



P2000

Security Management System

Software User Manual

PRELIMINARY

P2000

Security Management System

Software User Manual

Version 3.11 and higher, September, 2011

24-10618-147 Revision –



Copyright 2011
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
P2000 or P2K 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 or P2K system is 1000.
5. The P2000 or P2K 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.
10. The "Host Poll Delay" must not exceed 200 seconds.
11. P2000 or P2K 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 or P2K 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.
16. The workstation defined as "Server" must have the alarm monitor parameter set to "always active".

UNDERWRITERS LABORATORIES COMPLIANCE VERIFICATION SHEET

P2000 or P2K SYSTEM

Page 2 of 3

17. For P2000 or P2K software version 2.5 or later, when configuring “Service Startup” parameters the following services shall not be disabled.

P2000 RTL Route Service

P2000 CK720 Download Service

P2000 CK720 Priority Service v1.0

P2000 CK720 Priority Service v2.1

P2000 CK720 Upload Service

P2000 Periodic Service

P2000 S321 SIO Handler Service

P2000 S321-IP Interface Service

P2000 SIO Handler Service

P2000 Smart Download Service

18. For Line Security over the Internet, between the P2000 or P2K server and the controllers CK705, CK720, CK721, CK721-A, and S321-IP 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 or P2K 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 or P2K server and the controllers D620, D6AP, and S320, 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 EtherLite2 serial port server

The P2000 or P2K 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. For Line Security over the Internet, between the P2000 or P2K server and the controller S321-DIN, 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 or P2K 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.

21. The router and serial port server shall be installed within the same room as the controllers S320, D620 and/or D6AP and within 20 feet of the controller when employed for encrypted line security.

22. P2000 or P2K systems use the Digi International Model Digi One SP converter or B&B Electronics Model 485OT9L converter to communicate to S321-DIN controllers.

23. The B&B Electronics Model 485OT9L converter shall be installed within the same room as the P2000 or P2K server and within 20 feet of the server under all conditions of use.

24. 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.

25. 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, S320, S321-DIN, S321-IP, D620 and/or D6AP.

UNDERWRITERS LABORATORIES COMPLIANCE VERIFICATION SHEET
P2000 or P2K SYSTEM
Page 3 of 3

26. 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.
27. Alarm signals received at a remote P2000 or P2K server via the Remote Message Services from a different P2000 or P2K server are supplementary.
28. Alarm signals received at a P2000 workstation are supplementary.
29. Alarm signals received at a personal computer or personal digital assistant through the Web Access feature are supplementary.
30. P2000 or P2K systems use the PC232-S4-1 Protocol Converter to communicate to D620, D6AP and/or S320 controllers; a controller must be connected to the port defined as Loop 1 at the P2000 or P2K for Protocol Converter's tamper switch to report as an alarm.
31. 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.
32. The following features have not been investigated by Underwriters Laboratories:
 - BACNet interface
 - Dial-Up
 - Fire server
 - Intrusion server
 - Isonas interface
33. The following products have not been investigated by Underwriters Laboratories and shall not be used in a listed system:
 - P900 product line
 - OSI product line
 - Aritech® intrusion panel
 - Notifier fire alarm panel
34. The P2000 or P2K and HID Edge access control unit may be used for access control monitoring purposes only.
35. A Panel Down alarm message received at the central station may be an indication of a compromise attempt.
36. For the S321-IP, the "Heartbeat Transmit Interval" must not exceed 90 seconds and the "Host Reception Timeout" must not exceed 200 seconds.

PRELIMINARY

Table of Contents

Chapter 1: Introduction	1
Getting Started	1
Chapter Summaries	1
Manual Conventions.....	2
Basic System Components	2
Main Menu.....	5
Registration Parameters.....	6
System Overview	6
Basic Configuration	6
Network Communication.....	6
Loop Communication.....	7
Communication Modes	7
Types of Communication.....	8
Access Requests	8
Time and Time Zones.....	8
Valid or Invalid Badges	8
Badge Privileges.....	8
Controlling Special Access.....	9
Overriding Basic Access.....	9
Granting Badge Privileges	9
Alarms	9
External Device Alarms	9
Door Alarms	9
Software-Only Alarms.....	9
P2000 Host Alarms	10
Remote Alarms	10
Non-alarm Input Points	10
Output Relays	10
Input/Output Linking.....	10
Activating Outputs by Events.....	10
Activating Outputs Manually	10
Events	10
Database Partitioning.....	10
Logging On to the P2000 System Software	11
Changing the Default Login Values.....	12
Logging Off from the P2000 System Software	13
Navigating through the P2000 System.....	13
Mouse Conventions	13

Basic Window Components	14
Instruction Conventions	16
Menu Shortcuts	17
Verification Passwords	17
Context Sensitive Help	17
Online Help	17
P2000 Tutorial	17
Viewing the Toolbar	18
Chapter 2: Configuring the System	19
System Configuration Overview	19
Using the System Configuration Window	19
Set Up Workstations and Operators	21
Workstations	21
Workstation Field Definitions	22
Adding Operators to the System	23
Creating Permission Groups	23
Assigning Operators	25
P2000 Directory Services Password Validation	29
Changing the User Password	29
Setting Up User Accounts	30
Adding a Login Name and Password for the P2000 System into the Operating System	30
Configure System Components	37
Registration Parameters	38
Site Parameters	39
Site Parameters Field Definitions	40
Local Site	53
Local Configuration	54
Time Zones	55
Configuring Time Blocks	55
Holiday Types	57
Holiday	57
Using the Holiday Calendar	58
Assigning Holiday Types	58
Configure Hardware Components	59
Hardware Configuration Sequence	59
Create Panels	59
Panel Naming Conventions	59
Loop Configuration	60
Soft Input Points	62
Edit Panel Field Definitions	62
Configure Panel Components	71
Configure Panel Time Zones	72
Configure Panel Holidays	73

Enable Codes (EC) Definition.....	74
Configure Air Crew PIN Numbers.....	74
Configure Panel Card Formats.....	75
Configure Additional Panel Components.....	76
Create and Configure Terminals.....	76
Set up Terminals for each Panel	76
Edit Terminal Field Definitions	77
Use the Add Hardware Module.....	89
Create Terminal Groups	91
Configure PIN Codes.....	92
PIN Only	92
PIN + Card ID	93
PIN.....	93
Four-Digit PINs	94
PIN Duress	94
PIN Retry Alarm.....	94
Create Input and Output Points and Groups.....	94
Create Output Points and Groups	94
Create Input Points and Groups	96
Create Input Points	96
Input Point Field Definitions	96
Configuring Reader Terminal Hardwired Input Points	102
Using Reader Terminal Door Contact Input Points.....	102
Using the Terminal Down Input Point	103
Create Input Groups	103
Creating Instruction Text.....	104
Create Panel Card Events	105
Panel Card Event Field Definitions	106
Configure Soft Alarms.....	108
Soft Alarms Field Definitions.....	108
Configure P900 Panels and Components.....	109
P900 to P2000 Terminology Cross Reference	109
Import P900 Sequence Files	110
Configure P900 System Parameters	110
Configure P900 Panels.....	111
Configure P900 Terminals	113
P900 Terminal Field Definitions	114
Configure P900 Input/Output Points	118
P900 Input Field Definitions.....	118
P900 Soft Alarms.....	120
Configuring CLIC Components.....	120
P900 Counters.....	121
P900 Flags.....	121
P900 Trigger Events	122
P900 Trigger Event Field Definitions	123
P900 Trigger Links.....	126

Configure OSI Panels and Components	127
Unsupported OSI Features.....	127
Unsupported P2000 Features.....	127
System Architecture.....	127
Hardware Detection.....	128
Badge Access Rights.....	129
Configuration Sequence	129
Configure OSI Facility Parameters	129
OSI Facility Field Definitions.....	130
Adding New Portals.....	134
Configure OSI Panels	136
Configure OSI Terminals	137
OSI Terminal Field Definitions.....	138
Viewing OSI Wireless Devices Status	140
Rebuilding the WAMS Database	140
Configure S321-IP Panels and Components	141
S321-IP Naming Conventions	141
Configure S321-IP Panels	141
S321-IP Panel Field Definitions	142
Configure S321-IP Terminals	145
S321-IP Terminal Field Definitions	145
Configure S321-IP Input Points	148
S321-IP Input Point Field Definitions	150
Configure S321-IP Output Points	152
Configure Isonas Panels and Components	154
Configure Isonas Panels.....	154
Configure Isonas Terminals.....	155
Isonas Terminal Field Definitions.....	156
Configure Isonas Input Points.....	158
Configure Isonas Output Points.....	159
Configure HID Panels and Components	160
Hardware Requirements.....	160
HID Panel Naming Conventions	161
Configure HID Facility Parameters	161
Configure HID Panels	161
HID Panel Field Definitions	162
Configure HID Terminals	164
HID Terminal Field Definitions	165
Configure HID Input Points	168
HID Input Point Field Definitions	169
Configure HID Output Points	170
Troubleshooting Misconfigured HID Readers	171
Configure Assa Abloy® IP Door Locks and Components	172
Hardware Requirements.....	173
Assa Abloy Component Naming Conventions.....	173
Configure Assa Abloy Facility Parameters	173

Add a Door Service Router (DSR).....	176
Edit Assa Abloy Panels.....	177
Assa Abloy Panel Time Zones.....	178
Configure Assa Abloy Terminals	178
Assa Abloy Terminal Field Definitions	179
Configure Assa Abloy Soft Input Points.....	180
Assa Abloy Status Information.....	181
Real Time Functions.....	182
Lockout Mode with Assa Abloy Locks	182
File Maintenance on the DSR Server	182
P2000 Badge Format.....	182
Configure Elevators and Cabinets.....	186
Elevator Access Control.....	186
General Overview	186
Basic Definitions	187
Low Level Interface.....	187
KONE HLI/KONE ELINK High Level Interface	188
KONE IP High Level Interface	188
Otis EMS - Security / BMS Protocol High Level Interface	188
Otis Compass High Level Interface	189
Defining Floor Names	191
Defining Floor Masks	191
Configuring Elevators	192
Elevator Configuration Field Definitions.....	192
Configuring Floors	196
Configuring Otis Unsecured Elevators.....	196
Configuring KONE IP Elevators.....	197
Defining Floor Groups.....	202
Creating Access Groups for Elevator Floors	202
Cabinet Access Control.....	202
Defining Door Names	203
Defining Door Masks	204
Configuring Cabinets	204
Cabinet Configuration Field Definitions	204
Configuring Doors.....	206
Defining Door Groups	206
Creating Access Groups for Cabinet Doors.....	207
Configure Message Filtering and Message Routing	207
Operators and Messages.....	207
Basic Principles and Definitions	207
Sequence of Steps.....	208
Message Filtering	208
Create Message Filter Groups.....	215
Message Routing	216
Configuring P2000 Remote Servers	216
P2000 Remote Server Field Definitions.....	216

Set up Access Groups and Cardholders.....	218
Create Access Groups.....	218
Cardholder Options.....	220
Define Companies and Departments.....	220
Create Access Templates.....	222
Access Template Edit Field Definitions	222
Create Badge Formats	223
Create Badge Purposes	224
Create Badge Reasons	224
Create Required Cardholder Fields.....	225
Create User Defined Fields	225
Define Automatic Employee IDs	227
Entering Cardholders.....	228
Chapter 3: Operating the System	229
Providing Access to Cardholders and Visitors	229
Entering Cardholder Information.....	230
Viewing Cardholder Information	230
Cardholder Field Definitions	231
Adding a Cardholder Image.....	234
Adding a Cardholder Journal	234
User Defined Fields.....	235
Entering Badge Information	237
Badge Field Definitions.....	238
Viewing Badge Data	244
Bulk Badge Change.....	245
Entering Visitor Information.....	246
Add Visitor Field Definitions.....	247
Auto Badge Management	249
Badge Resync.....	250
Image Recall	252
Image Recall Filters.....	252
Image Recall FS (Full Screen).....	253
To Activate Image Recall FS:	253
Monitoring Alarms	255
Alarm Configuration	255
Alarm Category.....	255
Alarm Handling	256
Monitoring Remote Alarms	257
Alarm Monitor Definitions.....	258
Alarm Response Field Definitions.....	261
Configuring Alarm Colors	262
Creating Predefined Alarm Response Text	263
Monitoring Alarms Using the SIA Interface	264
Message Forwarding	266

Fire Alarm Control	267
Basic Definitions	267
Basic Fire Alarm Components	268
Fire Alarm Server Configuration	268
Fire Alarm Configuration	269
Fire Alarm Management	270
Controlling Fire Alarm Components.....	270
Viewing Fire Transactions Using the Real Time List.....	272
Monitoring Fire Components Using the Real Time Map.....	272
Viewing and Controlling Fire Components Using the System Status Window	272
Fire Component Events	272
Operator Controls.....	273
Controlling Doors	273
Controlling Outputs	274
Controlling Panel Relays.....	275
P900 CLIC Controls	275
To Manually Control a P900 Counter:	275
To Manually Control a P900 Flag:	276
To Manually Control a P900 Trigger Event:.....	276
Security Threat Level Control.....	277
Defining Security Levels	277
Applying Security Level	278
Input Point Suppression	279
Controlling Areas and Muster Zones.....	280
Area Control.....	280
Configuring the Area.....	280
Controlling the Area	283
Defining Area Filters	285
Displaying Area Details.....	285
Area Details Field Definitions.....	286
Area Layout	287
Area Reports.....	288
Mustering	289
Basic Definitions	289
Sequence of Steps	290
Define Risk Areas and Muster Zones	290
Muster Zone Definition Fields	291
Defining Zone Terminals.....	294
Defining Muster Terminals.....	294
Defining Sequester Terminals	295
Mustering Events	296
Controlling Muster Zones.....	297
Muster Zone Status and Control Field Definitions	297
Viewing and Printing Muster Transactions in Real Time	300
Muster Reports	300
Intrusion Detection	301

Basic Definitions	302
Sequence of Steps.....	302
Intrusion Configuration.....	303
OPC Aitech Intrusion Interface	303
Bosch Intrusion Interface	304
Intrusion Alarms	306
Intrusion Management	308
Controlling Intrusion Items Using the Intrusion Control Window.....	308
Viewing Intrusion Transactions Using the Real Time List.....	309
Monitoring Intrusion Using the Real Time Map.....	310
Viewing and Controlling Intrusion Items Using the System Status Window	310
Intrusion Events	311
Hours On Site.....	311
Configuring Hours On Site Zones	311
Hours On Site Reporting.....	312
Hours On Site (Detail) Report.....	313
Hours On Site - Simple Report	314
Creating Events.....	314
Using Event Configuration Dialog Boxes	314
Creating Triggers	315
Trigger Field Definitions.....	316
Creating Actions.....	317
Event Actions Field Definitions	318
OPC Server Event Actions	318
Counting Events.....	319
Creating Manual Triggers	321
Monitoring the System in Real Time	322
Using the Real Time List.....	322
Monitoring Remote Messages in Real Time.....	322
Viewing Real Time List Transactions.....	323
To Display Color Coded Transactions:	324
Printing the Real Time List.....	325
Using the Real Time Map	326
Sub Maps and Attachments.....	326
Opening a Door	328
Activating Events from the Real Time Map.....	328
Creating a Real Time Map	328
Handling Alarms from the Real Time Map.....	331
Adding Map Attachments	332
Duplicating Maps	332
Adding Image Sets.....	332

Chapter 4: Advanced Features	335
Partitions	335
Partition Types	336
Regular Partitions	336
The Super User Partition	336
Creating Partitions.....	337
Video Imaging	337
Video Imaging Specifications.....	338
Defining a Video Imaging Workstation.....	338
Printing a Badge	339
Capturing the Portrait and Signature Images	339
Viewing and Printing the Badge.....	340
MIS Interface	341
MIS Prerequisites.....	341
Understanding the Input and Output Tables	342
Partitioned Systems	342
Using the MIS Interface.....	342
Metasys Integration (BACnet)	343
Overview	343
Theory of Operation	343
System Setup.....	345
Setting Up BACnet Site Options	345
BACnet Site Field Definitions.....	345
Setting Up External IPs.....	346
Configuring Hardware Components for BACnet Interface	347
Setting Up BACnet Action Interlocks	347
Action Interlock Operation	347
M3/M5 Setup.....	348
Troubleshooting	348
Duplicate Object Name Errors	348
Msg Rejected Errors	348
Action Interlock Errors	349
Metasys System Extended Architecture.....	349
Defining MSEA Graphics	349
Registering the P2000 Server with a Site Director.....	350
Guard Tour	352
Basic Principles and Definitions.....	352
Sequence of Steps.....	353
Defining System Hardware for Guard Tour Operation	353
Assigning Tour Badges	353
Configuring Guard Tours.....	354
Using the Guard Tour Configuration Window	354
Timezones, Start and Abort Times	356
Additional Guard Tour Options	357
Adding Stations to the Guard Tour.....	358

Tour Station Definition Fields.....	359
Controlling Guard Tours.....	361
Guard Tour Handling	363
Guard Tour Details	364
Guard Tour Notes	365
Viewing and Printing Transactions in Real Time	365
Guard Tour Reports	366
Tour Configuration Report	366
Tour Transaction History Report.....	366
Tour Notes Report	366
CCTV.....	367
Using P2000 functions with the CCTV Feature	368
CCTV Configuration Overview	368
Points to Note	369
Using the CCTV/AV Configuration Window.....	369
Defining System Hardware for the CCTV Feature	370
Namespace and Database	370
Relationship Between the Namespace and Database	371
CCTV Naming Conventions.....	371
Naming Items for the CCTV Server Namespace	371
Defining the Number of Namespace Items.....	372
Number of Default Items Permitted	372
Changing the Number of Namespace Items.....	373
Switch Protocols	373
Tristate Check Boxes.....	373
CCTV Components.....	374
CCTV Server.....	375
Create and Configure the CCTV Server.....	375
Edit Server Field Definitions	376
Switches.....	376
Create and Configure Switches	376
Edit CCTV Switch Field Definitions.....	377
Alarms, Auxiliaries, Macros and Tours	379
Alarms.....	379
Auxiliaries	379
Macros	379
Tours.....	379
Edit CCTV Alarm, Auxiliary, Macro and Tour Field Definitions	380
Monitors	380
Create and Configure Monitors.....	380
Edit CCTV Monitor Tabs.....	381
Sequences	382
Edit CCTV Sequence Field Definitions	383
Cameras	383
Create and Configure Cameras	383
Edit CCTV Camera Tabs	384

Camera Auxiliaries, Patterns and Presets	386
Camera Auxiliaries.....	386
Patterns	386
Presets.....	386
Edit CCTV Named Camera Item Field Definitions.....	387
CCTV Control.....	387
CCTV Standard Controls	388
Selecting the Item to Control	388
Operating the Controls.....	388
Using Switch Controls.....	389
Selecting a Switch	389
Selecting a Tour, Macro or Switch Auxiliary	389
Using Tour, Macro or Switch Auxiliary Controls	389
Using the Monitor Controls	390
Selecting a Monitor	390
Selecting a Sequence	390
Using Sequence Controls	390
Using the Camera Controls	391
Selecting a Camera	391
Selecting a Pattern, Preset or Camera Auxiliary	391
Using Pattern, Preset or Camera Auxiliary Controls.....	391
CCTV Event Actions	392
CCTV Event Action Field Definitions	393
CCTV Reports.....	394
CCTV Switch Report.....	394
CCTV Monitor Report	394
CCTV Camera Report	394
CCTV Summary Report.....	394
DVR.....	394
Redundancy	395
FDA Part 11.....	395
Intercom	396
Hardware Requirements	396
Intercom System Hardware Verification	397
Intercom Configuration.....	397
Intercom Exchange	397
Intercom Stations.....	400
Intercom Control.....	402
Controlling Intercom Stations using the Real Time Map.....	404
Intercom Events	404
Intercom Transaction History Reports.....	404
P2000 Enterprise.....	405
Enterprise Parameters	406
Assign Cardholders Enterprise Access.....	407
Define Global Badge Access Rights	408
Web Access	409

Sequence of Steps.....	410
Creating and Assigning Web Access Menu Permissions	410
Defining Web Access Options	411
Web Access Options Field Definitions.....	411
Defining Request Approvers	413
Submitting Requests using Web Access	416
Web Access Functions	416
Employee Services.....	416
Guard Services	417
Management Services	417
Visitor Management.....	418
Emergency Access Disable	419
Processing Web Access Requests	419
Visitor Request Management Field Definitions.....	421
Customizing the Web Access Interface	423
Assigning Styles to Web Access Users	423
Web Access Smart Card Encoder Configuration.....	424
Chapter 5: System Maintenance.....	429
Downloading Data to Panels	429
Download Status	430
Smart Download Control	431
Controlling and Monitoring P2000 Services	432
Service Startup Configuration	432
P2000 Services Definitions	433
Starting and Stopping Service Control.....	435
Controlling Services through the Service Monitor.....	436
Workstation Status	436
Automatic Software Updates	437
System Status	439
Writing CK7xx Database to Flash Memory	446
Updating CK7xx Panels	447
Updating S321-DIN Panels	448
Database Maintenance	449
To Perform Database Maintenance Functions:.....	449
Database Maintenance Actions	450
Database Backup.....	452
Configuring a Backup Device	453
To Perform Manual Backups:.....	454
Advanced Backups	454
Automatic Backups	455
FDA Part 11 Backups	455
Database Restore	456
System Validation	458
Request Queue View	459

Searching Specific Requests	461
Viewing Request Details	462
Chapter 6: System Reports	463
Using P2000 Standard Reports.....	463
P2000 Standard Report Definitions.....	466
Selected Sample Reports.....	471
Running the Alarm History Report.....	471
Running the Cardholders - Preprocessed Report.....	472
Running the Cardholders without Badges Report	474
Running the Panel Report	475
Running the Transaction History Report.....	476
Creating Custom Reports.....	477
Creating a Custom Crystal Report for the P2000 System.....	477
Database Table Definitions.....	477
To Import a Custom Crystal Report into the P2000 System:.....	477
Editing a P2000 Standard Report in Crystal	478
To Export an Existing Standard Report from the P2000 System:.....	478
To Edit the P2000 Report in Crystal	478
Appendix A: Event Triggers/Actions	481
Trigger Types	481
Category: Alarm	481
Category: Area	482
Category: Audio-Visual	482
Category: Audit	483
Category: Badge	483
Category: Counter.....	484
Category: External Trigger	484
Category: Fire Detector.....	484
Category: Fire IO Module.....	485
Category: Fire Panel	485
Category: Fire Zone	485
Category: Inputs.....	485
Category: Integration Component	486
Category: Intercom.....	486
Category: Intrusion Annunciator.....	486
Category: Intrusion Area	487
Category: Intrusion Device	488
Category: Intrusion Zone.....	488
Category: Mustering.....	488
Category: Operator	489
Category: Outputs	489
Category: Panel	489

Category: Terminal	489
Category: Time Zone	490
Category: Time/Date	490
Event Action Types	491
Category: Audio-Visual	491
Category: BACnet	492
Category: Badge	492
Category: CCTV	492
Category: Download	492
Category: Fire Detector	493
Category: Fire IO Module	493
Category: Fire Zone	493
Category: Host	493
Category: Inputs	496
Category: Intercom	496
Category: Intrusion Announcer	496
Category: Intrusion Area	496
Category: Intrusion Zone	496
Category: Metasys Interlock	496
Category: Mustering	497
Category: OPC Server	497
Category: Outputs	497
Category: Panel	497
Category: Security Level	497
Category: Terminal	498
Appendix B: Message Types and Sub-Types	499
Appendix C: Panel Comparison Matrix	503
Appendix D: CCTV Switch Protocols	509
Communications	509
Camera Movement Actions	509
Monitor Sequences	510
General ASCII Protocol	510
Commands Supported	510
American Dynamics	511
The American Dynamics Protocol	511
Supported CCTV Controls	511
Supported CCTV Event Actions	511
Supported OPCWrite Event Actions	512
Autorepeat Actions	512
Automatic Status Update Tags	512

Maximum and Default Values	512
BetaTech	513
Switch Configuration	513
Keyboard 16 Commands	513
The BetaTech Protocol	513
Supported CCTV Controls	513
Supported CCTV Event Actions	513
Supported OPCWrite Event Actions	514
Autorepeat Actions	514
Automatic Status Update Tags	514
Maximum and Default Values	514
Geutebrück - GST Interface	515
The Geutebrück Protocol	515
Supported CCTV Controls	515
Supported CCTV Event Actions	516
Supported OPCWrite Event Actions	516
Macros	516
Camera Auxiliaries	516
Monitor Sequences	517
Autorepeat Actions	517
Automatic Status Update Tags	517
Maximum and Default Values	517
Panasonic®	518
Switch Configuration	518
Panasonic SX850 Protocol	518
Supported CCTV Controls	518
Supported CCTV Event Actions	519
Supported OPCWrite Event Actions	519
Camera Movement Commands	519
Autorepeat Actions	519
Automatic Status Update Tags	519
Maximum and Default Values	519
Pelco®	520
The Pelco 9760 Protocol	520
Supported CCTV Controls	520
Supported CCTV Event Actions	521
Supported OPCWrite Event Actions	521
Autorepeat Actions	521
Automatic Status Update Tags	522
Macro Programming	522
Recording Patterns	522
Maximum and Default Values	522
Philips Burle (Bosch®)	523
Switch Macros	523
The Philips Burle Protocol	523
Supported CCTV Controls	524

Supported CCTV Event Actions.....	524
Supported OPCWrite Event Actions	524
Autorepeat Actions	524
Automatic Status Update Tags.....	524
Maximum and Default Values	525
Cabling Configuration	525
Ultrak®	526
Switch Configuration	526
Keyboard 64 Commands	526
The Ultrak MaxPro-1000 Protocol.....	526
Supported CCTV Controls	526
Supported CCTV Event Actions.....	526
Supported OPCWrite Event Actions	527
Auxiliaries	527
Monitor Sequences.....	527
Autorepeat Actions	527
Automatic Status Update Tags.....	527
Maximum and Default Values	527
Vicon®.....	528
Switch Configuration	528
The Vicon Protocol.....	528
Supported CCTV Controls	528
Momentary and Latched Auxiliaries.....	529
Camera Lens Speed Control	529
Supported CCTV Event Actions.....	529
Supported OPCWrite Event Actions	529
Autorepeat Actions	530
Automatic Status Update Tags.....	530
Maximum and Default Values	530
Appendix E: CCTV Server Namespace Definitions	531
Flags	531
Notes.....	531
Namespace Tags	532
Switch Namespace Tags	532
Monitor Namespace Tags.....	537
Camera Namespace Tags.....	539
Macro Namespace Tags.....	543
Auxiliary Namespace Tags	543
Tour Namespace Tags	543
Alarm Namespace Tags	543
Sequence Namespace Tags	544
Pattern Namespace Tags	544
Preset Namespace Tags	544

Appendix F: DCOM Configuration.....	545
DCOM Installation.....	545
Appendix G: Using a Keypad Reader on CK7xx Panels.....	547
Invoking Access Requests from a Keypad	547
To invoke access with a Badge:	547
To invoke access with PIN Only:	547
To invoke access with Card ID:	547
To invoke access with PIN and Card ID:	547
To invoke access using PIN and badge:	548
To invoke access with PIN and badge, allowing PIN after badge:	548
Invoking Air Crew Access Requests from a Keypad	548
To invoke Air Crew access:	548
Invoking Timed Overrides from a Keypad	548
To invoke Timed Override with Badge:.....	548
To invoke Timed Override with PIN Only:.....	548
To invoke Timed Override with Card ID:.....	549
To invoke Timed Override with PIN and Card ID:.....	549
To invoke Timed Override with PIN and Badge:.....	550
To invoke Timed Override with PIN and Badge, allowing PIN after badge:	550
Invoking Panel Card Events from a Keypad.....	551
To invoke Panel Card Events with Badge:	551
To invoke Panel Card Events with PIN Only:	551
To invoke Panel Card Events with Card ID:	551
To invoke Panel Card Events with PIN and Card ID:	552
To invoke Panel Card Events with PIN and Badge:	552
To invoke Panel Card Events with PIN and Badge, allowing PIN after badge:	553
Quick Guide to Using Keypad Readers.....	553
Appendix H: Troubleshooting	557
Authentication Process.....	557
Windows Authentication.....	557
SQL Server Authentication.....	557
P2000 Authentication.....	558
Testing the Workstation	558
Troubleshooting Workstation Problems	558
P2000 Login Troubleshooting.....	559
P2000 Network Troubleshooting	560
CCTV Control Troubleshooting.....	561
Appendix I: Secured Premises Notification Settings	563

Index.....	565
-------------------	------------

PRELIMINARY

Chapter 1: Introduction

The Johnson Controls® P2000 security management system represents the latest technology in integrated security solutions. Built for use on Microsoft® Windows® operating systems, the P2000 software provides a user-friendly interface for easy configuration and operation.

Through its intuitively laid-out menus, users can create cardholder records, define hardware components, and control access through badging, Closed Circuit Television (CCTV), Digital Video Recorder (DVR), 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: *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 off, 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, Permissions, Site Parameters, Local Configuration, Time Zones, Holidays, Panels, Terminals, Input and Output definitions, Elevators/Cabinets, Message Filtering and Routing, Access Groups, and Cardholder 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 cardholders and visitors, 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: Advanced Features.** Describes features that provide a more efficient way to operate and monitor your access control system. 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 feature.
- **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 in order to assure proper CCTV configuration.
- **Appendix G: Using a Keypad Reader on CK7xx 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.

IMPORTANT: Important messages remind you that certain actions, if not performed exactly as stated, may cause damage to equipment or make your system non-operational.



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. Components are shown in two basic configurations: Figure 1-1 displays the P2000 System with Network Panels and Figure 1-2 displays the P2000 System with Serial Panels. For hardware installation of OSI, Isonas, HID, and Assa Abloy panels, refer to the manufacturer's documentation.

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.

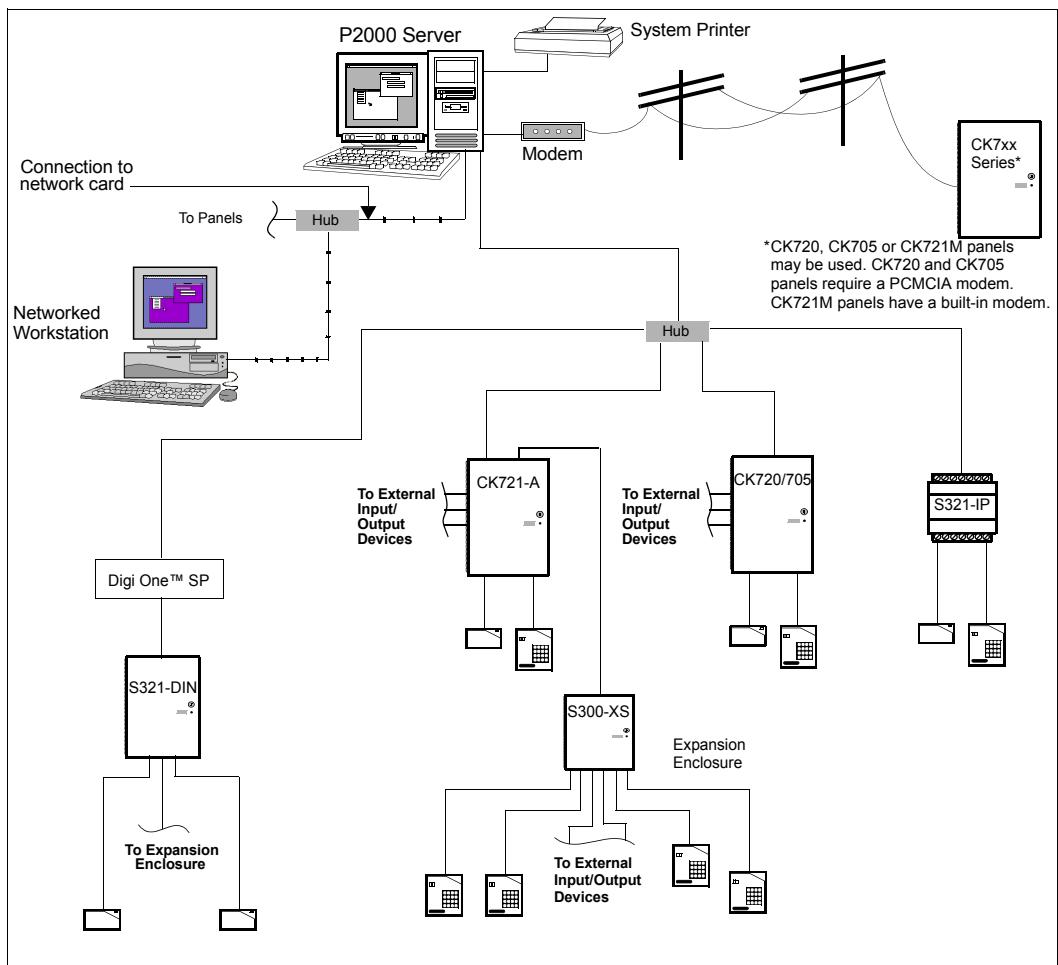


Figure 1-1.P2000 System with Network Panels

IMPORTANT: We recommend the system Server be used only as a Server and not as an additional day-to-day workstation. 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 network (LAN).

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.

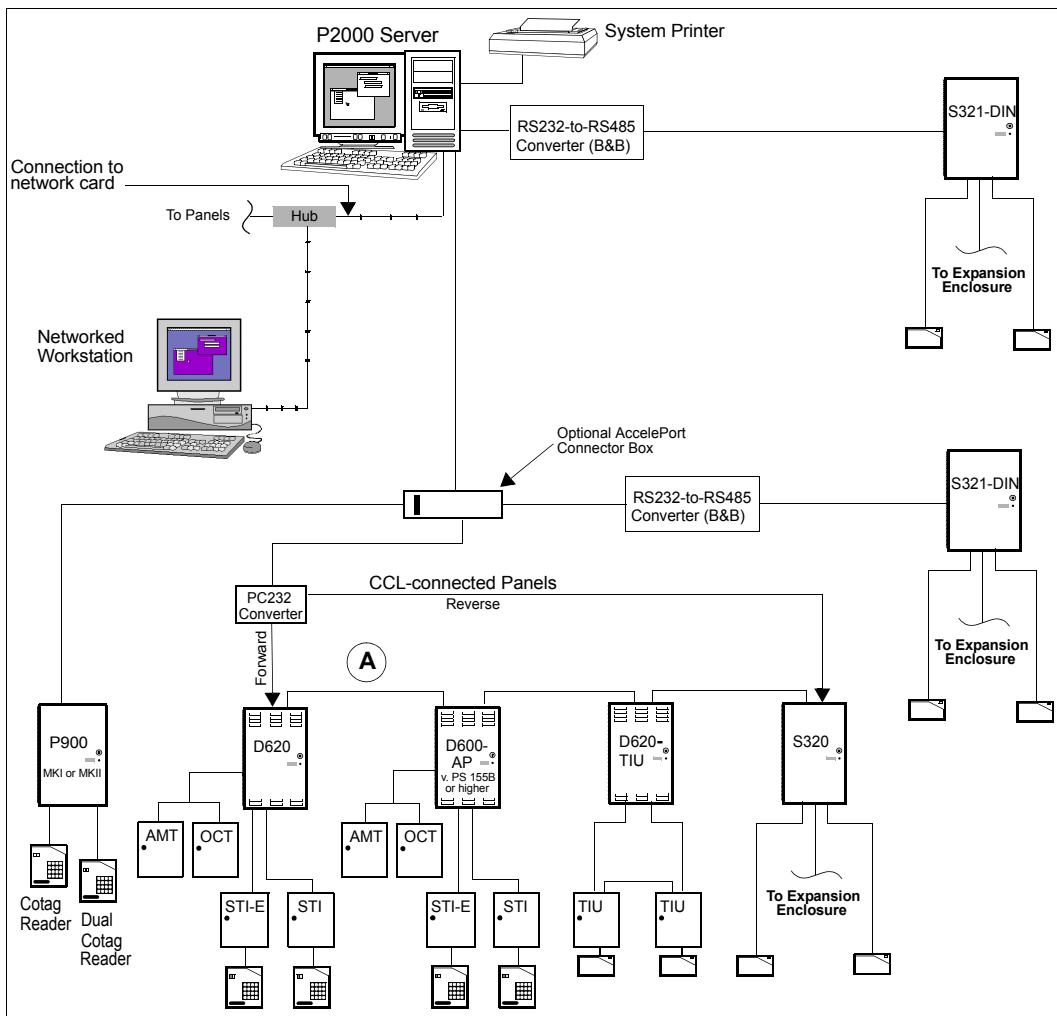


Figure 1-2. P2000 System with Serial Panels

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 CK7xx, S321-IP, OSI, Isonas, HID, and Assa Abloy network panels or S321-DIN, S320, D6xx series (D620, D620-TIU, and D600 AP), and P900 serial panels. These connect to terminals and communicate with the Server. S320 and

D6xx series panels are also called “legacy panels.” See *Appendix C: Panel Comparison Matrix* for a detailed list of features and capabilities.

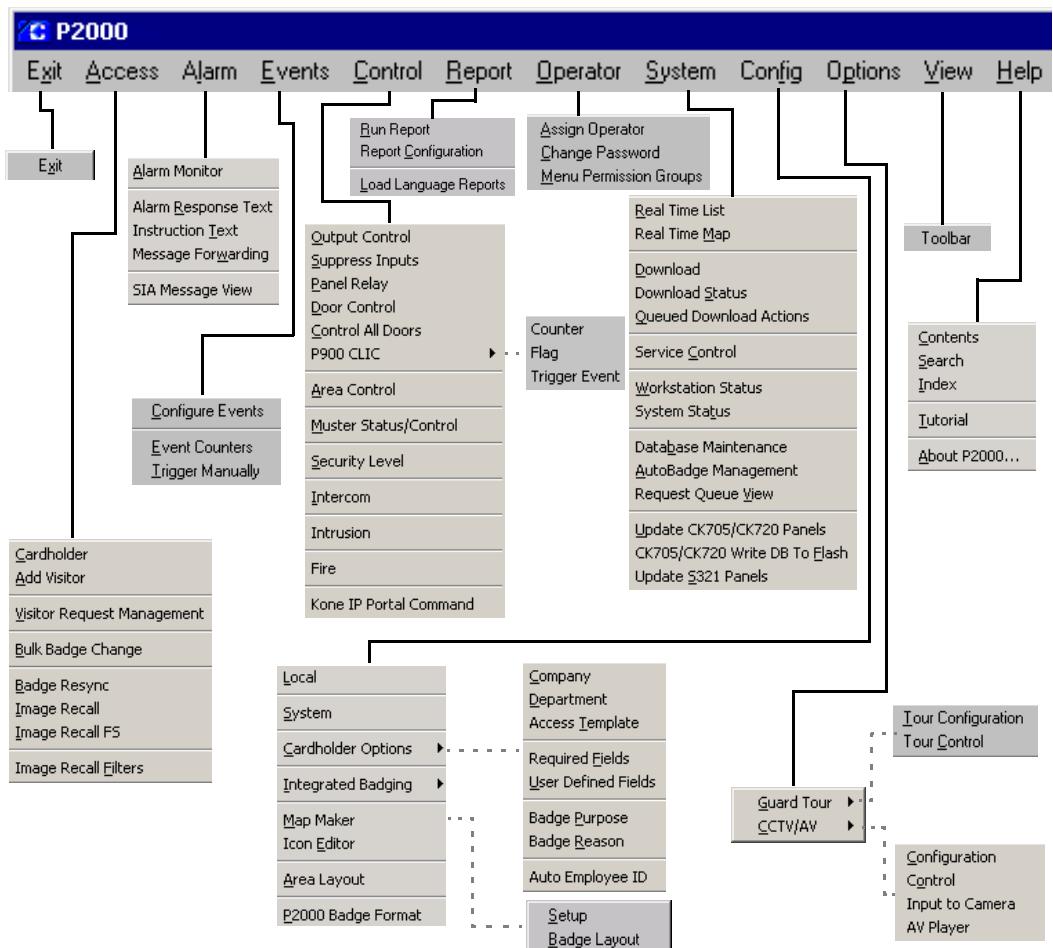
Note: Throughout this manual, the term CK7xx refers to CK705, CK720, CK721, and CK721-A panels.

Terminals – Terminals provide a point of contact with panels to facilitate a variety of functions. Depending on your panel type, some terminal boards can be used to connect readers, input points, and output points and can be mounted in the basic panel enclosure or an expansion enclosure. CK7xx terminals support the following module types: I16, IO8, SI8, SIO8, RDR2, RDR2S, RDR2S-A, and RDR8S. For D620, D620-TIU, and D600 AP panels, terminal hardware boxes, such as an STI/STI-E (Reader, I/O), AMT (Alarm Monitoring), or OCT (Output Control), provide the reader and input point or output point connection.

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.

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.



Registration Parameters

Parameters associated with your system, such as maximum number of badges, terminals, and workstations are enabled via the entry of a Registration Key. Also, if your system will take advantage of advance features such as Enterprise or integrate with third-party hardware such as OSI devices, it will require the entry of Option Keys to control those features (some of these features must be selected during installation). Both the Registration and Option keys are provided by Johnson Controls and are associated with your purchase contract. Refer to the *P2000 Server/Workstation Software Installation* manual for instructions.

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 a cardholder 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 16-reader capability for CK720s and CK721s, and 4-reader capability for CK705s. CK721-A version 3.0 and higher supports 32 readers.

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

You can configure an entire system using CK7xx panels, or use them in combination with S321-DIN, S321-IP, P900, and legacy panels; or use third-party devices such as OSI, Isonas, HID, or Assa Abloy controllers. 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 P900 and legacy panels, using an AccelePort® connector box and a PC232 Converter (legacy only). S321-DIN panels can also connect to the Server via a current loop configuration 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 sixteen legacy panels per loop, up to sixty-four P900 panels per loop, or up to thirty S321-DIN panels per loop. Different panel types cannot be mixed within one loop.

Forward and Reverse – Forward and reverse are terms used to describe the direction the Server *polls*, or communicates with the legacy panels in the loop configuration.

During operation, the Server contacts each panel to determine if the panel has information it needs to send to the Server. Each panel is polled in sequence. Panels may be polled in either forward or reverse direction. Once a polling sequence is begun, each panel is polled until all panels in the loop are polled.

If communication is interrupted on one direction, the Server will poll in the opposite direction to ensure that all panels are polled. All loops in the system are polled simultaneously.

We recommend that legacy panels are installed in a loop configuration to allow the Server to continue communication with all panels should a break in the loop occur. For example, should a break in communication occur at point “A” (see Figure 1-2 on page 4), the P2000 Server will automatically begin polling in the opposite direction in order to reestablish communication with panels on one side of the break or the other. Polling will automatically continue in both directions until the link is repaired as long as the loop configuration is utilized.

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 (through 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. Serial panels take a longer amount of time to download.

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 cardholders access to areas in and around your facility or facilities.

The P2000 system makes access decisions based on:

- Time and Time Zones
- Valid or invalid badges
- Badge privileges

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 a cardholder can be granted access at a reader-controlled door.
- Reader override.

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

Badge Privileges

Badge privileges relate to the time of day, areas, and access groups a cardholder can be granted access. A badge can be valid in all other respects, but the cardholder 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 cardholders special privileges, which is also described as *special access*.

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
- Granting Badge Privileges

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.

Granting Badge Privileges

The other means of providing special access is through badge privileges. Privileges are configured as part of a badge's definition. Badge privileges allow the cardholder 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 activated, 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, Mustering 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 predefined 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: Advanced Features* 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

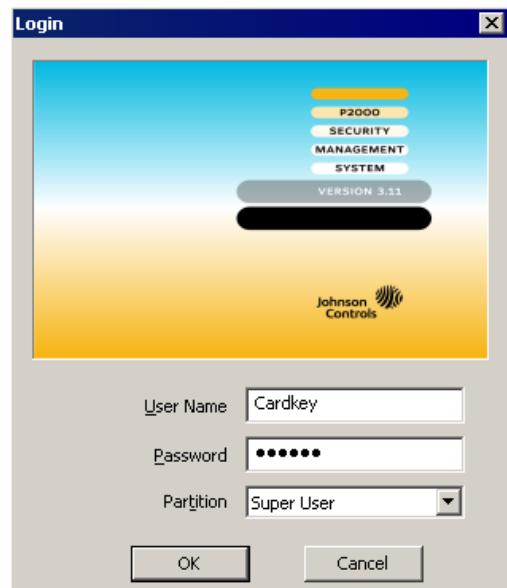
The P2000 system uses a User Name and unique password to establish each authorized user. Passwords are used to protect access within a database or system. A password is a unique combination of alphanumeric characters, such as in a string of letters and/or numbers.

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>P2000**. The P2000 Login window opens.



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 255.

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.

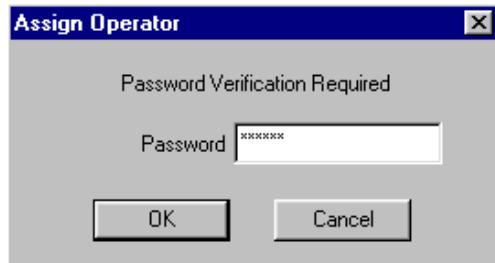
The default account cannot be removed from the system. Instead, use the following steps to change the default login name and password, thereby restricting access to the Super User account.

To Change the Default User Name and Password:

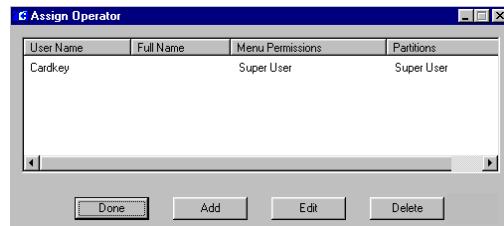
- From the P2000 Main menu, select **Operator>Assign Operator**.



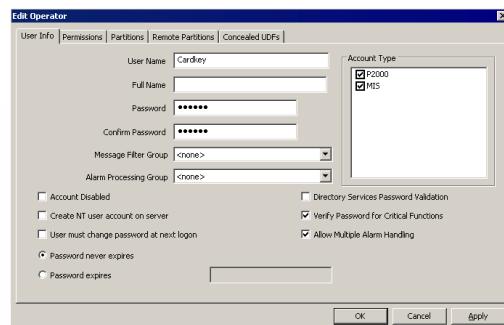
- The password verification dialog box displays. Type **master** and click **OK** or press <Enter> to continue.



- The Assign Operator window displays:



- For new systems, the only User Name will be the default, Cardkey. With Cardkey selected, click **Edit** at the bottom of the Assign Operator window (or double-click “Cardkey” in the list box). The Edit Operator dialog box opens.



- 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 **Confirm Password** field.

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

As an option, you can use the Full Name field. This field is usually the full name of the operator assigned to the User Name. For more details on adding operator information into the P2000 system, see “Adding Operators to the System” on page 23.

- Click **OK** to save your settings.
- Click **Done** to close the window.

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

Logging Off from the P2000 System Software

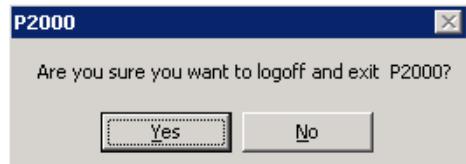
After changing the default User Name and Password, you must log off from the P2000 system; however, this does not require the Server or workstations to be shut down.

To Log Off from 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

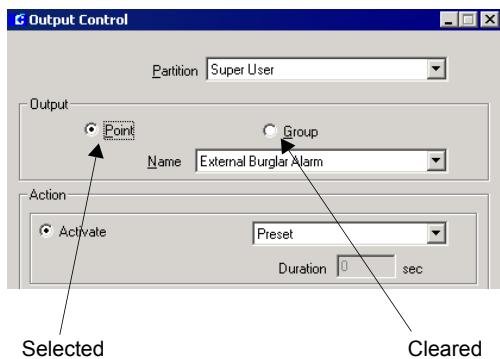
The standard pointing device for the P2000 Server and workstations is a two-button mouse. The left mouse button is the primary mouse button. The following terms are used throughout this manual to describe how you navigate through the P2000 system.

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.

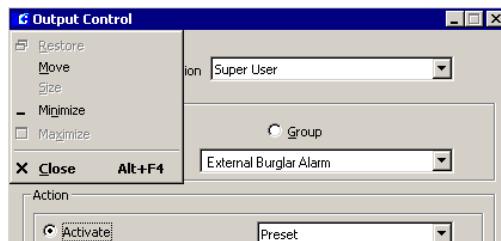
Click and Drag – Press and hold down the left mouse button to select an item, drag and point to where you want to place the object; then release the mouse button.

Basic Window Components

The illustration on page 15 shows a sample P2000 window with key components identified. Some windows may not contain all the components shown in this example.

Each window component is described.

System Menu Button – This button is located at the top of a window in the left corner. Clicking this button displays the following control menu box.



Each window menu item is described in the following paragraphs.

- **Restore** – Restores a minimized or maximized window to its previous size.
- **Move** – Allows the window to be repositioned on the screen. This can only be done by clicking the title bar, holding the mouse button, dragging the window to a new location and releasing the mouse button.
- **Size** – Adjusts the size of a window. This option is available for resizing certain windows only.
- **Minimize** – Changes the window into a button displaying in the Windows taskbar.
- **Maximize** – Expands a window to a full window size.
- **Close** – Exits the current window. This can also be accomplished by double-clicking the System Menu button.

Window Title – The window’s name.

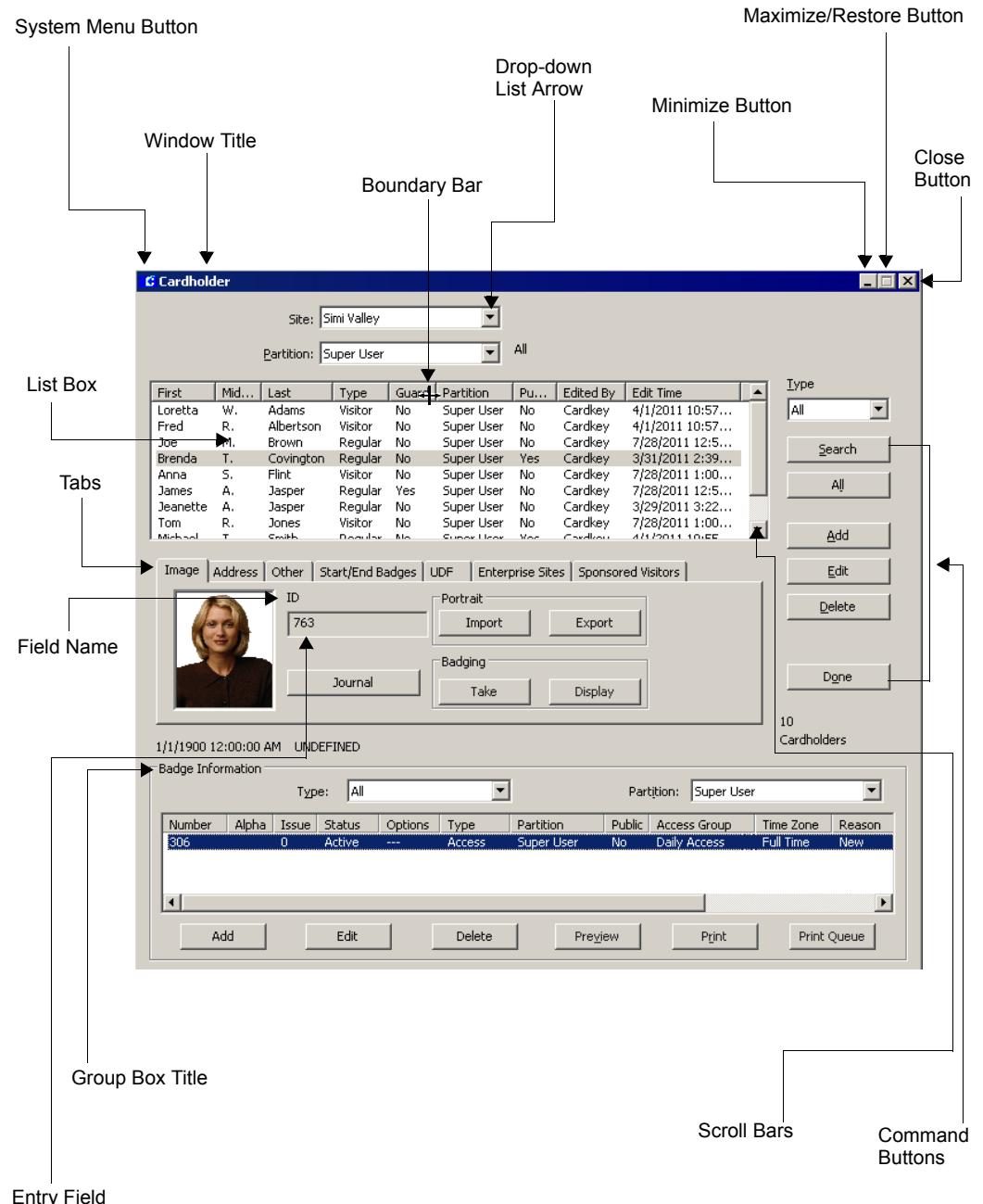
Minimize Button – This button allows you to minimize the window to a button displaying in the Windows taskbar. To restore the window, right-click once on the minimized button and select Restore, or click the minimized button.

Maximize/Restore Button – Expands the size of the window. Clicking this button again restores the window to its previous size. Available in certain windows only.

Boundary Bar – Expands or reduces the size of a column by dragging it until the column is the width you want.

Close Button – Exits the current window.

Drop-down List – Certain P2000 windows contain drop-down lists, which display a list of choices for a given selection. The items that display in drop-down lists vary according to the parameter being defined.



List Box – Contains a list of items you can select. You cannot type a selection on a list box.

Tabs – There are some windows designed with tabs that allow you to configure specific information within a window. To display the contents beneath a tab, click on the tab heading to bring the information forward.

Command Buttons – These buttons appear in almost every P2000 window and are used to perform an action such as Add, Edit, Delete, Cancel, Apply, etc. Note that some buttons are disabled when they appear in windows where their functions do not apply. The most commonly used buttons are described below:

- **Add** – to add a new item.
- **Edit** – to edit the selected item.
- **Delete** – to remove the selected item.
- **Done** – to complete the process and close the window.
- **OK** – to save your changes and exit the current window.
- **Apply** – to save your changes up to that point.
- **Cancel** – to close the window without saving.

If you click **Apply** and then click **Cancel** your settings are saved and the window closes.

If you click **Cancel** without clicking **Apply** your changes are lost and the window closes.

Group Box Title – Various P2000 windows are organized into boxes for clarity. Each box is titled.

Hot Key – Underlined characters within a window identify hot keys, which can be used as shortcuts to each selection. To use a hot key, press **<Alt>** + the underlined character. Available in certain windows and menus only.

Entry Field – Information you enter into the system.

Note: Field entries for all system devices, such as panels, input points, output points, can **only** be alphanumeric. No symbols, quotation marks, slashes, dashes, arrows, semi-colons or colons can be entered in the Entry field.

Field Names – Refers to the descriptive name given to an entry field.

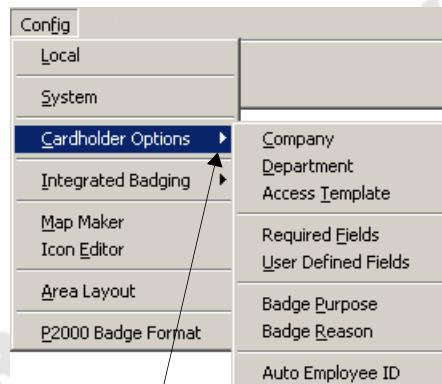
Scroll Bars – If a list box is not large enough to display all the information, a scroll bar displays at the side and/or bottom of the window. You can drag the scroll bar, or click the scroll arrows.

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>Cardholder Options>Company**.

In this example, you would click the **Config** option from the P2000 Main menu bar, then click the **Cardholder Options** menu, and then click the **Company** submenu item to open the **Company** dialog box:



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 Edit Operator dialog box (see page 27), 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.

P2000 Tutorial

The tutorial presents an overview of the P2000 security system's major features and options. It also covers a number of system configuration, installation, and troubleshooting tips. Adobe® Flash is required to run the tutorial and can be installed when you launch the tutorial program from the Help option in the P2000 menu bar.

The modular design enables navigation to all or specific tutorial topics. The tutorial introduces topics and sub-topics, which are discussed through Flash presentations that provide audio narration (with matching text if desired) to guide users on how to make the most of P2000's main popular features. Software screenshots are used to walk the user through actual configuration and installation steps.

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.



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

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 site 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.

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

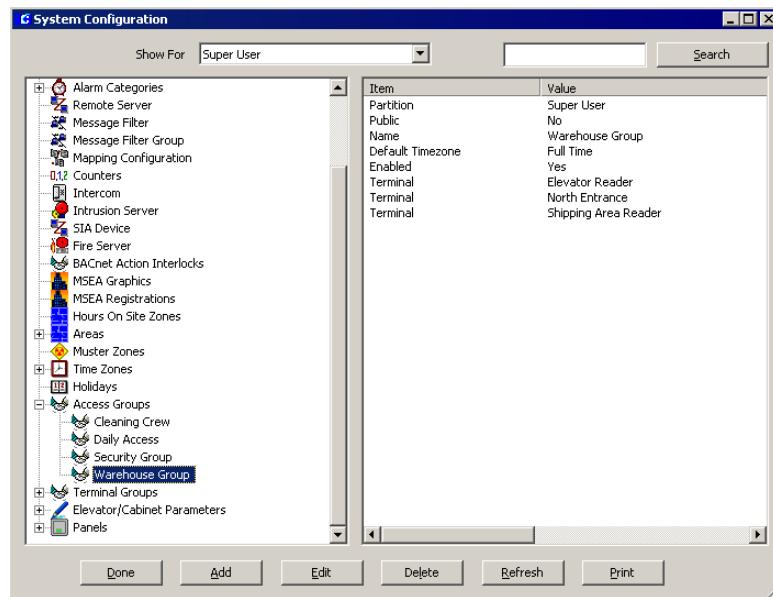
- **Set up Workstations and Operators**
- **Configure System Components**
- **Configure Hardware Components**
- **Configure Elevators and Cabinets**
- **Configure Message Filtering and Message Routing**
- **Set up Access Groups and Cardholders**

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 59 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:

- From the “configuration tree,” click the “root” icon for the item you wish to add.
- 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.



- 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 con-

figuration 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 window-pane.

- 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:

- 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.
- 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 window-pane.

To Search for System Configuration Items:

1. If you wish 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.

To Print System Configuration Items:

1. From the configuration tree, select the item you wish to print. The settings associated with the selected item will be listed on the right windowpane.
2. Click the **Print** button at the bottom of the window.
3. 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.
4. Click **OK** to print.

Set Up Workstations and Operators

Before configuring system and hardware components, Workstations and Operators should be properly set up in order to communicate with the Server. While Workstations are assigned from the System Configuration window, Operators are assigned via the P2000 Main menu. The following sections describe how to:

- **Set up Workstations**
- **Add Operators to the System**
- **Set up User Accounts**

Workstations

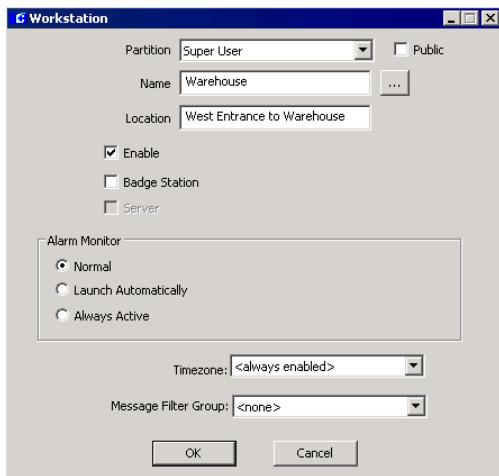
Workstations communicate with the Server via the network. The Server can communicate with a maximum number of Workstations concurrently, based on your registration options. Workstations are assigned a Partition, a name, a Timezone, and designated as Public to make the workstation visible to all partitions. 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 30.

To Add a Workstation:

1. In the System Configuration window, click the plus (+) sign next to the root **Site Parameters** icon to display default system parameters.

2. Click the **Workstation** root icon.
3. Click the **Add** button to access the Workstation dialog box.



4. Enter the information required. (Refer to “Workstation Field Definitions” for detailed information.)
5. Click **OK** to save your entries and return to the System Configuration window. The new Workstation displays beneath the main Workstation icon.
6. 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 you use the Partition feature, select the Partition to which the Workstation will have access. Partitions are described in detail on page 335.

Public – If you use the Partition feature, 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).

Location – Enter the location of the workstation. If you define this as a Badge Station (see page 338), this field describes the location where badges will be issued. You can also enter the name of the local site (see page 53).

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 operator 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. Operators with the appropriate permissions 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 operator. 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 55 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 207 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 Operators to the System

Access to the system is controlled by operators that have been assigned system privileges and characteristics that allow them to perform various system functions. Therefore, operator records must be created for each person who will operate the Server or a workstation in the P2000 system. The operator record consists of the operator's login name, password, menu permissions, and other features that determine how this person will operate. Menu permissions are assigned by group and must be cre-

ated before they will be available to assign to operators.

Creating Permission Groups

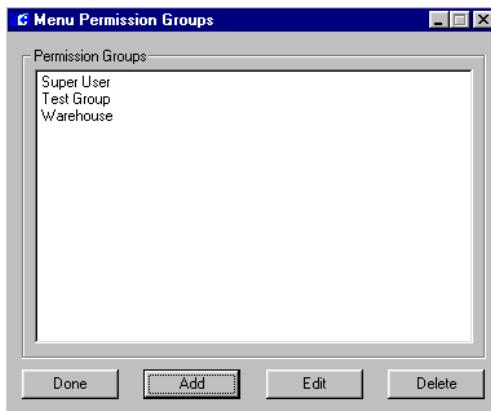
Menu permissions define the system elements to which an operator has access. For example, a guard operating a P2000 workstation at the warehouse gate will need to have access to alarm monitoring, but will not need access to the Cardholder functions. Some operators may need to view system functions, but will not be allowed to edit features, and some operators will need full permissions such as a system administrator or designee.

The P2000 software is delivered with a default operator that can be used to configure the system, and therefore has all menu permissions. You can completely configure the system using only the default operator, or you can create additional groups that include various combinations of permissions depending on the responsibilities and access needs of the individual operators. Once permission groups have been created, they will be accessible from the Assign Operator dialog box. Menu Permission Groups are password protected.

Menu permission groups can also be created for cardholders. These are assigned via the Cardholder Edit dialog box and provide permissions to Web Access functions, refer to “Web Access” on page 409.

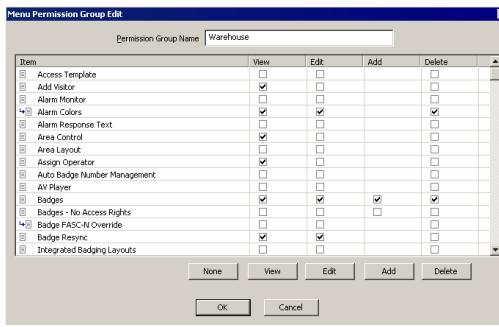
To Create a Permission Group:

1. From the P2000 Main menu, select **Operator>Menu Permission Groups**.
2. Enter your password if prompted. The Menu Permission Groups dialog box opens.



All currently defined menu permission groups will be listed here.

3. Click **Add**. The Menu Permission Group Edit dialog box opens.



4. Enter the **Permission Group Name**. The list box displays menu items preceded by the following icons:

– Menu list icon to indicate items that are accessible from the P2000 Main menu.

– Sub-menu list icon to indicate items that are accessible from the application.

– Tool icon to indicate items that are accessible from the System Configuration or CCTV/AV Configuration window.

– Sub-tool icon to indicate items that are accessible from the application in the System Configuration window.

– Web icon to indicate items that are defined for cardholders who require permissions to Web Access functions, refer to “Web Access” on page 409.

5. Select the check boxes for the items you wish to include in the permission group. Items left blank will not be included in the permission group. Each column provides the following permission levels:

View – The operator can see the element in the system, but cannot edit, add or delete items.

Edit – The operator can view and make changes to entries in these items, but cannot add or delete.

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

Delete – The operator can view, edit, add new, and delete existing items.

6. To assign all items with the same permission level, select the desired function button at the bottom of the screen.
7. To clear your selections, click **None** and reselect the items individually.
8. Click **OK**. The new permission group will be added to the Menu Permission Groups list.
9. Click **Done**. The new permission group will now be accessible from the Available Groups list in the Permissions tab of the Edit Operator dialog box. See “Assigning Operators” for more information.

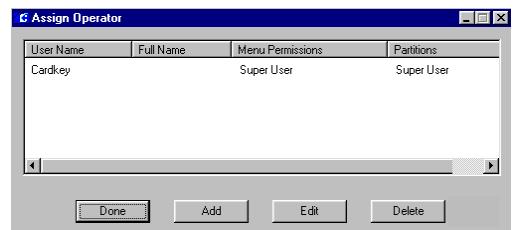
Note: If you delete a permission group, currently logged on operators who belong to that permission group will continue to access items in the permission group until they log out of the system.

Assigning Operators

After initial login, the system is ready for operator configuration. Every operator 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. Use the Assign Operator dialog box to set up user information, including menu permissions, partitions to which the user is assigned, and other system functions.

To Assign an Operator:

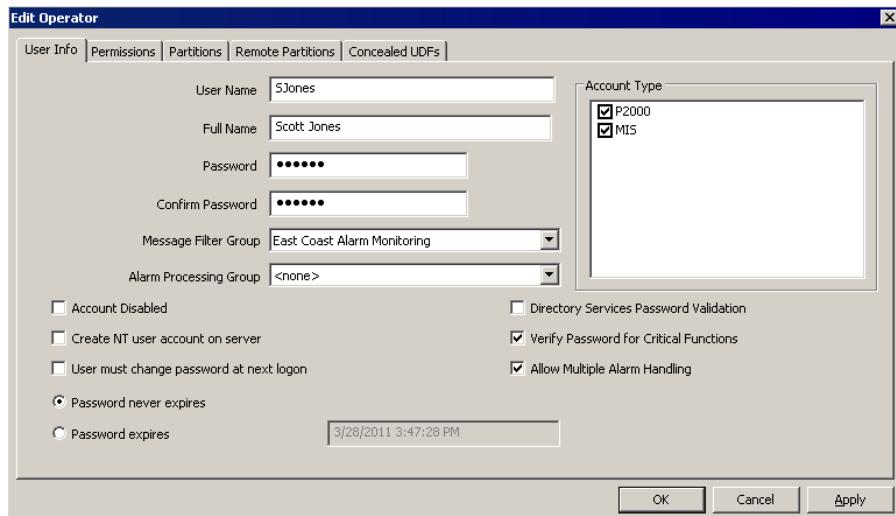
- From the P2000 Main menu, select **Operator>Assign Operator**.
- Enter your password if prompted. The Assign Operator dialog box opens. All operators that have been created in the system are listed along with their user name, full name, menu permissions to which the operator has access, and the partition to which they are assigned.



- To add a new operator, click **Add**. The Edit Operator dialog box opens.
- Enter the information in each tab, as described in the following tab definitions. You can click **Apply** to save your entries.

Note: If FDA Part 11 Record Retention Policy is enabled in Site Parameters, you will not be able to delete operators for the number of years specified in the Retention Period field, see page 46 for details.

- After you enter all the information, click **OK**. The operator will now have access to system elements as defined.
- Click **Done** to close.



User Info Tab

User Name – Enter the name the operator will type when logging on to the system. Although not required, it is recommended that you use the same user name that the operator uses to log on to Windows (passwords can be different).

Full Name – Enter the operator's full name.

Password – Enter the password the operator will type when logging on to the P2000 system. If you wish to change the password at a later time, refer to “Changing the User Password” on page 29. In addition, refer to the “Password Policy Tab” on page 47 for additional password complexity rules.

Confirm Password – Enter the password again to confirm.

Message Filter Group – Select from the drop-down list, the Message Filter Group that defines which messages the operator can see. If you select <none> the operator will be able to see all messages, provided the operator 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 23). Refer to “Configure Message Filtering and Message Routing” on page 207 and to “Operators and Messages” on page 207.

Alarm Processing Group – Select from the drop-down list the Message Filter Group that defines which alarms the operator can process (acknowledge, respond, or complete). If you select <none> the operator will be able to process all alarms that pass the Message Filter Group selection. If an operator 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.*

Account Type – Select the type of account that the operator is authorized to access. If FDA Part 11 Password Policy is enabled in Site Parameters (see page 47), then only one account type can be selected.

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 operator that the account has been disabled.

Create NT user account on server – If this check box is selected, a user account will be automatically added to the operating system on the Server. You must have administrative rights on the P2000 Server to select this option. This check box will not be available for selection if your Server is part of a domain. As an alternative, you can manually add the account using the Windows interface, refer to “Setting Up User Accounts” on page 30.

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. This option is only available if the Account Type selected is **P2000**; a password cannot be changed for MIS or XML RPC users.

Password never expires – 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 47).

Password expires – If you select this option, the password will expire on the displayed date. This date depends on the value defined in Site Parameters (page 47).

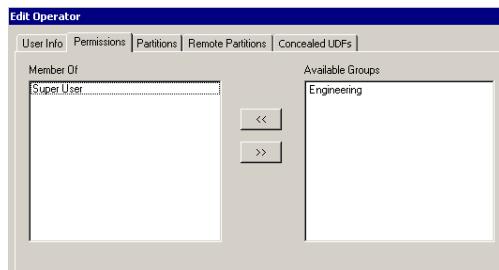
Directory Services Password Validation – When enabled, the password is validated by the network directory services, as defined in the Directory Services Path field, see page 48, and not by P2000. This feature requires Windows Active Directory to be installed and configured on your network. See “P2000 Directory Services Password Validation” on page 29.

Verify Password for Critical Functions – If this option is selected, the operator will be required to enter the login password to access certain system-critical functions.

Allow Multiple Alarm Handling – If you select this option, the operator can process more than one alarm at a time. This option is always enabled by default. When selected, the operator can acknowledge or complete multiple alarms in the Alarm Monitor window.

Permissions Tab

Permissions determine the functions that an operator can perform in the system. Each operator can be associated with different rights to different functions. Menu permissions must be defined otherwise the table will display empty. Refer to “Creating Permission Groups” on page 23 for more information.

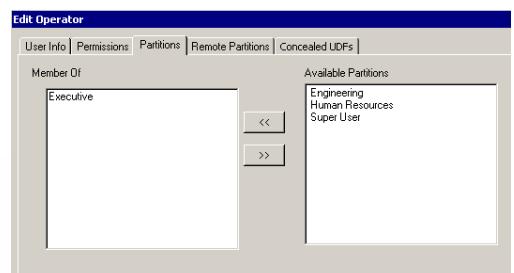


1. Select from the **Available Groups** box, the permission group that defines the functions that the operator can view or change. You can select multiple items by holding down the <Shift> key.
2. Click << to move the permission group from the Available Groups box to the **Member Of** box.

Note: An operator can perform any function if at least one menu permission group assigned to the operator allows permission to that function.

Partitions Tab

Operators 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 335 for more information.



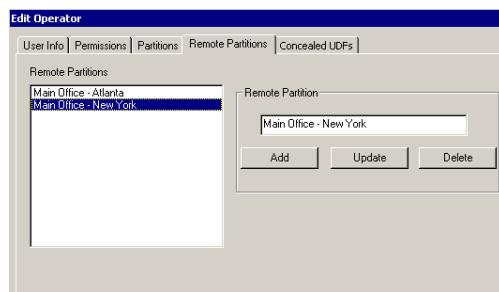
1. Select from the **Available Partitions** box, the partition to which this operator will have access. You can select multiple items by holding down the <Shift> key.
2. Click << to move the partition name from the Available Partitions box to the **Member Of** box.

Note: An operator 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 operator is monitoring the system from the Server, where all alarms and real time messages are visible, regardless of the partitions selected here. Operators that belong to the Super User partition have access to all partitions of the system.

Remote Partitions Tab

If the operator will be monitoring remote messages, use this tab to define the partitions to which the operator will have access. If you do not enter any partition names, the operator can monitor all messages from the remote site.

Note: Remote messages are any alarm or transaction messages originated at another P2000 site. Refer to "Message Filtering" on page 208.

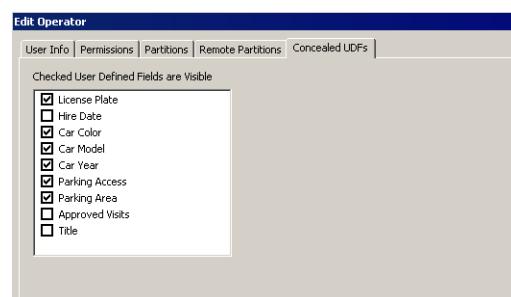


1. Enter the name of the partition at the remote site and click the **Add** button. The remote partition name will display in the Remote Partitions box.
2. If you wish to edit an existing remote partition name, select the name in the Remote Partitions box, make the change, then click the **Update** button.
3. If you wish to delete a remote partition name from the list, select the name in the

Remote Partitions box and click the **Delete** button

Concealed UDFs Tab

Use this tab if you wish to restrict operators from viewing certain fields in the Cardholder dialog box. For example, a guard operating a P2000 workstation at a parking structure will need to have access to car and parking information, but will not need to view personal Cardholder information.



1. All UDFs are enabled by default. Clear the check boxes next to the UDFs that you wish to disable for viewing.
2. Click **OK** to return to the Assign Operator dialog box.

Only the selected UDFs will be visible in the Cardholder dialog box. In addition, other P2000 applications that use UDFs, such as the Search tool, will not display the UDFs that are restricted from viewing.

To Edit an Operator Entry:

1. Select an Operator from the Assign Operator dialog box.
2. Click **Edit**. The Edit Operator dialog box opens.
3. Enter the necessary changes in each tab.
4. Click **OK** to save your changes.

P2000 Directory Services Password Validation

P2000 operator passwords can be authenticated against a directory service such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP). This eliminates operator 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 elements must be set up in the P2000 system:

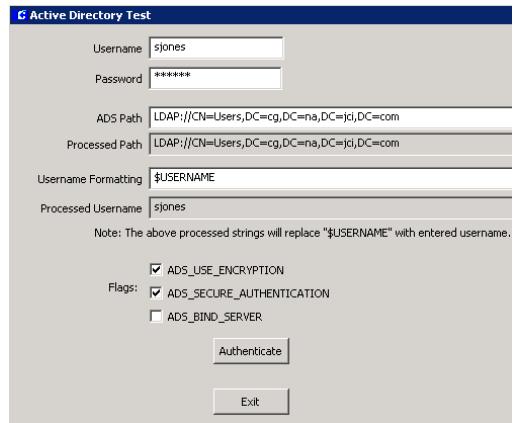
- The **Directory Services Path** field must be set in the Password Policy tab of Site Parameters (see page 48). The actual value to use for the Directory Services Path is unique to your specific network configuration and needs to be obtained from your network administrator.
- For each P2000 operator that you want their password verified by directory services, you need to select the **Directory Services Password Validation** check box in the Edit Operator dialog box (see page 27.) When the Directory Services Password Validation check box is selected, other password related fields are disabled.

Directory Services Path

The Directory Services Path is specific to your network layout and configuration. You must consult with your network administrator for the correct path. The path statement provides the network location for the “Users” object within the directory services hierarchy.

The P2000 software includes a utility that allows you to test the correct path statement.

You can find the **ActiveDirectoryTest.exe** application in the “bin” folder of the P2000 software installation. By using this application, you can easily try different path values to help determine the correct value for your network.



Refer to the following examples:

- Directory Services Path for a Windows domain named **Cardkey**:
WinNT://Cardkey/Users
- Directory Services Path for an Active Directory domain named **cardkey.cg.na.jci.com**:
LDAP://CN=Users,DC=cardkey,DC=cg,DC=na,DC=jci,DC=com

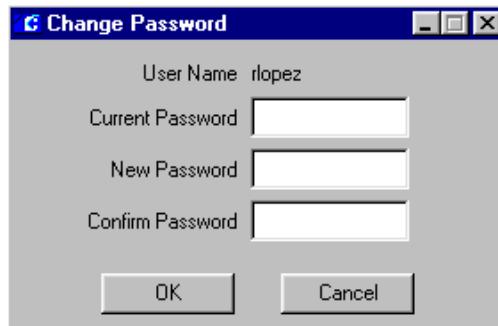
For more details on path values and typical examples, refer to **LDAP ADsPath** and to **WinNT ADsPath** on Microsoft’s MSDN Library.

Changing the User Password

Use the Change Password option to change a user’s password. Depending on the permissions assigned using the Menu Permission Groups, 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 **Operator>Change Password**. The Change Password dialog box 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 operators 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.

Note: If the “Create NT user account on server” option (see page 26) was checked at the time you added the user to the P2000 system, the following steps were performed automatically by the P2000 system.

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

When you add operators 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 operator 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.).

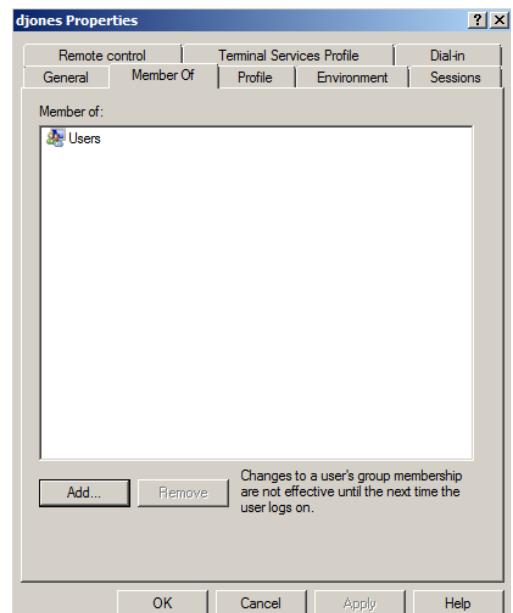
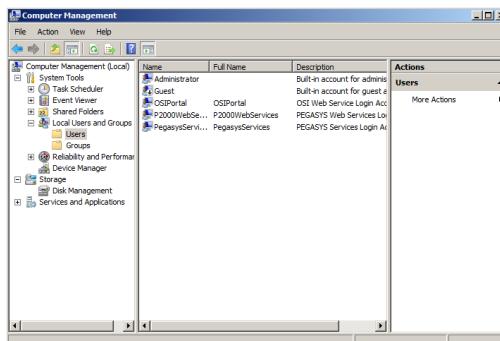
Users – Gives rights to log on to the server computer locally.

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

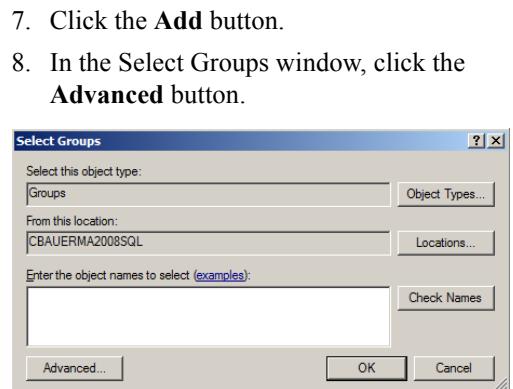
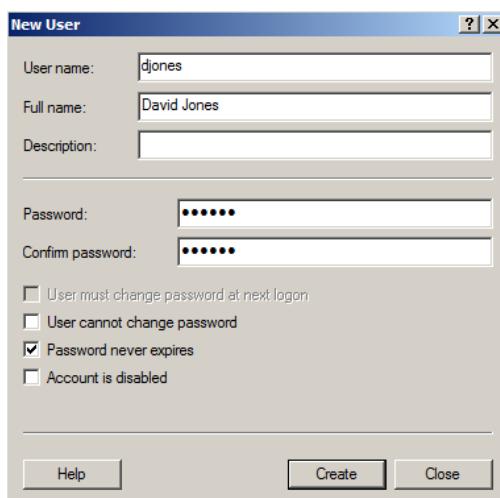
Note: The following instructions are provided for Windows 2008 and Window 2003 Server operating systems. For other operating systems, follow the general outline to enter your settings.

Windows 2008 Server Details

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



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

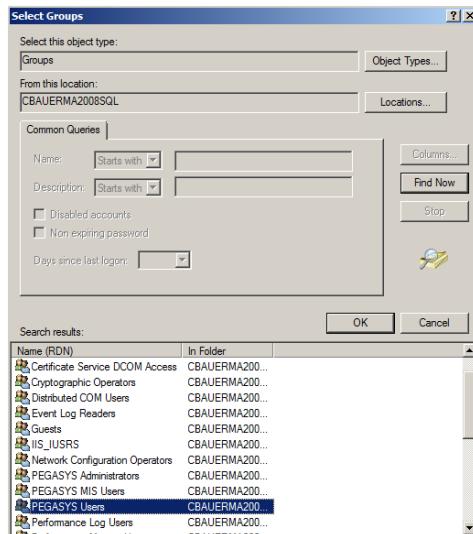


4. Enter the data for the new user, then click the **Create** button. Click **Close** to return to the Computer Management window.
5. Right-click the newly added user on the center pane and select **Properties**.
6. In the user Properties window, click the **Member Of** tab.

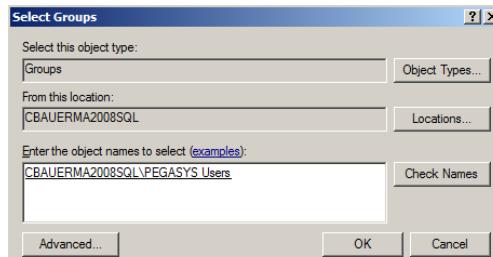
7. Click the **Add** button.
8. In the Select Groups window, click the **Advanced...** button.

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.



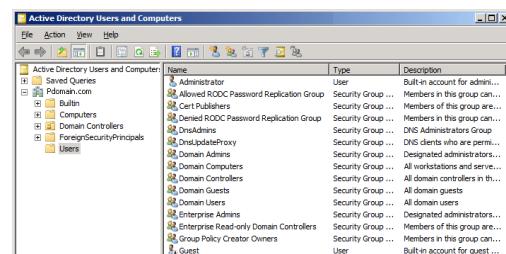
12. Repeat steps 7 - 11 for other groups you want to add, (see page 30 for reference), this time selecting that particular group from the list.
 13. Click OK to close the user Properties window.

Windows 2008 Server with Active Directory Details

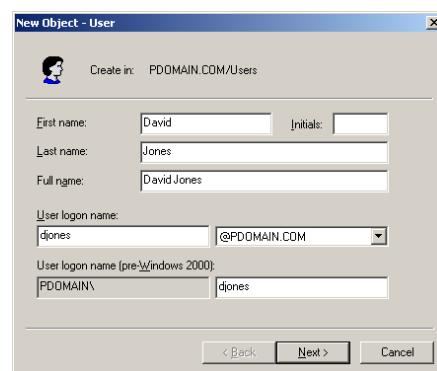
Follow this procedure if you are using Windows 2008 Server or Windows 2008 Server Enterprise Edition and the server is a member of a domain.

1. Run the Computer Management program (select Start>Programs>Administrative

Tools>Active Directory Users and Computers).



2. Expand Active Directory Users and Computers, right-click Users and select New>User.
3. The New Object - 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.



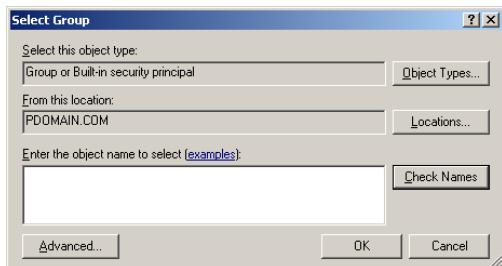
5. Verify the parameters, then click **Finish**.



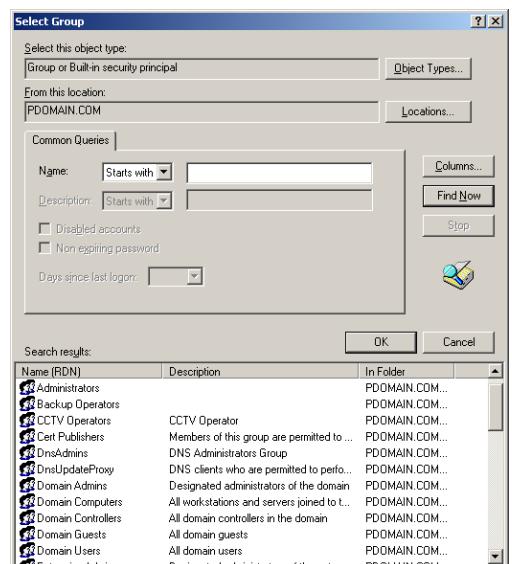
6. To add a member to a user group, from the Active Directory Users and Computers window, select the newly added user on the right pane, right-click and select **Add to a group**.

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

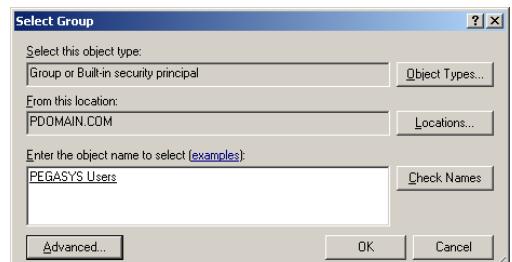
7. In the Select Group window, click the **Advanced** button.



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**.

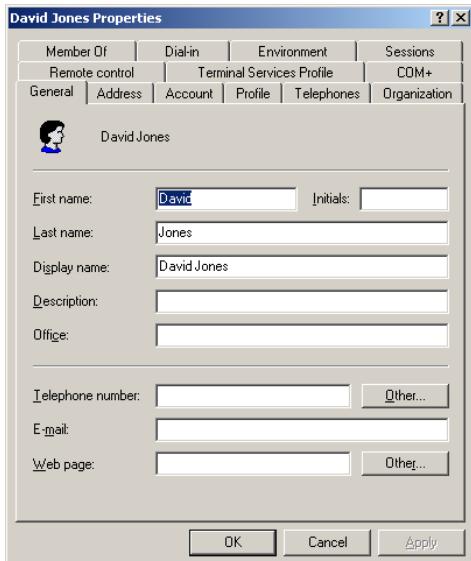


11. Click **OK** at the confirmation message.



12. Repeat steps 6 - 11 for other groups you want to add, (see page 30 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.

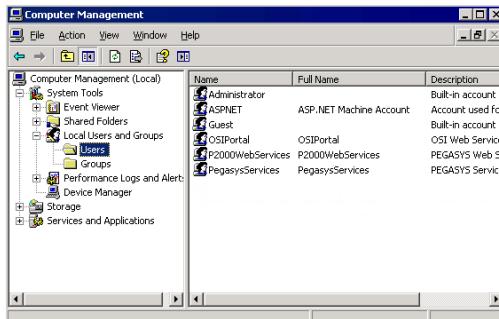


14. Complete each tab according to your needs, then click **OK**.

15. Close all windows.

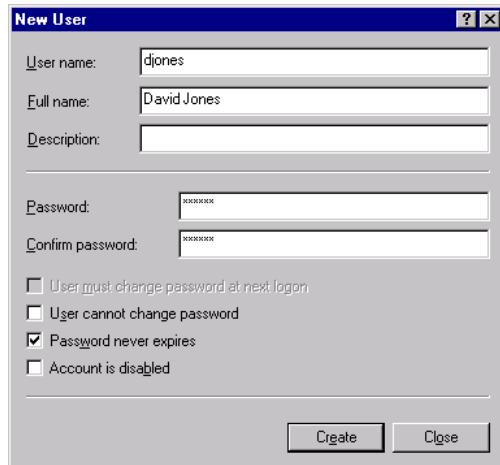
Windows 2003 Server Details

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

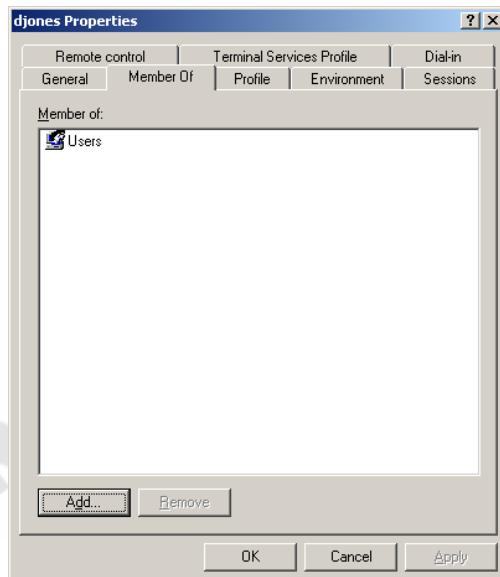


- Click **System Tools>Local Users and Groups>Users**.

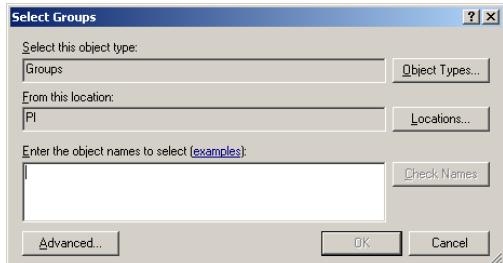
- From the Computer Management menu, select **Action>New User**. The New User dialog box opens.



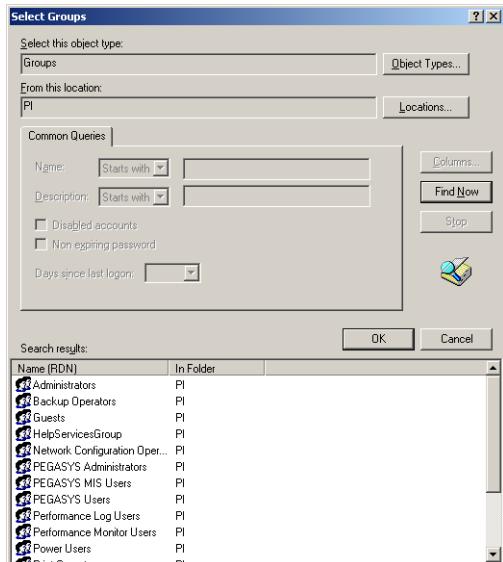
- Enter the data for the new user, then click the **Create** button. Click **Close** to return to the Computer Management window.
- Right-click the newly added user on the right pane and select **Properties**.
- In the user Properties window, click the **Member Of** tab.



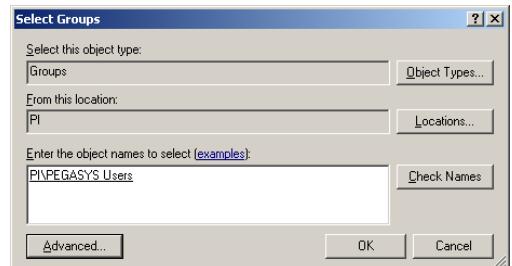
7. Click the **Add** button.
8. In the Select Groups window, click the **Advanced** button.



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**.

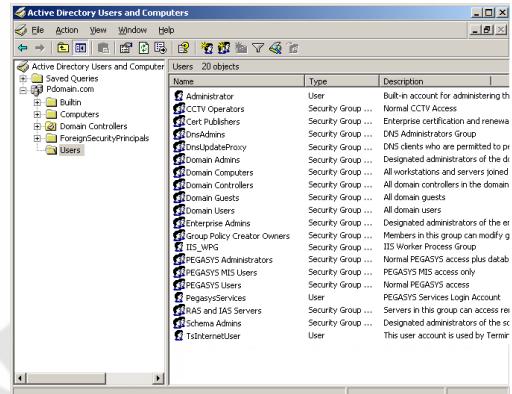


12. Repeat steps 7 - 11 for other groups you want to add, (see page 30 for reference), this time selecting that particular group from the list.
13. Click **OK** to close the user Properties window.

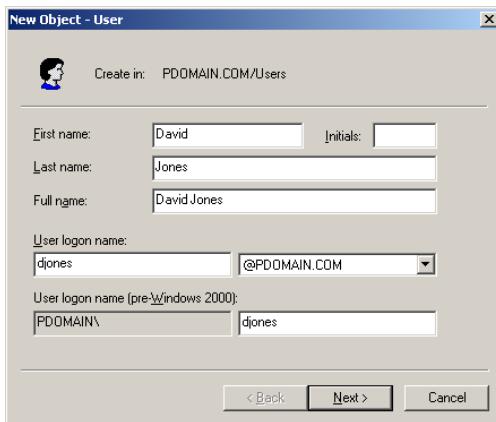
Windows 2003 Server with Active Directory Details

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.

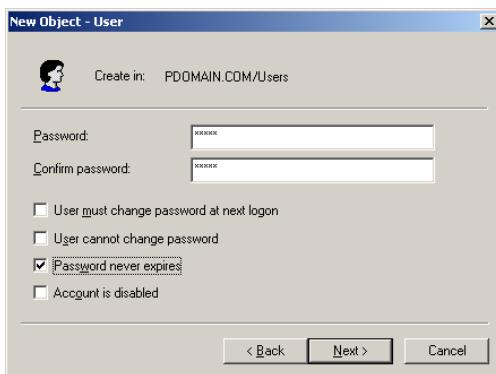
1. Run the Computer Management program (select Start>Programs>Administrative Tools>Active Directory Users and Computers).



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



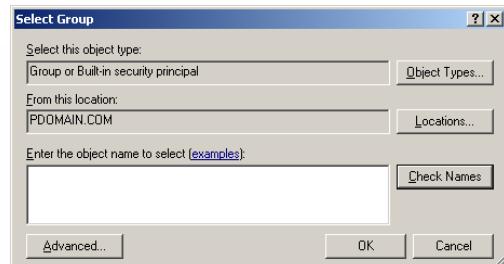
5. Verify the parameters, then click **Finish**.



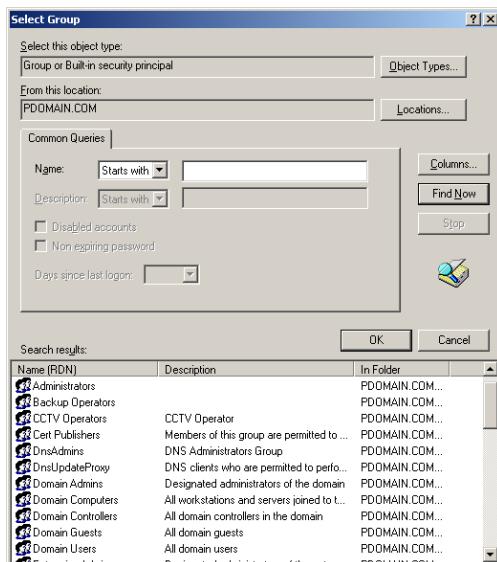
6. To add a member to a user group, from the Active Directory Users and Computers window, select the newly added user on the right pane, right-click and select **Add to a group**.

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

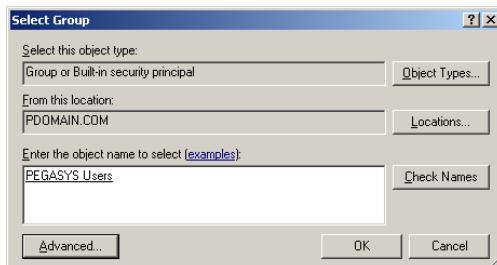
7. In the Select Group window, click the **Advanced** button.



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**.

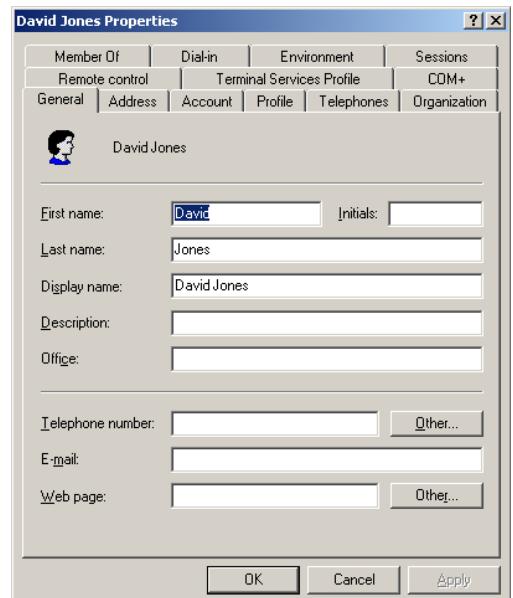


11. Click **OK** at the confirmation message.



12. Repeat steps 6 - 11 for other groups you want to add, (see page 30 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, Local Configuration, 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

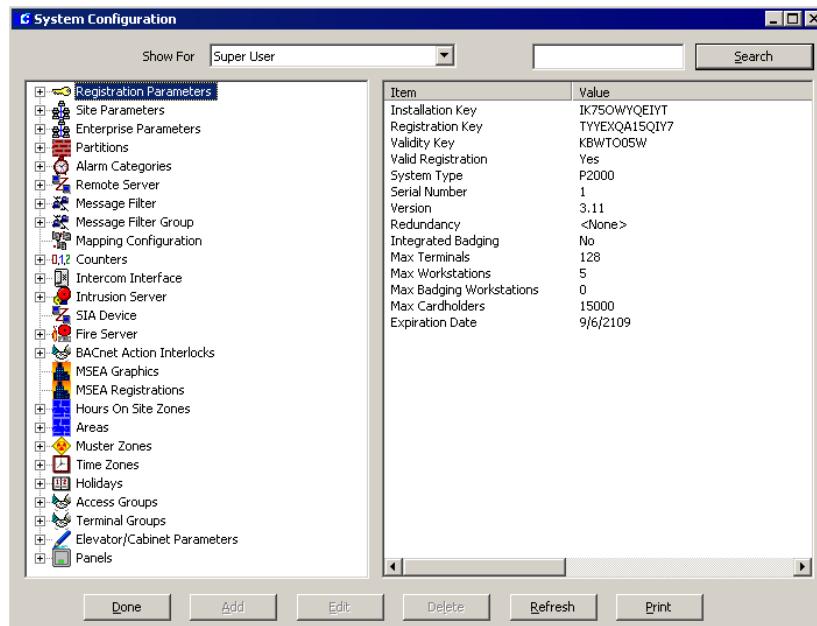
retention times, and other parameters that are specific for the entire facility.

2. **Partitions** – You can divide the P2000 database into smaller sections that can be individually managed. Partitions allow a system to function as multiple, separate systems. For more information on Partitions, see page 335.
3. **Local Configuration** – With Local Configuration, you can enter the database server source and application path of your P2000 system, select the language in which to run your P2000 software, and define the database connection settings for your local computer.
4. **Time Zones** – Times Zones are used throughout the system to define active and inactive time periods for various system components.
5. **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. In addition, you can click the plus (+) sign next to the **Registration Parameters** icon and select the **Option Keys** icon to display additional P2000 features available for your system.

All these parameters are enabled via the entry of your valid Registration Key and Option Keys provided by Johnson Controls. These keys are associated with your purchase contract and cannot be edited within the program.

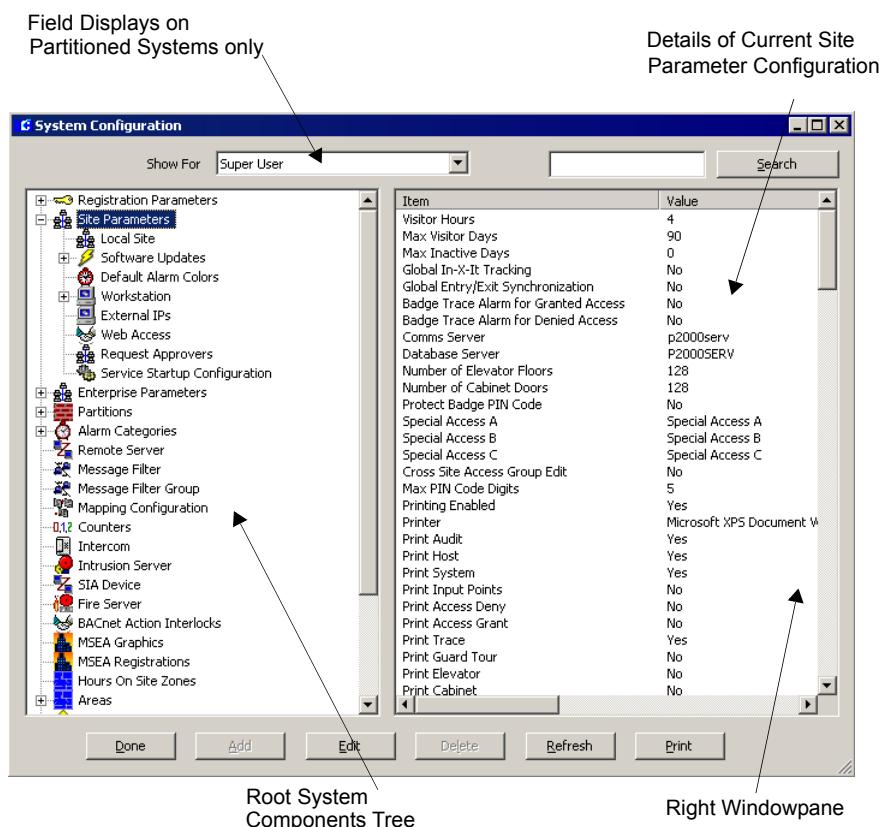


Site Parameters

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 visitor badge validity period, 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. Setup information associated with the BACNet, MIS, and Web Access features is described in *Chapter 4: Advanced Features*.

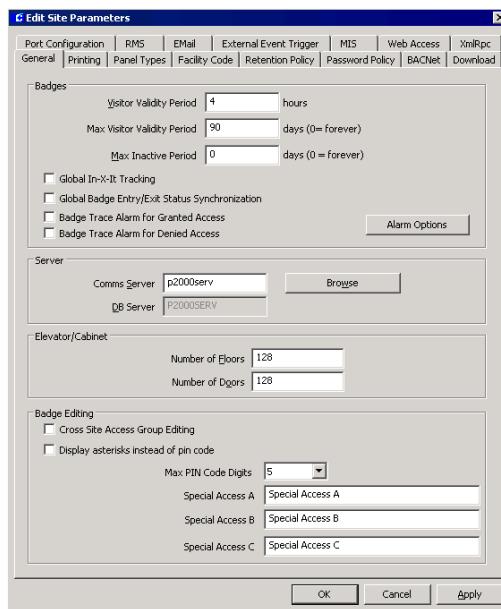
When you click Site Parameters in the System Configuration window, the current settings display on the right windowpane. You may edit these settings as desired. The Backup Device, DB Server, and Real Time Printer in Site Parameters can only be set at the Server. On a partitioned system, only users that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

IMPORTANT: *The Communication and Database Server settings 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

Visitor Validity Period – Enter the time, between 1 and 80 hours, after which a Visitor badge will expire by default.

Max Visitor Validity Period – Enter the maximum number of days that a Visitor badge will be valid. If an operator tries to set the validity period for a Visitor badge longer than the configured value, an error message will display and the badge will not be saved.

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 CK7xx of version 2.5 or higher. After you enable this feature, settings will only take effect after you stop and restart the following services:

- CK720 Download Service
- CK720 Priority Service v1.0 (optional)
- CK720 Priority Service v2.1
- CK720 Upload Service
- P900 SIO Handler Service
- S321 SIO Handler Service
- SIO Handler Service

Refer to “Starting and Stopping Service Control” on page 435 for details.

IMPORTANT: This feature must never be combined with the **Peer to Peer Badge Sync** option selection (see page 68). Selecting both features will cause badge entry/exit enforcement errors across multiple panels.

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, refer to “Alarm Configuration” on page 255.

Comms Server – Defaults to the server that handles communications.

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

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

Cross Site Access Group Editing – Select this check box to allow editing of access groups for other Enterprise sites.

Display asterisks instead of pin code – If selected, the PIN code entered in the Badge dialog box displays as asterisks.

Max PIN Code Digits – Select from the drop-down list the maximum number of PIN code digits that can be entered in the Badge dialog box.

Special Access – The system provides three Special Access flags to satisfy the requirements for assisted access according to ADA

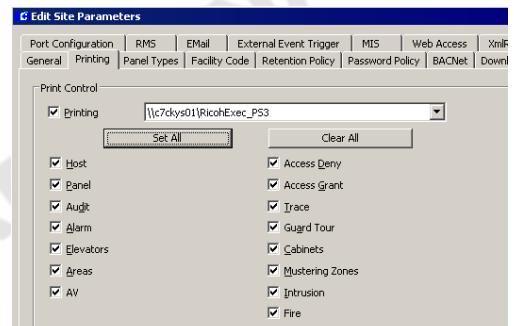
(Americans with Disabilities Act). The Special Access fields A, B, and C can be renamed according to your facility needs, *Handicap Access* for example. The names entered in these fields will become effective throughout the system. For configuring special access for S321-DIN and CK7xx panels, see “Assisted Access Box” on page 85; for OSI panels see “Configure OSI Facility Parameters” on page 129.

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.

IMPORTANT: Real time printing is not guaranteed on foreign language systems.



Printing – If you wish to print any transaction, select this box, and 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 if you wish 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 – Prints all audio-visual messages. DVR is described on page 394.

Access Deny – Prints all Access Deny messages.

Access Grant – Prints all Access Grant messages.

Trace – Prints all transactions associated with a badge. The Trace option must also be enabled on the Badge dialog box, see page 241.

Guard Tour – Prints all guard tour messages. Guard Tour is described in detail on page 352.

Cabinets – Prints all cabinet messages.

Mustering Zones – Prints all mustering zone messages.

Intrusion – Prints all intrusion messages.

Fire – Prints messages generated by the fire alarm panel.

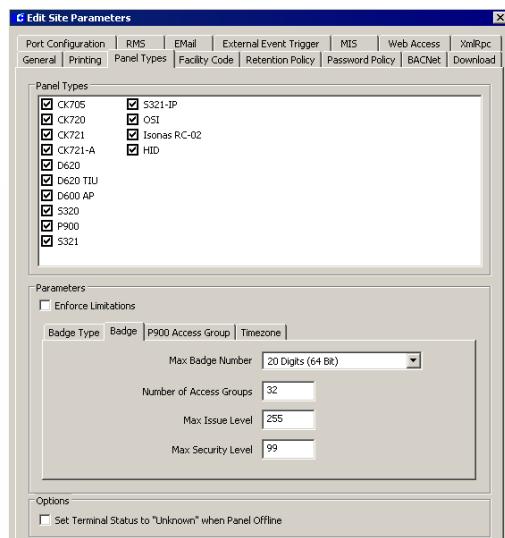
As a reference, see “Using the Real Time List” on page 322.

Panel Types Tab

Use this tab to select the panel types and related parameters that define how your system will be configured.

Panel Types Box

Select the panel types to be used at your facility. Specific features for the selected panel type will display when configuring the panels and their system and hardware components. For example if you only select the D620 panel type, features for a CK7xx panel such as Elevator and Cabinet in the Access Group dialog box will not display. Your system can be configured with any combination of panel types.



Parameters Box

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

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. For example, if you select CK720 and D620 as the panel types, you will only be able to configure up to 2 access groups and up to 7 issue levels, even though CK720 panels support 8 access groups and 255 issue levels.

- **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. For example, if you select CK720 and D620 as the panel types and you enter 8 in the Number of Access Groups, you will be able to download up to 8 access groups for CK720 panels, and only up to 2 access groups for D620 panels.

Parameters	Elements	CK7xx	Legacy	P900	S321-DIN	S321-IP	OSI	Isonas	HID	Assa Abloy
		CK705/CK720 CK721 CK721-A	D620 D620 TIU D600 AP/S320							
Badge	Max Badge Number	20 Digits	65,535	20 Digits	32 bit ¹	20 Digits	47 bit ²	32 bit ³	64 bit ⁴	19 Digits ⁷
	Number of Access Groups	8 ⁵	2	1	2	2	N/A	1	8	32
	Max Issue Level	255	7	7	7	N/A	99	255	N/A	255
	Max Security Level	99 (2.2 and higher)	99 (D600 AP only)	N/A	99	99 (2.6 and higher)	N/A	N/A	N/A	N/A
Timezone	Number of time pairs per day	4 ⁶	4	10	4	4	20	10	6	10
	Number of unique time pairs per Timezone	40	40	16	40	40	N/A	80	60	32 ⁸

1 Max Badge Number for S321-DIN and Isonas panels is 4,294,967,295

2 Max Badge Number for OSI panels is 140,737,488,355,327

3 Max Badge Format digits is 32 bits

4 Max Badge Format digits is 64 bits

5 CK721-A version 3.0 supports 32 access groups per badge

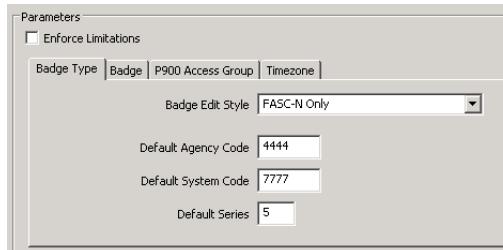
6 CK721-A version 3.0 supports 10 time pairs per timezone

7 19 digits for Mag Stripe, 48 bits for others

8 Each Assa Abloy lock can only store a maximum of 32 different time periods.

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 Only** – Select Normal if your facility uses any badge type other than FASC-N.
- **FASC-N Only** – 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 default values defined in this tab.
- **Normal and FASC-N** – Use this option if your facility uses both Normal and FASC-N badges.

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.

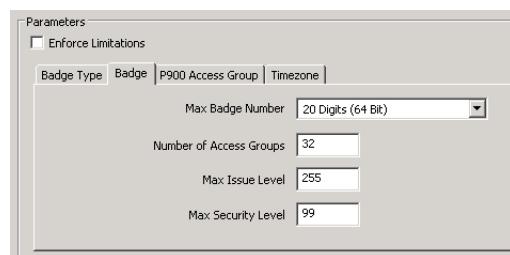
Default Series – Enter a 1-digit default series number to be used at your facility.

For more information, refer to “FASC-N Badges” on page 239.

Badge Tab

Settings entered in this tab govern how badges will be configured for the entire system. When you create a badge, the system uses this infor-

mation to determine the maximum allowed values. For more information, refer to “Badge Field Definitions” on page 238.



Max Badge Number – Select from the drop-down list the maximum number of characters allowed to be entered in the badge Number field. See the table on page 43 for the maximum default values for each panel type.

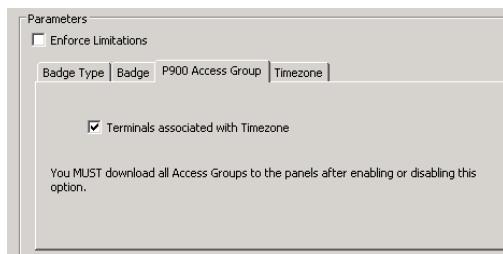
Number of Access Groups – Enter the maximum number of access groups that can be assigned to each badge. This is the number of access groups that will display in the Access Rights tab of the Badge dialog box. See the table on page 43 for the maximum default values for each panel type.

Max Issue Level – Enter the highest issue level that can be assigned to a badge. The maximum value will display in the Issue drop-down list of the Badge dialog box. See the table on page 43 for the maximum default values for each panel type.

Max Security Level – Enter the highest security level that can be assigned to a badge. This is the maximum number that will display in the Security Options tab of the Badge dialog box. Security levels are supported by D600 AP panels, S321-DIN panels, S321-IP panels (version 2.6 and higher), and CK7xx panels version 2.2 and higher. Refer to “Security Level” on page 70 (for D600 AP only), and “Security Threat Level Control” on page 277.

P900 Access Group Tab

This tab applies to P900 panels only.

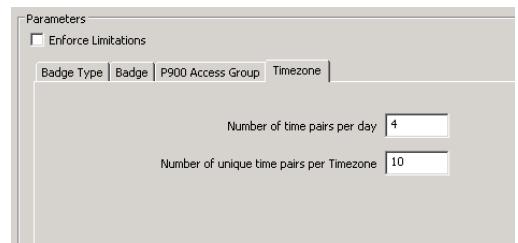


Terminals associated with Timezone – If you select this option, you will activate the *Details* tab in the Access Group dialog box, which will enable you to assign different time zones to each P900 terminal. For more information, see “Create Access Groups” on page 218.

Timezone Tab

Use the Timezone tab to enter the maximum number of time pairs per day and the maximum number of unique time pairs per time

zone that will be allowed for the entire system. A *time pair* is defined as a period of the day, with a starting and ending time. See “Time Zones” on page 55 for configuration instructions. To have a better understanding of how the *time pairs* work, refer to the illustration below.



Number of time pairs per day – Enter the maximum number of time pairs per day that can be configured for the entire system. The number of time pairs per day will be displayed in the Time Zone dialog box (see the illustration below). See the table on page 43 for the maximum default values for each panel type.

Assume you selected the CK720 panel type.

CK720 allows:

4 time pairs per day

40 unique time pairs per Timezone

Assume you selected the P900 panel type.

P900 allows:

10 time pairs per day

16 unique time pairs per Timezone

Assume you enable Enforce Limitations

NOTE: According to the Enforce Limitation rules (see page 43), the system uses the lowest values among the panel types selected. In this case **4 pairs per day** and **16 unique time pairs per Timezone**.

Using the above values, the Time Zone dialog box will display 4 time pairs for each day...

Periods		12:00:00 AM		6:00:00 AM		12:00:00 PM		1:00:00 PM		6:00:00 PM		10:00:00 PM		11:00:00 PM		11:59:00 PM	
Monday	Inactive																
Tuesday	Inactive																
Wednesday	Inactive																
Thursday	Inactive																
Friday	Inactive																
Saturday	Inactive																
Sunday	Inactive																
Holiday 1	Inactive																
Holiday 2	Inactive																
Holiday 3	Inactive																

... and allow you to configure up to 16 unique time pairs for the entire Time Zone.

Number of unique time pairs per Timezone –
Enter the maximum number of unique time pairs that can be created for each Time Zone. See the table on page 43 for the maximum default values for each panel type.

Options Box

Set Terminal Status to “Unknown” when Panel Offline – Select this option to set a terminal status to “Unknown” when a panel goes offline. For Assa Abloy panels, this setting becomes effective after the Assa Abloy DSR Interface Service is restarted.

Facility Code Tab

Some of the codes stored in every badge are known as *facility codes*. These codes are provided by Johnson Controls and allow you to identify the badges that belong to your facility. Refer to the instructions provided on page 237 to assign facility codes to badges.

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

You can define up to eight facility codes. 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 use 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. The maximum retention period is 24,855 days (about 68 years).

Audit Trail	30	Days
Transactions	30	Days
Alarms	30	Days
Master Data	30	Days
Request Queue	30	Days
Tour Note	30	Days

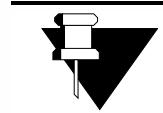
FDA Retention Policy
 Enforce FDA Title 21 CFR Part 11 Record Retention and Validation Policy

Retention Period (years): 10
Violation Alert Period (days): 30
Last FDA Backup: 1/23/2009

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 badge 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 459.

Tour Note – If your facility uses the Guard Tour feature, enter the time after which all notes will be deleted from the system. Refer to “Guard Tour Notes” on page 365.

FDA Retention Policy

Settings in this box are available if your facility uses the FDA Part 11 option. Refer to “FDA Part 11” on page 395.

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 455.

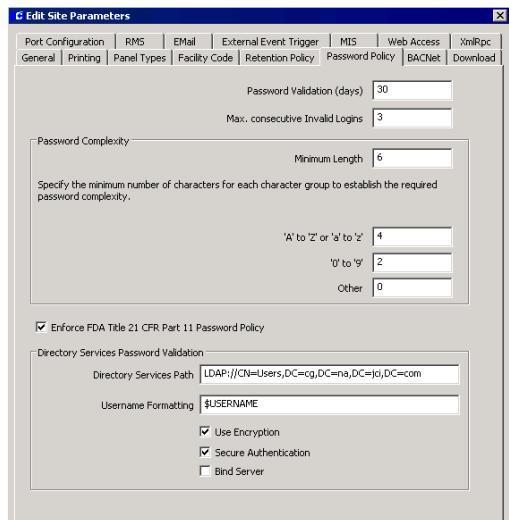
Last FDA Backup – This is a displayed field only and shows the date you informed the system that a backup was archived, according to your company policies to comply with FDA Part 11 record retention requirements.

IMPORTANT: 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 453.

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 indefi-

nately. 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 – If you wish 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 uses the FDA Part 11 feature. Select this box to enable FDA Part 11 password policy. For more information, see “FDA Part 11” on page 395.

IMPORTANT: 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

Directory Services Path – This is the Lightweight Directory Access Protocol (LDAP) path for the directory server. This setting is specific to the network; contact your network administrator for assistance. Refer to “P2000 Directory Services Password Validation” on page 29 for more information.

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.

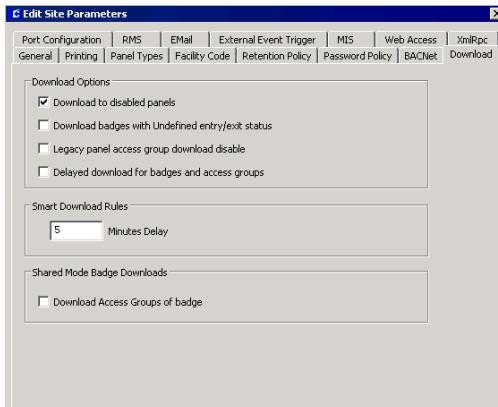
Use Encryption – Forces the connection to the Directory Services to use data encryption for network communications. Not recommended for Windows Active Directory. May be requested by your Directory Services administrator.

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 if you wish 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 429.*

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 badges to the panel when access groups are changed.

Delayed download for badges and access groups – If you select this option, badge and access group downloads to panels will be performed using Smart Download instead of per-

forming the download immediately. This moves the burden of building the download from the workstation to the server, in addition to delaying the download by the number of minutes set in the Smart Download Rules box. This option only effects downloads caused by editing badges, access groups, or terminal groups. This option does not apply to badge and access group downloads performed using the Download application. Refer to “Smart Download Control” on page 431.

Smart Download Rules – This option defines the time for downloading badges to panels when changes are made to access groups and terminal groups, as well as defines the time for downloading cardholder and badge changes. The download will start automatically whenever the system does not process any access groups, terminal groups, cardholder or badge 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 435.

Port Configuration Tab

Use the Port Configuration tab if you wish 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.



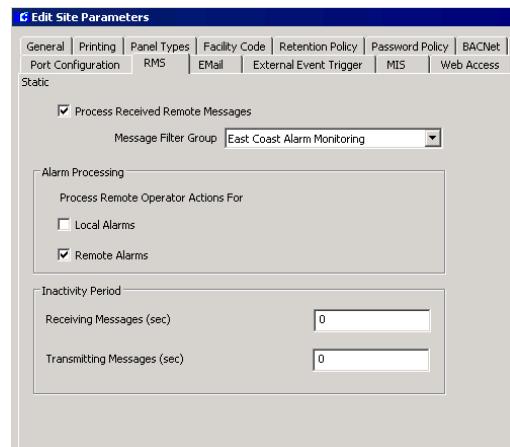
The CK720 Priority Port, CK720 Upload Port, and CK720 Download Port values (firmware version 2.2 and higher) **must** match the values configured at the panel, and **must** use TCP/IP port numbers above 41000. CK720 panels version 1.0 do not allow Priority and Download Port changes. See the following recommended port values:

	CK7xx 2.1 or lower	CK7xx 2.2 or higher
CK720 v2.1 Priority Port	10201	N/A
CK720 v.2.2 Priority Port	N/A	41012
CK720 v1.0 Upload Port	1199	N/A
CK720 v2.2 Upload Port	N/A	41013
CK720 v2.2 Download Port	N/A	41014

If the mix of panel versions in the P2000 system does not need a particular port, set the value to 0 to disable that port. If the P2000 system contains only CK7xx panels that are version 2.1 and higher, disable the CK720 Priority Service v1.0 using the Service Startup Configuration application, see page 432.

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.



Process Received Remote Messages – Select this check box if you wish 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 RTLRoute 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 “Configure Message Filtering and Message Routing” on page 207 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 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. See “Configuring P2000 Remote Servers” on page 216.

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 Username 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.

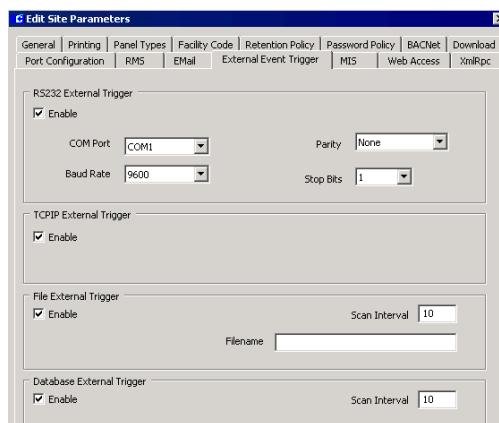
Username – Enter the name to be used to establish the dial-up connection.

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.

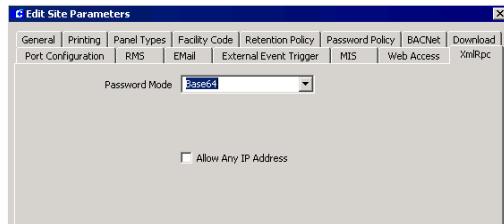
File External Trigger – If you select **Enable**, the P2000 system will periodically check the configured location to look for the existence of the configured file name. When the specified file is found it will be renamed to <original name>.BAK. After it has been renamed, the lines in the file will be 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 395.*

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.
- **Ignore** – Password parameter is not validated.

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 IP address(es) defined in the External IPs dialog box, see page 346 for details.

Local Site

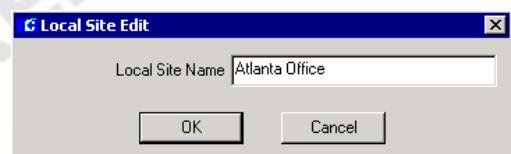
The P2000 Local Site name is assigned during the initial software installation and uniquely identifies the P2000 site within the P2000 Enterprise System.

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 plus (+) sign next to the root **Site Parameters** icon to display default system parameters.
2. Click the **Local Site** root icon.
3. Click the **Edit** button to open the Local Site Edit dialog box.

