Honeywell

Pro-Watch Software Suite
5.0

7-90107V19 | May 2020



User Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material. HII disclaims all responsibility for the selection and use of software and/or hardware to achieve intended results.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

Copyright © 2020 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidc.com

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

For patent information, refer to www.hsmpats.com.

Copyright © 2020 Honeywell. All rights reserved.

Pro-Watch® is a registered trademark of Honeywell Integrated Security. All other product and brand names are the service marks, trademarks, registered trademarks, or registered service marks of their respective owners. Printed in the United States of America. Honeywell reserves the right to change any information in this document at any time without prior notice.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation. Windows Server is a trademark of Microsoft Corporation.

XPSMTP - Copyright © SQLDev.Net 1991-2006 (<http://SQLDev.Net>)
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of SQLDev.Net nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Binaries, source code and any other parts of this distribution may not be incorporated into any software licensed under the terms of the GNU General Public License (GPL) or the GNU Lesser Public License (LGPL). Binaries, source code and any other parts of this distribution may not be incorporated into any software licensed under any license requiring source code disclosure of derivative works.

Modified redistributions of source code, binaries and/or documentation must carry the above copyright as required by clauses (1) and (2) and may retain the name "SQLDev.Net" in source code, documentation and metadata.

The name "SQLDev.Net" is a trademark of SQLDev.Net B.V. the Netherlands.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Ordering Information

Please contact your local Honeywell Integrated Security representative or visit us on the web at http://www.honeywellintegrated.com/ for information about ordering.

Feedback

Honeywell Integrated Security appreciates your comments about this manual. Please visit us on the web at http://www.honeywellintegrated.com/ to post your comments.

TABLE OF CONTENTS

Chapter 1
Overview of User Functions 1-1

Overview 1-2
Pro-Watch Login 1-3
Changing the Pro-Watch Authentication Type and Login Mode .1-3
Logging In to the Pro-Watch Server 1-5
Changing Passwords 1-8
Pro-Watch Functions 1-9
Function Categories 1-9
Tool Bar 1-12
Verification Window 1-22
Resized Verification Window 1-22
Minimized Verification Window 1-22
Maximized Verification Window 1-22
Two Verification Modes 1-22
Multiple Windows 1-24
Single Window 1-25
Color Coding 1-28
Managing the Server Switchboard 1-29
Badge Manager 1-29
Hardware Manager 1-29
Permissions Manager 1-29
Turning the Wizards Off 1-30
Other Quick Access Links 1-33
Tool and Utilities 1-33
Help 1-33
System Shortcuts 1-34
Pro-Watch System Configuration 1-35
Microsoft Azure Cloud 1-36
Architecture for Pro-Watch Azure V1.2 1-36
Setup Requirements and Virtual Machine Creation 1-37
Connecting to the Virtual Machines 1-37
Networking Rules 1-38
Supported Configurations 1-38
Connecting Cloud Resources with On-Premise Resources 1-39
Supported Components in Cloud 1-40
Installing Pro-Watch 1-40

Chapter 2
Advanced Badging 2-1

Overview **2-2**
Valid Pro-Watch Users for Application Login 2-2
Logging in to Advanced Badging **2-3**
Configuring the Advanced Badging Dashboard 2-5
Using the Menu Bar **2-8**
Console > Options 2-8
Badge 2-16
Navigate 2-18
Search 2-19
Tools 2-22
Using the Navigation Pane **2-30**
Using the Badging Screen 2-32
Adding a Badge **2-35**
Editing a Badge **2-36**
Searching for the Badge 2-36
Editing the Badge 2-39
Adding a Card **2-40**
Editing a Card **2-46**
Scheduling Clearance Codes **2-53**
Rules for Scheduled Clearance Codes 2-53
Assigning a Scheduled Clearance Code to a New Card 2-53
Assigning a Scheduled Clearance Code to an Existing Card 2-57
Unassigning Scheduled Clearance Code(s) 2-59
Copying Cards **2-60**
Downloading Cards **2-61**
Editing a Badge Holder's Card **2-62**
Deleting Cards **2-64**
Mobile Credentials (HID) **2-65**
Limitations 2-65
Introduction 2-65
Prerequisite: Create an HID Account 2-67
Steps to Follow 2-70
Assigning Assets **2-77**
Using E-Docs **2-78**
Enabling E-Docs 2-78
Performing Electronic Document Operations 2-80
Assigning Partitions **2-83**
Assigning Notes **2-84**
Previewing Badge Records **2-86**
Printing Badge and Card Records **2-87**
Displaying Print Preview 2-87
Printing Badges or Cards 2-87
Administration **2-88**
Companies 2-88
Company Types 2-90
Linked Badge Fields 2-90
Linked Null Fields 2-93
Application Settings 2-93
Compliance Reports 2-94

Opening Multiple Instances of Advanced Badging **2-95**

Chapter 3
Alarm Monitor 3-1

Overview **3-2**
VMS Client 3-2
Monitor Dispositions, Instructions, and Response Codes **3-3**
Dispositions 3-3
Instructions 3-7
Response Codes 3-9
Alarm Monitor Windows and Controls **3-11**
Window Panes 3-11
Toolbars 3-12
Using the Alarm Monitor **3-14**
Monitoring Alarms 3-14
Acting on Logical Devices 3-23
Using the Alarm Monitoring Tasks Tool Bar 3-26
Using the File Menu 3-26
Processing Events on a Map **3-30**
Using the Layers Map Function 3-31

Chapter 4
Reports 4-1

Overview **4-2**
To switch from one module to another 4-2
Screen Design **4-3**
Navigating Around the Application **4-5**
Report Types **4-6**
Functions **4-8**
Application Functions 4-8
Editing Reports 4-8
Deleting Reports 4-9
Copying Reports 4-9
Report Viewer Functions 4-12
Using the Application **4-18**
Generating Reports 4-18
Grouping Data **4-26**
Filtering Reports **4-28**
Using One Filter 4-28
Using Two Filters 4-31
Runtime Filter 4-32
In/Not In Filter 4-32
Defining a Query **4-34**
Defining a Query 4-34
Administrative Tasks **4-38**
Creating a New Connection 4-38
Setting Up a Shared Repository 4-38
Scheduling Reports 4-39
Deleting a Schedule 4-46

Running a Report on Demand **4-48**
Reviewing Schedule Run History **4-49**
Setting Display Parameters **4-50**
Switching the Report Modules **4-53**
To switch from classic reports to compliance reports 4-53

Chapter 5 Overview of Administrator Functions 5-1

Overview **5-2**
Pro-Watch Functions **5-4**
Badging 5-4
Hardware Configuration 5-4
Database Configuration 5-5
Monitor 5-5
Reports 5-5
Administration 5-6
Server Options **5-7**
Server Options Tab 5-8
Setting Event Log Thresholds 5-8
Setting Performance Options 5-10
Setting Timeout Option 5-10
Setting Logical Device Tags 5-10
Enhanced PIN Mode 5-11
Setting Logical Device Status Reporting 5-12
Setting APB Auto Load Balancing Option 5-12
Assigning Extended Instructions 5-13
Setting Card Options for PW-5000/6000/6101 Panels 5-14
Setting Hardware Change Notes 5-15
Hardware Notes Tab 5-17
Setting Mercury IP Client (Reverse IP) 5-18
Setting Privilege Management 5-21
Setting Device Status Filtering Options 5-27
Setting Additional Server Options 5-29
Setting Company Tabs 5-38
Setting Database Limits 5-39
Duress Signal via "Appended Digit" Option **5-40**
Setting the PIN Length 5-41
Appended Duress Digit Q & A 5-42
Test Your Knowledge 5-43
Answers to “Test Your Knowledge” Quiz 5-44
Setting the Log Size **5-45**
Pro-Watch Topologies **5-46**
Pro-Watch Remote Server Topology **5-47**
Editing the CommServerName Registry Setting 5-47
Designating the Primary Server 5-48
Designating the Remote Servers 5-48
Re-starting Pro-Watch on the Remote Servers 5-49
Pro-Watch Configuration Preview **5-50**
Tool Bar **5-51**

Chapter 6

Hardware Configuration (HW Config) 6-1

Overview **6-2**
Using the Hardware Manager Wizard **6-4**
Toggling Off the "Manage Your Server" Screen 6-4
Turning the User Wizard On and Off 6-4
Adding a Hardware Template 6-5
Adding a New Control Panel 6-6
Add Logical Device 6-8
Adding a System User 6-12
Configuring Device Types **6-14**
Adding or Editing a Device Type 6-16
Deleting a Device Type 6-20
Viewing the Dependencies of a Device Type 6-21
Copying Device Types 6-21
Viewing the Icons 6-21
Default Assignments for Readers 6-22
Configuring Hardware Classes **6-23**
Adding or Editing a Hardware Class 6-24
Deleting a Hardware Class 6-25
Viewing the Dependencies of a Hardware Class 6-25
Copying Hardware Classes 6-26
Viewing the Icons 6-26
Configuring Hardware Templates **6-27**
Adding or Editing a Hardware Template 6-28
Deleting a Hardware Template 6-43
Viewing the Dependencies of a Hardware Template 6-43
Configuring The Hardware System **6-45**
Procedures Common to All Panels 6-46
Add a Site 6-46
How to View and Edit Dependencies of a Site 6-48
How to Delete a Site 6-48
How to Add a Channel 6-49
How to View and Edit Dependencies of a Channel 6-51
How to Delete a Channel 6-51
How to Add a Panel 6-52
How to View and Edit Dependencies of a Panel 6-52
How to Delete a Panel 6-53
How to View and Edit Dependencies of a Logical Device 6-53
How to Delete a Logical Device 6-53
Editing Daylight Savings Time (DST) Zone 6-54
Status **6-55**
Channel Status 6-55
Panel Status 6-55
Panel Download **6-59**
Logical Device Icon **6-61**
Status Groups **6-62**
Guard Tours **6-63**
Adding a Guard Tour 6-63
Editing a Guard Tour 6-64

Chapter 7
HW Config - PW2000 7-1

Overview **7-2**
Adding a PW2000 Channel **7-3**
Viewing and Editing Dependencies of a PW2000 Channel **7-8**
Deleting a PW2000 Channel **7-9**
Adding a PW2000 Panel **7-10**
Configuring PW2000 Panel Tabs **7-12**
General Tab 7-12
Advanced Tab 7-14
Interlocks Tab 7-15
Output Groups Tab 7-16
Card Formats Tab 7-18
Time Zones Tab 7-19
Holidays Tab 7-20
Events Tab 7-22
Partitions Tab 7-22
Editing a PW2000 Panel **7-24**
Buffering or Un-buffering a PW2000 Panel 7-26
Viewing and Editing Dependencies of a PW2000 Panel **7-27**
Deleting a PW2000 Panel **7-28**
Adding a PW2000 Logical Device **7-29**
Editing a PW2000 Logical Device **7-31**
Define Logical Device Tab 7-32
Logical Device Details Tab 7-33
Default CCTV Tab 7-38
Transactions Tab 7-38
Partitions Tab 7-38
Viewing and Editing Dependencies of a PW2000 Logical Device **7-40**
Deleting a PW2000 Logical Device **7-41**

Chapter 8
HW Config - PW-5000/PW-6000/PW-6K1ICE Channel Type 8-1

Overview **8-3**
Adding a PW-5000/PW-6000/PW-6K1ICE Channel **8-4**
Encrypting a PW-5000/PW-6000/PW-6K1ICE Channel **8-10**
View and Edit Dependencies of PW-5000/PW-6000/PW-6K1ICE Channel **8-15**
Deleting a PW-5000/PW-6000/PW-6K1ICE Channel **8-15**
Adding a PW-6000/5000/3000 Panel **8-16**
PW-6000 Controller Panel Option 8-19
PW-5000 and PW-3000 Controller Panel Options 8-20
Configuring PW-6000/5000/3000 Panel Tabs 8-24
Editing a PW-6000/5000/3000 Panel **8-36**
Memory Warning for PW-6000 ..... **8-41**
"Why does this happen?" 8-41
Viewing and Editing Dependencies of a PW-6000/5000/3000 Panel

8-42

Deleting a PW-6000/5000/3000 Panel 8-42
PW-6000/5000/3000 Elevators 8-43
Overview - PW6K1ICE Panel 8-45
Background 8-45
Subpanel Limits 8-45
Adding a PW6K1ICE Panel 8-46
Adding PW6K1ICE with the User Wizard 8-46
Adding PW6K1ICE without the User Wizard 8-48
PW6K1ICE DS with RS-485 Downstream 8-50
Port Protocol 8-50
ACR Limits 8-50
Adding the PW6K1ICE DS Panel 8-51
Panel Properties 8-53
Configuring PW6K1ICE Panel Tabs 8-56
Panel Tab 8-56
Biometric Settings Tab 8-59
Time Zones Tab 8-60
Holidays Tab 8-61
Card Formats Tab 8-61
Procedures Tab 8-63
Triggers Tab 8-64
Resistance Values Tab 8-65
Events Tab 8-67
Partitions Tab 8-67
Configuring the PW6K1R1E Downstream I/O Boards 8-68
MR51e Subpanel Firmware Information 8-71
Viewing and Editing Dependencies of a PW6K1ICE Panel 8-71
Deleting a PW6K1ICE Panel 8-72
Adding a Mercury Panel 8-73
PART I: Unselecting the Honeywell Protocol 8-73
PART II: Creating the Third-Party Panel 8-74
PW-6000 Controller Panel Option 8-79
Viewing and Editing Dependencies of a Mercury Panel 8-80
Deleting a Mercury Panel 8-80
Mercury Text Output to LCD Terminal 8-81
Mercury Protocol 8-83
Overview of Mercury Protocol 8-83
PART I: Unselecting the Honeywell Protocol 8-83
PART II: Creating the Third-Party Panel 8-84
Mercury Intrusion 8-90
Overview of Mercury Intrusion 8-90
Prerequisites 8-90
New Tabs for Mercury Intrusion 8-91
Panel Tabs 8-92
Reader Tabs 8-94
General Steps 8-95
Software License for Mercury Intrusion 8-96
Mercury Intrusion Configuration Restrictions 8-97
Configuring the Mercury Keypad Settings 8-98
Configuring the PW-6000 Panel 8-100
Setting Intrusion Command Codes 8-103

Introduction to Intrusion Zones 8-105
Zone Types and Modes 8-105
Entry Delay Types 8-106
Creating Intrusion Zone (With Wizard) 8-107
Creating Intrusion Zone (Without Wizard) 8-109
Adding Intrusion Groups and Configuring Zones under Panel Properties 8-110
Introduction to Intrusion Groups 8-116
Creating Intrusion Group (With Wizard) 8-117
Intrusion Group Events 8-121
Creating MRDT Intrusion Terminal (With Wizard) 8-122
Creating MRDT Display Settings 8-126
Configuring Intrusion Terminal Command Maps 8-128
Wiring the MRDT Display Terminals 8-130
As a subpanel using the RS-485 port of a PW-6000 (or equivalent) IC 8-131
As a reader using the reader port of a PW-6000 2-Reader board 8-131
Connecting an external reader to the MRDT 8-132
Adding a Logical Device 8-133
Configuring a Logical Device 8-134
Define Logical Device Tab 8-135
Logical Device Details Tab 8-136
Viewing and Editing Dependencies of a Logical Device 8-149
Cypher Mode 8-150
Deleting a Logical Device 8-150

Chapter 9
HW Config - Cardkey 9-1

Overview 9-2
Adding a Cardkey Channel 9-3
Viewing and Editing Dependencies of a Cardkey Channel 9-10
Deleting a Cardkey Channel 9-11
Adding a Cardkey Panel 9-12
Configuring a Panel and Sub-Panels 9-13
Configuring the Panel 9-13
Configuring the Sub-Panels (STIs) 9-24
Editing the Panel's Communication Ports 9-33
Viewing and Editing Dependencies of a Cardkey Panel 9-34
Deleting a Cardkey Panel 9-35
Adding a Cardkey Logical Device 9-36
Editing a Cardkey Logical Device 9-40
Logical Device Details Tab 9-42
Readers 9-43
Input Points 9-46
Output Points 9-48
Default CCTV Tab 9-50
Transactions Tab 9-50
Partitions Tab 9-50
Viewing and Editing Dependencies of a Cardkey Logical Device 9-51
Deleting a Cardkey Logical Device 9-52
Cardkey Elevators 9-53

Chapter 10
HW Config - CHIP 10-1

Overview **10-2**
Adding a CHIP Channel **10-3**
Select a CHIP Channel Type 10-3
Define the CHIP Channel 10-3
Set CHIP Communications Parameters 10-4
Viewing and Editing Dependencies of a CHIP Channel **10-7**
Deleting a CHIP Channel **10-8**
Adding a CHIP Panel **10-9**
Configuring a CHIP Panel **10-10**
Adding a CHIP Panel 10-11
Editing a CHIP Panel **10-30**
Viewing and Editing Dependencies of a CHIP Panel **10-32**
Deleting a CHIP Panel **10-33**
Adding a CHIP Logical Device **10-34**
Editing a CHIP Logical Device **10-39**
Define Logical Device Tab 10-40
Logical Device Details Tab 10-41
Output Devices 10-54
Viewing and Editing Dependencies of a CHIP Logical Device **10-56**
Deleting a CHIP Logical Device **10-57**
Star II (CHIP) Elevators **10-58**
Known STAR II Issue 10-58

Chapter 11
HW Config - Matrix 11-1

Overview **11-2**
Adding a Matrix Channel **11-3**
Viewing and Editing Dependencies of a Matrix Channel **11-6**
Deleting a Matrix Channel **11-7**
Adding a Matrix Panel **11-8**
Panel Settings Tab 11-10
Advanced Options Tab 11-11
Advanced Options (cont.) Tab 11-13
Viewing and Editing Dependencies of a Matrix Panel **11-14**
Deleting a Matrix Panel **11-15**
Adding a Matrix Logical Device **11-16**
Configuring a Matrix Logical Device **11-20**
Define Logical Device Tab **11-21**
Logical Device Details Tab 11-22
Server Options Screen/Additional Server Options 11-27
Cardholder Screen/Panel-Specific Options 11-27
Viewing and Editing Dependencies of a Matrix Logical Device **11-29**
Deleting a Matrix Logical Device **11-30**

Chapter 12
HW Config - EP1502 12-1

Overview **12-2**
- Features Summary 12-2
- Benefits Summary 12-2

EP1502 Hardware **12-4**
EP1502 Panel Wiring and Setup **12-5**
- Configuring EP1502 Jumpers 12-6
- Configuring EP1502 DIP Switches 12-7
- Factory Default Communication Parameters: 12-8
- Bulk Erase Configuration Memory: 12-8

Input Power, Cabinet Tamper and UPS Fault Input Wiring **12-9**
Communication Wiring **12-10**
Reader Wiring **12-11**
Input Circuit Wiring **12-12**
Relay Circuit Wiring **12-13**
Memory and Real Time Clock Backup Battery **12-14**
Status LEDs **12-15**
Specifications **12-17**
Warranty **12-19**
Liability **12-20**

Chapter 13
HW Config - SEEP 13-1

Overview **13-2**
Adding a SEEP Channel **13-3**
- Select a Channel Type 13-3
- Set Communications Parameters 13-4

Viewing and Editing Dependencies of a SEEP Channel **13-6**
Deleting a SEEP Channel **13-7**
Adding a SEEP Panel **13-8**
Configuring a SEEP Panel **13-9**
- Panel Settings Tab 13-9
- More Panel Settings Tab 13-11
- Time Zones Tab 13-13
- Holidays Tab 13-14
- Reports Tab 13-15
- Transactions Tab 13-18
- Terminal Users Tab 13-18

Editing a SEEP Panel **13-20**
Viewing and Editing Dependencies of a SEEP Panel **13-23**
Deleting a SEEP Panel **13-24**
Adding a SEEP Logical Device **13-25**
Editing a SEEP Logical Device **13-30**
- Define Logical Device Tab 13-31
- Logical Device Details Tab 13-33
- Readers 13-34
- Input Points 13-39
- Output Points 13-40

Viewing and Editing Dependencies of a SEEP Logical Device 13-42
Deleting a SEEP Logical Device 13-43

Chapter 14
HW Config - SmartPlus Mobile 14-1

Overview 14-2
Adding a SmartPlus Mobile Channel 14-3
Viewing and Editing Dependencies of a SmartPlus Mobile Channel 14-6
Deleting a SmartPlus Mobile Channel 14-7
Adding a SmartPlus Panel 14-8
Viewing and Editing Dependencies of a SmartPlus Mobile Panel 14-10
Deleting a SmartPlus Mobile Panel 14-11
Adding a SmartPlus Mobile Logical Device 14-12
Editing a SmartPlus Mobile Logical Device 14-17
Define Logical Device Tab 14-18
Logical Device Details Tab 14-20
Readers 14-21
Input Points 14-23
Output Points 14-25
Default CCTV Tab 14-26
Viewing and Editing Dependencies of a SmartPlus Mobile Logical Device 14-28
Deleting a SmartPlus Mobile Logical Device 14-29

Chapter 15
HW Config - Vindicator V5 15-1

Overview 15-2
Adding a Vindicator V5 Channel 15-3
Viewing and Editing Dependencies of a Vindicator V5 Channel ... 15-6
Deleting a Vindicator V5 Channel 15-7
Adding a Vindicator V5 Panel 15-8
Viewing and Editing Dependencies of a Vindicator V5 Panel 15-12
Deleting a Vindicator V5 Panel 15-13
Adding a Vindicator V5 Logical Device 15-14
Editing a Vindicator V5 Logical Device 15-18
Define Logical Device Tab 15-19
Logical Device Details Tab 15-20
Readers 15-21
Input Points 15-23
Output Points 15-25
Default CCTV Tab 15-27
Transactions Tab 15-27
Partitions Tab 15-27
Viewing and Editing Dependencies of a Vindicator V5 Logical Device 15-28
Deleting a Vindicator V5 Logical Device 15-29

Chapter 16
HW Config - VISTA 16-1

Overview **16-2**
Update Intervals 16-2
Adding a VISTA Channel **16-3**
Viewing and Editing Dependencies of a VISTA Channel **16-6**
Deleting a VISTA Channel **16-7**
Viewing and Editing Dependencies of a VISTA Channel **16-8**
Adding a VISTA Panel **16-9**
Editing a VISTA Panel **16-15**
Viewing and Editing Dependencies of a VISTA Panel **16-16**
Deleting a VISTA Panel **16-17**

Chapter 17
HW Config - Generic Channels 17-1

Overview **17-2**
Selecting a Channel Type **17-3**
Setting Communications Parameters **17-4**
SQL Stored Procedures for Generic Channels **17-6**
Viewing and Editing Dependencies of a Generic Channel **17-8**
Deleting a Generic Channel **17-9**

Chapter 18
HW Config - Log Printers 18-1

Log Printers **18-2**

Chapter 19
HW Config - Wireless Readers 19-1

Overview **19-2**
Panel Initialization and System Download 19-2
Adding a Wireless Reader **19-3**
STEP 1: Create a PW-5000 Channel 19-3
STEP 2: Add the Wireless Reader Panel 19-3
Schlage AD-400 and AD-401 ..... **19-6**
Requirements 19-7
Step 1: Add the PW-6000 Panel 19-7
Step 2: Connect PW-6000 to PIM400-485 via RS-485 Port 19-7
Step 3: Configure PIM400-485 by using Schlage Hand Held Device (HHD) 19-8
Step 4: Connect the AD400/401 Door to the PIM400-485 19-9
Step 5a: Add the PIM400-485 Sub-Panel to PW-6000 19-10
Step 5b: Add the PIM400-485 Sub-Panel to PW-6000 via Wizard 19-13
SALTO and ASSA ABLOY **19-14**
SALTO System Configuration 19-14
ASSA ABLOY System Configuration 19-15
Notes on SALTO Locks **19-16**
Door Held Open Behavior 19-16

Request to Exit (REX) Behavior 19-16
Door Forced Open Behavior 19-16
External Door Contact / REX 19-16
No Host-Grants for SALTO Readers 19-16
Number of SALTO readers 19-17
Notes on ASSA ABLOY Locks 19-18
Unlock Operations Not Supported 19-18
Fixed-length PIN Codes 19-18
Switching the Reader to PIN Mode 19-18
No Host-Grants for ASSA ABLOY Readers 19-18
Mechanical Key May Generate “Forced Door” Message 19-20

Chapter 20
HW Config - Status & Panel Download 20-1

Overview 20-2
Channel Status 20-3
Panel Status 20-4
Panel Download 20-7

Chapter 21
HW Config - CCTV 21-1

Overview 21-2
Configuring CCTV 21-3
Configuring Analog CCTV 21-4
Adding CCTV Monitors 21-7
Deleting CCTV Monitors 21-8
Adding CCTV Camera Views 21-9
Calling Up Camera Views 21-10
Using CCTV Commands 21-11
CCTV Controls 21-14

Chapter 22
HW Config - DVR 22-1

Configuring Digital Video Recording (DVR) 22-2
Configuring HVMS in Pro-Watch 22-4
Using HVMS in Pro-Watch 22-13
Configuring DVR 22-15
Creating a Channel 22-15
Creating CCTV Camera Views 22-18
Calling Up a Camera View 22-19
Configuring VAST 22-24
Associating a Camera with an Alarm 22-26

Chapter 23
HW Config - Intercom 23-1

Overview 23-2
Adding an Intercom 23-3
Adding Intercom Stations 23-5

Chapter 24
HW Config - Hardware Actions 24-1

Hardware Actions 24-2

Chapter 25
HW Config - Edit Point 25-1

Overview 25-2
Event Information 25-3
Adding an Instruction Set 25-5
Adding a New Instruction 25-6
Adding a Disposition 25-7
Adding a New Disposition 25-7

Chapter 26
HW Config - MS-ICS 26-1

Overview 26-2
Typical Network Configuration 26-3
Board Properties 26-4
Configuration Limits 26-4
Related Mercury Documentation 26-4
Configuring an MS-ICS Network for Pro-Watch 26-5
Creating a Site 26-5
Creating a Channel 26-5
Creating a Panel 26-5
Creating a Logical Device 26-10

Chapter 27
Database Configuration (DBC) - Introduction 27-1

Overview 27-2
Viewing the Icons 27-4

Chapter 28
DBC - Alarm Page 28-1

Overview 28-2
Alarm Functions 28-3
Adding or Editing an Alarm Page 28-4
Alarm Page Information Tab 28-5
Alarm Page Event Types Tab 28-6
Alarm Page Columns Tab 28-7

Partitions Tab 28-7
Viewing Alarm Page Dependencies 28-9
Copying an Alarm Page 28-10
Deleting an Alarm Page 28-11

Chapter 29
DBC - Area 29-1

Overview 29-2
Area Functions 29-3
Adding or Editing an Area 29-4
Area Tab 29-6
Logical Device (Reader) Tab 29-11
Logical Device (Input) Tab 29-12
CHIP Reader Mode Tab 29-14
Area Occupants Tab 29-15
Partitions Tab 29-15
Deleting an Area 29-16
Locking or Unlocking an Area 29-17
Setting an Area's Zone Mode Properties 29-18
Anti-Pass-Back (APB) Update Limitations 29-19
An Example 29-19

Chapter 30
DBC - Badge Profiles 30-1

Overview 30-2
Badge-System Implementation Steps 30-3
Adding or Editing a Badge Profile 30-5
Badge Profile Info Tab 30-6
Search Configuration Tab 30-7
Partitions Tab 30-8
Deleting a Badge Profile 30-9
Viewing Dependencies of a Badge Profile 30-10
Copying a Badge Profile 30-11

Chapter 31
DBC - Badge Statuses 31-1

Overview 31-2
Badge Status Functions 31-3
Adding a Badge Status 31-4
Editing a Badge Status 31-5
Deleting a Badge Status 31-6

Chapter 32
DBC - Badge Types 32-1

Overview 32-2
Badge Type Functions 32-3
Adding Types 32-4
Editing Badge Types 32-5
Viewing Dependencies of a Badge Type 32-6
Copying Badge Types 32-7
Deleting Badge Types 32-8

Chapter 33
DBC - BLOB Types 33-1

Overview 33-2
BLOB Size Limit and Supported Formats 33-2
BLOB Type Functions 33-3
Adding or Editing BLOB Types 33-4
Viewing Dependencies of a BLOB Type 33-8
Partitions and BLOB Types 33-9
Deleting BLOB Types 33-10

Chapter 34
DBC - Brass Keys 34-1

Overview 34-2
Brass Keys Functions 34-3
Adding or Editing Brass Keys 34-4
Viewing Dependencies of a Brass Key 34-5
Partitions and Brass Keys 34-6
Deleting a Brass Key 34-7

Chapter 35
DBC - Card Formats 35-1

Overview 35-2
Card Format Functions 35-3
Adding or Editing a Card Format 35-4
Adding or Editing a Non PW2000 Card Format 35-5
Adding or Editing a PW2000 ABA Format 35-7
Adding or Editing a PW2000 Weigand/Tack One Format 35-8
Viewing Dependencies of a Card Format 35-11
Copying a Card Format 35-12
Partitions and Card Formats 35-13
Deleting a Card Format 35-14

Chapter 36
DBC - Classes 36-1

Overview **36-2**
Class Functions **36-3**
Adding or Editing a Class **36-5**
Class Tab 36-6
Programs Tab 36-6
Workstations Tab 36-7
Routing Groups Tab 36-8
Alarm Pages Tab 36-9
Badge Profiles Tab 36-10
Event Procedures Tab 36-10
Keystroke Accelerators Tab 36-10
Eventview Columns Tab 36-11
Event Toolbars Tab 36-11
Partitions Tab 36-12
Viewing Dependencies of a Class **36-13**
Copying a Class **36-14**
Deleting a Class **36-15**

Chapter 37
DBC - Clearance Codes 37-1

Overview **37-2**
Limitation 37-2
Clearance Codes Functions **37-3**
Adding or Editing Clearance Codes **37-4**
Clearance Code Tab 37-5
Logical Devices Tab 37-8
Elevator Outputs Tab 37-9
Output Groups Tab 37-9
Certifications Tab 37-9
Access Management Tab 37-10
Partitions Tab 37-11
Viewing Dependencies of a Clearance Code **37-12**
Copying a Clearance Code **37-13**
Clearance Codes and Code of Federal Regulations (21 CFR 11) 37-14
Adding a Clearance Code and 21 CFR 11- No Signature Asked 37-14
Editing a Clearance Code and 21 CFR 11- Signature Asked 37-14
Deleting a Clearance Code **37-16**

Chapter 38
DBC - Companies 38-1

Overview **38-2**
Companies Functions **38-3**
Adding or Editing Companies **38-4**
Information Tab 38-5
Clearance Codes Tab 38-5
Partitions Tab 38-6

Viewing Dependencies of a Company 38-7
Copying a Company 38-8
Deleting a Company 38-9

Chapter 39
DBC - Database Tables 39-1

Overview 39-2
Database Table Functions 39-3
Adding or Editing Database Tables 39-4
Table Information 39-4
Deleting a Database Table 39-6

Chapter 40
DBC - Default Events 40-1

Overview 40-2

Chapter 41
DBC - Deferred Access 41-1

Overview 41-2
Considerations and Limitations of Deferred Access 41-3
Starting and Ending a Deferred Access Project 41-4
Accessing the Deferred Access Functions 41-5
Adding or Editing a Deferred Access Project 41-6
Project Record Tab 41-7
Logical Devices Tab 41-8
Project Members Tab 41-8
Partitions Tab 41-9
Viewing Dependencies of a Deferred Access Project 41-10
Copying a Deferred Access Project 41-11
Deleting a Deferred Access Project 41-12

Chapter 42
DBC - Dial-Up Schedule 42-1

Overview 42-2
Dial-Up Schedule Functions 42-3
Adding or Editing Dial-up Schedules 42-4
Dial-up Schedule Tab 42-4
Partitions Tab 42-4
Viewing Dependencies of a Dial-up Schedule 42-6
Copying a Dial-up Schedule 42-7
Deleting a Dial-up Schedule 42-8

Chapter 43
DBC - Event Procedures 43-1

Overview 43-2
Event Procedure Functions 43-3
Adding or Editing Event Procedures 43-4
Event Procedures Tab 43-4
Partitions Tab 43-7
Viewing Dependencies of an Event Procedure 43-9
Copying an Event Procedure 43-10
Running an Event Procedure 43-11
Deleting an Event Procedure 43-12

Chapter 44
DBC - Event Triggers 44-1

Overview 44-2
Event Trigger Functions 44-3
Adding or Editing Event Triggers 44-4
Event Trigger Maintenance Tab 44-5
Event Trigger Procedures Tab 44-6
Partitions Tab 44-7
Copying an Event Trigger 44-8
Deleting an Event Trigger 44-9

Chapter 45
DBC - Event Types 45-1

Overview 45-2
Event Type Functions 45-3
Adding or Editing Event Types 45-4
Information Tab 45-5
Annunciation Tab 45-7
Partitions Tab 45-8
Viewing Dependencies of an Event Type 45-9
Copying an Event Type 45-10
Deleting an Event Type 45-11

Chapter 46
DBC - Galaxy User Management 46-1

Overview 46-2
Configuration Steps 46-3

Chapter 47
DBC - Groups 47-1

Overview 47-2
Groups Functions 47-3
Adding or Editing Groups 47-4
Group Maintenance Tab 47-4
Partitions Tab 47-5

Viewing Dependencies of a Group 47-6
Copying a Group 47-7
Deleting a Group 47-8

Chapter 48
DBC - Guard Tours 48-1

Overview 48-2
Guard Tour Functions 48-3
Adding or Editing Guard Tours 48-4
Guard TabTour 48-5
Partitions Tab 48-6
Viewing Dependencies of a Guard Tour 48-7
Copying a Guard Tour 48-8
Deleting a Guard Tour 48-9

Chapter 49
DBC - Holidays 49-1

Overview 49-2
A Note on Holiday Icons 49-2
Holiday Functions 49-3
Adding or Editing Holidays 49-4
Information Tab 49-4
Partitions Tab 49-5
Viewing Dependencies of a Holiday 49-6
Copying a Holiday 49-7
Deleting a Holiday 49-8

Chapter 50
DBC - Keyboard Accelerator 50-1

Overview 50-2
Keyboard Accelerator Functions 50-3
Adding or Editing Keyboard Accelerators 50-4
Keyboard Accelerator Tab 50-4
Partitions Tab 50-5
Viewing Dependencies of a Keyboard Accelerator 50-7
Copying a Keyboard Accelerator 50-8
Deleting a Keyboard Accelerator 50-9

Chapter 51
DBC - Maps 51-1

Overview 51-2
Maps Functions 51-3
Adding or Editing Maps 51-4
Map Information Tab 51-4
Partitions Tab 51-5

Viewing Dependencies of a Map 51-6
Copying a Map 51-7
Deleting a Map 51-8

Chapter 52
DBC - Modem Pools 52-1

Overview 52-2
Modem Pools Functions 52-3
Adding or Editing Modem Pools 52-4
Modem Pool Information Tab 52-4
Partitions Tab 52-5
Copying a Modem Pool 52-6
Viewing Dependencies of a Modem Pool 52-7
Deleting a Modem Pool 52-8

Chapter 53
DBC - Partitions 53-1

Overview 53-2
Partitions Functions 53-3
Adding or Editing Partitions 53-4
Partition Information Tab 53-4
Partition Map Tab 53-4
Viewing Dependencies of a Partition 53-5
Copying a Partition 53-6
Deleting a Partition 53-7

Chapter 54
DBC - Pathways 54-1

Overview 54-2
Pathway Functions 54-3
Adding or Editing Pathways 54-4
Pathway Info Tab 54-5
Partitions Tab 54-5
Viewing Dependencies of a Pathway 54-7
Deleting a Pathway 54-8

Chapter 55
DBC - Routing Groups 55-1

Overview 55-2
Routing Group Functions 55-3
Adding or Modifying a Routing Group 55-5
Configuring Channels 55-5
Configuring Event Types 55-5
Configuring Rollover Event Types 55-5
A Special Routing Group: “All System Events” 55-6
Configuring Workstations 55-6
Assigning a Routing Group to a User 55-7
Assigning a Routing Group to a Class 55-8

Applying a Routing Group Filter 55-8
Partitions 55-11
Viewing Dependencies of a Routing Group 55-12
Copying a Routing Group 55-13
Deleting a Routing Group 55-14

Chapter 56
DBC - Status Groups 56-1

Overview 56-2
Status Group Functions 56-3
Adding a User-Defined Status Group 56-4
Editing a User-Defined Status Group 56-5
Status Group Maintenance Tab 56-5
Partitions Tab 56-5
Copying a Status Group 56-7
Deleting a User-Defined Status Group 56-8
System All Installed Status Groups 56-9
System All Installed Channels 56-9
System All Installed Panels 56-10

Chapter 57
DBC - Time Zones 57-1

Overview 57-2
Time Zone Functions 57-3
Adding or Editing a Time Zone 57-4
Time Zone Maintenance Tab 57-5
Partitions Tab 57-6
Viewing Dependencies of a Time Zone 57-7
Copying a Time Zone 57-8
Deleting a Time Zone 57-9

Chapter 58
DBC - Users 58-1

Overview 58-2
User Functions 58-3
Adding a User 58-5
Editing a User 58-6
User Information Tab 58-7
Device Status Filtering Tab 58-12
Programs Tab 58-13
Workstations Tab 58-17
Routing Groups Tab 58-17
Eventview Columns Tab 58-18
Keystroke Accelerators Tab 58-18
Event Toolbars Tab 58-19
Partitions Tab 58-21
Alarm Pages Tab 58-21
Badge Profiles Tab 58-22
Event Procedures Tab 58-23

Copying a User 58-25
Types of User Icons 58-26
Deleting a User 58-27

Chapter 59
DBC - Workstations 59-1

Overview 59-2
Workstation Functions 59-3
Adding Workstations 59-4
Editing a Workstation 59-5
Information Tab 59-5
CCTV Monitors Tab 59-6
Intercoms Tab 59-6
Logical Devices Tab 59-7
Communications Server Tab 59-8
Partitions Tab 59-8
Viewing Dependencies of a Workstation 59-10
Types of Workstation icons 59-11
Code of Federal Regulations (21 CFR 11) Functionality 59-12
Deleting a Workstation 59-15

Chapter 60
Badge Building 60-1

Overview 60-2
Adding a Badge Profile 60-5
Adding Badge Profile Pages 60-7
Modifying Control Attributes 60-8
Adding a Badge Field to a Profile or Editing a Badge Field 60-10
Deleting a Badge Field from a Profile 60-11
Editing a Badge Profile 60-12
Using Badge Builder Layout Options 60-13
Aligning Badge Fields 60-13
Spacing Badge Fields 60-13
Sizing Badge Fields 60-13
Centering a Badge Field 60-14
Using Badge Builder Status Bar 60-14
Assigning a Badge Profile to a Class or a User 60-15
Testing a Badge Builder Layout 60-16
Badge Utilities 60-17

Chapter 61
Map Building 61-1

Overview 61-2
To Launch the Map Builder 61-2
Creating Maps 61-3
Map Builder Tool Bar 61-4
Map Building Functions 61-6
Adding a Map 61-6
Editing a Map 61-7

Deleting a Map 61-8
Displaying the Selected Map 61-8
Displaying the Layers of the Map 61-8
Displaying the Blocks in the Map 61-8
Adding, Editing, or Deleting Resources 61-9
Adding, Editing or Deleting a Logical Device 61-10
Adding, Editing or Deleting Groups 61-12
Adding, Editing or Deleting Map Files 61-13
Adding, Editing or Deleting a CCTV Camera View 61-14
Adding, Editing or Deleting a Camera 61-14
Adding, Editing or Deleting a Monitor 61-14
Adding, Editing or Deleting an Intercom 61-15
Editing Resource Properties 61-16
An Example 61-17
Locating a Resource 61-19
Cleaning Up a Resource 61-20
Show Resource Text 61-21
Linking Maps to Alarms 61-22
Add a Map with Resource(s) 61-22
Add an Alarm Map Page 61-22
Add Alarm Event Types 61-23
Add User Class or Individual User(s) 61-25
Display the Alarm Monitor 61-26
Linking Multiple Maps 61-29

Chapter 62
Biometric Reader Configuration 62-1

Overview 62-2
Setting Up the Hardware to Run with Pro-Watch 62-4
Wiring the PW-3000 RSI Board to the PW-5000 IC 62-4
Wiring the Readers 62-4
Setting the DIP Switches 62-6
Setting the Reader Menus 62-8
Configuring Pro-Watch to Support the Reader 62-10
Converting a PW-3000 Panel to an RSI Board 62-10
Configuring the Biometric Hand Geometry Reader 62-11
Converting an RSI Board Back to a PW-3000 Panel 62-20

Chapter 63
Data Management 63-1

Overview 63-2
Database Manager 63-3
Backup Database 63-3
Restore Database 63-8
Backup Device Maintenance 63-15
Scheduled Maintenance 63-17
Moving the Database to Another Drive 63-20

Chapter 64
Data Transfer Utility (DTU) 64-1

Overview **64-2**
Installing Real Time DTU **64-3**
Configuring Real Time DTU 64-4
Log File **64-5**
Data Transfer Interfaces **64-6**
Data Transfer Steps **64-7**
Importing PINs and Duress Digit 64-7
Adding a DTU Import or Export Profile **64-8**
Editing a DTU Profile **64-10**
Why Import Pro-Watch Data? 64-10
Editing a Delimited Database Import Profile 64-11
Editing a Fixed-Length Data Import Profile 64-21
Editing an SQL Database Import Profile 64-27
Editing an ODBC Database Import Profile 64-34
ODBC Import Mapping Rules **64-41**
Editing an LDAP Database Import Profile 64-42
Why Export Pro-Watch Data? 64-47
Editing a Delimited Data Export Profile 64-48
Logical Device Data check Boxes 64-54
Editing an ODBC Database Export Profile 64-57
Audit Log In 64-62
ODBC Export Mapping Rules **64-64**
Editing an Image Export Profile 64-65
Transferring the Data **64-68**
LDAP/Active Directory Integration **64-68**
Creating DTU LDAP Import Profile 64-68
Editing Active Directory User Attributes 64-69
DTU Import Profile General 64-70
LDAP Filtering **64-74**
Active Directory Filtering 64-74
LDAP Options **64-76**
Active Directory Import Options 64-76
Stored Procedure to Execute 64-77
DTU Logging and Preview **64-79**
DTU Logging 64-79
Sample Log Files 64-80
DTU Preview 64-81

Chapter 65
Archiving 65-1

Overview **65-2**
Discontinued Support 65-2
Format of the Archives 65-2
Event History **65-3**
Archiving and Purging Event History **65-4**
Adding or Editing an Archive **65-5**
Beware of “11:59:00 p.m.” and “11:59:59 p.m.” End Times 65-7

Using the Pro-Watch Query Analyzer 65-9
Deleting an Archive 65-10

Appendix
Secure Mode Verification A-1

Overview A-1
Considerations and Limitations A-2
Implementation A-3
How Secure Mode Verification Works A-4
Badge-Holder Photo Display A-5
Editing MaxTranLogSearch Registry Key A-5

Appendix
Assignable Programs B-1

Programs Assignable to Classes and Users B-1
Commands Assignable to Event Procedures B-24

Appendix
Dial-Up Configuration C-1

Overview C-1
PW-5000/3000 Dial-up Configuration C-2
PW-5000/3000 Dial-In C-2
PW-5000/3000 Dial-Out C-8
PW2000 Dial-Up Configuration C-11
PW2000 Dial-In C-11
PW2000 Dial-Out C-15
CHIP (Star II) Dial-up Configuration C-17
CHIP (Star II) Dial-In C-17
CHIP (Star II) Dial-Out C-20
SEEP Dial-up Configuration C-23
SEEP Dial-In C-23
SEEP Dial-Out C-25
Cardkey Dial-up Configuration C-28
Cardkey Dial-In C-28
Cardkey Dial-Out C-28

Appendix
Remote Terminal Services D-1

Overview D-2
Setting Up Terminal Services D-2
Installing Terminal Services D-2
Connecting to Terminal Services D-2
Creating a Share on the Server D-2
Installing the Terminal Services on the Client D-3

Using the Terminal Services Client D-3
Before Badging from the Terminal Client D-5

Appendix
Magicard Prima Printer Installation E-1

Overview E-1
Installing Magicard Prima Printer E-1
Printer Configuration E-1
Printing and Encoding Within Pro-Watch E-5

Appendix
Moving Panels F-1

Overview F-2
Moving the Panel F-3

Appendix
Badging G-1

Overview G-2
Badges G-4
Adding and Editing a Badge G-4
Concurrency Check G-35
Cards G-37
Adding or Editing a Card G-37
Exiting out of Card View Screen G-66
Downloading a Card G-66
Copying and Pasting a Card G-66
Deleting a Card G-69
Voiding a Card G-69
Badge Designer G-69
Badge Format Properties G-71
Badge Designer Tool Bar G-80
Exiting the Badge Designer G-103

Appendix
Reports H-1

Overview H-2
To switch from one module to another H-2
Limitation H-2
Creating Reports H-2
Vista Commercial Panels H-6
Using Reports H-7
Printing a Report H-7
Exporting a Report H-8
Saving Report Configurations to My Reports Folder H-12

Scheduling a Report H-13
Access Reports H-19
Badge Holder Reports H-21
Company Reports H-23
Configuration Reports H-23
Logging Reports H-27
User Reports H-31
Report Designer H-31
Design Report Tab H-32
Preview Report Tab H-37
Save Report Tab H-37
Open Existing Report Tab H-37

Appendix

Morpho Biometric Integration Guide I-1

Overview I-2
Pro-Watch/Morpho Process Diagram I-3
Pro-Watch/Morpho Biometrics Setup I-3
General Notes I-7
Pro-Watch Advanced Badging I-7
Enabling Morpho Biometrics I-7
Morpho Template Configuration I-10
Morpho Fingerprint Configuration I-12
MSO300 Biometric Enrollment I-15
Morpho Reader Network Configuration I-19
Pro-Watch/Morpho Template Download Windows Service I-20
Pro-Watch/Morpho Windows Service Configuration I-21
Pro-Watch/Morpho Windows Service Installation I-22
DESFire Smart Card Key Management I-22
Morpho Reader Smart Card Key Management I-24
Pro-Watch Panel Configuration I-26
Version Information I-28
Required Licensing I-28
Included Morpho Documentation & Software I-28
Add Biometric Field to Pro-Watch Advanced Badging I-29
Step 1: Add two Pro-Watch Blob Types I-29
Step 2: Add two Pro-Watch Blob Fields I-30
Step 3: Add New Badge Fields to Badging Forms I-31
Morpho Indoor 500 Series Reader I-33
Morpho Outdoor 500 Series Reader I-34
MSO300 Finger Enroller I-35
MorphoWave Reader I-35
Introduction I-35
Requirements I-36
Setup for Enrollment I-37
Morpho Biometrics Setup in Advanced Badging I-38
MorphoWave Tower Connection/Setup I-42
Quick Start for SSL I-43

Appendix

Mercury M5 Bridge J-1

Overview J-1
Equivalences J-2
Installation - General J-2
Installation Steps (Without Wizard) J-5
STEP1: Create a Site J-5
STEP 2: Create a Channel J-5
STEP 3: Create a Panel J-6
STEP 4: Select the Panel Type J-6
STEP 5: Allocate subpanels J-8
Installation Steps (With Wizard) J-10
STEP1: Create a Site J-10
STEP 2: Create a Channel J-10
STEP 3: Define the panel J-11
STEP 4: Adding subpanels J-11
Adding Subpanels through Panel Properties J-14
Mercury M5 Port Assignments J-17
Default Assignments for REX and DPOS J-18
M5-MUX8 ..... J-18
Installing the M5-MUX8 ..... J-19
Programming in Pro-Watch J-19
M5-2K J-20
Virtual Inputs and Outputs J-20
Reserved Inputs and Outputs J-20
Restrictions J-21
Test Your Knowledge J-21
ANSWERS to “Test Your Knowledge” Quiz J-21

Appendix

Two-Person Rule K-1

Overview K-1
Mercury Panel Area Support K-2
Activating the Two-Person Rule K-2
The Minimum Option K-3
FAQ K-4
Test Your Understanding K-5
Answers to “Test Your Knowledge” Quiz K-6

Appendix

PW5K Conversion Utility L-1

Overview L-1
Adding “PW5K Conversion Utility” Registry Key L-2
Granting the Functionality L-3

Appendix

Partition Manager M-1

Overview **M-1**
Running the Partition Manager **M-2**
Partition Management Layout **M-3**
Assigning Partitions **M-4**
Already Assigned Partitions M-7
Unassigning Partitions and Objects **M-9**
Unassigning Partitions Directly from the Object M-9
Unassigning Objects from the Partition M-9

Appendix

Registry Management N-1

Overview **N-1**
Editing the Registry Manager **N-2**

Appendix

Galaxy Dimension Integration Guide O-1

Overview **O-2**
Audience O-2
Installation Pre-requisites O-2
Integration Overview O-2
Required Galaxy Configuration parameters **O-3**
Configuring Pro-Watch **O-4**
Creating a Galaxy Channel. O-5
Creating the Galaxy Dimension panel **O-7**
Uploading the Galaxy Configuration Into Pro-Watch **O-8**
Create Event Procedures **O-11**
Enabling Galaxy Components **O-12**
Badgeholder Operation Permissions **O-13**
Managing Galaxy Users **O-16**
Creation of Galaxy users O-17
The Arm/Disarm Mechanism **O-18**
Arming Zone(s) O-18
Disarming Zone(s) O-18
New Trigger Options **O-20**
New Pro-Watch Registry Keys **O-21**
Process Flowchart **O-22**
Pro-Watch Icons **O-23**
Backup and Restoring a Galaxy Database Using RSS **O-24**
Backup of the Galaxy Database O-25
Restoring a Galaxy Database Backup O-26
Functional Testing **O-27**
Test Arm / Disarm by Card O-27

Appendix

Extended Card Number Support P-1

Overview **P-2**
Extended Card number support (up to 128 bits) P-2
Prerequisites **P-2**
Setup **P-2**
Configuring Pro-Watch P-2
Configure Advanced Badging P-4
Adding Card in Pro-Watch P-6

Appendix

IRIS ID Integration Q-1

Overview **Q-2**
General System Architecture **Q-2**
General Operation **Q-2**
Iris ID EAC Components **Q-2**
EAC Components Required for Pro-Watch Integration **Q-4**
Installation Prerequisites **Q-4**
Installation Notes **Q-5**
Creating the IrisServer Database **Q-6**
Configuring the IrisServer **Q-10**
Configuring the IrisManager **Q-13**
Starting the IrisManager **Q-14**
Creating the Remote Unit Connection **Q-15**
Creating the IrisEnroll Connection **Q-17**
Creating the Iris Manager Connection **Q-18**
Creating the Iris Monitor Connection **Q-19**
Using Iris Monitor **Q-19**
Using Iris Enroll **Q-20**
Connecting to the iCAM Web Configuration **Q-20**
Configuring the IP Address of the iCAM **Q-21**
Changing the Operational Mode of the iCAM **Q-23**
Security and Ports **Q-24**
Pro-Watch Configuration **Q-26**
Iris ID Badge Field Q-28

Appendix

Software Keys Licensing R-1

Overview **R-2**
Quick Start **R-3**
Two Options to Install a License Certificate R-3
How to Install a Regular License R-4
How to Activate a Demo License R-8
How to View License Information **R-10**
How to Supersede a License **R-12**
STEP 1: The User Contacts Pro-Watch Inside Sales Dept. R-12
STEP 2a: The User Generates the *HID file R-12

STEP 2b: The User Contacts SK Automated Server R-13
STEP 3: SK Automated Server Mails the User R-13
STEP 4: The User Installs the License Certificate R-14
How to Transfer the License to Another Machine R-15
STEP 1: The User Contacts Software Keys Automated Server and/or the Voucher Manager R-15
STEP 2: SK Automated Server Emails the User R-16
STEP 3: The User Installs the License Certificate R-16
How to Terminate a License R-17
Cut-over/Migration Licenses R-18
Definition R-18
Examples R-18
Why needed? R-18
How Does It Work? R-18

Appendix

TBS and Pro-Watch Integration S-1

Overview S-2
Typical Network Configuration S-2
Prerequisites S-3
Limitations of Pro-Watch-TBS Integration S-4
Badge/Card download S-4
Unique PIN S-4
Authentication and Authorization S-5
Manual Configuring on TBS Side S-6
WebEdition S-6
NETSDK100 ..... S-9
TBS EnrollClient S-10
Pro-Watch configuration S-10
TBS Configuration of Biometric Settings S-12
Configuring the Badge Field for TBS Enrollment S-14
Configuring TBS Terminal and Validating the Logical Device S-16
Enrolling the Badgeholder Fingerprint S-20

INDEX 1

LIST OF FIGURES

Pro-Watch Main Screen 1-9
Pro-Watch Licensing Information Screen 1-33
Pro-Watch Advanced Badging Main Screen 2-3
Deferred Access Projects folder in Classical Badging Module 2-4
Panel Specific Options in Classic Badging Module 2-5
Panel Specific Options in Advanced Badging Module 2-6
Pro-Watch Advanced Badge Manager Badging Screen 2-28
Single User, Multiple Instances of Advanced Badging 2-89
Multiple Users, Multiple Instances of Advanced Badging 2-89
Alarm Event Options for Mercury Panel 3-15
Alarm Event Options for Mercury Reader 3-16
Opening Screen 4-3
Typical Abbreviated Screen Display 4-4
Hardware Configuration Task Flow 6-3
PW-6000 Memory Warning Message 8-41
HID Wiegand Reader with default display. 8-81
HID OSDP Reader with 2 line text display. 8-82
MRDT, Mercury Display Terminal with Keypad 8-90
Map Clearance Codes Tab 8-92
Intrusion Groups Tab 8-93
Intrusion Command Maps Tab 8-94
Intrusion Settings Tab 8-95
Software License Feature for Mercury Intrusion Enabled 8-97
Edit Mercury Keypad Settings 8-98
Intrusion Support Selection Options 8-101
“Intrusion Enabled" Check-Box in Panel Properties Screen 8-102
“Intrusion Groups" Tab 8-102
Enable Intrusion Support and Intrusion Protocol Buttons 8-103
Command Code Prefixes 8-104
Zone Hardware Template 8-105
Zone Hardware Class 8-105
Intrusion Zone Logical Device Creation 8-107
Intrusion Zone Hardware Address Selection 8-108
Intrusion Zone Logical Devices 8-108
Intrusion Zone Display Name 8-109
Zone Events in Event Viewer 8-109
Selecting Hardware Template 8-110
Logical Device Details 8-110

Intrusion Groups Tab 8-111
Create Intrusion Group 8-112
Add Intrusion Zone 8-112
Assign Logical Device 8-112
Intrusion Zone Fields 8-113
Intrusion Group Fields 8-114
Group Hardware Template 8-116
Group Hardware Class 8-117
Intrusion Group Logical Device Creation 8-118
Intrusion Group Selection 8-119
Intrusion Group Logical Device Listed 8-120
Intrusion Group Actions 8-120
Intrusion Zone and Group Events 8-121
MRDT Intrusion Terminal Creation 8-122
Intrusion Terminal Selection 8-123
Hardware Template for MRDT Connected to a Reader Port 8-123
Intrusion Terminal Reader Settings 8-123
Intrusion Terminal Intrusion Settings 8-124
Database Configuration > Mercury Intrusion Settings 8-126
Mercury Intrusion Settings 8-127
Map Clearance Codes (Panel) 8-128
Intrusion Command Maps 8-128
MRDT J3 Terminal Block Pins 1 through 4 8-130
MRDT J3 Terminal Block Pins 9 through 14 8-131
PIM400-485 to ACP Wiring Diagram 19-7
Schlage Hand Held Device (HHD) 19-8
SUS PIM Properties Screen 19-9
SALTO Wireless Reader System Configuration 19-14
ASSA ABLOY Wireless Reader System Configuration 19-15
MS-ICS Panel Components 26-2
Typical MS-ICS Network Configuration 26-3
Database Configuration Task Flow 27-2
Areas connected to a Pro-Watch Server 29-19
Card transacted at Panel 1 of Site 1 (S1P1) 29-20
Badge Profile Components 60-2
Biometric Hand Reader, Standalone Configuration 62-2
Biometric Hand Reader, Enrollment Configuration 62-3
Wiring the Biometric Hand Reader, Standalone Configuration 62-5
Biometric Hand Reader, Enrollment Configuration 62-6
Secure Mode Time Zone v.s. Verification Window Interaction A-2
A badge photo A-5
PW-5000/3000 Connections C-2
Selecting Badge Manager Wizard G-2
Badge Designer Screen G-62
Report Designer Screen H-27
Pro-Watch/Morpho Process Diagram I-3
Morpho Indoor 500 Series Reader I-27
Morpho Outdoor 500 Series Reader I-28

MSO300 Enroller I-29
Typical M5-IC Installation J-3
Typical M5-COM Installation J-4
Server Options in Pro-Watch P-2
Card Formats in Database Configuration P-3
Panel Properties in Pro-Watch P-3
Mercury SCPLOG P-4
Pro-Watch Options in Advanced Badging P-4
Unknown Badge Event in Pro-Watch Event Viewer P-5
Last Read Feature Drop-Down P-5
Add New Card Screen P-6
Card Showing the Extended Card Number P-6
Card Events with Extended Card Number in Event Viewer P-7

LIST OF TABLES

Pro-Watch Advanced Badge Manager Toolbar Icons 2-29
Contact List Required Fields 3-19
Possible Duress Outcomes with 5-digit PIN and "9" for Duress Digit .. 5-42
Encryption Icon Color Coding 8-12
Selected Properties of Boards in a MS-ICS Network 26-4
ACS Address and DIP Switch #1 Position 26-7
RSI Board-to-PW-5000 IC Wiring 62-4
Standalone Reader Wiring 62-5
Enrollment Reader Wiring 62-6
Programs Assignable to Classes and Users B-1
Commands Assignable to Event Procedures B-21
Server (Host) Modem DIP Switch Settings C-5
PW-5000 Controller (Remote) Modem DIP Switch Settings C-6
DIGID XID440 Printer Preferences E-2
Registry Manager Fields, Functions and Sample Values N-2
Pro-Watch Icons O-22
Pro-Watch Icons - Maps O-23

Honeywell

Overview of User Functions

1

In this chapter ...

Overview
Pro-Watch Login
Pro-Watch Functions
Tool Bar
Verification Window
Color Coding
Managing the Server Switchboard
Turning the Wizards Off
Other Quick Access Links
Pro-Watch System Configuration
Microsoft Azure Cloud

1.1 Overview

The Pro-Watch platform is a complete access control system of hardware and software for small, mid-size, and global-enterprise sites. You can configure sites that range from five users and 64 doors to an unlimited number of users and doors.

The Pro-Watch system supports Honeywell and third-party access control hardware and software, including panels, readers, intercom units, and CCTV equipment.

There are two interfaces available for this product:

- A PC-based interface
- A Web-based interface

These interfaces support both a server component and a client component. This guide describes how to operate the PC-based system. For information on the Web-Based product, see the *Pro-Watch Web Interface User's Guide*.

Note:

- Microsoft .NET Framework 4 Client Profile and Extended is now REQUIRED for Pro-Watch 4.1 Software Suite installations.
- Pro-Watch Software Suite 4.0/4.1 can be installed on VMWare ESXi.

Part I of this guide (Chapters 1-4) and Appendix A are intended for the user of an installed and configured Pro-Watch system. It explains the following functions:

- Designing and implementing badging. See "".
- Alarm monitoring and responding to events. See "".
- Creating access control reports. See "".
- CCTV controls, which uses the Microsoft SQL-based MSDE data engine. See Appendix A, Secure Mode Verification.

Part II of this guide (Chapters 5-12 and Appendices B, C, D, E, F, G, H, and I) is intended for Pro-Watch system administrators. It explains how to configure the Pro-Watch hardware and database, create badging profiles, and perform other administrative tasks. See "Part II ~ Administrator Functions", for more information.

1.2 Pro-Watch Login

1.2.1 Changing the Pro-Watch Authentication Type and Login Mode

To enable the Pro-Watch application login feature, you must first:

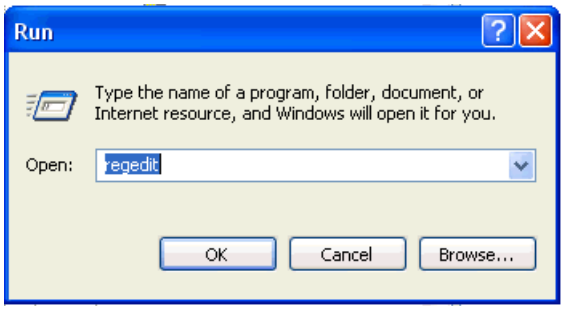
- either set the database to use “SQL Server and Windows” authentication, or change the MSSQL login mode in the registry from 1 to 2, then restart the SQL service.
- change the Pro-Watch authentication type in the registry from 0 to 1, then restart the Pro-Watch service.

1.2.1.1 Changing the Authentication Type

Note: The Pro-Watch authentication type should only be changed once after Pro-Watch is installed; it should not be changed again.

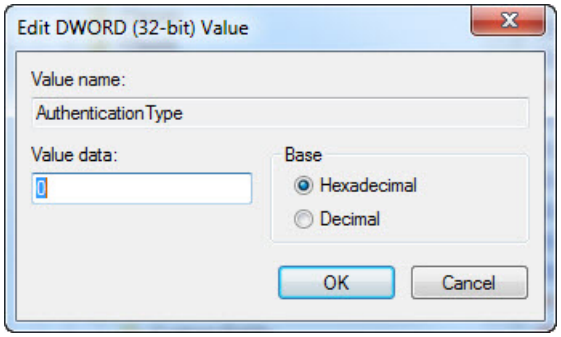
Follow these steps to switch from Windows to Pro-Watch authentication mode or vice-versa:

1. From the Windows desktop, select **Start > Run**.
2. Enter **regedit** in the Open field of the Run dialog box.



3. Click **OK** to launch the **Registry Editor** screen.
4. Navigate to [HKEY_LOCAL_MACHINE\SOFTWARE\Honeywell\ProWatch\Options].

5. Click **AuthenticationType** to display the authentication type editing dialog box:



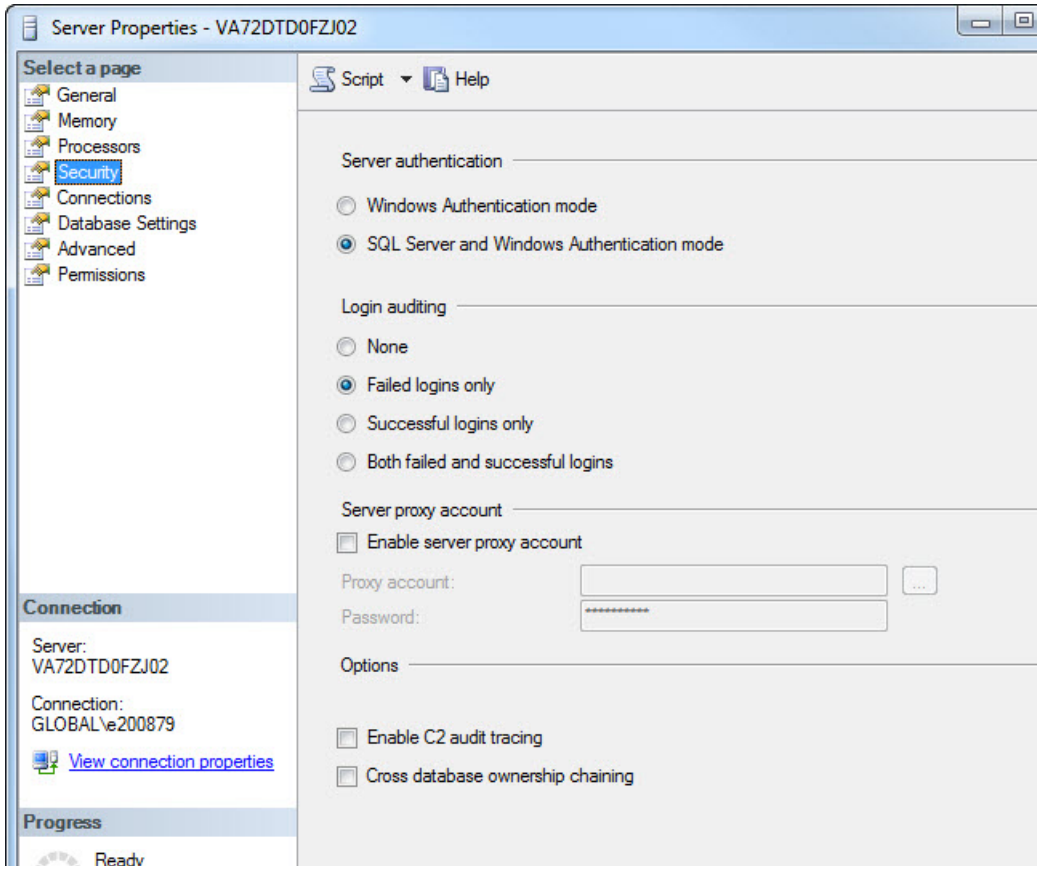
6. Change the **Value Data** field
   a. from 0 to 1 to allow application (i.e., Pro-Watch) authentication.
   b. from 1 to 0 to allow Windows authentication.
7. Click **OK**.
8. Close the **Registry Editor** screen.
9. Reboot the Pro-Watch server.

Caution: Because the authentication type should be changed only once, you will not be able to delete any of the existing users from the database after the change. Any attempt to do so may result in an error message and/or unpredictable behavior. Ensure that all unwanted users are removed from the system prior to making this change.

1.2.1.2 Changing the SQL Login Mode

Follow these steps:

1. Start **SQL Server 2012 Management Studio** or **SQL Server 2008 Management Studio**.
2. Right-click the server name and from the pop-up menu select **Properties** to display the **Server Properties** screen.
3. Select the **Security** option to display the security options:



4. Select "**SQL Server and Windows Authentication Mode**" option button.
5. Click the **OK** command button.
6. Restart the SQL Server.

1.2.2 Logging In to the Pro-Watch Server

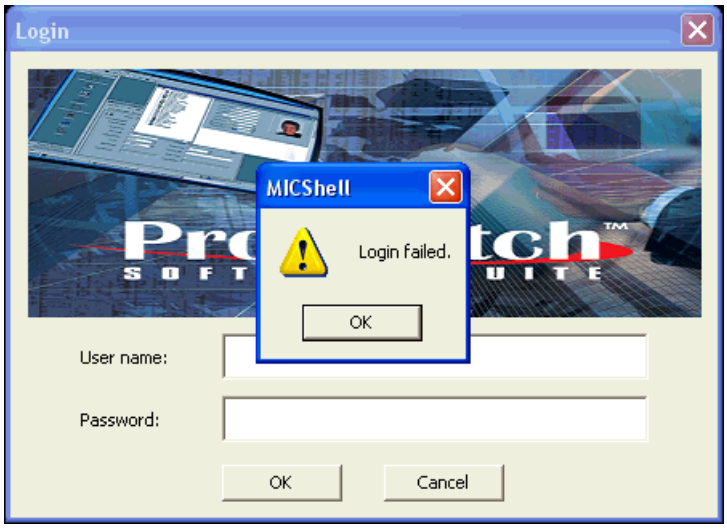
When you start Pro-Watch Server, the login screen appears:



1. If this is the first login, enter the default name **PWAdmin** in the User Name field. This field is not case-sensitive. Note that you cannot delete the PWAdmin user name. After you log in the first time, it is recommended that you create a new administrator user name.
2. Enter **ProWatch123** as the default password in the Password field. This field is case-sensitive. After logging in the first time, you can create a new password. Note that this field requires at least seven characters.

You only need to log in to Pro-Watch server once. As long as one Pro-Watch client is running thereafter, you can start another Pro-Watch client without being prompted for another login.

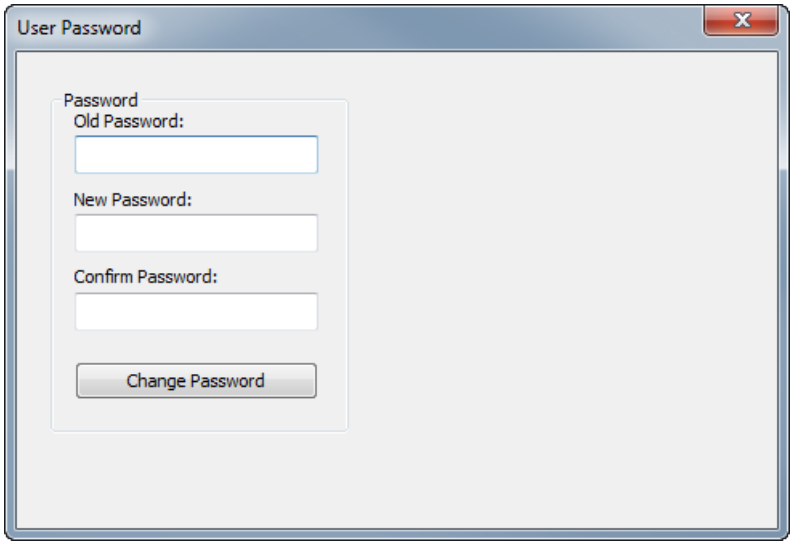
Note: You have three opportunities to enter the correct user name and password. When a login attempt fails, the following pop-up message appears:



Note: Pro-Watch stops running after a third consecutive login failure. If this should occur, you will need to wait 5 to 10 seconds before re-starting Pro-Watch.

1.2.3 Changing Passwords

Users can change their existing passwords any time they like by selecting **File > Change Password** from the main menu and displaying the **User Password** dialog box:



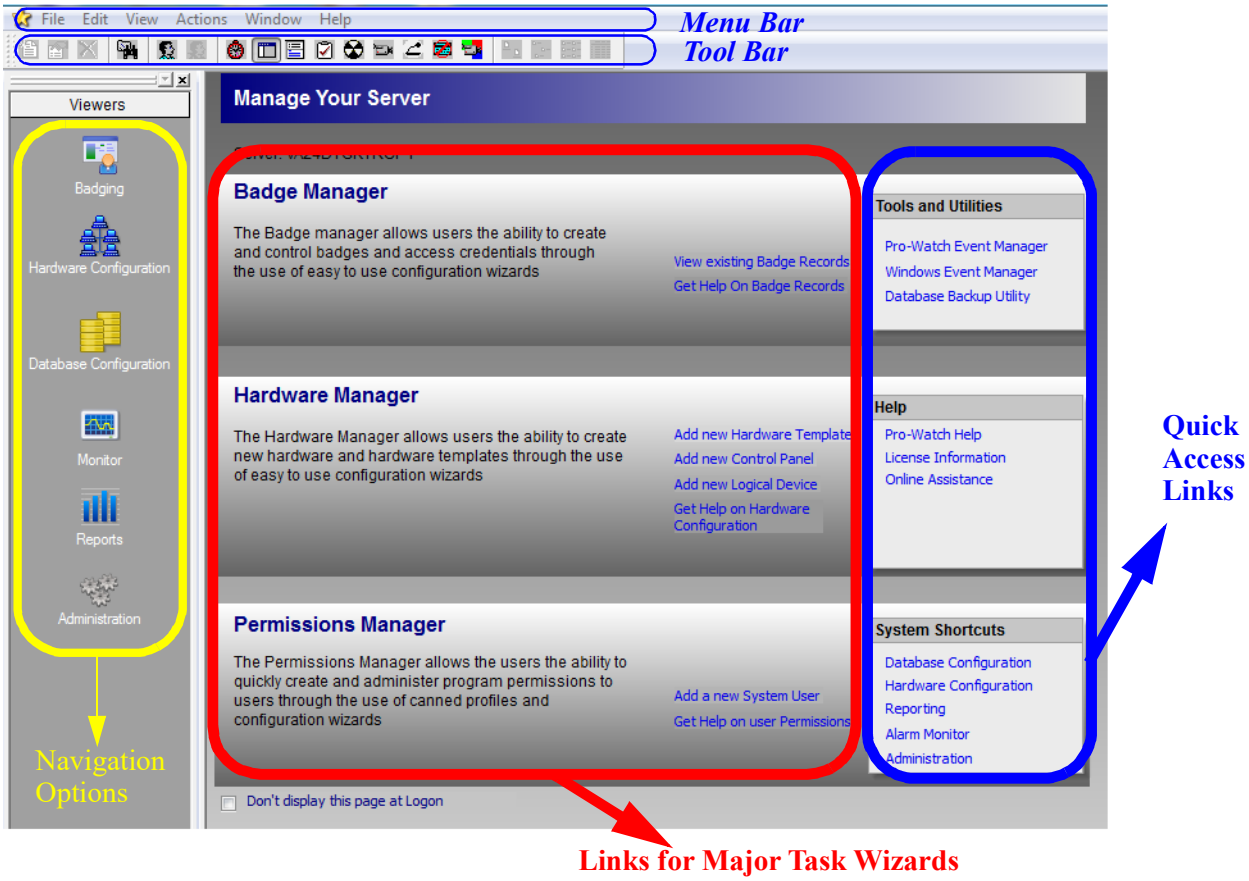
1. Enter your **Old Password**, the **New Password**, and enter it once again in the **Confirm Password** field.
2. Click the **Change Password** button to change your password.

1.3 Pro-Watch Functions

The Pro-Watch main screen below displays:

- Six categories of functions in the left pane.
- A menu bar.
- A tool bar.
- Manage Your Server Switchboard with links to major task groups.

Figure 1-1 Pro-Watch Main Screen



1.3.1 Function Categories

Pro-Watch provides all of the utilities necessary to configure the access management system's hardware and software, design and assign badges, monitor Pro-Watch events, design and produce access reports, and perform a variety of administrative tasks.

1.3.1.1 Badging

Pro-Watch Badging manages badge holder access privileges within your enterprise. A badge holder assumes the access privileges that are assigned

to the holder's company class. The badge holder's access privileges are further defined by the cards the holder uses to gain access to doors.

See Chapter 2, .

1.3.1.2 Hardware Configuration

The Pro-Watch access control system supports hardware, including Honeywell and third-party panels, logical devices (readers, monitorable inputs and controllable outputs), closed circuit television (CCTV) and digital video recorders (DVR).

Within the Hardware Configuration component, the above mentioned hardware types are added and configured. For example, logical devices are configured in functional groups, which are defined by hardware templates. These logical devices, as well as panels, CCTV and DVR hardware, are also governed in the Pro-Watch system by a number of database entities, such as routing groups, clearance codes, and time zones. Therefore, you also need to complete certain tasks within the Database Configuration component of the Pro-Watch to finish the Pro-Watch configuration.

See Chapter 6, .

1.3.1.3 Database Configuration

The Pro-Watch access control system is organized and managed by a variety of configurable software objects, or database elements. These database elements control the specific Pro-Watch hardware items.

See Chapter 27, *Database Configuration (DBC)*.

1.3.1.4 Monitor

The Alarm Monitor enables you to detect and act upon the real-time status of alarms as they occur. Alarms are reported on an alarm page which displays the alarm types. For each alarm type, the specific alarms appear in order of priority and occurrence.

The Alarm Monitor also provides an Alarm Rollup function that displays multiple events for a single logical device in a single line.

See Chapter 3, .

1.3.1.5 Reports

You can produce a comprehensive report of any Pro-Watch data group of your choice in a few keystrokes. You can select data to matrch specified criteria, sort the data by specified fields, and partition the report. You can preview, print, or export the report. The general categories of reports you can generate are:

- Access reports.
- Badge holder reports.

- Company reports.
- Configuration reports.
- Logging reports.
- User reports.

You can also design your own report.

See Chapter 4, .

1.3.1.6 Administration

Pro-Watch provides the following administrative applications:

- Badge Builder – builds a badge profile. See Chapter 60, *Badge Building*.
- Data Transfer Utility – transfers data between Pro-Watch and external data sources. See Chapter 63, *Data Management*. The following external data sources are used to export and import data from and to Pro-Watch database tables:
  - SQL/Microsoft Access database tables.
  - Delimited text files.
- Legacy Restore Utility – restores archive files back into the EV_LOG and Audit Log table. See Chapter 63, *Data Management*.
- Pro-Watch Registry Editor – edits Pro-Watch's registry key values. See Appendix N, Registry Management.
- Map Builder – places resource icons on a Pro-Watch map. See Chapter 61, *Map Building*.
- Report Viewer – creates, prints, or exports Pro-Watch reports. This is the same application that launches when you click the Reports icon on the left pane of the Pro-Watch main screen. See Chapter 4, .

1.4 Tool Bar

The Pro-Watch tool bar consists of the following buttons:



New

Click this context-sensitive button to add a new Pro-Watch object to the right pane. For example, in the Hardware Configuration module, if you select **Device Types** from the middle pane and click **New**, the Add Device Types dialog box opens where you can add a new device type.



Properties

Click this context-sensitive button to edit a Pro-Watch object selected from the right pane. For example, in the Hardware Configuration module, if you select the device type **Door Position** from the right pane and click **Properties**, the Edit Device Types dialog box opens where you can edit the attributes of the Door Position device.



Delete

Click this context-sensitive button to delete a Pro-Watch object selected from the right pane. For example, in the Hardware Configuration module, if you select the device type **Door Position** from the right pane and click **Delete**, the Door Position device will be deleted. However, item A cannot be deleted if it is used in item B (which is also known as item A's "dependency"). You must remove all the references to item B before you can delete A.

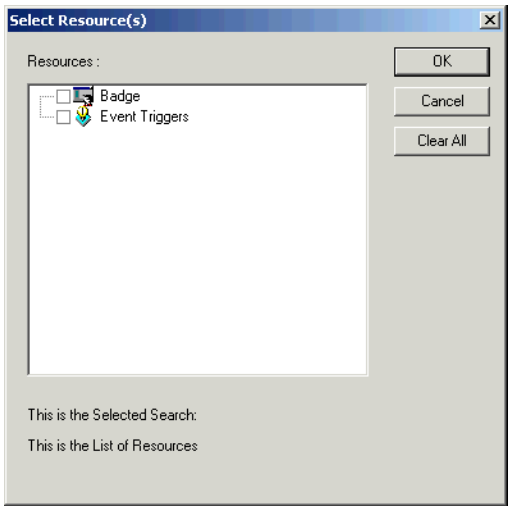


Find

Click this button to search and find a Pro-Watch object in any of the modules.

1. Click the **Find** icon  on the main toolbar to launch the search screen.
2. Select a **Pro-Watch component** from the **Look For** drop-down list.

Click **Browse** to display the Select Resource(s) screen:



3. Select as many **resources** as you like from the list and click **OK**.
4. If you also want to search by keyword(s), enter one or more **keywords** into the **Search for the word(s)** field.
5. Click on the **down arrow** at the end of the **In** field to display the drop-down list of targets in which you want Pro-Watch search for the keyword(s). Select a **keyword target**. Note that this is a context-sensitive drop-down list, and it displays differently according to the component you select in the Look For field.
6. Click **Find Now** to display all the search results in the grid below.
7. Click **New Search** to conduct a new search.



Shadow User

Pro-Watch allows a local administrator to login over a currently logged-on user without having the current user logoff Pro-Watch. For example, the system allows an administrator to login over a restricted class user to perform a function on the system that the current user does not have permission to perform. Thus, this means that the user's workstation never needs to go offline and never needs to be unattended.

1. Click the **Database Configuration** icon on the left pane.
2. Select **Users** from the Database Configuration tree view.
3. Click **New** and add a new user.

4. Go to SQL Server. Select **Enterprise Manager > Security > Logins** and add the user. Give the user access to Primary and Pro-Watch databases.
5. Go to Administrative Tools within the Control Panel and select **Local Security Policies > Local Policies > User Rights and Assignments**.
6. Grant "Logon as a Service" and "Act as part of the operating system."
7. When the shadow user has logged on, you will see his/her user ID in the status bar at the bottom of the Pro-Watch screen.



Logoff Shadow User

Click this button to logoff the shadow user. This button is enabled only when an administrator is logged on as a shadow user.



View Event Log

Click this button to display the event log dialog box. The Event Log allows you to create SQL queries using fields including:

- Database Field.
- Operator.
- Date and Time.
- Value.
- Sort By.

After defining the SQL queries, you may search for events in the event log or choose to view the last 500 alarms.



Viewer Bar

Click this button to hide or display the left panel.



Toggle Event (Event Monitor)

1. Click this button to display the event monitor screen to view events.

2. Click **Arrange** on the mini tool bar to display the Arrange Event Viewer Columns dialog box. You can select one of the following Database Fields from the drop-down list: Event Date, Logical Device Description, Alarm Type, Panel Name, Subpanel Name, Reader Name, Input Name, Output Name, Company Name, Workstation, User.
3. Click **Filter** on the mini tool bar to display the Event Viewer Filter dialog box where you can filter the events by Message Type, Workstation, and User ID by selecting appropriate values from the three respective drop-down lists.
4. Click the **Download Messages** tab at the bottom of the screen to view the list of downloaded messages.

   Click **Download Message Parameters** to display the Channel Download dialog box. In this dialog box, you can set the time interval (in seconds) for the download channel interval.



Verification

Verification viewer provides for remote, operator-validated access for particular access points. See Appendix A, Secure Mode Verification.

Note: The Verification Window changes for different users when the operator clicks on the badge photo of the respective users. The user information is not displayed automatically.

See Verification Window, page 23 below for an illustration.

1. Click the **Verification** icon to display the verification screen.

Note: Click **New** to display the Logical Devices screen where the devices are listed by Description and Location. Select a logical device by highlighting it. Click **OK** to add it to the Logical Device Name pane. The number of logical devices are unlimited.

The user can also search for logical devices that are not displayed in the Logical Devices screen. As the user types in a string into the “Search Key” field in the upper-right corner of the screen, the Logical Devices that have descriptions or locations that match are returned. This is helpful on sites that have a large number of logical devices.

2. Click **Live Video Window** to toggle the live video window on and off for all the logical devices selected in the left pane.
3. Click **Cascade** to cascade the verification windows for all the logical devices selected in the left pane.
4. Click **Freeze** to freeze the live video.

5. Click **Show Pictures Given Access (a.k.a. Grants)** to display in the verification window the photograph or signature of the card holder plus a video picture (live or frozen) for only those events with access-granted status.
6. Click **Sound Bell** to ring a bell when access is granted.
7. Click **Show Pictures Denied Access (a.k.a. Denies)** to display in the verification window the photograph or signature of the card holder plus a video picture (live or frozen) for only those events with access-denied status.
8. Click **Deny Bell** to ring a bell when access is denied.



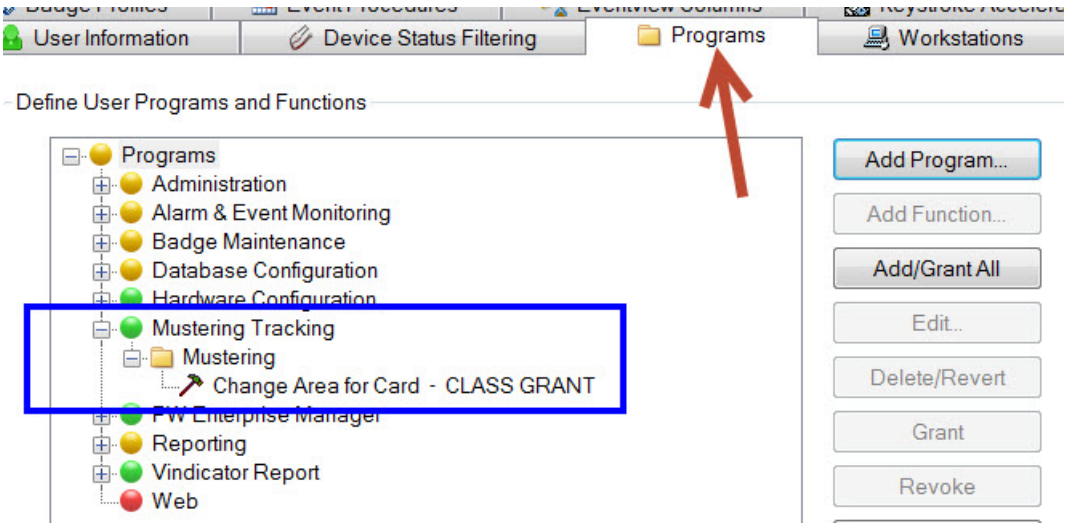
Mustering (Not available with Pro-Watch Lite)

Click the mustering button for real-time monitoring of who is in or out of a particular area. The information is listed across the **Event Time, Device Description, Name, Card No.**, and **Description** columns. The Mustering mini tool bar enables you to toggle the Freeze button to freeze the list on the verification viewer. In addition, you can toggle the **Bell** button to play a sound when a grant transaction is received by the viewer.

To print the mustering information, click **Print**.

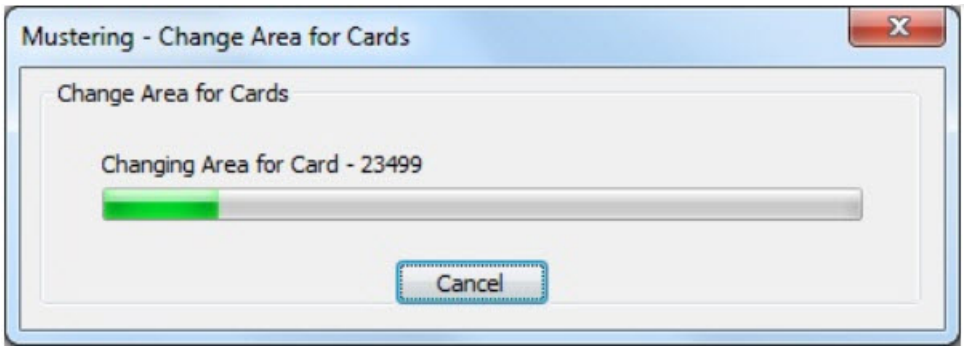
Moving Cards Between Areas

To move the cards between the areas, make sure "**Change Area for Card**" function (in **Database Configuration > Users > Properties > Programs > Mustering Tracking > Mustering**) is granted as shown below:

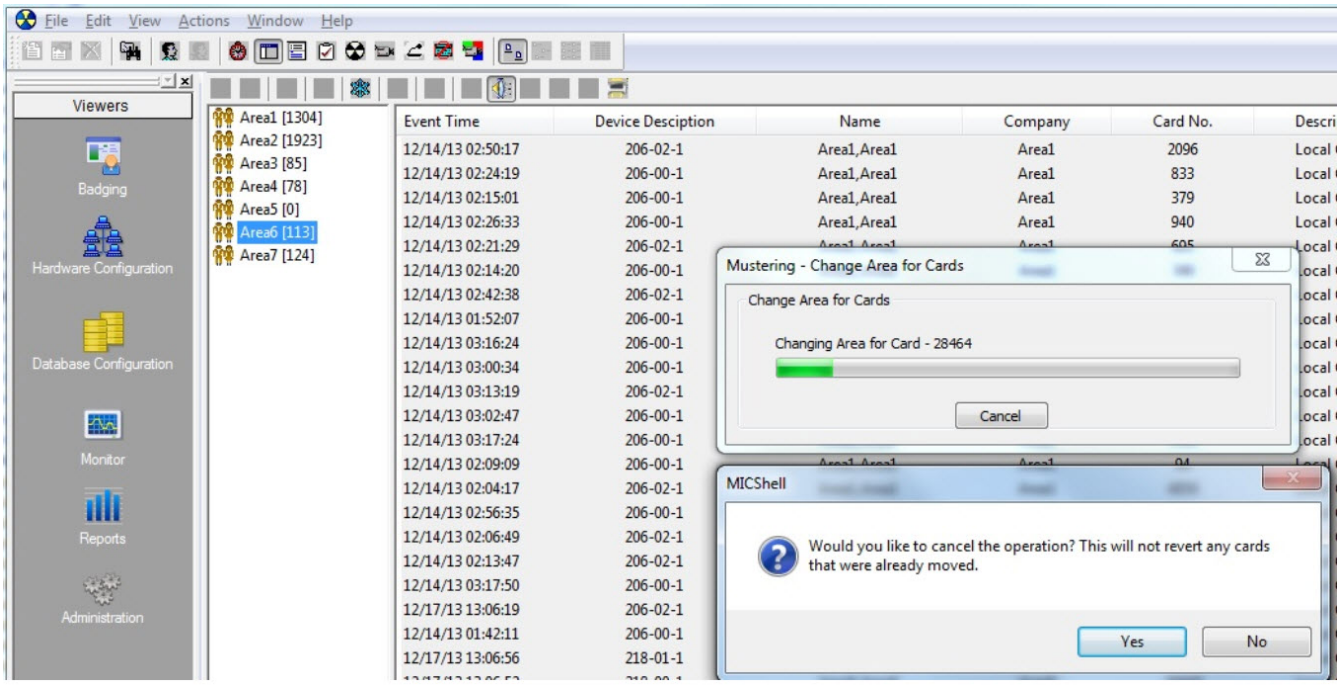


This program-function will be available by default for all **Root Class** users. **Non-Root Class** users will have to manually add this function by clicking the **Add Function** command button.

When you are moving cards from one mustering area to another, Pro-Watch displays a progress feedback bar, like the one below:



Pro-Watch also offers the user the chance to cancel the operation while the cards are being moved from one muster area to another by displaying the following MICShell prompt box:



Note: When the move operation is canceled Pro-Watch does not revert any cards that were already moved to the target mustering area.

Deleting Cards from Areas

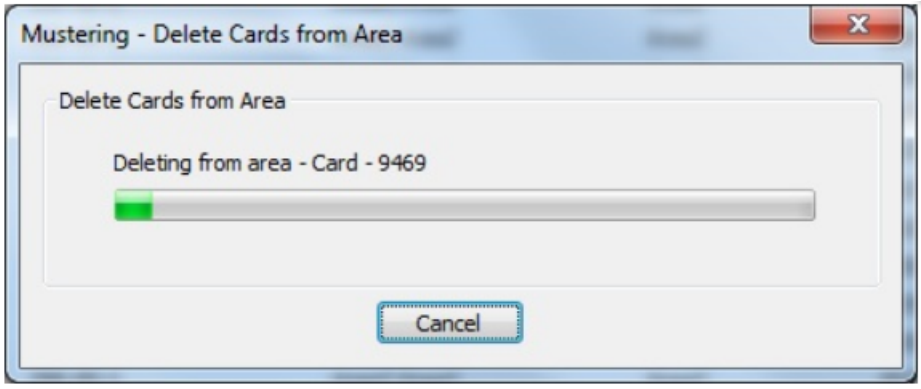
The user can delete cards from an area just as easily as moving them from one area to another.

To delete one or more cards from an area, select them in the card-list pane, right click and from the pop-up menu select the **Delete...** option.

Pro-Watch will generate a confirmation prompt alerting the user to how many cards will be deleted and if the deletion will generate any card downloads to remove the card(s) from the panel:



When deleting cards, Pro-Watch displays a progress feedback bar, like the one below:



Pro-Watch allows users to cancel the delete operation at any time. Please note that if the operation is canceled, Pro-Watch will not undelete cards that were already deleted from the muster area.



CCTV Controls

Click this button to display the CCTV Controls dialog box where you can select a camera and monitor, switch the camera's video to the selected monitor, view presets, pan/tilt, zoom, focus, and change the iris of the selected camera. See Creating CCTV Camera Views in Chapter 22, for more information about CCTV.

1. Select the **camera** from the pull-down Camera menu.

2. To switch the camera's view to a monitor, select the monitor from the pull-down Monitor menu and click **Switch**.
3. To set the camera and view to a preset position, select the position from the pull-down **Preset #** menu.
4. Use the **Pan/Tilt** arrows to move the view to the desired spot. Clicking an arrow moves the camera view in the indicated direction until you click the red stop sign.
5. Use the **Zoom** arrows to zoom in (Up arrow) or zoom out (Down arrow).
6. Use the **Focus** arrows to adjust the proper focus.
7. Use the **Iris** arrows to adjust the view's area.
8. Click **Set** to set the configuration.



Intercom Controls

Click this button to display the Intercom Controls dialog box where you can place a call from one intercom station to another.

1. Select a **Source Intercom** (the intercom station from which the call will be initiated) from the drop-down list.
2. Select a **Target Intercom** (the intercom station receiving the call) from the drop-down list.
3. Select a **Connection Priority** by selecting the appropriate option button.
4. "Dial" is the lowest priority call. If the target is in use, a busy signal is returned.
5. "Low Priority Direct" is a medium priority call. This call forces the target intercom to pick up on the first ring. If the target is in use, a busy signal is returned.
6. "High Priority Direct" is a high priority call. This call forces the target intercom to pick up on the first ring. This call also overrides any call on the target except for another High Priority Direct.
7. Click **Call** to initiate the call.
8. Click **Reset** to terminate an active intercom session and leave the dialog box ready to make another call.



Void Card

Click this button to display the Void Card dialog box where you can void a card.

1. Select a search field from the **Fields** drop-down list. Your options are Card Holder Last Name, Card Number, and Company.
2. Enter a search criterion into the **Criteria** field. When searching by card number, you have to enter the exact card number to find the correct card.

   When searching by last name, entering only the first letter (or the first few letters) of the last name as a "wild card" character will find all the last names that start with that letter (or letters).

   For example, if you select Card Holder Last Name as a search criterion, entering "J" or "j" (not case sensitive) in the Criteria field will return all cards with card holder last names that start with "J" including "James," "John," "Jameson," etc. Entering "Ja," however, will return "James" and "Jameson" but not "John."
3. Click **Find Now** to list the search results in the grid below.
4. Select the card you want to void and click **Void**.



Digital Video Recording

Click this button to configure Digital Video Recording (DVR) display. Pro-Watch supports Integral, Rapid Eye, and VAST DVR. See Configuring Digital Video Recording (DVR) in Chapter 22, for more information about DVR.

- Select a video display "dimension" from the **Dimensions** drop-down list. Your selection will determine how many camera views will be displayed simultaneously on this screen. For example, "1 X 1" will display video feed from only one camera whereas "4 X 4" will display a maximum of 16 video feeds from all the 16 cameras. Other available dimension options are 4 ("2 X 2") and 9 ("3 X 3") camera feeds.
- Select a channel from the **Channel** drop-down list. You can set up cameras on different channels.
- For **Rapid Eye DVR**, click one of the 16 buttons to select one or more of the 16 cameras. When you click on a number-button, the corresponding camera image will appear in the window. You can choose to view more that one image at a time through selecting a value from the Dimensions drop-down list (see the first bullet).
- The **Current Data/Time** field provides a "time stamp" for the video feed(s).



Large Icons

Click this button to list the Pro-Watch items by large icons.

For example:





Small Icons

Click this button to list the Pro-Watch items by small icons.

For example:





List

Click this button to list the Pro-Watch items alphabetically.

For example:

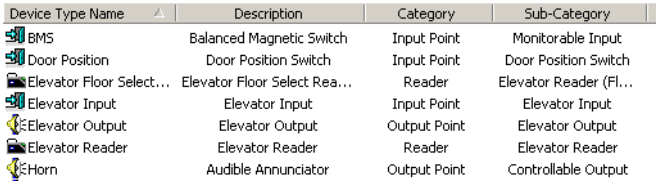




Details

Click this button to list the Pro-Watch items alphabetically and by details across columns determined by system settings.

For example:



Device Type Name	Description	Category	Sub-Category
BMS	Balanced Magnetic Switch	Input Point	Monitorable Input
Door Position	Door Position Switch	Input Point	Door Position Switch
Elevator Floor Select...	Elevator Floor Select Rea...	Reader	Elevator Reader (Fl...
Elevator Input	Elevator Input	Input Point	Elevator Input
Elevator Output	Elevator Output	Output Point	Elevator Output
Elevator Reader	Elevator Reader	Reader	Elevator Reader
Horn	Audible Annunciator	Output Point	Controllable Output

1.5 Verification Window

Verification window displays the following user information for a specific logical device:

- User Name
- Badge Number
- User Photo

This enables the operator to verify (through a camera or in person) whether the person using (e.g., swiping a card) the logical device (e.g., a door reader) is the same authorized user the name, badge number, and photo of whom are displayed in the verification window.

1.5.1 Resized Verification Window

A resized Verification Window maintains its size upon scan.

1.5.2 Minimized Verification Window

A minimized Verification Window is restored to its resized view upon scan.

1.5.3 Maximized Verification Window

A maximized Verification Window maintains its maximized size upon scan.

1.5.4 Two Verification Modes

There are two ways to display user information in a verification window.

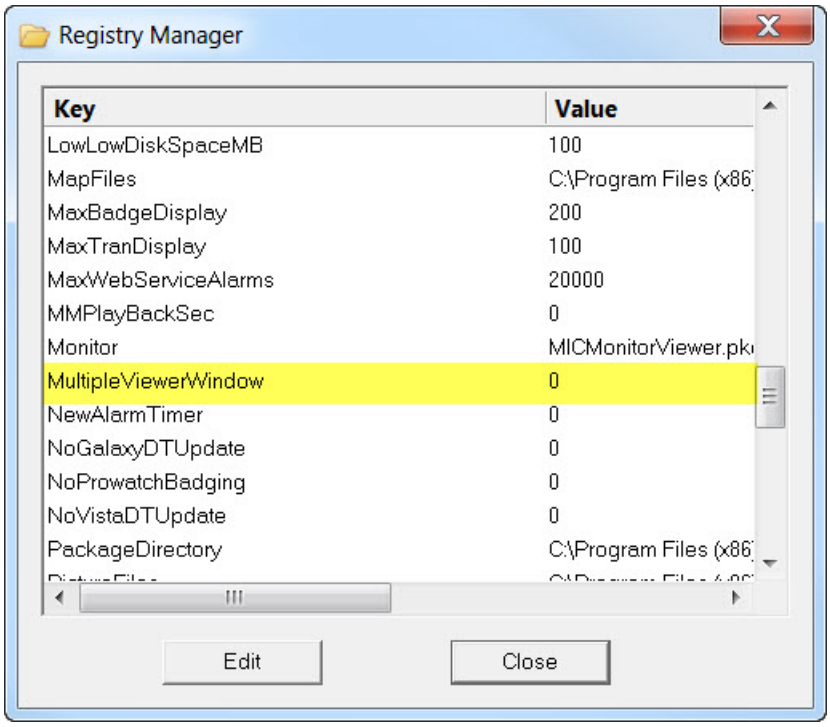
1. The "**Multiple Window**" option displays a separate window for each logical device.
2. The "**Single Window**" option displays a single window for all logical devices.

You can select one of these methods by editing the "**MultipleViewerWindow**" registry key.

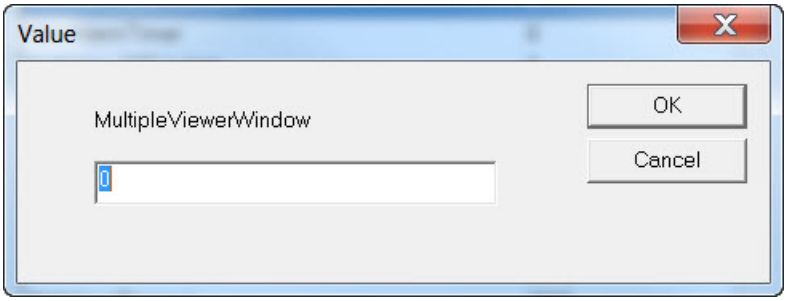
1.5.4.1 Setting the "MultipleViewerWindow" Registry Key

1. Launch the Pro-Watch.
2. From the **Viewers** navigation bar on the left, click and select **Administration** to display the tree-view list in the middle pane.
3. Click the "**+**" sign to the left of the "**Pro-Watch 4 Administration Viewer (PWAdmin)**" directory and expand it to view its subdirectories.
4. Click the "**+**" sign to the left of the "**Executables**" subdirectory and expand it to view its sub-folders.
5. Double-click the "**Pro-Watch Registry Editor**" sub-folder to display the **Registry Manager** screen.

6. In the **Registry Manager**, select the "**MultipleViewerWindow**" registry key:



7. Click **Edit** to display the **Value** editing screen:



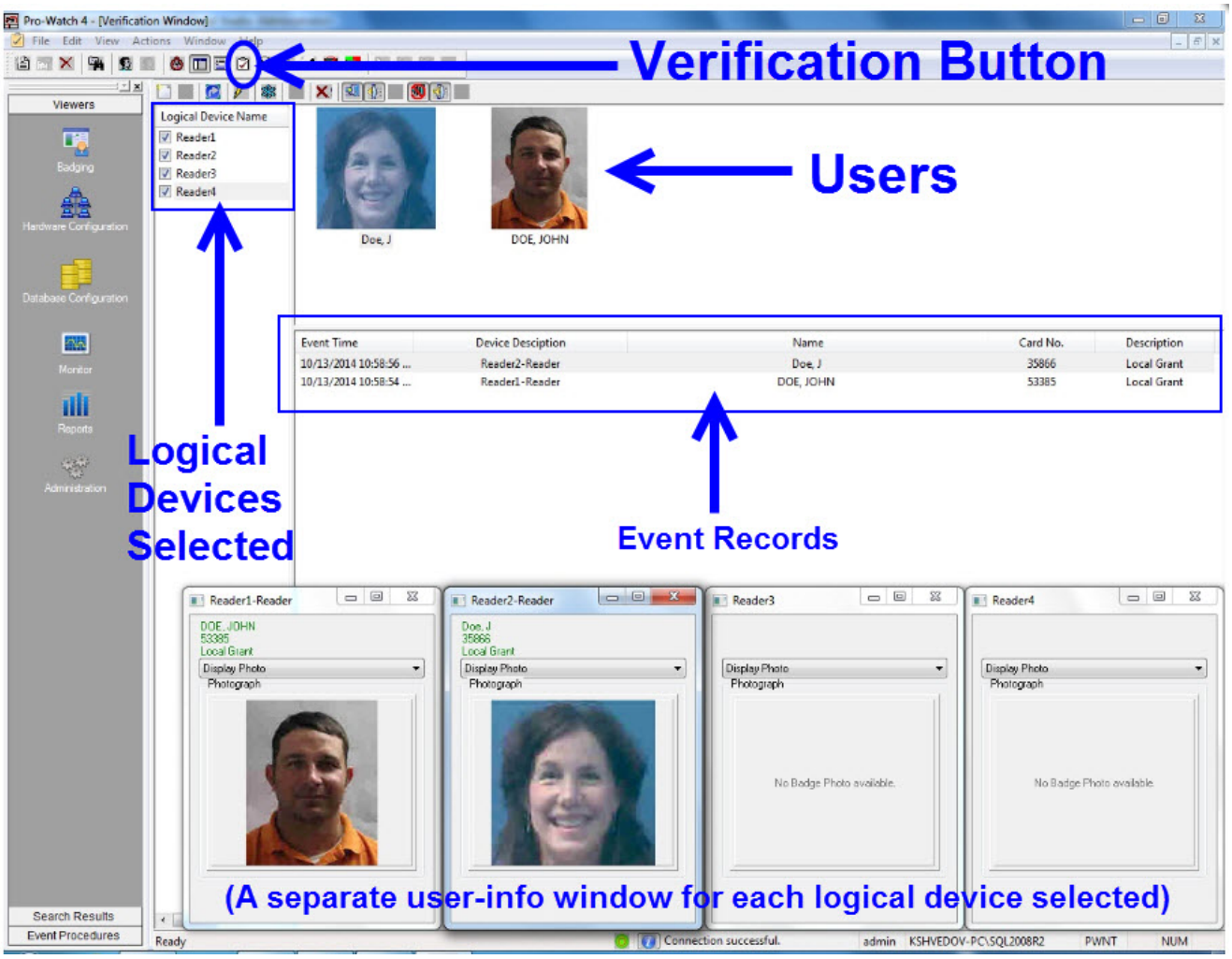
8. Enter one of the two possible values for the "**MultipleViewerWindow**" field, with different implications:
   a. Enter the value "**1**" (one) to have Pro-Watch display a separate window for each logical device. This is known as the "**Multiple Window**" configuration option.
   b. Enter the value "**0**" (zero) to have Pro-Watch display one window for all the logical devices. This is known as the "**Single Window**" configuration option.

9. Click **OK** and then click **Close** to close the **Registry Manager** window.

1.5.5 Multiple Windows

This option allows an operator to click the **Verification Button** and view the verification information in separate windows. The Pro-Watch automatically displays a separate screen for the last user on each logical device selected in the device list.

When a new event happens on a logical device (like when a user swipes a card at a reader) the corresponding window will automatically refresh with the information of this new event. A user does not need to double-click on the event to display this information. The last user that triggers an event is automatically displayed in the respective reader's window. If there are no users on a logical device, then a blank place-holder screen is displayed:



1.5.5.1 Limitation of the Multiple Windows Option

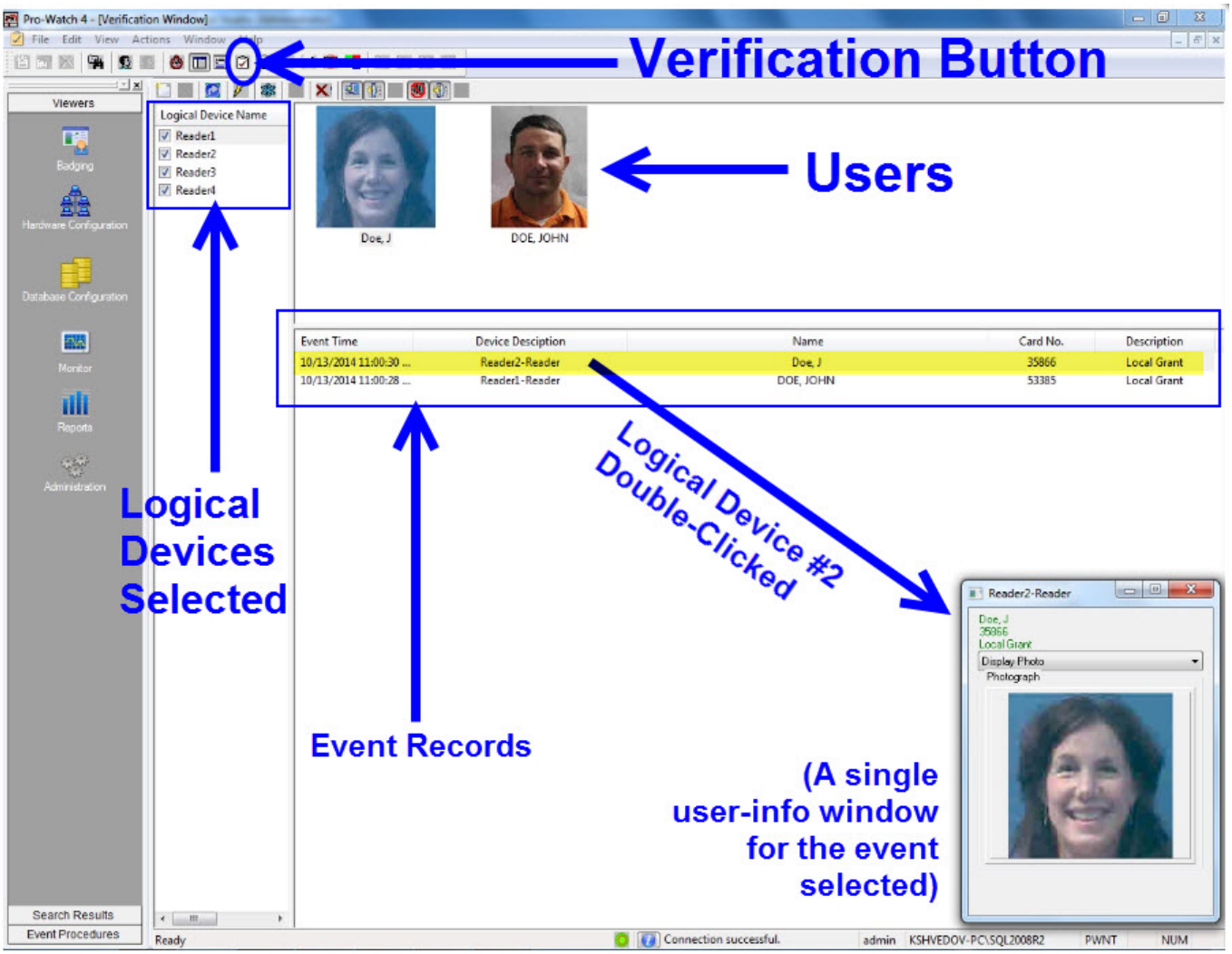
There are no limits to the number of multiple windows that the operator can select.

1.5.6 Single Window

This option allows an operator to click the **Verification Button** and view the verification information for logical devices in a separate window that displays the information about the last user who triggered an event at the device. Verification window displays the user information only for the specific logical-device event record that the operator clicks on.

For example, here below is an example of how the Verification Window changes depending on the logical-device event record that the operator selects.

In this instance only the event at "**Logical Device #2 (Reader 2)**" is selected. Thus only the information about the last user who triggered an event at that reader is displayed:



To display information about other users at other logical devices the operator must keep clicking on other event records, one record at a time.

1.5.6.1 Limitation of the Single Window Option

The operator can select only up to eight logical devices.

1.5.6.2 The Disadvantage of the Single Window Option

For each logical device the operator must click separately and view the respective user information on a separate window.

When the system supports only a few logical devices this might not be too hard at all. Yet, if the system has dozens or even hundreds of readers, the

operator(s) may find it difficult to retrieve information in a reliable manner from different combinations of eight logical devices selected and then clicking on their event records, one at a time.

1.6 Color Coding

Pro-Watch uses color coded icons to display the general status of system components at one quick look. Here are some general examples:

Color	Description
	GREEN - The Pro-Watch component is online and working normally.
	YELLOW - The Pro-Watch component has an indeterminate status.
	RED - The Pro-Watch component is not working.

1.7 Managing the Server Switchboard

The Manage Your Server switchboard provides links to three major task groups.

To prevent this welcome page from displaying, select the **Don't display this page at Logon** check box in the bottom-left corner.

1.7.1 Badge Manager

The Badge Manager enables the users to create and control badges and access credentials through the use of easy configurations wizards.

The following wizards can be launched by clicking their links:

- Add a new Badge Record.
- View existing Badge Records.
- Get Help on Badge Records.

1.7.2 Hardware Manager

The Hardware Manager enables the users to add new hardware and hardware templates through the use of easy configuration wizards.

The following wizards can be launched by clicking their links:

- Add new Hardware Template.
- Add new Control panel.
- Add new Local Device.
- Get Help on Hardware Configuration.

1.7.3 Permissions Manager

The Permissions Manager enables the users to quickly create and administer program permissions for the users through canned profiles and the use of easy configuration wizards.

The following wizards can be launched by clicking their links:

- Add a new System User.
- Get Help on User Permissions.

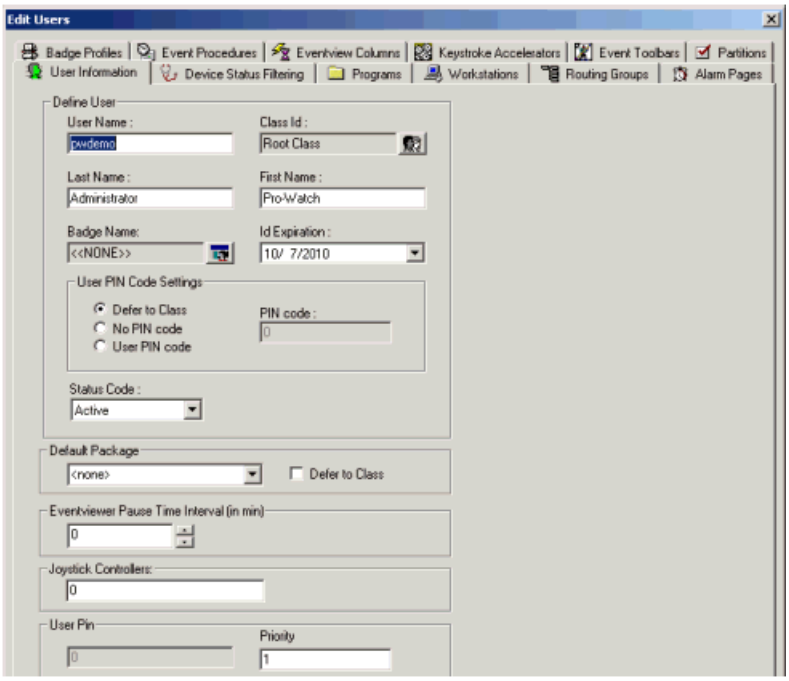
1.8 Turning the Wizards Off

There are four wizards that streamline the Badge Manager, Hardware Manager, and Permissions Manager tasks described above:

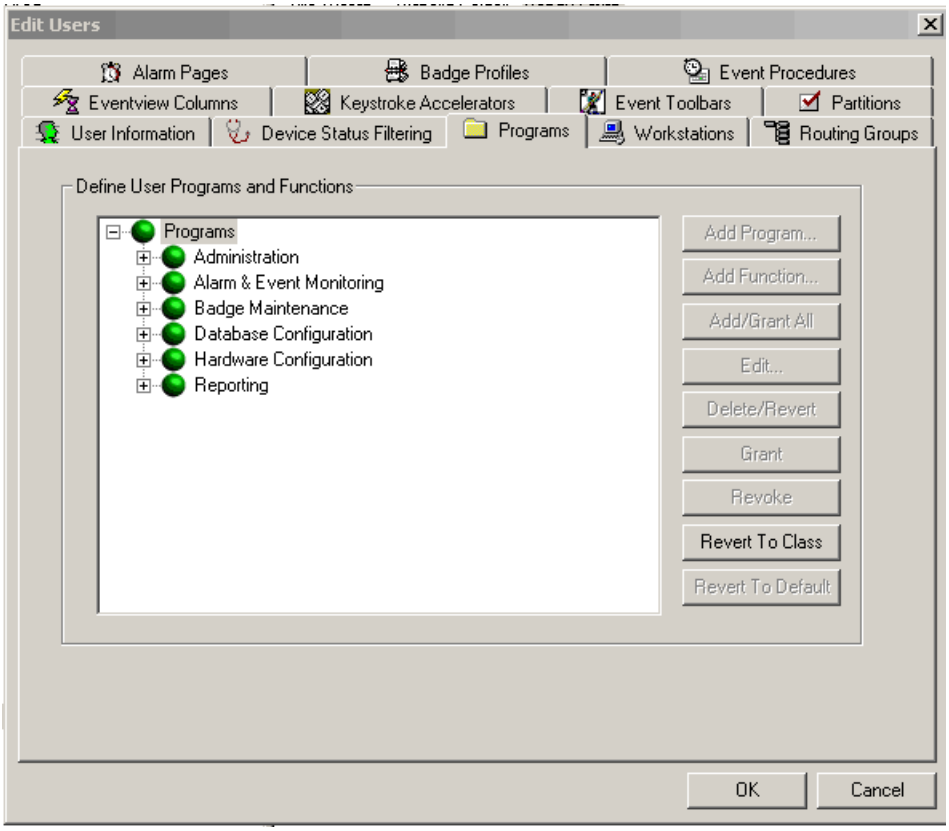
- Panel wizard
- Logical Device wizard
- Badging wizard
- User wizard

By default, all of these wizards are turned on when Pro-Watch starts. However, you can manually turn them off (and on again), if you desire. To turn the wizards off, follow these steps:

1. Select **Database Configuration > Users**. An icon for each configured user appears in the right panel of the window.
2. Click the user for whom you want to turn off the wizard or wizards. The Edit Users screen appears.



3. Click **Programs** to display the tree list of programs available to the user.



4. *In the Programs tree, locate the Use Wizard program for each of the four wizards:*

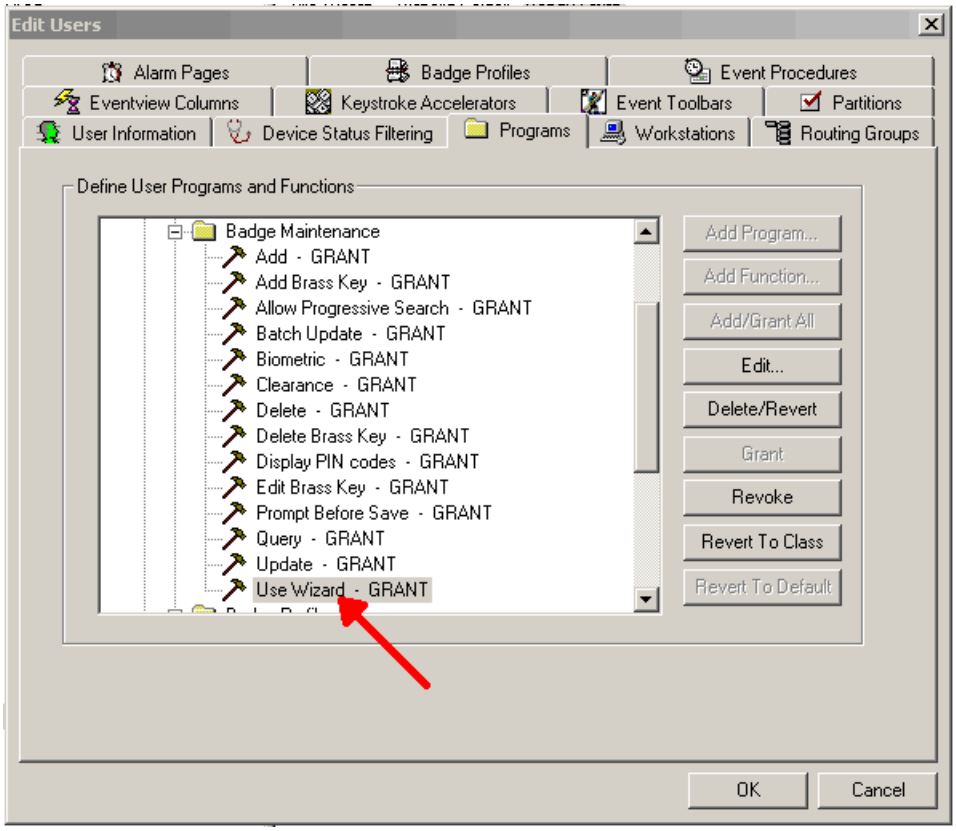
   a. For the Badging wizard, select **Badge Maintenance > Badge Maintenance**.

   b. For the User wizard, select **Database Configuration > User Defines**.

   c. For the Panel wizard, select **Hardware Configuration > Panel Maintenance**.

   d. For the Logical Device wizard, select **Hardware Configuration > Logical Devices**.

5. For example, the Use Wizard program appears at the bottom of this **Badge Maintenance > Badge Maintenance** display:



6. Highlight the Use Wizard program and click **Revoke.**
7. Click **OK**.

Note: You can turn the wizards back on by following the same procedure, except click **Grant** in Step 5.

1.9 Other Quick Access Links

Pro-Watch offers easy access to three other groups of functions, each launched by clicking its link:

1.9.1 Tool and Utilities

- Pro-Watch Event Manager.
- Windows Event Manager.
- Database Backup Utility.

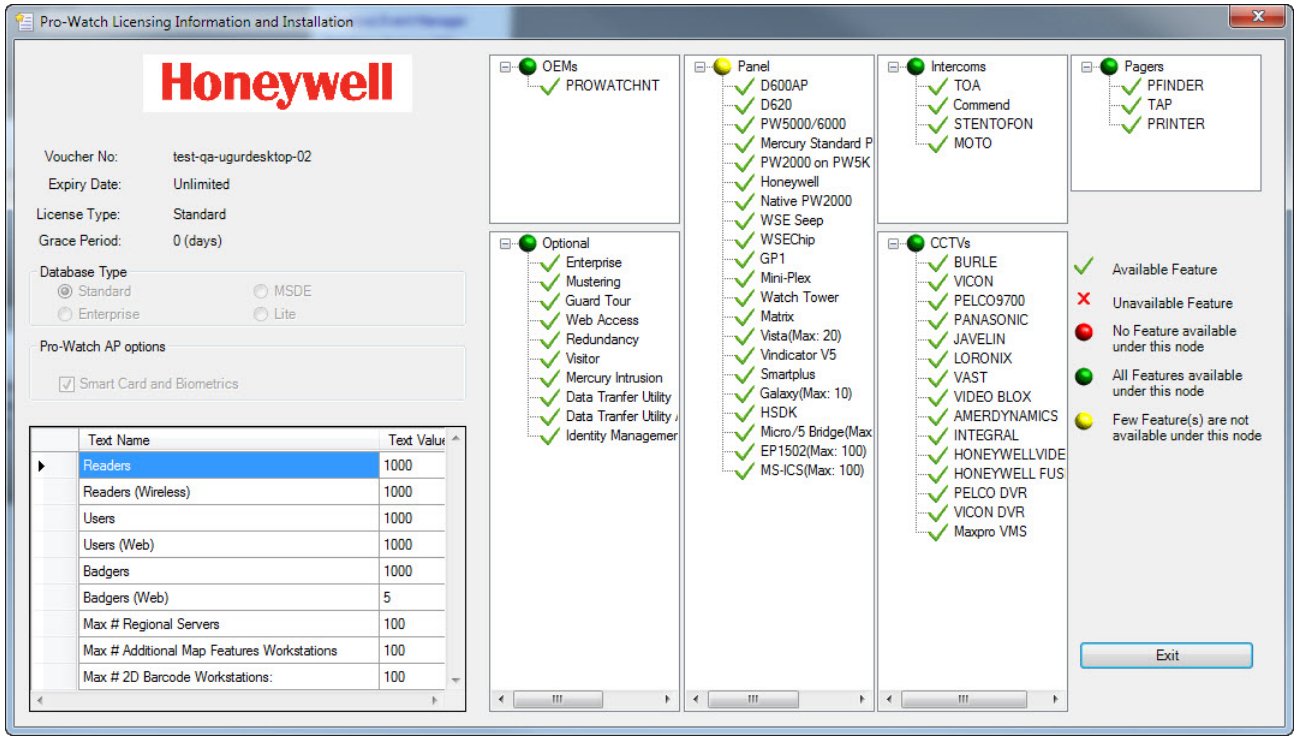
1.9.2 Help

- Pro-Watch Help.
- License Information.
- Online Assistance.

1.9.2.1 License Information

Click the **License Information** link to display "**Pro-Watch Licensing Information and Installation**" screen displaying all the licensing features available or unavailable to the user:

Figure 1-2 Pro-Watch Licensing Information Screen



This screen, listing all the panels, devices, and features which are licensed to the customer, if self explanatory. GREEN check-mark denotes a feature

available to the customer; and a RED cross designates a feature that is not available to the customer. However, we'd like to draw your attention to four fields on this screen.

Note: For more information on licensing, see Appendix S – "Software Keys Licensing".

1.9.2.2 Users and Badgers Fields

- **USERS** field displays the maximum number of total users allowed to use the Pro-Watch at any given time.
- **USERS (WEB)** field displays the maximum number of total users allowed to use the Pro-Watch's web client at any given time.
- **BADGERS** field displays the maximum number of times specific badge functions can be executed in any session by using the Pro-Watch's badging module. These specific badging functions include:
  - Capturing badge photos
  - Previewing cards
  - Printing cards
- **BADGERS (WEB)** field displays the maximum number of times specific badge functions can be executed in any session by using the Pro-Watch Web Client's badging module. These specific badging functions include:
  - Capturing badge photos
  - Previewing cards
  - Printing cards

1.9.3 System Shortcuts

- Database Configuration.
- Hardware Configuration.
- Reporting.
- Alarm Monitor.
- Administration.

1.10 Pro-Watch System Configuration

All Pro-Watch hardware and database configuration and badge profiling is performed by the authorized Pro-Watch Access Control System Administrator(s).

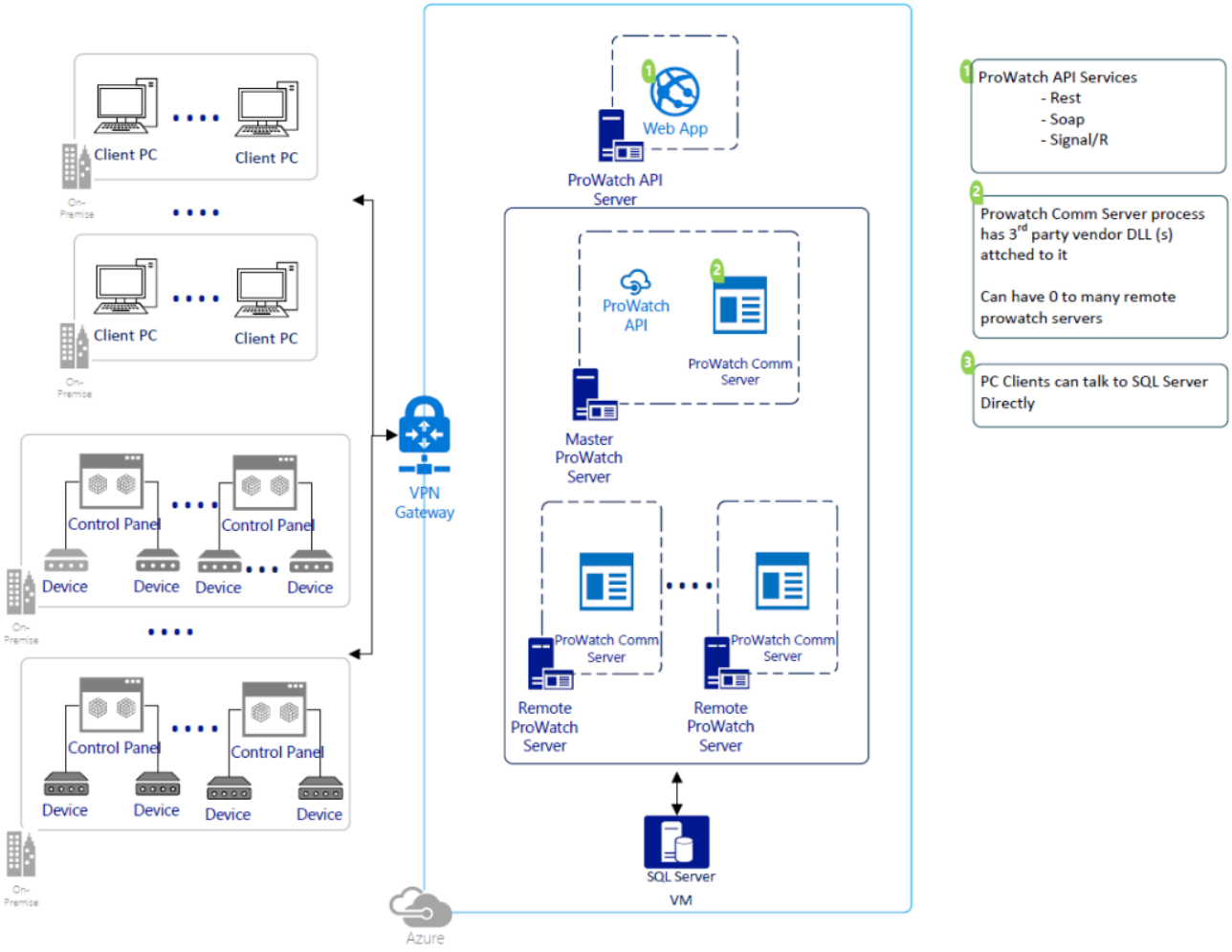
See "Part II ~ Administrator Functions" for information about these administrative tasks.

1.11 Microsoft Azure Cloud

Pro-Watch 4.4 supports Microsoft Azure platform in the form of IAAS (Infrastructure As A Service) support. Pro-Watch has been tested and qualified on virtual machines hosted in Microsoft Azure. Please see the below for the architecture diagram for Pro-Watch/Azure support in Pro-Watch Version 4.4.

Note: Only Windows operating systems are supported with Pro-Watch in the Azure cloud.

1.11.1 Architecture for Pro-Watch Azure V1.2



1.11.2 Setup Requirements and Virtual Machine Creation

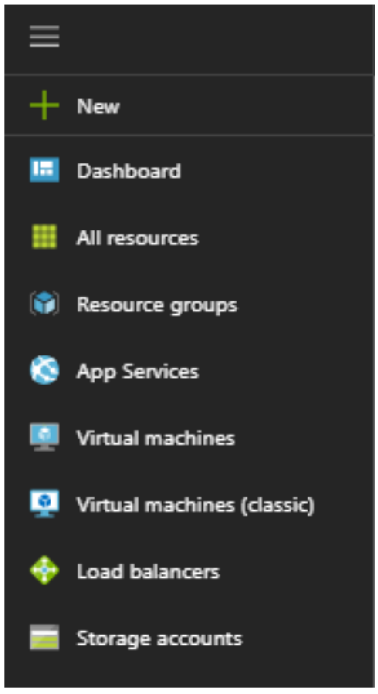
In order to use Pro-Watch in Azure cloud, there are several components that will need to be configured:

Step	Microsoft Resource
Create Azure Resource Group to manage Azure resources	https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-portal
Create a Virtual Network for the Azure IAAS VMs	https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-get-started-vnet-subnet
Create a Virtual Machine	https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal

Note: When creating a new **virtual machine**, Azure will ask for a deployment model for the VM. It is highly recommended that the **Resource Manager** deployment model is used:

1.11.3 Connecting to the Virtual Machines

After creating the virtual machine, navigate to the virtual machines through the Azure Portal by selecting Virtual Machines:

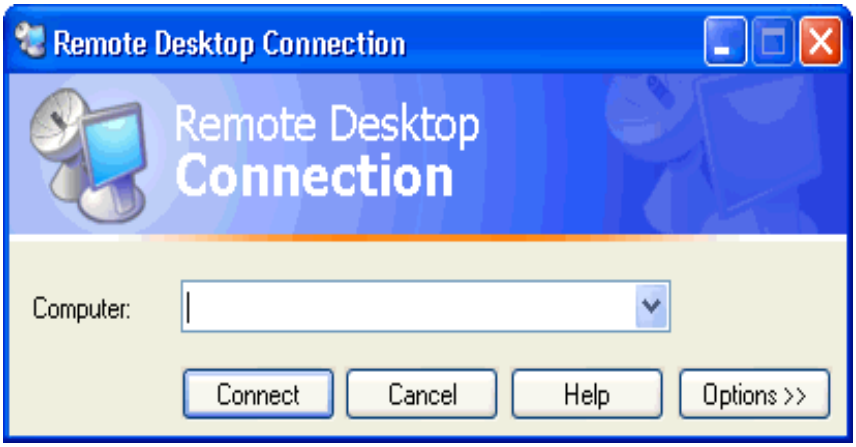


The list of all created virtual machines in Azure will be displayed.

Clicking on the virtual machine will display the general information of the virtual machine including the **resource group, status, location, subscription, subscription ID, computer name, operating system, size, public IP address, virtual network and subnet, and DNS name**.

In addition, a dashboard with several importance performance monitors will be displayed such as the **CPU usage, network usage, disk bytes**, and **disk operations**.

Connection to the machines are done via RDP using the DNS name, which can be changed depending on user preferences. For example, if the machine has a DNS name of mymachine.eastus.cloudapp.azure.com, then to connect to that virtual machine, use RDP and connect to that DNS name:



When the machine is created an Azure, an administrator user account is created as well. This is the user account that will be used to connect to this machine. For example: mymachine\administrator

1.11.4 Networking Rules

VMs hosted in the Cloud will be accessible via the Internet; so it's very important to setup the appropriate networking rules to prevent cybersecurity related issues. The Azure Portal allows individualized inbound and outbound port rules to allow traffic through the selected ports.

To view the network rules, in the Azure Portal, select **Virtual Machines > [Machine Name] > Networking**. Individual inbound and outbound port rules can be added here for each virtual machine.

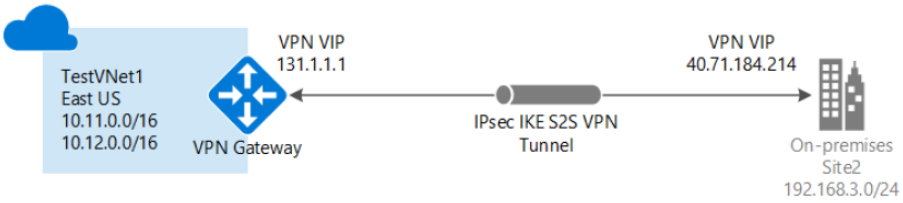
1.11.5 Supported Configurations

There are several different configurations that can be used in Azure:

- Virtual Machines can be standalone machines with no connection to on-premise resources. This can be used as a test environment.
- A domain controller can be hosted on an Azure VM with additional VMs added to the domain.
- The on-premise Active Directory can be synced with Azure Active Directory to offer seamless login using active directory accounts into Azure virtual machines.

1.11.6 Connecting Cloud Resources with On-Premise Resources

In order to connect the Azure Cloud VMs with on-premise network resources, a VPN or ExpressRoute will need to be setup. Please note that once this is setup, the VMs will no longer be accessible from the Internet and will only be accessible from within the VNET.



To find out more about connecting on-premise to the Cloud, please visit the following Microsoft resources:

Resource	Resource Link
Determinig Whether to Use VPN or Express Route	https://azure.microsoft.com/en-us/blog/expressroute-or-virtual-network-vpn-whats-right-for-me/
ExpressRoute Main Page	https://azure.microsoft.com/en-us/services/expressroute/
Azure Site-to-Site VPN	https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
Azure Point-to-Site VPN	https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

1.11.6.1 Other Options

For hardware panels (Mercury panels), if a VPN is not used, connection from the panel to the Azure resource can be done through IP Client. In the

webserver of the IC, the DNS of the Azure VM will be used in order to establish this connection.

1.11.7 Supported Components in Cloud

Pro-Watch 4.5 and 4.5 SP1 support **Microsoft Azure** set of cloud services.

For Pro-Watch 4.5, the following components can be hosted via IAAS in the Cloud:

- Pro-Watch with DB/App Server on the same machine
- Pro-Watch with separate DB/App Server
- Separate Pro-Watch comm server
- Pro-Watch 4.4 Web
- Pro-Watch API/Web DTU

1.11.8 Installing Pro-Watch

After the setup of Azure resources, installing Pro-Watch on the Cloud VM will be identical to installing Pro-Watch on an on-premise environment.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Advanced Badging

2

In this chapter ...

Overview
Logging in to Advanced Badging
Using the Menu Bar
Using the Navigation Pane
Adding a Badge
Editing a Badge
Adding a Card
Editing a Card
Scheduling Clearance Codes
Copying Cards
Downloading Cards
Editing a Badge Holder's Card
Deleting Cards
Mobile Credentials (HID)
Assigning Assets
Using E-Docs
Assigning Partitions
Assigning Notes
Previewing Badge Records
Printing Badge and Card Records
Administration
Opening Multiple Instances of Advanced Badging

2.1 Overview

Since Release 4.1, Pro-Watch software includes a badging module that you can use to create badges and assign card access privileges within your enterprise.

The Pro-Watch Badging module creates badges and assigns card access privileges within your enterprise. This chapter describes how to design and create badges and how to assign privileges to cards.

The complete badging process, however, includes other tasks not described in this chapter. For example, you must first create badge profiles in the Badge Builder utility described in Chapter 60, *Badge Building*. Other tasks, as well, must be completed within the Database Configuration component (see Chapter 27, *Database Configuration (DBC)*).

Note: For using Advanced Badging with Morpho Biometrics module, see Chapter I, Pro-Watch Biometric Service.

2.1.1 Valid Pro-Watch Users for Application Login

Those who are using Windows login must be **valid Pro-Watch users**. Otherwise the system displays an error message.

2.2 Logging in to Advanced Badging

Click the **Badging** icon on the Pro-Watch main navigation bar to display the **Advanced Badge Manager Dashboard** screen:

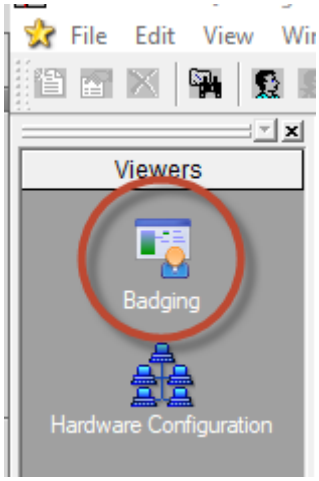
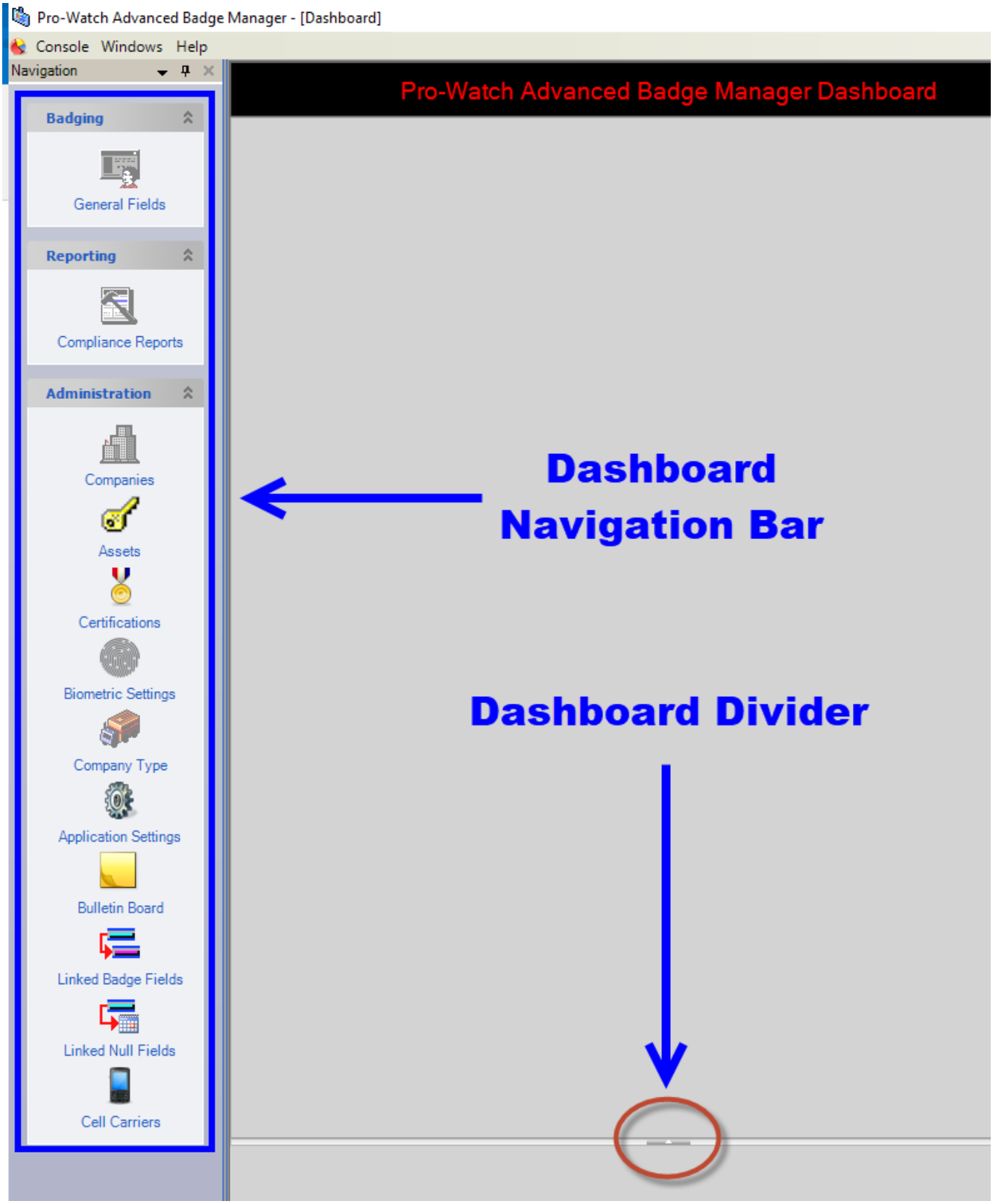
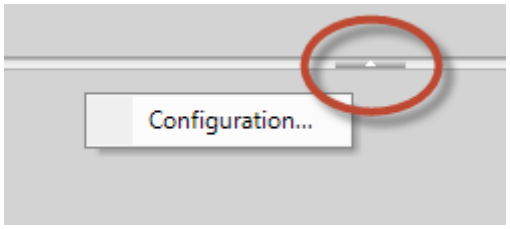


Figure 2-1 Pro-Watch Advanced Badge Manager Dashboard



2.2.1 Configuring the Advanced Badging Dashboard

1. **Right-click** in the are **below the Dashboard Divider** to display the configuration pop-up menu:



2. Select **Configuration** to display the **Dashboard Configuration** screen:

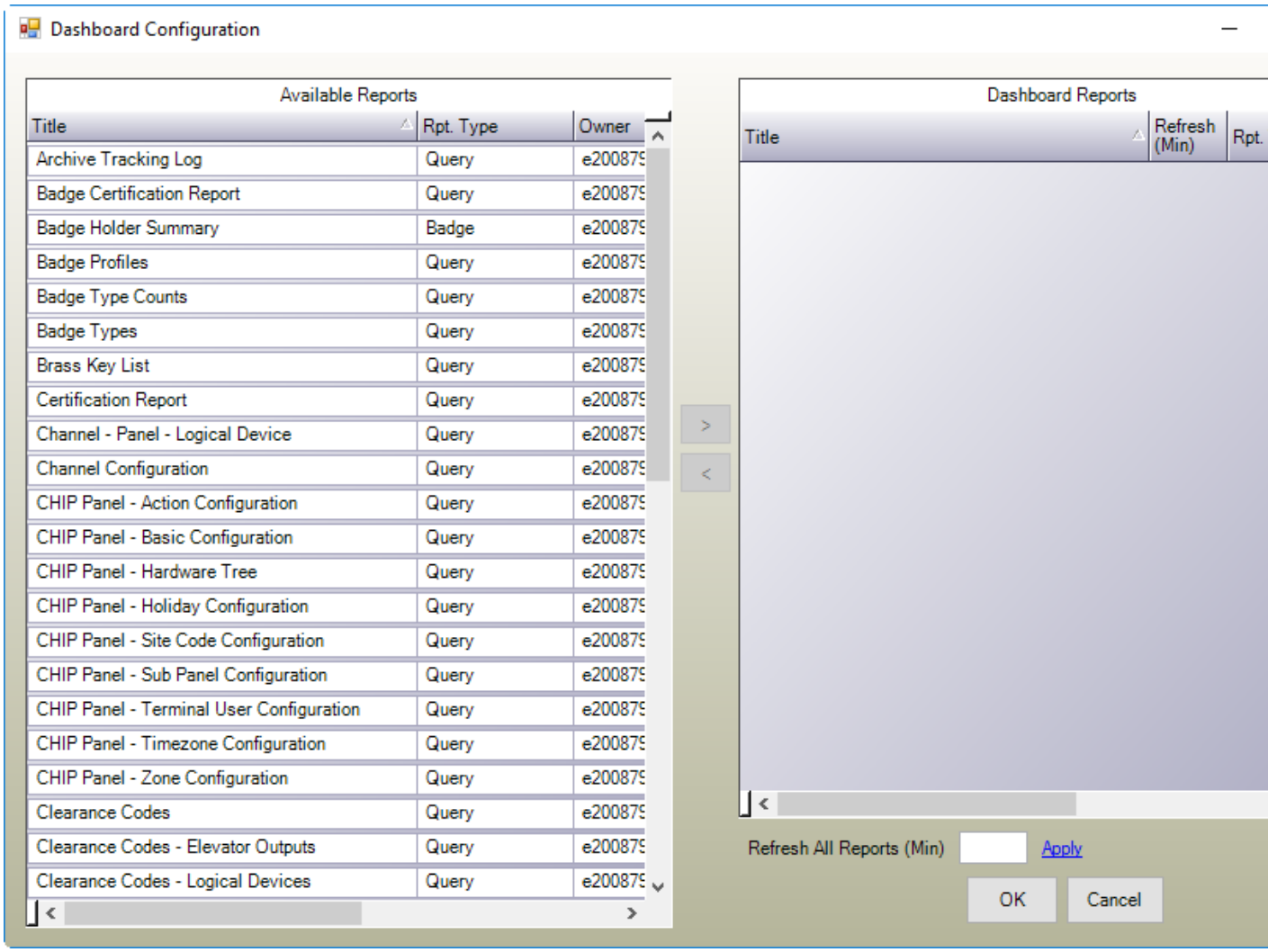


Figure 2-2 Advanced Badge Manager Dashboard Configuration Screen

3. To **add** reports to the **Dashboard Reports** list, select them from the **Available Reports** list and click the right-pointing arrowhead (>) to display them in the **Dashboard Reports** list.

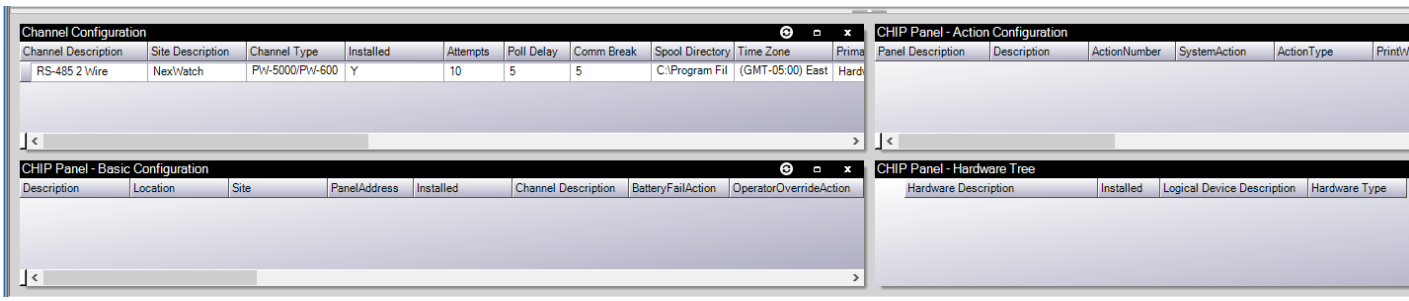
   NOTE: Press and hold the **CTRL** key to select multiple reports at the same time. Press and hold the **Shift** key to select a range of consecutive reports.

4. To **remove** reports from the **Dashboard Reports** list, select them from the **Dashboard Reports** list and click the left-pointing arrowhead (<) to display them in the **Available Reports** list.

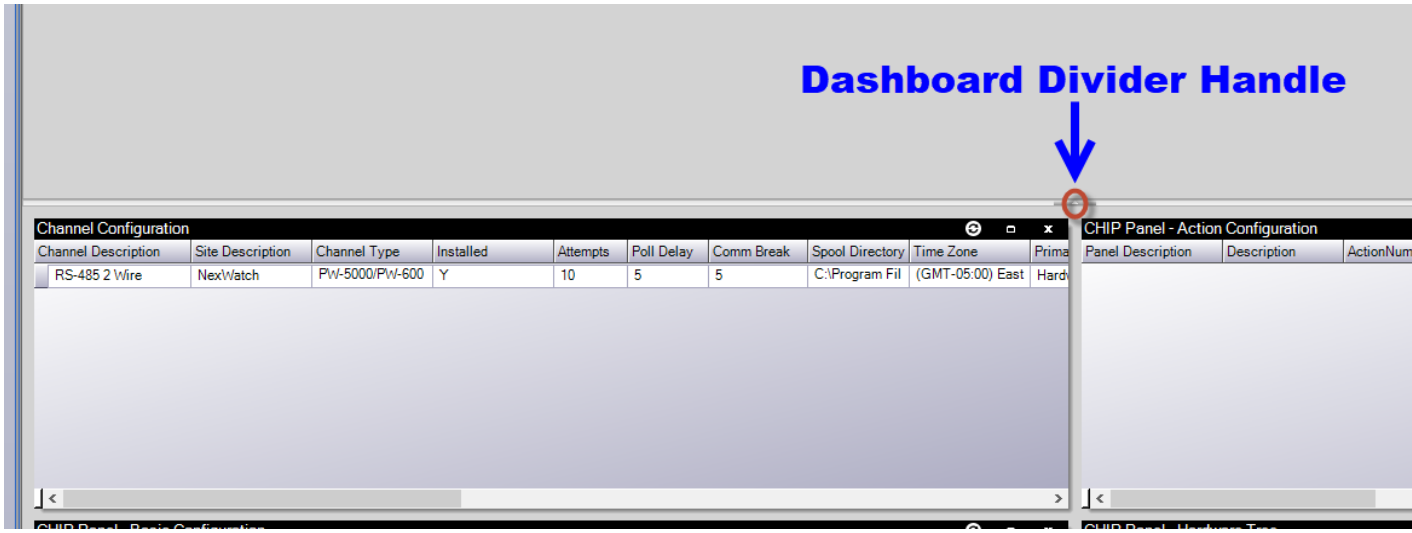
   NOTE: Press and hold the CTRL key to select multiple reports at the same time. Press and hold the **Shift** key to select a range of consecutive reports.

5. Enter an appropriate value (in minutes) to the "**Refresh All Reports**" field and click **Apply**.

6. When finished, click **OK** to display the selected reports below the **Dashboard Divider**:



7. Grab the **Dashboard Divider's handle** and drag it vertically for a larger display:



8. For a **full-screen display** of dashboard reports, **double-click** the **Dashboard Divider handle**:



2.3 Using the Menu Bar

The Pro-Watch Advanced Badge Manager menu bar is located at the top of the main screen:



Click **General Fields** in the navigation pane to view the full menubar. All the menubar options are explained below.

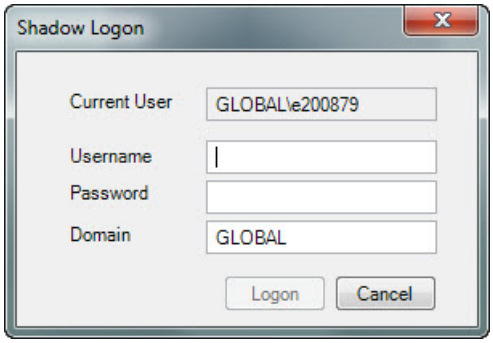
2.3.1 Console > Options

2.3.1.1 Shadow Logon

Shadow Logon allows anyone to log on (with the Username and Password you enter) over a currently logged-on user without having the current user log off from Pro-Watch or Windows.

For example, the system allows anyone to log on over a restricted class user to perform a function on the system that the current user does not have permission to perform. Thus, the user's workstation never needs to go offline and never needs to be unattended.

1) Select **Console > Shadow Logon** from the menu bar to display the logon dialog box:



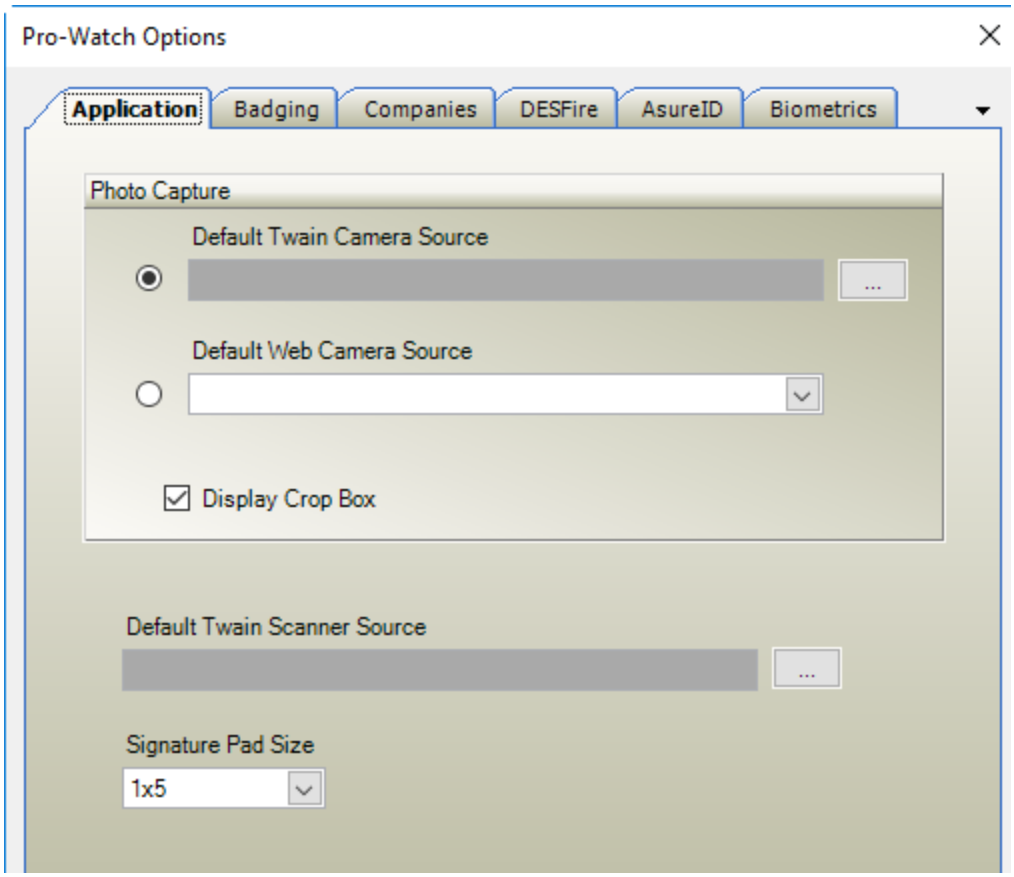
2) Enter the correct **Username**, **Password, Domain** and click **Logon**.

Shadow Logout — Logs off the shadow user. This button is enabled only when an administrator is logged on as a shadow user.

Options — Provides the following option tabs:

2.3.1.2 Application

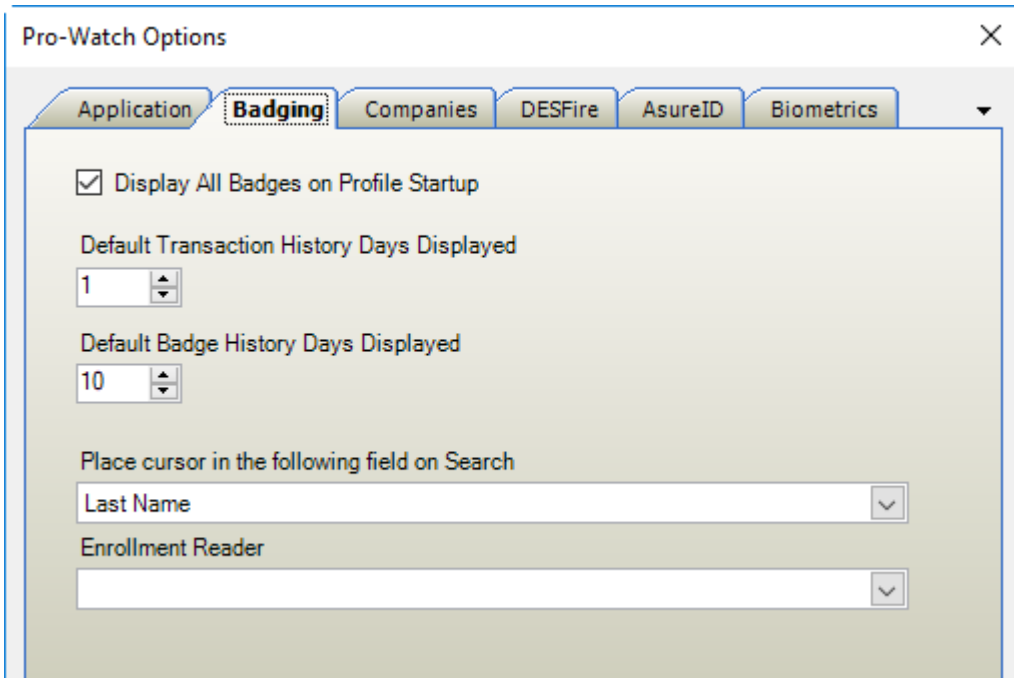
Select **Console > Options > Application**:



- **Default Twain Camera Source** — Select the camera used to take the badge photograph. Use the browse button to select a default Twain camera from the available Twain devices.
- **Display Crop Box** — Select this box if you want to crop and resize the photograph after it is taken. If you do not select this box, you will not be able to crop the photograph and the badge will display the original image capture.
- **Default Twain Scanner Source** — Select the scanner to be used to import company signatures in the Company Contacts screen. Use the browse button to select a default Twain scanner from the available Twain devices.
- **Signature Pad Size** — Select the signature pad size you like from the drop-down menu.
- Click **OK** when done.

2.3.1.3 Badging

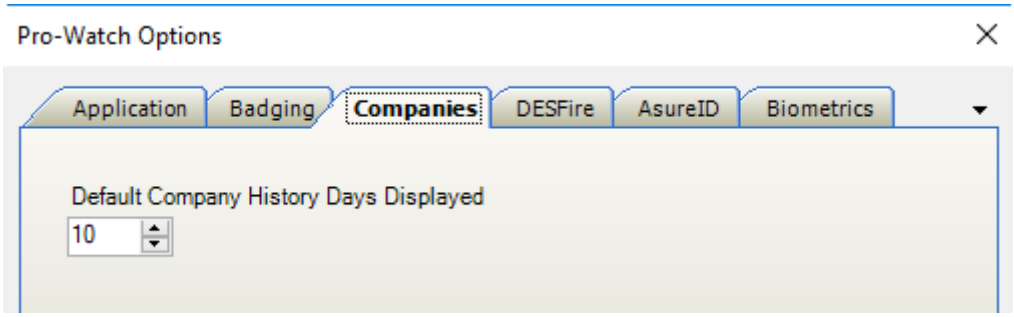
Select **Console > Options > Badging:**



- Select the **Display All Badges on Profile Startup** check-box to display all badges on profile setup.
- **Default Transaction History Days Displayed** — Sets the default number of days from the current date and time that a badge holder's transactions will appear in the Badge > Badge Transactions tab.
- **Default Badge History Days Displayed** — Sets the default number of days from the current date and time that a badge holder's audit information will appear in the Badge > History tab. This information includes what badge record information was changed, by whom it was changed, and when it was changed.
- **Search Field** — Select a search category from **Place cursor in the following field on Search** drop-down menu.
- **Enrollment Reader** — Select an enrollment reader from the drop-down menu.
- Click **OK** when done.

2.3.1.4 Companies

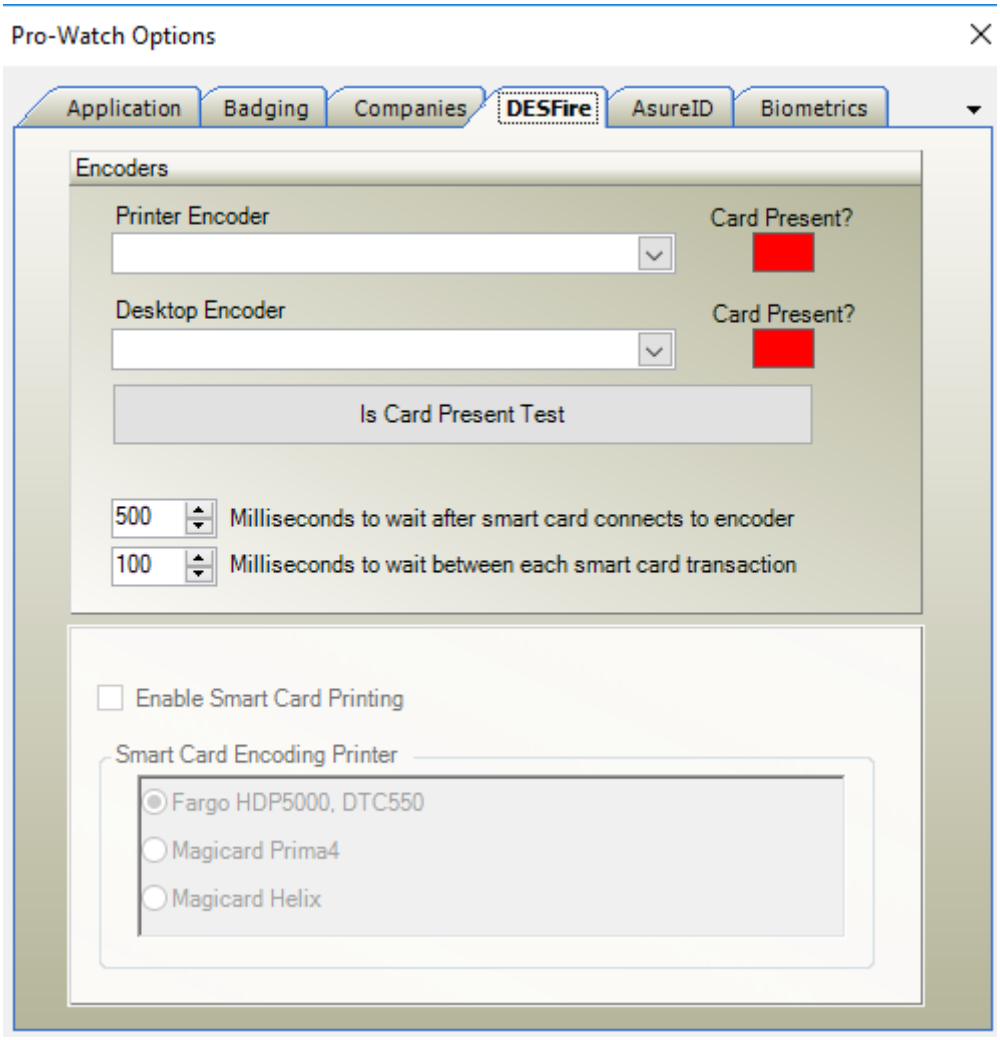
Select **Console > Options > Companies**:



- **Default Company History Days Displayed** — Select the days of company history to be displayed by default from the drop-down menu.
- Click **OK** when done.

2.3.1.5 DESFire

Select **Console > Options > DESFire**:



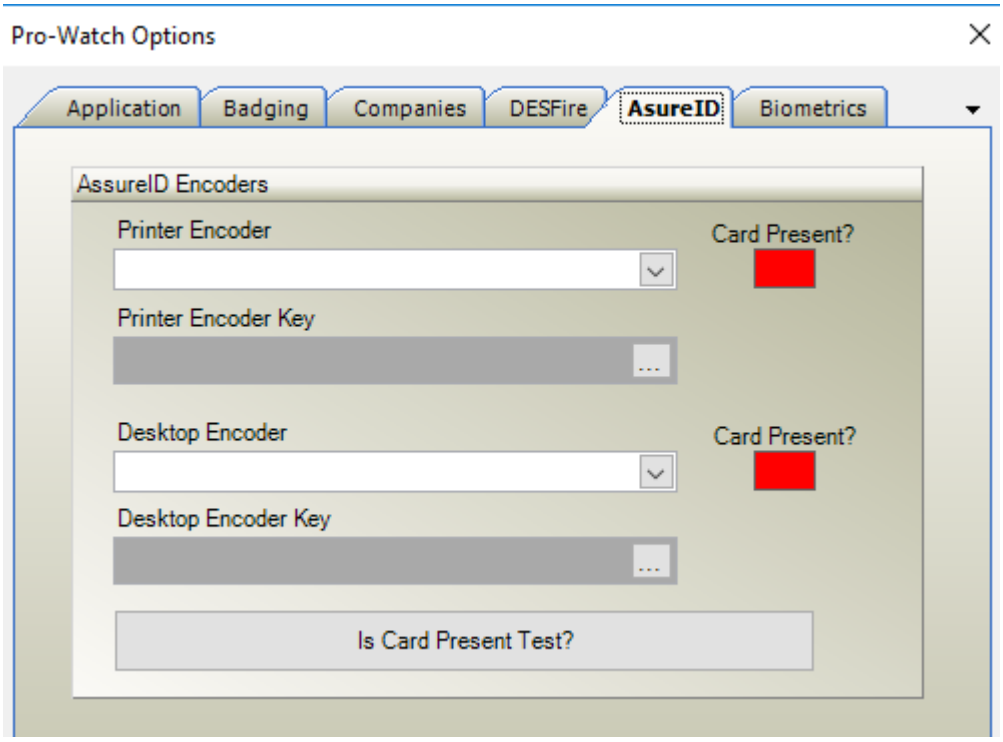
The card encoder and printing devices that are connected to the system will be displayed in the drop-down menus when their drives are installed.

1. Select the appropriate **Printer Encoder** and **Desktop Encoder** from the respective drop-down menus.
2. Click the first combo-box and select in milliseconds the **time to wait** after smart card connects to the encoder.
3. Click the second combo-box and select in milliseconds the **time to wait** in between each smart card transaction.
4. For testing, click the **Is Card Present Test** control button.
5. Select the **Enable Smart Card Printing** check-box for smart card printing. Then select a **Smart Card Encoding Printer** radio-button from the displayed list.

6. Click **OK** when done.

2.3.1.6 AsureID

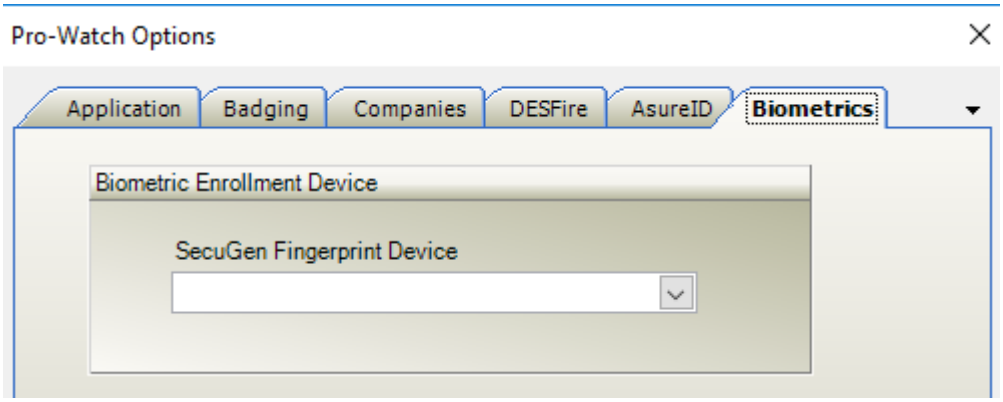
Select **Console > Options > AsureID**:



1. Select the appropriate **Printer Encoder** from the drop-down menu. Browse and select the **Printer Encoder Key**.
2. Select the appropriate **Desktop Encoder** from the drop-down menu. Browse and select the **Desktop Encoder Key**.
3. For testing, click the **Is Card Present Test** control button.
4. Click **OK** when done.

2.3.1.7 Biometrics

Select **Console > Options > Biometrics**:

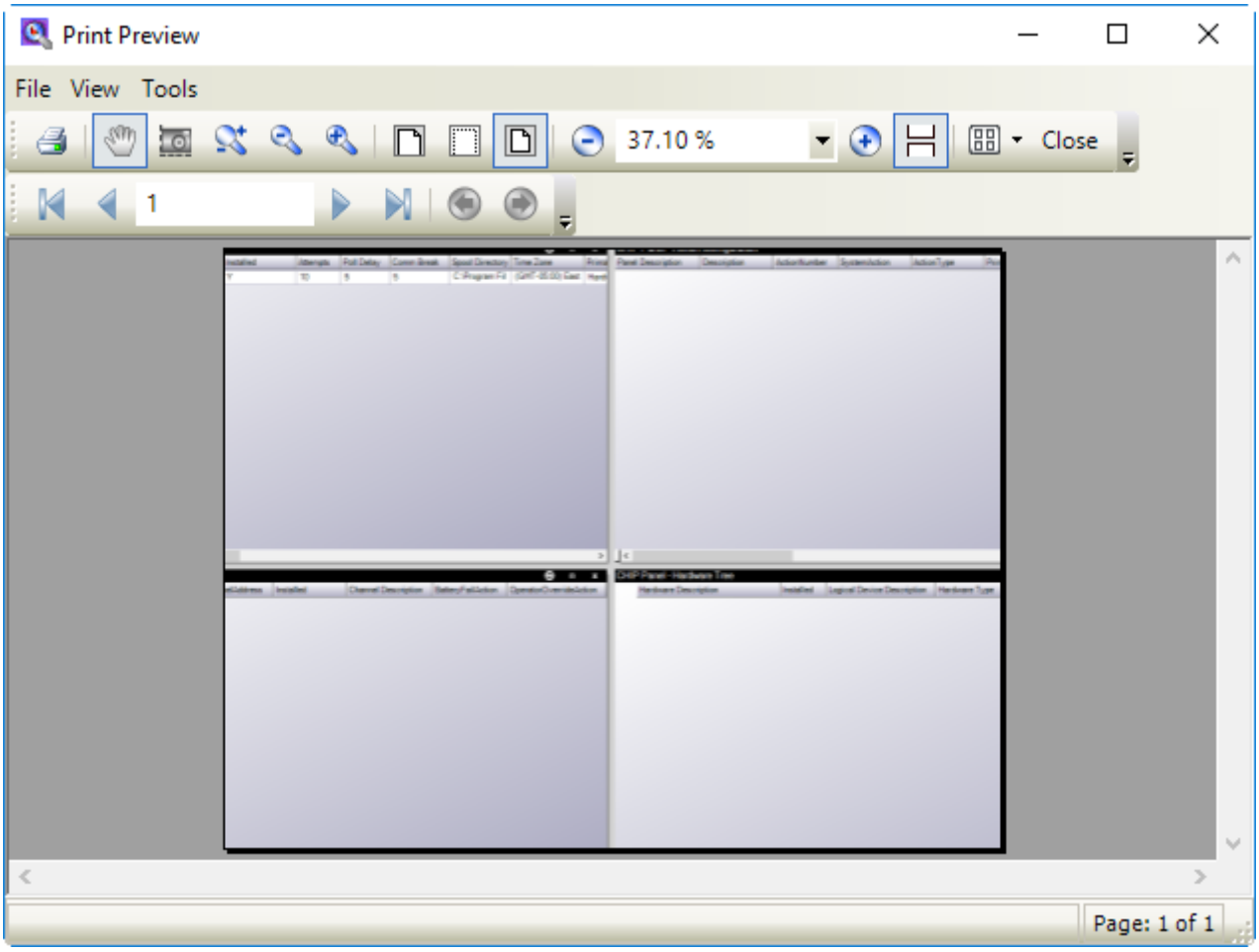


The biometric encoder device that is connected to the system will be displayed in the drop-down menu when its drives is installed.

1. Select the appropriate **SecuGen Fingerprint Device** from the drop-down menu.
2. Click **OK** when done.

2.3.1.8 Print Form

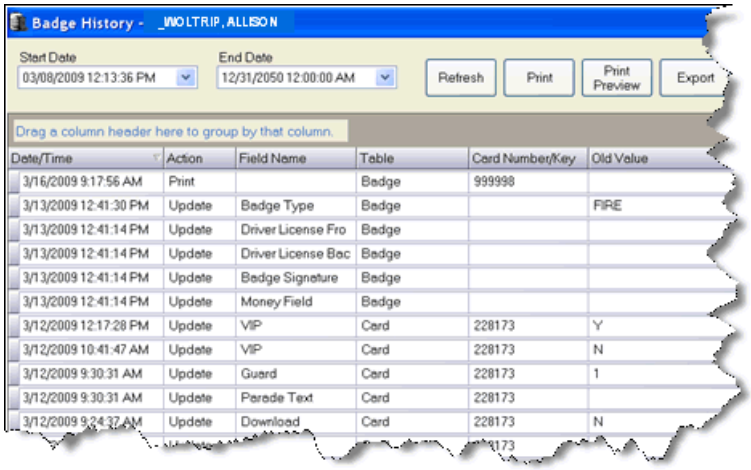
Select **Console > Print Form**:



Print Form option takes a screen shot of the current screen. Make the necessary adjustments to the image by using the tools available in the toolbar and then select **File > Print** to print it.

2.3.2 Badge

2.3.2.1 Badge > Badge History

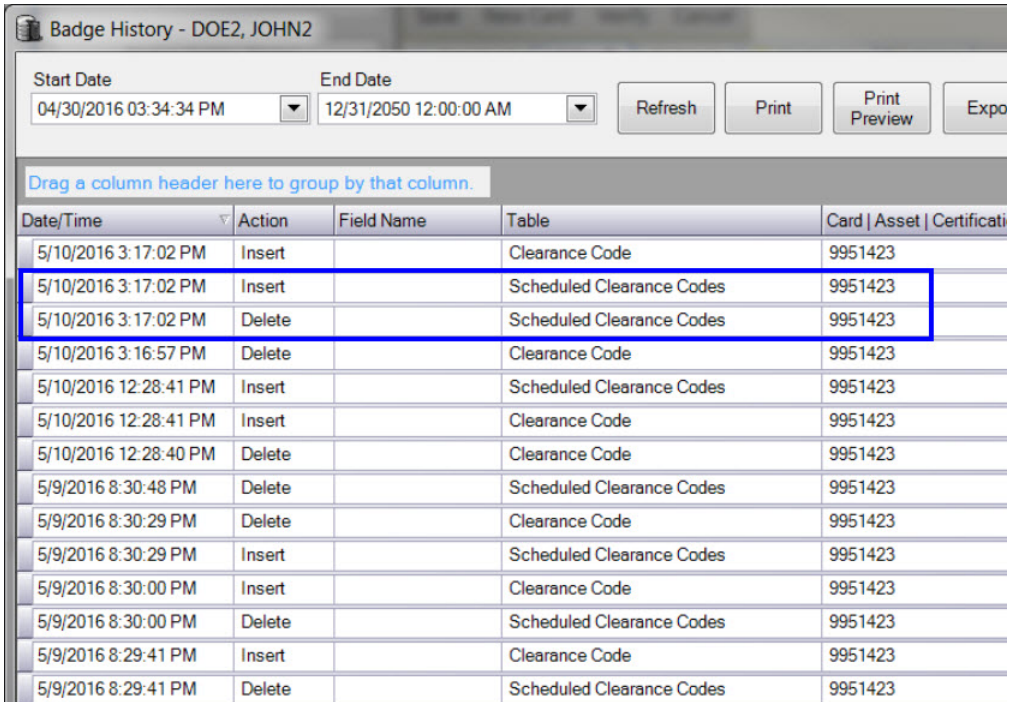


Badge History displays a complete log of all edits made to the selected badge holder record and card information, including **Clearance Codes**, **Logical Devices**, **Card information** and the **printing** of a card.

You can specify a date range for these edits, select the **Refresh** button to retrieve badge transactions for the listed date, print the list (**Print** button), and export the list as an Excel, PDF, XPS, text, or XML file (**Export** button).

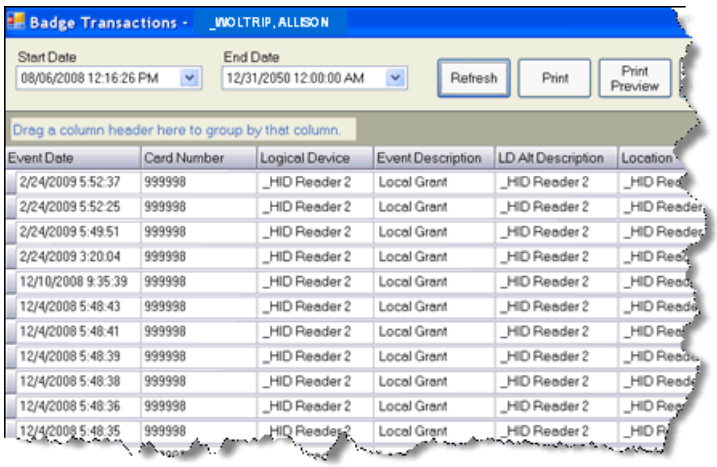
Badge History for Scheduled Clearance Codes

The inserted or deleted scheduled clearance codes will also be displayed in the **Badge History** screen together with the ID of the cards they are assigned to:



For more information on scheduled clearance codes please see the section "Scheduling Clearance Codes" in this chapter.

2.3.2.2 Badge > Badge Transactions



Badge Transactions displays a complete log of all event log transactions generated by the selected badge for given dates. You can specify a date range for these edits, select the **Refresh** button to retrieve badge

transactions for the listed date, print the list (**Print** button), and export the list as an Excel, PDF, XPS, text, or XML file (**Export** button).

Refresh — Refreshes the selected badge to display all recent edits to the badge.

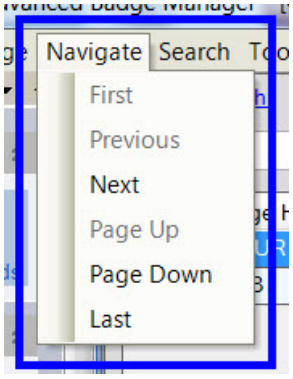
Print Review — Click this button for a print preview.

Print — Click this button to print the badge history.

Fit to Page — Select this check-box to make sure the whole badge history data table will fit to a single page.

2.3.3 Navigate

Select the **Navigate** item on the menu bar to display the navigation options:



First — Displays the first badge in the sorted Badge Holder Name window.

Previous — Displays the previous badge in the sorted Badge Holder Name window.

Next — Displays the next badge record.

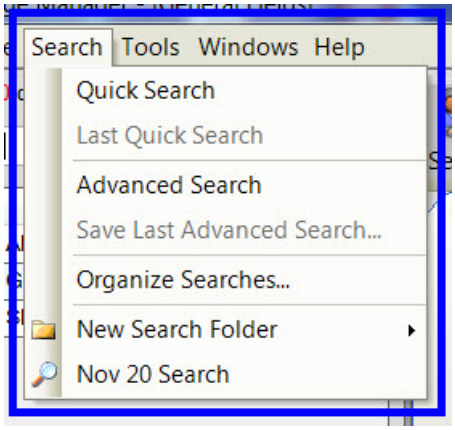
Page Up — Displays, by increment of a page, badge records up the list.

Page Down — Displays, by increment of a page, badge records down the list.

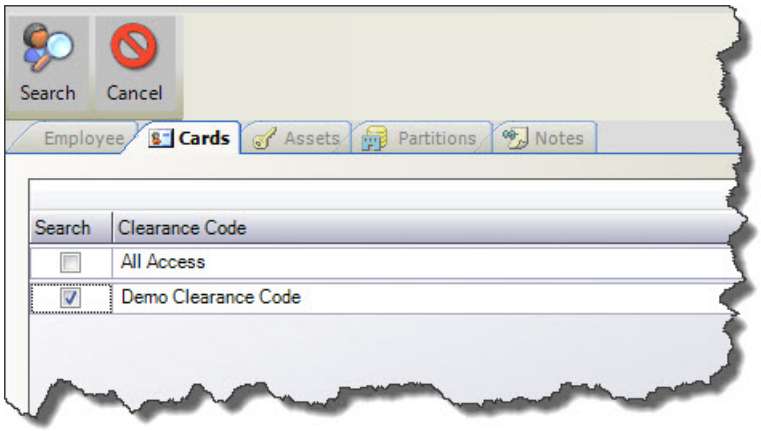
Last — Displays the last badge in the sorted Badge Holder Name window.

2.3.4 Search

Select the **Search** item on the menu bar (and not the one on the badging tool bar) to display the search options:



2.3.4.1 Search > Quick Search



Quick Search performs a simple search by selected Employee, Card, Asset, Partition, or Note field values. The quick search below returns all Cards assigned with Demo Clearance Code.

Last Quick Search — Displays the last Quick Search performed for convenient repeat use.

2.3.4.2 Search > Last Quick Search

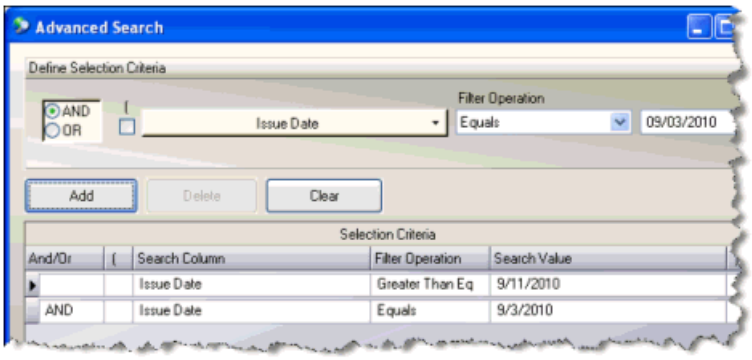
This option displays the very last search performed by the user so that it can be performed again easily, if desired.

2.3.4.3 Search > Advanced Search

Select the **Search > Advanced Search** option on the menu bar (not the one on the badging tool bar) to display this functionality.

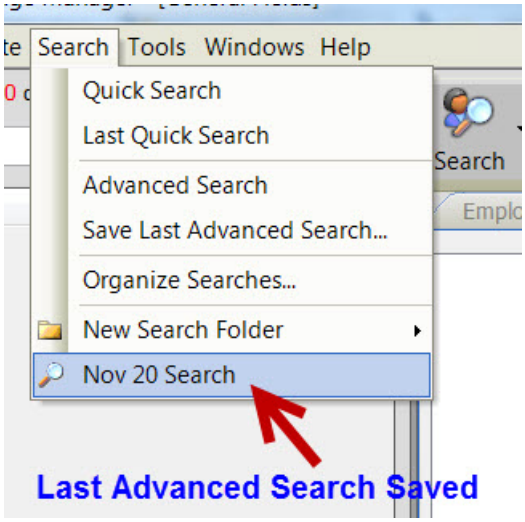
Advanced Search performs a search by any of the full set of fields for the following elements: Badges, Cards, Clearance Codes, Logical Devices, Assets, and Miscellaneous.

You can combine single searches by selecting Boolean operators AND or OR. For example, the advanced search below returns all badges issued on 9/11/2010 or later AND all badges issued on 9/3/2010:



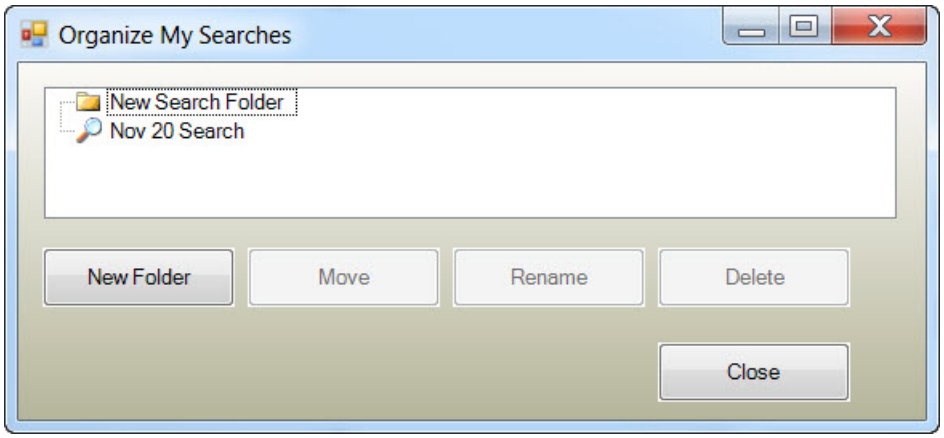
2.3.4.4 Search > Save Last Advanced Search

Save Last Advanced Search, as the name suggests, saves the last advanced search performed. The search thereafter appears as an easy-to-select option in the menu bar Search item:



2.3.4.5 Search > Organize Searches

Organize Searches enables the user to move, rename, or delete a saved search:

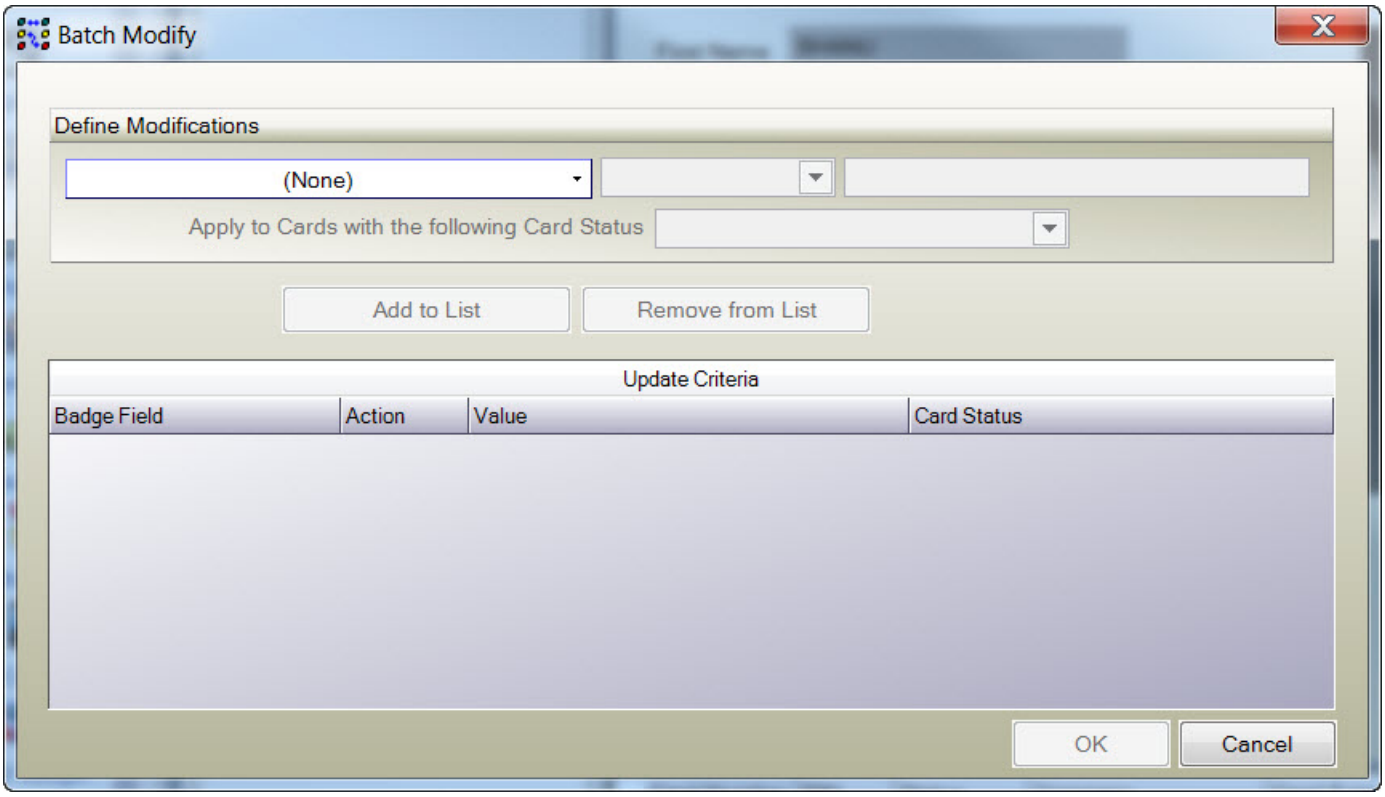


Use this functionality, for example, to organize your favorites in Internet browsers.

You can create a new folder in which to keep your saved searches as well as move, rename, and delete them.

2.3.5 Tools

2.3.5.1 Tools > Batch Modify



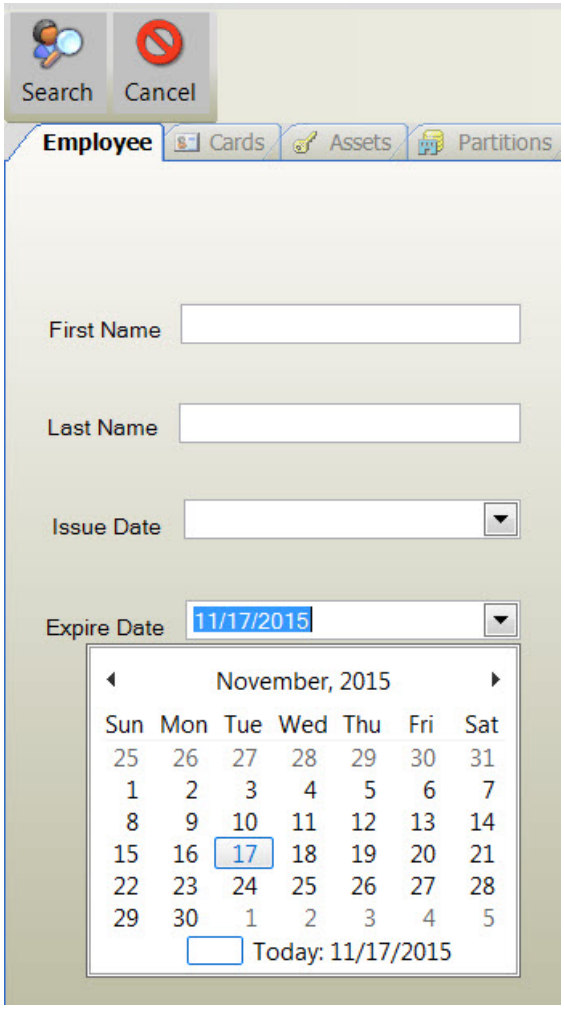
Batch Modify modifies badge or card fields in a large number of badge records.

Note: The Batch Modify function will change the data in the badge holder records for all badge holders listed in the Badge Holder Name list.

Follow these steps:

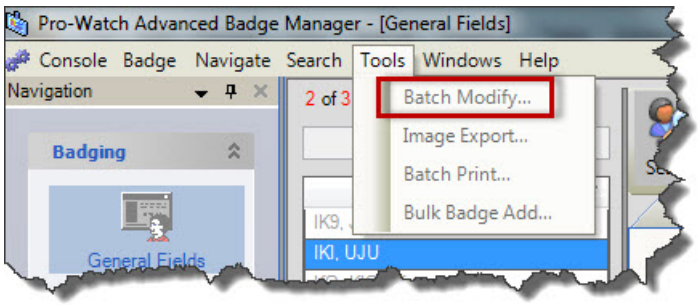
1. Click the **Search** icon at the top of the main screen.

