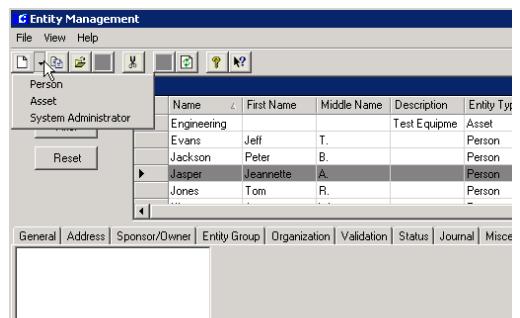
System Administrator – This entity type allows the configuration of system accounts, such as P2000 User accounts or MIS interface accounts.

Additional Entity Data

When you select an entity from the list, additional entity data such as Address, Organization, and Miscellaneous information, is displayed in the tabs in the middle of the Entity Management window. The tabs displayed depend on the type of entity selected; and certain features within each tab will be enabled/disabled depending on the panel type used. If your facility has purchased the P2000 Enterprise option, a drop-down list will be added at the top of the window (second list from the left), which allows you to select entities that belong to the selected Site name.

To Enter New Entity Information:

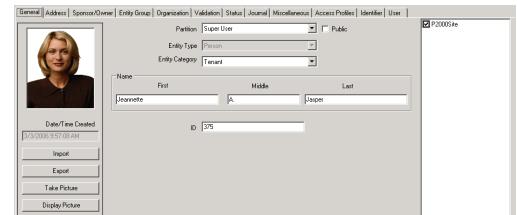
- From the Entity Management window menu bar, select **File>New** and select **Person**, **Asset**, or **System Administrator**. As an alternative, you can click the down arrow next to the **New** icon and make your selection.



- Enter the information as described in the Entity Field Definitions.
- You may click the **Save** icon at any time to save your settings, and then click the **Edit** icon to continue working on the record. When you finish click the **Save** icon, the name of the newly added entity will display highlighted in the list box.

Entity Field Definitions

General Tab



Partition – If this is a partitioned system, select from the drop-down list the Partition to which this entity is assigned.

Public – If this is a partitioned system, select the Public check box if you wish this entity record to be visible to all partitions.

Entity Type – This field displays the entity type selected.

Entity Category – Select an Entity Category to be assigned to this type of entity. Refer to

“Define Entity Categories” on page 119 for details.

First – If the Entity Type is Person, enter the first name of the entity.

Middle – If the Entity Type is Person, enter the middle name of the entity.

Last – If the Entity Type is Person, enter the last name of the entity.

Note: *If the Entity Type is Asset or System Administrator, enter the Name and Description of the entity.*

ID – Enter a unique ID for this entity (up to 25 characters).



APPLICATION NOTE

Entity ID: *It will be helpful to develop an identification numbering system for entities and identifier numbers BEFORE you begin entering entity information. Entity ID (not to be confused with Identifier Badge Number) is optional; however, it can be useful, depending on your organization and reporting requirements. For example, the Entity ID can correspond to an employee ID, social security, or building number, and then be used in creating custom reports sorted by those numbers.*

Enterprise Sites

If your facility has purchased the P2000 Enterprise option, the Enterprise box on the right side of the window will display all the sites defined in the system. Select the check box next to the site that this entity may access. Refer to “P2000 Enterprise” on page 291.

Adding an Entity Image

You can import an existing image to display in the General tab. The P2000 system supports a

large number of image formats; however, if your image format is not supported, you may need to use an image-editing program to convert to a supported format.

If the workstation is configured as a badging workstation, you can use the Badging buttons to capture an image. See “Video Imaging” on page 227 for details.

Address Tab

General		Address		Sponsor/Owner	Entity Group	Organization	Validation	Status	Journal	Miscellaneous	Ax
State	Suite 100	Street	435 W. Third Street								
City	Sacramento	State	CA	ZIP Code	95888						
Country	USA			EMAIL	Jasper@xxx.com						
				Phone	(800)111-2222						
				Extension	3333						

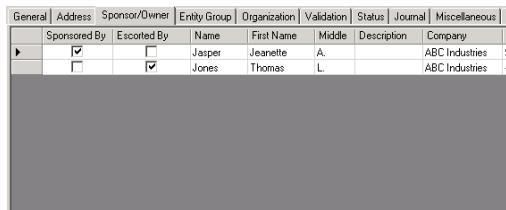
Use this tab to enter the primary address of a Person or Asset. For entities of type *Person*, this could be their private or company address. For entities of type *Asset*, this could be their normal “home” location. In addition, you can also enter email, and phone information, if desired.

Sponsor/Owner Tab

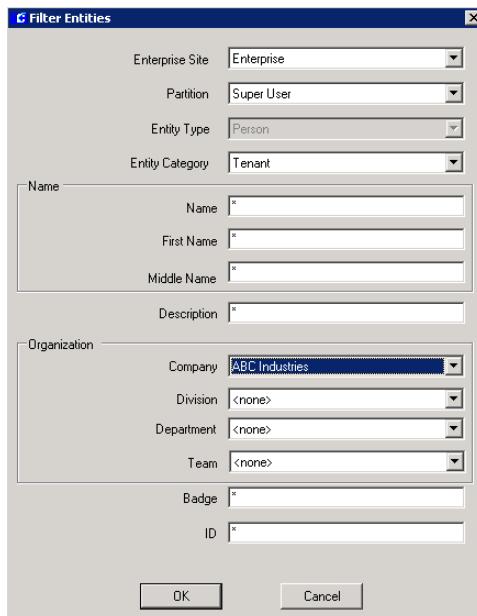
This tab is available when defining Persons and Assets that are given temporary or limited access to the facility and that require a company sponsor or owner to take responsibility for them while in the facility. A typical example is a temporary employee (person) who requires a sponsor such as a supervisor, or a piece of equipment (asset) that requires an entity person to be assigned as the owner of that asset.

For the most part, assigning sponsors/owners is optional, unless the entity is a person that

belongs to an Entity Category defined with a “Sponsor Required” business rule. Refer to “Define Entity Categories” on page 119.



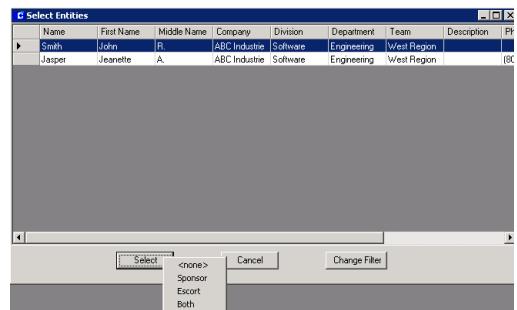
- In the Sponsor/Owner tab, right-click anywhere at the bottom of the window and select **Add**.



- Enter the necessary information in the Filter Entities dialog box and click **OK**.

Note: Enterprise Site and Partition filters will display if your facility has those options.

The Select Entities dialog box opens displaying the entities that match your filter criteria.

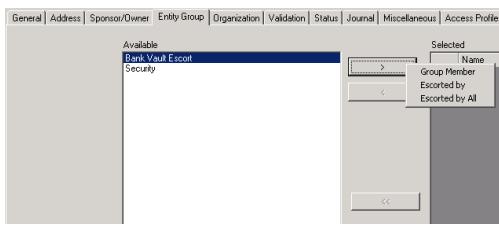


- Select the desired name and click the **Select** button at the bottom of the screen, then select one of the following options:
 - None** – The selected person can be later defined as a sponsor, escort, or both.
 - Sponsor** – The selected person will take responsibility of the entity while in the facility.
 - Escort** – The selected person will serve as an escort for the entity and will be required to present an identifier together with the entity to gain access at a door (depending on the Access Profiles assigned). Escort operation depends on the CK722 Access Control Object (ACO) configuration. For more information, refer to the *CK722 Commissioning Guide*.
 - Both** – The selected person will act as the Sponsor and the Escort of the entity.
- The selected name is inserted in the list box under the Sponsor/Owner tab. You may assign as many sponsors/owners as you wish and you may select or unselect the **Sponsored By** and/or **Escorted By** check boxes as needed.

Entity Group Tab

Entity Groups ensure that a single person or asset is not left alone in a high security area. This feature allows persons and/or assets with similar access control requirements to be

grouped together, requiring them to present their identifiers concurrently before being granted access to an area. In accordance to escort requirements (available only with CK722 panels), entities that are members of an Entity Group can only be granted access when the required members of the Entity Group are present at the door.



To be a member of an Entity Group select from the **Available** box a previously defined Entity Group, see page 121. Click the drop-down arrow and select one of the following choices:

Group Member – The entity is assigned to the selected Entity Group.

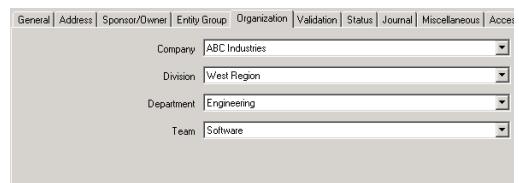
Escorted by – The entity is not a member of the group, but for the entity to be granted access, the entity must be escorted by at least one member of the selected Entity Group.

Escorted by All – The entity is a member of the group, and for the entity to be granted access, the entity must be escorted by all members of the selected Entity Group. Entities that are members of this group are required to enter a controlled area together. All entities must present and identify themselves within a defined period of time to be granted access.

Note: *Escort operation depends on CK722 Access Control Object configuration and the Access Profiles assigned to the entity.*

Organization Tab

Organization elements do not provide any access control or transaction processing functions; they are assigned to entities for reporting purposes only. You must define Organization elements before the selections will display in the drop-down lists. See “Define Organization Elements” on page 118 for detailed information.



To include Company, Division, Department and/or Team information in the Entity database, select a previously defined element from the associated drop-down list.

Validation Tab

This tab displays the validation range for each entity. This feature is typically used for temporary or visitor entities, but can also be edited as needed, for example to temporarily disable an entity without having to delete the entity record.

The validation date determines the validity of the entity record, and not when access becomes active or inactive, which is based on the entity’s access profile. However, the validation date range takes precedence over the access profile date range, meaning that the system will automatically void all access profiles and associated identifiers on the end date specified in this tab.

The screenshot shows the Validation tab of a software interface. It includes tabs for General, Address, Sponsor/Owner, Entity Group, Organization, Validation, Status, Journal, and Miscellaneous. Under the Validation tab, there are two date/time input fields: 'Valid From' (set to 1/17/2006 at 1:54:18 PM) and 'Valid To' (set to 1/17/2016 at 1:54:20 PM).

Valid From – This is the date and time that the entity becomes active. Select the check box and click the down arrow to select a start date from the system calendar. If you selected a start date, the time field is enabled. Click the spin box buttons to select the time that the entity will be activated.

Valid To – This is the date and time that the entity will be voided. Select the check box and click the down arrow to select an end date from the system calendar. The system will automatically void the entity on the date specified. If you selected an end date, the time field is enabled. Use the spin box arrows to select the time that the entity will be voided.

Status Tab

The Status tab displays the most recent identifier activity associated with the entity, based on the location of the reader where the identifier was last presented. You can display status information occurring at the local site as well as at any other enterprise sites (if applicable) that the entity is allowed to access. The status information displayed for enterprise sites shows last replicated data.

To display status information, select the desired site from the left box and click one of the following tabs:

Transaction – Select the Transaction tab to display the last valid and/or invalid transaction associated with the entity. This tab will display the date/time, transaction type and location where the identifier was last presented.

The screenshot shows the Mustering tab of a software interface. It includes tabs for General, Address, Sponsor/Owner, Entity Group, Organization, Validation, Status, Journal, and Miscellaneous. Under the Mustering tab, there is a table with columns for Type (Valid, Invalid), Date/Time, Reader Used, and Transaction.

Mustering – Select the Mustering tab to track entity movement in the event of an emergency. This tab will display the muster zone name and status of the entity (mustered, trapped, sequestered, etc.). For details see “Mustering” on page 186.

The screenshot shows the Area tab of a software interface. It includes tabs for General, Address, Sponsor/Owner, Entity Group, Organization, Validation, Status, Journal, and Miscellaneous. Under the Area tab, there is a table with columns for Type and Zone.

Area – Select the Area tab to track entity movement in specific controlled areas. This tab will display the area name, the type of area (access, facility, or parking), the date/time, and location where the identifier was last presented. For details see “Area Control” on page 178.

The screenshot shows the Journal tab of a software interface. It includes tabs for General, Address, Sponsor/Owner, Entity Group, Organization, Validation, Status, Journal, and Miscellaneous. Under the Journal tab, there is a table with columns for Type, Area, Date/Time, and Terminal.

Journal Tab

Journal entries supplement entity information by storing notes associated with each entity. For example, you may want to keep track of persons with parking violations, or keep a record of employees that attended specific company training, or track tenants with suspicious behavior.

You can also add notes for assets, such as serial numbers for computer equipment or keep a maintenance record of company cars.

The screenshot shows the Journal tab of a software application. On the left, a list box displays two entries: "1/18/2006 10:50 AM Vacations" and "3/3/2006 10:30 AM PC Training". To the right, a text area contains the message: "On vacations for two weeks starting 2/15/06." Below this, a large grayed-out area represents the rest of the window.

General | Address | Sponsor/Owner | Entity Group | Organization | Validation | Status | Journal | Miscellaneous

On vacations for two weeks starting 2/15/06.

General | Address | Sponsor/Owner | Entity Group | Organization | Validation | Status | Journal | Miscellaneous | Access Profiles |

Parking Information

Car Color	Green
Car Model	Ford
Plate Number	123456

Personal Information

Hire Date	11/28/2004
Job Classification	63
Supervisor Name	Jeff Evans

Training Information

Job Classification
Get information from HR.

Click to expand

- In the Journal tab, right-click anywhere on the list box located on the left side of the window and select **Add**. The current date and time automatically displays in the **Date** column.
- Enter a descriptive **Title** to identify the subject of this note.
- Click on the text area (right side of the window), and enter the details of the note.
- Add or edit journal entries as desired. The list box on the left side lists all available journal entries for the entity with the date and time when the journal was entered. After selecting an entry in the list box, the associated text displays on the right window.
- To delete a note, select the note from the list, right-click and select **Delete**.
- When you finish entering journals, click the **Save** icon.

Miscellaneous Tab

If you created User Defined Fields (UDFs) using the Entity Options menu, these fields are accessible from the Miscellaneous tab. Groups of UDFs must be previously defined separately for Persons and Assets. See “Create User Defined Fields” on page 125.

- Click the **Miscellaneous** tab. The fields on this tab are separated by Field Groups and will display according to the type of entity (Persons or Assets) selected.
- Click the plus (+) sign next to a Field Group title to display all fields under that group, then enter the information for each field. Use the Up and Down keys to navigate between cells. The box at the bottom of the window shows a description of each field.

Access Profiles Tab

Access Profiles define the access rights of an entity. You can define access profiles for a person or asset, and then associate their identifiers with the access profile. If an entity loses an identifier, the administrator will not be required to define new access rights, but associate the replacement identifier with the defined access profile.

Multiple access profiles can be associated with one entity, and one access profile can be applied to multiple identifiers.

The screenshot shows the Access Profiles tab. A table on the right lists a single row for "Daily Access". The "From" field is set to "1/18/2006 11:07:53 AM" and the "To" field is set to "1/18/2007 11:07:54 AM". The "Partition" dropdown is set to "Super User". The "Public" checkbox is checked. The "Name" field contains "Daily Access".

General | Address | Sponsor/Owner | Entity Group | Organization | Validation | Status | Journal | Miscellaneous | Access Profiles |

Daily Access

Partition	Super User
<input checked="" type="checkbox"/> Public	
Name	Daily Access
From	1/18/2006 11:07:53 AM
To	1/18/2007 11:07:54 AM

The list box on the left side of the window presents all access profiles created for the entity. To create an Access Profile, right-click on the list box and select **Add**. The list box will display <new> and will display the name of the Access Profile once the record is saved. The Access Profiles tab presents a General tab and a tab displaying the local site name.

Note: If your facility has purchased the P2000 Enterprise option, additional tabs will display the enterprise site name tabs that the entity may access. Refer to "Define Global Access Rights" on page 294.

Access Profiles - General Tab

This screenshot shows the 'General' tab of the Access Profiles interface. It includes fields for 'Partition' (set to 'Super User'), 'Name' (set to 'DailyAccess'), and two time/date fields: 'From' (1/18/2006 at 11:07:53 AM) and 'To' (1/18/2007 at 11:07:54 AM). There is also a checkbox for 'Public' which is checked.

Partition – If this is a partitioned system, select the Partition in which this access profile will be active.

Public – Select Public if you wish this access profile to be visible to all partitions.

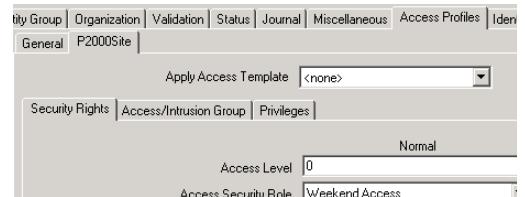
Name – Enter a descriptive name for this access profile. Names must be unique within each entity.

From – Select the date and time that the access profile becomes active. All identifiers using this access profile will be activated on this date. Click the down arrow to select a date from the system calendar and click the spin box buttons to select a time.

To – Select the date and time this access profile will be automatically voided. All identifiers using this access profile will be voided on this

date. Click the down arrow to select a date from the system calendar and click the spin box buttons to select a time.

Access Profiles - Local Site Tab



Apply Access Template – If a large number of entities will use access profiles with the same options, you can set all these options at once by applying an Access Profile Template. The Access Profile Template contains preset access options, access groups, time zones, etc. All entities that use the same Access Profile Template will use the same options and you can edit the options individually after the template is applied to suit the needs of individual entities; however, if you re-select the template, the settings will again mirror the access template options. In addition, if you make changes to an Access Profile Template, you will have to re-select the template to apply the new settings.

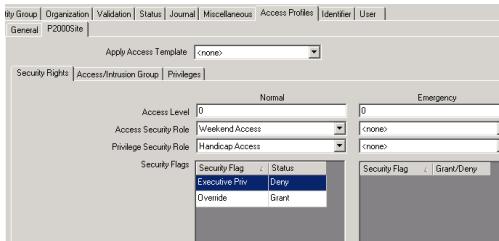
Note: Access Profile Templates must first be created before they are available in the Access Profiles tab. For more information, see "Create Access Profile Templates" on page 122.

Use the following tabs if you wish to override the settings applied from the Access Profile Template:

- Security Rights
- Access/Intrusion Group
- Privileges

If your facility has purchased the BACnet option, the Action Interlock tab will display. See "Action Interlock Operation" on page 237.

Security Rights



Security rights determine whether or not an access request made by the entity will be granted or denied. The panels will make the access decision based on the rights assigned to the entity. This tab allows you to define the access rights of an entity under normal and under emergency circumstances. In emergency situations, the system will switch the entity's normal access privilege to a set of alternative privileges without having to change the entity's rights, which may be time consuming during an emergency.

Access is granted or denied based on access levels and/or security roles.

Access Levels

Normal Access Level – Enter a normal access level from 0 (lowest) to 99. To obtain access at a door, this number must be equal to or greater than the Security Level set up for the terminal. If the Security Level at the terminal is raised, entities will be denied access, unless the access profile has the Executive privilege defined. Normal Access Level is considered an alternative access mode and is available only for CK722 panels.

Emergency Access Level – Enter an emergency access level from 0 (lowest) to 99. To obtain access at a door, this number must be equal to or greater than the Security Level set up for the terminal. If the Security Level at the terminal is raised, entities will be denied access, unless the access profile has the Executive privilege

defined. Emergency Access Level control provides a rapid method of restricting access in case of an emergency.

Security Roles

Entities can be assigned through their access profiles, two sets of security roles, one set for standard (**Normal**) operation and one set for elevated security (**Emergency**) operation.

Normal security roles are defined for normal daily access. **Emergency** security roles are defined for temporary emergency situations. When an emergency is declared, the selected **Emergency** security roles become active and are used instead of the **Normal** roles.

To assign Security Roles through this access profile, select from the associated drop-down lists any of the previously defined Access or Privilege Security Role, refer to “Security Roles” on page 127 for detailed information.

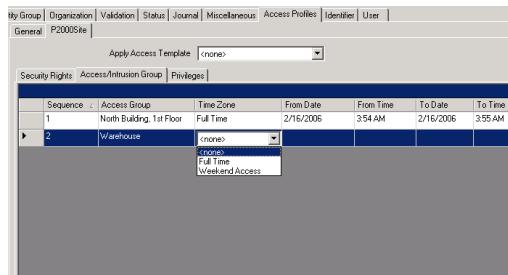
Access Security Role – Select from the drop-down list a previously defined Access Security Role. Select one for Normal and if you wish one for Emergency operation.

Privilege Security Role – Select from the drop-down list a previously defined Privilege Security Role. Select one for Normal and if you wish one for Emergency operation.

Security Flags – You can define security flags that override roles defined in the Access and Privilege security roles.

1. Right-click anywhere on the list box and select **Add**.
2. From the **Security Flag** drop-down list select the flag you wish to override.
3. From the **Status** drop-down list, select whether you wish to **Deny** or **Grant** the access based on the flag selected.

Access/Intrusion Group



Use this tab to define the Access/Intrusion Groups and corresponding Time Zones that will be assigned to this access profile. You can define an unlimited number of access/intrusion groups, but you can only download up to 100 groups if using CK722 panels; up to eight access groups if using CK720/CK705 panels; and up to two access groups if using S321 panels.

1. In the Access/Intrusion Group tab, right-click anywhere on the list box and select **Add**. The **Sequence** column automatically assigns a number to the entry. This number indicates the sequence order in which the access/intrusion group will be downloaded to the panel.

Note: To insert a group between two existing groups, you would select **Insert** instead of **Add**. You can also use “drag and drop” to change the position of a group within the list.

2. Select from the drop-down list, the **Access Group** you wish to assign to this access profile.
3. Select from the drop-down list, the **Time Zone** that will be assigned to the selected access/intrusion group.
4. To define a temporary access period for the selected group, click the **From Date** field, select the check box and click the down

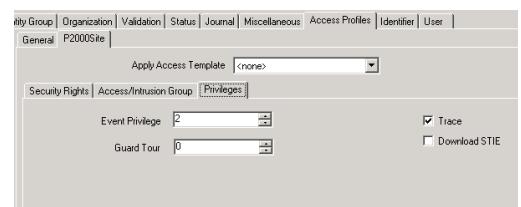
arrow to select a start date from the system calendar when permission for access will be granted. If the check box is not selected, access will be allowed immediately.

5. Click the **From Time** field and click the spin box buttons to select the time when permission for access will be granted.

Note: For example, if the reader doors included in the Access Group normally grant access from 8:00 A.M. to 5:00 P.M., you can set up temporary access on a selected date and time period that will grant the entity permission for limited access within the normal time zone. This feature is performed by the Smart Download service and therefore, you can use it only when Smart Download is running, see “P2000 Services Definitions” on page 314. This feature only works on terminals running in Local mode.

6. Select from the **To Date** and **To Time** fields the date and time when permission for access will expire.
7. To remove an entry, select the line item, right-click and select **Delete**.

Privileges



Event Privilege – Every access badge identifier has an event privilege level, ranging from 0 to 7, with zero as the lowest level. If an entity’s badge is to initiate a card event, his/her event privilege level must be equal to or greater than the privilege level defined in the Panel Card Event dialog box.

Guard Tour – This field is used if you have purchased the Guard Tour option. Select from the drop-down list a priority number from 1 (lowest) to 99. This number determines which tours the selected guard can perform. Only tour badges with equal to or greater than this priority can perform a tour.

Trace – If enabled, all identifier transactions associated with the entity's access profile will be traced and printed, as they occur, on any printer configured to print trace transactions, as long as the Badge Trace and Print options are selected in the Real Time List window.

Download to STIE – This option applies only to panels using STI-E terminal interfaces. If selected, the badge identifier is downloaded to the STI-E terminal. The STI-E terminal can save up to 1,000 badges in a resident database for use if the panel becomes inactive.

Identifier Tab

This tab lists all identifiers associated with the entity. An entity may have multiple identifiers. You can define Access Badge or Common PIN identifiers, which use Access Profiles to restrict access to authorized areas at authorized times. Some facilities require that the entity present an access badge at a door, and immedi-

ately enter a PIN code at a keypad, for the system to grant access to a controlled area.

You can also define ID badges that can be created strictly for identification purposes.

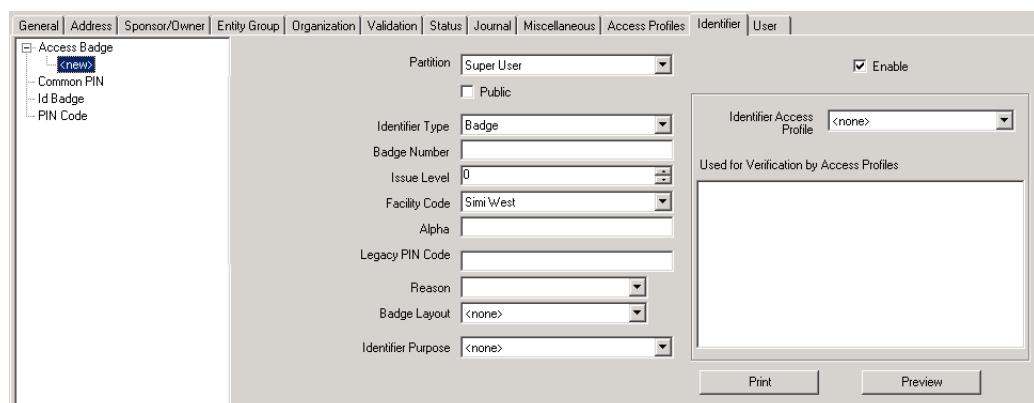
The following identifier types are provided:

- Access Badge
- Common PIN
- Id Badge
- PIN Code

1. To create an identifier, click the **Identifier** tab.
2. Right-click **Access Badge**, **Common PIN**, **Id Badge**, or **PIN Code** and select **Add** to create the desired identifier.
3. Refer to the following sections for detailed information.

Access Badge

Access Badge identifiers identify and track the location of an entity in the facility. Access Profiles are assigned to the Access Badge identifier to define the access rights assigned to the entity.



Partition – If this is a partitioned system, select the Partition in which this Access Badge identifier will be active.

Public – Select Public if you wish this badge identifier to be visible to all partitions.

Enable – When a badge identifier is created, it is automatically enabled. Clear this check box to temporarily disable this identifier. This function is useful when you wish to temporarily disable a badge identifier, but do not wish to re-issue or redefine the identifier.

Identifier Type – Select one of the following options. Once selected, and the record is saved, you cannot modify the identifier type.

- **Badge** – Visually identifies the entity and provides access to the entity based on his/her access profile.
- **Card ID** – This is the ID number that allows entities to get access by keying-in their card ID number. Available for legacy panels.
- **Badge/Card ID** – This badge visually identifies an entity and provides access control capabilities. The entity may be required to present the badge and key-in the card ID number to obtain access. Available for legacy panels.

Badge Number – Enter a badge number (the number of allowed characters depends on the parameters selected in the Site Parameters dialog box, see “Max Badge Number” on page 33). This number is usually pre-assigned to badges provided by *Johnson Controls*. If your system is configured to use FASC-N badges, see “FASC-N Badges” on page 146 for instructions on generating this number.

Note: You can assign any number of badge identifiers to an entity; however, if your facility uses legacy panels, each badge identifier must have a unique number.

Issue Level – Select an issue level per badge identifier number. If an entity loses a badge, you would give him/her the next available issue level and retain the same badge number. The number of badge issue levels supported depends on the panel type you use; see “Max Issue Level” on page 33.

Facility Code – Select from the drop-down list the type of facility code to be assigned to this badge identifier. Facility codes are provided by *Johnson Controls* and identify the badges that belong to your particular site. Facility codes for CK705 and CK720 panels are defined in the Edit Terminal dialog box; for S321 panels use the Edit Panel dialog box. For CK722 panels use SCT. Not available for FASC-N badges.

Alpha – Some custom badge identifiers may provide space for additional characters. If so, enter them here. (Limited to 10 characters.) Not available for FASC-N badges.

Legacy PIN Code – Enter the entity personal identification number (PIN) to be used with PIN readers connected to legacy panels. If an algorithmic PIN is used, leave this field blank. For PIN readers connected to CK722 panels, use the identifier type PIN Code described on page 145.

Reason – Select a Reason from the drop-down list to indicate why the badge identifier is being issued. The choices are: Damaged, Lost, New, Not Returned, Reissue, Returned, Stolen, Temporary, or Visitor.

Badge Layout – If you have created a number of badge designs using your Video Imaging software, you can select a badge layout from the drop-down list. (Badge design instructions are provided in the *P2000AE Integrated Video Imaging Installation and Operation Manual*.)

Identifier Purpose – To include this identifier information, select an Identifier Purpose from the drop-down list to indicate the identifier’s intention. You must define Identifier Purpose

fields before the selections will display in the drop-down list. Refer to “Define Identifier Purposes” on page 127.

Identifier Access Profile – Select from the drop-down list the Access Profile that provides the access rights of the entity, see “Access Profiles Tab” on page 138 for details.

Used for Verification by Access Profiles – In some applications, having a valid badge identifier at the correct time and reader is insufficient to grant access. To implement additional access grant requirements before allowing entry, you may also use additional access profiles to ensure that the identifier is used by the entity they are issued to. Select the Access Profiles that will be used for verification.

Common PIN

This identifier allows you to use a personal identification number (PIN) that will be common to a team of people, for example air crew or hospital personnel. You can create a PIN number to be assigned to a group of entities, or create a PIN number to be assigned individually to entities with different access needs. Presenting a badge identifier is not required when using Common PINs.

The screenshot shows the 'Identifier' tab of a software interface. The 'Identifier Type' dropdown is set to 'Common PIN'. The 'Partition' dropdown is set to 'Super User' and has a checked 'Public' option. The 'Identifier Access Profile' dropdown is set to '<none>'. Below these fields are 'Reason' and 'Identifier Purpose' dropdowns, both currently set to '<none>'.

Partition – If this is a partitioned system, select the Partition in which this Common PIN identifier will be active.

Public – Select Public if you wish this Common PIN identifier to be visible to all partitions.

Enable – When a Common PIN identifier is created, it is automatically enabled. Clear this check box to temporarily disable this identifier. If this identifier is enabled, the entity is required to enter the assigned Common PIN number to gain access at the door.

Identifier Type – The default type is Common PIN.

Common PIN – Enter the PIN code number to be assigned to the entity.

Reason – Select a Reason from the drop-down list to indicate why the Common PIN identifier is being issued.

Identifier Purpose – To include this identifier information, select an Identifier Purpose from the drop-down list to indicate the identifier’s intention. You must define Identifier Purpose fields before the selections will display in the drop-down list. Refer to “Define Identifier Purposes” on page 127.

Identifier Access Profile – Select from the drop-down list the Access Profile that provides the access rights of the entity, see “Access Profiles Tab” on page 138 for details.

Id Badge

Identification badges are used to visually identify an entity. However, unlike access badges, they do not have access control capabilities - they cannot be used to access a controlled area of a facility.

The screenshot shows the 'Identifier' tab of a software interface. The 'Identifier Type' dropdown is set to 'Id Badge'. Other fields include 'Badge Number' (empty), 'Issue Level' (0), 'Facility Code' (Smi-West), and 'Alpha' (empty). Below these are 'Reason' and 'Identifier Purpose' dropdowns, both currently set to '<none>'. A 'Print Badge' button is visible on the right.

Partition – If this is a partitioned system, select the Partition in which this Id Badge identifier will be active.

Public – Select Public if you wish this badge identifier to be visible to all partitions.

Identifier Type – The default type is Id Badge.

Badge Number – Enter a badge number (the number of allowed characters depends on the parameters selected in the Site Parameters dialog box, see “Max Badge Number” on page 33). This number is usually pre-assigned to badges provided by *Johnson Controls*.

Issue Level – Select an issue level per badge identifier number. If an entity loses a badge, you would give him/her the next available issue level and retain the same badge number. The number of badge issue levels supported depends on the panel type you use; see “Max Issue Level” on page 33.

Facility Code – Select from the drop-down list the type of facility code to be assigned to this badge identifier. Facility codes are provided by *Johnson Controls* and identify the badges that belong to your particular site. Facility codes for CK705 and CK720 panels are defined in the Edit Terminal dialog box; for S321 panels use the Edit Panel dialog box. For CK722 panels use SCT.

Alpha – Some custom badge identifiers may provide space for additional characters. If so, enter them here. (Limited to 10 characters.)

Reason – Select a Reason from the drop-down list to indicate why the badge identifier is being issued. The choices are: Damaged, Lost, New, Not Returned, Reissue, Returned, Stolen, Temporary, or Visitor.

Enable – When a badge identifier is created, it is automatically enabled. Clear this check box to temporarily disable this identifier. This function is useful when you wish to tempo-

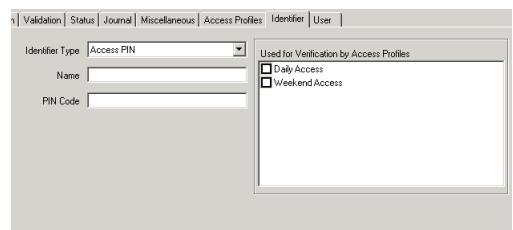
rarily disable a badge identifier, but do not wish to re-issue or redefine the identifier.

Badge Layout – If you have created a number of badge designs using your Video Imaging software, you can select a badge layout from the drop-down list. (Badge design instructions are provided in the *P2000AE Integrated Video Imaging Installation and Operation Manual*.)

Identifier Purpose – To include this identifier information, select an Identifier Purpose from the drop-down list to indicate the identifier’s intention. You must define Identifier Purpose fields before the selections will display in the drop-down list. Refer to “Define Identifier Purposes” on page 127.

PIN Code

You can create PIN Code identifiers that can be assigned to entities for authentication purposes. These PIN Code identifiers can only be used on keypads connected to CK722 panels. The P2000 system will grant or deny access to a controlled area based on the validity of the entered PIN Code.



Identifier Type – Select one of the following options:

- **Access PIN** – The identifier will be used for access requests.
- **Intrusion PIN** – This identifier will be used for intrusion requests.
- **Universal PIN** – This identifier will be used for access and intrusion requests.

Name – Enter a name to describe the selected PIN Code identifier.

PIN Code – Enter the entity personal identification number to be used with PIN readers connected to CK722 panels.

Used for Verification by Access Profiles – In some applications, having a valid PIN Code identifier at the correct time and reader is insufficient to grant access. To implement additional access grant requirements before allowing entry, you may also use additional access profiles to ensure that the identifier is used by the entity they are issued to. Select the Access Profiles that will be used for verification.

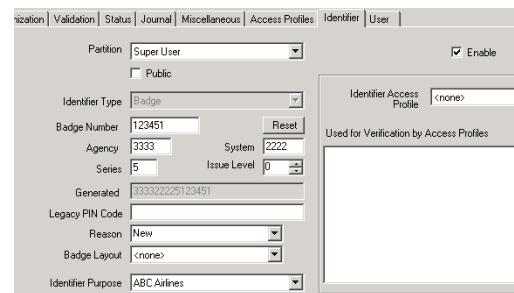
FASC-N Badges

The P2000 software supports the programming of smart cards that are compliant with the Government Smart Card Interoperability Specification (NIST IR 6887 - 2003 Edition, GSC-IS Version 2.1). These smart cards are programmed using a smart card encoder, physically located in the badge printer.

Note: Smart card encoding is only available if the Video Imaging software option used at your facility is EPI Builder.

To support the Federal Government smart card encoding protocol, an encoded access badge must include FASC-N (Federal Agency Smart Credential Number) data fields. A FASC-N badge number is a unique number assigned to one individual. This type of badge is typically issued to government employees, however it could also be used by any industry. Data elements in this number determine whether an entity should be granted access to specific buildings and controlled places.

If the Badge Edit Style selected for your facility is **FASC-N**, the system will use the default values defined in Site Parameters (see page 33) to generate a 15-digit badge number as described below.



Badge Number – This is a six-digit unique badge number assigned to the entity.

Reset – When you click the Reset button, the Agency, System, and Series default values will display and the Generated box will show the generated badge number.

You can however, enter specific values for a specific badge by changing any of the default values, which will be used instead of the configured default values for the badge currently being edited. If you want to go back to the default values, click the **Reset** button.

Agency – This is a four-digit unique number identifying the government agency issuing the badge.

System – This is a four-digit number identifying the specific government site or facility issuing the badge, that way each site within a government agency will have a system number which is unique to that agency.

Series – This is a one-digit number that can be left to the discretion of the site administrator as to how this number can be used.

Generated – This box displays the generated number containing the 15 digits as follows:

AAAASSSSRNNNNNN

where *A* is the Agency code, *S* is System code, *R* is Series, and *N* is the Credential Number.

User Tab

Every entity of the type Person or System Administrator can become a P2000 User. Entities can have multiple User accounts, and each account can be identified by a unique user name and password.

A User can be a Person, with access profiles, identifiers, etc.; or can be a System Administrator, which is a system account, such as “Cardkey” or an interface account such as the “MIS” account.

Note: *Every User in the system is an entity, but not every entity is a User.*

When you select the **User** tab in the Entity Management window, all user accounts that have been created for the selected entity are listed on the list box at left side of the window.

To add a new user account, right-click on the list box and select **Add**. The list box will display <new> and will display the name of the User account once the record is saved.

To delete an existing user account, select the user name, right-click on the list box and select **Delete**.

Note: *If FDA Part 11 Record Retention Policy is enabled in Site Parameters, you will not be able to delete users for the amount of time specified in the Retention Period field, see page 34 for details.*

General Tab

User Name – Enter the name of the user account that will be entered when logging on to the system.

User Account Type – Select from the drop-down list whether the password is maintained within **P2000** or within Active Directory Services (**ADS**), or both. The **ADS/P2000** option is a fall back if ADS is not available at the time when the user attempts to access the P2000.

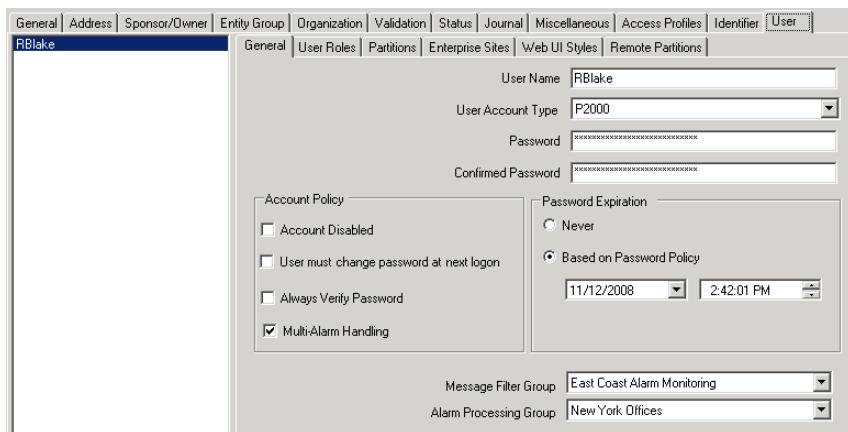
Password – Enter the password that will be entered when logging on to the P2000 system. The system will display an asterisk for each letter (****). To change the password at a later time, refer to “Changing the User Password” on page 23. In addition, you should refer to the “Password Policy Tab” on page 35 for additional password complexity rules.

Confirmed Password – Enter the password again to confirm.

Account Disabled – Select this option if you wish to disable this account. Once this option is selected, this account can no longer be used for logging into P2000, until the account is enabled again. A message will display at the next login informing the user that the account has been disabled.

User must change password at next logon – If a user forgets his or her password, the system administrator may grant a temporary password and force the user to change the password at the beginning of the next login. A password cannot be changed for MIS or XML RPC users.

Always Verify Password – If this option is selected, the user will be required to enter the login password to access certain system-critical functions.



Multi-Alarm Handling – If you select this option, the user can process more than one alarm at a time. This option is always enabled by default. When selected, the user can acknowledge or complete multiple alarms in the Alarm Monitor window.

Password Expiration: Never – Select this option to define passwords that never expire, for MIS users for example. This option is not available if FDA Part 11 Password Policy is enabled in Site Parameters (see page 35).

Password Expiration: Based on Password Policy – If you select this option, the password will only be valid for the number of days entered in the Password Validation field on the Password Policy tab (see page 35). If the Password Validation is set to 0 days, you can select the date and time when the password should expire.

Message Filter Group – Select from the drop-down list, the Message Filter Group that defines which messages the user can see. If you select <none> the user will be able to see all messages, provided the user has access to the Super User partition (or records are marked “Public”), and the Message Filter Group field defined at the workstation is also set to

<none> (see page 20). Refer to “Configure Message Filtering and Message Routing” on page 99 and to “Operators and Messages” on page 99.

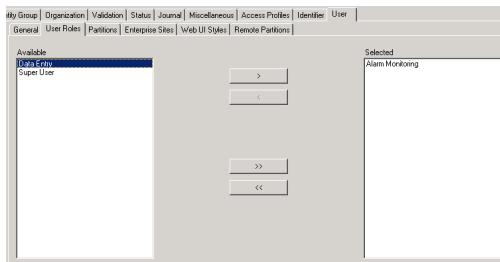
Alarm Processing Group – Select from the drop-down list the Message Filter Group that defines which alarms the user can process (acknowledge, respond to, or complete). If you select <none> the user will be able to process all alarms that pass the Message Filter Group selection. If a user should be able to receive and process all alarms, then both the **Message Filter Group** and **Alarm Processing Group** selections should be set to <none>.

Note: *Message Filtering and Alarm Processing Groups apply on P2000 Workstations only, not on P2000 Servers. In addition, partitioning rules still apply, regardless of filter group selections.*

User Roles Tab

User Roles determine the functions that a user can perform in the system. Each user account can be associated with different rights to applications, and in the case of Entity Management, dialog components and individual data fields.

User Roles must be defined otherwise the table will display empty. Refer to “User Role Management” on page 21 for more information.



1. Select from the **Available** box the User Role that defines the applications and/or database items that the user can view or change. You can select multiple items by holding down the **<Shift>** key.
2. Click the **>** button to move the User Role from the Available box to the **Selected** box.

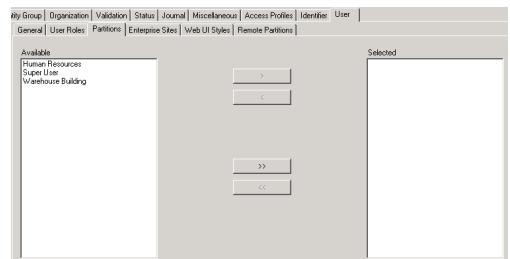
Note: A user can perform any function if at least one user role assigned to the user allows permission to that function.

3. To select all User Roles in the **Available** box, click the **>>** button.
4. To remove User Roles from the **Selected** box, select the desired User Roles and click the **<** button, or click **<<** if you want to remove them all.

Partitions Tab

This tab will display only if your system has the Partition option. Users can be assigned to single or multiple partitions and have unique access restrictions, such as the ability to add, modify, or view database information within their assigned partitions. Partitions must be defined otherwise the table will display empty.

Refer to “Partitions” on page 225 for more information.



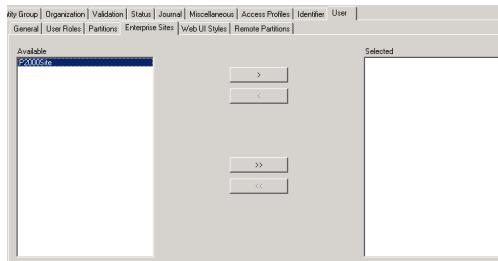
1. Select from the **Available** box the partition to which this user will have access. You can select multiple items by holding down the **<Shift>** key.
2. Click the **>** button to move the Partition from the Available box to the **Selected** box.
3. To select all Partitions in the **Available** box, click the **>>** button.
4. To remove Partitions from the **Selected** box, select the desired Partitions and click the **<** button, or click **<<** if you want to remove them all.

Note: A user will be able to see alarms and real time messages that are associated with the partitions selected here, unless records are marked “Public” or the user is monitoring the system from the Server, where all alarms and real time messages are visible, regardless of the partitions selected here. Users that belong to the Super User partition have access to all partitions of the system.

Enterprise Sites

This tab will display only if your system has the Enterprise option, and displays the different sites within the P2000 Enterprise. Users can only modify and manage records that belong to a site that this user can access. If a user has access to the site “Enterprise” the user

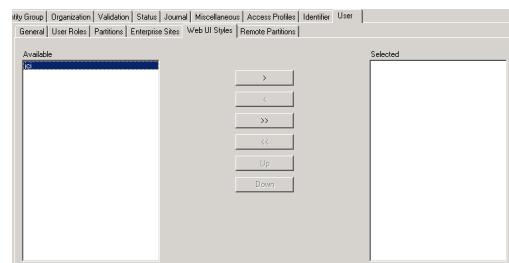
will have access to all sites, however partition restrictions may still apply. Enterprise sites must be defined otherwise the table will display empty. Refer to “P2000 Enterprise” on page 291 for more information.



1. Select from the **Available** box the Enterprise site to which this user will have access. You can select multiple items by holding down the <Shift> key.
2. Click the **>** button to move the Enterprise site from the Available box to the **Selected** box.
3. To select all sites in the **Available** box, click the **>>** button.
4. To remove sites from the **Selected** box, select the desired sites and click the **<** button, or click **<<** if you want to remove them all.

Web UI Styles

This tab will display only if your system has the Web Access option. The Web Access graphical user interface is controlled by styles, which can be fully customized according to individual needs, and can be assigned to users that are authorized to perform Web Access functions. The interface styles must be defined otherwise the table will display empty. Refer to the *Web Access Manual* for details in creating the styles.



1. Select from the **Available** box the Web Access interface style that will be assigned to the user. You can select multiple items by holding down the <Shift> key.
2. Click the **>** button to move the interface style from the Available box to the **Selected** box.
3. To select all styles in the **Available** box, click the **>>** button.
4. To remove styles from the **Selected** box, select the desired styles and click the **<** button, or click **<<** if you want to remove them all.
5. Use the **Up** or **Down** buttons to move the styles in the Selected box accordingly.

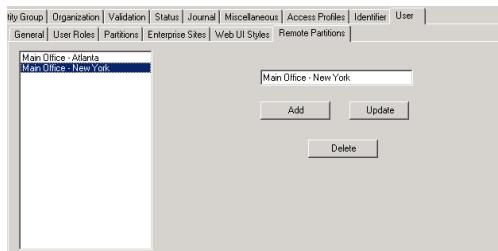
Note: The first style on the **Selected** box is the user's default style. If the user wishes to use a different style, then he or she will need to select a style using the User Preferences feature from the Web Access interface. Refer to the Web Access Manual for details.

Remote Partitions Tab

If the user will be monitoring remote messages, use this tab to define the partitions to which the user will have access. If you do not enter any remote partition names, the user can monitor all messages from the remote site.

Remote partitions are partitions from other Enterprise systems – not from other P2000 sites within the Enterprise System.

Note: *Remote messages are any alarm or transaction messages originated at another P2000 site. Refer to “Message Filtering” on page 100.*



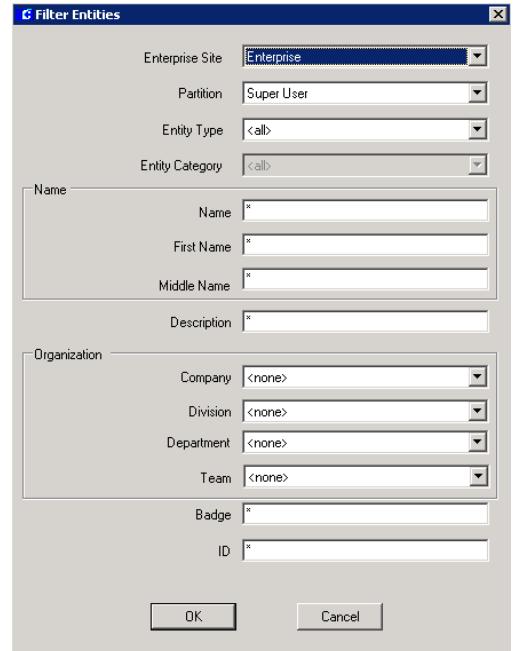
1. Enter the name of the partition at the remote site and click the **Add** button. The remote partition name will display in the list box.
2. To edit an existing remote partition name, select the name in the list box, make the change, then click the **Update** button.
3. To delete a remote partition name from the list, select the name in the list box and click the **Delete** button.

Filtering Entity Data

The P2000 software provides a way to filter records that display in the Entity Management window. This is useful in large facilities where it is often impossible to look at hundreds of records from one single view. The Filter Entities feature allows you to locate records quickly and easily. You can filter the database to show only a specific record, or filter it to show several records with a particular characteristic.

To Filter Entity Data:

1. In the Entity Management window, click the **Filter** button on the left side of the entity list. The Filter Entities dialog box opens.



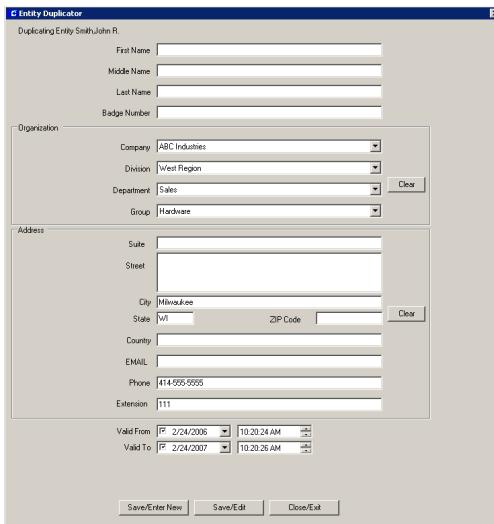
2. Enter the information on any or all of the fields to search for specific entities.
3. Click **OK** to begin your search. The Entity Management window opens showing the entities that match the filter criteria.
4. Click the **Reset** button on the left side of the entity list to restore it to display all entities.

Entity Duplicator

The Entity Duplicator feature allows the duplication of existing entities by copying the entity's basic data and access profiles. You can create master entity records with default information, which can be used as starting templates to create additional entities.

To Use the Entity Duplicator:

1. In the Entity Management window, select the entity record you wish to copy.
2. From the menu bar, select **File>Duplicate**. As an alternative, you can click the **Duplicate** icon in the Entity Management toolbar. The Entity Duplicator dialog box opens. The top left side shows the entity record being duplicated.



3. The first four fields (**First Name**, **Middle Name**, **Last Name**, and **Badge Number**) are always empty, and allow you to enter specific entity information.
4. The **Organization** box displays data from the master entity record. You can edit the desired fields or click the **Clear** button to replace all fields.
5. The **Address** box displays data from the master entity record. You can edit the desired fields or click the **Clear** button to replace all fields.
6. The **Valid From** and **Valid To** fields at the bottom of the dialog box display the validation range of the master entity record.

7. Once you enter the specific information for the new entity, select one of the following options at the bottom of the dialog box:

Save/Enter New – Select to save the entity record. The Entity Duplicator dialog box will remain open to enter another entity.

Save/Edit – Select to save the entity record. The Entity Duplicator dialog box will close and the new entity record will be selected for further editing.

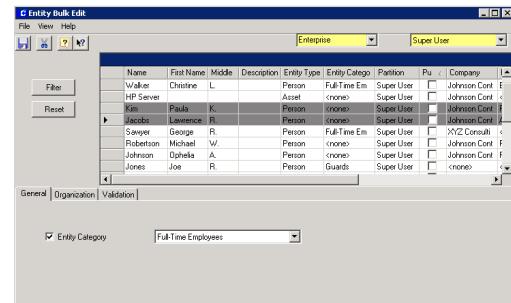
Close/Exit – Select if you do not wish to save the entity record. You will return to the Entity Management window.

Entity Bulk Edit

Entity Bulk Edit can speed up entity configuration by allowing modification of multiple entity records at once.

To Bulk Edit Entity Records:

1. From the P2000 Main menu, select **Access>Entity Bulk Edit**. The Entity Bulk Edit dialog box opens.



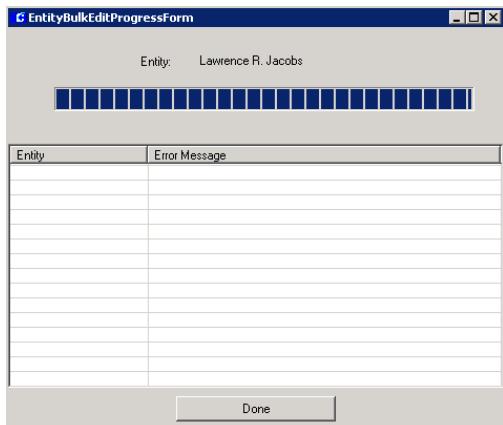
2. Select the entity records you wish to modify. You can use the Filter Entities application to show specific records.
3. When the selected records are highlighted, select one of the following tabs to change in bulk the desired parameters:

General – Allows you to select specific Entity Category and apply it to the selected entities. You must enable the **Entity Category** check box and select the specific category from the drop-down list.

Organization – Allows you to select one or all of the organizational units (**Company**, **Division**, **Department**, or **Team**) and apply it/them to the selected entities. You must enable the desired check box and select the associated unit name from the drop-down list.

Validation – Allows you to apply a validation range to the selected entities. This feature is typically used for example, to temporarily disable an entity without having to delete the entity record. Select from the **From Date/Time** the date and time when the entities will be activated; then select from the **To Date/Time** the date and time when the entity records will be disabled.

4. Once the desired values are set, click the **Save** button to apply the values to the selected entity records.
5. The EntityBulkEditProgressForm dialog box opens displaying the progress of the selected operation, and will indicate any errors encountered during the process.



6. Click **Done** to close the window.
7. If you wish to delete multiple entity records from the database, select the entities from the list and click the **Delete** button.
8. When you finish close the Entity Bulk Edit window.

Auto Badge Management

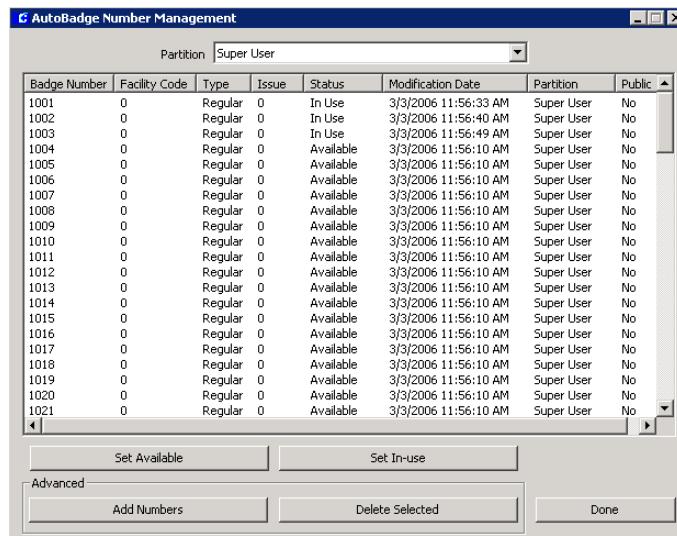
Note: *This feature is not available in this release.*

The Auto Badge Management feature allows you to control and manage badge numbers within a defined pool. Once the pool of numbers is defined and you are issuing a badge, you can click the **Auto** button to insert the next available badge number in the Number field.

To Create a Pool of Badge Numbers:

1. From the P2000 Main menu, select **System>AutoBadge Management**.
2. Enter your password if prompted. The AutoBadge Number Management dialog box opens.
3. If this is a partitioned system, select the **Partition** for which you want to display the badge numbers.
4. Click the **Add Numbers** button. The Add badge numbers dialog box opens.





5. If this is a partitioned system, select the **Public** check box to make these badge numbers visible to all partitions.
6. Define the pool of numbers by entering the **First badge** and **Last badge** numbers.
7. From the **Facility Code** drop-down list, select the facility code to be assigned to this pool of badge numbers.
8. From the **Type** drop-down list, select whether this pool of numbers will be assigned to Regular or Visitor badges.
9. From the **Issue** drop-down list, select the issue level for a badge with this number.
10. Click **OK** to return to the AutoBadge Number Management dialog box. The list box displays the pool of numbers defined for the selected partition, together with the Status of each number and the Modification Date when the entry was created or last modified.

When you assign numbers from this pool, the Status column will display one of the following status:

Available – this number can be assigned to a badge.

Reserved – this number has already been assigned, but a badge has not yet been issued.

In Use – this number is currently in use and cannot be assigned to another badge.

11. To change the status of a badge number from *Available* to *In Use*, click the **Set In-use** button.
12. To change the status of a badge number from *In Use* to *Available*, click the **Set Available** button.

Note: *The status of a badge number can be changed from **In Use** to **Available** only if the number has not yet been issued (it was in the “In Use” state because it was changed using the **Set In-use** button).*

13. To delete badge numbers from the pool, select the numbers and click the **Delete Selected** button.
14. Click **Done** to close AutoBadge Number Management.

Entity Resync

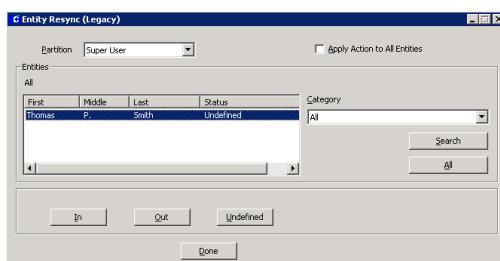
This feature allows you to re-synchronize an entity's status if out-of-sync, in areas controlled by legacy and CK722 panels.

Entity Status Resync in Legacy Panels

Entry and Exit terminals require entities to enter and exit an area in sequence. That is, when entities badge *in* at an entry terminal, they must badge *out* at the next badging. If, for example, they follow another entity *out* without swiping their badge, their badge will remain in the *In* state (out-of-sync). When they attempt to badge back into the area, they will be denied access. You can manually re-synchronize the in/out status of entities by adjusting the status of their badges and returning them to the correct state. You can also reconfigure the entity status as Undefined to clear the Entry/Exit status until the next badging.

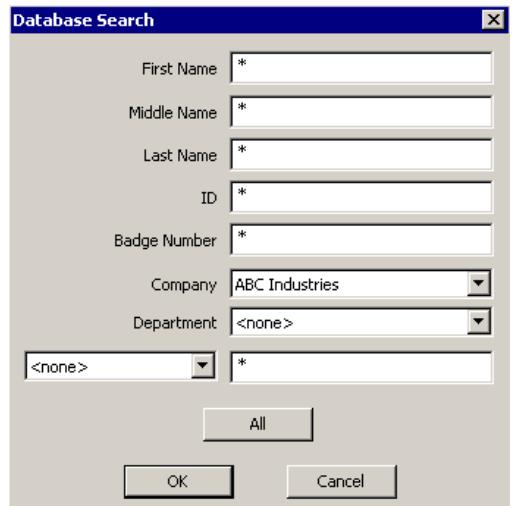
Note: For Entry/Exit to work, all Entry and all Exit terminals must either run in Central mode, or they must all be defined on the same panel and run in Local mode.

- From the P2000 Main menu, select **Access>Entity Resync>Legacy**. The Entity Resync dialog box opens.



- If this is a partitioned system, select the **Partition** in which the entities are active.

- Select from the **Category** drop-down list, the Entity Category that you wish to display in the list box.
- To display specific entities (within the Category selected), click the **Search** button. The Database Search dialog box opens.



- Enter the information on any or all of the fields. You may click **All** to replace the existing search criteria with wildcards.
- Click **OK** to begin the search. The list box in the Entity Resync dialog box will display the entities specified in the search criteria.
- To display all entities again (within the Category selected), click the **All** button.
- After you define the entities you wish to display in the list box, select an entity name from the list, or enable the **Apply Action to All Entities** check box to resync the status of all entities currently in the list.
- Click the appropriate button, **In**, **Out**, or **Undefined** to change the status of all badges that belong to the selected entity(ies).
- Click **Done**. The entity status is now changed.

Entity Status Resync in CK722 Panels

With Entity Resync you can issue appropriate commands to change the status of entities that have been placed in out-of-sync status in areas controlled by Anti-Passback, Anti-Loitering, and Occupancy objects configured for CK722 panels.

For more information on these CK722 objects, refer to the *CK722 Commissioning Guide*.

1. From the P2000 Main menu, select **Access>Entity Resync>CK722**. The CK722 dialog box opens.
2. Select from the top left box, the object type that you wish to control. Choices are:

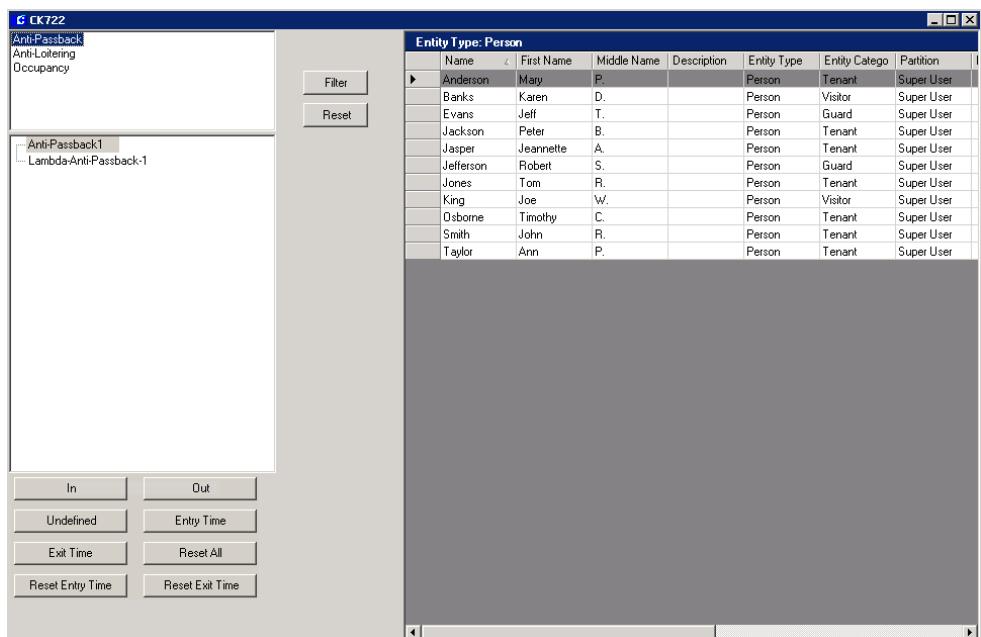
Anti-Passback – Enforces the use of entry and exit readers in accordance with the anti-passback rule by time, and the anti-passback rule by location (also known as the entry-exit rule). The Entity Resync

function allows you to change the status of entities who may be denied access because they violated one of the anti-passback rules.

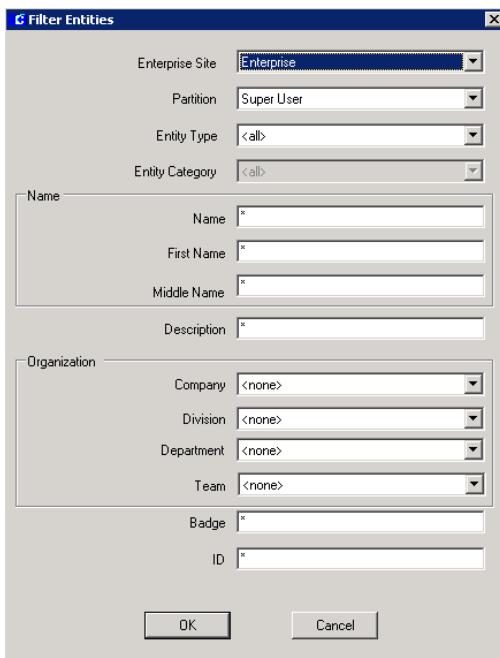
Anti-Loitering – Monitors the time individual entities spend in an anti-loitering area. If an entity exceeds the area's anti-loitering time, an anti-loitering notification is generated. The Entity Resync function allows you to change the status of entities who violated the defined anti-loitering rules.

Occupancy – Monitors the number of entities in an occupancy space. The Entity Resync function allows you to change the status of entities who violated the defined occupancy rules.

3. The middle box displays all the configured objects associated with the object type selected. Select the object you wish to control.



- Click the **Filter** button. The Filter Entities dialog box opens.



- Enter the information on any or all of the fields to search for specific entity records or leave the default fields to display all records.
- Click **OK** to begin your search. The list box on the right side of the window will display the entities specified in the filter criteria.
- If you entered a specific filter criteria and now wish to display all entities, click the **Reset** button.
- Select from the list box, the entity name whose status you wish to modify.
- The bottom left portion of the window displays command buttons according to the object type selected.
- To modify entity status in an **Anti-Pass-back** area select:

In – To change the status of the entity to *In*. The entity will be able to make exit requests again at the selected Anti-Pass-back area.

Out – To change the status of the entity to *Out*. The entity will be able to make entry requests again at the selected Anti-Pass-back area.

Undefined – To change the status of the entity to *Undefined*. The entity will be able to make entry or exit requests again at the selected Anti-Passback area.

Entry Time – To reset the entry time of the entity. The entity will be able to make entry requests again at the selected Anti-Passback area. For example, the Anti-Passback Entry Time is set to 2 hours and the entity presents his/her badge identifier at 8:00 AM to enter the facility. When the entity attempts to enter the facility again at 9:00 AM, the system denies the access request. When you reset the entry time, the entity can make an entry request and enter the facility, after which the entry time will start over.

Exit Time – To reset the exit time of the entity. The entity will be able to make exit requests again at the selected Anti-Passback area. For example, the Anti-Passback Exit Time is set to 30 minutes and the entity presents his/her badge identifier at 5:00 PM to exit the facility. When the entity attempts to exit the facility again at 5:15 PM, the system denies the exit request. However, if you reset the exit time, the entity can make an exit request and exit the facility, after which the exit time will start over.

Reset All – To change the entry/exit status of ALL entities in the selected Anti-Passback area. The status will change to the Default Status defined in the Anti-Passback object (In, Out, or Undefined). For

example, if the Anti-Passback Default Status is set to *In* and you select Reset All, the entry/exit status of all entities will change to *In*.



CAUTION *Use the Reset All function cautiously, since it changes the entry/exit status of ALL entities in the controller for the selected Anti-Passback object. Misuse of this function may result in entities being mistakenly locked out of or locked in the facility.*

Reset Entry Time – To reset the entry time of ALL entities. All entities will be able to make entry requests again at the selected Anti-Passback area.

Reset Exit Time – To reset the exit time of ALL entities. All entities will be able to make exit requests again at the selected Anti-Passback area.

- To modify entity status in an **Anti-Loitering** area select:

In – To change the status of the entity to *In*. The entity will be placed in the selected Anti-Loitering area.

Out – To change the status of the entity to *Out*. The entity will be placed out of the selected Anti-Loitering area.

- To modify entity status in an **Occupancy** area select:

In – To change the status of the entity to *In*. The entity will be placed in the selected Occupancy area.

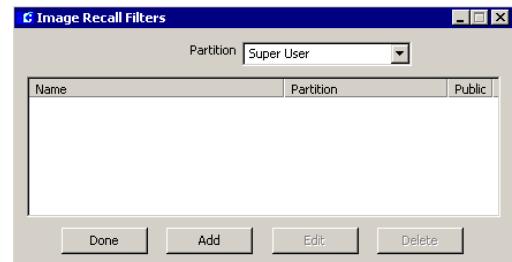
Out – To change the status of the entity to *Out*. The entity will be placed out of the selected Occupancy area.

Image Recall

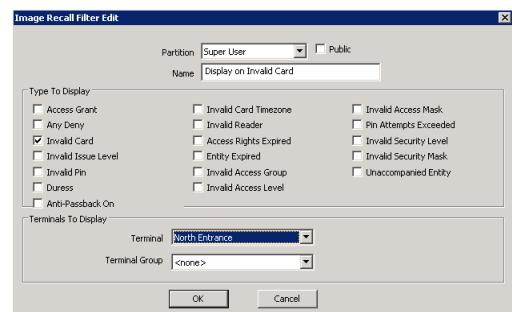
If the Image Recall window is open on the workstation, any badging (for the partition selected in Image Recall Filters) will display the entity's image and information. You can define access conditions and other filter criteria (transactions set up in the Image Recall Filter Edit dialog box, such as an Access Grant or any invalid transaction), to determine if an image will display in the Image Recall window.

To Set up Image Recall Filters:

1. From the P2000 Main menu, select **Access>Image Recall Filters**. The Image Recall Filters dialog box opens.



2. Click **Add**. The Image Recall Filter Edit dialog box opens.



3. If this is a partitioned system, select the **Partition** in which this image recall filter will be active.

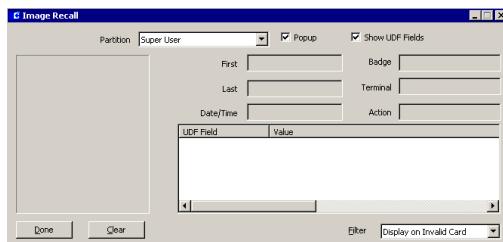
4. Select **Public** if you wish this image recall filter to be visible to all partitions.
5. Enter a descriptive **Name** for the image recall filter.
6. From the **Type to Display** box, select the transactions that you wish to monitor. You do not need to select all conditions. If you select Any Deny, all other filtering conditions will be grayed out, except *Access Grant* and *Duress*.

Note: Entity image and information will always display in the Image Recall window if the associated badge identifier has the **Trace** option enabled in Access Profiles, regardless of the filter conditions selected here.

7. Select a **Terminal** name from the drop-down list to specify the terminal to be monitored.
8. Select a **Terminal Group** name from the drop-down list if you wish to monitor a Terminal Group.
9. Click **OK**. The new image recall filter will display in the Image Recall Filters list.
10. Click **Done**.

To Activate Image Recall:

1. From the P2000 Main menu, select **Access>Image Recall**. The Image Recall window opens.



2. If this is a partitioned system, select the **Partition** in which the image recall will be active.
3. Select **Popup** if the Image Recall window is to move to the front of all windows on the P2000 screen whenever an access attempt that matches the current filter occurs.

Note: Some computers may not allow the Image Recall window to automatically pop up in front of other windows on the screen; instead, the Image Recall button will begin flashing in the Windows taskbar.

4. Select the **Show UDF Fields** check box to display the user defined fields associated with the entity.
5. Select a **Filter** from the drop-down list.
6. When an entity presents a badge at a terminal or group of terminals that meets the filtering conditions, the entity's image displays, along with the current entity information. This image and information will remain in the window until another entity badges within the partition, or until you click the **Clear** button to clear the information in the Image Recall window.
7. Leave the Image Recall window open on the workstation to view images displayed as a result of subsequent badgings.

Monitoring Alarms

Alarm monitoring is at the heart of the *P2000 Security Management* system. According to system devices configuration, alarms display in the Alarm Monitor queue as they occur.

Operators assigned to monitor alarms respond according to individual company policy, and the alarm instruction and response text configured for the various alarm types. The Alarm Response text can be pre-configured for operator selection and/or set to enter manually for a more appropriate response.

The Alarm Monitor window displays immediately after logging on to the Server, so that ongoing alarms are always visible. The Alarm Monitor window cannot be closed at the Server, to ensure that alarm conditions do not go unnoticed. However, it can be minimized using the minimize button on the title bar.

If the Alarm Monitor window is minimized, an alarm message popup can alert the operator that a new alarm has been reported. When an alarm is reported, the operator acknowledges the alarm, makes the appropriate response, and then completes the response.

Note: Some computers may not allow the Alarm Monitor window to automatically pop up in front of other windows on the screen; instead, the Alarm Monitor button will begin flashing in the Windows taskbar.

Pending alarm messages remain in the Alarm Queue until acknowledged and removed by an operator. Alarm History is stored in the system as configured in Site Parameters.

Note: Elements that report alarms, such as legacy input points, must have the **Enable Alarm** option selected to have the alarm displayed in the Alarm Monitor window, refer to page 76. For CK722 alarms, see “Set Up Message Data Configuration” on page 110.

Alarm Configuration

Alarm Category

Every alarm in the system must belong to at least one Alarm Category, but can also be assigned to multiple alarm categories, each with its own set of alarm options. The system creates a “P2000” base alarm category, which cannot be deleted or renamed.

An operator can define an unlimited hierachal tree of Alarm Categories under the P2000 base alarm category. When an alarm category displays in various P2000 screens, it typically displays in the form of a URL, for example: P2000\Maintenance\Building 1.

You can for example, define an input point to generate upon activation, two separate alarms for two configured alarm categories:

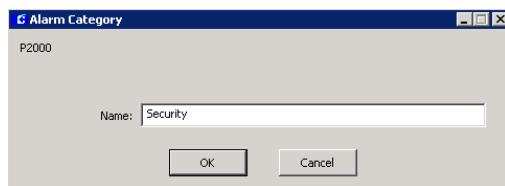
P2000\Maintenance\Building 1 and P2000\Security\Building 1. Typically, a single operator is configured to receive only a single category of alarms, and therefore would only receive a single alarm. However, higher level operators such as supervisors, or an operator at a central alarm monitoring location, may be configured to receive both of these alarms.

When deleting an existing Alarm Category, the P2000 searches the database and issues a warning if the category is referenced by any alarm configurations. If the operator chooses to continue, all existing references to the category being deleted will be changed to its parent category.

Alarm Categories are an Enterprise-wide configuration and therefore, if you are using the Enterprise option, a single set of categories is shared by all P2000 sites within an Enterprise system.

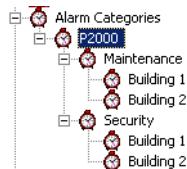
To Create Alarm Categories:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the plus (+) sign next to the root **Alarm Categories** icon to display the default P2000 alarm category.
3. Click the **P2000** alarm category and click **Add**. The Alarm Category dialog box opens.



4. Enter a **Name** for the alarm category.
5. Click **OK** to save the new alarm category.

The new alarm category is listed under the default P2000 category. You can create unlimited trees of alarm categories.



Alarm Handling

As an operator, you may be required to handle alarm conditions, depending on the Message Filter Group and Alarm Processing Group assigned, see “User Tab” on page 147. The Alarm Monitor verifies that alarms pass the Alarm Processing Group filter (if any) for the operator before allowing the operator to acknowledge, respond or complete alarms.

Note: *Message Filtering and Alarm Processing Groups apply on P2000 Workstations only, not on P2000 Servers.*

The alarm response will typically include steps similar to the following:

1. **Acknowledge** that an alarm condition has been reported by the system.
2. **Respond** by entering the appropriate response.
3. **Complete** the alarm.
4. **Remove** the completed alarm condition from the Alarm Monitor window.

Acknowledging an alarm – An operator may be required to acknowledge a new alarm as soon as it is received (see “To Acknowledge an Alarm:” on page 165). They may do so and then return later to actually respond to the alarm, depending on company policy and the priorities assigned to that alarm. The time and date of the acknowledgment is recorded in the alarm history. Acknowledging an alarm silences the audible beep (unacknowledged alarms will continue to beep until recognized). Alarm acknowledgment is optional and does not need to occur prior to response; its use is typically dictated by company policy.

Responding to an alarm – When an operator responds to an alarm, the operator name is entered in the User Name column of the Alarm

Monitor window. The Response time is date and time stamped for the alarm history record. The operator would typically review the Alarm State and Description to note any known conditions. Specific instructions created for the particular alarm will display in the Instruction box during the response to help the operator perform the appropriate action. (See “To Respond to an Alarm.” on page 165.)

Completing an alarm – Several actions may take place during the handling of an alarm. When all actions needed to process the alarm have been completed, the operator “completes” the alarm. This action is date and time stamped for the alarm history record. (See “To Complete an Alarm.” on page 166.) An alarm can only be completed if the alarm state is “secure.”

Note: *Responding to an alarm that has not been acknowledged will automatically cause an acknowledgment to occur. Similarly, completing an alarm causes an automatic acknowledge, if needed.*

Removing the Alarm from the queue – According to company policy, operators may remove completed alarms from the alarm queue. The alarm response sequence will remain in the alarm history record. (See “To Remove an Alarm Message from the Queue.” on page 166.)

Refreshing the Alarm Monitor window – The Refresh button on the Alarm Monitor window is used for two specific functions: 1) to return resized columns to their original positions, and 2) to read again all current alarms from the database (this should not be needed unless there was a loss of communication with the Server). In either case, simply click the Refresh button.

Access the Alarm Monitor from the P2000 Main menu. Select **Alarm>Alarm Monitor**, or if minimized just click the Alarm Monitor button to restore it.

The Alarm Monitor queue displays alarms in a scrolling list, as they occur. The alarm response changes as the operator performs the response steps (see the Alarm Status column header in the Alarm Monitor window); and the date and time of each step is recorded in the alarm history record.

When a new alarm displays in the Alarm Monitor window, an audible beep sounds, and a red color bell icon in the line item entry message begins flashing. The entry will continue in this “Pending” state until an operator acknowledges the alarm, after which the beep stops and the bell icon changes to yellow.

Monitoring Remote Alarms

You can configure your system to receive alarm messages from remote P2000 sites, allowing operators to simultaneously monitor alarms locally and at multiple remote sites. This feature is useful to monitor alarms at unattended sites that are closed for the weekend or a holiday, and ensures that all alarm conditions, even at far away locations, are watched closely at all times.

To be able to monitor remote alarms, both your local and the remote site have to be properly configured. The following conditions must be met:

- The **Remote Message Service** must be up and running at both the remote site (to send the alarm message) and at your local site (to receive the alarm message). The Remote Message Service can be started and stopped using the P2000 Service Control feature, just like the other P2000 services. Refer to “Starting and Stopping Service Control” on page 315.

- The **Message Filter Configuration** application (page 101), must be properly configured at your local site and each remote site, to control the type of messages transmitted between Servers, thereby reducing network traffic by transmitting only messages that pass the filter criteria.
- The **P2000 Remote Server** application (page 108), must be properly configured at each remote site to be able to send their alarm messages to your local site. The setup must include the name, IP address and Remote Message Service Listener Port number of your local site; the type of messages that will be forwarded to your site and at what times; and other related parameters.
- The **Processing Remote Message** option in the RMS tab of Site Parameters (page 38), must be selected at your local site to be able to receive messages from remote P2000 sites. If you select this option, the Remote Message Service will process incoming messages and pass them on to RTLRoute for distribution within the local system and, if applicable, to other remote sites.
- The **Message Filter Group** selected in the RMS tab of Site Parameters (page 38), defines which remote messages your Remote Message Service will process. If you select <None>, your local P2000 site will receive all remote messages.
- The **Local Alarms** option in the RMS tab of Site Parameters (page 38), must be selected at the remote site to allow remote operators to acknowledge, respond, and complete alarms originated at your local site.
- The **Remote Alarms** option in the RMS tab of Site Parameters (page 38), must be selected at the remote site to allow remote operators to acknowledge, respond, and complete alarms originated at other P2000 sites.

If these conditions are met, your local Alarm Monitor window will display alarm messages that are generated at remote sites when their alarm status or state changes.

The procedures for handling remote alarms are similar as for local alarms; however, the following points should be noted:

Responding to remote alarms – Alarm instructions are sent to remote sites; however, the alarm responses remain local. While the Alarm Status column in the Alarm Monitor displays a “Responded” status, the alarm response entered at a remote site will NOT be part of the alarm history in your local site.

Completing remote alarms – Remote alarms can be completed, regardless of the current alarm state.

Removing remote alarms – Remote alarms can be removed from the queue, regardless of the current alarm state. Removed alarm will be automatically completed.

Alarm Monitor Definitions

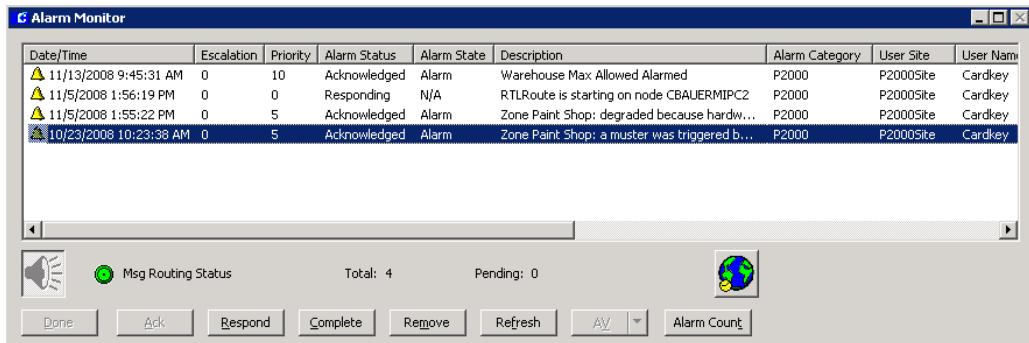
Date/Time – Displays the date and time the alarm was reported to the system. Alarms that are originated at remote sites with different geographical time zones will display the actual time at the remote site.

Note: Click any of the column headings to sort the alarms by the selected column heading.

Escalation – Displays the escalation level of the alarm (the highest is “10”).

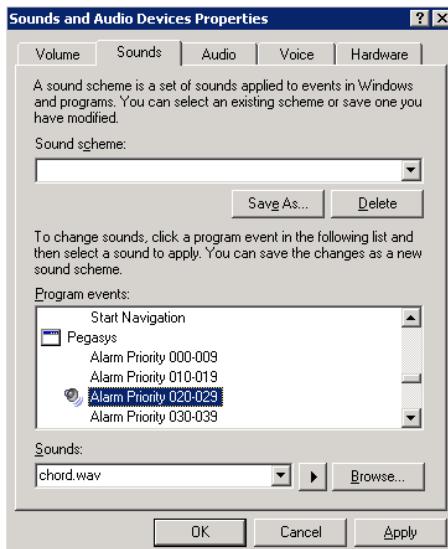
Priority – Displays the Alarm Priority set for each alarm type (the highest is “0”).

You can assign sounds to Alarm Priorities 0 to 255 in groups of 10. The sound files can be set up from the **Control Panel** in your Windows



desktop, clicking the **Sounds** icon. In the **Sounds** tab, select any of the Pegasys Alarm Priorities from the Program events box, then select the corresponding sound file from the Sounds drop-down list.

Note: To access the P2000 alarm priority sounds, you must open the Alarm Monitor window at least once at the workstation.



Alarm Status – Displays any of the following Alarm Status.

- **Pending** – Not yet acknowledged.
- **Acknowledged** – Acknowledged but no action taken.
- **Responding** – Acknowledged and response action in progress.
- **Complete** – Action taken.

Alarm State – Indicates the state of the alarm, such as Secure, Alarm, Open, Short, Suppressed, Tamper, Bypassed, etc.

Description – A description of the element that activated the alarm.

Alarm Category – Displays the Alarm Category to which the alarm belongs. The default category is “P2000.” When an alarm is assigned to multiple Alarm Categories, and the operator is configured to view alarms from these multiple categories, the alarm will display separately for each category.

User Site – Displays the site name from where the operator is handling the alarm.

User Name – The name of the operator who handles the alarm.

Action Date/Time – Displays the date and time the action (respond, complete, etc.) takes place. This will always be the local time, regardless if a remote site is in a different geographical time zone.

Query String – Displays the query string value (if it was defined) of the item associated with the alarm.

Alarm Site – Displays the name of the P2000 site where the alarm was originated.

Partition – Displays the name of the partition containing the item (input point, terminal, panel, etc.) that originated the alarm.

Public – Displays whether the alarm message is visible to other partitions.



Audible Alarm Button – Click the Audible Alarm button to temporarily disable the audible alarm beep. All alarms will be affected. Unless you acknowledge, respond, or complete the alarm, the beep will become audible again in two minutes. To turn off the audible alarm beep, select from the **Sounds** dialog box in the **Control Panel**, any of the Pegasys Alarm Priorities, then browse for the *None.wav* file located in the “bin” folder of the P2000 software installation.



Msg Routing Status – The Message Routing Status indicator will display in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.

Total – Displays the total alarm count in the Alarm Monitor window.

Pending – Displays the number of pending alarms in the Alarm Monitor window.



Map Button – You can see the location of an alarm on a Real Time Map from the Alarm Monitor window. Select an alarm and click the Map button. The map displays and the icon will blink indicating the location of the alarm. For more information see “Using the Real Time Map” on page 218. This feature is available for local alarms only.

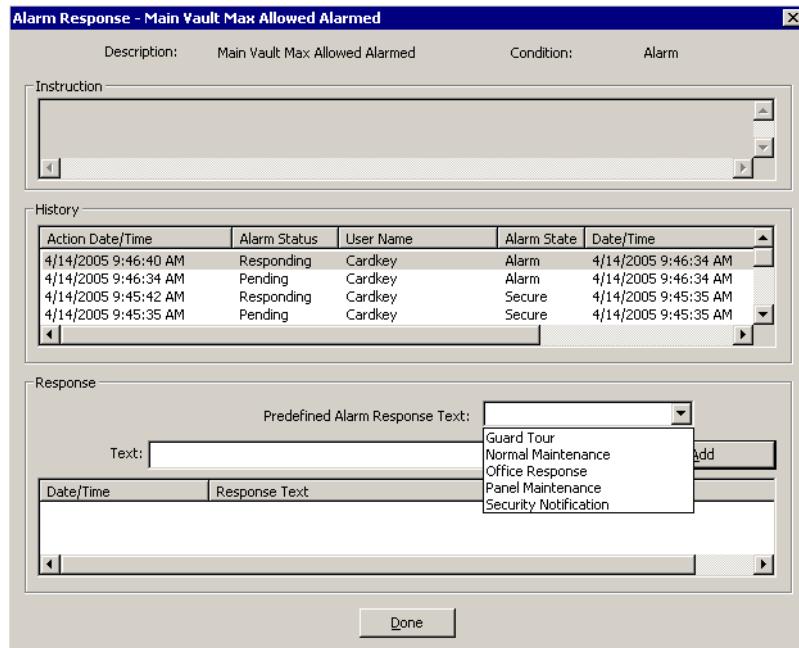
Note: If your facility has purchased the DVR option, the **AV** button will be available. If the alarm message displayed is associated with a camera, you can select the message line from the list and click the **AV** button, then select whether you want to display live or stored video. For more information refer to “DVR” on page 282.

To Acknowledge an Alarm:

1. Click the line item you wish to respond to and click the **Ack** button. The Alarm Status changes to “Acknowledged.” This informs the system and anyone else monitoring the system that the alarm has been recognized.
2. If a number of alarms come in at once, you can acknowledge them in any order you wish; however, company policy may dictate that you respond by priority. If desired, select the highest priority by number, or click the **Priority** column title to sort by priority, moving the highest priority to the top of the list.

To Respond to an Alarm:

1. With the line item to which you wish to respond selected, click the **Respond** button. The Alarm Response dialog box opens.
2. Enter the response information according to the Alarm Response Field Definitions described at the end of this section.
3. Click the **Add** button on the Response box to enter the current Date/Time and Response in the scrolling text box at the bottom of the Alarm Response dialog box. This will store a record of the response in the transaction history. The Alarm Status will change to Responding.
4. Click **Done** to return to the Alarm Monitor window.



Alarm Response Field Definitions

Description – Displays the description for the line item selected in the Alarm Monitor window.

Condition – Displays the alarm condition.

Instruction – If Instruction text was created, the instruction text will display here.

History – Displays all stored history for the line item selected from the Alarm Monitor.

Predefined Alarm Response Text – Lists names of any predefined response text. Refer to “Creating Predefined Alarm Response Text” on page 169 for more information.

Text – Displays the full text entered from the Predefined Alarm Response Text selection, or you can enter a specific response.

Note: You can have multiple Alarm Response windows open and respond to multiple alarms simultaneously. You can also acknowledge or complete alarms in the Alarm Monitor window while the Alarm Response window is open, but you cannot acknowledge or complete those alarms that are currently open in the Alarm Response windows.

To Complete an Alarm:

1. Click **Complete** to end the alarm processing sequence. The Alarm Status changes to Complete. Alarms can only be completed if the alarm state is “secure.”

To Remove an Alarm Message from the Queue:

The Complete and Remove buttons do not become active until the alarm is in the secure state.

1. Select a line item from the scrolling list.
2. Click **Remove**.

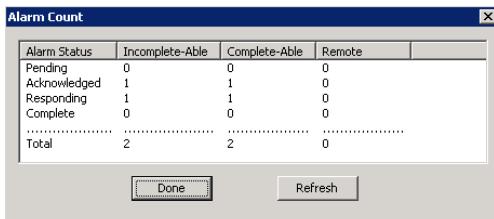
TIP: As an alternative, right-click a line item in the Alarm Monitor window to perform from the shortcut menu any of the above functions (acknowledge, respond, complete, and remove alarms). You can also display the alarm details for the line item selected, display the alarm instruction associated with the alarm, see the location of the alarm on a Real Time Map, display live or stored AV video (if available), or view all items when you click the **Display All** option. In addition, if the element that generated the alarm was configured to allow operators to manually activate events, the event name will also display in the shortcut menu.

To Activate an Event from the Alarm Monitor:

1. In the Alarm Monitor window, select the line item you are responding to and right-click to open the shortcut menu.
2. Click the event name you wish to activate. The event will be triggered.

To Display Alarm Count:

1. In the Alarm Monitor window, click the **Alarm Count** button. The Alarm Count dialog box opens.



2. The list displays the number of alarms for each alarm status currently in the queue and whether these alarms are Incomplete,

Complete, or Remote. To update the list with new data, click the **Refresh** button.

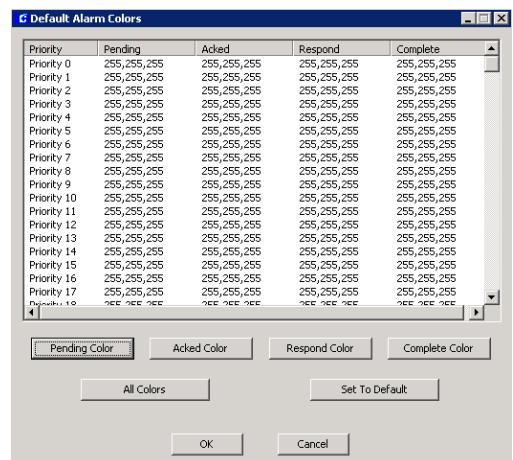
3. Click **Done** to close Alarm Count.

Configuring Alarm Colors

The P2000 system provides color configuration capability for each alarm priority (0 to 255) and its corresponding alarm status. Each alarm status can have a unique color assigned to help operators recognize specific alarms. When a new alarm displays in the Alarm Monitor window, the line for the affected alarm will display in the color that was assigned using the Default Alarm Colors dialog box.

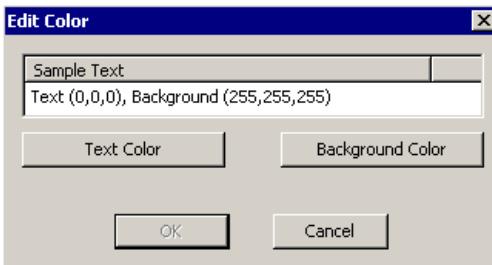
To Define Color-Coded Alarms:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the plus (+) sign next to the root **Site Parameters** icon to display default system parameters.
3. Click the **Default Alarm Colors** icon and click **Edit**. The Default Alarm Colors dialog box opens.



4. Click the **Priority** line you wish to define.
5. Click one of the following buttons:
 - **Pending Color** – to assign a specific color to alarms that have not yet been acknowledged.
 - **Acked Color** – to assign a specific color to alarms that have been acknowledged.
 - **Respond Color** – to assign a specific color to alarms that have been responded.
 - **Complete Color** – to assign a specific color to alarms that have been completed.
 - **All Colors** – to assign the same color to all alarm status for the priority selected.

Regardless of the option selected, the Edit Color dialog box opens.



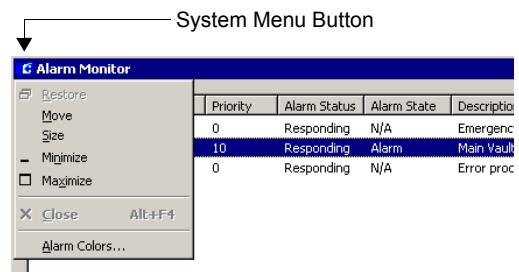
6. Click the **Text Color** button and select the desired text color from the color palette. Click **OK**.
7. Click the **Background Color** button and select the desired background color from the color palette. Click **OK**.
8. The Sample Text box will display the selected colors. Click **OK** to return to the Default Alarm Colors dialog box. You will not see the new color until you select other priority number or click anywhere on the screen.
9. Repeat the same steps if you wish to assign colors to other alarm priorities.
10. To reset to the default system colors, select the Priority line and click the **Set To Default** button.