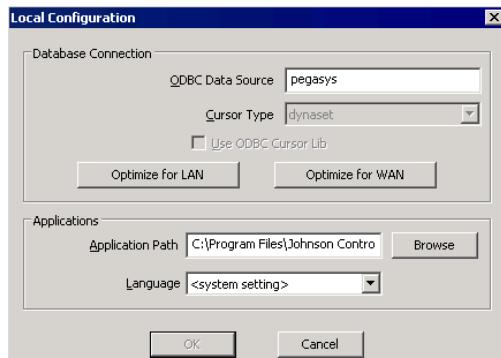


4. Enter a **Local Site Name** (up to 32 characters) that will easily identify your P2000 site.
5. Click **OK** to save the Local Site Name.
6. A message displays, warning that changing the site name requires you to update existing database records that refer to the current site name. Click **Yes** if you want to proceed to change the name.
7. You will be prompted to stop all P2000 services at the Server, refer to “Starting and Stopping Service Control” on page 435, and to log out of all workstations.
8. Click **OK** to proceed with the update of the database tables.
9. 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. Click one of the following buttons to change the database connection settings for the local computer:

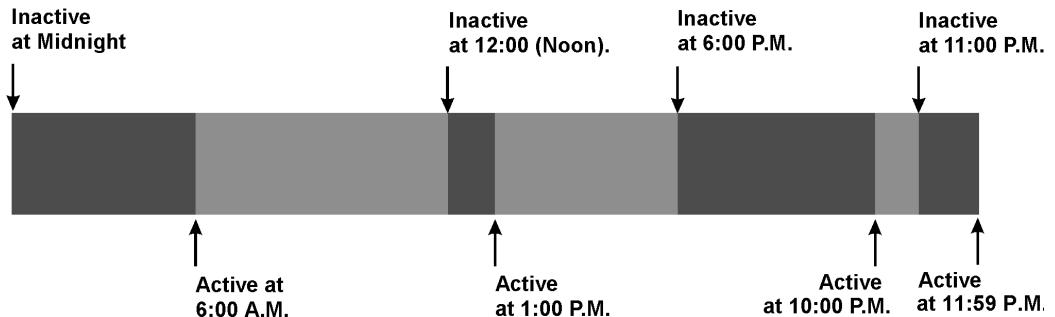
Optimize for LAN – To set the database connection settings to values that are appropriate to a Local Area Network (LAN).

Optimize for WAN – To set the database connection settings to values that are appropriate to a Wide Area Network (WAN) or any other type of connection to the P2000 database server with reduced bandwidth and/or high latency times.

4. The **Application Path** field displays the location of the P2000 program. Click **Browse** to find another path, if the location has changed.
5. 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.

6. 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, badge, 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.

You can define an unlimited number of time zones, but you must assign at least one time zone to each panel. This could be done at the time you create the panels or later. See “Configure Panel Time Zones” on page 72.

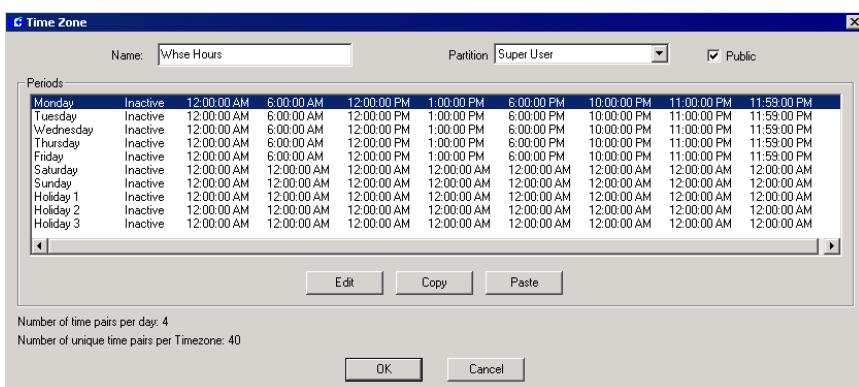
After you configure your time zones, click the plus (+) sign next to the Time Zones icon to display all configured time zones. When you click on a Time Zones icon in the System Configuration window, the values for the time

zone items display on the right windowpane. See *Appendix C: Panel Comparison Matrix* for the maximum number of time zones supported by each panel type.

Configuring Time Blocks

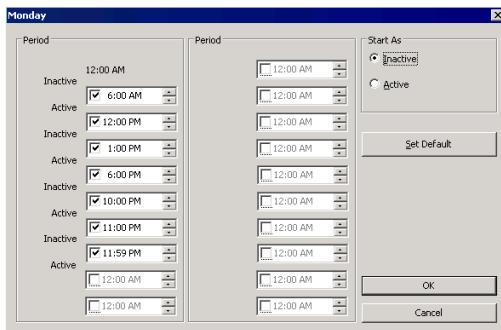
The period between an active and inactive time may be thought of as a time block. Some panel types allow up to four time pairs (four active and four inactive times); therefore, you can configure up to eight time blocks per day for those panels. Refer to the table on page 43 for the number of time pairs per day allowed for each panel type.

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 displaying the maximum number of time pairs, as defined in Site Parameters, see “Timezone Tab” on page 45.
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. The number of time periods available depends on the parameters selected in Site Parameters.



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.

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, if needed.

Note: The number of Active and Inactive times is limited to the “number of time pairs per day” defined in Site Parameters. 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**. If you wish 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 72.

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, cardholders, 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

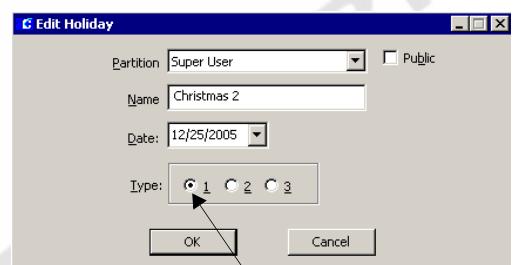
Use the Holiday window to define dates when the system will use Holiday 1, 2, or 3 active and inactive periods rather than the usual time zones set for those days of the week. When the system reaches midnight prior to a day defined as a Holiday, it switches to Active and Inactive periods, depending on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

You can define an unlimited number of holidays.

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.



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. Click **OK** to save the new Holiday. If you wish to add this Holiday to all panels, click **Yes**. Otherwise, you must add the new Holiday for each panel separately using the Panel Holiday application, see page 73.

Note: If you select to add the new Holiday to all panels, the system may display a message indicating that the number of panel holidays has exceeded (or there are duplicate dates in P900 Panel Holidays) for the panel names that display in the list box.

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 Month:

Do one of the following:

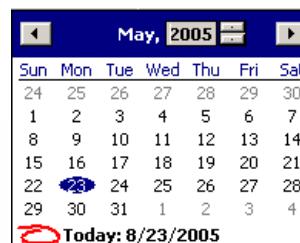
1. Use the left or right arrows in the Calendar header to move forward or backward through the months. You can also press Page Up or Page Down to move through the months, or
2. Click the name of the month in the Calendar header and choose a month from the list.



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.



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 55 for more information on creating Holiday types.)

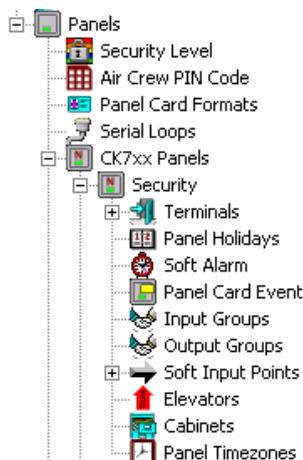
Configure Hardware Components

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.

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. Some panels (CK7xx, S321-DIN, S321-IP, OSI, Isonas, HID, and Assa Abloy), communicate with the Server via network connections.

Other panels (legacy, S321-DIN, and P900), communicate with the Server via a serial connection using loop configurations. You must set up loop configurations before creating these panels, see "Loop Configuration" on page 60.

Note: S321-DIN panels can be installed in a network or serial configuration.

Refer to the *P2000 Server Installation Manual* for instructions on connecting the Server to the panels. Also, for hardware installation and specification information, refer to the documentation that was shipped with your panel.

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.

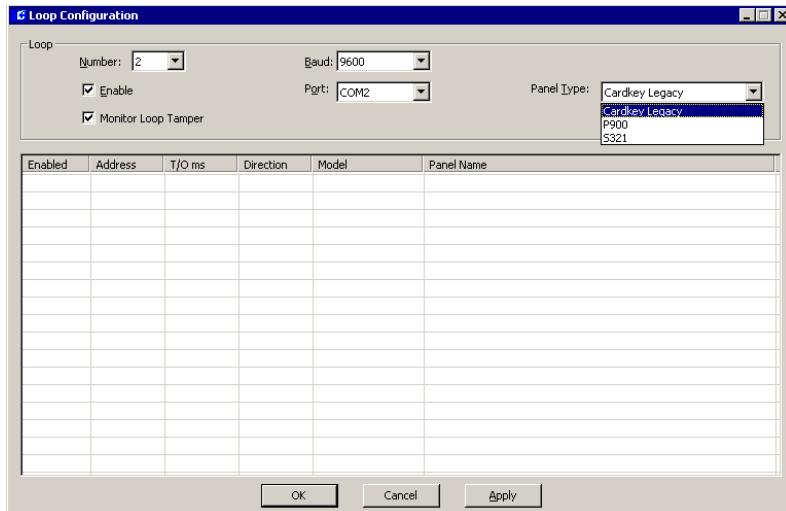
Loop Configuration

The P2000 Server uses loop configurations to communicate with legacy, S321-DIN, and P900 panels. The system supports up to 32 loops, with up to 16 legacy panels per loop, up to thirty S321-DIN panels per loop, and up to sixty-four P900 panels per loop. For more information, see “Loop Communication” on page 7. New loops can only be created at the Server.

To Set Up Loop Configurations:

1. From the System Configuration window, click the plus (+) sign next to the root **Panels** icon.

2. Select the root **Serial Loops** 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. If you wish 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 whether this loop will be used by Cardkey Legacy, P900, or S321 panels.
8. If this loop is used by Cardkey Legacy panels, enable the **Monitor Loop Tamper** check box to allow panels to monitor loop tamper alarms. This is the required option for UL listed sites, where all alarms must always be visible to meet UL requirements. Clear the check box if you wish to disable monitoring.



9. 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 (D620, S320, P900, S321, etc.), address, timeout setting, and loop direction (forward or reverse, for legacy only). 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.

Panel Configuration

Prior to configuring the panels that will control your security system, you must identify the type of panel installed at your facility and follow the pertained instructions.

The following sections describe procedures to configure CK7xx, S321-DIN, and Legacy panels and related components.

The steps to configure other panel types differ from the procedures described here. If you plan to configure P900, OSI, S321-IP, Isonas, or HID panels, you must skip the remaining sections and proceed to one of the following sections:

- ***Configure P900 Panels and Components*** on page 109.
- ***Configure OSI Panels and Components*** on page 127.
- ***Configure S321-IP Panels and Components*** on page 141.
- ***Configure Isonas Panels and Components*** on page 154.
- ***Configure HID Panels and Components*** on page 160.
- ***Configure Assa Abloy IP Door Locks and Components*** on page 172

Also, refer to *Appendix C: Panel Comparison Matrix* to see the features supported by each panel type.

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:
 - CK7xx Panels** – To configure CK705, CK720, CK721, and CK721-A panels.
 - S321 Panels** – To configure S321-DIN panels.
 - S321-IP Panels** – To configure S321-IP panels, go to page 141 for details.
 - Legacy Panels** – To configure D620, D620-TIU, D600 AP, and S320 panels.
 - Isonas Panels** – To configure Isonas panels, go to page 154 for details.
 - HID Network Panels** – To configure HID panels, go to page 160 for details.
 - OSI Panels** – To configure OSI panels, go to page 127 for details.
 - P900 Panels** – To configure P900 panels, go to page 109 for details.
 - Assa Abloy Panels** – To configure Assa Abloy panels, go to page 172 for details.
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 72.
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 display.

Note: For CK7xx panel software versions 1.1 and later, the panel version number will display on the right windowpane of the System Configuration window, after that panel establishes communication with the Server.

Soft Input Points

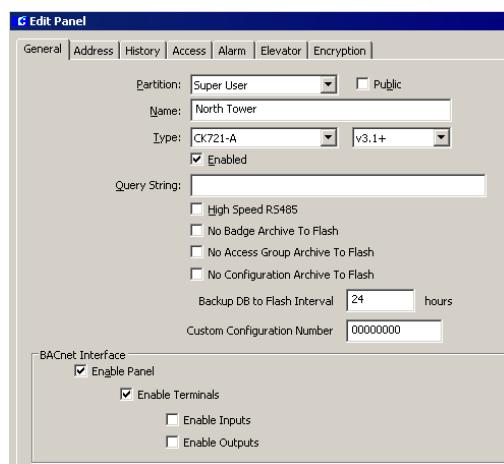
When a panel is created in the system, a Panel Down soft input point is automatically created for input point 25 and displays under the Soft Input Point icon as “Panel Down <panel name>.” If enabled in the Input Point dialog box, this input point will report to the Alarm Queue and Real Time List. If 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 96 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 and corresponding firmware version from the drop-down lists.

- **If you select a CKxx panel type,** the Address and Elevator tabs are available.
- **If you select a legacy or S321 panel type,** the Loop/Unit, Misc, and Mag Format tabs are available.

Note: Certain features will be enabled/disabled depending on the panel type and version selected. The version selected will be validated when the panel connects. CK7xx panels (version 2.1 and higher) that do not match will be put into a misconfigured state and will not be allowed to fully communicate until the problem is resolved.

Enabled – The system will not recognize the panel unless the **Enabled** check box is selected. If you wish 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 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

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.

Backup DB to Flash Interval – Available for CK721-A panels version 2.10 and higher. Enter the time interval (in hours) to schedule automatic backup of the panel database to flash memory. The default backup period is once every 24 hours. A backup period of 0 hours disables automatic database backups to flash memory. This feature is to be used in conjunction with the Write DB to Flash feature, see page 446 for details.

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 – These settings are available after you select the *Enable BACnet Interface* check box in Site Parameters, see page 345. 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

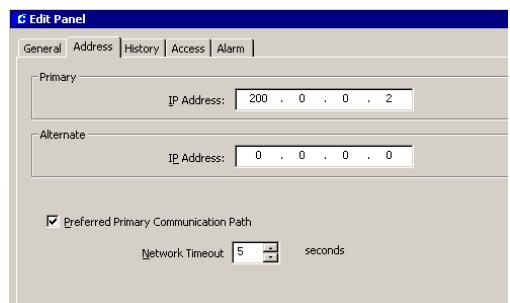
objects should not exceed 7200. Keep the number of BACnet objects reasonably low; otherwise, system performance can be adversely affected. Refer to the *P2000 Metasys® Integration Manual* for details.

Address Tab

Use this tab when configuring CK7xx panels. The information on this tab varies depending on the panel version selected. In general, 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.

Address Tab for Panel Versions 1.1 to 2.0



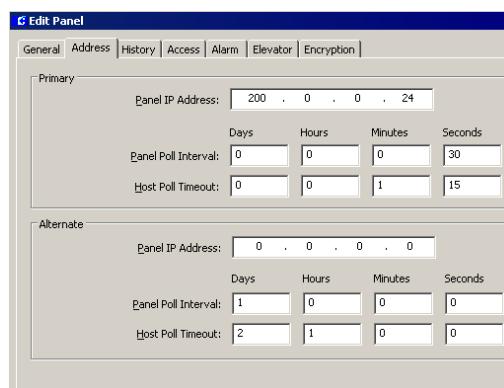
Primary IP Address – Enter the IP Address. This entry must match the IP address at the panel.

Alternate IP Address – Leave this field empty unless your panel has a second network connection.

Preferred Primary Communication Path – Select the check box to indicate that this will be the primary communication path between the panel and the Server.

Network Timeout – Some installations may require more time to complete communication between the Server and the panel. You can increase the time in seconds before a time out will occur between the P2000 Server and the panel. This value must match the panel local user interface; otherwise communication problems will exist.

Address Tab for Panel Versions 2.1 and Higher



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 CK705/CK720 panels (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.

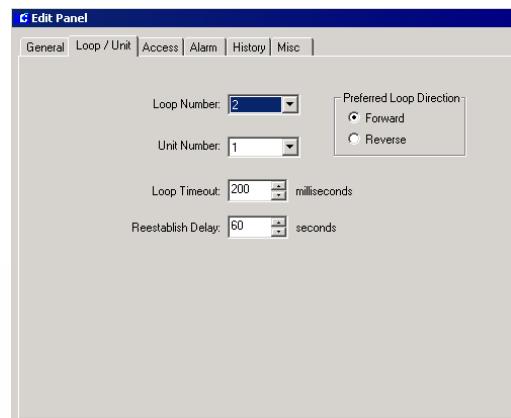
Alternate Panel IP Address – For panels with two network connections, enter the IP address of the alternate connection. This entry should be from a different subnet address and must match the IP address at the panel.

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 serial panels only.



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 sixteen legacy panels per loop and thirty S321-DIN 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.

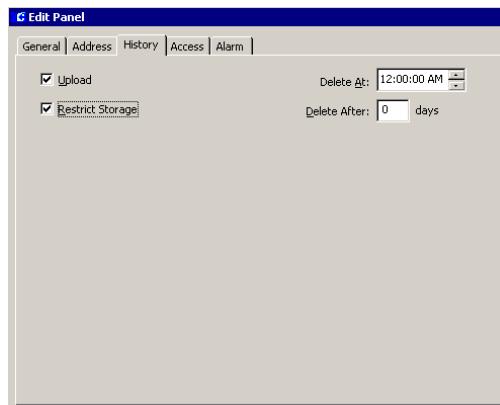
Reestablish Delay – Select the time from the spin box (5 to 32000 seconds) after which the panel will try to reestablish communication.

Preferred Loop Direction – Select the direction (**Forward** or **Reverse**) the Server will communicate with the panel in the loop configuration. Available for legacy panels only.

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.

History Tab for Serial and CK7xx (Versions 1.1 to 2.0) Panels



Upload – Enable Upload to constantly upload panel transactions directly to the Server in real time.

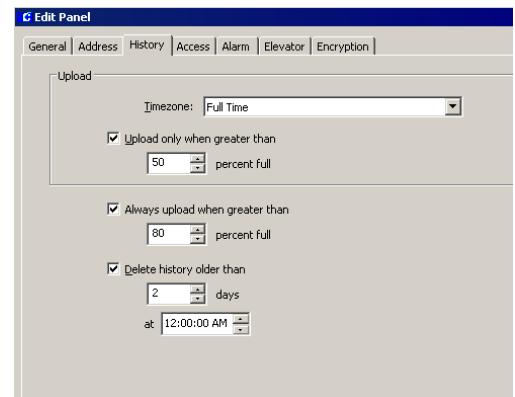
Restrict Storage – Enable Restrict Storage to limit the amount of data held at the panel. If Restrict Storage is enabled, you must also select a time at which data will be deleted, and

the number of days to hold data before deletion. This option is not available for TIU panels.

Delete At – Select a time from the drop-down list.

Delete After – Enter the number of days you wish the panel to hold data before deletion.

History Tab for CK7xx Panels Versions 2.1 and Higher



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

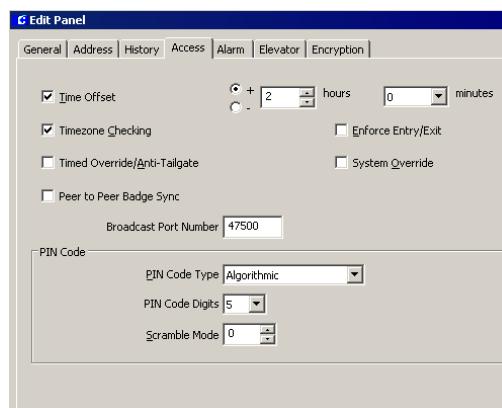
Upload only when greater than – To limit the panel from always uploading data to the Server during the time zone selected, select this box and select a percentage from the spin box only after which data will be uploaded.

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 67 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 based on 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 the cardholder 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.

Note: *Timed Override/Anti-Tailgate and the PIN Code box are disabled if using TIU panels.*

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.

Note: *The override state gets cancelled when communication with the panel is lost for more than 20 seconds (RDR2SA in physical addressing mode and RDR8S) or 5 seconds (RDR2SA in non-physical addressing mode and RDR2S). The override resumes when communication is re-established. In addition, be aware that if you perform the **Resume Normal Operation** function from the Control All Doors application, the override state gets cancelled, but the System Override option remains enabled.*

Peer to Peer Badge Sync – Available for CK721-A panels version 2.10 and higher. Enable this option to have entry/exit privileges enforced on reader terminals connected to different CK721-A panels. This feature allows a CK721-A panel to broadcast the entry/exit status of a badge to multiple CK721-A panels, via User Datagram Protocol (UDP). This allows an entry/exit zone to span across multiple panels within the same subnet or across multiple subnets using a properly configured multicast router.

IMPORTANT: This feature must never be combined with the **Global Badge Entry/Exit Status Synchronization** option selection (see page 40). Selecting both features will cause badge entry/exit enforcement errors across multiple panels.

Broadcast Port Number – Enter the UDP port number used by the Peer to Peer Badge Sync UDP Broadcast agents. This number must match that configured at the other CK721-A panels.

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 Badge window for each individual cardholder. (See the following *TIP* box for more information on PIN types, and refer to “Configure PIN Codes” on page 92 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 that will allow access at a keypad terminal. Refer to *Appendix C: Panel Comparison Matrix* for the maximum number of PIN code digits supported by each panel type.

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 Badge window.

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-DIN 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).

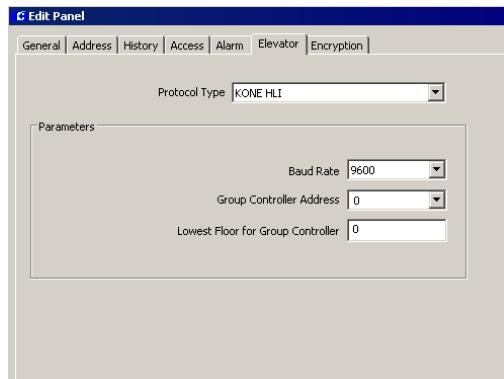
Enable Panel Relay Group Outputs – For use with CK7xx panels. If enabled, two output groups are created to represent the two physical output points on the panel CPU board: Relay 1 and Relay 2. These display as icons under the Output Groups icon for the panel selected. These output groups can be controlled as any other output group in the system.

Output Delay – Not available for S321-DIN 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 CK7xx panels to communicate with *High Level Interface* elevator control equipment via a 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 186.



Protocol Type – Select from the drop-down list the elevator protocol type to be used at your facility. Choices are: KONE HLI, Otis EMS - Security/BMS, Otis Compass, and Kone IP. See *Appendix C: Panel Comparison Matrix* for the elevator protocols supported by each panel type. Protocols 4 to 9 are reserved for future use. If KONE HLI is selected, you must complete the next fields.

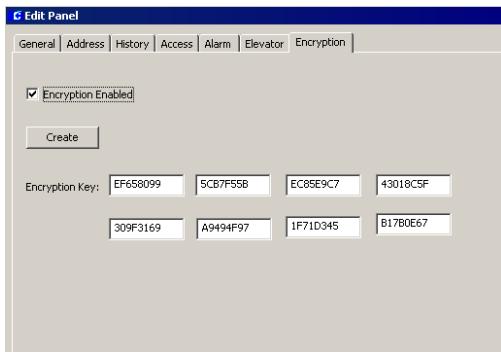
Baud Rate – Select the baud rate from the drop-down list, options are 9600 or 1200. This setting must match the baud rate configured at the elevator group controller.

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.

Encryption Tab

Use this tab to configure the P2000 software to secure every message to and from a CK721-A version 3.1 panel, using Advanced Encryption Standard (AES) to protect the P2000 system from unauthorized sources. This encryption methodology is supported for all three channels: Upload, Download, and Priority.



IMPORTANT: You must define the encryption key before enabling encryption.

Encryption Enabled – Select this check box to allow encryption of all messaging between the CK721-A version 3.1 panel and the P2000 Server. Encryption must be enabled at the CK721-A panel using its local user interface.

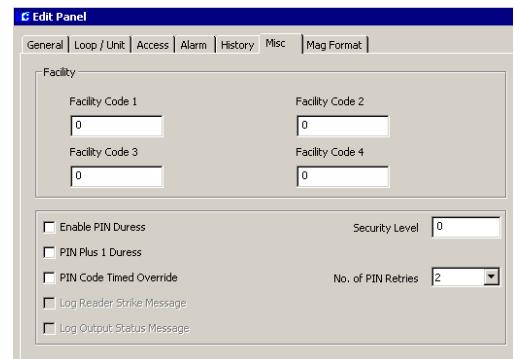
Note: While encryption is enabled, Telnet and FTP network connections will be rejected by the CK721-A panel.

Create – Click the Create button to generate a random encryption key.

Encryption Key – The Encryption Key text boxes will display the key to be used for encrypted communications. If you prefer you may enter your own key (not to exceed 64 digits) in the text boxes. This key must match the key configured at the CK721-A panel using its local user interface. Refer to the *CK721-A Version 3.1 Installation and Operation Manual* for details.

Misc Tab

Use this tab when configuring legacy and S321-DIN panels only. Not available for TIU panels.



Facility – Some of the codes stored in every badge are known as facility codes. These codes are provided by Johnson Controls and allow you to identify the badges that belong to your facility. Enter the facility code provided for your facility.

Note: CK7xx facility codes are assigned in the Edit Terminal dialog box.

Enable PIN Duress – For use with D600 AP panels only. If selected, a duress alarm is generated when a cardholder substitutes a "9" for one of the PIN code digits. If the check box is not selected, the cardholder can use the digit 9 without triggering a duress alarm. The digit 9 is usually reserved to indicate that a cardholder is seeking entry under duress (the door is opened, but an alarm is sent to local security that the user is being forced to make the entry request).

PIN Plus 1 Duress – For use with D600 AP panels only. This is a protected feature and can only be used by defining Enable Codes, see page 74 for details. If selected, a duress alarm is generated when a cardholder adds 1 to the last digit of the PIN code (for example, 5 becomes 6, not 51). 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 Enable PIN Duress option is not selected.

PIN Code Timed Override – For use with D600 AP panels only. If selected, an authorized cardholder may temporarily override access control at a keypad reader by performing a badging procedure. The override establishes an extended access time period from 0 to 1440 minutes (24 hours). During this period, the door is unlocked and the green indicator light on the reader remains lit. Cardholders can activate this feature as follows:

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

Security Level – For use with D600 AP panels only. Enter the security level number from 0 (lowest) to 99 that will be assigned to terminals connected to this panel. In the event of a security breach, a system administrator will be able to rapidly change access privileges for all cardholders at any door. For this feature to work, you also need to assign security levels to badges (page 241). To obtain access at a door, the badge security level must be equal to or higher than the security level entered here. If an event occurs, the system administrator can raise the security level of the terminals in question, and access will be immediately restricted. To restrict access at all terminals at once, simply raise the security level of the panel. Refer to “Security Threat Level Control” on page 277.

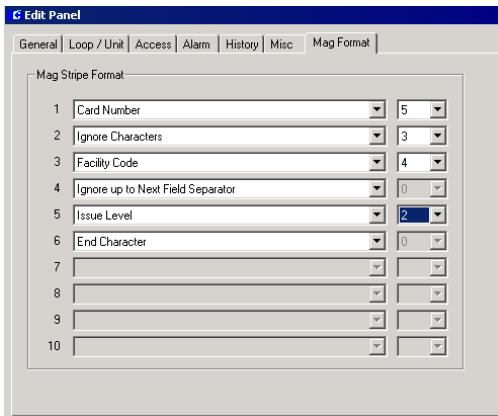
No. of PIN Retries – For use with D600 AP panels only. Select from the drop-down list the number of consecutive incorrect PIN code entries that will be allowed at a keypad reader before an alarm is generated.

Log Reader Strike Message – For use with S320 and S321-DIN panels only. If selected, the transaction will display in the Real Time List and on the System Status window.

Log Output Status Message – For use with S320 and S321-DIN panels only. 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.

Mag Format Tab

For D600 AP panels only. Since the encoding format may vary among card manufacturers, the system provides up to ten fields to define the magnetic stripe card format used at your facility (depending on the format, all fields may not be used). A magnetic stripe card contains card number, facility code, and issue level information required by the system. Each field format in a magnetic stripe formula is represented by the format type and the number of characters used in each format type. Select from the drop-down lists the format type and corresponding number of characters to be used for each type.



Ignore Characters – Select from the associated drop-down list, the number of characters that will be ignored.

Card Number – Select from the associated drop-down list, the number of characters in the card number.

Facility Code – Select from the associated drop-down list, the number of characters in the facility code.

Issue Level – Select from the associated drop-down list, the number of characters in the issue level.

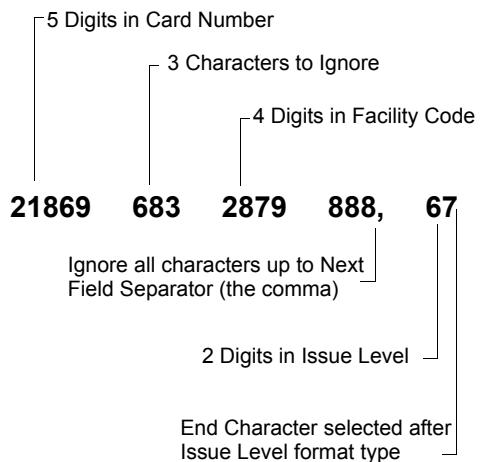
Ignore up to Next Field Separator – This field will always be “0.” The system will ignore any number of characters until it finds a field separator, a comma for example.

End Character – This is the last field in the format. This field will always be 0.

Using the values entered in the Mag Format tab:

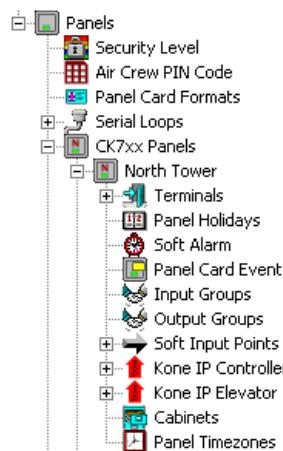
5 3 4 0 2 0

a card that uses these magnetic stripe values will display:



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**
- **Define Enable Codes**
- **Configure Air Crew PIN Numbers**
- **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. Refer to *Appendix C: Panel Comparison Matrix* for the number of panel time zones supported for each panel type. 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.

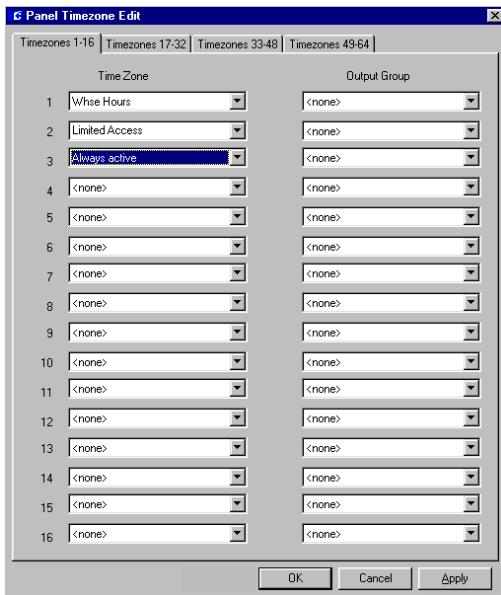
Note: *Each Assa Abloy lock can only store a maximum of 32 different time periods. Make sure the panel time zones assigned to an Assa Abloy panel do not exceed this number; otherwise the panel will be out of sync.*

You can automatically operate outputs such as lights, air conditioning, and so on, by associating Output Groups with Panel Time Zones (not available for OSI, S321-IP, Isonas, HID, or Assa Abloy panels).

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 your panel type allows it and 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 94.)

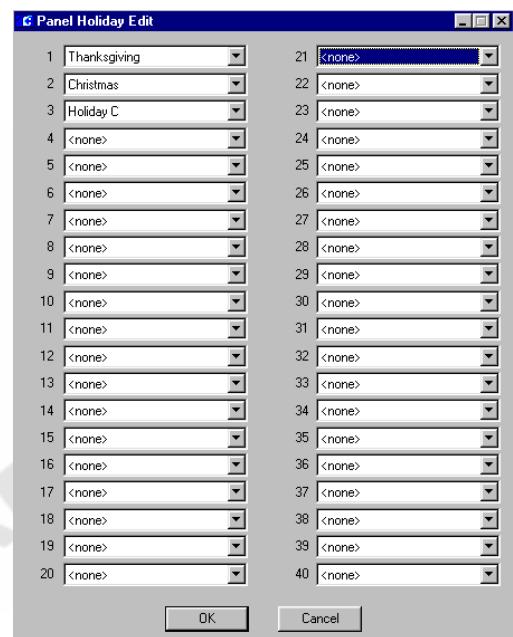
Configure Panel Holidays

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.

Refer to *Appendix C: Panel Comparison Matrix* for the number of panel holidays supported for each panel type.

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

Enable Codes (EC) Definition

The following D600 AP panel options are protected features and can only be used by entering an appropriate Enable Code:

- **PIN Plus 1 Duress**, set up at the panel Misc tab (see page 70).
- **Air Crew PIN Code**, set up at the terminal Air Crew Pin tab (page 89). You must first configure the numbers (see next section “Configure Air Crew PIN Numbers”).
- **Extended Shunt Time**, set up at the terminal Access tab (page 83).
- **Timed Override**, set up at the terminal Access tab (page 84).

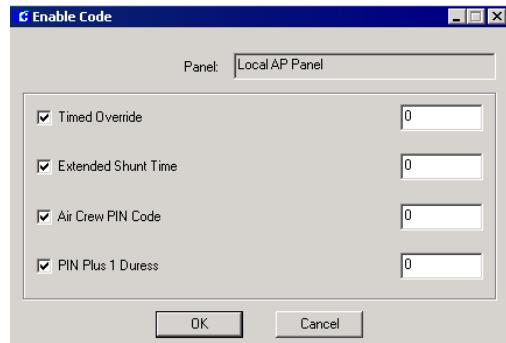
Enable Codes are provided by Johnson Controls and then entered into the system using the Enable Code dialog box. These codes are programmed from the customer’s facility codes to allow each customer to have unique Enable Codes. To obtain Enable Codes, you should contact our Technical Support team and provide your facility code together with a list of the panel options you wish to enable.

IMPORTANT: If you change any of the four facility codes set up at the D600 AP panel, the Enable Codes provided by Johnson Controls will be automatically turned off. You will have to obtain new codes and re-enter them into the system.

To Define Enable Codes:

1. In the System Configuration window, click the plus (+) sign next to the D600 AP panel where you wish to set up the Enable Codes.

2. Select the **Enable Code** icon and click **Edit**. The Enable Code dialog box opens. The Panel field displays the name of the D600 AP panel selected.



3. Select any of the options you wish to enable and enter the corresponding code provided by Johnson Controls.
4. Click **OK** to save the codes and return to the System Configuration window. Once the desired options have been turned on, you will be ready to configure the enabled features.

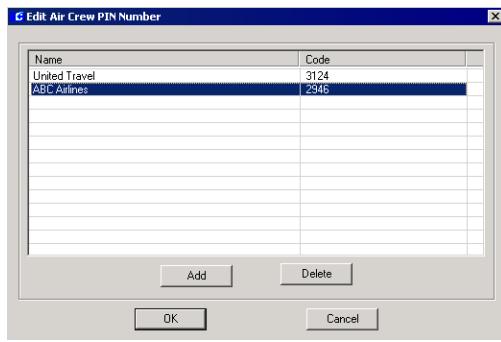
Configure Air Crew PIN Numbers

The P2000 system allows you to define air crew personal identification numbers (PIN) to be used at PIN readers connected to D600 AP panels and CK7xx panels version 2.3 and higher. Once the Air Crew PIN numbers are defined, a system administrator can enable or disable the Air Crew PIN feature from the Edit Terminal dialog box, see page 89 for details. When this feature is enabled, entering the assigned Air Crew PIN number will allow access at the door. You can create an Air Crew PIN number to be assigned to a group of people, or create a PIN number to be assigned individually to an Air Crew member with different access needs. Presenting a badge is not required when using the Air Crew PIN Number feature.

As an alternative, you can also refer to the instructions in *Appendix G: Using a Keypad Reader on CK7xx Panels*.

To Define Air Crew PIN Numbers:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.
2. Select the **Air Crew PIN Code** icon and click **Edit**. The Edit Air Crew PIN Number dialog box opens.



3. Click the **Add** button and enter the Name and Code information to define each Air Crew PIN Number. The Code number can have up to 16 digits.
4. When you finish defining all Air Crew PIN numbers, click **OK** to return to the System Configuration window. These names will display in the Air Crew Pin tab of the Edit Terminal dialog box.

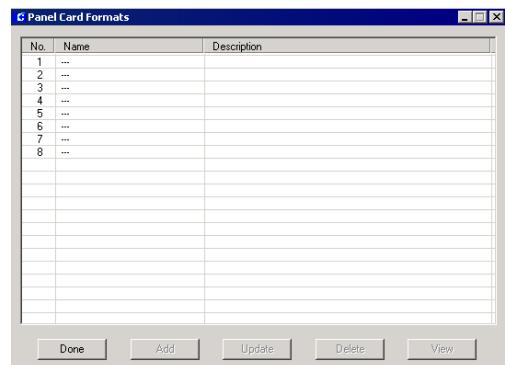
Configure Panel Card Formats

P2000 supports up to eight custom card formats that can be downloaded to S321-DIN, S321-IP, 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 Terminal dialog box.

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

To Add Custom Card Formats:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.
2. Select the **Panel Card Formats** icon and click **Edit**. The Panel Card Formats dialog box opens.



3. To add a custom card format, click the line item you wish to define and click the **Add** button.
4. Navigate to the directory where your card format files are stored and double-click the <name>.txt file you wish to use. Click **Yes** if you wish to enable the format for all CK7xx and S321-DIN terminals and also want to add it to S321-IP terminals with no custom card assignment. 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.
5. If you wish 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.

6. To delete a file format, select the file name from the list and click **Delete**. You will be prompted for verification.
7. 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.
8. Click **Done** to close the Panel Card Formats dialog box. The new card formats will be available from the Card Type tab in the 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 annunciators, 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

The following sections present instructions to configure terminals installed on CK7xx, S321-DIN, and Legacy panels. 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 59 for more information.

Set up Terminals for each Panel

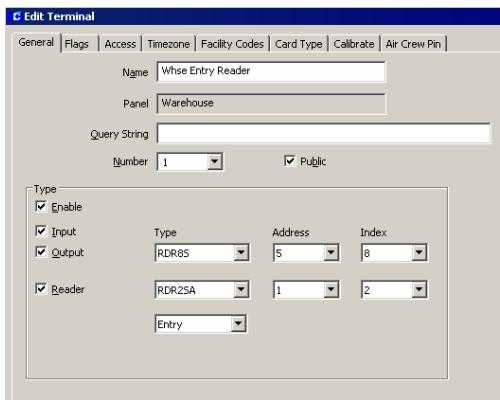
Terminals can control card readers, input points, output points, or a combination of the three, depending on the type of board installed in the panel. You must set up terminals for each panel configured in the P2000 software. As with all configuration operations, the Edit Terminal dialog box is accessed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

Note: Not all terminal options are available to all panel types. Certain features will be enabled or disabled depending on the panel type and version where the terminals are installed.

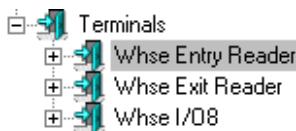
To Create a New Terminal:

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 **CK7xx 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.



- 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.

Note: You must perform the Write DB to Flash function (see page 446) when adding or deleting RDR2SA or RDR8S terminals, or when modifying general parameters of existing RDR2SA or RDR8S terminals (except Name, Public, or Query String fields).

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. For example, when configuring terminals for CK7xx panels, the Facility Codes tab is available. When configuring terminals for legacy panels, the Legacy tab will be available.

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 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

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 documentation if you need more information on terminal address assignment.)

Public – If this is a partitioned system, select the **Public** check box if you wish this terminal to be visible to all partitions.

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 run in Central mode or they must all be defined on the same panel and run in Local mode.

In addition, when configuring terminals connected to CK721-A panels version 3.0 and higher, you must select the module type installed at the panel, including the address and index of each module.

Type – Select from the drop-down list whether this is a Legacy, RDR2SA or RDR8S module.

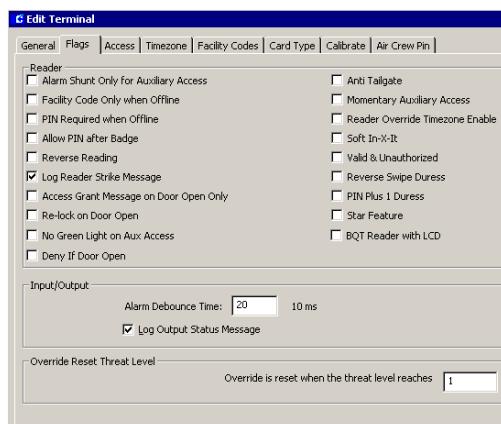
Note: A legacy module is any RDR2, SI08, SI8, IO8, or I16 device installed at the panel.

Address – Select from the drop-down list, the address (0 to 31) of the RDR2SA or RDR8S module. Not available for legacy modules.

Index – Select from the drop-down list, the index number of the RDR2SA (1 to 2) or of the RDR8S (1 to 8) module. Not available for legacy modules.

Flags Tab

The only available options when configuring TIU terminals are Reader Override Timezone Enable and Soft-In-X-It.



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-DIN 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-DIN panels.

Allow PIN after Badge – If enabled, the card-holder 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 92). If disabled, the conditions under Trigger Type in the Options box of the Panel Card Event will apply, see page 106.

Reverse Reading – Not available for legacy panels. 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 legacy or S321-DIN 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 – For this feature to work, the terminal must be configured to run in Local mode. If enabled, access grant messages are generated when the cardholder swipes the badge and opens the door. This option is only available for S321-DIN and CK7xx panels version 2.0 and higher.

When enabled on CK721-A panels version 3.0 and higher, the Keyless Override timer starts after swiping a badge (with override privileges) and immediately opening the door. When disabled, the Keyless Override timer starts after swiping a badge (with override privileges). Also, in the case of elevator readers when this flag is enabled, elevator access grant messages will be generated only when the cardholder presents a badge at an elevator reader and a valid floor is selected.

Re-lock on Door Open – This option is only available for S321-DIN and CK7xx panels version 2.2 and higher with modules RDR2 (PS201-E or higher), RDR2S, RDR2S-A or RDR8S. 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 with modules RDR2 (PS201-E or higher), RDR2S, RDR2S-A or RDR8S. 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 the RDR2S (firmware revision Q or higher), the RDR2S-A or RDR8S module.

Deny If Door Open – Available for CK7xx panels version 2.5 and higher. If enabled, an access denied message is generated when the cardholder 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, cardholders 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 108.)

Valid & Unauthorized – Not available for legacy panels. If enabled, a green light indicates that

badging has taken place; however, the system will not grant access to the cardholder. 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 – Not available for legacy panels. 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 108.) 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-DIN and CK7xx panels version 2.2 and higher. If enabled, a duress alarm is generated when a cardholder adds 1 to the last digit of the PIN code (for example, 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-DIN and CK7xx panels version 2.2 and higher. If enabled, the cardholder 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 cardholder can activate one of the following features:

0 = Local Override, followed by number of minutes

1 = Enable event, followed by event number

4 = Disable event, followed by event number

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

The cardholder must enter all PIN and Card ID information before selecting a feature. As an alternative, instead of pressing the (#) key, the cardholder 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 CK7xx Panels*.

BQT Reader with LCD – Available for CK7xx panels version 2.5 and higher. CK721-A version 3.0 does not support this feature. 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 85). 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

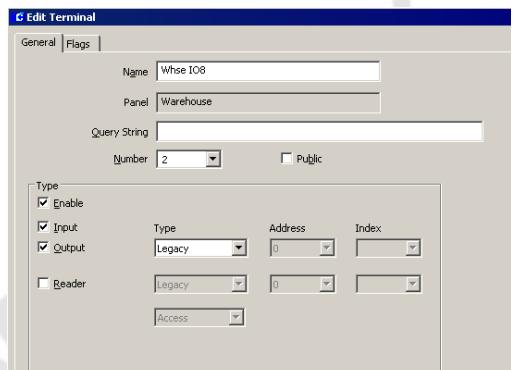
Alarm Debounce Time – (Inputs only) Not available for legacy panels. Enter a delay time in milliseconds that the system will wait to sample this terminal’s Supervised Input Point Circuits. The default is 20 msec. This improves system performance by ignoring a circuit disturbance, such as a door jiggle as it closes, rather than reporting an alarm.

Log Output Status Message – (Outputs only) Not available for legacy or S321-DIN 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:

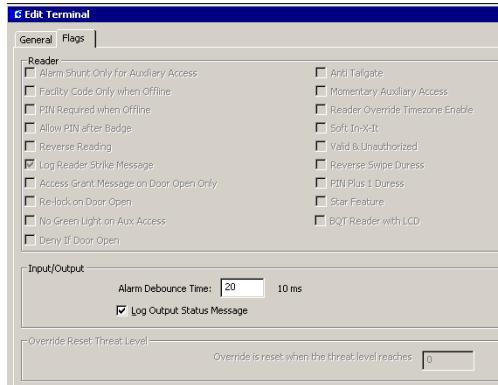
1. From the System Configuration window, select the panel to which the I/O terminal will be added.
2. Select the terminal to which you wish to add input points and click **Add**. The Edit Terminal dialog box opens.



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-DIN 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 cardholder overrides are immediately disabled. Subsequent attempts to invoke host initiated overrides or cardholder overrides will be denied.

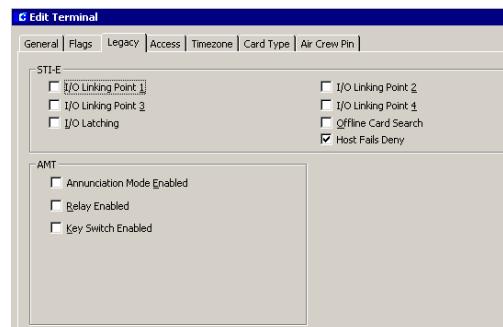
Once a terminal’s Security Level drops below the terminal’s Override Reset Threat Level, the time zone based override is restored immedi-

ately. Host initiated overrides and cardholder overrides are not automatically restored, but subsequent attempts to invoke host initiated overrides or cardholder 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.

Legacy Tab

The Legacy tab gives you access to STI-E and AMT options associated exclusively with legacy panels.



STI-E Box

I/O Linking Points 1 through 4 – If enabled, the specific alarm point to activate the associated output point is enabled.

I/O Latching – If enabled, the output relay is activated whenever its associated input goes into the alarm state and remains latched (activated) until reset by a card-activated event or by a reset output command from the Server. If disabled, output point N tracks input point N if I/O linking point N is enabled, where N=1 through 4. The output relay is activated only as long as its associated input is in the alarm state.

Offline Card Search – If enabled, the STI-E searches its own database when a badge is presented in the offline mode.

Note: If you enable the Offline Card Search function, you must also ensure that Download to STI-E has been enabled in the Badge dialog box.

Host Fails Deny – This option allows you to program the terminal to deny or accept access if the system is in Central mode and goes offline. If enabled, the terminal denies all access attempts. If this option is disabled, the terminal accepts all access requests and the panel makes an access decision in Local mode by checking the badge data against the data stored in the system database.

AMT Box

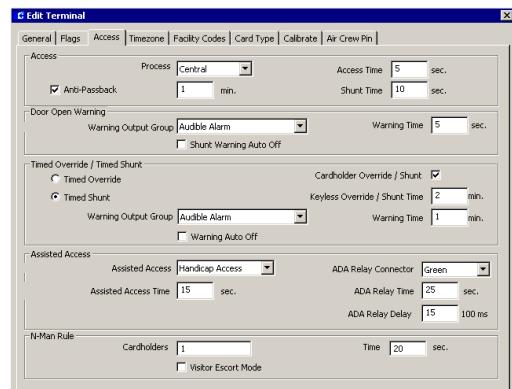
Annunciation Mode Enabled – If enabled, the annunciation mode is activated when an input point goes into an alarm state; to sound a siren, for example. Enable this option if the annunciation mode is to function.

Relay Enabled – If enabled, a local relay on AMT activates when any input point on this AMT goes into alarm state.

Key Switch Enabled – If enabled, the annunciation device can be deactivated by using a key-switch.

Access Tab

The Access tab defines the terminal's operating mode, and the access parameters and overrides allowed at the terminal. The only available options when configuring TIU terminals are Process mode and Anti-Passback option.



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 7.

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 (minutes if defining TIU panels) 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 (255 minutes for TIU panels).

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

This option is available for S321-DIN and CK7xx panels version 2.0 and higher.

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 – Not available for S321-DIN panels. If enabled, the Warning Output Group is reset when 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-DIN 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-DIN and CK7xx panels version 2.2 and higher with modules RDR2 (PS201-E or higher), RDR2S, RDR2S-A or RDR8S. 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 with modules RDR2 (PS201-E or higher), RDR2S, RDR2S-A or RDR8S. 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 has the Override option enabled in the Badge dialog box, 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 cardholder 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 cardholder must have the Override option enabled in the Badge dialog box. 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. If you wish 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 CK7xx Panels*.

Keyless Override/Shunt Time – Available for S321-DIN 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. When the Access Grant Message on Door Open Only flag is selected (see page 79), the keyless override timer starts after the cardholder swipes the badge with override privileges and then opens the door.

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 – Not available for S321-DIN panels. 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 with modules RDR2 (PS201-E or higher), RDR2S, RDR2S-A or RDR8S. 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-DIN or CK7xx panels version 2.2 and higher with modules RDR2 (PS201-E or higher), RDR2S, RDR2S-A or RDR8S. 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 in the Site Parameters dialog box

according to your facility needs, and then assigned to a cardholder that requires special access at a door.

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 cardholder's badge has the Special Access "A" flag enabled.
- **Always** – The door will always be opened for the Assisted Access Time, regardless if the cardholder's badge has the Special Access "A" flag enabled.
- **Special Access A** – The door will be opened for the Assisted Access Time, only if the cardholder's badge has the Special Access "A" flag enabled. If the Special Access "A" flag has been renamed using the Site Parameters dialog box, 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 cardholders 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 the RDR2, RDR2S, RDR2S-A or RDR8S module. Select from the drop-down list the module'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 supported module connector that normally drives the green light

■ **Shunt** – if the ADA relay is connected to the supported module connector that normally indicates the shunt condition

■ **None** – if the ADA relay is not connected to any supported module 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-DIN 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-DIN 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 cardholders who must present their badge as a group within a defined period of time in order to gain access at an N-Man Rule defined reader. For this option to work, the terminals are required to operate in Central mode.

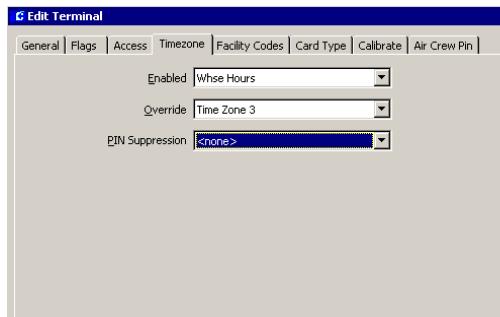
Cardholders – Enter the number of cardholders who must badge as a unit when entering an N-Man Rule controlled-reader.

Time – Enter the time in seconds during which the number of cardholders 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 cardholders 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 69 to assign facility codes to legacy and S321-DIN panels.

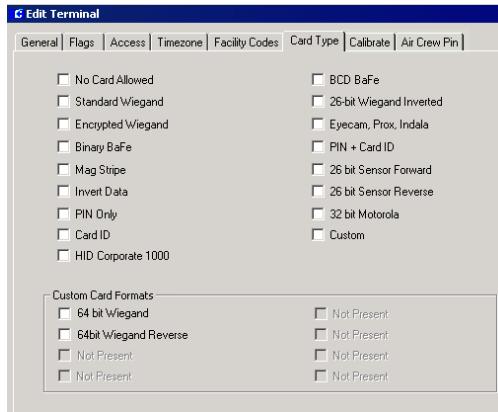
Edit Terminal						
1	468	Wiegand	7	0		
2	468	N-Crypt	8	0		
3	0		9	0		
4	0		10	0		
5	0		11	0		
6	0		12	0		

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." The Invert Data, HID Corporate 1000, 26-bit Wiegand Inverted, 32 bit Motorola, and Custom type cards are not available with legacy panels. TIU Panels do not use card types. HID Corporate 1000 is only available for S321-DIN and CK7xx panels version 2.2 and higher.

HID Corporate 1000 and Custom Card Format cards will work offline (using the Facility Code Only when Offline option), as long as the Binary BaFe card type is also selected. In addition, the first Facility Code entered in the Facility Code tab must be "4."

Note: HID Corporate 1000 card type will not work offline with RDR2 devices.



If you use S321-DIN or CK7xx panels version 2.2 and higher, the Custom Card Formats box will display the card formats that were downloaded into the panel, using the Panel Card Formats dialog box, see page 75 for detailed instructions.

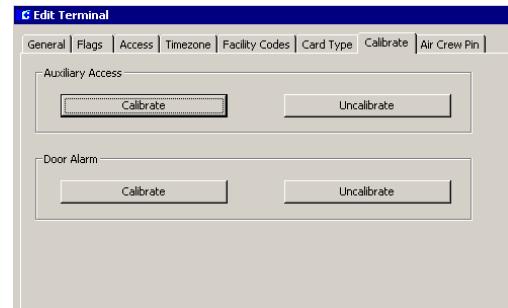
Only one type of card should be selected, with two exceptions:

- 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 92.
- 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 RDR2S, RDR2S-A or RDR8S module connected to CK7xx panels, version 2.2 and higher.



To calibrate or uncalibrate the auxiliary access, you must enable the Propped Door (24) soft alarm. After the calibration command has been successfully issued, input point 24 can be deleted if it is not being used.

IMPORTANT: 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 RDR2S, RDR2S-A or RDR8S module to initiate the input's calibration. When the module 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.

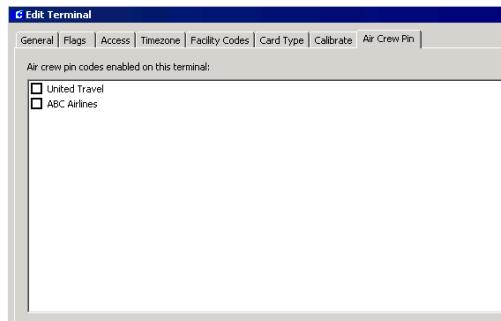
If you click either of the **Uncalibrate** buttons, the Server will send a command to the panel to uncalibrate the module's input. The panel will then send a transaction message to the Real Time List indicating the uncalibration result. After the uncalibration, four-state input statuses will no longer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

TIP: Once an input is calibrated, you will not need to use this feature again, unless you change the controller hardware or the input point's wiring.

Note: RDR2S-A and RDR8S modules with optional calibration resistors attached will automatically use this reference for calibration. Inputs calibrated in this way do not need to be secured at the time of calibration.

Air Crew Pin Tab

To be used only with D600 AP panels and CK7xx panels version 2.3 and higher.



To enable the use of PIN codes at this terminal, select from the list any or all previously defined **Air Crew PIN Codes** that were set up in the Edit Air Crew PIN Number dialog box (see page 74 for details).

When this feature is enabled, entering an assigned Air Crew PIN code will allow access at the door. If using D600 AP panels, the terminal must be running in Central mode. If selected, other terminal access options are still available (Card ID, PIN Only or PIN + Card ID). Follow these instructions to use the Air Crew PIN:

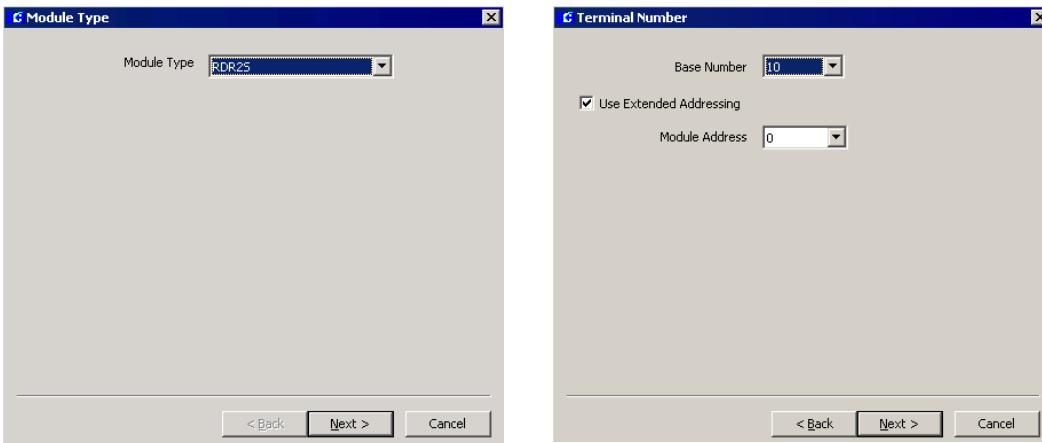
1. If you use the Star Feature, press the *2 keys to initiate the sequence. If you do not use the Star Feature, press the B key.
2. Enter the unique Air Crew PIN code. If an error is made, press the ** keys (with Star Feature) to clear the keypad buffer and start with step 1. To clear the keypad without the Star Feature, press the C key.
3. Press the # key to terminate the sequence.

Use the Add Hardware Module

The Add Hardware Module command launches a wizard style interface that simplifies the process of adding a new module to a CK7xx panel. It supports module types of I16, IO8, SI8, SIO8, RDR2S, RDR2S-A, and RDR8S. The wizard will ask the operator some basic configuration information specific to the module being added and automatically adds the necessary configuration items (terminals, input points, and output points) to the P2000 system.

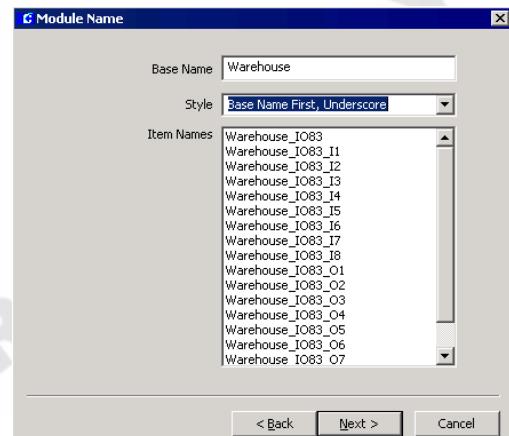
To Add a Hardware Module:

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 **CK7xx Panels** root icon and select the panel name where you want to add the new hardware module.
3. Right-click the panel name and select **Add Hardware Module** from the shortcut menu. The Module Type dialog box opens.



4. Select from the **Module Type** drop-down list one of the following options:
 - I16** – The wizard will create one input terminal with sixteen unsupervised 2-state input points.
 - IO8** – The wizard will create one input/output terminal with eight outputs and eight unsupervised 2-state input points.
 - SI8** – The wizard will create one input terminal with eight supervised 4-state input points.
 - SIO8** – The wizard will create one input/output terminal with eight outputs and eight supervised 4-state input points.
 - RDR2** – The wizard will create two RDR2 reader terminals
 - RDR2S** – The wizard will create two RDR2S reader terminals
 - RDR2SA** – The wizard will create two RDR2S-A reader terminals.
 - RDR8S** – The wizard will create eight RDR8S reader terminals. Available only for CK721-A panels version 3.0 and higher.
5. Make your selection and click **Next**. The Terminal Number dialog box opens.

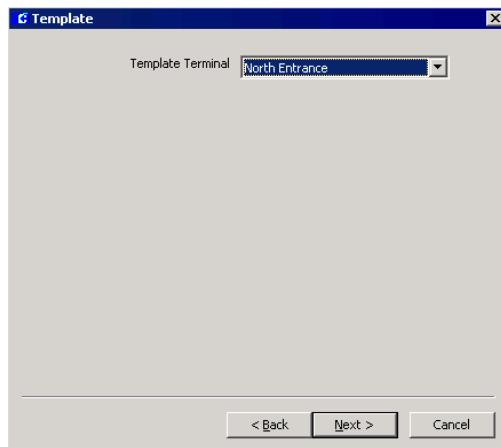
6. Select from the **Base Number** drop-down list the terminal address that corresponds to the physical address as installed at the panel.
 - For RDR2S-A modules, you have the option of using extended addressing. Select the **Use Extended Addressing** check box and select the **Module Address** from the drop-down list. If you do not select this option, the terminal will operate in Legacy mode.
 - For RDR8S modules, you must select the **Module Address** from the drop-down list.
7. Click **Next**. The Module Name dialog box opens.



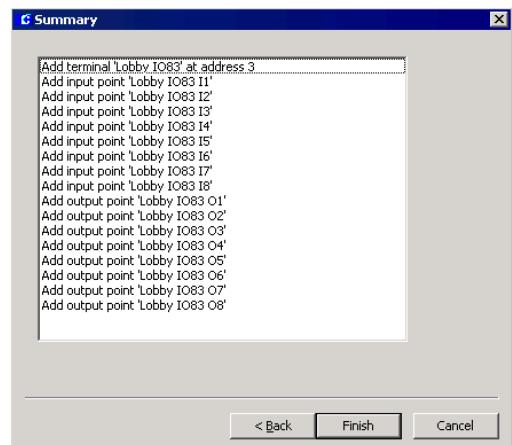
8. The **Base Name** displays the name of the selected CK7xx panel. You can however, change the name if you wish.
9. Select from the **Style** drop-down list one of the following name styles:
 - Base Name First, Space
 - Base Name First, Underscore
 - Base Name Last, Space
 - Base Name Last, Underscore

The Item Names box will display the items created with the name style selected.

10. Click **Next**. If you selected an input/output module, continue to step 12.
If you selected a reader type module (RDR2S, RDR2S-A, or RDR8S), the Template dialog box opens.



11. Select from the **Template Terminal** drop-down list, an existing reader terminal from which the access configuration parameters will be copied. Click **Next**.
12. The Summary dialog box opens.



13. Click **Finish**. The Create Items progress bar displays.
14. A message will display indicating that all items were successfully created. Click **OK** to finish. The System Configuration window will display the created items. You can edit any of the items to change configuration parameters.

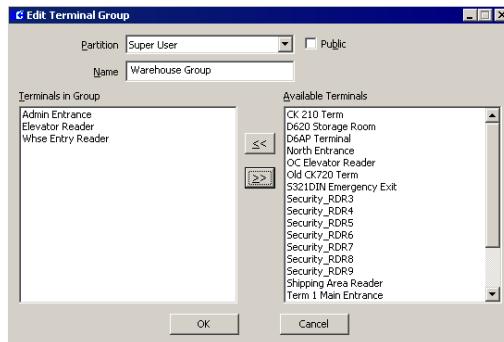
Create Terminal Groups

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 a warehouse area. When grouped together, you can assign cardholders that should have access to that area to the “Warehouse Doors” group, rather than assigning all ten terminals to the cardholders individually.

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

To Create a Terminal Group:

- From the System Configuration window, select the **Terminal Groups** icon and click **Add**. The 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 partition 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 Terminal Groups icon in the System Configuration window.

In the example, “Warehouse Group” has been added as a new terminal group.



Configure PIN Codes

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 CK7xx Panels* for further instructions. Also, refer to *Appendix C: Panel Comparison Matrix* for the number of PIN codes supported by each panel type.

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 67).
2. The panel's **PIN Code Digits** must be set to "5" (see page 67).
3. The panel's **Scramble Mode** must be set to the value used to create the PINs from the badge numbers (see page 67).
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 87).
5. The terminal's **Allow PIN after Badge** in the Flags tab has no effect (see page 78).
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 up to 9-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 87).
2. The terminal's **Allow PIN after Badge** in the Flags tab has no effect (see page 78).
3. The terminal's **PIN Suppression** in the Timezone tab has no effect, that is, 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 up to 9-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 87).
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 Badge dialog box (see page 238). 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 108).
2. The cardholder 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 108). 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

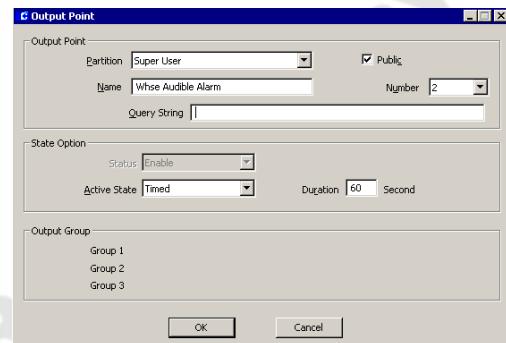
Input and output points and groups work together to control devices connected to the system terminals. For example, an *input* can be configured for a broken window contact and this can generate an *output* to an alarm annunciator. A group of inputs can generate the same output, no matter which input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

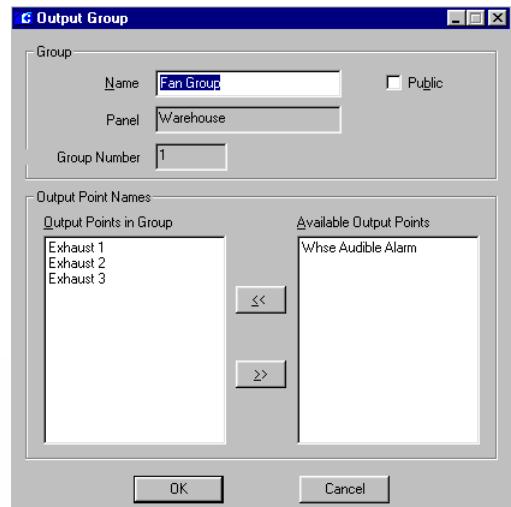
4. Enter a descriptive **Name** for the output point. (In the example, the name is Whse Audible Alarm.)
5. Select an output point **Number** from the drop-down list. This number represents the physical connection to the I/O terminal.
6. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).
7. If this is an S321-DIN output point, select Disable from the **Status** drop-down list if you wish to use the default S321-DIN 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.

Note: You must perform the Write DB to Flash function (see page 415) when adding or deleting RDR2SA or RDR8S output points.

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. In the System Configuration window, click the plus (+) sign next to the panel that contains the output points you wish to group.
2. Select the **Output Groups** icon and click **Add**. The Output Group dialog box opens.



3. In the Group box, enter a **Name** for the Output Group.
4. The **Panel** field displays the name of the Panel selected.
5. The **Group Number** field displays the number that is automatically assigned when you create an output group.

6. If your system is partitioned, select the **Public** box if you wish this group to be visible to all partitions.
7. In the Output Point Names box, select an **Output Point** from the list of Available Output Points.
8. Click **<<** to move the Output Point to the list of Output Points in Group.
9. 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.
10. To remove an output point from the Output Points in Group box, select the output point and click **>>**.
11. 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 76.)

To Create Input Points:

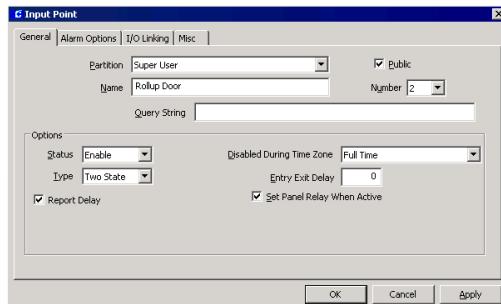
1. From the System Configuration window, select a Terminal that has been configured for inputs.

2. Click the **Input Points** icon (under the Terminal icon) and click **Add**. The Input Point dialog box opens at the General tab.
3. Enter the information in each tab, as described in the following “Input Point Field Definitions.”
4. 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.

Note: You must perform the Write DB to Flash function (see page 415) when adding or deleting RDR2SA or RDR8S input points.

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 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

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, a cardholder 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 cardholder 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.

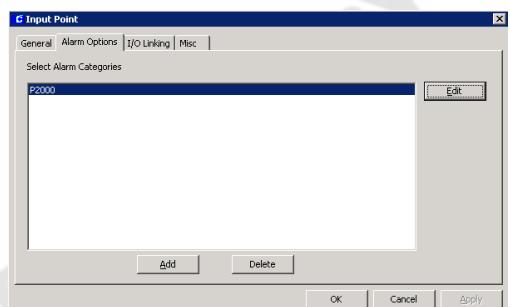
Set Panel Relay When Active – If enabled, the relay on the panel activates when the input point is activated. If disabled, the relay on the panel does not activate. Not available for S321-DIN panels.

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 255 for details), but can also be assigned to multiple alarm categories, each with its own set of alarm options.

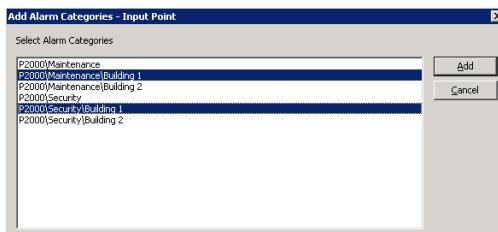
For example, if an input point connected to a glass breakage sensor generates an alarm, the P2000 system may create two separate alarms for two configured alarm categories: P2000\Maintenance\Building 1 and P2000\Security\Building 1. Typically, a single operator is configured to receive only a single 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. If you wish to assign this alarm to other alarm categories, click the **Add** button. The Add Alarm Categories dialog box

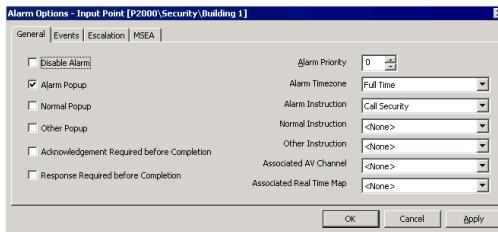
opens displaying all previously created alarm categories (see page 255 for details).



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. If you wish 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



Disable Alarm – Do not select this check box if you wish this alarm to be added to the alarm queue and displayed in the alarm monitoring

window to notify the operator of its activation. Enabling or disabling the alarm is specific to a particular Alarm Category. For example, you can enable an alarm for a “Security” alarm category and disable the same alarm for a “Maintenance” alarm category.

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.

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 104 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.”

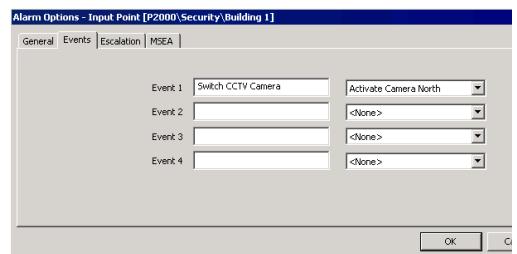
Acknowledgement Required before Completion – Select this check box to require acknowledgement of this alarm before its completion.

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 feature, 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 262.

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.

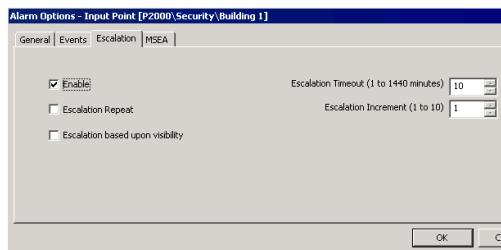
The alarm escalation feature provides for two different conditions when an alarm may be escalated:

- 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 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.

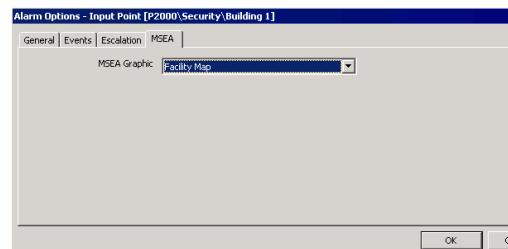
Escalation based upon visibility – When this check box is selected, the alarm will be immediately escalated by a defined increment if, at the time of occurrence, no operator able to receive alarms from this Alarm Category is logged on.

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 Metasys System Extended Architecture (MSEA), 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 349.



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 94 for detailed information.

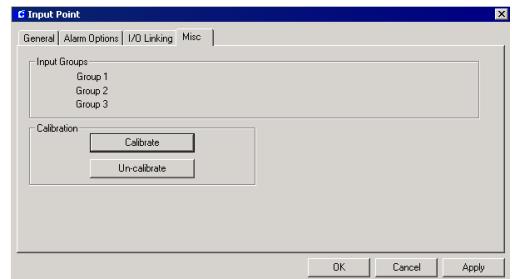


I/O Link Type – Select the appropriate link type from the drop-down list. Select one of the following choices:

- **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-DIN, RDR2S, RDR2S-A or RDR8S module connected to CK7xx panels version 2.2 and higher.

IMPORTANT: 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 S321-DIN, RDR2S, RDR2S-A or RDR8S module to initiate the input's calibration. When the S321-DIN, RDR2S, RDR2S-A or RDR8S module 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 S321-DIN, RDR2S, RDR2S-A or RDR8S input. The panel will then send a transaction message to the Real

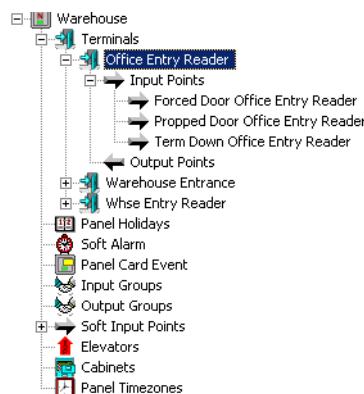
Time List indicating the un-calibration result. After the un-calibration, four-state input statuses will no longer be available for the input, only two-state statuses.

TIP: Once an input is calibrated, you will not need to use this feature again, unless you change the controller hardware or the input point's wiring.

Note: RDR2S-A and RDR8S modules with optional calibration resistors attached will automatically use this reference for calibration. Inputs calibrated in this way do not need to be secured at the time of calibration.

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 108), 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 Proposed 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 hard-wired 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.

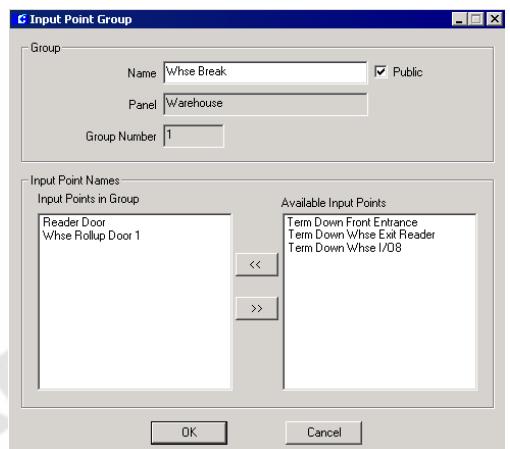
Note: If you rename a terminal that has a Terminal Down Input Point, you must edit the Terminal Down Input Point to manually enter the new terminal name, as in "Term Down <terminal name>."

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, click the plus (+) sign next to the panel that contains the input points you wish to group.
2. Select **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

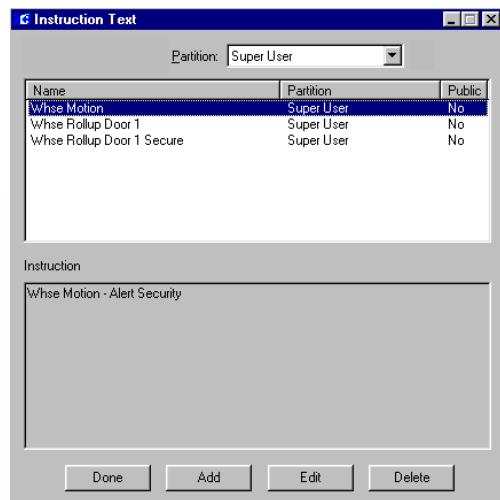
the URL. The alarm instruction detects URLs that begin with the following prefixes:

http:	file:	mailto:
ftp:	https:	gopher:
nntp:	prospero:	telnet:
news:	wais:	

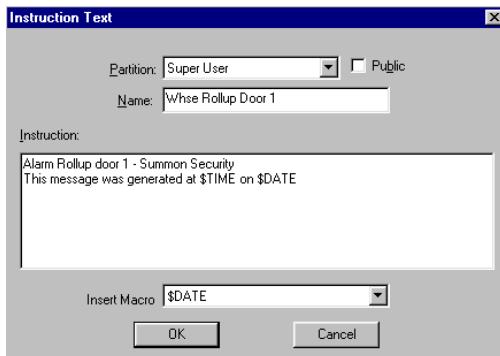
When one of the above URLs are found in the instruction text, Windows will perform its configured default action for the URL. For URLs of “http:” or “https:”, the Web Browser will be launched with that URL. If the URL begins with “mailto:”, Windows will launch your email program. If the URL begins with “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...
\$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 a Cardholder, 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 317.

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.

Use Macro....	To Insert...
\$ASCII(xxx)	ASCII Character
\$BADGE_DESCRIPTION	Badge Description
\$BADGE_NUMBER	Badge Number
\$BS	Backspace
\$CARDHOLDER_FIRSTNAME	Cardholder's First Name
\$CARDHOLDER_LASTNAME	Cardholder's Last Name
\$CARDHOLDER_NAME	Cardholder's First <space> Last Name
\$CR	Carriage Return
\$DATE	Today's Date
\$FF	Form Feed
\$INPUT_NAME	Input Name
\$INPUT_NUMBER	Input Number
\$LF	Line Feed
\$OPERATOR	Operator Name
\$PANEL_NAME	Panel Name
\$TAB	TAB

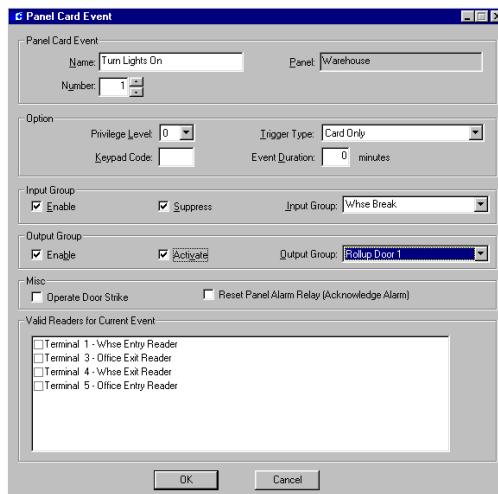
Note: Panel Card Events are configured for each panel while "System" events are configured for the Server. For more information on System Events, see "Creating Events" on page 314.

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 CK7xx 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 Cardholder's privilege level (from 0 to 7, with 0 being the lowest). The Cardholder's privilege level must be equal to or greater than the Privilege Level defined here in order to initiate the event, see “Entering Badge Information” on page 237 for more information.

Trigger Type – Indicates the condition that will trigger this card event. Select one of the following:

- Card Only** – Present badge. This trigger type does not generate *Invalid Event Privilege Level* messages.
- 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 list displays the special access flag names as configured in Site Parameters. Special access conditions are set up in the Access tab of the terminal dialog box, see page 85.

Note: If “Allow PIN after Badge” is enabled in the Terminal dialog box, the cardholder can enter the PIN number after presenting the badge, see page 78 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; that is, 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; that is, 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 legacy panels and 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-DIN 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. For legacy panels, if none of the boxes are enabled, no panel card event activation messages will be generated.

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.

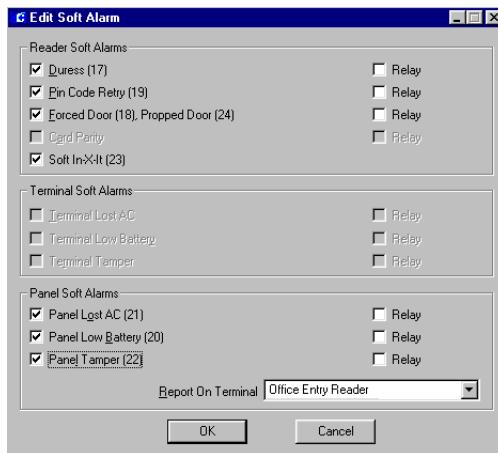
Configure Soft Alarms

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 cardholder 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 cardholder. 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 67.

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 – The binary card number includes a bit which confirms that the number of ones in that binary number is odd or even. This is compared to the card number by the STI, to confirm that the reader and/or the card is functioning properly. If an error is detected, a Card Parity Error message is sent and logged to Transaction History. This soft alarm type is not used with CK7xx, S321-DIN, S320 or TIU 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 cardholders 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 – On a UPS-equipped STI-E, an alarm is sent when power is lost. This soft alarm is equivalent to the “STI NO AC alarm” message that is printed in real time. This soft alarm type is not used with CK7xx, S321-DIN, S320 or TIU panels.

Terminal Low Battery – An alarm is sent when the battery in the terminal is low. This soft alarm type is not used with CK7xx, S321-DIN, S320 or TIU panels.

Terminal Tamper – A message is generated whenever the terminal enclosure is opened or closed. This soft alarm type is not used with CK7xx, S321-DIN, S320 or TIU panels.

Panel Lost AC – Used with the UPS option, this soft alarm sends an alarm if the panel loses power. Not available for S321-DIN panels.

Panel Low Battery – With UPS equipped panels, an alarm is sent when the battery in the panel is low. Not available for S321-DIN 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-DIN 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-DIN panels.

Configure P900 Panels and Components

Use this section to configure your P2000 system to communicate with P900 panels. P900 panels communicate with the Server via a loop configuration. It is assumed that the P900 hardware is already connected to the Server before you can configure and use the essential functions described in the following procedures. The following instructions describe how to:

- Import P900 Sequence Files
- Configure P900 System Parameters
- Configure P900 Panels
- Configure P900 Terminals
- Configure P900 Input/Output Points
- Configure CLIC Components
- Configure P900 Trigger Links

P900 to P2000 Terminology Cross Reference

The following table has been designed to assist P900 panel users become familiar with the terms used across the P2000 software.

P900	P2000
Controller	Panel
Access Point	Terminal
Site Code	Facility Code
Access Level	Access Group
Time Frame	Time Zone
Disable During Time Frame	Timezone Exception
Card	Badge
Reconfigure System	Download
Valid Entry	Access Granted
Local Anti-Passback Violation	Invalid In-X-It Status

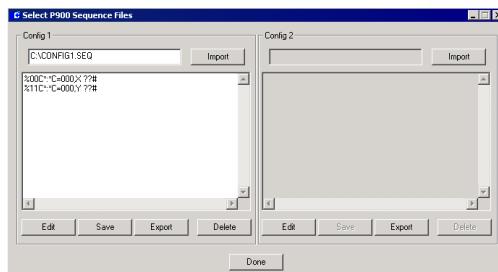
Import P900 Sequence Files

The P900 Sequence Files feature allows existing P900 users without full software support, to download commands for special usage, such as the card bit swapping command.

Sequence files are simple string files created using *Notepad* (or similar), with each line being one communication command. When the P2000 software downloads all badges, it checks if the files *Config1.Seq* or *Config2.Seq* exist, if they do, these commands are inserted into the download sequence as required. *Config1.Seq* is downloaded prior to badges, while *Config2.Seq* is downloaded after the badges.

To Import P900 Sequence Files:

- 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 **Panels** icon to display the root panel types.
- Click the plus (+) sign next to the root **P900 Panels** icon to open the P900 components.
- Click the **Sequence Files** icon and click **Edit**. The Select P900 Sequence Files dialog box opens.



- In the **Config 1** box, click the **Import** button and navigate to the directory where your command files are stored.

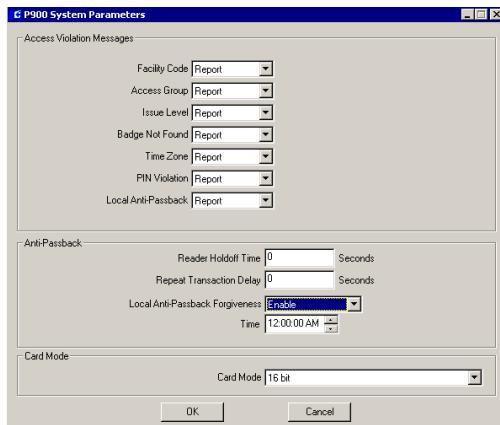
- Double-click the <**name**>.seq file you wish to import. The name and commands of the selected file displays.
- If you wish to modify the existing commands, click the **Edit** button and make your changes, then click **Save**.
- To export the command file under a different name, click the **Export** button.
- If you wish to delete the command file, click the **Delete** button.
- If you wish to import a second commands file, go to the **Config 2** box and repeat the above steps.
- Click **Done** to close the dialog box.

Configure P900 System Parameters

Prior to configuring P900 hardware components, you must define whether the P900 panels configured in the system will send messages to the Server to report certain types of access denied transactions. These messages will display in the Real Time List and will be saved in the database. You must also define Anti-Passback settings and the card format type used with P900 readers.

To Configure P900 System Parameters:

- 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 **Panels** icon to display the root panel types.
- Click the plus (+) sign next to the root **P900 Panels** icon to open the P900 components.
- Click the **P900 System Parameters** icon and click **Edit**. The P900 System Parameters dialog box opens.



5. In the Access Violation Messages box, select **Report** from the message type drop-down list that will be sent to the Real Time List on access denied transactions. Select <none> if you do not wish to send messages of this type.
6. In the **Reader Holdoff Time**, enter the time in seconds (0 to 255) after which a reader will be polled again.
7. Enter the **Repeat Transaction Delay** time in seconds (0 to 255) after which cardholders can use their badge at a different reader connected to the same panel. This allows a delay time for the badge not to be read immediately at for example, an Exit reader at the other side of the door.
8. In the **Local Anti-Passback Forgiveness** drop-down list select **Enable** to change the status of all badges to “undefined” and that way “forgive” anti-passback access violations at all P900 readers every day at the time selected in the **Time** field. Select **Reset** if you wish to immediately change the status of all badges to “undefined.”
9. In the **Card Mode** drop-down list, select the card mode that will be used at all P900 readers. The range of values within a card

number depends on the card mode selected. Refer to the following table:

Card Mode	Card Number Range
16 bit	1 - 65535
24 bit	1 - 16777215
30 bit	1 - 1073741823
P900 Cards 31 bit / Swipe Cards 32 bit	1 - 2147483647 / 1 - 4294967295
48 bit	1 - 281474976710655
64 bit	1 - 18446744073709551615

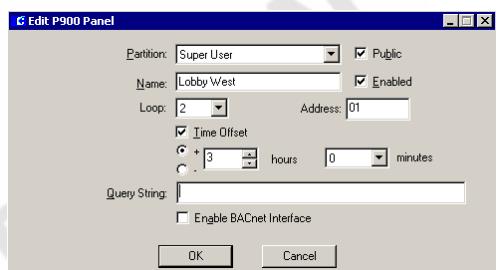
10. Click **OK** to save your settings and return to the System Configuration window.

Configure P900 Panels

P900 panels communicate with the Server via a serial connection using a loop configuration. With the serial connection, the system will support up to 32 loops, with up to sixty-four P900 panels per loop. You must set up loop configurations before configuring P900 panels. Complete instructions are presented in “Loop Configuration” on page 60.

To Create P900 Panels:

1. From the System Configuration window, click the plus (+) sign next to the root **Panels** icon to display the root panel types.
2. Select **P900 Panels** and click **Add**. The Edit P900 Panel dialog box opens.



3. If you use Partitioning, select the **Partition** that will have access to this panel informa-

tion, and select the **Public** check box if you wish to allow all partitions to see this panel.

4. Enter a descriptive **Name** for the panel, according to your Naming Conventions Plan, see page 59.
5. Select the **Enabled** check box so the panel can be recognized by the system. If you wish to temporarily disable the panel, without having to delete the panel, 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.
6. Select from the drop-down list any of the P900 **Loop** numbers defined in the Loop Configuration dialog box. The P2000 system can support up to 32 loops.
7. Enter the **Address** assigned to this panel (refer to the following section “P900 Panel Addressing Principles”). The P2000 system can support up to sixty-four P900 panels per loop.
8. 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.
9. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (see page 347).
10. Select the **Enabled for BACnet Interface** check box if you wish to define this panel as a BACnet panel object.
11. Click **OK** to save your entries. A message 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 72. If you select **Yes**, the time zones will be automatically added.

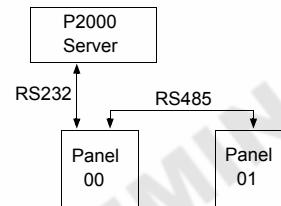
Note: In addition to applying time zones to the panels (described in “Configure Panel Time Zones” on page 72), you may also define panel holidays if you wish to restrict access in your facility during a holiday period, see “Configure Panel Holidays” on page 73.

When a P900 panel is created, the system automatically creates a *Panel Down* soft input point for input point 25 and displays under the **Soft Input Point** icon as “Panel Down <panel name>.” If you wish to report this type of alarm, edit the input point and make sure the *Disable Alarm* option is not selected in the General tab of Alarm Options, otherwise the alarm will not report to the Alarm Queue, but will continue to report to the Real Time List. Also, if you rename the panel, you must edit the input point to manually enter the new panel name, as in “Panel Down <panel name>.”

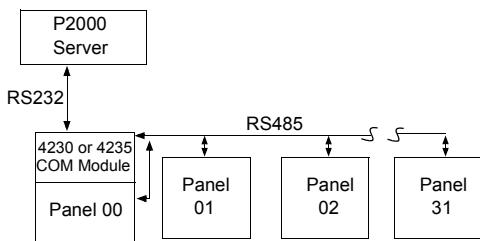
P900 Panel Addressing Principles

Panel address assignment depends on how the P900 panels are connected to the Server, which is done using one of the following three basic configurations:

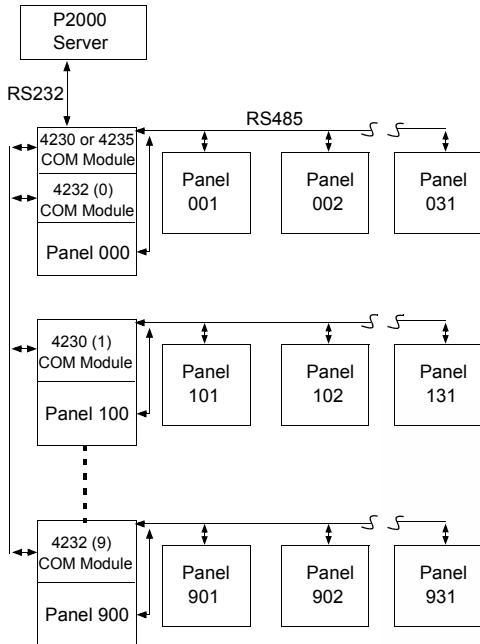
Server to One or Two Panels Only – This configuration uses an RS232 link. Addresses will be 00 and 01.



Server to up to 32 Panels – This configuration is done through a COM module. Addresses will be 00 through 31.



Server to Several Panels in a Branch Configuration – This configuration is done through COM modules in a branch configuration. There can be up to 10 branches (0 to 9), and each branch can have up to 32 panels. Addresses will be 000 to 931, and the last two digits must match the panel's physical address.



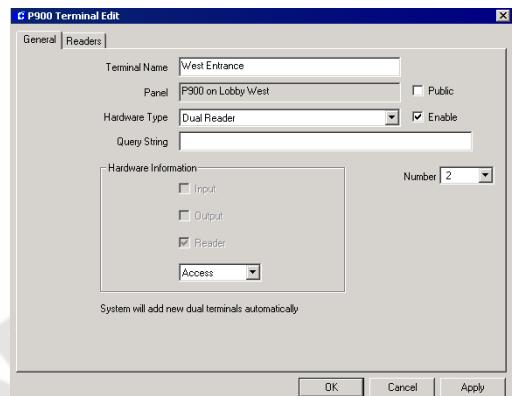
Configure P900 Terminals

Terminals are installed into the P900 panels to control devices such as card readers; inputs 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/Output Points and Groups. You must set up terminals for each P900 panel configured in the system. As with all configuration operations, the P900 Terminal Edit dialog box is accessed from the System Configuration window.

To Create a New Terminal:

1. Click the plus (+) sign next to the **P900 Panels** icon. All P900 panels currently configured in the system are listed.
2. 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.
3. Click the **Terminals** icon and click **Add**. The P900 Terminal Edit dialog box opens at the General tab. Enter the information in each tab according to your system requirements and naming conventions. See “P900 Terminal Field Definitions” for detailed information. As you work through the tabs, click **Apply** to save your settings.



4. 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.
5. Continue to create terminals for every P900 panel in which they are installed. If you wish to group P900 terminals that provide common access, refer to “Create Terminal Groups” on page 91 for detailed instructions.

P900 Terminal Field Definitions

The P900 Terminal Edit dialog box opens at the General tab. You must enter information in all tabs to complete configuration. Terminal options available in the P900 Terminal Edit dialog box are dependent on the type of hardware selected. For example, if you select any of the four Inputs/Outputs, only the General tab will be available. If you select any of the eight Readers, the Readers tab will be available. The Options tab is available if you select any of the Readers, except the Dual Reader and the Dual Cotag Reader.

General Tab

Terminal 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 P900 panel you selected from the System Configuration window.

Public – If you use Partitioning, select the **Public** check box if you wish this terminal to be visible to all partitions.

Hardware Type – Select from the drop-down list the board type installed into the P900 panel. Choices are:

- Dual Reader

- Single Reader
- Dual Cotag Reader
- Single Cotag Reader
- MK2 Dual Reader
- MK2 Dual Reader & PINpad I/F
- MK2 Dual Cotag Reader
- MK2 Dual Cotag Reader & PINpad I/F
- 16 Inputs/0 Outputs
- 8 Inputs/8 Outputs
- 8 Inputs/4 Outputs
- 16 Inputs/8 Outputs

Once you save this configuration, changes in this field can only be done within the same hardware type, e.g., you cannot change a reader type to an input/output point type or vice versa.

Enable – Select the **Enable** check box if you wish the system to recognize this terminal.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Number – Enter a terminal address number, 0 through 8. 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.) Reader terminals are numbered 0, 2, 4, or 6. Input/Output boards are numbered 0, 2, 4, 6, or 8.

If you select any of the **Dual** readers, the system will automatically add a new dual terminal to the panel, using an odd address number. For example, if you create a Dual Cotag Reader named “Warehouse Reader” with an address number of 2, the system will add a new dual terminal using the same hardware type, named “Warehouse Reader_1.” Note that if you wish

to edit the new added terminal, the hardware type and address number cannot be changed, unless you modify the first dual reader.

Hardware Information – This box displays one of the following terminal types, depending on your selection on the Hardware Type field:

- **Input** – Indicates a terminal that provides input points.
- **Output** – Indicates a terminal that provides output points.
- **Reader** – Indicates a card reader terminal. If a reader is selected as the hardware type, 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.

Readers Tab



Interface Type – Select from the drop-down list the interface setting used to decode the data from a swipe card reader. This field is not available for any Cotag readers. Choices are: 26 Bit, 34 Bit Cardkey, 34 Bit Cardkey Enc, 16 Char Cardkey Mag, and Other. If you select Other, you must enter an interface number, associated with the make and model of card reader installed.

Note: If you select **Other**, do not use the following interface numbers: 0, 4, 7, or 54. These numbers correspond to the interface types displayed in the drop-down list, e.g. 26 Bit is 0, 34 Bit Cardkey is 4, and so on.

Unlocked Time Zone – Select from the drop-down list, the Time Zone during which the reader does not require a card to open the door, and therefore allow unrestricted access. If you do not wish to enable this function, select <none> from the drop-down list.

Relay Time – Select the amount of time and select Seconds (1-180), or Minutes (1-60), or 100, 200 or 500 ms from the drop-down lists that the door relay is energized after each valid card access request.

Fixed Period – Select this option if the door relay is always energized within the Relay Time selected.

Auto Relock – Select this option to lock the door immediately when the door closes. This prevents reopening the door on one card access. If you select this option, you must select the **Enable Monitoring Action** function.

Enable Monitoring Action – Select this option if you wish to monitor Door Forced and Door Open alarms and/or warnings. This feature is required if you select the **Auto Relock** option.

Door Forced - Alarm – If enabled, an alarm message is generated whenever there is a door forced condition; the door was opened without a valid card read detected first.

Door Forced - Warning – If enabled, a warning output is activated whenever there is a door forced condition; the door was opened without a valid card read detected first.

Door Open - Alarm – If enabled, an alarm message is generated whenever there is a door open condition; the door was opened with a

valid card, but was left opened past the **Delay Time** (1 to 255 seconds).

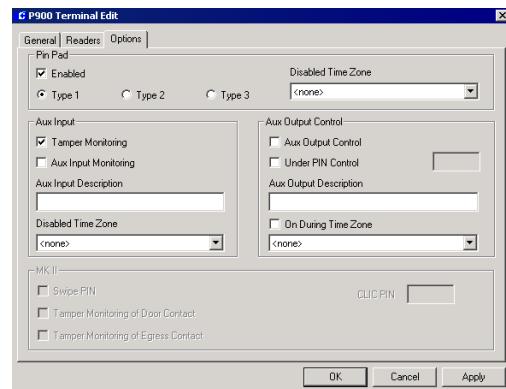
Door Open - Warning – If enabled, a warning output is activated whenever there is a door open condition; the door was opened with a valid card, but was left opened past the **Delay Time** (1 to 255 seconds).

Egress Actions – If you select **Enable**, the door relay is energized within the Relay Time selected, whenever the door exit control input is activated. If you select **Disabled**, the system will not respond to the door exit control input. If you select **Report**, the door relay is energized within the Relay Time selected, and a message is sent to the Real Time List to monitor the event.

Shunt Terminal (Anti-Passback) – Available for Entry and Exit readers only. Select from the drop-down list the reader that will be shunted whenever the door relay is energized simultaneously at an Entry and Exit reader. When you define an Entry reader, the Shunt Terminal you select here will be the Exit reader, which is usually installed at the other side of the door. The Shunt Terminal will suppress the door forced alarm after the cardholder swipes the card. When you define the Exit reader, the Shunt Terminal will be the Entry reader. We recommend you select the Shunt Terminal in both Entry and Exit readers to avoid reporting false alarms.

Manually Selected – Enable this feature if you want to allow an operator to manually control this door using the Door Control function, refer to “Controlling Doors” on page 273.

Options Tab



Pin Pad Box

Enabled – The system will not recognize the PINpad matrix connected to the reader, unless this check box is selected. The PINpad feature is available for the Single Reader, the Single Cotag Reader, and the MK2 Dual Cotag Reader & PINpad I/F. It could also be used by the MK2 Dual Reader & PINpad I/F, as long as the Swipe PIN option is disabled.

Type 1, 2, or 3 – Select the type of layout of the PINpad model connected to the reader. Refer to the following PINpad layouts:

<table border="1" style="border-collapse: collapse; width: 100px;"> <tr><td>1</td><td>2</td><td>3</td></tr> <tr><td>4</td><td>5</td><td>6</td></tr> <tr><td>7</td><td>8</td><td>9</td></tr> <tr><td>*</td><td>0</td><td>#</td></tr> </table>	1	2	3	4	5	6	7	8	9	*	0	#	<table border="1" style="border-collapse: collapse; width: 100px;"> <tr><td>1</td><td>2</td><td>3</td><td>A</td></tr> <tr><td>4</td><td>5</td><td>6</td><td>B</td></tr> <tr><td>7</td><td>8</td><td>9</td><td>C</td></tr> <tr><td>*</td><td>0</td><td>#</td><td>D</td></tr> </table>	1	2	3	A	4	5	6	B	7	8	9	C	*	0	#	D	<table border="1" style="border-collapse: collapse; width: 100px;"> <tr><td>0</td><td>1</td><td>2</td><td>3</td></tr> <tr><td>4</td><td>5</td><td>6</td><td>7</td></tr> <tr><td>8</td><td>9</td><td>A</td><td>B</td></tr> <tr><td>C</td><td>D</td><td>E</td><td>F</td></tr> </table>	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	<table border="1" style="border-collapse: collapse; width: 100px;"> <tr><td>1</td><td>2</td><td>3</td><td>A</td></tr> <tr><td>4</td><td>5</td><td>6</td><td>B</td></tr> <tr><td>7</td><td>8</td><td>9</td><td>C</td></tr> <tr><td>0</td><td>F</td><td>E</td><td>D</td></tr> </table>	1	2	3	A	4	5	6	B	7	8	9	C	0	F	E	D
1	2	3																																																													
4	5	6																																																													
7	8	9																																																													
*	0	#																																																													
1	2	3	A																																																												
4	5	6	B																																																												
7	8	9	C																																																												
*	0	#	D																																																												
0	1	2	3																																																												
4	5	6	7																																																												
8	9	A	B																																																												
C	D	E	F																																																												
1	2	3	A																																																												
4	5	6	B																																																												
7	8	9	C																																																												
0	F	E	D																																																												

↑
Type 1
↑
Type 2
↑
Type 3

A = *
B = #
A = *
B = #

Disabled Time Zone – Select from the drop-down list, the Time Zone during which a PIN code is not required to open the door, access will be granted by presenting the card only. Select <none> from the drop-down list if you require entering the PIN code at all times.

Aux Input Box

Options in this box are only available for the Single Reader and the Single Cotag Reader.

Tamper Monitoring – If enabled, a tamper alarm will be generated if the input reports an Open or Short condition.

Aux Input Monitoring – If enabled, an auxiliary input alarm will be generated if the input reports an Alarm or Secure condition.

Aux Input Description – Enter a name (up to 32 characters) for the auxiliary input. This name describes the function of the input. This will be the name of an unconfigurable input point created automatically by the Single Reader terminal.

Disabled Time Zone – Select from the drop-down list the Time Zone during which the auxiliary input monitoring will be disabled. Select <none> if you do not want to disable the auxiliary input monitoring.

Aux Output Control Box

Options in this box are only available for the Single Reader and the Single Cotag Reader.

Aux Output Control – If enabled, the auxiliary output is activated. An auxiliary output can be activated by entering a PIN at the reader or during the Time Zone selected.

Under PIN Control – If enabled, the auxiliary output will be activated when a valid card is read and the cardholder enters the correct PIN number at the reader. If you select this option, use the box at the right of this field to enter the PIN number (4 digits) that will be used to activate and de-activate the auxiliary output.

Aux Output Description – Enter a name (up to 32 characters) for the auxiliary output. This name describes the function of the output. This will be the name of an unconfigurable output

point created automatically by the Single Reader terminal.

On During Time Zone – Select from the drop-down list the Time Zone during which you can activate the auxiliary output. Select <none> if you wish to activate the auxiliary output at any time.

MK II Box

Options in this box apply to the MK2 readers only.

Swipe PIN – If enabled, a PIN will be required after swiping a card. This option is available for the MK2 Dual Reader. It could also be available for the MK2 Dual Reader & PINpad I/F, as long as the Pin Pad option is disabled. If you enable the Swipe PIN option, you can select a time zone from the **Disabled Time Zone** drop-down list in the Pin Pad box, during which the Swipe PIN option will not be active.

CLIC PIN – Enter a four-digit PIN code that will be used to activate any device connected to a Configurable Logical I/O Control (CLIC) component. See “Configuring CLIC Components” on page 120. This option is available for the following MK2 readers, in the following situations:

- **MK2 Dual Cotag Reader & PINpad I/F**
if Pin Pad is Enabled
- **MK2 Dual Reader**
if Swipe PIN is Enabled
- **MK2 Dual Reader & PINpad I/F**
if Pin Pad or Swipe PIN is Enabled

Tamper Monitoring of Door Contact – If enabled, a tamper alarm will be generated whenever the door detects a forced door or propped door condition.

Tamper Monitoring of Egress Contact – If enabled, a tamper alarm will be generated

whenever the door exit control input is activated.

Configure P900 Input/Output Points

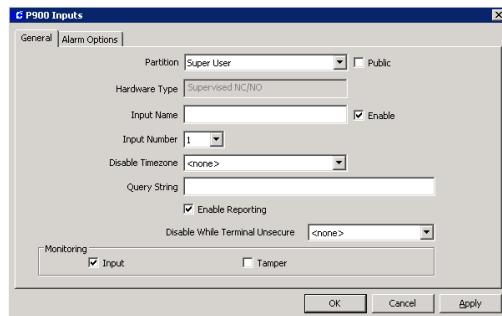
Input points are used to monitor external equipment connected to the P900 terminal; they are used to generate alarms, either when the input is activated, or if the connections to the input are tampered with or if the tamper switch in the equipment is activated. Output points control external devices connected to the P900 terminal using relay contacts located on the terminal board. Outputs can be switched on during a time zone, or can be activated in response to an access transaction or activated input point.

To Create an Input Point:

1. In the System Configuration window, click the plus (+) sign next to the P900 terminal that will provide the input point.
2. Click the **Input Points** icon and click **Add**. The P900 Inputs dialog box opens at the General tab. Enter the information in each tab. Refer to “P900 Input Field Definitions” for detailed information. As you work through the tabs, click **Apply** to save your settings.
3. Click **OK** to save your entries and return to the System Configuration window. After the input points are created, input points from the same panel can be grouped to perform related functions, refer to “Create Input Groups” on page 103 for detailed instructions.

P900 Input Field Definitions

General Tab



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

Public – Enable the **Public** check box if you wish to allow all partitions to see this input point.

Hardware Type – This field displays the “supervised input” connection type. Supervised inputs monitor tamper conditions and input state changes. Input numbers 1 to 4 are configured as NC/NO (Normally Closed/Normally Open); input numbers 5 to 8 are configured as NC (Normally Closed).

Input Name – Enter a descriptive name for this input point.

Enable – Select this check box to report all input point changes of state. Do not select the check box if you do not want these changes reported.

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

Disable Timezone – 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.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Enable Reporting – If this input point is not related to alarm monitoring, select this option to report input point changes of state to the Real Time List.

Disable While Terminal Unsecure – This option will disable this input point whenever the relay at the selected terminal is energized. If you do not wish to disable the input point, select <none>.

Input Monitoring – Enable this option if you wish to monitor input points that report Alarm or Secure conditions.

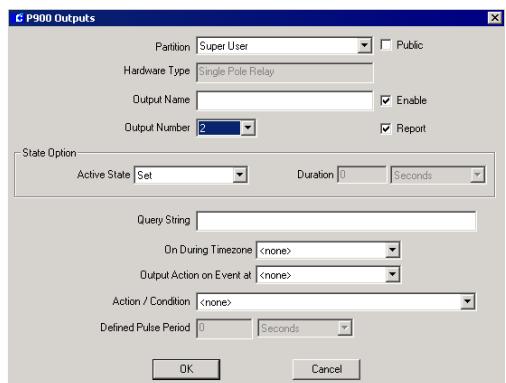
Tamper Monitoring – Enable this option if you wish to monitor input points that report Open or Short conditions. Conditions are reported as Short only.

Alarm Options Tab

Alarm options are described in detail on page 97.

To Create an Output Point:

1. In the System Configuration window, click the plus (+) sign next to the P900 terminal that will provide the output point.
2. Click the **Output Points** icon and click **Add**. The P900 Outputs dialog box opens.



3. If you use Partitioning, select the **Partition** that will have access to this output point and check **Public** if you wish the output point to be visible to all partitions.
4. The **Hardware Type** field displays the “pole relay” output type. The number 1 output on a 4250 I/O module is the only Double Pole Relay output type; all others are Single Pole Relay type.
5. Enter a descriptive **Name** for the output point.
6. Select the **Enable** check box if you wish to report all output point changes of state. Do not select the check box if you do not want these changes reported.
7. Select an **Output Number** from the drop-down list. This number represents the physical connection to the I/O terminal.
8. Select the **Report** check box if you wish to report output point changes of state to the Real Time List.
9. From the **Active State** drop-down list, select **Set** to turn on the output point, or **Timed** to turn on the output point for the specified time entered in the **Duration** field.
10. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature

(refer to “Configuring Hardware Components for BACnet Interface” on page 347).

11. From the **On During Timezone** field, select a time zone during which the output point will always be active. Select **<none>** if this output point is controlled with a trigger event.
12. To activate the output point whenever the access condition selected in the Action/Condition field occurs, select the terminal name from the **Output Action on Event at** drop-down list where this access condition should occur.
13. The choices in the **Action/Condition** drop-down list determine how the output is activated, and the type of access that causes it to be activated. See the following definitions:

Actions	Definitions
Toggle State	If the output is off, then turn it on. If the output is on, then turn it off.
Pulse	Turn the output on for the period defined in the next field, then turn it off again.
Energize	Turn the output on.
De-Energize	Turn the output off.
Conditions	Definitions
Valid Card	Access granted.
Invalid (Report Only) Card	Access denied: transaction message sent to Real Time List
ANY Invalid Card	Access denied: any or no message sent to computer.

Select **<none>** if this output point is controlled with a trigger event.

14. If you select any of the Pulse actions, you must enter the **Defined Pulse Period**.
15. Click **OK** to save your entries and return to the System Configuration window. After the output points are created, they can be grouped to perform common functions, see “To Create Output Groups:” on page 95 for detailed instructions.

P900 Soft Alarms

Soft alarm points and their addresses are created by the system during installation rather than hardwired to an actual input point. To open the Edit Soft Alarm dialog box, double-click the Soft Alarm icon that displays under the P900 panel name. The system automatically configures certain soft alarms for P900 panels and readers, for detailed descriptions see “Soft Alarms Field Definitions” on page 108. The only item you are allowed to configure is the selection of the terminal associated with the soft alarm.

Configuring CLIC Components

Configurable Logical I/O Control (CLIC) components can be set up to program inputs and outputs of I/O modules to control and act in response to external equipment such as intruder alarms, lights, detectors, etc. connected to the system. Input/Output operations can be integrated with the access control so actions can be taken based on access transactions, system alarms, and time zones to make the external equipment behave in any way you want, according to what is happening in the rest of the system.

The execution of CLIC relies on the definition of one or more Trigger Events, which link *Sources* with *Conditions* and *Actions*. The Sources that can initiate a **Trigger Event** are the change of state of a time zone, an access transaction, a system alarm, the change of state of an input or input group, a **Counter** reaching a specified value, and a change of state of a **Flag**.

Once a Trigger Event is initiated, it will test the *Condition* of a time zone, the value of a Counter, and the state of up to two Flags. If the *Sources* of a Trigger Event become active and its *Conditions* are met, then it will initiate an *Action* to change the state of any or all inputs,

outputs, counters or flags, and optionally send a message to the system.

To use programmable I/O (CLIC), you must configure the following components:

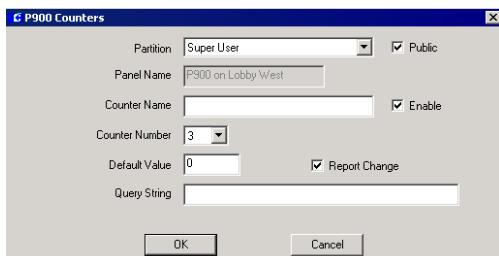
- Counters
- Flags
- Trigger Events

P900 Counters

You can create up to 64 counters for each P900 panel. A counter reaching a specified value can be the source used to initiate a Trigger Event, and can increment or decrement each time a trigger occurs. A counter might be used, for instance, to count certain access transactions such as entries to a parking structure. The value of a counter can also be changed as part of the action of a trigger event. Counter values can be reset using the P900 Counter Control dialog box, see page 275.

To Create a P900 Counter:

1. Click the plus (+) sign next to the **P900 Panels** icon. All P900 panels currently configured in the system are listed.
2. Click the plus (+) sign next to the panel where you wish to configure the CLIC components. All the items that can be configured for the panel are listed under it.
3. Click the plus (+) sign next to the root CLIC icon, select **P900 Counters** and click **Add**. The P900 Counters dialog box opens.



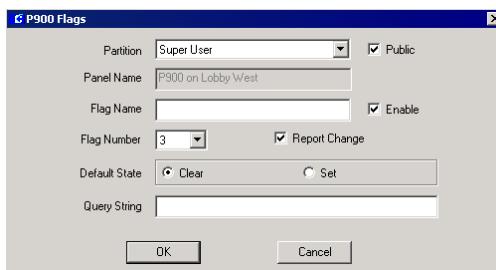
4. If you use Partitioning, select the **Partition** that will have access to this counter and check **Public** if you wish the counter to be visible to all partitions.
5. The **Panel Name** field displays the name of the panel selected.
6. Enter a **Counter Name** to describe the function of the counter.
7. Select the **Enable** check box to allow the counter to change values.
8. Select a **Counter Number** from the drop-down list.
9. Enter a **Default Value** for this counter. This is the value that the counter is set to when you reset the counter using the P900 Counter Control dialog box. Each counter can have any integer value from 0 to 65535.
10. Select the **Report Change** check box if you wish to report counter changes to the Real Time List.
11. The **Query String** value only applies if you have the P2000-Metasys integration feature. Refer to “Configuring Hardware Components for BACnet Interface” on page 347.
12. Click **OK** to save your entries and return to the System Configuration window.

P900 Flags

You can create up to 64 flags for each P900 panel. Flags provide a means for passing conditions from one Trigger Event to another. A flag changing to a specified state can be the source used to initiate a Trigger Event. The state of a flag can be defined as **Set** (when the flag is active) or **Clear** (when the flag is inactive). You can also use the P900 Flag Control dialog box to manually change the current state of the selected flag.

To Create a P900 Flag:

1. Click the plus (+) sign next to the **P900 Panels** icon. All P900 panels currently configured in the system are listed.
2. Click the plus (+) sign next to the panel where you wish to configure the CLIC components. All the items that can be configured for the panel are listed under it.
3. Click the plus (+) sign next to the root CLIC icon, select **P900 Flags** and click **Add**. The P900 Flags dialog box opens.



4. If you use Partitioning, select the **Partition** that will have access to this flag and check **Public** if you wish the flag to be visible to all partitions.
5. The **Panel Name** field displays the name of the panel selected.
6. Enter a **Flag Name** to describe the function of the flag.
7. Select the **Enable** check box to allow the flag to change states.
8. Select a **Flag Number** from the drop-down list.
9. Select the **Report Change** check box if you wish to report flag state changes to the Real Time List.
10. Select the **Default State** for this flag. Enable **Clear** if the flag's default state will always be inactive, or **Set** if the flag's default state will always be active.
11. The **Query String** value only applies if you have the P2000-Metasys integration

feature. Refer to “Configuring Hardware Components for BACnet Interface” on page 347.

12. Click **OK** to save your entries and return to the System Configuration window.

P900 Trigger Events

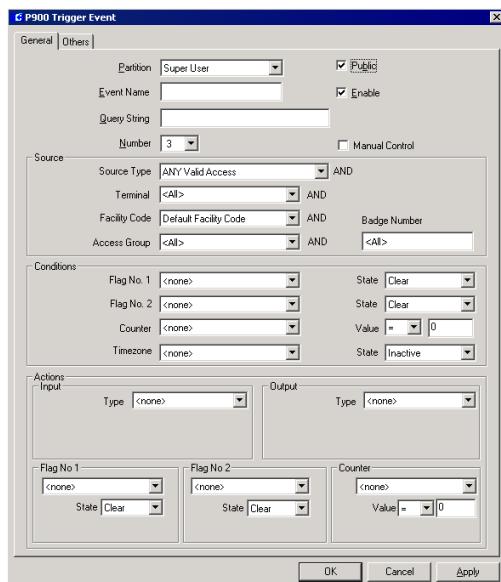
You can create up to 128 trigger events for each P900 panel. Trigger events define actions that are performed when specified conditions are met. Each trigger event is made of the following elements: the Source, the Conditions, and the Actions. When the Source changes state and the Conditions are met, the Actions are performed. Trigger events can also be forced to immediately perform one of its actions by manually activating it using the P900 Event Control dialog box, see page 276.

To Create a P900 Trigger Event:

1. Click the plus (+) sign next to the **P900 Panels** icon. All P900 panels currently configured in the system are listed.
2. Click the plus (+) sign next to the panel where you wish to configure the CLIC components. All the items that can be configured for the panel are listed under it.
3. Click the plus (+) sign next to the root CLIC icon, select **P900 Trigger Events** and click **Add**. The P900 Trigger Event dialog box opens.
4. Enter the information in each field, as described in the P900 Trigger Event Field Definitions.
5. When all information is completed, click **OK** to save the trigger event and return to the System Configuration window.

P900 Trigger Event Field Definitions

General Tab



Partition – If you use Partitioning, select the **Partition** in which this trigger event will be active.

Public – Enable the **Public** check box if you wish to allow all partitions to see this trigger event.

Event Name – Enter a descriptive name for the event.

Enable – Select this check box for the system to process this trigger event. If you wish to temporarily disable the trigger event, select the check box again to disable it.

Query String – This value only applies if you have the P2000-Metasys integration feature. Refer to “Configuring Hardware Components for BACnet Interface” on page 347.

Number – Select an event number from the drop-down list. This number determines the

order in which the trigger event will be performed.

Manual Control – Select this check box if you wish to allow this trigger event to be manually initiated by an operator using the P900 Event Control dialog box, see page 276.

Source Box

Select from the **Source Type** drop-down list the source whose change of state will start the trigger event. Specific parameters must be defined for each Source Type selected. The table on page 124 describes all the possible sources types and corresponding parameters.

Conditions Box

The trigger event can test the conditions of two flags, one counter, and one time zone. If you leave all the conditions set to <none>, then none is tested and the trigger event automatically proceeds to the “Actions” state.

Flag No. 1 – To test the condition of a flag, select from the drop-down list the flag name that the trigger event will use.

State – Select from the drop-down list whether the flag should be **Clear** or **Set** for the condition to be “true.”

Flag No. 2 – To test the condition of a second flag, select from the drop-down list the flag name that the trigger event will use.

State – Select from the drop-down list whether the second flag should be **Clear** or **Set** for the condition to be “true.”

Counter – To test the value of a counter, select from the drop-down list the counter name that the trigger event will use.

Source Type	Parameters			
ANY Valid Access Trigger event will be initiated by a badge that is granted access.	Terminal – The trigger event will be initiated by a badge read at the terminal selected here.	Facility Code – The trigger event will be initiated by a badge whose facility code is selected here.	Access Group – The trigger event will be initiated by any badge that belongs to the access group selected here.	Badge Number – The trigger event will be initiated only by the badge number entered here.
ANY Invalid Access Trigger event will be initiated by a badge whose code is read but no access is granted.	Terminal – The trigger event will be initiated by a badge read at the terminal selected here.	Invalid Type – The trigger event will be initiated by a badge that is denied access for the reason selected here.		
Input Point Trigger event will be initiated by the change of state of a single input.	Input – The trigger event will be initiated by the change of state of the input name selected here.	State – The trigger event will be initiated when the input goes into the <i>Alarm</i> , <i>Normal</i> or <i>Tamper</i> state.		
Input Group Trigger event will be initiated by the change of state of an input group.	Name – The trigger event will be initiated by the change of state of the input group name selected here.	Logic – Select <i>OR</i> if the input group will become active when one or more inputs are in the State selected, or select <i>AND</i> if the input group will become active when all the inputs are in the State selected.	State – The trigger event will be initiated when the input group goes into the <i>Clear</i> or <i>Set</i> state.	
Time Zone Trigger event will be initiated by the change of state of a Time Zone.	Name – The trigger event will be initiated by the change of state of the time zone selected here.	State – The trigger event will be initiated when the time zone becomes <i>Active</i> or <i>Inactive</i> .		
Flag Trigger event will be initiated by the change of state of a Flag.	Name – The trigger event will be initiated by the change of state of the flag selected here.	State – The trigger event will be initiated when the flag goes into the <i>Set</i> or <i>Clear</i> state.		
Counter Trigger event will be initiated by the change of value of a Counter.	Name – The trigger event will be initiated by the change of value of the counter selected here.	Value – Select whether the trigger event will be initiated when the counter becomes equal to (=), greater than (>), or less than (<) the value (0 and 65535) entered here.		
System Alarms Trigger event will be initiated by an alarm condition.	Sub Type – Select the type of alarm: <i>Controller Power</i> , <i>Controller Tamper</i> , <i>Terminal Open</i> or <i>Forced</i> , <i>Duress Entry</i> or <i>Polling Detected</i> .	State – The trigger event will be initiated when the alarm becomes active (<i>Alarm</i>) or when it becomes inactive (<i>Normal</i>).	Terminal – The trigger event will be initiated by an alarm generated at the terminal selected here.	

Value – Select from the drop-down list whether the value of the counter is equal to (=), greater than (>), or less than (<) the value entered in the next field, for the condition to be “true.”

Timezone – To test the state of a Time Zone, select from the drop-down list the time zone name that the trigger event will use.

State – Select from the drop-down list whether the Time Zone should be **Active** or **Inactive** for the condition to be “true.”

Actions Box

Define the actions that will be performed by the trigger event based on the sources and conditions selected.

Input Type – A trigger event can disable, enable, or shunt an input or an input group. When an input or input group is enabled, its state is being monitored. When an input or input group is disabled or shunted, its state is ignored. Select from the drop-down list one of the following input action types: Enable Input, Disable Input, Shunt Input, Enable Input Group, Disable Input Group, or Shunt Input Group.

Name – Select from the drop-down list the input or input group name that will be enabled, disabled, or shunted.

Input Period – If you select the Shunt Input or Shunt Input Group, select a shunt time in the Input Period field, enter the number, then on the next field select minutes, seconds or milliseconds.

Output Type – A trigger event can turn on, turn off, or pulse (temporarily turn on) an output or an output group. Select from the drop-down list one of the following output action types: Output On, Output Off, Output Pulse, Output Group On, Output Group Off, or Output Group Pulse.

Name – Select from the drop-down list the output or output group name that will be turned on, turned off, or pulsed.

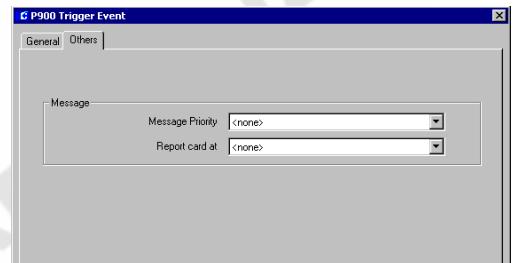
Output Period – If you select to pulse the output or output group, select a pulse time in the Output Period field, enter the number, then on the next field select minutes, seconds or milliseconds.

Flag No 1 – If you wish the trigger event to set, clear or pulse a flag, select the flag name from the drop-down list and from the State drop-down list select whether the trigger event will **Clear**, **Set** or **Pulse** the flag. If you select to Pulse the flag, you must also enter a pulse time.

Flag No 2 – If you wish the trigger event to set, clear or pulse a second flag, select the flag name from the drop-down list and from the State drop-down list select whether the trigger event will **Clear**, **Set** or **Pulse** the second flag. If you select to Pulse the flag, you must also enter a pulse time.