2. Enter or select the badge date upon which you want to search. The example below shows a search for all badges expiring on November 17, 2015:



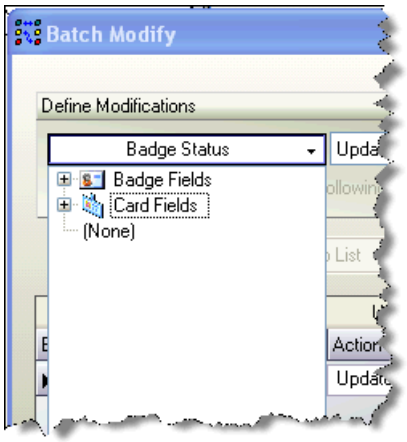
3. Click the **Search** icon again at the top of the above screen. Pro-Watch Advanced Badge Manager returns the list of badge records meeting the search criteria.

4. Select **Tools > Batch Modify**:

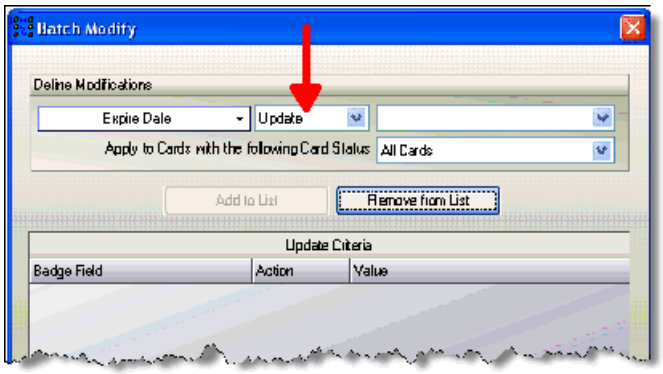


5. At the Batch Modify screen, define your modifications.

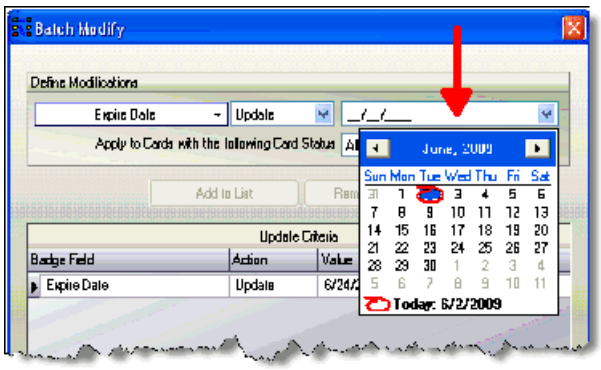
   a. Click the Badge Status button to display the Badge Fields and Card Fields trees:



6. Select the first field to modify.
7. In the next field, select the appropriate action you want to perform on the Badge or Card field:



8. In the third field, select the appropriate value from the drop-down list:



9. In the Apply to Cards with the Following Card Status field, select the appropriate value.
10. Click **Add to List** to add the modification to the Update Criteria list.
11. Repeat steps 6 through 11 until all modifications to the selected badge records are listed in the Update Criteria list.
12. Click **OK** at the bottom of the Batch Modify screen to execute the modifications. When **Batch Modify Progress** screen displays, click **Start** to continue.

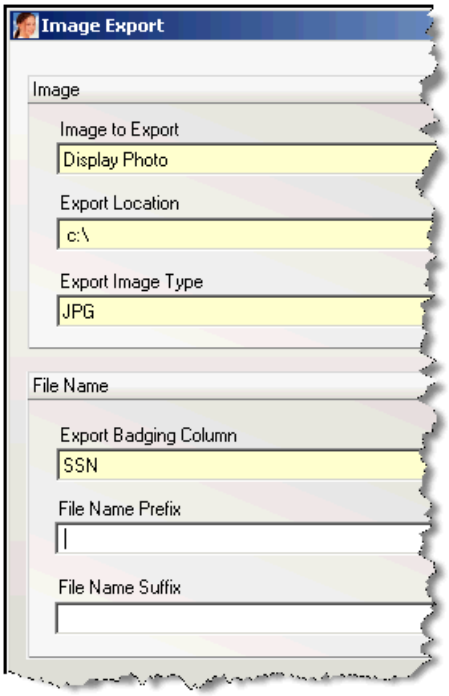
2.3.5.2 Tools > Image Export

Image Export exports a Pro-Watch image (for example, a photo ID, fingerprint, etc.) to another machine in the enterprise where there may be another use for the image. Image Export uses any badge field as a naming scheme. For example, if the employee number and badge photo are two fields captured on the badging forms, a badge operator can use Image Export to export all photos in the database to individual files in the form of 'EmployeeNumber.jpg.'

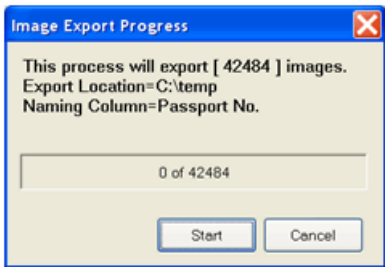
Follow these steps:

1. Search for the badge holder for whom you want to export images.
   a. In the Pro-Watch Advanced Badge Manager main screen, click the **Search** icon at the top of the screen. The Employee tab appears.
   b. Enter the employee search criteria, and click the **Search** icon again. The Badge Holder Name list displays the badge holders retrieved by the search.

2. Select **Tools > Image Export**. The Image Export dialog box appears:



3. Use the drop down lists and browse button to select the image to export, the export location, and the export image type (JPG, TIFF, or BMP). Use the export badging column to uniquely define the file name. The example above uses the Social Security number to create a unique file name.
4. Click **OK** to display the Image Export Progress box that will report the progress of the export:



5. Click **Start** on the Image Export Progress box to export the images.

2.3.5.3 Tools > Batch Print

Adds batches of cards to the Batch Printing queue. You can print by Card Status, Company, and Issue Date. Follow these steps:

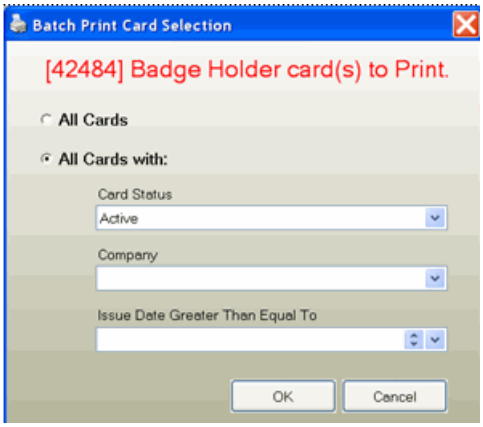
1. Search for the badge holders whose card(s) you want to print.

a. In the Pro-Watch Advanced Badge Manager main screen, click the **Search** icon at the top of the screen. The Employee tab appears.

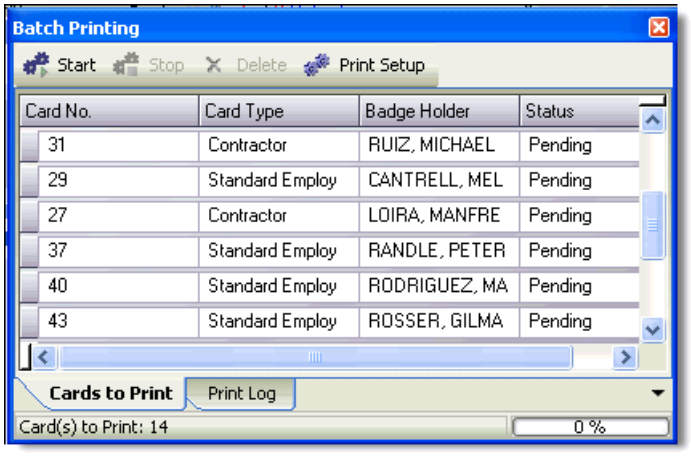
b. Enter the employee search criteria, and click the **Search** icon again. The Badge Holder Name list displays the badge holders retrieved by the search.

2. Select either **All Cards** or **All Cards with**:
   - **All Cards** adds all cards for each badge to the Batch Printing queue.
   - **All Cards with** allows you to select cards by their Card Status, Company, and Issue Date, and add them to the Batch Printing queue.

3. Select **Tools > Batch Print** to display the Badge Print Card Selection dialog box:



4. Click **OK** to compile the Batch Printing queue:



Note: From this screen, you can remove individual cards from the queue. Click to highlight the card and click the **Delete** button at the top of the box.

5. Click **Print Setup** to specify the printer and printer type. You can also re-set the horizontal and vertical alignment, magnetic stripe encoding,

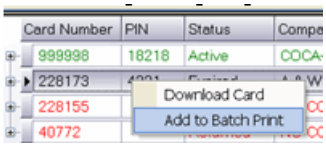
page orientation, page size, and whether to print on both sides of the paper sheet.

6. Click **Start** to start printing the cards listed in the Batch Printing queue. If for any reason you want to stop the printing, click the **Stop** button at the top of the box. Click **Delete** if you want to delete the card from the printing queue.

You can monitor the printing process events on the Print Log tab at the bottom of the box. The log reports when a card is added to the queue and when a card is printed. A printed card appears in green.

Note: You can also add cards to the Batch Printing queue in the following ways:

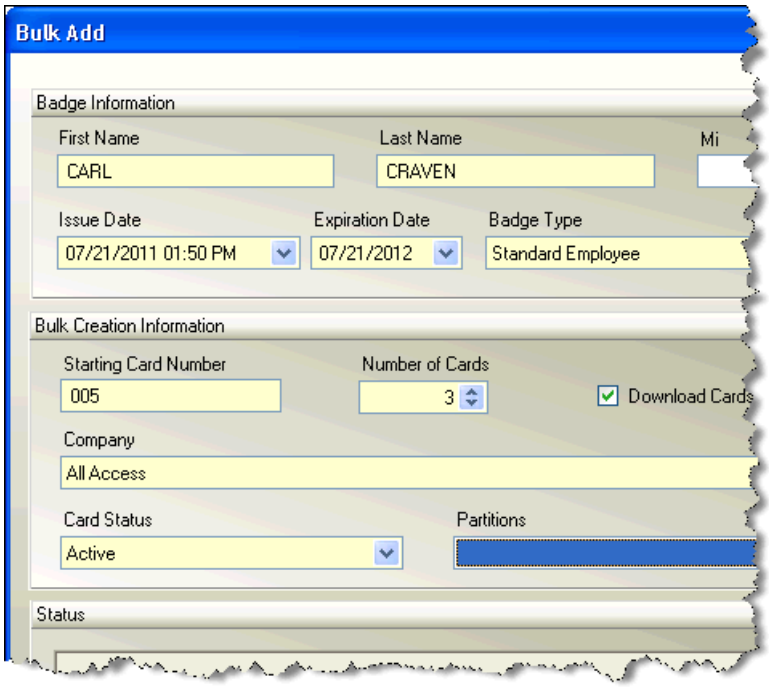
- In the Badge Holder Name list on the Pro-Watch Advanced Badge Manager main screen, right-click the badge holder for whom you want to print a card. Select **Send to Batch Print**. The Batch Print Card Selection dialog box appears. Select either **All Cards** or **All Cards with**. Click **OK** to add the card to the Batch Printing queue.
- In the card panel at the bottom of the main screen, right-click the card you want to add to the queue and select **Add to Batch Print:**



- In the card panel at the bottom of the main screen, drag and drop the card you want into the Batch Printing dialog box.

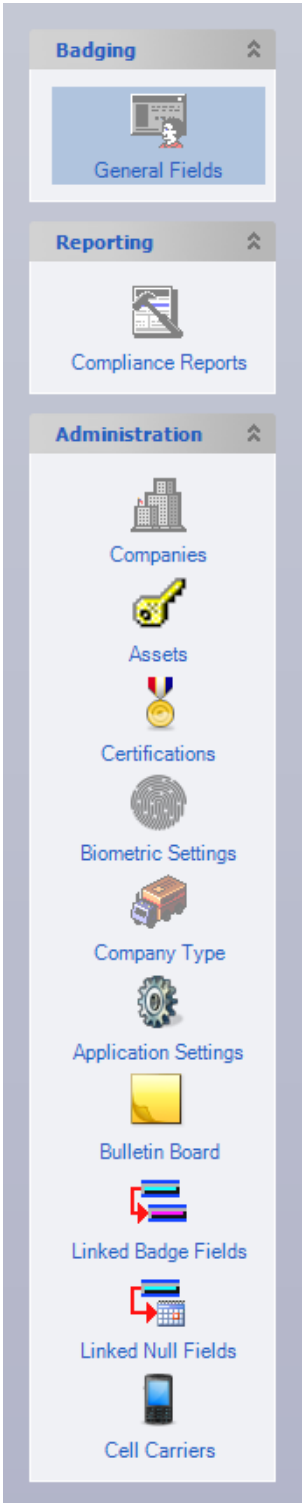
2.3.5.4 Tools > Bulk Badge Add

Bulk Badge Add creates multiple cards for a badge with one operation. The example below creates three cards, beginning with card number 005:



2.3 Using the Navigation Pane

From the Navigation pane, you can select badging, administrative, or reporting applications.



Badging General Fields — Creates and maintains badges and cards.

Reporting — Configures and runs compliance reports from the Badge Manager or card transaction records.

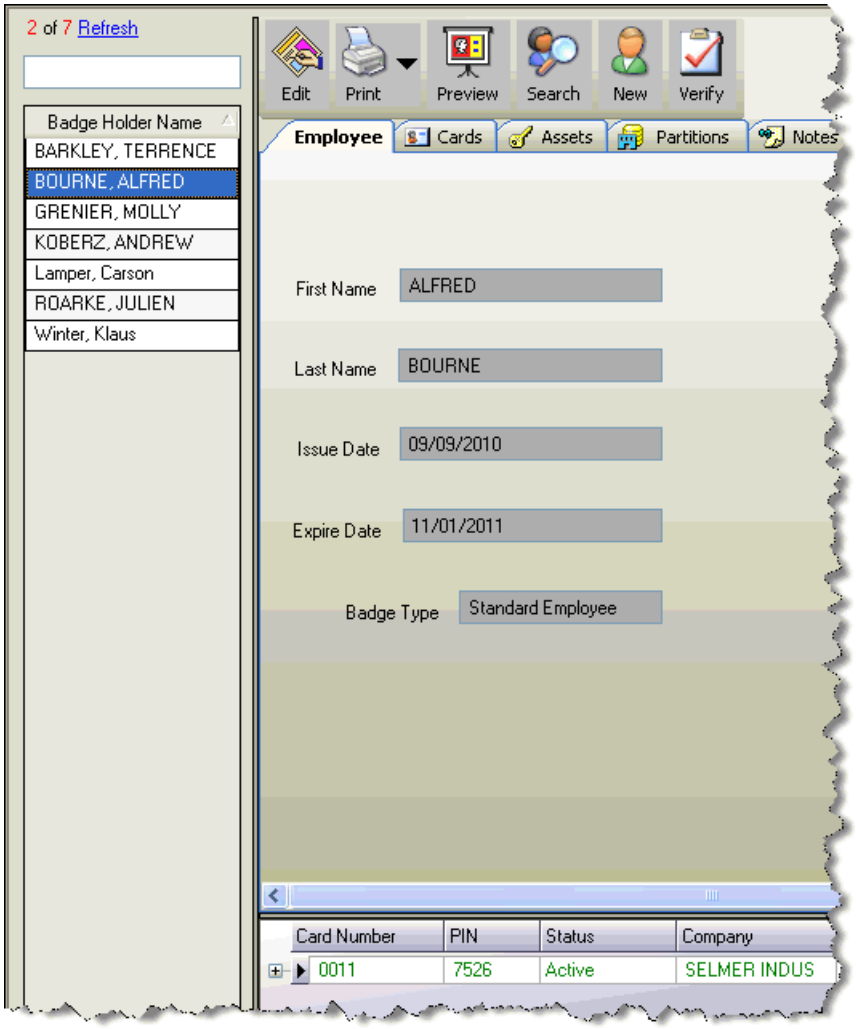
Administration options:

- **Companies** — Creates and maintains the list of companies whose employees you badge.
- **Assets** — Adds new assets to the assets list.
- **Certifications** — Adds new certifications.
- **Biometric Settings** — Offers controls to add, detect, and delete biometric terminals.
- **Company Type** — Specifies company types of company data elements that will be available in the Pro-Watch database for identity checks.
- **Application Settings** — Sets the Card Tab position, the casing (upper case or mixed case) on the Badging screen, enable Pro-Watch/Morpho Biometrics using an MSO300 enroller, display e-docs in Company/Employer module, copy PIN code when copying a card, and copy biometric PIN code when copying a card.
- **Bulletin Board** — Posts miscellaneous posts to the bulletin board.
- **Linked Badge Fields** — Links two badge fields of type “Drop Down” and /or “Resource” (Badge Type, Company, Badge Status). If the Primary field is set to a primary value, the secondary field will be automatically filled with the secondary value.
- **Linked Null Fields** — Links two badge fields. If the Primary field is NOT null, the Secondary field must NOT be null in order to save the badge record. An error will display if a user tries to save the badge record and the criteria is not met.
- **Cell Carriers** — Adds new cell carriers with text message addresses.

2.3.1 Using the Badging Screen

Click the **General Fields** button in the Navigation panel to display the Pro-Watch Advanced Badge Manager main screen:

Figure 2-3 Pro-Watch Advanced Badge Manager Badging Screen



The Pro-Watch Advanced Badge Manager screen opens with a list of all badge holders in the left (Navigation) panel. Badge profiles appear in the right panel. To add or edit badges, use one or more of the tabs in this panel which can all be configured in Pro-Watch. Note that the term “Assets” refers to what was formerly called “Brass Keys.”

Note the following:

- The card configuration for the displayed badge holder appears in the bottom-right panel. Click the card number to expand and display the card’s assigned Clearance Codes and Logical Devices. Logical Devices and cards are active when they appear in green and inactive when they appear in red.

- You can edit a badge record only by first clicking the **Edit** toolbar button, and all edits are saved only when you click the **Save** toolbar button.
- To clear a field, click the field label.
- Fields in yellow are required entries for a valid badge record. Fields in pink are required to print a card.
- You can apply formats to fields such as phone numbers and Social Security numbers.
- The status bar at the screen's bottom uses the following status keys:
  - **PWS**—Pro-Watch Server
  - **PWD**—Pro-Watch Database
  - **Wrkst**—workstation name
  - **User**—user who is currently logged in

Note: You can use the Pro-Watch Badge Builder utility to create or revise the Badge Manager screen. See the *Pro-Watch Software Suite Guide* for details.

The following table describes the toolbar icons at the top of the Badge Manager screen:

Table 2-1 Pro-Watch Advanced Badge Manager Toolbar Icons

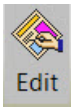
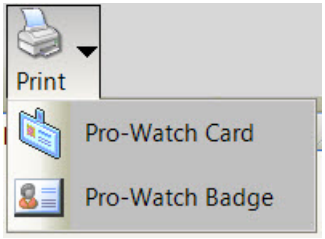
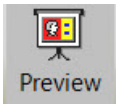
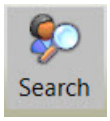
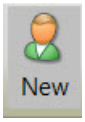
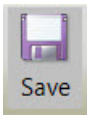
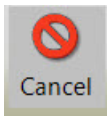
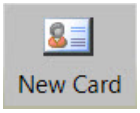
Icon	Description
	**Edit**—Activates the badge tab's fields and enables you to edit them.
	**Print**—Prints either the badge holder's badge or card data.
	**Preview**—Displays a preview of the print request.

Table 2-1 Pro-Watch Advanced Badge Manager Toolbar Icons (continued)

	**Search**—Enables you to search for and display badges by first name, last name, issue date, expiration date, or badge type. You can enter new search criteria, or you can select "Last Search" to search by the previous criteria entered.
	**New**—Creates a new badge.
	**Save**—Saves the edits made on the current badge tabs.
	**Cancel**—Cancels the current badging operation.
	**New Card**—Creates a new card for the current badge.

2.4 Adding a Badge

This procedure adds a badge from the Employee tab of the Pro-Watch Advanced Badge Manager main screen.

To add a new badge from the Employee tab:

1. Click the **New** icon at the top of the screen to display by default the **Employee** tab of a new badging window.
2. Enter the badge holder's first and last names, the issue date and expiration dates of the badge, and select the badge type.
3. Capture or import a badge holder photograph. To do this, you will either need a Twain device configured in Pro-Watch and connected to the Pro-Watch machine you are using, or a photo already stored in the Pro-Watch database. Follow these steps:

   a. Click the **Click Here to Capture** box to display the Capture Photo screen.

   b. If you are capturing a photograph of the badge holder with a Twain device:

   – Click **Select Source** and select the device.
   – Click **Acquire** to photograph the badge holder. The Twain device then reverts to Pro-Watch Advanced Badging and the photograph appears on the screen with a selection box that identifies the current cropping setting.
   – Use the Cropping Width and Height fields to adjust the cropping as desired.
   – Click **Print Image** to print the photograph.
   – Click **OK**.The image should now appear on the Badge tab.

   c. If you are importing an image from an existing file:

   – Click **Import from File** and select the file.
   – Use the Cropping Width and Height fields to adjust the cropping as desired.
   – Click **Print Image** to print the photograph.
   – Click **OK**. The image should now appear on the Badge tab.
   – Click **Save**.

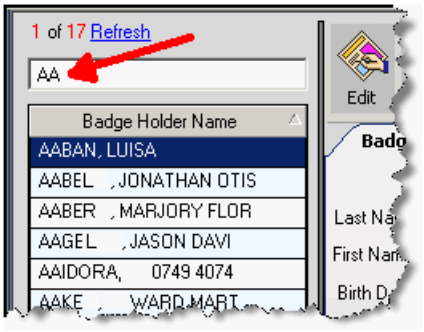
2.5 Editing a Badge

To edit an existing badge, first search for and select the badge holder from the badge holder list in the left panel. Follow any of the search methods described below.

2.5.1 Searching for the Badge

Searching for the Badge

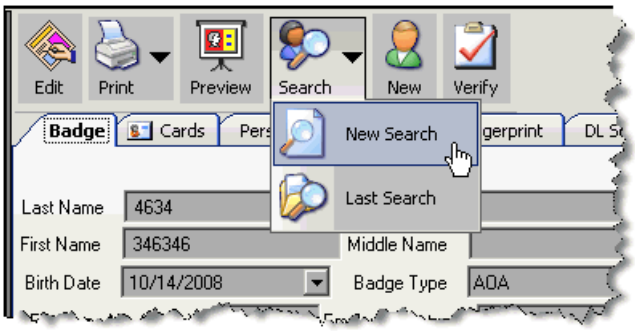
To find a single badge by searching on the badge holder's name, you can use the Badge Holder Name window. Enter the name in the search field:



You can also search for badge holders by searching on a particular field in their badge or card records. When you click the Search icon on the toolbar, all fields on all of the badge record tabs become "search-active." That is, you can enter a value in any of these fields and search on that value. You can search by first name, last name, issue date, expiration date, or badge type.

Follow these steps:

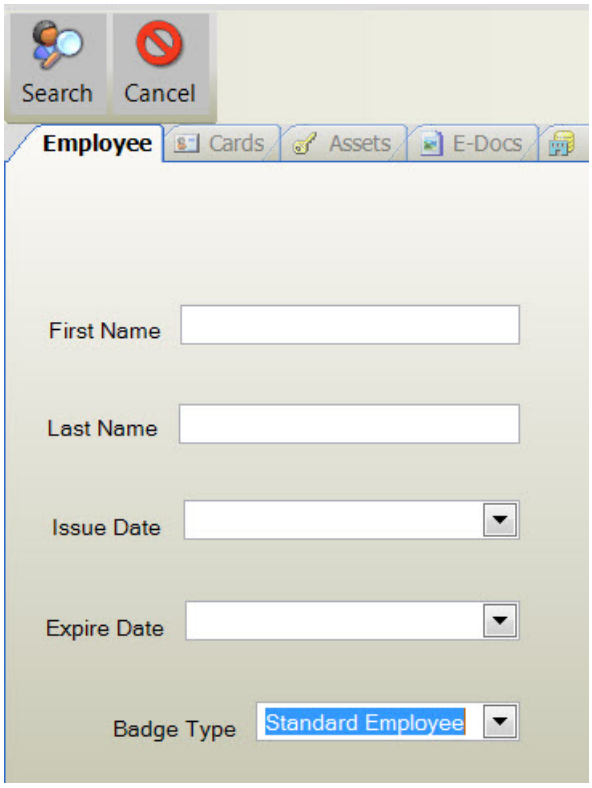
1. Click the **Search** icon from the function icon toolbar:



If you select **New Search**, an empty set of Badging tabs appears.

2. In the appropriate tab, enter or select the field value by which you want to search and then click the **Search** button. In the figure below,

for example, the search will retrieve all badge holders who have the "**Standard Employee**" badge type.



3. Click the **Search** icon in the upper left corner. All badge holders with "**Standard Employee**" badge types are listed in the adjacent Badge Holder Name window.

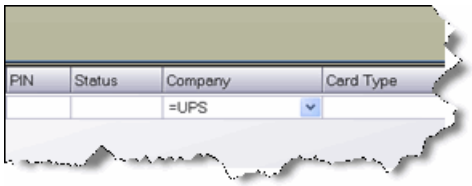
   Note that when you enter more than one search criterion, the search function "ANDs" together all of the entered fields and returns the names of all LIKE badge holder found. For example, if you search for a last name of "COCA," the LIKE search finds all last names that *start* with "COCA."

   Note, too, that you can use comparison operators to search. You can enter the operators in a text field, a numeric field, or a drop-down field. Use the following operators:

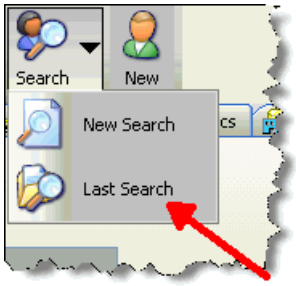
Operator	Description
=	Equal to
!= or <>	Not equal to
>	Greater than
<	Less than

Operator	Description
>=	Greater than or equal to
<=	Less than or equal to
%	Contains (not operative in numeric fields)

For example, if you enter “UPS” in the Card Company field, the search returns records that not only show “UPS” in the Card Company field, but also “like” entries such as “UPS Ground.” But if you enter “=UPS” in the Card Company field (as shown below), the search returns records that have only “UPS” in the Card Company field.



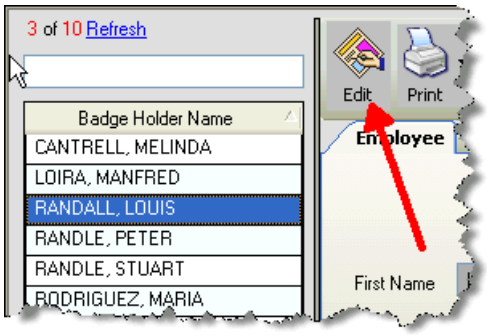
Note: After performing a search, you can re-run the same search without having to re-enter the search criteria. Click the drop-down arrow on the **Search** button and select **Last Search** (see the image below). All of the last search’s criteria appear in the search record. From here, you can also add to the displayed criteria to refine the search.



2.5.2 Editing the Badge

Follow these steps:

1. Click the **Edit** button on the toolbar. The badge record's fields all become active.



2. Make the desired changes in any of the record's fields.
3. Click the **Save** button on the toolbar. Note that the changes you make will not be saved until you click the **Save** button.

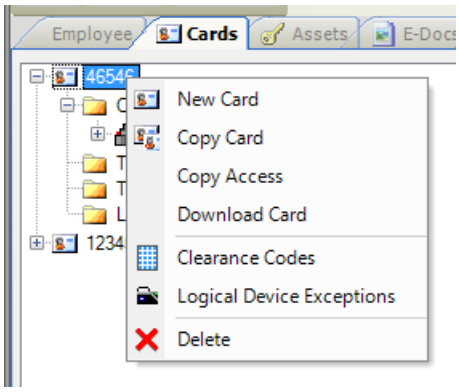
2.6 Adding a Card

Note: A single badge holder can be given multiple cards. A card is the actual plastic piece that the badge holder presents to a reader to gain access to your facility. A badge identifies the person, and the person's card (or cards) provide that person access. Some badge holders may need only a few cards; others may need many.

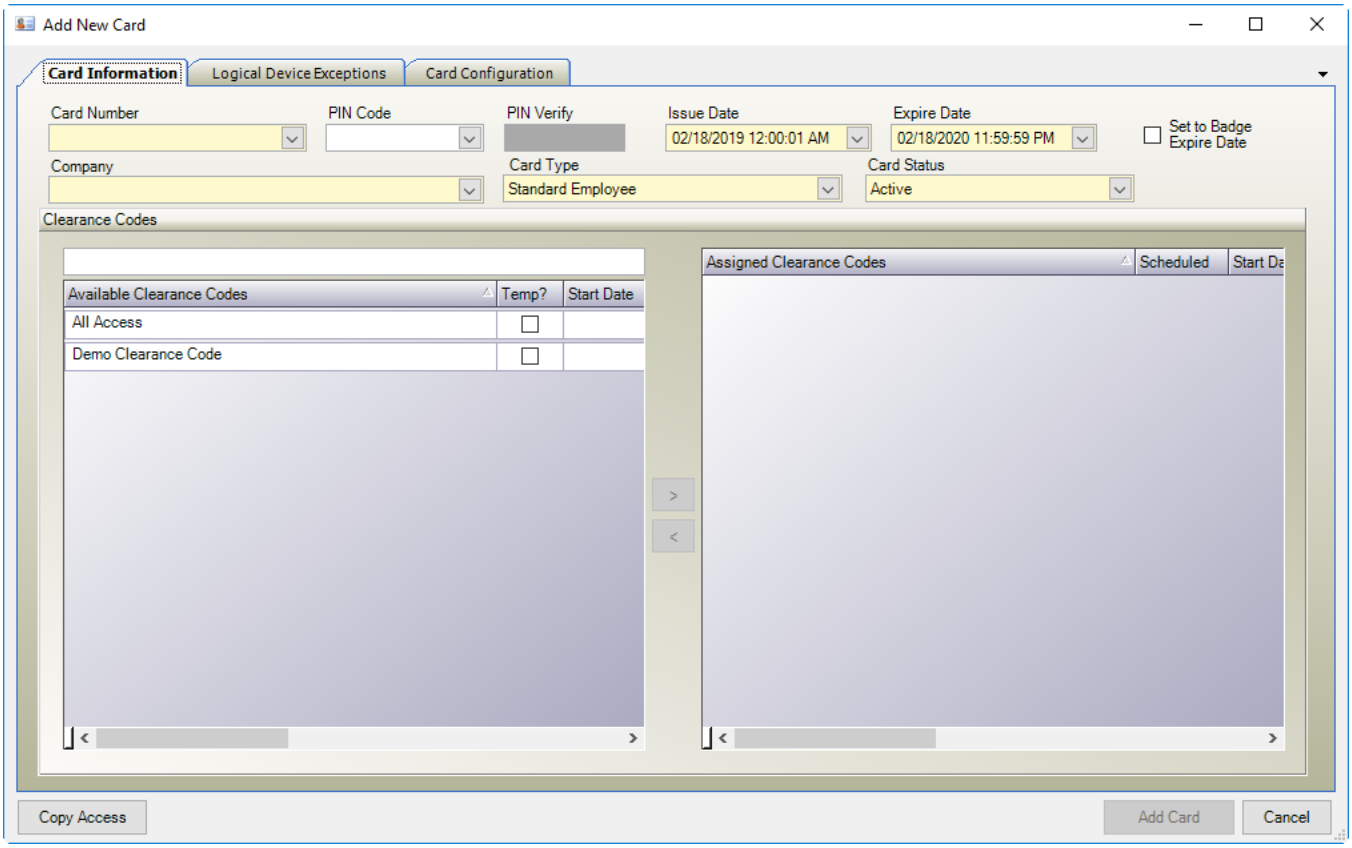
To add a new card to a badge:

1. Select the badge holder from the badge holder list in the left panel (or click the **Search** icon at the top of the screen and search for the badge holder) to display the Employee tab and the badge holder's record.
2. Click the **Edit** icon at the top of the screen.
3. Either:

a. Right-click in the Card (lower-right) panel and select **New Card**:



b. Or, click the **Cards** tab and click the **New Card** icon at the top of the screen. The **Card Information** tab of **Add New Card** screen appears:



4. Use the descriptions in the following table to select the appropriate values for the fields at the top of the tab. The yellow-highlighted fields are required.

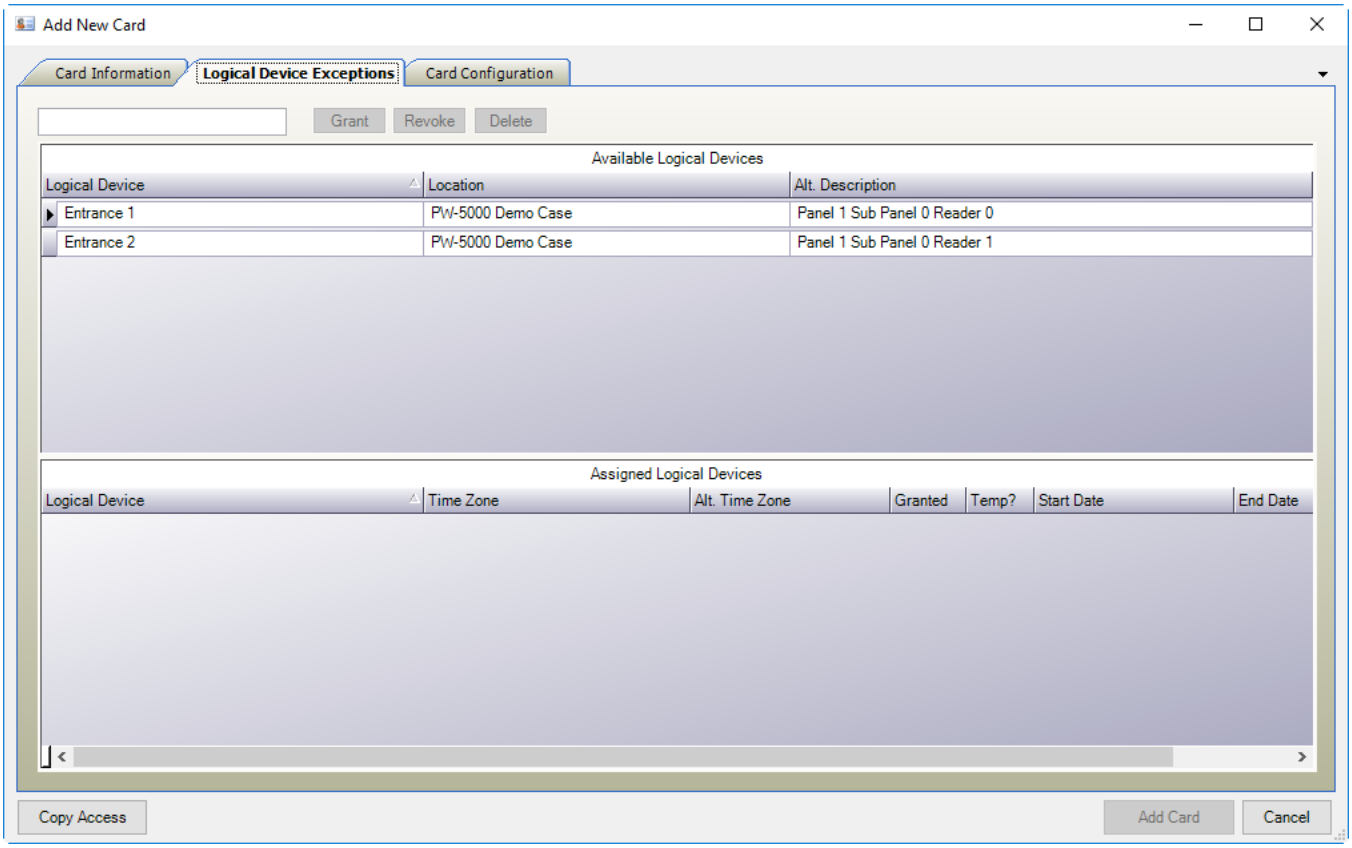
Field	Description
Card Number	A unique number identifying the card. If this field is grayed out, the card number is automatically generated from seed information derived from Pro-Watch setup parameters. If this field is not grayed out, enter a unique number. Pro-Watch Advanced Badging verifies the number's uniqueness.
PIN Code	The Personal Identification Number. You can either enter or automatically generate a number. To automatically generate the number, click the Generate PIN Number button.

Issue Date	The date and time the card will be effective. This date can be now or any time in the future.
Expire Date	The date the card expires. By default, this date is one year from the current date and time. Click the down arrow to select a new expiration date, or click "Never Expire." Note that you can also manage the expiration date by customizing the Company configuration in Pro-Watch.
Company	The Pro-Watch Company database element assigned to the card. See Chapter 7 of the *Pro-Watch Guide* for information about configuring the Pro-Watch Company. The Company configuration in Pro-Watch determines the default Clearance Codes and the expiration date assigned to the Pro-Watch Advanced Badging card. Note that you can pre-set the Company by creating a custom company resource badge field named BADGE_V.COMPANY1.
Card Type	The badge type of the card. The Card Type is derived from the Badge Type selected on the Pro-Watch Advanced Badging main screen.
Card Status	Select a Card Status from the drop-down menu options: Active, AutoDisable, Disabled, Expired, Lost, Stolen, Terminated, Unaccounted, Void.

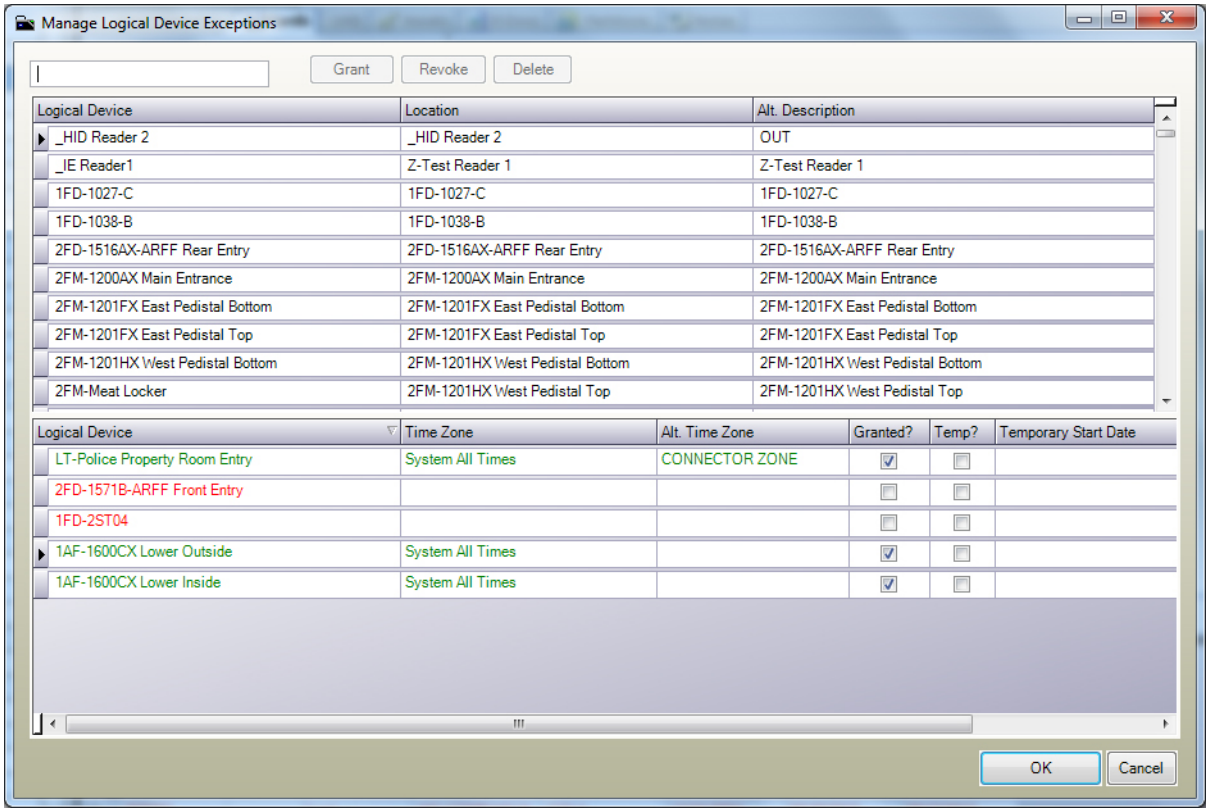
5. **Assign Clearance Code(s)** to the card. A Clearance Code grants or denies badge holder access to designated enterprise doors and elevators. In addition, you can define temporary Clearance Codes that are valid for a given number of days to support contractor work at your facilities, for example. Pro-Watch Clearance Codes are defined in the Pro-Watch Database Configuration application. See *Pro-Watch User Guide* for instructions.
6. The available **Clearance Codes** appear in the bottom-left pane. Click to highlight the desired Clearance Code, then click the right arrow to move the Clearance Code to the bottom-right pane.

   Note the search field above the list of available Clearance Codes. When you type the name of a Clearance Code in the field, Pro-Watch Advanced Badging automatically searches the Available Clearance Codes list and highlights that Clearance Code.

7. Click the **Logical Device Exceptions** tab to associate Logical Devices to this card.

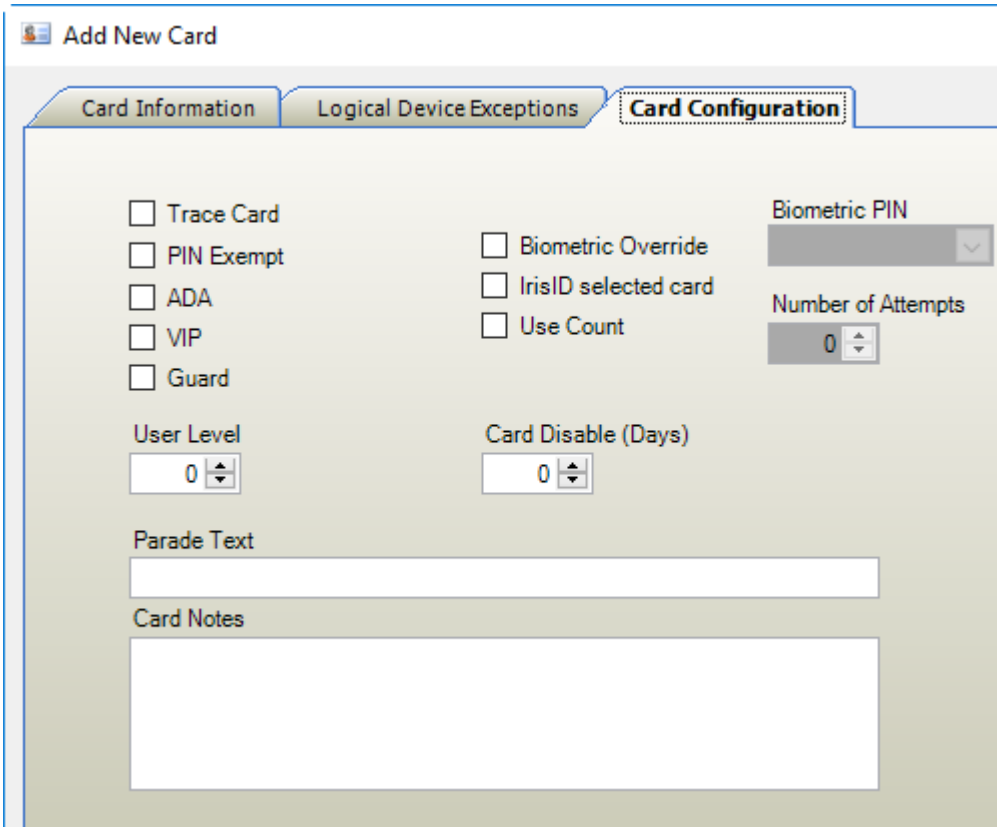


DEFINITION: A **Pro-Watch Logical Device** refers to an input device (such as a card reader) or an output device that is configured in Pro-Watch to control access at a point (such as a door). Logical Devices for your facility have already been configured in the Pro-Watch Hardware Configuration application. You see in the figure below, for example, the configured devices in the **Available Logical Devices** box.



8. The **Logical Device Exceptions** tab enables you to grant, revoke, or delete card access to Logical Devices. The dialog box has two panes: the **top pane** lists the Logical Devices that are available to the card, and the **bottom pane** displays the Logical Devices that are already assigned to the card. Logical Devices displayed in **green** are currently granted to the card, and those displayed in **red** are currently revoked from the card.
9. Note the search field at the top-left of the dialog box. When you type the name of a Logical Device in the field, Pro-Watch Advanced Badging automatically searches the Available Logical Devices list and displays the device listing.
10. Grant, revoke, or delete Logical Devices for this card. To do this, highlight the Logical Device and click either the **Grant**, **Revoke**, or **Delete** button.
11. Choose whether to make the device assignment active indefinitely or only temporarily. To make it active indefinitely, leave the **Temp?** check box deselected. To specify a limited period of activity, select the **Temp?** check box and enter the start and end dates in their respective fields. Note that if the logical device appears in green, it is still active. If the device appears in red, its active association with this card has expired.

12. Click the **Card Configuration** tab to configure various options for the card:



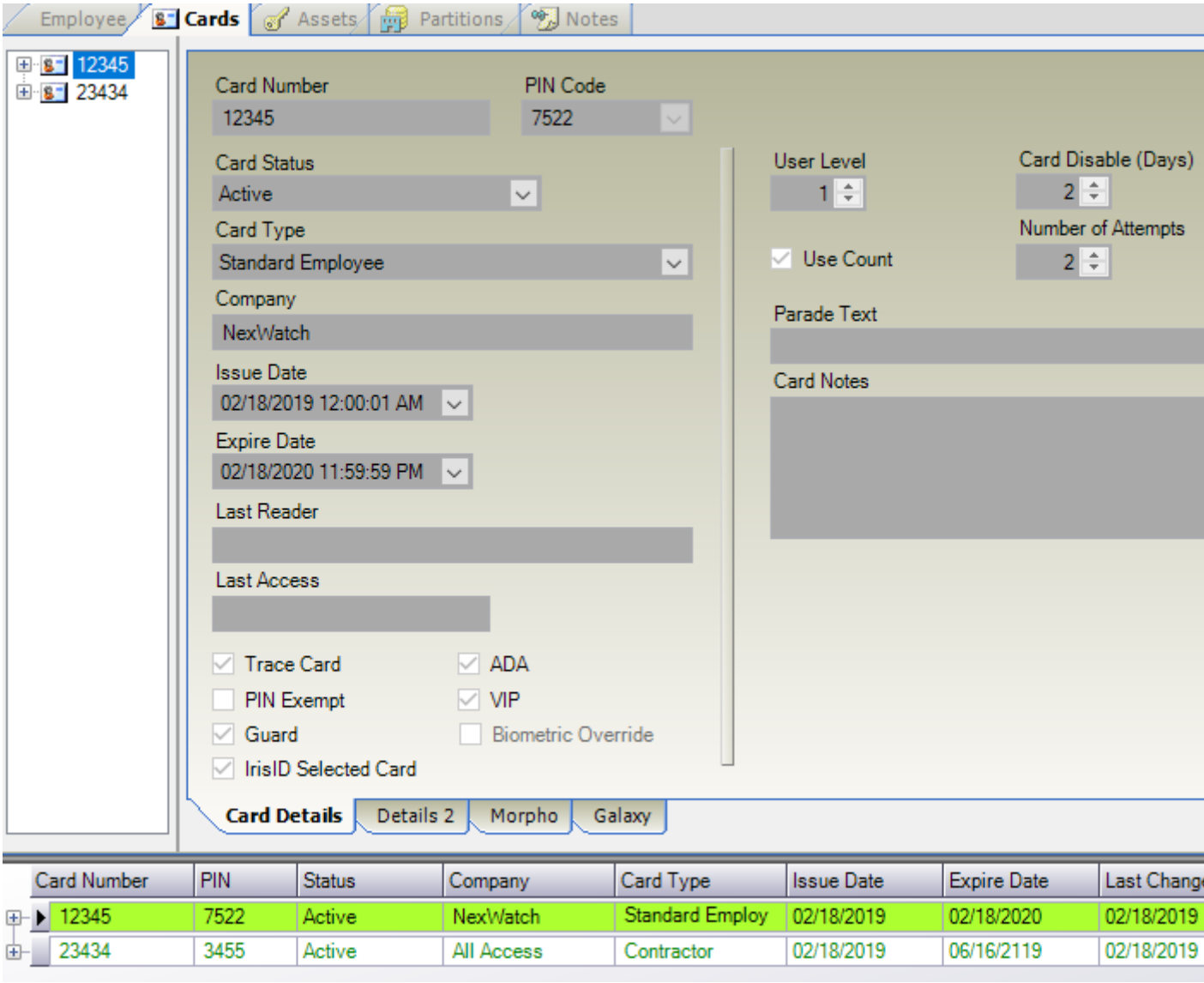
13. Select one or more of the following options by clicking their respective check-box: Trace Card, PIN Exempt, ADA, VIP, Guard, Biometric Override (enter Biometric PIN is selected), IrisID Selected Card, Use Count.

    Note: Selecting the **IrisID Selected Card** check-box configures that specific card as the only card number that would download to the panel when the IrisID reader is used.

14. Select **User Level**, **Card Disable (Days),** and **Number of Attempts** from their respective spin boxes.
15. Enter **Parade Text** (if any), and **Card Notes** (if any).
16. After you have added all **Clearance Codes** and **Logical devices** to this card and set the **Card Configuration**, click **Add Card** to add the Card to the badge record.

2.7 Editing a Card

1. Click the **Cards** tab on the Badge screen to view the Cards you have created. You will use this tab to quickly identify a badge holder's Cards and all of its Clearance Codes and Logical Devices. By default you'll be looking at the **Card Details** sub-tab:



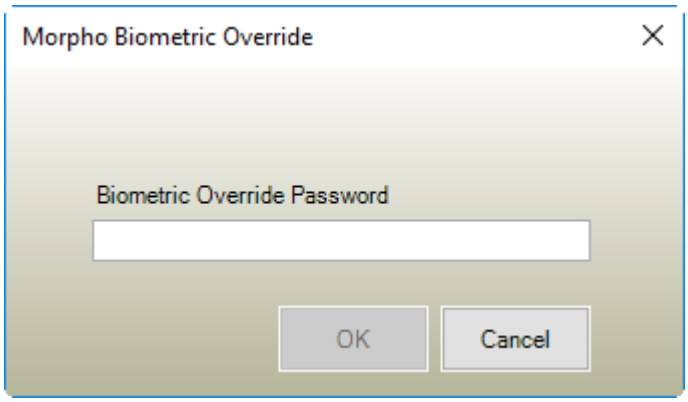
2. Click the **Edit** button on the toolbar to render all the card fields editable.

3. Follow the directions to edit the individual fields and/or check-boxes in the **Card Details** sub-tab:

   - **Card Number** — This field is populated automatically by Pro-Watch.

- **PIN Code** — Either type in one yourself or select the "Generate Random PIN" option from the drop-down menu.
- **Card Status** — Select a Card Status from the drop-down menu options: Active, AutoDisable, Disabled, Expired, Lost, Stolen, Terminated, Unaccounted, Void.
- **Card Type** — Select a card type from the drop-down menu.
- **Company** — Select a company by clicking the browse button and displaying the Company Selection screen.
- **Issue Date** — Click the drop-down arrow to display the calendar and select an issue date.
- **Expire Date** — Click the drop-down arrow to display the calendar and select an expiration date.
- **Last Reader** — The name of the last reader on which the card was used (view only field).
- **Last Access** — The date on which the card was last used on a reader (view only field).
- **Trace Card** — Select this check-box to record every transaction generated by this card in a log file.
- **PIN Exempt** — Select this check-box if you want this card to operate without PIN restrictions.
- **ADA** — ADA refers to "Americans with Disabilities Act." Select this check box to allow for extended shunt time on a door so that someone in a wheelchair, for example, has enough time to get through the door without generating an alarm. The "extended shunt time" needed is set up on the PW-5000 door configuration.
- **VIP** — Select this check box to exempt the cardholder from anti-passback restrictions. A cardholder with VIP privileges can pass his/her card to the next person to swipe and pass through a reader.
- **Guard** — Select this check box to authorize the cardholder to clear local alarms by using the "C" keypad key.
- **IrisID Selected Card**— Select this check-box to configure that specific card as the only card number that would download to the panel when the IrisID reader is used.

- **Biometric Override** — Select this check-box to allow the user to enter Biometric PIN (see below) when the biometric data (e.g., fingerprint) does not work. Enter the **Biometric Override Password** in the **Morpho Biometric Override** pop-up screen:



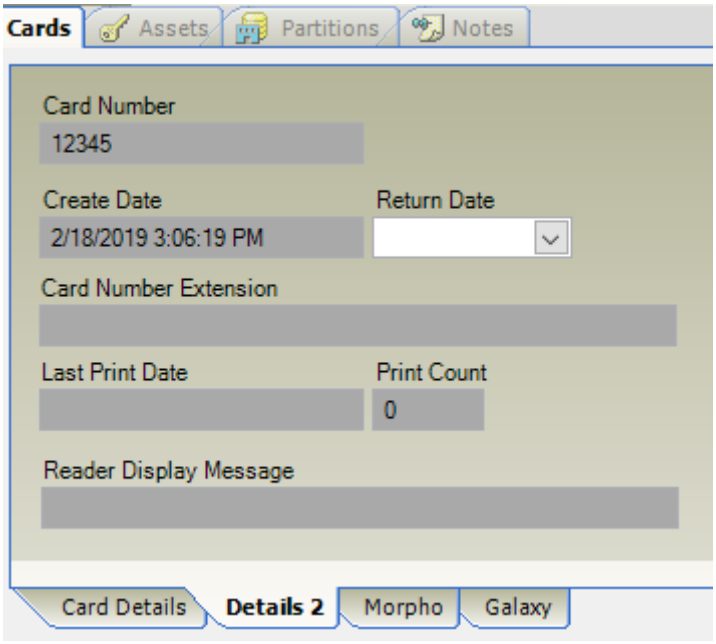
- **User Level** — The user level is often used to make some cards accomplish special tasks. For example, a manager may want to use such a card to automatically unlock the lobby doors at the beginning of a shift.

  Panel-level triggers and procedures can be written to trigger only on valid card accesses where the cardholder user level is equal to the user level set in the trigger.

  Allowed user level values range between 0 (zero) and 255. If a user enters anything out of this range Pro-Watch displays a validation error message and prompts the user to enter a proper value.

- **Card Disable (Days)** — Enter the desired number of days that must pass without card use before the card is disabled.
- **Number of Attempts** — Enter the maximum number of times a card/PIN can be used to gain access. For instance, if the number is set to 3, that particular card/PIN will be granted access three times. After that, access will be denied and the card will be disabled/deactivated.
- **Use Count** — Select this check-box to enable the use count.
- **Biometric PIN** — Select a Personal Identification Number (PIN) used to gain access through a biometric reader or lock.
- **Parade Text** — Enter the text (e.g., “Welcome...”) that will be paraded across the reader’s screen when the users swipe their cards, if the reader hardware supports this function.
- **Card Notes** — This field is for any miscellaneous notes you might want to record about the card.

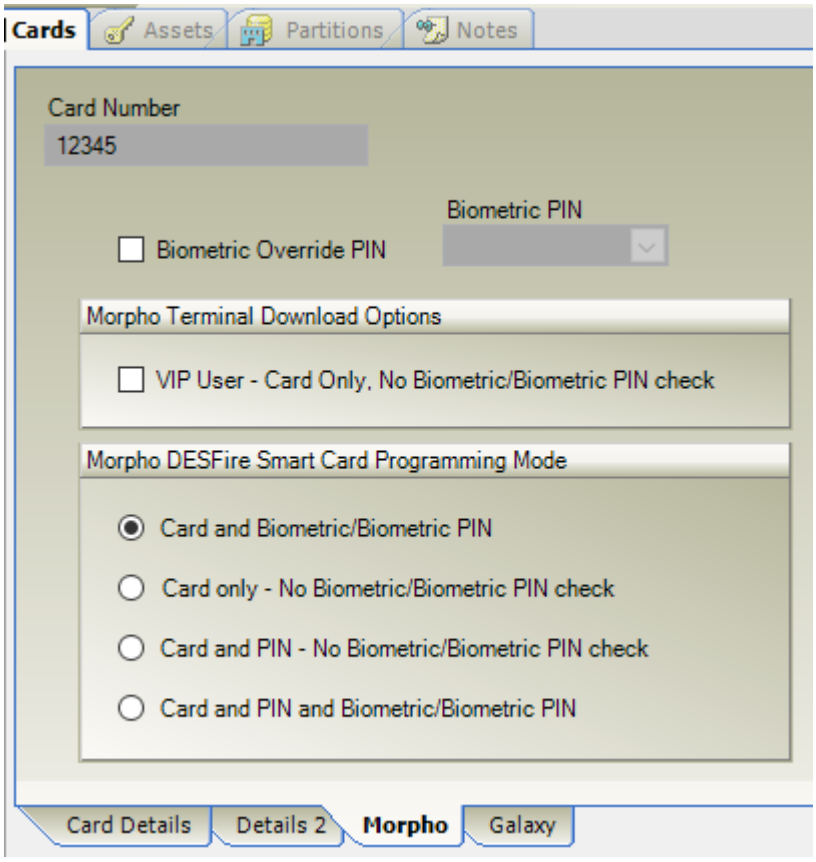
4. On the **Cards** tab, click the **Details 2** sub-tab to display it:



Follow the directions to edit the individual fields in the **Details 2** sub-tab:

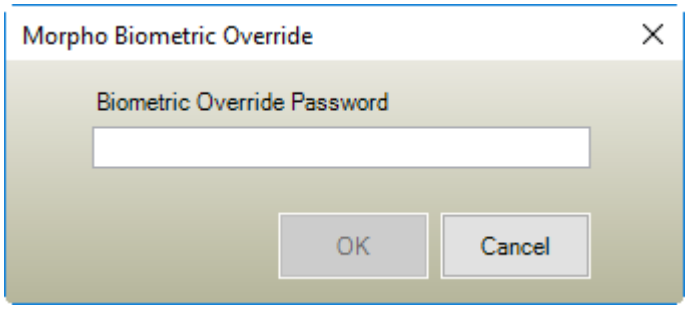
- **Card Number** field is populated automatically.
- **Create Date**field is populated automatically.
- **Return Date** — Click the drop-down arrow to display the calendar and select a return date. This is date on which the user has returned his or her card back to the company for leaving the company or any other similar reason.
- **Card Number Extension** field is populated automatically.
- **Last Print Date** — Displays the date on which this card was printed last. This field is populated automatically by Pro-Watch.
- **Print Count** — Displays the number of times the card has been printed. This field is populated automatically by Pro-Watch.
- **Reader Display Message** — Displays the text that you've configured earlier to display in the reader display.

5. On the **Cards** tab, click the **Morpho** sub-tab to display it:



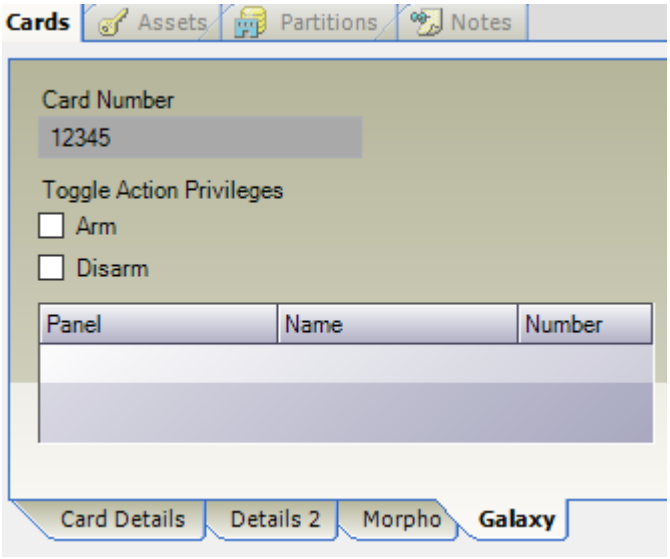
Follow the directions to edit the individual fields in the **Morpho** sub-tab:

- **Card Number** field is populated automatically.
- Select the **Biometric Override PIN** check-box if for some reason the user cannot produce a clear fingerprint on the bio-reader. Those persons can instead enter a **PIN (Personal Identification Number)** to gain access. When selected, the check-box displays the **administrative password** dialog box:



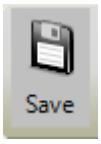
The administrative password enables the **operator** to enter a numeric PIN to the **Biometric PIN field** or select a numeric PIN from the **Biometric PIN drop-down menu**.

6. At the **Morpho** sub-tab, you can also select from the following self-explanatory options by selecting their respective check-box or radio-button:
    - **VIP User - Card only, No Biometric/Biometric PIN Check**
    - **Card and Biometric/Biometric PIN**
    - **Card Only - No Biometric/Biometric PIN Check**
    - **Card and PIN - No Biometric/Biometric PIN Check**
    - **Card and PIN and Biometric/Biometric PIN Check**
7. On the **Cards** tab, click the **Galaxy** sub-tab to display it:



- **Card Number** — This field is populated automatically by Pro-Watch.
- **Arm** — Select this check-box to arm the zone or group that the Galaxy panel controls.
- **Disarm** — Select this check-box to disarm the zone or group that the Galaxy panel controls.

8. Click the **Save** button on the toolbar.



9. Repeat this procedure to edit as many Cards as you need.

Note: Pro-Watch Advanced Badging tabs are customizable, and badging tabs are unique to each Pro-Watch installation. The following table presents only one of many possible tab sets. You can configure your own

tabs and fields by using Pro-Watch Badge Builder. See the *Pro-Watch Guide* for instructions.

2.8 Scheduling Clearance Codes

Scheduled clearance codes allow the user to assign an unassigned clearance code to a card with schedule.

The schedule is defined when the clearance code for the card is activated.

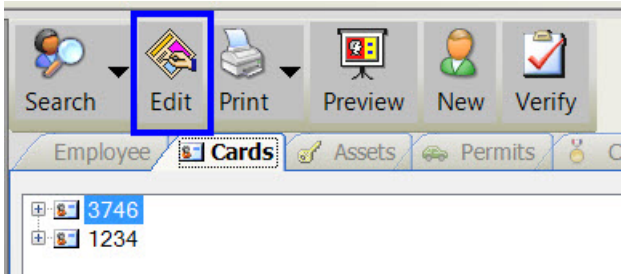
The difference between scheduled clearance codes and temporary clearance codes is that a scheduled clearance code is tied to a card while a temporary clearance code is not.

2.8.1 Rules for Scheduled Clearance Codes

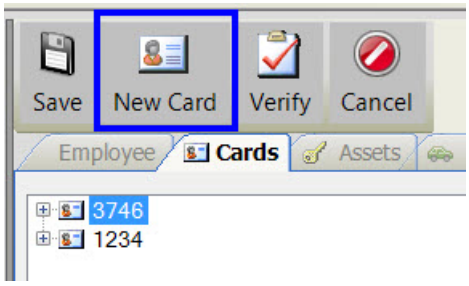
1. Scheduled clearance codes work only when the Pro-Watch server is up and running.
2. A scheduled clearance code cannot be
   - a timed clearance code
   - a temporary clearance code
3. Scheduled clearance codes are implemented in 30 minutes increment to avoid performance impact.
4. Scheduled clearance codes can be set for the future or the past.
5. Only the current or the future scheduled clearance codes count towards the access level count limit.
6. There are start and end dates for each scheduled clearance code. The end date is always after the start date.
7. The Start and End dates/hours are based on Pro-Watch server time.

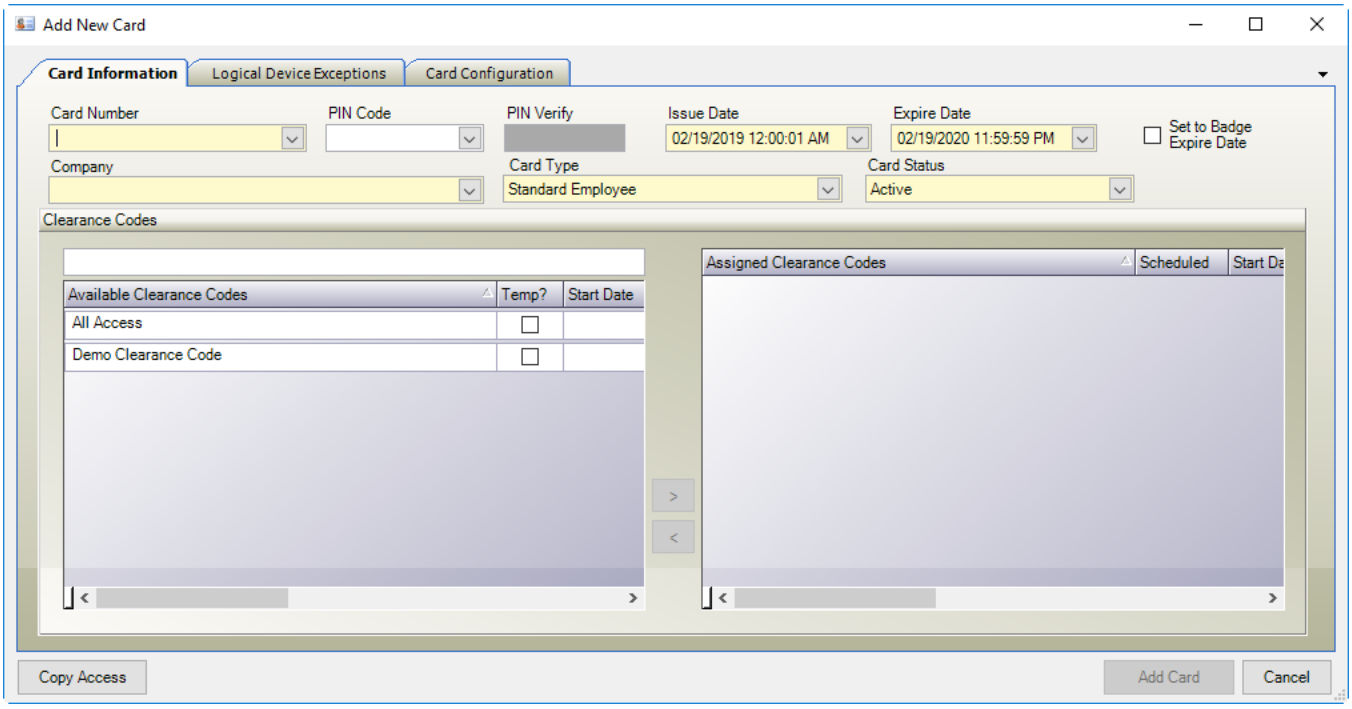
2.8.2 Assigning a Scheduled Clearance Code to a New Card

1. Go to the card tab and select the **Edit** tool icon.



2. In the dynamically changed tool bar, click the **New Card** tool icon to display the **Add New Card** screen:

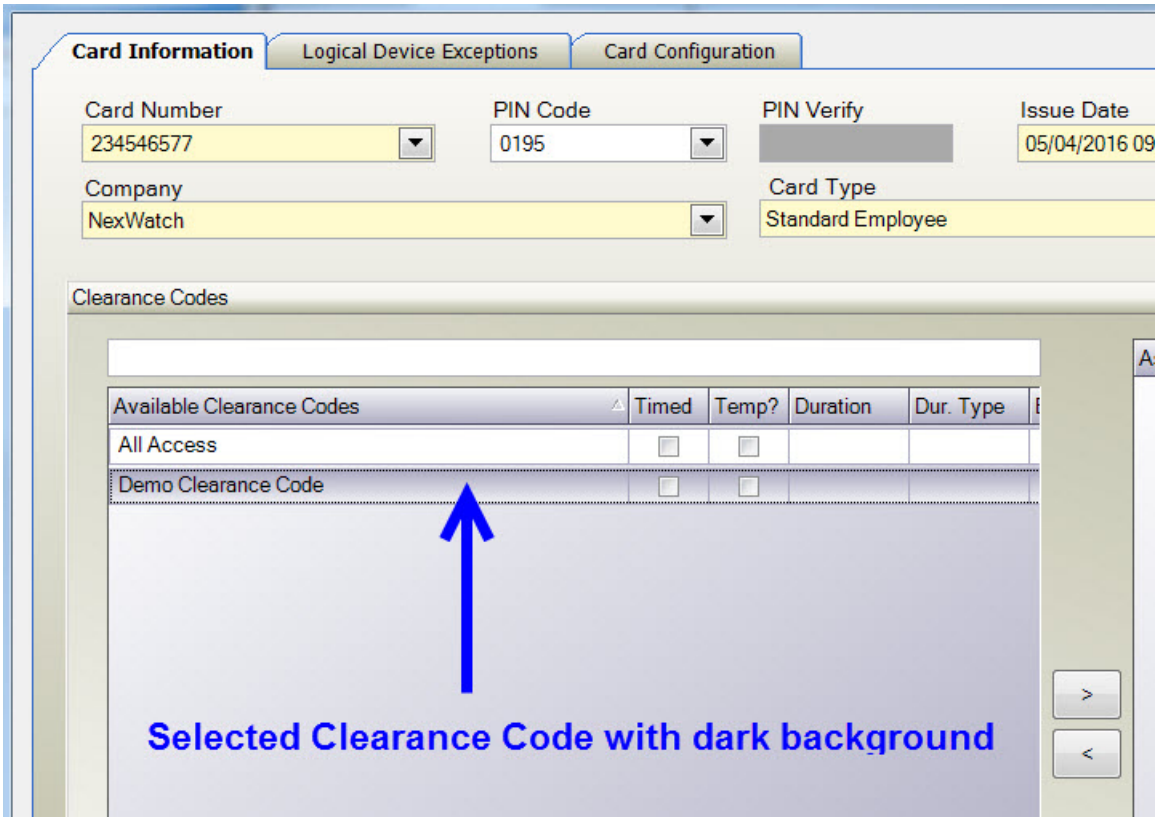




Note that the screen has two grids: **Available Clearance Codes** on the left, and **Assigned Clearance Codes** on the right. Since this is a new card, the **Assigned Clearance Codes** grid will be empty in the beginning.

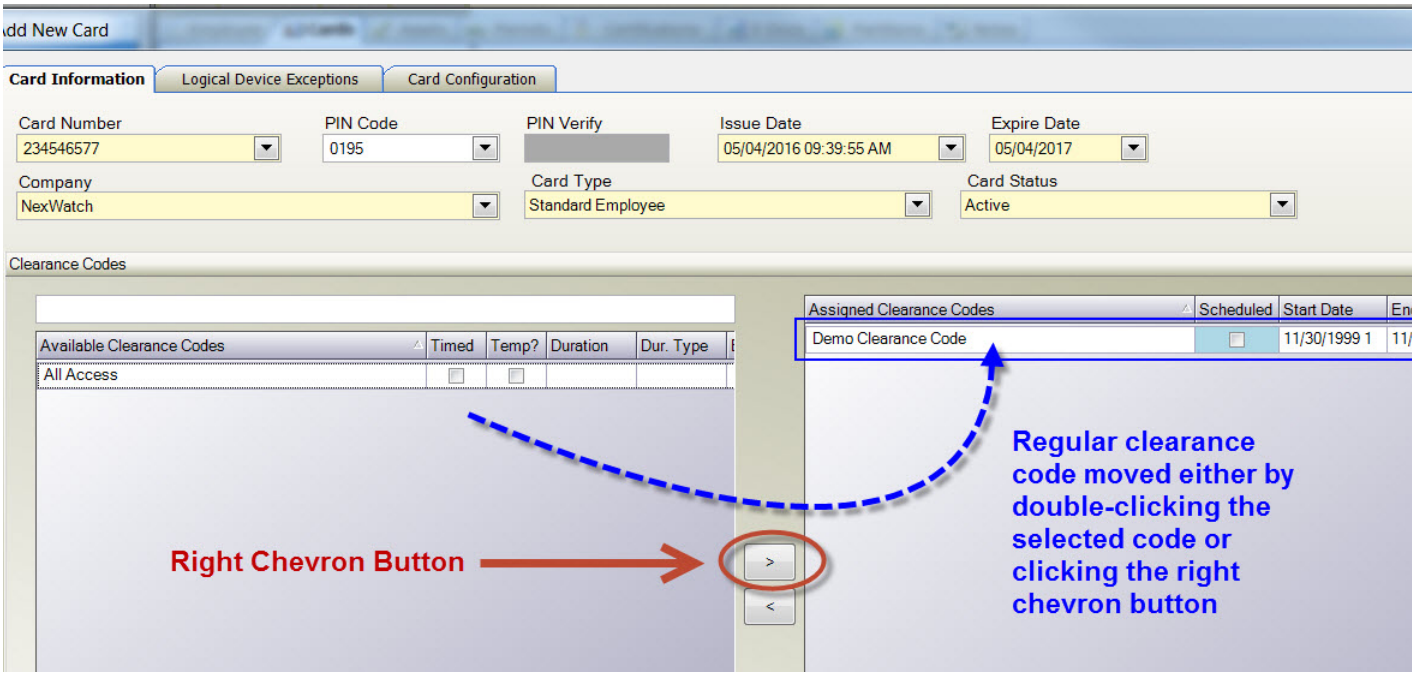
3. Enter all the card-related information.
4. Select a regular clearance code from the **Available Clearance Codes** grid (scheduled clearance code rules apply; no time or temp clearance

code). The background of the selected clearance code turns a dark shade of gray



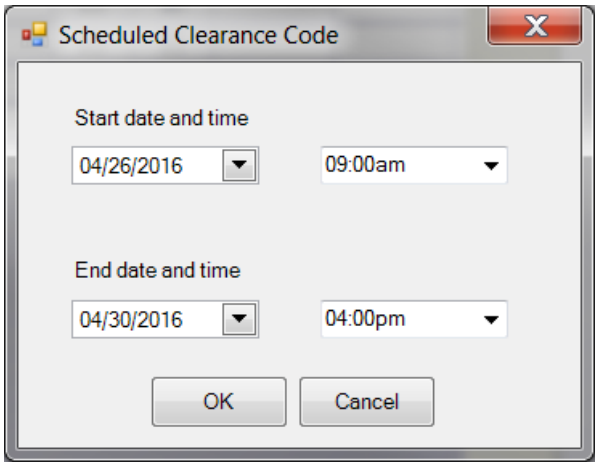
5. Move the selected regular clearance code in the **Available Clearance Codes** list-box to **Assigned Clearance Codes** list-box either by

clicking the right chevron button or double-clicking the clearance code.



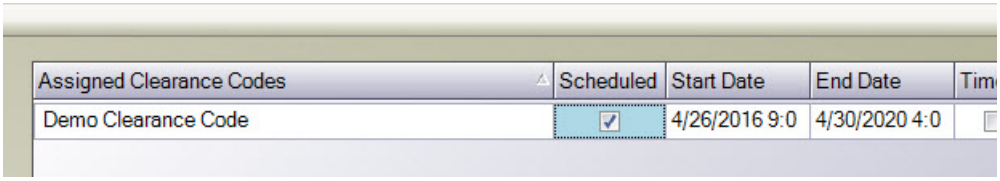
Note that the background of the **Scheduled** check-box will be **light blue**, indicating that you can select the check-box and schedule it.

6. Select the **Scheduled** check-box to display the **Start** and **End** date/time dialog box.

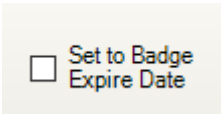


7. Select the **Start** and **End** dates and times you like from the drop-down lists and then click **OK** to assign those values to the selected scheduled

clearance code. Now the code will displayed the scheduled **Start** and **End** dates and times.



8. Select the **Set to Badge Expire Date** check-box to make the badge expiration date also the card's expiration date:

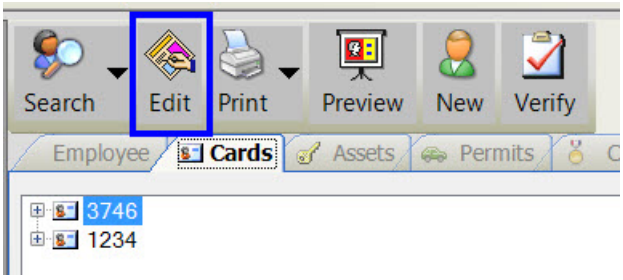


9. Click **Add Card** to add the card to the badge.

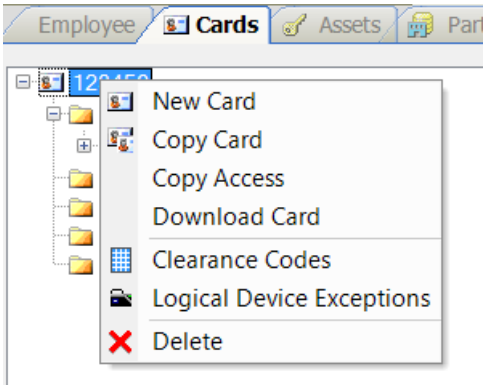
2.8.3 Assigning a Scheduled Clearance Code to an Existing Card

The process is almost exactly the same as assigning a scheduled clearance code to a new card (see "Assigning a Scheduled Clearance Code to a New Card"). You start the process by right-clicking an existing card.

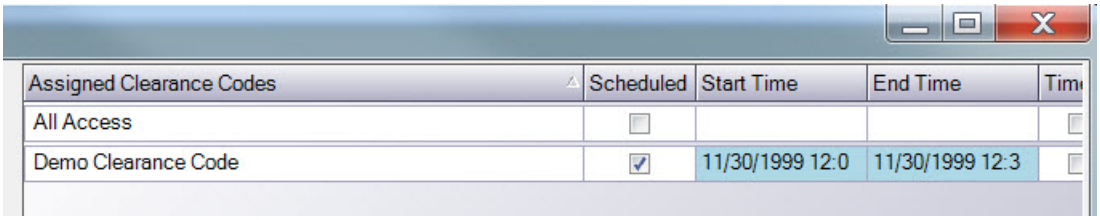
1. Go to the **Cards** tab and click the **Edit** tool icon.



2. Right-click the selected **Card** to display the pop-up menu.



3. Select **Clearance Codes** to display the **Clearance Code Management** screen.



Note that the **light blue** background for the **Start Time** and **End Time** fields indicates you can click on them for editing if you like.

4. Go to Step 4 of the section "Assigning a Scheduled Clearance Code to a New Card" and follow it to the end. When you are done, click **OK** to return to the main Card tab.

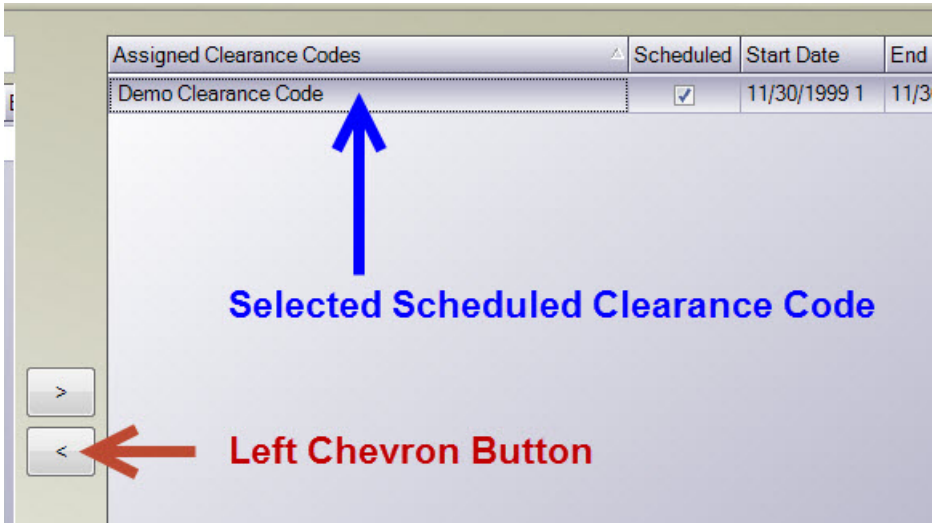
2.8.4 Unassigning Scheduled Clearance Code(s)

You can move a scheduled clearance code from the **Assigned Clearance Codes** grid to the **Available Clearance Codes** grid by either

- double-clicking the selected clearance code,

or

- selecting it and then clicking the left chevron button.



2.9 Copying Cards

Copying an existing card copies all Clearance Codes and Logical Devices from the original card; however, it derives a new calculation date from the Company configuration.

Follow these steps on the employee's Cards tab:

1. Click **Edit** on the toolbar.
2. Right-click the card you want to copy.
3. Select **Copy Card** to display the **Add New Card screen**.
4. Make the necessary changes and then click **Add Card**.

2.10 Downloading Cards

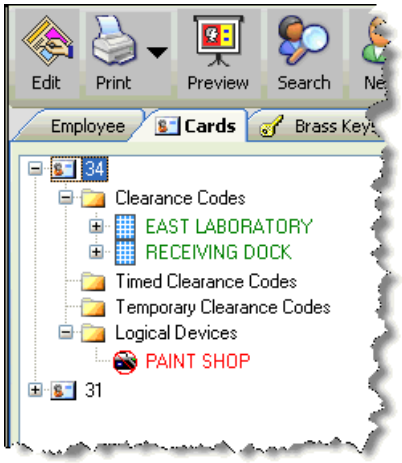
After you create a card, you need to download the information to its respective panel in order to grant access to card users. Follow these steps:

1. Select the badge holder from the badge holder list in the left panel (or click the **Search** icon at the top of the screen and search for the badge holder) to display the **Employee** tab and the badge holder's record.
2. Click to display the **Cards** tab.
3. Right-click the card you want to download and select **Download Card**.

2.11 Editing a Badge Holder's Card

To edit a badge holder's card:

1. Select the badge holder from the badge holder list in the left panel (or click the **Search** icon at the top of the screen and search for the badge holder) to display the Employee tab and the badge holder's record.
2. Click to display the **Cards** tab. If you want to display the Card's configuration of Clearance Codes and Logical Devices, expand the Card tree.



3. Click the **Edit** icon at the top of the screen.
4. To edit a Clearance Code, right-click the Card and select **Clearance Codes**. The **Clearance Code Management** screen appears.
5. Search to find the Clearance Code by entering the Clearance Code name in the blank field in the upper-left corner of the screen.
6. With the Clearance Code highlighted, use the right arrow and left arrow buttons in the center of the screen to either assign it as a new Clearance Codes or remove it.
7. To edit a Logical Device, right-click the Card and select **Logical Device Exceptions**. The **Manage Logical Device Exceptions** screen appears.
8. Search to find the Logical Device by entering the Logical Device name in the blank field in the upper-left corner of the screen.
9. With the Logical Device highlighted:
   a. Assign or remove the Logical Device by clicking either **Grant**, **Revoke**, or **Delete**.
   b. View the Logical Device's properties by right-clicking and selecting **Properties**. Here you can view the Logical Device's properties and Clearance Codes, as well as the device's most recent transactions.
10. Click **OK**.to accept all edits to the Card.

11. Make any appropriate edits in the Card Details and Details 2 tabs.
12. Click the **Save** icon at the top of the screen.

Note: When a card is opened in Advanced Badging, the user will **not** see the following GUI components:

- **Timed Points** tab.
- **Pathway** tab.
- **Panel Specific Options** tab.
- **Transaction** tab.
- **Optional Information** tab.

2.12 Deleting Cards

To delete a badge holder's card:

1. Select the badge holder from the badge holder list in the left panel (or click the **Search** icon at the top of the screen and search for the badge holder) to display the Employee tab and the badge holder's record.
2. Click to display the **Cards** tab.
3. Click **Edit** on the toolbar.
4. Right-click the card you want to delete and select **Delete**.

2.13 Mobile Credentials (HID)

You can add mobile credentials (from HID) to a Pro-Watch badge record if you'd like to use your smart phone to gain access through a reader via blue-tooth technology.

2.13.1 Limitations

1. Only one mobile credential is supported per badge holder.
2. If 'Card seed' option is enabled in Pro-Watch Server options, then Mobile Credential option won't be displayed when adding a new card.
3. After applying the hotfix (PW-10969), all badges/cards must be added/modified from Pro-Watch client only and the HID portal must not be used since it can lead to a data mismatch between PW and HID.
4. Badge holder e-mail ID correction from Pro-Watch will not send the enrollment email to the updated email ID. The operator must delete the Mobile credential and add it again to get the enrollment code to the correct email ID.
5. If the HID mobile credential is already in use when the card number is added manually in Pro-Watch as a normal card, then it will not be possible to convert the card number as a Mobile credential in Pro-Watch. Such cards will remain as normal cards in Pro-Watch.
6. Entering the HID mobile credential in Pro-Watch by using a specific HID company account and then switching to a different HID company account will lead to synchronization issues. Always use the same HID company account.
7. In any circumstance, if the same HID mobile credential card number (that is being allocated to Pro-Watch badge holder by HID) already exists in Pro-Watch as a normal card number, then the Badge/mobile credential creation will fail in Pro-Watch while the HID portal adds that user. That means, if the badge holder and the card get created in HID but not in Pro-Watch, then the PW and HID data will not match. As a result, even when the operator fails to add mobile credential in Pro-Watch, the HID will still send an email invitation to the specific badge holder's email box to download the mobile credential, and that badge holder will be able to gain access at doors depending on the privilege for that normal card as configured in Pro-Watch.
WORKAROUND SOLUTION: When this issue occurs, go to the HID portal and delete the offending mobile credential.

2.13.2 Introduction

A **mobile credential** allows Pro-Watch badge holders gain access through a mobile device.

Honeywell has integrated the mobile credential enrollment process into Pro-Watch to eliminate the need to enroll cards both in Pro-Watch and the reader manufacturer.

Before getting started, there are a few things that you need to complete before you can start to enroll mobile credential in Pro-Watch's Advance Badging module.

1. Make sure a login credential with administrative privilege is obtained from HID.
2. Once the proper login credentials are obtained, the Pro-Watch operator should logon to the HID website using the given admin account to create a system account (explained below).

HID system account is used by Pro-Watch to access HID portal. The following section will describe step-by-step how to enter the system account into Pro-Watch and how to enroll the mobile credential in Pro-Watch.

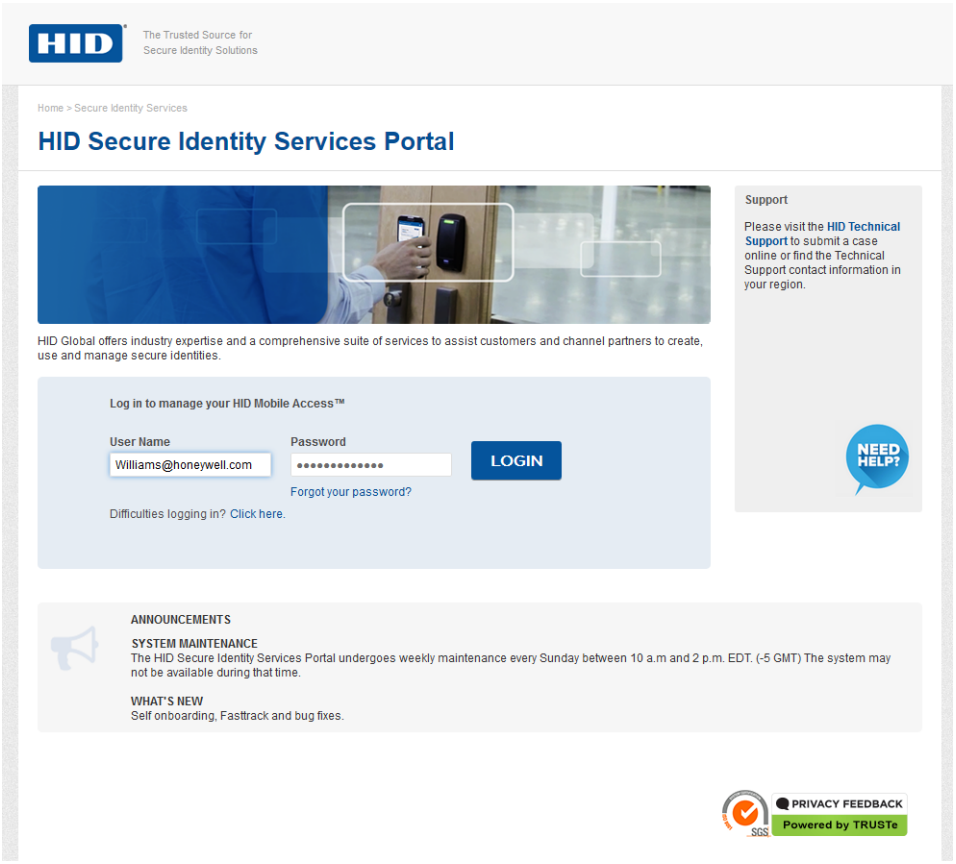
NOTE: **The mobile credential add option will be missing if Card Seed option is enabled in Pro-Watch client.** To enable or disable the Card Seed in Pro-Watch client:

1. Go to **File > Server Options > Additional Server Options** (tab).
2. Enter a seed value into the **Card Seed** field to enable it. Delete any value in the same field to disable it.
3. Click the **OK** button.

2.13.3 Prerequisite: Create an HID Account

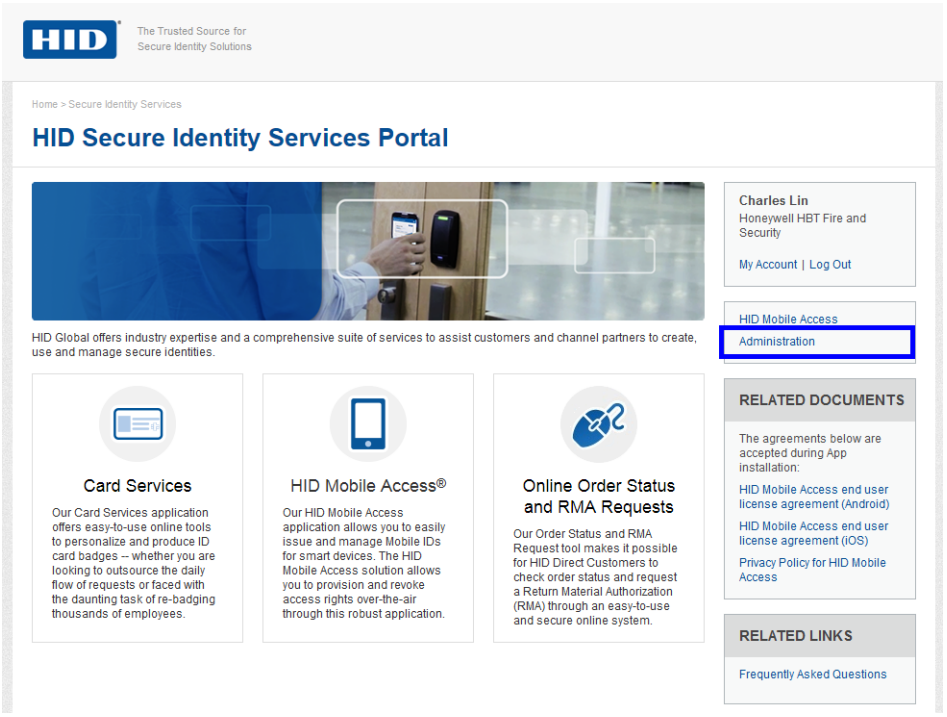
Create a system account at **HID portal by following these steps**.

1. Locate your **HID system account User ID** and **Password** and login to the HID portal:

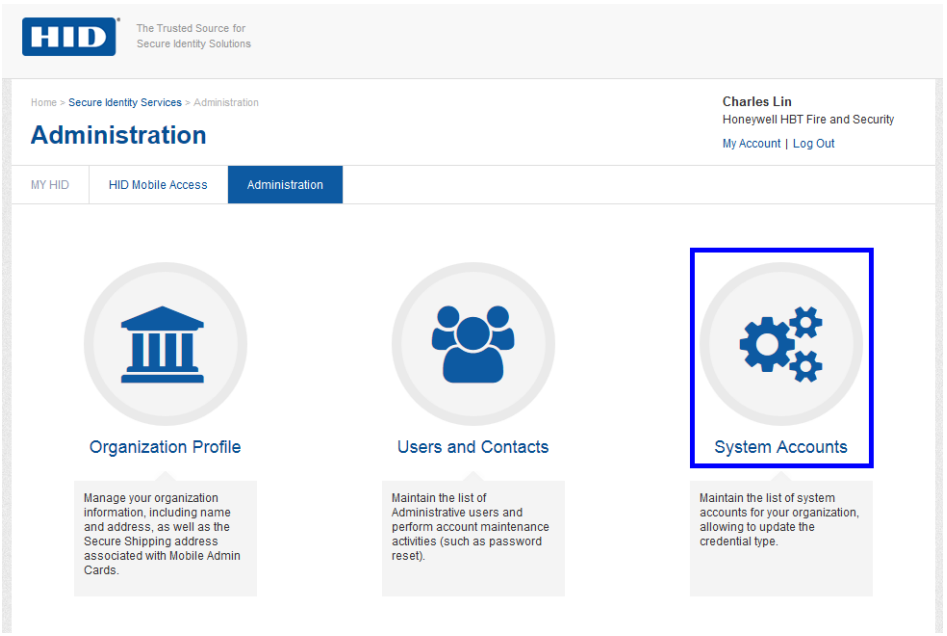


Note: The "HID system account" is different from the account used to login to HID).

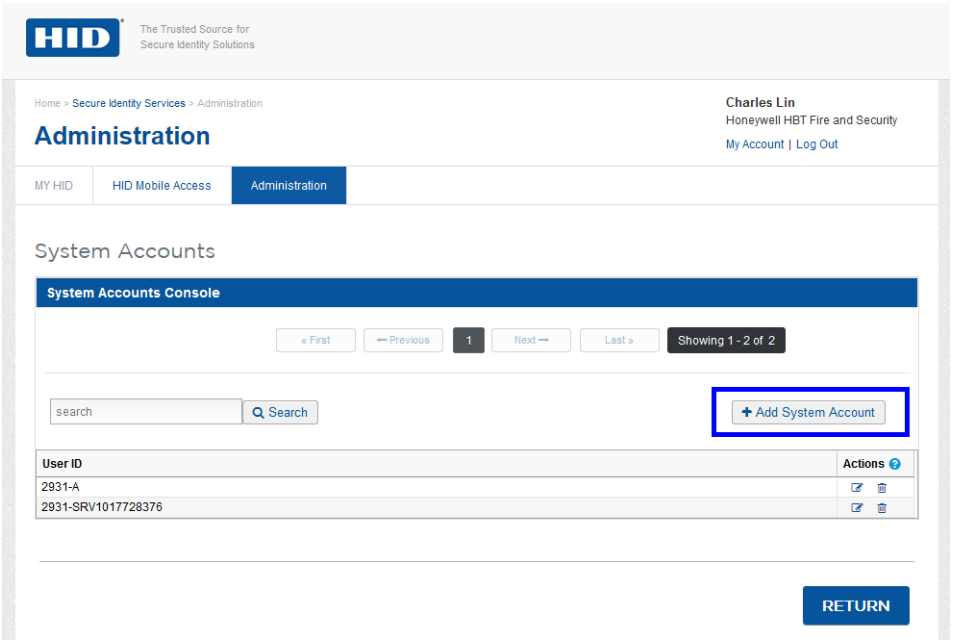
2. Click **LOGIN** button to display the **HID Secure Identity Services Portal s**creen:



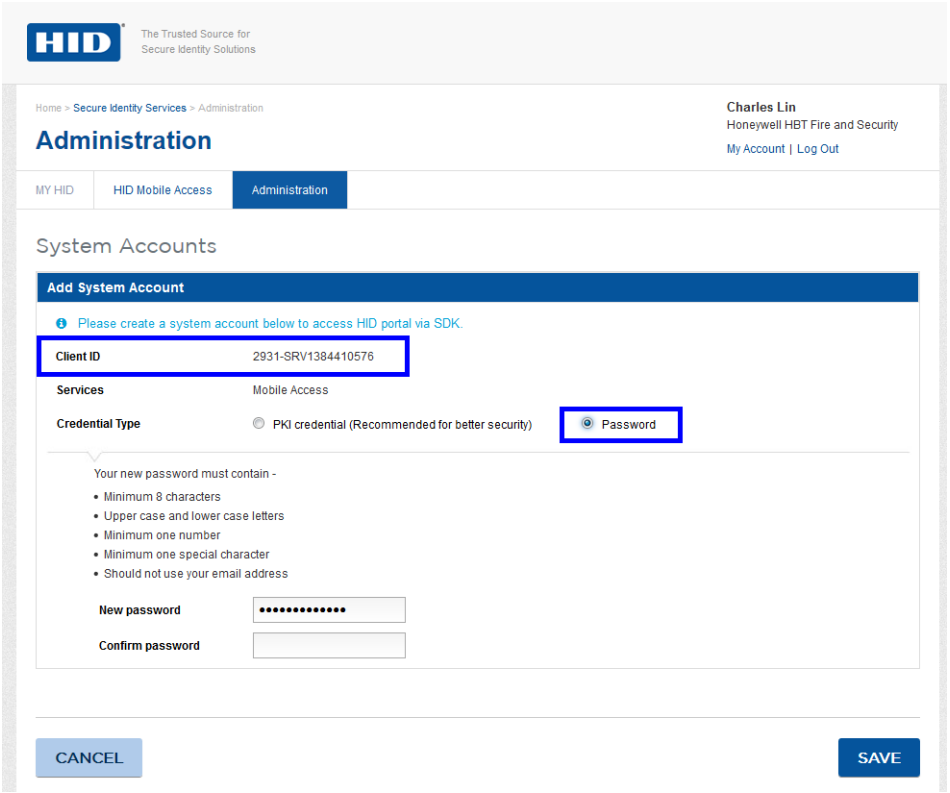
3. Click the **Administration** link to display the Administration screen:



4. Click the **System Accounts** link and then enter your **User ID** and **Password** to display the System Accounts screen:



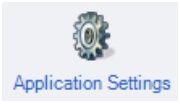
5. Click **Add System Account** to display the Add System Account screen:

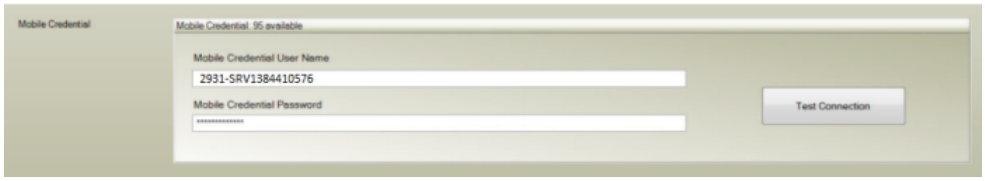


6. Make sure you select the **Password** option button. Enter and confirm your new password. The "**PKI credential (Recommended for better security)**" option is not supported at this time. The system automatically assigns a **Client ID.**

   The **Client ID** and the **Password** will now be used to connect Pro-Watch Advanced Badging module to the HIP portal, as described in the steps to follow.

7. Launch the **Pro-Watch AP Badge Manager.**
8. From the **Administration** set of links on the left navigation pane, click **Application Settings** (the GEAR icon) to display the **Mobile Credentials application settings screen** in the right pane:





9. Click **Edit** to enter the editing mode.
10. Update the **Mobile Credential User Name** and **Password** with the **Client ID** and **Password** from the **System Account**.
11. Click **Save** to leave the editing mode.
    Note: Changes you have made above do not take effect until you restart the Pro-Watch Advanced Badge Manager.

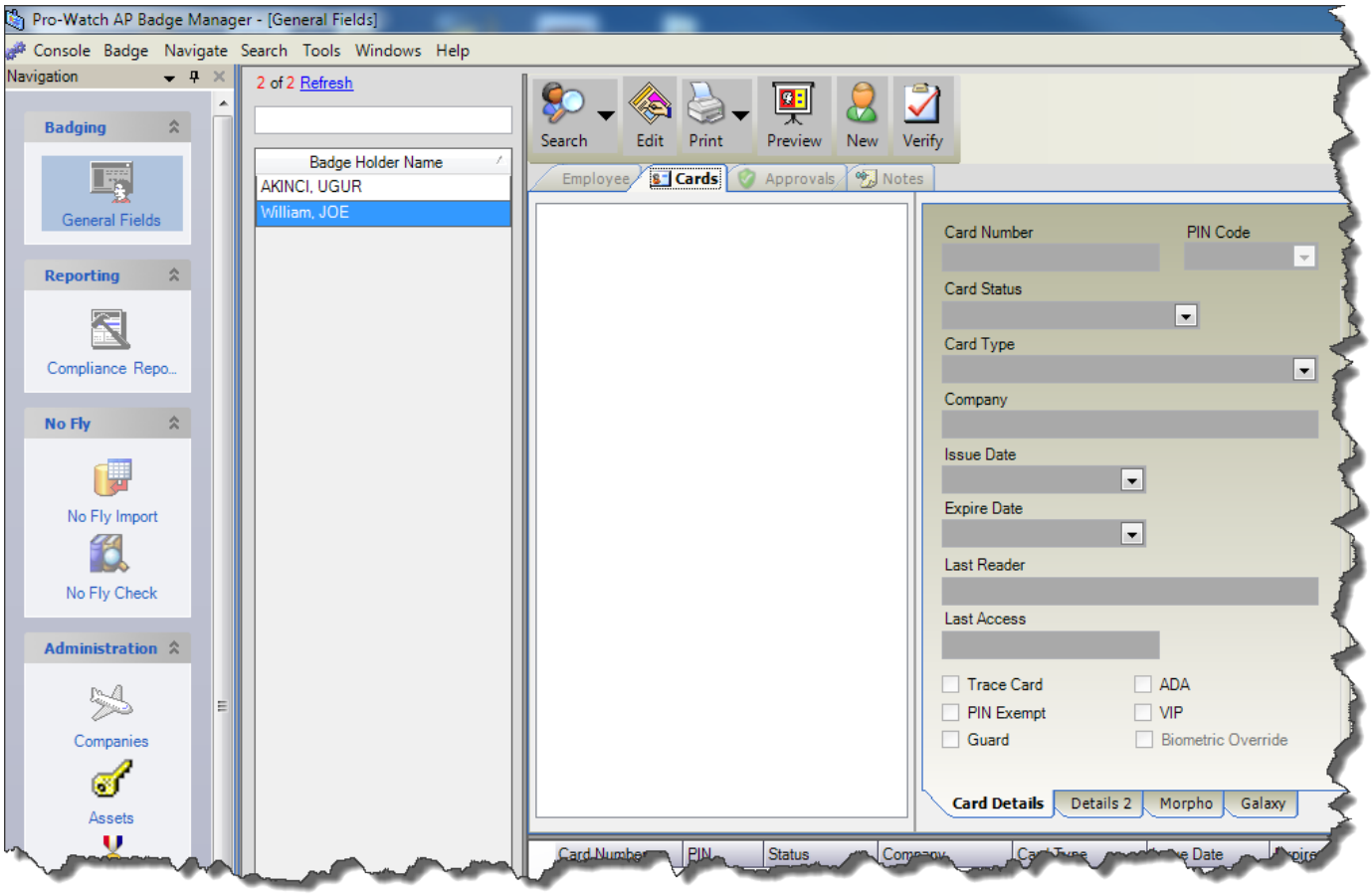
Now you are ready to assign a mobile credential number to your card by following the steps described below.

2.13.4 Steps to Follow

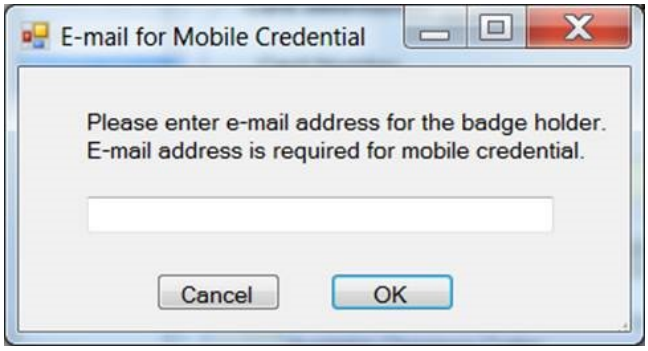
The procedure is very similar to adding a card to a badge-record.

1. Launch the **Pro-Watch AP Badge Manager.**
2. Select **General Fields** to display the mid- and right-panes of navigation:

3. Select a **User** from the mid-pane to display the related user information on the right-pane. Select the **Cards** tab:



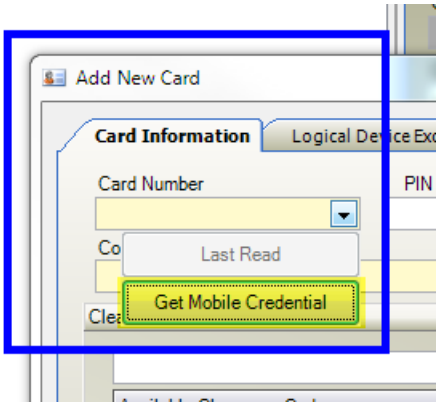
4. Click the **Edit** icon in the right-pane to display the **New Card** icon.
5. Click **New Card** to display the **Add New Card** screen.
6. Fill in all the fields applicable to your company.
7. Fill in the **email address**. If there is no email address saved in the badge record, the system will display the following warning message:



NOTE: "**E-mail**" is the name one of the default badge record fields. If a

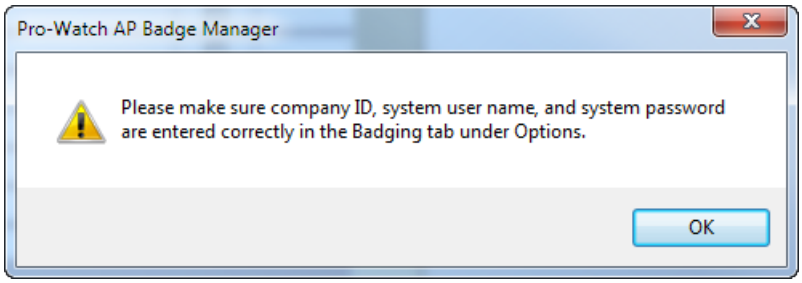
user fills that field in the badge profile screen, the above e-mail prompt dialog box will not be displayed.

8. Enter an appropriate email address and click **OK** to save the address into the badge record.
9. From the drop-down menu of the **Card Number** field, select **Get Mobile Credential:**



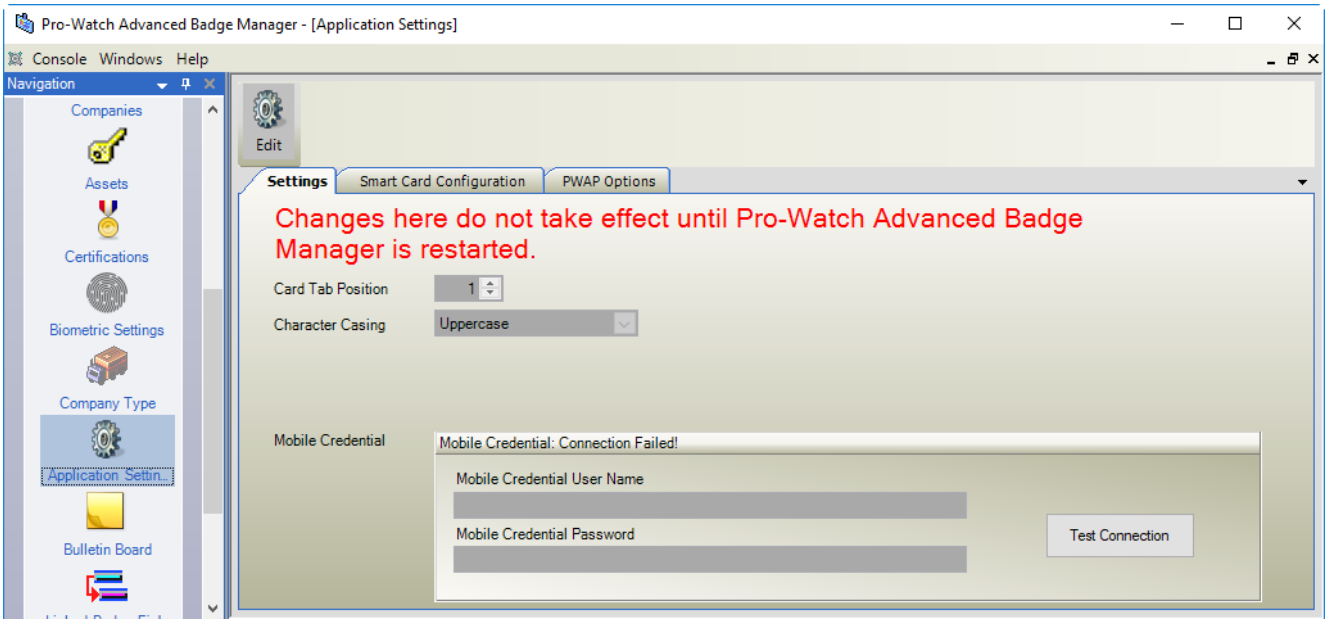
At this point the system will display a **temporary Card Number** starting with the letters **"MC"** which will be replaced by a real card number after you save the information entered.

10. If you receive the following error message



select the **Application Settings** navigation-sidebar option to display

the **Settings tab** where you can click **Edit**, enter your **Mobile Credential Password,** and then **Save**:



11. HID server will send an **email** to the **end user**. The end user opens the email which contains a **link** for the "**HID Mobile Access**" app. The end user must install the app to the mobile device.

HID sends an **invitation** to the end user by email with the subject like "**Your HID Mobile Access Invitation Code**." When the end user accepts the invitation, the mobile credential becomes active. **The typical invitation email text** looks like the following sample:

> Dear Tom Williams,
>
> Welcome to HID Mobile Access®
>
> Your organization has decided to embrace a new method of access control. Once enrolled, your Android™ or iOS® mobile device can be used for building and gate access by holding it close to or "tapping" it on the reader. Your organization may also have chosen to activate a long range read option. If this option has been enabled, you may have the opportunity to open doors and gates with the Twist and Go gesture as you approach the door. This can be confirmed by your Security Administrator.
>
> Please follow these simple steps to prepare your mobile device, receive your Mobile ID and make the move to HID Mobile Access.
>
> **Step 1:** Download the HID Mobile Access App:
> • From the App Store for iOS: http://appstore.com/hidmobileaccess

• From Google Play for Android :
https://play.google.com/store/apps/details?id=com.hidglobal.mobilekeys.android.v3

Step 2: Enter the invitation code when prompted, and get your device ready for Mobile Access.

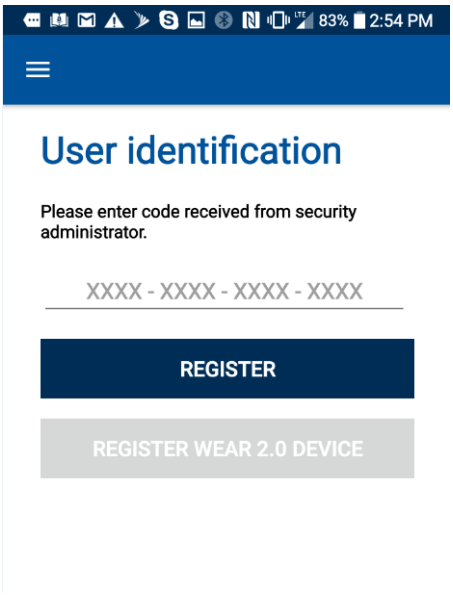
Step 3: Your Security Administrator will issue a Mobile ID that will be visible when you open the HID Mobile Access app

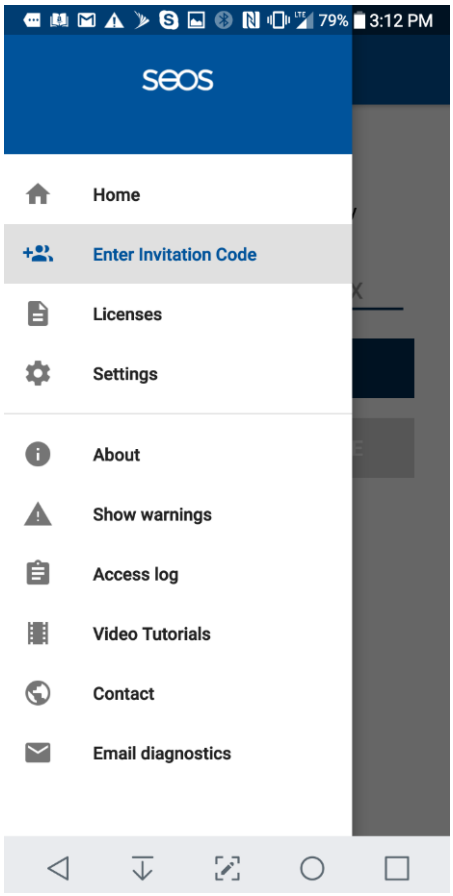
Step 4: Your Security Administrator will grant access rights.
Your invitation code is KOCB-TIKQ-AZDZ-IGXF, it expires on 18 Oct, 2017 18:47 UTC

Depending on your organization's process, the last two steps may take some time. Your Security Administrator will confirm when you can begin using your mobile device to enter the building. Please refer to the points below to help you get started.

Best regards,
Your HID Mobile Access team

12. In your smart-phone, **launch** the HID app, **enter the code** you received by the HID email (above step) and click **Register**:





13. Select one of the available mobile menu options to proceed:



Congratulations!

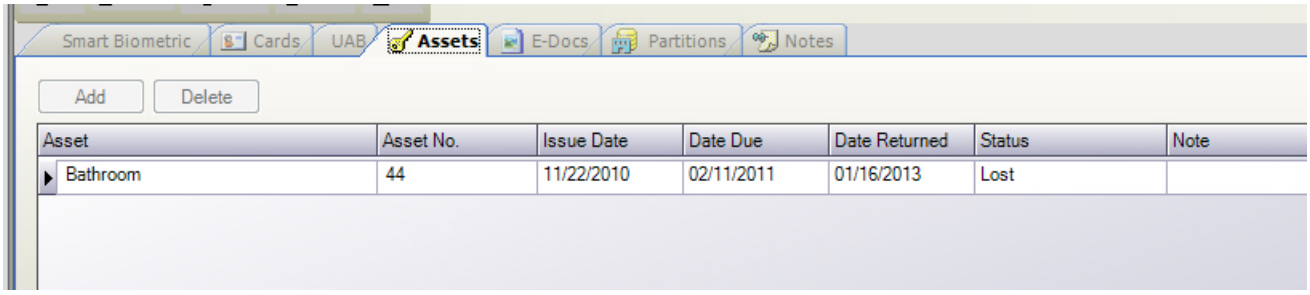
The badge holder is now good to use the mobile credential at supported readers.

2.14 Assigning Assets

An Asset (formerly called “Brass Key”) is a Pro-Watch database element that refers to a physical key assigned to a badge holder. See Chapter 7 of the *Pro-Watch Software Suite User Guide* for Brass Key, or Asset, configuration information.

To assign a Pro-Watch Asset to the Pro-Watch badge holder, click the Assets tab and follow these steps:

1. Click the **Add** button to display a new **Asset** record:



2. Enter (or select from the Asset dropdown list) the Asset you want to assign to this badge holder.
3. In the **Due Date** field, click the dropdown calendar and select the date that the badge holder must return the asset.
4. In the **Date Returned** field, click the dropdown calendar and select the date that the badge holder returned the asset.

To *remove* an Asset record from the badge, click the left margin of the asset’s record (see above), and then click the **Delete** button at the top of the tab.

2.15 Using E-Docs

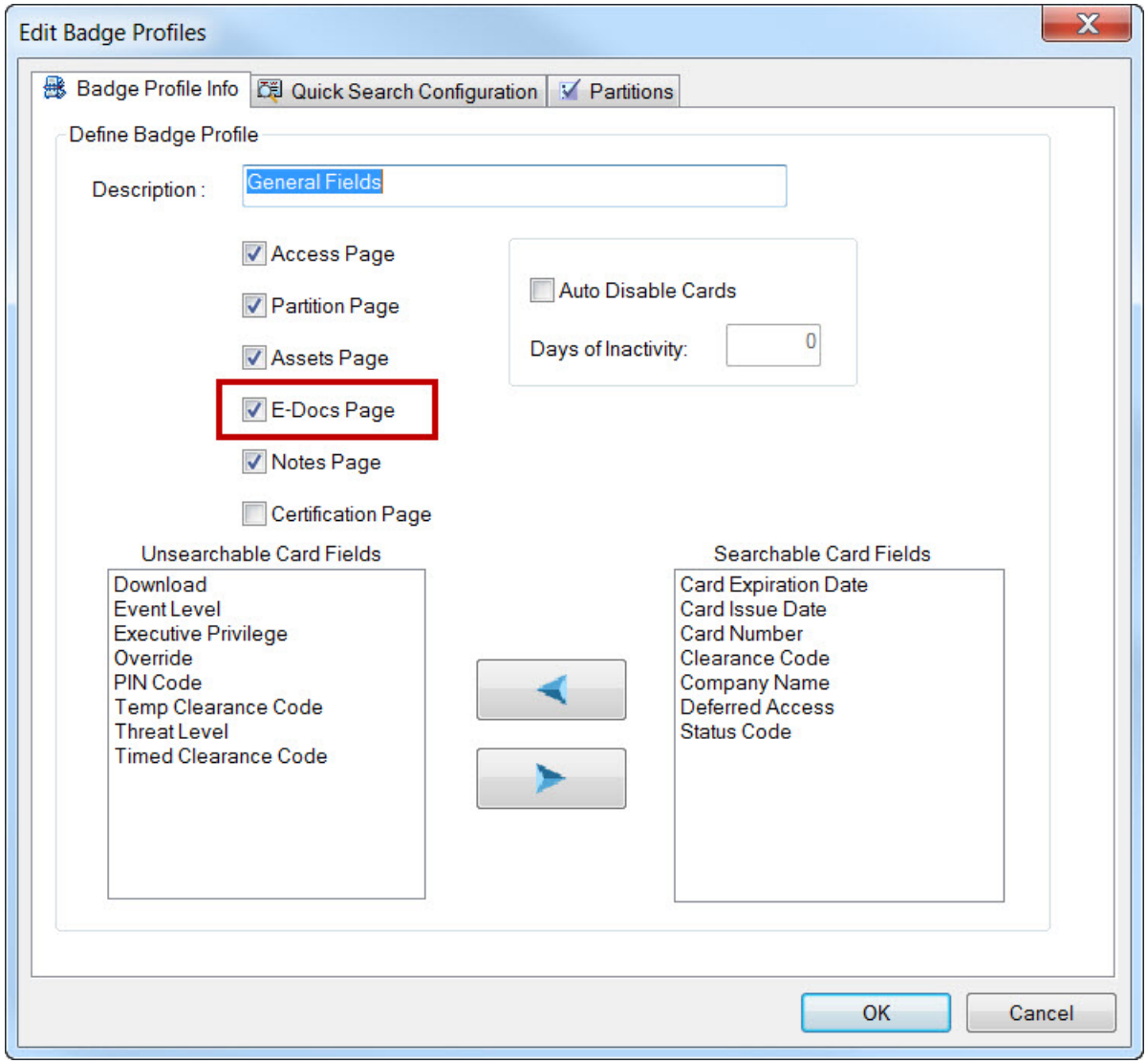
Use the E-Docs tab to work with Pro-Watch pictures, signatures, and any file-system file. Picture and signature operations are normal in Pro-Watch. In Pro-Watch Advanced Badging, you can associate a file-system file to a badge holder or to a Company.

For example, you can now link a badging application in PDF format to a badge holder or Company. You can view the application from the badge record or Company record by using Adobe Acrobat Reader. All electronic documents (including pictures and signatures) can be opened by using whatever application in Windows is associated with the electronic document. Windows associates applications with files, based on the extension of the file.

2.15.1 Enabling E-Docs

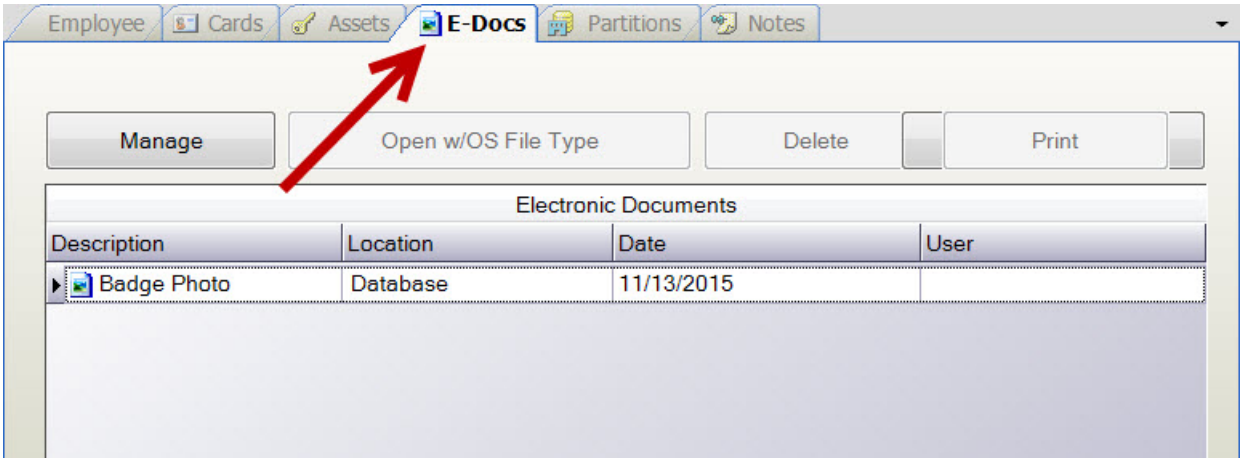
In Pro-Watch, select **Database Configuration > Badge Profiles**. Double-click the **General Fields** icon to display the **Edit Badge Profiles**

screen. Then select the **E-Docs Page** check-box as shown below, and click **OK**.



Now, in Pro-Watch Advanced Badging, you will see a tab named "**E-Docs**" on the Badging screen. This tab displays all pictures, signatures, and

file-system documents you for every badge holder. Electronic documents are identified by an icon that precedes the object's description.



Enabling E-Docs for Companies

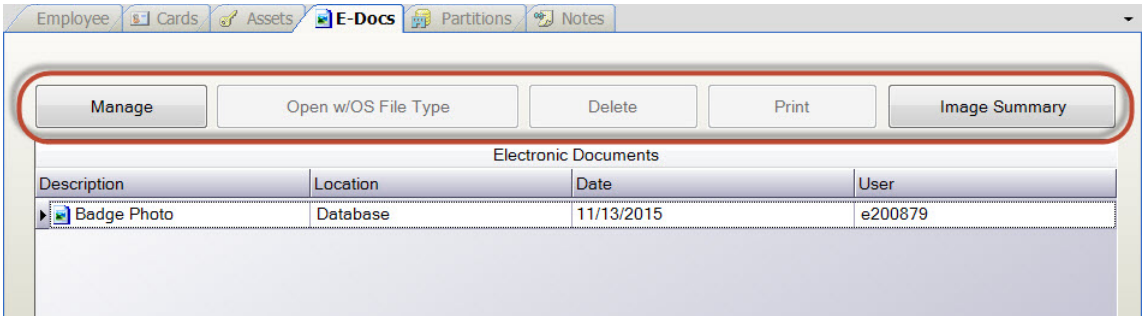
In Pro-Watch, create a new Blob Type and set the BLOB_TYPE.SYSTEM column database element
to 2:

1. Select **Database Configuration > Blob Types**.
2. Right-click in the Blob Type display window, and select **New Blob Types** to display the **Add Blob Types** screen.
3. Complete the Add Blob Types dialog box (refer to Adding or Editing Blob Types in Chapter 7 of the *Pro-Watch Software Suite Guide*).
4. Use **MS SQL Server Management Studio** to edit the Blob Type in the Pro-Watch database: in the BLOB_TYPES table, set the System column to 2.

2.15.2 Performing Electronic Document Operations

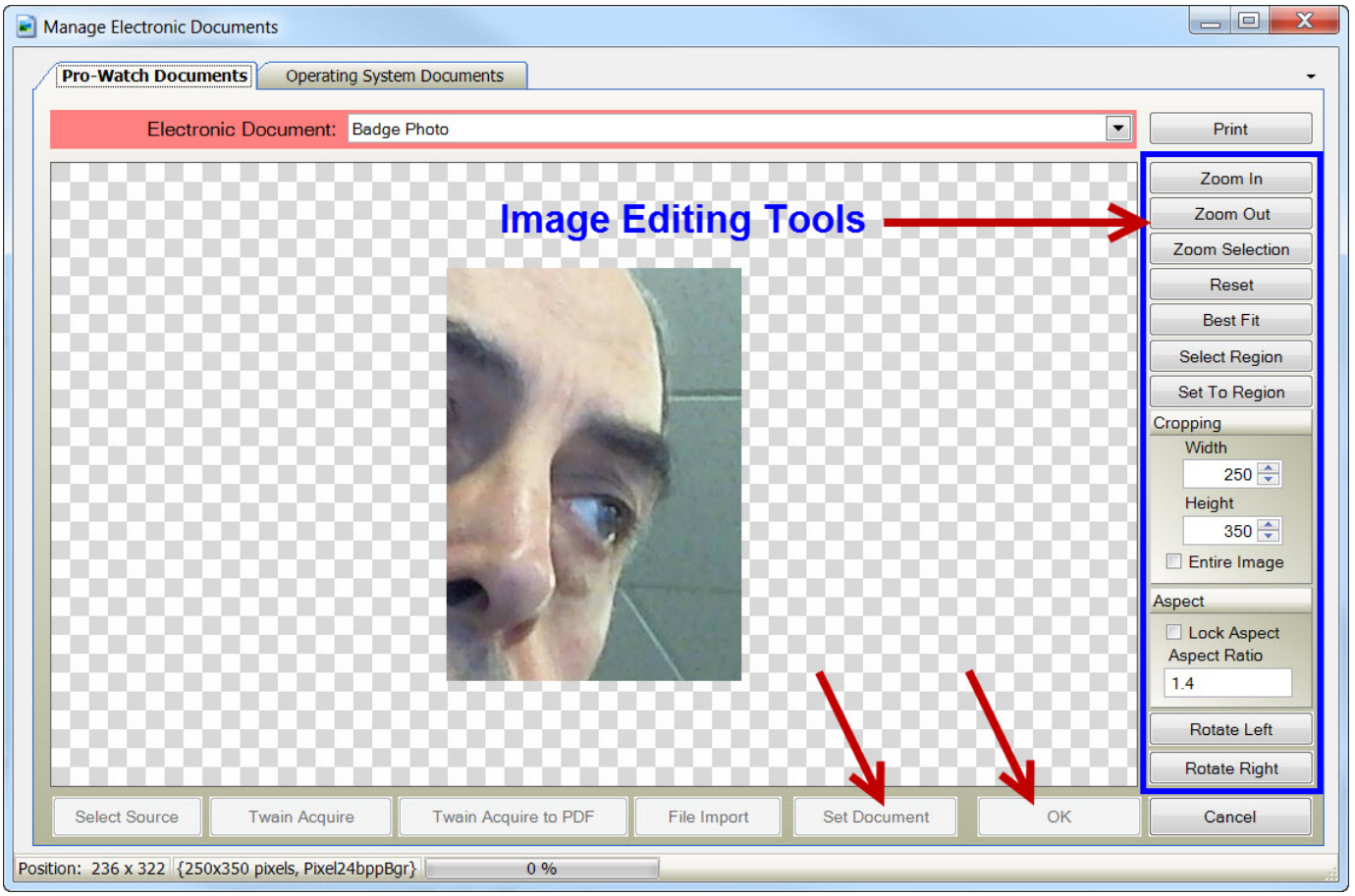
Click to select and display the electronic document you want.

Pro-Watch Advanced Badging provides the following three operations (buttons on the tab) available to you for the selected document:



- **Manage**—Displays the Manage Electronic Documents screen and enables you to perform a variety of image manipulations. This screen has the same functionality as Pro-Watch. Pro-Watch documents are pictures and signatures that are usually imported from a TWAIN device or signature pad.
- **Open wOS File Type**—Uses the Windows file system application to open the electronic document.
- **Delete**—Deletes the electronic document associated with the badge holder.
- **Print**—Prints the document.
- **Image Summary** — Displays the image summary characteristics page.

When you click **Manage**, the **Manage Electronics Documents** screen appears:



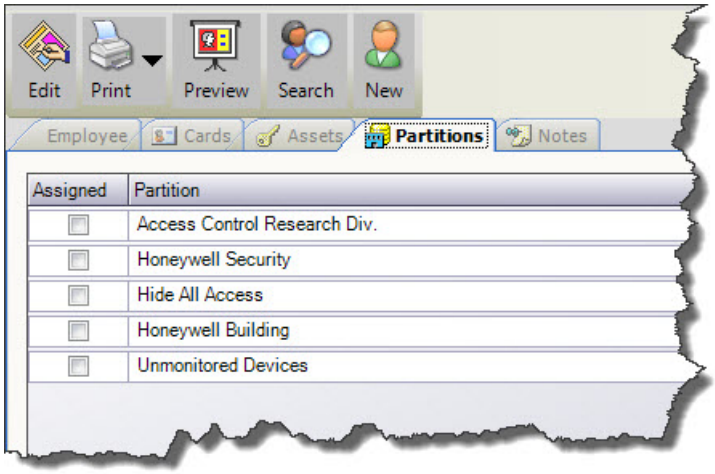
Use the image editing tools in the upper-right corner of the screen to edit the image. To save the edits, press **Set Document** and click **OK**. The edits become permanent when you save the badge holder.

2.16 Assigning Partitions

A Partition is a database element created in Pro-Watch (see DBC - Partitions, page 1 for information about creating Partitions). A Partition restricts a Pro-Watch badge holder to database resources that have been defined in Pro-Watch.

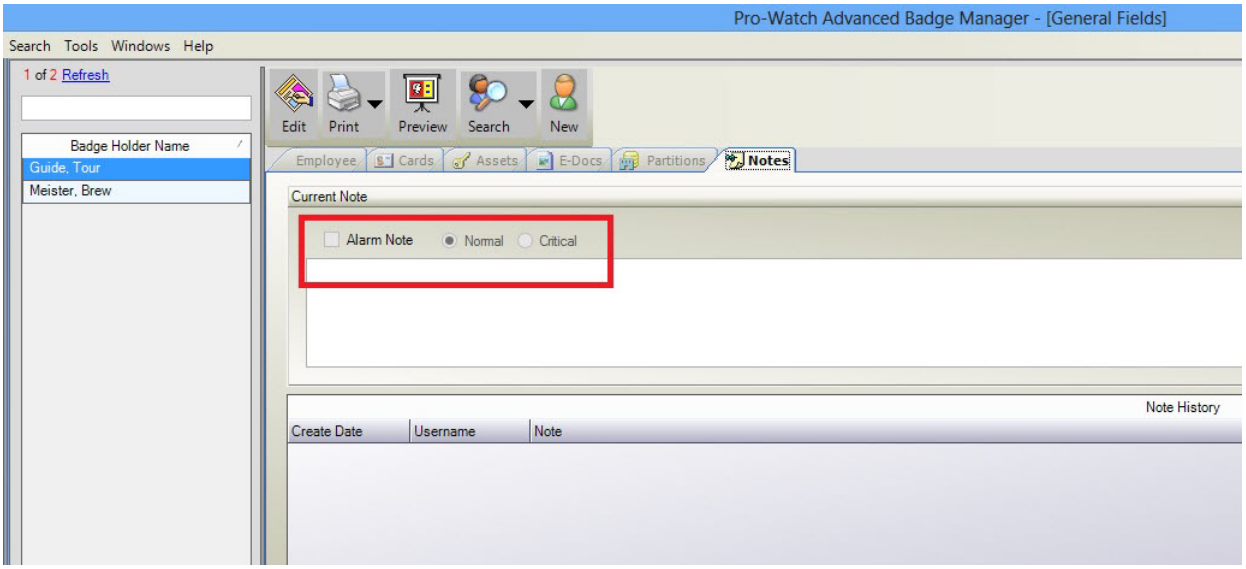
To assign a badge holder to a Partition:

1. Click the **Partitions** tab to display all Partitions in the Pro-Watch environment.



2. In the Assigned column, click the checkbox next to the Partition to which you want to assign the badge holder.

2.17 Assigning Notes

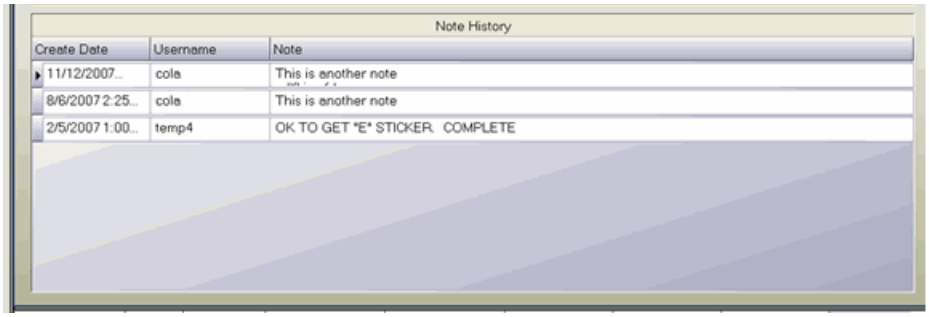


You can enter any pertinent piece of information about the badge holder in the **Notes** tab. Each time you add or modify a note, the previous note text moves to the **Note History** section.

There are two types of alarm notes:

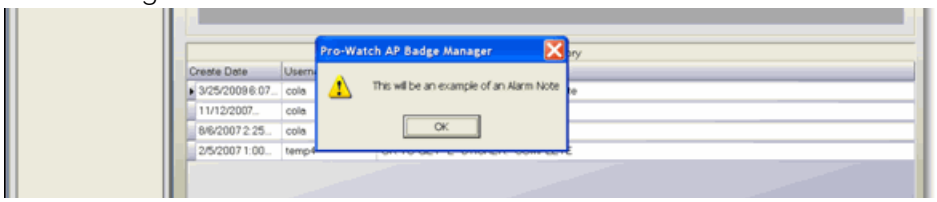
1. Normal
2. Critical

The **Note History** displays all historical notes for the badge holder, the date each note was created or modified, and the person who wrote the note.



Note that when the **Alarm Note** check-box is selected, the note text appears on the screen whenever a badge operator accesses the badge

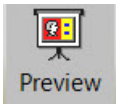
holder's record. As shown below, the screen requires the operator to acknowledge the note.



2.18 Previewing Badge Records

Follow these steps to preview a badge record:

1. Select the badge you want to preview from the Badge Holder Name window on the Badging screen.
2. Click the **Preview** icon from the function toolbar:



2.19 Printing Badge and Card Records

2.19.1 Displaying Print Preview

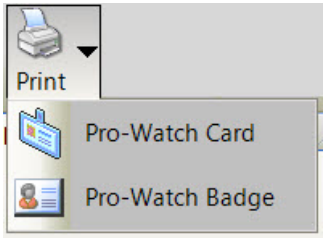
You need to add permissions to IIS_IUSRS to display badgeholder print review before printing. To do that, follow these steps:

1. Go to **Local > Temp** folder.
2. Right-click on the default user name and select **Properties**.
3. In the **Security** tab, add default user name **IIS_IUSRS**.
4. Click **OK** to close the Properties screen.

2.19.2 Printing Badges or Cards

You can print an entire badge record or a single card record. Follow these steps:

1. Select the badge you want to print from the Badge Holder Name window. If you want to print a single card, click to select the card in the card window at the bottom of the Badging screen.
2. Click the **Print** icon from the function toolbar:



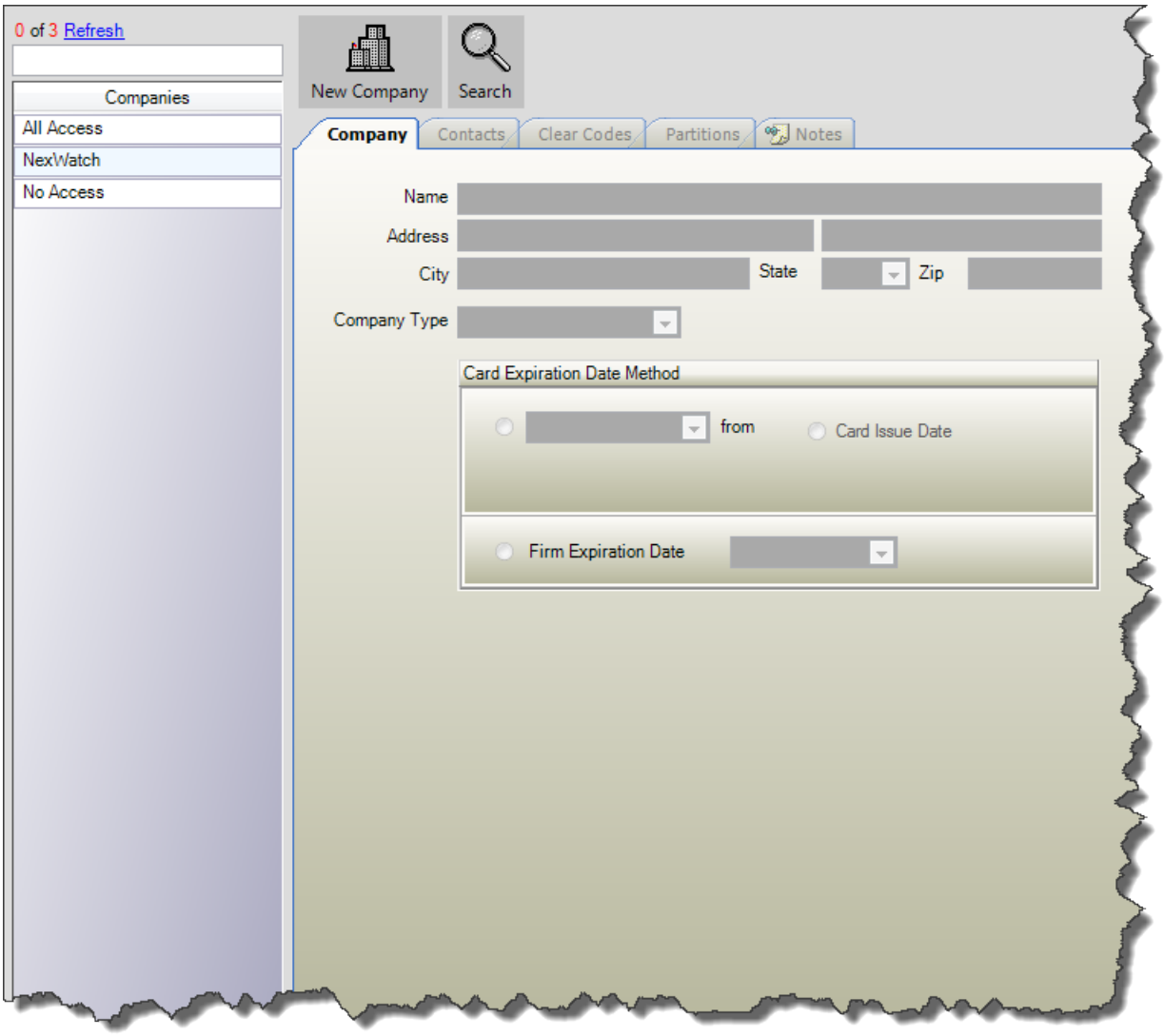
3. If you want to print the selected card, select **Pro-Watch Card**. If you want to print the entire badge record, select **Pro-Watch Badge**.

2.20 Administration

Pro-Watch Advanced Badge Manager administration is based on the Pro-Watch Company database element. A Pro-Watch Company allows many Clearance Codes to be grouped together; when a company is assigned to a card, the card is given all of the Clearance Codes that are assigned to that Company.

2.20.1 Companies

Company access is managed from the Company Information screen. Click **Companies** in the Navigation pane:



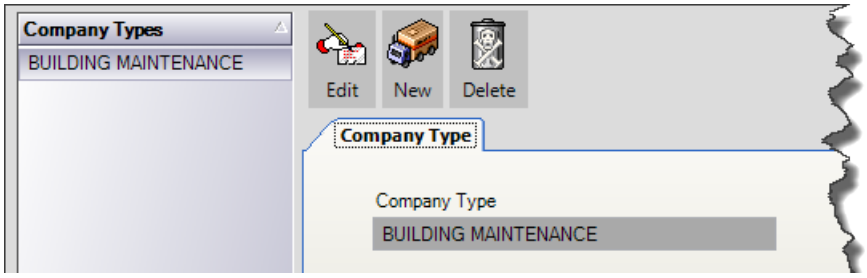
Use the following table descriptions to maintain the vital information about the companies at the airport:

Tab	Field	Description
Company	Name and address	Company's name and address.
	Company Type	Company's function at the airport. For example, security service, food service, etc. This field is useful for reporting.
	Card Expiration Date Method	Two options: either select a number of months and a start date, or select **Firm Expiration Date** and the actual date from the calendar dropdown.
Contacts	Add Contact	Click to add a company contact record. The Contact record includes the contact's signature with which new badge applications are verified. You can import the signatures of authorized signers from the file system, scan them in, capture them by using a signature pad device, or import them from Pro-Watch.
	Print Contact	Click to print the company contact record.
	Display Filter Row	Click to display the filter configuration for the row.
Clear Codes	N/A	This tab displays a list of all of the Pro-Watch Clearance Codes that are configured for the Company database element that is assigned to the company. Use the right and left arrow buttons in the middle of the screen to assign or remove the Clearance Codes you desire.
Partitions	N/A	This tab displays a list of all of the Pro-Watch partitions that are configured for the Company.

Tab	Field	Description
Notes	N/A	Enter any useful notes about this badge holder. When you modify or add a note, the previous note moves to the Note History section. The Note History section logs all of the badge holder's notes, the author of the note, and the date of the note. Select the Alarm Note checkbox if you would like to view the alarm note as you scroll through the list of companies.

2.20.2 Company Types

Company types are useful for grouping companies for reporting purposes. Click **Company Types** in the Navigation panel:



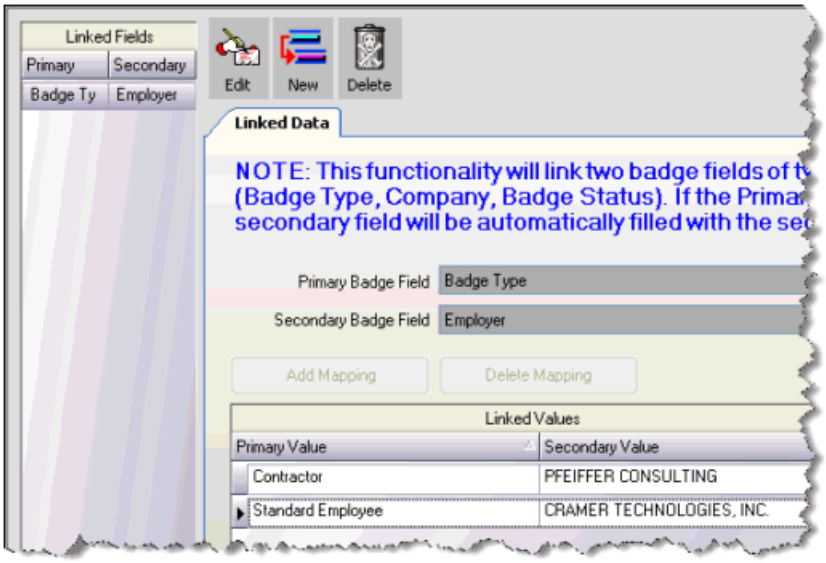
Create and edit company types by clicking the **Save/Edit**, **New** and **Delete** icons.

2.20.3 Linked Badge Fields

Click **Linked Badge Fields** in the navigation pane to link two badge drop-down and resource fields (the eligible fields are Badge Type, Company, and Badge Status).

For example, the linked badge field screen below shows the Badge Type selected as the primary field and the Badge Status as the secondary field. In this case, the Badge Type and Badge Status fields are linked, so that when "Contractor" is selected as the Badge Type, the Badge Status field is automatically populated with "Pfeiffer Consulting." Similarly, when

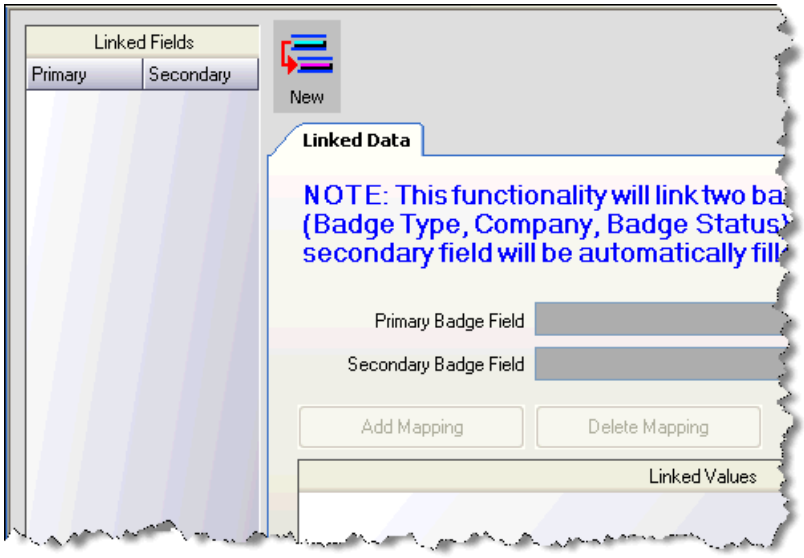
"Standard Employee" is selected as the Badge Type, the Badge Status field is automatically populated with "Cramer Technologies."



Note: The user who is linking fields must have Pro-Watch program access to **Administration > Badge Activities > Badge Fields**.

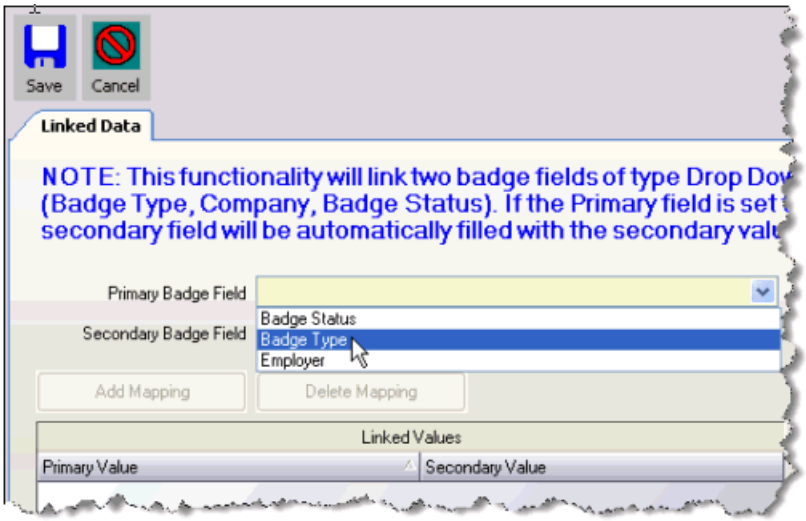
Follow these steps:

1. Select **Linked Badge Fields** on the main screen to display the Linked Badge Fields screen.

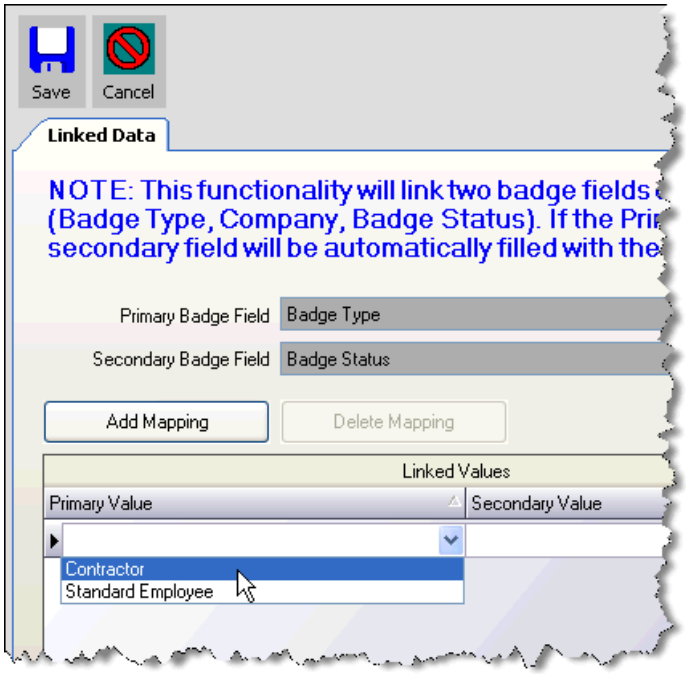


2. Click the **New** icon at the top of the screen to activate the Primary Badge Field and Secondary Badge Field.

3. From the Primary Badge Field drop-down list, select the field you want to be the primary field.



4. From the Secondary Badge Field drop-down list, select the field you want to be the secondary field.
5. Click the **Add Mapping** button to select the primary and secondary field values. From the Primary Value drop-down list, select the desired value:



Then, select the desired value from the Secondary Value drop-down list.

6. Repeat steps 2 through 5 to create as many additional field links as you desire.

7. Click the **Save** icon at the top of the screen to save the links.

Note: As stated on the Linked Badge Fields screen, you must restart Pro-Watch Advanced Badge Manager to activate the links you have created.

2.20.4 Linked Null Fields

You can also link two NULL badge drop-down and resource fields. Note that if the Primary Field is not NULL, the Secondary Field must not be NULL.

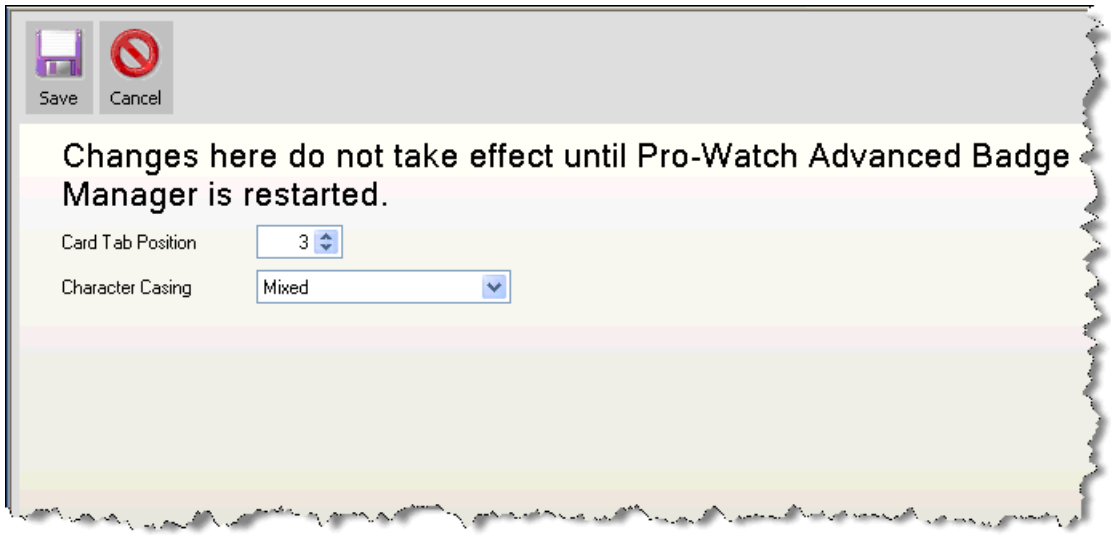
To link two NULL badge fields, select Linked NULL Fields from the main screen and follow the same steps given in the preceding section for linking badge fields.

Note: As stated on the Linked Badge Fields screen, you must restart Pro-Watch Advanced Badge Manager to activate the links you have created.

2.20.5 Application Settings

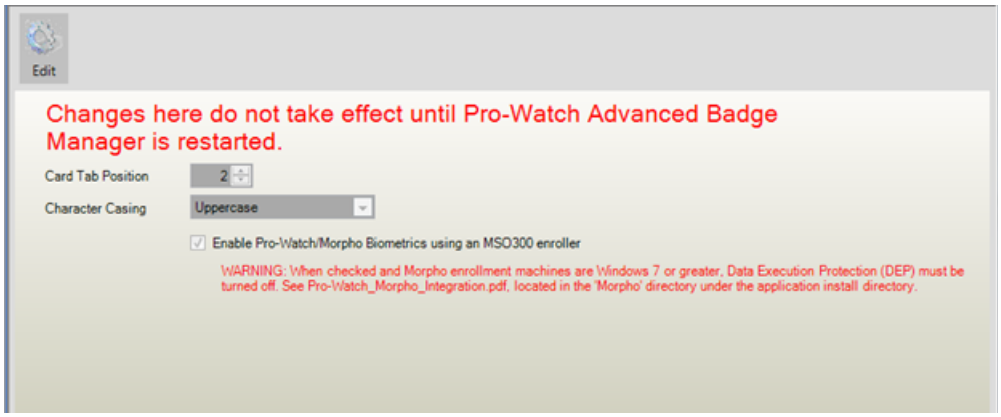
The Application Settings feature enables a Pro-Watch root user to change two Pro-Watch Advanced Badging application settings:

- the position of the Card tab in the Badging screen,
- the character casing (upper case or mixed case) for data entry.



Note: As stated on the Linked Badge Fields screen, you must restart Pro-Watch Advanced Badge Manager to activate the settings you've created.

If the **Morpho** biometric reader option is installed and activated, this screen may look like this:



2.20.6 Compliance Reports

For compliance reports, visit the following links in this document:

- "Compliance Reports" are available in several formats. See Exporting a Report, page 8 for a list of format choices.
- Opening Multiple Instances of Advanced Badging, page 95

2.21 Opening Multiple Instances of Advanced Badging

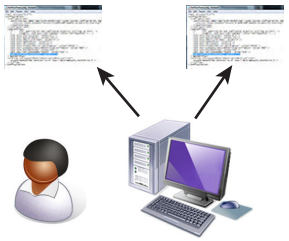
The Advanced Badging (AB) module's default configuration allows a single user or a group of multiple users connected to the same AB server to open only one instance of the application at any one time. This is to prevent simultaneous changes to the AB database made by a single user or a group of users.

However, there may be cases when the operators using Citrix or VMWare may want to launch multiple instances of Advanced Badging.

Here are two such multiple-instance scenarios:

Figure 2-4 Single User, Multiple Instances of Advanced Badging

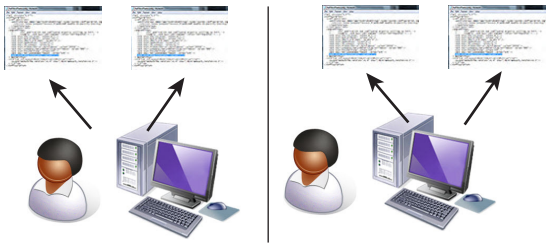
Scenario 1
Multiple Instances of AB
Open in Different Windows



1 User on 1 Workstation

Figure 2-5 Multiple Users, Multiple Instances of Advanced Badging

Scenario 2
Multiple Instances of AB
Open in Different Windows



Multiple Users on Multiple Workstations

Follow these steps to allow multiple instances of Advanced Badging:

1. Go to your **Advanced Badging** directory and open the file named **BadManAP.exe.config**:

```
<?xml version="1.0"?>
<configuration>
  <configSections>
    <sectionGroup name="applicationSettings" type="System.Configuration.App
      <section name="HoneywellAccess.ProWatchAP.BadMan.Properties.Settings"
    </sectionGroup>
  </configSections>
  <appSettings>
    <!--   User application and configured property settings go here.-->
    <!--   Example: <add key="settingName" value="settingValue"/> -->
    <add key="RegistryKeys" value="4.1"/>
    <add key="QueryTimeout" value="240"/>
    <add key="SmartCardFinger" value="1"/>
    <add key="AppRunMode" value="0"/>
    <add key="PW_Connect" value="1"/>
    <add key="ProWatchServerLoginTimeout" value="30000"/>
    <add key="CompanyClearCodeModificationTimeout" value="600"/>
    <add key="EncoderSleep" value="100"/>
    <add key="NoFlyDatabaseTimeout" value="120"/>
    <add key="SingleInstance" value="1"/>
  </appSettings>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>
  </startup>
</configuration>
```

2. Change the value of the “SingleInstance” key from “1” (one) to 0” (zero) to allow for multiple AB instances and save the file.
3. To switch back to the single-instance option, change “0” back to “1” and save the file.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Alarm Monitor

3

In this chapter ...

Overview
Monitor Dispositions, Instructions, and Response Codes
Alarm Monitor Windows and Controls
Using the Alarm Monitor
Processing Events on a Map

3.1 Overview

The Alarm Monitor enables you to view and act upon the real-time status of alarms as they occur.

An alarm page displays event types. See "Overview" for a detailed discussion of alarm pages.

For each event type, the specific alarms appear in order of priority and occurrence. The title bar displays the total number of alarms existing for all alarm pages, as well as a count of the number of unacknowledged and acknowledged alarms.

The Alarm Monitor also provides an Alarms Rollup function that displays multiple events for a single logical device in a single line. A counter field in that line indicates the total number of events received.

Events assigned to an event type are subject to alarm rollup under the following conditions:

- Rollup Events check box is selected on the **Event Type** configuration dialog box. See "DBC - Event Types".
- Rollup number is selected on the alarm page. See "Overview". You can view rolled-up events on the alarm page.

3.1.1 VMS Client

If VMS is used, you must install VMS client on the client machine.

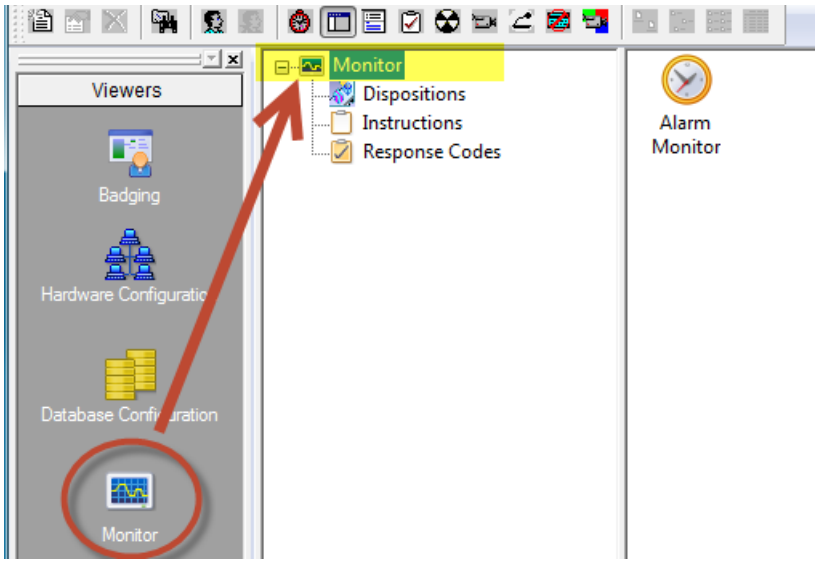
3.2 Monitor Dispositions, Instructions, and Response Codes

Before you use the Alarm Monitor, you must define dispositions, instructions, and response codes that the alarm monitor will recognize.

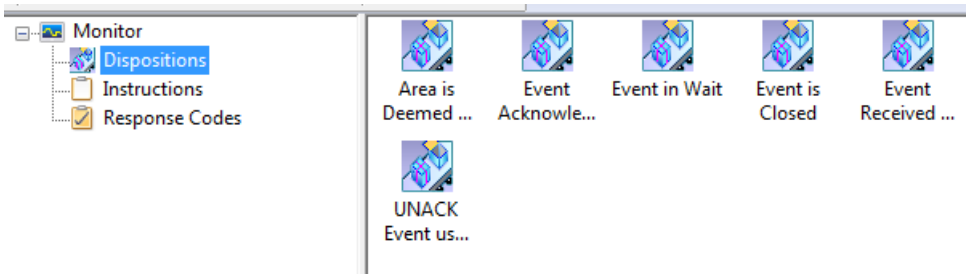
3.2.1 Dispositions

A disposition indicates the state of the alarm. *Acknowledged* and *Cleared* are system defaults. You can create additional dispositions to suit your needs.

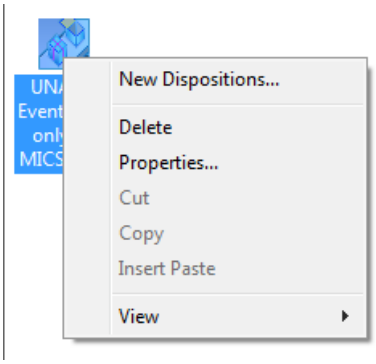
1. From the Monitor menu, click **the plus sign** before the **Monitor** icon to display all the available sub-folders:



2. Click the **Dispositions** icon to display the icons of the currently-configured dispositions in the right pane of the Pro-Watch window.



3. Right-click a disposition icon to display the shortcut menu (if no dispositions have been created yet, right-click anywhere in the right pane):



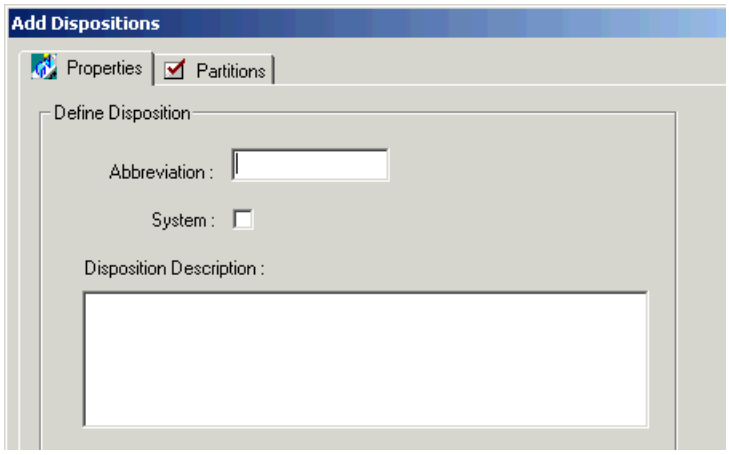
4. Use the following table to select a function:

Click...	To...
New Dispositions...	Select to add a new disposition. See "Adding or Editing a Disposition".
Delete	Select to delete a current disposition. See "Deleting a Disposition".
Properties...	Select to edit a current disposition configuration. See "Adding or Editing a Disposition".
View	Select to change the way the icons are displayed in the Pro-Watch window.

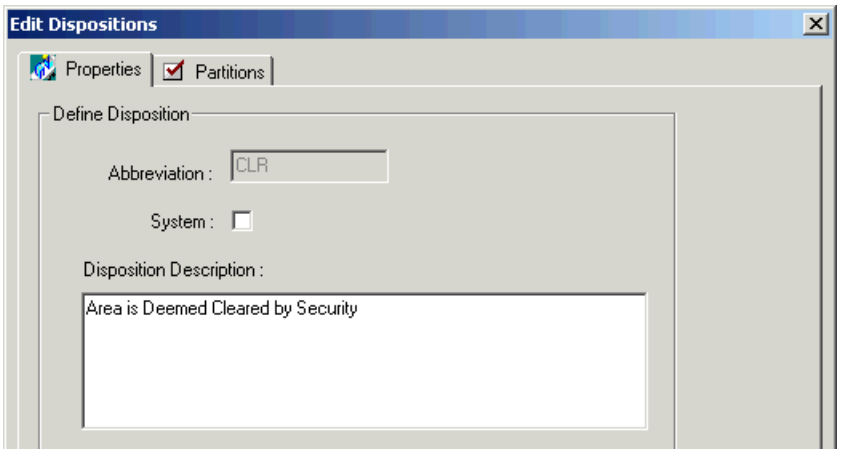
3.2.1.1 Adding or Editing a Disposition

1. To *add* a new disposition, right-click anywhere in the right pane of the Pro-Watch window and select **New Dispositions** to display the Add

Dispositions dialog box:



To *edit* an existing disposition, right-click the disposition icon and select **Properties** to display the Edit Dispositions dialog box:



2. Use the following property descriptions to complete either dialog box:

Field	Description
Abbreviation	Abbreviation for the disposition.
System	Displayed only for those dispositions that are used by the system. No action is required on the part of the user.
Disposition Description	Description of the disposition.

3. Click **OK** to accept the new or edited disposition.

3.2.1.2 Deleting a Disposition

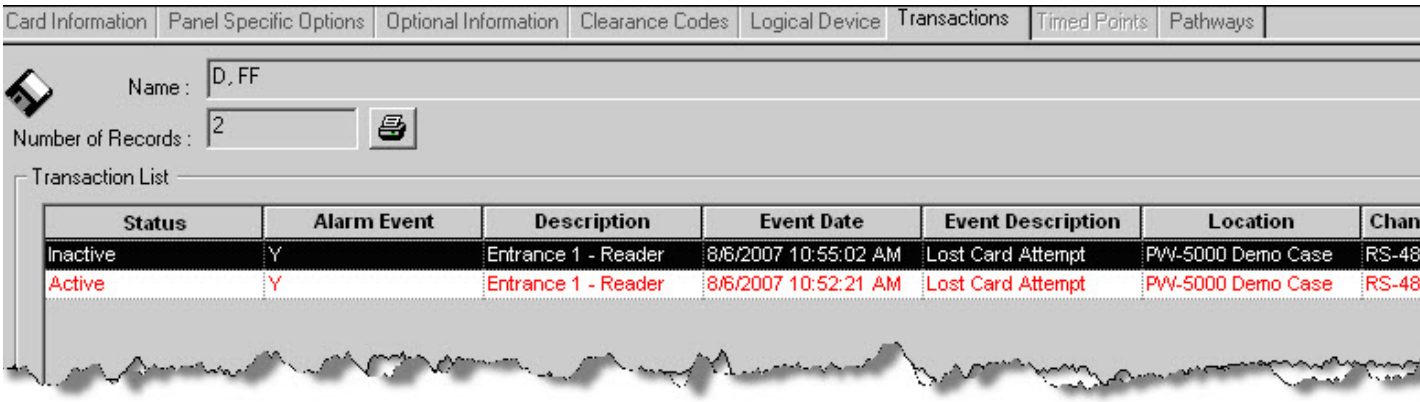
1. In the right Pro-Watch pane, right-click the disposition icon you want to delete.
2. Select **Delete**.
3. A confirmation box for the action appears. Click **Yes** to delete.

Note: System dispositions cannot be deleted.

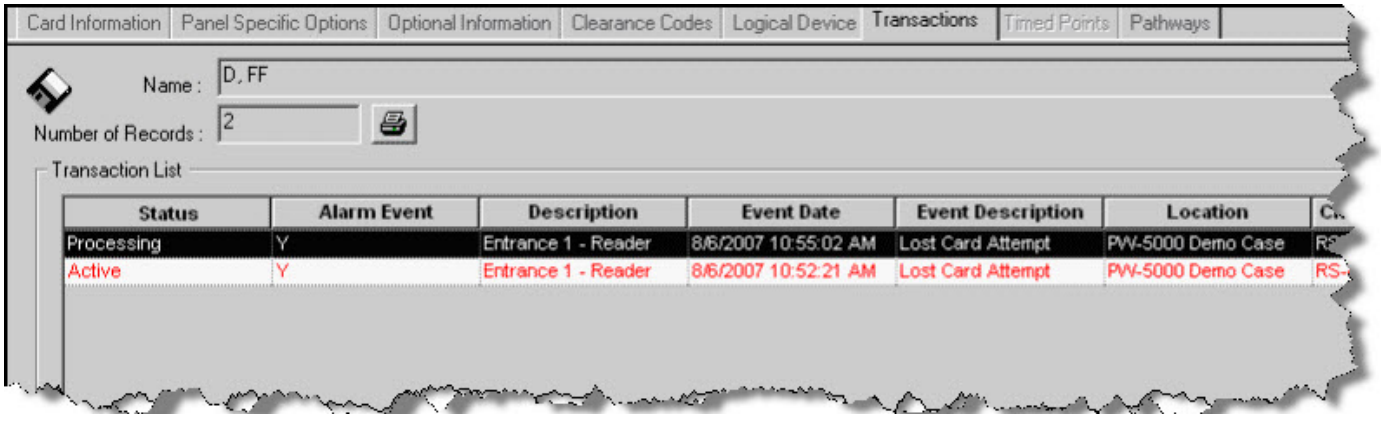
3.2.1.3 Restoring Cleared Events

Pro-Watch functionality includes the ability to restore a cleared event. Only inactive (cleared) alarm events can be moved to an unacknowledged state.

Before you restore an event, its status is **Inactive**.



To restore a cleared event back to the system from any of the transaction tabs (card, site, logical device properties), right-click on the event and select **Unacknowledge event** from the context menu. The status changes to **Processing**.

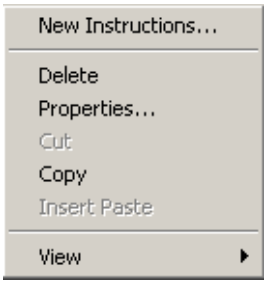


If you navigate to another tab and come back to the Transaction tab, the status for this event will be **Active**.

3.2.2 Instructions

An instruction creates a brief message that describes how to respond to an event by providing the correct procedure for it.

1. From the Monitor menu, click the plus sign before the **Monitor** icon to display all the available sub-folders.
2. Click the **Instructions** icon to display the icons of the currently-configured instructions in the right pane of the Pro-Watch window.
3. Right-click an instruction icon to display the shortcut menu (if no instructions have been created yet, right-click anywhere in the right pane):



4. Use the following table to select a function:

Click...	To...
New Instructions...	Select to add a new instruction. See "Adding or Editing an Instruction".
Delete	Select to delete a current instruction. See "Deleting an Instruction".
Properties...	Select to edit a current instruction configuration. See "Adding or Editing an Instruction".
Copy	Select to copy an instruction. You can then paste it by right-clicking and selecting Paste from the pop-up menu. To edit a copied and pasted instruction, right-click on the instruction and select Properties.
View	Select to change the way the icons are displayed in the Pro-Watch window. See "A confirmation box for the action appears. Click Yes to delete.".

3.2.2.1 Adding or Editing an Instruction

1. To *add* a new instruction, right-click anywhere in the right pane of the Pro-Watch window and select **New Instructions** to display the Add Instructions dialog box.

   To *edit* an existing instruction, right-click the instruction and select **Properties** to display the Edit Instructions dialog box.

2. Use the following property descriptions to complete either dialog box:

Field	Description
Description	Description of the instruction.
Instruction Procedure	The instruction for the operator to run the specific Pro-Watch procedure.
Instruction Message	Text to display to the operator.

3. Click **OK** to accept the new or edited instruction.

3.2.2.2 Deleting an Instruction

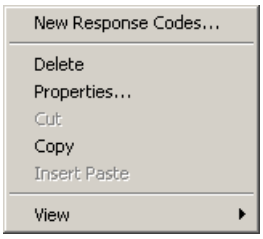
1. In the right Pro-Watch pane, right-click the instruction icon you want to delete.
2. Select **Delete**.
3. A confirmation box for the action appears. Click **Yes** to delete.

3.2.3 Response Codes

A response code is a prepared response that can be used to reply to an alarm. For example, “Alarm verified; police notified” is a response code. You can also create a response message that explains the response more fully.

Note: You can also invoke the Force Note function in the event type maintenance. Force Note by event type forces the dispatcher to enter what they did before the alarm went off. The Force Note may include a response code and a typed text.

1. From the Monitor menu, click the plus sign before the **Monitor** icon to display all the available sub-folders.
2. Click the **Response Codes** icon to display the icons of the currently-configured response codes in the right pane of the Pro-Watch window.
3. Right-click a response code icon to display the shortcut menu (if no response codes have been created yet, right-click anywhere in the right pane):



4. Use the following table to select a function:

Click...	To...
New Response Codes...	Add a new response code. See "Adding or Editing a Response Code".
Delete	Delete a current response code. See "Deleting a Response Code".
Properties...	Edit a current response code configuration. See "Adding or Editing a Response Code".

Click...	To...
Copy	Copy a response code. You can then paste it by right-clicking and selecting Paste from the pop-up menu. To edit a copied and pasted response code, right-click on the response code and select Properties.
View	Change the way the icons are displayed in the Pro-Watch window. See "Alarm Monitor Windows and Controls".

3.2.3.1 Adding or Editing a Response Code

1. To *add* a new response code, right-click anywhere in the center pane of the Pro-Watch window. Select **New** to display the Add Response Codes dialog box.

   To *edit* an existing response code, either double-click the response code in the right pane or right-click it and select **Properties** to display the Edit Response Codes dialog box.
2. Use the following property descriptions to complete either dialog box:

Field	Description
Description	Description of the response code.
Response Code Message	The text that will be entered into the alarm response box.

3. Add or delete partitions as needed from the Partitions tab.
4. Click **OK** to accept the new or edited response code.

3.2.3.2 Deleting a Response Code

1. In the right Pro-Watch pane, right-click the response code icon you want to delete.
2. Select **Delete**.
3. A confirmation box for the action appears. Click **Yes** to delete.

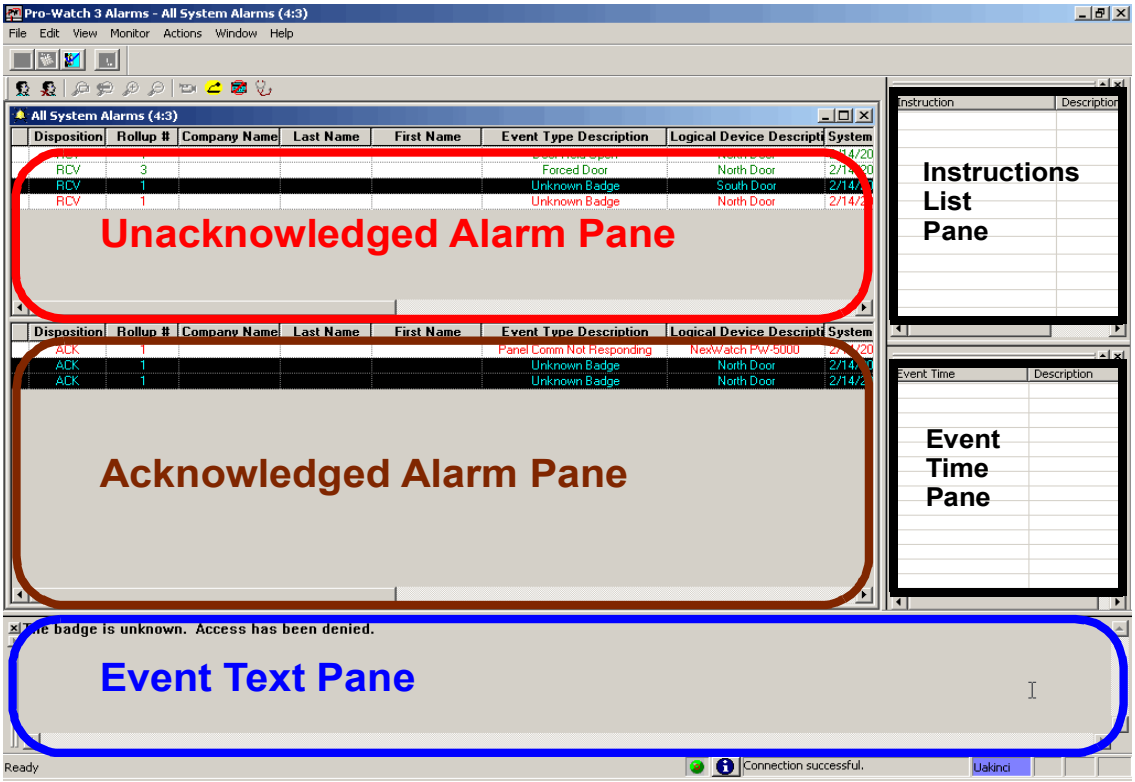
3.3 Alarm Monitor Windows and Controls

Select **File > Wizard** from the main menu (if the Wizard home page is not already displaying). On the Wizard home page double-click the **Alarm Monitor** link in the **Permissions Manager** group to display the **Alarm Monitor** screen in a separate window.

The Alarm Monitor screen consists of five window panes, two toolbars, and seven drop-down lists.

3.3.1 Window Panes

The following illustration identifies the Alarm Monitor screen's window panes:



- **Unacknowledged Alarm Pane** (upper-left pane) – Displays alarms in real time in the color defined for the event type. Alarms are listed in decreasing order of priority, and in reverse chronological order. The highest priority alarm is listed the most recent. You can also set the Alarm Monitor to beep when each alarm occurs. If a wave-format sound file is assigned to the alarm's event type, then the prerecorded wave file will play before the beep begins.
- **Acknowledged Alarm Pane** (below the Unacknowledged pane) – Lists all the acknowledged alarms.

- **Instructions List Pane** (upper-right pane) – Displays any instructions associated with the selected alarm. To set up instructions for a particular alarm point see "Instructions".
- **Rollup or Event Time Pane** (lower-right pane) – Lists the event time and description of alarms using the rollup function. To view this detail, right-click the alarm and select **Rollup Detail** from the pop-up menu.
- **Event Text Pane** (bottom pane) – Displays event text and status messages.

3.3.2 Toolbars

The **Alarm Toolbar** functions are user-definable on the class and user levels. See "DBC - Classes" in Chapter 36 or "DBC - Users" in Chapter 58 for instructions.

Note: Pro-Watch ships with the Acknowledge Alarm, Clear Alarm, Event Response, and Card Holder picture tool bar buttons configured.

Double-click the Alarm Monitor icon to launch the monitor window.

The **Alarm Monitor Toolbar** provides the following functions:

Alarm Monitor Toolbar Function	Description
Logon Shadow User	Logon over current user without having to log out of Windows. This option is good for an administrator or supervisor with special privileges beyond the person who is currently logged on.
Logoff Shadow User	Logs off Shadow User mode and returns to previous user's logon credentials.
Zoom Selected Area	Enlarges selected area.
Zoom Previous	Returns to previous zoom setting.
Zoom Closer	Magnifies selected area.
Zoom Away	Zooms out from selected area.

Alarm Monitor Toolbar Function	Description
CCTV Controls	Allows you to visually coordinate alarms with a surveillance camera and a selected monitor, switch the video of the selected camera to the selected monitor, set a preset, and Pan/Tilt, Zoom, Focus, and set the Iris of the selected camera for the best video contrast.
Intercom Controls	Enables you to configure a “Primary intercom” and its respective “Secondary Intercom.”
Void Card	Under certain security circumstances you may need to void a card of an employee who has just been terminated. This function enables you to do exactly that without using the badge module.
Hardware Status Groups	Views groups of Logical Devices and their associated status in real time.

3.4 Using the Alarm Monitor

3.4.1 Monitoring Alarms

When an alarm occurs in Pro-Watch, the alarm initially displays in the Unacknowledged Alarm pane.

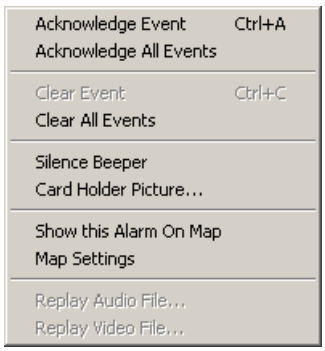
Note: The following conditions must exist for the alarm to appear in the Unacknowledged Alarm pane:

- The alarm's alarm page must include the alarm's channel and event type.
- The system must be in the time zone assigned to the event type.
- The system must be in the time zone assigned to your workstation in the alarm page.

To check the alarm's page status, select **View > Page Status**.

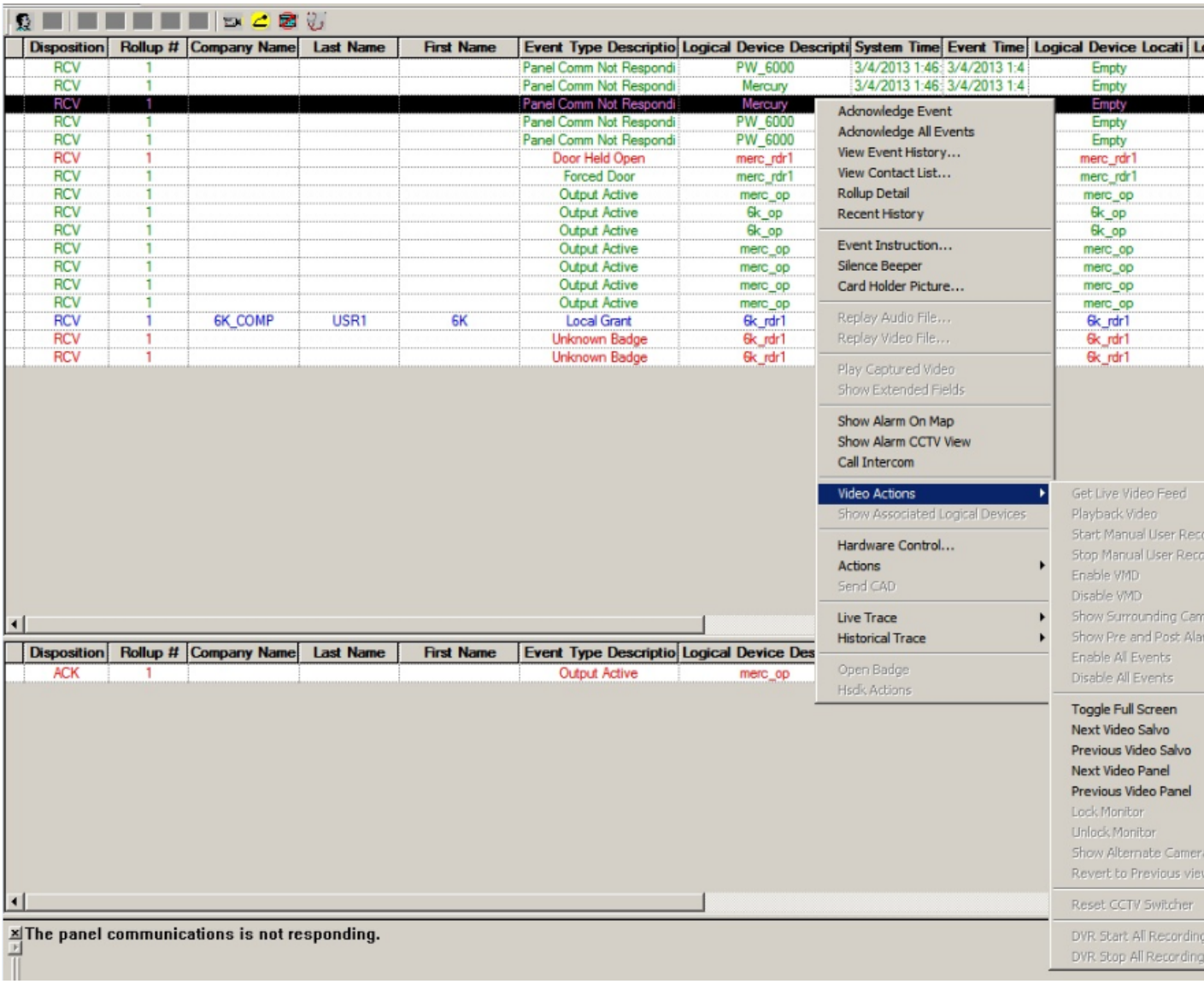
You can perform actions from the Alarm Monitor in two ways:

- Click **Monitor** in the menu bar at the top of the Alarm Monitor page to display the following menu:



- Select an alarm event and right click to display the following **pop-up menu**. The exact content of this pop-up menu will differ slightly from one panel and reader/logical-device to another. Here is how it looks like for the **Mercury panel**:

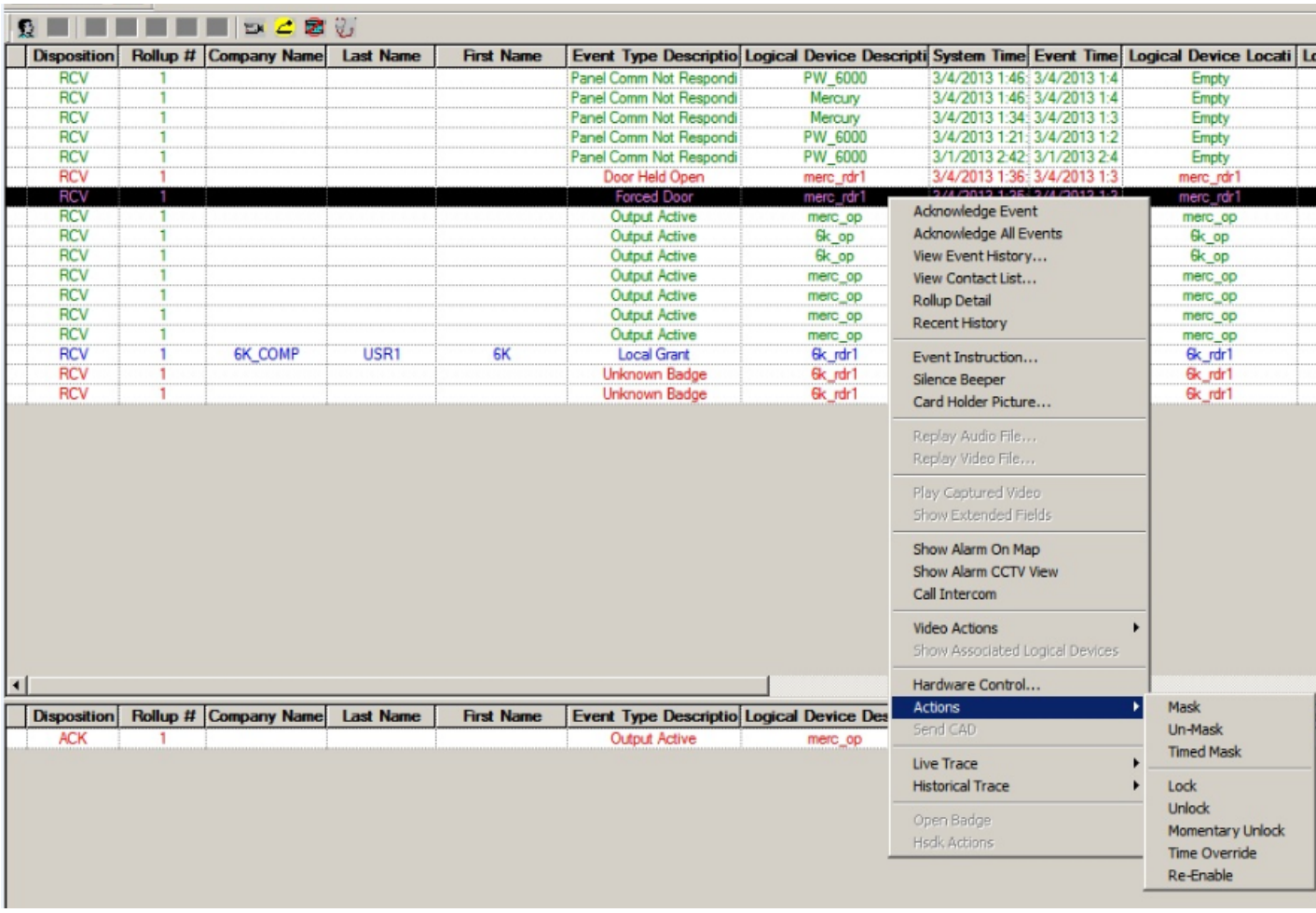
Figure 3-1 Alarm Event Options for Mercury Panel



The **Live Trace** and **Historical Trace** features shown in this display appear only if the Pro-Watch Trace-On feature is purchased with the software. **Actions** will display only if the panel is online.

This is how the same pop-up menu looks like for a **Mercury reader** connected to the downstream of the same Mercury panel:

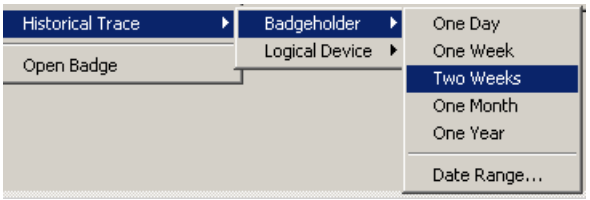
Figure 3-2 Alarm Event Options for Mercury Reader



Use the following table to choose the desired action:

Monitoring task	Description
Acknowledge Event	Changes the status of an event to Acknowledged.
Acknowledge All Events	Changes the status of all current unacknowledged events to Acknowledged.
Clear Event	Clears an acknowledged event from the Alarm Monitor.
Clear All Events	Clears all acknowledged events from the Alarm Monitor.

Monitoring task	Description
Silence Beeper	Silences the alarm beep until another alarm is received.
Card Holder Picture...	Displays the photo of the card holder associated with an event.
Show this Alarm On Map or Show Alarm On Map	Displays the event on the appropriate map.
Map Settings	Adjusts the size of the map associated with the selected alarm.
Replay audio file	Replays the audio file associated with the selected alarm.
Replay video file	Replays the video file associated with the selected alarm.
Play captured video	Plays the video file for an alarm that is associated with a digital video recorder.
Rollup Detail	Displays an event time and a description for each rolled-up event in the lower right pane.
Recent History	Displays event history on the selected logical device.
Event Instruction	Allows the operator to log a response to an event either by entering text in the text field or selecting a pre-written response from the Response Code drop-down list.
Show alarm CCTV view	Displays the Select CCTV View defined for the point in alarm on the alarm grid. If the view is not defined, Pro-Watch uses the Select CCTV View defined for the associated Logical Device. If no Select CCTV View is defined, no view is displayed.
Call intercom	Initiates an intercom call from Primary Intercom Station defined for the user's workstation to the intercom defined for the Logical Device associated with the point in alarm. If no Primary Intercom Station is defined for the workstation or there is no Intercom Station for the logical device, no call is initiated.

Monitoring task	Description
Hardware Control...	Enables you to invoke actions on logical devices or groups of logical devices that are not necessarily associated with an alarm displayed on the Alarm Monitor. See "Invoking Actions on Devices Not Associated with Particular Alarms".
Actions	Enables you to perform various actions on a logical device or groups of logical devices. See "Invoking Actions on Devices Associated with Alarms".
Send CAD	Enables you to send TCP/IP data packets, both old and new, to the CAD server when this function is enabled. If catintf service is available, the function uses the old format. If cadintf2 service is available, the function uses the new packet format.
Live Trace	Enables you to display (in a separate Alarm Monitor window) all current and future alarm events that are associated with a particular badgeholder or Logical Device. Select Live Trace > Badgeholder or Live Trace > Logical Device to display the separate Alarm Monitor window: 
Historical Trace	Enables you to display (in a separate Alarm Monitor window) all past alarm events occurring in a specified historical range that are associated with a particular badgeholder or Logical Device. Select Historical Trace > Badgeholder or Historical Trace > Logical Device to display the separate Alarm Monitor Window: 
Open Badge	Enables you to go directly to the badgeholder data associated with the selected event. (The selected event must have a badge associated with it, like a card event). You must have permission to use this function.