11. When you finish setting all alarm colors, click **OK**.

The assigned colors for each priority and corresponding alarm status will be the default colors for all operators; however, operators who are required to handle certain alarm conditions may want to use different colors for the alarms they need to see. In that case, the default alarm colors can be changed from the Alarm Monitor window.

Note: *The ability to change alarm colors from the Alarm Monitor window is controlled by User Roles. Therefore, if you do not want operators to override the default alarm colors, remove the "Alarm Colors" rights from their assigned User Roles.*

12. Open the Alarm Monitor window, and click the system menu button.



13. From the control menu select **Alarm Colors**. The Alarm Colors dialog box opens displaying the default colors that were defined from the System Configuration window.
14. Assign the desired colors as described before, then click **OK** to save your settings.

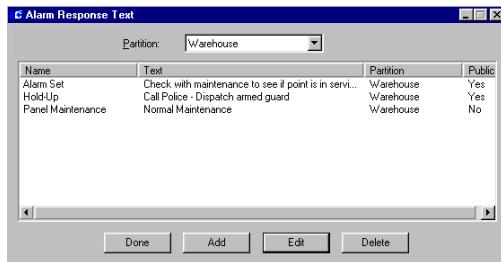
Note: *Alarm colors that are assigned from the Alarm Monitor window are associated with the operator who made the changes. In addition, the Set To Default button will reset to the default colors assigned from the System Configuration window.*

Creating Predefined Alarm Response Text

You can create Response text to speed alarm response to specific types of alarms. For example, when panels go down for regular maintenance, a “Panel Down” soft alarm is sent to the Alarm Queue. The operator can quickly respond by selecting a predefined response from the drop-down list.

To Create Predefined Alarm Response Text:

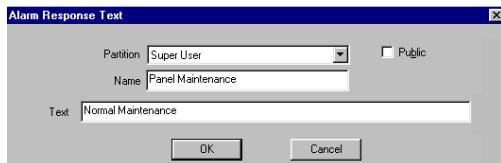
- From the P2000 Main menu, select **Alarm>Alarm Response Text**. The Alarm Response Text list opens.



- If this is a partitioned system, select the **Partition** in which this alarm response text will apply.

The Name, Text, Partition, and whether or not the text is Public will display in the list.

- Click **Add**. The Alarm Response Text dialog box opens.



- Select a **Partition**, if applicable, and select **Public** if you wish the text to be seen by all partitions.
- Enter a descriptive **Name** for the text.

- Enter the actual **Text** you wish to enter into the Alarm Response record.

- Click **OK**. The Response text name will be available in the drop-down list of the Alarm Response dialog box.

To Edit Alarm Response Text:

- In the Alarm Response list, select the entry you wish to edit.
- Click **Edit**. The Alarm Response Text dialog box opens.
- Make the appropriate changes and click **OK**.
- The changes will be reflected in the Alarm Response list.

To Delete an Alarm Response Text:

- In the Alarm Response list, select the entry you wish to delete.
- Click **Delete**. You will be prompted to confirm the deletion. The entry is deleted from the Alarm Response list and will not display in the Alarm Response dialog box.

Monitoring Alarms Using the SIA Interface

Note: P2000 only supports the Radionics system SIA mode using ADEMCO Contact ID protocol.

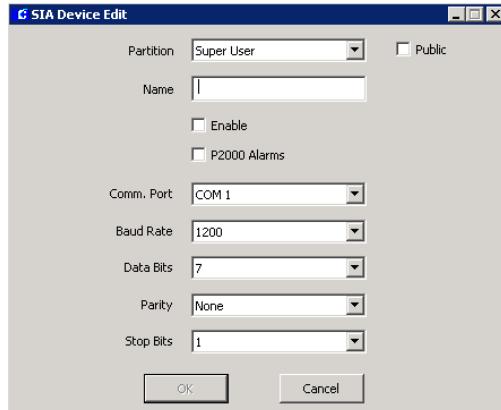
The Radionics D6500 Security Receiver/Controller is capable of receiving alarm and supervisory messages from the Radionics digital dialers over analog telephone lines. It can process up to eight individual telephone lines simultaneously. The Radionics Receiver/Controller is connected to the P2000 system via a standard RS232 serial interface.

The Radionics Receiver/Controller can also be programmed to send alarm messages through the COM RS232 port. The communications parameters must be programmed using a hand-held Radionics programmer. (Refer to the Radionics manual for programming instructions.) The communication takes place only in one direction; from the Radionics system to the P2000 Server. The P2000 Server does not transmit commands to the Radionics Receiver/Controller and cannot suppress any Radionics capabilities such as print or display audible indications. The P2000 Server acknowledges messages as they are received.

This section describes the configuration of the Radionics interface to the P2000 system. You must program the Radionics system prior to connecting it to the P2000 Server. All information must be supplied by the Radionics installer.

To Configure the SIA Interface:

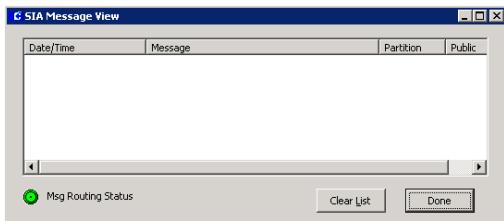
- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the **SIA Device** root icon and click **Add**. The SIA Device Edit dialog box opens.



- If this is a partitioned system, select the **Partition** to which the SIA device will have access.
- Select the **Public** check box to make this SIA device visible to all partitions.
- Enter the **Name** that identifies the SIA device.
- Select the **Enable** check box to enable the SIA device.
- Select the **P2000 Alarms** check box to display messages from the SIA device in the Alarm Monitor (in addition to the SIA Message Viewer window, where they display by default).
- Select the **Comm. Port** that the SIA device is physically connected to. Choices include serial input/output ports COM1 to COM32.
- Select the **Baud Rate** for the SIA device communications. The recommended value is 9600.
- Select the number of **Data Bits** for the SIA device communications. The recommended value is 8.
- Select the appropriate **Parity** for the SIA device communications. The recommended value is "None."
- Select the number of **Stop Bits** for the SIA device communications. The recommended value is 1.
- Click **OK** to save your settings.

To View Messages from the SIA Device:

- From the P2000 Main menu, select **Alarm>SIA Message View**. The SIA Message View dialog box opens.



The **Date/Time** column displays the date and time the message originated.

The **Message** column displays the text of the message.

The **Partition** column displays the name of the partition containing the SIA device that originated the alarm.

The **Public** column indicates whether the message is visible to other partitions.

Note: The *Message Routing Status* indicator displayed in green indicates that all communications between the workstation and the Server are up. If communications go down, the *Message Routing Status* indicator will turn red.

2. Click the **Clear List** button to remove all messages from the list.
3. Click **Done** to close the window.

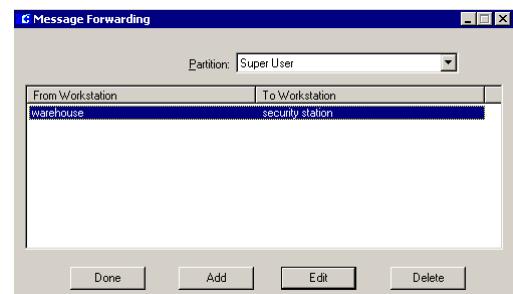
Message Forwarding

Message Forwarding is useful when using message filters. At times, it may be necessary to temporarily forward messages from one workstation to another; for example, if an operator must leave the workstation for a short period of time, or during a vacation or sick leave. When the operator is ready to receive messages at his/her workstation again, message forwarding for the workstation can be deleted.

Note: When forwarding messages from one workstation to another, the system must decide which messages are to be forwarded depending on the operator that is logged on at the receiving workstation. The system will only transmit messages that pass the filter criteria associated with the operator. See "Operators and Messages" on page 99.

To Forward Messages from One Workstation to Another:

1. From the P2000 Main menu, select **Alarm>Message Forwarding**. The Message Forwarding dialog box opens listing the workstations from where and to where all current messages are forwarded.



2. If this is a partitioned system, select the **Partition** in which the workstations are active.
3. Click **Add**. The Message Forwarding Edit dialog box opens.



4. From the **From Station** drop-down list, select the workstation that will be forwarding the messages.

5. From the **To Station** drop-down list, select the workstation to which you wish to forward the messages.
6. Click **OK**. The new entry will display in the Message Forwarding list.
7. Click **Done**.

To Edit Message Forwarding:

1. In the Message Forwarding list, select the line item you wish to edit.
2. Click **Edit**.
3. In the Message Forwarding Edit dialog box, select the desired workstations from the From Station and To Station drop-down lists.
4. Click **OK**. The change is reflected in the Message Forwarding list.
5. Click **Done**.

To Remove Message Forwarding:

1. In the Message Forwarding list, select the line item you wish to delete.
2. Click **Delete**. The message forwarding action is removed.
3. Click **Done**.

Operator Controls

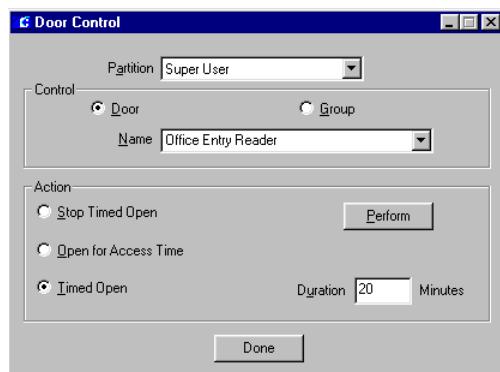
Most system functions operate automatically; however, some functions may be operated manually from a workstation. Operators with the appropriate rights (defined in User Roles), can manually control doors, output devices, and panel relays. For example, an operator can unlock all doors at once, manually trigger a certain event, or allow a guard to manually control access to a specific door during off business hours.

Controlling Doors

An operator can manually control a door, a group of doors, or all doors (override system controls) for a specific time period. (The operator must have rights to the Door Control application to use this feature.) If it is a partitioned system, the doors or door groups available from the drop-down list will be only those active in the operator's partition.

To Manually Control Doors:

1. From the P2000 Main menu select **Control>Door Control**.
2. Enter your password if prompted. The Door Control dialog box opens.



3. If this is a partitioned system, select the **Partition** in which this door is active.
4. In the Control box, select either **Door** or **Group** to populate the Name drop-down list with selections.
5. Select a **Name** from the drop-down list.
6. In the Action box, select one the following:
 - Open for Access Time** – to unlock the door for the amount of time set in the Access Time field defined for the door.
 - Timed Open** – to unlock the door for the number of minutes entered (up to 1440 minutes) in the **Duration** field, after which

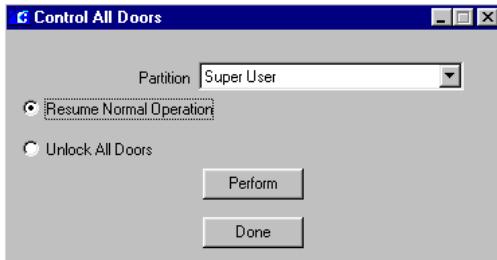
the doors will revert back to their original system-controlled condition.

Stop Timed Open – to cancel the Timed Open condition.

7. Click **Perform**. The Action selection goes into effect.
8. Click **Done** to exit the window.

To Control all Doors at once:

1. From the P2000 Main menu select **Control>Control All Doors**.
2. Enter your password if prompted. The Control All Doors dialog box opens.



3. If this is a partitioned system, select the **Partition** in which the doors are active.
4. Select the **Unlock All Doors** option if you wish to unlock all doors.
5. Click **Perform**. The system will inform you that the doors will remain unlocked until you lock the doors again, and prompt you to continue.
6. Click **Yes**. This will override the system control until you reverse the command.
7. To return all doors to their previous state, select the **Resume Normal Operation** option.
8. Click **Perform**. The system will prompt for verification.
9. Click **Yes**. The Door Control override is reversed.

Controlling Outputs

An operator can manually control an output (override system controls) for a specific output point or group. (The operator must have rights to the Output Control application to use this feature.) If it is a partitioned system, the outputs available from the drop-down list will be only those active in the operator's partition.

To Manually Control an Output Point:

1. From the P2000 Main menu, select **Control>Output Control**. The Output Control dialog box opens.



2. If this is a partitioned system, select the **Partition** in which this output is active.
3. In the Output box, select either **Point** or **Group** to populate the Name drop-down list with selections.
4. Select an output point or output group **Name** from the drop-down list.
5. Click **Activate** to activate the output point (or group) and select from the drop-down list one of the following choices:
 - **Preset** – to turn the output point to a pre-defined state.
 - **Set On** – to turn on the output point. Not available for CK722 panels.

- **Slow Flash** – to toggle the output point on and off slowly. Not available for CK722 panels.
 - **Fast Flash** – to toggle the output point on and off quickly. Not available for CK722 panels.
 - **Timed/Pulse** – to turn the output point for a specified time in seconds. If you select this option, you must enter the time in seconds in the **Duration** field.
6. Click **Perform** to manually activate the output point.
 7. To return the output point to a Normal state, click **Deactivate**, then click **Perform**.
 8. To temporary disable the output point, click **Disable**, then click **Perform**.
 9. Click **Exit** to close the dialog box.

Controlling Panel Relays

An operator with permissions can manually override system control of specific panel relays. For example, a panel relay may automatically operate lights in a specific area. An operator can manually set the panel relay to override system control and turn on the lights when they would normally be off. Not available for CK722 panels.

To Manually Control a Panel Relay:

1. From the P2000 Main menu, select **Control>Panel Relay**. The Panel Relay dialog box opens.



2. If this is a partitioned system, select the **Partition** in which this panel is active.
3. Select the Panel **Name** from the drop-down list.
4. Click **Set** to activate the relay.
5. Click **Reset** to deactivate the relay.
6. Click **Done** to exit the dialog box.

Security Threat Level Control

Security threat level control provides a rapid method of restricting access in case of an emergency. In the event of a security breach, an authorized operator will be able to quickly change access privileges for all entities at any terminal. The default security level for these terminals is 0 (the lowest) and could be raised up to 99 (the maximum security level).

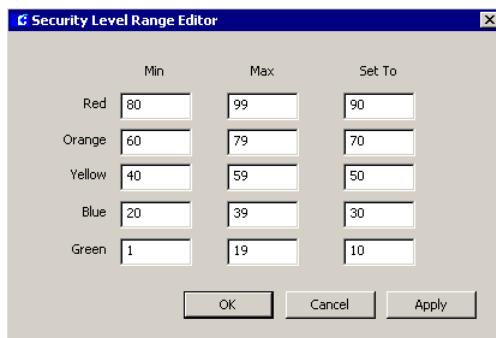
For this feature to work you must assign security levels to access badges using Access Profiles (see page 140). To obtain access at a door, the badge security level must be equal to or higher than the terminal security level. When an event occurs, the operator will raise the security level of the terminals in question, and access will be immediately restricted, unless the badge has the Executive privilege option enabled.

Defining Security Levels

The Security Level Range Editor allows you to modify the default values of the security level. Security levels are represented by five colored alert codes (Red, Orange, Yellow, Blue, and Green). For each color there is a range defined by Minimum, Maximum, and Set numeric values between 1 and 99. Once the ranges are defined, they can be assigned to selected terminals using the Security Level Control dialog box.

To Define Security Levels:

- From the P2000 Main menu select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Select the **Security Level** icon and click **Edit**. The Security Level Range Editor dialog box opens.



- Enter for each of the five colors, the **Minimum**, **Maximum**, and **Set To** values. Keep in mind that the Minimum has to be below the Maximum value, and that the Set To value must be in between the Minimum and Maximum values. The system does not allow overlapping of ranges.
- Once the security level color codes have been defined with acceptable ranges, click **Apply** to save the values while leaving the dialog box opened.
- Click **OK** to close the Security Level Range Editor dialog box.

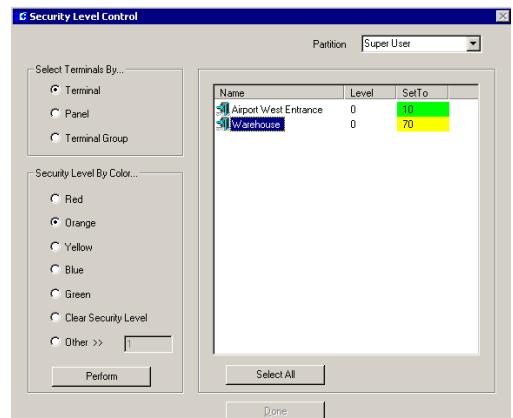
Applying Security Level

Once the Security Level is defined, you can rapidly apply a Security Level value to terminals using the Security Level Control dialog box.

To Apply Security Levels:

- From the P2000 Main menu, select **Control>Security Level**. The Security Level Control dialog box opens.

TIP: As an alternative, you can click the **Security Level Control** icon in the P2000 toolbar to rapidly open the Security Level Control dialog box.



- If this is a partitioned system, select the **Partition** in which the terminals reside.
- In the **Select Terminals By** box, select one of the following options:

Terminal – All terminals (for the partition selected) will be listed on the right side of the dialog box. Use this option to restrict access to the selected terminals.

Panel – All panels (for the partition selected) will be listed on the right side of the dialog box. Use this option to restrict access to all terminals connected to the selected panels. If you select a CK722 panel, the security level command is expanded to all ACO and DSO objects within the CK722 panel.

Terminal Group – All terminal groups (for the partition selected) will be listed on the

right side of the dialog box. Use this option to restrict at once access to all terminals that belong to the selected terminal groups.

4. Depending on your selection in the Select Terminals By box, select from the list box the desired terminal, terminal group or panel name. You can select multiple names by holding down the <Ctrl> key, or click the **Select All** button to select all items in the list.
5. In the **Security Level By Color** box, select one of the colored security levels you wish to apply, then click the **Perform** button.

The selected terminals in the list box will display in the **Set To** column the default value for that colored security level. The **Level** column will display the current security level at the terminal.

Note: If you raise the security level at terminals that use the "Override Reset Threat Level" option (terminals connected to S321 and CK705/CK720 panels 2.4 and higher), all time zone based overrides, host initiated overrides, and entity overrides will be immediately disabled. For more information, see "Override Reset Threat Level Box" on page 64. For terminals connected to CK722 panels, refer to the Security Mode Active Level feature described in the "Door Sequence Object" document.

6. To assign a particular value, select the **Other** option in the Security Level By Color box, enter the desired security level value, then click **Perform**. The selected terminals in the list box will be set to this value as well as display the color of that value.

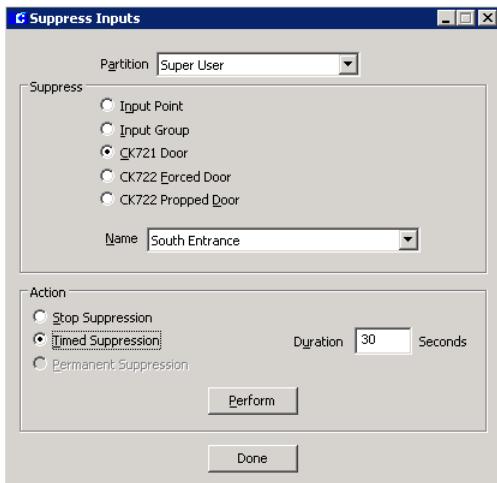
7. Once management determines that the emergency is over, you can either put the terminals in their previous level or remove the security level by selecting the item (terminal, terminal group or panel) from the list box then selecting the **Clear Security Level** option from the Security Level By Color box. The color will be removed from the terminal and the Set To and Level columns will display 0.
8. Click **Done** to close the Security Level Control dialog box.

Input Point Suppression

This feature allows an operator to rapidly suppress input points permanently or for a specific time period, during which the input point will stop reporting any changes of state and consequently will prevent alarms from displaying in the Alarm Monitor. For example, if an input point is constantly sending messages, the operator may want to suppress the input point until it can be determined what is causing the problem, and keep the input suppressed until the problem is resolved. This applies to forced door/proped door soft alarm inputs, as well as hardware inputs. The operator must have rights to the Suppress Inputs application to use this feature.

To Suppress Input Points:

1. From the P2000 Main menu select **Control>Suppress Inputs**.
2. Enter your password if prompted. The Suppress Inputs dialog box opens.



3. If this is a partitioned system, select the **Partition** in which the inputs are active.
4. In the Suppress box, select one of the following options:
 - Input Point** – to suppress the selected input point.
 - Input Group** – to suppress input points in the selected group. Not available for CK722.
 - CK721 Door** – to suppress forced/propped soft alarm input points associated with the selected CK721/CK720/CK705 door. This feature works if the Forced Door/Propped Door soft alarm is enabled.
 - CK722 Forced Door** – to suppress forced input points associated with the selected CK722 door.
 - CK722 Propped Door** – to suppress propped input points associated with the selected CK722 door.
5. Select a **Name** from the drop-down list.
6. In the Action box, select one the following:
 - Stop Suppression** – to cancel the Input Suppression condition. This will return the input point to fully functional status. (The

input point will start reporting changes of state alarms).

Timed Suppression – to suppress the input for the number of seconds entered in the **Duration** field. (The input point will not report alarms within this period). Not available for CK722. A value of zero will keep this input point suppressed until commanded to stop suppression.

Permanent Suppression – to suppress input points associated with CK722 panels. The input point will remain suppressed until commanded to stop suppression.

7. Click **Perform**. The Action selection goes into effect.
8. Click **Done** to exit the window.

Using the Control Center

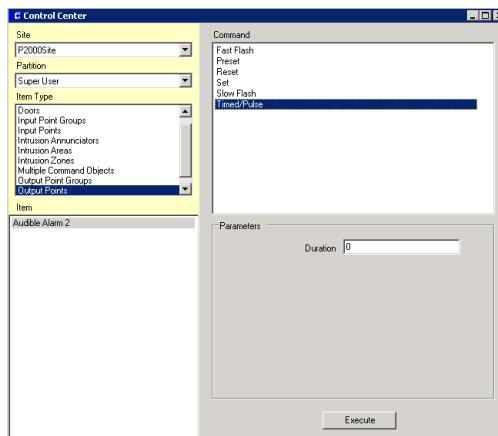
The Control Center application merges many of the operator-controlled functions, such as Door Control, Input Suppression, Output Control, etc. into one application. Almost all P2000 commands associated with a P2000 item (e.g. door, output point, intrusion area, etc.) can be performed from this single control application.

This application also enhances the available functionality, as the operator can control items at other P2000 sites, as long as that site is within the P2000 Enterprise.

In addition to the enhanced functionality, the Control Center application allows the system administrator to limit the operator to individual commands. For example, the system administrator can decide that an operator can perform an *Open for Access Time* task but not a *Timed Override* task. This granularity is not available in applications such as Door Control. These commands are assigned to operators using the Commands entry in User Role Management, see page 21.

To Use the Control Center:

1. From the P2000 Main menu select **Control>Control Center**. The Control Center dialog box opens.



2. From the **Site** drop-down list, select the site that contains the items you wish to control.
3. If this is a partitioned system, select the **Partition** in which the items you wish to control are active.
4. From the **Item Type** drop-down list, select the item type you wish to control. The bottom box will display all the configured items in the system of the item type selected.
5. In the **Item** box, select the item you wish to control. The Commands box on the right side will display the available commands to be performed for the selected item.
6. Select the **Command** you wish to perform. If additional parameters need to be configured, they will display in the box below.
7. After you enter the additional parameters, click the **Execute** button.
8. At the confirmation message, click **OK**.
9. Close the Control Center window.

Controlling Areas and Muster Zones

The Area Control and Mustering features provide additional security measures in specific areas of your facility, such as highly sensitive areas, dangerous areas, or areas that contain high-value materials. Using Area Control for example, an operator can define a minimum number of entities allowed in a *controlled area*, such as a bank vault. Alternatively, if using Mustering, the operator can define *muster terminals* as places of assembly, for tracking the location and movement of personnel in the event of an emergency.

Area Control

An Area is a designated section of a facility with one or more readers or input points assigned. The Area can be monitored at any time to determine the current count and the entry, or entry and exit of personnel or vehicles to, for example, a paint shop or parking structure within a plant or facility.

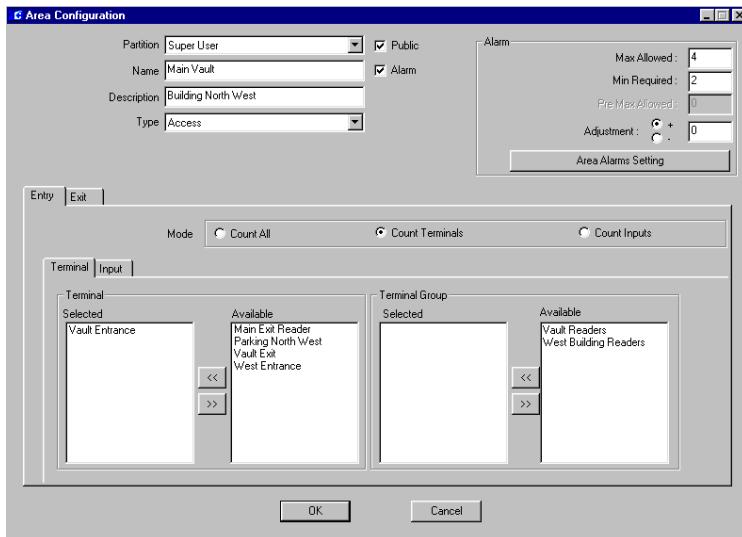
You can group readers and/or input points that are related to a particular section of your facility, for the purpose of reporting on the current whereabouts of entities. Areas do not have any access control or transaction processing functions; they are set up for reporting purposes only. This feature is useful on large sites with many card-controlled access points.

Configuring the Area

Use the Area Configuration dialog box to define the readers and input points that will monitor the entry and exit of persons or vehicles. Here you name and describe the specific Area, define the maximum and minimum entities allowed in the Area at any given time, and the count mode for the specific Area.

To Configure the Area:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the **Areas** root icon and click **Add**. The Area Configuration dialog box opens.
3. If this is a partitioned system, select the **Partition** that will have access to this Area, and select **Public** if you wish the Area to be visible to other partitions.
4. Enter a descriptive **Name** for the Area.
5. Enter an **Area Description** that will be meaningful to the operator.
6. Select the **Area Type** from the drop-down list. The options are:
 - Access** – Select Access to monitor entity count on a specific Area, for example a “Main Vault.”
 - Facility** – Select Facility to monitor entity count on the entire facility, for example “Bank ABC.”
 - Parking** – Select to monitor entity count in a parking structure, for example “Parking One.”



Note: It is possible for an entity to be counted on all three Area types at the same time, for example when the entity badges at the parking structure reader (Parking One), then badges at the facility reader (Bank ABC), and then proceeds to badge at a specific access Area (Main Vault).

7. Select the **Alarm** check box to define any or all of the following alarm fields:

Max Allowed – An alarm is generated when the maximum number of entities entered in this field has been exceeded. The status column in the Area Control dialog box will display *Max Allowed Alarmed*.

Min Required – An alarm is generated when the minimum number of entities entered in this field is not present at the same time in the specific Area. The status column in the Area Control dialog box will display *Min Required Alarmed*.

Pre Max Allowed – An alarm is generated when the pre-maximum number of entities entered in this field is reached. This field is available only if the Area Type selected is *Parking*. For example, if the Max Allowed

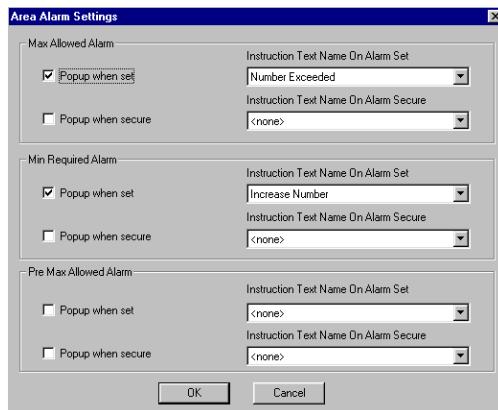
is 100 and the Pre-Max Allowed is 95, an alarm will be generated when 95 vehicles have entered the parking structure, that way the operator may advise other entities that the lot is full.

Note: In the Adjustment field, select the "+" or "-" sign, and enter a number to adjust any of the above counts by this number. For example if the Max Allowed is 100 and you entered a +2 in this field, an alarm will not be generated if the Max Allowed count is 102.

Area Alarms Setting

Area Alarms Setting enables the Alarm Monitor window to automatically pop up in front of other windows on the screen whenever any of the three Area Alarm types occur. The pop up will display a set of instructions related to that particular alarm. Before you assign instruction text to the various pop ups, you must first create instruction text. See "To Create Instruction Text:" on page 82.

1. In the Area Configuration dialog box, click the **Area Alarms Setting** button. The Area Alarm Settings dialog box opens.



2. In the Max Allowed Alarm box, enable the **Popup when set** and/or **Popup when**

secure check box, and select the **Instruction Text Name** from the associated drop-down list that will display in the Alarm Response window whenever the *Max Allowed Alarm* is in the alarm and/or secure state.

3. In the Min Required Alarm box, enable the **Popup when set** and/or **Popup when** **secure** check box, and select the **Instruction Text Name** from the associated drop-down list that will display in the Alarm Response window whenever the *Min Required Alarm* is in the alarm and/or secure state.
4. In the Pre Max Allowed Alarm box, enable the **Popup when set** and/or **Popup when** **secure** check box, and select the **Instruction Text Name** from the associated drop-down list that will display in the Alarm Response window whenever the *Pre Max Allowed Alarm* is in the alarm and/or secure state.
5. Click **OK** to return to the Area Configuration dialog box.

Note: The default Alarm Priority setting for Area alarms is 10.

Define Area Terminals and Inputs Points

1. In the Area Configuration dialog box, click the **Entry** tab to monitor Entry type reader terminals and input points.
2. Select one of the following count modes:
Count All – Select to count the number of entities that are granted access through both reader terminals and input points.
Count Terminals – Select to count the number of entities that are granted access through reader terminals only.

Count Inputs – Select to count the number of entities that are granted access through input points only.

3. Click the **Terminal** tab to select the terminals that will be monitored for Area count.
4. In the Terminal box, select the terminal from the Available list and click **<<** to move it to the Selected list.
5. In the Terminal Group box, select the terminal group from the Available list and click **<<** to move it to the Selected list.
6. Click the **Input** tab to select the input points that will be monitored for Area count.
7. In the Input box, select the input point from the Available list and click **<<** to move it to the Selected list.
8. In the Input Group box, select the input group from the Available list and click **<<** to move to the Selected list.

Note: *The terminal and/or input selected here cannot be assigned to another Area.*

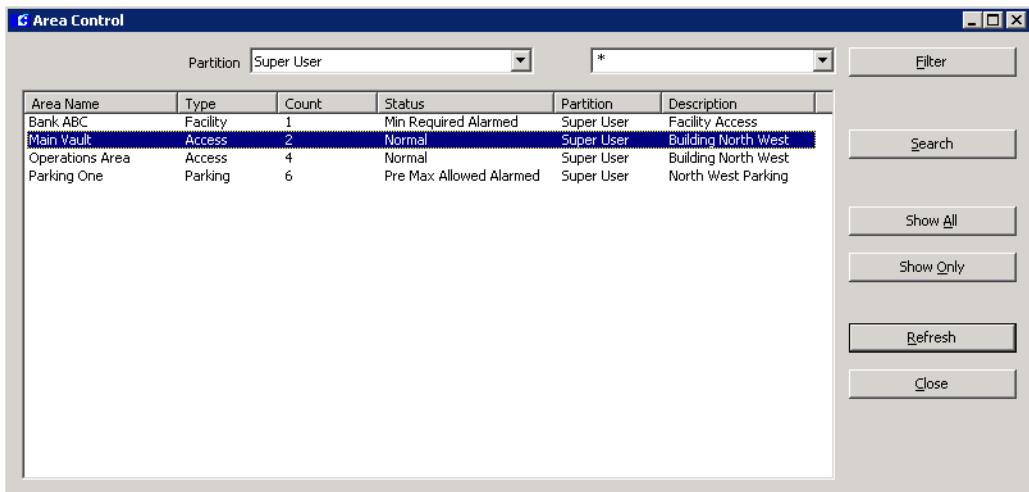
9. Click the **Exit** tab to monitor Exit type reader terminals and input points, and repeat the same steps above.
10. Click **OK**. A new icon will display under the root Area icon. When you click on the new Area icon, the parameters display on the right windowpane of the System Configuration window.

Controlling the Area

The Area Control dialog box is a real time control window that displays all the Areas defined in the Area Configuration dialog box. The default sort in the list box is by Area Name.

To Control each Defined Area:

1. From the P2000 Main menu, select **Control>Area Control**.
2. Enter your password if prompted. The Area Control dialog box opens.
3. Select the **Partition** from the drop-down list that contains the Areas you wish to control.



- To control a specific Area, use the **Filter** box to enter a filter criteria, such as “M*” then click the **Filter** button. The list box will display all Area Names that start with the letter “M”.

Note: You can also select a previously typed filter from the drop-down list. The list box will be refreshed when you select * from the Filter box or when you close the Area Control dialog box.

The list box displays the following information for each defined Area:

Area Name – The Area name, as configured in the Area Configuration dialog box.

Type – The Area type, as configured in the Area Configuration dialog box.

Count – Displays the number of entities currently in the specific Area.

Status – Displays one of the following:

- **Normal** – No alarm was generated.
- **Max Allowed Alarmed** – An alarm was generated because the maximum number of entities had exceeded.
- **Min Required Alarmed** – An alarm was generated because the minimum number of entities was not present at the same time in the specific Area.
- **Pre Max Allowed Alarmed** – An alarm was generated because the pre-maximum number of entities had been reached.

Partition – The Partition, as configured in the Area Configuration dialog box.

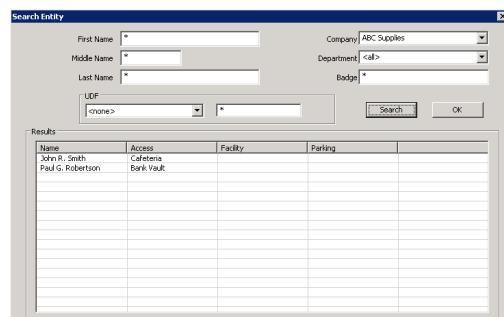
Description – The Description, as configured in the Area Configuration dialog box.

- To change the current sort order, click the specific column header in the list box.
- To display specific details of each Area, right-click the specific Area name, and select whether to **Show Only** the entities

passing the filter criteria entered in the Area Filter dialog box (refer to the next section “Defining Area Filters”), or to **Show All** entities in the Area Details dialog box (refer to “Displaying Area Details” on page 183). You can have any number of Area Details windows opened at the same time.

Note: You can also access the Area Filter and each Area Details dialog box by clicking the **Show Only** and **Show All** buttons on the right side of the Area Control dialog box.

- To search the whereabouts of a specific entity, click the **Search** button. The Search Entity dialog box opens.



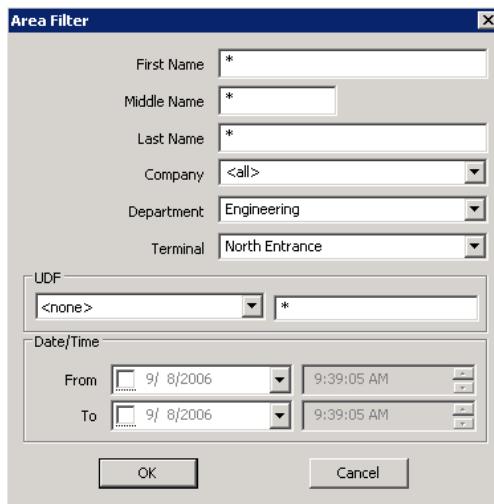
- Enter the information on any or all of the fields. For example, if you wish to search all entities that belong to the same Company or Department, you will enter the information in the associated field.
- To search by UDF, click the drop-down arrow and select any of the previously defined UDFs (Date type UDFs cannot be included in the search). Enter the UDF search criteria in the next field.
- Click **Search** to begin the search. The list box will display the names of the entities that match the search criteria. The respective Area Type column will display the Area name where the entity can be found.

11. Click **OK** to close the Search Entity dialog box and return to Area Control.
12. To manually update the current Count and Status displayed in the Area Control list box, click the **Refresh** button. This list is automatically updated every 10 seconds.
13. Click the **Close** button to exit Area Control.

Defining Area Filters

Each Area Details dialog box displays the total count of all entities that have been granted access to the specified Area. You can, however, define filter criteria to help you locate specific entities quickly and easily.

1. From the Area Control dialog box, right-click the Area Name that you wish to monitor and select **Show Only**, or select the Area Name and click the **Show Only** button on the right side of the screen. The Area Filter dialog box opens.



2. Enter the information on any or all of the fields to display specific entity information.

3. To search all entities that belong to the same Company or Department, click the specific drop-down arrows and select any of the previously defined Companies or Departments.
4. To search by UDF, click the drop-down arrow and select any of the previously defined UDFs (Date type UDFs cannot be included in the search). Enter the UDF search criteria in the next field.
5. To search by specific date and time, enter the information on the Date/Time box.
6. Click **OK**. The Area Details dialog box opens, displaying all the entities passing the filters defined in the Area Filter dialog box.

Displaying Area Details

The Area Details dialog box displays current count details and status information for the Area selected. Here you can monitor and manually change current entity count.

The Area Details can be accessed from the Area Control dialog box in one of the following ways:

- When you select an Area Name from the Area Control list box and click the **Show All** button, or right-click the Area Name and select **Show All**; or
- When you select an Area Name from the Area Control list box and click the **Show Only** button, or right-click the Area Name and select **Show Only**, enter the criteria in the Area Filter dialog box, and click **OK**.

In either case, the Area Details dialog box opens, showing the Area Name and Area Type in the window title. Refer to the following "Area Details Field Definitions" for details.

Area Details Field Definitions

Area Name – Displays the Area Name selected in the Area Control dialog box.

Current Status – Displays the current status of the Area. See the Status definitions on page 182.

Current Count – Shows the total number of entities currently in the Area, which were granted access through either reader terminals or input points.

Terminal Count – Shows the total number of entities currently in the Area, which were granted access through a reader terminal.

Input Count – Shows the total number of entities currently in the Area, which were granted access through an input point.

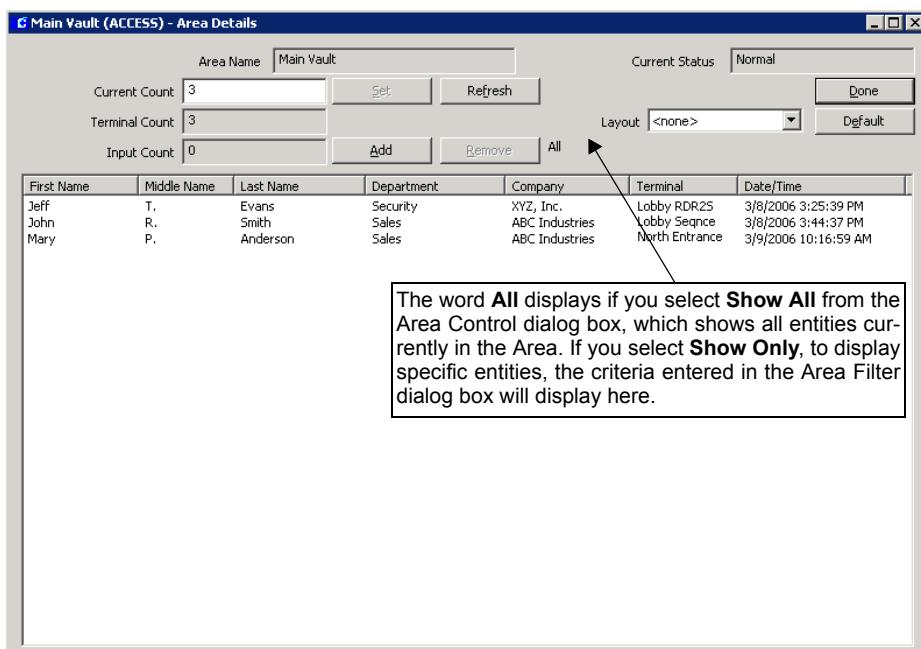
Set – This button is activated when the Current Count is manually changed, for example to add entities that you know are currently in the Area, but you do not know who they are. After

entering the new count, click the **Set** button then click **Yes** to confirm. The Input Count will increase or decrease by the number you manually enter in the Current Count field.

If you enter a new count in the Current Count field that is less than the total number of entities showing in the list box, you will be asked to remove some entities from the list, or set the count to a larger value.

Refresh – To manually update the Area Details list box, click the **Refresh** button. If a change in the Area count occurs, only the Count fields are updated automatically and the Refresh button changes color displaying a message to refresh the list in order to see the changes.

Add – If an entity is currently in the Area, but does not display in the Area Details list box, click the **Add** button and enter the information on any or all of the fields (or leave the default *), and click the **Search** button. Select the entity from the list and click **OK**. The name



will be added to the list and the Current Count and Terminal Count values will be updated.

Remove – This button is activated if one or more entities are selected in the list box. Click the **Remove** button to manually remove a selected entity, then click **Yes** to confirm. The Current Count and Terminal Count values will be updated.

Layout – This field relates to how the entity list displays in the list box. The drop-down list displays all Layout names that were previously defined in the Area Layout dialog box. (Refer to “Area Layout” for more information, and to the next section “Viewing the Details List” for instructions on changing the list box display.)

Done – Click **Done** to return to the Area Control dialog box.

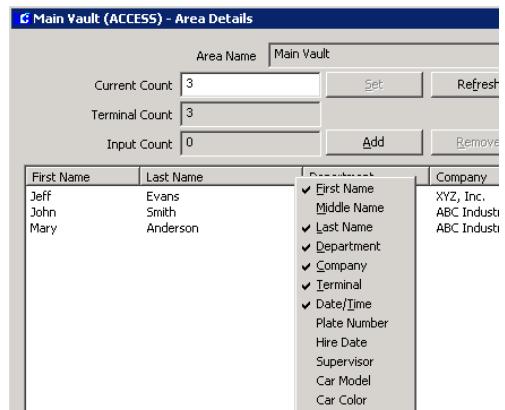
Default – Click the **Default** button to restore the seven default fields, refer to “Viewing the Details List”.

Viewing the Details List

The details list box displays all entities currently present in the Area. Individual operators can define how the information in the Area Details list box displays on their system. You may choose to display only specific data.

Note: *The previous sort order displays the next time you open the Area Details dialog box, but if the field you used to sort by is removed from the list, then the default sort is by the first column.*

1. To change the sort order, click the desired column header. The list will be sorted by the selected column.
2. To add or remove columns from the list box, right-click anywhere in the header to open a popup menu where you select the fields you wish to add or remove.



The popup menu displays seven default fields, plus any previously defined User Defined Fields. The check mark to the left of the field name shows which fields are currently displayed.

3. To change the position of the columns, drag and drop the column heading to desired position.
4. To select a previously defined layout, click the **Layout** drop-down arrow and select one from the list. See “Area Layout” for detailed instructions.
5. You can make modifications to previously defined layouts. Any changes made will be saved for future use and will be applied if you select <none> from the Layout drop-down list.
6. Click **Done** to return to the Area Control dialog box. If you apply a different layout or change the existing one, you will be asked if you wish to save the current view for future use.

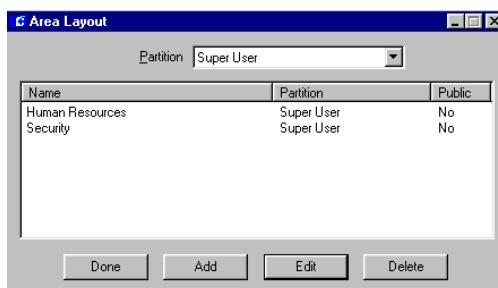
Area Layout

The Area Details dialog box displays a default view consisting of seven pre-stored fields. You can, however, create different layouts to display only certain information, according to your particular needs.

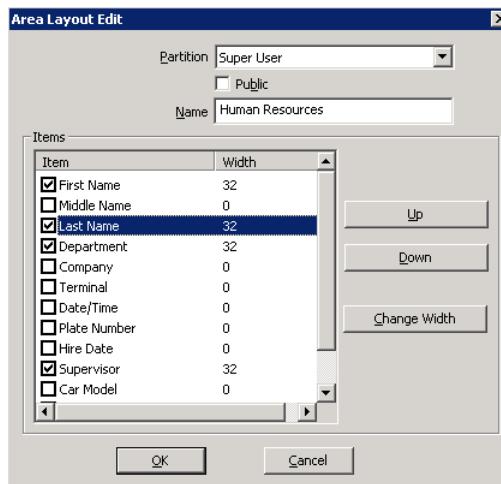
For example, a system administrator may want to monitor how many entities from a specific department are currently in the Area. In that case an Area Layout will be created to display only the fields selected on the Area Layout Edit dialog box.

To Define Area Layout:

- From the P2000 Main menu, select **Config>Area Layout**. The Area Layout dialog box opens.



- Click **Add**. The Area Layout Edit dialog box opens.



- If you use partitioning, select the **Partition** that will have access to this Area Layout.

- Select **Public** if you wish this Area Layout to be visible to all partitions.
- Enter the **Name** of the Area Layout. This name will display in the Layout field of the Area Details dialog box.
- The Items box displays seven default fields, plus any User Defined Fields, previously defined. Click the check box to select the fields you wish to display on the Area Details list dialog box. The default width (in characters) of the selected field will display.
- To change the width, either double-click the width field, or click the **Change Width** button and enter the new width.
- To change the order in which the fields will display, click the **Up** or **Down** button to move the field up or down on the list.
- When all information is entered, click **OK**. The new Area Layout displays in the Area Layout dialog box.
- Click **Done**. This Area Layout will now be accessible from the Area Details dialog box.

Mustering

The Mustering feature provides the capability of tracking personnel movement in the event of an emergency.

During the emergency, all personnel within a risk area are expected to evacuate and are required to present their identifier at a reader outside the risk area, thereby providing real time printed reports and/or online display information as to who may still be in a hazard area. The report and online display can be used to direct search and rescue operations. The list of personnel still in the risk area is derived from the last known access data, and then refined by tracking identifier activity as personnel move out of the risk area.

Mustering is initiated by a P2000 event, which triggers a *Muster*; or by manual action using the Muster Zone Status and Control dialog box. Once management or emergency personnel determine that the emergency is over, the *Muster* is terminated by an event that stops the *Muster*, or by manual action using the Muster Zone Status and Control dialog box.

Basic Definitions

Muster Zone – A Muster Zone is defined as any area within a facility that presents some risk to personnel; for example, a paint shop, an oil refinery, or a building’s electrical control center. In the P2000 Mustering feature, a Muster Zone is represented by one or more reader terminals.

Zone Terminal – Zone terminals are reader terminals that define a Muster Zone. These reader terminals can control entry to a zone, a paint shop for example, where the zone terminals would control the access. Zone terminals could also be readers at various locations where personnel are required to present their identifier as they move around, but which do not control access, as in an oil refinery for example. The general requirement is that when someone has presented their identifier at a zone reader terminal, it means that person is in the zone.

Muster Terminal – In an emergency, personnel are expected to move from the Muster Zone to a safe area, where muster terminals for the zone are located. As personnel arrive, they present their identifier at the muster terminal, allowing the system to know that they are no longer “at risk.” There can be any number of safe areas and muster terminals for a zone.

Sequester Terminal – Any terminal installed in a sequester zone. A sequester zone is defined as a secondary Muster Zone when the initial mustering may not provide permanent safety. In some cases a muster safe area may only provide temporary safety. If so, it is desirable to

move people to a safer (sequestered) area, where sequester terminals are set up and where arrival of personnel is recorded in the same way as muster terminals. Sequester Terminals are optional.

Muster – A Muster occurs when an event representing an emergency within the Muster Zone is triggered. Personnel in the Muster Zone are then expected to move to safety and present their identifier at a muster terminal to indicate that they are out of danger.

At Risk – When a Muster begins, all personnel within a Muster Zone are considered to be “at risk” until they present their identifier at a muster terminal so that their status can be upgraded according to the last used terminal.

Trapped – Personnel are considered trapped if they present their identifier at one or more zone terminal after the Muster begins, indicating that they are moving but possibly unable to escape the Muster Zone, for example due to a blocked exit.

Wandering – Personnel are considered to be “wandering” if they present their identifier at a terminal outside the Muster Zone, but not at a designated muster terminal. Wanderers are assumed to be on their way to a muster terminal, but because of circumstances, may be having difficulty finding a safe path. For example, a hazard may be spreading to other parts of the facility, causing difficulty escaping from the original event.

Mustered – Mustered personnel are those who have presented their identifier at a designated muster terminal since the start of a Muster.

Sequestered – Sequestered personnel are those who have presented their identifier at a designated “sequester terminal” since the start of the Muster.

Missing – Personnel are considered to be “missing” if they have presented their identi-

fier out of the zone, at an Exit terminal, but have not done it anywhere else.

Rescuer – Rescuers are personnel who present their identifier into the Muster Zone during the Muster. Rescuers are assumed to be carrying out search, rescue, or emergency control activities, and are tracked until they present their identifier at a muster or sequester terminal.

Note: *Trapped, Wandering, Missing, and Rescuer groups are only tracked if Track Movement is selected in the Muster Terminals tab, see page 193.*

Sequence of Steps

The basic procedures for defining and implementing Mustering are:

- Define Muster Zones and the terminals that are associated with it.
- Define the Events that start and end the Muster (alarms, card events, inputs), or any Events that are to be triggered when a Muster starts or stops (set outputs to turn lights on, open doors, activate alarms, etc.)
- Control Muster Zones before, during, and after a Muster.
- Generate reports and analysis reports.

Define Risk Areas and Muster Zones

Careful examination of a facility can disclose any potential risks and allow you to physically define the necessary Muster Zones. Following this process, use the Muster Zone Definition dialog box to define the Muster Zone, associate the necessary zone, muster, and sequester reader terminals with the Muster Zone, and select the appropriate options to control it.

To Define Muster Zones:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the **Muster Zones** icon and click **Add**. The Muster Zone Definition dialog box opens at the General tab.
3. Enter the required information in each tab according to your system requirements. See the following Muster Zone Definition Fields for details. As you work through the tabs, click **Apply** to save your settings.
4. When all entries are complete click **OK** to return to the System Configuration window. A new icon will display under the root Muster Zones icon. When you click the new Muster Zone icon, the parameters display on the right windowpane.

Muster Zone Definition Fields

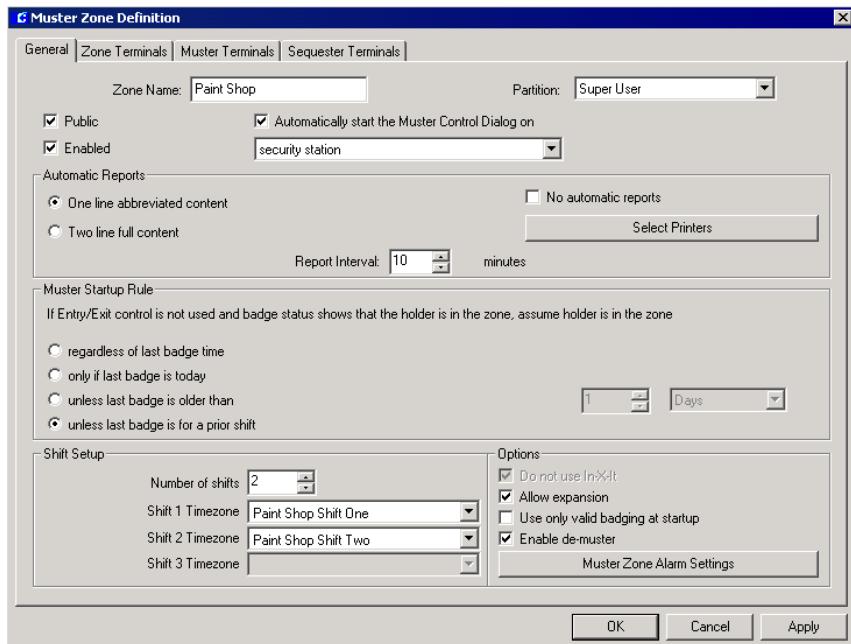
Zone Name – Enter a meaningful zone name. All zone names must be unique. Zones should be named logically, including information such as the zone location and what it contains, to be easily identified by rescue personnel in the event of an emergency.

Partition – Select the partition in which this Zone Name will be active.

Public – Select Public if you wish this Zone Name to be visible to all partitions.

Enabled – Select the Enabled check box for the system to recognize this Zone Name. To temporarily disable the Zone, select the check box again to disable it.

Automatically start the Muster Control Dialog – Select this check box to automatically open the Muster Zone Status and Control dialog box as soon as a Muster begins. If you enable this option, select from the drop-down list the



workstation that will automatically display the Muster Zone Status and Control dialog box when a Muster begins.

Note: To take advantage of this option, the P2000 software must be running at the designated workstation when the Muster begins.

One line abbreviated content – If enabled, a one-line report will be automatically printed when a Muster begins. This report will be printed at the Report Interval selected and will include first and last name, and date and time.

Two line full content – Select this option to automatically print more detailed entity information when a Muster begins. This report will be printed at the Report Interval selected and will include first and last name, date and time, terminal name, company, and department name.

Report Interval – Select from the spin box the report interval (in minutes) at which mustering reports will be printed during an emergency. When a Muster starts, the first report will be printed immediately.

No automatic reports – Select this check box if you do not wish to generate any of the above automatic reports.

Select Printers – Click this button to select a printer where either of the above report formats will be printed as soon as a Muster begins. When the Select Report Printers dialog box opens, select a previously defined printer name from the list and click **OK**. You can select more than one printer.

Note: Muster printers can only be selected from the system Server. We recommend setting up a printer to be used exclusively for printing Muster reports.

Muster Startup Rules

A number of rules are provided to guide you in determining whether an entity's last location will mean that the entity is inside or outside the Zone when a Muster is started. If an area has Entry/Exit control, the entry and exit status of each entity is used to determine if the entity is within the area at the time a Muster is started.

For mustering purposes, either the last valid or last invalid badging is used, depending on which has the latest date and time. You can prevent invalid badging from being used to determine the initial *At Risk* group, see "Use only valid badging at startup" on page 190 for details. Thereafter, a muster in progress will always use the last known badge activity, valid or invalid. Even invalid badging will show the entity's current location.

If Entry/Exit control is not used and badge status shows that the holder is in the zone, assume holder is in the zone (select one of the following options):

- **regardless of last badge time** – Select this option to include all entities regardless of the last badge time.
- **only if last badge is today** – Select this option to monitor who badged today.
- **unless last badge is older than** – Select this option to assume the entity is in the zone only if the last access grant was within the number of days, hours, or minutes selected.
- **unless last badge is for prior shift** – Select this option if your facility does shift work and the entity's last access grant was during a previous shift, to assume that the entity is no longer in the area. If enabled, the Shift Setup box is activated.

A basic rule for applying this option is to set up your time zones to start one after the other in the correct correlative order, for example Shift 2 should always start after

Shift 1, and Shift 3 should always start after Shift 2. See the example below.

Shift	Work Schedule	Week Days	Time Zone
Shift 1	8:00am - 5:00pm	Mon-Fri	7:30am - 5:30pm
Shift 2	5:00pm - 2:00am	Mon-Sat	4:30pm - 2:30am
Shift 3	2:00am - 8:00am	Tue-Sat	1:30am - 8:30am

Shift Setup

Number of shifts – If you enable "unless last badge is for prior shift," select from the spin box the number (1 to 3) of shifts in your facility.

Shift 1 - 3 Timezone – Select from the drop-down list the time zone assigned to each shift in your facility.

Muster Zone Definition Options

Do not use In-X-It – Not available in this version of the P2000 software.

Allow expansion – If selected, the Zone can be dynamically expanded during a Muster. This is useful in cases where the Zones are overlapped or not very rigidly defined. For example, an emergency event in one part of the facility might spread to adjacent areas and the Zone could be expanded to include terminals in those areas as the need arises. As expansion takes place, the badging activity at the newly incorporated terminals is examined to determine which personnel need to be added to the *At Risk* group.

Use only valid badging at startup – If selected, only valid badging will determine if the entity is inside a risk area. If this option is not selected, any invalid badging inside a risk area will be included in determining if the entity is inside the risk area.

Enable de-muster – If selected, and a Muster has been stopped, and prior to returning the Zone to the *Ready* status again, you can click

the **De-Muster** button in the Muster Zone Status and Control dialog box to put all personnel who were in the *At Risk* group back at their initial location when the Muster began. De-Muster can also be activated by a P2000 Event if desired.

Note: To end an emergency by a specific event, you must specify any number of different events as Muster terminating events. See "Mustering Events" on page 193.

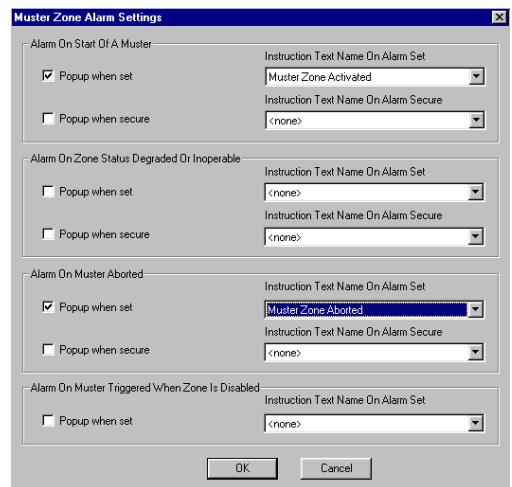
Muster Zone Alarm Settings

Muster Zone Alarm Settings enable the Alarm Monitor window to automatically pop up in front of all other windows on the screen whenever a Muster alarm condition occurs.

You can also specify instruction text that will display when an operator responds to a Muster alarm going into a Set and/or Secure state. Enabling the Popup feature and selecting Instruction Text are independent tasks, and can be used in any combination.

Before you assign instruction text to the various pop ups, you must first create instruction text. See "To Create Instruction Text:" on page 82.

1. In the Muster Zone Definition dialog box, click the **Muster Zone Alarm Settings** button. The Muster Zone Alarm Settings dialog box opens.



2. Enable any of the following **Popup when set** and/or **Popup when secure** check boxes, and select the **Instruction Text Name** from the associated drop-down lists that will display in the Alarm Response window whenever any of the following alarm conditions occur:

Alarm On Start of A Muster – An alarm message is generated at the start of a Muster.

Alarm On Zone Status Degraded or Inoperative – An alarm message is generated if one or more panels or terminals that belong to a Muster Zone are disabled or go down.

Alarm On Muster Aborted – An alarm message is generated if system operation is affected during the emergency. For example, if database problems are encountered during the Muster, the Muster cannot continue and will abort.

Alarm On Muster Triggered When Zone is Disabled – An alarm message is generated when a disabled Muster Zone is triggered to be started by an event. This option does not have a specific event or action of any kind that makes it Secure, and does not have a corresponding popup option and related instruction text.

3. Click **OK** to return to the Muster Zone Definition dialog box.

Note: *The default Alarm Priority setting for Muster alarms is 5.*

Defining Zone Terminals

Use the Zone Terminals tab to select the terminals and/or terminal groups that will provide access to the zone defined for mustering purposes. These terminals may be of any type, Access, Entry, or Exit.

1. From the Muster Zone Definition dialog box, click the **Zone Terminals** tab.
2. From the **Available Terminals** list, select the terminal that will provide access to the Muster Zone.
3. Click **<<**. The terminal will be included in the **Selected Terminals** box.
4. From the **Available Terminal Groups** list, select the terminal group that will provide access to the Muster Zone.
5. Click **<<**. The terminal group will be included in the **Selected Terminal Groups** box.

Note: *The Available Terminals and Available Terminal Groups boxes display only terminals that have not yet been defined as Muster or Sequester Terminals.*

Defining Muster Terminals

Use the Muster Terminals tab to select the terminals and/or terminal groups that will be designated as mustering terminals, and to associate these mustering terminals with each risk area.

Muster terminals should be dedicated to the mustering function; they should not control access. From an operational viewpoint, it does not matter if identifiers are valid at muster terminals. As long as they are recognized by the P2000 system, its use at muster terminals will be recognized during the Muster, regardless if a red or green light displays at the terminal.

During an emergency, all personnel within the risk zone are required to present their identifier at any defined muster terminal to provide real time information as to their location.

1. From the Muster Zone Definition dialog box, click the **Muster Terminals** tab.
2. From the **Available Terminals** list, select the terminal where entities will badge in the event of an emergency.
3. Click **<<**. The terminal will be included in the **Selected Terminals** box.
4. From the **Available Terminal Groups** list, select the terminal group where entities will badge in the event of an emergency.
5. Click **<<**. The terminal group will be included in the **Selected Terminal Groups** box.
6. Enable **Muster At Any Non Zone Terminal** if in the event of an emergency you wish to allow entities the option of badging at any terminal that has not been defined as a Zone Terminal.
If this option is selected, terminals not assigned to the zone are treated as muster terminals, and Movement Tracking is limited to *Trapped* and *Rescuers* only.
7. Enable **Muster Only At Terminals Selected Here** to have entities, in the event of an emergency, badge only at the muster terminals selected in this tab. This is the default option, and allows you to select specific muster terminals for the zone.

8. Select the **Track Movement** check box to trace entity movement within the defined Muster Zone. Entities may be considered *Missing, Trapped, Wandering, or Rescuers*, depending on where and when they badge. Refer to “Basic Definitions” on page 187 for details. To get the best use of this feature, do not enable the **Muster At Any Non Zone Terminal** option.
9. When you finish defining the zone and muster terminals, you may click **Apply** to save your entries and continue with defining the optional sequester terminals; or click **OK** to save your entries and close the Muster Zone Definition dialog box.

Note: *The Available Terminals and Available Terminal Groups boxes display only terminals that have not yet been defined as Zone or Sequester Terminals.*

Defining Sequester Terminals

In the event of an emergency, personnel who initially badged at a muster terminal can be moved in groups to a safer offsite location, a sequester zone, where they will be required to badge at a sequester terminal, and therefore, provide real time information that they have been moved outside the risk area to a safer location.

Use the Sequester Terminals tab to define the terminals and/or terminal groups that will be designated as sequester terminals. Sequester terminals are optional.

1. From the Muster Zone Definition dialog box, click the **Sequester Terminals** tab.
2. From the **Available Terminals** list, select the terminal where entities will badge once they are moved to a safer location.
3. Click **<<**. The terminal will be included in the **Selected Terminals** box.

4. From the **Available Terminal Groups** list, select the terminal group where entities will badge once they are moved to a safer location.
5. Click **<<**. The terminal group will be included in the **Selected Terminal Groups** box.
6. When you finish defining the zone, muster, and optional sequester terminals, you may click **Apply** to save your entries, or click **OK** to close the Muster Zone Definition dialog box.

Note: *The Available Terminals and Available Terminal Groups boxes display only terminals that have not yet been defined as Zone or Muster Terminals.*

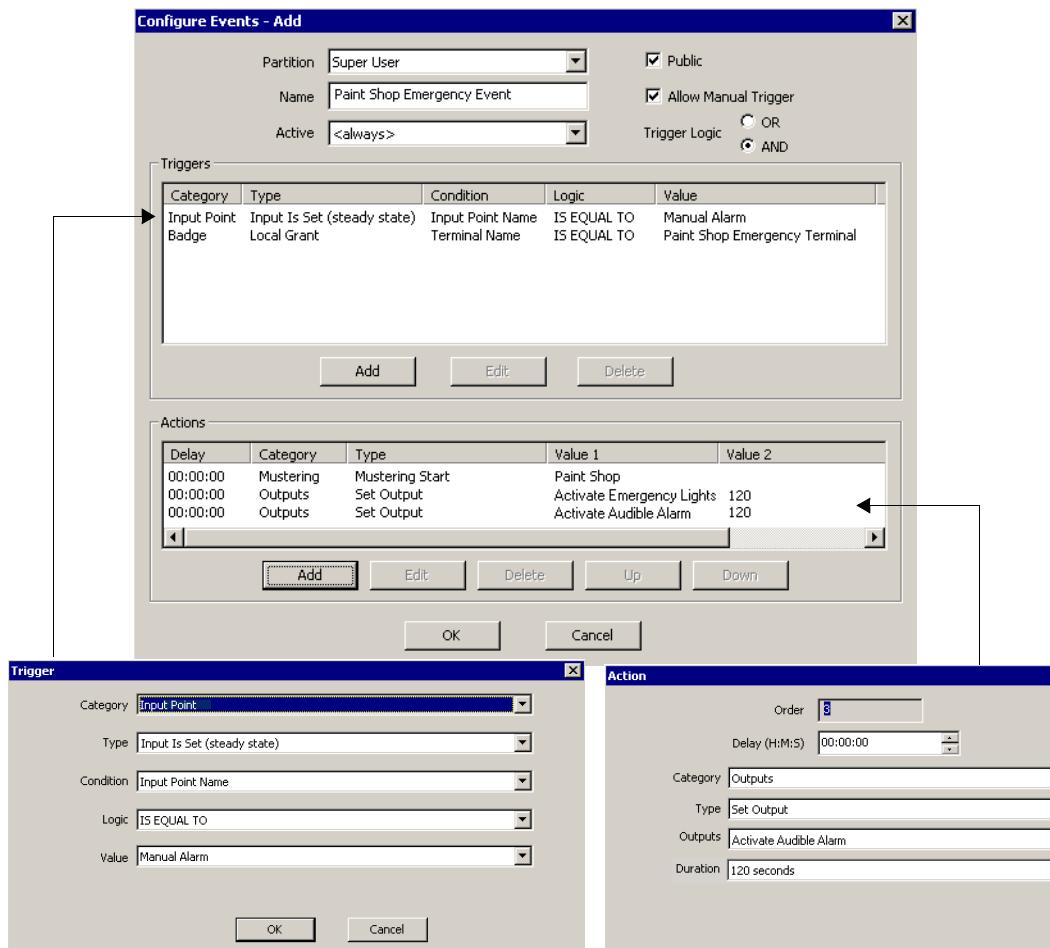
Mustering Events

After Muster Zones are defined, they can be associated with one or more events, each of which can trigger a Muster for that zone as one of its actions.

Event Actions allow an event to start and stop a Muster, while Event Triggers allow the starting and stopping of a Muster to trigger additional P2000 events, such as unlocking doors or turning on audible or visual alarms to alert personnel of danger in the area.

The events used can include one or more inputs going to an alarm state in response to a variety of possible signaling devices, alarms or manual actions. You can also specify one or more output points that will be set upon triggering of a Muster.

You can end the emergency (de-mustering) by a specified event or events, and specify any number of different events as muster terminating events.



The following event actions are required to start a Muster, stop it, save data, and/or de-muster, and then make the zone *Ready* for another Muster: Mustering Start, Mustering Stop, Make Zone Ready, De-Muster, and Save Muster Data (last two are optional).

To allow a Muster to be triggered by an event and to trigger other P2000 events, use the information on “Creating Events” on page 206 to create new event triggers and actions.

In the above example, the *Paint Shop Emergency Event* has been programmed to start the

mustering, turn emergency lights on, and activate an audible alarm (actions) when input point *Manual Alarm* goes into alarm after the operator presents the badge at the *Emergency Terminal* (triggers).

Controlling Muster Zones

Use the Muster Zone Status and Control dialog box to monitor the status of a Muster Zone; and when a Muster is initiated, to control all the activities of the Muster in progress.

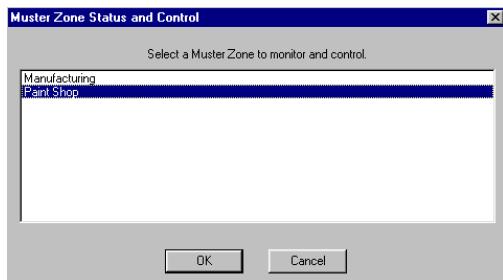
Mustering can be manually started and terminated by operator action using the Muster Zone Status and Control dialog box. When mustering is triggered by a P2000 event, the Muster Zone Status and Control dialog box automatically opens at the designated workstation selected in the Muster Zone Definition dialog box, if this option is selected for the zone.

When an initiating event occurs, the Muster Zone enters a *Running* state. Any events scheduled to occur on starting the Muster are triggered, and the zone determines the initial situation from last badge information and any time-based rules defined for the zone. Once the initial situation is known, the report of entities still inside the zone is output repeatedly at the interval set up when the zone was defined. As entities badge at the designated muster terminals the situation is updated to show the new list of entities still in the zone.

Operators must have Muster Control rights to use this feature. Depending on the permissions assigned using Users Roles, some or all operators may be able to control muster zones at any time. For detailed information see “User Role Management” on page 21.

To Manually Control a Muster:

- From the P2000 Main menu, select **Control>Muster Status/Control**. The Muster Zone Status and Control dialog box opens.



- Select the Muster Zone you wish to control and click **OK**. The Muster Zone Status and Control dialog box opens, showing the Muster Zone name in the window title.

The list box displays the name, last known location, and time of all entities currently in the defined Muster Zone. Refer to the following “Muster Zone Status and Control Field Definitions” for details.

Muster Zone Status and Control Field Definitions

Zone – Displays the name of the Muster Zone to be monitored.

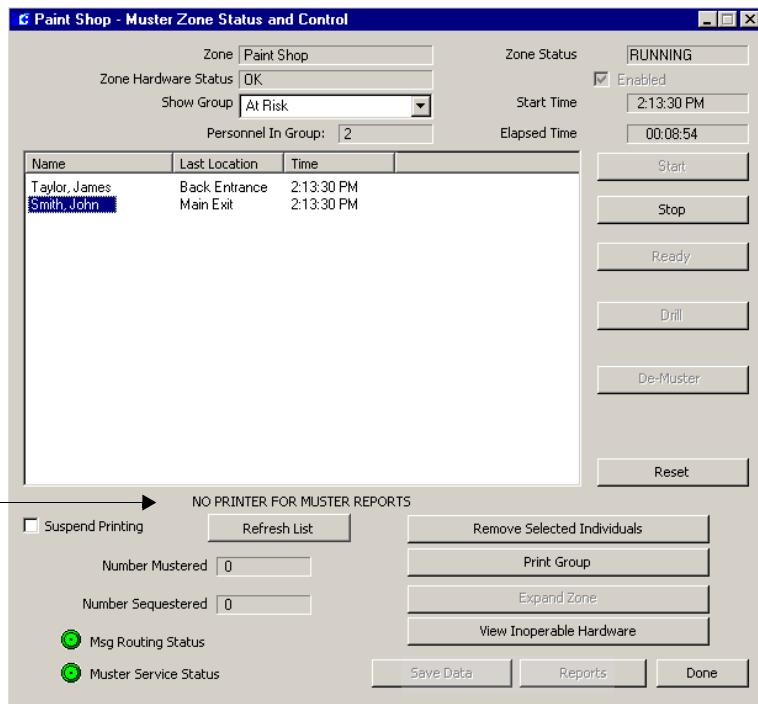
Zone Status – Displays the status of the Muster Zone. A Muster Zone can be *Ready*, *Running*, *Stopped*, *Aborted* or *Disabled*. As personnel, who were initially in the zone, badge at other readers during a *Running* Muster, their location is tracked and they are put in the appropriate group as their location changes.

Zone Hardware Status – Displays one of the following status:

- **Inoperable** – If all muster terminals or panels are disabled or down.
- **Degraded** – If one or more muster terminal or panel is disabled or down.
- **OK** – If all muster terminals or panels are enabled.

Show Group – Select from the drop-down list the group you wish to display. This allows switching the display to any of the available groups. Choices are: *At Risk*, *Missing*, *Trapped*, *Wandering*, *Mustered*, *Sequestered*, and *Rescuer*. Refer to “Basic Definitions” on page 187 for details. The *At Risk* group is the default display.

Personnel In Group – Displays the current number of entities in the group selected in the Show Group drop-down list.



Enabled – Select the Enabled check box for the system to control this Zone. To temporarily disable the Zone, select the check box again to disable it. You can disable a Zone only when it is in the *Ready* status.

Start Time – Displays the time the Muster was triggered or manually started.

Elapsed Time – Displays the time that has gone by since the Muster started.

Start – Click the **Start** button to manually start a Muster. To manually start a Muster, the Zone must be in the *Ready* status. Once started, the Muster Service determines the initial state of the Zone and the *At Risk* group displays by default.

Stop – Mustering is stopped by triggering an event designated to automatically stop a Muster. To manually terminate a Muster, click the **Stop** button. The Zone Status will display the

Stopped state and analysis reports become available by clicking first the **Save Data** button and then the **Reports** button.

Once the Muster is stopped the Zone Control quits updating the list of entities.

Ready – When a Muster is manually stopped, it may be necessary to ensure that all triggering devices, such as alarms, manual switches or push buttons are reset so that another Muster cannot be inadvertently started. Once it is determined that the Zone can be made ready for another Muster, click the **Ready** button to enter the *Ready* state.

Drill – To participate in a disaster preparedness exercise, a Muster can also be run as a drill by clicking the **Drill** button. A drill differs from the real thing by the fact that during a drill, events that would otherwise send external alarms to outside emergency response agencies can be suppressed.

This feature applies only to events triggered by the starting or stopping of a Muster; it cannot be applied to the events that normally start a muster. When you define the trigger, and select “Do not trigger for muster drill” it will prevent any event action from being carried out when a drill is in progress. A drill can only be initiated through the Muster Zone Status and Control dialog box.



De-Muster – Click this button to put all personnel who were initially in the zone back to their location when the muster began. This option is used when muster terminals are located within the Zone, in that case entities are not required to badge back into the Zone. All mustered entities can be automatically restored to their last badge location through the De-Muster capability, as long as the “Enable de-muster” option is selected in the Muster Zone Definition dialog box. This function is password protected.

Reset – Click this button to stop a Muster in progress and reset the Zone Status back to *Ready*. The Reset function is not normally used, but under unusual circumstances, such as database problems during a Muster causing the Muster to abort, the Reset button must then be used to reset the Zone.

Suspend Printing – Enable this option to momentarily suspend the automatic printing of the selected group, to add paper or take care of some other printer problem.

Refresh List – Click this button to update the list box.

Number Mustered – Displays the total number of entities who have badged at a designated muster terminal.

Number Sequestered – Displays the total number of entities who have badged at a designated sequester terminal.

Remove Selected Individuals – This button can be used to manually move one or more entities from any group to any other group while a Muster is *Running* or *Stopped*. You can use it to make the final group content reflect a situation where, for example, some personnel left the Muster Zone but did not badge at a muster terminal, yet their current location is known.

Print Group – Click this button to print the group currently being displayed. Printing will be done at the designated printers selected in the Muster Zone Definition dialog box.

Expand Zone – Use this option to expand a Muster Zone during an emergency. For instance, a hazard may spread requiring zones that initially were not involved, to be added to the active Muster Zone. You can only use this option if “Allow expansion” was enabled in the Muster Zone Definition dialog box. When you click this button, a list of available terminals displays, where you can select the terminals you wish to add. All personnel who last badged at any of the new terminals are added to the *At Risk* group.

View Inoperable Hardware – Click this button to view muster terminals or panels that are not enabled or are down.

Note: The Message Routing Status indicator at the bottom of the window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.

The Muster Service Status indicator will be displayed in green to indicate that Muster Service is up and running. If Muster Service goes down, the indicator will turn red.

Save Data – After the Muster is terminated, you may click this button to store the Muster data in the database for later evaluation.

Reports – Once the Muster is stopped and data has been saved, analysis reports can be run by clicking this button. These reports are run using the P2000 Standard Report feature. Reports can be run during the *Stopped* state, or at a later time when the Muster data has been saved. For more information see “Muster Reports”.

Viewing and Printing Muster Transactions in Real Time

Once a Muster is started, an alarm is generated and displayed in the Alarm Monitor window, and all mustering transactions are sent through real time messages to the Real Time List. As the Muster Zone status changes, corresponding Muster-related messages are generated and displayed. You must select the Mustering check box in the Real Time List window to display all mustering transactions as they occur. Refer to “Using the Real Time List” on page 213 for more information.

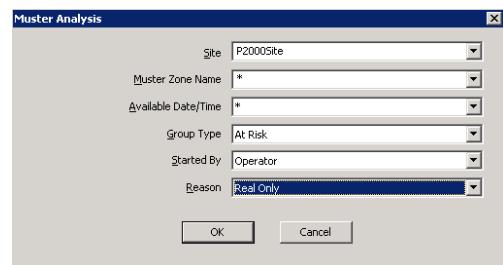
To print mustering transactions as they occur, you can either print them from the Real Time List window, or select the Mustering Zones check box in the Site Parameters dialog box, Printing tab. Refer to “Printing Tab” on page 31 for more information.

Note: The Muster Zone hardware status will also display in the System Status window. For more information see “System Status” on page 318.

Muster Reports

Muster reports are available while the Muster is in the *Stopped* state, or afterward if the Muster state is saved before returning the zone to the *Ready* state. These reports allow management to assess preparedness for emergencies and improvement of procedures for handling future events.

When you click the **Reports** button in the Muster Zone Status and Control dialog box, the Muster Analysis dialog box opens.



The **Site** field displays the name of your local site or any remote site on an Enterprise system.

The **Muster Zone Name** and **Available Date/Time** fields will only display selections if the Muster Zone was started at least once.

In the **Group Type** drop-down list select one of the following reports:

- **At Risk** – Displays the list of personnel who are within the Muster Zone and have not yet checked-in at a muster terminal.
- **Missing** – Displays the list of personnel who have not checked-in at any defined, mustered, or sequestered terminal.

- **Trapped** – Displays the list of all personnel who may be trapped in the Muster Zone.
- **Wandering** – Displays the list of all personnel who are not believed to be in the Muster Zone, but who have not yet checked-in at a muster terminal.
- **Mustered** – Displays the list of all personnel who have badged at a muster terminal.
- **Sequester** – Displays the list of all personnel who have badged at a sequester terminal.
- **Rescuer** – This report tracks all rescue personnel throughout the site.

In the **Started By** drop-down list select whether this Muster Zone was started by an *Operator* or by an *Event*.

In the **Reason** drop-down list select the reason why this Muster was started, whether it was a real Muster, a drill, or both.

After you have entered your selections, the Muster Analysis Report displays in the Crystal preview window showing the criteria selected and the total number of entities in the Muster Zone. This report lists all Mustering activity within a specified time frame by zone name, start and stop times and whether it was a drill or real emergency.

This report can also be generated using the **Report>Run Report** option and selecting the Muster Analysis report.

Intrusion Detection

The Intrusion Detection function has been designed to sense an intrusion into a protected building (detection) and report it to responsible parties (annunciation). This is accomplished with a combination of detection, control, and reporting devices such as a control

panel, input devices (sensors), output devices (bells, sirens), a keypad, and a central station.

The Intrusion Detection system consists of sensors, connected to a CK722 panel, capable of detecting various intrusion or burglary events. These intrusion detection sensors are associated with physical zones and grouped into areas; also intrusion events use audible annunciators to signal that a zone or area is in alarm condition.

Note: *Intrusion detection is also provided by the optional OPC Aritech® panel interface. Refer to “OPC Aritech Intrusion Interface” on page 205 for specific information.*

Areas are used to control Zones and can be commanded to be armed or disarmed, thereby causing all associated Zones to become armed or disarmed (or if armed possibly alarmed).

Areas are stateless objects that are only used to control zones. Zones maintain state and can be in states such as armed, disarmed, bypassed or alarmed. An authorized user at a P2000 workstation or CK722 connected keypad/display terminal can arm or disarm an area, bypass a zone, and silence or activate an annunciator, assuming that the user has the appropriate authorization.

A properly configured intrusion detection system should:

- Detect an unlawful intrusion
- Identify the location of the intrusion
- Inform local security forces that an intrusion has been detected
- Signal an alarm to a remote location (e.g. a central station), so the proper authorities can be dispatched
- Signal the intruder that has been detected

Basic Definitions

Annunciator – An Annunciator is any electrical device connected to a CK722 or Aritech output point, which is used to signal audibly a zone alarm. An annunciator can be silenced or activated manually.

Area – A group of zones within a building (e.g., the perimeter, the main entrance, the entire facility). This logical grouping is for the purpose of arming and disarming the associated zones.

Armed – The state of a zone that reports intrusions unless it is bypassed. When an area is armed or disarmed, it arms or disarms all associated zones.

Bypassed – The state of a zone that does not report intrusions. This state is intended for maintenance use. If a zone is bypassed an intrusion will not be detected nor sent to the P2000 Server.

Central Station – A system designed to monitor several remote locations. The connection to a central station is usually via a dial-up phone connection using a standard protocol.

Disarmed – The state of a zone that is disabled from reporting intrusion alarms. This state is typically used during hours when zones are occupied.

Intrusion – An unauthorized entry to an armed zone that results in an alarm state for the zone.

Keypad/Display – The Keypad/Display consists of a keypad and LCD display connected to the CK722 panel and used to arm or disarm an area, bypass a zone or silence or activate an annunciator.

Sensor – A device used to detect a change in a physical property. A sensor senses an event that could represent intrusion such as a glass break, motion or door contact.

Zone – A collection of one or more sensors used for intrusion detection.

Basic Intrusion Components

This section describes the basic components of an intrusion detection system. The intrusion detection system consists of the P2000 software, the panel (CK722 or Aritech) firmware, I/O modules (attached to sensors and annunciators), and CK722 connected keypad/display modules.

The P2000 software is used to:

- Configure CK722 intrusion items (areas, zones, and annunciators) using SCT. Refer to the *System Configuration Tool (SCT) Manual* and to the *CK722 Commissioning Guide* for details.
- Configure the authorization levels of the users (using User Roles), which allow precision control over what activity an operator can perform, such as intrusion group management, commands, (alarm, disarm, bypass), and viewing of intrusion status. See page 21 for details.
- Configure alarm options for intrusion areas, zones, and annunciators using the Message Data Configuration application, see page 110.
- Configure intrusion groups to define the intrusion operations an entity can perform, see page 201.
- Control, monitor, and display the status of areas, zones, and annunciators, see “Intrusion Management” on page 202.
- Forward the alarm status to the central station, see “Central Station Support” on page 205.
- Define event triggers and actions associated with intrusion areas, zones, and annunciators.

Intrusion Configuration

Refer to the instructions provided with the Aritech panel, and to the *SCT Manual* and *CK722 Commissioning Guide*, to define the intrusion system with the number and type of sensors, number of keypads (CK722 only) or annunciators required, how these input and output devices will be associated with zones, and how zones will be included within areas.

Once you configure the intrusion elements, these items will display in the P2000 screens for selection.

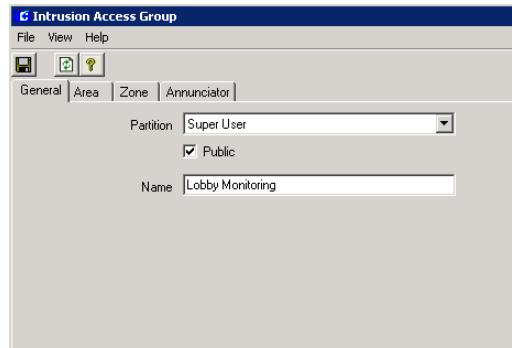
The following sections describe intrusion configuration and operation procedures using the P2000 software.

Intrusion Access Groups

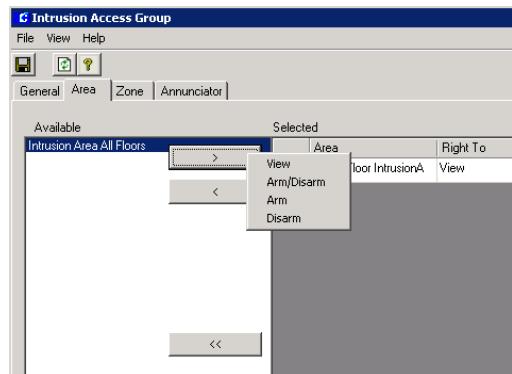
After intrusion elements have been defined, you can use the Intrusion Access Group application to establish what intrusion operations an entity can perform. An intrusion group is a collection of functions associated with intrusion areas, zones, and annunciators. You can create intrusion groups that allow entities to arm specific areas or silence specific annunciators. After Intrusion Access Groups are created, they are available to be assigned to entities via the Access Profiles tab in the Entity Management window.

To Create Intrusion Access Groups:

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Select the **Intrusion Groups** icon and click **Add**. The Intrusion Access Group window opens at the General tab.

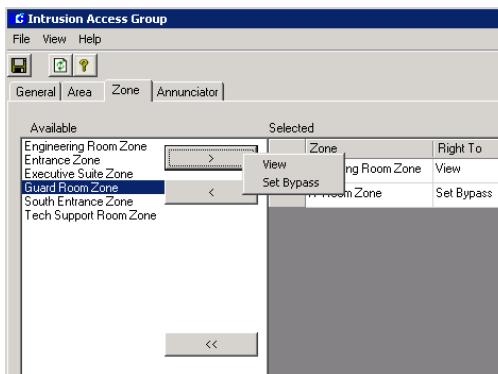


- If this is a partitioned system, select the **Partition** name in which the items for this Intrusion Access Group reside.
- Select **Public** if you wish this Intrusion Access Group to be visible to other partitions.
- Enter a descriptive **Name** for the Intrusion Access Group.
- To include Areas in this group, click the **Area** tab. From the list of **Available** Areas at the left side of the window, select the area you wish to include in the Intrusion Access Group.

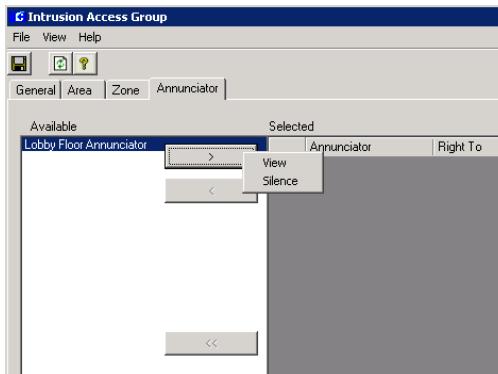


- Click the > button and select from the drop-down list the operation allowed to be performed for the selected Area. The **Selected** box will display the Area and function selected.

- To include Zones in this group, click the **Zone** tab. From the list of **Available** Zones at the left side of the window, select the zone you wish to include in the Intrusion Access Group.



- Click the > button and select from the drop-down list the operation allowed to be performed for the selected Zone. The **Selected** box will display the Zone and function selected.
- To include Annunciators in this group, click the **Annunciator** tab. From the list of **Available** Annunciators at the left side of the window, select the annunciator you wish to include in the Intrusion Access Group.



- Click the > button and select from the drop-down list the operation allowed to be

performed for the selected Annunciator. The **Selected** box will display the Annunciator and function selected.

- Click the **Save** icon. The Intrusion Access Group will be available for assignment in the Access Profiles tab of the Entity Management window.

Intrusion Management

Management of intrusion includes displaying the current state of intrusion items as well as issuing commands for such activities (arm, disarm, bypass, etc.). The following sections describe how to monitor and control intrusion items.

Using the Intrusion Command Center

The Intrusion Command Center application is a dynamic display of Areas, Zones, and Annunciators configured in the system. It allows operators to arm and disarm areas; start or stop bypass on selected zones; and silence or activate any annunciator.

To Use the Intrusion Command Center:

- From the P2000 Main menu select **Control>Intrusion Command Center**. The Intrusion Command Center window opens.



2. To display and control intrusion Area items, select **Area** from the top box. The middle box will display all the configured intrusion Areas in the system. Select the area you wish to control, and from the bottom portion of the window select the command you wish to perform.
3. To display and control intrusion Zone items, select **Zone** from the top box. The middle box will display all the configured intrusion Zones in the system. Select the zone you wish to control, and from the bottom portion of the window select the command you wish to perform.
4. To display and control intrusion Announcer items, select **Annunciator** from the top box. The middle box will display all the configured intrusion Announciators in the system. Select the annunciator you wish to control, and from the bottom portion of the window select the command you wish to perform.

Note: The function buttons at the bottom of the Intrusion Command Center vary according to the panel (CK722 or Aritech) where the selected intrusion item resides.

The intrusion item selected will display an icon representing its current state. Refer to the following condition indicators:

Area Icons	
	Disarming
	Disarmed
	Arming
	Armed
	Mixed
	Fault
	Unknown
	Disarmed,Bypassed,Sealed
	Disarmed,Bypassed,Unsealed
	Disarmed,No-bypass,Sealed
	Disarmed,No-bypass,Unsealed
	Armed,No-bypass,Sealed
	Armed,No-bypass,Unsealed
	Armed,Bypassed,Sealed
	Armed,Bypassed,Unsealed
	Alarmed,Disarmed,No-bypass,Sealed
	Alarmed,Disarmed,No-bypass,Unsealed
	Alarmed,Disarmed,Bypassed,Sealed
	Alarmed,Disarmed,Bypassed,Unsealed
	Alarmed,Armed,No-bypass,Sealed
	Alarmed,Armed,No-bypass,Unsealed
	Alarmed,Armed,Bypassed,Sealed
	Alarmed,Armed,Bypassed,Unsealed

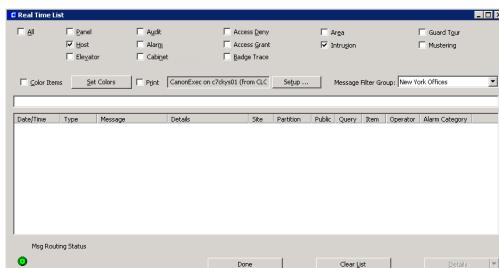
Zone Icons	
	Arming
	Armed
	Bypassed
	Disarming
	Disarmed
	Fault
	Unknown
	Normal
	Open
	Open and Bypassed
	Tamper
	Tamper and Open
	Tamper and Bypassed
	Tamper, Bypassed and Open
	Alarm
	Alarm and Open

**Annunciator Icons****3rd Party Intrusion Panel Icons**

- Close the window.

Viewing Intrusion Transactions Using the Real Time List

All intrusion detection transactions are sent through real time messages to the Real Time List. As the status of defined areas, zones, and annunciators changes, corresponding related messages are generated and displayed. You must select the **Intrusion** check box in the Real Time List window to display all intrusion transactions as they occur. Refer to “Using the Real Time List” on page 213 for more information.



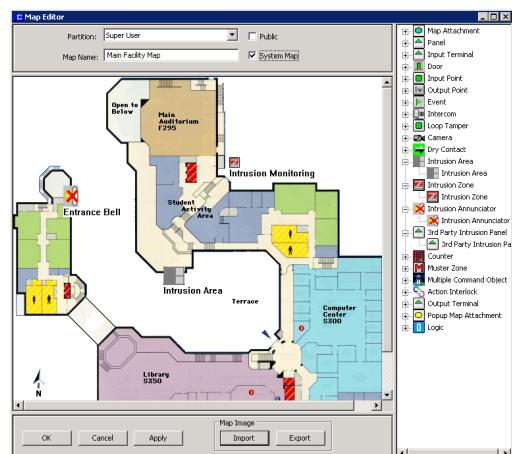
Monitoring Intrusion Using the Real Time Map

The Real Time Map displays the status of intrusion areas, zones, annunciators, and devices on a map layout of your facility. Upon intrusion activity, the map will show the state change and the exact location of the activity.

Refer to “Using the Real Time Map” on page 218.

When a status changes, the associated intrusion icon starts flashing. You can right-click the icon to open a shortcut menu and choose to, for example, arm or disarm an intrusion area or bypass an intrusion zone. If the intrusion icon was configured to allow the operator to activate events, the event name will also display in the shortcut menu.

To add intrusion icons to the Real Time Map, follow the instructions provided in “To Place Device Icons on a Real Time Map.” on page 221, and rather than defining input points, select from the drop-down list the Intrusion item you wish to display in the Real Time Map.



Map Maker provides a default intrusion image set to display various intrusion states such as “Intrusion Area Armed,” “Intrusion Zone Bypassed,” “Intrusion Announcer Active,” and so on. However, you can use your own icons to create custom image sets. Refer to “Adding Image Sets” on page 223 for details.

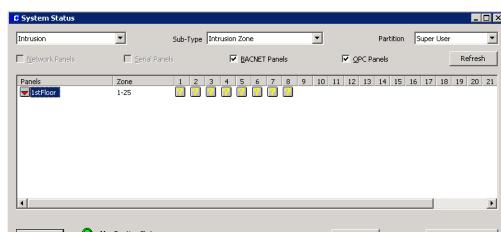
Viewing Intrusion Status Using the System Status Display

The System Status window displays the current status of intrusion areas, annunciators, and zones that have been configured to monitor intrusion detection, see “System Status” on page 318 for detailed instructions. You can display status of:

Intrusion Areas – All intrusion areas associated to the panel are displayed by number in the same row as their panel. The system will display the armed/disarmed/mixed status of each intrusion area.