Counter – If you wish the trigger event to increment, decrement or set the value of a counter, select the counter name from the drop-down list and from the Value drop-down list select whether the counter will add 1 (+), subtract 1 (-), or set the counter (=), to the value (0 to 65535) entered in the next field.

Others Tab



Message Priority – Select **Report** from the drop-down to send a trigger event activation message to the Real Time List. Select **<none>** if you do not wish to send messages of this type.

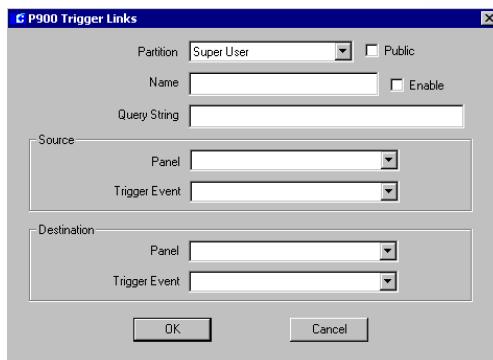
Report card at – If you select to Report trigger event activation messages to the Real Time List and wish to include a card number as part of the message, select from the drop-down list the terminal name where the valid card will be read. If you select **<none>** the card number in the message will always be 0.

P900 Trigger Links

The P900 Trigger Links function enables you to program a trigger event in one panel to initiate a trigger event in another panel, as long as the **Message Priority** of the first trigger event is set to **Report**. When the *Source* of the originating trigger event changes state and the *Conditions* are met, the destination trigger event's *Conditions* are tested and, if met, its *Actions* are performed.

To Configure P900 Trigger Links:

1. Click the plus (+) sign next to the **P900 Panels** icon to open the P900 components.
2. Click the **Trigger Link** icon and click **Add**. The P900 Trigger Links dialog box opens.



3. If you use Partitioning, select the **Partition** that will have access to this trigger link and check **Public** if you wish the trigger link to be visible to all partitions.
4. Enter a **Name** to describe the function of the link.
5. Select the **Enable** check box to allow the system to perform the trigger link between the selected panels.
6. The **Query String** value only applies if you have the P2000-Metasys integration feature. Refer to “Configuring Hardware Components for BACnet Interface” on page 347.
7. Select the source **Panel** from the drop-down list.
8. Select the source **Trigger Event** from the drop-down list. The list will display all trigger events configured for the panel selected.
9. Select the destination **Panel** from the drop-down list.
10. Select the destination **Trigger Event** from the drop-down list. The list will display all trigger events configured for the panel selected.
11. Click **OK** to save your entries and return to the System Configuration window.

Note: If the trigger link does not work, make sure the **Message Priority** of the source trigger event is set to **Report**.

Configure OSI Panels and Components

IMPORTANT: This release of the P2000 software is compatible with WAMS Web Service version 2.2.0 (Build 113), Portal Gateway version 2.2.0 (Build 117), and Reader version 2.30 (Build 20). Older versions of the OSI software are not compatible with this P2000 release.

Use this section to configure your P2000 system to communicate with OSI Wireless Access Management Solutions (WAMS) hardware. It is assumed that the OSI hardware is already installed before you can configure and use the essential functions described in this section. Refer to the OSI documentation for hardware installation instructions and to the *P2000 Server/Workstation Software Installation Manual* for instructions associated with the installation of the OSI Interface software.

IMPORTANT: The installation of the WAMS Web Service version 2.2.0 (Build 113) must follow some specific instructions. Contact Tech Support for detailed instructions.

The OSI Interface that resides on the P2000 Server is called P2000 OSI Interface Service, and provides an interface between the P2000 system and OSI OMNILOCK® 2000 Series readers. This integration allows P2000 operators to configure and control OSI readers to provide badge access using Access Groups. Transactions and alarm messages associated with these readers are sent to the Alarm Monitor and the Real Time List.

The OSI hardware consists of a Portal Gateway that provides wireless communications to the individual readers using a wireless personal area network (WPAN), and the individual OMNILOCK wireless readers. The portal gateway communicates with the P2000 Server

via standard 10/100Base-T Ethernet connectors. The transmit range from portal gateway to reader is typically 150 to 300 feet. Each portal gateway can support up to 128 readers. The wireless reader performs the actual access validation and can support up to 65,000 badges. The OSI interface has no hard limit on the number of portal gateways but enforces the existing P2000 limits on the number of readers.

The portal gateway includes a built-in Web server that provides a simple easy-to-use user interface for configuring the portal, monitoring the status of the portal, and updating the firmware loaded into the portal and the readers.

Unsupported OSI Features

The following OSI system features are not compatible with the P2000 system architecture:

- Access and Shunt Time per Badge
- PIN Expiration Dates
- Unlock with ID access mode
- OSI I/O modules

Unsupported P2000 Features

The following P2000 system features are not supported by the OSI system:

- Extensive badge specific time-controlled access rights (see “Badge Access Rights” on page 129 for more information)
- Quick detection of hardware offline

System Architecture

The communication to the OSI portal gateway is performed by the OSI Web Service, which is installed with the OSI Interface. The portal gateway in turn provides the wireless communication path to the individual OSI readers.

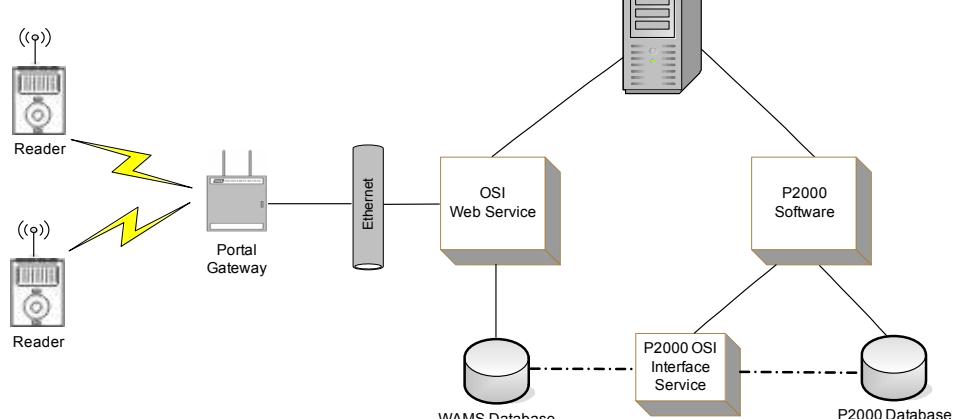
The OSI Web Service runs in the context of the Microsoft Internet Information Services (IIS) Web server, sends data and commands to the readers, and receives transaction data from the readers. The OSI Web Service reads and writes data to the OSI WAMS database that is hosted in the same SQL Server as the P2000 system. The P2000 OSI Interface Service provides the interface between the P2000 system and the OSI system. The OSI Interface Service performs all of its functions by reading and writing records to the OSI WAMS database. All other major principles of the P2000 architecture remain the same.

Hardware Detection

The OSI system provides automatic hardware detection. When new portal gateways or readers are added to the system, they are detected by the OSI Web Service and the appropriate record is created in the WAMS database. The P2000 OSI Interface Service will periodically scan for these new items. When a new item is found, the appropriate record is created in the P2000 database.

This automatic hardware detection also affects long term operation. If an OSI reader is unable to communicate with its portal gateway for a period of about 30 minutes or more, it will attempt to connect to any other portal gateway within wireless range. This provides communication redundancy if a reader is within communication range of multiple portal gateways. Since the P2000 software maintains a relationship between panels and terminals (and displays this relationship in several different locations), it must update the database when a reader switches to a new portal gateway. The P2000 OSI Interface Service detects this condition and updates the database as required.

Since the terminal record is only updated and not recreated, any links between terminals and access groups, or other items, remain unchanged. The only impact is for partitioned P2000 systems. Since by definition the terminal belongs to the same partition as its panel, moving a terminal to a different panel may require the partition of the terminal to change. In practice, this is usually not a problem since P2000 partitions usually correspond to some physical barrier or separation such as different



buildings or different areas of the same building. In most cases the physical separation between these areas will prevent readers from communicating with portals in other partitions.

Badge Access Rights

The P2000 software defines access rights for individual badges through multiple pairs of Access Groups and Timezones. OSI readers do not support this model of badge access rights. The OSI model consists of a list of readers that a badge has rights to use at any time in combination with membership in up to 32 User Groups. Since the P2000 system operates with a set of badge access rights across multiple types of controllers and readers, the P2000 OSI Facility Edit application is provided to configure these settings.

Using the OSI Facility Edit application, a P2000 operator can configure up to 32 pairs of Access Groups and Timezones as Facility Access Groups. These Facility Access Group pairs correspond to OSI User Groups. When Access Groups and Timezone pairs are assigned to an individual badge (using the Badge application), the Timezone values are ignored unless the Access Group has been configured as an OSI Facility Access Group. If the Access Group corresponds to an existing OSI Facility Access Group, then the Timezone configured for the Facility Access Group will define the time when access is allowed. If the Access Group is not defined as a Facility Access Group, then the badge will be granted access on a 24/7 basis.

Configuration Sequence

Once the hardware is installed, we recommend the following configuration sequence:

- Configure OSI Facility parameters.
- Establish network connections between OSI hardware devices and the P2000 Server

- Configure the portal gateways
- Configure readers

Configure OSI Facility Parameters

Before bringing any OSI hardware online, the OSI Facility record must be added to the P2000 database. The OSI Facility record defines settings that control all OSI portal gateways and wireless readers connected to a single P2000 server.

To Configure OSI Facility Parameters:

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 **Panels** icon to display the root panel types.
3. Click the plus (+) sign next to the root **OSI Panels** icon to open the OSI components.

Note: If the **OSI Panels** branch does not display, you need to enable the **OSI** panel type in the Panel Types tab of Site Parameters. This should only be necessary if you have upgraded from a prior version of P2000.

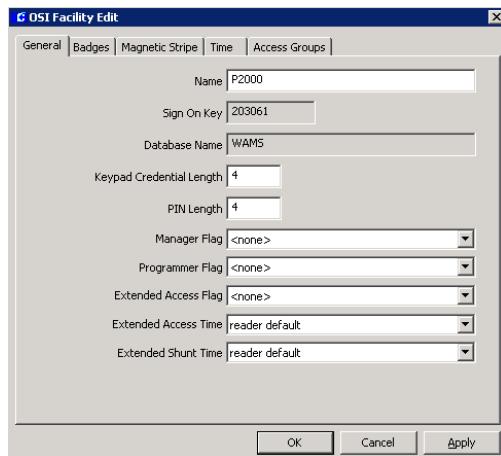
4. Select the **OSI Facility** icon and click **Add**. The OSI Facility Edit dialog box opens at the General tab.
5. Fill in the information on each tab according to the following OSI Facility Field Definitions.
6. As you work through the tabs, you may click **Apply** at any time to save your entries.
7. After you have entered all the information, click **OK** to save the settings and return to the System Configuration window.

Once the OSI Facility record is saved, it will be written in the OSI database. At that point, the system will automatically recognize new hardware when it is activated, as well as automatically add it to the P2000 database.

OSI Facility Field Definitions

General Tab

Use this tab to define general descriptive information of the OSI Facility record and the access parameters associated with the readers.



Name – Enter the name of the OSI Facility record. This field displays **P2000** by default, but you can change the name according to your facility needs.

Sign On Key – This is a six-digit number that is automatically assigned to each OSI Facility record. If your facility uses OSI readers with keypads, you will enter this number at each wireless reader to establish connection between the readers and the portal gateways, and ultimately to establish the communication with the WAMS software.

Database Name – This field displays the name of the OSI database.

Keypad Credential Length – Enter the number of digits that cardholders will need to enter at wireless keypad readers in your facility.

PIN Length – For facilities that require additional security, enter the number of PIN code digits that cardholders will need to enter at wireless keypad readers in your facility.

Manager Flag – Select one of the three special access flags to be assigned to users with Manager privileges who require special access at a reader.

Note: Special access allows a door's access time to be different. The list displays the special access flag names as configured in Site Parameters, see page 41.

Programmer Flag – Select one of the three special access flags to be assigned to users with Programmer privileges who require special access at a reader.

Extended Access Flag – Select one of the three special access flags to be assigned to users with Extended Access privileges who require special access at a reader.

Note: Manager, Programmer, and Extended Access privileges are assigned using the OSI software.

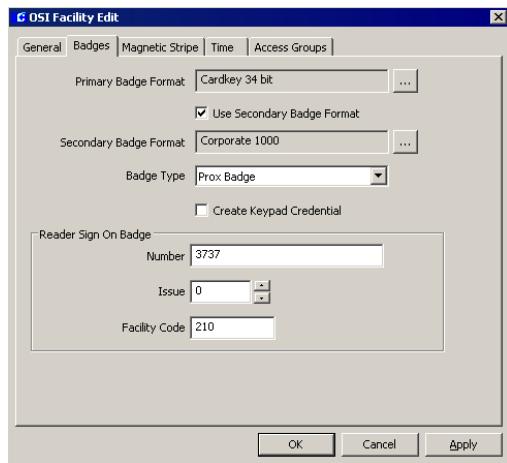
Extended Access Time – Select the amount of time that the door will remain unlocked to provide extended access time to cardholders with special needs.

Extended Shunt Time – Select the amount of time that the door alarm will be suppressed to allow access to cardholders with special needs. The Extended Shunt Time must exceed the Extended Access Time.

Note: The reader default option in the Extended Access Time and the Extended Shunt Time is the time defined at the Access tab of the OSI Terminal Edit dialog box, see page 139 for details.

Badges Tab

Use this tab to define the badge formats and type that will be used at all OSI readers. In addition, if the OSI readers do not have keypads, you will need to enter the Reader Sign On Badge information to be used at your facility.



Primary Badge Format – Click the [...] button and select the primary badge format to be used at your facility. The P2000 software provides badge formats that are located in the \Program Files\Johnson Controls\CARDKEY P2000\BadgeFormats folder. If a different format is needed, create a new badge format file by using the P2000 Badge Format tool, see page 182 for details.

Note: On 64-bit Windows operating systems use \Program Files (x86)\Johnson Controls\P2000\BadgeFormats folder.

Use Secondary Badge Format – Select this check box if your facility will use a secondary badge format.

Secondary Badge Format – Click the [...] button and select the secondary badge format to be used at your facility.

Badge Type – From the drop-down list select the badge type to be used at your facility. Options are: **Prox Badge**, **Mag Stripe Badge**, and **Smart Card Badge**.

Create Keypad Credential – Keypad Credential numbers are codes stored in every badge and allow you to identify the badges that belong to your facility. Select this check box if you wish to automatically assign these codes to all badges in your facility that will be used with OSI wireless readers.

Reader Sign On Badge

If your facility uses OSI readers with no keypads, you can create a master badge that will be assigned with a facility number. This badge will be used to establish communication between the readers and the software.

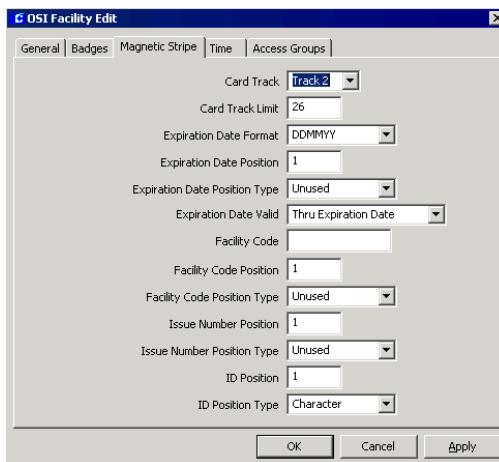
Number – Enter a badge number that will be used for the facility number. This badge number does not need to be a valid P2000 badge assigned to a cardholder.

Issue – Select the issue level from 0 to 255 that will be used for the facility number.

Facility Code – Enter the facility code number that will be used for the facility number.

Magnetic Stripe Tab

If your facility uses Magnetic Stripe cards, use this tab to configure the software to accept the card types and settings. Default settings will be sufficient for most systems.



Card Track – Select from the drop-down list **Track 2** or **Track 3** magnetic cards. The system can be used with either Track 2 or 3 cards; however, you cannot use both types within the same facility. Most users will use Track 2 cards and will not need to set up any type of advanced card parameters.

Card Track Limit – There is a limitation on the number of characters for each track. These characters include any digits and field separators; however, they exclude the starting and ending sentinels. The maximum number of characters that the system can read on Track 2 is **26** characters; Track 3 can read up to **70** characters. The P2000 software does not enforce these limits.

Expiration Date Format – Select from the drop-down list the card expiration date format.

Expiration Date Position – Enter the position in the card of the expiration date field.

Expiration Date Position Type – Select from the drop-down list if the position type is a **Character**, a **Field**, or **Unused**.

Expiration Date Valid – Select from the drop-down list if the expiration date is valid **Thru Expiration Date** or **To Expiration Date**.

Facility Code – Enter the facility code number that will be assigned to your cards.

Facility Code Position – Enter the position in the card of the facility code field.

Facility Code Position Type – Select from the drop-down list if the position type is a **Character**, a **Field**, or **Unused**.

Issue Number Position – Enter the position in the card of the issue number field.

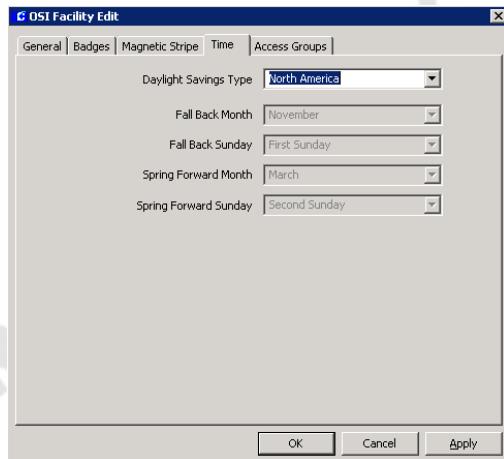
Issue Number Position Type – Select from the drop-down list if the position type is a **Character**, a **Field**, or **Unused**.

ID Position – Enter the position in the card of the ID field.

ID Position Type – Select from the drop-down list if the position type is a **Character**, a **Field**, or **Unused**.

Time Tab

Use this tab to adjust Daylight Savings Time (DST) settings according to your region. DST varies from country to country. Some countries may not observe DST, while in many other countries the start dates and end dates for DST change from year to year.



Daylight Savings Type – Select from the drop-down list the daylight savings type that applies to your region. Choices are **Custom**, **Europe**, **North America**, and **Southern Hemisphere**. When you select Europe, North America or Southern Hemisphere, the system defaults to the standard Daylight Savings Time settings for the selected region.

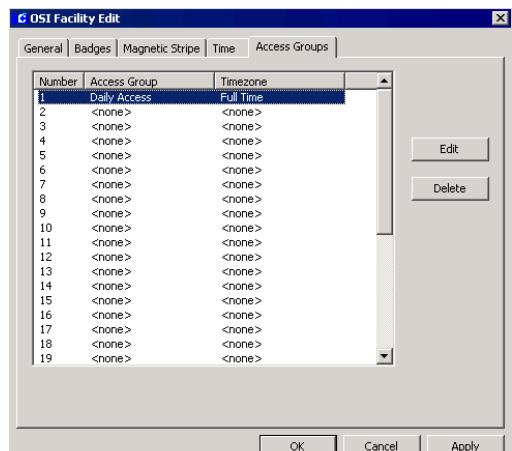
If you wish to change the default settings, select **Custom** from the Daylight Savings Type drop-down list and select:

- the **Fall Back Month**
- the **Fall Back Sunday**
- the **Spring Forward Month**
- the **Spring Forward Sunday**

Access Groups Tab

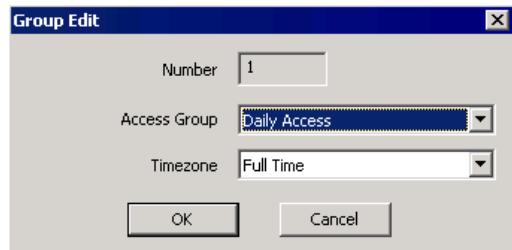
Use this tab to define up to 32 Access Groups and corresponding Timezones that can be assigned to all badges that are used at OSI readers. You must create Access Groups (page 218) and Time Zones (page 55) before the selections will display in the drop-down lists.

Note: *The P2000 software provides full support for direct access to readers on a 24/7 basis. It does not provide support for time controlled access thru OSI Facility Groups.*



To Define OSI Facility Access Groups:

1. In the Access Groups tab, double-click the line item you wish to define. The Group Edit dialog box opens.



The **Number** field displays a number that indicates the order in which the access group will be downloaded to the panels.

2. Select from the drop-down list, the **Access Group** you wish to assign to the badges that are used at OSI readers.
3. In the **Timezone** field, select a time zone that will be assigned to the selected Access Group.
4. Click **OK** to save your settings.
5. If you wish to remove a group from the list, select the line item and click the **Delete** button.

Adding New Portals

To add OSI hardware devices into the P2000 database, you must first establish the communication between the OSI portals and the software. Each portal gateway must be configured with its assigned IP address, the IP address of the P2000 Server, and the user name and password to use when connecting to the Server. The portal gateways have a built-in Web Interface that allows you to configure these settings.

You will need to connect a computer to the portal and assign the computer a static IP address with the same subnet mask as the portal gateway (the factory default IP address of the portal is 192.168.1.200). This can be done either over the network or by direct connection to the computer using a crossover Ethernet cable. The simplest approach is to configure the computer to temporarily have an IP address of 192.168.1.200 (or similar).

IMPORTANT: To avoid serious operational problems because of the IP subnet changes, you should use a computer and NOT the P2000 Server to perform this setting.

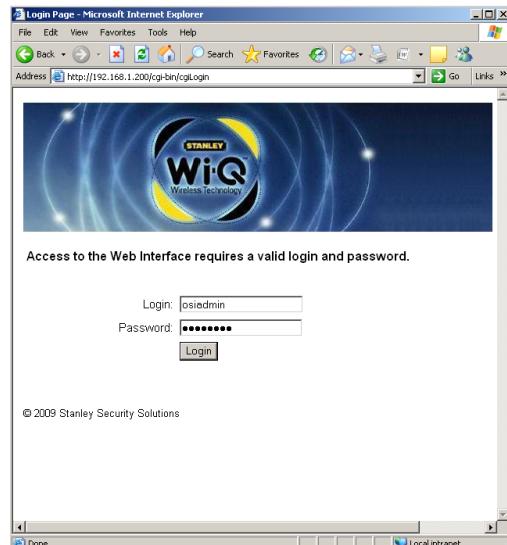
Once you assign the static IP address to the computer, you are ready to proceed to set up the portal gateway using the OSI Web Interface. After the portal gateway is set up and configured through the Web Interface, you can establish the connection between the portal gateway and the P2000 Server.

To Set Up the Portal Gateway:

- At the computer with the new static IP address, open the standard Web browser and type the following default address of the portal:

http://192.168.1.200

The Login Page opens.

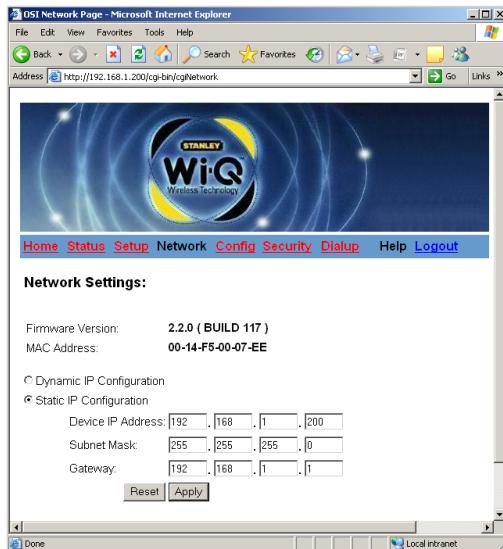


- Enter the following default OSI Web Interface Login and Password:

Login: osidadmin
Password: osilogin

Once you are logged on you can click the **Security** link from the OSI Web Interface menu bar to change the default login and password.

- Click the **Network** link to open the Network Settings page.



The current **Firmware Version** and **MAC Address** of the connected portal displays.

Note: The Media Access Control (MAC) address is a hardware address that uniquely identifies each node of a network, for example, a portal gateway or I/O device.

4. Select **Dynamic IP Configuration** (recommended for networked facility) or **Static IP Configuration** and enter an IP address specific to your network.
5. If you select Static IP Configuration, enter the **Device IP Address**, **Subnet Mask**, and **Gateway**. See your Network Administrator for the correct settings.
6. Click the **Apply** button. This will cause the portal to perform a reset.
7. Wait a couple of minutes for the portal to restart, open your Web browser and enter the new IP address of the portal.
8. In the login page, enter the **Login** and **Password**.
9. Click the **Setup** link to open the Portal Gateway Setup page.



10. Under Access IP Configuration, enter the **Server IP Address** of the P2000 Server.
11. Under Access Port Number, select the **Default Port Number** or **Specify Port Number**.
12. Under Secure Communications, select **Enable SSL** if you plan to use a secure socket layer connection over the internet.

Note: If you enable SSL, the server must have a valid certificate issued to it. If you don't have a certificate to your server, do not select this check box.

13. Under Host Access, enter the following Login name and Password, which allow logging on to IIS on the P2000 Server:

Login: osiportal
Password: Master1

14. Click the **Update** button to save your settings.
15. Scroll down to **Channel Selections** to configure the portal gateway to log on to the P2000 Server via your TCP/IP network. Click **Select All** to ensure appropriate channel settings. If you use the 802.11-B protocol, select only channels **25** and **26**. This ensures that the WAMS protocol does not interfere with your 802.11-B protocol.
16. Click the **Update** button to save all settings.

After a few minutes, the portal is automatically added to the P2000 System Configuration window as a new panel. Note that the Real Time List will display the *Add Panel Audit* message.

If after a few minutes the portal does not show in the P2000 System Configuration window, log back on to the portal and click the **Status** link. On the Status page, click the **Show Log** button to view the error messages from the portal. These messages usually point to the problem that needs to be corrected. If the portal displays “Unable to access OSI Web Services Log file” that indicates that the portal has no errors recorded.

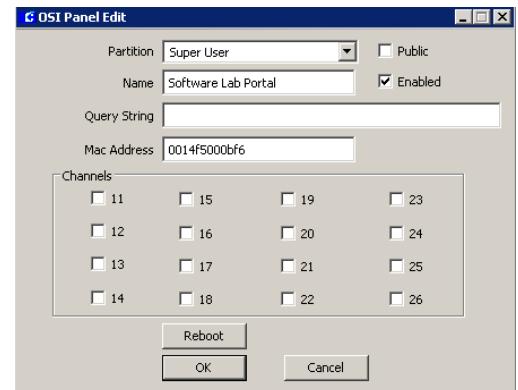
Configure OSI Panels

Once the portal gateway is set up and configured through the OSI Web Interface to establish the connection to the P2000 Server, the portal will display in the System Configuration window under the OSI Panels root icon. By default, portal names include their MAC address. You must now complete the configuration of the portal.

To Configure OSI Panels:

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 **Panels** icon to display the root panel types.
3. Click the plus (+) sign next to the root **OSI Panels** icon to open the OSI components.
4. Select the portal you wish to configure and click **Edit**. The OSI Panel Edit dialog box opens.



5. If you use Partitioning, select the **Partition** that will have access to this panel, and select the **Public** check box if you wish to allow all partitions to see the panel.
6. Enter a descriptive **Name** for the panel. By default the Name field displays the MAC address of the portal but you can change the name according to your facility needs.
7. Select the **Enabled** check box so the panel can be recognized by the system. If you wish to temporarily disable the panel, without having to delete the panel, 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.
8. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasy integration feature (see page 347).

9. The **Mac Address** field displays the Media Access Control address automatically assigned to the portal.
10. Select from the **Channels** box, the Radio Frequency (RF) channels or frequency bands that this panel will use to communicate with the readers.
11. The **Reboot** button is provided to restart the portal, for example if the portal is not responding or to recover from an error.
12. Click **OK** to save your entries.

After you create the OSI panel, the system automatically creates a *Panel Down* soft input point for input point 25 and displays it under the **Soft Input Points** icon. If you wish to report this type of alarm, edit the input point and make sure the **Disable Alarm** option is not selected in the General tab of Alarm Options, otherwise the alarm will not report to the Alarm Queue, but will continue to report to the Real Time List (see “Alarm Options Tab” on page 97).

Configure OSI Terminals

After a portal is up and functional, you can add new readers to the system. A new reader needs to be “enrolled” into the OSI system to become functional. The enrollment process is different for readers that have keypads and readers that do not.

Readers with Keypads – For a reader with a keypad, you must enter the Sign On Key from the P2000 OSI Facility record into the keypad, see page 130. To place the reader into enrollment mode, enter **5678** on the keypad. A green light on the reader will flash three times. Within five to six seconds, enter the six-digit Sign On Key from the OSI Facility record. The reader will now go thru a sequence of alternating red and green lights and should finish with three green flashes. That means the reader successfully communicated with the portal.

Readers without Keypads – For a reader without a keypad, the reader is placed into enrollment mode by presenting the default badge that was included in your package from OSI. Within five to six seconds, present the badge that was defined in the Reader Sign On Badge box of the OSI Facility record, see page 131. The reader will now go thru a sequence of alternating red and green lights and should finish with three green flashes. That means the reader successfully communicated with the portal.

After a successful sign on, the reader should be detected and automatically added to the P2000 database as a new terminal. Note that the Real Time List will display messages associated with the new OSI components.

Each reader 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 to provide common access throughout your facility.

To Create OSI Terminals:

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 **OSI Panels** icon. All OSI portals currently configured in the system are listed.
3. Click the plus (+) sign next to the portal that contains the readers you wish to configure.
4. Click the plus (+) sign next to the **Terminals** icon to display the readers that were successfully enrolled. By default, the reader names include their MAC address.
5. Select the reader you wish to configure and click **Edit**. The OSI Terminal Edit dialog box opens at the General tab. Enter the information in each tab according to your

system requirements. See the following OSI Terminal Field Definitions for detailed information.

6. As you work through the tabs, you may click **Apply** to save your settings.
7. When all entries are complete, click **OK** to save your settings and return to the System Configuration window.
8. If you wish to group OSI terminals that provide common access, refer to “Create Terminal Groups” on page 91 for detailed instructions.

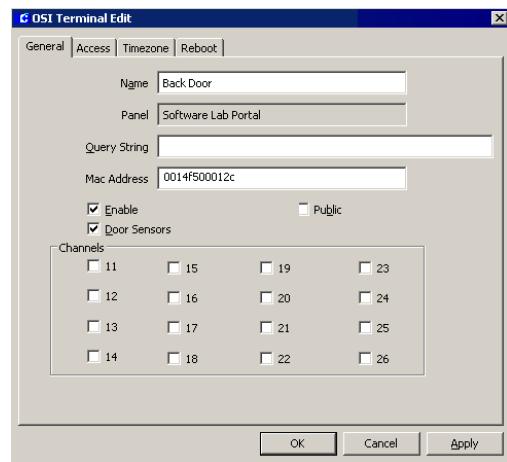
After you create the OSI reader terminal, the system automatically creates three soft input points: *Low Battery*, *Tamper*, and *Term Down*. These input points display under the **Input Points** icon as *Low Battery <reader name>*, *Tamper <reader name>*, and *Term Down <reader name>*. If you wish to report the associated alarms, edit the input point and make sure the **Disable Alarm** option is not selected in the General tab of Alarm Options, otherwise the alarm will not report to the Alarm Queue, but will continue to report to the Real Time List (see “Alarm Options Tab” on page 97). Also, if you rename the reader, you must edit the input point to manually enter the new reader name, as in *Term Down <reader name>*.

Note: The Tamper alarm for OSI soft input points is generated after five consecutive invalid credential attempts.

OSI Terminal Field Definitions

General Tab

Use this tab to enter general descriptive information of the OSI reader.



Name – Enter a descriptive Name for the terminal. By default the Name field displays the MAC address of the reader but you can change the name according to your facility needs.

Panel – This field displays the name of the portal you selected from the System Configuration window, which provides the wireless communication to the reader.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Mac Address – This field displays the Media Access Control address automatically assigned to the reader.

Enable – Select this check box if you wish the system to recognize this terminal.

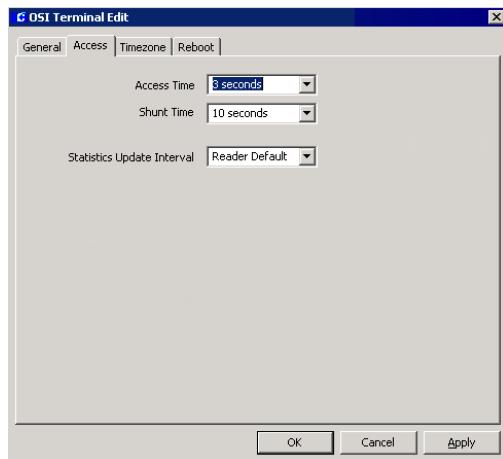
Public – If you use Partitioning, select this check box if you wish this terminal to be visible to all partitions.

Door Sensors – Select this check box if your reader has the optional Door Sense Module for monitoring of the actual strike status.

Channels – Select the Radio Frequency (RF) channels or frequency bands that this terminal will use to communicate with the readers.

Access Tab

This tab defines the OSI reader's time parameters.



Access Time – Select the amount of time that the door will remain unlocked to provide access.

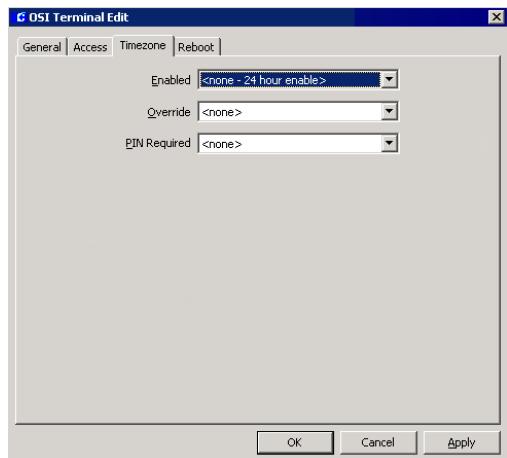
Shunt Time – Select the amount of time that the door alarm will be suppressed to allow access at the door. The Shunt Time should be longer than the Access Time.

Statistics Update Interval – Select the frequency at which the reader will send messages to the portal gateway with signal strength, battery voltage, external supply voltage and packet transfer ratio information.

Note: *The smaller the interval, the greater the battery use. For a high volume area, you may want to keep the interval time at 1 minute to ensure adequate coverage. (You will need to monitor battery use to ensure adequate power supply.) However, for little used areas, you can set the update interval up to 24 hours to preserve battery life.*

Timezone Tab

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



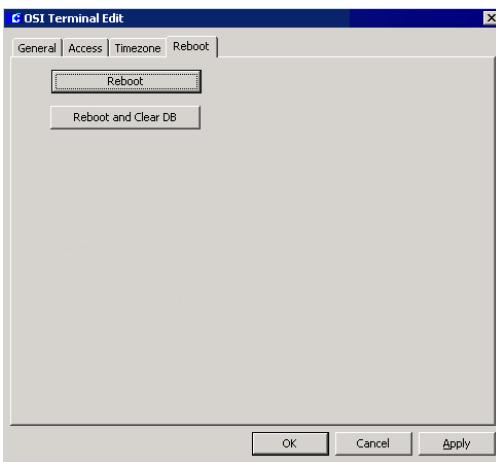
Enabled – Select from the drop-down list, the Time Zone during which the reader will allow access. If you do not wish to enable this function, select **<none - 24 hour enable>** to allow access at all times.

Override – Select a time zone from the drop-down list during which the reader does not require a badge to open the door.

PIN Required – Select a time zone from the drop-down list during which cardholders are required to enter a PIN number.

Reboot Tab

At times it may be necessary to use this tab to reset the reader. This would typically happen only if you were to take the reader offline, for example to change batteries.



Reboot – Click this button to reset the reader.

Reboot and Clear DB – Click this button to reset the reader and temporarily clear current reader data.

Note: After you click one of the above buttons, a “Reader Cleared” message will display in the Real Time List. The total time for these operations to complete and the time it takes for the corresponding message to display in the Real Time List will vary due to the wireless nature of the system.

Viewing OSI Wireless Devices Status

The System Status window displays the current status of all OSI devices that have been configured in the system. It also allows you to view portal and reader values related to the wireless signal they receive.

Refer to “System Status” on page 439 for instructions on how to display the status of OSI devices.

Rebuilding the WAMS Database

Under certain conditions, it may be necessary to rebuild the WAMS database of the OSI system. An example might be if the Server hard disk fails and must be replaced. If a database backup of the WAMS database is not available, it can be fully repopulated from the data contained in the P2000 database.

You will have to run again the P2000 installation, which in turn will cause the OSI Web Service installation to be run. The OSI Web Service installation will recreate a “blank” WAMS database as part of its installation process. To repopulate the WAMS database, simply open the P2000 Download application and download all items to all OSI panels. This will repopulate the WAMS database with all of the necessary data.

Refer to “Downloading Data to Panels” on page 429 for instructions on how to download items to OSI panels.

In addition, if you recreate or restore the WAMS database backup, you will have to perform the *Synchronize OSI Transaction Counter* action from the Database Maintenance dialog box, to set the P2000 OSI transaction counter to the last transaction currently in the OSI WAMS database, see page 449 for details.

Configure S321-IP Panels and Components

Use this section to configure your P2000 system to communicate with S321-IP panels. S321-IP panels communicate with the P2000 Server using a standard TCP/IP network protocol to provide badge access, alarm monitoring, history reporting, input/output linking, and card and system activated events.

The S321-IP is an advanced, intelligent, network panel capable of monitoring and controlling one or two fully-configured doors. The S321-IP panel provides the ability to configure supervised 4-state inputs and unsupervised 2-state inputs. When interfacing to a single door, you can configure the unused points as general purpose input/output points.

It is assumed that the S321-IP hardware is already connected to the P2000 Server before you can configure and use the functions described in this section. Refer to the *S321-IP Network Controller Hardware Installation Manual* for hardware installation instructions.

S321-IP Naming Conventions

S321-IP panel components are named using a consistent naming scheme. Terminals, input, and output point are automatically allocated an identifying name. This name comprises a fixed description of the item (such as Term 1 for terminals or Panel Battery for inputs), plus the panel name. In the case of terminal input and output points, the name of the terminal is also appended to the input and output names, that way, an input point for example, is recognized by its panel and terminal name.

You should logically name S321-IP panels, including information such as a panel's location or what it controls, but bear in mind that the maximum number of characters allowed in an S321-IP component name is 32. When you use long panel names, you need to remember that a terminal input point will be named as <input name> <terminal name> <panel name> and therefore, that combination should not exceed 32 characters. If the combination does exceed 32 characters the resulting name will be truncated to 32 characters.

Configure S321-IP Panels

To enable communication between the S321-IP panel and the P2000 Server, you have to configure the connection at both sides. First, you need to define the P2000 Server at the S321-IP panel, and then you need to enter the S321-IP information in the P2000 S321-IP Panel Edit dialog box.

Note: You must generate a Certificate using the S321-IP user interface to enable encrypted communications between the P2000 Server and the S321-IP panel.

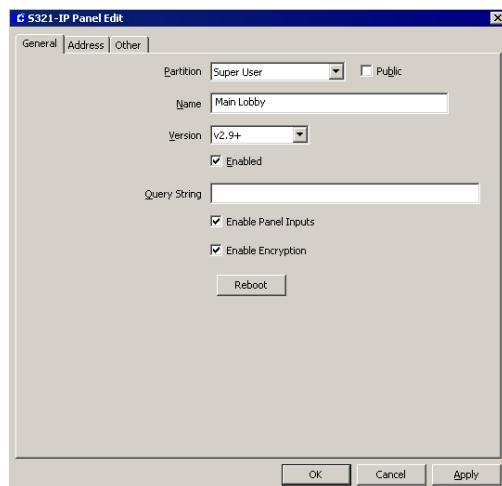
Refer to the *S321-IP Configuration and Operation Manual* to prepare the S321-IP panel for integration with the P2000 system.

Note: Due to S321-IP requirements, there must be at least one time zone available prior to creating or editing an S321-IP panel.

To Configure S321-IP Panels:

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 **Panels** icon.
3. Select the **S321-IP Panels** icon and click **Add**. The S321-IP Panel Edit dialog box opens.
4. Fill in the information on each tab. (See S321-IP 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 the panel information. 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 72.
7. If you select **Yes**, the time zones will be automatically added. When you return to the System Configuration window, a new S321-IP Panel icon bearing the name assigned will display under the root S321-IP Panels.

Note: In addition to applying time zones to the panels (described in “Configure Panel Time Zones” on page 72), you may also define panel holidays if you wish to restrict access in your facility during a holiday period, see “Configure Panel Holidays” on page 73.

S321-IP Panel Field Definitions**General Tab**

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

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. See “S321-IP Naming Conventions” on page 141 for more information.

Version – Select the firmware version of the S321-IP panel. Certain features will be enabled or disabled depending on the panel version selected.

Note: If you upgrade the panel firmware, you must edit the version field to match the updated panel's firmware. If the versions do not match, the panel will be put into a misconfigured state and will not be allowed to fully communicate until the problem is resolved.

Enabled – The system will not recognize the panel unless you select the Enabled check box.

If you wish to temporarily disable the panel, without having to delete the panel, 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 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Enable Panel Inputs – Select this check box to create two panel soft input points: Panel Tamper and Power Failure.

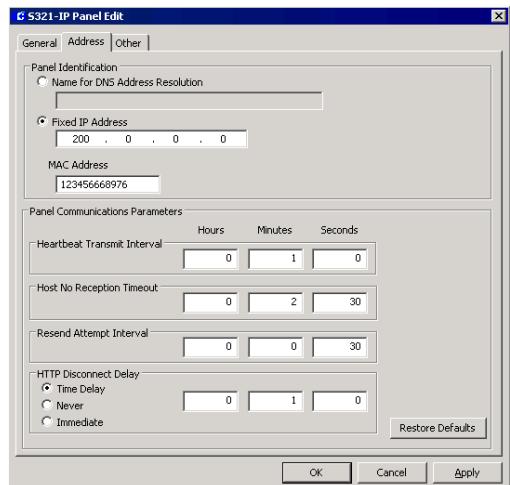
Enable Encryption – Select this check box to allow encryption of all messaging between S321-IP panels and the P2000 Server.

Note: To use encrypted communications, you must also configure the SSL settings at the S321-IP panel.

Note: You must disable the **Enable Encryption** option when performing the S321-IP firmware upgrade process. After the panel is updated, you can enable the encryption option again.

Reboot – Click this button to reboot the S321-IP panel. The Reboot button is provided to force the panel to restart, for example in cases when the panel is not functioning properly. This feature is available after you save the panel information.

Address Tab



Name for DNS Address Resolution – Click the radio button and enter the name assigned to the S321-IP panel. This name is used to communicate with the panel instead of the IP address if the Domain Name Server (DNS) is present on the network. This field must exactly match the S321-IP name defined using the S321-IP panel user interface.

Fixed IP Address – If your facility uses fixed IP addresses, click the radio button and enter the IP address assigned to the S321-IP panel.

MAC Address – Enter the Media Access Control (MAC) address assigned to the S321-IP panel.

Note: Changes to any of the following Panel Communication Parameters will cause the panel to go down and then up again.

Heartbeat Transmit Interval – Enter the number of hours, minutes, and/or seconds that determines how often the S321-IP panel will send “keepalive” messages to the P2000 system.

Host No Reception Timeout – Enter the number of hours, minutes, and/or seconds that must pass without receiving any notification, before

the P2000 system assumes the S321-IP panel is no longer available. If this value is set below 60 seconds, P2000 may report the S321-IP offline when a large number of badges are downloaded, due to S321-IP internal processing.

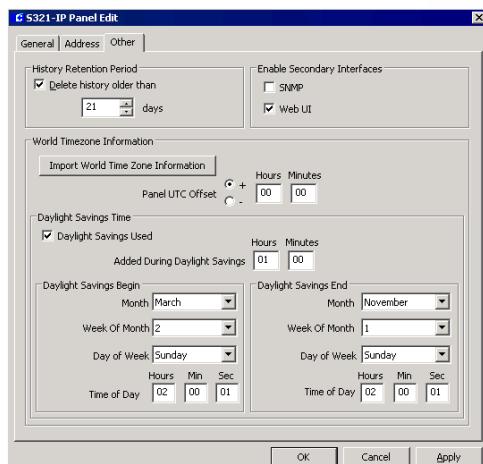
Resend Attempt Interval – Enter the number of hours, minutes, and/or seconds to define how long the S321-IP panel will wait before resending a message after the previous attempt failed.

HTTP Disconnect Delay – Determines how long the S321-IP panel will hold on to a connection if there is no activity. Select one of the following options:

- **Time Delay** – Select to tell the S321-IP panel to keep the underlying HTTP connection for the time specified in the Hours, Minutes and Seconds fields.
- **Never** – Select to tell the S321-IP panel to never drop the underlying HTTP connection.
- **Immediate** – Select to tell the S321-IP panel to drop the underlying HTTP connection immediately after each transmission.

Restore Defaults – Click this button if you wish to restore default values of all related communication timed values.

Other Tab



History Retention Period – This setting defines how long the panel retains data in the transaction database before older data is deleted.

Select the **Delete history older than** check box and enter the number of days the panel will hold data before deletion.

Enable Secondary Interfaces – Use this setting if you will use an external device to configure, monitor, and control the S321-IP panel.

- **SNMP** – The Simple Network Management Protocol (SNMP) option is used mostly by network connected devices to report conditions such as a high temperature alarm. You would have to provide a third party device for doing this monitoring.
- **Web UI** – The Web UI option is the interface method necessary for using a Web Browser to communicate with the S321-IP panel.

IMPORTANT: *It would be virtually impossible for the P2000 system to control and monitor the S321-IP panel correctly if you use either of these options to control or configure the S321-IP panel. If you only use SNMP or Web UI to monitor the S321-IP panel, while the P2000 system is in operation, then the risk of problems is greatly reduced, but not eliminated. Do not enable these secondary interfaces unless you need to obtain diagnostic information from the S321-IP panel during system startup, or you wish to monitor certain S321-IP items using SNMP and understand the risks.*

World Timezone Information Box

The information in this box defines time zone-related information and Daylight Savings Time (DST) settings.

Import World Time Zone Information – Click this button to select the time zone information that applies to the panel location.

Panel UTC Offset – Defines time offsets for remote panels, relative to Universal Time. Click the + or – radio button and enter the

appropriate hours and minutes for the time offset.

Daylight Savings Used – When you select a time zone, the system defaults to the standard daylight savings time settings for the selected region, the S321-IP's clock will be automatically adjusted for daylight savings time. If you wish to change the default settings, click the Daylight Savings Used check box and select:

- the Begin and End Month
- the Begin and End Week of Month
- the Begin and End Day of Week
- the Begin and End Time of Day

Added During Daylight Savings – A value of 1 hour is currently the world standard. You cannot change this value.

Configure S321-IP Terminals

The S321-IP panel can control two door terminals, which are automatically created after you configure and save the S321-IP panel. Either or both terminals can be configured as a reader terminal or with all input and output points designated as general purpose input/outputs.

When the terminals are created in the system, they display under the Terminals icon as Term 1 <panel name> and Term 2 <panel name>.

Note: *The Entry/Exit concept is not supported by S321-IP panels. In addition, the S321-IP terminal only supports Local access operation. Refer to Appendix C: Panel Comparison Matrix for detailed information on the features supported.*

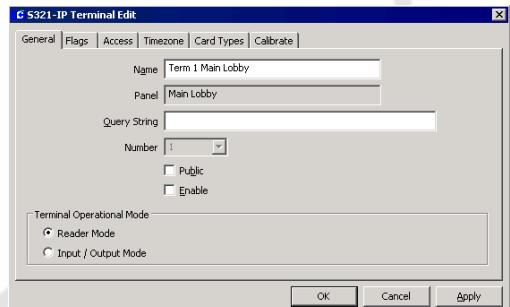
To Configure S321-IP Terminals:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.

2. Click the plus (+) sign next to the **S321-IP Panels** icon to display all S321-IP panels configured in the system.
3. Click the plus (+) sign next to the panel that contains the terminals you wish to configure. All the items that can be configured for the panel are listed under it.
4. Click the plus (+) sign next to the **Terminals** icon, select the terminal you wish to configure and click **Edit**. The S321-IP Terminal Edit dialog box opens at the General tab.
5. Enter the information in each tab according to your system requirements. (See S321-IP Terminal Field Definitions for detailed information.) As you work through the tabs, click **Apply** to save your settings.
6. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window. If you wish to include S321-IP terminals in groups that provide common access, refer to “Create Terminal Groups” on page 91.

S321-IP Terminal Field Definitions

General Tab



Name – This field displays the name automatically assigned to the terminal. You can however enter a different name for the terminal.

Panel – This field displays the name of the S321-IP panel you selected from the System Configuration window.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Number – This field displays the terminal index number (1 or 2). This number corresponds to the terminal index as assigned at the panel.

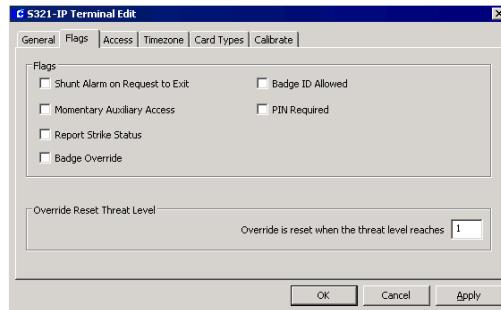
Public – If you use Partitioning, select the Public check box if you wish this terminal to be visible to all partitions.

Enable – Select Enable so the new terminal will be recognized by the system.

Reader Mode – Indicates a card reader terminal. If selected as the Terminal Operational Mode, additional tabs are added. If the Terminal is a reader terminal, only two input points can be utilized.

Input/Output Mode – Indicates a terminal that provides input and output points. In this mode, four input points and four output points can be utilized.

Flags Tab



Shunt Alarm on Request to Exit – If enabled, the system shunts the Request to Exit door alarm

when the system grants access through an auxiliary access point. If the Request to Exit alarm is shunted, the door can be opened and closed for a specific period of time (shunt time defined in the Access tab) after access has been granted. If a door is opened without access being granted, or if the door is held open beyond the alarm shunt time and the alarm signal is not suppressed, the alarm is detected immediately.

Momentary Auxiliary Access – Determines the total access time when a cardholder is entering or exiting a secured area via an auxiliary access point. When enabled, the access time (defined in the Access tab) will begin timing when a switch shorts the door’s auxiliary access input point contact (the door strike will unlock for the number of seconds defined in the Access Time field when the system first detects an entry or exit request through an auxiliary access point). If not enabled, the door’s auxiliary access input point contact will energize the door relay as long as the contact is shorted (the door strike will remain unlocked for the entire auxiliary access time, including the number of seconds defined in the Access Time field).

Report Strike Status – Enable this option if you wish to report the status of the door strike associated with the selected reader.

Badge Override – If enabled, cardholders with their badge’s Override option enabled can unlock the door controlled by the selected reader for a specified time period.

Badge ID Allowed – If enabled, a cardholder may enter the number of his/her badge onto a keypad to access a secured area. This feature enables cardholders who have forgotten their badge the opportunity to gain entry by keying in their badge number.

PIN Required – If enabled, all cardholders must enter a custom PIN on the selected reader when attempting to access a secured area.

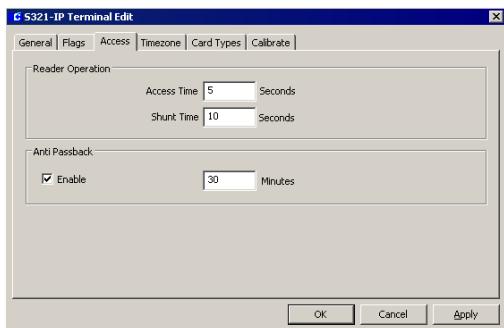
Override Reset Threat Level Box

Each reader terminal defined for an S321-IP panel can be configured with an Override Reset Threat Level ranging between 0 and 99.

Whenever a terminal's Security Level reaches or exceeds the terminal's Override Reset Threat Level, all overrides are immediately disabled. Subsequent attempts to invoke overrides will be denied.

All overrides will be restored once a terminal's Security Level drops below the terminal's Override Reset Threat Level. For more information, see "Security Threat Level Control" on page 277.

Access Tab



Access Time – Enter the time (in seconds) that the door strike remains energized after a cardholder presents a valid badge at the selected reader. The cardholder will have up to 60 seconds to open the unlocked door before it re-locks when the access time elapses.

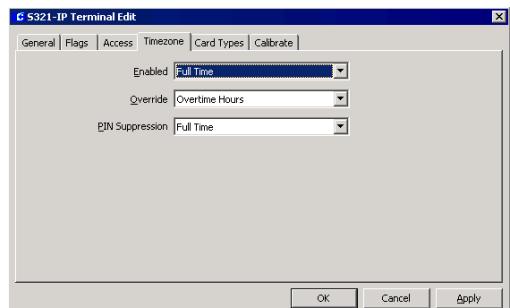
Shunt Time – Enter a time in seconds that the door open alarm is suppressed after a valid badge access request. The Shunt Time should be longer than the Access Time.

Anti Passback – This feature prevents unauthorized persons from using the badge of an authorized cardholder to gain access to a controlled area. Once an authorized cardholder

presents a valid badge to access the facility, he cannot access the facility again until the anti-passback time entered expires.

Timezone Tab

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



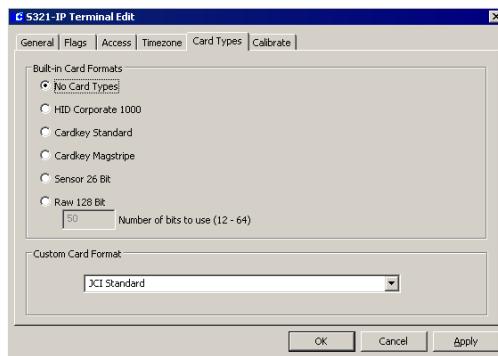
Enabled – Select a time zone from the drop-down list during which the terminal will be active. For example, you may not want the reader to be used between midnight and 5:00 AM, so assign a time zone with the desired inactive time period. If you select <none>, the terminal will always be active and will allow unrestricted access.

Override – Select a time zone from the drop-down list that can be set as an override for this terminal. If you select <none>, this terminal is never in override.

PIN Suppression – Select a time zone from the drop-down list during which cardholders do not have to enter a PIN number. If you select <none>, cardholders are never required to enter their PIN number.

Card Types Tab

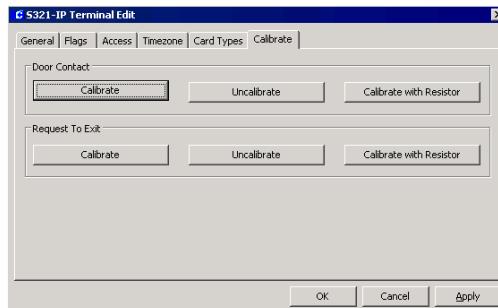
This tab determines which card type can be used at the selected reader. If a presented badge does not match the selected card type, the system will deny access to the cardholder.



- The S321-IP panel supports one built-in card type at a time, therefore select only one card type.
- Select **No Card Types** if this reader is disabled.
- The **Sensor 26 Bit** card format is compatible with the 26-bit Wiegand Inverted card format.
- If you select **Raw 128 Bit**, enter the Number of bits to use (12 - 64).
- If your facility uses **Custom Card Formats**, select from the drop-down list one of the formats previously downloaded into the panel using the Panel Card Formats application, see page 75 for detailed instructions.

Calibrate Tab

Use this tab to calibrate door contact input points as well as auxiliary access input point contacts on the terminal.



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

Calibrate – This command calibrates the S321-IP's selected input point contacts without using the panel's CAL RESISTOR points. Issuing this command determines the door's secure state and sets the selected input point as supervised (4-state).

Note: A "Reader Status Input Fault" message will display in the Real Time List when Door Contact or Exit Request 4-state inputs are opened or shorted.

Uncalibrate – This command uncalibrates the selected input point and sets it as unsupervised (2-state). After you uncalibrate the input point, four-state input statuses will no longer be available for the input, only two-state statuses.

Calibrate with Resistor – This command calibrates the S321-IP's selected input point contacts using the panel's CAL RESISTOR points. Issuing this command determines the door's secure state and sets the selected input point as supervised (4-state). Calibrating the input point based on the CAL RESISTOR points does not require the door to be in the secure state during the calibration process.

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

Configure S321-IP Input Points

S321-IP Panel and Terminal applications automatically generate input points and their addresses. These input points can be enabled to indicate the current state of a device and can be used for alarm or non-alarm purposes.

Some S321-IP input points have a predefined and unchanging purpose – indicating panel power failure and low battery power. When terminals are enabled, some input points are dedicated to access control functions, such as receiving input from door contacts and REX devices. Other input points can be used for a variety of purposes and devices (motion sensors, tamper switches, etc.) – these input points are referred to as general purpose inputs. The number of terminals enabled determines the available number of general purpose inputs.

Panel input points are automatically created under the selected S321-IP panel and are named using the input name and <panel name>, as in “Power Failure <panel name>.” Terminal input points are created under the selected S321-IP terminal and are named using the input name and <terminal name> <panel name>, as in “Forced Door <terminal name> <panel name>.” If you rename the panel or terminal, you can edit the input point to manually enter the new panel or terminal name.

The following possible input points are available:

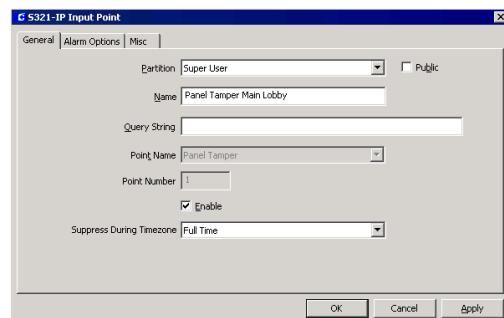
Input Type	Input Name	Generated for...	Description
Panel Inputs	Panel Tamper	S321-IP panels with the Enable Panel Inputs option selected.	General purpose input. Typically wired to a tamper switch on an enclosure to indicate tampering.
	Power Failure		With battery backup employed, this input point indicates power failure.
Panel Soft Inputs	Panel Battery	All S321-IP panels.	With battery backup employed, this input point provides a low battery indication during power failure.
	Clock Battery		Indicates when the panel's lithium battery, which is used to back up the real-time clock, is low.
	Panel Down		Internal to P2000 to indicate that the panel is not active.
Terminal Inputs	Forced Door	S321-IP terminals with the Reader Mode option selected.	Indicates when there is a door open condition without a valid badge read detected first.
	Propped Door		Indicates when there is a door open condition with a valid badge, but the door is left open past the entry time.
	Door Contact	S321-IP terminals with the Input/Output Mode option selected.	In Reader Mode, this input point receives input from the door contact associated with the terminal. In Input/Output Mode, this input point can be used as a general purpose input.
	Exit Request		In Reader Mode, this input point receives input from the REX device associated with the terminal. In Input/Output Mode, this input point can be used as a general purpose input.
	Spare	All S321-IP terminals.	General purpose input.
	Tamper		General purpose input.
	Term Down		Internal to P2000 to indicate that panel communications have ceased.

To Configure S321-IP Inputs:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.
2. Click the plus (+) sign next to the **S321-IP Panels** icon to display all S321-IP panels configured in the system.
3. Click the plus (+) sign next to the panel that contains the input points you wish to configure.
 - To configure panel inputs, click the plus (+) sign next to the **Input Points** icon, select the input point you wish to configure and click **Edit**.
 - To configure terminal inputs, click the plus (+) sign next to the terminal that contains the input point you wish to configure, then click the plus sign next to the **Input Points** icon, select the input point you wish to configure and click **Edit**.

The S321-IP Input Point dialog box opens at the General tab.

4. Enter the information in each tab according to your system requirements. The fields available for configuration depend on the type of input point selected. (See S321-IP Input Point Field Definitions for detailed information.) As you work through the tabs, click **Apply** to save your settings.
5. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window.

S321-IP 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 – This field displays the name automatically assigned to the input point, which consists of the <point name> <panel name>; the <terminal name> will display for terminal inputs. If you wish to change it, enter a descriptive name for the input point.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

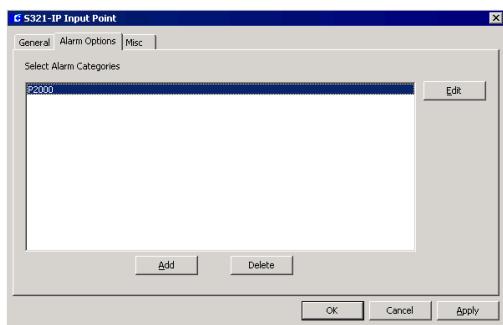
Point Name – Displays the point name defined by the S321-IP panel.

Point Number – Displays the number associated with the input point. This number represents the physical connection to the I/O terminal.

Enable – Select this check box to report all input point changes of state. Do not select the check box if you do not want these changes reported.

Suppress During Timezone – 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. This option is not available for Panel Down, Forced Door, Propred Door, and Term Down input points.

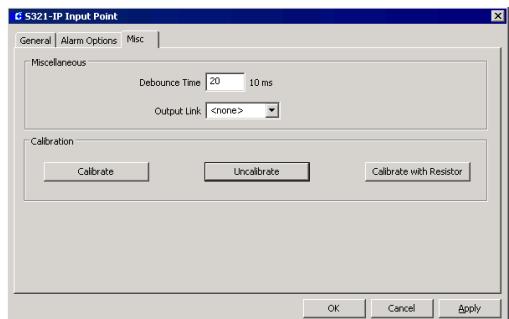
Alarm Options Tab



Alarm options are described in detail on page 97.

Misc Tab

Settings in this tab are not available for Panel Down, Forced Door, Propred Door, and Term Down input points.



Debounce Time – Enter the time in tens of milliseconds that the input must remain in a transition state to establish the detected state. Without a debounce time, the panel may detect that the input is in an incorrect state due to the “bouncing” of the input device’s contacts.

Output Link – This option links the input point to an output point, so that the output point can be triggered by a change in the input point’s state. For example, when an input point, such as a motion sensor, is tripped (the input point state changes from secure to alarm), an output point triggers an external device (a light is turned on). Select from the drop-down list, the number of the output point that will be triggered by the selected input point. The list display the output point number preceded by the terminal number, as in <terminal number>-<output number>.

Calibrate – This command calibrates the S321-IP’s selected input point contacts without using the panel’s CAL RESISTOR points. Issuing this command determines the door’s secure state and sets the selected input point as supervised (4-state).

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

Uncalibrate – This command uncalibrates the selected input point and sets it as unsupervised (2-state). After you uncalibrate the input point, four-state input statuses will no longer be available for the input, only two-state statuses.

Calibrate with Resistor – This command calibrates the S321-IP's selected input point contacts using the panel's CAL RESISTOR points. Issuing this command determines the door's secure state and sets the selected input point as supervised (4-state). Calibrating the input point based on the CAL RESISTOR points does not require the door to be in the secure state during the calibration process.

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

Configure S321-IP Output Points

S321-IP output points are automatically created under terminals that operate with the Input/Output Mode enabled. These output points are used to trigger external devices using the S321-IP panel. These devices might include warning indicators for alarm situations or non-alarm related functions, such as lighting or environmental control.

When the terminal operates in Reader Mode, the output points are dedicated to access control functions, such as controlling the door strike, shunting an alarm, and turning green and red LEDs on and off to indicate access granted or denied.

If the terminal operates in Input/Output Mode, the output points that were used by the reader can be used to trigger external devices, such as lights and sirens – these output points are referred to as general purpose outputs.

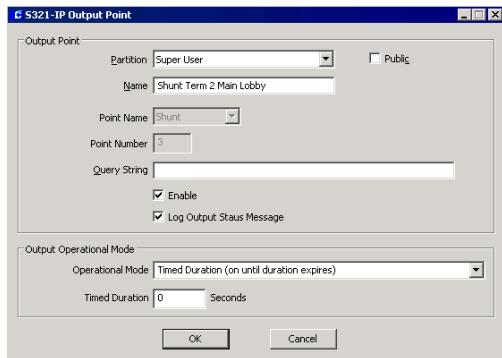
Output points are created under the selected S321-IP terminal and are named using the output name and <terminal name> <panel name>, as in "Shunt <terminal name> <panel name>." If you rename the panel or terminal, you can edit the output point to manually enter the new panel or terminal name.

The following possible output points are available:

Output Name	Description
Green	If the terminal is enabled, this output point controls a green LED associated with the terminal. When access is granted, this output is activated. If the terminal is disabled, this output point can be used as a general purpose output.
Red	If the terminal operates in Reader Mode, this output point controls a red LED associated with the terminal. When access is denied, this output is activated. If the terminal operates in Input/Output Mode, this output point can be used as a general purpose output.
Shunt	If the terminal operates in Reader Mode, the alarm shunt prevents the external alarm system from sounding an alarm when a valid access occurs. When a valid access occurs, the shunt relay is energized for the number of seconds entered in the Shunt Time field on the Access tab of the S321-IP Terminal Edit application. If the terminal operates in Input/Output Mode, this output point can be used as a general purpose output.
Strike	If the terminal operates in Reader Mode, the door strike controlled by the terminal will unlock for the number of seconds entered in the Access Time field on the Access tab of the S321-IP Terminal Edit application. If the terminal operates in Input/Output Mode, this output point can be used as a general purpose output.

To Configure S321-IP Outputs:

1. In the System Configuration window, locate the S321-IP terminal that contains output points.
2. Click the plus (+) sign next to the **Output Points** icon, select the output point you wish to configure and click **Edit**. The S321-IP Output Point dialog box opens.



3. If you use partitions, select the appropriate **Partition** that will have access to this output point.
4. If you use partitions, click the **Public** check box if you want this output point to be visible to all partitions.
5. The **Name** field displays the name automatically assigned to the output point, which consists of the <point name> <terminal name> <panel name>. If you wish to change it, enter a descriptive name for the output point.
6. The **Point Name** field displays the point name defined by the S321-IP panel.
7. The **Point Number** field displays the number associated with the output point. This number represents the physical connection to the I/O terminal.
8. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasy integration feature

(refer to “Configuring Hardware Components for BACnet Interface” on page 347).

9. Select the **Enable** check box to allow the output point to be activated or deactivated.
10. Select the **Log Output Status Message** check box if you want the status of the output point to display in the Real Time List and the System Status window.
11. Select from the **Operational Mode** drop-down list, one of the following options:

Latched (on until turned off, off until turned on) – to command the output point to be “set” and remain active, until commanded to be “reset.”

Latched with Fast Flash (flashes until turned off) – to toggle the output point on and off quickly (once per second).

Latched with Slow Flash (flashes until turned off) – to toggle the output point on and off slowly (once per two seconds).

Timed Duration (on until duration expires) – to turn on the output point for the time specified in the Timed Duration field.

Timed Duration with Fast Flash (flashes until duration expires) – to toggle the output point on and off quickly for the time specified in the Timed Duration field.

Timed Duration with Slow Flash (flashes until duration expires) – to toggle the output point on and off slowly for the time specified in the Timed Duration field.

12. If you selected any of the Timed Duration operational modes, enter a **Duration** in seconds.
13. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window.

Configure Isonas Panels and Components

This section describes the P2000 integration with Isonas RC-02 single door controllers. The Isonas panel has been designed using IP standards and technology with direct connectivity to the network and Power over Ethernet (PoE) built-in. Once installed, the readers use TCP/IP to communicate with the network and respond to specific commands and parameters. This allows access to be changed and maintained from anywhere at any time via the network.

It is assumed that the Isonas hardware has been properly installed and configured to communicate with the P2000 Server before you can use the functions described in this section. Refer to the *PowerNet IP Reader Hardware Installation Manual* for instructions.

IMPORTANT: This release of P2000 works with Isonas readers that use firmware of Freescale 9.21 and PIC 3.08. Other versions may not be compatible with this release of P2000.

Configure Isonas Panels

After you install the Isonas hardware and assign a static IP address, you are ready to configure the P2000 Server to communicate with the Isonas panel. You should logically name the Isonas panel, including information such as the panel's location or what it controls. Optionally, you can configure P2000 to secure each and every message to and from the Isonas panel using Advanced Encryption Standard (AES) to protect the P2000 system from unauthorized sources.

To Configure Isonas Panels:

- 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 **Panels** icon.
- Select the **Isonas Panels** icon and click **Add**. The Isonas Panel Edit dialog box opens.



- If you use Partitioning, select from the drop-down list, the **Partition** that will have access to this panel.
- If you use Partitioning, select the **Public** check box to allow all partitions to see this panel.
- Enter a descriptive **Name** for the panel.
- The **Enabled** check box is automatically selected for the system to recognize this panel. If you wish to temporarily disable the panel, without having to delete the panel, select the check box to disable it. When you disable a panel, the reader will continue to grant access, but the panel will not communicate with the Server until you enable the panel again.
- The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasya integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).
- Enter the **IP Address** assigned to the Isonas panel.

10. From the **Heartbeat Interval** spin box, select the number of seconds that determines how often the P2000 system will send heart beat messages that flash the LEDs on the reader to confirm continuous successful communication.
11. Select the **Encryption Enabled** check box to allow encryption of all messaging between the Isonas panel and the P2000 Server.
12. If you choose to enable encryption, you must click the **Create** button to generate a random Isonas encryption key.
13. The **Encryption Key** box will display the hexadecimal characters generated. The box on the right side displays the number of characters in the encryption key. There should always be exactly 64 characters
14. Click **OK** to save the panel information. 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 72.
15. If you select **Yes**, the time zones will be automatically added. When you return to the System Configuration window, a new panel icon bearing the name assigned will display under the root Isonas Panels.

Note: In addition to applying time zones to the panels (described in “Configure Panel Time Zones” on page 72), you may also define panel holidays if you wish to restrict access in your facility during a holiday period, see “Configure Panel Holidays” on page 73.

Configure Isonas Terminals

The Isonas RC-02 panel controls a single door terminal, which is automatically created after you configure and save the Isonas panel information. The Isonas terminal is a reader termin-

nal which consists of four input points and two TTL output points. These components are named using a consistent naming scheme. The terminal name is comprised of the panel name plus the word “Reader” and may be included in Terminal Groups that provide common access.

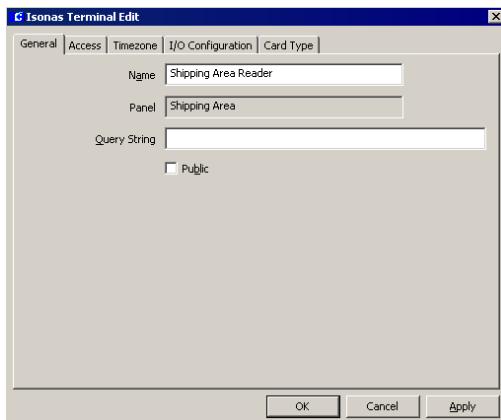
Note: The Entry/Exit concept is not supported by Isonas panels. In addition, the Isonas terminal only supports Local access operation. Refer to the Appendix C: Panel Comparison Matrix for detailed information on the features supported.

To Configure Isonas Terminals:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.
2. Click the plus (+) sign next to the **Isonas Panels** icon to display all Isonas panels configured in the system.
3. Click the plus (+) sign next to the panel that contains the terminal you wish to configure. All the items that can be configured for the panel are listed under it.
4. Click the plus (+) sign next to the **Terminals** icon, select the terminal and click **Edit**. The Isonas Terminal Edit dialog box opens at the General tab.
5. Enter the information in each tab according to your system requirements. (See Isonas Terminal Field Definitions for detailed information.) As you work through the tabs, click **Apply** to save your settings.
6. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window. If you wish to include Isonas terminals in groups that provide common access, refer to “Create Terminal Groups” on page 91.

Isonas Terminal Field Definitions

General Tab



Name – This field displays the name automatically assigned to the terminal. You can however enter a different name for the terminal.

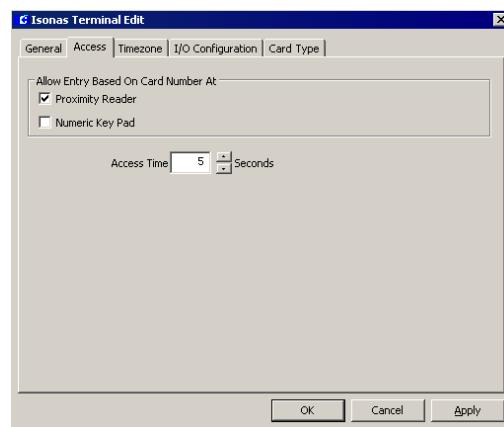
Panel – This field displays the name of the Isonas panel you selected from the System Configuration window.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Public – If you use Partitioning, select the Public check box if you wish this terminal to be visible to all partitions.

Access Tab

Door access will be allowed based on the parameters selected here.



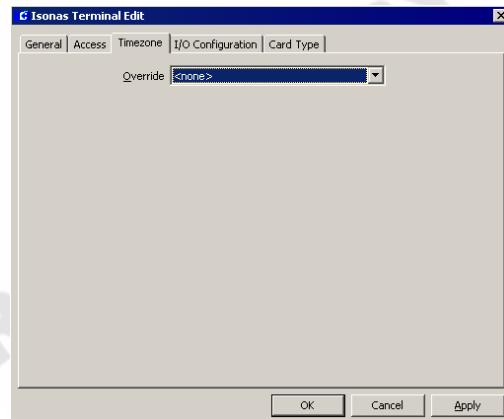
Proximity Reader – Select this check box to enable this reader as a proximity reader.

Numeric Key Pad – Select this check box to enable this reader as a keypad reader. If enabled, a cardholder must enter the badge number followed by the <#> key.

Access Time – Select from the spin box the time (in seconds) that the door remains unlocked after a cardholder presents a valid badge at this reader.

Timezone Tab

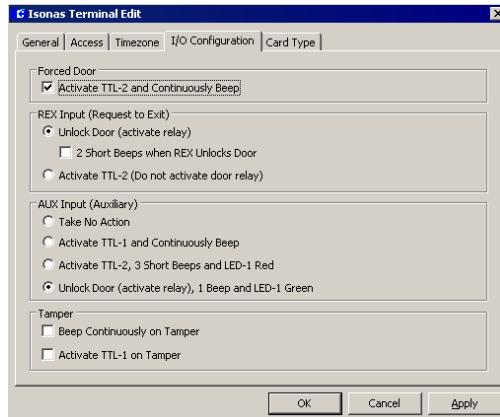
This tab defines the time zone during which this reader door will not be locked.



Override – Select a time zone from the drop-down list that can be set as an override for this terminal.

I/O Configuration Tab

Settings in this tab define how the reader's inputs and outputs will behave when activated.



Forced Door

A Forced Door condition occurs when a door is opened without a valid badge read detected first.

Activate TTL-2 and Continuously Beep – Select this option to activate the TTL-2 defined output when the forced door condition is reported. The reader will beep continuously.

REX Input (Request to Exit)

A Request to Exit (REX) Input is a signal received from a REX device associated with the reader, which prompts the reader to unlock the door without setting off the alarm.

Unlock Door (activate relay) – Select this option to unlock the door upon receiving a REX Input signal. The relay will be activated to unlatch the door. If you select this option, you can enable the **2 Short Beeps when REX Unlocks**

Door option if you wish the reader to beep upon activation.

Activate TTL-2 (Do not activate door relay)

Select this option to activate the TTL-2 defined output upon receiving a REX Input signal. This option does not activate the relay to unlatch the door.

AUX Input (Auxiliary)

An Auxiliary (AUX) Input is a signal received from an auxiliary device associated with the reader, such as a device controlled by a relay on an intercom at the door, a push button switch or a motion sensor.

Take No Action – Select this option if you do not want the reader to perform any special action.

Activate TTL-1 and Continuously Beep – Select this option to activate the TTL-1 defined output upon receiving the AUX Input signal. The reader will beep continuously.

Activate TTL-2, 3 Short Beeps and LED-1 Red – Select this option to activate the TTL-2 defined output upon receiving the AUX Input signal. The reader will emit 3 short beeps and the red LED will be lit.

Unlock Door (activate relay), 1 Beep and LED-1 Green – Select this option to unlock the door upon receiving the AUX Input signal. The relay will be activated to unlatch the door. The reader will emit 1 beep and the green LED will be lit.

Tamper

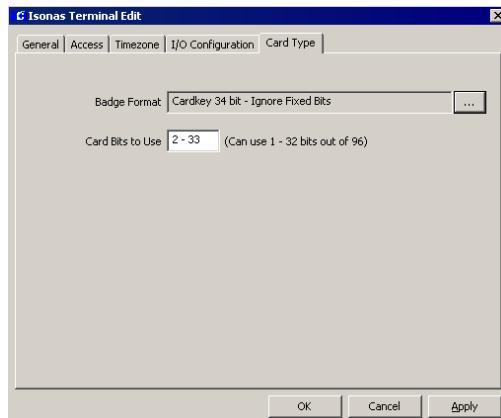
A tamper signal is received from a tamper switch on the reader to indicate a tamper condition if for example, the reader has been disturbed or removed from the wall.

Beep Continuously on Tamper – Select this option to send a continuous beep upon receiving a tamper signal.

Activate TTL-1 on Tamper – Select this option to activate the TTL-1 defined output upon receiving a tamper signal.

Card Type Tab

This tab determines which card type can be used at the selected reader. If a presented badge does not match the selected card type, the system will deny access to the cardholder.



Badge Format – Click the [...] button and select the badge format to be used by this reader. The P2000 software provides badge formats that are located in the \Program Files\Johnson Controls\CARDKEY P2000\BadgeFormats folder. If a different format is needed, create a new badge format file by using the P2000 Badge Format tool, see page 182 for details.

Note: On 64-bit Windows operating systems use \Program Files (x86)\Johnson Controls\ P2000\BadgeFormats folder.

Card Bits to Use – Enter the range of card bits to be used at this reader. Isonas readers limit the card formats to a maximum of 32 bits of the card data.

Configure Isonas Input Points

Isonas input points are automatically generated after you create and save the Isonas panel information. These input points are used to monitor external devices connected to the Isonas reader and can be used to generate alarms, either when the input is activated or if the tamper switch in the equipment is activated. Isonas input points are named using the input name plus the panel name, if you rename the panel, you can edit the input point to manually enter the new panel name. Refer to “I/O Configuration Tab” on page 157 to see how the reader’s inputs will behave when activated.

The following input points are available:

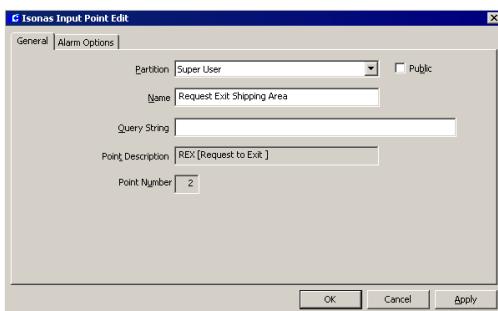
Input Type	Input Name	Description
Panel Soft Input Point	Panel Down	Internal to P2000 to indicate that the panel is not active.
Terminal Input Points	Aux Input	This input point receives input from the auxiliary device associated with the reader.
	Forced Door	Indicates when there is a door open condition without a valid badge read detected first.
	Request Exit	This input point receives signal from the REX device associated with the reader.
	Tamper	General purpose input. Typically wired to a tamper switch to indicate tampering.
	Terminal Down	Internal to P2000 to indicate that panel communications have ceased.

To Configure Isonas Inputs:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.

2. Click the plus (+) sign next to the **Isonas Panels** icon to display all Isonas panels configured in the system.
3. Click the plus (+) sign next to the panel that contains the input points you wish to configure.
 - To configure the panel input, click the plus (+) sign next to the **Soft Input Points** icon, select the input point you wish to configure and click **Edit**.
 - To configure terminal inputs, click the plus (+) sign next to the terminal that contains the input point you wish to configure, then click the plus sign next to the **Input Points** icon, select the input point you wish to configure and click **Edit**.

The Isonas Input Point Edit dialog box opens at the General tab.



4. If you use partitions, select the appropriate **Partition** that will have access to this input point.
5. If you use partitions, click the **Public** check box if you want this input point to be visible to all partitions.
6. The **Name** field displays the name automatically assigned to the input point, which consists of the <point name> plus the <panel name>. If you wish to change it, enter a descriptive name for the input point.

7. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).
8. The **Point Description** field displays the point name defined by the Isonas panel.
9. The **Point Number** field displays the number associated with the input point. This number represents the physical connection to the terminal.
10. As you work through the tabs, click **Apply** to save your settings.
11. To configure alarm options for Isonas input points, click the **Alarm Options** tab and follow the instructions provided on page 97.
12. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window.

Configure Isonas Output Points

Two Isonas output points are automatically generated after you create and save the Isonas panel information. These output points can be activated in response to an activated input point, and are used to trigger external devices, such as alarm warning indicators or emergency lights. Isonas output points are named TTL-1 Output <panel name> and TTL-2 Output <panel name>. If you rename the panel, you can edit the output point to manually enter the new panel name. Refer to “I/O Configuration Tab” on page 157 to see how the reader’s outputs will behave when activated.

To Configure Isonas Outputs:

1. In the System Configuration window, locate the Isonas terminal that contains output points.

- Click the plus (+) sign next to the **Output Points** icon, select the output point you wish to configure and click **Edit**. The Isonas Output Point Edit dialog box opens.



- If you use partitions, select the appropriate **Partition** that will have access to this output point.
- If you use partitions, click the **Public** check box if you want this output point to be visible to all partitions.
- The **Name** field displays the name automatically assigned to the output point. If you wish to change it, enter a descriptive name for the output point.
- The **Point Description** field displays the point name defined by the Isonas panel.
- The **Point Number** field displays the number associated with the output point.
- The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasy integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).
- When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window.

Configure HID Panels and Components

HID Edge readers interface with the P2000 Server using a TCP/IP connection to provide a single-door access control solution. The HID Edge readers are IP-based readers with Power over Ethernet (POE) capabilities and can be initially configured remotely over the network via standard Web browser.

IMPORTANT: This release of P2000 works with HID Edge readers that use firmware version 2.2.7.39. Other versions may not be compatible with this release of P2000.

Hardware Requirements

Before you can use the functions described in this section, the HID hardware must be properly installed and configured to communicate with the P2000 Server. Refer to the HID documentation for hardware installation instructions.

The connection settings are determined by HID guidelines; however, to ensure proper operation with the P2000 system, the following is required:

- If your HID model requires an external reader, we recommend using the following connections:
 - Pwr
 - Gnd
 - Data0
 - Data1
 - GrnLED
 - RedLED (optional)
 - Beeper
 - Hold
- When configuring the HID device via its built-in Web page, you must enter a value (no less than 20 seconds), in the *Here I Am Interval (sec)*: field; otherwise, the reader will not attempt to communicate with the P2000 Server.

HID Panel Naming Conventions

HID panel components are named using a consistent naming scheme. The system automatically allocates an identifying name to the terminal and associated input and output points. This name comprises a fixed description of the item (such as Term 1 for the terminal or Request Exit for an input), plus the panel name. In addition, the name of the terminal is also appended to the input and output names, that way, you can for example recognize an input point by its panel and terminal name.

You should logically name HID panels, including information such as the panel's location or what it controls. The maximum number of characters allowed for an HID component name is 32. If you use long panel names, you need to remember that a terminal input point will be named as <input name> <terminal name> <panel name> and therefore, that combination should not exceed 32 characters.

Configure HID Facility Parameters

Before configuring your HID components, use the following instructions to define facility parameters associated with HID readers.

To Configure HID Facility Parameters:

- 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 **Panels** icon to display the root panel types.
- Click the plus (+) sign next to the root **HID Network Panels** icon to open the HID components.
- Select the **HID Facility** icon and click **Add**. The HID Facility Edit dialog box opens.



- Enter the **Name** of the HID Facility record. This field displays P2000 by default, but you can change the name according to your facility needs.
- Select from the **Extended Access Flag** drop-down list, one of the three special access flags that are used by cardholders with extended access privileges who require special access at a reader. Special access allows a door's access time to be different. The list displays the special access flag names as configured in Site Parameters, see page 41.
- In the **Badge Format** field, click the [...] button and select the format to be used at your facility. The P2000 software provides badge formats that are located in the \Program Files\Johnson Controls\CARDKEY P2000\BadgeFormats folder. If a different format is needed, create a new badge format file by using the P2000 Badge Format tool, see page 182 for details. This field selection is required.

Note: On 64-bit Windows operating systems use \Program Files (x86)\Johnson Controls\P2000\BadgeFormats folder.

- After you enter all the information, click **OK** to save the settings and return to the System Configuration window.

Configure HID Panels

After you install the hardware and use the HID tools to locate and connect to the HID reader, you are ready to configure the P2000 Server to

communicate with the HID device by defining communication and time parameters. In addition, if you wish to protect the P2000 system from unauthorized sources, you can implement encryption using Advanced Encryption Standard (AES) to secure each and every message to and from the HID panel.

To Configure HID Panels:

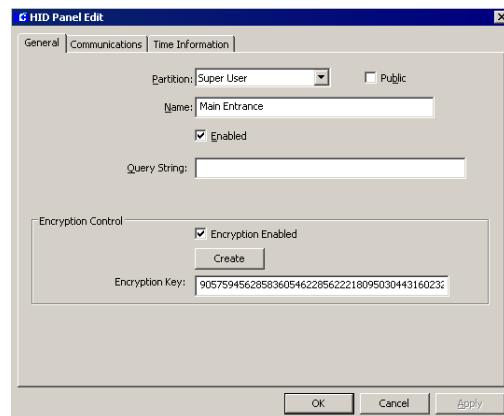
- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the plus (+) sign next to the root **Panels** icon.
- Select the **HID Network Panels** icon and click **Add**. The HID Panel Edit dialog box opens.
- Fill in the information on each tab. (See HID Panel Field Definitions for details.)
- As you work through the tabs, you may click **Apply** to save your entries.
- Click **OK** to save the panel information. 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 72.
- If you select **Yes**, the time zones will be automatically added. When you return to the System Configuration window, a new panel icon bearing the name assigned will display under the root HID Network Panels.

Note: In addition to applying time zones to the panels (described in “Configure Panel Time Zones” on page 72), you may also define panel holidays if you wish to restrict access in your facility during a holiday period, see “Configure Panel Holidays” on page 73.

HID Panel Field Definitions

Note: Changes to any of the following HID Panel parameters will cause the panel to go offline momentarily.

General Tab



Partition – If you use Partitioning, select from the drop-down list, the Partition that will have access to this panel.

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.

Enabled – The Enabled check box is automatically selected for the system to recognize this panel. If you wish to temporarily disable the panel, without having to delete the panel, select the check box to disable it. When you disable a panel, the reader 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 211), and is also used with the

P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

IMPORTANT: *The Encryption Control parameters described below, are not available until the panel information is saved. Communications with the panel must be established in a non-encrypted way before encrypted communications can be established.*

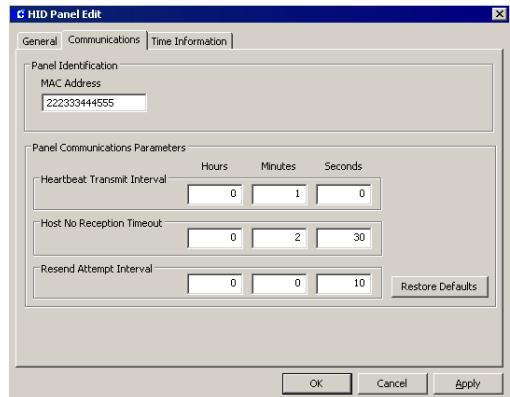
Encryption Enabled – Select this check box to allow encryption of all messaging between the HID panel and the P2000 Server. If you choose to enable encryption, you may click the **Create** button to generate a random HID encryption key, or if you prefer you may enter your own key (not to exceed 200 digits).

The **Encryption Key** box will display the key to be used for encrypted communications.

Important Notes

- When any encryption setting is changed, a warning message displays notifying the user that communications must exist and must not be interrupted while encrypted communications are established or ended.
- Only one encryption setting change can be made using the HID Panel Edit application per session (before the panel information is saved by using the **OK** button). The user must relaunch the HID Panel Edit application to make another change.
- If the user chooses to delete an HID panel from the System Configuration window, and that panel has encryption enabled, a warning message will display indicating the risk involved.

Communications Tab



MAC Address – Enter the Media Access Control (MAC) address assigned to the HID panel.

Heartbeat Transmit Interval – Enter the number of hours, minutes, and/or seconds that determines how often the HID panel will send heart beat messages that confirm successful communication. If you change the heartbeat interval, the panel will be rebooted after the update. You must confirm if you wish to continue.

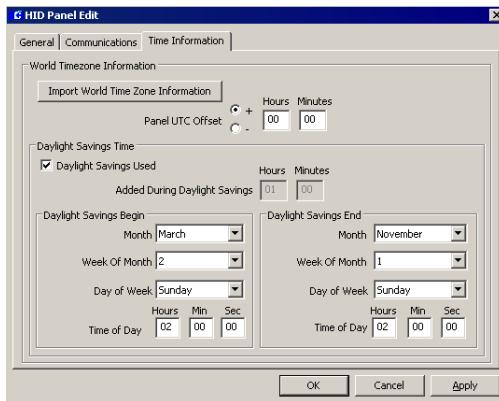
Host No Reception Timeout – Enter the number of hours, minutes, and/or seconds that must pass without receiving a heartbeat notification, before the P2000 system assumes the HID panel is no longer available.

Resend Attempt Interval – Enter the number of hours, minutes, and/or seconds to define how long the HID panel will wait before resending a message after the previous attempt failed.

Restore Defaults – Click this button if you wish to restore default values of all related communication timed values.

Time Information Tab

The information in this box defines time zone-related information and Daylight Savings Time (DST) settings.



Import World Time Zone Information – Click this button to select the time zone information that applies to the panel location.

Panel UTC Offset – Defines time offsets for remote panels, relative to Universal Time. Click the + or – radio button and enter the appropriate hours and minutes for the time offset.

Daylight Savings Used – When you select a time zone, the system defaults to the standard daylight savings time settings for the selected region, the HID's clock will be automatically adjusted for daylight savings time. If you wish to change the default settings, click the Daylight Savings Used check box and select:

- the Begin and End Month
- the Begin and End Week of Month
- the Begin and End Day of Week
- the Begin and End Time of Day

Note: Due to HID limitations, all minutes and seconds values must always be zero.

Added During Daylight Savings – A value of 1 hour is currently the world standard. You cannot change this value.

Configure HID Terminals

The HID panel controls a single door terminal, which is automatically created after you configure and save the HID panel information. The HID terminal is a reader terminal which consists of six input points and one output point. When the terminal is created, it displays under the Terminals icon as Term 1 <panel name>.

Note: The Entry/Exit concept is not supported by HID panels. In addition, the HID terminal only supports Local access operation. Refer to the Appendix C: Panel Comparison Matrix for detailed information on the features supported.

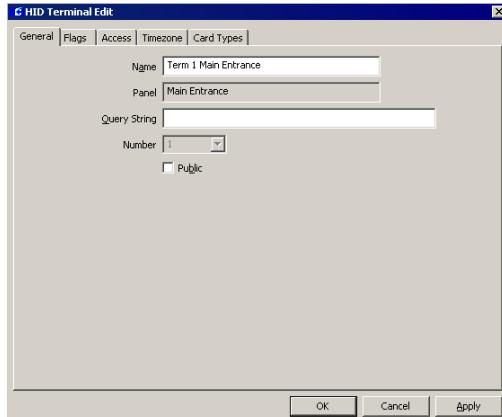
To Configure HID Terminals:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.
2. Click the plus (+) sign next to the **HID Network Panels** icon to display all HID panels configured in the system.
3. Click the plus (+) sign next to the panel that contains the terminal you wish to configure. All the items that can be configured for the panel are listed under it.
4. Click the plus (+) sign next to the **Terminals** icon, select the terminal and click **Edit**. The HID Terminal Edit dialog box opens at the General tab.
5. Enter the information in each tab according to your system requirements. (See HID Terminal Field Definitions for detailed information.) As you work through the tabs, click **Apply** to save your settings.
6. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window. If you wish to include HID terminals in groups that provide common access, refer to “Create Terminal Groups” on page 91.

IMPORTANT: Whenever an HID terminal configuration is downloaded, there is a 7 to 8 second window when a cardholder may gain access even if the enabled time zone does not allow it.

HID Terminal Field Definitions

General Tab



Name – This field displays the name automatically assigned to the terminal. You can however enter a different name for the terminal.

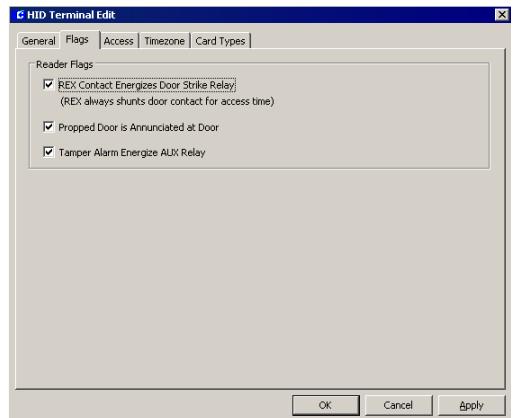
Panel – This field displays the name of the HID panel you selected from the System Configuration window.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Number – This field displays the terminal index number. This number corresponds to the terminal index as assigned at the panel.

Public – If you use Partitioning, select the Public check box if you wish this terminal to be visible to all partitions.

Flags Tab



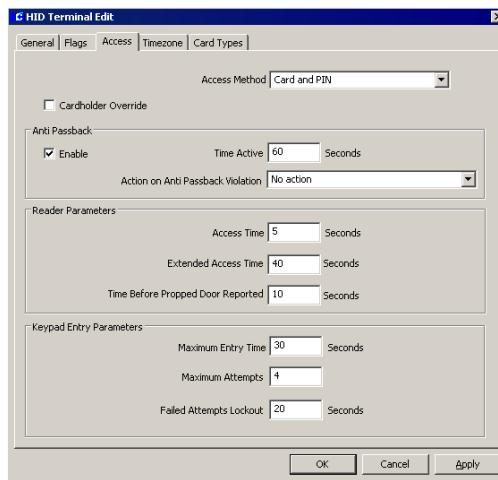
REX Contact Energizes Door Strike Relay (REX always shunts door contact for access time) – If enabled, the Request to Exit (REX) input point will automatically energize the door strike relay (unlock the door) without setting off the alarm. When pressed, the REX input always shunts the door contact for the access time defined. If not enabled, the REX contact will only shunt the door contact.

Proped Door is Annunciated at Door – If enabled, the reader will beep when the propped door condition is reported. A Proped Door condition occurs when a door is opened with a valid badge, but the door is left open past the entry time.

Tamper Alarm Energize AUX Relay – Select this option to activate the auxiliary relay upon receiving a tamper signal. A tamper signal is received from a tamper switch on the reader to indicate a tamper condition if for example, the reader has been disturbed or removed from the wall.

Access Tab

Door access will be allowed based on the parameters selected here.



Access Method – This option defines the type of credentials that must be presented to unlock the door. Select one of the following:

- **Card only** – The cardholder must swipe the badge to gain access.
- **Card and PIN** – The cardholder must swipe the badge and is also required to enter a PIN code. If this option is selected, you must complete the Keypad Entry Parameters settings.
- **Card ID only** – The cardholder must enter the badge number at the keypad. If this option is selected, you must complete the Keypad Entry Parameters settings.
- **Card or Card ID** – The cardholder could either swipe the badge or enter the badge number at the keypad. If this option is selected, you must complete the Keypad Entry Parameters settings.

Cardholder Override – This feature is not available if the Access Method is *Card only*. If Cardholder Override is enabled, an authorized cardholder may place the reader in an override condition by performing a badging procedure at the reader's keypad. The override will remain in effect until:

- An authorized cardholder takes it out of override by performing a badging procedure at the reader's keypad.
- The reader's override timezone enables or disables the door.
- A command is received from the Door Control application to change the door's condition.

The following describes the keypad sequence necessary to unlock the door and return the door to normal operation.

- Depending on the Access Method used (*Card and PIN*, *Card ID only*, or *Card or Card ID*) gain access and enter **9 9 #** to unlock the door.
- Depending on the Access Method used (*Card and PIN*, *Card ID only*, or *Card or Card ID*) gain access and enter **0 0 #** to return the door to normal operation.

Note: HID panels do not report transactions associated with Cardholder Override.

Anti Passback

Enable – Select this option to enable the anti-passback feature at this reader for the number of seconds entered in the **Time Active** field. The anti-passback function prevents cardholders from using their badge at the same reader until the timer has expired.

Note: If cardholders swipe their badge while the anti-passback timer is active, the anti-passback period is reset to its initial value. Also, badges with Executive privilege enabled, do not override the timed anti-passback feature.

Time Active – Enter the time in seconds that a badge used at the reader is invalid before it can be used at the same reader.

Action on Anti Passback Violation – Select from the drop-down list the action that will occur if the cardholder violates the anti-passback rule. Choices are:

- **No action** – Select this option if you do not want the reader to perform any special action.
- **Grant Access and Report Violation** – Select this option to allow access at the door and to report the anti-passback violation.
- **Deny Access and Report Violation** – Select this option to deny access at the door and to report the anti-passback violation.

Reader Parameters

Access Time – Enter the time (in seconds) that the door remains unlocked after a cardholder presents a valid badge at this reader. The cardholder will have up to 60 seconds to open the unlocked door before it re-locks when the access time elapses.

Extended Access Time – Enter the time (up to 1620 seconds) that the door will remain unlocked to provide extended access time to cardholders with special needs.

Time Before Propped Door Reported – Enter the number of seconds (up to 60) that the door can remain opened before the propped door alarm is reported.

Keypad Entry Parameters

Maximum Entry Time – Enter the number of seconds (up to 60) the user has to enter the PIN code or badge number at the keypad.

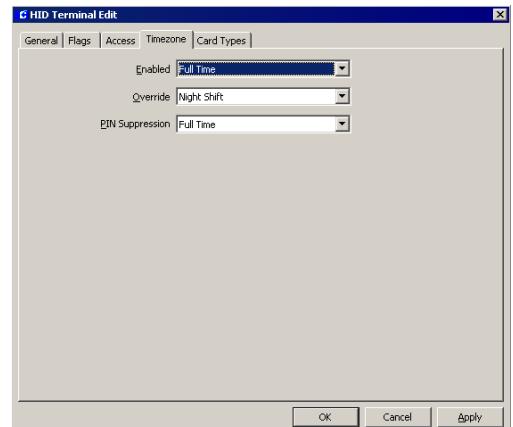
Maximum Attempts – Enter the number of attempts (up to 10) the user has to enter a correct PIN code or badge number at the keypad.

Failed Attempts Lockout – Enter the number of seconds (up to 99) the reader will be locked after the user exceeded the maximum attempts

to enter a PIN code or badge number at the keypad.

Timezone Tab

This tab defines the time zone during which the terminal will operate. Time zones must be set up before they display in drop-down lists.



Enabled – Select a time zone from the drop-down list during which the terminal will be active. For example, you may not want the reader to be used between midnight and 5:00 AM, so assign a time zone with the desired inactive time period. If you select <always enabled>, the terminal will always be active.

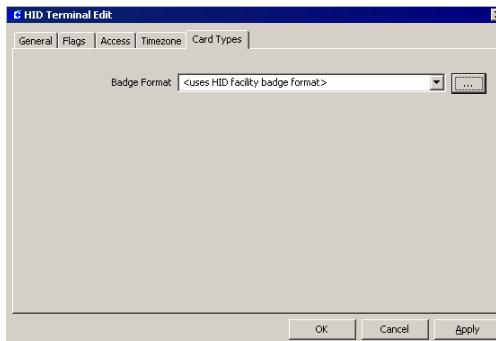
Override – Select a time zone from the drop-down list that can be set as an override for this terminal.

PIN Suppression – Select a time zone from the drop-down list during which cardholders are not required to enter a PIN code.

Card Types Tab

This tab determines which card type can be used at the selected reader. If a presented badge does not match the selected card type, the system will deny access to the cardholder. The Badge Format field displays the default

HID facility badge format as defined in the HID Facility application (see page 161). If this reader will use a different format, select the format here.



Badge Format – Click the [...] button and select the badge format to be used by this reader. The P2000 software provides badge formats that are located in the \Program Files\Johnson Controls\CARDKEY P2000\BadgeFormats folder. If a different format is needed, create a new badge format file by using the P2000 Badge Format tool, see page 182 for details.

Note: On 64-bit Windows operating systems use \Program Files (x86)\Johnson Controls\P2000\BadgeFormats folder.

Configure HID Input Points

HID panel and terminal applications automatically generate input points and their addresses. These input points can be enabled to indicate the current state of a device and can be used for alarm or non-alarm purposes.

Some HID input points have a predefined and unchanging purpose, such as to indicate panel tamper. Other input points are dedicated to access control functions, such as receiving input from door contacts and REX devices; and other input points can be used for a variety of purposes and devices, such as power failure

– these input points are referred to as general purpose inputs.

Panel input points are automatically created under the selected HID panel and are named using the input name and <panel name>, as in “Power Failure <panel name>.” Terminal input points are created under the selected HID terminal and are named using the input name and <terminal name> <panel name>, as in “Forced Door <terminal name> <panel name>.” If you rename the panel or terminal, you can edit the input point to manually enter the new panel or terminal name.

The following input points are available:

Input Type	Input Name	Description
Panel Input Point	Power Failure	Indicates the reader has a power failure.
	Panel Battery	Provides low battery indication.
	Panel Down	Internal to P2000 to indicate that the panel is not active.
Terminal Input Points	Door Monitor	This input point receives signal from the door contact device associated with the reader.
	Forced Door	Indicates when there is a door open condition without a valid badge read detected first.
	Propped Door	Indicates when there is a door open condition with a valid badge, but the door is left open past the entry time
	Request Exit	This input point receives signal from the REX device associated with the reader.
Tamper Switch	General purpose input. Typically wired to a tamper switch to indicate tampering.	
Terminal Down	Internal to P2000 to indicate that panel communications have ceased.	

To Configure HID Inputs:

1. In the System Configuration window, click the plus (+) sign next to the root **Panels** icon.
2. Click the plus (+) sign next to the **HID Network Panels** icon to display all HID panels configured in the system.
3. Click the plus (+) sign next to the panel that contains the input points you wish to configure.
 - To configure panel inputs, click the plus (+) sign next to the **Input Points** icon, select the input point you wish to configure and click **Edit**.
 - To configure terminal inputs, click the plus (+) sign next to the terminal that contains the input point you wish to configure, then click the plus sign next to the **Input Points** icon, select the input point you wish to configure and click **Edit**.

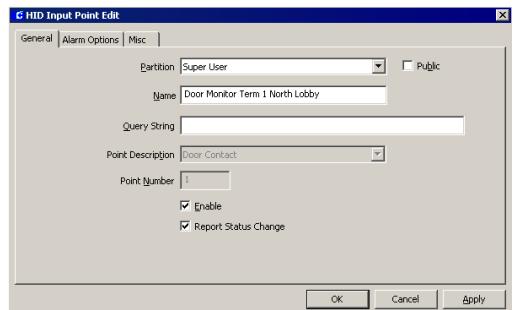
The HID Input Point Edit dialog box opens at the General tab.

4. Enter the information in each tab according to your system requirements. The fields available for configuration depend on the type of input point selected. (See HID Input Point Field Definitions for detailed information.) As you work through the tabs, click **Apply** to save your settings.
5. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window.

IMPORTANT: Whenever an HID input configuration is downloaded, there is a 7 to 8 second window when a cardholder may gain access even if the enabled time zone does not allow it.

HID 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 – This field displays the name automatically assigned to the input point, which consists of the <point name> <panel name>. For terminal inputs, the input name consists of the <point name> <terminal name> <panel name>. If you wish to change it, enter a descriptive name for the input point.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Point Description – Displays the point name defined by the HID panel.

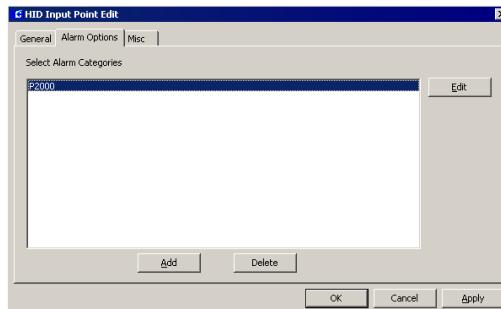
Point Number – Displays the number associated with the input point. This number represents the physical connection to the terminal and cannot be changed.

Enable – Select this option to allow the input point to operate as a predefined input, such as REX, Door Monitor or Tamper Switch.

Report Status Change – Select this option to report all input point changes of state. Do not select the check box if you do not want these changes reported.

Note: HID input points do not differentiate between short or open changes of state, they are both considered “fault” conditions; however, they are reported in the system as “short” alarms.

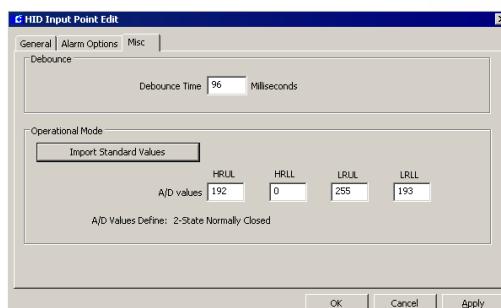
Alarm Options Tab



Alarm options are described in detail on page 97.

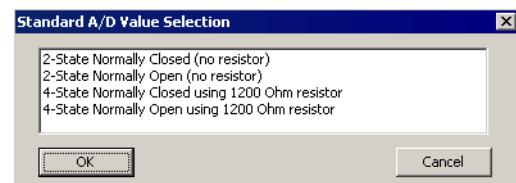
Misc Tab

Settings in this tab are not available for Panel Down, Forced Door, Propped Door, and Term Down input points.



Debounce Time – Enter the time in milliseconds that the input must remain in a transition state to establish the detected state. Without a debounce time, the panel may detect that the input is in an incorrect state due to the “bouncing” of the input device’s contacts.

Import Standard Values – Click this button if you wish to select a predefined mode of operation of the input point. Inputs can be used as either 2-state or 4-state inputs and can be Normally Open or Normally Closed. Once you make your selection, click **OK**.



A/D values – The Analog to Digital (A/D) default values displayed here represent the High Range Upper Limit (HRUL), High Range Lower Limit (HRLL), Low Range Upper Limit (LRUL), and Low Range Lower Limit (LRLL) values assigned for each operational mode and that match the end of line (EOL) resistors. You can however, change any of the four A/D values at any time.

Note: The A/D Values Define field displays how HID will use the four values. It also shows errors when an illegal combination of values is entered. This field is updated every time you make changes to the A/D values

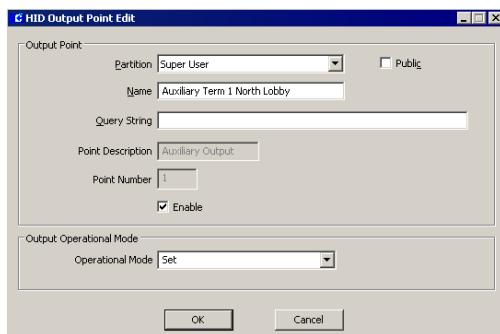
Configure HID Output Points

HID outputs consist of a single auxiliary output that is automatically generated after you create and save the HID panel information. The auxiliary output point can be activated in response to an activated input point, and can be

used to trigger external devices, such as alarm warning indicators or emergency lights. It can also be commanded from the P2000 Output Control application.

To Configure HID Outputs:

1. In the System Configuration window, locate the HID terminal that contains output point.
2. Click the plus (+) sign next to the **Output Points** icon, select the output point and click **Edit**. The HID Output Point Edit dialog box opens.



3. If you use partitions, select the appropriate **Partition** that will have access to this output point.
4. If you use partitions, click the **Public** check box if you want this output point to be visible to all partitions.
5. The **Name** field displays the name automatically assigned to the output point. If you wish to change it, enter a descriptive name for the output point.
6. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

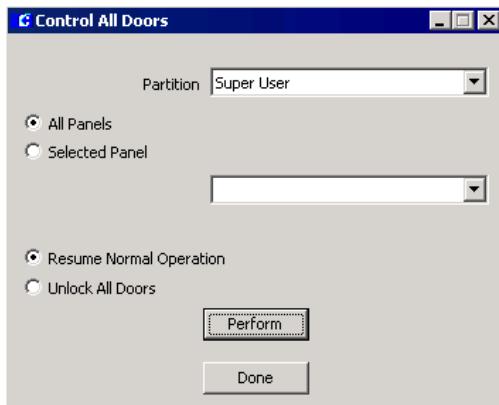
7. The **Point Description** field displays the point name defined by the HID panel.
8. The **Point Number** field displays the number associated with the output point and cannot be changed.
9. Select the **Enable** check box to allow the output point to be activated or deactivated.
10. Select from the **Operational Mode** drop-down list, the state in which the output point will operate. If you select *Set*, the output point will remain active, until commanded to be *Reset*.
11. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window.

Troubleshooting Misconfigured HID Readers

The HID ERW400, ER40, and ERP40 Edge devices have integrated R40 type HID readers. The integrated readers may ship from HID configured to either hold one card swipe or ignore all card swipes when disabled. If configured to hold a card swipe, when the device is re-enabled, card data will be presented to the Edge device for an access decision, possibly granting access. The ability to disable the reader is used within the P2000 software by Reader Enable Timezone, Reader Override Timezone and Control All Doors.

To Determine if an HID Reader is Storing Card Information:

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 HID doors are active.
4. Select the **Selected Panel** radio button.
5. From the drop-down list, select the HID panel you wish to test.
6. Select the **Unlock All Doors** option to unlock all doors connected to the selected panel.
7. Click **Perform**. The system will inform you that the doors will remain unlocked until you lock the doors again, and prompt you to continue.
8. Click **Yes**. This will put the device into override.
9. With the device in override swipe a card at the reader.
10. If the reader is configured incorrectly the reader will beep.
11. To return the doors to their previous state, select the **Resume Normal Operation** option.

12. Click **Perform**. The system will prompt for verification.
13. Click **Yes**. The Door Control override is reversed. The Real Time List will show the results of the card swipe if the reader is not properly configured.

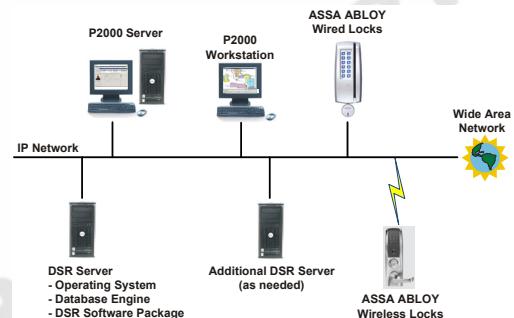
Note: Contact HID if you encounter this type of problem.

Configure Assa Abloy® IP Door Locks and Components

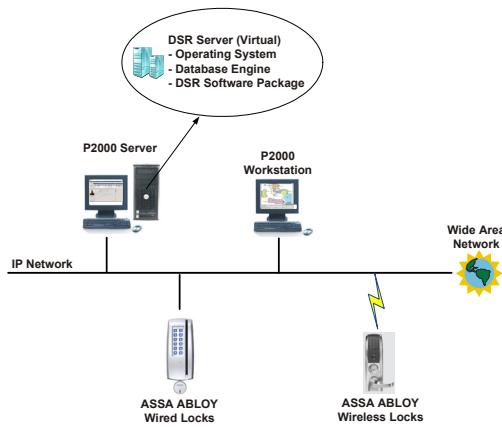
Assa Abloy Intelligent Locks provide a wired and wireless door locking security solution that can be integrated with the P2000 system. Integration between these two systems is possible via the Assa Abloy Door Service Router (DSR), which is installed on the DSR server, and the P2000 Assa Abloy DSR Interface Service, which runs on the P2000 server.

The DSR can be on a separate server or on a virtual computer on the P2000 server, and must have network access to the P2000 server. For large Assa Abloy installations, P2000 can also connect to multiple DSR servers, as needed.

The following figure illustrates a DSR running on physical computers.



The following figure illustrates a DSR running in a virtual environment.



Hardware Requirements

Before you use the functions described in this section, the Assa Abloy hardware and DSR server(s) must be properly installed. Refer to the Assa Abloy documentation for hardware installation assistance. For DSR installation information, refer to the *P2000 Server/Workstation Software Installation Manual*.

Assa Abloy Component Naming Conventions

Each Assa Abloy Intelligent Lock is represented by a panel and a single reader terminal in P2000. P2000 automatically adds Assa Abloy panels, terminals, and associated soft input points to the P2000 system configuration tree after the DSR detects the corresponding locks, which occurs after the DSR Interface Service restarts or when a change occurs to the fields on the Assa Abloy DSR Edit dialog box (see page 176). Each component has a pre-defined name, including a 16-character string identifying the panel serial number as defined in the DSR.

Panel names have the following predefined structure:

[PoE or Wi-Fi] [Lock Serial Number]

Example: PoE IT107E2577PA0BCE

Terminal names have the following predefined structure:

[PoE or Wi-Fi] [Lock Serial Number] Term

Example: PoE IT107E2577PA0BCE Term

Note: Predefined panel and terminal names enable you to determine whether the panel (or associated panel in the case of a terminal) is wired (PoE) or wireless (Wi-Fi).

Soft input points have the following pre-defined structure:

[Soft input point alarm name] [Lock Serial Number]

Example: Forced PoE IT107E2577PA0BCE

When renaming Assa Abloy panels, terminals, and soft input points, use a consistent naming scheme to avoid panel and component identification confusion.

Use logical names for Assa Abloy panels. For example, consider a name that identifies the panel's location. The maximum number of characters allowed for an Assa Abloy component name is 32.

Configure Assa Abloy Facility Parameters

Before configuring your Assa Abloy components, use the following instructions to define facility parameters associated with Assa Abloy panels.

Note: Facility parameter modifications affect all Assa Abloy panels and associated components defined in the P2000 System Configuration.

Configuring Assa Abloy facility parameters consists of the following:

- Assigning special access requirements for Assa Abloy panels (see “Special Access for Assa Abloy Panels” on page 174)
- Setting up badge formats for use with Assa Abloy panels (see “Set Up Badge Formats for Assa Abloy Panels” on page 175)

Special Access for Assa Abloy Panels

In addition to basic access, operators can control special access for overriding the normal operation of Assa Abloy panels. Special access options include:

- **Extended Access** – Extends the time a cardholder is permitted to hold a door open, which can be used to comply with Americans with Disabilities Act (ADA) requirements.
- **Deadbolt Override** – Enables a cardholder to unlock an Assa Abloy lock when the deadbolt is engaged.
- **Wakeup Communication (Wi-Fi only)** – Forces the Assa Abloy lock to connect to the DSR so P2000 can retrieve panel event data since the last panel-DSR connection.

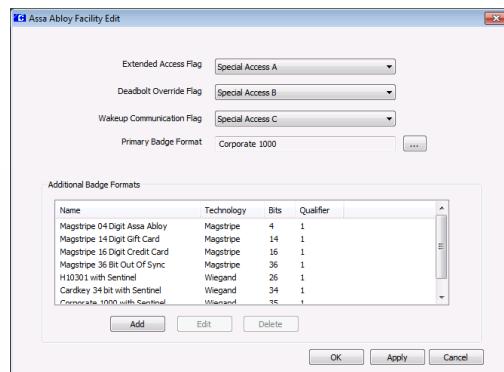
Note: Assa Abloy wireless locks connect to a DSR at specified time intervals, as a result of an alarm, or upon presentation of a badge with the Wakeup Communication capability. P2000 operators can only view panel event data that has occurred since the last lock-DSR connection.

Note: If a badge has both Deadbolt Override and Wakeup Communication capabilities, the Wakeup Communication function takes priority when the cardholder presents the badge (Deadbolt Override will not take effect).

Note: Badges with Wakeup Communication capability do not unlock any doors.

To Modify the Assa Abloy Facility Parameters for Special Access:

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 **Panels** icon to display the root panel types.
3. Select **Assa Abloy Panels** and click **Edit**. The Assa Abloy Facility Edit dialog box opens.



4. Assign the desired special access flags. The drop-down lists display the special access flag names as configured in Site Parameters; see page 41.
5. Click **Yes** when informed about the download requirement.
6. Click **OK**.

Set Up Badge Formats for Assa Abloy Panels

Assa Abloy intelligent locks support multiple badge formats. The integration with these locks requires P2000 operators to configure the P2000 system to support the badge formats that will be employed at the site. P2000 offers the flexibility of defining a primary badge format for the majority of badges used at Assa Abloy locks, and allows supplemental formats to be added for the rest.

To start, add any badge formats (*.bft files) not already defined that are required by Assa Abloy locks. See “P2000 Badge Format” on page 182 for more information. All badge formats (*.bft files) are located in \Program Files\Johnson Controls\P2000\BadgeFormats.

Note: On 64-bit Windows operating systems, the path is \Program Files (x86)\Johnson Controls\ P2000\BadgeFormats.

In addition to creating *.bft files, you must perform additional badge format configuration steps specific to Assa Abloy panels, as described in this section. These steps consist of the following:

- Creating badge formats to be assigned to cardholder badges (see “Create Badge Formats” on page 223). These settings must match the settings defined for Assa Abloy supplemental badge formats.
- Selecting the primary badge format for Assa Abloy locks (see “To Select a Primary Badge Format for Assa Abloy Locks:” on page 175).
- Adding supplemental badge formats, as needed (see “To Add Supplemental Badge Formats:” on page 175.)

To Select a Primary Badge Format for Assa Abloy Locks:

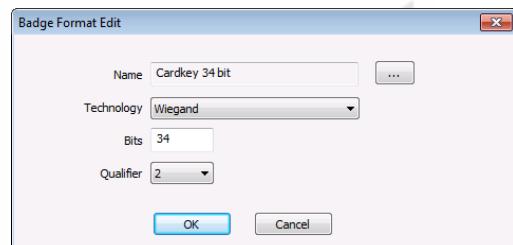
1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the plus (+) sign next to the root **Panels** icon to display the root panel types.
3. Select **Assa Abloy Panels** and click **Edit**. The Assa Abloy Facility Edit dialog box opens.
4. In the **Primary Badge Format** field, click the [...] button and select the badge format that will be the primary format used at the site for Assa Abloy locks.

Note: If a P2000 operator does not assign a badge format to a cardholder badge, the Primary Badge Format will be used.

5. Click **Apply**.

To Add Supplemental Badge Formats:

1. On the Assa Abloy Facility Edit dialog box, click **Add**. The Badge Format Edit dialog box opens.



2. Click the [...] button, select a *.bft file from the list, and click **Open**. The name of the selected *.bft file appears in the **Name** field. You cannot edit this name.

3. Select from the **Technology** drop-down list, the technology type.
4. Enter the total number of **Bits** expected to be returned from the reader when the badge is read.
5. Select a **Qualifier** number. The number selected represents a 32-bit numerical value that allows differentiating formats with the same technology and the same number of bits. The default value is 1.

IMPORTANT: *The Assa Abloy Technology, Bits, and Qualifier badge format settings must match the badge format settings defined for a cardholder badge (see “Create Badge Formats” on page 223).*

6. Click **OK**.
7. Verify that the badge format is listed under Additional Badge Formats.
8. Repeat these steps for each badge format to be used with Assa Abloy locks.

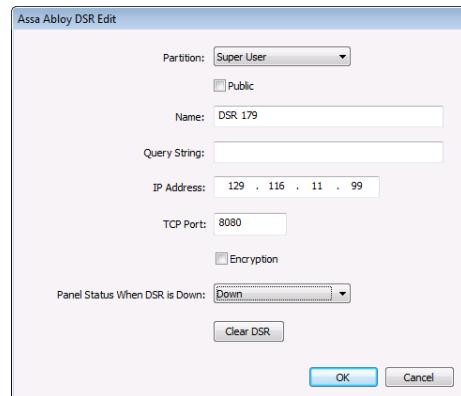
Add a Door Service Router (DSR)

The Assa Abloy DSR is the communication link between the P2000 server and Assa Abloy panels. Once you add a DSR on the P2000 System Configuration window, P2000 automatically adds all of the Assa Abloy panels and sub-components associated with the DSR.

Note: *If a lock is added to a DSR after you add the DSR to the P2000 system configuration, the lock will be added to P2000 only after the DSR Interface Service restarts or when a change occurs to the fields on the Assa Abloy DSR Edit dialog box.*

To Add an Assa Abloy DSR:

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 **Panels** icon to display the root panel types.
3. Click the plus (+) sign next to the root **Assa Abloy Panels** icon.
4. Right-click over **Integration Components** and click **Add**. The Assa Abloy DSR Edit dialog box opens.



5. If this is a partitioned system, select the **Partition** in which the Assa Abloy DSR is active
6. Select **Public** if you wish the Assa Abloy DSR to be visible to all partitions.
7. Enter a descriptive **Name** for this DSR.
8. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).
9. Enter the **IP Address** of the DSR.
10. Enter the **TCP Port** address of the DSR.
11. The **Encryption** feature is currently not supported in this release.

12. When a DSR status changes to Down, P2000 receives notifications about the panel status, according to the following selections in the **Panel Status When DSR is Down** drop-down list:

Down – P2000 receives a panel down notification for **each** panel associated with the DSR.

No Change – P2000 receives only a single notification that the DSR is currently down. P2000 will **not** receive panel down notifications for each panel associated with the DSR. This option is recommended for large installations.

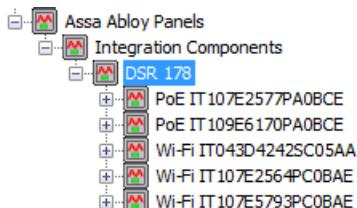
13. Click the **Clear DSR** button to delete all P2000 data (for example, badge data, access groups, etc.) from the DSR.

IMPORTANT: After clearing the DSR of P2000 data, once the DSR downloads these changes to the panels, P2000 cardholders will not be able to gain access via the Assa Abloy door locks. To repopulate the DSR with P2000 data, perform a P2000 download function to all Assa Abloy panels.