3.4.1.1 Contact Lists

Pro-Watch now includes functionality that enables Alarm monitor users to look up contacts associated with an alarm. Once a group of badge holders have been set up as contacts, you can associate contacts at different hardware levels (Site, Channel, Panel (PW-5000), Logical device, Point) much like extended instructions. Now when the Alarm monitor user looks up a contact list, all badge holders linked to its hardware hierarchy are displayed as contacts.

Table 3-1 lists the fields that need to be added to badge fields for the contact list functionality to function properly.

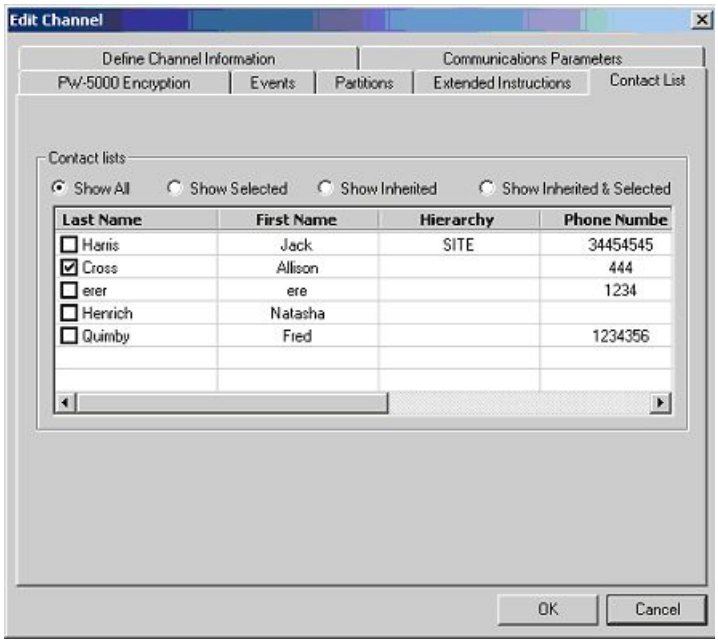
Table 3-1 Contact List Required Fields

Column name	Status	Type	Length
BADGE_ELIGIBLE_TO_BE_CONTACT	New field; required. This is the most important field; if this field is absent, the contact list functionality will not function at all. When this field is checked, the badge user is eligible to be a contact.	bool	N/A
LNAME	Existing field; required	varchar	40
FNAME	Existing field; required	varchar	40
BADGE_OFFICEPHONE	Existing field	varchar	20
BADGE_ADDRESS1	Existing field	varchar	40
BADGE_PASSCODE	New field	varchar	40
BADGE_PASSWORD	New field	varchar	40

Notes:

- Use Badge Builder to add the fields in this table to the badge screen.
- Only badge holders whose BADGE_ELIGIBLE_TO_BE_CONTACT field is selected can appear as a contact.
- The Contact List tab appears in points only for Channels, Panels, and Logical Devices.

You can access the Contact List tab via the properties for any node in the hardware hierarchy (site, channel, panel, logical device, or point).



The Contact List information can be displayed in a number of ways:

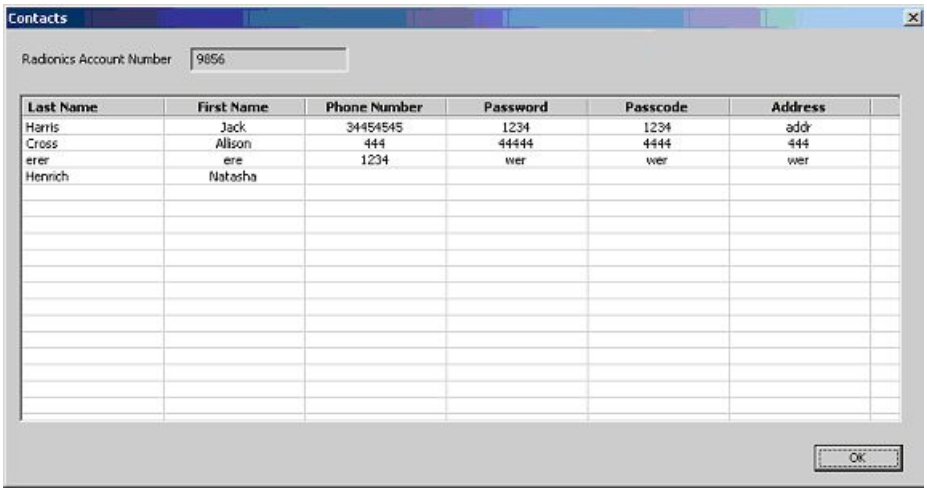
- Show All—displays all contacts in the Pro-Watch database.
- Show Selected—displays only selected contacts.
- Show Inherited—displays only inherited contacts.
- Show Inherited & Selected—displays both inherited and selected contacts.

The following information is listed for each contact:

- Last Name
- First Name
- Hierarchy—Indicates whether the field was inherited from hardware nodes higher up in the hierarchy. In the figure above, the contact Jack Harris was inherited from SITE.
- Phone Number
- Address
- Password
- Passcode

In the Alarm Monitor, a new context menu called **View Contact List** displays all contacts for a specified alarm. When you select the **View Contact List** context

menu, a dialog displays contacts set up at all levels of the hardware hierarchy.



3.4.1.2 Wait State

Pro-Watch provides two kinds of wait state functionality:

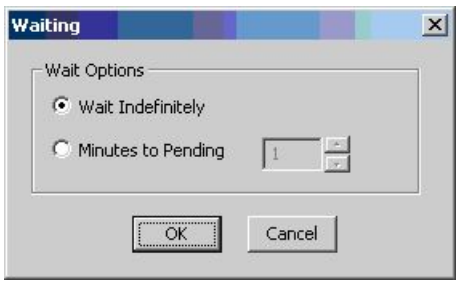
- Timed wait
- Indefinite wait

Only acknowledged events can be put in a wait state.

All wait state events appear in the bottom of the Alarm Page and have a priority of 9000. When an event is put in an indefinite wait state it appears in the bottom window of the Alarm Page and stays there until user deals with it. If the user puts the event in a timed wait state, then the event remains in the wait state for the selected time and when the wait time expires, the event comes back in the top window (Unacknowledged window) of the Alarm page.

To put an event or group of events in the Alarm Monitor into a wait state:

1. Right-click on the selection and click **Wait** or **Wait Indefinitely** to display the Waiting dialog box.



2. Select **Wait Indefinitely** if you're not sure how long you want the wait state to be

OR

3. Select **Minutes to Pending** to specify how long you want the wait state to be.
4. Click **OK**.

Note: Only users with permissions can put an event into a wait state, timed or indefinite.

3.4.2 Acting on Logical Devices

Information received on the Alarm Monitor may prompt you to perform actions on a logical device or groups of logical devices. The Alarm Monitor enables you to perform these actions in two ways:

- Invoke an action only on the logical devices associated with a particular alarm received on the Alarm Monitor.
- Invoke an action on any logical device or group of logical devices that is not associated with any alarms received on the Alarm Monitor.

3.4.2.1 Invoking Actions on Devices Associated with Alarms

An alarm may indicate a problem with a specific logical device that requires action. For example, a broken door may be causing a forced door alarm. You can initiate a mask action to temporarily remove the door from the access system in order to prevent continuous alarms during the repair of the door.

To perform this and other actions listed in the table below, follow these steps:

1. Double-click on an **Action Monitor** icon to display the Pro-Watch alarms screen in a new window.
2. Click to select the event associated with the logical device you want to act upon, and select **Actions > [action]**. Alternatively, right-click the alarm you want to act upon and select **Actions > [action]**. Both methods display an action dialog box.
3. In the dialog box, select the device you want to act upon. Or, if you want to act upon all applicable devices, select the **All Devices** check box.
4. Select the **Show Dialog ONLY on SHIFT Key** check box if you want this action to invoke in the future without displaying the dialog box except when you press the SHIFT key.

Notes:

- If the action note function in User/Class Program Functions is set to "Enforce," then this dialog box will appear regardless of whether the "Show Dialog ONLY on SHIFT Key" check box is selected. The "Enforce" setting also disables the **OK** button until a note is entered.

- Galaxy door alarms are associated with a DCM (door control module). The DCM must be set up as a logical device. Use the DCM property sheets to configure a DCM as a logical device.

The following table describes the actions you can invoke upon logical devices from the Alarm Monitor:

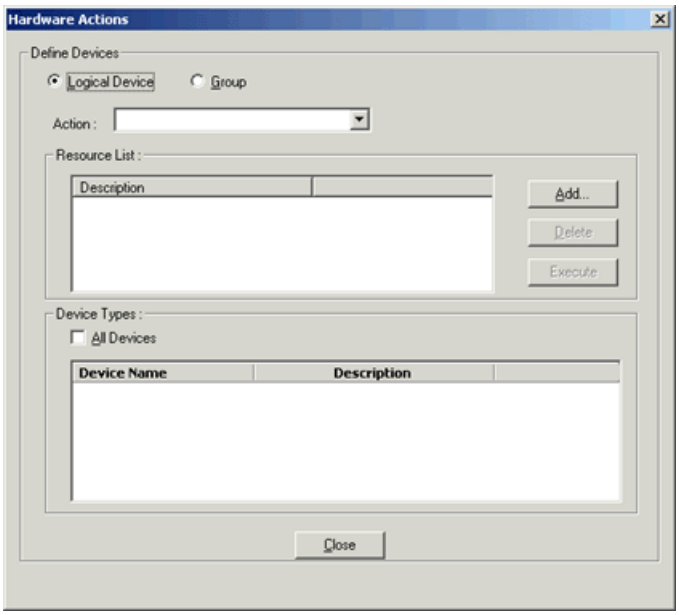
Alarm action	Description
Mask/unmask	Allows the operator to remove (mask) a device from the access system or restore (unmask) a device to the access system.
Activate/de-activate	Activates or de-activates an output.
Pulse	Pulses an output.
Time activate	Activates an output for a set duration.
Lock/unlock/momentary unlock	Locks, unlocks, or momentarily unlocks a reader associated with the selected logical device.
Time override	Specifies a period of time in minutes during which a door can be open without generating an alarm.
Re-enable	Sets the door on the selected logical device to its default state.

3.4.2.2 Invoking Actions on Devices Not Associated with Particular Alarms

The Hardware Control function on the Actions menu enables you to invoke actions on logical devices or groups of logical devices that are not necessarily associated with an alarm displayed on the Alarm Monitor.

Follow these steps:

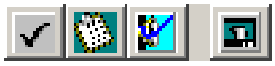
1. Either select **Actions > Hardware Control** or right-click anywhere in the alarm display and select **Hardware Control**. The Hardware Actions dialog box appears:



2. Select the **Logical Device** option button for an action on one or more ungrouped logical devices. Alternatively, select the **Group** option button for an action on a specified group of logical devices.
3. Select an action from the Action drop-down menu.
4. Click **Add** in the Resource List box to display a list of available devices or device groups to act upon, and select the device(s) or group(s) you want. The Device Types box in the Hardware Actions dialog box displays the physical devices or groups that are eligible for the action you selected in the Action field. Note that if no groups are currently configured, you can create one:
    - Click **Add** in the Groups dialog box to display the Add Groups dialog box.
    - Enter a group description.
    - Click **Add** to display a list of available devices.
    - Select the devices you want and click **OK**. Click **OK** again to return to the Groups dialog box.
5. In the Device Types dialog box, either select the **All Devices** check box or select specific devices from the list below the check box.
6. Click **Execute** to perform the selected action on the selected devices.
7. Click **Close**.

3.4.3 Using the Alarm Monitoring Tasks Tool Bar

You can access some of the alarm monitor task options through the Alarm Monitoring Tasks tool bar:



Task Button	Description
	Acknowledge. Click this button to acknowledge the alarm and move it to the bottom grid.
	Event Response. Click this button to log a response to an event.
	Clear. Click this button to delete an acknowledged alarm event from the bottom grid.
	Photo. Click this button to see the photo of the badgeholder who triggered the alarm event.

3.4.4 Using the File Menu

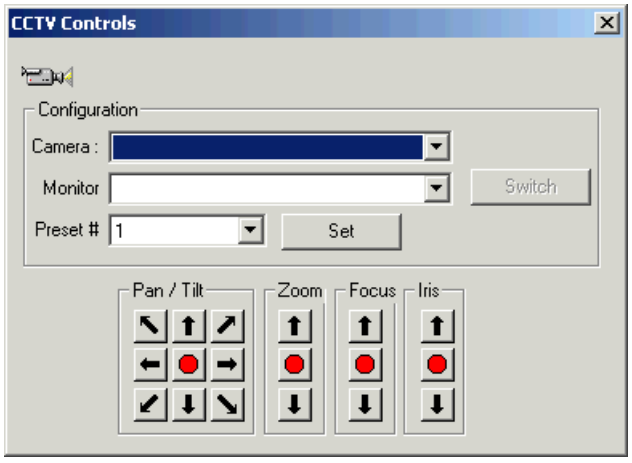
The Alarm Monitor File menu provides administrative tools.

3.4.4.1 Comm Status

Comm Status displays the status of the Alarm Monitor's connection to the Pro-Watch server. The dialog box shows the date, time, error code (if any), and text of the network status messages sent during the connection.

3.4.4.2 CCTV Controls

CCTV Controls enable you to select a camera and monitor, switch the camera's video to the selected monitor, view presets, pan/tilt, zoom, focus, and change the iris of the selected camera.



1. Select the camera from the drop-down Camera list.
2. To switch the camera's view to a monitor, select the monitor from the drop-down Monitor menu and click **Switch**.
3. To set the camera and view to a preset position, select the position from the drop-down Preset # list.
4. Use the **Pan/Tilt** arrows to move the view to the desired spot. Clicking an arrow moves the camera view in the indicated direction until you click the red stop sign.
5. Use the **Zoom** arrows to zoom in (Up arrow) or zoom out (Down arrow).
6. Use the **Focus** arrows to adjust the proper focus.
7. Use the **Iris** arrows to adjust the view's area.
8. Click **Set** to set the configuration.

3.4.4.3 Intercom Controls

Intercom Controls operates an intercom that has already been defined. See "HW Config - Intercom" in Chapter 23.



Use the following field descriptions to complete the Intercom Controls dialog box:

Field	Description
Source Intercom	Intercom station from which the call will be initiated.
Target Intercom	Intercom station receiving the call.
Dial	Lowest priority call. If the target is in use, a busy signal is returned.
Low Priority Direct	Medium priority call. This call forces the target intercom to pick up on the first ring. If the target is in use, a busy signal is returned.
High Priority Direct	High priority call. This call forces the target intercom to pick up on the first ring. This call also overrides any call on the target except for another High Priority Direct.
Call	Initiates the call.
Reset	Terminates an active intercom session and leaves the dialog box ready to make another call.

3.4.4.4 Void Card

Void Card enables you to void a card from the Alarm Monitor.

3.4.4.5 Status Groups

Status Groups enables you to create, view, and edit status group configurations from the Alarm Monitor.

A status group is a group of logical devices for which status is reported. For example, security personnel can conduct monthly checks of enterprise hardware categories. The status consists of events associated with the logical devices.

For instructions on creating or modifying status groups, see "DBC - Status Groups" in Chapter 56.

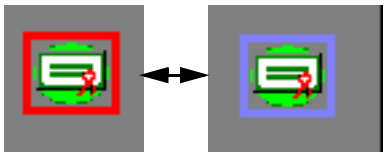
3.4.4.6 Reconnect

This function reconnects the Alarm Monitor to the Pro-Watch server.

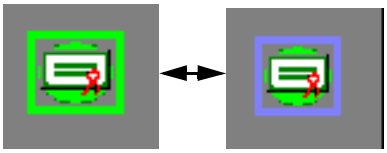
3.5 Processing Events on a Map

You can also monitor and respond to alarms from the Pro-Watch map view. Resources such as logical devices, groups, CCTV camera views, intercoms, or links to other maps appear on the map as icons.

Alarms associated with the resources appear on the map page as colored rectangles that surround the resource icon. A flashing red/blue rectangle means there is at least one unacknowledged alarm associated with the resource; a green/blue rectangle signifies acknowledged alarms.



Red/Blue: At least one unacknowledged alarm.



Green/Blue: Acknowledged alarms.

Note: Map pages display automatically when assigned to a class or user. If there is more than one alarm map page, then the multiple pages will display in cascaded or tiled windows.

You can perform the following monitoring functions and actions from the map display by right-clicking the icon and selecting from the menu:

- Acknowledge alarm.
- Acknowledge all alarms.
- Clear alarm.
- Clear all alarms.
- Hardware control.
- All actions.

You can also perform the following map-specific functions:

- **Zoom** – Expands a specified area of the map. Right-click a map and select **Zoom**, or select **View > Zoom**. Draw a box by clicking and dragging, and the map expands this box to fill the entire map area.
- **Zoom In** – Enlarges the view of a map each time the map is selected. Right-click a map and select **Zoom In**. Or, select **View > Zoom In**.
- **Zoom Out** – Reduces the view of a map each time the map is selected. Select this function by right-click a map and selecting Zoom Out. Or, select **View > Zoom Out**.
- **Zoom Previous** – Restores the previous view setting. This function is available only on AutoCAD maps.
- **Refresh** – Updates the status of alarms on a map.
- **Go to this Map** – Activates the map and enables you to move resources within the map.
- **Previous Maps** – Provides a list of previous maps viewed (if any) that you can revisit.
- **Layers** – Controls the display of AutoCAD maps.

3.5.1 Using the Layers Map Function

Using the Layers Map Function

The Layers function controls the display of AutoCAD maps. This feature is not yet implemented in Pro-Watch.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Reports

4

In this chapter ...

Overview
Screen Design
Navigating Around the Application
Report Types
Functions
Using the Application
Grouping Data
Filtering Reports
Defining a Query
Administrative Tasks
Running a Report on Demand
Reviewing Schedule Run History
Setting Display Parameters
Switching the Report Modules

4.1 Overview

This chapter describes how to use the **Compliance Reports** module. For information on the **Classic Reporting** module, see Appendix H, Reports.

The Pro-Watch **Compliance Report Manager (CRM)** application is a report tool that enables you to customize and generate a variety of reports. There are three ways to generate reports:

- Use the **sample reports** provided with the application. You simply input a relevant filter and the resulting screen displays the data appropriate to the sample selected.
- Use the **Report Wizard** that guides you through the process of designing your own report.
- Create an **SQL query** to specify the exact information you want.

You can not only specify the fields to be displayed, you can also design the appearance of the reports, specify the output format, and share and schedule reports. Other standard functions include editing, deleting, printing, saving, and exporting to a variety of formats, including Excel.

4.1.1 To switch from one module to another

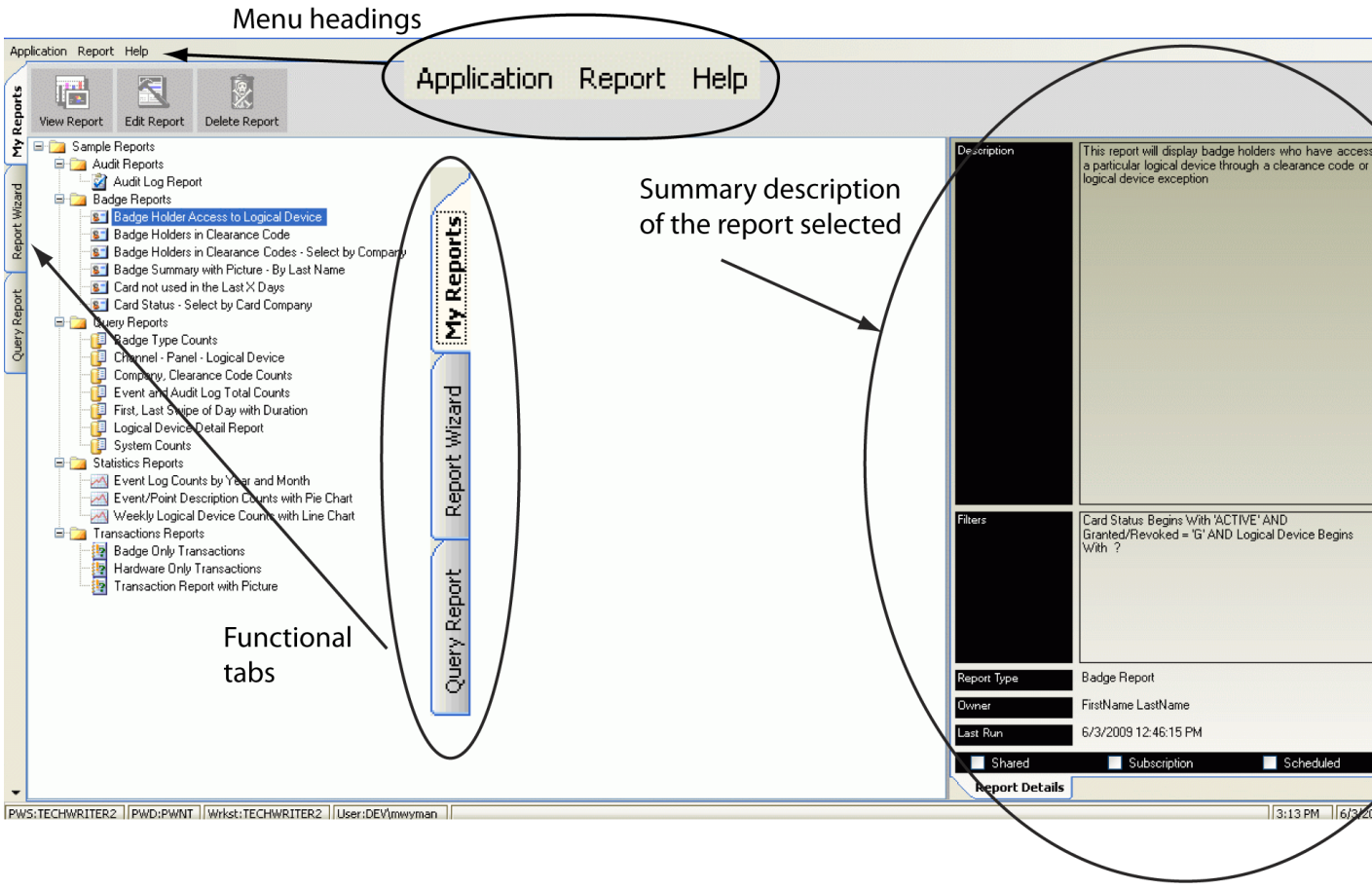
To switch from one report module to another please see "To switch from classic reports to compliance reports".

4.2 Screen Design

The opening screen has four main areas:

- Menu bar at the top
- Side tabs--Query Report, Report Wizard, and My Reports
- Left-side display area
- Right-side display area

Figure 4-1 Opening Screen



Across the top, the menu bar offers three main options:

- **Application**—Lists Administrator commands. (See “Administrative Tasks” on page 26.)
- **Report**—Lists standard functional commands, as well as export and import options. (See “Application Functions” on page 15.)
- **Help**—Displays information about the application.

In the upper left corner, three tabs enable you to perform different functions:

- Click **My Reports** to display a list of reports you have created.
- Click **Report Wizard** to start generating a report.

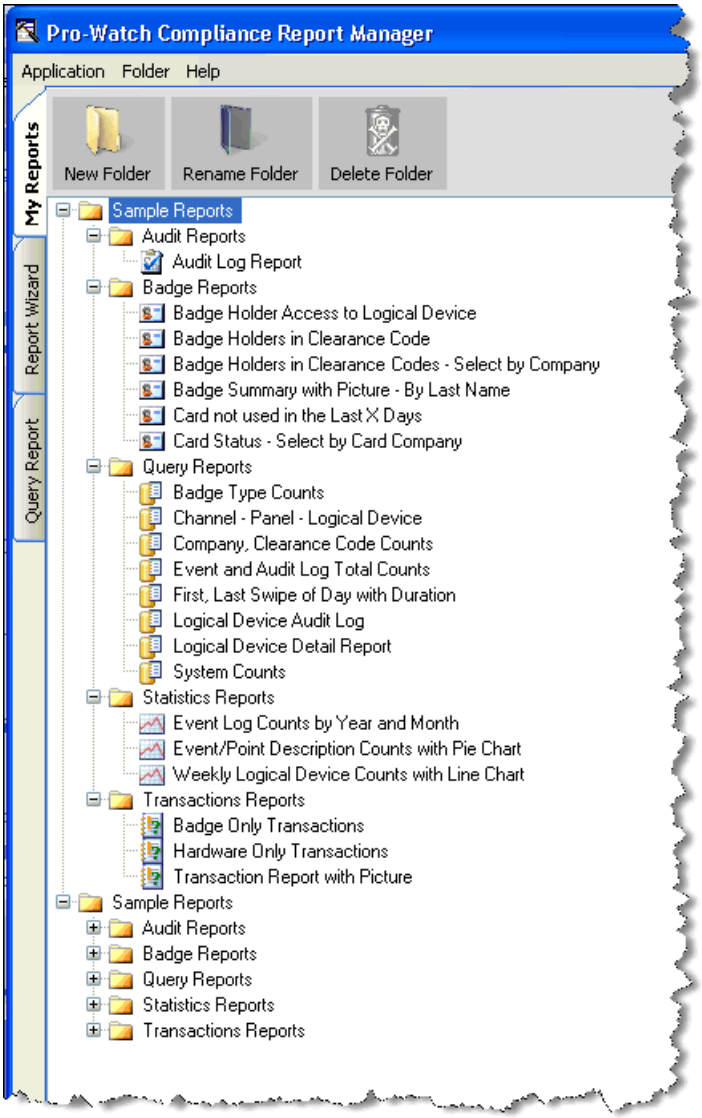
- Click **Query Report** to create a query.

The left side of the screen is the main display area for listing report types and reports.

The right side of the screen displays summary details about the report you have selected, including Description, Filter, Report Type, Owner, when it was last run, and whether it is shared, scheduled, or has any subscribers.

For greater legibility, where possible, screens are cropped to display a subset of the complete screen. For example, the following figure displays an abbreviated screen showing the available report types in the left pane.

Figure 4-2 Typical Abbreviated Screen Display



4.3 Navigating Around the Application

The Report Wizard provides four command buttons on every screen: the Back, Next, and Finish buttons at bottom right and the New/Clear button at bottom left.



Click the **Back**, **Next**, and **Finish** buttons to move from screen to screen in the Wizard. Click **New/Clear** to cancel your work so far and return to the opening Report Wizard screen.

If you are viewing a report and want to return to the previous screen, click the **Close** button in the upper right corner. This button acts as a back button and will return you to the immediately preceding screen.

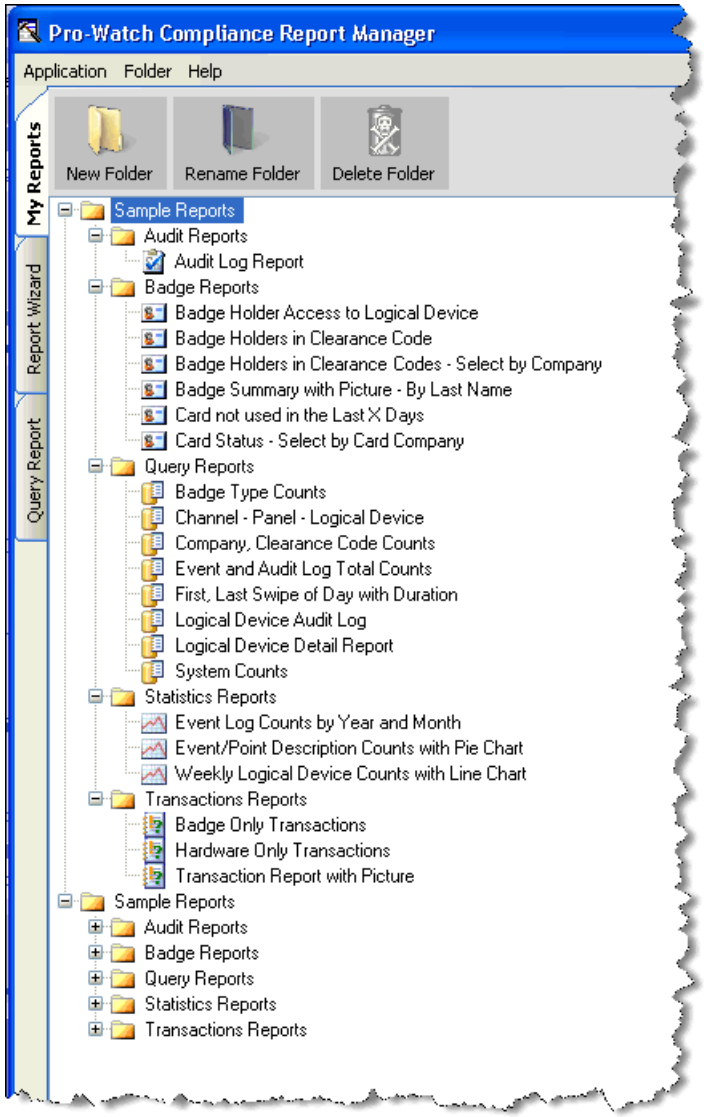
Caution: CLICK ONLY ONCE! If you click twice you exit the application entirely.

4.4 Report Types

The **Compliance Report Manager** provides five types of reports:

- **Audit**—Provides a record of all changes that are made in Pro-Watch.
- **Badge**—Provides Badge, Card, Clearance Code, and Logical Device Report fields with run-time parameters.
- **Query**—Enables you to enter specific database query and selection criteria to generate a completely customized report. You can also create queries for end users to run.
- **Statistics**—Provides group data from event logs.
- **Transaction**—Provides information about events.

The following figure displays the types of reports that may be created for each category.



To use a sample report to generate a report, you may select any report type, enter a filter, and generate the report according to the sample for that type.

You may also customize a report to meet your requirements. The information is available in the database; the Report Wizard guides you through the process of creating a report from this data, including selecting fields, creating filters, and creating a report title and description.

Note: The Report Wizard generates only the Audit, Badge, Statistics, and Transactions Reports. The Query Report is generated through a different process.

All reports are displayed in the Report Viewer, where they can be printed, exported, and saved.

4.5 Functions

This section describes application functions and Report Viewer functions.

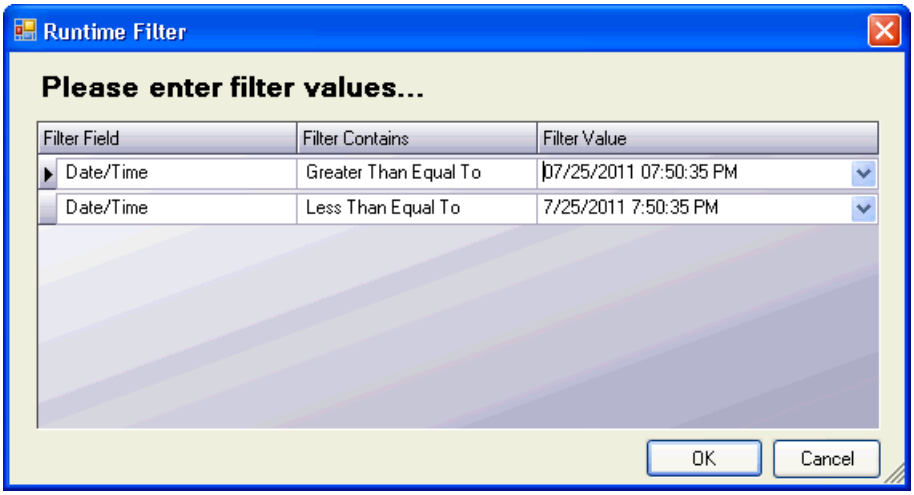
4.5.1 Application Functions

The Report menu on the My Reports tab lists several functions you can do with reports: view, edit, delete, copy, and share reports, and export and import report schemas.

4.5.1.1 Viewing Reports

To view a report:

1. Click the Compliance Report Manager icon on your desktop to display the initial screen. (See Figure 1 on page 3.)
2. Right-click the specific report you want to view—for example, Badge Holder Access to Logical Device, and select **View Report**. Or, click the View Report icon to display the Runtime Filter dialog box.



3. Select a Filter Value from the drop-down list.
4. Click **OK** to display the requested report.

4.5.2 Editing Reports

To edit a report:

1. Click the **Compliance Report Manager** icon on your desktop to display the initial screen. (See Figure 4-1 on page 3.)
2. Right-click the specific report you want to edit—for example, Badge Holder Access to Logical Device, and select **Edit Report**. Or, click the **Edit Report** icon at the top of the screen.

3. Follow the instructions for creating a report described in Generating Reports, page 18.

4.5.3 Deleting Reports

To delete a report:

1. Right-click the specific report you want to delete—for example, Badge Holder Access to Logical Device, and select Delete Report. Or, click the Delete Report icon at the top of the screen.

The Pro-Watch Compliance Report Manager dialog box appears.

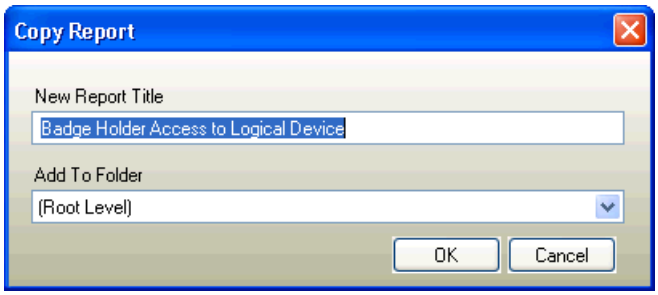


2. Verify that you have selected the correct report and click **OK**.

4.5.4 Copying Reports

To copy a report:

1. Right-click the specific report you want to copy—for example, Badge Holder Access to Logical Device, and select Copy Report to display the Copy Report dialog box.



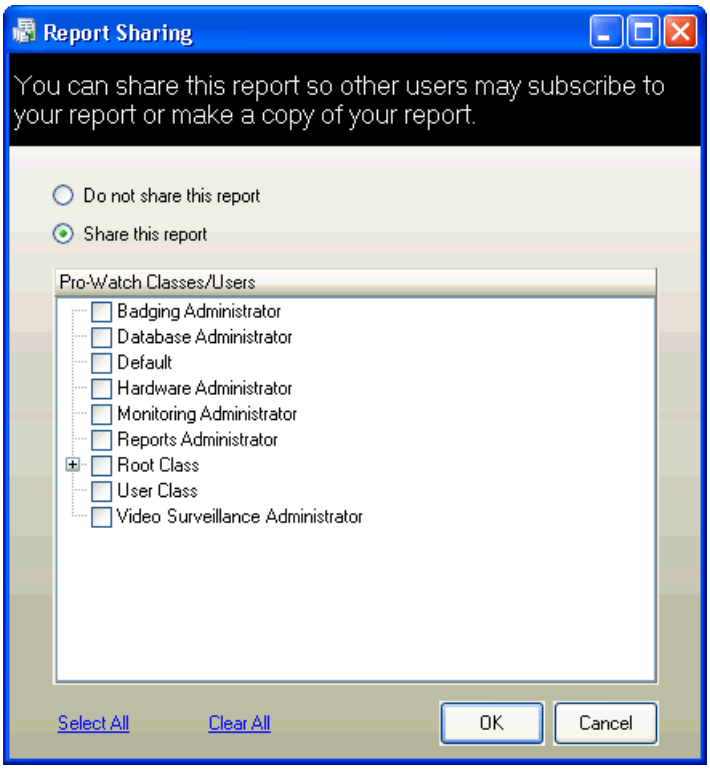
2. In the New Report Title field, enter the title of the copy you are making.
3. Select the directory where you want to store it, and click **OK**.

4.5.4.1 Sharing Reports

The Compliance Report Manager includes a function to share, or make available, your reports to users in the Pro-Watch environment.

To designate a report to be shared:

1. Right-click the specific report you want to share—for example, Badge Holder Access to Logical Device, and select Share Report to display the Report Sharing dialog box.



2. Click the button to share the report.
3. Select the personnel with whom you want to share the report. You can select a Pro-Watch class of users, or select individual users.
4. Click **OK**.

The report is now stored in a repository that may be accessed by you and by the users you have designated to share your reports with. (For more information on shared repositories, see "Setting Up a Shared Repository".)

4.5.4.2 Exporting the Report Schema

If you like the format or field selection of a report, you can save it in one of your own directories for subsequent use.

To export a report schema:

1. Click the specific report you want to export—for example, Badge Holder Access to Logical Device.
2. Click **Report > Export Report Schema** to display your Windows Explorer directories and folders.
3. Name the report and select your desired location for it and click **Save**.

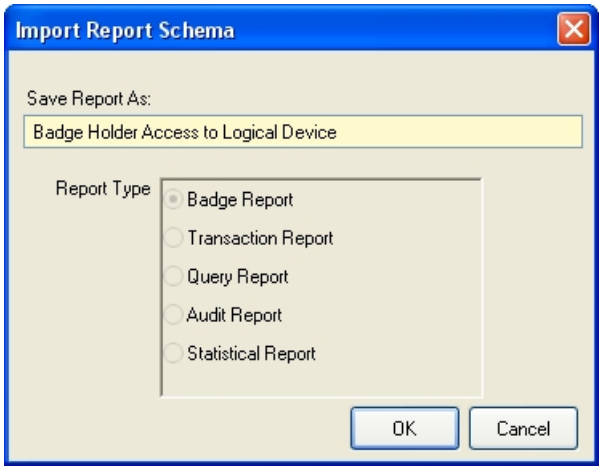
The report is now easily accessible to you for e-mailing and exchanging with others.

4.5.4.3 Importing the Report Schema

If you want to re-use a report format on your hard drive, import the report schema.

To import a report schema:

1. Click **Report > Import Report Schema** to display your Windows Explorer directories and folders.
2. Select the report and click **Open** to display the Import Report Schema dialog box.



> **Note:** In the **Save Report As** field enter the name of the new report you are creating. The Compliance Report Manager highlights the type of report you have entered in the **Save Report As** field.

3. Click **OK**.

4.5.5 Report Viewer Functions

The Report Viewer Displays six functional icons across the top: **Refresh**, **Print**, **Preview**, **Save**, **Grouping**, **Settings**, and **Export**..



4.5.5.1 Standard

Standard functions include printing, previewing, and saving.

Printing Reports

To print a report:

1. Click the **Print** icon to display the standard Microsoft Print dialog box.
2. Select the appropriate printer and specify any special properties.
3. Click **Print**.

Previewing Reports

The Preview function provides you with several options for customizing the display of the report when it is printed. To preview a report:

1. Click the **Preview** icon for a preliminary look at the report before it is printed.
2. Customize the printed display using the tools and functions described below.

   The **Preview** screen includes a menu bar and several options for customizing the printed view of the report. There are two ways to customize the preview display: select an option from a menu, or click the icon representing the function you want to use.

   There are three menus in the menu bar:

   a. **File**—Print, Page Setup, Exit

   b. **View**—Thumbnails, Zoom In, Zoom Out, Zoom, Page Width, Margin Width, Whole Page, Go To

c. **Tools**—Hand Tool, Snapshot Tool, Dynamic Zoom Tool, Zoom In Tool, and Zoom Out Tool.

These functions are also available using the icons.

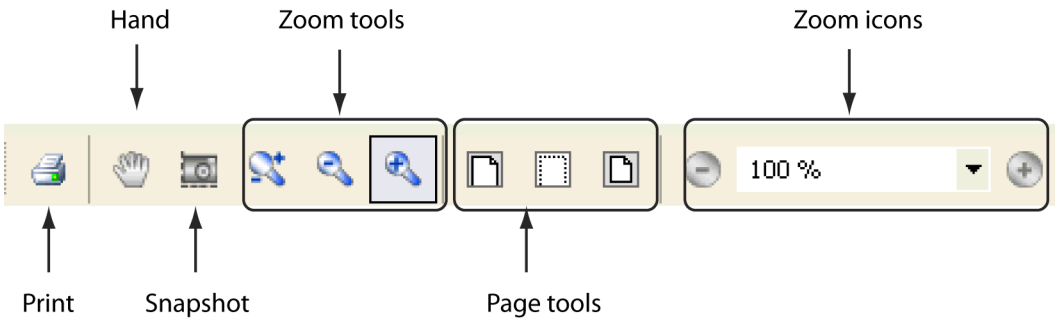


Table 4-1: Report Viewer Icons

Function	Description
Refresh	Refreshes the screen
Print	Prints the report on standard 8.5 x 11 page
Hand	Moves the page up and down to facilitate viewing
snapshot	Captures and places an image on the clipboard for possible use in another application
Zoom	**Dynamic** - Maintains proportions as you zoom in and out with the cursor **Out** - Reduces size of page incrementally **In** - Increases size of page incrementally **Note:** Use the tools to click and drag to the display area to apply. Use the automatic zoom in/out icons to resize the display when you click the icon.
Page Width	Sizes the print area to the entire page width
Margin Width	Sizes the print area to the display inside the margin
Whole Page	Sizes the print area to the entire page, including margins
Continuous	Prints the report on a continuous, uncut (no separate pages) paper supply
Page Layout	Controls the number of pages in the preview display. Can be vertical or horizontal

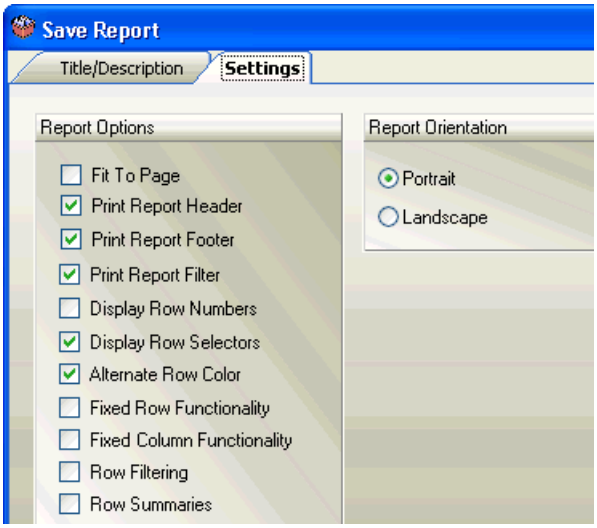
Table 4-1: Report Viewer Icons

Function	Description
Directional buttons	Moves the display from view to view or page to page.

3. When you have finished customizing the display, click **File > Print** or click the **Print** icon in the top toolbar
   OR
   Click **Close** to close the preview display.

Saving Reports

Click the **Save** icon to display the Save Report dialog box. The box has two tabs: Title/Description and Settings. The Title/Description tab displays the report title and description that you entered, as well as the Save In Folder field, where you can select from the drop-down box the folder that you want to save the report to. The Settings tab displays a list of Report Options and a box where you can specify the orientation of the report..



To save a report:

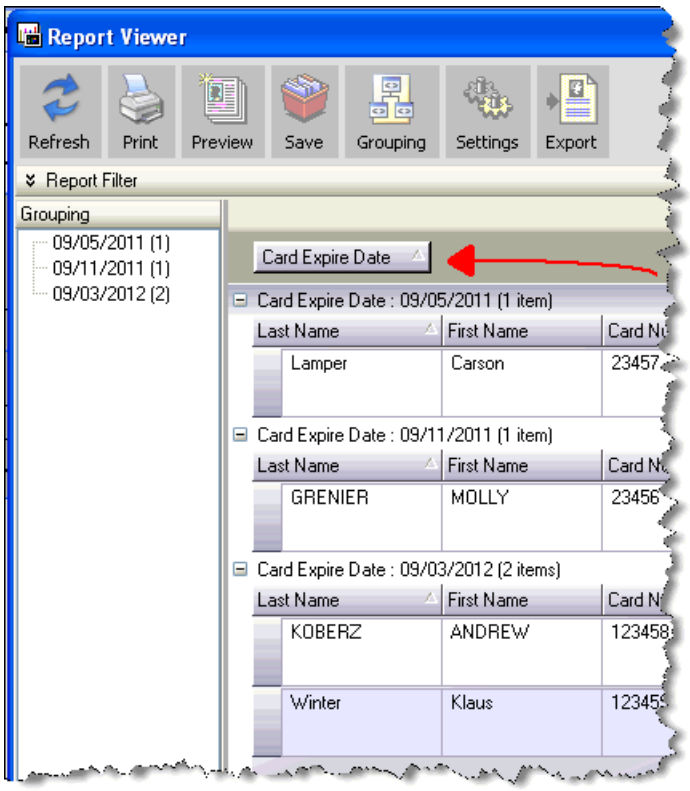
1. Click the Save icon to display the Save Report dialog box.
2. On the Title/Description tab, select the folder where you want to save the report.
3. On the Settings tab, click the boxes for the settings you want to apply to the report.
4. Select the desired orientation.
5. Click Save As to save the report under a different name OR click Save.

4.5.5.2 Special

Special functions include grouping data, specifying settings, and exporting reports.

Grouping Data in the Viewer

In the Viewer, you can organize the display by a specific column heading—for example, Card Expire Date—by clicking and dragging that heading into the area above the header row. The data is now grouped by Card Expire Date for each expiration date—09/05/2011, 09/11/2011, and 09/03/2012, and the left pane displays a summary of the data: one card expires on 09/05/2011, another on 09/11/2011, and two others expire on 09/03/2012. .



Click the **Grouping** button to alternately show and hide this summary pane.

For complete information on the Grouping feature, see “Grouping Data“ on page 26.

4.5.5.3 Customizing the Settings

Click the Setting icon any time you want to modify the appearance of a report. The resulting dialog box offers several choices.

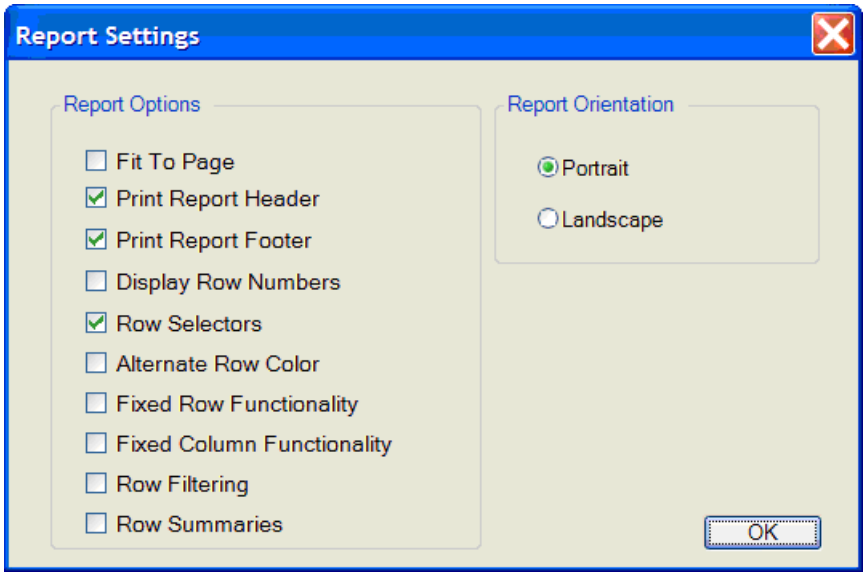


Table 4-2 describes these choices.

Table 4-2: Report Settings

Option	Description
Fit To Page	Scales the column widths of the report so the report can be printed on one page.
Print Report Header	Displays the report title in the page header when printing.
Print Report Footer	Displays the page number and date in the page footer when printing.
Display Row Numbers	Displays row numbers to the left of the rows in the report.
Row Selectors	Enables user to highlight a row.
Alternate Row Color	Displays color in alternate rows to enhance the readability of the data across the page
Fixed Row Functionality	Allows a row or rows to be fixed at the top of the viewer so it will always be in view when you scroll.
Fixed Column Functionality	Allows a column to be fixed to the left of the viewer when you scroll.

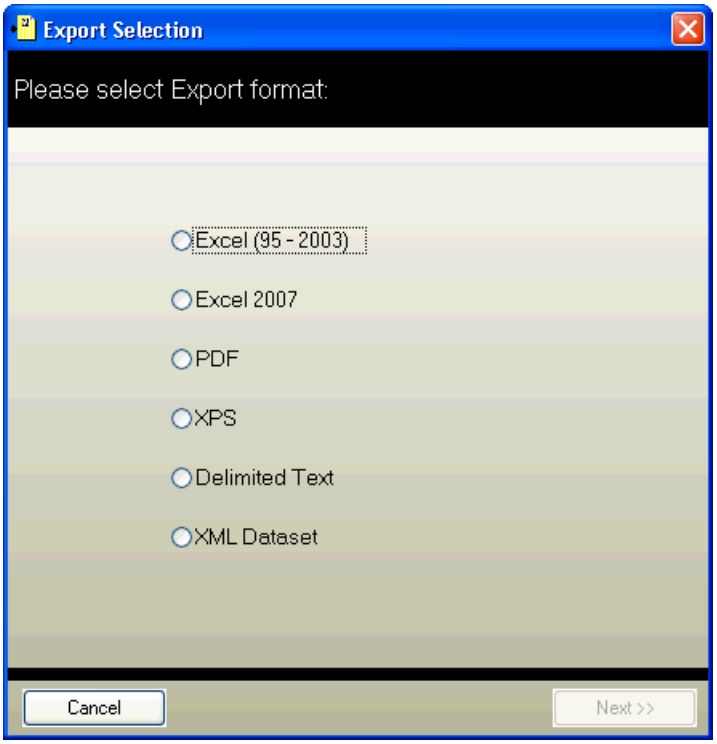
Table 4-2: Report Settings

Option	Description
Row Filtering	Enables you to filter on individual columns in the view.
Row Summaries	Allows columns to display summaries at the end of the report.
Portrait/Landscape	Determines the print orientation of the report.

When you have made your selections, click **OK**.

Exporting Reports

Compliance Reports are available in several formats. Click the **Export** icon to display a list of format choices..



To export a report:

1. Click the **Export** icon to display the Export Selection dialog box.
2. Click the desired format, then click **Next** to display the second page of the Export Selection dialog box.

4.6 Using the Application

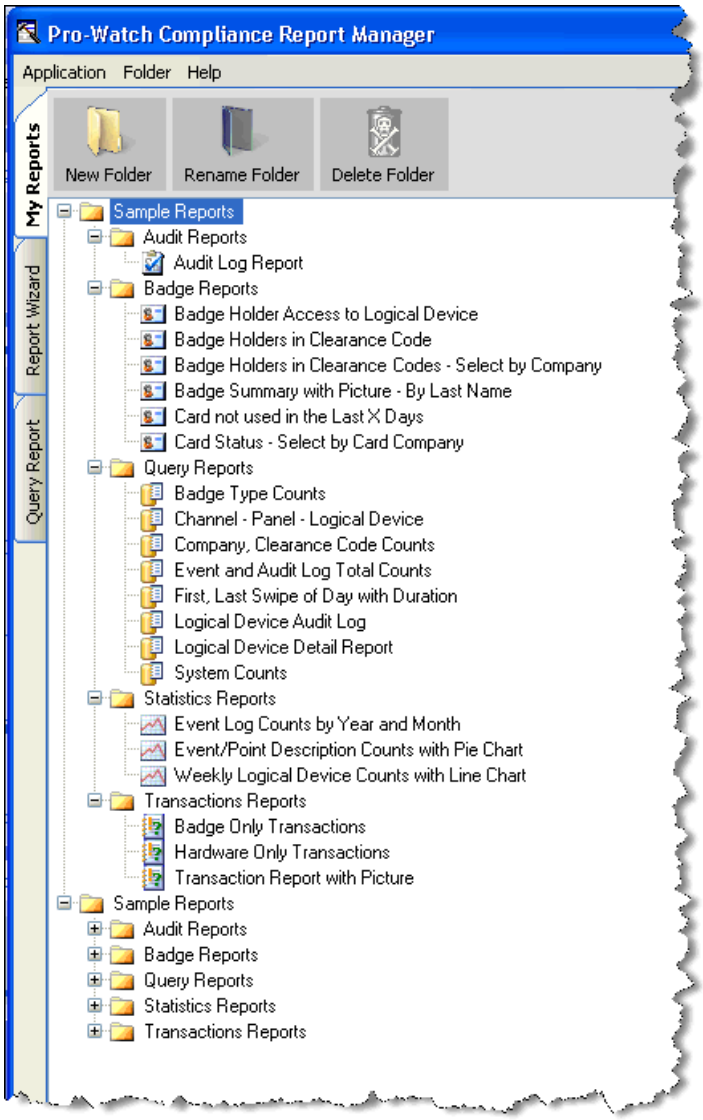
4.6.1 Generating Reports

The Compliance Report Manager offers two methods for generating a report:

- Using the sample reports provided
- Customizing your own report

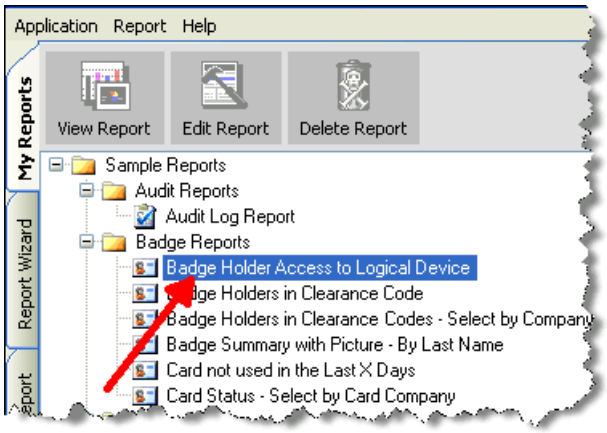
4.6.1.1 Using a Sample Report

Each type of report has several samples set up. The following figure displays each type of report and the samples available for that type..

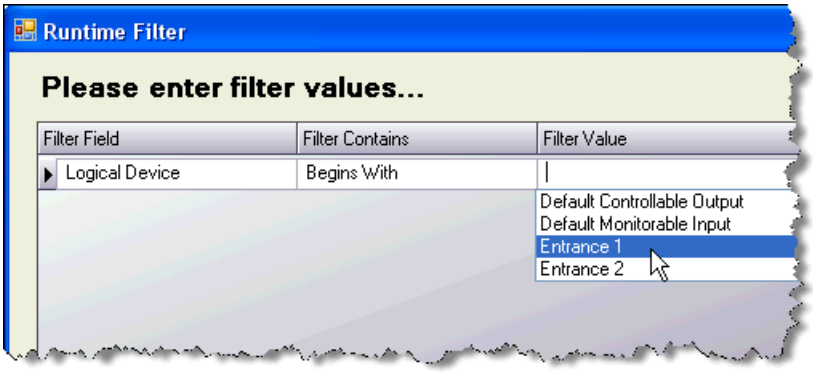


To use a sample report:

1. Click the **Compliance Report Manager** icon on your desktop to display the initial screen.
2. Either:
   - Double-click the specific report in the report tree display,
   - Click to highlight the specific report, and then either click the **View Report** toolbar icon or right-click the report and select **View Report**, or
   - Select **Report > View Report** from the toolbar menu.



The Runtime Filter dialog box appears..



In the example above, the dialog box requests a Logical Device as the Filter Value. Select the appropriate device. In this example, the selected Filter Value is Entrance 1.

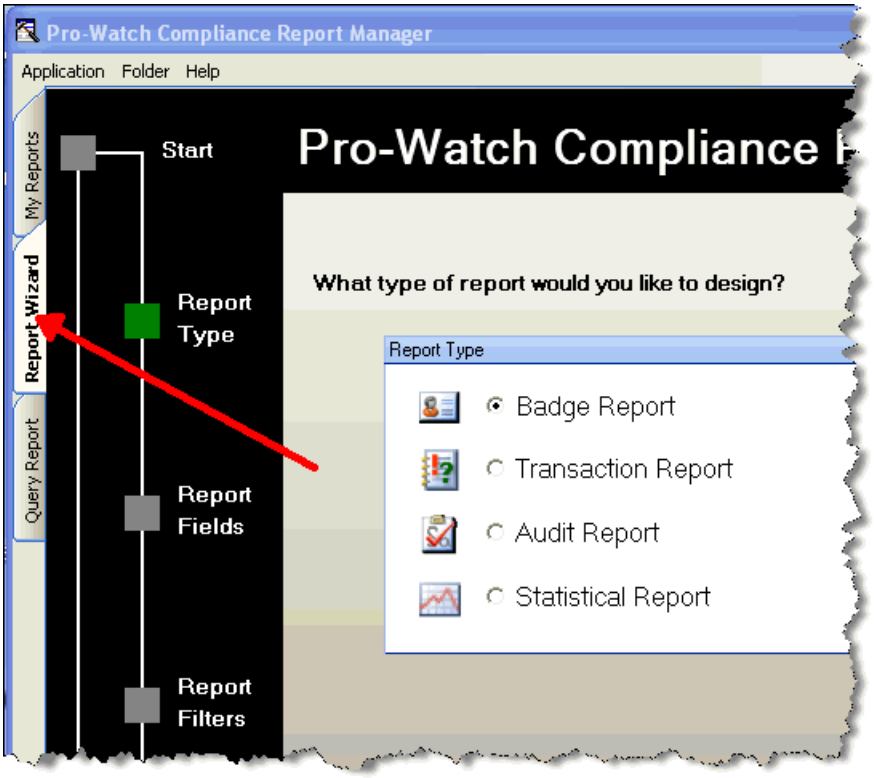
3. Click **OK** to display the requested report.

4.6.1.2 Using the Report Wizard

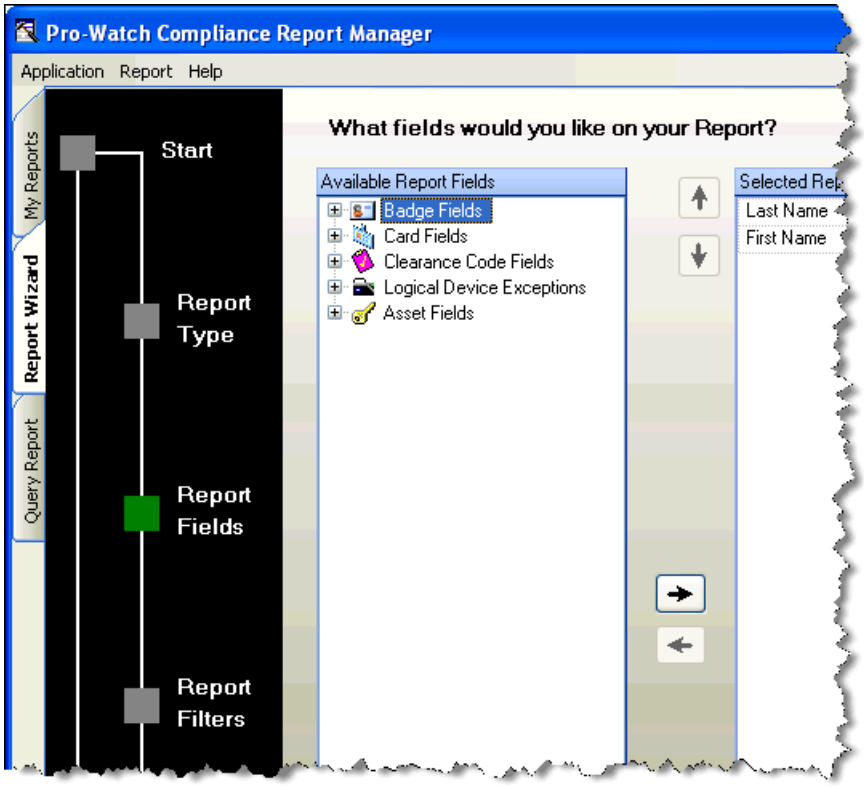
The Report Wizard guides you through the process of creating Audit, Badge, Statistics, and Transaction Reports. This section describes how to create these reports.

To use the Report Wizard:

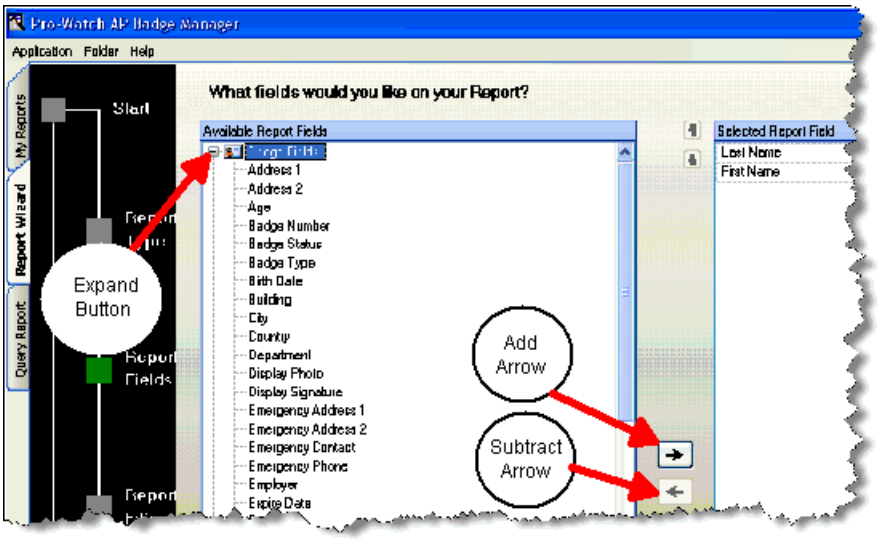
1. Click the **Report Wizard** tab to view the opening **Report Wizard** screen.



2. Select the type of report you want to create and click **Next** to view the screen that lists the fields available for the report type you selected..



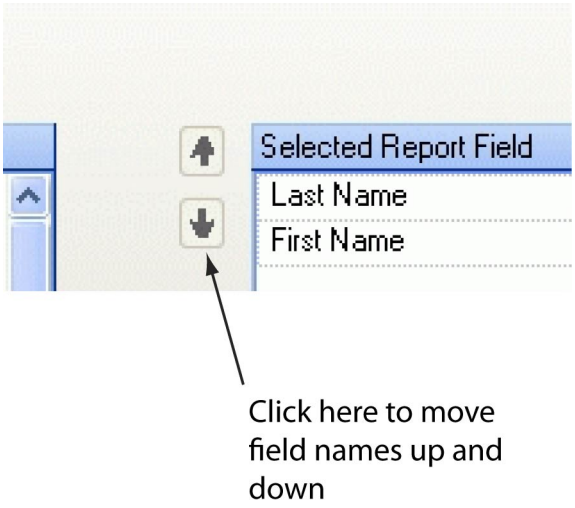
3. Click the expand button next to the type of fields you want to display. The following figure shows an abbreviated view of the Badge Fields expanded.



4. To select a field to display on your report, you can either:

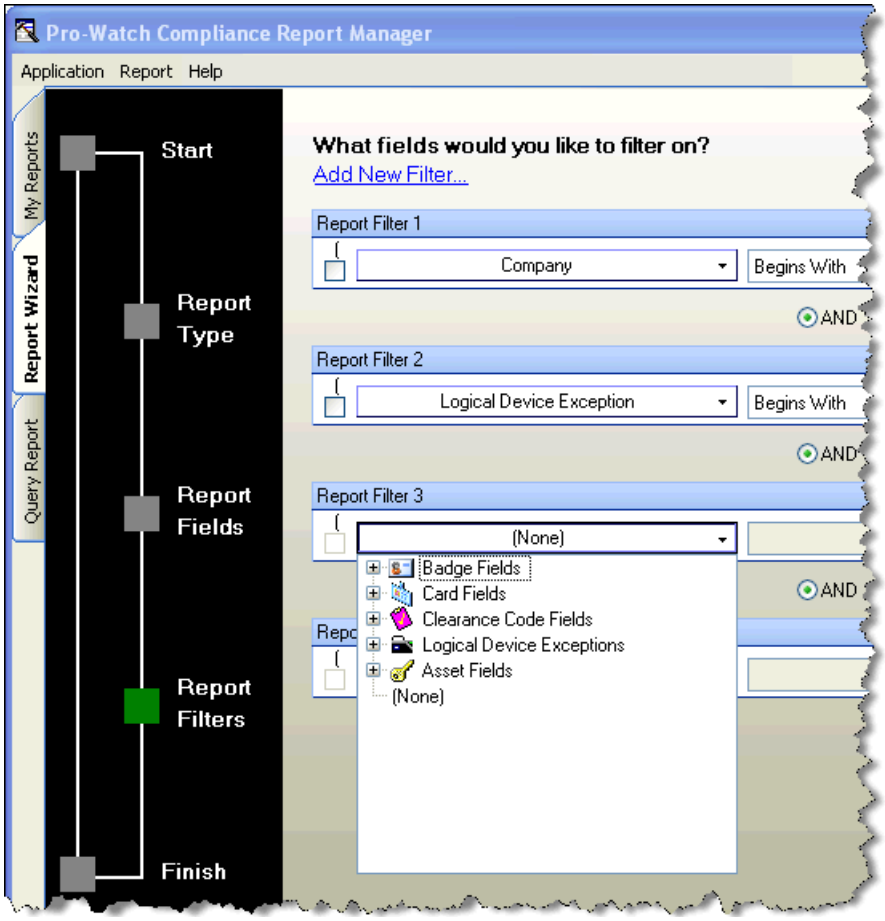
- click to highlight the field name, then click the “add” arrow to add the field to the list in the right-hand box (highlight and click the “subtract” arrow to move the field back to the Available Report Fields column), OR
- double-click the field name to add it to the list in the right-hand box, OR
- click the field name once and drag it to the right-hand box.

Note: The order in which you select the fields governs the order that the columns are arranged in the report.That is, if you select Card Number as the first field, then the first column of the report will be Card Number. If you want to change the order before moving on, click the field name then click the up arrow or the down arrow..



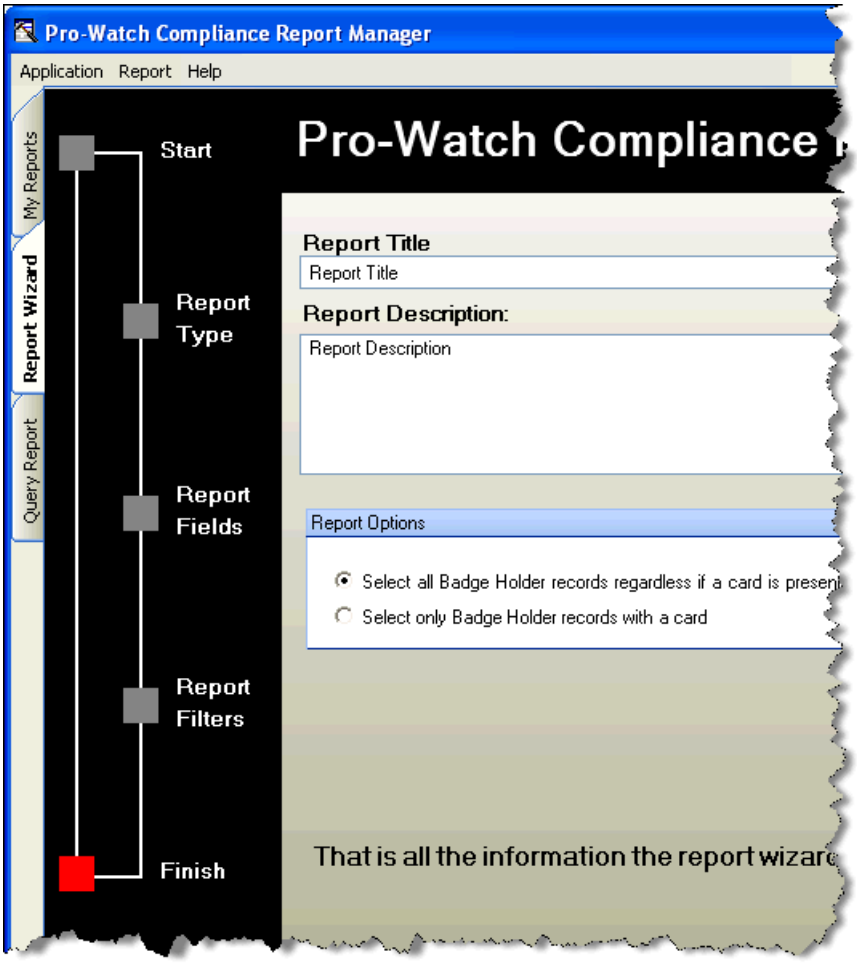
5. Repeat the selection process for any Event Log fields, Card fields, or Area fields you want to include in your report.

6. When you have selected all the fields you want in your report, click **Next** to display the filter fields screen.



7. Enter the fields you by which you want to filter. Note that the “Add New Filter” link at the top of the screen enables you to create additional filters. (For more information, see “Filtering Reports” on page 28.)

8. Click **Next** to display the **Report Title and Description** screen.



9. Enter the report title and description and select the appropriate Report Options and Report Data radio buttons described in the following table:

Table 4-3: Report Options and Report Data Radio Buttons

	Badge Report	Transaction Report	Audit Report
Report Options	• Select all Badge Holder records • Select only Badge Holder records with a card	• Select all Transaction records • Select only Card/Badge Holder Transaction events • Select only Hardware Transaction Events	**N/A**

Table 4-3: Report Options and Report Data Radio Buttons

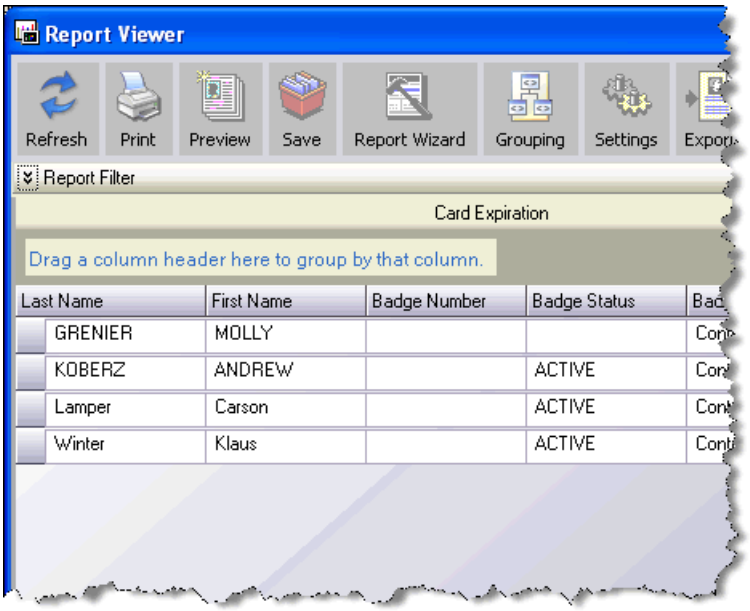
	Badge Report	Transaction Report	Audit Report
Report Data (data against which the report is run)	**N/A**	• Current Transaction Log • Archived Transaction Log	• Current Audit Log • Archived Audit Log

10. Click **Finish** to display your customized report.

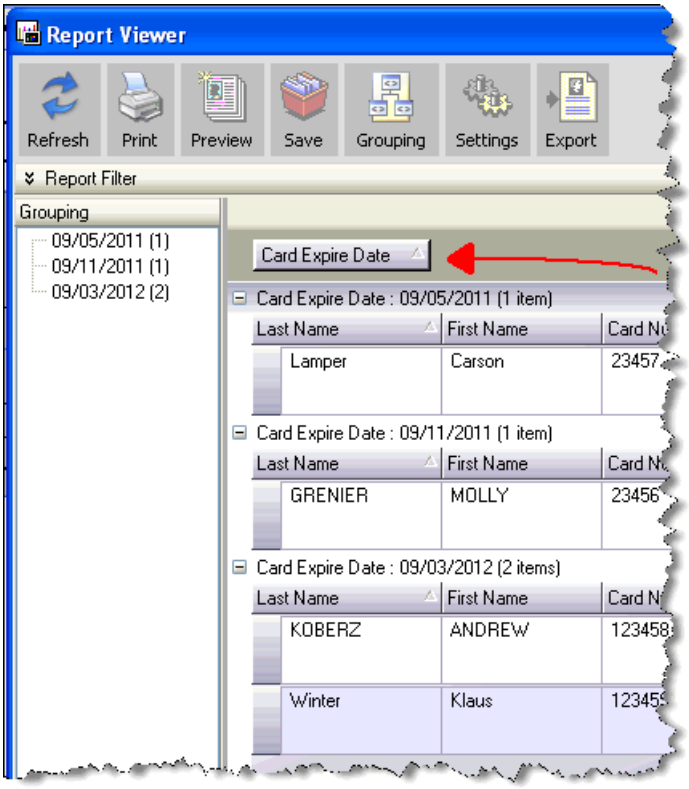
4.7 Grouping Data

There are several ways to arrange the display of data in your reports:

- On the **Report fields** screen in the Report Wizard, select the fields in the order that you want them displayed in the report. The result is a straightforward report, sorted in the order that you selected the fields on the **Report fields** screen..



- In the Viewer, you can organize the display by a different column heading—In the Viewer, you can organize the display by a specific column heading—for example, Card Expire Date—by clicking and dragging that heading into the area above the header row. The data is now grouped by Card Expire Date for each expiration date—09/05/2011, 09/11/2011, and 09/03/2012, and the left pane displays a summary of the data: one card expires on 09/05/2011, another on 09/11/2011, and two others expire on 09/03/2012..



Click the Grouping button to alternately show and hide this summary pane.

In the pane on the left, click a grouping heading to highlight the information for that grouping by moving it to the top of the display.

To return the display to its original state, click and drag the heading back to the heading row.

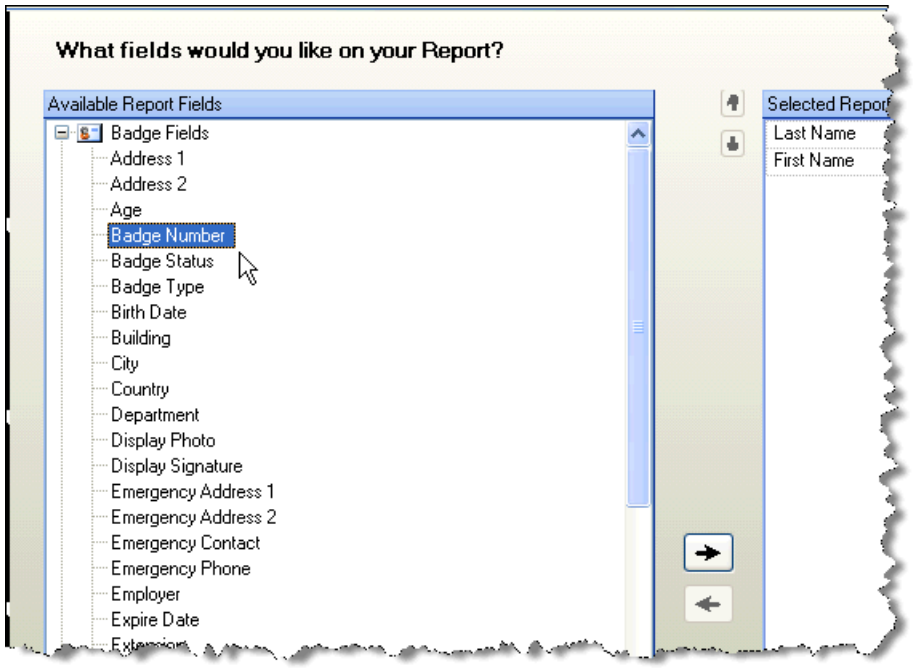
4.8 Filtering Reports

The filtering function in the Compliance Report Manager enables you to specify the data you want to display in a report. A filter consists of a field or category (Clearance Code, Logical Device, etc.), an operation (Begins With, Equals, Ends with, etc.) and a specific piece of information in the field or category specified. For example, the simple filter CLEARANCE CODE/EQUALS/ENGINEERING results in a report listing all employees who have a Clearance Code of Engineering. You can apply up to four filters to one report.

4.8.1 Using One Filter

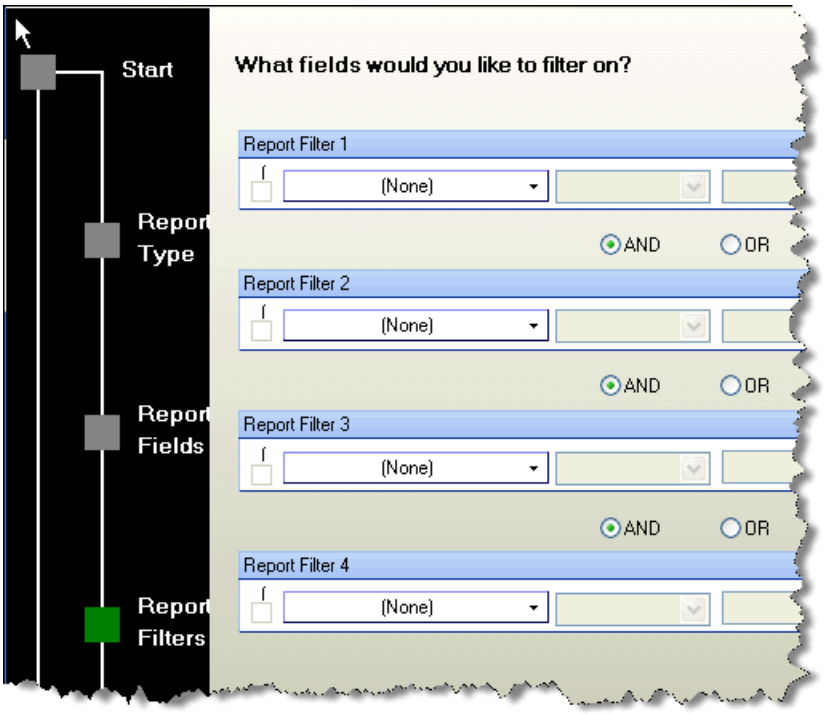
To apply one filter:

1. Open the Report Wizard.
2. Select the type of report you are creating and click **Next** to display the screen listing the fields available for the report type you selected.

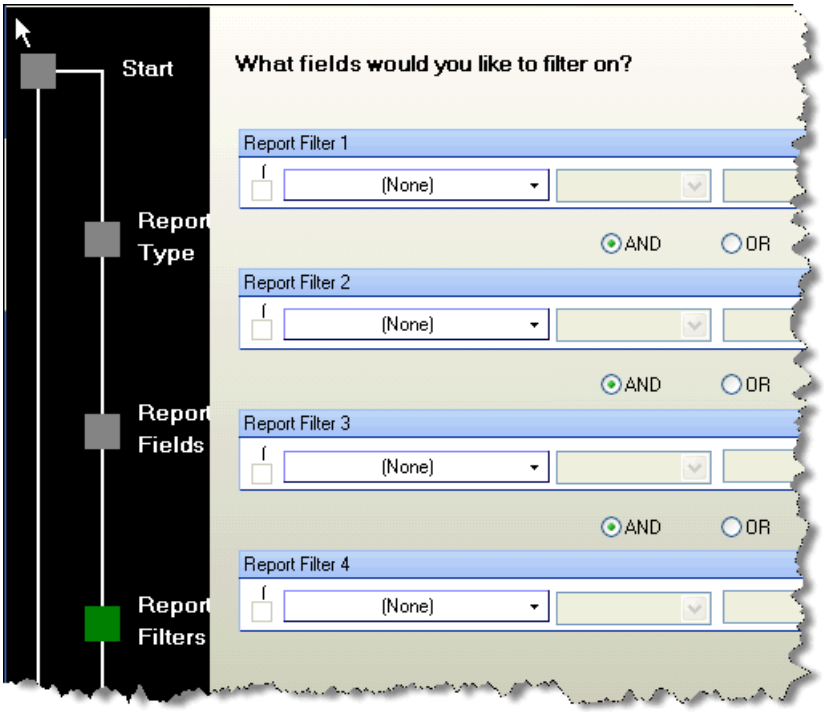


3. Select the fields you want to display in the report by clicking the field and then clicking the right arrow button in the middle of the screen.

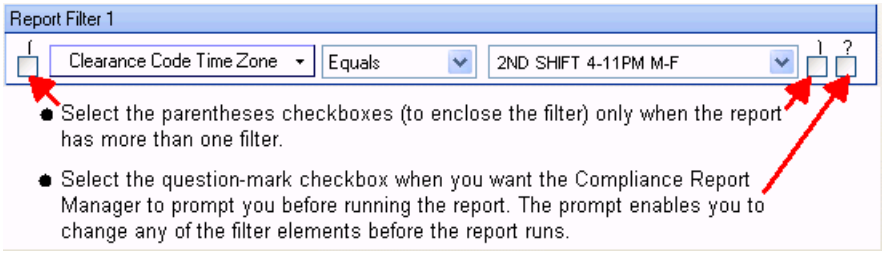
4. Click **Next** to display the **Report Filters** screen.



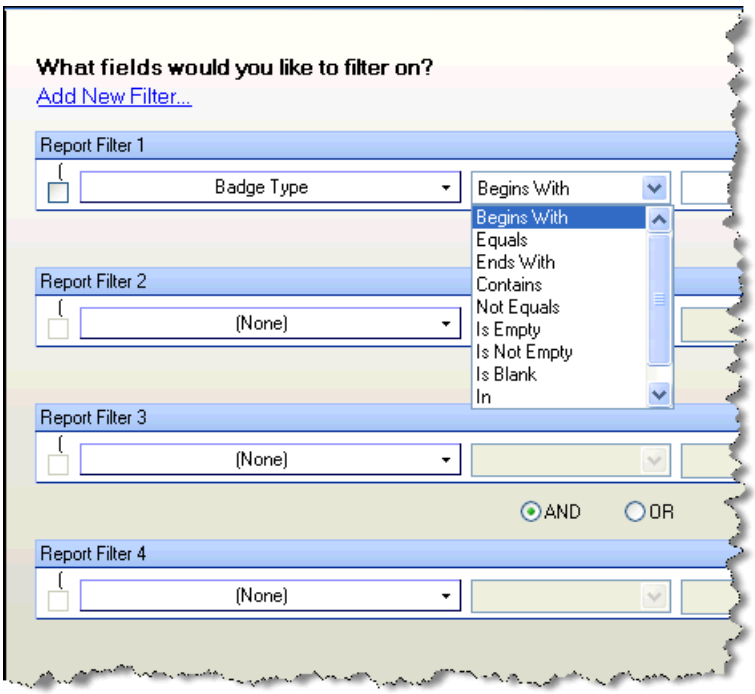
5. From the drop-down list for the first element of Report Filter 1, select the first element. Note that the operation field becomes active.



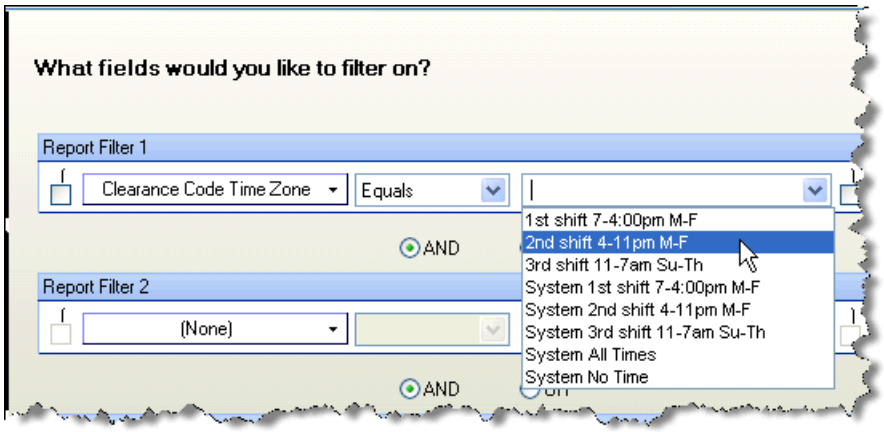
Note the two kinds of checkboxes at the ends of the Report Filter line--parentheses and question mark. Since this procedure configures only one filter, leave the parentheses checkboxes blank. Select the question-mark checkbox if you want to be able to change any of the filter elements before the report runs..



6. Select the operator you want.



7. From the drop-down list for the second element of Report Filter 1, select the value you want in order to complete the filter..



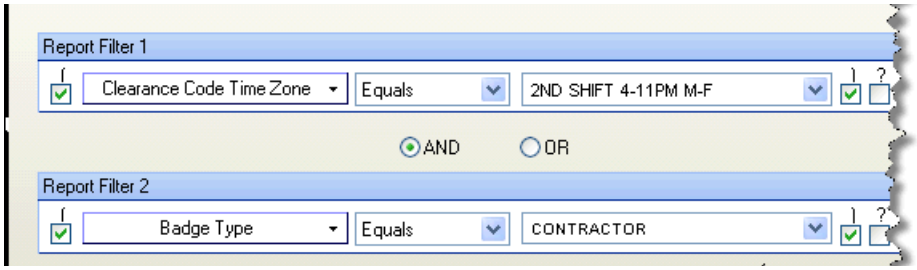
Note: For each filter you select, the corresponding types of the filter appear after the filter operation. For example, when you select **Clearance Code Time Zone** as a filter and specify an operation, the third field is automatically filled with a list of time zones. When you select **Clearance Code** and specify a filter operation, the third field is automatically filled with a list of available Clearance Codes, and so on.

8. Click **Finish** to accept the filter. The Compliance Report Manager generates a list of all employees whose Clearance Codes are assigned the 2nd shift Time Zone. This is a subset of all employees in the database.

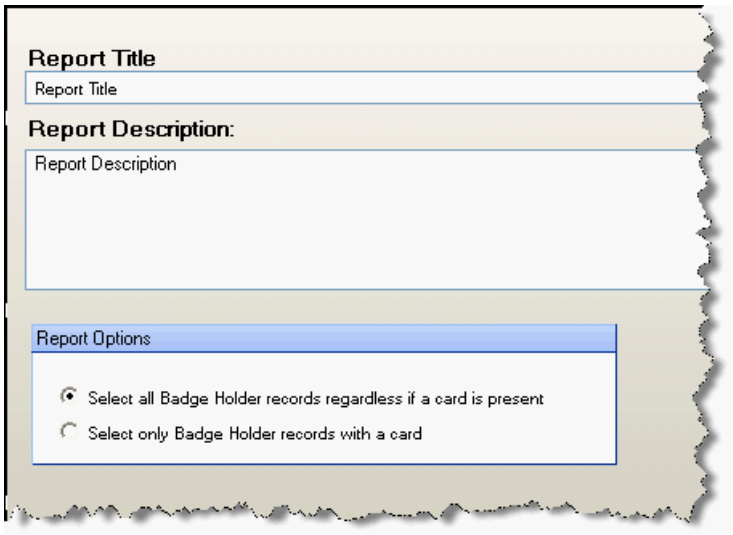
4.8.2 Using Two Filters

To generate a report with two filters, follow these steps:

1. Open the Report Wizard and follow the steps given in the preceding section, Using One Filter, page 76, to configure the first filter. Since this procedure configures more than one filter, be sure to “enclose” the filter with parentheses by selecting the parentheses checkboxes at the ends of the Report Filter line.
2. Select **AND** between Report Filter 1 and Report Filter 2.
3. Follow the steps given in the preceding section, Using One Filter, page 28, to configure the second filter. Remember to select the parentheses checkboxes. The resulting **Report Filter** screen should look like this:



4. Click **Next** to assign a title and description to the report.:



5. Click **Finish** to complete the report.

Note: To view the filters textually, click the down arrows next to Report Filter on the Report Viewer screen.

4.8.3 Runtime Filter

You can also designate a filter as a runtime filter—that is, a filter that must be applied whenever you run the report. Whenever you try to run a report that has a runtime filter on it, you will be prompted to input a filter value before you can run the report.

To designate a runtime filter, select the checkbox under the question mark at the far right of the Report Filter box.

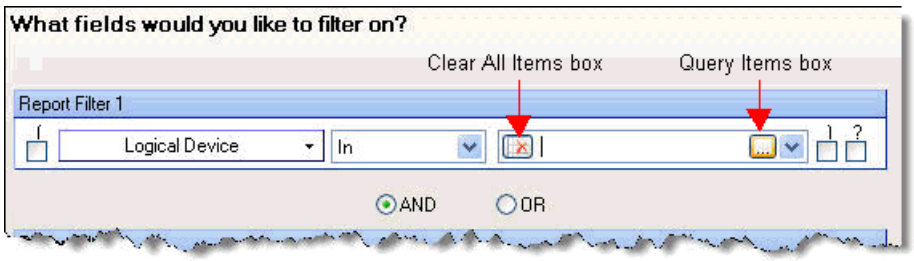
4.8.4 In/Not In Filter

In addition to the filtering already described, the Compliance Report Manager provides another operation, In/Not In, for grouping multiple instances of a field into one filter. The In/Not In operation applies to fields that have multiple Pro-Watch elements, such as Logical Devices, Companies, Time Zones, Channels, etc. The operation enables you to select, in the second filter element, more than one element to filter on.

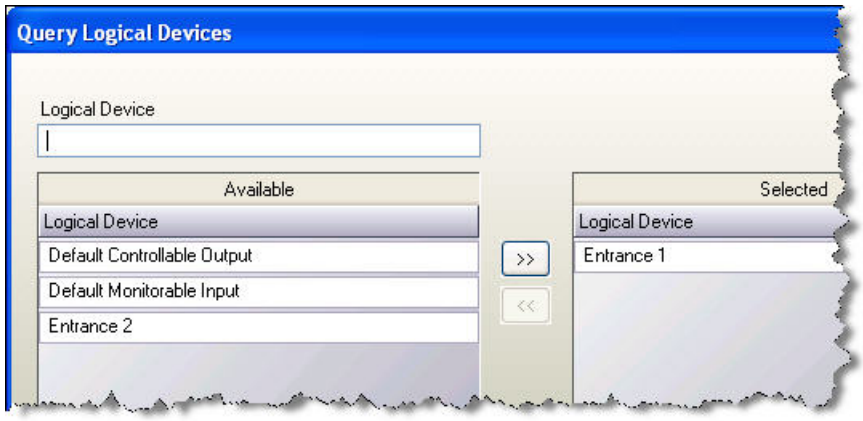
For example, to see who has access to a particular door and/or a second door, select **Logical Device** for the first element, select In as the operation, and in the second element box click the Query Items box to display all the Logical Devices. Select the two doors as the fields you want to designate as the filter options. When you click **Next** or **Finish**, the report shows all personnel who can access either one or both of these logical devices.

To use the In operation for a filter:

1. Click the drop-down list for the first element of Report Filter 1 and select a field with multiple selections as the first element.
2. Select In for the operation. The boxes for **Query items** and **Clear all items** appear in the second element field.
3. Click the **Query items** box to display the **Query [Field]** box.



4. In the **Query [Field]** box, select the devices in the **Available** box that you want to use and move (using arrows or double-clicking) them to the **Selected** box.:



5. Click **OK** to return to the **Report Filters** screen.
6. Click **Next** or **Finish** to display the report on the Report Viewer screen.

Use the Not In filter to exclude instances of a field from a report. For example, to see who can access all doors except the two selected doors, select **Not In** as the operation.

4.9 Defining a Query

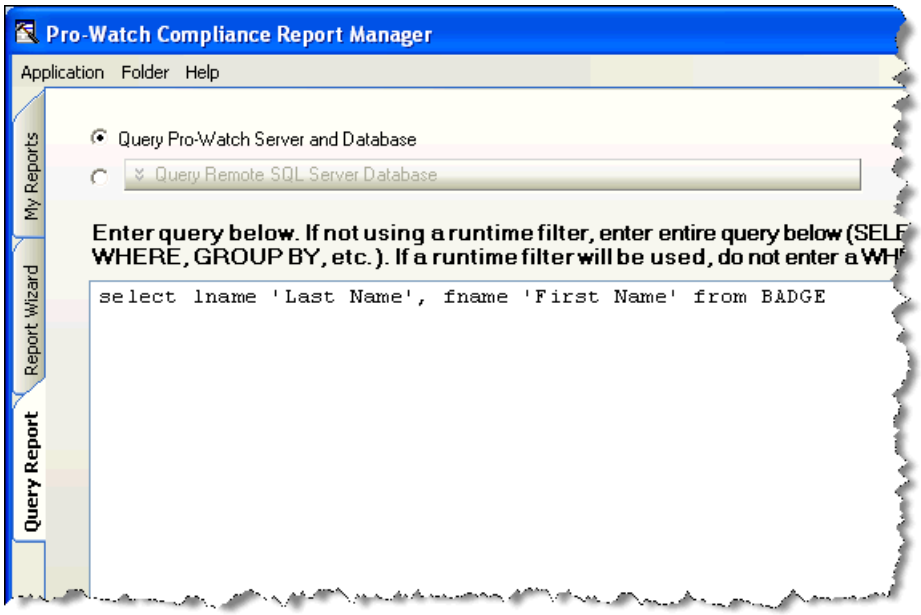
The Query function of the Compliance Report Manager enables advanced database users to create complicated and unique reports that cannot be created through the Report Wizard by extracting information according to the operations specified by the user to achieve a desired result set. The function is intended for use by advanced database users to display any database SQL query through the Report Viewer.

This chapter describes how to use the Query function of the Compliance Report Manager. Further explication is beyond the scope of this guide. For more information or assistance, see your system administrator.

Note: Do not use 'UPDATE' or 'DELETE' in the query. The report will not run.

4.9.1 Defining a Query

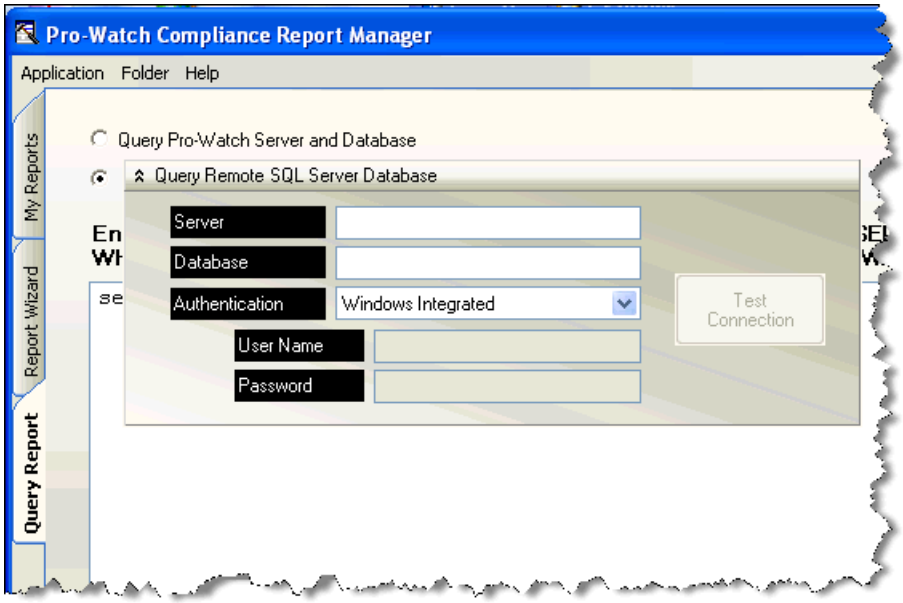
The Query Wizard enables you to run a query report from either a Pro-Watch or SQL remote database. The default option is to run a query report from a Pro-Watch Server and database::



1. Unless you are using a runtime filter to query, use the format shown to create the query:

   ```
   select lname 'Last Name', fname 'First Name' from BADGE
   ```

Alternatively, you can run a query report from a remote SQL Server database::

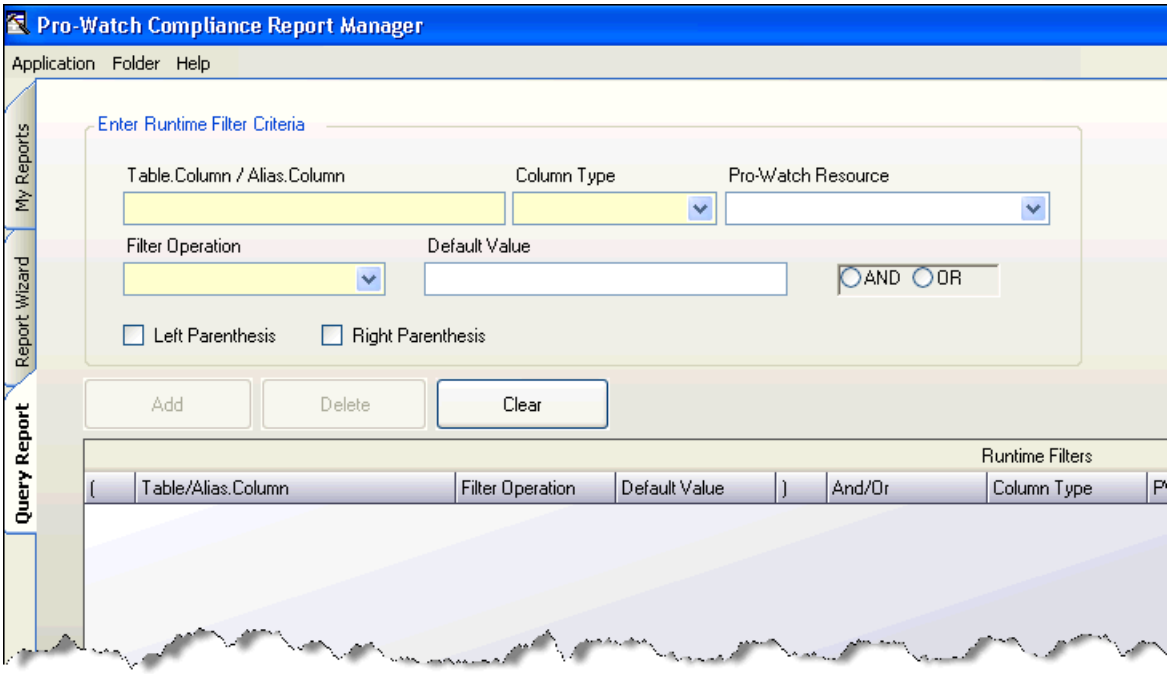


Complete the pop-up window:

Table 4-4: Query Remote SQL Server Database Fields

Field	Description
Server	Enter the server name.
Database	Enter the database name.
Authentication	Windows Integrated - SQL Server -
User Name	Enter a valid user ID for the server machine.
Password	Enter the password for the user ID.
Test Connection	Press this button to test for a valid server connection.

2. After entering the query, click **Next** to display the **Runtime Filter Criteria** screen.:

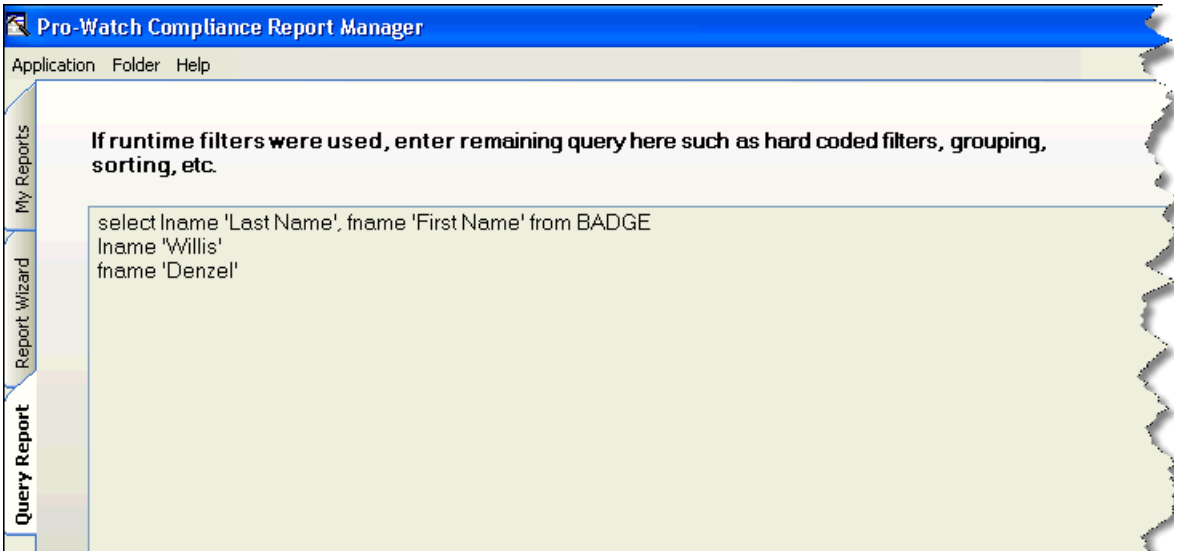


Use the information in Table 4-5 to complete the screen:

Table 4-5: Runtime Filter Criteria Fields

Field	Description
Table Name/Alias Column	The selection criteria database column or alias. If an alias is used in the query, the alias must be used here.
Column Type	Type of data (date, text, numeric, etc.) the user enters.
Pro-Watch Resource	If the run-time filter is from a list of values such as logical devices or Clearance Codes, the runtime filter can display a drop-down with the list of valid values.
Filter Operation	Equals, Begins With, etc.
Default Value	Default value to display to the user in the runtime filter.
AND/OR	AND or OR for the next filter.
Left/Right Parenthesis	Parenthesis can be used.

3. Click **Next**. If you used runtime filters, complete the query at this screen by adding any hard-coded filters or groupings. The top box displays the query as defined so far; the bottom box displays any additional query criteria that you are entering.:



4. Click **Next** to display the **Query Report Summary** screen.



5. Enter the Report Title in the top box. The **Final Query** box displays the query in its entirety.
6. Click **Finish** to display the resulting report.

4.10 Administrative Tasks

This section describes tasks related to managing and maintaining the Compliance Report Manager:

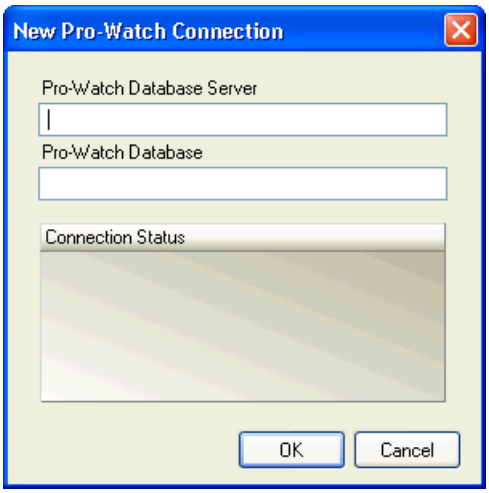
- Creating a new connection.
- Setting up a shared repository.
- Scheduling reports.
- Setting up display parameters.

4.10.1 Creating a New Connection

The Compliance Report Manager includes a function that enables you to access another database. For example, you can offload some information to another server, or, conversely, review or acquire data from other databases.

To create a new connection:

1. Click **Application > New Connection** to view the New Pro-Watch Connection dialog box.:



2. In the Pro-Watch Database Server field, enter the name of the server you are setting up a connection with.
3. In the Pro-Watch Database field, enter the name of the corresponding database on that server, and click **OK**. The Connection Status box displays the progress of the connection setup. If you enter any misspellings or errors, they appear in the Connection status box.
4. When the connection is established, the Compliance Report Manager display changes to show the content of the new server/database.

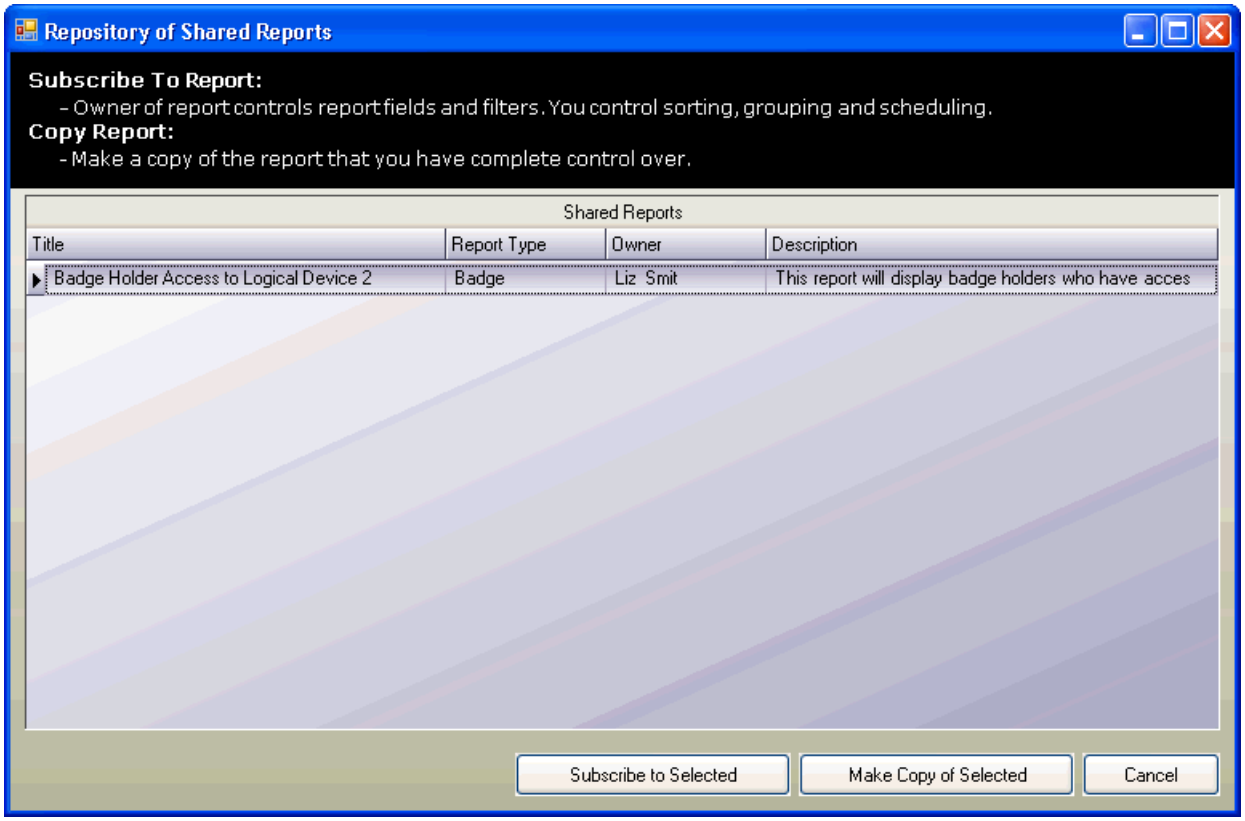
4.10.2 Setting Up a Shared Repository

"Sharing Reports" on page 17 describes how to share reports and where they can be accessed. The shared repository is created by default as soon

as one user designates a report to be shared by a user on another server/database. Users with access can subscribe to and copy reports in the repository.

To access and use a shared repository:

1. Click **Application > Shared Repository** to access the Repository of Shared Reports where shared reports are listed.



2. Select the report you want to access.
3. To subscribe to the selected report, click **Subscribe to Selected**. The report will appear on your My Reports tab and you can access it there.
4. To copy the selected report, click **Make Copy of Selected**. The report will appear on your My Reports tab; you now own the report and can make any edits to the report.

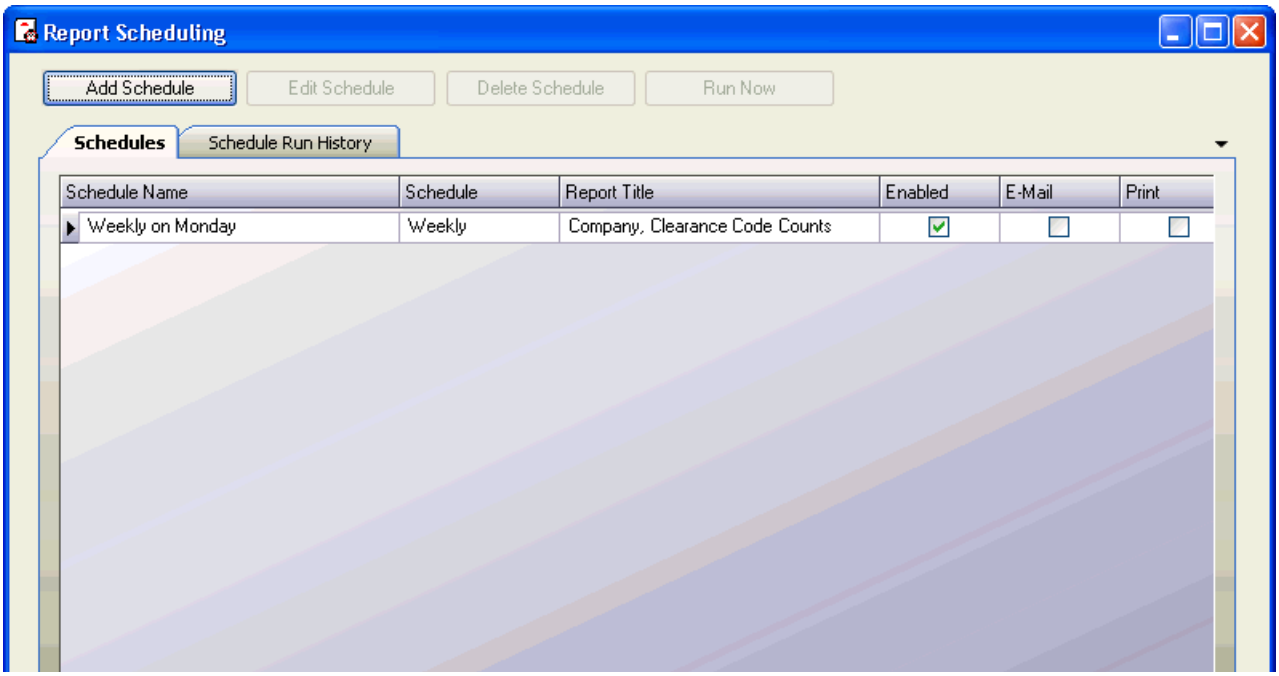
4.10.3 Scheduling Reports

The Report Scheduling function enables you to add, edit, delete, and run reports at scheduled intervals and export them to files or folders, and review historical information on the frequency and dates when a schedule has been run.

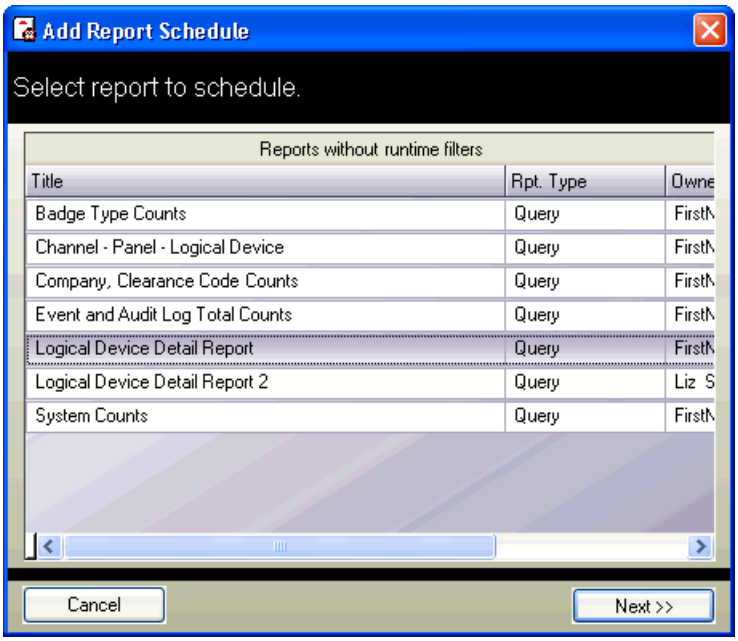
4.10.3.1 Adding a Schedule

To schedule a report:

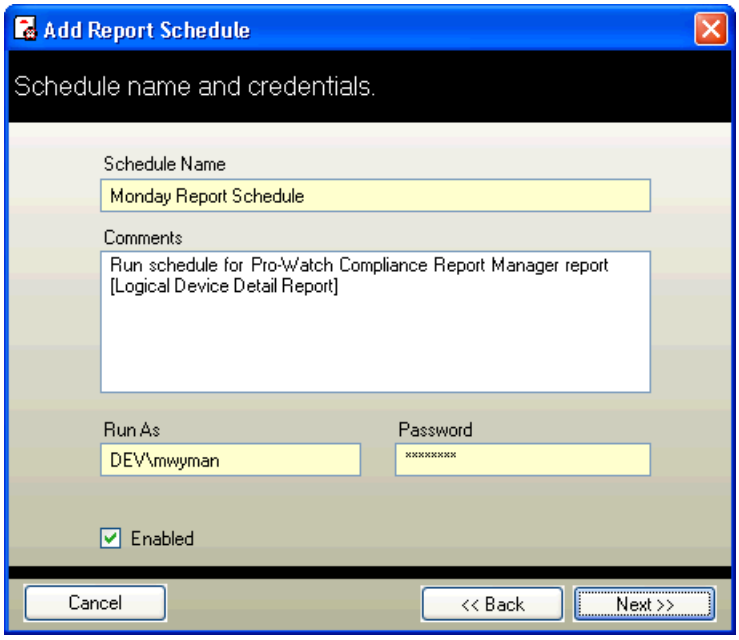
1. Click **Application > Schedule Reports** to display the **Report Scheduling** screen.



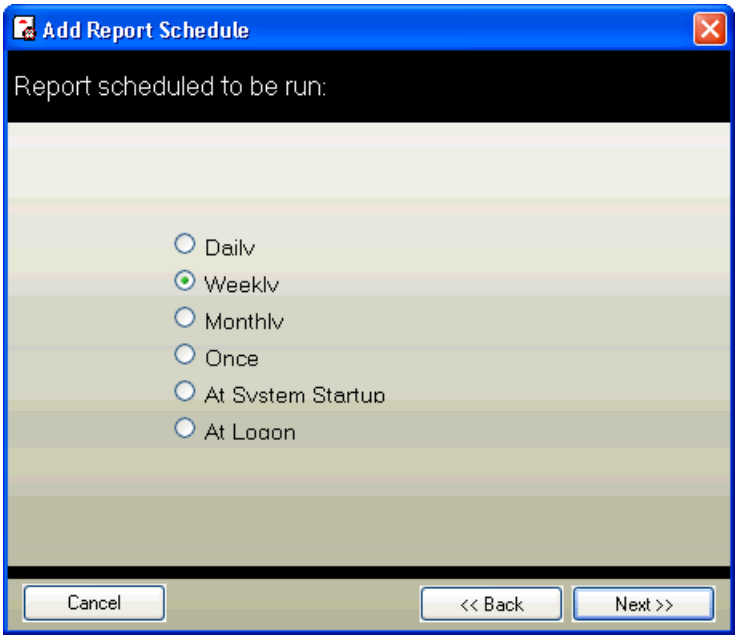
2. Click **Add Schedule** to display a list of reports without runtime filters that are available for scheduling.



3. Select the report and click **Next** to display the Schedule Name and Credentials dialog box.

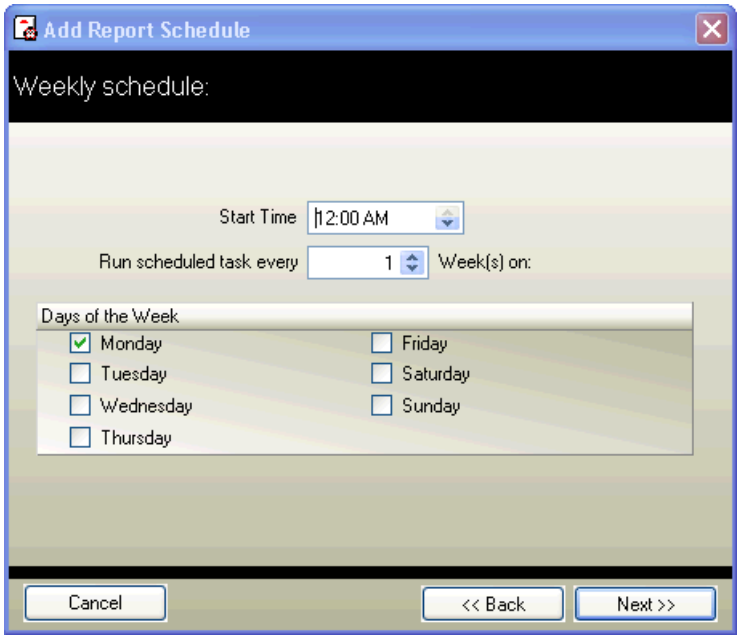


4. Enter a name for the schedule and enter your login password and click **Next** to display the Report Scheduled To Be Run box.

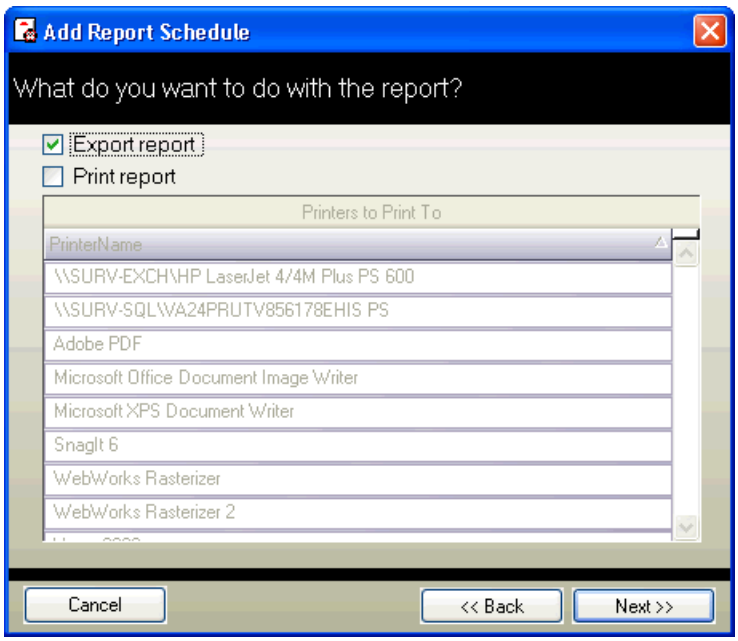


5. Click the desired frequency and click **Next** to display the screen of parameters for the frequency selected. The following screen shows

weekly schedule parameters; other frequencies show other parameters.

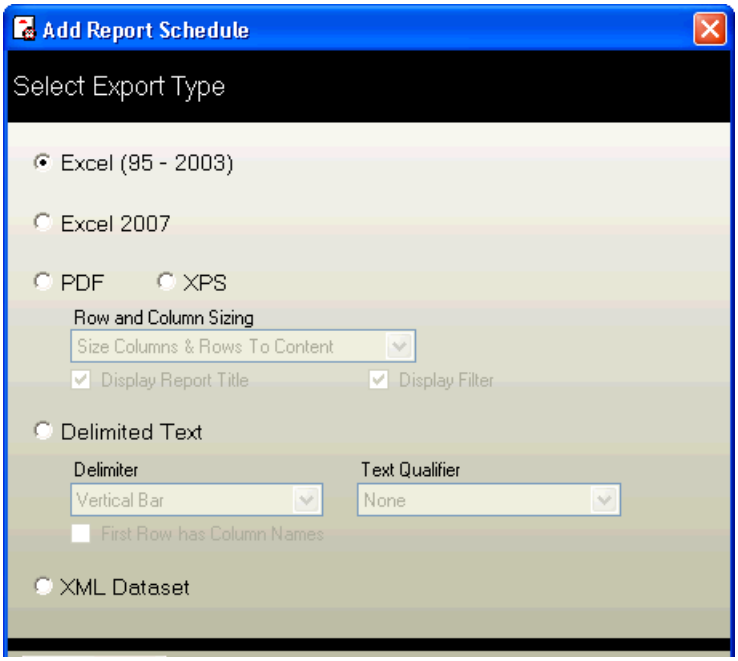


6. Enter the requested information and click **Next** to display the report disposition screen.



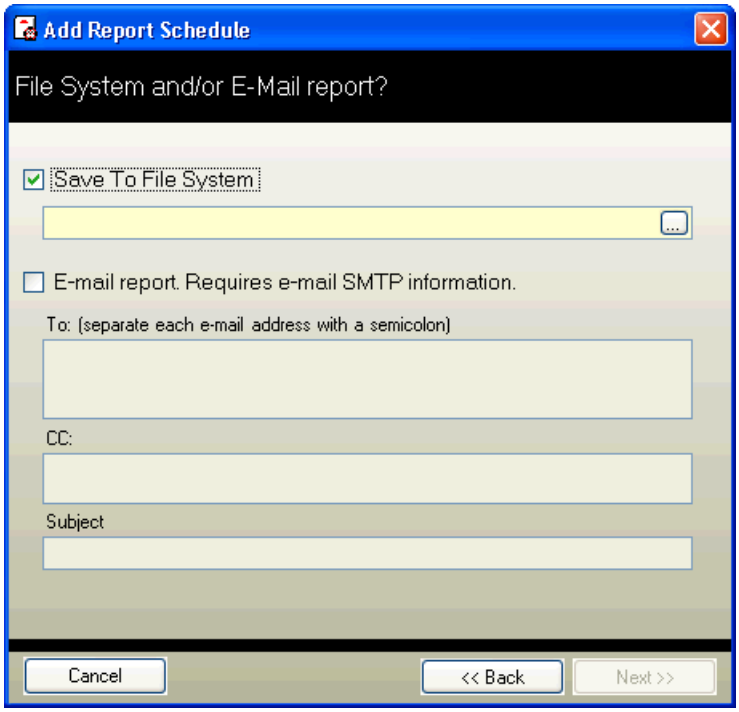
On this screen you can specify whether you want to export the report or print it, or both. To export the report, go to Step 7. To print the report, go to Step 10.

7. To export the report, click the checkbox for Export Report and click **Next** to display the Select Export Type box.



Depending on the export type you choose, additional specifications are required.

8. Select the export format you want and click **Next** to display the File System and/or E-Mail report box.

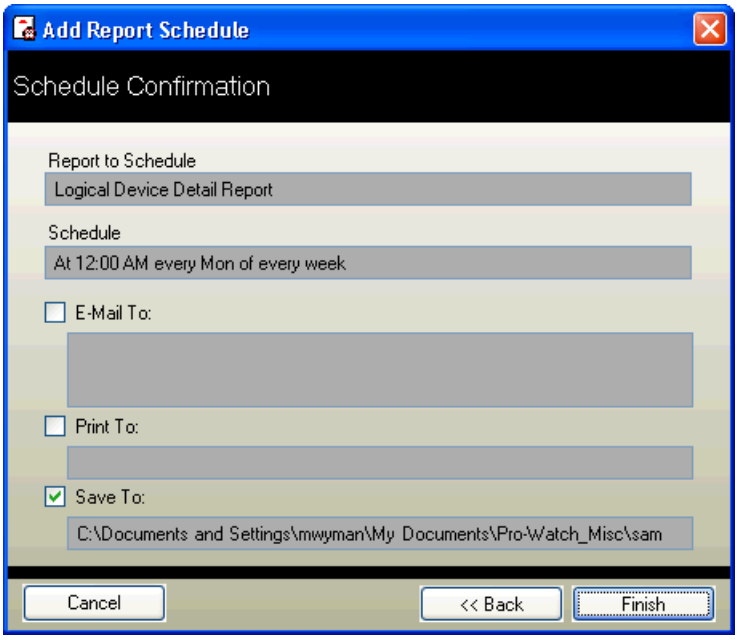


Note: While this example reflects the selection of Excel as the export type, the other export types also proceed to this screen. Use this box to indicate whether you want to save the report to a particular folder/directory, and/or e-mail it.

9. To save to a file, click the box for Save to File System and then click the **Browse** button to display your folders/directories and select the destination and click **Next** to display the Schedule Confirmation box.

   To e-mail the report, click the box for E-Mail report using default e-mail client and enter the requested information and click **Next** to display the Schedule Confirmation box.

10. To print the report, click the Print Report box to display a list of available printers. Select the desired printer and click **Next** to display the Schedule Confirmation box.

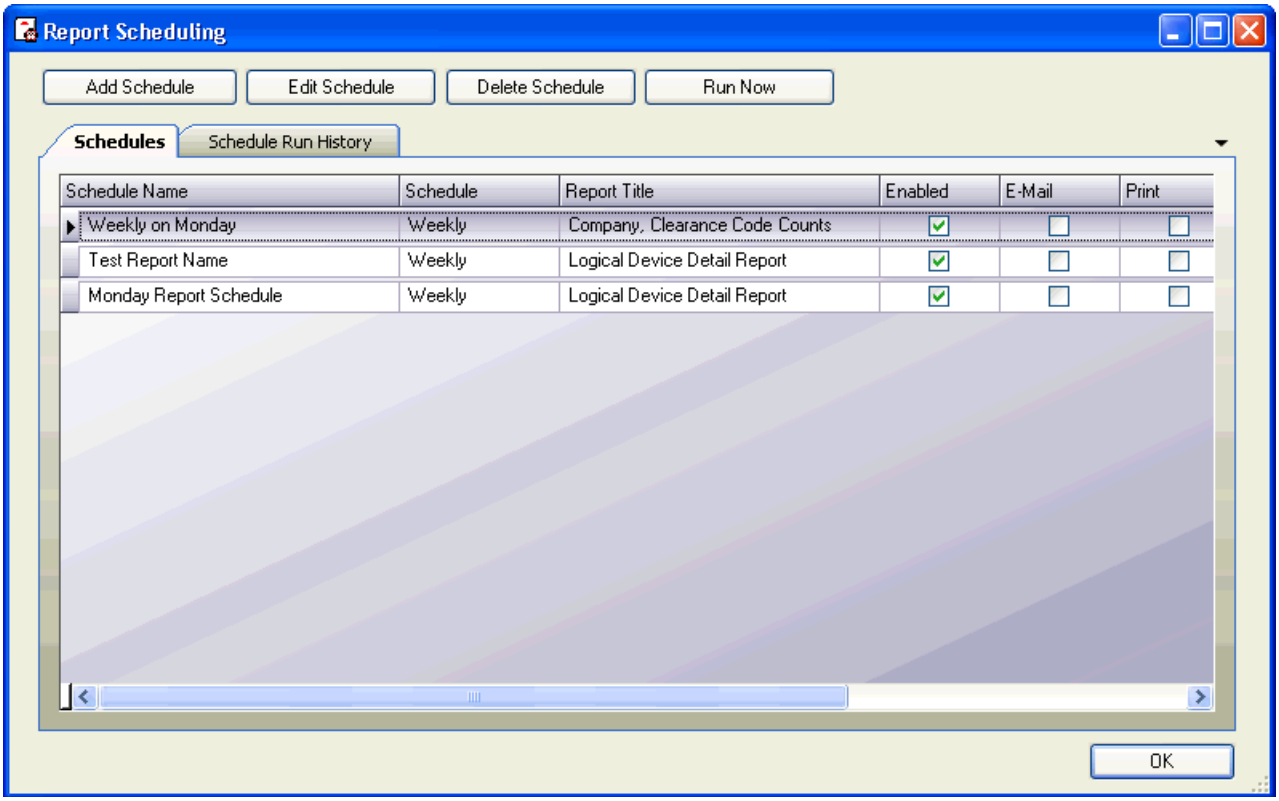


11. Review your selections. To accept them, click **Finish**; to change a selection, click **<<Back** to return to the screen that displays a selection you want to change.

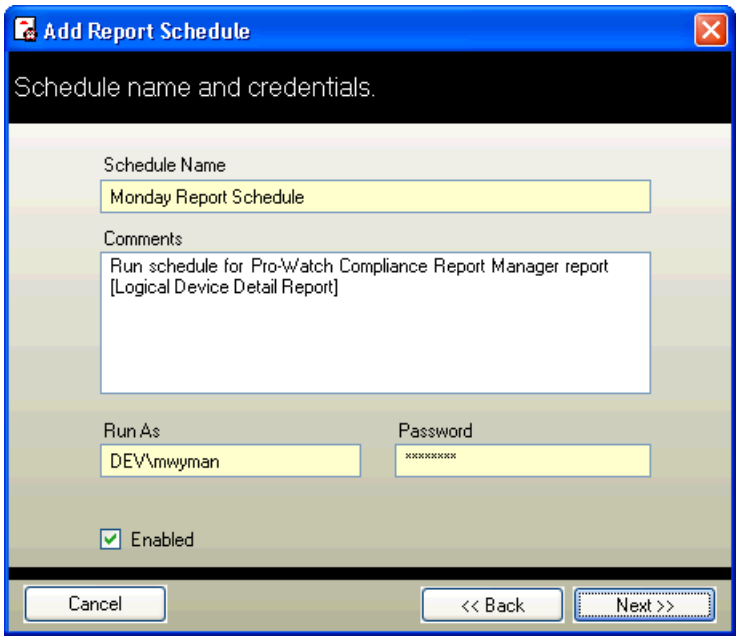
4.10.3.2 Editing a Schedule

To edit a schedule:

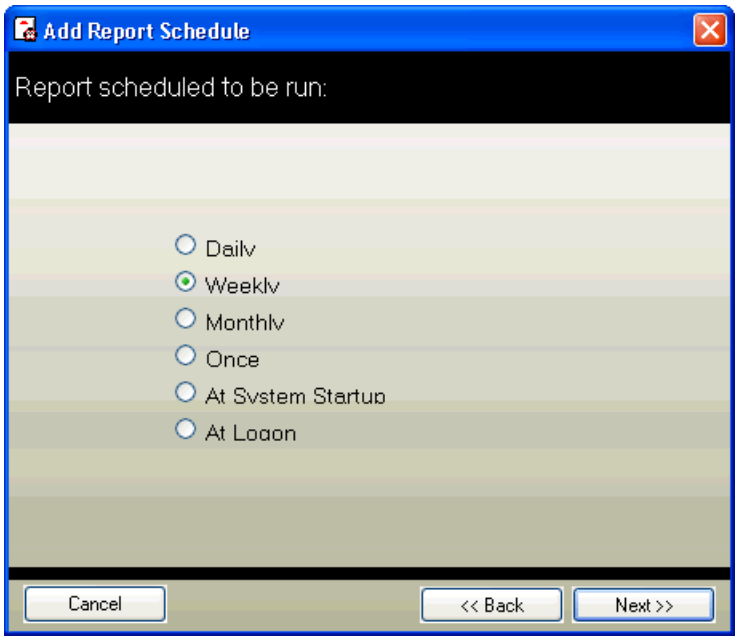
1. Click **Application > Schedule Reports** to display the **Report Scheduling** screen.



2. On the Schedules tab, select the schedule you want to edit and click **Edit Schedule** to display the Schedule Name and Credentials box.



3. The schedule name is already entered. Enter your password and click **Next** to display the Report Scheduled To Be Run box.

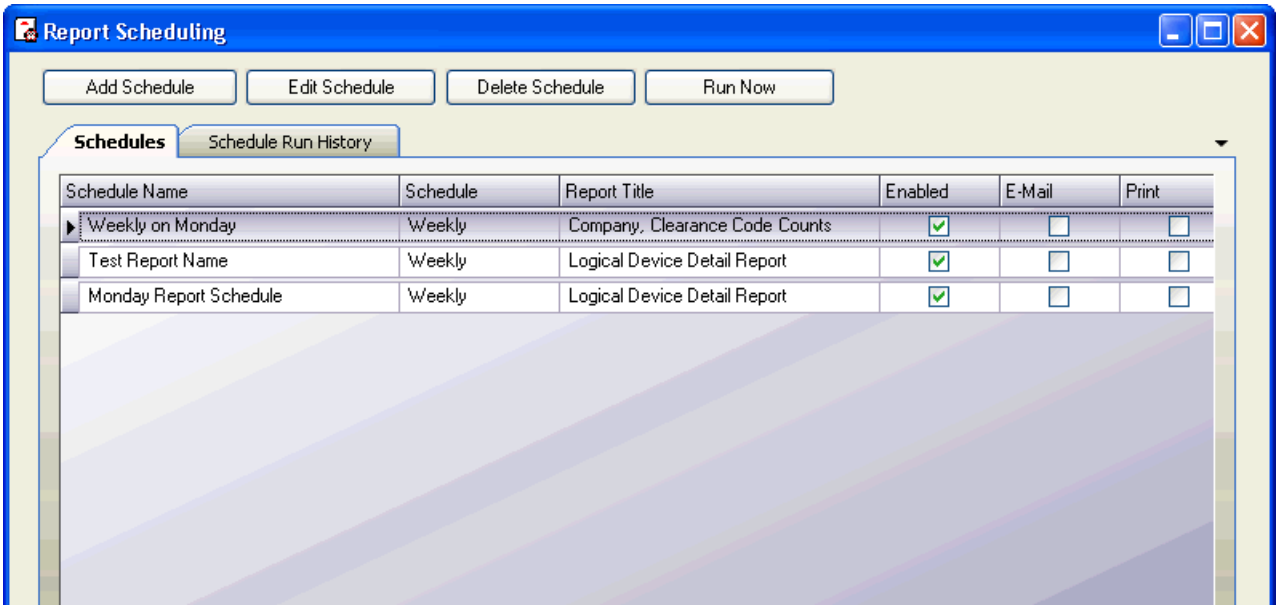


4. Repeat Steps 5-through-11 on page 41 through page 44 to make any necessary modifications.

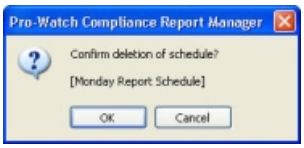
4.10.4 Deleting a Schedule

To delete a schedule:

1. Click **Application > Schedule Reports** to display the Report Scheduling screen.



2. On the Schedules tab, select the schedule you want to remove and click **Delete Schedule** to view the confirmation prompt.

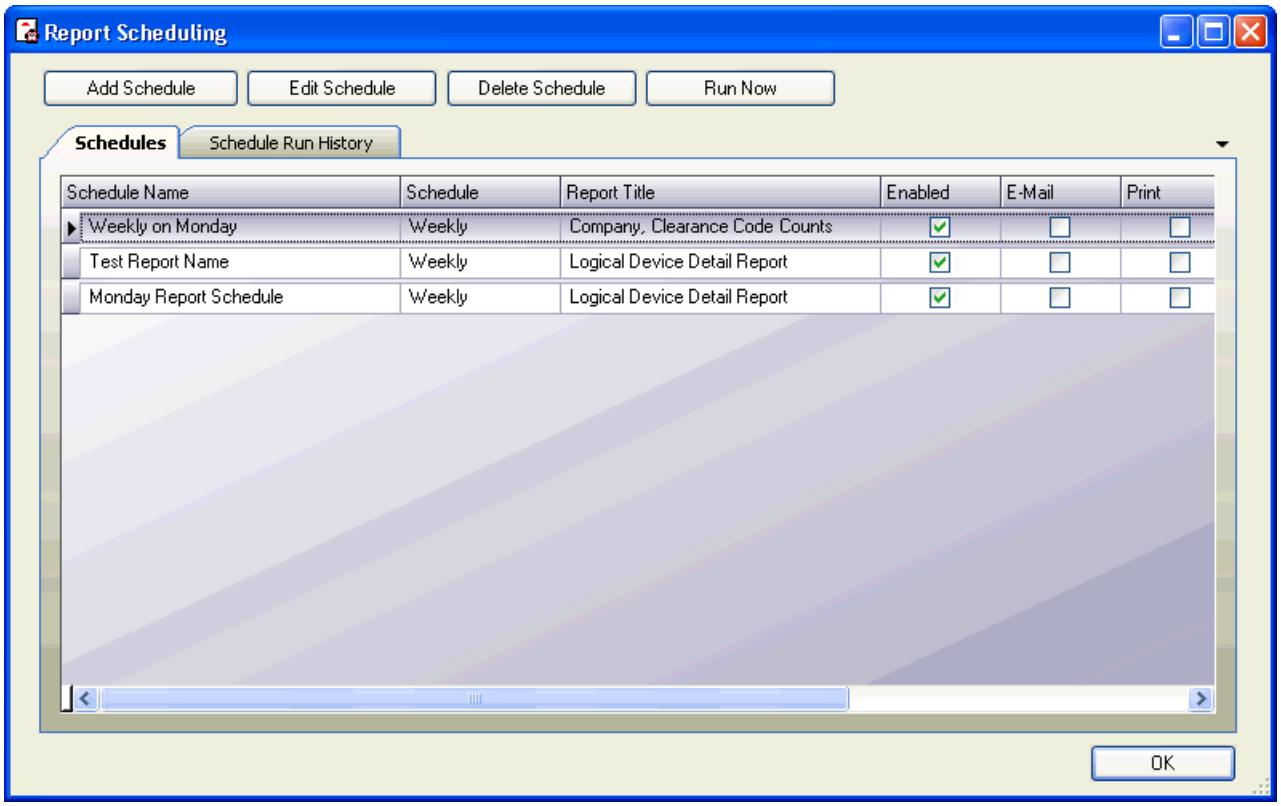


3. Click **OK**. The report is removed from the schedule.

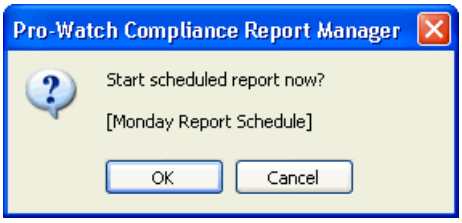
4.11 Running a Report on Demand

To run a report on demand:

1. Click A**pplication > Schedule Reports** to display the Report Scheduling screen.



2. On the Schedules tab, select the schedule you want to run and click **Run Now** to view the confirmation prompt.



3. Click **OK** to run the report. The report is exported or printed to a file you have previously specified.

4.12 Reviewing Schedule Run History

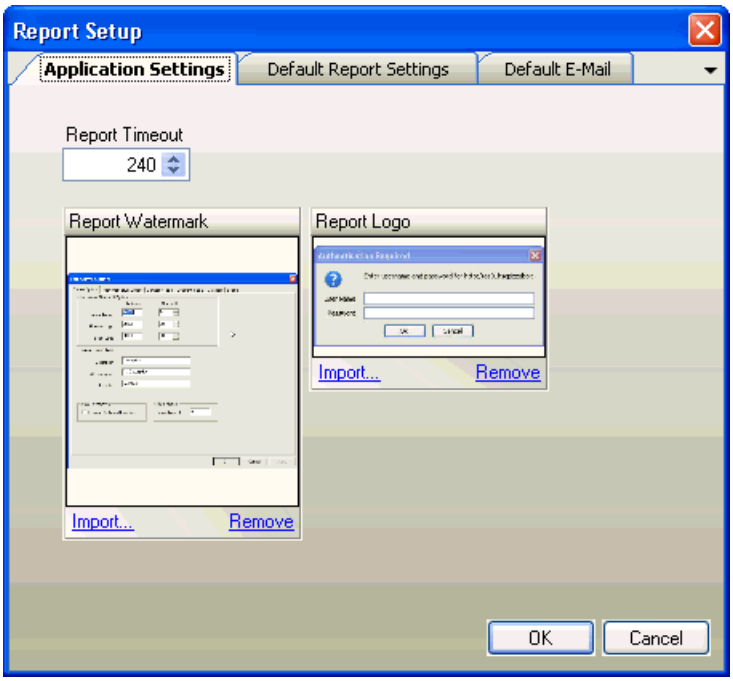
To review the schedule run history:

1. On the **Report Scheduling** screen, click the Schedule Run History tab. The tab displays the run history.
2. Click **OK** to close the display.

4.13 Setting Display Parameters

To set display parameters:

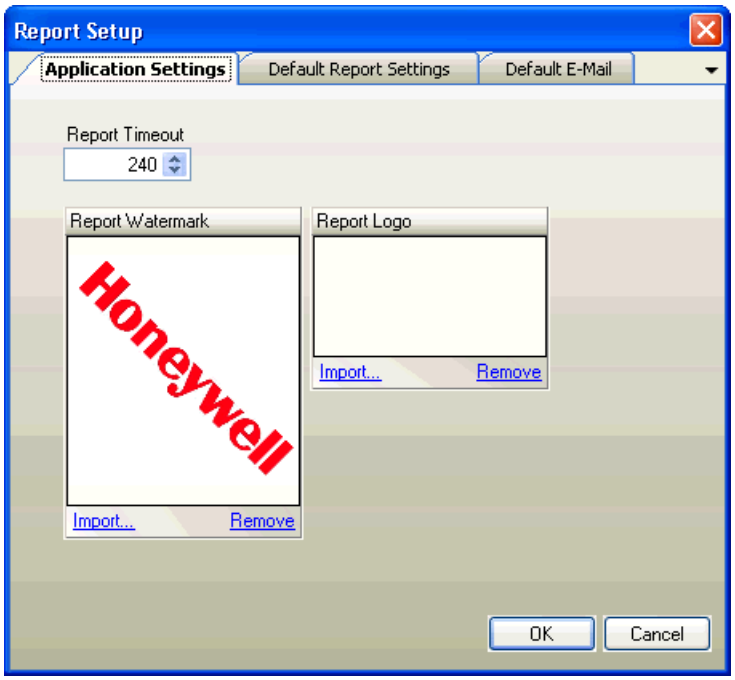
1. Click **Application > Setup** to view the Report Setup dialog box.



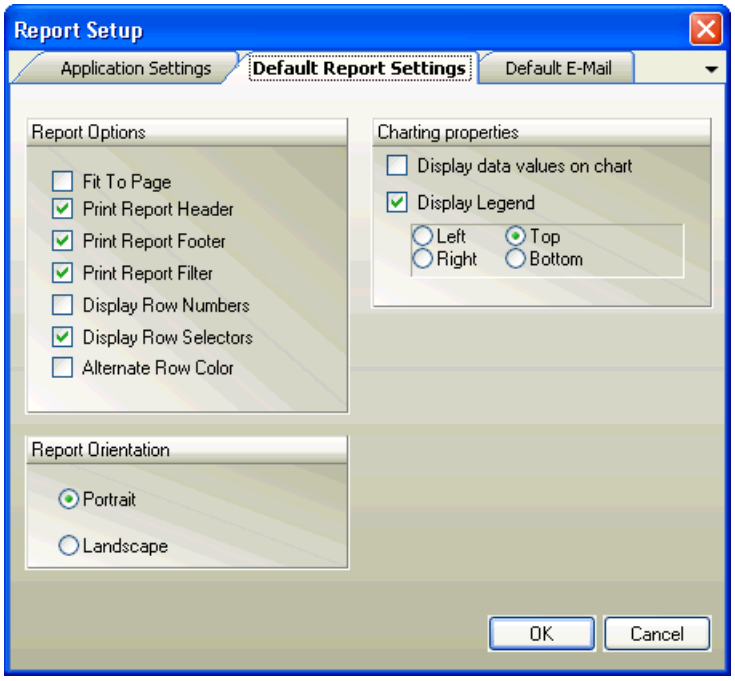
2. On the **Application Settings** tab, in the **Report Timeout** field, select the number of seconds you want to display the report before it closes.

   Note: After the number of seconds has elapsed, the report displays a timeout error. The purpose of this setting is to prevent reports that are not properly filtered from running endlessly and killing the database.

3. In the **Report Watermark** box, click **Import** to access the directory where the desired watermark is and select it.

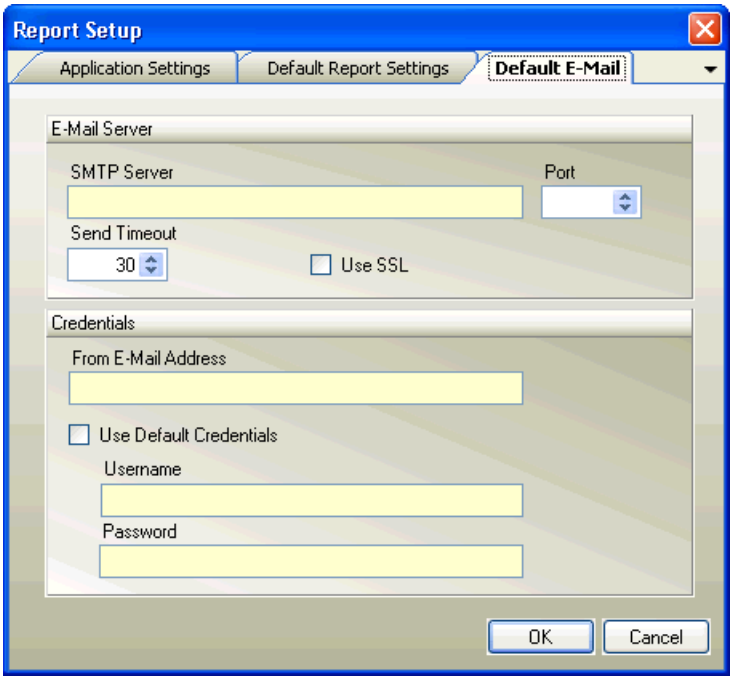


4. In the **Report Logo** field, click **Import** to access the directory where the desired logo is and select it to appear in the upper right-hand corner of the report.
5. Click the **Default Report Settings** tab to display it.



This box displays three types of settings: report display, orientation, and charting.

6. Check your desired selections and click **OK** to save them.
7. If necessary, click the Default E-Mail tab to enter your e-mail server parameters.



8. Enter your server and credential information and click **OK**.

4.14 Switching the Report Modules

Depending on whether you are a new user or an existing user, your Pro-Watch software will include the **Compliance Reports** module or the **Classic Reports** module.

This section describes how to change from one module to the other.

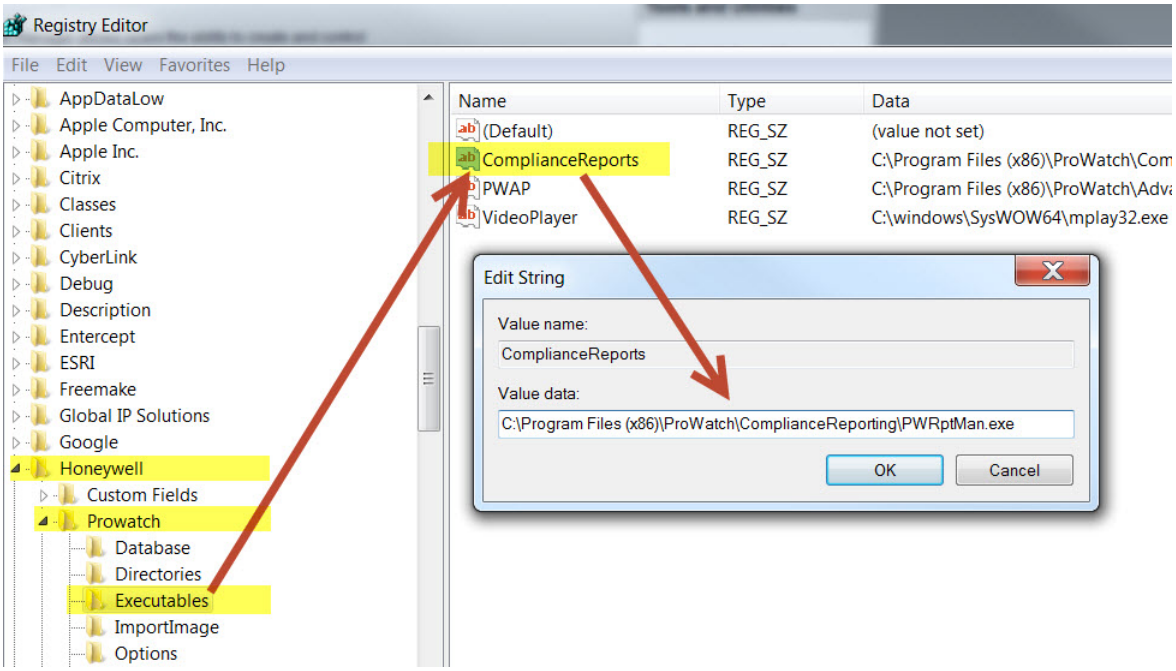
To make such a change, you must modify the **registry keys**.

Caution: The registry keys govern the operation of your PC, and any changes to registry keys may have a serious adverse impact on your PC. Therefore, any such changes should be performed only by someone who is qualified to make such changes. If you are not familiar with registry keys, contact your system administrator for assistance.

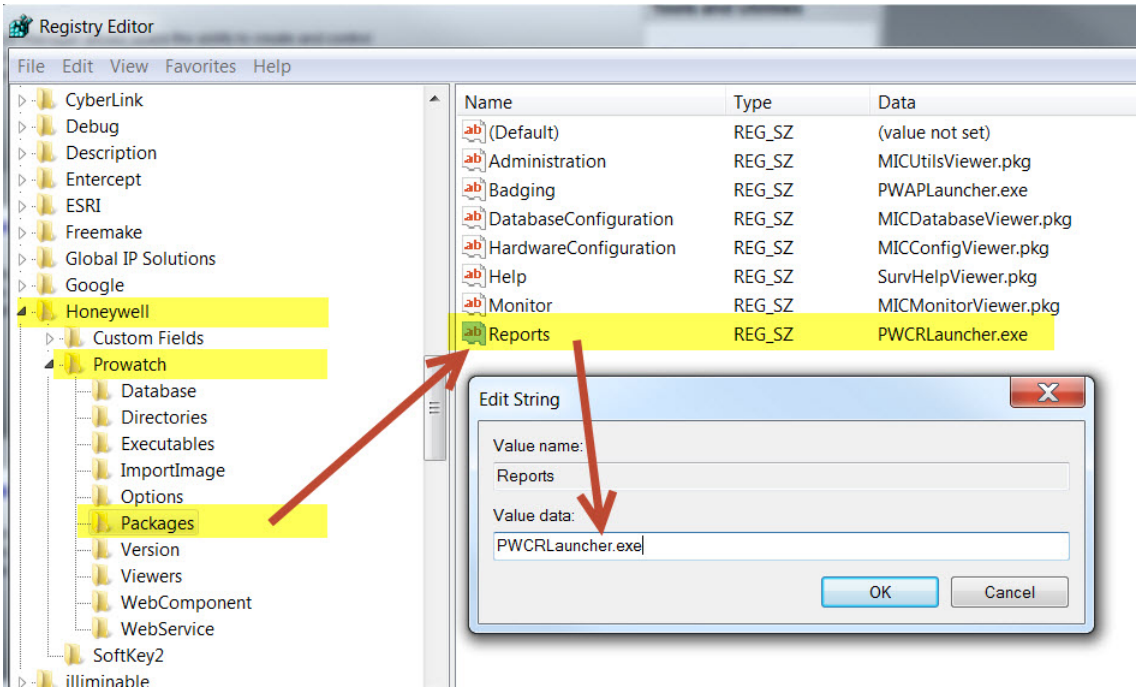
4.14.1 To switch from classic reports to compliance reports

1. Verify that the PWCRLauncher.exe executable file is located in the ProWatch\Bin directory.
2. On your Pro-Watch machine, click **Start > Run** and type **regedit** in the Open field to open the **Registry Editor**.
3. Navigate to the Pro-Watch registry settings at HKEY_LOCAL_MACHINE\Software\Honeywell\ProWatch for a 32-bit machine. For a 64-bit machine, navigate to the Pro-Watch registry settings at HKEY_LOCAL_MACHINE\Software\WOW6432Node\Honeywell\ProWatch.
4. In the Honeywell\ProWatch Executables directory, create a new string key for **Compliance Reports** and point it to the executable for

Compliance Reports (usually C:\Program Files (x86)\ProWatch\ComplianceReporting\PWRptMan.exe):



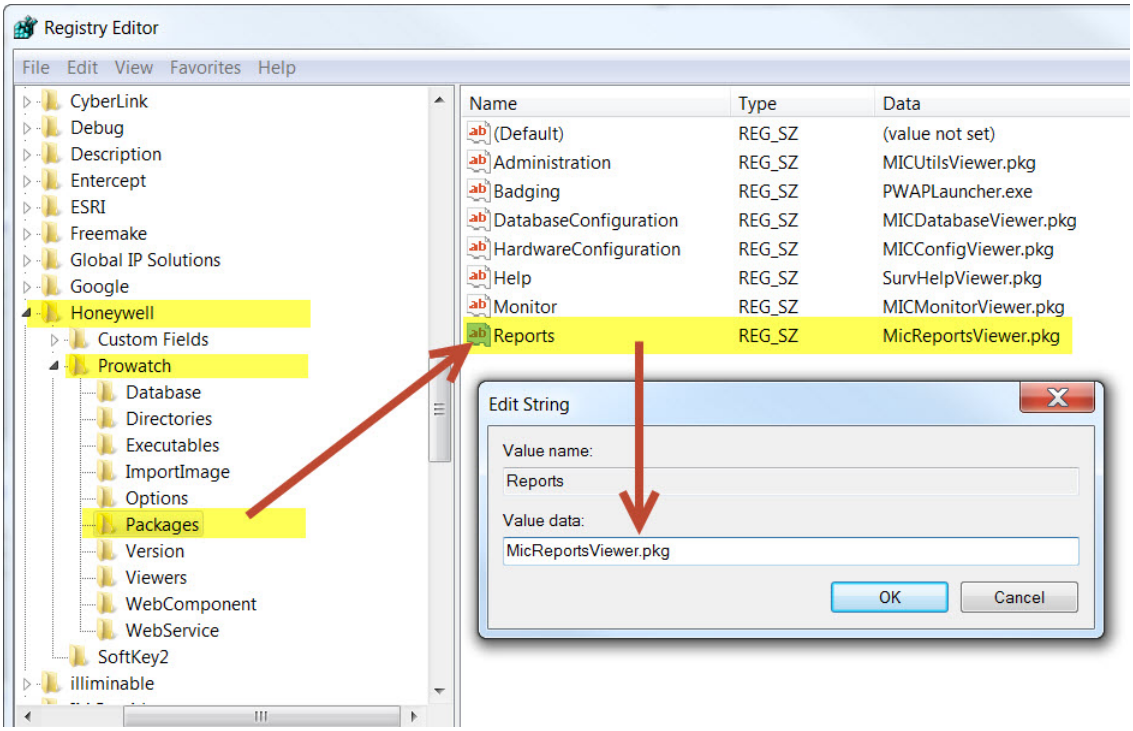
5. In the Honeywell\ProWatch\Packages directory, edit the **Reports** key to PWCRLauncher.exe :



6. Restart Pro-Watch for the change to take effect.

4.14.1.1 To switch from compliance reports to classic reports

1. In the Honeywell\ProWatch\Packages directory, edit the **Reports** key to MicReportsViewer.pkg :



2. Restart Pro-Watch for the change to take effect.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Overview of Administrator Functions

5

In this chapter ...

Overview

Pro-Watch Functions

Server Options

Duress Signal via "Appended Digit" Option

Setting the Log Size

Pro-Watch Topologies

Pro-Watch Remote Server Topology

Pro-Watch Configuration Preview

Tool Bar

5.1 Overview

The Pro-Watch platform is a complete access control system of hardware and software for small, mid-size, and global-enterprise sites. You can configure sites that range from five users and 64 doors to an unlimited number of users and doors.

NOTE: Creating more than 100 channels per site is not recommended since it may lead to database corruption.

The Pro-Watch system supports Honeywell and third-party access control hardware and software, including panels, readers, intercom units, and CCTV equipment.

Part II of this guide (Chapters 5-12 and Appendices B through M) is intended for Pro-Watch system administrators. It explains how to configure the Pro-Watch hardware and database, create badging profiles, and perform other administrative tasks. Specifically, the administrator functions include the following:

- Designing and configuring the Pro-Watch topology for the facility. See "Pro-Watch Topologies".
- Configuring the system's hardware. See Chapter 6, .
- Configuring the system's database. See Chapter 27, *Database Configuration (DBC)*.
- Managing the system's data. See Chapter 63, *Data Management*.
- Configuring the system's badging profiles. See Chapter 60, *Badge Building*.
- Managing the registry. See Chapter N, *Registry Management*.
- Building maps. See Chapter 61, *Map Building*.
- Setting up the Biometric Hand Reader. See Chapter 62, *Biometric Reader Configuration*.
- Enabling Pro-Watch Secure Mode. See Appendix A, Secure Mode Verification.
- Assigning program access to database entities such as Classes, Users, and Event Procedures. See Appendix B, Assignable Programs.
- Configuring dial-up communications. See Appendix C, Dial-Up Configuration.
- Managing the Pro-Watch database size with Remote Terminal Services. See Appendix D, Remote Terminal Services.
- Installing the Magicard Prima Printer. See Appendix E, Magicard Prima Printer Installation.
- Moving panels. See Appendix F, Moving Panels.
- Badging. See Appendix G, Badging.
- Generating various types of reports. See Appendix H, Reports.
- Configuring the Pro-Watch/Morpho Biometric integration. See Appendix I, Pro-Watch Biometric Service.

- Configuring Mercury M5 Bridge. See Appendix J, Mercury M5 Bridge.
- Configuring the Two-Person Rule. See Appendix K, Two-Person Rule.
- Configuring the PW5K Conversion Utility. See Appendix L, PW5K Conversion Utility.
- Configuring the Partition Manager. See Appendix M, Partition Manager.
- The Registry Management. See Appendix N, Registry Management.
- Galaxy Dimension Integration Guide. See Appendix O, Galaxy Dimension Integration Guide.
- Extended Card Number Support. See Appendix P, Extended Card Number Support.
- IRIS ID Integration. See Appendix Q, IRIS ID Integration.
- Software Keys Licensing. See Appendix R, Software Keys Licensing.
- TBS Integration. See.Appendix S, TBS and Pro-Watch Integration

Note: This part of the guide is not intended for the individual who will use Pro-Watch after it is configured. Typically, security personnel or another user will use the configured Pro-Watch system to monitor and respond to reported events, issue badges to employees, or create reports of system activity. See "Part I ~ User Functions" for information about these user functions.

5.2 Pro-Watch Functions

The Pro-Watch main screen below displays six categories of functions in the left pane as well as a menu bar and a tool bar. This part of the guide describes the functions in the following three categories:

- Hardware configuration.
- Database configuration.
- Administration.

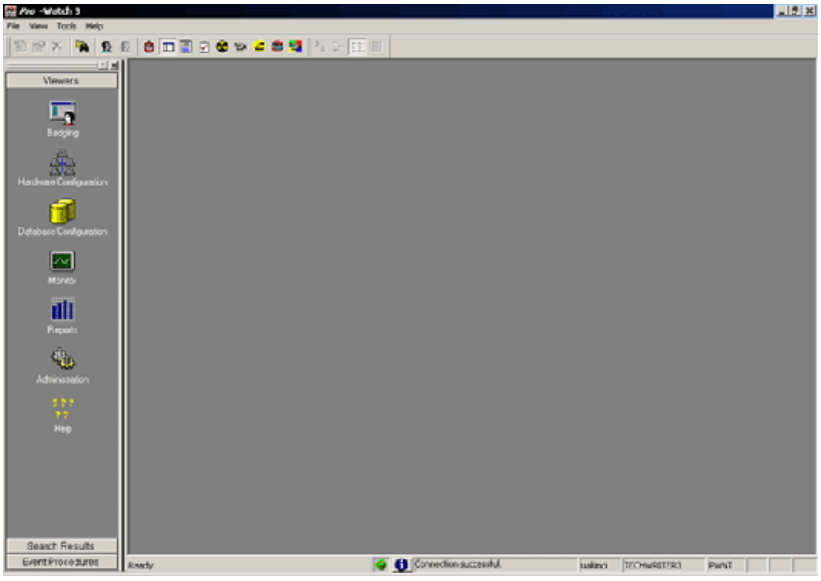


Figure 5-1 Pro-Watch Main Screen

5.2.1 Badging

Pro-Watch Badging manages badge holder access privileges within your enterprise. A badge holder assumes the access privileges that are assigned to the holder's company class. The badge holder's access privileges are further defined by the cards the holder uses to gain access to doors.

See Chapter 2, .

5.2.2 Hardware Configuration

The Pro-Watch access control system supports hardware, including Honeywell and third-party panels, logical devices (readers, monitorable inputs and controllable outputs), closed circuit television (CCTV) and digital video recorders (DVR).

Within the Hardware Configuration component, these various hardware types are added and configured; for example, logical devices are configured in functional groups, which are defined by hardware templates. These logical devices, as well as panel, CCTV and DVR hardware, are also

governed in the Pro-Watch system by a number of database entities, such as routing groups, clearance codes, and time zones. Therefore, completing the Pro-Watch configuration requires tasks to be executed within the Database Configuration component of Pro-Watch as well.

See Chapter 6, .

5.2.3 Database Configuration

The Pro-Watch access control system is organized and managed by a variety of software objects, or database elements, which you configure. These database elements control the specific Pro-Watch hardware items.

See Chapter 27, Database Configuration (DBC).

5.2.4 Monitor

The Alarm Monitor enables you to see and act upon the real-time status of alarms as they occur. Alarms are reported on an alarm page which displays the alarm types. For each alarm type, the specific alarms appear in order of priority and occurrence.

The Alarm Monitor also provides an Alarm Rollup function that displays multiple events for a single logical device in a single line.

See Chapter 3, .

5.2.5 Reports

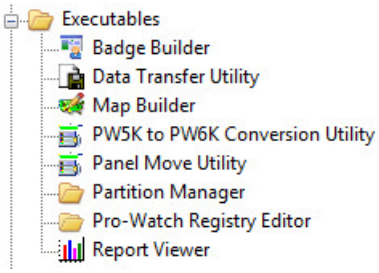
You can produce a comprehensive report of any Pro-Watch data group of your choice in a few keystrokes. You can select data to match specified criteria, sort the data by specified fields, and partition the report. You can preview, print, or export the report. These are the general categories of reports you can generate:

- Access reports
- Badge holder reports
- Company reports
- Configuration reports
- Logging reports
- User reports

You can also design your own report.

See Chapter 4, .

5.2.6 Administration



Pro-Watch provides the following administrative executable applications:

- **Badge Builder** – builds a badge profile. See Chapter 60, *Badge Building*.
- **Data Transfer Utility** – imports and exports data to and from Pro-Watch database tables to and from the following:
  - SQL/Microsoft Access database tables.
  - Delimited text files. See Chapter 63, *Data Management*.
- **Map Builder** – places resource icons on a Pro-Watch map. See Chapter 61, *Map Building*.
- **PW5K to PW6K Conversion Utility.** See Appendix L, PW5K Conversion Utility.
- **Panel Move Utility**. See Appendix F, Moving Panels.
- **Partition Manager**. See Appendix M, Partition Manager.
- **Pro-Watch Registry Editor** – edits Pro-Watch's registry key values. See Chapter N, *Registry Management*,
- **Report Viewer** – creates, prints, or exports Pro-Watch reports. See Appendix H, Reports.

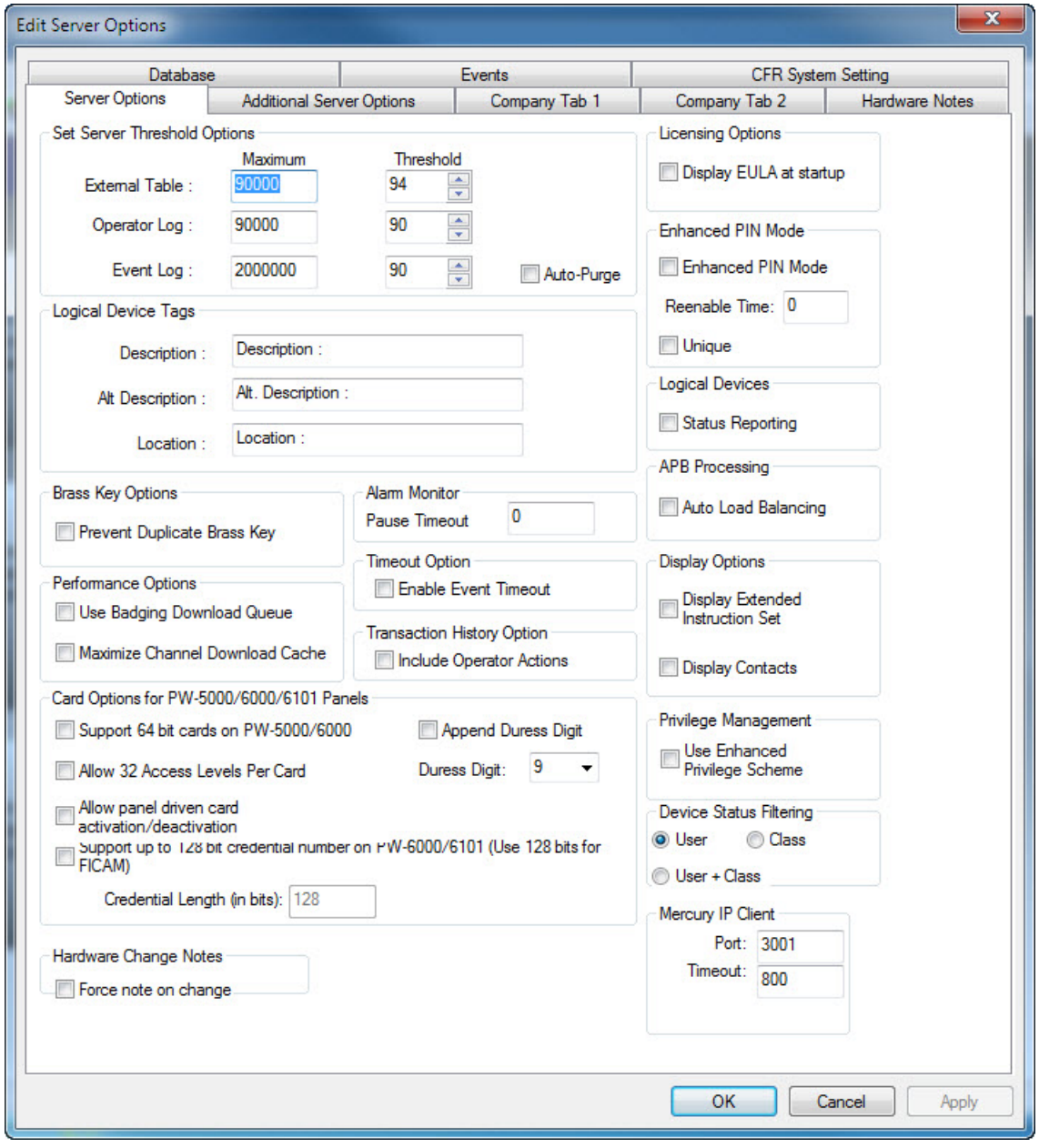
5.3 Server Options

You can also set the following administrative values at the server level:

- Event log thresholds.
- Logical device tags.
- Clearance code, logical device, and company tab labels.
- Card number seed, or card number starting point.
- Set mail options.
- Badge photo compression and intensity.

- Company tabs.
- Database limits.

5.3.1 Server Options Tab



5.3.2 Setting Event Log Thresholds

Pro-Watch maintains an event log that records all transactions. This log is checked periodically by the server and a message is generated in the Windows event log when the log exceeds a specified threshold. You can

specify the event log threshold and the frequency that the log is checked. This function prevents a system shutdown caused by excessive database size.

When a threshold is breached, you must purge the database. There are two ways to purge the database:

- Using Auto-Purge (only available with an MSDE database). If Auto-Purge is set, when the system determines that a log has exceeded a specified threshold, it purges the database of records based on the oldest timestamps. The auto-purge function is not supported on SQL-based servers. When in use, Auto-Purge starts **at the top of the hour** after the maximum event level threshold is breached. Auto-Purge never starts immediately.
- Purging the database manually.

Caution: The database **MUST** be purged periodically. If it is not, it will reach its maximum limit and shut down.

Note: Pro-Watch does not currently support the Operator threshold or the External Table threshold.

To set a threshold for the event log:

1. Select **File > Server Options** from the Pro-Watch menu bar to display the **Edit Server Options** dialog box, **Server Options** tab.

Note: In the **Maximum** field, enter the maximum number of messages or rows that you would like the log file to maintain. This number might depend upon the size and general usage of your database. Note that the log file will not stop accumulating messages at this maximum number, unless you are using an MSDE-based server and you have checked the Auto-Purge checkbox on the Server Options tab.

Auto-Purge works only with an **MSDE database** and starts at the **top of the hour** after the maximum event level threshold is breached. Auto-Purge never starts immediately.

Note: In the **Threshold** field, enter a percentage of the maximum number you entered in the previous step. When Pro-Watch generates this percentage of messages, it generates a threshold crossing alert. This alert enables you to archive, or off-load, the log file before exceeding your desired maximum number of messages. For example, if you entered 90,000 in the Maximum field and 90 in the Threshold field, the threshold is set at 90% of 90,000, or 81,000 events. Pro-Watch would generate an alert at 81,000 events, but it will continue to add messages to the event log beyond the 90,000 maximum unless you are running an MSDE-based server and you have checked the Auto-Purge check box.

Auto-Purge works only with an **MSDE database** and starts at the **top of the hour** after the maximum event level threshold is breached. Auto-Purge never starts immediately.

2. For MSDE-based servers only, activate or de-activate the auto-purge function by checking or un-checking the **Auto-Purge** check box.
3. Click **OK**.

5.3.3 Setting Performance Options

You can set performance options by selecting one or both of the following check-boxes:

- **Use Badging Download Queue --** Select to improve performance by using the stored procedure "THROTTLE_CARD_DN" when downloading a single card to all the installed panels.
- **Maximize Channel Download Cache --** Select to improve performance specifically that of Mercury panels by caching the downloads to the Mercury driver.

5.3.4 Setting Timeout Option

Select the "**Enable Event Timeout**" check-box to set LOCK_TIMEOUT SQL environment variable for event processing (in the "PROC_EVENT" stored procedure).

5.3.5 Setting Logical Device Tags

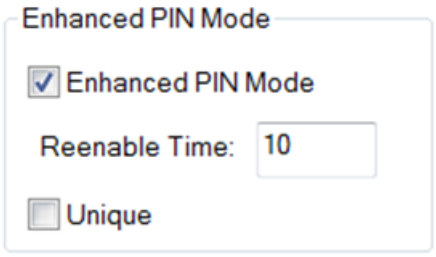
Pro-Watch logical device screens often include description, alternate description, and location fields. You can assign different labels for these fields. For example, you might prefer to change "Description" to "Name."

To rename logical devices:

1. Select **File > System Options > Server Options** from the Pro-Watch menu bar to display the **Edit Server Options** dialog box, **Server Options** tab.
2. In the Logical Device Tags section, enter Description, Alt Description, and Location information.

3. Click **OK**.

5.3.6 Enhanced PIN Mode



Enhanced PIN Mode group of controls provides two different check-boxes which can be selected independently of each other.

5.3.6.1 Check-Box 1: Enhanced PIN Mode

The Difference of the "Enhanced Mode"

Pro-Watch always requires the users to enter a correct PIN code whether the "enhanced mode" is selected or not.

However, by selecting the **Enhanced PIN Mode** check-box, the administrator can make sure that when the users enter consecutive incorrect PIN codes they will not have access to a door or logical device for a specified time period, a.k.a. "**Reenable Time**".

Reenable Time

The system bars the user from entering any PIN codes for the number of minutes specified in the **Reenable Time** field. The user can again try to enter the correct PIN only after the time entered into the **Reenable Time** field expires.

Note: There is no fixed number of times that the user can enter the wrong PIN code before the system denies any further tries. That number is set for each reader at the "**PIN Retries**" field of the **Reader Settings** tab of each panel.

PIN Code Requirements

A PIN code must be:

- at least 4 digits, and
- not have 3 or more repeating digits or 3 consecutive digits.

5.3.6.2 Check-Box 2: "Unique"

Unique check-box, when selected, makes sure that the PIN is unique. After the administrator makes this selection, he or she will be prompted to restart all badging applications currently in use.

5.3.7 Setting Logical Device Status Reporting

To enable the Logical Device Status Reporting option, select the **Logical Device Status Reporting** check-box in the **Edit Server Options** screen's **Server Options** tab as shown below, and then click **OK** at the bottom of the tab:



When selected, this feature provides an instant snapshot of the current status of a door.

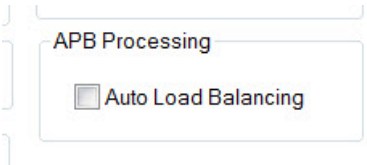
Without this functionality, the only way for a Pro-Watch user to get the current status is to go to Status Groups and select each status group. For a large site, this can take over a half hour. If someone masks a door or unlocks a door and a shift change happens, the new operator has no idea that a door was unlocked or masked.

5.3.8 Setting APB Auto Load Balancing Option

Pro-Watch offers the option to balance the load of APB (Anti-Passback) card downloads.

Pro-Watch dedicates a number of threads for APB cards download. The card downloads have to be processed in a first-in first-out fashion to avoid cards being processed out of order problem. Thus only one card from one panel can be processed at a time, which means each panel can only be processed by one thread at any given time.

You can select **APB auto load balancing** by selecting its respective check-box in the **Edit Server Options** screen:



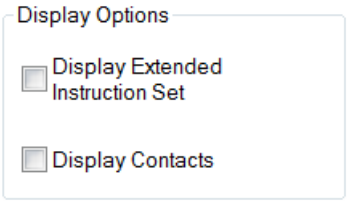
Selecting this option prevents two panels with the most card downloads among all the panels from being processed by the same thread while the rest of the threads process panels with very little or no card download at all.

5.3.9 Assigning Extended Instructions

You can assign an extended instruction set at Site, Channel and Logical device level, as well as to panels of type PW-5000, in addition to the Point level. The extended instructions can be linked to hardware hierarchy (Site, Channel, Panel (only PW-5000 currently)) through an Extended Instruction tab available on the Site, Panel (PW-5000) or Channel. This feature looks similar to adding an extended instruction to a Point.

To display an extended instruction set:

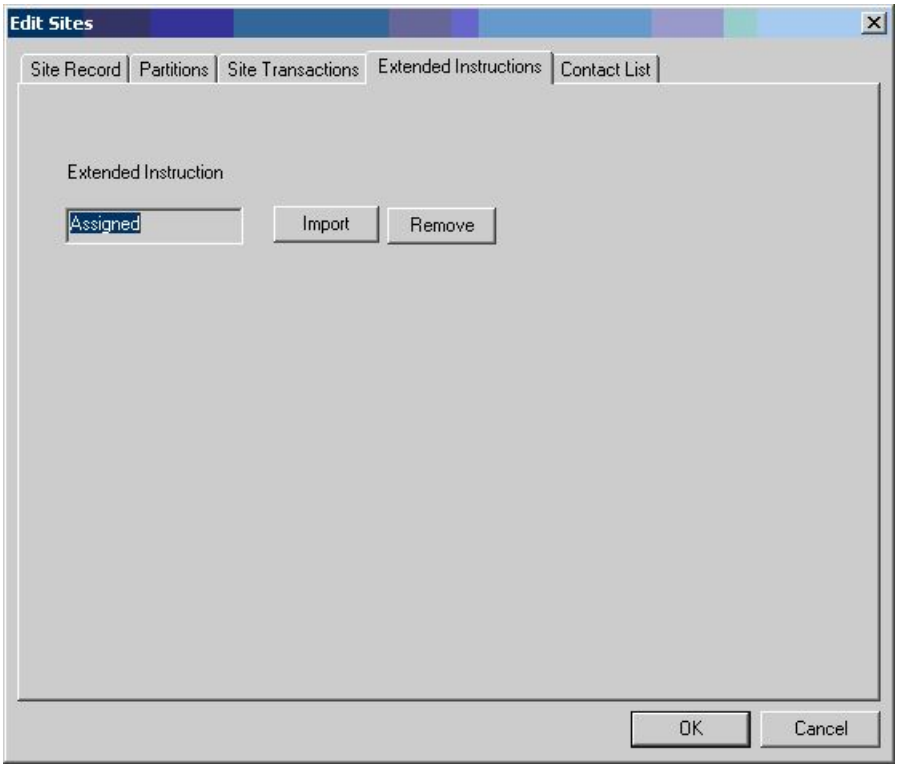
1. On the Pro-Watch menu bar click **File > Server Options** to display the **Edit Server Options** dialog box, **Server Options** tab:



2. Select the **Display Extended Instruction Set** check box and click **OK** to return to the previous display.

To assign extended instructions to a component:

1. Double-click the Hardware Configuration icon in the left navigation pane to display the Hardware Configuration opening screen, showing channels/panels/logical devices that are configured.
2. Click the hardware component for which you want to configure the option of setting extended instructions to display the Edit <Component> dialog box.
3. Click the Extended Instructions tab in the dialog box. This tab appears on this dialog box because you selected the Display Extended Instruction Set on the Edit Server Options screen.

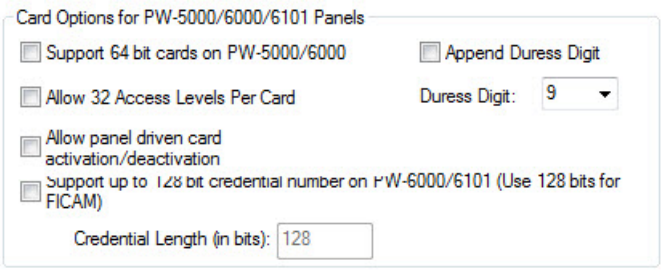


4. Click Import to open a Browse function to help you locate and select the instruction file. The file mus be either an .HTML or an .HTM file with no embedded images.
5. When you have selected the file, click **OK**.

Double-click an event in the Alarm Monitor to bring up a dialog box that displays the extended instruction. You can now look for extended instructions assigned to **Point, Logical Device, Panel (PW-5000 only), Channel and Site** (in the **same order**). The extended instruction assigned to the first hardware in the hierarchy will be displayed.

For more information on extended instructions, see the Information Tab.

5.3.10 Setting Card Options for PW-5000/6000/6101 Panels



1. Select the "**Support 64 bit cards on PW-5000/6000**" check-box to enable 64-bit support.
2. Select the "**Support FICAM compliant 128 bit credential number on PW-6000/6101**" check-box to enable that capability.
3. Select the "**Allow 32 Access Levels per Card**" check-box to enable 32 access levels.

   Caution: Once the "Allow 32 Access Levels Per Card" check-box is selected and the panel is set to 32 clearance codes, the number of clearance codes cannot be switched back to 12 for the panels connected to that server.

   Caution: The use of Mercury intrusion and specification of 32 access levels are mutually exclusive. If the access level count is set to 32, then the Mercury panel can NOT be configured to use Intrusion.

   Caution: In addition, there will also be a significant reduction in the number of cards available per panel.

   Since Mercury data structures are restricted to 32 access levels per card, **if the user wants to have 32 clearance codes per card instead of the default of 12, then they will not be able to use Mercury Intrusion**.

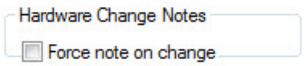
   Similarly, if any Mercury panels are using intrusion, the "Allow 32 Access Levels Per Card" check-box on the Server Options tab that is normally used to select 32 clearance codes will be grayed out and cannot be selected.
4. Select "**Allow panel driven card activation/deactivation**" check-box to activate the card at the panel level, by using the **Issue Date** and **Expire Date** configured at the card's edit screen:



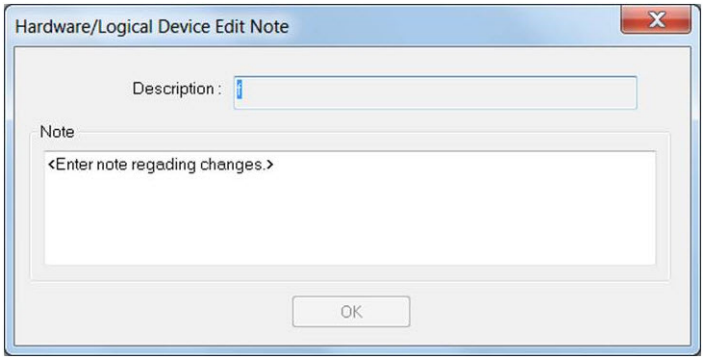
5. For the "**Append Duress Digit**" option see "Duress Signal via "Appended Digit" Option" on page 5-40.
6. Select "**Support up to 128 bit credential number on PW-6000/6101 (Use 128 bits for FICAM)**" check-box to enable that support.

5.3.11 Setting Hardware Change Notes

This check-box enables enforcement of adding hardware notes when a change is made to a channel, panel, logical device, or other hardware.



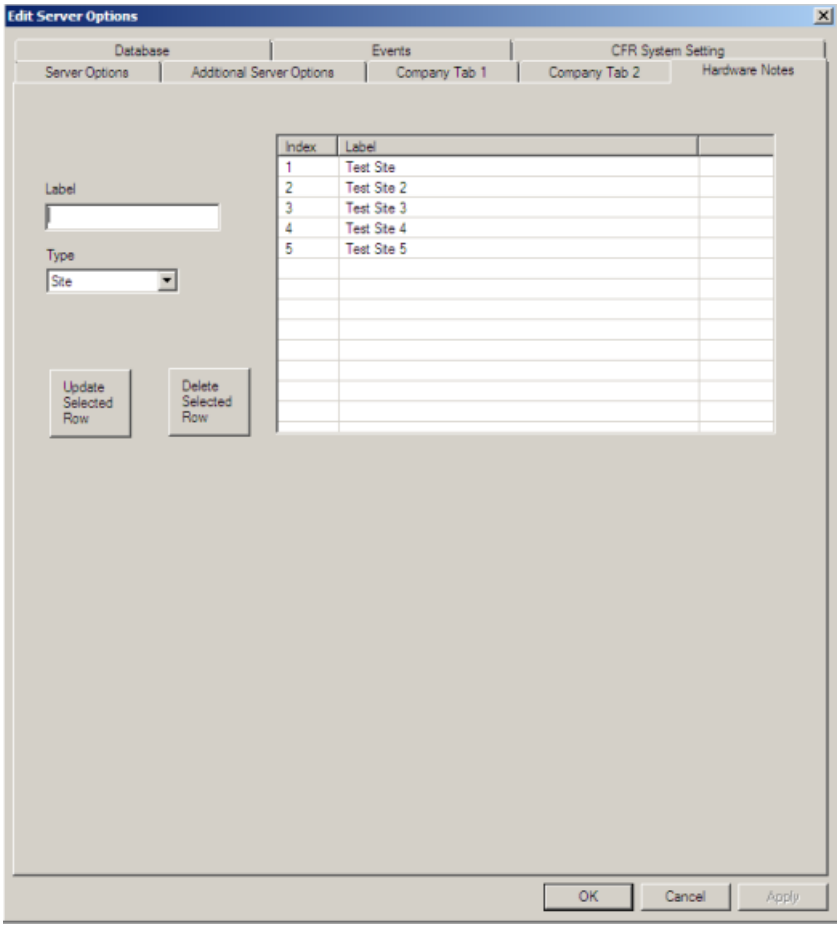
Select "**Force Note on Change**" check-box Ito make changes to any hardware or logical device. That will pop up a window soliciting a note indicating the reason for the change. Here is an example:



Note: When the above screen is displaying, the user has to enter a text into the **Note** field which will enable the **OK** command button. Otherwise the user cannot get out of this screen.

5.3.12 Hardware Notes Tab

In the Hardware Notes tab, you can add up to 5 notes for each hardware type - Site, Channel, Panel and Logical Device.

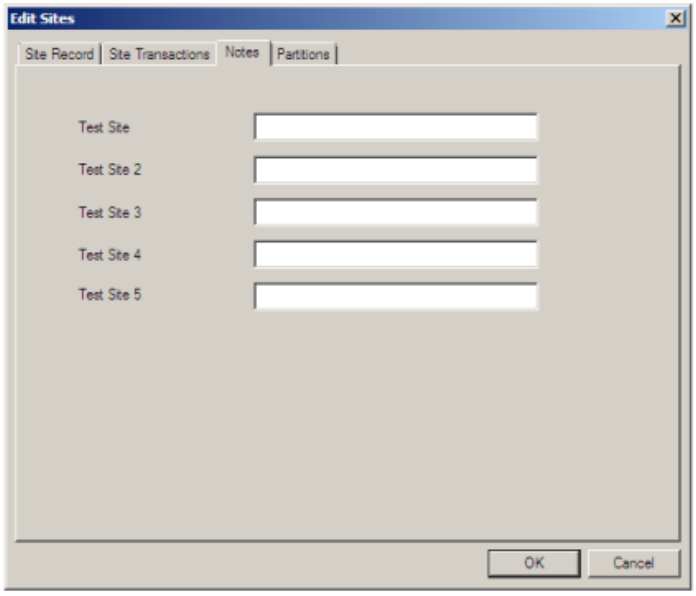


This functionality enables the users to add more data to the hardware tree for whatever they like.

For example, some sites will use the “Alt. Description” field in Logical Devices for something completely different than the “Alternate Location.”

Here are some hypothetical examples for these new text fields:

- “Install Date”
- “Warranty Date”
- “Offline”
- Etc.



Once the notes are created in the Server Options, they will become available in the hardware properties.

5.3.13 Setting Mercury IP Client (Reverse IP)

5.3.13.1 About Mercury IP Client

Mercury IP Client (Reverse IP) is a new feature in Pro-Watch 4.3.5 that allows multiple connections back to the Pro-Watch Application on the same server port number.

Benefits of Mercury IP Client:

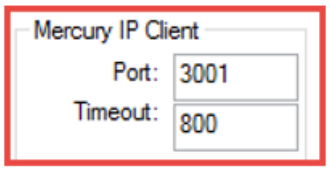
- Enables DHCP setting in the panel and minimizes the maintenance of IP addressing & network changes.
- Helps reduce configuration time via minimum firewall configuration changes.
- Enables the panel to support cloud deployment of Pro-Watch server without need for VPN connection (future option).

5.3.13.2 Mercury IP Client Configuration Steps

1. **Launch Pro-Watch Software Suite**

   a. Click **FILE > SERVER OPTIONS**

      1. The default **Mercury IP Client Port** number and **Timeout** (delay) time are displayed and can be changed if necessary:



The changes take effect the next time the server is started.

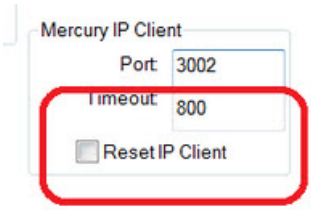
For the **Port** number, either use the default Port value (3001), used by all reverse IP Client controllers, or enter the new port number.

For the **Timeout** value, either use the default Timeout value (800) or enter the new number.

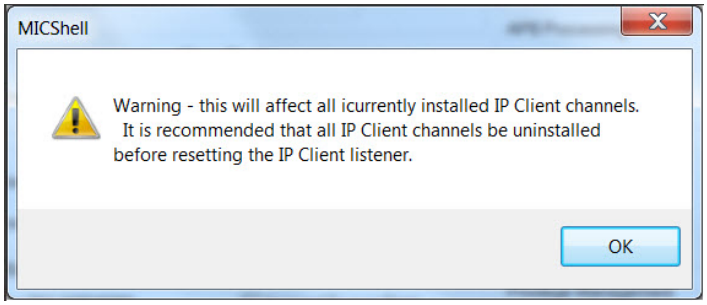
These two **Mercury IP Client** configuration fields enable the Mercury panels to initiate a connection rather than having the Pro-Watch server start the process.

Resetting Mercury IP Client Values

When you change the default values, Pro-Watch displays a new **Reset IP Client** check-box:



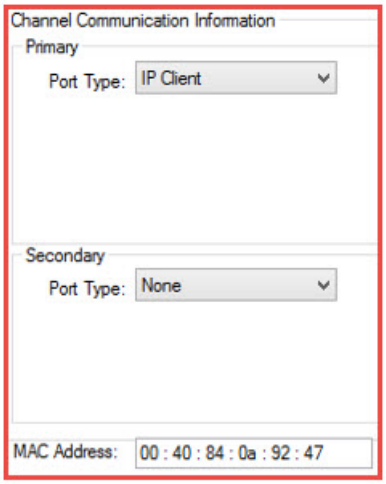
When you select this check-box, you can reset the IP client values without shutting down the server. However, the system first issues a **warning message**:



Click **OK** to reset the Mercury IP Client values.

b. Click **HARDWARE CONFIGURATION**. Edit the **CHANNEL PROPERTIES.**

1. The Communication Parameters tab must define the **Primary Port Type** box to IP CLIENT. Controller **MAC Address** must be specified (as shown below):



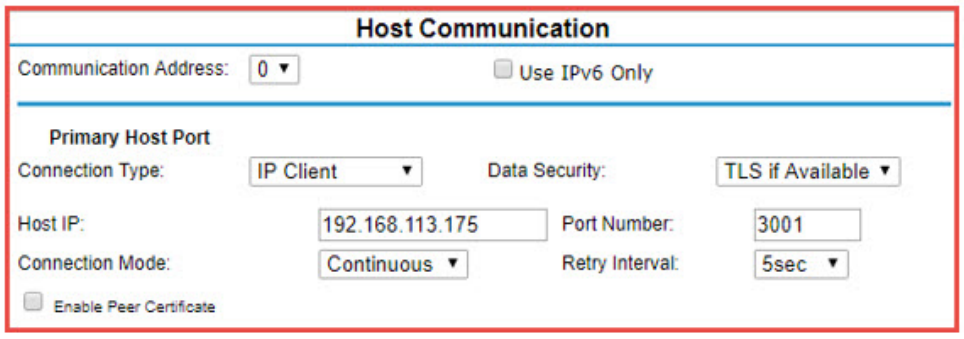
c. Click **HARDWARE CONFIGURATION**. Edit the **PANEL PROPERTIES**.

1. The panel address must be addressed 0 (zero) with no exceptions.

Note: "Panel Move Utility" can be used to reassign panel addresses. Create a backup first!