Intrusion Annunciators – All intrusion annunciator devices associated to the panel are displayed by number in the same row as their panel. The system will display the active/silent status of each intrusion annunciator.

Intrusion Zones – All intrusion zones associated to the panel are displayed by number in the same row as their panel. The system will display the armed/disarmed/bypassed status of each intrusion zone.



Central Station Support

In addition to the standard P2000 message handling, the intrusion system can communicate with a Central Station using a protocol defined by SIA (Security Industry Association). The SIA link support is bi-directional, since the P2000 system acts as a central station when receiving alarms from other intrusion systems.

The latest communications protocol documents can be viewed at: www.siaonline.org as “SIA Format Dialer Protocol Standard – SIA DC-03 (R2003.10).”

Intrusion Events

The intrusion detection system hardware connected to the P2000 system can trigger events and respond to event actions using the P2000 Event application. For specific instructions refer to “Creating Events” on page 206. Typical intrusion commands to be included and linked to specific actions are as follows:

- An armed intrusion zone (trigger) forces the door override to be cancelled (action).
- An access grant command (trigger) disables intrusion for a fixed time (action).
- An access denied message generated by the panel (trigger) bypasses or arms an intrusion zone or area (action).
- A particular badge identifier that is granted access (trigger) silences an intrusion annunciator (action).

For a complete list of event triggers and actions associated with intrusion zones, areas, and annunciators, refer to *Appendix A: Event Triggers/Actions*.

OPC Aritech Intrusion Interface

The P2000 intrusion detection system has been designed to operate with OPC Aritech panels. Once the OPC Aritech intrusion panels and associated items have been configured using the instructions provided with the Aritech panel, they must be enabled in the Data Message Configuration application to populate the associated data into the P2000 database.

For detailed instructions, refer to the “Set Up Message Data Configuration” on page 110.

Creating Events

Events are system actions that you can program to occur automatically. Events can be triggered by the system or card activated. An event comprises a trigger and an action. For example, you can program an event that increments a counter (the action) when an entity badges at a specific reader (the trigger).

Using Event Configuration Dialog Boxes

Event configuration dialog boxes change appearance, depending on the category selected; some category selections present more fields on a dialog box than others. The following sections present general instructions and examples for creating triggers and actions; however, not every dialog box and field is illustrated. For a complete list of all available categories and associated types and conditions, see *Appendix A: Event Triggers/Actions*.



APPLICATION NOTE

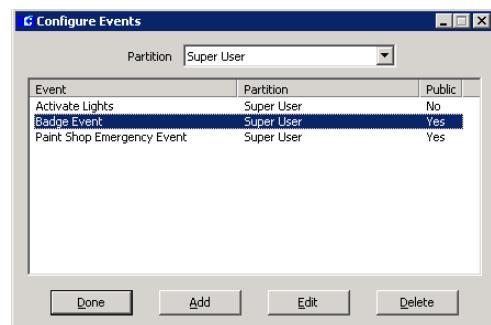
System Events vs. Panel Card Events: System and card-activated events, as created via the P2000 Main menu Events feature, create system-wide events initiated from the Server. These events can be triggered from a number of sources including badges, panels, terminals, inputs, outputs, operators, and so on. Panel card events are created via the System Configuration window for a specific panel and operate independently from the system. If the system network goes down for any reason, the panel card events will continue to operate, even while the panel is offline. For more information on Panel Card Events, see “Create Panel Card Events” on page 83.

Creating Triggers

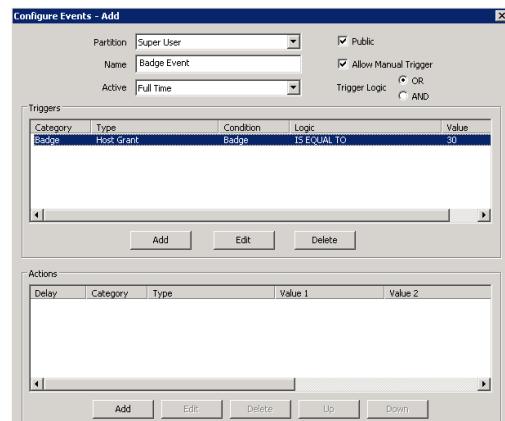
Triggers determine what conditions must be met to initiate a specific action. The type, condition, logic, and value that can be assigned to the trigger are specific to the category selected. For example, when you select “Badge” as the category, specific event action types are available; when you select “Panel” as the category, a different set of event action types are available.

To Create Trigger Conditions:

- From the P2000 Main menu, select **Events>Configure Events**. The Configure Events list displays. All events currently configured for the system will be listed.



- Click **Add**. The Configure Events – Add dialog box opens.

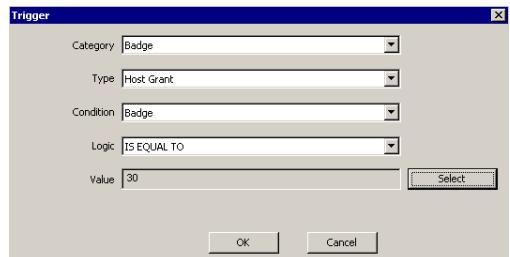


3. If this is a partitioned system, select the **Partition** in which this event will be active and select **Public** if you wish this event to be visible to all partitions.
4. Enter a descriptive **Name** for the event. When the event is configured, this name will display in the Configure Events list, so make it meaningful to those who must work with it.
5. In the **Active** field, select from the drop-down list the **Time Zone** in which this event will be active.
6. Select **Allow Manual Trigger** if an operator will manually initiate this trigger. Refer to “Creating Manual Triggers” on page 212 for detailed information.
7. In the **Trigger Logic** field, select either **AND** or **OR**. If more than one group of conditions have been created for this trigger and you wish all groups of conditions to be met to activate the trigger, select **AND**. If you wish any of the groups of conditions to trigger the action, select **OR**.

TIP: *Event triggers with multiple **OR** conditions can be made more efficient by defining the most specific and most likely triggers first (i.e., listed first in the trigger list). For example, Access Grant triggers should be defined before Counter triggers because Counters change less frequently than the system grants access. Triggers that check if certain items are members of groups (such as the granting terminal being in a specific access group) are very costly to process and should be last on the list, and therefore checked only when all other conditions are exhausted.*

Note: *It is possible to define a trigger (or set of triggers) that would always be true. When using a steady-state trigger, be sure to use the **AND** logic with another trigger that is not a steady-state trigger. Steady-state triggers are the status triggers for panels, terminals, input points, and output points.*

8. In the **Triggers** box, click **Add**. The Trigger dialog box opens.



9. Enter the information in each field as described in the Trigger Field Definitions.
10. When all information is completed, click **OK** to save the trigger conditions and return to the Configure Events dialog box. The new conditions will be listed in the Triggers list.

Note: *Event triggers that use steady-state conditions, which can be modified by other event actions such as Output Status and Host Counters, may not be triggered reliably when **AND** is used with other conditions. For example, creating 2 triggers that will activate when a badge is presented at a door **AND** a counter is set at a certain value, may fail if one of the actions changes the value of the counter.*

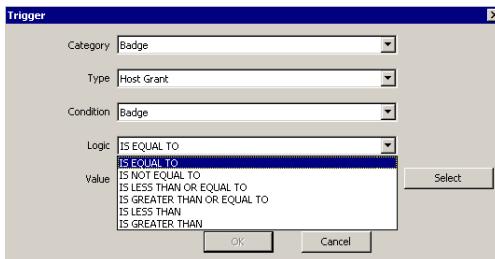
Trigger Field Definitions

Category – Select a category from the drop-down list.

Type – Select a type from the drop-down list. The types available for selection will be limited to those appropriate to the category selected.

Condition – Select a condition from the drop-down list. The conditions available will be limited to those appropriate for the category and type selected.

Logic – Select the logic that applies to the condition from the drop-down list. The choices are: is equal to, is not equal to, is less than or equal to, is greater than or equal to, is less than, and is greater than.



Value – Click the **Select** button to select a value that applies from the Select list. For example, if the category is “Badge” you could select “is less than or equal to” and select a badge number from the list to create the condition all badges less than or equal to a specific badge number.

In the previous example, we have created a trigger using the “Badge” category, with a type *Host Grant* that will trigger an event action if the value (in this case, the badge number) is equal to 32.

To Edit a Trigger Condition:

- From the Configure Events list, select an event and click **Edit**. The Configure Events dialog box opens, displaying the current settings for that event.
- In the Triggers box, select the trigger you wish to change and click **Edit**. The Trigger dialog box opens.
- Change the selections as appropriate and click **OK** to return to the Configure Events dialog box. The Triggers list will reflect the changes.

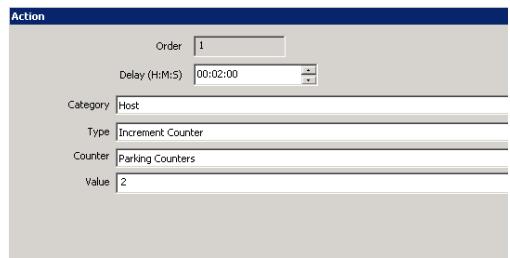
Creating Actions

An Action, as defined in the Actions list at the bottom of the Configure Events dialog box, is performed by the system when the related trigger occurs. You can program a wide variety of event actions using the Category and Type fields provided in the Action dialog box. As with Triggers, the Action types available depend on the Category type selected.

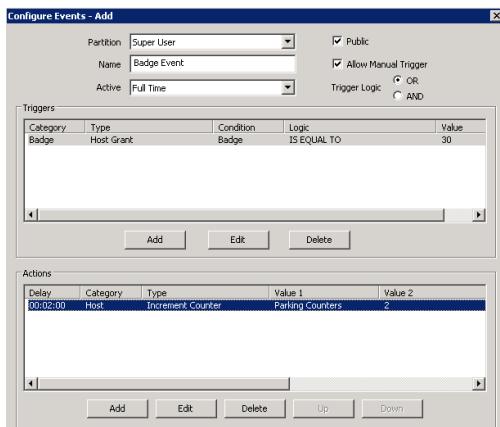
An event can trigger more than one action. You can create a number of actions and specify in what order the actions will occur.

To Create an Action:

- In the Configure Events dialog box, go the Actions box at the bottom of the dialog box and click **Add**. The Action dialog box opens.



- Enter the information according to Event Actions Field Definitions.
- When all conditions are defined, click **OK** to return to the Configure Events dialog box. The new Action will display in the Actions list.



4. Continue to add actions as required.

To Change Event Action Order of Occurrence:

1. From the Actions box at the bottom of the Configure Events dialog box, select an action line.
2. Click the **Up** or **Down** buttons at the bottom of the dialog box to move the line item as desired. The action displayed at the top of the list will occur first.

Event Actions Field Definitions

The available fields to define any Action are dependent on which category is selected. Because there are so many combinations of categories, types, and related selections, the following list of field definitions contains only a sampling of available fields. For a complete list of categories and related selections, see *Appendix A: Event Triggers/Actions*.

Order – If more than one action has been defined for this trigger, the order of the action will display in this field. For example, if the action selected is first in the Action list, this field will display “1.”

Delay (H:M:S) – Select hour, minutes, and/or seconds from the spin box to enter a delay time after which the action will occur. This is useful with an anti-passback action, for example.

Note: *Delayed event actions should not contain macros. The information needed for the macros is not available when the action is delayed.*

Category – Select a category from the drop-down list. The category selected will determine what Action types will be available.

Type – Select a type from the drop-down list. The type selected may add, remove, or change any additional fields available for definition. For example, when *Increment Counter* is selected as the Type for the Host Category, additional fields display to select counter name and specific value.

If *Display Message* is selected as the Type for the Host Category, additional fields are added from which to select the Instruction Text to be used and the workstation on which to display the message.

OPC Server Event Actions

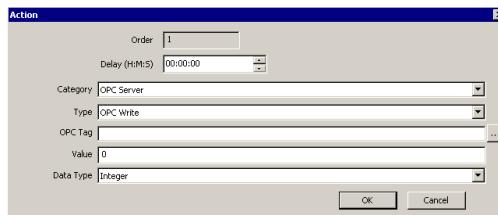
CAUTION *Do not configure OPC Server Event actions before reading and understanding OPC Server. If OPC Server Event actions are not configured correctly, the equipment may not work properly!*

The following applies to OPC (OLE for Process Control) Server events:

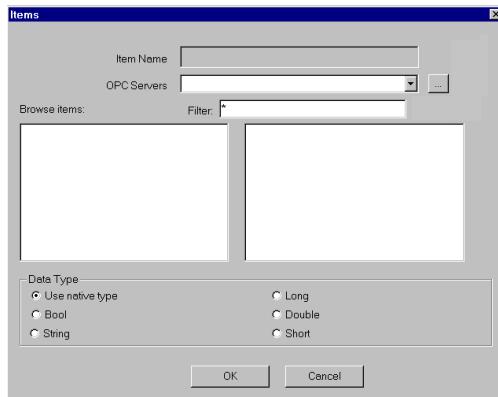
- If the PC on which the selected Server resides is switched OFF, then the event would have no effect.
- However, if the PC is ON and the OPC Server has been switched OFF, then the event would only be actioned if the appropriate launch and access rights are granted.

- Similarly, if the PC and the OPC Server are running, then the event would only be actioned if it has the correct access rights (that is, the sending user and password must be correctly set up at the receiving PC together with the correct DCOM rights). Note that the set up is correct when the software is installed. For more information see *Appendix F: DCOM Configuration*.

To select an OPC Server and view the available tags, a tag browser is provided in the event Action dialog box. Note that to select an OPC Server, the OPC Server must be running and you must have the appropriate rights.

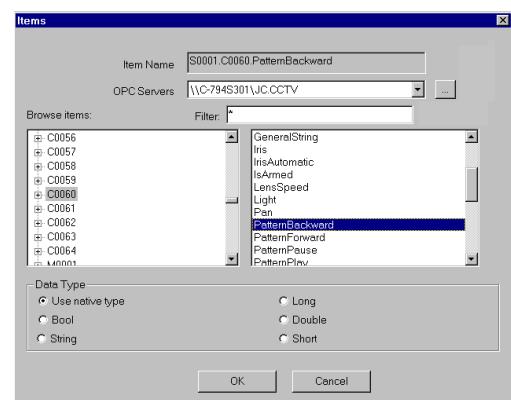


- In the Action dialog box, click the **Category** drop-down list and select OPC Server.
- From the **Type** drop-down list select OPCWrite.
- To select an **OPC Tag** from those available for the selected OPC Server, click the [...] button. The Items dialog box opens.



- Click the [...] button to locate the OPC Server, or select the Server from the **OPC Servers** drop-down list.
- Select the **Data Type** (the default option is *Use native type*, which displays all tags).
- In the Browse Items box, select the item and the tag for the event action.

The selected item will display in the **Item Name** field.



- Click **OK** to enter the Item Name into the OPC Tag field in the Action dialog box. The PC name and Prog ID are prefixed to the item name.

Note: *The Tag Browser can access the OPC Server only if the log on operator has the appropriate rights to the OPC Server (see Appendix F: DCOM Configuration).*

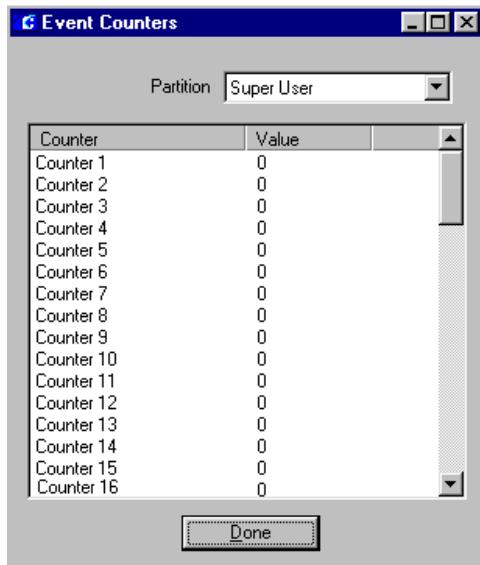
- Enter the **Value** that is to apply to the OPC Tag.
- Select the appropriate **Data Type** from the drop-down list for the event action value.
- Click **OK** to return to the Configure Events dialog box. The new event action will display in the Actions list.

Counting Events

You can create an unlimited number of counters for event programming, which will increment or decrement each time a trigger occurs, depending on the category and type selected for the event. For example, you can create a badge swipe trigger for a specific badge and then create an action that will increment Counter 1 each time the Server grants access to that badge. Then you can view the event counters list to monitor the action. Event counters accumulate value until they are reset.

To View Event Counters:

- From the P2000 Main menu, select **Events>Event Counters**. The Event Counters list displays.



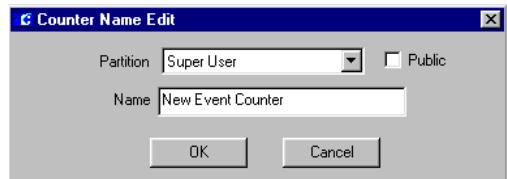
Event counters are listed under the Counter column. The Value column lists the accumulated number of events attached to each counter. You can add as many counters as you wish, or change the event counter name to give the counter a meaningful

name, refer to the following section for detailed information.

- Click **Done** to close the Event Counters dialog box.

To Add Event Counters:

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the **Counters** root icon and click the **Add** button. The Counter Name Edit dialog box opens.



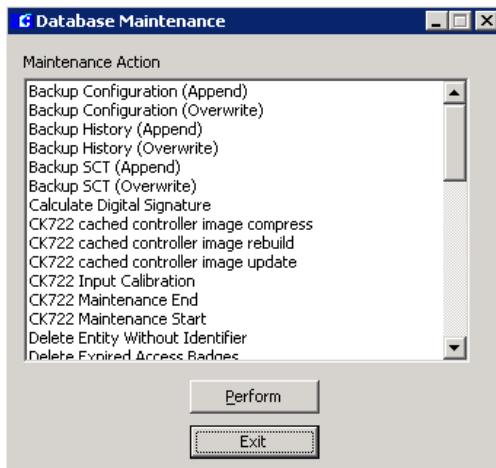
- If this is a partitioned system, select a **Partition** where the counter will apply and select **Public** if you wish this counter to be visible to all partitions.
- Enter a descriptive **Name** for the counter.
- Click **OK**. The new counter displays beneath the main Counters icon.

To Edit Event Counters:

- In the System Configuration window, click the plus (+) sign next to the root **Counters** icon to display all configured counters.
- Select the counter you wish to edit and click the **Edit** button. The Counter Name Edit dialog box opens.
- Enter the new information.
- Click **OK** to save your changes and return to the System Configuration window.

To Reset Event Counters:

- From the P2000 Main menu, select **System>Database Maintenance**. Enter your password if prompted. The Database Maintenance dialog box opens.



- Under Maintenance Action, select **Reset Counters to Zero**.
- Click **Perform**. Since this action cannot be undone, a verification message displays to confirm your action.
- Click **Yes** to reset counters to zero. The Reset Counters dialog box opens.



- Click **Reset to Zero**. All values in the Event Counters list will be reset to zero.
- Click **Done** to return to the Database Maintenance dialog box.
- Click **Exit**.

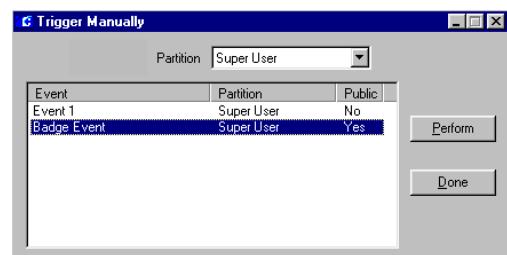
Creating Manual Triggers

Triggers can be programmed to be activated manually by an operator. In this case, the Configure Events window is set to “Allow Manual Trigger” and linked to an action. The event is then initiated by the operator from the **Events>Trigger Manually** menu, rather than by trigger conditions set up in the Configure Events window.

Note: *Events can also be manually initiated by an operator from the Alarm Monitor window (see page 167), as long as the item that generated the alarm was configured to activate events; or can also be manually initiated from the Real Time Map (see page 220), regardless if the “Allow Manual Trigger” option was enabled in the Configure Events dialog box.*

To Manually Trigger an Event:

- From the P2000 Main menu, select **Events>Trigger Manually**. The Trigger Manually dialog box opens.



- All the events that have the “Allow Manual Trigger” option selected in the Configure Events window will display in the list.
- Select an event from the list, and click **Perform**. The trigger will be activated.
- Click **Done** to close the window.

Monitoring the System in Real Time

The Real Time List and Real Time Map are dynamic displays of system transactions and operations. The Real Time List is a time-stamped display of all (or specified) local or remote transactions as they occur. The Real Time Map displays the current status of local terminals, inputs, outputs, and other defined elements on a map layout of your site. The Real Time List and Real Time Maps are typically used by operators and system administrators not only to view current status, but as troubleshooting tools.

Using the Real Time List

The Real Time List is a time-stamped display of all system transactions as they occur. If desired, an operator can monitor only specific transaction types. For example, an operator concerned with learning when an entity is denied access can select only Access Deny to filter the information displayed. The Real Time List will then display only who, what, when, where, and why the access was denied.

You can open multiple windows of the Real Time List. For example, you could have one window open with all the types enabled. You could open a second window with only the Badge Trace option selected that would display only those transactions.

Note: A description of each transaction type is presented in the Printing tab of Site Parameters on page 31. The Printing function of Site Parameters operates independently from the Real Time List function.

A system administrator may want to look at the Real Time List as a “health check”; for

example, to ensure all transaction types are being processed, or trace why a specific entity is being denied access.

Monitoring Remote Messages in Real Time

As with remote alarm monitoring (page 162), you can monitor transactions from multiple facilities at multiple geographical locations. Although each remote site administrator has total control over their access control hardware and system information related to their site, operators can control system and event information from different sites. This means that remote operators might for example, monitor their transactions locally during normal working hours, while your local operators might monitor transactions messages generated at their remote sites after hours, as long as both the local and remote P2000 sites are set up and configured to receive and send transaction messages across P2000 sites during such periods.

With the proper configuration, an unlimited number of sites can be monitored simultaneously, allowing operators to administer multiple regions from a single site. To monitor remote messages, both your local and the remote sites have to be properly configured. The following conditions must be met:

- The **Remote Message Service** must be up and running at both the remote site (to send the transaction messages) and at your local site (to receive the transaction messages). Refer to “Starting and Stopping Service Control” on page 315.
- The **Message Filter Configuration** application (page 101), must be properly configured at your local site and each remote site, to control the type of messages transmitted between Servers, thereby reducing network traffic by transmitting only messages that pass the filter criteria.

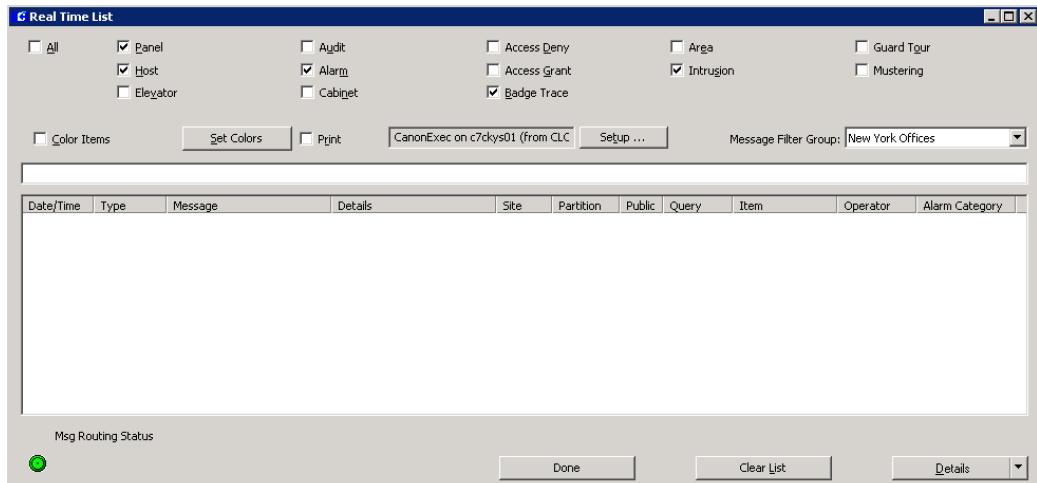
- The **P2000 Remote Server** application (page 108), must be properly configured at each remote site to send their transactions messages to your local site. The setup must include the name, IP address and Remote Message Service Listener Port number of your local site; the type of messages that will be forwarded to your site and at what times; and other related parameters.
- The **Processing Remote Message** option in the RMS tab of Site Parameters (page 38), must be selected at your local site to be able to receive messages from remote P2000 sites. If you select this option, the Remote Message Service will process incoming messages and pass them on to RTLRoute for distribution within the local system and, if applicable, to other remote sites.
- The **Message Filter Group** selected in the RMS tab of Site Parameters (page 38), defines which remote messages your Remote Message Service will process. If you select <**None**>, your local P2000 site will receive all remote messages.

Viewing Real Time List Transactions

To access the Real Time List, select **System> Real Time List**. Transaction types displayed in the list area of the Real Time List can be color coded to help operators recognize a specific type of transaction. You can use the default system colors, or customize a transaction type with a different color. You can also set up a printer to output hard copy line items that are date and time stamped.

A Message Filter Group selection is provided to allow operators to select which messages are displayed in the Real Time List. This option can be used to diagnose message filters for workstations or to determine whether the correct messages are forwarded to an external system via the Remote Message Server.

The Real Time List displays transaction messages in the order they are received. When a message is received, it displays in the row above the scrolling list and in the first line of the list. As new transactions occur, they move to the top of the list.



When you open the Real Time List for the first time in the session, the scrolling list will be empty. Depending on the transaction types selected at the top of the window, transactions will begin to display in Date/Time order at the top of the list. As transactions occur, the older ones will scroll down in the list as the newer ones are added at the top.

The following information is shown for each transaction in the list.

Date/Time – Displays the date and time of the message. Transaction messages that are originated at remote sites with different geographical time zones will display the actual time at the remote site. However, remote alarms will display the time at which they were received at your local site.

Type – Displays the transaction types that were selected for monitoring (Audit, Access Deny, Badge Trace, and so on).

Message – Displays a message related to the transaction type, for example Invalid Card for an Access Deny transaction type.

Details – Displays details related to the message, such as Badge number, Terminal and Entity name.

Site – Displays the name of the local or remote P2000 site where the message was originated.

Partition – Normally displays the name of the partition containing the item (input point, terminal, panel, etc.) associated with the message.

Public – If the item associated with the message is marked as Public, this column will normally display whether the message is visible to other partitions.

Query – Displays the query string value (if it was defined) of the item associated with the message.

Item – Displays the name of the item (panel, terminal, input point, etc.) that is associated with the message.

Operator – Displays the name of the operator who handled the message (alarms in non pending state or audit messages only).

Alarm Category – Displays the Alarm Category to which the associated alarm belongs.

Note: *The Message Routing Status indicator at the bottom of the Real Time List window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.*

Note: *If your facility has purchased the DVR option and the selected transaction message displayed is associated with a camera, click the Details button located at the bottom of the window to launch the AV Player in live mode. As an alternative, you can click the associated drop-down list and select AV Player (Live) to launch AV Player in live mode or select AV Player (Stored) to launch AV Player in video retrieval mode. For more information refer to the DVR option page 282.*

To View all Options in the Real Time List:

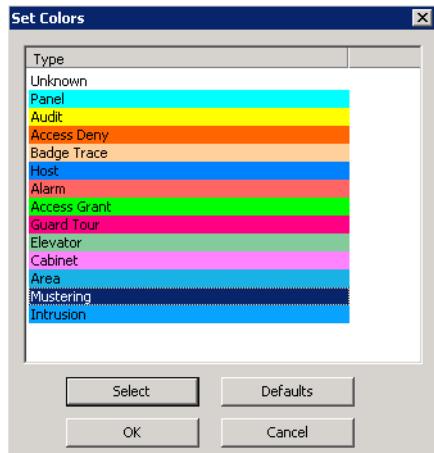
1. From the Real Time List window, select All from the options at the top of the window. All transactions will begin to accumulate in the scrolling list.

To View Specific Options in the Real Time List:

1. Clear the All option and select only those options you wish to view. Only those options will begin to accumulate in the scrolling list.

To Display Color Coded Transactions:

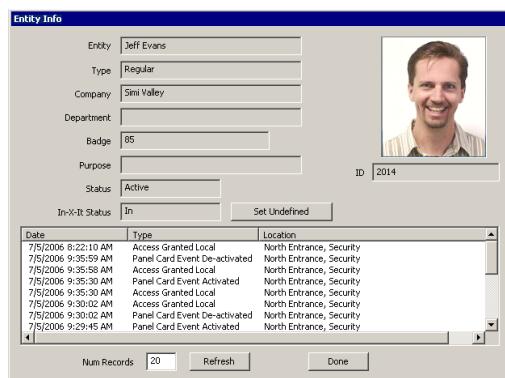
1. Select the **Color Items** box. All transactions will display in a different color, using the default system colors.
2. To display a transaction type with a different color, click the **Set Colors** button. The Set Colors dialog box opens.



3. Select a transaction type, then click the **Select** button. A Color dialog box opens.
4. Select the desired color and click **OK** to return to the Set Colors dialog box.
5. Click the **Defaults** button to reset the colors to the default system colors.
6. Click **OK** to return to the Real Time List window.

To Display Entity Details:

1. Select from the scrolling list, the transaction line item associated with an entity (Access Deny, Access Grant or Badge Trace transactions).
2. Click the **Details** drop-down arrow located at the bottom of the window, and select **Entity Info**. The Entity Info dialog box opens.



The top portion of the window shows the entity details including image, if available.

The bottom portion includes a chronological list of badge transactions associated with the entity.

3. To manually adjust the In or Out state of a badge until next badging, click the **Set Undefined** button.
4. To change the number of transactions displayed, enter the desired number in the **Num Records** field.
5. To update the list box with new data, click the **Refresh** button.
6. Click **Done** to return to the Real Time List.

Printing the Real Time List

An operator can print transactions as they occur from the workstation. Line items from the Real Time List will continue to print as long as the Real Time List window is open or minimized on the workstation. Line items will stop printing when the Real Time List window is closed.

To Print Real Time List Line Items from a Workstation:

1. In the Real Time List window, select **Print** in the top portion of the window.

Note: We recommend a dot matrix printer be used exclusively for printing line items from the Real Time List, and independently from the transactions printed from the Site Parameters window.

2. Click the **Setup** button to select a printer name and any other information for the printer to be used. (Printers must first be set up using the Windows Printer Settings dialog box. See your system administrator if you need more information, or refer to your Microsoft Windows documentation.)
3. Click **OK**. The printer name should display in the Printer field on the Real Time List window.

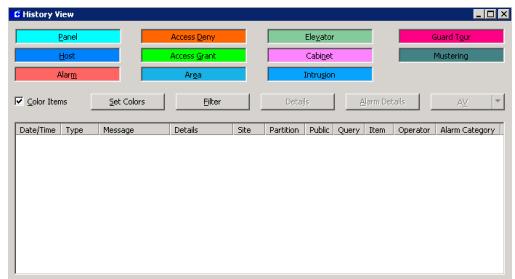
Note: Printing transactions from the Real Time List (performed from a workstation) is different from Real Time Printing (performed at the System Server). For information on Real Time Printing, see Site Parameters "Printing Tab" on page 31.

Viewing History Information

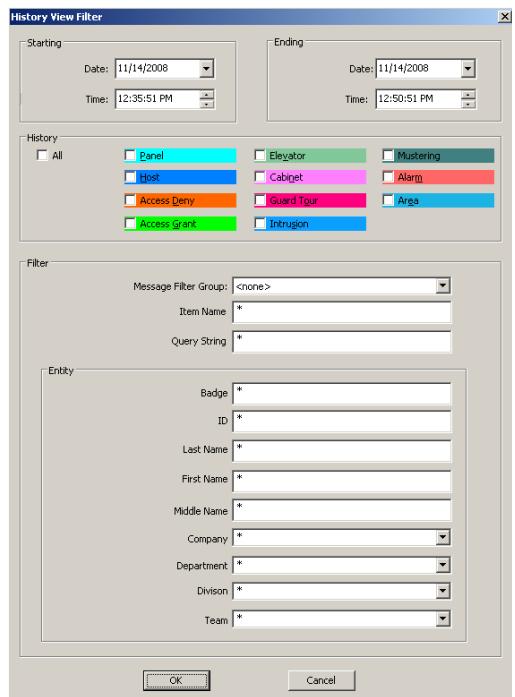
Use the History View application to review alarm and transaction history information based on the provided filter criteria. This feature is similar to the Real Time List as it displays the same type of messages and allows operators to retrieve entity and video information associated with these messages.

To Review History Information:

1. From the P2000 Main menu, select **System>History View**. The History View dialog box opens.



2. Click the **Filter** button. The History View Filter dialog box opens.



3. From the **Starting** and **Ending** boxes select the date and time during which the transactions occurred.
4. In the **History** box, select the type of transactions you wish to view.
5. In the **Filter** box, select the Message Filter Group that contains the message types to view, the Item Name, and if applicable the Query String.

6. If you wish to view transactions associated with a specific entity, use the **Entity** box to enter the necessary information.
7. Click **OK**. The History View window will display the transactions that meet the filter criteria.
8. To view entity information, select the transaction line associate with the entity, then click the **Details** button.
9. To view alarm information, select the transaction line associated with the alarm, then click the **Alarm Details** button.
10. If the selected transaction message is associated with a camera, click the **AV** button to retrieve video associated with the transaction.
11. When you finish, close the History View dialog box.

Using the Real Time Map

The Real Time Map displays the current status of terminals, inputs, outputs, and other defined elements on a map layout of your facility and can be used similarly to the System Status window. Maps are created using the Map Maker feature to “drag-and- drop” dynamic terminal icons to their actual locations on imported layout images. All you need are simple layout maps that can be either scanned or drawn in any draw application, then saved in an importable format.

Once the maps are created, they are accessed from the P2000 System menu. If a terminal goes down or an alarm sets, the Real Time Map shows you the state change and exactly where the device is located.

The operator must have the appropriate rights defined in User roles to access Real Time Maps. See “User Role Management” on page 21.

Sub Maps and Attachments

You can create facility-level maps and attach sub maps that detail specific areas in the facility. Sub maps may also contain sub maps to add further detail; you can create as many levels as you need. Use the **Prev** button to return to the previous map, or use the **Home** button to return to the main facility-level map. Clicking the **Up level** button will take you to the previous facility-level map.

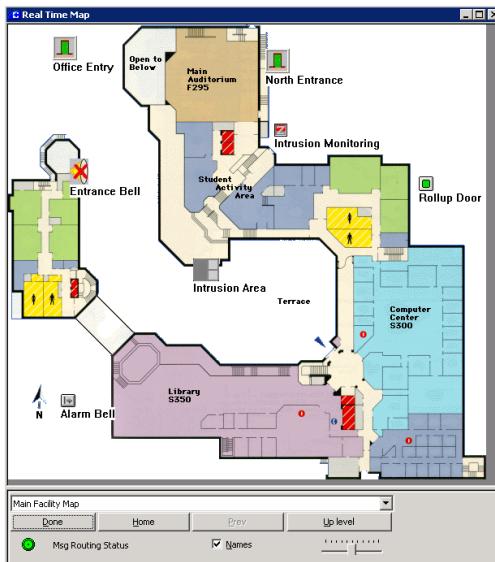
If an alarm sets in an area detailed in a sub map, the sub map icon will blink, indicating the location of the alarm. You can double-click the blinking sub map icon to jump to the associated detail map. (See “Adding Map Attachments” on page 222 for more information about creating multi-level maps.)

Map Maker provides image sets to display various device states such as “panel up,” “panel down,” “input set,” and so on. However, you can create your own icons and include them in image sets in Map Maker.

Note: *The Message Routing Status indicator at the bottom of the Real Time Map window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.*

To View the Real Time Map:

1. From the P2000 Main menu, select **System>Real Time Map**. The Real Time Map window opens.



- The current status of Panels, I/O Terminals, Readers, Input and Output points, and other defined elements will display as designed in Map Maker. The Main Map will display as assigned on Map Maker; however, you can select any map created in the system.

Note: If your facility has purchased the DVR option, when you right-click a map icon that is associated with a camera, a popup menu will display the "AV Player (Live)" option. If there are stored videos (associated with alarms), the popup menu will display the "Show Alarm Video" and "Start Recording" options. For more information refer to the DVR option on page 282.

- Clear the **Names** box if you wish to view the icons only; select it to display names.

TIP: You may want to view icons only on a large facility map, and display names on maps of specific areas.

- From the drop-down list at the bottom of the window, select the name of the map you wish to view. You can leave the window open to monitor system elements in Real Time.
- Use the slider control to enlarge or reduce the view of the active map. The zooming of the map can also be controlled with the mouse wheel.
- Click **Done** to exit the window.

Opening a Door

You can open a door from a Real Time Map. The door will remain open for the time configured in the door terminal's access settings, and then close. When a door is opened in this manner, the map icon image for the terminal changes from a closed door to an opened door, as long as the door is opened, then reverts back to a closed door image when the door closes. Use the instructions in "To Place Device Icons on a Real Time Map:" on page 221 to insert a door icon.

To Open a Door from a Real Time Map:

- Locate the door terminal icon for the door you wish to open.
- Right-click the icon and select **Open Door** from the shortcut menu. The door opens for the configured time period, then closes.

Note: If you need to open the door for a period other than that configured, you must do so from the Door Control function.

Activating Events from the Real Time Map

Events can be manually activated by an operator from the Real Time Map, rather than by the trigger conditions set up in the Configure Events dialog box. Icons on the Real Time Map, such as Panels, Terminals or Input Points, can be configured to initiate events; or you can just place Event icons on the Map.

To Activate an Event from a Real Time Map:

1. In the Real Time Map, locate the icon that contains the event you wish to activate.
2. Right-click the icon and select the Event name from the shortcut menu. The event will be triggered.

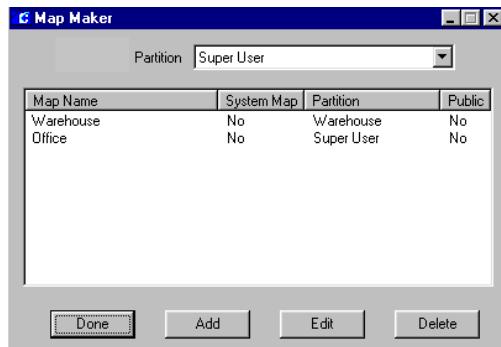
Creating a Real Time Map

It is easy to create a Real Time Map using Map Maker's drag-and-drop feature. It is basically a four-step process:

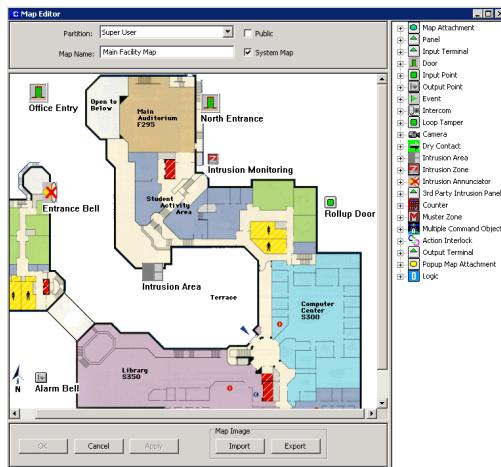
- Set up the Map Maker window
- Create an importable image
- Import the image to Map Maker
- Drag-and-drop map icons onto the map

To Set up the Map Maker Window:

1. From the P2000 Main menu, select **Config>Map Maker**. The Map Maker dialog box opens.



2. Click **Add**. The Map Editor window opens.



3. If this is a partitioned system, select the **Partition** in which the map will be active and select **Public** if you wish the map to be visible in all partitions.
4. Enter a descriptive **Map Name**, such as Warehouse or Office.
5. Select **System Map** if this is the map you want displayed on opening the Real Time Map from the System menu. Otherwise, the map will be stored in the system and displayed when selected from the Real Time Map drop-down list.

To Create an Importable Image:

Map Maker can import most popular image formats: *.bmp*, *.tif*, *.wmf*, *.jpg*, *.pcx*, and *.eps*, to name a few. (To see all available formats, see the Files of type drop-down list on the Import dialog box.)

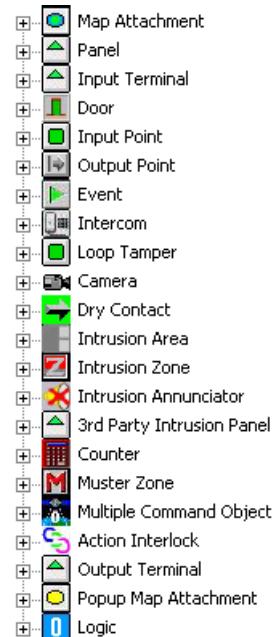
1. **If floor plans or maps exist in a compatible electronic format**, you can import them directly.
2. **If floor plans or maps exist in hard copy**, have them scanned and saved in a compatible format.
3. **If floor plans or maps do not exist**, you can create them using a draw program such as Windows Paint™, Corel Draw™, or other drawing utility, then save or export the image in a compatible format.
4. Copy the image file to a directory that is accessible to the P2000 system.

To Import an Image to Map Maker:

1. From the P2000 Main menu, select **Config>Map Maker**. The Map Maker dialog box opens.
2. Click **Add**. The Map Editor window opens. When you import an image into the Map Maker editor, it displays in the background of the large image area. You can use the mouse pointer to pull the corners and sides of the window to increase the size as necessary, or click the maximize/minimize button in the top right of the window.
3. In the Map Image box at the bottom of the window, click **Import** and navigate to the directory in which your layout image is stored.
4. Select an image to import.
5. Click **Open**. The image displays in the background of the image area of the Map Editor window.

To Place Device Icons on a Real Time Map:

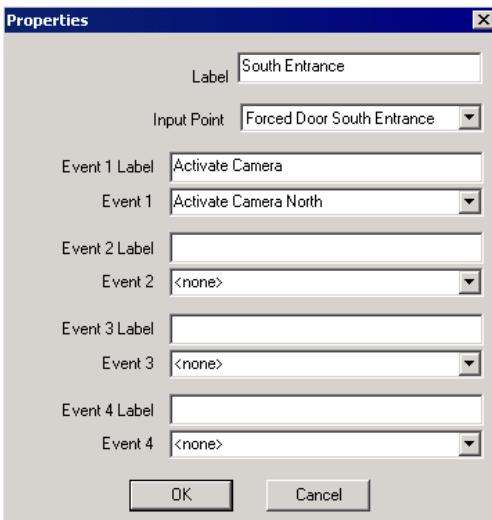
When you open Map Maker, map icons representing Panels, Terminals, Inputs, Outputs, and other system elements are listed on the right windowpane.



Note: If your facility has purchased options such as Intercom or DVR, the associated map icons will display in the list. Refer to the respective section in Chapter 4: System Options, for more information.

1. Click the element you wish to add. To select an input point, for example, click the plus (+) sign next to the Input Point icon. An Input icon is added under it.
2. Use the left mouse button to drag the new icon to the desired position on the map. For example, an input point could be dragged near the door representing where the input point is actually installed. When

you release the mouse button, a Properties dialog box opens.



- In the **Label** field, enter a descriptive name that can easily identify the icon in the Real Time Map. This name will display next to the icon on your layout.
- Select from the drop-down list the **Input Point** name that represents the location on the map. All available input points (or all input points in the partition selected) will display in the drop-down list. If you are placing a panel, the drop-down list will include all panels (or all panels in the partition).
- To assign events to the input point, enter a descriptive event name and select a previously configured event from the associated drop-down list. You can define up to four events for each map icon.
- Click **OK** to close the Properties dialog box. The icon will be inserted in the map.
- Do this for each device or event you wish to add to the map.
- When all elements have been added, click **OK** to close the Map Editor window. The

map will now be available to choose from the Real Time Map drop-down list.

- Click **Done** to close the Map Maker dialog box.

TIP: *The top left corner of the icon will be anchored exactly where the tip of the mouse pointer is released.*

Adding Map Attachments

You can add map attachments to Real Time Maps that, when right-clicked, can open another map. For example, you can place a map attachment on the “Office” map that will open the “Warehouse” map. Or you can place several area map attachments on the System Map.

To Add a Map Attachment:

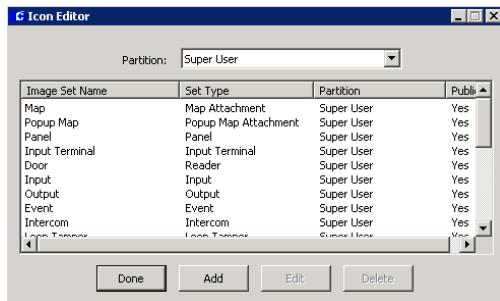
- From the P2000 Main menu, select **Config>Map Maker**. The Map Maker list box opens.
- Select the map to which you wish to add a map attachment.
- Click **Edit**. The Map Editor window opens with the selected map in the image area.
- Drag a **Map Attachment** icon to the image area. When you release the mouse button, select from the drop-down list the map you wish to attach.
- Click **OK**. Now when you open the map in Real Time Map, you can right-click the Attachment icon and select **Open** to open the attached map.

Adding Image Sets

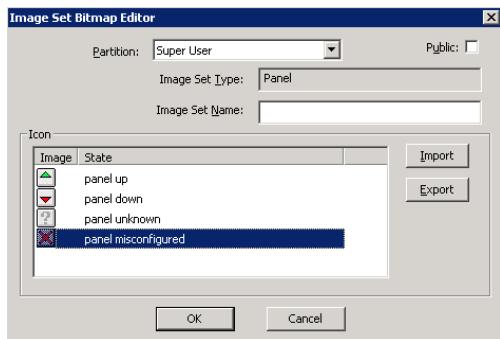
Map Maker provides image sets to display various device states such as “panel up,” “panel down,” “input set,” and so on. However, you can use your own icons to create custom image sets.

To Create a Custom Image Set for Map Maker:

- From the P2000 Main menu, select **Config>Icon Editor**. The Icon Editor dialog box lists the default image set names.



- Click **Add**. The Image Set Bitmap Editor opens.



- Select the **Image Set Type** you wish to create. The default image for each state displays in the Icon list.
- Type in an **Image Set Name** for the new image set.

- From the Icon list, select the image you wish to replace and click **Import**.
- Navigate to the directory where your new images are stored, select the image and click **Open**. The default icon in your new image set is replaced with the new icon.
- Continue to import and replace images until all the items have been replaced as desired.
- Click **OK**. Your new image set displays in the Icon Editor list, and will now be accessible from the right windowpane in the Map Editor window.

Chapter 4: System Options

A number of options are available for use with your *P2000 Security System*. These options are bundled separately from the P2000 software, and some of them are shipped with their own manuals. Since various elements within the P2000 software must be set up and configured to interface with the options, this chapter presents the information you need to set up and configure each of the following options:

- **Partitions** – Divide your P2000 system databases into sections that can be managed individually.
- **Video Imaging** – Improve your security by creating badge identifiers to provide a visual identification of every entity.
- **MIS Interface** – Add, update, delete, or query the P2000 Entity database from an external database system.
- **Metasys Integration (BACnet)** – Allow P2000 security tasks to be handled by Metasys Workstations.
- **Metasys System Extended Architecture** – Allow a number of P2000 security tasks to be handled via Metasys system extended architecture user interface.
- **Guard Tour** – Define a sequence of transactions that must occur at specific intervals to ensure your facility is properly monitored by security personnel.
- **CCTV** – Control CCTV installations via the P2000 CCTV option.
- **DVR** – Provide controls to search, retrieve, and download real time or archived audio and video recording from surveillance cameras.

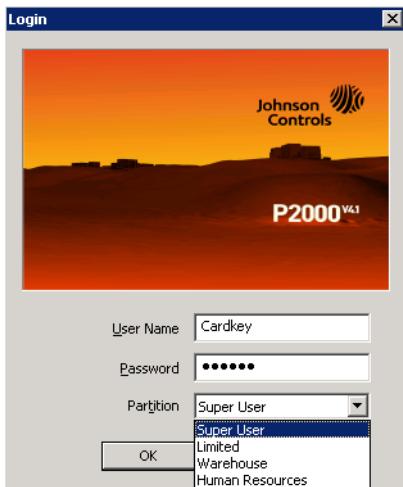
- **Redundancy** – Run the P2000 software in a “recovery configuration” to ensure uninterrupted operations.
- **FDA** – Define parameters to assure FDA Title 21, Code of Federal Regulation (CFR) Part 11 compliance.
- **Intercom** – Define and control intercom calls from P2000 Workstations.
- **P2000 Enterprise** – Allow multiple P2000 sites to communicate with each other to share Entity/Identifier data.
- **Web Access** – Perform various P2000 tasks from any web-ready PC or compatible PDA device.

Partitions

You can divide the P2000 database into smaller sections that can be individually managed. Partitions structure what data is accessible by an individual user, or by a group of users. You can create as many partitions as you need, depending on your system requirements. For example, if you manage a building with several tenants, you could use partitions to segregate the databases and system functions, so that Tenant A cannot see, access, or change Tenant B's records.

Partition fields and Public boxes will display on windows and dialog boxes only if your system specification includes the Partition option.

When users are assigned to a particular partition, they select the partition to which they have been assigned from the Login dialog box.



The first partition assigned to the logged on user automatically displays in the Partition field. For multiple partition users, click on the button to the right of the Partition field to display all partitions assigned to the user. The partition selected will be the active partition for the user.

When a Partition field displays on a window, the items displayed in the window are only for the partition selected from the drop-down list.

After partitions are set up, they are available for assignment to all major system components, such as Entities, System Devices, Access Groups, and Terminal Groups. For detailed information about using Partitions with these components, see the component sections in *Chapter 2: Configuring the System*.

Partition Types

Users are assigned to single or multiple partitions and have unique access restrictions. Examples of access restrictions include the ability to add, modify, or view database information within their assigned partitions. Access restrictions for individual users are defined in the User Role Management window. When a

user initially logs on to the P2000 system, the partition chosen during login is the active partition for the user. After logging on, a user has the option to access other partitions, assuming they have been given access to other partitions using the Entity Management window. Refer to "Adding Users to the System" on page 21.

Any database items created by a user in a partition are owned by that partition. That is, the information resides in that partition and it could be accessible for use by other partition users if the database item has the Public check box enabled or the users have been assigned to the same partition. Users that belong to the Super User partition may access all database items.

There are two types of database partitions: Regular and Super User.

Regular Partitions

Regular partition users may belong to multiple partitions or just a single partition. Access restrictions include the ability to add, modify, or delete items that belong only to their assigned partitions. Items that have been marked as "Public" in other than their assigned partitions can be selected for viewing, however the information is not accessible for modification.

The Super User Partition

The Super User partition is the main partition in the database. Only one Super User partition can be defined. Users that belong to the Super User partition have access to all other partitions; are responsible for assigning partitions to database users; and have the ability to add, modify, and delete any items in the database. Super User members are also responsible for performing system maintenance and system configuration functions.

The Super User member can access all system data regardless of partition ownership. Regular

partition users cannot change parameters defined in the Super User partition.

Note: If you disable the **Public** flag for an item (such as a terminal), all records that contain that item (such as an access group), must be edited to manually remove the items that have changed to non-public.

Creating Partitions

Create partitions to divide the P2000 database into smaller sections. The newly created partitions will be added under the root partition icon, and will display in drop-down list boxes throughout the system. Once partitions have been defined, users can be assigned to a specific partition, or to multiple partitions by using the User tab in the Entity Management window.

Note: If you have the optional MIS Interface in your system, you need database administrative rights to add, edit or delete partitions. (See “Setting Up User Accounts” on page 23).

To Create a New Partition:

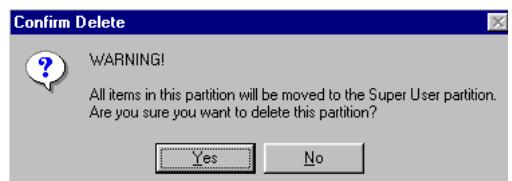
1. In the System Configuration window, click the **Partitions** root icon.
2. Click the **Add** button to access the Partition Edit dialog box.



3. Enter a **Name** for the new partition.
4. Click **OK** to save the partition name and return to the System Configuration window.

To Delete a Partition:

1. From the System Configuration window, click the plus (+) sign next to the **Partitions** icon. All the partitions currently configured in the system are listed.
2. Select the partition you wish to delete, and click **Delete**.
3. At the Confirm Delete dialog box, click **Yes**. The following warning message displays.



4. Click **Yes**. All items under this partition will be moved to the Super User partition.

Video Imaging

Video Imaging is a full-featured video imaging and badging system that is fully integrated with your *P2000 Security Management System*. Video Imaging improves your security by providing a visual identification of every entity. Through the imaging software’s graphical user interface, you can create custom badge layouts easily and quickly.

You can include a number of elements on a badge, such as company logos or other important identifying images, photographs, custom text, barcodes, and signatures. You can also add user-defined fields (UDFs) to give you the flexibility to produce sophisticated designs with a minimum of time and effort.

The P2000 system supports two Video Imaging software options: ID Server and EPI Builder. Complete software and hardware

installation and operation instructions are provided in the *P2000AE Integrated Video Imaging Installation and Operation Manual* that was shipped with your Video Imaging option.

The following sections describe basic video imaging configuration and use, including:

- **Video Imaging specifications**
- **Defining a Video Imaging workstation**
- **Printing a badge identifier**

Video Imaging Specifications

Video Imaging provides a full-featured badge design and imaging solution. The following are Video Imaging specifications:

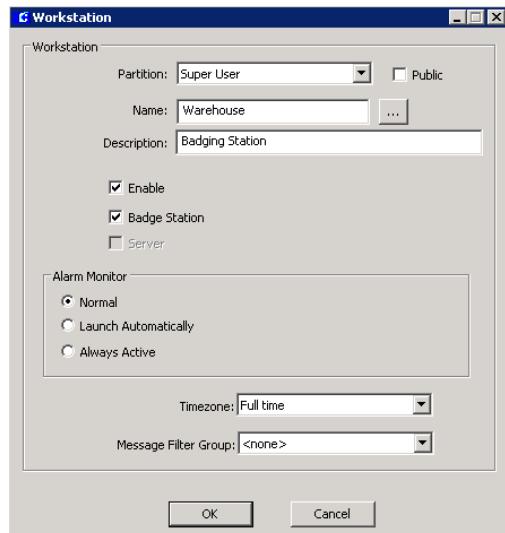
- Integration with the *P2000 Security Management System*. All entity records, images, and so forth are stored centrally at the P2000 Server.
- The P2000 workstation with Video Imaging functions as a fully-capable P2000 workstation as well as a badging workstation.
- Easy-to-use WYSIWYG (what you see is what you get) badge design.
- The number of badge designs created is limited only by available hard disk space.
- Supports digital camera and signature pad video capture options.
- Simple to capture photos and signatures.
- Magnetic stripe or G&D smart card encoding.
- Can be used with partitioned or non-partitioned P2000 systems.

Defining a Video Imaging Workstation

Like any P2000 workstation, the Video Imaging workstation must be defined at the P2000 Server before the station can properly connect to the Server.

To Configure a Workstation for Badging:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted.
2. In the System Configuration window, click the **Workstation** root icon.
3. Click the **Add** button to access the Workstation dialog box. The Workstation dialog box opens.



4. Enter the information required, see “Workstations” on page 19.
5. Select the **Badge Station** box to define this workstation as a Video Imaging station.

Note: If you edit an existing workstation and define it as a Video Imaging station, you must exit the P2000 software and restart the application for the change to take effect.

6. Click **OK** to save your entries and return to the System Configuration window.

Note: Configuring a workstation as a Badge Station only authorizes that workstation to perform badging operation. The badging software must still be correctly installed at that workstation.

Printing a Badge

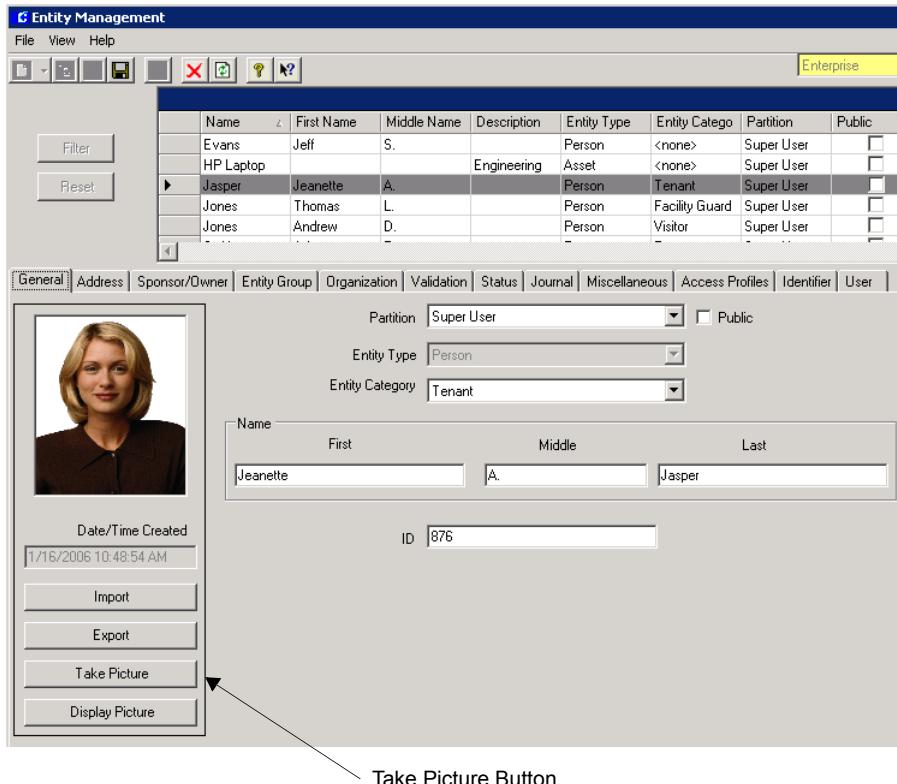
Printing a badge requires the following steps:

- **Creating an entity record.** (See “Entering Entity Information” on page 132.)
- **Assigning the badge to the entity.** (See “Identifier Tab” on page 142.)
- **Capturing the portrait and signature images.**
- **Viewing and printing the badge.**

Capturing the Portrait and Signature Images

1. From the P2000 Main menu, select **Access>Entity Management**. The Entity Management window opens.
2. Select an entity from the list and click the **Edit** icon.
3. In the General tab, click the **Take Picture** button to begin the process of capturing the portrait and signature images.

Note: The following sequence of steps assumes you are using all available capture devices for Video Imaging (camera and signature pad). Any devices not used, and therefore not configured, will automatically be skipped by the Video Imaging application.



4. The first capture window displayed will be the portrait window. If you do not see an image when the portrait capture window opens, check your camera cable connections and ensure the camera was properly configured.

For information on hardware installation, see the *P2000AE Integrated Video Imaging Installation and Operation Manual* that was shipped with your system. Elements on each capture window will display according to the type of devices you are using. Follow the respective instructions in your Video Imaging manual.

5. Capture the portrait image and make adjustments with the tools provided. Experiment with the various image controls. After you capture the portrait image, it will be automatically linked to the current entity record.
6. After capturing the portrait image, the signature capture window automatically opens (if previously configured). Use the special plastic-tipped pen, shipped with the pad, to write a signature on the pad.
7. Make the necessary adjustments and accept the signature to assign it to the current entity.

Viewing and Printing the Badge

After capturing all the images, you can now view and print your badge design. Note that since the captured images are usually large files, it takes a few seconds to save them into the database. You should always wait a few seconds after capturing images before printing a badge.

To View a Badge Before Printing:

1. In the Entity Management window, select an entity from the list and click the **Edit** icon.

2. Click the **Identifier** tab.
3. Click the plus (+) sign next to **Access Badge** or **ID Badge**. All selected badges are listed.
4. Select the badge you wish to see and click the **Preview** button at the bottom of the Entity Management window.
5. Your design will display in its own window with all the images you have captured.

To Print a Badge:

1. Before printing the badge, make sure you have loaded the ribbon and cards according to the printer's manual.
2. In the Entity Management window, select an entity from the list and click the **Edit** icon.
3. Click the **Identifier** tab.
4. Click the plus (+) sign next to **Access Badge** or **ID Badge**. All selected badges are listed.
5. Select the badge you wish to print and click the **Print** button at the bottom of the Entity Management window.

To Import an Image:

1. In the Entity Management window, select an entity from the list and click the **Edit** icon.
2. In the General tab, click the **Import** button. The system displays a browse screen.
3. Navigate to the directory where your images are stored. Double-click the image file, or select the image and click **Open**. The Image displays in the General tab.

Note: Once an image has been placed in the entity record, you cannot delete it; you must import a new image to replace it.

MIS Interface

The MIS Interface provides a means for the P2000 system to receive entity information and queries from an external source such as a Human Resource system. Using the MIS Interface Service and an external ODBC-based program, you can add, modify, or delete entities and their identifiers in the P2000 system, or you can query entity information using “wild-cards.”

The MIS Interface that resides on the P2000 Server is called P2000 MIS Interface Service, which is a Windows service designed to import and export data.

MIS Prerequisites

The following elements are external to the P2000 software. They must be in place, or the MIS Interface will be unable to receive data or respond to queries.

- Network connection to link the external system with the P2000 Server.
- MIS Interface (purchased separately from *Johnson Controls*, no separate installation media is required).
- ODBC 3.0, or later (installed in the external system).
- Microsoft SQL Server ODBC driver (already installed in the P2000 system).
- An ODBC-based software program that communicates between the external data source and MIS Input/Output tables.

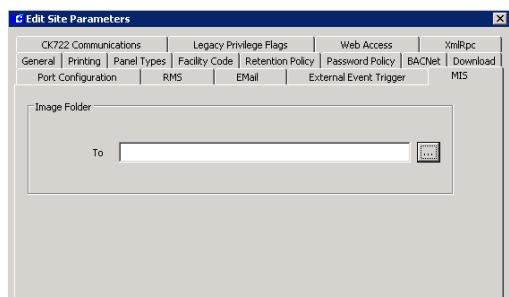
Note: *The external system can be any ODBC-capable application. This system is supplied by the user and is not included in the P2000 software.*

Once the previous components are in place, the following elements must be set up at the P2000 Server:

- The user assigned to manage the MIS Interface must have the appropriate permission level defined in **User Role Management**, see page 21.
- Since passwords cannot be changed for MIS users, the **Password Expiration** option must be set to **Never** in the User tab of the Entity Management window, see page 148.
- At least one P2000 user should be a member of the **PEGASYS Administrators group**, as defining UDF fields requires a higher level of DB privileges. This is done by setting up the Windows account of those P2000 users accordingly, see page 24.
- The **P2000 MIS Interface Service** must be running using the Service Control application, see page 315.
- The **MIS** tab in Site Parameters must be configured to select the location where exported badge images will be stored if the Export Image command will be used.

To Select a Location to Store Badge Images:

1. From the System Configuration window, select **Site Parameters** and click **Edit**. The Edit Site Parameters dialog box opens at the General tab.
2. Click the **MIS** tab.



3. Enter the name of the **Image Folder** or click the [...] button to find the folder where the badge images will be stored.
4. Click **OK** to save the settings and return to the System Configuration window.

Understanding the Input and Output Tables

The MIS Interface communicates with the external application via an ODBC connection to receive data and return query results through two database tables: an Input table and an Output table. These tables are created automatically. The Input table receives data and commands from the external system. The results of the commands issued to the P2000 system from the Input table are returned to the Output table.

When the external program writes a record into the Input table, the P2000 system reads that record and performs the requested action (Add, Delete, Update, Query, or Export Images). The results of that operation are written to the Output table and the record in the Input table is deleted. The external software should enter a unique Request ID for each record. Results are reported by Record ID and can be reviewed via the external program.

Results can be either “successful” or report an error on a specific Request ID. If multiple records are sent to the Input table, they are processed in the same manner: as a group of records is processed and clears the Input table, the next group is read and processed. (Request IDs remain intact, though records may not necessarily be processed in any particular order.) Records are removed from the Output table by the external system. All successful operations will be logged in the normal P2000 Audit database table.

Partitioned Systems

On a P2000 system that has the Partitioning option, a set of Input and Output tables will be created for each partition. The table names will be prefixed by the Partition name. These tables are in addition to the normal Input and Output tables, which will be used for the Super User partition.

Using the MIS Interface

When the Interface is run and whether it is run continuously or at prescribed intervals is up to your management procedures.

For example, you may want to start the MIS and run it to populate the P2000 entity database for the first time, entering all entity information for all personnel at one time. After that is done, you may want to only run the MIS Interface once a day or once a week.



APPLICATION NOTE

MIS Interface Application:
The MIS Interface is intended ONLY as a tool to allow an external system to Export Images and Add, Update, Delete, or Query the P2000 entity database. It is not intended to keep the P2000 database and the external data in absolute “sync.” Records deleted from within the P2000 system are not automatically deleted from the external database. We recommend that specific procedures be established to manage your use of the MIS Interface.

For detailed information about how to use the MIS Interface, (operated *outside* of the P2000 software), see the *MIS Interface Configuration* documentation.

Metasys Integration (BACnet)

Overview

The BACnet Interface allows the P2000 system to be integrated into the *Johnson Controls Metasys* building automation system. The P2000 system can be monitored and controlled from a Metasys M3 or M5 workstation. This interface provides a BACnet gateway through which P2000 hardware configuration and status information can be accessed. It allows an M3/M5 workstation to receive and acknowledge P2000 alarms and events. In addition, the P2000 software can be configured to cause actions to occur within the Metasys system when access is granted.

BACnet software has to be installed on a *different computer* than the P2000 server. Refer to the *Metasys® and P2000AE Integration Manual* for complete instructions.

Theory of Operation

BACnet (**B**uilding **A**utomation and **C**ontrol **n**etwork) is a standard protocol from the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). This protocol provides a standard for allowing computers and equipment controllers to transfer data between the devices in an object-oriented fashion. The BACnet standard defines the types of information and attributes that any device must maintain, and defines how BACnet messages are communicated between the various devices.

The attributes associated with a particular device are grouped together into “Objects.” BACnet defines a standard set of objects, and a device may be represented by, or contain a number of these objects. A device MUST con-

tain at least one BACnet object, called a Device Object. Objects have “attributes” and provide standardized functions to read and write those attributes. BACnet also provides defined methods to send event and alarms between equipment.

The BACnet objects associated with the P2000 system represent the P2000 hardware. There are objects for the P2000 host, counters, panels, terminals, readers, input points, and output points. Each of these objects has attributes that contain the configuration parameters and status for that object. For instance, commands to open doors and set output points are sent to the P2000 system by writing specific attributes. The P2000 BACnet Interface also contains Notification Class objects. These objects hold the names of recipients for P2000 alarms and events.

The P2000 BACnet Interface that resides on the P2000 BACnet Host computer is called BACnet Service. BACnet Service is a Windows NT service, like the other P2000 communication services. BACnet Service creates the BACnet objects that represent the P2000 hardware, and updates the hardware attributes and status in real time as changes occur in the P2000 system. BACnet Service sends data to and receives data from the Metasys system over the network using the BACnet protocol.

BACnet Service will read from the P2000 database any status information it needs, and will use the standard P2000 message routing service (RTLRoute Service) to receive real time status and alarm changes.

To prevent unauthorized BACnet devices from accessing the P2000 system, the P2000 system will only communicate with those devices that have been configured as allowed BACnet devices in the P2000 database. Communication attempts by other devices over the BACnet interface will cause the P2000 system to log a system error and deny communication. A

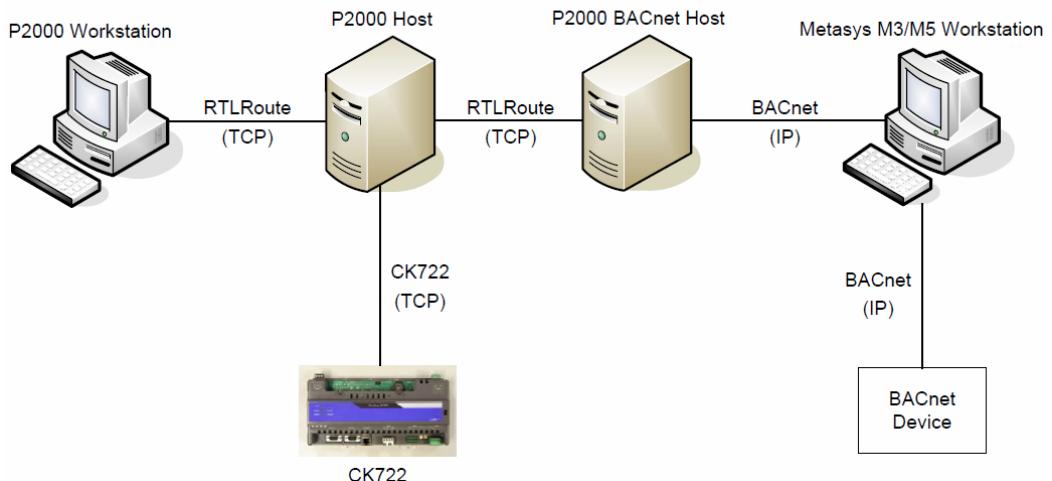
device can also be configured in the P2000 software as a disallowed BACnet device. In this case the P2000 system will not log any error messages but will deny the communication. Typical BACnet devices are M3/M5 workstations and N30 controllers. The following figure shows a logical view of this architecture using a CK722 controller.

The BACnet Interface also provides a way for the P2000 system to initiate actions in other BACnet devices. This capability is called Action Interlock. Action Interlock is an action caused by a write of the specified value to a specific attribute of a specific BACnet object. This allows the P2000 software to initiate actions in an N30 controller or other BACnet device if the proper attribute is known. The P2000 system allows a badge identifier to be assigned up to two actions (Action Interlocks) that are triggered when that badge is granted access, and also allows Action Interlocks to be assigned as a Host Event Action. A typical use of an Action Interlock would be to cause the lights in a person's office to turn on when they are granted access at the door.

The P2000 software will send out its messages and alarms as BACnet event/alarm messages. To receive these BACnet event/alarm messages, a BACnet device must have been added to the recipient list contained in the appropriate Notification Class object. The P2000 BACnet Interface provides for the following event categories:

- Host Events
- Host Log
- Host Logic (not used in this version)
- Audit Log
- Panel Events
- Panel Hardware Status
- Input Status
- Output Status
- Access Grant
- Access Deny
- Access Trace
- Time and Attendance (not used in this version)

Logical Architecture



System Setup

The P2000 software requires minor configuration steps to get its BACnet Interface functional. The only required setup steps are to use the External IP application to define the BACnet devices that will communicate with the P2000 system, and to use Site Parameters to enter the IP address of the computer running the BACnet Service.

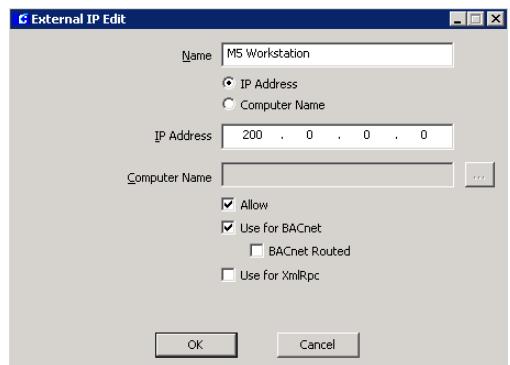
If the P2000 system is registered for the BACnet option, the BACnet communication (BACnet Service) will start automatically when the host starts up. Note that the BACnet Service can be started and stopped using the P2000 Service Control feature, just like the other P2000 communication services. Refer to “Starting and Stopping Service Control” on page 315.

Setting Up External IPs

Here you will define a computer or device to accept messages from external devices. You can also define a computer or device from which the P2000 system will not accept external messages (using the Allow option). If the P2000 system receives an external message from a source that is not configured, the P2000 software will log an error message and not process the message.

To Set Up External IPs:

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the plus (+) sign next to the root **Site Parameters** icon to display default system parameters.
- Click the **External IPs** icon and click the **Add** button. The External IP Edit dialog box opens.



- Enter a descriptive **Name** of the external device.
- Select either **IP Address** or **Computer Name**.
- If you select IP Address, enter the **IP Address** of the computer or device from which to accept messages. Use this option for a device that is not a Windows computer.
- If you select Computer Name, enter the Windows **Computer Name** from which to accept messages, or click the browse [...] button to find a computer by name on your network.
- If you select the **Allow** check box, the P2000 software will allow communication with this device. If Allow is not selected, the P2000 system will deny communication with this device but will not log any error messages for this device.

Note: When configuring BACnet devices, note that since the BACnet protocol includes broadcast messages that are sent to all BACnet devices on the network, the P2000 software may generate a lot of error messages about rejecting messages from unknown BACnet devices. Since these error messages can cause a significant slowdown in the processing of other messages, add these devices as a BACnet device but DO NOT select the Allow option.

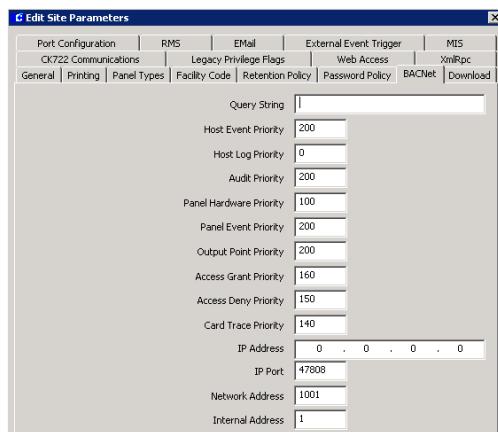
9. Select the **Use for BACnet** check box if this is a BACnet device.
10. If this is a BACnet device, select the **BACnet Routed** check box to send certain messages directly to the device instead of broadcasting them. If the **BACnet Routed** check box is not selected, certain messages will be broadcasted between this device and the P2000 Server. If this device is connected on the other side of a network router, but the check box is not selected, the device will not see broadcasted messages.
11. Select the **Use for XmlRpc** check box if this device uses the XmlRpc protocol. For more information, see “**XmlRpc Tab**” on page 42.
12. Click **OK** to save the settings and return to the System Configuration window.

Setting Up BACnet Site Options

BACnet Site options allow you to configure many system wide settings, defining various parameters of the BACnet Interface.

To Edit BACnet Site Parameters:

1. From the System Configuration window, select **Site Parameters** and click **Edit**. The Edit Site Parameters dialog box opens at the General tab.



2. Click the **BACNet** tab and enter the information on each field according to your system requirements. (See **BACnet Site Field Definitions** for detailed information.)
3. After you have entered all the information, click **OK** to save the settings and return to the System Configuration window.

BACnet Site Field Definitions

Query String – This is a 64-character string that is used to set the Query String attribute for the Host Device object, Counter objects, and Notification Class objects. This value is used in the Metasys M3/M5 Workstation software.

Priority Values – This is the BACnet priority level used when sending the corresponding event or alarm.

IP Address – Enter the IP Address of the BACnet Server to be used for BACnet broadcast messages. If the address is 0.0.0.0, the BACnet interface will use the address of the first network interface card (NIC). This setting is only important on computers with more than one NIC.

IP Port – This is a BACnet protocol addressing parameter. The default value is 47808. This may need to be changed if your existing BACnet devices are using different values.

Network Address – This is also a BACnet protocol addressing parameter. The default value is 1001. This may need to be changed if your existing BACnet devices are using different values.

Internal Address – This should only need to be changed if there is another P2000 Server on the same network. If needed, set this value to be unique to every P2000 Server on the network.

Configuring Hardware Components for BACnet Interface

When configuring legacy Panels, Terminals, Input Points, and Output Points, described in *Chapter 2: Configuring the System*, you may enter a Query String value. This is a 64-character text field that will be used in the Query-FilterString property of Event Notification messages.

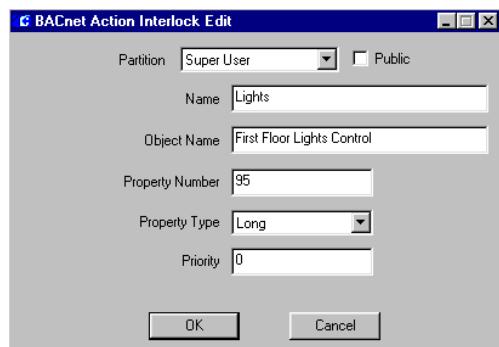
Note: To define legacy panels, terminals, input points, and output points as BACnet objects, refer to the panel “General Tab” on page 50. For CK722 controllers, follow the instructions in “Set Up Message Data Configuration” on page 110.

Setting Up BACnet Action Interlocks

You must define Action Interlocks for the P2000 system to initiate actions in BACnet devices. Here you define the BACnet object and properties that will be written to by an Action Interlock. A typical use of an Action Interlock includes turning on lights and air conditioning at a person’s office when they are granted access at a door.

To Set Up BACnet Action Interlocks:

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the **BACnet Action Interlocks** icon and click the **Add** button. The BACnet Action Interlock Edit dialog box opens.



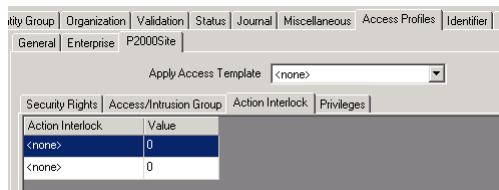
- If this is a partitioned system, select the **Partition** that will have access to this action interlock information, and select **Public** if you wish the action interlock to be visible to all partitions.
- Enter a descriptive **Name** of the BACnet Action Interlock.
- Enter the **Object Name** of the BACnet object to write to.
- Enter the **Property Number** of the BACnet property to write to.
- From the **Property Type** drop-down list, select the data type of the property.
- Enter the BACnet **Priority** used when writing the property. If you enter 0, a non-prioritized write will be used.
- Click **OK** to save the settings and return to the System Configuration window.

Action Interlock Operation

Once the Action Interlocks have been configured, they will be available for assignment to badge identifiers through Access Profiles in the Entity Management window. The object property defined in the Action Interlock will be written with the value associated with the badge identifier. Each badge identifier can be configured to activate up to two Action Interlocks that will be triggered when that badge is granted access.

To Assign Action Interlocks to a Badge Identifier:

1. From the P2000 Main menu, select **Access>Entity Management** to display the Entity Management window.
2. Select an entity from the list and click the **Edit** icon.
3. Click the **Access Profiles** tab.
4. From the list box on the left side of the window, select the Access Profile that will include the action interlocks. Refer to “Access Profiles Tab” on page 138 for more information.
5. Click the local site tab.
6. Click the **Action Interlock** tab. If this is an Enterprise system, refer to “Define Global Access Rights” on page 294 for additional information when assigning access privileges to Enterprise badges.



7. From the first **Action Interlock** drop-down list, select the Action Interlock that will be written when the badge is granted access.
8. Enter the **Value** to write to the first Action Interlock when the badge is granted access. This value will be converted into the correct data type to match the Action Interlock configuration.
9. From the second **Action Interlock** drop-down list, select the Action Interlock that will be written when the badge is granted access.
10. Enter the **Value** to write to the second Action Interlock when the badge is granted access. This value will be converted into

the correct data type to match the Action Interlock configuration.

11. After you define the Action Interlocks, click the **Save** icon to save the Access Profile, and proceed to assign the Access Profile to the badge identifier. Refer to “Identifier Tab” on page 142 for details.

M3/M5 Setup

Refer to the *Metasys® and P2000AE Integration Manual* for instructions on setting up M3/M5 Workstations.

Troubleshooting

Duplicate Object Name Errors

The P2000 system may report errors about Duplicate Object Names when the BACnet Service is started. The error message will give the name of the object that caused the error. This is caused when the name of one object is the same as another object. All terminals, input points, and output points must be unique from each other. An example is when an input point and an output point have the same name.

To correct the error, rename the object specified in the error message.

Msg Rejected Errors

The P2000 system will report a Msg Rejected error when BACnet receives a message from an IP Address that does not correspond to a configured BACnet device. The error message will contain the IP Address of the device that sent the message.

To correct the error, add a BACnet device for the IP Address specified in the error message. If this device has no reason to communicate with the P2000 BACnet Interface, clear the **Allow** check box.

Action Interlock Errors

When you use Action Interlocks, you may see one of the following error messages:

- ActionInterlock OpenConnection error
- WriteAttributeWait error
- Error writing object

All these errors indicate a failure to write to the object defined in the Action Interlock dialog box. Most likely, the problem is due to incorrect values in the Action Interlock definition. Verify the Object Name, Property Number, and Property Type in the Action Interlock dialog box in the P2000 system. Note that the Object Name must match exactly the name of the object, including the case.

If the Action Interlock is defined correctly, then there is a BACnet communication problem between the P2000 Server and the device containing the object. Verify basic network connectivity using the “ping” command on the P2000 Server to ping the IP address of the device. If you can’t ping the device, then most likely there is a routing problem that is blocking the BACnet broadcast messages between the device and the P2000 Server. Refer to the BACnet Communication Troubleshooting section of your M3/M5 documentation.

Metasys System Extended Architecture

This option allows the P2000 system to be integrated with building management components designed for Metasys system extended architecture using Web Services technology. The integration provides the ability for objects in the P2000 security system to be viewed from a single user interface, along with all other building systems controlled by the Metasys system extended architecture.

Through this integration, the P2000 system can expose *HostEngine* and *Panel* objects to the Metasys system extended architecture user interface, allowing clients to browse through the P2000 object tree with the purpose to read object attributes, change those object attributes which are “writable,” and send commands to objects for readers and output points.

For detailed instructions refer to the *Metasys System Extended Architecture Integration Option* documentation.

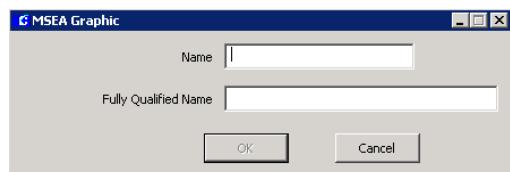
Defining MSEA Graphics

The MSEA Graphic feature allows you to assign a graphic reference to P2000 alarms. When the P2000 alarm is received and displayed by the Metasys system extended architecture, the operator can click the alarm to display the graphic item associated with the alarm and the item that caused the alarm.

Prior to assigning the MSEA graphic to the alarm (see page 78), you must configure the Fully Qualified Reference Name (FQRN) of the graphic item, as defined by the Metasys system extended architecture.

To Define MSEA Graphics:

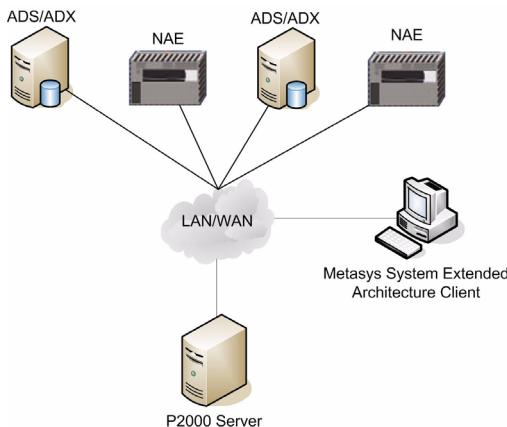
1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted.
2. In the System Configuration window, click the **MSEA Graphics** icon and click the **Add** button. The MSEA Graphic dialog box opens.



3. Enter an alias **Name** for the Fully Qualified graphic reference name.
4. Enter the **Fully Qualified Name** of the graphic item, as defined by Metasys system extended architecture.
5. Click **OK** to save the MSEA graphic name.

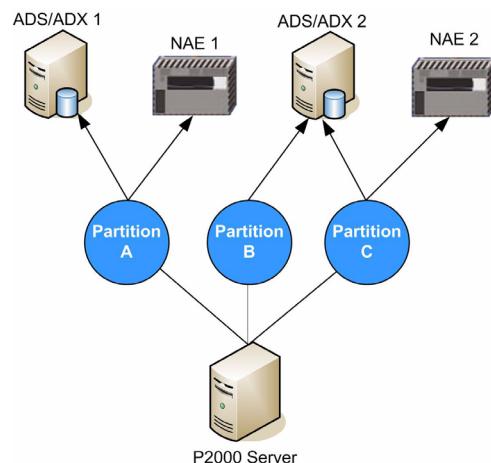
Registering the P2000 Server with a Site Director

To expose P2000 objects to the Metasys system extended architecture, you must register the P2000 server with a Metasys Site Director (ADS/ADX server or NAE controller) by adding a MSEA Registration definition in the P2000 server. P2000 enables you to create multiple MSEA Registration definitions, so you can register the P2000 server with multiple Site Directors.



CAUTION If a NAE controller is used as the Site Director, the controller can only receive four events per second from the P2000 server. If more than four events are received per second, the NAE may erroneously indicate that the P2000 server is offline.

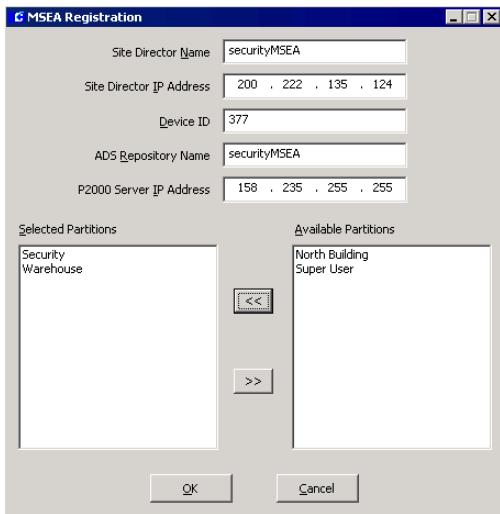
In addition, you may register certain partitions with a particular Site Director, so that only those P2000 objects associated with the selected partition(s) are visible from the Metasys system extended architecture (see the following illustration).



In the example above, the P2000 objects associated with Partition A will only be visible from ADS/ADX 1 and NAE 1; the P2000 objects associated with Partition B will only be visible from ADS/ADX 2; and the P2000 objects associated with Partition C will only be visible from ADS/ADX 2 and NAE 2.

To Register a P2000 Server with one or more Site Directors:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the **MSEA Registrations** icon and click **Add**. The MSEA Registration dialog box opens.



3. Enter the **Site Director Name** where the Site Director is installed (the server name of the ADS/ADX or the name of the NAE).
4. Enter the **Site Director IP Address** of the server where the Site Director is installed (the IP address of the ADS/ADX or the NAE).
5. Enter the **Device ID**. If the P2000 system interfaces with Metasys system extended architecture release 2.1 or earlier, enter **185**. For later releases of Metasys, enter **377** or contact *Johnson Controls* Technical Support for the Device ID used on the version of Metasys you are currently running.

6. Enter the **ADS Repository Name** (computer name) of the Metasys ADS Repository.

Note: The ADS Repository stores messages forwarded by the P2000 system; however, a NAE device used as a Site Director cannot store these messages. If you have a NAE defined as a Site Director, to view messages forwarded from the P2000 system, you must define a valid ADS Repository name for the NAE device. Refer to the *Metasys System Extended Architecture Integration manual* for more information.

7. Enter the **P2000 Server IP Address**.
8. In the **Available Partitions** box, select the partition(s) you wish to register with the Metasys Site Director. To assign partitions, simply select one or more partitions and click the left arrow button to move them to the **Selected Partitions** box.
9. Click **OK** to save the MSEA Registration.
10. Repeat the previous steps for each Site Director with which you wish to register the P2000 server.
11. To complete the P2000 MSEA Registration, you must stop and restart the **P2000 XmlRpc Interface Service**. For details, refer to “Starting and Stopping Service Control” on page 315.

The P2000 should now appear as a device in the Metasys system extended architecture user interface for the associated Site Director. Refer to the *Metasys System Extended Architecture* manual for information on launching and logging into the Metasys system extended architecture user interface.

Guard Tour

Guard Tour is a sequence of transactions, that must be performed within a specified time frame, to ensure your facility is properly monitored by security personnel. The main purpose of a tour is to ensure and record that an area has been physically visited. It provides real time monitoring of guard activities, reporting if a guard arrives early or late at designated tour stations. Guard Tour stations can be either readers or input points.

Tours may run to occur at regular time intervals or they can be started manually. They can also be run in forward or reverse order.

The P2000 system allows 256 Guard Tour definitions. Each tour may contain up to 16,000 stations, which comprises the individual readers or input points where transactions occur.

If the P2000 system is registered for the Guard Tour option, the Guard Tour Service communication (GTService) will start automatically when the host starts up. Note that GTService can be started and stopped using the P2000 Service Control feature, just like the other P2000 communication services. Refer to “Starting and Stopping Service Control” on page 315.

Basic Principles and Definitions

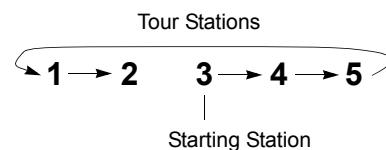
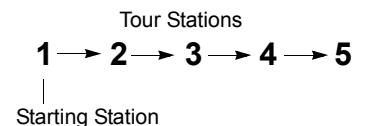
Guard Tour – A defined set of check-in stations and minimum and maximum times for checking in at each station.

Check-in Station – Also called simply station. A reader or input point defined as part of a Guard Tour.

Forward – The expected sequence the tour will take place. Beginning with the starting check-in station, the tour will progress sequentially through all stations in a forward direc-

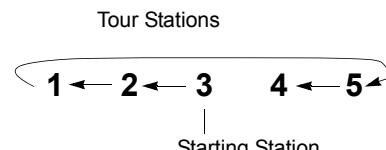
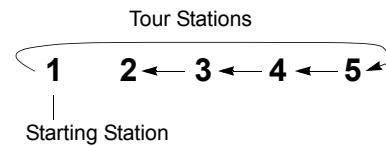
tion. The starting tour station can be selected automatically or manually.

Forward Tour Example



Reverse – The expected sequence the tour will take place. Beginning with the starting check-in station, the tour will progress sequentially through all stations in reverse order. The tour still begins at the starting station, regardless of Forward or Reverse direction. The starting tour station can be selected automatically or manually.

Reverse Tour Example



Tour Badge – An access badge used during an actual guard tour to check-in at readers.

Tour Guard – The name of the person that was assigned a Tour Badge.

Tour Activation – Guard Tours may be activated automatically by time zones or start times, or manually by a system user.

Tour Abort – The P2000 system will discontinue tracking a Guard Tour if 1) the tour Abort Time defined in the tour has exceeded, or 2) a user manually aborts a tour.

Sequence of Steps

The basic procedure for defining and implementing Guard Tours are:

- Define system hardware
- Define entities and assign Tour Badges to the appropriate personnel
- Configure Guard Tours
- Define Tour Stations
- Control and manipulate Guard Tour activities

Steps to perform each procedure are presented in the following sections.

Defining System Hardware for Guard Tour Operation

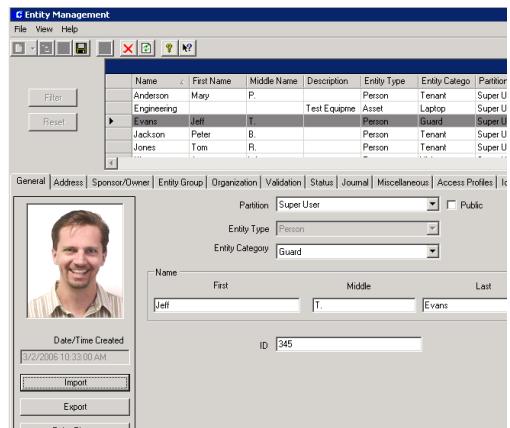
Prior to defining Guard Tours you must properly configure the system hardware and its components; specifically, the readers and inputs points you intend to use in defining tours. If this has not been completed, some of the functions described in this section will not be ready to operate. Refer to *Chapter 2: Configuring the System* for details.

Assigning Tour Badges

The main purpose of a tour is to ensure and record that an area has been physically visited. While a guard may check-in at a reader defined in a Guard Tour as a station, access through that reader-controlled door may or may not be desired. Use the following instructions to assign tour badges to the persons who will participate in guard tour operations.

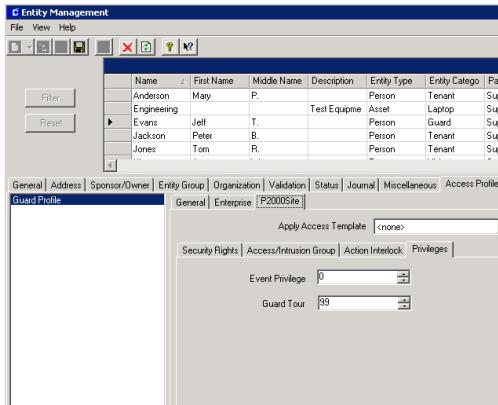
To Assign a Tour Badge:

1. From the P2000 Main menu, select **Access>Entity Management**. The Entity Management window opens.
2. Create a new record or edit an existing record as desired. For details, refer to “Entering Entity Information” on page 132.