14. Click **OK**.

Edit Assa Abloy Panels

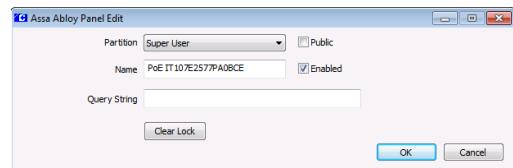
After you add a DSR, a panel list appears under the DSR in the System Configuration tree.



New panels cannot be added manually. However, you can edit or delete the panels, as necessary.

To Edit an Assa Abloy Panel:

- 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 **Panels** icon to display the root panel types.
- Click the plus (+) sign next to the root **Assa Abloy Panels** icon.
- Click the plus (+) sign next to the root **Integration Components** icon.
- Click the plus (+) sign next to the **DSR** that has the panel you wish to edit.
- Right-click over the panel you wish to edit and select **Edit**. The Assa Abloy Panel Edit dialog box opens.



- If this is a partitioned system, select the **Partition** in which the Assa Abloy panel is active.
- Select **Public** if you wish the Assa Abloy panel to be visible to all partitions.
- The **Name** field displays the name automatically assigned to the panel. You can however enter a different name.
- Select the **Enabled** check box to enable the Assa Abloy panel.
- The **Query String** value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).
- Click the **Clear Lock** button to delete all P2000 data (for example, badge data,

access groups, etc.) from the Assa Abloy panel.

13. Click **OK** to save the panel information.

To Delete an Assa Abloy Panel:

IMPORTANT: *Deleting the panel from P2000 does not delete the panel from the DSR. Therefore, the next time the DSR Interface Service restarts, the panel will reappear, along with the associated components, on the System Configuration window. You can only delete an Assa Abloy panel from the P2000 system if the lock is no longer connected to the DSR.*

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 **Panels** icon to display the root panel types.
3. Click the plus (+) sign next to the root **Assa Abloy Panels** icon.
4. Click the plus (+) sign next to the root **Integration Components** icon.
5. Click the plus (+) sign next to the **DSR** that has the panel you wish to delete.
6. Right-click over the panel you wish to delete and select **Delete**.
7. On the Confirm Delete dialog box, click **Yes**.

Assa Abloy Panel Time Zones

By default, P2000 time zones are not automatically assigned to Assa Abloy panels. See the instructions described in “Configure Panel Time Zones” on page 72 to assign up to 32 time zones to an Assa Abloy panel.

IMPORTANT: *Each Assa Abloy lock can only store up to 32 time periods. A time zone may have multiple time periods, which include holidays. For example, a time period of Monday from 8 AM to 12 PM and a Holiday period of Monday from 8 AM to 12 PM count as two time periods.*

Note: *If a panel is deleted and then re-added by the DSR, any time zones previously assigned to the panel will be cleared. Reassign the time zones, if necessary.*

Configure Assa Abloy Terminals

Each Assa Abloy panel controls a single door terminal, which is automatically created with each panel added to the System Configuration window via the DSR. The Assa Abloy terminal consists of seven soft input points.

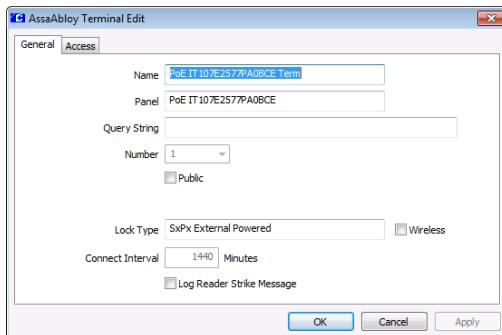
To Configure Assa Abloy Terminals:

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 **Panels** icon to display the root panel types.
3. Click the plus (+) sign next to the root **Assa Abloy Panels** icon.
4. Click the plus (+) sign next to the root **Integration Components** icon.
5. Click the plus (+) sign next to the **DSR** that has the panel/terminal you wish to configure.
6. Click the plus (+) sign next to the panel that has the terminal you wish to configure.
7. Right-click over the terminal and select **Edit**. The Assa Abloy Terminal Edit dialog box opens at the General tab.

8. Enter the information in each tab according to your system requirements. (See Assa Abloy Terminal Field Definitions for detailed information.) As you work through the tabs, click **Apply** to save your settings.
9. When you finish with all the entries, click **OK** to save your settings and return to the System Configuration window. If you wish to include Assa Abloy terminals in groups that provide common access, refer to “Create Terminal Groups” on page 91.

Assa Abloy Terminal Field Definitions

General Tab



Name – This field displays the name automatically assigned to the terminal. You can however enter a different name for the terminal.

Panel – Displays the name of the Assa Abloy panel you selected from the System Configuration window.

Query String – This value is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Number – This field displays the terminal number automatically assigned and cannot be edited.

Public – If you use Partitioning, select the Public check box if you wish the Assa Abloy terminal to be visible to all partitions.

Lock Type – Displays the name indicating the terminal lock type, as defined by the DSR. This field cannot be edited.

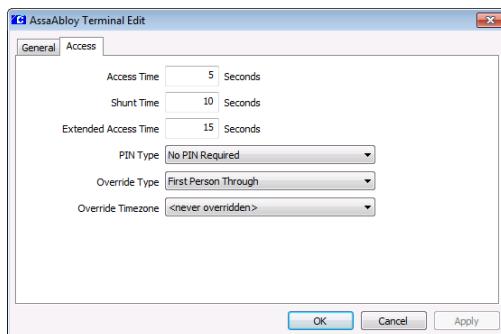
Wireless – By default, this check box is selected for Assa Abloy wireless locks (indicated as *Wi-Fi* in the default name) and not selected for wired locks (indicated as *PoE* in the default name). Do **not** change the default setting unless special circumstances require it.

This field enables you to define the time interval when the lock will connect to the DSR. Since wireless Assa Abloy locks typically run on battery power, configuring the lock to connect to the DSR too often significantly drains the lock’s battery power.

Connect Interval – For wireless locks only; use this field to set the time interval (in minutes) to have the lock connect to the DSR for updates and event information. The **Wireless** check box must be selected to modify the time interval.

Log Reader Strike Message – For PoE locks only; if selected, door strike locked and unlocked status messages are reported to P2000. If this information is not of interest, or to keep the number of status messages to a minimum, clear this check box. The **Wireless** check box must not be selected to modify this field.

Access Tab



Access Time – Enter a time in seconds that the door strike is energized after each valid badge access request. The default value is 5 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 default value is 10 seconds.

Extended Access Time – Select the amount of time that the door will remain unlocked to provide extended access time to cardholders with special needs.

PIN Type – Determines the use of PIN codes. Select one of the following options:

- **No PIN Required** – In this mode, cardholders do not enter a PIN to gain access through a door.
- **PIN Required** – In this mode, cardholders must enter a PIN in conjunction with presenting a valid badge. PIN codes can be entered before or after presenting a badge. Not supported on all locks (e.g. Persona™ Passport™ locks). Check with your local Assa Abloy dealer for information on PIN support with other locks.
- **PIN After Badge** – In this mode, cardholders must enter a PIN in conjunction with presenting a valid badge. PIN codes **must** be entered **after** presenting a badge.

Note: For information on the number of supported PIN digits on Assa Abloy locks, check with your local Assa Abloy dealer.

Override Type – If a time zone is selected in the **Override Timezone** drop-down list, the Override feature functions according to one of the following options:

- **Unlock** – The door automatically unlocks and remains unlocked during the active period of the selected time zone.
- **First Person Through** – The door remains locked during the active period of the selected time zone until a cardholder presents a valid badge at the reader, at which time the door will remain unlocked for the remainder of the time zone's active period.
- **User Unlock** – Magstripe readers only; the door remains locked during the selected time zone's active period until a cardholder has swiped a valid magstripe badge twice in succession. Swiping only once with a valid badge unlocks the door, which then relocks after the access time expires.

Override Timezone – To disable the Override feature, select <**never overridden**>. To use the Override feature in accordance with the **Override Type** selected, select a time zone during which the override period will be active.

Configure Assa Abloy Soft Input Points

P2000 monitors the following soft input points for Assa Abloy panels/terminals:

Battery Low (Batt Low) – Indicates that the wireless lock's battery is failing. Does not apply to wired locks.

Forced Door (Forced) – Indicates when the door has been opened without a valid badge having been presented to the reader first.

Out of Sync (OutOfSync) – Indicates when the DSR and lock are out of sync, which can be caused by numerous events (for example, downloading a badge with an invalid badge format for the lock, exceeding the number of time periods for the lock, etc.).

Propped Door (Propped) – Indicates when a door has been opened with a valid badge but has been held open longer than the shunt time.

Tamper – Indicates when someone has tampered with the lock or firmware.

Terminal Down (Term Down) – Since an Assa Abloy panel and terminal are essentially the same in P2000, watch for panel down indications.

Panel Down (PanelDown) – Listed under **Soft Input Points** in the System Configuration tree; this soft input point indicates when panel communications have ceased.

To Configure Assa Abloy Soft Input Points:

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 **Panels** icon to display the root panel types.
3. Click the plus (+) sign next to the root **Assa Abloy Panels** icon.
4. Click the plus (+) sign next to the root **Integration Components** icon.
5. Click the plus (+) sign next to the **DSR** that has the panel/terminal and the soft input point you wish to configure.
6. Click the plus (+) sign next to the panel that has the terminal and soft input point you wish to configure.
7. Click the plus (+) sign next to the terminal to view the available soft input points.

8. Right-click over the soft input point you wish to edit and select **Edit**. The Input Point dialog box opens. This dialog box consists of four tabs: **General**, **Alarm Options**, **I/O Linking**, and **Misc**.

Note: All of the fields on the **I/O Linking** and **Misc** tabs, including many fields on the **General** tab, cannot be modified.

9. Modify the fields on the desired tabs accordingly.

For information on the **General** and **Alarm Options** tabs, see “Input Point Field Definitions” on page 96.

10. Click **OK**.

Assa Abloy Status Information

The status of Assa Abloy components can be monitored on the P2000 System Status window.

DSR Status Information

The DSR is represented as an **Integration Component** in System Status with the following states:

- **Unknown** – The status has not yet been determined.
- **Up** – P2000 is communicating with the DSR.
- **Down** – P2000 is not communicating with the DSR.

Panel/Terminal Status Information

Each **door lock** is represented in the P2000 as a **panel** in System Status with the following states:

Unknown – The status has not yet been determined.

Up – The panel is currently online with the DSR.

Down – The panel is currently offline with the DSR. This is the normal state for wireless locks.

Disabled – The P2000 has been instructed not to communicate with the panel.

Real Time Functions

Wireless locks are not permanently connected to the DSR. For this reason, real-time functions, such as operating a door, and real time database modification and event reporting are not supported. Communication between the DSR and the locks may be as frequent as once per day, but can be less frequent.

Wired locks are permanently connected to the DSR, and real-time operations as well as real-time database modification and event reporting are supported.

For information, see “Using the Real Time List” on page 322.

Lockout Mode with Assa Abloy Locks

The P2000 Door Control application supports the ability to set an Assa Abloy door into **Lockout** mode. In this mode, the lock denies access to all users, except those that have the Assa Abloy Emergency privilege. P2000 operators cannot assign this privilege due to restrictions with the DSR.

For information see, “Controlling Doors” on page 273.

File Maintenance on the DSR Server

The DSR produces *.zip files that contain archived logs and stores them on the computer hosting the DSR.

However, the DSR does not purge them automatically or regularly.

To avoid running out of disk space on the computer that hosts the DSR, we recommend periodically deleting these files manually.

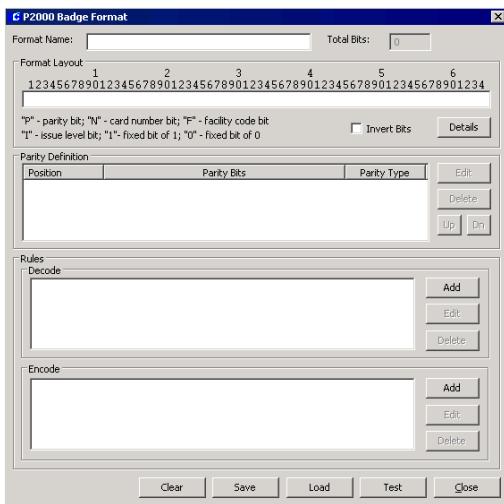
P2000 Badge Format

Use the P2000 Badge Format application to create badge formats for badges that will be used with OSI, Isonas, and HID readers. You can create a new badge format, load an existing format, or load and modify an existing format to create a new one.

Once you create a new badge format, it will be available for assignment from the Badge tab of the OSI Facility record (see page 131), from the Card Type tab of the Isonas Terminal application (see page 158), and from the HID Facility (page 161) and HID Terminal applications (see page 167).

To Create P2000 Badge Formats:

1. From the P2000 Main menu, select **Config>P2000 Badge Format**. The P2000 Badge Format dialog box opens.



2. In the **Format Name** field enter the name of the badge format.
3. The **Total Bits** displays the total number of bits in the format.
4. In the **Format Layout** box specify the layout of the bits on the badge:

P: Bits allocated to parity
 N: Bits allocated to card number
 I: Bits allocated to issue level
 1: Fixed bit of 1
 0: Fixed bit of 0

For example, starting the format with "PP" indicates that the first two bits are allocated to parity.

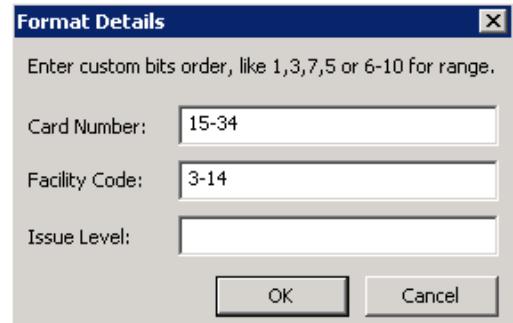
Every parity bit position entered in the **Format Layout** box is automatically added to the **Parity Definition** list where it needs to be defined. See page 183 for details.

5. Select the **Invert Bits** check box if the bits are to be inverted when the raw badge format is processed by P2000.
6. Click the **Details** button to see bit locations for card number, facility code, and issue level. Edit the text in the box only if you

need to reverse the order of the bits when they are processed by P2000.

For example, if the raw card number bits are "15-34," and they must be reversed, enter "34-15."

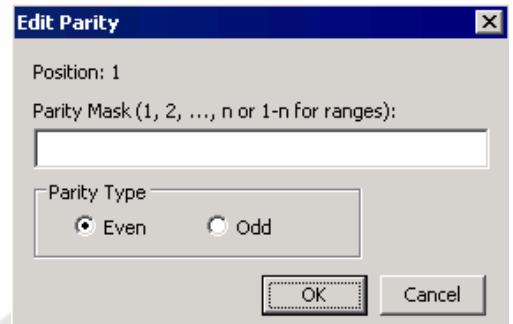
Note: You cannot use this window to change bits allocation as defined in Format Layout.



7. Click **OK** to close Format Details.

To Define Parity Bits:

1. Select an item from the Parity Definition box and click the **Edit** button. The Edit Parity dialog box opens.



2. In the **Parity Mask** field enter the bits that will be used to calculate parity.
3. Select **Even** or **Odd** to specify parity type.

4. Click **OK** to save the changes and to close Edit Parity.
5. To delete parity definitions, select an entry from the list and click **Delete**.

Note: Delete a parity definition only if you have removed the corresponding parity bit from the Format Layout box.

6. Once all parity positions are defined, use the **Up** and **Dn** buttons to change the order in which the parity is calculated.

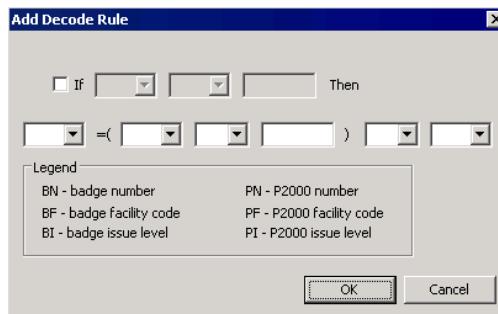
For example, if parity in position 1 uses in its calculation the value of parity in position 35, then it must be listed below position 35.

To Add Decoding Rules:

Decoding rules are used to convert a raw number received from a badge reader into P2000 badge number, facility code, and issue level.

Note: For each decoding rule, you must also add an encoding rule that matches it in reverse form.

1. In the P2000 Badge Format dialog box click the **Add** button in the Decode box. The Add Decode Rule dialog box opens.



2. Specify the rule to be used by P2000 for decoding raw card format. To enable condition fields select the **If** check box.

The “Bs” indicate the values returned from the badge reader, while the “Ps” indicate the values as displayed in the P2000 user interface.

3. Click **OK** to close Add Decode Rules.

To Add Encoding Rules:

Encoding rules are used to convert P2000 badge number, facility code, and issue level into a single number for a badge reader.

Each encoding rule must match a decoding rule in reverse form. See the following example of a pair of matching decoding/encoding rules.

Decoding rule: If $BI = 500$

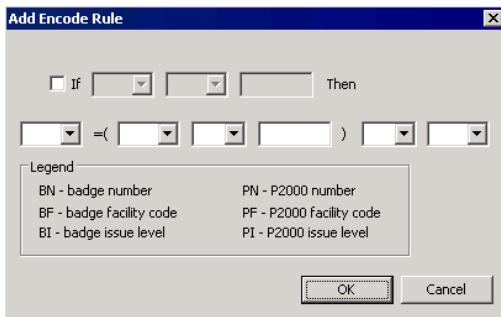
Then $PN = (BN + 10000)$

Encoding rule: If $PI = 500$

Then $BN = (PN - 10000)$

Follow the steps below to create an encoding rule.

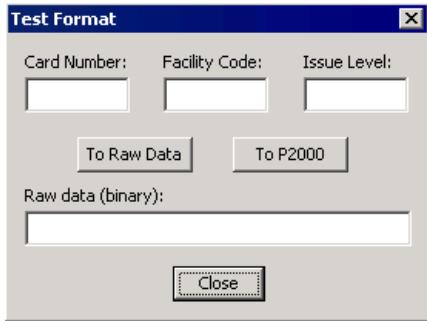
1. In the P2000 Badge Format dialog box click the **Add** button in the Encode box. The Add Encode Rule dialog box opens.



2. Specify the rule to be used by P2000 for encoding card format. To enable condition fields select the **If** check box.
The “Ps” indicate the values as displayed in the P2000 user interface, while the “Bs” indicate the values for the badge reader.
3. Click **OK** to close Add Encode Rules.

To Test the Badge Format:

1. To test the format, click the **Test** button at the bottom of the P2000 Badge Format dialog box. The Test Format dialog box opens.

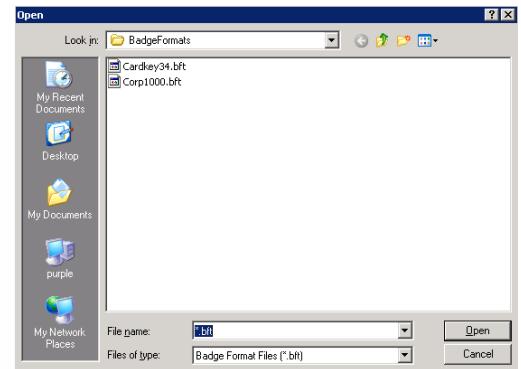


2. In the upper boxes enter the card number, facility code, and issue level as would be displayed in the P2000 interface.
3. Click **To Raw Data**. The bit string displayed in the lower box should be a valid raw data card number.

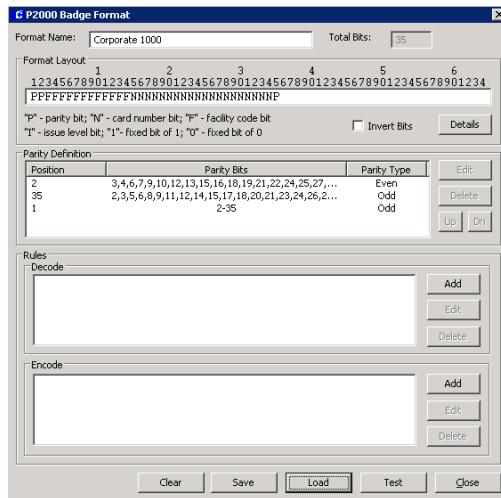
4. Clear the **Raw data** box and enter in it the single number as would be received from a badge reader. The number has to be provided in the data type selected.
5. Click **To 2000**. The card number, facility code, and issue level as would be displayed in the P2000 interface should appear in the upper boxes.
6. Click **Close** to return to the P2000 Badge Format dialog box.
7. Click **Save** to save the badge format.
8. The Save As window opens. Enter the file name and click **Save**.
9. In the P2000 Badge Format window click **Close**.

To Load/Edit Badge Format:

1. From the P2000 Main menu, select **Config>P2000 Badge Format**. The P2000 Badge Format dialog box opens.
2. Click **Load**.
3. Browse for the badge format to load and select the appropriate *.bft file.



4. Click **Open**.



5. Edit the badge format if desired.

Note: *Each modified format should be tested before saving.*

6. Click **Save**.
7. The Save As window opens. Enter the file name and click **Save**.
8. To define additional badge formats, click the **Clear** button and enter the new data.
9. In the P2000 Badge Format window click **Close**.

Configure Elevators and Cabinets

The P2000 system supports the elevator and cabinet access control using CK7xx panels, version 2.0 and higher.

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 cardholders 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 cardholders.

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.

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 floors are enabled by an elevator access grant. Relinquishing an elevator access grant does not disable an elevator floor 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 cardholder 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; that is, override per timezone, per panel system override and per the “Unlock All Doors” command from the Server. Override has no effect on Otis Compass elevators.

Executive Privilege – Badges with executive privilege enable all floors of the elevator per elevator access grant. Executive privilege does not modify the floor’s granted access when using PIN codes in Otis Compass elevators.

Low Level Interface

Low level interface elevators have readers associated with a set of output points and an optional set of input points. The field panel works 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 (see page 192), 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.

D620-ECG Elevator Mode

The P2000 system provides a low level 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 194 for more information.

KONE HLI/KONE ELINK 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 a KONE group controller to a CK721 or CK721-A panel, use the RS232C B (J2) connector. To connect a KONE group controller to a CK705 or CK720 panel, 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.

KONE IP High Level Interface

CK721-A panels version 3.1 and higher provide the communication necessary for KONE IP elevators. In this high-level elevator integration, the CK721-A panel interfaces with the elevator control system through a communications protocol. Granting access to floors is achieved by sending messages to the elevator controller; reporting destination floors is achieved by receiving messages from the elevator controller (you must select the Floor Tracking function).

Each CK721-A panel can connect to multiple KONE IP group controllers, each controller with up to 8 elevators, each elevator serving up to 128 floors. To define a KONE IP elevator, you must first select the **Kone IP** protocol type in the Panel Elevator tab.

The KONE IP elevator interface provides two types of group controllers, the KONE KIC and the Primary/Backup KGC. There are different rules when interfacing to a KONE KIC as opposed to a Primary/Backup KGC controller. KONE KIC controllers only support Car Operation Panels (COPs), and not Destination Operation Panels (DOPs). You can define up to 33 elevator groups for each KONE KIC controller. KONE IP controllers, configured in primary/backup pairs, support a single elevator group per controller pair.

For detailed instructions, see “Configuring KONE IP Elevators” on page 197.

Otis EMS - Security / BMS Protocol High Level Interface

The Otis Elevator Management System (EMS) controls up to 8 groups of elevators, each group consisting of up to 8 elevators. It interfaces to the Building Management System (BMS) through an RS422 interface. This elevator protocol is available with CK721-A panels version 2.10 and higher.

The number of elevators, and their assignment to elevator groups determines the number of CK721-A panels required. All elevators of each single group must be handled by the same CK721-A panel. Each CK721-A can support multiple groups, as long as the total number of elevators in these groups does not exceed 16.

To define an Otis EMS - Security / BMS elevator, you must select the High Level Interface flag. When you configure the Otis EMS elevator floors, you must define the public access timezone, 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.

Note: When downloading elevators to a panel running the Otis EMS integration, make sure the "Delete Elevators From Panel Before Download" option is not selected, as otherwise, the temporary deletion of the elevators would temporarily disrupt communication with the Otis EMS, see page 429 for details.

Otis Compass High Level Interface

The Otis Compass interface is a high level interface that uses a TCP/IP network to send elevator commands to the Otis system, and also receives historical information from the Otis system.

The P2000 system provides the communication between the Otis Compass elevator system and CK721-A panels version 3.0 and higher. When a cardholder swipes a badge, a message from the CK721-a panel is routed to the Otis Compass elevator system to identify the authorized floors for this cardholder.

The Otis Compass interface requires the P2000 Server to have a dedicated network interface card (NIC) connected to the Otis Compass network with an assigned static IP address of 192.168.50.250 and a mask of 255.255.255.0 with no default gateway. To configure a permanent static network route for the Otis system, a static route must also be configured at the P2000 Server by issuing once the following command (CMD) during commissioning: **"route add -p 192.168.0.0 mask 255.255.0.0 192.168.50.254."**

Note: The P2000 Otis Interface Service must be running at all times if Otis Compass elevators are being used, even during maintenance operations if possible, so it has the correct information to send to the Otis Compass system when it is reactivated. To disable P2000 control of the Otis Compass system for testing or maintenance operations, the network connection between the systems can be disconnected, but the Otis Interface Service must be left operational on the P2000 system.

The Otis system differs from typical elevator systems because the floor selection is done outside of the elevator cab. Access to the floor entry keypad, called a Destination Entry Computer (DEC), can be controlled by a reader connected to a CK721-A panel, if configured to do so. The Otis system allows operation of the DECs in 4 different modes that define the availability of floors and the order in which floors and badges are presented to the system.

Once a P2000 system is connected to an Otis Compass system, the P2000 system is in full control of what each DEC is able to do. This means that until an elevator is defined in the P2000 system and its access parameters are configured, no use of the elevator is permitted.

Important Notes

- Each CK721-A panel can control as many DECs as it has readers configured, using a one to one mapping.
- The P2000 system allows for the configuration of public use of a DEC through the configuration of unsecured elevator entry points.
- The P2000 also allows for configuration of secured entry points and the association of access rights on a badge to those secured entry points.
- The P2000 supports the Otis concepts of “Allowed Floors” and “Authorized Floors” through its configuration screens.
- The P2000 supports the ability to enter a PIN code on the DEC which is associated with a badge in the P2000 system and granted appropriate access if allowed.
- The P2000 also allows configuration of the ADA access and VIP access features, as well as the Default Floor feature in the Otis system.
- The PIN Access and Default Floor settings are defined using the Badge application.

Otis Compass Elevator Modes

The Otis Compass system provides the following elevator mode types:

Mode 1 – Initially allows entry of a requested floor or the presentation of a badge. If a cardholder enters a floor request, and is an allowed floor, an elevator is dispatched. If a cardholder presents a badge first, that badge’s default floor is used to dispatch an elevator, assuming the default floor is an authorized or an allowed floor. To configure Mode 1 elevators, use the Elevator Configuration application, see page 192 and/or the Otis Unsecured Elevator Configuration application, see page 196.

Mode 2 – These elevators must have a reader associated with the elevator and operate when the cardholder presents a valid badge at the reader/DEC combination. The cardholder must present the badge before selecting a floor, if the floor is authorized or allowed, an elevator is dispatched. This is the common mode of operation for secured elevator entry points. To configure these elevators use the Elevator Configuration application, see page 192.

Mode 3 – Initially allows entry of a requested floor. If the floor is allowed, an elevator is dispatched. If the floor is not allowed, a request is made for the user to provide a badge, if the badge presented authorizes the floor requested, an elevator is dispatched. This is the most common mode of operation for unsecured elevator entry points. To configure Mode 3 elevators use the Elevator Configuration application, see page 192 and/or the Otis Unsecured Elevator Configuration application, see page 196.

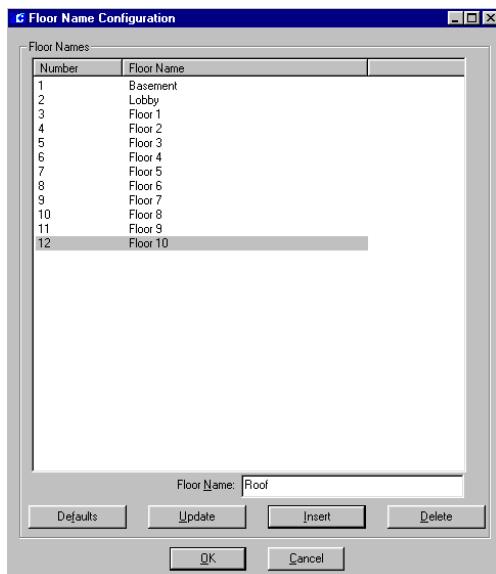
Mode 4 – The cardholder must present a badge before selecting a floor; the system preselects the badge’s default floor for the user, but the user has a short time to select a different floor. If the floor selected after the time-out is authorized or allowed, an elevator is dispatched. To configure these elevators use the Elevator Configuration application, see page 192.

In all modes, if the cardholder presents an invalid badge or enters an illegal floor, the system will inform the cardholder using the DECs display. If the cardholder makes a valid combination of badge and floor selection, the system will inform the cardholder what elevator to board using the DECs display. All transactions occurring at secured elevator entry points are logged in the P2000 system.

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 (127 floors with Otis Compass elevators).

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 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 “Site Parameters Field Definitions” on page 40).

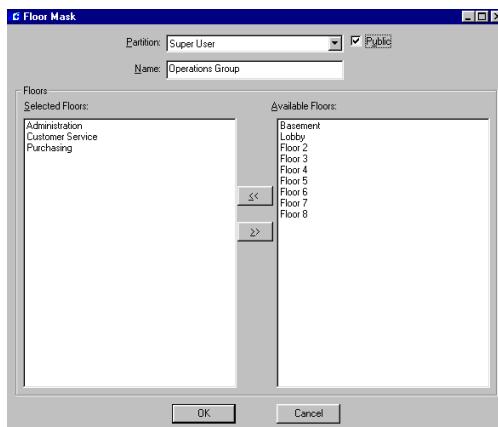
3. Click on the floor you wish to rename. The floor name will display in the **Floor Name** field at the bottom of the window.

4. 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. If you wish 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 cardholders that should have access to the three floors to the “Operations” group, rather than assigning all three floors to the cardholders 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, if applicable, the associated output and optional input points that will operate with your particular elevator controller type.

Note: Refer to specific instructions when configuring Unsecured Otis Compass elevators (page 196) and KONE IP elevators (page 197).

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.

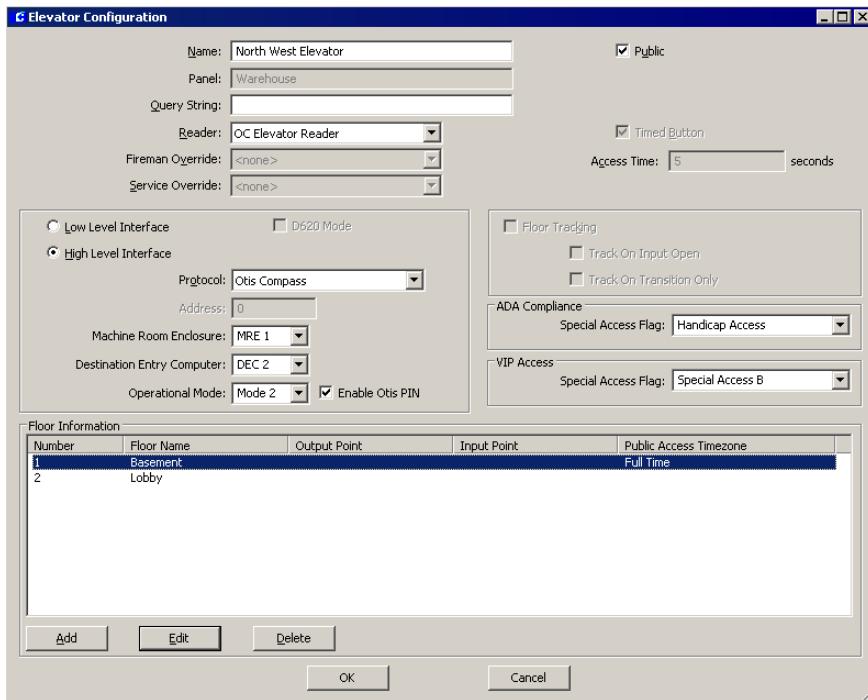
Elevator Configuration Field Definitions

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 is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).



Reader – Select an available reader from the drop-down list that has not yet been assigned to an elevator or cabinet, and that has an address number no higher than 16.

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. Not available for Otis Compass elevators.

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. Not available for Otis Compass elevators.

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. Not available for Otis Compass elevators.

Otis EMS elevators may report with a significant delay, landing numbers that were selected after a badge was used to de-secure floors. Therefore, the P2000 system does not take any actions to re-secure those floors, as this may interfere with subsequent access requests. This implies that the Timed Button flag should always be selected. The P2000 system then re-securces the floors after the configured elevator access time has elapsed, or when a new access request is processed that de-secures dif-

ferent floors. If the Timed Button flag is not selected, the P2000 system re-secures the elevator as soon as it receives a reported landing number.

Access Time – Enter the amount of time in seconds (2 to 600) that cardholders 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. Not available for Otis Compass elevators.

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 protocol used to communicate to the elevator control equipment. To select this option, you must define the protocol parameters in the Elevator tab, see page 68.

Note: After you create or edit Otis Compass elevator settings, you are required to restart the P2000 Otis Interface Service to make effective the changes.

Address – When configuring KONE HLI elevators, you must 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.

Machine Room Enclosure – Available for Otis Compass elevators only. A Machine Room Enclosure (MRE) defines a group of elevators that serve a set of floors. Select the MRE (1 to 8) that is associated with the elevator reader. As an option, you can select a Destination

Entry Redirector (DER) that connects to all elevator groups for building-wide dispatching. Select the DER (1 or 2) that is associated with the elevator reader.

Destination Entry Computer – Available for Otis Compass elevators only. A Destination Entry Computer (DEC) is a user interface device into which the desired floor is entered. Select the DEC that is associated with the MRE or DER selected, and is also associated with the elevator reader.

Note: *The MRE and DEC combination settings must be unique throughout the system.*

Operational Mode – Select from the drop-down list one of the four elevator modes provided with the Otis Compass system. Refer to “Otis Compass Elevator Modes” on page 190 for more information.

Enable Otis PIN – Available for Otis Compass elevators only. Select this check box if you allow cardholders to enter a PIN code on the DEC in order to gain access to a floor.

Floor Tracking – Floor tracking is permanently enabled for Otis Compass elevators. If enabled, the panel generates a history message identifying the badge number, cardholder’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.*

Otis EMS elevators report landing numbers that were selected after a badge was used to de-secure floors. When the floor tracking option is enabled, the P2000 system creates a floor tracking message for each landing number that is reported by the Otis EMS. The P2000 system associates the reported landing number with the last person that was granted access at the elevator.

ADA Compliance – Select one of the three special access flags that was also assigned to cardholders with ADA privileges and that will inform the Otis Compass system that the person requires special access at a reader.

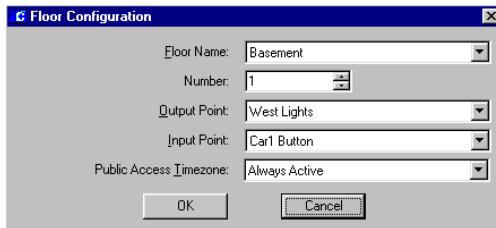
VIP Access – Select one of the three special access flags that was also assigned to cardholders with VIP privileges and that will inform the Otis Compass system that the person requires special access at a reader.

Note: The ADA Compliance and VIP Access lists display the special access flag names as configured in Site Parameters, see page 41. These are global settings and will be effective for all Otis Compass configured elevators in the system.

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.

- In the Elevator Configuration dialog box, click the **Add** button at the bottom of the window. The Floor Configuration dialog box opens.



- 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.
- 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.
- Select from the **Output Point** drop-down list an available output point that has not yet been assigned to an elevator or cabinet. Not available for Otis Compass elevators.
- Select from the **Input Point** drop-down list an available input point that has not yet

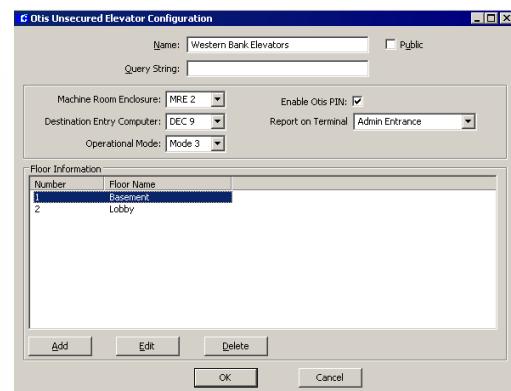
been assigned to an elevator or cabinet. Not available for Otis Compass elevators.

- Select from the **Public Access Timezone** drop-down list the time zone defined to allow cardholders 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.
- Click **OK** to save your settings and return to the Elevator Configuration dialog box.

Configuring Otis Unsecured Elevators

Use this section to configure unsecured Otis Compass elevators. Unsecured elevators are not associated with readers, input or output points and include floors that users are allowed to access without any specific access right.

- From the System Configuration window, click the plus (+) sign next to the root **Elevator/Cabinet Parameters** icon to display the elevator parameters.
- Click the **Otis Unsecured Elevators** icon and click **Add**. The Otis Unsecured Elevator Configuration dialog box opens.



- Enter a descriptive **Name** for this elevator.
- Select **Public** if you wish the elevator to be visible to all partitions.

5. The **Query String** value is used with message filtering (see “Define Query String Filters” on page 192), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 315).
6. Select from the **Machine Room Enclosure** drop-down list the MRE (1 to 8) that defines a group of elevators that will serve a set of floors. As an option, you can select the Destination Entry Redirector (DER 1 or 2) that connects to all elevator groups for building-wide dispatching.
7. Select from the **Destination Entry Computer** drop-down list the user interface device number into which the desired floor will be entered. This DEC number is associated with the MRE or DER selected.

Note: *The MRE and DEC combination settings must be unique throughout the system.*

8. Select from **Operational Mode** drop-down list whether this is a Mode 1 or Mode 3 elevator. Refer to “Otis Compass Elevator Modes” on page 175 for more information.
9. Select the **Enable Otis PIN** check box to allow unsecured elevators to accept a PIN code to gain access to a floor.
10. Select from the **Report on Terminal** drop-down list, the terminal that will be used to report access grant decisions.

11. Click the **Add** button at the bottom of the window. The Floor Configuration dialog box opens.



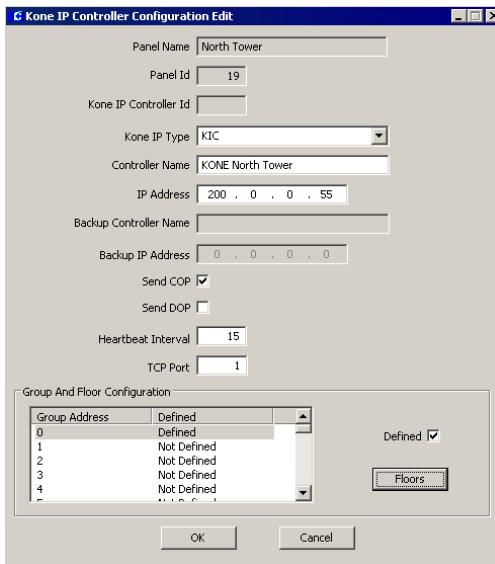
12. Select a **Floor Name** from the drop-down list. The list will display the floors names as configured in the Floor Name Configuration dialog box, see page 191.
13. The floor **Number** index will automatically display in the Number field. You could select the Number first, and the associated floor name will display in the Floor Name field.
14. Click **OK** to return to the Otis Unsecured Elevator Configuration dialog box.
15. After you enter all the information, click **OK** to save your settings and return to the System Configuration window. You will be required to restart the P2000 Otis Interface Service to make effective the changes.

Configuring KONE IP Elevators

Prior to configuring a KONE IP elevator, you must define the KONE IP controller that will serve as the interface to set the configuration parameters related to the elevator controller, as well as the interface to monitor the status of the elevator controller and its communication with the CK721-A panel.

KONE IP Controller Configuration

- In the System Configuration window, click the plus (+) sign next to the panel (CK721-A version 3.1) that will communicate with the KONE IP Controller.
- Select the **Kone IP Controller** icon and click **Add**. The Kone IP Controller Configuration Edit dialog box opens.

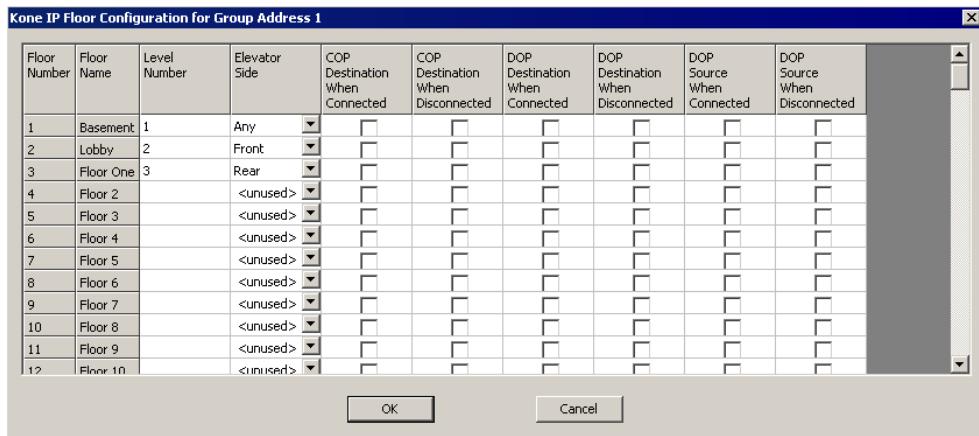


- The **Panel Name** field displays the name of the selected panel, which will be used to communicate with the KONE IP controller.
- The **Panel Id** field displays the identification number assigned to the panel.
- The **Kone IP Controller Id** displays the identification number of the KONE IP controller. This number only displays after you save the record.

- Select from the **Kone IP Type** drop-down list, whether this is a KIC or a Primary/Backup KGC controller.
- Enter the **Controller Name** of the KONE IP controller.
- Enter the **IP Address** of KONE IP controller.
- If you selected a Primary/Backup KGC controller type, enter the **Backup Controller Name** and **Backup IP Address** of the primary/backup controller.
- Select the **Send COP** check box if you wish the system to send COP global default masks messages to the KONE IP elevator controller.
- Select the **Send DOP** check box if you wish the system to send DOP global default masks messages to the KONE IP elevator controller.
- In the **Heartbeat Interval**, enter the time interval at which heartbeat messages are sent to the KONE IP elevator controller.
- Enter the **TCP Port** number of the KONE IP elevator controller.

Kone IP Group and Floor Configuration

The Group and Floor Configuration box at the bottom of the Kone IP Controller Configuration dialog box displays the Group Number of the KONE IP controller and whether the group was defined. You can define up to 33 elevator groups for each KONE KIC controller. Primary/Backup KGC controllers support a single elevator group per controller pair.



- In the Group and Floor Configuration box, select the group number you wish to define and click the **Floors** button. The Kone IP Floor Configuration dialog box opens.
- The **Floor Number** column displays the number of floors configured in Site Parameters.
- The **Floor Name** column displays the floor name assigned to each floor number. Refer to the “Defining Floor Names” on page 191.
- Enter the floor **Level Number** as defined by the KONE equipment.
- Select from the **Elevator Side** drop-down list, the side of the elevator cab through which the selected floor is accessible.
- Select the **COP Destination When Connected** check box to specify whether the selected floor is publicly accessible as a COP destination when the KONE IP controller is online. This value is ignored when communicating to KONE KIC controllers.
- Select the **COP Destination When Disconnected** check box to specify whether the selected floor is publicly accessible as a COP destination when the KONE IP controller is offline. This value is ignored when communicating to KONE KIC controllers.
- Select the **DOP Destination When Connected** check box to specify whether the selected floor is publicly accessible as a DOP destination when the KONE IP controller is online. This value is ignored when communicating to KONE KIC controllers.
- Select the **DOP Destination When Disconnected** check box to specify whether the selected floor is publicly accessible as a DOP destination when the KONE IP controller is offline. This value is ignored when communicating to KONE KIC controllers.
- Select the **DOP Source When Connected** check box to specify whether the selected floor is publicly accessible as a DOP source when the KONE IP controller is online. This value is ignored when communicating to KONE KIC controllers.
- Select the **DOP Source When Disconnected** check box to specify whether the selected floor is publicly accessible as a DOP source when the KONE IP controller is offline. This value is ignored when communicating to KONE KIC controllers.

12. Click **OK** to save the KONE IP group and floor configuration.
13. Select the KONE IP group number just defined and click the **Defined** check box.
14. Click **OK** to save the KONE IP controller.

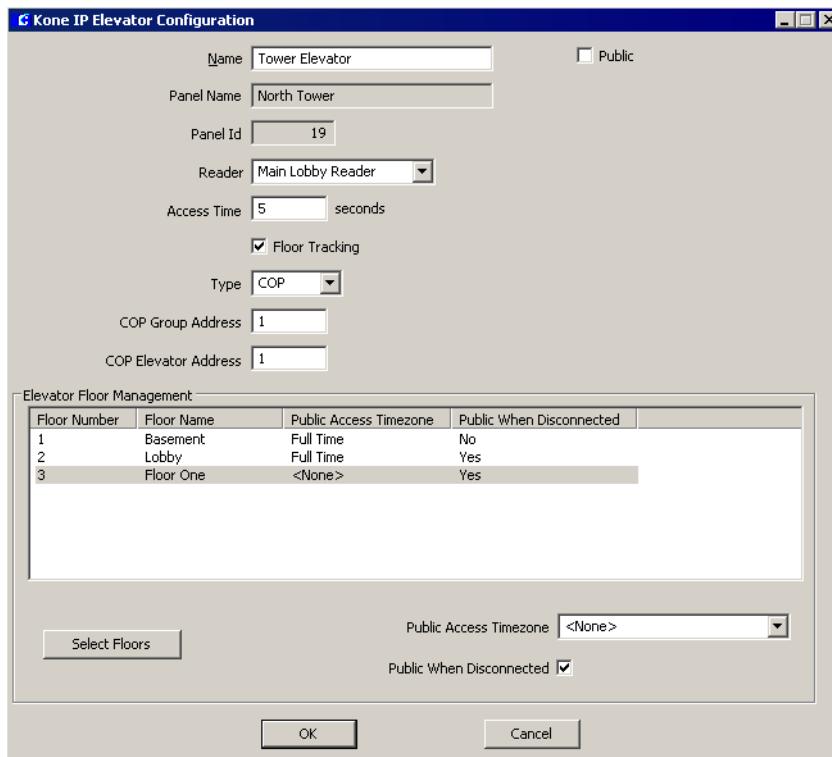
Kone IP Elevator Configuration

Use the Kone IP Elevator Configuration dialog box to define the reader, group and elevator address, and the floor parameters associated with your KONE IP elevator.

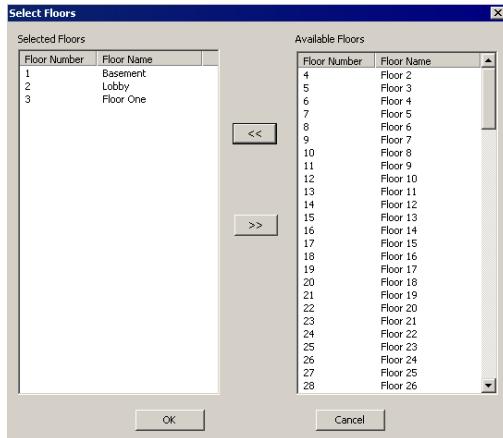
To Configure KONE IP Elevators:

1. In the System Configuration window, click the plus (+) sign next to the panel (CK721-A version 3.1) that will communicate with the KONE IP elevator.

2. Select the **Kone IP Elevator** icon and click **Add**. The Kone IP Elevator Configuration dialog box opens.
3. Enter a descriptive **Name** for the KONE IP elevator.
4. The **Panel Name** field defaults to the panel you selected from the System Configuration window.
5. The **Panel Id** field displays the identification number assigned to the panel.
6. Select from the **Reader** drop-down list, the reader terminal that will provide the access in the elevator cab.
7. In the **Access Time** field, enter the time in seconds that cardholders have to press a car-call button after badging at the elevator.



8. Select the **Floor Tracking** check box to allow the panel to generate a history message identifying the badge number, card-holder's name, elevator, and floor selected when the car-call button is pressed.
9. Select from the **Type** drop-down list, whether this is a COP or DOP KONE IP elevator.
10. Enter the **COP Group Address or DOP Address** of the elevator group. This value must match the address of the elevator group controller.
11. Enter the **COP Elevator Address or DOP Level Number** of the elevator cab.
12. In the Elevator Floor Management box, click the **Select Floors** button. The Select Floors dialog box open.



13. From the **Available Floors** list, select the floors you wish to include in your elevator configuration.
14. Click <<. The floors will be included in the Selected Floors box.
15. Click **OK**.
16. In the Elevator Floor Management list box, select a floor number. From the **Public Access Timezone** drop-down list, select the time zone defined for public access. If

no time zone is selected, this floor is not active for public access.

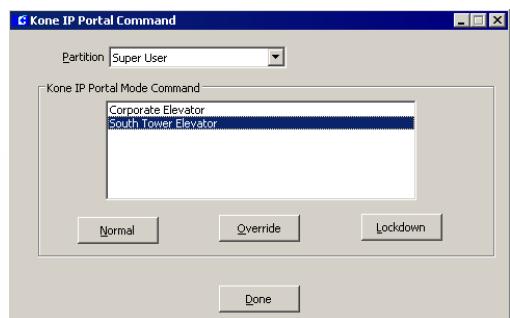
17. Select the **Public When Disconnected** check box to specify whether the floor should be in public access when the KONE IP controller is offline.
18. Repeat this steps for each floor.
19. Click **OK** to save your KONE IP elevator configuration.

Controlling the KONE IP Portal

Operators with the appropriate permissions can manually change a specific KONE IP elevator's mode of operation from a workstation.

To Change Mode of Operation of a KONE IP Elevator:

1. From the P2000 Main menu select **Control>Kone IP Portal Command**. The Kone IP Portal Command dialog box opens.



2. If this is a partitioned system, select the **Partition** in which the elevators are active.
3. Select from the **Kone IP Portal Mode Command** list box, the elevator you wish to control
4. Select one of the following actions:
Normal – to return the elevator to its previous state.

Override – to override access at the elevator. All floors defined for the selected elevator are in public access.

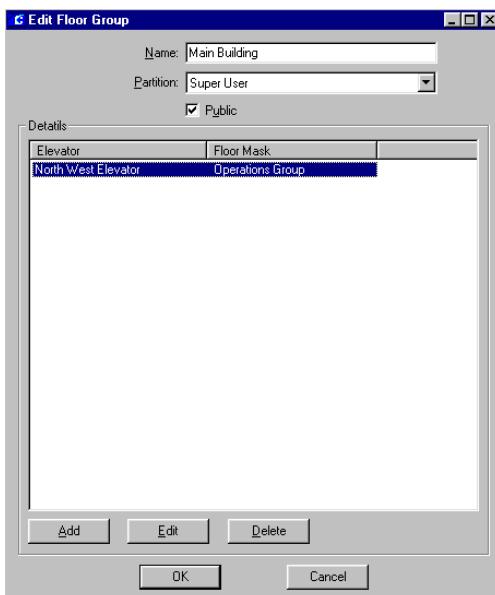
Lockdown – to prevent access to all destination floors.

- Click **Done** to exit the window.

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 218. Refer to this section for detailed information.

Cabinet Access Control

The Cabinet Access Control feature protects sensitive information by monitoring and controlling access to files and equipment contained in a cabinet. The P2000 system allows a single reader to provide access to up to 32 cabinets. Cabinet readers are associated with a set of output points to unlock cabinet doors and an optional set of 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 at the cabinet.

The cabinet access control gives you the ability to assign cardholders 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 cardholders.

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

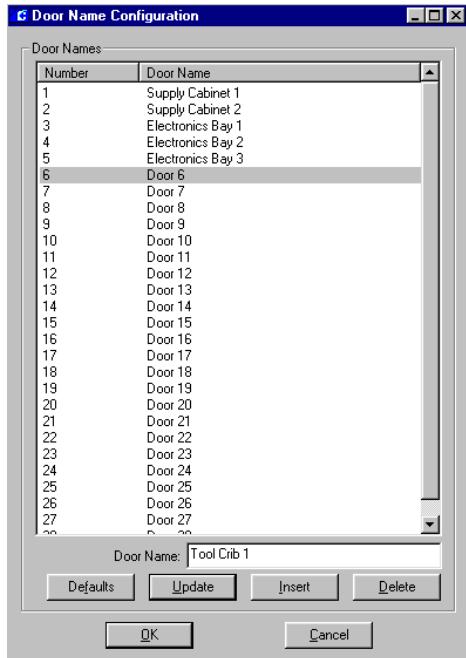
Steps to perform each procedure are presented in the following sections. To successfully implement the cabinet access control, configure these steps in the order presented.

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 "Site Parameters Field Definitions" on page 40.)

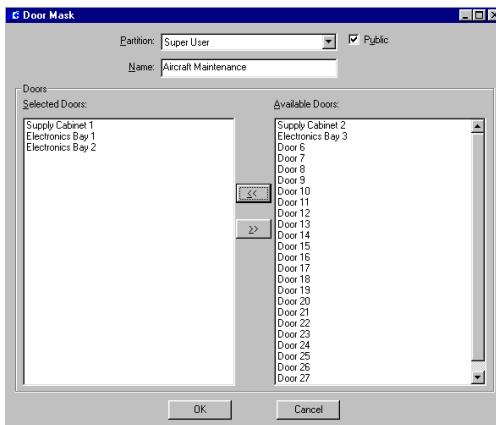
3. Click on the door you wish to rename. The door name will display in the **Door Name** field at the bottom of the window.
4. Rename the door accordingly and click **Insert**. The new name will display and the list of door names will move down one position. For example, if you rename door 1 and door 2, Number 3 on the list will become Door 1.
5. If you wish 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.
8. 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.

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 Masks** icon and click **Add**. The Door Mask dialog box opens.



3. 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.
4. Select the **Public** check box to allow all partitions to see this Door Mask.
5. Enter a descriptive **Name** for the Door Mask. In the example, “Aircraft Mainte-

nance Group” includes Supply Cabinet 1, Electronics Bay 1, and Electronics Bay 2 doors.

6. From the **Available Doors** list, click the door you wish to include in your group.
7. Click **<<**. The door moves to the left side of the dialog box, to be included in the **Selected Doors** box.
8. To remove a door from the Selected Doors box, select the door and click **>>**.
9. 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.

1. From the System Configuration window, click the **Panel** to which you wish to assign a cabinet.
2. Select the **Cabinets** icon and click **Add**. The Cabinet Configuration dialog box opens.
3. Enter the required information according to the following Cabinet Configuration Field Definitions.
4. 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 is used with message filtering (see “Define Query String Filters” on page 211), and is also used with the P2000-Metasys integration feature (refer to “Configuring Hardware Components for BACnet Interface” on page 347).

Reader – Select an available reader from the drop-down list that has not yet been assigned to an elevator or cabinet, and that has an address number no higher than 16.

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

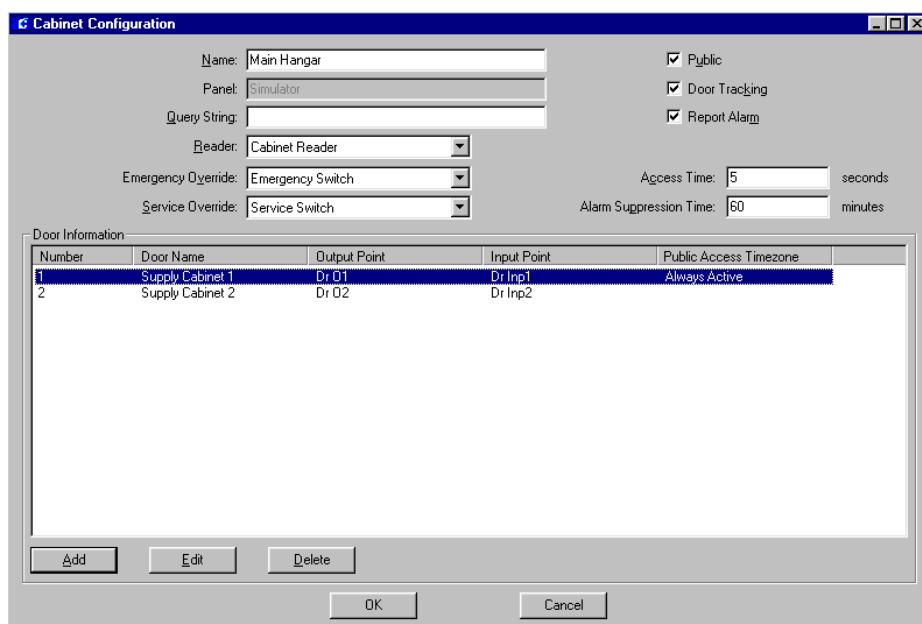
an available input point that has not yet been assigned to an elevator or cabinet. The only purpose of this input point is to send messages to the Real Time List; it does not control Service Override.

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 cardholders have to open a door after badging at the cabinet.

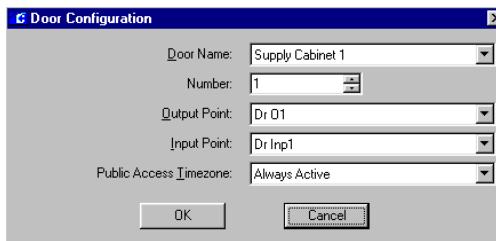
Alarm Suppression Time – Enter the amount of time in minutes (2 to 1440) for a door to remain open.



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.



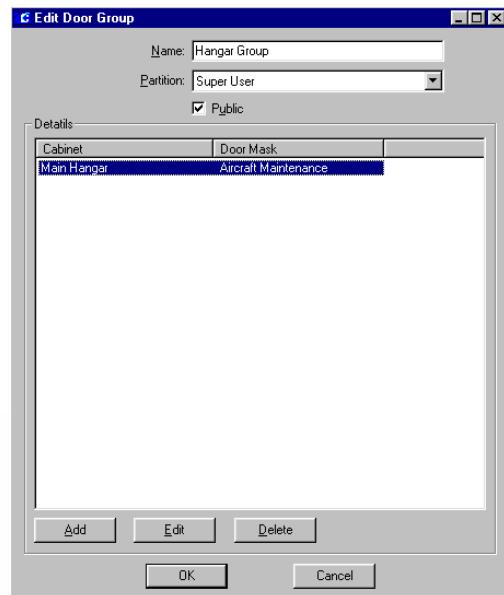
2. Select a **Door Name** from the drop-down list that has not yet been assigned to this cabinet. The list will display the doors names as configured in the Door Name Configuration dialog box.
3. The door **Number** index will automatically display in the Number field. You could select the Number first, 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 cardholders 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.

- Click the **Add** button at the bottom of the dialog box. The Group Detail dialog box opens.



- Select from the **Cabinet** drop-down list a cabinet name, previously configured in the Cabinet Configuration dialog box.
- Select from the **Door Mask** drop-down list a door mask name, previously configured in the Door Mask dialog box.
- Click **OK** to save your entries and return to the Edit Door Group dialog box.
- 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 218. Refer to this section for detailed information.

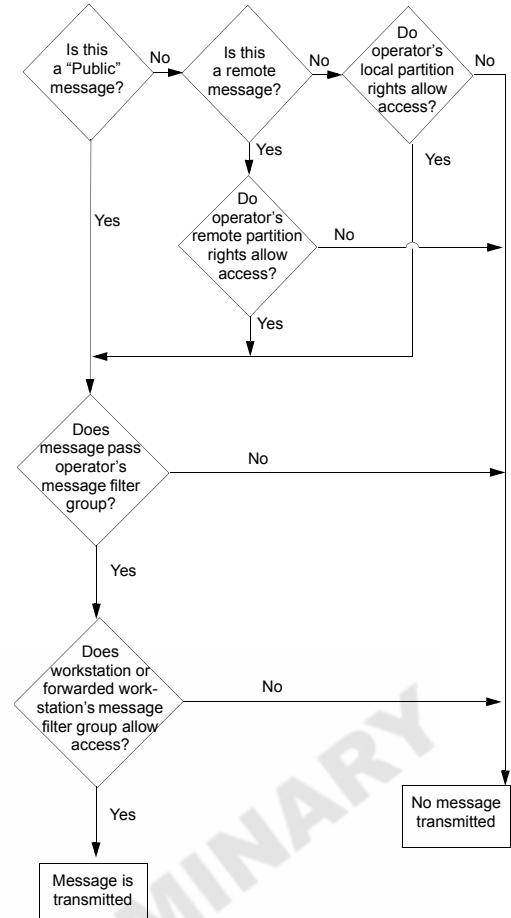
Configure Message Filtering and Message Routing

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 mes-

sages 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 23), operators (page 26), and remote servers (page 217).
- Define Remote Message Service settings in Site Parameters, see “RMS Tab” on page 50.

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.

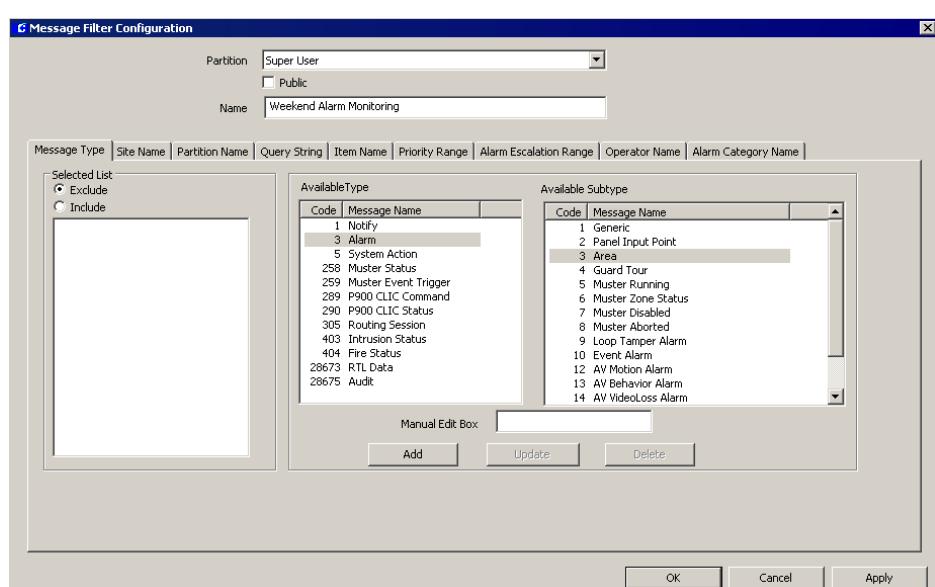
To Create a Message Filter:

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.

- Select the **Message Filter** icon and click **Add**. The Message Filter Configuration dialog box opens.
- If you use Partitioning, select the **Partition** that will have access to this Message Filter.
- If you use Partitioning, select the **Public** check box to allow all partitions to see this Message Filter.
- Enter a descriptive **Name** for this Message Filter.
- 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.

- 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.

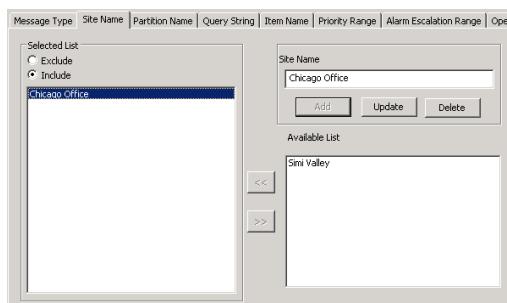


Define Message Types

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.

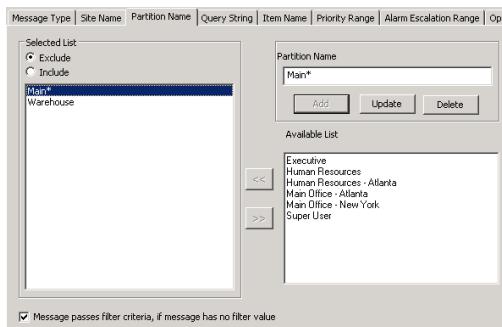
Note: The wildcard character * (asterisk) in a filter string means that all possible selections will be listed. The wildcard character is supported at the end of the filter value only.

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 Edit Operator dialog box.



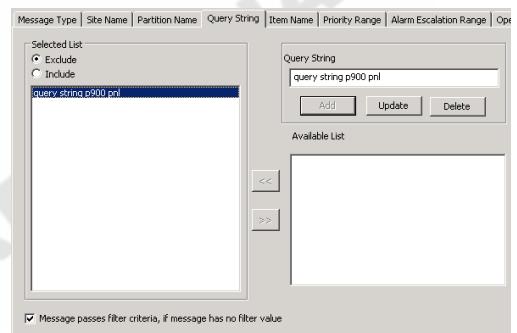
1. Click the **Partition Name** tab.
 2. Select from the **Available List** the Partition Name and click **<<** to move it to the **Selected List**. To remove it from the **Selected List**, click **>>**.
 3. To add a remote partition name to the **Selected List**, enter the name in the **Partition Name** 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.

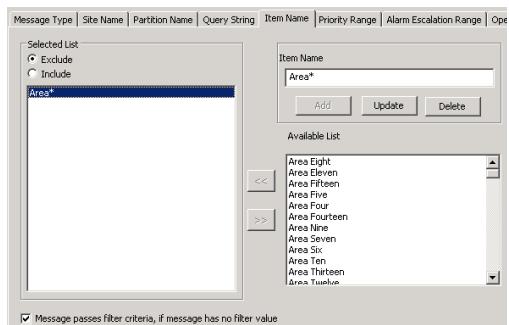
You may enter a filter string to specify more than one Query String, then click the **Add** button.

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.

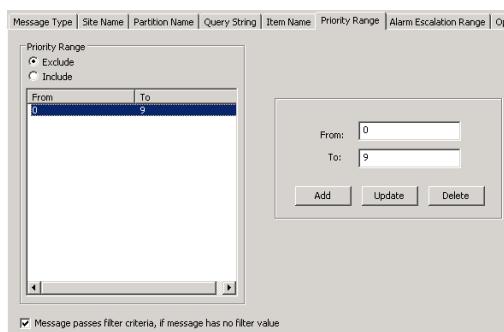
You may enter a filter string to specify more than one Item Name.

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).



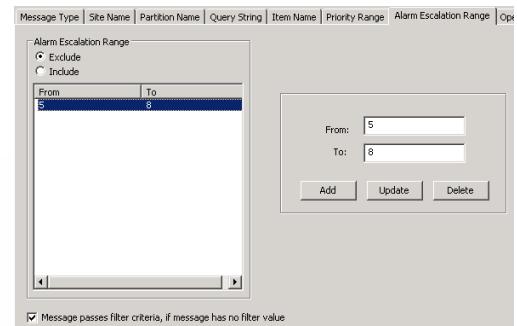
- Click the **Priority Range** tab.
- Enter in the **From** field the start of the priority range.
- Enter in the **To** field the end of the priority range.
- Click the **Add** button. The selected values will display in the **Priority Range** box.
- If you wish to edit the priority range, select the 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 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 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).

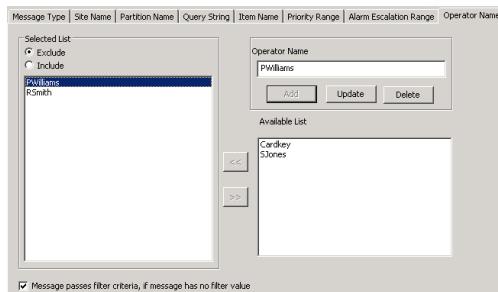


- Click the **Alarm Escalation Range** tab.
- Enter in the **From** field the start of the alarm escalation range.
- Enter in the **To** field the end of the alarm escalation range.
- Click the **Add** button. The selected values will display in the **Alarm Escalation Range** box.

5. If you wish 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 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 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.

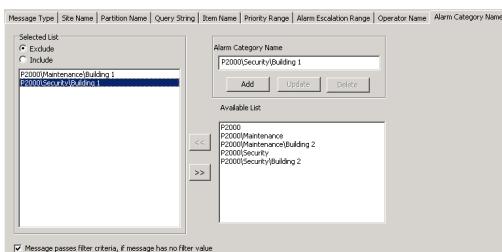
7. To reject all messages associated with the Operator Names selected, click **Exclude**.

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.

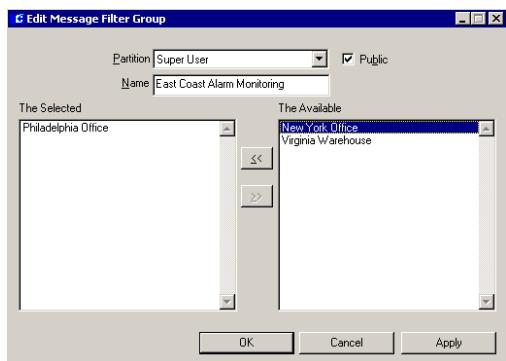
Create Message Filter Groups

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 is 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.

6. 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.

7. To remove a message filter from the **Selected** box, select the message filter and click **>>**.
8. 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 257) and the Real Time List application (see “Monitoring Remote Messages in Real Time” on page 322).

Note: Before you configure any P2000 Remote Servers, verify your settings in the RMS tab of Site Parameters (page 50), to make sure your system is ready to process remote messages.

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:

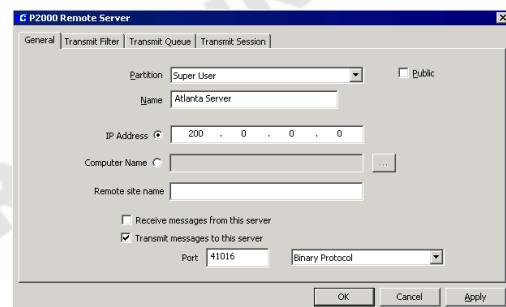
1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Select the **Remote Server** icon and click **Add**. The P2000 Remote Server dialog box opens at the General tab.
3. Fill in the information on each tab according to the following P2000 Remote Server Field Definitions.
4. As you work through the tabs, you may click **Apply** at any time to save your entries.
5. 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 435.

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. This name must match exactly the name of the server at the remote site, including the case.

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.

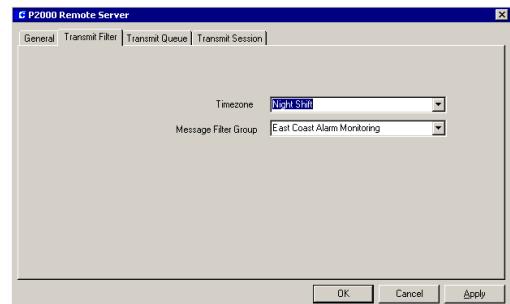
Receive messages from this server – Select this option if you wish to receive messages from this remote server.

Transmit messages to this server – Select this option if you wish 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.



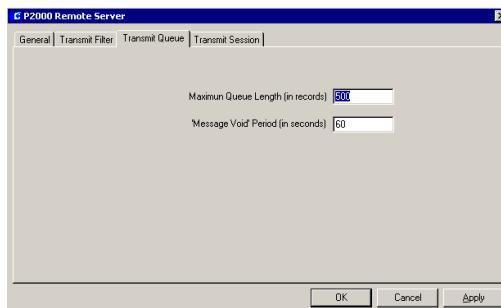
Timezone – Select from the drop-down list the time zone during which messages, that pass the Message Filter Group criteria, will be transmitted to the P2000 remote server. Select <Always Enabled> if you wish to send messages at all times.

IMPORTANT: 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> if you wish to transmit all messages to this remote server.

Transmit Queue Tab

Use this tab to define message queue parameters for the remote server.

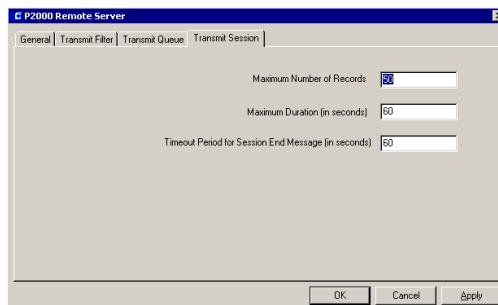


Maximum Queue Length – Enter the maximum number of messages that can be placed in the transmission queue. Messages are transmitted based on the First-In-First-Out (FIFO) principle.

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.



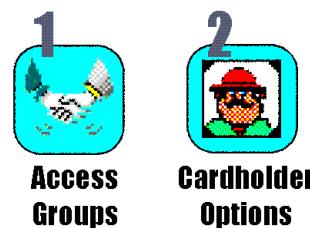
Maximum Number of Records – Enter the maximum number of messages than can be transmitted within one session.

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 Access Groups and Cardholders

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 and Cardholder Options. While Access Groups are assigned from the System Configuration window, Cardholder Options are assigned via the P2000 Main menu. We recommend these elements be assigned in the following sequence:



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 warehouse, to an access group. When you assign a cardholder badge to that access group, the cardholder will be granted access to both doors in the group. This is a quick way to assign badges access to a large number of doors and areas.

If your system is configured to operate elevators and cabinets, elevators floors and cabinet doors can also be assigned to control which floors and doors a cardholder can access.

Once access groups are created, they will be available for assignment in the applications that use access groups. You can assign up to 32 access groups to a badge (depending on the parameters selected in Site Parameters, see “Number of Access Groups” on page 44). In addition, you can also define personalized access groups for each individual cardholder. (See “Personalized Access Groups” on page 243).

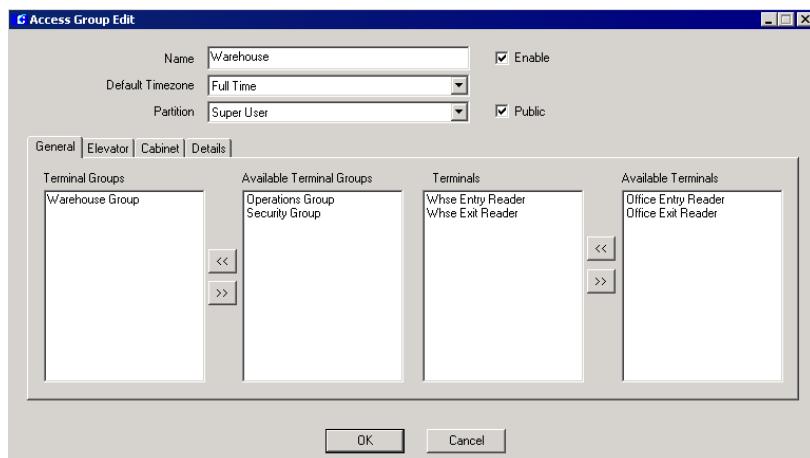
To Create an Access Group:

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. Select the **Default Timezone** during which all terminals (P900 only) included in this

access group will be active. To assign different time zones to the P900 terminals in this access group, click the **Details** tab and follow the instructions provided in step 14.

Note: *The Details tab is only available if you select the “Terminals associated with Timezone” option in the Edit Site Parameters dialog box.*

6. If this is a partitioned system, select the **Partition** name in which the items for this access group reside.
7. Select **Public** if you wish this Access Group to be visible to other partitions.
8. 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.
9. Click **<<** to move the terminal into the **Terminals** box.
10. From the **Available Terminal Groups** list, select the Terminal Group you wish to include in the Access Group.
11. Click **<<** to move it into the **Terminals Groups** box.



12. If you wish 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.
13. If you wish 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.
14. If you wish to assign a different time zone to the any of the P900 terminals selected in this access group, click the **Details** tab, double click the time zone name you wish to change, and select a new time zone from the drop-down list.
15. Click **OK**. The new access group will display under the root Access Groups icon. When you click on the new Access Group icon, the parameters display on the right windowpane of the System Configuration window.

Cardholder Options

At a minimum, a first and last name must be entered into the Cardholder database for each person who will have access to your facility. Cardholder 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 cardholder 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 cardholders, to make this information accessible from the Cardholder Edit dialog box.

You can also create access templates to speed cardholder and badge data entry, as well as create badge purposes to specify the badge's

intention. Complete instructions are presented in the following sections:

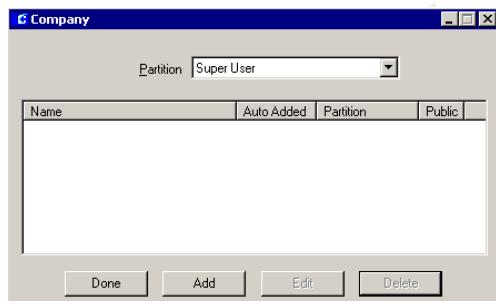
- **Define Companies and Departments**
- **Create Access Templates**
- **Create Badge Formats**
- **Create Badge Purposes**
- **Create Badge Reasons**
- **Create Required Cardholder Fields**
- **Create User Defined Fields**
- **Define Automatic Employee IDs**
- **Entering Cardholders**

Define Companies and Departments

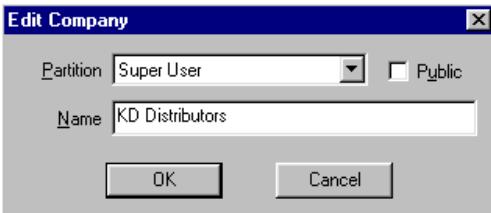
If your facility will include Company and Department as part of Cardholder definition, you must first configure Companies and Departments from the **Config>Cardholder Options** menu. The company and department names will then be available for assignment to cardholders in the Cardholder Edit dialog box.

To Define a Company:

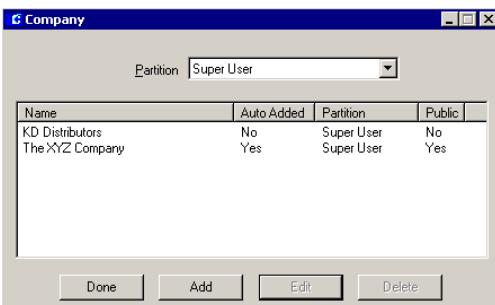
1. From the P2000 Main menu, select **Config>Cardholder Options>Company**. The Company dialog box opens.



2. Click **Add**. The Edit Company dialog box opens.



3. If this is a partitioned system, select the **Partition** to which this company belongs and select **Public** if you wish this company to be visible to all partitions.
4. Enter the **Name** of the company.
5. Click **OK**. The new company name displays in the Company dialog box.

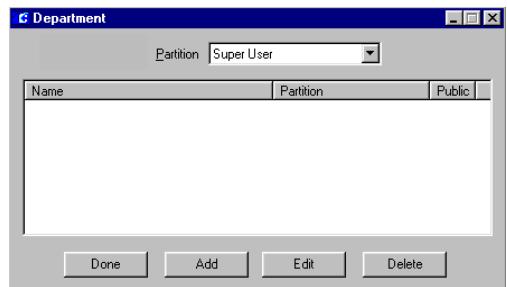


The **Auto Added** column displays company names that were added using other P2000 applications.

6. Click **Done**. Company names will be accessible from the Cardholder Edit dialog box. (See “Entering Cardholder Information” on page 230.)

To Define a Department:

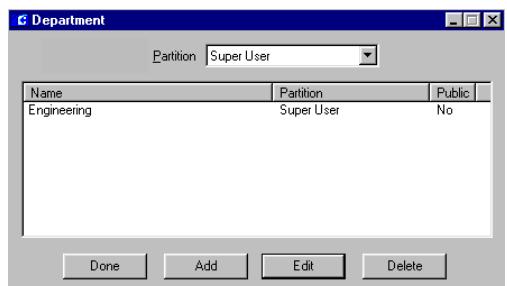
1. From the P2000 Main menu, select **Config>Cardholder Options>Department**. The Department dialog box opens.



2. Click **Add**. The Edit Department dialog box opens.



3. If this is a partitioned system, select the **Partition** to which this department belongs and select **Public** if you wish this department to be visible to all partitions.
4. Enter the **Name** of the department.
5. Click **OK**. The new department name displays in the Department dialog box.



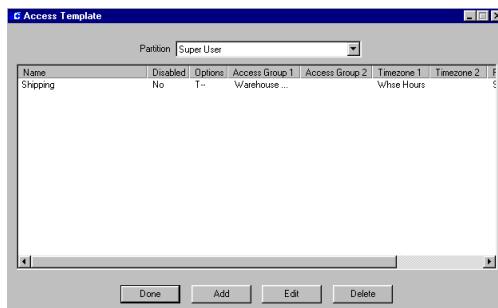
6. Click **Done**. This department name will now be accessible from the Cardholder Edit dialog box.

Create Access Templates

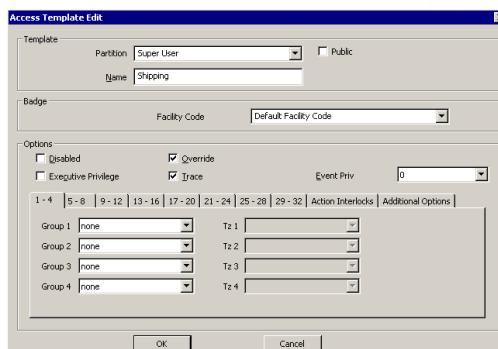
Access Templates are an excellent tool for speeding the entry of cardholders and badges into your system. You may have a large group of cardholders that need badges with the same access privileges. For example, your entire Day Shift Shipping Department may need access to the same group of doors, time zones, and associated input and output groups. An Access Template can be created to apply up to 32 Access Groups and time zones to a badge, simply by selecting the template from the Badge dialog box. You can create a number of Access Templates to speed cardholder data entry.

To Create an Access Template:

1. Select **Config>Cardholder Options> Access Template**. The Access Template window opens.



2. Click **Add**. The Access Template Edit dialog box opens.



3. Enter the information as described in the Access Template Edit Field Definitions.
4. After you have entered all the information, click **OK**. The new Access Template will be listed in the Access Template window. These Access Templates will now be available to assign to badges from the Badge dialog box.

Access Template Edit Field Definitions

Note: The definitions in this section are described in detail in “Badge Field Definitions” on page 238.

Template Box

Partition – If this is a partitioned system, select the Partition in which this access template will be used.

Public – If this is a partitioned system, select Public if you wish this Access Template to be visible to all partitions.

Name – Enter a descriptive Name for the Access Template.

Badge Box

Facility Code – Select from the drop-down list the type of facility code to be assigned to this Access Template. Facility codes are provided by Johnson Controls and identify the cards that belong to your particular site.

Options Box

Disabled – Select if you wish to disable the badges that use this Access Template.

Override – Select if you wish to give override privileges to the badges that use this Access Template.

Executive Privilege – Select if you wish to give executive privileges to the badges that use this Access Template.

Trace – Select if you wish the badges that use this Access Template to be traced throughout the facility.

Event Privilege – Select a privilege level you wish to assign to the badges that use this Access Template.

1-4 through 29-32 Tabs

Use these tabs to select the Access Groups and associated Time Zones to be assigned to the badges that use this Access Template.

Action Interlocks Tab

Use this tab if you wish to allow badges that use this Access Template to activate up to two action interlocks that will be triggered when the badge is granted access. For more information, see “To Set Up BACnet Action Interlocks:” on page 347.

Additional Options Tab

Security Level – Select a security level number from 0 (lowest) to 99 that defines the access privilege to be assigned to badges that use this Access Template.

Guard Tour Priority – Select a priority number from 1 (lowest) to 99 that determines which tours the badges that use this Access Template can perform.

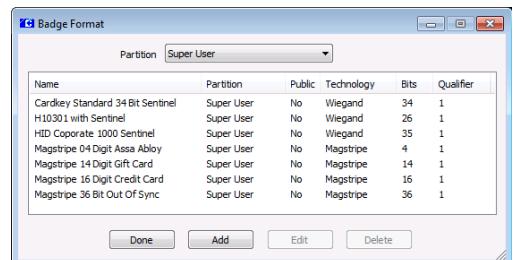
Special Access – Select the special access flags that will be assigned to badges that use this Access Template.

Create Badge Formats

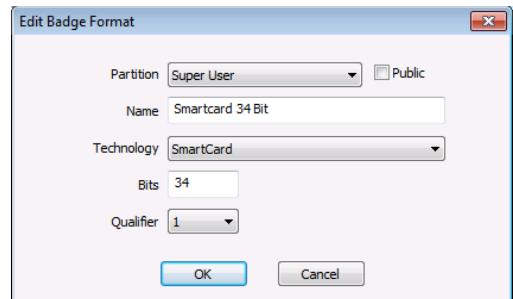
This feature allows you to configure badge format categories to assign to badges. This allows facilities that use multiple badge technologies or formats to differentiate their badges.

To Create Badge Formats:

- From the P2000 Main menu, select **Config>Cardholder Options>Badge Format**. The Badge Format dialog box opens.



- Click **Add**. The Edit Badge Format dialog box appears.



- If this is a partitioned system, select the **Partition** in which the badge format is active.
- Select **Public** if you wish the badge format to be visible to all partitions.
- Enter a descriptive **Name** for this badge format.

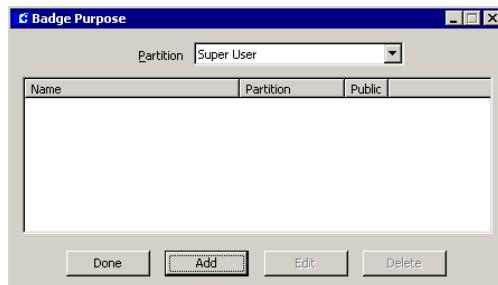
6. Select from the **Technology** drop-down list, the technology type.
7. Enter the total number of **Bits** expected to be returned from the reader when the badge is read.
8. Select a **Qualifier** number. The number selected represents a 32-bit numerical value that allows differentiating formats with the same technology and the same number of bits. The default value is 1.
9. Click **OK**.
10. Click **Done**.

Create Badge Purposes

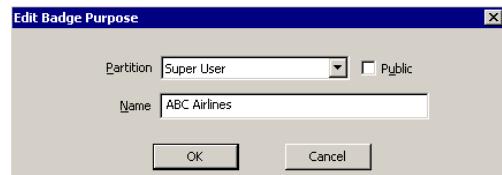
Users can assign a purpose to a badge in order for example, to specify the badge's intention. The Purpose field can be used for different applications. For example, an airport employee may have multiple badges, one for each airline terminal he is allowed to access. The Purpose field for each badge could be used to identify the airline where the badge is valid. Use the Badge Purpose tool to create the different Purpose field values that will be available for assignment in the Badge dialog box.

To Create Badge Purpose Fields:

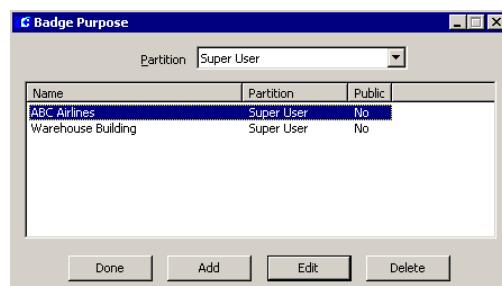
1. From the P2000 Main menu, select **Config>Cardholder Options>Badge Purpose**. The Badge Purpose dialog box opens.



2. Click **Add**. The Edit Badge Purpose dialog box opens.



3. If this is a partitioned system, select the **Partition** to which this badge purpose field belongs and select **Public** if you wish this purpose field to be visible to all partitions.
4. Enter the **Name** of the badge purpose.
5. Click **OK**. The new badge purpose field displays in the Badge Purpose dialog box.



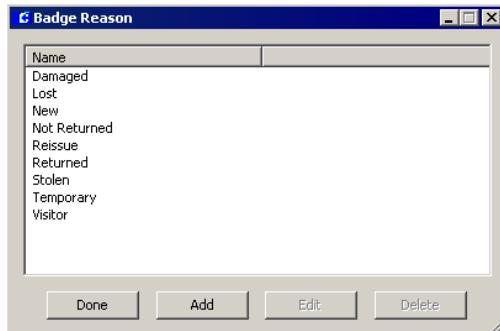
6. Click **Done**. This purpose field will be available from the Badge dialog box.

Create Badge Reasons

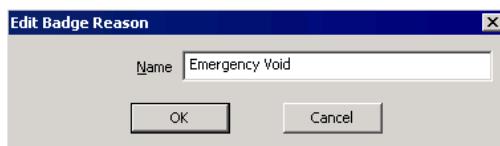
The P2000 system provides a list of predefined badges reasons that are used to indicate why a badge is being issued. This application allows you to define new badge reasons or modify existing ones according to your facility needs, and then assign these reasons to badge records for filtering and reporting purposes.

To Create Badge Reasons:

- From the P2000 Main menu, select **Config>Cardholder Options>Badge Reason**. The Badge Reason dialog box opens.



- Click **Add**. The Edit Badge Reason dialog box opens.



- Enter the **Name** of the badge reason.
- Click **OK**. The new item is added to the list of badge reasons.
- Click **Done**. The badge reason will be available from the Badge dialog box.

Create Required Cardholder Fields

The P2000 system requires that at a minimum, a first and last name must be entered into the Cardholder database for each person that will have access to your facility. However, you can define additional cardholder fields as required fields, which must be completed before a cardholder record is saved.

The Cardholder dialog box will display an asterisk (*) next to a field to indicate a required field. If a required field is left empty, the system will display a warning message to

indicate that a required field has not been completed.

To Create Required Cardholder Fields:

- From the P2000 Main menu, select **Config>Cardholder Options>Required Fields**. The Cardholder Required Fields dialog box opens.



- From the list of **Available** cardholder fields at the right side of the window, select the field you wish to define as a required field.
- Click the << button to move the required field to the **Selected** box. You can add as many fields as you wish.
- To remove a required field from the **Selected** box, select the field and click >>.
- When all the required fields are defined, click **OK**.

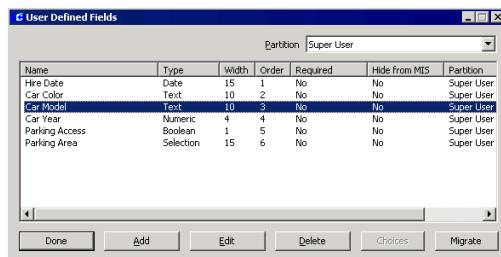
Create User Defined Fields

Use the User Defined Fields (UDF) tool to define your own data fields, which you can access from the Cardholder dialog box to store additional cardholder information.

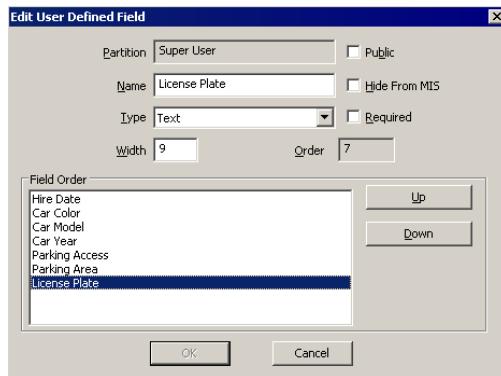
If you wish to restrict operators from viewing certain user defined fields in the Cardholder dialog box, see the instructions provided in “Concealed UDFs Tab” on page 28.

To Create User Defined Fields:

- From the P2000 Main menu, select **Config>Cardholder Options>User Defined Fields**. The User Defined Fields dialog box opens.



- Click **Add**. The Add User Defined Field dialog box opens.



- If this is a partitioned system, the partition name will display in the **Partition** field.
- If this is a partitioned system, select the **Public** check box if you wish to make this field visible to all partitions.
- Enter the **Name** you wish to display as the field title. Names can contain alphanumeric characters, symbols, spaces or underlines.
- Select the **Hide from MIS** check box if you do not wish to display this field in the MIS Interface tables.

7. Select from the **Type** drop-down list, the format in which the data is to be displayed. Select either Text, Numeric, Boolean (toggle field), Date or Selection. The Selection type allows you to define set values to choose from a drop-down list.

8. Select the **Required** check box if this field must always be completed. The system will display a warning message if the field is left empty.

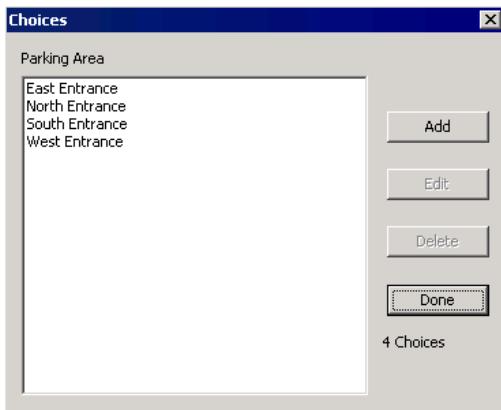
9. In the **Width** field, enter the maximum number of characters allowed in this field.

10. The **Order** box displays the order in which the fields appear in the UDF tab of the Cardholder dialog box. As you add user defined fields, they display in the order they are created. You can however, change the order in which the fields will display by selecting the field from the Field Order box and clicking the **Up** or **Down** button to move the field up or down on the list.

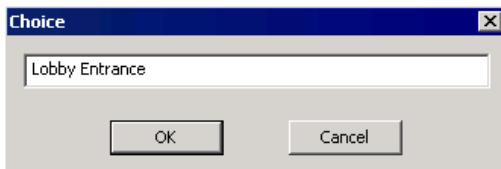
11. After you enter all the information, click **OK** to return to the User Defined Fields dialog box.

12. To delete a user defined field, select the field from the list and click the **Delete** button. A message will display if there are cardholders with values entered in this field. Click **Yes** to continue. When the Delete User Defined field dialog box opens, click **Yes** to delete the field.

13. To add choices to Selection type fields, select the field from the list and click the **Choices** button. The Choices dialog box opens displaying the name of the UDF and the current number of choices.



14. Click the **Add** button. The Choice dialog box opens.



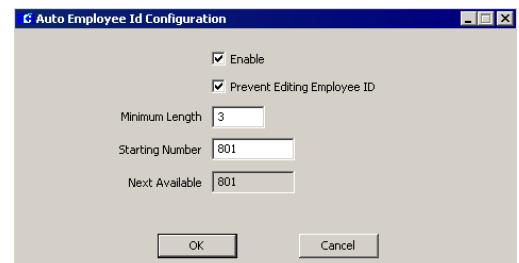
15. Enter the set value for this field and click **OK**.
16. The choice displays in the list. Click **Done** to return to the User Defined Fields dialog box.
17. If you wish to convert a Text type field into a Selection type field, select the Text field from the list and click the **Migrate** button. In the New Type dialog box click **Next**.
18. A Summary window displays a description of the change. All previously values defined for the Text field will be converted to Choices for the new Selection field. Click **Finish**.
19. A message will indicate that the UDF was successfully migrated. Click **OK**.
20. Click **Done** to close the User Defined Fields dialog box.

Define Automatic Employee IDs

Use the Auto Employee Id Configuration tool to define a pool of consecutive ID numbers that will be automatically assigned to each cardholder record created in the system. This means that every time you create a cardholder record you will no longer have to keep track of the last number assigned or the minimum number of characters used for each ID number.

To Configure Automatic Employee ID Numbers:

- From the P2000 Main menu, select **Config>Cardholder Options>Auto Employee ID**. The Auto Employee Id Configuration dialog box opens.



- Select the **Enable** check box to enable the automatic generation of employee IDs. If you wish to use a different number scheme for a particular cardholder, disable this check box and manually assign the ID number.
- Select the **Prevent Editing Employee ID** check box if you wish to make the ID field a display field, no editing allowed.
- In the **Minimum Length** field, enter the minimum number of characters allowed in the ID field. A cardholder ID can have up to 25 characters.
- Define the pool of numbers by entering the first number in the **Starting Number** field.

6. The **Next Available** field displays the next number that will be assigned to the cardholder record.

Note: Automatic Employee IDs are only assigned when you create a new cardholder record. If you wish to edit an existing cardholder record and assign a number from the pool, disable the **Prevent Editing Employee ID** check box and manually enter the next available number from the pool.

7. Click **OK** to save your settings.

Next time you create a cardholder record, the ID field will display the number that was automatically assigned from the pool, and whether the field allows editing.

Entering Cardholders

After all configuration elements have been defined; along with companies, departments, and user defined fields, if applicable; you are ready to enter cardholders into the database. See “Entering Cardholder Information” on page 230 for more detailed information.



APPLICATION NOTE

Commissioning the System: When commissioning the system, we recommend you create at least one or two cardholder records and badges, 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:

- **Provide access to cardholders and visitors**
- **Monitor alarms**
- **Manually control doors, outputs, panel relays, P900 CLIC components, security threat levels, and suppress inputs**
- **Control areas and muster zones**
- **Detect and control intrusion in a facility**
- **Track cardholder's hours on site**
- **Create events**
- **Monitor the system in Real Time**

IMPORTANT: 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.

Providing Access to Cardholders and Visitors

Access privileges define which cardholder or visitor 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; these devices are assigned to specific access groups, and then when cardholder records are added to the database, the cardholders are assigned to the access groups.

The Access feature provides flexible tools to create cardholder records and assign badges with which to grant or deny facility access. At a minimum, a first and last name must be entered into the Cardholder database for each person who will have access to your facility. Additional cardholder information can include personal information such as address and phone; company 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: Cardholder information can be added, deleted, or updated from a database outside the P2000 software using the MIS Interface, see page 341 for more information. MIS is a low-level interface that requires programming to implement.

Cardholder and Visitor information is entered via the Access feature on the P2000 Main menu. The procedures are presented in the following sections:

- **Entering Cardholder Information**
- **Entering Badge Information**
- **Entering Visitor Information**

Entering Cardholder Information

Every person who needs access to the facility must have a Cardholder and Badge record entered into the P2000 system. Cardholders can be entered all at once at system startup, and then added, edited, or removed as necessary thereafter. Permanent cardholders and visitor cardholders are viewed and added in the same Cardholder window.

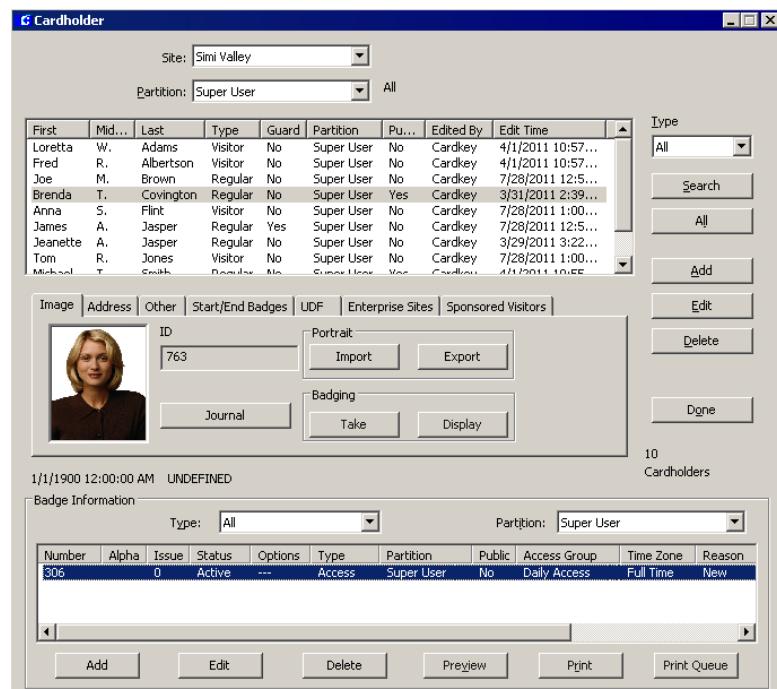
If you use database partitioning, the cardholder can belong to one partition, and could have multiple badges, each in a different partition with different access parameters.

A cardholder may have a number of different badges; however, each access badge must have a unique number.

Viewing Cardholder Information

1. Select **Access>Cardholder** from the P2000 Main menu to open the Cardholder window.
2. To view current cardholder information, select a **Type** from the drop-down list at the right side of the window (All, Regular, or Visitor).

Note: *The system displays up to 20,000 cardholders at a time, for the partition selected in the Partition field. If the number of cardholders in your system exceeds 20,000, you must use the Search feature, described in “To Search for Specific Cardholders.” on page 236.*



Cardholder Types

Regular – These are the permanent cardholders in the system. Their access begins with a start date, but unless terminated or temporarily reassigned, no end date will be specified. Select Regular from the Cardholder window Type drop-down list to view only the regular cardholders.

Visitor – A visitor is given temporary access to the system on a limited basis. Their access will be limited by start and end dates and times, and they are assigned a company Sponsor to take responsibility for them while visiting the facility. Select Visitor from the Cardholder window Type drop-down list to view only visitor cardholders in the system.

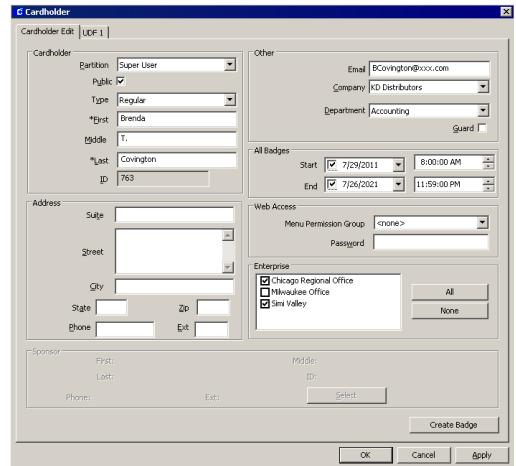
All – When you select All from the Cardholder window Type drop-down list, all cardholders currently in the system display, regardless of cardholder type.

Additional Cardholder Data

When you select a cardholder from the list, additional cardholder data such as Image, Address, Start/End Badges, UDFs, and other information display in the tabs in the middle of the Cardholder window. If the cardholder selected is a Visitor, a Sponsor tab is added to the window and displays limited Sponsor information. Regular cardholders display the Sponsored Visitors tab, which displays the visitors sponsored by the selected cardholder. If your facility uses P2000 Enterprise, a Site field is added at the top of the window, which allows you to view only cardholders that belong to the selected Site name. In addition, the Enterprise Sites tab is also added to the window to display the site names assigned to the cardholder. See “P2000 Enterprise” on page 405 for details.

To Enter New Cardholder Information:

- From the Cardholder window, click **Add**. The Cardholder dialog box opens at the Cardholder Edit tab.



- Enter the information as described in the Cardholder Field Definitions. Required fields are indicated by an asterisk and must be completed before a record is saved.
- You may click **Apply** at any time to save your settings. When you finish click **OK** to return to the Cardholder window, the name of the newly added cardholder will display highlighted in the list box.

Cardholder Field Definitions

Cardholder Tab

Partition – If this is a partitioned system, select from the drop-down list the Partition to which this cardholder is assigned.

Public – If this is a partitioned system, select the Public check box if you wish this cardholder record to be visible to all partitions.

Type – Select Regular or Visitor. If you select Visitor, the Sponsor box at the bottom of the window is activated. (See “Sponsor” on page 233 for more information.)

First – Enter the first name of the cardholder.

Middle – Enter the middle name of the cardholder.

Last – Enter the last name of the cardholder.

ID – This field displays the ID number that was automatically assigned from the Automatic Employee ID pool numbers. Depending on your settings, this field may allow editing. See “Define Automatic Employee IDs” on page 227.

Address

Address fields are optional, unless they are defined as required fields in your facility. Enter the suite, street, city, state, Zip, phone number, and extension, if required.

Other

Email – If available in your facility, enter the email address assigned to this cardholder.

Company and Department – To include this information in your Cardholder database, select a Company and/or Department from the drop-down lists. You must create Companies and Departments before the selections will display in the drop-down lists. See “Define Companies and Departments” on page 220 for detailed information.

Guard – This field is used with the Guard Tour feature and allows you to assign Tour Badges to cardholders who will participate in guard tour operations, see “Guard Tour” on page 352.

All Badges

Start – This is the date and time that badges become active. Select the check box and click the down arrow to select a start date from the system calendar. This date will apply to all badges assigned to this cardholder. If you selected a start date, the time field is enabled. Click the spin box buttons to select the time that badges will be activated.

End – This is the date and time that badges will be voided. Select the check box and click the down arrow to select an end date from the system calendar. This date will apply to all badges assigned to this cardholder. This box is typically used for Visitor badges, but can also be edited as needed to void badges for a terminated employee or similar application. The system will automatically void the badge 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 badges will be voided.

Note: If you create a Visitor badge and do not enter an End date and time, the date and time will default to the Visitor Validity Period value specified in your Site Parameters setting.

Web Access

Menu Permission Group – If your facility uses the Web Access feature, select from the drop-down list the permission group that will be assigned to this cardholder. The cardholder will be allowed to perform any Web Access function defined in this permission group. See “Web Access” on page 409 for detailed information.

Password – Enter the password that the cardholder will use to log on to the P2000 Web Access site.

Enterprise

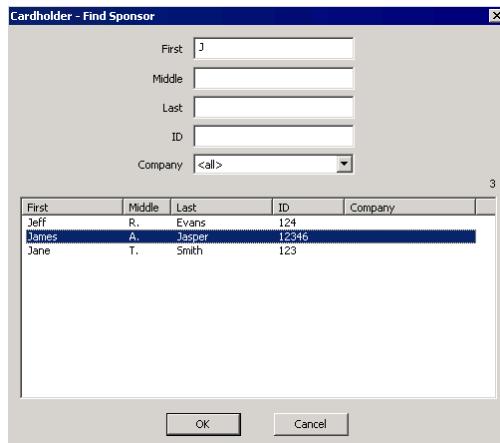
If your facility uses P2000 Enterprise, the Enterprise box will display all the sites defined in the system. Select the check box next to the site that this cardholder may access. See “P2000 Enterprise” on page 405.

Sponsor

If you selected Visitor as the Cardholder Type, the Sponsor box is activated. A sponsor is the name of the cardholder responsible for the visitor.

To Enter a Visitor Sponsor:

- Once the Sponsor box is activated at the bottom of the Cardholder Edit dialog box, after you select **Visitor** as the Cardholder Type, click **Select**. The Cardholder – Find Sponsor dialog box opens.



- Enter a value in any of the fields. The list box will display the cardholder records that match the entered values.

- Select a cardholder name and click **OK** to save the setting and return to the Cardholder Edit dialog box. Basic Cardholder information displays in the Sponsor box.

This information will also display in the Sponsor tab of the Cardholder window.

In addition, when you select a sponsor name from the Cardholder window and click the Sponsored Visitors tab, the list displays all visitors sponsored by the selected cardholder. If you double-click a visitor name in the list, the visitor becomes the selected cardholder.

Adding a Cardholder Image

You can import an existing image to display in the Cardholder Image 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.

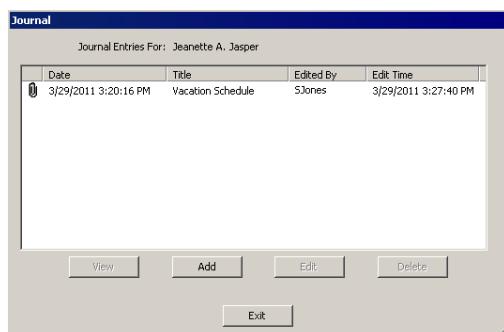
If the workstation is configured as a badging workstation, you can use the Badging buttons to capture an image. See “Video Imaging” on page 337 for details.

Adding a Cardholder Journal

Journal entries supplement cardholder information by storing notes associated with each cardholder. For example, you may want to keep track of cardholders with parking violations, or keep a record of cardholders that attended specific company training, or track cardholders with suspicious behavior.

To Enter Journal Entries:

1. Select a cardholder from the Cardholder list.
2. Click the **Journal** button located in the Image tab in the center of the window. The Journal dialog box opens displaying the journal entries associated with the cardholder together with the date and time when the journal was entered, the name of the operator who last edited the journal, the date and time the journal was last edited, and whether there is an attachment file associated with the journal entry.



3. Click the **Add** button. The Journal Edit dialog box opens.



4. Enter a descriptive **Title** to identify the subject of this note.
5. Click in the text area and enter the details of the note.
6. If you want to add additional information to the note, click the **Import** button and navigate to the directory that contains the text file you want to include. Select the file and click **Open**. The text file will display in the text area.

7. If you wish to save the note as a text file, click the **Export** button and navigate to the directory where the exported notes will be stored. Enter a file name and click **Save**.
8. If you wish to attach a file to the journal entry, click the **Attach** button and navigate to the directory that contains the file you wish to attach. Select the file and click **Open**.
9. If you do not wish to use the attachment file, select the file and click the **Detach** button. The attachment file will be removed from the list.
10. If you wish to save the attachment file, click the **Save** button and navigate to the directory where the attachment file will be stored.
11. If you wish to view the contents of the attachment file, click the **Open** button.
12. To e-mail the attachment file, click the **Email** button. The program will launch your default email client with the file attached. Check with your Internet Service Provider (ISP) or IT department to verify the required email client settings.
13. When you finish with the note details, click **OK** to save the entry and return to the Journal dialog box.
14. To view the contents of a note, select the note from the list and click **View**. When you finish viewing the note click **Cancel**.
15. If you wish to modify an existing note, select the note from the list and click **Edit**; make your changes, then click **OK**.
16. To delete a note, select the note from the list and click **Delete**. You will be prompted for verification.
17. When you finish with the Journal entries, click **Exit**. The Journal button will display the number of notes associated with the cardholder.

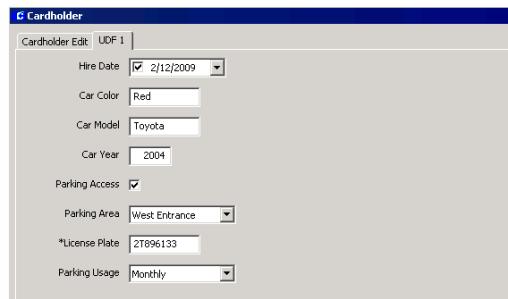
User Defined Fields

After you create User Defined Fields (see page 225), use the UDF tab in the Cardholder dialog box to enter additional cardholder information. The number of UDF tabs displayed depends on the number of UDF fields created. Select additional UDF tabs and enter the data as needed.

Note: The UDF tab displays only the user defined fields that were assigned to the operator. See “Concealed UDFs Tab” on page 28 for details.

To Enter User Defined Field Information:

1. Select a cardholder from the Cardholder list.
2. Click the **Edit** button on the right side of the window. The Cardholder dialog box opens.
3. Click the **UDF 1** tab to display the user defined fields. Required fields are indicated by an asterisk and must be completed before a record is saved.



4. After you enter the information, click **OK** to return to the Cardholder window.
5. Click the **UDF** tab located in the middle of the Cardholder window. The User Defined Fields and entries display for the cardholder selected.

Field		Value
Hire Date	2/12/2009	
Car Color	Red	
Car Model	Toyota	
Car Year	2004	
Parking Access	Yes	

To Edit Cardholder Information:

1. From the Cardholder window, select a cardholder from the Cardholder list.
2. Click **Edit**. The Cardholder dialog box opens.
3. Enter the necessary changes.
4. Click **OK** to save your changes and return to the Cardholder window. Changes will be reflected in the Cardholder list and in the appropriate tabs in the center of the window.

To Search for Specific Cardholders:

1. In the Cardholder window, click the **Search** button on the right side of the cardholder list. The Database Search dialog box opens.

Database Search

First Name	<input type="text"/>
Middle Name	<input type="text"/>
Last Name	Jasper
ID	<input type="text"/>
Company	<all>
Department	<all>
Car Model	Toyota
<none>	<input type="text"/>
Badge Number	<input type="text"/>
Badge Reason	<all>
Badge Purpose	<all>
<input type="button" value="Clear"/> <input type="button" value="Partial Match"/> <input type="button" value="Exact Match"/> <input type="button" value="Cancel"/>	

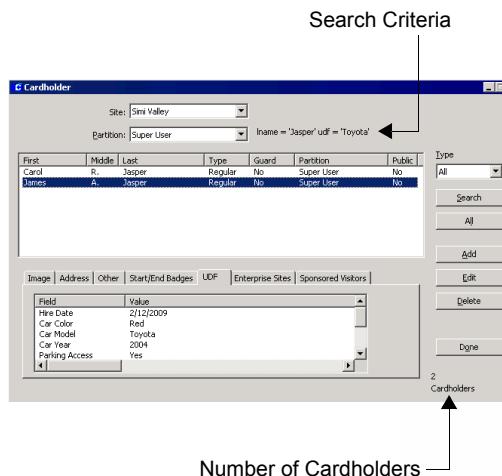
Click to select a UDF

Select UDF search criteria

2. Enter or select from the associated drop-down lists, the information for any or all of the fields to search for specific cardholders.
3. If you wish to search by **Company** and/or **Department**, select a previously defined name from the drop-down list.
4. You can also search by UDF (up to two UDF fields). Select any of the previously defined UDFs (Date type UDFs cannot be included in the search) from the drop-down lists. Then select the associated UDF from the drop-down list.

Note: The UDF list will only display the UDF fields associated with the operator record, see "Concealed UDFs Tab" on page 28 for details.

5. If you wish to clear the existing search criteria, click the **Clear** button.
6. After you define the search criteria, click one of the following buttons:
 - Exact Match** – to display an exact match to your search criteria.
 - Partial Match** – to display all possible selections that match the initial characters of the search criteria, for example if you enter *Carl* in the First Name field, the list box will display names such as Carla, Carlos, Carlton, etc.
7. The Cardholder window opens showing the number of cardholders and the match specified in the search criteria.



8. Click the **All** button on the right side of the Cardholder window to restore it to display all cardholders.

Entering Badge Information

The Badge Information box in the Cardholder window displays all badge information for the cardholder selected from the Cardholder list. A badge can be created strictly for identification, or it can be assigned access privileges.

To Enter Badge Information:

1. In the Cardholder window, select a cardholder from the Cardholder list.
2. In the **Badge Information** box at the bottom of the Cardholder window, click **Add**. The Badge dialog box opens.

The screenshot shows the 'Badge' dialog box. It has tabs for 'Badge' and 'Cardholder'. The 'Badge' tab is active, showing fields for Partition (Super User), Number (302), Facility Code (Default Facility Code), Alpha (AA1), Issue (0), Description (empty), Pin (12345), Purpose (ABC Airlines), Reason (New), Start (10/7/2011 8:00:00 AM), End (10/4/2021 11:59:00 PM), and Design (<none>). Below these are sections for 'Simi Valley | Enterprise' with 'Security Options' (checkboxes for Disabled, Executive, Trace, Override, Download STI E, Special Access A, Special Access B, Special Access C) and 'Event Privilege' (checkboxes for Level, Privilege, Guard Tour Priority). Buttons at the bottom include 'Duplicate', 'Print', 'Preview', 'OK', 'Cancel', and 'Apply'.

TIP: You can also access the Badge dialog box from the Cardholder Edit tab by selecting **Create Badge** at the bottom of the window.

3. Enter the information as described in the Badge Field Definitions.
4. When all information is entered, click **OK** to return to the Cardholder window. The

new badge will be listed in the Badge Information box at the bottom of the window.

Note: Use the **Duplicate** button at the bottom of the Badge dialog box to create any number of badges for a cardholder. All current badge information will be copied; however, each badge must have a unique number.

Badge Field Definitions

Badge

Partition – If this is a partitioned system, select the Partition in which this badge will be active.

Public – Select Public if you wish this badge record to be visible to all partitions.

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 44). This number is usually pre-assigned to badges provided by Johnson Controls. Access and Identification badges can have the same number. If your system is configured to use FASC-N badges, see “FASC-N Badges” on page 239 for instructions on generating this number.

Auto – If your facility is set up to use the Auto-Badge Management feature (see page 249), click the Auto button to insert the next available badge number in the Number field. Not available for FASC-N badges.

Facility Code – Select from the drop-down list the facility code to be assigned to this badge. Facility codes are defined in Site Parameters (see page 46), and identify the badges that belong to your particular site. Not available for FASC-N badges.

Alpha – Some custom badges may provide space for additional characters. If so, enter them here. (Limited to 4 characters.) Not available for FASC-N badges.

Issue – Select an issue level. If a cardholder 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 44.

Description – If desired, enter a description of this badge. (Up to 32 characters.)

Pin – Enter the cardholder or visitor personal identification number (PIN) to be used with PIN readers. If an algorithmic PIN is used, leave this field blank.

Start – Select the date and time this badge becomes active. Click the down arrow to select a date from the system calendar and click the spin box buttons to select a time.

End – Select the date and time this badge will be automatically voided. Click the down arrow to select a date from the system calendar and click the spin box buttons to select a time. If this is a Visitor badge and no End date and time is entered, the badge will be automatically voided as configured in Site Parameters, see page 40 for more information.

Note: The time used to void a badge is based on the P2000 Server time and not the time defined for a panel. The panel time may be different if a Time Offset was defined, see page 66 for details.

Type – Select a badge Type from the drop-down list. Choices are: Access or Identification.

Format – Select from the drop-down list, the badge format to be assigned to this badge.

Purpose – If you wish to include this Badge information, select a Purpose from the drop-down list to indicate the badge's intention. You must create Purpose fields before the selections will display in the drop-down list. See “Create Badge Purposes” on page 224.

Reason – Select a Reason from the drop-down list to indicate why the badge is being issued. You can add or edit badge reasons using the Edit Badge Reason application, see “Create Badge Reasons” on page 224.

Design – If you have created a number of badge designs using your Video Imaging software, you can select a design from the drop-down list. (Badge design instructions are provided in the *P2000 Integrated Video Imaging Installation and Operation Manual*.)

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.

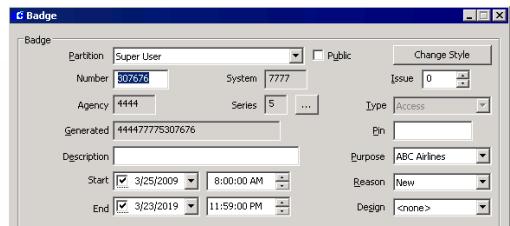
Note: *Smart card encoding is only available if the Video Imaging software option used at your facility is EPI Builder.*

To support the Federal Government smart card encoding protocol, an encoded 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 a cardholder should be granted access to specific buildings and controlled places.

To create FASC-N badges, the Badge Edit Style selected for your facility (see page 44), must be defined as **FASC-N Only** or **Normal and FASC-N**.

- If **FASC-N Only** was selected, click the **Add** button in the Badge Information box at the bottom of the Cardholder window, or click the **Create Badge** button in the Cardholder Edit tab.
- If **Normal and FASC-N** was selected, click the **Add** down arrow in the Badge Information box at the bottom of the Cardholder window and select **Add FASCN**. The **Create Badge** button in the Cardholder Edit tab will only allow you to create FASC-N badges.
- To create Normal badges if **Normal and FASC-N** is selected, click the **Add** down arrow in the Badge Information box at the bottom of the Cardholder window and select **Add Normal**.

When the badge dialog box opens, the fields will display the default values defined in Site Parameters (see page 44) to generate a 15-digit badge number as described below.



Number – This is a six-digit unique badge number assigned to the cardholder.

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.

Agency – This is a four-digit unique number identifying the government agency issuing the badge.

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.

The Agency, System, and Series default values will be used for all badges created in the system, however, an authorized operator can enter specific values for a specific badge. The [...] button on the right side of the Series field opens the FASC-N Fields dialog box.



You can change 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 **Defaults** button.

Once the badge record is saved, and if the Badge Edit Style used at your facility is **Normal and FASC-N**, you can edit the badge and use the **Change Style** button at the top right corner of the window to change the badge style, if necessary.

Security Options Tab

These options allow you to define access privileges for a cardholder. Access decisions are made based on the privileges assigned to the badge.

Note: Some security options are panel specific. See Appendix C: Panel Comparison Matrix for a detailed list of features and capabilities supported by your panel type.

In Enterprise systems, the Badge dialog box displays the site name tabs of the sites assigned to the cardholder. The first tab is always the local site tab and is used to assign local access privileges. The second tab is the Enterprise tab and is used to assign global access privileges. Additional tabs show other site names assigned to the cardholder.

Assigning access privileges is determined by the following conditions:

- When you define access to the local site, and select the **Apply Security Options ‘Enterprise’** check box, the security options defined in the Enterprise tab will be applied.
- When you define access at a different site, and select the **Apply Security Options ‘Enterprise’** check box, the security options defined in the Enterprise tab will be applied to that site.

For more information, see “P2000 Enterprise” on page 405.

Disabled – When a badge is created, it is automatically enabled. Select this check box to disable this badge. This function is useful when you wish to disable a badge, but do not wish to re-issue or redefine a badge for this cardholder.

Executive – If enabled, the cardholder will have unlimited access to all operational doors controlled by the access control system, regardless of any other privileges programmed for this badge. (If a specific terminal requires the use of a PIN code with a badge, the PIN code is still required.)

Trace – Enable to trace cardholder movement throughout the facility. Badge transactions will be printed, as they occur, on any printer configured to print trace transactions, as long as the Badge Trace and Printing options are selected in the Real Time List window.

Override – If enabled, the cardholder can unlock any door controlled by a keypad reader that has the Override option enabled. See page 84 and page 146 for information on setting up this option at the Terminal.

Download to STI-E – This option applies only to legacy panels using STI-E terminal interfaces. If selected, the badge 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.

Special Access – Special Access flags are defined in the Site Parameters dialog box, see page 41. Enable any of the three special access flags if the cardholder requires special access at a reader. Special access allows a door's access time to be different. See “Assisted Access Box” on page 85 and “Configure OSI Facility Parameters” on page 129.

Security Level

Select from the drop-down list a security level number from 0 (lowest) to 99 or the maximum security level set up at the Site Parameters dialog box. To obtain access at a door, this number must be equal to or greater than the security level set up at the terminal. If the security level at the terminal is raised, cardholders will

be denied access, unless the badge has the Executive privilege enabled.

Event Privilege

Every badge has an event privilege level, ranging from 0 to 7, with zero as the lowest level. If a cardholder'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

The Priority field is used with the Guard Tour feature. Select from the drop-down list a priority number from 1 (lowest) to 99. This number determines which tours the selected cardholder can perform. Only tour badges with equal to or greater than this priority can perform a tour.

Access Rights Tab

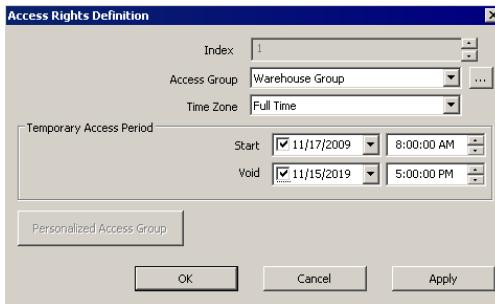
Use this tab to define the Access Groups and corresponding Time Zones that will be assigned to this badge. The number of groups displayed here depends on the parameters selected in the Site Parameters dialog box (see “Number of Access Groups” on page 44). See “Badge Access Rights” on page 129 for details associated with OSI panels.