2. Launch the PW6K1IC Web Page

a. Click the **HOST COMM** tab:



1. Define the following Connection Type parameters (as shown above):

- **Communication Address** - 0 (zero)
- **Connection Type** - "IP Client"
- **Host IP** - Must be the Pro-Watch APP Server IPV4 address

- **Port Number** - Must match the port number defined in Pro-Watch Server Options
- **Data Security** - “TLS if available”
- **Connection Mode** - “Continuous”
- **Retry Interval** - “5 sec”
- Additional Troubleshooting:

a. Option A:

1. Mark channel and panel 'uninstalled'.
2. Restart the Pro-Watch Server service.
3. Mark channel and panel 'installed'.

b. Option B:

1. Upgrade controller firmware.

5.3.14 Setting Privilege Management

Privilege Management enables a Pro-Watch unrestricted user to designate “restricted users.” A restricted user can create other users who can have only the privileges that are less than or equal to those of the restricted user. These privileges include user program access and partitions. If the new user created by the unrestricted user is a member of a class (such as the root class) that would normally afford the user more privileges than the restricted user has, these additional privileges are automatically revoked from the new user. That is, the new user retains only the privileges that the restricted user owns. Note the following rules:

- Should the restricted user try to add, revoke, or delete any of the new user’s privileges that he (the restricted user) does not have himself, an error message will appear.
- A restricted user cannot modify his or her own privileges.
- A restricted user cannot delete himself, nor can he delete an unrestricted user.
- A restricted user cannot edit an unrestricted user’s configuration on the User Information, Program Functions, and Partitions tabs on the Edit User screen.

Before configuring unrestricted and restricted users, be sure that the following conditions are configured properly in Pro-Watch:

- Revoke the privileges to add or edit an existing class from prospective restricted users, since changes to the class will affect the partitions, programs, and functions available to the user.
- Revoke the privileges to add, update, and delete a partition from restricted users.

- Revoke the rights to update “System Options” from prospective restricted users by revoking the Update function for Control Record under Administration program in the Programs tab.

Note that the new privilege scheme does not filter what a user can see.

To implement the Privilege Management feature, you must:

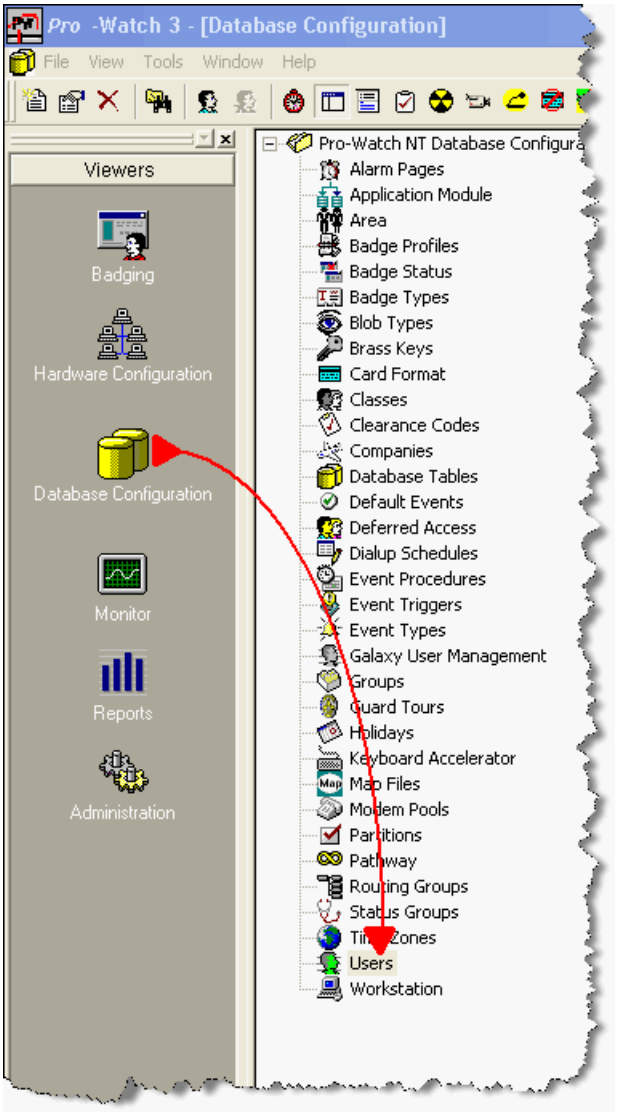
1. Configure an unrestricted user or class of users who will be enabled to configure restricted users. See "Step 1: Configure the Unrestricted User".
2. Turn on the Enhanced Privilege Scheme in **File > Server Options**. See "Step 2: Turning on the Enhanced Privilege Scheme".
3. Set the restricted user’s Restrict User Privilege on the User Information tab at the Edit User screen. See "Step 3: Setting the Restrict User Privilege".

5.3.14.1 Step 1: Configure the Unrestricted User

Follow these steps to configure the unrestricted user, who will be creating restricted users:

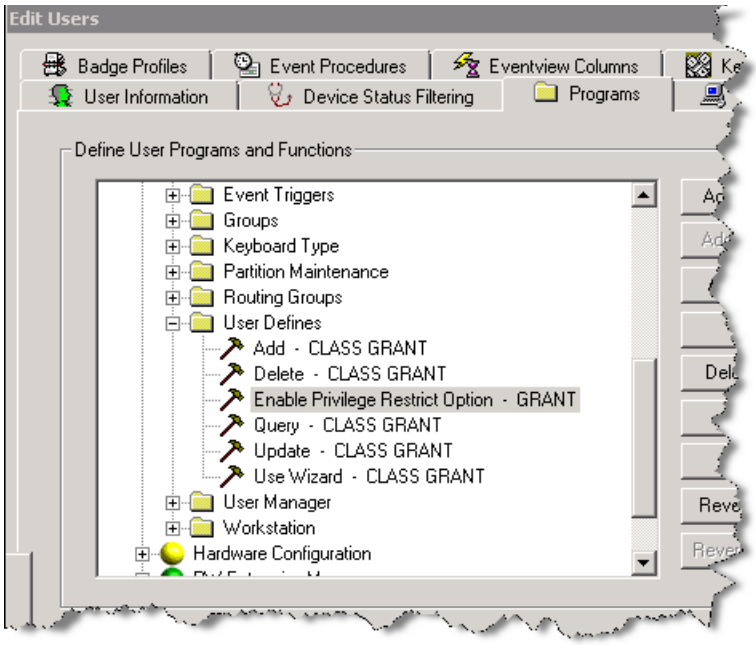
1. Click **Database Configuration** in the left pane of the Pro-Watch main screen, and then click **Users** in the Database Configuration tree:

Note:



You can also configure unrestricted users by class.

2. If the user you want to designate as an unrestricted user appears in the displayed list of users in the right pane of the screen, double-click that user to display the Edit Users screen. If the user does not appear in the list, right click in the right (user list) pane, select **New User** from the pop-up menu, follow the instructions given in "DBC - Users" in Chapter 7 to create the user, and then proceed with the step below.
3. At the Edit Users screen, click the **Programs** tab and double-click **Database Configuration** to display the tree of Database Configuration programs. Then scroll down the tree and double-click the **User Defines** folder to display the following screen:

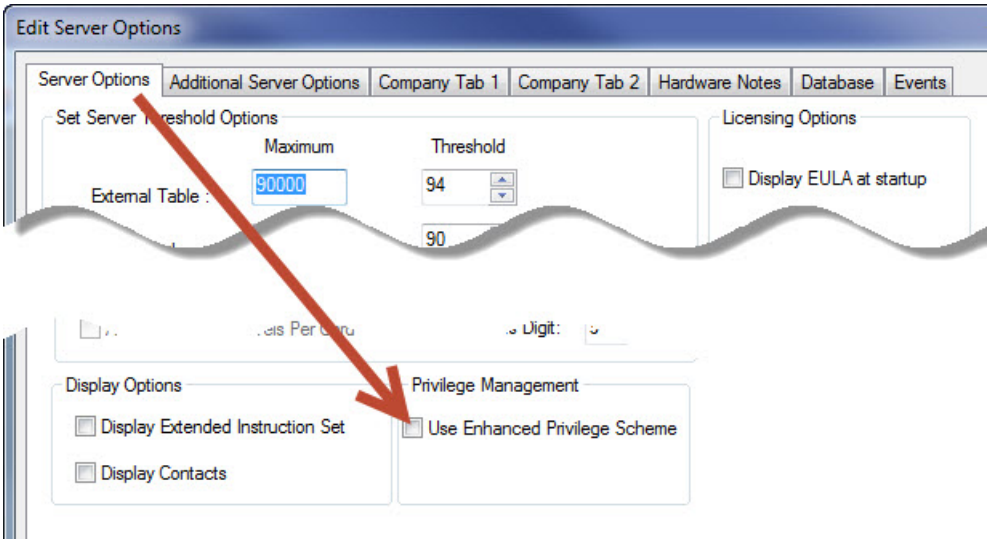


4. Click **Enable Privilege Restrict Option** to highlight the line, and then click the **Grant** button at the right. **Important**: this privilege must be granted only to the unrestricted user(s).
5. Click **OK** at the bottom of the screen. This user is now configured as an unrestricted user.

5.3.14.2 Step 2: Turning on the Enhanced Privilege Scheme

To create a restricted user, you must turn on the Enhanced Privilege scheme before configuring the restricted user. If the scheme is not turned on, the Privilege Management feature is not active and Pro-Watch user permissions operate as before.

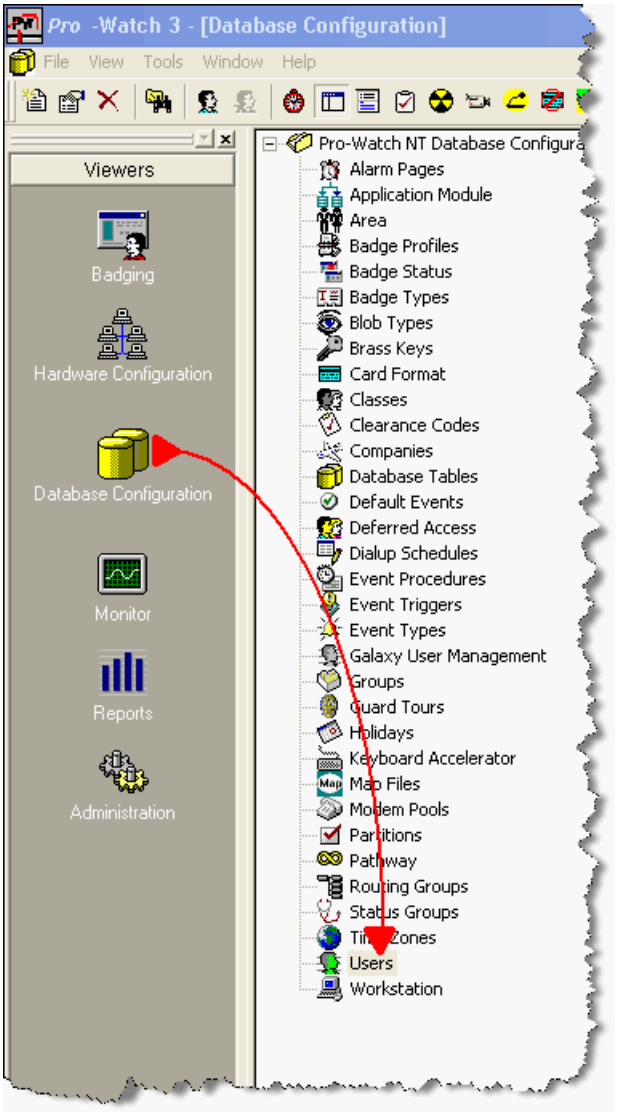
From the Pro-Watch toolbar, select **File > Server Options** to display the Edit Server Options screen, and select the **User Enhanced Privilege Scheme** checkbox, as shown below.



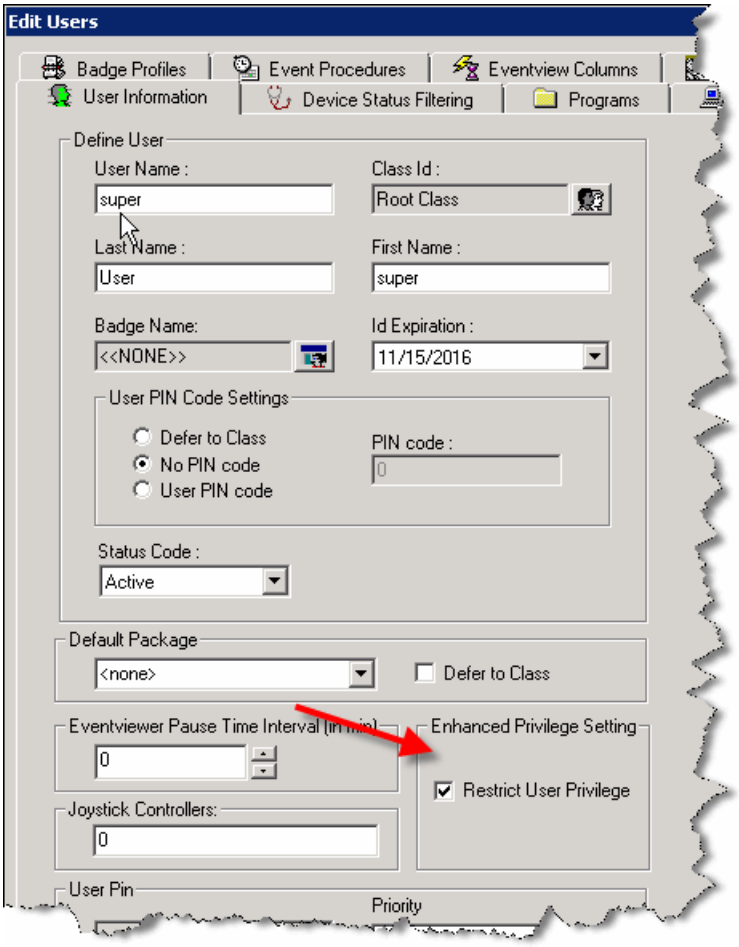
Note: The Privilege Management feature is active only when the Use Enhanced Privilege Scheme server option is selected. If this option is not selected, the feature is not operative.

5.3.14.3 Step 3: Setting the Restrict User Privilege

1. Click **Database Configuration** in the left pane of the Pro-Watch main screen, and then click **Users** in the Database Configuration tree:



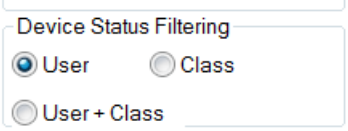
2. If the user you want to designate as a restricted user appears in the displayed list of users in the right pane of the screen, double-click that user to display the Edit Users screen. If the user does not appear in the list, right click in the right (user list) pane, select **New User** from the pop-up menu, follow the instructions given in "DBC - Users" in Chapter 7 to create the user, and then proceed with the step below.
3. At the Edit Users screen, click the **User Information** tab:



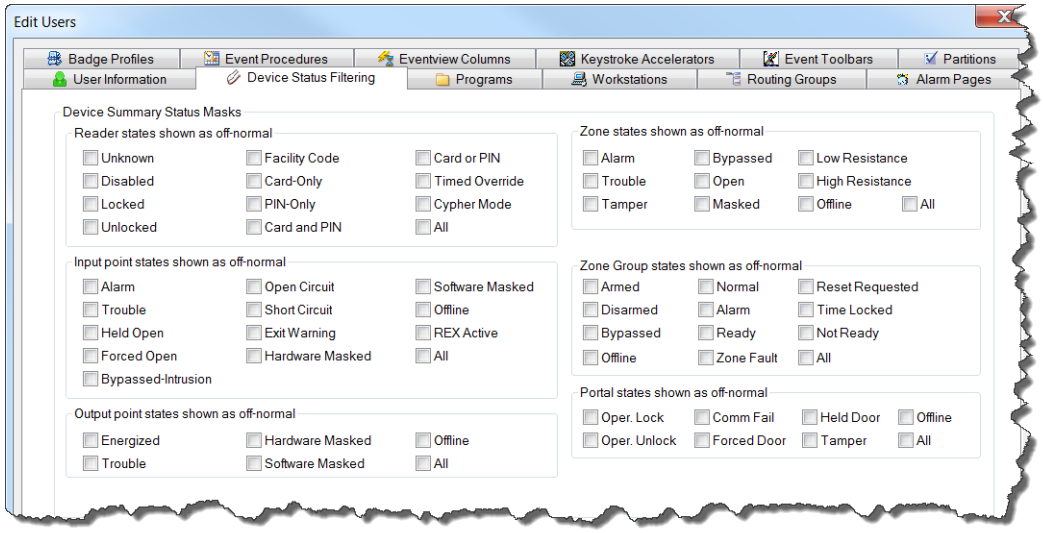
4. At the Edit Users screen, click the **User Information** tab, and select the **Restrict User Privilege** checkbox at the bottom, as shown above.

5.3.15 Setting Device Status Filtering Options

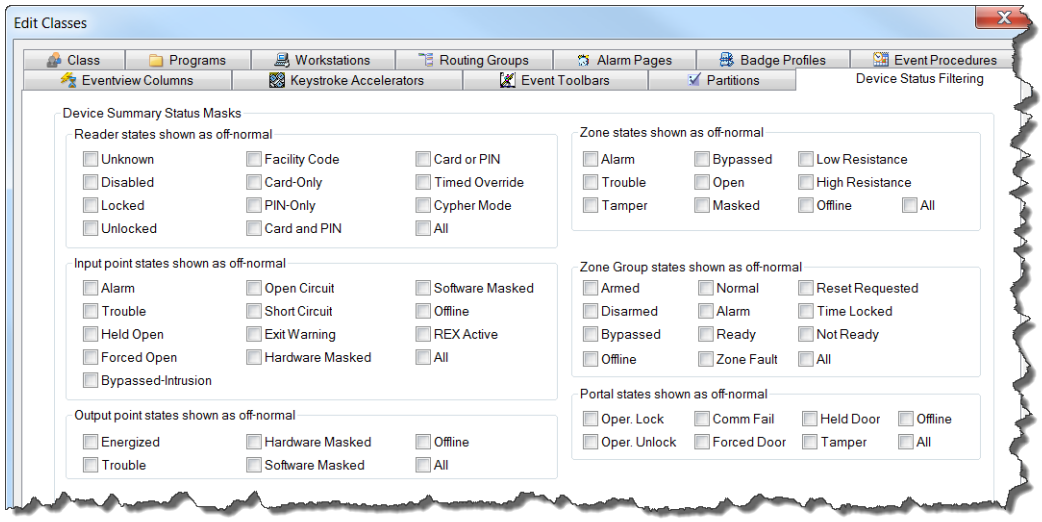
The users can set device filters by user alone, class alone, or both user and class. To do that, select one of the three option buttons available:



1. Selecting the **User** option button will enable only those options selected at the User Device Status Filtering tab:



2. Selecting the **Class** option button will enable only those options selected at the User Device Status Filtering tab:

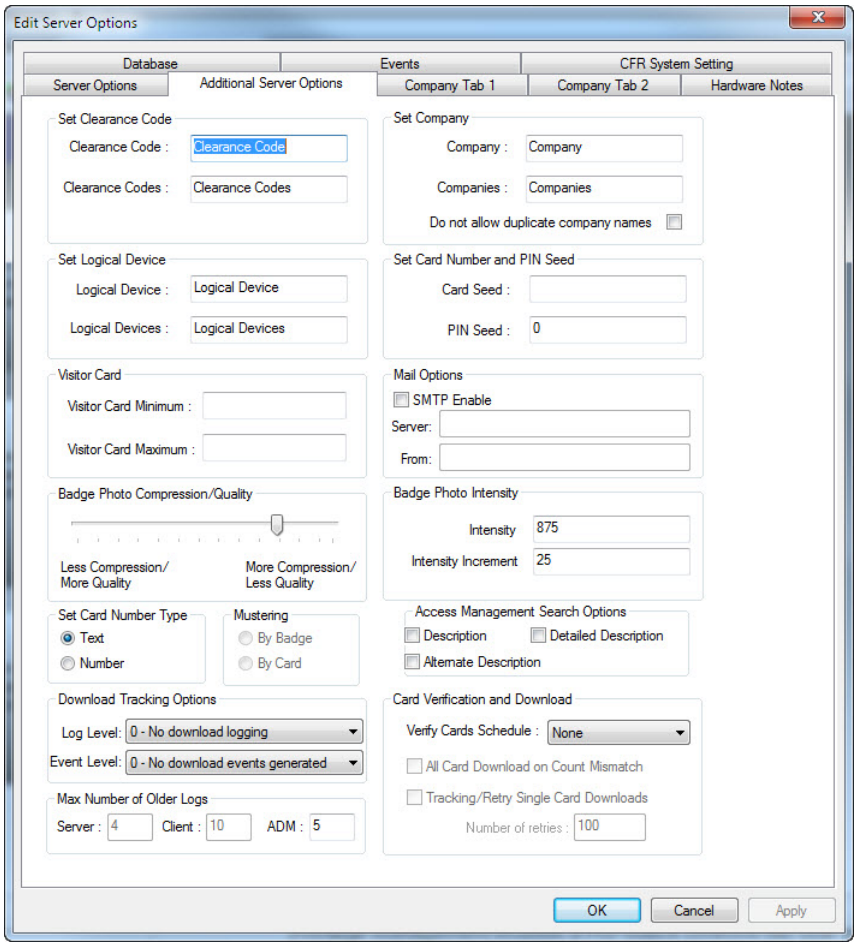


3. Selecting the **User+Class** option button will enable all the options selected at both the User Device Status Filtering tab and the Classes Device Status Filtering tab.

5.3.16 Setting Additional Server Options

5.3.16.1 Clearance Code, Company, and Logical Device Settings

Pro-Watch uses “Clearance Code,” “Company,” and “Logical Device” to name three of its database entities. You can change the names of these entities on the **Additional Server Options** tab of the **Edit Server Options** dialog tab:



To set clearance code, company, and logical device labels:

1. Select **File > Server Options** from the Pro-Watch menu bar to display the **Edit Server Options** dialog box, **Additional Server Options** tab.
2. In the Set Clearance Code section, enter the clearance code(s).

3. In the Set Company section, enter the company name(s).
4. In the Set Logical Device section, enter the name(s) of the logical device(s).

5.3.16.2 Setting the Card and PIN Seed Numbers

The card seed number is the starting number in a Pro-Watch automatic card numbering procedure.

To set the card and PIN seed numbers:

1. Select **File > Server Options** from the Pro-Watch menu bar to display the **Edit Server Options** dialog box, **Additional Server Options** tab.
2. In the **Set Card Number and PIN Seed** group, enter a **Card Seed** number and a **PIN Seed** number. The PIN seed number field length is nine digits. If the PIN seed number is fewer than nine digits, leading zeros fill the field. Enter a starting number here only if you will be assigning card numbers automatically. Note that the **Matrix Remote Control Module (RCM)** uses algorithmic PIN codes. The Matrix PIN codes are code-generated from the card number itself and a PIN seed number.
3. Click **OK**.

5.3.16.3 Setting Mail Options

SMTP Enable Checkbox

Pro-Watch supports e-mail in both MS SQL 32-bit and 64-bit operation.

In 32-bit operation, Pro-Watch supports two email protocols—SMTP and MAPI. If you select the SMTP Enable checkbox, the SMTP database mail protocol is used. Note, however, that before Pro-Watch can e-mail successfully via SMTP, you must configure SMTP e-mail in the MS SQL Management Studio application. To do this in MS SQL Management Studio, select **Management > Database Mail** to start the Database Mail Configuration Wizard. Refer to the MS SQL documentation for further instructions on configuring SMTP e-mail.

In 32-bit operation, if you leave the SMTP checkbox unselected, Pro-Watch will use the MAPI protocol by default. However, for Pro-Watch to successfully use the MAPI protocol, you must first configure MS Outlook Client; that is, you must install Outlook with a valid e-mail account.

In 64-bit operation, Pro-Watch supports only the SMTP protocol. Pro-Watch does not support MAPI when it is installed with 64-bit MS SQL. If Pro-Watch is installed with 64-bit MS SQL, you can either select the SMTP Enable checkbox or leave it unselected. Either way, Pro-Watch will attempt to use the SMTP protocol. For this to succeed, however, you must

configure SMTP e-mail in the MS SQL Management Studio application, as described above for 32-bit operation.

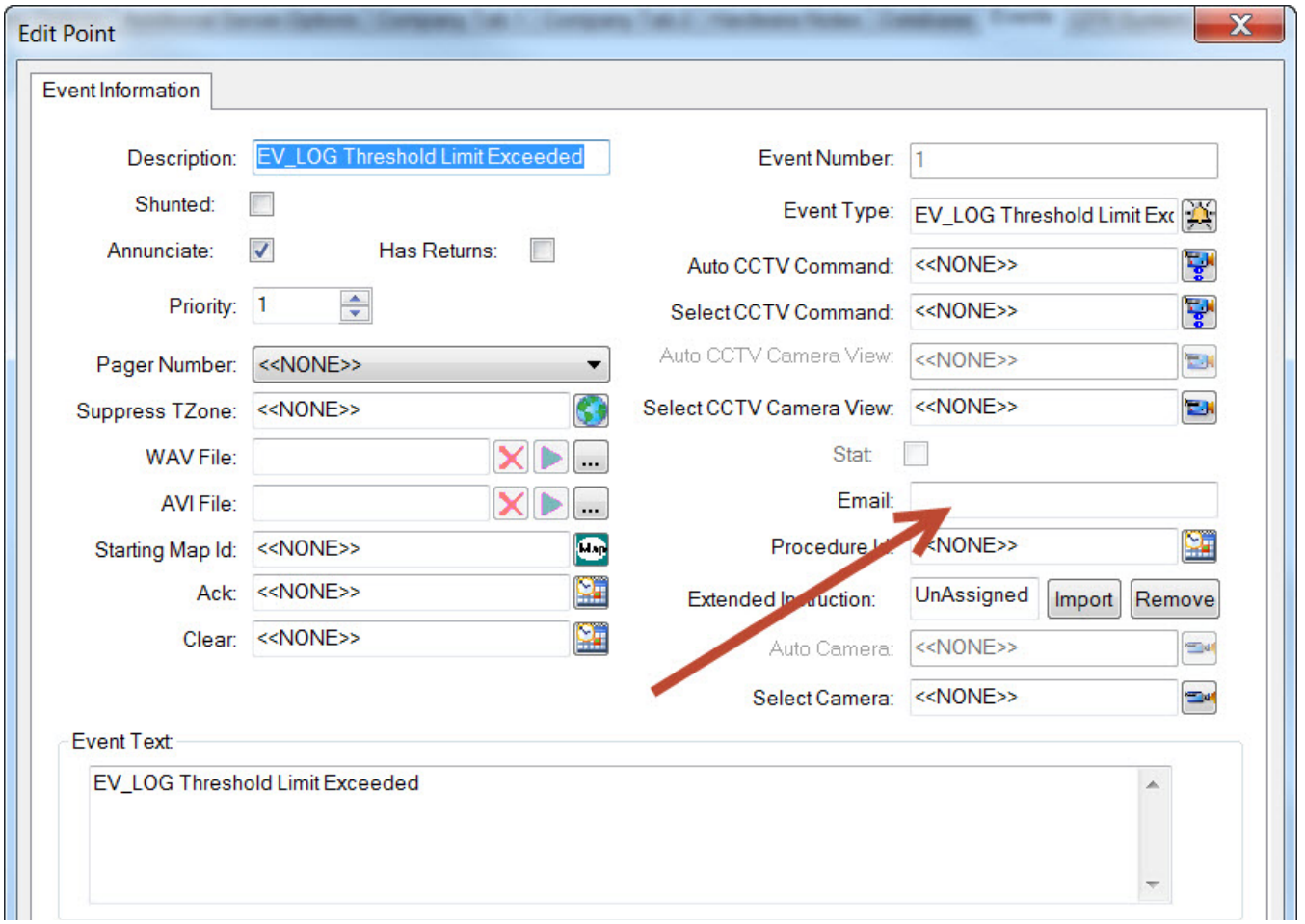
Server

Enter the name of the mail server Pro-Watch is using.

From

Enter a valid e-mail account that will indicate the source of the email.

Note: In addition to completing these fields in the Mail Options box on the Additional Server Options tab, you will also need to specify the e-mail address of the recipient of specific events. This is accomplished in the event's Edit Point dialog box in Hardware Configuration (see "HW Config - Edit Point" in Chapter 25 for details).



5.3.16.4 Setting Badge Photo Compression and Intensity

You can set badge photo compression and intensity levels at the bottom of the Additional Server Options tab.

To set badge photo compression/quality and intensity parameters:

1. Select **File > Server Options** from the Pro-Watch menu bar to display the **Edit Server Options** dialog box, **Additional Server Options** tab.
2. In the Badge Photo Compression/Quality section, move the slider to the level that you want.
3. In the Badge Photo Intensity section, click the buttons for Intensity and Intensity Increment and enter the settings for these parameters.
4. Click **OK**.

5.3.16.5 Setting Mustering by Badge or Card

When mustering is set, Pro-Watch tracks who is in or out of a particular Area.

If you select **Additional Server Options > Mustering > By Badge**, the mustering screen displays the badgeholder in the last area he entered. When mustering by Badge and a user has more than one card, the user can enter and exit using different cards.

If you select **Additional Server Options > Mustering > By Card**, he mustering screen displays the cardholder in the last area he entered. The user must enter and exit with the same card.

In both cases, when the user exits, his name is removed from the area.

5.3.16.6 Setting Download Tracking

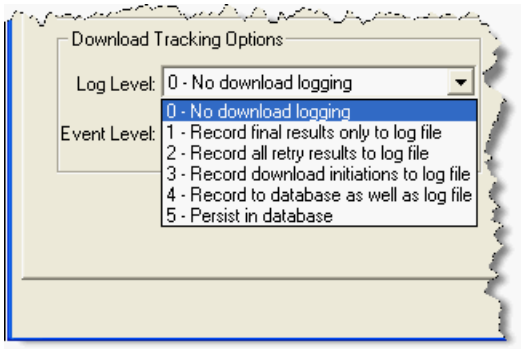
Pro-Watch enables you to track the download of any card initiated from a client or server. Using this log, you can determine the download's success or failure. Database entries are created for all relevant CARD_DN and HI_-QUEUE single card downloads for PW-5000 and PW-6000 panels. After the HI_QUEUE record is processed by the server, all subsequent information about the downloads is maintained in server memory and updated in the database. Note that only card downloads, not system downloads, are logged.

All information about a download from a particular card to a particular panel is logged in a new table named DOWNLOAD_TRACKING. The log entries are created by database triggers during the INSERT of records to the CARD_DN and HI_QUEUE tables. These insertions are executed only by single-card download commands.

Setting the Card Download Options

From the Pro-Watch toolbar, select **File > Server Options > Additional Server Options > Download Tracking Options**. The Download Tracking Options box provides two card download settings:

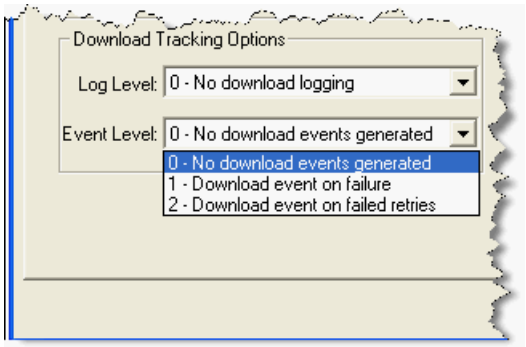
- Log Level



  Five levels enable you to determine how much logging is done—the higher the level, the more logging (also, the more resource overhead):

  - **Level 0**—No logging.
  - **Level 1**—Logs to the server's log file only the success or failure for any given download.
  - **Level 2**—Includes Level 1 logging and also logs (to the server's log file) the result of all retries.
  - **Level 3**—Includes Level 2 logging, and also logs (to the server and client log files) the initiation of downloads from the client and server.
  - **Level 4**—Includes Level 3 logging, and also logs Level 3 logging to the database.
  - **Level 5**—Includes Level 4 logging, and also makes the log information persistent in the database across the server sessions when the server is shut down and restarted. The log entries in the database table remain in that table until the download is complete, unless the entries are manually removed.

- Event Level



Three levels control the events (if any) that are generated and displayed in the the Pro-Watch Event Monitor as a result of card downloads—the higher the level, the more events that can be generated (also, the more resource overhead):

- **Level 0**—No events generated.
- **Level 1**—Generates events on failed downloads after all retries have been attempted.
- **Level 2**—Generates events for failures on all retry attempts.

Note: The Log Level and Event Level control fields are mutually independent. Logging can occur with or without event generation, and event generation can occur with or without logging.

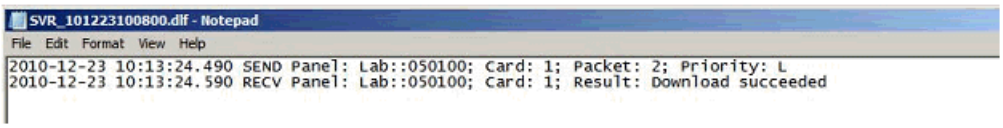
Reading the DOWNLOAD_TRACKING Table

You can find the DOWNLOAD_TRACKING table in the ProWatch\Logs directory. Note that at midnight each night, Pro-Watch closes and renames the previous day's log file and creates a new log file. In order to conserve disk space, only the current and last four log files are kept in the Pro-Watch\Logs directory. To keep log files before they are removed from Pro-Watch\Logs directory, save them to another directory.

The following DOWNLOAD_TRACKING log samples show the results of the various Pro-Watch download logging settings:

Example: Record Final/Retry Results to Log File (Download Log Level 1 or 2)

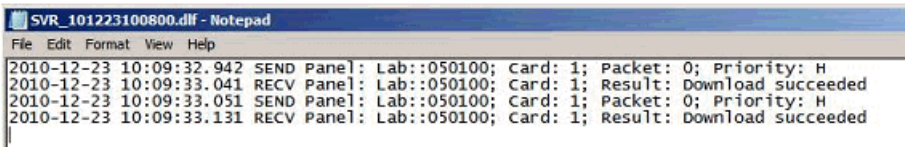
Columns include the date, time, transaction type (SEND/RECV), site and panel, card number, packet number, and priority.



Note that the panel sends a message to Pro-Watch indicating that the card download was successful; "L" signifies low priority, and "H" signifies high priority.

Example: Record Final/Retry Results to Log File (Download Log Level 1 or 2)

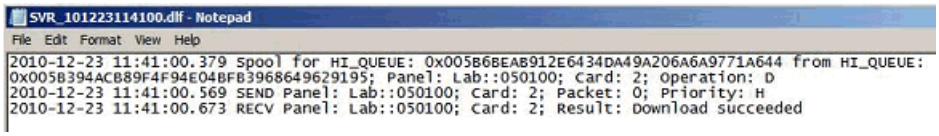
Shows the log file for a single- card download.



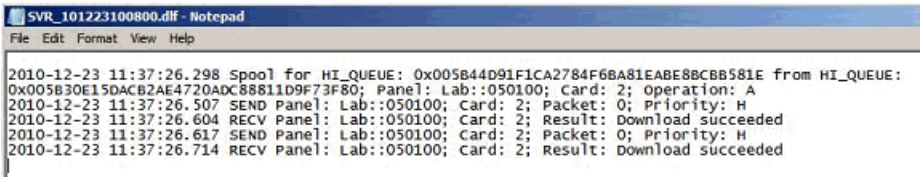
Note that there will be two entries for a single-card download.

Example: Record Download Initiations to Log File (Download Log Level 3)

The extra header includes the Pro-Watch spool file ID, the HI_QUEUE ID, and the operation that is executed.

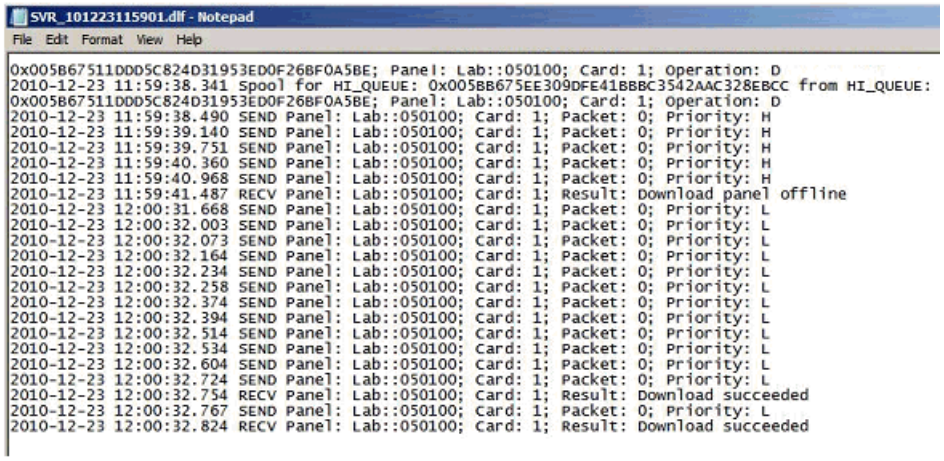


Example: Record Single-Card Download (Download Log Level 3):



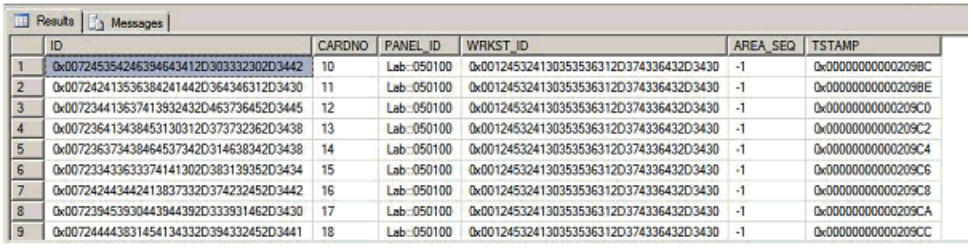
Example: Record Download to an Off-line Panel

The log shows a status message saying “Download panel offline” to indicate that Pro-Watch is unable to communicate with the download panel. After the panel is back on-line, Pro-Watch resumes the download until it receives a “Download succeeded” status from the panel.



Example: Reading the CARD_DN Table

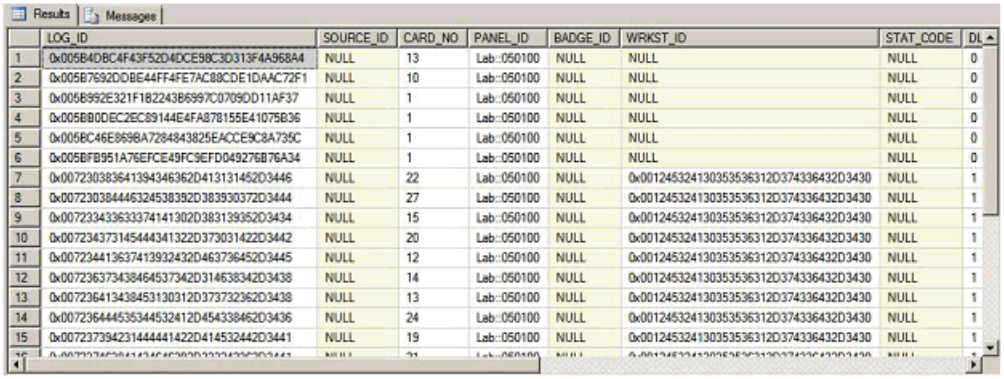
The following CARD_DN table sample shows the queue when a card download is initiated. Entries in this table are deleted after the download is confirmed successful.


Results | Messages

	ID	CARDNO	PANEL_ID	WRKST_ID	AREA_SEQ	TSTAMP
1	0x007245354246394643412D303332302D3442	10	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209BC
2	0x007242413536384241442D364346312D3430	11	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209BE
3	0x007234413637413932432D463736452D3445	12	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209C0
4	0x007236413438453130312D373732362D3438	13	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209C2
5	0x007236373438464537342D314638342D3438	14	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209C4
6	0x007233433633374141302D383139352D3434	15	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209C6
7	0x007242443442413837332D374232452D3442	16	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209C8
8	0x007239453930443944392D333931462D3430	17	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209CA
9	0x007244443831454134332D394332452D3441	18	Lab::050100	0x0012453241303535363 12D374336432D3430	-1	0x00000000000209CC

Example: Reading the DL_TRACKING Table

The following DL_TRACKING table sample stores card download information when Download Log Level is 4 or 5. Tracking information is included in the .dlf log files as well as in the database.



Results | Messages

	LOG_ID	SOURCE_ID	CARD_NO	PANEL_ID	BADGE_ID	WRKST_ID	STAT_CODE	DL
1	0x005B4DBC4F43F52D4DCE98C3D313F4A968A4	NULL	13	Lab::050100	NULL	NULL	NULL	0
2	0x005B7692DDBE44FF4FE7AC88CDE1DAAC72F1	NULL	10	Lab::050100	NULL	NULL	NULL	0
3	0x005B992E321F1B2243B6997C0709DD11AF37	NULL	1	Lab::050100	NULL	NULL	NULL	0
4	0x005BB0DEC2EC89144E4FA878155E41075B36	NULL	1	Lab::050100	NULL	NULL	NULL	0
5	0x005BC46E8698A7284843825EACCE9C8A735C	NULL	1	Lab::050100	NULL	NULL	NULL	0
6	0x005BFB951A76EFCE49FC9EFD049276B76A34	NULL	1	Lab::050100	NULL	NULL	NULL	0
7	0x00723038364139434636 2D4131314 52D3446	NULL	22	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
8	0x00723038444632453839 2D383930372D3444	NULL	27	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
9	0x00723343363337414130 2D383139352D3434	NULL	15	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
10	0x00723437314544434132 2D37303142 2D3442	NULL	20	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
11	0x00723441363741393243 2D463736452D3445	NULL	12	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
12	0x00723637343846453734 2D314638342D3438	NULL	14	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
13	0x00723641343845313031 2D373732362D3438	NULL	13	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
14	0x00723644453534453241 2D4543384 62D3436	NULL	24	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1
15	0x00723739423144444142 2D414532442D3441	NULL	19	Lab::050100	NULL	0x00124532413035353631 2D374336432D3430	NULL	1

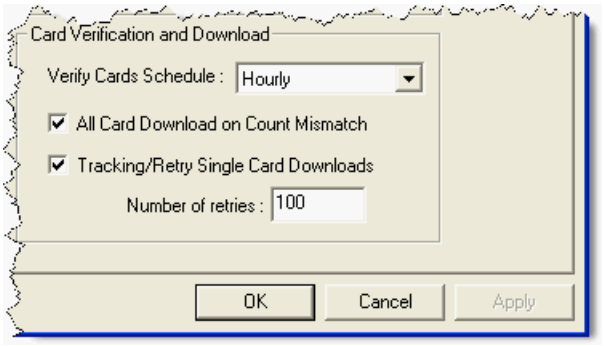
5.3.16.7 Setting Card Verification and Download

In the Card Verification and Download box you can perform the following download verifications:

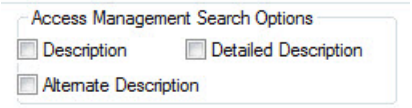
- **All Card Download on Count Mismatch**—Verifies that the panel and the database have the same number of cards. If the panel and database do not have matching numbers of cards, this setting also causes the system to download all of the cards in the current database to the panel.
- **Tracking/Retry Single Card Downloads**—Verifies that all cards were successfully downloaded. If a download fails, the system will retry the download. The number you enter in the Number of Retries box is the number of times the system will attempt a retry.

First, activate the two checkboxes by setting the verification schedule in the Verify Cards Schedule dropdown box. If you select **Hourly**, the verification operations are performed each hour; if you select **Daily**, the operations are performed each day.

Next, select either or both of the download verifications you need performed, and click **OK**.



5.3.16.8 Setting Access Management Search Options

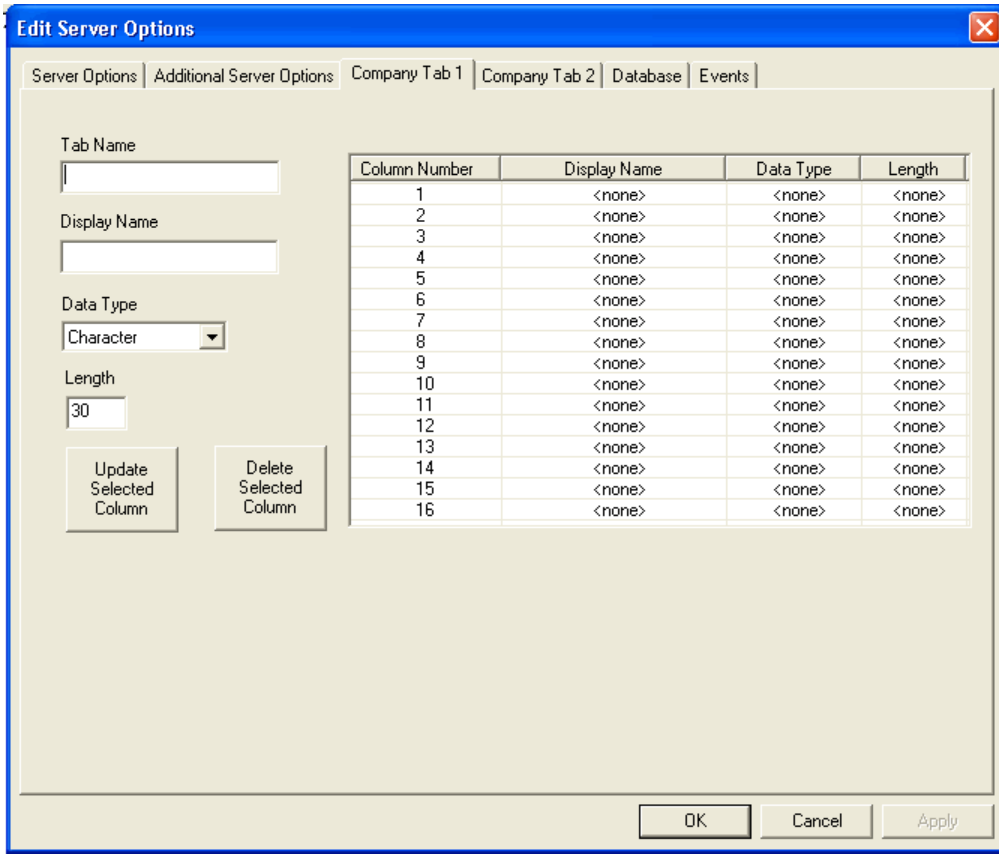


1. Select the **Description** check-box to allow searching for a clearance code by description in the access management portal.
2. Select the **Detailed Description** check-box to allow searching for a clearance code by detailed description in the access management portal.
3. Select the **Alternate Description** check-box to allow searching for a clearance code by alternate description in the access management portal.

NOTE: As soon as a user selects two of these check-boxes, the third is grayed out, so that all three can never be selected at the same time.

5.3.17 Setting Company Tabs

You can customize the Add/Edit Companies dialog box that displays in the Database Configuration utility (see "DBC - Companies" in Chapter 38) by adding up to two tabs.



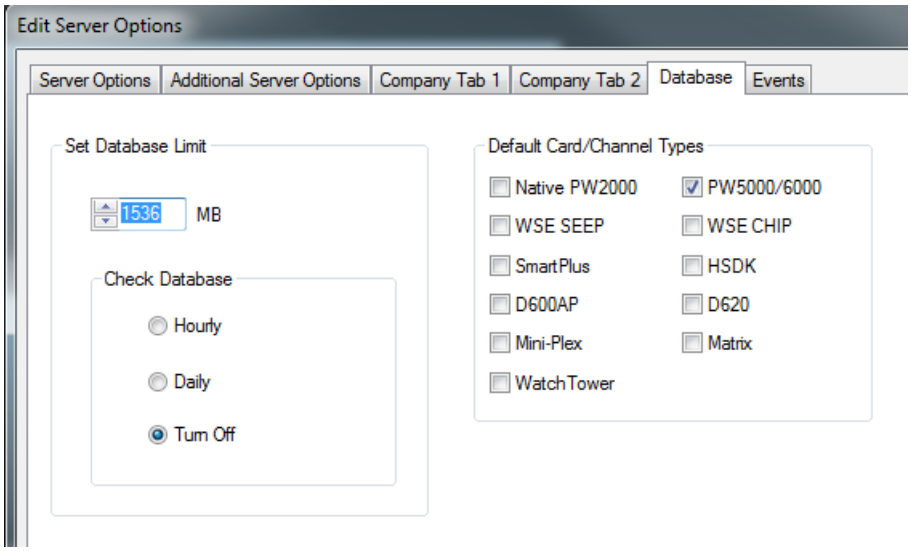
To customize the Companies dialog box:

1. Click the **Company Tab 1** or **Company Tab 2** tab.
2. Select a column number in the Column Number column.
3. In the Tab Name field, enter a tab name.
4. In the Display Name field, enter the name of the column, or field, that will appear on the new tab.
5. In the Data Type field, select either Character, Date, or Numeric.
6. If you selected Character in step 5, enter a field length in the Length box.
7. Click **Update Selected Item** to create the new tab.

8. Click **OK**.

5.3.18 Setting Database Limits

At the server level, you can specify the size of the database and the frequency it should be checked. A message is generated if the limit is exceeded.



To specify a database size:

1. Select **File > Server Options** from the Pro-Watch menu bar to display the **Edit Server Options** dialog box, **Database** tab.
2. In the Set Database Limit section, enter the estimated size.
3. In the Check Database section, click **Hourly**, **Daily**, or **Turn Off.**
4. Click **OK**.

To specify card/channel type:

Select one or more of the option buttons available.

Note: This selection will determine the number of digits you can select for a card number. See Section *G.3.1.4, Optional Information Tab* in Appendix G, "Badging".

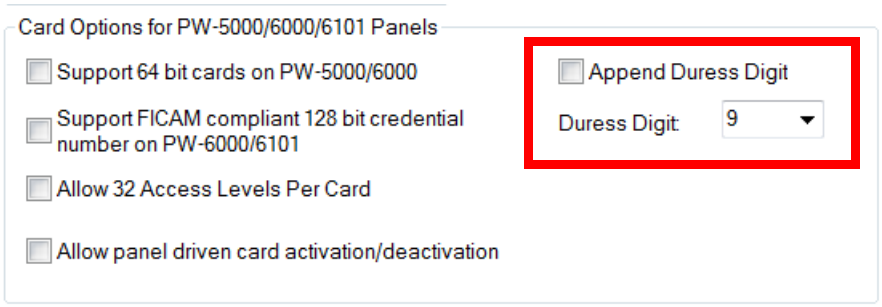
5.4 Duress Signal via "Appended Digit" Option

"Appended Duress Digit" is a Pro-Watch security feature configured as a server option for PW-6000/6101 panels. This feature works in "Card and PIN", "Card or PIN" or "PIN Only" modes. PIN is an acronym that stands for "Personal Identification Number."

This features makes it possible for users to send a duress message from a reader to the Pro-Watch operator by entering the duress digit right after they enter their unique PIN number.

This feature, once enabled at the server level, becomes operational for all PW6K series panels on the site. The user cannot select only a subset of the installed panels for this feature.

1. Click and display the Edit Server Options screen. The "Appended Duress Digit" is configured at the "Card Options for PW-5000/6000/6101 Panels" group of controls on this dialog box screen.
2. Select the "**Append Duress Digit**" **check-box** to enable this feature.

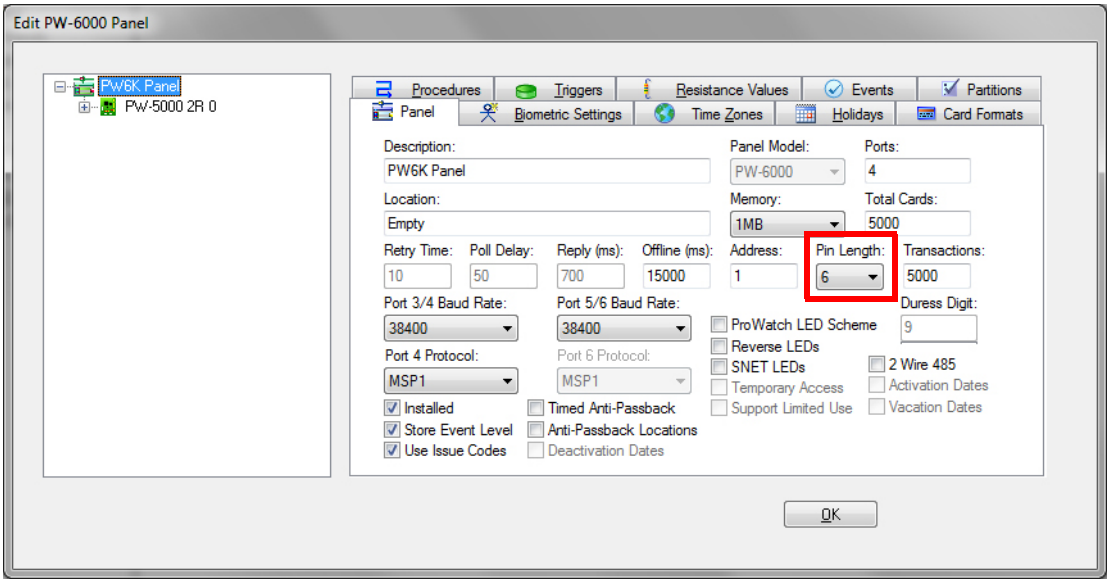


3. Select any Duress Digit you like by using the combo box displayed. The default Duress Digit is set to 9 (nine).
4. Click OK to save.
5. Restart the Pro-Watch server to enable the feature.

Once configured, Pro-Watch will expect the users to enter that additional duress digit after entering the PIN number at a logical device when the users want to send a duress message to the operator.

5.4.1 Setting the PIN Length

Setting the PIN length at the Edit [YOUR PANEL'S NAME] Panel screen is important to use this feature properly.



You must set the PIN length for the panel by selecting a number from the PIN Length combo box at the Panel tab of your panel's properties editing screen (Edit [YOUR PANEL'S NAME] Panel screen).

This number should equal to the PIN number length set at the card configuration screen, plus one (1). For example, if your cards are configured to have a PIN number 3 digits in length, then your panel PIN number length should be 4 (3 + 1) to accommodate the last "appended duress digit."

Pro-Watch decides whether the PIN and the duress digit you enter at the reader is a valid one by referring to this PIN length information.

Once the appended duress digit feature is enabled at the Edit Server Options screen, the system expects the last digit of an N-digit PIN to be either the duress digit or the place-holder termination character "#" (hash tag).

For example, let's consider the following hypothetical case in which the user has the unique PIN number "1234".

Let's say that in the Edit Server Options screen we have:

1. Selected the "Append Duress Digit" check-box, and
2. Selected "9" as our Duress Digit and restarted the Pro-Watch.

Then, in the Edit [YOUR PANEL'S NAME] Panel screen, let's say that we have:

3. Selected "5" as our PIN Length. The Duress Digit field should display "9" since that's the selection we've made in Step 2.

Here are some possible outcomes:

Table 5-1 Possible Duress Outcomes with 5-digit PIN and "9" for Duress Digit

If we enter...	The result will be...
12349	Pro-Watch will allow us to pass AND send a duress signal to the operator.
12348	Pro-Watch will NOT allow us to pass and will NOT send a duress signal to the operator since we have used the wrong duress digit.
1234#	Pro-Watch will allow us to pass BUT will NOT send a duress signal to the operator.
1239	Pro-Watch will NOT allow us to pass AND will NOT send a duress signal to the operator. We have used the wrong PIN.
123#	Pro-Watch will NOT allow us to pass AND will NOT send a duress signal to the operator. We have used the wrong PIN.
12349jk!8	Pro-Watch will allow us to pass AND send a duress signal to the operator. Digits after the 5th digit will be ignored.
1234#jk!8	Pro-Watch will allow us to pass BUT will NOT send a duress signal to the operator. Digits after the 5th digit will be ignored.

5.4.2 Appended Duress Digit Q & A

Q: "How can I visually check whether the duress digit is operational?"

A: Display the "Edit Properties" screen for your panel. Select the Panel tab. The Duress Digit field will display the duress digit selected and saved in the server options screen. If the duress digit is not activated, the Duress Digit field will be blank.

Q: "What if I'd like to change the duress digit later on, some time in the future?"

A: Once set as a server option, changing the duress digit requires calling Honeywell's technical service. Therefore, the users must be careful in selecting their duress digits.

Q: "What if the card reader is not equipped with a PIN entry keyboard?"

A: Then this feature cannot be used. The extra duress digit requires a PIN reader.

Q: "What if I just want to use my PIN number without sending a duress signal to the operator?"

A: Enter the default value of hash-tag (#) after your PIN number. For example, if your PIN number is "1234" (without the quotation marks) but if you do not want to send a duress signal, then you enter "1234#" and you'll be able to pass through that reader without generating a duress signal.

Q: "How does the system know it's me who is sending the duress signal?"

A: Pro-Watch 4.1 makes sure all users do have unique PIN numbers. Thus, only you can send the PIN+Duress-Digit signal that's generated by using the duress digit.

Q: "What if the system expects me to type in an N-digit number (PIN+Duress-Number) but I type in a number N-1 digits in length, a number that does not include the last duress digit?"

A: Pro-Watch will not recognize the PIN number. It will not allow you to pass. But it will not generate a duress signal either.

Q: "What if the system expects me to type in an N-digit number (PIN+Duress-Number) but I type in a number N+m digits in length, a number that does include the duress digit but also additional digits after that? For example, what happens if the system is expecting the correct 5-digit number "77659" but I type in "77569m7@!"? "

A: Pro-Watch will recognize the PIN number. It will allow you to pass since the number includes a duress digit. And it will generate a duress signal if the duress digit is the correct number. If the duress digit is a hash tag (#), it will not generate a duress signal. It will discard all the extra digits.

Q: "Can you tell me one good practice that I should follow in using this feature?"

A: Always make sure your users have fixed-length PIN numbers. Avoid variable-length PINs.

5.4.3 Test Your Knowledge

(Correct answers are at the end of this chapter.)

1. At which Pro-Watch screen do you select the "appended duress digit" option? At the ...

   a. Edit Card Properties screen

   b. Edit Panel Properties screen

   c. Edit Server Options screen

2. The panel-level PIN length should be equal to:

   a. Card number minus 1

   b. Card PIN length plus 1

   c. Card PIN length minus 1

3. What is the place-holder termination character that we use to end a PIN number with?

   a. 9

   b. *

   c. #

4. It is easy to change the Duress Digit after it's set and saved. You can do it yourself without calling Honeywell's technical service.

   a. True

   b. False

5. You can use the "appended duress digit" feature even if the reader is not equipped with a PIN entry keyboard.

   a. True

   b. False

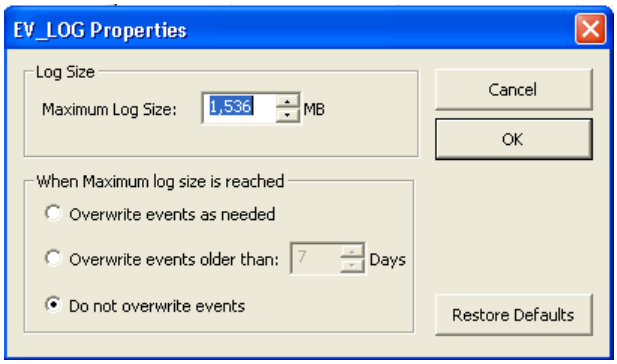
5.4.4 Answers to “Test Your Knowledge” Quiz

Answers to quiz Test Your Knowledge, page 43:

1. C
2. B
3. C
4. False
5. False

5.5 Setting the Log Size

Pro-Watch enables you to specify log size and the time period after which records are purged. If the time parameter is specified, the oldest 5% of records are purged. If neither is specified, nothing is purged:



To specify a log size:

1. In the left pane, select **Administration**.
2. In the tree structure, select **Event Manager**. A list of available logs appears.
3. Right-click the appropriate log and select **Properties**. The above screen appears.
4. In the Log Size section, either enter or use the arrows to select the appropriate log size.
5. In the When Maximum log size is reached section, click the appropriate overwrite button.
6. Click **OK**.

5.6 Pro-Watch Topologies

A Pro-Watch access management control system consists of at least one Pro-Watch server, Pro-Watch clients, many devices, and a database that collects and supplies information that all of the components share. You can implement the system with either of two topologies:

- The remote server topology allows you to configure hardware to poll locally, either by local area network (LAN) or by hardwired channels. Typically, hardware is connected via a wide-area-network (WAN). Configuring hardware to poll locally over a LAN or hardwired channels allows the polling traffic to be isolated from the WAN. This reduces the amount of bandwidth consumed on the WAN. Events, downloads, and status messages are sent between the “Remote” server and either the standard server or the “Primary” server.
- The Pro-Watch Enterprise server topology consists of multiple regional Pro-Watch installations and a central Enterprise server used as a data repository and central hub. This distributed system uses merge and transactional replication to coordinate badging and event transactions across the distributed system. See the *Pro-Watch Enterprise Configuration Guide* (800-00766, Revision A) for a full description and configuration instructions.

5.7 Pro-Watch Remote Server Topology

Pro-Watch Remote Server allows you to configure hardware to poll locally, either by local-area-network (LAN) or by hardwired channels. Typically, hardware is connected via a wide-area-network (WAN). Configuring hardware to poll locally over a LAN or hardwired channels allows the polling traffic to be isolated from the WAN. This reduces the amount of bandwidth consumed on the WAN. Events, downloads, and status messages are sent between the "Remote" server and either the standard server or the "Primary" server.

Consider these remote server characteristics:

- Remote servers are not designed to operate independently of the Primary server or the database server. The remote server must be connected to the database server; however, it is designed to withstand occasional disconnections from the Primary server.
- Remote servers cannot host client workstation connections. Only the Primary server can support client workstations. A workstation, nonetheless, can act as both a remote server and a client workstation to the Primary server.
- If a remote server should lose connection to the Primary server, it immediately stops polling the hardware. The remote server cannot process events received from the hardware, but reconnecting with the Primary server causes polling to resume.
- Remote servers do not require additional hardware keys; however, each remote server requires a separate workstation license.

Setting up a remote server topology requires the following tasks:

- Edit the CommServerName registry setting.
- Designate the Primary server.
- Designate the remote servers.
- Restart the Pro-Watch service on the remote servers.

5.7.1 Editing the CommServerName Registry Setting

You must edit the CommServerName registry setting on all remote servers so that the CommServerName registry setting on each remote server points to the Primary server. See Chapter N, *Registry Management*.

Note: The procedures in this appendix assume that Pro-Watch Server is installed on each machine and the hardware is configured and sorted into sites on a logical and geographical basis. For example, there should be at least one site for each city, as installation spans across multiple cities connected via a WAN. See Chapter 6, for more information about site configuration.

Follow these steps:

1. Select **Start > Programs > Pro-Watch > Registry Manager** to open the Registry Manager.
2. Select the **CommServerName** registry setting and click **Edit**.
3. Within the Value dialog box, enter the name of the Primary server. Click **OK**.
4. Click **Close** to close the Pro-Watch Registry Manager.

Note: The Primary server and all remote servers must point to the same database server.

5.7.2 Designating the Primary Server

Each site requires a Primary server to manage the site's hardware. The procedure in this section designates the Primary server. The Primary server should either be the server closest to the database server or the database server itself.

Also, the Primary server and all remote servers must have workstation records in the Pro-Watch database. Therefore, after you assign a server to each site to manage the applicable hardware, you must declare the Primary server and each of the remote servers within the Database Configuration component of Pro-Watch. See Chapter 27, *Database Configuration (DBC)* for information about configuring the workstation records.

To designate a workstation as the Primary or remote server:

1. Open Database Configuration and click Workstation on the Database Configuration tree list.
2. Right-click the workstation to be designated as the Primary server and select **Properties**. The Edit Workstations dialog box appears.
3. Select the **Comm Server Tab**.
4. Select the **Communications Server** check box and select the **Primary** option button.
5. Click **OK**.

5.7.3 Designating the Remote Servers

After designating the Primary server, you must designate the applicable remaining servers as remote servers:

1. Open Database Configuration and click Workstation on the Database Configuration tree list.
2. Right-click the workstations to be designated the remote servers and select **Properties**. The Edit Workstations dialog box appears.

3. Select the **Comm Server Tab**.
4. Select the **Communications Server** check box and select the **Remote** option button.
5. Click **OK**.

You will notice distinct icons for each workstation designated as remote server. These icons appear blue if communication is active or successful; they are red if communication is inactive or lost.

5.7.4 Re-starting Pro-Watch on the Remote Servers

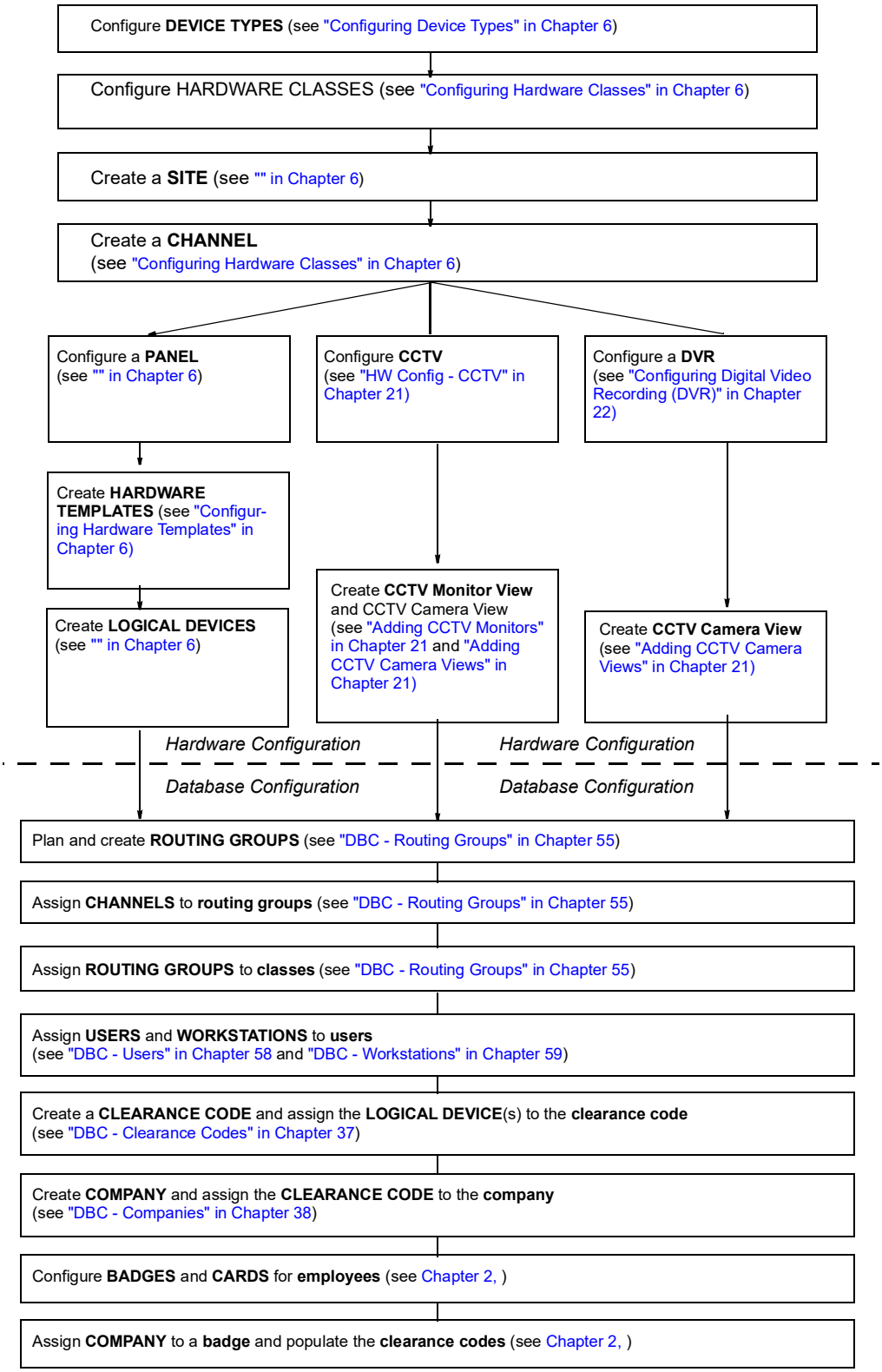
After configuring the workstations, you must re-start the Pro-Watch Service on each remote server. After the service starts, the remote servers try to connect to the Primary server. This can take up to one minute to occur.

Note: You must perform the core Pro-Watch functions such as configuring routing groups and classes before you can view any events. See Chapter 27, *Database Configuration (DBC)*.

The remote servers poll the hardware associated with the site(s). The hardware events that occur are forwarded to the Primary server to process and distribute to client workstations. Any download requests from client workstations are relayed through the Primary server to be processed locally by a remote server.

Note: The icon displayed for the remote server is the only explicit indication that the server is online or offline. Hardware connected to a remote server that is online reports status within the Logical Device, Channel, Panel, and Status Group views. Hardware connected to a remote server that is offline reports status as unknown (yellow).

5.8 Pro-Watch Configuration Preview



5.9 Tool Bar

The Pro-Watch tool bar consists of the following icons:

Button	Description
	New Click this context-sensitive button to add a new Pro-Watch object to the right pane. For example, in the Hardware Configuration module, if you select Device Types from the middle pane and click New, the Add Device Types dialog box opens to enable you to add a new device type.
	Properties Click this context-sensitive button to edit a Pro-Watch object selected from the right pane. For example, in the Hardware Configuration module, if you select the device type Door Position from the right pane and click Properties, the Edit Device Types dialog box opens to enable you to edit the attributes of the Door Position device.
	Delete Click this context-sensitive button to delete a Pro-Watch object selected from the right pane. For example, in the Hardware Configuration module, if you select the device type Door Position from the right pane and click Delete, the Door Position device will be deleted. However, an item cannot be deleted if it is used somewhere else. You must remove all the references to item before it can be deleted.
	Find Click this button to search and find a Pro-Watch object in any of the modules.

Button	Description
	Shadow User Pro-Watch allows a local administrator to login over a currently logged-on user without having the current user logoff Pro-Watch. For example, the system allows an administrator to login over a restricted class user to perform a function on the system that the current user does not have permission to perform. Thus, this means that the user's workstation never needs to go offline and never needs to be unattended. Click the Database Configuration icon on the left pane. Select Users from the Database Configuration tree view. Click New and add a new user. Go to SQL Server. Select Enterprise Manager > Security > Logins and add the user. Give the user access to Primary and Pro-Watch databases. Go to Administrative Tools within the Control Panel and select Local Security Policies > Local Policies > User Rights and Assignments. Grant "Logon as a Service" and "Act as part of the operating system." When the shadow user has logged on, you will see his/her user ID in the status bar at the bottom of the Pro-Watch screen.
	Logoff Shadow User Click this button to logoff the shadow user. This button is enabled only when an administrator is logged on as a shadow user.
	View Event Log Click this button to display the event log dialog box. The Event Log allows you to create SQL queries using fields including: Database Field Operator Date and Time Value Sort By After defining the SQL queries, you may search for events in the event log or choose to view the last 500 alarms.
	Viewer Bar Click this button to hide or display the left panel.

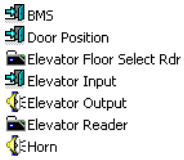
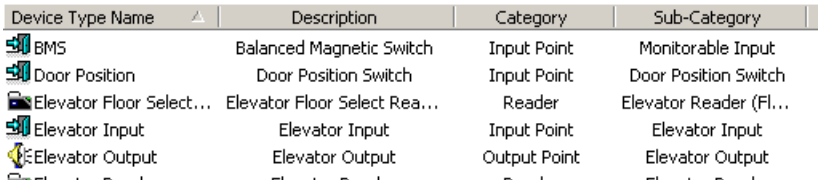
Button	Description
	Toggle Event (Event Monitor) Click this button to display the event monitor screen to view events. Click Arrange on the mini tool bar to display the Arrange Event Viewer Columns dialog box. You can select one of the following Database Fields from the drop-down list: Event Date, Logical Device Description, Alarm Type, Panel Name, Subpanel Name, Reader Name, Input Name, Output Name, Company Name, Workstation, User. Click Filter on the mini tool bar to display the Event Viewer Filter dialog box where you can filter the events by Message Type, Workstation, and User ID by selecting appropriate values from the three respective drop-down lists. Click the Download Messages tab at the bottom of the screen to view the list of downloaded messages. Click Download Message Parameters to display the Channel Download dialog box. In this dialog box, you can set the time interval (in seconds) for the download channel interval.

Button	Description
	Verification Verification viewer provides for remote, operator-validated access for particular access points. See Appendix A, Secure Mode Verification. **Note:** Click **New** to display the Logical Devices screen where the devices are listed by Description and Location. Select a logical device by highlighting it. Click **OK** to add it to the Logical Device Name pane. You can have an unlimited number of logical devices added for verification. The user can also search for logical devices that are not displayed in the Logical Devices screen. As the user types in a string into the "Search Key" field in the upper-right corner of the screen, the Logical Devices that have descriptions or locations that match are returned. This is helpful on sites that have a large number of logical devices. Click **Live Video Window** to toggle the live video window on and off for all the logical devices selected in the left pane. Click **Cascade** to cascade the verification windows for all the logical devices selected in the left pane. Click **Freeze** to freeze the live video. Click **Erase All** to erase all video. Click **Show Pictures Given Access** to display in the verification window the photograph or signature of the card holder plus a video picture (live or frozen) for only those events with access-granted status. Click **Sound Bell On Grant Transaction** to ring a bell when a grant transaction is received by the operator. Click **Show Pictures Denied Access** to display in the verification window the photograph or signature of the card holder plus a video picture (live or frozen) for only those events with access-denied status. Click **Sound Bell On Grant Transaction** to ring a bell when a grant transaction is received by the operator. Click **Print Area Members** to print the area members.

Button	Description
	Mustering Click the mustering button for real-time monitoring of who is in or out of a particular area. The information is listed across the Event Time, Device Description, Name, Card No., and Description columns. The Mustering mini tool bar enables you to toggle the **Freeze** button to freeze the list on the verification viewer. Also, you can toggle the **Bell** button to play a sound when a grant transaction is received by the viewer. To print the mustering information, click **Print**.
	CCTV Controls Click this button to display the CCTV Controls dialog box where you can select a camera and monitor, switch the camera's video to the selected monitor, view presets, pan/tilt, zoom, focus, and change the iris of the selected camera. See "HW Config - CCTV" in Chapter 21 for more information about CCTV. Select the camera from the pull-down Camera menu. To switch the camera's view to a monitor, select the monitor from the pull-down Monitor menu and click **Switch**. To set the camera and view to a preset position, select the position from the pull-down Preset # menu. Use the Pan/Tilt arrows to move the view to the desired spot. Clicking an arrow moves the camera view in the indicated direction until you click the red stop sign. Use the Zoom arrows to zoom in (Up arrow) or zoom out (Down arrow). Use the Focus arrows to adjust the proper focus. Use the Iris arrows to adjust the view's area. Click Set to set the configuration.

Button	Description
	Intercom Controls Click this button to display the Intercom Controls dialog box where you can place a call from one intercom station to another. Select a Source Intercom (the intercom station from which the call will be initiated) from the drop-down list. Select a Target Intercom (the intercom station receiving the call) from the drop-down list. Select a Connection Priority by selecting the appropriate option button. “Dial” is the lowest priority call. If the target is in use, a busy signal is returned. “Low Priority Direct” is a medium priority call. This call forces the target intercom to pick up on the first ring. If the target is in use, a busy signal is returned. “High Priority Direct” is a high priority call. This call forces the target intercom to pick up on the first ring. This call also overrides any call on the target except for another High Priority Direct. Click Call to initiate the call. Click Reset to terminate an active intercom session and leave the dialog box ready to make another call.
	Void Card Click this button to display the Void Card dialog box where you can void a card. Select a search field from the Fields drop-down list. Your options are Card Holder Last Name, Card Number, and Company. Enter a search criterion into the Criteria field. When searching by card number, you have to enter the exact card number to find the correct card. When searching by last name, entering only the first letter (or the first few letters) of the last name as a “wild card” character will find all the last names that start with that letter (or letters). For example, if you select Card Holder Last Name as a search criterion, entering “J” or “j” (not case sensitive) in the Criteria field will return all cards with card holder last names that start with “J” including “James,” “John,” “Jameson,” etc. Entering “Ja,” however, will return “James” and “Jameson” but not “John.” Click Find Now to list the search results in the grid below. Select the card you want to void and click Void.

Button	Description
	Digital Video Recording Click this button to configure the numbers and channels of digital video recording display. See "Configuring Digital Video Recording (DVR)" in Chapter 22 for more information about DVR. Select a video display “dimension” from the Dimensions drop-down list. Your selection will determine how many camera views will be displayed simultaneously on this screen. For example, “1 X 1” will display video feed from only one camera whereas “4 X 4” will display a maximum of 16 video feeds from all the 16 cameras. Other available dimension options are 4 (“2 X 2”) and 9 (“3 X 3”) camera feeds. Select a channel from the Channel drop-down list. You can set up cameras on different channels Click one of the 16 Rapid Eye buttons to select one or more of the 16 cameras. When you click on a number-button, the corresponding camera image will appear in the window. You can choose to view more that one image at a time through selecting a value from the Dimensions drop-down list (see step 1). The Current Data/Time field provides a “time stamp” for the video feed(s).
	Large Icons Click this button to have the Pro-Watch items listed by large icons. For example: 
	Small Icons Click this button to have the Pro-Watch items listed by small icons. For example: 

Button	Description
	List Click this button to have the Pro-Watch items listed in an alphabetical list. For example: 
	Details Click this button to have the Pro-Watch items listed in an alphabetical list, across detail columns determined by system settings. For example: 

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Hardware Configuration (HW Config)

6

In this chapter ...

Overview
Using the Hardware Manager Wizard
Configuring Device Types
Configuring Hardware Classes
Configuring Hardware Templates
Configuring The Hardware System
Status
Panel Download
Logical Device Icon
Status Groups
Guard Tours

6.1 Overview

The Pro-Watch access control system supports hardware, including multiple panel types, Logical Devices (readers, monitorable inputs and controllable outputs), closed circuit television (CCTV), digital video recorders (DVR), and intercoms produced by Honeywell and third-party manufacturers.

Within the Hardware Configuration component, these various hardware types are added and configured; for example, Logical Devices are configured in functional groups, which are defined by hardware templates. These Logical Devices, as well as panel, CCTV, DVR, and Intercom hardware, are also governed in the Pro-Watch system by a number of database entities, such as routing groups, clearance codes, workstations, and time zones. Therefore, to complete the Pro-Watch configuration you must complete tasks within the Database Configuration component of Pro-Watch as well. The following chart illustrates the core Pro-Watch hardware configuration tasks described in this chapter.

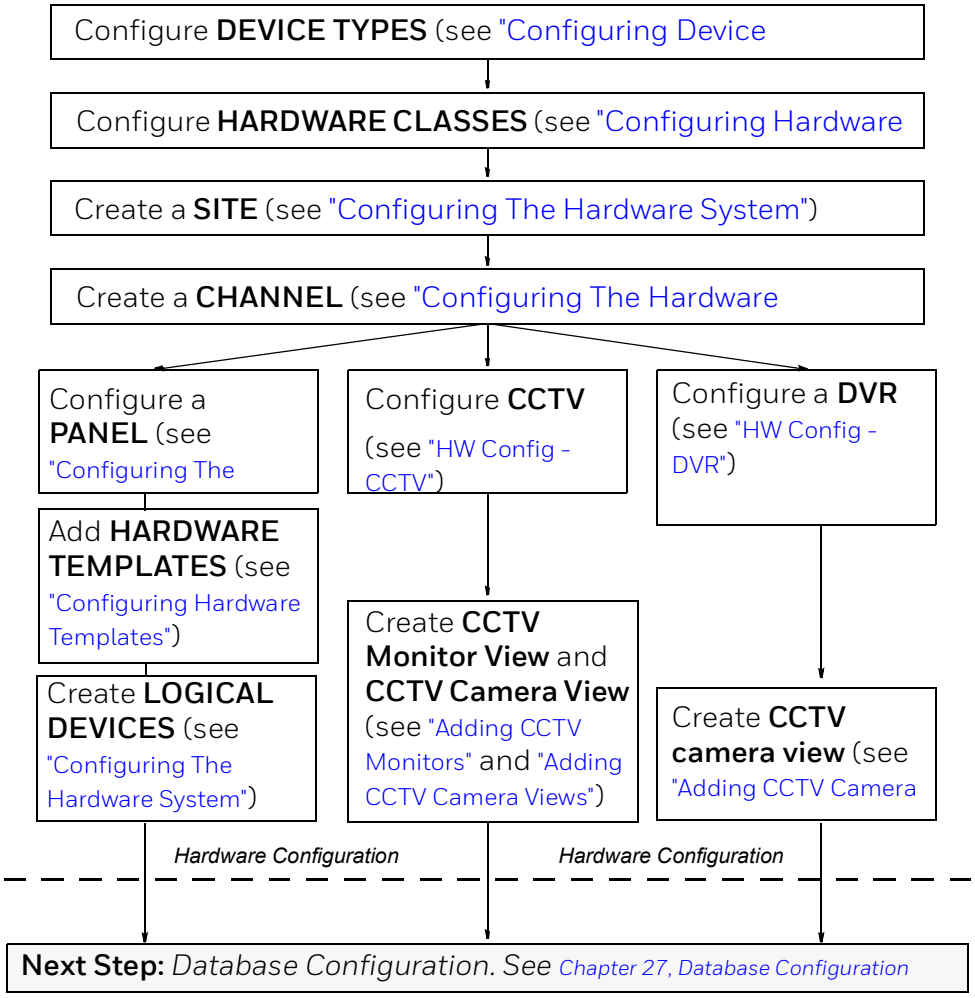
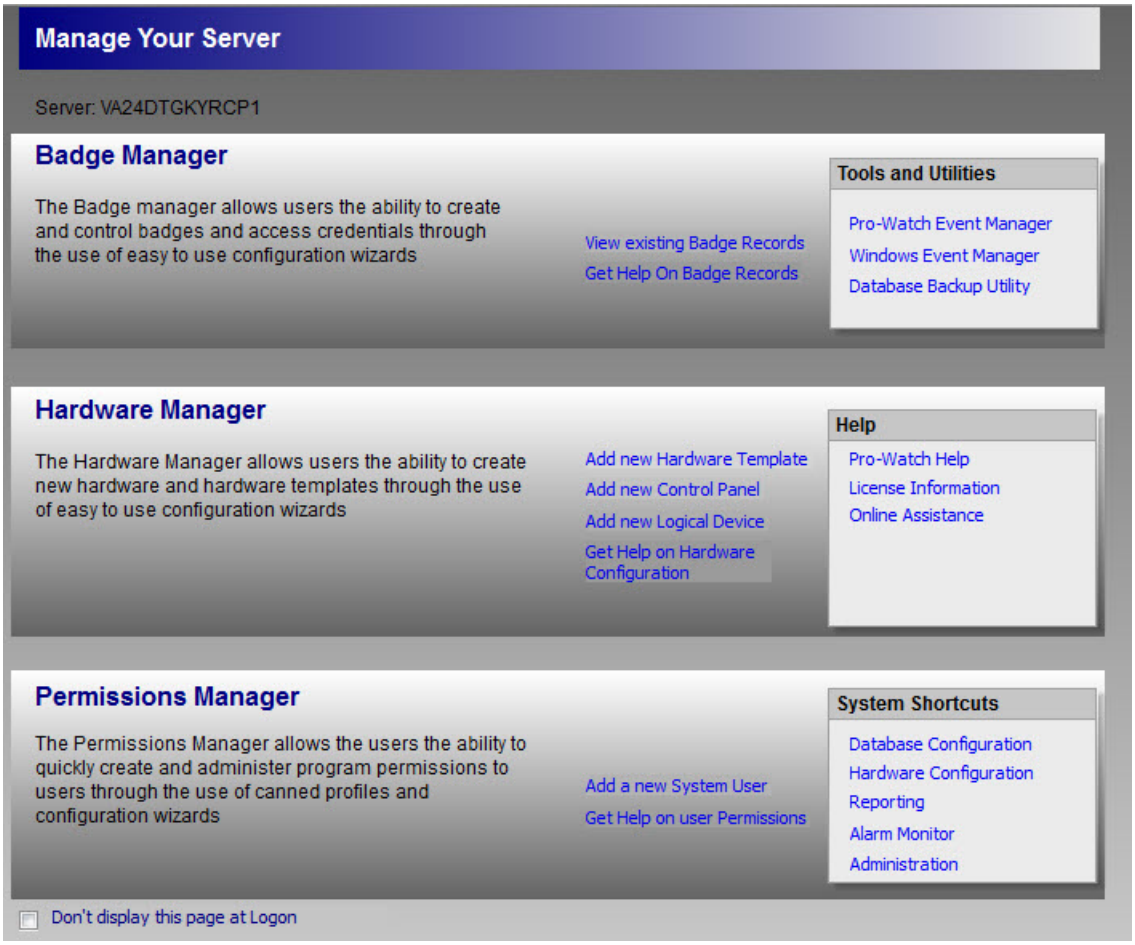


Figure 6-1 Hardware Configuration Task Flow

Pro-Watch provides the Hardware Manager wizard that automates tasks shown in the figure above to help you add a new Hardware Template, a Panel, and a Logical Device more quickly.

6.2 Using the Hardware Manager Wizard

The Hardware Manager wizard automates the tasks necessary to add a new Hardware Template, Panel, or Logical Device. To access the wizard, select **File > Wizard** to display the **Manage Your Server** window:



Note: The "**File > Wizard**" sub-menu option will dynamically display under the **File** menu only when the user is not at the **Manage Your Server** screen.

6.2.1 Toggling Off the "Manage Your Server" Screen

The Manage Your Server window displays the Badge Manager, Hardware Manager, and Permissions Manager wizards by default on startup. To prevent the Manage Your Server window from appearing, select the "**Don't display this page at Logon**" check box in the lower-left corner.

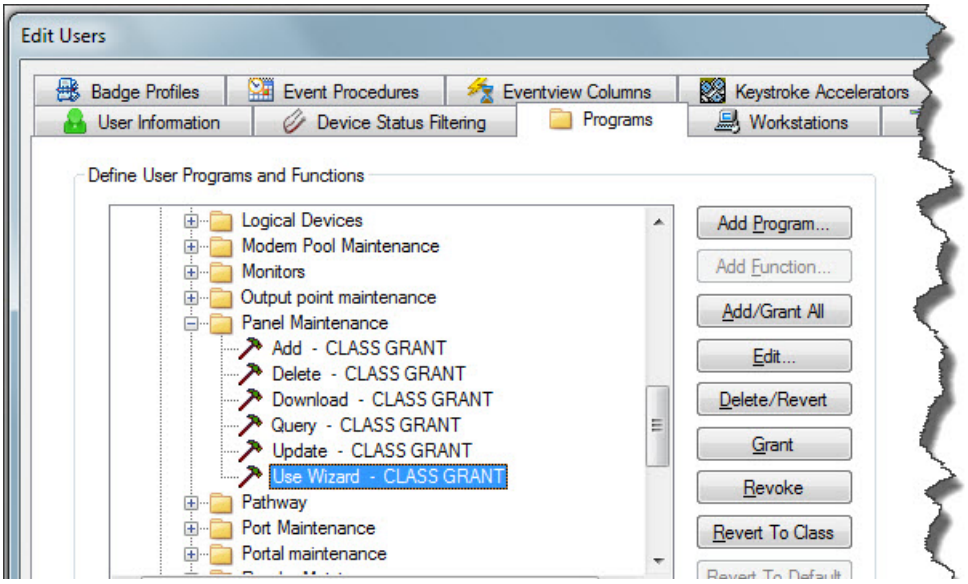
6.2.2 Turning the User Wizard On and Off

Caution: There are two different "wizards" in Pro-Watch.

1. Select **File > Wizard** to display the **"Manage Your Server" wizard screen**. This screen offers convenient links to the three main modules: Badge Manager, Hardware Manager, and Permissions Manager.
2. The **"Hardware Use Wizard"** that allows a user to add a panel or a logical device easily is **turned on by default** when the Pro-Watch is launched.

Follow these steps to turn on or off the Hardware Use Wizard:

1. From the left navigation pane, double-click and select **Database Configuration**.
2. Double-click and display all the **Users** in the right pane.
3. Select a **User** icon and right-click to display the **Properties** screen.
4. Select the **Programs** tab.
5. Click and open the **Hardware Configuration** tree-list.
6. Click and open the **Panel Maintenance** tree-list:



7. Select the **Use Wizard.** Click **Revoke** to turn it off, and click **Grant** to turn it on (if it's off). Click **OK** to close the dialog box.

6.2.3 Adding a Hardware Template

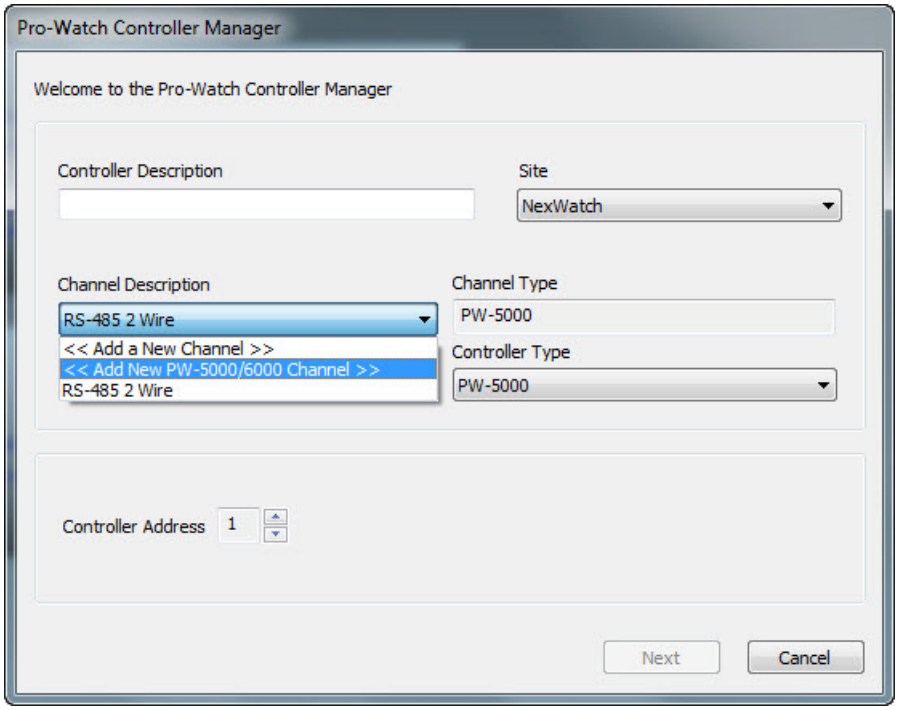
A Pro-Watch hardware template is a pre-defined set of control panel configuration information. You specify a hardware template when you add a new control panel to the Pro-Watch system. The template then automatically configures the panel with basic Pro-Watch information, including Logical Device configuration, PW-5000 interlocks, PW2000 interlocks, SEEP interlocks, guard tours, and events.

To add a hardware template, click **Add new Hardware Template** to display the Add Hardware Templates dialog box. Refer to "Adding or Editing a Hardware Template" to complete the tab information.

6.2.4 Adding a New Control Panel

To add a new control panel from the **Manage Your Server** window, perform the following steps:

1. Click **Add new Control Panel** to display the **Pro-Watch Controller Manager** dialog box:



   a. Enter a **Controller Description** (name).

   b. Select the **Site** associated with the controller.

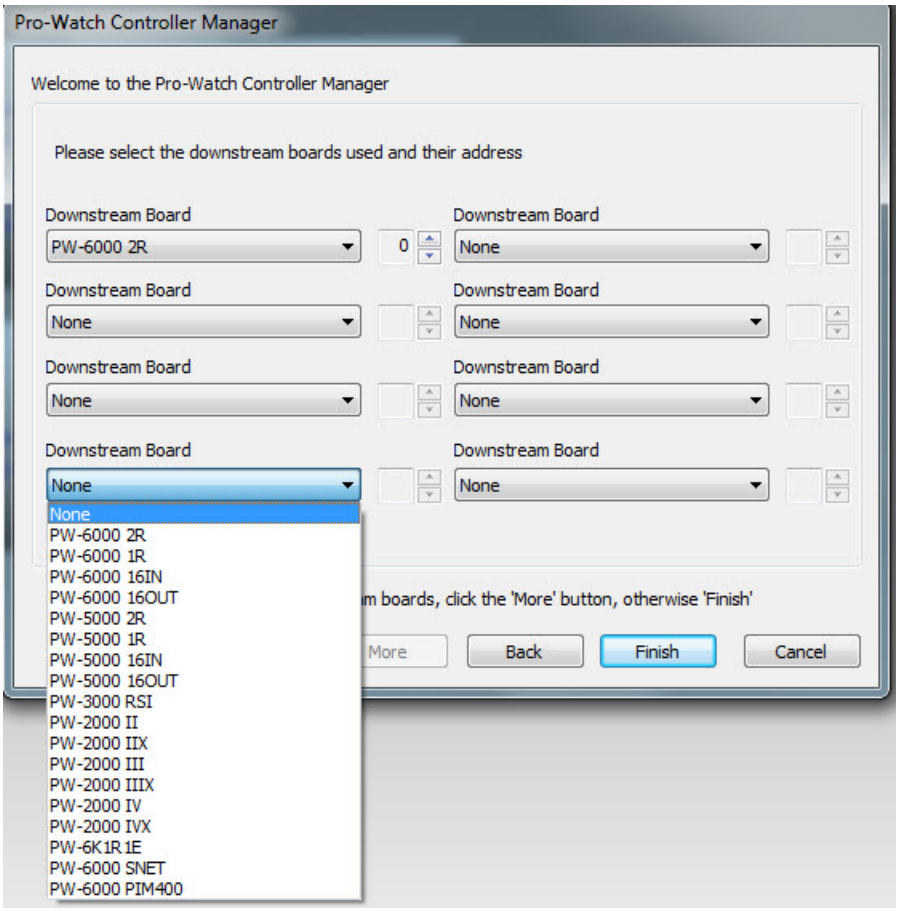
   c. Select the **Channel Description** (channel name) the controller will use.

   d. Select the Channel Type.

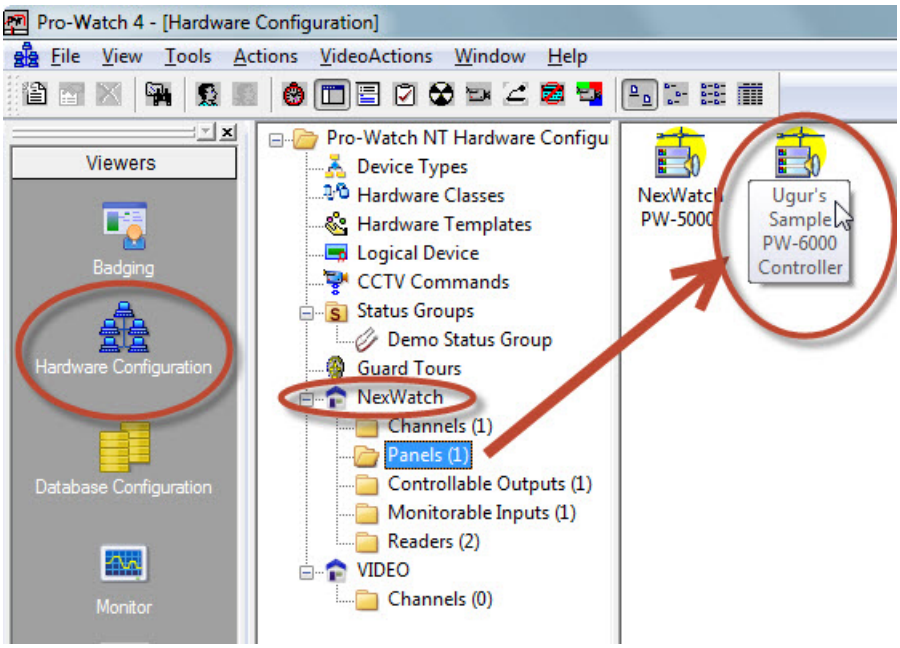
   e. Select the Controller Type.

   f. Select a **Controller Address** from the combo-box.

g. Click **Next** to display the downstream board dialog box:



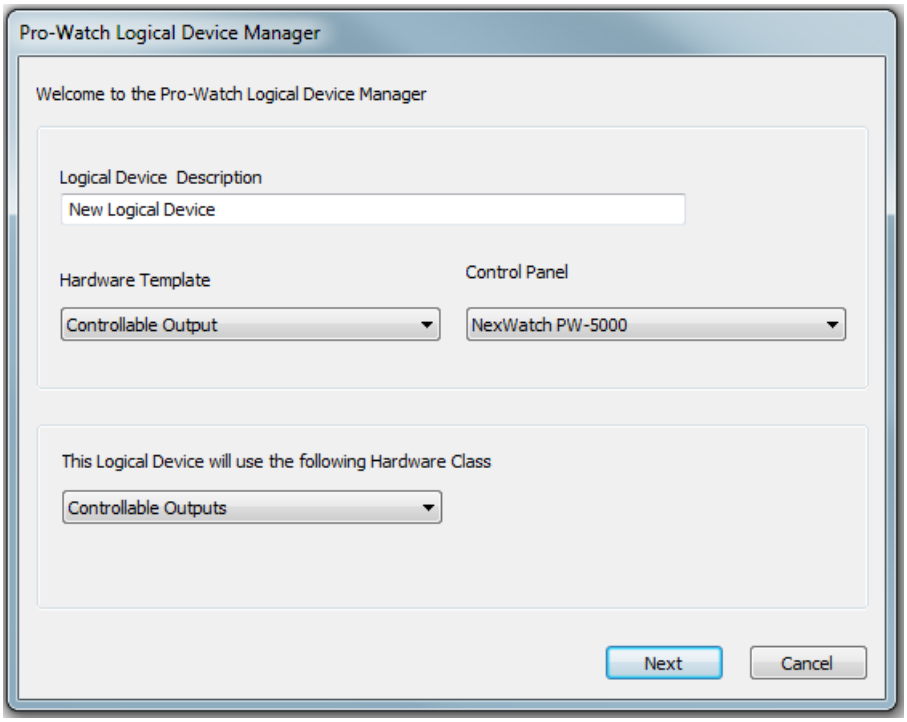
2. Select all of the panel's **downstream** (or sub-panel) **board**(s), and enter their **addresses** in the respective combo-box.
3. Click **Finish** to complete the panel addition. Pro-Watch will display the newly created panel in the respective site (**NexWatch** in our case), under the list of panels:



6.2.5 Add Logical Device

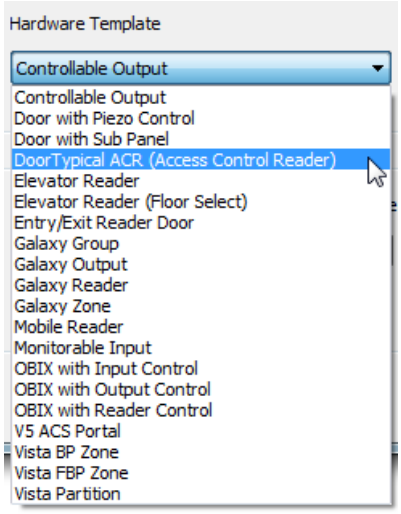
To add a new Logical Device from the **Manage Your Server** window, click **Add new Logical Device** to display the **Pro-Watch Logical Device**

Manager dialog box:



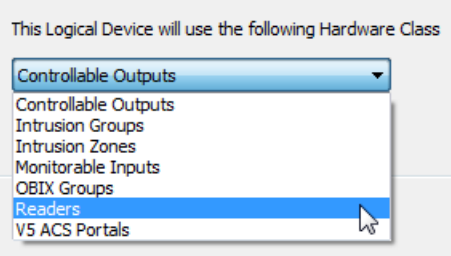
Perform the following steps:

1. Enter a **Logical Device Description**. For example: “New Logical Device.”
2. Select the **Hardware Template** that is appropriate for the Logical Device you want to add. Here are some of the possible options:

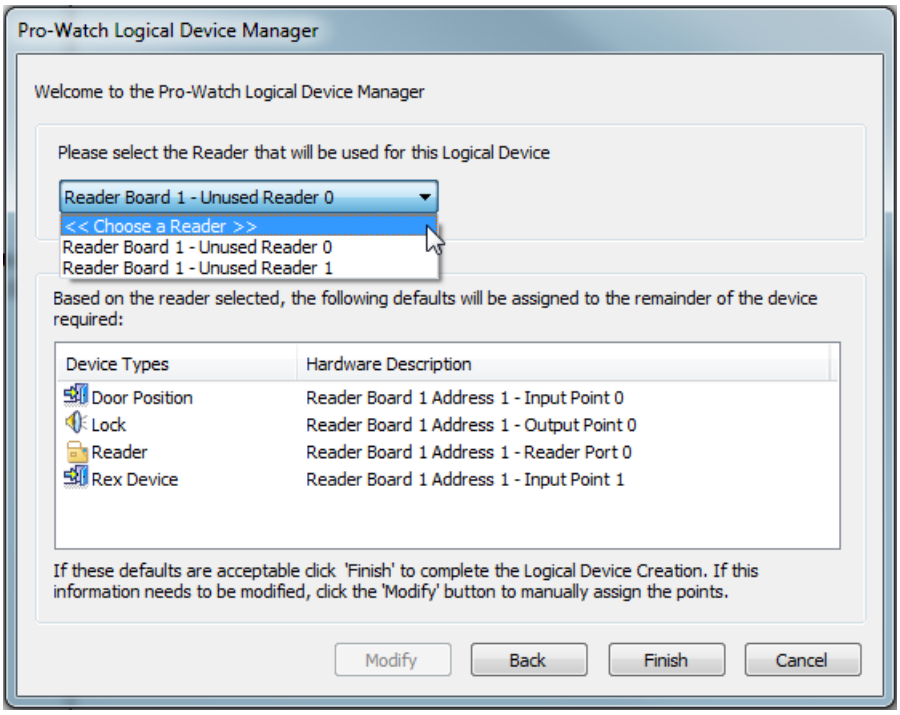


3. Select the **Control Panel** that will control the new Logical Device.

4. Select the appropriate **Hardware Class** for the new Logical Device. Here are some of the possible options:

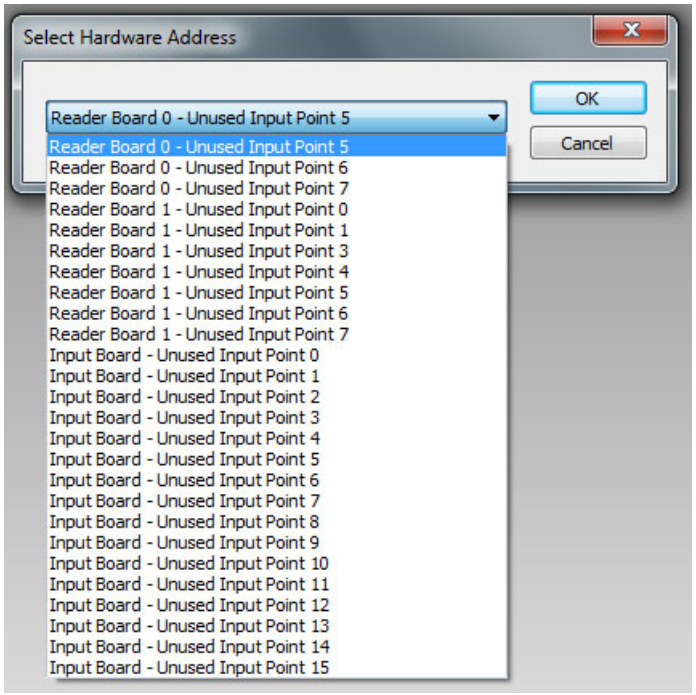


5. Click **Next** to display the next dialog box, presented dynamically depending on the choices you've made above:



6. Select the actual **Reader** that will be used for the Logical Device you want to add. The **Device Types** associated with the reader you have selected appear with their default hardware addresses.

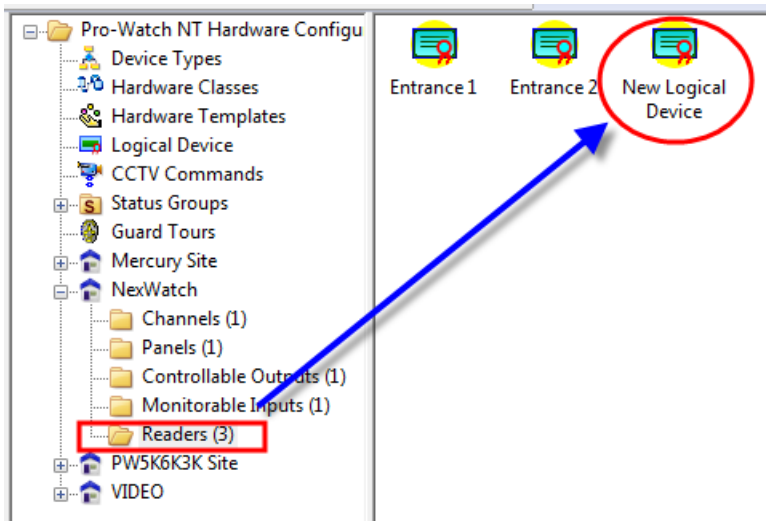
7. If you wish to assign different hardware to any of the device types, select and then click **Modify** to modify in the **Select Hardware Address** dialog box:



8. Click **OK** to return to the previous screen.
9. Click **Finish** to add the Logical Device.

Note: After you create a Logical Device, the Logical Device icon appears under its assigned **Site** (NexWatch in our case) in the Hardware Configuration tree, in its respective folder determined by your choice of **Hardware Class** in Step 4 above. For example, in the above exercise, we've

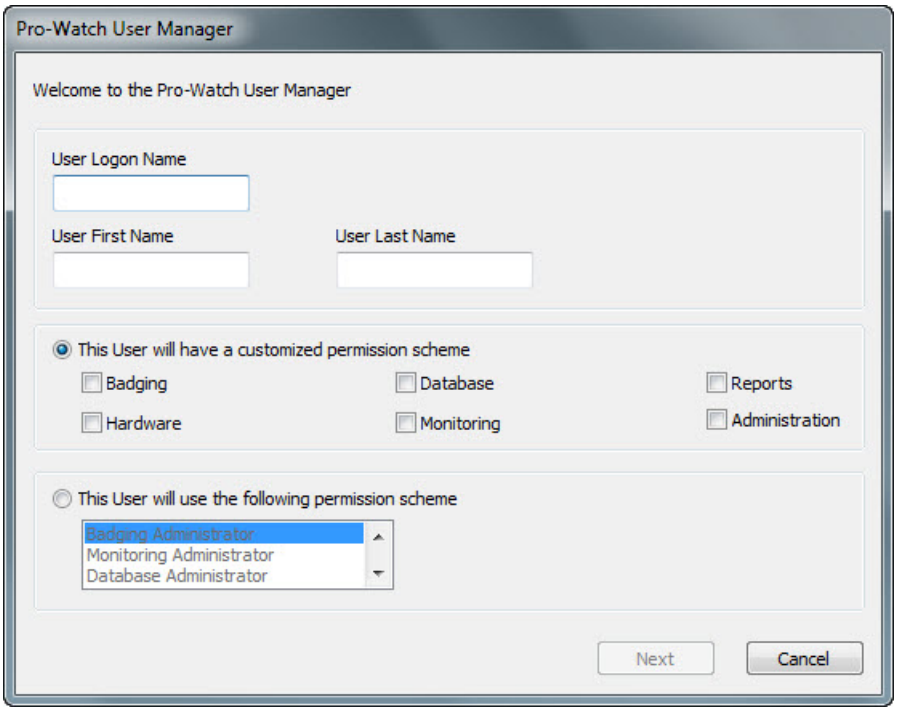
chosen "**Readers**" as a hardware template. That's why the logical device we've created is displayed inside the **Readers** folder:



6.2.6 Adding a System User

To add a system user from the **Manage Your Server** window, follow these steps:

1. Click **Add a new System User** to display the **Pro-Watch User Manager** dialog box:



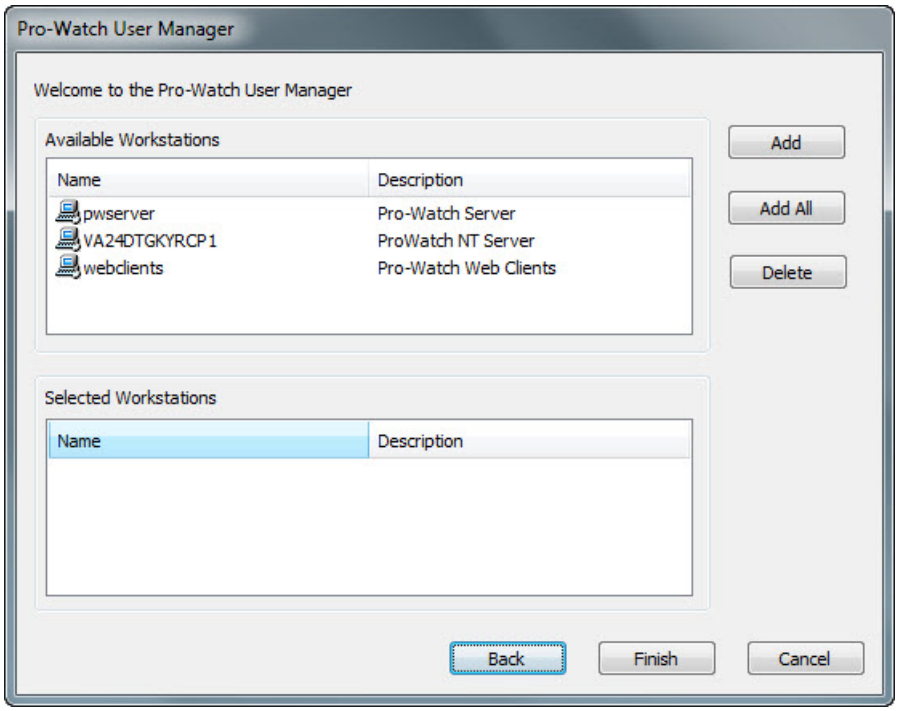
2. Enter a unique **User Logon Name**.
3. Enter a **User First Name** and **User Last Name**.

4. Select an appropriate **Customized Permission Schedule** by selecting the **"This user will have a customized permission scheme"** option button. The schedule options are **Badging, Database, Reports, Hardware, Monitoring, Administration**.

   Note: You can select multiple customized permission schemes simultaneously.

5. Or, select the **"This user will use the following permission scheme"** option button and select a permission scheme from the class of options displayed in the list box like Badging Administrator, Monitoring Administrator, etc. See "DBC - Classes" in Chapter 36 for information about Classes.

6. Click **Next** to display the workstation assignment dialog box:



7. **Take one of the following alternative actions** to select and display the workstation(s) you want in the **Selected Workstations** box:

   a. **Double-click** the workstation in the **Available Workstations** box.

   b. Select the workstation in the **Available Workstations** box and then click **Add**. To add all the workstations, click **Add All**.

   c. **Click and drag** the workstation you want down to the **Selected Workstations** box below.

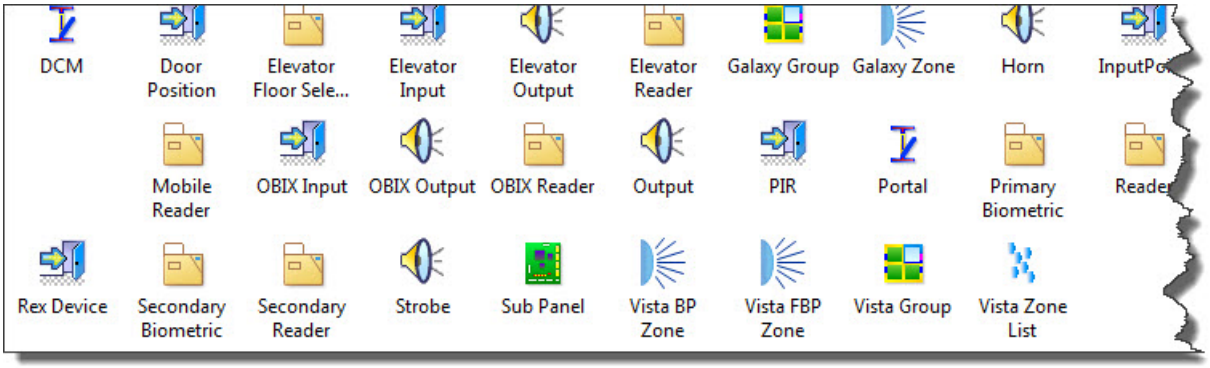
8. Click **Finish**. The new user created will be displayed in the **Database Configuration > Users** pane.

6.3 Configuring Device Types

In the Pro-Watch system, a device type is a **hardware device** or device category, such as a reader, an **input point,** or an **output point**. You must define all device types before grouping them within templates, which in turn will be used to create Logical Devices.

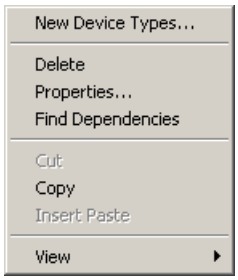
To access Device Type functions:

1. From the Hardware Configuration tree view, click **Device Types** to display the icons of the default device types in the right pane of the Pro-Watch window:



Note: Right-click any device type icon to display the shortcut menu. If no device types have been created yet, right-click anywhere in the right pane.

If no device types have been created yet, this shortcut menu only shows a subset of these functions.



2. Use the following table to select a function:

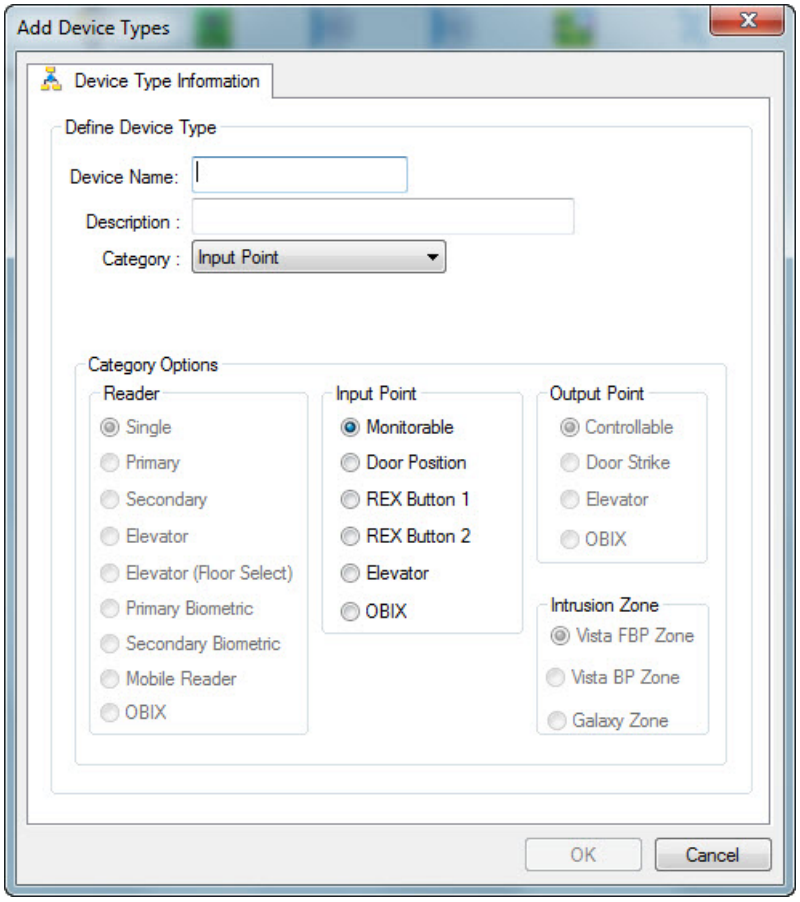
Click ...	To ...
New Device Type...	Adds a new device type. See "Adding or Editing a Device Type".
Delete	Deletes a current device type. See "Copying Device Types".

Click ...	To ...
Properties...	Edits a current device type. See "Adding or Editing a Device Type".
Find Dependencies	Display the type and name of the dependencies for the selected device type. See "Viewing the Dependencies of a Device Type".
Cut	Cuts the device information and icon and saves it in the clipboard.
Copy	Makes a copy of the device type configuration. See "Copying Device Types".
Insert Paste	Inserts the device information and icon from the clipboard.
View	Changes the way the icons are displayed in the Pro-Watch window. Viewing options are Large Icons, Small Icons, List, Details. See "Viewing the Icons".

Complete the following sections to add, edit, delete, copy, or view the device types.

6.3.1 Adding or Editing a Device Type

Right-click in the device type pane and select **New Device Type** to display the **Add Device Types** dialog box:

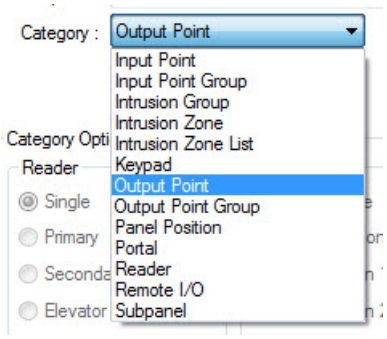
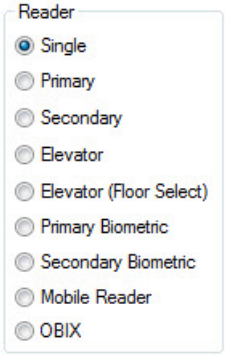


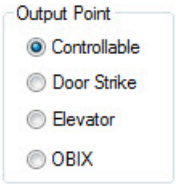
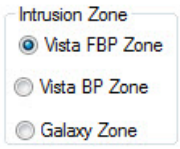
Note: To edit, right-click and select the **Properties** pop-up menu option to display the identical **Edit Device Types** dialog box.

From the Add Device Types or Edit Device Types dialog box, complete the **Device Type Information** tab.

Use the following field definitions to complete the **Device Type Information** tab:

Field	Description
Device Name	Identifies the name of the device type.
Description	Provides a description of the device type.

Field	Description
Category	Identifies the category of the device type. Here are some of the options: 
Category Options: Reader	Enabled only if Reader is selected for the Category (see the row for Category above). Identifies the different reader type options:  (For more information, see "Category Option Definitions" below).
Category Options: Input Point	Enabled only if Input Point is selected for the Category (see the row for Category above). Identifies the different input type options:  (For more information, see "Category Option Definitions" below).

Field	Description
Category Options: Output Point	Enabled only if Output Point is selected for the Category (see the row for Category above). Identifies the different output point options:  (For more information, see "Category Option Definitions" below).
Category Options: Intrusion Zone	Enabled only if Intrusion Zone is selected for the Category (see the row for Category above). Identifies the different intrusion zone options:  (For more information, see "Category Option Definitions" below).

6.3.1.1 Category Option Definitions

Reader

- ***Single***: Configures the reader as a stand-alone reader. It will have no inherent physical relationship to any other hardware assigned in the hardware template.
- ***Primary***: Configures a reader to be the primary reader that is typically placed on the non-secure side of the door. When a reader is set to be a primary reader in a hardware template, that template must also include door-specific categories such as request-to-exit buttons (REX) and door-position switches (DPS).
- ***Secondary***: Configures the reader as secondary reader in a Primary/secondary configuration for an Entry/Exit door. A secondary reader is typically placed on the secure side of a door. The secondary reader will read the values of the configured fields like "Strike time", "Held time", "Log Pre-Grant Event" etc. from the primary reader. And secondary will grant access to all the card formats accepted by the primary reader.

- ***Elevator*:** Configures the reader as a part of an elevator configuration. Elevator readers limit cardholder access to floors; however, you cannot record which floor the cardholder selected.

Note: *Elevator (Floor Select):* Configures the reader as a part of an elevator floor-select configuration. Elevator floor-select readers limit cardholder access and record the actual floor selected by the cardholder.
This option is not available on CHIP panels.

- *Primary Biometric*: Configures a primary biometric hand geometry reader as a primary reader that is typically placed on the non-secure side of the door. See Chapter 62, *Biometric Reader Configuration* for biometric hand geometry reader configuration instructions.
- *Secondary Biometric*: Configures a biometric hand geometry reader as a secondary reader that is typically placed on the non-secure side of the door.
- *Mobile Reader.* Configures the mobile reader.
- *OBIX*. Configures the OBIX reader.

Input Point

- *Monitorable:* Establishes an input as a standard input or a monitored input (i.e. motion detectors). All inputs that are not part of door or elevator configurations, such as REX buttons and DPS, are monitored inputs.
- *Door Position*: Establishes the input is specifically used to determine whether or not the door is open or closed. Requires the existence of a primary reader in the template.
- *REX Button 1:* Establishes the input as a standard request-to-exit button (REX). It requires the existence of a primary reader in the template.
- *REX Button 2:* Establishes the input as a secondary request-to-exit button (REX). Secondary REX buttons are often used in ADA (Americans with Disabilities Act)-compatible panels. It requires the existence of a primary reader in the template.

Note: *Elevator*: Establishes the input as a floor-button sensor in a floor-select elevator. It requires the existence of an Elevator (Floor Select) reader in the template. There must be one elevator input in the template for each access-controlled floor serviced by the elevator cab.
This option is not available on CHIP panels.

- *OBIX*.

Output Point

- *Controllable:* Establishes an output as a standard output or controllable output (that is, A/V sirens or lighting control). All outputs that are not part of door or elevator configurations, such as a lock, are controllable outputs.

- *Door Strike:* Establishes the output as a door strike or lock. A door strike energizes the latch or bolt on a door so that it may physically be opened. It requires the existence of a primary reader in the template.

Note: *Elevator*: Establishes the output as a message to call an elevator cab to a particular floor. It requires the existence of a reader of either elevator type in the template. On a non-floor-select elevator, it enables/disables the physical connection between the call button for a floor and the elevator controller. There must be one elevator output in the template for each access-controlled floor serviced by the cab.

Partitions must be added upon an edit of the Device Type.

- *OBIX*.

Intrusion Zone

- *Vista FBP Zone*.
- *Vista BP Zone*.
- *Galaxy Zone*.

To assign a partition to an existing device type:

1. Click the Partitions tab and then click **Add**.
2. Select an available partition, and then click **OK**. See "DBC - Partitions" in Chapter 53 for more information about partitions.

6.3.2 Deleting a Device Type

Use this function to delete a Device Type from the Pro-Watch database.

1. In the Pro-Watch Hardware Configuration tree list, click **Device Types** to display the Device Type icons in the right pane.

Note: Right-click the Device Type you want to delete and select **Delete**.

You cannot delete a Device Type that has dependencies. A dependency is another database object that includes the Device Type in its configuration. The Device Type object depends upon the Company, Event Trigger, and Hardware Template objects. If the Device Type has no current dependencies, you are prompted to confirm the deletion. However, if the Device Type does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Device Type:

    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.

b. Either change or delete each of the objects listed as dependencies.

3. Repeat step 2 and click **Yes** at the prompt to delete the Device Type.

6.3.3 Viewing the Dependencies of a Device Type

Use this function to view and modify the Device Type's dependencies. Device Type objects depend upon the Company, Event Trigger, and Hardware Template objects.

To view the current dependencies for the selected Device Type:

1. Right-click the icon of an existing **Device Type** in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** The Dependencies dialog box appears and lists the Device Type's existing dependencies.
2. To modify or remove the dependency, double-click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

6.3.4 Copying Device Types

To copy a device type:

1. In the Hardware Configuration tree view, click **Device Types** to display the device types in the right pane.
2. Right-click the device type and select **Copy**.
3. Right-click anywhere in a blank area of the right pane.
4. Select **Paste**. A new Device Type icon with the name "Copy of [device type name]" appears.
5. To rename and edit the new device type, see "Adding or Editing a Device Type".

6.3.5 Viewing the Icons

Use this function to change the visual display of the icons in the right pane of the Pro-Watch Hardware Configuration window.

1. Right-click anywhere in the right pane of the Hardware Configuration window and select **View**.
2. Click one of the following four view options:
   - Large icons – displays larger icons.
   - Small icons – displays smaller icons.
   - List – displays the icons in an alphabetical list.

- Details – displays the icons across system-defined detail columns.

6.3.6 Default Assignments for Readers

The default assignments for the REX and DPOS are determined in three ways:

1.For **ASSA/ABLOY Aperio Hub readers**, the inputs, outputs and readers are hard coded in groups; with the first output and the first three inputs always associated with the first reader; the second output and the second three inputs associated with the second reader, etc. Of the three inputs, the first input is always the DPOS, the second is always REX0 and the third is always REX1. A database view groups and arranges the hardware accordingly.

2.For **PIM, SALTO and F/2F readers on an M5-8RP board**, the inputs, outputs and readers are also hard coded in groups like the ASSA ABLOY readers, but with only two inputs instead of three for each reader. For PIM and SALTO, the first input is always the DPOS, and the second is always the REX. For the M5-8RP, the first input is always the REX and the second is always the DPOS. A database view groups and arranges the hardware accordingly.

3.For **all other hardware**, if there are two inputs, the first is always the DPOS and the second is always the REX. The order in which the inputs are listed in the hardware template doesn't matter. This is currently hard coded.

This means, when doing the default assignments for a F/2F reader, the inputs will be backwards for M5-2RP and M5-2SRP boards. Thus they must be reassigned.

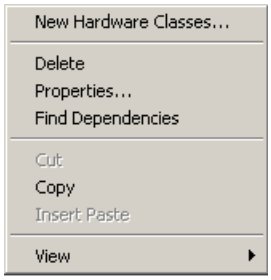
6.4 Configuring Hardware Classes

In the Pro-Watch system, you will need to group the system hardware into different hardware classes for organizational purposes. A hardware class is a category of associated Logical Devices.

For example, you may have a group of readers that only work with a particular panel. In this case, you would create a new reader hardware class.

To access Hardware Class functions:

1. From the Hardware Configuration tree view, click **Hardware Classes** to display the icons of the default hardware classes in the right pane of the Hardware Configuration window.
2. Right-click any hardware class icon to display the shortcut menu (if no hardware classes have been created yet, right-click anywhere in the right window):



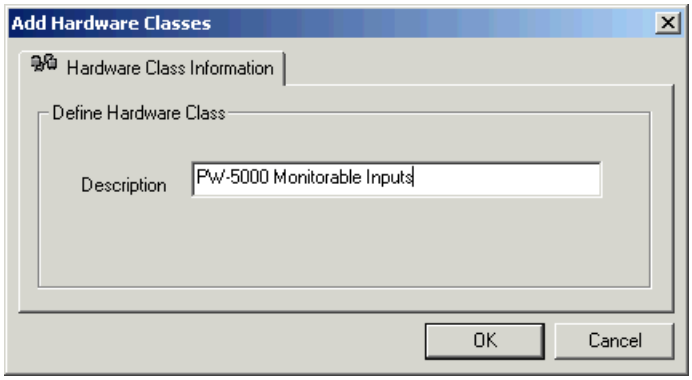
3. Use the following table to select a function:

Click ...	To ...
New Hardware Classes...	Adds a new hardware class. See "Adding or Editing a Hardware Class".
Delete	Deletes a current hardware class. See "Deleting a Hardware Class".
Properties...	Edits a current hardware class. See "Adding or Editing a Hardware Class".
Find Dependencies	Display the type and name of the dependencies for the selected hardware class. See "Viewing the Dependencies of a Hardware Class".
Copy	Makes a copy of the hardware class configuration. See "Copying Hardware Classes".
View	Changes the way the icons are displayed in the Pro-Watch window. See "Viewing the Icons".

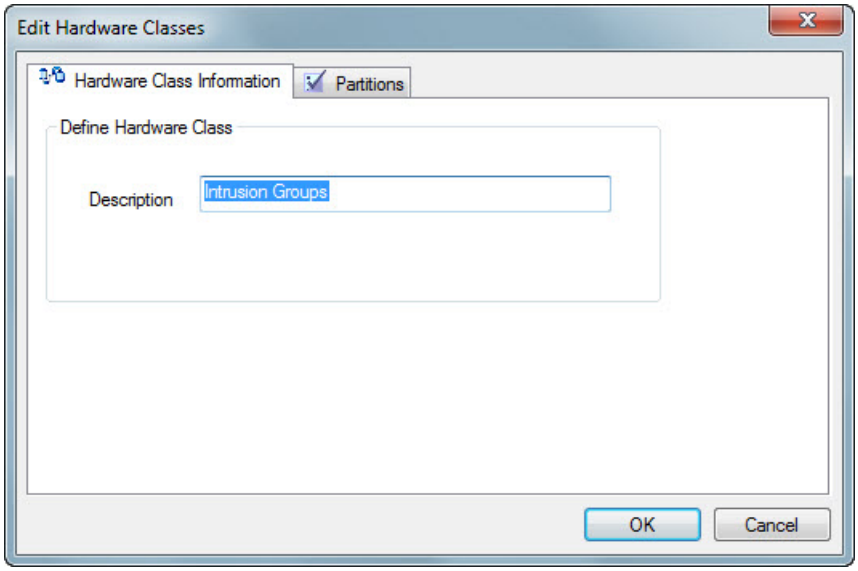
Complete the following sections to add, edit, delete, copy, or view the hardware classes.

6.4.1 Adding or Editing a Hardware Class

1. To *add* a new hardware class, right-click either the Hardware Class icon in the Hardware Configuration tree view or anywhere in the right pane of the Pro-Watch window and select **New Hardware Classes**. The Add Hardware Class dialog box appears.



2. To *edit* an existing hardware class, right-click the Hardware Class icon in the right pane of the Hardware Configuration window and select **Properties** to display the **Edit Hardware Classes** dialog box:



   In the **Hardware Class Information** tab, enter or edit a description in the **Description** field and click **OK**.

3. To add a hardware class partition (for more information about partitions, see "DBC - Partitions" in Chapter 53):

   a. Click the **Partitions** tab.

b. Click **Add**.

c. Select an available partition.

d. Click **OK**.

4. To delete a hardware class partition:

   a. Click the **Partitions** tab.

   b. Select the partition.

   c. Click **Delete**.

6.4.2 Deleting a Hardware Class

Use this function to delete a Hardware Class from the Pro-Watch database.

1. In the Pro-Watch Hardware Configuration tree list, click **Hardware Class** to display the Hardware Class icons in the right pane.

Note: Right-click the Hardware Class you want to delete and select **Delete**.

You cannot delete a Hardware Class that has dependencies. A dependency is another database object that includes the Hardware Class in its configuration. The Hardware Class object depends upon the Logical Device object. If the Hardware Class has no current dependencies, you are prompted to confirm the deletion. However, if the Hardware Class does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Hardware Class:

   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.

   b. Either change or delete each of the objects listed as dependencies.

3. Repeat step 2 and click **Yes** at the prompt to delete the Hardware Class.

6.4.3 Viewing the Dependencies of a Hardware Class

Use this function to view and modify the Hardware Class's dependencies. Hardware Class objects depend upon the Logical Device object.

To view the current dependencies for the selected Hardware Class:

1. Right-click the icon of an existing Hardware Class in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** The Dependencies dialog box appears and lists the Hardware Class's existing dependencies.
2. To modify or remove the dependency, double-click the specific dependency in the list to display its Edit dialog box.

3. After you finish viewing, click **OK** to close the dialog box.

6.4.4 Copying Hardware Classes

To copy a hardware class:

1. In the Hardware Configuration tree view, click **Hardware Classes** to display the hardware classes in the right pane.
2. Right-click the hardware class, and click **Copy**.
3. Right-click anywhere in a blank area of the right pane.
4. Select **Paste**. A new Hardware Class icon with the name “Copy of [hardware class name]” appears.
5. To rename and edit the new Hardware Class, see "Adding or Editing a Hardware Class".

6.4.5 Viewing the Icons

Use this function to change the visual display of the icons in the right pane of the Pro-Watch window.

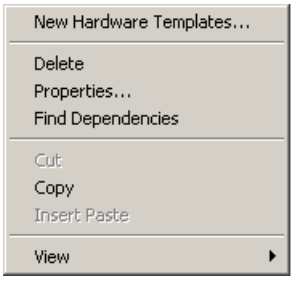
1. Right-click anywhere in the right pane of the Hardware Configuration window and click **View**.
2. Click one of the following four view options:
   - Large icons – displays larger icons.
   - Small icons – displays smaller icons.
   - List – displays the icons in an alphabetical list.
   - Details – displays items across system-defined detail columns.

6.5 Configuring Hardware Templates

Hardware templates are configured after you define the relevant channels, panels, CCTV monitors and camera views, intercoms, and device types. During the hardware template configuration process you determine the related template information such as Logical Device configuration, PW-5000 interlocks, PW2000 interlocks, SEEP interlocks, guard tours, events, and intrusion groups and intrusions zones.

To access Hardware Template functions:

1. From the Hardware Configuration tree view, click **Hardware Templates** to display the icons of the currently-configured hardware templates in the right pane of the Pro-Watch window.
2. Right-click any hardware template icon to display the shortcut menu (if no hardware templates have been created yet, right-click anywhere in the right pane). Note that if no Hardware Templates have been created yet, this shortcut menu only shows a subset (New Hardware Templates and View) of these functions:



3. Use the following table to select a function:

Click ...	To ...
New Hardware Template...	Adds a new hardware template. See "Adding or Editing a Hardware Template".
Delete	Deletes a current hardware template.
Properties...	Edits a current hardware template.
Find Dependencies	Display the type and name of the dependencies for the selected hardware template. See "Viewing the Dependencies of a Hardware Template".
Copy	Makes a copy of the hardware template configuration.

Click ...	To ...
View	Changes the way the icons are displayed in the Pro-Watch window.

Complete the following sections to add, edit, delete, copy, or view the hardware templates:

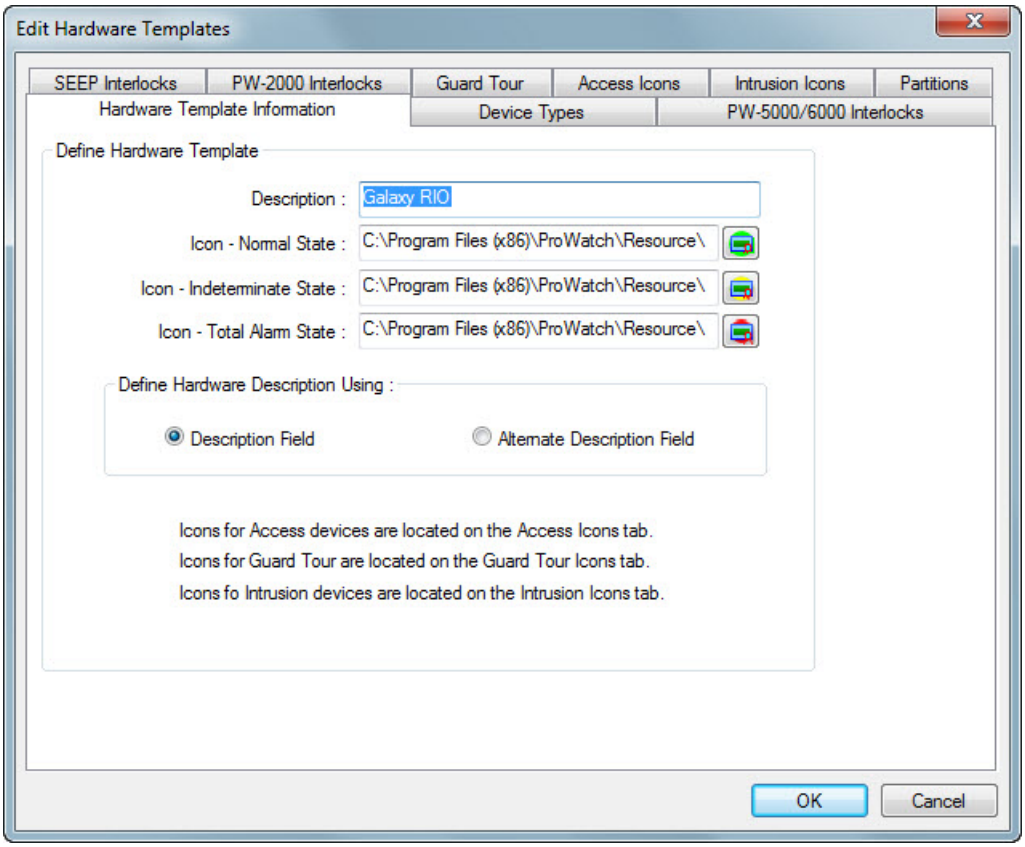
6.5.1 Adding or Editing a Hardware Template

To add or edit a hardware template:

1. To *add* a new hardware template, right-click either the Hardware Template icon in the hardware configuration tree view or anywhere in the right pane of the Hardware Configuration window and select **New Hardware Templates**. The Add Hardware Templates dialog box appears.

   To *edit* an existing hardware template, right-click the Hardware Template icon in the right pane of the Hardware Configuration window and select **Properties** to display the **Edit Hardware Templates** dialog

box:



Note that changes made to a Hardware Template will only effect new Logical Devices not existing Logical Devices.

2. Complete each appropriate tab to configure the hardware template. See the following tab list and tab sections for the configuration information:

EDIT HARDWARE TEMPLATE TABS LIST

- "Hardware Template Information Tab"
- "Device Types Tab"
- "PW-5000/6000 Interlocks Tab"
- "SEEP Interlocks Tab"
- "PW2000 Interlocks Tab"
- "Guard Tour Tab"
- "Access Icons Tab"
- "Intrusion Icons Tab"
- "Partitions Tab"

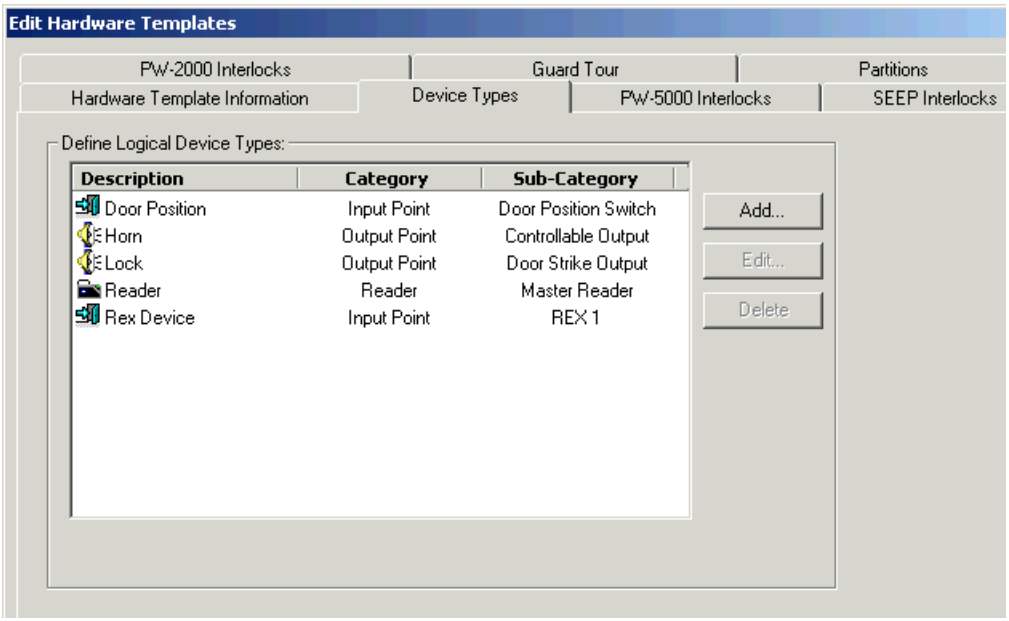
6.5.1.1 Hardware Template Information Tab

Use the following field descriptions to complete the Hardware Template Information tab:

Field	Description
Description	Provides the description of a Hardware Template.
Icon - Normal State	Icon display for a Logical Device in normal state.
Icon - Indeterminate State	Icon display for a Logical Device in an indeterminate state.
Icon - Reader Off-Normal	Icon display for a reader in an off normal state.
Icon - Input Off-Normal	Icon display for an input in an off normal state.
Icon - Output Off-Normal	Icon display for an output in an off normal state.
Icon - Reader + Input Off-Normal	Icon display for a reader and input in an off normal state.
Icon - Reader + Output Off-Normal	Icon display for a reader and output in an off normal state.
Icon - Input + Output Off-Normal	Icon display for an input and output in an off normal state.
Icon - Total Alarm State	Icon display for a Logical Device in total alarm state.
Hardware Description	Identifies which description will be used for the hardware (description is specified during Logical Device configuration).

6.5.1.2 Device Types Tab

View, add, edit, or delete the template's device types on this tab:



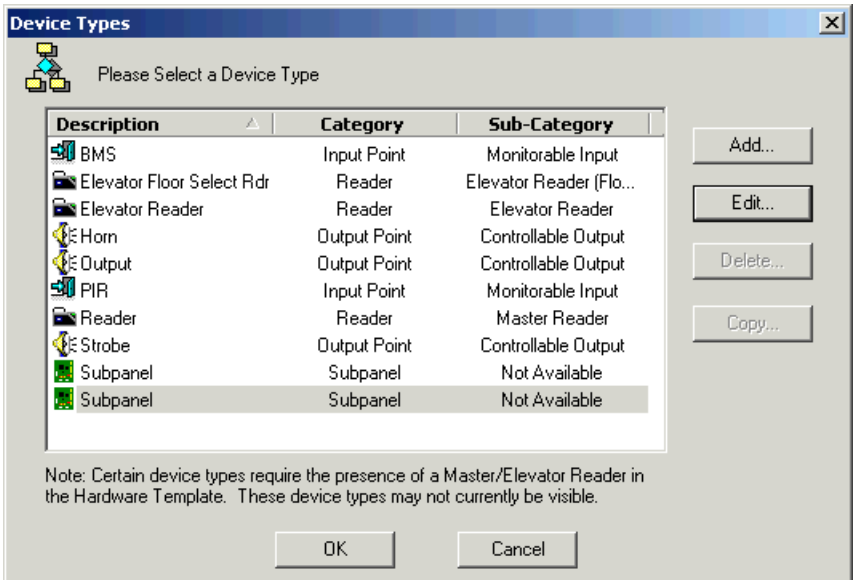
Use the following field descriptions to configure device types:

Field	Description
Balanced Magnetic Switch (BMS)	A monitorable input, which supervises the open or closed position of movable assemblies such as doors.
Door Position Switch (DPS)	An input, which is part of a door, that determines whether or not the door is open or closed.
Elevator Floor Select Reader	Elevator floor-select readers limit cardholder access and record the actual floor selected by the cardholder. **Note:** This option is not available on CHIP panels.
Elevator Input	A floor-button sensor in a floor-select elevator. There must be one elevator input for each access-controlled floor serviced by the elevator cab. **Note:** This option is not available on CHIP panels.

Field	Description
Elevator Output	On floor-select elevators, the output relays the message to an elevator controller to call the cab to a particular floor. On a non-floor-select elevator, it enables/disables the physical connection between the call button for a floor and the elevator controller. There must be one elevator output for each access-controlled floor serviced by the cab. **Note:** This option is not available on CHIP panels.
Elevator Reader	Elevator floor-select readers limit cardholder access but do not record the actual floor selected by the cardholder. **Note:** This option is not available on CHIP panels.
Horn	A controllable output, which acts as an audio alarm, if there is a forced door or similar event.
Lock	An output, which is part of a door configuration, that energizes the latch or bolt on a door so that it may physically be opened. Also referred to as a door strike.
PIR	A monitorable input, which is a passive infrared device. Can act as a REX device.
Reader	A reader is typically used in a door configuration. A reader can be part of a primary/secondary design or as a stand-alone reader.
REX Device	An input, which is part of a door configuration, that serves as a standard request-to-exit, typically on the secure side of a door.
Strobe	A controllable output, which acts as a visual alarm, if there is a forced door or similar event.
Sub Panel	A controller attached to a panel, which provides the ability to add inputs, outputs, or readers.

To add a device type to a hardware template:

1. Click **Add**. The Device Types dialog box appears.



2. Select the device type you want to add, and then click **OK**. If the device type you want does not appear in the list of device types, click **Add** on the Device Types dialog box to display the Add Device Types dialog box. For instructions on completing the Add Device Types dialog box, see "Configuring Device Types".

3. To edit a template's device type configuration, select the device type in the Device Types dialog box, and click **Edit** to display the Device Types dialog box.

   There are multiple tabs to consider when editing a device type, and the tab's field values vary according to your hardware. Field values, for example, will be different for a PW-5000 based control system than they will for a SEEP-based control system. To configure the devices to operate in your access control system, use the appropriate tab field information provided in "Adding or Editing a Device Type".

   Note: You can also configure the Device Types or Logical Devices after adding the Logical Devices to the panel. See the Logical Devices section that corresponds to your hardware.

To configure a PW-5000/Smart Card device type:

1. In the Device Types dialog box, double-click the Smart Card Reader row, or select the Smart Card Reader row and click **Edit** to display the Hardware Configuration screen.

2. Click and select the **PW-5000/Smart Card tab**.

3. Select the **Tamper Enabled** option button to enable the OmniSmart card reader tamper functionality for a PW-5000 control board.This setting will be valid for all Logical Devices that use this hardware template, but it can be changed on a reader-by-reader basis. Select the **Tamper Disabled** option button to disable this functionality.

Note: Select the **Supervision Enabled** option button to enable the OmniSmart card reader supervision functionality for a PW-5000 control board. This setting will be valid for all Logical Devices that use this hardware template, but it can be changed on a reader-by-reader basis. Select the **Supervision Disabled** option button to disable this functionality.

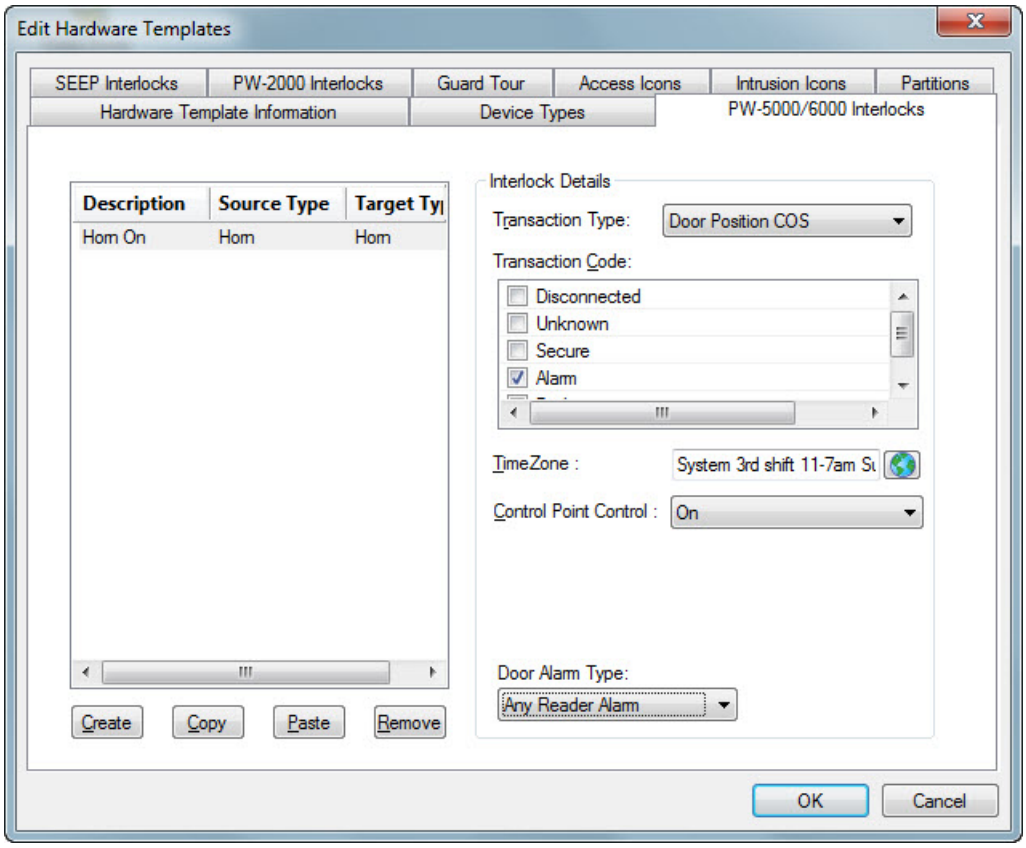
Enabling the functionality displays the **Seconds** selection box where you can select the frequency (between 0 and 127 seconds) at which the OmniSmart reader sends an 8-bit Wiegand byte message (the value of which is also programmable). The Pro-Watch host computer monitors this message and when it stops, Pro-Watch signals a problem.

4. Select the **Encryption Enabled** option button to enable the OmniSmart card reader encryption functionality for a PW-5000 control board. This setting will be valid for all Logical Devices that use this hardware template, but it can be changed on a reader-by-reader basis. Select the **Encryption Disabled** option button to disable this functionality.
5. If you have enabled the encryption function in the above step, select the **Passphrase** option button in the Master Key Settings group of variables. When you click OK, Pro-Watch automatically translates the passphrase you enter into hexadecimal code.
6. As an option, you can select the **64 Bit HEX Key** option button and then enter a hexadecimal expression in the next four alphanumeric fields.
7. Click **OK** to save all the PW-5000/Smart Card settings you have entered.

6.5.1.3 PW-5000/6000 Interlocks Tab

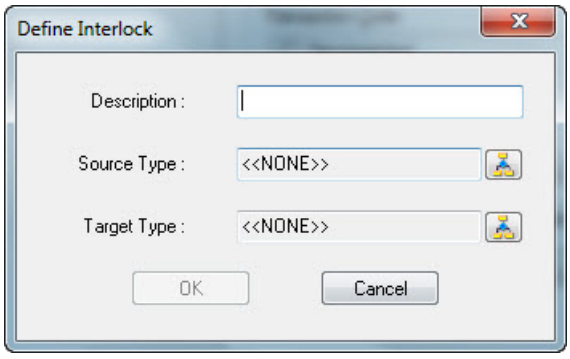
A PW-5000/6000 interlock is a defined action that occurs within a PW-5000 or PW-6000 panel at a destination device whenever an event occurs at the source device. For example, a REX input device (source) receives a request to exit and passes the order to the door strike device (destination) to open the door latch. For each interlock, you define a source and a destination device (or group of devices).

You can add, copy and paste, and remove PW-5000 or PW-6000 interlocks on this tab:



To add a PW-5000 Interlock:

1. Click **Create** to display the **Define Interlock** dialog box:



2. Enter a description that identifies the interlock.
3. Click the icon next to the **Source Type** field.
4. Select a device type from the dialog box and click **OK**.
5. Click the icon next to the **Target Type** field.

6. Select a device type from the dialog box and click **OK**.
7. Click **OK** on the Define Interlock dialog box. The interlock appears in the left list-box on the PW-5000/6000 Interlocks tab.
8. Select the interlock in the left list-box of the PW-5000 Interlocks tab and specify the transaction type, transaction code, and time zone for the interlock. Note that the Transaction Codes will vary depending on the Transaction Type chosen. Use the following field descriptions to make these selections:

Field	Description
Transaction Type	Defines the trigger type.
Transaction Code	Defines the individual attributes of the trigger.
Time Zone	Time Zone in which the created interlock will be valid.

To copy an existing interlock:

1. Select the template.
2. Click **Copy**.
3. Click **Paste**.
4. Enter a new interlock description and click **OK**.
5. Edit the interlock details as needed.

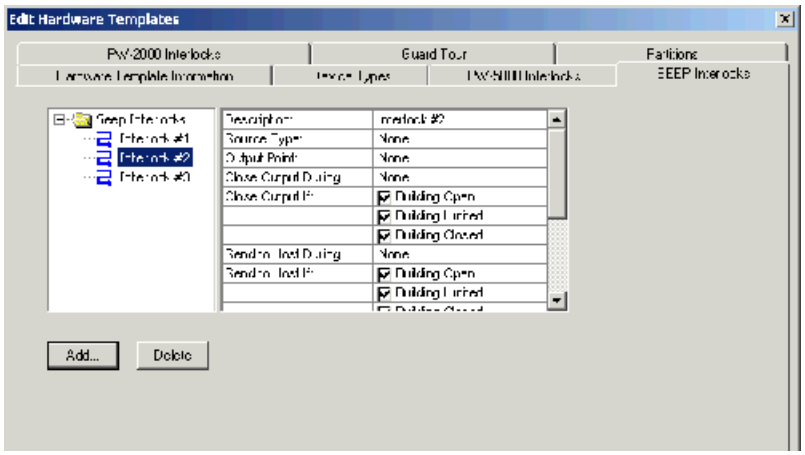
To remove an interlock from the template:

Select the interlock and then click **Remove**.

6.5.1.4 SEEP Interlocks Tab

A SEEP interlock is a defined action that occurs within a SEEP panel at a destination device whenever an event occurs at the source device. For example, a REX input device (source) receives a request to exit and passes the order to the door strike device (destination) to open the door latch. For each interlock, you define a source and a destination device.

From the SEEP Interlock tab, you can add or delete SEEP interlocks:



To add a SEEP interlock:

Click **Add** and use the following field descriptions to set its parameters:

Field	Description
Description	Provides the description of the report.
Report Type	Defines the report as system or user.
Output Point	Defines the output point for the report.
Close Output During	Defines the time zone in which the output is closed (activated) in the event the report occurs within that time zone.
Close Output If	See below.
Building Open	When enabled, when the building is open the output is closed (activated).
Building Limited	When enabled, when the building is limited the output is closed (activated).
Building Closed	When enabled, when the building is closed the output is closed (activated).
Send to Host During	Defines the time zone in which the log is sent to the host.
Send to Host If	See below.

Field	Description
Building Open	When enabled, logs are sent to the host when the building is open.
Building Limited	When enabled, logs are sent to the host when the building is limited.
Building Closed	When enabled, logs are sent to the host when the building is closed.
Close Latched During	Defines the time zone in which the output is closed (activated) and latched in the event the report occurs within that time zone.
Closed Latched If	See below.
Building Open	When enabled, when the building is open the output is closed (activated) and latched.
Building Limited	When enabled, when the building is limited the output is closed (activated) and latched.
Building Closed	When enabled, when the building is closed the output closed (activated) and latched.
Prevent Building Closure	When enabled, prevents the building from closure.
Print * with Log	When enabled, places an asterisk in front of the log comment.

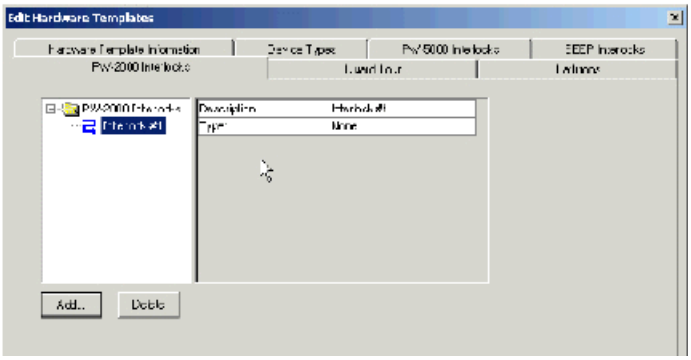
To delete a SEEP interlock:

1. Select the interlock.
2. Click **Delete**.

6.5.1.5 PW2000 Interlocks Tab

A PW2000 interlock is a defined action that occurs within a PW2000 panel at a destination device whenever an event occurs at the source device. For example, a REX input device (source) receives a request to exit and passes the order to the door strike device (destination) to open the door latch. For each interlock, you define a source and a destination device.

You can add or delete PW2000 interlocks.



To add a PW2000 interlock:

Click **Add** and use the following field definitions to set its parameters:

Field	Description
Description	The description of the interlock.
Type	Identifies the interlock type (reader, input, output, duress).

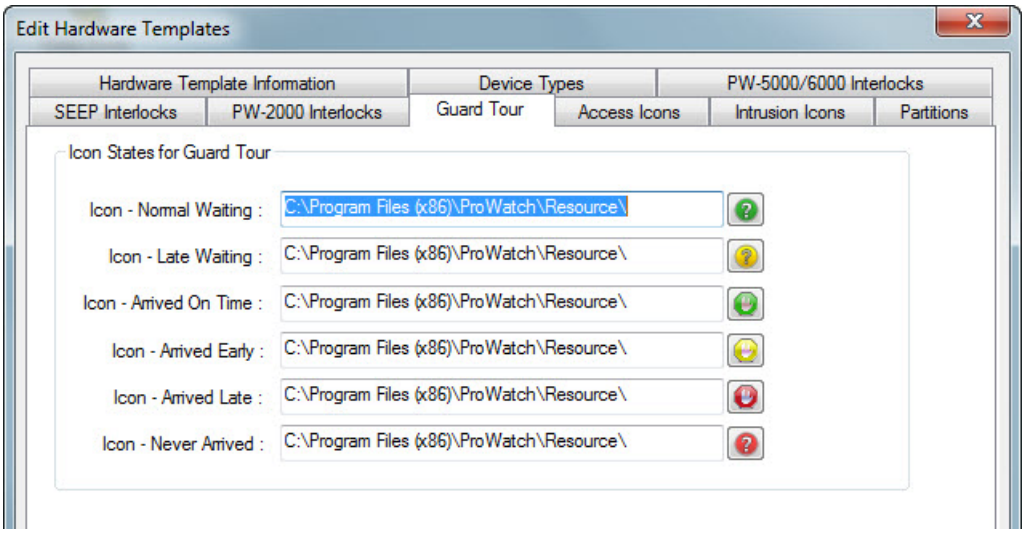
Note: Additional fields will appear upon selecting the interlock type. These fields will vary depending on the interlock type chosen.

To delete a PW2000 interlock:

1. Select the interlock.
2. Click **Delete**.

6.5.1.6 Guard Tour Tab

Use this function to create icons to represent six guard tour status labels:



- Normal waiting – guard remains within the normal waiting period.
- Late Waiting – guard has not arrived at the checkpoint during the allotted time.
- Arrived on time – guard arrives at the checkpoint at the configured time.
- Arrived early – guard arrives at the checkpoint before the defined time.
- Arrived late – guard arrives at the checkpoint after the defined time.
- Never arrived – guard never arrives at the checkpoint.

A Pro-Watch guard tour creates a facility walk-through that is defined by a series of reader checkpoints. The cardholder, or guard, walks through the facility and presents his card at predefined readers within time windows.

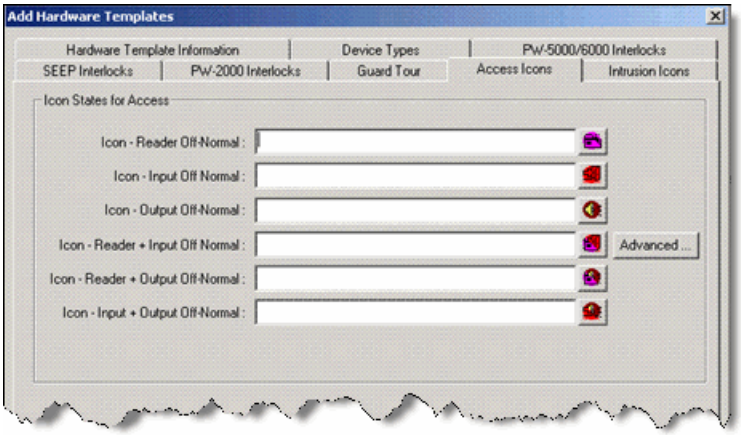
Failure to arrive at a checkpoint within the window generates notification to those who must respond.

Example: A prison warden would follow a guard tour through his cell blocks. Should he arrive early or late at a reader, an event is logged to the database and sent to operators who view this information. The event is identified by the icon you select in this tab.

To select the icons, click the icon next to each field and select the file for the icon you want.

6.5.1.7 Access Icons Tab

Use this function to indicate a status you want to assign to a file.



The following statuses are available:

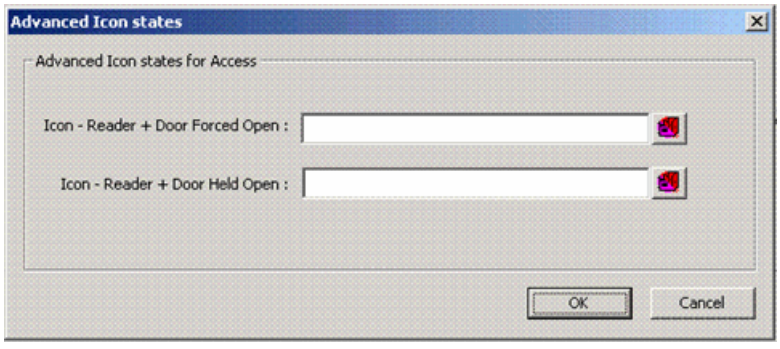
- Reader Off-Normal
- Input Off-Normal
- Output Off-Normal
- Reader + Input Off-Normal
- Reader + Output Off-Normal
- Input + Output Off-Normal

To select an icon, click the icon next to the appropriate field and select the file for the icon you want and click **OK**.

The **Advanced** button enables you to select icons that will represent two separate sub-statuses within the Icon-Reader + Input Off Normal status:

- Icon-Reader + Door Forced Open
- Icon-Reader + Door Held Open

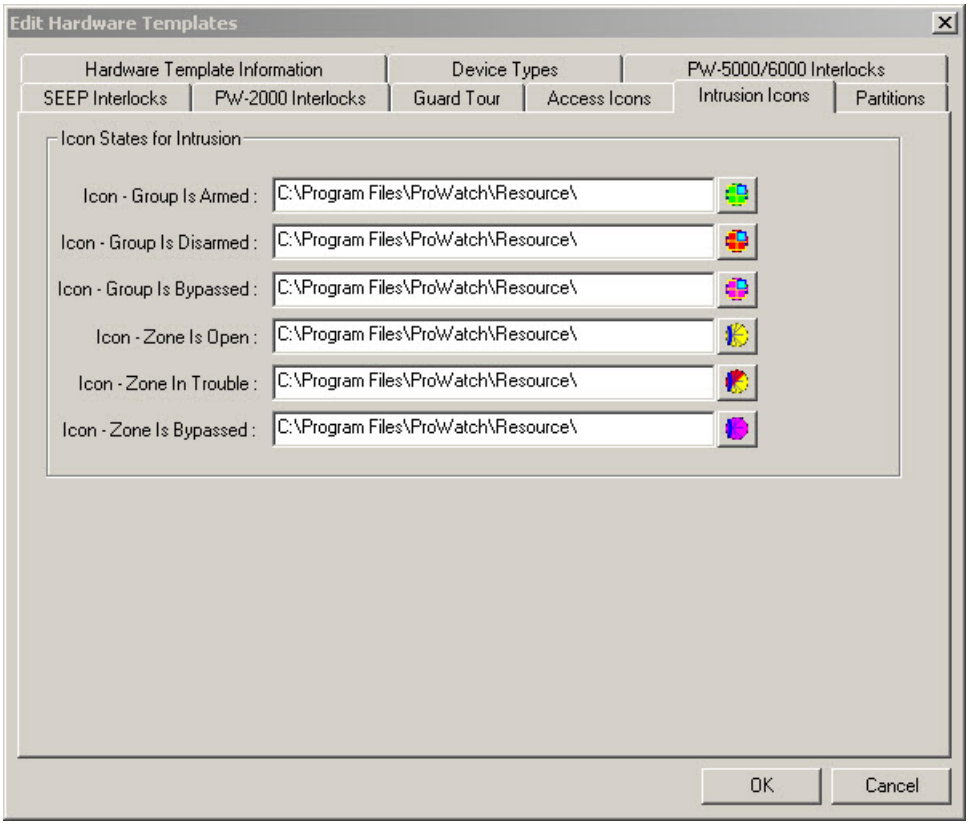
Click **Advanced** to display the Advanced Icon States dialog box.



To assign separate icons for the Door Forced Open and Door Held Open statuses, click the button next to each field and select the desired icon. Then, click **OK**.

6.5.1.8 Intrusion Icons Tab

Use this function to create icons that indicate the status of intrusion groups and intrusion zones:



The following statuses are available:

- Group is armed
- Group is disarmed
- Group is bypassed
- Zone is open
- Zone in trouble
- Zone is bypassed

To select an icon, click the icon next to the appropriate field and select the file for the icon you want and click **OK**.

6.5.1.9 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

To assign a partition to an existing hardware template:

1. Click the Partitions tab.
2. Click **Add**.
3. Select an available partition.
4. Click **OK**.

See "DBC - Partitions" in Chapter 53 for more information about defining partitions.

6.5.2 Deleting a Hardware Template

Use this function to delete a Hardware Template from the Pro-Watch database.

1. In the Pro-Watch Hardware Configuration tree list, click **Hardware Templates** to display the Hardware Template icons in the right pane.

Note: Right-click the Hardware Template you want to delete and select **Delete**.

You cannot delete a Hardware Template that has dependencies. A dependency is another database object that includes the Hardware Template in its configuration. The Hardware Template object depends upon the Logical Device object. If the Hardware Template has no current dependencies, you are prompted to confirm the deletion. However, if the Hardware Template does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Hardware Template:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Hardware Template.

6.5.3 Viewing the Dependencies of a Hardware Template

Use this function to view and modify the Hardware Template's dependencies. Hardware Template objects depend upon the Logical Device object.

To view the current dependencies for the selected Hardware Template:

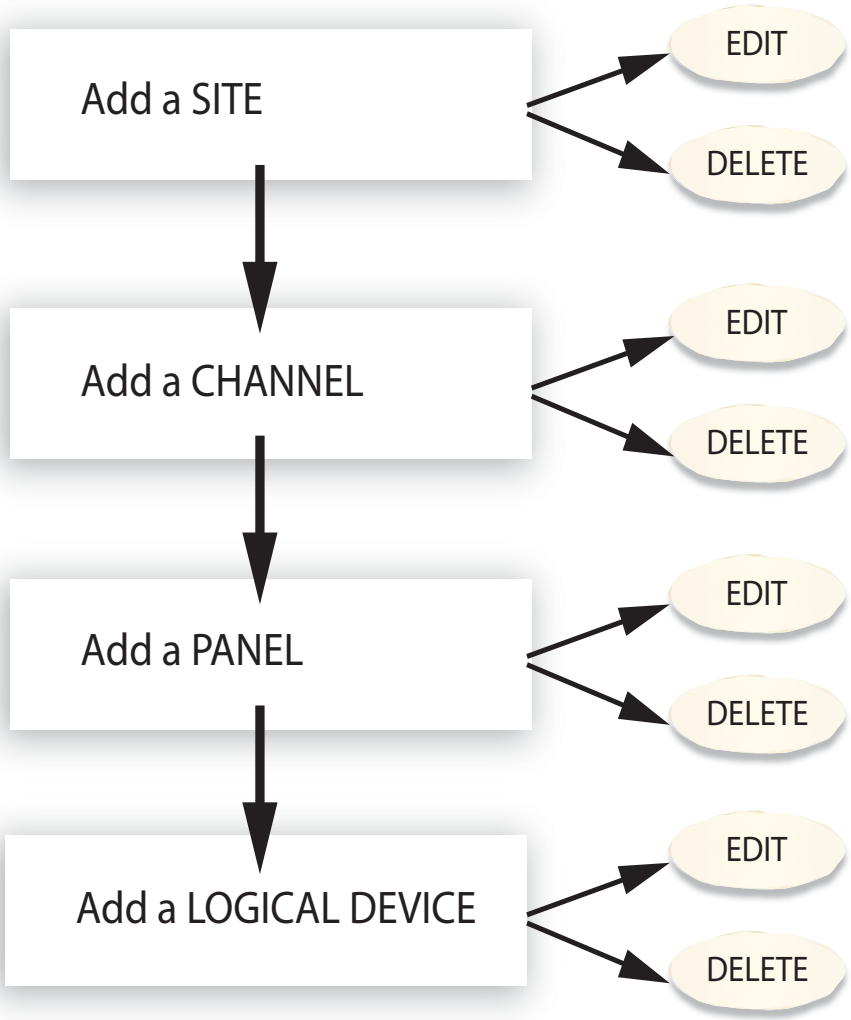
1. Right-click the icon of an existing Hardware Template in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** The Dependencies dialog box appears and lists the Hardware Template's existing dependencies.

2. To modify or remove the dependency, double-click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

6.6 Configuring The Hardware System

This section describes how to configure the hardware components as a working Pro-Watch hardware system. It includes the following tasks:

- Adding a site.
- Adding a channel.
- Adding and configuring a panel.
- Adding and configuring Logical Devices.



In addition, there are core database configuration and badging resources that need to be configured. It includes the following tasks:

- Configuring routing groups.
- Adding resources to a class.
- Adding clearance codes.
- Assigning the clearance codes to companies.
- Adding and configuring a badge.

Some of the procedures required to complete these tasks vary from panel to panel. However, all panels share the same basic procedures required to add a site, a channel, etc. Therefore we will cover such common procedures first and then provide specific procedures required by each individual panel.

6.6.1 Procedures Common to All Panels

The following procedures are common to all the panels:

1. Add a Site, page 46.
2. How to View and Edit Dependencies of a Site, page 48.
3. How to Delete a Site, page 48.
4. How to View and Edit Dependencies of a Channel, page 51.
5. How to Delete a Channel, page 51.
6. How to View and Edit Dependencies of a Panel, page 52
7. How to Delete a Panel, page 53
8. How to View and Edit Dependencies of a Logical Device, page 53.

You can proceed directly to the section written for your panel and refer back to the common procedures to refresh your memory.

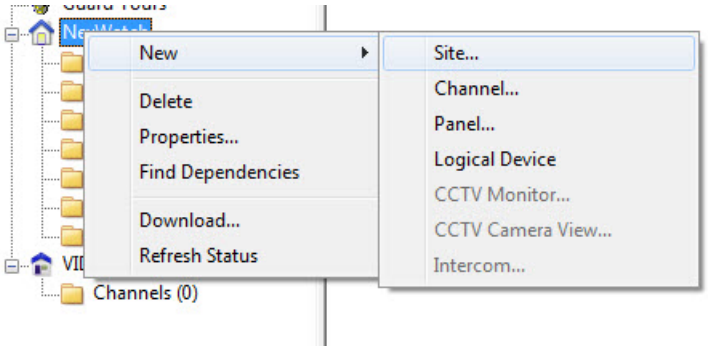
Here are the individual panel chapters:

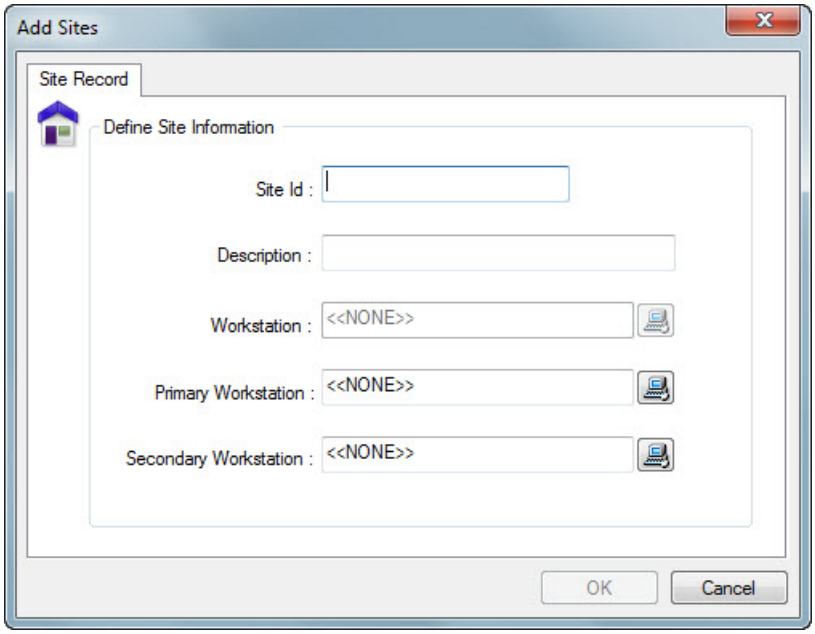
- Chapter 7, *HW Config - PW2000*
- Chapter 8, *HW Config - PW-5000/PW-6000/PW-6K1ICE Channel Type*
- Chapter 9, *HW Config - Cardkey*
- Chapter 10, *HW Config - CHIP*
- Chapter 11, *HW Config - Galaxy*
- Chapter 11, *HW Config - Matrix*
- Chapter 13, *HW Config - SEEP*
- Chapter 14, *HW Config - SmartPlus Mobile*
- Chapter 15, *HW Config - Vindicator V5*
- Chapter 16, *HW Config - VISTA*
- Chapter 17, *HW Config - Generic Channels*

6.6.2 Add a Site

A Pro-Watch site refers to the area of controlled access. For example, a site could be an airport terminal. You must create a site before you create a channel, panel, subpanel, and logical device.

1. From the Hardware Configuration tree view, right-click and select **New > Site** to display the **Add Sites** dialog box:





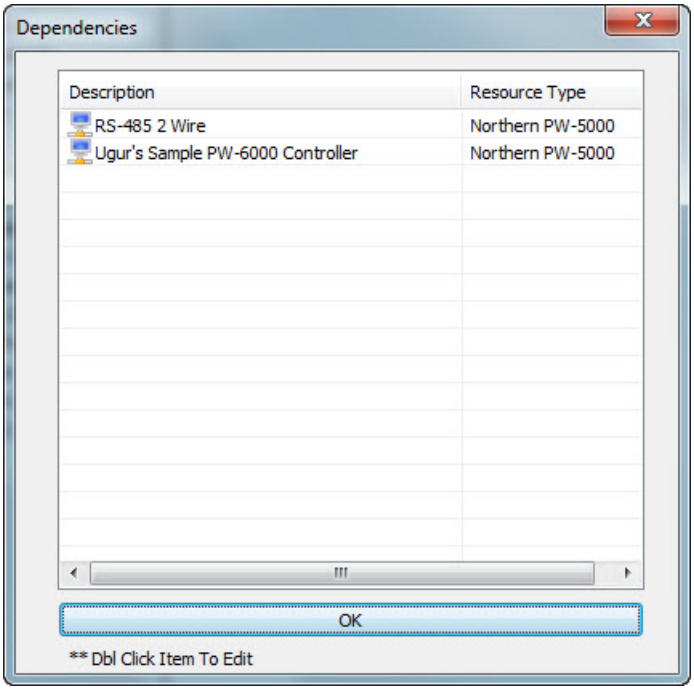
2. Enter a **Site ID**, a unique name that identifies the site. You cannot have duplicate Site IDs.
3. Enter a **Description** of the site.
4. Click the icon next to the **Workstation** field and select the workstation that will poll the panel on this site.
5. Click the icon next to the **Primary Workstation** field and select the primary workstation that will poll the panel on this site.
6. Click the icon next to the **Secondary Workstation** field and select the secondary workstation that will poll the panel on this site.
7. Click **OK**. The new site appears in the tree view in the Pro-Watch Hardware Configuration window.

Note: When you create a new site, Pro-Watch by default creates **an empty Channels directory** under the new site.

6.6.3 How to View and Edit Dependencies of a Site

Follow these steps to view and edit a Site's dependencies:

1. Right-click the **icon** of an existing Site in the navigation page and select **Find Dependencies** from the pop-up menu to display the **Dependencies** dialog box:



2. To edit or delete the dependency, **double-click** the specific dependency in the list to display its **Edit** dialog box.
3. After you finish editing and viewing, click **OK** to close the dialog box.

6.6.4 How to Delete a Site

Warning: Deleting a site will also delete all the Points and Resources that belong to the site.

Follow these steps to delete a Site from the Pro-Watch database:

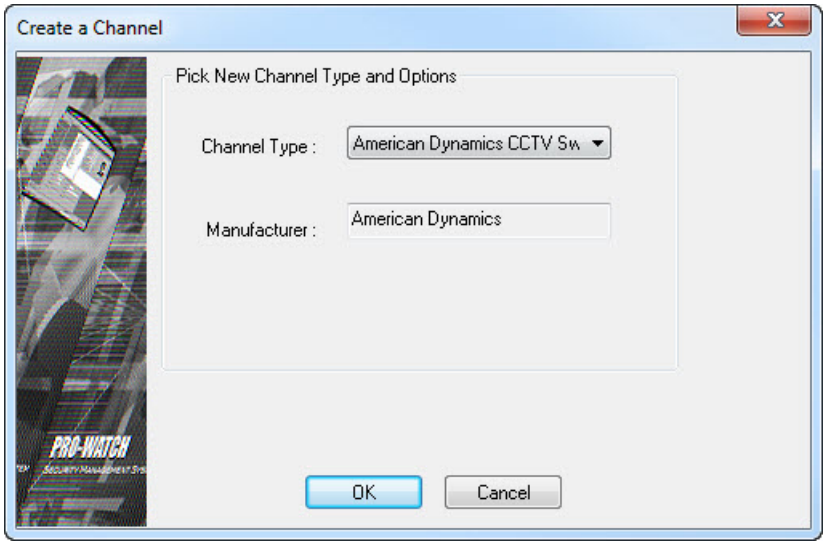
1. Right-click the **icon** of an existing Site in the navigation page and select **Delete** from the pop-up menu. If there are live references to the site, Pro-Watch will display an error message and decline to delete the site. You have to remove all the references to the site before you can delete it.

2. Click **Yes** to delete site.

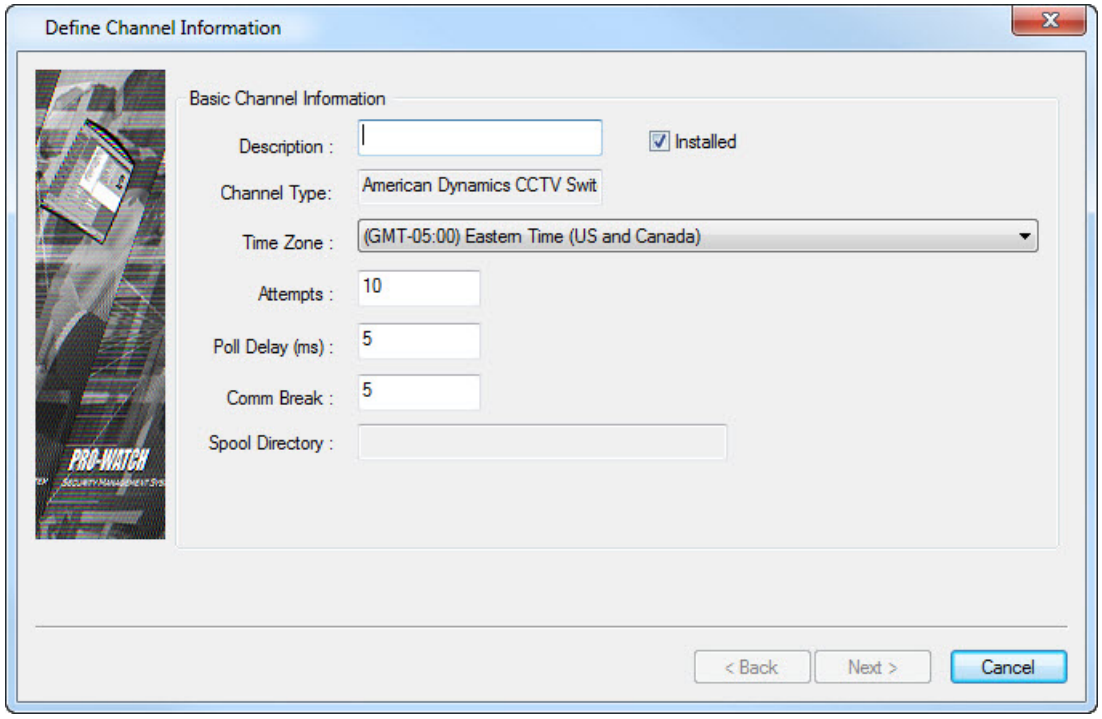
6.6.5 How to Add a Channel

You must create a site before you create a channel, panel, subpanel, and logical device.

1. From the Hardware Configuration tree view, right-click a site and select **New > Channel** to display the **Create a Channel** dialog box:



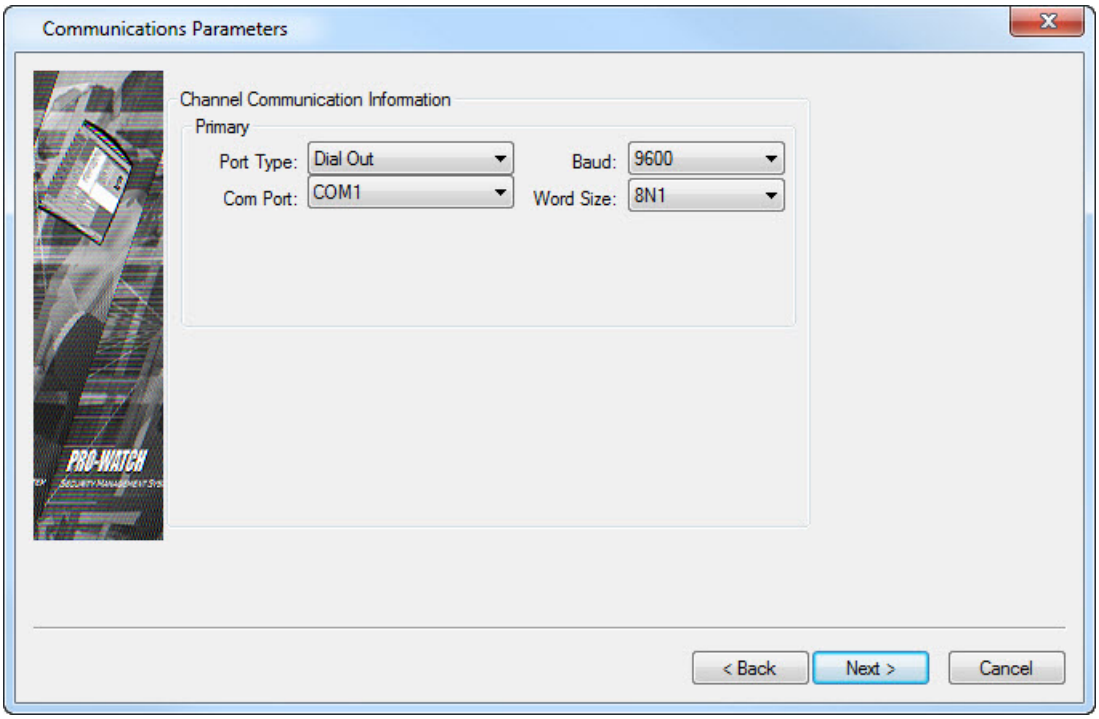
2. Select a **Channel Type** and click **OK** to display the **Define Channel Information** dialog box:



3. Enter a **Description** for the channel. Select an appropriate **Time Zone** from the drop-down list. Also enter the appropriate values for **Attempts**, **Poll Delay**, **Comm Break** and **Spool Directory** (if any) fields.

Note: The **Installed** check-box is selected by default when you create a channel. But if for some reason you'd like to cancel the panel that the channel is assigned to, then clear the **Installed** check-box. This may be necessary for example when you are setting up a Pro-Watch site with a lot of panels and do not want to be bothered with system or temporary error messages until the whole system configuration is finished. Once the system is configured you can go back and select the **Install** check-box to turn on the panel. Canceling the panel by clearing this check-box will also cancel all the sub-panels and downstream devices attached to the panel.

4. Click **Next** to display the **Communications Parameters** dialog box:



5. Select the appropriate values for the **Port Type, Com Port**, **Baud**. and **Word Size** fields through their respective drop-down lists.
6. Click **Next** to display the **Partitions** screen. Add any partitions you like by clicking the **Add** button.
7. Click **Finish** when you are done to create the new channel.

6.6.6 How to View and Edit Dependencies of a Channel

Follow these steps to view and modify the Channel's dependencies. The Channel object depends upon the Site and Routing Group objects.

1. Right-click the icon of an existing Channel in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The **Dependencies** dialog box appears and lists the Channel's dependencies.
2. To edit or delete the dependency, **double-click** the specific dependency in the list to display its **Edit** dialog box.
3. After you finish editing and viewing, click **OK** to close the dialog box.

6.6.7 How to Delete a Channel

Follow these steps to delete a Channel from the Pro-Watch database:

1. In the Pro-Watch Hardware Configuration tree list, click **Channels** to display the Channel icons in the right pane.
2. Right-click the Channel you want to delete and select **Delete**. Note that you cannot delete a Channel that has dependencies. A dependency is another database object that includes the Channel in its configuration. The Channel object depends upon the Site and Routing Group objects. If the Channel has no current dependencies, you are prompted to confirm the deletion. However, if the Channel does have current dependencies, the Dependencies dialog box appears.
3. If you still want to delete the Channel:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
4. Repeat step 2 and click **Yes** at the prompt to delete the Channel.

6.6.8 How to Add a Panel

1. From the Hardware Configuration tree view, right-click a channel and select **New > Panel** to display the **Pro-Watch Control Manager** dialog box.
2. Enter a **Controller Description** for the new panel. Select the appropriate **Site** from its respective drop-down list. If dynamically displayed, also select a **Controller Type** from its drop-down menu.
3. Click **Next** to display the **Downstream Board** screen. Select one or more downstream board.
4. Click **Finish** to create the new panel.

6.6.9 How to View and Edit Dependencies of a Panel

Follow these steps to view and modify the Panel's dependencies. The Panel object depends upon the Channel object.

1. Right-click the icon of an existing Panel in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The **Dependencies** dialog box appears and lists the Channel's dependencies.
2. To edit or delete the dependency, **double-click** the specific dependency in the list to display its **Edit** dialog box.

3. After you finish editing and viewing, click **OK** to close the dialog box.

6.6.10 How to Delete a Panel

Follow these steps to delete a Panel from the Pro-Watch database:

1. In the Pro-Watch Hardware Configuration tree list, click **Panels** to display the Panel icons in the right pane.
2. Right-click the Panel you want to delete and select **Delete**. Note that you cannot delete a Panel that has dependencies. A dependency is another database object that includes the Panel in its configuration. The Panel object depends upon the Channel object. If the Panel has no current dependencies, you are prompted to confirm the deletion. However, if the Panel does have current dependencies, the Dependencies dialog box appears.
3. If you still want to delete the Channel:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.

Repeat step 2 and click **Yes** at the prompt to delete the Panel.

6.6.11 How to View and Edit Dependencies of a Logical Device

Follow these steps to view and edit a Logical Device's dependencies:

1. Right-click the **icon** of an existing Logical Device in the navigation page and select **Find Dependencies** from the pop-up menu to display the **Dependencies** dialog box.
2. To edit or delete the dependency, **double-click** the specific dependency in the list to display its **Edit** dialog box.
3. After you finish editing and viewing, click **OK** to close the dialog box.

6.6.12 How to Delete a Logical Device

Follow these steps to delete a Logical Device from the Pro-Watch database:

1. Right-click the **icon** of an existing Logical Device in the navigation page and select **Delete** from the pop-up menu. If there are live references to the site, Pro-Watch will display an error message and decline to delete the logical device. You have to remove all the references to the logical device before you can delete it.
2. Click **Yes** to delete the Logical Device.

6.6.13 Editing Daylight Savings Time (DST) Zone

6.6.13.1 The Problem

Sometimes the system may not reflect the correct Daylight Savings Time (DST) for one of the two reasons:

1. Software has been upgraded but the technician did not Initialize and download the System and the Cards after the upgrade. An outdated GTZ table conflicts with current year DST.
2. Different calendar years can mean a different Daylight Savings Time schedule based on local and state governments' planning.

6.6.13.2 The Solutions

1. Perform a controller Initialize, and then a System and Card download together. If the issue is resolved no further action is needed.
2. If the issue persists and server time and channel timezone are correct, then run the executable file (**ValidateTZ.exe**) that you can find in the Utilities folder of the distribution disk (DISK 2).
3. Once the executable completes successfully, perform a controller Initialize then Download System and Cards

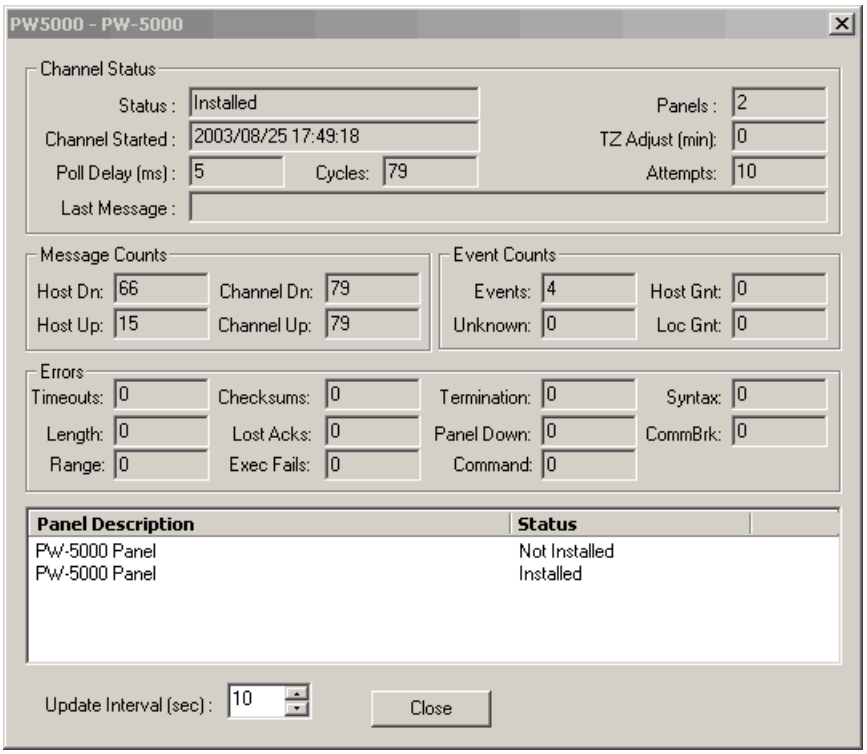
6.7 Status

Pro-Watch allows the user to check channel as well as panel status.

6.7.1 Channel Status

To view channel status:

1. Select the channel and right-click.
2. Select **Status**. The Channel Status dialog box displays information regarding the channel and any panels attached to the channel, including any transactions that may have of occurred.