3. In the General tab, select from the drop-down list the **Entity Category** that has been assigned with a “Guard” business rule. Refer to “Define Entity Categories” on page 119.
4. Click the **Access Profiles** tab. The General tab under Access Profiles displays basic profile information associated with the guard. Refer to the “Access Profiles Tab” on page 138 for details.

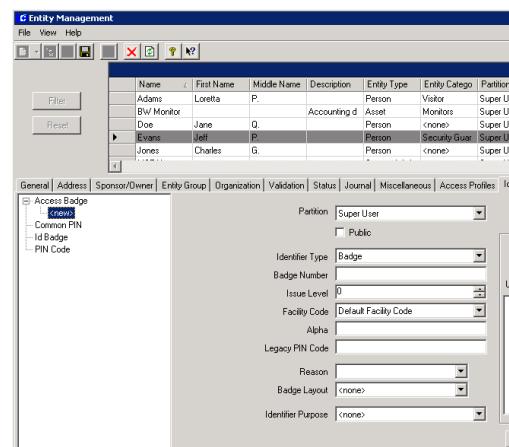
- Click the **local site** tab under Access Profiles. This tab displays access options associated with the guard.
- Click the **Privileges** tab and from the **Guard Tour** drop-down list select the priority number to be assigned to the Tour Badge.



APPLICATION NOTE

Tour priority determines which tours the selected guard can perform. These can be all defined tours with a priority less than or equal to the guard's assigned Guard Tour priority. For example, a guard with Guard Tour priority 45 is authorized to complete tours with a priority of 1 through 45. If the guard attempts to check-in at stations of a tour defined as priority 46, their badgings will be ignored by the Guard Tour.

- Click the **Identifier** tab.
- Right-click **Access Badge** and select **Add** to create the Tour Badge.



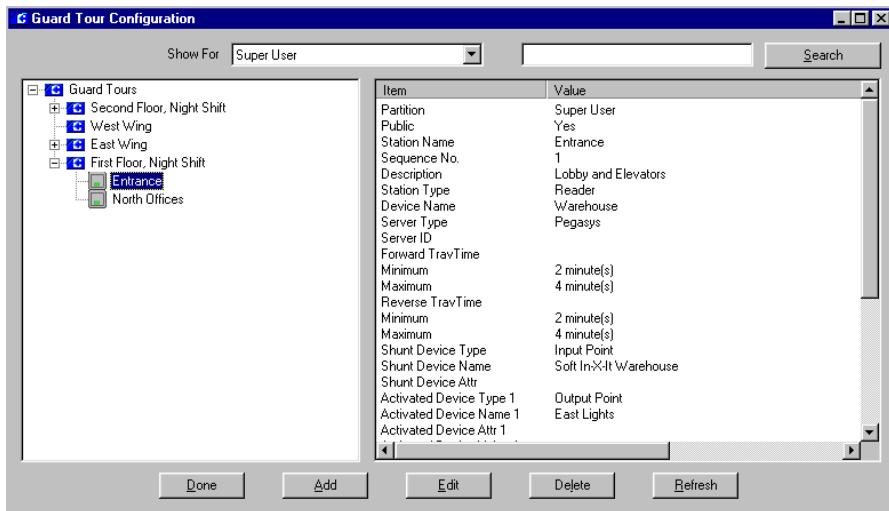
- Enter the badge number. For additional information refer to “Identifier Tab” on page 142.
- Assign the Access Profile that contains the Guard Tour privilege.
- After creating the Tour Badge, click the **Save** icon and close the Entity Management window.

Configuring Guard Tours

The following steps are used to define Guard Tours. Before proceeding, you must define input points and terminals (readers) to be used in tours. In addition, Tour Badges should have been assigned to the appropriate persons.

Using the Guard Tour Configuration Window

The Guard Tour Configuration window provides quick access to all guard tour component configurations. When you select **Options>Guard Tour>Tour Configuration** from the P2000 Main menu bar, the Guard Tour Configuration window opens, displaying the actual Partition, Workstation, and User Name on the right windowpane. All defined Guard Tours display on the left side of the window. A plus



(+) sign next to a defined Guard Tour indicates that Tour Stations exist beneath it. When you select a Guard Tour or Tour Station, the detailed settings and values relating to that selection are listed on the right windowpane.

Note: You cannot edit Tour Definitions or Stations from the Guard Tour Configuration window while a tour is running.

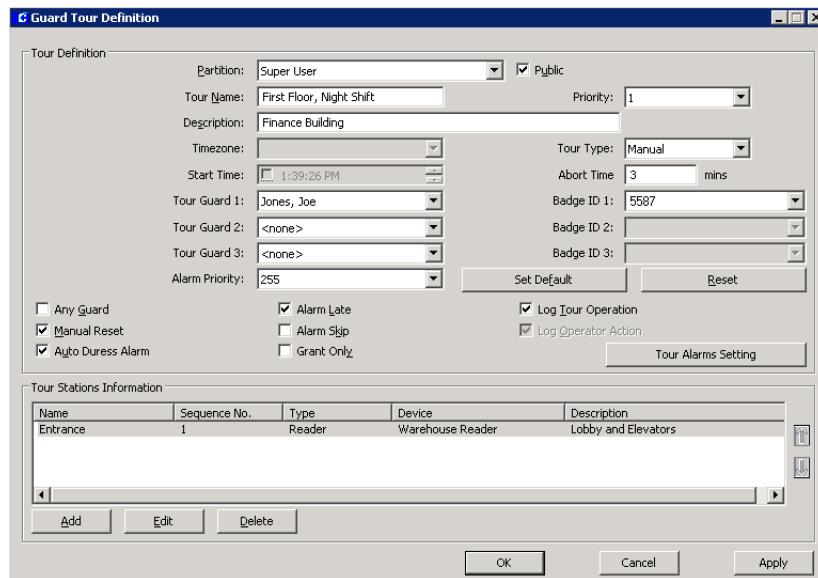
To search for specific items, enter the name of the item in the search field at the top right corner of the window. You can enter complete or partial words; no wildcards are needed, and this field is not case sensitive.

Click the **Search** button. The window will display the match entered in the search field. Continue clicking **Search** until you find the item you are looking for.

To Define a Guard Tour:

- From the P2000 Main menu, select **Options>Guard Tour>Tour Configuration**. The Guard Tour Configuration window opens.
- Click the **Guard Tours** root icon, then click the **Add** button to access the Guard Tour Definition dialog box.
- If this is a partitioned system, select the **Partition** that will have access to this Tour, and select **Public** if you wish to make this Tour visible to all partitions.
- Enter the **Tour Name** and optional **Description**.
- From the **Priority** drop-down list, select the tour's priority from 1 (lowest) to 99. Only tour badges with equal to or greater than this priority can perform the tour.
- Select one of the following **Tour Types** from the drop-down list:

Manual – The tour must be initiated manually from the Guard Tour Control window, described on page 251.



Auto Forward – The tour will be initiated at a time specified by the Timezone or Start Time fields. The guard will be expected to begin at the first defined station and proceed through all stations in a forward direction.

Auto Reverse – The tour will be initiated at a time specified by the Timezone or Start Time fields. The guard will be expected to begin at the first defined station, and proceed through all stations in a reverse direction.

Random Watch – There is no sequencing in this mode. All defined stations are monitored at all times, until the time entered in the Run Time expires. This is to assure that no station goes unchecked for greater than a specific stated time.

Timezones, Start and Abort Times

If you select Manual as the tour type, the Timezone and Start Time fields are disabled; these are only enabled when you select Auto Forward, Auto Reverse, or Random Watch.

Timezones – The purpose of selecting a Timezone is to provide an automatic starting time for the Guard Tour. You need to define Time Zones prior to defining Guard Tours. Refer to “Time Zones” on page 44 for detailed instructions.

In the following example, a Time Zone was defined to be assigned to a tour, the start (active) time for the tour is 8:00 p.m. Monday through Friday.

Time Zone							
Name: Tour Schedule							
Periods							
Monday	Inactive	12:00:00 AM	8:00:00 PM	12:00:00 AM	12:00:00		
Tuesday	Inactive	12:00:00 AM	8:00:00 PM	12:00:00 AM	12:00:00		
Wednesday	Inactive	12:00:00 AM	8:00:00 PM	12:00:00 AM	12:00:00		
Thursday	Inactive	12:00:00 AM	8:00:00 PM	12:00:00 AM	12:00:00		
Friday	Inactive	12:00:00 AM	8:00:00 PM	12:00:00 AM	12:00:00		
Saturday	Inactive	12:00:00 AM	12:00:00 AM	12:00:00 AM	12:00:00		
Sunday	Inactive	12:00:00 AM	12:00:00 AM	12:00:00 AM	12:00:00		
Holiday 1	Inactive	12:00:00 AM	12:00:00 AM	12:00:00 AM	12:00:00		

Note: Stop (inactive) times are not necessary in a Time Zone, unless a Guard Tour is to be run more than once per day. In this case, you would enter a stop time to disable the time zone so it can become active again that day, at another time.

If you define several time blocks, ensure that enough time is allotted between the active and inactive times to realistically complete the tour.

Start Time – When you click the Start Time check box, the Timezone field is automatically disabled. Enter the time the tour is scheduled to start.

Abort Time – Enter the time in minutes (from 2 to 1440). This is the maximum time allowed to expire, before a tour is automatically aborted. This field changes to **Run Time** if Random Watch is selected as the Tour Type.

Once these times are assigned, you can assign the tour to a specific guard, or allow any guard with the appropriate priority to perform the tour.

To Assign the Tour to a Specific Guard:

1. In the Guard Tour Definition dialog box, click the **Tour Guard 1** drop-down list and select a name. Only names with the appropriate Entity Category selected in the Entity Management window will display in the list.
2. Once a Tour Guard is selected, the corresponding **Badge ID** field is enabled. Select a badge from the drop-down list. Only badge numbers with priority greater than or equal to the Tour Priority will display in the list.
3. To select additional guards, select **Tour Guard 2** and **Tour Guard 3**, and their corresponding **Badge ID** numbers.
4. To allow any guard with the proper priority to perform the tour, click the **Any Guard** box. Refer to “Additional Guard Tour Options” for more information.

Note: One guard can run only one tour at the same time. In addition, one tour can be run only by one guard, even if two guards were to walk the same tour; it is the guard that badged at the initial station who must complete the tour using the same badge at the remaining stations.

Additional Guard Tour Options

The remaining options in the Guard Tour Definition dialog box are described in the following paragraphs.

Alarm Priority – Select from the drop-down list an alarm priority from 0 to 255, in which the Guard Tour alarm message will be placed in the queue.

Set Default – Click the **Set Default** button to store the default preference values, which include Tour Priority, Tour Type, Alarm Priority, and all check boxes.

Reset – Click the **Reset** button to restore the pre-stored preference values.

Any Guard – Select to allow any guard with the proper priority to perform the tour. When you select this box, the Tour Guard 1 to 3 and corresponding Badge ID fields become disabled.

Manual Reset – If selected, the user has to click the **Complete** button in the Guard Tour Control dialog box to remove the tour from the tour list. This is to indicate that the tour has completed.

Auto Duress Alarm – If selected, an auto duress alarm is generated when a guard registers three consecutive times at a station within one minute, for example by swiping the badge three times, or by activating a tour input three times. If Manual Reset is not selected and Auto Duress Alarm is enabled, the tour status changes to Idle after one minute when it completes.

Alarm Late – If selected, an alarm is generated when a guard checks in later than expected at a

station. If the check box is not selected and a guard is late, this will simply be considered as a tour operation event.

Note: Operation events include, for example, *Tour Alarmed, Tour Started, Station Checked in On Time, Station Checked in Early, Station Checked in Late, Station Checked in Out of Order, Tour Stopped, Tour Restarted, Tour Aborted, Tour Completed, Tour Terminated, Station Late Timer Reached*.

Alarm Skip – If selected, an alarm is generated when a guard skips a tour station. If the check box is not selected and a guard skips a station, this will simply be considered as a tour operation event.

Grant Only – If selected, the system will register only access grant transaction messages when the guard swipes the badge at the station. If not selected, either access grant or deny messages will be registered.

Log Tour Operation – If selected, all tour operation events are logged to the system as events, and therefore are available for history, event processing, and so forth.

Log Operator Action – All operator actions, such as configuring the Guard Tour, or controlling a Guard Tour are logged as events. This option is selected by default and is not configurable.

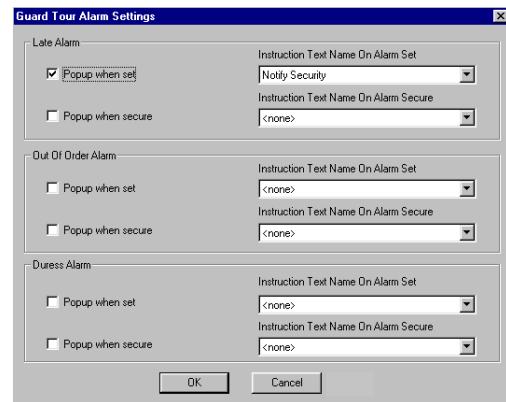
Tour Alarms Setting

Tour Alarms Setting enable the Alarm Monitor window to automatically pop up in front of all other windows on the screen whenever a Guard Tour alarm condition occurs.

You can also specify instruction text that will display when an operator responds to a Guard Tour alarm going into a Set and/or Secure state. Enabling the Popup feature and selecting Instruction Text are independent tasks, and can be used in any combination.

Before you assign instruction text to the various pop ups, you must first create instruction text. See “To Create Instruction Text:” on page 82.

1. In the Guard Tour Definition dialog box, click the **Tour Alarms Setting** button. The Guard Tour Alarm Settings dialog box opens.



2. Enable any of the following **Popup when set** and/or **Popup when secure** check boxes, and select the **Instruction Text Name** from the associated drop-down lists that will display in the Alarm Response window whenever any of the following alarm conditions occur:

Late Alarm – An alarm message is generated when a guard checks in later than expected at a station. This option is available if you select the Alarm Late check box in the Guard Tour Definition dialog box.

Out Of Order Alarm – An alarm message is generated if a guard skips a tour station. This option is available if you select the Alarm Skip check box in the Guard Tour Definition dialog box.

Duress Alarm – An alarm message is generated if a guard registers three consecutive times at a station within one minute or by activating a tour input three times. This

option is available if you select the Auto Duress Alarm check box in the Guard Tour Definition dialog box.

- Click **OK** to return to the Guard Tour Definition dialog box.

Adding Stations to the Guard Tour

Tour Station information, such as Station Name, Sequence Number, Type, Device, and Description displays in the list box at the bottom of the Guard Tour Definition dialog box, for all the stations assigned to that Guard Tour.

Guard Tour Stations can be either readers or input points.

To Add Stations to the Guard Tour:

- Click the **Add** button at the bottom of the Guard Tour Definition dialog box. The Tour Station Definition dialog box opens

showing the Guard Tour Definition name on the title bar.

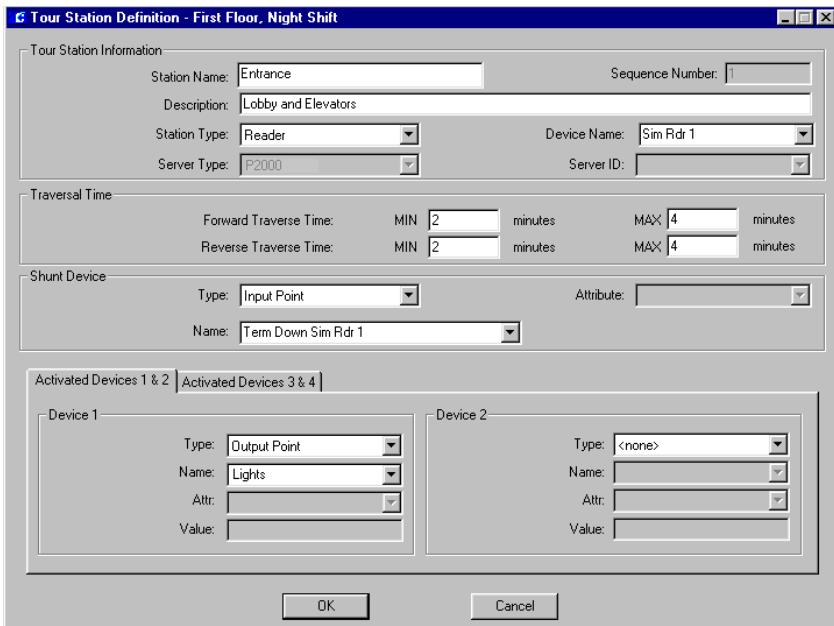
- Enter the required information. See “Tour Station Definition Fields” for detailed information.

Tour Station Definition Fields

Tour Stations Information Box

Station Name – Enter a descriptive name for the station.

Sequence Number – This field displays the number that is automatically assigned when you define a new station. The Tour Stations Information list at the bottom of the Guard Tour Definition dialog box shows the stations assigned to this tour in sequence. You can change the sequence of the stations by clicking the **Up** or **Down** arrows in the Tour Stations Information list box, to change the sequence of the selected station.



Description – Enter a description of this station, if desired.

Station Type – Click the drop-down list button to select either **Input** or **Reader** as the station type.

Device Name – Click the drop-down list to select a previously defined input point or reader (terminal) that has not been assigned to another station. The list will only display the devices associated with the Station Type. If the input point selected is already assigned to a cabinet door, the Report Alarm option in the Cabinet Configuration dialog box should be selected to be able to report guard tour messages.

Server Type – This field is not currently used in this version of the P2000 software.

Server ID – This field is not currently used in this version of the P2000 software.

Traversal Time Box

Traverse Time (**Forward** or **Reverse**) sets the amount of time in minutes a guard has to reach the defined station. The maximum value is 1440 minutes. Traverse Times work in relation to a tour's Start and Abort Times. One of six possible values is assigned when a guard reaches a station:

- Early
- Running
- Late
- Out of Order
- Completed
- Idle

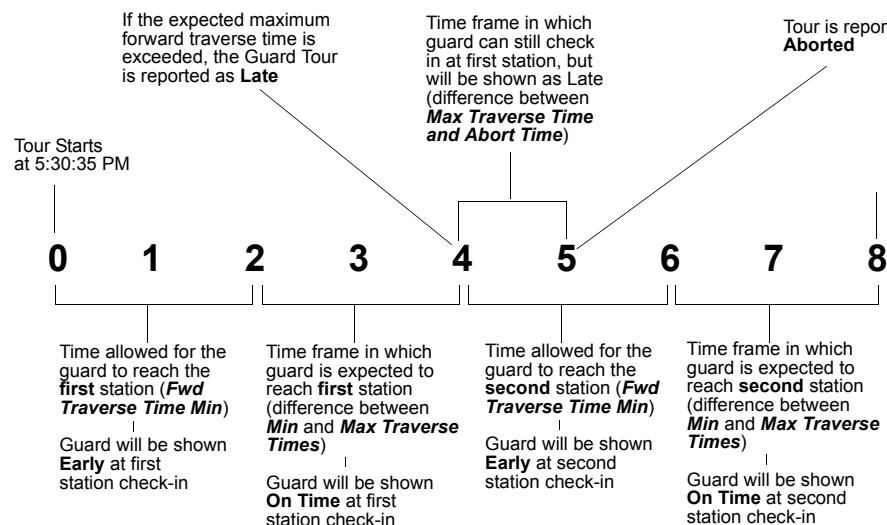
Traverse Times are started at station check-in. For example, suppose the guard reaches station one at the two-minute mark (see illustration). The check-in would be reported as Early and the Traverse Timer for the next station would

Assume the tour has:

Start Time: 5:30:35 PM
Abort Time: 5 minutes

Assume Station 1 is defined as: 0 - 8 are minute increments

Forward Traverse Time Min: 2
Forward Traverse Time Max: 4



start. If the minimum and maximum values were set at 2 for station two, the on time check-in for station 2 would be between the 4 and 6-minute marks. These same timing principles apply to all stations defined in the tour as well as Guard Tours designed to run in reverse order.

Note: *If the Tour Type selected is Random Watch, the Forward Traverse Time defines how often the guard will check a defined station. Reverse Traverse Time is not available if Random Watch is selected.*

Shunt Device Box

During the course of the Guard Tour, you may need to suppress alarms (shunt input points) as part of the tour.

This operation is similar to suppressing an input point or input group as part of an Event, except that an input point or input group will remain suppressed until the next station in the tour is reached, a tour alarm is set, or the tour is aborted.

Type – Click the drop-down list button to select either **Input Point** or **Input Group** as the Shunt Device Type.

Name – Click the drop-down list to select a previously defined input point or input group. The list will only display the devices associated with the Shunt Device Type.

Attribute – This field is not currently used in this version of the P2000 software.

Activated Devices Box

During the course of the Guard Tour, you may need to activate devices (set or reset output points) as part of the tour.

This operation is similar to setting or resetting an output point or output group in the main

Control menu, except that an output point or output group will remain set until the next station in the tour is reached, a tour alarm is set, or the tour is aborted.

Type – Click the drop-down list button to select either **Output Point** or **Output Group** as the Activated Device Type.

Name – Click the drop-down list to select a previously defined output point or output group. The list will only display the devices associated with the Activated Device Type.

Attribute – This field is not currently used in this version of the P2000 software.

Value – This field is not currently used in this version of the P2000 software.

To activate more than one device, you can define them in the **Device 2** box, then click the **Activated Devices 3 & 4** tab and follow the same steps.

Note: *The system does not shunt input points or activate output points assigned to the last station defined in the tour.*

Saving the Station as Part of the Tour

After defining a station, click **OK** to return to the Guard Tour Definition dialog box, the station displays in the Tour Stations Information box.

Continue to add stations as necessary. When finished, click **OK** to return to the Guard Tour Configuration window. The Guard Tour will be written to the database.

Controlling Guard Tours

Use the Guard Tour Control window to start and stop tours and monitor their progress.

To Control Guard Tours:

1. From the P2000 Main menu, select **Options>Guard Tour>Tour Control**. Enter your password if prompted. The Guard Tour Control dialog box opens.
2. Select the **Partition** that contains the Guard Tours you wish to control.
3. Select the **Active Tours** option to display all tours currently in the status database, for the partition selected, and that are in non-idle state.
4. Select the **All Tours** option to display all tours currently in the database, for the partition selected, regardless of their state.
5. Click the **Set Alarm Color** button to display all Alarmed records in a different color. A Color dialog box opens where you select the desired color, then click **OK** to return to the Guard Tour Control dialog box.
6. To display a specific Guard Tour, use the **Filter** box to enter a filter criteria, such as “w*”, then click the **Show** button. The list will display all Guard Tours that start with the letter “W.”

Note: You can also select a previously typed filter from the drop-down list. This list will be cleared when you close the Guard Tour Control dialog box.

7. To display all Guard Tours again (Active or All), select <**none**> from the Filter drop-down list.
8. If you wish to sort the list of tours shown on the list box, click the specific column header. The current sort order can be set as default by clicking the **Set Current Sort Order Default** button. The default sort before clicking this button is by Start Time.

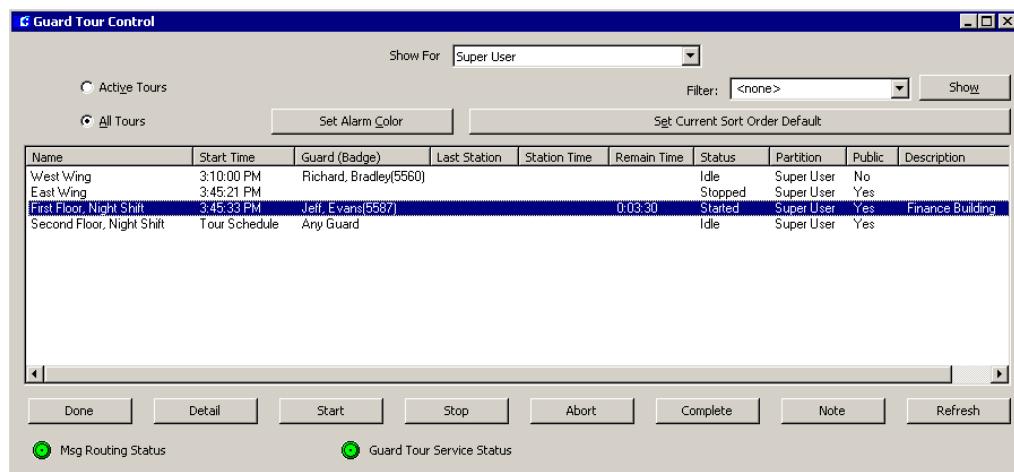
Viewing the Tour Control List Box

The following information is shown for each tour in the list.

Name – The tour name, as configured in the Guard Tour Definition dialog box.

Start Time – This column displays either a defined start time, a Timezone name, or if it was defined as a Manual tour type.

Guard (Badge) – If a tour is assigned to a specific guard, the name displays here with the corresponding Badge number.



Last Station – Displays the number of the last station that the guard registered at.

Station Time – Displays the time that the guard registered at the last station.

Remain Time – Displays the time remaining for the guard to reach the next station, without being late. The time displayed decreases by 30-second increments if more than one minute remains. If less than one minute remains, the time displayed decreases every one second.

Status – Displays one of the following status:

- **Alarm** – An alarm has occurred within the guard tour, such as guard late, duress, etc.
- **Started** – The tour has been started, either manually or automatically, but the first station has not been reached.
- **Running** – Status given to an active tour after the first station has been reached.
- **Early** – When a tour station check-in is sooner than expected.
- **Late** – When a tour station check-in is later than expected.
- **Out of Order** – When a tour station check-in occurs out of sequence.
- **Stopped** – The tour has been manually stopped.
- **Aborted** – The tour has been cancelled either manually or because of an expired Abort Time (stations not reached in time).
- **Completed** – The tour has completed successfully without any alarms.
- **Idle** – The tour is not running.

Partition – Displays the partition as configured in the Guard Tour Definition dialog box.

Public – Displays whether or not this guard tour is made public, as configured in the Guard Tour Definition dialog box.

Description – Displays the description of the tour, as configured in the Guard Tour Definition dialog box.

Note: *The Message Routing Status indicator at the bottom of the window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.*

The Guard Tour Service Status indicator will be displayed in green to indicate that the Guard Tour Service is up and running. If Guard Tour Service goes down, the indicator will turn red.

To Start a Manual Tour:

1. Select a tour from the Guard Tour Control list that has a **Manual** tour type in the Start Time column.
2. Click the **Start** button at the bottom of the Guard Tour Control dialog box. The Start Tour dialog box opens.



3. Click the **Guard** drop-down list and select a name to assign a guard to run the selected tour. If only one guard was defined to run this tour, the name of the guard will automatically display on this field.
4. Click the **Badge** drop-down list and select a badge number. If only one badge was assigned to this guard, that number will automatically display on this field.

Note: If Any Guard was selected in the Guard Tour Definition dialog box, the above fields will be disabled.

5. Click the **Starting Station** drop-down list and select any station in the tour to be station 1.
6. Select whether this tour will start in **Forward** or **Reverse** order.
7. Click **OK** to start the tour.

Guard Tour Handling

The Guard Tour Service communication (GTService) will check the Start Time or Time-zone definitions every one minute to determine whether to start automatic tours.

As an operator or guard, you may be required to handle tour conditions. The tour control will typically include steps similar to the following:

Stopping a Tour – You can temporarily stop a tour by clicking the **Stop** button. The status of the tour will change to *Stopped*, and the Stop button will change to *Restart*. At this point the tour can be either restarted or aborted.

Restarting a Tour – If the tour has been temporarily stopped or alarmed, you can click the **Restart** button to update the status of the tour to its previous status, before it was stopped or alarmed.

Aborting a Tour – To manually end a tour, click the **Abort** button. The status will change to *Aborted*, or to *Idle* if Manual Reset was not enabled.

Completing the Tour – When all actions needed to complete a tour have been completed, and Manual Reset was selected in the Guard Tour Definition dialog box, the status of the tour will display as *Completed*, click the **Complete** button to terminate the tour. The status will change to *Idle*. If Manual Reset was not

selected and Auto Duress Alarm is enabled, the status of the tour will display as *Completed* and after one minute will change to *Idle*.

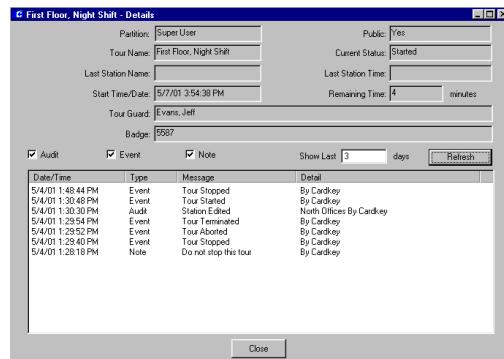
Refreshing the Tour Control window – The Guard Tour Control list is updated every one minute, or when the **Refresh** button is selected.

Guard Tour Details

You can monitor the activity occurring within Guard Tours. The Detail button on the Guard Tour Control dialog box displays current Guard Tour status information for the selected tour.

To Display Guard Tour Details:

1. Select a tour in the list.
2. Click the **Detail** button. The guard tour Details dialog box opens. The top portion of the window shows the tour details.



The scroll list includes a chronological list of all activities for the specific tour, such as events, audits, and operator notes. If Set Alarm Color was selected in the Guard Tour Control dialog box, the alarms will display in the color selected.

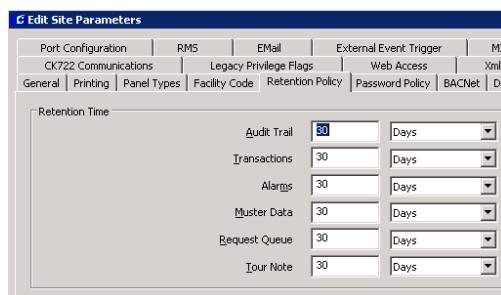
3. Enable the **Audit** box to display all audit transactions.

4. Enable the **Event** box to display all event transactions. If Log Tour Operation was enabled in the Guard Tour Definition dialog box, this option is already enabled.
5. Enable the **Note** box to display all Notes related to this tour. See the following section on “Guard Tour Notes” for more information.
6. In the **Show Last** box, enter the number of days of tour activity you wish to display.
7. Click the **Refresh** button to update the list.
8. Click **Close** to return to the Guard Tour Control dialog box.

Guard Tour Notes

The tour Note dialog box provides a place to enter instructions for a particular tour. The amount of time after which all notes will be purged is set up in the Site Parameters dialog box.

1. From the System Configuration window select **Site Parameters** and click **Edit**. The Edit Site Parameters dialog box opens at the General tab.
2. Click the **Retention Policy** tab and enter the amount of time and select Minutes, Hours, or Days from the **Tour Note** drop-down list, after which all notes will be deleted from the system.



3. Click **OK** to save the settings and return to the System Configuration window.

To Add Tour Notes:

1. From the Guard Tour Control dialog box, select a non-Idle tour from the list.
2. Click the **Note** button. The Note dialog box opens.



3. Enter the note you want to display in the Detail dialog box.
4. Click the **Add** button. The list box will display the Date/Time the note was added, with the User Name, and the actual note text.
5. Click **Done** to return to the Guard Tour Control dialog box.

Viewing and Printing Transactions in Real Time

Tour transactions will be sent through real time messages to the Real Time List. You will be able to monitor real time messages, such as tour alarm messages and see the status of a tour. Once the status changes or the tour proceeds, corresponding real time message will be generated. Select the Guard Tour box in the Real Time List window, to display all guard tour transactions as they occur. Refer to “Using the Real Time List” on page 213 for more information.

To print tour transactions as they occur, you can either print them from the Real Time List window, or select the Guard Tour check box in the Site Parameters dialog box, Printing tab. Refer to “Printing Tab” on page 31 for more information.

CCTV

The P2000 system can interface with approved closed circuit television (CCTV) systems via a Host computer connected through an RS-232 serial communications line.

System actions can be sent by CCTV control to the CCTV Switch or run by event actions. The commands can:

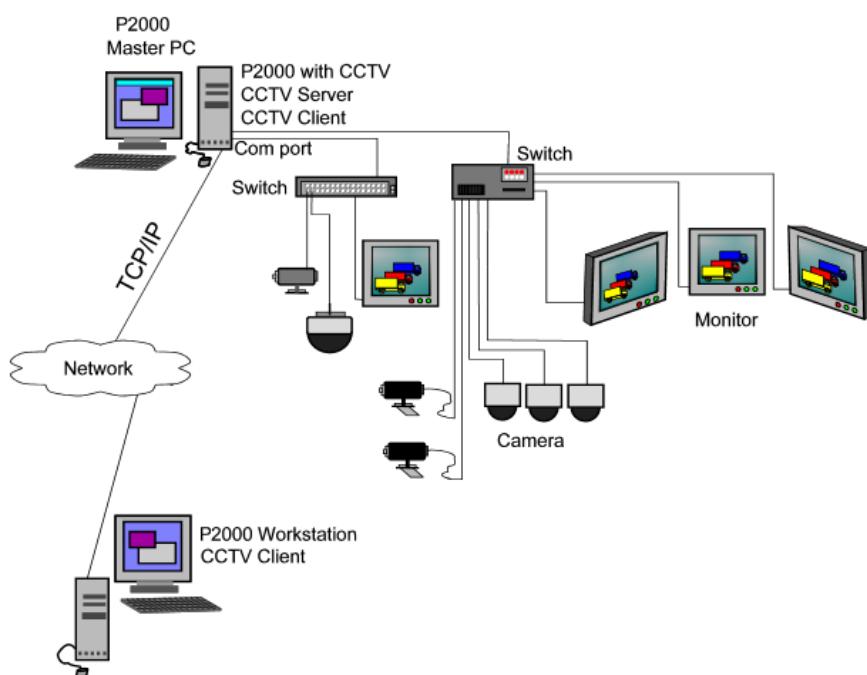
- Place a Camera on a Monitor
- Run a Sequence on a Monitor
- Pan, tilt, zoom; focus and control iris functions; and switch on wipers, washers, and lights for a given Camera
- Run Tours and Macros
- Run Patterns and Presets, and use Auxiliaries

Settings and options vary, depending on the type of CCTV Switch selected. Installation of

the CCTV equipment will be in accordance with the manufacturers' instructions. For a complete list of the protocols supported by the CCTV option, refer to *Appendix D: CCTV Switch Protocols*.

The following diagram illustrates the possible configurations of the CCTV system equipment. The software provided by the CCTV option has two main components; the CCTV Server and the CCTV Client. The CCTV Server consists of the OPC Server, drivers and port controllers, and the CCTV Client consists of the CCTV Configuration and CCTV Control software. For instructions about installing CCTV, please refer to the *P2000AE Server/Workstation Software Installation Manual*.

When the CCTV option is installed on your system, the CCTV communication service (CCTV Server) will start automatically when you start the PC.



Using P2000 functions with the CCTV Option

The CCTV option benefits from the following standard P2000 features:

Partitioning – If you are using Partitioning, then the Switch and all the items associated with the Switch should be in the same partition. However, there is no check in the software to prevent a user from setting up partitions that are not practicable. For example, if a Switch is assigned to Partition A, Camera for the Car Park to Partition B and a Preset for the Camera is assigned to Partition A, then users logged on to Partition A would not see the Car Park Camera nor would they be able to run the Preset. You should also take care when assigning partitions as Public. You may prevent logged on users from accessing items, since a user can log on with one partition only.

User Roles – Create and assign user roles to perform CCTV Configuration and Control functions.

Event Actions – The equipment connected to the system is capable of responding to event actions launched from the P2000 software. For full details, refer to the appropriate sections later in this chapter and also to “Creating Actions” on page 208.

Audit Trail – Changes to the database are listed in the audit trail. You can use the standard P2000 Audit Trail report for details.

CCTV Configuration Overview

To operate your *Johnson Controls* CCTV System, the CCTV option must be set up and configured to communicate with system hardware. Configuration is typically performed by a System Engineer or System Administrator.

Although it is simple to use the CCTV option on a daily basis, the System Engineer will need some specific knowledge of the CCTV equipment to configure the hardware. The hardware is set up from the CCTV/AV Configuration window.

The CCTV system hardware includes the CCTV Server and Switches, Monitors, and Cameras.

The CCTV Server is OPC (OLE for Process Control) compliant. For further information relating to the OPC Interface Standard, see the OPC Foundation Interface Specification.

The CCTV Server and at least one Switch and the CCTV Protocol that it uses must be defined using the CCTV/AV Configuration window. The configuration of the Cameras and Monitors may be automatically generated or customized to your particular requirements. Other items that can be automatically set up or may need to be specifically configured are Alarms, Tours, Macros and System Auxiliaries, Sequences, Patterns, Presets, and Camera Auxiliaries.

Configuration should progress in a logical sequence. For example, you must configure the CCTV Server before you can configure any Switches. To customize the configuration of the Monitors and Cameras, you must first define the Switch to which they are attached. After the system is configured, you always have the option to return to a component and make changes if necessary.

TIP: It will be helpful to develop a Naming Plan to apply to Switches, Monitors, and Cameras before you begin programming the software. A fully developed plan can speed the configuration process by creating a quick reference to system component names.

Points to Note

- Changes to the configuration settings will not take effect until the CCTV service has been restarted. This means that if it is currently running, you will need to stop it and then start it.
- As long as you have the CCTV Server and one Switch configured, you can use the equipment using the default settings.
- For better operation you should define your equipment and give it meaningful names so that operators can quickly understand the system.
- You should be familiar with the individual manufacturer's equipment and how it operates.

Using the CCTV/AV Configuration Window

The CCTV/AV Configuration window provides quick access to all the component configurations. All “root” items in the CCTV/AV Configuration “tree” display on the left side of the window (windowpane). A + sign next to an item indicates that “branches” exist beneath them. When you select a branch in the tree, the detailed settings and values relating to that selection are listed on the right windowpane.

You can add as many items to the CCTV/AV Configuration window as you need. After items have been added, you can edit them as desired.

The CCTV/AV Configuration window is accessed from the P2000 Main menu. Select **Options>CCTV/AV>Configuration** from the P2000 Main menu bar and enter your password if prompted. The CCTV/AV Configuration window opens.

To Add an Item to the CCTV/AV Configuration Window:

1. From the “configuration tree,” click the “root” icon for the item you wish to add.
2. To access configuration dialog boxes, either click the **Add** button at the bottom of the window or right-click to access a shortcut menu and select **Add**. The appropriate dialog box opens.

3. After you have added the information according to the field definitions, click **OK** to return to the CCTV/AV Configuration window. When dialog boxes offer several configuration tabs, such as in the Edit CCTV Switch dialog box, configure each tab in turn, as applicable. You may not be able to access some tabs until a minimum of information has been entered into the tab that is displayed uppermost when the dialog box is opened.
4. When all settings have been entered, click **OK** to save your settings and return to the CCTV/AV Configuration window. The settings for the new item will be listed in the right windowpane.
5. Continue to add items in this manner until all items and their related controls have been configured.

To Edit CCTV/AV Configuration Items:

1. From the configuration tree, click the item you wish to edit and click the **Edit** button at the bottom of the window (or right-click the item and select **Edit** from the shortcut menu). The Edit dialog box opens.
2. After you have completed your changes, click **OK** to save the settings and return to the CCTV/AV Configuration window. The changes will be reflected in the right windowpane.

Note: Any changes will take effect only after the CCTV Server has been stopped and restarted using Service Control from the System Menu, see "Starting and Stopping Service Control" on page 315.

Defining System Hardware for the CCTV Option

Provided you have configured the CCTV Server and at least one Switch, and the Cameras and Monitors are connected to the configured addresses, you do not need to specifically configure any other equipment. The Switch configuration will contain the necessary global configuration information for all the Cameras and Monitors connected to it.

However, you may want to define specifically the operation of a piece of equipment. For example you may have one Camera that is fixed, so do not want to enable the move functions for the operator when running CCTV Control. In this case you would specifically set up and configure a named Camera. Any functions expressly defined for the named Camera will override the global Camera information in the Switch configuration.

Similarly, the Camera configuration will define global information about the Auxiliaries, Presets and Patterns for the Camera, including the number of these items that are to be generated

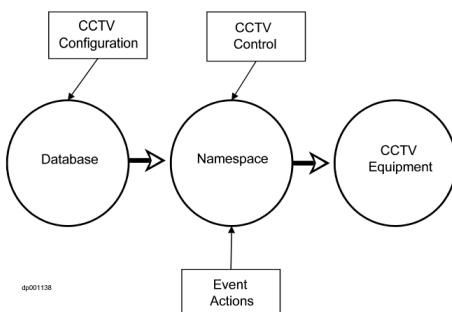
in the namespace. If the Camera definition generates 20 Patterns for example, then the 20 Patterns will exist in the namespace tagged with the namespace name. However, the user may wish to give a specific name to the Patterns, in which case each Pattern would need to be specifically set up and defined in the CCTV/AV Configuration window.

Namespace and Database

The software creates a database table and a valid entry for the Switch in the Server namespace. If the system then uses the default settings for the CCTV Switch Protocol, as many entries are added to the namespace as there are default items, but no database tables will be created for these items until one of the items has been specifically created, configured and saved. For example, if you specifically create a Tour, a record will be created and it will contain information about the named Tour. When you create the Tour, you will allocate the Tour a number, which the software will use to create the namespace name (OPC name) for the Tour. The namespace entry will be updated from any information in the database when the Server is next started.

Relationship Between the Namespace and Database

The following illustration summarizes how the various system activities relate to the namespace and database.



CCTV Naming Conventions

Where there is a large number of Cameras and Monitors in a CCTV system it would be helpful to name the components with a consistent naming scheme. For example, a Camera may be assigned a name that also includes the switch name (OfficeCam1), or it may be named with the location of the Camera (Floor 4), or the area of its view (West Car Park). These names are added to the CCTV database. Using sensible names will help new users of the system.

The CCTV Server namespace names are assigned automatically using the number assigned to the item when it is explicitly or automatically configured.

Naming Items for the CCTV Server Namespace

Each of the items that you define specifically in the CCTV/AV Configuration window is automatically allocated an identifying name that is recognized by the CCTV Server. The name comprises the number of the item and a fixed description. In the case of Cameras and Monitors the number is the physical address that the equipment is wired to at the Switch; in the case of the other Switch elements, the address is a logical address that can be recognized by the Server. The CCTV software assigns the fixed description automatically when the item number is added to the CCTV/AV Configuration window.

The item name is tagged automatically with the inherent names, so that a Pattern for example is recognized by its Switch, Camera and Pattern name. This means that for example Patterns that are created for different Cameras can have the same number but will have a different namespace name.

When you create records in the CCTV/AV Configuration window, you need to enter a

number for the address of the item that you are adding. Each number is prefixed by one or two letters. The following table shows the prefix letters and the range of numbers permitted for each item.

Name space Item	Parent Item	Prefix	Range
Switch	Server	S	1 to 9999
Alarm	Switch	Al	1 to 9999
Switch Auxiliary	Switch	Au	1 to 20000
Macro	Switch	Ma	1 to 9999
Tour	Switch	T	1 to 9999
Monitor	Switch	M	1 to 9999
Monitor Sequence	SwitchMonitor	Se	1 to 9999
Camera	Switch	C	1 to 9999
Camera Auxiliary	SwitchCamera	Au	1 to 8
Camera Presets	SwitchCamera	Pr	1 to 9999
Camera Patterns	SwitchCamera	Pa	1 to 9999

Note that the number of Monitors and Cameras is determined by the capacity of the Switch. The capacity of other items is determined by the hardware and the CCTV Switch Protocol.

Switches must be numbered consecutively starting from S0001.

The CCTV/AV Configuration window automatically inserts the prefix letters for the item. The user selects the number. For Cameras and Monitors this must be the hardware address at the Switch. There is no checking that the number is correct for the Camera or Monitor. Where a large number of Monitors and Cameras is installed it is recommended that the installing engineer develops a plan for the addressing process so that the correct numbers

can be entered into the CCTV/AV Configuration window.

It is always a good idea to connect Cameras and Monitors to the low numbered addresses at the Switch, to keep the number of CCTV Server namespace entries as small as possible.

Note that because the CCTV Server system uses intrinsic addressing, it is recommended that you do not change the address of the items once they have been configured. If you do, you may find that actions that use intrinsic addressing (for example, OPCWrite event actions) refer to a different item.

Also, to make it easier for the operator, when configuring the system, Switches numbered S0001 to S0006, Monitors numbered M0001 to M0020 and Cameras numbered C0001 to C0040 should be those that will be used most frequently so that the names (or numbers) display on the lists in the CCTV Control dialog box.

Defining the Number of Namespace Items

When you create and configure items for the CCTV Server, you need to give each item in the namespace a number. The range of numbers permitted is dependent on the number of items configured for the namespace.

A powerful feature of the CCTV Server software allows the namespace items to be configured automatically. You can decide whether the total number of items in the namespace is based on the default number of names defined by CCTV Switch Protocol or whether it is based on a specific user defined number.

This feature will be extremely valuable for setting up and commissioning the software initially, since you would need only to configure a Server and Switch with the CCTV Switch Protocol defaults, and provided the Cameras

and Monitors are physically connected to a valid address at the Switch, you would have a working system.

Number of Default Items Permitted

When a CCTV Server and a Switch are configured, database entries are created for each item. It is not necessary to create named records for the items that belong to a Switch. If you create and configure a CCTV Server and Switch and no other item, the system will use the system default number of namespace items as the maximum number of items that can be addressed by the CCTV Server. The default values are protocol specific; refer to *Appendix D: CCTV Switch Protocols*.

You may wish to keep the maximum number of items as the default values, however, if you use fewer or more items of equipment you may wish to change the number of items that are allowed.

Note that if you use the system default values for the number of Switch items, no records or database entries are created; the system works from the namespace entries that are automatically created.

Changing the Number of Namespace Items

The default number of Cameras is 64 but your system may use only 25; there will be 39 redundant entries in the namespace. In such a case, it would be advisable to specifically define the number of entries that you want to generate in the namespace. You would change the number of items from the Edit CCTV Switch window by entering the number of items that you want to generate. In this example you would enter 25. This would generate 25 entries numbered from 1 to 25. You would then need to ensure that each Camera is connected to a physical address between 1 and 25.

The number of namespace items generated may be changed at any time but the CCTV Server will need to be stopped and restarted for the changes to be effective.

You should note that the system defaults are not necessarily the maximum capacity for the particular CCTV Switch Protocol. If the number of Cameras to be used is 150, you would configure the Switch to cope with 150 Cameras.

If you select the number of Cameras to be 150, for example, and you specifically define a Camera as number 135, it implies that it is physically connected to address 135 at the Switch. If later you attempt to reduce the number of namespace entries to fewer than 135 you will not be allowed to make the change provided a Camera number 135 is still defined. In this case, the number of namespace entries would be the number of the highest defined Camera.

Switch Protocols

The CCTV Switch Protocol is the protocol that is defined by the manufacturer of the Switch. Each Switch can be associated with one Protocol only, but the system can support Switches using different protocols.

It is also possible to define a Switch that uses a General ASCII protocol. This means in effect that the Switch is a message-handling device. To define a Switch as General ASCII you would enter the item number and then enter the protocol as General ASCII.

Tristate Check Boxes

Tristate check boxes allow the following choices:

Ticked	This option will be available at the control application
Not ticked	This option will not be available at the control application
Gray ticked	The control options will default to the manufacturer's controls

It would be normal to set the functions to manufacturer's defaults (gray tick).

Any selection made for specific Cameras and Monitors, that is those that have been created in the CCTV/AV Configuration window, will override the selections of controls at Switch level.

You should note that the software does not check to see if the equipment can handle the selected functions. When CCTV Control is running the control dialog box may display capabilities that the equipment is unable to perform. For example, if the Camera is a fixed Camera and the configuration setup requested all functions (all check boxes ticked), then the operator would in theory be able to operate the pan, tilt, zoom etc. options. However, of course in reality there would be no Camera movement.

CCTV Option Components

Components that operate within the CCTV option include Servers, Switches, Monitors and Cameras. To speed the configuration process, we recommend that you set up system components in the following order:

CCTV Server – CCTV Server defines information about the CCTV Server for the CCTV option. The CCTV Server namespace is initialized from the P2000 database each time that the CCTV Server is started. If the CCTV

Server cannot find the P2000 database, then the namespace is initialized from a local copy. However, the local copy will have been made when the P2000 database was last read, so may not be up-to-date.

Switches – Switches define general system information about the Switch and about the global information for Alarms, Auxiliaries, Macros, Tours, Monitors and Cameras that are connected to the Switch. The Switch also determines how the CCTV Server namespace for this Switch is to be generated. You must define at least one Switch for each configured CCTV Server, but you can install more than one Switch for each CCTV Server.

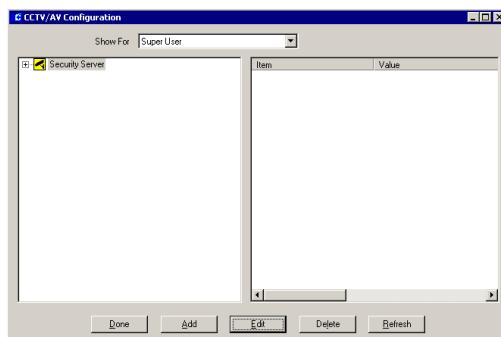
Monitors – You may specifically define the Monitors that you will use on your system and the Sequences that can be played for each Monitor.

Cameras – You may specifically define the Cameras that you will use on your system and the controls that will be available for this Camera, the Presets, Patterns and Auxiliaries that can be played for each Camera.

The following sections give details about how to configure and control the CCTV equipment.

To Configure the CCTV Option:

- From the P2000 Main menu, select **Options>CCTV/AV>Configuration**. The CCTV/AV Configuration opens.



For any CCTV configuration changes to take effect, the CCTV Server must be stopped and restarted. This should be done on the completion of your configuration session.

When you configure the system for the first time (only), the CCTV/AV Configuration window will display the Server icon. To add a Server, select the displayed icon and click **Add**. Define and save the Server information. The new Server icon will display.

The following setup and configuration sequence is recommended:

- Add a Server
- Create and Configure Switches
- Create and Configure Monitors
- Create and Configure Cameras

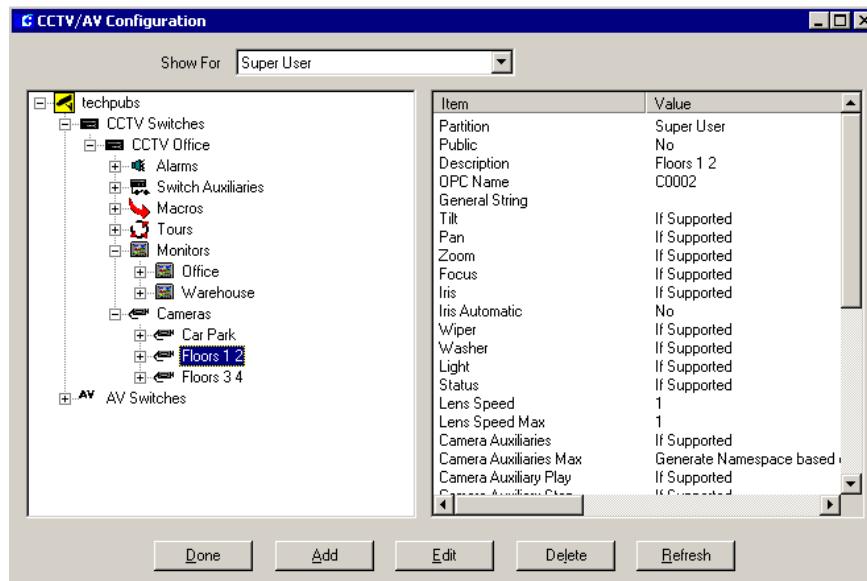
If you have not already developed naming conventions for these program elements, it will be helpful to do so before beginning this procedure. Refer to “CCTV Naming Conventions” on page 260 for more information.

A fully configured system will display the configured items in the left pane and information about the item in focus in the right pane.

CCTV Server

Create and Configure the CCTV Server

The CCTV Server will create and maintain (in RAM) a namespace, which is made available to all CCTV Controls and other OPC Clients. The namespace contains abstract descriptions of the equipment controlled by the Server. CCTV Controls query the namespace to find out what and how much equipment is available. To send commands to specific items of equipment, values are written to specific

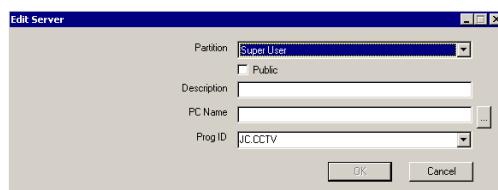


namespace positions and the Server will interpret and action these commands accordingly based on the information it has about the various manufacturers' equipment.

The CCTV Server installed in your system must be set up and configured in the CCTV/AV Configuration window to establish communication and control. The CCTV/AV Configuration window displays the Server at the highest level.

To Add a Server:

- From the CCTV/AV Configuration window, select the **Server** icon and click **Add**. The Edit Server dialog box opens.



- Fill in the information for each field according to the following "Edit Server Field Definitions".
- Click **OK** to save the new Server information.

Edit Server Field Definitions

Partition – If partitioning is available, select the Partition that will have access to this Server information.

Public – If partitioning is available, select the Public check box to allow all partitions to see this Server.

Description – This is a user defined description of up to 30 characters to describe the Server.

PC Name – Enter the name of the PC on which the Server resides. This will be the name of the P2000 Server on which you are operating.

Prog ID – An installed Server is associated with a Program ID. Select the Program ID for the

Server. The default Program ID for the Server is JC.CCTV. Sub versions may be released from time to time (numbered consecutively starting with JC.CCTV1), but using JC.CCTV ensures that you use the latest version.

Switches

A Switch is a piece of equipment that receives video inputs from Cameras and outputs the data to video outputs such as Monitors. Each Switch will operate using the manufacturer's CCTV Switch Protocol; the functionality of the Switch will largely be determined by the Protocol provided and the capacity of the equipment connected to the Switch.

Some manufacturers refer to a Matrix, which is sometimes combined with a CPU. This is considered to be a Switch.

Optionally it is possible to define a general purpose Switch that uses a General ASCII Protocol.

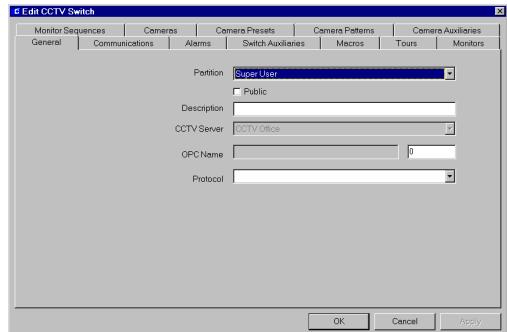
Create and Configure Switches

A Switch is connected to a PC and the PC must have the CCTV Server running on it. The Switch will have a variety of equipment connected to it, including Cameras, Monitors and Auxiliaries. Equipment connected to a Switch is presumed to be compatible with the Switch. A Server system may include a number of separately connected Switches and each may use a different Protocol.

Each Switch installed in your system must be set up and configured in the CCTV/AV Configuration window to establish communication and control. CCTV configuration displays the Server at the highest level. Click the Server icon to display the CCTV Switches icon.

To Add CCTV Switch Definitions:

- From the CCTV/AV Configuration window, select the root **CCTV Switches** icon and click **Add**. The Edit CCTV Switch dialog box opens at the General tab.



- Fill in the information for each field in each of the tabs. (See "Edit CCTV Switch Field Definitions" for details.)
- As you work through the tabs, you may click **Apply** to save your entries.
- Click **OK** to save your entries.

When a new Switch is created, the new Switch icon is listed under the root CCTV Switches icon in the CCTV/AV Configuration window, and icons for all Switch components are listed under the new Switch.

Edit CCTV Switch Field Definitions

The Edit CCTV Switch dialog box opens at the General tab. You must enter information in all Edit CCTV Switch tabs to complete your configuration of the Switch.

The General and Communications tabs give information about how the Switch is defined. The other tabs give information about the other elements of the CCTV system that will be available to the operator.

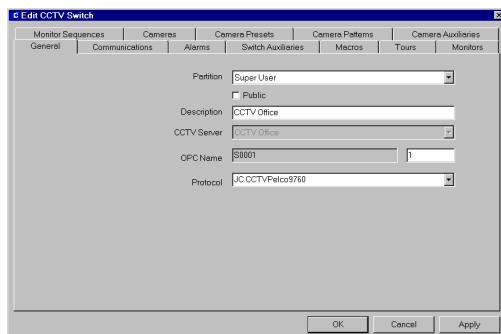
However, you should note that even if you enable a function, if that function is not available for the particular protocol then the operator's action will have no effect. The system does not check whether the functions selected at the Switch are compatible with the functionality of the equipment.

You should also note that if you set up global items under the Switch and then create a specific CCTV item (for example a Camera) then the settings defined for the individual item override the global Switch settings.

You will need to configure global information about the following components:

- General Tab
- Communications Tab
- Alarms Tab
- Switch Auxiliaries Tab
- Macros Tab
- Tours Tab
- Monitors Tab
- Monitor Sequences Tab
- Cameras Tab
- Camera Presets Tab
- Camera Patterns Tab
- Camera Auxiliaries Tab

Switch General Tab



Partition – If partitioning is available, select the Partition that will have access to this Switch information.

Public – If partitioning is available, select the Public check box to allow all partitions to see this Switch.

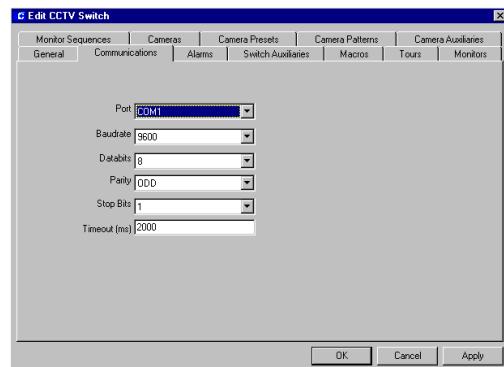
Description – This is the user defined name of the Switch. The name will display in the CCTV Control window.

CCTV Server – This is the name of the Server that resides on the PC that the Switch is physically connected to. The software automatically enters this name.

OPC Name – Enter the number of the item. The number is automatically appended to the prefix letter and added to the OPC Name field. For further information about namespace names and item numbers, see “Naming Items for the CCTV Server Namespace” on page 260.

Protocol – This is the CCTV Switch Protocol for this make and model of Switch. For information about the Protocol see “Switch Protocols” on page 262 and *Appendix D: CCTV Switch Protocols*.

CCTV Switch Communications Tab



The manufacturer of the Switch will specify the information entered into the Communica-

tions tab You should refer to the manufacturer's documentation.

Port – This is the COM port that the Switch is physically connected to. Note that the software will check with the Server to establish whether there is a clash in port usage but will not check with any other equipment that may be running.

Baud – This is the Baud for the Switch communications.

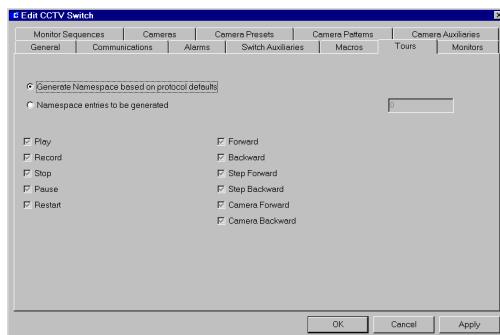
Databits – This is the number of Databits for the Switch communications.

Parity – This is the Parity for the Switch communications.

Stop Bits – This is the number of Stop Bits for the Switch communications.

Timeout (ms) – This is the period (in milliseconds) by which the CCTV matrix should have responded. Default for all switches is 2000 ms.

All Other CCTV Switch Tabs



Generate namespace based on protocol defaults

defaults – The CCTV Server software provides default values for the maximum number of items that will be generated in the namespace. To generate the default value for an item, select this radio button from the appropriate tab. For example, where the default number of Monitors is to be generated, open the Monitors

tab and select this radio button. See also “Number of Default Items Permitted” on page 261.

Namespace entries to be generated – The user can select the number of entries that are to be generated in the namespace. Select this radio button and enter the number of items to be generated in the namespace. See also “Defining the Number of Namespace Items” on page 261.

Each tab will display the functions appropriate for the item. The associated check boxes are tristate boxes and would normally be gray ticked which is the default setting (refer to page 262 for further information). The functions available are from the following:

Play – If available, tick the check box to enable Play for the items controlled by this Switch.

Record – If available, tick the check box to enable Record for the items controlled by this Switch.

Stop – If available, tick the check box to enable Stop for the items controlled by this Switch.

Pause – If available, tick the check box to enable Pause for the items controlled by this Switch.

Restart – If available, tick the check box to enable Restart for the items controlled by this Switch.

Forward – If available, tick the check box to enable Forward for the items controlled by this Switch.

Backward – If available, tick the check box to enable Backward for the items controlled by this Switch.

Step Forward – If available, tick the check box to enable Step Forward for the items controlled by this Switch.

Step Backward – If available, tick the check box to enable Step Backward for the items controlled by this Switch.

Camera Forward – If available, tick the check box to enable Camera Forward for the items controlled by this Switch.

Camera Backward – If available, tick the check box to enable Camera Backward for the items controlled by this Switch.

Alarms, Auxiliaries, Macros and Tours

Numbered Alarms, Auxiliaries, Macros and Tours will automatically be defined as part of the Switch definition; specifically named Alarms, Auxiliaries, Macros or Tours can be defined in the CCTV/AV Configuration window. If the item is a named item, the name will display in the CCTV Control window. Named and numbered items can be used from the CCTV Control window provided the equipment is available and is able to perform the required functions.

If the item is an Alarm, when it is played from the CCTV Control window the Alarm will be set or reset.

Alarms

A Switch may provide alarms that can be set and reset. In such cases an Alarm can be used to start a Macro or Tour associated with the same Switch.

Auxiliaries

Switches may provide relays that can be addressed to provide output control functions.

Macros

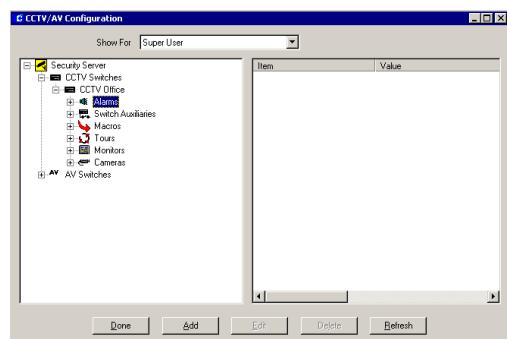
Macros are programmed sets of steps that are to be performed. The program steps can include any function provided by the associated Switch.

Tours

A Tour is a programmed set of Camera, Monitor and Preset movements. The functionality of the Tour will depend on the capability of the equipment connected to the Switch.

To Add an Alarm, Auxiliary, Macro or Tour:

- From the CCTV/AV Configuration window, click the plus (+) sign next to the **Server** icon.
- Click the plus (+) sign next to the **CCTV Switches** icon.



- Click the appropriate icon (**Alarms, Auxiliaries, Macros or Tours**) and click **Add**. The appropriate Edit CCTV dialog box opens.



4. Fill in the information for each field according to the “Edit CCTV Alarm, Auxiliary, Macro and Tour Field Definitions”.
5. Click **OK** to save the new information.

Edit CCTV Alarm, Auxiliary, Macro and Tour Field Definitions

Partition – If partitioning is available, select the Partition that will have access to this information.

Public – If partitioning is available, select the Public check box to allow all partitions to see this item.

Description – This is the user defined name of the Switch item. The name will display in the CCTV Control window.

CCTV Switch – This is the name of the Switch that the item is connected to. The Switch name is automatically entered into this field.

OPC Name – Enter the number of the item. The number is automatically appended to the prefix letter and added to the OPC Name field. For further information about namespace names and item numbers, see “Naming Items for the CCTV Server Namespace” on page 260.

Monitors

Create and Configure Monitors

A Switch will have a variety of equipment physically connected to it, including Cameras, Monitors and Auxiliaries.

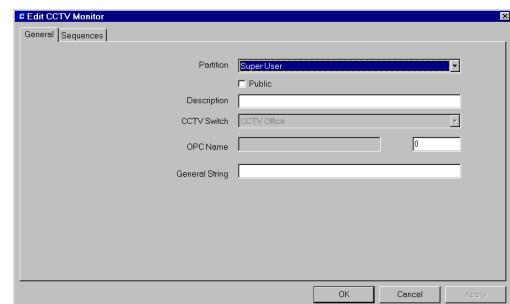
The Monitors connected to the Switch need not be expressly defined. The Switch can implicitly define a number of Monitors that will be added to the CCTV Server namespace automatically. Any Monitor connected to the Switch will be recognized by its physical

address. The global functions selected in the Monitor tab in the Switch definition will apply to each Monitor connected to the Switch, although the Monitor may not be capable of responding.

For commissioning and testing, there would be no need to explicitly define individual Monitors, in practice there are good reasons for doing so; in particular it will simplify the day to day operation of the system for new users. Therefore, it is recommended that when the system is proven to perform correctly, then the Monitors to be used are defined as named Monitors. Refer to “CCTV Naming Conventions” on page 260 for more information.

To Add a Named Monitor:

1. From the CCTV/AV Configuration window, click the **CCTV Switch** icon that the Monitor is associated with. Click the + to open the items for the Switch.
2. Click the **Monitor** icon and click **Add**. The Edit CCTV Monitor dialog box opens.



3. Fill in the information for each field in each of the tabs according to the following field definitions.
4. As you work through the tabs, you may click **Apply** to save your entries.
5. Click **OK** to save your entries.

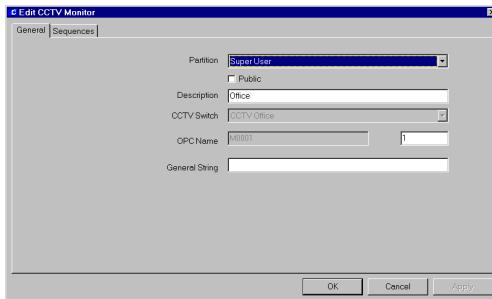
Edit CCTV Monitor Tabs

The Edit CCTV Monitor dialog box opens at the General tab. You must enter information in all Edit CCTV Monitor tabs to complete configuration.

- General Tab
- Sequences Tab

The General tab gives information about how the Monitor is defined. The Sequences tab gives information about the Sequence functions that are to be available to the operator from CCTV Control. These definitions will override the global settings in the Switch dialog box.

Monitor General Tab



Partition – If partitioning is available, select the Partition that will have access to this Monitor information.

Public – If partitioning is available, select the Public check box to allow all partitions to see this Monitor.

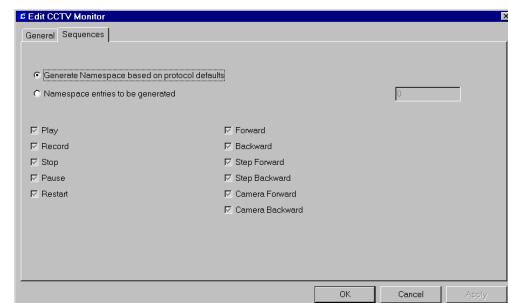
Description – This is the user defined name of the Monitor. The name will display in the CCTV Control window.

CCTV Switch – This is the name of the Switch that the Monitor is physically connected to. The Switch name is automatically entered into this field.

OPC Name – Enter the number of the Monitor. The number is automatically appended to the prefix letter and added to the OPC Name field. For further information about namespace names and item numbers, see “Naming Items for the CCTV Server Namespace” on page 260.

General String – This is any user string that will display when CCTV Control is running.

Monitor Sequences Tab



Generate namespace based on protocol defaults

defaults – The CCTV Server software provides default values for the maximum number of items that will be generated in the namespace. To generate the default value for an item, select this radio button from the appropriate tab. For example, where the default number of Sequences is to be generated, open the Sequences tab and select this radio button. See also “Number of Default Items Permitted” on page 261.

Namespace entries to be generated – The user can select the number of entries that are to be generated in the namespace. Select this radio button and enter the number of items to be generated in the namespace. See also “Defining the Number of Namespace Items” on page 261.

Select the functions that will be available for Sequences that are controlled by this Monitor.

The associated check boxes are tristate boxes and would normally be gray ticked. The functions available are from the following:

Play – If available, tick the check box to enable Play for Sequences controlled by this Monitor.

Record – If available, tick the check box to enable Record for Sequences controlled by this Monitor.

Stop – If available, tick the check box to enable Stop for Sequences controlled by this Monitor.

Pause – If available, tick the check box to enable Pause for Sequences controlled by this Monitor.

Restart – If available, tick the check box to enable Restart for Sequences controlled by this Monitor.

Forward – If available, tick the check box to enable Forward for Sequences controlled by this Monitor.

Backward – If available, tick the check box to enable Backward for Sequences controlled by this Monitor.

Step Forward – If available, tick the check box to enable Step Forward for Sequences controlled by this Monitor.

Step Backward – If available, tick the check box to enable Step Backward for Sequences controlled by this Monitor.

Camera Forward – If available, tick the check box to enable Camera Forward for Sequences controlled by this Monitor.

Camera Backward – If available, tick the check box to enable Camera Backward for Sequences controlled by this Monitor.

Sequences

A Sequence is similar to a Tour except that it applies to a single Monitor. A Sequence is a set of programmed Camera, Monitor and Preset movements.

A Sequence is defined in the CCTV/AV Configuration window, either by default from the Switch or Monitor or by being specifically named. The Sequence is played from the CCTV Control window.

A numbered Sequence will be defined as part of the Switch or Monitor definition; a specifically named Sequence can be defined in the CCTV/AV Configuration window. If the Sequence is a named item, the name will display in the CCTV Control window. Named and numbered Sequences can be used from the CCTV Control window provided the equipment is available and is able to perform the required functions.

To Add a Named Monitor Sequence:

- From the CCTV/AV Configuration window, click the **CCTV Switch** icon that the Monitor is associated with. Click the + to open the items for the Switch.
- Click the + to open the items for the Monitor.
- Click the **Sequence** icon and click **Add**. The Edit CCTV Sequence dialog box opens.



- Fill in the information for each field according to the "Edit CCTV Sequence Field Definitions".

- Click **OK** to save your entries.

Edit CCTV Sequence Field Definitions

Partition – If partitioning is available, select the Partition that will have access to this Sequence information.

Public - If partitioning is available, select the Public check box to allow all partitions to see this Sequence.

Description – This is the user defined name of the Monitor Sequence. The name will display in the CCTV Control window.

CCTV Monitor – This is the name of the Monitor that the Sequence is connected to. The Monitor name is automatically entered into this field.

OPC Name – Enter the number of the Sequence. The number is automatically appended to the prefix letter and added to the OPC Name field. For further information about namespace names and item numbers, see “Naming Items for the CCTV Server Namespace” on page 260.

Cameras

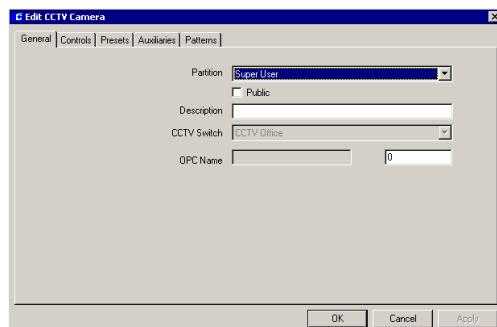
Create and Configure Cameras

A Switch will have a variety of equipment physically connected to it, including Cameras, Monitors and Auxiliaries. The Cameras connected to the Switch need not be expressly defined. The Switch can implicitly define a number of Cameras that will be added to the CCTV Server namespace automatically. Any Camera connected to the Switch will be recognized by its physical address. The global functions selected in the Camera tab in the Switch definition will apply to each Camera connected to the Switch, although the Camera may not be capable of responding.

Although for commissioning and testing, there would be no need to explicitly define individual Cameras, in practice there are good reasons for doing so. Therefore, it is recommended that when the system is proven to perform correctly, then the Cameras to be used are defined as named Cameras. Refer to “CCTV Naming Conventions” on page 260 for more information.

To Add a Named Camera:

- From the CCTV/AV Configuration window, click the **CCTV Switch** icon that the Camera is associated with. Click the + to open the items for the Switch.
- Click the **Camera** icon and click **Add**. The Edit CCTV Camera dialog box opens.



- Fill in the information for each field according to the following field definitions.
- As you work through the tabs, you may click **Apply** to save your entries.
- Click **OK** to save your entries.

Edit CCTV Camera Tabs

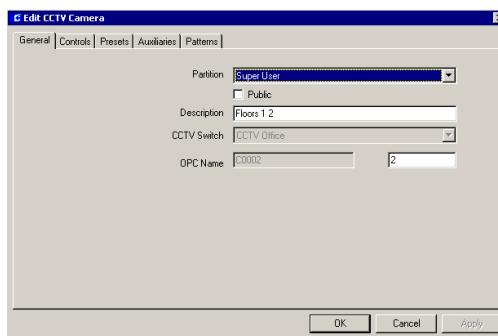
The Edit CCTV Camera dialog box opens at the General tab. You must enter information in all Edit CCTV Camera tabs to complete configuration.

- General Tab
- Controls Tab

- Presets Tab
- Auxiliaries Tab
- Patterns Tab

The General and Controls tabs give information about how the Camera is defined. The other tabs give information about the elements of this particular Camera that are to be available to the operator. These definitions will override the global settings in the CCTV Switch dialog box.

Camera General Tab



Partition – If partitioning is available, select the Partition that will have access to this Camera information.

Public – If partitioning is available, select the Public check box to allow all partitions to see this Camera.

Description – This is the user defined name of the Camera. The name will display in the CCTV Control window.

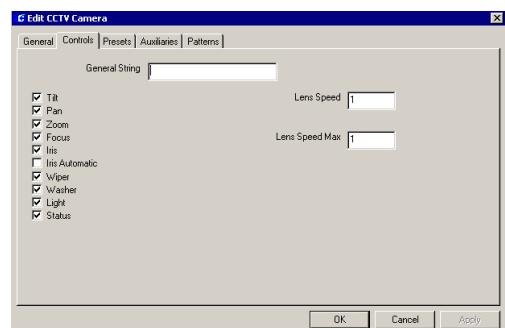
CCTV Switch – This is the name of the Switch that the Camera is physically connected to. The Switch name is automatically entered into this field.

OPC Name – Enter the number of the Camera. The number is automatically appended to the prefix letter and added to the OPC Name field. For further information about namespace names and item numbers, see “Naming Items

for the CCTV Server Namespace” on page 260.

Camera Controls Tab

If the majority of your Cameras are of one type (fixed for example), it would be advisable to select the Camera functions that apply to the majority (for example leave the moving functions, Pan/Tilt etc., unselected). You would then be able to specifically configure those Cameras that have different capabilities.



General String – This is up to 50 characters that may display at the Monitor when the Camera is operating from the CCTV Control window provided the protocol allows it. It could be the name of the Camera or a description of the location of the Camera. This is an optional field.

Note that the following check boxes are tristate boxes.

Tilt – If available, tick the check box to enable Tilt for this Camera.

Pan – If available, tick the check box to enable Pan for this Camera.

Zoom – If available, tick the check box to enable Zoom for this Camera.

Focus – If available, tick the check box to enable Focus for this Camera.

The following check boxes are two state check boxes:

Iris – If available, tick the check box to enable Iris for this Camera.

Iris Automatic – If available, tick the check box to enable Iris Automatic for this Camera.

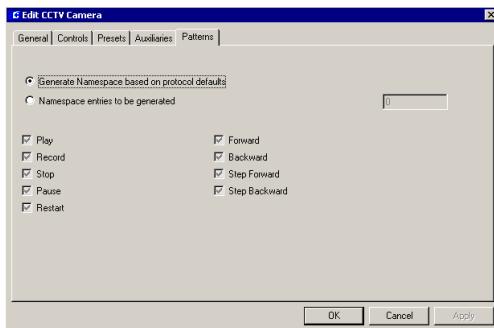
Wiper – If available, tick the check box to enable Wiper for this Camera.

Washer – If available, tick the check box to enable Washer for this Camera.

Light – If available, tick the check box to enable Light for this Camera.

Status – If available, tick the check box to enable Status for this Camera.

Camera Presets, Auxiliaries, and Patterns Tabs



Generate namespace based on protocol defaults

defaults – The CCTV Server software provides default values for the maximum number of items that will be generated in the namespace. To generate the default value for an item, select this radio button from the appropriate tab. For example, where the default number of Patterns is to be generated, open the Patterns tab and select this radio button. See also “Number of Default Items Permitted” on page 261.

Namespace entries to be generated – The user can select the number of entries that are to be generated in the namespace. Select this radio button and enter the number of items to be generated in the namespace. See also “Defining the Number of Namespace Items” on page 261.

Select the functions that will be available for Presets, Auxiliaries, and Patterns that are controlled by this Camera. Note that the check boxes are tristate boxes.

Play – If available, tick the check box to enable Play for the items controlled by this Camera.

Record – If available, tick the check box to enable Record for the items controlled by this Camera.

Stop – If available, tick the check box to enable Stop for the item controlled by this Camera.

Pause – If available, tick the check box to enable Pause for the item controlled by this Camera.

Restart – If available, tick the check box to enable Restart for the item controlled by this Camera.

Forward – If available, tick the check box to enable Forward for the items controlled by this Camera.

Backward – If available, tick the check box to enable Backward for the items controlled by this Camera.

Step Forward – If available, tick the check box to enable Step Forward for the items controlled by this Camera.

Step Backward – If available, tick the check box to enable Step Backward for the items controlled by this Camera.

Camera Auxiliaries, Patterns and Presets

Numbered Camera Auxiliaries, Patterns and Presets will be defined as part of the Switch or Camera definition; specifically named Camera Auxiliaries, Patterns and Presets can be defined in the CCTV/AV Configuration window. If the item is a named item, the name will display in the CCTV Control window. Named and numbered Camera Auxiliaries, Patterns and Presets can be used from the CCTV Control window provided the equipment is available and is able to perform the required functions.

Camera Auxiliaries

Cameras may provide relays that can be addressed to provide output control functions. Camera Auxiliaries perform according to the capability of the hardware and the Switch CCTV Protocol.

Patterns

A Pattern is user defined viewable Camera path with a beginning and an end. According to the capability of the hardware and the Switch CCTV Protocol, a Pattern may be required to complete within a specified time.

Presets

A preset camera position is a user defined position which may include pan, tilt, zoom and focus adjustments.

To Add a Named Camera Item:

- From the CCTV/AV Configuration window, click the **CCTV Switch** icon that the Camera is associated with. Click the + to open the items for the Switch.

- Click the + to open the items for the **Camera**.

- Click the appropriate icon (Auxiliary, Pattern or Preset) and click **Add**. The appropriate **Edit CCTV** dialog box opens.



- Fill in the information for each field according to the following field definitions.
- Click **OK** to save your entries.

Edit CCTV Named Camera Item Field Definitions

Partition – If partitioning is available, select the Partition that will have access to this Camera item information.

Public – If partitioning is available, select the Public check box to allow all partitions to see this item.

Description – This is the user defined name of the Camera item. The name will display in the CCTV Control window.

CCTV Camera – This is the name of the Camera that the item is connected to. The Camera name is automatically entered into this field.

OPC Name – Enter the number of the item. The number is automatically appended to the prefix letter and added to the OPC Name field. For further information about namespace names and item numbers, see “Naming Items for the CCTV Server Namespace” on page 260.

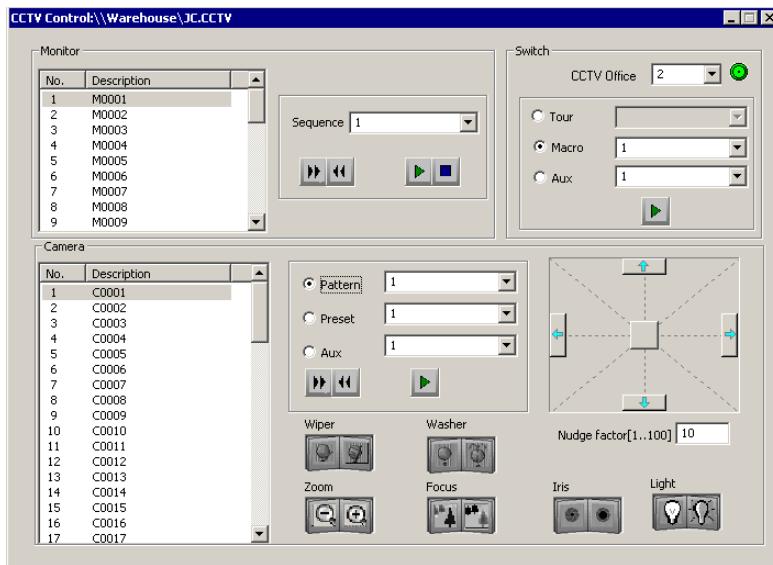
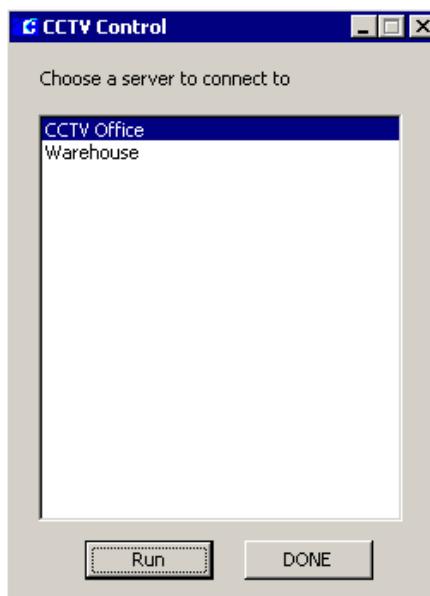
CCTV Control

The CCTV Control software is part of the CCTV Server system. It provides controls to operate the Cameras and Monitors that are part of the CCTV system. In addition, it also provides the controls to select and use Alarms, Macros, Auxiliaries and Tours from the Switches, Sequences from the Monitors and Patterns, Presets and Auxiliaries from the Cameras.

To run the control software, the user needs to select a CCTV Server. The Server to select will depend on the configuration of your system and the number of Servers that are installed.

To Run CCTV Control:

1. From the P2000 Main menu, select **Options>CCTV/AV>Control**. The CCTV Control selection dialog box opens. If you have only one server, this dialog box will display minimized and the CCTV Control window for that server will open automatically.
2. If you have multiple servers, select a server from the list and click **Run**. The CCTV Control window opens displaying the name of the server you are connected to in the title bar.



CCTV Standard Controls

Selecting the Item to Control

The Switch is selected from a drop-down list or by directly entering the switch number. Monitors and Cameras are selected by clicking the item from their respective list boxes.

The items displayed in the CCTV Control window will depend on the configuration of your system. If the equipment is configured and named, the name will display on the lists, otherwise the namespace name will display.

Other items (such as Camera Patterns or Switch Tours) are selected from drop-down lists or by directly entering the item number.

Operating the Controls

You can perform CCTV functions from the P2000 PC or a workstation using the CCTV Control window. Switch Tours, Macros and Auxiliaries; Monitor Sequences; and Camera Patterns, Presets and Auxiliaries that have been configured can be activated and controlled from this window.

You should note that if the CCTV equipment is capable of operating from its own control device (a keyboard for example), then that control device would need to release control to operate the equipment from the P2000 CCTV Control. Similarly, CCTV Control would need to release control in order for the device to function correctly.

The following control buttons may be available depending on the availability of the functions for the selected equipment:



Step Backward



Step Forward



Restart



Pause



Play



Stop



Record

In addition the following Camera controls may be available:



Wiper



Washer



Light



Zoom



Focus

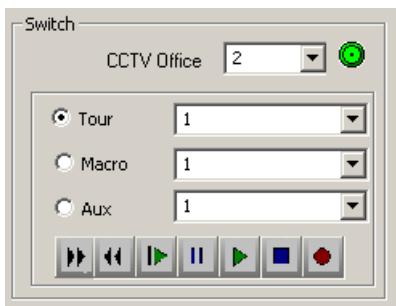


Iris

Using Switch Controls

The Switch box provides the controls that allow you to select a Switch and select and use Tours, Macros and Switch Auxiliary functions for the selected Switch if they are available. A Tour is a programmed set of Camera, Monitor

and Preset selections. Macros are programmed sets of steps that are to be performed. The program steps can include any function provided by the associated Switch. Switch Auxiliaries can be activated using the control buttons in the Switch box.



Selecting a Switch

Only switches that are configured for the selected CCTV Server are displayed in the Switch drop-down list. A switch is selected either from the drop-down list or by entering the switch number in the Switch field.

If a switch button is red the switch has communication problems. The associated error message will display below the Camera list box.

Selecting a Tour, Macro or Switch Auxiliary

A Tour, Macro or Switch Auxiliary is selected either from the associated drop-down list or by entering the item number in the respective field.

Using Tour, Macro or Switch Auxiliary Controls

The precise functions of the Tour, Macro and Switch Auxiliary controls will depend on the Protocol for the associated Switch and their application by the CCTV Server system. The controls that may be available are as follows:

Step Backward – The Tour will move back to the previous Camera, or if the Tour is playing forward, will reverse the sequence of operation.

Step Forward – The Tour will move forward to the next Camera, or if the Tour is playing backward, will reverse the sequence of operation.

Restart – If the function has been stopped, the restart button will start the selected Tour or Macro from the beginning.

Pause – This will stop the selected Tour or Macro running but allow you to continue playing from the point at which the Tour or Macro stopped.

Play – This will activate the selected Tour, Macro or Switch Auxiliary.

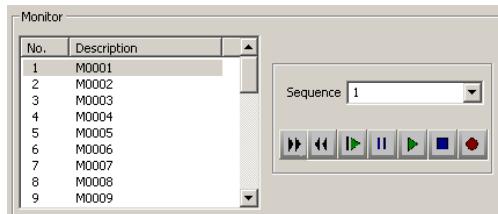
Stop – This will stop the selected Tour, Macro or Switch Auxiliary. With some equipment the stop button may also stop recording a Tour or Macro.

Record – You record Tours and Macros by clicking the record button and then playing the required sequence of activities. The sequence of activities is dependent on the functions available for the protocol and the equipment installed. Stopping recording will also depend on the protocol but recording will probably stop if you click either the record button again or the stop button. You should consult the manuals supplied with the CCTV equipment for your site for full details.

Note that Tours, Macros and Sequences for some manufacturers can only be recorded using their proprietary setup methods. However, they can still be played using the play control described here.

Using the Monitor Controls

The Monitor list box allows you to select a Monitor and select and use Sequence functions for the selected Monitor if they are available.



Selecting a Monitor

The number of monitors displayed in the Monitor list box depends on the configuration of your system. If the monitor is configured and named, the name will display on the list, otherwise the namespace name will display. Click the monitor name to select the monitor you wish to control.

Selecting a Sequence

A sequence is selected either from the Sequence drop-down list or by entering the number in the Sequence field.

Using Sequence Controls

The precise functions of the Sequence controls will depend on the Protocol for the associated Switch and their application by the CCTV Server system. The controls that may be available, depending on the selected Switch, are as follows:

Step Backward – The Sequence will move back to the previous Camera, or if the Sequence is playing forward, will reverse the sequence of operation.

Step Forward – The Sequence will move forward to the next Camera, or if the Sequence is

playing backward, will reverse the sequence of operation.

Restart – If the function has been stopped, the restart button will start the selected Sequence from the beginning.

Pause – This will stop the selected Sequence running but allow you to continue playing from the point at which the Sequence stopped.

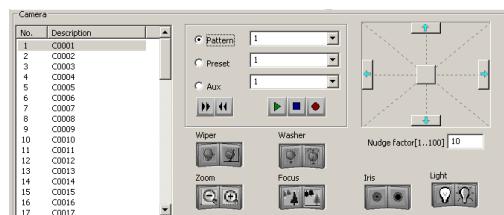
Play – This will activate the selected Sequence.

Stop – This will stop the selected Sequence. With some equipment the stop button may also stop recording a Sequence.

Record – You record a Sequence by clicking the record button and then playing the required sequence of activities. The sequence of activities is dependent on the functions available for the protocol and the equipment installed. Stopping recording will also depend on the protocol but recording will probably stop if you click either the record button again or the stop button. You should consult the manuals supplied with the CCTV equipment for your site for full details.

Using the Camera Controls

The Camera list box allows you to select a Camera and select and use Patterns, Presets and Camera Auxiliary functions for the selected Camera if they are available.



Selecting a Camera

The number of cameras displayed in the Camera list box depends on the configuration of your system. If the camera is configured and named, the name will display on the list, otherwise the namespace name will display. Click the camera name to select the camera you wish to control.

Selecting a Pattern, Preset or Camera Auxiliary

A Pattern, Preset or Camera Auxiliary is selected either from the associated drop-down list or by entering the item number in the respective field.

Using Pattern, Preset or Camera Auxiliary Controls

The precise functions of the controls will depend on the Protocol for the associated Switch and their application by the CCTV Server system. The controls that may be available, depending on the selected Switch, are as follows:

Step Backward – The Pattern will move back to the last Camera, or if the Pattern is playing forward, will reverse the sequence of operation.

Step Forward – The Pattern will move forward to the next Camera, or if the Pattern is playing backward, will reverse the sequence of operation.

Play – This will activate the selected Pattern, Preset or Camera Auxiliary.

Stop – This will stop the selected Pattern or Camera Auxiliary. With some equipment the stop button may also stop recording a Pattern.

Record – You record a Pattern or Preset by clicking the record button and then playing the required sequence of activities. The sequence

of activities is dependent on the functions available for the protocol and the equipment installed. Stopping recording will also depend on the protocol but recording will probably stop if you click either the record button again or the stop button. You should consult the manuals supplied with the CCTV equipment for your site for full details.

Pan/Tilt – Click and hold down the mouse on the movement control square in the Pan/Tilt area to move the selected Camera. The movement control returns to the center of the Pan/Tilt area when at rest. The position of the Camera is as is and not centered. To Pan the Camera you move the movement control along the horizontal; to tilt the Camera you move the Camera along the vertical. Movements between the horizontal and vertical are proportional. The further from the center, the faster the movement.

The selected Camera can also be moved using the nudge arrows on each side of the Pan/Tilt area. The Camera will be moved at a speed defined by the nudge factor. The nudge factor is a value in the range 1 to 100 which determines the speed of the Camera movements. The larger the number, the faster the Camera movements.

Wiper – There are two wiper buttons. The left button switches off the Camera wiper; the right button switches on the Camera wiper.

Washer – There are two washer buttons. The left button switches off the Camera washer; the right button switches on the Camera washer.

Zoom – There are two Zoom buttons. The left button zooms out from the object; the right button zooms in on the object.

Focus – There are two Focus buttons. The left button focuses on far objects; the right button focused on near objects.

Iris – There are two Iris buttons. The left button closes the iris; the right button opens the iris.

Light – There are two light buttons. The left button switches off the Camera light; the right button switches on the Camera light.

To Set Up a Preset:

This example is to illustrate how to use the CCTV controls to set up a Preset. Other functions would be set up in a similar way. It should be noted that the Preset will run only if the equipment will support these functions.

1. Select the Switch.
2. Select the Monitor.
3. Select the Camera.
4. Using the controls available (Pan/Tilt, Zoom etc.), move the Camera to the position that is to be recorded as the Preset position.
5. Select the Preset number either from the Preset drop-down list or by entering the number in the Preset field.
6. Click the Record button.

If the Preset is not already named, you may want to name it. To do this, you would need to run CCTV Configuration. The associated camera would also need to be named before the Preset can be named. For details about naming Cameras and Presets see “Create and Configure Cameras” on page 272. You would need to stop the CCTV service and start it again for the named item to be available in CCTV Control.

CCTV Option Event Actions

CCTV Event Actions are a category of the standard P2000 event action dialog box. If you have installed the CCTV option, you will be able add event actions for Switches, Monitors

and Cameras. Note that event actions that are created for the category CCTV are sent via the CCTV Server, which is an OPC Server. CCTV events can therefore be created either by selecting the category CCTV from the Action dialog box or if the action that you wish to define is not available from the category CCTV or you have not fully configured the CCTV equipment from the CCTV/AV Configuration window, you can select OPC Server as the category and write an OPCWrite action.

If you chose CCTV as the category in effect, you are building an OPC Server namespace tag from your field selections. However, when you select the equipment, if you are building a CCTV action you will select it by the name that you gave it when the item was configured and the namespace tag is selected from a drop down list of action types. If you are building an OPC Server tag you will be selecting an intrinsic name (that is, the default namespace name, s0001 for example). The value for an OPC Server tag will be the value of the action type associated with the namespace. Full details of the namespace tags and their values are given in *Appendix E: CCTV Server Namespace Definitions*.