Index	Access Group	Timezone	Valid From
1	Night Shift	Full Time	
2	Warehouse	Whse Hours	
3	<none>	<none>	
4	<none>	<none>	
5	<none>	<none>	
6	<none>	<none>	
7	<none>	<none>	
8	<none>	<none>	
9	<none>	<none>	

Buttons at the bottom: Edit, Remove, ...

To Define Access Rights:

1. In the Access Rights tab, double-click the line item you wish to define. The Access Rights Definition dialog box opens.



2. The **Index** number automatically displays. Select from the drop-down list, the **Access Group** you wish to assign to this badge.
3. If you wish to modify the settings in the selected Access Group, click the [...] button to open the Access Group Edit dialog box. Make your changes and click **OK** to return to the Access Rights Definition dialog box.
4. In the **Time Zone** field, select a time zone that will be assigned to the selected Access Group. If the Access Group selected includes P900 terminals, the system will use the default time zone defined for each P900 terminal, regardless of the time zone selected here. See page 219 for details on creating access groups.
5. If you wish to define a **Temporary Access Period** for the selected Access Group, select the check box and use the drop-down lists to select the **Start** date and time when permission for access will be granted. If the check box is not selected, access will be allowed immediately.

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 cardholder 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 433. This feature only works on terminals running in Local mode.

6. Select the **Void** check box and use the drop-down lists to select the stopping date and time when permission for access will expire.
7. Click **Apply** to save your settings. To assign another access group to this badge or see other definitions, click the spin box next to the Index field.
8. To define personalized settings, click the **Personalized Access Group** button and enter your settings. See "Personalized Access Groups" at the end of this section.
9. Click **OK** to return to the Access Rights tab.
10. To remove a definition, select the line item and click the **Remove** button.
11. The list displays the access groups assigned to the badge. To edit an access group, select the line item and click the [...] button.

Personalized Access Groups

When assigning access groups to a badge, you can use personalized access group for each cardholder. The Personalized Access Group button provides a shortcut to set up access groups without the need of scanning through all existing access groups.

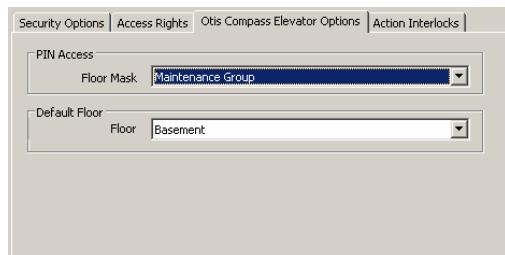
By default, the Name of the access group will always be the name of the cardholder. However, be aware that the name of the access group is NOT automatically modified if you change the name of the cardholder.

Once you have all the access group elements defined, such as terminals, terminal groups, elevators or cabinets, click **OK**. The new personalized access group will display automatically in the Access Group field. Assign a time zone to the new access group as you would for any other access group.

Note: Although initially created for a particular cardholder, a personalized access group becomes a standard access group within the P2000 system and CAN also be assigned to other cardholders.

Otis Compass Elevator Options Tab

Use this tab to define parameters for cardholders that need access to Otis Compass elevators.



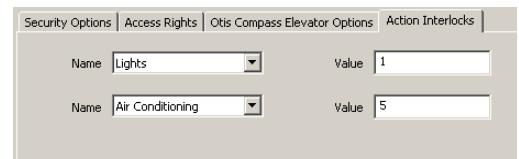
Floor Mask – For Otis Compass elevators that are configured for PIN entry, select from the

drop-down list the floor mask that contains the floors that this badge is able to gain access to when they enter a PIN code at the elevator.

Floor – Select from the drop-down list the default floor for the user. When the badge is swiped, depending on the operational mode of the elevator that is being used, that badge's default floor is used to dispatch an elevator, assuming the default floor is an authorized or an allowed floor.

Action Interlocks Tab

Action Interlocks allow the P2000 system to initiate actions in BACnet devices. Use this tab if you wish a badge to activate up to two action interlocks that will be triggered when the badge is granted access. For more information, see “Setting Up BACnet Action Interlocks” on page 347.



Access Template

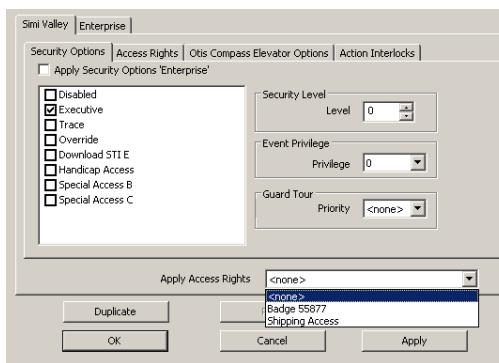
If a large number of cardholders will use badges having the same options, you can set all badge options at once by applying an Access Template. The Access Template contains preset badge options, access groups, and time zones, and will override any settings already defined in the Badge dialog box, before the template was applied. You can edit badge options individually after the template is applied; if you re-select the template, the settings will again mirror the template settings. In addition, if you make changes to an Access Template, you will have to re-select the template to apply the new settings.

Note: Access Templates must first be created before they are available in the Badge dialog box. For more information, see “Create Access Templates” on page 222.

Note: In addition to selecting Access Templates from the **Apply Access Rights** drop-down list, you can also select another badge owned by the same cardholder and apply the same access rights from the selected badge.

To Apply Access Rights to a Badge:

- From the **Apply Access Rights** drop-down list, at the bottom of the Badge dialog box, select the Access Template or badge number you wish to apply to the badge. All access options defined for the Access Template or selected badge number, will be applied to the badge.



- If you wish to change specific badge options, access groups, or time zones for this badge, you may do so. All other settings will remain in effect.

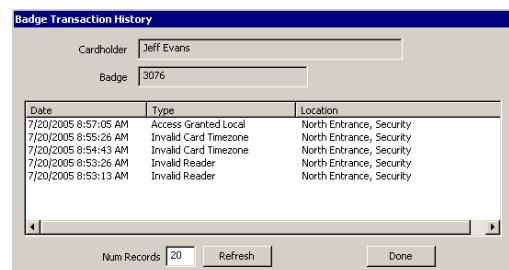
Viewing Badge Data

Badge information such as Number, Status, Options, Type, Partition, and Access Group displays in the list box at the bottom of the

Cardholder window. When you select a cardholder from the Cardholder list, all badges assigned to that cardholder display in the Badge Information box. You can also display the badge’s transaction history.

To Display Badge Transaction History:

- In the Cardholder window, select a cardholder from the list.
- In the **Badge Information** box, right-click the badge number you wish to view.
- From the shortcut menu select **Transaction History**. The Badge Transaction History dialog box opens displaying the selected Cardholder name and Badge number.



The list box displays the date, transaction type and location where the badge was presented.

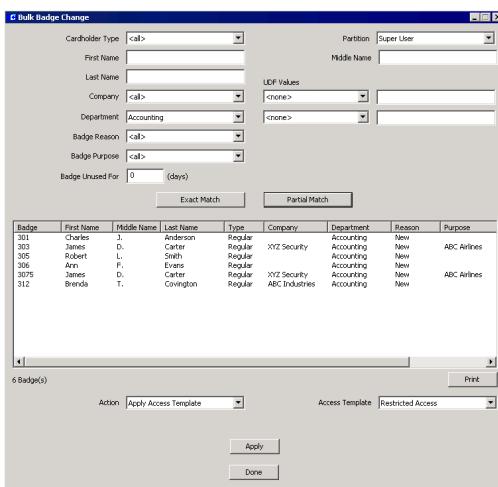
- To change the number of transactions displayed, enter the desired number in the **Num Records** field.
- To update the list box with new data, click the **Refresh** button.
- Click **Done** to close the dialog box.

Bulk Badge Change

The Bulk Badge Change tool is used to change badge parameters across multiple records, in a single operation. This feature not only allows you to save time by modifying multiple records at once, but also improves the accuracy from single record editing, and avoids the hassle of updating badge records one entry at a time. In addition, you can also delete multiple badges and/or associated cardholder records at the same time.

To Bulk Change Badge Records:

- From the P2000 Main menu, select **Access>Bulk Badge Change**. The Bulk Badge Change dialog box opens.



- Enter or select from the associated drop-down lists, the information for any or all of the fields to search for specific cardholder records.
- If you wish to search by **Company** and/or **Department**, select a previously defined name from the drop-down list.
- You can also search by UDF (up to two UDF fields). Select any of the previously defined UDFs (Date type UDFs cannot be included in the search) from the

drop-down lists. Then enter the UDF search criteria in the associated fields.

- If you wish to search for badges that have not been used for a while, enter in the **Badge Unused For** field the number of days that the badges have not been used.

- After you define the search criteria, click one of the following buttons:

Exact Match – to display an exact match to your search criteria.

Partial Match – to display all possible selections that match the initial characters of the search criteria, for example if you enter *Carl* in the First Name field, the list box will display names such as Carla, Carlos, Carlton, etc.

- Once the list box displays the cardholders specified in the search criteria, select from the **Action** drop-down list one of the following options:

Add Access Group – to assign all badges in the list box with access to all terminals defined in the access group. Select the **Access Group** and **Timezone** that will be assigned to the selected badges. The access group will be added to the first available slot on the badges.

Apply Access Template – to apply all preset access privileges, badge options, access groups, and time zones that were defined in the access template. Select from the **Access Template** drop-down list, the Access Template that will be applied to the selected badges.

Note: You cannot apply Facility Code settings using the Bulk Badge Change function.

Delete Access Group – to remove from the selected badges access to all terminals defined in the access group. Select the **Access Group** to remove.

Delete Badge – to delete all badges in the list box.

Delete Badge and Cardholder – to delete all badges and associated cardholders in the list box.

Note: If a cardholder owns more than one badge, and that badge is not included in the list box, the cardholder record will not be deleted.

Disable Badge – to disable all badges in the list box.

Replace Access Group – to replace the existing access group. Select from the **New Access Group** drop-down list the access group you wish to assign. Select from the **Old Access Group**, the access group you wish to replace. The original timezone for the access group will not be changed.

8. If you wish to print the data in the list box, click the **Print** button.
9. Click **Apply** to change the selected badge records.
10. Click **Done** to close Bulk Badge Change.

Entering Visitor Information

The Add Visitor function introduces an easier and faster way to enter visitor and badge information, by allowing authorized operators to enter visitor and badge data using a single user interface. Prior to a visitor's arrival, the operator enters the appropriate visitor data into the system, assigns a visitor sponsor, enters the date and time period of the scheduled visit, and assigns access privileges using Access Templates, subsequently and from the same screen, the visitor badge is printed.

To Enter Visitor Information:

1. From the P2000 Main menu, select **Access>Add Visitor**. The Add Visitor dialog box opens.
2. See the following “Add Visitor Field Definitions” for detailed information.
3. After you enter all the information, click the **Save** button to save the visitor and badge information. The new visitor data will also be reflected in the Cardholder window.

4. If you wish to save and print the badge, click the **Save and Print** button (requires the Video Imaging application).
5. If you wish to enter additional visitors, click the **Clear** button, then enter the information according to the “Add Visitor Field Definitions”.
6. Click **Exit** to close the Add Visitor dialog box.

Add Visitor Field Definitions

Visitor Box

First – Enter the first name of the visitor.

Middle – Enter the middle name of the visitor.

Last – Enter the last name of the visitor.

ID – Enter a unique ID for this visitor (up to 25 characters).

Company – Select from the drop-down list, the visitor’s Company name. If the company name does not already exist in the database for the visitor’s assigned partition, click the browse button [...] to open the Company window. See “Define Companies and Departments” on page 220 for information on adding a company name to the P2000 database.

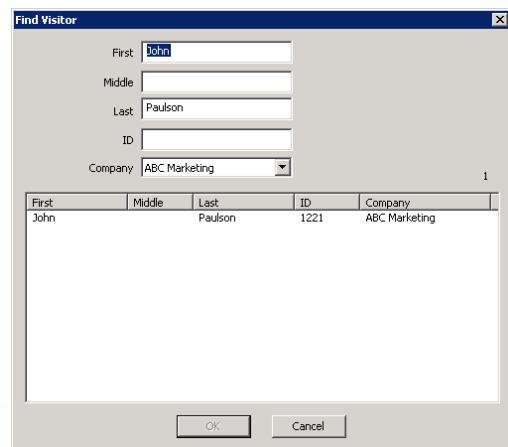
Partition – Select from the drop-down list, the partition to be assigned to the visitor.

Found in DB – Indicates whether or not P2000 has identified a matching Visitor record in the cardholder database after you click the **Search** button. If **Found in DB** shows **Yes**, then the existing visitor record in the P2000 database will be updated. If it shows **No**, the new visitor will be added when you click the **Save** button.

Approved Visits – Displays the number of approved visits. This field is only valid if the **Found in DB** field displays **Yes**.

Note: The Add Visitor application creates four UDFs: **Approved Visits**, **Most Recent Visit**, **Second Most Recent Visit**, and **Third Most Recent Visit**. These UDFs are automatically updated and allow you to monitor the visits associated with the selected visitor.

Search – If the visitor information already exists in the database, you may search the database by entering a value in any of the Visitor fields and then clicking the **Search** button. The Find Visitor dialog box opens displaying the visitor record(s) that match the entered value(s). You may also click the **Search** button without entering any values to display all visitors in the database.



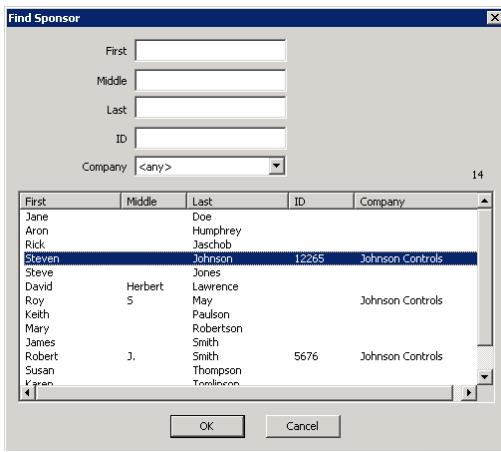
Select the visitor’s name and click **OK**.

Take – If your facility uses the Video Imaging application, click the **Take** button to capture the visitor’s portrait. See the instructions on page 340 (step 4.) for details on capturing portrait images.

Sponsor Box

- First** – Displays the first name of the person who will sponsor this visitor.
- Middle** – Displays the middle name of the person who will sponsor this visitor.
- Last** – Displays the last name of the person who will sponsor this visitor.
- ID** – Displays the unique ID assigned to the sponsor (up to 25 characters).
- Company** – Displays the sponsor's Company name.
- Partition** – Displays the partition assigned to the sponsor.

Search – Click this button to find a Sponsor in the database. The Find Sponsor dialog box opens. When you enter a value in any of the fields, the list box displays the sponsor record(s) that match the entered value(s). If no value was entered, all cardholders in the database will be displayed.



Select the sponsor's name and click **OK**.

Badge Box

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 44).

Note: *The Add Visitor application does not support FASC-N badge numbers.*

Auto – If your facility is set up to use the Auto-Badge Management feature (see page 249), click the **Auto** button to insert the next available badge number in the Number field.

Issue – Enter an issue level per badge number. If a visitor loses a badge, you would give 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 44.

Template – Select from the drop-down list the access template to be applied to this badge. See “Access Template” on page 243.

Design – Select from the drop-down list the badge design that was created using the Video Imaging application.

Start Date – Enter the date this badge becomes active. Click the down arrow to select a date from the system calendar.

Start Time – Enter the time this badge becomes active. Click the spin box buttons to select a time.

Void Date – Enter the date this badge will be automatically voided. Click the down arrow to select a date from the system calendar.

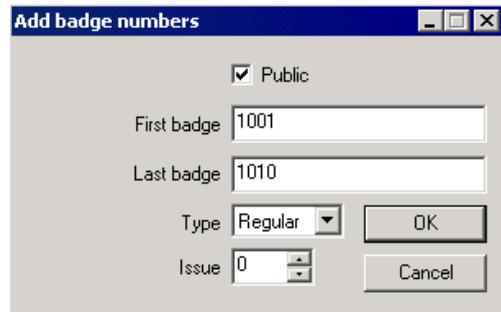
Void Time – Enter the time this badge will be automatically voided by the system. Click the spin box buttons to select a time.

Auto Badge Management

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 **Type** drop-down list, select whether this pool of numbers will be assigned to Regular or Visitor badges.
8. From the **Issue** drop-down list, select the issue level for a badge with this number.
9. Click **OK** to return to the AutoBadge Number Management dialog box. The list



AutoBadge Number Management						
Badge Number	Type	Issue	Status	Modification Date	Partition	Public
1001	Regular	0	In Use	4/28/2004 11:27:53 AM	Super User	Yes
1002	Regular	0	In Use	4/28/2004 11:28:04 AM	Super User	Yes
1003	Regular	0	In Use	4/28/2004 11:28:15 AM	Super User	Yes
1004	Regular	0	Available	4/28/2004 11:26:55 AM	Super User	Yes
1005	Regular	0	Available	4/28/2004 11:26:55 AM	Super User	Yes
1006	Regular	0	Available	4/28/2004 11:26:55 AM	Super User	Yes
1007	Regular	0	Available	4/28/2004 11:26:55 AM	Super User	Yes
1008	Regular	0	Available	4/28/2004 11:26:55 AM	Super User	Yes
1009	Regular	0	Available	4/28/2004 11:26:55 AM	Super User	Yes
1010	Regular	0	Available	4/28/2004 11:26:55 AM	Super User	Yes
1011	Visitor	0	In Use	4/28/2004 11:28:27 AM	Super User	Yes
1012	Visitor	0	Available	4/28/2004 11:27:13 AM	Super User	Yes
1013	Visitor	0	Available	4/28/2004 11:27:13 AM	Super User	Yes
1014	Visitor	0	Available	4/28/2004 11:27:13 AM	Super User	Yes
1015	Visitor	0	Available	4/28/2004 11:27:13 AM	Super User	Yes
1016	Regular	0	Available	4/28/2004 11:27:24 AM	Super User	Yes
1017	Regular	0	Available	4/28/2004 11:27:24 AM	Super User	Yes
1018	Regular	0	Available	4/28/2004 11:27:24 AM	Super User	Yes
1019	Regular	0	Available	4/28/2004 11:27:24 AM	Super User	Yes
1020	Regular	0	Available	4/28/2004 11:27:24 AM	Super User	Yes
1021	Regular	0	Available	4/28/2004 11:27:24 AM	Super User	Yes
1022	Regular	0	Available	4/28/2004 11:27:24 AM	Super User	Yes

Buttons at the bottom include Set Available, Set In-use, Advanced, Add Numbers, Delete Selected, and Done.

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.

10. To change the status of a badge number from *Available* to *In Use*, click the **Set In-use** button.
11. 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).

12. To delete badge numbers from the pool, select the numbers and click the **Delete Selected** button.
13. Click **Done** to close AutoBadge Number Management.

Badge Resync

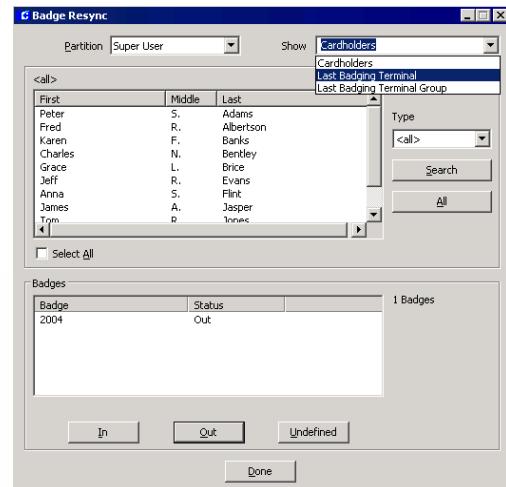
Entry and Exit terminals require cardholders to enter and exit an area in sequence. That is, when cardholders badge *in* at an entry terminal, they must badge *out* at the next badging. If, for example, they follow another cardholder

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 adjust the state of a badge to return it to the correct state. You can also reconfigure this badge 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.

To Resync Badges:

1. From the P2000 Main menu, select **Access>Badge Resync**. The Badge Resync dialog box opens.



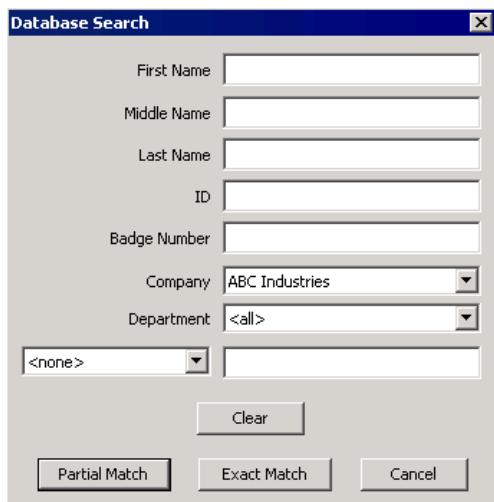
2. If this is a partitioned system, select the **Partition** in which the badges are active.
3. From the **Show** drop-down list, select one of the following options:
 - Cardholders** – to resync the status of badges that belong to all or specific cardholders.

Last Badging Terminal – to resync the status of all badges last presented at the selected terminal.

Last Badging Terminal Group – to resync the status of all badges last presented at all terminals in the selected terminal group.

Note: The **Last Badging Terminal** and **Last Badging Terminal Group** options are used for example, to quickly reset the status of all badges after a mustering event or reset the status of badges in situations when cardholders badged in at an entry terminal and they were not able to badge out at an exit terminal because the exit terminal was down.

4. If you selected **Last Badging Terminal** or **Last Badging Terminal Group**, select a terminal or terminal group from the list and continue with step 16.
5. If you selected **Cardholders**, select from the **Type** drop-down list the cardholder type (Regular, Visitor, or <all>) that you wish to display in the list box.
6. If you wish to display specific cardholders (within the type selected), click the **Search** button. The Database Search dialog box opens.



7. Enter the information on any or all of the fields to search for specific cardholders.
8. If you wish to search by **Company** and/or **Department**, select a previously defined name from the drop-down list.
9. You can also search by UDF. Select any of the previously defined UDFs (Date type UDFs cannot be included in the search) from the drop-down list. Then enter the UDF search criteria in the associated field.
10. If you wish to clear the existing search criteria, click the **Clear** button.

11. After you define the search criteria, click one of the following buttons:

Exact Match – to display an exact match to your search criteria.

Partial Match – to display all possible selections that match the initial characters of the search criteria, for example if you enter *Carl* in the First Name field, the list box will display names such as Carla, Carlos, Carlton, etc.

12. The list box in the Badge Resync dialog box opens displaying the cardholders specified in the search criteria.
13. If you wish to display all cardholders again (within the type selected), click the **All** button.
14. After you define the cardholders you wish to display in the list box, select a cardholder name from the list.
15. The badge number and status of all badges assigned to this cardholder will display in the Badges list. Select the badge or badges to be resync.

Note: To resync the status of all badges of all cardholders currently in the list, enable the **Select All** check box.

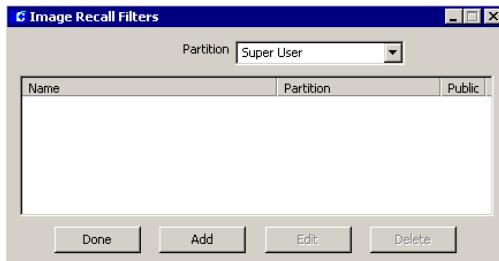
16. Click the appropriate button, **In**, **Out**, or **Undefined** to change the status of the badge(s).
17. Click **Done**. The badge status is now changed.

Image Recall

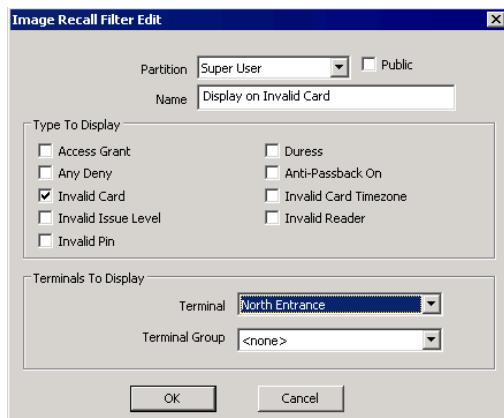
If the Image Recall window is open on the workstation, any badging (for the partition selected in Image Recall Filters) will display the cardholder's image and information. An operator with proper menu permissions can define access conditions and other filter criteria (transactions set up in the Image Recall Filter dialog box, such as an Access Grant or any invalid transaction), to determine if an image will display in the Image Recall window.

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.



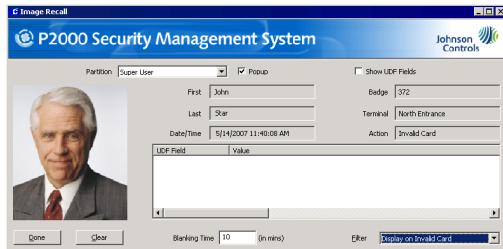
3. If this is a partitioned system, select the **Partition** in which this image recall filter will be active.
4. Select **Public** if you wish this image recall filter to be visible to all partitions.
5. Enter a descriptive **Name** for the image recall filter.
6. From the **Type to Display** box, select 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: Cardholder image and information will always display in the Image Recall window if the associated badge has the Trace option enabled, 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:

- From the P2000 Main menu, select **Access>Image Recall**. The Image Recall window opens.



- If this is a partitioned system, select the **Partition** in which the image recall will be active.
- 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.

- Select the **Show UDF Fields** check box, if you wish to display the user defined fields associated with the cardholder.
- In the **Blanking Time** field, enter the time in minutes after which the image and the data will be cleared. If you enter a value of zero the display will not be blanked.
- Select a **Filter** from the drop-down list.
- When a cardholder presents a badge at a terminal or group of terminals that meets the filtering conditions, the cardholder's image displays, along with the current cardholder information.
- This image and information will remain in the window until another cardholder

badges within the partition, or until the **Blanking Time** defined elapses, or until you click the **Clear** button to clear the information in the Image Recall window.

- Leave the Image Recall window open on the workstation to view images displayed as a result of subsequent badgings.

Image Recall FS (Full Screen)

The Image Recall FS feature offers a simplified display and works in both default and full screen modes.

When the Image Recall FS window is open and a cardholder presents a badge at a terminal or group of terminals that meets the filtering conditions, the cardholder's image displays along with the cardholder name. Optionally, one or two of the following can also display: Company, Department, ID, and any text or numeric user defined field (UDF).

To Activate Image Recall FS:

- From the P2000 Main menu, select **Access>Image Recall FS**. The Image Recall FS window opens.



- Select **Edit>Options** to open the Image Recall Options dialog box and define the elements you wish to display.



3. If this is a partitioned system, select the **Partition** in which the image recall will be active.
4. Select a **Filter** from the drop-down list that contains the access conditions that determine which images to display. See “Image Recall Filters” on page 252.
5. Select the **Popup** check box if the Image Recall FS 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.

6. From the **Line 2** drop-down list, select the data to be displayed in the second line under the cardholder’s image. You can select Company, Department, ID, Badge Expiration Date, Cardholder Expiration Date, or any text or numeric user defined field.
7. From the **Line 3** drop-down list, select the data to be displayed in the third line under the cardholder’s image. You can select

Company, Department, ID, Badge Expiration Date, Cardholder Expiration Date, or any text or numeric user defined field.

Note: The first line of text under the image always displays the cardholder’s name.

8. Click the **Text Font** browse button [...] to open the Font window and select the font type you wish to display. The font style and size are not configurable.
9. Click the **Text Color** browse button [...] to open the standard Color window and select the text color you wish to display.
10. Click the **Background Color** browse button [...] to open the standard Color window and select the background color you wish to display.
11. Click the **Background Image** browse button [...] to select a background image.
12. In the **Blanking Time** field, enter the time in minutes after which the image and the data are erased and the background is displayed. If you enter a value of zero the display will not be blanked.
13. Click **OK** to save your options and return to the Image Recall FS window.
14. Select **View>Full Screen** to change the display mode to “full screen.” Click <**Esc**> to return to previous view.
15. The image and information will remain in the window until another cardholder badges within the partition, or until the **Blanking Time** defined in Image Recall Options elapses, or until you select **View>Clear** to clear the information.
16. Leave the Image Recall FS window open on the workstation to view images displayed as a result of badgings, or select **File>Exit** to close.

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 opens 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 input points, must NOT have the **Disable Alarm** option selected to have the alarm displayed in the Alarm Monitor window, see page 98.

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 hierarchical 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.

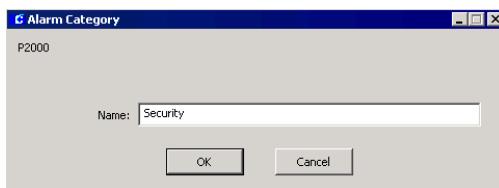
You can for example, define an input point to generate upon activation, two separate alarms for two configured alarm categories: P2000\Maintenance\Building 1 and P2000\Security\Building 1. Typically, a single operator is configured to receive only a single category of alarms, and therefore would only 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 feature, a single set of categories is shared by all P2000 sites within an Enterprise system.

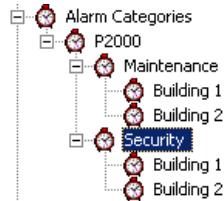
To Create Alarm Categories:

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 Info Tab” on page 26. 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 260). 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 260.)

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 261.) 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 261.)

Refreshing the Alarm Monitor window – The Refresh button on the Alarm Monitor window is used to read again all current alarms from the database (this should not be needed unless there was a loss of communication with the Server).

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. See “Starting and Stopping Service Control” on page 435.

- The **Message Filter Configuration** application (page 209), 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 216), 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 **Process Received Remote Messages** option in the RMS tab of Site Parameters (page 50), 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 50), 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 50), 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 50), 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

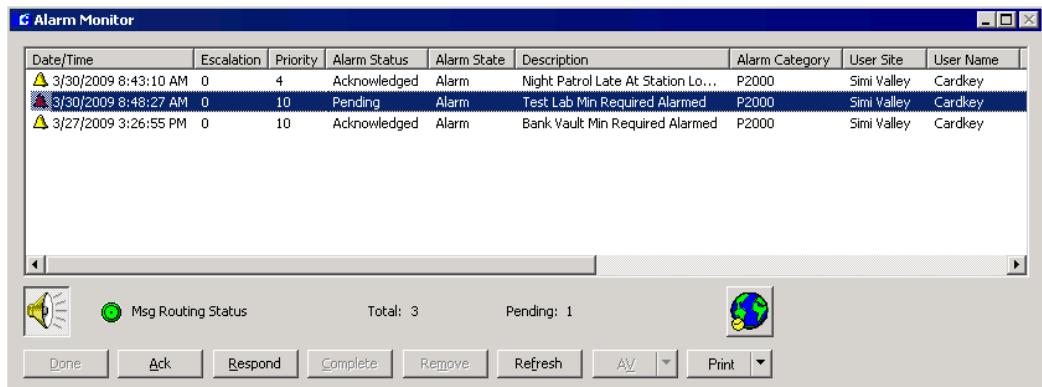
Date/Time – Displays the date and time the alarm was reported to the system. Alarms that are originated at remote sites with different geographical time zones will display the actual time at the remote site.

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”).

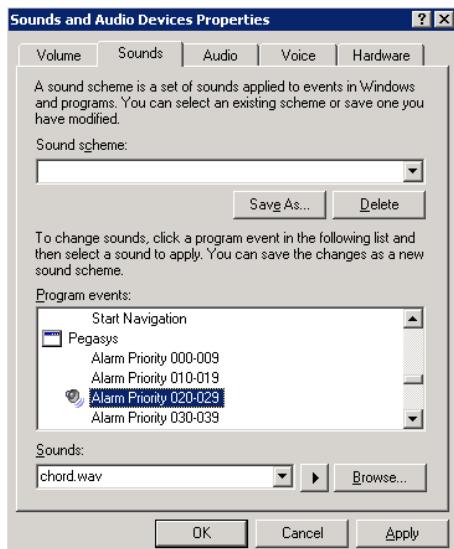
Priority – Displays the Alarm Priority set for each alarm type (the highest is “0”).

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. If you wish 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 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.

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 326. This feature is available for local alarms only.

AV – This button is enabled if your facility uses the DVR feature. If the alarm message displayed is associated with a camera, you can select the message line from the list and click the AV arrow, then select whether you want to display live or stored video. For more information, refer to your DVR documentation.

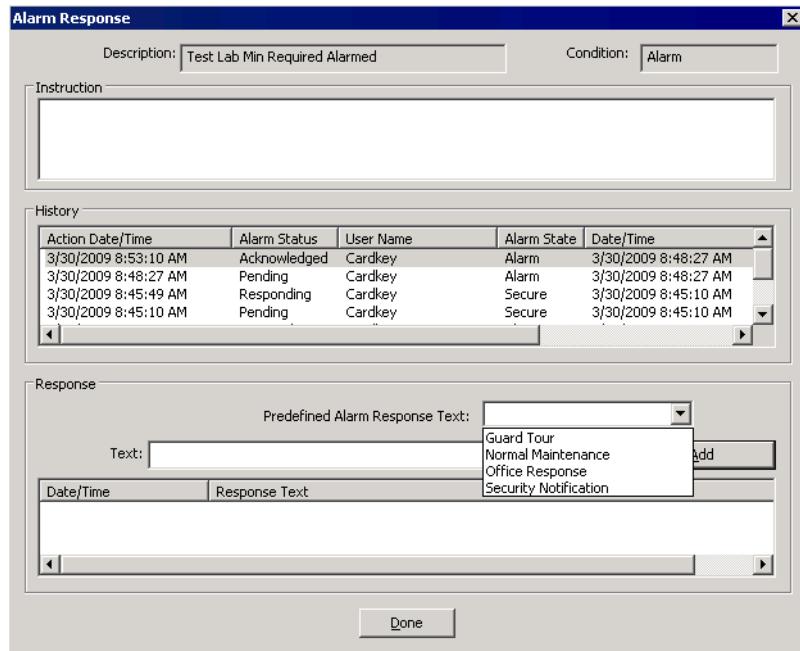
Print – Click the Print arrow and select whether you want to **Print All** alarms in the queue or select **Print Displayed** to print the alarms that are visible in the Alarm Monitor list box.

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.
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.



- 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. See “Creating Predefined Alarm Response Text” on page 263 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:

- 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.

- Select a line item from the scrolling list.

- 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 generates the alarm was configured to allow operators to manually activate events, the event name will also display in the shortcut menu. Also, the shortcut menu allows you to print All alarms in the queue or only the alarms that **Displayed** in the list box.

To Activate an Event from the Alarm Monitor:

- In the Alarm Monitor window, select the line item you are responding to and right-click to open the shortcut menu.
- Click the event name you wish to activate. The event will be triggered.

Configuring Alarm Colors

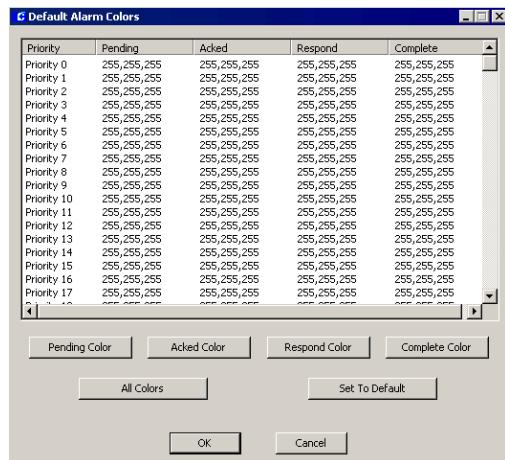
The P2000 system provides color configuration capability for each alarm priority (0 to 255) and its corresponding alarm status. Each alarm status can have a unique color assigned to help operators recognize specific alarms. When a new alarm displays in the Alarm Monitor window, the line for the affected alarm will display in the color that was assigned using the Default Alarm Colors dialog box.

To Define Color-Coded Alarms:

- From the P2000 Main menu, select **Config>System**. Enter your password if

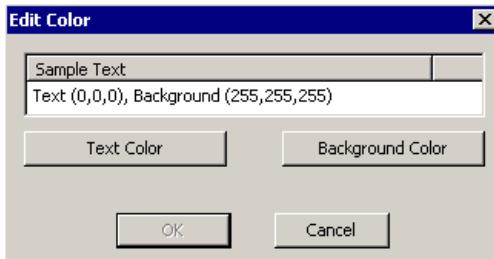
prompted. The System Configuration window opens.

- Click the plus (+) sign next to the root **Site Parameters** icon to display default system parameters.
- Click the **Default Alarm Colors** icon and click **Edit**. The Default Alarm Colors dialog box opens.



- Click the **Priority** line you wish to define.
- 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.

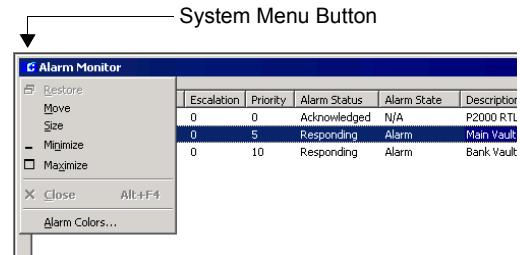


6. Click the **Text Color** button and select the desired text color from the color palette. Click **OK**.
7. Click the **Background Color** button and select the desired background color from the color palette. Click **OK**.
8. The Sample Text box will display the selected colors. Click **OK** to return 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. If you wish 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 menu permissions. Therefore, if you do not want operators to override the default alarm colors, remove the "Alarm Colors" permission from their Menu Permission Group.

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.

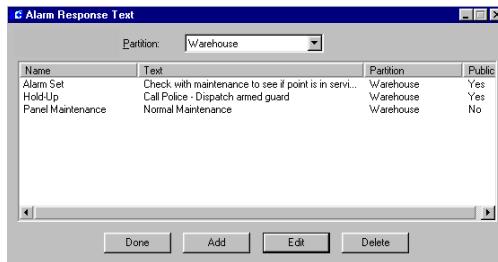
Note: Alarm colors that are assigned from the Alarm Monitor window are associated with the operator who made the changes. In addition, the **Set To Default** button will reset to the default colors assigned from the System Configuration window.

Creating Predefined Alarm Response Text

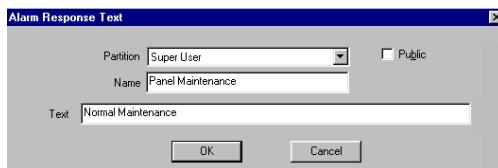
You can create Response text to speed alarm response to specific types of alarms. For example, when panels go down for regular maintenance, a "Panel Down" soft alarm is sent to the Alarm Queue. The operator can quickly respond by selecting a predefined response from the drop-down list.

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.

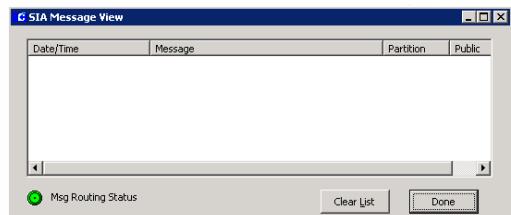


- If this is a partitioned system, select the **Partition** to which the SIA device will have access.
- Select the **Public** check box to make this SIA device visible to all partitions.
- Enter the **Name** that identifies the SIA device.
- Select the **Enable** check box to enable the SIA device.

- 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** to which the SIA device is physically connected. 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.

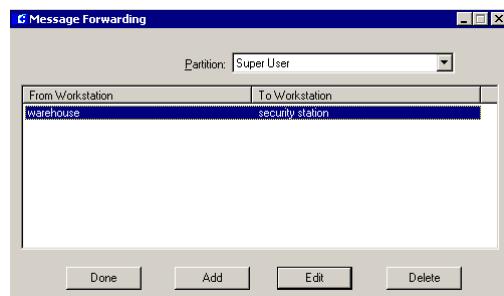
Message Forwarding

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 207.

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**.

Fire Alarm Control

The P2000 fire alarm control application has been designed to operate with Notifier® fire alarm panels using Johnson Controls Fire OPC Server. This integration allows the P2000 system to control alarms generated by fire devices connected to the Notifier panel. The fire system consists of sensors, connected to the Notifier fire panel, capable of detecting fire events. These detectors are grouped into zones that use audible signals (input/output modules) to indicate that a zone is in alarm condition. Use the instructions provided in the *Notifier AMx000 unit OPC Server Application* to define your fire system, such as fire detectors, input/output modules, and how these input and output devices will be associated with fire zones.

IMPORTANT: The Notifier panel is not available in North America. Contact Johnson Controls Systems Integration Services Europe for information.

The Notifier fire system benefits from P2000 powerful alarm capability, which provides tools that define how these alarms respond when activated, whether or not they trigger output relays, and at which times an alarm can be activated.

An authorized operator at a P2000 workstation can enable or disable a fire detector alarm or fire zone alarm, and activate or deactivate a fire signal. When properly configured, the P2000 system should:

- receive notification from the fire panel that a fire has been detected in the building
- identify the location of the fire
- inform building personnel that a fire has been detected
- warn the occupants of the building that a fire has been detected to ensure that all are able to exit the building before escape routes become impassable.

Basic Definitions

Activated – The state of a device connected to a fire input/output module, such as evacuation signals or a sprinkler system. The output of an input/output module can be activated manually or by system events.

Deactivated – The state of a device connected to a fire input/output module after the fire alarm is reset. The output of an input/output module can be deactivated manually or by system events.

Detector – Device connected to the fire panel and that reports physical changes associated with fire such as a heat detector, a smoke detector, or a carbon monoxide detector.

Disabled – The state of a fire detector, zone or input/output module that is disabled from reporting fire alarms. This state is typically used with devices that report false alarms or can be used to turn off fire devices after an alarm condition. Fire devices can be disabled manually or by system events.

Enabled – The state of a fire detector, zone or input/output module that is enabled for reporting fire alarms. Fire devices can be enabled manually or by system events.

Fire Panel – Device that is the controlling component of a fire alarm system. The panel receives information from sensors designed to detect changes associated with fire (detectors), monitors the operation of these detectors, and activates equipment (input/output modules) designed to alert building personnel of potential danger.

Input/Output Modules – Device connected to a fire panel that can detect input from switched devices, such as sprinkler systems; and activate notification signals, such as alarm bells or telephone dialers. Traditionally, when an input device is activated, a certain output device (or relay) is also activated.

Zone – An area in a facility that is associated with fire detectors and input/output modules.

Basic Fire Alarm Components

This section describes the basic components of a fire alarm control system. The fire alarm control system consists of the P2000 software, the panel (Notifier) firmware, and the panel components (fire detector, zone, and input/output modules).

The P2000 software is used to:

- Create and assign menu permissions to perform fire alarm control functions, see page 23.
- Provide the communication between P2000 applications and the Fire OPC Server using the P2000 OPC Proxy Service, see page 432.
- Enable the fire server, see page 268.

- Configure alarm options for fire alarm panels, detectors, zones, and input/output modules, see page 269.
- Control, monitor, and display the status of fire detectors, zones, and input/output modules, see page 270.
- Define event triggers and actions associated with fire detectors, zones, and input/output modules, see page 272.

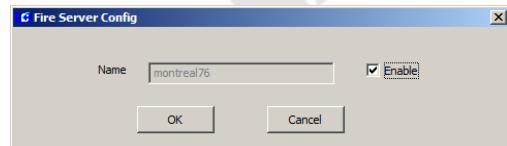
The following sections describe fire alarm configuration and control procedures using the P2000 software.

Fire Alarm Server Configuration

Once you configure your fire panel and associated items using the instructions provided with your Notifier unit, you must enable the fire server in the P2000 System Configuration window to populate the associated data into the P2000 database.

To Enable the Fire Server:

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 **Fire Server**. The name of the fire server will display.
3. Select the fire server name and click **Edit**. The Fire Server Config dialog box opens.



4. Verify that the fire server name displays in the **Name** field.

5. Select the **Enable** check box.
6. Click **OK**.

Once you enable the fire server, the System Configuration window is automatically populated with the fire panel and associated fire zones, detectors, and input/output modules.



The P2000 system is now ready to operate with the Notifier fire panel.

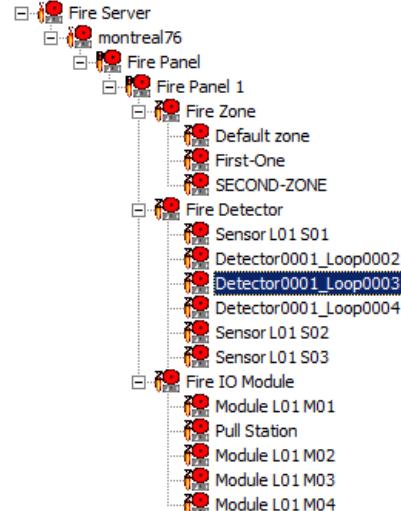
Fire Alarm Configuration

Every alarm that is generated in the P2000 system, must belong to at least one Alarm Category (see “Alarm Configuration” on page 255 for details), but can also be assigned to multiple alarm categories, each with its own set of alarm options. For example, if a fire input/output module connected to a push-button switch generates an alarm, you can define this push-button switch to generate upon activation two separate alarms for two configured alarms categories, for example one for *P2000\Maintenance\Building 1* and one for *P2000\Fire\Building 1*. The *P2000\Fire* alarm can be configured with a higher priority, enabled escalation settings, and to be monitored by security personnel. The *P2000\Maintenance* alarm can be configured with a lower priority, no escalation settings, and to be monitored by maintenance personnel.

Use the following instructions to assign fire related alarms to one or more Alarm Categories.

To Configure Fire Alarms:

1. In the System Configuration window, click the plus (+) sign next to the root **Fire Server** to display all the fire panel components.
2. Select a Fire Panel or component (Zone, Detector, or IO Module). Click **Edit**.



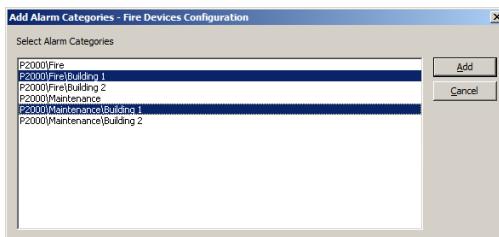
3. The Fire Devices Configuration dialog box opens for the selected item.



4. If you are configuring alarm options for a Fire Panel, select from the **Partition** drop-down list, the appropriate Partition that will have access to the Fire Panel. Par-

tition selection is only available at the Fire Panel level.

5. Select the **Public** check box if you wish the fire device to be visible to all partitions.
6. Specify the **Query String** value to be used with message filtering and with the P2000-Metasys integration feature.
7. Click the **Add** button to assign this alarm to one or more Alarm Categories. The Add Alarm Categories dialog box opens displaying all previously created alarm categories (see page 255 for details).



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

8. Select one or more categories and click the **Add** button. The list will display all the selected alarm categories.
9. If you wish to remove a category from the list, select the alarm category and click **Delete**.
10. 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. See the definitions provided on page 97.

Fire Alarm Management

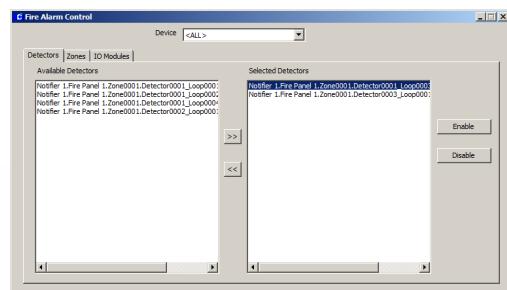
Management of fire alarms includes displaying the current state of fire alarm items as well as issuing commands for such activities (disable, enable, activate, etc.). The following sections describe how to monitor and control fire alarm components.

Controlling Fire Alarm Components

Use the Fire Alarm Control window to perform alarm commands for fire detectors, zones, and input/output modules. It allows operators to enable or disable alarms for these fire components. In addition, operators can also activate or deactivate the output of an input/output module from this window.

To Control Fire Alarm Components:

1. From the P2000 Main menu select **Control>Fire**. The Fire Alarm Control dialog box opens.



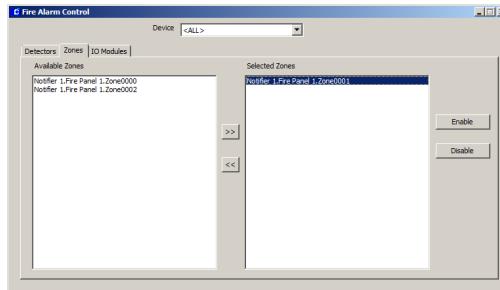
2. From the **Device** drop-down list, select the device (Notifier panel) name you wish to control.
3. If you wish to control a fire Detector, click the **Detectors** tab. From the list of Available Detectors at the left side of the window, select the fire detector you wish to control.

- Click the >> button to move the selected fire detector to the **Selected Detectors** box. You can add as many Detectors as you wish. Once you have the selected Detectors, click the function button on the right side of the window to perform the associated operation. The choices are:

Enable – Enables the selected fire detector(s).

Disable – Disables the selected fire detector(s).

- If you wish to control a fire Zone, click the **Zones** tab. From the list of **Available Zones** at the left side of the window, select the fire zone you wish to control.

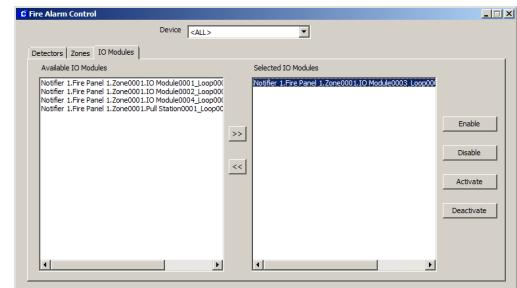


- Click the >> button to move the selected fire zone to the **Selected Zones** box. You can add as many Zones as you wish. Once you have the selected Zones, click the function button on the right side of the window to perform the associated operation. The choices are:

Enable – Enables the selected fire zone(s).

Disable – Disables the selected fire zone(s).

- If you wish to control a fire input/output module, click the **IO Modules** tab. From the list of Available IO Modules at the left side of the window, select the fire input/output module you wish to control.



- Click the >> button to move the selected fire input/output module to the **Selected IO Modules** box. You can add as many IO Modules as you wish. Once you have the selected IO Modules, click the function button on the right side of the window to perform the associated operation. The choices are:

Enable – Enables the selected input/output module(s).

Disable – Disables the selected input/output module(s).

Activate – Activates the selected output of an input/output module(s).

Deactivate – Deactivates the selected output of an input/output module(s).

- When you finish controlling the fire items, close the Fire Alarm Control dialog box.

Viewing Fire Transactions Using the Real Time List

All fire transactions are sent through real time messages to the Real Time List. As the status of defined fire detectors, zones, and input/output modules changes, corresponding related messages are generated and displayed. You must select the **Fire** check box in the Real Time List window to display all fire transactions as they occur. See “Using the Real Time List” on page 322 for more information.

Note: If you wish to print fire transactions as they occur, you can either print them from the Real Time List window, or select the **Fire** check box in the Site Parameters dialog box, Printing tab, see page 41.

Monitoring Fire Components Using the Real Time Map

The Real Time Map displays the status of fire panels, detectors, zones, and input/output modules on a map layout of your facility. Upon fire alarm activity, the map will show the state change and the exact location of the activity. See “Using the Real Time Map” on page 326.

When a status changes, the associated fire icon starts flashing. You can right-click the icon to open a shortcut menu and choose to, for example, enable or disable a fire panel or activate a fire input/output module. If the fire icon was configured to allow the operator to activate events, the event name will also display in the shortcut menu.

To add fire icons to the Real Time Map, follow the instructions provided in “Creating a Real Time Map” on page 328.

Map Maker provides a default fire component image set to display various fire states. However, you can use your own icons to create cus-

tom image sets. See “Adding Image Sets” on page 332 for details.

Viewing and Controlling Fire Components Using the System Status Window

The System Status window displays the current status of fire zones, detectors, and input/output modules that have been configured for fire alarm control. It also allows you to issue commands for the fire zones, detectors, and input/output modules displayed.

See “System Status” on page 439 for instructions on how to display fire components status and/or issue commands.

Fire Component Events

The fire alarm system connected to the P2000 system can trigger events and respond to event actions using the P2000 Event application. For specific instructions, see “Creating Events” on page 314. Typical fire commands to be included and linked to specific actions are as follows:

- An alarmed fire zone (trigger) forces a door to be locked to control the spread of smoke fumes and fire (action).
- An access grant command (trigger) activates the output of a fire input/output module, such as an emergency notification signal (action).
- A fire panel that enters the trouble state (trigger) sets the badge security level at a specified value (action).

For a complete list of event triggers and actions associated with fire panels, detectors, zones, and input/output modules, see *Appendix A: Event Triggers/Actions*.

Operator Controls

Most system functions operate automatically; however, some functions may be operated manually from a workstation. Operators with the appropriate permissions 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. Operator controls are panel specific. See *Appendix C: Panel Comparison Matrix* for a detailed list of features and capabilities supported by your panel type.

Note: When you manually control doors or output devices associated with serial panels, there might be an operation delay of 5 to 10 seconds if data is being currently downloaded to the panel.

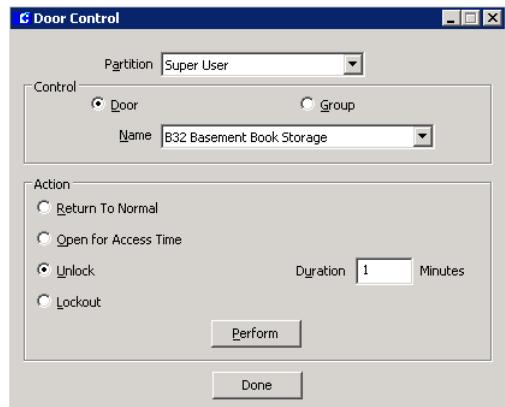
Controlling Doors

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 first have menu permissions for Door Control 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.

Note: Isonas panels do not report transactions associated with manual door control changes.

To Manually Control Doors:

- From the P2000 Main menu select **Control>Door Control**.
- Enter your password if prompted. The Door Control dialog box opens.



- If this is a partitioned system, select the **Partition** in which this door is active.
- In the Control box, select either **Door** or **Group** to populate the Name drop-down list with selections.
- Select a **Name** from the drop-down list.
- In the Action box, select one the following:

Return to Normal – to return the door to its normal state.

Open for Access Time – to unlock the door for the amount of time set in the Access Time field defined in the Terminal dialog box.

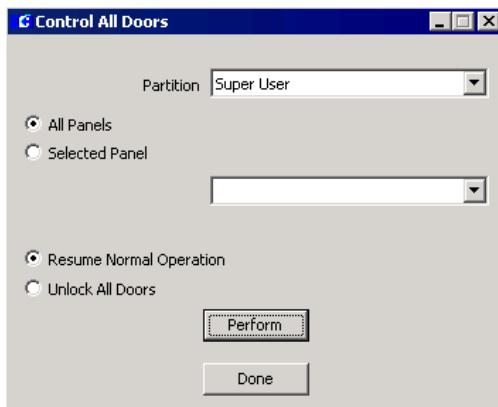
Unlock – to unlock the door for the number of minutes entered (up to 1440 minutes) in the **Duration** field, after which the doors will revert back to their original system-controlled condition.

Lockout – to prevent access by all badges at the door. Only supported by OSI and Assa Abloy panels.

- Click **Perform**. The Action selection goes into effect.
- 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 **All Panels** radio button if you wish to control all doors in the system, or select **Selected Panel** and select a panel from the drop-down list to control all doors connected to the selected panel.
5. Select the **Unlock All Doors** option if you wish to unlock all doors.
6. Click **Perform**. The system will inform you that the doors will remain unlocked until you lock the doors again, and prompt you to continue.
7. Click **Yes**. This will override the system control until you reverse the command.
8. To return the doors to their previous state, select the **Resume Normal Operation** option.
9. Click **Perform**. The system will prompt for verification.
10. Click **Yes**. The Door Control override is reversed.

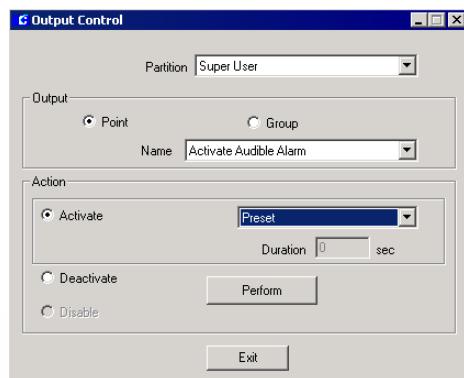
Controlling Outputs

An operator can manually control an output (override system controls) for a specific output point or group. (The operator must first have menu permissions for Output Control 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.

Note: Isonas and HID panels do not report transactions associated with output point status changes.

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 (the actions available in the list depend on the panel type):

- **Preset** – to turn the output point to a pre-defined state.
- **Set On** – to turn on the output point.
- **Slow Flash** – to toggle the output point on and off slowly.
- **Fast Flash** – to toggle the output point on and off quickly.
- **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.

Note: If you manually turn a P900 output point for a timed duration, you must click the **Refresh** button in the System Status window to update the P900 output point status information after the timed duration has expired.

6. Click **Perform** to manually activate the output point.
7. If you wish to return the output point to a Normal state, click **Deactivate**, then click **Perform**.
8. If you wish to temporary disable a P900 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.

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.

Note: For D6xx series panels, the **Latch Output** option must be enabled on the **Alarm** tab of the **Edit Panel** dialog box to manually control a panel relay.

P900 CLIC Controls

The P2000 system also provides manual control of P900 counters, flags, and trigger events. An operator with menu permissions for P900 Control can set counters to any value, set or clear flags, or force a trigger event to perform its actions. If this is a partitioned system, the options available from the drop-down lists will be only those active in the operator's partition. See "Configuring CLIC Components" on page 120.

To Manually Control a P900 Counter:

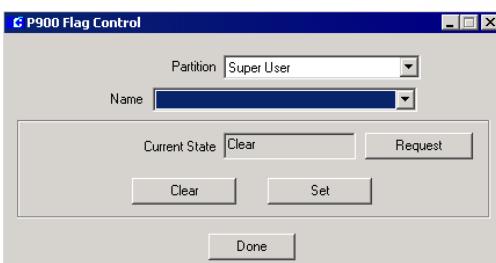
1. From the P2000 Main menu, select **Control>P900 CLIC>Counter**.
2. Enter your password if prompted. The P900 Counter Control dialog box opens.



3. If this is a partitioned system, select the **Partition** in which this P900 Counter is active.
4. Select a counter **Name** from the drop-down list. The dialog box displays the **Current Value** of the selected P900 Counter.
5. If you wish to update the Current Value, click the **Request** button.
6. To force the counter to a different value, click the **Force Value** spin box and select a new number.
7. Click the **Action** button to force the new counter value.
8. Click **Done** to close the dialog box.

To Manually Control a P900 Flag:

1. From the P2000 Main menu, select **Control>P900 CLIC>Flag**.
2. Enter your password if prompted. The P900 Flag Control dialog box opens.



3. If this is a partitioned system, select the **Partition** in which this P900 Flag is active.
4. Select a flag **Name** from the drop-down list. The dialog box displays the **Current State** of the selected P900 Flag.
5. If you wish to update the Current State, click the **Request** button.
6. Click **Set** if you wish to force the flag to be set. The flag still acts as normal afterwards.
7. Click **Clear** if you wish to force the flag to be clear. The flag still acts as normal afterwards.
8. Click **Done** to close the dialog box.

To Manually Control a P900 Trigger Event:

1. From the P2000 Main menu, select **Control>P900 CLIC>Trigger Event**.
2. Enter your password if prompted. The P900 Event Control dialog box opens.



3. If this is a partitioned system, select the **Partition** in which this P900 Trigger Event is active.
4. Select a trigger event **Name** from the drop-down list.
5. Click **Enable** to have the P900 panel process the trigger event.
6. Click **Disable** if you do not wish to have the P900 panel process the trigger event.

7. Click **Force** to immediately perform the trigger event action.
8. Click **Done** to close 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 cardholders at any reader terminal connected to a panel that supports security threat level control. 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 badges (see page 241). 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.

To obtain access at a terminal connected to a D600 AP panel, the terminal security level must be equal to or higher than the panel security level, but never higher than the security level set up at the badge. To raise the security level at a D600 AP panel, see page 70.

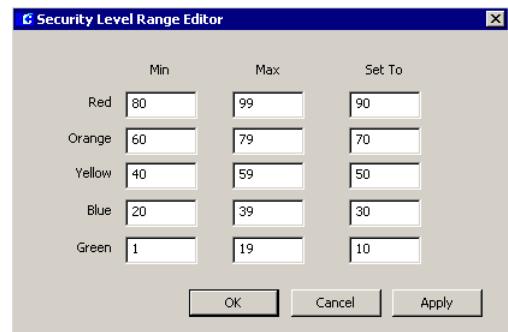
Defining Security Levels

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 ter-

minals using the Security Level Control dialog box.

To Define Security Levels:

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 **Panels** icon to display panel components.
3. Select the **Security Level** icon and click **Edit**. The Security Level Range Editor dialog box opens.



4. 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.
5. Once the security level color codes have been defined with acceptable ranges, click **Apply** to save the values while leaving the dialog box opened.
6. Click **OK** if you wish to close the Security Level Range Editor dialog box.

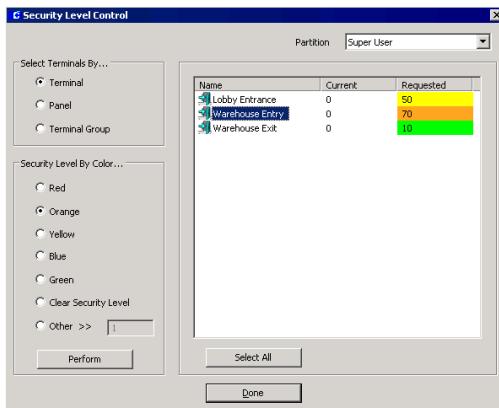
Applying Security Level

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 at

once access to all terminals connected to the selected panels.

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.

- 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.
- 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 **Requested** column the default value for that colored security level. The **Current** 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, all time zone based overrides, host initiated overrides, and cardholder overrides will be immediately disabled. For more information, see “Override Reset Threat Level Box” on page 82 and page 147.

- If you wish 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.
- 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 Requested and Current columns will display 0.

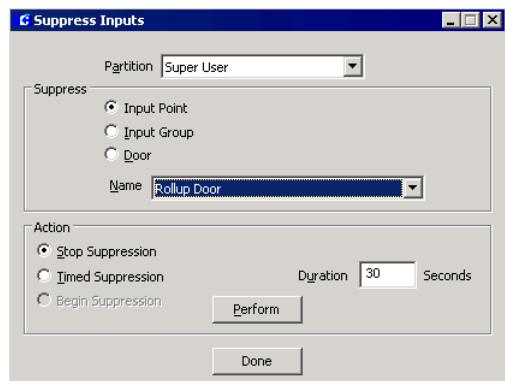
8. Click **Done** to close the Security Level Control dialog box.

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/propped door soft alarm inputs, as well as hardware input points. See *Appendix C: Panel Comparison Matrix* to verify if your panel type supports this feature. The operator must have Suppress Inputs menu permissions 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 all input points in the selected group.

Door – to suppress forced/propped soft alarm input points associated with the selected door. This feature works if the Forced Door/Propped Door soft alarm is enabled.

5. Select an input point, input group, or door **Name** from the drop-down list.
6. In the Action box, select one the following (only the actions available for your panel type will be enabled):

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). A value of zero will keep this input point sup-

pressed until commanded to stop suppression.

Begin Suppression – to suppress an S321-IP input point. The S321-IP input point will remain suppressed until you click the **Stop Suppression** option.

7. Click **Perform**. The Action selection goes into effect.
8. Click **Done** to exit the 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 cardholders 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 cardholders. Areas do not have any access control or transaction processing functions; they are set up for reporting pur-

poses 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 cardholders or vehicles. Here you name and describe the specific Area, define the maximum and minimum cardholders 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 cardholder count on a specific Area, for example a “Main Vault.”
 - Facility** – Select Facility to monitor cardholder count on the entire facility, for example “Bank ABC.”
 - Parking** – Select to monitor cardholder count in a parking structure, for example “Parking One.”

Note: It is possible for a cardholder to be counted on all three Area types at the same time, for example when the cardholder 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:

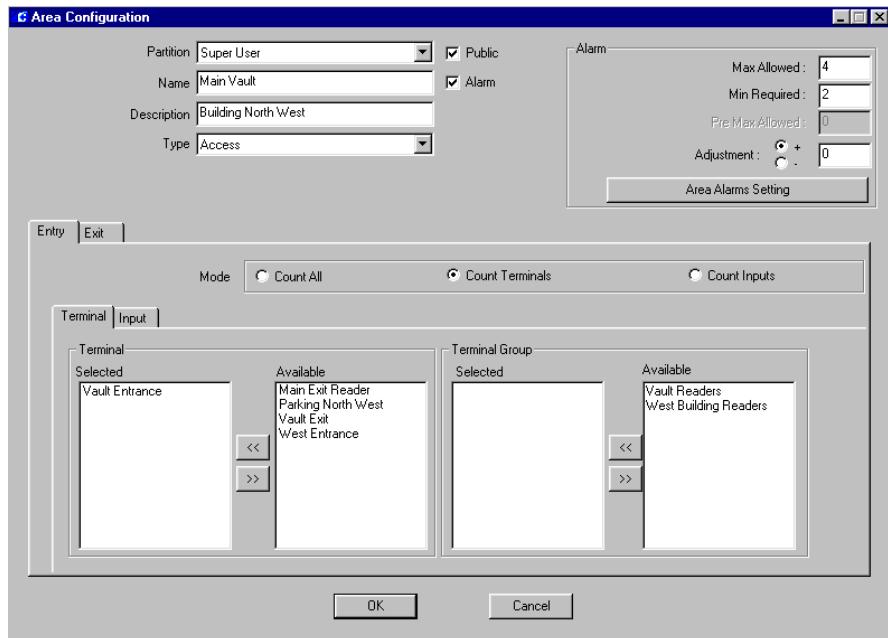
Max Allowed – An alarm is generated when the maximum number of cardholders entered in this field has been exceeded. The status column in the Area Control dialog box will display *Max Allowed Alarmed*.

Min Required – An alarm is generated when the minimum number of cardholders 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 cardholders 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 cardholders that the lot is full.

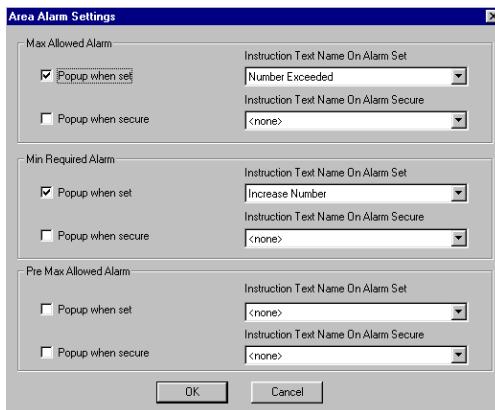
Note: In the **Adjustment** field, select the "+" or "-" sign, and enter a number to adjust any of the above counts by this number. For example if the Max Allowed is 100 and you entered a +2 in this field, an alarm will not be generated if the Max Allowed count is 102.



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 104.

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 if you wish to count the number of cardholders that are granted access through both reader terminals and input points.
 - Count Terminals** – Select if you wish to count the number of cardholders that are granted access through reader terminals only.
 - Count Inputs** – Select if you wish to count the number of cardholders 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 if you wish 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 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.
4. If you wish 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”.

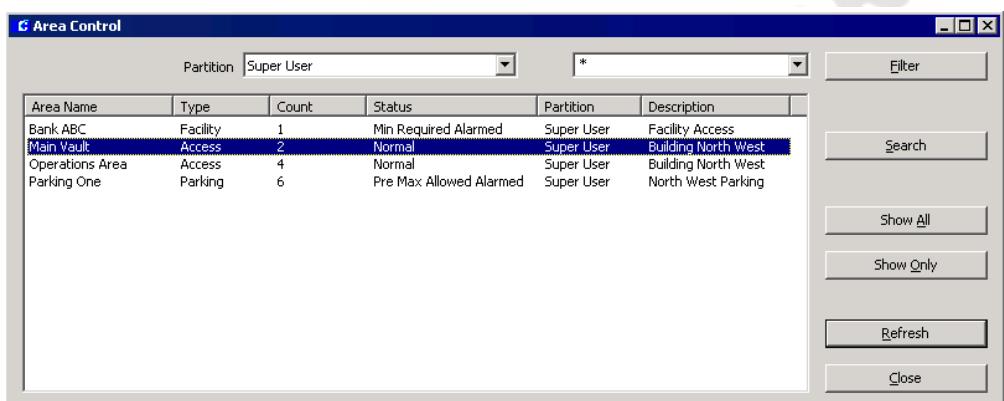
Note: You can also select a previously typed filter from the drop-down list. The list box will be refreshed when you select * from the Filter box or when you close the Area Control dialog box.

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 cardholders 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 cardholders had exceeded.
- **Min Required Alarmed** – An alarm was generated because the minimum number of cardholders 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 cardholders had been reached.

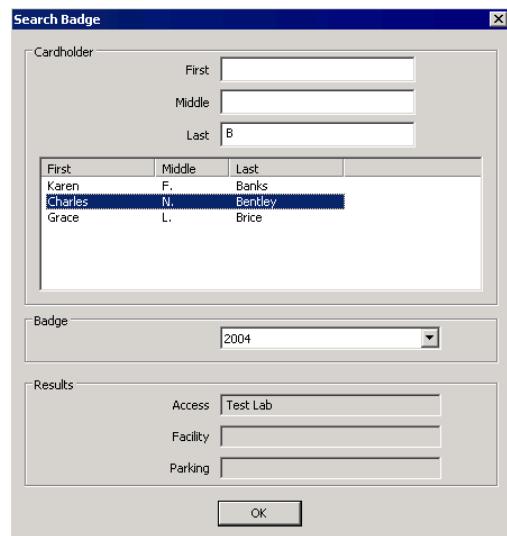
Partition – The Partition, as configured in the Area Configuration dialog box.

Description – The Description, as configured in the Area Configuration dialog box.

5. If you wish to change the current sort order, click the specific column header in the list box.
6. To display specific details of each Area, right-click the specific Area name, and select whether to **Show Only** the cardholders passing the filter criteria entered in the Area Filter dialog box (see the next section “Defining Area Filters”), or to **Show All** cardholders in the Area Details dialog box (see “Displaying Area Details” on page 285). 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.

7. To search the whereabouts of a specific cardholder, click the **Search** button. The Search Badge dialog box opens.

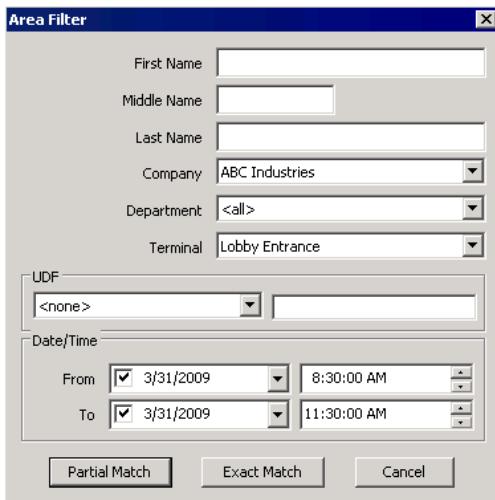


8. Enter a value in any of the Cardholder fields. The list box will display the cardholder record(s) that match the entered value(s).
9. Select a cardholder from the list box. If only one badge was assigned to this cardholder, that number will automatically display on the Badge field, and the respective Area Type field will display the Area name where the cardholder is located.
10. If the cardholder has more than one badge assigned, click the **Badge** drop-down list and select a badge number. The respective Area Type field will display the Area name where the cardholder can be found.
11. Click **OK** to close the Search Badge 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 cardholders that have been granted access to the specified Area. You can, however, define filter criteria to help you locate specific cardholders quickly and easily.

- 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.



- Enter the information on any or all of the fields to display specific cardholder count.
- If you wish to search all cardholders that belong to the same **Company** or **Department**, click the specific drop-down arrows and select any of the previously defined Companies or Departments.
- To search by location, select from the **Terminal** drop-down list the terminal name where cardholders last presented their badge.
- If you wish 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.

- If you wish to search by specific date and time, enter the information on the **Date/Time** box.
- After you define the search criteria, click one of the following buttons:
Exact Match – to display an exact match to your search criteria.
Partial Match – to display all possible selections that match the initial characters of the search criteria, for example if you enter *Carl* in the First Name field, the list box will display names such as Carla, Carlos, Carlton, etc.
- The Area Details dialog box opens, displaying all the cardholders 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 cardholder 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**, and enter the criteria in the Area Filter dialog box.

In either case, the Area Details dialog box opens, showing the Area Name and Area Type in the window title. See “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 284.

Current Count – Shows the total number of cardholders currently in the Area, which were granted access through either reader terminals or input points.

Terminal Count – Shows the total number of cardholders currently in the Area, which were granted access through a reader terminal.

Input Count – Shows the total number of cardholders currently in the Area, which were granted access through an input point.

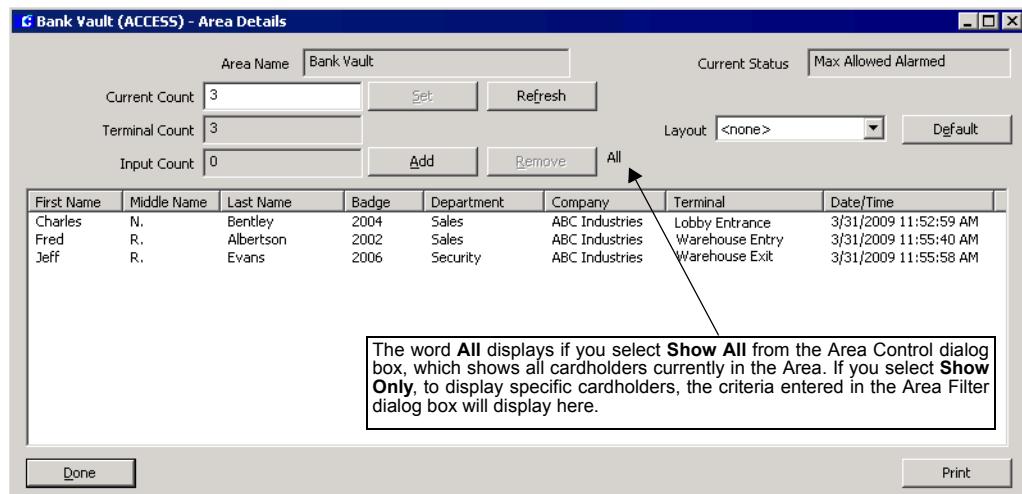
Set – This button is activated when the Current Count is manually changed, for example to add cardholders that you know are currently in the Area, but you do not know who they are. After entering the new count, click the **Set** button, then click **Yes** to confirm. The Input Count will increase or 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 cardholders showing in the list box, you will be asked to remove some cardholders 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 a cardholder is currently in the Area, but does not display in the Area Details list box, click the **Add** button and select the cardholder name and badge number, click **OK**, then click **Yes** to confirm. The cardholder 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 cardholders are selected in the list box. Click the **Remove** button if you wish to manually remove a selected cardholder, then click **Yes** to confirm. The Current Count and Terminal Count values will be updated.



Layout – This field relates to how the cardholder list displays in the list box. The drop-down list displays all Layout names that were previously defined in the Area Layout dialog box. (See “Area Layout” for more information, and the next section “Viewing the Details List” for instructions on changing the list box display.)

Default – Click the **Default** button to restore the eight default fields, see “Viewing the Details List”.

Done – Click **Done** to return to the Area Control dialog box.

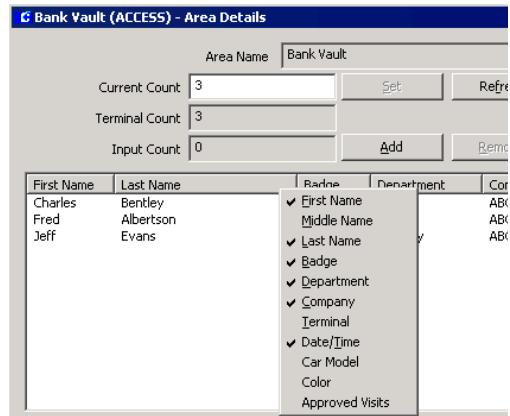
Print – Click **Print** to print the details list.

Viewing the Details List

The details list box displays all cardholders 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. If you wish 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 eight 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. If you wish 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

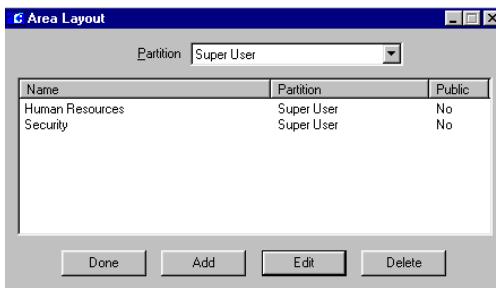
The Area Details dialog box displays a default view consisting of eight pre-stored fields. You can, however, create different layouts to dis-

play only certain information, according to your particular needs.

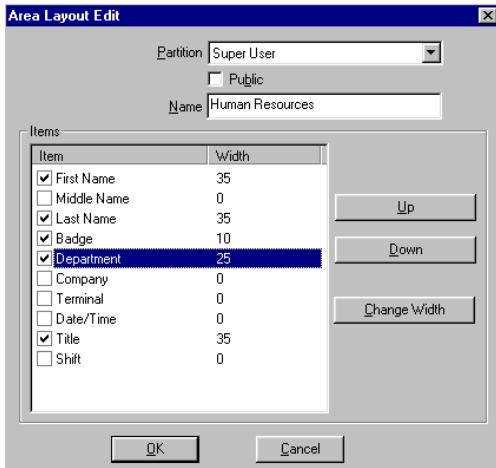
For example, a system administrator may want to monitor how many cardholders from a specific department are currently in the Area. In that case an Area Layout will be created to display only the fields selected on the Area Layout Edit dialog box.

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 eight 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 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.
- If you wish 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.

Area Reports

Five Area reports are provided as part of the standard P2000 reports:

All Areas to Cardholder - Preprocessed – Lists by cardholder name, all areas the cardholder can access and the terminal doors defined for the area.

All Cardholders to Area - Preprocessed – Lists by area name, the cardholders and badges that have access to the area.

Note: Preprocessed reports display current data. Any changes made to database items will not be reflected until the following day, unless you manually update the report table using the Update Preprocessed Reports table task in Database Maintenance, see page 449.

Area Configuration – Lists by area name, all configuration information entered in the Area Configuration dialog box.

Area Control – Lists the cardholders currently in the area, including the total number of cardholders for each count mode.

Area Transaction – Lists all transactions performed in the system for the specific area. You can select to run the report on transactions at your local site or you can enter the name of the remote site that you want to report on.

See *Chapter 6: System Reports* for detailed instructions on running P2000 Standard Reports.

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 badge 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 badge 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 badge reader terminals.

Zone Terminal – Zone terminals are badge 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 badge 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 badged 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 badge 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 badge 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 badge at a muster terminal so that their status can be upgraded according to the last used terminal.

Trapped – Personnel are considered trapped if they badge 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 badge 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 badged at a designated muster terminal since the start of a Muster.

Sequestered – Sequestered personnel are those who have badged at a designated “sequester terminal” since the start of the Muster.

Rescuer – Rescuers are personnel who badge 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 badge at a muster or sequester terminal.

Note: *Trapped, Wandering, and Rescuer groups are only tracked if Track Movement is selected in the Muster Terminals tab, see page 295.*

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.

- 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.

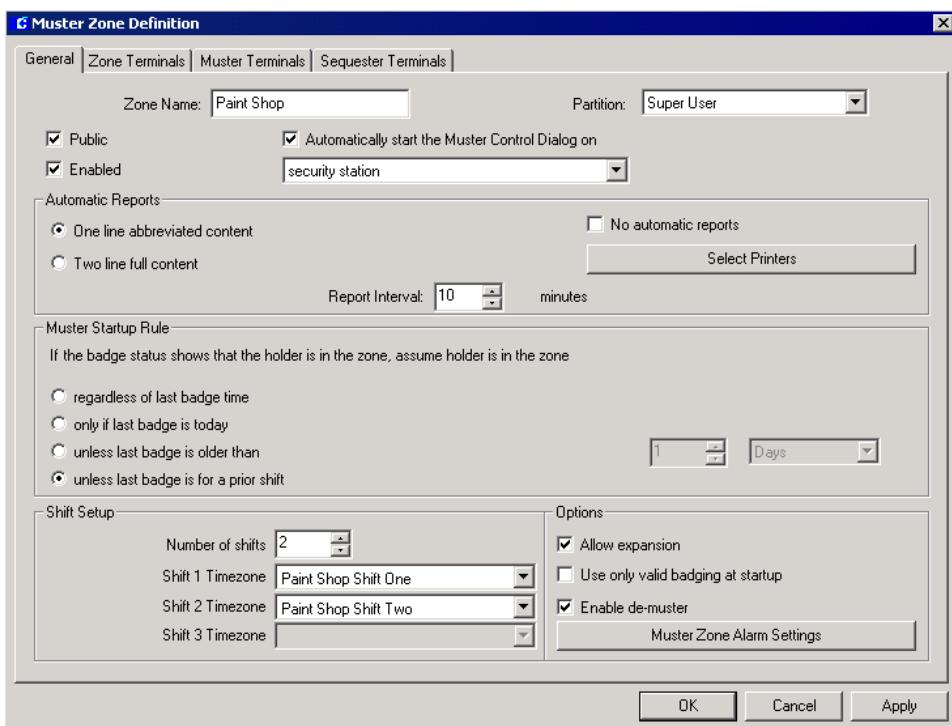
Partition – Select the partition in which this Zone Name will be active.

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. If you wish to temporarily disable the Zone, select the check box again to disable it.

Automatically start the Muster Control Dialog – Select this check box if you wish 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, badge number, and last badging date and time.

Two line full content – Select this option if you wish to automatically print more detailed cardholder information when a Muster begins. This report will be printed at the Report Interval selected and will include first and last name, badge number, last badging 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.

IMPORTANT: *Printing muster reports is not guaranteed on foreign language systems.*

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 Muster reports will be printed as soon as a Muster begins. When the Select Report Printers dialog box opens, select a printer name from the list and click **OK**. You can select one or more printers, as long as the *PegasysServices* Windows user account that runs the P2000 Muster Service has the appropriate access rights to those printers.

Note: *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 a cardholder's last badge location will mean that he is inside or outside the Zone when 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 293 for details. Thereafter, a muster in progress will always use the last known badge activity, valid or invalid. Even invalid badging will show the cardholder's current location.

If the 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 cardholders regardless of the last badge time.
- **only if last badge is today** – Select this option if you wish to monitor who badged today.
- **unless last badge is older than** – Select this option to assume the cardholder 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 cardholder's last access grant was during a previous shift, to assume that the cardholder 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

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 cardholder 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 cardholder 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 296.

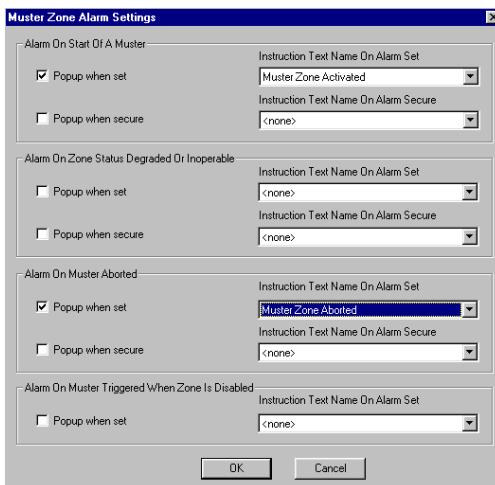
Muster Zone Alarm Settings

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 104.

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 Inoperable – 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 badges 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 badge 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 cardholders 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 cardholders 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 cardholders 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 cardholders, 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 if you wish to trace cardholder movement within the defined Muster Zone. Cardholders may be considered *Trapped*, *Wandering*, or *Rescuers*, depending on where and when they badge. See “Basic Definitions” on page 289 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 cardholders 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 cardholders 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

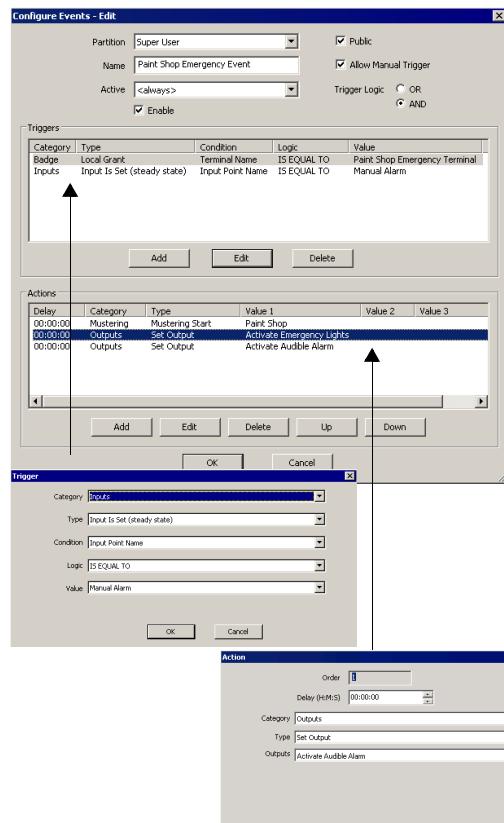
After Muster Zones are defined, they can be associated with one or more events, each of which can trigger a Muster for that zone as one of its actions.

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.

In the following 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).



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 314 to create new event triggers and actions.

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.

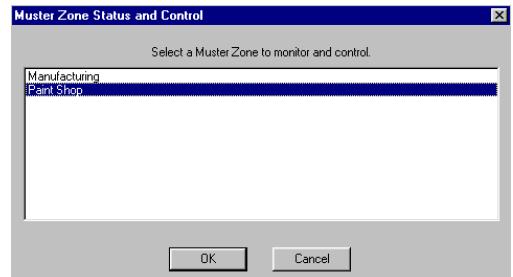
Mustering can be manually started and terminated by operator action using the Muster Zone Status and Control dialog box. When mustering is triggered by a P2000 event, the Muster Zone Status and Control dialog box automatically opens at the designated workstation selected in the Muster Zone Definition 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 cardholders still inside the zone is output repeatedly at the interval set up when the zone was defined. As cardholders badge at the designated muster terminals the situation is updated to show the new list of cardholders still in the zone.

Operators must first have Muster Control menu permissions to use this feature. Depending on the permissions assigned using the Menu Permission Groups, some or all operators may be able to control muster zones at any time. For detailed information see “Creating Permission Groups” on page 23.

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, badge number, and last known location and time of all cardholders currently in the defined Muster Zone. See the following “Muster Zone Status and Control Field Definitions” for details.

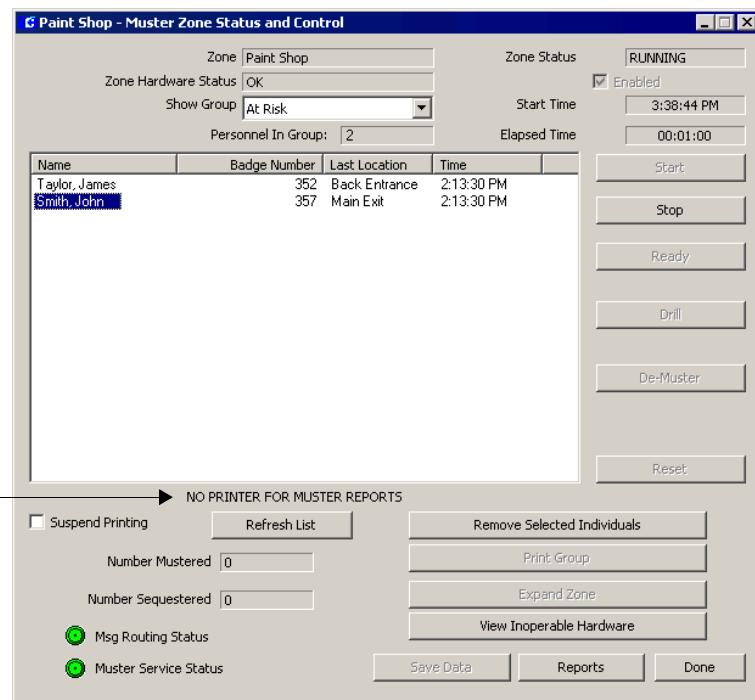
Muster Zone Status and Control Field Definitions

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*, *Trapped*, *Wandering*, *Mustered*, *Sequestered*, and *Rescuer*. See “Basic Definitions” on page 289 for details. The *At Risk* group is the default display.

Personnel In Group – Displays the current number of cardholders in the group selected in the Show Group drop-down list.

Enabled – Select the Enabled check box for the system to control this Zone. If you wish 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. If you wish to manually terminate a Muster, click the **Stop** button. The Zone Status will display the *Stopped* state and analysis reports

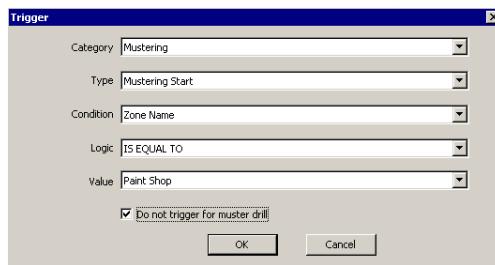
become available by clicking first the **Save Data** button and then the **Reports** button.

Once the Muster is stopped the Zone Control quits updating the list of cardholders.

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 cardholders are not

required to badge back into the Zone. All mustered cardholders 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, in order to add paper or take care of some other printer problem.

IMPORTANT: *Printing muster reports is not guaranteed on foreign language systems.*

Refresh List – Click this button to update the list box.

Number Mustered – Displays the total number of cardholders who have badged at a designated muster terminal.

Number Sequestered – Displays the total number of cardholders who have badged at a designated sequester terminal.

Remove Selected Individuals – This button can be used to manually move one or more cardholders from any group to any other group while a Muster is *Running*. 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 if you wish 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. See “Using the Real Time List” on page 322 for more information.

If you wish 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. See “Printing Tab” on page 41 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 439.*

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 **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.
- **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 cardholders 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.

In addition to the Muster Analysis report, the P2000 Standard Reports set includes the Muster Configuration report, which lists by Muster Zone name, all the zone definition configuration, as set up in the Muster Zone Definition dialog box. This report lists each Muster Zone and shows its defining and mustering terminals, and all associated events.

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), and output devices (bells, sirens).

The Intrusion Detection system consists of sensors, connected to the intrusion panel, capable of detecting various intrusion or burglary events. These intrusion detection sensors are associated with physical zones/points and grouped into areas; also intrusion events use audible annunciators to signal that a zone or area is in alarm condition.

The P2000 Intrusion Service resides on the P2000 Server and provides the communication between the P2000 system and third-party intrusion panels. This service allows the P2000 system to obtain status information whenever an intrusion component changes and issues commands to control the intrusion zones,

areas, and annunciators that are part of the intrusion system.

The P2000 system supports two intrusion detection integrations: OPC Aritech® and Bosch® (model D9412GV3). Complete hardware installation and operation instructions are provided with the intrusion system that is shipped with your option.

IMPORTANT: *The Aritech panel is not available in North America. Contact Johnson Controls Systems Integration Services Europe for 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 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
- Signal an alarm to inform local security forces that an intrusion has been detected
- Signal the intruder that has been detected

Basic Definitions

Annunciator – An annunciator is any electrical device connected to an Aritech or Bosch output point, which is activated when an intrusion is detected (for example, a siren). An annunciator can be silenced or activated manually.

Area – A group of zones within a facility (for example, 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.

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.

Intrusion Input Point – A device used to detect a change in a facility. A point senses an event that could represent intrusion such as a glass break, motion or door contact.

Intrusion Interface – Interface TCP/IP, RS232C, or OPC that is used to communicate with one or more intrusion servers.

Intrusion Server – A physical device or software component that controls one or more intrusion zones and/or areas.

Zone – A collection of one or more input points that are used to monitor a particular zone within the facility.

Sequence of Steps

The following sequence of steps are involved in the process of configuring, controlling, and monitoring intrusion components:

- Create and assign menu permissions to perform Intrusion Configuration and Control functions, see page 23.
- Enable the intrusion server (Aritech only), see page 303.
- Configure the Bosch intrusion panel (Bosch only), see page 304.
- Configure alarm options for intrusion devices. This allows you to view intrusion-related alarms on the P2000 Alarm Monitor and act accordingly, such as acknowledging the alarm, see page 306.
- Issue commands to control intrusion components, see page 308.
- View and monitor intrusion activity from the Real Time List and Real Time Map as they occur, see page 309.
- Control, monitor, and display the status of intrusion devices, areas, zones, and annunciators, see page 310.
- Define event triggers and actions associated with intrusion devices, areas, zones, and annunciators, see page 311.

Intrusion Configuration

The intrusion detection system consists of the P2000 software, the panel (OPC Aritech or Bosch) firmware, and I/O modules (attached to sensors and annunciators). Use the instructions provided with your intrusion hardware to define your intrusion system, such as the number and type of sensors, number of annunciators required, how these input and output devices will be associated with zones, and how zones will be included within areas.

The following sections describe intrusion configuration and operation procedures using the P2000 software.

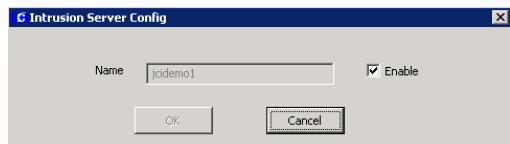
OPC Aritech Intrusion Interface

This interface controls the Intrusion OPC Server, which connects to Aritech devices to control intrusion zones, areas, and annunciators. The P2000 Intrusion Service connects to a single Intrusion OPC Server to support multiple intrusion devices.

Once you use the instructions provided with your Aritech panel to configure your intrusion panel and associated items, you must enable the intrusion server in the P2000 System Configuration window to populate the associated data into the P2000 database.

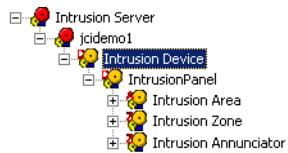
To Enable the Aritech Intrusion Server:

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 **Intrusion** icon.
3. Select the **Intrusion Server** icon and click **Add**. The Intrusion Server Config dialog box opens.



4. Verify that the Aritech intrusion server name displays in the **Name** field.
5. Select the **Enable** check box.
6. Click **OK**.

Once you enable the Aritech intrusion server, the System Configuration window is automatically populated with the intrusion device and associated intrusion areas, zones, and annunciators.



The P2000 system is now ready to operate with the Aritech intrusion panel, continue with “Intrusion Alarms” on page 306.

OPC Tags

The P2000 Intrusion Service obtains status information by monitoring the OPC tags defined within the Intrusion OPC Server and issue commands by writing values to the appropriate OPC tags.

The following table displays nine tags that are associated with the OPC Aritech panel, including the corresponding value for each of the tags. You must set up the panel correctly to communicate with the P2000 system to achieve these values.

Tag Number	Description	Value
1	Connected	True
2	InvalidVendorAddress	False
3	PortOpened	True
4	MainsFailure	False
5	BatteryLow	False
6	BatteryTest	False
7	BatteryTestFail	False
8	BatteryMissing	False
9	Tamper	False

Be aware that under certain conditions, the P2000 system may indicate that the Aritech panel is in fault status, but the overall operation of the Aritech interface is normal. For example:

If tags 2, 4, and 5 are set with a value of True, it indicates that:

2 = vendor Address format is incorrect

4 = Aritech panel is working in battery mode

5 = battery charge is Low

Under these conditions, the Aritech panel is still operational because:

Tag 2: Vendor Address is invalid – Even if the address format is invalid, maybe that default values are already correct. If panel address is equal to 1 and the password is set to the default value “0000000000,” the Aritech panel still communicates with OPC Server; therefore, the invalid address fault is displayed but ignored. Also, note that each field (Address, Password, and System) is independent from others. For example, if the Password field is correct and Address field is incorrect, the driver will successfully parse the password value and will return the InvalidVendorAddress condition because the Address is wrong (but it will set Address to the default value 1).

Tag 4: Mains failure – This means that the Aritech panel is working in battery mode, but it stays online while the battery works.

Tag 5: Battery charge is Low – In this case the Aritech panel is working with a battery in low condition, but not yet exhausted. So, it will communicate until power is present.

Bosch Intrusion Interface

This integration allows P2000 operators to configure and control Bosch intrusion devices. The intrusion system may have multiple, independent Bosch intrusion panels, and each Bosch intrusion panel can support multiple intrusion areas/zones.

Before you configure your Bosch intrusion panels, ensure that the following settings are in place to establish the communication between the P2000 Server and the Bosch intrusion panel:

- The Bosch intrusion integration uses TCP/IP protocol to communicate between the Bosch panel and the P2000 Server; therefore, you must establish the availability of a network interface module (Connetix DX4020):
 1. This is provided by Bosch to connect with the Bosch panel via TCP/IP protocol.
 2. After setting up the DX4020 module based on the instructions provided by Bosch, change the dip switch address on the network interface module to reflect address “80.”
 3. Telnet into the network module via the command “Telnet <ip address> 9999” and change the channel 1 settings.
 - a. Set Connectmode to c0 for P2000/third party automation.
 - b. Do not change any other settings and press <Return> to leave the default settings.

Send ‘+++’ in Modem Mode (Y) ?
Auto increment source port (N) ?
Remote IP Address : (000) .(000) .(000) .(000)
Remote Port (0) ?
DisConnMode (02) ?
FlushMode (00) ?
DisConnTime (00:00) ?:

- You must modify some parameters using Bosch Remote Programming Software (RPS) to program the panel.
 1. Verify that under the AUXPARM settings, the SDI RPS Automation is enabled. This enables the third-party communication for the panel.
 2. Verify that under the “POINTS” section, the point indexes have the parameters as listed below:

a. Bypassable (enables bypassing from the Third party automation) : -	Yes
b. Defer Bypass Report : -	No
c. Alarm Abort : -	No

After you define the above settings and configure your intrusion devices using the instructions provided with your Bosch panel, you must define the Bosch panel using the P2000 software.

To Configure the Bosch Intrusion Panel:

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 **Intrusion** icon.
3. Select the **Bosch Intrusion** icon and click **Add**. The Bosch Intrusion Panel Edit dialog box opens.

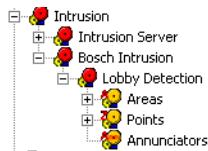


4. If you use Partitioning, select the **Partition** that will have access to this panel, and select the **Public** check box if you wish to allow all partitions to see the panel.
5. Enter a descriptive **Name** for the panel.
6. Enter the **IP Address** of the intrusion panel.
7. Enter the **Port Number** of the intrusion panel.
8. Enter the **Query String** value to be used with message filtering (see “Define Query String Filters” on page 211), and also with the P2000-Metasy integration feature (see “Configuring Hardware Components for BACnet Interface” on page 347).

9. The **Read Configuration** button is provided to refresh the configuration in this panel with information from the Bosch panel. This button is only available after you save the panel information.

10. Click **OK** to save your settings.

After you save the Bosch intrusion panel, the System Configuration window is automatically populated with the associated intrusion areas, zones, and annunciators that were configured using the Bosch user interface.

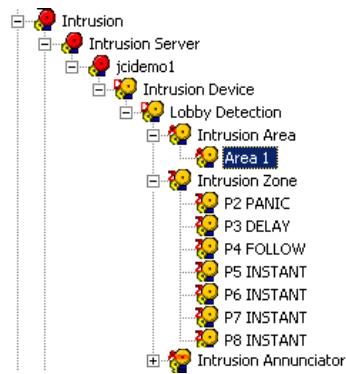


Intrusion Alarms

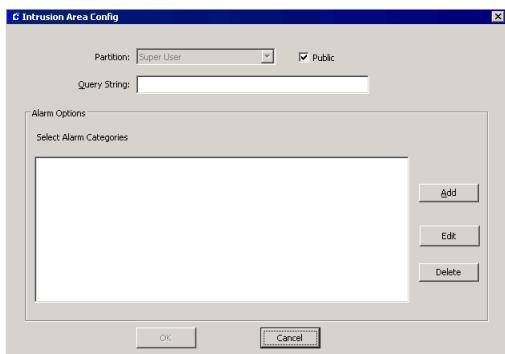
Intrusion components that generate alarms must belong to at least one alarm category, and must provide their own set of alarm options and parameters to define how the alarms will behave when activated, whether or not they need to be acknowledged, at what time an alarm can be activated, and other alarm settings that provide the flexibility of automating the alarm operation.

To Configure Aritech Intrusion Alarms:

1. In the System Configuration window, click the plus (+) sign next to the root **Intrusion** icon.
2. Click the plus (+) sign next to the **Intrusion Server** icon to display all Aritech intrusion components.
3. Select an Intrusion component (Device, Area, Zone, or Announcer). Click **Edit**.

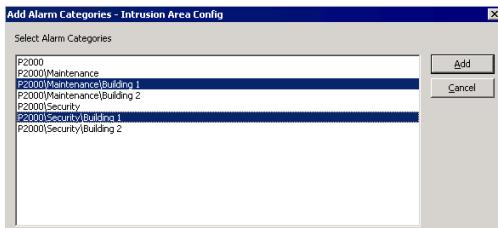


4. The **Intrusion Config** dialog box opens for the selected item (Device, Area, Zone or Announcer).



5. If you are configuring alarm options for an **Intrusion Device**, select from the **Partition** drop-down list, the appropriate Partition that will have access to the **Intrusion Device**. Partition selection is only available at the **Intrusion Device** level.
6. Select the **Public** check box if you wish the Device/Area/Zone/Announcer to be visible to all partitions.
7. Specify the **Query String** value to be used with message filtering and with the P2000-Metasys integration feature.
8. Click the **Add** button to assign this alarm to one or more **Alarm Categories**. The **Add Alarm Categories** dialog box opens dis-

playing all previously created alarm categories (see page 255 for details).

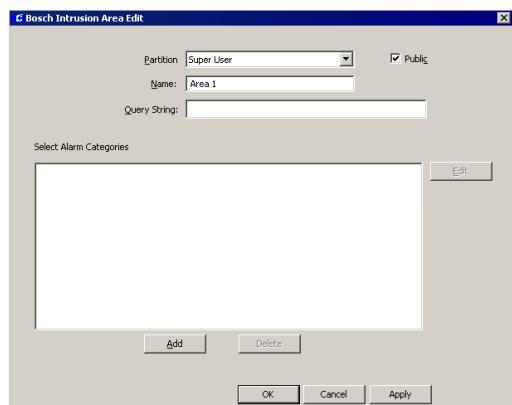


Note: If you use the Enterprise feature, the Alarm Categories defined for all P2000 sites within an Enterprise system will be listed.

9. Select one or more categories and click the **Add** button. The list will display all the selected alarm categories.
10. If you wish to remove a category from the list, select the alarm category and click **Delete**.
11. 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. See the definitions provided on page 97.

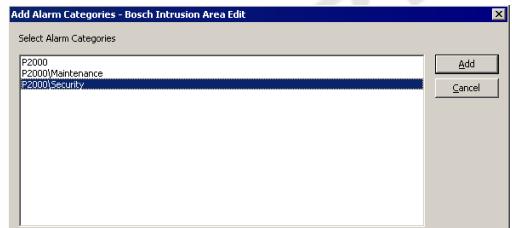
To Configure Bosch Intrusion Alarms:

1. In the System Configuration window, click the plus (+) sign next to the root **Intrusion** icon.
2. Click the plus (+) sign next to the **Bosch Intrusion** icon to display all Bosch intrusion panels.
3. Select the intrusion area you wish to configure and click **Edit**. The Bosch Intrusion Area Edit dialog box opens.



Note: You can only configure alarms that are associated with Bosch Intrusion Areas.

4. Select from the **Partition** drop-down list, the appropriate Partition that will have access to the Bosch Intrusion Area.
5. Select the **Public** check box if you wish the area to be visible to all partitions.
6. Specify the **Query String** value to be used with message filtering and with the P2000-Metasy integration feature.
7. Click the **Add** button to assign this alarm to one or more Alarm Categories. The Add Alarm Categories dialog box opens displaying all previously created alarm categories (see page 255 for details).



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

8. Select one or more categories and click the **Add** button. The list will display all the selected alarm categories.
9. If you wish to remove a category from the list, select the alarm category and click **Delete**.
10. 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. See the definitions provided on page 97.

Intrusion Management

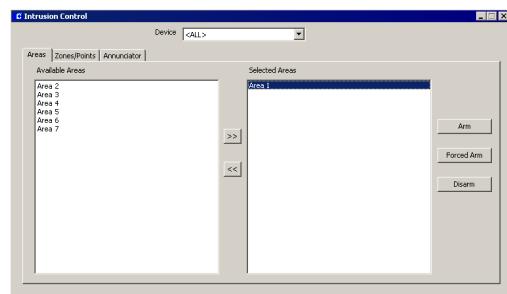
Management of intrusion includes displaying the current state of intrusion items as well as issuing commands for such activities (arm, disarm, bypass, etc.). The following sections describe how to monitor and control intrusion items.

Controlling Intrusion Items Using the Intrusion Control Window

Use the Intrusion Control window to perform commands for areas, zones, and annunciators. It allows operators to arm and disarm areas; reset, bypass, and make any zones operational; and silence or activate any annunciator.

To Control Intrusion Items:

1. From the P2000 Main menu select **Control>Intrusion**. The Intrusion Control dialog box opens.



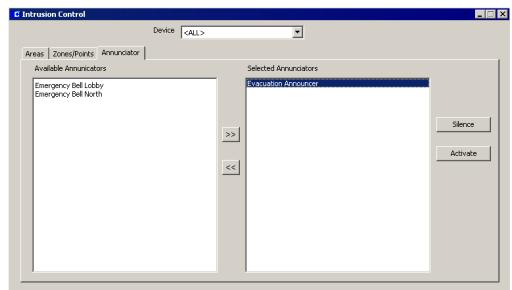
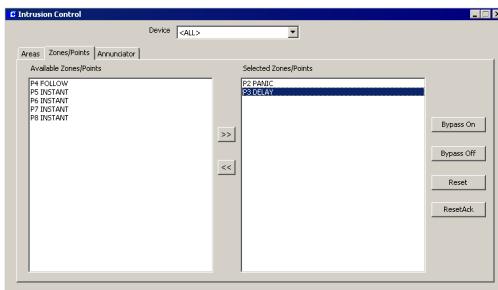
2. From the **Device** drop-down list, select the device (Aritech or Bosch panel) name you wish to control.
3. If you wish to control an intrusion area, click the **Areas** tab. From the list of **Available Areas** at the left side of the window, select the area you wish to control.
4. Click the **>>** button to move the selected area to the **Selected Areas** box. You can add as many areas as you wish. Once you have the selected areas, click the function button on the right side of the window to perform the associated operation. The choices are:

Arm – Arms the selected area(s) if at the time that you issue the command the area's state permits it.

Forced Arm – Arms the selected area(s) regardless of the area's state at the time when you issue the command.

Disarm – Disarms the selected area(s).

5. If you wish to control an intrusion zone, click the **Zones/Points** tab. From the list of **Available Zones/Points** at the left side of the window, select the zone you wish to control.



6. Click the >> button to move the selected zone to the **Selected Zones/Points** box. You can add as many zones as you wish. Once you have the selected zones, click the function button on the right side of the window to perform the associated operation. The choices are:

Bypass On – Commands the selected zone(s) to be bypassed.

Bypass Off – Turns off bypassing of the selected zone(s).

Reset – Resets the state of the selected zone(s). If you issue this command while the input point is still in alarm due to still being unsealed, you must seal the input and send this command again to reset it.

ResetAck – Resets the state of the selected zone(s). If you issue this command while the input point is still in alarm due to still being unsealed, there is no need to re-send the command after the input is sealed. The command will remain valid and reset the zone(s) as soon as the input seals.

7. If you wish to control an intrusion annunciator, click the **Annunciator** tab. From the list of **Available Annunciators** at the left side of the window, select the annunciator you wish to control.

8. Click the >> button to move the selected annunciator to the **Selected Annunciators** box. You can add as many annunciators as you wish. Once you have the selected annunciators, click the function button on the right side of the window to perform the associated operation. The choices are:

Silence – Silences the selected annunciator(s).

Activate – Activates the selected annunciator(s).

9. When you finish controlling the intrusion items, close the Intrusion Control dialog box.

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. See “Using the Real Time List” on page 322 for more information.

Note: If you wish to print intrusion transactions as they occur, you can either print them from the Real Time List window, or select the **Intrusion** check box in the Site Parameters dialog box, *Printing* tab, see page 41.

Monitoring Intrusion Using the Real Time Map

Use the Real Time Map tool to display the status of intrusion areas, zones/points, annunciators, and intrusion 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. See “Using the Real Time Map” on page 326.

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/point. 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 “Creating a Real Time Map” on page 328.

Map Maker provides a default intrusion image set to display various intrusion states. However, you can use your own icons to create custom image sets. See “Adding Image Sets” on page 332 for details.

Viewing and Controlling Intrusion Items Using the System Status Window

The System Status window displays the status of intrusion components that are configured to monitor intrusion detection. It also allows you to issue the commands, depending on the state of the following intrusion component:

Intrusion Areas – The system displays the status of all intrusion areas associated with the selected intrusion panel. You can issue commands for the area by right-clicking the associated status icon. The following commands may be available, depending on the current state of the area:

- **Arm** – Arms the selected area if at the time that you issue the command the area’s state permits it.
- **Forced Arm** – Arms the selected area regardless of the area’s state at the time when you issue the command.
- **Disarm** – Disarms the selected area.

Intrusion Zones – The system displays the status of all intrusion zones associated with the selected intrusion panel. You can issue commands for the zone by right-clicking the associated status icon. The following commands may be available, depending on the current state of the zone:

- **Bypass On** – Commands the selected zone to be bypassed.
- **Bypass Off** – Turns off bypassing of the selected zone.
- **Reset** – Resets the state of the selected zone. If you issue this command while the input point is still in alarm due to still being unsealed, you must seal the input and send this command again to reset it.
- **ResetAck** – Resets the state of the selected zone. If you issue this command while the input point is still in alarm due to still being unsealed, there is no need to re-send the command after the input is sealed. The command will remain valid and reset the zone as soon as the input seals.

Intrusion Announciators – The system displays the status of all intrusion annunciators associated with the selected intrusion panel. You can issue commands for the annunciator by right-clicking the associated status icon. The following commands may be available, depending on the current state of the annunciator:

- **Activate** – Activates the selected annunciator.

- **Deactivate** – Deactivates the selected annunciator.

See “System Status” on page 439 for instructions on how to display intrusion status and/or issue commands.

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 see “Creating Events” on page 314. 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 that is granted access (trigger) silences an intrusion annunciator (action).

For a complete list of event triggers and actions associated with intrusion devices, areas, zones, and annunciators, see *Appendix A: Event Triggers/Actions*.

Hours On Site

This feature allows you to record a cardholder’s accumulated number of hours present at a site. The Hours On Site application is used exclusively for tracking and reporting purposes and works by recording the cardholder’s time interval between an **in** badging and **out** badging at reader terminals that are defined to monitor Hours on Site.

Time is accrued only from the latest in and out badging. For example, when a cardholder badges at a reader defined as an *Entry Terminal*, the cardholder’s time is accrued. If the same cardholder badges at the same or other Entry Terminal, the first badging is ignored and the time is accrued from the latest badging. The reverse is true for an *Exit Terminal*. Hours On Site will accurately report hours present between matched pairs of in and out badgings (that is, an in badging followed by an out badging, with no other badgings in between).

Configuring Hours On Site Zones

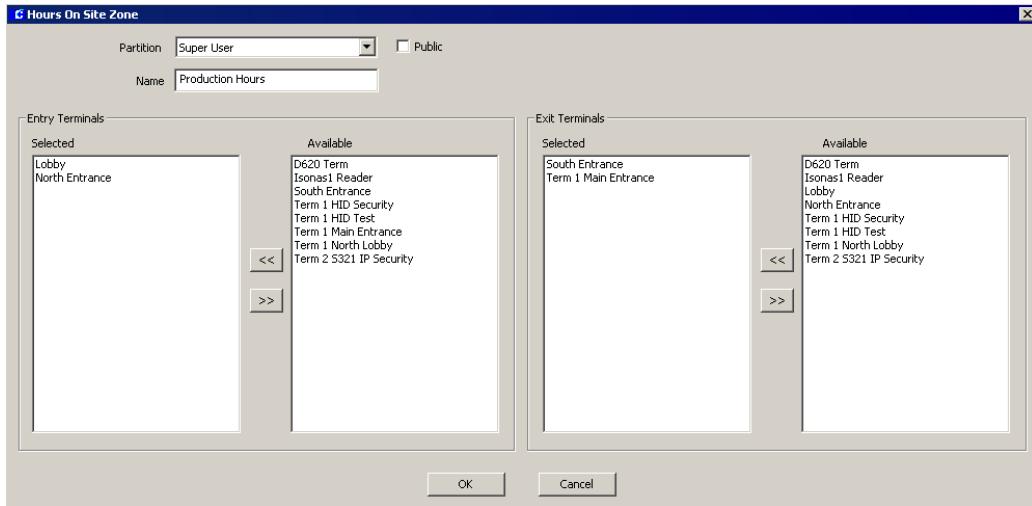
Before you initiate data collection, you must define the readers that will provide real time information to track a cardholder’s time spent at a particular area.

Use readers that are related to a particular section of your facility. For example, you may want to select readers located at the entrance of a production facility that will provide for the **in** hours, and select readers located at the exit of the facility that will be used for the purpose of reporting the **out** hours.

The Hours On Site feature does not determine where and when cardholders have access in and around a facility – there is no access control or transaction processing associated with this function, the terminals that are selected for this feature are defined for time tracking purposes only.

To Define Hours On Site Zones:

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



2. Click the **Hours On Site Zones** root icon and click **Add**. The Hours On Site Zone dialog box opens.
3. If this is a partitioned system, select the **Partition** that will have access to this Hours On Site zone, and select **Public** if you wish the Hours on Site zone to be visible to other partitions.
4. Enter a descriptive **Name** for the Hours On Site zone.
5. In the **Entry Terminals** box, select the terminals from the **Available** list that will be used for Hours on Site *in* transactions. Cardholders should use any of these terminals when entering a facility or area within a facility, to start the accumulation of hours present.
6. In the **Exit Terminals** box, select the terminals from the **Available** list that will be used for Hours on Site *out* transactions. Cardholders should only use any of these terminals when leaving a facility or area within a facility, to stop the accumulation of hours present.
7. Click **OK**. A new icon will display under the root Hours On Site Zones icon in the System Configuration window.

Hours On Site Reporting

You can run Hours On Site reports at any time to determine cardholders' current number of hours present at a specified area in a facility.

These reports display calculated attendance and are ready for evaluation and printing. You can also export these reports into a payroll or human resources system for further calculation.

Hours On Site reports are provided as a subset of the standard P2000 report set. This section describes details specific to Hours On Site reports. For detailed information on running reports, see *Chapter 6: System Reports*.

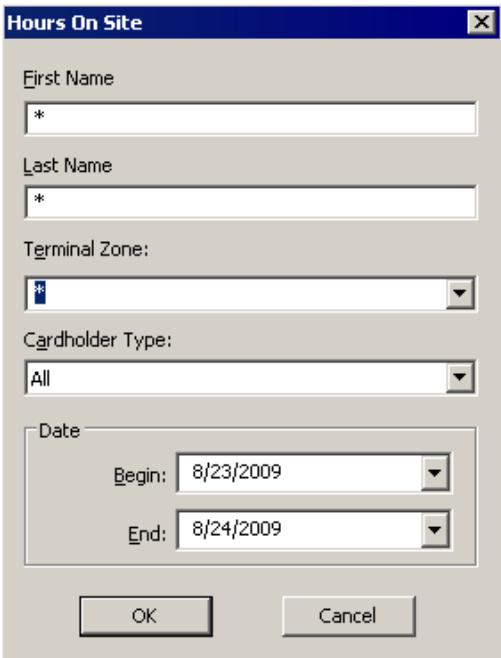
To Run Hours On Site Reports:

1. From the P2000 Main menu, select **Report>Run Report**. The Run Report dialog box opens.
2. Scroll down to the two Hours On Site reports provided and select one of the following:

Hours on Site – Lists a detailed report of a cardholder's accumulated number of hours present at a site.

Hours on Site - Simple – Lists a summary report of a cardholder's accumulated number of hours present at a site.

Regardless of your selection, the Hours On Site dialog box opens displaying filtering options.



3. The default (*) reports all cardholders. Enter a **First Name** or **Last Name** to limit the report to a specific cardholder.
4. From the **Terminal Zone** drop-down list, select the zone that contains the readers that were defined to track hours on site; or select the (*) to report on all defined terminal zones.

5. From the **Cardholder Type** drop-down list, select whether you want to report on Regular cardholders, Visitors, or All.
6. Select a **Begin** and **End** date for the transactions you wish to see. Only records within these dates will be listed in the report.
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 Hours On Site report displays in the Crystal preview window. The top section of the report displays information according to the filtering options that you selected in the Hours On Site dialog box. 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 export or print all or single pages of the report.

Hours On Site (Detail) Report

This report provides detail cardholder activity based on your selected search criteria. The report displays the cardholder name, badge number used, specific terminal name where the badge was presented, the terminal zone that contains the specified terminal, and the in and out date and time when the cardholder badged at the terminal. In addition, this report also displays the total number of hours on site per day, per badge, and for the entire report.

This information is updated each time the cardholder badges at the terminals included in Hours On Site zones.

Hours On Site Report

Report Filter:

First Name:	Jenny
Last Name:	Hkg
Terminal Zone:	*
Date Range:	From 8/25/2009 through 8/26/2009
Cardholder Type:	All

Cardholder Name: King, Jenny

Time and Attendance Details: 8/25/2009

Badge Number	Terminal Name	Terminal Zone	In / Out	In / Out Time
369	CH21A_A225 T1	Production Hours	In	8/25/2009 8:24:24AM
369	CH21A_A225 T2	Production Hours	Out	8/25/2009 8:24:41AM
				In - Out Hours: 00:00:17
369	CH21A_A225 T2	Production Hours	Out	8/25/2009 4:23:37PM
				In - Out Hours: 07:58:07

Total time for 8/25/2009: 07:59:13 *

Time and Attendance Details: 8/26/2009

Badge Number	Terminal Name	Terminal Zone	In / Out	In / Out Time
369	CH21A_A225 T1	Production Hours	In	8/26/2009 5:11:24AM
369	CH21A_A225 T2	Production Hours	Out	8/26/2009 4:07:58PM
				In - Out Hours: 07:58:46

Total time for 8/26/2009: 07:58:46

Total Time for Badge 369 for 8/25/2009 to 8/26/2009: 15:55:59 *

Total Time for Entire Report: 15:55:59 *

End of Report

Records marked with an * indicate out of sequence in/out times
Hours On Site Report
Report Filter: First Name = Jenny; Last Name = Kwon; Terminal Zone = *;
Date Range = 8/25/2009 through 8/26/2009

Note that records marked with an asterisk (*) indicate out of sequence in/out times. This occurs when:

- a cardholder badged more than once at designated in readers without badging at an out reader
- a cardholder badged more than once at designated out readers without badging at an in reader
- a cardholder badged in and no subsequent out badging occurred on that calendar day
- the first badging of the first day of the report is an out
- the last badging of the last day of the report is an in.

The asterisk could also indicate that the report might be displaying incomplete badging information, depending on what time of day and date the report is run.

Hours On Site - Simple Report

This summary report is run using the same Run Report criteria as the detailed report. The difference between this report and the detailed report is that the “Simple” report only shows total times for each cardholder, not badging time details.

Hours On Site Report - Simple

Report Filter:

First Name:	*
Last Name:	*
Terminal Zone:	*
Date Range:	From 8/25/2009 through 8/26/2009
Cardholder Type:	All

Cardholder Name: DAM, TIEN **Badge Number:** 6

Total time for 8/25/2009: 16:23:29 *

Total time for 8/26/2009: 07:56:30

Total Time for Badge 6 for 8/25/2009 to 8/26/2009: 24:19:59 *

Cardholder Name: Kwon, Jenny **Badge Number:** 369

Total time for 8/25/2009: 07:59:13 *

Total time for 8/26/2009: 07:58:46

Total Time for Badge 369 for 8/25/2009 to 8/26/2009: 15:55:59 *

Total Time for Entire Report: 40:15:58 *

End of Report

Records marked with an * indicate out of sequence in/out times
Hours On Site Report - Simple
Report Filter: First Name = *; Last Name = *; Terminal Zone = *;
Date Range = 8/25/2009 through 8/26/2009

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 a cardholder 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 105.

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.

Event	Partition	Public
Event 1	Super User	No
Badge 14321 Event	Super User	Yes
Activate Lights	Warehouse	No

- Click **Add**. The Configure Events – Add dialog box opens.

Category	Type	Condition	Logic	Value
Badge	Host Grant	Badge	IS EQUAL TO	301

Delay	Category	Type	Value 1	Value 2
0	None	None	None	None

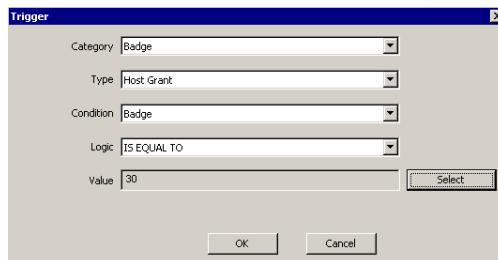
- If this is a partitioned system, select the **Partition** in which this event will be active and select **Public** if you wish this event to be visible to all partitions.
- Enter a descriptive **Name** for the event. When the event is configured, this name will display in the Configure Events list, so make it meaningful to those who must work with it.
- In the **Active** field, select from the drop-down list the **Time Zone** during which this event will be active.
- Select **Allow Manual Trigger** if an operator will manually initiate this trigger. See “Creating Manual Triggers” on page 321 for detailed information.