3. Click **Close** once you have completed examining the channel status.

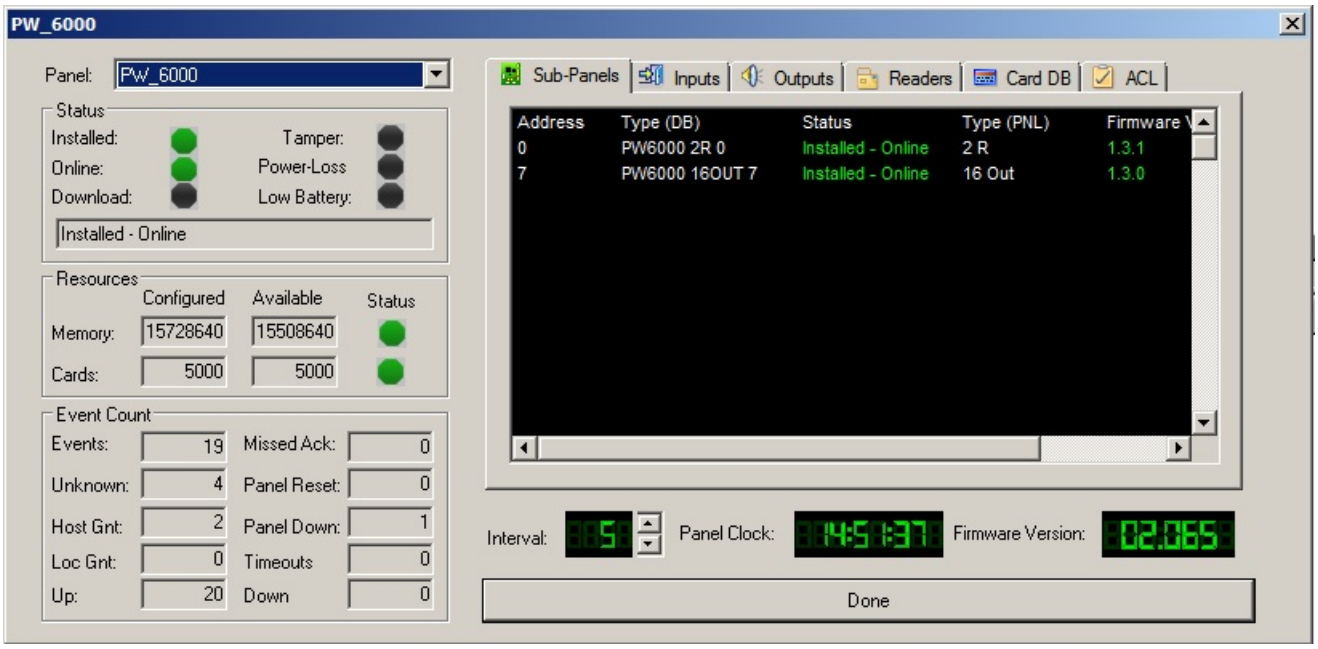
6.7.2 Panel Status

To view panel status (or Status Monitor):

1. Select the panel and right-click.
2. Select **Status**. The Panel Status dialog box appears. The Status Monitor allows you to view the status of the panel, sub-panels, and

Logical Devices in real-time. For some panel types, the dialog box also displays the **Firmware Version**.

Note: In addition, the **Subpanel tabs** of **PW-3000, PW-5000, PW-6000** and **Mercury** panels also display **subpanel firmwave versions** (see the screenshot below).
You can use the encrypted (E) version of firmware for both encrypted and nonencrypted communication.



3. Select the panel you want to view from the panel drop-down list. The panel status information automatically refreshes.The panel status dialog box shows when there is a download occurring, any alarm states such as Tamper, Power-Loss, and Low Battery, as well as the number of specific events that have occurred. If there are multiple panels attached to the channel, you may select each panel to view the status.
4. Select the applicable tab. Each Logical Device tab displays the status of each Logical Device.
5. The PW6K1ICE panels report additional status information. To view the PW6K1ICE reporting status, click the **Card DB** tab. The table below summarizes the PW6K1ICE panel reporting capabilities.

Parameter	Value
Number of Card Holders	Reports the number of cardholders the panel will support.

Parameter	Value
Number of ALVL per Card	Reports the number of access levels allowed per card. Note that a Clearance Code is correlated with an access level; therefore, you can set only 12 Clearance Codes per Card.
Number of PIN Digits	Reports the number of PIN digits the panel will support.
Issue Code	Reports the issue code.
Store Anti-passback location	Reports whether anti-passback locations are supported.
Store Activation Date	Reports whether the activation date is stored.
Store Deactivation Date	Reports whether the deactivation date is stored.
Store Vacation Date	Reports whether the vacation date is stored.
Store Temp ALVL Upgrade Date	Reports whether the temporary access level upgrade date is stored.
Store User Level	Reports whether the user level is stored. Note that this field corresponds to the Store Event Level check box on the panel tab.
Store Use Limit	Reports whether the use limit is stored.
Store Time of Last Entry	Reports whether the time of last entry is stored.
Precision Acc: Number of ACR to Save TZ	Reports the number of door time zones that is saved per card.
Enable Precision Access	Reports whether precision access is enabled.

Note: To refresh the panel reporting information, click **Card DB Info**. Note that the PW6K1ICE panel also reports access level status. To view which access levels are downloaded to the panel, click the **ACL** tab. To refresh the access level information, click **ACL Info**. The ACL Info list includes the Clearance Codes that are assigned to the Logical Devices configured for the panel. There can be a maximum of 128 (0-127) access levels (Clearance Codes) for a PW-5000 panel. ACL=0 is the default level and provides all access.

Within the status monitor, you can also perform hardware actions for output and input points.

To initiate a hardware action for an output point:

1. Click the **Outputs** tab.
2. Select an output point. Note the output point must be a member of a Logical Device.
3. Click **Activate**, **Deactivate**, or **Pulse**. To refresh click **Output Info**.

To initiate a hardware action for an input point:

1. Click the **Inputs** tab.
2. Select an input point. Note the input point must be a member of a Logical Device
3. Click **Mask** to mask the action on the monitor, or **Unmask** to display the action on the monitor. To refresh, click **Input Info**.

To initiate a hardware action for a reader:

1. Click the **Readers** tab.
2. Select an reader. Note the reader must be a member of a Logical Device
3. Click **Re-enable**, **Lock**, or **Unlock**.To refresh, click **ACR Info**.

When you have completed viewing the status monitor, click **Done**.

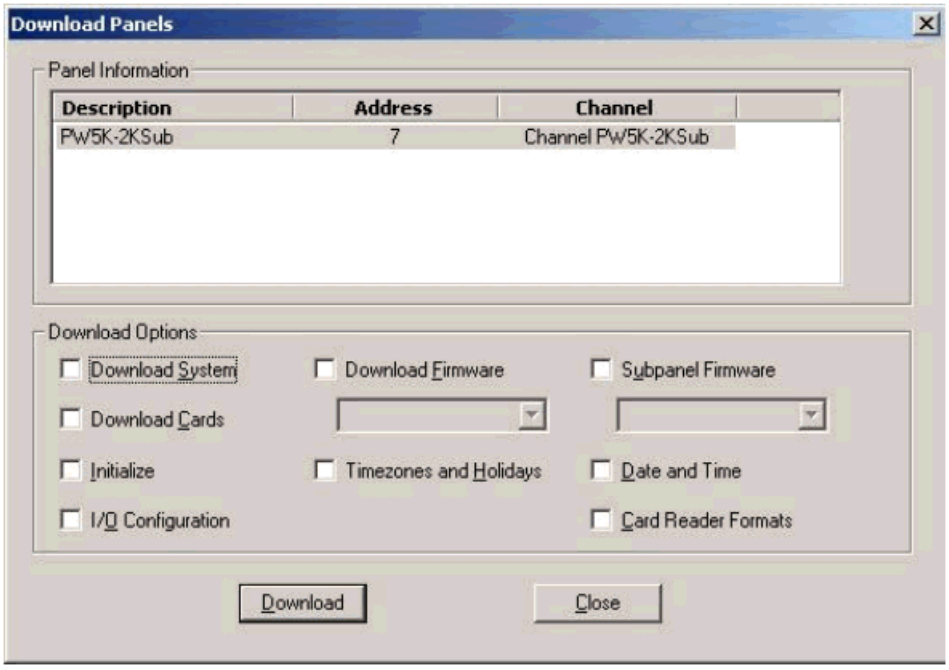
6.8 Panel Download

Pro-Watch allows the user to initialize and download the panel or particular resources to the panel.

Note: If you are downloading PW-3000 firmware to configure a panel for the Pro-Watch biometric hand geometry reader, use the downloading procedures given in Chapter 62, *Biometric Reader Configuration*.

Follow these steps:

1. Select the panel and right-click.
2. Select **Download**.



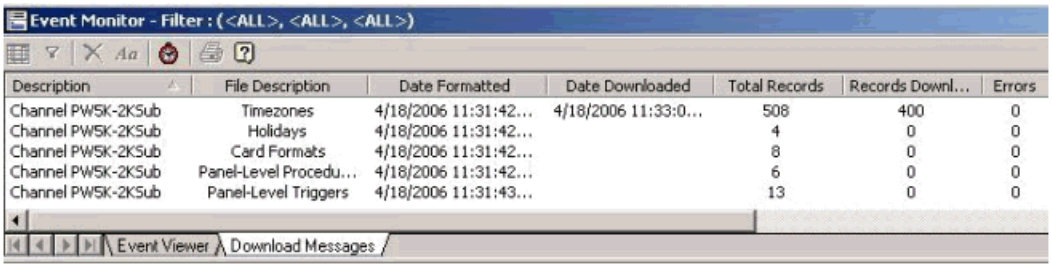
The following table describes the function of each check box:

Field	Description
Download System	Downloads everything to the panel except cards.
Download Cards	Downloads cards to the panel.
Initialize	Erases the panel's memory (PW2000); erases the cards from the panel. (PW6K1ICE and Cardkey).
I/O Configuration	Downloads the I/O configuration to the panel.
Download Firmware	Downloads the firmware of the panel (PW6K1ICE).

Field	Description
Timezones and Holidays	Downloads time zones and holidays to the panel.
Subpanel Firmware	Downloads the sub-panel's firmware to the panel (PW6K1ICE). Does not include PW2000 as a sub-panel.
Card Reader Formats	Downloads card reader formats to the panel.
Date and Time	Downloads the date and time to the panel.

3. Select the check boxes in which you want to download to the panel and click **Download** to accept the changes to the panel. Although this changes the panel's properties, you must still re-initialize and download the panel manually.
4. Click **Panels** under the appropriate Site folder in the Hardware Configuration tree to display the panel icon.
5. Right-click the panel's icon and select **Download**.
6. De-select **Download System**.
7. Select **Initialize**.
8. Click **Download** to re-initialize the panel. Note that this step only re-initializes the panel.
9. When the panel icon re-appears, right-click the icon and select **Download**.
10. Select **Download System** and **Download Cards**.

For more information on downloading panels, see "Panel Download". You can monitor the downloading status in the Download Messages tab in the Event Monitor, as shown below:



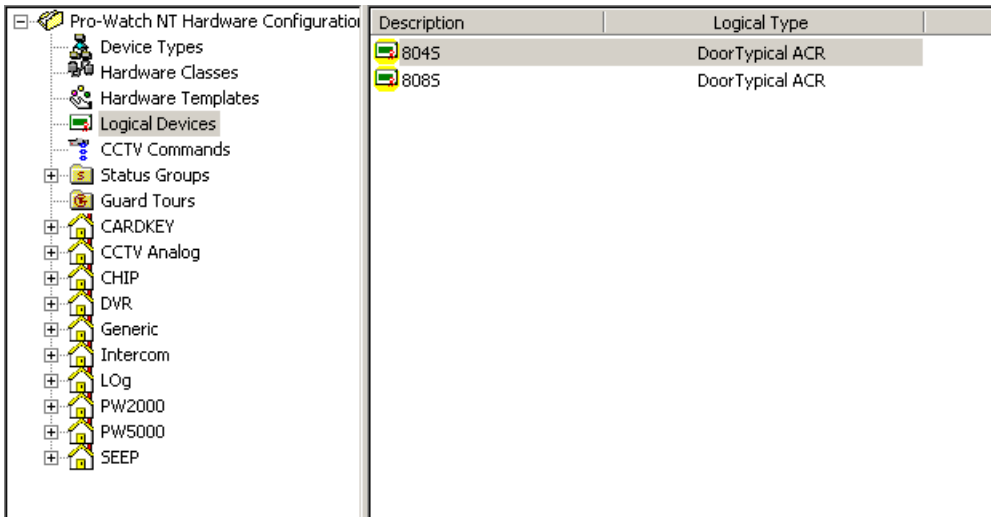
6.9 Logical Device Icon

The Logical Device Icon within the Hardware Configuration tree view contains a grouping of Logical Devices that are configured for the Verification Window. See Appendix A, Secure Mode Verification.

You can assign an unlimited number of Logical Devices to a workstation for the purposes of the Verification window. See "DBC - Workstations" in Chapter 59.

The purpose of the Logical Device Icon is to group the Logical Devices per workstation and see the Logical Devices within the Verification Window (See Appendix A, Secure Mode Verification). These Logical Devices are grouped by workstation; therefore, if you log in on a different workstation, an alternate group of Logical Devices might be viewed.

Note: You cannot delete a Logical Device from the Logical Device Icon; however, you can initiate applicable "HW Config - Hardware Actions". For more information, see "HW Config - Hardware Actions".

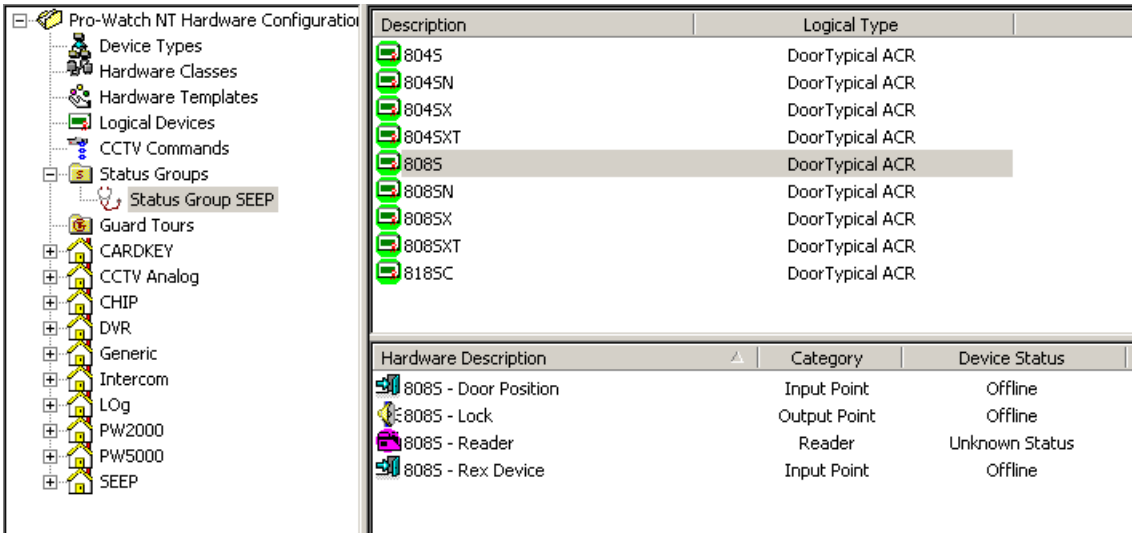


6.10 Status Groups

Status Groups allow you to organize Logical Devices and view the status of each device type within the Logical Device. Hardware Actions can be initiated from the Logical Devices grouped within Status Groups. See "HW Config - Hardware Actions".

Status Groups are configured within Database Configuration. See "DBC - Status Groups" in Chapter 56. After they are configured, status groups are displayed the Hardware Configuration component of Pro-Watch. You can select and expand a status group subdirectory within the Hardware Configuration tree view to display a list of the groups.

Select the Status Group that corresponds to the Logical Devices you want to view. The Logical Devices are displayed in the Hardware Configuration window, within the upper pane. The device types are displayed within the lower pane.



6.11 Guard Tours

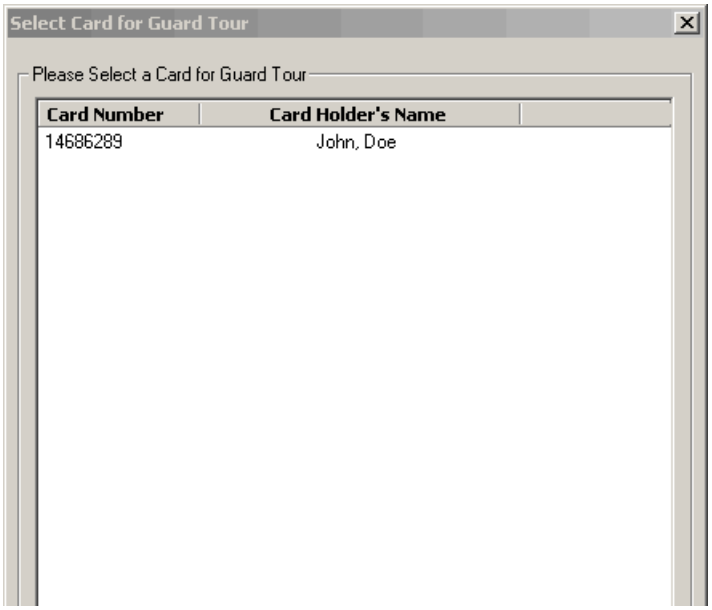
A Pro-Watch guard tour creates a facility walk-through that is defined by a series of reader checkpoints. The cardholder, or guard, walks through the facility and presents his card at predefined readers within time windows. Failure to arrive at a checkpoint within the window generates notification to those who must respond.

Guard Tours are configured within Database Configuration. See "DBC - Guard Tours" in Chapter 48. Once Guard Tours are configured, they are displayed within Hardware Configuration.

6.11.1 Adding a Guard Tour

Follow these steps:

1. Select and expand the Guard Tours' subdirectory. A list of Guard Tours appears. Select the Guard Tour you want to initiate and right-click.
2. Select **Start Guard Tour**. The Select Card for Guard Tour dialog box appear. This dialog box contains a list of cards that are applicable to participate in Guard Tours.



3. Select the appropriate card number and click **OK.**

The Logical Devices (or check points) that are assigned to the Guard Tour enable and appear as the "Normal Waiting" status icon. See "Adding or Editing a Hardware Template". These Logical Devices appear in the Hardware Configuration window. From the toolbar, select **View** > **Details**. This allows you to see specific details for the active Guard Tour.

These details include:

- Card Number – card number of the cardholder or guard.
- Start Time – start time of the Guard Tour.
- End Time – end time of the guard tour. This information does not appear until the guard tour ends. The guard tour may end by two methods, by right-clicking the guard tour from the Hardware Configuration tree view and selecting **Stop Guard Tour**, or by the guard completing the guard tour.
- Earliest Arrival Time – earliest time the guard may arrive at the checkpoint, as set by the tolerance, before an alarm is reported.
- Latest Arrival Time – latest time the guard may arrive at the checkpoint, as set by tolerance, before an alarm is reported.
- Arrived Time – actual arrival time of the guard at each checkpoint. This information is displayed once the guard presents the card at the reader.
- Current Status – current status of the checkpoint. This information changes as the guard tour progresses. For status definitions, see "Configuring Hardware Templates".

You may also edit a guard tour from within Hardware Configuration.

6.11.2 Editing a Guard Tour

Follow these steps:

1. Select and expand the Guard Tours' subdirectory in the Hardware Configuration tree view.
2. Right-click the guard tour you want to edit and select **Properties**.

The Edit Guard Tours dialog box appears. For more information, see "DBC - Guard Tours" in Chapter 48.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config – PW2000

7

In this chapter ...

Overview
Adding a PW2000 Channel
Viewing and Editing Dependencies of a PW2000 Channel
Deleting a PW2000 Channel
Adding a PW2000 Panel
Configuring PW2000 Panel Tabs
Editing a PW2000 Panel
Viewing and Editing Dependencies of a PW2000 Panel
Deleting a PW2000 Panel
Adding a PW2000 Logical Device
Editing a PW2000 Logical Device
Viewing and Editing Dependencies of a PW2000 Logical Device
Deleting a PW2000 Logical Device

7.1 Overview

Caution: The PW2000 panel is not supported in Pro-Watch Lite.

This chapter explains how to configure a site using PW2000 panel.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

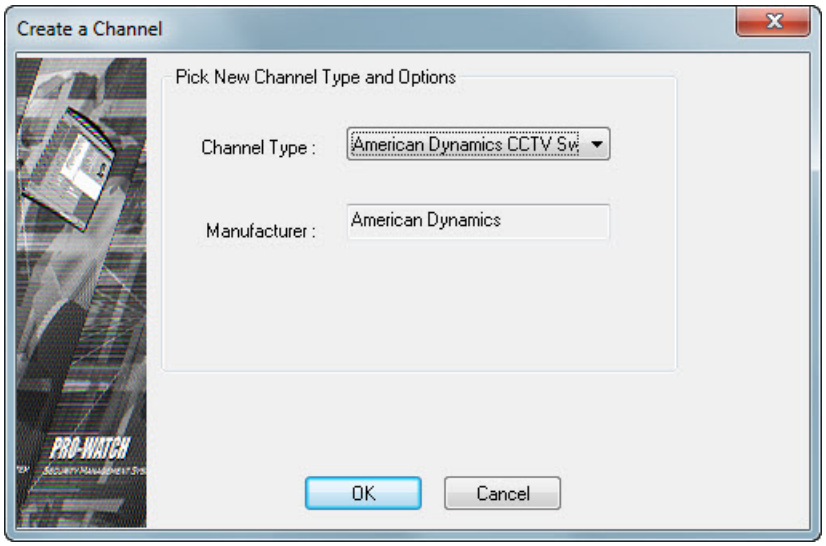
7.2 Adding a PW2000 Channel

A Pro-Watch channel is the communications path between the Pro-Watch server and the panel. You must identify the channel before adding a Panel and Logical Device.

Note: The recommended maximum number of channels per site is 99.

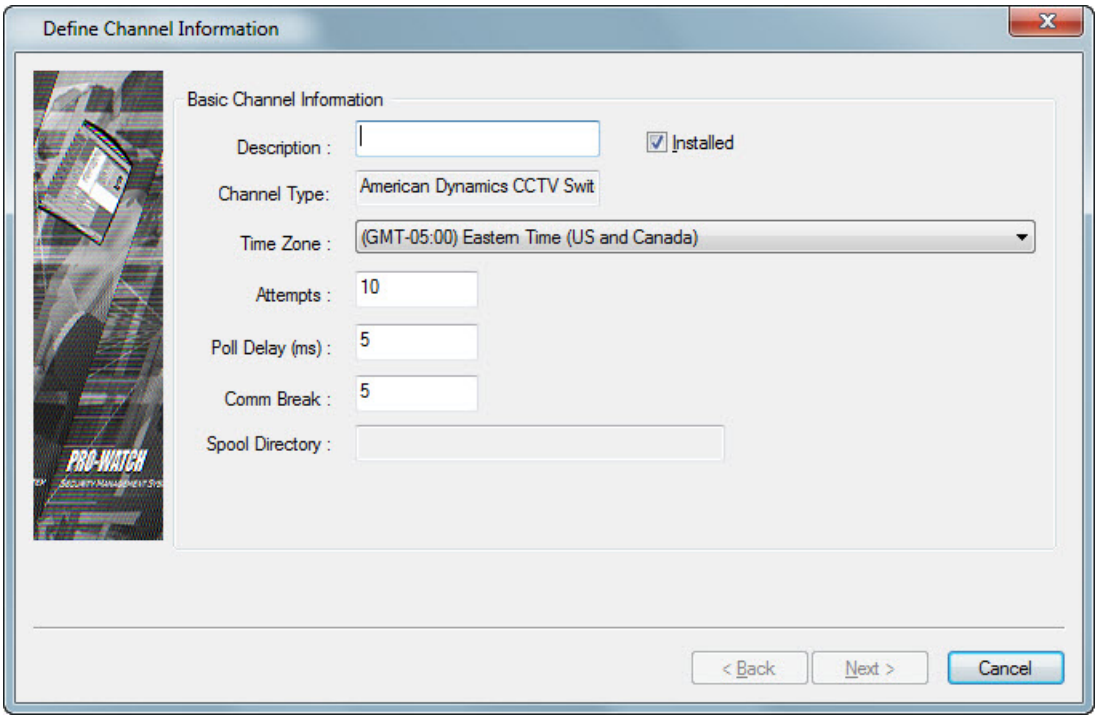
To add a channel:

1. Select a Channel Type.
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel** to display **t**he **Create a Channel** dialog box:



   b. Select a **Channel Type** specific to your hardware manufacturer from the drop-down list.
   c. Click **OK** to display the **Define Channel Information** dialog box.
2. Define the Channel.

a. In the **Define Channel Information** dialog box, enter an identifying channel **Description**:



b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.

c. From the **Time Zone** drop-down list, select the time zone that is appropriate for your site's geographic location.

d. In the **Attempts** field, enter the maximum number of times the Pro-Watch server will poll a panel before determining a panel timeout.

e. Ignore the **Poll Delay** field. The polling delay for a PW2000 configuration is not user-defined.

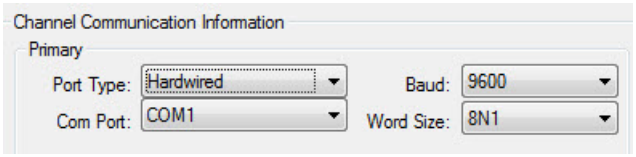
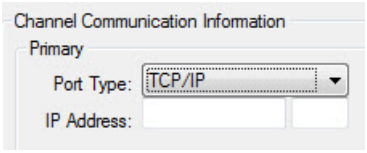
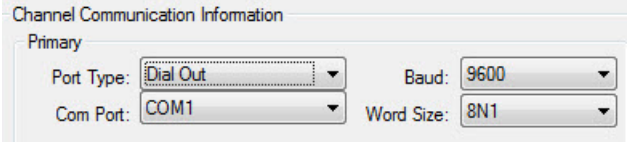
f. In the **Comm Break** field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.

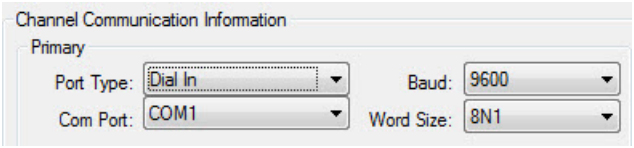
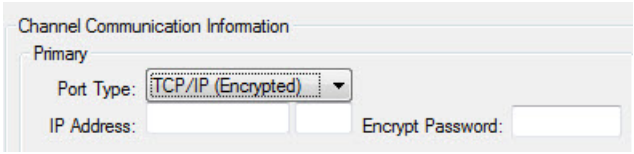
g. The communications **Spool Directory** is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.

h. Click **Next** to display the **Communications Parameters** dialog box.

3. Set Communications Parameters.

a. Select the **Port Type** from the following drop-down list options to dynamically display (if any) associated drop-down sub-options:

Option	Comments
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel. Word Size – First character is the number of data bits. The second character is the parity indicator (N = no parity, E = even parity, O = odd parity). The third character is the number of "stop" bits. 
TCP/IP	Specifies that the channel is a network connection. IP Address – the IP address of the panel. 
Dial Out	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel. Word Size – First character is the number of data bits. The second character is the parity indicator (N = no parity, E = even parity, O = odd parity). The third character is the number of "stop" bits. 

Option	Comments
Dial In	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel. Word Size – First character is the number of data bits. The second character is the parity indicator (N = no parity, E = even parity, O = odd parity). The third character is the number of "stop" bits. 
TCP/IP (Encrypted)	This functionality is provided by the network connection hardware. “TCP/IP encrypted” encrypts messages between the host and the panel. IP Address – the IP address of the panel. Encrypt Password – the password assigned. 
Modem Pools	Modem pools are used for dial out. Model Pool – collection of modems. Baud – the rate of communication between the host and the panel. Flow Control – starts and stops the transmission between the host and the panel.

b. Click **Next** to display the **Channel Dialup** dialog box. When selecting dial-up communication parameters, you must complete the settings within the channel dial-up dialog box. Please see Appendix C, Dial-Up Configuration for more information on configuring dial-up for the PW2000 panel.

Field	Description
Dialup Schedule	Determines how often you want to call the panel. Dial-up Schedules are configured in Database Configuration. See "DBC - Dial-Up Schedule" in Chapter 42 for more information.
Password	The password of the remote ‘hub’ unit.

Field	Description
Remote Site Phone Number	Defines the phone number for the remote site to establish a connection to the PCI.
Host Phone Number	Defines the phone number for the host site.
Phone Host After # of Events	Initiates dial-up after a specified number of events have occurred.
Serial Number	Automatically populated; it is used for the panel driver's identification scheme.
Dialup Retries	Defines the number of times the host attempts to dial up.
Site ID	Determined by the PCI upon calling the host. This site ID tells Pro-Watch which PCI is calling. The site ID must follow the format A0xxx,S0xxx where xxx may be any value between 1-999.
Forcibly Disconnect After (minutes)	Defines the amount of time in minutes until the connection is forced to disconnect.
Disconnect After (sec)	Defines the amount of time of inactivity that can pass before disconnect.
Delay Connect Time	Defines the delay time before the PCI attempts to dial another connection.
Delay Retry Time	Defines the number of times the PCI attempts to re-connect. Zero sets the PCI to attempt re-connects indefinitely.
Prefix	Determined by the PCI, the prefix is sent to the modem to get its attention.
Modem Init String	Defines the initialization string the PCI should use to initialize the modem.

c. Click **Next** to display the Partitions dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.

d. Click **Finish** to complete the channel. A warning message appears reminding you that you must add the channel to the appropriate routing group before you can view any events using the channel. It is recommended that you assign the channel to a routing group after you plan and configure routing groups. See "DBC - Routing Groups" in Chapter 55.

7.3 Viewing and Editing Dependencies of a PW2000 Channel

Please refer to How to View and Edit Dependencies of a Channel, page 51.

7.4 Deleting a PW2000 Channel

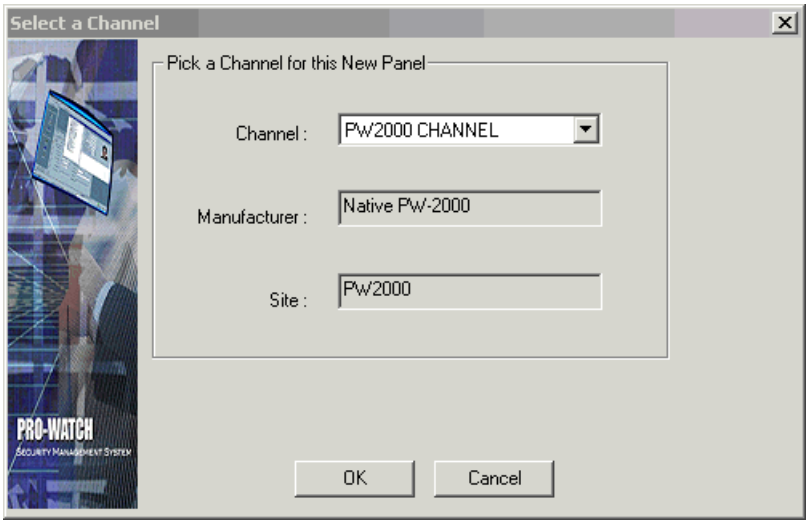
Please refer to How to Delete a Channel, page 51.

7.5 Adding a PW2000 Panel

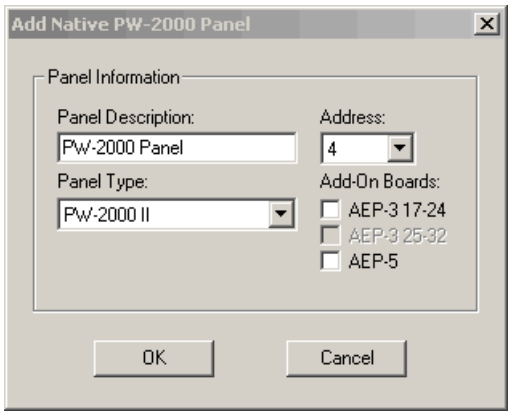
To turn the User Wizard on and off, see Turning the User Wizard On and Off, page 4.

To add a panel:

1. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
2. Select **New > Panel** to display the **Pro-Watch Controller Manager** screen.
3. Select the **Channel** you have created for this panel from the **Channel Description** drop-down list and click **OK**.



4. In the **Add Native PW2000 Panel** dialog box, enter the **Panel Description**.
5. Select the panel address from the drop-down list.
6. Select the panel type from the drop-down list. There are six different PW2000 panel types to choose from: II, II-X, III, III-X, IV, or IV-X. Select the panel type that corresponds to your hardware.



You may choose to include Add-On Boards for the PW2000 panel: AEP-3 17-24, AEP-3 25-32, and AEP-3 5 (AEP-3 5 is only available to the PW2000 II and II-X panels). Select the applicable Add-On Board check box and click **OK**.

7.6 Configuring PW2000 Panel Tabs

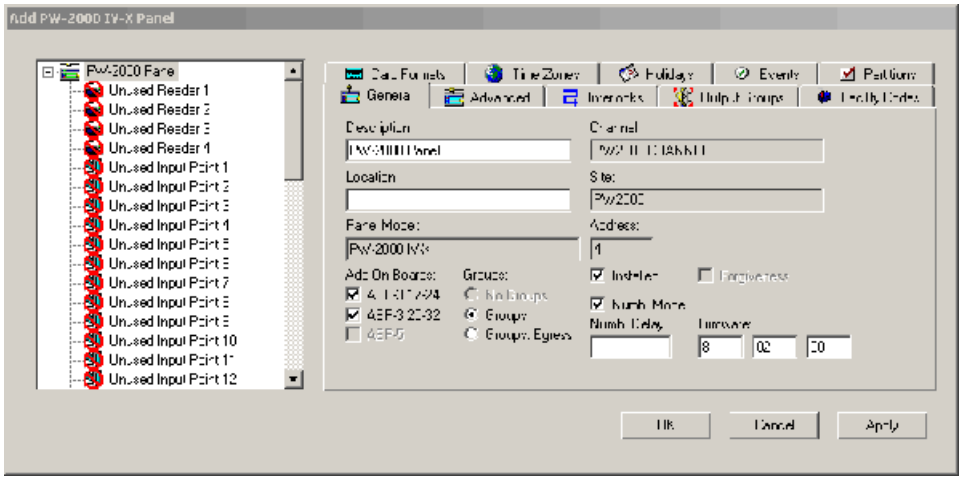
The Add PW2000 Panel dialog box includes the following tabs that you need to complete to configure the panel:

ADD A PW2000 PANEL TABS LIST

- "General Tab".
- "Advanced Tab".
- "Output Groups Tab".
- "Facility Codes Tab".
- "Card Formats Tab".
- "Time Zones Tab".
- "Holidays Tab".
- "Partitions Tab".

7.6.1 General Tab

The General tab includes hardware settings for the panel including initial configuration for add-on boards, if applicable.



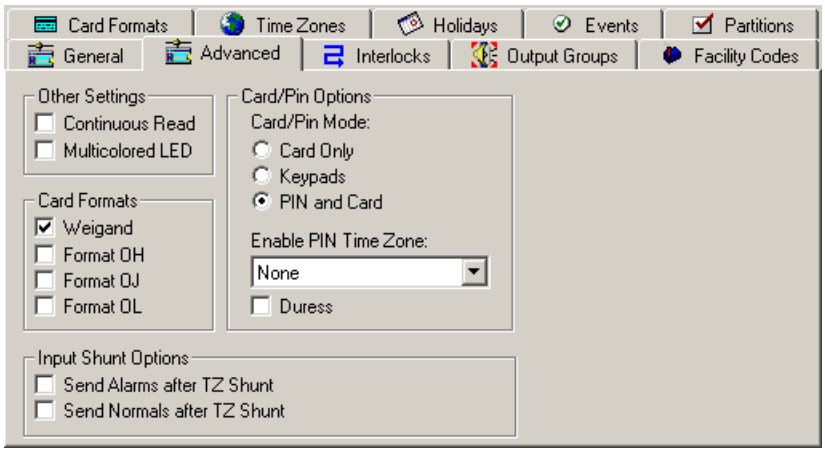
Use the following field descriptions to complete the General tab:

Field	Description
Description	Provides the description of the panel as defined by the user.
Location	Identifies the location of the panel as defined by the user.
Panel Model	Identifies the panel model type.

Field	Description
Channel	Identifies the channel the panel is assigned to.
Site	Identifies the site the panel is assigned to.
Address	Identifies the address of the panel.
Installed	Required for the panel to be installed and operational.
AEP-3 17-24	Add-on board for 8 additional outputs.
AEP-3 25-32	Add-on board for 8 additional outputs.
AEP-5	Add-on-Board (PW2000 II, II-X).
No Groups	Establishes zero outputs groups are assigned or configured.
Groups	When configuring a panel with groups then all the readers assigned to the panel trips the same group.
Groups, Egress	When configuring a panel with groups, egress, reader 1 trips the group and all other readers trip their respective outputs.
Numb. Mode	When enabled, after the card is presented to a reader, that card is not usable at any reader associated with the panel for a specified amount of time.
Numb. Delay	Specifies the amount of time the card remains unusable as described in Numb. Mode.
Forgiveness	Enables forgiveness for anti-passback when the panel contains Logical Devices that are part of an anti-passback configuration.
Firmware	Identifies the firmware version of the panel.

7.6.2 Advanced Tab

The Advanced tab enables you to configure additional settings for the panel including card specific configuration.

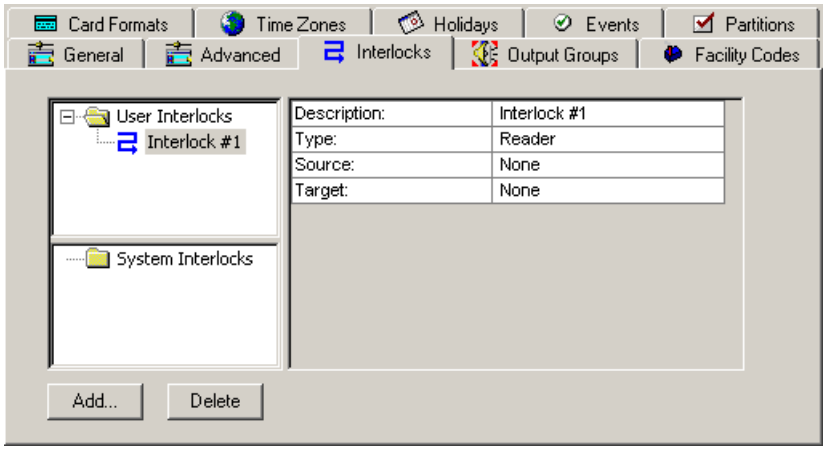


Use the following field descriptions to complete the Advanced tab:

Field	Description
Continuous Read	When enabled, while the card remains within the reader's range, the reader continuously reads the card.
Multicolor LED	Enables multicolored LEDs.
Weigand	Required to receive valid card reads from a weigand reader.
Format OH	Defines the specific format of a Weigand card.
Format OJ	Defines the specific format of a Weigand card.
Format OL	Defines the specific format of a Weigand card.
Send Alarms after TZ Shunt	When enabled, alarms are reported when an input comes out of a time zone shunt or mask.
Send Normals after TZ Shunt	When enabled, normals are reported when an input comes out of a time zone shunt or mask.
Card Only	Enables a valid card only.
Keypads	Enables a valid card number to be entered at a keypad.
PIN and Card	Enables a valid PIN and card.
Enable PIN Time Zone	Defines the time zones in which PIN is enabled.
Duress	Enables duress functionality. The "Duress" functionality enables the user to trigger an alarm event in times of duress such as when the site is under attack or the operator is forced to grant access to an unauthorized user.

7.6.3 Interlocks Tab

A PW2000 interlock is a defined action that occurs within a PW2000 panel at a destination device whenever an event occurs at the source device. For example, a REX input device (source) receives a request to exit and passes the order to the door strike device (destination) to open the door latch. For each interlock, you define a source and a destination device.



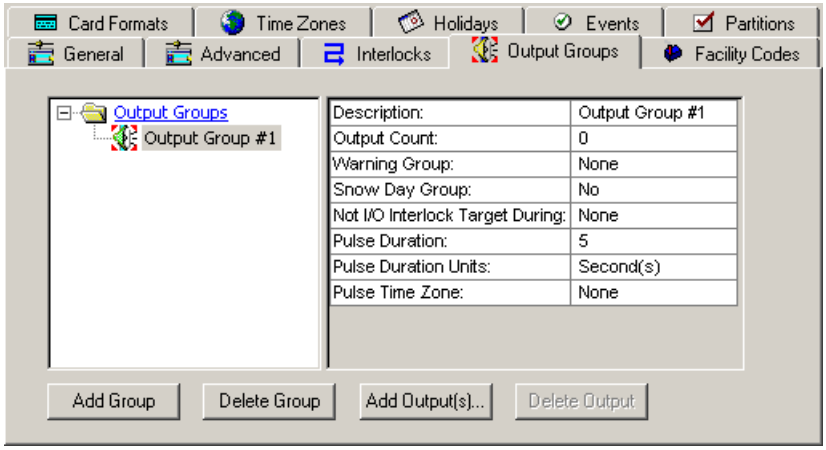
To add interlocks:

1. Click **Add** in the User Interlocks window. System Interlocks are coded and cannot be changed or deleted.
2. In the right pane, enter the description of the Interlock.
3. Select **Type** from the drop-down list. Also see PW2000 Interlocks under Adding or Editing a Hardware Template, page 28.

Note: Additional fields will appear upon selecting the interlock type.These fields will vary depending on the interlock type chosen.

7.6.4 Output Groups Tab

An output group tab allows you to configure output groups and define their attributes. You may also assign individual output point(s) to the output group.



To add an output group, click **Add Group**. Use the following field descriptions to configure the output group.

Field	Description
Description	Provides the description of the output group as defined by the user.
Output Count	Defines how many outputs are in an output group.
Warning Group	A warning group is used to indicate that another group is about to become active.
Snow Day Group	Snow day groups are special groups that are used to allow the first person (or a specific person) at a site in the morning to swipe a card and activate the group. If there is a snow day, and that person never arrives, the facility remains locked.
Not I/O Interlock Target During	Indicates the time zone in which the output is not a target of an interlock.
Pulse Duration	Defines the duration that the output pulses.
Pulse Duration Units	Defines the unit of measurement (seconds, minutes) for the pulse duration.
Pulse Time Zone	Defines the time zone in which the output pulses.

To add outputs to an Output Group:

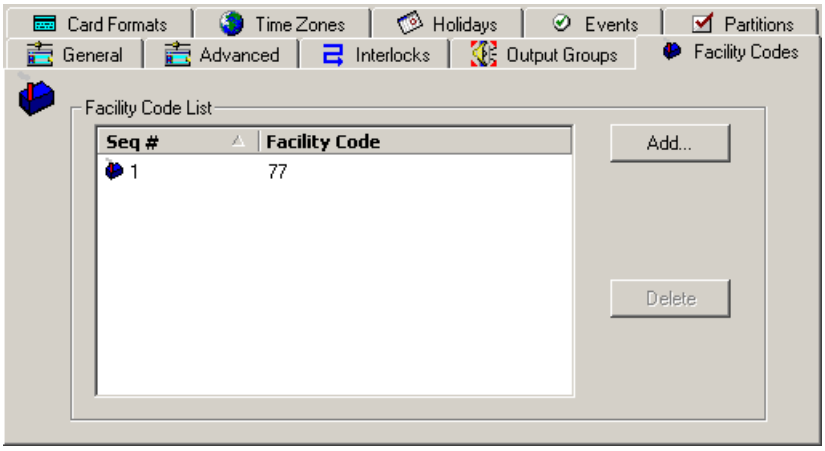
1. Click **Add Output(s)** to display the Add Output to Output Group dialog box. To add an available output to current outputs, select the available output and click on the single arrow icon (click on the double arrow icon to add all available outputs to current outputs).
2. Click **OK.**

To delete outputs from the Output Group:

1. Select the output you want to delete.
2. Click **Delete Output.**

Facility Codes Tab

Facility Codes are optional characteristics of formatted cards. The facility code serves as a secondary ID beyond the card number.



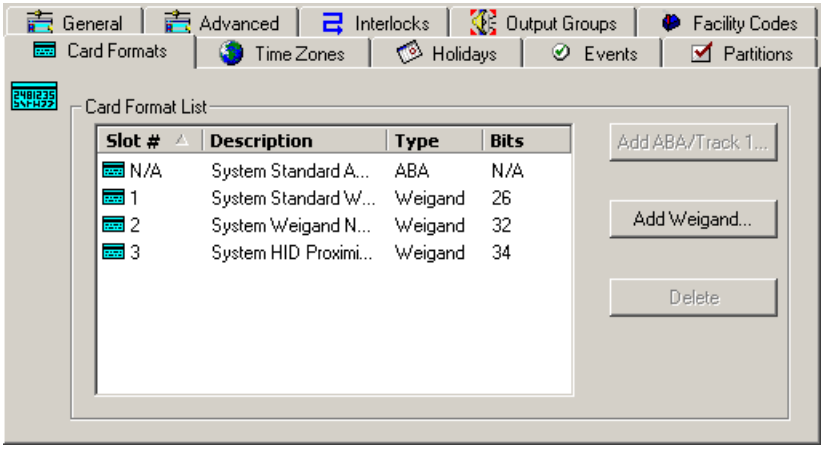
Facility Codes are required to obtain valid card reads.

To add a facility code to the panel:

1. Click **Add**.
2. Select the Sequence Number.
3. Enter the Facility Code that is assigned to each card and click **OK**. Facility Codes are assigned to the cards during manufacture.
4. Repeat step 1 through step 3 until all applicable Facility Codes are added.

7.6.5 Card Formats Tab

A card format tells the panel how to interpret data on the card to determine the card number. You must add the card format corresponding to the applicable cards before a reader allows a valid card read.



There are two types of card formats that can be added to the panel, ABA and Weigand. Four default card formats are provided.

To add an alternate ABA card format, you must first delete the default ABA card format:

1. Select the default ABA format.
2. Click **Delete.**
3. Click **Add ABA/Track 1...** If the ABA card format you want appears in the dialog box:
   a. Select the card format.
   b. Click **OK**.
4. If the card format you want does not appear in the dialog box:
   a. Click **Add.**
   b. Select the Card Format Type (PW2000 ABA).
   c. Click **OK.**

To complete the card format configuration, see "DBC - Card Formats" in Chapter 35.

To add additional Weigand card formats:

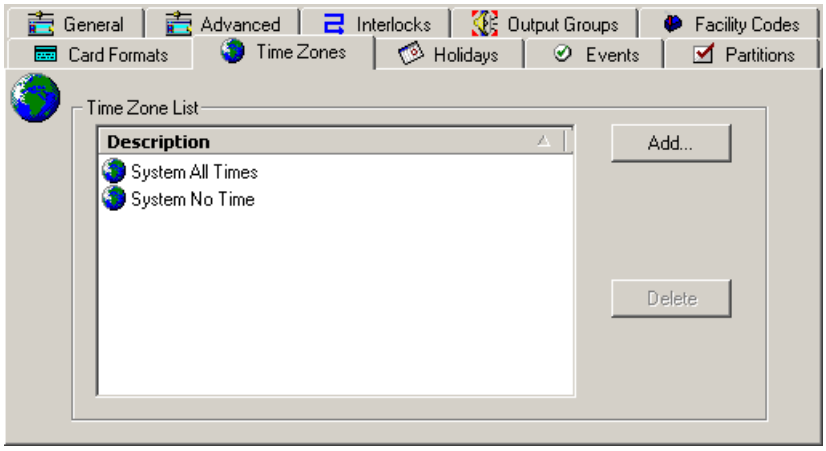
1. Click **Add Weigand**... If the Weigand card format you want appears in the dialog box:
   a. Select the card format.
   b. Click **OK**.
2. If the card format you want does not appear in the dialog box:
   a. Click **Add.**
   b. Select the Card Format Type (PW2000 Weigand/Track One).
   c. Click **OK.** To complete the card format configuration, see "DBC - Card Formats" in Chapter 35.

To delete a card format from the panel:

1. Select the card format you want to delete.
2. Click **Delete.**

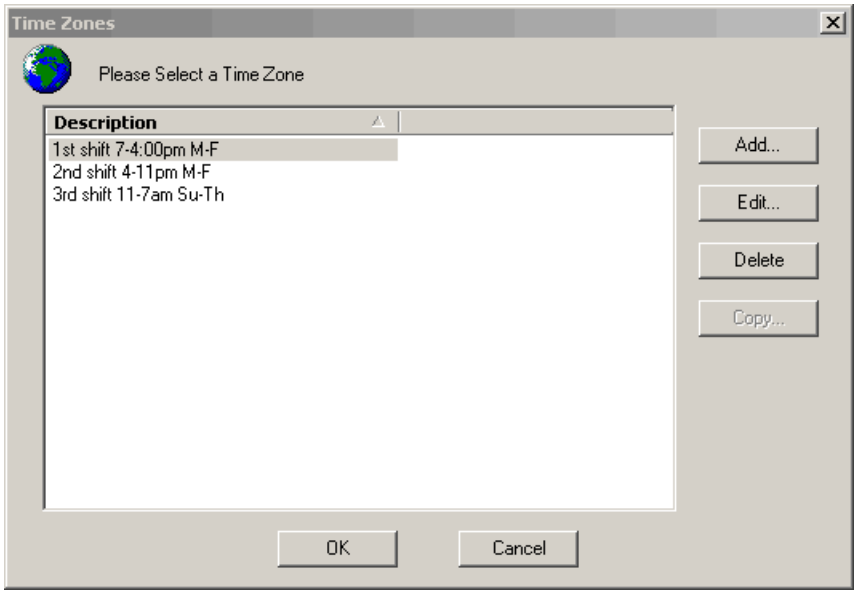
7.6.6 Time Zones Tab

The Time Zones tab enables you to add time zones to the panel; only time zones that have been added to the panel are available to configure applicable panel and reader fields:



To add a time zone to the panel:

1. Click **Add** to display the Time Zones dialog box:

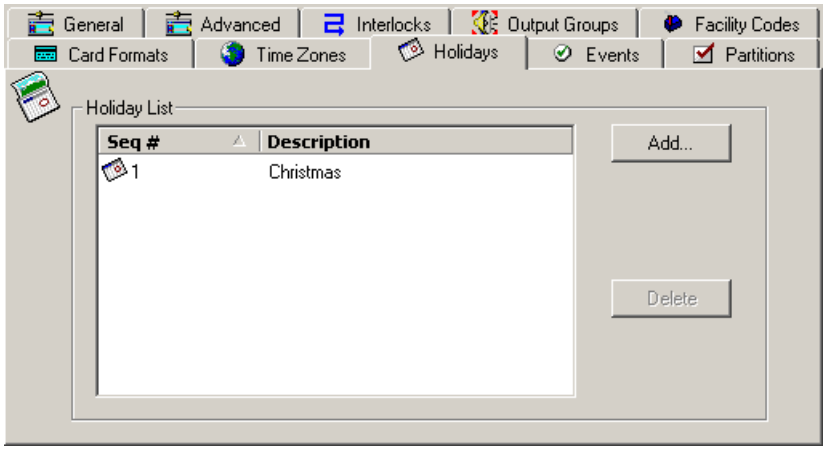


2. Select the Time Zone.
3. Click **OK.**

If the time zone you want does not appear in the Time Zones dialog box, or if the time zone list is empty, you can create a new time zone by clicking **Add**. To complete adding a new Time Zone, see "DBC - Time Zones" in Chapter 57.

7.6.7 Holidays Tab

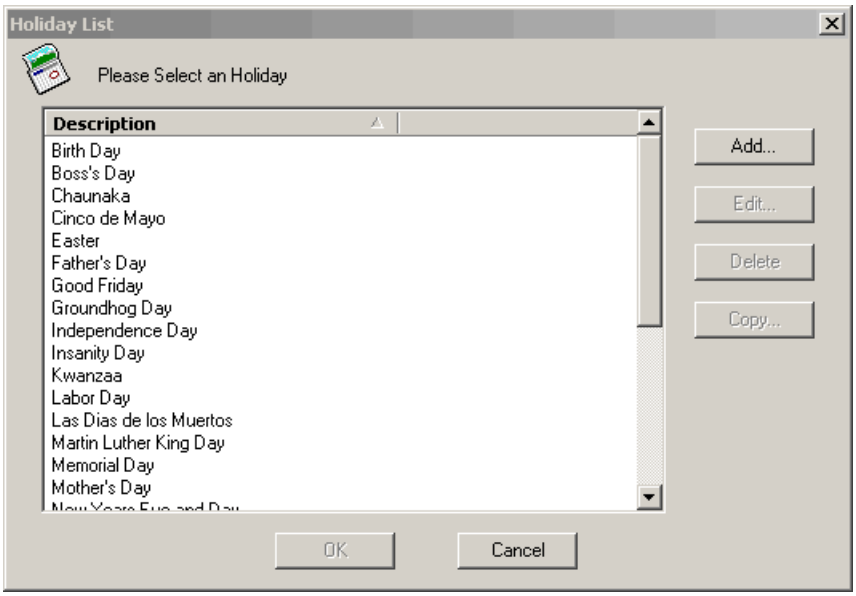
Holidays enable you to edit normal Time Zone behavior on specific days. You can enable connected panels to restrict access on holidays.



To add a holiday to the panel:

1. Click **Add** to display the Select Holiday dialog box.
2. Select the sequence number you want to assign to the holiday from the drop- down list.
3. Click the icon next to the Holiday field.
4. Click **Define.**
5. Select the holiday from the holiday list and click **OK**.
6. Click **OK** at the Select Holiday dialog box. If the holiday you want does not appear in the holiday list dialog box you can create a new holiday.

To create a new holiday from the Holiday List dialog box, click **Add**. To complete adding a new holiday, see "DBC - Holidays" in Chapter 49.



7.6.8 Events Tab

The Events tab displays the default event types that are applicable to the PW2000 panel.

To define an event:

- Either double-click the event you want to define or select and click **Edit** to display the Edit Point dialog box. For more information on editing events, see "HW Config - Edit Point".

7.6.9 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. For information about creating a partition, see "DBC - Partitions" in Chapter 53.

To add or delete an already-created partition to the panel:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition.
3. Click **Add**.

To delete a partition from the Partitions List dialog box:

1. Select the partition.
2. Click **Delete**.

After completing each tab within the panel, you will need to save the panel configuration.

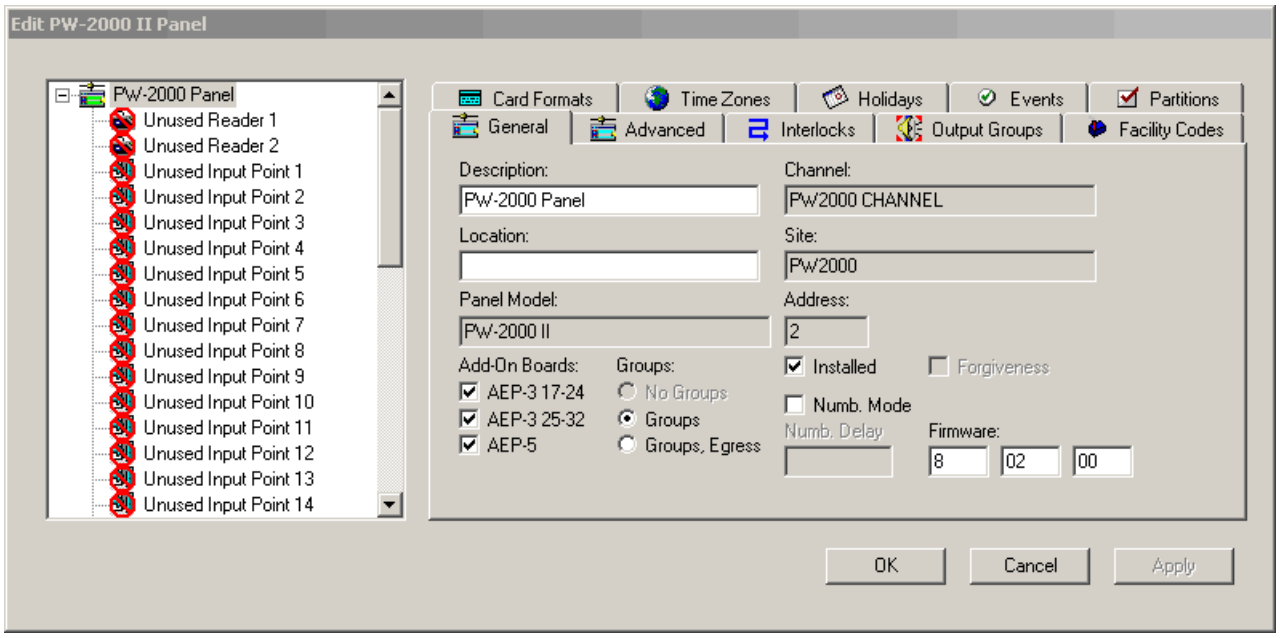
To save the panel configuration:

- Click **OK** at the Add [Panel Name] Panel dialog box.

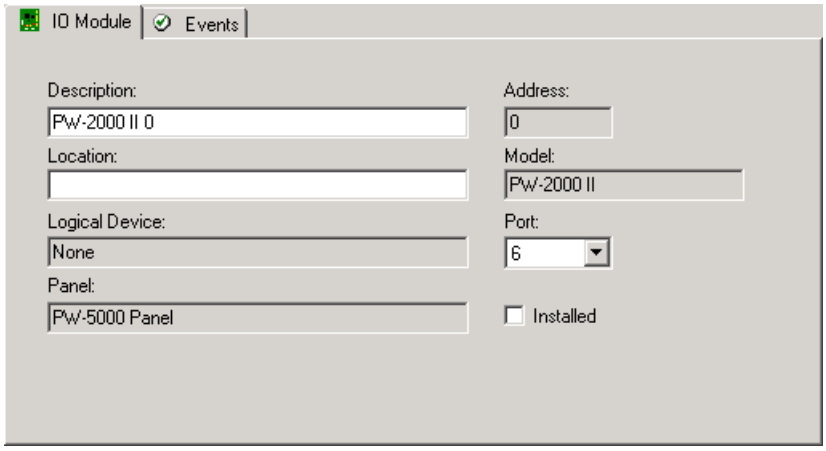
7.7 Editing a PW2000 Panel

To edit a panel:

1. In the Pro-Watch Hardware Configuration tree view, click the site to which the panel is assigned.
2. Click the Panel's subdirectory. The icons of the existing panels appear in the right pane of the window.
3. Right-click the panel you want to edit, and select **Properties**. The Edit [Panel Name] Panel dialog box appears.



4. Configure the I/O modules listed in the panel tree list in the Add [panel name] Panel dialog box.
   a. Click the first I/O Module listed in the panel tree list to display the I/O Module and Events configuration tabs.



b. Use the following field descriptions to complete the I/O Module tab:

Field	Description
Description	Provides a description of the I/O Module.
Location	Identifies the location of the I/O Module.
Logical Device	Identifies the name of the Logical Device.
Panel	Identifies the panel type to which the I/O module has been added.
Address	Identifies the address of the I/O Module.
Model	Identifies the I/O Module model type.
Port	Defines which port the I/O Module is connected to on the panel.
Installed	Required to install the I/O Module.

c. Click the Events tab to display the events that can support this input/output module.

d. Either double-click the event you want to define or select the event and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point". Note that you can also add and delete input/output modules. To add an input/output module, right-click anywhere in the panel tree and select **Add IO Module**. To delete an input/output module, right-click the module you want to delete and click **Delete IO Module**.

5. Display the panel's configuration tabs by clicking the panel in the panel tree list.
6. Complete each tab to configure the panel. See the following tab list and the corresponding tab sections in "Configuring PW2000 Panel Tabs" for the configuration information:

   EDIT A PW2000 PANEL TABS LIST

   - "General Tab".
   - "Advanced Tab".
   - "Output Groups Tab".
   - "Facility Codes Tab".
   - "Card Formats Tab".
   - "Time Zones Tab".
   - "Holidays Tab".
   - "Partitions Tab".

7.7.1 Buffering or Un-buffering a PW2000 Panel

The PW2000 Panel allows you to buffer and un-buffer the panel.

- When a panel is buffered, no events are received by Pro-Watch and no events can be seen in the event viewer.
- When a panel is un-buffered, events are received by Pro-Watch and they can be seen in the event viewer.

To buffer or un-buffer a panel:

1. Select the panel from the Hardware Configuration window.
2. Right-click on the panel and select **Actions > Buffer** or **Actions > Un-Buffer** option:

The PW2000 Panel also allows you to forgive anti-passback (see "DBC - Area" in Chapter 29) for all cards.

To forgive anti-passback:

1. Select the panel from the Hardware Configuration window.
2. Right-click on the panel and select **Actions > Forgive Anti-Passback**:

7.8 Viewing and Editing Dependencies of a PW2000 Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

7.9 Deleting a PW2000 Panel

Please refer to How to Delete a Panel, page 53.

7.10 Adding a PW2000 Logical Device

A Logical Device is a single physical device or group of selected physical devices, which are defined by a hardware template. For example, a template may define a door that is equipped with a card reader, a REX input device, a DPS input device, and a door strike (lock) output device as one Logical Device.

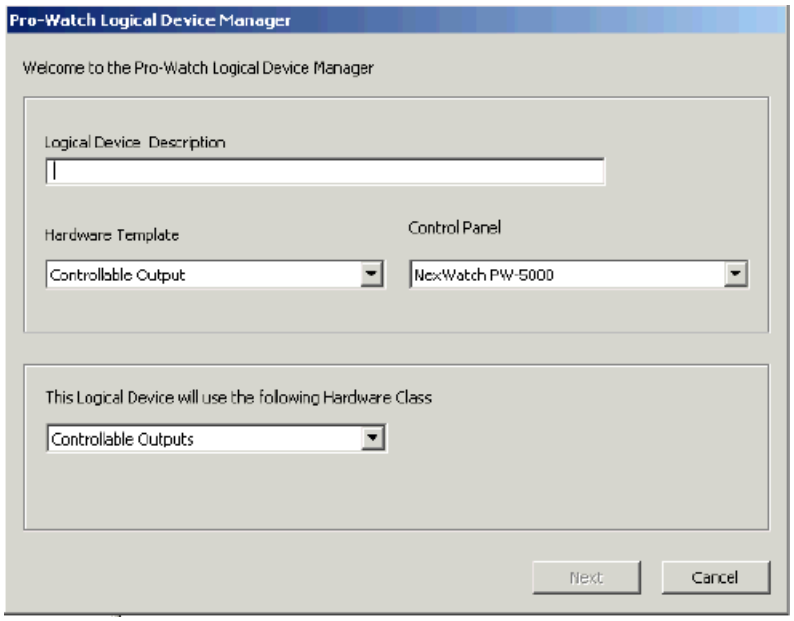
As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system. For example, you can assign the door, reader, input devices, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you create Logical Devices, you must create the following:

- Site. See Add a Site, page 46.
- Channel. See "Adding a PW2000 Channel".
- Panel. See "Adding a PW2000 Panel".
- Hardware Template. See "Adding or Editing a Hardware Template".

To add a Logical Device:

1. From the Pro-Watch Hardware Configuration tree view, right-click the site to which you want to assign the Logical Device and select **New > Logical Device**. The Pro-Watch Logical Device Manager dialog box appears.



2. Enter a description that will identify the Logical Device in the Logical Device Description field.
3. Select a hardware template from the Hardware Template drop-down list. See "Adding or Editing a Hardware Template".

4. Select a Hardware Class from the drop-down list in the Hardware Class field.
5. Select the Device Types that the Logical Device will include.
6. Click **Finish** to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the type of panel and any add-on boards applied.

7.11 Editing a PW2000 Logical Device

You can edit Logical Devices after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices will already be configured. See "Adding or Editing a Hardware Template" for more information. However, it is a good idea to visit the Logical Device configuration tabs in this section, since these tabs contain field information that hardware templates do not.

To configure a Logical Device, right-click the Logical Device you want to configure or edit, and select **Properties**. The Edit Logical Devices: [Logical Device name] dialog box appears.

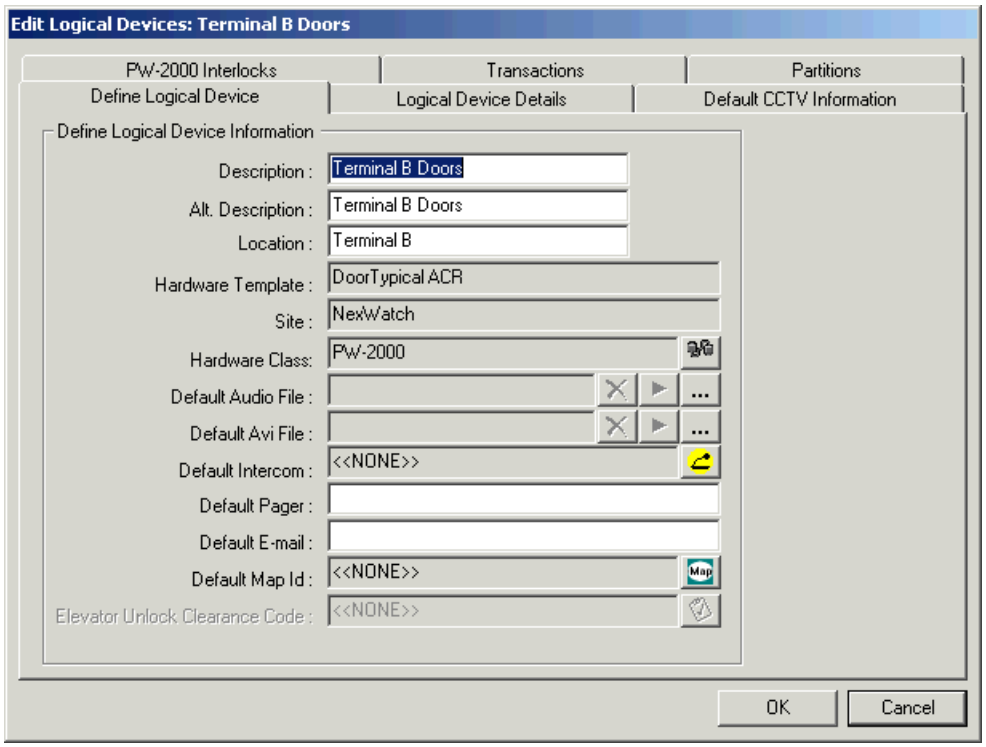
The Edit Logical Devices dialog box includes multiple tabs. Complete each of the following tabs to configure the panel:

EDIT A PW2000 LOGICAL DEVICE TABS LIST

- "Define Logical Device Tab".
  - Reader Devices
    - "Reader Tab".
    - "Events Tab".
  - Input Point Devices
    - "**Input Tab**".
    - "Events Tab".
  - Output Point Devices
    - "Output Tab".
    - "Events Tab".
    - "Default CCTV Tab".

- "Transactions Tab".

7.11.1 Define Logical Device Tab

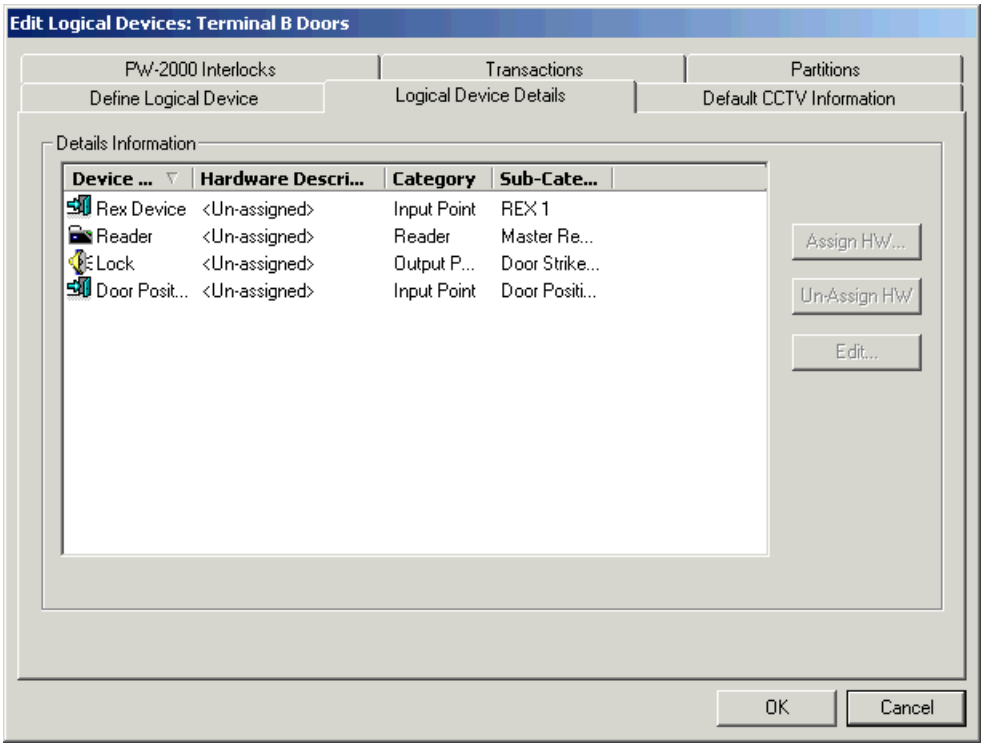


Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See "Adding or Editing a Hardware Template".
Site	Identifies the Site in which the Logical Device is assigned.
Hardware Class	Defines the hardware class in which the Logical Device resides. See "Adding or Editing a Hardware Class".
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point".

Field	Description
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point".
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point".
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point".
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point".
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. See "DBC - Clearance Codes" in Chapter 37 for more information.

7.11.2 Logical Device Details Tab

This tab displays all of the device types included in the Logical Device. At this tab you can assign, un-assign, or edit the device types.



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click **OK**.

To un-assign a device type:

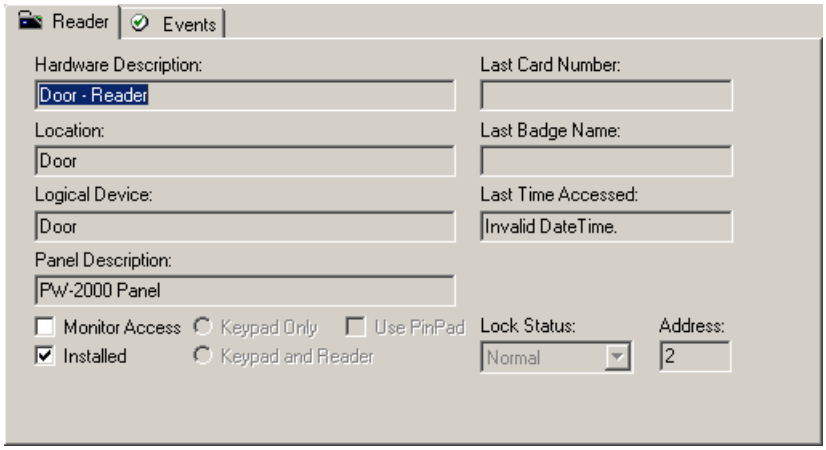
- Click to select the device type and click **Un-Assign HW**.

To edit the current configuration of a device type:

- Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete. Use the appropriate table below to edit or configure the device type you have selected.

Logical Device Details > Readers

Reader Tab



Field	Description
Hardware Description	Description of the Logical Device.
Location	Identifies the physical location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel Description	Identifies the panel in which the Logical Device is assigned.

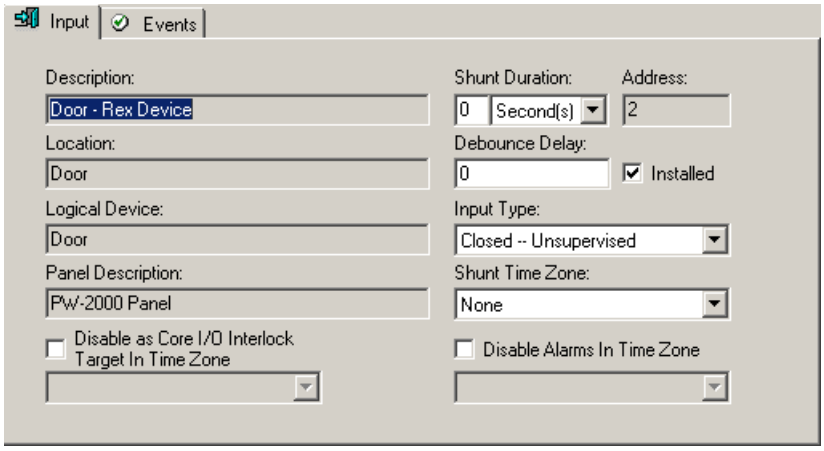
Field	Description
Monitor Access	Enables monitor access (card trace) for the Logical Device.
Installed	Required for the Logical Device to be enabled and operational.
Keypad Only	Designated the reader as a keypad only reader.
Keypad and Reader	Designates the reader as a keypad and card reader.
Use PinPad	Designates the reader as a keypad (PINpad) in which you would enter a personal identification number (PIN) after a card swipe.
Last Card Number	Identifies the last card number presented to the Logical Device.
Last Badge Name	Identifies the last badgeholder name of the badge presented to the Logical Device.
Last Time Accessed	Identifies the last time the Logical Device was accessed.
Lock Status	Identifies the lock status of the reader.
Address	Identifies the address of the Logical Device.

Events Tab

To define an event, either double-click the event you want to define, or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point".

Logical Device Details > Input Points

Input Tab



Field	Description
Description	The description of the Logical Device.
Location	Identifies the physical location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel Description	Identifies the panel in which the Logical Device is assigned.
Disable as Core I/O Interlock Target in Time Zone	If the Logical Device is the target of a core interlock (Input/Output Group), then the action that the Logical Device would normally take when the interlock fired does not occur during the assigned time zone.
Shunt Duration	Defines the duration of a shunt or mask. An input that is shunted or masked cannot cause an alarm.
Address	Identifies the address of the Logical Device.
Debounce Delay	Defines the pause between input alarms. When an input is triggered, a pause occurs before the next input alarm is sent.
Installed	Required for the Logical Device to be enabled and operational.
Input Type	Defines the input type (Closed - Unsupervised or Open - Unsupervised).
Shunt Time Zone	Identifies the time zone in which the input point is shunted or masked.

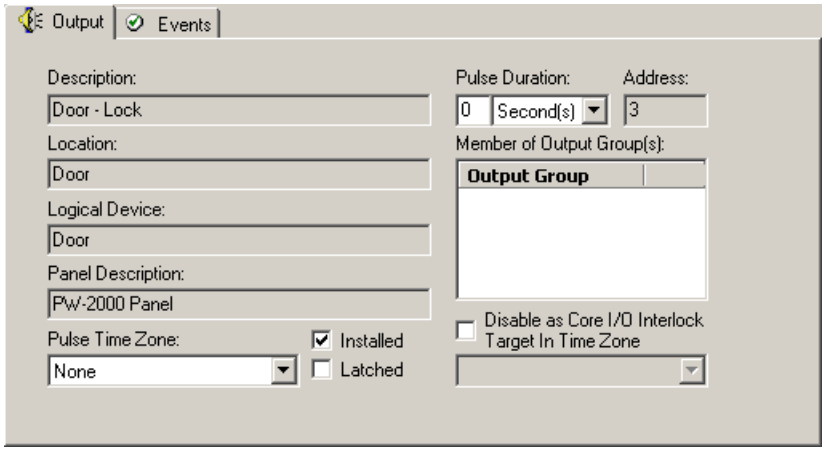
Field	Description
Disable Alarms in Time Zone	Identifies the time zone in which alarms associated with input points are disabled.

Events Tab

To define an event, either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point".

Logical Device Details > Output Points

Output Tab



Field	Description
Description	The description of the Logical Device.
Location	Identifies the physical location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel Description	Identifies the panel in which the Logical Device is assigned.
Pulse Time Zone	Defines the time zone in which the output pulses.
Installed	Required for the Logical Device to be enabled and operational.
Latched	When enabled, the output, once activated, remains activated until manually deactivated.

Field	Description
Pulse Duration	Defines the duration of an output pulse.
Address	Identifies the address of the Logical Device.
Member of Outputs Groups	Identifies the output group in which the output point is a member of, if any.
Disable as Core I/O Interlock Target in Time Zone	If the Logical Device is the target of a core interlock (Input/Output Group), then the action that the Logical Device would normally take when the interlock fired does not occur during the assigned time zone.

Events Tab

To define an event:

1. Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point".
2. Click the **PW2000 Interlocks** tab.
3. Click the **Transactions** tab.
4. Click the **Partitions** tab.

7.11.3 Default CCTV Tab

If you added Logical Devices that included CCTV, the CCTV information you configured already appears on this tab. Click the appropriate icons to select the default auto CCTV command, select CCTV view, and select CCTV command for this device.

7.11.4 Transactions Tab

The Transactions tab displays all the transactions that have occurred at that particular reader. The number of records also appears, and you can print the list of transactions.

7.11.5 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

To assign a partition to an existing Logical Device:

1. Click the Partitions tab.
2. Click **Add**.
3. Select an available partition.
4. Click **OK**.

See "DBC - Partitions" in Chapter 53 for more information about defining partitions.

7.12 Viewing and Editing Dependencies of a PW2000 Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 53.

7.13 Deleting a PW2000 Logical Device

Please refer to How to Delete a Logical Device, page 53.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config -

PW-5000/PW-6000/PW-6K1ICE Channel Type

8

In this chapter ...

Overview

> Channel

Adding a PW-5000/PW-6000/PW-6K1ICE Channel

Encrypting a PW-5000/PW-6000/PW-6K1ICE Channel

Viewing and Editing Dependencies of a PW-5000/PW-6000/PW-6K1ICE Channel

Deleting a PW-5000/PW-6000/PW-6K1ICE Channel

> PW-6000/5000/3000 Panel

Adding a PW-6000/5000/3000 Panel

Editing a PW-6000/5000/3000 Panel

Memory Warning for PW-6000

Viewing and Editing Dependencies of a PW-6000/5000/3000 Panel

Deleting a PW-6000/5000/3000 Panel

PW-6000/5000/3000 Elevators

> PW6K1ICE Panel

Overview - PW6K1ICE Panel

Adding a PW6K1ICE Panel

PW6K1ICE DS with RS-485 Downstream

Configuring the PW6K1R1E Downstream I/O Boards

Viewing and Editing Dependencies of a PW6K1ICE Panel

Deleting a PW6K1ICE Panel
> Mercury Panel
Adding a Mercury Panel
Viewing and Editing Dependencies of a Mercury Panel
Deleting a Mercury Panel
Mercury Text Output to LCD Terminal
Mercury Protocol
Mercury Intrusion
> Logical Device
Adding a Logical Device
Configuring a Logical Device
Viewing and Editing Dependencies of a Logical Device
Cypher Mode
Deleting a Logical Device

8.1 Overview

This chapter describes how to configure the **PW-6000/5000/PW6K1ICE channel type**. It includes information on how to configure to following type of panels:

- PW-3000
- PW-5000
- PW-6000
- PW6K1ICE
- Mercury family of equivalent panels.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

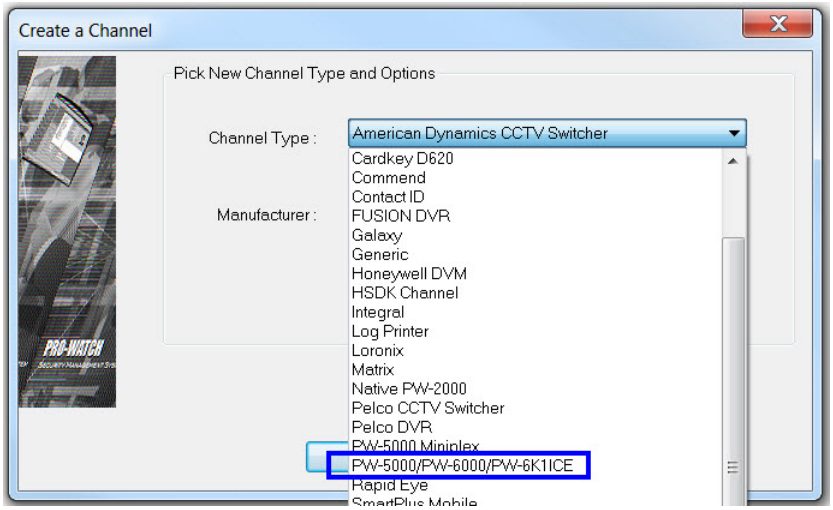
8.2 Adding a PW-5000/PW-6000/PW-6K1ICE Channel

A Pro-Watch channel is the communications path between the host and panels. You must identify the channel before adding a panel and Logical Device.

Note: The recommended maximum number of channels per site is 99.

To add a channel:

1. Select a channel type:
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created.
   b. Select **New > Channel**. The **Create a Channel** dialog box appears.
   c. Select "**PW-5000/PW-6000/PW-6K1ICE**" for **Channel Type** from the drop-down list:



   d. Click **OK** to display the **Define Channel Information dialog box**.
2. Define the channel:
   a. In the **Define Channel Information** dialog box, enter an identifying channel **Description**.
   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
   c. From the **Time Zone** drop-down list, select the time zone that is appropriate for your site's geographic location.
   d. In the **Attempts** field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.
   e. In the **Poll Delay** field, enter the Pro-Watch server-to-panel poll interval in milliseconds. Note that the minimum interval in a

PW-5000 networked configuration is 300 milliseconds, even if you should enter a smaller number.

f. In the **Comm Break** field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.

g. The communications **Spool Directory** is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.

Note: Spool File Count field is autopopulated.

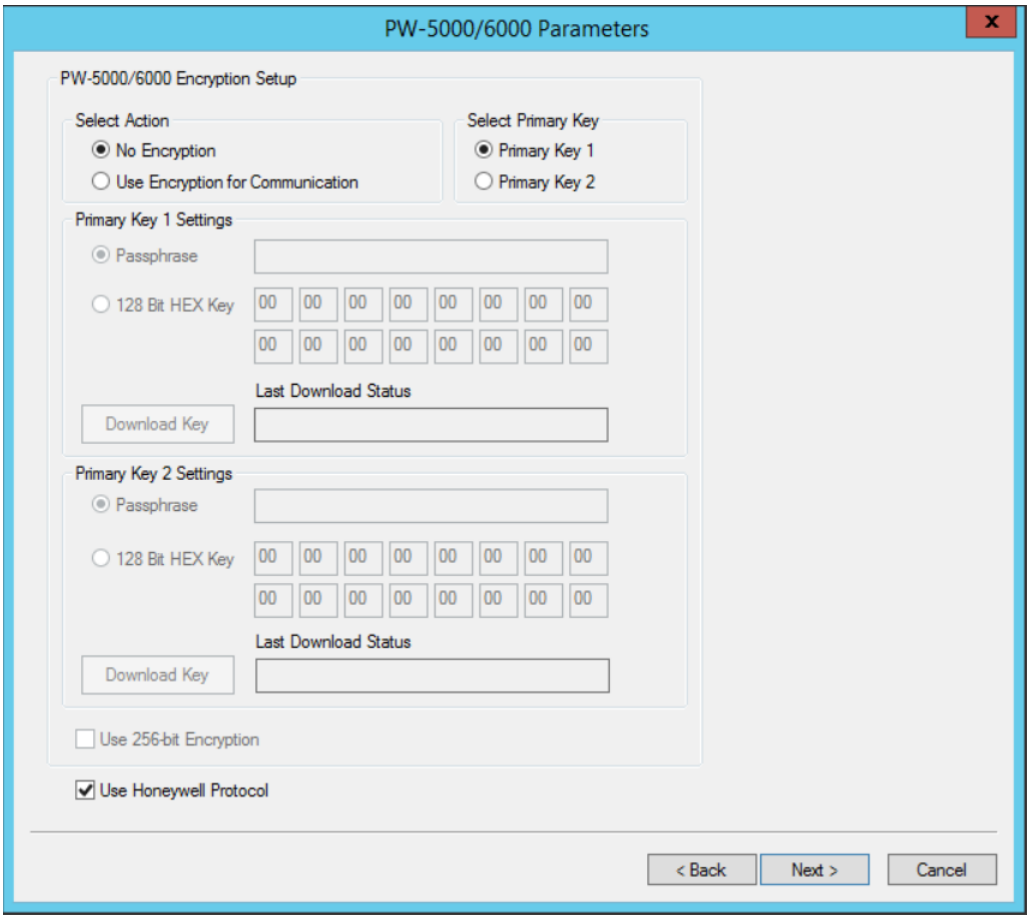
h. Click **Next** to display the **Communications Parameters** dialog box.

3. Set the **Communications Parameters**:

   a. Select the port type for the **Primary** and (if needed) **Secondary** ports from the following drop-down list options:

Option	Comments
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
TCP/IP	Specifies that the channel is a network connection. IP Address – the IP address of the panel.
Dial Out	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
Dial In	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
Modem Pools	Modem pools are used for dial out. Model Pool – collection of modems. Baud – the rate of communication between the host and the panel. Flow Control – starts and stops transmission between the host and the panel.
Secondary Channel	Acts as a fail-safe; secondary channel communication comes online if the primary channel communication breaks.

4. Click **Next** to proceed to the **PW-5000/6000 Parameters** dialog box:



Encryption keys are used to encrypt the communication between the host and the panel. Keys are always downloaded to panels on demand. Note that the ability to download encryption keys is disabled by default. To enable the download, a user must be granted the permission to download by an administrator. To do this, the administrator selects **Database Configuration > Users,** selects the user, selects **Programs > Hardware Configuration > Panel Maintenance > Download Keys**, and clicks the **Grant** button. If "Download Keys" is not displayed in the list of Panel Maintenance functions, click the **Add Function** command button and add that function.

You can download encryption keys with either the hardwired or TCP/IP physical port type. Upon download, you can change the communication parameters.

Note: The panel must be added before encryption parameters are configured. To learn more about panel encryption please refer to the

upcoming section **Encrypting a PW-5000/PW-6000/PW-6K1ICE Channel**, page 10.

Note: If a panel that is using encrypted communications starts going offline/online several times a minute, the panel might have undergone a cold reset and its RAM might have been cleared. To recover from this, disable encryption at the channel level. This de-encrypts communications, so it will need to download the encryption keys again later.

Field	Description
Use 256-bit Encryption check-box	Select this check-box to use 256-bit encryption.
"Use Honeywell Protocol" check-box	Make sure this is selected to ensure that the communication to the panel will be using the Honeywell Protocol. Note: This check-box cannot be edited once the channel is created.

5. If the **Primary** or **Secondary** port is **Modem Pool**, **Dial In**, or **Dial Out**, click **Next** to display **Channel Dialup** dialog box. When selecting dial-up communication parameters, you must complete the settings within the channel dialup box. Please see Appendix C, Dial-Up Configuration for more information on configuring dial-up settings.

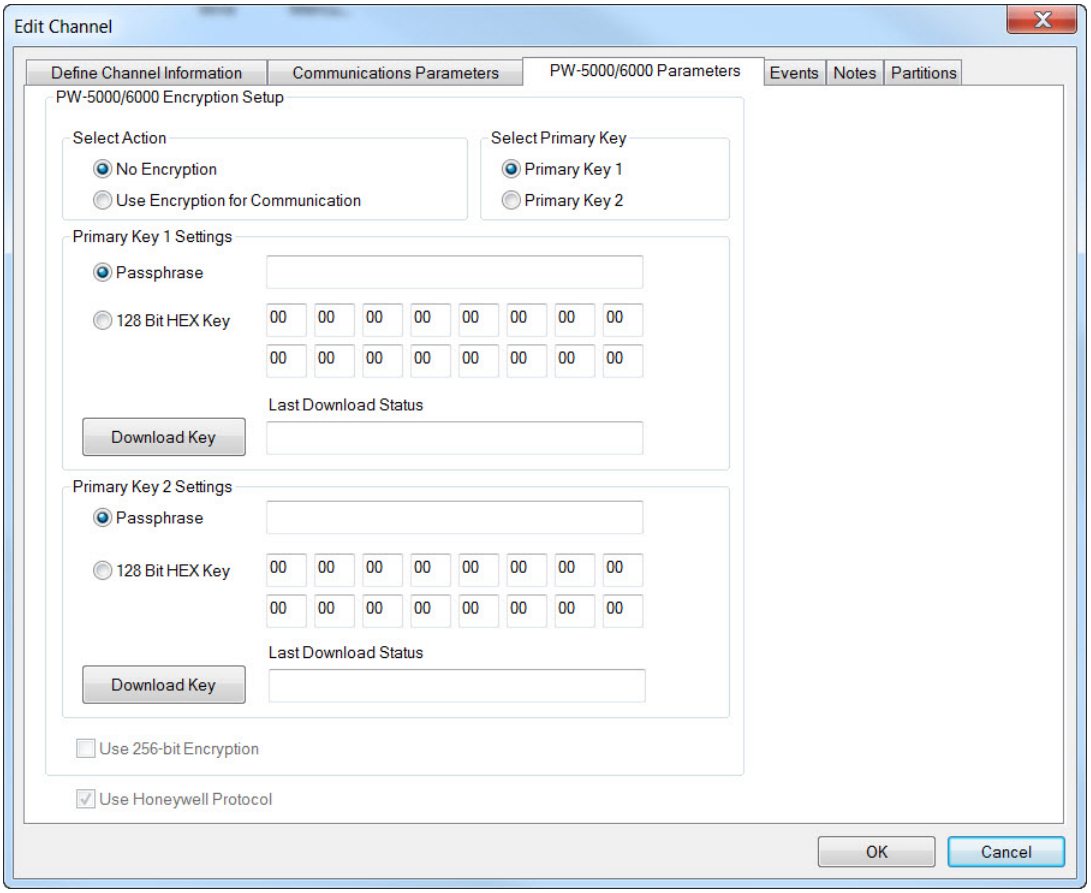
Field	Description
Dialup Schedule	Determines how often you want to call the panel. Dial-up Schedules are configured in Database Configuration. For more information, see "DBC - Dial-Up Schedule" in Chapter 42.
Password	Identifies the password to the remote hub.
Remote Site Phone Number	Defines the phone number for the remote site.
Host Phone Number	Not applicable. Dial-in is initiated by panel-level triggers and procedures. See Appendix C, Dial-Up Configuration for more information.
Phone Host After # of Events	Initiates dial up after a specified number of events have occurred.
Serial Number	Automatically populated; it is used for the panel driver's identification scheme.

Field	Description
Dialup Retries	Defines the number of times the host attempts to dial up.
Site ID	This function is currently not supported.
Forcibly Disconnect After (minutes)	Defines the amount of time in minutes until the connection is forced to disconnect.
Disconnect After (sec)	Defines the amount of time of inactivity that can pass before disconnect.
Delay Connect Time	This function is currently not supported.
Delay Retry Time	This function is currently not supported.
Prefix	Defines the area code. Not applicable since the area code is typically included when the number is defined.
Modem Init String	This function is currently not supported.

6. Click **Next** to display the **Partitions** dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.
7. Click **Finish** to complete the channel. A warning message appears reminding you that you must add the channel to the appropriate routing group before you can view any events using the channel. It is recommended that you assign the channel to a routing group after you plan and configure routing groups. For more information, see "DBC - Routing Groups" in Chapter 55.

8.3 Encrypting a PW-5000/PW-6000/PW-6K1ICE Channel

To configure encryption for a channel, select the channel, right-click to display the pop-up menu and select **Properties** options to display the **Edit Channel** screen. Then select the **PW-5000/6000 Parameters** tab:



.

Field	Description
No Encryption	Encryption is not enabled. You can disable encryption at any time.
Use Encryption for Communication	Encryption is enabled for communication. Encryption can only be enabled when one or more keys have been downloaded.
Primary Key 1	Selects the settings by which the key is downloaded. The key settings are defined on the Edit Channel screen.
Primary Key 2	Selects the settings by which the key is downloaded. The key settings are defined on the Edit Channel screen.

Field	Description
Passphrase	Provides the ability to create a key. Any characters may be used to create a key.
128 Bit HEX key	Must be 32 digits from 0-9, A-F. For example: 1A 5F 56 78 AC 01 45 19 F2 86 33 3D 42 9A 12 EE
Download Key	Downloads the key. The communication mode must either be hardwired or TCP/IP. Only one key can be downloaded at a time.
Use 256-bit Encryption	Select this to enable 256-bit encryption. See section "256-Bit Encryption" for more information.

256-Bit Encryption

The "**Use 256-bit Encryption**" check-box can be selected only if

- "**Use Encryption for Communication**" radio-button is selected, AND
- Both sets of master keys (**Primary Key 1** and **Primary Key 2)** are defined either by a **Passphrase** or through the **128 Bit HEX Keys**.

The master keys (**Primary Key 1** or **Primary Key 2**) cannot be modified and downloaded to panel while 256-bit encrypted communication is in use.

Note: The minimum firmware version to support 256-bit encryption for several panels is listed below:

- PW-6000 IC added in Version 2.060
- PW6K1ICE (EP1501) Version 1.16.0
- EP2500 Version 1.16.0
- EP1502 Version 1.16.0

Encryption Icons Color Coding

Channel and Panel list view will display the channel and panel status with a different icon, depending on whether 128-bit or 256-bit encryption is enabled and if Pro-Watch can communicate to the channel/panel or not.

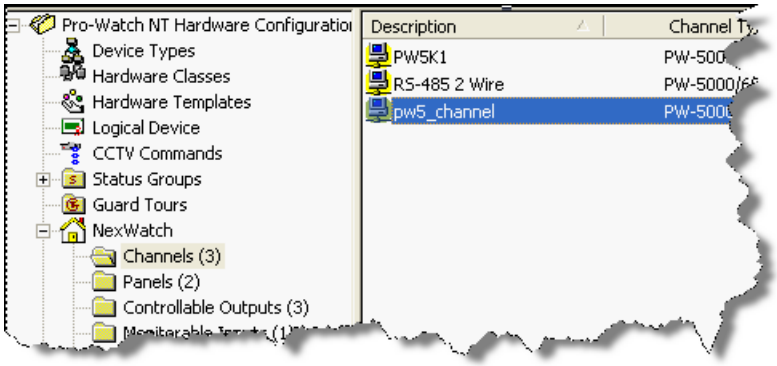
The icon will display DOUBLE KEYS to signify that 256-bit encryption is in effect and a SINGLE KEY for the 128-bit encryption.

Table 8-1 Encryption Icon Color Coding

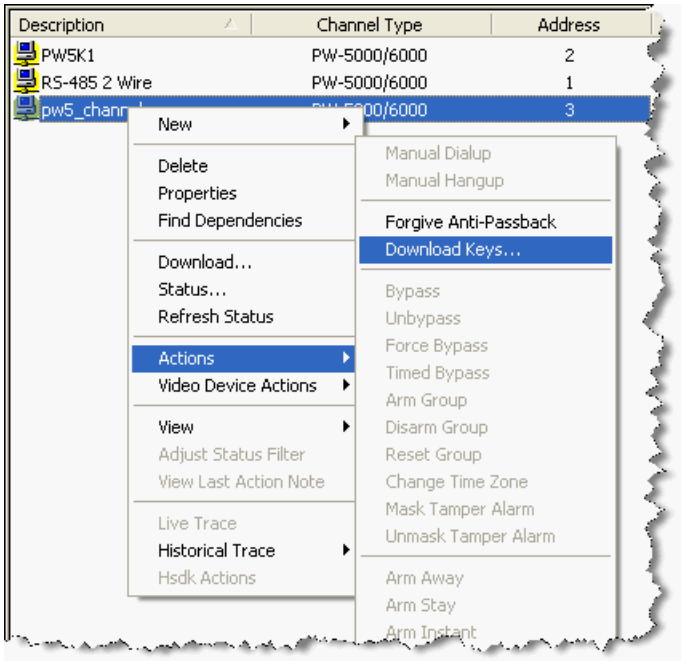
Icon	Description
	Channel is on-line and communicating via 256-bit encryption.
	Channel is off-line or not communicating via 256-bit encryption.
	Panel is on-line and communicating via 256-bit encryption.
	Panel is off-line or not communicating via 256-bit encryption.
	Channel is on-line and communicating via 128-bit encryption.
	Channel is off-line or not communicating via128-bit encryption.
	Panel is on-line and communicating via 128-bit encryption.
	Panel is off-line or not communicating via 128-bit encryption.

To perform the encryption key download:

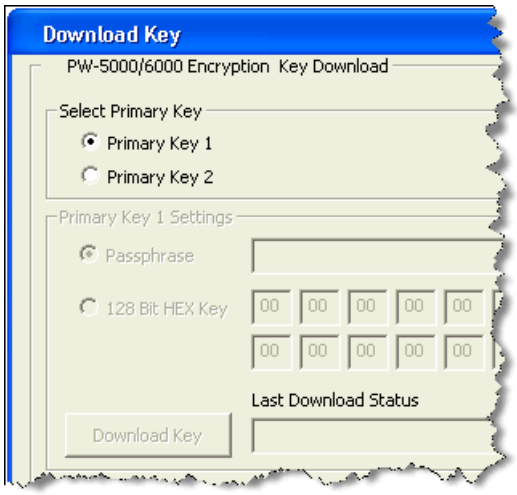
1. In Hardware Configuration, click **Channels** in the appropriate site to display the configured channels for that site in the right-hand pane.



2. Right-click the appropriate channel and select **Actions > Download Keys** to display the Download Key dialog box.

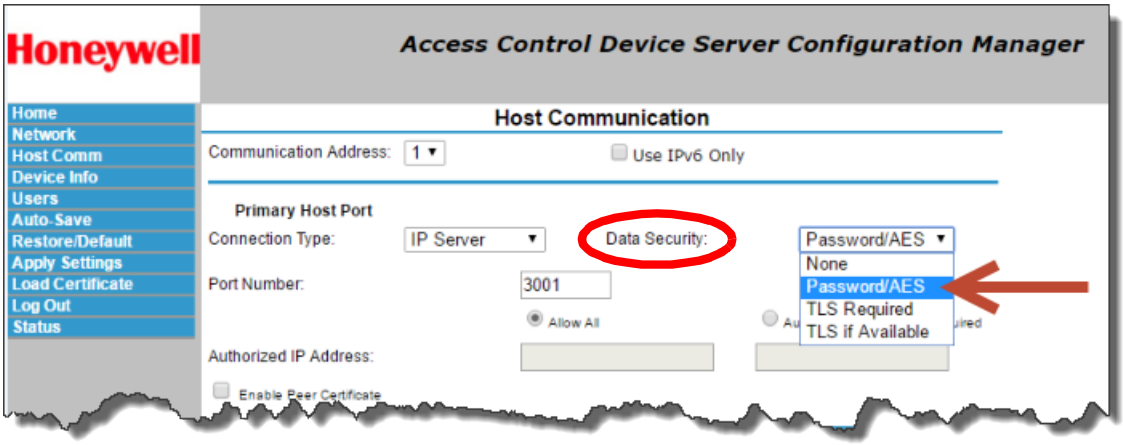


The Download Key dialog box appears:



3. Select the Primary Key(s) you desire and click the **Download Key** button. The download status appears in the Last Download Status box.

Note: Encryption must be enabled both in Pro-Watch and in the panel through the panel's web-based configuration manager. As shown below, in the panel **Host Communication** screen of the **Access Control Device Server Configuration Manager**, select the "**Password/AES**" option for the **Data Security** field to enable encryption in the panel:



To learn more about enabling panel encryption, please refer to the user guide of the individual panel.

8.4 Viewing and Editing Dependencies of a PW-5000/PW-6000/PW-6K1ICE Channel

Please refer to How to View and Edit Dependencies of a Channel, page 51.

8.5 Deleting a PW-5000/PW-6000/PW-6K1ICE Channel

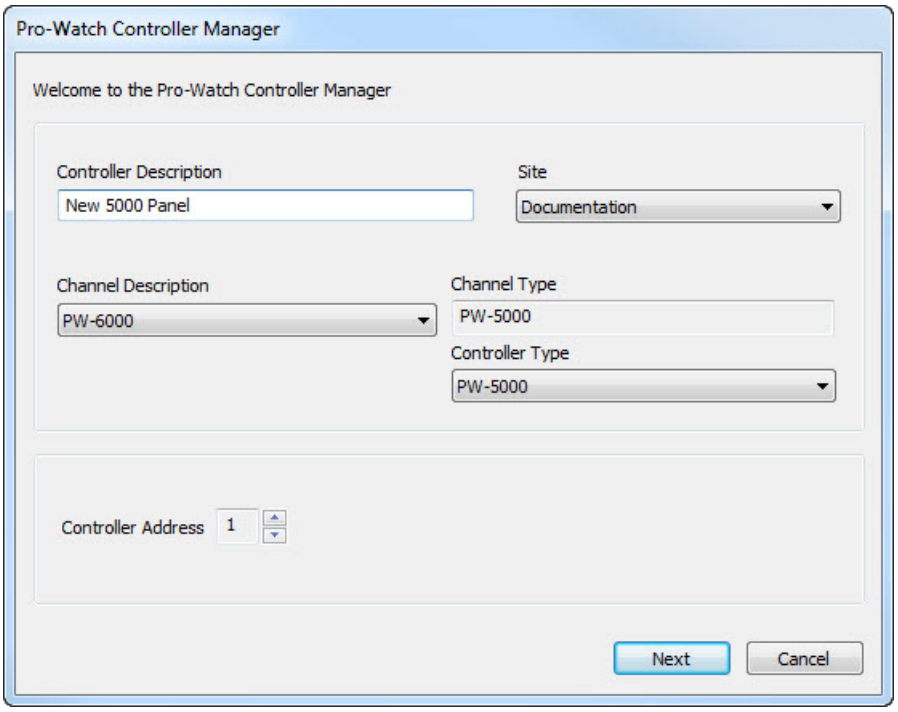
Please refer to How to Delete a Channel, page 51.

8.6 Adding a PW-6000/5000/3000 Panel

Note: The following steps assume that the Hardware Use Wizard is granted. The Hardware Use Wizard is turned on by default. See Turning the User Wizard On and Off, page 4.

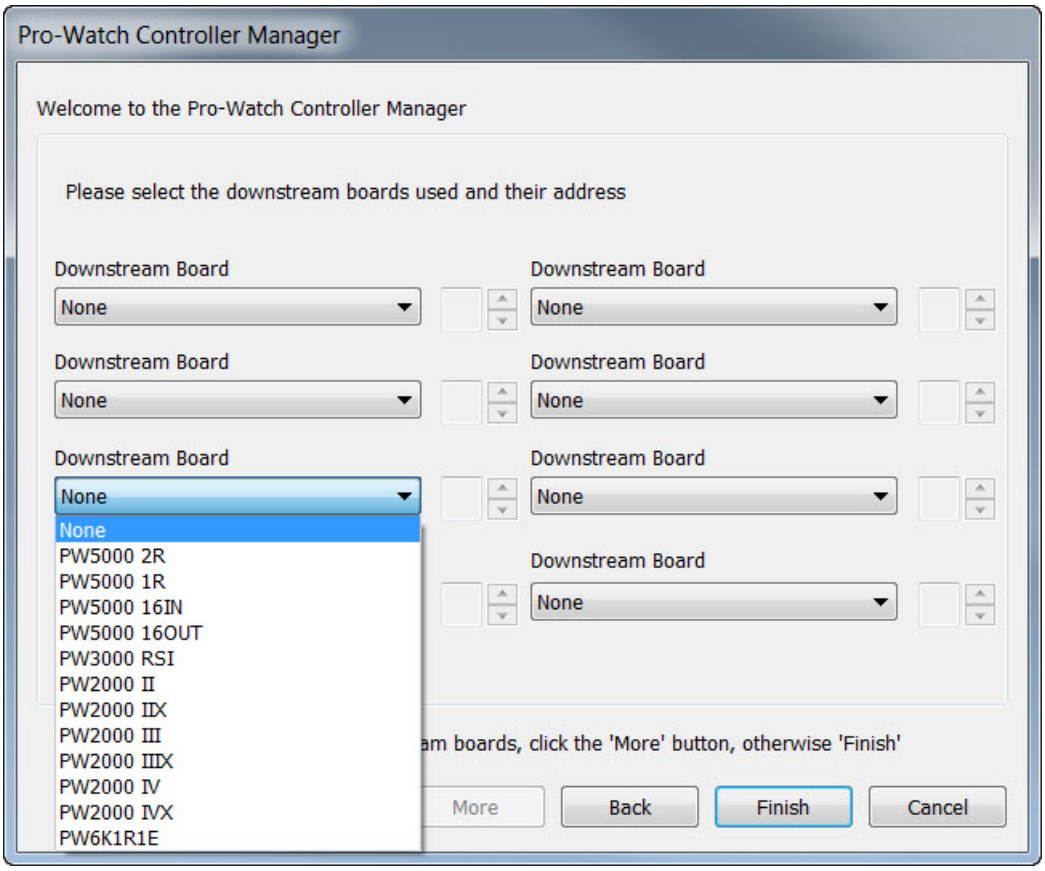
To add a PW-6000/5000/3000 panel:

1. Click the **Add New Control Panel** link on the **Manage Your Server** screen (the default home screen).
2. In the Controller Description field, enter a description that identifies the controller.



3. In the **Channel Description** field, select the channel you have created for this panel from the drop-down list.

4. In the **Controller Type** field, select the appropriate **Controller Type** (PW-3000, PW-5000 or PW-6000) from the drop-down list.
5. Click **Next** to display the **downstream board** dialog box:



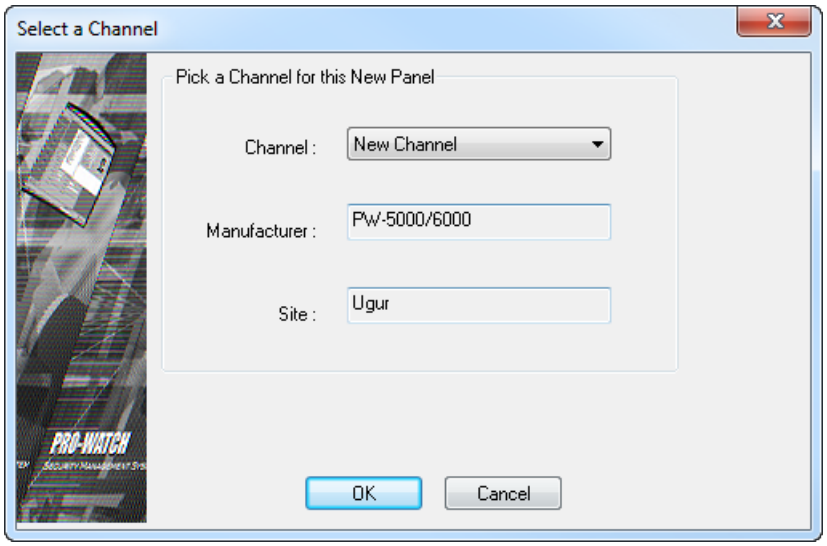
6. Select the appropriate downstream board(s) from drop-down menus.
7. Click **Finish** to complete the panel configuration.

To add a PW-6000/5000/3000 panel without the Hardware Manager wizard:

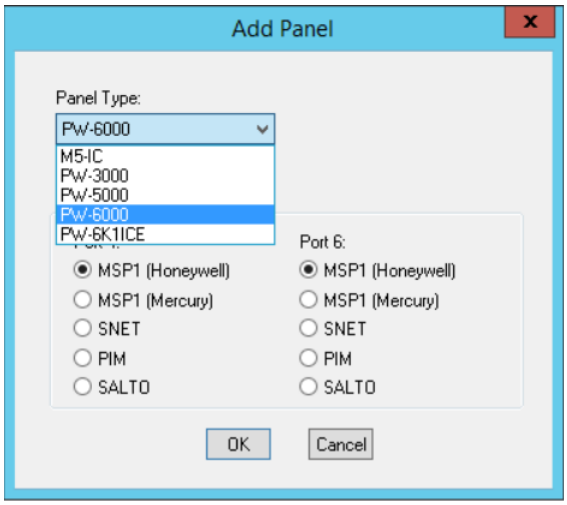
Note: For more information on the User Wizard, see *Turning the User Wizard On and Off*, page 4. Unless the User Wizard is turned off by the user, it is displayed by default every time the user wants to create a new Panel or Logical Device.

1. In the **Hardware Configuration** module, select a **Site** and a **Channel**.

2. Right-click on a **Channel** icon to display the pop-up menu. Select **New > Panel t**o display the **Select a Channel** dialog box:



3. Click **OK** to display the **Add Panel** dialog box. Here are the **panel options** available:

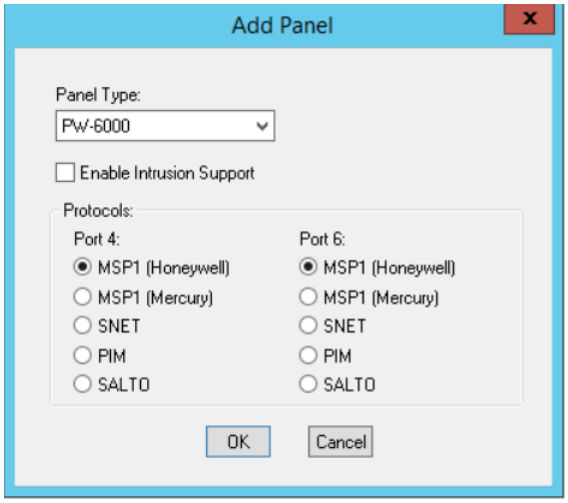


4. If you select **PW-6000** panel, go to the "PW-6000 Controller Panel Option" section.

5. If, on the other hand, you select **PW-3000**, **PW-5000**, or **PW6K1ICE**, go to the "PW-5000 and PW-3000 Controller Panel Options" section.

8.6.1 PW-6000 Controller Panel Option

If at the **Add Panel** screen you have chosen **PW-6000** from the **Panel Type** drop-down list, proceed as follows:

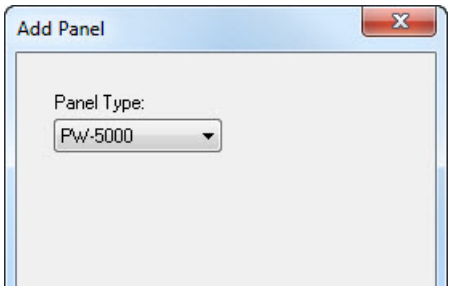


1. Select the "**Enable Intrusion Support"** check-box to enable intrusion support.
2. Select the appropriate **Protocol** for **Port 4** and **Port 6**. For both ports, select:
   - SALTO option-button if you are using SALTO routers.
   - SNET option-button if you are using SNET readers.
   - PIM option-button if you are using Ingersol-Rand PIMs.
   - MSP1 (Honeywell) or MSP1 (Mercury) option-button if you have any subpanels that use either the Mercury or Honeywell protocol.

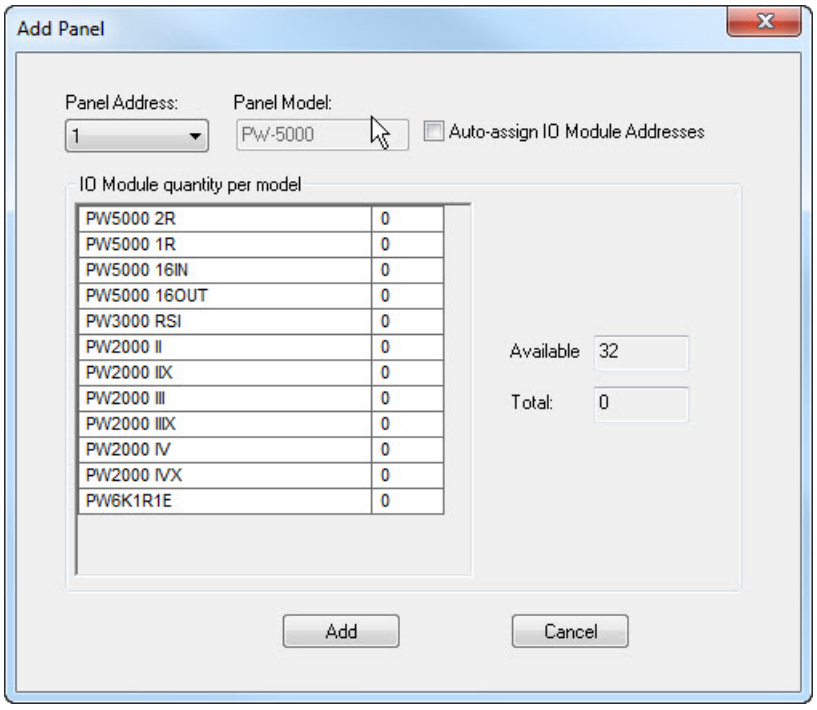
3. Click **OK** to display the **Add Panel** dialog box and continue with **Step 1** in the "PW-5000 and PW-3000 Controller Panel Options" section (below) since the rest of the steps are identical.

8.6.2 PW-5000 and PW-3000 Controller Panel Options

If at the **Add Panel** screen you have chosen **PW-3000** or **PW-5000** from the **Panel Type** drop-down list, proceed as follows

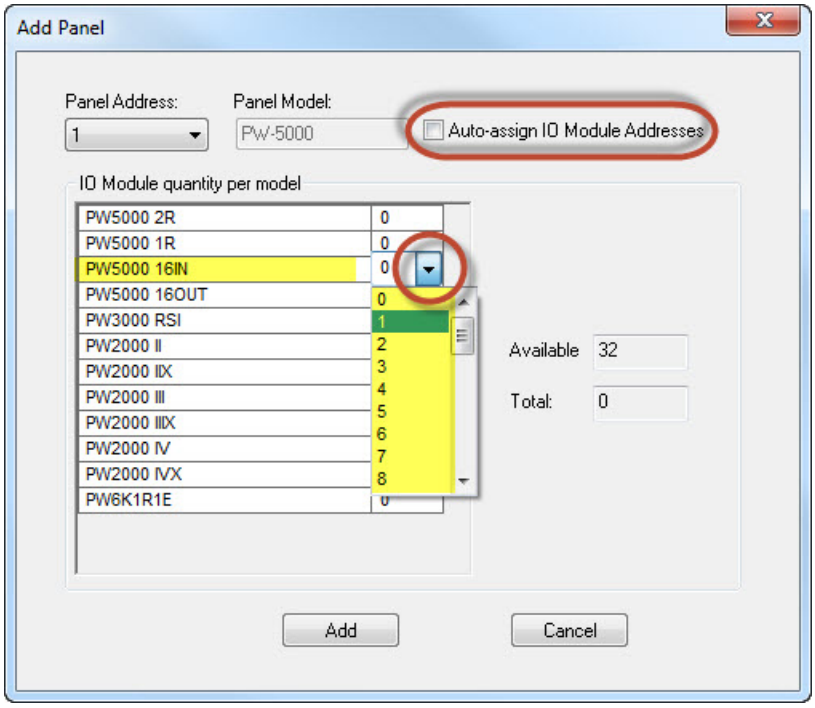


1. Click **OK** to display the **Add Panel** dialog box:

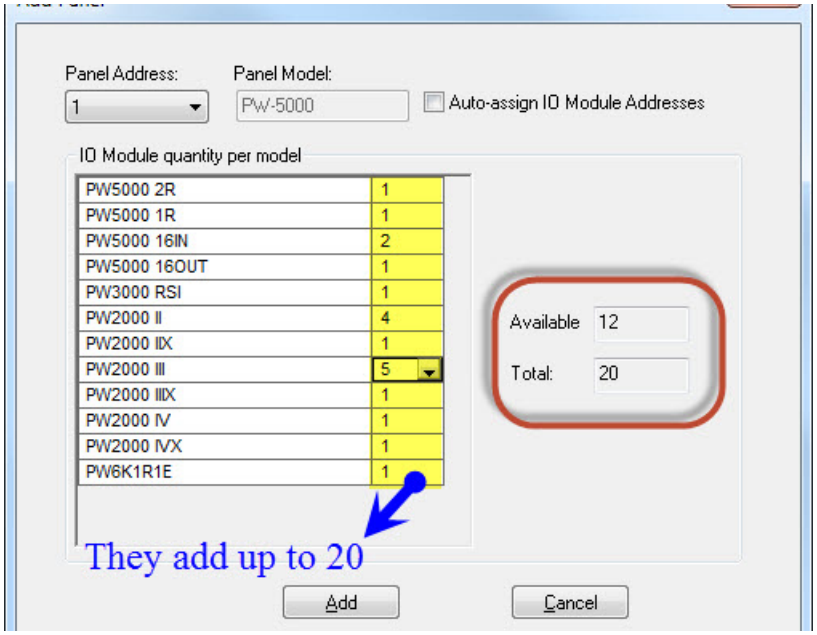


2. Select appropriate quantities for the IO modules listed. The total cannot be more than 32. **For example**, if you would like to select the number of IO subpanels to attach to the non-PW-6000 panel

(PW-5000 in this example), click the quantity cell right after the subpanel's name and select a quantity from the drop-down list:



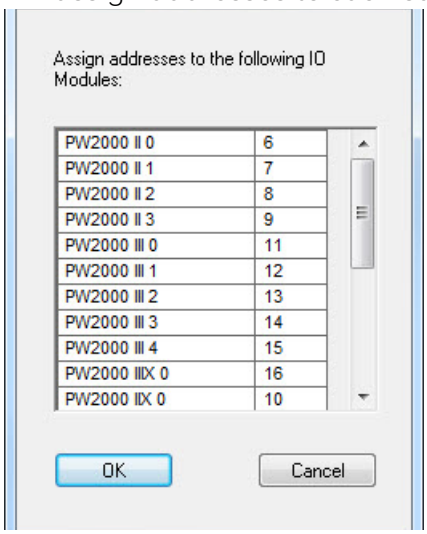
3. To have the Pro-Watch automatically assign addresses to the selected IO modules, select the "**Auto-assign IO Module Addresses**" check-box.
4. For the purposes of this illustration, we have selected one of each from all available IO modules:



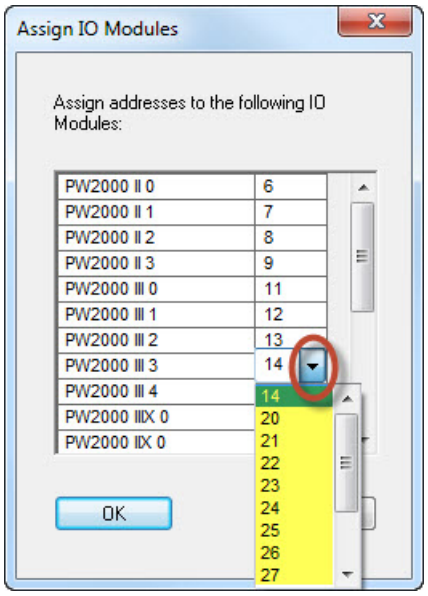
As you can see, the system automatically deducted the number of IO

modules selected (20) and deducted it from the number of total possible subpanels, which is 32.

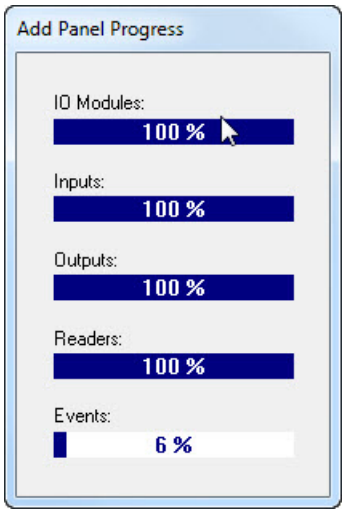
5. Click **Add** to display the **Assign IO Modules** dialog box where you can assign addresses to each subpanel:



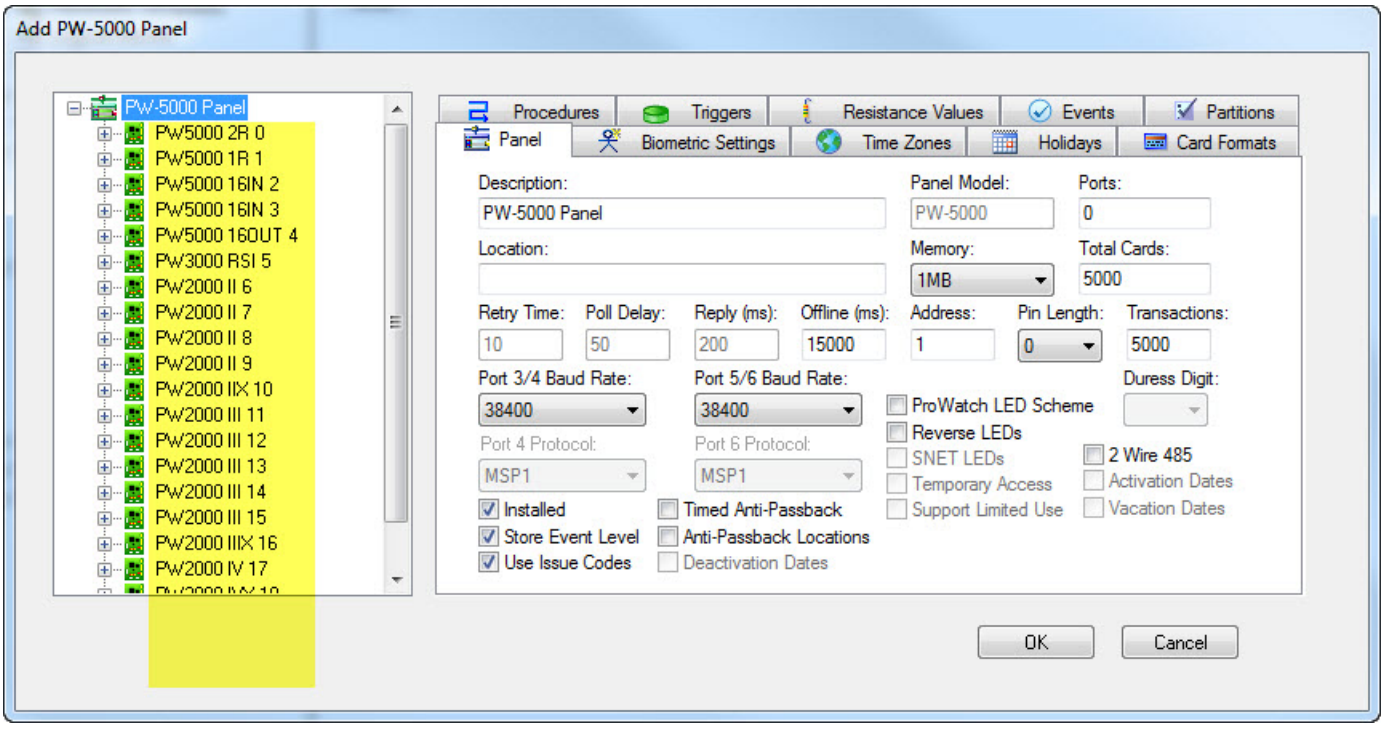
6. If you do not like the addresses assigned by default to these subpanels, click the quantity cell following the name of each subpanel and assign a new address from the drop-down list of available addresses:



7. Click **OK** to start adding the panels; a process during which the system will display the following **progress bars** box:



8. When the addition process is completed, the Pro-Watch will display the **Add PW-5000 Panel** (or **Add PW-3000 Panel** or **Add PW6K1ICE Panel**) dialog screen:



Note how all the previously selected IO modules (subpanels) are listed under the PW-5000 (or **PW-3000 Panel**) Panel.

9. Click **OK** to finish the panel-adding process and return to the “Add PW-xxxxx Panel” (either for PW-5000 or PW-3000) screen.

8.6.3 Configuring PW-6000/5000/3000 Panel Tabs

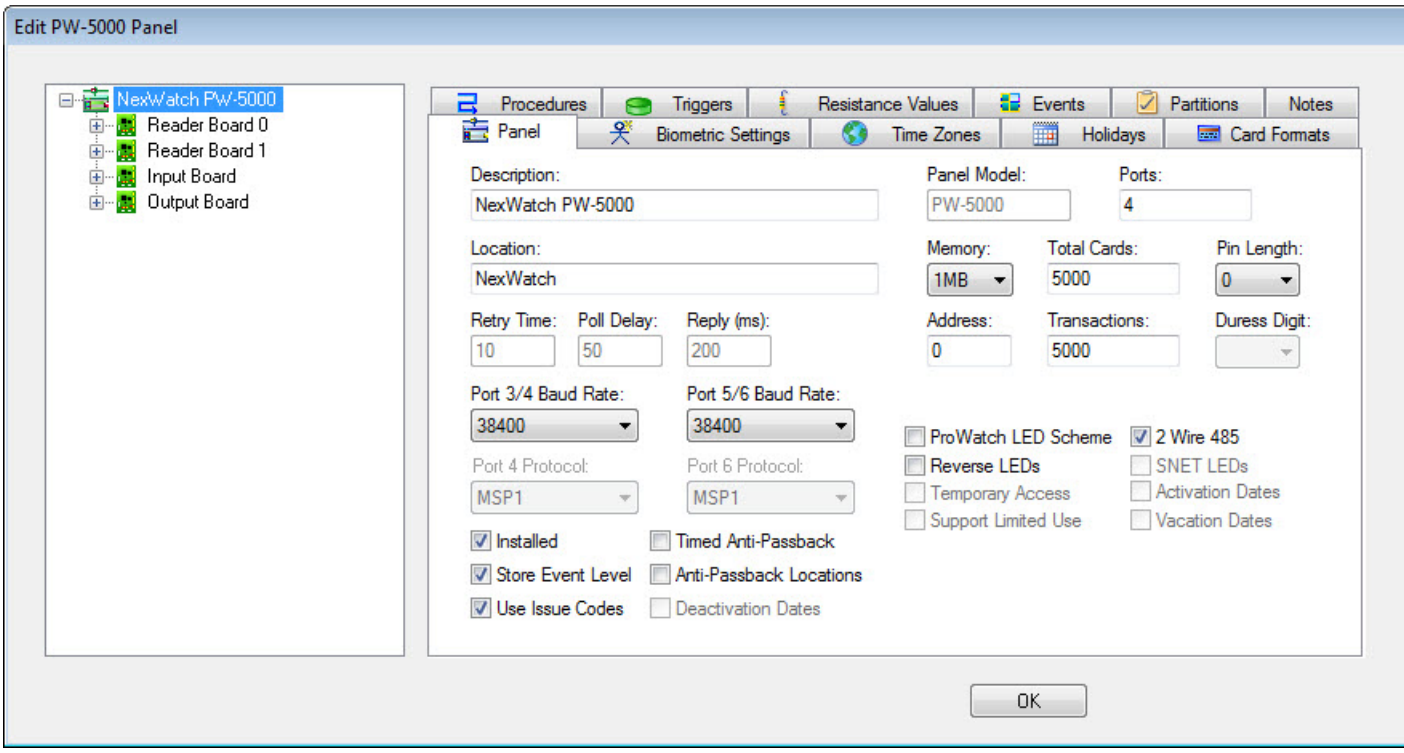
See the following tab list and tab sections for the configuration information:

ADD A PW-6000/5000/3000 PANEL TABS LIST

- "Panel Tab".
- "Biometric Settings Tab".
- "Time Zones Tab".
- "Holidays Tab".
- "Card Formats Tab".
- "Procedures Tab".
- "Triggers Tab".
- "Resistance Values Tab".
- "Events Tab".
- "Partitions Tab".

8.6.3.1 Panel Tab

The Panel tab includes basic hardware settings for the panel. This tab allows you to set the panel memory, transactions, and other panel related features.



Use the following field descriptions to complete the Panel tab:

Field	Description
Description	Provides the description of the panel as defined by the user.
Panel Model	Identifies the panel model.
Ports	Defines the number of downstream ports on the panel.
Location	Identifies the location of the panel as defined by the user.
Memory	Identifies the total memory on the panel.
Total Cards	Defines the amount of cards that can be in the panel.
Retry Time (sec)	Defines the panel/host connection retry time. A read-only field.
Poll Delay (ms)	Defines how long for the panel to wait between polls. A read-only field.

Field	Description
Reply (ms)	Defines how long the panel should wait for a reply. A read-only field.
Address	Identifies the address of the panel.
PIN Length	Assigns the PIN characters that must be used when creating a PIN number for cardholders. This number should be the same number specified for a PIN length when creating a Card (see "Adding a Card" in Chapter 2, "").
Transactions	Defines how many transactions to buffer in the panel. Be careful with the number of expected transactions entered into the "Transactions" field of PW-6000 panel's editing screen since this number has implications for buffering events when the panel goes offline. If this number is too small, some events may not get buffered while the panel is offline. IMPORTANT: The number of transactions entered into the "Transactions" field of PW-6000 panel's editing screen is an approximate number. The panel allocates memory for offline buffering on the basis of the number of expected transactions and the (assumed) "average" size of each transaction. If the transactions are larger than the average, it's possible that the memory allocation may not be enough to buffer all the offline transactions.
Port 3/4 Baud Rate	Defines the baud rate for ports 3 and 4. Note that if you are configuring a PW-6000 panel for S-Net communications, you must select 9600 in this field.
Port 4 Protocol	Specifies the communications protocol for port 4.
Port 5/6 Baud Rate	Defines the baud rate for ports 5 and 6.
Installed	Required for the panel to be installed and operational.
Store Event Level	Causes the panel to store the user level parameter as defined in the PW tab in card configuration.
2 Wire 485	Required for hardwire communication through a 485 converter.
Use Issue Codes	Enables the panel to use card formats that check the issue level of a card.

Field	Description
Timed Anti-Passback	Enables timed anti-passback. When anti-passback is timed, Pro-Watch grants access by the same card (without an exit) for a second entry after a specified time period has elapsed. Note that you must also set the Logical Device (in the Logical Device "Anti-passback Settings Tab") for successful anti-passback operation. See also "DBC - Area" in Chapter 29.
Temporary Access	This function is currently not supported.
Activation Dates	This is the Card Issue Date. To enable this function, the "Allow panel driven card activation/deactivation" check-box must be selected in the Server Options screen, Server Options tab. See Chapter 5, Server Options.
Deactivation Dates	This is the Card Expire Date. To enable this function, the "Allow panel driven card activation/deactivation" check-box must be selected in the Server Options screen, Server Options tab. See Chapter 5, Server Options.
Pro-Watch LED Scheme	Identifies an LED scheme for readers.
Reverse LEDs	Defines the LED scheme as reversed from the normal LED scheme.
S-Net LEDs	Specifies an LED scheme for S-Net-connected readers. Note that if you are configuring LED emulation on a PW-6000, you must select the S-Net LED checkbox. This selects the following scheme: • Normal/Locked Mode = Red • Door Unlocked = Green • Waiting for PIN = amber
Anti-Passback Locations	Enables anti-passback operation in Areas. See "DBC - Area" in Chapter 29.
Support Limited Use	This function is currently not supported.
Vacation Dates	This function is currently not supported.

Note: If you edit the Panel properties and change the panel database, you must manually re-initialize and download the panel. Follow these steps:

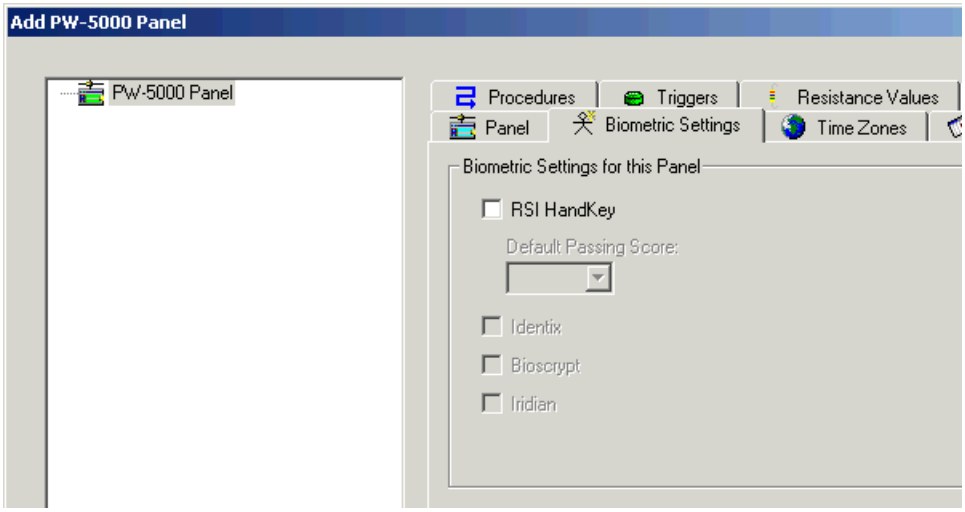
1. Click **Panels** under the appropriate Site folder in the Hardware Configuration tree to display the panel icon.
2. Right-click the panel's icon and select **Download**.
3. De-select **Download System**.
4. Select **Initialize**.

5. Click **Download** to re-initialize the panel. Note that this step only re-initializes the panel.
6. When the panel icon re-appears, right-click the icon and select **Download**.
7. Select **Download System** and **Download Cards**.
8. Click **Download** to download the newly-configured panel.

For more information on downloading panels, see Panel Download, page 59.

8.6.3.2 Biometric Settings Tab

The Biometric Settings tab enables you to configure the panel for the Pro-Watch biometric hand geometry reader. This reader grants access by a geometric scan of the badge holder's hand as well as by keypad. See Chapter 62, *Biometric Reader Configuration* for more information about the biometric hand geometry reader.



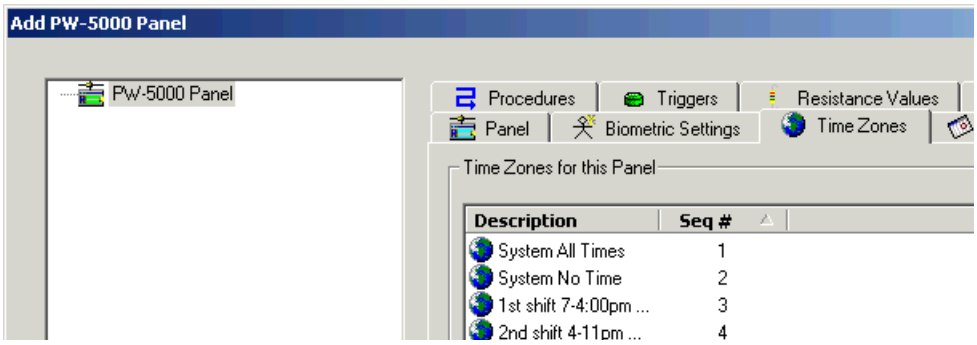
Use the following field descriptions to complete the Biometric Settings tab:

Field	Description
RSI Handkey	Indicates that the panel will support a biometric hand geometry reader.
Default Passing Score	Indicates the score a hand reading must receive before the biometric hand geometry reader grants access. It is recommended that you leave the number at 100.
Identix	N/A.
Bioscript	N/A.

Field	Description
Iridian	N/A.

8.6.3.3 Time Zones Tab

The Time Zones tab enables you to add time zones to the panel; only the times zones that have been added to the panel can be applied to panel and reader fields:



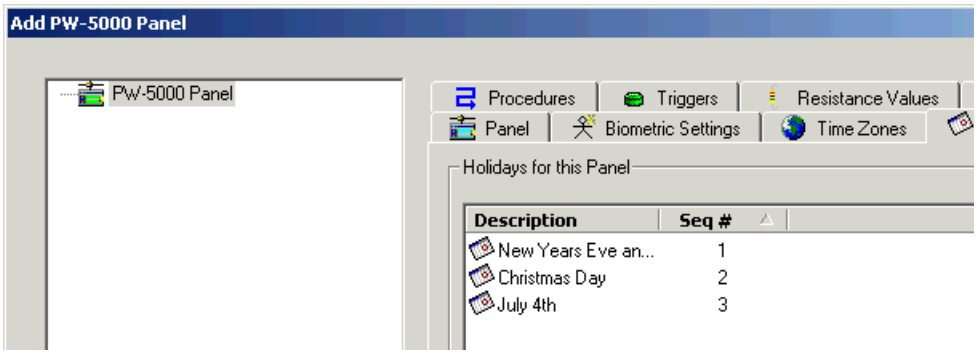
To add a time zone to the panel:

1. Click **Add** to display the **Time Zones** dialog box.
2. Select the time zone and then click **OK**.
3. To add a new time zone, click **Add**.
4. To edit an existing time zone, select it from the list and click **Edit**.
5. To delete an existing time zone, select it from the list and click **Delete**.
6. Click **OK** again at the Select Time Zone dialog box.

For more information on configuring time zones, see "DBC - Time Zones" in Chapter 57.

8.6.3.4 Holidays Tab

Holidays enable you to edit normal Time Zone behavior on specific days. Holidays are assigned to time zones.



To add a holiday to the panel:

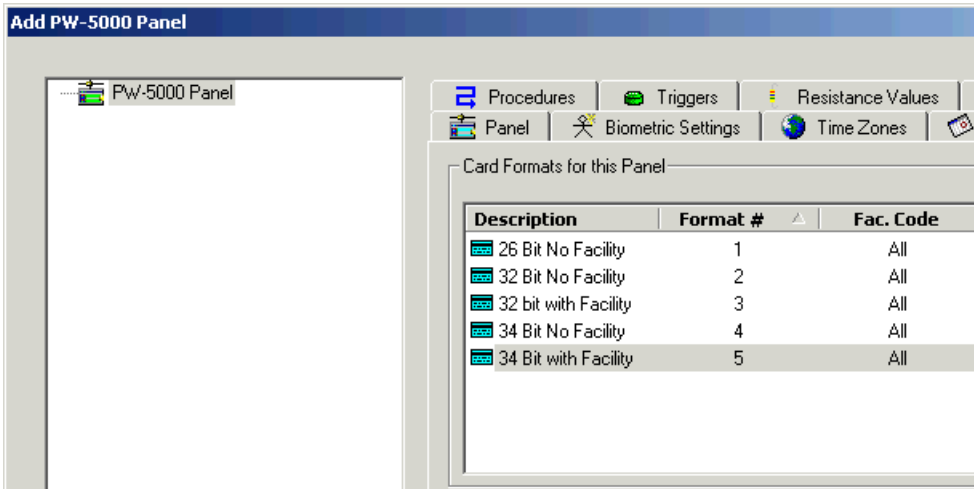
1. Click **Add** to display the Select Holiday dialog box.
2. Click the icon next to the Holiday field.
3. Click **Define**.
4. Select the holiday and click **OK**.
5. Click **OK** again at the Select Holiday dialog box.

If the holiday you want does not appear in the dialog box you can create a new time zone. Click **Add** on the Select Holiday dialog box.

For more information on configuring holidays, see "DBC - Holidays" in Chapter 49.

8.6.3.5 Card Formats Tab

A card format tells the panel how to determine the card number. You must add the card format to a card before a reader can read the card. Valid card formats are defined in Database Configuration. See "DBC - Card Formats" in Chapter 35.

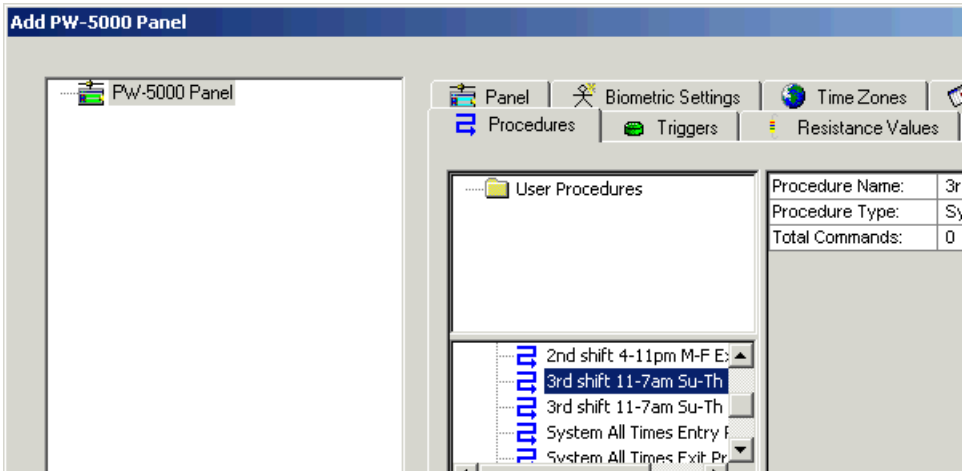


To add a Card Format to the panel:

1. Click **Add** to display the Select Card Format dialog box.
2. Click the icon next to the Card Format field.
3. Click **Define**.
4. Select the desired Card Format and click **OK**. Note that if you are adding a Card Format to support S-Net reader communications with a PW-6000 panel, you must first create the format. To do this, go to Database Configuration > Card Format tab, create a new Card Format using the PW-5000 Wiegand format type. See "Adding or Editing a Non PW2000 Card Format" on page 5 for details.
5. Select the **Format Number** from the drop-down list.
6. Enter the **Facility Code** or select the **All Facility Codes** check box. Note that facility codes are coded at time of manufacture.
7. Click **OK**.

8.6.3.6 Procedures Tab

The Procedures tab displays the user and system procedures assigned to the panel in the event of a trigger. System procedures are coded and cannot be edited or deleted.



User procedures perform customized panel functions. For example, a procedure allows you to define the action upon a particular trigger. See "Triggers Tab" for more information on configuring triggers.

To add procedures:

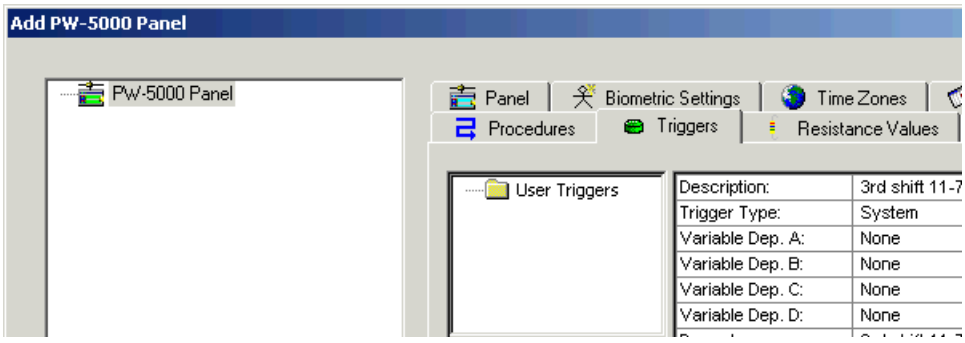
1. Right-click **User Procedures** and select **Add Procedure**.
2. To add a command to the procedure, right-click on the new procedure and select **Add Command**.

3. Click the **Command Type** field to display the drop-down command type list.
4. Select the type of command.
5. Edit the command parameters by clicking on the parameter fields and selecting parameter values from the drop-down lists.
6. Repeat steps 2 through step 5 to add any additional commands to the procedure.
7. Click **OK** to accept the procedure.

Note: Also see PW-5000/6000 Interlocks Tab, page 34 under Hardware Templates or "Adding a Logical Device".

8.6.3.7 Triggers Tab

The Triggers tab displays the user and system triggers that invoke the panel's procedures. See "Procedures Tab" for more information on configuring procedures. System triggers are coded and cannot be edited or deleted.



To configure triggers:

1. Right-click **User Triggers**, and select **Add Trigger**. The trigger appears in the User Triggers tree.
2. Select the created trigger in the User Triggers tree to display the trigger configuration box. This box displays the following

configuration elements for the trigger. Note that transaction Codes will vary depending on the Transaction Type chosen:

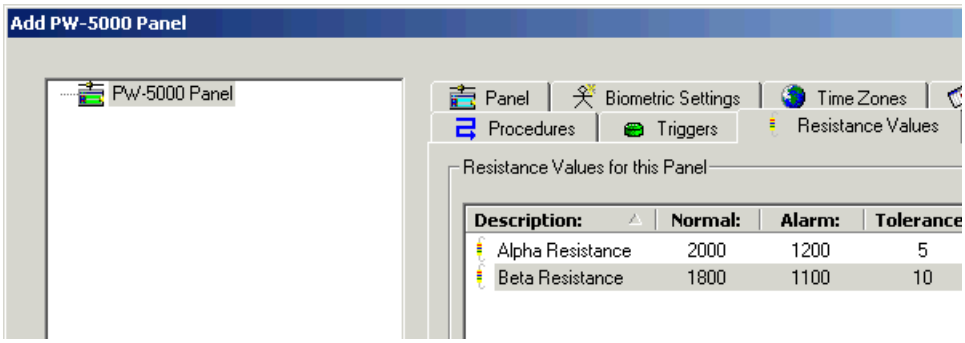
Field	Description
Description	Provides the description of the trigger as defined by the user.
Trigger type	Defines whether the trigger is user or system created.
Variable dependencies	Allows multiple input conditions and cascading triggers.
Procedure	Defines the Procedure to initiate in the event the trigger initiates.
Procedure command	Defines the action to be performed.
Time zone	Defines the time zone in which the trigger is enabled.
Source type	Defines the source of the event.
Transaction type	Defines the trigger type.
Transaction code	Defines the individual attributes of the trigger.

3. Configure the trigger's parameters listed in step 2 by clicking the parameter field to display the drop-down list and selecting field values.

Note: Also see PW-5000/6000 Interlocks Tab, page 34 under Hardware Templates or "Adding a Logical Device". PW-5000 Interlocks will also create user triggers and procedures.

8.6.3.8 Resistance Values Tab

This tab displays the default resistance values. Applicable for the panel's supervised inputs, resistance values determine what the resistance is going to be for the four states (normal, alarm, short, open). Open and short states are defined as 0 ohms and infinite.



*To **add** a set of resistance values to the panel:*

1. Click **Add** to display the Resistance Values dialog box.
2. Use the following field descriptions to create or edit the resistance values:

Field	Description
Description	Provides the description of the resistance value as defined by the user.
Normal	Defines the resistance for normal.
Alarm	Defines the resistance for alarm.
Tolerance	Determines the fluctuation +/- a percentage of the normal and alarm values.

3. Click **OK** to accept the resistance value.

To edit a set of resistance values:

1. Click the resistance values entry (or select the entry and click **Edit**) to display the Resistance Values dialog box.
2. Use the table presented above to edit the fields of the Resistance Values dialog box.

8.6.3.9 Events Tab

The Events tab displays the default event types that are applicable to the PW-6000/5000/3000 panel.

To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears.

For more information on editing events, see "HW Config - Edit Point".

8.6.3.10 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. For information about creating a partition, see "DBC - Partitions" in Chapter 53. Use this function to assign or delete an already-created partition to the panel:

To assign a partition to the panel:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition.
3. Click **Add**.

To delete a partition from the Partitions List dialog box:

1. Select the partition.
2. Click **Delete**.

After completing each tab within the panel, you will need to save the panel configuration.

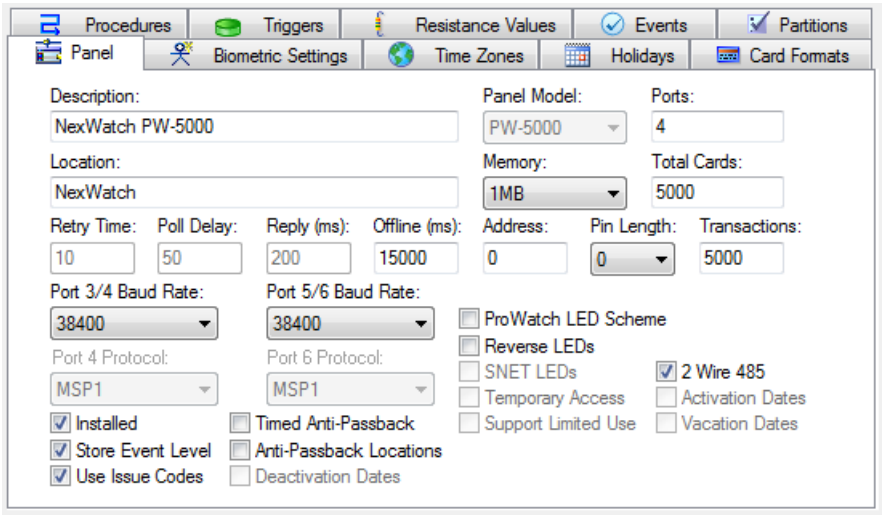
To save the panel configuration:

Click **OK** at the Add [Panel Name] Panel dialog box.

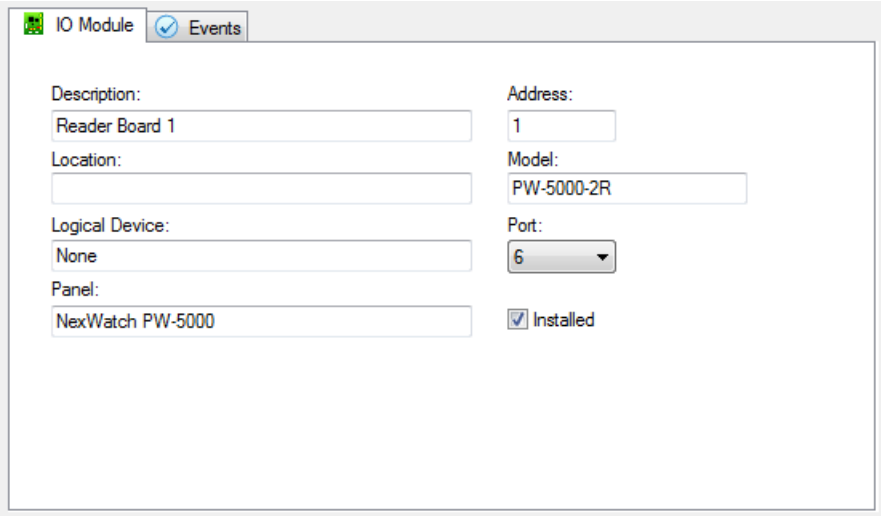
8.7 Editing a PW-6000/5000/3000 Panel

To edit a panel:

1. In the Pro-Watch Hardware Configuration tree, click the site to which the panel is assigned.
2. Click the Panel's subdirectory. The icons of the existing panels appear in the right pane of the window.
3. Right-click the panel you want to edit and select **Properties**. The Edit [panel name] Panel dialog box appears. This box lists the I/O modules configured for each panel and displays nine information tabs with which you will configure each panel.



4. Configure the I/O modules listed in the panel tree list in the Add [panel name] Panel dialog box.
   a. Click the first I/O Module listed in the panel tree list to display the I/O Module and Events configuration tabs.



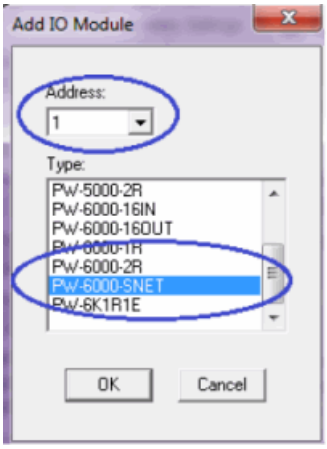
   b. Use the following field descriptions to complete the I/O Module tab:

Field	Description
Description	Provides a description of the I/O Module.
Location	Identifies the location of the I/O Module.
Logical Device	Identifies the name of the Logical Device.
Panel	Identifies the panel type to which the I/O module has been added.
Address	Identifies the address of the I/O Module. Note that S-Net readers being configured with a PW-6000 must have the same address (set by a DIP switch) as the I/O address set in this field.
Model	Identifies the I/O Module model type.

Field	Description
Port	Defines which port the I/O Module is connected to on the panel. Note that when defining an S-Net reader on a PW-6000, set the Port number to the same number set in the Ports field on the Panel tab (see step 3 of this procedure). This number should either be 4 or 6 when configuring an S-Net reader on a PW-6000; port 4 in this field configures port 2 on a PW-6000 board, and port 6 in this field configures port 3 on the PW-6000 board..
Installed	Required to install the I/O Module.

c. Click the Events tab to display the events that can support this input/output module.

d. Either double-click the event you want to define, or select the event and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point". Note that you can also add and delete input/output modules. To add an input/output module, right-click anywhere in the panel tree and select **Add IO Module**. You can also add and delete input/output modules. To add an input/output module, right-click anywhere in the panel tree and select **Add IO Module** to display the Add IO Module box.



In the Address field, enter the same address that is set by DIP switches on the I/O module, and select the I/O module type. If the I/O module is an S-Net reader, the address cannot be 0. It is recommended that you use 1 for the address of an S-Net reader, both in this Add IO Module box and with the DIP switches on the

reader.

To delete an input/output module, right-click the module you want to delete and click **Delete IO Module**.

5. Display the panel's configuration tabs by clicking the panel in the panel tree list.

6. Complete each tab to configure the panel. See the following tab list and the corresponding tab sections in "Adding a PW-6000/5000/3000 Panel" for the configuration information:

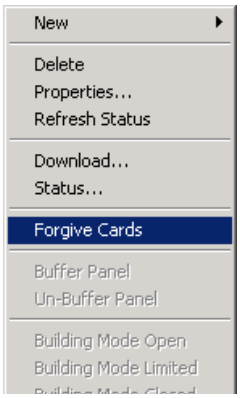
   EDIT A PW-6000/5000/3000 PANEL TABS LIST

   - "Panel Tab".
   - "Biometric Settings Tab".
   - "Time Zones Tab".
   - "Holidays Tab".
   - "Card Formats Tab".
   - "Procedures Tab".
   - "Triggers Tab".
   - "Resistance Values Tab".
   - "Events Tab".
   - "Partitions Tab".

Note: The PW-6000/5000/3000 Panel allows you to forgive anti-passback (see "DBC - Area" in Chapter 29) for all cards.

To forgive anti-passback:

1. Select the panel from the Hardware Configuration window.
2. Right-click on the panel and select **Forgive Cards**:



8.8 Memory Warning for PW-6000

The user can get a “not sufficient memory” warning message for PW-6000 and PW-6101 panels depending on the number of access levels (i.e., clearance codes) selected in the Server Options screen (see Server Options Tab, page 8).

The warning message looks like this:

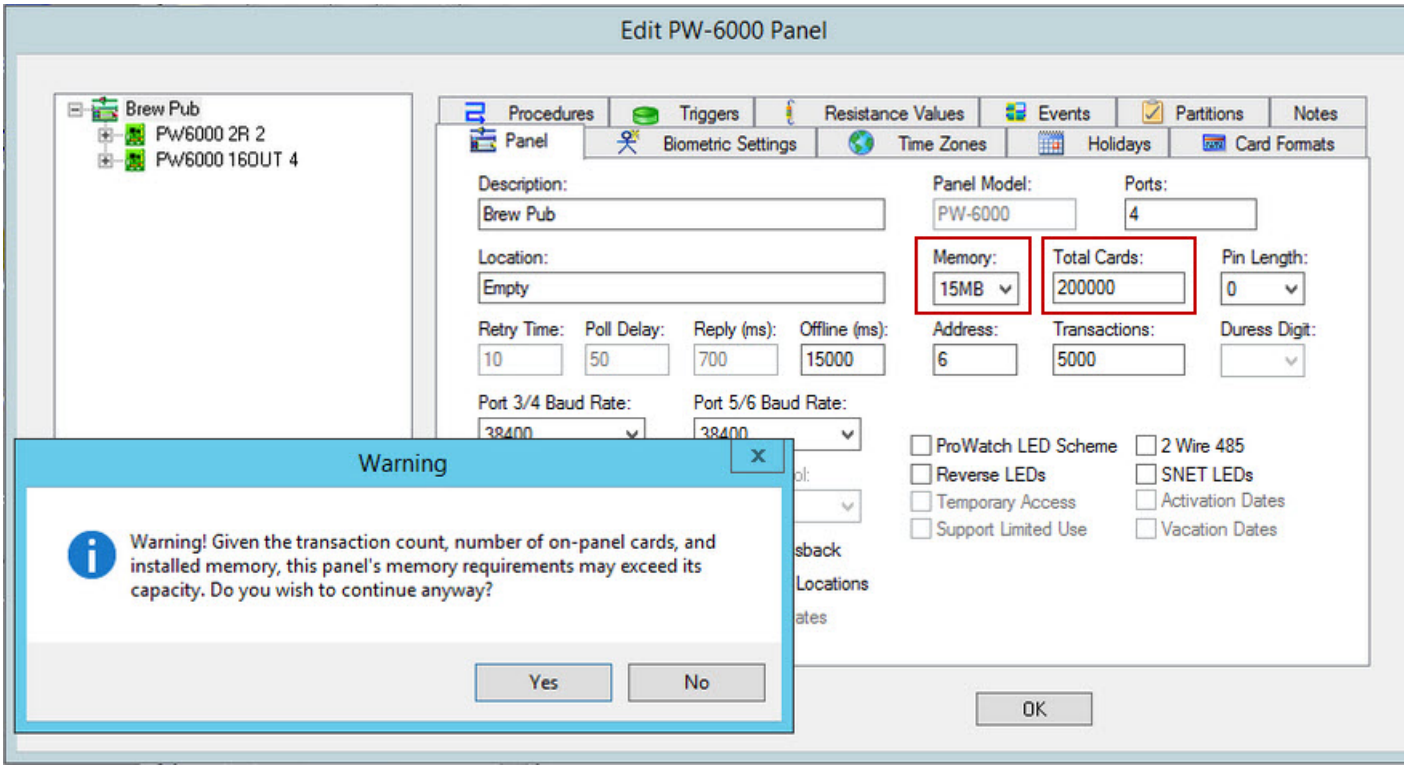


Figure 8-1 PW-6000 Memory Warning Message

Warning: If you click “Yes” you may lose data. We recommend you click the “No” command button.

8.8.1 “Why does this happen?”

This happens when an existing panel is switched from 12 to 32 access levels in the Server Options screen (see Server Options Tab, page 8).

For the PW-6000 panel, the default total number of cards is 200,000 and the default memory is 15 MB. These settings are sufficient when 12 access levels are selected. But when 32 access levels are selected, then the panel memory cannot accommodate that much extra data. Thus Pro-Watch issues the warning message you see in the above figure.

If 32 access levels option is selected for a new panel, the card number is automatically adjusted as 100,000 and thus a similar memory problem is averted.

8.9 Viewing and Editing Dependencies of a PW-6000/5000/3000 Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

8.10 Deleting a PW-6000/5000/3000 Panel

Please refer to How to Delete a Panel, page 53.

8.11 PW-6000/5000/3000 Elevators

The PW-6000/5000/3000 panel supports elevator configuration. A maximum of 128 floors may be assigned. Both elevator readers and elevator floor select readers are supported.

To configure elevators using the elevator reader device type:

1. Configure the hardware template. For more information, see Adding or Editing a Hardware Template, page 28.
    - In the Device Types tab of the hardware template, you must add one reader and an output for each floor up to 128 floors.
    - Configure the elevator reader device type and each output device type.
2. After configuring the hardware template, you must add the Logical Device to the panel. For more information, see "Adding a Logical Device". Each output must be assigned and addressed sequentially.
3. Upon assigning the first output, a message box will appear asking to assign hardware for all the elevator outputs.
    - If you click **Yes**, all outputs are assigned or addressed automatically.
    - If you click **No**, no outputs are assigned or addressed.

Note: The elevator readers control access to floors and do not record which floor the user chooses.

To configure elevators using the elevator reader (floor select) device type:

1. Configure the hardware template. For more information, see Configuring Hardware Templates, page 27.
    - In the Device Types tab of the hardware template, you must add one reader as well as one output and one input for each floor up to 128 floors.
    - Configure the elevator reader device type, each output device type, and each input device type.
2. After configuring the hardware template, you must add the Logical Device to the panel. For more information, see "Adding a Logical Device". Each output and input must be assigned or addressed sequentially.

3. Upon assigning the first output, a message box will appear asking to assign hardware for all the elevator outputs.
    - If you click **Yes**, all outputs are assigned or addressed automatically.
    - If you click **No**, no outputs are assigned or addressed.
4. Upon assigning the first input, a message box will appear asking to assign hardware for all the elevator inputs.
    - If you click **Yes**, all inputs are assigned or addressed automatically.
    - If you click **No**, no inputs are assigned or addressed.

Note: The elevator readers (floor select) control access to floors and record which floor the user chooses.

8.12 Overview - PW6K1ICE Panel

Pro-Watch supports the PW6K1ICE panel, a two-reader/one-door panel, to which a total of 16 PW6K1R1E boards can be connected. For additional PW6K1ICE panel configuration instructions, see the *PW6K1ICE Installation and Configuration Guide* (800-07985). For PW6K1R1E I/O board configuration instructions, see the *PW6K1R1E Input/Output Module Installation and Configuration Guide* (800-07986).

8.12.1 Background

The PW6K1ICE panel allows users to use onboard Reader Port 1 for 2-wire RS-485 multi-dropped devices, such as up to two (2) readers (e.g. OSDP) or up to eight (8) remote serial I/O devices. This would be in addition to the connections to any PW6K1R1E IP subpanels.

The remote subpanel devices are connected to Reader Port 1 of the PW6K1ICE through Power, CLK/TR+, DAT/TR-, and GROUND. Reader Port 2 of the PW6K1ICE can be used for a reader, but in software this will be treated as Reader 0.

To find more information about using the RS-485 downstream port on the PW6K1ICE please refer to section 8.14.

8.12.2 Subpanel Limits

- Up to eight (8) subpanels can be connected to Port 1 of the PW6K1ICE using RS-485.
- Up to sixteen (16) IP subpanels can be connected to Port 4 of the PW6K1ICE.

However, the total number of devices combined on the PW6K1ICE physical ports 1 and 4 cannot exceed 16. In other words, there is a subpanel maximum limit of 16 for the PW6K1ICE.

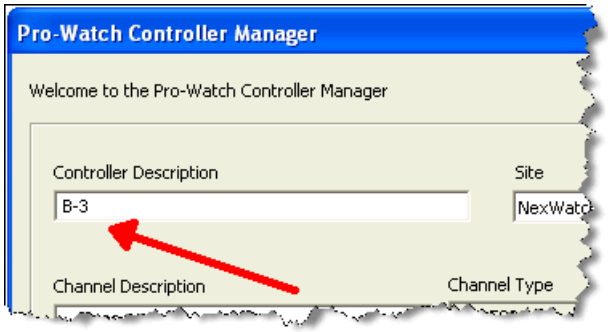
8.13 Adding a PW6K1ICE Panel

8.13.1 Adding PW6K1ICE with the User Wizard

To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 4.

Follow these steps:

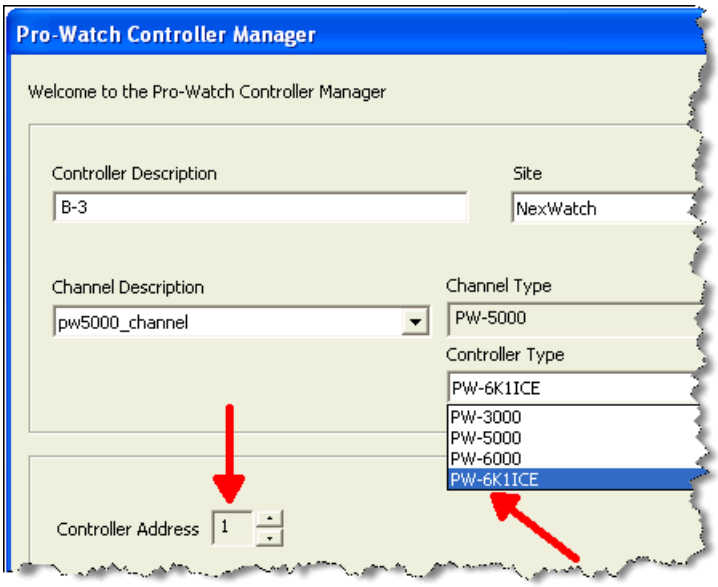
1. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
2. Select **New > Panel** to display the Pro-Watch Controller Manager dialog box.
3. In the Controller Description field, enter a name that will identify the panel.



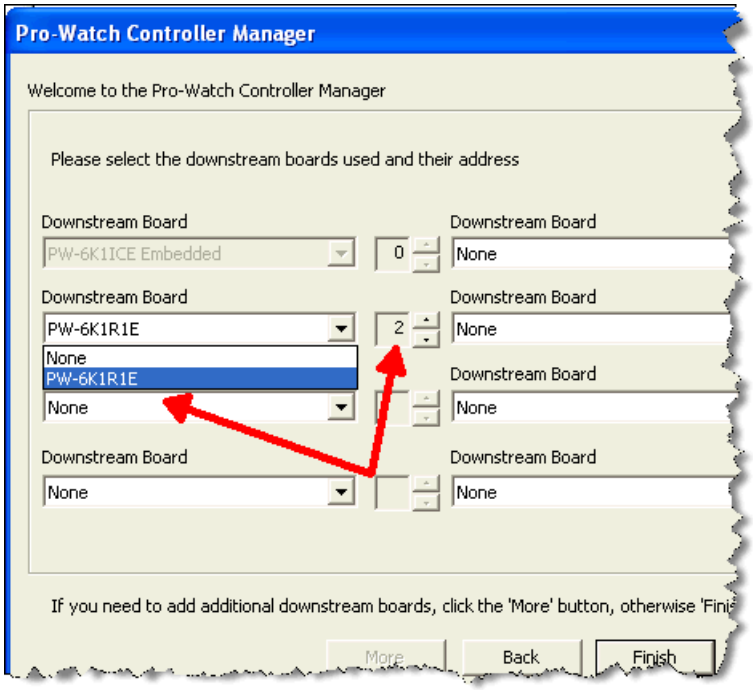
4. In the Channel Description field, select the channel you have created for this panel from the drop-down list and click **Next.**



5. In the Controller Type field, select PW6K1ICE.



6. Use the Controller Address toggle field to set the system address of the controller, and click **NEXT** to display the downstream board dialog box. In this box, you can configure one or more PW-6K1R1E downstream input-output boards for this panel. See the *PW-6K1R1E Input/Output Module Installation and Configuration Guide* (800-07986)for the description of the PW-6K1R1E input-output board.

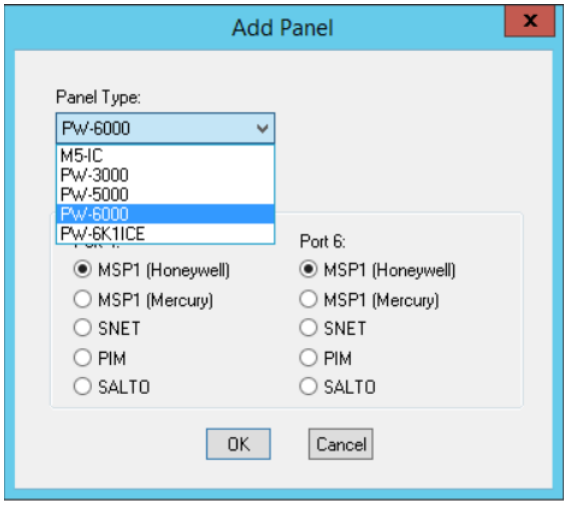


7. Select one or more PW-6K1R1E downstream boards for this panel. For each downstream board selected, use its adjacent toggle field to set the board's system address.
8. Click **Finish** to complete the panel configuration.

8.13.2 Adding PW6K1ICE without the User Wizard

Note: For more information on the User Wizard, see "Turning the User Wizard On and Off". Unless the User Wizard is turned off by the user, it is displayed by default every time the user wants to create a new Panel or Logical Device.

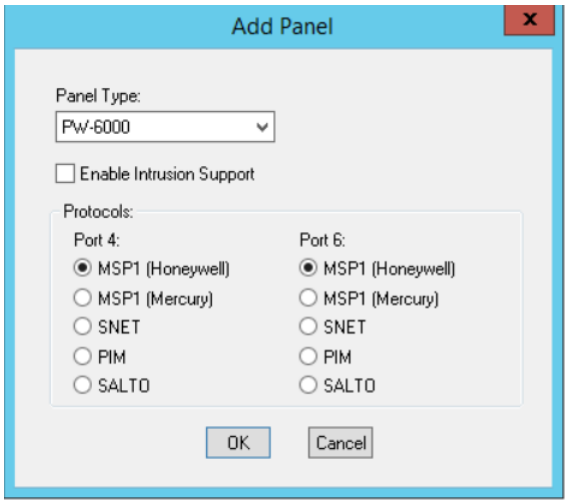
1. In the **Hardware Configuration** module, select a **Site** and a **Channel**.
2. Right-click on a **Channel** icon to display the pop-up menu. Select **New > Panel t**o display the **Add Panel** dialog box. Here are the **panel options** available:



3. If you select **PW-6000** panel, go to the "PW-6000 Controller Panel Option" section.
4. If, on the other hand, you select **PW-3000**, **PW-5000**, or **PW6K1ICE**, go to the "PW6K1ICE DS with RS-485 Downstream" section.

8.13.2.1 PW-6000 Controller Panel Option

If at the **Add Panel** screen you have chosen **PW-6000** from the **Panel Type** drop-down list, proceed as follows:



1. Select the appropriate **Protocol** for **Port 4** and **Port 6**. For both ports, select:
   - SALTO option-button if you are using SALTO routers.
   - SNET option-button if you are using SNET readers.
   - PIM option-button if you are using Ingersol-Rand PIMs.
   - MSP1 (Honeywell) or MSP1 (Mercury) option-button if you have any subpanels that use either the Mercury or Honeywell protocol.
2. Click **OK** to display the **Add Panel** dialog box and continue with **Step 1** in the "PW6K1ICE DS with RS-485 Downstream" section (below) since the rest of the steps are identical.

8.14 PW6K1ICE DS with RS-485 Downstream

Note: For the Assa Abloy Aperio, the protocol requires both the Channel and sub-panel protocols to match the protocol of the Aperio hubs, which can be purchased as Mercury or Honeywell.

8.14.1 Port Protocol

In addition to the channel protocol, the user can select from PW6K1ICE DS Port 1 protocol values: MSP1 Honeywell, MSP1 Mercury, or SALTO.

Port 1 Protocol	Available Subpanels
MSP1 Honeywell	Assa Abloy Aperio (Honeywell AH30)
	PW6000 16IN
	PW6000 16OUT
	PW6000 1R
	PW6000 2R
	PW6K1R1E
MSP1 Mercury	Assa Abloy Aperio (Mercury AH30)
	Mercury MR16IN
	Mercury MR16OUT
	Mercury MR50
	Mercury MR52
	Mercury MRDT
	PW6K1R1E
SALTO	SALTO Sallis
	PW6K1R1E

MSP1 Honeywell port dialect allows addition and communication with the PW-series of subpanels and the Honeywell version of the ASSA ABLOY hub. MSP1 Mercury port dialect allows addition and communication with the MR-series of subpanels and the Mercury version of the ASSA ABLOY hub.

8.14.2 ACR Limits

There is a seventeen (17) reader/ACR limit for the PW6K1ICE. This includes all ACRs in a hardware template so a Entry/Exit Reader will be treated as

two (2) ACRs and a standard door typical ACR reader will be treated as one (1) ACR.

Once sixteen (16) ACRs have been reached, no additional logical devices with two plus (2+) ACRs can be defined.

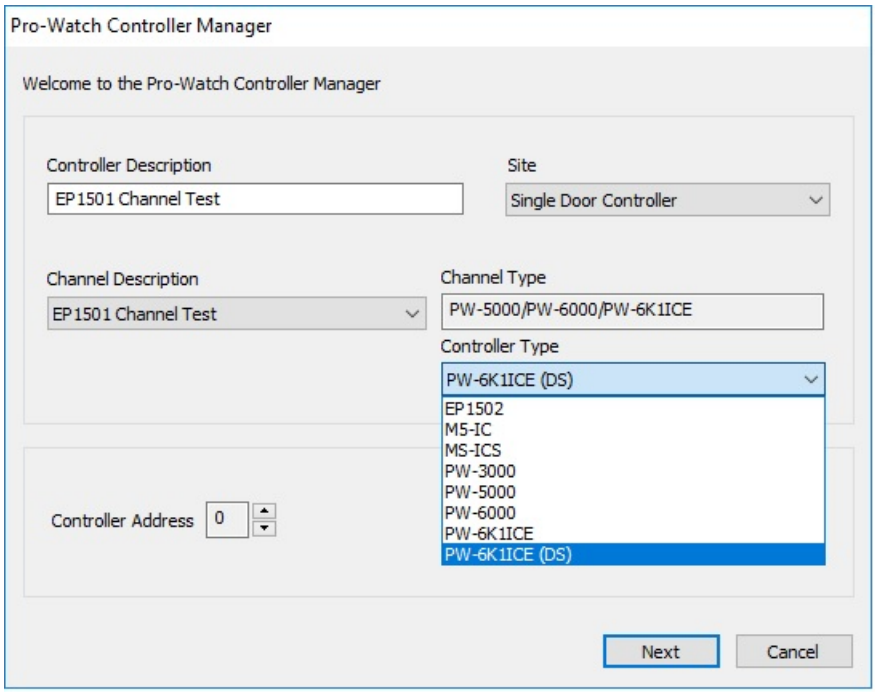
Once seventeen (17) ACRs are reached, no additional logical devices with ACRs can be defined.

Note: The count is based on the ACRs defined, not installed. In other words, if an ACR is defined, it will count against the 17 ACR limit even if it is uninstalled.

8.14.3 Adding the PW6K1ICE DS Panel

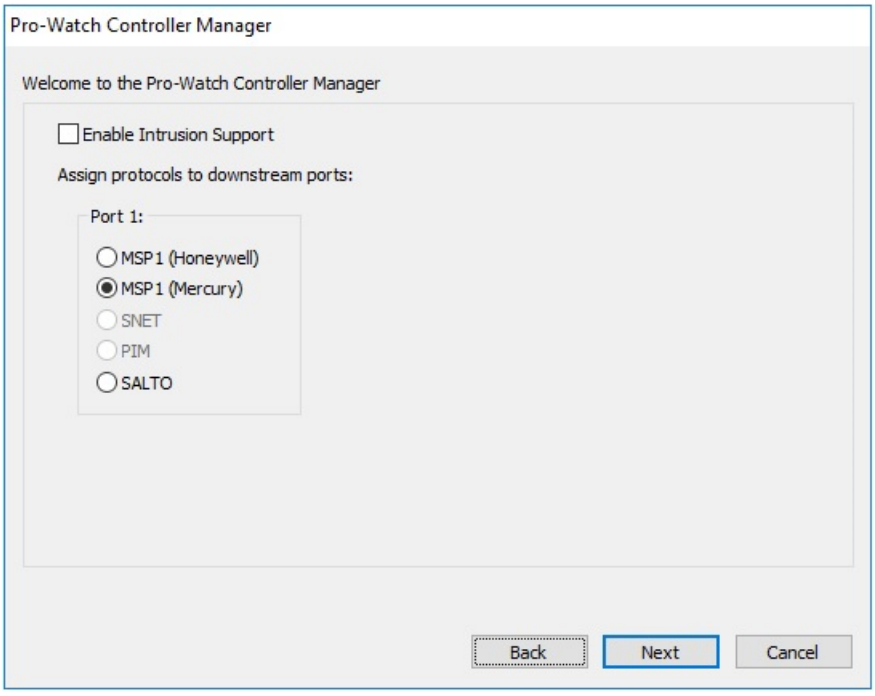
In order the use the downstream ports of the PW6K1ICE panel, a new panel type is added called PW6K1ICE (DS).

Note: An existing PW6K1ICE panel cannot be converted in order to access the downstream ports. A new PW6K1ICE (DS) panel must be created.



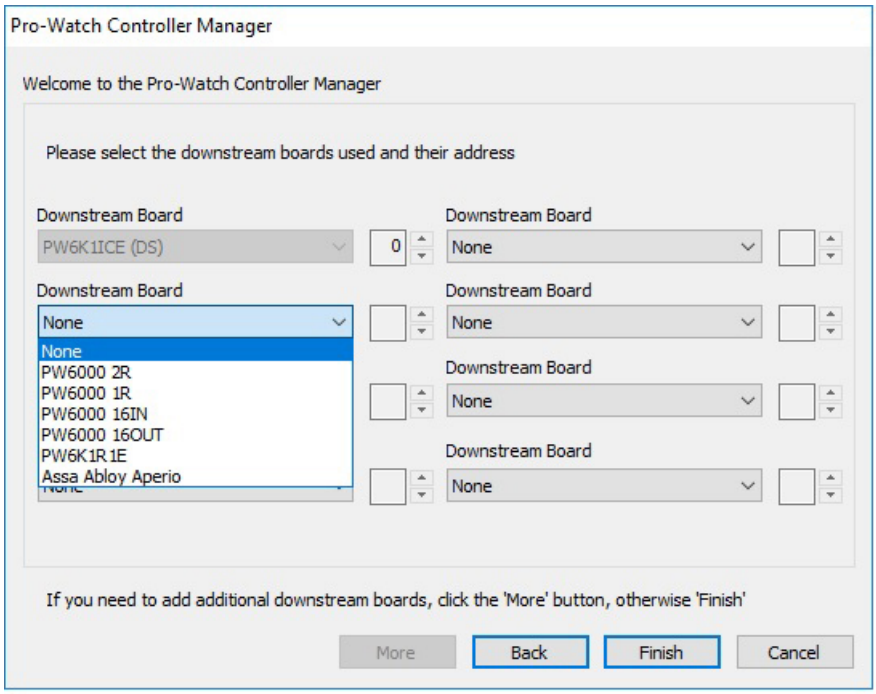
In the panel add wizard, there will be an additional step in selecting the protocol/dialect of the downstream port.

Note: RS-485 downstream subpanels communicate on Port 1. IP-based PW6K1R1E subpanels communicate on Port 0.



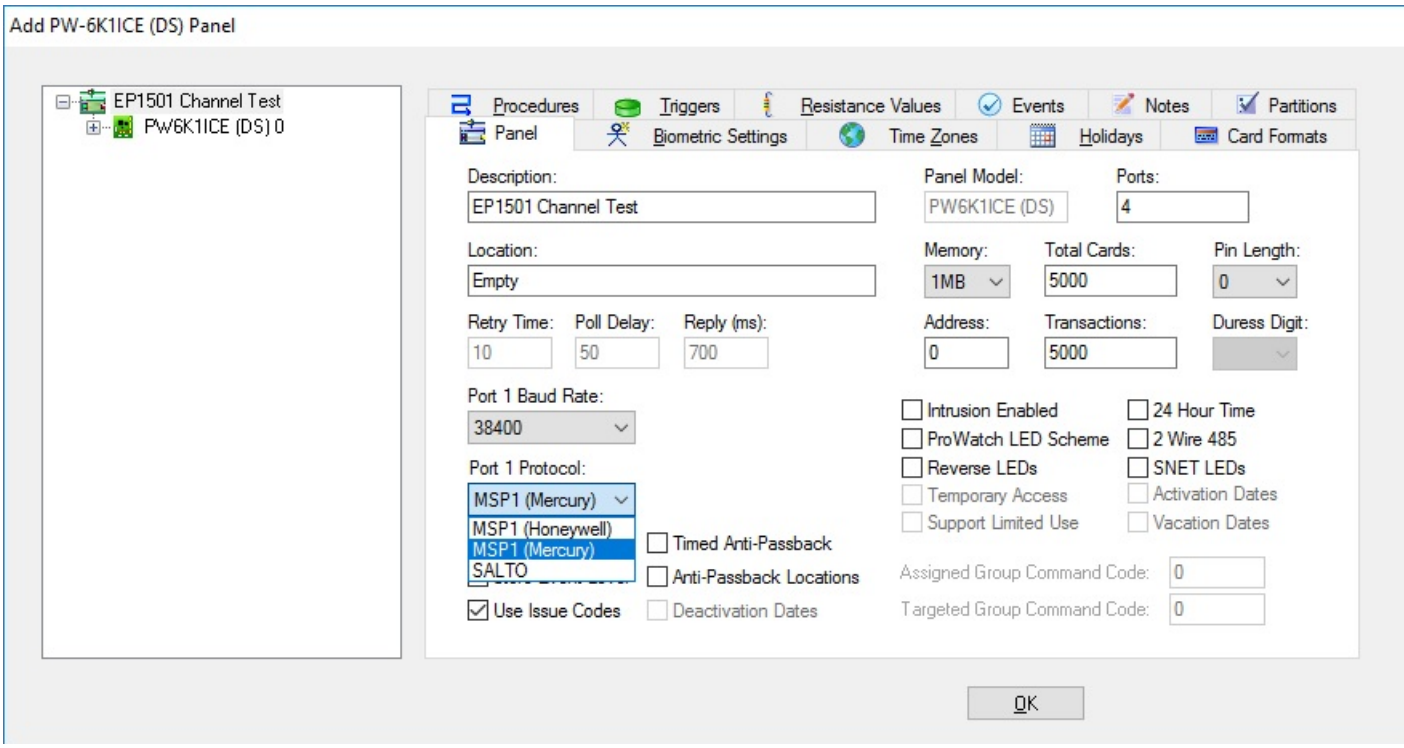
The next step will add subpanels to the setup. The list of available subpanels will depend on the Port 1 protocol selected in the previous step. A default PW6K1ICE (DS) embedded subpanel will be added. Note that a total of sixteen (16) subpanels can be added and this is a combination of RS-485 and IP-based subpanels.

If the protocol selected for Port 1 is MSP1 (Honeywell), the list of sub-panels looks like this:

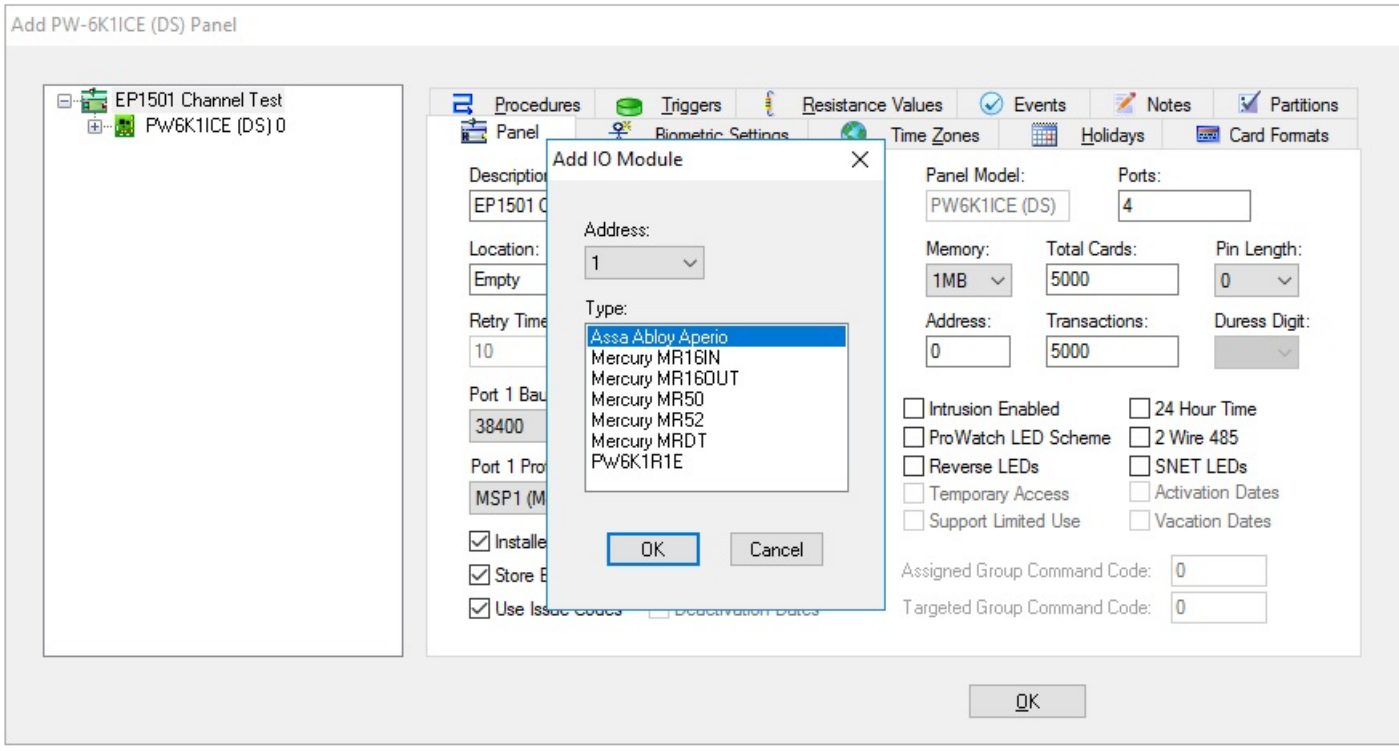


8.14.4 Panel Properties

After panel creation, there will be a couple new fields in the Panel Properties of the panel: the Port 1 Baud Rate selection and the Port 1 Protocol selection. Protocol selection for Port 1 can be changed as long as there is not an existing subpanel added to Port 1 in software.


Add PW-6K1ICE (DS) Panel
EP1501 Channel Test
PW6K1ICE (DS) 0
Procedures
Triggers
Resistance Values
Events
Notes
Partitions
Panel
Biometric Settings
Time Zones
Holidays
Card Formats
Description:
EP1501 Channel Test
Panel Model:
PW6K1ICE (DS)
Ports:
4
Location:
Empty
Memory:
1MB
Total Cards:
5000
Pin Length:
0
Retry Time:
10
Poll Delay:
50
Reply (ms):
700
Address:
0
Transactions:
5000
Duress Digit:
Port 1 Baud Rate:
38400
Port 1 Protocol:
MSP1 (Mercury)
MSP1 (Honeywell)
MSP1 (Mercury)
SALTO
Intrusion Enabled
24 Hour Time
ProWatch LED Scheme
2 Wire 485
Reverse LEDs
SNET LEDs
Temporary Access
Activation Dates
Support Limited Use
Vacation Dates
Timed Anti-Passback
Anti-Passback Locations
Deactivation Dates
Use Issue Codes
Assigned Group Command Code:
0
Targeted Group Command Code:
0
OK

When adding a subpanel through Panel Properties dialog box, the list of available subpanels will depend on the Port 1 selection:



8.15 Configuring PW6K1ICE Panel Tabs

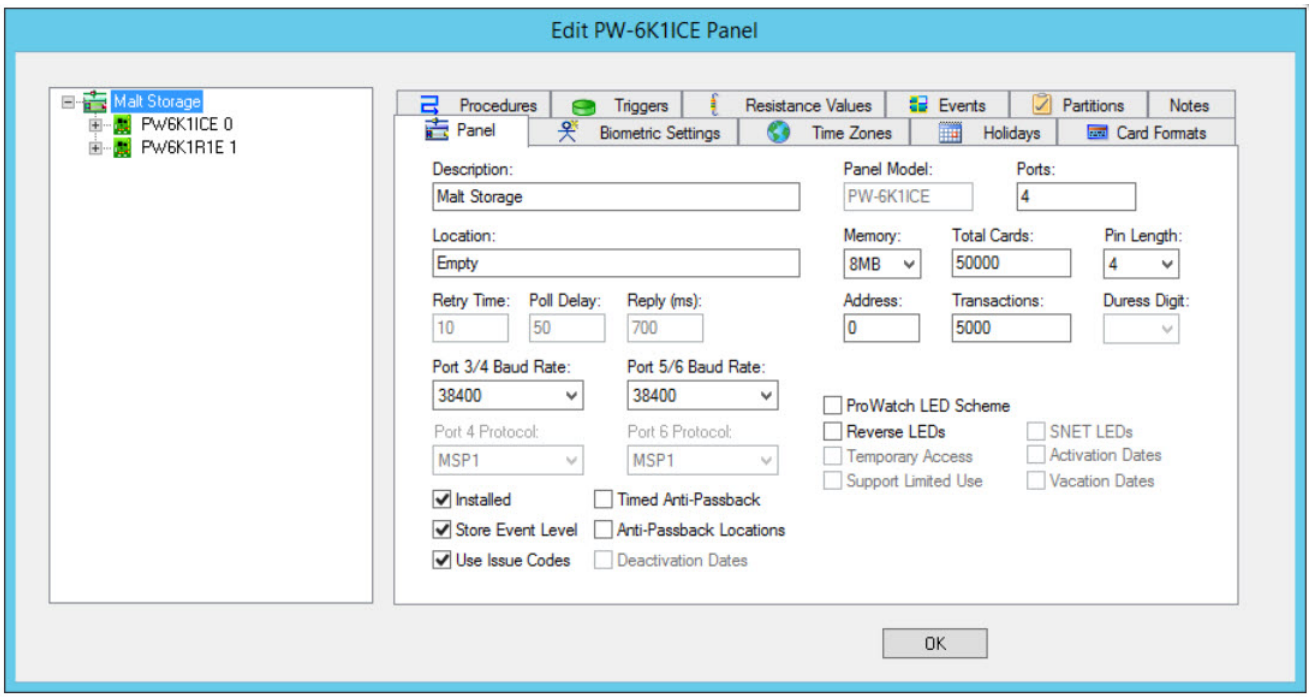
See the following tab list and tab sections for the configuration information:

ADD A PW6K1ICE PANEL TABS LIST

- "Panel Tab"
- "Biometric Settings Tab"
- "Time Zones Tab"
- "Holidays Tab"
- "Card Formats Tab"
- "Procedures Tab"
- "Triggers Tab"
- "Resistance Values Tab"
- "Events Tab"
- "Partitions Tab"

8.15.1 Panel Tab

The Panel tab includes basic hardware settings for the panel. This tab allows you to set the panel memory, transactions, and other panel related features.



Use the following field descriptions to complete the Panel tab:

Field	Description
Description	Provides the description of the panel as defined by the user.
Panel Model	Identifies the panel model.
Ports	Defines the number of downstream ports on the panel.
Location	Identifies the location of the panel as defined by the user.
Memory	Identifies the total memory on the panel.
Total Cards	Defines the amount of cards that can be in the panel.
Retry Time (sec)	Defines the panel/host connection retry time. A read-only field.
Poll Delay (ms)	Defines how long for the panel to wait between polls. A read-only field.
Reply (ms)	Defines how long the panel should wait for a reply. A read-only field.
Address	Identifies the address of the panel.
PIN Length	Assigns the PIN characters that must be used when creating a PIN number for cardholders. This number should be the same number specified for a PIN length when creating a Card (see "Adding a Card" in Chapter 2, "").
Transactions	Defines how many transactions to buffer in the panel.
Port 3/4 Baud Rate	Defines the baud rate for ports 3 and 4.
Port 5/6 Baud Rate	Defines the baud rate for ports 5 and 6.
Installed	Required for the panel to be installed and operational.
Store Event Level	Causes the panel to store the user level parameter as defined in the PW tab in card configuration.
Use Issue Codes	Enables the panel to use card formats that check the issue level of a card.