Do not configure OPC Server Event actions before reading and understanding OPC Server. If OPC Server Event actions are not configured correctly, the equipment may not work properly!

The following notes apply to CCTV actions as well as to OPC Server events:

- If the PC on which the selected Server resides is switched off, then the event would have no effect.
- However, if the PC is on and the OPC Server has been switched off, then the event would only be actioned if the appropriate launch and access rights are granted.

- Similarly, if the PC and the OPC Server are running then the event would only be actioned if it has the correct access rights (that is, the sending user and password must be correctly set up at the receiving PC together with the correct DCOM rights). Note that the set up is correct when the software is installed. For more information see *Appendix F: DCOM Configuration*.
- Some CCTV equipment may need to gain control from other control devices (a keyboard for example) before event actions such as pan, tilt and focus can function correctly. You would need to be familiar with the operating requirements of the particular equipment.

To create a CCTV event action:

You would create a CCTV action in the same way as any other event action (see “Creating Actions” on page 208 for further details). You would normally select the CCTV category to add your CCTV event action but you may choose the Category OPC Server and Type OPCWrite.

CCTV Event Action Field Definitions

If CCTV is selected as the Category then the following fields display:

Type – Select from the drop-down list of available action types, please refer to *Appendix A: Event Triggers/Actions* for details.

Items – Select the equipment that is to be actioned. The selection is dependent on the type. For example, if you select a Switch Alarm action type, then you will need to select the Switch and the Alarm from those configured that are to be associated with the action.

If OPCWrite is selected as the Type for the Category OPC Server then the following fields display:

OPC Tag – Select an OPC Tag from those available for the selected OPC Server. The field is associated with a Browse button, which allows you to display a list of those available for the selected server. For a complete list of the CCTV Server namespace tags and their values, please refer to *Appendix E: CCTV Server Namespace Definitions*.

Value – Enter the value that is to apply to the OPC Tag.

Data Type – Select the data type appropriate for the event action value from the drop-down list.

Note that if you are defining a CCTV Server tag, you should select the Program ID JC.CCTV to ensure that all versions of the interface are supported.

DVR

P2000 provides seamless integration with approved Digital Video Recording (DVR) systems. The integration allows authorized users to manage camera functions, including frame rate and resolution, from a single P2000 workstation, as well as to tie an event generated on P2000 to live or stored audio-visual (AV) recording. Depending on the DVR equipment used, it also enables the user to search, retrieve, and download real time or archived AV recording from any transaction or surveillance camera, from any place, at any time.

Audio and video can be recalled by a variety of query options, including date and time, alarm events, camera ID, or DVR ID.

Audio and video is accessed from the Alarm Monitor, Real Time List, and Real Time Map.

The DVR system communicates with the P2000 Server via TCP/IP connections. The communication is provided by the P2000

CCTV Server service, a software component installed automatically with the DVR option.

Additionally, the DVR option can be configured with a CCTV Switch for added control of the CCTV cameras and monitors. For detailed configuration instructions, refer to the *DVR Integration Option* documentation.

Redundancy

Johnson Controls® provides a Fault Tolerance solution (with Marathon everRun FT™) to their P2000 Security Management System.

Marathon Technologies everRun software runs on standard Windows® servers and provides a high availability solution for the P2000 Security Management System.

The Marathon everRun FT software is layered on to standard Microsoft server software. It creates the Marathon FTvirtual Server™, ensures *lockstep* process and maintains full data integrity between two redundant physical servers.



CAUTION
The installation and configuration of a P2000 redundancy system with Marathon everRun should be performed by qualified professionals who possess a reasonable level of experience with advanced configurations. You must contact Technical Support to complete appropriate training prior to installing and configuring this option.

Contact your sales representative for more detailed information.

FDA Part 11

The P2000 software provides features designed to assist facilities that may be subject to Food and Drug Administration (FDA) Title 21, Code of Federal Regulation (CFR) Part 11 for electronic records and electronic signatures. The Title 21 CRF Part 11 provides the criteria under which the FDA accepts electronic records and electronic signatures as equivalent to paper-based records and traditional handwritten signatures, and regulates how these electronic records should be created, modified, maintained, archived, and transmitted.

Note: *An electronic record is a combination of text, graphics, or data that is created, modified, maintained, archived, retrieved, or distributed by a computer system. An electronic signature is a computer data compilation of any symbol or series of symbols (ID/password combination), and is the electronic equivalent of a handwritten pen on paper signature.*

P2000 allows customers to define parameters to assure Part 11 compliance. The following are general Part 11 requirements applicable to the P2000.

Audit Trail – P2000 provides valuable time-stamped reports to monitor day-to-day operator activity, such as how the hardware is controlled, when alarms are acknowledged, when entity records are changed, and more. A complete list of P2000 Standard Reports is presented in “P2000 Standard Report Definitions” on page 342, along with a brief description of each and how they can be used.

Authorized Users – The P2000 software limits system access only to authorized individuals. Authorized users are identified by their unique combination of user name and password. The passwords for these individuals can be configured to change periodically and have a minimum password length. Additionally, the software disables user access on multiple invalid login attempts and provides for automatic log off due to user inactivity. Refer to the “User Tab” on page 147 for detail instructions on adding users to the system. In addition, the “Password Policy Tab” on page 35 presents a number of parameters to define passwords that comply with FDA regulations.

Record Validation – The P2000 software provides a tampering tool to detect unauthorized record modifications. Refer to “System Validation” on page 334 for instructions on how the system validates digital signatures, points out discrepancies, and corrects discrepancies to ensure that records now have a valid digital signature.

Record Persistence – All original records are saved in the P2000 database, even if records are modified. The P2000 software generates detailed, time-stamped audit trails reports, assuring that all record changes maintain the original recorded information and thereby protecting all previous data. Refer to “P2000 Standard Report Definitions” on page 342 for a complete list of P2000 Standard Reports.

Record Retention – Through software configuration, a system administrator can define parameters to backup and retrieve records to ensure the availability of all records for a specified period of time. Refer to “Retention Policy Tab” on page 34 to enforce FDA Part 11 record retention policy. Also, “FDA Part 11 Backups” on page 332 provide instructions to perform periodic backups to comply with FDA Part 11 record retention requirements.

Intercom

The P2000 system provides the capability to interface with *Zenitel AlphaCom* series intercom systems via an RS232 serial connection. When the Intercom option is installed in your system, the P2000 Intercom Interface Service running on the Server allows an operator to establish an audio communication link between any two or more defined intercom stations that are controlled by the AlphaCom intercom system.

Once the intercom stations are defined and the communication link is established, you will be able to control intercom calls using the P2000 Intercom Control application. The Intercom Control displays all incoming call requests from intercom stations. You can select a call request from the list and connect your master intercom station to the selected calling station.

Hardware Requirements

Prior to configuring the P2000 software components to control the intercom equipment, you must ensure that at least basic intercom hardware components are up and running. Installation of the intercom equipment must be made in accordance with the manufacturer’s instructions. Ensure that:

- The AlphaCom intercom system is operational. Refer to the manufacturer’s documentation for assistance.
- The MPC data output port in the AlphaCom intercom system is enabled.
- The Intercom Exchange box is connected to the P2000 Server. Use an RS232 DB9 cable to connect the specific COM port on the Exchange box to an available COM port on the P2000 Server.

Note: The COM port to be used at the Exchange box depends on the AlphaCom model used at your facility.

- At least one Master Station is configured in the intercom system.
- At least one Sub-Station is configured to link to the Master Station. The Sub-Station should be configured to send call requests to its Master Station.

Intercom System Hardware Verification

1. From the Master Station, dial a Sub-Station.
2. Verify that the call is received and that the Sub-Station name displays on the Master Station control screen.
3. Repeat steps 1 and 2 for each Sub-Station.
4. Send a call request from the configured Sub-Station.
5. Verify that the Master Station rings from the call request and that the Sub-Station name displays on the Master Station control screen.
6. Receive the call request from the Sub-Station.
7. Verify communication from the Sub-Station and that its name displays on the Master Station control screen.
8. Repeat steps 4-7 for each Sub-Station configured to send call requests to the Master Station.

Intercom Configuration

The following sections describe the procedures to define the parameters used by the P2000 system to communicate with the AlphaCom intercom system. Intercom configuration can only be performed at the Server.

If you use the Partitioning option, then the intercom stations can be assigned to a partition. The operator will only be able to handle call requests and connect or disconnect with other stations that belong to partitions that the operator can access.



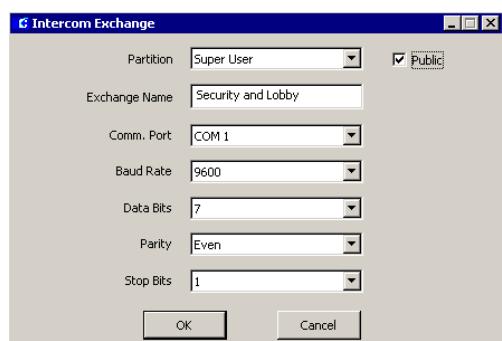
For any intercom configuration changes to take effect, the P2000 Intercom Interface Service must be stopped and restarted using Service Control, see "Starting and Stopping Service Control" on page 315.

Intercom Exchange

Each P2000 workstation acting as an intercom control Master Station will be associated with a specific Intercom Exchange. Intercom exchanges can be linked to extend the number of intercom stations controlled by a single master intercom station.

To Define an Intercom Exchange:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the **Intercom** icon and click **Add**. The Intercom Exchange dialog box opens.



3. If this is a partitioned system, select the **Partition** in which this intercom exchange will be active.
4. Select the **Public** check box if you wish this intercom exchange to be visible to all partitions.
5. Enter a descriptive **Exchange Name** to identify the intercom exchange box to which the stations are connected.

Note: If the programming in the intercom equipment changes, you will have to make the corresponding changes in the P2000 intercom configuration.

6. Select from the **Comm. Port** drop-down list, the P2000 Server port to which the Intercom Exchange box is connected.
7. The values for the **Baud Rate**, **Data Bits**, **Parity**, and **Stop Bits** should be set to match the settings in the AlphaCom intercom hardware settings. Edit the settings if necessary.
8. Click **OK** to save your settings. The Exchange name displays under the Intercom icon in the System Configuration window.

Intercom Stations

Once you create an Intercom Exchange in the System Configuration window, an Intercom Station icon is automatically added under the Intercom Exchange name. Now you should define the intercom stations to open an audio channel for communication. P2000 will establish a connection between the selected stations and the workstation where the operator is logged on. The P2000 workstation associated with the exchange will be able to control the calls only from the stations assigned to that exchange.

To Add an Intercom Station:

1. In the System Configuration window, click the plus (+) sign next to the Intercom Exchange name where you want to define the stations.
2. Click the **Intercom Station** icon and click **Add**. The Intercom Station dialog box opens.



3. Enter a descriptive **Name** that identifies the location of the station.
4. Enter the **Address** assigned to this station. P2000 will connect to the station based upon the address entered here. This address has to match the address assigned at the station equipment.
5. From the **Priority** drop-down list, select a priority value from 0 (highest) to 255 that determines the order the call request will be placed in the Intercom Control queue.
6. From the **Type** drop-down list, select one of the following:
 - Sub-Station** – At least one Sub-Station should be configured to send call requests to its Master Station.
 - Global Sub-Station** – Select to allow Sub-Stations to connect to other Master Stations.
 - Station Group** – Select to connect to multiple stations at the same time. P2000 will establish a connection between the stations that are part of the group selected and the

workstation where the operator is logged on.

Master Station – The Intercom Exchange must have at least one Master Station to link to other stations.

7. If you are defining a Master Station, select from the **Workstation** drop-down list, the workstation name that controls the Master Station.
8. Click **OK**. The station name displays under the Intercom Station root icon.

Intercom Control

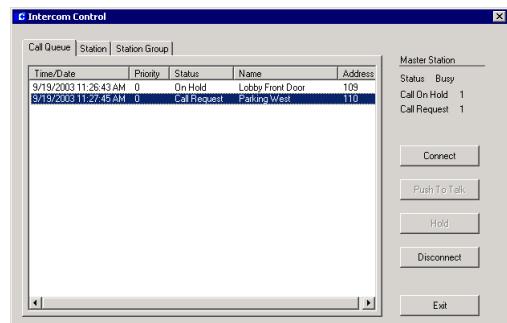
The P2000 Intercom Control window allows the operator to monitor incoming call requests and to connect with stations or station groups that are part of the workstation's exchange. The Intercom Control dialog box will allow the operator to sort the list of call requests by request time, priority, status, or name.

When the call comes the operator can select any call in the queue and connect the master intercom station to the calling intercom station. Once connected, the operator can place the call on Hold or Disconnect the call.

Note: Stations can also be connected or disconnected using the Real Time Map, see "Controlling Intercom Stations using the Real Time Map" on page 289.

To Control Intercom Stations:

1. From the P2000 Main menu, select **Control>Intercom**. The Intercom Control dialog box opens at the Call Queue tab.



The top right section of the dialog box displays general information related to the Master Station. The list box displays the calls currently in the queue, either from Sub-Stations or Station Groups. The following information is shown for each call in the list:

Time/Date – The date and time when the call was placed.

Priority – The priority that was set in the Intercom Station dialog box.

Status – Displays one of the following status: Call Request, On Hold, Idle, or Busy.

Name – The name of the Sub-Station or Station Group that is placing the call.

Address – The address assigned to the Sub-Station or Station that is placing the call.

2. Select any call in the queue and click the **Connect** button. This will connect your master intercom station to the calling intercom station selected.
3. Once connected, you may communicate (talk and listen) with the person(s) at the Sub-Station. You can also perform the following actions:

Push to Talk – Click and hold to talk (not listen) to the person(s) at the selected calling station. Release the button to only listen (not talk) to the person(s) at the Sub-Station. To return to duplex communication (the ability to talk and listen without holding/releasing the button), click the Push to Talk button without holding it down.

Hold – Disconnects from the calling station and leaves the call in the queue.

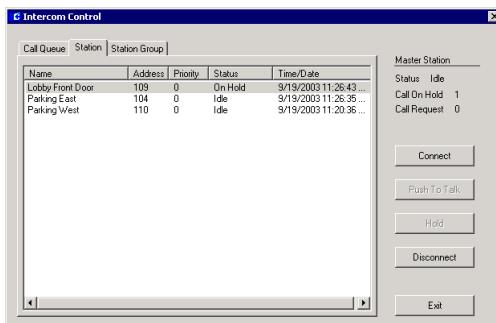
Disconnect – Disconnects from the calling station and removes the entry from the queue.

Connect – Selecting another entry in the queue and clicking Connect will perform a Hold on the currently connected call.

4. Click **Exit** to close the Intercom Control dialog box.

To Control Sub-Stations Only:

1. From the P2000 Main menu, select **Control>Intercom**. The Intercom Control dialog box opens.
2. Click the **Station** tab.



The list box displays the Name, Address, and Priority of the Sub-Station, as well as the current status of the call request and the time/date when the change of status took place.

3. In the list box, select a station to which you wish to connect.
4. Click the **Connect** button.
5. You may now communicate with the person(s) at the selected station. You may also perform the actions described earlier (e.g., Push to Talk, Hold, etc.).
6. Click **Exit** to close the Intercom Control dialog box.

To Control Station Groups:

1. From the P2000 Main menu, select **Control>Intercom**. The Intercom Control dialog box opens.
2. Select the **Station Group** tab.



The list box displays the Name, Address, and Priority of the Station Group.

3. In the list box, select a station group to which you wish to connect.
4. Click the **Connect** button.
5. You may now communicate with the person(s) at the stations of the Station Group selected. You may also perform the actions described earlier (e.g., Push to Talk, Hold etc.).
6. Click **Exit** to close the Intercom Control dialog box.

Controlling Intercom Stations using the Real Time Map

The Real Time Map displays the current status of intercom stations on a map layout of your facility. If an intercom status changes, the Real Time Map shows the state change and the location of the intercom device. Refer to “Using the Real Time Map” on page 218.

When a call request is received for a station, the intercom icon starts flashing. You can right-click the icon to open a shortcut menu and choose to connect or disconnect the call. If the intercom icon was configured to allow the operator to activate events, the event name will also display in the shortcut menu.

To add intercom icons to the Real Time Map, follow the instructions provided in “To Place Device Icons on a Real Time Map:” on page 221 and rather than defining input points, select from the drop-down list the Intercom stations you wish to display in the Real Time Map.

Note: *Map Maker provides a default intercom image set to display various intercom states such as “Station Idle,” “Station Busy,” “Station Call Request,” and so on. However, you can use your own icons to create custom image sets. Refer to “Adding Image Sets” on page 223 for details.*

Intercom Events

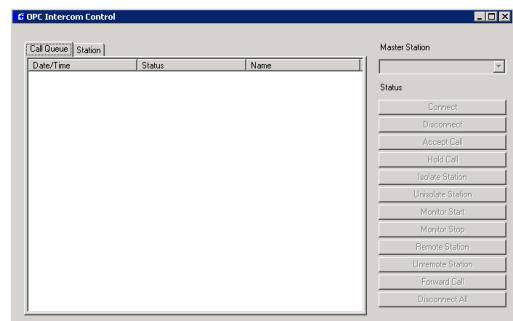
The intercom equipment connected to the system can respond to event actions using the P2000 Event application. You can define Event Actions that *Connect* or *Disconnect* stations, or events that are to be triggered upon a *Station Busy*, *Station Call Request*, *Station Connected*, or *Station Idle*. Refer to “Creating Events” on page 206 to create new event triggers and actions.

OPC Intercom Control

This application allows you to control third party intercom equipment from the P2000 system. Once the intercom equipment is installed using the instructions provided by the manufacturer, you must use the Data Message Configuration application to enable the OPC intercom equipment to communicate with the P2000 system. Refer to “Set Up Message Data Configuration” on page 110.

To Control OPC Intercom Equipment

- From the P2000 Main menu, select **Control>OPC Intercom Control**. The OPC Intercom Control dialog box opens.



- If you click the **Call Queue** tab, the list box displays all current calls in the queue for the P2000 workstation controlling the intercom calls (this workstation). The list includes the station name, corresponding status, and the date and time of the intercom call.
- If you click the **Station** tab, the list box displays all intercom stations in the system with their corresponding status, date and time of the associated status, and the type of station (master or slave).
- Select from either list box the station name you wish to control and click one the following action buttons on the right side:

Connect – Establishes a connection to the selected intercom station. Applies only if the intercom station is in *Idle* state.

Disconnect – Disconnects the current connection between the P2000 workstation and the specified intercom station.

Accept Call – Accepts the call from the selected intercom station.

Hold Call – Puts the current call on hold.

Isolate Station – Isolates the selected intercom station, so that the station is no longer able to receive or make any calls.

Unisolate Station – Removes the selected intercom station from the isolated state by returning the station to “normal” operation.

Monitor Start – Starts monitoring activity on the selected intercom station.

Monitor Stop – Stops monitoring activity on the selected intercom station.

Remote Station – Remotes the selected intercom station, so that all calls to this station are redirected to the current station.

Unremote Station – Removes the selected intercom station from the remoted state by returning the station to “normal” operation.

Forward Call – Forwards a call to the selected intercom station.

Disconnect All – Disconnects all connections from the selected intercom station.

5. When you finish controlling the intercom stations, close the window.

Note: *Third party intercom stations can also be controlled from the Real Time Map, see “Controlling Intercom Stations using the Real Time Map” on page 289. In addition, the intercom equipment can respond to event actions using the P2000 Event application. You can define Event Actions that Connect or Disconnect stations, or events that are to be triggered upon a “Call Terminated” or station “Isolated.” Refer to “Creating Events” on page 200 to create new event triggers and actions.*

P2000 Enterprise

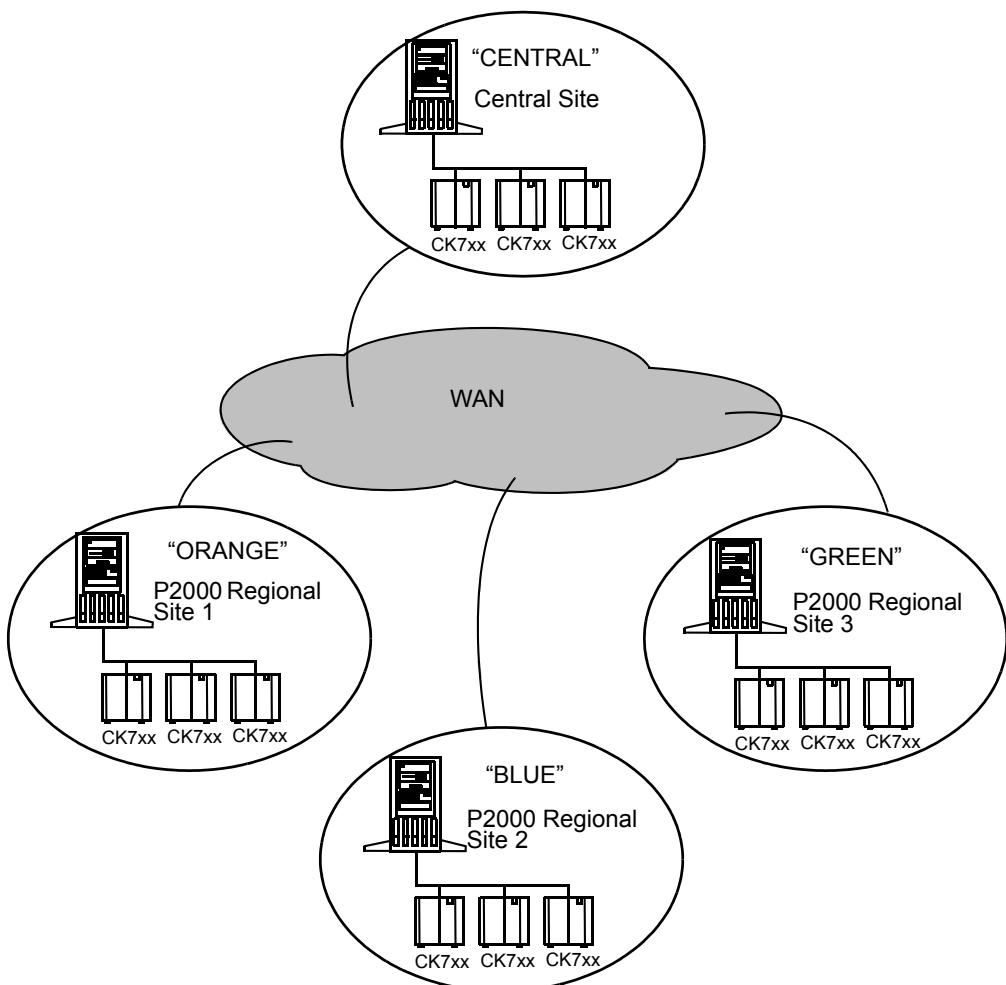
The P2000 Enterprise option allows customers with multiple sites to communicate with each other to share Entity/Identifier information. Entities can be granted access to doors at all assigned sites within the Enterprise system.

In the P2000 Enterprise Configuration, one P2000 site becomes the P2000 Central Site and all other P2000 systems within the enterprise become P2000 Regional Sites. Each regional site synchronizes its data with the

central site. Database replication is implemented through the use of Microsoft SQL Server database technologies.

Prior to defining Enterprise parameters using the P2000 software, you must refer to the *Enterprise Configuration Option* manual for instructions on:

- Configuring the P2000 Central Site
- Moving data from existing P2000 Regional Sites to the P2000 Central Site
- Configuring a P2000 Regional Site



Once you complete Enterprise Configuration, you are ready to set up Enterprise parameters within the P2000 software. Follow these basic procedures:

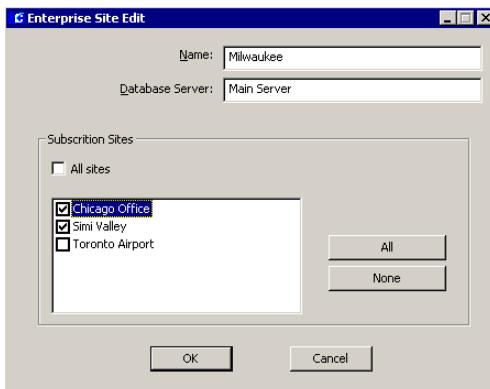
- Define Enterprise Parameters
- Assign Entities with the sites they are allowed to access
- Define the access rights and security privileges at the assigned sites

Enterprise Parameters

Prior to assigning Entities access to multiple sites, you should define global Enterprise Sites, Time Zones, and Access Groups.

To Define Enterprise Sites:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the plus (+) sign next to the root **Enterprise Parameters** icon to display the enterprise parameters.
3. Click the **Enterprise Sites** icon.
4. Click **Add**. The Enterprise Site Edit dialog box opens. The list box displays the name of your local site.



5. In the **Name** field, enter the name of the regional Site exactly as defined at the P2000 site that will provide access.
6. In the **Database Server** field enter the Server name of the regional site.
7. In the Subscription Sites box, select the site names that can be associated with this site. Any changes in this Site will be reflected on the site names selected in this box.
8. To select all sites, click the **All** button. This option allows you to unselect site names individually.
9. To clear your selections, click the **None** button.
10. To select all sites, select the **All sites** check box. This option does not allow editing.
11. Click **OK** to save your settings.

To Define Enterprise Parameters:

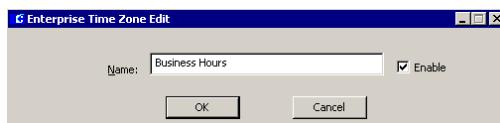
1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the **Enterprise Parameters** icon and click **Edit**. The Enterprise Parameters Edit dialog box opens.



3. Select from the **Enterprise Site** drop-down list, the site name that will be defined as the central Enterprise site.
4. Select from the **Alternate Enterprise Site** drop-down list, the site name that can be defined as the alternate Enterprise site.
5. Click **OK** to save your settings.

To Define Enterprise Time Zones:

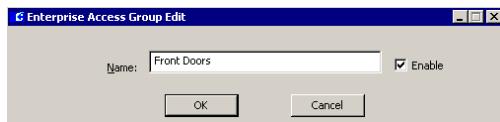
1. Click the plus (+) sign next to the root **Enterprise Parameters** icon to display the enterprise parameters.
2. Click the **Time Zones** icon.
3. Click **Add**. The Enterprise Time Zone Edit dialog box opens.



4. In the **Name** field, enter the name of the Time Zone exactly as defined at the P2000 site that will provide access.
5. Click the **Enable** check box for the system to recognize this time zone.
6. Click **OK** to save your settings.

To Define Enterprise Access Groups:

1. Click the plus (+) sign next to the root **Enterprise Parameters** icon to display the enterprise parameters.
2. Click the **Access Groups** icon.
3. Click **Add**. The Enterprise Access Group Edit dialog box opens.



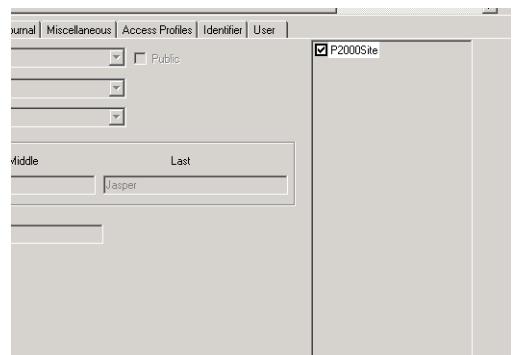
4. In the **Name** field, enter the name of the Access Group exactly as defined at the P2000 site that will provide access.
5. Click the **Enable** check box for the system to recognize this access group.
6. Click **OK** to save your settings.

Assign Entities Enterprise Access

Use the Entity Management application to assign the sites an entity can access. Once the sites are assigned, the entity information will be sent to the selected sites for download.

To Assign Enterprise Access to an Entity:

1. From the P2000 Main menu, select **Access>Entity Management**. The Entity Management window opens.
2. Create a new record or edit an existing entity as desired. For details, refer to “Entering Entity Information” on page 132.



The General tab displays a list box at the bottom right side of the window showing all the Enterprise sites defined in the System Configuration window. See “To Define Enterprise Sites.” on page 292.

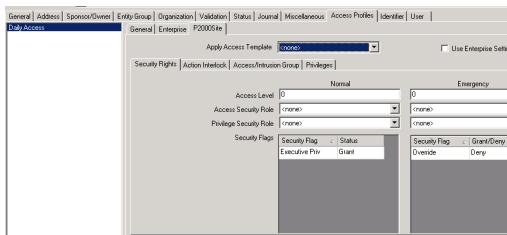
3. In the Enterprise box, select the check box next to the site that this entity may access. You may select as many sites as needed.
4. Once the sites are assigned, click the **Save** icon. The Access Profiles tab will display the Enterprise Sites that the entity can access.

Define Global Access Rights

Once the entity has been assigned to the selected sites, you may define the security privileges and access rights using Access Profiles.

To Define Access Rights:

1. In the Entity Management window, select from the list an entity that has Enterprise access and click the **Edit** icon.
2. Click the **Access Profiles** tab.



3. Enter the information on the General tab. For detailed information refer to “Access Profiles Tab” on page 138.

The Access Profiles tab displays the site name tabs of the sites assigned to this entity. The Enterprise tab is used to assign global access privileges. The local site tab is used to assign local access privileges. Additional tabs show other site names assigned to the entity.

Assigning access privileges is determined by the following conditions:

- When you define access to the local site, and select the **Use Enterprise Settings** check box, the security options defined in the Enterprise tab will be applied.
- When you define access at a different site, and select the **Use Enterprise Settings** check box, the security options defined in the Enterprise tab will be applied to that site.

- Security Rights, Access/Intrusion Groups, and Privileges can be accessed for your own site, the Enterprise site or for any site within the Enterprise system.
- On each site, a maximum of 64 Access/Intrusion Groups are applicable (32 local and 32 Enterprise).
- P2000 will only download the maximum number of Access/Intrusion Groups for each panel type, giving priority to the local settings.
- 4. Once the Access Profiles are defined, click the **Save** icon.
- 5. Click the **Identifiers** tab and click the **Edit** icon.
- 6. Create or edit an existing Access Badge. Refer to “Identifier Tab” on page 142 for instructions.
- 7. From the **Identifier Access Profile** drop-down list select the Access Profile that contains the Enterprise access rights and click the **Save** icon. This will initiate all required downloads.

Note: The Status tab in the Entity Management window displays status information occurring at the local site, and if selected, at other enterprise sites. The status information displayed for enterprises sites shows last replicated data. Refer to “Status Tab” on page 137.

Web Access

Web Access is a suite of applications that enables authorized users to perform various P2000 tasks from any web-ready PC or compatible Personal Digital Assistant (PDA) device. Web Access offers many features such as employee, visitor, and contractor management applications, entity activity tracking and synchronization, alarm monitoring, emergency access disable, and a customizable user interface.

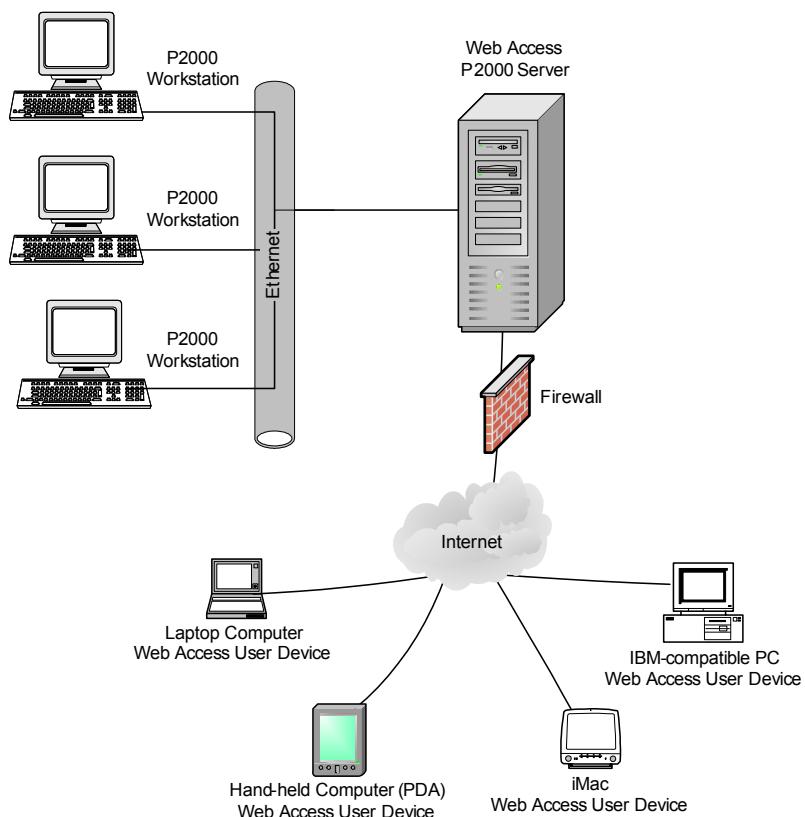
Web Access can support different hardware configurations, the most common (shown on the illustration), uses a single server. In this configuration, the P2000 Server runs the Web

Access front-end and back-end services.

Essentially, the P2000 Server is also used as the web server. The Web Access front-end services handle the web browser HTTP requests, while the Web Access back-end services handle the application's XML requests from the front end.

In another configuration, the P2000 Server can run the Web Access back-end services, and a separate PC can be used to run the front-end services.

Before you define Web Access parameters using the P2000 software, you must refer to the *Web Access Manual* for the software components required to operate the P2000 Web Access application.



Sequence of Steps

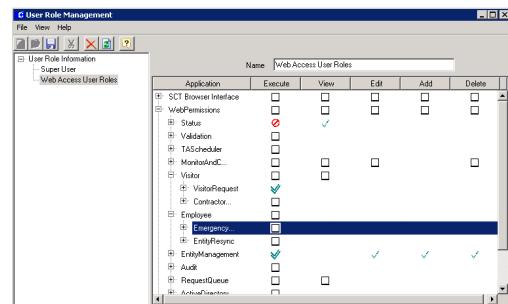
Once the Web Access option is installed at the Server and front-end PCs, follow these basic procedures for defining, implementing, and using Web Access:

- Create and assign user roles to perform Web Access functions
- Define Web Access options
- Define request approvers
- Submit requests using Web Access
- View the status of a request
- Approve the request
- Process the request

Creating and Assigning Web Access User Roles

To prevent unauthorized users from performing high-level actions, such as deleting entity records or rejecting requests, the system administrator must create user roles, which are assigned to users who perform Web Access functions.

Each individual Web Access function is controlled by user roles and each user role group can include various combinations of permissions.



The Web Access applications are listed under the **WebPermissions** tree structure, and can provide up to five permission levels. For details on the different permission levels and options, refer to “User Role Management” on page 21. Once the user roles are defined, they will be available for assignment from the User tab in the Entity Management window.

The following table lists the Web Access functions that can be performed according to the permission operation selected.

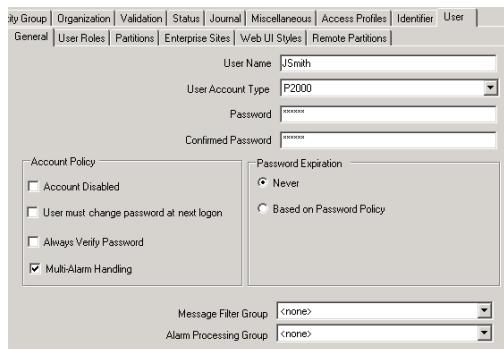
Application – Operation	Execute	View	Edit	Add	Delete
Status	Can access all Status sub-functions.	Can view all Status sub-functions.			
ActivityStatus		Can view the Activity Status page.			
EntityDetails		Can view the Entity Details page.			
EntityIOStatus		Can view the Entity I/O Status page.			
EntitySearch		Can view the Entity Search page.			
AreaStatus		Can view the Area Status page.			
IdentifierDetails		Can view the Identifier Details page.			
Validation	Can access all Validation sub-functions.				
ValidateJournal	Can validate a journal request.				

Application – Operation	Execute	View	Edit	Add	Delete
ValidateVisitorRequest	Can validate a visitor request.				
ValidateUserAccount	Can validate a user account request.				
ValidateContractorRequest	Can validate a contractor request.				
ValidateEntity	Can validate an entity request.				
ValidateEmergencyDisableRequest	Can validate an Emergency Access Disable request.				
ValidateAccessProfile	Can validate an access profile request.				
ValidateRelationship	Can validate a relationship request.				
ValidateEntityResync	Can validate an entity resync request.				
ValidateIdentifier	Can validate an identifier request.				
TAScheduler	Can access the listed T&A Scheduler sub-functions.				
TASMonitor		Can view the T&A Area Monitor page.			
TASDetails		Can view T&A schedule details.	Can edit T&A Work Schedule entries.		
TABroadcast Message			Can make edits in the T&A Broadcast Message page.		
TASView		Can view T&A schedules from the Monthly page.			
MonitorAndCommand	Can access the listed Monitor and Command sub-functions.				
OutputControl	Can control P2000 outputs.				
DoorControl	Can control door functions, such as lock or unlock.				
AlarmMonitor	Can use Alarm Monitor functions.				
Visitor	Can access the listed Visitor sub-functions.				
VisitorRequest	Can send a visitor request.				
ContractorRequest	Can send a contractor request.				
Employee	Can access the listed Employee sub-functions.				
EmergencyDisable	Can perform an Emergency Access Disable command.				
EntityResync	Can perform the Entity Resync command.				
EntityManagement	Can access the listed Entity Management sub-functions.		Can make edits in the listed Entity Management sub-functions.	Can add items in the listed Entity Management sub-functions.	Can delete items from the listed Entity Management sub-functions.

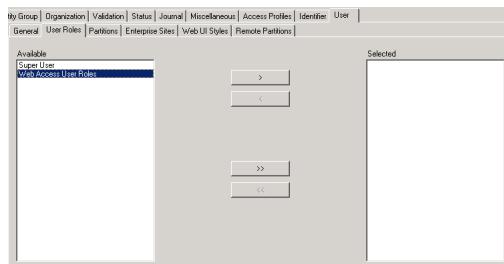
Application – Operation	Execute	View	Edit	Add	Delete
EntityRelationship			Can edit an entity's relationship.	Can assign a relationship to an entity.	Can delete a relationship from an entity's record.
AccessProfile			Can edit an entity's access profile.	Can assign an access profile to an entity.	Can delete an access profile from an entity's record.
Identifier			Can edit an identifier in an entity's record.	Can add an identifier to an entity's record.	Can delete an identifier from an entity's record.
Journal			Can edit an entity's journal.	Can add a journal to an entity's record.	Can delete a journal from an entity's record.
Entity			Can edit an entity's record.	Can add an entity record.	Can delete an entity record.
UserAccount			Can edit an entity's user account.	Can add a user account to an entity's record.	Can delete a user account from an entity's record.
Audit	Can access the listed Audit sub-functions.				
AuditList		Can view the Audit List page.			
RecordChangeAndTracking		Can view the Record Change Tracking page and perform its report functions.			
RequestQueue	Can access Management Services options.				
RequestQueue.Personal	Can list self-submitted requests.	Can view self-submitted requests' details.			Can cancel self-submitted pending requests.
RequestApproval	Can approve requests.				
RequestQueue.All	Can list all requests.	Can view all requests' details.			
ActiveDirectory	Can use Active Directory authentication, if available.				

To Assign Web Access Permissions:

- From the P2000 Main menu, select **Access>Entity Management**. The Entity Management window opens.
- Create a new record or edit an existing record. For details, refer to “Entering Entity Information” on page 132. Click the **User** tab.



- In the General tab, enter the **User Name** and **Password** that the entity will use to log on to the P2000 Web Access site.
- Click the **User Roles** tab under User.



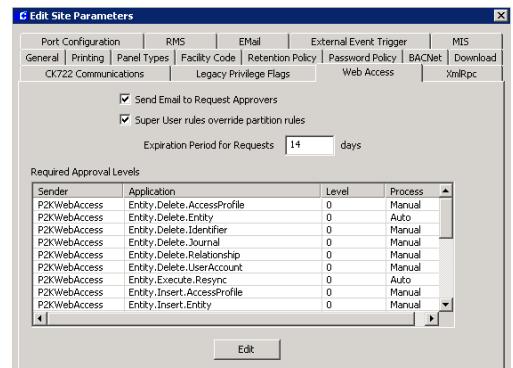
- Select from the **Available** box the Web Access roles that will be assigned to this entity. The entity will be allowed to perform any function defined in this User Role.
- Click the > button to move the User Role from the Available box to the Selected box.
- Save the record.

Defining Web Access Options

The P2000 system allows you to set up system wide settings to define how web access requests are managed. Use the Web Access tab in Site Parameters to define the default Web Access options, approval levels, and processing method for Web Access requests.

To Edit Web Access Parameters:

- From the System Configuration window, select **Site Parameters** and click **Edit**. The Edit Site Parameters dialog box opens at the General tab.



- Click the **Web Access** tab and refer to the following section for detailed information.
- Click **OK** to save the settings and return to the System Configuration window.

Web Access Options Field Definitions

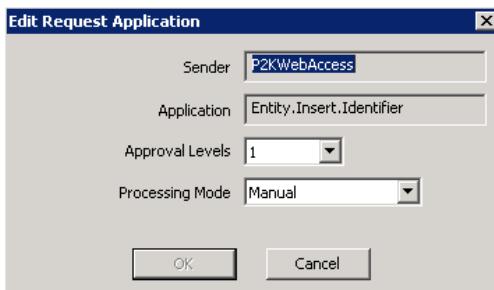
Send Email to Request Approvers – If you select this option, when a person submits a Web Access request that requires approval, an email notification will be sent to the approvers defined in the Request Approvers dialog box; see “Defining Request Approvers” on page 300. The email message will contain a hyperlink to the request, which will take the approver directly to the Request Approval application, assuming the approver has been

assigned with the proper Web Access user roles. The approver's email address is defined in the entity record.

Super User rules override partition rules – If this option is selected, any approvers defined in the Super User partition will override any approvers defined in specific partitions. If this option is not selected, approvers from the specific partition will be used.

Expiration Period for Requests – Enter the number of days after which all Web Access requests will expire. The expiration date is calculated by adding the number of days entered here to the initial date when the request is submitted.

Required Approval Levels – This box displays default approval levels for each of the P2000 Web Access applications. To change the default values, double-click the application name you wish to modify. The Edit Request Application dialog box opens.



Sender – This field displays the Sender that originated the Web Access request.

Application – This field displays the name of the P2000 Web Access application you are currently modifying.

Approval Levels – Select a number from the drop-down list to define how many approvers are required to approve this type of Web Access request. If you select **0**, the Web Access request is sent directly for processing.

Processing Mode – This field defines how the request will be processed after the Web Access request has been approved. Select from the drop-down list one of the following options:

- **Auto** – Select this option if the request will be processed automatically (without intervention).
- **Manual** – Select this option if this application requires an authorized user to manually process the request, refer to “Processing Web Access Requests” on page 307.

Defining Request Approvers

Depending on settings previously defined in Site Parameters, each Web Access request may require up to three active approvers. The approver is an entity who has been assigned Request Approval user roles. The approvers are ordered in a sequence and they receive and approve requests in the way they are ordered.

For example, an application requires three approvers: John (Level 1), Mary (Level 2), and Bob (Level 3). When a request is submitted, an e-mail notification is sent to John, who will approve the request first. After John approves the request, an e-mail notification is sent to Mary; then after Mary approves the request, an e-mail notification is sent to Bob. After Bob approves the request, the approval process is complete. Bob will never see requests that have not been approved by Mary, and Mary will never see requests that have not been approved by John.

Approvers only see requests that are waiting for their approval and each request waits for a single approver at any time. When a request becomes ready for the next approver an e-mail notification is sent to the approver.

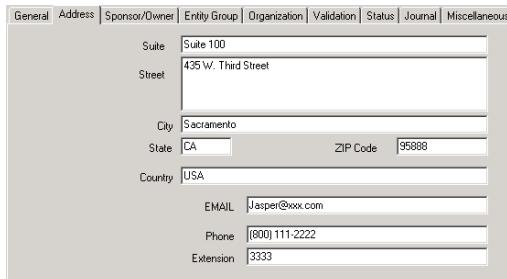
If an application requires a single approver, after the approver approves the request, the approval process is complete.

The P2000 system will ignore all requests that do not have all required approvals completed.

The approver's e-mail address for sending notifications is entered in the entity record.

To Enter the Entity Email Address:

1. From the P2000 Main menu, select **Access>Entity Management**. The Entity Management window opens.
2. Create a new record or edit an existing record. For details, refer to "Entering Entity Information" on page 132. Click the **Address** tab.



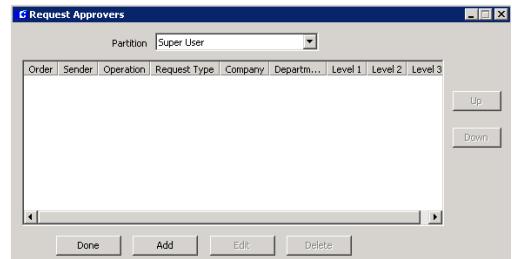
3. Enter the **Email** address that has been assigned to this entity and where notifications will be sent to approve Web Access requests.

Note: To configure your Email Server, refer to "EMail Tab" on page 39, and also check with your IT department for the required email settings in your facility.

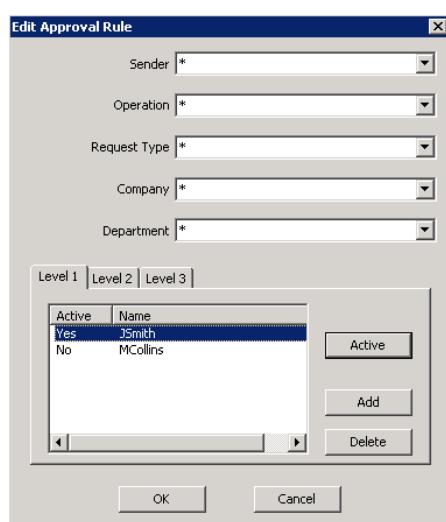
4. Click **OK** to save your settings.

To Define Request Approvers:

1. From the System Configuration window, click the plus (+) sign next to the root **Site Parameters** icon.
2. Click the **Request Approvers** icon and click **Edit**. The Request Approvers dialog box opens.



3. Select the **Partition** from the drop-down list that contains the entities that will be assigned as approvers. Requesters and approvers need to be in the same partition, unless the approver is in the Super User partition.
4. Click the **Add** button. The Edit Approval Rule dialog box opens. If you leave an asterisk (*) in a field, the Approval Rule will include all records for that field.



5. Select from the drop-down list, the **Sender** that originated the request. The selected entity can only approve requests coming from this sender.
6. From the **Operation** drop-down list, select the type of operation (Delete, Execute, Insert, or Update) that the selected entity will be allowed to approve.
7. From the **Request Type** drop-down list, select the type of Web Access request that the selected entity will be allowed to approve.
8. From the **Company** drop-down list, select a Company name to have the selected entity approve only requests coming from the company selected here.
9. From the **Department** drop-down list, select a Department name to have the selected entity approve only requests coming from the department selected here.
10. Click the **Level 1** tab and click the **Add** button. The Select User dialog box opens.
12. Select an entity from the list and click **OK**. The name will be added to the Level 1 list box. You can add as many Level 1 approvers as needed, but only one can be the active Level 1 approver.
13. From the Level 1 list box, select the entity who will be the active Level 1 approver of the type of request and/or operation selected (for the company and/or department selected, if applicable). Click the **Active** button. You can change the Active approver as needed.
14. To remove an entity from the list, select the name and click the **Delete** button.
15. Repeat the procedure, starting with step 4, for the Web Access requests that require **Level 2** and/or **Level 3** approvers.

Note: *The system will generate an error message if a request is submitted and the number of required approvers has not been defined.*



11. Enter the **User Name** (or leave the default *), and click the **Search** button.
16. Once you define the rules for the requests that require approvals, click **OK**. The Request Approvers dialog box will display a list of approval filters. To move an approval filter up or down on the list, select the line item and click the **Up** or **Down** buttons.

The order in which approval filters display in the Request Approvers list box is significant. When a request is submitted, the approval filters in the list are scanned from the top down until the first request/filter match is found. When a match is found the attached approver list is used. If two approval filters include the same rules, the filter above will have precedence over the one below.

Rule 1 requires three approvers for adding entities (from any company and/or department).

Rule 2 requires only one approver for adding visitors (from any company and/or department).

The screenshot shows a software interface titled 'Request Approvers'. At the top, there is a dropdown menu labeled 'Partition' with 'Super User' selected. Below this is a table with columns: Order, Sender, Operation, Request Type, Company, Department, Level 1, Level 2, and Level 3. There are four rows of data:

Order	Sender	Operation	Request Type	Company	Department	Level 1	Level 2	Level 3
1	P2KWebAccess	Insert	Entity.Insert.Entity	*	*	JSmith	MCollins	JKing
2	P2KWebAccess	Insert	Entity.Insert.Entity@AddVisitor	*	*	KBanks		
3	P2KWebAccess	*	*	DEFG Inc.	*	R.Temple		
4	P2KWebAccess	*	*	*	*	GBrice		

On the right side of the table, there are 'Up' and 'Down' buttons for reordering rows. At the bottom of the window are buttons for 'Done', 'Add', 'Edit', and 'Delete'.

Rule 3 requires one approver for any type of request submitted for the DEFG company (any department), except that new entities (rule 1) and new visitors (rule 2) will be approved by the approval filters above.

Rule 4 requires one approver for any request submitted, except that new entities (rule 1), new visitors (rule 2), and DEFG company (rule 3) requests will be approved by the approval filters above.

Submitting Requests using Web Access

The Web Access interface can be accessed via an internet-connected PC or PDA device. This section provides a description of the features available from Web Access. For detailed information on how to use this web-friendly interface, refer to the *Web Access Manual*.

To Log on to Web Access:

- Using a web browser, type the following in the address bar, replacing *ServerName* or *IP Address* with the name or IP address of the Web Access server:

<http://ServerName or IP Address/P2000>

or enter the following if the P2000 Server is configured as a secure server:

<https://ServerName or IP Address/P2000>

Contact your system administrator for the correct settings. The P2000 Web Access Log In screen displays.



2. Enter the **User Name**. This is the name of the entity entered in the User tab of the Entity Management window and that has Web Access user roles assigned.
3. Enter a valid **Password**. This is the password entered in the User tab of the Entity Management window.
4. Click **Log In**. The Welcome page opens.



The links in the User Preference box allow you to change password, default login partition, and default login Web Access style of the current user. The links under Web-Book Favorites provide a way to bookmark Web Access pages and entries most often used. Refer to the *Web Access Manual* for details.

5. To log out and return to the Log In screen, click the **Log Out** link at the upper-right corner of any Web Access page.

Web Access Functions

While each of the following procedures is described in detail in the *Web Access Manual*, a basic description is given here for your convenience.

Employee Services

These services allow authorized users to search for entity records, track entity activity through-

out a facility, and perform entity resync operations.

Entity Search

This feature allows searching for entity records in the P2000 database. Users may search by entity name, badge number, department, company, category, type, and partition.

Area Search

This feature allows users to search for entities that occupy a specific controlled area in a facility. A controlled area is a designated section of a facility, with one or more readers or input points assigned, with the purpose of reporting on the current whereabouts of entities.

Entity Activity

This feature allows users to trace the most recent entity activity and view the identifier transaction associated with the entity, based on the location and time where the identifier was last presented.

Asset Finder

This feature allows users to quickly locate assets in a facility. Once you locate an asset, you may view transaction information associated with the asset.

Entity Resync

This feature allows users to resynchronize their In/Out status if out-of-sync, including the status in areas controlled by Anti-Passback, Anti-Loitering, and Occupancy objects associated with CK722 controllers.

Guard Services

These services allow authorized users to perform a number of guard-related actions, such as view, acknowledge, and remove alarms; and manually control doors and output devices.

Alarm Monitor

P2000 alarms can be monitored, acknowledged and removed using the Web Access interface. This feature is useful to monitor alarms at unattended sites, allowing authorized users to acknowledge alarm conditions as soon as they are reported. Once an alarm is in a “secure” state, the user can remove the alarm from the queue.

Command Outputs

Output devices can be manually activated or deactivated by authorized users to control devices connected to them such as lights, warning indicators or sirens.

Door Command

This feature allows an authorized user to manually lock or unlock a door (override system controls) for a specific time. The user will be able to unlock all doors at once or return all doors to their previous state.

Management Services

Through Management Services, an authorized user can add or edit entity records, including badge identifier and associated entity information. In addition, the user can also view, approve and process Web Access requests, or audit user actions.

Request Status

The Request Status page allows authorized users to view the status of their requests, and depending on their user roles, the status of all requests or the status of requests submitted by other users that belong to the same department or company. The top portion of the screen displays the *Request Search Parameters* box where users can search for specific requests. The bottom portion displays the *Request List*, which displays requests in the order they are received. The links under the *Request* column allows you to view the details of the requests.

Request Approval

The approval process provides additional security measures by confirming the validity of a request before the request is presented for processing. Depending on the settings previously defined in Site Parameters (see “Defining Web Access Options” on page 299), up to three authorized users may be required to approve Web Access requests. The Request Approval page displays the requests that require approval.

Add Entity

This feature allows authorized users to submit requests to enter entity information into the system. Depending on the user roles assigned, users can enter entity related information such as user-defined fields, journals, identifier information, sponsor information (if the entity is a visitor), or attach a portrait to the entity record.

Edit/Delete Entity

In addition to submitting requests for new entities, authorized users can also request to change existing entity records, including deleting records from the system.

Validate

This function is used to process Web Access requests that require manual processing. Refer to “Processing Web Access Requests” on page 307.

Audit

This feature allows authorized users to track changes to the software based on who performed the action, the data affected by the action, the date and time the action occurred, and the action itself, such as Add Entity Group, Edit Entity, Execute Application, etc.

Visitor Management

Visitor Management enables authorized users to add visitors to the system or extend the validation period of contractor badges. In addition, users can also view the status of their requests.

Visitor Request

Web Access provides a faster way for users to make visitor badge requests, so badges are ready when a visitor arrives at a building. Users can simply enter the appropriate visitor data into the system, assign a visitor sponsor, enter the date and time period of the scheduled visit, or enter notes for visitors with special needs.

Contractor Request

Enables authorized users to extend the badge validity period for selected entities. This feature is typically used for visitor badges that are about to expire, but can also be used as needed to extend the badge validity period for regular entities. Users can only extend the badge validity period for entities who belong to the same partition and entity category as the user.

Request Status

This function is also accessed from Management Services, refer to “Request Status” on page 305.

Work Scheduler

This is a Time and Attendance system designed to record and track an entity’s work schedule and attendance record, which can be integrated with a 3rd-party application, such as a payroll system. Using this feature in Web Access, you can define a particular work schedule for an entity, broadcast a message that appears on the Time and Attendance terminal where the entity signs-on, and monitor the entity’s Time and Attendance status.

Current

This tab displays the current work schedule of each entity for the current week. The column listing the schedule of the current day is highlighted in pink. When accessing this tab, the current day always appears in the middle of the week.

Weekly

This tab displays the current week’s work schedule starting with the day of the week defined as the schedule start day (determined by the **Schedule start on** field value of the Work Schedule object, which is defined using the Message Data Configuration application, see page 110. Unlike the Current tab, this tab enables you to view the work schedule of a different week by selecting the **Next Week** and **Previous Week** links.

Monthly

This tab provides a month-to-month view of each entity’s work schedule. Days with a green

sphere icon indicate that the entity has a schedule defined for those days. Days with a dash indicate that the entity does not have a schedule defined on those days.

Broadcast Message

Allows you to modify the general message broadcasted to Time and Attendance terminals.

Area Monitor

This tab enables you to view an entity's current Time and Attendance status such as whether the entity is scheduled to work for the current day, whether he has presented a valid identifier to enter the building, and whether he has checked in for work according to his schedule.

Emergency Access Disable

This feature provides a rapid method of disabling access in case of an emergency. An authorized user can quickly disable all identifiers associated with a selected entity and access will be immediately denied at all doors. In addition, the selected entity will not be able to perform any Web Access functions. Once it is determined that the emergency is over, the identifiers can be enabled again using the Edit/Delete Entity function from the Web Access interface.

Processing Web Access Requests

Web Access requests are processed either automatically or manually, depending on the configuration defined in Site Parameters (see “Defining Web Access Options” on page 299).

For Web Access requests that are set to be automatically processed, once the request is submitted and the approval is completed (if

approval is part of the process), the request is added to the P2000 database. If an error occurs during this process, the request will display in the Request Queue table (see “Request Queue View” on page 335) as “Error” or “Rejected” and the requester is subsequently notified of the problem.

Web Access requests that are set to Manual process, require an authorized user to manually process the request. After the request is submitted and the approval is completed (if approval is part of the process), the request is sent out for validation.

Customizing the Web Access Interface

Web Access graphical user interface is controlled by styles, which can be fully customized according to individual needs. The interface is built with XML (Extensible Markup Language) technology and can be customized using the Altova® StyleVision® designer software tool to modify the following Web Access interface components:

- Caption font size, type, and color
- Field type (e.g. combo box, text box, etc.), location, and size
- Images (e.g. company log)
- Button types
- Background colors

Note: The customization feature also allows Web Access pages to be displayed in different languages.

Web Access provides a default style (*jci*), which is assigned to all Web Access users. You can however, modify the default style and assign it to all users, or create multiple styles to be assigned to specific users using the Web

UI Styles tab in the Entity Management window (see “Assigning Styles to Web Access Users” for details).

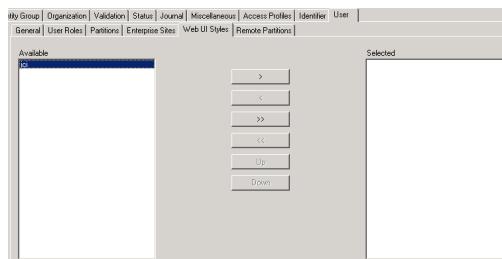
For detailed instructions on creating customized styles, refer to the *Web Access Manual*.

Assigning Styles to Web Access Users

Once the Web Access interface styles have been created using the instructions provided in the Web Access Manual, they will be available for assignment via the *Web UI Styles* tab in the Entity Management window.

To Assign Styles to Web Access Users:

1. From the P2000 Main menu, select **Access>Entity Management**. The Entity Management window appears.
2. Select an entity that is allowed to perform Web Access functions. Refer to “To Assign Web Access Permissions:” on page 299. Click the **Edit** icon.
3. Click the **User** tab.
4. Click the **Web UI Styles** tab.



5. Select from the **Available** box the Web Access interface style that will be assigned to the user. You can select multiple items by holding down the **<Shift>** key.

6. Click the **>** button to move the interface style from the Available box to the **Selected** box.
7. To select all styles in the **Available** box, click the **>>** button.
8. To remove styles from the **Selected** box, select the desired styles and click the **<** button, or click **<<** if you want to remove them all.
9. Use the **Up** or **Down** buttons to move the styles on the Selected box accordingly.

Note: *The first style on the Selected box is the user's default style. If the user wishes to use a different style, then he or she will need to select a style using the User Preferences feature from the Web Access interface. Refer to the Web Access Manual for details.*

Chapter 5: System Maintenance

The P2000 software provides several functions to help you maintain your security management system once it is up and running. These functions are considered non-routine and are typically performed by a system administrator. Some of these functions can be performed only from the Server.

The following sections describe how to:

- **Download Data to Panels**
- **Monitor Download Status**
- **Monitor Smart Download Activities**
- **Control and Monitor Services**
- **Monitor Workstation Status**
- **Monitor System Status**
- **Write Controller DB to Flash Memory**
- **Update CK705/CK720 Panels**
- **Update CK722 Panels**
- **Update S321 Panels**
- **Perform Database Maintenance**
- **View and Filter Request Queue Items**

Each function is described in detail in the following sections.

Downloading Data to Panels

Under normal operating conditions, data such as additions to the entity database and other changes to the system are downloaded automatically to the panels and no specific downloading procedures are required. With the Download function, you can manually down-

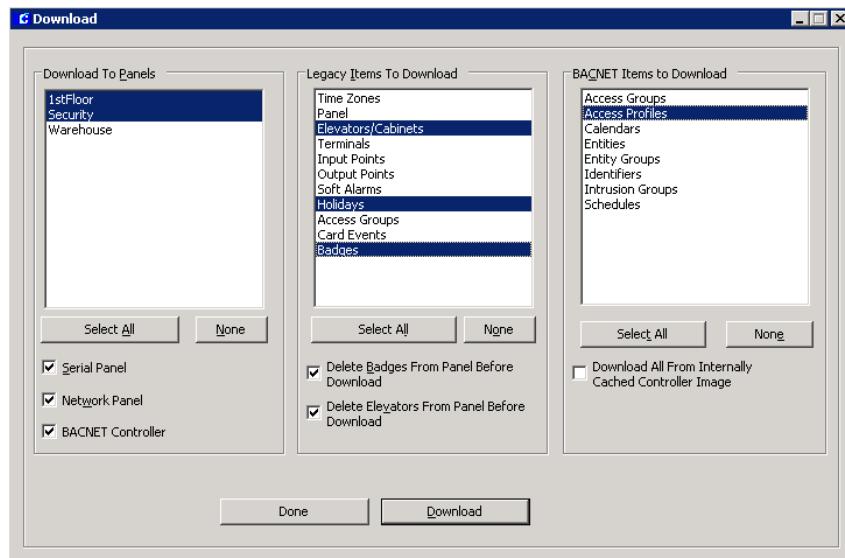
load data to panels if there has been an interruption in communication. For example, if a panel or group of panels has been offline for maintenance, you can use Download to update panels with system changes that occurred while they were down. Or, you may need to download data to all panels after a complete power failure or system upgrade. The Download function should be performed only by a system administrator, and is password protected.

You can download individual items such as a change in holiday schedule or added card events, or you can download all items at once.

TIP: Open the Download Status dialog box to monitor the records in the download queue as the download takes place.

To Download Data to Panels:

1. From the P2000 Main menu, select **System>Download**.
2. Enter the password if prompted. The Download dialog box opens.
3. From the Download To Panels box, select the **Serial Panel**, **Network Panel** and/or **BACNET Controller** check box. The list of panels displayed will be limited according to the type of panel selected here.
4. Select the panel(s) to which you wish to download data, or click **Select All** to select all panels in the list. (Click **None** to clear your selections and reselect the panels individually.)



5. From the Items To Download (Legacy and/or BACNET boxes), select the items you wish to download to the panel(s), or click **Select All** to select all items in the list(s). (Click **None** to clear your selections and reselect the items individually.)
6. To download all badges to a legacy panel and still allow access through a door of the panel while being updated, select **Badges** from the Legacy Items To Download box, and clear the **Delete Badges From Panel Before Download** check box.
7. To download elevator data without deleting all elevators from the legacy panel, select **Elevators/Cabinets** from the Legacy Items To Download box, and clear the **Delete Elevators From Panel Before Download** check box.
8. If you are downloading data to CK722 (BACNET) panels, you can select the **Download All From Internally Cached Controller Image** check box to quickly download CK722 database items. This feature is provided through the Fast Download option, which allows CK722 database items to be downloaded much more quickly than using the standard download method. Refer to “Database Maintenance Actions” on page 326 for a description of Fast Download operations.
9. When all selections have been made, click **Download**. The records queued during the download will display in the Download Status message box. (In large downloads, the number of items queued may fluctuate if data is transferred faster than the panels can receive it. This is normal. The download is complete when the Records Queued returns to “0”.)

Note: *If you do not delete all badges first, and the panel being updated has any badges that should not be there, they will not be removed.*

Download Status

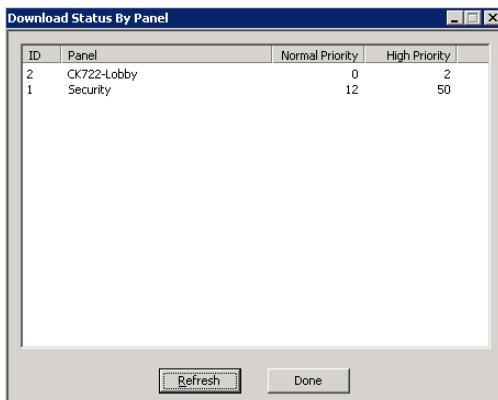
Download Status displays the status of any items automatically downloaded by the system, and can be used in conjunction with the Download function.

To Monitor Download Status:

- From the P2000 Main menu, select **System>Download Status**. The Download Status message box opens.



- Drag the Download Status message box to where it will be visible during the download process. The number of records queued during the download will display as the download progresses.
- To see the number of records queued at each panel, click the **Details** button. The Download Status By Panel dialog box opens.



The list displays all panels configured in the system. The ID column shows a number that is automatically assigned to each

panel and is used primarily to troubleshoot the system. All items are downloaded at a **High Priority**, with the exception of Badges, which are downloaded at a **Normal Priority**.

- Click the **Refresh** button to update the screen with new data as the download progresses.
- Click **Done** to close the Download Status By Panel dialog box.
- Close the Download Status message box.

Smart Download Control

The Smart Download Control application allows you to closely monitor Smart Download queue activities, such as downloading badges to panels when changes are made to access groups and terminal groups, as well as downloading entity and badge changes.

You should use the Download tab in Site Parameters (see page 37) to set up rules that determine the time when these downloads will take place.

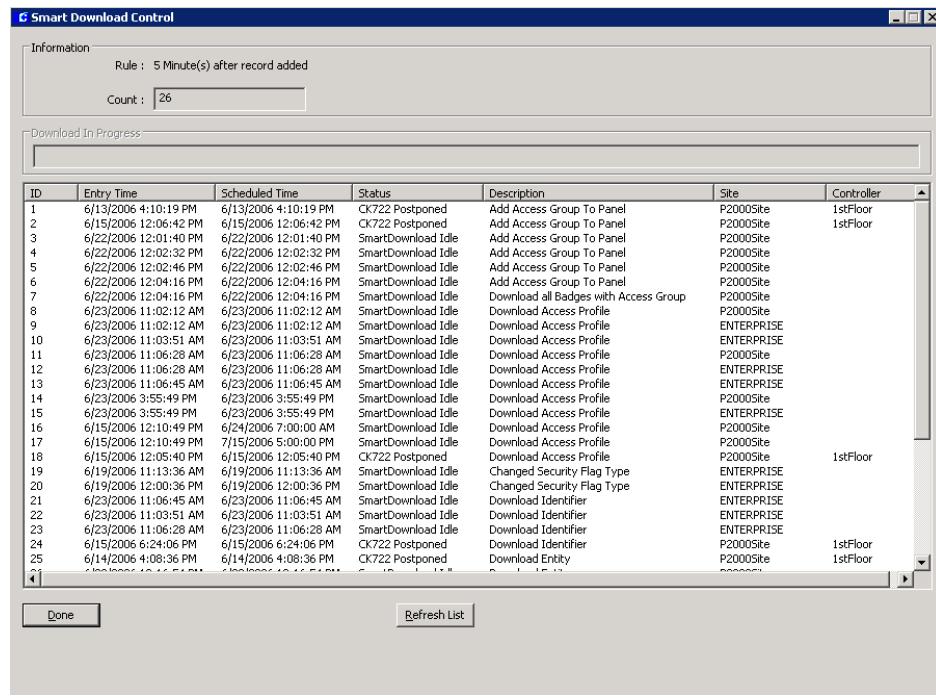
To Monitor Smart Downloads:

- From the P2000 Main menu, select **System>Queued Download Actions**. The Smart Download Control dialog box opens.

The Information box displays the Smart Download **Rule** defined in the Site Parameters dialog box. The **Count** box displays the number of records queued for download.

The following information is shown for each download in the queue:

ID – The ID column shows a number that is automatically assigned to each download.



Entry Time – This field displays the time of each download request entry.

Scheduled Time – This field displays the scheduled download time of each timed download request entry.

Status – This field displays the status of each download request entry.

Description – This field displays the text description of each download request entry.

Site – This field displays the site name where the download request entry originated.

Controller – This field displays the panel name to which items are downloaded.

2. Click the **Refresh List** button to update the screen with new data as the download progresses.
3. Click **Done** to close the Smart Download Control dialog box.

Controlling and Monitoring P2000 Services

A service is a process that performs specific system functions and operates in the background without user intervention.

This section describes the procedures for controlling and monitoring P2000 services, as well as outlines the steps to customize which of these services will be automatically initiated at system startup.

Service Startup Configuration

Service Startup Configuration allows you to enable or disable any of the P2000 services at the start of communications, as well as set up recovery actions to take place if a service fails. If the *Auto Start* flag is enabled for a particular service, that service will start automatically and can be stopped or restarted using the Ser-

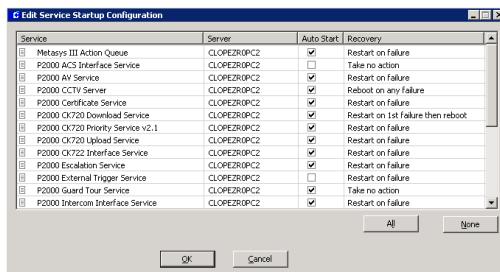
vice Control or the Service Monitor application. If the *Auto Start* flag is disabled, the service will not start automatically and will not display in Service Control.

By managing P2000 services, you can reduce system load by running only the required services. Before disabling a service, you must ensure that this service is not required to support a particular system function. If your system is registered for additional options, such as Guard Tour or BACnet, those services could also be enabled or disabled to start automatically when the Server starts up.

This function is accessed through the System Configuration window, which is password-protected, and can be performed from the Server or a workstation. We recommend defining User Roles to restrict access to this feature only to system administrators to prevent unauthorized personnel from stopping critical services.

To Edit Service Startup Configuration:

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the **Service Startup Configuration** icon and click **Edit**. The Edit Service Startup Configuration dialog box opens.



The list displays all services installed in the system, along with the **Server** name

and a check mark in the **Auto Start** column to indicate whether the service is automatically initiated at system startup. See the next section, “P2000 Services Definitions” for a brief description of these services.

- Select the service that you wish to auto start and click the associated check box in the **Auto Start** column.
- To auto start all services, click the **All** button, or click **None** to clear the selections and reselect the services individually.
- To restrict a service from starting automatically at system startup, select the service and click the associated check box to remove the check mark.
- To set up recovery actions to take place if a service fails, select the service, and under the **Recovery** column select from the drop-down list one of the following options:

Take no action – No action will take place after a service fails.

Restart on failure – Default option. Restarts the service after failure.

Restart on 1st failure then reboot – Restarts the service after first failure, then reboots the computer.

Restart on 2 failures then reboot – Restarts the service after two failures, then reboots the computer.

Reboot on any failure – Reboots the computer on any service failure.

- Click **OK** to return to the System Configuration window. The Service Control dialog box will be modified to display only the enabled services.

P2000 Services Definitions

Metasys III Action Queue – Provides the communication between SCT and CK722 panels.

P2000 ACS Interface Service – Provides the communication between the P2000 Server and the ACS Plaza system (service used by third party applications).

P2000 AV Service – Provides communication with Audio Visual components. Refer to the DVR option on page 282.

P2000 CCTV Server – Communicates with the CCTV and the DVR hardware. Refer to the CCTV and the DVR options, described in *Chapter 4: System Options*.

P2000 BACnet Service – Starts the BACnet Interface communication. The BACnet software has to be installed on a different computer than the P2000 server. Refer to the Metasys Integration (BACnet) option on page 233.

P2000 Certificate Service – Provides an interface between the CK722 and Microsoft Certificate Authority. The CK722 sends certificate requests to our service, our service sends the request to Microsoft Certificate Authority, and when the reply comes back, it sends it to the CK722.

P2000 CK720 Download Service – Performs Server downloads going to all CK705/CK720/CK721 panels in the system.

P2000 CK720 Priority Service v2.1 – Performs CK705/CK720/CK721 panel online and offline notifications (for panel version 2.1 and higher).

P2000 CK720 Upload Service – Performs CK705/CK720/CK721 panel uploads to the Server.

P2000 CK722 Interface Service – Performs communications between the P2000 Server and CK722 panels.

P2000 Escalation Service – Performs the alarm escalation function to monitor alarms that have the escalation option enabled.

P2000 External Trigger Service – Receives messages from external systems to be used as P2000 Host Event Triggers.

P2000 Guard Tour Service – Starts Guard Tour Service and receives real time event messages from RTLRoute services. Refer to the Guard Tour option on page 242.

P2000 Intercom Interface Service – Provides the communication with the Intercom hardware. Refer to the Intercom option on page 284.

P2000 MIS Interface Service – Imports and exports data for the MIS Interface. Refer to the MIS Interface option on page 231.

P2000 Muster Control Service – Monitors the status of all Muster Zones, and when a Muster is initiated, controls all the activities of the Muster.

P2000 Object Engine Service – Provides communication services with panels that use the BACnet protocol.

P2000 OPC Proxy Service – Provides the communication between P2000 applications and certain servers, such as the CCTV Server or the OPC Server.

P2000 Periodic Service – Performs periodic tasks such as deleting old history, synchronizing time of panels with server, and enabling/disabling badges based upon badge start and void dates.

P2000 Remote Message Service – Receives messages from the local RTL Route Service and transmits these messages to the remote P2000 Remote Message Service. When receiving a remote message, the local Remote Message Service will process the message and pass it on to the local RTL Route Service for distribution to the local workstations.

P2000 Request Queue Service – Processes Request Queue entries into the P2000 database.

P2000 RTL Route Service – Routes all real-time messages to workstations and services. Also processes Host Events.

P2000 S321 SIO Handler Service – Performs communications between the P2000 Server and S321 panels. (Not available in this release.)

P2000 SIA Interface Service – Provides the communication with configured SIA devices.

P2000 Smart Download Service – Downloads badges to panels when changes are made to access groups and terminal groups. It also downloads entity and badge changes. In addition, controls badges with temporary access.

P2000 Stop and Search Service – Starts the Stop and Search service to evaluate whether a person needs to be searched (service used by third party applications).

P2000 Time and Attendance Interface Service – Provides the communication between the P2000 Server and the Time and Attendance system (service used by third party applications).

P2000 Watchdog Service – Monitors other P2000 services to verify that they are operating and generates an alarm when a P2000 service fails.

P2000 Work Schedule Service – Starts the Work Schedule service to monitor work schedule and generate history transactions as employees go on/off schedule (service used by third party applications).

P2000 XmlRpc Interface Service – Provides communication over the network, using the XML-RPC interface to communicate with remote devices such as building management components designed for Metasys system

extended architecture, or with Web Access servers.

P2000 XPortal Interface Service – Performs communications between the P2000 Server and Pelco DVRs (Endura and DX8100). It handles Host Event actions and processes alarms from the Pelco DVR. This service is not involved in video playback.

P2000 uses the following additional service, which is controlled using the Windows 2003 Administrative Tools application:

Internet Information Services (IIS) – Installed with Windows 2003 operating system to provide Web server capabilities. This service provides the communications with SCT, Web Access, and Metasys System Extended Architecture.

Starting and Stopping Service Control

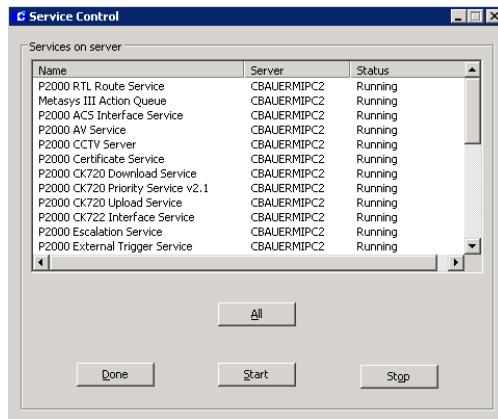
Service controls are provided specifically to stop and restart communications between panels and the Server to perform system maintenance functions, or during network troubleshooting operations. For example, the system administrator would be required to stop all communication services between panels and the Server when performing database backup and restore functions; or could stop uploads only between panels and the Server as part of system troubleshooting.

Service Control should be used only as directed by our Technical Support personnel, and should be performed only by a system administrator at the Server or workstation. This function is password protected.

Refer to “Controlling Services using Windows Administrative Tools” on page 316 to control IIS service.

To Stop or Start All Services:

- From the P2000 Main menu, select **System>Service Control**. You may be prompted for a password. The Service Control dialog box opens.



The Service Control dialog box displays all services installed in the system, along with the Server name and its current status, stopped or running.

- Click **All**, then click **Stop** or **Start**. If you click **Stop**, all services will be stopped and no communication will occur between the Server and the panels. If you click **Start**, all services will start running again.
- Click **Done**.

To Stop or Start a Specific Service:

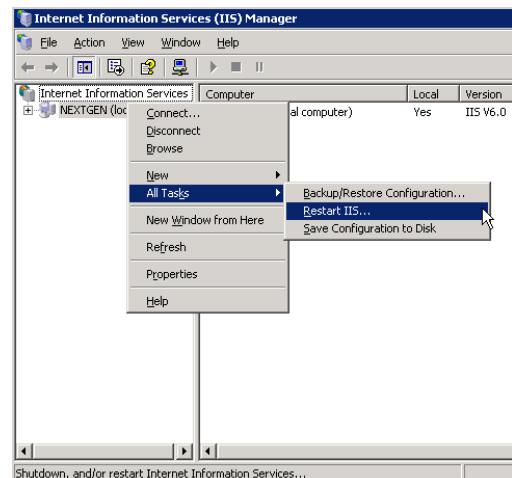
- Select the service to be stopped (or started) from the scrolling list and click **Stop** (or **Start**). Only the services selected will be stopped (or started) and the Stopped (or Running) status will display.
- Click **Done**.

Controlling Services using Windows Administrative Tools

In addition to the steps described earlier to stop ALL services to perform certain maintenance functions, you are also required to stop the IIS service using the Windows Administrative Tools application. The following section describes how to perform the procedure.

To Stop or Start IIS Service:

- On the Windows Server desktop, go to **Start>Programs>Administrative Tools>Internet Information Services (IIS) Manager**. The Internet Information Services (IIS) Manager window opens.



- On the left windowpane find the local computer and right-click to select **All Tasks>Restart IIS**. The Stop/Start/Restart dialog box opens.



3. Select from the drop-down list whether you wish to Start, Stop, or Restart the service, and click **OK**.
4. Close the Internet Information Services (IIS) Manager window.

Controlling Services through the Service Monitor

The **P2000 Service Monitor** application is automatically installed at the Server during initial software installation. This application is represented by a “traffic signal” icon located in the system tray (right side of the Windows taskbar).

Each color in the traffic signal represents the status of P2000 services:

Red – Indicates that all services are *Stopped*.

Green – Indicates that all services are *Running*.

Yellow – Indicates that at least one service is *Running* and/or one service is *Stopped*.

When you right-click the traffic signal icon, a dialog box opens where you can start, stop, and refresh P2000 services; or open the Service Control dialog box.



Note: The procedure to control services at redundancy systems might be different from the steps described here. Refer to your redundancy documentation for details.

Workstation Status

An operator can see which workstations are logged on. This is a display-only feature, and is helpful to determine who is logged on at what workstation, and at what time they logged on.

TIP: While this function might typically be performed by a system administrator, it may also be appropriate to a supervisor, shift leader, or building manager.

To View Workstation Status:

1. From the P2000 Main menu, select **System>Workstation Status**. The Workstation Status window opens.

Workstation Status						
Workstation	Logged In	User Name	Login Date/Time	Badging	Server	Partition
delta	Yes	Sjones	6/23/2008 3:11:13 PM	No	Yes	Super User
lopez	Yes	Cardkey	6/23/2008 2:44:58 PM	Yes	No	

The names of all workstations (and the Server) display in the Workstation column. The **Logged In** column indicates whether or not the workstations are currently logged on. The **Badging** column indicates if the workstations are configured as badging workstations. The **Server** column indi-

cates the workstations that operate as system Servers.

2. If this is a partitioned system, select the **Partition** you wish to view. All workstations active in the partition are displayed.
3. If the workstation is logged on, the **User Name** and **Login Date Time** are displayed.
4. Click **Done** to exit the window.

System Status

The System Status window is a dynamic display of the status of panels and associated devices configured in the system. This is a useful troubleshooting tool that allows you to quickly determine if panels and connected devices are communicating. If communications go down between the Server and the panels, the System Status window reports the last known status of the devices.

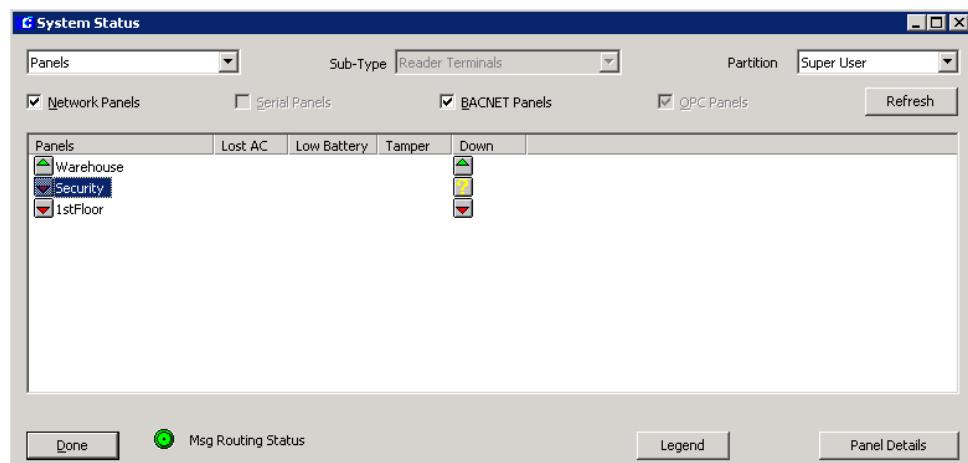
The System Status window is view only. You can manually change the status of a component using features accessed from the Control menu. See “Operator Controls” on page 172.

To Access the System Status Window:

1. From the P2000 Main menu, select **System>System Status**. The System Status window opens.
2. Select a component (Terminals, Inputs, Outputs, Panels, Logical, S300 Hardware, or Intrusion) from the drop-down list at the top left of the window. Information displayed for each component is presented at the end of this section.
3. If this is a partitioned system, select the **Partition** to which the component belongs.
4. Select the **Network Panels** (CK0705/CK720/CK721), **BACNET Panels** (CK722), and/or **OPC Panels** check box. The list of displayed devices will be limited according to the type of panel selected here.

Note: *The Serial Panels option is not available in this release.*

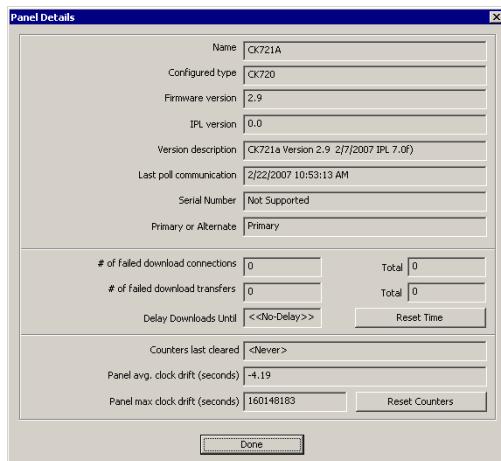
5. Click the **Refresh** button to manually update the system status display.



- To see icon definitions for the different condition indicators, click the **Legend** button at the bottom of the window.



- The System Status Legend dialog box opens displaying condition indicators associated with the selected component. Click **Done** to return to the System Status window.
- To display panel information, select the panel and click the **Panel Details** button. A Panel Details dialog box opens displaying current panel information.



Name – Displays the name given to the panel.

Configured type – Displays the panel type.

Firmware version – Displays the firmware version of the panel.

IPL version – Displays the IPL (Initial Program Load) version of the panel.

Version description – Displays the version description of the panel.

Last poll communication – Displays the last time the Server received information from the panel.

Serial Number – Displays the serial number assigned to the panel. Available only for S321 panels.

Primary or Alternate – Displays whether the Primary or Alternate connection is in use for a network panel.

of failed download connections – Displays the number of times the Server has failed to connect to this panel.

of failed download transfers – Displays the number of times an in-progress transfer was aborted.

Delay Downloads Until – Displays the time the Server will attempt the next download connection to this panel.

Reset Time – Click this button to immediately try a new download connection to this panel.

Counters last cleared – Displays the last time you clicked the Reset Counters button.

Panel avg. clock drift (seconds) – Displays the average time difference between the Server and the panel.

Panel max clock drift (seconds) – Displays the largest time difference between the Server and the panel.

Reset Counters – Click this button to reset the values to 0.

- Click **Done** to close the Panel Details dialog box and return to the System Status window.

Note: The Message Routing Status indicator at the bottom of the System Status window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.

10. Click **Done** to close the System Status window.

System Status – Terminals

Select **Terminals** from the drop-down list to monitor *Reader Terminals*, *Input Terminals* or *Output Terminals* (select the desired option from the **Sub-Type** drop-down list). All network panels in the system (the **Network Panels** check box must be selected) are listed by name in the Panels column. The terminals connected to the panels are displayed by number in the same row as their panel. (The numbers correspond directly to the terminal number assigned when configuring the terminals. For more information see “Create and Configure Terminals” on page 58.) When you place the cursor over the terminal icon, the terminal name displays in a popup box.

System Status – Inputs

When you select **Inputs** from the drop-down list, all terminals in the system for the type of panel selected (**Network Panels** and/or **BAC-NET Panels**), are listed by name in the Terminals column.

A status icon is represented for each possible input state. If no icons are present, no input points are associated with the terminal.

The input points are displayed by number in the terminal row. When you place the cursor over the input point icon, the input point name displays in a popup box.

System Status – Outputs

When you select **Outputs** from the drop-down list, all terminals in the system for the type of panel selected (**Network Panels** and/or **BAC-NET Panels**), are listed by name in the Terminals column.

A status icon is represented for each possible output state. The output points are displayed by number in the terminal row. When you place the cursor over the output point icon, the output point name displays in a popup box.

Note: To display outputs associated with Network Panels, you must select “Log Output Status Message” in the Edit Terminal, Flags tab (see page 60).

System Status – Panels

When you select **Panels** from the drop-down list, all panels in the system for the type of panel selected (**Network Panels** and/or **BAC-NET Panels**), are listed by name in the Panels column.

This display indicates the status of each panel, and also indicates soft alarm conditions associated with network panels (*Lost AC*, *Low Battery*, *Tamper* and *Down*). Each defined panel is listed with a row of icons that represent each possible panel state. You must enable panel soft alarms to display the conditions on the System Status window.

System Status – Logical

Select **Logical** from the drop-down list to monitor one of the following device types selected from the **Sub-Type** down-down list:

ACO – All Access Control Object terminals connected to the panels (**BACNET Panels** only), are displayed by number in the same

row as their panel. The system will display the status of the Access Control Object terminals. The Terminal Ranges column indicates the number of terminals per panel.

Door Terminals – All door terminals connected to the panels (**BACNET Panels** only), are displayed by number in the same row as their panel. The system will display the status of the Door Sequence terminals. The Terminal Ranges column indicates the number of terminals per panel.

Mustering Zones – The system displays the zone hardware status (panels or terminals) of each Muster Zone. Refer to “Muster Zone Status and Control Field Definitions” on page 195.

Security Level Terminals – All panels that have security level terminals in the system, for the type of panel selected, are listed by name in the Panels column. All security level terminals are displayed in their respective panel row, showing the security level setting for each terminal. A number 0 indicates the security level is not used or is not assigned. The Type column indicates whether these terminals are ACO (Access Control Objects) or DSO (Door Sequence Objects). The Terminal Ranges column indicates the number of terminals per panel.

System Status – S300 Hardware

Select **S300 Hardware** from the drop-down list to monitor devices associated with the S300 hardware. You must select *Generic, I/O Module* or *Reader* from the **Sub-Type** drop-down list. All BACNET panels in the system (the **BACNET Panels** check box must be selected) are listed by name in the Panels column. The terminals connected to the panels are displayed by number in the same row as their panel. The numbers correspond directly to the terminal number assigned when config-

uring the terminals. The Trunk column indicates the trunk number (1 or 2) associated with the panel. The Terminal Ranges column indicates the number of terminals per panel.

System Status – Intrusion

Select **Intrusion** from the drop-down list to monitor the status of intrusion items associated with BACNET and/or OPC Panels (the **BACNET Panels** and/or **OPC Panels** check box must be selected). Select from the **Sub-Type** drop-down list one of the following options:

Intrusion Area – All intrusion areas associated to the panel are displayed by number in the same row as their panel. The system will display the status of each intrusion area.

Intrusion Announcer – All intrusion annunciator devices associated to the panel are displayed by number in the same row as their panel. The system will display the status of each intrusion announciator.

Intrusion Zone – All intrusion zones associated to the panel are displayed by number in the same row as their panel. The system will display the status of each intrusion zone.

Writing the Controller Database to Flash Memory

CK721-A and CK722 panels’ RAM based database is automatically backed up and stored at the panel level flash memory according to their auto database backup archive schedule. With the Controller Write DB To Flash function, you can manually archive the panel’s RAM based database more frequently as major changes are made to the system database. For example, if you delete a number of badges from the system, it would be appropriate to write the panel’s RAM based database to flash

memory. That way, if the RAM based database is lost (before the auto database backup archive schedule is performed), the most recent saved flash memory database archive will contain the latest badge information.

Since the data stored at each panel is different, this procedure must be performed for each panel in the system.

This function is password protected and must be performed only by a system administrator.

To Manually Write the Controller Database to Flash Memory:

1. From the P2000 Main menu, select **System>Controller Write DB To Flash**. You may be prompted for a password. The Controller Write DB to Flash dialog box opens.



2. Select the **Panel To Write** from the drop-down list.
3. Click **Write**. All data stored in the panel's RAM is backed up to its flash memory.
4. Click **Done**.

Updating CK705/CK720 Panels

This function updates CK705/CK720 panel firmware. In addition, you can also update terminal firmware, as long as the terminals are installed into CK705/CK720 panels of version 2.3 or higher. *Johnson Controls* will provide the update file, along with documented instructions. This function should be performed only

by a system administrator at the Server, and is password protected.

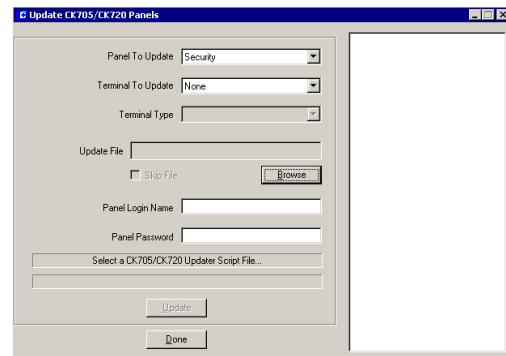
This function requires the login names and passwords of all CK705/CK720 panels in the system. The default panel name and password for the panel is given in the CK705 or CK720 Installation and Operation manuals. If your panel's login name has been changed, you must enter the new name and password to perform this function.



CAUTION *Each version upgrade is delivered with separate documented instructions (Software Release Notes). Be sure to read and follow all specific upgrade documentation instructions before performing an update.*

To Update CK705/CK720 Panels and Terminals:

1. From the P2000 Main menu, select **System>Update CK705/CK720 Panels**. You may be prompted for a password. The Update CK705/CK720 Panels dialog box opens.



2. Select the **Panel To Update** from the drop-down list.
3. If the system detects that this is a panel version 2.3 or higher, the **Terminal to Update** drop-down list will display all the

terminals connected to the panel selected. Select the terminal name you wish to update. If you do not wish to update terminal firmware, select **None**.

4. If you select to update a specific terminal, you must select the **Terminal Type** that you wish to update.
5. Click **Browse** to navigate to the directory in which the update file resides. This file will be typically provided by *Johnson Controls* on a CD.
6. Select the file from the CD. The file name will display in the **Update File** field.
7. Enter the **Panel Login Name** as programmed at the CK705/CK720 panel.
8. Enter the **Panel Password** as programmed at the CK705/CK720 panel.
9. Click **Update**. The information contained in the update file is downloaded to the panel or terminal selected. This process may take several minutes.
10. After the update process is complete, select another terminal name and type and click **Update**. If the **Skip File** check box is selected, the system uses the same update file name.
11. After the update process is complete, click **Done** to close the dialog box.

Note: After a panel version upgrade, open the System Status window to check the status of the panel. If the panel shows a “panel version mismatch” condition indicator, you must open the Edit Panel dialog box and in the General tab change the panel’s type to the updated panel’s firmware version. Then wait until the panel is shown as up in the System Status window.