- 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 (that is, 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.

- Select the **Enable** check box to enable the event.
- In the **Triggers** box, click **Add**. The Trigger dialog box opens.



- Enter the information in each field as described in the Trigger Field Definitions.

- 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.

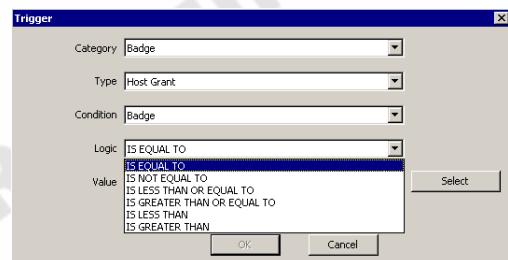
Trigger Field Definitions

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 30.

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.

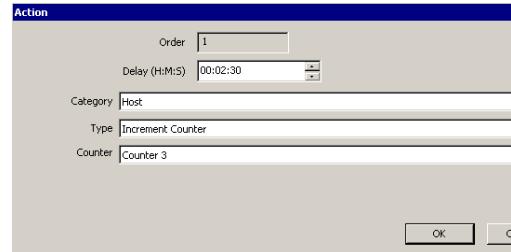
Creating Actions

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.

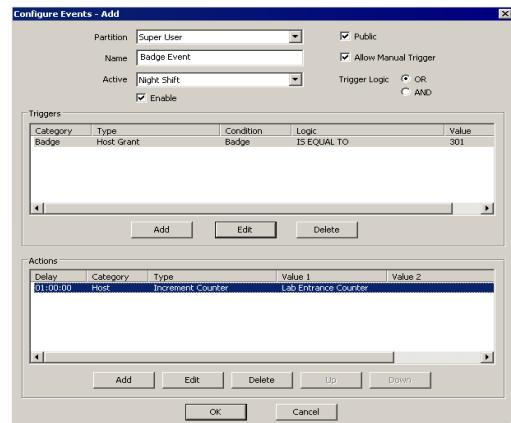
An event can trigger more than one action. You can create a number of actions and specify in what order the actions will occur.

To Create an Action:

- In the Configure Events dialog box, go to 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.



- Continue to add actions as required.

To Change Event Action Order of Occurrence:

- 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 would be 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, an additional field is created that lists the counters available.

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.

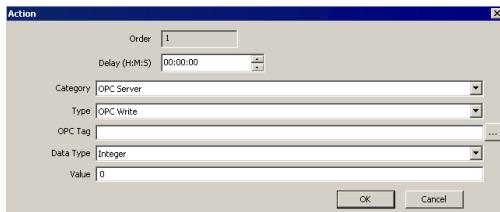
OPC Server Event Actions

IMPORTANT: *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.*

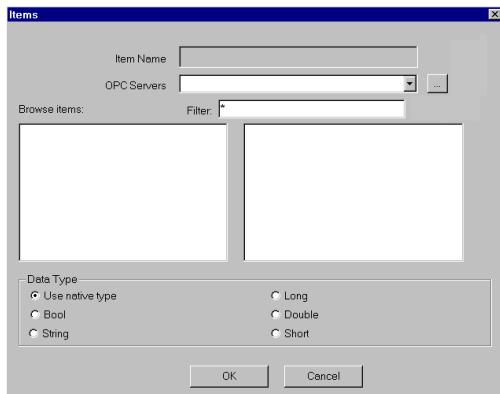
The following applies to OPC (OLE for Process Control) Server events:

- 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*.

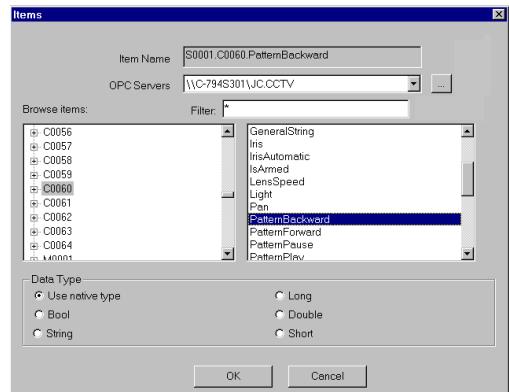
In order to select an OPC Server and view the available tags, a tag browser is provided in the event Action dialog box. Note that to select an OPC Server, the OPC Server must be running and you must have the appropriate rights.



- 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).

- Select the appropriate **Data Type** from the drop-down list for the event action value.
- Enter the **Value** that is to apply to the OPC Tag.
- Click **OK** to return to the Configure Events dialog box. The new event action will display in the Actions list.

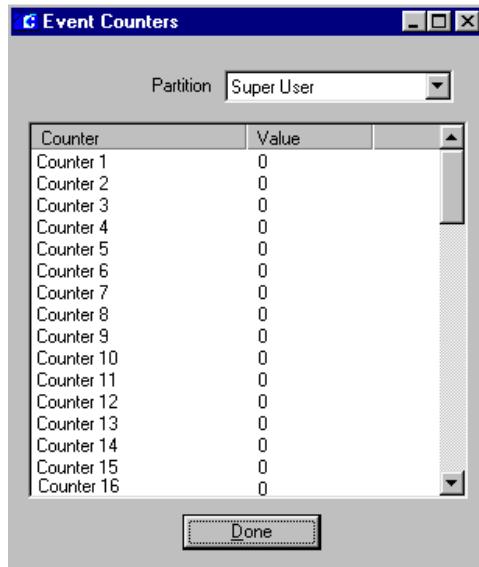
Counting Events

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.



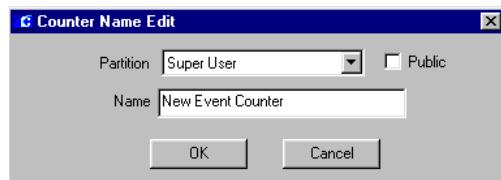
Event counters are listed under the Counter column. The Value column lists the accumulated number of events attached to each counter. You can add as many counters as you wish, or change the event counter name to give the counter a meaningful name, see the following section for detailed information.

- 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.



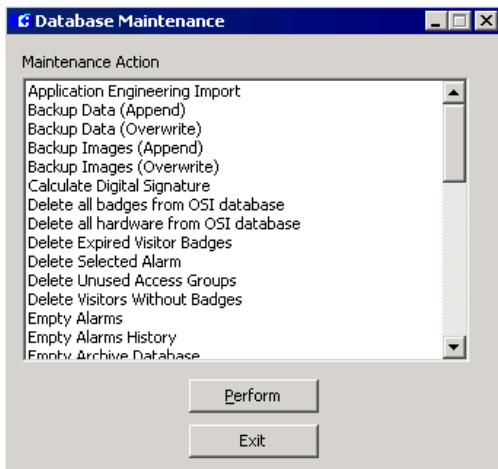
- If this is a partitioned system, select a **Partition** where the counter will apply and select **Public** if you wish this counter to be visible to all partitions.
- Enter a descriptive **Name** for the counter.
- Click **OK**. The new counter displays beneath the main Counters icon.

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.



2. Under Maintenance Action, select **Reset Counters to Zero**.
3. Click **Perform**. Since this action cannot be undone, a verification message displays to confirm your action.
4. Click **Yes** if you wish to reset counters to zero. The Reset Counters dialog box opens.



5. If this is a partitioned system, select the **Partition** in which the counters are active.
6. Click **Reset to Zero**. All values in the Event Counters list will be reset to zero.
7. Click **Done** to return to the Database Maintenance dialog box.
8. Click **Exit**.

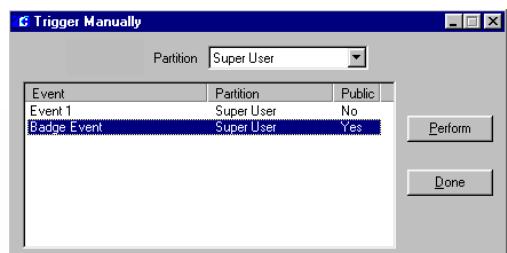
Creating Manual Triggers

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 262), 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 328), regardless if the “Allow Manual Trigger” option was enabled in the Configure Events dialog box.

To Manually Trigger an Event:

1. From the P2000 Main menu, select **Events>Trigger Manually**. The Trigger Manually dialog box opens.
2. All the events that have the “Allow Manual Trigger” option selected in the Configure Events window will display in the list.
3. Select an event from the list, and click **Perform**. The trigger will be activated.
4. 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 a cardholder 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 41. 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 exam-

ple, to ensure all transaction types are being processed, or trace why a specific cardholder is being denied access.

Monitoring Remote Messages in Real Time

As with remote alarm monitoring (page 257), 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). See “Starting and Stopping Service Control” on page 435.
- The **Message Filter Configuration** application (page 209), 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.

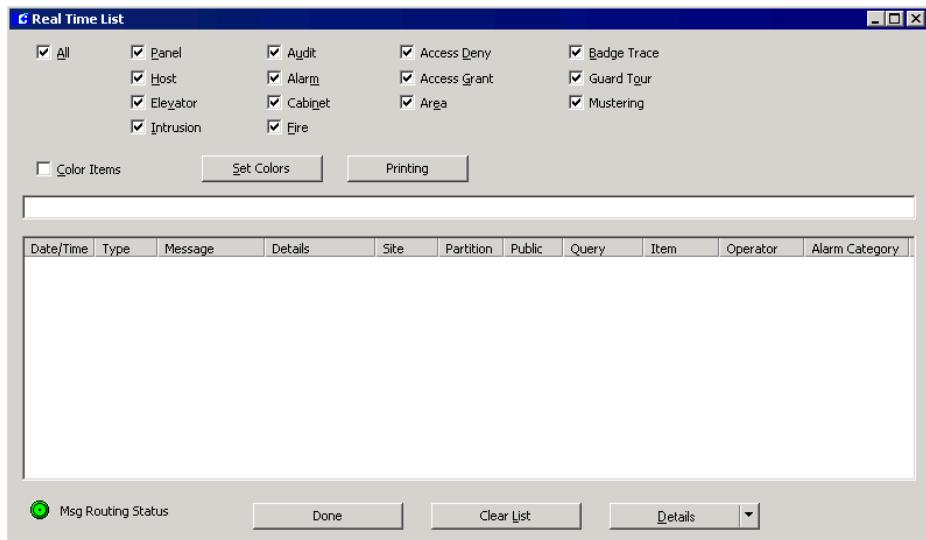
- The **P2000 Remote Server** application (page 216), must be properly configured at each remote site in order to send their transactions messages to your local site. The setup must include the name, IP address and Remote Message Service Listener Port number of your local site; the type of messages that will be forwarded to your site and at what times; and other related parameters.
- The **Process Received Remote Messages** option in the RMS tab of Site Parameters (page 50), 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 50), 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 print transactions as they occur, or print all transactions in the list.

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 Cardholder 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 uses the DVR feature 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 **Details** drop-down arrow 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 your DVR documentation.

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** check 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 if you wish to reset the colors to the default system colors.
6. Click **OK** to return to the Real Time List window.

To Display Cardholder Details:

1. Select from the scrolling list, the transaction line item associated with a cardholder (Access Deny, Access Grant or Badge Trace transactions).
2. Click the **Details** drop-down arrow located at the bottom of the window, and select **Cardholder Info**. The Cardholder Info dialog box opens.



The top portion of the window shows the cardholder details including image, if available.

The bottom portion includes a chronological list of badge transactions associated with the cardholder.

3. If you wish 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 from the workstation, all (or all displayed) transactions in the Real Time List, or print individual transactions as they occur.

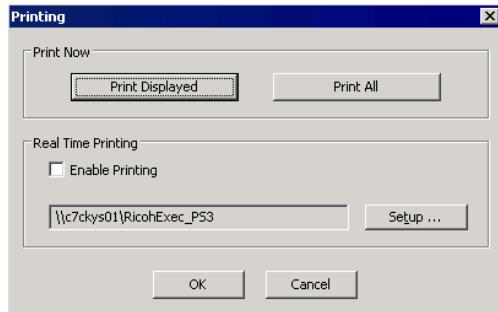
IMPORTANT: Real time printing is not guaranteed on foreign language systems.

Printers must first be set up using the Windows Printer Settings dialog box. See your system administrator if you need more information.

mation, or refer to your Microsoft Windows documentation.

To Print the Real Time List:

1. In the Real Time List window, select the **Printing** button in the top portion of the window. The Printing dialog box opens.



2. Click the **Print Displayed** button to print the transactions that are visible in the Real Time List box, or click the **Print All** button to print all transactions in the list.
3. Select a printer name and any other information for the printer to be used.
4. Click **OK** to start printing.

To Print Real Time List Line Items:

1. In the Real Time List window, select the **Printing** button in the top portion of the window. The Printing dialog box opens.
2. Click the **Enable Printing** check box. Line items will continuously 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.
3. Click the **Setup** button to select a printer name and any other information for the printer to be used.

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.

4. Click **OK**. The printer name displays.
5. Click **OK** to enable printing.

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 41.

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 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.

Sub Maps and Attachments

You can create facility-level maps and attach sub maps (Normal and Popup 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.

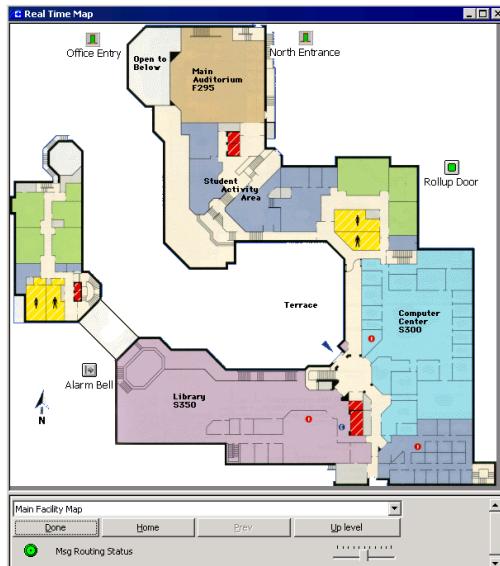
If an alarm sets in an area detailed in a sub map, the sub map icon will blink, indicating the location of the alarm. You can double-click the blinking sub map icon to jump to the associated detail map. (See “Adding Map Attachments” on page 332 for more information about creating multi-level maps.)

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. See “Adding Image Sets” on page 332 for details.

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:

- 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: Icons that are crossed out with a yellow bar indicate that the items' parent devices are not functioning. For example, an input point will be marked as unreliable if its parent terminal or panel is down.

Note: If your facility uses the DVR feature, 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 your DVR documentation.

- From the drop-down list at the bottom of the window, select the name of the map you wish to view. The list only displays Normal maps.
- If your facility uses Map Attachments, 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.

Note: The **Prev**, **Home**, and **Up level** navigation tools are not used with Popup Map Attachments.

- 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. You can also use keyboard commands to enlarge or reduce the view of

the active map. Use the **Up** or **Left** arrow keys to reduce the view and the **Down** or **Right** arrow keys to enlarge the view.

6. 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 330 to insert a door icon.

To Open a Door from a Real Time Map:

1. Locate the door terminal icon for the door you wish to open.
2. 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.

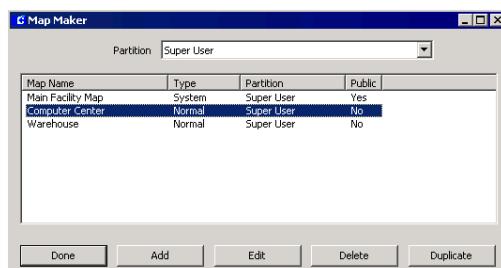
Creating a Real Time Map

The following steps allow you to create a Real Time Map using Map Maker's drag-and-drop feature:

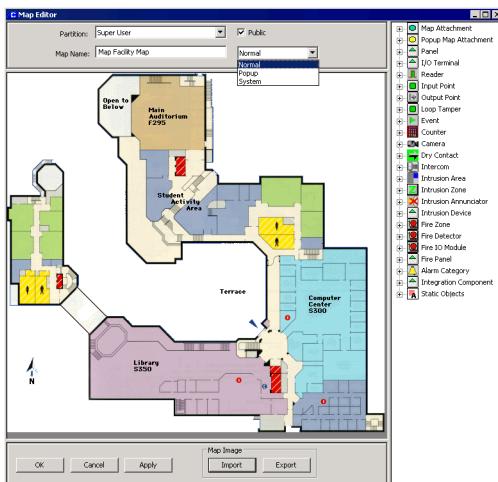
- Set up the Map Maker window
- Create an importable image
- Import the image to Map Maker
- Drag-and-drop map icons onto the map
- Add Map Attachments
- Duplicate a Map

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**.
5. From the drop-down list, on the right side of the Map Name, select one of the following options:

System – A system map automatically displays when you open the Real Time Map. You can only create one system map. The system map will display any defined sub maps (Normal or Popup).

Normal – A normal map is a sub map that can be used as a Map Attachment or Popup Map Attachment on another map. It can also be selected from the drop-down list at the bottom of the Real Time Map window.

Popup – A popup map is a sub map that can be used as a Map Attachment or Popup Map Attachment on another map. It is not selectable from the Real Time Map drop-down list.

Note: Normal and Popup maps that are used as Popup Map Attachments do not provide tools to navigate to other maps.

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 when you click the **Import** button.)

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.
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. 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.

Note: If you wish to export the map image, click the **Export** button. Navigate to the directory where the exported map will be stored, give it a name, and select the file type and other related parameters.

To Place Device Icons on a Real Time Map:

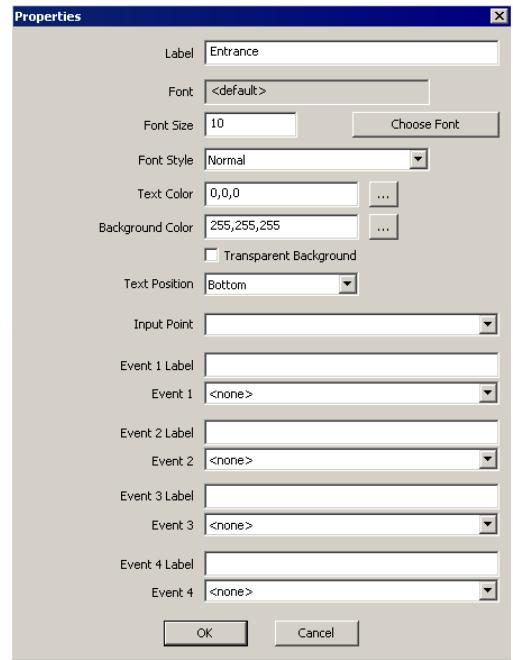
When you open Map Maker, map icons representing Panels, Terminals, Inputs, Outputs, and other system elements are listed on the right windowpane.



Note: If your facility uses advanced features, such as Intercom or DVR, the associated map icons will display in the list. See the respective section in Chapter 4: Advanced Features, for more information.

1. Click plus (+) sign next to the element you wish to add. To add 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.

TIP: The top left corner of the icon will be anchored exactly where the tip of the mouse pointer is released.



3. In the **Label** field, enter a descriptive name that can easily identify the icon in the Real Time Map. This name will display under the icon on your layout.

4. The **Font** box displays the default font or the font selected for the icon name.
5. In the **Font Size** box enter the font size for the name appearing under the icon.
6. To make all font changes at once, click the **Choose Font** button and select a font type, style, and size for the name appearing under the icon.
7. If you wish to change the **Font Style**, select from the drop-down list whether the text should be Bold, Bold Italic, Italic or Normal.
8. To display the text in a different color, click the **Text Color** browse button [...] and select a color from the Color dialog box.
9. Click the **Background Color** browse button [...] to open the Color dialog box and select the background color for the icon name.
10. Select the **Transparent Background** check box if you wish the background of the text to be transparent.
11. From the **Text Position** drop-down list, select whether you want to place the text at the Bottom, Left, Right, or Top of the icon.
12. Select from the drop-down list the name of the item you wish to place in the map. If you are placing an input point, 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).
13. To assign events to the item, 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.
14. Click **OK** to close the Properties dialog box. The icon will be inserted in the map.
15. Repeat the same steps for each device or event you wish to add to the map.
16. 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.
17. Click **Done** to close the Map Maker dialog box.

Handling Alarms from the Real Time Map

You can place an **Alarm Category** icon on a Real Time Map and issue commands for all P2000 items that generate alarms, (such as input points or cameras) and that use the Alarm Category selected.

When an alarm is reported in the system, the Alarm Category icon will flash on the map. You can right-click the icon to issue from a shortcut menu one of the alarm commands (acknowledge, respond, or complete). If you select *Acknowledge* or *Complete*, all alarms that use the Alarm Category selected will be acknowledged or completed at once. However, if you select *Respond*, the Alarm Monitor window will display so you can respond to each alarm by entering specific instructions for each particular alarm.

In addition, the shortcut menu allows you to open the Alarm Monitor window or display the alarm details associated with the Alarm Category selected.

Note: You can also place static text objects in the map to indicate for example, the name of an entire area, or a number to dial in case of emergency.

13. To assign events to the item, enter a descriptive event name and select a previous-

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:

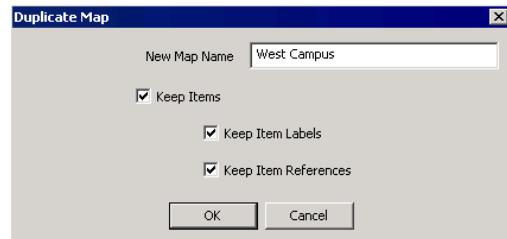
1. From the P2000 Main menu, select **Config>Map Maker**. The Map Maker list box opens.
2. Select the map to which you wish to add a map attachment.
3. Click **Edit**. The Map Editor window opens with the selected map in the image area.
4. Drag a **Map Attachment** icon to the image area. When you release the mouse button, select from the drop-down list the map you wish to attach.
5. 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.

Duplicating Maps

The Duplicate Map feature allows the duplication of existing maps. This feature is useful in buildings where the layout is the same throughout all floors. You can create a master map with default information, and then use that map as a template to create additional maps. All current map information will be copied; however, each map must have a unique name.

To Duplicate a Map:

1. From the P2000 Main menu, select **Config>Map Maker**. The Map Maker list box opens.
2. Select the map you wish to duplicate and click the **Duplicate** button. The Duplicate Map dialog box opens.



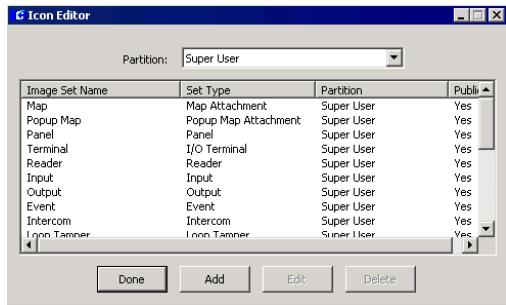
3. Enter the **New Map Name**.
4. Select the **Keep Items** check box if you wish to keep all items from the master map.
5. Select the **Keep Item Labels** check box if you wish to keep the labels from the master map.
6. Select the **Keep Item References** check box if you wish to keep all references from the master map.
7. Click **OK** to create the new map. The Map Editor window opens displaying the selected items. Make any additional changes if necessary.

Adding Image Sets

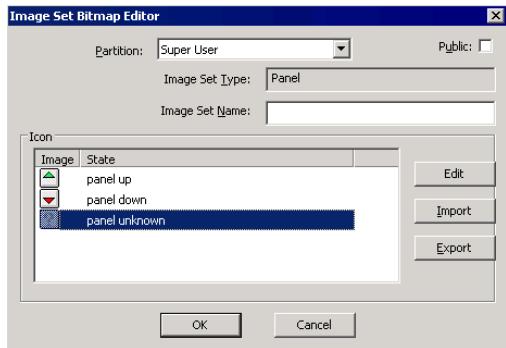
Map Maker provides image sets to display various device states such as “panel up,” “panel down,” “input set,” and so on. However, you can use your own icons to create custom image sets.

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.



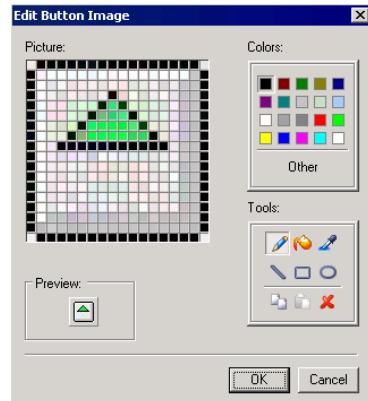
- Click **Add**. The Image Set Bitmap Editor opens.



- 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.

- Select an icon from the list, and use one of the following function buttons:

Edit – The Edit Button Image dialog box opens. Use the editing tools and colors to edit the existing icon. Click **OK** to save.



Import – Select if you wish to replace the existing icon. 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.

Export – Select if you wish to export the existing icon.

- 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.

PRELIMINARY

Chapter 4: Advanced Features

This chapter describes a number of advanced features that, when properly configured and utilized, allow for a more secure and efficient way to operate and monitor your access control system. Some of these features are bundled separately from the P2000 software, and some of them are shipped with their own manuals. Refer to your purchase contract to see what is available in your system. This chapter presents the information you need to set up and configure each of the following features:

- **Partitions** – Divide your P2000 system databases into sections that can be managed individually.
- **Video Imaging** – Improve your security by creating badges to provide a visual identification of every cardholder.
- **MIS Interface** – Add, update, delete, or query the P2000 Cardholder 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** – Provides controls to operate cameras, monitors, and other CCTV elements.
- **DVR** – Provide controls to search, retrieve, and download real-time or archived audio

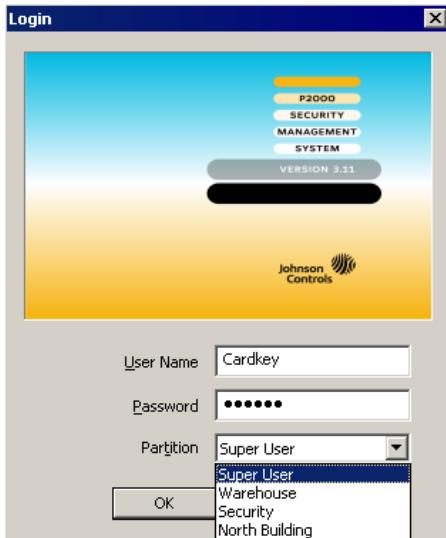
and video recording from surveillance cameras.

- **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 Cardholder/Badge 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 operator, or by a group of operators. 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.

When operators 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 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 Operators, System Devices, Cardholders, 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

Operators 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 operators are defined in the Menu Permission Groups window.

When an operator initially logs on to the P2000 system, the partition chosen during login is the active partition for the operator. After logging on, an operator has the option to access other partitions, assuming they have been given access to other partitions in the Edit Operator dialog box. See “Adding Operators to the System” on page 23.

Any database items created by an operator 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 operators if the database item has the Public check box enabled or the operators have been assigned to the same partition. Operators 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 operators 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. Operators that belong to the Super User partition have access to all other partitions; are responsible for assigning partitions to database operators; and have the ability to add, modify, and delete any items in the database. Super User members are also respon-

sible for performing system maintenance and system configuration functions.

The Super User member can access all system data regardless of partition ownership. Regular partition operators cannot change parameters defined in the Super User partition.

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, operators can be assigned to a specific partition, or to multiple partitions by using the “Assign Operator” window.

Note: If the MIS Interface feature is available in your system, you need database administrative rights in order to add, edit or delete partitions. (See “Setting Up User Accounts” on page 30).

To Create a New Partition:

1. In the System Configuration window, click the **Partitions** root icon.

Note: In Enterprise systems, you can only create partitions at central or alternate sites.

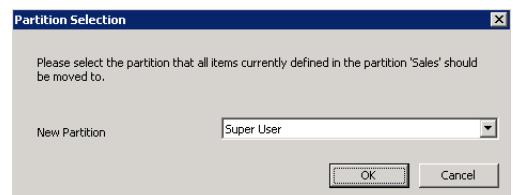
2. Click the **Add** button to access the Partition Edit dialog box.



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. The Partition Selection dialog box opens. Select from the **New Partition** drop-down list, the partition to which all items from the deleted partition will be moved.



4. Click **OK**.
5. At the Confirm Delete dialog box, click **Yes**. All items under the deleted partition will be moved to the new partition.

Note: Deleting a partition may take a considerable amount of time, if records are still associated with the deleted 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 cardholder. 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, cardholder photo-

graphs, 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 *P2000 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**

Video Imaging Specifications

Video Imaging provides a full-featured badge design and imaging solution. The following are Video Imaging specifications:

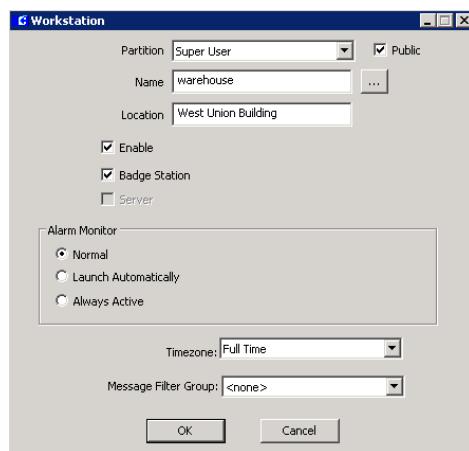
- Integration with the *P2000 Security Management System*. All cardholder records, images, and so forth are stored centrally at the P2000 Server.
- The P2000 workstation with Video Imaging functions as a fully capable P2000 workstation as well as a badging workstation.
- Easy-to-use WYSIWYG (what you 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. 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 **Workstation** root icon and click **Add**. The Workstation dialog box opens.



4. Enter the information required, see “Workstations” on page 21.
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.

- 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:

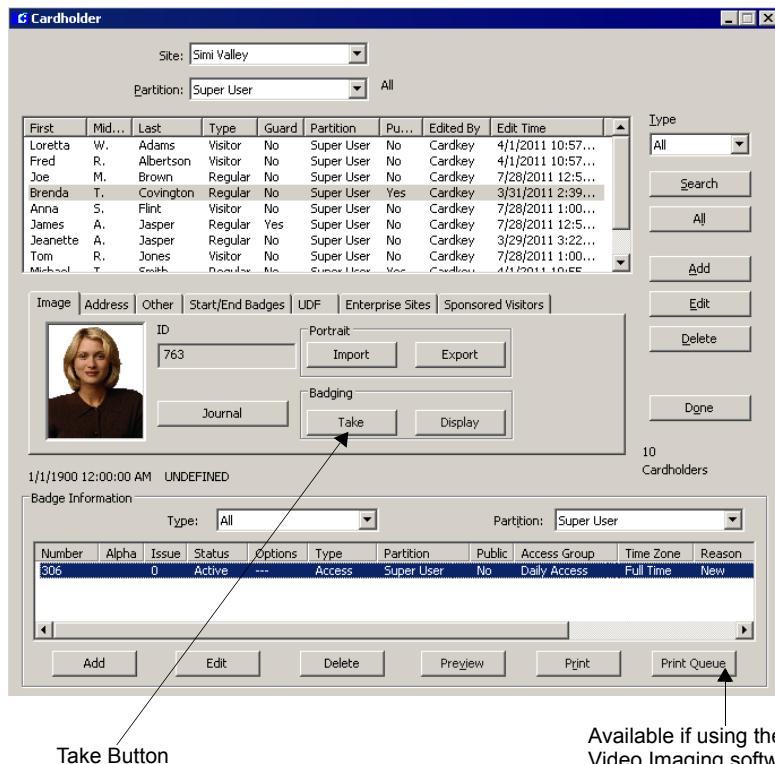
- Creating a cardholder record.** (See “Entering Cardholder Information” on page 230.)
- Assigning the badge to the cardholder.** (See “Entering Badge Information” on page 237.)
- Capturing the portrait and signature images.**

Viewing and printing the badge.

Capturing the Portrait and Signature Images

- From the P2000 Main menu, select **Access>Cardholder**. The Cardholder window opens.
- Select a cardholder from the list.
- Click **Take** 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 *P2000 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 cardholder 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 sign your name.
7. Make the necessary adjustments and accept the signature to assign it to the current cardholder.

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 may take 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:

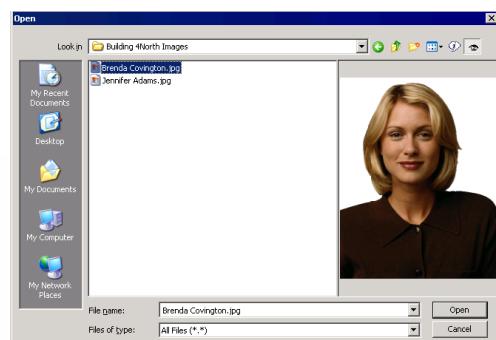
1. Click the **Preview** button at the bottom of the Cardholder dialog box.
2. Your design will display in its own window with all the images you have captured.

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. Then simply click the **Print** button at the bottom of the Cardholder dialog box.

To Import an Image:

1. From the Cardholder window, select a cardholder from the list.
2. Click the **Image** tab. The ID for the cardholder selected displays in the ID field.
3. Under the Portrait box, click **Import**. The system displays a browse screen.



4. 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 Image tab.

Note: Once an image has been placed in the cardholder 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 cardholder information and queries from an external source such as a Human Resource system. Using the MIS Interface Service and an external Open Database Connectivity (ODBC) based program, you can add, modify, or delete cardholders and their badges in the P2000 system, or you can query cardholder 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 (no separate installation media is required).
- ODBC 2.6 or higher (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.

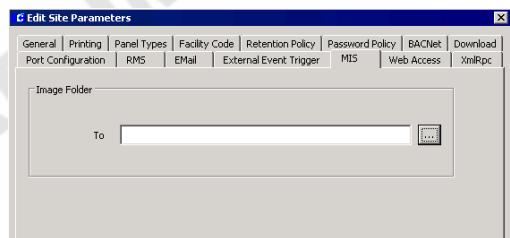
Note: *The external system can be any ODBC-capable application. This system is supplied by the user and is not included in the P2000 software.*

Once the previous components are in place, the following elements must be set up at the P2000 Server:

- The operator assigned to use the MIS Interface must have the MIS account type enabled. To do this, simply select the **MIS** check box in the Edit Operator dialog box, see page 26 for details. We strongly recommend using a separate Operator account for the MIS interface.
- Since passwords cannot be changed for MIS users, you must select the **Password never expires** option in the Edit Operator dialog box, see page 26.
- To add or modify UDFs for use in the MIS interface, the P2000 operator must be a member of the **PEGASYS Administrators** group. This is done by setting up the Windows account of those P2000 operators accordingly, see page 30.
- The **P2000 MIS Interface Service** must be running using the Service Control application, see page 435.
- If you use the **Export Image** command, you must configure the **MIS** tab in Site Parameters to select the location where exported badge images will be stored.

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 command and 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, Query Multiple, Export Images, or Delete Badge). 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 that modify a P2000 record will generate a message in the normal P2000 Audit log.

Partitioned Systems

On P2000 systems that use the Partitioning feature, 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 cardholder database for the first time, entering all cardholder 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 cardholder 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), refer to 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.

Refer to the *P2000 Metasys® 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 contain 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 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.

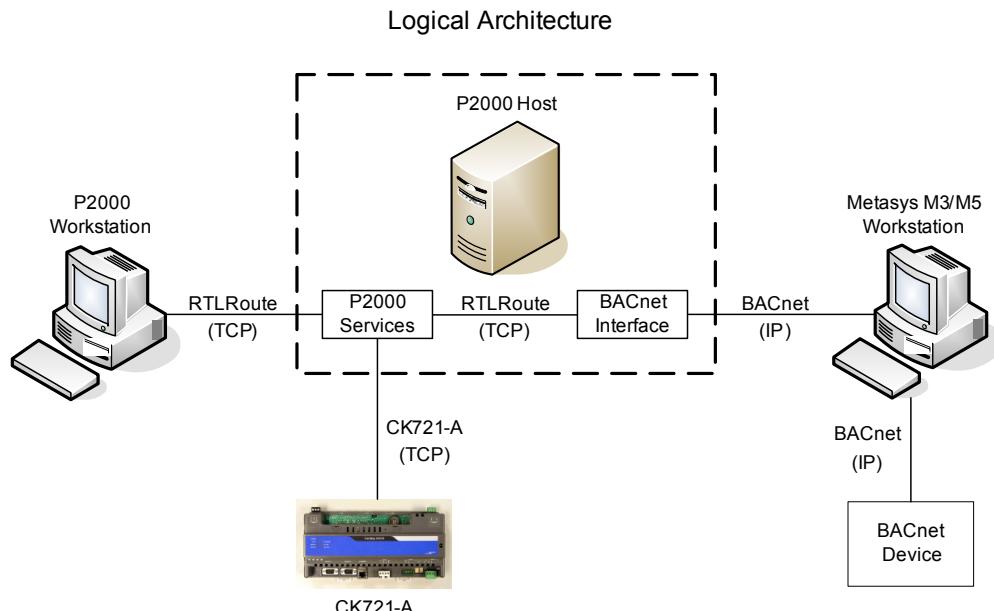
To prevent unauthorized BACnet devices from accessing the P2000 system, the P2000 system will only communicate with those devices that have been configured as allowed BACnet devices in the P2000 database. Communication attempts by other devices over the BACnet interface will cause the P2000 system to 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.

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 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. In order 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)



System Setup

The P2000 software requires the following configuration steps to get its BACnet Interface functional:

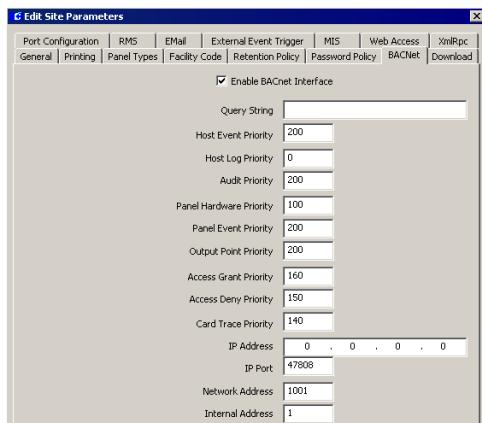
- Set up BACnet site options to define the parameters of the BACnet Interface, see next section.
- Enable the P2000 BACnet Service to automatically start by configuring the Service Startup Configuration, see page 432.
- Add entries to the External IPs application to define the BACnet devices that will communicate with P2000, see page 346.
- Configure the hardware components for BACnet Interface, see page 347.
- Set up BACnet Action Interlocks to initiate actions in BACnet devices, see page 347.

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.

3. Enter the information on each field according to your system requirements. (See BACnet Site Field Definitions for detailed information.)
4. After you have entered all the information, click **OK** to save the settings and return to the System Configuration window. You must stop and restart the BACnet Service.

BACnet Site Field Definitions

Enable BACnet Interface – BACnet settings will only be available after you select this check box.

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 – If the P2000 Server has a single network interface card (NIC), you do not need to enter an IP Address in this field (you may leave the default value of 0.0.0.0). If the P2000 server has more than one NIC, enter the IP Address the P2000 Server will use to receive BACnet broadcast messages over the network.

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.

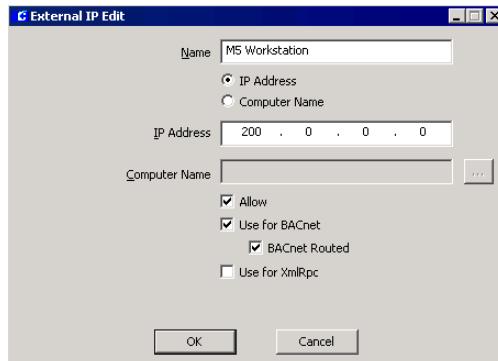
Internal Address – This should only need to be changed if there is another P2000 Server on the same network. If needed, set this value to be unique to every P2000 Server on the network.

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 Source but do **not** select the Allow option.

- Select the **Use for BACnet** check box if this is a BACnet device.
- 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. See “**XmlRpc Tab**” on page 53 for details.
12. Click **OK** to save the settings and return to the System Configuration window.

Configuring Hardware Components for BACnet Interface

When configuring 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 QueryFilterString property of Event Notification messages.

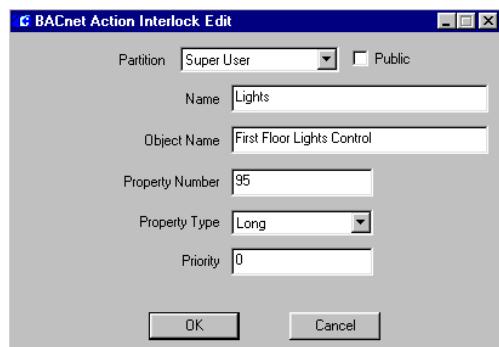
Note: To define panels, terminals, input points, and output points as BACnet objects, see the “General Tab” on page 62.

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 cardholder’s office when they are granted access at a door.

To Set Up BACnet Action Interlocks:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the **BACnet Action Interlocks** icon and click the **Add** button. The BACnet Action Interlock Edit dialog box opens.



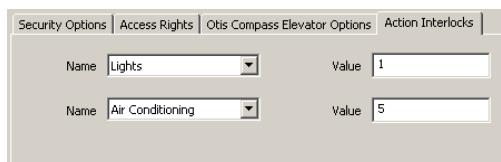
3. If this is a partitioned system, select the **Partition** that will have access to this action interlock information, and select **Public** if you wish the action interlock to be visible to all partitions.
4. Enter a descriptive **Name** of the BACnet Action Interlock.
5. Enter the **Object Name** of the BACnet object to which to write.
6. Enter the **Property Number** of the BACnet property to which to write.
7. From the **Property Type** drop-down list, select the data type of the property.
8. Enter the BACnet **Priority** used when writing the property. If you enter 0, a non-prioritized write will be used.
9. 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 cardholders in the Badge dialog box. The object property defined in the Action Interlock will be written with the value associated with the badge. Each badge 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:

1. From the P2000 Main menu, select **Access>Cardholder** to open the Cardholder window.
2. Select a cardholder from the Cardholder list.
3. In the Badge Information box at the bottom of the window, select the badge to which you wish to assign Action Interlocks and click the **Edit** button.
4. Click the **Action Interlocks** tab. If this is an Enterprise system, see “Define Global Badge Access Rights” on page 408 for additional information when assigning access privileges to Enterprise badges.



5. From the **Name** drop-down list, select the first Action Interlock that will be written when this badge is granted access.
6. Enter the **Value** to write to the first Action Interlock when this badge is granted access. This value will be converted into the correct data type to match the Action Interlock configuration.
7. Select the **Name** of the second Action Interlock that will be written when this badge is granted access.
8. Enter the **Value** to write to the second Action Interlock when this badge is granted access. This value will be converted into the correct data type to match the Action Interlock configuration.
9. When all information is entered, click **OK** to return to the Cardholder window.

M3/M5 Setup

Refer to the *P2000 Metasys® 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 feature 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* 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 100), 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.



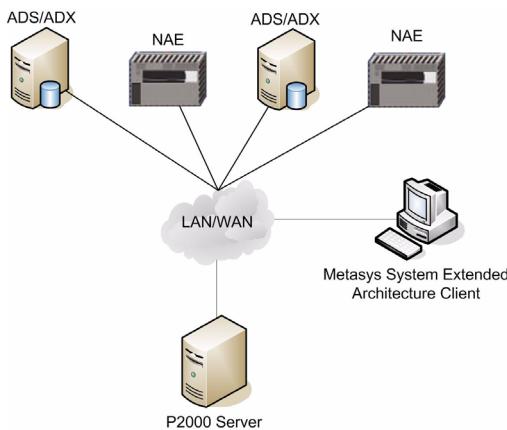
3. Enter an alias **Name** for the Fully Qualified graphic reference name.

4. Enter the **Fully Qualified Name** of the graphic item, as defined by Metasys system extended architecture. Fully Qualified Name entries are case sensitive.
5. Click **OK** to save the MSEA graphic name.

Registering the P2000 Server with a Site Director

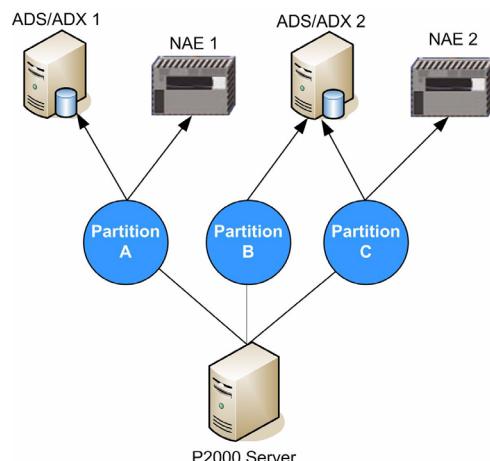
To expose P2000 objects to the Metasys system extended architecture, you must register the P2000 Server with a Metasys Site Director (ADS/ADX server or NAE controller) by adding a MSEA Registration definition in the P2000 Server. P2000 enables you to create multiple MSEA Registration definitions, so you can register the P2000 Server with multiple Site Directors.

Note: If using an NAE controller as the Site Director, contact Johnson Controls Technical Support for assistance.



IMPORTANT: 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).

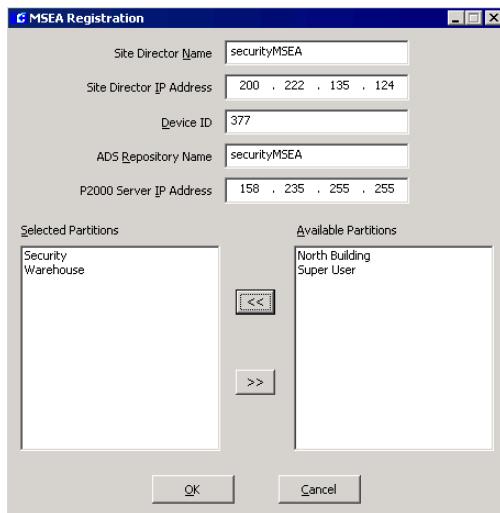


In the example above, the P2000 objects associated with Partition A will only be visible from ADS/ADX 1 and NAE 1; the P2000 objects associated with Partition B will only be visible from ADS/ADX 2; and the P2000 objects associated with Partition C will only be visible from ADS/ADX 2 and NAE 2.

Note: The partition rule previously described has the following exceptions: 1) If you register the **Super User** partition to a particular Site Director, P2000 objects will be visible from **all** partitions, even from those that were not registered with the Site Director. 2) Any P2000 device, such as a panel or terminal, set to **Public** will be visible from all partitions, regardless of the ones registered to a particular Site Director.

To Register a P2000 Server with one or more Site Directors:

- From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
- Click the **MSEA Registrations** icon and click **Add**. The MSEA Registration dialog box opens.



- Enter the **Site Director Name** where the Site Director is installed (the server name of the ADS/ADX or the name of the NAE).
- 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).
- Enter the **Device ID**. If the P2000 system interfaces with Metasys system extended architecture Release 2.1 or earlier, contact Johnson Controls Technical Support for assistance. 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.

- Enter the **ADS Repository Name** (computer name) of the Metasys ADS Repository.

Note: The ADS Repository stores messages forwarded by the P2000 system; however, an NAE device used as a Site Director cannot store these messages. If you have an 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.

- Enter the **P2000 Server IP Address**.
- 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.
- Click **OK** to save the MSEA Registration.
- Repeat the previous steps for each Site Director with which you wish to register the P2000 Server.
- To complete the P2000 MSEA Registration, you must stop and restart the **P2000 XmlRpc Interface Service**. For details, see “Starting and Stopping Service Control” on page 349.

The P2000 Server 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 your facility uses the Guard Tour feature, 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. See “Starting and Stopping Service Control” on page 435.

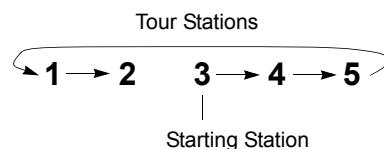
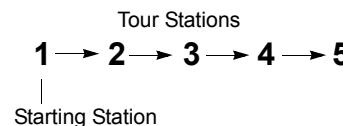
Basic Principles and Definitions

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.

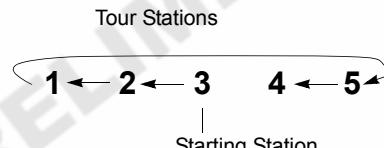
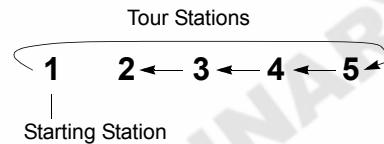
Forward – The expected sequence the tour will take place. Beginning with the starting check-in station, the tour will progress sequentially through all stations in a forward direction. The starting tour station can be selected automatically or manually.

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 – A 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 operator.

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) an operator manually aborts a tour.

Sequence of Steps

The basic procedure for defining and implementing Guard Tours are:

- Define system hardware
- Define cardholders and assign Tour Badges to the appropriate personnel
- Configure Guard Tours
- Define Tour Stations
- Control and manipulate Guard Tour activities
- Generate Guard Tour Reports

Steps to perform each procedure are presented in the following sections.

Defining System Hardware for Guard Tour Operation

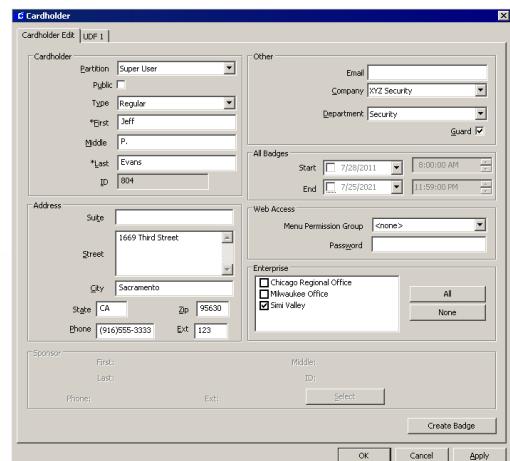
Prior to defining Guard Tours you must properly configure the system hardware and its components; specifically, the readers and inputs points you intend to use in defining tours. If this has not been completed, some of the functions described in this section will not be ready to operate. See *Chapter 2: Configuring the System* for details.

Assigning Tour Badges

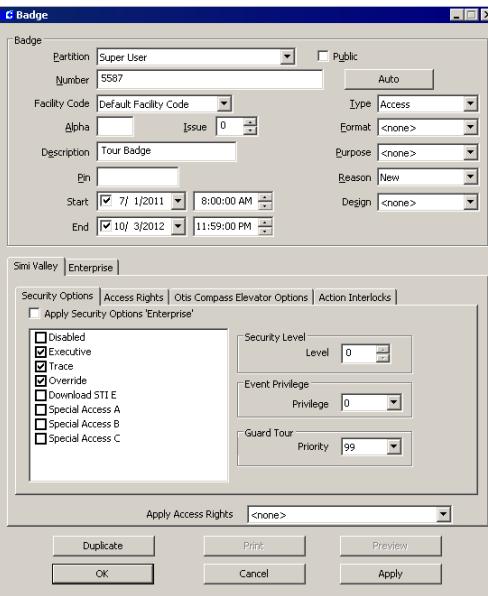
The main purpose of a tour is to ensure and record that an area has been physically visited. While a guard may check-in at a reader defined in a Guard Tour as a station, access through that reader-controlled door may or may not be desired. Use the following instructions to assign badges to cardholders who will participate in guard tour operations.

To Assign a Tour Badge to a Cardholder:

1. From the P2000 Main menu, select **Access>Cardholder**. The Cardholder window opens.
2. Create a new record or edit an existing cardholder as desired. For details, see “Entering Cardholder Information” on page 230.



3. In the Other box, select the **Guard** check box to assign a Tour Badge to the selected cardholder. This will be reflected in the Guard column of the Cardholder window.
4. Click the **Create Badge** button at the bottom of the window. The Badge dialog box opens.



5. Enter the badge number and optional description. For detailed information, see “Entering Badge Information” on page 237.
6. Click the **Security Options** tab. If this is an Enterprise system, see “Define Global Badge Access Rights” on page 408 for additional information when assigning access privileges to Enterprise badges.
7. In the Guard Tour box, assign a **Priority** to the Tour Badge.

**APPLICATION NOTE**

Guard Tour Priority: When you define a Guard Tour, it is assigned a priority number from 1 to 99. In the cardholder badge record, the Tour Priority determines which tours the selected cardholder can perform. These can be all defined tours with a priority less than or equal to the badge's assigned Tour Priority. For example, a cardholder badge with Tour Priority 45 is authorized to complete tours with a priority of 1 through 45. If the cardholder badge is used to attempt to check-in at stations of a tour defined as priority 46, their badgings will be ignored by the Guard Tour.

8. After adding the Tour Badge, click **OK** to return to the Cardholder 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 cardholders.

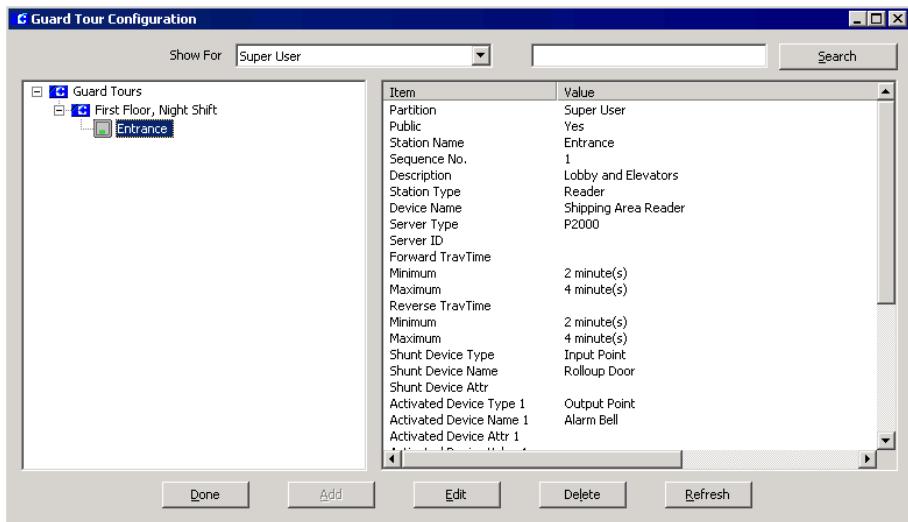
Using the Guard Tour Configuration Window

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.

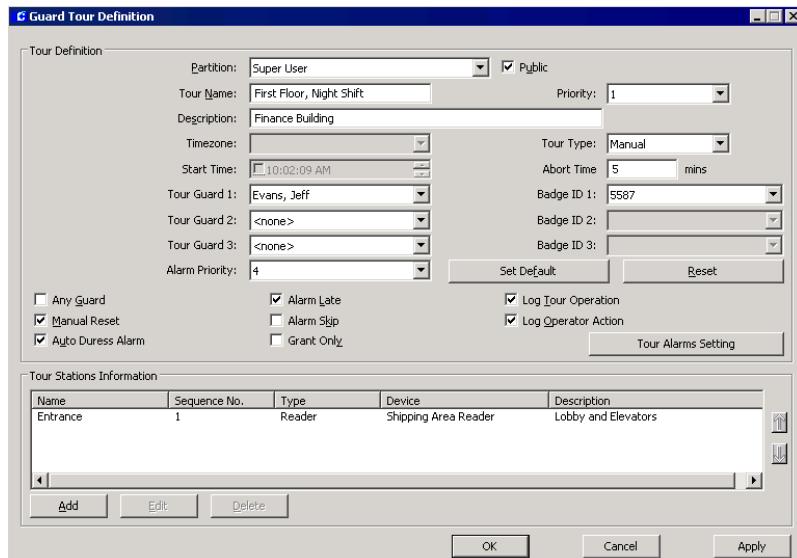
Click the **Search** button. The window will display the match entered in the search field. Continue clicking **Search** until you find the item you are looking for.



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 361.

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. See “Time Zones” on page 55 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.

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 (hours and minutes only) 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.

Note: A tour is automatically aborted only if there are no tour alarms or the Manual Reset option is not enabled.

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 cardholders with the Guard option enabled in the Cardholder Edit dialog box 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. If you wish 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. See “Additional Guard Tour Options” below 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 – If selected, all operator actions, such as starting or aborting a tour will be logged as events.

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 104.

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.

3. 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:

1. 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.
2. 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

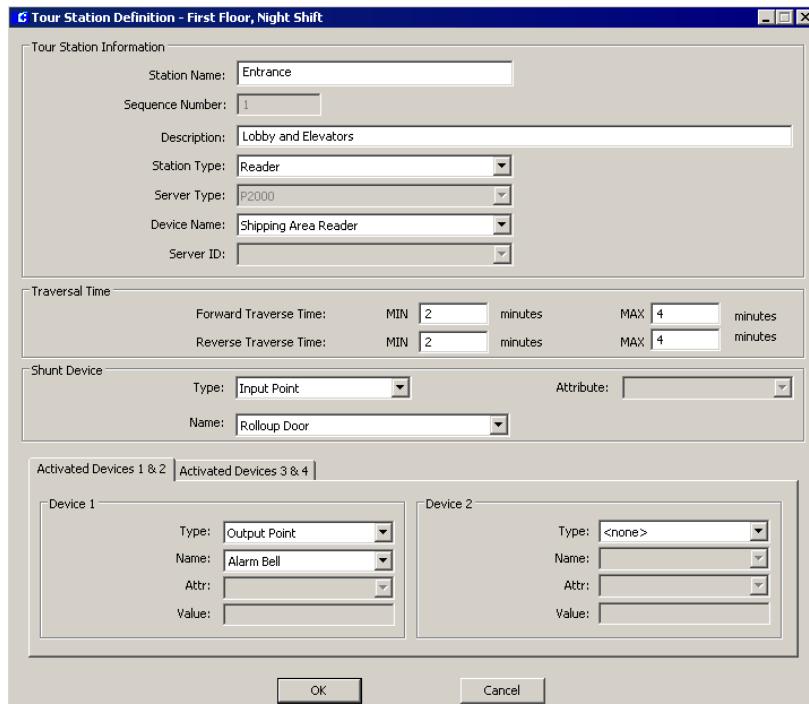
Tour Definition dialog box shows the stations assigned to this tour in sequence. You can change the sequence of the stations by clicking the **Up** or **Down** arrows in the Tour Stations Information list box, to change the sequence of the selected station.

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.

Server Type – This field is not currently used in this version of the P2000 software.

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 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

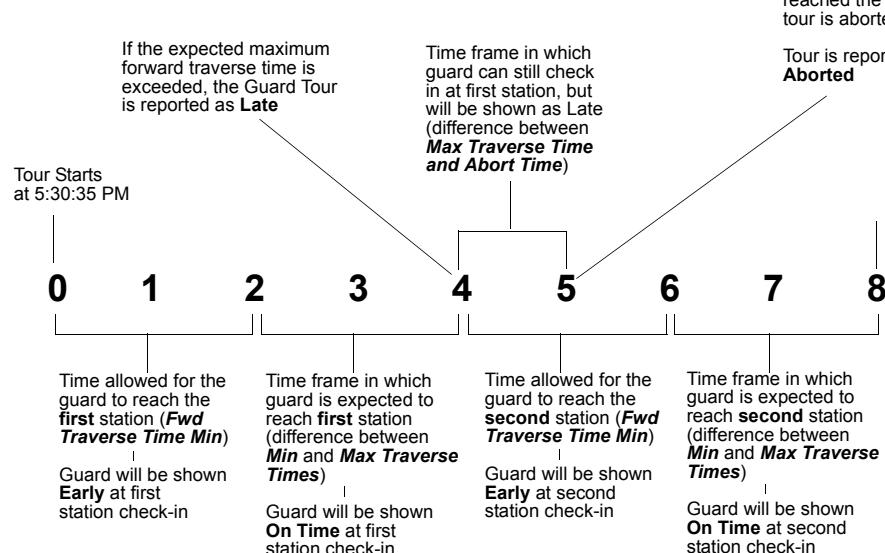
- Completed
- Idle

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 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.

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



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.

If you wish 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.

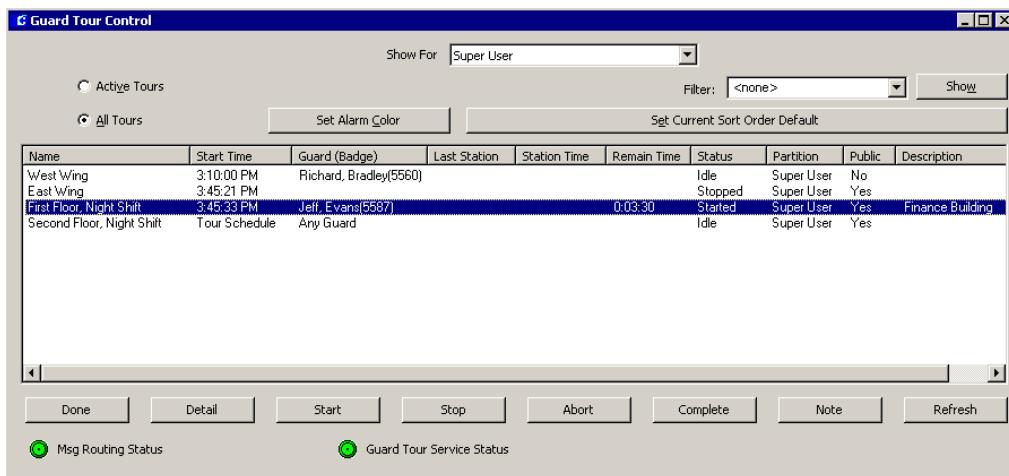
Continue to add stations as necessary. When finished, click **OK** to return to the Guard Tour Configuration window. The Guard Tour will be written to the database.

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 if you wish 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 if you wish to display all tours currently in the database, for the partition selected, regardless of their state.



- Click the **Set Alarm Color** button if you wish 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.
- If you wish 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.

- To display all Guard Tours again (Active or All), select <none> from the Filter drop-down list.
- 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 ID.

Last Station – Displays the name 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.

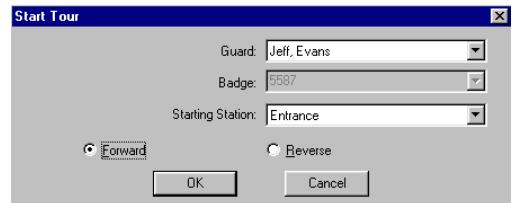
Description – Displays the description of the tour, as configured in the Guard Tour Definition dialog box.

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 Timezone 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 – If you wish 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.

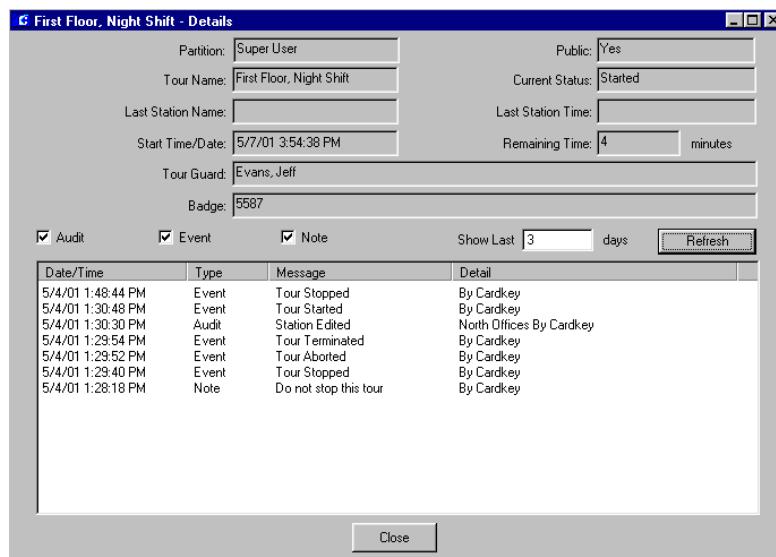
Guard Tour Details

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.
5. Enable the **Note** box to display all Notes related to this tour. See the following section “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.

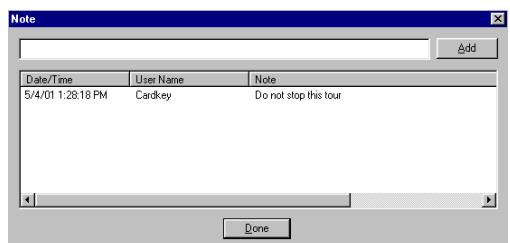
1. From the System Configuration window select **Site Parameters** and click **Edit**. The Edit Site Parameters dialog box opens at the General tab.
2. Click the **Retention Policy** tab and enter the amount of time and select Minutes, Hours, or Days from the **Tour Note** drop-down list, after which all notes will be deleted from the system.

Setting	Value	Unit
Audit Trail	30	Days
Transactions	30	Days
Alarms	30	Days
Muster Data	30	Days
Request Queue	30	Days
Tour Note	30	Days

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. See “Using the Real Time List” on page 322 for more information.

If you wish 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. See “Printing Tab” on page 41 for more information.

Guard Tour Reports

Guard Tour reports are provided as a subset of the standard P2000 report set. For detailed information on running reports, see *Chapter 6: System Reports*.

Three types of Guard Tour reports are provided: Tour Configuration, Tour Transaction History, and Tour Notes. The following sections describe each of these reports.

Tour Configuration Report

The Tour Configuration report lists by tour name, all tour definition configuration, and associated stations, as set up in the Guard Tour Definition window. When you select **Tour Configuration** from the Run Report window, the Tour Configuration dialog box opens. You can select a **Tour Name** from the drop-down list to limit the report to a specific tour or leave the default (*) to report on all tours configured in the system.

Tour Transaction History Report

This report lists every guard tour transaction in the system, or can be filtered to list by specific Partition, Tour Name, Transaction Type, specific Dates and Times, and any combination of these. In addition, you can select to run the report on transactions at your local site or you can enter the name of the remote site that you want to report on.

When you select **Tour Transaction History** from the Run Report window, the Tour Transaction History dialog box opens. Select either your local **Site** or enter the name of the remote site that you want to report on. The default (*) reports all tours in the system, or you can select a specific **Partition**, **Tour Name**, and **Transaction Type** from the drop-down lists. After you select a **Begin** and **End** Date and Time for the transactions you wish to see, the Tour Transaction History report displays in the Crystal preview window. The top of the report shows the Tour Name, Transaction Type and Site, and the date and time settings selected. Each transaction is listed as a separate date and time stamped record.

Tour Notes Report

This report lists all the tour notes assigned to a specific tour name, as set up in the Guard Tour Control window, or can be filtered to list by specific Tour Name, specific Dates and Times, and any combination of these. When you select **Tour Notes** from the Run Report window, the Tour Notes dialog box opens. The default (*) reports all tours in the system, or you can select a specific **Tour Name** from the drop-down list. After you select a **Begin** and **End** Date and Time for the notes you wish to see, the Tour Notes report displays in the Crystal preview window. The top of the report shows the date and time settings for the report and the Tour Name selected. Each note is listed as a separate date and time stamped record.

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:

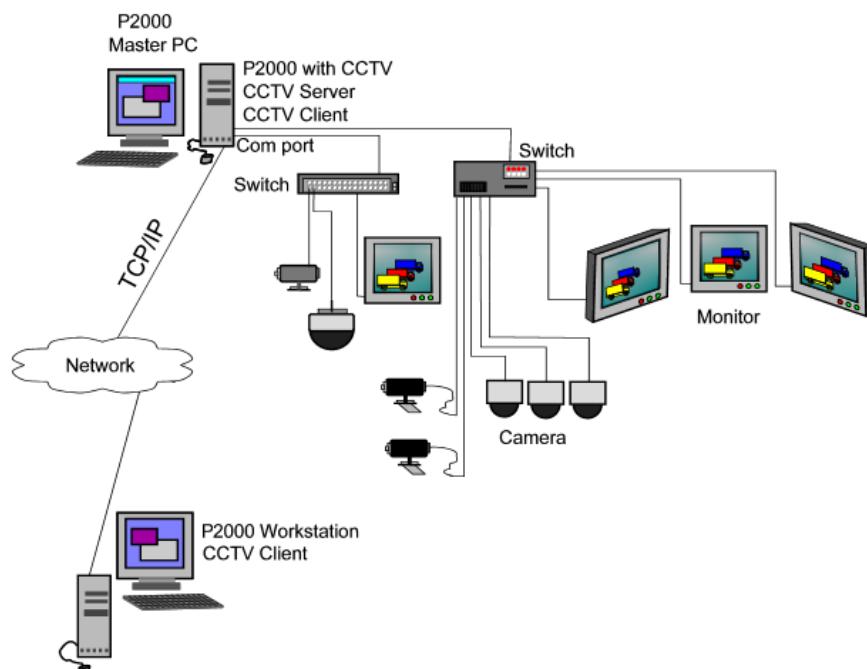
- Place a Camera on a Monitor
- Run a Sequence on a Monitor
- Pan, tilt, zoom; focus and control iris functions; and switch on wipers, washers, and lights for a given Camera
- Run Tours and Macros
- Run Patterns and Presets, and use Auxiliaries

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 feature, see *Appendix D: CCTV Switch Protocols*.

The following diagram illustrates the possible configurations of the CCTV system equipment. The software provided by the CCTV feature 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, refer to the *P2000 Server/Workstation Software Installation Manual*.

If your facility uses the CCTV feature, the CCTV communication service (CCTV Server) will start automatically when you start the PC.



Using P2000 functions with the CCTV Feature

The CCTV feature 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.

Menu Permissions – Create and assign menu permissions 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, see the appropriate sections later in this chapter and also “Creating Actions” on page 317.

Audit Trail – Changes to the database are listed in the audit trail. You can use the standard P2000 Audit report for details.

Reports – The CCTV feature provides a number of standard reports. Details are given at the end of the section. For full details about the standard P2000 reports, see *Chapter 6: System Reports*.

CCTV Configuration Overview

To operate your Johnson Controls CCTV System, the CCTV feature 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 feature on a daily basis, the System Engineer will need some specific knowledge of the CCTV equipment in order 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, refer to 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. If you wish 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 435.

Defining System Hardware for the CCTV Feature

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.

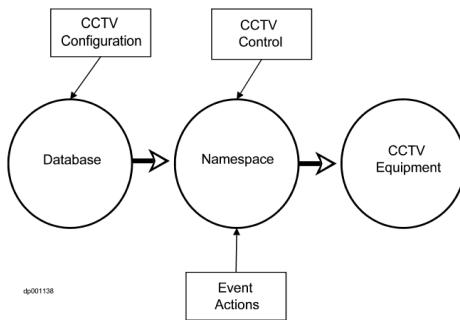
Similarly, the Camera configuration will define global information about the Auxiliaries, Presets and Patterns for the Camera, including the number of these items that are to be generated in the namespace. If the Camera definition generates 20 Patterns for example, then the 20 Patterns will exist in 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, in order 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, in order 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; see *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 Components

Components that operate within the CCTV feature 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 feature. 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.

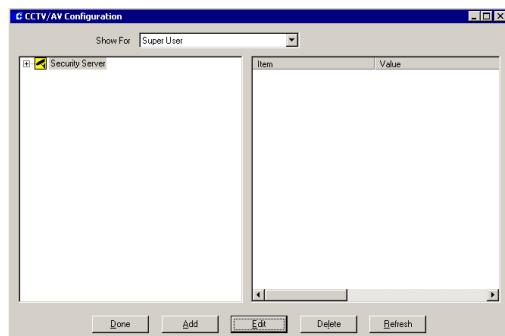
Monitors – You may specifically define the Monitors that you will use on your system and the Sequences that can be played for each Monitor.

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 Feature:

- From the P2000 Main menu, select **Options>CCTV/AV>Configuration**. The CCTV/AV Configuration window opens.



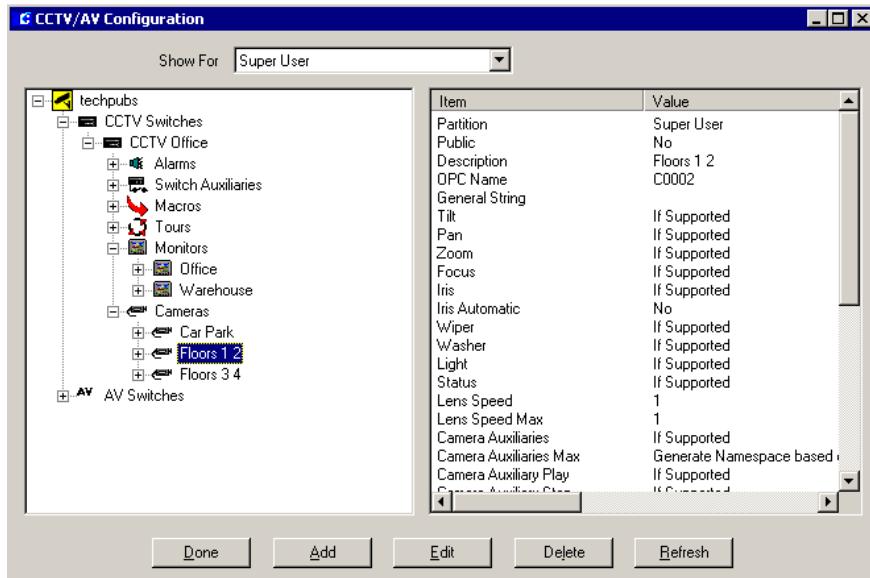
IMPORTANT: For any CCTV configuration changes to take effect, the CCTV Server must be stopped and restarted. This should be done on the completion of your configuration session.

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. See “CCTV Naming Conventions” on page 371 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

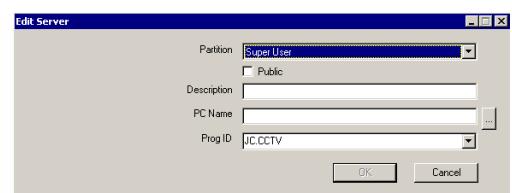
The CCTV Server will create and maintain (in RAM) a namespace, which is made available to all CCTV Controls and other OPC Clients. The namespace contains abstract descriptions of the equipment controlled by the Server. CCTV Controls query the namespace to find out what and how much equipment is available. In order 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.

Note: *The CCTV Server must be set to Public if you wish to assign a CCTV Switch or AV Switch in a different partition.*

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.

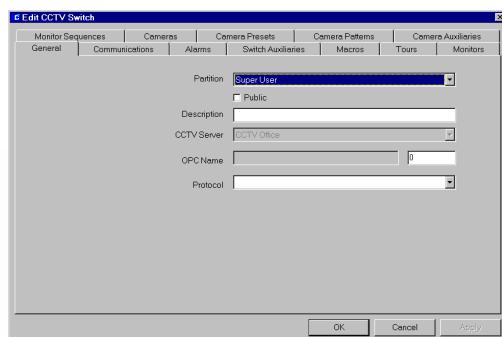
Create and Configure Switches

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 would have no effect. The system does not check whether the functions selected at the Switch are compatible with the functionality of the equipment.

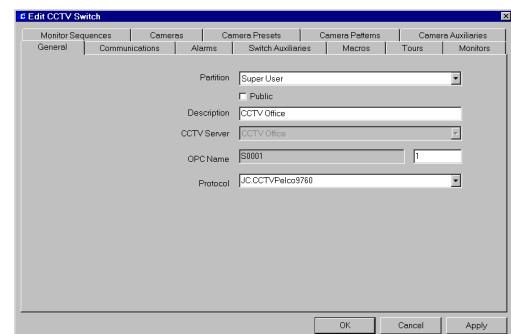
You should also note that if you set up global items under the Switch and then create a specific CCTV item (for example a Camera) then the settings defined for the individual item override the global Switch settings.

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.

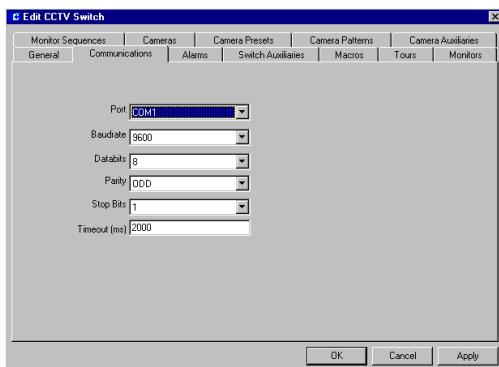
Public – If partitioning is available, select the Public check box to allow all partitions to see this Switch.

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 to which the Switch is physically connected. 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 371.

Protocol – This is the CCTV Switch Protocol for this make and model of Switch. For information about the Protocol, see “Switch Protocols” on page 373 and *Appendix D: CCTV Switch Protocols*.

CCTV Switch Communications Tab

The manufacturer of the Switch will specify the information entered into the Communications tab. You should refer to the manufacturer's documentation.

Port – This is the COM port to which the Switch is physically connected. 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.

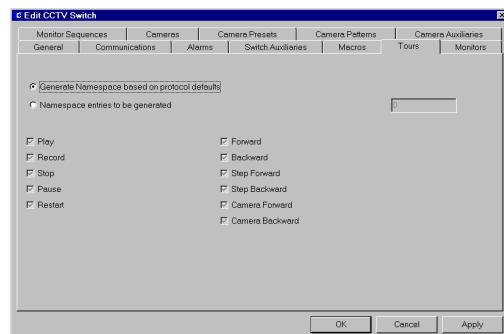
Baud – This is the Baud for the Switch communications.

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 372.

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 372.

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 (see page 373 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 equip-

ment 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

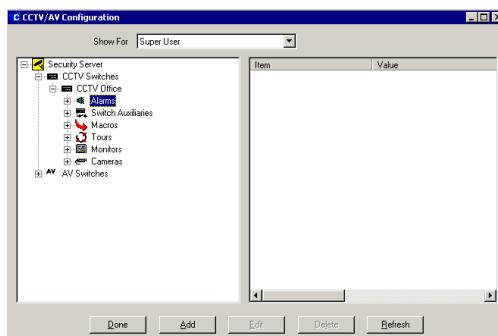
Macros are programmed sets of steps that are to be performed. The program steps can include any function provided by the associated Switch.

Tours

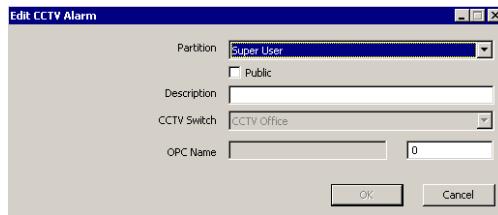
A Tour is a programmed set of Camera, Monitor, and Preset movements. The functionality of the Tour will depend on the capability of the equipment connected to the Switch.

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.



3. 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 to which the item is connected. 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 371.

Monitors

Create and Configure Monitors

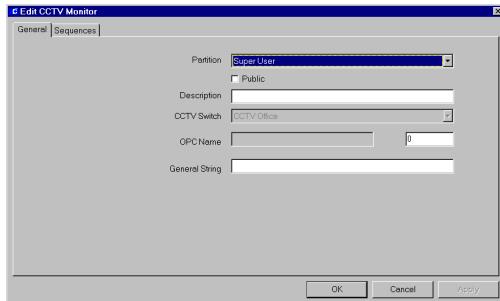
A Switch will have a variety of equipment physically connected to it, including Cameras, Monitors and Auxiliaries.

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. See “CCTV Naming Conventions” on page 371 for more information.

To Add a Named Monitor:

- From the CCTV/AV Configuration window, click the **CCTV Switch** icon with which the Monitor is associated. Click the + to open the items for the Switch.
- Click the **Monitor** icon and click **Add**. The Edit CCTV Monitor dialog box opens.



- Fill in the information for each field in each of the tabs 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.

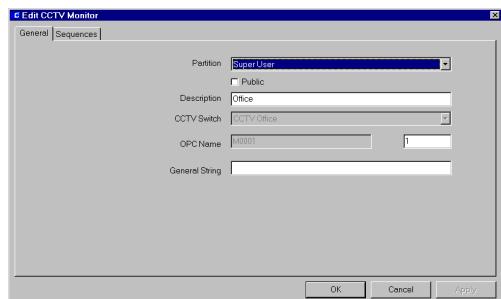
Edit CCTV Monitor Tabs

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.

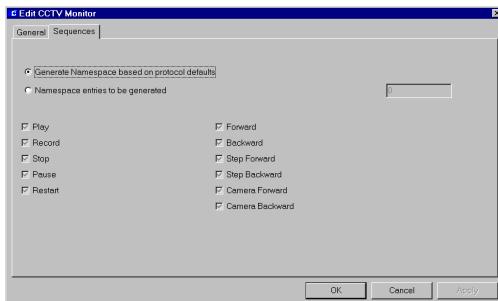
Description – This is the user defined name of the Monitor. The name will display in the CCTV Control window.

CCTV Switch – This is the name of the Switch to which the Monitor is physically connected. 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 371.

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 372.

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 372.

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:

1. From the CCTV/AV Configuration window, click the **CCTV Switch** icon with which the Monitor is associated. Click the + to open the items for the Switch.
2. Click the + to open the items for the Monitor.
3. Click the **Sequence** icon and click **Add**. The Edit CCTV Sequence dialog box opens.



4. Fill in the information for each field according to the "Edit CCTV Sequence Field Definitions".
5. 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 to which the Sequence is connected. 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 371.

Cameras

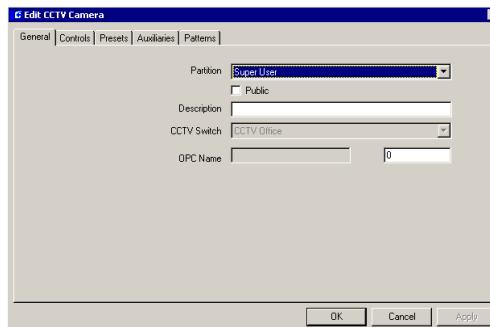
Create and Configure Cameras

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. See "CCTV Naming Conventions" on page 371 for more information.

To Add a Named Camera:

- From the CCTV/AV Configuration window, click the **CCTV Switch** icon with which the Camera is associated. 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.

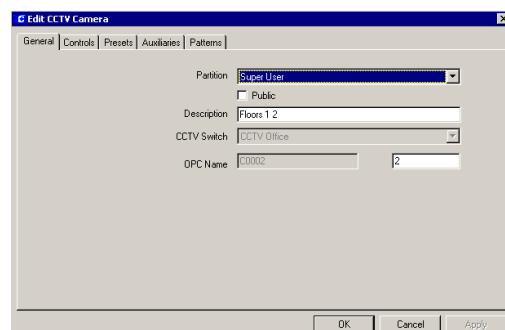
Edit CCTV Camera Tabs

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.

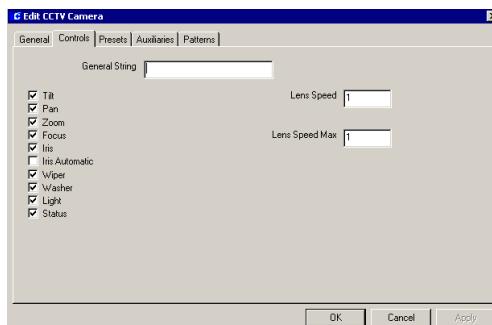
Description – This is the user defined name of the Camera. The name will display in the CCTV Control window.

CCTV Switch – This is the name of the Switch to which the Camera is physically connected. 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 371.

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.

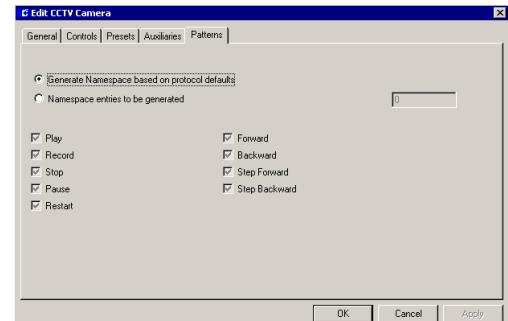
Wiper – If available, tick the check box to enable Wiper for this Camera.

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 372.

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 372.

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 with which the Camera is associated. 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 to which the item is connected. The Camera name is automatically entered into this field.

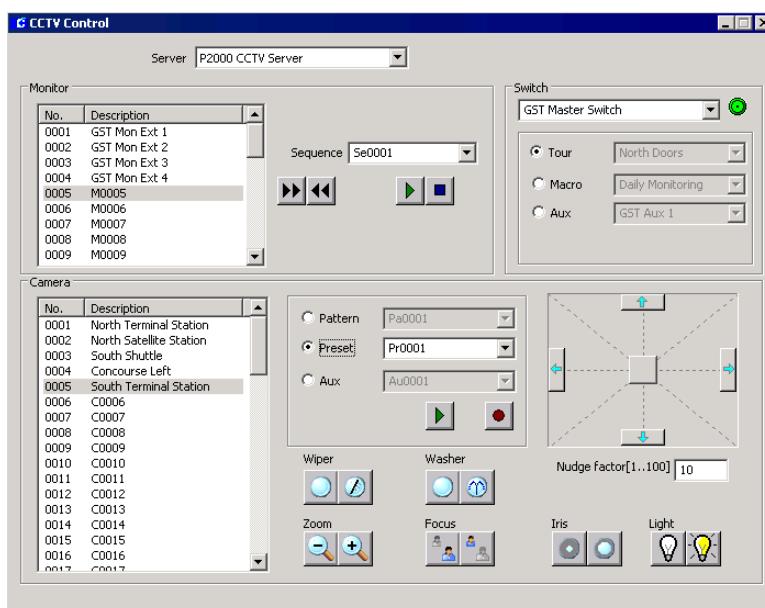
OPC Name – Enter the number of the item. The number is automatically appended to the prefix letter and added to the OPC Name field. For further information about namespace names and item numbers, see “Naming Items for the CCTV Server Namespace” on page 371.

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 CCTV Control:

1. From the P2000 Main menu, select **Options>CCTV/AV>Control**. The CCTV Control dialog box opens.
2. If you have multiple servers, select a **Server** from the drop-down list. The Server to select will depend on the configuration of your system and the number of Servers that are installed.



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 in order 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



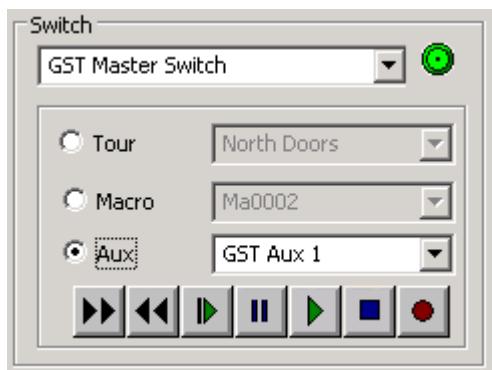
Focus



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.

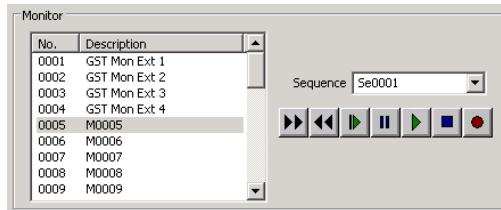
Stop – This will stop the selected Tour, Macro or Switch Auxiliary. With some equipment the stop button may also stop recording a Tour or Macro.

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.

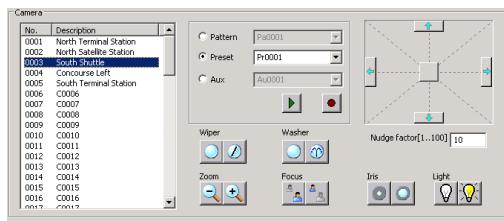
Play – This will activate the selected Sequence.

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 383. You would need to stop the CCTV service and start it again for the named item to be available in CCTV Control.

CCTV Event Actions

CCTV Event Actions are a category of the standard P2000 event action dialog box. If your facility uses the CCTV feature, 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*.

IMPORTANT: 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 317 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, see *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, see *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.

CCTV Reports

CCTV reports are provided as a subset of the standard P2000 report set. For detailed information on running reports, see *Chapter 6: System Reports*.

Four types of CCTV reports are available: CCTV Switch, CCTV Monitor, CCTV Camera, and CCTV Summary. The following sections describe each of these reports.

CCTV Switch Report

The CCTV Switch report lists by name all Switches specifically configured in the CCTV/AV Configuration window. When you select **CCTV Switch** from the Run Report window, the CCTV Switch dialog box opens. You can select a **Server Name** and/or a **Switch Name** from the drop-down lists to limit the report to specific Switches or leave the default (*) to report on all switches defined for all servers.

CCTV Monitor Report

The CCTV Monitor report lists by name all Monitors specifically configured in the CCTV/AV Configuration window. When you select **CCTV Monitor** from the Run Report window, the CCTV Monitor dialog box opens. You can select a **Server Name** and/or a **Switch Name** from the drop-down lists to limit the report to Monitors associated with a specific Switch or Server, or leave the default (*) to report on all Monitors defined for all switches and servers.

CCTV Camera Report

The CCTV Camera report lists by name all Cameras specifically configured in the CCTV/AV Configuration window. When you select **CCTV Camera** from the Run Report window, the CCTV Camera dialog box opens. You can select a **Server Name** and/or a **Switch Name** from the drop-down lists to limit the report to Cameras associated with a specific Switch or Server, or leave the default (*) to report on all Cameras defined for all switches and servers.

CCTV Summary Report

The CCTV Summary report lists by name all items defined in the CCTV/AV Configuration window. When you select **CCTV Summary** from the Run Report window, the CCTV Summary dialog box opens. You can select a **Server Name** and/or a **Switch Name** from the drop-down lists to limit the report to items associated with a specific Switch or Server, or leave the default (*) to report on all items defined for all switches and servers.

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, and DVR ID. Live video and audio playback options are available from the Alarm Monitor, Real Time List, and Real Time Map.

The DVR system communicates with the P2000 Server via a TCP/IP connection. The communication is provided by the P2000 CCTV Server, a software component installed automatically with the DVR option.

Additionally, the DVR feature 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* 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.

IMPORTANT: *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 software.*

Contact your sales representative for more detailed information.

FDA Part 11

The P2000 software provides change tracking parameters 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 CFR 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 cardholder records are changed, and more. A complete list of P2000 Standard Reports is presented in “P2000 Standard Report Definitions” on page 466, 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. See “Assigning Operators” on page 25 for detail instructions on adding operators to the system. In addition, the “Password Policy Tab” on page 47 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. See “System Validation” on page 458 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. See “P2000 Standard Report Definitions” on page 466 for a complete list of P2000 Standard Reports.

Record Retention – Through software configuration, a system administrator can define parameters to back up and retrieve records to ensure the availability of all records for a specified period of time. See “Retention Policy Tab” on page 46 to enforce FDA Part 11 record retention policy. Also, “FDA Part 11 Backups” on page 455 provide instructions to perform periodic backups to comply with FDA Part 11 record retention requirements.

Intercom

The P2000 Intercom interface allows the P2000 server to retrieve messages coming from approved intercom equipment and use them for event processing and distribution to P2000 workstations for the processing of intercom history messages and alarms. The P2000 Intercom Interface Service that resides on the P2000 server provides the communication between the P2000 system and the intercom equipment. This interface enables audio communication links between any two or more defined intercom stations.

The P2000 system provides applications to control and display all intercom call requests coming from defined intercom stations. The operator can select a call request from the list and connect to any single intercom station or to a group of stations.

The P2000 system supports two intercom integrations: *Zenitel AlphaCom* and *Commend* (GE300, GE800, and any Commend intercom model compatible with the ICX Protocol Version 1.1/0910) systems. Complete intercom hardware installation and operation instructions are provided with the intercom system that was shipped with your option.

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.

For Zenitel AlphaCom systems 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.

For Command systems ensure that:

- The Intercom Server is defined using the Command system software, including connection settings and other system parameters. Refer to the manufacturer's documentation for assistance.
- If your intercom system will support output setting, use the Command system software to configure these outputs, and then add them to the intercom exchange and/or station definition.
- The Command Intercom Server is licensed and configured to use a TCP/IP channel.
- You have configured at least two stations that will communicate with each other.

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 intercom system.

If you use Partitions, you can assign the intercom stations 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.

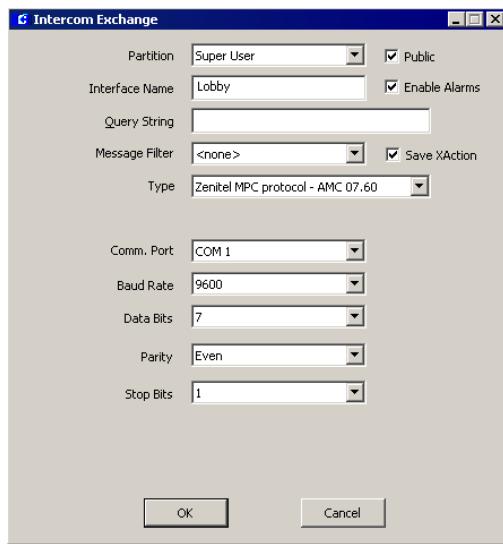
IMPORTANT: *For any intercom configuration changes to take effect, you must stop and restart the P2000 Intercom Interface Service using Service Control, see "Starting and Stopping Service Control" on page 435.*

Intercom Exchange

Each P2000 workstation acting as an intercom Master Station must be associated with a specific Intercom Exchange. You can link each intercom exchange to extend the number of intercom stations controlled by a single master intercom station.

To Define a Zenitel 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 Interface** 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 **Interface Name** to identify the intercom exchange to which the stations are connected.

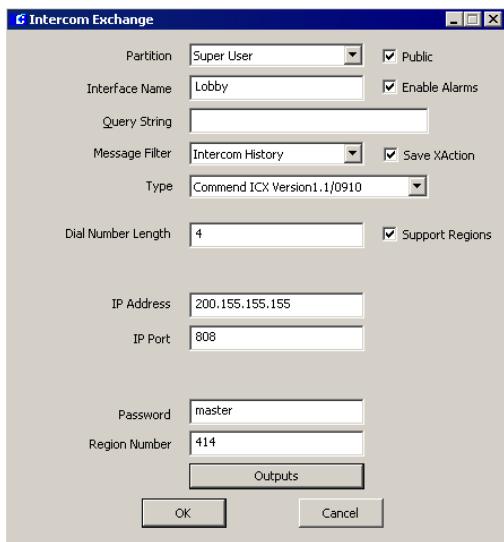
Note: Configuration settings defined for Intercom Exchanges and Intercom Stations must match the settings defined at the intercom equipment. If the programming at the intercom equipment changes, you will have to make the corresponding changes in the P2000 intercom configuration (Exchanges and/or Stations).

6. Select the **Enable Alarms** check box, if you wish to report all alarms generated by the intercom equipment. The P2000 Alarm Monitor will display alarms associated with the Zenitel Exchange, such as *Connect* and *Disconnect*.
7. Enter the **Query String** value that is used with message filtering (see “Define Query String Filters” on page 211).
8. Select the **Message Filter Group** that contains the intercom history messages that will be saved in the P2000 Transaction History database. Select **<none>** if you wish to save all intercom history messages.
9. To save the intercom history messages in the P2000 Transaction History database, you must select the **SaveXAction** check box. For more information, see “Intercom Transaction History Reports” on page 404.
10. Select from the **Type** drop-down list, the Zenitel intercom protocol to be used at your facility.
11. Select from the **Comm. Port** drop-down list, the P2000 Server port to which the Intercom Exchange box is connected.
12. The values for the **Baud Rate**, **Data Bits**, **Parity**, and **Stop Bits** should be set to match the settings in the Zenitel intercom hardware settings. Edit the settings if necessary.
13. Click **OK** to save your settings. The Intercom Exchange name displays under the Intercom Interface icon in the System Configuration window.

To Define a Command Intercom Exchange:

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

- Click the **Intercom Interface** icon and click **Add**. The Intercom Exchange dialog box opens.



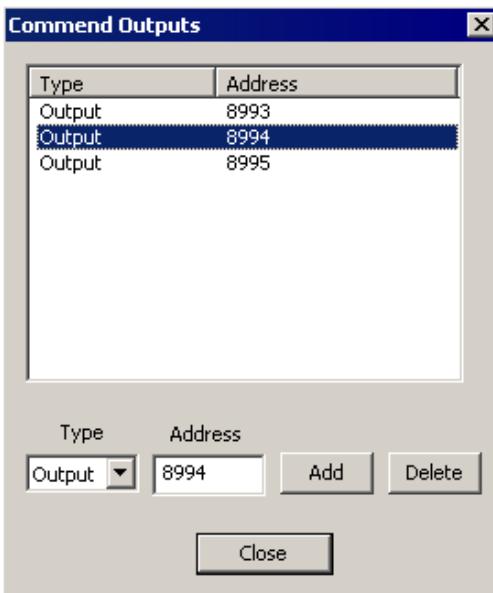
- If this is a partitioned system, select the **Partition** in which this intercom exchange will be active.
- Select the **Public** check box if you wish this intercom exchange to be visible to all partitions.
- Enter a descriptive **Exchange Name** to identify the intercom exchange box to which the stations are connected.

Note: Configuration settings defined for Intercom Exchanges and Intercom Stations must match the settings defined at the intercom equipment. If the programming at the intercom equipment changes, you will have to make the corresponding changes in the P2000 intercom configuration (Exchanges and/or Stations).

- Select the **Enable Alarms** check box, if you wish to report all alarms generated by the intercom equipment. The P2000 Alarm Monitor will display alarms associated

with the Command Exchange, such as *Connect* and *Disconnect*; and alarms associated with Command stations, such as *Station Alarm Set* and *Station Alarm Reset*.

- Enter the **Query String** value that is used with message filtering (see “Define Query String Filters” on page 211).
- Select the **Message Filter Group** that contains the intercom history messages that will be saved in the P2000 Transaction History database. Select <none> if you wish to save all intercom history messages.
- To save the intercom history messages in the P2000 Transaction History database, you must select the **SaveXAction** check box. For more information, see “Intercom Transaction History Reports” on page 404.
- Select from the **Type** drop-down list, the Command intercom protocol to be used at your facility.
- In the **Dial Number** Length field, enter the number of digits to assign to each station call number.
- Select the **Support Regions** check box, if your facility will support logical grouping of one or more intercom servers.
- Enter the **IP Address** of the Command Intercom Server.
- Enter the **IP Port** number for communicating with the Command Intercom Server.
- Enter the **Password** that will be used for connecting to the Command Intercom Server.
- If your facility supports regions, enter **Region Number** assigned to the group of intercom servers.
- If your intercom system supports output setting, click the **Outputs** button. The Command Outputs dialog box opens.



Note: The Command interface allows you to set or reset outputs that for example, open doors, turn on lights, or activate alarm sirens. You must first configure these outputs using the Command software and then add them to the intercom exchange definition. Intercom exchange outputs are only used for event processing and reporting purposes. If you wish to control these outputs, you must add them to the intercom station definition.

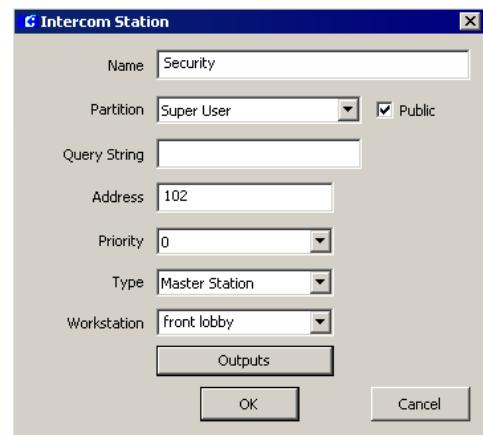
18. The default **Type** is Output. In the **Address** field enter the Output address and click the **Add** button. You may add as many outputs as needed. If you wish to remove an output from the list, select the output item and click the **Delete** button.
19. Click **Close** to save your settings and return to the Intercom Interface configuration.
20. Click **OK** to save your settings. The Intercom Exchange name displays under the Intercom Interface 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 call stations that will be used for audio channel 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 from the stations assigned to that exchange, as well as process intercom history messages and alarms.

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. If this is a partitioned system, select the **Partition** in which this intercom station will be active.

5. Select the **Public** check box if you wish this intercom station to be visible to all partitions.
6. Enter the **Query String** value that is used with message filtering (see “Define Query String Filters” on page 211).
7. 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.

Note: For a Command station group, you can enter a 1-digit number. This number must match the 1-digit Direct Dialing number configured for a Master station (using the Command interface), and that will be used to activate a group number.

8. 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.
9. From the **Type** drop-down list, select one of the following:

Sub-Station – You should configure at least one Sub-Station to send call requests to its Master Station.

Global Sub-Station – Select to allow Sub-Stations to connect to other Master Stations.

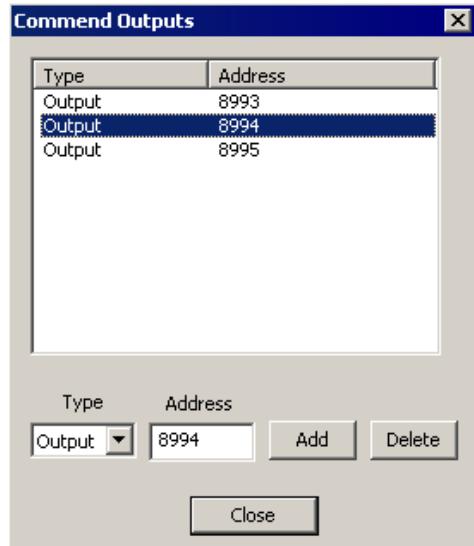
Station Group – Select to connect to multiple stations at the same time. P2000 will establish a connection between the stations that are part of the group selected and the workstation where the operator is logged on.

Master Station – The Intercom Exchange must have at least one Master Station to link to other stations.

10. If you are defining a Master Station, select from the **Workstation** drop-down list, the workstation name that controls the Master Station.

Note: You can only associate a P2000 workstation with one Master Station within an intercom switch.

11. If this is a Command intercom station, and your intercom system supports output setting, click the **Outputs** button. The Command Outputs dialog box opens.



Note: The Command interface allows you to set or reset outputs that for example, open doors, turn on lights, or activate alarm sirens. You must first configure these outputs using the Command software and then add them to the intercom station definition.

12. The default **Type** is Output. In the **Address** field enter the Output address and click the **Add** button. You may add as many outputs as needed. If you wish to remove an output from the list, select the output item and click the **Delete** button.
13. Click **Close** to save your settings and return to the Intercom Station configuration.
14. Click **OK**. The station name displays under the Intercom Station root icon.

Intercom Control

The P2000 Intercom Control window allows operators to monitor incoming call requests and to connect with stations or station groups that are part of the workstation's exchange. In facilities that use Command Intercom systems, operators can control outputs associated with the Command intercom equipment. The Intercom Control dialog box allows operators 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.

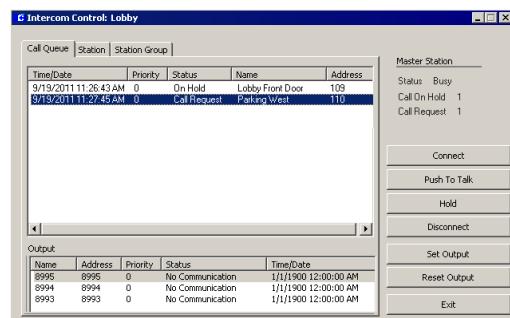
Note: Stations can also be connected or disconnected using the Real Time Map, see "Controlling Intercom Stations using the Real Time Map" on page 404.

To Control Intercom Stations:

- From the P2000 Main menu, select **Control>Intercom**. The Intercom Exchange Selection dialog box opens.



- Select the intercom exchange you wish to control and click **OK**. This selection list only displays in facilities that have more than one Intercom Exchange defined. 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 – The status of the selected station, such as Call Request, On Hold, Idle, Busy, etc.

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.

- Select any call in the queue and click the **Connect** button. This will connect your master intercom station to the calling intercom station selected.

- 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.

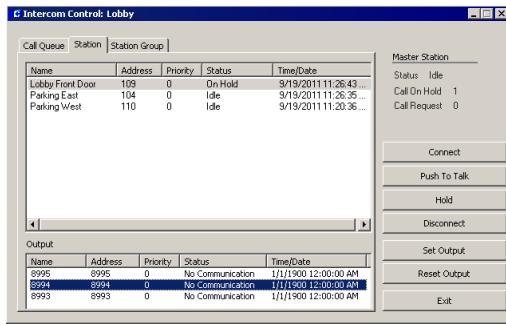
Disconnect – Disconnects from the calling station and removes the entry from the queue.

Connect – Selecting another entry in the queue and clicking Connect will perform a Hold on the currently connected call.

5. If the selected intercom station is associated with outputs (Commend systems only), select the output from the Output list box and click the **Set Output** button to activate the output, or the **Reset Output** button to reset the output.
6. Click **Exit** to close the Intercom Control dialog box.

To Control Sub-Stations Only:

1. In the Intercom Control dialog box, click the **Station** tab.



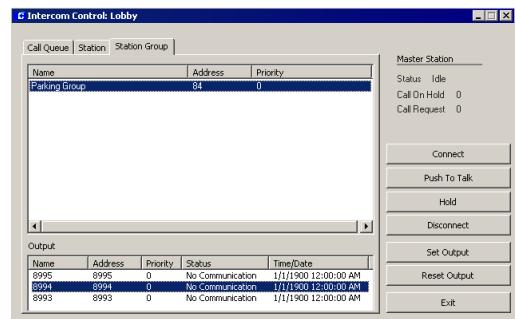
The list box displays the Name, Address, and Priority of the Sub-Station, as well as the current status of the call request and the time/date when the change of status took place.

2. In the list box, select a station to which you wish to connect.
3. Click the **Connect** button.
4. 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.).
5. If the selected intercom station is associated with outputs (Commend systems only), select the output from the Output list box and click the **Set Output** button to activate the output, or the **Reset Output** button to reset the output.

6. Click **Exit** to close the Intercom Control dialog box.

To Control Station Groups:

1. In the Intercom Control dialog box, click the **Station Group** tab.



The list box displays the Name, Address, and Priority of the Station Group.

2. In the list box, select a station group to which you wish to connect.
3. Click the **Connect** button.
4. 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.).

5. If the selected intercom station group is associated with outputs (Command systems only), select the output from the Output list box and click the **Set Output** button to activate the output, or the **Reset Output** button to reset the output.
6. Click **Exit** to close the Intercom Control dialog box.

Controlling Intercom Stations using the Real Time Map

The Real Time Map displays the 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. See “Using the Real Time Map” on page 326.

Note: *Intercom station groups are stateless; therefore, the Real Time Map does not display status changes associated with intercom station groups.*

When you receive a call request 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 you configured the intercom to allow the operator to activate events, the event name will also display in the shortcut menu. In addition, if the intercom station is associated with outputs (Command systems only), you can choose to set or reset all outputs associated with the station from 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 330 and 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 332 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 314 to create new event triggers and actions.

Intercom Transaction History Reports

The **SaveXAction** option in the intercom exchange definition allows you to save all intercom transactions in the P2000 Transaction History database.

Once the transaction history messages are saved, you can use the P2000 Transaction History report to list all intercom transactions in the system. The Transaction History report can be filtered to list by specific Site, Partition, Date and Time, and any combination of these. You can also select to run the report to list all intercom history types, or select a specific type such as *Intercom - Station Busy* or *Intercom - Call Station OK*. The options available for selection in the History Type field depend on the equipment used at your facility.

For detailed information on running reports, see *Chapter 6: System Reports*.

P2000 Enterprise

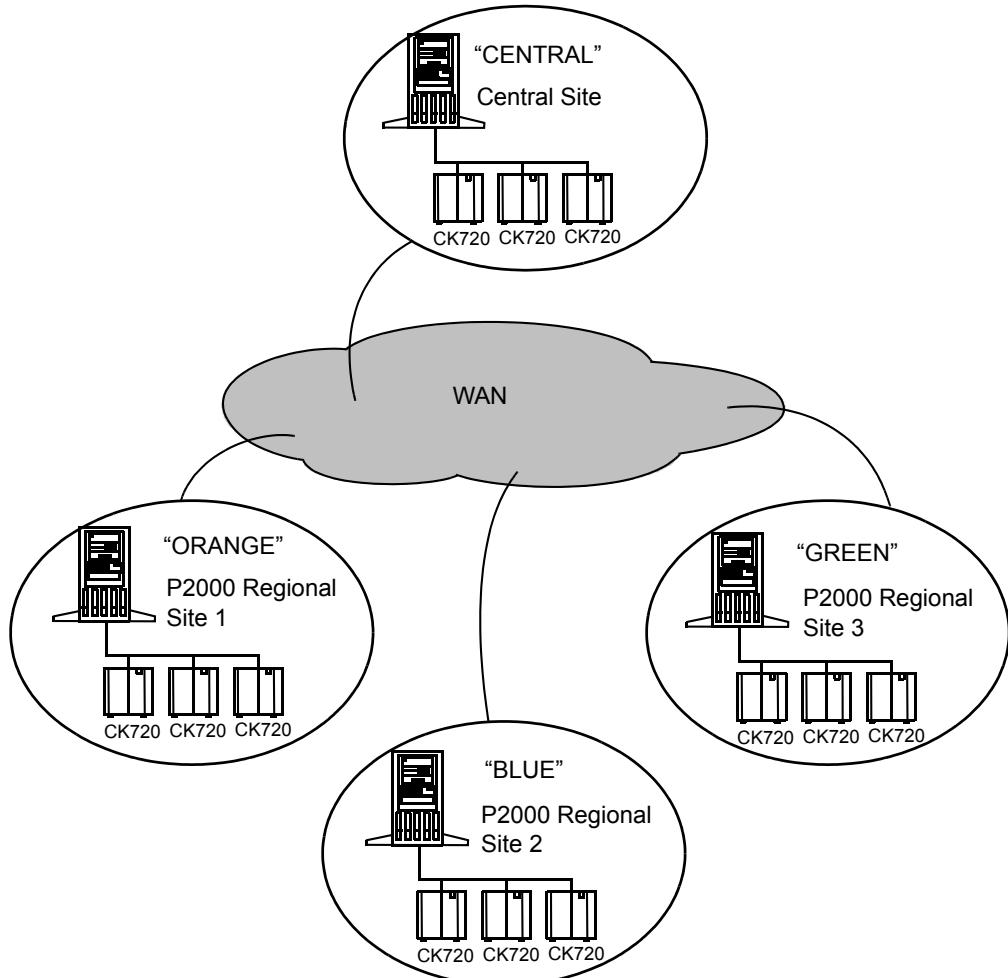
The P2000 Enterprise feature allows customers with multiple sites to communicate with each other to share Cardholder/Badge information. Cardholders can be granted access to doors at all assigned sites within the Enterprise system.

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 using Microsoft SQL Server database technologies.

Prior to defining Enterprise parameters using the P2000 software, you must refer to the *Enterprise Configuration* 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:

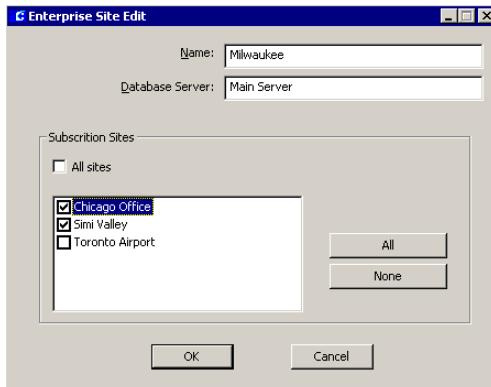
- Define Enterprise Parameters
- Assign Cardholders with the sites they are allowed to access
- Define the Badge access rights and security privileges at the assigned sites

Enterprise Parameters

Prior to assigning Cardholders 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. If you wish to select all sites, click the **All** button. This option allows you to unselect site names individually.
9. If you wish to clear your selections, click the **None** button.
10. If you wish 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:

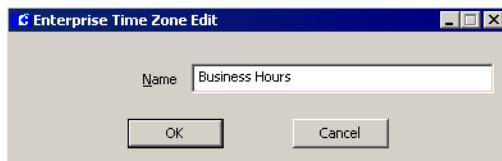
1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the **Enterprise Parameters** icon and click **Edit**. The Enterprise Parameters Edit dialog box opens.



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 **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.



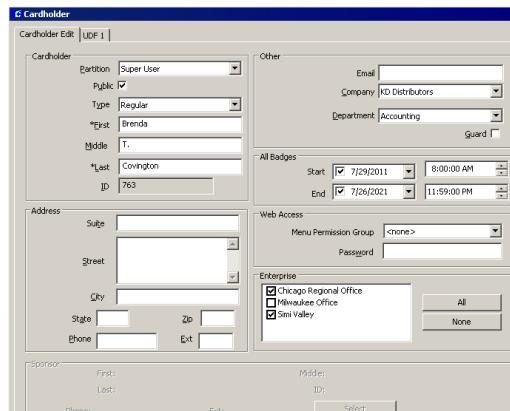
4. In the **Name** field, enter the name of the Access Group exactly as defined at the P2000 site that will provide access.
5. Click **OK** to save your settings.

Assign Cardholders Enterprise Access

Use the Cardholder application to assign the sites a cardholder can access. Once the sites are assigned, the cardholder information will be sent to the selected sites for download.

To Assign Enterprise Access to a Cardholder:

1. From the P2000 Main menu, select **Access>Cardholder**. The Cardholder window opens.
2. Create a new record or edit an existing cardholder as desired. For details, see “Entering Cardholder Information” on page 230. The Cardholder Edit dialog box opens.



The Enterprise box displays all the sites defined in the System Configuration window. See “To Define Enterprise Sites:” on page 406.

3. In the Enterprise box, select the check box next to the site that this cardholder may access. You may select as many sites as needed.
4. To select all sites, click the **All** button.
5. To clear your selections, click the **None** button.

- Once the sites are assigned, click **OK** to return to the Cardholder window. The information will also display in the Enterprise Sites tab located in the center of the window.

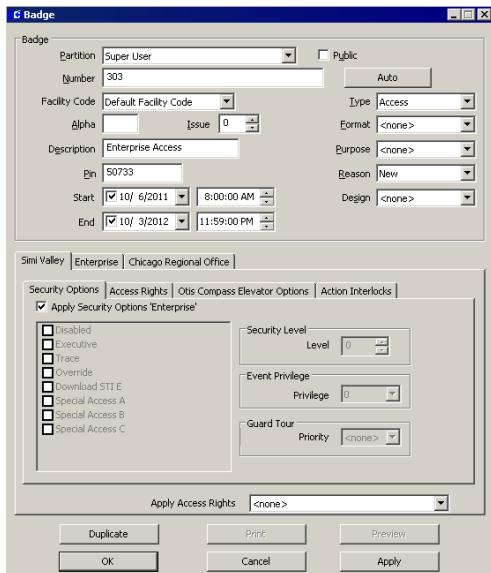


Define Global Badge Access Rights

Once the cardholder has been assigned to the selected sites, you may define the security privileges and access rights using the Badge application.

To Define Badge Access Rights:

- In the Cardholder window, select a cardholder from the Cardholder list that has Enterprise access.
- In the **Badge Information** box at the bottom of the Cardholder window, click **Add**. The Badge dialog box opens.



- Enter the badge number and optional description. For detailed information, see “Entering Badge Information” on page 237.

The Badge dialog box displays the site name tabs of the sites assigned to this cardholder. The first tab is always the local site tab and is used to assign local access privileges. The second tab is the Enterprise tab and is used to assign global access privileges. Additional tabs show other site names assigned to the cardholder.

Assigning access privileges is determined by the following conditions:

- When you define access to the local site, and select the **Apply Security Options ‘Enterprise’** check box, the security options defined in the Enterprise tab will be applied.
- When you define access at a different site, and select the **Apply Security Options ‘Enterprise’** check box, the security options defined in the Enterprise tab will be applied to that site.
- Access Groups and Time Zones 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 Groups/Time Zones are applicable (32 local and 32 Enterprise).
- P2000 will only download the maximum number of Access Groups/Time Zones for each panel type, giving priority to the local settings.
- Once the badge access parameters are defined, click **OK** to return to the Cardholder window. This will initiate all required downloads.

Note: The Status column in the Badge Information box at the bottom of the Cardholder window, displays the status of badges for the local site only.

Web Access

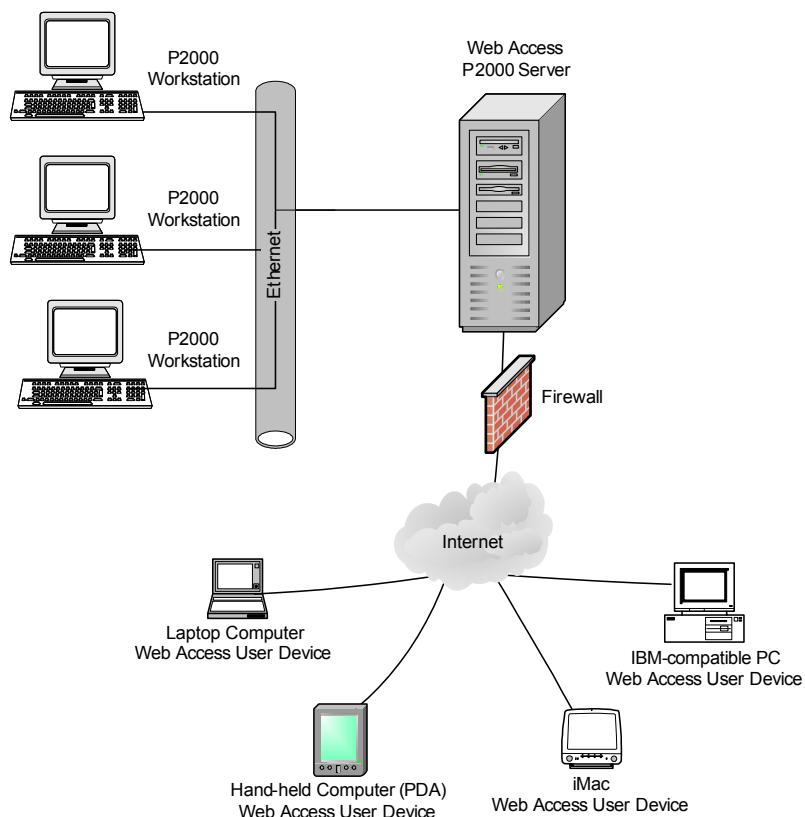
Web Access is a suite of applications that enables authorized users to perform various P2000 tasks from any web-ready PC or compatible Personal Digital Assistant (PDA) device. Web Access offers many features such as employee, visitor, and contractor management applications, badge activity tracking and synchronization, alarm monitoring, emergency access disable, web badging capabilities, 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

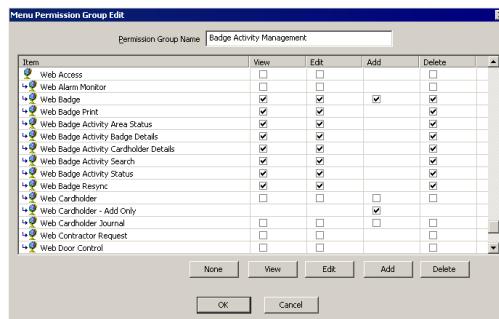
Once Web Access is installed at the Server and front-end PCs, follow these basic procedures for defining, implementing, and using Web Access:

- Create and assign menu permissions 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 Menu Permissions

To prevent unauthorized users from performing high-level actions, such as deleting cardholder records or rejecting requests, the system administrator must create menu permission groups, which are assigned to users who perform Web Access functions.

Each individual Web Access function is controlled by menu permissions and one menu permission group can include various combinations of permissions.



Some Web Access items, such as *Web Badge*, *Web Cardholder* or *Web Cardholder Journal*, provide up to four permission levels that allow the following functionalities:

View – View records.

Edit – Submit requests to edit records.

Add – Submit requests to add records.

Delete – Submit requests to delete records.

The *Web Request Queue Status* item allows users to view Web Access requests according to the following selections:

View – View requests from own department

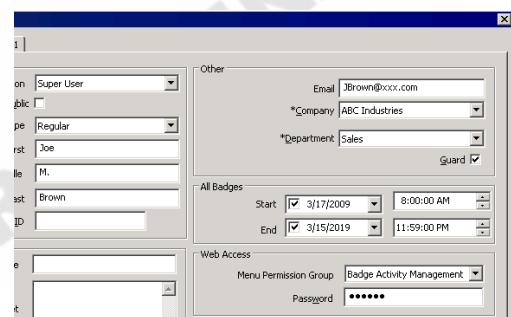
Edit – View requests from own company

Delete – View all requests

Other Web Access items provide only one permission level, which is selected by clicking on any of the permission levels (View, Edit, Add, or Delete), and allow users to perform the associated function. For example selecting any of the *Web Alarm Monitor* permission levels, allows the user to perform alarm monitoring functions. For detailed instructions, see “Creating Permission Groups” on page 23. Once the menu permissions are defined, they will be available for assignment from the Cardholder Edit dialog box.

To Assign Web Access Permissions:

1. From the P2000 Main menu, select **Access>Cardholder**. The Cardholder window opens.
2. Create a new cardholder record or edit an existing cardholder record. For detailed instructions, see “Entering Cardholder Information” on page 230. The Cardholder Edit dialog box opens.



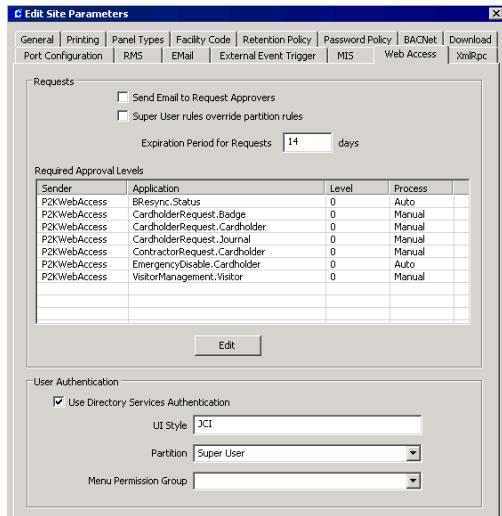
3. In the Web Access box, select from the **Menu Permission Group** drop-down list the group that will be assigned to this cardholder. The cardholder will be allowed to perform any function defined in this permission group.
4. In the **Password** box, enter the password that the cardholder will use to log on to the P2000 Web Access site.
5. Click **OK** to save your settings.

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. You can also configure User Authentication parameters to set up directory services for Web Access.

To Edit Web Access 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 **Web Access** tab and see the following section for detailed information.
3. Click **OK** to save the settings and return to the System Configuration window.

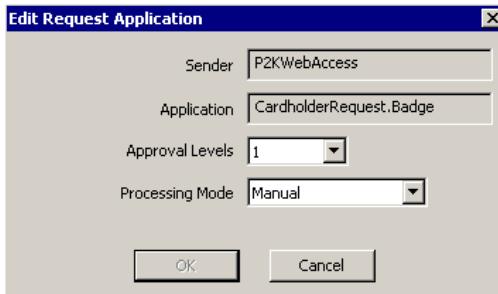
Web Access Options Field Definitions

Send Email to Request Approvers – If you select this option, when a cardholder 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 413. 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 menu permissions. The approver’s email address is defined in the cardholder 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. The *EmergencyDisable.Cardholder* application does not allow editing.