Field	Description
Timed Anti-Passback	Enables timed anti-passback. When anti-passback is timed, Pro-Watch grants access by the same card (without an exit) for a second entry after a specified time period has elapsed. Note that you must also set the Logical Device (in the Logical Device "Anti-passback Settings Tab") for successful anti-passback operation. See also "DBC - Area" in Chapter 29.
Temporary Access	This function is currently not supported.
Activation Dates	This function is currently not supported.
Deactivation Dates	This function is currently not supported.
Pro-Watch LED Scheme	Identifies an LED scheme for readers.
Reverse LEDs	Defines the LED scheme as reversed from the normal LED scheme.
Anti-Passback Locations	Enables anti-passback operation in Areas. See "DBC - Area" in Chapter 29.
Support Limited Use	This function is currently not supported.
Vacation Dates	This function is currently not supported.

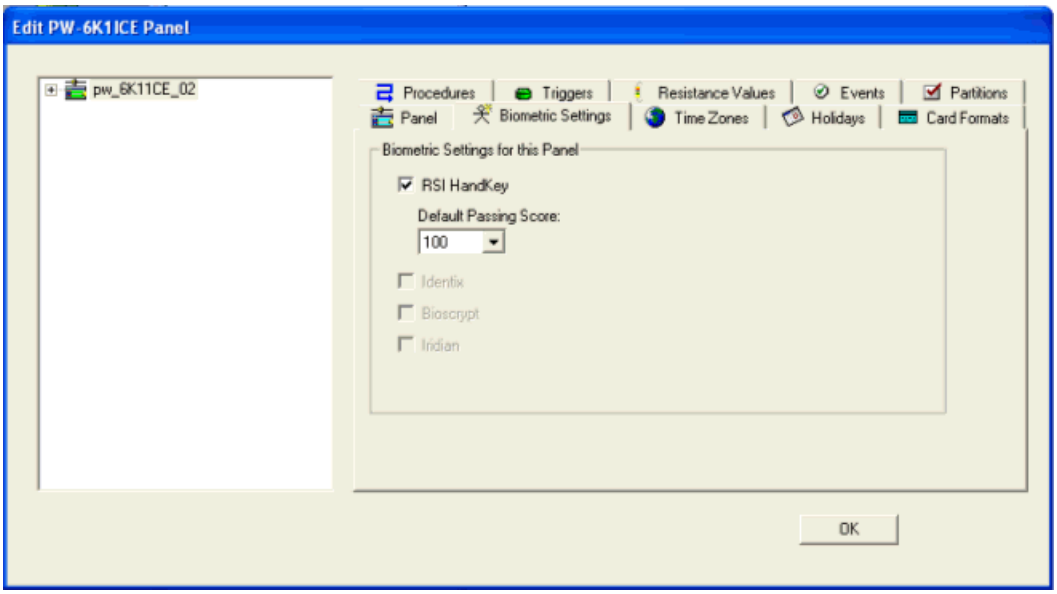
Note: If you edit the Panel properties and change the panel database, you must manually re-initialize and download the panel. Follow these steps:

1. Click **Panels** under the appropriate Site folder in the Hardware Configuration tree to display the panel icon.
2. Right-click the panel's icon and select **Download**.
3. De-select **Download System**.
4. Select **Initialize**.
5. Click **Download** to re-initialize the panel. Note that this step only re-initializes the panel.
6. When the panel icon re-appears, right-click the icon and select **Download**.
7. Select **Download System** and **Download Cards**.
8. Click **Download** to download the newly-configured panel.

For more information on downloading panels, see "Panel Download".

8.15.2 Biometric Settings Tab

The Biometric Settings tab enables you to configure the panel for the Pro-Watch biometric hand geometry reader. This reader grants access by a geometric scan of the badge holder's hand as well as by keypad. See Chapter 62, *Biometric Reader Configuration* for more information about the biometric hand geometry reader.

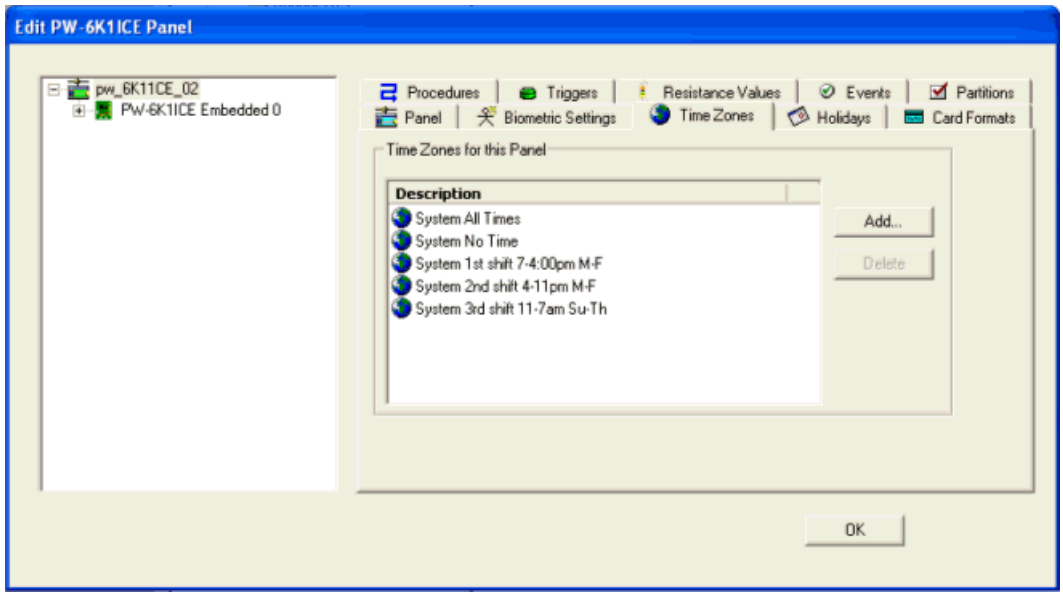


Use the following field descriptions to complete the Biometric Settings tab:

Field	Description
RSI Handkey	Indicates that the panel will support a biometric hand geometry reader.
Default Passing Score	Indicates the score a hand reading must receive before the biometric hand geometry reader grants access. It is recommended that you leave the number at 100.
Identix	N/A.
Bioscript	N/A.
Iridian	N/A.

8.15.3 Time Zones Tab

The Time Zones tab enables you to add time zones to the panel; only the times zones that have been added to the panel can be applied to panel and reader fields:



To add a time zone to the panel:

1. Click **Add** to display the **Time Zones** dialog box.
2. Select the time zone and then click **OK**.
3. To add a new time zone, click **Add**.
4. To edit an existing time zone, select it from the list and click **Edit**.

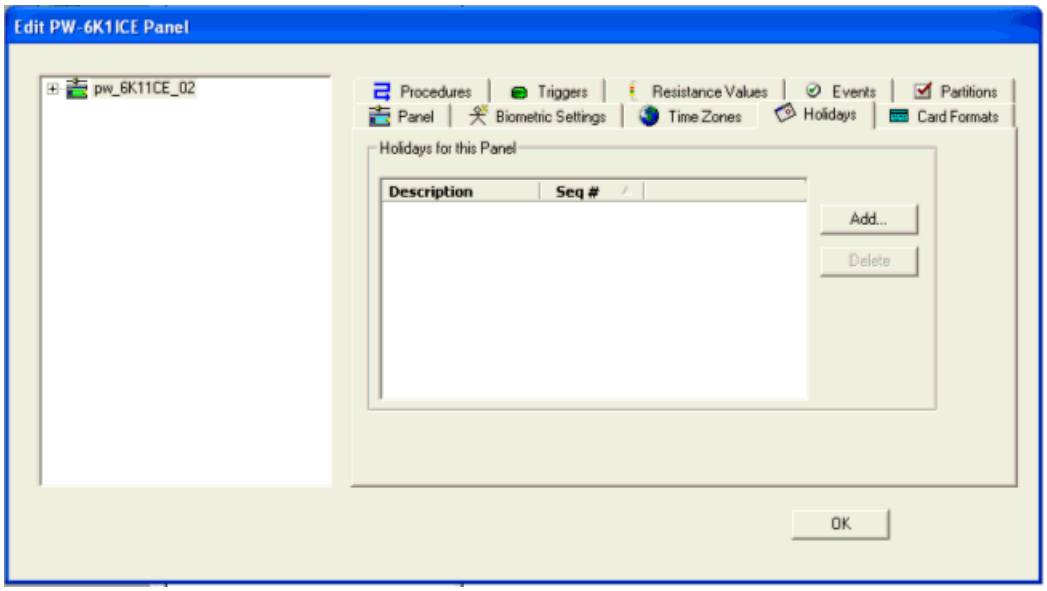
5. To delete an existing time zone, select it from the list and click **Delete**.

Click **OK** again at the Select Time Zone dialog box.

For more information on configuring time zones, see "DBC - Time Zones" in Chapter 57.

8.15.4 Holidays Tab

Holidays enable you to edit normal Time Zone behavior on specific days. Holidays are assigned to time zones.



To add a holiday to the panel:

1. Click **Add** to display the Select Holiday dialog box.
2. Click the icon next to the Holiday field.
3. Click **Define**.
4. Select the holiday and click **OK**.
5. Click **OK** again at the Select Holiday dialog box.

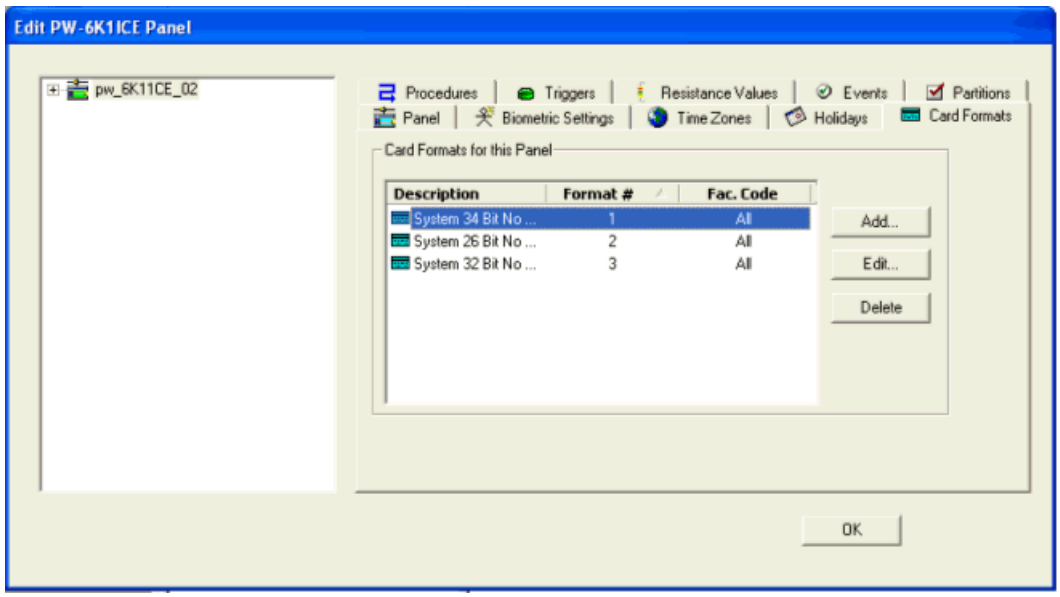
If the holiday you want does not appear in the dialog box you can create a new time zone. Click **Add** on the Select Holiday dialog box.

For more information on configuring holidays, see "DBC - Holidays" in Chapter 49.

8.15.5 Card Formats Tab

A card format tells the panel how to determine the card number. You must add the card format to a card before a reader can read the card. Valid card

formats are defined in Database Configuration. See "DBC - Card Formats" in Chapter 35.



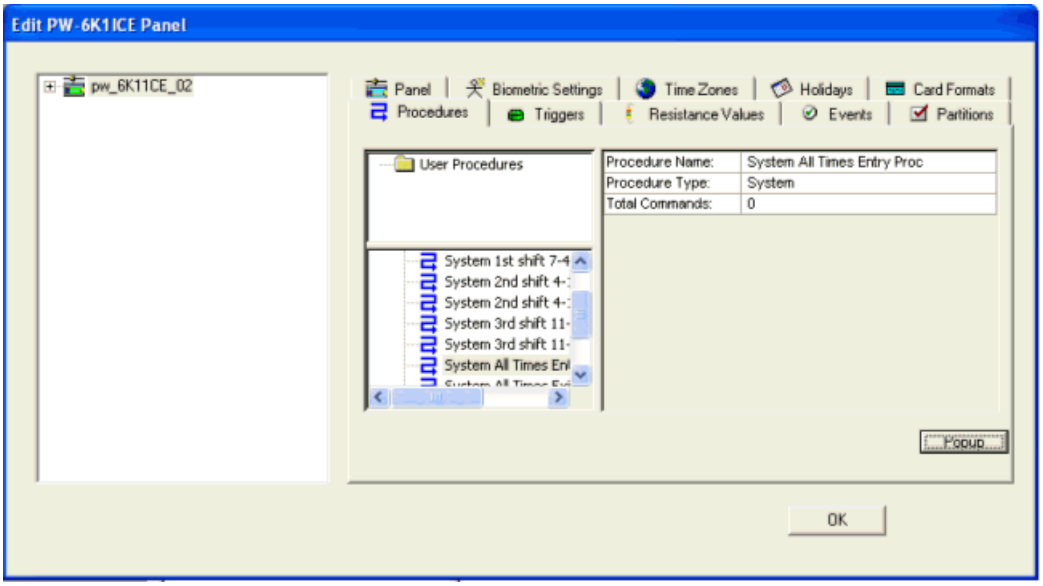
To add a card format to the panel:

1. Click **Add** to display the Select Card Format dialog box.
2. Click the icon next to the Card Format field.
3. Click **Define**.
4. Select the card format and click **OK**.
5. Select the **Format Number** from the drop-down list.
6. Enter the **Facility Code** or select the **All Facility Codes** check box. Note that facility codes are coded at time of manufacture.

7. Click **OK**.

8.15.6 Procedures Tab

The Procedures tab displays the user and system procedures assigned to the panel in the event of a trigger. System procedures are coded and cannot be edited or deleted.



User procedures perform customized panel functions. For example, a procedure allows you to define the action upon a particular trigger. See "Triggers Tab" for more information on configuring triggers.

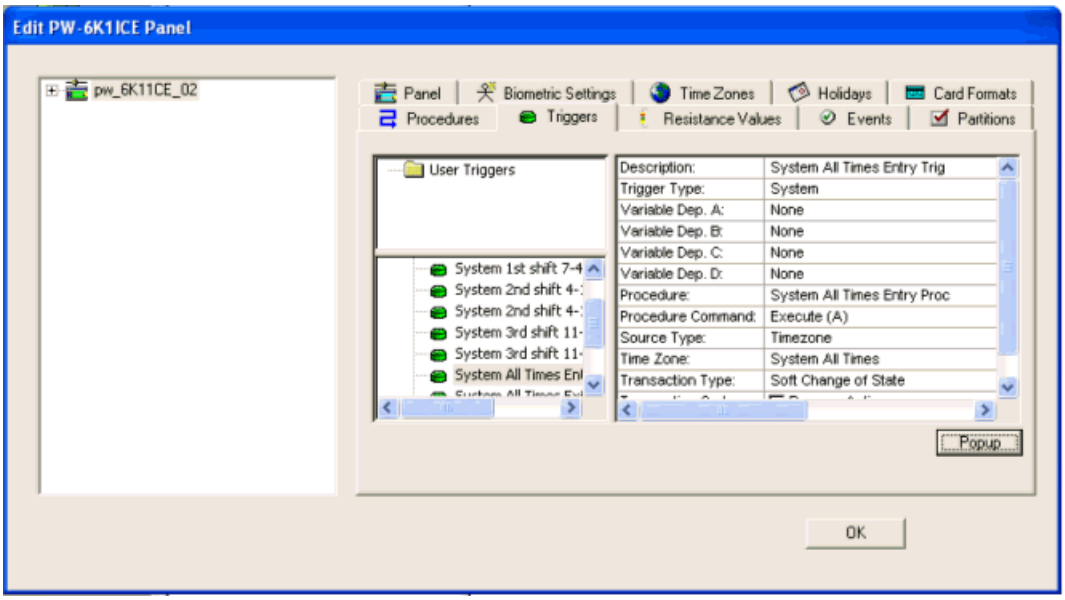
To add procedures:

1. Right-click **User Procedures** and select **Add Procedure**.
2. To add a command to the procedure, right-click on the new procedure and select **Add Command**.
3. Click the **Command Type** field to display the drop-down command type list.
4. Select the type of command.
5. Edit the command parameters by clicking on the parameter fields and selecting parameter values from the drop-down lists.
6. Repeat steps 2 through step 5 to add any additional commands to the procedure.
7. Click **OK** to accept the procedure.

Note: Also see "Viewing and Editing Dependencies of a PW6K1ICE Panel" and "Configuring a Logical Device".

8.15.7 Triggers Tab

The Triggers tab displays the user and system triggers that invoke the panel's procedures. See "Procedures Tab" for more information on configuring procedures. System triggers are coded and cannot be edited or deleted.



To configure triggers:

1. Right-click **User Triggers**, and select **Add Trigger**. The trigger appears in the User Triggers tree.
2. Select the created trigger in the User Triggers tree to display the trigger configuration box. This box displays the following

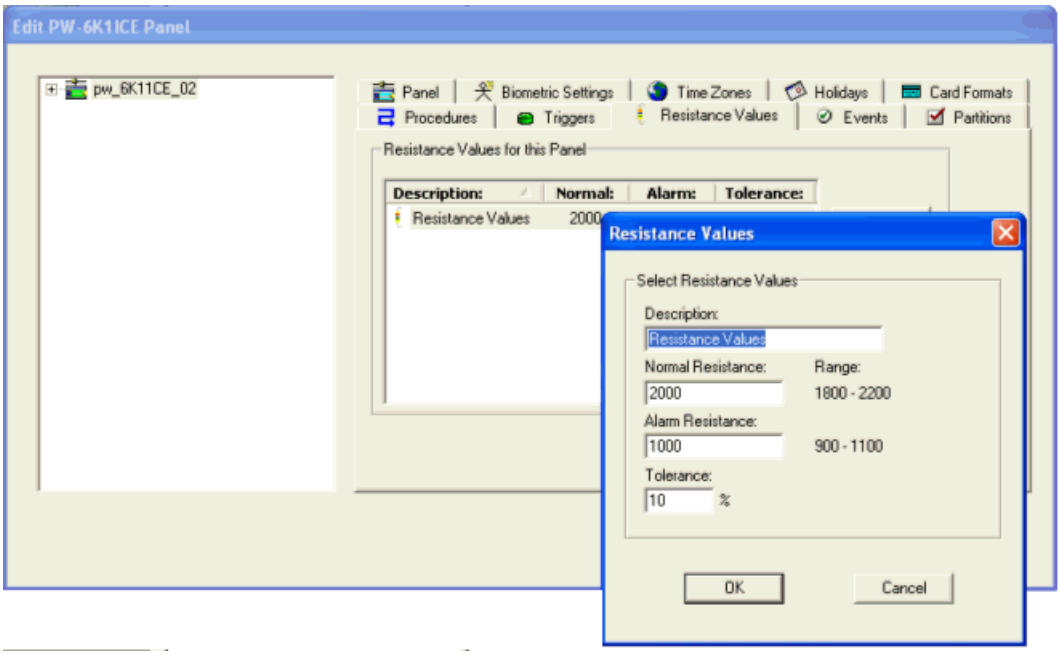
configuration elements for the trigger. Note that transaction Codes will vary depending on the Transaction Type chosen:

Field	Description
Description	Provides the description of the trigger as defined by the user.
Trigger type	Defines whether the trigger is user or system created.
Variable dependencies	Allows multiple input conditions and cascading triggers.
Procedure	Defines the Procedure to initiate in the event the trigger initiates.
Procedure command	Defines the action to be performed.
Time zone	Defines the time zone in which the trigger is enabled.
Source type	Defines the source of the event.
Transaction type	Defines the trigger type.
Transaction code	Defines the individual attributes of the trigger.

3. Configure the trigger's parameters listed in step 2 by clicking the parameter field to display the drop-down list and selecting field values.

8.15.8 Resistance Values Tab

This tab displays the default resistance values. Applicable for the panel's supervised inputs, resistance values determine what the resistance is going to be for the four states (normal, alarm, short, open). Open and short states are defined as 0 ohms and infinite.



*To **add** a set of resistance values to the panel:*

1. Click **Add** to display the Resistance Values dialog box.
2. Use the following field descriptions to create or edit the resistance values:

Field	Description
Description	Provides the description of the resistance value as defined by the user.
Normal	Defines the resistance for normal.
Alarm	Defines the resistance for alarm.
Tolerance	Determines the fluctuation +/- a percentage of the normal and alarm values.

3. Click **OK** to accept the resistance value.

To edit a set of resistance values:

1. Click the resistance values entry (or select the entry and click **Edit**) to display the Resistance Values dialog box.

2. Use the table presented above to edit the fields of the Resistance Values dialog box.

8.15.9 Events Tab

The Events tab displays the default event types that are applicable to the PW6K1ICE panel.

To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears.

For more information on editing events, see "HW Config - Edit Point".

8.15.10 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. For information about creating a partition, see "DBC - Partitions" in Chapter 53. Use this function to assign or delete an already-created partition to the panel:

To assign a partition to the panel:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition.
3. Click **Add**.

To delete a partition from the Partitions List dialog box:

1. Select the partition.
2. Click **Delete**.

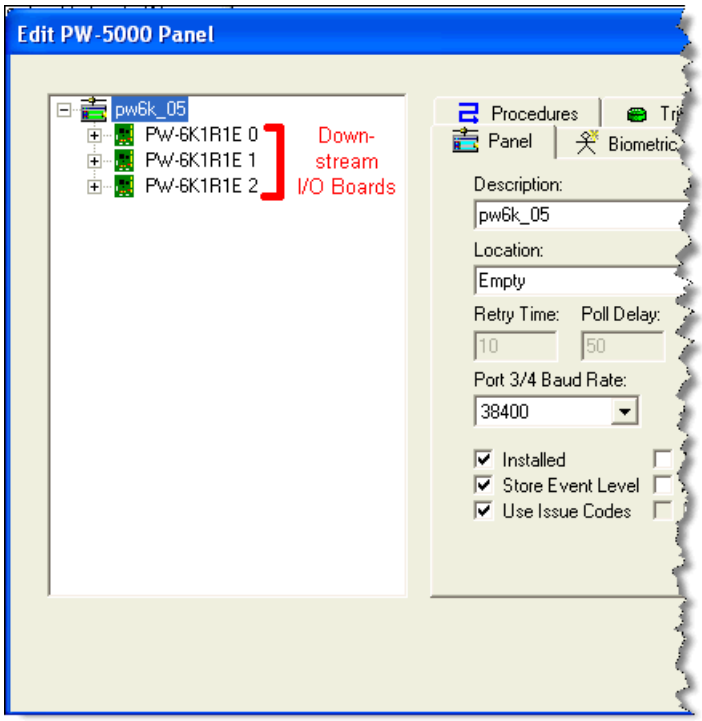
After completing each tab within the panel, you will need to save the panel configuration.

To save the panel configuration:

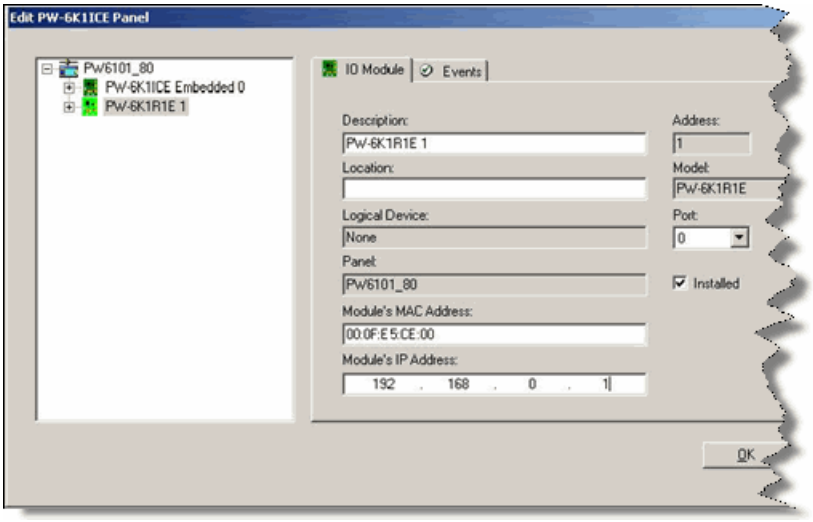
Click **OK** at the Add [Panel Name] Panel dialog box.

8.16 Configuring the PW6K1R1E Downstream I/O Boards

1. In the Pro-Watch Hardware Configuration tree, click the site to which the panel is assigned.
2. Click the Panel's subdirectory. The icons of the existing panels appear in the right pane.
3. Right-click the appropriate panel, and select **Properties**. The Edit [panel name] Panel dialog box appears. This box lists the I/O modules configured for each panel.



4. Click the first I/O Module listed in the panel tree list to display the I/O Module and Events configuration tabs.



5. Use the following field descriptions to complete the I/O Module tab:

Field	Description
Description	Description of the I/O Module.
Location	Location of the I/O Module.
Logical Device	Name of the Logical Device.
Panel	Panel type to which the I/O module has been added.
Module's MAC Address	MAC address of the I/O module. Note that the MAC address's octets must be separated by a colon. For example: 00:0F:E5:CE:00.
Module's IP Address	Address of the I/O Module.
Model	I/O Module model type.
Port	Panel port the I/O Module uses to connect to the panel.
Installed	Required to install the I/O Module.

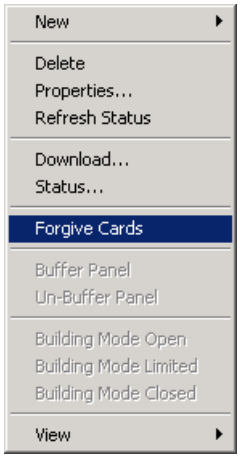
6. Click the Events tab to display the events that can support this input/output module.
7. Either double-click the event you want to define, or select the event and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point". Note that you can also add and delete input/output modules. To add an

input/output module, right-click anywhere in the panel tree and select **Add IO Module**. To delete an input/output module, right-click the module you want to delete and click **Delete IO Module**.

Note: The PW6K1ICE Panel allows you to forgive anti-passback (see "DBC - Area" in Chapter 29) for all cards.

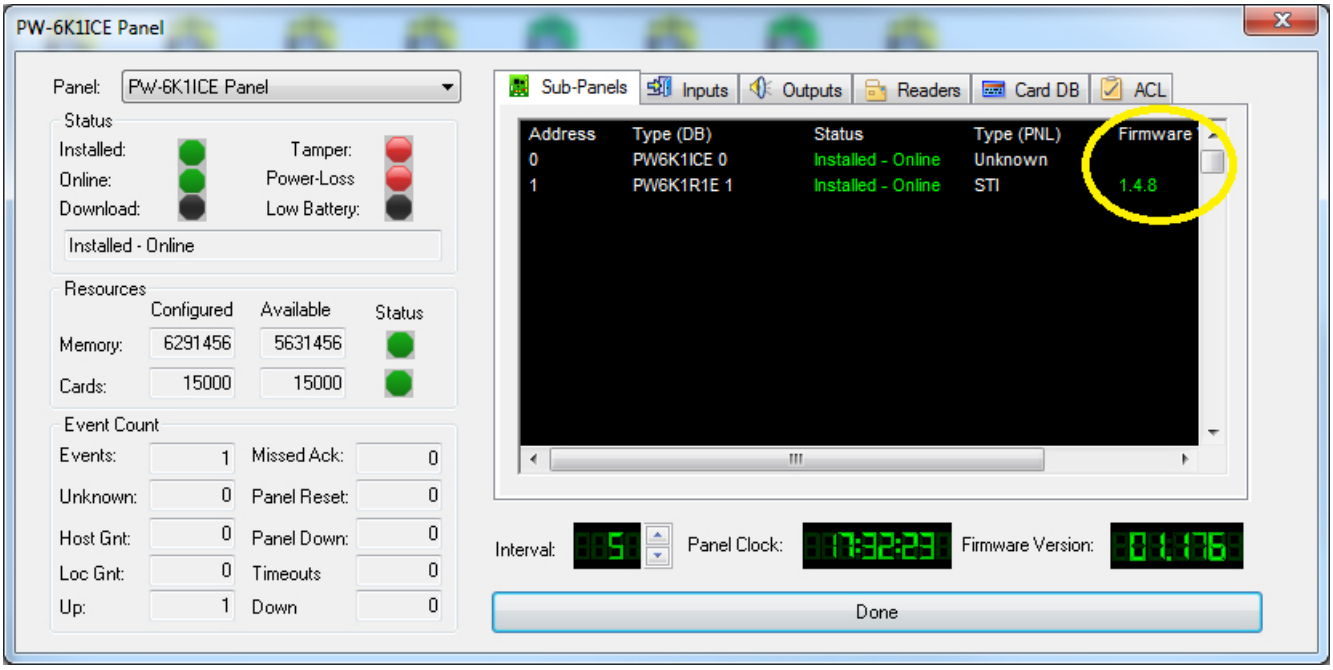
To forgive anti-passback:

1. Select the panel from the Hardware Configuration window.
2. Right-click on the panel and select **Forgive Cards**:



8.16.1 MR51e Subpanel Firmware Information

The firmware of MR51e subpanel, a.k.a. PW6K1R1E, should be set to 1.4.8 or higher according to Mercury's recommendations:



8.17 Viewing and Editing Dependencies of a PW6K1ICE Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

8.18 Deleting a PW6K1ICE Panel

Please refer to How to Delete a Panel, page 53.

8.19 Adding a Mercury Panel

This section describes how to specify and configure the Mercury protocol for PW-5000/6000-like third-party panels.

It consists of two parts:

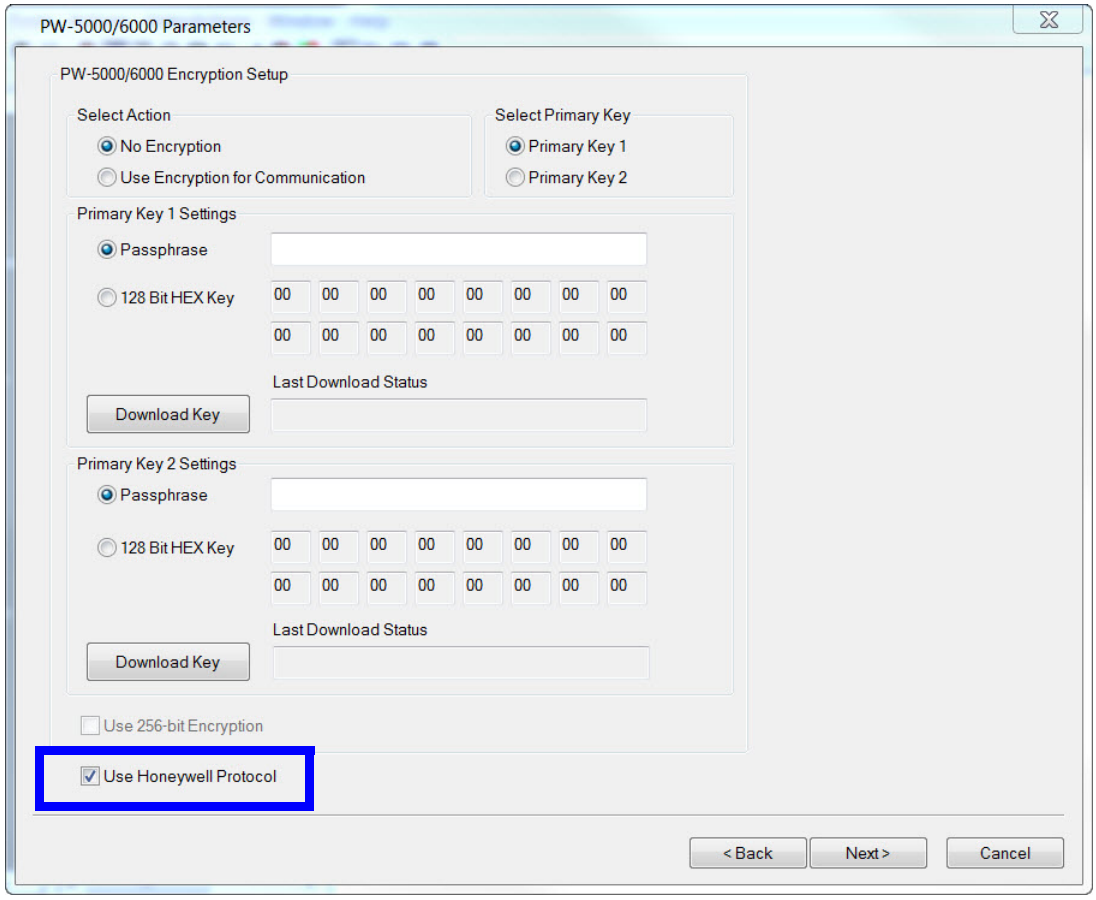
1. The first part describes how to specify the protocol type (Honeywell or Mercury) when the channel is defined. Once the channel is initially defined, this cannot be changed.
2. The second part describes how to create a panel by using Mercury protocol. Please note that a channel's protocol type controls the panels attached to that channel. A channel set up for Honeywell protocol will allow the same capabilities for panel definition, whether or not the panel definition wizard is used. Likewise, use of the PW-5000/6000 panel property sheets will not change for panels connected to a channel using the Honeywell protocol.

For channels using the Mercury protocol, the dialogs and property sheets used for panel definition and maintenance will be modified to restrict the types of panel and subpanel models available to those valid for the Mercury Standard protocol.

8.19.1 PART I: Unselecting the Honeywell Protocol

1. In the left navigation pane, select the appropriate **Site** in the **Hardware Configuration** tree-view.
2. Under the Site, double click the appropriate **Channel** icon to display the **Edit Channel** screen

3. Select the **PW-5000/6000 Parameters tab**:



Note: If the "Mercury Standard Protocol" option is enabled under Panels in the Software Keys module (only your Pro-Watch Software Keys Licensing Manager can do this for you), the **"Use Honeywell Protocol" check-box** is displayed at the bottom of the screen. The "**Use Honeywell Protocol**" check-box is checked by default. Once the channel is defined, this check box will be visible but disabled (grayed out).

Note: In earlier versions of Pro-Watch, this screen used to be dedicated to PW-5000/6000 Encryption only.

4. Unselect the "**Use Honeywell Protocol**" check-box.

8.19.2 PART II: Creating the Third-Party Panel

This section describes the panel creation process through two methods:

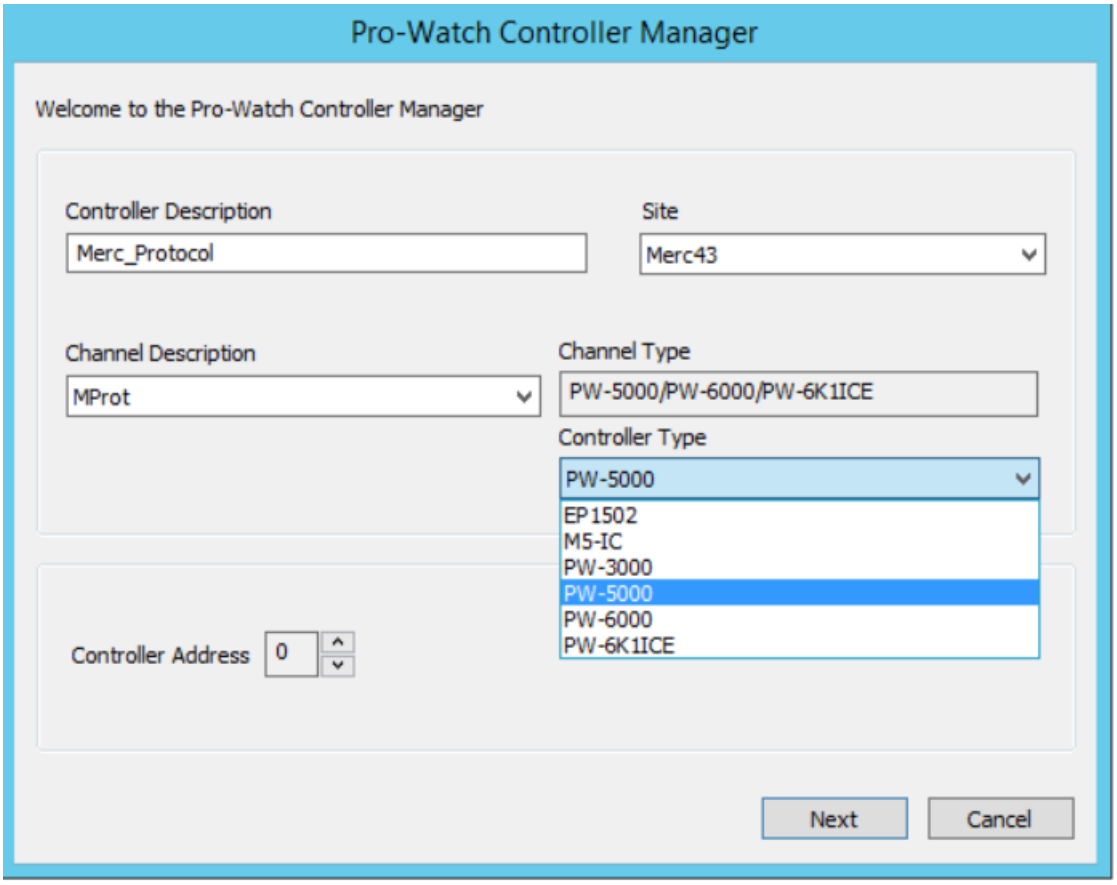
1. By using the user (panel definition) wizard, and
2. Without using the user (panel definition) wizard.

Note: The contents of some of the drop-down lists in the screenshots to follow are restricted to only those panel and subpanel types which are supported when using the Mercury Standard protocol.

By Using the User Wizard

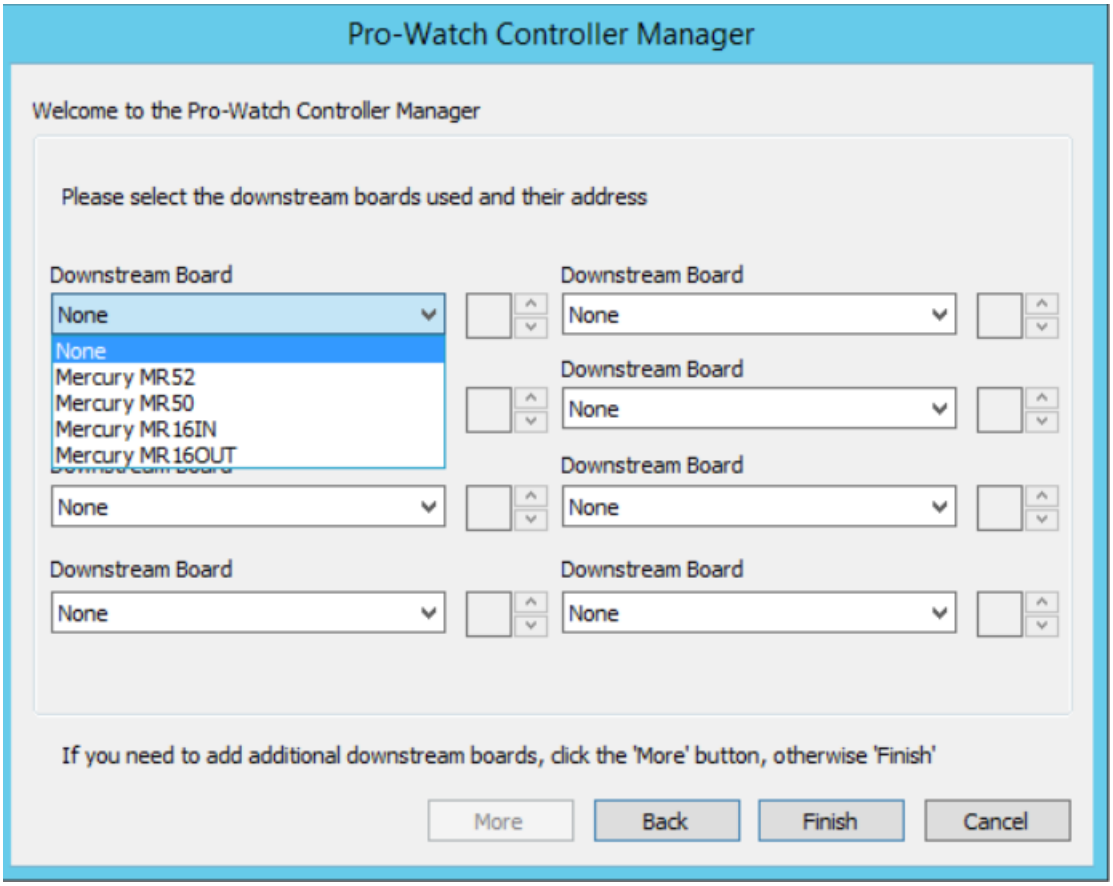
Note: For more information on the User Wizard, see Turning the User Wizard On and Off, page 4. Unless the User Wizard is turned off by the user, it is displayed by default every time the user wants to create a new Panel or Logical Device.

1. Click **Hardware Configuration** on the left navigation bar.
2. Right-click the appropriate **Site** icon. From the pop-up menu, select **New > Panel** to display the **Pro-Watch Controller Manager** screen:

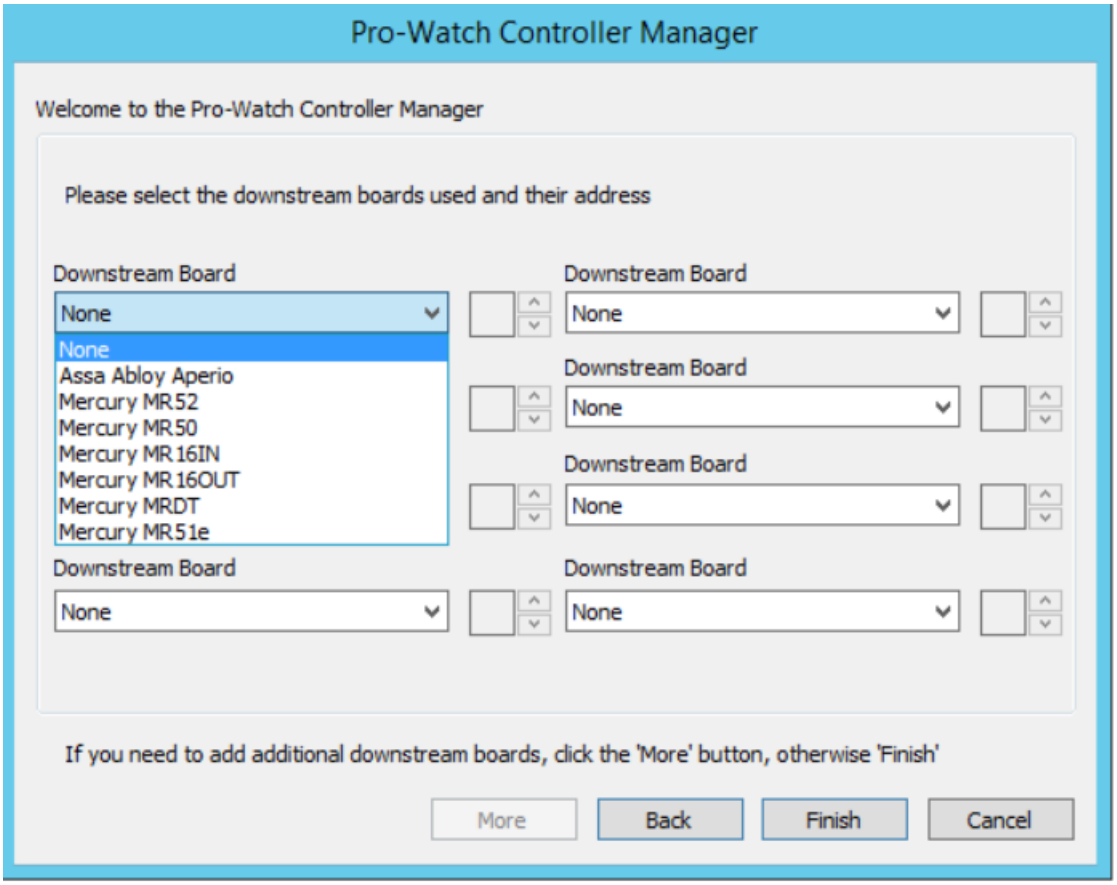


3. Click **Next**. The next screens to display will depend on whether you've selected PW-5000 or PW-6000 as Controller Type.

For **PW-5000 Controller Type**, you'll see the following screen:



For **PW-6000 Controller Type**, you'll see the following screen:



Note: In both screens, please note the restricted number of subpanel selections in the **Downstream Board** drop-down list.

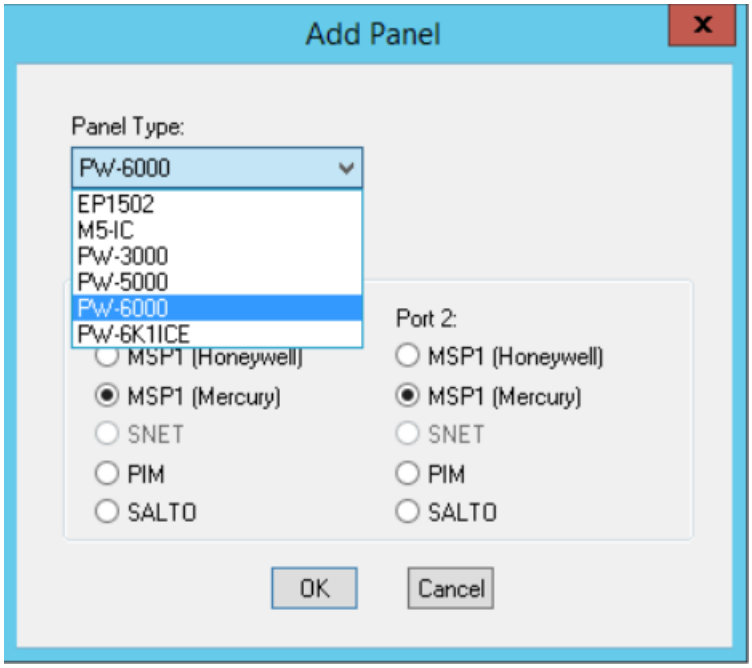
4. Make the necessary selections and click **Finish**.

Without Using the User Wizard

Note: For more information on the User Wizard, see Turning the User Wizard On and Off, page 4. Unless the User Wizard is turned off by the user, it is displayed by default every time the user wants to create a new Panel or Logical Device.

1. In the **Hardware Configuration** module, select a **Site** and a **Channel**.

2. Right-click on a **Channel** icon to display the pop-up menu. Select **New > Panel t**o display the **Add Panel** dialog box. Here are the **panel options** available:

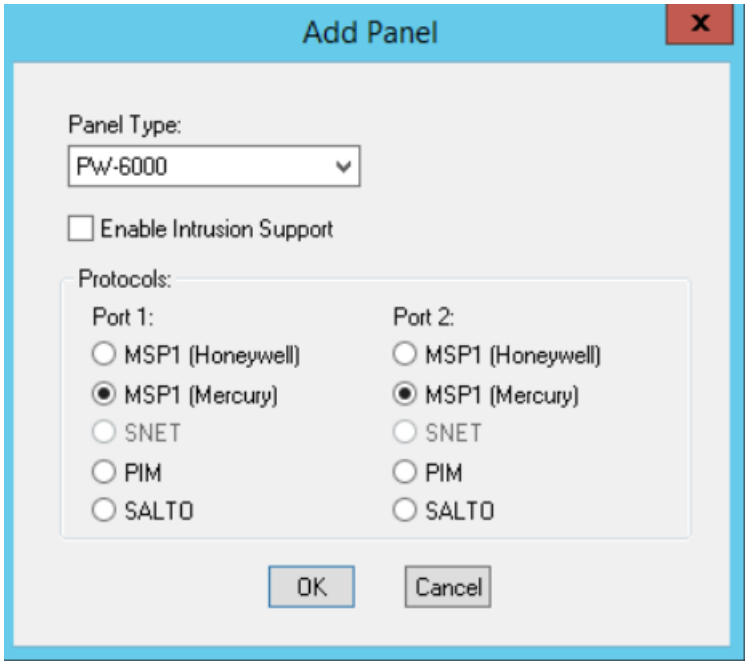


3. If you select **PW-6000** panel, go to the PW-6000 Controller Panel Option, page 79 section.
4. If, on the other hand, you select **PW-3000**, **PW-5000**, or **PW6K1ICE**, go to the Click OK to display the Add Panel dialog box and continue with Step 1 in the Click OK to display the Add Panel dialog box and continue with Step 1 in the Click OK to display the Add Panel dialog box and continue with Step 1 in the section (below) since the rest of the steps are identical., page 79 section (below) since the rest of the

steps are identical., page 79 section (below) since the rest of the steps are identical., page 79 section.

8.19.3 PW-6000 Controller Panel Option

If at the **Add Panel** screen you have chosen **PW-6000** from the **Panel Type** drop-down list, proceed as follows:



1. Select the appropriate **Protocol** for **Port 4** and **Port 6**. For both ports, select:
   - SALTO option-button if you are using SALTO routers.
   - SNET option-button if you are using SNET readers.
   - PIM option-button if you are using Ingersol-Rand PIMs.
   - MSP1 (Honeywell) or MSP1 (Mercury) option-button if you have any subpanels that use either the Mercury or Honeywell protocol.
2. Click **OK** to display the **Add Panel** dialog box and continue with **Step 1** in the Click OK to display the Add Panel dialog box and continue with Step 1 in the Click OK to display the Add Panel dialog box and continue with Step 1 in the section (below) since the rest of the steps are identical., page 79 section (below) since the rest of the steps are identical., page 79 section (below) since the rest of the steps are identical., page 79 section (below) since the rest of the steps are identical.

8.20 Viewing and Editing Dependencies of a Mercury Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

8.21 Deleting a Mercury Panel

Please refer to How to Delete a Panel, page 53.

8.22 Mercury Text Output to LCD Terminal

Pro-Watch can send text output to supported LCD terminals like MRDTs and OSDP readers.

See "Configuring the Mercury Keypad Settings" for configuration info.

Host-Driven Functionality

This functionality is a host-driven functionality. The Pro-Watch Server has to be online in order for the messages to be sent to the reader. If the Pro-Watch server is offline, no messages will be sent.

System Time vs. Event Time

Pro-Watch server will not send down the message if there is a greater than 5 second difference between the system time and event time. This is to prevent outdated messages from being sent to the reader during unbuffering of offline events from the panel while the Pro-Watch server was offline.

Reader Display Lines and Background Info

Although a reader can support multiple lines and configurations, Mercury's implementation restricts the number of display lines to two.

Although both lines can be used to display text, Pro-Watch will only send text to the first row (**Row 0**) of the reader display.

The second line is reserved for the background text set in the Mercury Keypad Settings and the time; so any text sent to the second row (**Row 1**) of the reader display is almost immediately overwritten by the scrolling background text and time.

Each row of the reader display is capable of supporting a maximum of 16 characters.

In addition to the row selection, Pro-Watch does not support column selection.



Figure 8-2 HID Wiegand Reader with default display.



Figure 8-3 HID OSDP Reader with 2 line text display.

8.23 Mercury Protocol

8.23.1 Overview of Mercury Protocol

This section describes how to specify and configure the Mercury protocol for PW-5000/6000-like third-party panels.

It consists of two parts:

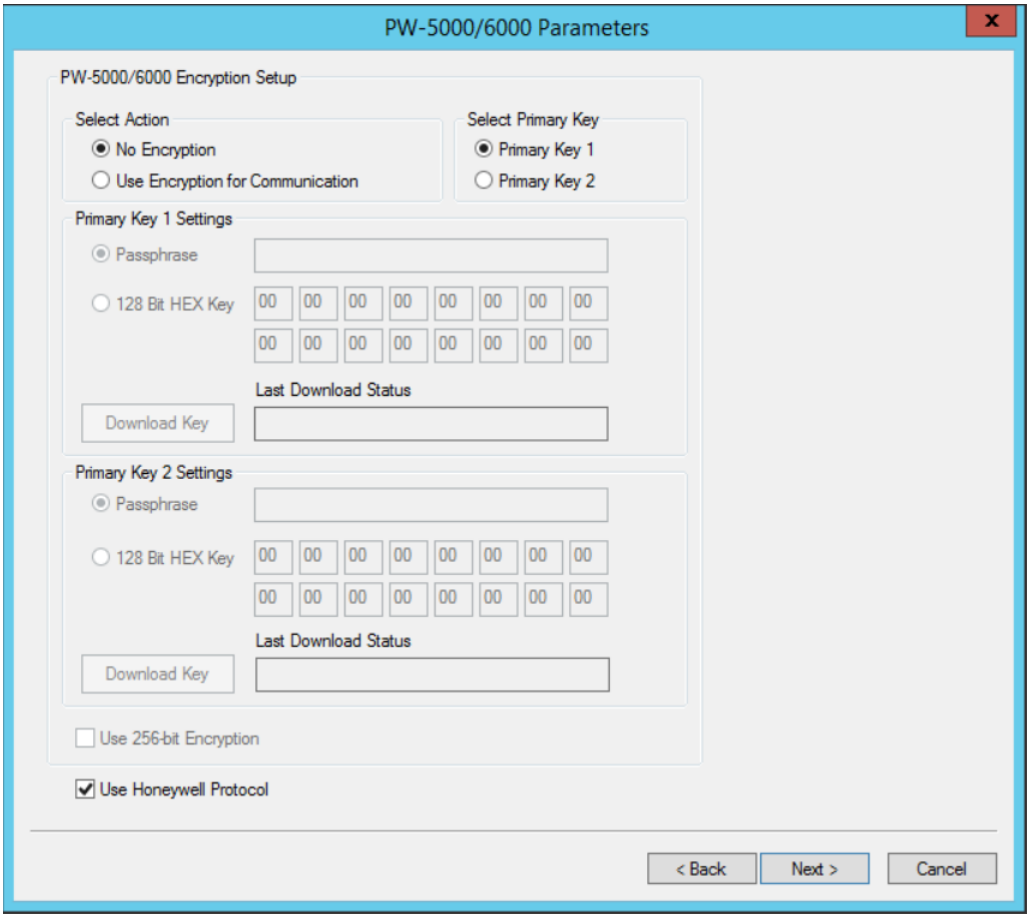
1. The first part describes how to specify the protocol type (Honeywell or Mercury) when the channel is defined. Once the channel is initially defined, this cannot be changed.
2. The second part describes how to create a panel by using Mercury protocol. Please note that a channel's protocol type controls the panels attached to that channel. A channel set up for Honeywell protocol will allow the same capabilities for panel definition, whether or not the panel definition wizard is used. Likewise, use of the PW-5000/6000 panel property sheets will not change for panels connected to a channel using the Honeywell protocol.

For channels using the Mercury protocol, the dialogs and property sheets used for panel definition and maintenance will be modified to restrict the types of panel and subpanel models available to those valid for the Mercury Standard protocol.

8.23.2 PART I: Unselecting the Honeywell Protocol

1. In the left navigation pane, select the appropriate **Site** in the **Hardware Configuration** tree-view.
2. Under the Site, double click the appropriate **Channel** icon to display the **Edit Channel** screen

3. Select the **PW-5000/6000 Parameters tab**:



Note: If the "Mercury Standard Protocol" option is enabled under Panels in the Software Keys module (only your Pro-Watch Software Keys Licensing Manager can do this for you), the **"Use Honeywell Protocol" check-box** is displayed at the bottom of the screen. The "**Use Honeywell Protocol**" check-box is checked by default. Once the channel is defined, this check box will be visible but disabled (grayed out).

Note: In earlier versions of Pro-Watch, this screen used to be dedicated to PW-5000/6000 Encryption only.

4. Unselect the "**Use Honeywell Protocol**" check-box.

8.23.3 PART II: Creating the Third-Party Panel

This section describes the panel creation process through two methods:

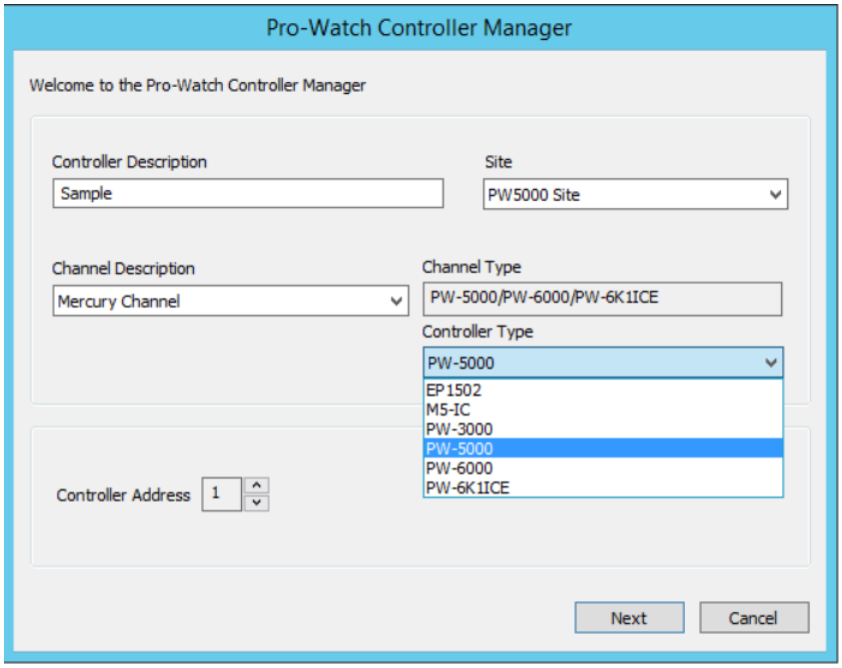
1. By using the user (panel definition) wizard, and
2. Without using the user (panel definition) wizard.

Note: The contents of some of the drop-down lists in the screenshots to follow are restricted to only those panel and subpanel types which are supported when using the Mercury Standard protocol.

8.23.3.1 By Using the User Wizard

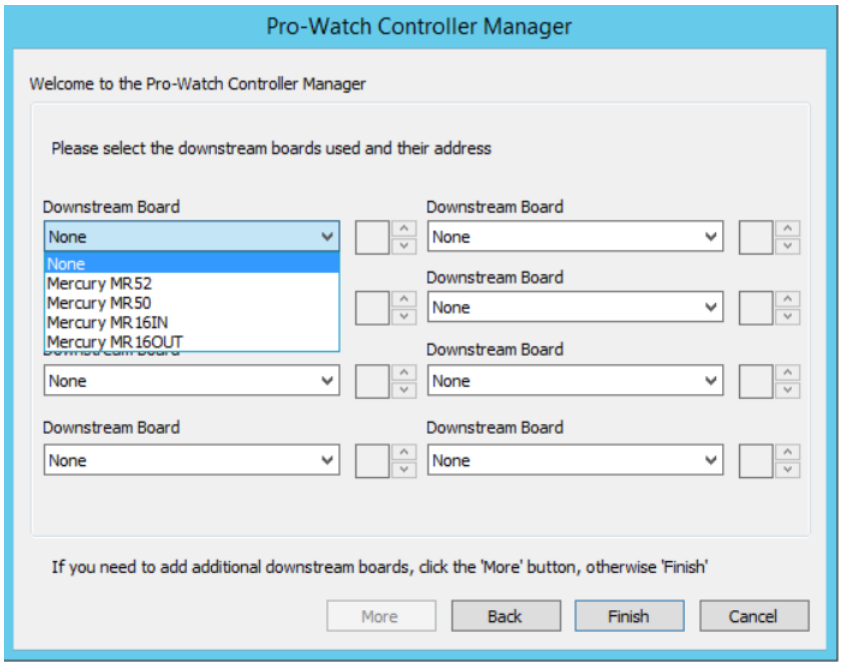
Note: For more information on the User Wizard, see "Turning the User Wizard On and Off". Unless the User Wizard is turned off by the user, it is displayed by default every time the user wants to create a new Panel or Logical Device.

1. Click **Hardware Configuration** on the left navigation bar.
2. Right-click the appropriate **Site** icon. From the pop-up menu, select **New > Panel** to display the **Pro-Watch Controller Manager** screen:

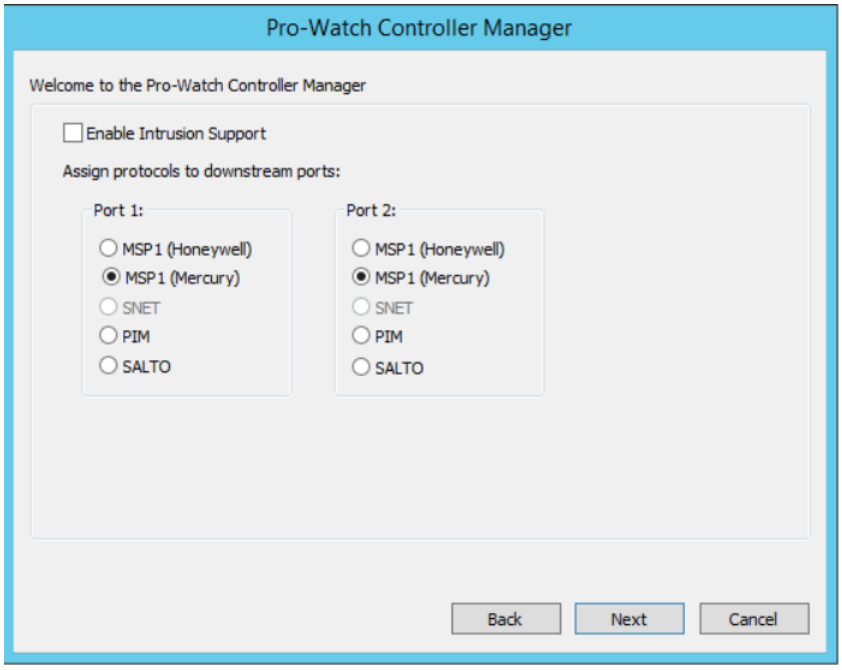


3. Click **Next**. The next screens to display will depend on whether you've selected PW-5000 or PW-6000 as Controller Type.

For **PW-5000 Controller Type**, you'll see the following screen:



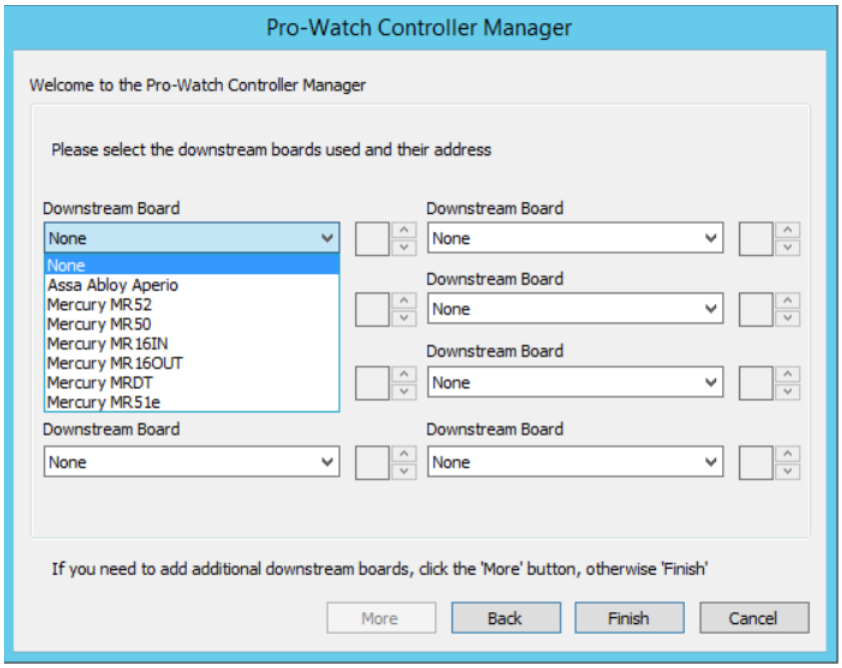
For **PW-6000 Controller Type**, when you click **Next** you will see the following screen:



Selecting the protocols determines what subpanel types can be added to the panel, and how many can be added for a given type. The two sets of radio buttons select the Port 4 and Port 6 protocols. SALTO routers require SALTO protocol, SNET readers require SNET

protocol, and Ingersol-Rand PIMs require PIM protocol. All other subpanels use the Mercury standard (MSP1) protocol.

4. Click **Next** to display the downstream subpanel selection screen:



Note: In both screens, please note the restricted number of subpanel selections in the **Downstream Board** drop-down list.

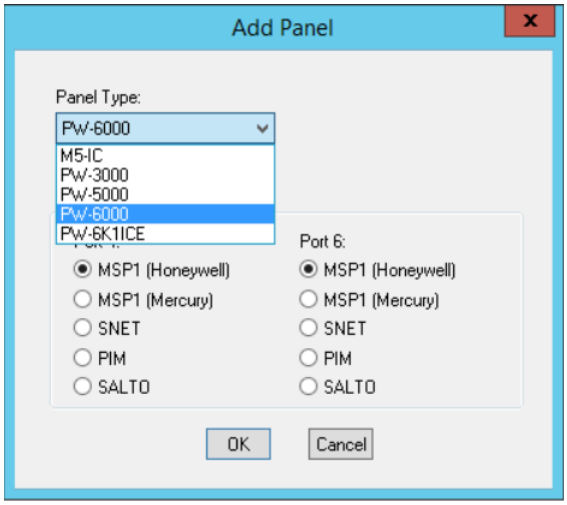
5. Make the necessary selections and click **Finish**.

8.23.3.2 Without Using the User Wizard

Note: For more information on the User Wizard, see "Turning the User Wizard On and Off". Unless the User Wizard is turned off by the user, it is displayed by default every time the user wants to create a new Panel or Logical Device.

1. In the **Hardware Configuration** module, select a **Site** and a **Channel**.

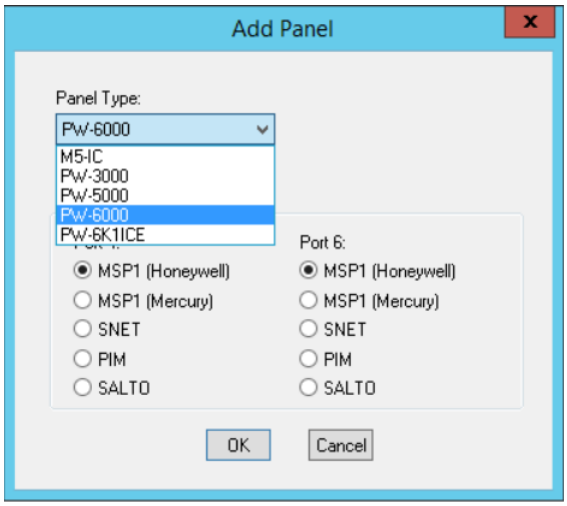
2. Right-click on a **Channel** icon to display the pop-up menu. Select **New > Panel t**o display the **Add Panel** dialog box. Here are the **panel options** available:



3. If you select **PW-6000** panel, go to the "PW-6000 Controller Panel Option" section.
4. If, on the other hand, you select **PW-3000**, **PW-5000**, or **PW6K1ICE**, go to the "PW-5000 and PW-3000 Controller Panel Options" section.

8.23.3.3 PW-6000 Controller Panel Option

If at the **Add Panel** screen you have chosen **PW-6000** from the **Panel Type** drop-down list, proceed as follows:



1. Select the appropriate **Protocol** for **Port 4** and **Port 6**. For both ports, select:
   - SALTO option-button if you are using SALTO routers.
   - SNET option-button if you are using SNET readers.

- PIM option-button if you are using Ingersol-Rand PIMs.
- MSP1 (Honeywell) or MSP1 (Mercury) option-button if you have any subpanels that use either the Mercury or Honeywell protocol.

2. Click **OK** to display the **Add Panel** dialog box and continue with **Step 1** in the "PW-5000 and PW-3000 Controller Panel Options" section (below) since the rest of the steps are identical.

8.24 Mercury Intrusion

8.24.1 Overview of Mercury Intrusion

MRDT acronym stands for "**Mercury Display Terminal**" (with Keypad). Pro-Watch can accommodate Mercury Intrusion hardware like the Mercury MRDT with keypad, as shown below:



Figure 8-4 MRDT, Mercury Display Terminal with Keypad

This appendix explains what you need to do to integrate the Mercury Intrusion keypad with the Pro-Watch system.

8.24.2 Prerequisites

8.24.2.1 PW-6000 IC "2.071" Firmware

The "2.071" firmware that the PW-6000 IC panel is shipped with is the minimum firmware that can be used for the Mercury Intrusion functionality.

8.24.2.2 32 Access Levels / Clearance Codes

Note: Throughout this chapter the terms "**Access Level**" and "**Clearance Code**" are used interchangeably. They mean the same thing.

Note: To configure the panel to use 32 access levels, see "Setting Card Options for PW-5000/6000/6101 Panels" in Chapter 5.

Caution: The use of Mercury Intrusion and configuring the panel to use 32 access levels are mutually exclusive.

- If the access level count is set to 32, then no panels can be configured to use Mercury Intrusion.

- If the user wants to configure the system for 32 access levels per card instead of the default of 12, then the user will not be able to use Mercury Intrusion.

8.24.2.3 PW-6000 Panel or Equivalents

Mercury Intrusion works only with the PW-6000 panel or PW-6000 equivalents like the EP2500. With the EP2500, you must use the Mercury protocol instead of the Honeywell protocol.

8.24.3 New Tabs for Mercury Intrusion

8.24.3.1 Prerequisites for the New Tabs

When the following prerequisites are satisfied, Pro-Watch displays the new tabs in the panel editing screen:

1. The panel type is **PW-6000** or equivalent **EP2500**.
2. Mercury Intrusion is configured in software keys and the user has installed the appropriate Pro-Watch software key license.
3. The number of clearance codes is left at the default value of 12 (twelve).
4. The "**Enable Intrusion Support"** check-box is selected when creating the new panel.

Mercury Intrusion support adds a few new tabs to the panel properties and reader properties screen.

8.24.3.2 New Panel Tabs

1. **Map Clearance Codes** tab specifies which clearance codes can be assigned to a reader command map.
2. **Intrusion Groups** tab is where intrusion groups get defined. Intrusion Groups are collections of Intrusion Zones (i.e., monitorable inputs used for intrusion).

8.24.3.3 New Reader Tabs

1. **Intrusion Command Maps** tab is used to assign clearance codes to a custom command map, which controls what intrusion commands users with the clearance code can perform.

2. **Intrusion Settings** tab assigns the MRDT logical device to the Intrusion Display Settings and the Intrusion Group. Users can also configure certain keypad behaviors on this tab.

8.24.4 Panel Tabs

8.24.4.1 Map Clearance Codes Tab

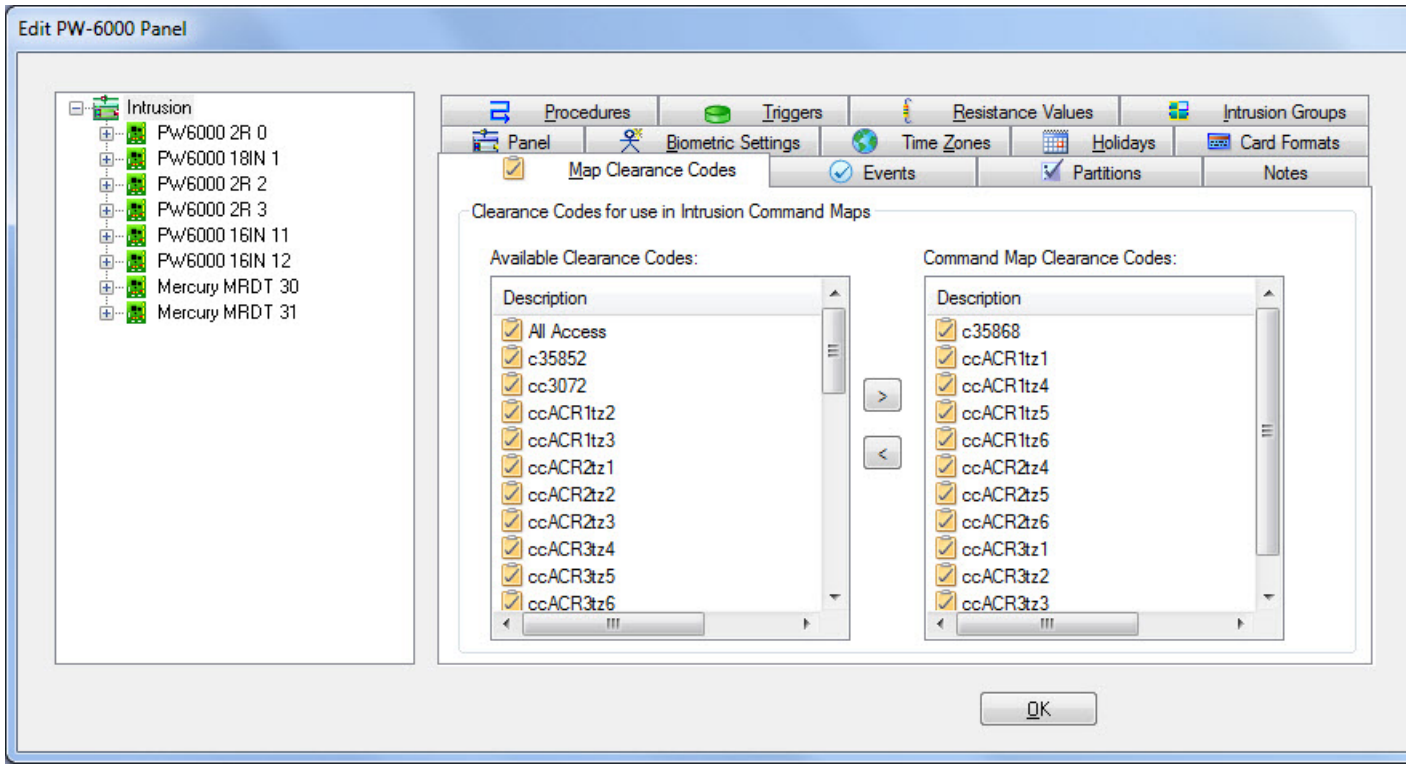


Figure 8-5 Map Clearance Codes Tab

The **Available Clearance Codes** list box on the left displays the clearance codes with access to the defined MRDT terminal logical devices. Up to 12 of them can be moved to the **Command Map Clearance Codes** list box on the right by selecting them and clicking the right arrow.

The set of clearance codes marked as "**Command Map Clearance Codes**" will be displayed under the "Map Clearance Codes" drop-down lists on the reader's Intrusion Command Maps tab (see the next section).

8.24.4.2 Intrusion Groups Tab

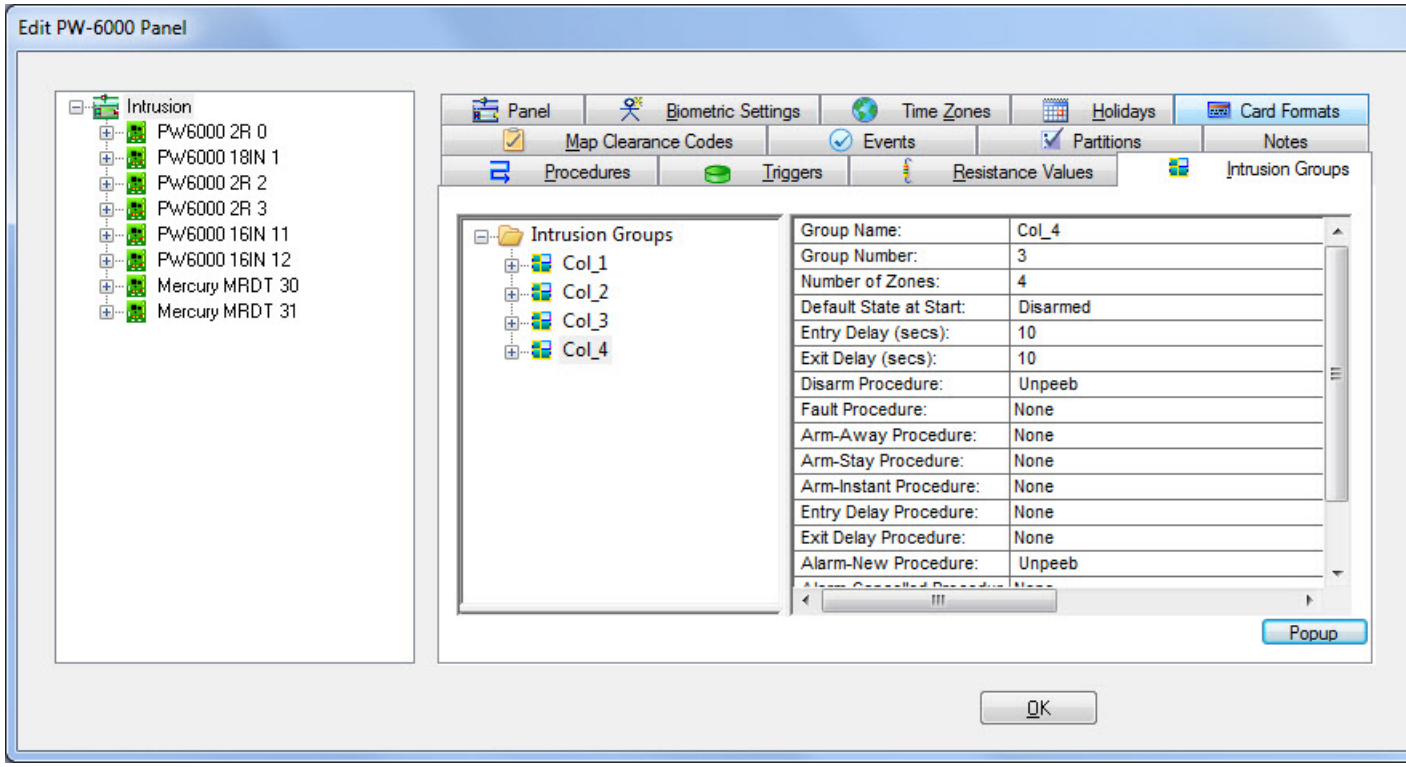


Figure 8-6 Intrusion Groups Tab

Intrusion groups are collections of Intrusion Zones (i.e., monitorable inputs used for intrusion).

1. Click on each **Intrusion Group** in the navigation tree-view to display its **Intrusions Zones**.
2. Configure the attributes of each group by selecting the appropriate options in the right panel.

8.24.5 Reader Tabs

8.24.5.1 Intrusion Command Maps Tab

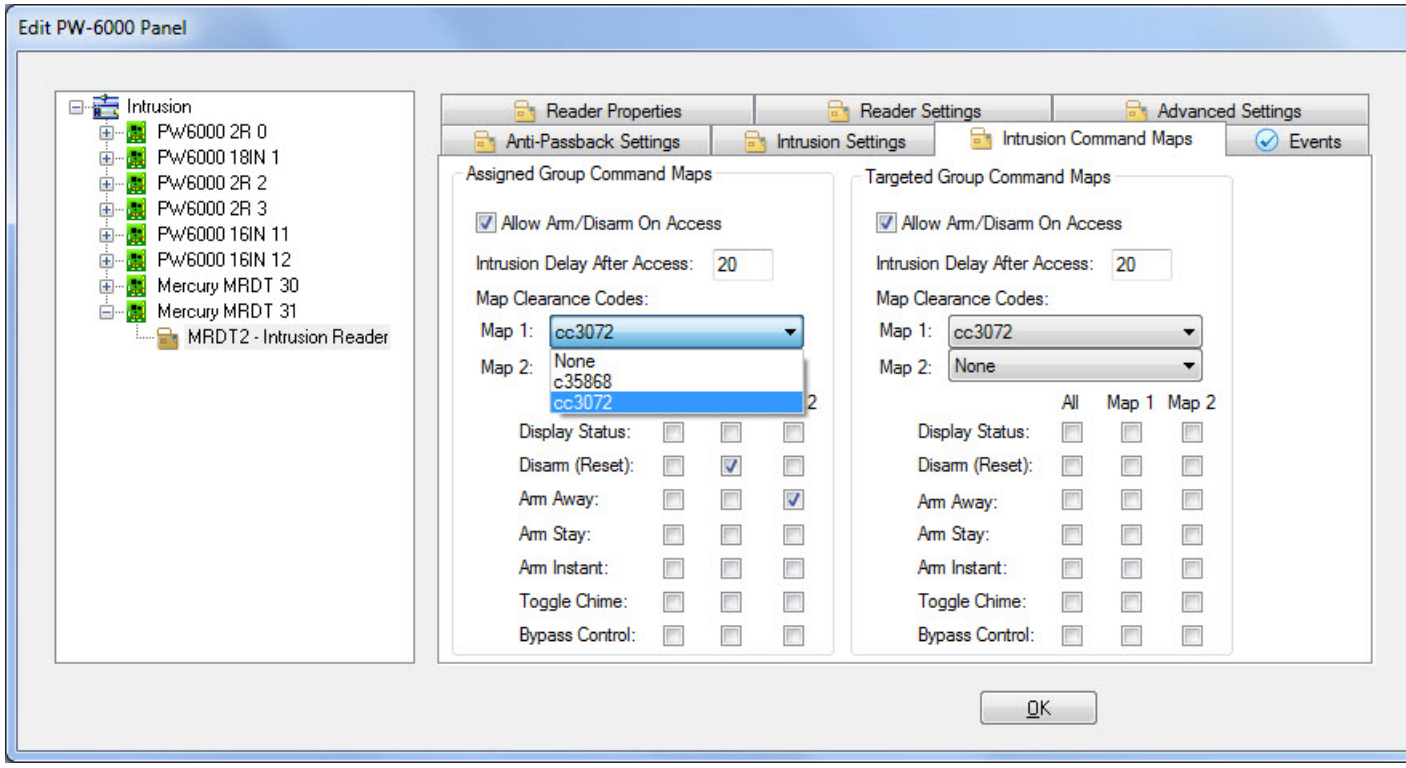


Figure 8-7 Intrusion Command Maps Tab

The **Intrusion Commands Maps** tab controls the permissions that users have to perform intrusion commands. Additionally, this tab allows the user to configure command maps resulting in further customization of user permissions.

8.24.5.2 Intrusion Settings Tab

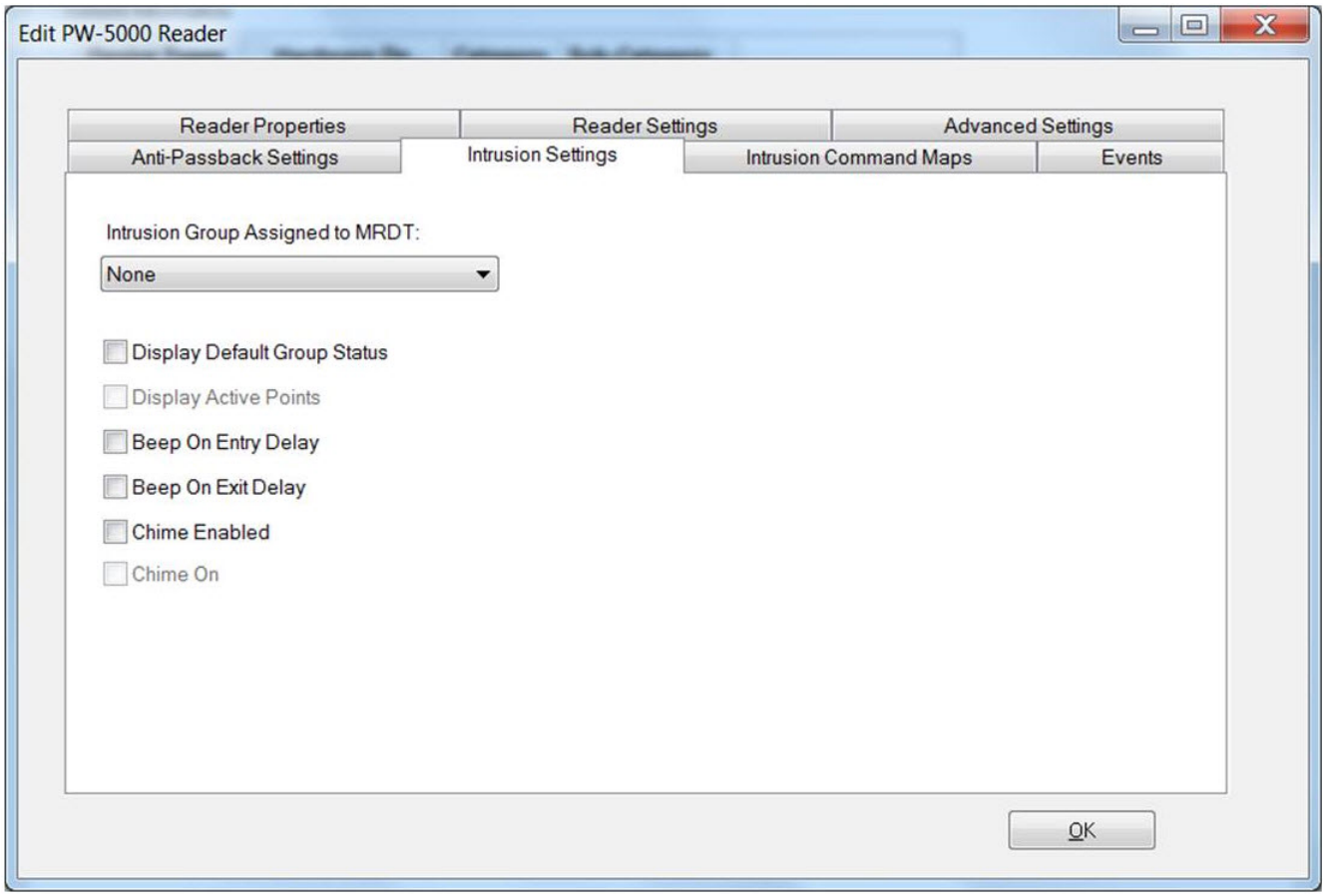


Figure 8-8 Intrusion Settings Tab

1. Configure the **Intrusion Display Settings** by selecting an appropriate options form the drop-down menu.
2. Configure the **Intrusion Group Assigned to MRDT** by selecting an appropriate options form the drop-down menu.
3. Configure various **display options** by selecting the respective check-boxes from the list.
4. Click **OK** when you're done.

8.24.6 General Steps

In order to setup and use the MRDT Intrusion, the user must follow the below sequence of procedures:

1. Obtain a valid Pro-Watch license with the Mercury Intrusion enabled. For more information, see the *Software Key User Guide, Document # 800-08123V5*.

2. Install that license to your Pro-Watch machine. For more information, see the *Pro-Watch Installation Guide, Document # 7-901073V5*.
3. Configure the Mercury Intrusion Settings in the Database Configuration module. See "Configuring the Mercury Keypad Settings".
4. Configure the PW-6000 panel to enable Mercury Intrusion support.
5. Create Intrusion Zone logical devices.
6. Create Intrusion Groups. Click here to learn how: "Creating an Intrusion Group on Panel"
7. In the Intrusion Groups tab of the Panel Properties screen, assign Zones to the Groups. Click here to learn how.
8. Configure Intrusion Terminal settings.
9. Create MRDT Intrusion Terminals. Click here to learn how.
10. Configure Intrusion Terminal Command Maps. Click here to learn how.

When all these steps are completed, the task of configuring the MRDT will be accomplished.

8.24.7 Software License for Mercury Intrusion

The Mercury Intrusion feature is governed by the Software License feature "Mercury Intrusion" under the "Optional" category of the software license.

If this feature is not enabled in the software license, users will NOT be able to

1. set the port protocols of the IC to "MSP1 Intrusion" under panel properties, and
2. mark the panel to support intrusion as "Intrusion Enabled" under when creating the panel.

Both of these are required for intrusion features to work correctly.

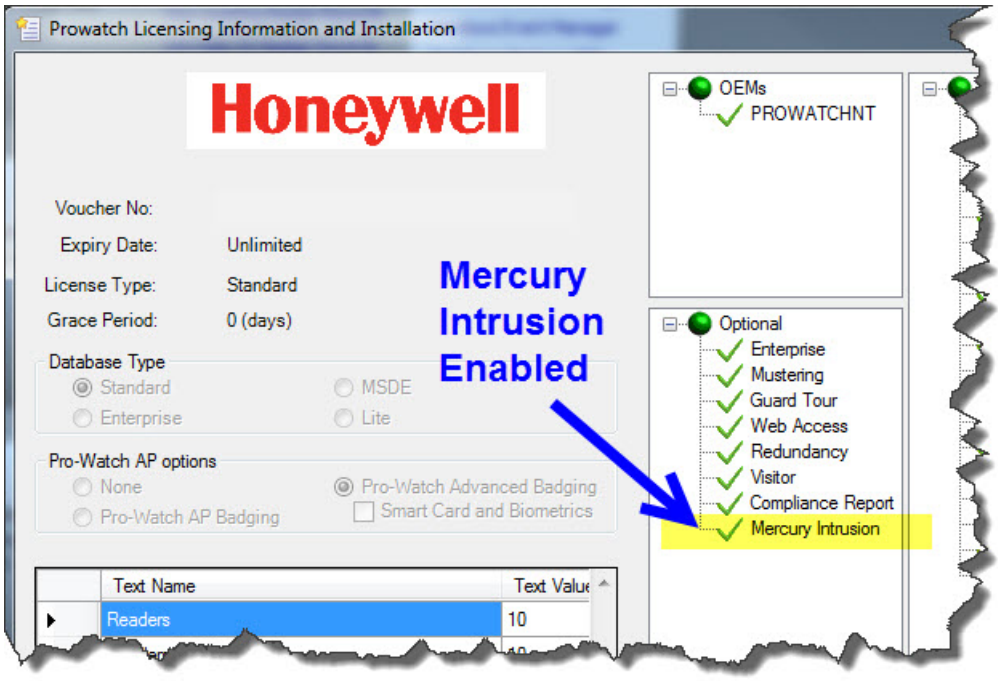


Figure 8-9 Software License Feature for Mercury Intrusion Enabled

8.24.8 Mercury Intrusion Configuration Restrictions

1. If the MRDT is wired as a subpanel, the RS-485 port that the Terminal is connected to must be configured for protocol "MSP1 Intrusion." Users will not be able to add the MRDT as a subpanel if the port is not selected for this protocol.
2. Ports marked for "MSP1 Intrusion" protocol will ONLY support the MRDT terminal. Standard MSP boards (Reader, I/O, etc) subpanels will not be supported on these ports. Ports marked for "MSP1" protocol will ONLY support standard MSP boards. Adding a MRDT as a subpanel will not be supported on these ports.
3. In order for Intrusion to work properly, Zones/Inputs are required so the IC must be connected to corresponding I/O boards. This means that at maximum, only one (1) RS-485 Port can be marked for "MSP1 Intrusion" for the IC.
4. If the MRDT Terminal is wired off the reader port, the "MSP1 Intrusion" protocol is not required for the RS-485 port. However, the panel must be marked for "Intrusion Enabled" under the panel properties in order for correct operation.
5. A complete intrusion system is controlled by one (1) IC. One (1) IC is capable of supporting multiple zones, groups, and MRDT Display

Terminals. There is no way for a MRDT Display Terminal to control zones and view alarms of zones/groups on another ICs.

6. If Intrusion is configured, Pro-Watch will not allow 32 clearance code support and vice versa.
7. Each MRDT Display Terminal may have a reader wired off of it (refer to the Mercury MRDT documentation for wiring information). Therefore, each MRDT Display Terminal is treated as a reader and will count against the panel's reader count even if an external reader is not connected to the MRDT Display Terminal.

8.24.9 Configuring the Mercury Keypad Settings

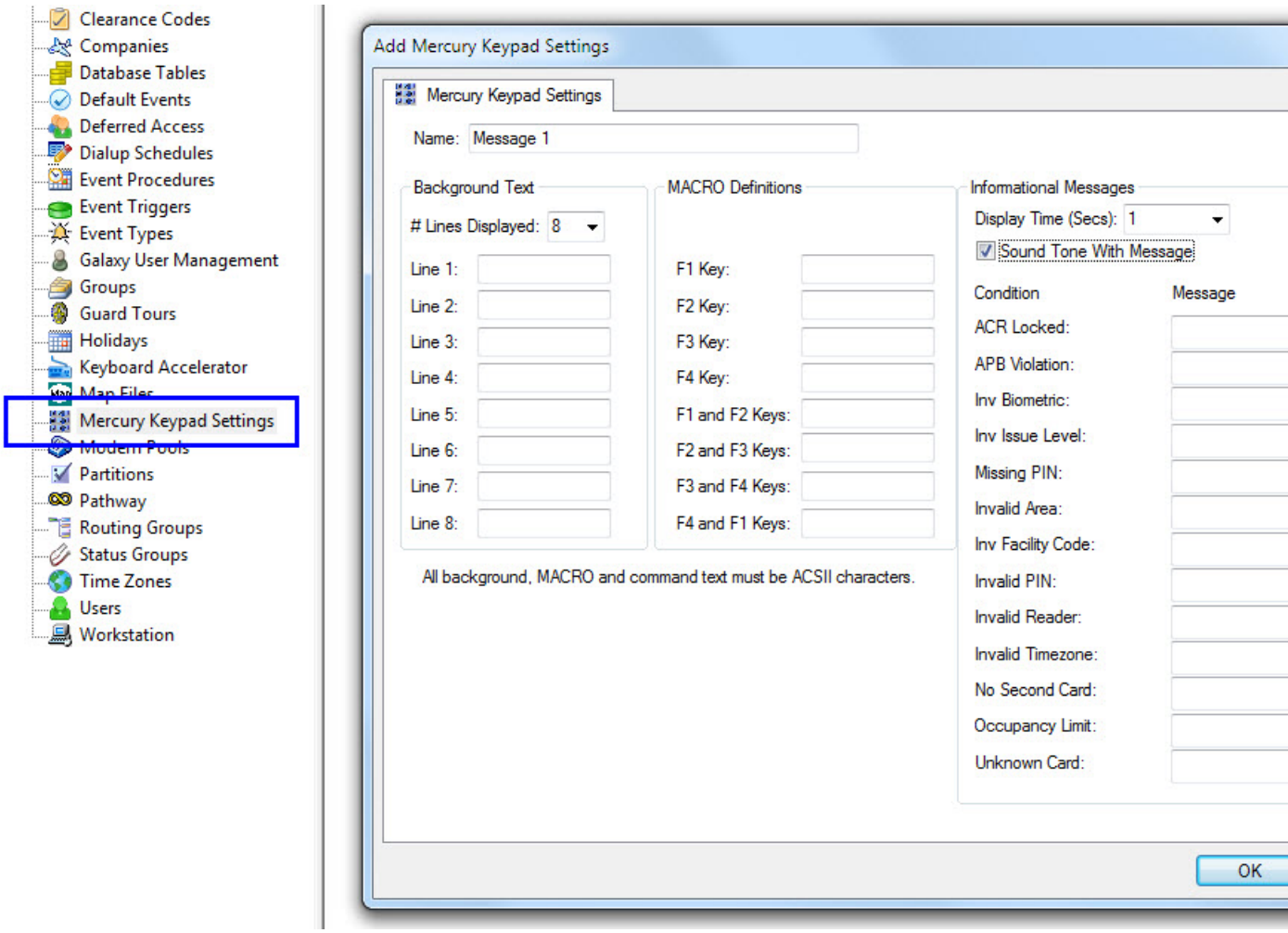


Figure 8-10 Edit Mercury Keypad Settings

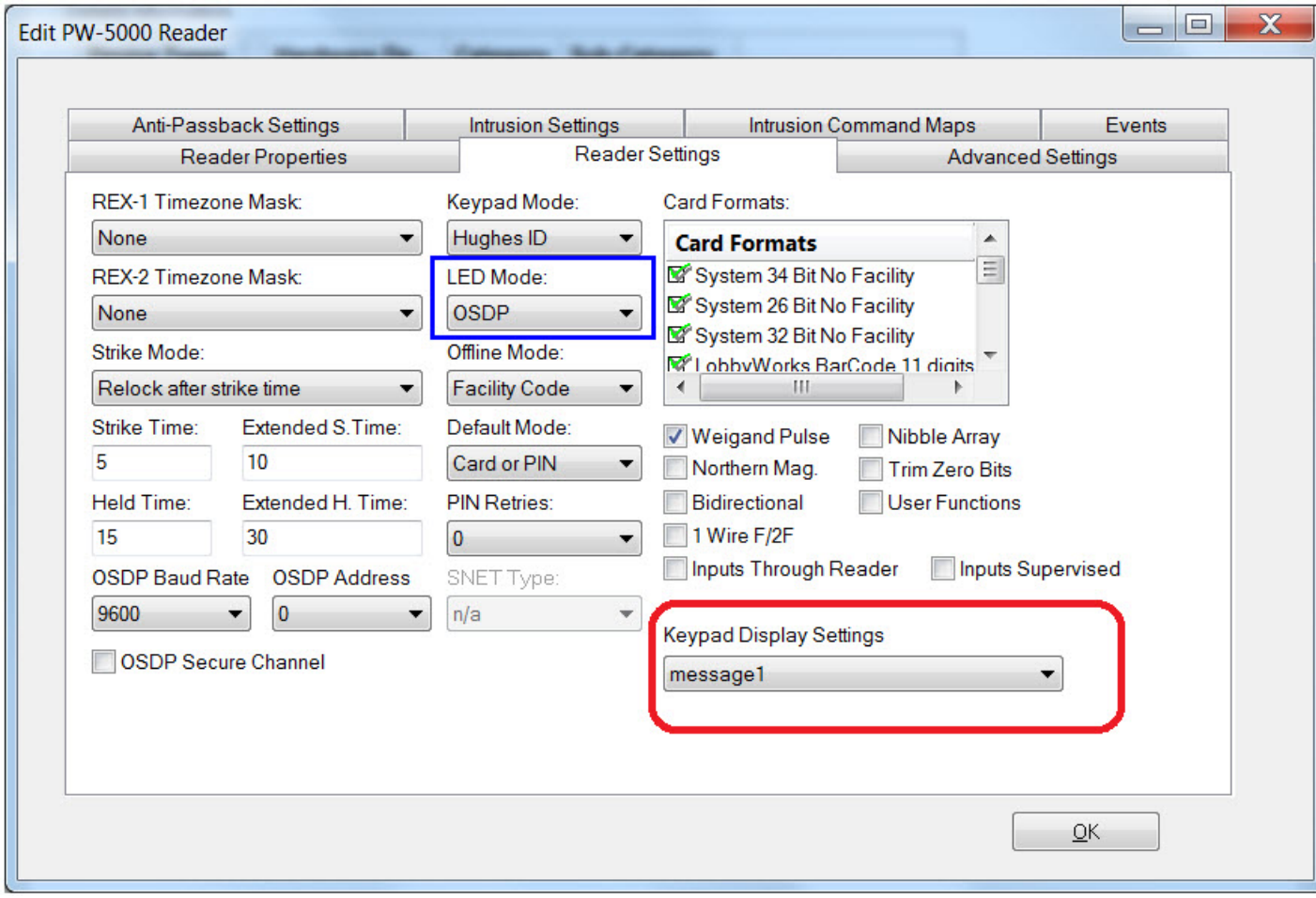
1. In Pro-Watch's **Database Configuration** module, click the **Mercury Keypad Settings** link to display the list of settings in the right pane that will be used for the MRDT display.
2. Right-click and select "**New Mercury Keypad Settings**" to create a new Mercury Keypad Settings or double-click on a selected setting to display the "**Edit Mercury Keypad Settings**" dialogue box.
3. Use the **Background Text** fields to add optional text lines (up to a maximum of 8) to display in MRDT's text window.
4. Define function key sequences for the MRDT by entering the desired values into the **F-Key** fields in the **MACRO Definitions** pane. **Macros** are shortcuts that allow users to enter commands without typing out having to enter the whole command. For example, to disarm a group, the user would have to enter "[Command][Group Code]1[Command]"; instead of doing that manually, a function F-Key can be tied to the command so to disarm a group, all the user would have to do is press the "F1" key. **Note:** The [Command] button corresponds to the hash-tag (#) character so to create a macro to disarm the group, enter "#[Group Code]1#" into the desired F-key.



These display settings will be carried over to the "Intrusion Settings Tab" for the MRDT terminal logical devices.

8.24.9.1 Keypad Display Settings

The display message created in **Mercury Keypad Settings** is displayed in the **Keypad Display Settings** drop-down list of the **Reader Settings tab** of **Edit PW-5000 Reader** screen, as shown below:



Note: You must select "**OSDP**" as **LED Mode** to enable the **Keypad Display Settings** drop-down list.

8.24.10 Configuring the PW-6000 Panel

8.24.10.1 Adding Intrusion to Panel (With Wizard)

When creating the PW-6000 panel in Pro-Watch, the user will be presented the option "Enable Intrusion Support." With this check-box selected, the user will be allowed to select "Intrusion" under the port.

Note: Intrusion can only be selected on one port. Once it is selected on one port, the intrusion selection will become unavailable for the second port. Select "Intrusion" for Port 4 to attach MRDT keypad directly to the port. If you do that for Port 4, the "Intrusion" option for Port 6 will be disabled since

other subpanel types cannot be connected to a port set up for Intrusion support. Since MRDT subpanels have no inputs, the inputs required for intrusion zones must be defined on some other subpanel type (e.g., a 2-reader board or a 16-input board). For this reason, one cannot have both ports set up for intrusion.

1. Select the “Enable Intrusion Support” check-box and select the “Intrusion” protocol button either for Port 4 or Port 6.

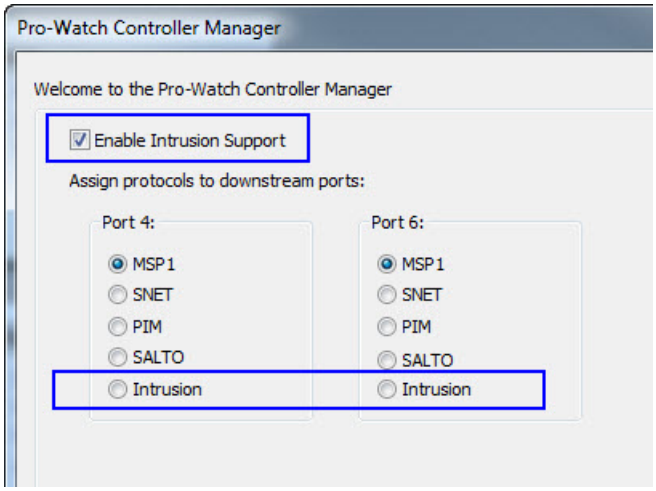


Figure 8-11 Intrusion Support Selection Options

2. Click **OK** to add all the **IO modules** you need in the next screen.
3. Click **Add** to assign **addresses** in the next screen to the IO modules you have specified.
4. Click **Add** to display the **Add Panel Progress** screen.

8.24.10.2 "Intrusion Enabled" Check-Box in Panel Properties

The "Intrusion Enabled" check-box is also available under the panel properties after the panel has been created. This check-box designates if the panel supports intrusion.

After selecting “Intrusion Enabled,” the user must confirm changes to the panel and then go back into the panel in order to see the "Intrusion Groups" and "Map Clearance Codes" tab. User will also need to initialize the panel and perform a system download.

Notes: There are a couple of notes regarding the "Intrusion Enabled" panel check-box:

- If "Intrusion" support is not selected at panel creation, then the "MSP1 Intrusion" port protocol will not be available until the "Intrusion Enabled" check-box is selected.

- Once a port has been designed for MSP1 intrusion, the "Intrusion Enabled" check-box will become grayed out and read-only. To change this field again, user must deselect the "MSP1 Intrusion" from the Port 4/6 protocols.
- If the MRDT is connected off the 2-Reader board (no MRDT connected to the RS-485 port of the IC), the user must still select the "Intrusion Enabled" check-box in order for correct operation of the intrusion hardware.

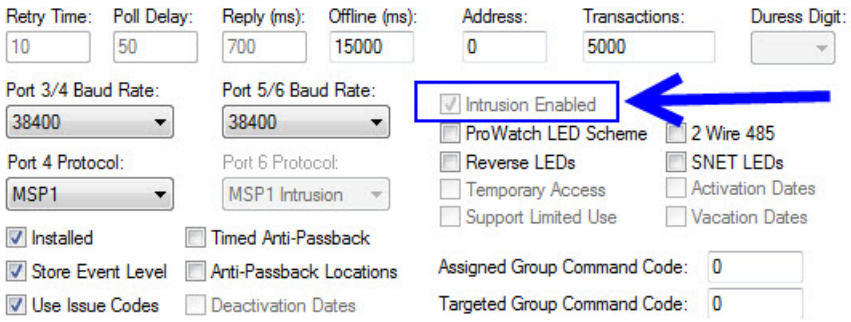


Figure 8-12 "Intrusion Enabled" Check-Box in Panel Properties Screen

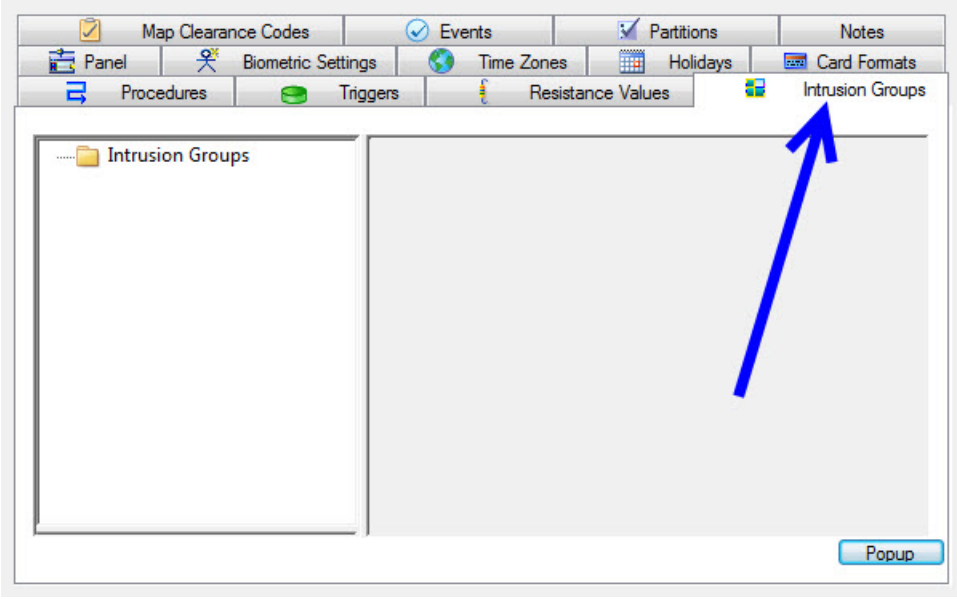


Figure 8-13 "Intrusion Groups" Tab

Once the "Intrusion Enabled" check-box is selected under the panel, the user will be presented with a new tab under panel properties for "Intrusion Groups." This is where the users will create and designate intrusion groups.

Note: After selecting "Intrusion Enabled" for the first time, the user must confirm changes to panel and then go back into the panel in order to see the "Intrusion Groups" tab.

8.24.10.3 Adding Intrusion to Panel (Without Wizard)

If the **Panel Add Wizard** is not used, the layout of the panel add screen for Intrusion will look different, but behave the same way as if using the Wizard.

Select the "**Enable Intrusion Support**" check-box to enable the Intrusion port protocol for Port 4 and Port 6. Follow additional steps documented in "Adding Intrusion to Panel (With Wizard)".

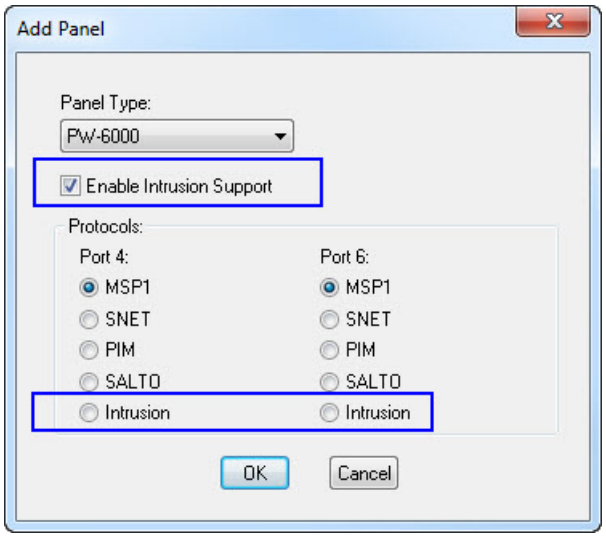


Figure 8-14 Enable Intrusion Support and Intrusion Protocol Buttons

8.24.11 Setting Intrusion Command Codes

The MRDT Display Terminal command codes are as follows:

Table 1: MRDT Display Terminal command codes

Code	Description
Command 1	DISARM
Command 2	ARMED - AWAY
Command 3	ARMED - STAY
Command 4	ARMED - INSTANT
Command 5	Toggle Chime ON/OFF

Table 1: MRDT Display Terminal command codes

Code	Description
Command 6	BYPASS
Command 0	SYSTEM STATUS

The MRDT can only be assigned to one (1) intrusion group, however one (1) intrusion group can be assigned to multiple MRDTs. The user may also be granted the ability to control other intrusion groups through the MRDT provided that the group number is known.

Actions performed on the MRDT are governed by two command code prefixes, which must be entered before the command. This tells the MRDT whether the command will be run on the assigned group or target group.

1. Assigned Group Command Code: The default assigned Intrusion Group for the MRDT.
2. Targeted Group Command Code: Controls a target Intrusion Group provided that the Pro-Watch Intrusion Group number is known.

The **Assigned** and **Targeted Group Command Codes** are set at the panel level via panel properties. The command codes can be any sequence of numbers that the user selects provided that the **Assigned Group Command Code** is not the same as the **Target Group Command Code**.

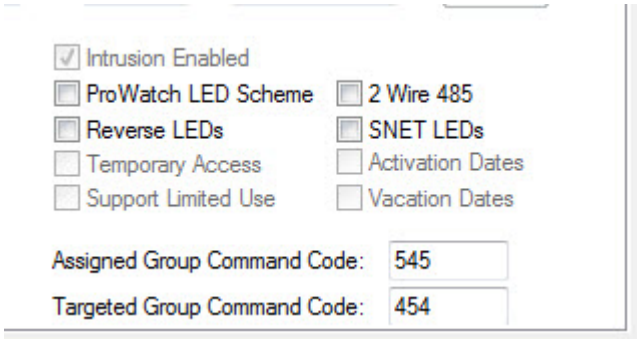


Figure 8-15 Command Code Prefixes

The MRDT commands are in one of the following formats:

1. *COMMAND* [Assigned Group Prefix] [Command Number] *COMMAND*
2. *COMMAND* [Targeted Group Prefix] [Group Number] [Command Number] *COMMAND*

For example, based on the group numbers above ("545" and "454):

1. **Arm Assigned Group:** *COMMAND* 5452 *COMMAND* (For armed away)

2. **Disarm Assigned Group:** *COMMAND* 5451 *COMMAND*
3. **Arm Targeted Group:** *COMMAND* 454002 *COMMAND* (Group #00, for armed away)
4. **Disarm Targeted Group:** *COMMAND* 454001 *COMMAND* (Group #00)

8.24.12 Introduction to Intrusion Zones

Intrusion zones must be created before they can be assigned to an Intrusion Group. A "zone" is a monitorable input. However, the door position switch (DPS) of an access control reader (ACR) can also be used, which means that forced door or held door events can trigger group alarms.

To support the Intrusion hardware, there are new templates and classes that were added for the Zones, Groups, and Terminals.

For the Intrusion Zones:

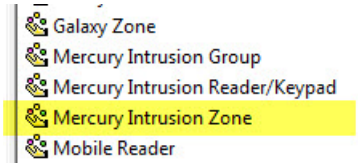


Figure 8-16 Zone Hardware Template

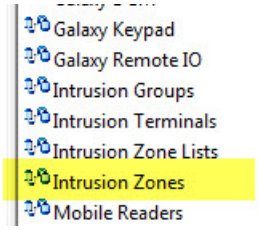


Figure 8-17 Zone Hardware Class

8.24.13 Zone Types and Modes

The type and mode of the Zone can only be configured when the Zone is part of a group. Likewise, Zone commands (Activate, Bypass, Disable) will not work unless the Zone is configured to a group.

8.24.13.1 Zone Modes

Zones can have three (3) modes (Default on startup or configured via hardware actions):

1. **Normal:** An open zone event will be used as input in determining the group state.

2. **Bypassed:** Zone status will be disregarded until the next disarm for the group.
3. **Disabled:** Zone will be disregarded until it is again explicitly put into normal mode.

8.24.13.2 Zone Types

There are three (3) types of Zones:

1. **24-Hour Zones:** These zones are always monitored, even if the group is not armed.
2. **Perimeter Zones:** These zones will be monitored during the Arm-Stay, Arm-Away, or Arm-Instant modes.
3. **Interior Zones:** These zones will be monitored during the Arm-Away mode.

Alternatively:

1. **Arm Away:** 24-hour zone, Interior Zone, Perimeter Zone
2. **Arm Stay:** 24-hour zone, Perimeter Zone
3. **Arm Instant:** 24-hour zone, Perimeter Zone

Note: Depending on the "Group Arm" type, Zone Faults may or may not affect whether the Group can be armed. For example: An Arm-Stay or Arm-Instant do not monitor the Interior Zone. Arm-Away does monitor the Interior Zone.

8.24.14 Entry Delay Types

An entry delay is a set amount of time for the user to disarm the group at the terminal before the group goes into alarm. If the zone is not using entry delay or using Entry Delay Follow, then an activation of the zone while the group is armed will automatically cause the group to go into alarm.

Each zone may be configured for one (1) of the following entry delays types:

1. **None/Not Used:** Zone does not trigger an entry delay and cannot be active during an entry delay.
2. **Entry Delay Trigger:** Zone will trigger an entry delay. Entry delay time is set at the group level in panel properties.
3. **Entry Delay Follow:** Zone may be active during an entry delay, but will not trigger an entry delay.

Note: The Entry Delay ONLY works for the Arm-Stay and Arm-Away modes.

8.24.15 Creating Intrusion Zone (With Wizard)

Zones are essentially logical devices. Thus a logical device must be created for the zone.

- For Zones to be set up as monitorable inputs, a monitorable input logical device must be created.
- For Zones to be set up for an ACR, the ACR must be created.

To create a Zone, start the process for creating a new logical device.

Set the Hardware Template to "Mercury Intrusion Zone" and the Hardware Class for “Intrusion Zones.” Select the hardware that will be used for the Zone.

Note: This above step will only be for Zones set up as a monitorable input.

For Zones set up as an ACR, go through the normal process of creating an ACR. These Zones will be available for adding to the Group later when defining the group in the panel.

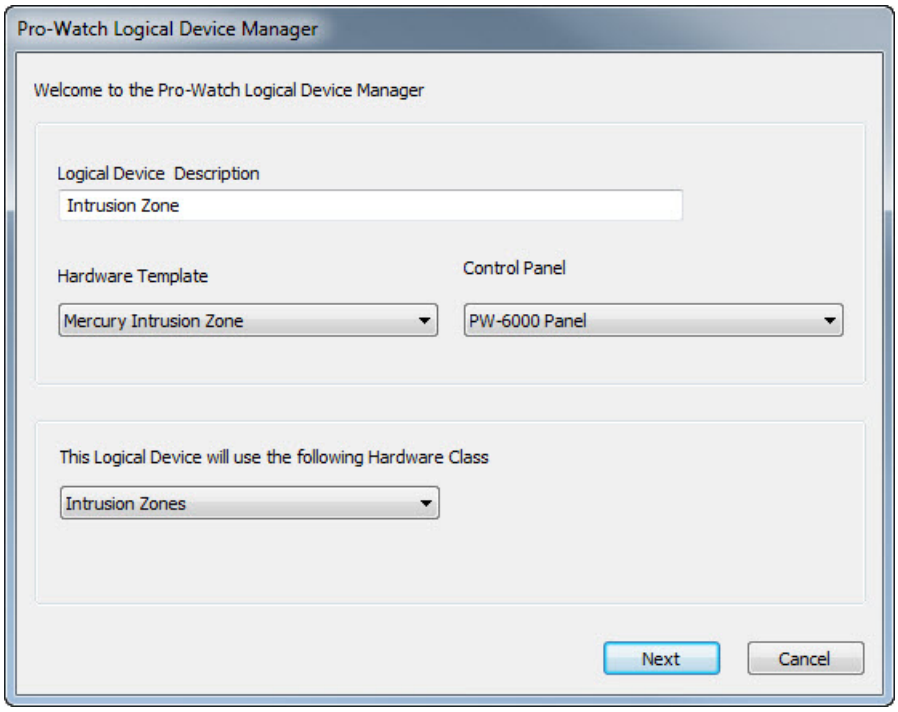


Figure 8-18 Intrusion Zone Logical Device Creation

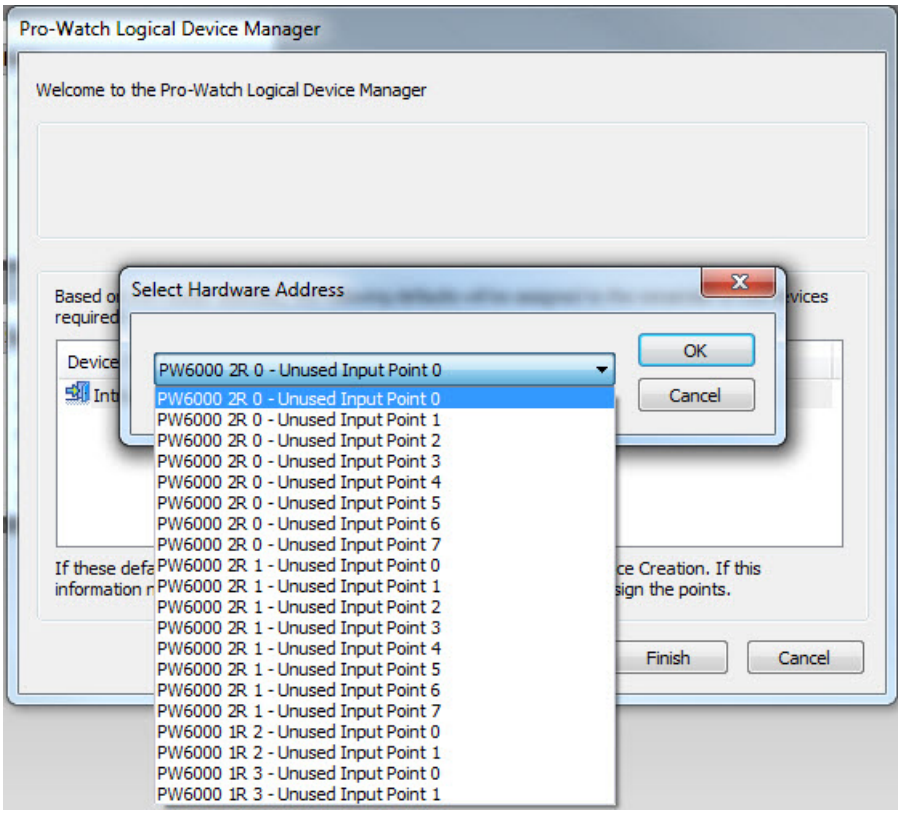


Figure 8-19 Intrusion Zone Hardware Address Selection

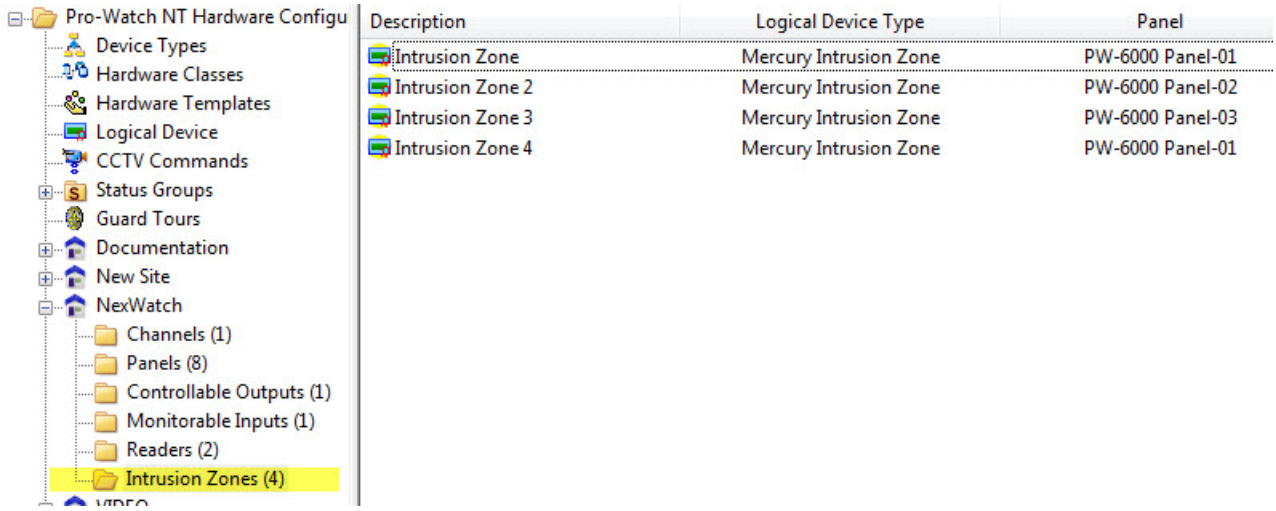


Figure 8-20 Intrusion Zone Logical Devices

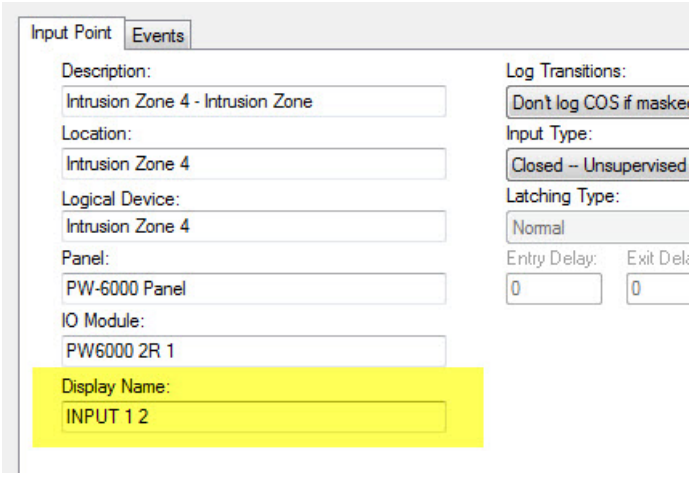


Figure 8-21 Intrusion Zone Display Name

Figure 8-21 on page 109 shows an input configured as an Intrusion Zone. Note that a new field called "Display Name" has been added to the input point properties. This field contains text which will be displayed on the MRDT Terminals in conjunction with any status messages involving the Zone. The contents of this text box must be ASCII characters.

After the Zone has been created, triggering the Zone generates events for "Intrusion Zone Active" and the "RTN" in the Pro-Watch Event Viewer.

Resource Id	Address	Hardware	Point Description	Logical	Event Type	Mes
PW6K_225::05	10621	0	Intrusion Zone Active - RTN	Intrusion Zone	Zone Active	
PW6K_225::05	621	0	Intrusion Zone Active	Intrusion Zone	Zone Active	
PW6K_225::05	10621	0	Intrusion Zone Active - RTN	Intrusion Zone	Zone Active	
PW6K_225::05	621	0	Intrusion Zone Active	Intrusion Zone	Zone Active	

Figure 8-22 Zone Events in Event Viewer

8.24.16 Creating Intrusion Zone (Without Wizard)

When adding an Intrusion Zone without the Wizard, the user must manually specify the hardware template and hardware class for the Zone. After assigning the hardware point for the zone, the Intrusion Zone is created.

The Zone display name can be configured by accessing the Zone properties either through the panel or the logical device (See Figure 8-21 on page 109).

The Zone should already be reporting events (See Figure 8-28 on page 112).

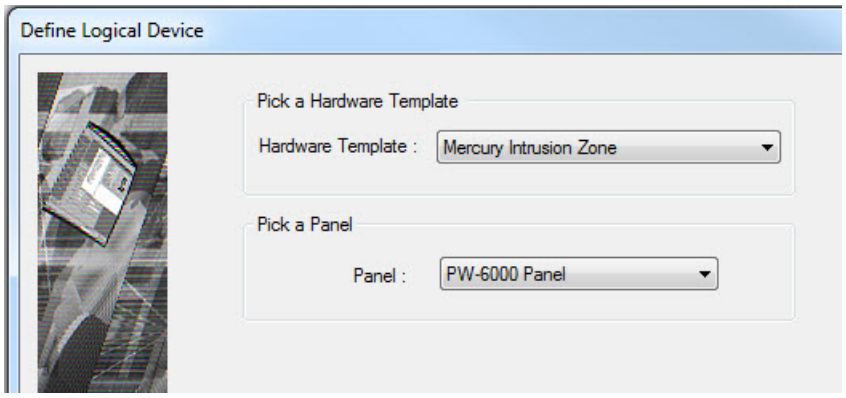


Figure 8-23 Selecting Hardware Template

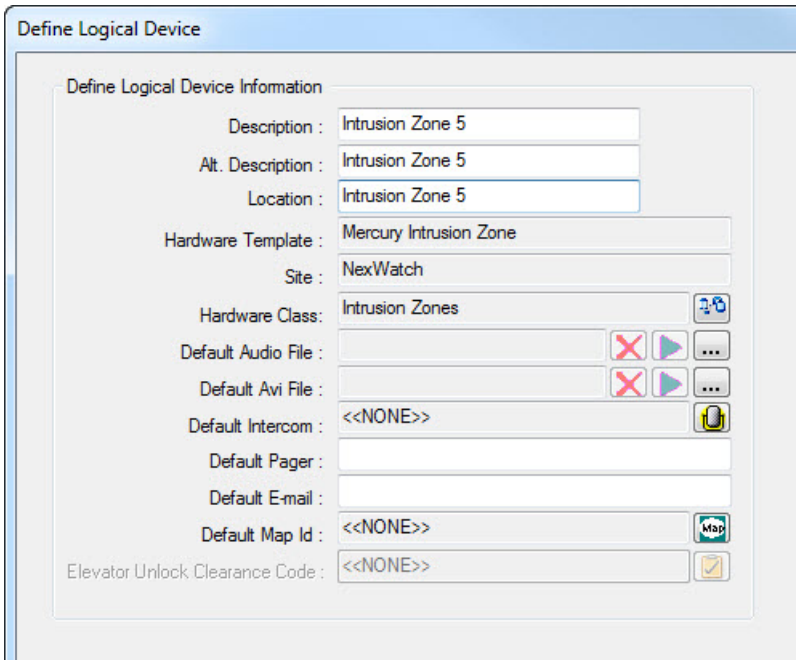


Figure 8-24 Logical Device Details

8.24.17 Adding Intrusion Groups and Configuring Zones under Panel Properties

The typical use of an Intrusion Group is for security monitoring of an area.

An Intrusion Group is a collection of Zones, which are grouped together into a unit for intrusion monitoring purposes. The events from these Zones will be used to determine the group state.

An Intrusion Group can be armed or disarmed, which affects the way events are handled for the groups.

- **If a group is armed**, then changes of state to its inputs can cause it to go into alarm, indicating that a breach has occurred in the area monitored by the group.
- **If a group is disarmed**, such events may generate audio or visual signals like chimes, without generating a security breach event.

The Intrusion Groups are created in two steps:

1. Create the Intrusion Group and set Zone Assignments on the Panel
2. Create the Intrusion Group Logical Device

8.24.17.1 Creating an Intrusion Group on Panel

1. Edit Panel Properties and click on "Intrusion Groups" tab.

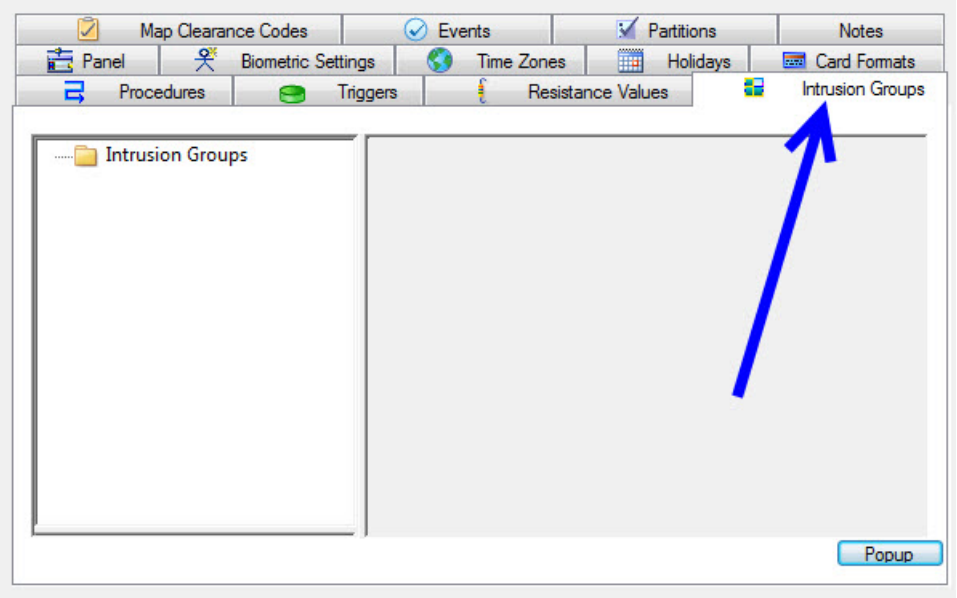


Figure 8-25 Intrusion Groups Tab

2. Add the Intrusion Group.

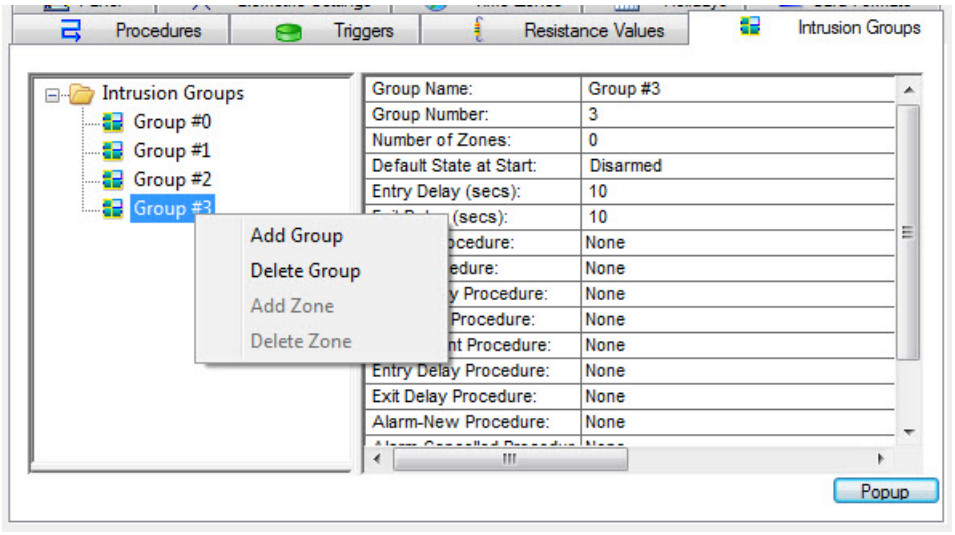


Figure 8-26 Create Intrusion Group

3. Add Intrusion Zone to the Group by right-clicking on the Group:

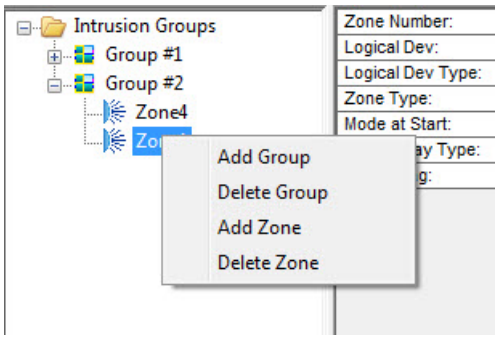


Figure 8-27 Add Intrusion Zone

4. Assign logical device to Intrusion Zone.

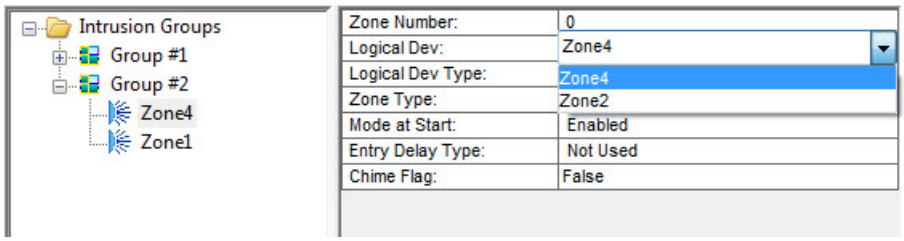


Figure 8-28 Assign Logical Device

8.24.17.2 Intrusion Zone Fields and Notes

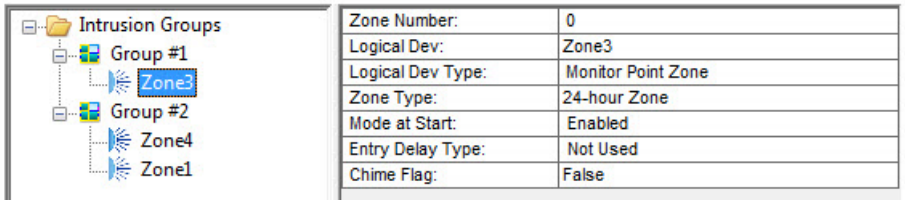


Figure 8-29 Intrusion Zone Fields

Zone Number - The unique zone number - this value is automatically assigned by Pro-Watch.

Logical Dev - The logical device assigned for this zone. This can be the Door Position Switch (DPS) or an ACR or monitorable input point logical device. For ACRs, the door position switch acts as the zone, so that open door/forced door/held door alarms are treated as zone alarms for the group. Valid logical devices are listed in the drop-down box.

Logical Dev Type - This value is automatically set by Pro-Watch based on the type of the logical device assigned to the zone.

Zone Type - This drop-down menu sets the zone type and consists of three (3) choices: 24-hour Zone, Interior Zone, and Perimeter Zone.

1. 24-Hour Zone: Always monitored even if the group is not armed.
2. Interior Zone: Monitored for Arm-Away ONLY.
3. Perimeter Zone: Monitored for Arm-Stay, Am-Away, and Arm-Instant.

Mode at Start - This drop-down menu sets the default zone mode at start (default state/initial state) and consists of three (3) choices: Enabled, Bypassed, Disabled.

1. **Enabled:** The zone is active and follows normal monitoring rules for arm and disarm.
2. **Bypassed:** The zone is not active and will not set off the alarm when the group is first armed no matter how often the zone is tripped. The zone will become active after the first DISARM command. When the zone is bypassed, zone events will still be reported, but trippingthe zone will not put the group into alarm.
3. **Disabled:** The zone is not active and will be inactive until activated by the user. When the zone is disabled, zone events will still be reported, but tripping the zone will not put the group into alarm.

The initial state for a zone can be triggered by a system download (or Panel Initialize -> System Download)

Entry Delay Type - This drop-down menu sets the allowed zone behavior when the group is armed and consists of three (3) choices: Entry Delay Trigger, Entry Delay Follow, and Not Used.

1. **Entry Delay Trigger:** Indicates that the activation of the zone should trigger an entry delay. Entry delay times are set at the Intrusion Group level under Panel Properties. Entry delays will be observed only for the Armed-Away and Armed-Stay settings. If the group is already in an entry delay state (i.e. some other zone has triggered the entry delay), tripping this zone will not generate an alarm. (Flag: Entry = Yes, Follow = Don't Care)
2. **Entry Delay Follow:** Indicates that this zone may be active during an Entry Delay. The zone will not trigger an entry delay so if the system is armed and the zone is tripped, the group will be put into alarm. However, if the system is already in an entry delay state, this zone may be tripped without putting the group into alarm. (Flag: Entry = No, Follow = Yes)
3. **Not Used:** Indicates that the zone will not trigger an entry delay and cannot be active during an entry delay state. Activating the zone during an entry delay will put the group into alarm. (Flag: Entry = No, Follow = No)

Chime Flag - Indicates if the zone will cause the keypad to chime when the zone is open. Note that the Chime setting must be "ON" at the keypad in order for the chime to operate correctly (Keypad Command "5").

8.24.17.3 Intrusion Group Fields and Notes

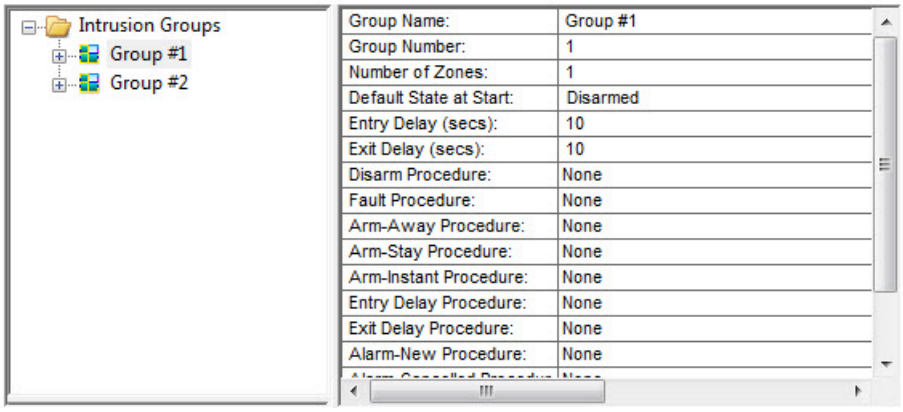


Figure 8-30 Intrusion Group Fields

Group Name - The user-defined name of the Intrusion Group. When creating Intrusion Group logical devices, the assigned hardware group will be referred to by the Group Name.

Group Number - The assigned number of the group on the Mercury panel. This is assigned by the user interface as groups are defined. This is also the group number used when the MRDT Display Terminal is used on a targeted group.

Number of Zones - The number of intrusion zones for the group, maintained by Pro-Watch.

Keypad/Reader - The ACR/Keypad assigned to the group. This is typically, but not necessarily, an MRDT Terminal ACR. The drop-down contains a list of the ACRs for the panel which are not already assigned to some other group.

Default Start At Start - The state the group is set to when the panel starts up. This is downloaded to the panel as part of group configuration (panel download/system download). There are nine (9) possible default states, although it's not recommended that all of them be used as a default state:

1. **Alarm - New:** The group will default to the alarm state.
2. **Armed - Away:** The group will default to an armed-away state.
3. **Armed - Instant:** The group will default to an armed-instant state.
4. **Armed - Stay:** The group will default to an armed-stay state.
5. **Canceled Alarm:** The group will default to a canceled alarm state.
6. **Disarmed:** The group will default to a disarmed state.
7. **Entry Delay in Progress:** The group will default to an entry delay.
8. **Exit Delay in Progress:** The group will default to an exit delay.
9. **Fault:** The group will default to a fault (open circuit/short circuit condition).

Entry Delay - The number of seconds between an entry delay intrusion zone alarm is detected and the group goes into alarm. This allows the user to make it to the keypad to disarm the group on entry.

Exit Delay - The number of seconds between when a group is armed and when it starts reporting zone alarms. This allows the user time to exit the area after arming the group.

Fault Procedure - The panel procedure to run when a fault is detected for the group. This must be an existing panel procedure.

Caution: Fault Procedure does not run when **Zone Type** is set to "**24 hour zone.**" Fault procedure runs successfully when **Zone Type** is set to "**Perimeter**" or "**Interior**."

Arm-Away Procedure - The panel procedure to run when the group is armed for away. This procedure will be run when the group enters the Armed-Away state (after entry delay). This must be an existing panel procedure.

Arm-Stay Procedure - The panel procedure to run when the group is armed for stay. This procedure will be run when the group enters the Armed-Stay state (after entry delay). This must be an existing panel procedure.

Arm-Instant Procedure - The panel procedure to run when the group is instant armed. This must be an existing panel procedure.

Entry Delay Procedure - The panel procedure to run when the group goes into entry delay. This must be an existing panel procedure.

Exit Delay Procedure - The panel procedure to run when the group goes into exit delay. This must be an existing panel procedure.

Alarm-New Procedure - The panel procedure to run when a new alarm is detected for the group. This must be an existing panel procedure.

Alarm-Canceled Procedure - The panel procedure to run when the user cancels the alarm for a group. This must be an existing panel procedure.

Disarming Procedure - The panel procedure that is run when the group is disarmed. This must be an existing panel procedure.

8.24.17.4 Disarming Procedure

Skip Canceled Flag - The skip canceled flag is a True/False flag. When True, the system will skip the "Alarm Cancelled" state when the group is in alarm and will straight to the "Disarmed" state.

8.24.18 Introduction to Intrusion Groups

After creating the Intrusion Group in the panel, the next step is to create the Intrusion Group logical device.

To support the Intrusion hardware, there are new templates and classes that were added for the Zones, Groups, and Terminals.

For the Intrusion Groups:

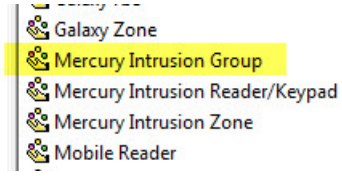


Figure 8-31 Group Hardware Template

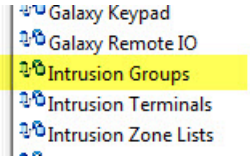


Figure 8-32 Group Hardware Class

8.24.19 Creating Intrusion Group (With Wizard)

Intrusion Groups are just a collection of **Intrusion Zones**. While the Zones are the devices that monitor intrusion, the Intrusion Group serves to manage and monitor the Zones.

Creating the Intrusion Groups under the panel properties ties the Zones to the Group. Creating the Intrusion Group Logical Device and tying it to the Intrusion Group is what actually allows the Intrusion System to monitor the zones.

To create an Intrusion Group Logical Device, start the process for creating a new logical device. Set the Hardware Template to "**Mercury Intrusion Group**" and the Hardware Class for "**Intrusion Groups**." Select the panel intrusion group that will be used for the Intrusion Group.

Note: The Intrusion Groups that appear under this list will be the panel Intrusion Groups not already assigned to a Intrusion Group Logical Device. The Panel Intrusion Groups will be listed by the Group Name.

Follow these steps:

1. Right-click and from the pop-up menu select "**Logical Device"** to display the P**ro-Watch Logical Device Manager** screen.
2. Enter a **Description**. For **Hardware Template,** select "**Mercury Intrusion Group.**" For **Control Panel**, select the name of your control panel. For **Hardware Class,** select "**Intrusion Groups**."

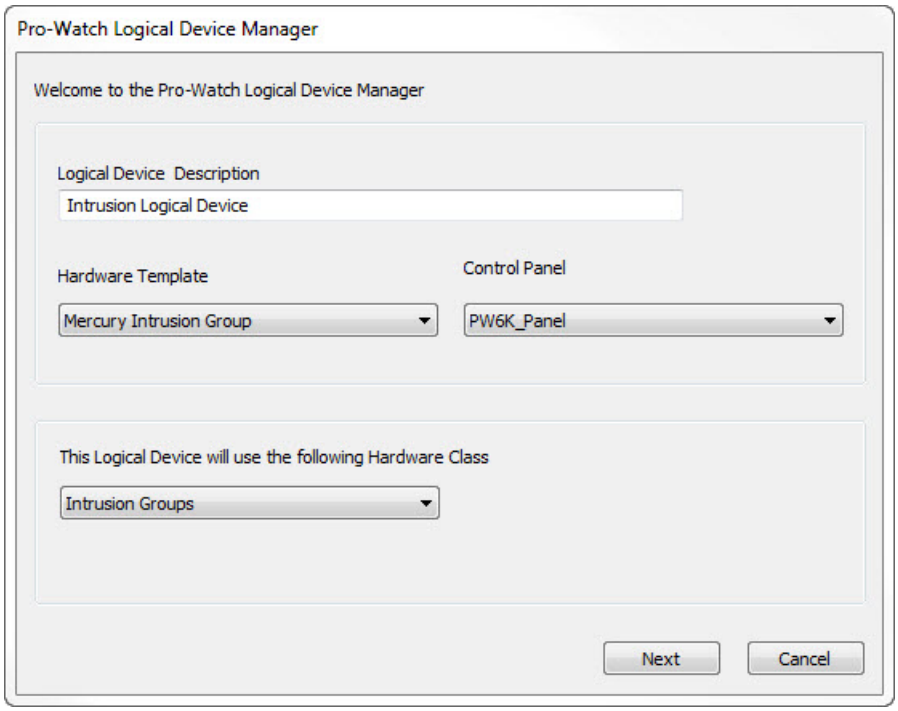


Figure 8-33 Intrusion Group Logical Device Creation

3. Click **Next** to display the **Hardware Assignment** screen.

4. Double-click the intrusion group to display the **Select Intrusion Group** dialog box:

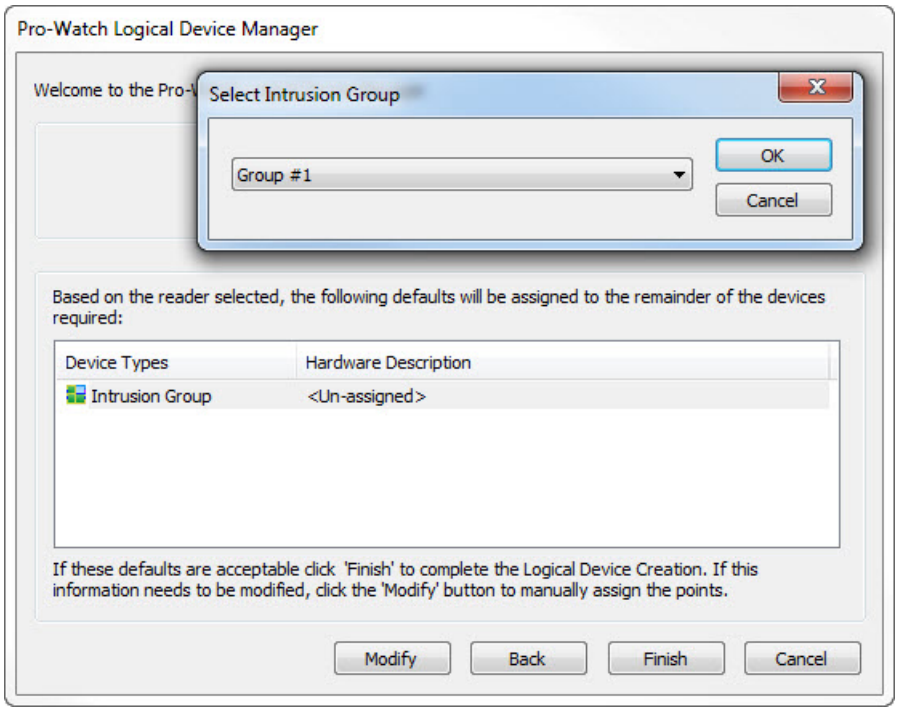


Figure 8-34 Intrusion Group Selection

5. Select an intrusion group from the drop down menu and click **OK**. That group will be assigned to the new intrusion logical device you are creating.
6. Click **Finish**. The new intrusion logical device will be listed in the **Intrusion Groups** sub-directory:

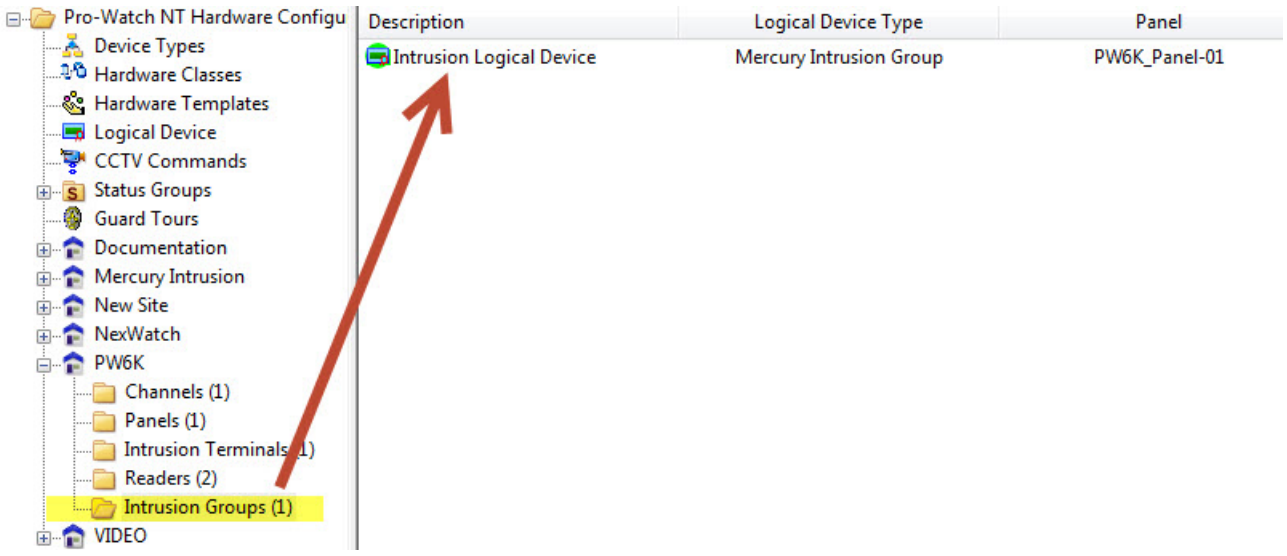


Figure 8-35 Intrusion Group Logical Device Listed

After the Intrusion Group Logical Device is created, the Intrusion system is basically set up and will function (minus the MRDT). The Group Logical Device can be added to Status Groups for status monitoring as can each individual Zone Logical Device.

Additionally, the Intrusion Group Logical Device will allow the following actions to be performed:

1. **Arm Away:** Host Arm the group to Arm Away.
2. **Arm Stay:** Host Arm the group to Arm Stay.
3. **Arm Instant:** Host Arm the group to Arm Instant.
4. **Disarm:** Disarm the Group.
5. **Activate All Zones:** Activate all Intrusion Zones within Group.
6. **Bypass All Zones:** Bypass all Intrusion Zones within Group.
7. **Disable All Zones:** Disable all Intrusion Zones within Group.
8. **Call Intercom**
9. **Show CCTV Camera View**
10. **CCTV Controls**

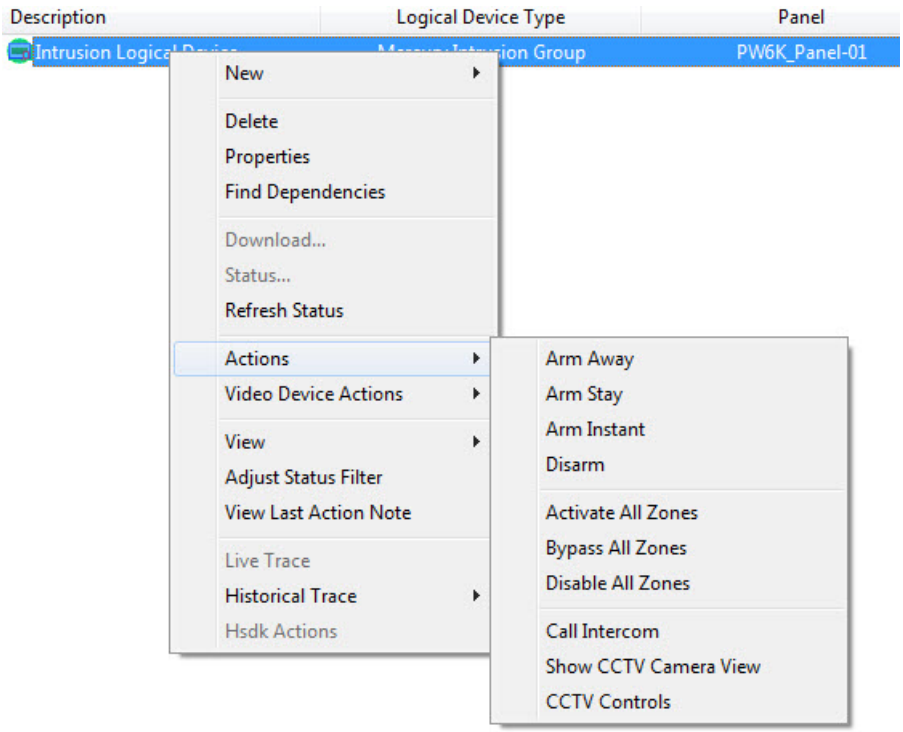


Figure 8-36 Intrusion Group Actions

8.24.20 Intrusion Group Events

If any of the Intrusion Zones within the Intrusion Group is tripped, then the whole Intrusion Group will go into alarm. Event Viewer and Alarm Monitor will display the Zone Active alarms as well as the Group New Alarm.

ware	Point Description	Logical Device Description	Event Type Description	Mes
	Output point is active-RTN	COOP 1	Output Active	
	Output point is active	COOP 1	Output Active	
	Intrusion Group New Alarm	Group 1/Building 1	Group New Alarm	
	Intrusion Zone Active	Intrusion Zone - 03 - Zone 01	Zone Active	
	Intrusion Zone Active - RTN	Intrusion Zone - 03 - Zone 04	Zone Active	
	Intrusion Zone Active	Intrusion Zone - 03 - Zone 04	Zone Active	
	Intrusion Zone Active - RTN	Intrusion Zone - 03 - Zone 03	Zone Active	
	Intrusion Zone Active	Intrusion Zone - 03 - Zone 03	Zone Active	

Figure 8-37 Intrusion Zone and Group Events

Notes:

1. Actions performed on the Intrusion Group from Pro-Watch will be listed as a "host" action. Actions performed on the MRDT Display Terminal will be listed as a "local" action.
2. There are up to two (2) different steps when transitioning a group alarm from Alarm to Disarmed. This is governed by the "**Skip Cancelled Flag**" setting under the Intrusion Group options in the Panel Properties.
   a. If the "Skip Cancelled Flag" is "True", then a group alarm will go straight from "In Alarm" to "Disarmed".
   b. If the "Skip Cancelled Flag" is “False,” then a group alarm will go from "In Alarm" to "Cancelled Alarm" to "Disarmed.
      i. **Canceled Alarm:** Alarm is "acknowledged" and canceled. In this state, the group cannot be armed and all subsequent alarms will not cause the group to issue a new alarm. When attempting to arm the group, Pro-Watch Event Viewer and the MRDT Display Terminal will display the current status of the group.

ii. **Group Disarm:** Group is disarmed.

8.24.21 Creating MRDT Intrusion Terminal (With Wizard)

To create an MRDT Intrusion Terminal Logical Device, start the process for creating a new logical device.

1. Set the Hardware Template to "**Mercury Intrusion Reader/Keypad**" and the Hardware Class to "**Intrusion Terminals.**"
2. Select the **Control Panel** that will be used for the Intrusion Terminal.

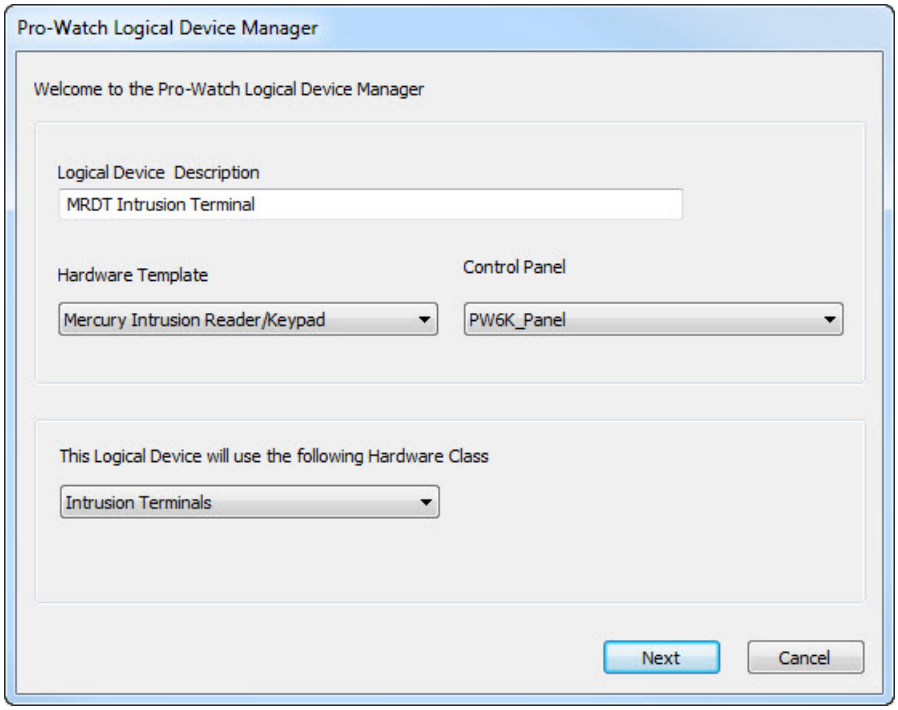


Figure 8-38 MRDT Intrusion Terminal Creation

3. Click **Next** to display the **Reader Assignment** screen:

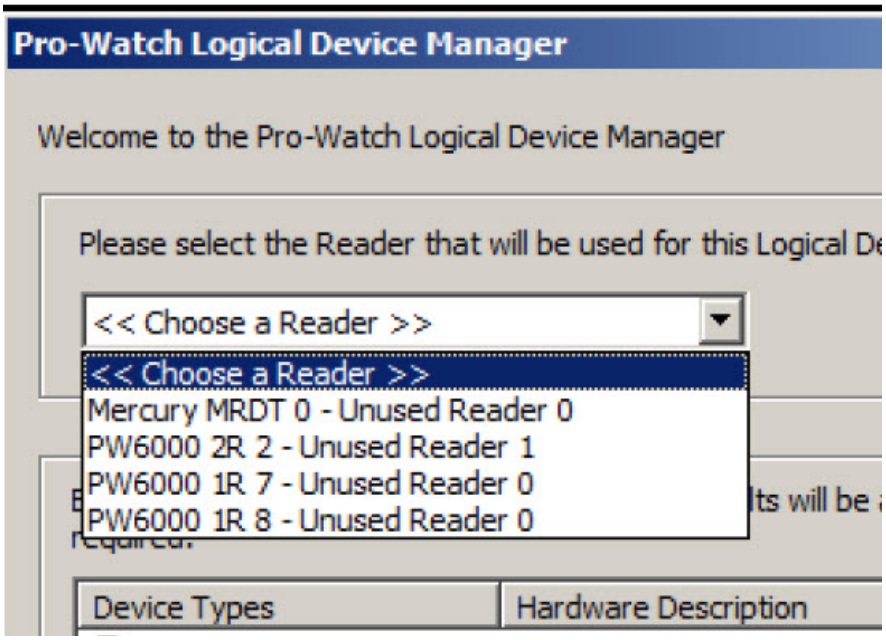


Figure 8-39 Intrusion Terminal Selection

8.24.21.1 Hardware Template for Connecting MRDT with an ACR

If you'd like to use the MRDT connected to the reader port of a reader board, use the "**ACR with MRDT Intrusion Terminal**" template, as shown below:

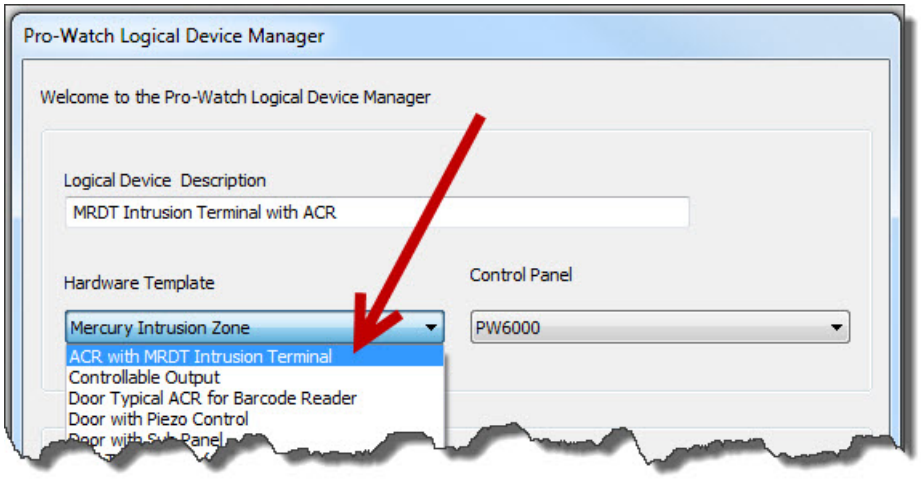


Figure 8-40 Hardware Template for MRDT Connected to a Reader Port

8.24.21.2 Configuring Intrusion Terminal Settings

Note: The LED Mode of the MRDT Terminal Keypad/Reader logical device must be set to "MRDT".

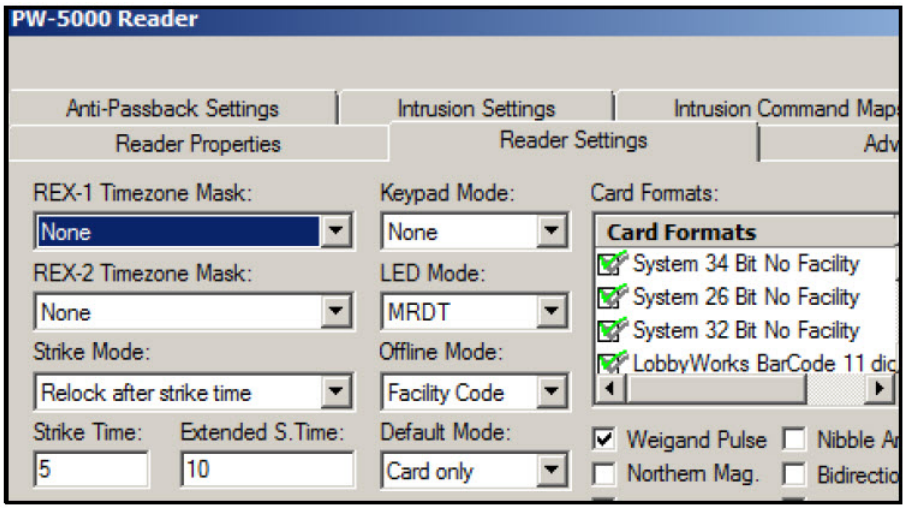


Figure 8-41 Intrusion Terminal Reader Settings

The "Intrusion Settings" tab controls of behavior of the MRDT Display Terminal as well as assigns the Display Settings and the Intrusion Group.

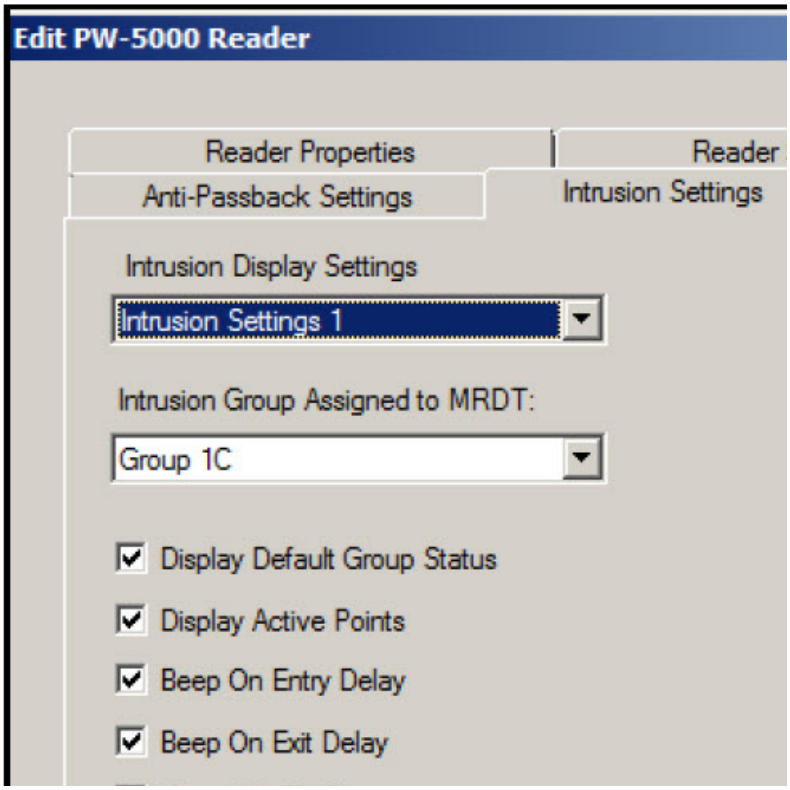


Figure 8-42 Intrusion Terminal Intrusion Settings

8.24.21.3 Intrusion Terminal Fields

Intrusion Display Settings drop-down menu lists all of the Mercury Intrusion Display Settings created under Database Configuration. This governs what is displayed on the MRDT Display Terminal's screen.

Intrusion Group Assigned to MRDT drop-down menu assigns the MRDT to the Intrusion Group.

Note:

1. A MRDT Display Terminal may only be linked to one (1) Intrusion Group. However, multiple MRDT's can be linked to the same group. This would allow one MRDT to be used as a master disarm device at one location while another could be used for arming only at some other door.
2. The Intrusion Group listed on the drop-down is the name of the Intrusion Group under Panel Properties, not the Intrusion Group Logical Device.

Display Default Group Status check-box: If selected, the MRDT's LCD screen will add the group status ("Armed", "Disarmed", etc) to its display cycle. The display cycle displays the time, the lines configured in the

Mercury Intrusion Settings, the Group Status (if configured), and the Active Points (if configured).

Display Active Points check-box: This option is tied to the "Display Default Group Status" option. If the above option is not selected, then this option will also not be selected (disabled). If the above option is selected, then the user will have the ability to either select or not to select this option. When selected, the MRDT's LCD screen adds the current active points (zones) to its display cycle. Each Intrusion Zone can be configured to have a custom name; this is edited through the Intrusion Zone logical device.

Beep on Entry Delay check-box: (If selected) when the group goes into Entry Delay, the MRDT will beep continuously until the Entry Delay is finished or the group is disarmed.

Beep on Exit Delay check-box: (If selected) when the group is armed and goes into Exit Delay, the MRDT will beep continuously until the Exit Delay is finished.

Note: **Chime Enabled check-box:** When selected it enables the chime on the MRDT. this option is independent of the Chime command on the MRDT. If the Chime is disabled via Pro-Watch, then the Chime command on the MRDT will have no effect on anything.

Chime On check-box: This is tied to the "Chime Enabled" option. This option is connected with the Chime command on the MRDT, but the value listed here is the default behavior. If the "Chime On" is not selected, the user has the ability to enable it at the MRDT.

8.24.22 Creating MRDT Display Settings

The MRDT Display Terminal is governed by a set of Mercury Intrusion Display Settings. Only one set of settings can be linked to one MRDT Display Terminal.

The MRDT Display Terminal has the numeral buttons 0-9, an arrow button, the "COMMAND" button, and four (4) macro buttons on top that translates to the F1 - F4 keys.

To create a new Display Setting, go to **Database Configuration > Mercury Intrusion Settings**.

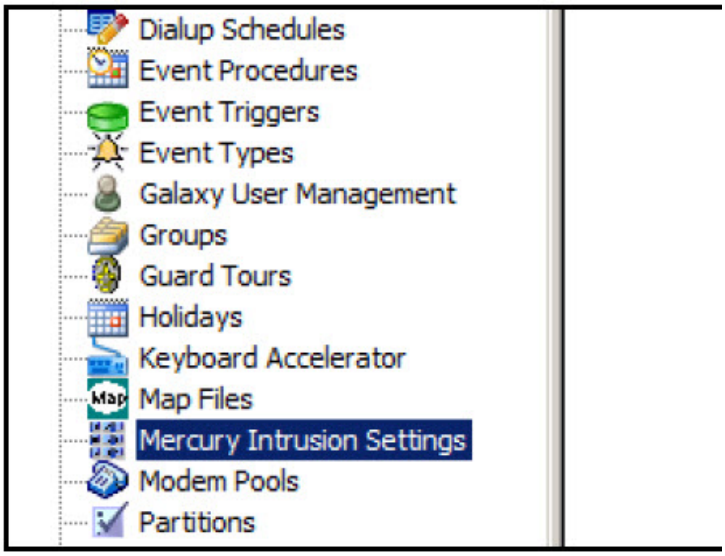


Figure 8-43 Database Configuration > Mercury Intrusion Settings

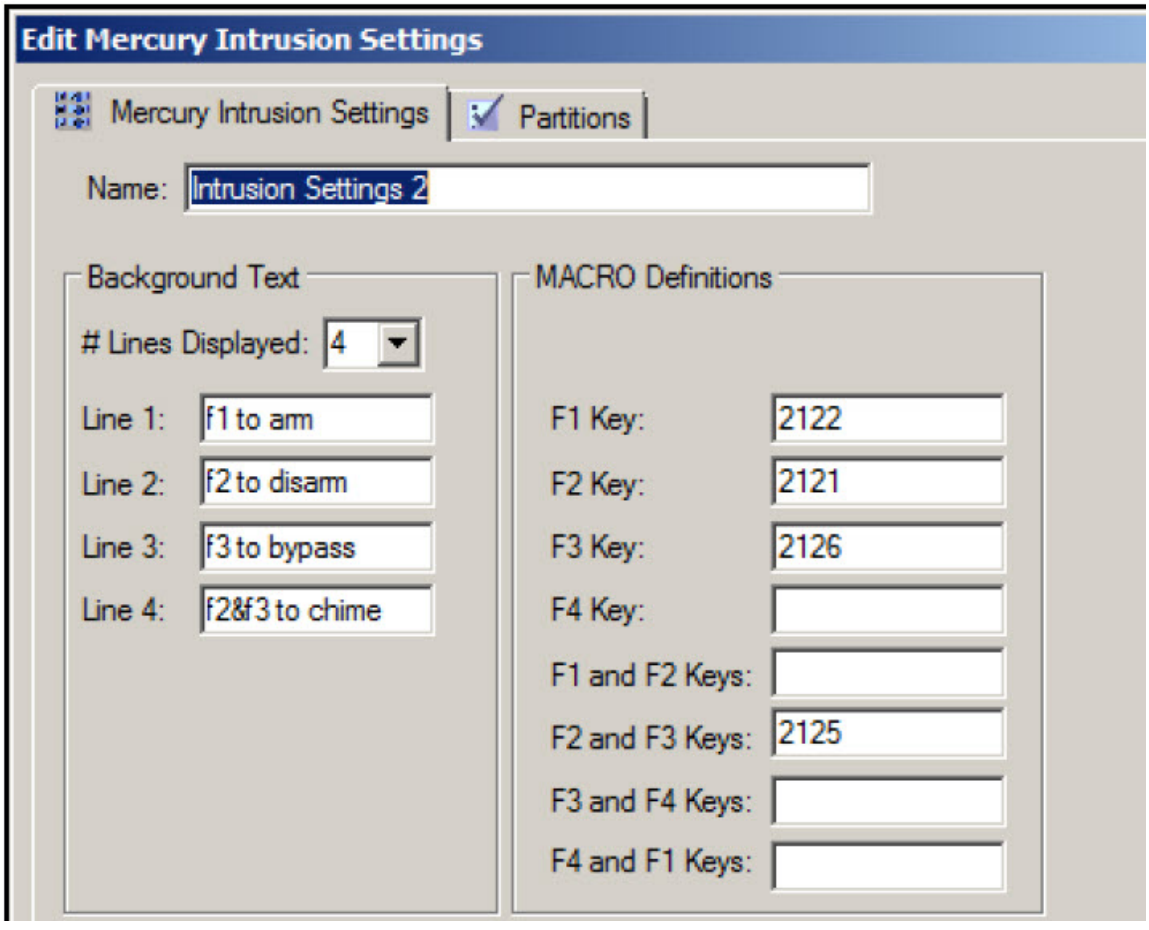


Figure 8-44 Mercury Intrusion Settings

The MRDT Display Terminal can cycle through 8 lines of custom text. In addition, macros can get set up for the macro keys.

For example, if the assigned group code is 545 and target group code is 454:

1. Macro to disarm assigned group: F1 key set to ***5451***. When the user presses the F1 key, the group will automatically be disarmed.
2. Macro to arm target group with group code 01: F2 key set to ***454012***. When the user presses the F2 key, the group with assigned code “01” will be armed.

Note: The asterisk symbol (*****) represents the “COMMAND” button on the MRDT.

Another example: press F2 and F3 keys simultaneously to enter the arm instant code into the terminal.

8.24.23 Configuring Intrusion Terminal Command Maps

Command Maps may be used to control user access to the MRDT. Each MRDT is capable of supporting 2 Command Maps (In addition to the "All" map). Each command map is linked to a Pro-Watch clearance code. The use case here is if the user wants to give one set of employees the ability to arm the group and a different set of employees the ability to disarm the group.

To configure command maps, the user must:

1. Add the clearance code to the list of command map clearance codes
2. Map the clearance code and assign permissions.

To add available clearance codes to the list of command map clearance codes, open up the Panel Properties and move the desired clearance code to the panel.

Note: The list of available clearance codes contain clearance codes that have the MRDT Keypad/Reader Logical Device within the clearance code. If the clearance code does not have a MRDT Keypad/Reader Logical Device, then it will not appear in this list.

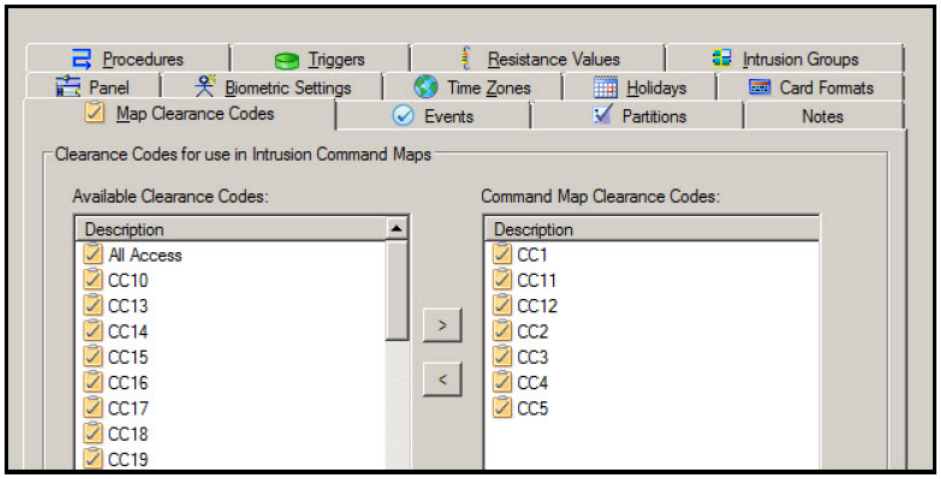


Figure 8-45 Map Clearance Codes (Panel)

After the clearance code is added to the panel, then it can be assigned to a command map. This is done in the MRDT Keypad/Reader Logical Device settings under the "Intrusion Command Maps" tab.

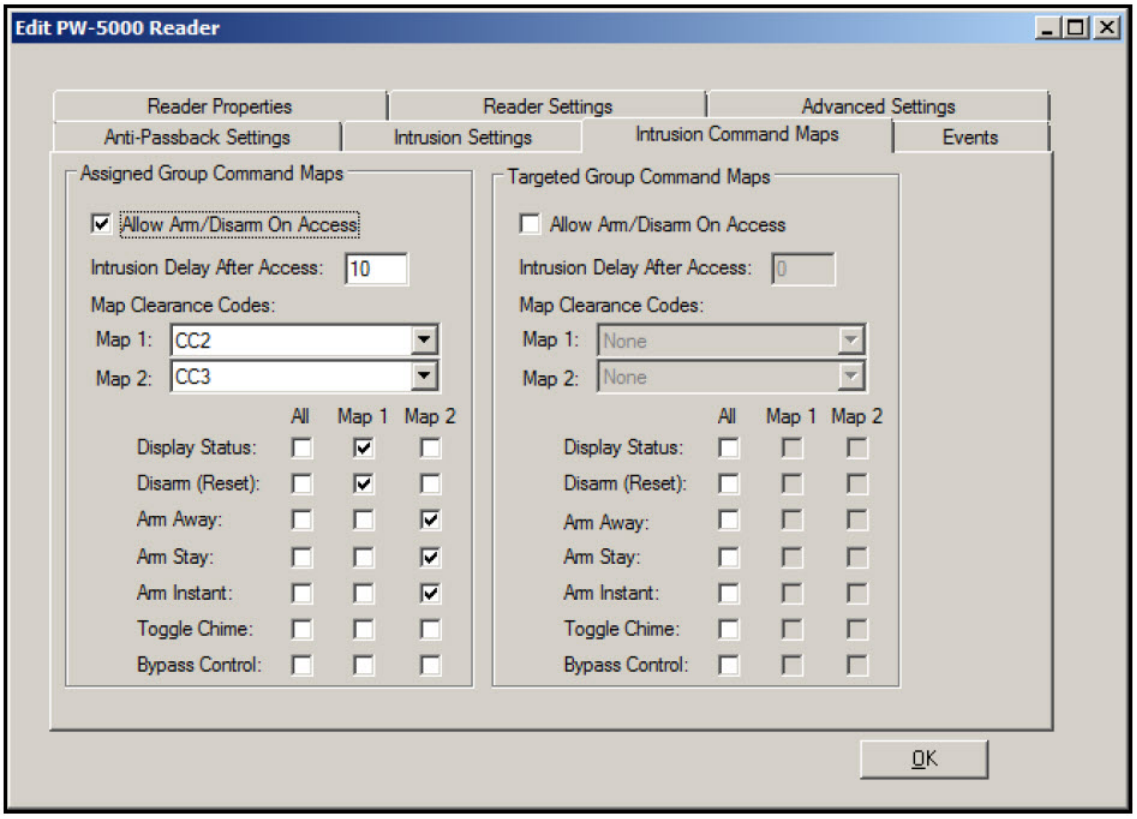


Figure 8-46 Intrusion Command Maps

8.24.23.1 Intrusion Command Maps Fields

Allow Arm/Disarm on Access check-box: When selected, enables arm/disarm on access. If this check-box is unchecked, then the selections for the mapped clearance codes and the map permissions will be grayed out. In this case, only the permissions checked under the "All" selection will be available for the user.

Note: The "All" map will always supersede any permissions given to Map 1 and Map 2.

Intrusion Delay After Access: In seconds and cannot be a non-zero number. This value determines how long the user has after scanning a card to enter a valid command.

Map 1: Clearance Code that will be mapped to Map 1. This is from the list of panel mapped clearance codes.

Map 2: Clearance Code that will be mapped to Map 2. This is from the list of panel mapped clearance codes.

8.24.24 Wiring the MRDT Display Terminals

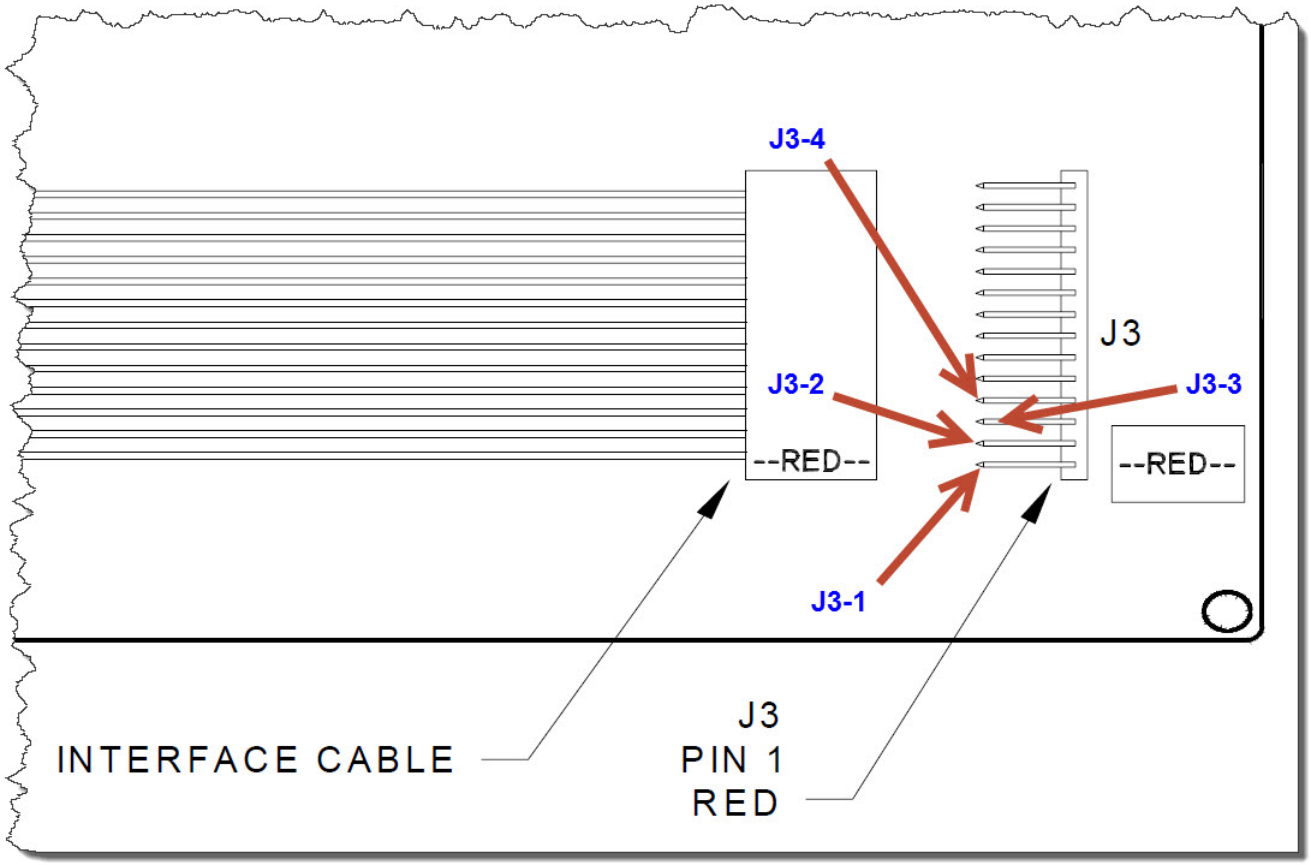


Figure 8-47 MRDT J3 Terminal Block Pins 1 through 4

The MRDT can be wired two (2) ways:

8.24.25 As a subpanel using the RS-485 port of a PW-6000 (or equivalent) IC

8.24.25.1 Wiring:

J3-1 RED to 12VDC Input

J3-2 BLACK to Ground

J3-3 BLUE to RS-485 TR+

J**3-4 GRAY** to RS-485 TR-

8.24.25.2 MRDT Display Terminal Settings:

Comm: RS485

Protocol: MSP1

Baud Rate:38.4 (Match Pro-Watch port baud rate)

Comm Address:<RS-485 Address>

Backlight:<User select>

LED:1Wire

Note: Multiple MRDT Display Terminals may be daisy chained off this configuration.

8.24.26 As a reader using the reader port of a PW-6000 2-Reader board (or equivalent)

8.24.26.1 Wiring:

J3-1 RED to 12VDC Input

J3-2 BLACK to Ground

J3-3 BLUE to D1/TR+

J3-4 GRAYto D0/TR-

8.24.26.2 MRDT Display Terminal Settings:

Comm: RS485

Protocol: MSP1

Baud Rate: 9600

Comm Address: 00 (Doesn't really matter)

Backlight: <User select>

LED: 1Wire

8.24.27 Connecting an external reader to the MRDT

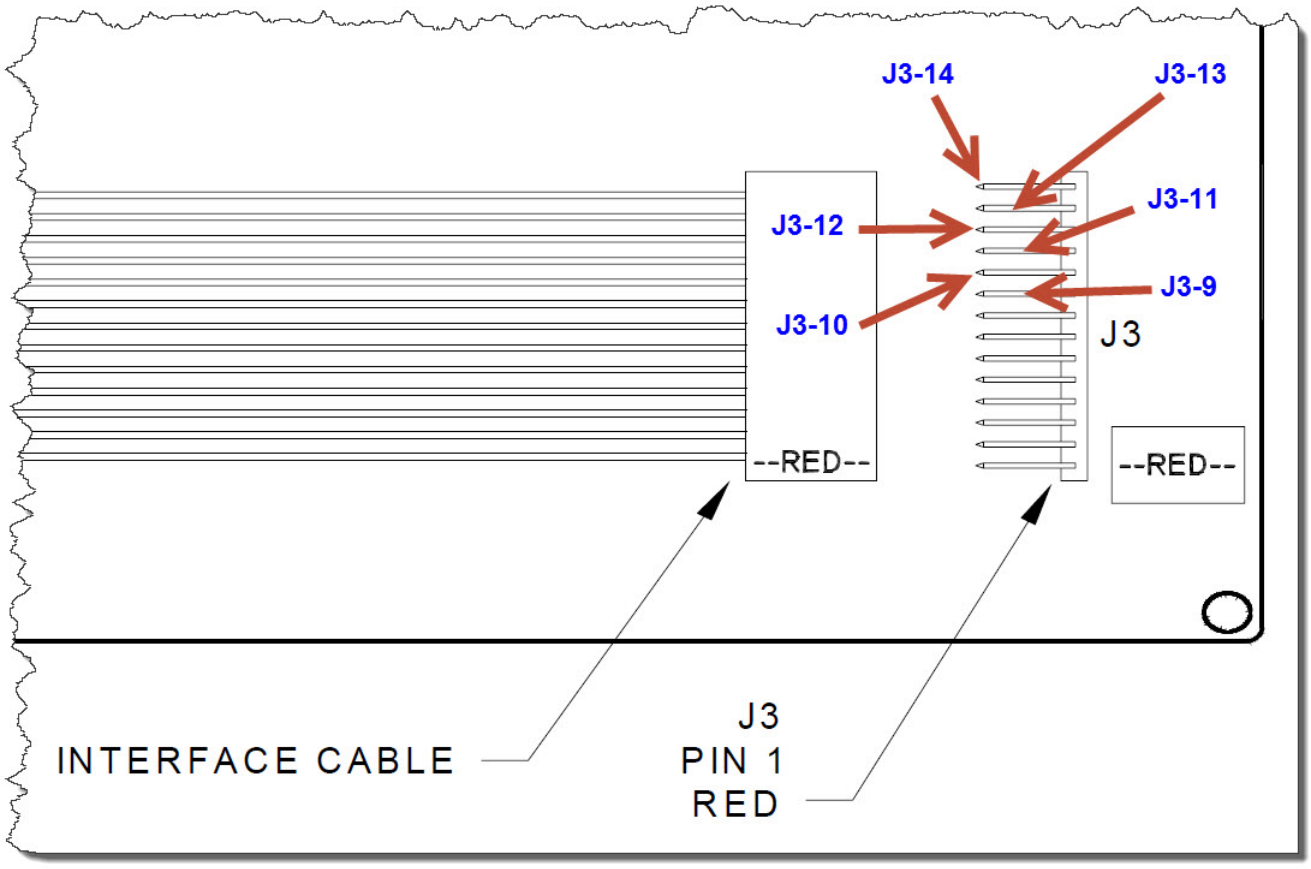


Figure 8-48 MRDT J3 Terminal Block Pins 9 through 14

8.24.27.1 Wiring:

J3-9 RED to 12VDC Input
J3-10 GREEN to Reader DATA/DATA 0
J3-11 WHITE to Reader CLOCK/DATA 1
J3-12 BROWN to Reader LED
J3-13 ORANGE to Reader Buzzer
J3-14 BLACK to Ground

8.25 Adding a Logical Device

A Logical Device is a single physical device or a group of selected physical devices, which are defined by a hardware template. For example, a template may define a door that is equipped with a card reader, a REX input device, and a door strike output device as one Logical Device.

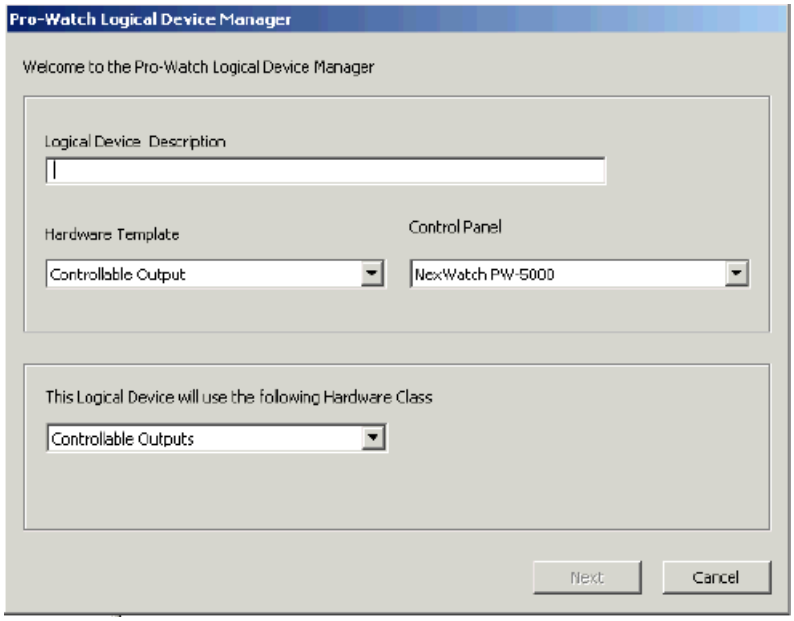
As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system. For example, you can assign the door, reader, input device, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you add Logical Devices, you must create the following:

- Site. See "Add a Site".
- Channel. See "Adding a PW-5000/PW-6000/PW-6K1ICE Channel".
- Panel. See "Adding a PW-6000/5000/3000 Panel".
- Hardware Template. See Adding or Editing a Hardware Template, page 28.