12. Follow the procedure on page 309 to download data items to the recently updated panel.

Updating CK722 Panels

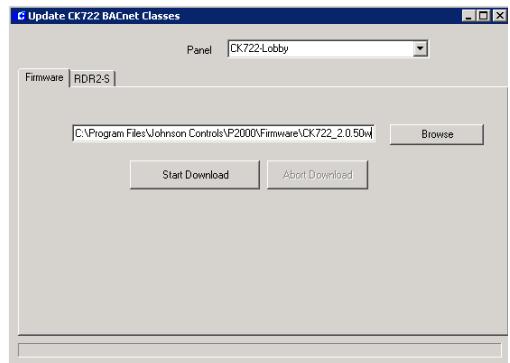
This function updates CK722 panel firmware. In addition, you can also perform firmware updates of any RDR2S or Keypad Display Module (KDM) connected to CK722 panels. *Johnson Controls* will provide the update file, along with documented instructions. This function should be performed only by a system administrator.



Each version upgrade is delivered with separate documented instructions (Software Release Notes). Be sure to read and follow all specific upgrade documentation instructions before performing an update.

To Update CK722 Panels:

1. From the P2000 Main menu, select **System>Update CK722 BACnet Classes**. The Update CK722 BACnet Classes dialog box opens.



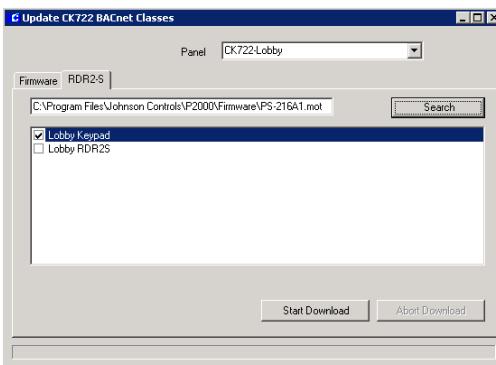
2. From the **Panel** drop-down list, select the panel name you wish to update.
3. Make sure the **Firmware** tab is selected.
4. Click the **Browse** button to navigate to the directory in which the update file resides.

This file will be typically provided by *Johnson Controls* on a CD.

5. Select the <name>.fwu file and click **Open**. The file name will display.
6. Click the **Start Download** button. The status bar at the bottom of the dialog box will indicate the progress during the download.
7. After the download is completed, the CK722 panel will reboot automatically. The message “*The firmware successfully upgrade*” will display above the status bar.
8. If while downloading you decide to cancel the process, click the **Abort Download** button. The download process will be terminated immediately.

To Update Modules Used with CK722 Panels:

1. From the P2000 Main menu, select **System>Update CK722 BACnet Classes**. The Update CK722 BACnet Classes dialog box appears.



2. From the **Panel** drop-down list, select the panel name you wish to update.
3. Make sure the **RDR2-S** tab is selected.

4. Click the **Search** button to navigate to the directory in which the update file resides. This file will be typically provided by *Johnson Controls* on a CD.
5. Select the <name>.mot file and click **Open**. The file name will display.
6. In the list box, select the check box next to the RDR2S or KDM module you wish to update.
7. Click the **Start Download** button. The status bar at the bottom of the dialog box will indicate the progress during the download.
8. After the download is completed, the CK722 panel will reboot automatically. The message “*The firmware successfully upgrade*” will display above the status bar.
9. If while downloading you decide to cancel the process, click the **Abort Download** button. The download process will be terminated immediately.

Updating S321 Panels

Note: S321 Panels are not available in this release.

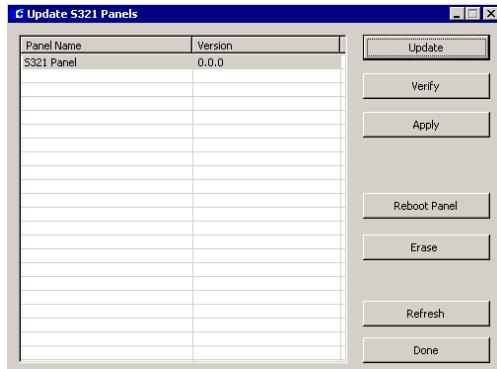
This function updates S321 panel firmware. *Johnson Controls* will provide the update file, along with documented instructions. This function should be performed only by a system administrator, and is password protected.



Each version upgrade is delivered with separate documented instructions (Software Release Notes). Be sure to read and follow all specific upgrade documentation instructions before performing an update.

To Update S321 Panels:

- From the P2000 Main menu, select **System>Update S321 Panels**. You may be prompted for a password. The Update S321 Panels dialog box opens.



- Select from the list box the panel name you wish to update. You can select multiple names by holding down the <**Ctrl**> key.

Note: Open the Real Time List to monitor panel update transactions as they occur.

- Click the **Update** button to navigate to the directory in which the update file resides. This file will be typically provided by Johnson Controls on a CD.
- Select the <name>.bz2 file and click **Open**. The information contained in the update file is queued. This process may take several minutes. After this process is completed, the Real Time List will display a *Code Image download success* message.
- Click the **Verify** button to send a verification command to the panel. The Real Time List will display a *Code Image download success* message to indicate that the verification was successfully completed.

- Click the **Apply** button. The panel reboots, it takes about 2 minutes to download the code into the flash. The Real Time List will indicate that the panel and associated devices are down. After the code is downloaded, the panel will reboot again.
- When the panel is back online, click the **Refresh** button. The Version column in the list box will display the updated version number.

Note: The **Reboot Panel** button is provided to force the panel to restart, for example in cases when the panel is not functioning properly. The **Erase** button is provided to delete the configuration data at the panel. After you click **Erase**, the panel reboots; when it comes back online, you should proceed to download data items to the panel, using the procedure on page 309.

- After the update process is complete, click **Done** to close the dialog box.

Database Maintenance

You can perform a database backup, empty various data histories, load an archived database from backup, or reset event counters from the Database Maintenance dialog box. This function is password protected and should be accessible only by a system administrator or a designee.

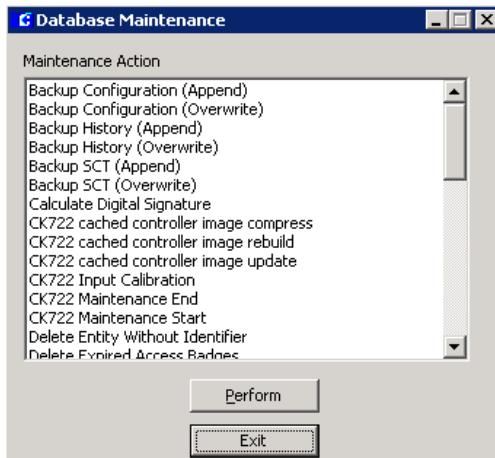
Note: Some Database Maintenance tasks, such as "Shrink Database," can only be performed by users that are members of the Windows or PEGASYS Administrators group, refer to "Setting Up User Accounts" on page 23.

You may have scheduled certain functions like database backup or Empty Audit History to occur automatically. This option lets you over-

ride the system and perform manual maintenance.

To Perform Database Maintenance Functions:

- From the P2000 Main menu, select **System>Database Maintenance**. You may be prompted to enter a password. The Database Maintenance dialog box opens.



- Under **Maintenance Action**, select the function you wish to perform. Refer to the next section, “Database Maintenance Actions” for a description of each function.
- Click **Perform**. A confirming message box will display. Depending on your selection, click the appropriate action.
- Click **Exit**.

Database Maintenance Actions

Backup Configuration (Append) – Creates a backup of P2000 configurable items such as entities and hardware devices, without overwriting existing backups.

Backup Configuration (Overwrite) – Creates a backup of P2000 configurable items such as

entities and hardware devices, by overwriting existing backups.

Backup History (Append) – Creates a backup of P2000 audit, alarm, and transaction history without overwriting existing backups.

Backup History (Overwrite) – Creates a backup of P2000 audit, alarm, and transaction history by overwriting existing backups.

Backup SCT (Append) – Creates a backup of items that were configured in SCT such as CK722 hardware devices, without overwriting existing backups.

Backup SCT (Overwrite) – Creates a backup of items that were configured in SCT such as CK722 hardware devices, by overwriting existing backups.

Note: For more information on the previous Backup functions, refer to “Database Backup” on page 329.

Calculate Digital Signature – Validates the digital signatures, points out discrepancies, and corrects the discrepancies to ensure that records have a valid digital signature. This function is available if your system is registered for the FDA Part 11 option. Refer to “FDA Part 11” on page 283. See also “System Validation” on page 334.

CK722 cached controller image compress – Removes download commands stored in the CK722 download table that are no longer needed, such as an entity deleted.

CK722 cached controller image rebuild – Erases the entire SQLite database and forces all the data stored in the CK722 download table to be written to the SQLite tables and then rebuilds the SQLite tables.

CK722 cached controller image update – Causes the information stored in the CK722

download table, since the last update, to be processed and used to update the CK722 database stored in the SQLite database files.

CK722 Input Calibration – Gives you the option of calibrating 4-state input points or uncalibrating 2-state input points associated with CK722 panels.

CK722 Maintenance End – Brings the selected CK722 controller(s) back online from the host point of view.

CK722 Maintenance Start – Takes the selected CK722 controller(s) offline from the host point of view.

Delete Entity Without Identifier – All entities that have no assigned identifier will be deleted from the database.

Delete Expired Access Badges – All access badges that have expired will be deleted from the database. Each access badge has a validation period (defined in Access Profiles), during which the access badge is valid.

Delete Unused Access Groups – All unused access groups (i.e. access groups not assigned to any Access Profile) will be deleted from the database.

Delete Unused Access Profiles – All unused access profiles (i.e. access profiles not assigned to any identifier) will be deleted from the database.

Delete Unused Intrusion Groups – All unused intrusion groups (i.e. intrusion groups not assigned to any Access Profile) will be deleted from the database.

Empty Alarms – Removes all alarms from the alarm queue. This action will typically be performed when the queue displays alarms that cannot be secured, and thus cannot be discarded.



*The Empty Alarms action does not remove selected alarms. **ALL** alarms will be deleted, so proceed with caution.*

Empty Alarms History – All alarms in the Alarms History database table will be deleted.



This action should only be performed with the aid of a Johnson Controls Technical Support specialist.

Empty Audit History – Purges all audit history data from the database. The audit history data is time/date stamped records of user actions.



This action should only be performed with the aid of a Johnson Controls Technical Support specialist.

Empty Download Queue – Purges the actions from the Download Queue. This queue downloads P2000 data to selected panels. This function will typically be performed when a panel is no longer in use, but the queue still lists downloads for that panel.

Empty Guard Tour Note – Purges all guard tour notes from the P2000 database. P2000 can also be configured to remove these notes after a pre-determined amount of time, refer to “Guard Tour Notes” on page 255.

Empty P2000EntityConfig Archive Database – Removes the data that was archived in the P2000EntityConfig database, such as entities and hardware devices. This database is used for running P2000 reports.

Empty P2000History Archive Database – Removes the data that was archived in the P2000History database, such as audit, alarm, and transaction history. This database is used for running P2000 reports.

Empty Saved Muster Data – Purges all of the muster data from the database. This data is normally saved to the database for evaluation once a Muster is terminated.

Empty Smart Download Queue – Purges the actions from the Smart Download Queue. For more information, refer to “Smart Download Control” on page 311.

Empty Transaction History – Purges the Transaction History data from the database. Transactions indicate some form of system activity. They can include such items as access requests and general system messages such as when a panel loses communication with a reader. Typically, transactions represent communication initiated at field panels and sent to the P2000 Server.



This action should only be performed with the aid of a Johnson Controls Technical Support specialist.

FDA Backup Performed – Informs the P2000 system that the FDA backup is archived, in accordance with company policies to meet FDA Part 11 record retention policy. For more information, refer to “FDA Part 11 Backups” on page 332.

Load CK722 Identifier Format – Loads identifier formats so SCT can make them available for use in CK722 panels.

Load P2000EntityConfig Archive Database from Backup – Loads the data that was archived in the P2000EntityConfig database, such as entities and hardware devices. This database is used for running P2000 reports.

Load P2000History Archive Database from Backup – Loads the data that was archived in the P2000History database, such as audit, alarm, and transaction history. This database is used for running P2000 reports.

Remove Access Profile from Disabled Identifiers

Identifiers – Removes access profiles from disabled identifiers. This in turn allows the Delete Unused Access Profiles command to be used more efficiently.

Remove Access/Intrusion Groups from Unused Access Profiles

Access Profiles – Removes access and/or intrusion groups from unused access profiles. This in turn allows the Delete Unused Access Groups and Delete Unused Intrusion Groups commands to be used more efficiently.

Reset Counters to Zero – All values in the Event Counters list will be reset to zero. For more information, refer to “Counting Events” on page 211.

Reset Reserved Autobadge Numbers – Resets these numbers, making them available. An available number can be assigned to a badge. A reserved autobadge number is a number that has already been assigned, but a badge has not yet been issued.

Set all Input Status to Unknown – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

Set all Output Status to Unknown – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

Set all Panel Status to Unknown – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

Set all Terminal Status to Unknown – Used if a panel is down (e.g. for maintenance) and alarms are being generated.

Shrink Database – Commands SQL Server to free up space in the database. This process is normally performed automatically at various intervals.

Validate Digital Signature – Ensures the integrity of all records and provides evidence when records have been altered. A digital signature

verifies that unauthorized users have not modified the values in the columns of a record. This function is available if your system is registered for the FDA Part 11 option. Refer to “FDA Part 11” on page 283. See also “System Validation” on page 334.

Database Backup

The P2000 system should be backed up on a regular basis. Backups can be performed using several supplied methods, and can be made to any backup device supported by Microsoft SQL Server. Tape backup systems are usually the most cost-effective while also being fast and reliable, and are the only type that allows backups larger than a single media.



To avoid serious operational problems, you must back up or restore the SCT database every time you back up or restore the P2000 databases. Refer to the System Configuration Tool (SCT) Manual.

The P2000 History database should be backed up frequently, while the P2000 Entity Configuration database should only be backed up when configuration items are modified. Backups can be performed without stopping the P2000 communication services; therefore the system will remain operational during the backup process.

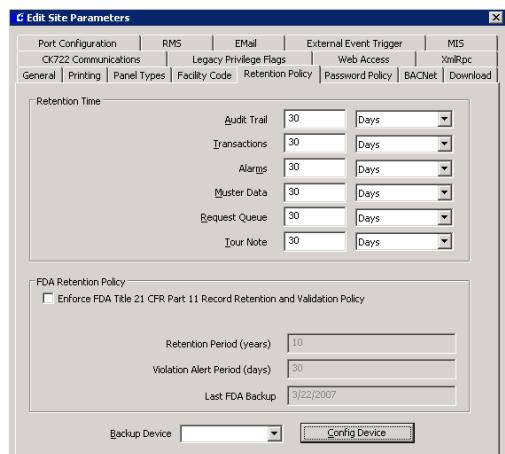
This function should be performed by a system administrator.

Note: Badge layouts that are created using the ID Server software option, cannot be backed up using any of the Database Maintenance backup options. To maintain up-to-date backups of your Video Imaging layout files, refer to the Video Imaging manual that was shipped with your option.

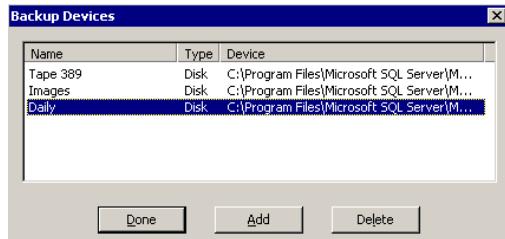
Configuring a Backup Device

- From the System Configuration window, select **Site Parameters** and click **Edit**. The Edit Site Parameters dialog box opens.
- Click the **Retention Policy** tab.

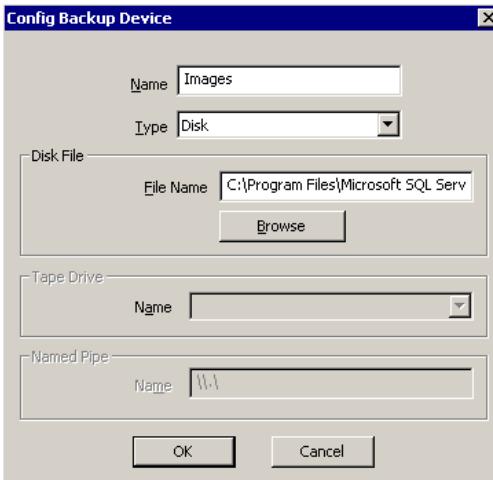
Note: Configuring a Backup Device can only be performed at the Server.



- At the bottom of the window, select a **Backup Device** from the drop-down list. If no devices are listed, or you want to add a new one, click the **Config Device** button. The Backup Devices dialog box opens.



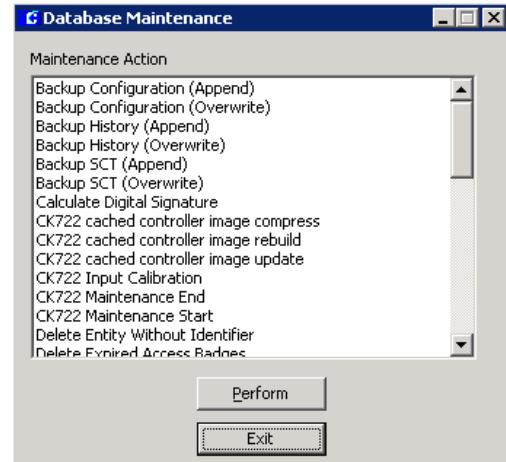
- Click the **Add** button. The Config Backup Device dialog box opens.



5. Enter a descriptive **Name** for the device.
6. Select the **Type** of backup device from the drop-down list. Options include: Disk, Tape, and Pipe.
7. If you select **Disk**, you must enter in the Disk File box, a valid path and file name for the backup file.
8. If you select **Tape**, click the drop-down button in the Tape Drive box, and select from the available Windows tape devices.
9. If you select **Pipe**, you must enter in the Named Pipe box, a valid system pipe name. This option is provided to interface with third-party backup software.
10. Click **OK** to save your settings. The new device will be listed in the Backup Devices dialog box and will also display in the Backup Device drop-down list of the Edit Site Parameters dialog box.
11. To remove a device, select it and click **Delete**.
12. Click **Done** to close the Backup Devices dialog box.

To Perform Manual Backups:

1. From the P2000 Main menu, select **System>Database Maintenance**. You may be prompted to enter a password. The Database Maintenance dialog box appears.



2. Select one of the following backup functions:
 - Backup Configuration (Append or Overwrite)
 - Backup History (Append or Overwrite)
 - Backup SCT (Append or Overwrite)

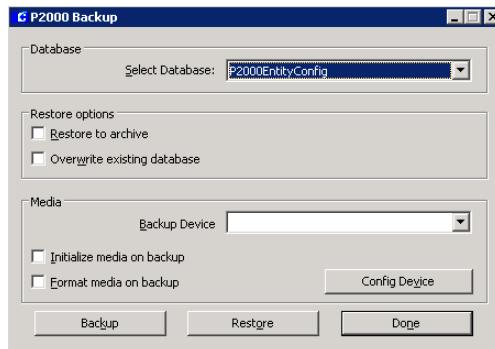
Refer to “Database Maintenance Actions” on page 326 for a description of each of these backup operations.
3. Click **Perform**. Since this action cannot be undone, a verification message displays to confirm your action. Click **Yes** if you wish to perform the backup operation.
4. The P2000 Backup utility will open and immediately begin the backup. The P2000 Backup utility will exit when the backup is complete.
5. Click **Exit** to close the Database Maintenance dialog box.

Advanced Backups

Backups can also be performed using the stand-alone P2000 Backup utility located in the “Bin” directory of the P2000 software installation.

Note: Advanced backups must be performed at the Server.

- From your Windows desktop, select **Start>Programs>Johnson Controls>P2000 Workstation>Launch Backup**. The P2000 Backup dialog box opens.



- From the **Select Database** drop-down list, select the database you wish to back up.
- In the Media box, select a **Backup Device** from the drop-down list. If you wish to add a new device, click the **Config Device** button and follow the steps provided in “Configuring a Backup Device” on page 329.

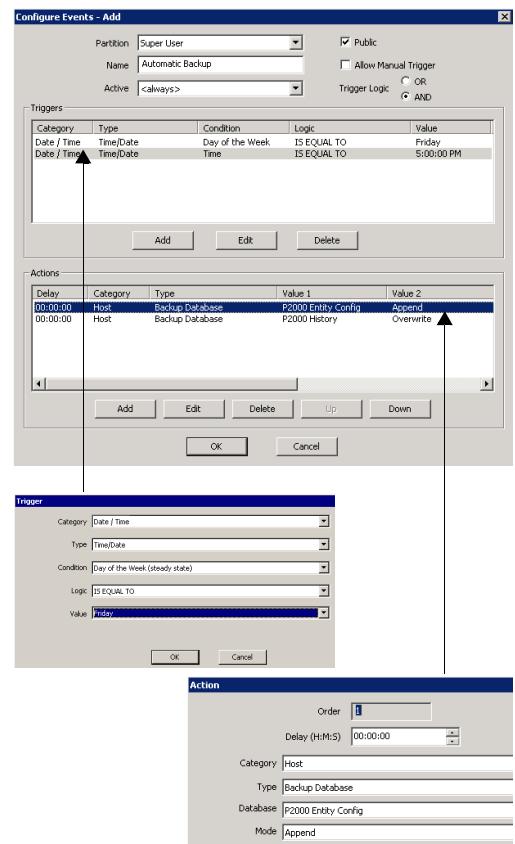
Note: The **Initialize media on backup** and **Format media on backup** options are provided to allow older backup media to be reused. For more information on these options, refer to the Microsoft SQL Server documentation.

- Click **Backup** to start the backup process.

- Click **Done** when the backup operation finishes.

Automatic Backups

Backups can be configured as P2000 event actions to allow automatic backups, based on a time setting or any other P2000 event trigger. In the following example an event has been programmed to back up the database (the action) every Friday at 5:00 P.M. (the trigger). For more detail information refer to “Creating Events” on page 206.



Program this event trigger, as you would any other event triggers in the system, giving it a descriptive name, and selecting a partition and time zone. Make sure you select **AND** in the

Trigger Logic field to create more than one condition to be met to activate this trigger.

Two conditions have been defined in the Triggers box: first you select the Day of the Week condition to be equal to Friday, then you select a Time condition to be equal to 5:00 P.M.

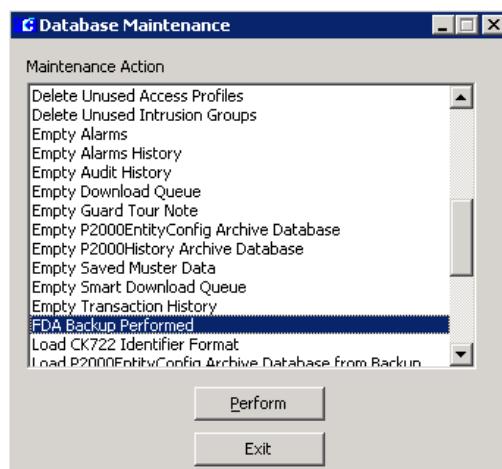
In the Actions box, two actions have been defined: one to backup the P2000 Entity Configuration database, and the second to backup the P2000 History database. Make sure you select Category “Host” and Type “Backup Database” in the Action dialog box.

FDA Part 11 Backups

Depending on the parameters defined in the Retention Policy tab of Site Parameters (page 34), you must perform periodic backups to comply with FDA Part 11 record retention requirements. Backups must be done using the standard backup procedures described in “Database Backup” on page 329.

Once the backup process has been completed, use the following steps to inform the P2000 system that the backup is archived, in accordance with your company policies to meet FDA Part 11 record retention policy.

- From the P2000 Main menu, select **System>Database Maintenance**. You may be prompted to enter a password. The Database Maintenance dialog box opens.



- Select **FDA Backup Performed** from the Maintenance Action list.
- Click **Perform**. Since this action cannot be undone, a verification message displays to confirm your action. Click **Yes** to continue.
- A message displays to confirm that you have just completed a backup, which will be archived according to your company policies to meet FDA Part 11 record retention requirements. Click **OK** to confirm. The *Last FDA Backup* field in the Retention Policy tab of Site Parameters, see page 34, will be updated to match the current system date. Any FDA Retention Policy alarms will change their alarm status to *Secure*.
- Click **Exit** to close the Database Maintenance dialog box.

Database Restore

Under normal operating conditions, the P2000 database should never need to be restored, but if the database is lost it can be restored from a recent backup, using the P2000 Backup utility. An older P2000 database can also be restored to an archive database for the purpose of printing reports or examining old settings, without affecting the currently active P2000 system.



Restoring the database can only be performed at the Server. If you restore the database to a different Server other than where it was originally backed up, you will need to contact Technical Support for a new Registration Key, and you will also need to reconfigure your Server (DB and COMM), see "Site Parameters" on page 29.

A non-archive restore can only be performed when all P2000 applications on all workstations and the Server have exited, and the P2000 communication services have been stopped (see “Starting and Stopping Service Control” on page 315 and “Controlling Services using Windows Administrative Tools” on page 316).

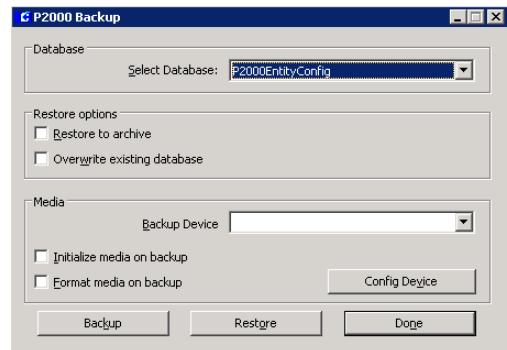


To avoid serious operational problems, you must back up or restore the SCT database every time you back up or restore the P2000 databases. Refer to the System Configuration Tool (SCT) Manual.

The **P2000 Service Monitor** application must also be shutdown at the Server. Do this by right clicking the “traffic signal” icon located in the system tray (right side of the Windows taskbar), if it exists, and selecting “Quit” from the menu. All P2000 communication services and applications can be restarted after the restore process finishes. It is recommended that all panels in the system be downloaded immediately after a database restore (see “Downloading Data to Panels” on page 309).

To Restore the Database:

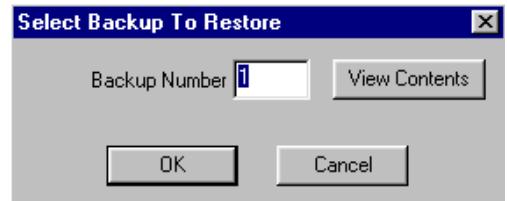
- From your Windows desktop, select **Start>Programs>Johnson Controls>P2000 Workstation>Launch Backup**. The P2000 Backup dialog box opens.



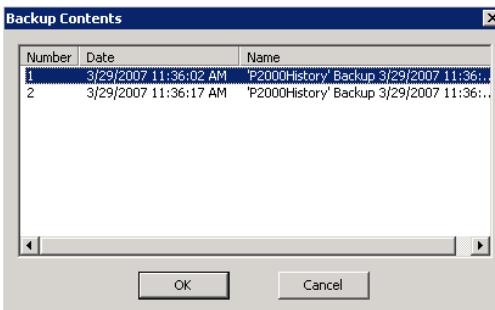
- From the **Select Database** drop-down list, select the database you wish to restore.
- In the Media box, select a **Backup Device** from the drop-down list. If you wish to add a new device, click the **Config Device** button and follow the steps provided in “Configuring a Backup Device” on page 329.
- Select **Restore to archive** to place the database in an offline location, that way reports can be generated using its data without affecting the currently operating system.

Note: *The Overwrite Existing Database option is provided to force the SQL Server to load a database, regardless of where it was created, normally only backups created on the current machine can be restored. This option should only be used when instructed to do so.*

- Click **Restore** to start the restore process. The Select Backup To Restore dialog box opens.



- Click **View Contents**. The Backup Contents dialog box opens.



- Select the backup you wish to restore, and click **OK**.
- A message will notify you that the restore process has been completed, click **OK** to return to the P2000 Backup dialog box.
- Click **Done** to close the P2000 Backup dialog box.

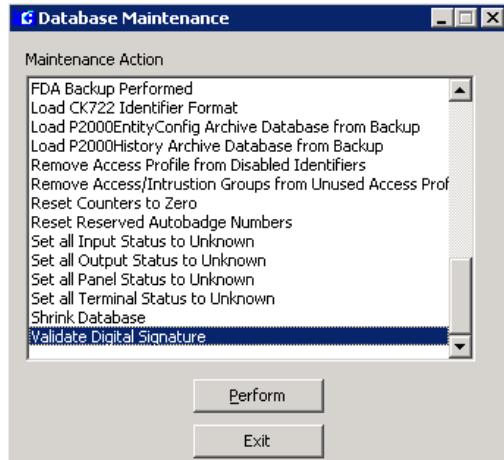
Note: After the database is restored, use the Service Startup Configuration application to enable or disable P2000 services as well as define the related recovery actions that were set up prior to the database restore, see page 312.

System Validation

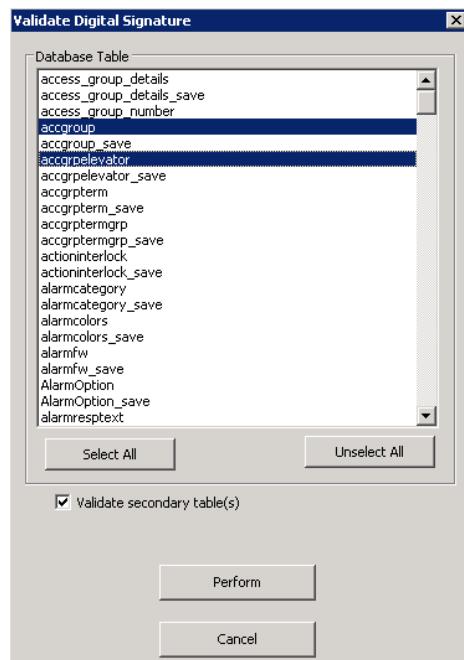
As a system administrator, you should schedule validation of your system on a regular basis to minimize the possibility of record tampering. The Validate Digital Signature feature ensures the integrity of all records and provides evidence when records have been altered. This function is available if your system is registered for the FDA Part 11 option. Refer to “FDA Part 11” on page 283.

Note: A digital signature verifies that unauthorized users have not modified the values in the columns of a record.

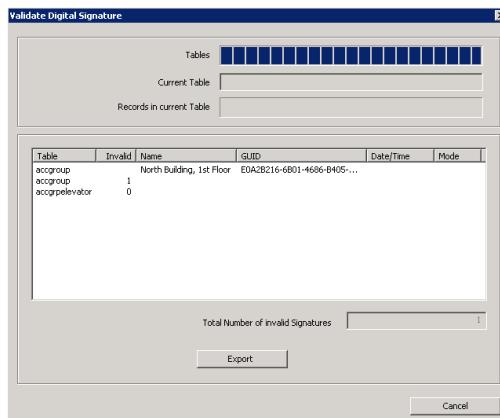
- From the P2000 Main menu, select **System>Database Maintenance**. You may be prompted to enter a password. The Database Maintenance dialog box opens.



- Select **Validate Digital Signature** from the Maintenance Action list.
- Click **Perform**. The Validate Digital Signature dialog box opens.



4. Select the database table you wish to verify. You can select to verify multiple tables, or click the **Select All** button to verify all tables at once.
5. To clear your selections, click the **Unselect All** button.
6. To verify secondary database tables, click the **Validate secondary table(s)** check box to add the secondary tables to the selection list. Clear this check box to remove all secondary tables from the list.
7. Click **Perform** to start the validation.



The list box displays the following information:

Table – The name of the table being validated.

Invalid – The number of invalid signatures found in the table.

Name – The name of the record, for example entity or panel name, as defined in the applicable P2000 application.

GUID – Global unique identifier of the record.

Date/Time – The date/time when modification took place. Only applicable for secondary tables, that is tables with the suffix _save.

Mode – The type of modification performed, such as delete (0), edit (1) or insert (2).

Total Number of Invalid Signatures – The number of records that have been tampered with.

8. Click the **Export** button to save the results in a file. This result file can be easily imported into, for example an *Microsoft Excel* file, and formatted according to your requirements.
9. Click **Cancel** to close the dialog box.
10. Click **Cancel** to return to the Database Maintenance dialog box.
11. Click **Exit** to close the Database Maintenance dialog box.

Note: In addition to using the “Validate Digital Signature” function, you can also use the “Calculate Digital Signature” function, which not only validates the digital signatures and points out discrepancies, but also corrects the discrepancies to ensure that records have a valid digital signature.

Request Queue View

The P2000 system provides a Request Queue database table that contains requests originated from external sources, such as Web Access requests (refer to “Web Access” on page 295).

Since external requests involve adding, deleting or modifying data in the P2000 database, the Request Queue has been designed to provide additional security measures in the request processing by checking all records before they are allowed to enter the P2000 system. The Request Queue allows P2000 users to intercept requests for the purpose of reviewing, editing, and finally letting request data enter the P2000 database system. The requests

are packaged as XML documents and saved into the P2000 Request Queue table.

Once these requests enter the P2000 database, a system administrator can use the Request Queue View application to resolve Request Queue-related problems. The Request Queue View window displays current requests or requests that were archived in the Request Queue database table. This tool is useful to, for example, verify which requests are pending for an approval, which requests have been completed, or have been rejected.

Note: *The amount of time that request records are kept in the Request Queue history table is defined in Site Parameters; see “Retention Policy Tab” on page 34.*

To View Request Queue Items:

- From the P2000 Main menu, select **System>Request Queue View**. The Request Queue View dialog box opens.

The list box displays the following information for each of the requests:

Create Time – Displays the date and time the request was submitted.

Expire Time – Displays the date and time the request will expire. This date is defined by the number of days entered in Site Parameters, see page 300.

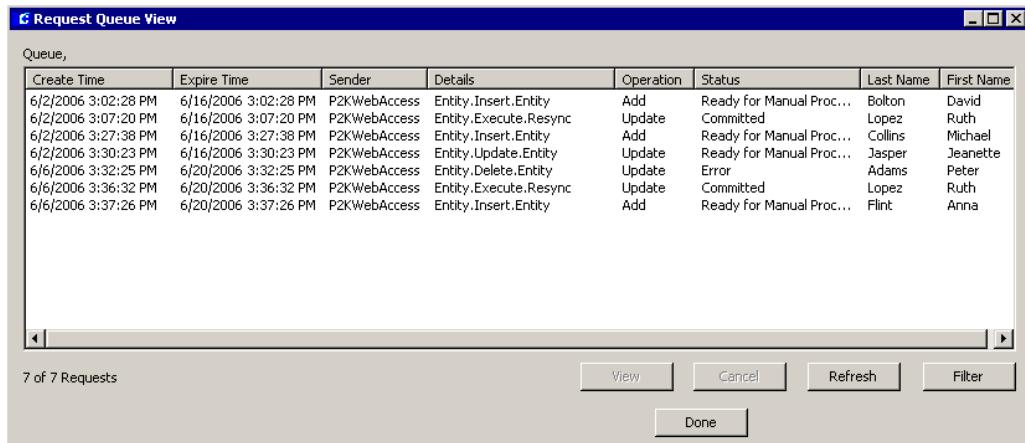
Sender – Displays the source that originated the request.

Details – This is the Sender application requested for processing.

Operation – This is the action (Add, Delete, Update) requested and that is associated with the Sender application.

Status – Displays one of the following:

- **Cancelled** – The request was cancelled before being processed.
- **Committed** – The request has been completed.
- **Error** – There is an error in the request.
- **Pending Approval 1** – The request is waiting to be approved by the required approver.
- **Pending Approval 2** – The request was approved by Approver 1, and requires approval of a second approver.



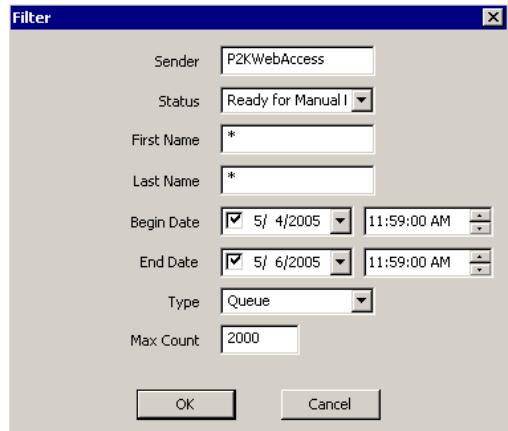
- **Pending Approval 3** – The request was approved by Approvers 1 and 2, and requires approval of a third approver.
 - **Processing** – The request is currently being processed.
 - **Ready for Auto Processing** – This request has been approved and is ready for automatic processing; without user intervention.
 - **Ready for Manual Processing** – This request has been approved and is ready for manual processing.
 - **Rejected** – The request was rejected.
- Last Name** – This is the last name of the entity specified in the request.
- First Name** – This is the first name of the entity specified in the request.

2. To display the details of a specific request, select the line item in the list box and click the **View** button. Refer to “Viewing Request Details” on page 338.
3. To cancel a specific request, select the line item in the list box and click the **Cancel** button, then click **Yes** to confirm.
4. To update the Request Queue View list box with new data, click the **Refresh** button.
5. To search for specific requests, click the **Filter** button and follow the instructions provided at the end of this section.
6. Click **Done** to close the Request Queue View dialog box.

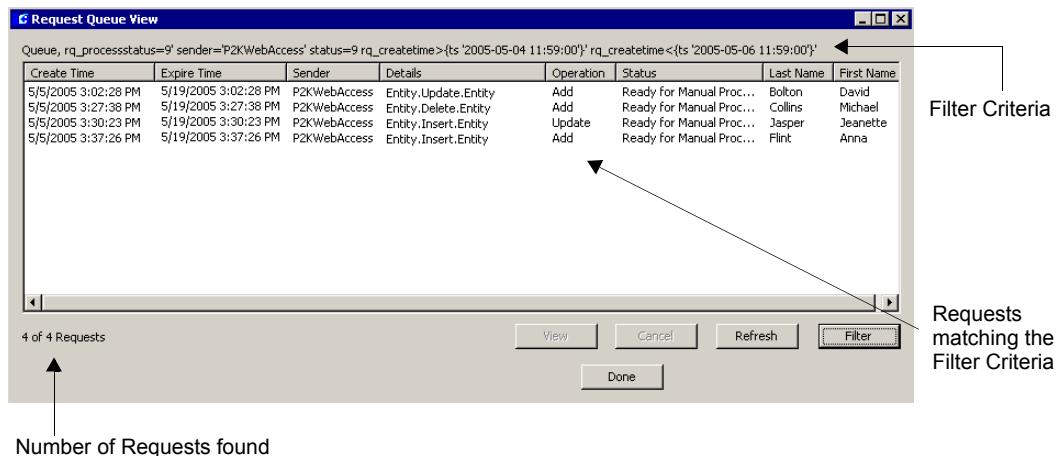
Searching Specific Requests

The Request Queue View application allows you to define filters to help you locate specific requests quickly and easily, and in that way reduce the number of requests displayed on screen. You can, for instance, define a filter to show only requests that were submitted on a specific date and that are waiting for manual processing.

1. In the Request Queue View dialog box, click the **Filter** button. The Filter dialog box opens. If you leave an asterisk (*) in a field, the filter criteria will include all records for that field.



2. Enter a **Sender** name to view only requests that were originated from that source.
3. Select from the **Status** drop-down list the specific request status you wish to view. For example you may want to review only requests that have been rejected or requests that require manual processing.
4. To view requests submitted for a specific entity, enter the **First Name** and/or **Last Name** of that entity.
5. To view requests that were submitted during a specific period, select a **Begin Date** and **End Date**. You may also enter a specific time if needed.
6. In the **Type** drop-down list, select whether you wish to view requests that are currently on **Queue** or requests that are archived in the **History** table.
7. In the **Max Count** field, enter the number of records you wish to display in the list.
8. Click **OK** to begin the search. The Request Queue View dialog box opens showing the results.

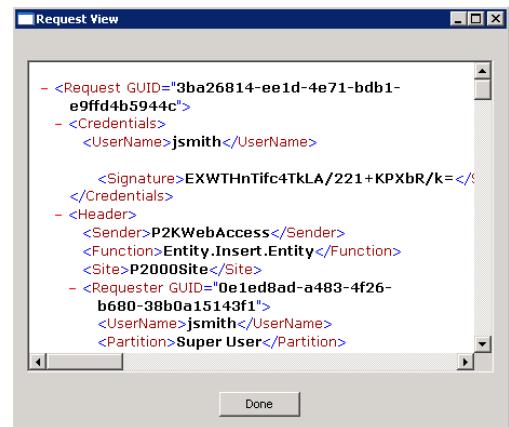


requests that meet the filter criteria and the number of requests found.

9. To display the details of a specific request, select the line item in the list box and click the **View** button. Refer to the next section "Viewing Request Details".
10. To restore the list to display all requests, you can either close and then open the Request Queue View dialog box, or click the **Filter** button and select to display all requests.

Viewing Request Details

1. In the Request Queue View dialog box, select the individual request you wish to display and click the **View** button. The Request View window opens displaying information in XML format.



The XML document contains information about the originator of the request and information regarding the actual request.

2. After reviewing the request details, click **Done** to close the window.

Chapter 6: System Reports

The P2000 Report feature gives you access to system data. Whether you want a printout of Entity information or a list of specific system transactions, there is most likely a P2000 Standard Report that will meet your needs. P2000 Standard Reports have been created using Crystal Reports®, most of which can be sorted to produce the data you need, and they can be reviewed on screen or printed. A complete list of P2000 Standard Reports is presented on page 342, along with a brief description of each and how they can be used. Some of the most commonly used reports are described in detail later in this chapter, including samples of each.

If you do not find a report that meets your needs within P2000 Standard Reports, you can create custom reports in your own copy of Crystal Reports. You can then import them into the P2000 system, or you can export a P2000 Standard Report, import it into Crystal, edit it, and then import it back into the P2000 system.

Note: While P2000 Standard Reports are very easy to understand and run, custom reports should be created by someone experienced with report design and operation, and should be attempted only by those qualified to do so. You must have a copy of Crystal Reports to create a custom report. See "Creating Custom Reports" on page 349 for detailed information.

This chapter includes the following topics:

- **Using P2000 Standard Reports**
- **P2000 Standard Report Definitions**
- **Selected Sample Reports**
- **Creating Custom Reports**

Using P2000 Standard Reports

For most applications, P2000 Standard Reports provide the fields you need to generate reports on system databases and activities. These reports are easily run from the P2000 Main menu, Report option. When you select a report from the Run Report list, the report previews on screen in a Crystal Reports window. You can use the Crystal Reports tool bar at the top of the window to scroll through pages of the report, resize the window, or search for a specific record. (Some preview options are available only in Crystal Reports.)

Prior to running any of the P2000 Standard Reports, you must use the **Load Language Reports** feature to load the report templates into the database. The steps to complete this process are presented in the following section.

To Load P2000 Reports:

1. From the P2000 Main menu, select **Report>Load Language Reports**. The Load Language Reports dialog box displays.



- Select the desired language from the drop-down list. **English** is the default selection.

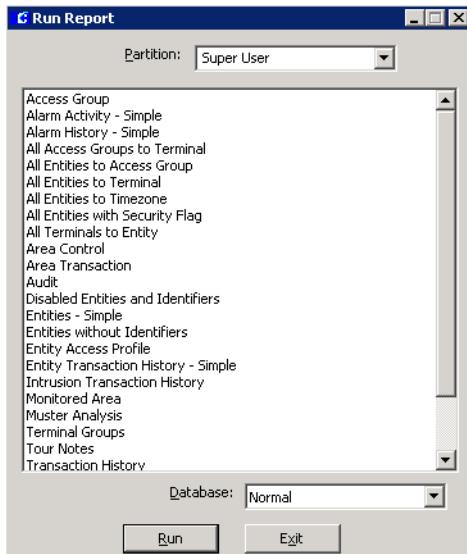
This feature also allows you to load reports in other languages. If your facility has purchased a foreign language option, select the desired language (previously installed from the foreign language CD).

Note: Some translated reports may have to be modified using Crystal Reports to fix truncated text issues. In addition, due to a parameter value limitation in Crystal Reports, some reports have been hard-coded and have not been translated, these reports also need to be modified using Crystal Reports.

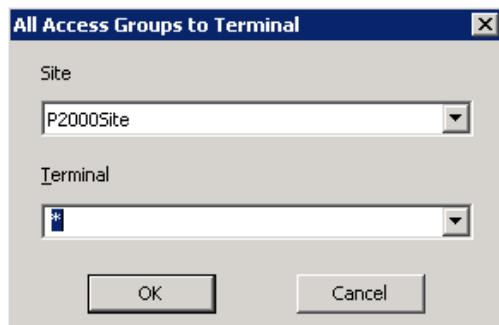
- Click **Load** to load the reports into the database, then click **OK**.
- Click **Done**. Once the selected language reports are loaded you do not need to perform this procedure again.

To Run a Standard Report:

- From the P2000 Main menu, select **Report>Run Report**. The Run Report dialog box appears.



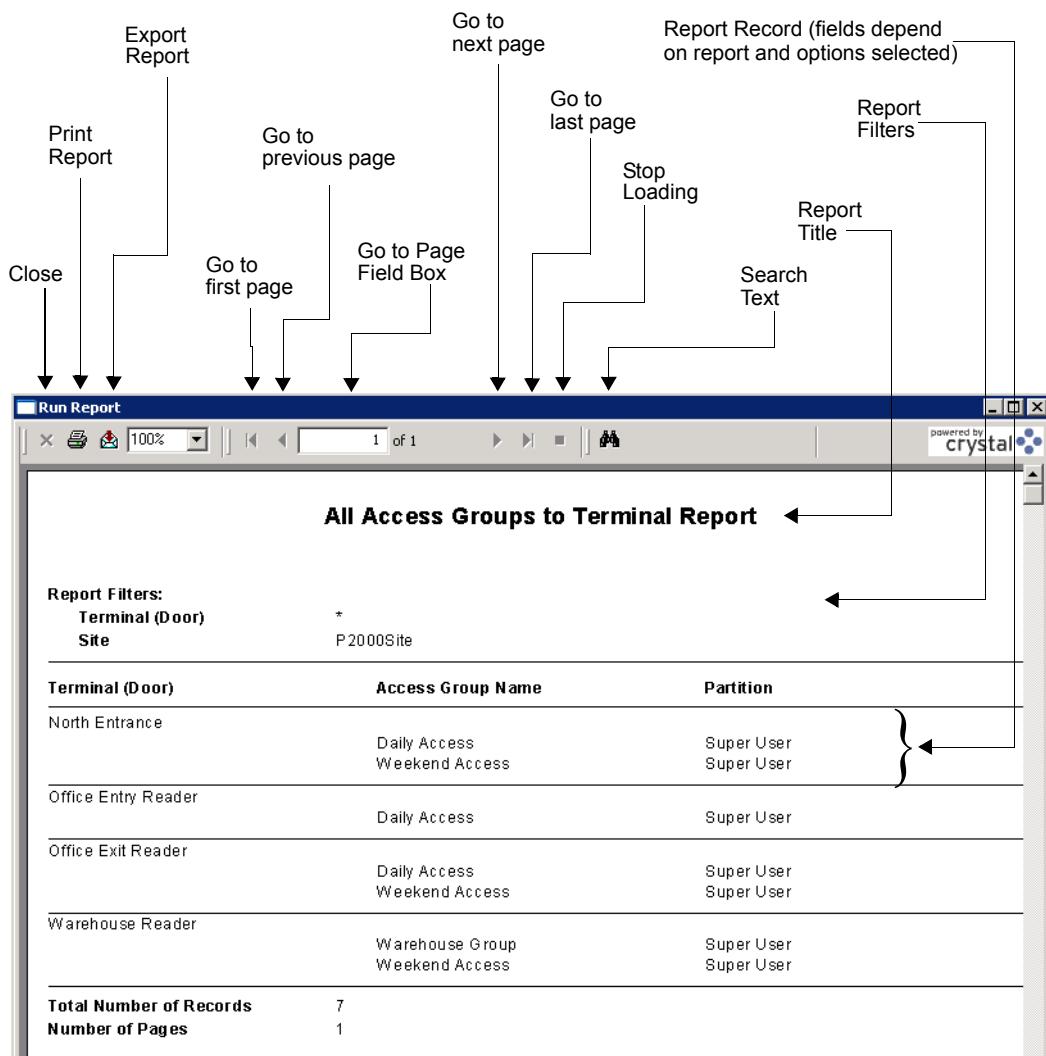
- If your system is partitioned, select the **Partition** that contains the data you want to report on. In addition, the list box will display only the report names that belong to the partition selected.
- Select the name of the report you wish to run.
- Select the **Database** source: select **Normal** if the report will be generated from the current system data; or select **Archive** if you wish to run the report from an archived database.
- Click **Run**. Some reports, such as *Disabled Entities and Identifiers*, have no specific options and display directly in the Crystal preview window after you click **Run** and enter the printer options. Most reports, however, have several filtering options and present a dialog box in which to select your choices.



- To run the default report, which lists all records, leave the asterisk in the field box.
- To run a report on a specific option, choose the option from the drop-down list. (See “Selected Sample Reports” on page 344 for detailed instructions.)
- Click **OK**. Select a printer name and any other information for the printer to be used.

Note: A default printer must be configured to retain the fonts displayed on a report. It is not necessary to have a printer physically connected to the workstation, only that a default printer is set up. Do not use "Generic Text" printers. See your system administrator if you need more information, or refer to your Microsoft Windows documentation.

9. Click **OK**. After a moment, the report displays in the Crystal Reports preview window.
10. Click the Printer icon to print the report. (Your system must have been set up to communicate with a printer to use this option. See your system administrator if you need more information.)



P2000 Standard Report Definitions

Following is a list of all P2000 Standard Reports, a brief description of each default configuration, and the options that can be used to filter or limit the data. Any time you select an asterisk (*) in a field, the report will include all records for that field. Some reports present check boxes listing all available values for a field, allowing you to select multiple items.

If you use the Partition option, report data is restricted to the partition selected from the Run Report window. However, some reports ignore the partition selected and may report data across all partitions, unless you select a specific partition name within the specific report to limit the data.

In addition, when running some of these reports on Enterprise systems, you have the option of selecting to report data from your local site, or you can select the name of the remote site that you want to report on, or you can select to report data from all sites.

To get the fullest benefit of this powerful feature, it may be helpful to read through the entire list to get a complete understanding of what is available.

Access Group – Lists all terminals, terminal groups, floor groups, and door groups by access group. You can select a specific or multiple access groups.

Alarm Activity - Simple – Lists all pending alarm activities, or you can select specific alarm category, type, and associated alarm item; as well as date and time beginning and ending periods. (An example of this report is given in the “Selected Sample Reports” section.)

Alarm History - Simple – Lists all alarm history in the system or you can select specific alarm category, type, associated alarm item, description; as well as date and time beginning and ending periods.

All Access Groups to Terminal – Lists all access groups and the terminals assigned, or select a specific terminal.

All Entities to Access Group – Lists by access group the entities assigned to that access group. Select specific access group and entity category to limit the data.

All Entities to Terminal – Lists by terminal all entities that have access to that terminal. Select a specific terminal and entity category to limit data.

All Entities to Timezone – Lists by time zones all entities assigned to that time zone. Select specific time zone and entity category.

All Entities with Security Flag – Lists by security flag all entities assigned with that security flag. Select a specific security flag and whether you wish to list active and/or disabled entities.

All Terminals to Entity – Lists by entity name all terminals and access groups assigned to the entity. Select Persons or Assets, specific names, and specific entity category.

Area Control – Lists the entities currently in the area, including the total number of entities for each count mode.

Area Transaction – Lists area transactions performed in the system for the specific area. You can select a specific or multiple areas and specific or all area transaction types.

Audit – Lists by operator name the menu items and associated actions performed by that operator during the date and time period selected.

Disabled Entities and Identifiers – Lists all entities that have been disabled or have disabled/inactive identifiers.

Entities - Simple – Lists entity information, including identifier numbers, access groups, time zones, etc. (An example of this report is given in the “Selected Sample Reports” section.)

Entities without Identifiers – Finds all entities in the system without identifiers assigned. (An example of this report is given in the “Selected Sample Reports” section.)

Entity Access Profile – Lists access profile information, including security rights, privileges, access/intrusion groups for the selected entities. You can select specific entity, entity category, company or department to limit data.

Entity Transaction History - Simple – Lists transaction history by entity. You can select specific entity, identifier number, transaction and history type, terminal, elevator or cabinet transaction, begin and end dates and times.

Intrusion Transaction History – Lists all intrusion transactions performed in the system. You can select specific intrusion and history type, terminal, and begin and end dates and times.

Monitored Area – Lists the status of entities that are present in areas controlled by Anti-Passback objects. You can select specific entity, entity category, company or department, anti-passback area or status type to limit data.

Muster Analysis – Displays by group type the list of personnel who are within a Muster Zone in the specified time frame, and whether it was a drill or real emergency.

Terminal Groups – Lists by terminal group the terminals associated with the terminal group. Select a specific terminal group to limit your search.

Tour Notes – Lists all the tour notes assigned to a specific tour name, as set up in the Guard Tour Control window.

Transaction History – Lists all transactions performed in the system. (An example of this report is given in the “Selected Sample Reports” section.)

Unused Active Identifiers – Displays a list of active identifiers that have not been used during the specified period of time.

Verification - CK720/CK721 – These are internal reports, which are used by Johnson Controls installation team to generate a list of work required on commissioning and list of items for verification of the installation of CK721/720 hardware.

Verification - CK722 – These are internal reports, which are used by Johnson Controls installation team to generate a list of work required on commissioning and list of items for verification of the installation of CK722 hardware.

Selected Sample Reports

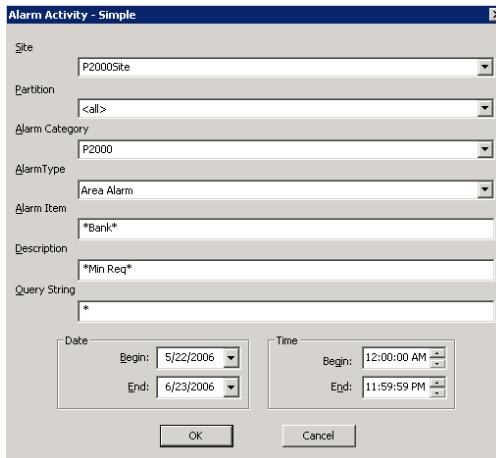
Following are detailed instructions on how to run some sample reports. Once you have experimented with these, you should have a good understanding of how to select options and run reports to get the results you need.

Each example shows a reporting criteria window and the associated report generated from the configuration selected.

Running the Alarm Activity Report

The Alarm Activity report gives you an overview of alarm activity throughout the system. You can run it for all alarm types in the system (the default), or select a specific alarm type. You can also specify a particular date and time and review only those alarms that occurred during that time. If your system is partitioned, select the partition you want to report on. In addition, you can select to run the report for alarms generated at your local or at a remote site.

- From the Run Report list, select **Alarm Activity - Simple** and click **Run**, or double-click on **Alarm Activity - Simple**. The **Alarm Activity - Simple** dialog box opens.



- By default, the system displays the name of the local site in the **Site** field. If you wish to run the report on alarms generated at a remote site, select from the drop-down list the name of the remote site.
- If your system is partitioned, the default **Partition** entry is **<all>**. Select a specific partition name to gather data only from that partition.
- The default **Alarm Category** is **P2000**. Select a specific alarm category to report only on the alarm category selected.
- The default **Alarm Type** entry is **<all>**. Select a specific Alarm Type to report on only one alarm type in the system.
- To further refine your search, you may enter an **Alarm Item** to display items that are associated with the selected Alarm Type. Wildcards are permitted. For example, you can enter ***Bank*** to report on all items that have the word **Bank** as part of their name.
- Enter a **Description** of the alarm. Wildcards are permitted. For example, you can enter ***Min Req*** to report only on alarms generated when the minimum number of entities is not present at the same time in the specific Area.
- If you wish, enter a **Query String** associated with the alarm. You can also use wildcards in this field.
- Select a **Begin** and **End** date for the alarms you wish to see.

Alarm Activity Log Report

Report Filter

Alarm Type	Area Alarm
Alarm Item	*Bank*
Alarm Category	P2000
Date (>=)	5/22/2006 12:00:00AM
Date (<=)	6/23/2006 11:59:59PM
Site	P2000Site
Description	*Min Req*
Query String	*

<u>Alarm Date</u>	<u>Partition</u>	<u>Alarm State</u>	<u>Alarm Status</u>
<u>Escalation</u>	<u>Description</u>		
6/23/2006 9:58:40AM 0	Super User Bank Vault Area Min Required Alarmed	Alarm	Pending
6/23/2006 9:59:01AM 0	Super User Bank Vault Area Min Required Alarmed	Secure	Pending
Total Number of Records	2		
Number of Pages	1		

10. Select a **Begin** and **End** time for the alarms you wish to see.
11. Click **OK**. Select a printer name and any other information for the printer to be used. See your system administrator if you need more information, or refer to your Microsoft Windows documentation.
12. Click **OK**. The Alarm Activity report displays in the Crystal preview window. You can use the arrows at the top of the window to scroll forward and back through the pages; resize the window for the best display, and print all or single pages of the report.

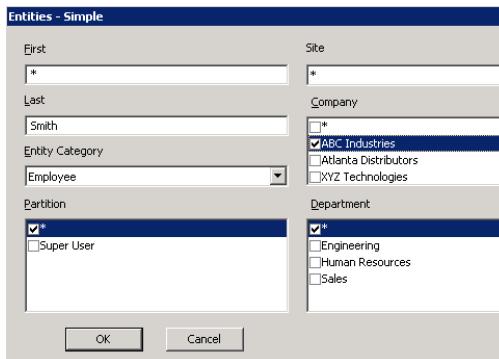
The report displays the information according to the options that you selected in the Alarm Activity dialog box. The report filter options selected for reporting are presented just under the report title. The results of the report query begin in the next section. In the example, the first record shows an alarm that came in on 6/23/2006 at 9:58:40 A.M.

The alarm is in the *Alarm* state and is *Pending*, that is, it has not yet been acknowledged. When the alarm is acknowledged, the report will show that as another date and time-stamped record, with the alarm state as *Secure*.

Running the Entities Report

The Entities report gives you basic information about all the entities in the system. This report contains personal, identifier, and access information as configured in the Entity Management window.

1. From the Run Report list, select **Entities - Simple** and click **Run**, or double-click on Entities - Simple. The Entities - Simple dialog box opens.



2. The default (*) reports all entities. Select a **First** or **Last** name to limit the report to a specific entity.
3. Select an **Entity Category** from the list to report only on the entity category selected.
4. The default **Partition** is All, represented by an asterisk. The list box only displays partitions that are available to the user who is generating the report. Select a specific or multiple Partitions to report only on the partitions selected.

5. From the **Company** list box, select a specific or multiple company names; or select the * to report on all company names.

6. From the **Department** list box, select a specific or multiple department names; or select the * to report on all department names.

7. Click **OK**. Select a printer name and any other information for the printer to be used. See your system administrator if you need more information, or refer to your Microsoft Windows documentation.

8. Click **OK**. The Entities report displays in the Crystal preview window. You can use the arrows at the top of the window to scroll forward and back through the pages; resize the window for the best display, and print all or single pages of the report.

The record lists the entity's name, along with Company, Department, Entity Category, and identifier information.

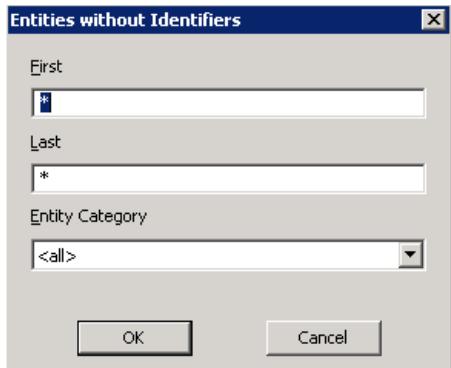
Entities - Simple Report

Report Filters:			
Site	*		
First Name	*		
Last Name	Smith		
Entity Category	Employee		
Partition	*		
Company	ABC Industries		
Department	*		
Partition			
First Name	James	Middle	R.
Last Name	Smith		
Company	ABC Industries		
Department	Sales		
Entity Category	Employee		
E-Mail			
Identifier Number	311	Identifier Status	Active
Access Profile Name	Daily Access	Access Profile Status	Active
Access Groups			
Warehouse Group		Timezones	
Weekend Access		Full Time	
		OT Hours	
Total Number of Identifiers	1		

Running the Entities without Identifiers Report

The Entities without Identifiers report is useful to locate entities who have no access badge identifiers. A popular use is to locate entity records that were not deleted when identifiers were removed.

- From the Run Report list, double-click **Entities without Identifiers**. The Entities without Identifiers dialog box opens.



- The default (*) reports all entities. Select a **First** or **Last** name to limit the report to a specific entity.
- Select an **Entity Category** from the list to report only on the entity category selected.
- Click **OK**. Select a printer name and any other information for the printer to be used. See your system administrator if you need more information, or refer to your Microsoft Windows documentation.
- Click **OK**. The Entities without Identifiers report displays in the Crystal preview window. You can use the arrows at the top of the window to scroll forward and back through the pages; resize the window for the best display, and print all or single pages of the report.

This report lists the entity by first and last name, along with Company, Department, and Entity Category. Sponsor information will be included if the entity is a visitor.

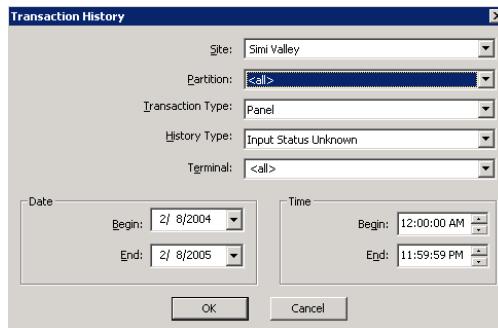
Entities without Identifiers Report

First *	Last *
Entity Category	
Public	No
First	Loretta
Last	Adams
Company	ABC Industries
Address	
Phone	
Ext	
Site	P2000Site
Guard	No
Requires Sponsor	Yes
Sponsor Name	Jones, Charles
E-Mail	

Running the Transaction History Report

One of the most commonly used reports in the system is the Transaction History report. This report can list every transaction in the system, or be filtered to list by specific Site, Partition, Terminal, Transaction Type, History Type, specific Dates and Times, and any combination of these. The options available for selection depend on the transaction type selected.

- From the Run Report list, select **Transaction History** and click **Run**, or double-click on Transaction History. The Transaction History dialog box opens.



- By default, the system displays the name of the local site in the **Site** field. If you wish

to run the report on transactions that were originated at a remote site, enter the name of the remote site in this field.

- If your system is partitioned, the default **Partition** entry is **<all>**. Select a partition name to gather data only from that partition.
- Select a **Transaction Type**: **<all>**, Host, Input Point, Output Point, Panel, Terminal.
- Select a **History Type**. History types available from the drop-down list depend on the selection in the Transaction Type field.
- If Terminal, Input Point, or Output Point is selected in the Transaction Type field, you can enter a specific **Terminal** to limit your search.
- Select a **Begin** and **End** date for the transactions you wish to see.
- Select a **Begin** and **End** time for the transactions you wish to see.
- Click **OK**. Select a printer name and any other information for the printer to be used. See your system administrator if you need more information, or refer to your Microsoft Windows documentation.
- Click **OK**. The Transaction History report displays in the Crystal preview window. You can use the arrows at the top of the

Transaction History Report

Date (>=)	2/8/2004 12:00:00AM			
Date (<=)	2/8/2005 11:59:59PM			
Transaction Type	Panel			
Terminal	*			
History Type	Input Status Unknown			
Site	Simi Valley			
Partition	Super User			
Date	2/7/2005 9:53:05AM	Terminal	Public	No
Panel	North Entrance		Security Office	
History Message	Input Status Unknown			
Partition	Super User			
Date	2/7/2005 9:53:05AM	Terminal	Public	No
Panel	North Entrance		Main Door	
History Message	Input Status Unknown			

window to scroll forward and back through the pages; resize the window for the best display, and print all or single pages of the report.

The top of the report shows the date and time settings for the report and the Transaction Type selected. Each transaction is listed as a separate date and time stamped record of the options selected in the Transaction History dialog box.

Creating Custom Reports

If you have an independent copy of Crystal Reports, custom reports can be created in Crystal and imported into the P2000 system, or existing P2000 reports can be edited in Crystal and imported into the P2000 system. Each method is described in the following sections:

- **Creating a custom Crystal report for the P2000 system**
- **Editing a P2000 Standard Report in Crystal**

Creating a Custom Crystal Report for the P2000 System

Because the P2000 system uses Crystal Reports as its report engine, you can create custom Crystal reports that are compatible with the P2000 system. You must have your own copy of Crystal Reports and you must have access to the field and table relationships used within the P2000 software (see the following section “Database Table Definitions”). Once the report is completed, it is exported as an *.rpt* file, and then can be imported into the P2000 system.

Note: Advanced Crystal Reports users who plan to include customized queries (manually-edited queries) in their reports, should note that to run a manually-edited query against the archived database, the database name must be dynamically assigned in the customized query object using the parameter “DBName.” The P2000 software will then pass the correct database name to the report table in Crystal Reports.

Database Table Definitions

To create a custom report that is compatible with the P2000 system, contact Technical Support for the *P2000 Database Table Definitions* Supplement. Once you have the field/table relationship information, create your report according to the methods presented in your Crystal Reports documentation.

Report Interfaces

When you configure a custom report in P2000, you must select the database that will be used to run the report. This is selected from the **Use Dialog** drop-down list in the Edit Report application. You can use the P2000EntityConfig database or the P2000History database.

Custom reports must be coded against only one of the two databases. If the report is required to access multiple databases, the report should be executed against a stored procedure residing on one of the databases, with any further database connections specified in the stored procedure. The report will still need to be configured for a specific database in the Edit Report dialog box, in this case pointing to the database in which the stored procedure resides.

Alternatively, you can also add or configure custom reports using one of the user interface reports associated with existing P2000 Standard Reports. Instead of selecting a specific database from the **Use Dialog** drop-down list

in the Edit Report application, you may select one of the standard report interfaces.

Selecting a standard report interface requires that the report be coded to point to the same database that the report interface uses. The list of user interfaces and their related databases is listed at the end of this section. If the report is required to access multiple databases, you should use a stored procedure that resides on the same database as accessed by the standard report interface.

By selecting one of the standard report interfaces, the parameters used by the interface can in this way be used in the report. If a copy of the existing P2000 report that is executed by the specific standard report interface is opened in Crystal Reports, you can view under the “parameters list” a list of parameters that are passed in by the P2000 standard report interface.

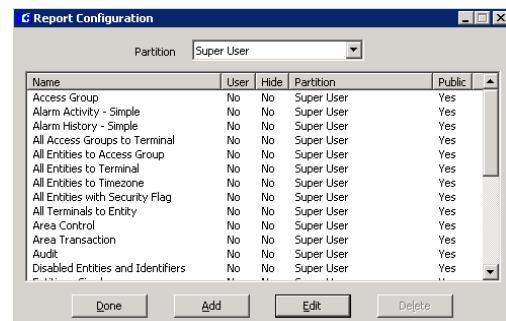
If you select one of the two generic interfaces from the **Use Dialog** drop-down list (P2000EntityConfig or P2000History), the standard Crystal Parameter dialog will be used for any parameters that have been configured in the report.

Report User Interface	Associated Database
Access Group	P2000EntityConfig
Alarm Activity - Simple	P2000History
Alarm History - Simple	P2000History
All Access Groups to Terminal	P2000EntityConfig
All Entities to Access Group	P2000EntityConfig
All Entities to Terminal	P2000EntityConfig
All Entities to Timezone	P2000EntityConfig
All Entities with Security Flag	P2000EntityConfig
All Terminals to Entity	P2000EntityConfig
Area Control	P2000History
Area Transaction	P2000History
Audit	P2000History
Disabled Entities and Identifiers	P2000EntityConfig
Entities - Simple	P2000EntityConfig
Entities without Identifiers	P2000EntityConfig

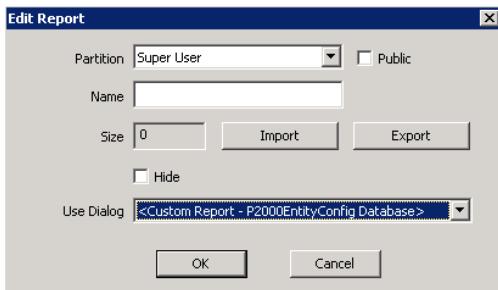
Report User Interface	Associated Database
Entity Access Profile	P2000EntityConfig
Entity Transaction History - Simple	P2000History
Intrusion Transaction History	P2000History
Monitored Area	P2000EntityConfig
Muster Analysis	P2000History
Terminal Groups	P2000EntityConfig
Tour Notes	P2000History
Transaction History	P2000History
Unused Active Identifiers	P2000EntityConfig
Verification - CK720/CK721	P2000EntityConfig
Verification - CK722	P2000EntityConfig

To Import a Custom Crystal Report into the P2000 System:

1. Save your custom Crystal report in <name>.rpt format and copy it to a directory that is accessible to the P2000 Server.
2. From the P2000 Main menu, select **Report>Report Configuration**. The Report Configuration dialog box appears.



3. If your system is partitioned, select the **Partition** that will contain the imported report.
4. Click **Add**. The Edit Report dialog box opens.



5. Select **Public** to make this report visible to all partitions.
6. Enter a name for your custom report. (This is the name that will display in your Run Report list once the report is imported.)
7. From the **Use Dialog** drop-down list, select whether you want to use one of the databases (P2000EntityConfig or P2000History) or if you want to use one of the existing report user interfaces. Refer to “Report Interfaces” on page 349 for details.
8. Click **Import**.
9. From the Windows Open dialog box, navigate to the directory in which the report resides and select the report.
10. Click **Open**, the Size of the selected report displays.
11. Select the **Hide** check box if you do not wish to display this report in the Run Report dialog box. Clear the **Hide** check box if for example, you wish to run this report often and therefore you want to select it from the Run Report dialog box.
12. Click **OK**. The new report will display in the Report Configuration dialog box and will also be added to the P2000 system Run Reports list for the partition selected.

You can now select the report and run it as you would any other Standard Report.

Editing a P2000 Standard Report in Crystal

A P2000 Standard report may have exactly what you need with the exception of a couple of fields. You can export a Standard Report and then import it into Crystal for revision; save it in .rpt format and import it back into the P2000 system.

To Export an Existing Standard Report from the P2000 System:

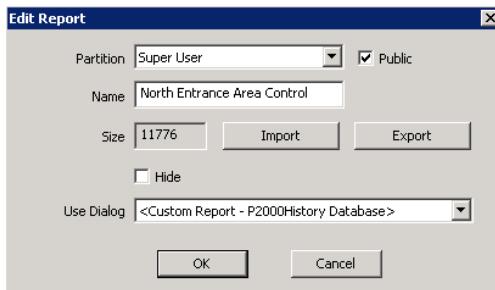
1. From the P2000 Main menu, select **Report>Report Configuration**. The Report Configuration dialog box opens.
2. Select from the scrolling list the report you wish to edit in Crystal.
3. Click **Edit**. The Edit Report dialog box opens. The Name and Size of the selected report display.
4. Click **Export**. A Windows Save As dialog box opens. Navigate to a directory that will be accessible from your Crystal Reports program.

To Edit the P2000 Report in Crystal

As with full custom reports, you must know the field/table relationships for the information you need before you can create new fields for the report. Contact Technical Support for the *P2000 Database Table Definitions Supplement*. After the report is edited and saved in <name>.rpt format, you are ready to import it back into the P2000 system. Save or copy the new report file to a directory that is accessible to the P2000 Server.

1. From the P2000 Main menu, select **Report>Report Configuration**. The Report Configuration dialog box opens.

2. If your system is partitioned, select the **Partition** that will contain the imported report.
3. Click **Add**. The Edit Report dialog box opens.



4. Select **Public** to make this report visible to all partitions.
5. Enter a name for your edited report. You may want to rename it something other than the original. (This is the name that will display in your Run Report list once the report is imported.)
6. From the **Use Dialog** drop-down list, select whether you want to use one of the databases (P2000EntityConfig or P2000History) or if you want to use one of the existing report user interfaces. Refer to "Report Interfaces" on page 349 for details.

7. Click **Import**.
8. From the Windows Open dialog box, navigate to the directory in which the report resides and select the report.
9. Click **Open**, the Size of the selected report displays.
10. Select the **Hide** check box if you do not wish to display this report in the Run Report dialog box. Clear the **Hide** check box if for example, you wish to run this report often and therefore you want to select it from the Run Report dialog box.
11. Click **OK**. The new report will display in the Report Configuration dialog box and will also be added to the P2000 system Run Reports list for the partition selected.

You can now select the report and run it as you would any other Standard Report.

Appendix A: Event Triggers/Actions

This appendix lists all Trigger Categories, Trigger Types, Trigger Conditions, and Event Action Types available for Event configuration. For more information see “Creating Events” on page 206.

Trigger Types

Category: Alarm

Area – Triggers when an Area alarm is created or acted upon.

AV Behavior Alarm – Triggers when an Audio Visual Behavior alarm is created or acted upon.

AV Dry Contact Alarm – Triggers when an Audio Visual Dry Contact alarm is created or acted upon.

AV Motion Alarm – Triggers when an Audio Visual Motion alarm is created or acted upon.

AV System Alarm – Triggers when an Audio Visual System alarm is created or acted upon.

AV Video Loss Alarm – Triggers when an Audio Visual Video Loss alarm is created or acted upon.

Cluster Redundancy Failover – Triggers when an alarm is generated in the P2000 system with Cluster Redundancy when NodeA fails over to NodeB.

DT Redundancy Failover – Triggers when an alarm is generated in the P2000 system with Remote Redundancy when the Primary Server fails over to the Standby Server.

DT Redundancy Monitoring – Triggers when an alarm is generated in the P2000 system with Remote Redundancy when monitoring of the Primary Server is enabled at the Standby Server.

DT Redundancy Standby Server Isolation IP Failure

– Triggers when an alarm is generated in the P2000 system with Remote Redundancy when monitoring is disabled because of the Standby Server’s failure to successfully ping at least 50% of the defined IP addresses.

DT Redundancy Standby Server Offline – Triggers when an alarm is generated in the P2000 system with Remote Redundancy when the Standby Server goes offline.

Event Alarm – Triggers when an Event alarm is created or acted upon.

FDA – Triggers when an FDA alarm is created or acted upon.

Guard Tour – Triggers when a Guard Tour alarm is created or acted upon.

Inputs – Triggers when an Input alarm is created or acted upon.

Intrusion Area – Triggers when an Intrusion Area alarm is created or acted upon.

Intrusion Zone – Triggers when an Intrusion Zone alarm is created or acted upon.

Loop Tamper – Triggers when a hardware Loop Tamper switch alarm is created or acted upon.

Muster Aborted – Triggers when a Muster Aborted alarm is created or acted upon.

Muster Running – Triggers when a Muster Running alarm is created or acted upon.

Muster When Disabled – Triggers when a Muster When Disabled alarm is created or acted upon.

Muster Zone Status – Triggers when a Muster Zone Status alarm is created or acted upon.

Private Connection Disconnected (Temporary Server) – Triggers when an alarm is generated in the P2000 system with Remote Redundancy when a Primary Server's connection (in temporary boot) over the private network is lost.

Private Connection Disconnected on Standby Server – Triggers when an alarm is generated in the P2000 system with Remote Redundancy when a Standby Server's connection over the private network is lost.

Public Connection Disconnected on Standby Server – Triggers when an alarm is generated in the P2000 system with Remote Redundancy when a Standby Server's connection over the public network is lost.

Public Connection Disconnected on Temporary Server – Triggers when an alarm is generated in the P2000 system with Remote Redundancy when a Primary Server's connection (in temporary boot) over the public network is lost.

Remote Messaging Receive – Triggers when an alarm is generated when a remote message is received.

Remote Messaging Transmit – Triggers when an alarm is generated when a remote message is transmitted.

Remote Redundancy Primary Server Operational – Triggers when a Remote Redundancy Primary Server Operational alarm is created or acted upon.

Remote Redundancy Standby Server Operational – Triggers when a Remote Redundancy

Standby Server Operational alarm is created or acted upon.

Time Sync – Triggers when a time synchronization alarm is created or acted upon.

Conditions

- Alarm Category
- Alarm State
- Date
- Day of the Month
- Day of the Week
- Escalation Level
- Month
- Time

Category: Anti-Loitering Object

Violation – Triggers when the system reports a violation in an anti-loitering area.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Anti-Passback Object

All events are triggered when the described condition is entered.

Entity - Reset Entry Time – Triggers when the Entity - Reset Entry Time history message is received.

Entity - Reset Exit Time – Triggers when the Entity - Reset Exit Time history message is received.

Entity - Resynchronize Request – Triggers when the Entity - Resynchronize Request history message is received.

Entity - Set to Default Status – Triggers when the Entity - Set to Default Status history message is received.

Entity - Transition In – Triggers when the Entity - Transition In history message is received.

Entity - Transition Out – Triggers when the Entity - Transition Out history message is received.

Entity - Transition Undefined – Triggers when the Entity - Transition Undefined history message is received.

Not operational – Triggers when an anti-passback object starts up, has a problem, or is not supported by the CK722 panel.

Operational – Triggers when an anti-passback object works without any problems.

Peers offline – Triggers when an anti-passback object works in shared mode, but cannot inform one or more of its peers.

Star center offline – Triggers when an anti-passback object works in central mode, but cannot reach the central anti-passback object.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Area

Area Maximum allowed alarm – Triggers when an alarm is set or reset when the maximum number of entities allowed in the selected Area has exceeded.

Area Minimum required alarm – Triggers when an alarm is set or reset when the minimum number of entities required is not present at the same time in the selected Area.

Area Pre-Maximum allowed alarm – Triggers when an alarm is set or reset when the pre-maximum number of entities allowed in the selected Area is reached.

Conditions

- Reset
- Set

Category: Audit

Add Badge – Triggers when an audit message is generated because an operator has added a badge to the system.

Delete Badge – Triggers when an audit message is generated because an operator has deleted a badge from the system.

Edit Badge – Triggers when an audit message is generated because an operator has changed a badge in the system.

Conditions

- Badge
- Badge Configuration
- Badge Purpose
- Badge Reason
- Cardholder
- Date
- Day of the Month
- Day of the Week
- Month
- Time

Category: Automatic Payment Machine

APM Clear – Triggers when the APM Clear history message is received.

APM Clear (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the APM Clear state.

APM Tamper – Triggers when the APM Tamper history message is received.

APM Tamper (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the APM Tamper state.

Conditions

- <always>
- Name
- Timezone Active

Category: AV

AV Behavior Alarm – Triggers when an AV Behavior alarm is created or acted upon.

AV Dry Contact Alarm – Triggers when an AV Dry Contact alarm is created or acted upon.

AV Motion Alarm – Triggers when an AV Motion alarm is created or acted upon.

AV System Alarm – Triggers when an AV System alarm is created or acted upon.

AV Video Loss Alarm – Triggers when an AV Video Loss alarm is created or acted upon.

Conditions

- AV Camera Name
- AV Dry Contact Name
- AV Switch Name
- Date
- Day of the Month
- Day of the Week

- Month
- Time

Category: Badge

Access rights expired – Triggers when the entity is denied access because of expired access rights.

Alternate Access – Triggers when the entity is granted alternate access.

Anti-Passback Timer On – Triggers when a badge is presented at an anti-passback reader where the timer is on.

Central access denied – Triggers when the entity is denied access by the Server.

Central data unreachable – Triggers when the Access Control object cannot reach the P2000 Server.

Central status unreachable – Triggers when a controller is not able to obtain information from another controller, for example, in a central Anti-Passback application.

Denied intrusion area armed – Triggers when the badge presented at a reader has no rights to arm the intrusion area.

Deny Open Door – Triggers when a Deny Door Open message is received from a panel. This message is only available from CK720/CK705 panels version 2.5 and higher that have the reader flag “Deny If Door Open” enabled.

Entity expired – Triggers when the entity is denied access because it expired.

Executive Privilege – Triggers when the badge presented has executive privileges, i.e., has unlimited access and bypasses all time zones and access groups.

Host Grant – Triggers when the badge is presented and the host grants access.

Host Grant Entry – Triggers when the badge is presented and the host grants access at an entry reader.

Host Grant Exit – Triggers when the badge is presented and the host grants access at an exit reader.

Incomplete group rule – Triggers when an entity is denied access because there is an incomplete group in the vicinity of the door.

Inconsistent identifiers – Triggers when an entity uses more than one identifier (for example, badges) that do not belong to the same set of access rights.

Invalid access group – Triggers when the badge presented at a reader has an invalid access group.

Invalid Access Group Timezone – Triggers when the badge presented at a reader has an access group with an invalid time zone.

Invalid access level – Triggers when the badge presented at a reader has an invalid access level.

Invalid access mask – Triggers when the badge presented at a reader has an invalid access mask.

Invalid access profile – Triggers when the badge presented at a reader has an invalid access profile (the access profile cannot be located).

Invalid Badge – Triggers when the badge presented at the reader is not valid.

Invalid Biometric – Triggers when the badge presented at the reader does not match the information at the biometric device.

Invalid Event Privilege Level – Triggers when the badge presented at the reader has an invalid privilege level.

Invalid In-X-It Status – Triggers when the badge is presented at the reader in an out-of-sequence manner, i.e., two times sequentially at an exit reader or two times sequentially at an entry reader.

Invalid Issue Level – Triggers when the badge presented at the reader has an invalid issue level.

Invalid Keypad Event – Triggers when an invalid keypad code has been entered.

Invalid override privilege – Triggers when the badge presented at a reader has an invalid override privilege.

Invalid Override Time – Triggers when the user enters an invalid override time at the door's keypad.

Invalid Pin Code – Triggers when an invalid PIN code has been entered.

Invalid Reader – Triggers when the badge presented has no access rights assigned to the reader.

Invalid Reader Time Zone – Triggers when a badge is presented at a reader that has a disabled time zone.

Invalid Security Level – Triggers when a badge is denied access at a reader because of an invalid security level.

Invalid security mask – Triggers when the badge presented at a door has an invalid security mask.

Invalid smart card signature – Triggers when the reader detects an invalid electronic signature on a smart card. This condition may indicate that someone has tampered with the contents of the smart card.

Local Grant – Triggers when the badge is presented and the panel grants access.

No Entry – Triggers when an entity is granted access, but does not open the door within the access time.

Occupancy violation – Triggers when an entity is denied entry because the occupancy space has already reached its maximum occupancy, or when an entity is denied exit because the occupancy space has already reached its minimum occupancy.

Panel Card Event Activated – Triggers when a badge is presented at a reader and activated an event.

Panel Card Event Deactivated – Triggers when a badge is presented at a reader and deactivated an event.

Pin attempts exceeded – Triggers when the maximum number of consecutive invalid PIN attempts has been entered.

Soft In-X-It Violation – Triggers when the badge presented generated an entry/exit violation, i.e., access is granted, but an error message is created.

Unaccompanied asset rule – Triggers when an entity is denied access because there are unaccompanied assets in the vicinity of the door.

Unaccompanied entity rule – Triggers when an entity is denied access because there are unaccompanied entities in the vicinity of the door.

Valid & Unauthorized Access – Triggers when the badge presented at the reader is valid, but the door remains locked, because further authorization (e.g. by the guard) is required.

Conditions

- Access Group of Badge
- Access Group of Terminal
- Badge
- Badge Configuration
- Badge Purpose

- Badge Reason
- Cardholder
- Date
- Day of the Month
- Day of the Week
- Entity Category
- Month
- Panel Name
- Terminal Index *
- Terminal Name
- Time
- Timezone Active

* Not available for CK722 panels.

Category: Counter

Triggers when the selected counter reaches the specified value.

Condition

- Value

Category: Date / Time

Time/Date – Event trigger is activated on the specified time and date.

Conditions

- Date (transition)
- Day of the Month (steady state)
- Day of the Week (steady state)
- Month (steady state)
- Time (transition)

Category: External Trigger

Database – Triggers when an external input in the form of a database write has been sent to the P2000 system to trigger a host event.

File – Triggers when an external input in the form of an ASCII file has been sent to the P2000 system to trigger a host event.

RS232 – Triggers when an external input in the form of an RS232 serial message has been sent to the P2000 system to trigger a host event.

TCP/IP – Triggers when an external input in the form of a TCP/IP message has been sent to the P2000 system to trigger a host event.

Conditions

- Substring (the string sent to the host from the external input).

Category: Input Point

Input Goes Open (transition) – Triggers when the state of an input point has changed to open.

Input Goes Reset (transition) – Triggers when the state of an input point has changed to reset.

Input Goes Set (transition) – Triggers when the state of an input point has changed to set.

Input Goes Short (transition) – Triggers when the state of an input point has changed to short.

Input Goes Suppressed (transition) – Triggers when the state of an input point has changed to suppressed.

Input Goes Unknown (transition) – Triggers when the state of an input point has changed to an unknown state. This happens when the field device that the input point resides on goes offline.

Input Is Open (steady state) – Triggers when an input is in open state. This trigger is to be used in combination with other trigger(s).

Input Is Secure (steady state) – Triggers when an input is in secure state. This trigger is to be used in combination with other trigger(s).

Input Is Set (steady state) – Triggers when an input is in set state. This trigger is to be used in combination with other trigger(s).

Input Is Short (steady state) – Triggers when an input is in short state. This trigger is to be used in combination with other trigger(s).

Input is suppressed (steady state) – Triggers when an input is in suppressed state. This trigger is to be used in combination with other trigger(s).

Conditions

- Date
- Day of the Month
- Day of the Week
- Input Point Name
- Input Point Number
- Month
- Panel Name
- Terminal Index*
- Terminal Name
- Time
- Timezone Active

* Not available for CK722 panels.

Category: Integration Device

Integration Device Down – Triggers when the Integration Device Down history message is received.

Integration Device Down (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Integration Device Down state.

Integration Device Up – Triggers when the Integration Device Up history message is received.

Integration Device Up (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Integration Device Up state.

Conditions

- Date

- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Integration Server

Integration Server Down – Triggers when the Integration Server Down history message is received.

Integration Server Down (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Integration Server Down state.

Integration Server Up – Triggers when the Integration Server Up history message is received.

Integration Server Up (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Integration Server Up state.

Time Synch Problem – Triggers when the Time Synch Problem history message is received.

Time Synch Problem (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Time Synch Problem state.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Integration Station

Busy – Triggers when the Busy history message is received.

Busy (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Busy state.

Hold – Triggers when the Hold history message is received.

Hold (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Hold state.

Logged Off – Triggers when the Logged Off history message is received.

Logged Off (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Logged off state.

Logged On – Triggers when the Logged On history message is received.

Logged On (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Logged On state.

Not Installed – Triggers when the Not Installed history message is received.

Not Installed (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Not Installed state.

Not Ready – Triggers when the Not Ready history message is received.

Not Ready (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Not Ready state.

Ready – Triggers when the Ready history message is received.

Ready (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Ready state.

Conditions

- Date
- Day of the Month

- Day of the Week
- Month
- Name
- Time

- Month
- Name
- Time

Category: Interlock Object

Interlock State False – Triggers when the Interlock State False history message is received.

Interlock State Fault – Triggers when the Interlock State Fault history message is received.

Interlock State True – Triggers when the Interlock State True history message is received.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Intrusion Annunciator

All events are triggered when the described condition is entered.

Annunciator Active – Triggers when the intrusion annunciator is active.

Annunciator Error – Triggers when the intrusion annunciator encounters an error.

Annunciator Inactive – Triggers when the intrusion annunciator is not active.

Annunciator Silenced – Triggers when the intrusion annunciator is silenced.

Conditions

- Date
- Day of the Month
- Day of the Week

Category: Intrusion Area

All events are triggered when the described condition is entered.

Area Alarm – Triggers when the intrusion area enters the alarm state.

Area Alarm Off – Triggers when the intrusion area is no longer in alarm state.

Area Armed (Steady) – Triggers when the intrusion area enters the armed state. This trigger is to be used in combination with other trigger(s).

Area Armed (Transition) – Triggers when the intrusion area enters the armed state.

Area Arming – Triggers when the intrusion area enters the arming state.

Area Disarmed (Steady) – Triggers when the intrusion area enters the disarmed state. This trigger is to be used in combination with other trigger(s).

Area Disarmed (Transition) – Triggers when the intrusion area enters the disarmed state.

Area Disarming – Triggers when the intrusion area enters the disarming state.

Area Error – Triggers when the intrusion area encounters an error while writing to the associated output point.

Area Fault – Triggers when the intrusion area enters the fault state.

Area Mixed – Triggers when the intrusion area has armed and disarmed zones.

Area Zones Bypassed – Triggers when the intrusion area contains zones that enter the bypassed state.

Area Zones Sealed – Triggers when the intrusion area contains zones that enter the sealed state.

Area Zones Unbypassed – Triggers when the intrusion area contains zones that enter the no bypassed state.

Area Zones Unsealed – Triggers when the intrusion area contains zones that enter the unsealed state.

Zone Not Bypassed (Steady) – Triggers when the intrusion area contains zones that enter the no bypassed state. This trigger is to be used in combination with other trigger(s).

Zone Sealed (Steady) – Triggers when the intrusion area contains zones that enter the sealed state. This trigger is to be used in combination with other trigger(s).

Zone Unsealed (Steady) – Triggers when the intrusion area contains zones that enter the unsealed state. This trigger is to be used in combination with other trigger(s).

Zones Bypassed (Steady) – Triggers when the intrusion area contains zones that enter the bypassed state. This trigger is to be used in combination with other trigger(s).

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Intrusion Device

Battery In Place – Triggers when the missing battery of the intrusion device is in place.

Battery Low – Triggers when the battery of the intrusion device is low.

Battery Missing – Triggers when the battery of the intrusion device goes into missing state.

Battery Normal – Triggers when the battery of the intrusion device is back in normal state.

Battery Test – Triggers when the battery of the intrusion device is in test.

Battery Test Done – Triggers when the battery of the intrusion device has completed its test.

Battery Test Failure – Triggers when the battery of the intrusion device has failed its test.

Battery Test Success – Triggers when the battery of the intrusion device has succeeded its test.

Device Connected – Triggers when the intrusion device goes into connected state.

Device Disconnected – Triggers when the intrusion device goes into disconnected state.

Invalid Vendor Address – Triggers when the vendor address of the intrusion device goes into invalid state.

Mains Failure – Triggers when the maintenance of the intrusion device goes into failed state.

Mains Normal – Triggers when the maintenance of the intrusion device is normal.

Port Closed – Triggers when the intrusion device port is closed.

Port Opened – Triggers when the intrusion device port is open.

Valid Vendor Address – Triggers when the vendor address of the intrusion device goes into valid state.

Conditions

- Date
- Day of the Month
- Day of the Week

- Month
- Time

Category: Intrusion Keypad

Keypad Error – Triggers when an error is detected at the S300 Keypad/Display Module.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Intrusion Zone

All events are triggered when the described condition is entered.

Zone Acknowledged – Triggers when the intrusion zone alarm has been acknowledged.

Zone Alarm – Triggers when the intrusion zone enters the alarm state.

Zone Alarm Off – Triggers when the intrusion zone is no longer in alarm state.

Zone Alarm/Open – Triggers when the intrusion zone enters the open alarm state.

Zone Alarm/Short – Triggers when the intrusion zone enters the short alarm state.

Zone Alarm/Tamper – Triggers when the intrusion zone enters the tamper alarm state.

Zone Alarm/Trouble – Triggers when the intrusion zone enters the trouble alarm state.

Zone Alarmed – Triggers when the intrusion zone enters the alarmed state.

Zone Alarmed (Steady) – Triggers when the intrusion zone enters the alarmed state. This

trigger is to be used in combination with other trigger(s).

Zone Armed – Triggers when the intrusion zone enters the armed state.

Zone Arming – Triggers when the intrusion zone enters the arming state.

Zone Bypassed – Triggers when the intrusion zone enters the bypassed state.

Zone Bypassed (Steady) – Triggers when the intrusion zone enters the bypassed state. This trigger is to be used in combination with other trigger(s).

Zone Disarmed – Triggers when the intrusion zone enters the disarmed state.

Zone Disarming – Triggers when the intrusion zone enters the disarming state.

Zone Error – Triggers when the intrusion zone encounters an error while writing to the associated output point.

Zone Fault – Triggers when the intrusion zone enters the fault state.

Zone Normal – Triggers when the intrusion zone has returned to a normal state.

Zone Normal (Steady) – Triggers when the intrusion zone has returned to a normal state. This trigger is to be used in combination with other trigger(s).