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). Not available for the *VisitorManagement.Visitor* application.
- **Manual** – Select this option if this application requires an authorized user to manually process the request, see “Processing Web Access Requests” on page 419.

User Authentication Box

P2000 Web Access operator passwords can be authenticated against a directory service such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP). This eliminates operator 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 elements must be set up:

- The **Directory Services Path** field must be set in the Password Policy tab of Site Parameters (see page 48). The actual value to use for the Directory Services Path is unique to your specific network configuration and needs to be obtained from the network administrator.
- Select the **Directory Services Password Validation** check box in the Edit Operator dialog box (see page 27) for each P2000 Web Access operator whose password will be verified by directory services.

Once the previous elements are configured, define the following parameters in the User Authentication box:

Use Directory Services Authentication – Enable the check box if you wish to set up directory services for Web Access.

UI Style – Enter the Web Access user interface style that users will be assigned when logging on using directory services authentication.

Partition – Select from the Partition drop-down list, the Web Access partition that users will be assigned when logging on using directory services authentication.

Menu Permission Group – Select from the drop-down list, the permission group that Web Access users will be assigned when logging on using directory services authentication.

Note: The UI Style, Partition, and Menu Permission Group assigned affects all P2000 operators whose accounts are enabled for directory services authentication. These parameters cannot be assigned individually (you cannot assign styles, partitions, or groups to specific users).

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 a cardholder who has been assigned *Web Request Approval* menu permissions. 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.

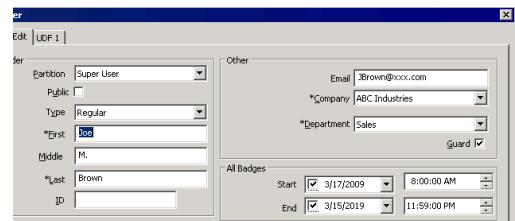
If an application requires a single approver, after the approver approves the request, the approval process is complete.

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 cardholder record.

To Enter the Cardholder Email Address:

- From the P2000 Main menu, select **Access>Cardholder**. The Cardholder window opens.
- Create a new cardholder record or edit an existing cardholder record. For detailed instructions, see "Entering Cardholder Information" on page 230. The Cardholder Edit dialog box opens.



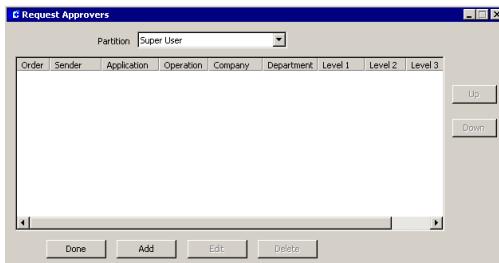
- Enter the **Email** address that has been assigned to this cardholder and where notifications will be sent in order to approve Web Access requests.

Note: To configure your Email Server, see "EMail Tab" on page 51, and also check with your IT department for the required email settings in your facility.

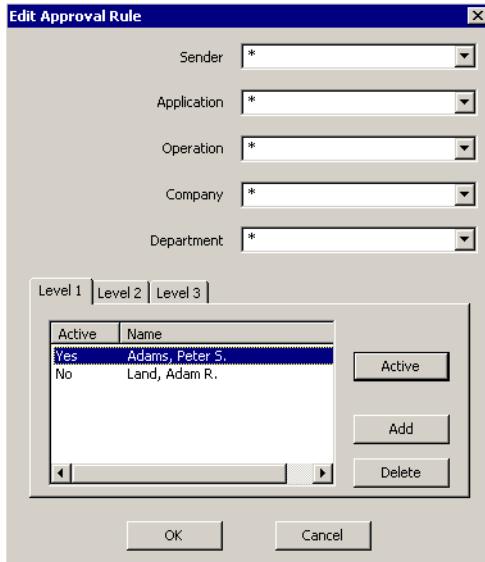
- Click **OK** to save your settings.

To Define Request Approvers:

- From the System Configuration window, click the plus (+) sign next to the root **Site Parameters** icon.
- Click the **Request Approvers** icon and click **Edit**. The Request Approvers dialog box opens.

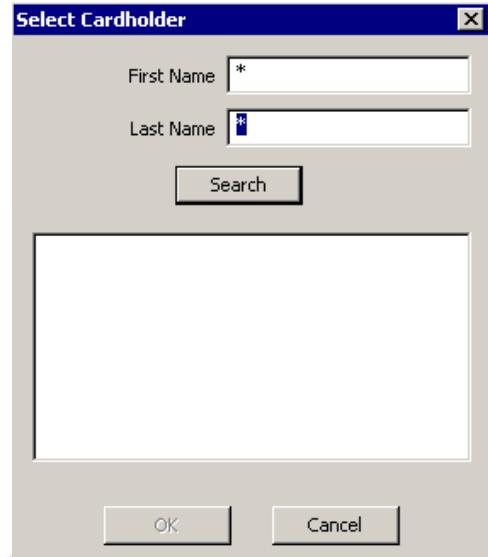


3. Select the **Partition** from the drop-down list that contains the cardholders that will be assigned as approvers. Requesters and approvers need to be in the same partition, unless the approver is in the Super User partition.
4. Click the **Add** button. The Edit Approval Rule dialog box opens. If 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 cardholder(s) can only approve requests coming from this sender.

6. From the **Application** drop-down list, select the name of the Web Access function that the selected cardholder(s) will be allowed to approve.
7. From the **Operation** drop-down list, select the type of operation (Add, Delete, or Update) that the selected cardholder(s) will be allowed to approve.
8. From the **Company** drop-down list, select a Company name if you wish to have the selected cardholder(s) approve only requests coming from the company selected here.
9. From the **Department** drop-down list, select a Department name if you wish to have the selected cardholder(s) approve only requests coming from the department selected here.
10. Click the **Level 1** tab and click the **Add** button. The Select Cardholder dialog box opens.



11. Enter the **First Name** and/or **Last Name** (or leave the default *), and click the **Search** button.

12. Select a cardholder 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 cardholder who will be the active Level 1 approver of the type of application and 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 a cardholder 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.

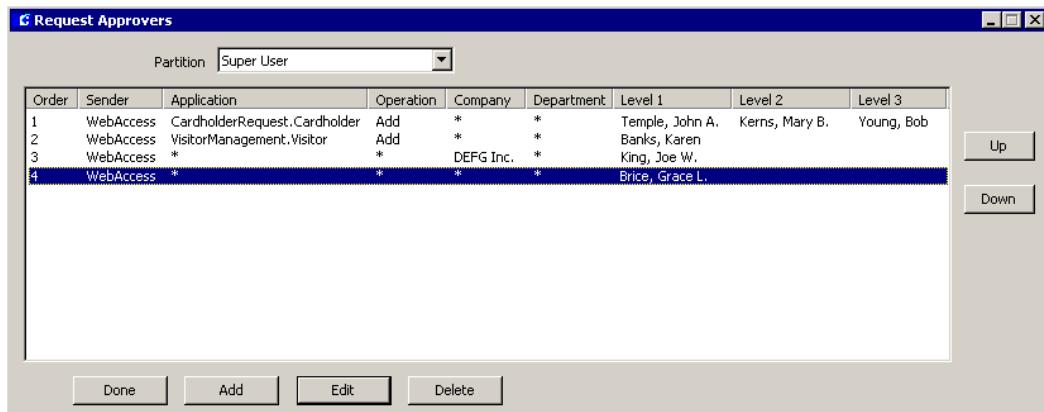
Rule 1 requires three approvers for adding cardholders (from any company and/or department).

Rule 2 requires only one approver for adding visitors (from any company and/or department).

Note: The system will generate an error message if a request is submitted and the number of required approvers has not been defined.

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 3 requires one approver for any type of request submitted for the DEFG company (any department), except that new cardholders (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 cardholders (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:

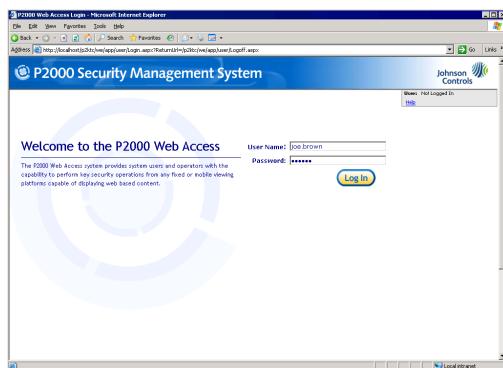
1. Using a web browser, type the following in the address bar, replacing *ServerName* or *IP Address* with the name or IP Address of the Web Access server:

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** (*firstname.lastname*). This is the name of any cardholder who has Web Access menu permission.

For systems that use multiple interface styles, the **User Name** may include the style name (*firstname.lastname@stylename*). Refer to the *Web Access Manual* for details.

3. Enter a valid **Password**. This is the password entered in the Cardholder Edit dialog box.

4. Click **Log In**. The Welcome page displays.



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.

Note: To access Web Access from the P2000 Server, you can also select **Start>Programs>Johnson Controls>P2000>P2000 Web Access Home 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 track the badge activities of cardholders, request a Badge Resync, which returns a badge to its correct state if it is out-of-sync, or print and encode a badge.

Cardholder Search

This feature allows searching for cardholder records in the P2000 database. Users may

search by cardholder name, badge number, ID number, department, and company.

Area Search

This feature allows users to view which cardholders currently 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 cardholders.

In Out Displays

This feature allows users to see which cardholders are “in” or “out” of the facility, or specific areas of the facility, based on their badge activity. If a cardholder has badged to enter the facility the status will be “In.” If a cardholder has not badged to enter the facility, the status will be “Out.”

Badge Resync

This feature allows users to manually adjust the status of their badge if it has been placed in an out-of-sync state. A badge is out-of sync when cardholders (that are required to enter and exit an area in sequence using entry and exit terminals), badge *IN* at an entry terminal and don’t badge *OUT* at the next badging if, for example, they follow another cardholder *OUT* without swiping their badge. In that case, the badge remains in the *IN* state (out-of-sync) and will be denied access the next time they attempt to badge back into the area.

Badge Print

Allows you to locate cardholder records using various search filters. After you perform a search, Web Access lists the badge ID number, cardholder name, personal identification number, company, and department of each card-

holder record located in the search; then you can preview, print, and/or encode a cardholder’s badge by clicking the badge ID number.

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 cardholder records, including badge and associated cardholder information. In addition, the user can also view, approve and process Web Access requests.

Request Status

The Request Status page allows authorized users to view the status of their requests, and depending on their menu permissions, 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 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 411), up to three authorized users may be required to approve Web Access requests.

Add Cardholder

This feature allows authorized users to submit requests to enter cardholder information into the system. Depending on the permissions assigned, users can enter cardholder related information such as user-defined fields, journals, badge information, sponsor information (if the cardholder is a visitor), or attach a portrait to the cardholder record.

Edit Cardholder

In addition to submitting requests for new cardholders, authorized users can also request to change existing cardholder records, including deleting records from the system.

Validate

This function is used to process Web Access requests that require manual processing. See “Processing Web Access Requests” on page 419.

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 Badge, Edit Cardholder, Execute Application, etc.

WebBadging Setup

Allows you to download and run the WebBadgingSetup.exe file, which installs the WebUSB application to enable the use of USB-compatible badging devices via the P2000 Web Access interface. This service must be running on the client computer running Web Access or the badging devices cannot be controlled.

Visitor Management

Allows authorized users to request a visitor badge or request to extend the validation period of a cardholder badge. 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, and enter notes for visitors with special needs. Visitor requests are processed using the P2000 Visitor Request Management application, see “To Process Visitor Requests.” on page 419.

Contractor Request

Enables authorized users to extend the badge validity period for selected cardholders. 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 cardholders. Users can only extend the badge validity period for cardholders who belong to the same company as the user.

Request Status

This function is also accessed from Management Services, see “Request Status” on page 418.

Emergency Access Disable

This feature provides a rapid method of disabling access in case of an emergency. An authorized user can quickly disable all badges associated with a selected cardholder(s) and access will be immediately denied at all doors. In addition, the selected cardholder will not be able to perform any Web Access functions. Once it is determined that the emergency is over, the badges can be enabled again using the Badge application.

Note: Badges cannot be enabled using 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 411).

With the exception of Visitor Requests, all Web Access requests can be processed automatically. Once a 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 459) 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. With the exception of Visitor Requests, all Web Access requests are processed from the Validation page. See the following section for instructions on manually processing Visitor Requests.

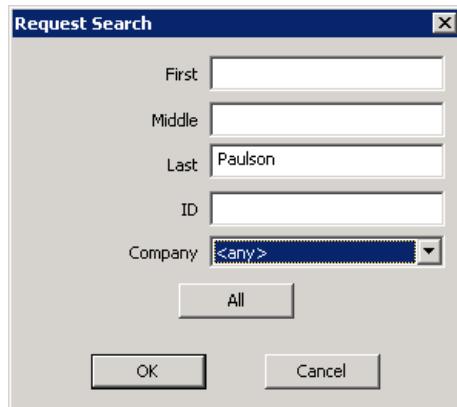
To Process Visitor Requests:

1. From the P2000 Main menu, select **Access>Visitor Request Management**. The Visitor Request Management dialog box opens. The list box (top portion of the screen) displays a queue of requests submitted using Web Access.

Note: The Visitor Request Management dialog box should be kept opened at all times for the person to manually process and act upon incoming visitor requests.

2. Select from the **Partition** drop-down list, the partition that contains the visitor requests.
3. To display today’s requests only, select the **Today Only** check box.
4. To display requests that will be processed at the workstation location, select the **This Location Only** check box. The list will display requests that have the location name entered in the Location field of the workstation dialog box (see page 22).

- To search the request queue for a specific record, click the **Search** button located above the list box, enter the visitor data into the fields on the Request Search dialog box, and click **OK**.



- You may click the **All** button to display all visitors currently in the queue.

Note: You can also display all visitors in the queue by using the **All** button located above the list box in the Visitor Request Management dialog box.

- Highlight an entry from the queue to pre-fill the Visitor and Sponsor fields. Other information related to the selected Visitor, such as Request Notes, will also display.

Note: The **Found in DB** fields indicate whether or not P2000 has identified a matching Visitor and/or Sponsor record in the cardholder database. A picture will also display, if there is one previously saved for the selected visitor.

- See the following Visitor Request Management Field Definitions for more detailed information.

Location	Arrival Time	Visitor	ID	Company	Requestor	Requestor Co.	Start Date	End Date
West Union Bu...	7/22/2008 8:...	Anderson, Wil...	5883	XYZ Consulting	Smith, Robert J.	Johnson Controls	7/22/2008 8:...	7/22/2008 6...
West Union Bu...	7/22/2008 8:...	Gray, Albert	5443	XYZ Consulting	Smith, Robert J.	Johnson Controls	7/22/2008 8:...	7/22/2008 6...
West Union Bu...	7/22/2008 9:...	Humphrey, Ri...	2543	XYZ Consulting	Smith, Robert J.	Johnson Controls	7/22/2008 8:...	7/22/2008 6...
West Union Bu...	7/22/2008 10...	Paulson, John	1221	United Networking	Smith, Robert J.	Johnson Controls	7/22/2008 10...	7/22/2008 6...

9. When all the information is entered, click the **Save** button to complete the request and save the visitor and badge information. The new visitor data will also be reflected in the Cardholder window.
10. If you wish to save and print the badge, click the **Save and Print** button (requires the Video Imaging application).
11. To process additional visitor requests, click the **Clear** button to clear the information on the screen, then select another visitor name from the queue or enter the information according to the Visitor Request Management Field Definitions.
12. If a visitor request is to be rejected, select the name from the queue and click the **Deny** button.
13. Click **Exit** to close the Visitor Request Management dialog box.

Visitor Request Management Field Definitions

Visitor Box

First – Displays the first name of the visitor selected in the queue. You may also enter a value to search the cardholder database by first name.

Middle – Displays the middle name of the visitor. You may also enter a value to search the cardholder database by middle name.

Last – Displays the last name of the visitor. You may also enter a value to search the cardholder database by last name.

ID – Displays the ID of the visitor. You may also enter a value to search the cardholder database by this field.

Company – Displays the visitor's Company name. You may also enter a value to search the cardholder database by company name.

If the company name does not already exist in the database for the visitor's assigned partition, you will be notified upon selecting the visitor request in the queue. To add the company name to the P2000 database, click the browse button to open the Company window. See "Define Companies and Departments" on page 220 for information on adding a company name to the P2000 database.

Partition – Displays the partition assigned to the visitor. To change the assigned partition, select a new one from the drop-down list. If you change the partition, you may also have to reassign the visitor's company to a company that belongs to the same partition.

Notes – Displays the visitor request notes entered by the requestor.

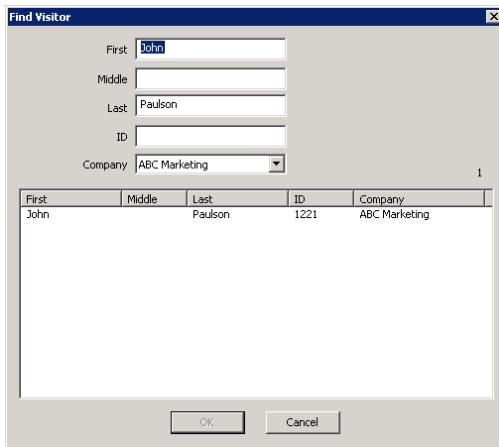
Found in DB – Indicates whether or not P2000 has identified a matching Visitor record in the cardholder database. If no match is identified, click the **Search** button to manually search for a matching record.

If **Found in DB** shows **Yes**, then the existing visitor record in the P2000 database will be updated. If it shows **No**, the new visitor will be added when you click the **Save** button.

Approved Visits – Displays the number of approved visits. This field is only valid if the **Found in DB** field displays **Yes**.

Note: The Visitor Request Management application creates four UDFs: **Approved Visits**, **Most Recent Visit**, **Second Most Recent Visit**, and **Third Most Recent Visit**. These UDFs are automatically updated and allow you to monitor the visits associated with the selected visitor.

Search – If P2000 did not identify a matching Visitor record in the database, you may search the database by entering a value in any of the Visitor fields and then clicking the **Search** button. The Find Visitor dialog box opens displaying the visitor record(s) that match the entered value(s). You may also click the **Search** button without entering any values to display all visitors in the database.



Select the visitor's name and click **OK**.

Take – If your facility uses the Video Imaging application, click the **Take** button to capture the visitor's portrait. See the instructions on page 340 (Step 4.) for details on capturing portrait images.

Sponsor Box

First – Displays the first name of the person who will sponsor this visitor.

Middle – Displays the middle name of the person who will sponsor this visitor.

Last – Displays the last name of the person who will sponsor this visitor.

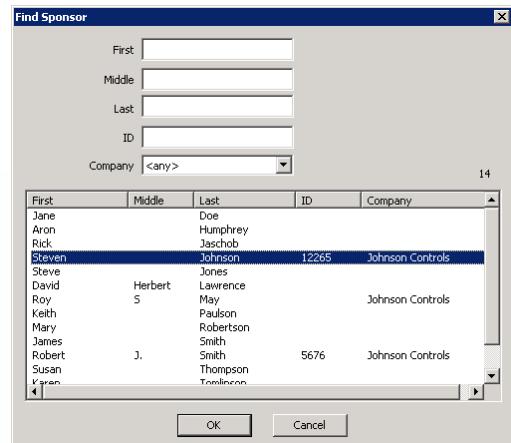
ID – Displays the unique ID assigned to the sponsor.

Company – Displays the sponsor's Company name.

Partition – Displays the partition assigned to the sponsor.

Found in DB – Indicates whether or not P2000 has identified a matching Sponsor record in the cardholder database. If no match is identified, click the **Search** button to manually search for a matching record.

Search – If P2000 did not identify a matching Sponsor record in the database, you may search the database by clicking the **Search** button. The Find Sponsor dialog box opens displaying the sponsor record(s) that match the entered value(s). If no value was entered, all cardholders in the database will be displayed.



Select the sponsor's name and click **OK**.

Badge Box

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 44).

Auto – If your facility is set up to use the Auto-Badge Management feature (see page 249), click the **Auto** button to insert the next available badge number in the Number field.

Issue – Enter an issue level per badge number. If a visitor loses a badge, you would give 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 44.

Template – Select from the drop-down list the access template to be applied to this badge. See “Access Template” on page 243.

Design – Select from the drop-down list the badge design that was created using the Video Imaging application.

Start Date – Enter the date this badge becomes active. Click the down arrow to select a date from the system calendar.

Start Time – Enter the time this badge becomes active. Click the spin box buttons to select a time.

Void Date – Enter the date this badge will be automatically voided. Click the down arrow to select a date from the system calendar.

Void Time – Enter the time this badge will be automatically voided by the system. Click the spin box buttons to select a time.

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
- Images (for example, a company logo)
- Field type (combo box, text box, etc.), location, and size
- 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 via UDFs (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 *UIstyle* user-defined field (UDF).

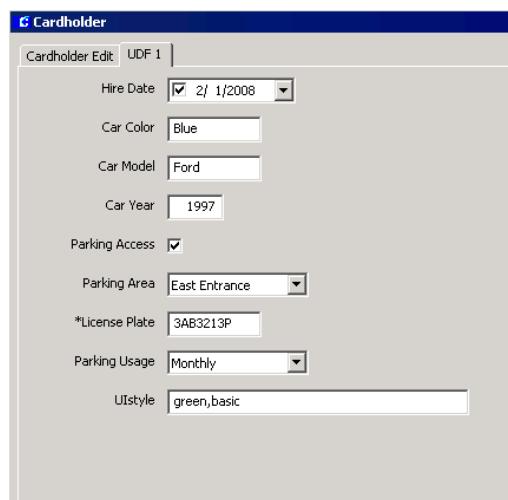
To Create the User Interface Style UDF:

- From the P2000 Main menu, select **Config>Cardholder Options>User Defined Fields**. The User Defined Fields dialog box opens.
- Click **Add**. The Add User Defined Field dialog box opens.
- In the **Name** field, enter *UIstyle*. Enter the name exactly as shown. The letter case must match: *UI* should be uppercase letters and *style* should be lowercase letters. Do not add spaces.
- From the **Type** drop-down list, select *Text*.
- In the **Width** field enter 32.
- Click **OK** to save the *UIstyle* UDF, then click **Done** to close the User Defined Fields dialog box.

The *UIstyle* UDF will be available in the Cardholder window to assign one or more of the new styles to the desired Web Access users.

To Assign Styles to Web Access Users:

- From the P2000 Main menu, select **Access>Cardholder**. The Cardholder window opens.
- Select a cardholder that is allowed to perform Web Access functions. See “To Assign Web Access Permissions:” on page 410.
- Click the **Edit** button on the right side of the window. The Cardholder dialog box opens.
- Click the **UDF 1** tab to display the user defined fields. Required fields are indicated by an asterisk and must be completed before a record is saved.



The dialog box displays all UDFs defined for your facility.

- To assign a style to the cardholder, enter the style name into the **UIstyle** field. The name must match the directory style name, for example, *green*. Refer to the *Web Access Manual* for details in creating customized styles.
- If you wish to assign multiple styles to the cardholder, enter the names of the styles separated with a comma, for example, *green,basic*.
- Click **OK** to return to the Cardholder window.

Web Access Smart Card Encoder Configuration

Web Access offers web badging capabilities, which allow among other things, encoding cardholder badges from a Web Access computer.

To support the programming of smart cards using the ACS® Model ACR120 MIFARE smart card encoder, the Web Access computer must be configured as a web badging station.

The encoder requires a simple USB cable connection from the device to the Web Access computer.

Note: *The encoder must be connected to the USB port on the Web Access computer. Do not connect to a USB hub. Refer to the Web Access manual to install and configure the proper hardware and software components.*

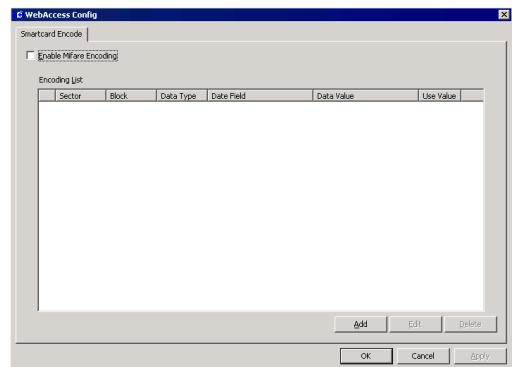
MIFARE is a contactless smart card technology that has 16 sectors; each sector with 64 bytes (512 bits) of memory. Each sector can contain up to 4 blocks, each block containing 16 bytes (128 bits).

After you configure the web badging station, use the WebAccess Config function to configure the parameters for encoding badges from web badging stations.

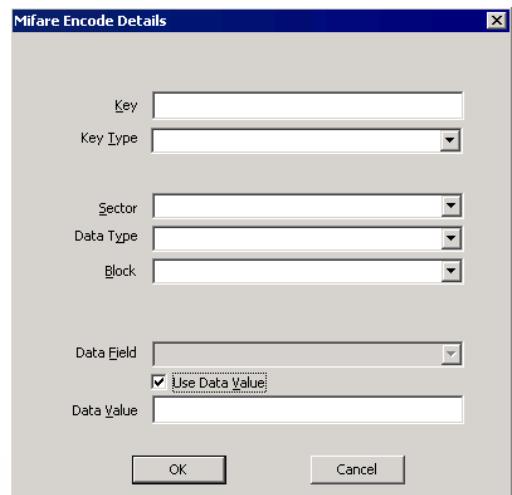
IMPORTANT: *Before configuring the smart card encoder, the user must have a reasonable level of experience with encoding configuration and a thorough understanding of the MIFARE functional specification, including sector and block organization. Refer to your card manufacturer documentation for specific settings.*

To Configure the Web Access Smart Card Encoder:

- 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 **Web Access** icon and click the **Edit** button. The WebAccess Config dialog box opens.



- Click the **Add** button to open the Mifare Encode Details dialog box.



- Enter the **Key** that was assigned to the card. A Key is basically a password. The Mifare card uses 48-bit keys, made of up to 12 Hex characters: “0” to “9” and/or “a” to “f” (uppercase or lowercase). This key is usually provided by the manufacturer.
- Select from the **Key Type** drop-down list, whether this is a Key A or Key B. These keys perform different functions. For example, Key A could be required to read data in a sector, while Key B could be required to write data to a sector.

7. Select from the **Sector** drop-down list, a sector number from 0 to 15 for the card. Each sector can store its own pair of keys (A and B).
8. Select from the **Data Type** drop-down list, whether the type is Data or Keys. See page 427 for more details.
9. Select from the **Block** drop-down list, the block that will be assigned to the sector. Depending on the data type selected above, each sector can contain up to 4 blocks. By default, block 3 is assigned to any sector whose Data Type is Keys. See the table below for memory organization details.
10. If you wish to include a P2000 database field as part of the encoding information, select from the **Data Field** drop-down list the desired field.
11. If you wish to customize the encoding details, check the **Use Data Value** check box, and enter the desired data in the **Data Value** field. If the Data Type is Data, the Data Value must be a decimal number string. If the Data Type is Keys, the Data Value must be a Hex string.
12. Click **OK** to save the encoding details and return to the WebAccess Config dialog box.
13. The P2000 system will not allow encoding badges from a Web Access computer unless the **Enable Mifare Encoding** check box is selected. If you wish to disable badge encoding from a Web Access computer, select the check box again to disable it.
14. Click **OK** to save the encoding parameters.

		Byte Number within a Block															Description	
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
15	3	Key A				Access Bits				Key B								Sector Trailer 15
	2																Data	
	1																Data	
	0																Data	
14	3	Key A				Access Bits				Key B								Sector Trailer 14
	2																Data	
	1																Data	
	0																Data	
:																		
1	3	Key A				Access Bits				Key B								Sector Trailer 1
	2																Data	
	1																Data	
	0																Data	
0	3	Key A				Access Bits				Key B								Sector Trailer 0
	2																Data	
	1																Data	
	0																Manufacturer Block	

Mifare Encoding Scheme

Data Type: Data / User Data Value: false

- If the value of the selected Data Field is a number, it will be encoded in binary with an ending semi-byte ‘0x0’; example:
for data field “Cardholder ID” with a value of “123.”
123 in binary is “0000007B” and with the ending semi-byte ‘0x0’ it will be encoded as “000007B0.”
- If the value of the selected Data Field is not a number, it will be treated as ASCII string and attached with a leading semi-byte ‘0x0’; example:
for data field “first name” with a value of “John.”
John in ASCII is “6A6F686E” and with a leading semi-byte ‘0x0’ it will be encoded as “06A6F686E0.”

Data Type: Key / User Data Value: false

- The selected Data Field will be treated as Hex string with an ending semi-byte ‘0x0’
- If the Data Field can’t be translate into Hex string, it will be converted as ‘0x00’; example:
if the selected datafield’s value is “E324FD” it will be encoded as “0E324FD0”

PRELIMINARY

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 CK7xx to Flash Memory**
- **Update CK7xx Panels**
- **Update S321-DIN 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 cardholder 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 download data to panels if there has been an interruption in communication. For example, if a panel or group of panels has been offline for mainte-

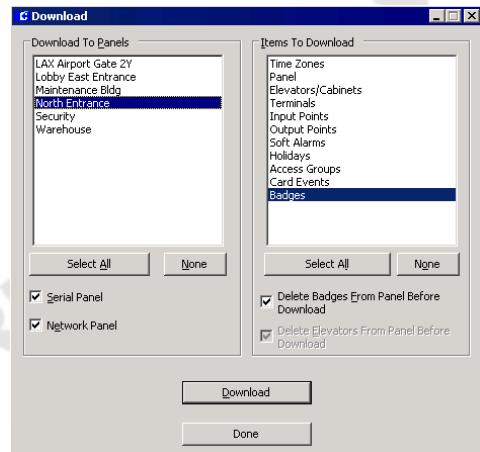
nance, you can use Download to update panels with system changes that occurred while they were down. Or, you may need to download data to all panels after a complete power failure or system upgrade. The Download function should be performed only by a system administrator, and is password protected.

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** (legacy and P900) and/or **Network Panel** (all other panels) 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 box, select the items you wish to download to the panel(s), or click **Select All** to select all items in the list. (Click **None** to clear your selections and reselect the items individually.)

Note: HID panels will go offline temporarily whenever a panel download is initiated. Also, whenever an HID terminal or input configuration is downloaded, there is a 7 to 8 second window when a cardholder may gain access even if the enabled time zone does not allow it.

6. If you wish to download all badges to a panel and still allow access through a door of the panel while being updated, select **Badges** from the Items To Download box, and clear the **Delete Badges From Panel Before Download** check box.

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.

7. If you wish to download elevator data without deleting all elevators from the panel, select **Elevators/Cabinets** from the Item To Download box, and clear the **Delete Elevators From Panel Before Download** check box.
8. 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”.)

Download Status

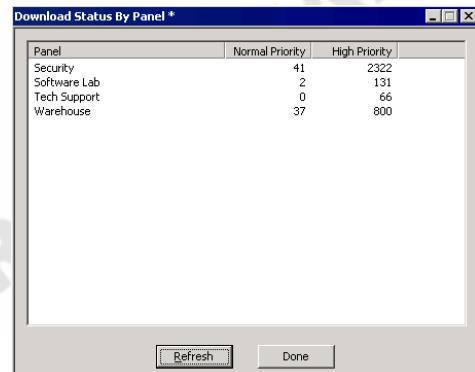
Download Status displays the status of any items automatically downloaded by the system, and can be used in conjunction with the Download function.

To Monitor Download Status:

1. From the P2000 Main menu, select **System>Download Status**. The Download Status message box opens.



2. 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.
3. If you wish 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. All items are downloaded at a **High Priority**, with the exception of Badges, which are downloaded at a **Normal Priority**.

4. Click the **Refresh** button to update the screen with new data as the download progresses.
5. Click **Done** to close the Download Status By Panel dialog box.
6. 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 cardholder and badge changes.

You should use the Download tab in Site Parameters (see page 49) to set up rules that determine the time when these downloads will take place.

To Monitor Smart Downloads:

1. 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 **In Progress** box displays the number of records currently being downloaded.

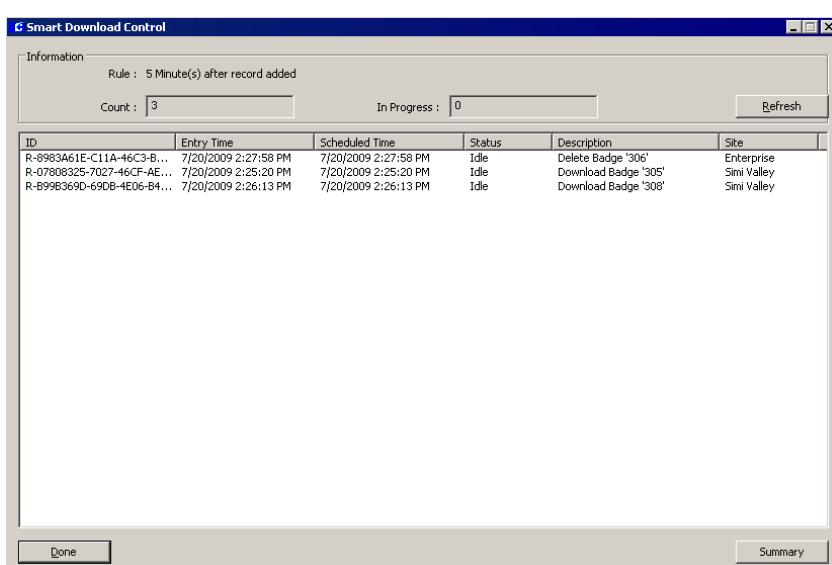
The following information is shown for each download in the queue:

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 (Idle or In Progress).



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.

2. Click the **Refresh** button to update the screen with new data as the download progresses.
3. Click the **Summary** button to display a summary of record counts and time information associated with the records currently displayed in the Smart Download Control screen.
4. 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 Service Control or the Service Monitor application. If the *Auto Start* flag is disabled, the ser-

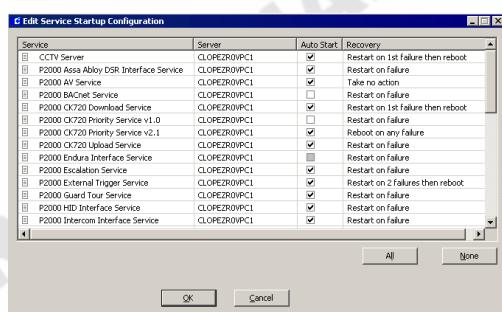
vice will not start automatically and will not display in Service Control.

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 facility uses advanced features, 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 Menu Permissions to restrict access to this feature only to system administrators to prevent unauthorized personnel from stopping critical services.

To Edit Service Startup Configuration:

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 **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.

4. Select the service that you wish to auto start and click the associated check box in the **Auto Start** column.
5. If you wish to auto start all services, click the **All** button, or click **None** to clear the selections and reselect the services individually.
6. To restrict a service from starting automatically at system startup, select the service and click the associated check box to remove the check mark.
7. 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.
8. 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

CCTV Server – Communicates with the CCTV and the DVR hardware. See the CCTV and the DVR features, described in *Chapter 4: Advanced Features*.

P2000 Assa Abloy DSR Interface Service – Provides the communication between the P2000 Server and the Assa Abloy Door Service Router (DSR).

P2000 AV Service – Provides communication with Audio Visual components. See the DVR feature on page 394.

P2000 BACnet Service – Starts the BACnet Interface communication. See the Metasys Integration (BACnet) feature on page 343.

P2000 CK720 Download Service – Performs Server downloads going to all CK705, CK720, CK721, and CK721-A panels in the system.

P2000 CK720 Priority Service v1.0 – Performs CK705/CK720 panel online and offline notifications (for panel versions earlier than 2.1).

P2000 CK720 Priority Service v2.1 – Performs CK705, CK720, CK721, and CK721-A panel online and offline notifications (for panel version 2.1 and higher).

P2000 CK720 Upload Service – Performs CK705, CK720, CK721, CK721-A panel uploads to the Server.

P2000 Endura Interface Service – Performs communications between the P2000 Server and Pelco® Endura™ DVRs. It handles Host Event actions and processes alarms from the Pelco Endura DVR. This interface service uses Pelco API that supports H.264 cameras. This service is not involved in video playback.

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. See the Guard Tour feature on page 352.

P2000 HID Interface Service – Provides the communication between the P2000 Server and HID readers.

P2000 Intercom Interface Service – Provides the communication with the Intercom hardware. See the Intercom feature on page 396.

P2000 Intrusion Interface Service – Provides the communication between the P2000 system and third-party intrusion panels. This service allows the P2000 system to obtain status information whenever an intrusion component changes and issues commands to control the intrusion zones, areas, and annunciators that are part of the intrusion system.

P2000 Isonas Interface Service – Provides the interface between the P2000 system and the Isonas readers.

P2000 Milestone Interface Service – Performs communications between the P2000 Server and Milestone® XProtect™ Corporate DVRs. It handles Host Event actions and processes alarms from the Milestone DVR. This service is not involved in video playback.

P2000 Milestone MIP Interface Service – Performs communications between the P2000 Server and Milestone Interface Protocol (MIP) XProtect Corporate and XProtect Enterprise DVRs. It handles Host Event actions and processes alarms from the Milestone DVR. This service is not involved in video playback.

P2000 MIS Interface Service – Imports and exports data for the MIS Interface. See the MIS Interface feature on page 341.

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 Nice Interface Service – Performs communications between the P2000 Server and Nice® DVRs. It handles Host Event actions and processes alarms from the Nice DVR. This service is not involved in video playback.

P2000 OnSSI Interface Service – Performs communications between the P2000 Server and OnSSI® DVRs. It handles Host Event actions and processes alarms from the OnSSI DVR. This service is not involved in video playback.

P2000 OPC Proxy Service – Provides the communication between P2000 applications and certain servers, such as the CCTV Server or the OPC Server.

P2000 OSI Interface Service – Provides the interface between the P2000 system and the OSI system.

P2000 Otis Interface Service – Provides the interface between the P2000 system and the Otis Compass Destination Entry elevator system. The P2000 Server will serve as a message router for the messages going between the Otis system and CK721-A panels.

P2000 P900 SIO Handler Service – Performs communications between the P2000 Server and P900 panels.

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 Rapid Eye Interface Service – Performs communications between the P2000 Server and Honeywell® Rapid Eye™ DVRs. It handles Host Event actions and processes alarms from the Rapid Eye DVR. This service is not involved in video playback.

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-DIN panels.

P2000 S321-IP Interface Service – Provides the communication between the P2000 Server and S321-IP panels.

P2000 SIA Interface Service – Provides the communication with configured SIA devices.

P2000 SIO Handler Service – Performs communications between the P2000 Server and legacy panels.

P2000 Smart Download Service – Downloads badges to panels when changes are made to access groups and terminal groups. It also downloads cardholder and badge changes. In addition, controls badges with temporary access.

P2000 SMTE Service – Provides front end translation and mapping of external Request Queue interfaces.

P2000 Watchdog Service – Monitors other P2000 services to verify that they are operating and generates an alarm when a P2000 service fails.

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). It handles Host Event actions and processes alarms from the Pelco DVR. This interface service uses Pelco API that does not support H.264 cameras. This service is not involved in video playback.

Starting and Stopping Service Control

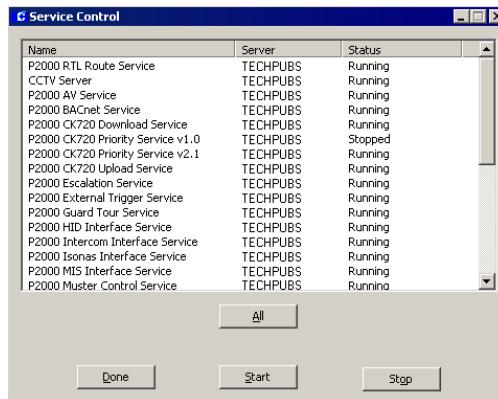
Service controls are provided specifically to stop and restart communications between panels and the Server to perform system maintenance functions, or during network troubleshooting operations. For example, the system administrator would be required to stop all communication services between panels and the Server when performing a P2000 version upgrade; 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.

Note: The procedure to control services at redundancy systems might be different from the steps described here. Refer to your redundancy documentation for details.

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 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.

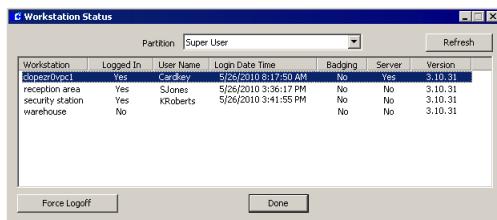
Workstation Status

This application displays workstation status information, including the workstation's current P2000 software version installed. Operators with proper permissions can monitor all the users currently 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:

- From the P2000 Main menu, select **System>Workstation Status**. The Workstation Status window opens.



- If this is a partitioned system, select the **Partition** that contains the workstations you wish to view. All workstations active in the partition are displayed.
- The list box displays the following information for each workstation:

Workstation – Indicates the name given to the workstation (and the Server).

Logged In – This column indicates whether or not the workstation is currently logged on.

User Name – If the workstation is logged on, this column displays the name of the user logged on at the workstation.

Login Date Time – This column displays the date and time when the user logged on at the workstation.

Badging – This column indicates if the workstation is configured as a badging workstation.

Server – Indicates the workstation that operates as the system Server.

Version – Displays the P2000 version installed at the workstation.

- If you wish to log off a workstation that is currently logged on, select the workstation name and click the **Force Logoff** button.
- To update the list box with current workstations status, click the **Refresh** button.
- Click **Done** to exit the window.

Automatic Software Updates

P2000 supports the automatic distribution of software updates to workstations in a P2000 Security Management System. P2000 administrators can configure the P2000 Server to force update all P2000 workstations in the system or allow workstation operators to accept or deny the update when logging into the system. The Automatic Update feature eliminates the need to manually update each workstation when a new P2000 software version or service pack is released. This feature is available for workstations running P2000 version 3.10 and higher.

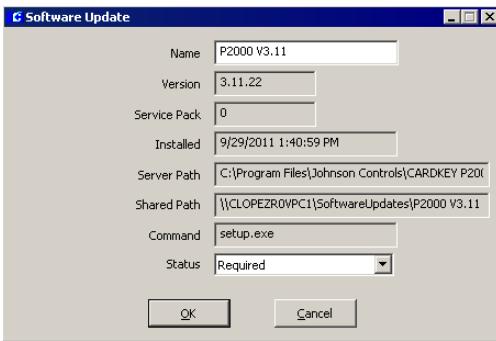
The P2000 Server software tracks each software update installed on the Server, providing detailed information such as the version number, service pack number, installation date, the location of installation files, and the update control setting (Not Available, Optional, or Required).

This function should be performed by a system administrator at the Server.

To View or Modify Software Updates

- 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.

3. Click the plus (+) sign next to **Software Updates**. All updates currently installed on the P2000 Server are listed under this option.
4. To view detailed update information, select an update in the list and click **Edit**. The Software Update dialog box opens.



The following information displays:

Name – This is the name of the update. Change the name, if necessary.

Version – Software version number of the selected update.

Service Pack – Number of the service pack provided in the selected update.

Installed – Date and time the selected update was installed on the P2000 Server.

Server Path – P2000 Server directory location that houses the files installed from the update.

Shared Path – The network directory share accessible from workstations that houses the installation files used to update the P2000 workstations.

Command – Executable file that will be launched to update the P2000 workstations.

Status – Update control setting, which enables you to configure the P2000 Server to update its workstations according to one of the following options:

- **Not Available** – Prevents the P2000 Server from updating its workstations. Select this option if you wish to wait before updating the client computers.
- **Optional** – Allows workstation operators to accept or deny a P2000 software update when prompted during login.

IMPORTANT: *The P2000 Server and its workstations must run the same software version and service pack. If operators deny an update to their workstation, the P2000 software may not function correctly.*

- **Required** – Force updates all P2000 workstations in the system. When selected, workstations will not be able to login if they deny a software update.

Note: *After you update the P2000 Server software, the system does not automatically update P2000 workstations (or prompt the operator to install the update) if the workstation operator is currently logged into the P2000 software. The operator must log out and log back into the P2000 software before the software can be automatically updated. To help avoid mismatched software versions between the P2000 Server and its workstations, you may perform a **Force Logoff** command, if necessary, to force the user to log off of a selected workstation, see page 437 for details.*

Note: *After you update the P2000 Server software, the default **Status** setting may vary according to the type of update (for example, new version or service pack). Always verify and change, if necessary, the current **Status** setting after each server update.*

5. In the **Status** drop-down list, change the update control setting, if necessary.
6. Click **OK**.

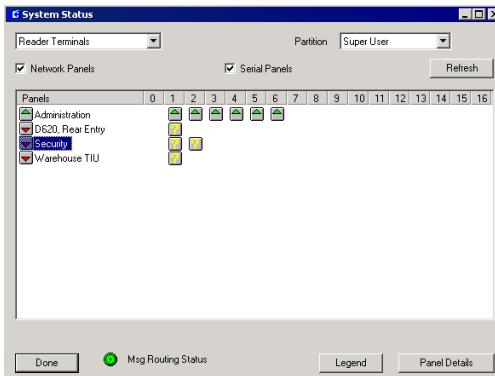
System Status

The System Status window is a dynamic display of the status of panels, associated devices, and other integration components 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 273.

To Access the System Status Window:

- From the P2000 Main menu, select **System>System Status**. The System Status window opens.



- Select a component (Reader Terminals, Input Terminals, Output Terminals, Inputs, Outputs, OTIS Elevator Status, Mustering Zones, Security Level Terminals, Intrusion Areas, Intrusion Zones, Intrusion Annunciators, Fire Zone, Fire Detector, Fire IO Module, Wireless Parameters, or Integration Components) from the drop-down list

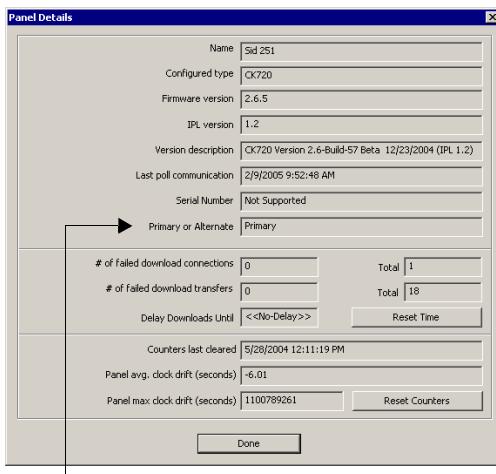
at the top left of the window. Information displayed for each component is presented at the end of this section.

- If this is a partitioned system, select the **Partition** to which the component belongs.
- Select the **Network Panels** and/or **Serial Panels** check box. The list of displayed devices will be limited according to the type of panel selected here.
- Click the **Refresh** button to update the system status display.
- To see icon definitions for the different condition indicators, click the **Legend** button at the bottom of the window.



Note: *Unreliable icons (crossed out with a yellow bar), indicate that the items' parent devices are not functioning. For example, an input point will be marked as unreliable if its parent terminal or panel is down.*

- Click **Done** to close the System Status Legend dialog box.
- To display Serial or Network panel information, select the panel and click the **Panel Details** button. A Panel Details dialog box opens displaying current panel information. (To display information associated with Intrusion panels, go to step 10. For Fire panel information, go to step 13.)



Changes to Polling Direction for Serial Panels

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-DIN panels.

Primary or Alternate – Displays whether the Primary or Alternate connection is in use for a network panel.

Polling Direction – Displays the polling direction (forward or reverse) in which the Server communicates with a legacy panel in a loop configuration.

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.

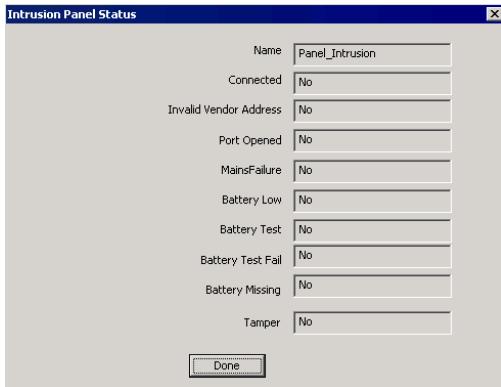
Counters last cleared – Displays the last time you clicked the Reset Counters button.

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.
- To display the status of intrusion panels, select one of the intrusion components (Intrusion Areas, Intrusion Zones or Intrusion Annunciators) from the drop-down list at the top left of the window, the associated intrusion panel displays.
- Select the intrusion panel from the list box, then click the **Panel Details** button. The Intrusion Panel Status dialog box opens.



Name – Displays the name of the intrusion panel.

Connected – Displays whether the panel is connected.

Invalid Vendor Address – Displays whether the vendor address of the intrusion panel is invalid.

Port Opened – Displays whether the intrusion panel port is open.

MainsFailure – Displays whether the maintenance of the intrusion panel has failed.

Battery Low – Displays whether the battery of the intrusion panel is low.

Battery Test – Displays whether the battery of the intrusion panel is in test.

Battery Test Fail – Displays whether the battery of the intrusion panel has failed its test.

Battery Missing – Displays whether the battery of the intrusion panel is missing.

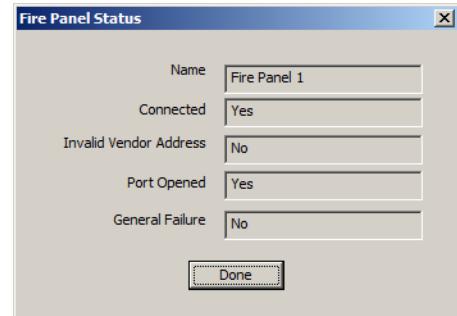
Tamper – Displays whether the intrusion panel has been tampered.

12. Click **Done** to close the Intrusion Panel Status dialog box and return to the System Status window.

13. To display the status of fire alarm panels, select one of the fire alarm components

(Fire Zone, Fire Detector or Fire IO Module) from the drop-down list at the top left of the window, the associated fire alarm panel displays.

14. Select the fire alarm panel from the list box, then click the **Panel Details** button. The Fire Panel Status dialog box opens.



Name – Displays the name of the fire alarm panel.

Connected – Displays whether the fire alarm panel is connected.

Invalid Vendor Address – Displays whether the vendor address of the fire alarm panel is invalid.

Port Opened – Displays whether the fire alarm panel port is open.

General Failure – Displays whether the fire alarm panel has failed.

15. Click **Done** to close the Fire Panel Status 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.

16. Click **Done** to close the System Status window.

System Status – Reader Terminals

When you select **Reader Terminals** from the drop-down list, all panels in the system for the type of panel selected are listed by name in the Panels column. The reader 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. See “Create and Configure Terminals” on page 76 for more information.) When you place the cursor over the terminal icon, the terminal name displays in a popup box.

System Status – Input Terminals

When you select **Input Terminals** from the drop-down list, all panels in the system for the type of panel selected are listed by name in the Panels column.

The input terminals are displayed by number in the same panel row. When you place the cursor over the input terminal icon, the input terminal name displays in a popup box.

System Status – Output Terminals

When you select **Output Terminals** from the drop-down list, all panels in the system for the type of panel selected are listed by name in the Panels column.

The output terminals are displayed by number in the same panel row. When you place the cursor over the output terminal icon, the output terminal name displays in a popup box.

System Status – Inputs

When you select **Inputs** from the drop-down list, all terminals and panels in the system for the type of panel selected, are listed by name in the Terminals/Panels column.

A status icon is represented for each possible input state. If no icons are present, no input points are associated with the terminal/panel.

The input points are displayed by number in the terminal or panel row. When you place the cursor over the input point icon, the input point name displays in a popup box.

All input points above 16 are reserved for Soft inputs. You can expand the size of the window to view these inputs (up to 25).

System Status – Outputs

When you select **Outputs** from the drop-down list, all I/O terminals in the system for the type of panel selected 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: You must select the “Log Output Status Message” option to display outputs in the System Status list (see pages 70, 81, and 153).

System Status - OTIS Elevator Status

When you select **OTIS Elevator Status** from the drop-down list, all Otis elevator servers in the system are listed by name. The individual status icon indicates if the associated Otis Destination Entry Computers is Up or Down.

System Status – Mustering Zones

When you select **Mustering Zones** from the drop-down list, the system displays the zone hardware status of each Muster Zone. See “Muster Zone Status and Control Field Definitions” on page 297.

System Status – Security Level Terminals

When you select **Security Level Terminals** from the drop-down list, 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.

System Status – Intrusion Areas

When you select **Intrusion Areas** from the drop-down list, all intrusion areas associated to the intrusion panel are displayed in the same row as their panel indicating their current status. You can issue commands for the areas by right-clicking the associated status icon. The following commands may be available, depending on the current state of the area:

Arm – Arms the selected area if at the time that you issue the command the area's state permits it.

Forced Arm – Arms the selected area regardless of the area's state at the time when you issue the command.

Disarm – Disarms the selected area.

System Status – Intrusion Zones

When you select **Intrusion Zones** from the drop-down list, all intrusion zones associated to the intrusion panel are displayed in the same row as their panel indicating their current status. You can issue commands for the zones by right-clicking the associated status icon. The following commands may be available, depending on the current state of the zone:

Bypass On – Commands the selected zone to be bypassed.

Bypass Off – Turns off bypassing of the selected zone.

Reset – Resets the state of the selected zone. If you issue this command while the input point is still in alarm due to still being unsealed, you must seal the input and send this command again to reset it.

ResetAck – Resets the state of the selected zone. If you issue this command while the input point is still in alarm due to still being unsealed, there is no need to re-send the command after the input is sealed. The command will remain valid and reset the zone as soon as the input seals.

System Status – Intrusion Annunciators

When you select **Intrusion Annunciators** from the drop-down list, all intrusion annunciators associated to the intrusion panel are displayed in the same row as their panel indicating their current status. You can issue commands for the annunciators by right-clicking the associated status icon. The following commands may be available, depending on the current state of the annunciator:

Activate – Activates the selected annunciator.

Deactivate – Deactivates the selected annunciator.

System Status – Fire Zone

When you select **Fire Zone** from the drop-down list, all fire zones associated to the fire alarm panel are displayed in the same row as their panel indicating their current status. The fire zones are displayed by number. You can display the status of up to 20 fire zones per row. If more than 20 fire zones are defined,

they will display in the following rows. Place the cursor over a fire zone icon to display the fire zone name. You can issue commands for the fire zones by right-clicking the associated status icon. The following commands may be available, depending on the current state of the zone:

Disable Zone – Disables the selected fire zone(s).

Enable Zone – Enables the selected fire zone(s).

System Status – Fire Detector

When you select **Fire Detector** from the drop-down list, all fire detectors associated to the fire alarm panel are displayed in the same row as their panel indicating their current status. The fire detectors are displayed by number. You can display the status of up to 20 fire detectors per row. If more than 20 fire detectors are defined, they will display in the following rows. Place the cursor over a fire detector icon to display the fire detector name. You can issue commands for the fire detectors by right-clicking the associated status icon. The following commands may be available, depending on the current state of the detector:

Disable Detector – Disables the selected fire detector(s).

Enable Detector – Enables the selected fire detector(s).

System Status – Fire IO Module

When you select **Fire IO Module** from the drop-down list, all fire IO modules associated to the fire alarm panel are displayed in the same row as their panel indicating their current status. The fire IO modules are displayed by number. You can display the status of up to 20 fire IO modules per row. If more than 20 fire IO modules are defined, they will display in

the following rows. Place the cursor over a fire IO module icon to display the fire IO module name. You can issue commands for the fire input/output modules by right-clicking the associated status icon. The following commands may be available, depending on the current state of the IO module:

Disable Module – Disables the selected fire input/output module(s).

Enable Module – Enables the selected fire input/output module(s).

Activate Module – Activates the selected output of a fire input/output module(s).

Deactivate Module – Deactivates the selected output of a fire input/output module(s).

System Status – Wireless Parameters

In addition to the normal Up, Down, or Override status of OSI devices, you can also verify status values of OSI devices that are related to the wireless signal they receive. When you select **Wireless Parameters** from the drop-down list, the list box displays the signal strength, packet ratio, and battery voltage values that are reported by the OSI devices.

These parameters are only updated by the reader about every 30 minutes (to conserve battery power). The System Status window will automatically refresh itself approximately every 30 seconds.

Terminals	Time	Overall Signal	Packet Ratio	Reader Signal	Reader Ratio	Batt Voltage	Fwd Voltage
Brown Hall 2nd Floor Star 3	4/26/2007 9:00:41 AM	99.5	45	100.0	5.000	0.000	0.000
Brown Hall 5th Floor Star 2	4/26/2007 9:05:45 AM	99.3	47	99.5	5.213	0.007	0.000
Brown Hall 3rd Floor Star 2	4/26/2007 9:09:45 AM	99.4	48	99.4	5.194	0.000	0.000
Brown Hall 2nd Floor Star 1	4/26/2007 9:31:16 AM	99.7	51	99.8	5.176	0.000	0.000
Brown Hall 2nd Floor Star 2	4/26/2007 9:41:25 AM	99.8	53	99.9	5.368	0.007	0.000
C01 TEST READER	4/26/2007 9:43:36 AM	100.0	57	99.4	5.980	0.000	0.000
Brown Hall 1st Floor Star 2	4/26/2007 9:45:46 AM	99.5	58	99.5	5.100	0.000	0.000
Brown Hall 1st Floor Star 2	4/26/2007 9:52:04 AM	99.0	45	97.9	5.060	0.007	0.000
Brown Hall 3rd Floor Star 2	4/26/2007 9:59:12 AM	99.2	66	97.3	5.140	0.000	0.000
Brown Hall 4th Floor Star 3	4/26/2007 9:59:14 AM	99.1	47	99.2	5.040	0.000	0.000
Brown Hall 4th Floor Star 3	4/26/2007 9:59:36 AM	99.1	47	99.5	5.077	0.000	0.000
Brown Hall 3rd Floor Star 3	4/19/2007 5:49:49 PM	94.2	79	93.3	5.050	0.000	0.000
Brown Hall 3rd Floor Star 3	4/26/2007 9:53:47 AM	99.0	45	99.9	5.740	0.004	0.000
Brown Hall 5th Floor Star 1	4/26/2007 9:53:53 AM	99.1	45	99.1	5.140	0.000	0.000
Brown Hall 1st FDR	4/26/2007 9:54:09 AM	99.1	44.2	99.8	5.023	0.000	0.000

The Wireless Parameters display can be sorted by any column by clicking on the desired column header.

Green bars indicate that the OSI devices are operating within acceptable parameters. **Yellow** bars indicate a weakness in the devices (you will want to investigate further to determine the cause and if corrective action is required). **Red** bars indicate a fatal breakdown in the OSI devices.

The display indicates the following status values for each OSI reader:

Portal Signal Strength and Reader Signal Strength

Strength – These values indicate the Radio Frequency (RF) signal level being received by the portal and reader respectively as measured in decibel milliwatts (dBm). The signal level is affected by the distance between the portal and reader and the type number of obstructions between the portal and reader. Walls and doors between the portal and reader will reduce the signal level especially if they contain metal. A signal level of -50 dBm or higher is considered good. A signal level of -70 to -50 dBm is considered marginal. A signal level of below -70 dBm is considered unacceptable and needs to be corrected to ensure proper operation. Improving signal strength is a physical installation issue and is different for every installation. Techniques for improving signal strength include reducing the distance from portal to reader, moving the portal to a location with fewer obstructions between it and the reader, installing additional portals, and changing the portal antenna to a high-gain directional antenna.

Portal Packet Ratio and Reader Packet Ratio

These values indicate the ratio of good to invalid data packets received from the wireless signal as measured in percentage. The packet ratio is affected by signal strength and external interference. A packet ratio of 50 to 100% is considered good. A packet ratio of 30 to 50% is marginal and should be improved for optimum operation. A packet ratio of less than 30% is considered unacceptable and may prevent proper operation. If both the portal and reader are reporting good signal strength levels but either the portal or reader is reporting a poor packet ratio, it usually indicates some type of interference. Typical causes of interference are electrical noise from other electrical equipment (large electrical motors or microwave ovens), nearby strong RF transmissions (radio or TV station transmitting antennas), or other wireless equipment or networks (Wi-Fi wireless networks or cordless phones). Moving the portal to a different position further away from interfering sources may help. Another solution may be to change the RF channels used by the portal for communicating with the readers.

Battery Voltage – This value indicates the current voltage from the reader's batteries. As the batteries are depleted, the reported voltage will drop. Weak batteries can effect the wireless communication if the reader is seeing low signal strength or if there is large amounts of interference. If the voltage drops too low, the reader will shutdown. A voltage of 5.0 volts or higher is considered good. A voltage of 4.5 to 5.0 volts is considered marginal and the batteries should be replaced soon. A voltage of below 4.5 volts is considered unacceptable and the batteries must be replaced as soon as possible or the reader may shutdown.

External Voltage – Displays the voltage of the external power supply.

Note: The OSI portal has the capability to communicate with the reader over 16 different RF channels or frequency bands. These channels can be configured thru the Web UI of the portal. By default, all 16 channels are enabled in the portal. The portal will use the first configured channel that it finds available. The reader will scan thru all 16 channels until it is able to establish communication with the portal over that channel. By enabling only one or two channels on the portal, you can control the frequency bands used for communication. Using a different channel may isolate the portal and reader from the interfering frequency. In particular, channels 25 and 26 are outside the frequency bands used by Wi-Fi networks and therefore good choices if a Wi-Fi network is suspected to be causing your interference.

System Status - Integration Components

Select **Integration Components** from the drop-down list to display the status of all Assa Abloy Door Service Routers (DSR) configured in the system. The status column indicates one of the following states:

Unknown – The status of the DSR has not yet been determined.

Up – The P2000 system is able to communicate with the DSR.

Down – The P2000 system is not able to communicate with the DSR.

Disabled – The P2000 system has been instructed not to communicate with the interface.

Writing CK7xx Database to Flash Memory

CK721-A 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 CK7xx 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.

This function **must** always be performed after:

- Adding or deleting RDR2SA or RDR8S terminals.
- Modifying general parameters of existing RDR2SA or RDR8S terminals (except Name, Public, or Query String fields).
- Adding or deleting RDR2SA or RDR8S input or output points.

Since the data stored at each panel is different, this procedure must be performed for each panel in the system (CK705, CK720, CK721, or CK721-A panels only).

This function is password protected and must be performed only by a system administrator.

To Manually Write CK7xx Database to Flash Memory:

1. From the P2000 Main menu, select **System>CK705/CK720 Write DB To Flash**. You may be prompted for a password. The CK705/CK720 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 CK7xx Panels

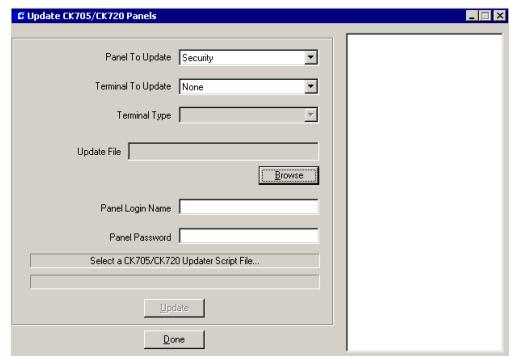
This function updates CK705, CK720, CK721, or CK721-A panel firmware. In addition, you can also update terminal firmware, as long as the terminals are installed into panels of version 2.3 or higher. Johnson Controls will provide the update file, along with documented instructions. This function should be performed only by a system administrator at the Server, and is password protected.

This function requires the login names and passwords of all panels in the system. The default panel name and password for the panel is given in the panel's Installation and Operation manual. If your panel's login name has been changed, you must enter the new name and password to perform this function.

Note: *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 CK7xx 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.
6. Select the file. The file name will display in the **Update File** field.
7. Enter the **Panel Login Name** as programmed at the panel.
8. Enter the **Panel Password** as programmed at the 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.

Note: *The firmware update process requires waiting for the current terminal firmware update to complete before proceeding to update the next terminal. Do not attempt to update multiple terminals at the same time.*

10. After the update process is complete, select another terminal name and type and click **Update**.

Note: During the terminal firmware update process, all terminals connected to a CK721-A panel will go offline. If the Facility Code Only when Offline flag is configured, the offline terminals will allow access.

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 429 to download data items to the recently updated panel.

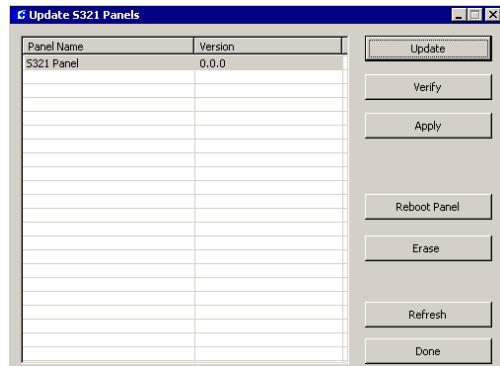
Updating S321-DIN Panels

This function updates S321-DIN 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.

Note: 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-DIN Panels:

1. From the P2000 Main menu, select **System>Update S321 Panels**. You may be prompted for a password. The Update S321 Panels dialog box opens.



2. 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.

3. Click the **Update** button to navigate to the directory in which the update file resides. This file will be typically provided by Johnson Controls.
4. Select the <name>.bz2 file and click **Open**. The information contained in the update file is queued. You can monitor the download progress via the Download Status dialog box. This process may take several minutes. After this process is completed, the Real Time List will display a *Code Image download success* message.
5. If the *Code Image download success message* is not reported after several minutes, click the **Reboot Panel** button. After the panel reboots and reports back online (approximately 30 seconds), repeat step 4.

6. 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.
7. 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.
8. 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 429.

9. After the update process is complete, click **Done** to close the dialog box.

Database Maintenance

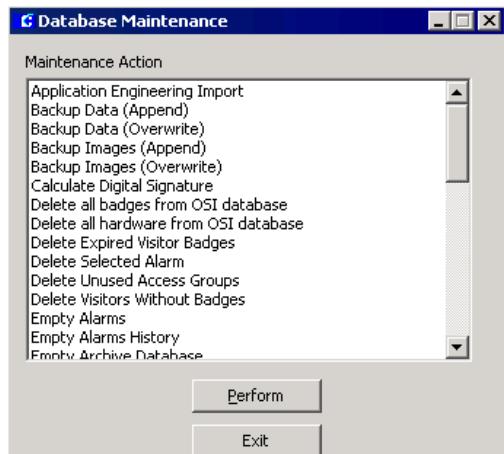
You can perform a database backup, empty various data histories, load an archived database from backup, or reset event counters from the Database Maintenance dialog box. This function is password protected and should be accessible only by a system administrator or a designee.

Some Database Maintenance tasks, such as “Shrink Database,” can only be performed by operators that are members of the Windows or PEGASYS Administrators group, see “Setting Up User Accounts” on page 30.

You may have scheduled certain functions like database backup or Empty Audit History to occur automatically. This option lets you override the system and perform manual maintenance.

To Perform Database Maintenance Functions:

1. From the P2000 Main menu, select **System>Database Maintenance**. You may be prompted to enter a password. The Database Maintenance dialog box opens.



2. Under **Maintenance Action**, select the function you wish to perform. See the next section, “Database Maintenance Actions” for a description of each function.
3. Click **Perform**. A confirming message box will display. Depending on your selection, click the appropriate action.
4. Click **Exit**.

Database Maintenance Actions

Application Engineering Import – Imports a file from JCI Applications Engineering that provide baseline hardware configuration data for P2000.

Backup Data (Append) – Creates a backup of P2000 data without overwriting existing backups. For example, backing up data each day for an entire week will result in a single backup file containing data from each day the backup was performed.

Backup Data (Overwrite) – Creates a backup of P2000 data by overwriting existing backups. For example, backing up data each day for an entire week will result in a single backup file containing data only from the last day the backup was performed.

Backup Images (Append) – Creates a backup of P2000 images without overwriting existing backups. For example, backing up images each day for an entire week will result in a single backup file containing images from each day the backup was performed.

Backup Images (Overwrite) – Creates a backup of P2000 images by overwriting existing backups. For example, backing up images each day for an entire week will result in a single backup file containing images only from the last day the backup was performed.

Note: For more information on the previous Backup functions, see “Database Backup” on page 452.

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 facility uses the FDA Part 11 feature. See “FDA Part 11” on page 395 and “System Validation” on page 458.

Delete all badges from OSI database – All badges will be deleted from the OSI database.

Delete all hardware from OSI database – All hardware will be deleted from the OSI database.

Delete Expired Visitor Badges – All visitor badges that have expired will be deleted from the database. Each visitor badge has a *Visitor Validity Period* (defined in Site Parameters), during which the badge is valid.

Delete Selected Alarm – Deletes the selected alarm from the database.

Delete Unused Access Groups – All unused access groups (access groups not assigned to any badge) will be deleted from the database.

Delete Visitors Without Badges – All visitors who have no assigned badges 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.

IMPORTANT: 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.

IMPORTANT: The Empty Alarms History and Empty Audit History actions should only be performed with the aid of a Johnson Controls Technical Support specialist.

Empty Archive Database – Removes the data from the Archive Database. This database is used for running P2000 reports.

Empty Audit History – Purges all audit history data from the database. The audit history data is time/date stamped records of user actions.

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 Fire Data – Purges all fire alarm panel data from the database.

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, see “Guard Tour Notes” on page 365.

Empty Intrusion Data – Purges all the intrusion data from the database.

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, see “Smart Download Control” on page 431.

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.

IMPORTANT: *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, see “FDA Part 11 Backups” on page 455.

Kill All Reports – Attempts to stop all database queries issued by a P2000 report. This is helpful if an operator accidentally tries to run an extreme report, such as all transaction history for the last two years. This action is not guaranteed to work in all cases.

Load Archive Database from Backup – Loads the data from the Archive Database. This database is used for running P2000 reports.

Mark Secondary Tables – Marks the starting point of FDA data for later analysis.

Migrate Panel – Allows you to change the panel type from D6xx or S320 to a specified CK705, CK720, CK721, CK721-A panel or STI-MUX to match the new hardware installed in the field. The former panel’s settings, such as associated terminals, output points, and input points, will be applied to the new panel.

Remove Access Groups from Disabled Badges – Removes access groups from disabled badges. This in turn allows the Delete Unused Access Groups command to be used more efficiently.

Remove Expired Access Groups from Badges – Removes from badges any access group assignment that is past its Temporary Access Period Void date.

Reset Counters to Zero – All values in the Event Counters list will be reset to zero. For information, see “Counting Events” on page 319.

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 (for example, for maintenance) and alarms are being generated.

Set all Output Status to Unknown – Used if a panel is down (for example, for maintenance) and alarms are being generated.

Set all Panel Status to Unknown – Used if a panel is down (for example, for maintenance) and alarms are being generated.

Set all Terminal Status to Unknown – Used if a panel is down (for example, for maintenance) and alarms are being generated.

Set Computer Default Language – This task is to be used on P2000 systems operating in a foreign language, and allows you to change the P2000 default language for all users using this computer. This will also set the language in which the P2000 services operate.

Shrink Database – Commands SQL Server to free up space in the database. This process is normally performed automatically at various intervals.

Sync cardholder/badge active flags – Synchronizes the cardholder/badge active flags, in case this uncommon problem occurs.

Synchronize OSI Transaction Counter – Sets the P2000 transaction counter to the last transaction currently in the OSI WAMS database. It would typically be used only if the OSI WAMS database was destroyed and recreated. You must stop the P2000 OSI Interface Service before performing this task. After the task is run, restart the P2000 OSI Interface Service.

IMPORTANT: *This action should only be performed with the aid of a Johnson Controls Technical Support specialist because it can cause transactions to be processed multiple times.*

Update Database Default Strings – This task is to be used on P2000 systems operating in a foreign language and causes all default data in the database (such as “Super User” partition, “Super User” menu permission group, default icon image set names, etc.) to be rewritten to the database in the current P2000 language.

Update Preprocessed Report Archive tables – Perform this action if you wish to run a Preprocessed report against an archived database.

Update Preprocessed Report tables – Normally, this process occurs automatically each night. However, if the data has changed and you wish to run a Preprocessed report with current data, you may manually start this process.

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 facility uses the FDA Part 11 feature. See “FDA Part 11” on page 395 and “System Validation” on page 458.

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.

The P2000 Data database should be backed up frequently, while the P2000 Images database should only be backed up when cardholder images are modified. Backups can be performed without stopping the P2000 communication services; therefore, the system will remain operational during the backup process.

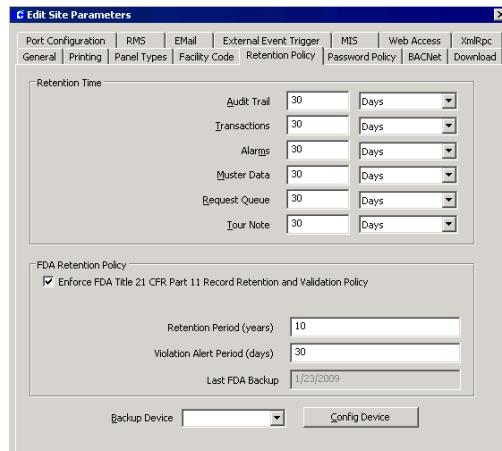
This function should be performed by a system administrator.

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.

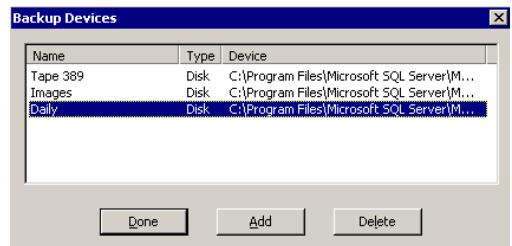
Configuring a Backup Device

- 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.

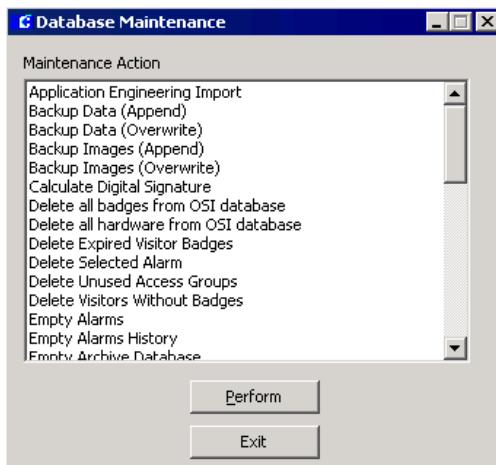


- Enter a descriptive **Name** for the device.
- Select the **Type** of backup device from the drop-down list. Options include: Disk, Tape, and Pipe.
- If you select **Disk**, you must enter in the Disk File box, a valid path and file name for the backup file.
- If you select **Tape**, click the drop-down button in the Tape Drive box, and select from the available Windows tape devices.
- 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 opens.



2. Select **Backup Data** or **Backup Images** (Append or Overwrite) from the Maintenance Action list to backup the P2000 Data or the P2000 Images database.
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.

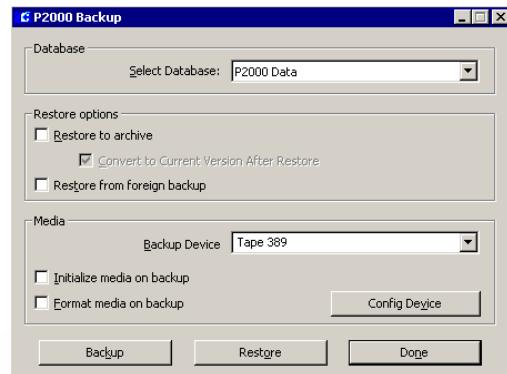
5. Click **Exit** to close the Database Maintenance dialog box.

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.

1. From your Windows desktop, select **Start>Programs>Johnson Controls>P2000>Database Backup**. The P2000 Backup dialog box opens.



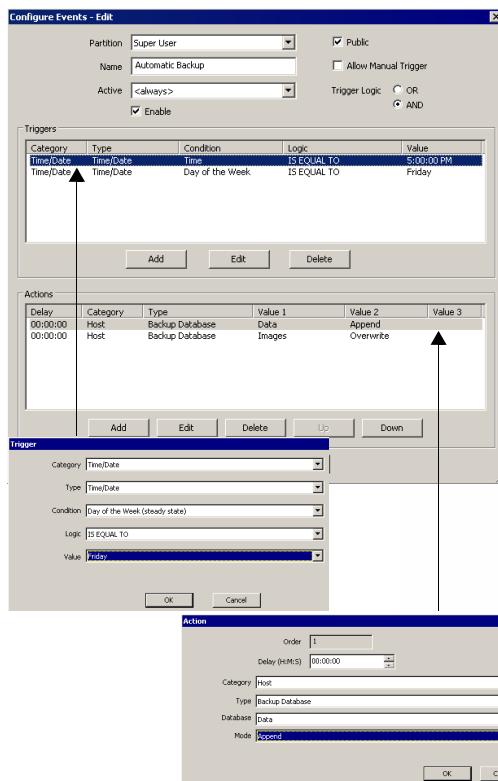
2. From the **Select Database** drop-down list, select either **P2000 Data** or **P2000 Badge Images**.
3. In the **Media** box, select a **Backup Device** from the drop-down list. If you wish to add a new device, click the **Config Device** button and follow the steps provided in “Configuring a Backup Device” on page 453.

Note: The **Initialize media on backup** and **Format media on backup** options are provided to allow old backup media to be reused. For more information on these options, refer to the Microsoft SQL Server documentation.

4. Click **Backup** to start the backup process.
5. 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, see “Creating Events” on page 314.



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.

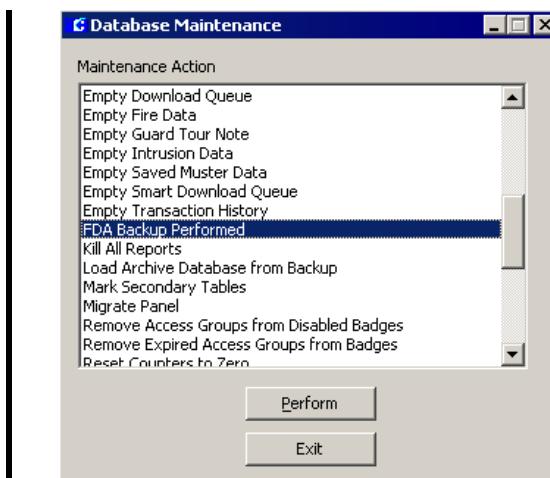
In the Actions box, two actions have been defined: one to backup the Data database, and the second to backup the Images database. Make sure you select Category “Host” and Type “Backup Database” in the Action dialog box.

FDA Part 11 Backups

Depending on the parameters defined in the Retention Policy tab of Site Parameters (page 46), 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 452.

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.

1. From the P2000 Main menu, select **System>Database Maintenance**. You may be prompted to enter a password. The Database Maintenance dialog box opens.



2. Select **FDA Backup Performed** from the Maintenance Action list.
3. Click **Perform**. Since this action cannot be undone, a verification message displays to confirm your action. Click **Yes** to continue.
4. 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 system updates the *Last FDA Backup* field in the Retention Policy tab of Site Parameters (see page 46), to match the current system date. Any FDA Retention Policy alarms will change their alarm status to *Secure*.
5. 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 print-

ing reports or examining old settings, without affecting the currently active P2000 system.

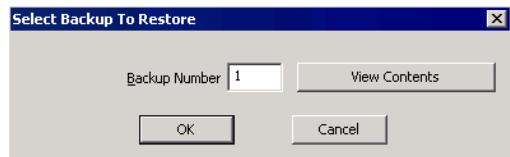
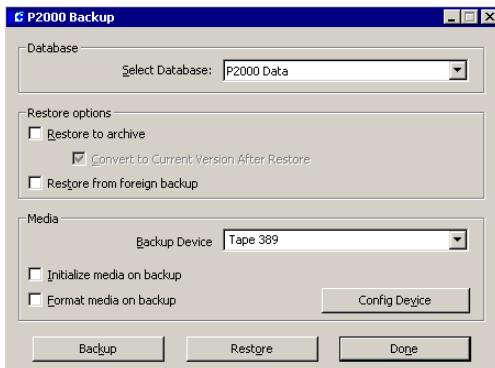
IMPORTANT: Restoring the database can only be performed at the Server. If you restore the database to a different Server other than where it was originally backed up, you will need to contact Technical Support for a new Registration Key, and you will also need to reconfigure your Server (DB and COMM), see “Site Parameters” on page 40.

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 435).

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 task-bar), 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 429).

To Restore the Database:

1. From your Windows desktop, select **Start>Programs>Johnson Controls>P2000>Database Backup**. The P2000 Backup dialog box opens.



7. Click **View Contents**. The Backup Contents dialog box opens.

Number	Date	Name
1	4/30/2007 4:11:33 PM	P2000 Images Backup 4/30/2007 4:11:3..
2	7/26/2007 11:34:01 AM	P2000 Images Backup 7/26/2007 11:34:..
3	12/10/2007 3:37:29 PM	P2000 Data Backup 12/10/2007 3:37:29..
4	3/12/2009 1:11:53 PM	P2000 Images Backup 3/12/2009 1:11:5..
5	3/12/2009 1:58:34 PM	P2000 Data Backup 3/12/2009 1:58:33 PM

8. Select the backup you wish to restore, and click **OK**.
9. A message will notify you that the restore process has been completed, click **OK** to return to the P2000 Backup dialog box.
10. Click **Done** to close the P2000 Backup dialog box.

Note: *The Restore from foreign backup 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.*

6. Click **Restore** to start the restore process. The Select Backup To Restore dialog box opens.

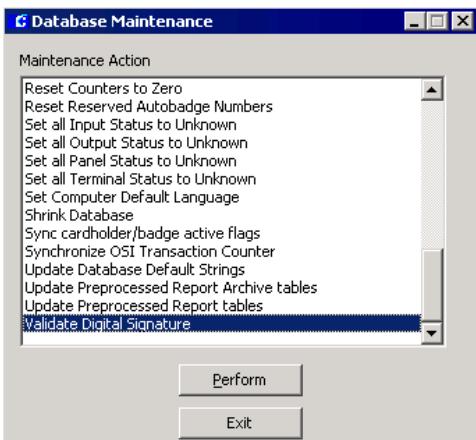
Note: *After the database is restored, use the Service Startup Configuration application to enable or disable P2000 services as well as define the related recovery actions that were set up prior to the database restore, see page 432.*

System Validation

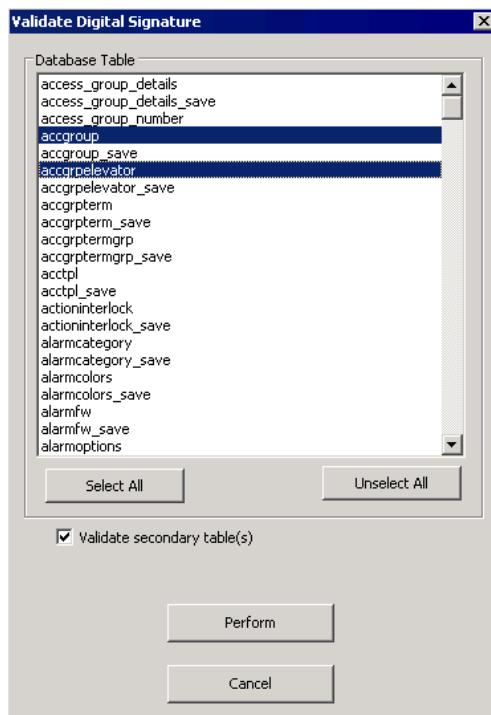
As a system administrator, you should schedule validation of your system on a regular basis to minimize the possibility of record tampering. The Validate Digital Signature feature ensures the integrity of all records and provides evidence when records have been altered. This function is available if your facility uses the FDA Part 11 feature. See “FDA Part 11” on page 395.

Note: A digital signature verifies that unauthorized users have not modified the values in the columns of a record.

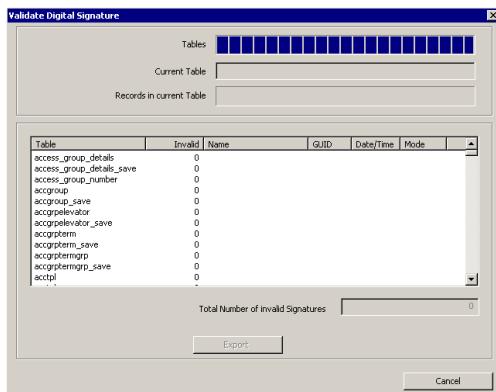
- From the P2000 Main menu, select **System>Database Maintenance**. You may be prompted to enter a password. The Database Maintenance dialog box opens.



- Select **Validate Digital Signature** from the Maintenance Action list.
- Click **Perform**. The Validate Digital Signature dialog box opens.



- 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.
- To clear your selections, click the **Unselect All** button.
- 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 if you wish to remove all secondary tables from the list.
- 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 cardholder 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 a 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 (see “Web Access” on page 409).

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 operators 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 46.

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 411.

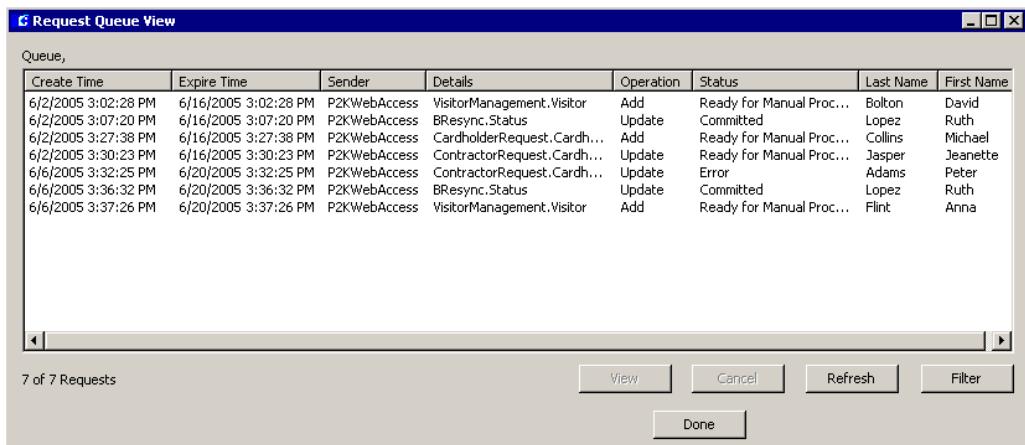
Sender – Displays the source that originated the request.

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 operator intervention.
- Ready for Manual Processing** – This request has been approved and is ready for manual processing.
- Rejected** – The request was rejected.



The screenshot shows a Windows-style dialog box titled "Request Queue View". The title bar includes standard window controls (minimize, maximize, close). The main area is a table titled "Queue," displaying 7 rows of request data. The columns are: Create Time, Expire Time, Sender, Details, Operation, Status, Last Name, and First Name. The data is as follows:

Create Time	Expire Time	Sender	Details	Operation	Status	Last Name	First Name
6/2/2005 3:02:28 PM	6/16/2005 3:02:28 PM	P2KWebAccess	VisitorManagement.Visitor	Add	Ready for Manual Proc...	Bolton	David
6/2/2005 3:07:20 PM	6/16/2005 3:07:20 PM	P2KWebAccess	BResync.Status	Update	Committed	Lopez	Ruth
6/2/2005 3:27:38 PM	6/16/2005 3:27:38 PM	P2KWebAccess	CardholderRequest.Cardh...	Add	Ready for Manual Proc...	Collins	Michael
6/2/2005 3:30:23 PM	6/16/2005 3:30:23 PM	P2KWebAccess	ContractorRequest.Cardh...	Update	Ready for Manual Proc...	Jasper	Jeanette
6/6/2005 3:32:25 PM	6/20/2005 3:32:25 PM	P2KWebAccess	ContractorRequest.Cardh...	Update	Error	Adams	Peter
6/6/2005 3:36:32 PM	6/20/2005 3:36:32 PM	P2KWebAccess	BResync.Status	Update	Committed	Lopez	Ruth
6/6/2005 3:37:26 PM	6/20/2005 3:37:26 PM	P2KWebAccess	VisitorManagement.Visitor	Add	Ready for Manual Proc...	Flint	Anna

At the bottom left, it says "7 of 7 Requests". At the bottom right are buttons for "View", "Cancel", "Refresh", "Filter", and "Done".

Last Name – This is the last name of the cardholder specified in the request.

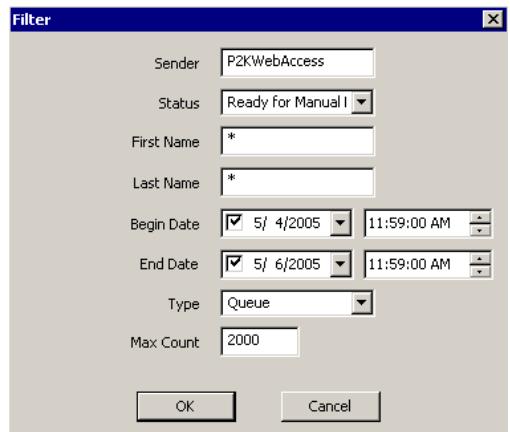
First Name – This is the first name of the cardholder specified in the request.

2. To display the details of a specific request, select the line item in the list box and click the **View** button. See “Viewing Request Details” on page 462.
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.

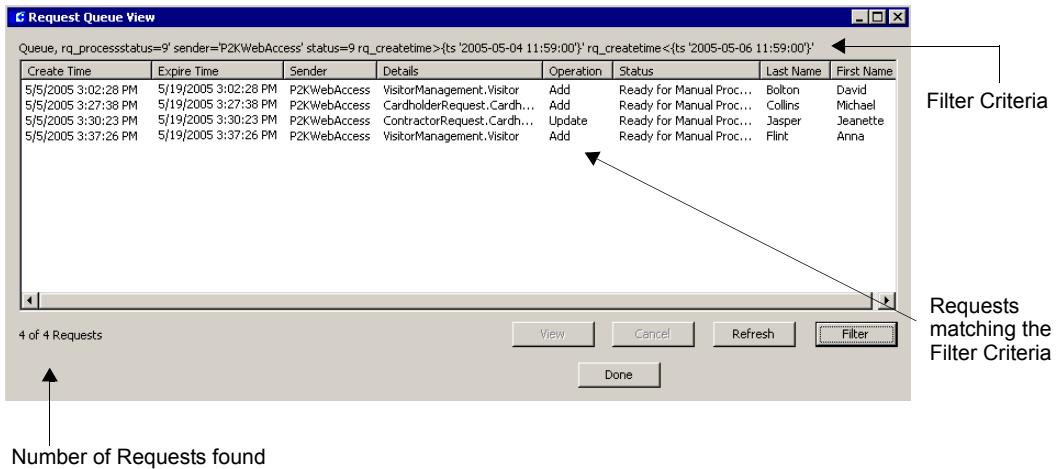
Searching Specific Requests

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.



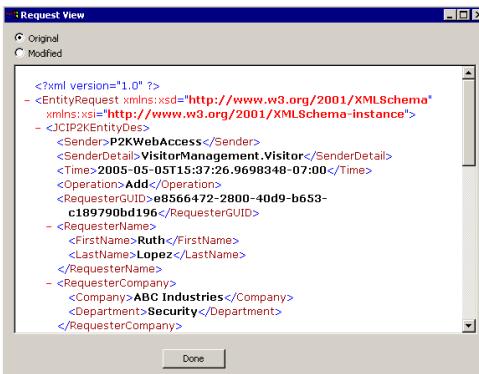
2. Enter a **Sender** name to view only requests that were originated from that source.
3. Select from the **Status** drop-down list the specific request status you wish to view. For example, you may want to review only requests that have been rejected or requests that require manual processing.
4. To view requests submitted for a specific cardholder, enter the **First Name** and/or **Last Name** of that cardholder.
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 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. See the next section “Viewing Request Details”.



- 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

- 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.

The top left side of the window offers two viewing options:

- Original** – Displays request information, as it was originally submitted.
- Modified** – Displays modified request information. For example, if a request is rejected, the requester can edit the request to correct errors and then resubmit the request for processing.

- 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 Cardholder 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 SAP® Crystal Reports®, most of which can be sorted to produce the data you need, and they can be reviewed on screen or printed. See page 466 for a complete list of these reports, a brief description of each, and how to use them. Also, later in this chapter you will find some commonly used reports, including samples of each.

If you do not find a report that meets your needs within P2000 Standard Reports, you can create custom reports using SAP Crystal Reports and then import them into the P2000 system. You can also export a P2000 Standard Report, open it in SAP Crystal Reports, 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 SAP Crystal Reports to create a custom report. See "Creating Custom Reports" on page 477 for detailed information.

This chapter includes the following topics:

- **Using P2000 Standard Reports**
- **P2000 Standard Report Definitions**
- **Selected Sample Reports**
- **Creating Custom Reports**

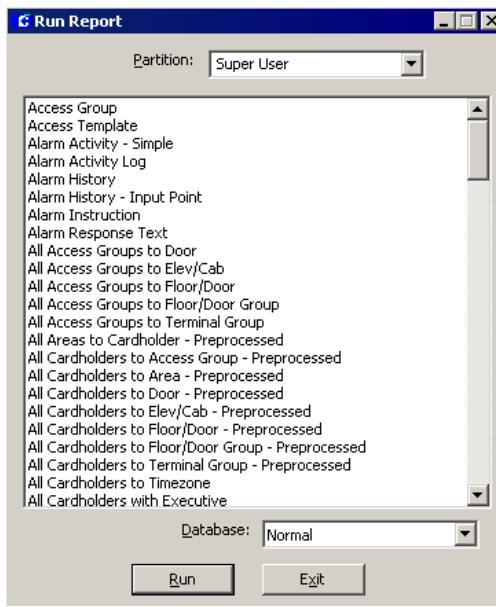
Using P2000 Standard Reports

For most applications, P2000 Standard Reports provide the fields you need to generate reports on system databases and activities. You can easily generate these reports using the Report option on the P2000 Main menu. When you select a report from the list, the report displays on a SAP Crystal Reports preview window. You can use the SAP 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 SAP Crystal Reports.)

Note: The Load Language Reports feature in the Report menu allows you to load reports in different languages. Use this feature if you have installed the language CD in your system. When you select **Report>Load Language Reports** from the P2000 Main menu, a dialog box opens where you select the desired language (previously installed from the foreign language CD), then click **Load** to load the SAP Crystal Reports template into the database. Once the selected language reports are loaded you do not need to perform this procedure again. You may have to modify some translated reports using SAP Crystal Reports to fix truncated text issues. In addition, due to a parameter value limitation in SAP Crystal Reports, some reports have been hard-coded and have not been translated, these reports also need to be modified using SAP Crystal Reports.

To Run a Standard Report:

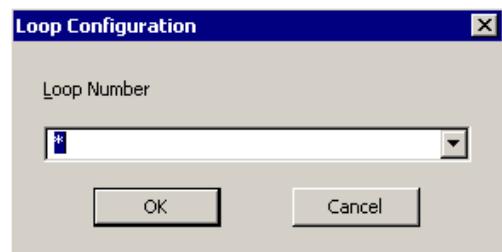
- From the P2000 Main menu, select **Report>Run Report**. The Run Report dialog box opens.



- 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.

Note: Before you run any “Preprocessed” report against an archived database, you must perform the “Update Preprocessed Report Archive tables” task from the Database Maintenance application, see page 449.

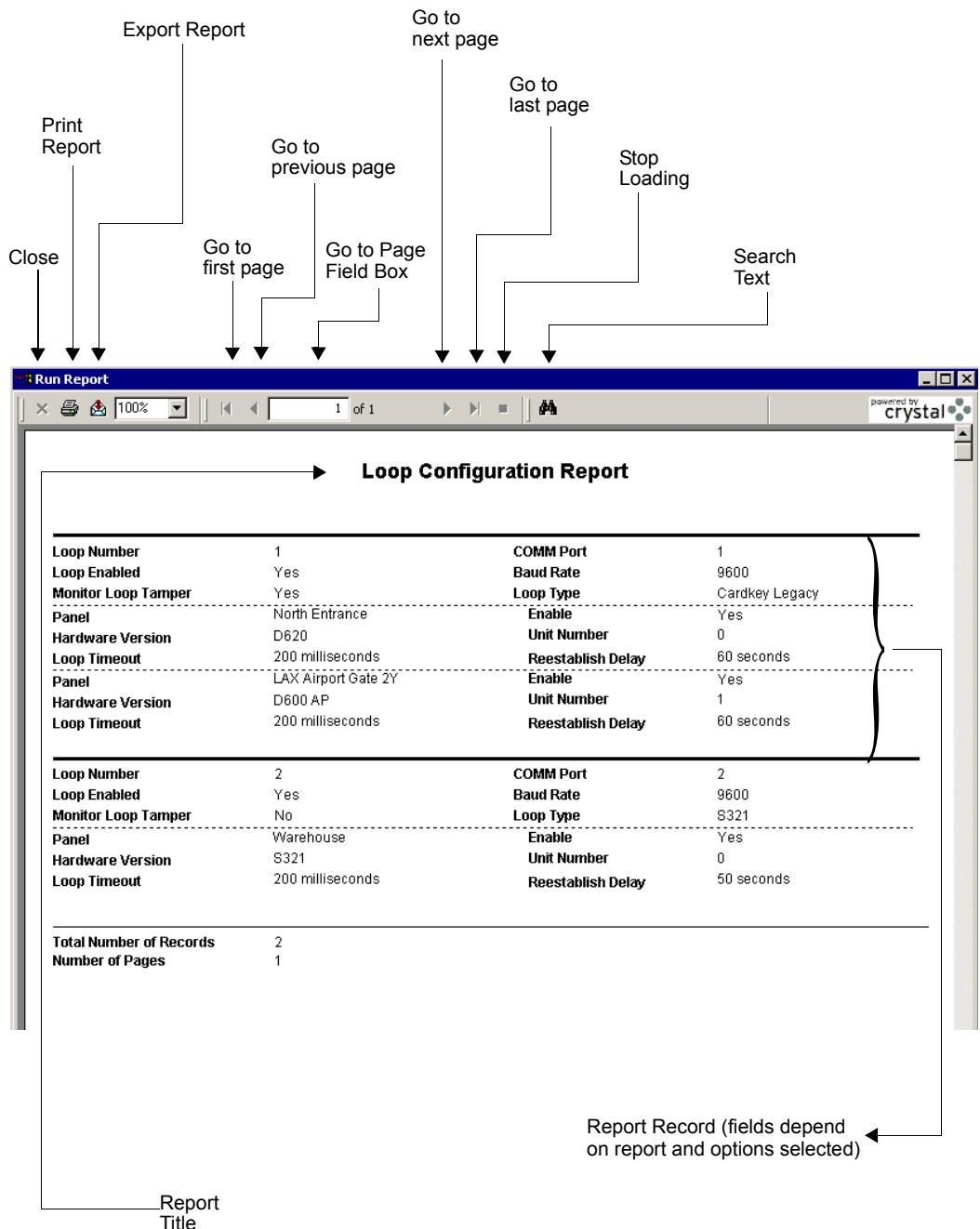
- Click **Run**. Some reports, such as *Message Forwarding*, have no specific options and display directly in the preview window after you click **Run** and enter the printer options. Most reports, however, have several filtering options and present a dialog box in which to select your choices.



- 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 471 for detailed instructions.)
- Click **OK**. Select a printer name and any other printer setup information.

Note: You must configure a default printer to retain the fonts displayed on a report. It is not required to have a printer physically connected to the workstation; you only need to setup the default printer. Do not use “Generic Text” printers. The **No Printer** option in the Print Setup dialog box displays P2000 reports correctly and is selected by default if you have not installed any printer drivers. Alternatively, you can manually select the **No Printer** option if you have installed one or more drivers, but you want to use a generic printer driver.

- Click **OK**. After a moment, the report displays in the Crystal Reports preview window, as shown on the following page.
- Click the Printer icon to print the report. (To use this option, you must set up your system to communicate with a printer. If you need more information, see your system administrator.)



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 feature, 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 any of the audit, alarm or transaction history reports, you have the option of selecting to report transactions at your local site or you can enter the name of the remote site that you want to report on.

Preprocessed reports display current data. Any changes made to database items in a Preprocessed report will not be reflected until the following day, unless you manually update the report table using the *Update Preprocessed Report tables* task in Database Maintenance, see page 449.

Also, report names that start with “RAW” are duplicates of existing reports, with the difference that these RAW reports have been formatted to be exported into an Excel spreadsheet. The preview window for these reports may not display correctly, but the resulting Excel spreadsheet will contain valid data.

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.

Access Template – Lists the details of all access templates created for the system, or you can specify a particular access template.

Alarm Activity - Simple – Lists alarm activities in a simpler format than the Alarm Activity Log report. You can list all alarm activities or select specific alarm category, type, description, associated alarm item; as well as date and time beginning and ending periods.

Alarm Activity Log – Lists all alarm activities, or you can select specific alarm category, type, description, associated alarm item; as well as date and time beginning and ending periods.

Alarm History – Lists all alarm history in the system or you can select specific alarm category, type, description, 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 - Input Point – Similar to the Alarm History report, except that it only displays Panel Input Point alarms, and groups them together by their associated terminal, followed by input point. The alarms are listed for each input point chronologically. This report allows users to see a list of alarms and state changes for the input points that are configured in the system.

Alarm Instruction – Lists all alarm instructions and associated text created for the system.

Alarm Response Text – Lists all response text created for the system.

All Access Groups to Door – Lists all access groups and the door terminals assigned to each, or select a specific terminal.

All Access Groups to Elevator/Cabinet – Lists all access groups and the elevators or cabinets

assigned to each. Select a specific elevator or cabinet name to limit data.

All Access Groups to Floor/Door – Lists all access groups and the floors/doors assigned to each. Select elevator or cabinet and specific floor/door name to limit data.

All Access Groups to Floor/Door Group – Lists all access groups and the floor/door groups assigned to each. Select elevator or cabinet and specific floor/door group name to limit data.

All Access Groups to Terminal Group – Lists all access groups and the terminal groups assigned, or select a specific terminal group.

All Areas to Cardholder - Preprocessed – Lists by cardholder name, all areas the cardholder can access and the terminal doors defined for the area.

All Cardholders to Access Group - Preprocessed – Lists by access group the cardholders assigned to that access group. Select specific access group and badge type.

All Cardholders to Area - Preprocessed – Lists by area name, the cardholders and badges that have access to the area.

All Cardholders to Door - Preprocessed – Lists by door terminal all cardholders that have access to that terminal. Select a specific terminal and cardholder type to limit data.

All Cardholders to Elevator/Cabinet - Preprocessed – Lists all cardholders and the elevators or cabinets assigned to each. Select a specific elevator or cabinet name and the cardholder type to limit data.

All Cardholders to Floor/Door - Preprocessed – Lists all cardholders and the floors/doors assigned to each. Select elevator or cabinet, the floor/door name, and cardholder type.

All Cardholders to Floor/Door Group - Preprocessed – Lists all cardholders and the

floor/door groups assigned to each. Select elevator or cabinet, the floor/ door group name, and cardholder type.

All Cardholders to Terminal Group - Preprocessed – Lists by terminal group all cardholders that have access to that terminal group. Select a specific terminal group and cardholder type to limit data.

All Cardholders to Timezone – Lists by time zone all cardholders assigned to that time zone. Select specific time zone and badge type.

All Cardholders with Executive – Lists the names of all cardholders with executive privileges. You can list active and/or disabled cardholders.

All Doors to Cardholder - Preprocessed – Lists by cardholder name all doors and access groups assigned to the cardholder.

All Elevator/Cabinet to Cardholder - Preprocessed – Lists by cardholder name the elevators or cabinets assigned to the cardholder.

All Floor/Door Groups to Elevator/Cabinet – Lists by elevator or cabinet name all floor or door groups assigned to the elevator or cabinet.

All Floor/Door Groups to Floor/Door – Lists by elevator floor or cabinet door all floor or door groups assigned to the elevator floor or cabinet door.

All Floors/Doors to Cardholder - Preprocessed – Lists by cardholder name all elevator floors or cabinet doors assigned to the cardholder.

All Terminal Groups to Door – Lists by terminal group the terminals (doors) assigned to each group. Select a specific terminal to limit data.

Area Configuration – Lists by area name, all configuration information entered in the Area Configuration dialog box.

Area Control – Lists the cardholders currently in the area, including the total number of cardholders for each count mode.

Area Transaction – Lists all transactions performed in the system for the specific area.

Audit – Lists by operator name the menu items selected by that operator during the date and time period selected.

Auto-badge Number – Lists the number and status of the badges that were created using the AutoBadge Management feature.

AV Camera – Lists all Audio Visual cameras and their associated configuration. Select a specific server and/or switch name to limit the data.

AV Dry Contact – Lists all Audio Visual Dry Contact relays and their configuration. Select a specific server and/or switch name to limit the data.

AV Input Point to Camera – Lists all Audio Visual Input to Camera mappings and their configuration, or select a specific mapping.

AV Monitor – Lists all Audio Visual monitors and their associated configuration. Select a specific server and/or switch name to limit the data.

AV Summary – Lists by name all Audio Visual items defined in the CCTV/AV Configuration window. Select a specific server and/or switch name to limit the data.

AV Switch – Lists all Audio Visual switches and their associated configuration. Select a specific server and/or switch name to limit the data.

Cardholder Entry–Exit Status – Lists cardholder information, the entry/exit times, and status of the badge. This is useful to review cardholder movement throughout the facility.

Cardholder Last Badge – Locates a cardholder by last badging at a terminal (door).

Cardholder Transaction History – Lists transaction history by cardholder, including issue level and timed override parameters. You can select specific cardholder, badge number, terminal, history type, elevator or cabinet transactions, begin and end dates and times.

Cardholder Transaction History - Simple – This report is similar to the Cardholder Transaction History report, except that it is presented in a simpler format.

Cardholders - Preprocessed – Lists by cardholder all personal and system information, including badge numbers, access groups, card options, time zones, etc. (A detailed example of this report is given in the “Selected Sample Reports” section.)

Cardholders - Preprocessed - with UDF – This report is similar to the Cardholders - Preprocessed report, except that it lists any User Defined Fields (UDFs) filled in for that cardholder. Each cardholder record will show only those UDFs that have had data entered into them from the Cardholder window. A record that contains no data in a UDF field will have no UDF entries in this report.

Cardholders - Simple - Preprocessed – This is a simplified version of the Cardholders - Preprocessed report that displays basic cardholder information.

Cardholders - Simple - Preprocessed - with UDF – This report is similar to Cardholders - Simple report plus any UDFs that have data entered.

Cardholders with Web Access - Preprocessed – Lists the cardholders that have been assigned with menu permissions to perform Web Access functions.

Cardholders without Badges – Finds all cardholders in the system without badges assigned. (A detailed example of this report is given in the “Selected Sample Reports” section.)

CCTV Camera – Lists all CCTV cameras and their associated configuration. Select a specific server and/or switch name to limit the data. See “CCTV Reports” on page 394.

CCTV Monitor – Lists all CCTV monitors and their associated configuration. Select a specific server and/or switch name to limit the data. See “CCTV Reports” on page 394.

CCTV Summary – Lists by name all CCTV items defined in the CCTV/AV Configuration window. Select a specific server and/or switch name to limit the data. See “CCTV Reports” on page 394.

CCTV Switch – Lists all CCTV switches and their associated configuration. Select a specific server and/or switch name to limit the data. See “CCTV Reports” on page 394.

Disabled Cardholders and Badges – Lists all cardholders that have been disabled or have disabled/inactive badges.

Elevator/Cabinet Configuration – Lists by elevator or cabinet name all configuration information entered in the Elevator or Cabinet Configuration dialog box for all elevators or cabinets, or select a specific elevator or cabinet, and panel name to limit data.

Elevator/Cabinet Transaction – Lists all transactions performed in the system for the specified elevator or cabinet name.

Enable Code – Lists by panel name (for D600 AP panels only), the Enable Codes used at your facility.

Events – Lists by event name all configuration information entered in the Configure Events dialog box, including event trigger and action information.

Floor/Door Group – Lists all elevator or cabinet floor/door groups and the floor/door masks assigned to each group.

Floor/Door Mask – Lists all elevator or cabinet floor/door masks and the floors/doors assigned to each.

Floor/Door Name – Lists all elevator or cabinet floor/doors and the floor/door numbers and names assigned to each.

Hardware Up/Down Status – Lists the name and status of all operating hardware.

Holiday – List all holidays configured for the system.

Hours on Site – Lists a detailed report of a cardholder’s accumulated number of hours present at a site.

Hours on Site - Simple – Lists a summary report of a cardholder’s accumulated number of hours present at a site.

Input Group – Lists by input group the associated input points and panels, or select a specific input group.

Input Point – Lists by input point all configuration information entered in the Input Point dialog box for all input points, or select a specific input point to limit your search.

Input Point Disable/Suppressible – Lists all input points in the system that are disabled or suppressed.

Loop Configuration – Lists by loop number all loop configuration information entered for all loops, or select a specific loop number to limit your search.

Message Filter – Lists by message filter name all the filtering information entered in the Message Filter Configuration dialog box for all message filters, or select a specific message filter to limit your search.

Message Filter Group – Lists by message filter group the message filters associated with the

message filter group. Select a specific message filter group to limit your search.

Message Forwarding – Lists the workstation names “From” where and “To” where all current messages are forwarded.

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.

Mustering Configuration – Lists by Muster Zone name, all the zone definition configuration, as set up in the Muster Zone Definition dialog box.

Operator – Lists all operator information entered in the Edit Operator dialog box.

Operator Permissions – Lists the permissions assigned to each operator.

Output Group – Lists by output group the associated output points and panels.

Output Point – Lists by output point all configuration information entered in the Output Point dialog box for all output points, or select a specific output point to limit your search.

P900 Counter – Lists all counter information, as set up in the P900 Counters dialog box.

P900 Flag – Lists all flag information, as set up in the P900 Flags dialog box.

P900 System Parameters – Lists the details of the P900 parameters, as set up in the P900 System Parameters dialog box.

P900 Trigger Event – Lists all trigger event information, as set up in the P900 Trigger Event dialog box.

P900 Trigger Link – Lists all trigger link information, as set up in the P900 Trigger Links dialog box.

Panel – Lists all panels in the system with their associated configuration as set up in the Panel dialog box. Select a specific panel to limit the report to that panel. (A detailed example of this report is given in the “Selected Sample Reports” section.)

Panel Card Event – Lists by panel card event name all panel card event details configured for the system. Select a specific panel card event to limit the report to that event.

Remote Server – Lists all remote servers in the system with their associated configuration, as set up in the P2000 Remote Server dialog box.

Security Level Ranges – Lists the security levels defined in the Security Level Range Editor dialog box.

Site Parameters – Lists the details of the current site parameters as set up in System Configuration.

Station – Lists by workstation all workstation configuration.

Terminal – Lists by terminal name all terminal configuration as set up in the Terminal dialog box.

Terminal Groups – Lists by terminal group the terminals associated with the terminal group. Select a specific terminal group to limit your search.

Terminal Unshunted – Lists all terminals with a shunt time of zero.

Time Zone – Lists all Time Zones configured for the system.

Tour Configuration – Lists by tour name, all tour definition configuration, as set up in the Guard Tour Definition window. See “Guard Tour Reports” on page 366.

Tour Notes – Lists all the tour notes assigned to a specific tour name, as set up in the Guard

Tour Control window. See “Guard Tour Reports” on page 366.

Tour Transaction History – Lists all tour transactions performed in the system. See “Guard Tour Reports” on page 366.

Transaction History – Lists all transactions performed in the system. (A detailed example of this report is given in the “Selected Sample Reports” section.)

Unused Active Badges – Displays a list of active badges that have not been used during the specified period of time.

Verification – Allows for a verification of the commissioning process by providing a list of all hardware to be checked off by the contractor. This list includes a list of all panels in the system and their associated terminals, inputs, and outputs.

Selected Sample Reports

Following are detailed instructions on how to run reports. Once you have experimented with these, you should have a good understanding of how to select options and to get the results you need.

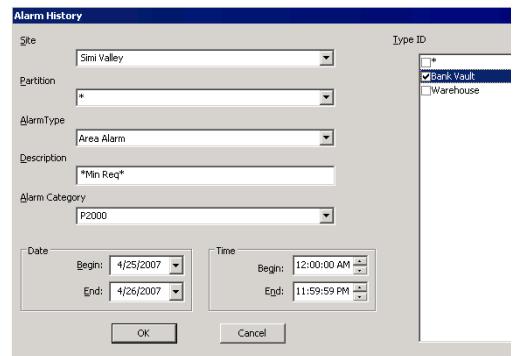
Each example shows a reporting criteria window and the associated report generated from the configuration selected.

Running the Alarm History Report

The Alarm History 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 History** and click **Run**, or double-click **Alarm History**. The Alarm 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 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** represented by an asterisk. Select a specific partition name to gather data only from that partition.
- The default **Alarm Type** entry is **All**, represented by an asterisk. Select a specific Alarm Type to report on only one alarm type in the system.
- The **Type ID** list box displays items that are associated with the selected Alarm Type. The default Type ID is **All**, represented by an asterisk. You can select a specific or multiple Type IDs to report only on those entries selected.
- Enter a **Description** of the alarm. You can use wildcards. For example, you can enter ***Min Req*** to report only on alarms generated when the minimum number of card-

Alarm History Report

Report Filter			
Alarm Type	Area Alarm		
Alarm Device Name	Bank Vault		
Date (>=)	4/25/2007 12:00:00AM		
Date (=)	4/26/2007 11:59:59PM		
Description	*Min Req*		
Site	Simi Valley		
Alarm Category	P2000		
Description	Bank Vault Min Required Alarmed		
Partition	Super User	Public	No
Alarm State	Alarm	Alarm Date	4/26/2007 4:25:15PM
Alarm Status	Pending	Ack Date	4/26/2007 4:25:15PM
Alarm Priority	10	Operator Site	Simi Valley
Escalation	0	Alarm Category	P2000
Operator Name	Cardkey		
Alarm State	Alarm	Alarm Date	4/26/2007 4:25:15PM
Alarm Status	Acked	Ack Date	4/26/2007 4:25:58PM
Alarm Priority	10	Operator Site	Simi Valley
Escalation	0	Alarm Category	P2000
Operator Name	Cardkey		
Alarm State	Alarm	Alarm Date	4/26/2007 4:25:15PM
Alarm Status	Responding	Ack Date	4/26/2007 4:27:14PM
Alarm Priority	10	Operator Site	Simi Valley
Escalation	0	Alarm Category	P2000
Operator Name	Cardkey		
Response Text	Operator Name	Date/Time	
Responded from Security Station	Cardkey	4/26/2007 4:27:14PM	

holders is not present at the same time in the specific Area.

7. The default **Alarm Category** is **P2000**. Select a specific alarm category to report only on the alarm category selected.
8. Select a **Begin** and **End** date for the alarms you wish to see.
9. Select a **Begin** and **End** time for the alarms you wish to see.
10. 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.
11. Click **OK**. The Alarm History report displays in the 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 History dialog box. The report filter options

selected for reporting display 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 4/26/2007 at 4:25:15 P.M.

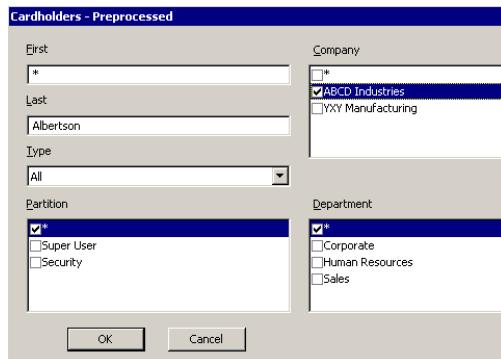
The alarm is in the *Alarm* state and is *Pending*, that is, it has not yet been acknowledged. When the alarm is acknowledged, the report will show that as another date and time-stamped record, with the alarm status as *Acknowledged*, and the *Operator Name* of the person who acknowledged the alarm. The *Operator Site* displays the site name from where the operator handled the alarm.

Running the Cardholders - Preprocessed Report

The Cardholders report gives you information about all the cardholders in the system. This report contains personal, badge, and access information as configured in the Cardholders window.

Note: Preprocessed reports display current data. Any changes made to database items in a Preprocessed report will not be reflected until the following day, unless you manually update the report table using the "Update Preprocessed Report tables" task in Database Maintenance, see page 449.

- From the Run Report list, double-click **Cardholders - Preprocessed**. The Cardholders - Preprocessed dialog box opens.



- The default (*) reports all cardholders. Select a **First** or **Last** name to limit the report to a specific cardholder.
- Select a Cardholder **Type**.
- 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.
- From the **Company** list box, select a specific or multiple company names; or select the * to report on all company names.
- From the **Department** list box, select a specific or multiple department names; or select the * to report on all department names.
- 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.

Cardholders Report			
First Name	*		
Last Name	Albertson		
Card Type (A=All, R=Regular, V=Visitor)	All		
Partition	*		
Company	ABCD Industries		
Department	*		
Partition	Super User	Public	Yes
First Name	Fred	Middle Name	R.
Last Name	Albertson	ID	4899
Company	ABCD Industries	Department	Sales
Address	109B 1440 E. Chapala Street Santa Barbara CA 93103	All Badges	
Phone	555-3322	Start	4/1/2005 8:00:00AM
Ext	312	Void	3/30/2015 11:59:00AM
Guard	No	Card Type (A=All, R=Regular, V=Visitor)	Visitor
Sponsor		E-Mail	FAlbert@xxx.com
First Name	James	Web Access	<none>
Last Name	Jasper		
Middle Name	A.		
Identification Badge			
Badge Number	44561	Issue	0
Badge Alpha	ENG	Description	Lab Identification Only
Start			
Void			
Access Badge			
Badge Number	44562	Badge Reason	New
Badge Alpha	VIS	Design	
Start Date	4/1/2005 8:57:00AM	Void Date	4/1/2005 12:57:00PM
Issue	0	PIN Code	123
Description	North Building Access		
Facility Code	Default Facility Code		

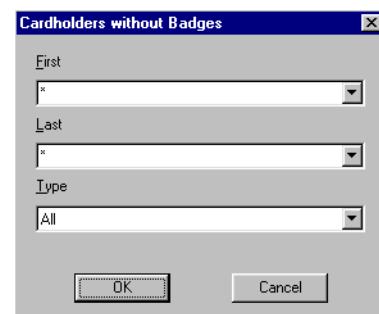
- Click **OK**. The Cardholders report displays in the preview window. You can use the arrows at the top of the window to scroll forward and back through the pages; resize the window for the best display, and print all or single pages of the report.

The top part of the record lists the cardholder's name and personal information, along with Company, Department, Cardholder type, and badge start and void dates. Sponsor information will be included if the cardholder is a visitor. The bottom section of the record lists the badge information associated with the cardholder.

Running the Cardholders without Badges Report

The Cardholders without Badges report is useful to locate cardholders who have no access badges. A popular use is to locate cardholder records that were not deleted when badges were removed.

- From the Run Report list, double-click **Cardholders without Badges**. The Cardholders without Badges dialog box opens.



- The default (*) reports all cardholders. Select a **First** or **Last** name to limit the report to a specific cardholder.
- Select a Cardholder **Type**.
- 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 Cardholder without Badges report displays in the 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.

Cardholders without Badges Report

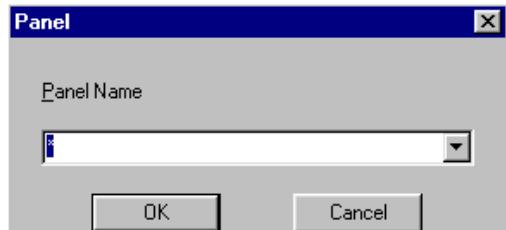
First	*	Last	*
Card Type (A=All, R=Regular, V=Visitor)			
Public	Yes	Partition	Super User
First	Loretta	Middle	W.
Last	Adams	ID	125
Company	YXY Manufacturing	Department	Sales
Address		Start	12/5/2004 8:00:00AM
		Void	2/5/2005 11:59:00AM
		Card Type	Visitor
Phone	222-3333	E-Mail	
Ext	123	Web Access	<none>
Site	Simi Valley		
Guard	No		
Sponsor			
First Name	James	ID	12345
Last Name	Jasper	Phone	555-3333
Middle Name	A.	Ext	123

This report lists the cardholder by first and last name, personal information, along with Company, Department, Cardholder Type, and Start and Void dates. Sponsor information will be included if the cardholder is a visitor.

Running the Panel Report

The Panel Report lists by Panel name the complete panel configuration for each panel in the system. Or you can select a specific panel to report only that panel's configuration.

- From the Run Report list, double-click **Panel**. The Panel dialog box opens.



- The default (*) reports on all panels. Select a **Panel Name** to limit the report to a specific panel.
- 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 Panel report displays in the preview window. You can use the arrows at the top of the window to scroll forward

Panel Report

Partition	Super User	Public	No
Panel	Security		
Type	CK721-A	Enable	Yes
Query String			
Enabled for BACnet	No	High speed RS485	No
Enable Terminals	Yes		
Enable Inputs	Yes		
Enable Outputs	Yes		
Primary IP Address	200.0.0.1	Alternate IP Address	0.0.0.0
Primary Poll Interval	30 seconds	Alternate Poll Interval	86400 seconds
Primary Poll Timeout	75 seconds	Alternate Poll Timeout	176400 seconds
History			
Upload Timezone	<always>	Delete History	Yes
Upload Only	No	Cap. Threshold for Upload-only	50
Upload Always	No	Cap. Threshold for Upload-always	80
Delete At	12:00:00AM	Delete After	30 day(s)
Access			
Time Offset Enable	Yes	Time Offset	2 hour(s) 30 minute(s)
Timezone Checking	Yes	Entry/Exit	No
Timed Over/Tailgate	No	System Override	No
PIN Code Digits	9	Pin Code Type	Custom
Scramble Mode	0		
Peer to Peer Badge Sync	Yes	Broadcast Port Number	47500
Alarm			
Report Delay	35 seconds	Latch Output	No
Output Delay	25 seconds	Enable Panel Relay Output Groups	No
Enable Input Suppression Messages	No		

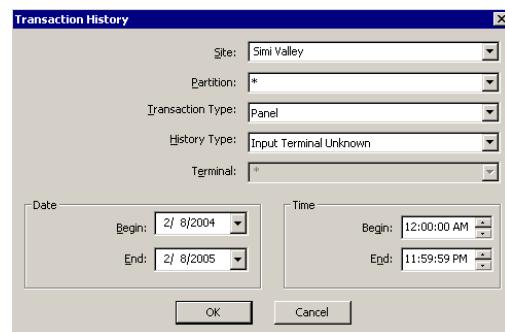
and back through the pages, resize the window for the best display, and print all or single pages of the report.