To add a Logical Device:

1. From the Pro-Watch Hardware Configuration tree view, right-click the site to which you want to assign the Logical Device and select **New > Logical Device**. The Pro-Watch Logical Device Manager dialog box appears.



2. Enter a description that will identify the Logical Device in the Logical Device Description field.

3. Select a hardware template from the Hardware Template drop-down list. See Adding or Editing a Hardware Template, page 28.
4. Select a Hardware Class from the drop-down list in the Hardware Class field.
5. Select the Device Types that the Logical Device will include.
6. Click **Finish** to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the number of sub-panels (I/O Modules) that are added to the panel.

8.26 Configuring a Logical Device

You can edit and configure Logical Devices after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices are already configured. For more information, see Adding or Editing a Hardware Template, page 28.

Note: You should visit the Logical Device configuration tabs, since these tabs contain fields that hardware templates do not.

To configure a Logical Device:

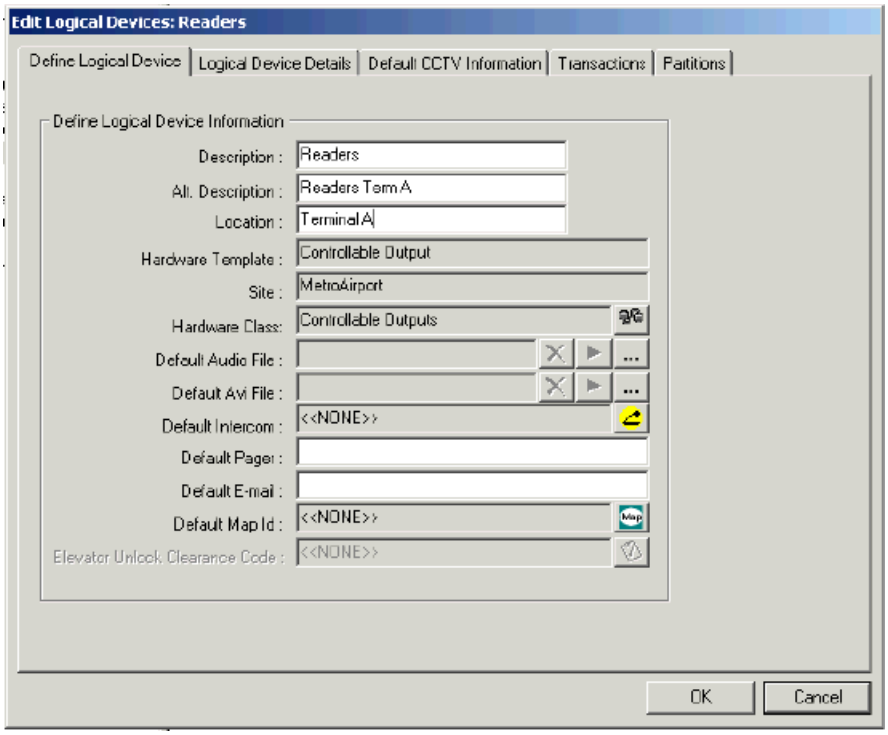
1. Click the appropriate Logical Device folder in the Hardware Configuration screen to display the site's existing Logical Devices.
2. Right-click the Logical Device you want to configure, and select **Properties**. The Edit Logical Devices: [Logical Device name] screen appears.
3. Complete the following information tabs to configure the Logical Device:

CONFIGURE A PW-6000/5000/3000 LOGICAL DEVICE TABS LIST

- "Define Logical Device Tab".
- "Logical Device Details Tab".
  - Reader Devices
    - "Reader Properties Tab".
    - "Reader Settings Tab".
    - "Advanced Settings Tab".
    - "Anti-passback Settings Tab".
    - "Events Tab".
  - Input Point Devices
    - "Input Point Tab".
    - "Events Tab".

– Output Point Devices
  * "Output Tab".
  * "Events Tab".

8.26.1 Define Logical Device Tab

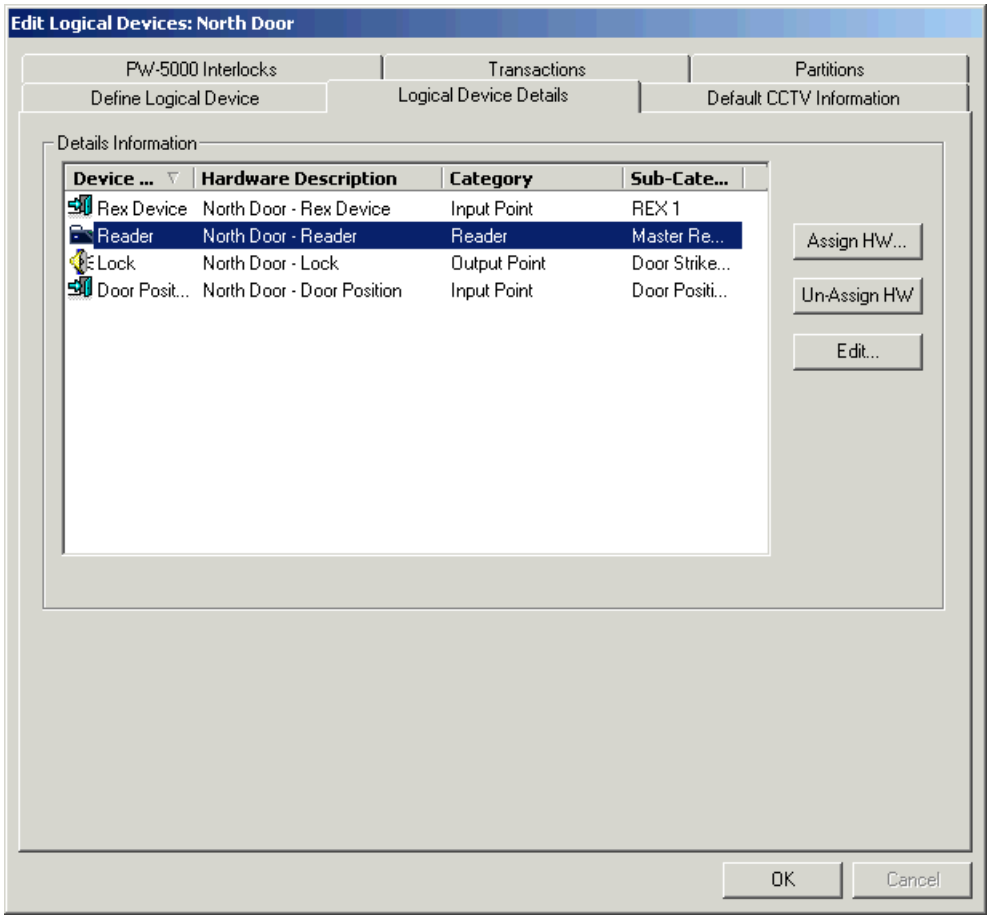


Use the following field descriptions to complete the Define Logical Device tab.

Field	Description
Description	Identifies the name of the Logical Device as defined by the user and the Logical Device type.
Alt. Description	Allows an alternative description to further identify the device.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Identifies the hardware template used to create the Logical Device.
Site	Identifies the site associated with the Logical Device.
Hardware Class	Identifies the hardware class to which the Logical Device is assigned.
Default Audio File	Identifies a default audio file that the Logical Device will play.
Default Avi File	Identifies a default video file that the Logical Device will play.
Default Intercom	Identifies a default intercom that will belong to the Logical Device.
Default Pager	Identifies a default pager device that will belong to the Logical Device.
Default Email	Identifies a default email address for the Logical Device.
Default Map ID	Identifies a default map which includes the Logical Device.

8.26.2 Logical Device Details Tab

This tab displays all of the device types included in the Logical Device. At this tab you can assign, un-assign, or edit the device types.



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click **OK**.

To unassign a device type:

- Click to select the device type and click **Un-Assign HW**.

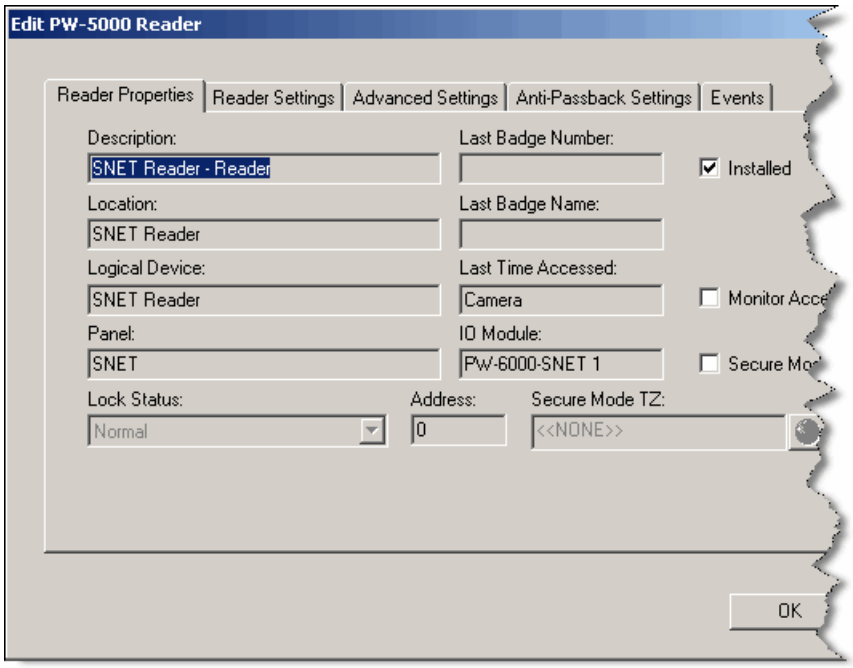
To edit the current configuration of a device type:

- Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete. Use the appropriate table below to edit or configure the device type you have selected.

Reader Device

Use the tables in the following sections to complete the Reader information tabs.

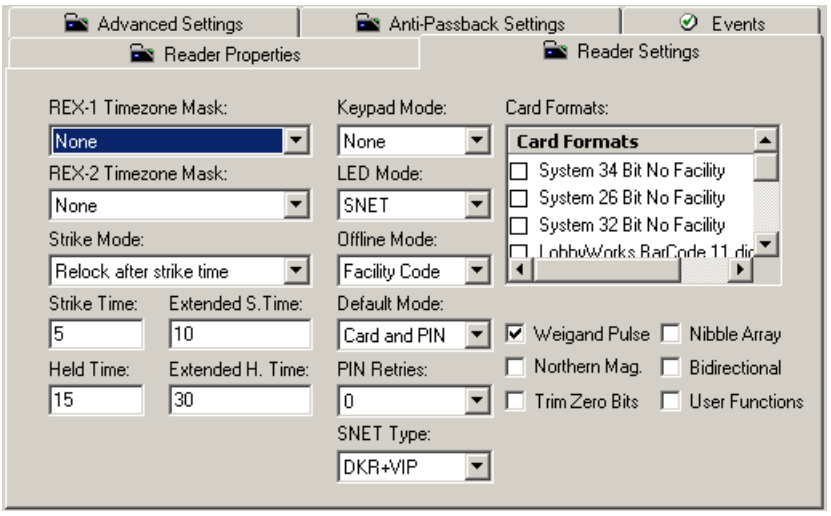
Reader Properties Tab



Field	Description
Description	Identifies the name of the Logical Device as defined by the user and the Logical Device type.
Last Badge Number	Identifies the last badge number that was presented at the Logical Device.
Location	Identifies the physical location of the Logical Device as defined by the user.
Last Badge Name	Identifies the badge holder name of the last badge that was presented to the Logical Device.
Logical Device	Identifies the name of the Logical Device.
Last Time Accessed	Identifies the last time the Logical Device was accessed.
Panel	Identifies the panel in which the Logical Device is assigned.
I/O Module	Identifies the I/O Module in which the Logical Device resides.

Field	Description
Address	Identifies the address of the Logical Device.
Lock Status	Identifies the lock status of a door (locked, open, normal).
Monitored Access	Enables Monitored Access (card trace) on a reader.
Secure Mode	Enables secure mode for a particular door. See Verification Window in Appendix A, Secure Mode Verification.
Secure Mode Time Zone	Identifies the time zone during which the reader is in secure mode.
Installed	Required for the Logical Device to be enabled and operational.

Reader Settings Tab



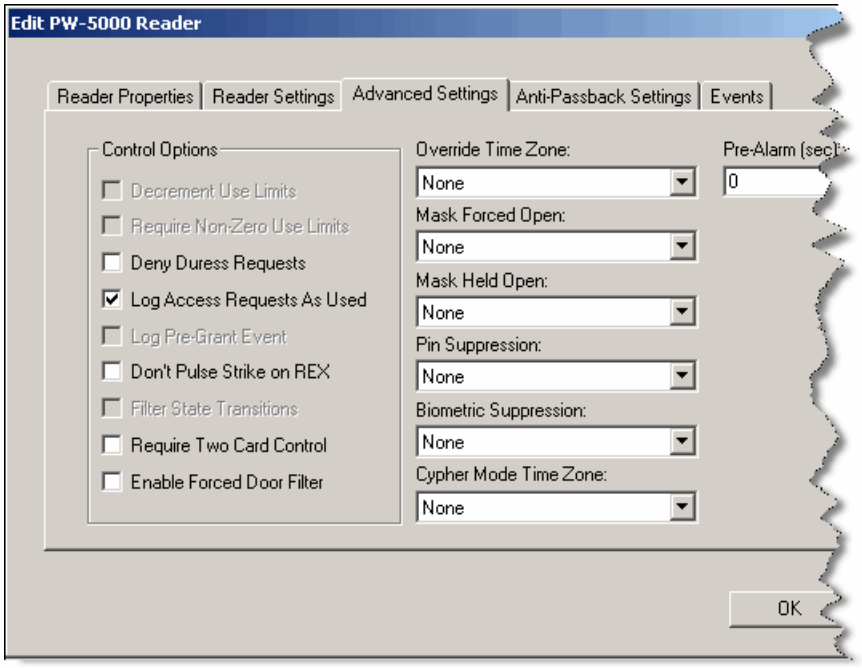
Field	Description
REX-1 Time Zone Mask	Defines the time zone in which the REX remains masked, or shunted.
Keypad Mode	Defines the manufacturer of the keypad and therefore the keypad mode. For all magstripe readers with PIN on a PW-6000, set the Keypad Mode to Indala. For magstripe readers without a keypad, set the Keypad Mode to None.

Field	Description
Card Formats	**Note:** Defines the card format for cards that are presented and accepted at the Logical Device. These card formats must be added to the panel first. If you are configuring S-Net readers on a PW-6000 panel, you must select a Card Format in this field that has been created specifically for S-Net communications. Use the following guidelines to create this Card Format: 1. In Database Configuration > Card Format tab, create a new Card Format using the PW-5000 Wiegand format type. See "Adding or Editing a Non PW2000 Card Format" on page 5 for details. 2. In Hardware Configuration > Panel tab (for the PW-6000 being configured for S-Net readers), add the Card Format you created in step 1. See "Panel Tab" on page 25 for details. 3. In this Card Formats field in the Reader Settings tab, select the Card Format you added to the panel in step 2.
REX-2 Time Zone Mask	Defines the time zone in which the REX-2 remains masked.
LED Mode	Defines the LED mode for the Logical Device. Note that for S-Net readers on a PW-6000, you must select S-Net from the drop-down menu.
Strike Mode	Defines when a door should re-lock.
Offline Mode	Identifies the mode of the reader in the event the Reader Board I/O Module goes offline with either the PW-5000 panel or the PW-5000 controller.
Strike Time	Defines the strike time for a standard door.
Extended Strike Time (ADA)	Defines the strike time for a door configured for persons that require more time. "ADA" stands for "Americans with Disabilities Act."

Field	Description
Default Mode	Defines the default mode of the reader (Card only, PIN only, Card and PIN). For S-Net readers on a PW-6000: • For readers without a keypad, set the Default Mode field to **Card Only**. • For readers with a keypad, set the Default Mode to either **Card and PIN**, **Card or PIN**, or **PIN Only**.
Held Time	Defines the amount of time a door can be held open before sending an alarm.
Extended Held Time (ADA)	Defines the amount of time a door can be held open before sending an alarm for persons that require more time. “ADA” stands for “Americans with Disabilities Act.”
PIN Retries	Identifies the number of times a PIN can be entered at a keypad before sending an alarm.
Weigand Pulse	A particular type of Weigand card; must be enabled when using this type of card to be able to receive valid card reads.
Honeywell Mag	A particular type of ABA card; must be enabled when using this type of card to be able to receive valid card reads.
Trim Zero Bits	When enabled, zero bits on card number are removed.
Nibble Array	When enabled, the reader uses track 2, 5-bit per character encoding when reading cards.
Bidirectional	When enabled, an ABA card may be swiped in either direction.

Field	Description
User Functions	When enabled, provides the ability for a user to enter a number on the keypad to perform a specified special function (for example, a door unlock for 55 minutes).
S-Net Type	Specifies the type of reader connected to a PW-6000 via S-Net. • For all S-Net readers without a keypad, set the S-Net Type to **DKR**. • For all S-Net readers with a keypad, select **DKR+VIP**. • For all magstripe readers, select **MSRK**. Also, be sure to set the Default Mode field above to Card Only for readers without a keypad, and set the Default Mode to either Card and PIN, Card or PIN, or PIN Only for readers with a keypad.

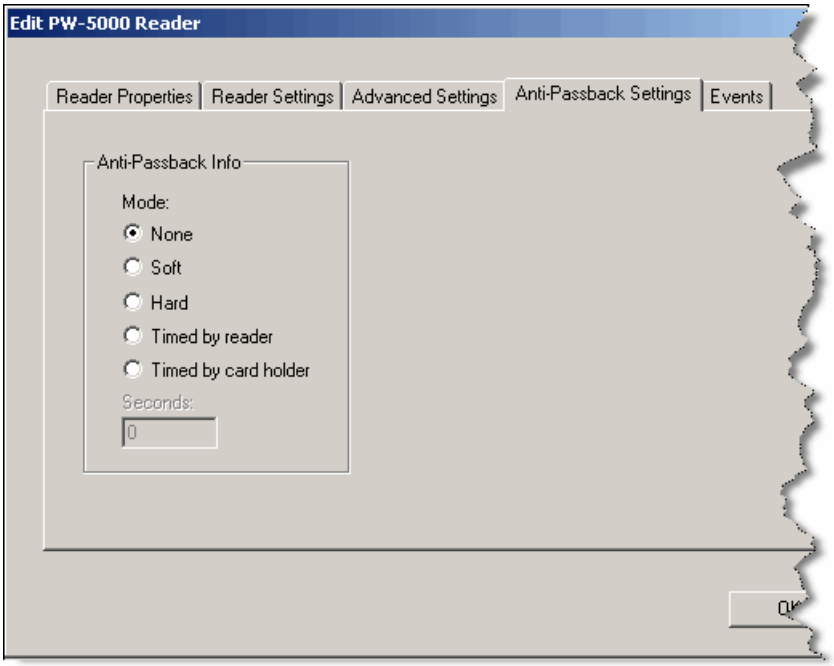
Advanced Settings Tab



Field	Description
Decrement Use Limits	This function is currently not supported.
Require Non-Zero Use Limits	This function is currently not supported.
Deny Duress Requests	When enabled, all duress requests are denied. The “Duress” functionality enables the user to trigger an alarm event in times of duress such as when the site is under attack or the operator is forced to grant access to an unauthorized user. **Note:** The duress functionality is always on by default. When “Deny Duress Requests” check box is selected, the panel assumes that the user has merely “fat-fingered” the PIN code and reports “invalid PIN” instead of triggering an alarm event. The user can enter the duress code for PW-5000 by adding 1 to the last digit of the PIN code. The digit 9 becomes zero.

Field	Description
Log Access Requests as Used	When enabled, the panel reports access as cards are presented to the reader. It is recommended this check box not be enabled when using mustering (see "DBC - Area" in Chapter 29); otherwise, the panel reports the cardholder as being in the area once the card is swiped at the 'in' reader, whether or not the door was actually opened.
Log Pre-Grant Event	When enabled, access is granted when the card is read; however, the panel does not report the cardholder as being in the area until, and unless, the cardholder physically opens the door to enter the area. When the Log Access Requests as Used option is enabled, the Log Pre-Grant Event option is not available. Also, this option is available only for the PW-5000.
Don't Pulse Strike on REX	When enabled, the door does not unlock upon the push of a REX button.
Filter State Transitions	When enabled, the change of state for a DPS is not reported.
Require Two Card Control	Requires two valid cards to unlock the door.
Enable Forced Door Filter	When enabled, a forced door must be open for a fixed duration before an alarm is generated.
Override Time Zone	Defines the time zone in which the door unlocks.
Mask Forced Open	When enabled, forced door events are masked and will cause no alarms.
Mask Held Open	When enabled, door held events are masked and will cause no alarms.
PIN Suppression	Defines the time zone in which PIN numbers are not required.
Pre-Alarm (sec)	Defines the amount of time a configured condition warns or indicates a door held open before sending an alarm or entering the alarm condition.

Anti-passback Settings Tab



Field	Description
None	Prevents the Logical Device from operating under anti-passback rules.
Soft	Allows a second entry on the same card without an exit; however, an event is generated that indicates the second entry. Note that you must also set the panel (in the "Panel Tab") for anti-passback operation. See also "DBC - Area" in Chapter 29.
Hard	Does not allow a second entry on the same card without an exit. Note that you must also set the panel (in the "Panel Tab") for anti-passback operation. See also "DBC - Area" in Chapter 29.
Timed by Reader	Tracks and times only the last card read, as well as the time of the reading. After the reader reads another card, the previous card read will again be accepted by the reader. Therefore, the “Timed by reader” option offers only limited control. Note that you must also set the panel (in the "Panel Tab") for anti-passback operation.

Field	Description
Timed by Card	Tracks and times each card read, even after subsequent cards are read. Pro-Watch keeps a separate timer for each card, and the lockout extends to any door in the Area. “Timed by card” keeps a separate timer for each card. Note that “Timed by card” offers more control than “Timed by reader,” but it consumes significantly more panel memory. Note that you must also set the panel (in the "Panel Tab") for anti-passback operation.
Seconds	For Timed by Reader and Timed by Card, defines the time period during which the device will not grant access to a swipe of the same card without an exit.

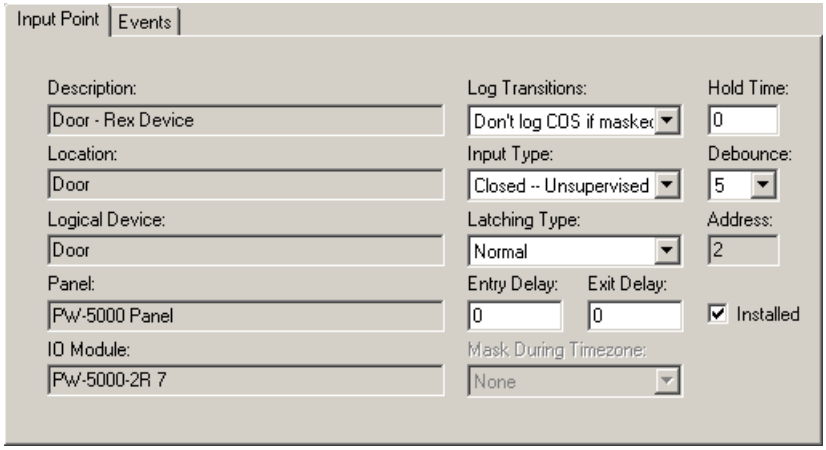
Events Tab

To define an event:

- Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point".

Input Point Devices

Input Point Tab



Field	Description
Description	Provides the name of the Logical Device and the device type as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.

Field	Description
Logical Device	Identifies the name of the Logical Device.
Panel	Identifies the panel in which the Logical Device is assigned.
I/O Module	Identifies the I/O module in which the Logical Device is assigned.
Log Transitions	Determines what is logged when the input is shunted or masked.
Input Type	Determines the input type (that is, Closed - Unsupervised, Open - Supervised).
Latching Type	Determines if the input type is latching, non-latching, or normal.
Entry Delay	If the input type is latching, defines the amount of time to shunt or mask a door after going through the door before an alarm is reported. If the input type is non-latching, the door may close, the door does not need to be masked, and an alarm is not be reported.
Exit Delay	If the input type is latching, defines the amount of time to go through a door before the door is armed (un-masked).
Mask During Time Zone	Defines the time zone in which the input point is masked.
Hold Time	Defines the amount of time a point of entry/exit (i.e., a window or a door) can be held open before an alarm is reported.
Debounce	Defines how long the input must stay in a state before a change of state is reported.
Address	Identifies the address of the Logical Device.
Installed	Required for the Logical Device to be enabled and operational.

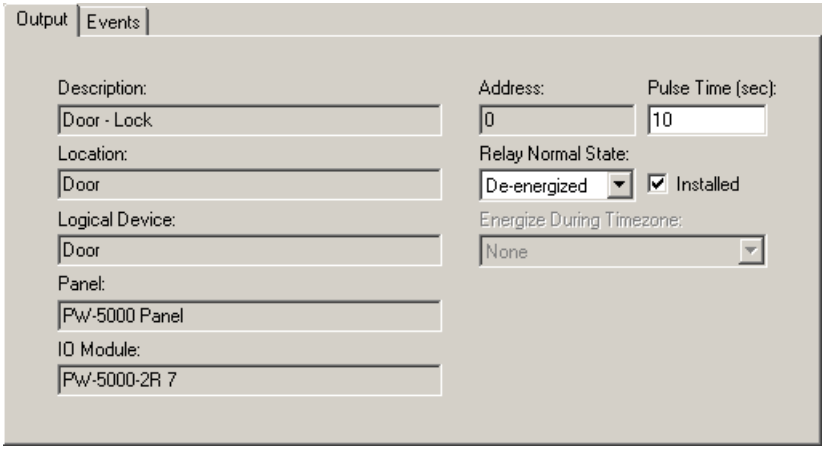
Events Tab

To define an event:

- Either double-click the event you want to define, or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point".

Output Point Devices

Output Tab



Field	Description
Description	Provides the name of the Logical Device and the device type as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel	Identifies the panel in which the Logical Device is assigned.
I/O Module	Identifies the I/O Module in which the Logical Device is assigned.
Address	Identifies the address of the Logical Device.
Pulse Time (sec)	Identifies the pulse time for the output.
Relay Normal State	Defines the normal state for the relay (i.e. energized or de-energized).
Installed	Required for the Logical Device to be enabled and operational.

Field	Description
Energize During Time Zone	Identifies the time zone in which the output should be energized or activated.

Events Tab

To define an event:

1. Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point".
2. Click the **Default CCTV Information** tab. The default CCTV information was configured while adding Logical Devices, if the Logical Devices included CCTV information.
3. Click the **PW-5000 Interlocks** tab. For more information on configuring PW-5000 Interlocks see Adding or Editing a Hardware Template, page 28.
4. Click the **Transactions** tab. The Transactions tab displays all the transactions that have occurred at that particular reader. The number of records are also displayed. The option to print transactions is provided.
5. Click the **Partitions** tab. See "DBC - Partitions" in Chapter 53 to complete configuration.

8.27 Viewing and Editing Dependencies of a Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 53.

8.28 Cypher Mode

When a reader is in cypher mode, a user can enter a sequence of digits on the keypad which is interpreted as a card number.

Cypher mode works on a PW6K1ICE; however, it is different than the PW6000IC. When you enter the card number on the keypad of the reader, you must start with * and then the card number and finish with #.

For example, if the card number is 20418, you enter *20418#. The PW-6000 requires #21418#.

8.29 Deleting a Logical Device

How to Delete a Logical Device, page 53.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Cardkey

9

In this chapter ...

Overview

Adding a Cardkey Channel

Viewing and Editing Dependencies of a Cardkey Channel

Deleting a Cardkey Channel

Adding a Cardkey Panel

Configuring a Panel and Sub-Panels

Editing the Panel's Communication Ports

Viewing and Editing Dependencies of a Cardkey Panel

Deleting a Cardkey Panel

Adding a Cardkey Logical Device

Editing a Cardkey Logical Device

Viewing and Editing Dependencies of a Cardkey Logical Device

Deleting a Cardkey Logical Device

Cardkey Elevators

9.1 Overview

This chapter describes how to configure a site that uses a CARDKEY panel.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

9.2 Adding a Cardkey Channel

The Pro-Watch channel is the communications path between the host and the panel. You must identify the channel before adding a panel and Logical Device.

Note: The recommended maximum number of channels per site is 99.

To add a channel:

1. Select a Channel Type:
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.
   b. Select a channel type specific to your hardware manufacturer from the drop-down list.
   c. Click **OK**. The Define Channel Information dialog box appears.
2. Define the Channel:
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
   c. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.
   d. In the Attempts field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.
   e. In the Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds.
   f. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.
   g. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.
   h. Click **Next** to display the Communications Parameters dialog box.
3. Set Communications Parameters:

a. Select the port type from the following drop-down list options:

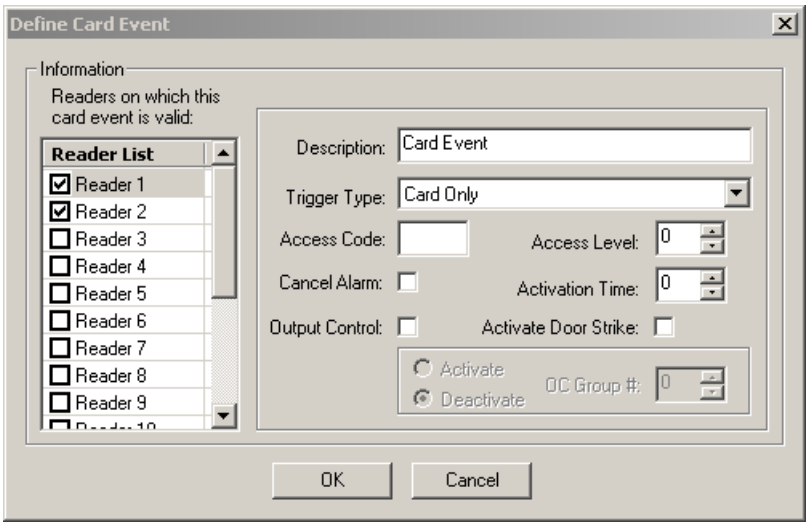
Option	Description
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
TCP/IP	Specifies that the channel is a network connection. IP Address – the IP address of the panel.
Dial Out	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
Dial In	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
TCP/IP (Encrypted)	This functionality is provided by the network connection hardware. “TCP/IP encrypted” encrypts messages between the host and the panel. IP Address – the IP address of the panel. Encrypt Password – the password assigned.

Option	Description
Modem Pools	Modem pools are used with dial-out. Modem Pool – collection of modems. Baud – the rate of communication between the host and the panel. Flow Control – starts and stops the transmission between the host and the panel.
Secondary Channel	Acts as a fail-safe; secondary channel communication comes online if the primary channel communication breaks.

b. Click **Next** to display the Card Events dialog box. Card events are similar to panel triggers and procedures. You must add card events to the channel before you add them to the panel.

4. To add a card event:

   a. Click **Add** to display the Define Card Event dialog box.

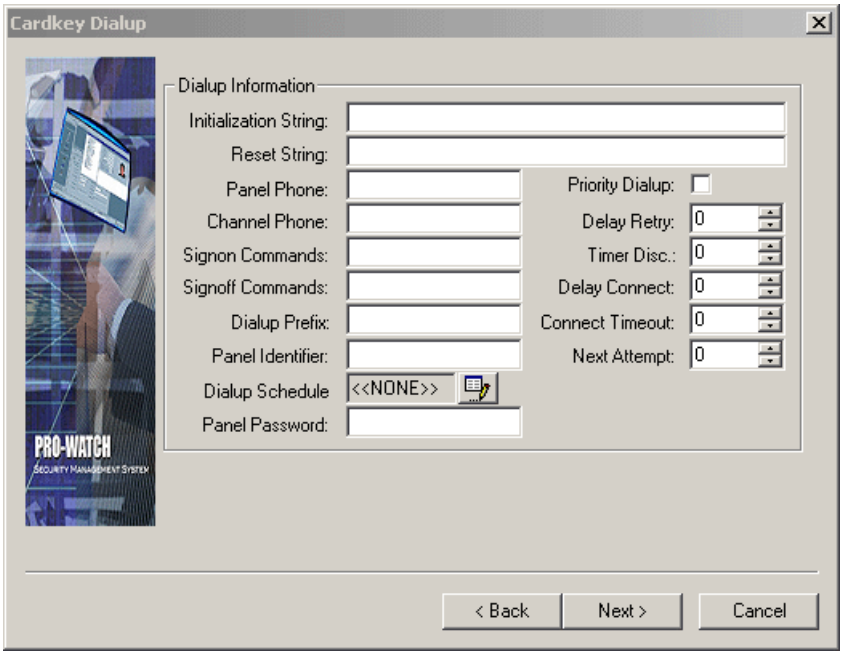


b. Use the table below to complete card event configuration:

Field	Description
Description	Provides the description of the card event.
Trigger Type	Defines the trigger type for the card event.
Access Code	Defines the code or sequence a cardholder enters at a keypad to initiate the card event (that is, to de-activate the output device after a valid card swipe).
Access Level	Defines the access level for the card event. If an access level is assigned, the badgeholder's card must have an access level assigned greater than or equal to the access level for the card event in order for the event to initiate.
Cancel Alarm	When enabled, the relay on the panel is disabled.
Activation Time	Defines the amount of time (sec) the output(s) energize.
Output Control	When enabled, allows you to define an output control for an output group.
Activate Door Strike	Indicates whether the door strike should activate.
Activate/ Deactivate	Indicates whether the door strike should de-activate.
OC Group #	Identifies the output control group number defined in the Logical Device configuration. For more information, see Adding a Cardkey Logical Device.
Reader List	Identifies the readers to which the card events apply.

c. Click **OK** to complete the Card Event dialog box.

d. Click **Next** to display the Cardkey Dialup dialog box. Please see Appendix C, Dial-Up Configuration for more information on configuring dial-up for the Cardkey Panels.

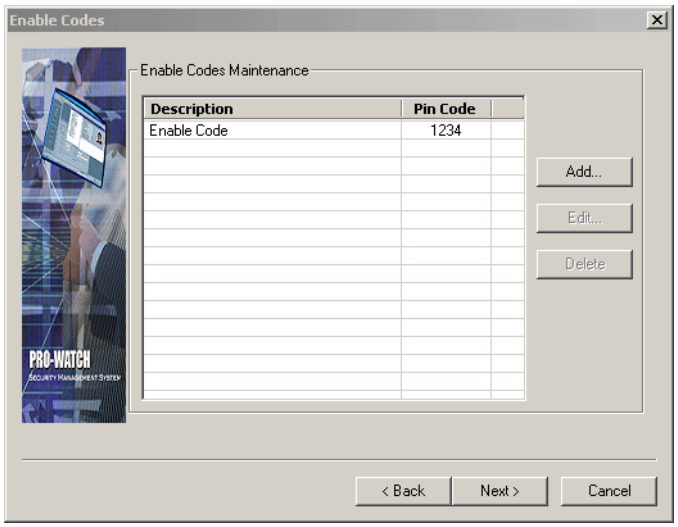


5. Use the following field definitions to complete the settings within the Cardkey Dialup dialog box:

Field	Description
Initialization String	Defines the string to initialize the modem.
Reset String	Defines the string to reset the modem.
Panel Phone	Defines the remote phone number.
Priority Dialup	When enabled, the dial-up is a priority dial-up.
Channel Phone	Defines the host phone number.
Delay Retry	Defines the length of time between dial-up retries (sec).
Signon Commands	Defines the command to log into the panel.
Timer Disc.	Defines the amount of time to wait before disconnecting.
Signoff Commands	Defines the command to log out of the panel.
Delay Connect	This function is currently not supported.

Field	Description
Dialup Prefix	Defined the prefix that must be entered before dial-up (i.e. dial 9).
Connect Timeout	Defines the amount of time to wait before no longer attempting to make a connection.
Panel Identifier	Defines the unique panel identifier. It identifies which panel is attempting to connect.
Next Attempt	This function is currently not supported.
Dialup Schedule	Identifies the dial-up schedule for the panel. See "DBC - Dial-Up Schedule" in Chapter 42.
Panel Password	This function is currently not supported.

6. Click **Next** to display the enable codes dialog box. Enable codes are codes that allow for feature add-ons. You must add these codes to the channel before you add them to the panel. Only the first three enable codes are accepted and operational. Enable codes apply only to D600AP.
7. To add an enable code:
   a. Click **Add**.
   b. Enter the description for the enable code.
   c. Select the **Code Type** from the drop-down list.
   d. Enter the **Code Digits** (four digits) and click **OK**.



e. Click **Next** to display the Partitions dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.

f. Click **Finish** to complete the channel. A warning message appears reminding you that you must add the channel to the appropriate routing group before you can view any events using the channel. It is recommended that you assign the channel to a routing group after you plan and configure routing groups. See "DBC - Routing Groups" in Chapter 55.

9.3 Viewing and Editing Dependencies of a Cardkey Channel

Please refer to How to View and Edit Dependencies of a Channel, page 51.

9.4 Deleting a Cardkey Channel

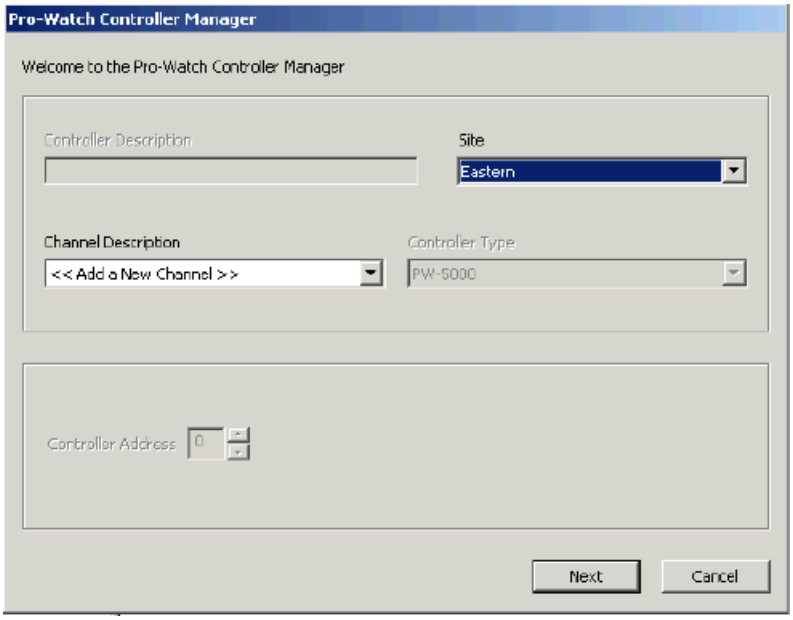
Please refer to How to Delete a Channel, page 51.

9.5 Adding a Cardkey Panel

To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 4.

To add a panel:

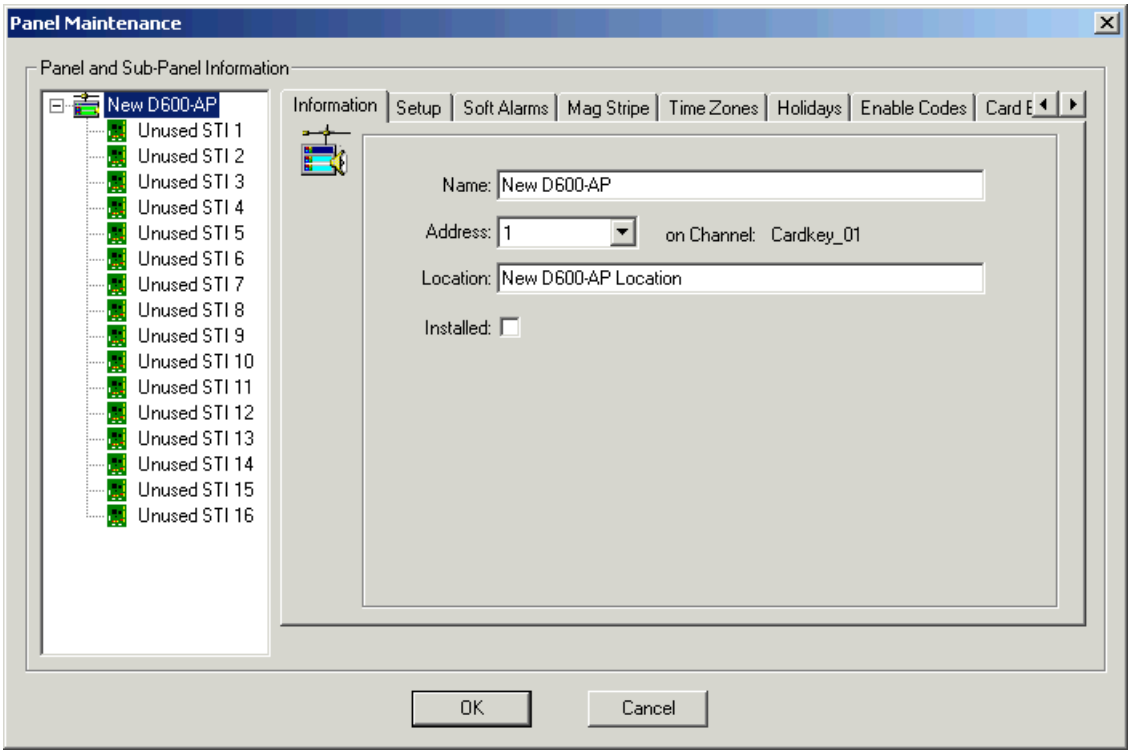
1. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
2. Select **New > Panel** to display the Pro-Watch Controller Manager dialog box.



3. Select the channel you have created for this panel from the Channel Description drop-down list and click **Next**. The Panel Maintenance dialog box appears.
4. Use the tab and field descriptions in the following section to configure the Cardkey panel in the Panel Maintenance dialog box.
5. Click **OK**.

9.6 Configuring a Panel and Sub-Panels

Pro-Watch supports the Cardkey D600AP and D620 panels. Each of these panel types share similar configuration tasks. In the Panel Maintenance dialog box, the panel tree view lists each panel and its respective sub-panels, which are also called STIs. In the figure below, New D600AP is the panel and the indented icons beneath it are the sub-panels, or STIs.



You can display the Panel Maintenance dialog box either when you configure a new panel (right-click on a channel icon and select **New**) or edit an existing panel (right-click the existing panel's icon and select **Properties**).

If you are adding a new panel, you must configure the panel before configuring the panel's sub-panels or STIs.

9.6.1 Configuring the Panel

Edit the Cardkey panel before editing each of its sub-panels. To edit the panel, complete each of the following information tabs in the Panel Maintenance dialog box:

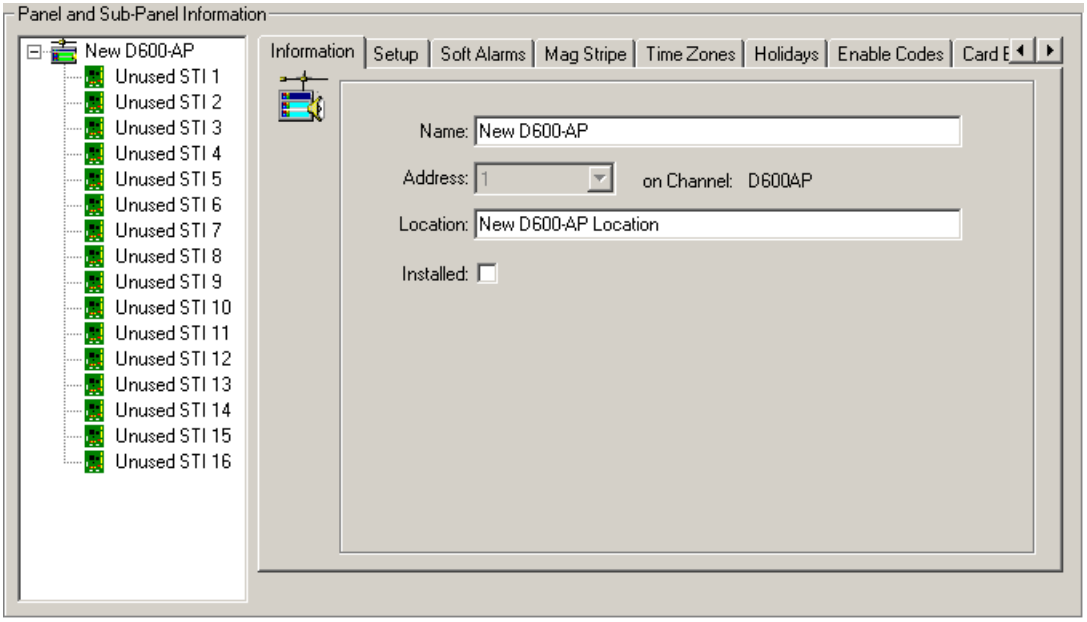
PANEL MAINTENANCE TABS LIST

- Information Tab.
- Setup Tab.
- Soft Alarms Tab.

- Mag Stripe Tab.
- Time Zones Tab.
- Holidays Tab.
- Enable Codes Tab.
- Card Events Tab.
- Events Tab.
- Partitions Tab.

Information Tab

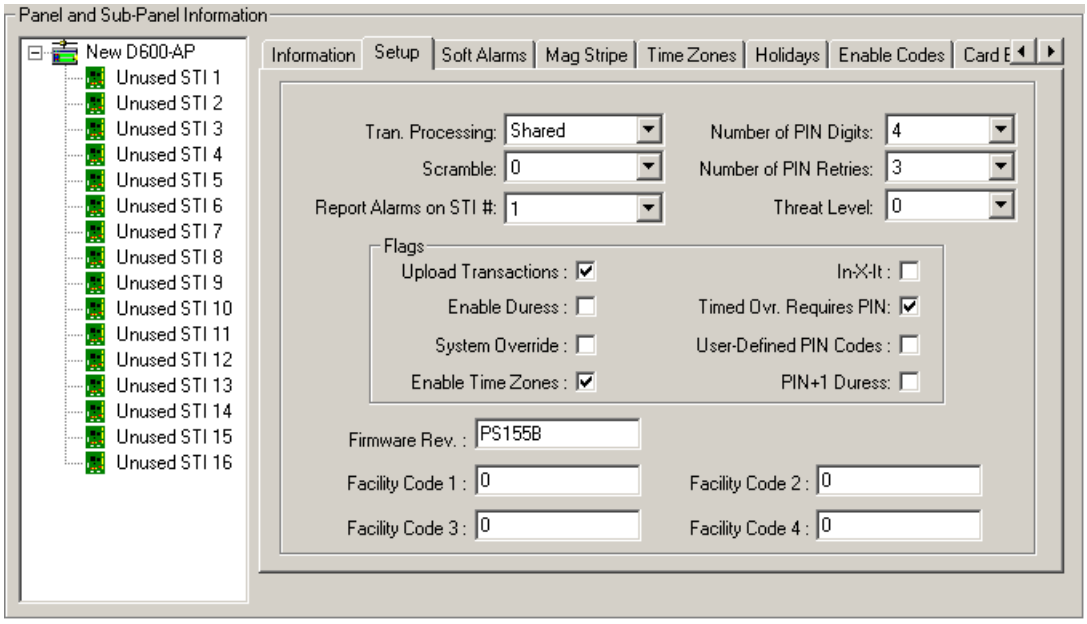
The Information tab includes hardware setting information for the panel and allows you to install the panel.



Field	Description	Panel Type
Name	Identifies the panel.	All panel types.
Address	Identifies the address of the panel, from 1 to 30.	All panel types.
Location	Identifies the location of the panel as defined by the user.	All panel types.
Installed	Required for the panel to be installed and operational.	All panel types.

Setup Tab

The Setup tab enables you to configure hardware settings for the panel.



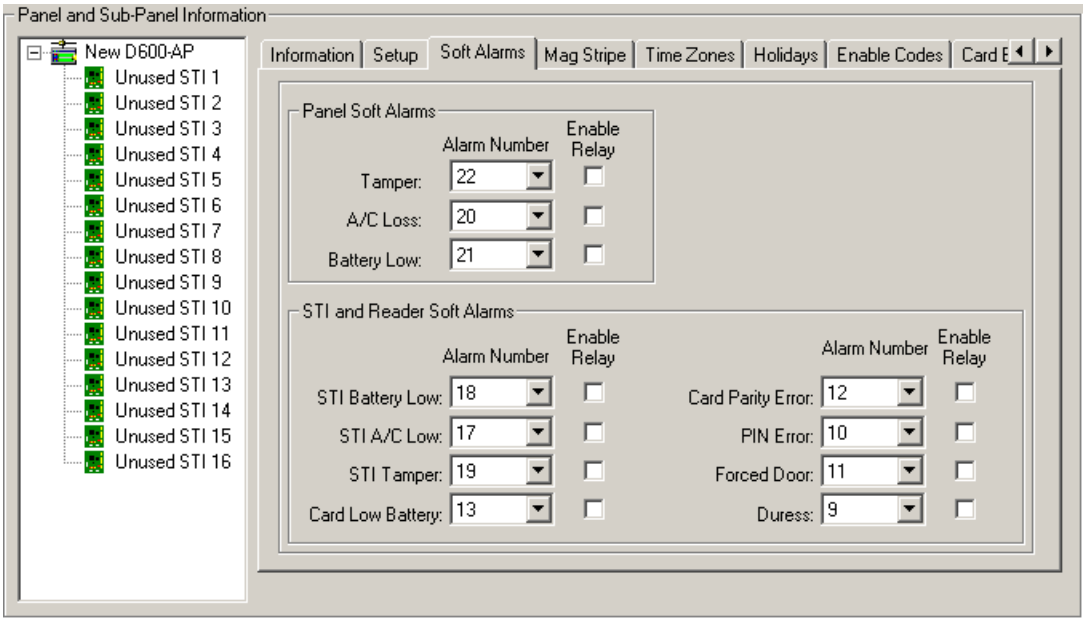
Field	Description	Panel Type
Tran. Processing	Defines where the card transactions are processed (local, shared, control).	All Panel Types.
Number of PIN Digits	Defines the number of PIN digits that can be assigned in a PIN number.	All Panel Types.
Scramble	Scrambles the card number according to the “Cardkey proprietary scramble mode”.	All Panel Types.
Number of PIN Retries	Defines the number of attempts a PIN holder has to correctly enter the PIN number before sending an alarm, in the event the first attempt was incorrect.	Cardkey D600AP.
Report Alarms on STI #	Identifies the STI in which the panel alarms get reported as Pro-Watch required this field to be set to 1.	All Panel Types.
Threat Level	Defines the threat level for the panel. Badgeholders must have a threat level greater than or equal to the panel threat level assigned to the card to get access.	Cardkey D600AP.

Field	Description	Panel Type
Upload Transactions	When enabled, transactions are sent to the host.	All Panel Types.
In-X-It	Enables anti-passback. See "DBC - Area" in Chapter 29.	All Panel Types.
Enable Duress	Enables duress. The “Duress” functionality enables the user to trigger an alarm event in times of duress such as when the site is under attack or the operator is forced to grant access to an unauthorized user.	Cardkey D600AP.
Timed Ovr. Requires PIN	When enabled, programming a door to stay open for a specified amount of time requires a PIN.	Cardkey D600AP.
System Override	When enabled, all doors unlock.	All Panel Types.
User-Defines PIN Codes	When enabled, a user can define the PIN number. If disabled all PIN numbers are algorithmic.	All Panel Types.
Enable Time Zones	Required to enable use of time zones.	All Panel Types.
PIN + 1 Duress	When enabled, duress can be initiated in two ways: entering 9 on the keypad or entering the PIN+1 on the keypad. The “Duress” functionality enables the user to trigger an alarm event in times of duress such as when the site is under attack or the operator is forced to grant access to an unauthorized user.	Cardkey D600AP.
Firmware Rev.	Identifies the firmware version; for information purposes only.	All Panel Types.
Facility Code 1	Identifies a generic facility code for the panel.	Cardkey D600AP.
Facility Code 2	Identifies a generic facility code for the panel.	Cardkey D600AP.
Facility Code 3	Identifies a generic facility code for the panel.	Cardkey D600AP.
Facility Code 4	Identifies a generic facility code for the panel.	Cardkey D600AP.

Field	Description	Panel Type
Weigand Fac Code	Identifies the Weigand card facility code.	Cardkey D620.
Mag Fac Code	Identifies the Mag Stripe card facility code.	Cardkey D620.
N-Crypt Fac Code	Identifies the N-Crypt facility code. N-Crypt is Cardkey specific.	Cardkey D620.

Soft Alarms Tab

The Soft Alarms tab enables you assign a number to a particular alarm. The Soft Alarms tab also allows you to enable the relay that activates in the event the alarm occurs.

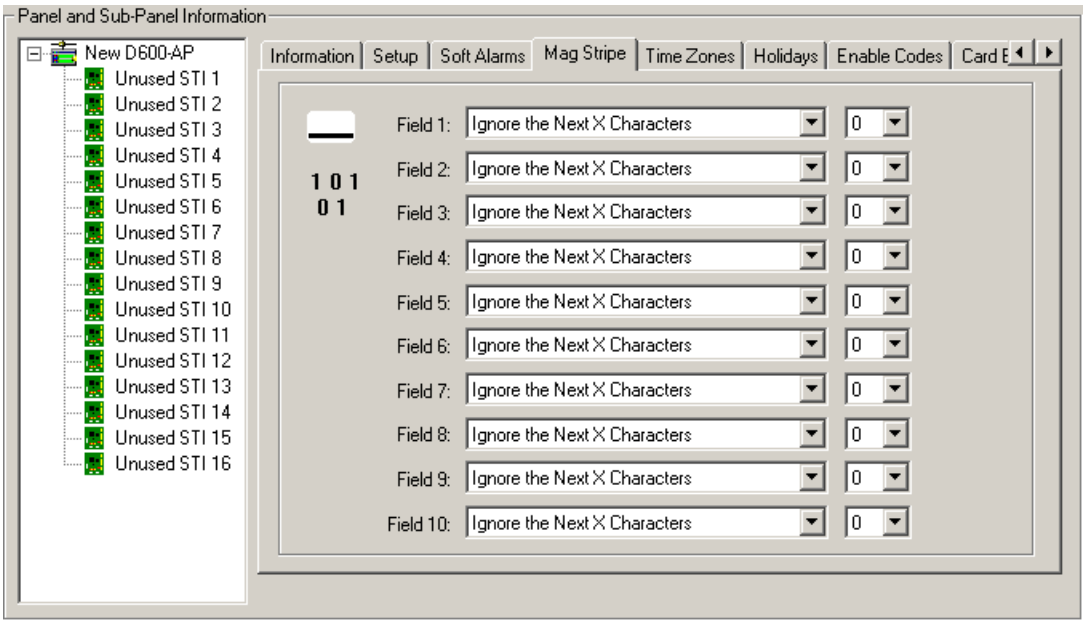


Field	Description	Panel Type
Tamper	Defines the number the alarm reports as. Using the defaults is strongly recommended.	All Panel Types.
A/C Loss	Defines the number the alarm reports as. Using the defaults is strongly recommended.	All Panel Types.

Field	Description	Panel Type
Battery Low	Defines the number the alarm reports as. Using the defaults is strongly recommended.	All Panel Types.
STI Battery Low	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
Card Parity Error	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
STI A/C Low	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
PIN Error	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
STI Tamper	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
Forced Door	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
Card Low Battery	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
Duress	Defines the number the alarm reports as. It is strongly recommend using the defaults.	All Panel Types.
Enable Relay (Panel)	When enabled, if the corresponding alarm occurs, the relay activates.	All Panel Types.

Mag Stripe Tab

The Mag Stripe tab allows you to define parameters for specific fields on a Mag Stripe configuration. The Mag Stripe tab applies only to the D600AP.



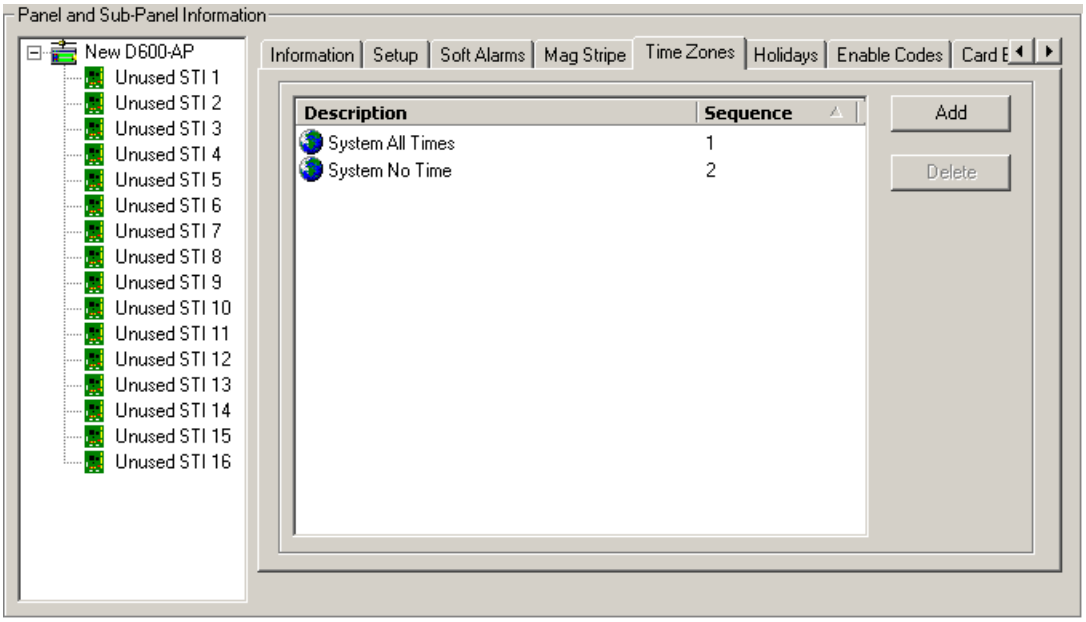
To define parameters for each field:

1. Select the instruction from the drop-down list.
2. Assign the number to the field by selecting the number from the drop-down list.

   Example: If you select for Field 1: “Ignore the Next X Characters” and select “3”. The next 3 characters will be ignored on the Mag Stripe card. In Field 2: “Card Number Field” and “4”, the next 4 characters will be the card number. You cannot overlap when defining fields.

Time Zones Tab

The Time Zones tab enables you to add time zones to the panel; only time zones that have been added to the panel are available to configure applicable panel and reader fields.



To add a time zone to the panel:

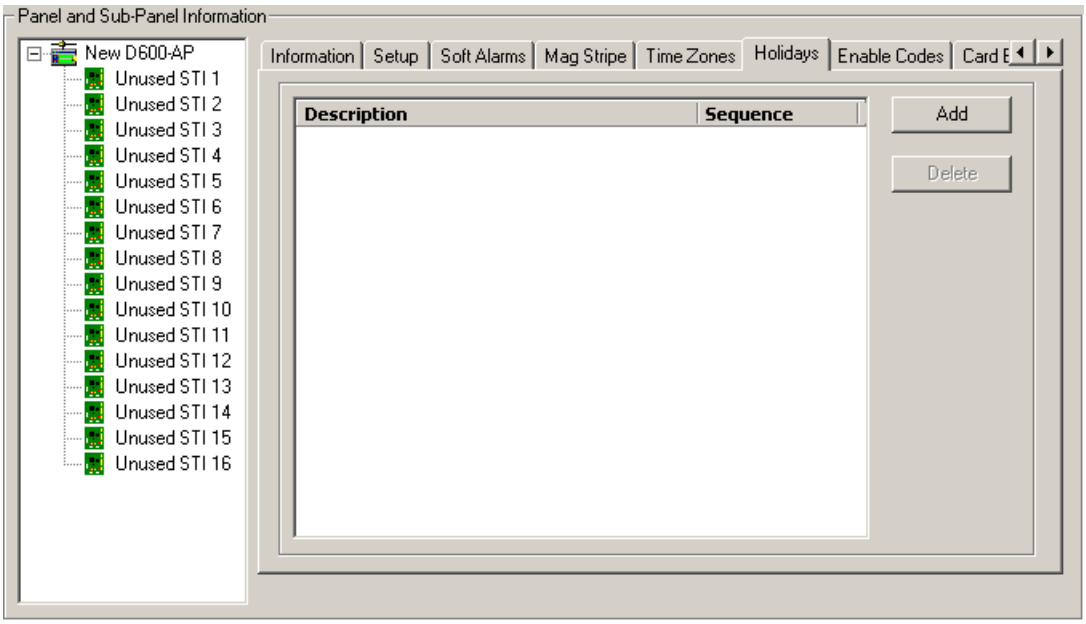
1. Click **Add** to display the **Time Zones** dialog box.
2. Select the time zone and then click **OK**.
3. To add a new time zone, click **Add**.
4. To edit an existing time zone, select it from the list and click **Edit**.
5. To delete an existing time zone, select it from the list and click **Delete**.

Click **OK** again at the Select Time Zone dialog box.

To create a new Time Zone to appear in the Time Zones dialog box, see "DBC - Time Zones" in Chapter 57.

Holidays Tab

The Holidays tab enables you to edit normal Time Zone behavior on specific days. You can enable panels to restrict access on holidays.



To add a holiday to the panel:

1. Click **Add.**
2. Click the icon next to the Holiday field.
3. Click **Define**.
4. Select the holiday from the **Holiday List** dialog box and click **OK**.
5. Select the sequence number from the drop-down list and click **OK**.

If the holiday you want does not appear in the Holiday List dialog box you can create a new holiday.

To add a new holiday:

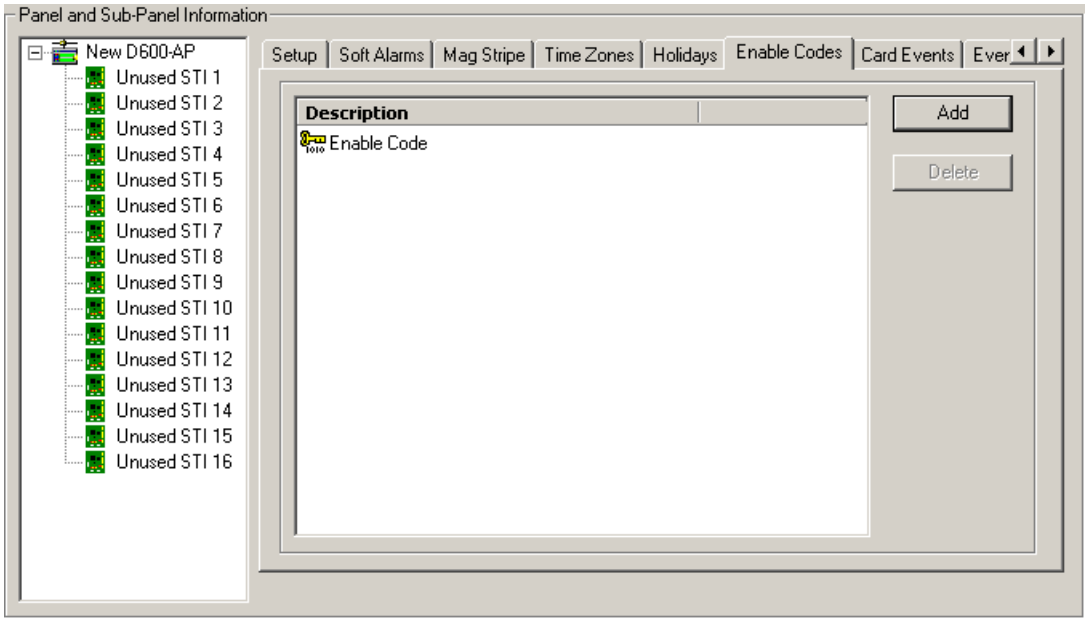
Click **Add** within the Holiday List dialog box.

To complete adding a new holiday:

See "DBC - Holidays" in Chapter 49.

Enable Codes Tab

You must add enable codes to the channel before you can add to the panel; only the first three are operational/accepted. Enable codes apply only to the D600AP.



To add an enable code to the panel:

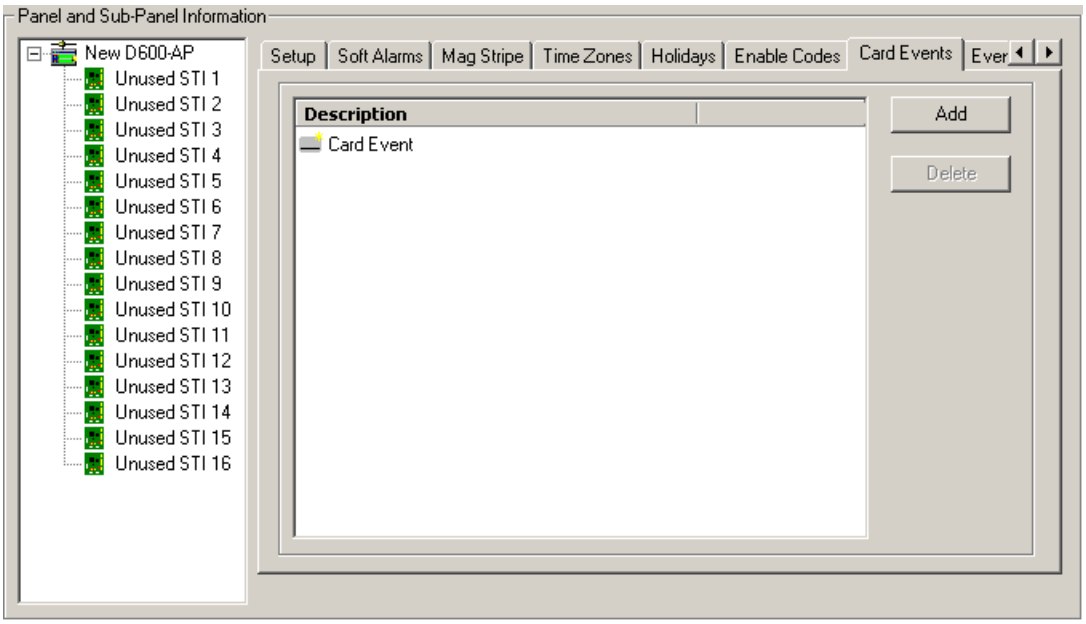
1. Click **Add** to display the Select Enable Code dialog box.
2. Select the **Enable Code** from the drop-down list.
3. Click **OK**.

To delete an enable code from the panel:

1. Select the **Enable Code**.
2. Click **Delete**.

Card Events Tab

Card events must be added to the channel before you can add to the panel.



To add a card event to the panel:

1. Click **Add** to display the Select Card Event dialog box.
2. Select the **Card Event** from the drop-down list.
3. Click **OK**.

To delete an card event from the panel:

1. Select the **Card Event**.
2. Click **Delete**.

Events Tab

The Events tab displays the default event types that are applicable to the Cardkey panel.

To define an event:

Either double-click the event you want to define or select and click **Edit**. The **Edit Point** dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

Partitions Tab

Partitions determine the view of the resources within Pro-Watch. For information about creating a partition, see "DBC - Partitions" in Chapter 53. Use this function to assign or delete an already-created partition to the panel.

To add a partition to the panel:

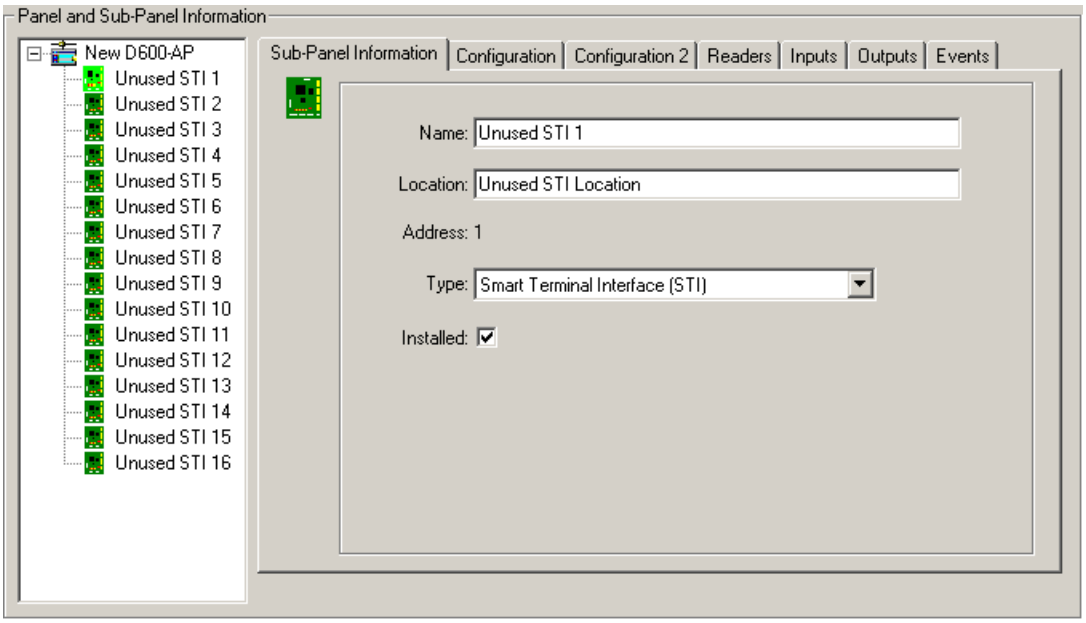
1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition.
3. Click **Add**.

To delete a partition from the Partitions List dialog box:

1. Select the partition.
2. Click **Delete**.

9.6.2 Configuring the Sub-Panels (STIs)

1. In the Panel and Sub-Panel Information tree view, click the icon of the sub-panel you want to edit to display the sub-panel's information tabs.



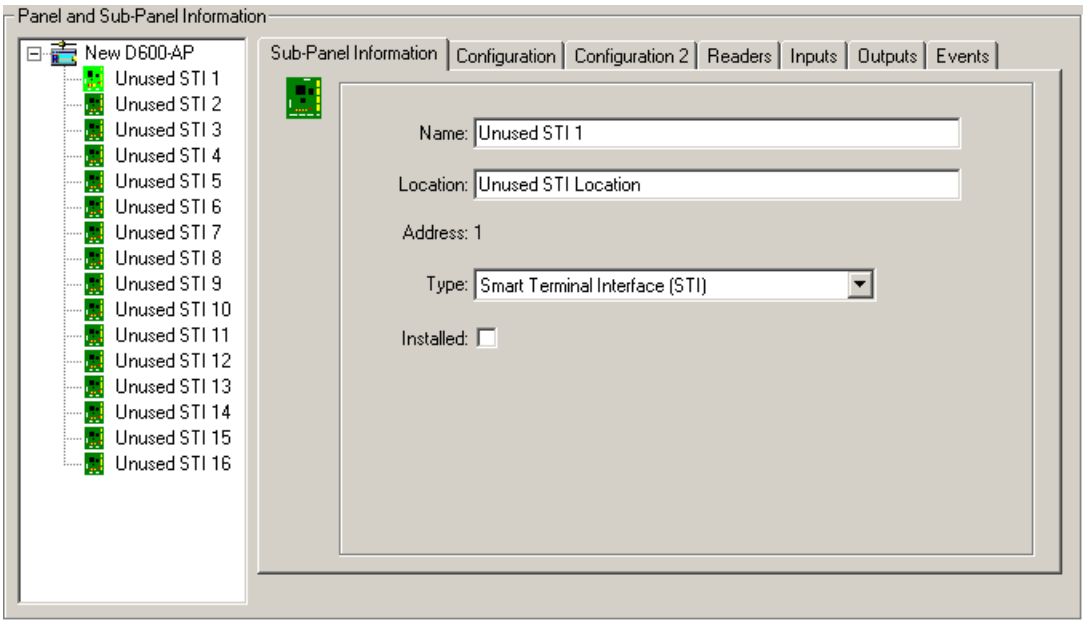
2. Complete each of the following information tabs to finish the panel configuration:

SUB-PANEL INFORMATION TABS LIST

- Sub-Panel Information Tab.
- Configuration Tab.
- Configuration 2 Tab.
- Readers Tab.
- Inputs Tab.

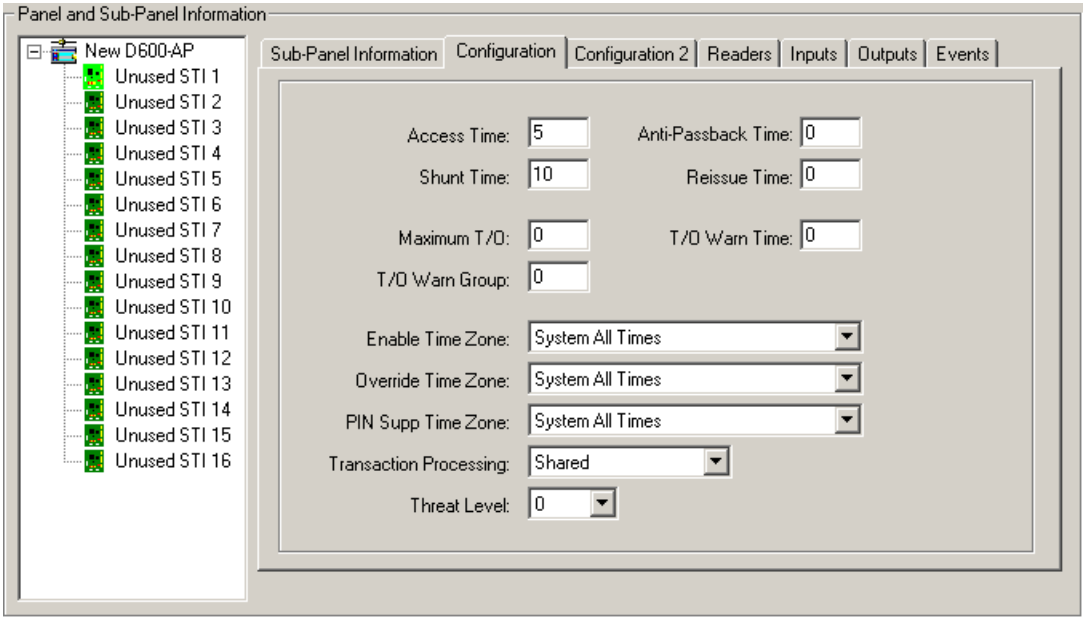
- Outputs Tab.
- Events Tab.

Sub-Panel Information Tab



Field	Description
Name	Identifies the name of the sub-panel
Location	Identifies the location of the sub-panel as defined by the user.
Address	Identifies the address of the sub-panel.
Type	Defines the type of sub-panel (STI, OCT, AMT).
Installed	Required for the sub-panel to be enabled and operational.

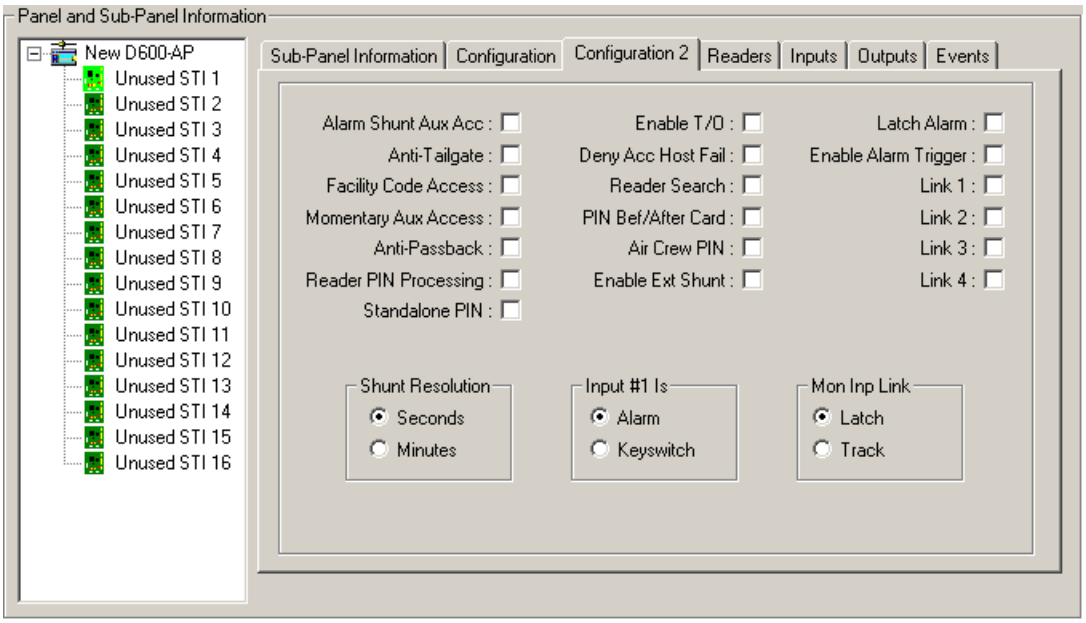
Configuration Tab



Field	Description
Access Time	Defines the time (sec) that a door strike relay is energized after a valid card swipe. The maximum access time is 25 seconds.
Anti-Passback Time	Defines the time in which a card can no longer be used at a particular reader configured for anti-passback (or at any other anti-passback reader).
Shunt Time	Defines the time (sec) that a door open alarm is suppressed after a valid card swipe.
Reissue Time	This function is currently not supported.
Maximum T/O	Defines the maximum amount of time you can override a door (maximum of 1440 minutes).
T/O Warn Time	Defines the amount of time (min) up to 10 minutes for a warning the timed override is about to expire.
T/O Warn Group	Defines the output control group to activate when a timed override is about to expire.
Enable Time Zone	Defines the time zone in which the STI is valid.
Override Time Zone	Defines the time zone in which the doors are unlocked.

Field	Description
PIN Suppression Time Zone	Defines the time zone in which the PIN number is suppressed; the cardholder is not required to enter a PIN.
Transaction Processing	Defines where the card transactions are processed (local, shared, control).
Threat Level	Defines the threat level for the panel. Badgeholders must have a threat level greater than or equal to the panel threat level assigned to the card to get access.

Configuration 2 Tab



Field	Description
Alarm Shunt Aux Acc	When this is enabled, you cannot open the door by using an auxiliary switch. The auxiliary switch will not energize the door relay; however, the shunt timer will start. This will shunt alarms.
Enable T/O	Enables timed override.

Field	Description
Latch Alarm	Allows the input point to latch or track the output point. For example, if a horn is associated with a door, you can configure the horn to either continue to sound (latch) or silence (track) after the door is closed. This applies only to STI sub-panels.
Anti-Tailgate	Monitors the door-open detector. When a door input point indicates the door is open, the door strike de-activates. When the door input point indicates the door is closed, the suppression is removed from the door open alarm. **Note:** Anti-tailgate should not be used with MagLock doors.
Deny Acc Host Fail	Denies all access attempts if the panel loses communication with the host.
Enable Alarm Trigger	When enabled, on an AMT sub-panel, allows for the output to energize when one or more of the inputs activate. This feature works in conjunction with Monitor Inp. Link.
Facility Code Access	When enabled, the STI grants access to any card with the correct facility code in the event communication is lost with the controller.
Reader Search	When enabled, when a card is presented to a reader, that reader checks the card against the data in its memory to determine access. This occurs if the communication is lost with the controller. Data is downloaded to the reader from a maximum of 1000 cards.
Link 1	Defines how to link inputs to outputs. When enabled, turns on/off the links between the input and corresponding output.
Link 2	Defines how to link inputs to outputs. When enabled, turns on/off the links between the input and corresponding output.
Link 3	Defines how to link inputs to outputs. When enabled, turns on/off the links between the input and corresponding output.
Link 4	Defines how to link inputs to outputs. When enabled, turns on/off the links between the input and corresponding output.

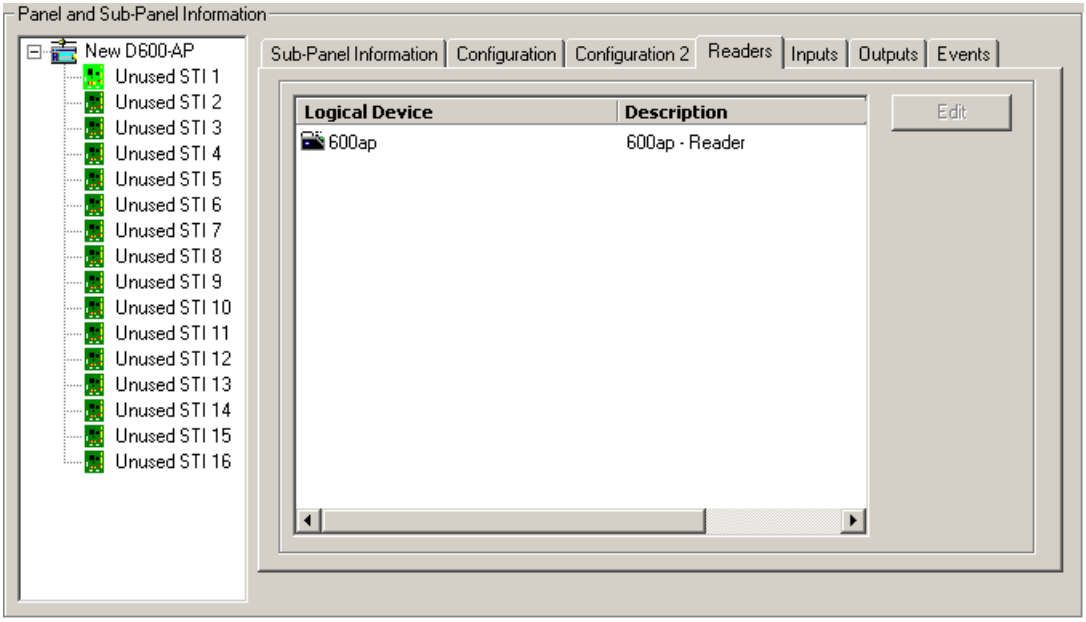
Field	Description
Momentary Auxiliary Access	When enabled, the access timer is initiated when the auxiliary access switch is pressed. The access timer times out even if the switch is continuously pressed or if the switch remains closed. **Note:** This can only be enabled if the Alarm Shunt Auxiliary Access is disabled.
PIN Bef/After Card	When enabled, allows you to enter a PIN number before or after the card is swiped.
Anti-Passback	When enabled, allows for anti-passback configuration.
Air Crew PIN	When enabled, allows for the use of Air Crew PIN. Air Crew PIN requires the enable code to be entered. Air Crew PIN allows you to enter up to 12 digit number on the keypad that requires the host to make the access decisions.
Reader PIN Processing	When enabled, the reader processes the PIN numbers locally.
Enable Ext Shunt	Requires an enable code. When enabled, it allows an extended shunt time with a normal door strike unlock time.
Standalone PIN	When enabled, the cardholder is required to enter the PIN number in addition to a card swipe if the STI loses communication.
Shunt Resolution (Seconds/ Minutes)	When defining the shunt time, it designates the unit of measurement.
Input #1 is (Alarm/ Keyswitch)	Assigns Input # 1 as either a DPS or a keyswitch.
Monitor Inp Link (Latch/ Track)	When enabled, allows the input to latch or track the output. Example**:** If a horn is associated with a door, the horn will continue to sound after the door is closed (latch), or the horn will be silenced once the door is closed (track). Applicable on AMT sub-panels only.

Readers Tab

The reader tab displays all assigned (and unassigned) readers on the STI.

To edit the reader configuration:

1. Select the reader.
2. Click **Edit**. to display the Edit Logical Device dialog box.
3. See the field descriptions given in Adding a Cardkey Logical Device to complete the dialog box.

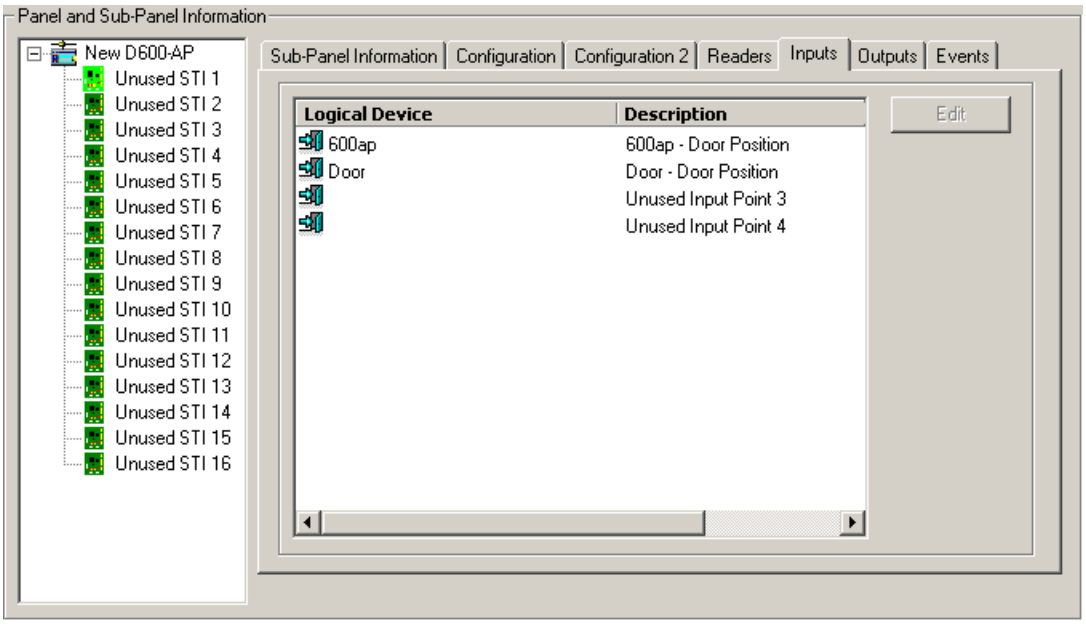


Inputs Tab

The Inputs tab displays all assigned (and unassigned) input points on the STI.

To edit the input point configuration:

1. Select the input point.
2. Click **Edit**. For more information, see Adding a Cardkey Logical Device.

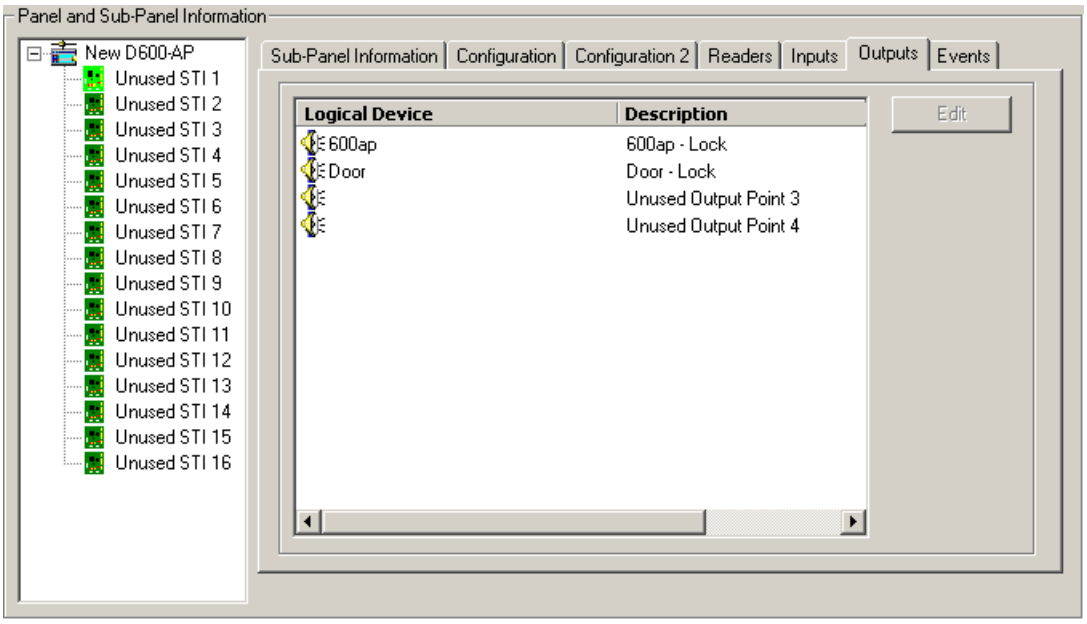


Outputs Tab

The Outputs tab displays all assigned (and unassigned) output points on the STI.

To edit the output point configuration:

1. Select the output point.
2. Click **Edit**. For more information, see Adding a Cardkey Logical Device.



Events Tab

The Events tab displays the default event types that apply to the Cardkey panel.

To define an event:

Either double-click the event you want to define or select and click **Edit**. The **Edit Point** dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

The Panel Maintenance dialog box includes multiple tabs that you must address in order to complete panel configuration.

To display the Panel Maintenance tabs:

Click the panel name within the panel tree view.

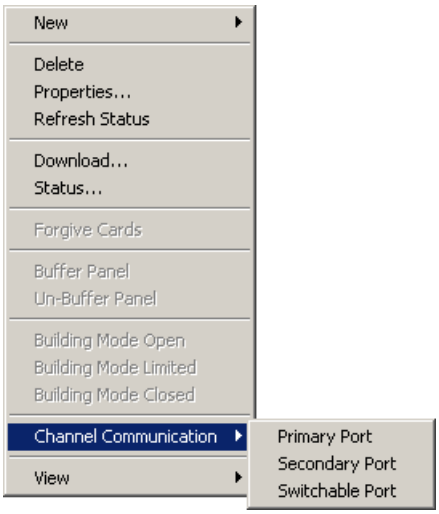
Note: After completing each tab within the panel, you will need to save the panel configuration. To save the panel configuration, click **OK** at the Panel Maintenance dialog box.

9.7 Editing the Panel's Communication Ports

The Cardkey panel(s) allow you to change channel communication ports. For more information, see Adding a Cardkey Channel. You can select to change the port to Primary, Secondary, or Switchable.

To change the channel communication:

1. Select the panel from the Hardware Configuration tree view and right-click.
2. Select **Channel Communications** > **Primary Port/Secondary Port/Switchable Port**.



Selecting Primary Port forces the panel to communicate only to the channel's Primary port. Selecting Secondary port forces the panel to communicate only to the channel's secondary port. Finally, selecting Switchable Port relinquishes the constraint that the Cardkey panel must communicate to only one port.

Note: When selecting these options from the panel right-click, only that panel is affected; however, when selecting the channel communication from a channel right-click, all panels are affected.

9.8 Viewing and Editing Dependencies of a Cardkey Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

9.9 Deleting a Cardkey Panel

Please refer to How to Delete a Panel, page 53.

9.10 Adding a Cardkey Logical Device

A Logical Device is a single physical device or group of selected physical devices, which are defined by a hardware template. For example, a template may define a door that is equipped with a card reader, a REX input device, and a door strike output device as one Logical Device.

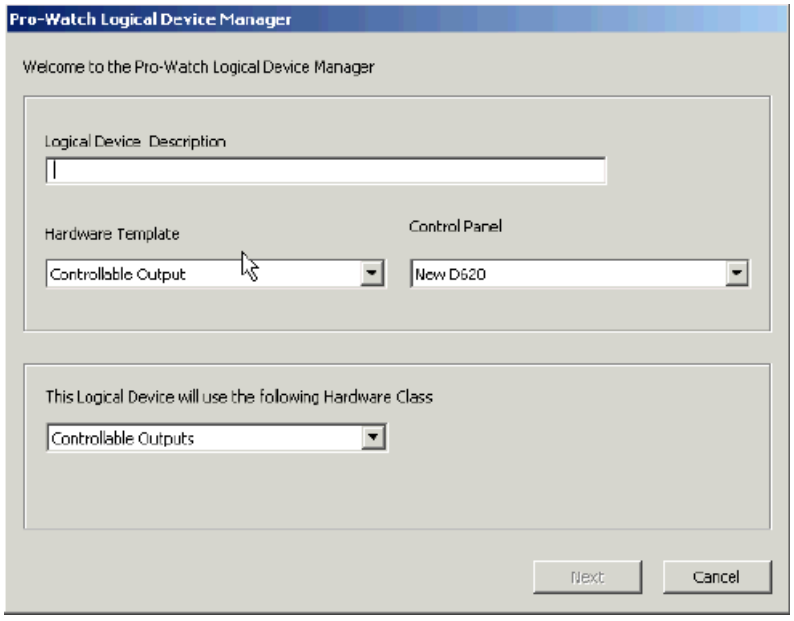
As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system. For example, you can assign the door, reader, input device, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you create Logical Devices, you must create the following:

- Site. See Adding a Cardkey Channel.
- Channel. See Adding a Cardkey Channel.
- Panel. See Adding a Cardkey Panel.
- Hardware Template. See Adding or Editing a Hardware Template, page 28.

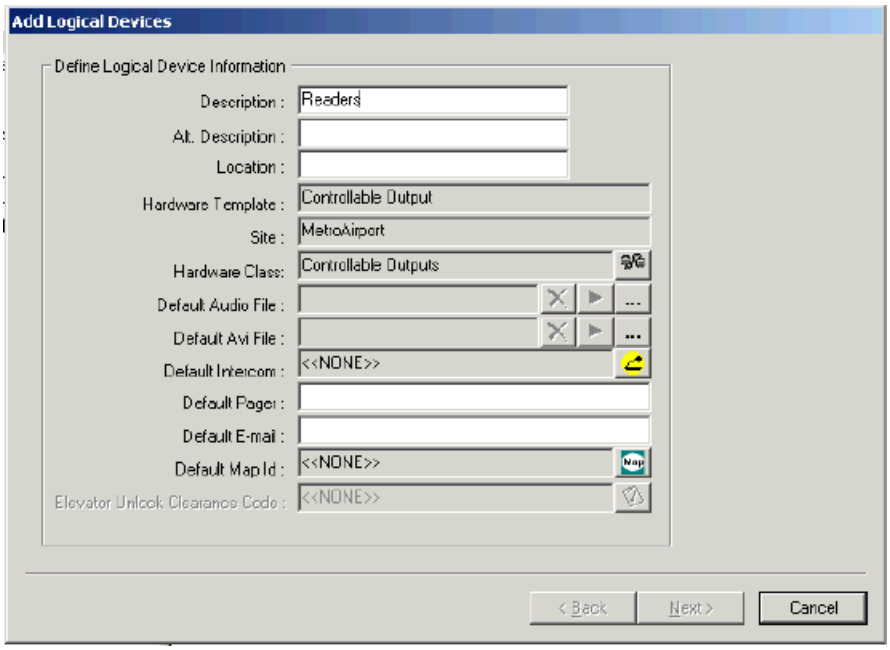
To add a logical device:

1. From the Pro-Watch Hardware Configuration tree view, right-click the site to which you want to assign the Logical Device, and select **New > Logical Device**. The Logical Device Manager dialog box appears:



2. Enter a description that will identify the Logical Device in the Logical Device Description field.
3. Select a Hardware Template from the drop-down list in the Hardware Template field.

4. Select a Hardware Class from the drop-down list in the Hardware Class field.
5. Click **Next**. The Add Logical Devices dialog box appears.

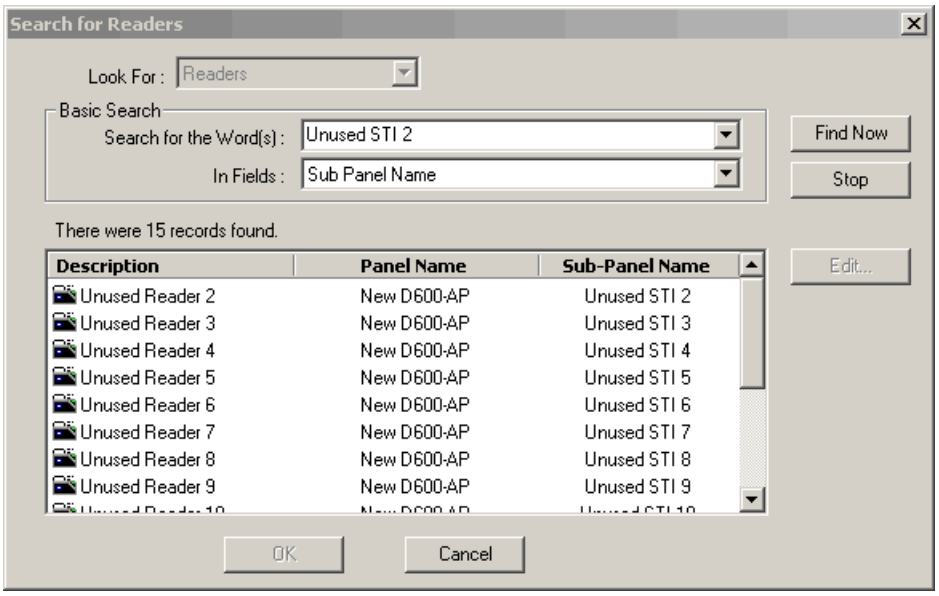


6. Use the following table to complete the Define Logical Device field entries:

Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.

Field	Description
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "DBC - Routing Groups" in Chapter 55.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. For more information, see "DBC - Clearance Codes" in Chapter 37.

7. Click **Next**. The Logical Device Details dialog box appears:
8. Select a device type and click **Assign HW** to display the Search for [Device Type] dialog box:



9. Enter the description in the 'Search for Word(s)' field; this is the description that is used to search for available addresses.
10. Select the field name from the 'In Fields' drop-down list and click **Find Now**.
11. Select the record and click **OK**.
12. Repeat step 5 through step 9 until all device types have been assigned.
13. Click **Next**. The Default CCTV Information dialog box appears.
14. CCTV may be associated with Logical Devices. You may assign the default view and commands for this device. For more information, see "HW Config - CCTV" in Chapter 21. To assign a Default Command or View, click on the icon and select the command or view. Click **OK** and then click **Next**. The Partitions dialog box appears.
15. To assign a partition to this Logical Device, click **Add**, select the partition, and click **Add** again. For information about partitions, see "DBC - Partitions" in Chapter 53.
16. Click **Finish** to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the number of STI sub-panels assigned. You can have a maximum of 16 STI sub-panels, 16 readers (1 reader per subpanel), 256 inputs (16 inputs per sub-panel), and 512 outputs (32 outputs per sub-panel).

9.11 Editing a Cardkey Logical Device

Logical Devices can be configured or edited after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices will already be configured. See Adding or Editing a Hardware Template, page 28.

Tip: It is a good idea to visit the Logical Device configuration tabs, as these tabs contain additional fields hardware templates do not.

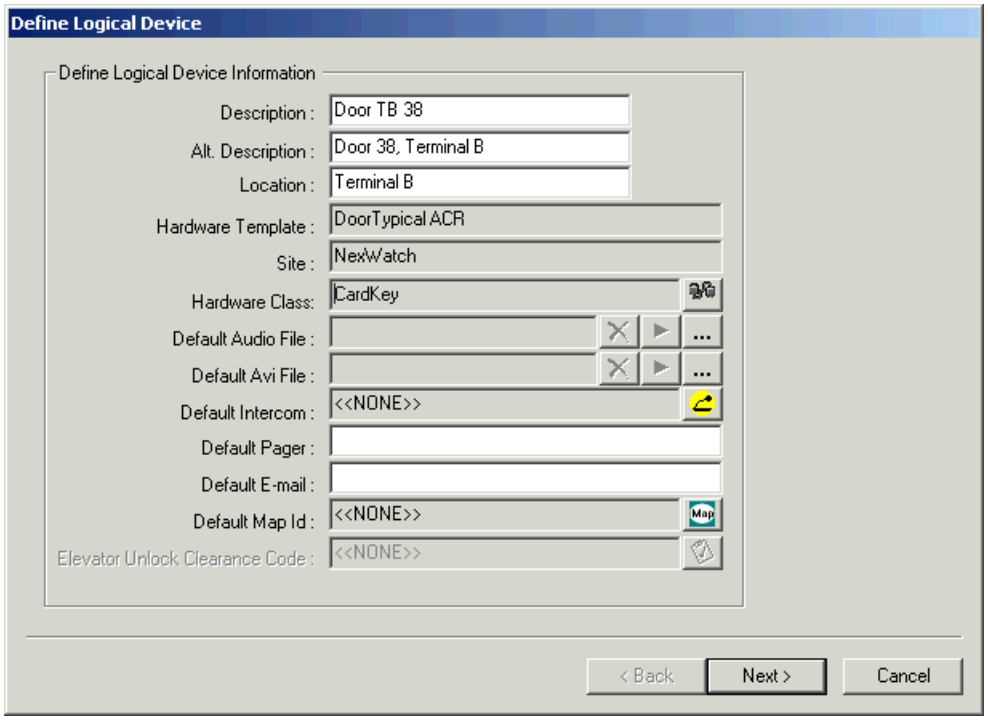
To configure a Logical Device:

1. Click the appropriate Logical Device folder in the Hardware Configuration screen to display the site's existing Logical Devices.
2. Right-click the Logical Device you want to configure, and select **Properties**. The Edit Logical Devices [Logical Device name] screen appears. The screen contains six information tabs. Complete the following information tabs to configure the Logical Device:

EDITING LOGICAL DEVICES TABS LIST

- Define Logical Device Tab.
- Logical Device Details Tab.
  - Readers
    - Reader Information Tab.
    - Configuration Tab.
    - Events Tab.
  - Input Points
    - Input Point Information Tab.
    - Configuration Tab.
    - Events Tab.
  - Output Points
    - Output Point Information Tab.
    - Configuration Tab.
    - Events Tab.
- Default CCTV Tab.
- Transactions Tab.
- Partitions Tab.

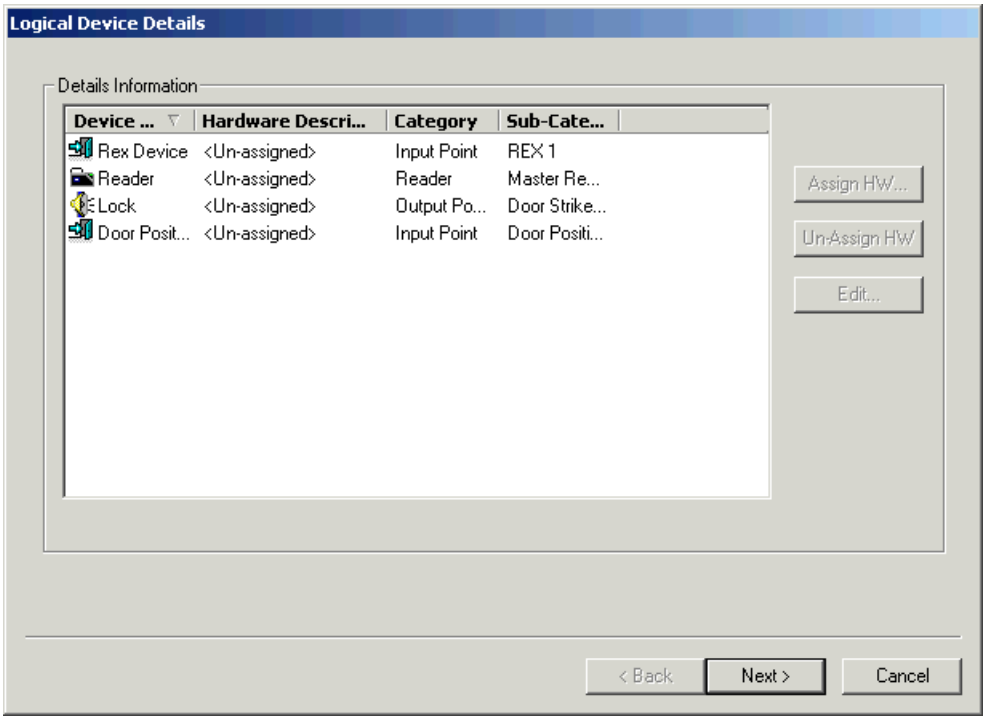
9.11.0.1 Define Logical Device Tab



Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.

Field	Description
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. For more information, see "DBC - Clearance Codes" in Chapter 37.

9.11.1 Logical Device Details Tab



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click **OK**.

To un-assign a device type:

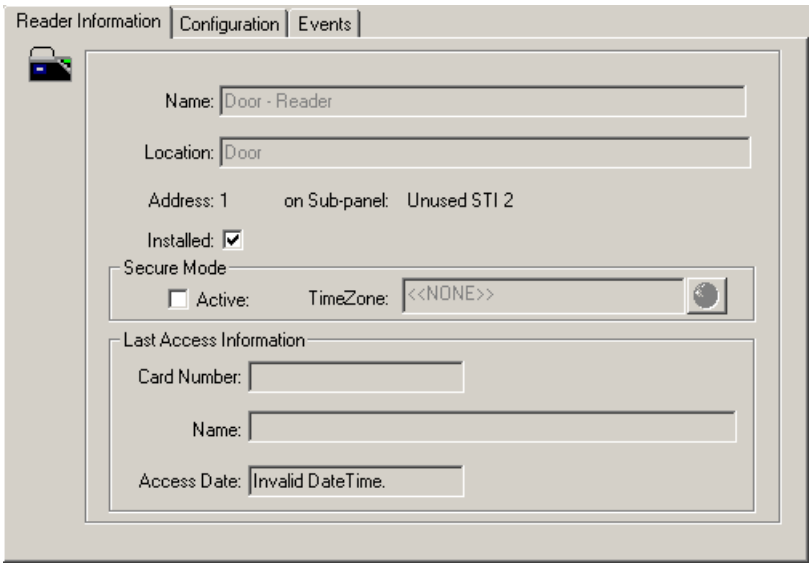
1. Click to select the device type and click **Un-Assign HW**.

To edit the current configuration of a device type:

1. Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete.
2. Use the appropriate section below to edit or configure the device type you have selected.

9.11.2 Readers

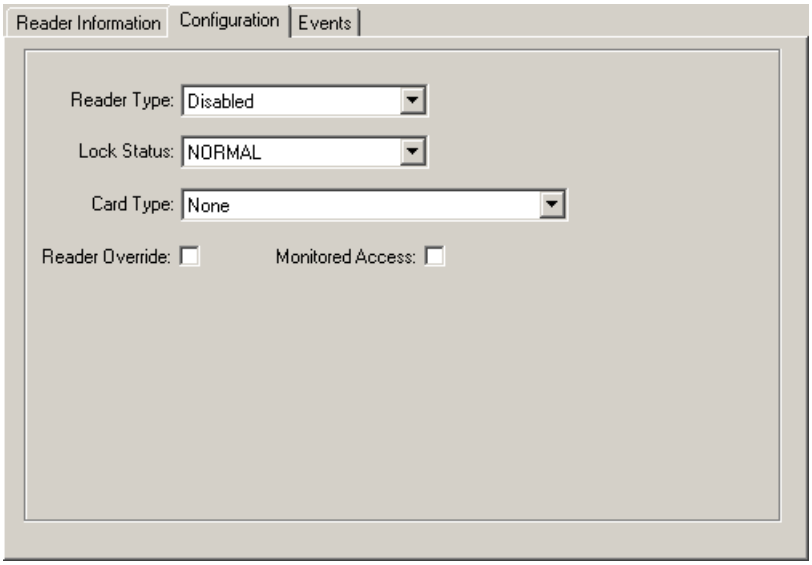
Reader Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.

Field	Description
Address_on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.
Installed	Required for the Logical Device to be enabled and operational.
Active (Secure Mode)	Enables secure mode for a particular door. See Appendix A, Secure Mode Verification.
Time Zone (Secure Mode)	Defines the time zone during which the reader is in secure mode.
Card Number (Last Access)	Identifies the card number which accessed the Logical Device last.
Name (Last Access)	Identifies the name of the badgeholder who last accessed the Logical Device.
Access Date	Identifies the date of last access.

Configuration Tab



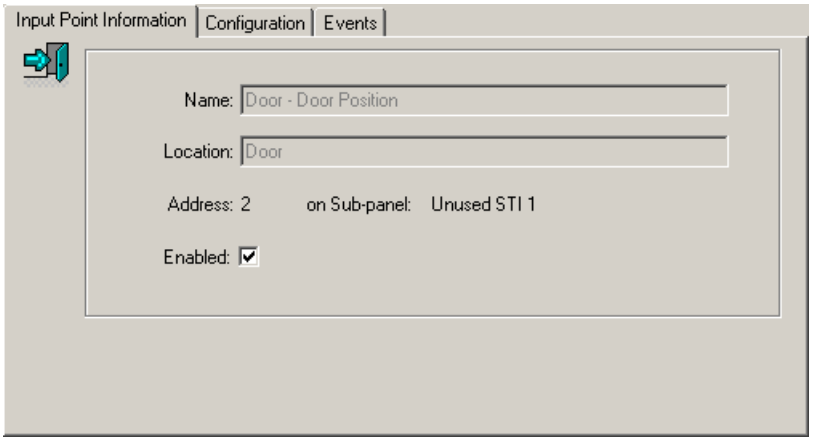
Field	Description
Reader Type	Defines the reader type (Disabled, Access, In In-X-It, Out In-X-It). In/Out In-X-It are used to designate the reader is part of an area, either as an in or an out reader. See "DBC - Area" in Chapter 29.
Lock Status	Defines the lock status of the reader. If the reader is locked, no cards gain access.
Card Type	Identifies the card type.
Reader Override	When enabled, the door remains unlocked indefinitely.
Monitored Access	Enables monitored access (card trace) on a reader.

Events Tab

To define an event, either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

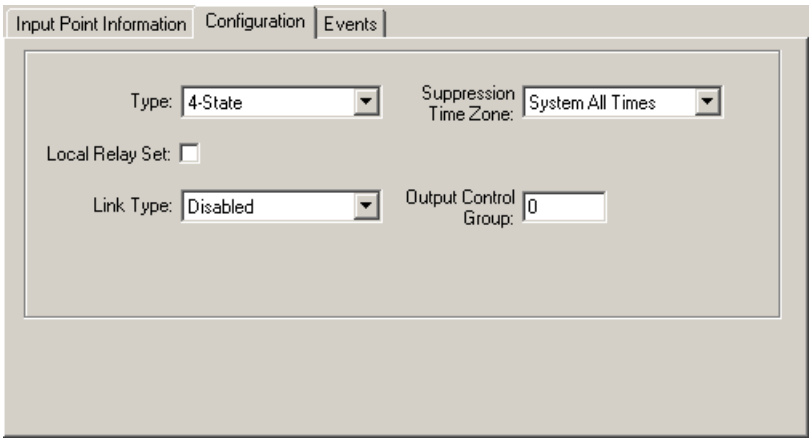
9.11.3 Input Points

Input Point Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.
Enabled	Required for the Logical Device to be operational.

Configuration Tab



Field	Description
Type	Defines the input type (2-State or 4-State).
Suppression Time Zone	Defines the time zone in which alarms associated with the input point are suppressed.
Local Relay Set	When enabled, upon the input point entering an alarm state, the panel relay activates. **Note:** This relay is the same relay as in Soft Alarms and Card Events.
Link Type (refers to output control group)	Defines the function of the associated output upon the input going into alarm. *Disabled* – The output point disables. *Active* – The output control group is activated when the input is in alarm. *Secure* – The output is not active when the input is secure (not in alarm). *Track* – The output is active when the input is in alarm but not in a trouble condition. *MIMIC* – The output is active when the input is in alarm, including a trouble condition. *Active Off* – The output is active when the input is secure (not in alarm). *Secure Off* – The output is inactive when the input is secure (not is alarm). *Reverse Trac* – The output is active when the input is secure; otherwise the output is inactive.

Field	Description
Output Control Group	Defines the output control group(1-600).

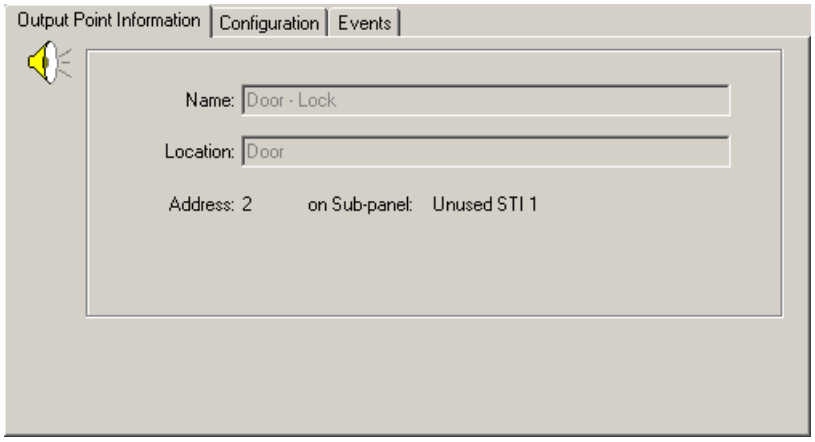
Events Tab

To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

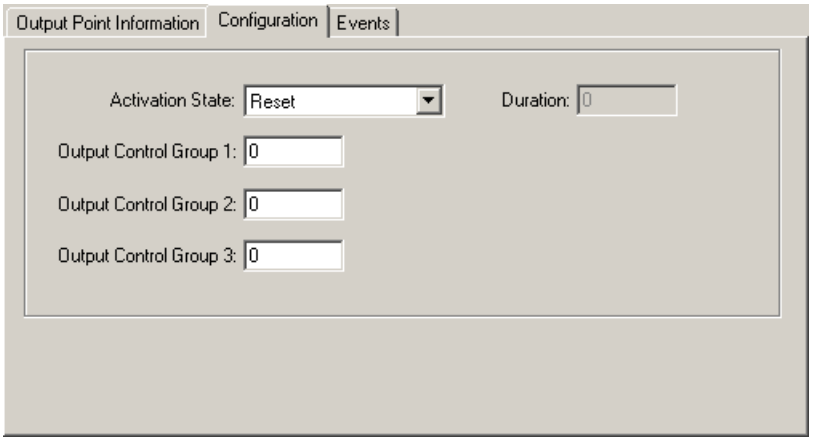
9.11.4 Output Points

Output Point Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_ on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.

Configuration Tab



Field	Description
Activation State	Defines the activation state of the output. When the output activate, this setting defines how the output is supposed to react. *Reset* - Turns the output off (inactive). *Set* - Turns the output on (activate). *Fast Flash* - Pulses the output every half second. *Slow Flash* - Pulses the output every second *Timed* - Pulses the output for a specified number of seconds up to 255 (defined in duration).
Duration	For a Timed activation state, specifies the number of seconds an output pulses.
Output Control Group 1	Designates the output is part of an output control group (1-600). An output can be a member of three groups.
Output Control Group 2	Designates the output is part of an output control group (1-600). An output can be a member of three groups.
Output Control Group 3	Designates the output is part of an output control group (1-600). An output can be a member of three groups.

Events Tab

To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

9.11.5 Default CCTV Tab

If you added Logical Devices that included CCTV, the CCTV information you configured already appears on this tab. Click the appropriate icons to select the default auto CCTV command, select CCTV view, and select CCTV command for this device.

9.11.6 Transactions Tab

The Transactions tab displays all the transactions that have occurred at that particular reader. The number of records also appears, and you can print the list of transactions.

9.11.7 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

To assign a partition to an existing Logical Device:

1. Click the Partitions tab.
2. Click **Add**.
3. Select an available partition.
4. Click **OK**. See "DBC - Partitions" in Chapter 53 for more information about defining partitions.

9.12 Viewing and Editing Dependencies of a Cardkey Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 53.

9.13 Deleting a Cardkey Logical Device

Please refer to How to Delete a Logical Device, page 53.

9.14 Cardkey Elevators

The Cardkey panels can support elevators. Elevators are controlled through card events. Therefore, Cardkey panels do not have the flexibility to support large multi-level buildings.

Note: It is recommended that you plan which output control groups will be used for the elevator controller before configuring elevators for Cardkey.

To configure elevators for the Cardkey panels:

Program the output points using output control groups. See Adding a Cardkey Logical Device.

The next step is to build card events within the channel. See the Adding a Cardkey Channel > Card Events tab.

Tip: You may add up to 20 card events.

To build card events within the channel:

1. In the Card Events tab:
   a. Select the **Output Control** check box.
   b. Select the **Activate** option button.
   c. Assign the Output Control Group number.
   d. Select the reader(s).
   e. Select the Trigger Type from the drop-down list.
      - Select Card Only if you do not want to require the cardholder to enter a PIN or an Event Code.
      - Select Card and PIN and Event Code if you want to require the cardholder to present the card, enter a PIN as well as enter an Event Code.
      - Select Card and Event Code if you want to require the cardholder to present a card and enter an event code.
2. If you require an event code, you must assign a code in the Access Code field. The terms Access Code and Event Code are used interchangeably.
3. Next, add the card events to the panel.

Note: Cardkey does not support the concept of floor-select. Both the STI and the Output Control Terminal (OCT) sub-panels can be used for elevator applications. The OCT sub-panel provide 32 outputs and is typically used for elevators.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - CHIP

10

In this chapter ...

Overview
Adding a CHIP Channel
Viewing and Editing Dependencies of a CHIP Channel
Deleting a CHIP Channel
Adding a CHIP Panel
Configuring a CHIP Panel
Editing a CHIP Panel
Viewing and Editing Dependencies of a CHIP Panel
Deleting a CHIP Panel
Adding a CHIP Logical Device
Editing a CHIP Logical Device
Viewing and Editing Dependencies of a CHIP Logical Device
Deleting a CHIP Logical Device
Star II (CHIP) Elevators

10.1 Overview

This chapter describes how to configure a site that uses a CHIP panel.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

10.2 Adding a CHIP Channel

The Pro-Watch channel is the communications path between the host and the panel. You must identify the channel before adding a panel and Logical Device.

To add a channel, complete the steps in the following sections.

Note: The recommended maximum number of channels per site is 99.

10.2.1 Select a CHIP Channel Type

1. In the Pro-Watch Hardware Configuration tree, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.
2. Select a CHIP channel type from the drop-down list.
3. Click **OK**. The Define Channel Information dialog box appears.

10.2.2 Define the CHIP Channel

1. In the Define Channel Information dialog box, enter an identifying channel description.
2. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
3. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.
4. In the Attempts field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.
5. In the Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds.
6. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.
7. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.

8. Click **Next** to display the Communications Parameters dialog box.

10.2.3 Set CHIP Communications Parameters

Follow these steps:

1. Select the port type from the following drop-down list options:

Option	Description
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. Com Port – The communication port on the host computer. Baud – The rate of communication between the host and the panel.
TCP/IP	Specifies that the channel is a network connection. IP Address – The IP address of the panel.
Dial Out	Defines a modem port as the primary mode of communication for the selected channel. Com Port – The communication port on the host computer. Baud – The rate of communication between the host and panel.
Dial In	Defines a modem port as the primary mode of communication for the selected channel. Com Port – The communication port on the host computer. Baud – The rate of communication between the host and the panel.
TCP/IP (Encrypted)	This functionality is provided by the network connection hardware. “TCP/IP encrypted” encrypts messages between the host and the panel. IP Address – The IP address of the panel. Encrypt Password – The password assigned.

Option	Description
Modem Pools	Modem pools are used for dial out. Modem Pool – Collection of modems. Baud – The rate of communication between the host and the panel. Flow Control – Starts and stops the transmission between the host and the panel.

2. Click **Next** to display the Channel Dialup dialog box. When choosing dial-up communication parameters, you must complete the settings within the channel dial-up box. See Appendix C, Dial-Up Configuration, for more information on configuring dial-up for the Star II (CHIP) panel.

Field	Description
Dialup Schedule	Determines how often you want to call the panel. Dial-up Schedules are configured in Database Configuration. See "DBC - Dial-Up Schedule" in Chapter 42 for more information.
Password	Specifies the password to the remote 'hub'.
Remote Site Phone Number	Defines the phone number for the remote site.
Host Phone Number	Defines the phone number for the host site.
Phone Host After # of Events	Initiates dial up after a specified number of events have occurred.
Serial Number	Specifies a number used for the panel driver's identification scheme. The serial number is automatically generated.
Dialup Retries	Defines the number of times the host attempts to dial up.
Site ID	This function is not currently supported.
Forcibly Disconnect After (minutes)	Defines the amount of time in minutes until the connection is forced to disconnect.
Disconnect After	Defines the amount of time in minutes until the connection is forced to disconnect.
Delay Connect Time	This function is currently not supported.

Field	Description
Delay Retry Time	This function is currently not supported.
Prefix	Defines the area code. Not applicable since the area code is usually included when the number is defined.
Modem Init String	Defines the initialization string to initialize the modem.

3. Click **Next** to display the Partitions dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.
4. Click **Finish** to complete the channel. A warning message appears reminding you that you must add the channel to the appropriate routing group before you can view any events using the channel.

It is recommended that you assign the channel to a routing group after you plan and configure routing groups. See "DBC - Routing Groups" in Chapter 55. Use this procedure to add a channel.

A Pro-Watch channel is the communications path between the Pro-Watch server and the panel. You must identify the channel before adding a panel and Logical Device.

10.3 Viewing and Editing Dependencies of a CHIP Channel

Please refer to How to View and Edit Dependencies of a Channel, page 51.

10.4 Deleting a CHIP Channel

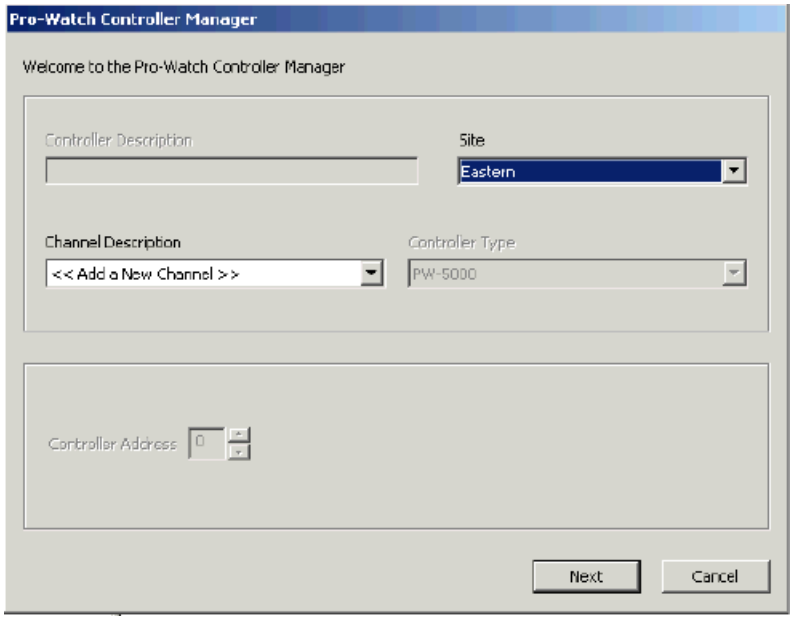
Please refer to How to Delete a Channel, page 51.

10.5 Adding a CHIP Panel

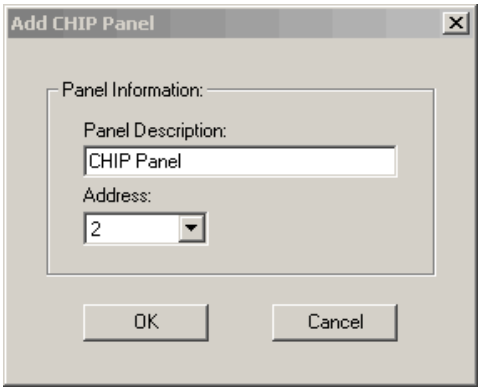
To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 4.

To add a panel:

1. In the Pro-Watch Hardware window, right-click the site you have created for this panel.
2. Select **New > Panel** to display the Pro-Watch Controller Manager dialog box.



3. Select a channel from the drop-down list in the Channel Description field, and click **Next**. The Add CHIP Panel dialog box appears.
4. In the Add CHIP Panel dialog box, enter the **Panel Description**.
5. Select the panel address from the drop-down list.



10.6 Configuring a CHIP Panel

In the panel tree view, you will see an on-board sub-panel, also called a MIRO (Monitorable Inputs and Relay Outputs). MIROs provide additional monitor inputs and relay outputs to a CHIP panel. MIRO expansion can consist of up to 16 units per panel with a maximum support for 255 monitor inputs and 96 relay outputs. There are various types of MIROs that

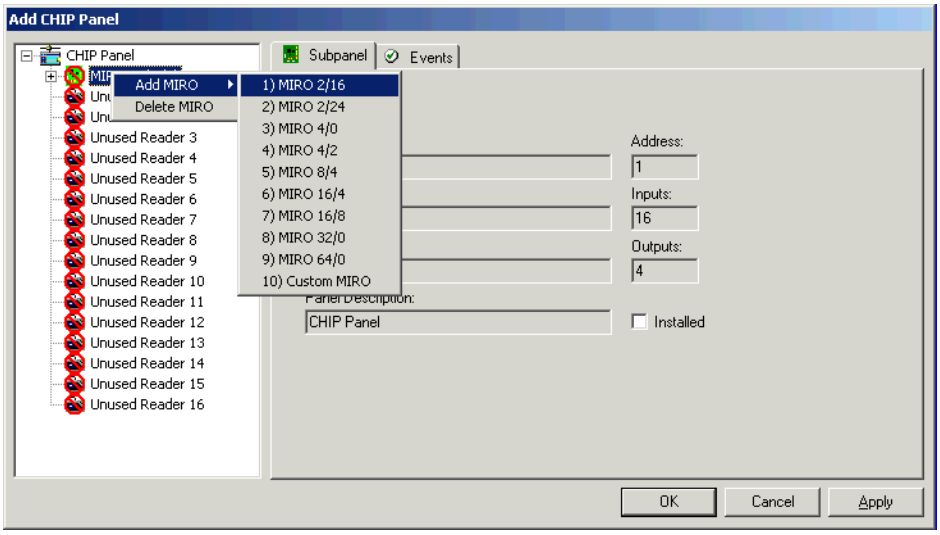
can be added to a CHIP panel. The table below lists the different varieties of MIRO boards available.

Sub-Panel	Inputs/Outputs
MIRO 16/4 (on-board MIRO)	16 monitor inputs/4 relay outputs.
MIRO 2/16	2 monitor inputs/16 relay outputs.
MIRO 2/24	2 monitor inputs/24 relay outputs.
MIRO 4/0	4 monitor inputs/0 relay outputs.
MIRO 4/2	4 monitor inputs/2 relay outputs.
MIRO 8/4	8 monitor inputs/4 relay outputs.
MIRO 16/4	16 monitor inputs/4 relay outputs.
MIRO 16/8	16 monitor inputs/8 relay outputs.
MIRO 32/0	32 monitor inputs/0 relay outputs.
MIRO 64/0	64 monitor inputs/0 relay outputs.
Custom MIRO	Custom configuration of a MIRO.

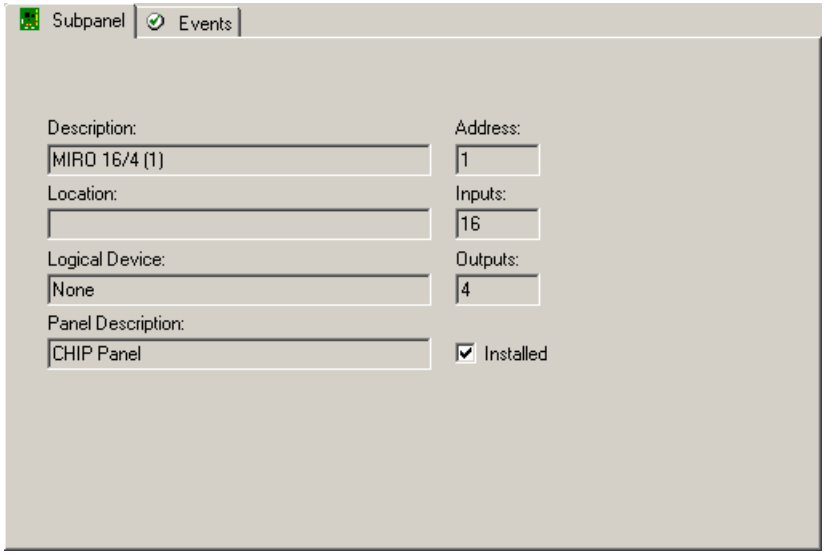
10.6.1 Adding a CHIP Panel

To add a MIRO board to a CHIP panel:

1. Select the on-board MIRO and right-click:



2. Select **Add MIRO** and then from the submenu select the MIRO type you want to add.
3. Select the address of the MIRO type from the drop-down list.
4. If you chose to create a Custom MIRO:
   a. Select the number of monitor inputs from the drop-down list.
   b. Select the number of relay outputs from the drop-down list.
   c. Select the address of the Custom MIRO from the drop-down list.
5. Install the MIRO:
   a. Select the MIRO.
   b. Select the **Installed** check box within the Sub-panel tab.



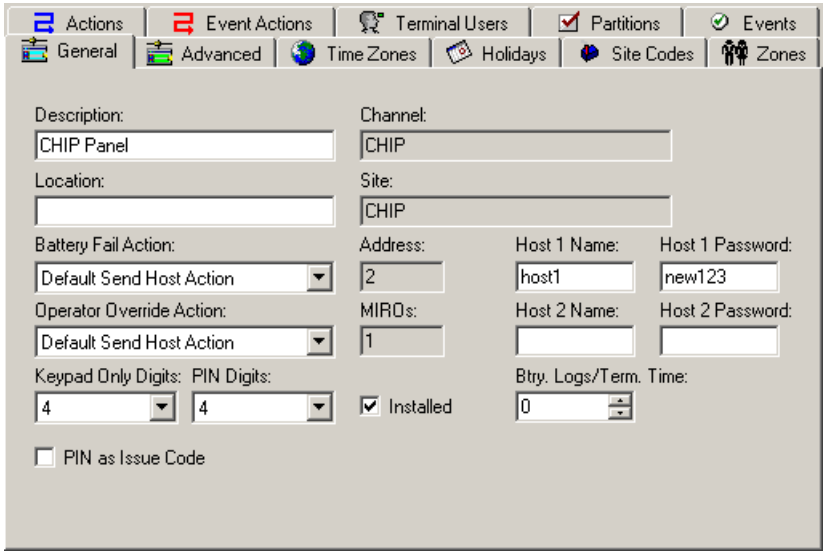
6. Repeat step 5 until all MIROs have been installed.
7. Click the **Events** tab. This tab displays the event types that you can define to support the MIRO board. To define an event, select the event type and click **Edit**. For more information, see "HW Config - Edit Point" in Chapter 25.
8. From the panel tree view, click the panel's icon to display the Add [panel name] Panel dialog box and the panel's configuration tabs. Complete each of the following tabs to configure the panel:

   ADD A CHIP PANEL TABS LIST

   - **"General Tab"**.
   - **"Advanced Tab"**.
   - **"Time Zones Tab"**.
   - **"Holidays Tab"**.
   - **"Site Codes Tab"**.
   - **"Zones Tab"**.
   - **"Actions Tab"**.
   - **"Event Actions Tab"**.
   - **"Terminal Users Tab"**.
   - **"Events Tab"**.
   - **"Partitions Tab"**.

General Tab

The General tab includes some basic hardware settings such as keypad or PIN settings for the reader, if applicable. The General tab also includes the ability to set actions. See "**Actions Tab**" below:



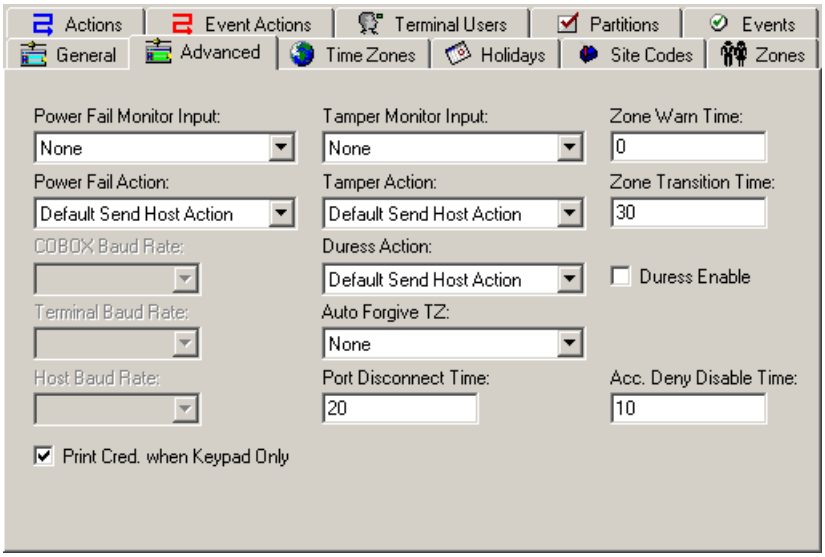
Use the following field descriptions to complete the General tab:

Field	Description
Description	Provides the description of the panel.
Location	Identifies the location of the panel.
Battery Fail Action	Defines the Action upon battery fail.
Operator Override Action	Defines the Action upon operator override.
Keypad Only Digits	Defines the number of keypad only digits (4-8).
PIN Digits	Defines the number of PIN digits used for both Keypads and Readers.
PIN as Issue Code	Enables the PIN to be used as an issue code.
Channel	Identifies the channel in which the panel is assigned to.
Site	Identifies the site in which the panel is assigned to.
Address	Identifies the address of the panel.
MIROs	Identifies the number of MIROs assigned.
Installed	Indicates that the panel is installed and operational.
Host 1 Name	Identifies the login name for the host to open the database to add or edit commands and download. This field can be edited but caution is encouraged.
Host 1 Password	Identifies the password for the host to open the database to add or edit commands and download. This field can be edited but caution is encouraged.
Host 2 Name	Identifies the second login name for the host to open the database to add or edit commands and download.
Host 2 Password	Identifies the second password for the host to open the database to add or edit commands and download.
Btry. Logs/Term. Time	Sets the interval for a battery status log to be sent to terminal.

Advanced Tab

The Advanced tab includes additional hardware settings to include assigning inputs and actions for those inputs. The first two inputs,

assigned from the on-board MIRO, are reserved for the Tamper and Power Fail. However, you can choose to assign the input points to alternative functions. You must first add and configure the input points. For more information, see "Adding a CHIP Logical Device".



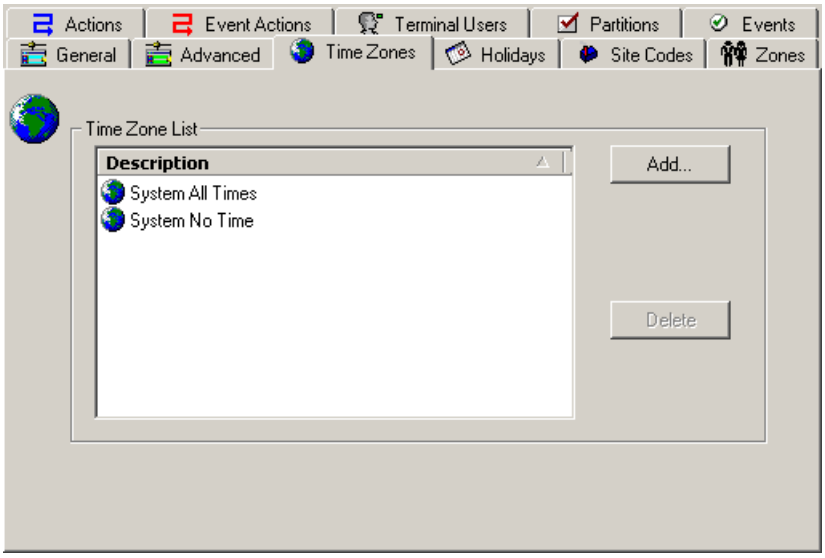
Use the following field descriptions to complete the Advanced tab:

Field	Description
Power Fail Monitor Input	Assigns an input point to power fail.
Power Fail Action	Defines the Action upon power fail.
Print Cred. When Keypad Only	Required on a keypad only reader to receive PIN numbers in the event viewer.
Tamper Monitor Input	Assigns an input point to tamper.
Tamper Action	Defines the Action upon panel tamper.
Duress Action	Defines the Action upon duress. The “Duress” functionality enables the user to trigger an alarm event in times of duress such as when the site is under attack or the operator is forced to grant access to an unauthorized user.
Auto Forgive TZ	Identifies the time zone in which anti-passback is forgiven for all cards. Doors must be part of an anti-passback configuration. See "DBC - Area" in Chapter 29.
Port Disconnect Time	Specifies the amount of time until terminal disconnects.
Zone Warn Time	Specifies the amount of time for the warning the zone is going to arm.
Zone Transition Time	Specifies the amount of time for transition from a disarmed zone to an armed zone.
Duress Enable	Enables duress. The “Duress” functionality enables the user to trigger an alarm event in times of duress such as when the site is under attack or the operator is forced to grant access to an unauthorized user.
Acc. Deny Disable Time	If an unknown card is presented to the reader; the reader will disable for the specifies amount of time; the reader will not read additional cards for that amount of time.

Time Zones Tab

The Time Zones tab enables you to add time zones to the panel; only times

zones that have been added to the panel are be available to configure applicable panel and reader fields.



To add a time zone to the panel:

1. Click **Add** to display the Select Time Zone dialog box.
2. Select the time zone.
3. Click **OK**.

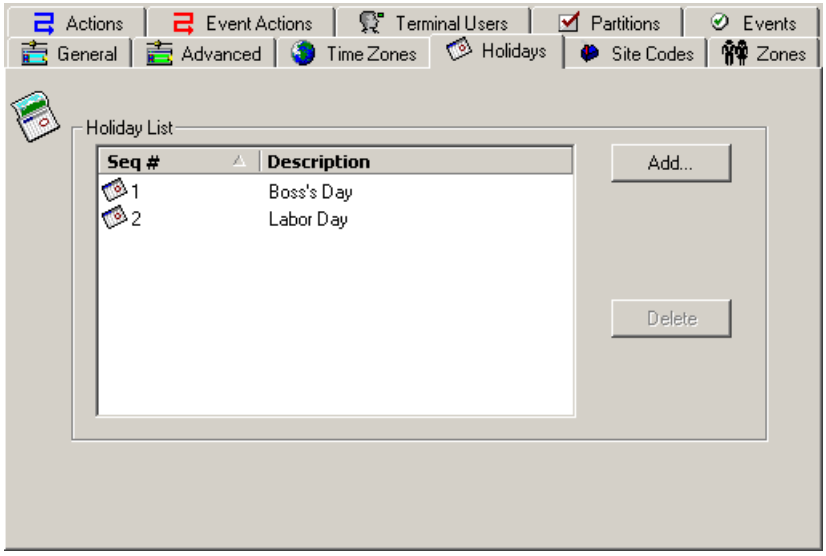
If the time zone you want does not appear in the dialog box you can create a new time zone.

To add a new time zone, click Add in the Select Time Zone dialog box. To complete adding a new Time Zone, see "DBC - Time Zones" in Chapter 57.

Holidays Tab

The Holidays tab enables you to edit normal Time Zone behavior on specific days. Holidays are assigned to time zones, therefore, enabling restricted access on specific holidays. The Star II panel accepts a maximum of 30 holidays. If a multi-day holiday exists, each day will be individually sent to the panel. For instance, a holiday with a duration of two days will

take two 'slots' in the panel and as a result you will only be able to add 28 more single day holidays.



To add a holiday to the panel:

1. Click **Add.**
2. Select the sequence number you want to assign to the holiday from the drop-down list.
3. Click the icon next to the Holiday field.
4. Click **Define**.
5. Select the holiday from the Holiday List dialog box and click **OK**.
6. Click **OK** again at the Select Holiday dialog box. If the holiday you want does not appear in the Holiday List dialog box you can create a new holiday.

To add a new holiday:

Click Add within the Holiday List dialog box.

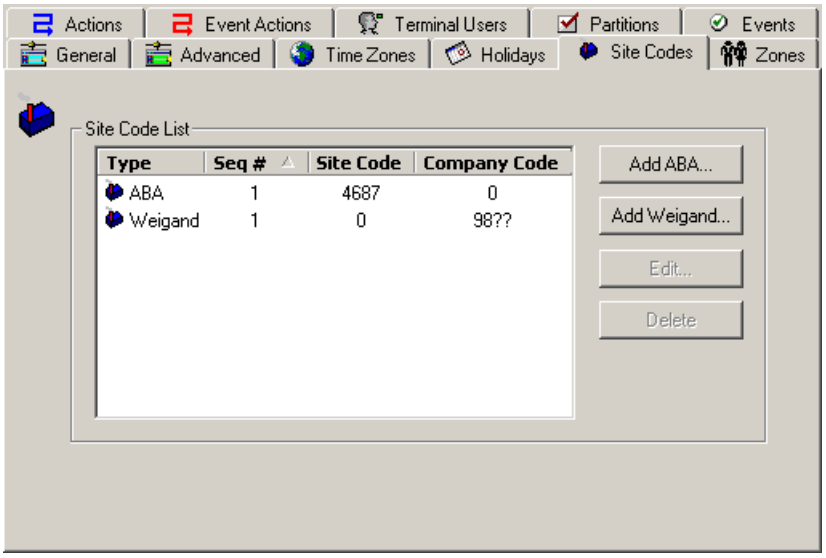
To complete adding a new holiday:

See "DBC - Holidays" in Chapter 49.

Site Codes Tab

Site Codes are optional characteristics of both ABA formatted Magstripe cards as well as cards using the Weigand Reader-to-Controller protocol.

The site code serves as a secondary ID beyond the card number. A Star II panel accepts a maximum of 64 site codes.



You can add two types of card formats to the panel: ABA and Weigand.

To add an ABA type card format to the panel:

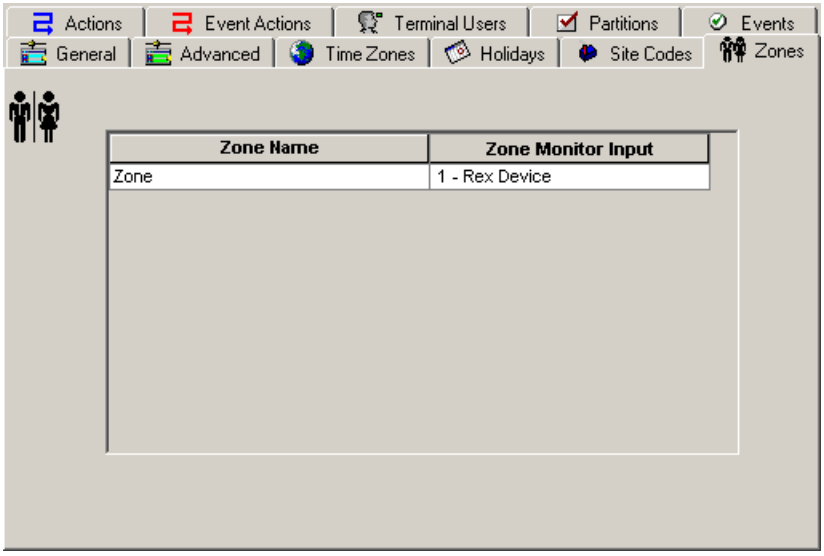
1. Click **Add ABA** to display the Add Site Code dialog box.
2. Select the site code address from the drop-down list.
3. Enter the site code. Use "?" for wildcard numbers. Site codes are coded to the card during manufacture.
4. Select the type of Card, ABA.
5. Enter the company code. Use "?" for wildcard numbers.
6. Click **OK.**

To add a Weigand type card format to the panel:

1. Click **Add Weigand** to display the Add Site Code dialog box.
2. Select the site code address from the drop-down list.
3. Enter the site code. Use "?" for wildcard numbers. Site codes are coded to the card during manufacture.
4. Select the type of Card, Weigand.
5. Enter the company code. Use "?" for wildcard numbers.
6. Click **OK.**

Zones Tab

Zones cannot be configured until you have added Logical Devices (inputs) as well as configured an area. See "DBC - Area" in Chapter 29. A CHIP panel can support up to 16 zones; the panel sets two zones by default.



Zones must be configured from the edit panel dialog box.

To edit a panel:

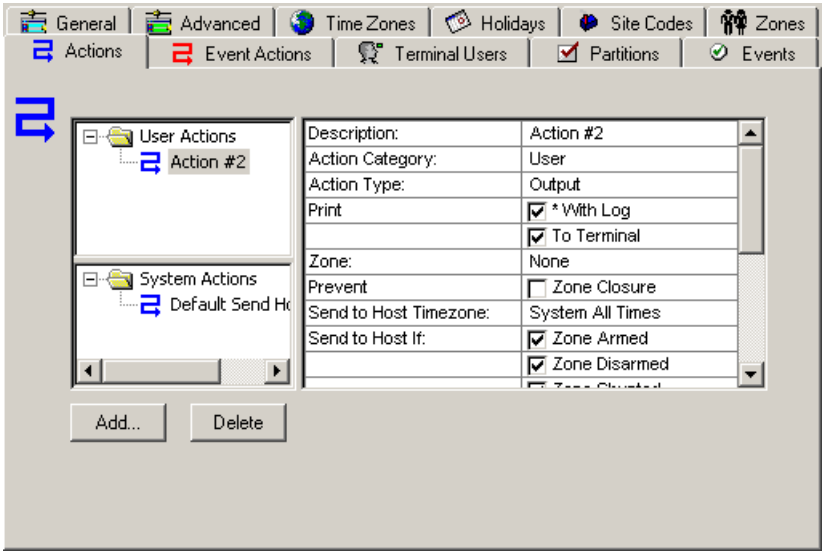
See "Editing a CHIP Panel".

To assign a Zone Monitor Input:

Select an input point from the drop-down list.

Actions Tab

The Actions tab displays the user and system actions. System actions are coded and cannot be edited or deleted.



To add a CHIP Action:

Click Add and use the following field definitions to set its parameters:

Field	Description
Description	The description of the action.
Action Category	Defines if it is a system or user action.
Action Type	Defines the action as an output or a sequence. Sequence must be set if configuring an event action.
Print	See Below.
* With Log	When enabled, places an asterisk in front of the log comment.
To Terminal	When enabled, sends the log to terminal.
Zone	Defines the zone (area).
Prevent (Zone Closure)	When enabled, prevents the zone from being armed.
Send to Host Time Zone	Defines the time zone in which the log is sent to the host.
Send To Host If	See Below.
Zone Armed	When enabled, logs are sent to the host when the zone is armed.
Zone Disarmed	When enabled, logs will be sent to the host when the zone is disarmed.
Zone Shunted	When enabled, logs are sent to the host when the zone is shunted or masked.
Zone Disabled	When enabled, logs are sent to the host when the zone is disabled.
Zone Monitor	When enabled, logs are sent to the host when the zone is monitored.
Output Point	Defines the output point for the action.
Close Output During	Defines the time zone in which the output is closed (activated) in the event the action occurs within that time zone.

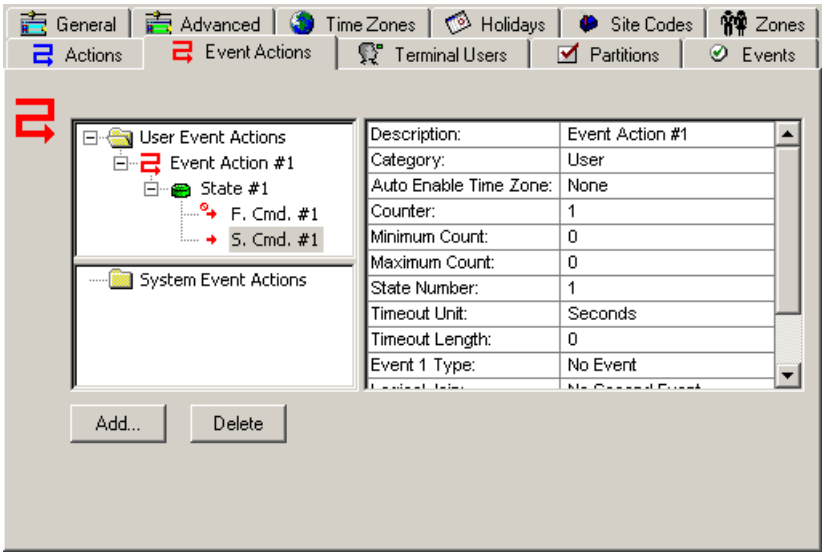
Field	Description
Close Output If	See Below.
Zone Armed.	Closes and activates the output point when the zone is armed.
Zone Disarmed	When enabled and when the zone is disarmed, the output closes (activate).
Zone Shunted	When enabled and when the zone is shunted or masked, the output closes (activate).
Zone Disabled	When enabled and when the zone is disabled, the output closes (activate).
Zone Monitor	When enabled and when the zone is monitored, the output closes (activate).

To delete a CHIP Action:

1. Select the action.
2. Click **Delete**.

Event Actions Tab

The Event Actions tab displays the user defined event actions. Event action sequences are used to supplement the method of fixed events and actions. This allows the system to be customized to fit a particular need.



Note: The tables presented below are for defining the field's functions and do not provide a valid event action example.

To add a CHIP Event Action:

1. Click **Add.**
2. Select **Add Action**. You can add a maximum of 64 Event Action**s.** Use the following field descriptions to set its parameters:

Field	Description
Description	The description of the event action.
Category	Defines the event action as system or user.
Auto Enable Time Zone	Defines the time zone in which the event action is valid regardless if the sequence action activates outside of that time zone.
Counter	There are 64 independent counters with 1 counter per event action up to 64 event actions. Counters do not need to be sequential but cannot be re-used. Not every event action needs a counter.
Minimum Count	When applicable, sets the baseline count the event action uses as a check to activate the event action.
Maximum Count	When applicable, sets the baseline count the event action uses as a check to perform an event action function.

To add a State to the Event Action:

1. Click **Add**.
2. Select **Add State**. You can add a maximum of eight States per Event Action. Use the following field descriptions to set its parameters:

Field	Description
State Number	Identifies the state number.
Timout Unit	Defines the unit of measurement for the time out length (Seconds or Minutes).
Timout Length	When applicable, defines the timeout duration for a specific event type within the state.
Event 1 Type	Defines the event type the event action is waiting to occur before the success commands initiate.

Field	Description
Logical Join	When applicable, can enable you to define an additional event type or to set the alternate event type in which the event action waits to occur before the success command initiates.
Event 2 Type	Defines the second event type the event action is waiting to occur before the success commands initiate. **Note:** This only applies if Logical Join is set to something other than 'None'.

To add a Success Command to the State:

1. Click **Add**.
2. Select **Add Success Command**. You can add a maximum of eight Success Commands per State. Use the following field descriptions to set its parameters:

Field	Description
Command Category	Defines the command category.
Command Number	Defines the command number. Does not need to be sequential. Success commands are initiated in the sequential order.
Command Type	Defines the command type that initiates upon the state event type being successful.

To add a Failure Command to the State:

1. Click **Add**.
2. Select **Add Failure Command**. You can add a maximum of four Failure Commands per State. Use the following field descriptions to set its parameters:

Field	Description
Command Category	Defines the command category.
Command Number	Defines the command number. Does not need to be sequential. Failure commands are initiated in the sequential order.
Command Type	Defines the command type that initiates upon the state event type being a failure.

Note: After creating the Event Action, you must set the action within reader or input/output point configuration. For more information, see "Adding a CHIP Logical Device".

To delete a CHIP Event Action:

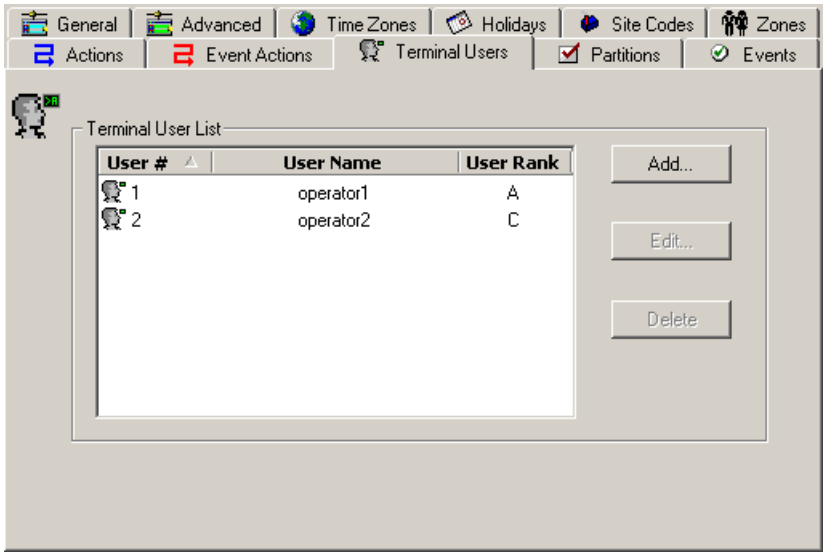
1. Select the Event Action.
2. Click **Delete**.

To delete a State, Success Command, or Failure Command:

1. Select the item and right-click.
2. Click **Delete**.

Terminal Users Tab

The Terminal Users tab allows you to give users terminal mode access for Star II.



To add a Terminal User:

1. Click **Add.**
2. Select the **User Number** from the drop-down list.
3. Enter the **User Name**.
4. Enter the **User Rank** [A-F]. The User Rank determines user access within Terminal (see your CHIP Panel manual for Terminal instructions), with rank A having the greatest access and rank F having the most restricted access.
5. Enter the **User Password** and click **OK.**

Events Tab

The Events tab displays the default event types that are applicable to the Star II panel.

To define an event:

Either double-click the event you want to define or select and click Edit. The Edit Point dialog box appears.

For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

Partitions Tab

Partitions determine the view of the resources within Pro-Watch. For information about creating a partition, see "DBC - Partitions" in Chapter 53. Use this function to assign or delete an already-created partition to the panel.

To assign a partition to the panel:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition and click **Add**.

To delete a partition from the Partitions List dialog box:

1. Select the partition.
2. Click **Delete**.

Note: After completing each tab within the panel, you will need to save the panel configuration.

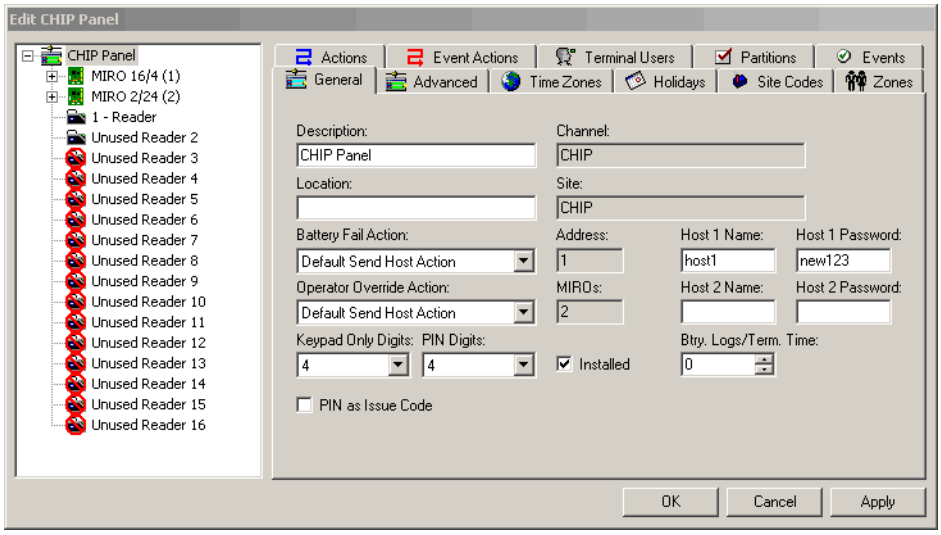
To save the panel configuration:

Click OK at the Add [Panel Name] Panel dialog box.

10.7 Editing a CHIP Panel

To edit a CHIP panel:

1. In the Pro-Watch Hardware Configuration tree view, click the site to which the panel is assigned.
2. Click the Panel's subdirectory. The icons of the existing panels appear in the right pane of the window.
3. Right-click the panel you want to edit.
4. Select **Properties**. The Edit [panel name] Panel dialog box appears.



5. Display the panel's configuration tabs by clicking the panel in the panel tree view list.
6. Complete each tab to configure the panel. See the following tab list and the corresponding tab sections in "Configuring a CHIP Panel" for the configuration information:

   EDIT A CHIP PANEL TABS LIST

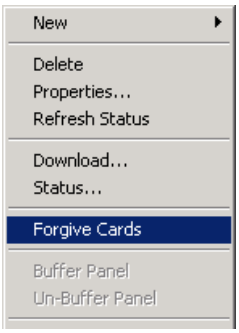
   - **"General Tab"**.
   - **"Advanced Tab"**.
   - **"Time Zones Tab"**.
   - **"Holidays Tab"**.
   - **"Site Codes Tab"**.
   - **"Zones Tab"**.
   - **"Actions Tab"**.
   - **"Event Actions Tab"**.

- **"Terminal Users Tab"**.
- **"Events Tab"**.
- **"Partitions Tab"**.

The Star II Panel allows you to forgive anti-passback (see "DBC - Area" in Chapter 29) for all cards.

To forgive anti-passback:

1. Select the panel from the Hardware Configuration window.
2. Right-click on the panel.
3. Select **Forgive Cards**:



10.8 Viewing and Editing Dependencies of a CHIP Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

10.9 Deleting a CHIP Panel

Please refer to How to Delete a Panel, page 53.

10.10 Adding a CHIP Logical Device

A Logical Device is a single physical device or group of selected physical devices, which are defined by a hardware template.

Examples:

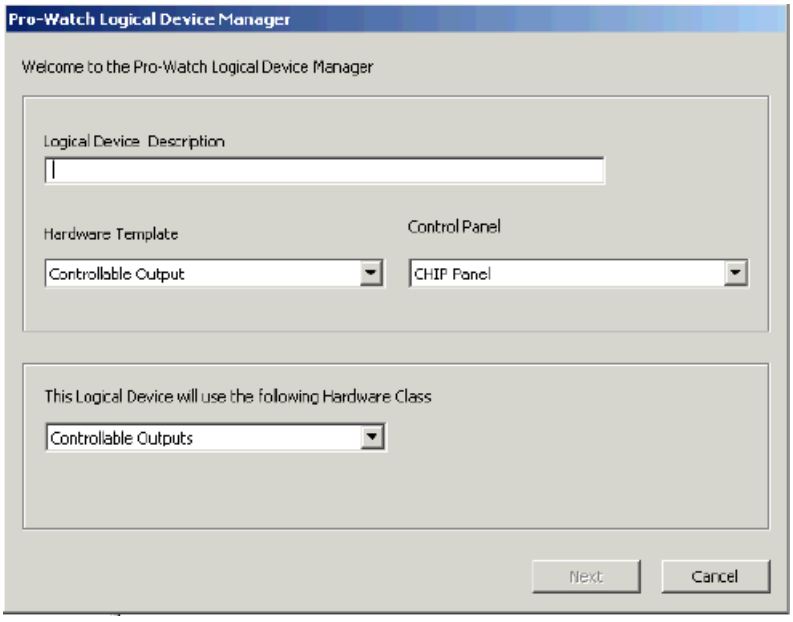
- A template may define a door that is equipped with a card reader, a REX input device, and a door strike output device as one Logical Device. As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system.
- You can assign the door, reader, input device, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you create Logical Devices, you must create the following:

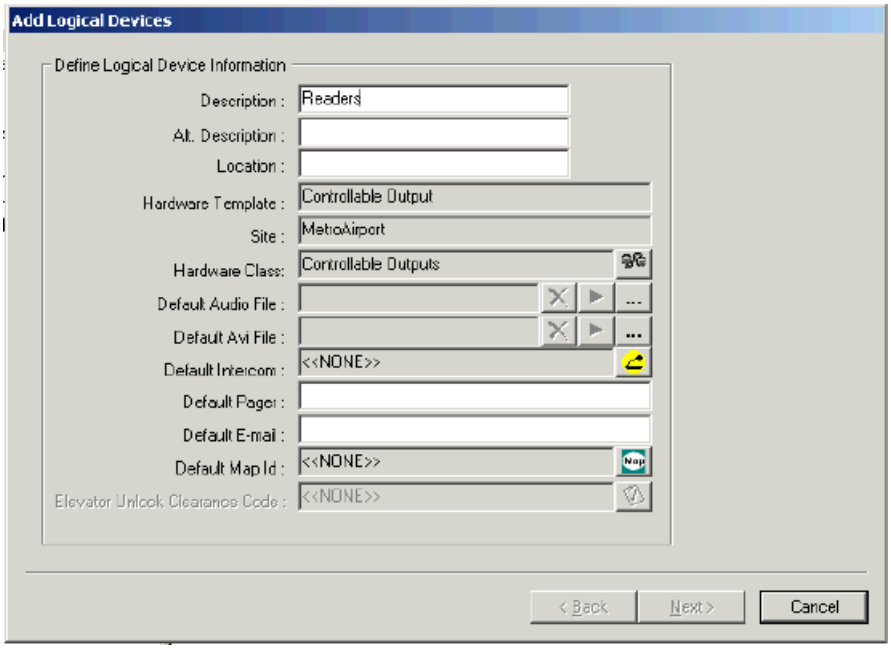
- Site. See "Adding a CHIP Channel".
- Channel. See "Adding a CHIP Channel".
- Panel. See "Adding a CHIP Panel".
- Hardware Template. See Adding or Editing a Hardware Template, page 28.

To add a Logical Device:

1. From the Pro-Watch Hardware Configuration tree view, right-click the site to which you want to assign the Logical Device, and select **New > Logical Device**. The Pro-Watch Logical Device Manager dialog box appears.



2. Enter a description that will identify the Logical Device in the Logical Device Description field.
3. Select a Hardware Template from the drop-down list in the Hardware Template field.
4. Select a Hardware Class from the drop-down list in the Hardware Class field.
5. Click **Next**. The Add Logical Devices dialog box appears.

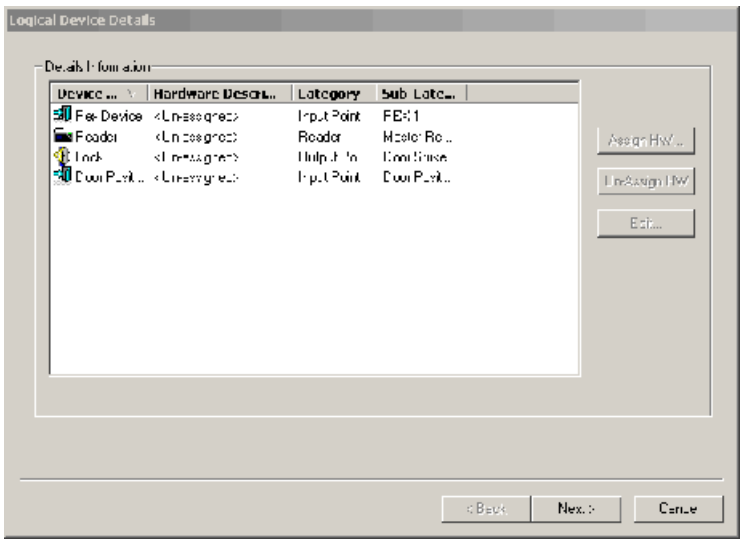


6. Use the following table to complete the Define Logical Device field entries:

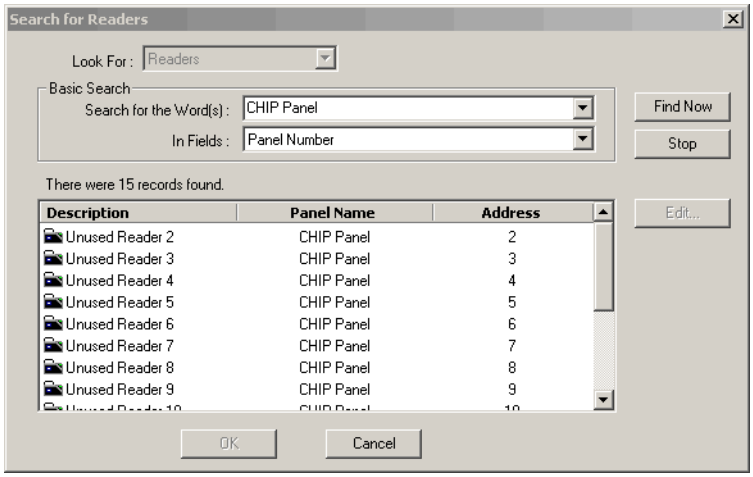
Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned.
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.

Field	Description
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. See "DBC - Clearance Codes" in Chapter 37for more information.

7. Click **Next**. The Logical Device Details dialog box appears.



8. Select the device type and click **Assign HW** to display the Search for [Device Type] dialog box.



9. Enter the description in the 'search for words' field; this is the description that will be used to search for available addresses.

10. Select the field name from the 'in fields' drop-down list and click **Find Now.**
11. Select the record and click **OK.**
12. Repeat step 5 through step 8 until all device types have been assigned.
13. Click **Next**. The Default CCTV Information dialog box appears.
14. CCTV may be associated with Logical Devices. You may assign the default view and commands for this device. See "HW Config - CCTV" in Chapter 21 for more information.
15. To assign a Default Command or View, click on the icon and select the command or view. Click **OK** and then click **Next**. The Partitions dialog box appears.
16. To assign a partition to this Logical Device, click **Add**, select the partition, and click **Add** again. For information about partitions, see "DBC - Partitions" in Chapter 53.
17. Click **Finish** to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the personality chip of the panel as well as the MIRO expansion. Star II (CHIP) personality chips include 2, 4, 8, and 16 doors. MIRO expansion can add up to 255 monitorable inputs and 96 relay outputs. Note that if you physically connect more devices to the panel than the panel's personality chip supports, those devices may appear in the Alarm Monitor status to be operative devices. However, they are not.

10.11 Editing a CHIP Logical Device

You can edit Logical Devices after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices will already be configured. See Adding or Editing a Hardware Template, page 28 for more information. However, it is a good idea to visit the Logical Device configuration tabs in this section, since these tabs contain field information that hardware templates do not.

To configure a Logical Device:

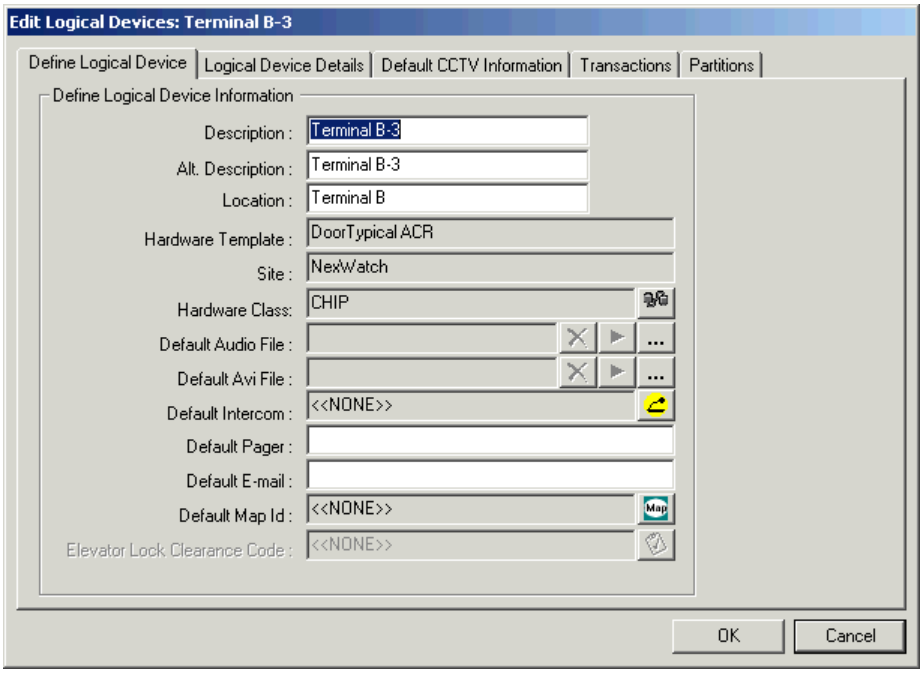
1. Right-click the Logical Device you want to configure or edit, and select **Properties**. The Edit Logical Devices: [Logical Device name] dialog box appears.
2. Complete each of the following tabs in the Edit Logical Devices dialog box to configure the device:

   EDIT A CHIP LOGICAL DEVICE TABS LIST

   - "Define Logical Device Tab".
   - "Logical Device Details Tab".
     - Reader Devices
       - **"Reader (General) Tab"**.
       - **"Reader (Advanced) Tab"**.
       - **"Keypad Tab"**.
       - **"S-Net/LED Tab"**.
       - **"Actions/Digital Tab"**.
       - **"Weigand/ABA Tab"**.
       - **"Weigand Raw Tab"**.
       - **"Events Tab"**.
     - Input Point Devices
       - "Input Tab".
       - **"Events Tab"**.
     - Output Point Devices
       - **"Output Tab"**.

* "**Events Tab**".

10.11.1 Define Logical Device Tab

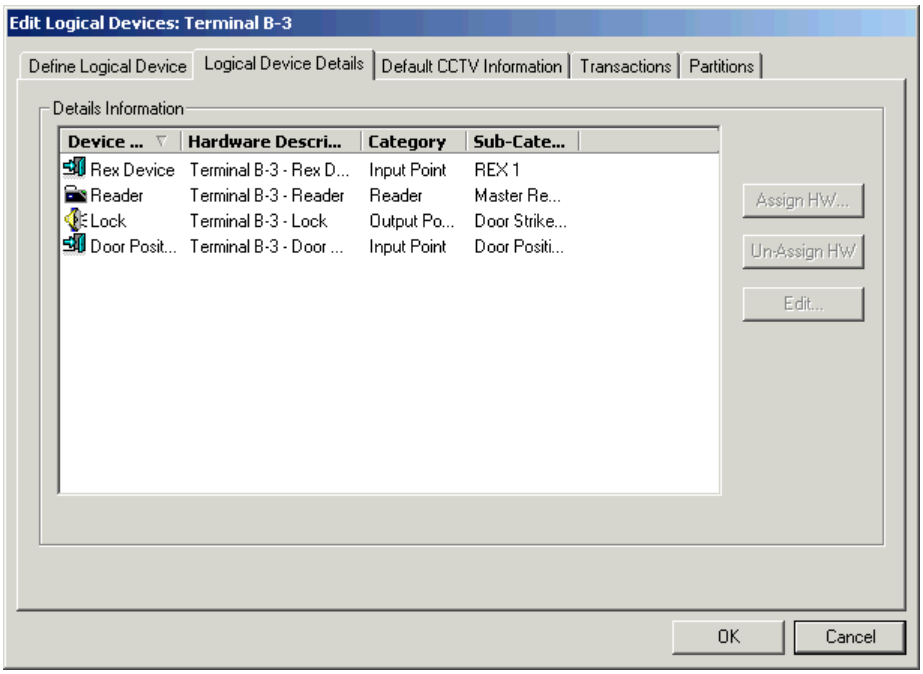


Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned.
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. See "DBC - Clearance Codes" in Chapter 37 for more information.

10.11.2 Logical Device Details Tab

This tab displays all of the device types included in the Logical Device. At

this tab you can assign, un-assign, or edit the device types.



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click **OK**.

To un-assign a device type:

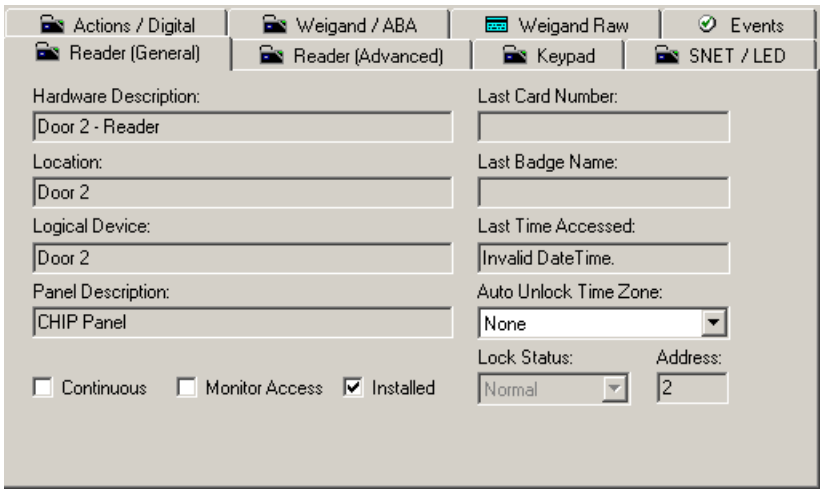
Click to select the device type and click Un-Assign HW.

To edit the current configuration of a device type:

1. Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete.
2. Use the appropriate table below to edit or configure the device type you have selected.

Reader Devices

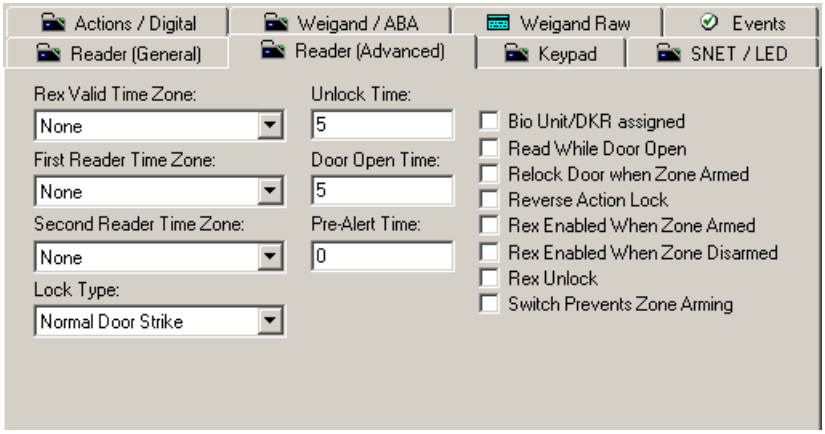
Reader (General) Tab



Field	Description
Hardware Description	The description of the Logical Device or reader.
Location	Identifies the physical location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel Description	Identifies the panel in which the Logical Device is assigned.
Continuous	When a card remains within the read range of the reader, the reader remains open.
Monitor Access	Enables monitored access (card trace) for the reader.
Installed	Required for the Logical Device to be enabled and operational.
Last Card Number	Identifies the last card number presented to the Logical Device.
Last Badge Name	Identifies the name of the badgeholder who last accessed the Logical Device.
Last Time Accessed	Identifies the last time the Logical Device was accessed.

Field	Description
Auto Unlock Time Zone	Identifies the time zone in which the Logical Device automatically unlocks.
Lock Status	Identifies the lock status of the Logical Device (Normal, Open, Locked).
Address	Identifies the address of the Logical Device.

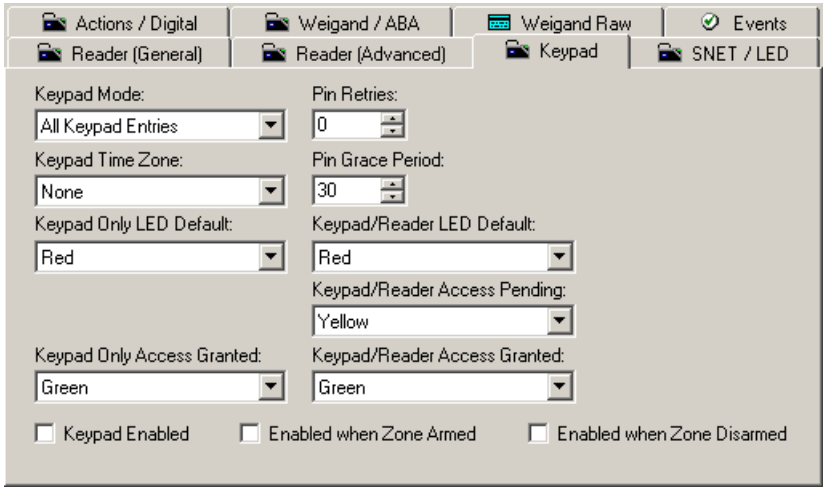
Reader (Advanced) Tab



Field	Description
REX Valid Time Zone	Identifies the time zone in which a REX is valid.
First Reader Time Zone	Identifies the time zone in which a reader is valid.
Second Reader Time Zone	Identifies the time zone in which the second reader with the same address is valid. You cannot have two of the same reader types with the same address. for MAG readers, you must set both time zones for a single reader.
Lock Type	Identifies the lock type of the door. Lock type affects the door only when a DPS is assigned.
Unlock Time	Defines the amount of time a door remains unlocked upon a valid card read.
Door Open Time	Defines the amount of time a door may remain open before sending an alarm.

Field	Description
Pre-Alert Time	Defines the amount of time a reader should 'beep' and 'blink' to indicate a door held open before sending an alarm.
Bio Unit/DKR Assigned	Required when a biometric unit is assigned to the panel. However, Pro-Watch does not support Bio Unit on a CHIP panel.
Read While Door Open	Enables the reader to continue to read cards while open.
Relock Door when Zone Armed	Enables a door re-lock when a zone (area) has been armed.
Reverse Action Lock	Acts as a fail-safe. In the event of a power failure, when enabled, the door is prevented from being locked.
REX Enabled when Zone Armed	Enables the REX when a zone (area) has been armed.
REX Enables when Zone Disarmed	Enables the REX when a zone (area) has been disarmed.
REX Unlock	When a REX is assigned, when enabled, requires the REX button to be pressed before the door unlocks.
Switch Prevents Zone Arming	When enabled, the DPS prevents the zone from arming.

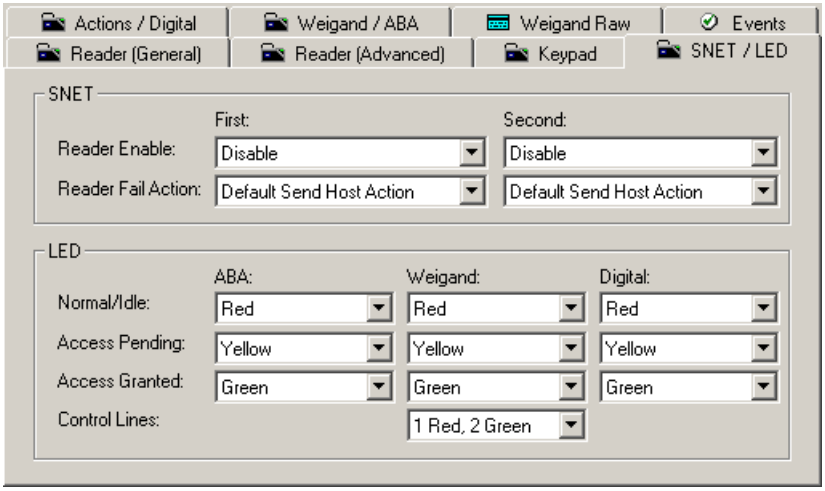
Keypad Tab



Field	Description
Keypad Mode	Defines the keypad mode. Currently, only “All Keypad Entries” is functional.
Keypad Time Zone	Identifies the time zone in which the keypad is active and required to gain access.
Keypad Only LED Default	Defines the default LED scheme for a keypad only reader.
Keypad Only Access Granted	Defines the default LED scheme for a keypad only reader in an access granted state.
PIN Retries	Defines the number of attempts to enter a correct PIN, in the event the first attempt was incorrect.
PIN Grace Period	Defines the amount of time allowed for a user to complete entry of a PIN number after the card swipe.
Keypad/Reader LED Default	Defines the default LED scheme for a keypad/reader.
Keypad/Reader Access Pending	Defines the default LED scheme for a keypad/reader in an access pending state.
Keypad/Reader Access Granted	Defines the default LED scheme for a keypad/reader in an access granted state.
Keypad Enabled	Required to enable a keypad and force its use to gain access during a specified time zone (See Keypad Time Zone above).

Field	Description
Enabled when Zone Armed	Enables a keypad when the zone is armed. Can be used instead of a time zone or in conjunction with a time zone.
Enabled when Zone Disarmed	Enables the keypad when the zone is disarmed. Can be used instead of a time zone or in conjunction with a time zone.

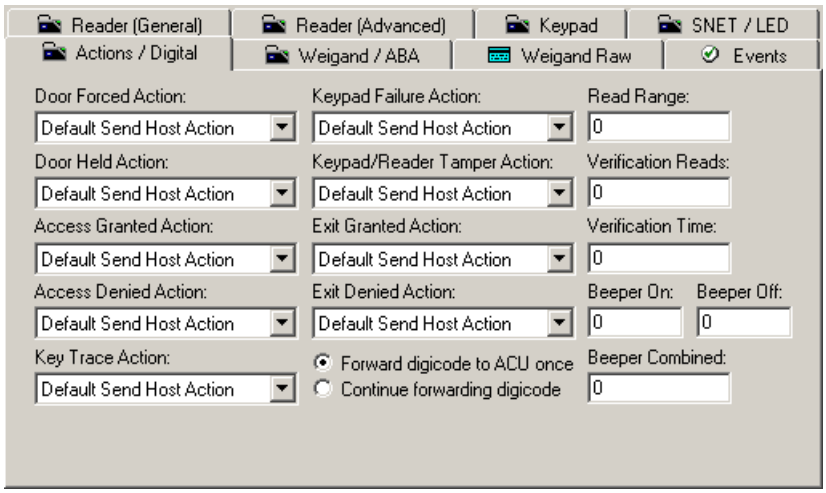
S-Net/LED Tab



Field	Description
First Reader Enable	Defines the reader type and enables the reader.
Second Reader Enable	Defines the reader type and enables the reader. The Star II panel allows for two different reader types to control a single door. When using a magstripe reader, both first and second reader fields must be defined for a single reader.
First Reader Fail Action	Defines the action upon first reader fail.
Second Reader Fail Action	Defines the action upon second reader fail.
Normal/Idle LED (ABA, Weigand, Digital)	Defines the LED scheme for a door in a normal state.

Field	Description
Access Pending (ABA, Weigand, Digital)	Defines the LED scheme for a door in an access pending state.
Access Granted (ABA, Weigand, Digital)	Defines the LED scheme for a door in an access granted state.
Control Lines (Weigand)	Defines the control lines for a Weigand reader. A Weigand reader may be wired to control the auxiliary function such as a buzzer or tri-state LED.

Actions/Digital Tab

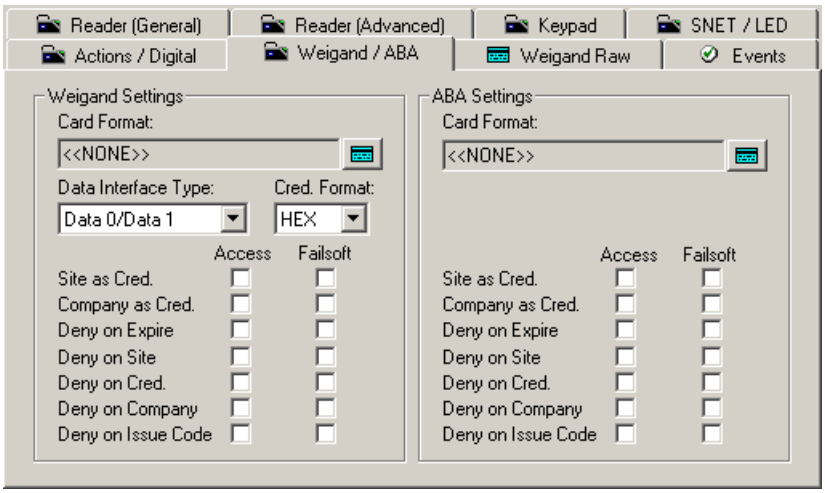


Field...	Description...
Door Forced Action	Defines the action upon a forced door.
Door Held Action	Defines the action upon a door held.
Access Granted Action	Defines the action upon an access granted.
Access Denied Action	Defines the action upon an access denied.
Key Trace Action	Defines the action upon a key trace.
Keypad Failure Action	Defines the action upon a keypad failure.

Field...	Description...
Keypad/Reader Tamper Action	Defines the action upon a keypad/reader tamper.
Exit Granted Action	Defines the action upon an exit granted.
Exit Denied Action	Defines the action upon an exit denied.
Forward Digicode to ACU Once	Allows for messages originating from the reader to be sent to the ACU only once. This is the recommended setting.
Continue Forwarding Digicode	Allows for messages originating from the reader to be sent to the ACU continuously. This setting is not recommended.
Read Range	Defines the read range or allowable distance between a card and a reader in order for the reader to be able to recognize the card. The read range is between 1-255 where 253 is the strongest and 254/255 is reserved for Power Switching Modes used for DuraKey. The read range can be lowered to account for RF interference.
Verification Reads	Defines the amount of times a card must be read before forwarding the request to the host. DKR readers only.
Verification Time (ms)	Defines the amount of time a card must be out of the read range before it can be read again.
Beeper On	Defines the length of time a beeper pulses (beep).
Beeper Off	Defines the length of time for silence after a beeper has pulsed.
Beeper Combined	Determines how many times the cycle (on/off) repeats.

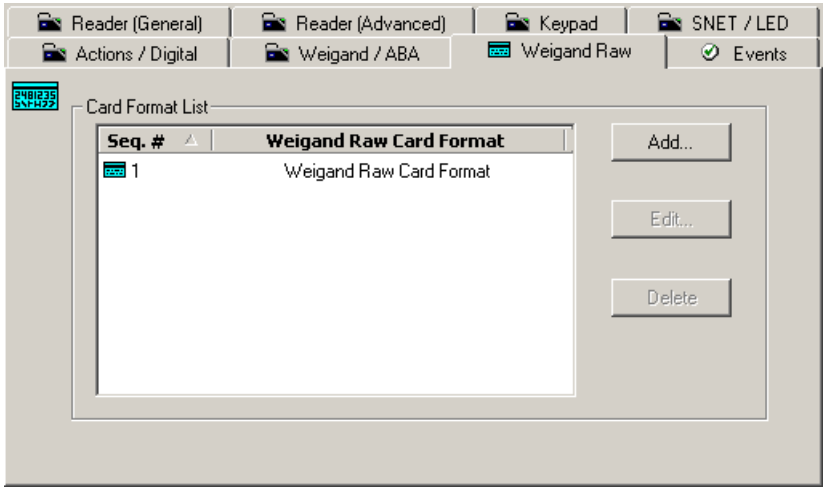
Weigand/ABA Tab

(Return to "EDIT A CHIP LOGICAL DEVICE TABS LIST")



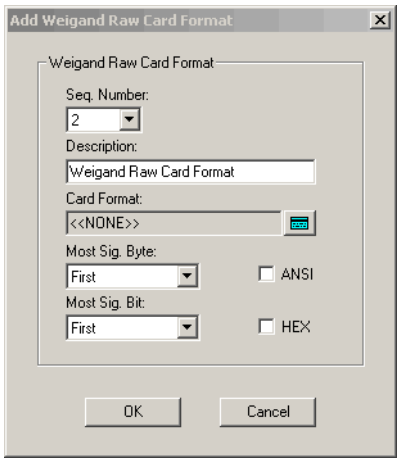
Field	Description
Card Format	Defines the Weigand or ABA card format type.
Data Interface Type	Defines the data interface (i.e. Data 0/Data 1 or Clock/Data).
Cred. Format	Defines the credential format (i.e. Hexadecimal or Binary Coded Decimal).
Site as Cred.	Allows for the site code to be used as the card number. Set as access and failsoft.
Company as Cred.	Allows for the company code to be used as the card number. Set as access and failsoft.
Deny on Expire	Prevents cards from gaining access with an expired expiration date.
Deny on Site	Allows the card's site code to be used as part of the access decision.
Deny on Cred.	Allows the card's number to be used as part of the access decision.
Deny on Company	Allows the card's company code to be used as part of the access decision.
Deny on Issue Code	Allows the card's issue code to be used as part of the access decision.

Weigand Raw Tab



To add a Weigand Raw card format:

1. Click **Add** to display the Add Wiegand Raw Card format dialog box:



2. Use the table below to complete the Weigand Raw Card Format dialog box:

Field	Description
Seq. Number	Defines the sequence number for the card format.
Description	The description for the card format as defined by the user.

Field	Description
Card Format	Defines the Weigand card format. For more information on configuring card formats, see "DBC - Card Formats" in Chapter 35.
Most Sig. Byte	Defines the most significant byte in the card format for data encryption purposes.
ANSI	Defines if the data format conforms to ANSI standard.
Most Sig. Bit	Defines the most significant bit in the card format for encryption purposes.
HEX	Defines if the data format is in Hexadecimal format instead of Binary.

Events Tab

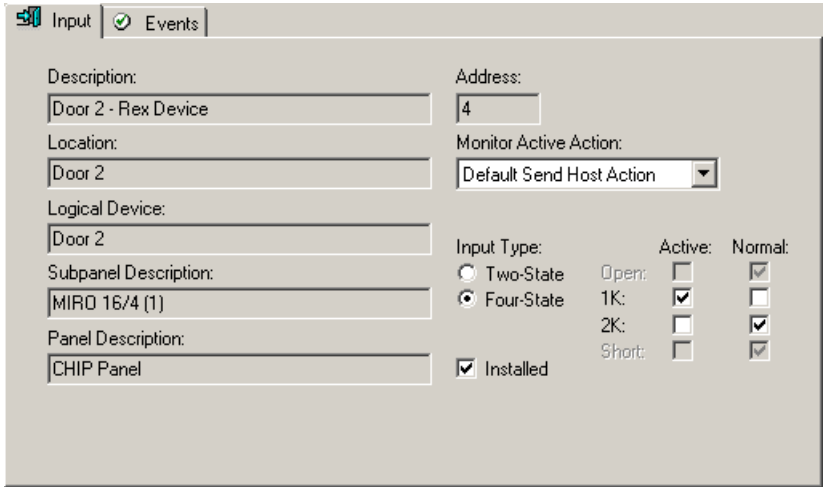
To define an event, follow these steps:

Either double-click the event you want to define or select and click Edit. The Edit Point dialog box appears.