Zone Open – Triggers when the intrusion zone enters the open state.

Zone Open (Steady) – Triggers when the intrusion zone enters the open state. This trigger is to be used in combination with other trigger(s).

Zone Tampered – Triggers when the intrusion zone enters the tampered state.

Zone Tampered (Steady) – Triggers when the intrusion zone enters the tampered state. This

trigger is to be used in combination with other trigger(s).

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Jacques Intercom Station

Call Request – Triggers when the Call Request history message is received.

Call Terminated – Triggers when the Call Terminated history message is received.

Connect Station – Triggers when the Connect Station history message is received.

Fault – Triggers when the Fault history message is received.

Fault Recovered – Triggers when the Fault Recovered history message is received.

Idle – Triggers when the Idle history message is received.

Isolated – Triggers when the Isolated history message is received.

Offline – Triggers when the Offline history message is received.

Remoted – Triggers when the Remoted history message is received.

Tamper – Triggers when the Tamper history message is received.

Tamper Recovered – Triggers when the Tamper Recovered history message is received.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Lane Equipment Cabinet Door

LEC Closed – Triggers when the LEC Closed history message is received.

LEC Forced – Triggers when the LEC Forced history message is received.

LEC Open – Triggers when the LEC Open history message is received.

LEC Propped – Triggers when the LEC Propped history message is received.

Conditions

- <always>
- Name
- Timezone Active

Category: Multi Command Object

MCO State (0 to 31) (Transition) – Triggers when the MCO State history message is received.

MCO State (0 to 31) (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the MCO State state.

MCO State All (Transition) – Triggers when the MCO State All history message is received.

Conditions

- Date
- Day of the Month

- Day of the Week
- Month
- Name
- Time

Category: Mustering

Mustering Start – Triggers when Mustering has been started at a specified zone.

Mustering Stop – Triggers when Mustering has been stopped at a specified zone.

Conditions

- Zone Name

Category: Notification Object

Notification Events dropped – Triggers after events were dropped from the FIFO (first-in first-out buffer) mechanism employed by event notification messages because the FIFO overflows.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Occupancy Object

All events are triggered when the described condition is entered.

Occupancy above high limit – Triggers when the maximum number of entities allowed in an occupancy space has been exceeded.

Occupancy at high limit – Triggers when the number of entities in an occupancy space has reached the high limit (maximum occupancy).

Occupancy at low limit – Triggers when the number of entities in an occupancy space has reached the low limit (minimum occupancy).

Occupancy below low limit – Triggers when the number of entities in an occupancy space is less than the low limit (minimum occupancy).

Occupancy within limits – Triggers when the number of entities required in an occupancy space is within the defined limits (between maximum and minimum occupancy).

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Operator

Invalid Logon – Triggers when there has been an attempt to log on with an invalid user name or password.

Logon Disabled – Triggers when an operator has been inactive at the workstation for a specified period of time and has been automatically logged off.

Operator Logoff – Triggers when an operator has logged off from the workstation.

Operator Logon – Triggers when an operator has logged on to the workstation.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Operator
- Station Name
- Time

Category: Output Point

Output Goes Reset (transition) – Triggers when the state of an output point has changed to reset.

Output Goes Set (transition) – Triggers when the state of an output point has changed to set.

Output Goes Unknown (transition) – Triggers when the state of an output point has changed to an unknown state. This happens when the field device that the output point resides on goes offline.

Output Is Reset (steady state) – Triggers when an output is in reset state. This trigger is to be used in combination with other trigger(s).

Output Is Set (steady state) – Triggers when an output is in set state. This trigger is to be used in combination with other trigger(s).

Output state is unknown (steady state) – Triggers when an output point is in an unknown state. This trigger is to be used in combination with other triggers.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Output Point Name
- Output Point Number
- Panel Name
- Terminal Index*
- Terminal Name
- Time
- Timezone Active

* Not available for CK722 panels.

Category: Panel

CPU Usage Too High – Triggers when the CPU usage at the CK722 panel is too high.

Fast Download Failed – Triggers when the Fast Download operation has failed. CK722 only.

Fast Download Started – Triggers when the Fast Download operation has started. CK722 only.

Fast Download Successful – Triggers when the Fast Download operation has successfully completed. CK722 only.

Firmware Upgrade Failed – Triggers when the firmware upgrade has failed at the CK722 panel.

Memory Low – Triggers when the CK722 panel memory is running low.

Memory Ok – Triggers when the CK722 panel memory is OK.

Panel Goes Offline (transition) – Triggers when the panel state has changed to offline.

Panel Goes Online (transition) – Triggers when the panel state has changed to online.

Panel Is Down (steady state) – Triggers when the panel is down. This trigger is to be used in combination with other trigger(s).

Panel Is Up (steady state) – Triggers when the panel is up. This trigger is to be used in combination with other trigger(s).

Panel Load Database From Flash (transition) – Triggers when the panel has loaded the database from flash memory. CK721 only.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Panel Name
- Time
- Timezone Active

Category: S300 Hardware

All events are triggered when the described condition is entered.

Hardware module fault – Triggers when the S300 hardware module is online, but indicates an error.

Hardware module not operational – Triggers when the S300 hardware module is down and not running.

Hardware module operational – Triggers when the S300 hardware module is up and running.

Hardware module upgrade failed – Triggers when the S300 hardware module firmware upgrade has failed.

Hardware module upgrading – Triggers when the S300 hardware module is receiving its firmware.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Station

Station Active (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Station Active state.

Station Inactive (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Station Inactive state.

Conditions

- Date

- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Stop and Search

Free Pass – Triggers when the Free Pass history message is received.

Interviewed – Triggers when the Interviewed history message is received.

Released – Triggers when the Released history message is received.

Released After Interview – Triggers when the Released After Interview history message is received.

Retained After Interview – Triggers when the Retained After Interview history message is received.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Terminal

All events are triggered when the described condition is entered.

Central data request – Triggers when the access decision is made by the server and not the panel.

Central status request – Triggers when the access decision is made either at the panel level or by the server.

DSO unknown – Triggers when any equipment associated with the Door Sequence Object (related inputs and outputs) is in an unknown state.

Incomplete group – Triggers when a badge presented at a reader is part of an incomplete group, and the entity group has been incomplete for more time than specified.

Input Terminal Goes Down (transition) – Triggers when an input terminal state has changed to down.

Input Terminal Goes Up (transition) – Triggers when an input terminal state has changed to up.

Input Terminal Is Down (steady state) – Triggers when an input terminal is down. This trigger is to be used in combination with other trigger(s).

Input Terminal Is Up (steady state) – Triggers when an input terminal is up. This trigger is to be used in combination with other trigger(s).

Output Terminal Goes Down (transition) – Triggers when an output terminal state has changed to down.

Output Terminal Goes Up (transition) – Triggers when an output terminal state has changed to up.

Output Terminal Is Down (steady state) – Triggers when an output terminal is down. This trigger is to be used in combination with other trigger(s).

Output Terminal Is Up (steady state) – Triggers when an output terminal is up. This trigger is to be used in combination with other trigger(s).

Reader fault – Triggers when the reader door is in fault state, indicating that there is an electrical or mechanical malfunction on the field equipment.

Reader forced open – Triggers when the reader door is opened without a valid badge read detected first.

Reader held open – Triggers when the reader door is opened with a valid badge, but the door is left opened past the shunt time.

Reader locked – Triggers when the reader door strike is locked and the door contact is not defined.

Reader locked and closed – Triggers when the reader door strike is locked and the door contact is closed.

Reader locked and Open – Triggers when the reader door strike is locked and the door contact is opened.

Reader Terminal Goes Down (transition) – Triggers when a reader terminal state has changed to down.

Reader Terminal Goes Up (transition) – Triggers when a reader terminal state has changed to up.

Reader Terminal Is Down (steady state) – Triggers when a reader terminal is down. This trigger is to be used in combination with other trigger(s).

Reader Terminal Is Up (steady state) – Triggers when a reader terminal is up. This trigger is to be used in combination with other trigger(s).

Reader unlocked – Triggers when the reader door strike is unlocked and the door contact is not defined.

Reader unlocked and closed – Triggers when the reader door strike is unlocked and the door contact is closed.

Reader unlocked and open – Triggers when the reader door strike is unlocked and the door contact is opened.

SUPPRESS forced door off – Triggers when a forced door exits the suppression state.

SUPPRESS FORCED DOOR ON – Triggers when a forced door enters the suppression state.

SUPPRESS PROPPED DOOR OFF – Triggers when a propped door exits the suppression state.

SUPPRESS PROPPED DOOR ON – Triggers when a propped door enters the suppression state.

SYSTEM FACILITY CODE ERROR – Triggers when a badge presented at the reader has an invalid facility code.

TIME OVERRIDE EXPIRED – Triggers when a timed override has expired.

TIMED OVERRIDE DISABLED – Triggers when a timed override has been manually disabled.

TIMED OVERRIDE DISABLED HOST – Triggers when a timed override has been manually disabled from the host.

TIMED OVERRIDE ENABLED – Triggers when a timed override has been manually enabled.

TIMED OVERRIDE ENABLED HOST – Triggers when a timed override has been manually enabled from the host.

UNACCOMPANIED ASSET – Triggers when a badge presented at a reader belongs to an unaccompanied asset, and the asset is not accompanied by the defined owner within the specified time.

UNACCOMPANIED ENTITY – Triggers when a badge presented at a reader belongs to an unaccompanied entity, and the entity is not accompanied by the defined sponsor within the specified time.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Panel Name
- Terminal Index*

- Terminal Name
- Time
- Timezone Active

* Not available for CK722 panels.

Category: Time & Attendance Reader

TIME&ATTENDANCE BREAK END – Triggers when the Time&Attendance Break End history message is received.

TIME&ATTENDANCE BREAK START – Triggers when the Time&Attendance Break Start history message is received.

TIME&ATTENDANCE LUNCH END – Triggers when the Time&Attendance Lunch End history message is received.

TIME&ATTENDANCE LUNCH START – Triggers when the Time&Attendance Lunch Start history message is received.

TIME&ATTENDANCE SHIFT END – Triggers when the Time&Attendance Shift End history message is received.

TIME&ATTENDANCE SHIFT START – Triggers when the Time&Attendance Shift Start history message is received.

Conditions

- <always>
- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Time Zone

BEGINNING OF PERIOD – Triggers when the time zone period has started.

End Of Period – Triggers when the time zone period has ended.

Conditions

- Time Zone

Category: Work Schedule

Work Schedule End – Triggers when the Work Schedule End history message is received.

Work Schedule Grace Period End – Triggers when the Work Schedule Grace Period End history message is received.

Work Schedule Grace Period Start – Triggers when the Work Schedule Grace Period Start history message is received.

Work Schedule Start – Triggers when the Work Schedule Start history message is received.

Conditions

- <always>
- Date
- Day of the Month
- Day of the Week
- Entity Category
- Month
- Name
- Time

Category: XMan Holding Room

Scan Aborted – Triggers when the Scan Aborted history message is received.

Scan Do – Triggers when the Scan Do history message is received.

Scan Done – Triggers when the Scan Done history message is received.

Scan Done Forced – Triggers when the Scan Done Forced history message is received.

Scan Dummy – Triggers when the Scan Dummy history message is received.

Scan Dummy Forced – Triggers when the Scan Dummy Forced history message is received.

Scan Error – Triggers when the Scan Error history message is received.

Scan Manual Rec – Triggers when the Scan Manual Rec history message is received.

Scan Operator Override – Triggers when the Scan Operator Override history message is received.

Scan Rejected – Triggers when the Scan Rejected history message is received.

Scan Search – Triggers when the Scan Search history message is received.

Scan Search Forced – Triggers when the Scan Search Forced history message is received.

Scan Status Invalid – Triggers when the Scan Status Invalid history message is received.

Scan Timeout – Triggers when the Scan Timeout history message is received.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: XMan XRay Machine

Busy – Triggers when the Busy history message is received.

Busy (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Busy state.

Configured – Triggers when the Configured history message is received.

Configured (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Configured state.

Created – Triggers when the Created history message is received.

Created (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Created state.

Fatal Error – Triggers when the Fatal Error history message is received.

Fatal Error (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Fatal Error state.

Invalid – Triggers when the Invalid history message is received.

Invalid (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Invalid state.

Not Connected – Triggers when the Not Connected history message is received.

Not Connected (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Not Connected state.

Not Ready – Triggers when the Not Ready history message is received.

Not Ready (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Not Ready state.

Ready – Triggers when the Ready history message is received.

Ready (Steady) – This trigger can be used to ensure that the event only triggers if the associated item is in the Ready state.

Conditions

- Date
- Day of the Month
- Day of the Week
- Month
- Name
- Time

Category: Zenitel Intercom Station

Station Busy (transition) – Triggers when the intercom station is busy.

Station Call Request (transition) – Triggers when a call request has been placed to the intercom station.

Station Connected (transition) – Triggers when the intercom station has been connected.

Station Idle (transition) – Triggers when the intercom station shows no activity.

Conditions

- Date
- Day of the Month
- Day of the Week
- Intercom Station
- Month
- Time

Event Action Types

Category: Anti-Passback

Entity In – Adjust the status of entities to *In*. Entities will be able to make exit requests again at the selected Anti-Passback area.

Entity Out – Adjust the status of entities to *Out*. Entities will be able to make entry requests again at the selected Anti-Passback area.

Entity Undefined – Adjust the status of entities to *Undefined*. Entities will be able to make entry or exit requests again at the selected Anti-Passback area.

Reset All – Changes the entry/exit status of ALL entities in the selected Anti-Passback area. The status will change to the Default Status defined in the Anti-Passback object (In, Out, or Undefined). For example, if the Anti-Passback Default Status is set to In and you select Reset All, the entry/exit status of all entities will change to In.

Resynchronize Entity Status – Adjusts the status of entities to *In*, *Out* or *Undefined*.

Category: Audio-Visual

Camera Complete Alarm – Completes an alarm generated by the selected camera.

Camera Complete Alarm Associated Input – Completes an alarm generated by any configured camera that is associated with an input created in Input to Camera mapping.

Camera Complete Alarm Associated Terminal – Completes an alarm generated by any configured camera that is associated with a terminal mapped in Input to Camera.

Camera Preset – Activates the camera's preset action.

Camera Recording Quality – Changes the camera's recording quality.

Camera Send Alarm – Sends an alarm message of any configured camera.

Camera Send Alarm Associated Input – Sends an alarm message of any configured camera that is associated with an input created in Input to Camera mapping.

Camera Send Alarm Associated Terminal – Sends an alarm message of any configured

camera that is associated with a terminal mapped in Input to Camera.

Camera Start Recording – Starts the recording of any configured camera.

Camera Start Recording and Archiving – Starts the recording and archiving of any configured camera.

Camera Start Recording Associated Input – Starts the recording of any configured camera that is associated with an input created in Input to Camera mapping.

Camera Start Recording Associated Terminal – Starts the recording of any configured camera that is associated with a reader reporting access grant or access deny transactions.

Camera Stop Recording – Stops the recording of any configured camera.

Camera Stop Recording Associated Input – Stops the recording of any configured camera that is associated with an input created in Input to Camera mapping.

Camera Stop Recording Associated Terminal – Stops the recording of any configured camera that is associated with a terminal mapped in Input to Camera.

Launch AV Player – Launches de AV Player application at the selected workstation.

Monitor Camera – Displays the image from a particular camera on the monitor.

Category: BACnet

Interlock – Activates an action interlock to initiate an action in a BACnet device.

Category: Badge

Add Access Group and Timezone – Adds the specified access group and time zone to the

badge associated with the message that triggered the event. The access group and time zone are added in the first available position of the badge.

Add Access Group and Timezone to Cardholder

– Adds the specified access group and time zone to all badges associated with the entity displayed in the message that triggered the event. The access group and time zone are added in the first available position of all badges.

Delete Access Group – Deletes the specified access group from the badge associated with the message that triggered the event.

Delete Access Group to Cardholder – Deletes the specified access group from all badges associated with the entity displayed in the message that triggered the event.

Set Badge Security Level – Sets the badge security level at the specified value.

Set Badge Security Level to Reader Security Level – Sets the badge security level to match the security level at the terminal.

Category: CCTV

Camera Auxiliary Play – Activates the camera's auxiliary relay.

Camera Auxiliary Stop – Deactivates the camera's auxiliary relay.

Camera Pattern Play – Activates the camera's pattern.

Camera Pattern Stop – Deactivates the camera's pattern.

Camera Preset – Activates the camera's preset action.

Monitor Camera – Displays the image from a particular camera on the monitor.

Monitor Sequence Play – Displays a sequence of camera images on the monitor.

Monitor Sequence Stop – Stops the display of a sequence of camera images on the monitor.

Switch Alarm Play – Activates the alarm switch.

Switch Alarm Stop – Deactivates the alarm switch.

Switch Auxiliary Play – Activates the auxiliary switch.

Switch Auxiliary Stop – Deactivates the auxiliary switch.

Switch Macro Play – Activates a set of programmed steps to be performed by the switch.

Switch Macro Stop – Deactivates a set of programmed steps to be performed by the switch.

Switch Tour Play – Activates a combination of camera patterns and monitor sequences.

Switch Tour Stop – Deactivates a combination of camera patterns and monitor sequences.

Category: CK722 BACNet

Write Attribute – Writes a value in the attribute type selected to the selected object type.

Write Attribute from Counter – Writes a counter value in the attribute type selected to the selected object type.

Category: Download - BACNet

All Access Groups – Downloads all defined access groups to the selected CK722 panel.

All Access Profiles – Downloads all defined access profiles to the selected CK722 panel.

All Entities – Downloads all defined entities to the selected CK722 panel.

All Entity Groups – Downloads all defined entity groups to the selected CK722 panel.

All Identifiers – Downloads all defined identifiers to the selected CK722 panel.

All Intrusion Groups – Downloads all defined intrusion groups to the selected CK722 panel.

Category: Download - Legacy

Download Access Groups – Downloads all defined access groups to the selected panel.

Download All Badges – Downloads all defined badges to the selected panel.

Download All Input Points – Downloads all defined input points to the selected panel.

Download All Output Points – Downloads all defined output points to the selected panel.

Download All Terminals – Downloads all defined terminals to the selected panel.

Download All Time Zones – Downloads all defined time zones to the selected panel.

Download All to All Panels – Downloads all defined access groups, badges, input and output points, terminals, time zones, card events, holidays, and soft alarms to all panels.

Download All to Panel – Downloads all defined access groups, badges, input and output points, terminals, time zones, card events, holidays, and soft alarms to the selected panel.

Download Card Events – Downloads all defined card events to the selected panel.

Download Holidays – Downloads all defined holidays to the selected panel.

Download Panel – Downloads panel information to the selected panel.

Download Soft Alarms – Downloads all defined soft alarms to the selected panel.

Category: Host

Backup Database – Performs database backup of the P2000 Entity Configuration and/or the P2000 History according to schedule.

Cancel Event – Cancels the selected event.

Create Alarm – Creates an alarm and sends it to the Alarm Monitor using an alarm instruction text as the description and a specified alarm category.

Create Alarm Unique – Creates a unique alarm and sends it to the Alarm Monitor using an alarm instruction text as the description and a specified alarm category.

Decrement Counter – Decrements the value of the selected counter.

Delete Expired Visitor Badges – Deletes expired visitor badges.

Delete Unused Access Groups – Deletes all unused access groups in the system.

Delete Visitors Without Badges – Deletes visitors without badges.

Disable Badge – Disables the selected badge number.

Display Map – Displays a specified map at the selected workstation.

Display Message – Displays a pre-defined instruction text message at the selected workstation.

Execute Application – Launches an application at the workstation selected.

Increment Counter – Increments the value of the selected counter.

Message Filter – Adds or removes a specified Message Filter to the selected Message Filter Group. This action only deletes filters that have been “Auto Added” by another event. It

never deletes the original filters configured for this group.

Message Filter Group – Adds or removes a specified Message Filter Group to the selected Message Filter Group. This action only deletes filters that have been “Auto Added” by another event. It never deletes the original filters configured for this group.

Message Forwarding – Enables or disables message forwarding from/to the selected workstation.

Net Send Message – Uses the Net Send command to send instruction text to a selected computer on the network.

Open Document – Opens a document at the workstation selected.

Print Message – Sends a pre-defined instruction text message to a selected printer.

Real Time Printing – Enables or disables real time printing.

Real Time Printing Access Deny – Enables or disables real time printing of Access Deny transactions.

Real Time Printing Access Grant – Enables or disables real time printing of Access Grant transactions.

Real Time Printing Alarm – Enables or disables real time printing of Alarm transactions.

Real Time Printing Area – Enables or disables real time printing of Area transactions.

Real Time Printing Audit – Enables or disables real time printing of Audit transactions.

Real Time Printing AV – Enables or disables real time printing of Audio-Visual transactions.

Real Time Printing Cabinet – Enables or disables real time printing of Cabinet transactions.

Real Time Printing Elevator – Enables or disables real time printing of Elevator transactions.

Real Time Printing Guard Tour – Enables or disables real time printing of Guard Tour transactions.

Real Time Printing Host – Enables or disables real time printing of Host transactions.

Real Time Printing Intrusion – Enables or disables real time printing of Intrusion transactions.

Real Time Printing Mustering – Enables or disables real time printing of Mustering transactions.

Real Time Printing Panel – Enables or disables real time printing of Panel transactions.

Real Time Printing Trace – Enables or disables real time printing of Trace transactions.

Remote Server Receive – Enables or disables receiving remote messages at the selected remote server.

Remote Server Transmit – Enables or disables transmitting remote messages at the selected remote server.

Resync Badges – Adjusts the state of the selected badge(s) to In, Out or Undefined and gives you the option to download the change.

Resync Badges - Last Terminal – Adjusts the state of all badges presented at the selected terminal to In, Out or Undefined and gives you the option to download the change.

Resync Badges - Last Terminal Group – Adjusts the state of all badges presented at the terminals in the selected terminal group to In, Out or

Undefined and gives you the option to download the change.

Send Email – Sends a pre-defined instruction text message as email to the specified address.

Serial Port Message – Sends a pre-defined instruction text message as a serial port message using the COM port selected.

Set Counter – Sets the counter to a selected value.

Trigger Event – Triggers the selected event.

UDF Decrement – Decrements the specified numeric UDF field by one for the entity displayed in the message that triggered the event.

UDF Increment – Increments the specified numeric UDF field by one for the entity displayed in the message that triggered the event.

UDF Set – Sets the specified numeric UDF field to the specified value for the entity displayed in the message that triggered the event.

UDF Set to UDF – Sets the first specified numeric UDF field to the value of the second specified numeric UDF field for the entity displayed in the message that triggered the event.

Category: Inputs

Acknowledge Alarm – Acknowledges an alarm.

Complete Alarm – Completes an alarm.

Input Group Disable – Disables an input group.

Input Group Enable – Enables an input group.

Input Group Suppress – Suppresses the selected Input Group for the specified time (0 seconds means forever). This action is only valid for CK720/CK705 panels version 2.5 and higher.

Input Group Suppression Time Zone – Suppresses the selected Input Group during the specified Time Zone.

Input Group Unsuppress – Unsuppresses the selected Input Group. This action is only valid for CK720/CK705 panels version 2.5 and higher.

Input Point Disable – Disables a selected input point.

Input Point Enable – Enables a selected input point.

Input Point Suppress – Suppresses the selected Input Point for the specified time (0 seconds means forever). This action is only valid for CK720/CK705 panels version 2.5 and higher.

Input Point Suppression Time Zone – Suppresses the selected Input Point during the specified Time Zone.

Input Point Unsuppress – Unsuppresses the selected Input Point. This action is only valid for CK720/CK705 panels version 2.5 and higher.

Category: Intercom

Connect – Connects the selected intercom station.

Disconnect – Disconnects the selected intercom station.

Category: Intrusion Announcer

Activate – Activates the selected intrusion annunciator.

Silence – Deactivates the selected intrusion annunciator.

Category: Intrusion Area

Arm – Arms the selected area.

Disarm – Disarms the selected area.

Category: Intrusion Zone

Reset – Resets the selected intrusion zone.

ResetAck – Resets and acknowledges the selected intrusion zone.

Zone Bypass Off – Intrusion activities will not be detected at the selected intrusion zone.

Zone Bypass On – Intrusion activities will be detected at the selected intrusion zone.

Category: MCO

Change MCO State – Changes the selected Multiple Command Object to the selected state.

Category: Metasys Interlock

Metasys Interlock – Writes to a selected Metasys system extended architecture object.

Category: Mustering

De-Muster – Resets personnel to their last badge location after the Muster is terminated for the selected Zone.

Make Zone Ready – Resets zone status after a muster is stopped so that the zone is ready for another muster.

Mustering Start – Starts the muster in the selected Zone.

Mustering Stop – Ends the muster at the selected Zone.

Save Muster Data – Saves the muster data in the database.

Category: Occupancy

Set maximum number of occupancy – Sets the number of entities allowed in the selected occupancy space.

Category: OPC Server

OPC Write – Writes an OPC Tag value in the data type selected.

Category: Outputs

Reset Output – Resets the selected output.

Reset Output Group – Resets the selected output group.

Set Output – Sets the selected output for the specified duration.

Set Output Group – Sets the selected output group for the specified duration.

Category: Panel

Doors - Resume Normal Operation – Returns all doors to their previous state.

Doors - Unlock All Doors – Unlocks all doors.

History Upload Disable – Disables history upload at the selected panel.

History Upload Enable – Enables history upload at the selected panel.

In-X-It Disable – Disables the entry/exit feature at the selected panel.

In-X-It Enable – Enables the entry/exit feature at the selected panel.

Set Time Offset – Sets the time offset of the selected panel by the specified number of minutes.

Time Zone Check No – Disables time zone checking.

Time Zone Check Yes – Enables time zone checking.

Category: Security Level

Clear – Removes the security level at the selected Panel, Terminal or Terminal Group.

Set to Blue – Applies a Blue code security level at the selected Panel, Terminal or Terminal Group.

Set to Green – Applies a Green code security level at the selected Panel, Terminal or Terminal Group.

Set to Orange – Applies an Orange code security level at the selected Panel, Terminal or Terminal Group.

Set to Other – Applies a specific code security level at the selected Panel, Terminal or Terminal Group.

Set to Red – Applies a Red code security level at the selected Panel, Terminal or Terminal Group.

Set to Yellow – Applies a Yellow code security level at the selected Panel, Terminal or Terminal Group.

Category: Terminal

Anti-Passback Disable – Disables the anti-passback feature at the selected reader, that is, a person will be able to re-badge at the same door without delay.

Anti-Passback Enable – Enables the anti-passback feature at the specified reader for the period of time selected.

Door Timed Override – Enables from the host, the door timed override feature at the specified reader for the period of time selected.

Local Timed Override Disable – Disables timed override at the specified reader for the period of time entered at the keypad.

Local Timed Override Enable – Enables timed override at the specified reader for the period of time entered at the keypad.

Open for Access Time – Unlocks the door for the number of seconds defined at the reader.

Pin Suppression - set Time Zone – Enables PIN Suppression at the specified reader during the Time Zone selected.

Reader - set Time Zone – Enables the specified reader during the Time Zone selected.

Reader Override - Disable – Disables reader override at the specified reader.

Reader Override - Enable – Enables reader override at the specified reader.

Reader Override - set Time Zone – Unlocks the specified reader door during the Time Zone selected.

Reader Valid & Unauthorized - Disable – Disables the valid & unauthorized feature at the specified reader.

Reader Valid & Unauthorized - Enable – Enables the valid & unauthorized feature at the specified reader.

Soft In-X-It Processing Disable – Disables the Soft In-X-It Processing feature at the specified reader.

Soft In-X-It Processing Enable – Enables the Soft In-X-It Processing feature at the specified reader.

Stop Timed Override – Stops the time override mode. The door will no longer be unlocked for an extended period of time.

Suppress Forced/Propped Inputs – Suppresses forced/propped inputs at the selected reader for the specified time (0 seconds means forever). This action is only valid for CK720/CK705 panels version 2.5 and higher.

Terminal Enable – Enables or disables the terminal selected.

Unsuppress Forced/Propped Inputs – Unsuppresses forced/propped inputs at the selected reader. This action is only valid for CK720/CK705 panels version 2.5 and higher.

Appendix B: Message Types and Sub-Types

This appendix lists all Message Types and Sub-Types available for Message Filtering configuration. For more information see “Message Filtering” on page 100.

Message Types
1 – Notify
3 – Alarm
5 – System Action
258 – Muster Status
259 – Muster Event Trigger
305 – Routing Session
417 – SIA Messages
28673 – RTL Data
28675 – Audit

Message Sub-Types
1 – Notify
204 – Alarm Filter
207 – Comms Up
208 – Comms Down
210 – Guard Tour Up
3 – Alarm
1 – Generic Alarm
2 – Panel Input Point Alarm
3 – Area Alarm
4 – Guard Tour Alarm
5 – Muster Running Alarm
6 – Muster Zone Status Alarm
7 – Muster When Disabled Alarm
8 – Muster Aborted
9 – Loop Tamper Alarm
10 – Host Event Generated Alarm
11 – MSEA Alarm
12 – AV Motion Alarm
13 – AV Behavior Alarm

Message Sub-Types (Continued)
3 – Alarm (continued)
14 – AV Video Loss Alarm
15 – AV Dry Contact Alarm
16 – AV System Alarm
17 – Intrusion Zone Alarm
18 – Access Rights Expired
19 – Alternate Access Granted
20 – Asset Tracked
21 – Central Access Denied
23 – Central Data Unreachable
24 – Central Status Unreachable
25 – Entity Expired
26 – Entity Tracked
27 – Entity Validated
28 – Error
29 – Incomplete Group
30 – Incomplete Group Rule
31 – Inconsistent Identifiers
32 – Invalid Access Level
33 – Invalid Access Mask
34 – Invalid Access Profile
35 – Invalid Access Group
36 – Invalid Access Group Timezone
37 – Invalid Override Privilege
38 – Invalid Override Time
39 – PIN Attempts Exceeded
40 – Invalid Security Mask
41 – Invalid Smart Card Signature
42 – Manual Panel Event
43 – No Entry
44 – Occupancy Violation
45 – Portal Open Violation
46 – Team Member Validated
47 – Unaccompanied Asset
48 – Unaccompanied Asset Rule
49 – Unaccompanied Entity
50 – Unaccompanied Entity Rule
51 – Anti-Loitering Violation
52 – Occupancy Limit
53 – Fault
54 – Anti-Passback Not Operational
55 – Anti-Passback On
58 – Output
59 – Biometric Mismatch
60 – Deny Intrusion Area Armed

Message Sub-Types (Continued)	Message Sub-Types (Continued)
3 – Alarm (continued) 61 – Door Status 62 – Facility Code Error 63 – Hardware Module not operational 64 – Hardware Module upgrade failed 65 – Hardware Module upgrading 66 – Intrusion Annunciator 67 – Intrusion Area Arm State 71 – Intrusion Zone Arm State 74 – Invalid Card 75 – Invalid Entity 76 – Invalid Event 77 – Invalid Event Privilege 78 – Invalid Entry-Exit 79 – Invalid Issue Level 80 – Invalid PIN Code 81 – Invalid Reader 82 – Invalid Security Level 83 – Local Grant 84 – Manual Reader 85 – Notification Event Dropped 89 – Timed Override 90 – Panel Down 91 – Forced Door Suppressed 92 – Controller Event Activate 93 – Controller Event Inactive 94 – Memory Low 95 – Propped Door Suppressed 96 – Intrusion Area 97 – Fast Download Started 98 – Fast Download Failed 99 – Fast Download Succeeded 100 – Elevator 101 – Elevator Controller Not Operational 102 – Reader Dures 103 – Soft AntiPassback Violation 104 – Soft Occupancy Violation 105 – Executive Privilege 106 – Intrusion Annunciator Silence 107 – Firmware Upgrade Failed 108 – High CPU Usage 109 – Anti-Passback Resynch 110 – Anti-Passback Reset 112 – Entity Transition In 113 – Entity Transition Out 114 – Entity Transition Undefined 115 – Entity Entry Time Reset 116 – Entity Exit Time Reset 117 – Entity Configuration Mismatch 118 – ACO not operational 119 – Interlock State 120 – Integration Server 121 – Time Synchronization Problem	3 – Alarm (continued) 122 – XMan X-Ray Machine 123 – Device Failure 124 – Device Down 125 – LEC Door Status 126 – APM Status
	5 – System Action 2 – Error or Log 4 – Counter Changed 5 – Muster Control Started
	258 – Muster Status
	259 – Muster Event Trigger
	305 – Routing Session
	417 – SIA Messages
	28673 – RTL Data 1 – Panel: Reader Up 3 – Panel: System Restart 5 – Panel: Reader Down 8 – Panel: System Image Success 9 – Panel: System Image Fail 10 – Panel: Facility Code Error 11 – Panel: System Event Activated 12 – Panel: System Event Deactivated 15 – Panel: Unlock All Doors 16 – Panel: Lock All Doors 17 – Panel: Output Set 18 – Panel: Output Reset 19 – Panel: Reader Locked 20 – Panel: Reader Unlocked 21 – Panel: Reader Held Open 22 – Panel: Reader Forced Open 23 – Panel: Valid and Unauthorized 32 – Terminal: Major Deny 33 – Access Deny: Invalid Card 34 – Access Deny: Anti-Passback On 35 – Access Deny: Invalid Reader 36 – Access Deny: Invalid Entry-Exit 37 – Access Deny: Invalid Access Gr Timezone 38 – Access Deny: Invalid PIN Code 39 – Access Deny: Invalid Issue Level 40 – Access Deny: Host Deny (NMAN Rule) 41 – Access Deny: Invalid Security Level 42 – Panel: Invalid Reader Timezone 43 – Panel: Timed Override Expired 44 – Access Deny: Invalid Event 45 – Access Deny: Invalid Event Privilege

Message Sub-Types (Continued)	
28673 – RTL Data (continued)	
46 – Access Deny: Biometric Mismatch	258 – Host: Redundancy Data Link
47 – Access Deny: Open Door	259 – Host: Redundancy IO Link
48 – Access Deny: Denied Intrusion Area Armed	260 – Host: Redundancy HD Primary System
64 – Access Grant: Major Grant	261 – Host: Redundancy HD Standby System
65 – Access Grant: Host Grant	264 – Host: Redundancy Serial PS Link
67 – Access Grant: Executive Privilege	266 – Access Grant: Host Grant Entry
68 – Access Grant: Local Grant	267 – Access Grant: Host Grant Exit
69 – Access Grant: Timed Override Enabled	268 – Access Grant: Host Duress Grant (Entry)
70 – Access Grant: Timed Override Disabled	269 – Access Grant: Host Duress Grant (Exit)
71 – Access Grant: Timed Override Enabl Host	287 – Audio Visual: VCR Tape Low
72 – Access Grant: Timed Override Disabl Host	288 – Audio Visual: Major Module
73 – Panel: Panel Card Event Activated	289 – Audio Visual: VCR Reel Lock
74 – Panel: Panel Card Event Deactivated	290 – Audio Visual: VCR Cylinder Lock
75 – Access Grant: Soft In-X-It Violation	291 – Audio Visual: VCR Mechanical Lock
76 – Assisted Access: Assisted Access	292 – Panel: Input Module Up
77 – Assisted Access: Assisted Access Host	293 – Panel: Output Module Up
78 – Access Grant: Manual Reader	294 – Panel: Input Module Down
79 – Elevator: Elevator Access Grant	295 – Panel: Output Module Down
80 – Access Grant: Reader Egress	296 – Terminal: All Modules Up
81 – Access Grant: Duress Grant	297 – Terminal: All Modules Down
82 – Access Grant: Host Duress Grant	768 – Audio Visual: CCTV No Response
96 – Input Point History: Alarm Set	769 – Audio Visual: CCTV Incorrect Response
97 – Input Point History: Alarm Reset	770 – Audio Visual: CCTV Control Down-Up
98 – Panel: Alarm Acknowledge	771 – Audio Visual: CCTV Control Up-Down
99 – Panel: D620 Tamper Alarm Set	772 – Audio Visual: CCTV Normal
100 – Panel: D620 Tamper Alarm Reset	773 – Audio Visual: AV Monitor Set
101 – Panel: Door Open Alarm	774 – Audio Visual: AV Monitor Not Set
102 – Panel: Duress	775 – Audio Visual: AV Camera Set
103 – Panel: PIN Code Retry Alarm	776 – Audio Visual: AV Camera Not Set
104 – Panel: Forced Door Alarm	777 – Audio Visual: CCTV Command Error
105 – Panel: Card Parity Alarm	778 – Audio Visual: CCTV Transmission Error
106 – Panel: Prox Card Low Battery Alarm	784 – Input Point: Input Point Pending Alarm
107 – Panel: D620 AC Power Set Alarm	785 – Input Point: Input Point Acknwl. Alarm
108 – Panel: D620 AC Power Reset Alarm	786 – Input Point: Input Point Responded Alarm
109 – Panel: D620 Low Battery Set Alarm	787 – Input Point: Input Point Pending Secure
110 – Panel: D620 Low Battery Reset Alarm	788 – Input Point: Input Point Acknwl. Secure
111 – Panel: Reader Low Battery Set Alarm	789 – Input Point: Input Point Responded Secure
112 – Panel: Reader Low Battery Reset Alarm	790 – Input Point: Input Point Pending Open
113 – Panel: Reader AC Set Alarm	791 – Input Point: Input Point Acknwl. Open
114 – Panel: Reader AC Reset Alarm	792 – Input Point: Input Point Responded Open
115 – Panel: Reader Tamper Set Alarm	793 – Input Point: Input Point Pending Short
116 – Panel: Reader Tamper Reset Alarm	794 – Input Point: Input Point Acknwl. Short
117 – Input Point History: Alarm Open	795 – Input Point: Input Point Responded Short
118 – Input Point History: Alarm Short	1024 – Host: Redundancy Crash
123 – Panel: Calibrated	1025 – Host: Redundancy Restore
125 – Input Point History: Alarm Suppressed	1026 – Host: Redundancy Power Up
224 – Panel: Node Up	1027 – Host: Redundancy Shutdown
225 – Panel: Fallback	1028 – Host: Redundancy Started
226 – Panel: Converter Tamper Set Alarm	1029 – Host: Redundancy Network Failure
227 – Panel: Converter Tamper Reset Alarm	1030 – Host: Redundancy Network Restore
228 – Panel: Node Down	1031 – Host: Redundancy Serial Failure
256 – Host: Redundancy Primary System	1032 – Host: Redundancy Serial Restore
257 – Host: Redundancy Standby System	1033 – Host: Redundancy Wall Power UPS

Message Sub-Types (Continued)	Message Sub-Types (Continued)
<p>28673 – RTL Data (continued)</p> <p>1034 – Host: Redundancy Periodic Check 1035 – Host: Redundancy Modem Check 1280 – Intrusion Annunciator: Intrs Annun Silence 1281 – Panel: Intrusion Annunciator Error 1282 – Intrusion Annunciator: Intr Annun Unknown 1283 – Intrusion Annunciator: Intrs Annun Active 1284 – Intrusion Annunciator: Intrs Annun Inactive 1296 – Intrusion Area: Intrusion Area Armed 1297 – Intrusion Area: Intrusion Area Disarmed 1298 – Intrusion Area: Intrusion Area Mixed 1300 – Intrusion Area: Intrusion Area Arming 1301 – Intrusion Area: Intrusion Area Disarming 1302 – Panel: Intrusion Area Error 1303 – Intrusion Area: Intrusion Area Unknown 1304 – Intrusion Zone: Intrusion Area Fault 1312 – Panel: Intrusion Keypad Error 1313 – Intrusion Keypad: Intrs Keypad Unknown 1328 – Intrusion Zone: Intrusion Zone Alarm 1329 – Intrusion Zone: Intrusion Zone Bypass 1332 – Intrusion Zone: Intrusion Zone Acknow. 1333 – Panel: Intrusion Zone Error 1334 – Intrusion Zone: Intrusion Zone Unknown 1335 – Intrusion Zone: Intrusion Zone Normal 1337 – Intrusion Zone: Intrs Zone Alarm Trouble 1338 – Intrusion Zone: Intrs Zone Alarm Tamper 1339 – Intrusion Zone: Intrusion Zone Alarm Open 1340 – Intrusion Zone: Intrusion Zone Alarm Short 1341 – Intrusion Zone: Intrusion Zone Armed 1342 – Intrusion Zone: Intrusion Zone Disarmed 1343 – Intrusion Zone: Intrusion Zone Fault 1344 – Intrusion Zone: Intrusion Zone Arming 1345 – Intrusion Zone: Intrusion Zone Disarming 1346 – Intrusion Zone: Zone Unbypassed 1347 – Intrusion Zone: Zone Tamper 1348 – Intrusion Zone: Zone Open 1349 – Intrusion Zone: Zone Sealed 1350 – Intrusion Area: Area Zones Bypassed 1351 – Intrusion Area: Area Zones Unbypassed 1352 – Intrusion Area: Area Zones Sealed 1353 – Intrusion Area: Area Zones Unsealed 1354 – Intrusion Device: Device Connected 1355 – Intrusion Device: Device Disconnected 1356 – Intr Device: Device Invalid Vendor Address 1357 – Intr Device: Device Valid Vendor Address 1358 – Intrusion Device: Device Port Opened 1359 – Intrusion Device: Device Port Closed 1360 – Intrusion Device: Device Mains Failure 1361 – Intrusion Device: Device Mains Normal 1362 – Intrusion Device: Device Battery Low 1363 – Intrusion Device: Device Battery Normal 1364 – Intrusion Device: Device Battery Test 1365 – Intrusion Device: Device Battery Test Done</p>	<p>28673 – RTL Data (continued)</p> <p>1366 – Intr Device: Device Battery Test Failure 1367 – Intr Device: Device Battery Test Success 1368 – Intr Device: Device Battery Test Missing 1369 – Intr Device: Device Battery Test Inplace 1536 – Access Deny: Invalid Entity 2023 – Panel: Memory Low 2024 – Panel: Memory Normal 4096 – Panel: ACO Error 4097 – Panel: Central Data Request 4098 – Panel: Central Status Request 4099 – Panel: Manual Panel Event 4101 – Panel: Asset Tracked 4102 – Panel: Entity Tracked 4103 – Panel: Entity/Asset Validated 4104 – Panel: Team Member Validated 4105 – Access Grant: Alternate Access Granted 4107 – Access Grant: No Entry 4111 – Access Deny: PIN Attempts Exceeded 4113 – Access Deny: Invalid Access Group 4115 – Access Deny: Invalid Access Mask 4116 – Access Deny: Invalid Access Level 4117 – Access Deny: Invalid Security Mask 4121 – Access Deny: Occupancy Violation 4122 – Access Deny: Invalid Override Time 4123 – Access Deny: Invalid Override Privilege 4124 – Access Deny: Central Data Unreachable 4125 – Access Deny: Central Status Unreachable 4126 – Access Deny: Central Access Denied 4127 – Access Deny: Access Rights Expired 4128 – Access Deny: Entity Expired 4129 – Access Deny: Unaccompanied Asset Rule 4130 – Access Deny: Unaccompanied Entity Rule 4131 – Access Deny: Incomplete Group Rule 4132 – Access Deny: Portal Open Violation 4133 – Access Deny: Unaccompanied Asset 4134 – Access Deny: Unaccompanied Entity 4135 – Access Deny: Incomplete Group 4137 – Access Deny: Invalid Access Profile 4138 – Access Deny: Inconsistent Identifiers 4140 – Access Deny: Invalid Smart Card Signature 4353 – Panel: DSO Fault 4354 – Panel: Door Locked and Open 4355 – Panel: Door Locked and Closed 4356 – Panel: Door Unlocked and Open 4357 – Panel: Door Unlocked and Closed 4358 – Panel: Door Status Unknown 4359 – Panel: Suppress propped door on 4360 – Panel: Suppress propped door off 4361 – Panel: Suppress forced door on 4362 – Terminal: Suppress forced door off 4384 – Panel: Fast Download Started 4385 – Panel: Fast Download Succeeded</p>

Message Sub-Types (Continued)	Message Sub-Types (Continued)
<p>28673 – RTL Data (continued)</p> <p>4386 – Panel: Fast Download Failed 4608 – Input Point History: Supervised Inpt Unknw 4688 – Panel: Output Unknown 4704 – Panel: Notification Events Dropped 4720 – Panel: Controller Event Activated 4721 – Panel: Controller Event Deactivated 4722 – Panel: Controller Event Error 20481 – Panel: Node Up Duplicate 20482 – Panel: Reader Status Unknown 20483 – Panel: Input Status Unknown 20484 – Panel: Output Status Unknown 20485 – Panel: Node Disconnected 20486 – Panel: Node Misconfigured 20487 – Panel: Panel Reboot from Flash 20576 – Input Point State Change: Input Point Set 20577 – Input Point State Change: Input Pt Reset 20597 – Input Point State Change: Input Pt Open 20598 – Input Point State Change: Input Pt Short 20599 – Input Point State Change: Input Pt Suppres. 20600 – Input Point State Change: Input Pt Unknw 24577 – Host: Event Triggered 24578 – Host: Event Triggered Manually 28673 – Tour: Duress Alarm 28674 – Tour: Start 28675 – Tour: Running 28676 – Tour: Station Early 28677 – Tour: Station Late 28678 – Tour: Out of Order 28679 – Tour: Stopped 28680 – Tour: Restarted 28681 – Tour: Aborted 28682 – Tour: Completed 28683 – Tour: Late Time 28684 – Tour: Terminated 32769 – Area: Area Reader Exit 32770 – Area: Area Reader Entry 32771 – Area: Area Input Exit 32772 – Area: Area Input Entry 32773 – Area: Area Manual Exit 32774 – Area: Area Manual Entry 36865 – Audio-Visual: AV Motion 36866 – Audio-Visual: AV Behavior 36867 – Audio-Visual: AV Video Loss 36868 – Audio-Visual: AV Dry Contact 36869 – Audio-Visual: AV System 40976 – Panel: Occupancy Within Limits 40977 – Panel: Occupancy At Low Limit 40978 – Panel: Occupancy At High Limit 40979 – Panel: Occupancy Below Limit 40980 – Panel: Occupancy Above High Limit 40981 – Panel: Fault 40982 – Panel: Fault - Invalid Configuration 40983 – Panel: Out of Memory Fault</p>	<p>28673 – RTL Data (continued)</p> <p>40984 – Panel: General Fault 40985 – Panel: Occupancy Fault 40992 – Panel: Anti-Passback Operational 40993 – Panel: Anti-Passback not Operational 40994 – Panel: Anti-Passback Peers Offline 40995 – Panel: Anti-Passback-Star Center Offline 40996 – Panel: Anti-Passback Fault 41008 – Panel: Hardware Module Operational 41009 – Panel: Hardware Module not Operational 41010 – Panel: Hardware Module Upgrading 41011 – Panel: Hardware Module Upgrade Failed 41012 – Panel: Hardware Module Fault 41040 – Panel: Anti-Loitering Violation 41041 – Host: Unprocessed Event 41066 – Panel: Security Level Changed 45057 – Host: Intrusion Up 45058 – Host: Intrusion Down</p> <p>28675 – Audit</p> <ul style="list-style-type: none"> 0 – Unknown 1 – User 2 – Badge 3 – Badge Layout 4 – Badge Fields 5 – Badge Encode 6 – ID Badge 7 – Entity 8 – Panel 9 – Terminal 10 – Partition 11 – Terminal Group 12 – Access Group 13 – Holiday 14 – Timezone 15 – Input Point 16 – Input Group 17 – Panel Holiday 18 – Access Template 19 – Alarm Response Text 20 – Alarm Instruction 21 – Company 22 – Output Point 23 – Output Group 24 – Department 25 – Panel Timezone 26 – Soft Alarm 27 – Site Parameters 28 – Workstation 29 – Map 30 – Map Icon Set 31 – User Defined Field 32 – Event 33 – Panel Card Event 34 – Alarm Filter

Message Sub-Types (Continued)		Message Sub-Types (Continued)	
28675 – Audit (continued)		28675 – Audit (continued)	
35 – Message Forwarding		89 – Security Level Range	
37 – Permission Group		90 – Import File	
38 – Panel Relay		91 – Import Consolidation	
39 – Report		92 – Import Badge Format	
40 – MIS Interface		94 – Audit	
41 – Image Recall Filter		95 – Alarm History	
42 – Counter		96 – Alarm	
43 – Action Interlock		97 – Generic Text	
44 – External IP Address		98 – Muster History	
45 – Guard Tour Definition		99 – Guard Tour History	
46 – Tour Station Definition		100 – Transaction History	
47 – Loop		101 – Redundancy	
48 – Elevator		102 – Mapping Configuration	
49 – Floor Mask		103 – Mapping Data Fields Configuration	
50 – Floor Group		104 – Intercom Exchange	
51 – Floor Name Configuration		105 – Intercom Station	
52 – Cabinet		106 – AV Site	
53 – Door Group		107 – AV Camera	
54 – Door Mask		108 – AV Monitor	
55 – Door Name Configuration		109 – AV Preset	
56 – Area		110 – Input To Camera	
57 – Muster Zone		112 – Enterprise Site	
58 – Area Control Layout		113 – Enterprise Parameters	
59 – Connections		114 – AV Dry Contact	
60 – CCTV Server		115 – Alarm Colors	
61 – CCTV Switch		116 – Badge Setup	
62 – CCTV Tour		117 – Request Approver	
63 – CCTV Alarm		118 – FASC-N CCC	
64 – CCTV Macro		119 – Identifier Purpose	
65 – CCTV System Auxiliary		120 – Alarm Options	
66 – CCTV Monitor		122 – SIA Device	
67 – CCTV Sequence		123 – Alarm Category	
68 – CCTV Camera		124 – MSEA Graphic	
69 – CCTV Preset		125 – Entity Group	
70 – CCTV Pattern		126 – Access Profiles	
71 – CCTV Camera Auxiliary		127 – Application Resource	
72 – Enable Code		128 – Security Flag	
73 – P900 Flag		129 – Security Role	
74 – P900 Counter		130 – Entity Category	
75 – P900 Trigger Event		131 – Team	
76 – P900 Trigger Link		132 – Division	
77 – P900 System Parameters		133 – Database Version	
78 – Auto-badge Number		134 – User Role	
79 – Common PIN		135 – Intrusion Group	
80 – P900 Sequence File		136 – SCT File Object	
81 – Remote Server		137 – SCT Notification Object	
82 – Message Filter		138 – SCT Calendar Object	
83 – Message Filter Group		139 – SCT CK722 Device Object	
84 – Local Site		140 – SCT Schedule Object	
85 – Service Startup Configuration		141 – SCT Access Control Object	
86 – Application		142 – SCT Door Sequence Object	
87 – Panel Card Format		143 – SCT S300 Trunk Object	
88 – Reason		144 – SCT Anti Passback Object	

Message Sub-Types (Continued)**28675 – Audit (continued)**

- 145 – SCT Protocol Engine Object
- 146 – SCT S300 Reader Object
- 147 – SCT Binary Output Object
- 148 – SCT S300 Module Object
- 149 – SCT Anti-Loitering Object
- 150 – SCT Data Record Object
- 151 – SCT Ethernet Link Object
- 152 – SCT Occupancy Object
- 153 – SCT Interlock Object
- 154 – Intrusion Annunciator
- 155 – Intrusion Area
- 156 – SCT Intrusion Keypad Display Object
- 157 – Intrusion Zone
- 158 – SCT Multi Command Object
- 159 – SCT Name List Object
- 160 – SCT Supervised Input Object
- 161 – SCT Controller Event Object
- 162 – Request Configuration
- 163 – Web UI Style
- 164 – PIN Code
- 165 – Intrusion Device
- 166 – Intrusion Server
- 167 – Elevator Integration
- 168 – Elevator Controller
- 169 – Work Schedule Object
- 170 – Time & Attendance Reader
- 171 – Work Schedule
- 172 – T&A Integration
- 173 – MSEA ADX Map
- 174 – MSEA Partition Map
- 175 – Mifare Encode
- 176 – Web Access Config
- 177 – Integration Server
- 178 – Voorspoed Stop Search
- 179 – Integration Station
- 180 – XMan XRAY Machine
- 181 – Integration Device
- 182 – XMan Holding Room
- 183 – ACS APM
- 184 – ACS Lane Equipment Cabinet Door
- 185 – ACS Interface Integration
- 186 – MSEA Item Category

Appendix C: Panel Comparison Matrix

Feature	Panel Type							
	CK720 (2.3)	CK705 (2.3)	CK720 (2.6)	CK705 (2.6)	CK721 (2.8)	CK721-A (2.10)	CK722 (2.0)	
Output Status	✓	✓	✓	✓	✓	✓	✓	✓
Strike Status	✓	✓	✓	✓	✓	✓	✓	✓
History Upload With Seconds	✓	✓	✓	✓	✓	✓	✓	✓
4-State Alarms	✓	✓	✓	✓	✓	✓	✓	✓
Custom Card Formats	✓	✓	✓	✓	✓	✓	✓	✓
Access Groups Per Badge	8	8	8	8	8	8	100	2
Timezones per badge	8	8	8	8	8	8	100	2
Timezones Per Panel	64	64	64	64	64	64	64	64
Maximum Inputs	256	64	256	64	256	256	256	6
Maximum Outputs	128	32	128	32	128	128	256	10
Elevator Support	✓	✓	✓	✓	✓	✓	✓	-
Invalid Privilege Level Message	✓	✓	✓	✓	✓	✓	✓	✓
Multiple Facility Codes per Badge Type	✓	✓	✓	✓	✓	✓	✓	✓
Custom PIN Code	✓	✓	✓	✓	✓	✓	✓	✓
Reverse Card Reading	✓	✓	✓	✓	✓	✓	✓	✓
Reverse Swipe Duress	✓	✓	✓	✓	✓	✓	✓	✓
Override Expiration Warning	✓	✓	✓	✓	✓	✓	✓	✓
Door Shunt Expiration Warning	✓	✓	✓	✓	✓	✓	✓	✓
High Speed 485	✓	✓	✓	✓	✓	✓	✓	✓*
Network	✓	✓	✓	✓	✓	✓	✓	✓*
Terminal Readers	16	4	16	4	16	16	64	2
Holidays	40	40	40	40	40	40	40	40
Valid and Unauthorized	✓	✓	✓	✓	✓	✓	✓	✓
Alarm Debounce	✓	✓	✓	✓	✓	✓	✓	✓
Multi Card Types	✓	✓	✓	✓	✓	✓	✓	✓
Door Open Warning	✓	✓	✓	✓	✓	✓	✓	✓
Access Grant on Door Open	✓	✓	✓	✓	✓	✓	✓	✓

Feature	Panel Type							S321
	CK720 (2.3)	CK705 (2.3)	CK720 (2.6)	CK705 (2.6)	CK721 (2.8)	CK721-A (2.10)	CK722 (2.0)	
Panel Relays	2	2	2	2	1	1	1	0
Local Mode (Card Processing)	✓	✓	✓	✓	✓	✓	✓	✓
Shared Mode (Card Processing)	✓	✓	✓	✓	✓	✓	✓	✓
Central Mode (Card Processing)	✓	✓	✓	✓	✓	✓	✓	✓
Number of Facility Codes	12	12	12	12	12	12	100**	4
Executive Privilege	✓	✓	✓	✓	✓	✓	✓	✓
Security Level	✓	✓	✓	✓	✓	✓	✓	✓
Americans with Disabilities Act (ADA)	✓	✓	✓	✓	✓	✓	✓	✓
Calibration/Uncalibration	✓	✓	✓	✓	✓	✓	✓	✓
Extended Time Override	✓	✓	✓	✓	✓	✓	✓	✓
Extended Shunt Time	✓	✓	✓	✓	✓	✓	✓	✓
Common PIN	✓	✓	✓	✓	✓	✓	✓	-
PIN + 1 Duress	✓	✓	✓	✓	✓	✓	✓	✓
Keyless Override Feature	✓	✓	✓	✓	✓	✓	***	✓
Star Feature	✓	✓	✓	✓	✓	✓	Only	✓
HID Corp. 1000 Card Format	✓	✓	✓	✓	✓	✓	✓	✓
High Level Elevator	✓	✓	✓	✓	✓	✓	✓	-
D620-ECG Elevator Mode	-	-	✓	✓	✓	✓	✓	-
KONE HLI Elevator Support	✓	✓	✓	✓	-	✓	-	-
KONE IP HLI Elevator Support	-	-	-	-	-	-	✓	-
Otis HLI Elevator Support	-	-	-	-	-	✓	✓	-
Special Flags	3	3	3	3	3	3	100	3
Dial-Up Support	✓	✓	✓	✓	✓*****	-	-	-
Override Reset Threat Level	-	-	✓	✓	✓	✓	✓	✓
Dual Ethernet Support	-	-	✓	✓	-	-	-	-
BQT Reader Support	-	-	✓	✓	✓	✓	-	-
Auto Save /ramdisk DB to Flash Memory	-	-	✓	✓	-	✓	✓	✓
Exempt from Archive to Flash	-	-	✓	✓	✓	✓	-****	-
Global Entry/Exit at the Panel (via UDP Broadcast)	-	-	-	-	-	✓*****	-	-
Access Masks	-	-	-	-	-	-	✓	-
Access Levels	-	-	-	-	-	-	✓	-
Security Masks	-	-	-	-	-	-	✓	-
Asset Processing	-	-	-	-	-	-	✓	-
Entity Processing	-	-	-	-	-	-	✓	-
Group Processing	-	-	-	-	-	-	✓	-

Feature	Panel Type							S321
	CK720 (2.3)	CK705 (2.3)	CK720 (2.6)	CK705 (2.6)	CK721 (2.8)	CK721-A (2.10)	CK722 (2.0)	
Team Processing (N-Man Rule)	-	-	-	-	-	-	✓	-
Anti-Passback Areas	1	1	1	1	1	1	45	1
Occupancy Spaces	0	0	0	0	0	0	100	0
PIN Attempt Sectors	1	1	1	1	1	1	10	1
Anti-Loitering Areas	0	0	0	0	0	0	100	0
Peer to Peer Anti-Passback	-	-	-	-	-	-	✓	-
Panel Card Events	20	20	20	20	20	20	100	20
Lockdown Mode	-	-	-	-	-	-	✓	-
Individual Door Contact and REX Debounce Times	-	-	-	-	-	-	✓	-
Intrusion	-	-	-	-	-	-	✓	-

- * S321 panels can communicate with the P2000AE Server through network connection using a Digi One SP converter box.
- ** Per door, 6400 total.
- *** Achieved by controller event.
- **** Not required.
- ***** Available for CK721M.
- ***** Configured at the Panel, not the Host.

Appendix D: CCTV Switch Protocols

This appendix describes the CCTV Switch Protocols that are supported by the CCTV option. The protocols supported will vary according to the current manufacturers' products. Those listed here will be for a specific version of the driver for the item.

For each of the supported Switches, this appendix gives information about the controls that are available in CCTV Control and the actions that are available when defining CCTV event actions and OPCWrite actions.

You can define CCTV event actions using the standard P2000 event action functions. For details, refer to "Creating Actions" on page 208. However you may also wish to use the standard P2000 OPCWrite function if what you want to do is not available with the CCTV event actions or you have not fully configured the CCTV equipment from the CCTV/AV Configuration window.

Note that when OPCWrite is used, any changes to the namespace may not be automatically reflected.

The actions that are available in the OPC Server namespace are listed in *Appendix E: CCTV Server Namespace Definitions*. The Switch Protocols that are supported by the CCTV option use a subset of the namespace tags.

The CCTV option does not include support for multiplexers, VCRs and video on screen.

Communications

The communication settings for each Switch is determined by the manufacturer. The user should ensure that the protocol and COM port settings at the Switch matches that configured in the Edit CCTV Switch dialog box. You should refer to the manufacturer's specification for details of what the settings should be.

In addition, the Timeout setting in the Communications tab of the Edit CCTV Switch dialog box will only be applied by the CCTV driver if the matrix transmits results, or the configured timeout is longer than the hard-coded timeout.

Camera Movement Actions

Most protocols specify that Camera movements are sent once to initiate the movement in a given direction. Once movement has started a separate stop action must be sent to stop the movement. Some protocols include a timeout function, so that Camera movement stops automatically after a specified time. You should refer to the manufacturer's specification for details.

For diagonal movement both the pan and tilt commands are sent.

A Monitor Selection action is sent prior to each action. This means that simultaneously several operators at different workstations can independently move the individual cameras they each have selected.

Monitor Sequences

Monitor Sequences are normally associated with a particular Monitor. However some CCTV manufacturers use Monitor Sequences that are independent of the Monitor. This means that the same sequence is used by all monitors. Therefore, sequence 1 would be the same sequence when used by any Monitor on the system.

General ASCII Protocol

The General ASCII protocol uses the CCTV Server as a general OPC Server that can send ASCII control strings to devices in order to control them. Typically, the devices will exist in the building management and process control industry as well as the access control industry.

This protocol uses the GeneralString Tag in the Switch to send a string of ASCII characters out of the COM port. Once the string has been sent the data is cleared. Any ASCII string can be sent. A sequence of strings could be sent for more complex applications. The assumption is that there is no protocol control required and that no responses are processed.

The standard control/client will not have a Switch - General String field. It is envisaged that this feature will be driven by the event action processing in the P2000 software or by a specially written OPC Client interface.

Commands Supported

The General ASCII Switch protocol supports up to 50 characters (from the General String field) to be stored and sent. Both printable and non-printable ASCII characters are supported, however, nulls are not supported.

Note that if the Switch Protocol selected in the Edit CCTV Switch window is General ASCII then a record is not saved in the configuration database. Since the data for reports is that in the database, it is not possible to run reports for General ASCII Switches.

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVGeneralASCII.

American Dynamics

This section describes the American Dynamics Switch protocol for the Switch model AD1024. The American Dynamics protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to an American Dynamics AD1024 Switch.

The CCTV option should work with other American Dynamics Switches provided that they comply with the communications protocol specified in the American Dynamics manual AN001 for general commands and AN005 for the date/time command only. The only issue that may arise when operating with Switches other than the AD1024 is that they may support numbers of Cameras and Monitors in excess of the maximum values set for the AD1024.

All basic camera/monitor selection and camera movement commands including latched auxiliaries are supported.

The American Dynamics features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control (fixed speed only)
- Camera Auxiliary On and Off for latched auxiliaries only
- Camera Call and Set Shot (preset)
- New Alarm, Clear Alarm and Acknowledge Alarm. The Clear and Acknowledge Alarm are sent simultaneously in response to a P2000 Alarm Stop event action.

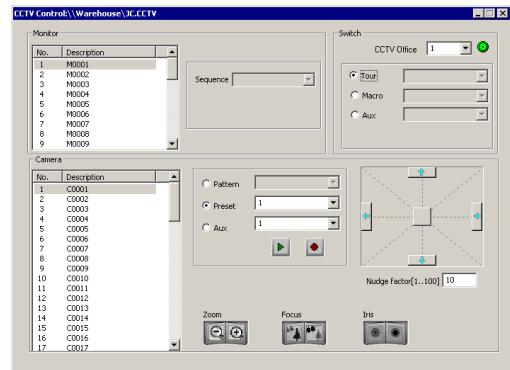
The American Dynamics Protocol

The protocol is assumed to be in one direction only, that is the CCTV Server sends commands to the Switch and does not expect any replies. The CCTV Server ignores any responses that may be received.

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVAmerican-Dynamics.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for an American Dynamics AD1024 Switch.



Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for American Dynamics 1024 Switch are:

Supported Actions
Switch Alarm Play
Switch Alarm Stop
Monitor Camera
Camera Preset
Camera Auxiliary Play
Camera Auxiliary Stop

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for an American Dynamics 1024 Switch:

Supported Tags
S%.AlarmPlay
S%.AlarmStop
S%.DateTime
M#.Camera
C#.PresetRecord
C#.PresetPlay
C#.AuxiliaryPlay
C#.AuxiliaryStop
C#.Tilt
C#.Pan
C#.Zoom
C#.Focus
C#.Iris

Autorepeat Actions

The following actions are repeated until specifically reset to zero:

C#.Tilt
C#.Pan
C#.Zoom
C#.Focus
C#.Iris

For these commands, the Client would need to issue a stop command otherwise the command will repeat indefinitely.

See also Note 1 in *Appendix E: CCTV Server Namespace Definitions*.

Automatic Status Update Tags

American Dynamics does not support periodic status updates. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The table below lists those applicable to American Dynamics.

The maximum values define the number of items that are allowed in the protocol. The values below were derived from the American Dynamics manual *AD1024 CPU System Programming and Operating Instructions*.

The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

	Maximum Value	Default Value
SwitchAlarmMax	8192	64
SwitchMonitorMax	128	32
SwitchCameraMax	1024	64
CameraAuxiliaryMax	32 (per camera)	8 (per camera)
CameraPresetMax	72 (per camera)	8 (per camera)

BetaTech

This section describes the BetaTech Switch protocol. The BetaTech protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to the Ademco VideoBlox Switch.

The CCTV Option should work with any of the Surveillance Mate Master Series (Revision III) at firmware version 4.69g.

All basic camera/monitor selection and camera movement commands are supported.

The BetaTech features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control
- Camera Auxiliaries
- Record and Play Camera Presets
- Play/Stop a Sequence on a Monitor
- System/Switch auxiliaries
- System date and time

Note that a BetaTech Sequence is a Monitor independent Sequence and in addition can be set up to behave as if it is running Macros, Tours or Sequences.

The following command in the BetaTech protocol that is not supported:

- Status enquiries

In addition, note that the BetaTech protocol does not allow alarms.

Switch Configuration

Keyboard 16 Commands

It is possible to disable functions when the Switch is set up. The serial port is associated

with keyboard 16 and any functions that are blocked for keyboard 16 are automatically disabled for the serial port. This means that some functions, for example Presets, Sequences, etc., may be disabled.

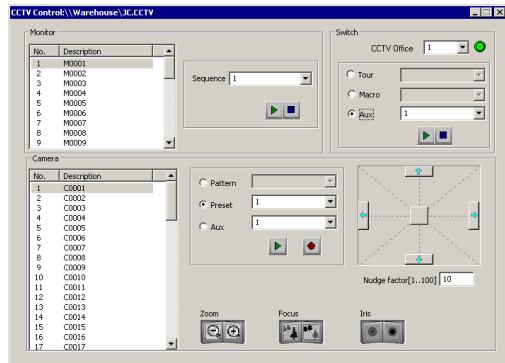
The BetaTech Protocol

Baudrate	9600
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	Hardware

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVBetaTech.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for a supported BetaTech Switch.



Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for BetaTech are:

Supported Actions
Switch Auxiliary Play
Switch Auxiliary Stop
Monitor Sequence Play
Monitor Sequence Stop
Monitor Camera
Camera Preset
Camera Auxiliary Play
Camera Auxiliary Stop

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for a BetaTech Switch:

Supported Tags
S%.AuxiliaryPlay
S%.AuxiliaryStop
S%.DateTime
M#.SequencePlay
M#.SequenceStop
M#.Camera
M#.GeneralString
C#.PresetRecord
C#.PresetPlay
C#.AuxiliaryPlay
C#.AuxiliaryStop
C#.Tilt
C#.Pan
C#.Zoom
C#.Focus
C#.Iris

Autorepeat Actions

Autorepeat functions are not required.

Automatic Status Update Tags

Status enquiries are not supported. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The following table lists those applicable to BetaTech.

The maximum values define the number of items that are allowed in the protocol. The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

	Maximum Value	Default Value
SwitchMonitorMax	256	32
SwitchCameraMax	4096	64
SwitchAuxiliaryMax	256	64
MonitorSequenceMax	1024	8
CameraAuxiliaryMax	64	8 (per camera)
CameraPresetMax	128	8 (per camera)

Geutebrück - GST Interface

This section describes the Geutebrück GST Interface Switch protocol. The Geutebrück protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to one of the following Geutebrück Switches:

- CPX 24/8
- CPX 48/8
- VX 3 (Vicros III)
- KS 48 (Vicros II)
- KS 40

The CCTV Option should work with other Geutebrück Switches provided that they adhere to the communications protocol specified by the GST interface if the MicroLink controller with VicroSoft version 5.27 or higher. Note that currently the MultiScope hardware and GeVi software interface is not supported.

All basic camera/monitor selection and camera movement commands are supported.

The Geutebrück GST interface features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control
- Camera Wiper, Washer and Light
- Camera Auxiliaries On and Off
- Camera Call and Set Pre-Position (preset)
- Activate an Alarm
- Play and Stop a Sequence
- Set Date and Time
- Camera Home
- Autopanning

Note that the Camera Home function is played using Pattern 1 and Autopanning is played using Pattern 2, however, the protocol cannot be used to define the Camera Home position or Autopanning.

The following commands in the Geutebrück GST protocol are not supported. These are:

- Activate/deactivate Input Activities (Macros); although a Macro can be triggered provided it has been deactivated
- Switching cameras On and Off
- User program restarts or changes
- Programming sequences
- Monitor Status enquiries
- Date and Time enquires
- Remote controllable camera
- Sequence Dwell time
- Acknowledge/reset alarms
- Toggle switch auxiliaries

The Geutebrück Protocol

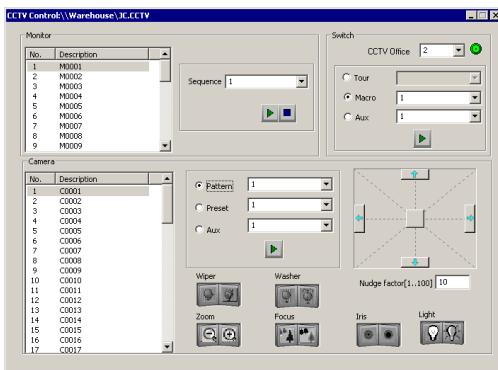
The default communications parameters for the GST interface are:

Baudrate	1200
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	Hardware

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVGeutebrueck.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for a Geutebrück Switch.



Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for a Geutebrück switch are:

Supported Actions
Switch Macro Play
Switch Alarm Play
Switch Auxiliary Play
Switch Auxiliary Stop
Monitor Sequence Play
Monitor Sequence Stop
Monitor Camera
Camera Pattern Play
Camera Preset
Camera Auxiliary Play
Camera Auxiliary Stop

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for a supported Geutebrück Switch:

Supported Tags

S%.MacroPlay
S%.MacroStop
S%.AlarmPlay
S%.AuxiliaryPlay
S%.AuxiliaryStop

S%.DateTime

M#.SequencePlay
M#.SequenceStop

M#.Camera

C#.PatternPlay

C#.PresetRecord
C#.PresetPlay

C#.AuxiliaryPlay
C#.AuxiliaryStop

C#.Tilt

C#.Pan

C#.Zoom
C#.Focus
C#.Iris
C#.Wiper
C#.Washer
C#.Light

Macros

Macros are the same as Input Activities (AK). Macros can be deactivated but once deactivated the macro cannot be started using the CCTV driver.

Camera Auxiliaries

Camera Auxiliaries 1 to 4 are used to implement the following functions:

Camera Auxiliary	Function
1	X
2	Y
3	U
4	V

The maximum values define the number of items that are allowed in the protocol. The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

Monitor Sequences

Geutebrück GST Sequences are Monitor independent. The Monitor can only play sequences that are higher than or equal to the Monitor number.

Sequences contain no positional commands for a camera (including Presets).

Note that the dwell time is associated only with the monitor on which the sequence was set up. It does not apply when running a Sequence on a different monitor.

Autorepeat Actions

The Geutebrück protocol does not require autorepeat functions.

Automatic Status Update Tags

The Geutebrück driver does not support status updates. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The following table lists those applicable to the supported Geutebrück Switch.

	Maximum Value	Default Value
SwitchMacroMax	9999	8
SwitchAlarmMax	9999	64
SwitchAuxiliaryMax	384	8
SwitchMonitorMax	99	32
SwitchCameraMax	255	64
MonitorSequenceMax	99	8
CameraAuxiliaryMax	2 (per camera)	2 (per camera)
CameraPatternMax	2 (per camera)	2 (per camera)
CameraPresetMax	200 (per camera)	8 (per camera)

Panasonic

This section describes the Panasonic Switch protocol. The Panasonic SX850 protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to the SX850 Panasonic Switch.

The CCTV Option should work with other Panasonic Switches provided that they adhere to the same communications protocol as described in the manual *SX850 Protocol Information RS-232 Version 1.4 01.24/00*. However, other Panasonic Switches may support more cameras and monitors than the maximum allowed for the SX850 Switch.

All basic camera/monitor selection and camera movement commands are supported.

The Panasonic SX850 features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control (fixed speed only)
- Camera Preset
- Alarm Point Set and Reset sent in response to P2000 event actions
- Run Stop Pause Resume Step Forward Step Backward Monitor Tour Sequences

A few of the commands in the Panasonic SX850 protocol are not supported. These are:

- Status Inquiry Commands
- Priority Lock On/Off
- Pan/Tilt Fast/Slow
- Alarm Processing (except Alarm Point Set/Rest)
- Reverse Sequence

Panasonic equipment does not support simultaneous movement of more than one camera connected to a Switch.

However, if up to 3 Switches are configured in the CCTV/AV Configuration window, then up to 3 Cameras (one per Switch) could be controlled simultaneously by using up to 3 separate COM lines between the PC and the Switch.

Note that Panasonic supports one client only. You should be aware that if you attempt to use more than one client the commands may have unexpected results.

Switch Configuration

Auto Log-Off must be disabled. Please refer to your Panasonic manual for details.

Panasonic SX850 Protocol

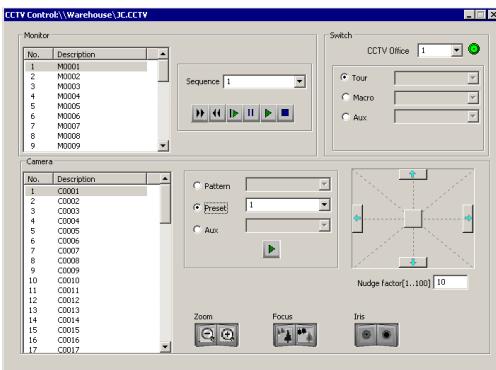
The communications parameters are:

Baudrate	9600
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	None

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVPanasonic.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for a supported Panasonic Switch.



Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for a supported Panasonic Switch are:

Supported Actions

- Switch Alarm Play
- Switch Alarm Stop
- Monitor Sequence Play
- Monitor Sequence Stop
- Monitor Camera
- Camera Preset

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for a Panasonic SX850 Switch:

Supported Tags

- | | |
|------------------------|-------------------------|
| S%.AlarmPlay | S%.AlarmStop |
| M#.SequencePlay | M#.SequenceStop |
| M#.SequencePause | M#.SequenceRestart |
| M#.SequenceStepForward | M#.SequenceStepBackward |
|
 | |
| M#.Camera | |
| C#.PresetPlay | |
| C#.Tilt | C#.Pan |
| C#.Zoom | |
| C#.Focus | |
| C#.Iris | |

Camera Movement Commands

Panasonic does not support movement of more than one camera (at one Switch) at a time. This means that if a camera movement is being performed and a second camera is selected, the first camera will stop.

Autorepeat Actions

The Panasonic SX850 protocol does not support the autorepeat functions.

Automatic Status Update Tags

Panasonic does not support periodic status updates. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The following table lists those applicable to Panasonic SX850.

The maximum values define the number of items that are allowed in the protocol. The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

	Maximum Value	Default Value
SwitchAlarmMax	128	64
SwitchMonitorMax	65534	32
SwitchCameraMax	99999	64
MonitorSequenceMax	65534	8

Pelco

This section describes the Pelco Switch protocol. The Pelco 9760 protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to one of the following Pelco Switches:

- Pelco 9760
- CM 6700
- CM 6800

The CCTV Option should work with other Pelco Switches provided that they adhere to the communications protocol specified in Chapter 4 of the Pelco document *C542M-B* (8/00). In some of the newer Pelco Switches the functionality of the data translator is built into the Switch; for these a data translator may not be required.

A Pelco 9760 Switch assumes a Pelco CM9760-DT or CM9760-DT4 data translator is connected in the RS232 line between the PC running the CCTV Server and the CC1 CPU of the CM9760 Switch. The CM 6700 and CM 6800 do not require a data translator.

All basic camera/monitor selection and camera movement commands are supported.

The Pelco 9760 features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control (fixed speed only)
- Switch Camera Auxiliaries and System Auxiliaries On and Off
- Set and Go to Camera Presets
- Record and Play Camera Patterns
- Trigger and Clear/Reset Alarms
- Play and Stop Macros. Play and Stop Tours and Monitor Sequences also appear in the

window and have the same effect as Play and Stop Macros.

A few of the commands in the Pelco 9760 protocol are not supported. These are:

- Set Preset with a Label
- Query Device
- Video Loss Detect
- Report Revision
- Select Next/Previous Camera

The Pelco 9760 Protocol

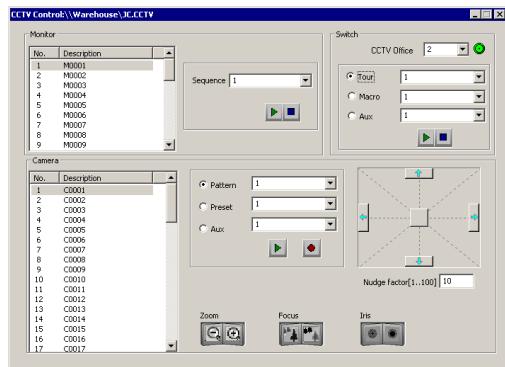
The protocol used is bidirectional. If the matrix recognizes a command an acknowledgement is sent back to the CCTV Server. If a command is not recognized, a negative acknowledge is returned.

The predefined timeout for the Pelco Switch is 500 ms.

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVPelco9760.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for a Pelco 9760 Switch.



Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for a Pelco 9760 are:

Supported Actions
Switch Tour Play
Switch Tour Stop
Switch Macro Play
Switch Macro Stop
Switch Alarm Play
Switch Alarm Stop
Switch Auxiliary Play
Switch Auxiliary Stop
Monitor Sequence Play
Monitor Sequence Stop
Monitor Camera
Camera Pattern Play
Camera Preset
Camera Auxiliary Play
Camera Auxiliary Stop

Supported Tags
S%.TourPlay
S%.TourStop
S%.MacroPlay
S%.MacroStop
S%.AlarmPlay
S%.AlarmStop
S%.AuxiliaryPlay
S%.AuxiliaryStop
S%.DateTime
M#.SequencePlay
M#.SequenceStop
M#.Camera
C#.PatternPlay
C#.PatternRecord
C#.PresetRecord
C#.PresetPlay
C#.AuxiliaryPlay
C#.AuxiliaryStop
C#.Tilt
C#.Pan
C#.Zoom
C#.Focus
C#.Iris

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for a Pelco 9760 Switch:

Autorepeat Actions

The Pelco 9760 protocol does not support the autorepeat function for the following commands:

C#.Tilt
C#.Pan
C#.Zoom
C#.Focus
C#.Iris

See also Note 1 in *Appendix E: CCTV Server Namespace Definitions*.

Automatic Status Update Tags

Pelco 9760 does not support periodic status updates. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Macro Programming

Macros are programmed into the system using the 9760-MGR software shipped with each Switch. They cannot be programmed from the CCTV Client at a P2000 workstation.

Tour and Monitor Sequence commands from a P2000 workstation are executed as play or stop Macro commands with the same number. Tours and Sequences do not exist as separately programmable functions - there are only Macros.

	Maximum Value	Default Value
SwitchAlarmMax	9999	64
SwitchMonitorMax	9999	32
SwitchCameraMax	9999	64
SwitchAuxiliaryMax	20000	64
SwitchMacroMax	999	8
SwitchTourMax	99	8
MonitorSequenceMax	99 (per monitor)	8 (per monitor)
CameraAuxiliaryMax	8 (per camera)	8 (per camera)
CameraPatternMax	99 (per camera)	2 (per camera)
CameraPresetMax	9999 (per camera)	8 (per camera)

Recording Patterns

If you are recording Patterns, you should ensure that no other OPC Client is using the Switch.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The following table lists those applicable to Pelco 9760.

The maximum values define the number of items that are allowed in the protocol. The values below were derived from Section 4 of the Pelco manual *C54M-B (8/00)*

CM9760-DT/DT4 Data Translator Installation/Operation.

The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

Philips Burle (Bosch)

This section describes the Philips Burle Switch protocol. The Philips Burle protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to one of the following Philips Burle Switches:

- LTC 8100 Series
- LTC 8200 Series
- LTC 8300 Series
- LTC 8500 Series
- LTC 8600 Series
- LTC 8800 Series
- LTC 8900 Series

Each Switch requires CPU Revision Level 8.1.

All basic camera/monitor selection and camera movement commands are supported. Commands relating to logical camera/monitor numbers are supported.

The LTC 8x00 Series switch features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control (fixed speed only)
- Switch Camera Auxiliary On and Off
- Camera Call and set Pre-position (Preset)
- Activate and Deactivate an Alarm
- Run or Hold a Sequence
- Step Forward and Step Backward in a Sequence
- Set Time and Set Date
- Run system macros

The following commands in the protocol are not supported. These are:

- “Lockouts”
- Commands using a keyboard number
- Latch Auxiliary On, Latch Auxiliary Off and Cancel Auxiliary Latch commands
- Auxiliary Toggle
- System Status Commands
- Video Detection Commands
- Allegiant Coaxial Transmission System (ACTS) Commands
- On Screen Display Commands (except Send Monitor/Camera Title)
- System Commands (except Set Date & Set Time)
- Allegiant Diagnostic Commands

Switch Macros

Philips Switches support system macros that are input using the Philips Master Control Software. These macros can be run (but not stopped) from the CCTV Server as long as they follow the correct naming convention.

The macro name must be in the form:

MACRO_nnnnnn

For example, Macro 1 would start with the statement:

Begin MACRO_000001

The Philips Burle Protocol

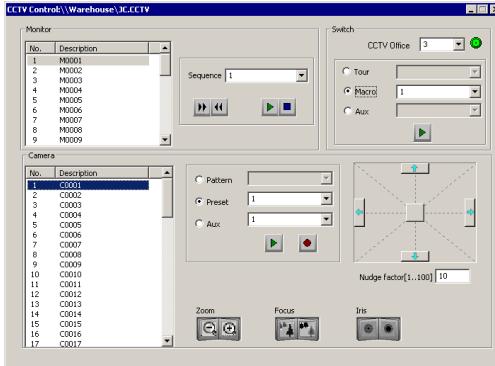
The communications parameters are:

Baudrate	19200
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	Hardware, but can be disabled by connecting pins 4 and 5 at the Switch's COM port

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVPhilips.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for supported Philips Burle Switches.



Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for a supported Philips Burle switch:

Supported Actions

- Switch Alarm Play
- Switch Alarm Stop
- Switch Macro Play
- Monitor Sequence Play
- Monitor Sequence Stop
- Monitor Camera
- Camera Preset
- Camera Auxiliary Play
- Camera Auxiliary Stop

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for a supported Philips Burle Switch:

Supported Tags

- | |
|-------------------------|
| S%.AlarmPlay |
| S%.AlarmStop |
| S%.MacroPlay |
| S%.DateTime |
| M#.SequencePlay |
| M#.SequenceStop |
| M#.SequenceStepForward |
| M#.SequenceStepBackward |
| M#.Camera |
| C#.PresetRecord |
| C#.PresetPlay |
| C#.AuxiliaryPlay |
| C#.AuxiliaryStop |
| C#.Tilt |
| C#.Pan |
| C#.Zoom |
| C#.Focus |
| C#.Iris |

Autorepeat Actions

The Philips Burle Switch protocol does not require the autorepeat function.

Automatic Status Update Tags

The Philips Burle Switches do not support periodic status updates. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The following table lists those applicable to a Philips Burle Switch.

The maximum values define the number of items that are allowed in the protocol. The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

	Maximum Value	Default Value
SwitchAlarmMax	9999	64
SwitchMacroMax	10000	8
SwitchMonitorMax	9999	32
SwitchCameraMax	9999	64
MonitorSequenceMax	9999	8 (per monitor)
CameraAuxiliaryMax	9999 (per camera)	8 (per camera)
CameraPresetMax	9999 (per camera)	8 (per camera)

Note: This protocol applies to a number of Switches that have differing maximum values. The maximum value allowed by the software is the biggest maximum for the supported Philips Burle Switches. System operators should reset these maximum values from the CCTV/AV Configuration window for smaller configurations.

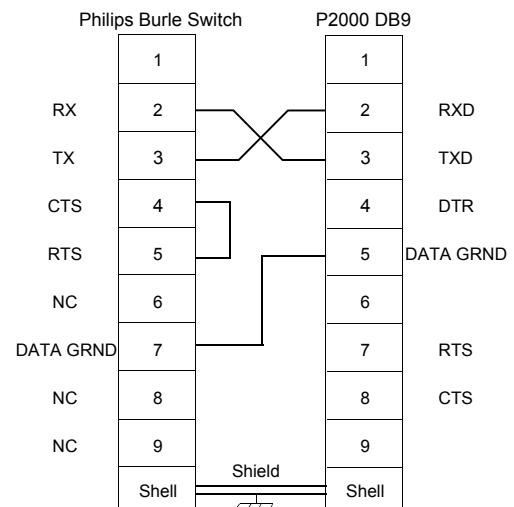
Cabling Configuration

The communication between the Philips Burle Switch and the P2000 Server computer is established via an RS232 cable.

To allow the communication, the Philips Burle Switch requires PIN 4 (CTS) to be held high. To accomplish this, PIN 4 (CTS) must be jumped to PIN 5 (RTS) at the Philips Burle Switch.

The following procedure presents the recommended cable configuration.

1. Attach one end of the RS232 cable to the serial port (example: COM1) of the P2000 Server.
2. Attach the other end of the RS232 cable to the TCX01 main CPU bay connector marked **CONSOLE**.
3. Place a jumper across PINs 4 and 5 of the CONSOLE port.



Ultrak

This section describes the Ultrak Switch protocol. The Ultrak MaxPro-1000 protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to the MaxPro-1000 Ultrak Switch:

All basic camera/monitor selection and camera movement commands are supported.

The Ultrak MaxPro-1000 features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control (fixed speed only)
- Camera Call and Set Views (Presets)
- Camera Washer and Wiper
- Trigger and Clear Alarms

A few of the commands in the Ultrak Max-Pro-1000 protocol are not supported. These are:

- Selecting alternate camera(s)
- Video Recorder features
- Selecting Next/Previous source for video signals
- Std / Smart device operations
- Recording /changing Scans (Sequences)
- User and system macros are not supported (but they can be triggered indirectly via alarms).

Switch Configuration

Keyboard 64 Commands

The CCTV driver transmits all its commands as if from Keyboard 64 so Keyboard 64 needs to be configured in the Ultrak Switch. Nor-

mally each keyboard is associated with an operator. The CCTV access rights for this operator need to be configured correctly (ideally access to all equipment) and this operator should have the highest priority otherwise commands issued from the CCTV driver may be rejected.

The Ultrak MaxPro-1000 Protocol

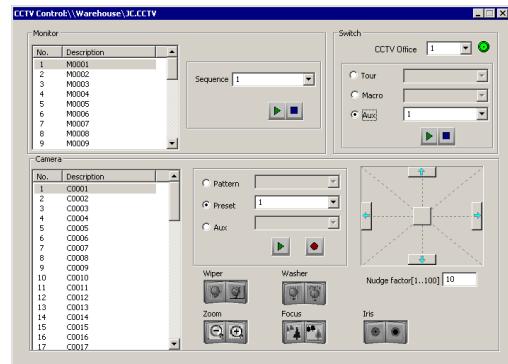
The communications parameters are:

Baudrate	19200 or 9600
Data bits	7
Stop bits	1
Parity	Even
Timeout (ms)	500

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVUltrak.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for a Ultrak Switch.



Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for an Ultrak Switch are:

Supported Actions
Switch Alarm Play
Switch Alarm Stop
Switch Auxiliary Play
Switch Auxiliary Stop
Monitor Sequence Play
Monitor Sequence Stop
Monitor Camera
Camera Preset

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for a supported Ultrak Switch:

Supported Tags
S%.AlarmPlay
S%.AlarmStop
S%.DateTime
M#.SequencePlay
M#.SequenceStop
M#.Camera
C#.PresetRecord
C#.PresetPlay
C#.Tilt
C#.Pan
C#.Zoom
C#.Focus
C#.Iris
C#.Wiper
C#.Washer

Auxiliaries

Ultrak Switch and Camera Auxiliaries are mapped to System Auxiliaries. The System Auxiliaries are numbered and can be activated and deactivated using the CCTV driver.

Monitor Sequences

An Ultrak scan is a sequence of CCTV commands defined at the Switch and activated for a particular monitor. Therefore, Sequence 1 for example is the same set of commands for all monitors.

Autorepeat Actions

The Ultrak protocol does not require the autorepeat functions.

See also Note 1 in *Appendix E: CCTV Server Namespace Definitions*.

Automatic Status Update Tags

The Ultrak protocol does not support periodic status updates. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The following table lists those applicable to Ultrak MaxPro-100.

The maximum values define the number of items that are allowed in the protocol.

The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

	Maximum Value	Default Value
SwitchAlarmMax	8192	64
SwitchMonitorMax	2048	32
SwitchCameraMax	9999	64
MonitorSequenceMax	1999 (per monitor)	8 (per monitor)
CameraPresetMax	99 (per camera)	8 (per camera)

Vicon

This section describes the Vicon Switch protocol. The Vicon protocol enables an operator at a suitably configured P2000 workstation to control CCTV equipment connected to one of the following Vicon Switches:

- VPS1300
- VPS1344
- V1422
- VPS1466

The CCTV Option should work with other Vicon Switches provided that they adhere to the same communications protocol. The only disparity with Switches other than the supported Vicon Switches is that they may support a number of cameras or monitors greater than the maximum permitted.

All basic camera/monitor selection and camera movement commands are supported.

The Vicon features supported are:

- Monitor and Camera Selection
- Camera Pan and Tilt with variable speed
- Camera Zoom, Focus and Iris control (up to three speeds dependent on the lens control setting)
- Camera Lens Speed control using Auxiliary 7
- Camera Auto Iris On and Off
- Camera Auxiliaries On and Off
- Camera Preset Recall and Preset Store
- Alarm Point Set and Reset sent in response to P2000 event actions

Note: *Alarm resets can be sent to the switch at a maximum rate of 10 per second.*

- Run Tour (No Stop Tour in protocol). Also indirectly supports Salvos via Salvo Tours.

A few of the commands in the Vicon protocol are not supported. These are:

- Sequence programming commands
- Status reports (with the exception of Receiver Status used for Auto Iris ON/OFF)
- System Data Upload/Download
- Keypad commands
- Alarm processing commands (except Alarm Point Set/Reset)

Switch Configuration

The Tour dialup numbers must be set at 800 plus the number. For example Tour 1 will have the Tour number 801. Please refer to the appropriate Switch programming manual for details.

The Vicon Protocol

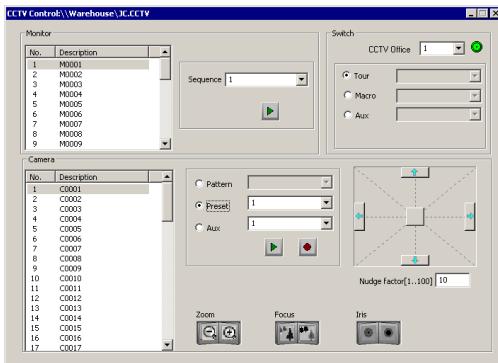
The communications parameters are:

Baudrate	9600
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	Hardware

The protocol name to be entered in the Edit CCTV Switch window is JC.CCTVVicon13xx (sic) for Vicon 1300 and 1344 Switches or JC.CCTVVicon14xx for Vicon 1422 and 1466 Series Switches.

Supported CCTV Controls

The following dialog box displays some of the controls that are available for a Vicon Switch.



Momentary and Latched Auxiliaries

The Vicon protocol supports up to 6 auxiliaries per camera. The auxiliaries can be either momentary or latched. The CCTV Option cannot differentiate between latched and momentary auxiliaries and they require different protocol messages to be sent to the Switch. The following auxiliary numbers have been assigned:

- 1 to 6 for latched auxiliaries
- 8 to 13 for momentary auxiliaries

Camera Lens Speed Control

The Vicon protocol supports up to 3 camera speeds to operate zoom, focus and iris controls. Speed control is activated by playing Auxiliary 7. It operates as a toggle so that each time it is played the lens speed changes.