This report lists the panels with their associated configuration, as set up in the Panel window.

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. If you select <all> as the transaction type, the History Type will be grayed out (history type will be included under the All option).

- From the Run Report list, double-click **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, select from the drop-down list the name of the remote site.
- If your system is partitioned, the default **Partition** entry is **All** represented by an asterisk. Select a specific partition name to gather data only from that partition.
- The default **Transaction Type** entry is **<all>**. Select a specific Transaction Type to report on only one transaction type in the system.
- Select a **History Type**. History types available from the drop-down list depend on the selection in the Transaction Type field.

Transaction History Report

Date (>=)	2/8/2004 12:00:00AM
Date (<=)	2/8/2005 11:59:59PM
Transaction Type	Panel
Terminal	*
History Type	Input Terminal Unknown
Site	Simi Valley
Partition	Super User
Date	2/7/2005 9:53:05AM
Panel	North Entrance
History Message	Input Terminal Unknown
Input Point	
Partition	Super User
Date	2/7/2005 9:53:05AM
Panel	North Entrance
History Message	Input Terminal Unknown
Input Point	

6. If available for selection, select a specific **Terminal** to limit your search.
7. Select a **Begin** and **End** date for the transactions you wish to see.
8. Select a **Begin** and **End** time for the transactions you wish to see.
9. 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.
10. Click **OK**. The Transaction History report displays in the 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 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.

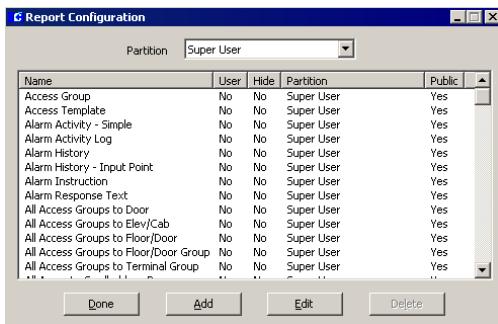
Database Table Definitions

To create a custom report that is compatible with the P2000 system, refer to the *P2000 Database Table Definitions* Supplement. Once you have the field/table relationship information, create your report according to the methods presented in your SAP Crystal Reports documentation.

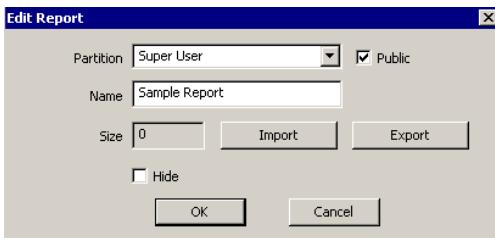
To Import a Custom Crystal Report into the P2000 System:

1. Save your custom Crystal report in <name>.rpt format and copy it to a directory that is accessible to the P2000 Server.

- From the P2000 Main menu, select **Report>Report Configuration**. The Report Configuration dialog box opens.



- If your system is partitioned, select the **Partition** that will contain the imported report.
- Click **Add**. The Edit Report dialog box opens.



- Select **Public** to make this report visible to all partitions.
- Enter a name for your custom report. (This is the name that will display in your Run Report list once the report is imported.)
- Click **Import**.
- From the Windows Open dialog box, navigate to the directory in which the report resides and select the report.
- Click **Open**, the Size of the selected report displays.
- 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.

- 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:

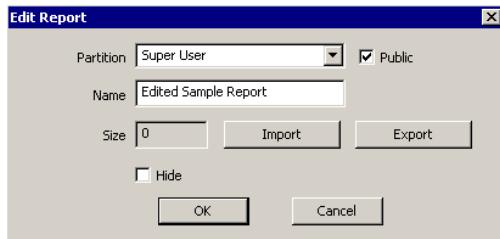
- From the P2000 Main menu, select **Report>Report Configuration**. The Report Configuration dialog box opens.
- Select from the scrolling list the report you wish to edit in Crystal.
- Click **Edit**. The Edit Report dialog box opens. The Name and Size of the selected report display.
- Click **Export**. 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, refer to 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. Click **Import**.
7. From the Windows Open dialog box, navigate to the directory in which the report resides and select the report.
8. Click **Open**, the Size of the selected report displays.
9. 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.
10. 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.

PRELIMINARY

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 314.

To ensure that your events work properly, we strongly recommend that you verify if the events you define work as you expected. Some event triggers and actions that use hardware values such as panels, terminals, inputs, or outputs, may not be available if your hardware does not support the associated functions. For example, the **Badge** trigger type *Deny Open Door* is only available for CK7xx panels of version 2.5 and higher, whereas a **Security Level** action category is only available with panels that support the Security Level feature, such as CK7xx, S321-DIN, S321-IP, D600 AP. Before programming your system events, refer to the instructions provided with your hardware to ensure that the triggers and actions are available to you.

Trigger Types

Category: Alarm

Any Alarm – Triggers when the system creates or acts upon any alarm.

Area – Triggers when the system creates or acts upon an Area alarm.

AV Behavior Alarm – Triggers when the system creates or acts upon an Audio Visual Behavior alarm.

AV Dry Contact Alarm – Triggers when the system creates or acts upon an Audio Visual Dry Contact alarm.

AV Motion Alarm – Triggers when the system creates or acts upon an Audio Visual Motion alarm.

AV System Alarm – Triggers when the system creates or acts upon an Audio Visual System alarm.

AV Video Loss Alarm – Triggers when the system creates or acts upon an Audio Visual Video Loss alarm.

Event Alarm – Triggers when the system creates or acts upon an Event alarm.

FDA – Triggers when the system creates or acts upon an FDA alarm.

Fire Detector – Triggers when the system creates or acts upon a fire detector alarm.

Fire I/O Module – Triggers when the system creates or acts upon a fire Input/Output module alarm.

Fire Zone – Triggers when the system creates or acts upon a fire zone alarm.

Guard Tour – Triggers when the system creates or acts upon a Guard Tour alarm.

Inputs – Triggers when the system creates or acts upon an Input alarm.

Integration Component – Triggers when the system creates or acts upon an Integration Component alarm.

Intercom Station – Triggers when the system creates or acts upon an Intercom Station alarm.

Intrusion Area – Triggers when the system creates or acts upon an Intrusion Area alarm.

Intrusion Zone – Triggers when the system creates or acts upon an Intrusion Zone alarm.

Loop Tamper – Triggers when the system creates or acts upon a hardware Loop Tamper switch alarm.

Muster Aborted – Triggers when the system creates or acts upon a Muster Aborted alarm.

Muster Running – Triggers when the system creates or acts upon a Muster Running alarm.

Muster When Disabled – Triggers when the system creates or acts upon a Muster When Disabled alarm.

Muster Zone Status – Triggers when the system creates or acts upon a Muster Zone Status alarm.

Remote Messaging Receive – Triggers when the system generates an alarm when a remote message is received.

Remote Messaging Transmit – Triggers when the system generates an alarm when a remote message is transmitted.

Timesync – Triggers when the system creates or acts upon a time synchronization alarm.

Conditions

- Alarm Category
- Alarm State
- Date (steady state)
- Day of the Month
- Day of the Week
- Escalation Level
- Month
- Time

Category: Area

Area Maximum allowed alarm – Triggers when the system sets or resets an alarm when the maximum number of cardholders allowed in the selected Area has exceeded.

Area Minimum required alarm – Triggers when the system sets or resets an alarm when the minimum number of cardholders required is not present at the same time in the selected Area.

Area Pre-Maximum allowed alarm – Triggers when the system sets or resets an alarm when the pre-maximum number of cardholders allowed in the selected Area is reached.

Conditions

- Reset
- Set

Category: Audio-Visual

AV Behavior Alarm – Triggers when the system creates or acts upon an AV Behavior alarm.

AV Dry Contact Alarm – Triggers when the system creates or acts upon an AV Dry Contact alarm.

AV Motion Alarm – Triggers when the system creates or acts upon an AV Motion alarm.

AV System Alarm – Triggers when the system creates or acts upon an AV System alarm.

AV Video Loss Alarm – Triggers when the system creates or acts upon an AV Video Loss alarm.

Conditions

- AV Camera Name
- AV Dry Contact Name
- AV Switch Name
- Date (steady state)

- Day of the Month
- Day of the Week
- Month
- Time

Category: Audit

Add Badge Audit – Triggers when the system generates an audit message because an operator has added a badge to the system.

Delete Badge Audit – Triggers when the system generates an audit message because an operator has deleted a badge from the system.

Edit Badge Audit – Triggers when the system generates an audit message because an operator has changed a badge in the system.

Conditions

- Badge
- Badge Configuration
- Badge Purpose
- Badge Reason
- Cardholder
- Date (steady state)
- Day of the Month
- Day of the Week
- Month
- Time

Category: Badge

Anti-Passback Timer On – Triggers when a cardholder presents a badge at an anti-passback reader where the timer is on.

Deny Open Door – Triggers when a panel receives a Deny Door Open message. This message is available from CK7xx panels version 2.5 and higher that have the reader flag “Deny If Door Open” enabled.

Executive Privilege – Triggers when the badge presented has executive privileges; that is, it

has unlimited access and bypasses all time zones and access groups.

Host Grant – Triggers when the cardholder presents a badge and the host grants access.

Host Grant Entry – Triggers when the cardholder presents a badge and the host grants access at an entry reader.

Host Grant Exit – Triggers when the cardholder presents a badge and the host grants access at an exit reader.

Invalid Badge – Triggers when the badge presented at the reader is not valid.

Invalid Badge Time Zone – Triggers when the badge presented at the reader has a disabled time zone.

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 cardholder presents the badge at the reader in an out-of-sequence manner; that is, 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 the cardholder enters an invalid keypad code.

Invalid Pin Code – Triggers when the cardholder enters an invalid PIN code.

Invalid Reader – Triggers when the badge presented has no access rights assigned to the reader.

Invalid Reader Time Zone – Triggers when a cardholder presents a badge at a reader that has a disabled time zone.

Invalid Security Level – Triggers when the system denies access to a badge at a reader because of an invalid security level.

Local Grant – Triggers when the cardholder presents a badge and the panel grants access.

Panel Card Event Activated – Triggers when the cardholder presents a badge at a reader and activates a panel card event.

Panel Card Event Deactivated – Triggers when the cardholder presents a badge at a reader and deactivates a panel card event.

Soft In-X-It Violation – Triggers when the badge presented generated an entry/exit violation; that is, the system grants access but creates an error message.

Valid & Unauthorized Access – Triggers when the badge presented at the reader is valid, but the door remains locked because further authorization (for example, by the guard) is required.

Conditions

- Access Group of Badge
- Access Group of Terminal
- Badge
- Badge Configuration
- Badge Purpose
- Badge Reason
- Cardholder
- Date (steady state)
- Day of the Month
- Day of the Week
- Month
- Panel Name
- Terminal Index
- Terminal Name
- Time
- Timezone Active

Note: Badge conditions include all UDFs of type Numeric defined in the system, which you can use to activate a trigger.

Category: Counter

Triggers when the selected counter reaches the specified value.

Condition

- Value

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: Fire Detector

Fire Detector Alarmed – Triggers when the fire detector enters the alarmed state.

Fire Detector Disabled – Triggers when the fire detector enters the disabled state.

Fire Detector Enabled – Triggers when the fire detector enters the enabled state.

Fire Detector Troubled – Triggers when the fire detector enters the trouble state.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Fire Detector Name
- Month
- Time

Category: Fire IO Module

Fire IO Module Activated – Triggers when the fire Input/Output module is activated.

Fire IO Module Disabled – Triggers when the fire Input/Output module enters the disabled state.

Fire IO Module Enabled – Triggers when the fire Input/Output module enters the enabled state.

Fire IO Module Troubled – Triggers when the fire Input/Output module enters the trouble state.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Fire IO Module Name
- Month
- Time

Category: Fire Panel

Fire Panel Down – Triggers when the fire panel is down.

Fire Panel Troubled – Triggers when the fire panel is in trouble state.

Fire Panel Up – Triggers when the fire panel is up.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Fire Panel Name
- Month
- Time

Category: Fire Zone

Fire Zone Alarmed – Triggers when the fire zone enters the alarmed state.

Fire Zone Disabled – Triggers when the fire zone enters the disabled state.

Fire Zone Enabled – Triggers when the fire zone enters the enabled state.

Fire Zone Troubled – Triggers when the fire zone enters the trouble state.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Fire Zone Name
- Month
- Time

Category: Inputs

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 Is Open (steady state) – Triggers when an input is in open state. Use this trigger in combination with other trigger(s).

Input Is Secure (steady state) – Triggers when an input is in secure state. Use this trigger in combination with other trigger(s).

Input Is Set (steady state) – Triggers when an input is in set state. Use this trigger in combination with other trigger(s).

Input Is Short (steady state) – Triggers when an input is in short state. Use this trigger in combination with other trigger(s).

Input Is Suppressed (steady state) – Triggers when an input is in suppressed state. Use this trigger in combination with other trigger(s).

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Input Point Name
- Input Point Number
- Month
- Panel Name
- Terminal Index
- Terminal Name
- Time
- Timezone Active

Category: Integration Component

Down – Triggers when the selected integration component is down.

Misconfigured – Triggers when the selected integration component is misconfigured.

Unavailable – Triggers when the selected integration component is not available.

Up – Triggers when the selected integration component is up.

Conditions

- Integration Component Name

Category: Intercom

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.

Station Output Active – Triggers when the intercom station output is active

Station Output Inactive – Triggers when the intercom station output shows no activity.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Intercom Station
- Month
- Time

Category: Intrusion Annunciator

Activated – Triggers when the intrusion annunciator has been activated.

Deactivated – Trigger when the intrusion annunciator has been deactivated.

Conditions

- Announcer Name
- Date (steady state)
- Day of the Month
- Day of the Week
- Month
- Time

Category: Intrusion Area

Alarmed/Armed/Bypassed/Sealed (transition) – Triggers when the intrusion area enters the alarmed, armed, bypassed, or sealed state.

Alarmed/Armed/Bypassed/Unsealed (transition) – Triggers when the intrusion area enters the alarmed, armed, bypassed, or unsealed state.

Alarmed/Armed/No-Bypass/Sealed (transition) – Triggers when the intrusion area enters the alarmed, armed, not bypassed, or sealed state.

Alarmed/Armed/No-Bypass/Unsealed (transition) – Triggers when the intrusion area enters the alarmed, armed, not bypassed, or unsealed state.

Alarmed/Disarmed/Bypassed/Sealed (transition) – Triggers when the intrusion area enters the alarmed, disarmed, bypassed, or sealed state.

Alarmed/Disarmed/Bypassed/Unsealed (transition) – Triggers when the intrusion area enters the alarmed, disarmed, bypassed, or unsealed state.

Alarmed/Disarmed/No-Bypass/Sealed (transition) – Triggers when the intrusion area enters the alarmed, disarmed, not bypassed, or sealed state.

Alarmed/Disarmed/No-Bypass/Unsealed (transition) – Triggers when the intrusion area enters the alarmed, disarmed, not bypassed, or unsealed state.

Armed (steady state) – Triggers when the intrusion area enters the armed state. Use this trigger in combination with other trigger(s).

Armed (transition) – Triggers when the intrusion area enters the armed state.

Armed/Bypassed/Sealed (transition) – Triggers when the intrusion area enters the armed, bypassed, or sealed state.

Armed/Bypassed/Unsealed (transition) – Triggers when the intrusion area enters the armed, bypassed, or unsealed state.

Armed/No-Bypass/Sealed (transition) – Triggers when the intrusion area enters the armed, not bypassed, or sealed state.

Armed/No-Bypass/Unsealed (transition) – Triggers when the intrusion area enters the armed, not bypassed, or unsealed state.

Disarmed (steady state) – Triggers when the intrusion area enters the disarmed state. Use this trigger in combination with other trigger(s).

Disarmed (transition) – Triggers when the intrusion area enters the disarmed state.

Disarmed/Bypassed/Sealed (transition) – Triggers when the intrusion area enters the disarmed, bypassed, or sealed state.

Disarmed/Bypassed/Unsealed (transition) – Triggers when the intrusion area enters the disarmed, bypassed, or unsealed state.

Disarmed/No-Bypass/Sealed (transition) – Triggers when the intrusion area enters the disarmed, not bypassed, or sealed state.

Disarmed/No-Bypass/Unsealed (transition) – Triggers when the intrusion area enters the disarmed, not bypassed, or unsealed state.

Conditions

- Area Name
- Date (steady state)
- Day of the Month
- Day of the Week
- Month
- Time

Category: Intrusion Device

Intrusion Device Goes Down (transition) – Triggers when an intrusion device state has changed to down.

Intrusion Device Goes Fault (transition) – Triggers when an intrusion device state has changed to fault.

Intrusion Device Goes Normal (transition) – Triggers when an intrusion device state has changed to normal.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Device Name
- Month
- Time

Category: Intrusion Zone

Alarmed (steady state) – Triggers when the intrusion zone enters the alarmed state. Use this trigger in combination with other trigger(s).

Alarmed (transition) – Triggers when the intrusion zone enters the alarmed state.

Bypassed (steady state) – Triggers when the intrusion zone enters the bypassed state. Use this trigger in combination with other trigger(s).

Bypassed (transition) – Triggers when the intrusion zone enters the bypassed state.

Normal (steady state) – Triggers when the intrusion zone enters the normal state. Use this trigger in combination with other trigger(s).

Normal (transition) – Triggers when the intrusion zone enters the normal state.

Open (steady state) – Triggers when the intrusion zone enters the open state. Use this trigger in combination with other trigger(s).

Open (transition) – Triggers when the intrusion zone enters the open state.

Tampered (steady state) – Triggers when the intrusion zone enters the tampered state. Use this trigger in combination with other trigger(s).

Tampered (transition) – Triggers when the intrusion zone enters the tampered state.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Month
- Time
- Zone Name

Category: Mustering

Mustering Start – Triggers when the Mustering starts at a specified zone.

Mustering Stop – Triggers when Mustering stops at a specified zone.

Conditions

- Zone Name

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 (steady state)
- Day of the Month
- Day of the Week
- Month
- Operator
- Time

Category: Outputs

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 Is Reset (steady state) – Triggers when an output is in reset state. Use this trigger in combination with other trigger(s).

Output Is Set (steady state) – Triggers when an output is in set state. Use this trigger in combination with other trigger(s).

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week

- Month
- Output Point Name
- Output Point Number
- Panel Name
- Terminal Index
- Terminal Name
- Time
- Timezone Active

Category: Panel

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. Use this trigger in combination with other trigger(s).

Panel Is Up (steady state) – Triggers when the panel is up. Use this trigger in combination with other trigger(s).

Panel Load Database From Flash (transition) – Triggers when the panel has loaded the database from flash memory.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Month
- Panel Name
- Time
- Timezone Active

Category: Terminal

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. Use this trigger in combination with other trigger(s).

Input Terminal Is Up (steady state) – Triggers when an input terminal is up. Use this trigger 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. Use this trigger in combination with other trigger(s).

Output Terminal Is Up (steady state) – Triggers when an output terminal is up. Use this trigger in combination with other trigger(s).

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. Use this trigger in combination with other trigger(s).

Reader Terminal Is Up (steady state) – Triggers when a reader terminal is up. Use this trigger in combination with other trigger(s).

System Facility Code Error – Triggers when a badge presented at the reader has an invalid facility code.

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.

Timed Override Expired – Triggers when a timed override has expired.

Conditions

- Date (steady state)
- Day of the Month
- Day of the Week
- Month
- Panel Name
- Terminal Index
- Terminal Name
- Time
- Timezone Active

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: Time/Date

Time/Date – The system activates the trigger on the specified time and date.

Conditions

- Date (steady state)
- Date (transition)
- Day of the Month (steady state)
- Day of the Week (steady state)
- Month (steady state)
- Time (transition)

Event Action Types

Category: Audio-Visual

Note: *The following event actions will function depending on the set of features provided by the DVR manufacturer's integration software. Refer to the DVR documentation for details.*

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. You cannot manually trigger this event action.

Camera Complete Alarm Associated Terminal – Completes an alarm generated by any configured camera that is associated with a terminal mapped in Input to Camera. You cannot manually trigger this event action.

Camera Preset – Activates the camera's preset action.

Camera Recording Quality – Changes the camera's recording quality. Enter a value from 1 to 255 (255 provides the highest quality). Not all DVR brands accept this command and some may have a limited quality range. Refer to the DVR documentation for details on recording quality settings.

Camera Send Alarm – Sends an alarm message generated by the selected camera.

Camera Send Alarm Associated Input – Sends an alarm message generated by any configured camera that is associated with an input created in Input to Camera mapping. You cannot manually trigger this event action.

Camera Send Alarm Associated Terminal – Sends an alarm message generated by any configured camera that is associated with a terminal mapped in Input to Camera. You cannot manually trigger this event.

Camera Start Recording – Starts the recording of the selected camera.

Camera Start Recording and Archiving – Starts the recording and archiving of the selected 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. You cannot manually trigger this event.

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. You cannot manually trigger this event.

Camera Stop Recording – Stops the recording of the selected 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. You cannot manually trigger this event.

Camera Stop Recording Associated Terminal – Stops the recording of any configured camera that is associated with a terminal mapped in Input to Camera. You cannot manually trigger this event.

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

Action 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 Cardholder 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 Cardholder displayed in the message that triggered the event.

Increment Start Date of Access Group – Increments the start date of the selected access group by the number of days entered for the associated badge.

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 that the switch will perform.

Switch Macro Stop – Deactivates a set of programmed steps that the switch will perform.

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: Download

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: Fire Detector

Detector Disable – Disables the selected fire detector.

Detector Enable – Enables the selected fire detector.

Category: Fire IO Module

IO Module Activate – Activates the output of the selected fire Input/Output module.

IO Module Deactivate – Deactivates the output of the selected fire Input/Output module.

IO Module Disable – Disables the selected fire Input/Output module.

IO Module Enable – Enables the selected fire Input/Output module.

Category: Fire Zone

Zone Disable – Disables the selected fire zone.

Zone Enable – Enables the selected fire zone.

Category: Host

Access Group Enable – Enables or disables the selected access group.

Backup Database – Performs database backup of data and/or images according to schedule.

Cancel Event – Cancels any scheduled event actions for the selected event. Note there will only be scheduled actions if you use a delay between the actions.

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. Click the shortcut button to edit Alarm Options for the selected 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. Click the shortcut button to edit Alarm Options for the selected Alarm Category.

Decrement Counter – Decrements the value of the selected counter.

Delete All Visitor Badges – Deletes all visitor badges in the system.

Delete All Visitors – Deletes all visitors and their badges in the system.

Delete Associated Badge – Deletes the badge associated with the message that triggered the event.

Delete Associated Cardholder – Deletes the cardholder and his/her badges associated with the message that triggered the event.

Delete Associated Visitor – Deletes the visitor and his/her badges associated with the message that triggered the event.

Delete Associated Visitor Badge – Deletes the visitor badge associated with the message that triggered the event.

Delete Expired Visitor Badges – Deletes visitor badges that have been expired for the selected number of days.

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 predefined instruction text message at the selected workstation.

Execute Application – Launches an application at the workstation selected.

Execute Server Process – Launches a configured process. The process will be launched on the server and will run in the security context of the RTL Route service. The process will not have access to the Windows desktop.

Increment Counter – Increments the value of the selected counter.

Message Filter – Adds or removes a specified Message Filter to (or from) 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 (or from) 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 – Sends a message to the specified computer, using Windows *net send* command. The *net send* command only works on computers running Windows NT, Windows 2000, Windows XP, or Windows 2003. For this command to work, you must start the Windows Messenger Service at both the sending and receiving computers.

Open Document – Opens a document at the workstation selected.

Print Message – Sends a predefined 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 Fire – Enables or disables real-time printing of Fire 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 predefined instruction text message as email to the specified address.

Serial Port Message – Sends a predefined instruction text message as a serial port message using the COM port selected.

Set Counter – Sets the counter to a selected value.

TCP/IP Port Message – Sends the configured instruction text to the specified TCP/IP port on the specified computer. The port will be closed after the text is sent.

Text to Speech – Sends the selected instruction text to a workstation using the Windows Text to Speech feature. If the computer has a sound card, the text will be spoken using a synthesized voice. The voice characteristics can be adjusted from the Speech icon in Windows Control Panel.

Trigger Event – Triggers the selected event.

UDF Decrement – Decrements the specified numeric UDF field by one for the Cardholder displayed in the message that triggered the event.

UDF Increment – Increments the specified numeric UDF field by one for the Cardholder displayed in the message that triggered the event.

UDF Set – Sets the specified numeric UDF field to the specified value for the Cardholder

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 Cardholder 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).

Input Group Suppression Time Zone – Suppresses the selected Input Group during the specified Time Zone.

Input Group Unsuppress – Unsuppresses the selected Input Group.

Input Point Disable – Disables a selected input point.

Input Point Enable – Enables a selected input point.

Input Point Enable Alarm – Enables or disables the alarm of the selected input point.

Input Point Suppress – Suppresses the selected Input Point for the specified time (0 seconds means forever).

Input Point Suppression Time Zone – Suppresses the selected Input Point during the specified Time Zone.

Input Point Unsuppress – Unsuppresses the selected Input Point.

Category: Intercom

Connect – Connects the selected intercom station.

Disconnect – Disconnects the selected intercom station.

Intercom Station Reset Output – Resets the output associated with the master station and intercom station selected.

Intercom Station Set Output – Sets the output associated with the master station and intercom station selected.

Category: Intrusion Annunciator

Activate – Activates the selected intrusion annunciator.

Deactivate – Deactivates the selected intrusion annunciator.

Category: Intrusion Area

Arm – Arms the selected intrusion area.

Disarm – Disarms the selected intrusion area.

Category: Intrusion Zone

Bypass Off – The system will not detect intrusion activities at the selected intrusion zone.

Bypass On – The system will detect intrusion activities at the selected intrusion zone.

Reset – Resets the selected intrusion zone.

Reset Ack – Resets and acknowledges the selected intrusion zone.

Category: Metasys Interlock

Metasys Interlock – Activates the selected Metasys system extended architecture object.

You can only configure Metasys Interlocks from a P2000 Server. For details, refer to the Metasys System Extended Architecture Integration Option documentation.

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: 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.

Set Output - Timed – Sets the selected output for the specified duration.

Set Output Group – Sets the selected output group for the specified duration.

Category: Panel

Doors - Lock All Doors – Locks all doors.

Doors - Lock All Doors On Panel – Locks all doors associated with the selected panel.

Doors - Unlock All Doors – Unlocks all doors.

Doors - Unlock All Doors On Panel – Unlocks all doors associated with the selected panel.

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 security level code 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 Access – Unlocks the door (it will not be monitored whether the door is actually accessed or not).

Door Relock – Locks the door.

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.

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.

SUPPRESS FORCED/PROPPED INPUTS – Suppresses forced/propped inputs at the selected reader for the specified time (0 seconds means forever).

Terminal Enable – Enables or disables the terminal selected.

UNSUPPRESS FORCED/PROPPED INPUTS – Unsuppresses forced/propped inputs at the selected reader.

Appendix B: Message Types and Sub-Types

This appendix lists all message types and sub-types available for configuring Message Filters. For more information see “Message Filtering” on page 129.

Message Types	
1 – Notify	
3 – Alarm	
5 – System Action	
258 – Muster Status	
259 – Muster Event Trigger	
289 – P900 CLIC Command	
290 – P900 CLIC Status	
305 – Routing Session	
403 – Intrusion Status	
404 – Fire Status	
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	
2 – Panel Input Point	
3 – Area	
4 – Guard Tour	
5 – Muster Running	
6 – Muster Zone Status	
7 – Muster Disabled	
8 – Muster Aborted	
9 – Loop Tamper Alarm	
10 – Event Alarm	
12 – AV Motion Alarm	
13 – AV Behavior Alarm	

Message Sub-Types (Continued)	
3 – Alarm (continued)	
14 – AV VideoLoss Alarm	
15 – AV DryContact Alarm	
17 – Intrusion Alarm	
18 – Fire Alarm	
19 – Integration Component	
20 – Intercom Station	
5 – System Action	
2 – Error Or Log	
4 – Counter Changed	
5 – Muster Control Started	
258 – Muster Status	
259 – Muster Event Trigger	
289 – P900 CLIC Command	
290 – P900 CLIC Status	
1 – Unknown	
2 – Counter	
3 – Flag	
305 – Routing Session	
403 – Intrusion Status	
404 – Fire Status	
28673 – RTL Data	
1 – Panel: Reader Up/Normal	
3 – Panel: System Restart	
5 – Panel: Reader Down	
10 – Panel: System Facility Code Error	
11 – Panel: System Event Activated	
12 – Panel: System Event De-activated	
15 – Panel: Unlock All Doors	
16 – Panel: Lock All Doors	
17 – Panel: Output Set	
18 – Panel: Output Reset	
19 – Panel: Terminal Reader Strike Locked	
20 – Panel: Terminal Reader Strike Unlocked	
21 – Panel: Terminal Door Held Open	

Message Sub-Types (Continued)	Message Sub-Types (Continued)
<p>28673 – RTL Data (continued)</p> <p>22 – Panel: Terminal Door Forced Open 23 – Panel: Terminal Valid and Unauthr Access 33 – Access Deny: Invalid Card 34 – Access Deny: Anti-passback Timer On 35 – Access Deny: Invalid Reader 36 – Access Deny: Invalid In-X-It Status 37 – Access Deny: Invalid Card Timezone 38 – Access Deny: Invalid Pin Code 39 – Access Deny: Invalid Issue Level 40 – Access Deny: Access Denied Central 41 – Access Deny: Invalid Security Level 42 – Panel: Invalid Reader Timezone 43 – Panel: Timed Override Expiration 44 – Access Deny: Invalid Event 45 – Access Deny: Invalid Event Privilege Level 46 – Access Deny: Invalid Biometric 47 – Access Deny: Open Door 48 – Elevator: Elevator Invalid Floor 49 – Elevator: Elevator Invalid Timezone 50 – Elevator: Elevator Invalid Card 65 – Access Grant: Access Granted Central 67 – Access Grant: Executive Privilege 68 – Access Grant: Access Granted Local 69 – Access Grant: Timed Override Enabled 70 – Access Grant: Timed Override Disabled 71 – Access Grant: Timed Override Enabl Host 72 – Access Grant: Timed Override Disabl Host 73 – Panel: Panel Card Event Activated 74 – Panel: Panel Card Event De-activated 75 – Access Grant: Soft In-X-It Violation 76 – Assisted Access: Assisted Access 78 – Access Grant: Manual Valid&Unauth Accss 79 – Elevator: Access Granted 80 – Access Grant: Reader Egress 96 – Input Point History: Alarm 97 – Input Point History: Secure 98 – Panel: Alarm Acknowledged Locally 99 – Panel: D620 Tamper Alarm Set 100 – Panel: D620 Tamper Alarm Reset 101 – Panel: Door Open Alarm 102 – Panel: Duress Alarm 103 – Panel: Pincode Retry Alarm 104 – Panel: Forced Door Alarm 105 – Panel: Card Parity Alarm 106 – Panel: Prox Card Low Battery Alarm 107 – Panel: D620 AC Power Set Alarm 108 – Panel: D620 AC Power Reset Alarm 109 – Panel: D620 Low Battery Set Alarm 110 – Panel: D620 Low Battery Reset Alarm 111 – Panel: Reader Low Battery Set Alarm 112 – Panel: Reader Low Battery Reset Alarm 113 – Panel: Reader AC Set Alarm 114 – Panel: Reader AC Reset Alarm</p>	<p>28673 – RTL Data (continued)</p> <p>115 – Panel: Reader Tamper Set Alarm 116 – Panel: Reader Tamper Reset Alarm 117 – Input Point History: Open 118 – Input Point History: Short 123 – Panel: Calibration results 125 – Input Point History: Input Suppressed 129 – Kone IP Elevator: Kone IP Status Response 130 – Kone IP Elevator: Kone IP Disconnect Msg 224 – Panel: Node Went Up 225 – Panel: Fallback 226 – Panel: Converter Tamper Set Alarm 227 – Panel: Converter Tamper Reset Alarm 228 – Panel: Node Went Down 266 – Access Grant: Entry Granted Central 267 – Access Grant: Exit Granted Central 292 – Panel: Input Module Up 293 – Panel: Output Module Up 294 – Panel: Input Module Down 295 – Panel: Output Module Down 529 – Intercom: Busy 10752 – Intercom: Intercom Server Up 10753 – Intercom: Intercom Server Down 10754 – Intercom: Intercom Idle 10755 – Intercom: Intercom Server Disconnected 10756 – Intercom: Connected 10757 – Intercom: Call Request 10758 – Intercom: Unknown 10759 – Intercom: Station Output Set 10760 – Intercom: Station Output Reset 20481 – Panel: Node Went Up Duplicate 20482 – Panel: Reader status unknown 20483 – Panel: Input status unknown 20484 – Panel: Output status unknown 20486 – Panel: Node is Misconfigured 20503 – Panel: Panel Badge Database Full 20504 – Panel: Panel Message Buffer Overflow 20505 – Panel: Panel Message Buffer Cleared 20506 – Panel: Panel Fault 20507 – Panel: Panel Firmware Update Initiated 20508 – Panel: Panel Firmware Update Failed 20509 – Access Deny: No Override Privilege 20510 – Access Deny:Timed Override Value Invalid 20511 – Panel: Reader Status Input Fault 20576 – Input Point State Change: Alarm 20577 – Input Point State Change: Secure 20597 – Input Point State Change: Open 20598 – Input Point State Change: Short 20599 – Input Point State Change:Input Suppressed 24577 – Host: Event Triggered 24578 – Host: Event Triggered Manual 28673 – Tour: Tour Alarmed 28674 – Tour: Tour Started 28675 – Tour: Station Checked in On Time</p>

Message Sub-Types (Continued)	Message Sub-Types (Continued)
<p>28673 – RTL Data (continued)</p> <p>28676 – Tour: Station Checked in Early 28677 – Tour: Station Checked in Late 28678 – Tour: Station Checked in Out of Order 28679 – Tour: Tour Stopped 28680 – Tour: Tour Restarted 28681 – Tour: Tour Aborted 28682 – Tour: Tour Completed 28683 – Tour: Station Late Timer Reached 28684 – Tour: Tour Terminated 32769 – Area: Reader Exit 32770 – Area: Reader Entry 32771 – Area: Input Exit 32772 – Area: Input Entry 32773 – Area: Manual Exit 32774 – Area: Manual Entry 36865 – Audio-Visual: Motion 36866 – Audio-Visual: Behavior 36867 – Audio-Visual: Video Loss 36868 – Audio-Visual: Dry Contact 41296 – Fire Alarm: Fire Server Connection Up 41297 – Fire Alarm: Fire Server Connection Down 41472 – Otis System: Component Went Up 41473 – Otis System: Component Went Down 41728 – Integration Component: Up 41729 – Integration Component: Down 41730 – Integration Component: Unknown 41731 – Integration Component: Unavailable 41732 – Integration Component: Misconfigured</p>	<p>28675 – Audit (continued)</p> <p>24 – Department 25 – Panel Timezone 26 – Soft Alarm 27 – Site Parameters 28 – Workstation 29 – Map 30 – Map Icon Set 31 – User Defined Fields 32 – Event 33 – Panel Card Event 34 – Alarm Filter 35 – Message Forwarding 37 – Permission Group 38 – Panel Relay 39 – Report 40 – MIS Interface 41 – Image Recall Filter 42 – Counter 43 – Action Interlock 44 – External IP 45 – Guard Tour Definition 46 – Tour Station Definition 47 – Loop 48 – Elevator 49 – Floor Mask 50 – Floor Group 51 – Floor Name Configuration 52 – Cabinet 53 – Door Group 54 – Door Mask 55 – Door Name Configuration 56 – Area 57 – Muster Zone 58 – Area Control Layout 60 – CCTV Server 61 – CCTV Switch 62 – CCTV Tour 63 – CCTV Alarm 64 – CCTV Macro 65 – CCTV System Auxiliary 66 – CCTV Monitor 67 – CCTV Sequence 68 – CCTV Camera 69 – CCTV Preset 70 – CCTV Pattern 71 – CCTV Camera Auxiliary 72 – Enable Code 73 – P900 Flag 74 – P900 Counter 75 – P900 Trigger Event 76 – P900 Trigger Link 77 – P900 System Parameters</p>
<p>28675 – Audit</p> <p>1 – User 2 – Badge 3 – Badge Layout 4 – Badge Fields 5 – Badge Encoding 6 – ID Badge 7 – Cardholder 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</p>	

Message Sub-Types (Continued)	
28675 – Audit (continued)	
78 – Auto-badge Number	
79 – Air Crew PIN Number	
80 – P900 Sequence Files	
81 – Remote Server	
82 – Message Filter	
83 – Message Filter Group	
84 – Local Site	
85 – Service Startup Configuration	
86 – Application	
87 – Panel Card Format	
88 – Reason	
89 – Security Level Range	
94 – Audit	
95 – Alarm History	
96 – Alarm	
97 – Generic Text	
98 – Muster History	
99 – Guard Tour History	
100 – Transaction History	
101 – Redundancy	
102 – Mapping Configuration	
103 – Mapping Data Fields Configuration	
104 – Intercom Exchange	
105 – Intercom Station	
106 – AV Site	
107 – AV Camera	
108 – AV Monitor	
109 – AV Preset	
110 – Input To Camera	
112 – Enterprise Site	
113 – Enterprise Parameters	
114 – AV Dry Contact	
115 – Alarm Colors	
116 – Badging Setup	
117 – Request Approvers	
118 – FASC-N CCC	
119 – Badge Purpose	
120 – Alarm Options	
121 – Intrusion Entity	
122 – SIA Device	
123 – Alarm Category	
124 – MSE Graphic	
125 – OSI Facility	
173 – MSE Registration	
174 – MSE Partition	
176 – WebAccess Configuration	
177 – Fire Alarm	
178 – Software Update	
179 – Badge Reason	
180 – Required Fields	
182 – HID Facility	
183 – Kone IP Elevator	
184 – Intercom Interface	

Message Sub-Types (Continued)	
28675 – Audit (continued)	
185 – Integration Component	
186 – AssaAbloy Facility	
187 – Badge Format	
188 – Assa Abloy Badge Format	

Appendix C: Panel Comparison Matrix

Feature	CK720 (2.6)	CK705 (2.6)	CK721 (2.8)	CK721-A (2.10)	CK721-A (3.0 / 3.1)	S321-DIN	S321-IP	OSI	Isonas	HID	Assa Abloy
4-State Alarms Even/Odd (E/O) Address	E/O	E/O	E/O	E/O	E/O	E/O	–	–	–	–	–
Access Grant on Door Open	✓	✓	✓	✓	✓	✓	–	–	–	–	–
Access Groups Per Badge	8	8	8	8	32	2	1	8	1	8	8
Add Hardware Module Wizard	✓	✓	✓	✓	✓	–	–	–	–	–	–
Air Crew PIN	✓	✓	✓	✓	✓	–	–	–	–	–	–
Alarm Debounce	✓	✓	✓	✓	✓	✓	✓	–	✓	✓	–
Americans with Disabilities Act (ADA)	✓	✓	✓	✓	✓	✓	–	✓	–	✓	✓
Anti-Passback	✓	✓	✓	✓	✓	✓	✓	–	–	✓	–
Anti-Tailgate	✓	✓	✓	✓	✓	✓	–	–	–	–	–
Backup DB to Flash Interval	–	–	–	✓	✓	–	–	–	–	–	–
Badge Capacity	15K ¹	15K ¹	100K	120K	200K ²	30K	5K	65K	64K	44K	2400
Badge Event Privilege Support	✓	✓	✓	✓	✓	✓	–	–	–	–	–
Badge Override Support	✓	✓	✓	✓	✓	✓	✓	–	–	✓	–
BQT Reader Support	✓	✓	✓	✓	✓	–	–	–	–	–	–
Calibration/Uncalibration	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Card Formats (simultaneously supported)	21	21	21	21	21	21	1	2	1	1	U ⁵
Card ID Support	✓	✓	✓	✓	✓	✓	–	✓	✓	✓	–
Central Mode (Card Processing)	✓	✓	✓	✓	✓	✓	–	–	–	–	–
Custom Card Formats	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Custom PIN Code	✓	✓	✓	✓	✓	✓	✓	✓	–	✓	✓
D620-ECG Elevator Mode	✓	✓	✓	✓	✓	–	–	–	–	–	–
Door Control - Access Time (manual)	✓	✓	✓	✓	✓	✓	–	✓	✓	✓	✓ ³
Door Control - Timed (manual)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓ ³
Door Open Warning	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Door Shunt Expiration Warning	✓	✓	✓	✓	✓	✓	✓	–	–	–	–
Dual Ethernet Support	✓	✓	–	–	–	–	–	–	–	–	–
Elevator Readers (max. per panel)	16	4	16	16	16	–	–	–	–	–	–
Elevator Support	✓	✓	✓	✓	✓	–	–	–	–	–	–

Feature	CK720 (2.6)	CK705 (2.6)	CK721 (2.8)	CK721-A (2.10)	CK721-A (3.0 / 3.1)	S321-DIN	S321-IP	OSI	Isonas	HID	Assa Abloy
Encrypted Communications	-	-	-	-	✓ ⁴	-	✓	-	✓	✓	-
Entry/Exit Enforce	✓	✓	✓	✓	✓	-	-	-	-	-	-
Executive Privilege	✓	✓	✓	✓	✓	✓	-	✓	-	✓	✓
Exempt from Archive to Flash	✓	✓	✓	✓	✓	-	-	-	-	-	-
Extended Shunt Time	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Extended Time Override	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Facility Codes	12	12	12	12	12	4	U ⁵				
HID Corp. 1000 Card Format	✓	✓	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓
High Level Elevator	✓	✓	✓	✓	✓	-	-	-	-	-	-
High Performance Entry/Exit Status Synchronization	✓	✓	✓	✓	✓	-	-	-	-	-	-
High Speed 485	✓	✓	✓	✓	✓	✓ ⁷	-	-	-	-	-
History Upload With Seconds	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Holidays	40	40	40	40	40	40	40	40	64	16	64
Input Groups	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Input Suppression	✓	✓	✓	✓	✓	-	✓	-	-	-	-
Inputs (max. per panel)	256	64	256	256	256 ⁸ 326 ⁹	6	12	-	4	5	-
Issue Level per Badge	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓
Keyless Override Feature	✓	✓	✓	✓	✓	✓	-	-	-	-	-
KONE HLI Elevator Support	✓	✓	-	✓	✓	-	-	-	-	-	-
KONE IP Elevator Support	-	-	-	-	✓ ⁴	-	-	-	-	-	-
Multi Card Types	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓
Multiple Facility Codes per Badge Type	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓
N-Man Rule	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Network	✓	✓	✓	✓	✓	✓ ⁷	✓	✓	✓	✓	✓
Otis Compass Elevator Support	-	-	-	-	✓	-	-	-	-	-	-
Otis EMS - Security / BMS	-	-	-	✓	✓	-	-	-	-	-	-
Output Control (manual)	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	-
Output Groups	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Output Groups associated with Time-zones	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Output Status Reporting	✓	✓	✓	✓	✓	✓	✓	-	-	-	-
Outputs (max. per panel)	128	32	128	128	128 ⁸ 208 ⁹	10	8	-	2	2	-
Override Expiration Warning	✓	✓	✓	✓	✓	✓	-	-	-	-	-
Override Reset Threat Level	✓	✓	✓	✓	✓	✓	✓	-	-	-	✓

Feature	CK720 (2.6)	CK705 (2.6)	CK721 (2.8)	CK721-A (2.10)	CK721-A (3.0 / 3.1)	S321-DIN	S321-IP	OSI	Isonas	HID	Assa Abloy
Panel Card Events	20	20	20	20	20	20	—	—	—	—	—
Panel Relay Set/Reset	✓	✓	✓	✓	✓	—	—	—	—	—	—
Panel Relays	2	2	1	1	1	—	—	—	—	—	—
Peer to Peer Badge Sync	—	—	—	✓	✓	—	—	—	—	—	—
PIN + 1 Duress	✓	✓	✓	✓	✓	✓	—	—	—	—	—
PIN Code Digits supported (Custom)	5	5	5	5	9	5	4	9	10 ¹⁰	9	—
Power over Ethernet (PoE) Connection	—	—	—	—	—	—	—	—	✓	✓	✓ ¹¹
Raw 128 Bit Card Format	—	—	—	—	—	—	✓	—	—	—	—
Reader Override	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	—
Reverse Card Reading	✓	✓	✓	✓	✓	✓	—	—	—	—	—
Reverse Swipe Duress	✓	✓	✓	✓	✓	✓	—	—	—	—	—
Security Level	✓	✓	✓	✓	✓	✓	✓	—	—	—	—
Special Flags (A, B, C)	✓	✓	✓	✓	✓	✓	—	✓	—	✓	✓
Star Feature	✓	✓	✓	✓	✓	✓	—	—	—	—	—
Strike Status	✓	✓	✓	✓	✓	✓	✓	✓	—	—	—
Terminal Override Status	✓	✓	✓	✓	✓	—	—	✓	✓	✓	✓
Terminal Readers	16	4	16	16	64	2	2	128	1	1	1
Terminal Timezone Enabled	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	—
Terminal Timezone Override	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Terminal Timezone PIN Suppression	✓	✓	✓	✓	✓	✓	✓	✓	—	✓	—
Timezones per Badge	8	8	8	8	32	2	2	—	1	8	8
Timezones per Panel	64	64	64	64	64	64	64	32	32	64	32
Valid and Unauthorized	✓	✓	✓	✓	✓	✓	—	—	—	—	—

- 1 Without memory expansion.
- 2 When the number of badges exceeds 120,000, the number of access groups should be limited to 50,000.
- 3 Supported by hardwired version only.
- 4 Supported by CK721-A version 3.1 only.
- 5 Unlimited.
- 6 No formats are built-in, all are custom with a maximum of 32-bits.
- 7 S321-DIN panels can communicate with the P2000 Server through network connection using a Digi One SP converter box.
- 8 Maximum number supported by RDR2, SI08, SI8, IO8, I16.
- 9 Maximum number supported by RDR2S-A and RDR8S.
- 10 This is the maximum number; however, the number of digits supported depends on the card format assigned to the reader.
- 11 PoE version only.

Legacy and P900 Panels

Feature	D620 (143G)	D620-TIU (173E)	D600 AP (PS 155B)	S320	P900
4-State Alarms Even/Odd Address	Odd	Odd	Odd	-	Even/Odd
Access Grant on Door Open	-	-	-	-	✓
Access Groups Per Badge	2	2	2	2	1
Add Hardware Module Wizard	-	-	-	-	-
Air Crew PIN	-	-	✓	-	-
Alarm Debounce	-	-	-	-	-
Americans with Disabilities Act (ADA)	-	-	-	-	-
Anti-Passback	✓	✓	✓	✓	✓
Anti-Tailgate	✓	-	✓	✓	-
Backup DB to Flash Interval	-	-	-	-	-
Badge Capacity	5K ¹	5K ¹	5K ¹	5K ¹	10K ²
Badge Event Privilege Support	✓	✓	✓	✓	-
Badge Override Support	✓	-	-	✓	-
BQT Reader Support	-	-	-	-	-
Calibration/Uncalibration	-	-	-	-	-
Card Formats (simultaneously supported)	1	-	1	1	1
Card ID Support	✓	-	✓	✓	-
Central Mode (Card Processing)	✓	✓	✓	✓	-
Custom Card Formats	-	-	-	-	-
Custom PIN Code	✓	-	✓	✓	✓
D620-ECG Elevator Mode	-	-	-	-	-
Door Control - Access Time (manual)	✓	✓	✓	✓	-
Door Control - Timed (manual)	✓	✓	✓	✓	-
Door Open Warning	-	-	-	✓	✓
Door Shunt Expiration Warning	-	-	-	-	✓
Dual Ethernet Support	-	-	-	-	-
Elevator Readers (max. per panel)	-	-	-	-	-
Elevator Support	-	-	-	-	-
Encrypted Communications	-	-	-	-	-
Entry/Exit Enforce	✓	✓	✓	✓	✓
Executive Privilege	✓	✓	✓	✓	-
Exempt from Archive to Flash	-	-	-	-	-
Extended Shunt Time	-	-	✓	-	-

Legacy and P900 Panels

Feature	D620 (143G)	D620-TIU (173E)	D600 AP (PS 155B)	S320	P900
Extended Time Override	–	–	✓	–	–
Facility Codes	3	–	4	3	8
HID Corp. 1000 Card Format	–	–	–	–	–
High Level Elevator	–	–	–	–	–
High Performance Entry/Exit Status Synchronization	–	–	–	–	–
High Speed 485	–	–	–	–	–
History Upload With Seconds	–	–	–	–	✓
Holidays	21	21	21	21	40
Input Groups	✓	✓	✓	✓	✓
Input Suppression	–	–	–	–	–
Inputs (max. per panel)	128	384	128	128	80
Issue Level per Badge	✓	✓	✓	✓	✓
Keyless Override Feature	–	–	–	–	–
KONE HLI Elevator Support	–	–	–	–	–
Multi Card Types	–	–	–	–	–
Multiple Facility Codes per Badge Type	–	–	–	–	–
N-Man Rule	–	–	–	–	–
Network	–	–	–	–	–
Otis Compass Elevator Support	–	–	–	–	–
Otis EMS - Security / BMS	–	–	–	–	–
Output Control (manual)	✓	✓	✓	✓	✓
Output Groups	✓	✓	✓	✓	✓
Output Groups associated with Timezones	✓	✓	✓	✓	✓
Output Status Reporting	–	–	–	✓	–
Outputs (max. per panel)	512	512	512	128	40
Override Expiration Warning	–	–	–	–	–
Override Reset Threat Level	–	–	–	–	–
Panel Card Events	20	20	20	20	–
Panel Relay Set/Reset	✓	✓	✓	✓	–
Panel Relays	1	1	1	2	–
Peer to Peer Badge Sync	–	–	–	–	–
PIN + 1 Duress	–	–	✓	–	–
PIN Code Digits supported	5	–	5	5	4
Power over Ethernet (PoE) Connection	–	–	–	–	–

Legacy and P900 Panels

Feature	D620 (143G)	D620-TIU (173E)	D600 AP (PS 155B)	S320	P900
Raw 128 Bit Card Format	–	–	–	–	–
Reader Override	✓	✓	✓	✓	✓
Reverse Card Reading	–	–	–	–	–
Reverse Swipe Duress	–	–	–	–	–
Security Level	–	–	✓	–	–
Special Flags (A, B, C)	–	–	–	–	–
Star Feature	–	–	–	–	–
Strike Status	–	–	–	✓	–
Terminal Override Status	–	–	–	–	–
Terminal Readers	16	16	16	16	8
Terminal Timezone Enabled	✓	✓	✓	✓	–
Terminal Timezone Override	✓	✓	✓	✓	✓ ³
Terminal Timezone PIN Suppression	✓	✓	✓	✓	✓
Timezones per Badge	2	2	2	2	–
Timezones per Panel	16	16	16	16	64
Valid and Unauthorized	–	–	–	–	–

1 Without MX2.

2 Without memory expansion.

3 Use the Unlocked Time Zone function to configure P900 terminal timezone override.

Appendix D: CCTV Switch Protocols

This appendix describes the CCTV Switch Protocols that the CCTV feature supports. The protocols supported vary according to the current manufacturers' products. Those listed here are 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, see “Creating Actions” on page 317. 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 the CCTV feature supports use a subset of the namespace tags.

The CCTV feature does not include support for multiplexers, VCRs, and video on screen.

Communications

The communication settings for each Switch are determined by the manufacturer. Ensure that the protocol and COM port settings at the Switch matches those configured in the Edit CCTV Switch dialog box. Refer to the manufacturer's specification for details of what the settings should be.

In addition, the CCTV driver will only apply the Timeout setting in the Communications tab of the Edit CCTV Switch dialog box 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 be 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. 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 all monitors use the same sequence. 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 applications that are more complex. 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. The event action processing in the P2000 software or a specially written OPC Client interface will drive this feature.

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 the system does not save a record 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 select 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 feature should work with other American Dynamics Switches, if 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.

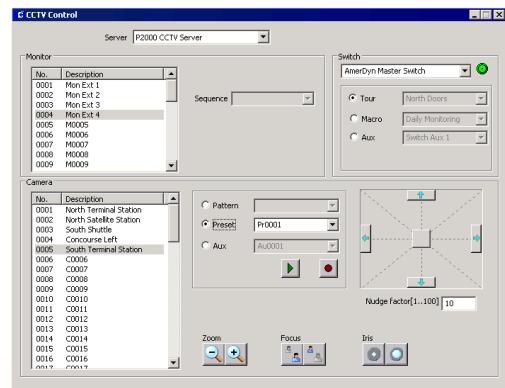
The American Dynamics Protocol

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 select in the Edit CCTV Switch window is **JC.CCTVAmericanDynamics**.

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 the CCTV feature supports 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

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. 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 repeat 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 display 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 American Dynamics.

The maximum values define the number of items that the protocol allows. The values 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 feature 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 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 you set up the Switch. 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.

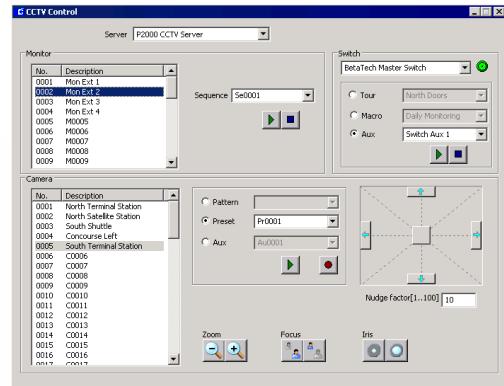
The BetaTech Protocol

Baudrate	9600
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	Hardware

The protocol name to select 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 the CCTV feature supports 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

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. 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 display 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 the protocol allows. 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 feature should work with other Geutebrück Switches, if they adhere to the communications protocol specified by the GST interface if the MicroLink controller with VicroSoft version is 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.

- 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

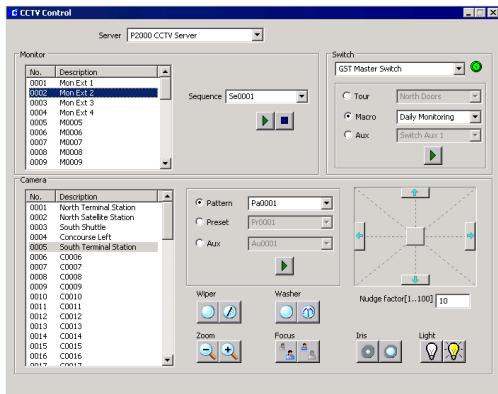
The default communications parameters for the GST interface are:

Baudrate	1200
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	Hardware

The protocol name to select 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 the CCTV feature supports 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

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. If you are using OPCWrite to create an event action, the following namespace tags are supported for a 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 the protocol allows. 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 display 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 feature should work with other Panasonic Switches, if 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

The following commands in the Panasonic SX850 protocol are not supported:

- 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 three Switches are configured in the CCTV/AV Configuration window, then up to three Cameras (one per Switch) could be controlled simultaneously by using up to three separate COM lines between the PC and the Switch.

Note that Panasonic supports one client only. If you attempt to use more than one client, the commands may have unexpected results.

Switch Configuration

Auto Log-Off must be disabled. Refer to your Panasonic manual for details.

Panasonic SX850 Protocol

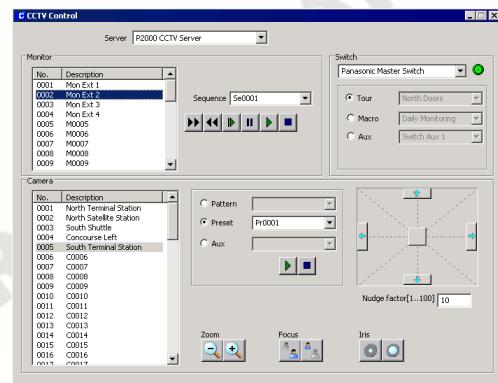
The communications parameters are:

Baudrate	9600
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	None

The protocol name to select 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 the CCTV feature supports for a 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

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. 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 display 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 the protocol allows. 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 feature should work with other Pelco Switches, if 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

TIP: *To stop a Camera Pattern, select the **Aux** radio button, then click **Stop**.*

- 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.

The following commands in the Pelco 9760 protocol are not supported:

- Set Preset with a Label
- Query Device
- Video Loss Detect
- Report Revision
- Select Next/Previous Camera

The Pelco 9760 Protocol

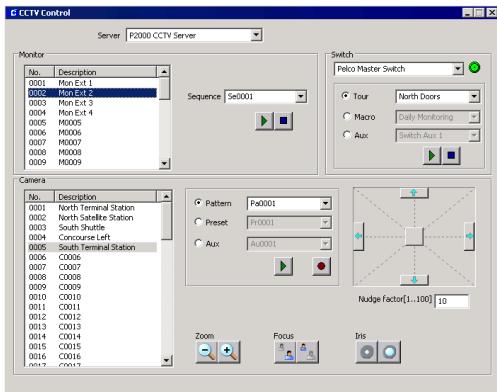
The protocol used is bidirectional. If the matrix recognizes a command, an acknowledgement is sent back to the CCTV Server. If a command is not recognized, a negative acknowledgement is returned.

The predefined timeout for the Pelco Switch is 500 ms.

The protocol name to select 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 the CCTV feature supports 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 OPCWrite Event Actions

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. If you are using OPCWrite to create an event action, the

following namespace tags are supported for a Pelco 9760 Switch:

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

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 display 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, ensure that no other OPC Client is using the Switch. In addition, if you wish to stop recording a Pattern, you must click the **Record** button again.

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 the protocol allows. The values 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:

- “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

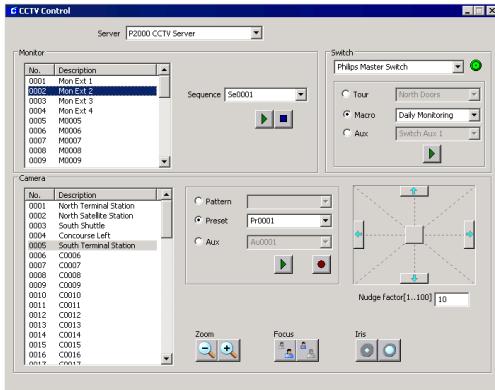
The communications parameters are:

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 select 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 the CCTV feature supports for a 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

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. If you are using OPCWrite to create an event action, the following namespace tags are supported for a 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 display 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 the protocol allows. 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.

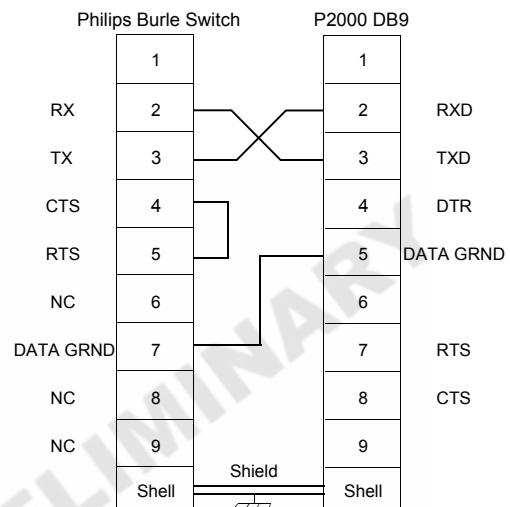
Cabling Configuration

Use an RS232 cable to establish the communication between the Philips Burle Switch and the P2000 Server computer.

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

The following commands in the Ultrak Max-Pro-1000 protocol are not supported:

- 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. Normally 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

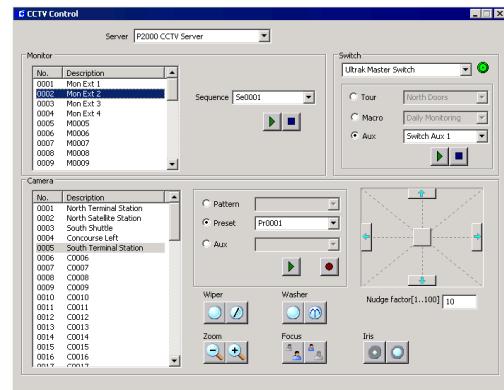
The communications parameters are:

Baudrate	19200 or 9600
Data bits	7
Stop bits	1
Parity	Even
Timeout (ms)	500

The protocol name to select 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 the CCTV feature supports 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

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. If you are using OPCWrite to create an event action, the following namespace tags are supported for the 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 auto-repeat 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 display 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 the protocol allows. 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 feature should work with other Vicon Switches, if 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.

The following commands in the Vicon protocol are not supported:

- 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. Refer to the appropriate Switch programming manual for details.

The Vicon Protocol

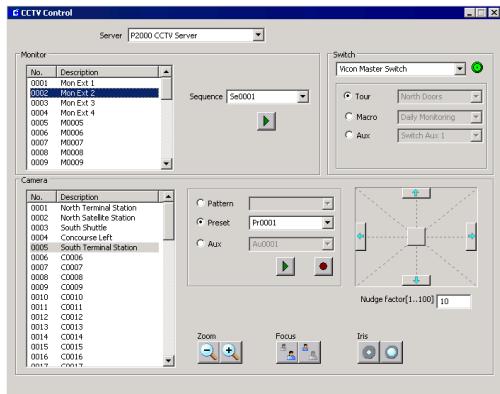
The communications parameters are:

Baudrate	9600
Data bits	8
Stop bits	1
Parity	None
Timeout (ms)	500
Handshake	Hardware

The protocol name to select 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.



Supported Actions

Switch Alarm Play
Switch Alarm Stop

Monitor Sequence Play
Monitor Sequence Stop

Monitor Camera

Camera Preset

Camera Auxiliary Play
Camera Auxiliary Stop

Momentary and Latched Auxiliaries

The Vicon protocol supports up to six auxiliaries per camera. The auxiliaries can be either momentary or latched. The CCTV feature 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 three 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 the CCTV feature supports for a Vicon Switch are:

Supported OPCWrite Event Actions

Appendix E: CCTV Server Namespace Definitions displays a full list of the namespace tags that an OPC Client can interrogate. If you are using OPCWrite to create an event action, the following namespace tags are supported for a 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 auto-repeat functions

Automatic Status Update Tags

The Vicon protocol does not support periodic status updates. These tags display 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 the protocol allows. 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. Note that the appendix lists all the possible tags; however, only a subset of namespace tags is available for each supported Switch Protocol. See *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 the device and updated to reflect the value in the 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 namespace 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 namespace 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 namespace 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 display 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 <u>not</u> 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 1 to this property to stop 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 a 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 you install the P2000 software and the CCTV application on a computer, the installation process makes changes to the Distributed Component Object Model (DCOM) settings to allow communication between P2000 event actions and the CCTV Server, and between the CCTV Client and the CCTV Server; and possibly other installed options on the network.

Before you install the software, be aware of the changes that the process makes to avoid conflicts of interest with other software installed on the computer. Note that the P2000 software and the CCTV application will not operate cor-

rectly if the changes made during installation are subsequently changed.

DCOM Installation

The changes made to the computer are dependent on whether the installation is a P2000 Server, a CCTV Server, or a CCTV Client installation, and the Windows operating system.

The following table shows the changes that the process makes. Note that when you install more than one option, you should combine the appropriate columns to indicate the overall changes.

Change Made to		P2000 Server	P2000 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	✓	✓

PRELIMINARY

Appendix G: Using a Keypad Reader on CK7xx Panels

The following sections describe how to invoke access requests, Air Crew access requests, Timed Overrides, and Panel Card Events using a keypad reader on CK721-A, CK721, CK720, and CK705 panels.

Note: For information on using keypad readers that connect to other panel types, refer to the instructions provided with those panels.

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 badge 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 invoke access using a badge 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. Select the terminal's **PIN Only** option in the Card Type tab. **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 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. Select the terminal's **Card ID** option in the Card Type tab.
3. Verify that the terminal's **PIN Only** option in the Card Type tab is not selected.
4. Verify that the terminal's **PIN + Card ID** option in the Card Type tab is not selected.
5. At the keypad reader, enter the Card ID number and press the # key.

To invoke access with PIN and Card ID:

1. Select the terminal's **PIN + Card ID** option in the Card Type tab.
2. Verify that the terminal's **PIN Only** option in the Card Type tab is not selected.
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. Set the terminal's **PIN Suppression** in the Timezone tab to an inactive timezone.
2. Verify that the terminal's **Allow PIN After Badge** option in the Flags tab is not selected.
3. At the keypad reader, enter PIN and then present the badge.

To invoke access with PIN and badge, allowing PIN after badge:

1. Set the terminal's **PIN Suppression** in the Timezone tab to an inactive timezone.
2. Select the terminal's **Allow PIN After Badge** option in the Flags tab.
3. At the keypad reader, present the badge, enter PIN, and press the # key. You may preset the badge at any time before pressing the # key.

Invoking Air Crew Access Requests from a Keypad**To invoke Air Crew access:**

1. The Server must be online.
2. Enable the respective **Air Crew PIN** for the terminal.
3. To request Air Crew access:

Without the Star Feature, press the B key followed by the Air Crew PIN number and the # key.

With the Star Feature, press the star (*) key, then press number 2, followed by the Air Crew PIN number and the # key.

Invoking Timed Overrides from a Keypad**To invoke Timed Override with Badge:**

1. Select the terminal's **Cardholder Override/Shunt** option in the Access tab.
2. Set the badge's **Override** option in the Security Options tab.
3. 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. Select the terminal's **Cardholder Override/Shunt** option in the Access tab.
2. Set the badge's **Override** option in the Security Options tab.
3. Select the terminal's **PIN Only** option in the Card Type tab. **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. Select the terminal's **Cardholder Override/Shunt** option in the Access tab.
2. Set the badge's **Override** option in the Security Options tab.
3. 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. Select the terminal's **Card ID** option in the Card Type tab.
5. Verify that the terminal's **PIN Only** option in the Card Type tab is not selected.
6. Verify that the terminal's **PIN + Card ID** option in the Card Type tab is not selected.

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. Select the terminal's **Cardholder Override/Shunt** option in the Access tab.
2. Set the badge's **Override** option in the Security Options tab.
3. Select the terminal's **PIN + Card ID** option in the Card Type tab.
4. Verify that the terminal's **PIN Only** option in the Card Type tab is not selected.
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, and 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, 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. Select the terminal's **Cardholder Override/Shunt** option in the Access tab.
2. Set the badge's **Override** option in the Security Options tab.
3. Set the terminal's **PIN Suppression** in the Timezone tab to an inactive zone.
4. Verify that the terminal's **Allow PIN After Badge** option in the Flags tab is not selected.

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. Select the terminal's **Cardholder Override/Shunt** option in the Access tab.
2. Set the badge's **Override** option in the Security Options tab.
3. Set the terminal's **PIN Suppression** in the Timezone tab to an inactive zone.
4. Select the terminal's **Allow PIN After Badge** option in the Flags tab.

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 the 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) You may present the badge at any time before pressing the # key.

Invoking Panel Card Events from a Keypad

Note: When invoking panel card events using CK705 or CK720 panels version 2.2, use the keypad sequence of the star (*) key followed by number 2.

To invoke Panel Card Events with Badge:

1. Set the panel card event's **Trigger Type** to **Card/Keypad Code**.
2. 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. Set the panel card event's **Trigger Type** to **Card/Keypad Code or Card/PIN/Keypad Code**.

2. If set to **Card/PIN/Keypad Code**, set the terminal's **PIN Suppression** in the Timezone tab to an inactive timezone.
3. Select the terminal's **PIN Only** option in the Card Type tab. **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**.

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.

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. Set the panel card event's **Trigger Type** to **Card/Keypad Code**.
2. 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. Set the terminal's **Card ID** option in the Card Type tab.
4. Verify that the terminal's **PIN Only** option in the Card Type tab is not selected.
5. Verify that the terminal's **PIN + Card ID** option in the Card Type tab is not selected.

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. Set the panel card event's **Trigger Type** to **Card/Keypad Code or Card/PIN/Keypad Code**.

2. If set to **Card/PIN/Keypad Code**, set the terminal's **PIN Suppression** in the Timezone tab to an inactive timezone.

3. Select the terminal's **PIN + Card ID** option in the Card Type tab.

4. Verify that the terminal's **PIN Only** option in the Card Type tab is not selected.

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. Set the panel card event's **Trigger Type** to **Card/Keypad Code or Card/PIN/Keypad Code**.

2. Set the terminal's **PIN Suppression** in the Timezone tab to an inactive timezone.

3. Verify that the terminal's **Allow PIN After Badge** option in the Flags tab is not selected.

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. Set the panel card event's **Trigger Type** to **Card/Keypad Code or Card/PIN/Keypad Code**.
2. Set the terminal's **PIN Suppression** in the Timezone tab to an inactive timezone.
3. Select the terminal's **Allow PIN After Badge** option in the Flags tab.
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) You may present the badge at any time before pressing the # key.

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 that you have configured all terminal and panel settings 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 A and D keys.

Legend

Keypad Code	Enter the Keypad Code.	badge	Present the badge.
PIN	Enter the PIN number.	* 0 1	Press the specified key.
Card ID	Enter the Card ID number.	# A D	
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 badge¹ #**

¹⁾ You may present the badge at any time before pressing the # key, that is, before, during or after you enter the PIN.

Invoking Air Crew Access Requests from a Keypad

To request access without Star Feature:

B Air Crew PIN #

To request access with Star Feature:

*** 2 Air Crew 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⁾ You may present the badge at any time before pressing the # key, that is, before, during or after you enter the PIN and the Timed Override sequence.

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

 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 #

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⁾ You may present the badge at any time before pressing the # key, that is, before, during or after you enter the PIN and the Panel Card Event sequence.

Use the keypad sequence * 2 if using CK705/CK720 panels version 2.2.

Appendix H: Troubleshooting

This section explains the authentication process for a P2000 user. This will help you to understand what goes on behind the scenes, the reason for each step, and how to troubleshoot when problems arise.

Authentication Process

Windows Authentication

The first level of authentication for a P2000 Workstation is the connection to the P2000 Server. The Workstation must connect to the Server over the network to gain access to the database. Your Windows operating system performs this authentication. 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 in Windows. In order for the Workstation to connect to the Server, this username and password must be a valid account on the Server.

The P2000 Server installation creates three Windows user groups, which you can assign to a user account to allow connection to the Server.

The P2000 installation creates the following user groups:

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 P2000 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 P2000 ODBC connection is to pass the Windows username and password. The username and password that the ODBC connection sends must be a valid account in SQL Server for the Workstation to connect to the database. The P2000 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 that the P2000 Server installation created, assigning a Windows user account to one of those groups will automatically grant access to the SQL Server database.

P2000 Authentication

The third level of authentication for a P2000 Workstation is the list of users configured into the P2000 software. When the P2000 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 P2000 software. The Workstation is also checked against the list of valid workstations configured into the P2000 system.

Testing the Workstation

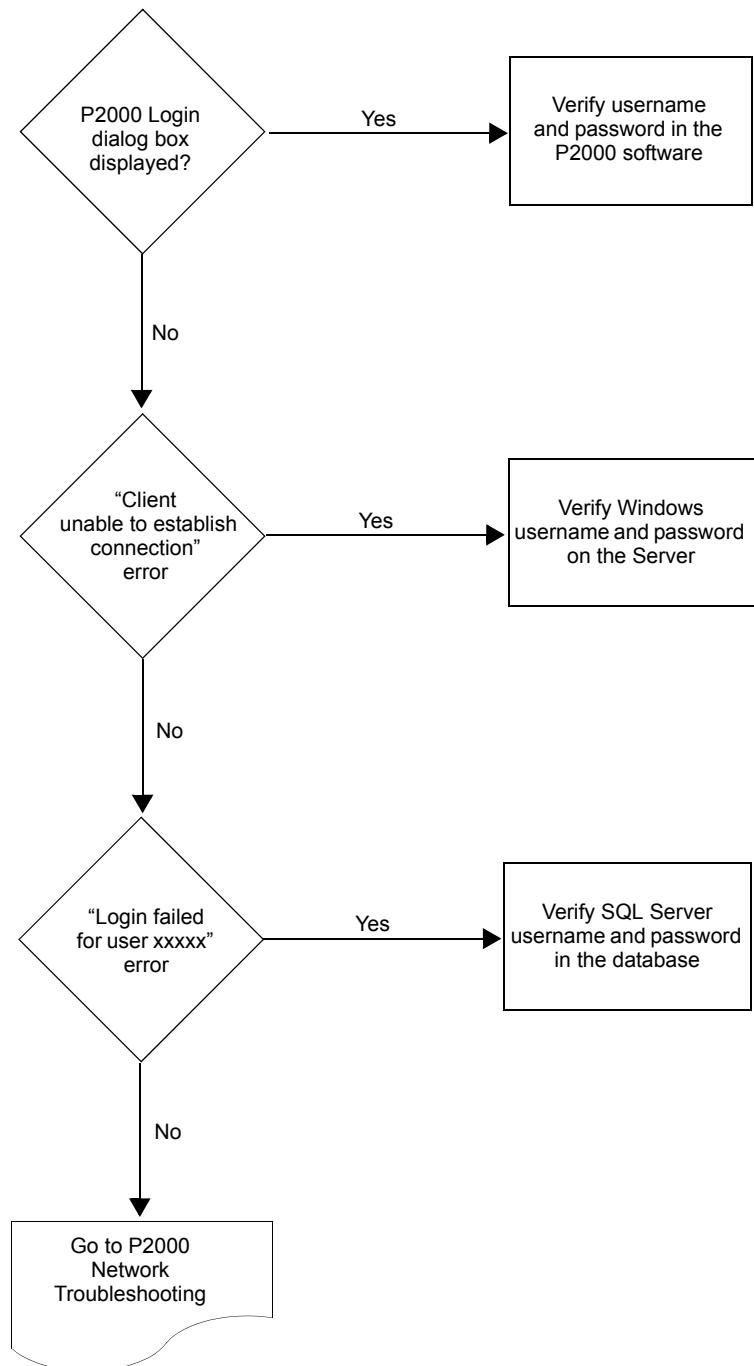
Launch the P2000 software and log on with the correct username and password. If the login succeeds, everything is OK. If the login fails, see the “P2000 Login Troubleshooting” on page 559.

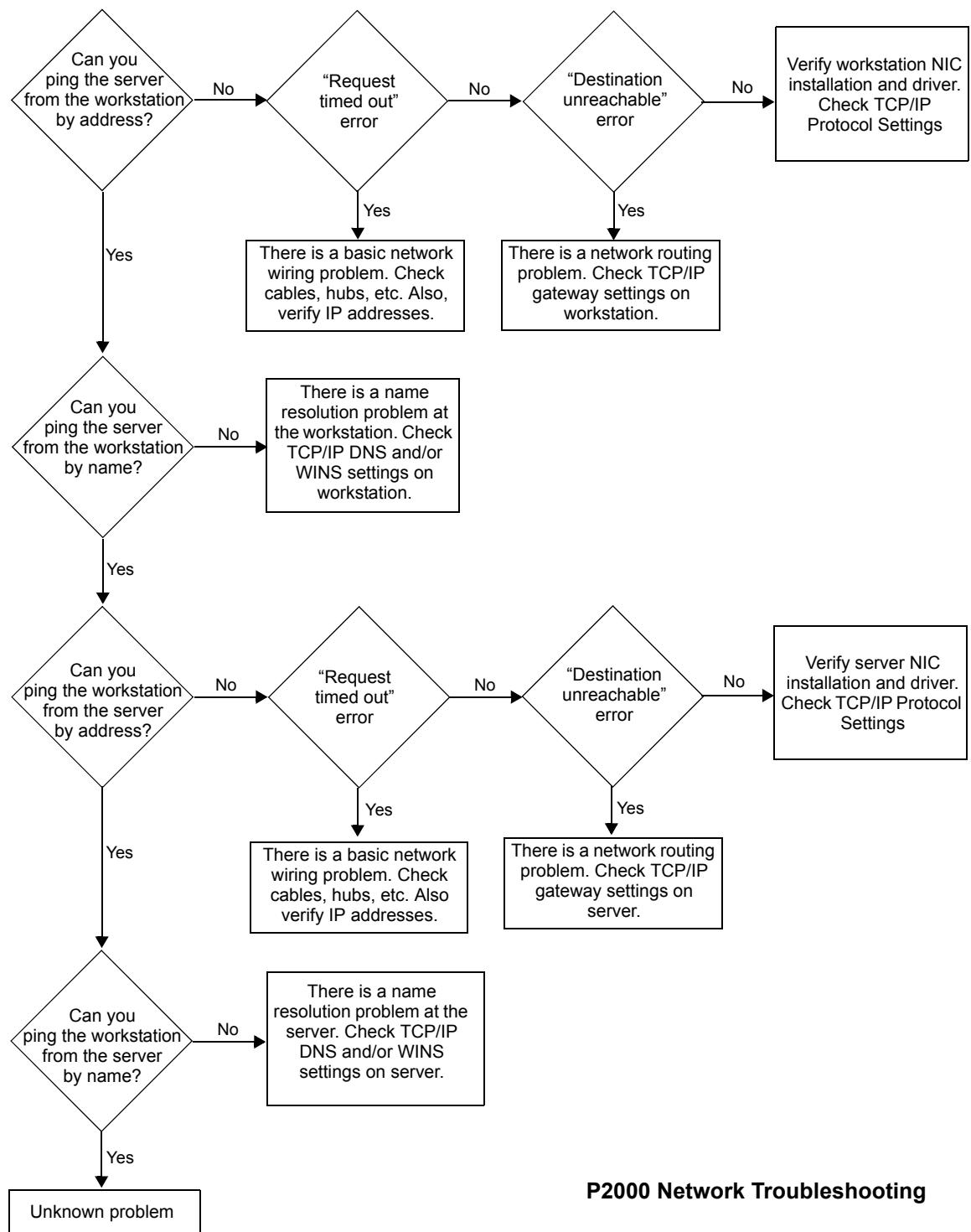
Troubleshooting Workstation Problems

If the P2000 Login dialog box displays, follow “P2000 Login Troubleshooting” on page 559. Otherwise, follow “P2000 Network Troubleshooting” on page 560.

For troubleshooting CCTV, see “CCTV Control Troubleshooting” on page 561.

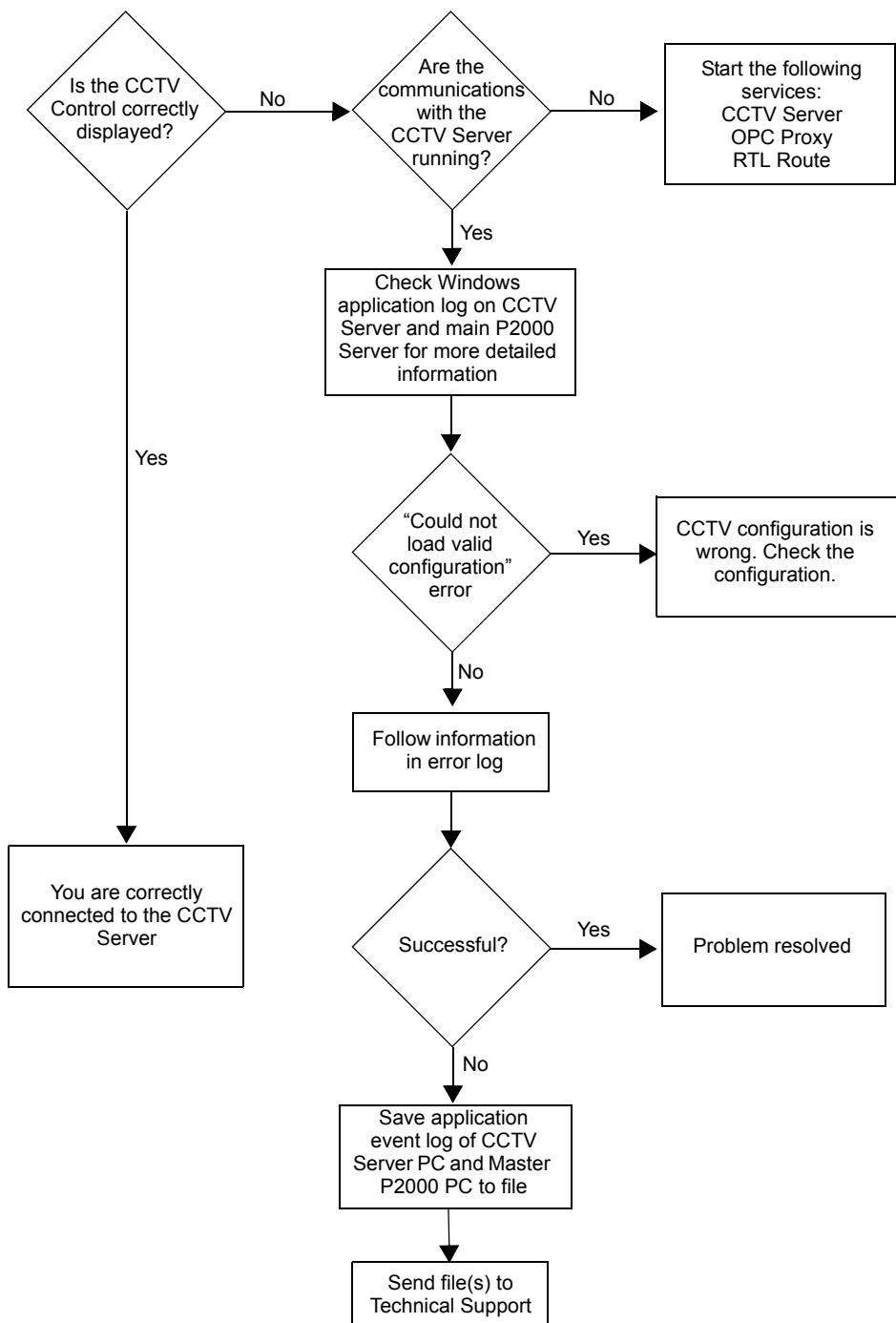
P2000 Login Troubleshooting





P2000 Network Troubleshooting

CCTV Control Troubleshooting



PRELIMINARY

Appendix I: Secured Premises Notification Settings

The following steps are specific for panels that support the Panel Card Event feature, and are necessary to ensure UL 1076 compliance when you use a panel card event to unsuppress (arm) life safety alarm signals.

According to UL 1076 requirements, if you unsuppress life safety alarms at the protected premises (for example, through a panel card event), when this event is invoked, you must receive an indication, either audible or visible, that the P2000 Server received the message that the panel generated after the event was processed. If you do 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.

Before you define the Host event configuration (page 564), you should verify the following settings. Use your discretion to program any parameters not specified.

Cardholder Configuration

1. Create a badge for a cardholder with an **Event Privilege** equal to or greater than the panel card event privilege level used for suppressing/unsuppressing life safety alarms.

See “Entering Badge Information” on page 237 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. See “Configure Hardware Components” on page 59.

Input Point Configuration

1. You must set the life safety input point’s **Status** to **Enable**.
2. Set the **Disabled During Time Zone** option to <none>.
3. From the **Alarm Priority** drop-down list, select 4, 3, 2, 1, or 0, depending on individual company policy for life safety alarms.

See “Create Input Points” on page 96.

Output Point Configuration

1. You must set the output point’s **Active State** to **Timed**.
2. Set the **Duration** to 5 seconds or longer.
3. You must wire the output point to an audible or visible indicator. Depending on the terminal type used and the device selected, you may need to supply external power for the indicating device.
4. The indicator must be visible or audible from the point (location) the panel card event is deactivated.

See “Create Output Points and Groups” on page 94.

Input Group Configuration

1. Define the input group that you will use with the panel card event, and that includes the life safety alarm input points defined in “Input Point Configuration” on page 563.
See “Create Input Groups” on page 103.

Panel Card Event Configuration

1. Select an appropriate **Privilege Level** for use with the card.
2. You must set the event’s **Trigger Type** to **Card/Keypad Code** or **Card/PIN/Keypad Code**.
3. Set the **Event Duration** to **0**. (The panel card event must 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.
See “Create Panel Card Events” on page 105.

Host Event Configuration

To meet the UL requirement, you must create a Host event, 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 the badges that are allowed to unsuppress life safety alarms.

4. Define the **Action** condition as:

- **Delay:** 00:00:00 (none).
- **Category:** Outputs.
- **Type:** Set Output - Timed.
- **Outputs:** select the output defined in “Output Point Configuration” on page 563.
- **Duration:** 0 seconds.

See “Creating Events” on page 314.

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 cardholder 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 cardholder 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

A

A/D values 170
 Abort Time 356
 access deny 42
 access grant 42
 Access Grant Message 187
 Access Grant Message on Door
 Open Only 79
 Access Groups 218
 creating an access group 219
 Access Privileges 229
 Access Requests 8
 badge privileges 8
 invalid badges 8
 time 8
 valid badges 8
 Access Rights 241
 Access Template 222, 243
 apply options to badges 244
 creating an access template 222
 field definitions 222
 access time 83, 194
 Account Disabled 26
 Acknowledgement Required before
 Completion 99
 Action Date/Time 259
 Action Interlock Errors 349
 Action Interlock Operation 347
 Action Interlocks 347
 Action Interlocks tab 348
 Actions 317
 create an action 317
 definitions 318
 order of occurrence 317
 Activate TTL-1 157, 158
 Activate TTL-2 157
 Activated Devices 361
 Active Tours 361
 active-off 101
 active-on 101
 ADA Compliance 195
 ADA Relay Connector 86
 ADA Relay Delay 86
 ADA Relay Time 86
 Add Hardware Module 89
 Add Visitor 246
 sponsor information 248
 ADS Repository Name 351
 ADS/ADX server 350
 Air Crew PIN 74, 89
 alarm beep 260

Alarm Category 255, 259
 Alarm Category Filters 214
 Alarm Colors 262
 alarm debounce time 81
 Alarm Description 259
 Alarm Details 262
 Alarm Escalation Ranges 213
 Alarm Instruction 98
 Alarm Late 357
 Alarm Monitoring 255
 acknowledge alarms 256, 260
 activate an event 262
 alarm handling 256
 alarm monitor definitions 258
 alarm response 261
 audible alarm button 260
 complete an alarm 257, 261
 date/time 258
 escalation 258
 locate alarms on maps 260
 priorities 258
 priority sounds 258
 refresh the window 257
 remove an alarm 257, 261
 respond 256, 260
 Alarm Options 41, 97, 119
 Alarm Popup 98
 Alarm Priority 98
 Alarm Processing Group 26
 alarm shunt only for aux. access 78
 Alarm Site 260
 Alarm Skip 357
 Alarm State 259
 Alarm Status 259
 Alarm Timezone 98
 Alarms 9
 door alarms 9
 external device alarms 9
 host alarms 10
 remote alarms 10
 software only alarms 9
 Alarms, Auxiliaries, Macros and
 Tours 379
 Allow Any IP Address 53
 Allow devices 346
 Allow expansion 293
 Allow Manual Trigger 315
 Allow Multiple Alarm Handling 27
 allow PIN after badge 78
 Alternate Enterprise Site 406
 Always upload when greater
 than 65
 American Dynamics Switch 511
 Maximum and Default
 Values 512
 Supported CCTV Controls 511
 Supported CCTV Event
 Actions 511
 Supported OPCWrite Event
 Actions 512
 annunciation mode enabled 83
 Annunciator 302
 Anti Passback Violation 167
 anti tailgate 79
 anti-passback 83
 Any Guard 357
 Application Engineering
 Import 450
 application path 54
 Apply Security Options
 'Enterprise' 408
 Apply Security Options
 Enterprise 240
 Approval Levels 412
 Approved Visits 247, 421
 Area Alarms Setting 282
 Area Control 280
 Area Filters 285
 configure the Area 280
 control the Area 283
 display details 285
 reports 288
 Terminals and Inputs Points 282
 Area Details 285
 Area Filters 285
 Area Layout 287
 armed 302
 ASSA ABLOY Door Locks 172
 Assa Abloy DSR Interface
 Service 433
 Assisted Access 85
 Assisted Access Time 86
 Associated AV Channel 99
 Associated Real Time Map 99
 At Risk 290, 301
 Audit Trail 46, 395
 Authorized Users 396
 Auto Added 221
 Auto Badge Management 249
 Auto Duress Alarm 357
 Auto Employee Id 227
 Auto Forward 356

- Auto Process 412
 Auto Relock 115
 Auto Reverse 356
 Automatic Software Updates 437
 Aux Input 117
 Aux Output Control 117
 Auxiliary Access 9
 AV Service 433
- B**
- Backup Data (Append) 450
 Backup Data (Overwrite) 450
 Backup DB to Flash Interval 63
 Backup Images (Append) 450
 Backup Images (Overwrite) 450
 Backups 452
 advanced 454
 automatic 455
 backup device 47, 453
 manual 454
 restoring database 456
 BACnet Action Interlocks 347
 BACnet Interface 63, 343
 System Setup 345
 Theory of Operation 343
 BACnet Internal Address 346
 BACnet object 343
 BACnet Query String 347
 BACnet Routed 346
 BACnet Service 343, 433
 BACnet Site Options 345
 BACnet Troubleshooting 348
 Badge Data
 badge field definitions 238
 entering badge information 237
 Facility Code 238
 issue level 238
 viewing 244
 Badge Edit Style 44
 Badge Format 131, 158, 168, 182
 Badge Formats 223
 Badge ID Allowed 146
 Badge Information 244
 Badge Override 146
 Badge Purpose 224, 239
 Badge Reason 239
 Badge Reasons 224
 Badge Resync 250
 Badge Station 22, 338
 Badge Trace Alarm for Denied
 Access 41
 Badge Trace Alarm for Granted
 Access 41
 Badge Transaction History 244
 Badge Type 44
 Basic Configuration 6
 Basic System Components 2
 external device 5
 field panels 4
 Server 2
- system printer 4
 terminals 5
 workstations 3
- Basic Window Components 14
 boundary bar 14
 command buttons 16
 drop-down lists 14
 entry fields 16
 field names 16
 group box title 16
 hot keys 16
 list box 16
 maximize/restore buttons 14
 minimize button 14
 scroll bars 16
 system menu button 14
 tabs 16
 window title 14
- Begin Suppression 280
 BetaTech Switch Protocol 513
 Maximum and Default
 Values 514
 Supported CCTV Controls 513
 Supported CCTV Event
 Actions 513
 Supported OPCWrite Event
 Actions 514
 Switch Configuration 513
 Bind Server 48
 Blanking Time 253, 254
 BQT Reader with LCD 80
 Broadcast Port Number 67
 Bulk Badge Change 245
 Bypass Off 309
 Bypass On 309
 bypassed 302
- C**
- Cabinet Access Control 202
 Cabinet Configuration 204
 Cabinet Door Groups 206
 Cabinet Door Masks 204
 Cabinet Door Names 203
 Calculate Digital Signature 450, 459
 Calibrate 88, 148, 151
 Calibrate with Resistor 148, 152
 Calibration 101
 Camera Auxiliaries, Patterns and
 Presets 386
 Camera Controls 384, 391
 Camera Movement Actions 509
 Cameras 374, 383
 Card Bits to Use 158
 Card Events 10
 Card Formats 88
 Card Mode 111
 card parity 108
 Card Type 87
 Cardholder Data 231
- cardholder email address 413
 Cardholder Information 325
 Cardholder Options 220
 Cardholder Override/Shunt 84
 Cardholders
 cardholder field definitions 231
 cardholder image 234
 cardholder information 230
 cardholder types
 regular 231
 visitor 231
 edit cardholder information 236
 Journals 234
 searching 236
 user defined fields 235
 visitor sponsor 233
 CCTV 367
 Components 374
 Control 387
 Event Actions 392
 Naming Conventions 371
 Reports 394
 Server 374, 375
 Standard Control Buttons 388
 Switch Communications 378
 System Hardware 370
 CCTV Server 433
 CCTV Server Namespace 531
 CCTV Switch Protocols 509
 central 83
 central Enterprise site 406
 Change Style 240
 Choices 226
 CLIC Components 120
 CLIC PIN 117
 Clock Battery 149
 Comms Server 41
 Communication
 downloads 8
 operating modes 7
 central 7
 local 7
 shared 7
 transactions 8
 Communication Modes 7
 Companies and Departments 220
 defining a company 220
 defining a department 221
 Company 232
 Concealed UDFs 28
 Configuration Sequence 19
 Configure Cameras 383
 Configure CCTV Servers 375
 Configure Monitors 380
 Configure Switches 376
 Configuring Hardware
 Components 59
 Configuring System
 Components 37
 Contractor Request 419
 Control all Doors 274

- Control Station Groups 403
- Control Sub-Stations 403
- Controls
 - Camera 391
 - Monitor 390
 - Switch 389
- Convert to Current Version After Restore 457
- Count All 282
- Count Inputs 282
- Count Terminals 282
- Counters 275
- Create NT user account on server 26
- Cross Site Access Group Editing 41
- Current Count 286
- Custom Configuration Number 63
- Custom Reports 477
 - create custom reports 477
 - edit reports in Crystal 478
 - export existing reports 478
 - import custom reports 477
- D**
- D620 Mode 194
- Database and Namespace 370
- Database External Trigger 53
- Database Maintenance 449
 - advanced backups 454
 - automatic backups 455
 - backup device 453
 - database backup 452
 - database restore 456
 - manual backups 454
- Database Server 406
- Database Table Definitions 477
- Daylight Savings Time 132
- Daylight Savings Used 145, 164
- DB Server 41
- DCOM Configuration 545
- DCOM Installation 545
- Debounce Time 151, 170
- Default Alarm Colors 262
- Default Timezone 219
- Degraded 298
- Delay Downloads Until 440
- Delayed download for badges and access groups 49
- Delete all badges from OSI database 450
- Delete all hardware from OSI database 450
 - delete badges from panel before download 430
 - delete elevators from panel before download 430
- Delete Expired Visitor Badges 450
- Delete history older than 65
- Delete Selected Alarm 450
- Delete Unused Access Groups 450
- Delete Visitors Without Badges 450
- De-Muster 293, 299
- Deny If Door Open 79
- Department 220, 232
- Destination Entry Computer 195
- Details 364
- Direct Output Control 187
- Directory Services Password Validation 27, 29, 412
- Directory Services Path 29, 48, 412
- Disable Alarm 98
- disabled during Time Zone 97
- Disarmed 302
- Display All alarm options 262
- Door Configuration 206
- Door controls 273
- Door Forced - Alarm 115
- Door Forced - Warning 115
- Door Open - Alarm 115
- Door Open - Warning 116
- Door Open Warning 84
- Door Tracking 205
- Download Access Groups of badge 49
- Download badges with Undefined entry/exit status 49
- Download Function 429
- Download options 49
- Download Service 433
- Download Status 430
 - by panel 430
- Download to disabled panels 49
- Download to STI-E 241
- Drill 299
- Dual Ethernet 64
- Dual Reader 114
- Duplicate Maps 332
- duress 108
- Duress Alarm 358
- DVR 394
- E**
- Edit Button Image 333
- Egress Actions 116
- Elevator Access Grant 187
- Elevator/Cabinet Parameters 202
- Elevators 186
 - basic definitions 187
 - configuring 192
 - general overview 186
 - high level interface 188
 - low level interface 187
- Email 232
- E-mail setting 51
- Emergency Access Disable 419
- Emergency Override 205
- Empty Alarms 450
- Empty Alarms History 450
- Empty Archive Database 450
- Empty Audit History 451
- Empty Download Queue 451
- Empty Fire Data 451
- Empty Guard Tour Note 451
- Empty Intrusion Data 451
- Empty Saved Muster Data 451
- Empty Smart Download Queue 451
- Empty Transaction History 451
- Enable Codes 74
- Enable Input Suppression Messages 68
- Enable Mifare Encoding 426
- Enable Monitoring Action 115
- Enable Otis PIN 195
- Enable Panel Inputs 143
- enable panel relay group outputs 67
- Enable PIN Duress 69
- Enable Printing 326
- Enable Reporting 119
- Enable Secondary Interfaces 144
- Encoder Configuration 424
- Encryption 68, 143, 155
- Encryption Key 155, 163
- Endura Interface Service 433
- enforce entry/exit 66
- Enforce Limitations 43
- Enterprise 3, 405
 - Access Groups 407
 - Global Access Rights 408
 - Parameters 406
 - Sites 233, 406
 - Time Zones 407
- Entry Exit Delay 97
- Escalation 99
- Escalation based upon visibility 100
- Escalation Increment 100
- Escalation Repeat 100
- Escalation Service 433
- Escalation Timeout 100
- Event 1-4 99
- Event Action Types 491
- Event Actions 317
- Event Counters 319
 - add event counters 320
 - edit event counters 320
 - reset event counters 320
 - view event counters 320
- event duration 107
- Event Privilege 241
- Events 10
 - card events 10
 - create events 314
 - event configuration 314
 - system events 10
 - timed events 10
- Exact Match 237, 245, 251, 285
- Executive Privilege 241
- Expand Zone 300
- Expiration Period for Requests 411
- Export 330
- Extended Access 9
- Extended Access Flag 130

Extended Access Time 130
Extended Shunt Time 130
External Event Trigger 52
External IPs 346
External Trigger Service 434

F

Facility Code 46, 69, 87
facility code only when offline 78
Failed Attempts Lockout 167
failed download connections 440
failed download transfers 440
FASC-N Badges 44, 239
Fast Flash 95, 275
FDA 48
 Enforce Part 11 48
FDA Backup Performed 451
FDA Backups 47, 455
FDA Retention Policy 47
FDA Title 21 CFR Part 11 395
Field Separator 71
File External Trigger 52
Fire Alarm 267
Fire Devices Configuration 269
Fire Panel Status Details 441
Fireman Override 193
Fixed Period 115
Flags 276
Floor Configuration 196
Floor Groups 202
Floor Masks 191
Floor Names 191
Floor Tracking 195
Force Logoff 437
Force Value 276
Forced Arm 308
forced door/propped door 108
Format media on backup 455
forward and reverse 7
Found in DB 247, 421
Four-Digit PINs 94
FS (Full Screen) 253
Fully Qualified Name 350

G

General ASCII Protocol 510
 commands supported 510
Generate namespace based on
 protocol defaults 378
Gutebrück Switch Protocol 515
 Maximum and Default
 Values 517
 Supported CCTV Controls 515
 Supported CCTV Event
 Actions 516
 Supported OPCWrite Event
 Actions 516
Global Badge Entry/Exit Status
 Synchronization 40

Global In-X-It Tracking 40
Global Sub-Station 401
Grant Only 357
Group Controller Address 68
Guard 353
Guard Tour 352
 adding stations 358
 assigning to a specific guard 357
 assigning tour badges 353
 configuring guard tours 354
 control all tours 361
 controlling guard tours 361
 Details 364
 forward and reverse 352
 guard tour priority 354
 principles and definitions 352
 scheduled times 356
 system hardware 353
 tour abort 353
 traversal time 360
Guard Tour Control 361
Guard Tour Priority 241
Guard Tour Reports 366
Guard Tour Service 352, 434

H

Hardware Configuration 59
Hardware Module 89
Heartbeat Interval 155
Heartbeat Transmit Interval 143, 163
Help 17
 context sensitive 17
 online 17
HID Input Points 168
HID Interface Service 434
HID Output Points 170
HID Panels 160
HID Terminals 164
Hide from MIS 226
Hide reports 478
High Level Interface 188, 194
High Priority 431
High Speed RS485 62
History Retention Period 144
Holidays 57
 adding a holiday 57
 assigning holiday types 58
 holiday calendar 58
 changing the month 58
 changing the year 58
Host Fails Deny 83
Host No Reception Timeout 143, 163
Host Poll Timeout 64
Hours On Site 311
 Reporting 312
 Zones 311
HTTP Disconnect Delay 144

I

I/O latching 82
I/O Linking 101
I/O linking points 82
Ignore Characters 71
Image Recall 252
 activate 253
 filters 252
Image Recall FS 253
Import Standard Values 170
importing an image 340
Initialize media on backup 455
Inoperable 297
Input and Output Points and
 Groups 94
Input Count 286
Input Point Suppression 279
Input Points
 input point field definitions 97
 non-alarms 10
 reader terminal hardwired 102
 configuring a reader terminal
 down 103
 configuring reader terminal
 door contact 102
 door contact input points 102
 using input point 25 103
Input Points and Groups 96
 creating input groups 103
 creating input points 96
Input/Output Mode 146
Instruction Conventions 16
 menu shortcuts 17
Instruction Text
 creating instruction text 104
 inserting macros 105
Intercom 396
 Control 402
 Events 404
 Exchange 397
 Real Time Map Control 404
 Stations 400
Intercom Interface Service 434
Interface Type 115
Intrusion Alarms 306
Intrusion Area 302
Intrusion Configuration 303
Intrusion Control 308
Intrusion Detection 301
Intrusion Events 311
Intrusion Interface Service 434
Intrusion Panel Status Details 440
Intrusion Status 310
Intrusion Transactions 309
Invalid Logins 48
IO Modules 271
IPL version 440
Isonas Input Points 158
Isonas Interface Service 434
Isonas Output Points 159
Isonas Panels 154

- Isonas Terminals 155
Item Name Filters 212
- J**
Journal 234
- K**
key switch enabled 83
Keyless Override/Shunt Time 85
Keypad 547
keypad code 107
Keypad Credential 130, 131
Kill All Reports 451
KONE 188
- L**
LAN (local area network) 3
language selection 54
languages 54
Last poll communication 440
latch output 67
Late Alarm 358
Launch Automatically 22
Legacy panel access group
 download disable 49
Load Archive Database from
 Backup 451
Load Language Reports 463
local 83
Local Alarms 50, 258
Local Anti-Passback
 Forgiveness 111
Local Configuration 54
Local Site 53
Lockout 273
Log Operator Action 358
Log Output Status Message 70, 81
Log Reader Strike Message 70, 79
Log Tour Operation 358
Logging on to P2000 11
 changing the default login
 name 12
 default login values 12
 passwords 11
 Super User 12
 User Name 11
Logging Out of P2000 13
Loop Communication 7
Loop Configuration 60
Loop Number 64
Loop Timeout 65
Low Level Interface 187, 194
Lowest Floor for Group
 Controller 68
- M**
M3/M5 Workstations 343
- MAC Address 143
Mac Address 137
Machine Room Enclosure 194
Magnetic Stripe 131
Main Menu 5
Manager Flag 130
Manual Conventions 2
Manual Process 412
Manual Reset 357
Manual Tour 356, 363
map icons 330
Map Maker 326, 328
 create an importable image 329
 image sets 332
 import an image 329
 map attachments 332
 normal map 329
 place device icons 330
 popup map 329
 system map 329
Mark Secondary Tables 451
Master Station 401
Max Allowed 281
Max Allowed Alarmed 284
Max Badge Number 44
Max Inactive Period 40
Max Issue Level 44
Max PIN Code Digits 41
Max Security Level 44
Max Visitor Validity Period 40
Maximum Attempts 167
Maximum Entry Time 167
Message Filter Configuration 258,
 322
Message Filter Group 23, 50, 215,
 258
Message Filtering 207, 208
Message Forwarding 266
Message Routing 207, 216
Message Routing Status 260
Message Types 210, 499
Metasys 343
Metasys system extended
 architecture 349
Mifare Encoder 424
Migrate 227
Migrate Panel 451
Milestone Interface Service 434
mimic 101
Min Required 281
Min Required Alarmed 284
MIS image folder 342
MIS Interface 341
 input and output tables 342
 partitioned systems 342
 prerequisites 341
 using the interface 342
MIS Interface Service 434
MK2 114
Momentary Auxiliary Access 146
momentary auxiliary access 79
- Monitor Controls 390
Monitor Sequences 382, 510
Monitoring Remote Alarms 257
Monitors 374, 380
Mouse Conventions 13
MSEA Graphic 100
MSEA Graphics 349
MSEA Registration 351
Muster 289
Muster Control 291
Muster Control Service 434
Muster Reports 292
Muster Shift Setup 293
Muster Startup Rules 292
Muster Terminals 289, 294
Muster Zone 289
Muster Zone Alarm Settings 293
Mustered 290, 301
Mustering 289
 control 297
 define Muster Zones 290
 events 296
 reports 300
- N**
NAE controller 350
Name for DNS Address
 Resolution 143
Namespace
 Changing Number of Items 373
 Naming Items 371
 Number of Items 372
 Number of Permitted Items 372
Namespace and Database 370
Namespace entries to be
 generated 378
Namespace Tags 532
 Alarm 543
 Auxiliary 543
 Camera 539
 Macro 543
 Monitor 537
 Pattern 544
 Preset 544
 Sequence 544
 Switch 532
 Tour 543
Navigating through the System 13
Network Communication 6
Network Panel 439
network timeout 64
Nice Interface Service 434
N-Man Rule 86
No Access Group Archive to
 Flash 63
No Badge Archive to Flash 63
No Configuration Archive to
 Flash 63
No Green Light on Aux Access 79
No. of PIN Retries 70

None.wav 260
 Normal and FASC-N 44, 239
 Normal Instruction 99
 Normal Popup 98
 Normal Priority 431
 Notification Class objects 343
 Number of Doors 41
 Number of Floors 41
 Numeric Key Pad 156

O
 ODBC Data Source 54
 offline card search 83
 OnSSI Interface Service 434
 OPC Name 377
 OPC Proxy Service 434
 OPC Server 318
 OPC Tag 319
 Open for Access Time 273
 Operate Door Strike 107
 Operating the System 229
 Operational Mode 171
 Operator Controls 273
 control doors 273
 control panel relays 275
 Operator Name Filters 214
 Operators 23
 Account Type 26
 adding operators to the system 23
 assigning operators 25
 editing an operator entry 28
 messages 207
 Optimize for LAN 54
 Optimize for WAN 54
 Option Keys 38
 OSI Access Groups 133
 OSI badges 131
 OSI Facility Access Groups 133
 OSI Facility Parameters 129
 OSI Interface 127
 OSI Interface Service 434
 OSI Panels 127, 136
 OSI Terminals 137
 OSI Wireless Devices 140
 OSI wireless readers 444
 Otis Compass 189
 Otis Compass Elevator Modes 190
 Otis Compass Elevator Options 243
 Otis EMS - Security / BMS 188
 Otis Interface Service 434
 Otis Unsecured Elevators 196
 Out Of Order Alarm 358
 Output Control 274
 output delay 68
 Output Link 151
 Output Points and Groups 94
 creating output groups 95
 creating output points 94
 Output Relays 10
 activated by events 10

activated manually 10
 input linking 10
 output linking 10
 Override 241
 Override Reset Threat Level 82,
 147

P

P2000 Authentication 558
 P2000 Location 3, 208
 P2000 Remote Server 208, 216,
 258, 323
 P2000 Services 432
 P2000 Services Definitions 433
 P2000-Metasy 343
 P900 CLIC Controls 275
 counters 275
 flags 276
 trigger event 276
 P900 Panels 109, 111
 Addressing Principles 112
 Counters 121
 Flags 121
 Inputs/Outputs 117
 Soft Alarms 120
 System Parameters 110
 Trigger Events 122
 Trigger Links 126
 P900 Sequence Files 110
 P900 SIO Handler Service 434
 P900 Terminals 113
 P900 Trigger Events 276
 Panasonic Switch Protocol 518
 Maximum and Default
 Values 519
 Supported CCTV Controls 518
 Supported CCTV Event
 Actions 519
 Supported OPCWrite Event
 Actions 519
 Switch Configuration 518
 Panel avg. clock drift (seconds) 440
 Panel Battery 149
 Panel Card Events 105
 creating a panel card event 106
 field definitions 106
 Panel Card Formats 75
 Panel Comparison Matrix 503
 Panel Details 439
 panel lost AC 109
 panel low battery 109
 Panel max clock drift (seconds) 440
 Panel Poll Interval 64
 Panel Relay Control 275
 panel tamper 109
 panel time zones 72
 Panel Types 42
 Panel UTC Offset 144, 164
 Panels 4, 59
 adding a new panel 61
 configuring panel components 71
 configuring panel holidays 73
 assigning a panel holiday 73
 configuring panel time zones 72
 assigning a panel time zone 72
 output groups and panel time
 zone 73
 edit panel field definitions
 access tab 66
 address tab 63
 alarm tab 67
 elevator tab 68
 general tab 62
 history tab 65
 loop/unit tab 64
 mag format tab 71
 misc tab 69
 naming conventions 59
 panel field definitions 62
 Partial Match 237, 245, 251, 285
 Partition Name Filters 211
 Partitions 10, 335
 creating partitions 337
 deleting partitions 337
 regular 336
 super user 336
 types 336
 Password change 29
 Password Mode 53
 Password Policy 47
 Password Validation 47
 Password Verification 17
 Passwords
 expiration 26
 Peer to Peer Badge Sync 66
 Pelco Switch Protocol 520
 Macro Programming 522
 Maximum and Default
 Values 522
 Recording Patterns 522
 Supported CCTV Controls 520
 Supported CCTV Event
 Actions 521
 Supported OPCWrite Event
 Actions 521
 Periodic Service 434
 Permission Groups 23
 creating permission groups 23
 Permissions 27
 Personalized Access Groups 243
 Philips Burle Switch Protocol 523
 Cabling Configuration 525
 Maximum and Default
 Values 525
 Supported CCTV Controls 524
 Supported CCTV Event
 Actions 524
 Supported OPCWrite Event
 Actions 524
 Switch Macros 523
 PIN 93
 PIN + Card ID 93

- PIN Code 41, 238
 - configuring 92
- PIN Code Digits 67
- PIN code retry 108
- PIN Code Timed Override 70
- PIN code type 67
- PIN Duress 94
- PIN Only 92
- PIN Plus 1 Duress 70, 80
- PIN required when offline 78
- PIN Retry Alarm 94
- PIN Suppression 147
- PIN suppression 87
- PINpad 116
- poll 7
- Port Configuration 49
- Portal Gateway 127, 134
- Power Failure 149
- Pre Max Allowed 281
- Pre Max Allowed Alarmed 284
- Predefined Alarm Response
 - Text 261
- Preferred Loop Direction 65
- preferred primary communication path 63
- Preprocessed reports 466
- Prevent Editing Employee ID 227
- Print All 260, 326
- Print Displayed 260, 326
- Priority Ranges 213
- Priority Service 433
- privilege level 106
- Process Received Remote
 - Messages 50, 258, 323
- Processing Mode 412
- Programmer Flag 130
- Property Number 347
- Proposed Door 165
- Protocol 377
- Protocol Type 68
- Proximity Reader 156
- public 22
- Public Access Timezone 196, 206
- Push to Talk 402

- Q**
- Query String 62, 260
- Query String Filters 211
- Queued Download Actions 431

- R**
- Radionics 264
- Random Watch 356
- Rapid Eye Interface Service 434
- Raw 128 Bit 148
- RAW reports 466
- reader 78
- Reader Holdoff Time 111
- Reader Mode 146
- reader override timezone enable 79
- Reader Sign On Badge 131
- Real Time List 322
 - color coded transactions 324
 - printing 325
 - view all options 324
 - view specific options 324
- Real Time List Transactions 323
- Real Time Map 326
 - activate events 328
 - create a real time map 328
 - open a door 328
 - sub maps and attachments 326
 - view the real time map 327
- Real Time Printing 41
- Reboot 139
- Reboot and Clear DB 140
- Reboot on any failure 433
- Rebuilding the WAMS
 - Database 140
- Receiving Messages 51
- Record Persistence 396
- Record Retention 396
- Record Validation 396
- Redundancy 395
- Reestablish Delay 65
- Registration Parameters 6, 38
- relay enabled 83
- Relay Time 115
- Re-lock on Door Open 79
- Remain Time 362
- Remote Alarms 51, 257, 258
- Remote Message Service 50, 257, 322, 435
- Remote Messages in Real Time 322
- Remote Partitions 28
- Remove Access Groups from
 - Disabled Badges 451
- Remove Expired Access Groups
 - from Badges 451
- Repeat Transaction Delay 111
- Report Alarm 205
- Report Configuration 478
- report on terminal 109
- Report Strike Status 146
- reporting delay 67, 97
- Reports 463
 - alarm history report 471
 - cardholders without badges report 474
 - cardholders-preprocessed report 472
 - custom reports 477
 - database table definitions 477
 - definitions 466
 - field/table relationship 477
 - load language reports 463
 - panel report 475
 - print 464
 - samples 471
 - transaction history report 476

- S**
- S321 SIO Handler Service 435
- S321-DIN Panels 448
- S321-IP Input Points 148
- S321-IP Interface Service 435
- S321-IP Output Points 152
 - Operational Mode 153
- S321-IP Panels 141
- S321-IP Terminals 145
- scramble mode 67
- searching for cardholders 236
- Secure Authentication 48
- Secured Premises Notification Settings 563
- secure-off 101

- secure-on 101
 - Security Level 70, 241, 277
 - Security level control 277
 - Security Options 240
 - Send Email to Request
 - Approvers 411
 - Sensor 26 Bit 148
 - Sequence Number 359
 - Sequester 301
 - Sequester Terminals 289, 295
 - Sequestered 290
 - Serial Panel 439
 - Server 2
 - Service Controls 435
 - stop and start services 435
 - stop/star a specific service 436
 - stop/start all services 436
 - Service Monitor 436
 - Service Override 193, 205
 - Service Startup Configuration 432
 - Set Alarm Color 362
 - Set all Input Status to Unknown 452
 - Set all Output Status to
 - Unknown 452
 - Set all Panel Status to
 - Unknown 452
 - Set all Terminal Status to
 - Unknown 452
 - Set Computer Default
 - Language 452
 - set panel relay when active 97
 - shared 83
 - Shared Path 438
 - Show All 284, 285
 - Show Only 284, 285
 - Show UDF Fields 253
 - Shrink Database 452
 - Shunt Alarm on Request to Exit 146
 - shunt devices 361
 - Shunt Terminal
 - (Anti-Passback) 116
 - shunt time 83
 - Shunt Warning Auto Off 84
 - SIA Device 265
 - SIA Interface 264
 - SIA Interface Service 435
 - SIA Message View 265
 - Sign On Key 130
 - Silence 309
 - SIO Handler Service 435
 - Site Director 350
 - Site Name Filters 210
 - Site Parameters 39
 - definitions 40
 - editing 40
 - Slow Flash 95, 275
 - Smart Download Control 431
 - Smart Download Rules 49
 - Smart Download Service 435
 - SMTE Service 435
 - SMTP Hello Domain 51
 - SMTP Server 51
 - Soft Alarms 108
 - enabling soft alarms 108
 - soft alarms field definitions 108
 - Soft Input Points 62
 - soft in-x-it 79, 108
 - Software Updates 437
 - Special Access 9, 41, 86, 241
 - basic access override 9
 - auxiliary access 9
 - extended access 9
 - timed override 9
 - granting badge privileges 9
 - sponsors 233
 - SQL Server Authentication 557
 - Standard Reports 463
 - run a standard report 464
 - Star Feature 80
 - static text objects 331
 - Station Group 401
 - Station Type 359
 - Statistics Update Interval 139
 - Stop Suppression 279
 - Sub-Station 401
 - Super User 11, 12, 336
 - Suppress Input Points 279
 - Swipe PIN 117
 - Switch Controls 389
 - Switch Protocols 373, 509
 - American Dynamics 511
 - BetaTech 513
 - communications 509
 - General ASCII 510
 - Geutebrück GST Interface 515
 - Panasonic 518
 - Pelco 520
 - Philips Burle 523
 - Ultrak 526
 - Vicon 528
 - Switches 374, 376
 - Sync cardholder/badge active
 - flags 452
 - Synchronize OSI Transaction Counter 452
 - System Configuration 19
 - adding configuration items 20
 - editing configuration items 20
 - printing 21
 - searching configuration items 21
 - System Events 10
 - System Maintenance 429
 - system override 66
 - System Overview 6
 - System Status 439
 - Fire Detector 444
 - Fire IO Module 444
 - Fire Zone 443
 - Input Terminals 442
 - Inputs 442
 - Intrusion Annunciators 443
 - Intrusion Areas 443
 - Intrusion Zones 443
 - Legend 439
 - Mustering Zones 442
 - OTIS Elevator Status 442
 - Output Terminals 442
 - Outputs 442
 - Reader Terminals 442
 - Security Level Terminals 443
 - Wireless Parameters 444
 - System Validation 458
- T**
- Tamper Alarm Energize AUX Relay 165
 - TCP/IP External Trigger 52
 - Template Terminal 91
 - Temporary Access 242
 - Terminal Count 286
 - Terminal Groups 91
 - creating a terminal group 92
 - Terminal Lost AC 109
 - Terminal Low Battery 109
 - Terminal Tamper 109
 - Terminal Unsecure 119
 - Terminals 76
 - creating a new terminal 76
 - creating an I/O terminal 81
 - edit terminal field definitions 77
 - access tab 83
 - air crew pin tab 89
 - calibrate tab 88
 - card type tab 87
 - facility codes tab 87
 - flags tab 78
 - general tab 77
 - legacy tab 82
 - timezone tab 87
 - legacy tab
 - AMT box 83
 - STI-E box 82
 - set up terminals for each panel 76
 - Terminals associated with
 - Timezone 45
 - This Location Only 419
 - time offset 66
 - time pairs 45
 - Time Zones 55
 - active/inactive 56
 - configuring time blocks 55
 - copying a time zone 57
 - creating a new time zone 56
 - holiday types 57
 - Timed Button 193
 - Timed Events 10
 - Timed Override 9, 84
 - timed override/anti-tailgate 66
 - Timed Override/Timed Shunt 84
 - Timed Shunt 84
 - Timed Suppression 279
 - Timed/Pulse 275
 - timezone checking 66

- Today Only 419
 Toolbar 18
 Tour Activation 353
 Tour Alarms Setting 358
 Tour Badge 353
 Tour Badge priority 354
 Tour Configuration 354
 Tour Configuration Report 366
 Tour Notes 365
 Tour Notes Report 366
 Tour Station 358
 Tour Transaction Report 366
 Tour Types 356
 Trace 241
 trace 42
 track 101
 Track Movement 295
 Track On Input Open 195
 Track On Transition Only 195
 Transmit Filter 217
 Transmit Queue 217
 Transmit Session 218
 Transmitting Messages 51
 Trapped 290, 301
 traverse time 360
 Trigger Logic 316
 Trigger Manually 321
 Trigger Types 106, 481
 Triggers
 create triggers 315
 edit a trigger condition 317
 field definitions 316
 manual triggers 321
 trigger conditions 315
 Tristate Check Boxes 373
 Troubleshooting
 CCTV Control 561
 Login 559
 Network 560
 Workstation Problems 558
- U**
 UI Style 412
 Ulstyle 424
 Ultrak Switch Protocol 526
 Maximum and Default
 Values 527
 Supported CCTV Controls 526
 Supported CCTV Event
 Actions 526
 Supported OPCWrite Event
 Actions 527
 Switch Configuration 526
 Uncalibrate 88, 101, 148, 152
 unique time pairs 46
 Unit Number 64
 Unlock 273
 Unlock All Doors 172, 274
 Unlocked Time Zone 115
 unreliable icons 327
- unsuppress life safety alarms 563
 Update CK7xx Panels 447
 Update Database Default
 Strings 452
 Update Preprocessed Report Archive
 tables 452
 Update Preprocessed Report
 tables 452
 Update S321-DIN Panels 448
 upload 65
 Upload only when greater than 65
 Upload Service 433
 Use Authorized SMTP 51
 Use Directory Services
 Authentication 412
 Use Encryption 48
 Use for XmlRpc 347
 User Accounts 30
 adding name and password 30
 User Authentication 412
 User Defined Fields 226, 235
 creating user defined fields 226
 User Name 259
 User Site 259
 Username Formatting 48
 Using a Keypad Reader 547
 invoking access requests 547
 invoking air crew access 548
 invoking panel card events 551
 invoking timed overrides 548
 Quick Guide 553
- V**
 valid & unauthorized 79
 Valid Readers for Current
 Event 107
 Validate 418
 Validate Digital Signature 452, 458
 Verify Password for Critical
 Functions 27
 Version description 440
 Vicon Switch Protocol 528
 Camera Lens Speed Control 529
 Maximum and Default
 Values 530
 Momentary and Latched
 Auxiliaries 529
 Supported CCTV Controls 528
 Supported CCTV Event
 Actions 529
 Supported OPCWrite Event
 Actions 529
 Switch Configuration 528
 Video Imaging 337
 defining a workstation 338
 printing a badge 339
 specifications 338
 viewing and printing a badge 340
 View Backup Contents 457
 View Inoperable Hardware 300
- Violation Alert Period 47
 VIP Access 195
 Visitor Escort Mode 87
 Visitor Information 246
 Visitor Management 418
 Visitor Request 418
 Field Definitions 421
 sponsor 422
 visitor validity period 40
 visitors 231
- W**
 WAMS 127
 Wandering 290, 301
 Warning Auto Off 85
 Warning Output Group 84, 85
 Warning Time 84, 85
 Watchdog Service 435
 Web Access 409
 Alarm Monitor 417
 Area Search 417
 Audit 418
 Badge Print 417
 Badge Resync 417
 Cardholder Search 416
 Command Outputs 417
 Customizing the interface 423
 Door Command 417
 Employee Services 416
 Guard Services 417
 In Out Displays 417
 Logging on 416
 Management Services 417
 Menu Permissions 232, 410
 Options 411
 Processing requests 419
 Submitting Requests 416
 WebBadging Setup 418
 Windows Authentication 557
 Wireless Access Management
 Solutions 127
 Workstation Status 436
 Workstation Test 558
 Workstations 21
 adding a workstation 21
 editing a workstation 23
 Launching the alarm monitor 22
 Location 22
 workstation field definitions 22
 Workstations and Operators 21
 World Time Zone Information 144, 164
 Write CK7xx to Flash Memory 446
- X**
 XmlRpc 53
 XmlRpc Interface Service 435
 XPortal Interface Service 435

Z

Zone 297
Zone Hardware Status 297
Zone Name 291
Zone Status 297
Zone Terminals 289, 294

PRELIMINARY