Supported CCTV Event Actions

The CCTV event actions that are supported by the CCTV Option for a supported Vicon Switch are:

Supported Actions

- | |
|-----------------------|
| Switch Alarm Play |
| Switch Alarm Stop |
| Monitor Sequence Play |
| Monitor Sequence Stop |
| Monitor Camera |
| Camera Preset |
| Camera Auxiliary Play |
| Camera Auxiliary Stop |

Supported OPCWrite Event Actions

A full list of the namespace tags that can be interrogated by an OPC Client is given in *Appendix E: CCTV Server Namespace Definitions*. If you are using OPCWrite to create an event action, the following namespace tags are supported for a supported Vicon Switch:

Supported Tags

- | |
|------------------|
| S%.AlarmPlay |
| S%.AlarmStop |
| S%.DateTime |
| M#.SequencePlay |
| M#.SequenceStop |
| M#.Camera |
| C#.PresetRecord |
| C#.PresetPlay |
| C#.AuxiliaryPlay |
| C#.AuxiliaryStop |
| C#.Tilt |
| C#.Pan |
| C#.Zoom |
| C#.Focus |
| C#.Iris |

Autorepeat Actions

The Vicon protocol does not support the autorepeat functions

Automatic Status Update Tags

The Vicon protocol does not support periodic status updates. These tags are denoted by a U flag in *Appendix E: CCTV Server Namespace Definitions*.

Maximum and Default Values

Some items in the CCTV Server namespace have maximum and default values associated with them. The following table lists those applicable to Vicon.

The maximum values define the number of items that are allowed in the protocol.

The default value is the number of items generated in the namespace if the operator does not explicitly define the number from within the CCTV/AV Configuration window.

	Maximum Value	Default Value
SwitchAlarmMax	9999	64
SwitchMonitorMax	999	32
SwitchCameraMax	9999	64
MonitorSequenceMax	9999 (per monitor)	8 (per monitor)
CameraAuxiliaryMax	13 (per camera)	13 (per camera)
CameraPresetMax	99 (per camera)	8 (per camera)

Appendix E: CCTV Server Namespace Definitions

This appendix describes the CCTV Server namespace tags. You should note that the appendix lists all the possible tags. However, only a subset of namespace tags is available for each supported Switch Protocol. You should refer to *Appendix D: CCTV Switch Protocols* for information regarding the supported set of tags.

Flags

The following flags are used in the namespace tag tables.

Flags	Meaning
C	Configured Value (persistence required)
D	Decrement/Increments towards 0 until value becomes 0
R	Readable
U	The value is periodically scanned from device and value updated to reflect value in device. If the CCTV Switch protocol does not allow the scanning of this information, then the CCTV module updates the value after transmitting the command to the CCTV switch. If updated by the module the OPC status information for the data item should return UNCERTAIN rather than GOOD.
W	Writable
Z	Server immediately resets this value to '0', after it processes the value written to it by a client.

Notes

- If the command auto-repeats and the associated Flags are WZ, then Z is ignored.

- This note refers to all Exists tags except S%.Exists, M%.Exists, and C%.Exists. If a command has an associated Exists tag, then the changes to the value of the command tag are allowed or actioned if the Exists flag shows that the command is supported by the protocol.

During CCTV Server run up all Exists tags are checked against the current CCTV Switch Protocol.

Configured Value	Value in Namespace
0	0
1	0 = if not supported by protocol
	1 = if supported by protocol
2	0 = if not supported
	1 = if supported by switch and/or protocol
Exists tags are checked in the hierarchical order of the equipment, that is, Switch then protocol. Therefore if a switch item is unsupported at switch level then the associated Exists tag is not supported.	

- Except for S%.Description, if the description has been defined in the CCTV/AV Configuration window this tag has the same value. Otherwise it defaults to the namespace name (prefix followed by its number, for example M0002, Pa0005).

Namespace Tags

Switch Namespace Tags

Tag Name	Data Type	Flags	Description
S%.Exists	Integer	CR	Only present if a configuration database exists. The parameter is set in the database to establish that this switch exists. 0 = does not exist 1 = exists
S%.Description	String	CR	Name as defined in CCTV/AV Configuration or S%
S%.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
S%.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)
S%.Type	Integer	CR	1 = SERIAL 2 = TCP/IP (not supported)
S%.Port	String	CR	Name of serial port that this is connected to Needs to contain the text COM Changes are only allowed if the port type is serial. See tag S%.baudrate
S%.Baudrate	Integer	CR	Baud is one of the following values: 115200 57600 38400 19200 14400 9600 4800 2400 1200
S%.DataBits	Integer	CR	Word size is one of the following values: 7 8
S%.Parity	Integer	CR	Parity is one of the following values: 0 = None 1 = ODD 2 = EVEN
S%.StopBits	Integer	CR	Stop Bits are one of the following values: 0 1 2
S%.IPAddress	String	CR	IP address of network connected interfaces; this field might either hold a TCP/IP address or a computer name.
S%.Error	Integer	R	Error indicator used by the CCTV Server to indicate communication problems
S%.CCTVProtocolType	String	CR	Switch Protocol is one of the following: JC.CCTVPelco9760 JC.CCTVAmericanDynamics JC.CCTVGeneralASCII Other protocols may be added to this list.

Tag Name	Data Type	Flags	Description
S%.MonitorCount	Integer	CR	Number of Monitors configured.
S%.MonitorMax	Integer	CR	Number of monitors to be created in the name space for this switch -1 = use protocol default during run up
S%.CameraCount	Integer	CR	Number of cameras configured.
S%.CameraMax	Integer	CR	Number of cameras to be created in the name space for this switch -1 = use protocol default during run up
S%.TourExists	Integer	CR	Identifies whether the switch supports tours See Note 2
S%.TourCount	Integer	CR	Number of tours configured
S%.TourMax	Integer	CR	Number of tours to be created in the name space for this switch -1 = use protocol default during run up
S%.TourPlayExists	Integer	CR	Identifies whether tours can be played See Note 2.
S%.TourPlay	Integer	WZ	Number of the tour to start. System starts to play all recorded actions for this tour 0 = new tour start pending >0 = start of tour # pending
S%.TourRecordExists	Integer	CR	Identifies whether tours can be recorded See Note 2
S%.TourRecord	Integer	WZ	Number of the tour to be recorded. It must be non-negative & within range for protocol. 0 = new tour record pending >0 = record tour # pending
S%.TourStopExists	Integer	CR	Identifies whether tours can be stopped See Note 2
S%.TourStop	Integer	WZ	Number of the tour to be stopped. It must be non-negative & within range for protocol. 0 = new tour stop pending >0 = stop tour # pending
S%.TourPauseExists	Integer	CR	Identifies whether tours can be paused See Note 2.
S%.TourPause	Integer	WZ	A non-zero value pauses the tour It must be non-negative & within range for protocol.
S%.TourCameraSwitchForwardExists	Integer	CR	See Note 2
S%.TourCameraSwitchForward	Integer	WZ	
S%.TourCameraSwitchBackwardExists	Integer	CR	See Note 2
S%.TourCameraSwitchBackward	Integer	WZ	
S%.TourForwardExists	Integer	CR	See Note 2
S%.TourForward	Integer	WZ	

Tag Name	Data Type	Flags	Description
S%.TourBackwardExists	Integer	CR	See Note 2
S%.TourBackward	Integer	WZ	
S%.TourRestartExists	Integer	CR	See Note 2
S%.TourRestart	Integer	WZ	use protocol default during run up 0 = no action >0 = restart tour #
S%.TourStepForwardExists	Integer	CR	See Note 2
S%.TourStepForward	Integer	WZ	
S%.TourStepBackwardExists	Integer	CR	See Note 2
S%.TourStepBackward	Integer	WZ	
S%.MacroExists	Integer	CR	See Note 2
S%.MacroCount	Integer	CR	
S%.MacroMax	Integer	CR	0 = not supported -1 = use protocol default during run up
S%.MacroPlayExists	Integer	CR	See Note 2
S%.MacroPlay	Integer	WZ	
S%.MacroRecordExists	Integer	CR	See Note 2
S%.MacroRecord	Integer	WZ	
S%.MacroRestartExists	Integer	CR	See Note 2
S%.MacroRestart	Integer	WZ	
S%.MacroStopExists	Integer	CR	See Note 2
S%.MacroStop	Integer	WZ	
S%.MacroPauseExists	Integer	CR	See Note 2
S%.MacroPause	Integer	WZ	
S%.AlarmExists	Integer	CR	See Note 2
S%.AlarmCount	Integer	CR	
S%.AlarmMax	Integer	CR	0 = not supported -1 = check with protocol during run up
S%.AlarmPlayExists	Integer	CR	See Note 2
S%.AlarmPlay	Integer	WZ	Sets the alarm 0 = new alarm start pending >0 = start alarm # pending <integer>
S%.AlarmStopExists	Integer	CR	See Note 2
S%.AlarmStop	Integer	WZ	Clears the alarm 0 = new alarm stop pending >0 = stop alarm # pending
S%.AuxiliaryExists	Integer	CR	See Note 2
S%.AuxiliaryCount	Integer	CR	
S%.AuxiliaryMax	Integer	CR	0 = not supported -1 = use protocol default during run up

Tag Name	Data Type	Flags	Description
S%.AuxiliaryPlayExists	Integer	CR	See Note 2
S%.AuxiliaryPlay	Integer	WZ	Sets the auxiliary 0 = new auxiliary start pending >0 = start auxiliary # pending
S%.AuxiliaryStopExists	Integer	CR	See Note 2
S%.AuxiliaryStop	Integer	WZ	Clears the auxiliary 0 = new auxiliary stop pending >0 = stop auxiliary # pending <integer>
S%.DateTime	Integer	WZ	Sends date and time to the switch if applicable 0 = no action 1 = download time to switch
S%.AlarmClearAll	Integer	WZ	0 = no action 1 = clear all alarms
S%.Login	Integer	RWZ	0 = no action 1 = log on
S%.Logoff	Integer	RWZ	0 = no action 1 = log off
S%.LoginState	Integer	RW	0 = no action 1 = check whether logged onto the system
S%.MimicSwitch	Integer	WZ	Mimic a video switch
S%.TestPort	Integer	WZ	0 = no action 1 = test the validity of the port connected to the switch Watchdogs not implemented.
S%.CheckPIN	Integer	WZ	0 = no action 1 = check PIN for equipment or operator
S%.ErrorSend	Integer	WZ	Send error message
S%.FatalErrorSend	Integer	WZ	Send fatal error message
S%.Special	Integer	WZ	Request a special feature
S%.Priority	Integer	CR	Priority number of the device on the CCTV bus used to control a specific camera
S%.GeneralString	String	WZ	This sends the string from the port without any protocol adjustments. No reply is expected. When sent, the string is cleared from the namespace.
S%.CameraInfoUpdate S%.MonitorInfoUpdate S%.AlarmInfoUpdate S%.CameraNumberInfoUpdate S%.TimeDateInfoUpdate S%.SpecialMessageInfoUpdate	Integer	WZ	These commands receive an information update for the equipment associated with the switch. 0 = no action 1 = request info for all items in the group
S%.CameraAttributeUpdate S%.MonitorAttributeUpdate S%.AlarmAttributeUpdate S%.CameraNumberAttributeUpdate S%.TimeDateAttributeUpdate S%.SpecialMessageAttributeUpdate	Integer	WZ	These commands request an attribute update for the equipment associated with the switch. 0 = no action 1 = request info for all attributes for items in the group

Tag Name	Data Type	Flags	Description
S%.SequenceExists S%.SequencePlayExists S%.SequenceRecordExists S%.SequenceStopExists S%.SequencePauseExists S%.SequenceCameraSwitchForwardExists S%.SequenceCameraSwitchBackwardExists S%.SequenceRestartExists S%.SequenceStepForwardExists S%.SequenceStepBackwardExists S%.PresetExists S%.PresetStopExists S%.PresetRecordExists S%.PresetPlayExists S%.CameraAuxiliaryExists S%.CameraAuxiliaryPlayExists S%.CameraAuxiliaryStopExists S%.PatternExists S%.PatternPlayExists S%.PatternRecordExists S%.PatternStopExists S%.PatternPauseExists S%.PatternRestartExists S%.PatternStepForwardExists S%.PatternStepBackwardExists	Integer	CR	See Note 2
S%.SequenceMax S%.PresetMax S%.CameraAuxiliaryMax S%.PatternMax	Integer	CR	0 = not supported -1 = use protocol default during run up

Monitor Namespace Tags

Tag Name	Data Type	Flags	Description
M#.Exists	Integer	CR	Only present if a configuration database exists. 0 = no action 1 = check that this monitor exists.
M#.Description	String	CR	See Note 3
M#.ClientLockID	String	WR	This is a 32 character string.
M#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
M#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)
M#.GeneralString	String	CWR	Up to 50 characters that will be forwarded to display at the monitor.
M#.MonStatus	Integer	WRU	Bit flagged field to define the equipment status. The status field is only to be used for those status identifications that are NOT part of the original item list.
M#.GetSelected	Integer	WZ	Gets information on current assignment. Receives the current macro, auxiliary, camera and whether the macro has stopped, camera is locked and/or controllable, an alarm is armed or tripped and video loss is detected use protocol default during run up 0 = no action 1 = perform command
M#.VideoLossMask	Integer	WR	Activate/deactivate the video fail circuit use protocol default during run up 0 = unknown 1 = deactivated 2 = activated
M#.Salvo	Integer	WZ	Calls up a group of cameras 0 = no action 1 >= Calls up the numbered group of cameras
M#.SequenceExists	Integer	CR	Defines whether the monitor supports sequences See Note 2
M#.SequenceCount	Integer	CR	Defines the number of Sequences in the configuration database
M#.SequenceMax	Integer	CR	Defines the maximum number of sequences 0 = not supported -1 = use protocol default during run up
M#.SequencePlayExists	Integer	CR	See Note 2
M#.SequencePlay	Integer	WR	Forces monitor to execute camera tour sequence
M#.SequenceRecordExists	Integer	CR	See Note 2
M#.SequenceRecord	Integer	WZ	Forces monitor to record camera tour sequence
M#.SequenceStopExists	Integer	CR	See Note 2
M#.SequenceStop	Integer	WZ	0 = no action 1 = stop the defined tour
M#.SequencePauseExists	Integer	CR	See Note 2
M#.SequencePause	Integer	WZ	

Tag Name	Data Type	Flags	Description
M#.SequenceCameraSwitchForwardExists	Integer	CR	See Note 2
M#.SequenceCameraSwitchForward	Integer	WRD	
M#.SequenceCameraSwitchBackwardExists	Integer	CR	See Note 2
M#.SequenceCameraSwitchBackward	Integer	WZ	
M#.SequenceForwardExists	Integer	CR	See Note 2
M#.SequenceForward	Integer	WZ	
M#.SequenceBackwardExists	Integer	CR	See Note 2
M#.SequenceBackward	Integer	WZ	
M#.SequenceRestartExists	Integer	CR	See Note 2
M#.SequenceRestart	Integer	WZ	Check that protocol supports this command 0 = no action 1 = restart
M#.SequenceStepForwardExists	Integer	CR	See Note 2
M#.SequenceStepForward	Integer	WZ	
M#.SequenceStepBackwardExists	Integer	CR	See Note 2
M#.SequenceStepBackward	Integer	WZ	
M#.Camera	Integer	WR	The number of the camera that is to be assigned to this monitor
M#.CameraSwitch	Integer	WRZ	Switch to a next/previous logical camera accessible < 0 previous logical camera > 0 next logical camera

Camera Namespace Tags

Tag Name	Data Type	Flags	Description
C#.Exists	Integer	CR	Only present if a configuration database exists. The parameter is set in the database by the CCTV configuration to show that this Camera exists. 0 = no action 1 = check that this camera exists
C#.Description	String	CR	See Note 3
C#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
C#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)
C#.ClientLockId	String	WR	32 character string. Can be used by a client to lock access to this camera
C#.GeneralString	String	CWR	A string of characters (50 characters maximum) that is written to the specific camera to annotation of all that is being recorded or monitored from it
C#.CamStatus	Integer	WRU	Bit flagged field to define the equipment status. The status flags are to be defined at a later stage. The status field is only to be used for those status identifications that are NOT part of the original item list
C#.PresetExists	Integer	CR	If configuration database exists, this defines if this camera has this ability See Note 2
C#.PresestCount	Integer	CR	
C#.PresetMax	Integer	CR	If the camera supports presets, this is the value of the maximum number of presets. Presets are numbered from 1 to (PresetMax)
C#.PresetStopExists	Integer	CR	See Note 2
C#.PresetStop	Integer	WZ	Clears the preset <integer> 0 = no action 1 >= number of the preset to clear
C#.PresetRecordExists	Integer	CR	See Note 2
C#.PresetRecord	Integer	WZ	Defines the current camera position as preset <integer>
C#.PresetPlayExists	Integer	CR	See Note 2
C#.PresetPlay	Integer	WR	Forces camera to pre-specified position
C#.TiltExists	Integer	CR	See Note 2
C#.Tilt	Signed Integer	WR	Moves camera vertically with given speed. 0 = stop -100 to +100 = % of protocol's maximum capability See Note 1
C#.PanExists	Integer	CR	See Note 2

Tag Name	Data Type	Flags	Description
C#.Pan	Signed Integer	WR	Moves camera with this speed 0 = stop -100 to +100 = % of protocol's maximum capability See Note 1
C#.StopAllPT	Integer	WZ	Stops all Pan and Tilt commands that have not yet been issued 0 = no action 1 = stop all pan & tilt commands
C#.ZoomExists	Integer	CR	See Note 2
C#.Zoom	Integer	WR	Controls the camera zoom 0 = stop zoom 1 = zoom wide -1 = zoom narrow See Note 1
C#.FocusExists	Integer	CR	If configuration database exists, this defines if this camera has this ability See Note 2
C#.Focus	Integer	WR	Controls the camera focus 0 = stop focus 1 = focus near -1 = focus far See Note 1
C#.IrisExists	Integer	CR	See Note 2
C#.IrisAutomatic	Integer	CWR	Controls the camera iris 0 = iris not automatic 1 = iris automatic
C#.Iris	Integer	WR	Controls the camera iris 0 = stops iris 1 = drives iris open -1 = drives iris closed See Note 1
C#.StopAllZFI	Integer	WZ	Write one to this property stops all Zoom, Iris and Focus commands 0 = no action 1 = stops all Zoom, Iris and Focus commands
C#.LensSpeedMax	Integer	CR	The maximum speed of the lens. 1 = fixed speed lens 1 > maximum speed of the lens
C#.LensSpeed	Integer	CWR	Number which is the lens speed See Lens speed max
C#.Arm	Integer	WZ	Arms the camera 0 = no action 1 = arms the camera
C#.Disarm	Integer	WZ	Disarms the camera 0 = no action 1 = disarms the camera

Tag Name	Data Type	Flags	Description
C#.IsArmed	Integer	RWU	Checks whether the camera is armed 0 = no action 1 = check whether the camera is armed
C#.StatusExists	Integer	CR	See Note 2
C#.WiperExists	Integer	CR	See Note 2
C#.Wiper	Integer	WR	Turns wipers on or off 0 = turns the wipers off 1 = turns the wipers on
C#.WasherExists	Integer	CR	See Note 2
C#.Washer	Integer	WR	Activate washers 0 = turns the washers off 1 = turns the washers on
C#.LightExists	Integer	CR	See Note 2
C#.Light	Integer	WR	Turns lights on or off 0 = turns the lights off 1 = turns the lights on
C#.AuxiliaryExists	Integer	CR	See Note 2
C#.AuxiliaryCount	Integer	CR	
C#.AuxiliaryMax	Integer	CR	-1 = use protocol default during run up
C#.AuxiliaryPlayExists	Integer	CR	See Note 2
C#.AuxiliaryPlay	Integer	WZ	Sets the auxiliary <integer>
C#.AuxiliaryStopExists	Integer	CR	See Note 2
C#.AuxiliaryStop	Integer	WZ	Clears the auxiliary <integer>
C#.PatternExists	Integer	CR	Defines whether the camera supports patterns See Note 2.
C#.PatternCount	Integer	CR	Defines the number of Patterns in the configuration database
C#.PatternMax	Integer	CR	Defines the maximum number of patterns -1 = check with switch 0 = not supported
C#.PatternPlayExists	Integer	CR	See Note 2
C#.PatternPlay	Integer	WR	Executes a pattern for a camera
C#.PatternRecordExists	Integer	CR	See Note 2
C#.PatternRecord	Integer	WZ	Records a pattern for a camera
C#.PatternStopExists	Integer	CR	See Note 2
C#.PatternStop	Integer	WZ	Stops the defined tour 0 = no action 1 = stop tour
C#.PatternPauseExists	Integer	CR	See Note 2
C#.PatternPause	Integer	WZ	
C#.PatternForwardExists	Integer	CR	See Note 2
C#.PatternForward	Integer	WZ	Check that protocol supports this command

Tag Name	Data Type	Flags	Description
C#.PatternBackwardExists	Integer	CR	See Note 2
C#.PatternBackward	Integer	WZ	
C#.PatternRestartExists	Integer	CR	See Note 2
C#.PatternRestart	Integer	WZ	0 = done 1 = restart Zero
C#.PatternStepForwardExists	Integer	CR	See Note 2
C#.SequenceStepForward	Integer	WZ	Check that protocol supports this command
C#.PatternStepBackwardExists	Integer	CR	See Note 2
C#.PatternStepBackward	Integer	WZ	

Macro Namespace Tags

Tag Name	Data Type	Flags	Description
Ma#.Description	String	CR	See Note 3
Ma#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
Ma#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)

Auxiliary Namespace Tags

Tag Name	Data Type	Flags	Description
Au#.Description	String	CR	See Note 3
Au#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
Au#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)
Au#.Closed	Integer	WRU	Shows whether an relay is closed 1 = closed 0 = open

Tour Namespace Tags

Tag Name	Data Type	Flags	Description
T#.Description	String	CR	See Note 3
T#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
T#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)

Alarm Namespace Tags

Tag Name	Data Type	Flags	Description
Al#.Description	String	CR	See Note 3.
Al#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
Al#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)

Sequence Namespace Tags

Tag Name	Data Type	Flags	Description
Se#.Description	String	CR	See Note 3
Se#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
Se#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)

Pattern Namespace Tags

Tag Name	Data Type	Flags	Description
Pa#.Description	String	CR	See Note 3
Pa#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
Pa#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)

Preset Namespace Tags

Tag Name	Data Type	Flags	Description
Pr#.Description	String	CR	See Note 3
Pr#.Partition	Integer	CR	Reserved for database partitioning > 0 Partition ID (default = 1)
Pr#.Public	Integer	CR	Reserved for database partitioning 0 = not public 1 = public (default)

Appendix F: DCOM Configuration

When the P2000AE software and the CCTV option are installed on a PC, the installation process makes changes to the Distributed Component Object Model (DCOM) settings to allow communication between P2000AE event actions and the CCTV Server and between the CCTV Client and the CCTV Server, and possibly other installed options on the network.

The installing engineer must be aware of the changes that are made so that the proper level of liaison with the customer is made before installation, to ensure that conflicts of interest with other software installed on the PC are avoided. The installing engineer should also be

aware that the P2000AE software and the CCTV option will not operate correctly if the changes made during installation are subsequently changed.

DCOM Installation

The changes made to the PC are dependent on whether the installation is a P2000AE or CCTV Server or Client installation with Windows XP or Windows 2003.

The changes made are shown in the following table. Note that where more than one option is installed, the appropriate columns should be combined to indicate the overall changes.

Change Made to		P2000AE Server	P2000AE Client
Operating System	Create PegasysServices user account as Administrator	✓	
DCOM	Activate DCOM	✓	
	Grant DCOM access rights to PegasysServices user account	✓	
Registry	Add Program ID for JC.CCTV, JC.CCTV.2 and subsections	✓	
	Add Registry settings for CCTV Selection	✓	✓

Appendix G: Using a Keypad Reader on CK721/720/705 Panels

The following sections describe how to invoke access requests, access requests with a Common PIN, Timed Overrides, and Panel Card Events using a keypad reader.

Note: For CK722 panels, refer to the instructions provided in the CK722 Commissioning Guide.

There is a 15 second time-out on all keypads. Whenever the keypad is idle for more than 15 seconds, all keys entered so far will be ignored, and the entire key sequence needs to be re-entered.

Note: Card ID (the access badge identifier number) can have up to 19 digits. However, the total number of keys pressed for PIN and Card ID combined must not exceed 21.

Invoking Access Requests from a Keypad

To invoke access with a Badge:

1. To be able to invoke access using a badge identifier at any time, set the terminal's **PIN Suppression** in the Timezone tab to <none>. Otherwise, access will be granted only during active timezones.
2. At the keypad reader, present the badge.

To invoke access with PIN Only:

1. The terminal's **PIN Only** flag must be set. **PIN Only** works exclusively with 5-digit algorithmic PINs.
2. Set the panel's **PIN Code Type** to **Algorithmic**.
3. Set the panel's **PIN Code Digits** to **5**.
4. At the keypad reader, enter PIN, and press the # key.

To invoke access with Card ID:

1. To be able to invoke access with Card ID at any time, set the terminal's **PIN Suppression** in the Timezone tab to <none>. Otherwise, access will be granted only during active timezones.
2. The terminal's **Card ID** flag must be set.
3. Make sure the terminal's **PIN Only** flag is *not* set.
4. Make sure the terminal's **PIN + Card ID** flag is *not* set.
5. At the keypad reader, enter the Card ID number and press the # key.

To invoke access with PIN and Card ID:

1. The terminal's **PIN + Card ID** flag must be set.
2. Make sure the terminal's **PIN Only** flag is *not* set.
3. At the keypad reader, enter PIN, then enter the Card ID number and press the # key.

To invoke access using PIN and badge:

1. The terminal's **PIN Suppression** in the Timezone tab must be set to an inactive timezone.
2. Make sure the terminal's **Allow PIN After Badge** flag is *not* set.
3. At the keypad reader, enter PIN and then present the badge identifier.

To invoke access with PIN and badge, allowing PIN after badge:

1. The terminal's **PIN Suppression** in the Timezone tab must be set to an inactive timezone.
2. The terminal's **Allow PIN After Badge** flag must be set.
3. At the keypad reader, present the badge¹, enter PIN and press the # key.

¹⁾ The badge identifier can be presented at any time before the # key is pressed.

Invoking Access Requests from a Keypad with a Common PIN**To invoke access with a Common PIN:**

1. The Server must be online.
2. A **Common PIN** must be defined (in Entity Management) and assigned with the **Access Profile** that contains the terminal (keypad reader).
3. To request PIN Code access:

Without the Star Feature, press the B key followed by the PIN Code number and the # key.

With the Star Feature, press the star (*) key, then press number 2, followed by the PIN Code number and the # key.

Invoking Timed Overrides from a Keypad**To invoke Timed Override with Badge:**

1. The terminal's **Cardholder Override/ Shunt** flag must be set.
2. The badge identifier must be associated with an Access Profile that has the **Override** flag set in Privilege Security Roles.
3. To be able to invoke Timed Override using badge at any time, set the terminal's **PIN Suppression** in the Timezone tab to <none>. Otherwise, Timed Override will be invoked only during active timezones.
4. To start Timed Override:

Without the Star Feature, press the star (*) key, enter the number of minutes, and present the badge.

With the Star Feature, press the star (*) key followed by number 0, enter the number of minutes, and present the badge.

5. To stop Timed Override:

Without the Star Feature, press the star (*) key, enter 0 (for minutes), and present the badge.

With the Star Feature, press the star (*) key followed by number 0 and present the badge.

To invoke Timed Override with PIN Only:

1. The terminal's **Cardholder Override/ Shunt** flag must be set.
2. The badge identifier must be associated with an Access Profile that has the **Override** flag set in Privilege Security Roles.

3. The terminal's **PIN Only** flag must be set. **PIN Only** works exclusively with 5-digit algorithmic PINs.

4. Set the panel's **PIN Code Type** to **Algorithmic**.

5. Set the panel's **PIN Code Digits** to **5**.

6. To start Timed Override:

Without the Star Feature, enter PIN, press the star (*) key, enter the number of minutes, and press the # key.

With the Star Feature, enter PIN, press the star (*) key followed by number 0, enter the number of minutes, and press the # key.

7. To stop Timed Override:

Without the Star Feature, enter PIN, press the star (*) key, enter 0 (for minutes), and press the # key.

With the Star Feature, enter PIN, press the star (*) key followed by number 0, and press the # key.

To invoke Timed Override with Card ID:

1. The terminal's **Cardholder Override/ Shunt** flag must be set.
2. The identifier badge must be associated with an Access Profile that has the **Override** flag set in Privilege Security Roles.
3. To be able to invoke Timed Override using badge at any time, set the terminal's **PIN Suppression** in the Timezone tab to <none>. Otherwise, Timed Override will be invoked only during active timezones.
4. The terminal's **Card ID** flag must be set.
5. Make sure the terminal's **PIN Only** flag is *not* set.
6. Make sure the terminal's **PIN + Card ID** flag is *not* set.

7. To start Timed Override:

Without the Star Feature, enter the Card ID number, press the star (*) key, enter the number of minutes, and press the # key.

With the Star Feature, enter the Card ID number, press the star (*) key followed by number 0, enter the number of minutes, and press the # key.

8. To stop Timed Override:

Without the Star Feature, enter the Card ID number, press the star (*) key, enter 0 (for minutes), and press the # key.

With the Star Feature, enter the Card ID number, press the star (*) key followed by number 0, and press the # key.

To invoke Timed Override with PIN and Card ID:

1. The terminal's **Cardholder Override/ Shunt** flag must be set.
2. The badge identifier must be associated with an Access Profile that has the **Override** flag set in Privilege Security Roles.
3. Terminal's **PIN + Card ID** flag must be set.
4. Make sure the terminal's **PIN Only** flag is *not* set.
5. To start Timed Override:

Without the Star Feature, enter PIN, enter the Card ID number, press the star (*) key, enter the number of minutes, press the # key.

With the Star Feature, enter PIN, enter the Card ID number, press the star (*) key followed by number 0, enter the number of minutes, and press the # key.

6. To stop Timed Override:

Without the Star Feature, enter PIN, enter the Card ID number, press the star (*) key, enter 0 (for minutes), and press the # key.

With the Star Feature, enter the PIN, number, enter the Card ID number, press the star (*) key followed by number 0, and press the # key.

To invoke Timed Override with PIN and Badge:

1. The terminal's **Cardholder Override/ Shunt** flag must be set.
2. The badge identifier must be associated with an Access Profile that has the **Override** flag set in Privilege Security Roles.
3. The terminal's **PIN Suppression** in the Timezone tab must be set to an inactive zone.
4. Make sure the terminal's **Allow PIN After Badge** flag is *not* set.

5. To start Timed Override:

Without the Star Feature, enter PIN, press the star (*) key, enter the number of minutes, and present the badge.

With the Star Feature, enter PIN, press the star (*) key followed by number 0, enter the number of minutes, and present the badge.

6. To stop Timed Override:

Without the Star Feature, enter PIN, press the star (*) key, enter 0 (for minutes), and present the badge.

With the Star Feature, enter PIN, press the star (*) key followed by number 0, and present the badge.

To invoke Timed Override with PIN and Badge, allowing PIN after badge:

1. The terminal's **Cardholder Override/ Shunt** flag must be set.
2. The badge identifier must be associated with an Access Profile that has the **Override** flag set in Privilege Security Roles.
3. The terminal's **PIN Suppression** in the Timezone tab must be set to an inactive zone.
4. The terminal's **Allow PIN After Badge** flag must be set.

5. To start Timed Override:

Without the Star Feature, enter PIN, press the star (*) key, enter number of minutes, present the badge¹, and press the # key.

With the Star Feature, enter PIN, press the star (*) key followed by number 0, enter number of minutes, present the badge¹, and press the # key.

6. To stop Timed Override:

Without the Star Feature, enter PIN, press the star (*) key, enter 0 minutes, present the badge¹, press the # key.

With the Star Feature, enter PIN, press the star (*) key followed by number 0, present the badge¹, and press the # key.

¹) The badge can be presented at any time before the # key is pressed.

Invoking Panel Card Events from a Keypad

Note: When invoking panel card events using panels CK720 or CK705 version 2.2, use the keypad sequence of the star (*) key followed by number 2.

To invoke Panel Card Events with Badge:

1. The event's **Trigger Type** must be set to **Card/Keypad Code**.
2. To be able to invoke a Panel Card Event using a badge at any time, set the terminal's **PIN Suppression** in the Timezone tab to <none>. Otherwise, the Panel Card Event will be invoked only during active timezones.
3. To activate event:

Without the Star Feature, press A, enter the keypad code, and present the badge.

With the Star Feature, press the star (*) key followed by number 1, enter the keypad code, and present the badge.

4. To deactivate event:
- Without the Star Feature*, press D, enter the keypad code, and present the badge.
- With the Star Feature*, press the star (*) key followed by number 4, enter the keypad code, and present the badge.

To invoke Panel Card Events with PIN Only:

1. The event's **Trigger Type** should be set to **Card/Keypad Code** or **Card/PIN/Keypad Code**.

2. If set to **Card/PIN/Keypad Code**, the terminal's **PIN Suppression** in the Timezone tab must be set to an inactive timezone.
3. The terminal's **PIN Only** flag must be set. **PIN Only** works exclusively with 5-digit algorithmic PINs.
4. Set the panel's **PIN Code Type** to **Algorithmic**.
5. Set the panel's **PIN Code Digits** to **5**.
6. To activate event:

Without the Star Feature, enter PIN, press A, enter the keypad code, and press the # key.

With the Star Feature, enter PIN, press the star (*) key followed by number 1, enter the keypad code, and press the # key.

7. To deactivate event:
- Without the Star Feature*, enter PIN, press D, enter the keypad code, and press the # key.
- With the Star Feature*, enter PIN, press the star (*) key followed by number 4, enter the keypad code, and press the # key.

To invoke Panel Card Events with Card ID:

1. The event's **Trigger Type** must be set to **Card/Keypad Code**.
2. To be able to invoke a Panel Card Event using Card ID at any time, set the terminal's **PIN Suppression** in the Timezone tab to <none>. Otherwise, the Panel Card Event will be invoked only during active timezones.
3. The terminal's **Card ID** flag must be set.
4. Make sure the terminal's **PIN Only** flag is *not* set.
5. Make sure the terminal's **PIN + Card ID** flag is *not* set.

6. To activate event:

Without the Star Feature, enter the Card ID number, press A, enter the keypad code, and press the # key.

With the Star Feature, enter the Card ID number, press the star (*) key followed by number 1, enter the keypad code, and press the # key.

7. To deactivate event:

Without the Star Feature, enter the Card ID number, press D, enter the keypad code, and press the # key.

With the Star Feature, enter the Card ID number, press the star (*) key followed by number 4, enter the keypad code, and press the # key.

To invoke Panel Card Events with PIN and Card ID:

1. The event's **Trigger Type** should be set to **Card/Keypad Code or Card/PIN/Keypad Code**.

2. If set to **Card/PIN/Keypad Code**, the terminal's **PIN Suppression** in the Timezone tab must be set to an inactive timezone.

3. The terminal's **PIN + Card ID** flag must be set.

4. Make sure the terminal's **PIN Only** flag is *not* set.

5. To activate event:

Without the Star Feature, enter PIN, enter the Card ID number, press A, enter the keypad code, and press the # key.

With the Star Feature, enter PIN, enter the Card ID number, press the star (*) key followed by number 1, enter the keypad code, and press the # key.

6. To deactivate event:

Without the Star Feature, enter PIN, enter the Card ID number, press D, enter the keypad code, and press the # key.

With the Star Feature, enter PIN, enter the Card ID number, press the star (*) key followed by number 4, enter the keypad code, and press the # key.

To invoke Panel Card Events with PIN and Badge:

1. The event's **Trigger Type** must be set to **Card/Keypad Code or Card/PIN/Keypad Code**.

2. The terminal's **PIN Suppression** in the Timezone tab must be set to an inactive timezone.

3. Make sure the terminal's **Allow PIN After Badge** flag is *not* set.

4. To activate event:

Without the Star Feature, enter PIN, press A, enter the keypad code, and present the badge.

With the Star Feature, enter PIN, press the star (*) key followed by number 1, enter the keypad code, and present the badge.

5. To deactivate event:

Without the Star Feature, enter PIN, press D, enter the keypad code, and present the badge.

With the Star Feature, enter PIN, press the star (*) key followed by number 4, enter the keypad code, and present the badge.

To invoke Panel Card Events with PIN and Badge, allowing PIN after badge:

1. The event's **Trigger Type** must be set to **Card/Keypad Code or Card/PIN/Keypad Code**.
2. The terminal's **PIN Suppression** in the Timezone tab must be set to an inactive timezone.
3. The terminal's **Allow PIN After Badge** flag must be set.
4. To activate event:

Without the Star Feature, enter PIN, press A, enter the keypad code, present the badge¹, and press the # key.

With the Star Feature, enter PIN, press the star (*) key followed by number 1, enter the keypad code, present the badge¹, and press the # key.

5. To deactivate event:

Without the Star Feature, enter PIN, press D, enter the keypad code, present the badge¹, and press the # key.

With the Star Feature, enter PIN, press the star (*) key followed by number 4, enter the keypad code, present the badge¹, and press the # key.

¹) The badge can be presented at any time before the # key is pressed.

Quick Guide to Using Keypad Readers

Use the following quick guide to determine the key sequence at a keypad reader required for a particular action. This section assumes all terminal's and panel's settings have already been configured for this action.

Note: Use the terminal's Star Feature if you want to invoke Panel Card Events on a keypad that does not have the keys A and D.

Legend

Keypad Code	Enter the Keypad Code.	badge	Present the badge.
PIN	Enter the PIN number.	* 0 1	
Card ID	Enter the Card ID number.	# A D	Press the specified key.
Minutes	Enter the number of minutes.		

Invoking Access Requests from a Keypad

With Badge

To request access: **badge**

With PIN Only

To request access: **PIN #**

With Card ID

To request access: **Card ID #**

With PIN and Card ID

To request access: **PIN Card ID #**

With PIN and Badge

To request access: **PIN badge**

With PIN and Badge, allowing PIN after Badge

To request access: **PIN badge#**

1) The badge can be presented at any time before the # key is pressed, that is, before, during or after the PIN is entered.

Invoking Access Requests from a Keypad with a Common PIN

To request access without Star Feature:

B Common PIN #

To request access with Star Feature:

*** 2 Common PIN #**

Invoking Timed Overrides from a Keypad

With Badge

- To start override without Star Feature: * Minutes badge
- To stop override without Star Feature: * 0 badge
- To start override with Star Feature: * 0 Minutes badge
- To stop override with Star Feature: * 0 badge

With PIN Only

- To start override without Star Feature: PIN * Minutes #
- To stop override without Star Feature: PIN * 0 #
- To start override with Star Feature: PIN * 0 Minutes #
- To stop override with Star Feature: PIN * 0 #

With Card ID

- To start override without Star Feature: Card ID * Minutes #
- To stop override without Star Feature: Card ID * 0 #
- To start override with Star Feature: Card ID * 0 Minutes #
- To stop override with Star Feature: Card ID * 0 #

With PIN and Card ID

- To start override without Star Feature: PIN Card ID * Minutes #
- To stop override without Star Feature: PIN Card ID * 0 #
- To start override with Star Feature: PIN Card ID * 0 Minutes #
- To stop override with Star Feature: PIN Card ID * 0 #

With PIN and Badge

- To start override without Star Feature: PIN * Minutes badge
- To stop override without Star Feature: PIN * 0 badge
- To start override with Star Feature: PIN * 0 Minutes badge
- To stop override with Star Feature: PIN * 0 badge

With PIN and Badge, allowing PIN after Badge

- To start override without Star Feature: PIN * Minutes badge¹ #
- To stop override without Star Feature: PIN * 0 badge¹ #
- To start override with Star Feature: PIN * 0 Minutes badge¹ #
- To stop override with Star Feature: PIN * 0 badge¹ #

¹⁾ The badge can be presented at any time before the # key is pressed, that is, before, during or after the PIN and the Timed Override sequence are entered.

Invoking Panel Card Events from a Keypad

With Badge

To activate event without Star Feature: A Keypad Code badge

To deactivate event without Star Feature: D Keypad Code badge

To activate event with Star Feature: * 1 Keypad Code badge

To deactivate event with Star Feature: * 4 Keypad Code badge

With PIN Only

To activate event without Star Feature: PIN A Keypad Code #

To deactivate event without Star Feature: PIN D Keypad Code #

To activate event with Star Feature: PIN * 1 Keypad Code #

To deactivate event with Star Feature: PIN * 4 Keypad Code #

With Card ID

To activate event without Star Feature: Card ID A Keypad Code #

To deactivate event without Star Feature: Card ID D Keypad Code #

To activate event with Star Feature: Card ID * 1 Keypad Code #

To deactivate event with Star Feature: Card ID * 4 Keypad Code #

With PIN and Card ID

To activate event without Star Feature: PIN Card ID A Keypad Code #

To deactivate event without Star Feature: PIN Card ID D Keypad Code #

To activate event with Star Feature: PIN Card ID * 1 Keypad Code #

To deactivate event with Star Feature: PIN Card ID * 4 Keypad Code #

With PIN and Badge

To activate event without Star Feature: PIN A Keypad Code badge

To deactivate event without Star Feature: PIN D Keypad Code badge

To activate event with Star Feature: PIN * 1 Keypad Code badge

To deactivate event with Star Feature: PIN * 4 Keypad Code badge

With PIN and Badge, allowing PIN after Badge

To activate event without Star Feature: PIN A Keypad Code badge¹ #

To deactivate event without Star Feature: PIN D Keypad Code badge¹ #

To activate event with Star Feature: PIN * 1 Keypad Code badge¹ #

To deactivate event with Star Feature: PIN * 4 Keypad Code badge¹ #

¹⁾ The badge can be presented at any time before the # key is pressed, that is, before, during or after the PIN and the Panel Card Event sequence are entered.

Use the keypad sequence * 2 if using CK720/CK705 panels version 2.2.

Appendix H: Troubleshooting

This section explains the authentication process for a P2000AE user. This will help you to understand what goes on behind the scenes and the reason for each step, and how to troubleshoot when problems arise.

Windows 2003 Authentication

The first level of authentication for a P2000AE Workstation is the connection to the P2000AE Server. The Workstation must connect to the Server over the network to gain access to the database. This authentication is performed by the Windows 2003 operating system. The Workstation sends to the Server the username and password that the user used when logging on to Windows. The Server then compares this username and password with the users configured into Windows. In order for the Workstation to connect to the Server, this username and password must be a valid account on the Server.

The P2000AE Server installation creates three Windows user groups that can be assigned to a user account to allow connection to the Server.

The user groups created by the P2000AE installation are:

User Group	Properties
PEGASYS Users	Allowed to connect to the Server and database over the network.
PEGASYS Administrators	Allowed to connect to the Server and database over the network, and also have database administrative rights (needed to drop and create database tables, and to restore the database).
PEGASYS MIS Users	Allowed to connect to the Server and MIS Interface portions of the database.

SQL Server Authentication

The second level of authentication for a P2000AE Workstation is the SQL Server database. The Workstation connects to the SQL Server with an ODBC connection. The ODBC connection passes a username and password to the SQL Server to be authenticated. The default configuration of a P2000AE ODBC connection is to pass the Windows username and password. The username and password sent by the ODBC connection must be a valid account in SQL Server for the Workstation to connect to the database. The P2000AE Server installation creates SQL Server accounts for each of the three Windows user groups mentioned earlier. Since SQL Server has accounts for the user groups created by the P2000AE Server installation, assigning a Windows user account to one of those groups will automatically grant access to the SQL Server database.

P2000AE Authentication

The third level of authentication for a P2000AE Workstation is the list of users configured into the P2000AE software. When the P2000AE software is launched, the user is presented with a login screen. The username and password entered by the user is compared with the users configured in the P2000AE software. The Workstation is also checked against the list of valid workstations configured into the P2000AE system.

Testing the Workstation

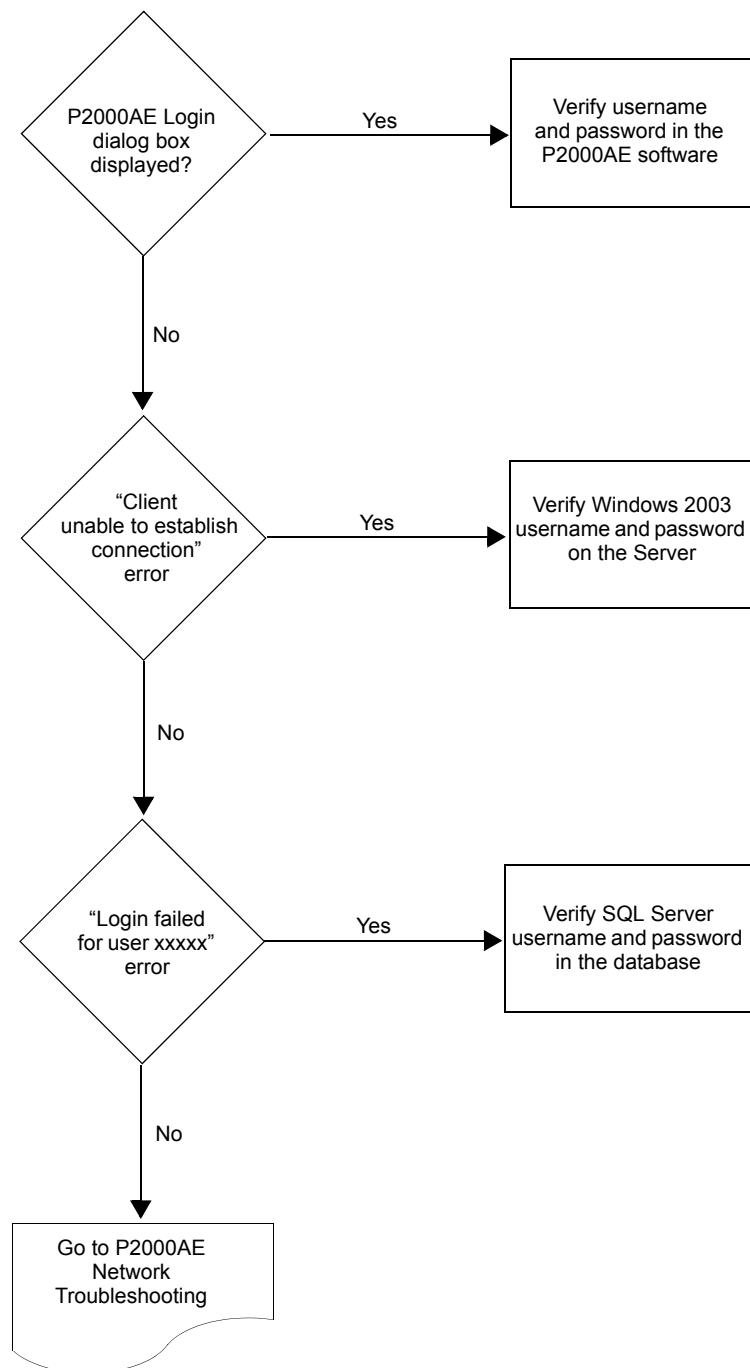
Launch the P2000AE software and log on with the correct username and password. If the login succeeds, everything is OK. If the login fails, see the “P2000AE Login Troubleshooting” on page 453.

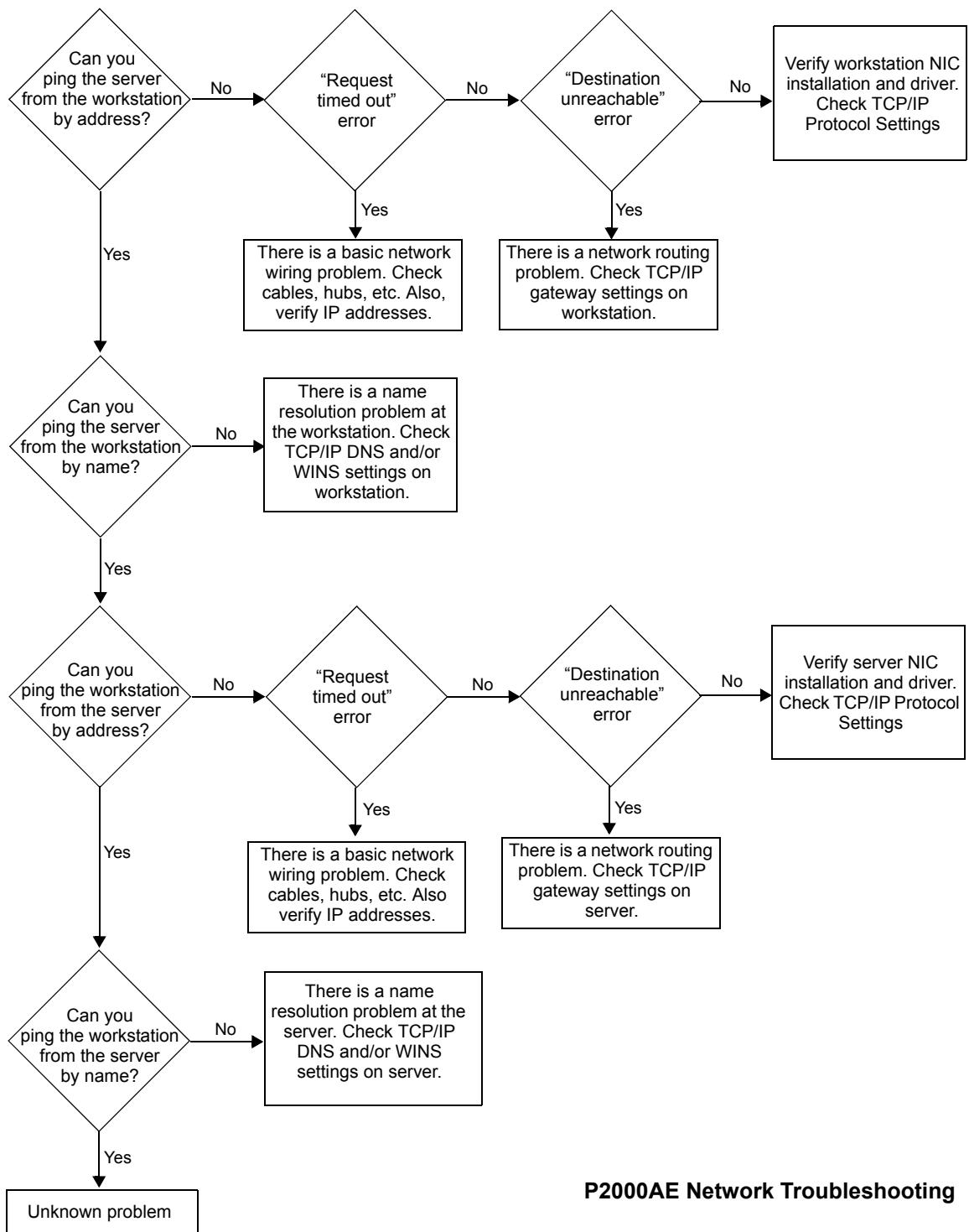
Troubleshooting Workstation Problems

If the P2000AE Login dialog box displays, follow “P2000AE Login Troubleshooting” on page 453. Otherwise follow “P2000AE Network Troubleshooting” on page 454.

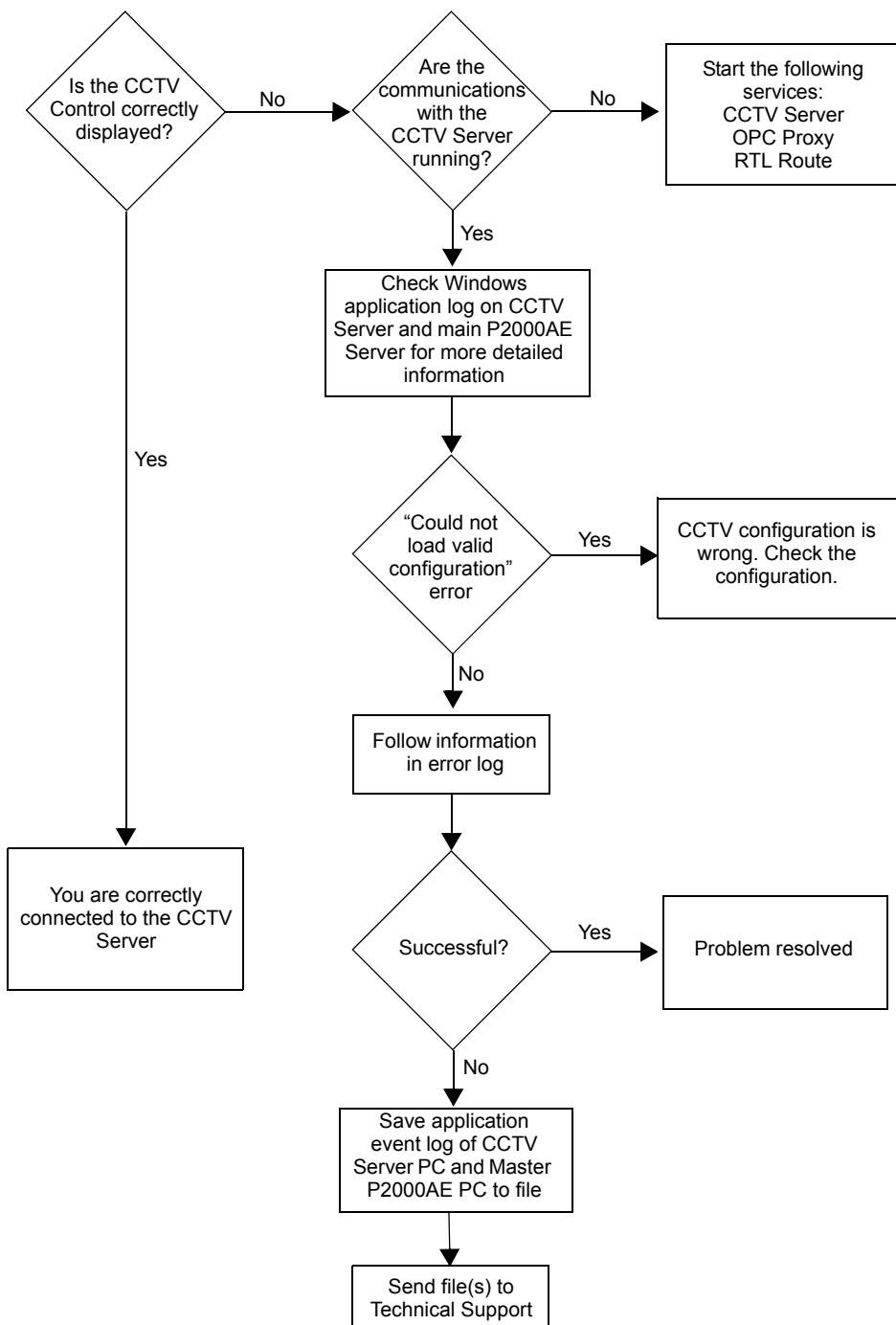
For troubleshooting CCTV, see “CCTV Control Troubleshooting” on page 455.

P2000AE Login Troubleshooting



**P2000AE Network Troubleshooting**

CCTV Control Troubleshooting



Appendix I: Secured Premises Notification Settings

The steps described in this appendix are necessary to ensure UL 1076 compliance when a panel card event is used to unsuppress (arm) life safety alarm signals.

Per UL 1076, if a user can unsuppress life safety alarms at the protected premises, e.g. through a panel card event, then when this event is invoked the user must receive an indication, either audible or visible, that the P2000AE Server received the message generated by the panel after the event was processed. If the user does not receive the expected indication, then either the panel is offline from the Server or the panel did not process the panel card event request.

Note: If you use CK722 panels, refer to the CK722 Hardware Installation Manual for the procedures to define the objects.

Before defining the Host event configuration (page 458), the following configuration information should be verified. Any parameters not specified may be programmed at the end-users discretion.

Entity Configuration

1. Create an Access Badge identifier and assign it an Access Profile that has an **Event Privilege** equal to or greater than the panel card event privilege level used for suppressing/unsuppressing life safety alarms.

Refer to “Entity Field Definitions” on page 133 for detailed instructions.

Panel Configuration

1. The panel must contain at least one input/output terminal in addition to a reader terminal. An acceptable alternative is a terminal that includes input, output, and reader capabilities, such as the S300-DIN-RDR2S. Refer to “Configure Hardware Components” on page 48.

Input Point Configuration

1. The life safety input point’s **Status** must be set to **Enable**.
2. Set the **Disabled During Time Zone** option to <none>.
3. In the **Alarm Priority** drop-down list select 4, 3, 2, 1, or 0, depending on individual company policy for life safety alarms. Refer to “Create Input Points” on page 74.

Output Point Configuration

1. The output point’s **Active State** must be set to **Timed**.
2. Set the **Duration** to 5 seconds or longer.
3. The output point shall be wired to an audible or visible indicator supplied by the end-user. Depending on the terminal type used and the device selected, the end-user may need to supply external power for the indicating device.
4. The indicator shall be visible or audible from the point (location) the panel card event is deactivated. Refer to “Create Output Points and Groups” on page 73.

Input Group Configuration

1. Define an input group that will be used with the panel card event, and that includes the life safety alarm input points defined in “Input Point Configuration” on page 457.

Refer to “Create Input Groups” on page 81.

Panel Card Event Configuration

1. Select an appropriate **Privilege Level** for use with the card.
2. The event’s **Trigger Type** must be set to **Card/Keypad Code** or **Card/PIN/Keypad Code**.
3. The **Event Duration** must be **0**. (The panel card event shall NOT specify an event duration time.)
4. In the Input Group box, select the **Enable** and **SUPPRESS** check boxes and select the affected **Input Group** (defined above).
5. In the **Valid Readers for Current Event** box, select the readers that will be used to initiate the card event.

Refer to “Create Panel Card Events” on page 83.

Host Event Configuration

To meet the UL requirement, a Host event must be created, which will be triggered when a panel card event is deactivated.

1. Create an Event.
2. Make sure the event’s **Allow Manual Trigger** flag is NOT selected.
3. Define the **Trigger** condition as:
 - **Category:** *Badge*.
 - **Type:** *Panel Card Event Deactivated*.
 - **Condition:** *Badge*.
 - **Logic:** *make appropriate selection*.
 - **Value:** *make appropriate selection*.

Note: The **Logic** and **Value** selected must include Access Badge identifiers with the appropriate Event Privilege (defined in Access Profiles), and that are allowed to unsuppress life safety alarms.

4. Define the **Action** condition as:

- **Delay:** *00:00:00* (none).
- **Category:** *Outputs*.
- **Type:** *Set Output*.
- **Outputs:** select the output defined in “Output Point Configuration” on page 457.
- **Duration:** *0 seconds*.

Refer to “Creating Events” on page 206.

Host Event Configuration (CK722 Only)

To meet the UL requirement, a Host event must be created, which will be triggered when a panel card event is deactivated.

1. Create an Event.
2. Make sure the event’s **Allow Manual Trigger** flag is NOT selected.
3. Define the **Trigger** condition as:
 - **Category:** *Multiple Command Object*.
 - **Type:** *MCO State 0 (Transition)*.
 - **Condition:** *Name*.
 - **Logic:** *make appropriate selection*.
 - **Value:** *make appropriate selection*.

Note: The **Logic** and **Value** selected must be equal to the Multiple Command Object defined to unsuppress life safety alarms.

4. Define the **Action** condition as:

- **Delay:** *00:00:00* (none).
- **Category:** *Outputs*.
- **Type:** *Set Output*.

- **Outputs:** select the output defined in “Output Point Configuration” on page 457.
- **Duration:** *0 seconds*.

Refer to “Creating Events” on page 206.

Sequence of Events

The following information describes a typical sequence of events given the configurations described before.

1. Applicable life safety alarms are in a secure state and are not suppressed.
2. An authorized person initiates (activates) a panel card event, which suppresses an input group including life safety alarm signals.

3. All life safety alarm signals associated with the panel card event are now suppressed and will not report to the host.
4. An authorized person deactivates the previously activated panel card event.
5. All life safety alarm signals associated with the panel card event are now unsuppressed (armed) and will report to the host (if the panel is online).
6. The host, having received the panel card event deactivate message, initiates its event and sets the appropriate output point.
7. The output point activation causes an audible or visible indicator to be annunciated at the location where the panel card event was deactivated.

Index

Symbols

- # of failed download connections 319
- # of failed download transfers 319

A

- Abort Time 247
- Access Badge 142
- access deny 31
- access grant 31
- Access Grant Message 89
- Access Grant Message on Door Open Only 61
- Access Groups 117
 - creating an access group 117
- Access Levels 123, 140
- Access PIN 145
- Access Profile Template 122
- Access Profiles 138
- Access Requests 7
 - access profiles 7
 - invalid badges 7
 - time 7
 - valid badges 7
- Access Security Role 124, 140
- Access Security Roles 129
- Access Template 139
- access time 65, 92
- Access/Intrusion Group 141
- Access/Intrusion Groups 124
- Account Disabled 147
- Acknowledgement Required before Completion 77
- ACO Terminal Groups 70
- ACS Interface Service 314
- Action Date/Time 164
- Action Interlock Errors 239
- Action Interlock Operation 237
- Action Interlock tab 238
- Action Interlocks 237
- Actions 208
 - changing order of occurrence 209
 - creating an action 208
 - event actions field
 - definitions 209
- Activated Devices 251
- Active Tours 252
- active-off 79
- active-on 79
- ADA Relay Connector 67

- ADA Relay Delay 67
- ADA Relay Time 67
- ADS 147
- ADS Repository Name 241
- ADS/ADX server 240
- AES-CBC 41
- alarm beep 165
- Alarm Category 160, 164
- Alarm Category Filters 106
- Alarm Colors 167
- Alarm Count 167
- alarm debounce time 63
- Alarm Description 164
- alarm details 167
- Alarm Escalation Ranges 105
- Alarm Instruction 77
- Alarm Late 247
- Alarm Monitoring 160
 - acknowledging an alarm 161, 165
 - activating an event 167
 - alarm handling 161
 - alarm monitor definitions 163
 - alarm response field
 - definitions 166
 - audible alarm button 165
 - completing an alarm 162, 166
 - date/time 163
 - escalation 163
 - locating alarms on maps 165
 - priorities 163
 - refreshing the window 162
 - removing an alarm from the queue 162
 - removing an alarm message from the queue 166
 - responding to an alarm 161, 165
 - setting priority sounds 163
- Alarm Options 30, 75
- Alarm Popup 77
- Alarm Priority 76
- Alarm Processing Group 148
- alarm shunt only for aux. access 60
- Alarm Site 165
- Alarm Skip 248
- Alarm State 164
- Alarm Status 164
- Alarm Timezone 76
- Alarms 8
 - door alarms 8
 - external device alarms 8

- host alarms 8
- remote alarms 8
- software only alarms 8
- Alarms, Auxiliaries, Macros and Tours 268
- Allow Any IP Address 42
- Allow devices 235
- Allow expansion 190
- Allow Manual Trigger 207
- allow PIN after badge 61
- Alpha 143, 145
- Alternate Connection 52
- Alternate Enterprise Site 292
- Always upload when greater than 53
- American Dynamics Switch Protocol 397
- CCTV Controls 397
- CCTV Event Actions 397
- Maximum and Default Values 398
- OPCWrite Event Actions 398
- Annunciator 200
- anti tailgate 61
- Anti-Loitering 156
- Anti-Passback 156
- anti-passback 65
- Any Guard 247
- application path 43
- Approval Levels 300
- Area Alarms Setting 180
- Area Control 178
 - configuring the Area 178
 - controlling the Area 181
 - defining Area Filters 183
 - displaying details 183
- Area Details 183
- Area Filters 183
- Area Layout 185
- Area Monitor 307
- Area Terminals and Inputs Points 180
- Aritech Intrusion 205
- Aritech Intrusion Server 111
- armed 200
- Asset 133
- Assisted Access 66
- Assisted Access Time 67
- Associated AV Channel 77
- Associated Real Time Map 77
- At Risk 187, 198
- Audit Trail 283

audit trail history 34
 Authorized Users 284
 Auto Badge Management 153
 Auto Duress Alarm 247
 Auto Forward 246
 Auto Process 300
 Auto Reverse 246
 Auxiliary Access 8
 AV Service 314

B

Backup Configuration 326
 Backup History 326
 Backup SCT 326
 Backups 329
 advanced 331
 automatic 331
 backup device 35, 329
 manual 330
 restoring database 332
 BACnet
 Troubleshooting 238
 BACnet Action Interlocks 237
 BACnet Interface 51, 233
 System Setup 235
 Theory of Operation 233
 BACnet Internal Address 236
 BACnet object 233
 BACnet Query String 237
 BACnet Routed 236
 BACnet Service 233, 314
 BACnet Site Options 236
 Badge Edit Style 33
 Badge Layout 143, 145
 Badge Station 228
 badge station 20
 Badge Trace Alarm for Denied
 Access 30
 Badge Trace Alarm for Granted
 Access 30
 Badge Type 33
 Based on Password Policy 148
 Basic Configuration 5
 Basic System Components 2
 external device 4
 field panels 4
 Server 2
 system printer 4
 terminals 4
 workstations 3
 Beginning Grace Period 114
 BetaTech Switch Protocol 399
 CCTV Controls 399
 CCTV Event Actions 399
 Maximum and Default
 Values 400
 OPCWrite Event Actions 400
 Switch Configuration 399
 Bind Server 36
 BQT Reader with LCD 62

Broadcast Message 307
 bypassed 200

C

Cabinet Access Control 94
 Cabinet Configuration 96
 Cabinet Door Groups 98
 Cabinet Door Masks 96
 Cabinet Door Names 95
 Calculate Digital Signature 326,
 335
 Calibration 69, 79
 Camera Auxiliaries, Patterns and
 Presets 275
 Camera Controls 273, 279
 Camera Movement Actions 393
 Cameras 263, 272
 Card Events 9
 Card Formats 58, 69
 Card Type 68
 Cardholder Override/Shunt 65
 CCTV 256
 Naming Conventions 260
 CCTV Components 262
 CCTV Control 276
 CCTV Event Actions 281
 CCTV Server 262, 263, 314
 CCTV Server Namespace
 Definitions 425
 CCTV Standard Control
 Buttons 277
 CCTV Switch Communications 266
 CCTV Switch Protocols 262, 393
 CCTV System Hardware 259
 central 64
 central Enterprise site 292
 Central Station 200
 Certificate Authority 30
 Certificate Service 314
 Cipher Algorithm 41
 CK705/CK720 Panel
 updating 322
 CK722 cached controller image
 compress 326
 CK722 cached controller image
 rebuild 326
 CK722 cached controller image
 update 326
 CK722 Communications 40
 CK722 Forced Door 177
 CK722 Input Calibration 327
 CK722 Interface Service 314
 CK722 Maintenance End 327
 CK722 Maintenance Start 327
 CK722 Message Configuration 111
 CK722 Propped Door 177
 Commands 22, 177
 Common PIN 144
 Comms Server 30
 Communication
 downloads 7
 operating modes 6
 central 6
 local 6
 shared 6
 transactions 6
 Communication Modes 6
 Configuration DB Server 30
 Configuration Sequence 17
 Configure Cameras 272
 Configure CCTV Servers 263
 Configure Monitors 269
 Configure Switches 265
 Configuring Hardware
 Components 48
 Configuring System
 Components 27
 Connections 49
 Control Center 177
 Control Station Groups 288
 Control Sub-Stations 288
 Controller Write DB To Flash 321
 Controls
 Camera 279
 Monitor 279
 Switch 277
 Count All 180
 Count Inputs 181
 Count Terminals 180
 Creation Tab 114
 Current Count 184
 Custom Configuration Number 51
 Custom Reports 349
 create custom reports 349
 edit reports in Crystal 351
 export existing reports 351
 import custom reports 350

D

D620 Mode 92
 Database and Namespace 259
 Database External Trigger 40
 Database Maintenance 325
 advanced backups 331
 automatic backups 331
 backup device 329
 database backup 329
 database restore 332
 manual backups 330
 Database Server 292
 Database Table Definitions 349
 DCOM Configuration 439
 DCOM Installation 439
 Default Alarm Colors 167
 Degraded 195
 Delay Downloads Until 319
 delete badges from panel before
 download 310
 delete elevators from panel before
 download 310

- Delete Entity Without Identifier 327
- Delete Expired Access Badges 327
- Delete history older than 53
- Delete Unused Access Groups 327
- Delete Unused Access Profiles 327
- Delete Unused Intrusion Groups 327
- De-Muster 191, 197
- Deny All 22
- Deny If Door Open 61
- DES-CBC 41
- Details 254
- Direct Output Control 89
- Directive Services Password Validation 36
- Directory Services Path 36
- disabled during Time Zone 75
- Disarmed 200
- Display All alarm options 167
- Door Configuration 98
- Door controls 172
- Door Open Warning 65
- Door Tracking 97
- Download Access Groups of badge 37
- Download All From Internally Cached Controller Image 310
- Download badges with Undefined entry/exit status 37
- Download Function 309
 - download data to panels 309
- Download options 37
- Download Service 314
- Download Status 311
 - by panel 311
 - monitor download status 311
- Download to disabled panels 37
- Download to STI-E 125, 142
- Drill 196
- DSO Terminal Groups 70
- Dual Ethernet 52
- duress 86
- Duress Alarm 248
- DVR 282

- E**
- Elevator Access Grant 89
- Elevator/Cabinet Parameters 94
- Elevators 87
 - basic definitions 88
 - configuring 91
 - general overview 87
 - high level interface 88
 - low level interface 88
- E-mail setting 39
- Emergency Access 140
- Emergency Access Level 123
- Emergency Override 97
- Employee Message 113
- Empty Alarms 327
- Empty Alarms History 327
- Empty Audit History 327
- Empty Download Queue 327
- Empty Guard Tour Note 327
- Empty P2000EntityConfig Archive Database 327
- Empty P2000History Archive Database 327
- Empty Saved Muster Data 328
- Empty Smart Download Queue 328
- Empty Transaction History 328
- Enable Alarm 76
- Enable BACnet Interface 111
- Enable Input Suppression Messages 55
- enable panel relay group outputs 54
- Ending Grace Period 114
- enforce entry/exit 53
- Enforce Limitations 32
- Enterprise 3, 291
 - Entity Access 293
 - Global Access Rights 294
- Enterprise Access Groups 293
- Enterprise Parameters 292
- Enterprise Sites 134, 292
- Enterprise Time Zones 293
- Entities
 - adding an entity image 134
 - Address 134
 - entering entity information 132
 - entity field definitions 133
 - Organization 136
 - Privileges 141
 - Sponsor/Owner 134
 - Status 137
 - user defined fields 138
 - Validation 136
 - viewing entity information 132
- Entity Bulk Edit 152
- Entity Categories 119
- Entity Data 133
- Entity Details 216
- Entity Duplicator 151
- Entity Groups 121, 135
- Entity Management 131
- Entity Options 118
- Entity Resync 155
- Entity Types 133
- Entry Exit Delay 75
- Escalation 78
 - Escalation based upon visibility 78
- Escalation Increment 78
- Escalation Repeat 78
- Escalation Service 314
- Escalation Timeout 78
- Escort 135
- Escorted by All 136
- Event 1-4 77
- Event Action Types 371
- Event Actions 208
- Event Counters 211
 - adding event counters 211
 - editing event counters 211
 - resetting event counters 212
 - viewing event counters 211
- event duration 85
- Event Privilege 125, 141
- Events 9
 - card events 9
 - creating events 206
 - system events 9
 - timed events 9
 - using event configuration dialog boxes 206
- Expand Zone 197
- Expiration Period for Requests 300
- Export XML 113
- Extended Access 8
- External Event Trigger 39
- External IPs 235
- External Trigger Service 314

- F**
- Facility Code 34, 55, 143, 145
- facility code only when offline 61
- Facility Codes 68
- FASC-N Badges 33, 146
- Fast Flash 174
- fast flash 73
- FDA 36
 - Enforce Part 11 36
- FDA Backup 35
- FDA Backup Performed 328
- FDA Backups 332
- FDA Retention Policy 35
- FDA Title 21 CFR Part 11 283
- File External Trigger 40
- Filtering Entity Data 151
- Fireman Override 91
- Floor Configuration 93
- Floor Groups 94
- Floor Masks 90
- Floor Names 89
- Floor Tracking 93
- forced door/proped door 86
- Format media on backup 331
- Four-Digit PINs 72
- Fully Qualified Name 240

- G**
- General ASCII Protocol 395
 - commands 395
- General Message 113
- Generate namespace based on protocol defaults 267
- Geutebrück Switch Protocol 401
 - CCTV Controls 401
 - CCTV Event Actions 402

- M**
- Maximum and Default
 - Values 403
 - OPCWrite Event Actions 402
 - Global Badge Entry/Exit Status
 - Synchronization 30
 - Global In-X-It Tracking 30
 - Global Sub-Station 286
 - Grant All 22
 - Grant Only 248
 - Group Controller Address 55
 - Group Member 136
 - Guard 243
 - Guard Tour 242
 - adding stations 249
 - assigning to a specific guard 247
 - assigning tour badges 243
 - configuring guard tours 244
 - Control all tours 252
 - controlling guard tours 251
 - Details 254
 - forward and reverse 242
 - guard tour priority 244
 - principles and definitions 242
 - scheduled times 246
 - system hardware 243
 - tour abort 243
 - traversal time 250
 - Guard Tour Control 251
 - Guard Tour Priority 125, 142
 - Guard Tour Service 242, 314
- H**
- Hardware Configuration
 - Sequence 48
 - Help 14
 - context sensitive 14
 - online 14
 - Hide reports 351
 - High Level Interface 88, 92
 - High Priority 311
 - High Speed RS485 51
 - History DB Server 30
 - Holidays 46
 - adding a holiday 46
 - assigning holiday types 47
 - holiday calendar 47
 - changing the calendar month 47
 - changing the calendar year 47
 - Host Poll Timeout 52
- I**
- I/O Linking 79
 - Id Badge 144
 - Identifier 142
 - Identifier Access Profile 144
 - Identifier Purpose 127, 145
 - Identifier Type 143
 - IIS Service 316
- J**
- Journal 137
- K**
- KDM Update 324
 - Key Size 41
 - Keyless Override/Shunt Time 66
 - Keypad 441
 - keypad code 85
 - Keypad/Display 200
- L**
- LAN (local area network) 3
 - language selection 43
 - languages 43
 - Last poll communication 319
 - latch output 54
 - Late Alarm 248
 - Launch Automatically 20
 - LDAP 36
 - Legacy panel access group
 - download disable 37
 - Legacy PIN Code 143
 - Legacy Privilege Flags 41
 - Legacy Terminal Groups 70
 - Load CK722 Identifier Format 328
 - Load Language Reports 339
 - Load P2000EntityConfig Archive
 - Database from Backup 328
 - Load P2000History Archive
 - Database from Backup 328
 - local 64
 - Local Alarms 38, 163
 - Local Configuration 43
 - Local Site 42, 139
 - Log Operator Action 248
 - log output status message 63
 - log reader strike message 61
 - Log Tour Operation 248
 - Logging on to P2000 10
 - changing the default login name 11
 - default login values 11
 - passwords 10
 - Super User 11
 - User Name 10
 - Logging Out of P2000 12
 - Loop Communication 6
 - Loop Configuration 48
 - Loop Number 52
 - Loop Timeout 52
 - Low Level Interface 88, 92
 - Lowest Floor for Group Controller 55
- M**
- M3/M5 Workstations 233
 - Main Menu 4
 - Manual Conventions 2
 - Manual Process 300
 - Manual Reset 247
 - Manual Tour 245, 253
 - Map Maker 218
 - adding image sets 223
 - adding map attachments 222
 - creating an importable image 221
 - importing an image to map maker 221

- placing device icons on a real time map 221
- system map 220
- to setup the map maker window 220
- Master Station 287
- Max Allowed 179
- Max Allowed Alarmed 182
- Max Badge Number 33
- Max Inactive Period 30
- Max Issue Level 33
- Max Security Level 33
- Message Data Configuration 110
- Message Filter Configuration 163, 213
- Message Filter Group 20, 38, 163
- Message Filter Groups 107
- Message Filtering 99, 100
- Message Forwarding 171
 - editing message forwarding 172
 - forwarding to another station 171
 - removing message forwarding 172
- Message Routing 99, 108
- Message Routing Status 165
- Message Types 102
- Message Types and Sub-Types 381
- Metasys 233
- Metasys III Action Queue 314
- Metasys system extended architecture 239
- mimic 79
- Min Required 179
- Min Required Alarmed 182
- MIS image folder 231
- MIS Interface 231
 - input and output tables 232
 - partitioned systems 232
 - prerequisites 231
 - using the interface 232
- MIS Interface Service 314
- Missing 187, 198
- momentary auxiliary access 61
- Monitor
 - Sequence 271
- Monitor Controls 279
- Monitor Sequences 271, 394
- Monitoring Remote Alarms 162
- Monitoring Remote Messages in Real Time 213
- Monitors 263, 269
- Mouse Conventions 12
- MSEA 78
- MSEA Graphic 78
- MSEA Graphics 239
- MSEA Registration 240
- Multi-Alarm Handling 148
- Muster 187
- Muster Control 188
- Muster Control Service 314
- Muster Reports 189
- Muster reports 198
- Muster Shift Setup 190
- Muster Startup Rules 190
- Muster Terminals 187, 192
- Muster Zone 187
- Muster Zone Alarm Settings 191
- Mustered 187, 199
- Mustering 186
 - controlling 194
 - defining Muster Zones 188
 - events 193
- N**
- NAE controller 240
- Namespace
 - Changing the Number of Items 261
 - Naming Items 260
 - Number of Items 261
 - Number of Permitted Items 261
- Namespace and Database 259
- Namespace entries to be generated 267
- Namespace Tags 426
 - Alarm 437
 - Auxiliary 437
 - Camera 433
 - Macro 437
 - Monitor 431
 - Pattern 438
 - Preset 438
 - Sequence 438
 - Switch 426
 - Tour 437
- Navigating through the System 12
- Network Communication 5
- Network Panel 318
- N-Man Rule 67
- No Access Group Archive to Flash 51
- No Badge Archive to Flash 51
- No Configuration Archive to Flash 51
- No Green Light on Aux Access 61
- None.wav 165
- Normal Access 140
- Normal Access Level 123
- Normal Popup 77
- Normal Priority 311
- Notification Class objects 233
- Number of Doors 31
- Number of Floors 30
- O**
- Object Engine Service 314
- Occupancy 156
- ODBC Data Source 43
- OPC Intercom 289
- OPC Intrusion 110
- OPC Name 266
- OPC Proxy Service 314
- OPC Server 209
- OPC Tag 210
- Open for Access Time 172
- Operate Door Strike 85
- Operating the System 131
- Operator Controls 172
 - controlling doors 172
 - controlling outputs 173
 - controlling panel relays 174
- Operator Name Filters 106
- Operators and Messages 99
- Options 225
- Organization Elements 118
- Out Of Order Alarm 248
- Output Control 173
- output delay 54
- Output Points and Groups 73
 - creating output groups 73
 - creating output points 73
- Output Relays 9
 - activated by events 9
 - activated manually 9
 - input linking 9
 - output linking 9
- Override Reset Threat Level 64
- Overwrite Existing Database 333
- P**
- P2000 Location 3, 99
- P2000 Remote Server 100, 108, 163, 214
- P2000 Services 312
- P2000 Services Definitions 314
- P2000 Thick Client 22
- P2000AE Authentication 452
- P2000-Metasys 233
- Panasonic Switch Protocol 405
 - CCTV Controls 405
 - CCTV Event Actions 406
 - Maximum and Default Values 407
 - OPCWriTe Event Actions 406
 - Switch Configuration 405
- Panel avg. clock drift 319
- Panel Card Events 83
 - creating a panel card event 84
 - panel card event field definitions 84
- Panel Card Formats 58
- Panel Comparison Matrix 389
- Panel Details 319
- panel lost AC 87
- panel low battery 87
- Panel max clock drift 319
- Panel Poll Interval 52
- Panel Relay Control 174
- panel tamper 87
- panel time zones 56

- Panel Types 32
- Panels 4, 48
 - adding a new panel 49
 - configuring additional panel components 58
 - configuring panel components 56
 - configuring panel holidays 57
 - assigning a panel holiday 57
 - configuring panel time zones 56
 - assigning a panel time zone 56
 - assigning an output group to a panel time zone 57
 - edit panel field definitions 50
 - access tab 53
 - address tab 51
 - alarm tab 54
 - elevator tab 55
 - general tab 50
 - history tab 52
 - loop/unit tab 52
 - misc tab 55
 - panel naming conventions 48
- Partition Name Filters 103
- Partitions 9, 225
 - creating partitions 227
 - deleting partitions 227
 - regular 226
 - super user 226
 - types 226
- Password change 23
- Password Mode 42
- Password Policy 35
- Password Validation 35
- Password Verification 13
- Passwords
 - expiration 148
- Pelco Switch Protocol 409
 - CCTV Controls 409
 - CCTV Event Actions 410
 - Macro Programming 411
 - Maximum and Default Values 411
- OPCWrite Event Actions 410
- Recording Patterns 411
- Periodic Service 314
- Permanent Suppression 177
- Person 133
- Philips Burle Switch Protocol 413
 - Cabling Configuration 415
 - CCTV Controls 414
 - CCTV Event Actions 414
 - Maximum and Default Values 415
- OPCWrite Event Actions 414
- Switch Macros 413
- PIN 71
- PIN + Card ID 71
- PIN Code 31, 145
 - configuring 70
- PIN Code Digits 54
- PIN code retry 86
- PIN code type 54
- PIN Duress 72
- PIN Only 71
- PIN Plus 1 Duress 62
- PIN required when offline 61
- PIN Retry Alarm 72
- PIN suppression 68
- Port Configuration 37
- Pre Max Allowed 179
- Pre Max Allowed Alarmed 182
- Predefined Alarm Response Text 166
- Preferred Loop Direction 52
- Preview a badge 230
- Priority Ranges 105
- Priority Service 314
- privilege level 84
- Privilege Security Role 124, 140
- Privilege Security Roles 130
- Privileges 141
- Processing Mode 300
- Processing Remote Message 38, 163, 214
- Property Number 237
- Protocol 266
- Protocol Type 55
- public 20
- Public Access Timezone 93, 98
- Purpose 143
- Push to Talk 288
- Q**
- Query String 165, 237
- Query String Filters 103
- Queued Download Actions 311
- R**
- Random Watch 246
- RDR2S/KDM Update 324
- reader 60
- reader override timezone enable 61
- Real Time List 213
 - color coded transactions 216
 - printing the real time list 216
 - viewing all options in the list 215
 - viewing specific options in the list 215
- Real Time Map 218
 - activating events 220
 - creating a real time map 220
 - opening a door 219
 - sub maps and attachments 218
 - using the real time map 218
 - viewing the real time map 218
- Real Time Printing 31
- Reason 143, 145
- Reboot on any failure 313
- Receiving Messages 38
- Record Persistence 284
- Record Retention 284
- Record Validation 284
- Reestablish Delay 52
- Registration Parameters 4, 28
- Re-lock on Door Open 61
- Remain Time 253
- Remote Alarms 38, 162, 163
- Remote Message Service 38, 162, 213, 314
- Remote Partitions 150
- Remote Servers 108
- Remote Station 290
- Remove Access Profile from Disabled Identifiers 328
- Remove Access/Intrusion Groups from Unused Access Profiles 328
- Renegotiate Interval 41
- Report Alarm 97
- Report Configuration 350
- Report Interfaces 349
- report on terminal 87
- reporting delay 54, 75
- Reports 339
 - alarm activity report 344
 - custom reports 349
 - database table definitions 349
 - databases 351, 352
 - definitions 342
 - entities report 345
 - entities without identifiers report 347
 - field/table relationship 349
 - print 341
 - samples 344
 - transaction history report 348
- Request Approvers 300
- Request Queue 335
- Request Queue Service 315
- Request Queue View 336
 - details 338
 - filtering 337
- Required Approval Levels 300
- Rescuer 188, 199
- Reset Counters 319
- Reset Counters to Zero 328
- Reset Reserved Autobadge Numbers 328
- Reset Time 319
- Response Required before Completion 77
- Response Text 169
 - creating predefined alarm response text 169
 - deleting an alarm response text 169
 - editing alarm response text 169
- Restart on 1st failure then reboot 313
- Restart on 2 failures then reboot 313
- Restart on failure 313
- Restore to archive 333

Resume Normal Operation 173
 Retention Policy 34
 reverse reading 61
 reverse swipe duress 62
 reverse track 79
 RS232 External Trigger 39
 RTL Route Service 315
 Run Time 247

S

S321 Panels 324
 S321 SIO Handler Service 315
 Schedule start on 114
 scramble mode 54
 SCT 14
 SCT Browser Interface 22
 Secure Authentication 36
 Secured Premises Notification
 Settings 457
 secure-off 79
 secure-on 79
 Security Flags 124, 128, 140
 Security level control 174
 Security Levels 174
 Security Rights 123, 140
 Security Roles 123, 127, 140
 Send Email to Request
 Approvers 299
 Sequence Number 249
 Sequester 199
 Sequester Terminals 187, 193
 Sequestered 187
 Server 2
 Service Controls 315
 stop and start 315
 stop/start a specific service 316
 stop/start all services 316
 Service Monitor 317
 Service Override 92, 97
 Service Startup Configuration 312
 Set Alarm Color 252
 Set all Input Status to Unknown 328
 Set all Output Status to
 Unknown 328
 Set all Panel Status to
 Unknown 328
 Set all Terminal Status to
 Unknown 328
 set panel relay when active 75
 shared 64
 Show All 182, 183
 Show Only 182, 183
 Show UDF Fields 159
 Shrink Database 328
 shunt devices 251
 shunt time 65
 Shunt Warning Auto Off 65
 SIA Interface 169
 SIA Interface Service 315
 SIA Message View 170

Site Director 240
 Site Name Filters 102
 Site Parameters 29
 editing site parameters 30
 site parameters field
 definitions 30
 Slow Flash 174
 slow flash 73
 Smart Download Control 311
 Smart Download Rules 37
 Smart Download Service 315
 SMTP Hello Domain 39
 SMTP Server 39
 Soft Alarms 86
 enabling soft alarms 86
 soft alarms field definitions 86
 Soft Input Points 50
 soft in-x-it 62, 87
 Special Access 7, 67
 assigning access profiles 8
 basic access override 7
 auxiliary access 8
 extended access 8
 timed override 7
 Sponsor 135
 Sponsor Required 120
 SQL Server Authentication 451
 Standard Reports 339
 run standard reports 340
 Star Feature 62
 Station Group 286
 Station Type 250
 Stop and Search Service 315
 Stop Suppression 177
 Stop Timed Open 173
 Sub-Station 286
 Super User 10, 11, 226
 Suppress Input Points 176
 Switch Controls 277
 Switch Protocols 262, 393
 American Dynamics 397
 BetaTech 399
 communications 393
 General ASCII 395
 Geutebrück GST Interface 401
 Panasonic 405
 Pelco 409
 Philips Burle 413
 Ultrak 417
 Vicon 421
 Switches 263, 265
 System Administrator 133
 System Configuration 17
 adding system configuration
 items 18
 editing system configuration
 items 18
 searching system configuration
 items 19
 system configuration window 17
 System Events 9

System Maintenance 309
 System Options 225
 system override 54
 System Overview 4
 System Status 318
 accessing the window 318
 inputs 320
 intrusion 321
 Legend 319
 logical 320
 outputs 320
 panels 320
 S300 hardware 321
 terminals 320
 System Validation 334

T

T&A Interface 113
 T&A Terminal 112
 TCP/IP External Trigger 40
 Temporary Access 124, 141
 Terminal Count 184
 Terminal Groups 69
 creating a terminal group 70
 Terminal Lost AC 87
 Terminal Low Battery 87
 Terminal Tamper 87
 Terminals 58
 creating a new terminal 59
 creating an I/O terminal 63
 edit terminal field definitions 60
 access tab 64
 card type tab 68
 flags tab 60
 general tab 60
 timezone tab 68
 set up terminals for each panel 59
 Testing the Workstation 452
 Time & Attendance Object 113
 Time and Attendance Interface 112
 Time and Attendance Interface
 Service 315
 time offset 53
 Time Zones 44
 active/inactive 45
 configuring time blocks 44
 copying a time zone 46
 creating a new time zone 45
 holiday types 46
 creating holiday types 46

Timed Button 92
 Timed Events 9
 Timed Open 172
 Timed Override 7
 timed override/anti-tailgate 53
 Timed Override/Timed Shunt 65
 Timed Suppression 177
 Timed/Pulse 174
 timezone checking 53
 Toolbar 14

- Tour Activation 243
 Tour Alarms Setting 248
 Tour Badge 243
 Tour Badge priority 244
 Tour Configuration 244
 Tour Notes 255
 Tour Priority 245
 Tour Station 249
 Tour Types 245
 trace 31, 125, 142
 track 79
 Track Movement 193
 Track On Input Open 93
 Track On Transition Only 93
 Transmit Filter 109
 Transmit Queue 109
 Transmit Session 110
 Transmitting Messages 38
 Trapped 187, 199
 traverse time 250
 Trigger Logic 207
 Trigger Types 84, 353
Triggers
 creating trigger conditions 206
 creating triggers 206
 editing a trigger condition 208
 manual triggers 212
 trigger field definitions 207
Troubleshooting
 CCTV Control 455
 Login 453
 Network 454
 Workstation Problems 452
- U**
 Ultralx Switch Protocol 417
 CCTV Controls 417
 CCTV Event Actions 417
 Maximum and Default
 Values 418
 OPCWrite Event Actions 418
 Switch Configuration 417
 Un-calibrate 80
 Uncalibrate 69
 Unisolate Station 290
 Unit Number 52
 Universal PIN 145
 Unlock all Doors 173
 Unremote Station 290
 unsuppress life safety alarms 457
 Update CK705/CK720 Panels 322
 Update CK722 Panels 323
 Update S321 Panels 325
 Upload only when greater than 53
 Upload Service 314
 Use Authorized SMTP 39
 Use Encryption 36
 Use Enterprise Settings 294
 Use for XmlRpc 236
 User Accounts 23
 adding user name and
 password 23
User Defined Fields 125
 creating user defined fields 125
User Name 164
User Preference 304
User Role Management 21
User Roles 148
User Site 164
User Tab 147
Username Formatting 36
Users
 adding users to the system 21
 assigning users 23
Using a Keypad Reader 441
 access requests 441
 access with Common PIN 442
 panel card events 445
 Quick Guide 447
 timed overrides 442
- V**
 valid & unauthorized 62
Valid Readers for Current Event 86
Validate Digital Signature 328, 334
Verification by Access Profiles 144
Verify Password 147
Version description 319
Vicon Switch Protocol 421
 Camera Lens Speed Control 422
 CCTV Controls 421
 CCTV Event Actions 422
 Maximum and Default
 Values 423
 Momentary and Latched
 Auxiliaries 422
 OPCWrite Event Actions 422
 Switch Configuration 421
Video Imaging 227
 capturing images 229
 defining a workstation 228
 printing a badge 229
 specifications 228
 viewing and printing a badge 230
View Contents 334
View Inoperable Hardware 197
View XML 113
Viewing Real Time List
 Transactions 214
Violation Alert Period 35
Visitor Escort Mode 68
Visitor Management 306
- W**
 Wandering 187, 199
Warning Auto Off 66
Warning Output Group 65, 66
Warning Time 65, 66
Watchdog Service 315
Web Access 295
 Add Entity 305
 Alarm Monitor 305
 Approver Levels 302
 Area Search 304
 Asset Finder 304
 Audit 306
 Command Outputs 305
 Contractor Request 306
 Customizing the interface 307
 Door Command 305
 Edit/Delete Entity 305
 Emergency Access Disable 307
 Employee Services 304
 Entity Activity 304
 Entity Resync 304
 Entity Search 304
 Guard Services 305
 Logging on 303
 Management Services 305
 Options 299
 Processing requests 307
 Request Approval 305
 Request Status 305, 306
 styles 308
 Submitting Requests 303
 User Roles 296
 Validate 306
 Visitor Request 306
 Web UI Styles 150, 308
 WebBook Favorites 304
 WebPermissions 22
 Windows 2003 Authentication 451
Work Schedule Object 113
Work Schedule Service 315
Work Scheduler 112, 306
Workstation Status 317
 view workstation status 317
Workstations 19
 adding a workstation 19
 editing a workstation 20
 Launching the alarm monitor 20
 workstation field definitions 20
Workstations and Users 19
- X**
XmlRpc 42
XmlRpc Interface Service 315
- Z**
Zone 195
Zone Hardware Status 195
Zone Name 188
Zone Status 195
Zone Terminals 187, 192