For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

10.11.2.1 Input Devices

Input Tab



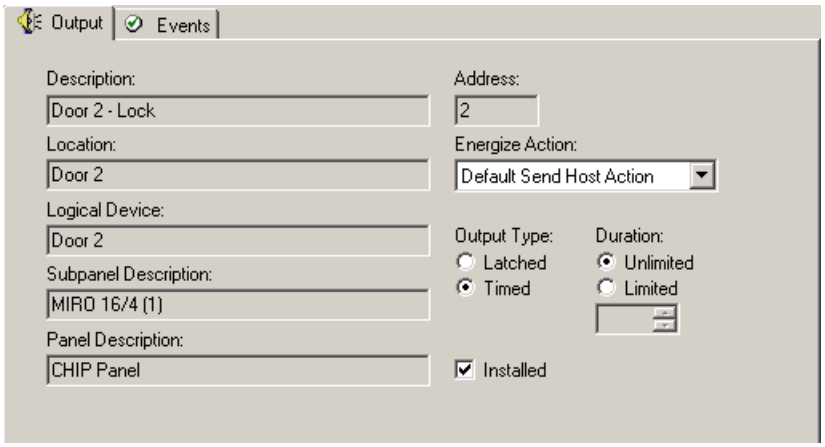
Field	Description
Description	Provides the description of the input point.
Location	Identifies the location of the input point as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Sub-Panel Description	Identifies the sub-panel in which the input point is assigned.
Panel Description	Identifies the panel in which the input point is assigned.
Address	Identifies the address of the input point.
Monitor Active Action	Identifies the action for monitor active.
Two State Input Type	Defines the input type as Two State (Active or Normal).
Four State Input Type	Defines the input type as Four State (Active, Normal, Open, or Short).
Installed	Required for the input point to be enabled and operational.

Events Tab

To define an event, either double-click the event you want to define or select and click Edit. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

10.11.3 Output Devices

Output Tab



Field	Description
Description	Provides the description of the output point.
Location	Identifies the location of the output point as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Sub-Panel Description	Identifies the sub-panel in which the output point is assigned.
Panel Description	Identifies the panel in which the output point is assigned.
Address	Identifies the address of the output point.
Energize Action	Defines the action upon the output energizing.
Timed Output Type	Designates the output type as timed.
Latched Output Type	Designates the output type as latched. A latched relay closes when triggered and remain closed until another event or an operator override commands it to open, unless the relay is used as a door lock.

Field	Description
Unlimited Duration	If the timed output type is set to unlimited, it follows the duration of the triggering event.
Limited Duration	If the timed output type is set to limited, the relay can be closed for a designated amount of time.
Installed	Required for the output point to be enabled and operational.

Events Tab

To define an event:

1. Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.
2. Click the **Default CCTV Information** tab. The default CCTV information was configured while adding Logical Devices, if the Logical Devices included CCTV information.
3. Click the **Transactions** tab. The Transactions tab displays all the transactions that have occurred at that particular reader. The number of records will also be displayed. The option to print transactions is also available.
4. Click the **Partitions** tab. To complete configuration, see "DBC - Partitions" in Chapter 53.

10.12 Viewing and Editing Dependencies of a CHIP Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 53.

10.13 Deleting a CHIP Logical Device

Please refer to How to Delete a Logical Device, page 53.

10.14 Star II (CHIP) Elevators

The Star II panel supports elevator configuration. A maximum of 96 floors may be assigned. Both elevator readers and elevator floor select readers are supported.

To configure elevators using the elevator reader device type:

1. Configure the hardware template. See Adding or Editing a Hardware Template, page 28.
   a. In the Device Types tab of the hardware template, you must add one reader and an output for each floor up to 96 floors.
   b. Configure the elevator reader device type and each output device type.
2. After configuring the hardware template, you must add the Logical Device to the panel. See "Adding a CHIP Logical Device". You do not need to assign and address each output sequentially. Note that elevator readers control access to floors and do not record which floor the user chose.

To configure elevators using the elevator reader (floor select) device type:

1. Configure the hardware template. See Adding or Editing a Hardware Template, page 28.
   a. In the Device Types tab of the hardware template, you must add one reader as well as one output and one input for each floor up to 96 floors.
   b. Configure the elevator reader device type, each output device type, and each input device type.
2. After configuring the hardware template, you must add the Logical Device to the panel. See "Adding a CHIP Logical Device". You do not need to assign and address each output and input sequentially. Note that elevator readers (floor select) control access to floors and record which floor the user chose.

10.14.1 Known STAR II Issue

When a STAR II door is time masked, the panel does not issue a “door open” alarm event if the door is open at the time the mask expires.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Matrix

11

In this chapter ...

Overview
Adding a Matrix Channel
Viewing and Editing Dependencies of a Matrix Channel
Deleting a Matrix Channel
Adding a Matrix Panel
Viewing and Editing Dependencies of a Matrix Panel
Deleting a Matrix Channel
Adding a Matrix Logical Device
Configuring a Matrix Logical Device
Viewing and Editing Dependencies of a Matrix Logical Device
Deleting a Matrix Logical Device

11.1 Overview

This chapter describes how to configure a site that uses a Matrix panel.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

11.2 Adding a Matrix Channel

Note: The recommended maximum number of channels per site is 99.

The Pro-Watch channel is the communications path between the host and the panel. You must identify the channel before adding a panel and Logical Device.

To add a channel:

1. Select a channel type:
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created.
   b. Select **New > Channel**. The Create a Channel dialog box appears.
   c. Select "Matrix" from the drop-down list.
   d. Click **OK**. The Define Channel Information dialog box appears.
2. Define the channel:
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
   c. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.
   d. In the Attempts field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.
   e. In the Poll Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds. Note that the minimum interval in a PW-5000 networked configuration is 300 milliseconds, even if you should enter a smaller number.
   f. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.
   g. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.
   h. Click **Next** to display the Communications Parameters dialog box.

3. Set the communications parameters:

   a. Select the port type from the following drop-down list options:

Option	Comments
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
TCP/IP	Specifies that the channel is a network connection. IP Address – the IP address of the panel.
Dial Out	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
Dial In	Defines a modem port as the primary mode of communication for the selected channel. Com Port – the communication port on the host computer. Baud – the rate of communication between the host and the panel.
Modem Pools	Modem pools are used for dial out. Model Pool – collection of modems. Baud – the rate of communication between the host and the panel. Flow Control – starts and stops transmission between the host and the panel.
Secondary Channel	Acts as a fail-safe; secondary channel communication comes online if the primary channel communication breaks.

   b. Click **Next** to display the Partitions dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.

   c. Click **Finish** to complete the channel. A warning message appears reminding you that you must add the channel to the appropriate routing group before you can view any events using the channel. It

is recommended that you assign the channel to a routing group after you plan and configure routing groups. For more information, see "DBC - Routing Groups" in Chapter 55.

11.3 Viewing and Editing Dependencies of a Matrix Channel

Use this function to view and modify the Channel's dependencies. The Channel object depends upon the Site and Routing Group objects.

To view and modify a Channel's dependencies:

1. Right-click the icon of an existing Channel in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Channel's dependencies.
2. To modify or remove the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

11.4 Deleting a Matrix Channel

Use this function to delete a Matrix channel from the Pro-Watch database.

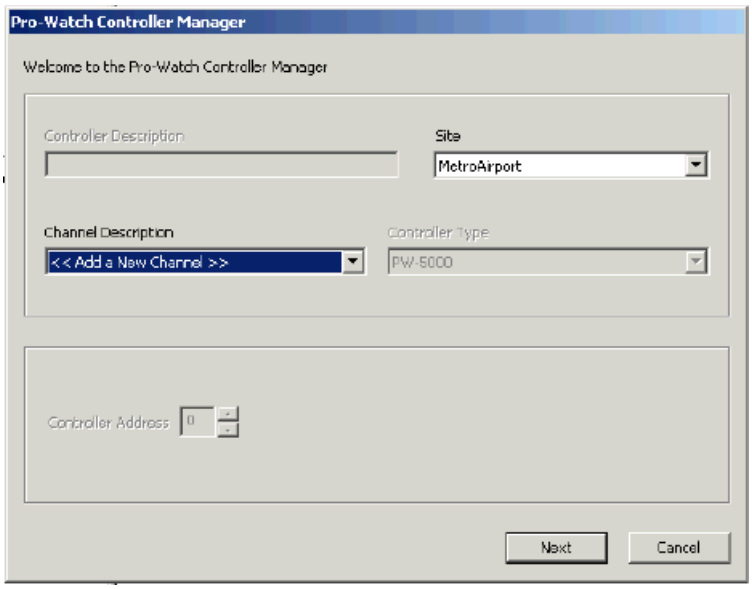
1. In the Pro-Watch Hardware Configuration tree list, click **Channels** to display the Channel icons in the right pane.
2. Right-click the Channel you want to delete and select **Delete**. Note that you cannot delete a Channel that has dependencies. A dependency is another database object that includes the Channel in its configuration. The Channel object depends upon the Site and Routing Group objects. If the Channel has no current dependencies, you are prompted to confirm the deletion. However, if the Channel does have current dependencies, the Dependencies dialog box appears.
3. If you still want to delete the Channel:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
4. Repeat step 2 and click **Yes** at the prompt to delete the channel.

11.5 Adding a Matrix Panel

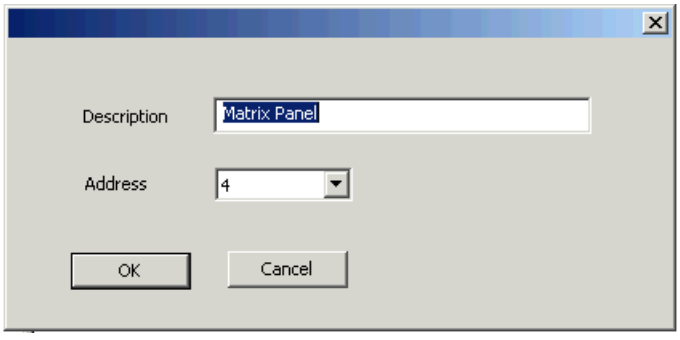
To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 4.

To add a Matrix panel:

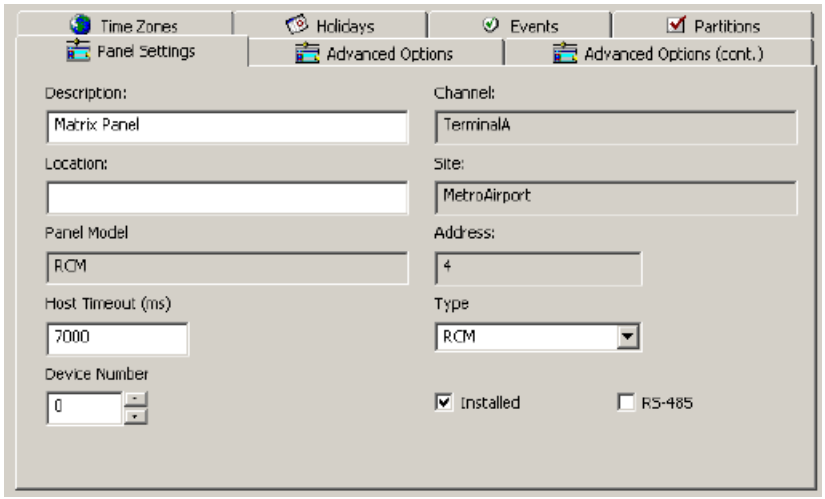
1. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
2. Select **New > Panel** to display the Pro-Watch Controller Manager dialog box.



3. Select the channel you have created for this panel from the drop-down list and click **Next**. The following dialog box appears:



4. Click **OK** to display the Add Matrix Panel dialog box, which contains the following tabs:



5. Use the field descriptions given in the following sections for each tab in the Add Matrix Panel dialog box to complete the Matrix panel configuration.

11.5.1 Panel Settings Tab

Field	Description
Description	Provides a description of the panel.
Location	Identifies the location of the panel.
Model	Identifies the panel model type.
Host Timeout	Sets a time period in milliseconds. If this period expires, and if the host has stopped polling the panel, the panel (RCM) switches to offline mode. The default for this period is seven seconds. Caution: Setting this value too low will affect communications. For example, setting the value to anything less than the communications "poll delay" value renders the panel unable to respond to a single download packet before going off line.
Device Number	Identifies the panel with a number. This field has no operational significance. It is a legacy bookkeeping value that was used for older Matrix hosts.
Channel	Specifies the name of the channel.
Site	Specifies the name of the site.
Address	Specifies the panel's address on the channel. Note that the number is displayed in hexadecimal.
Type	Identifies the panel as a Reader Control Module (RCM) or an MS-Reader module. Currently, Pro-Watch supports only RCMs.
Installed (check box)	Leave this box selected if you want the panel to be installed and operational.
RS-485 (check box)	Indicates whether or not the RCM is set up to participate in RS-485 communications.

11.5.2 Advanced Options Tab

Field	Description
Local Always	Indicates that the RCM will always make access decisions based only on its local card database. Host grants would be unavailable. Cards denied access on this basis could be granted access on later attempts, since corrective single-card downloads can still occur. This field is not active if the “Local Pref” option is selected.
Local Pref	Specifies that the RCM will make immediate decisions on access requests by cards that exist in its local database, and it will send host grant requests for cards that do not exist in the local database. This selection is already made by default, since this is the normal operation for many panels. Note that selecting Local Pref disables Local Always. If neither of these two options is selected, the panel enters a “host-only” mode. In the host-only mode, every access request must be validated by a host grant when the panel is on line with the server. If panels are off line, they make their own decisions.
Inverse DB	Inverts the card database. That is, any card with correct privileges is denied access, and cards that do not have correct privileges are granted access.
Split DB	Separates cardholders on the panel by Issue level. Cards with Issue levels of 10 or greater are accepted either on the card reader itself or by keypad entry of the card number. This is similar to Cypher Mode on other panels. Cards with Issue levels less than 10 are not eligible for keypad entry at all. This option might be useful when Cypher Mode functionality is desired for a reader only for particular cardholders.
Soft Fail	Grants access to cards when the panel is offline from the host and the facility codes are correct.
Wrap	Takes the panel off line and uses up its entire available memory for events. Then, subsequent new events replace the oldest events in memory. These replaced events are lost. If this field is left unchecked, events that occur after the log has filled will not be logged at all.
Facility Code	Causes the panel to accept cards only if they have the facility code.

Field	Description
Magbond Timing	Supports the use of a magnetic door lock instead of a door strike. This generally means that the “strike output” is expected to remain energized until the door position input completes an active/secure cycle. This prevents the door from magnetically “slamming shut” immediately after a cardholder starts to open the door. Typical door strike functionality de-energizes the output as soon as the door is opened in order to prevent tailgating.
Mod Egress	Causes a Request to Exit to mask the Door Forced event for this panel’s doors, but does not energize the door strike output. This field is the equivalent of Alarm Shunt ONLY on REX for Cardkey equipment.
Bound Unlock	Prevents doors from being unlocked when “armed.”
Special Material	Allows the panel to use the strike input for special materials detection.
Keys + Head	Enables a reader on the panel to allow regular card reads when the reader is configured for keypad input of card numbers (known on some panels as Cypher Mode).
PIN Style	Specifies the type of PIN codes the reader on the panel will accept.
Strike Debounce	Specifies the debounce of the door strike. The term “debounce” refers to the amount of time an input must remain active or inactive before a true change of state is considered. It denotes the number of consecutive input scans, with each scan period equal to 1/60th of a second, or 16.7 milliseconds. The selection allows for a maximum of 15, which would equal 1/4 of a second.
Mag Settle	Specifies a period of time a door remains closed in milliseconds. When the period expires, the strike input is monitored.
Early Release	Specifies the number of seconds before the normal Ajar Time expires, should the magnetic lock become re-energized. This field is active only when Magbond Timing is selected.
Tailgating	Specifies the number of seconds after door closure that tailgating is allowed. The door strike does not remain active; rather, it could be re-opened without the alarm.
Min. Local Alarm	Specifies the minimum amount of time for which the output should energize when the Local Alarm feature is active.
Access Time in 10ths	Causes the door strike time to be measured in tenths of seconds.

11.5.3 Advanced Options (cont.) Tab

Field	Description
Scan Mask	Specifies a 7-bit bitmap that includes seven output voltages that should be monitored for alarm inputs.
Scan Retries	Specifies the number of scans on an input point that must agree before considering a change of state. This helps to prevent false alarms in “noisy” electrical conditions.
Min Alarm Voltage	Specifies the minimum percentage of the output voltage read across an input point. If the voltage exceeds that percentage, the input generates an alarm.
Max Alarm Voltage	Specifies the maximum percentage of the output voltage read across an input point. If the voltage exceeds this percentage, the input generates an alarm.
Min Normal Voltage	Specifies the minimum percentage of the output voltage read across an input point. If the voltage exceeds that percentage, the input generates an alarm.
Max Normal Voltage	Specifies the maximum percentage of the output voltage read across an input point. If the voltage exceeds this percentage, the input generates an alarm.
Prox Head	Causes the readers on this panel to display “PRESENT CARD” instead of “INSERT CARD.”
Multilingual	Enables a multi-lingual capacity for the card reader. The first line of the LCD display continues to show the default English instruction, while the second line displays the localized language of the cardholder.
Date/Time Format	Changes the LCD behavior on the reader between the “Normal” option (that is, no date and time) and the various regional time represenations.
A/D Output	Causes the auxiliary outputs for the panel’s doors to energize whenever the doors are disarmed and de-energize whenever the doors are armed.
Duress Alarm	Energizes the remote outputs for a door on this panel when a duress alarm occurs.
Pulsed Local Alarm	Energizes the output for the number of seconds specified for Min Local Alarm when a local alarm occurs. If this option is not selected, the alarm output tracks the sum of alarm conditions. When all local alarms are cleared, the output is de-energized.

11.6 Viewing and Editing Dependencies of a Matrix Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

11.7 Deleting a Matrix Panel

Please refer to How to Delete a Panel, page 53

11.8 Adding a Matrix Logical Device

A Logical Device is a single physical device or a group of selected physical devices, which are defined by a hardware template. For example, a template may define a door that is equipped with a card reader, a REX input device, and a door strike output device as one Logical Device.

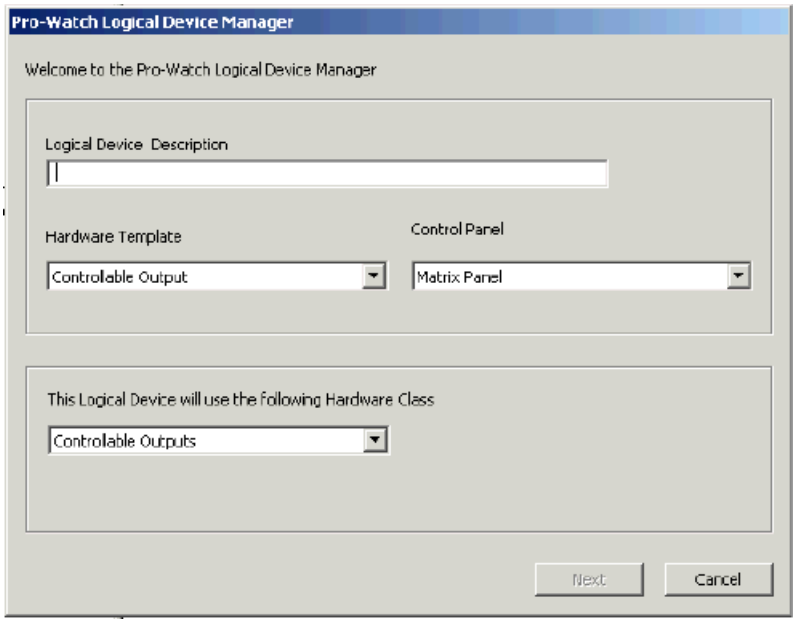
As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system. For example, you can assign the door, reader, input device, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you add Logical Devices, you must create the following:

- Site. See "Adding a Matrix Channel".
- Channel. See "Adding a Matrix Channel".
- Panel. See "Adding a Matrix Panel".
- Hardware Template. See Adding or Editing a Hardware Template, page 28.

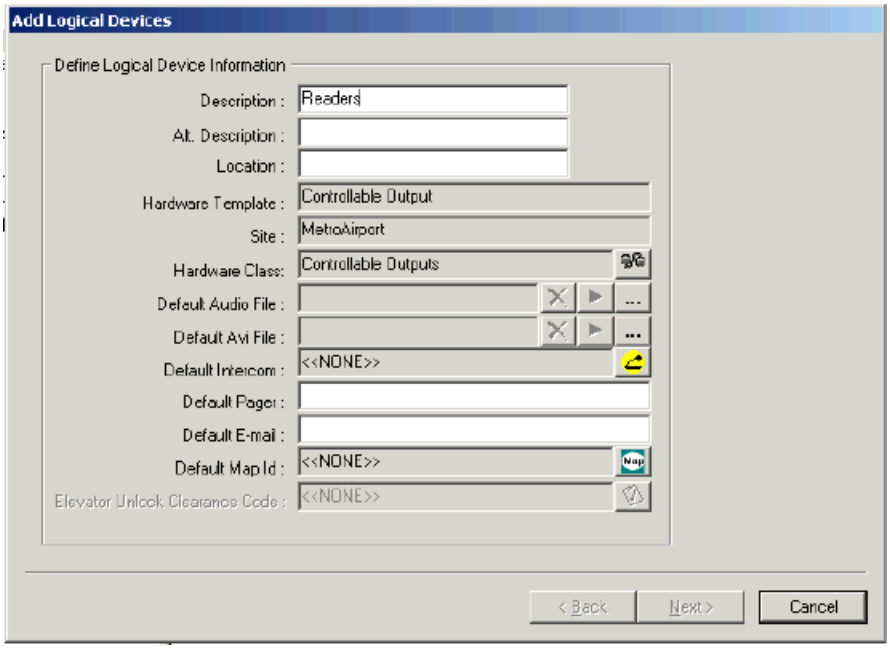
To add a Logical Device:

1. From the Pro-Watch Hardware Configuration tree, right-click the site to which you want to assign the Logical Device and select **New > Logical Device**. The Pro-Watch Logical Device Manager dialog box appears:



2. Enter a Logical Device description.
3. Select a hardware template from the Hardware Template drop-down list.

4. Select **Matrix Panel** from the Pick a Panel drop-down list.
5. From the Hardware Class drop-down list, select the Hardware Class that the Logical Device will use.
6. Click **Next** to display the second Add Logical Device dialog box.

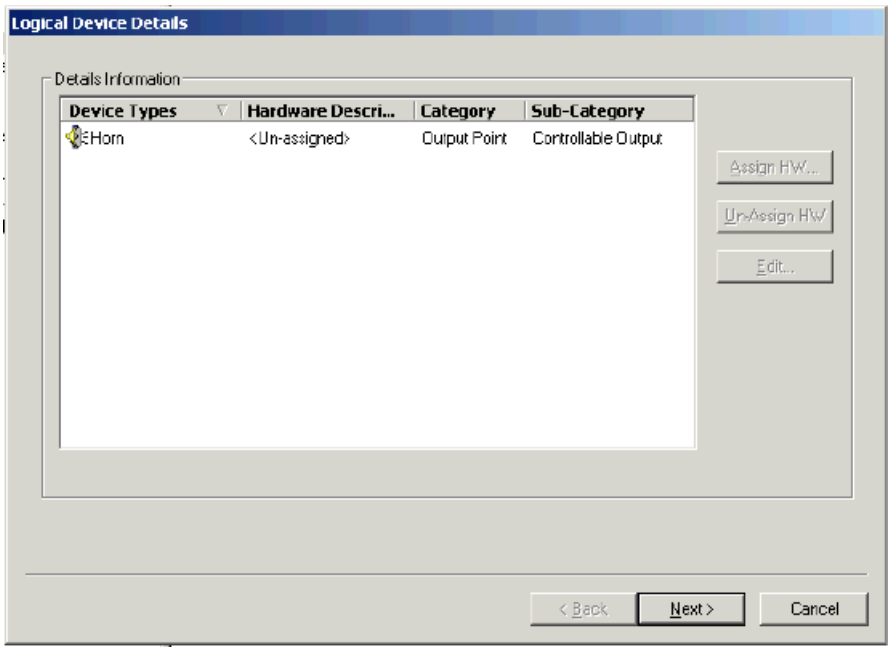


7. Use the following table to complete the second Add Logical Devices dialog box:

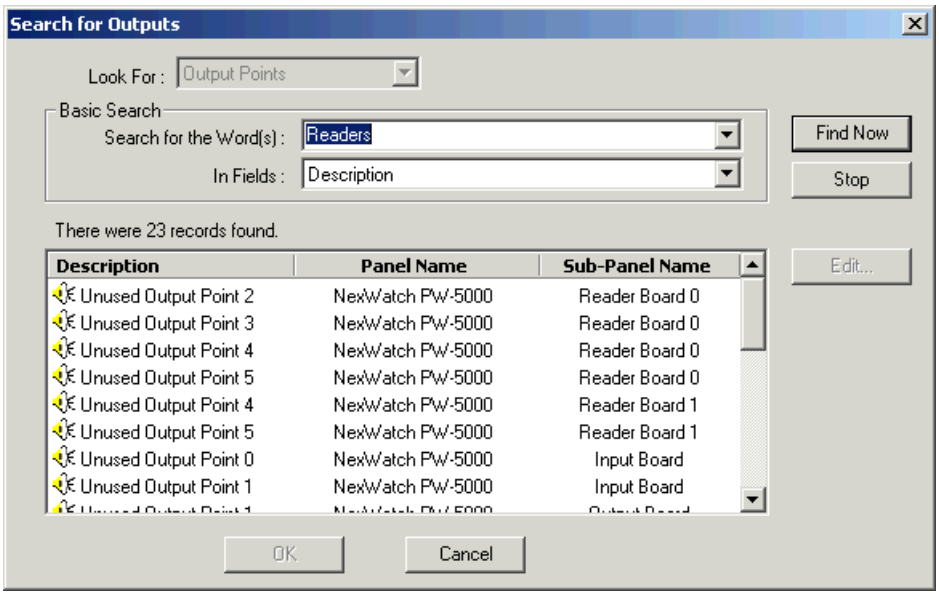
Field	Description
Description	Describes the Logical Device.
Alt. Description	Specifies an alternate description of the Logical Device.
Location	Identifies the physical location of the Logical Device.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site to which the Logical Device is assigned.
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.

Field	Description
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. See "DBC - Clearance Codes" in Chapter 37 for more information.

8. Click **Next** to display the Logical Device Details dialog box:



9. Select a device type and click **Assign HW** to display the Search for [Device Type] dialog box.



10. Enter the description in the 'search for words' field; this is the description that will be used to search for available addresses.
11. Select the field name from the 'in fields' drop-down list and click **Find Now.**
12. Select the record and click **OK.**
13. Repeat step 5 through step 10, until all device types have been assigned.
14. Click **Next**. The Default CCTV Information dialog box appears.
15. You can associate CCTV Logical Devices. You may assign the default view and commands for this device. For more information, see "HW Config - CCTV" in Chapter 21. To assign a Default Command or View, click on the icon and select the command or view. Click **OK** and then click **Next**. The Partitions dialog box appears.
16. To assign a partition to this Logical Device, click **Add**, select the partition, and click **Add** again. For information about partitions, see "DBC - Partitions" in Chapter 53.
17. Click **Finish** to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the number of sub-panels (I/O Modules) that are added to the panel.

11.9 Configuring a Matrix Logical Device

You can edit and configure Logical Devices after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices are already configured. For more information, see Adding or Editing a Hardware Template, page 28.

Note: You should visit the Logical Device configuration tabs, since these tabs contain fields that hardware templates do not.

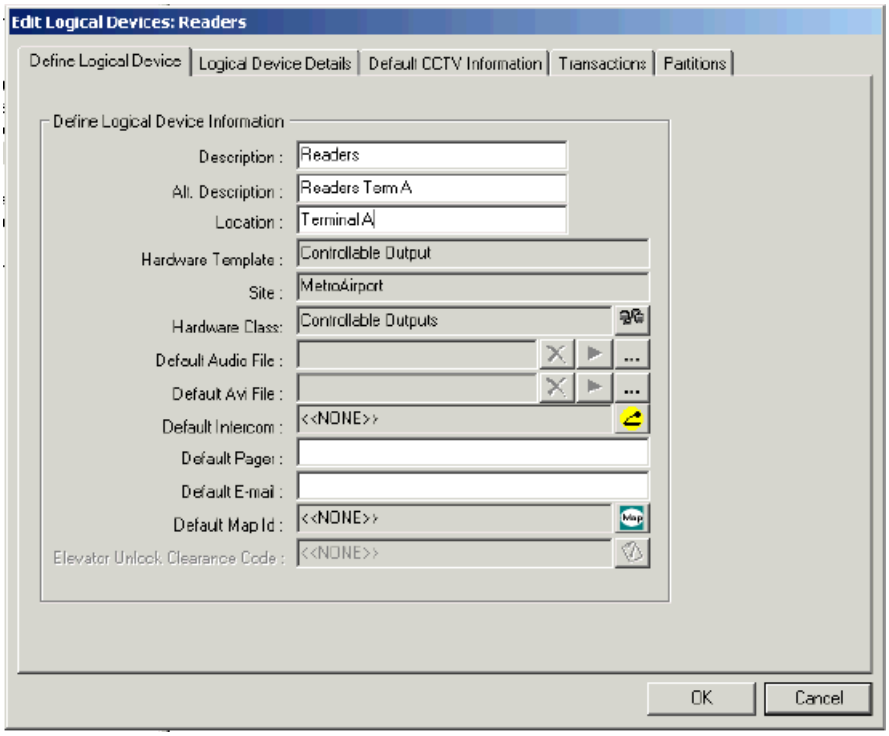
To configure a Logical Device:

1. Click the appropriate Logical Device folder in the Hardware Configuration screen to display the site's existing Logical Devices.
2. Right-click the Logical Device you want to configure, and select **Properties**. The Edit Logical Devices [Logical Device name] screen appears. The screen contains six information tabs. Complete the following information tabs to configure the Logical Device:

CONFIGURE A MATRIX LOGICAL DEVICE TABS LIST

- "Define Logical Device Tab".
- "Logical Device Details Tab".
  - Reader Devices
    - "Reader Properties Tab".
    - "Reader Settings Tab".
    - "Reader Settings (Cont.) Tab".

11.10 Define Logical Device Tab



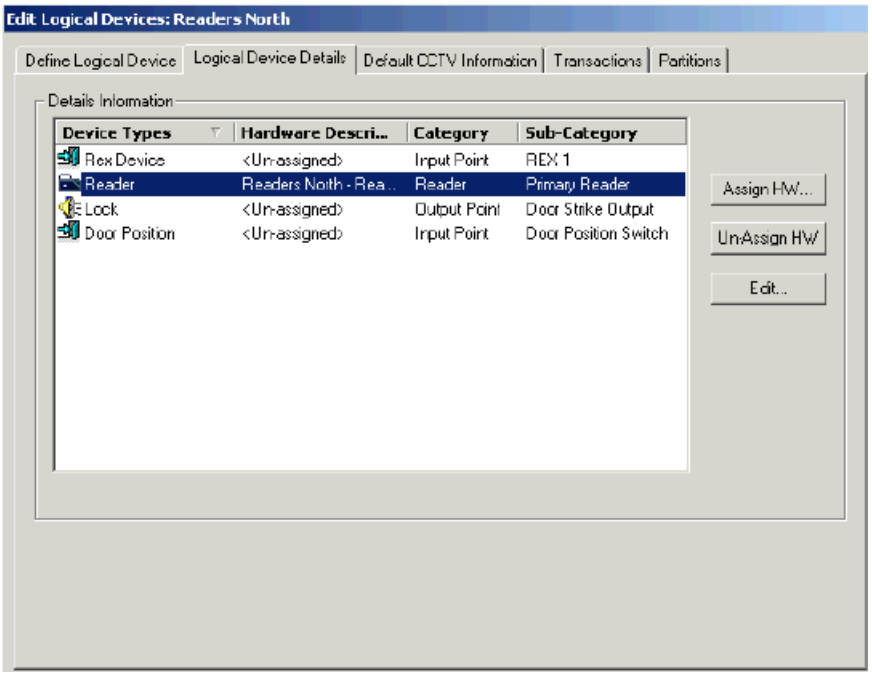
Use the following field descriptions to complete the Define Logical Device tab.

Field	Description
Description	Identifies the name of the Logical Device as defined by the user and the Logical Device type.
Alt. Description	Allows an alternative description to further identify the device.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Identifies the hardware template used to create the Logical Device.
Site	Identifies the site associated with the Logical Device.
Hardware Class	Identifies the hardware class to which the Logical Device is assigned.
Default Audio File	Identifies a default audio file that the Logical Device will play.
Default Avi File	Identifies a default video file that the Logical Device will play.
Default Intercom	Identifies a default intercom that will belong to the Logical Device.

Field	Description
Default Pager	Identifies a default pager device that will belong to the Logical Device.
Default Email	Identifies a default email address for the Logical Device.
Default Map ID	Identifies a default map which includes the Logical Device.

11.10.1 Logical Device Details Tab

This tab displays all of the device types included in the Logical Device. At this tab you can assign, un-assign, or edit the device types.



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click **OK**.

To unassign a device type:

- Click to select the device type and click **Un-Assign HW**.

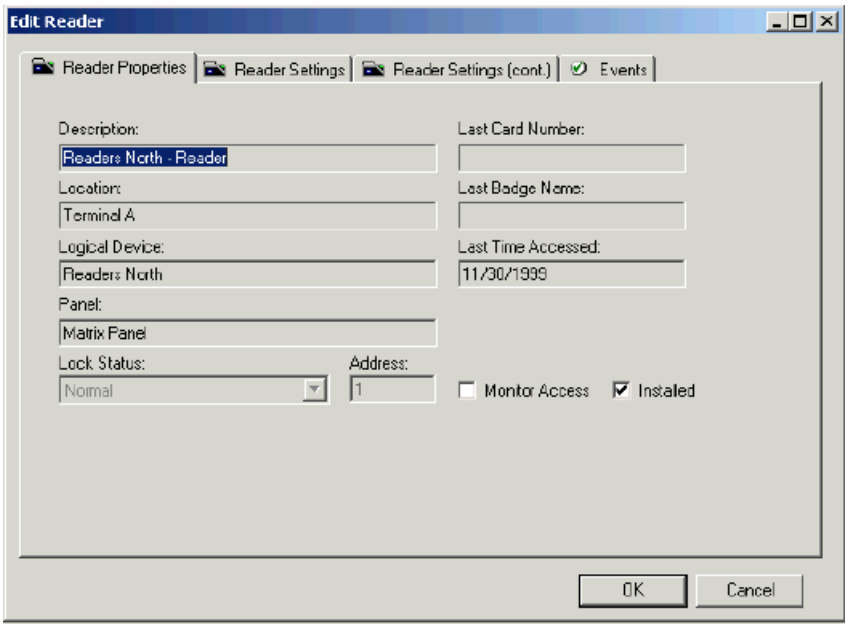
To edit the current configuration of a device type:

- Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete. Use the appropriate table below to edit or configure the device type you have selected.

Reader Device

Use the tables in the following sections to complete the Reader information tabs.

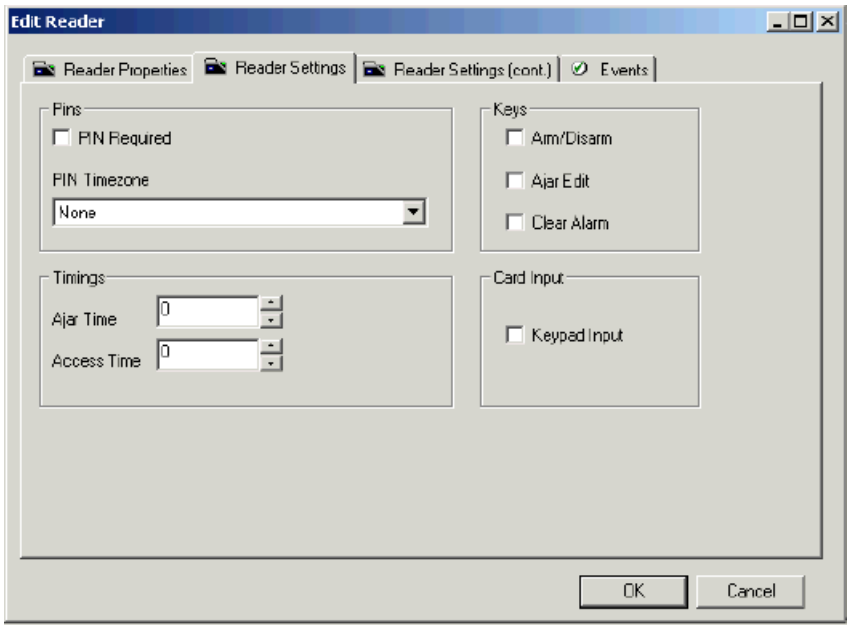
Reader Properties Tab



Field	Description
Description	Identifies the name of the Logical Device as defined by the user and the Logical Device type.
Last Card Number	Identifies the last card number that was presented at the Logical Device.
Location	Identifies the physical location of the Logical Device as defined by the user.
Last Badge Name	Identifies the badge holder name of the last badge that was presented to the Logical Device.
Logical Device	Identifies the name of the Logical Device.
Last Time Accessed	Identifies the last time the Logical Device was accessed.

Field	Description
Lock Status	Identifies the lock status of a door (locked, open, normal).
Monitored Access	Enables monitored access (card trace) on a reader.
Address	Identifies the address of the Logical Device. Note that Matrix readers are zero-based; that is, the four possible readers on a Matrix panel are numbered 0 through 3. The primary reader must be 1 or 3. The secondary reader must be 0 or 2.
Installed	Required for the Logical Device to be enabled and operational.

Reader Settings Tab



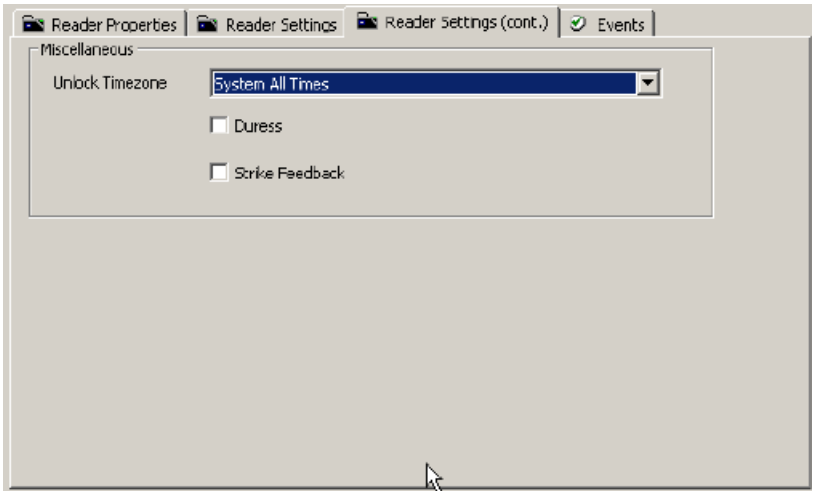
Use the following field descriptions to complete the Reader Screen/Reader Settings tab:

Field	Description
PIN Required	Puts the reader into Card-and-PIN mode indefinitely. If the option is not selected, the reader mode will be Card-Only (depending on PIN timezones and Keypad Input settings).
PIN Timezone	Specifies the timezone, if any, during which the reader should go into Card-and-PIN mode. This option is only available if "PIN Required" is not set.

Field	Description
Ajar Time	Specifies the length of time (in seconds) the door may be held open. This feature is also called “Door Held Open” time or “Propped Door” time.
Access Time	Specifies the period of time (in seconds) for which the door strike output is energized after a valid card presentation.
Arm/Disarm	Enables the cardholder to enter an Arm Zone or Disarm Zone request from the keypad, by entering an "A" or a "D" after the PIN code.
Ajar Edit	Enables a cardholder to override the standard Ajar Time with a different time. This would be done by entering the "B" key, and the number of minutes, after entering the PIN code.
Clear Alarm	Enables a cardholder to silence (deactivate) the local alarm output (for example, a local "horn" that annunciates an alarm). This would be done by entering the "C" key, and the number of minutes, after entering the PIN code.
Keypad Input	Enables a mode in which a card's number need only be entered on the keypad for access. Note that if the panel-level option "Split Database" is enabled, then a card record must have issue level 10 or higher to be used as a Cypher code. Otherwise, any card is eligible.

Reader Settings (Cont.) Tab

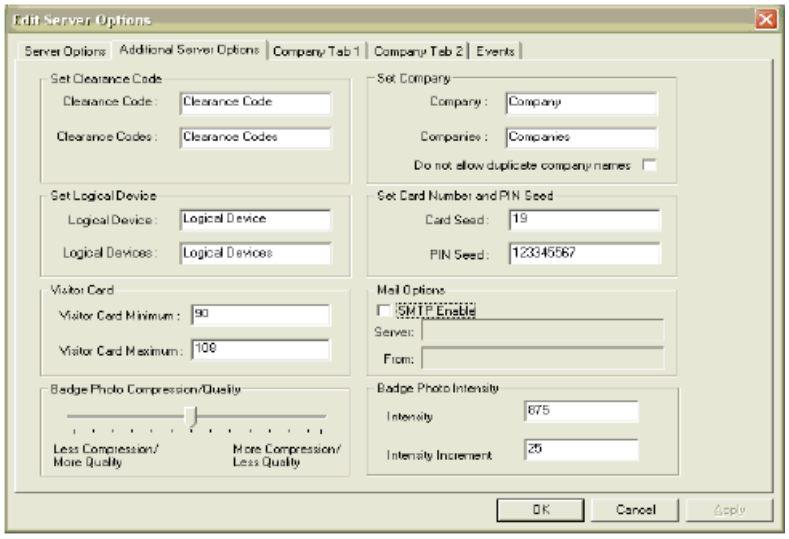
The Reader Screen/Reader Settings (Cont.) tab enables you to set timezone, duress, and strike feedback relating to the Matrix reader.



Use the following field descriptions to complete the Reader Screen/Reader Settings (Cont.) tab:

Field	Description
Unlock Timezone	Specifies the timezone, during which this door is to unlock automatically.
Duress	Enables Duress for the reader. This requires a PIN code to have been enabled on the previous screen.
Strike Feedback	Enables the Strike Input for a door. This feature also monitors the locking mechanism.

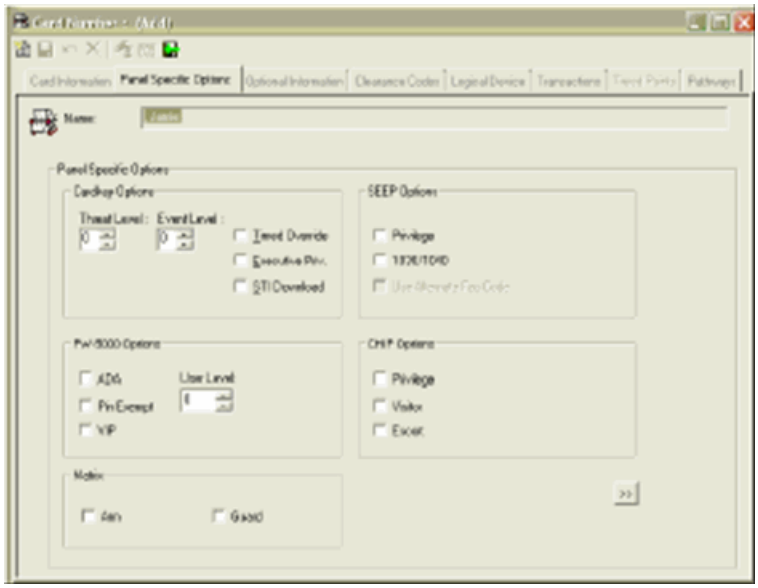
11.10.2 Server Options Screen/Additional Server Options



Use the following field descriptions to complete the Server Options Screen/Additional Server Options tab:

Field	Description
PIN Seed	Specifies the algorithmic “seed” to use for the Matrix PIN Code algorithm. This number must be 9 digits or less. If less than 9 digits, it will be interpreted as if it had leading zeroes, when separated into 3 sets of 3 numbers, as used by Matrix.

11.10.3 Cardholder Screen/Panel-Specific Options



Use the following field descriptions to complete the cardholder Screen/Panel-Specific Options tab:

Field	Description
Arm	Indicate that the cardholder is authorized to use the “A” and “D” keypad keys to arm and disarm a reader and/or zone. This function is not currently supported.
Guard	Indicates that the cardholder is authorized to clear alarms by using the “C” keypad key. This function is not currently supported.

11.11 Viewing and Editing Dependencies of a Matrix Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 53.

11.12 Deleting a Matrix Logical Device

Please refer to How to Delete a Logical Device, page 53.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - EP1502

12

In this chapter ...

Overview
EP1502 Hardware
EP1502 Panel Wiring and Setup
Input Power, Cabinet Tamper and UPS Fault Input Wiring
Communication Wiring
Reader Wiring
Input Circuit Wiring
Relay Circuit Wiring
Memory and Real Time Clock Backup Battery
Status LEDs
Specifications
Warranty
Liability

12.1 Overview

This chapter describes how to configure a EP1502 panel.

Note: The procedures in this chapter assume that an EP1502 site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

The EP1502 intelligent controller provides decision making, event reporting, and database storage for the Mercury hardware platform. Two reader interfaces provide control for two doors, managing up to a total of 64 doors.

EP1502 communicates with the Windows or Linux host via on-board 10-BaseT/100Base-TX Ethernet port. Alternatively, port 1 (RS-232) can be used for host communication.

Two physical barriers can be controlled with the EP1502.

Each reader port can accommodate a readhead that utilizes Wiegand magnetic stripe, or 2-wire RS-485 electrical signaling standards, one or two wire LED controls, and buzzer control (one wire LED mode only).

Four Form-C relay outputs may be used for strike control or alarm signaling.

The relay contacts are rated at 5 A @ 30 VDC, dry contact configuration.

Eight inputs are provided for monitoring the door contacts, exit push buttons and alarm contacts.

The EP1502 requires 12-24 VDC for power. It is recommended that the EP1502 be mounted .25" minimum above any conductive surface.

12.1.1 Features Summary

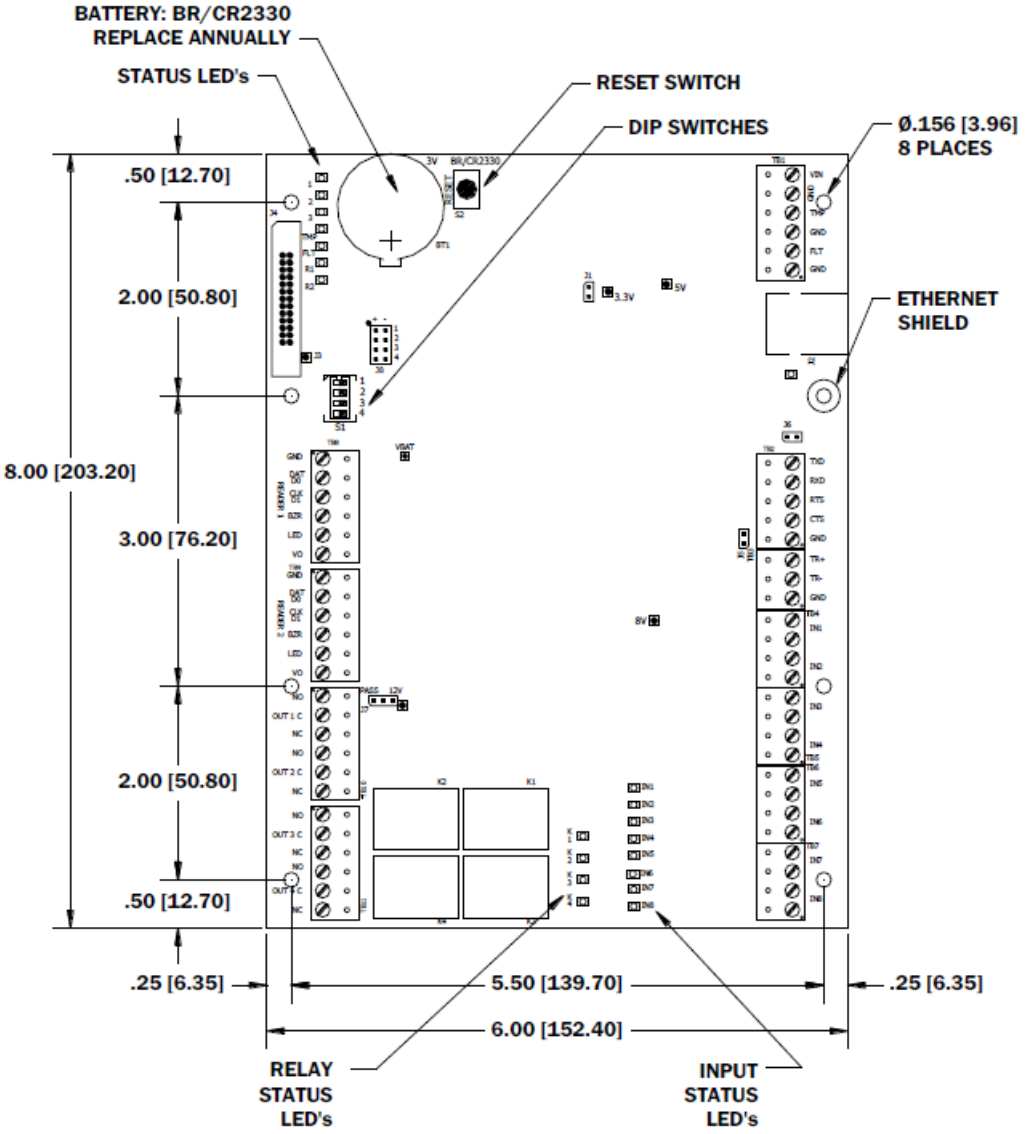
- Multi-operating system interface
- Multi-host interface communications
- AES 128 bit data encryption support
- Alarm keypad support
- Function key support
- Universal I/O device
- HSPD-12/FIPS201 compliant
- UL 294 recognized

12.1.2 Benefits Summary

- Scalable to 64 doors/openings

- Connects to a Windows or Linux host for increased programming versatility
- Supports a range of wired and wireless reader technologies
- Supports multiple card formats for flexibility
- Intelligent oversight of auxiliary point control and monitoring

12.2 EP1502 Hardware



12.3 EP1502 Panel Wiring and Setup

Table 12-1 EP1502 Panel Wiring and Setup

CONNECTIONS		
TB1	Power Input	VIN: 12 to 24 Vdc GND
	Cabinet Tamper Input	TMP GND
	Power Fault Input	FLT GND
TB2	Host Port 1	TXD (RS-232) RXD (RS-232) RTS (RS-232) CTS (RS-232) GND (RS-232)
TB3	SIO Port	TR+ (2-wire RS-485) TR- (2-wire RS-485) GND (2-wire RS-485)
TB4	Input 1	IN1 IN1
	Input 2	IN2 IN2
TB5	Input 3	IN3 IN3
	Input 4	IN4 IN4
TB6	Input 5	IN5 IN5
	Input 6	IN6 IN6
TB7	Input 7	IN7 IN7
	Input 8	IN8 IN8
TB8	Reader 1	GND: Ground DAT/D0: Data/Data 0/TR- CLK/D1: Clock/Data 1/TR+ BZR: Reader Buzzer LED: Reader LED VO: Reader Power

Table 12-1 EP1502 Panel Wiring and Setup

CONNECTIONS		
TB9	Reader 2	GND: Ground DAT/D0: Data/Data 0/TR- CLK/D1: Clock/Data 1/TR+ BZR: Reader Buzzer LED: Reader LED VO: Reader Power
TB10	Out 1	NO: Normally Open Contact C: Common NC: Normally Closed Contact
	Out 2	NO: Normally Open Contact C: Common NC: Normally Closed Contact
TB11	Out 3	NO: Normally Open Contact C: Common NC: Normally Closed Contact
	Out 4	NO: Normally Open Contact C: Common NC: Normally Closed Contact

12.3.1 Configuring EP1502 Jumpers

The EP1502 processor hardware interface is configured using jumpers to setup the port interface and end of line termination.

Table 12-2 EP1502 Panel Jumper Settings

JUMPERS	SET AT	DESCRIPTION
J1	N/A	N/AFactory Use Only
J2	N/A	10Base-T/100Base-Tx Ethernet Connection (Port 0)
J3	N/A	Factory Use Only
J4	N/A	Factory Use Only
J5	OFF	Port 2 RS-485 EOL Terminator is Off
	ON	Port 2 RS-485 EOL Terminator is On
J6	N/A	Factory Use Only
J7		Reader Power Select. See Note 1
	12V	12 Vdc at Reader Ports
	PASS	VIN "Pass Through" to Reader Ports

Table 12-2 EP1502 Panel Jumper Settings

JUMPERS	SET AT	DESCRIPTION
J8-1	N/A	Remote Status Led #1. See Note 2
J8-2	N/A	Remote Status Led #2. See Note 2
J8-3	N/A	Remote Status Led #3. See Note 2
J8-4	N/A	Remote Status Led #4. See Note 2

Note 1: The input power (VIN) must be 20 Vdc minimum if the 12 Vdc selection is to be used.

Note 2: Observe POLARITY connection to LED. External current limiting is not required.

12.3.2 Configuring EP1502 DIP Switches

The four switches on S1 DIP switch configure the operating mode of the EP1502 processor.

DIP switches are read on power-up except where noted. Pressing switch S2 causes the EP1502 to reset.

Table 12-3 EP1502 DIP Switches

1	2	3	4	DEFINITIONS
OFF	OFF	X	OFF	Normal operating mode.
ON	X	X	X	After initialization, enable default User Name (admin) and Password (password). The switch is read on the fly, no need to re-boot.
OFF	ON	X	OFF	Use factory default communication parameters.
ON	ON	X	OFF	Use OEM default communication parameters. Contact system manufacture for details. See Bulk Erase below.
X	X	ON	X	Disable TLS secure link. Switch is read only when logging on.
ON	ON	OFF	OFF	Bulk Erase prompt mode at power up. See Bulk Erase below.

All other switch settings for unassigned and are reserved for future use.

X = don't care.

Caution: In the factory or OEM default modes, downloaded configuration/database is not saved to flash memory.

12.3.3 Factory Default Communication Parameters:

Network: static IP address: 192.168.0.251

Communication address: 0

Primary Host port: IP server, no encryption, port 3001.

Alternate Host Port 1: RS-232, 38,400 baud, no encryption, no flow control.

12.3.4 Bulk Erase Configuration Memory:

The bulk erase function can be used for the following purposes:

- To erase all configuration and cardholder database data.
- To recover from a corrupted database in the unlikely event the database gets corrupted and causes the EP1502 to continuously reboot.

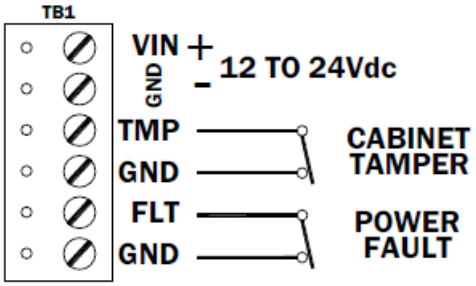
When power is applied with S1 switches set to 1 & 2 ON and 3 & 4 OFF, there is a 10-second window that if switch 1 or 2 is changed to the OFF position memory is erased.

The LEDs flash the following pattern when in the reset window: LED 1 & 2 and LED 3 & 4 flash alternately at .5 second rate.

When erasing memory, LED 2 flashes at a 2 second rate; **DO NOT CYCLE POWER**. It takes less than 60 seconds to erase the memory. LEDs 1 and 4 flash for 10 seconds after the memory has been erased, then the EP1502 will re-boot.

12.4 Input Power, Cabinet Tamper and UPS Fault Input Wiring

The EP1502 requires 12-24 Vdc power. Locate power source as close to the unit as possible.



Caution: Connect power with minimum of 18 AWG wire. Connect the GND signal to earth ground in ONE LOCATION within the system! Multiple earth ground connections may cause ground loop problems and is not advised.

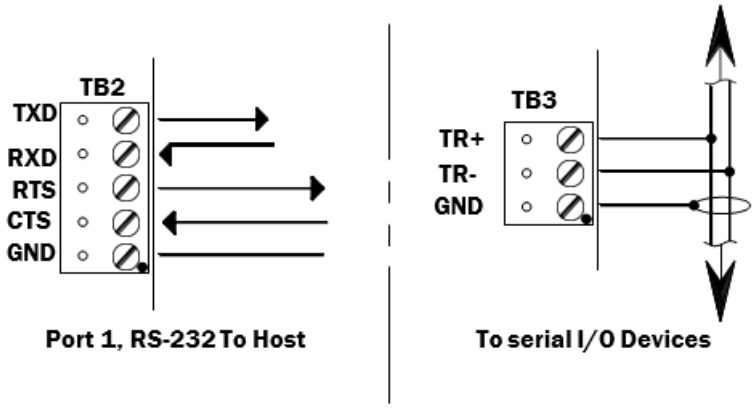
Caution: Observe POLARITY on 12-24 Vdc input!

There are two dedicated inputs for cabinet tamper and UPS fault monitoring. Normal (safe) condition is a closed contact. If these inputs are not used, install a jumper wire.

12.5 Communication Wiring

The EP1502 controller communicates to the host via the on-board 10-BaseT/100Base-TX Ethernet interface (port 0) and/or RS-232 interface (port 1). RS-232 interface is for direct one to one connection to a host computer port or via modem, 25 feet maximum.

The serial I/O device communication port (TB3) is a 2-wire RS-485 interface which can be used to connect additional I/O panels. The interface allows multi-drop communication on a single bus of up to 4,000 feet (1,219 m). Use twisted pairs (minimum 24 AWG) with an overall shield for communication.



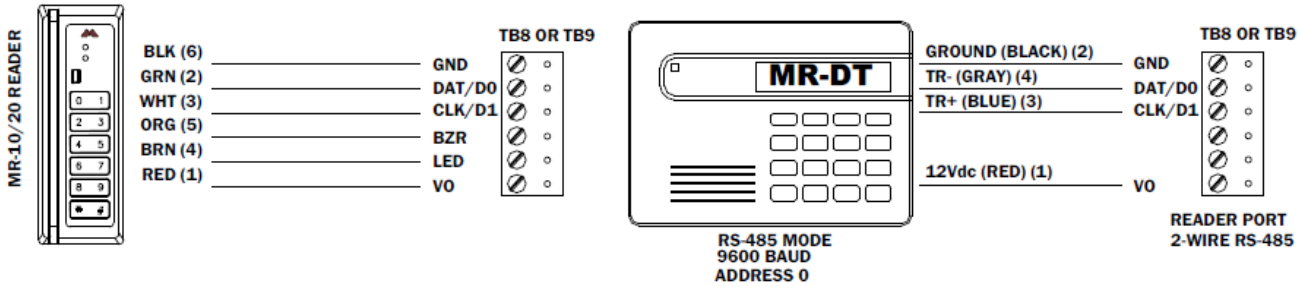
Caution: Install the termination jumper ONLY on the panel at each end of the RS-485 bus. Failure to do so will compromise the proper operation of the communication channel!

12.6 Reader Wiring

Each reader port supports Wiegand, magnetic stripe, and 2-wire RS-485 electrical interfaces. Power to the reader is selectable: 12 Vdc (VIN must be greater than 20 Vdc), or power is passed-through (PT) from the input voltage of the EP1502 (TB1-VIN) and is current limited to 150 mA for each reader port. Readers that require different voltage or have high current requirements should be powered separately. Refer to the reader manufacture specifications for cabling requirements. In the 2-wire LED mode the Buzzer output in used to drive the second LED. Reader port configuration is set via the host software.

PASS 12V	READER POWER
	12Vdc IS AVAILABLE ON READER PORTS (VIN≥20Vdc)
	VIN POWER IS "PASSED THROUGH" TO READER PORTS

J7 - READER POWER SELECT



DATA1/DATA0 - CLOCK/DATA

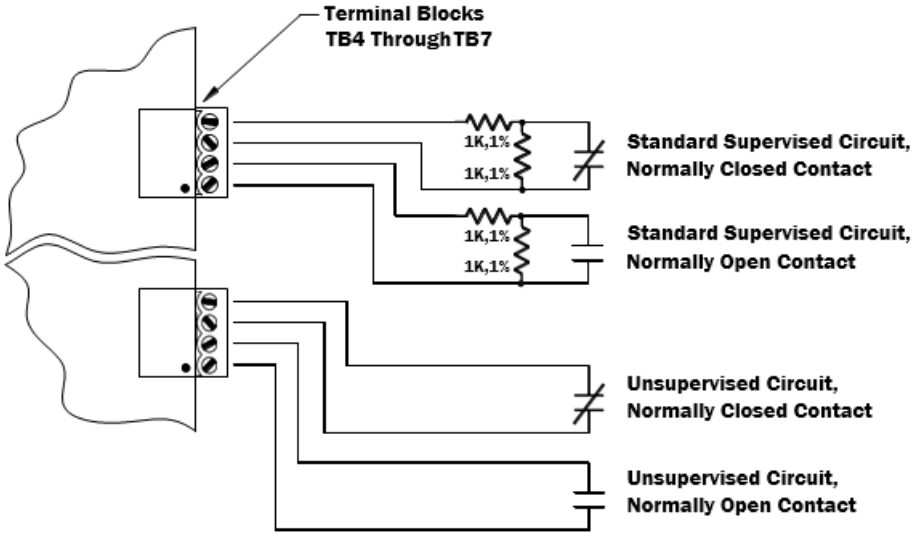
2-WIRE RS-485

12.7 Input Circuit Wiring

Typically, these inputs are used to monitor door position, request to exit, or alarm contacts. Input circuits can be configured as unsupervised or supervised. When unsupervised, reporting consists of only the open or closed states. When configured as supervised, the input circuit will report not only open and closed, but also open circuit, shorted, grounded*, and foreign voltage*. A supervised input circuit requires two resistors be added to the circuit to facilitate proper reporting. The standard supervised circuit requires 1k Ohm, 1% resistors and should be located as close to the sensor as possible. Custom end of line (EOL) resistances may be configured via the host software.

* Grounded and foreign voltage states are not a requirement of UL 294 and therefore not verified by UL.

The input circuit wiring configurations shown are supported but may not be typical:



12.8 Relay Circuit Wiring

Four relays with Form-C contacts are provided for controlling door lock mechanisms or alarm signaling.

The relay contacts are rated at 5 A @ 30 Vdc, dry contact configuration.

Each relay has a Common pole (C), a Normally Open pole (NO) and a Normally Closed pole (NC).

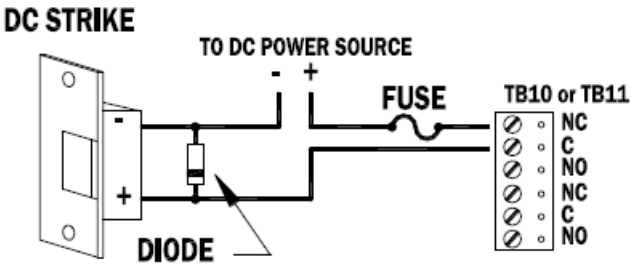
When you are controlling the delivery of power to the door strike, the Normally Open and Common poles are used.

When momentarily removing power to unlock the door, as with a mag lock, the Normally Closed and Common poles are used.

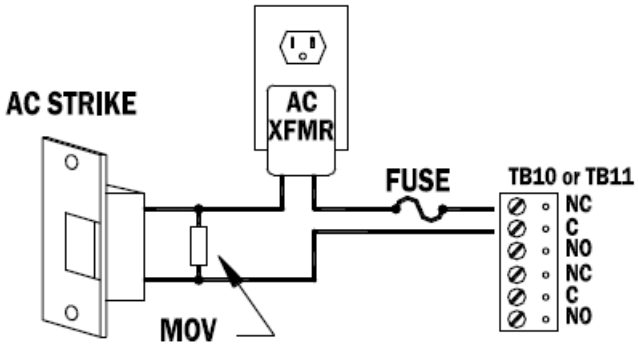
Check with local building codes for proper egress door installation.

Door lock mechanisms can generate feedback to the relay circuit that can cause damage and premature failure of the relay.

For this reason, it is recommended that either a diode or MOV (metal oxide varistor) be used to protect the relay. Wire should be of sufficient gauge to avoid voltage loss.



Diode Selection:
Diode current rating: 1x strike count
Diode breakdown voltage: 4x strike voltage
For 12 Vdc or 24 Vdc strike, diode 1N4002 (100V/1A) typical.



MOV Selection:
Clamp voltage: 1.5x Vac RMS.
For 24 Vac strike, Panasonic: ERZ-C07DK470 typical

12.9 Memory and Real Time Clock Backup Battery

The static RAM and the real time clock are backed up by a lithium battery when input power is removed. This battery should be replaced annually. If data in the static RAM is determined to be corrupt after power up, all data, including flash memory, is considered invalid and is erased All configuration data must be re-downloaded. Remove the insulator from the battery holder after installation. Battery type: BR2325, BR2330, or CR2330.

12.10 Status LEDs

Power-up: All LED's **OFF**.

Initialization: LED's 1, 2, 3, TMP, FLT, R1, R2, IN1, IN2, IN3, IN4, IN5, IN6, IN7 and IN8 are sequenced during initialization. LED's 1, 3, and TMP are turned ON for approximately 4 seconds after the hardware initialization has completed, then the application code is initialized. The amount of time the application takes to initialize depends on the size of the database, about 3 seconds without a card database. Each 10,000 cards will add about 3 seconds to the application initialization. When LED's 1, 2, 3 and TMP flash at the same time, data is being read from or written to flash memory, do not cycle power when in this state.

Running: After initialization is complete, the LEDs have the following meanings: At power up, LEDs 2 through 6 are turned ON then OFF in sequence.

Table 12-4 Status LEDs

LED	DESCRIPTION
1	Off-Line / On-Line and Battery Status
	Off-Line = 20% ON, On-Line = 80% ON
	Double Flash if Battery is Low
2	Host Communication Activity (Ethernet or Serial Port 1)
3	Internal SIO Communication Activity
TMP	External SIO Communication Activity
FLT	Unassigned
R1	Reader 1: Clock/Data or D1/D0 Mode = Flashes when Data is Received, Either Input. RS-485 Mode = Flashes when Transmitting Data
R2	Reader 2: Clock/Data or D1/D0 Mode = Flashes when Data is Received, Either Input. RS-485 Mode = Flashes when Transmitting Data
D16	Flashes with Host Communication (Ethernet Port 0)
YEL	Ethernet Speed: OFF = 10Mb/S, ON = 100Mb/S
GRN	OFF = No Link, ON = Good Link, Flashing = Ethernet Activity
IN1	Input IN1 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.
IN2	Input IN2 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.
IN3	Input IN3 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.
IN4	Input IN4 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.
IN5	Input IN5 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.
IN6	Input IN6 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.
IN7	Input IN7 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.

Table 12-4 Status LEDs (continued)

LED	DESCRIPTION
IN8	Input IN8 Status: OFF = Inactive, ON = Active, Flash = Trouble. See Note 1.
K1	Relay K1: ON = Energized
K2	Relay K1: ON = Energized
K3	Relay K1: ON = Energized
K4	Relay K1: ON = Energized

Note: If this input is defined, every three seconds the LED is pulsed to its opposite state for 0.1 seconds, otherwise, the LED is off.

12.11 Specifications

The interface is for use in low voltage, Class 2 Circuits only.

The installation of this device must comply with all local fire and electrical codes.

Table 12-5 Specifications

Primary Power	12-24 Vdc±10%, 500 mA maximum (reader current not included) 12 Vdc @ 250 mA (plus reader current) nominal 24 Vdc @ 150 mA (plus reader current) nominal
Memory and Clock Backup Battery	3 Volt Lithium, type BR2325, BR2330 or CR2330
Host Communication	Ethernet: 10BaseT/100Base-TX, and RS-232; 9,600 to 115,200 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit.
SIO Communication	2-wire RS-485, 2,400 to 115,200 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit.
Inputs	Two dedicated for tamper and UPS fault monitoring. Eight for door position monitoring, request to exit or alarm contacts.
Relays	Four each: Form-C, 5 A @ 30 Vdc, resistive
READER INTERFACE	
Reader Power	12 Vdc±10% regulated, current limited to 150 mA for each reader. (jumper selectable) or 12 to 24 Vdc±10% (input voltage passed through) current limited to 150 mA for each reader
Data Inputs	TTL compatible inputs, mag stripe and Wiegand standards supported. Maximum cable length: 500 ft (152 m).
RS-485 Mode	9,600 to 38,400 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit. Maximum cable length: 2000 ft (609.6 m)
LED Output	TTL levels, high>3 V, Low<0.5 V, 5 mA source/sink maximum.
Buzzer Output	TTL levels, high>3 V, Low<0.5 V, Low=Active, 5 mA source/sink maximum.
CABLE REQUIREMENTS	
Power	1 twisted pair, 18 AWG
Ethernet	CAT-5. minimum
RS-485 (I/O Device Port)	24 AWG, 4,000 ft (1,219 m) maximum, twisted pair(s) with an overall shield
RS-485 (Reader Port)	24 AWG, 2,000 ft (609.6 m) maximum, twisted pair(s) with an overall shield
RS-232	24 AWG, 25 ft (7.6 m) maximum.
Alarm Input	1 twisted pair, 30 ohms maximum, typically 22 AWG @ 1000 ft (304.8 m).
ENVIRONMENTAL	
Temperature	0 to 70 °C, operating, -55 to +85 °C, storage

Table 12-5 (continued)***Specifications***

Humidity	10 to 95% RHNC
MECHANICAL	
Dimension	8 in (203.2 mm) W x 6 in (152.4 mm) L x 1 in (25 mm) H
Weight	9 oz (255 g) nominal, board only

12.12 Warranty

Mercury Security Corporation warrants the product is free from defects in material and workmanship under normal use and service with proper maintenance for one year from the date of factory shipment. Mercury Security Corporation assumes no responsibility for products damaged by improper handling or installation. This warranty is limited to the repair or replacement of the defective unit.

There are no expressed warranties other than set forth herein. Mercury Security Corporation does not make, nor intends, nor does it authorize any agent or representative to make any other warranties, or implied warranties, and expressly excludes and disclaims all implied warranties of merchantability or fitness for a particular purpose.

Returned units are repaired or replaced from a stock of reconditioned units. Returns must be accompanied by a return authorization number (RMA) obtained from customer service, and prepaid postage and insurance.

12.13 Liability

The Interface should only be used to control exits from areas where an alternative method for exit is available. This product is not intended for, nor is rated for operation in life-critical control applications. Mercury Security Corporation is not liable under any circumstances for loss or damage caused by or partially caused by the misapplication or malfunction of the product. Mercury Security Corporation's liability does not extend beyond the purchase price of the product.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - SEEP

13

In this chapter ...

Overview
Adding a SEEP Channel
Viewing and Editing Dependencies of a SEEP Channel
Deleting a SEEP Channel
Adding a SEEP Panel
Configuring a SEEP Panel
Editing a SEEP Panel
Viewing and Editing Dependencies of a SEEP Panel
Deleting a SEEP Panel
Adding a SEEP Logical Device
Viewing and Editing Dependencies of a SEEP Logical Device
Deleting a SEEP Logical Device

13.1 Overview

This chapter describes how to configure a site that uses a SEEP panel.

Note: The SEEP panel is not supported in Pro-Watch Lite.

Note 2: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

13.2 Adding a SEEP Channel

The Pro-Watch channel is the communications path between the Pro-Watch server and the panel. You must identify the channel before adding a panel and Logical Device.

To add a channel, complete the steps in the following sections.

Note: The recommended maximum number of channels per site is 99.

13.2.1 Select a Channel Type

1. In the Pro-Watch Hardware Configuration tree, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.
2. Select a channel type specific to your hardware manufacturer from the drop-down list.
3. Click OK. The Define Channel Information dialog box appears.
4. Define the Channel.
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
   c. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.
   d. In the Attempts field, enter the maximum number of times the Pro-Watch server will poll a panel before determining a panel timeout.
   e. In the Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds.
   f. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.
   g. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.

h. Click **Next** to display the Communications Parameters dialog box.

13.2.2 Set Communications Parameters

1. Select the port type from the following drop-down list options:

Option	Description
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. This option is valid for all panels and devices except VAST. Com Port – The communication port on the host computer. Baud – The communication speed between the host and the panel.
TCP/IP	Specifies that the channel is a network connection. IP Address – The IP address of the panel.
Dial Out	Defines a modem port as the primary mode of communication for the selected channel. Com Port – The communication port on the host computer. Baud – The communication speed between the host and the panel.
Dial In	Defines a modem port as the primary mode of communication for the selected channel. Com Port – The communication port on the host computer. Baud – The communication speed between the host and the panel.
TCP/IP (Encrypted)	This functionality is provided by the network connection hardware. "TCP/IP encrypted" encrypts messages between the host and the panel. IP Address – The IP address of the panel. Encrypt Password – The password assigned.
Modem Pools	Modem Pools are used for dial out. Modem Pool – A collection of modems. Baud – The communication speed between the host and the panel. Flow Control – Starts and stops the transmission between the host and the panel.

2. Click Next **to display the Channel Dialup dialog box. When choosing dial-up communication parameters, you must complete the settings within the channel dial-up dialog box. See** Appendix C,

Dial-Up Configuration for more information on configuring dial-up for the SEEP panels.

Field	Description
Dialup Schedule	Determines how often you want to call the panel. Dial-up Schedules are configured in Database Configuration. For more information, see "DBC - Dial-Up Schedule" in Chapter 42.
Password	The password to the remote 'hub'.
Remote Site Phone Number	Defines the phone number for the remote site.
Host Phone Number	Defines the phone number for the host site.
Phone Host After # of Events	Initiates dial up after a specified number of events have occurred.
Serial Number	Automatically populated; it is used for the panel driver's identification scheme.
Dialup Retries	Defines the number of times the host will attempt to dial up.
Site ID	This function is currently not supported.
Forcibly Disconnect After (minutes)	Defines the amount of time in minutes until the connection will be forced to disconnect.
Disconnect After	Defines the amount of time of inactivity that can pass before disconnect.
Delay Connect Time	This function is currently not supported.
Delay Retry Time	This function is currently not supported.
Prefix	Defines the area code. Not applicable since the area code is usually included when the number is defined.
Modem Init String	Defines the initialization string to initialize the modem.

3. Click Next to display the Partitions dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.
4. Click Finish to complete the channel. A warning message appears reminding you that you must add the channel to the appropriate routing group before you can view any events using the channel. It is recommended that you assign the channel to a routing group after you plan and configure routing groups. See "DBC - Routing Groups" in Chapter 55.

13.3 Viewing and Editing Dependencies of a SEEP Channel

Use this function to view and modify the Channel's dependencies. The Channel object depends upon the Site and Routing Group objects.

To view and modify a Channel's dependencies:

1. Right-click the icon of an existing Channel in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Channel's dependencies.
2. To modify or remove the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click OK to close the dialog box.

13.4 Deleting a SEEP Channel

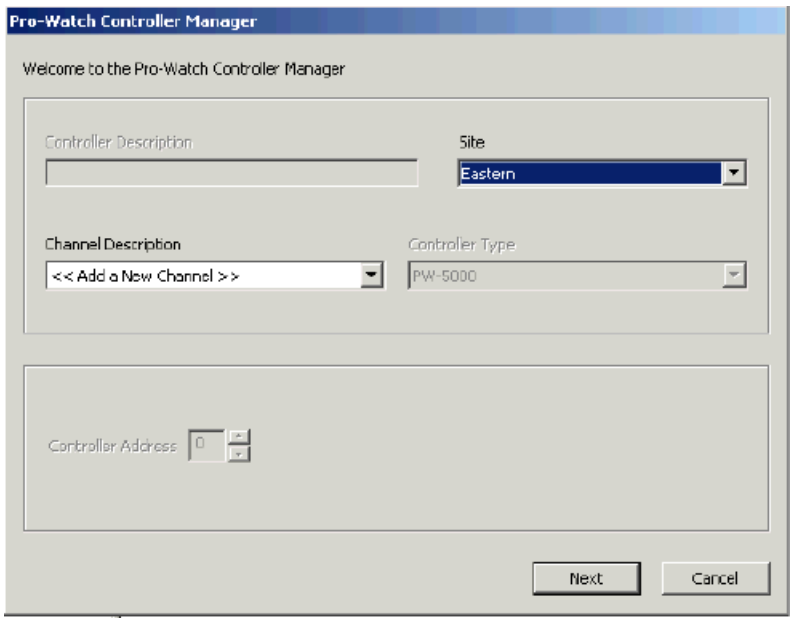
Please refer to How to Delete a Channel, page 51.

13.5 Adding a SEEP Panel

To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 4.

To add a panel:

1. In the Pro-Watch Hardware tree view, right-click the site you have created for the panel.
2. Select New > Panel to display the Pro-Watch Controller Manager dialog box.



3. Select the channel you have created for this panel from the Channel Description drop-down list and click OK.
4. In the Add Panel dialog box, enter the Panel Description.
5. Select the panel address from the drop-down list.
6. Select the panel type from the drop-down list that corresponds to your hardware and click OK.

The SEEP family of panels supported by Pro-Watch consists of multiple panel types: 804S, 804SN, 804SX, 804SXT, 808S, 808SN, 808SX, 808SXT, 818SC, SE4100, and Star I. Each of these panel types have distinct differences but they share similar configuration tasks. These panel types will be grouped and explained accordingly.

The Add SEEP Panel dialog box will encompass multiple tabs that will need to be addressed in order to complete panel configuration.

13.6 Configuring a SEEP Panel

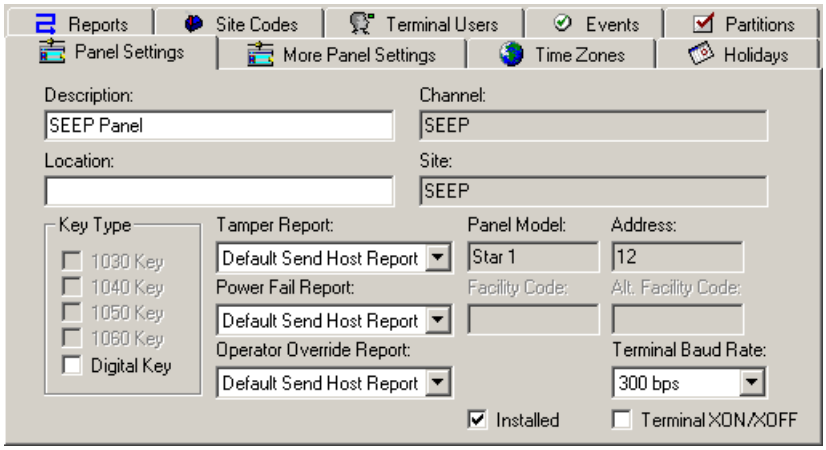
The Add SEEP Panel dialog box includes the following tabs that you need to complete to configure the panel:

CONFIGURE SEEP PANEL TABS LIST

- "Panel Settings Tab".
- "More Panel Settings Tab".
- "Time Zones Tab".
- "Holidays Tab".
- "Reports Tab".
- "Transactions Tab".
- "Terminal Users Tab".
- "Events Tab".
- "Partitions Tab".

13.6.1 Panel Settings Tab

The Panel Settings tab contains hardware settings to include identifying key type and assigning reports.



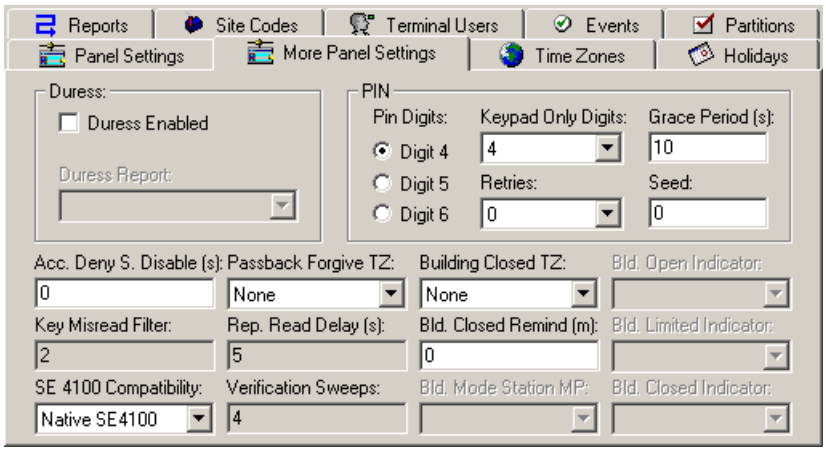
Use the following field descriptions to complete the Panel Settings tab:

Field	Description	Panel Type ...
Description	Provides the Description of the Panel.	All Panel Types.
Location	Identifies the location of the Panel as defined by the user.	All Panel Types.
Channel	Identifies the Channel in which the panel is assigned.	All Panel Types.
Site	Identifies the Site in which the panel is assigned.	All Panel Types.
Key Type	Identifies the Key Type for the Panel (1030,1040,1050, Digital) Not all keys are applicable to every panel type. For example, Digital is not applicable for the 800 series panels.	804S, 804SN, 804SX, 808S, 808SN, 808SX, 808SXT, 818SC, SE4100, Star I.
Tamper Report	Identifies the Report upon Tamper. See "Reports Tab".	All Panel Types.
Power Fail Report	Identifies the Report upon Power Fail. See "Reports Tab".	All Panel Types.
Operator Override Report	Identifies the Report upon Operator Override. See "Reports Tab".	All Panel Types.
Panel Model	Identifies the Panel Model.	All Panel Types.
Address	Identifies the Address of the Panel.	All Panel Types.
Facility Code	Identifies the facility code for 1030/1040 cards	804S, 804SN, 804SX, 808S, 808SN, 808SX, 818SC.
Alt. Facility Code	Allows you to have cards with the same card number but a different facility code.	804S, 804SN, 804SX, 808S, 808SN, 808SX, 818SC.
Installed	Required for the panel to be installed and operational	All Panel Types.

Field	Description	Panel Type ...
Terminal Baud Rate	Identifies the Terminal Baud Rate of the panel terminal mode.	804SN, 804SX, 804SXT, 808SN, 808SX, 808SXT, 818SC, SE4100, Star I.
Terminal XON/XOFF	Identifies the flow control for the panel terminal mode.	All Panel Types.

13.6.2 More Panel Settings Tab

The More Panel Settings tab enables you to configure additional hardware settings. The More Panel Settings tab is only applicable to 804SN, 804SX, 804SXT, 808SN, 808SX, 808SXT, 818SC, SE4100, and Star I panels.



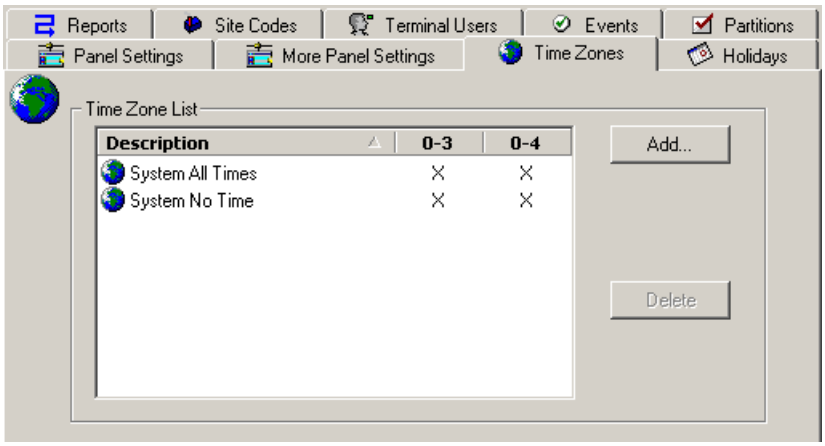
Use the following field descriptions to complete the More Panel Settings tab:

Field	Description	Panel Type ...
Duress	Enables Duress. The “Duress” functionality enables the user to trigger an alarm event in times of duress such as when the site is under attack or the operator is forced to grant access to an unauthorized user.	818SC, SE4100, Star I.
Duress Report	Identifies the Report upon Duress. See "Reports Tab".	818SC, SE4100, Star I.
PIN Digits	Identifies the Number of PIN Digits.	818SC, SE4100, Star I.
Keypad Only Digits	Identifies the Number of Keypad Only Digits.	818SC, SE4100, Star I.
Retries	Identifies the Number of attempts a PIN user has to enter the PIN correctly in the event the first attempt was incorrect.	818SC, SE4100, Star I.
Grace Period	Defines the amount of time allowed for a user to complete entry of a PIN number after a card swipe.	818SC, SE4100, Star I.
Seed	Defines the PIN seed. A PIN seed allows for the generation of a random PIN number.	818SC, SE4100, Star I.
Acc. Deny S. Disable	On an invalid card or access denied report, the reader disables for the specified number of seconds. (0-255 with 0 being off).	All Panel Types.
Key Misread Filter	Defines the number of successive invalid cards reads which need to occur to deny access. Applicable to analog readers.	All Panel Types.
SE 4100 Compatibility	Defines the mode the panel operates in, for example, the manner in which cards are processed.	808SXT, SE4100, Star I.
Passback Forgive TZ	Identifies the time zone in which anti-passback is forgiven for all cardholders. Anti-passback must be configured.	All Panel Types.

Field	Description	Panel Type ...
Rep. Read Delay(s)	Defines the amount of time, in seconds, between card reads before it can be read again. Applicable to analog readers.	All Panel Types.
Verification Sweeps	Defines how many times the card has to be read before it can be verified. Applicable to analog readers.	All Panel Types.
Building Closed TZ	Defines the time zone in which the building is closed.	All Panel Types.
Bld. Closed Remind (m)	Defines the interval in which a log message is sent to the host reminding the operator the building should be closed. It is based on the building closed time zone.	All Panel Types.
Bld. Mode Station MP	This function is currently not supported.	
Bld. Open Indicator	This function is currently not supported.	
Bld. Limited Indicator	This function is currently not supported.	
Bld. Closed Indicator	This function is currently not supported.	

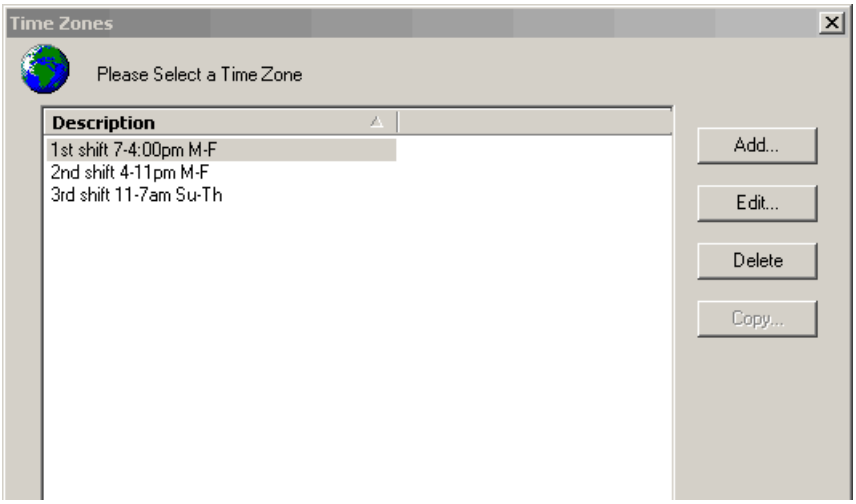
13.6.3 Time Zones Tab

The Time Zones tab enables you to add time zones to the panel. Only times zones that have been added to the panel are available to configure applicable panel and reader fields.



To add a time zone to the panel:

1. Click **Add** to display the **Time Zones** dialog box.



2. Select the time zone and click OK.

If the time zone you want does not appear in the dialog box you can create a new time zone.

To add a new time zone:

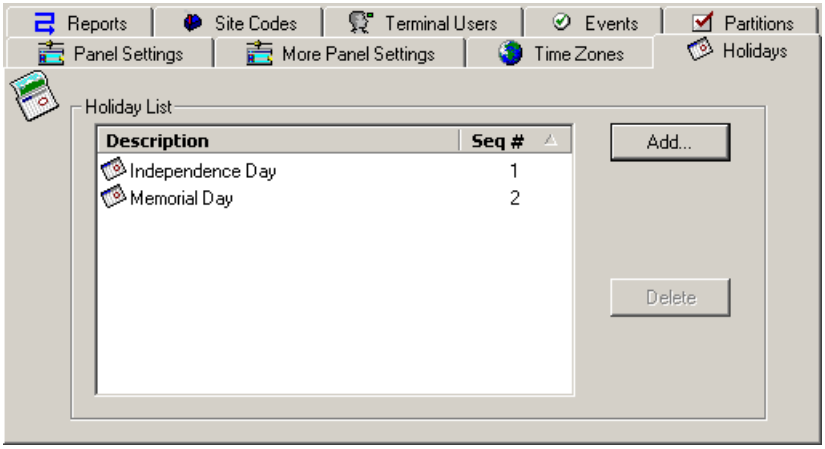
Click **Add** in the Time Zone dialog box.

To complete adding a new Time Zone:

See "DBC - Time Zones" in Chapter 57.

13.6.4 Holidays Tab

Holidays enable you to edit normal Time Zone behavior on specific days. You can enable connected panels to restrict access on holidays.



To add a holiday to the panel:

1. Click **Add.**
2. Select the sequence number from the drop-down list.
3. Click the icon next to the Holiday field.
4. Click Define.
5. Select the holiday from the Holiday List dialog box and click OK.
6. Click OK again at the Select Holiday dialog box.

If the holiday you want does not appear in the Holiday List dialog box you can create a new holiday.

To add a new holiday:

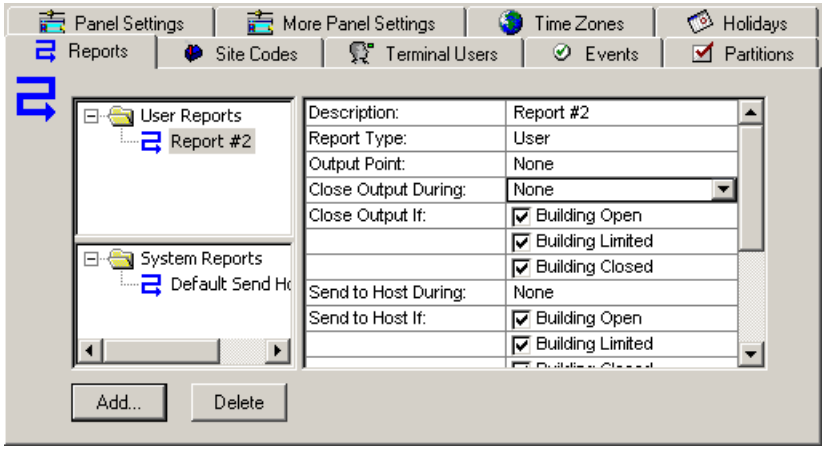
Click **Add** within the Holiday List dialog box.

To complete adding a new holiday:

See "DBC - Holidays" in Chapter 49.

13.6.5 Reports Tab

The Reports tab displays the user and system reports. System reports are coded and cannot be edited or deleted.



To add a report:

1. Click **Add** and use the following field definitions to set its parameters:

Field	Description
Description	Provides the description of the report.

Field	Description
Report Type	Defines the report as system or user.
Output Point	Defines the output point for the report.
Close Output During	Defines the time zone in which the output is closed (activated) in the event the report occurs within that time zone.
Close Output If	See Below.
Building Open	When enabled, when the building is open the output closes (activates).
Building Limited	When enabled, when the building is limited the output closes (activates).
Building Closed	When enabled, when the building is closed the output closes (activates).
Send to Host During	Defines the time zone in which the log is sent to the host.
Send to Host If	See Below.
Building Open	When enabled, logs are sent to the host when the building is open.
Building Limited	When enabled, logs are sent to the host when the building is limited.
Building Closed	When enabled, logs are sent to the host when the building is closed.
Close Latched During	Defines the time zone in which the output is closed (activated) and latched in the event the report occurs within that time zone.
Closed Latched If	See Building Open, Building Limited, and Building Closed below.
Building Open	When enabled, when the building is open the output closes (activates) and is latched.
Building Limited	When enabled, when the building is limited the output closes (activates) and is latched.
Building Closed	When enabled, when the building is closed the output closes (activates) and is latched.

Field	Description
Prevent Building Closure	When enabled, prevents the building from closure.
Print * with Log	When enabled, places an asterisk in front of the log comment.

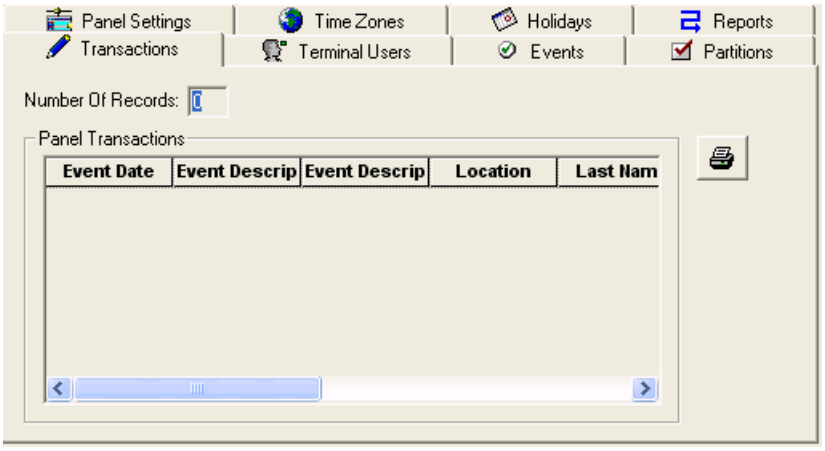
To delete a report:

1. Select the report.
2. Click Delete.

Note: Also see SEEP Interlocks Tab, page 36 within Hardware Templates or "Adding a SEEP Logical Device".

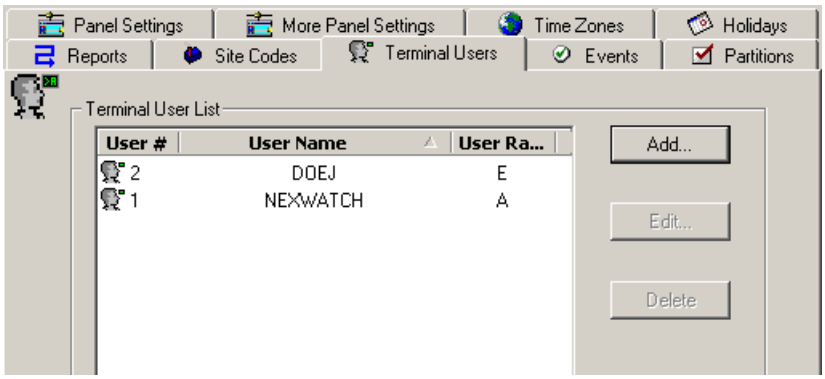
13.6.6 Transactions Tab

The Transactions tab displays the panel's events and provides event data. The Transaction tab does not display events generated from sub-hardware.



13.6.7 Terminal Users Tab

The Terminal Users tab allows you to add additional users with access to terminal mode.



To add a Terminal User:

1. Click **Add.**
2. Select the User Number from the drop-down list.
3. Enter the User Name.
4. Enter the User Rank [A-F]. The User Rank determines user access within Terminal (see your SEEP Panel manual for Terminal

instructions), with rank A having the greatest access and rank F having the most restricted.

5. Enter the User Password and click OK.

13.6.7.1 Events Tab

The Events tab displays the default event types that are applicable to the SEEP panel.

To define an event:

Either double-click the event you want to define or select and click **Edit**. The "HW Config - Edit Point" in Chapter 25 dialog box appears.

For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

13.6.7.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. For information about creating a partition, see "DBC - Partitions" in Chapter 53. Use this function to assign or delete an already-created partition to the panel.

To assign a partition to the panel:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition and click Add.

To delete a partition from the Partitions List dialog box:

1. Select the partition.
2. Click Delete.

After completing each tab within the panel, you must save the panel configuration.

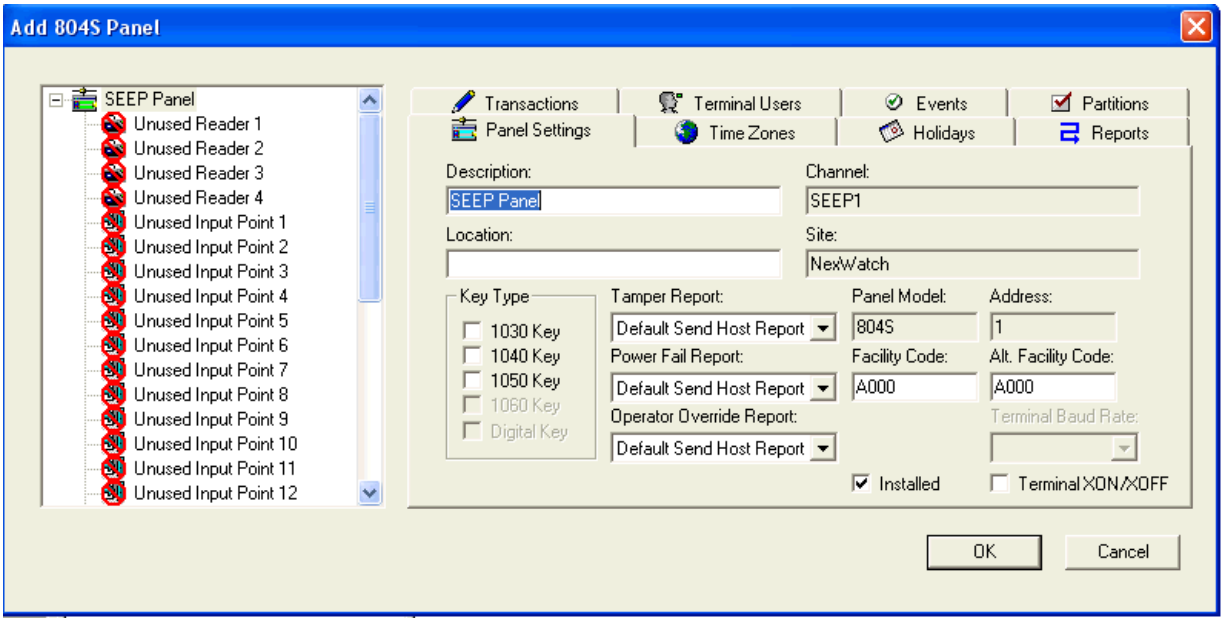
To save the panel configuration:

Click **OK** at the Add [Panel Name] Panel dialog box**.**

13.7 Editing a SEEP Panel

To edit a panel:

1. In the Pro-Watch Hardware Configuration tree, click the site to which the panel is assigned and then click the Panel's subdirectory. The icons of the existing panels appear in the right pane of the window.
2. Right-click the panel you want to edit, and select Properties. The Edit [Panel Name] Panel dialog box appears.



3. Complete each tab to configure the panel. See the following tab list and the corresponding tab sections in "Configuring a SEEP Panel" for the configuration information:

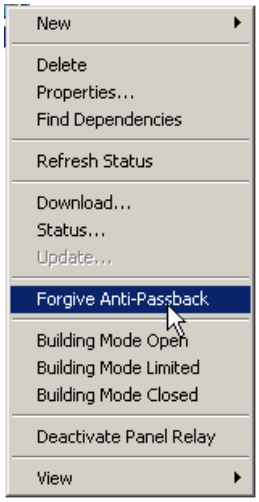
EDIT A PANEL TABS LIST

- "Panel Settings Tab".
- "More Panel Settings Tab".
- "Time Zones Tab".
- "Holidays Tab".
- "Reports Tab".
- "Transactions Tab".
- "Terminal Users Tab".
- "Events Tab".
- "Partitions Tab".

The SEEP panel(s) allows you to forgive anti-passback (see "DBC - Area" in Chapter 29) for all cards.

To forgive anti-passback:

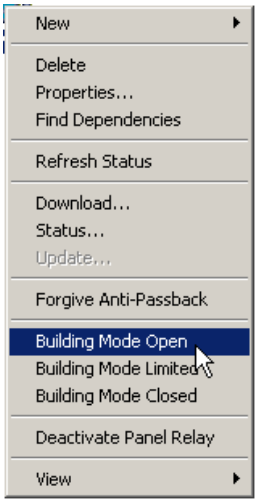
1. Select the panel from the Hardware Configuration window.
2. Right-click on the panel.
3. Select Forgive Anti-Passback:



The SEEP panel(s) also allows you to manually change building modes from the host.

To change building modes:

1. Select the panel from the Hardware Configuration window.
2. Right-click on the panel and select the building mode (Building Mode Open, Building Mode Limited, Building Mode Closed). Note that you can also select a SEEP building mode under event triggers.



See your SEEP manual for more information on building modes.

13.8 Viewing and Editing Dependencies of a SEEP Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

13.9 Deleting a SEEP Panel

Please refer to How to Delete a Panel, page 53.

13.10 Adding a SEEP Logical Device

A Logical Device is a single physical device or group of selected physical devices, which are defined by a hardware template. For example, a template may define a door that is equipped with a card reader, a REX input device, and a door strike output device as one Logical Device.

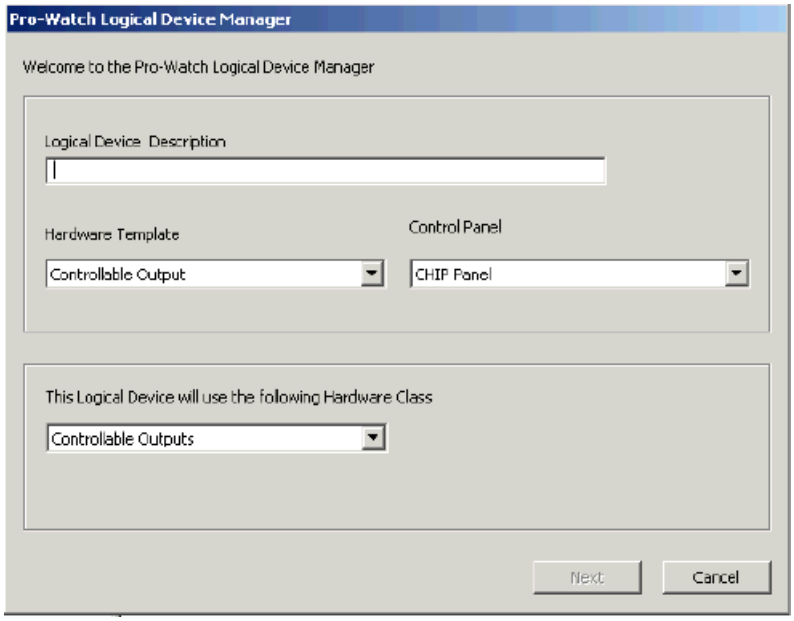
As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system. For example, you can assign the door, reader, input device, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you create Logical Devices, you must create the following:

- Site. See "Adding a SEEP Channel".
- Channel. See "Adding a SEEP Channel".
- Panel. See "Adding a SEEP Panel".
- Hardware Template. See Adding or Editing a Hardware Template, page 28.

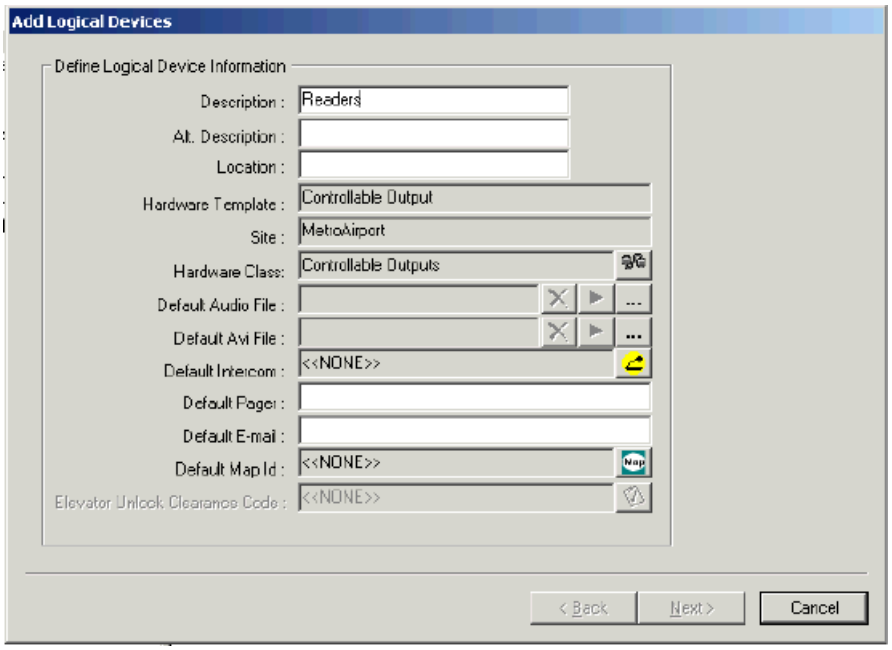
To add a Logical Device:

1. From the Pro-Watch Hardware Configuration tree view, right-click the site to which you want to assign the Logical Device, and select **New > Logical Device**. The Pro-Watch Logical Device Manager dialog box appears:



2. Enter a description that will identify the Logical Device in the Logical Device Description field.

3. Select the desired Hardware Template from the drop-down list in the Hardware Template field.
4. Select the desired Hardware Class from the drop-down list in the Hardware Class field.
5. Click Next to display the Add Logical Devices dialog box.

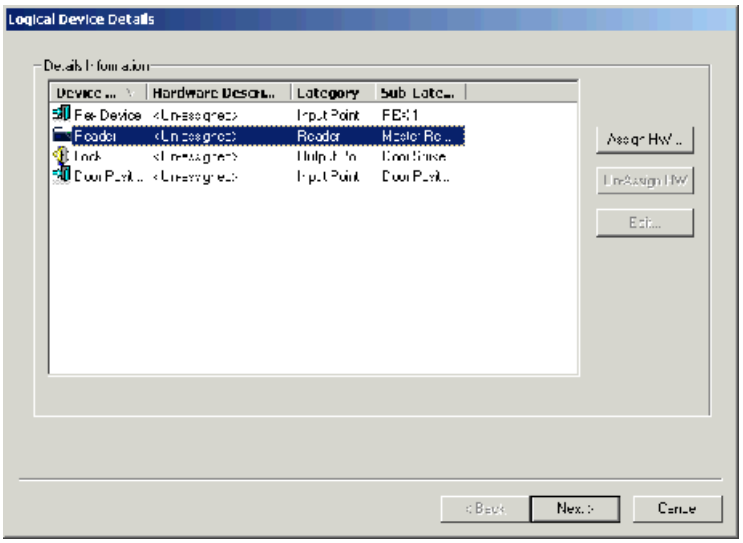


6. Use the following table to complete the Define Logical Device field entries:

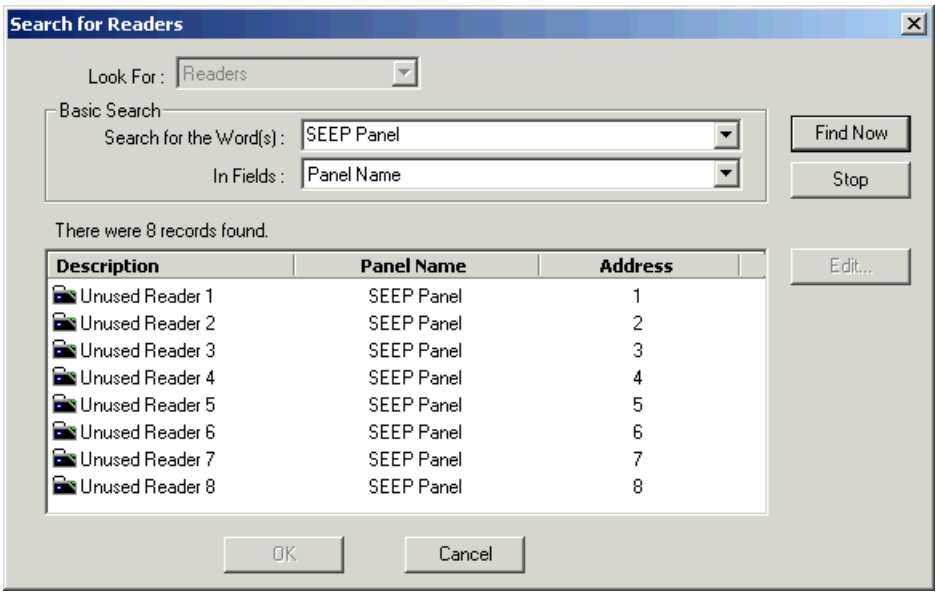
Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned.

Field	Description
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. See "DBC - Clearance Codes" in Chapter 37 for more information.

7. Click Next to display the Logical Device Details dialog box:



8. Select a device type and click Assign HW to display the Search for [Device Type] dialog box.



9. Enter the description in the ‘search for words’ field; this is the description that will be used to search for available addresses.
10. Select the field name from the ‘in fields’ drop-down list and click Find Now.
11. Select the record and click OK.
12. Repeat step 5 through step 9 until all device types have been assigned.
13. Click Next. The Default CCTV Information dialog box appears.

14. CCTV may be associated with Logical Devices. You may assign the default view and commands for this device. See "HW Config - CCTV" in Chapter 21 for more information. To assign a Default Command or View, click the icon and select the command or view. Click OK and then click Next. The Partitions dialog box appears.
15. To assign a partition to this Logical Device, click Add, select the partition, and click Add again. For information about partitions, see "DBC - Partitions" in Chapter 53.
16. Click Finish to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the type of SEEP panel. The table below outlines the various SEEP panel types as well as their Logical Device capabilities:

Panel ...	Inputs/Outputs ...	Readers
804S	16/12	4
804SN	16/12	4
804SX	16/12	4
804SXT	16/12	4
808S	32/16	8
808SN	32/16	8
808SX	32/16	8
808SXT	32/16	8
818SC	32/16	8
SE4100	32/16	8
Star I	Assigned through the Host: 32/16 Assigned through Terminal: 64/32.	2, 4, 8 (Dependent on personality chip).

13.11 Editing a SEEP Logical Device

Logical Devices can be configured or edited after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices will already be configured. See Adding or Editing a Hardware Template, page 28.

It is a good idea to visit the Logical Device configuration tabs, as these tabs contain additional fields hardware templates do not.

To configure a Logical Device:

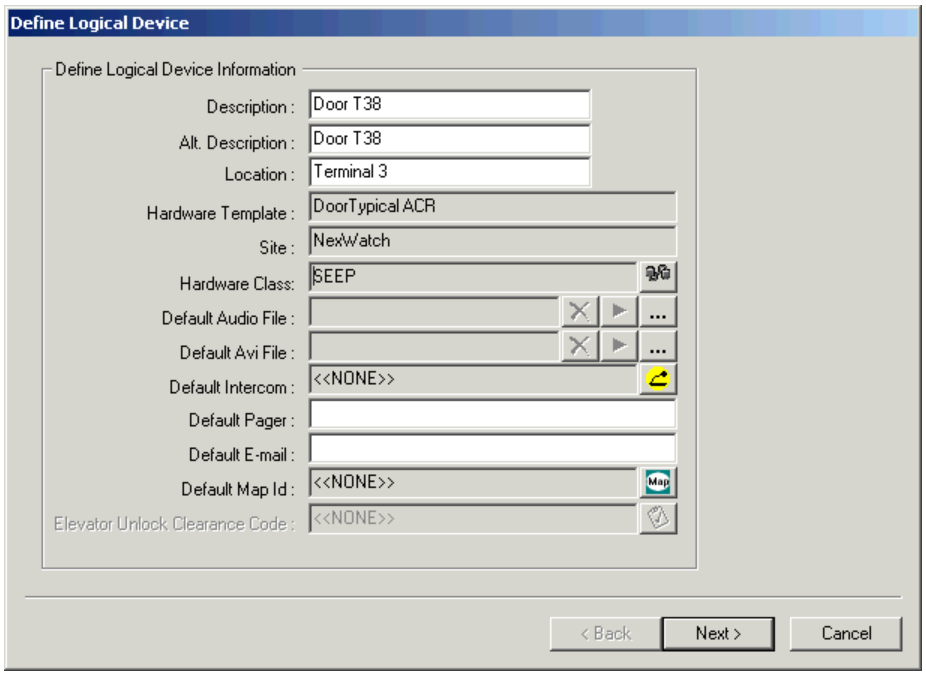
1. Click the appropriate Logical Device folder in the Hardware Configuration screen to display the site's existing Logical Devices.
2. Right-click the Logical Device you want to configure, and select Properties. The Edit Logical Devices [Logical Device name] screen appears. The screen contains six information tabs. Complete the following information tabs to configure the Logical Device:

EDIT A LOGICAL DEVICE TABS LIST

- "Define Logical Device Tab".
- "Logical Device Details Tab".
  - Readers
    - "Door Properties Tab".
    - "Door Settings Tab".
    - "REX/Keypad/Sensor Tab".
    - "Events Tab".
  - Input Points
    - "Input Tab".
    - "Events Tab".
  - Output Points
    - "Output Tab".

* "Events Tab".

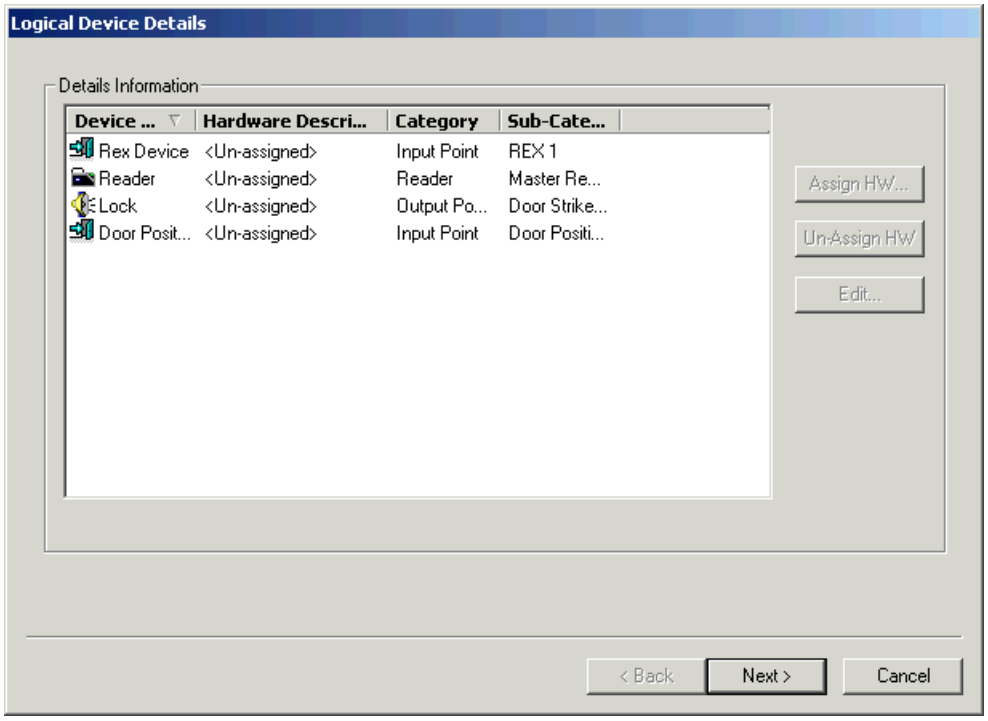
13.11.1 Define Logical Device Tab



Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned.
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.

Field	Description
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. See "DBC - Clearance Codes" in Chapter 37 for more information.

13.11.2 Logical Device Details Tab



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click OK.

To un-assign a device type:

Click to select the device type and click **Un-Assign HW**.

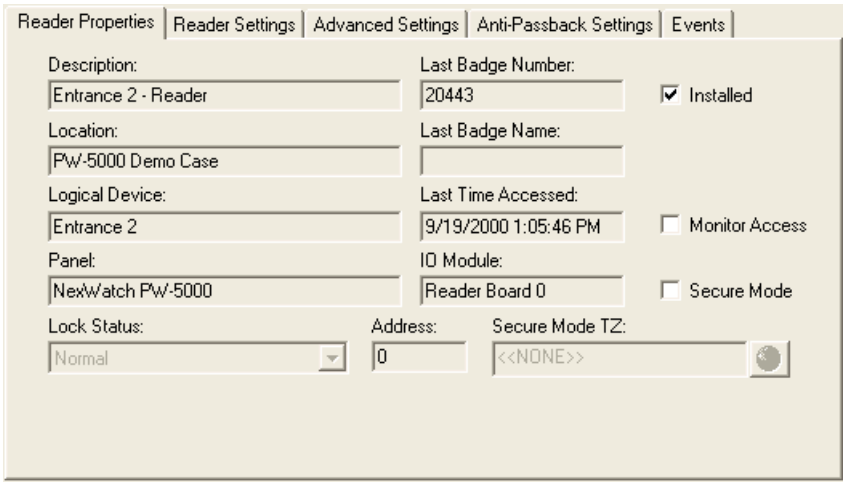
To edit the current configuration of a device type:

Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete.

Use the appropriate section below to edit or configure the device type you have selected.

13.11.3 Readers

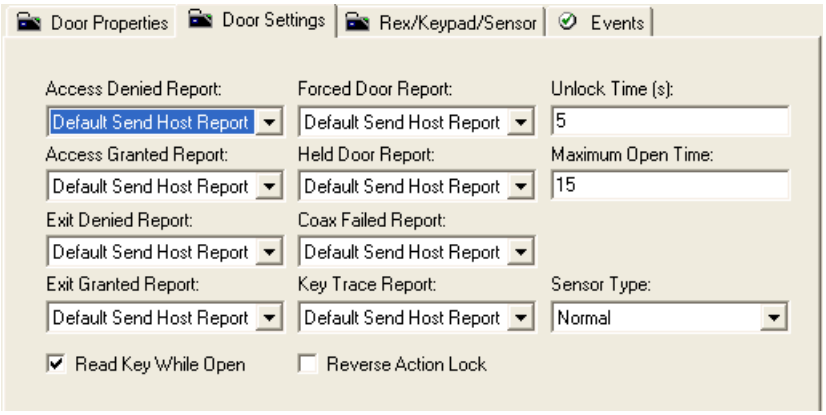
Door Properties Tab



Field	Description
Description	Provides the description of the Logical Device.
Location	Defines the physical location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel	Identifies the panel in which the Logical Device is assigned.
Lock Status	Defines the lock status of a door (locked, open, normal).
Address	Identifies the address of the Logical Device.
Last Card Number	Identifies the card number of the last card to be presented to the Logical Device.
Last Badge Name	Identifies the badgeholder name of the last badge that was presented to the Logical Device.
Last Time Accessed	Identifies the last time the Logical Device was accessed.
Auto Unlock Time Zone	Defines the time zone in which a reader automatically unlocks.

Field	Description
Monitor Access	Enables monitored access (card trace) on a reader.
Installed	Required for the Logical Device to be installed and operational.

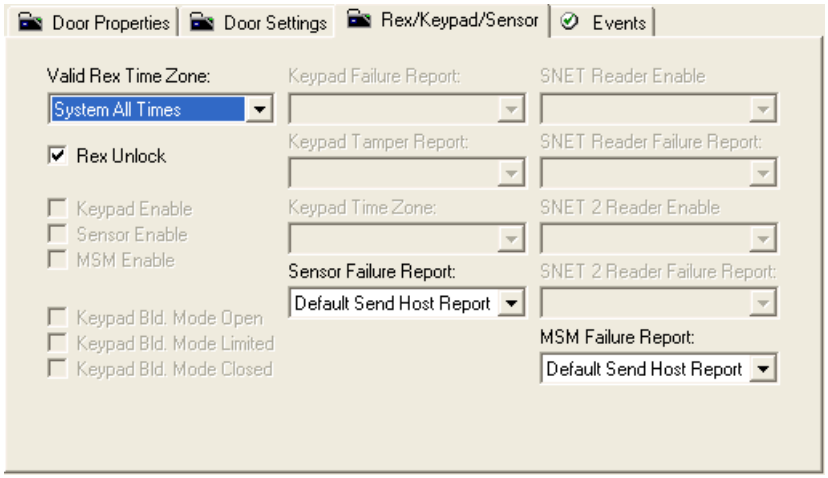
Door Settings Tab



Field	Description
Access Denied Report	Defines the report upon an access denied event.
Access Granted Report	Defines the report upon an access granted event.
Exit Denied Report	Defines the report upon an exit denied event.
Exit Granted Report	Defines the report upon an exit granted event.
Read Key While Open	Allows for additional cards to be read while the door is open.
Forced Door Report	Defines the report upon a forced door event.
Held Door Report	Defines the report upon a held door event.
Coax Failed Report	Defines the report upon a coax failed event (Analog panels only).
Key Trace Report	Defines the report on a key trace event.

Field	Description
Reverse Action Lock	Allows the lock to act as a fail-safe device such as a MagLock; the lock relay is activated to close the normally open contacts to lock the device.
Unlock Time(s)	Defines the amount of time a door remains unlocked after a valid card read.
Maximum Open Time	Defines the maximum amount of time a door can be held open before an alarm is sent.
Passback Type	Defines the passback type for the reader. The reader must be part of an area. See "DBC - Area" in Chapter 29.
Sensor Type	Defines the reader type for building modes. See your SEEP manual for more information on building modes.

REX/Keypad/Sensor Tab

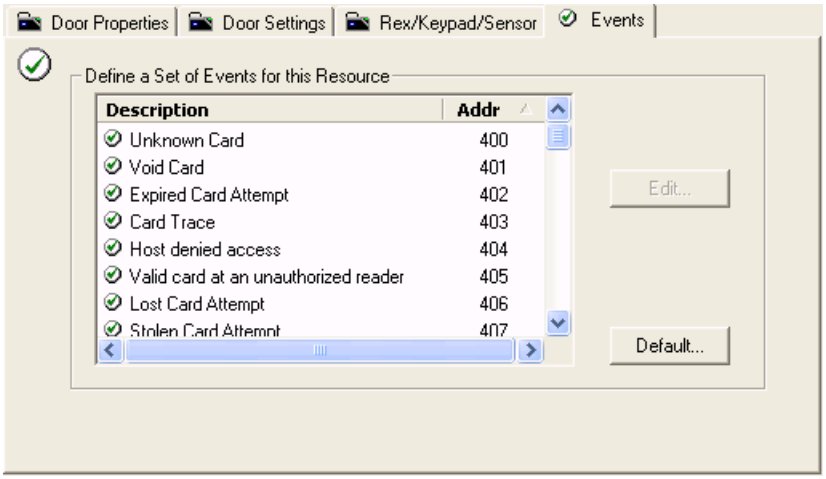


Field	Description	Panel Type
Valid REX Time Zone	Defines the time zone a REX is valid.	All Panel Types.
REX Unlock	When enabled, requires the use of the REX button for the door to unlock. A time zone must be defined.	818SC, SE4100, Star I.

Field	Description	Panel Type
Keypad Enable	Enables the keypad on a keypad reader. A time zone must be defined.	818SC, SE4100, Star I.
Sensor Enable	Required for analog readers to be enabled. Sensor is an alternative term for readers.	804S, 804SN, 804SX, 804SXT, 808S, 808SN, 808SX, 808SXT.
MSM Enable	A Multiple Switch Monitor must be enabled to allow for a REX and DPS to be assigned.	804S, 804SN, 804SX, 804SXT, 808S, 808SN, 808SX, 808SXT.
Keypad Bld. Mode Open	Enables the keypad when the building mode is Open. May be used in lieu of a keypad time zone. See your SEEP manual for more information on building modes.	818SC, SE4100, Star I.
Keypad Bld. Mode Limited	Enables the keypad when the building mode is Limited. May be used in lieu of a keypad time zone. See your SEEP manual for more information on building modes.	818SC, SE4100, Star I.
Keypad Bld. Mode Closed	Enables the keypad when the building mode is Closed. May be used in lieu of a keypad time zone. See your SEEP manual for more information on building modes.	818SC, SE4100, Star I.
Keypad Failure Report	Defines the report upon a keypad failure event.	818SC, SE4100, Star I.
Keypad Tamper Report	Defines the report upon a keypad tamper event.	818SC, SE4100, Star I.
Keypad Time Zone	Defines the time zone a keypad is active.	818SC, SE4100, Star I.
Sensor Failure Report	Defines the report upon a sensor failure event.	All Panel Types.

Field	Description	Panel Type
S-Net Reader Enable	Defines the reader type. Required to enable a reader. If the reader is a PIN only reader, this field must be set to disable.	818SC, SE4100, Star I.
S-Net Reader Failure Report	Defines the report upon an S-Net reader failure event.	818SC, SE4100, Star I.
S-Net 2 Reader Enable	Defines the second reader type. Required to enable a second reader. There cannot be two of the same reader types with the same address; the reader types must differ. A single magstripe reader must have both S-Net fields defined.	818SC, SE4100, Star I.
S-Net 2 Reader Failure Report	Defines the report upon an S-Net 2 reader failure event.	818SC, SE4100, Star I.
MSM Failure Report	Defines the report upon an MSM failure event.	804S, 804SN, 804SX, 804SXT, 808S, 808SN, 808SX, 808SXT.

Events Tab



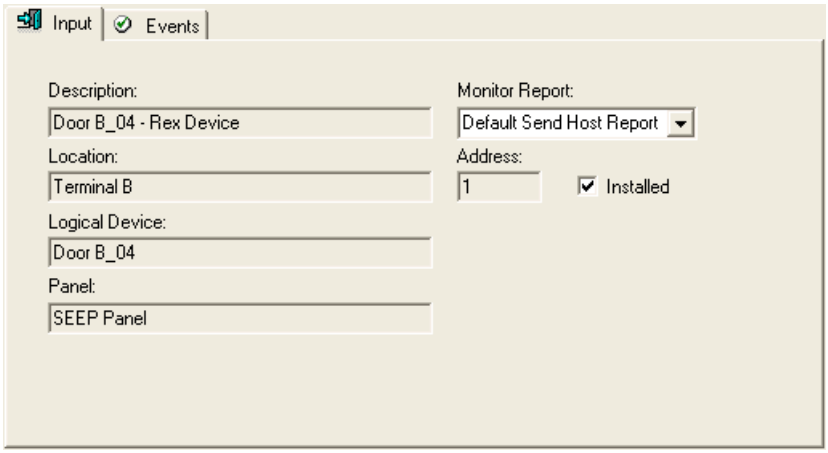
To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears.

For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

13.11.4 Input Points

Input Tab



Field	Description
Description	Provides the description of the Logical Device.
Location	Defines the location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel	Identifies the panel in which the Logical Device is assigned.
Monitor Report	Defines the report associated with the monitor input point. The report initiates upon a change of state.
Address	Identifies the address of the Logical Device.
Installed	Required for the Logical Device to be enabled and operational.

Events Tab

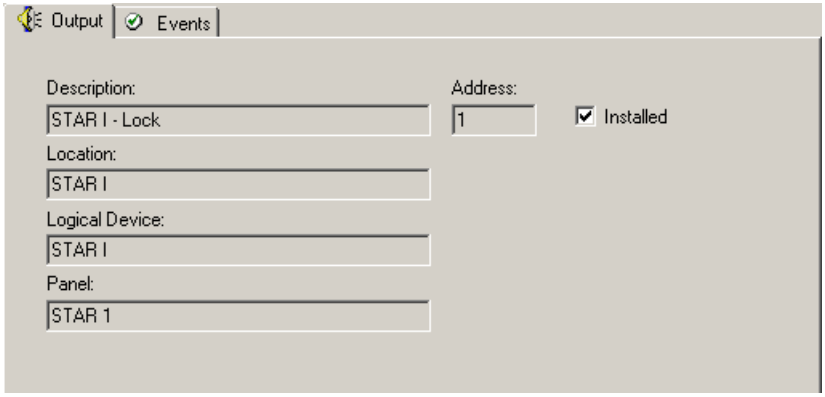
To define an event:

Either double-click the event you want to define, or select and click **Edit**. The Edit Point dialog box appears.

For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

13.11.5 Output Points

Output Tab



Field	Description
Description	Provides the description of the Logical Device.
Location	Defines the location of the Logical Device as defined by the user.
Logical Device	Identifies the name of the Logical Device.
Panel	Identifies the panel in which the Logical Device is assigned.
Address	Identifies the address of the Logical Device.
Installed	Required for the Logical Device to be enabled and operational.

Events Tab

To define an event:

1. Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.
2. Click the Default CCTV Information tab. The default CCTV information was configured while adding Logical Devices, if the Logical Devices included CCTV information.
3. Click the SEEP Interlocks tab. For more information see SEEP Interlocks Tab, page 36 within Hardware Templates.
4. Click the Transactions tab. The Transactions tab displays all the transactions that have occurred at that particular reader. The number of records will also be displayed. The option to print transactions is also available.
5. Click the Partitions tab. To complete configuration, see "DBC - Partitions" in Chapter 53.

13.12 Viewing and Editing Dependencies of a SEEP Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 53.

13.13 Deleting a SEEP Logical Device

Please refer to How to Delete a Logical Device, page 53.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - SmartPlus Mobile

14

In this chapter ...

Overview
Adding a SmartPlus Mobile Channel
Viewing and Editing Dependencies of a SmartPlus Mobile Channel
Deleting a SmartPlus Mobile Channel
Adding a SmartPlus Panel
Viewing and Editing Dependencies of a SmartPlus Mobile Panel
Deleting a SmartPlus Mobile Panel
Adding a SmartPlus Mobile Logical Device
Editing a SmartPlus Mobile Logical Device
Viewing and Editing Dependencies of a SmartPlus Mobile Logical Device
Deleting a SmartPlus Mobile Logical Device

14.1 Overview

This chapter describes how to configure a site that uses a SmartPlus panel.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 6-46.
- How to View and Edit Dependencies of a Site, page 6-48.
- How to Delete a Site, page 6-48.

14.2 Adding a SmartPlus Mobile Channel

The Pro-Watch channel is the communications path between the host and the panel. You must identify the channel before adding a panel and Logical Device.

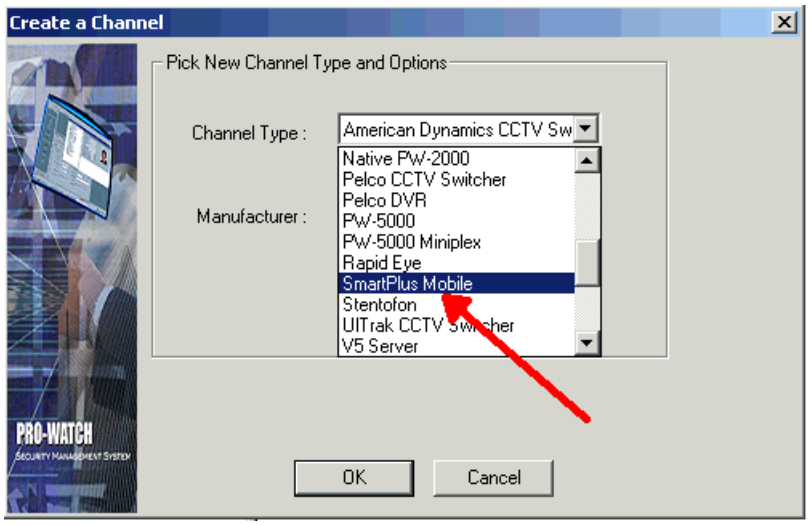
Note: The recommended maximum number of channels per site is 99.

To add a channel:

1. Select a Channel Type:

   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.

   b. Select **SmartPlus Mobile** from the drop-down list



   c. Click **OK**. The Define Channel Information dialog box appears.

2. Define the Channel:

   a. In the Define Channel Information dialog box, enter an identifying channel description.

   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.

   c. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.

   d. In the Attempts field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.

   e. In the Poll Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds.

f. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.

g. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.

h. Click **Next** to display the Communications Parameters dialog box.

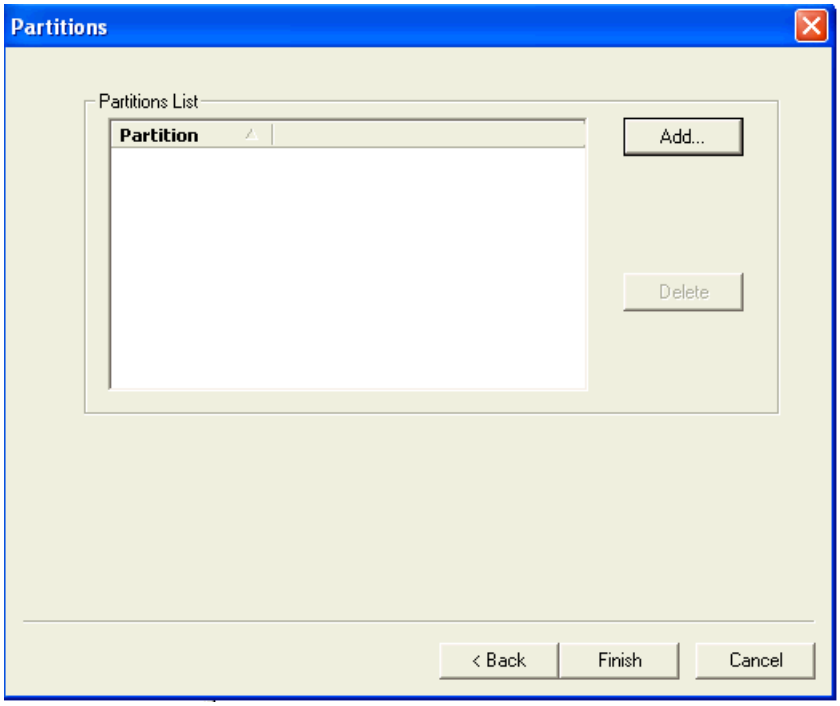
3. Set Communications Parameters:

a. Select the port type from the following drop-down list options:

Option	Description
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
TCP/IP	Specifies that the channel is a network connection. IP Address – the IP address of the panel.

b. If you are using the TCP/IP port on the server, enter the SmartPlus Mobile panel's IP address, the port number, a user name and password with SmartPlus Mobile access, and a new poll interval and retry time if desired. The poll interval sets the number of seconds that elapses between each poll by the host computer. The retry time sets the number of seconds that must elapse before a communications retry will be attempted.

c. Click **Next** to display the Partitions dialog box.



If you are using Pro-Watch partitions, click **Add** to add the partition to which the channel will be assigned. For information about adding partitions, see "DBC - Partitions" in Chapter 53. If you are not using Pro-Watch partitions, leave this box blank.

4. Click **Finish** to complete the channel configuration. A warning appears reminding you that no events on this channel can be reported until you add the channel to the appropriate Routing Group in Database Configuration. See "DBC - Status Groups" in Chapter 56. If you are not using Routing Groups, Pro-Watch adds the channel to the default routing group automatically.



5. Click **OK**. The new channel is complete.

14.3 Viewing and Editing Dependencies of a SmartPlus Mobile Channel

Use this function to view and modify the Channel's dependencies. The Channel object depends upon the Site and Routing Group objects.

To view and modify a Channel's dependencies:

1. Right-click the icon of an existing Channel in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Channel's dependencies.
2. To modify or remove the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

14.4 Deleting a SmartPlus Mobile Channel

Use this function to delete a Channel from the Pro-Watch database.

1. In the Pro-Watch Hardware Configuration tree list, click **Channels** to display the Channel icons in the right pane.

Note: Right-click the Channel you want to delete and select **Delete**.

You cannot delete a Channel that has dependencies. A dependency is another database object that includes the Channel in its configuration. The Channel object depends upon the Site and Routing Group objects. If the Channel has no current dependencies, you are prompted to confirm the deletion. However, if the Channel does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Channel:

    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.

    b. Either change or delete each of the objects listed as dependencies.

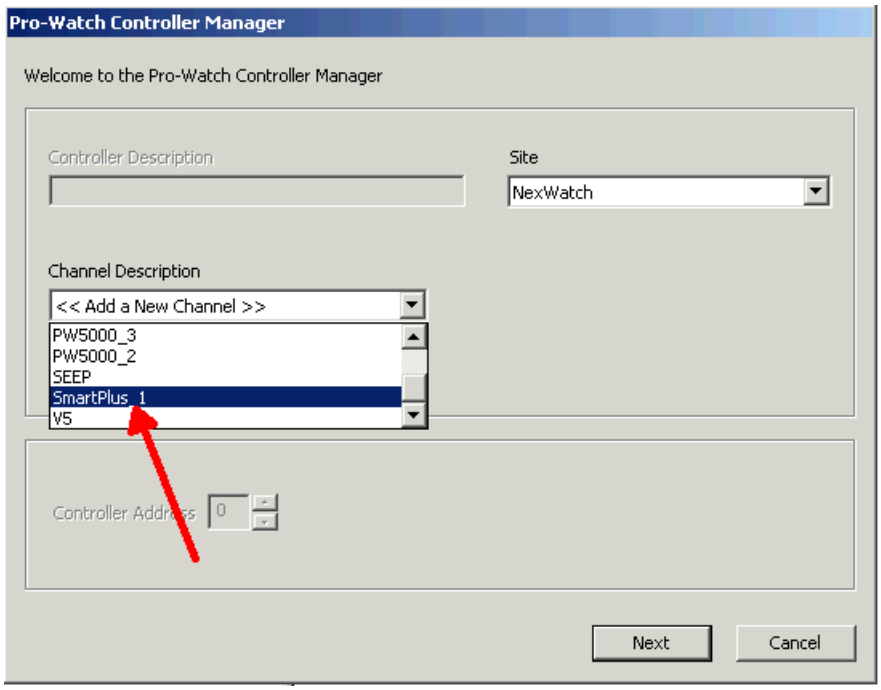
Repeat step 2 and click **Yes** at the prompt to delete the channel.

14.5 Adding a SmartPlus Panel

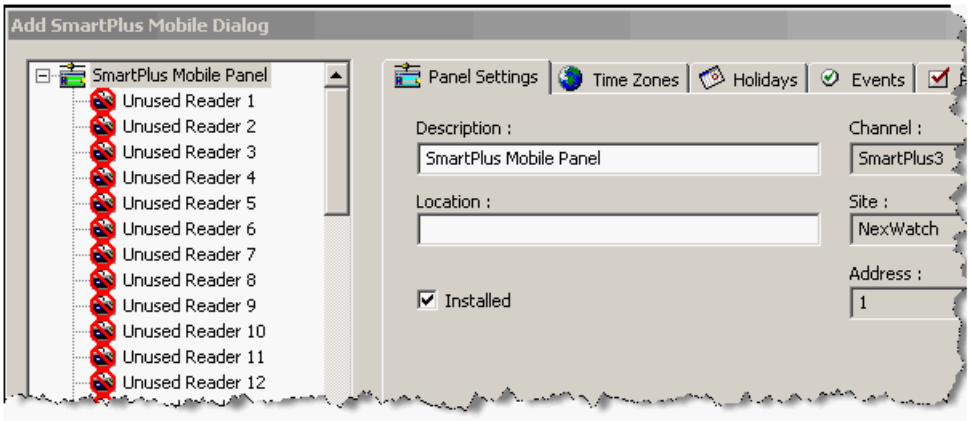
To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 6-4.

To add a SmartPlus Mobile panel:

1. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
2. Select **New > Panel** to display the Pro-Watch Controller Manager dialog box.
3. In the Channel Description field, select the SmartPlus Mobile channel you have created for the panel.



4. Click **Next** to display the Add SmartPlus Mobile dialog box.



5. Perform the following:
   a. If you desire, revise the default description in the Description field on the Panel Settings tab.
   b. Enter an identifiable location of the panel in the Location field.
6. Select the Time Zones tab to assign any additional Time Zones you desire. Click **Add** to display the Time Zones dialog box, select any of the available Time Zones listed, and click **OK**.
7. Select the Holidays tab to define holidays:
   a. Click **Add.**
   b. Select the sequence number from the drop-down list.
   c. Click the icon next to the Holiday field.
   d. Click **Define**.
   e. Select the holiday from the Holiday List dialog box and click **OK**.
   f. Click **OK** again at the Select Holiday dialog box.
8. Select the Events tab to define events reported by the panel. To edit an event, either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25. To re-set the event configuration to the default setting, click **Default**.
9. Select the Partitions tab to assign Pro-Watch partitions. Click the **Add** button to display a list of the available partitions that have already been created in Pro-Watch (see "DBC - Partitions" in Chapter 53 for instructions) appears. Select the desired partitions and click **Add**: The added partitions are now available to be assigned to users and classes.
10. Click **OK** at the bottom of the Add SmartPlus Mobile dialog box to create the new panel.

14.6 Viewing and Editing Dependencies of a SmartPlus Mobile Panel

Please refer to How to View and Edit Dependencies of a Panel, page 6-52.

14.7 Deleting a SmartPlus Mobile Panel

Please refer to How to Delete a Panel, page 6-53.

14.8 Adding a SmartPlus Mobile Logical Device

A Pro-Watch Logical Device is a single physical device or group of selected physical devices, which are defined by a hardware template. For example, a template may define a door that is equipped with a card reader, a REX input device, and a door strike output device as one Logical Device.

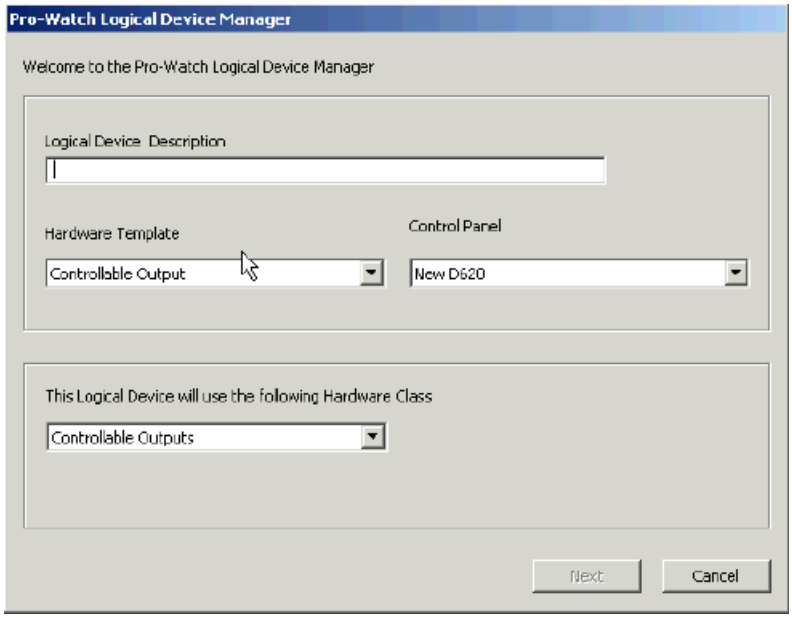
As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system. For example, you can assign the door, reader, input device, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you create Logical Devices, you must create the following:

- Site. See "Adding a SmartPlus Mobile Channel".
- Channel. See "Adding a SmartPlus Mobile Channel".
- Panel. See "Adding a SmartPlus Panel".
- Hardware Template. See Adding or Editing a Hardware Template, page 6-28.

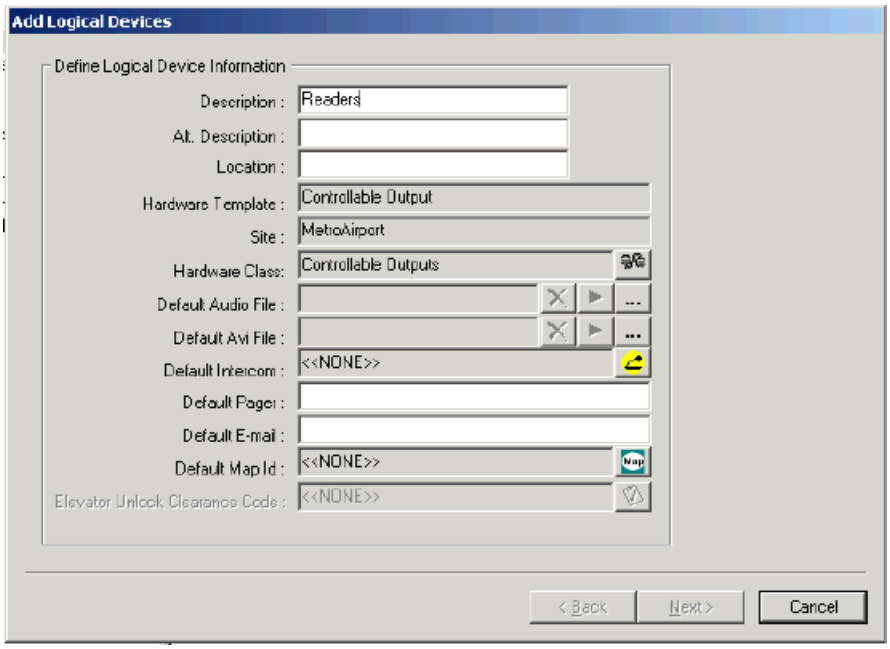
To add a Logical Device:

1. From the Pro-Watch Hardware Configuration tree view, right-click the site to which you want to assign the Logical Device, and select **New > Logical Device**. The Logical Device Manager dialog box appears:



2. Enter a description that will identify the Logical Device in the Logical Device Description field.
3. Select a Hardware Template from the drop-down list in the Hardware Template field.

4. Select a Hardware Class from the drop-down list in the Hardware Class field.
5. Click **Next**. The Add Logical Devices dialog box appears.

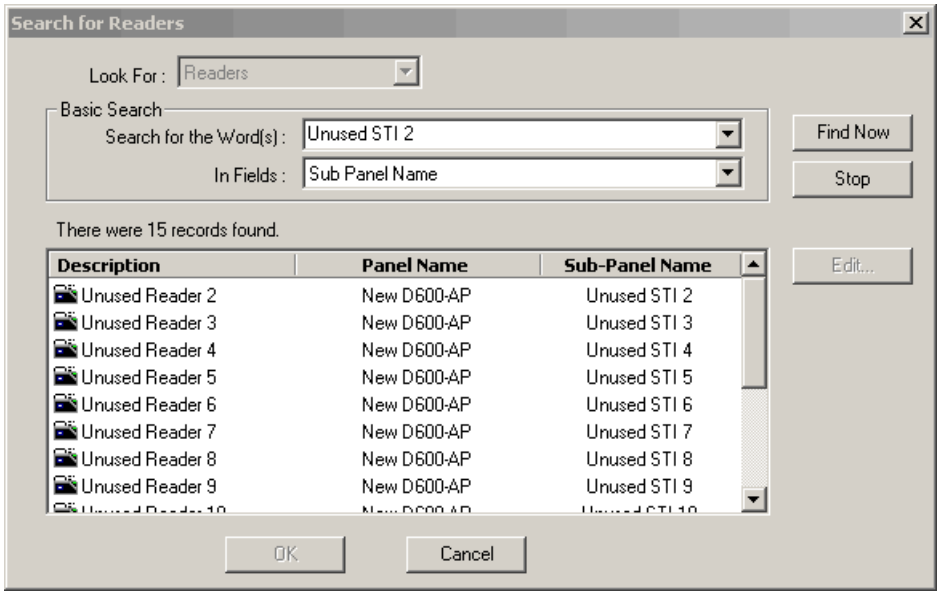


6. Use the following table to complete the Define Logical Device field entries:

Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 6-28.
Site	Identifies the Site in which the Logical Device is assigned
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 6-24.
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.

Field	Description
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. For more information, see "DBC - Clearance Codes" in Chapter 37.

7. Click **Next**. The Logical Device Details dialog box appears:
8. Select a device type and click **Assign HW** to display the Search for [Device Type] dialog box:



9. Enter the description in the 'Search for Word(s)' field; this is the description that is used to search for available addresses.
10. Select the field name from the 'In Fields' drop-down list and click **Find Now**.
11. Select the record and click **OK**.
12. Repeat step 5 through step 9 until all device types have been assigned.
13. Click **Next**. The Default CCTV Information dialog box appears.
14. CCTV may be associated with Logical Devices. You may assign the default view and commands for this device. For more information, see "HW Config - CCTV" in Chapter 21. To assign a Default Command or View, click on the icon and select the command or view. Click **OK** and then click **Next**. The Partitions dialog box appears.

15. To assign a partition to this Logical Device, click **Add**, select the partition, and click **Add** again. For information about partitions, see "DBC - Partitions" in Chapter 53.
16. Click **Finish** to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the number of STI sub-panels assigned. You can have a maximum of 16 STI sub-panels, 16 readers (1 reader per subpanel), 256 inputs (16 inputs per sub-panel), and 512 outputs (32 outputs per sub-panel).

14.9 Editing a SmartPlus Mobile Logical Device

Logical Devices can be configured or edited after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices will already be configured. See Adding or Editing a Hardware Template, page 6-28.

Tip: It is a good idea to visit the Logical Device configuration tabs, as these tabs contain additional fields hardware templates do not.

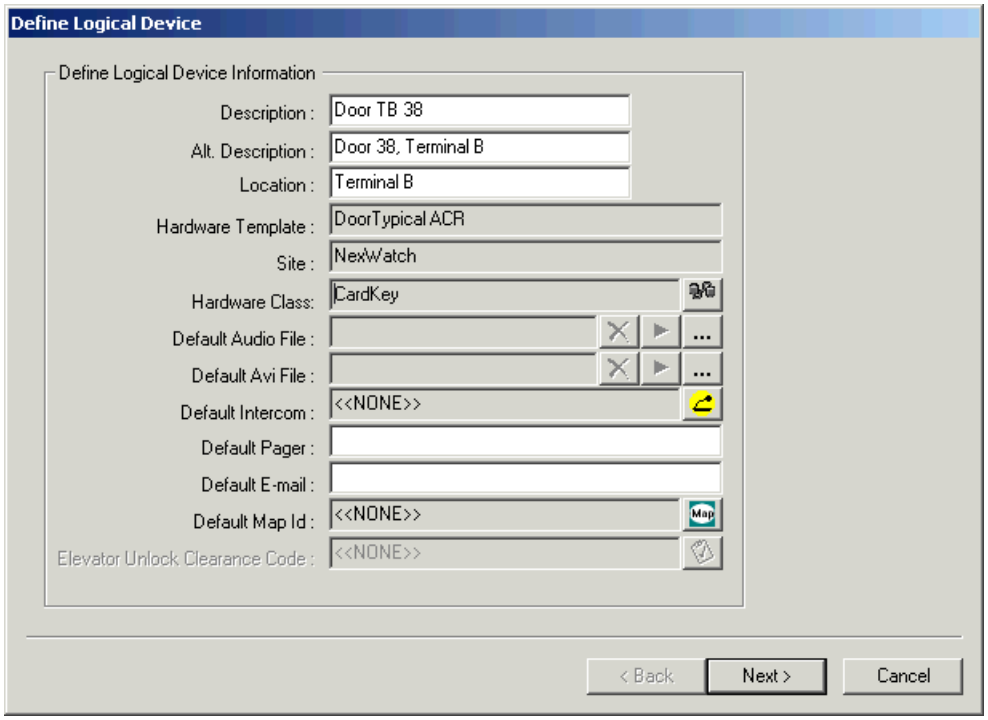
To configure a Logical Device:

1. Click the appropriate Logical Device folder in the Hardware Configuration screen to display the site's existing Logical Devices.
2. Right-click the Logical Device you want to configure, and select **Properties**. The Edit Logical Devices [Logical Device name] screen appears. The screen contains six information tabs. Complete the following information tabs to configure the Logical Device:

EDITING SmartPlus Mobile LOGICAL DEVICES TABS LIST

- "Define Logical Device Tab".
- "Logical Device Details Tab".
  - "Readers"
    - Reader Information Tab.
    - Configuration Tab.
    - Events Tab.
  - "Input Points"
    - Input Point Information Tab.
    - Configuration Tab.
    - Events Tab.
  - "Output Points"
    - Output Point Information Tab.
    - Configuration Tab.
    - Events Tab.
- "Default CCTV Tab".
- "Transactions Tab".
- "Partitions Tab".

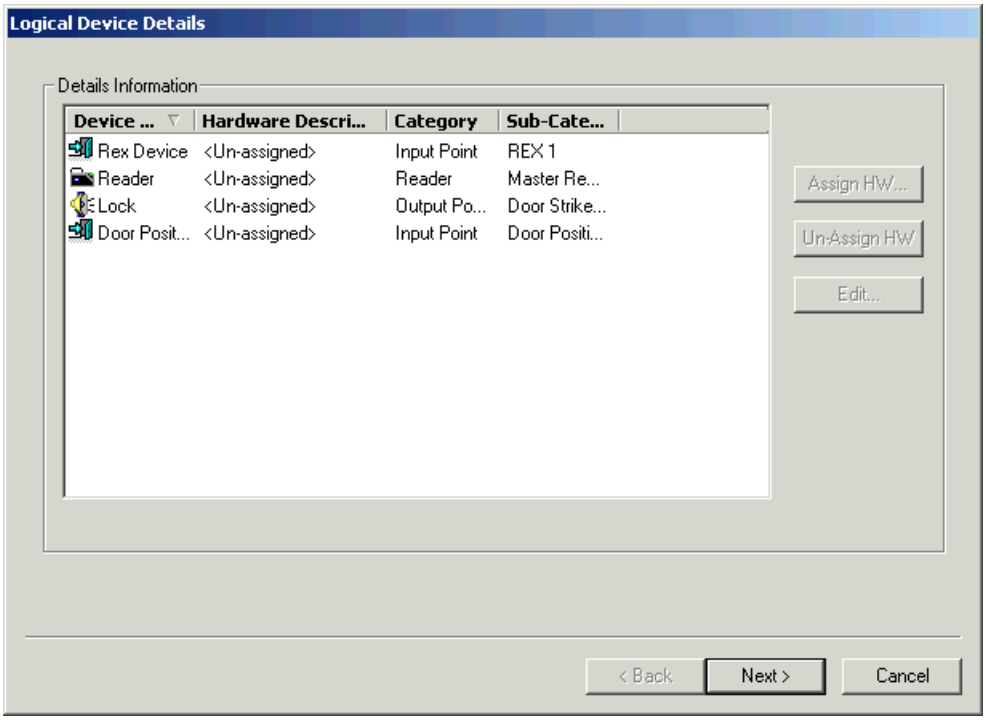
14.10 Define Logical Device Tab



Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 6-28.
Site	Identifies the Site in which the Logical Device is assigned
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 6-24.

Field	Description
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. For more information, see "DBC - Clearance Codes" in Chapter 37.

14.10.1 Logical Device Details Tab



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click **OK**.

To un-assign a device type:

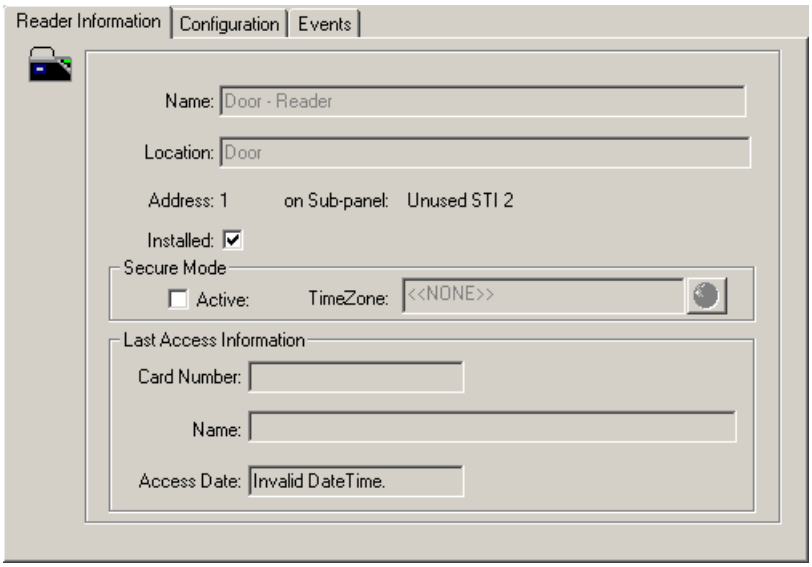
1. Click to select the device type and click **Un-Assign HW**.

To edit the current configuration of a device type:

1. Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete.
2. Use the appropriate section below to edit or configure the device type you have selected.

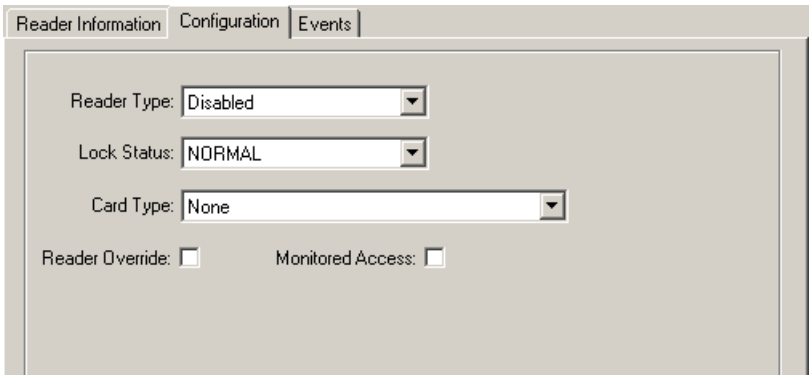
14.10.2 Readers

Reader Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.
Installed	Required for the Logical Device to be enabled and operational.
Active (Secure Mode)	Enables secure mode for a particular door. See Appendix A, Secure Mode Verification.
Time Zone (Secure Mode)	Defines the time zone during which the reader is in secure mode.
Card Number (Last Access)	Identifies the card number which accessed the Logical Device last.
Name (Last Access)	Identifies the name of the badgeholder who last accessed the Logical Device.
Access Date	Identifies the date of last access.

Configuration Tab



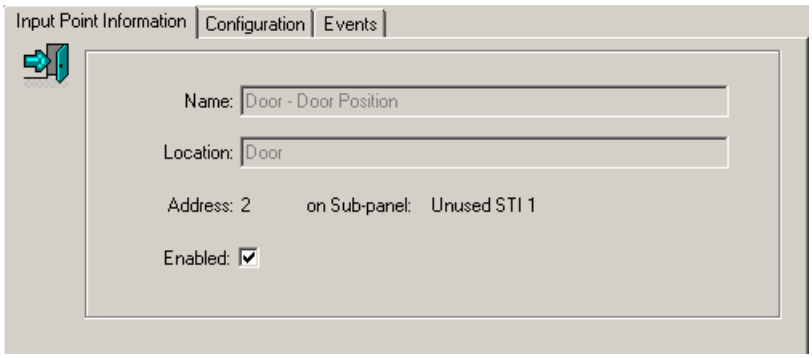
Field	Description
Reader Type	Defines the reader type (Disabled, Access, In In-X-It, Out In-X-It). In/Out In-X-It are used to designate the reader is part of an area, either as an in or an out reader. See "DBC - Area" in Chapter 29.
Lock Status	Defines the lock status of the reader. If the reader is locked, no cards gain access.
Card Type	Identifies the card type.
Reader Override	When enabled, the door remains unlocked indefinitely.
Monitored Access	Enables monitored access (card trace) on a reader.

Events Tab

To define an event, either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

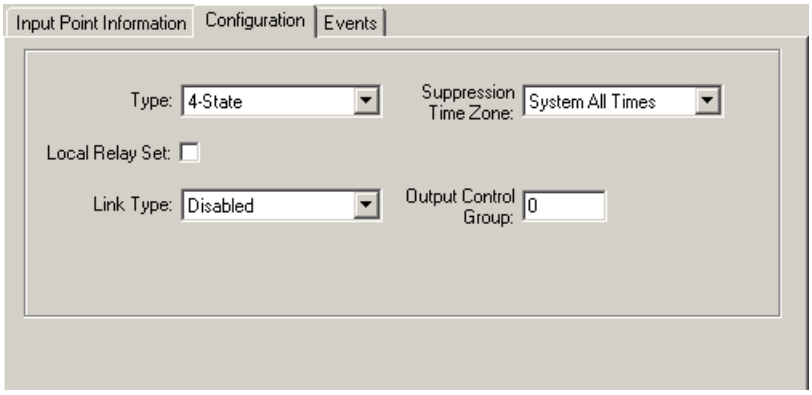
14.10.3 Input Points

Input Point Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.
Enabled	Required for the Logical Device to be operational.

Configuration Tab



Field	Description
Type	Defines the input type (2-State or 4-State).

Field	Description
Suppression Time Zone	Defines the time zone in which alarms associated with the input point are suppressed.
Local Relay Set	When enabled, upon the input point entering an alarm state, the panel relay activates. **Note:** This relay is the same relay as in Soft Alarms and Card Events.
Link Type (refers to output control group)	Defines the function of the associated output upon the input going into alarm. *Disabled* – The output point disables. *Active* – The output control group is activated when the input is in alarm. *Secure* – The output is not active when the input is secure (not in alarm). *Track* – The output is active when the input is in alarm but not in a trouble condition. *MIMIC* – The output is active when the input is in alarm, including a trouble condition. *Active Off* – The output is active when the input is secure (not in alarm). *Secure Off* – The output is inactive when the input is secure (not is alarm). *Reverse Trac* – The output is active when the input is secure; otherwise the output is inactive.
Output Control Group	Defines the output control group(1-600).

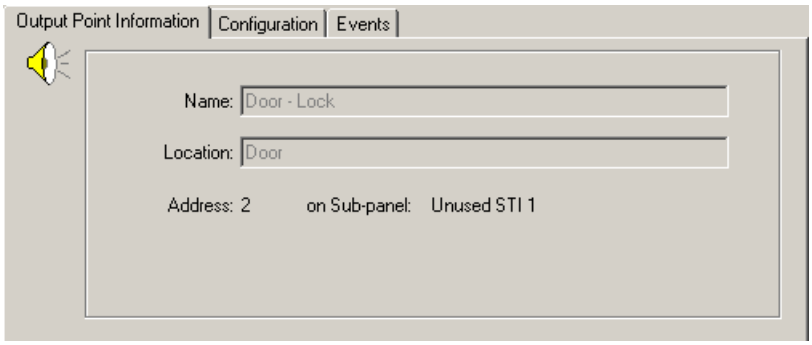
Events Tab

To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

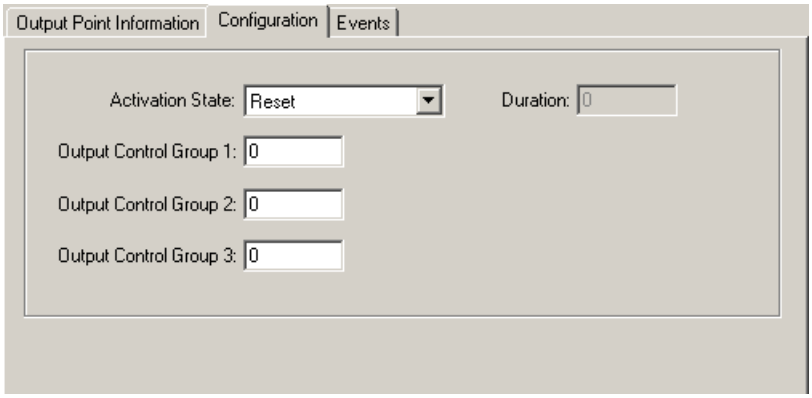
14.10.4 Output Points

Output Point Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_ on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.

Configuration Tab



Field	Description
Activation State	Defines the activation state of the output. When the output activate, this setting defines how the output is supposed to react. *Reset* - Turns the output off (inactive). *Set* - Turns the output on (activate). *Fast Flash* - Pulses the output every half second. *Slow Flash* - Pulses the output every second *Timed* - Pulses the output for a specified number of seconds up to 255 (defined in duration).
Duration	For a Timed activation state, specifies the number of seconds an output pulses.
Output Control Group 1	Designates the output is part of an output control group (1-600). An output can be a member of three groups.
Output Control Group 2	Designates the output is part of an output control group (1-600). An output can be a member of three groups.
Output Control Group 3	Designates the output is part of an output control group (1-600). An output can be a member of three groups.

Events Tab

To define an event:

Either double-click the event you want to define or select and click **Edit**. The **Edit Point** dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

14.10.5 Default CCTV Tab

If you added Logical Devices that included CCTV, the CCTV information you configured already appears on this tab. Click the appropriate icons to select the default auto CCTV command, select CCTV view, and select CCTV command for this device.

14.10.5.1 Transactions Tab

The Transactions tab displays all the transactions that have occurred at that particular reader. The number of records also appears, and you can print the list of transactions.

14.10.5.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

To assign a partition to an existing Logical Device:

1. Click the Partitions tab.
2. Click **Add**.
3. Select an available partition.
4. Click **OK**. See "DBC - Partitions" in Chapter 53 for more information about defining partitions.

14.11 Viewing and Editing Dependencies of a SmartPlus Mobile Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 6-53.

14.12 Deleting a SmartPlus Mobile Logical Device

Please refer to How to Delete a Logical Device, page 6-53.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Vindicator V5

15

In this chapter ...

Overview
Adding a Vindicator V5 Channel
Viewing and Editing Dependencies of a Vindicator V5 Channel
Deleting a Vindicator V5 Channel
Adding a Vindicator V5 Panel
Viewing and Editing Dependencies of a Vindicator V5 Panel
Deleting a Vindicator V5 Panel
Adding a Vindicator V5 Logical Device
Editing a Vindicator V5 Logical Device
Viewing and Editing Dependencies of a Vindicator V5 Logical Device
Deleting a Vindicator V5 Logical Device

15.1 Overview

This chapter describes how to configure a site that uses a Vindicator V5 panel.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

15.2 Adding a Vindicator V5 Channel

The Pro-Watch channel is the communications path between the host and the panel. You must identify the channel before adding a panel and Logical Device.

To add a channel:

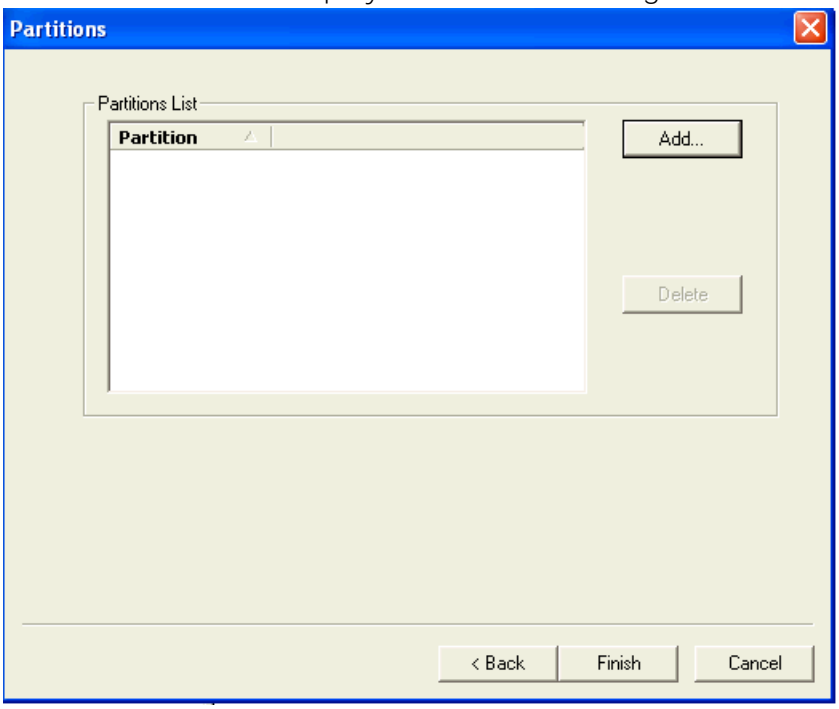
1. Select a Channel Type:
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.
   b. Select **V5 Server** from the drop-down list.
   c. Click **OK**. The Define Channel Information dialog box appears.
2. Define the Channel:
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
   c. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.
   d. In the Attempts field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.
   e. In the Poll Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds.
   f. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.
   g. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.
   h. Click **Next** to display the Communications Parameters dialog box.
3. Set Communications Parameters:

a. Select the port type from the following drop-down list options:

Option	Description
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
TCP/IP	Specifies that the channel is a network connection. IP Address – the IP address of the panel.

b. If you are using the TCP/IP port on the server, enter the V5 server's IP address, the port number, a user name and password with V5 server access, and a new poll interval and retry time if desired. The poll interval sets the number of seconds that elapses between each poll by the host computer. The retry time sets the number of seconds that must elapse before a communications retry will be attempted.

c. :Click **Next** to display the Partitions dialog box.



4. If you are using Pro-Watch partitions, click **Add** to add the partition to which the channel will be assigned. For information about adding

partitions, see "DBC - Partitions" in Chapter 53. If you are not using Pro-Watch partitions, leave this box blank.

5. Click **Finish** to complete the channel configuration. A warning appears reminding you that no events on this channel can be reported until you add the channel to the appropriate Routing Group in Database Configuration. See "DBC - Routing Groups" in Chapter 55. If you are not using Routing Groups, Pro-Watch adds the channel to the default routing group automatically.



6. Click **OK**. The new channel is complete.

15.3 Viewing and Editing Dependencies of a Vindicator V5 Channel

Use this function to view and modify the Channel's dependencies. The Channel object depends upon the Site and Routing Group objects.

To view and modify a Channel's dependencies:

1. Right-click the icon of an existing Channel in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Channel's dependencies.
2. To modify or remove the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

15.4 Deleting a Vindicator V5 Channel

Use this function to delete a Channel from the Pro-Watch database.

1. In the Pro-Watch Hardware Configuration tree list, click **Channels** to display the Channel icons in the right pane.

Note: Right-click the Channel you want to delete and select **Delete**.

You cannot delete a Channel that has dependencies. A dependency is another database object that includes the Channel in its configuration. The Channel object depends upon the Site and Routing Group objects. If the Channel has no current dependencies, you are prompted to confirm the deletion. However, if the Channel does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Channel:

    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.

    b. Either change or delete each of the objects listed as dependencies.

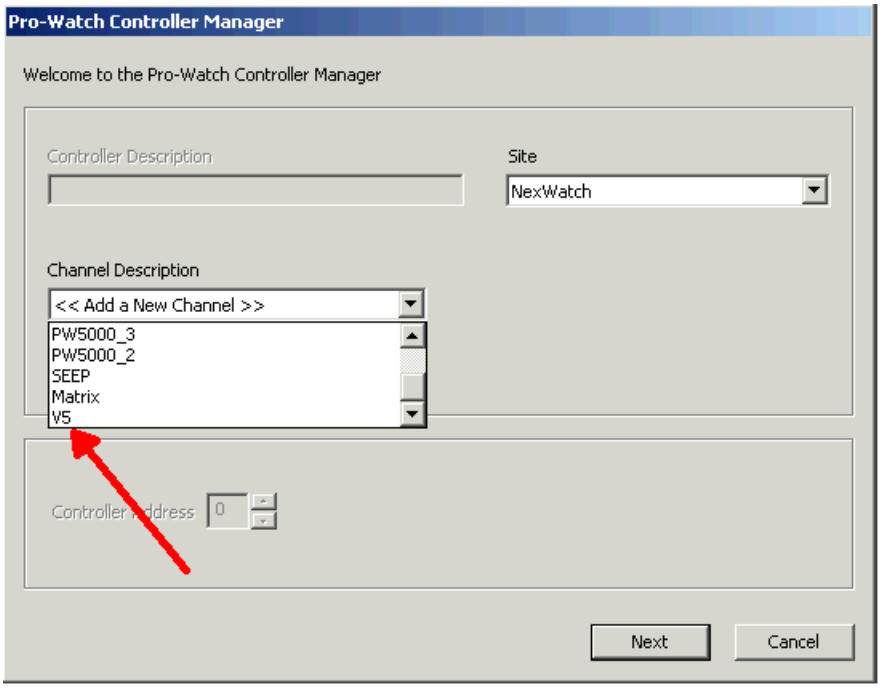
Repeat step 2 and click **Yes** at the prompt to delete the channel.

15.5 Adding a Vindicator V5 Panel

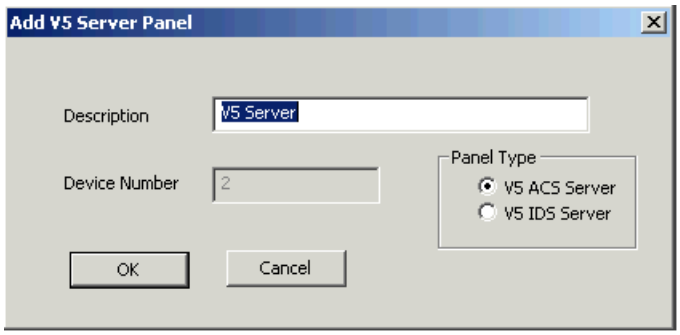
To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 4.

To add a Vindicator V5 panel:

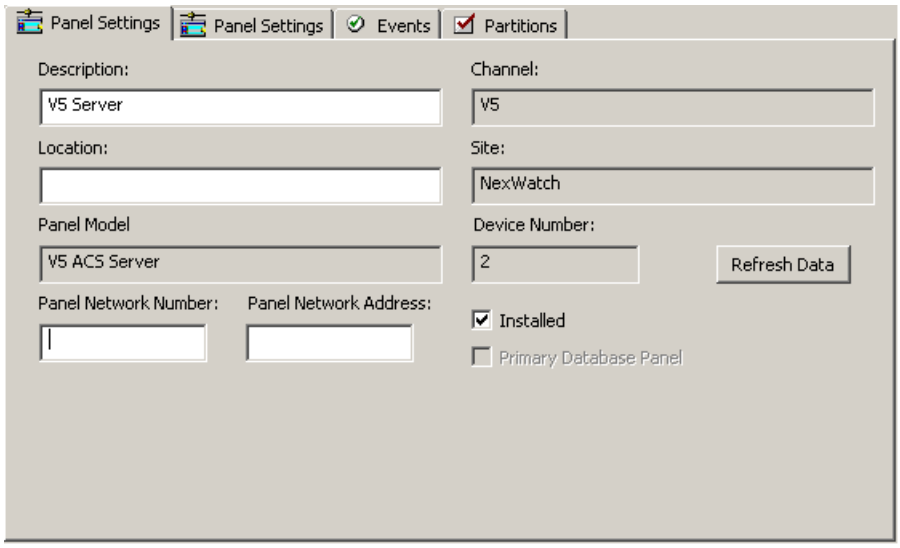
1. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
2. Select **New > Panel** to display the Pro-Watch Controller Manager dialog box.
3. In the Channel Description field, select the V5 Server channel you have created for the panel.



4. Click **Next**. The first Add V5 Server Panel dialog box appears.

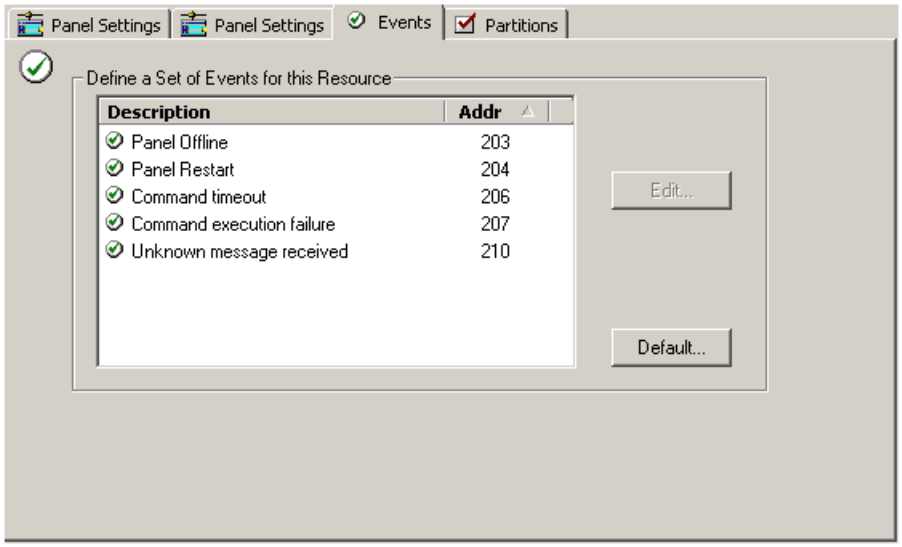


5. Select the correct panel type in the Panel Type field. Select “V5 ACS Server” for a Vindicator V5 Access Control System panel, or “VS IDS Server” for a Vindicator V5 Intrusion Detection System.
6. Click **OK** to display the Add V5 Server Panel dialog box.



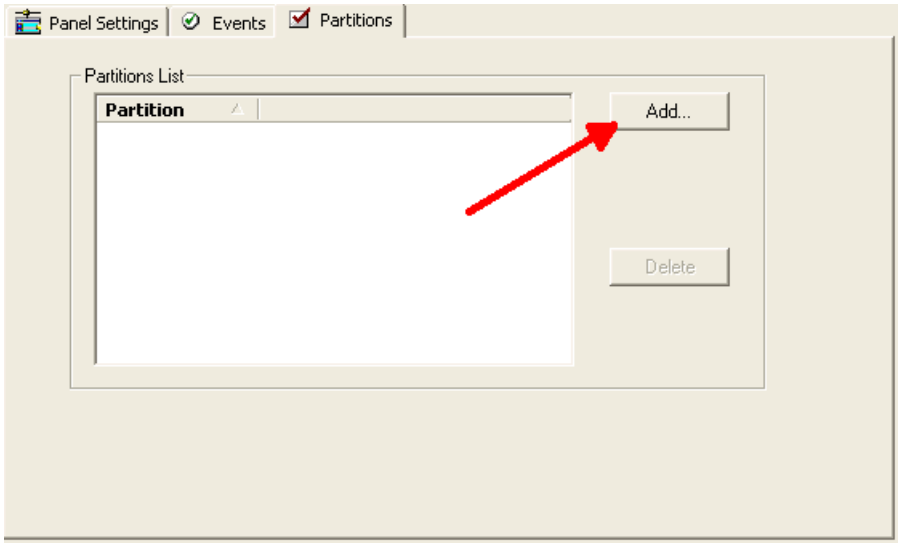
7. Perform the following:
   a. If you desire, revise the default description in the Description field in the first Panel Settings tab.
   b. In the Location field on the Panel Settings tab, enter a string that identifies the location of the panel. This field is not required, but it can help you to troubleshoot later if necessary.
   c. In the Panel Network Number field, enter the number of the Vindicator network in which the V5 panel will function. This is a network administrator-assigned number.
   d. In the Panel Network Address field, enter a three-digit number that is unique in the network. This is also a network administrator-assigned number.
   e. Leave the **Installed** check box selected if you want the configured panel to be installed and operational.
   f. Click **OK** to complete the panel settings.

8. To define a set of the panel's events, click the **Events** tab.



9. To edit an event, either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25. To re-set the event configuration to the default setting, click **Default**.
10. Click the **Partitions** tab to define any Pro-Watch partitions you may wish to assign to Pro-Watch users or classes. A Pro-Watch partition is a logical division of access control that is assigned at the Pro-Watch User or Class level through the Pro-Watch Database Configuration application. The Pro-Watch partition determines the view of the resources within Pro-Watch. See "DBC - Partitions" in Chapter 53 for more details.

To assign Pro-Watch partitions, select the Partitions tab and click **Add**:



A list of the available partitions that have already been created in Pro-Watch (see "DBC - Partitions" in Chapter 53 for instructions) appears. Select the desired partitions and click **Add**: The added partitions are now available to be assigned to users and classes.

15.6 Viewing and Editing Dependencies of a Vindicator V5 Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

15.7 Deleting a Vindicator V5 Panel

Please refer to How to Delete a Panel, page 53.

15.8 Adding a Vindicator V5 Logical Device

A Pro-Watch Logical Device is a single physical device or group of selected physical devices, which are defined by a hardware template. For example, a template may define a door that is equipped with a card reader, a REX input device, and a door strike output device as one Logical Device.

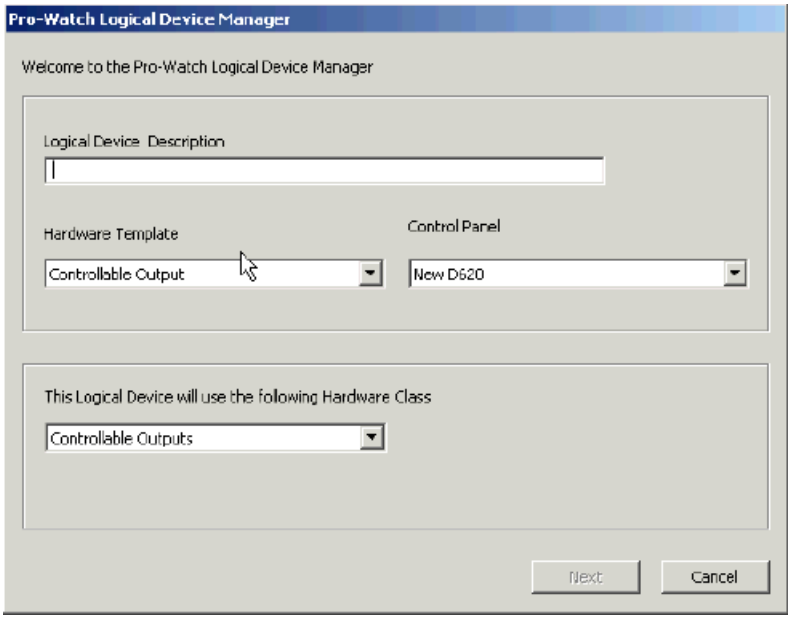
As a logical entity, the door can easily be configured in the Pro-Watch system by associating it (and its devices) to other elements in the system. For example, you can assign the door, reader, input device, and output device as a functioning unit to a controlling panel in one procedure.

Note: Before you create Logical Devices, you must create the following:

- Site. See "Adding a Vindicator V5 Channel".
- Channel. See "Adding a Vindicator V5 Channel".
- Panel. See "Adding a Vindicator V5 Panel".
- Hardware Template. See Adding or Editing a Hardware Template, page 28.

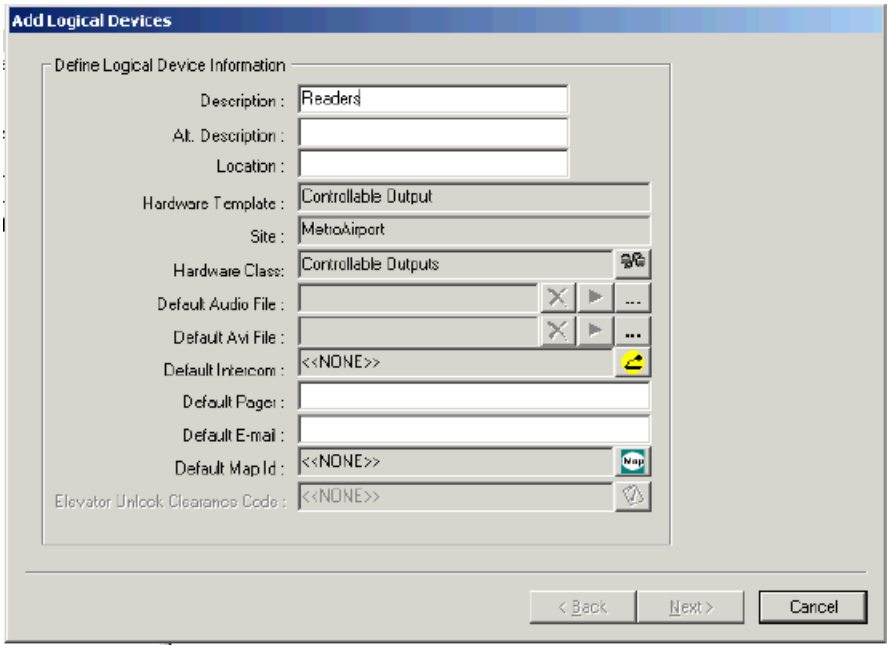
To add a Logical Device:

1. From the Pro-Watch Hardware Configuration tree view, right-click the site to which you want to assign the Logical Device, and select **New > Logical Device**. The Logical Device Manager dialog box appears:



2. Enter a description that will identify the Logical Device in the Logical Device Description field.
3. Select a Hardware Template from the drop-down list in the Hardware Template field.

4. Select a Hardware Class from the drop-down list in the Hardware Class field.
5. Click **Next**. The Add Logical Devices dialog box appears.

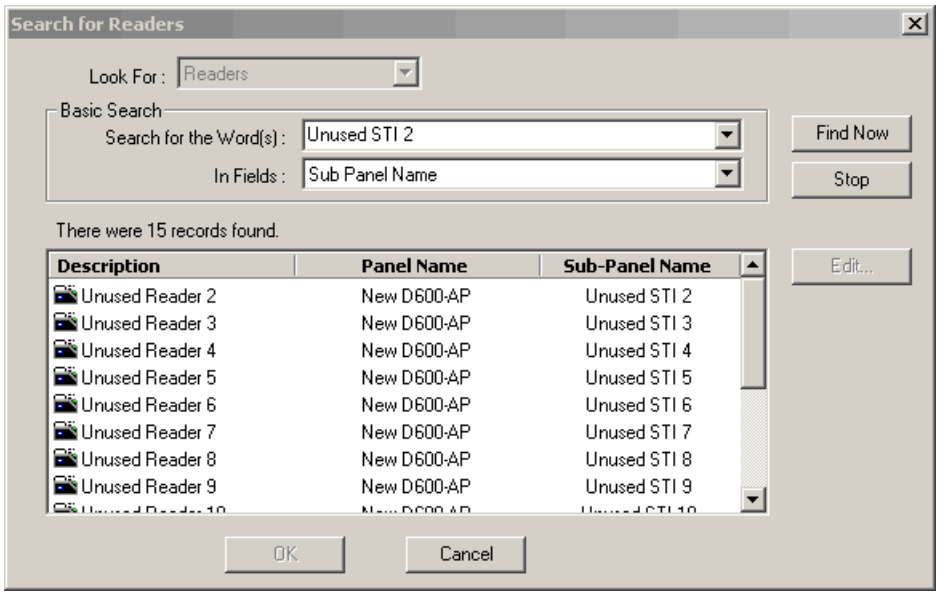


6. Use the following table to complete the Define Logical Device field entries:

Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.

Field	Description
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23 for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. For more information, see "DBC - Clearance Codes" in Chapter 37.

7. Click **Next**. The Logical Device Details dialog box appears:
8. Select a device type and click **Assign HW** to display the Search for [Device Type] dialog box:



9. Enter the description in the 'Search for Word(s)' field; this is the description that is used to search for available addresses.
10. Select the field name from the 'In Fields' drop-down list and click **Find Now**.
11. Select the record and click **OK**.
12. Repeat step 5 through step 9 until all device types have been assigned.
13. Click **Next**. The Default CCTV Information dialog box appears.
14. CCTV may be associated with Logical Devices. You may assign the default view and commands for this device. For more information, see "HW Config - CCTV" in Chapter 21. To assign a Default Command or View, click on the icon and select the command or view. Click **OK** and then click **Next**. The Partitions dialog box appears.
15. To assign a partition to this Logical Device, click **Add**, select the partition, and click **Add** again. For information about partitions, see "DBC - Partitions" in Chapter 53.
16. Click **Finish** to complete the Logical Device configuration.

Note: The number of Logical Devices available to add to the panel is dependent upon the number of STI sub-panels assigned. You can have a maximum of 16 STI sub-panels, 16 readers (1 reader per subpanel), 256 inputs (16 inputs per sub-panel), and 512 outputs (32 outputs per sub-panel).

15.9 Editing a Vindicator V5 Logical Device

Logical Devices can be configured or edited after assigning an address. If you have configured the hardware template before adding a Logical Device and selected that hardware template while adding a Logical Device, the Logical Devices will already be configured. See Adding or Editing a Hardware Template, page 28.

Tip: It is a good idea to visit the Logical Device configuration tabs, as these tabs contain additional fields hardware templates do not.

To configure a Logical Device:

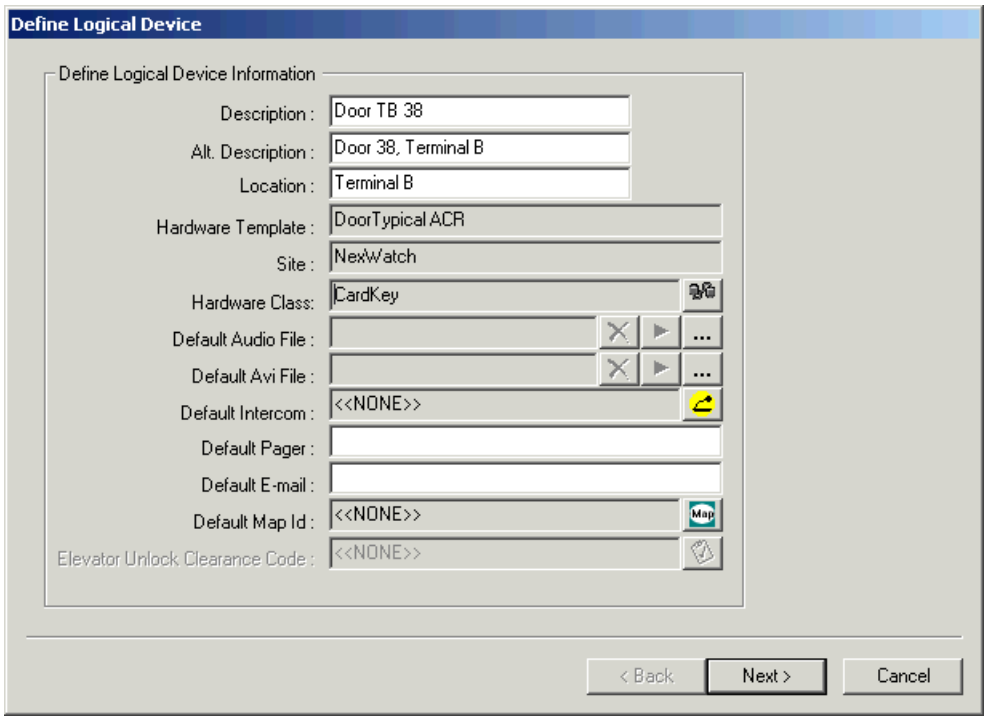
1. Click the appropriate Logical Device folder in the Hardware Configuration screen to display the site's existing Logical Devices.
2. Right-click the Logical Device you want to configure, and select **Properties**. The Edit Logical Devices [Logical Device name] screen appears. The screen contains six information tabs. Complete the following information tabs to configure the Logical Device:

EDITING LOGICAL DEVICES TABS LIST

- "Define Logical Device Tab".
- "Logical Device Details Tab".
  - Readers
    - "Reader Information Tab".
    - "Configuration Tab".
    - "Events Tab".
  - Input Points
    - "Input Point Information Tab".
    - "Configuration Tab".
    - "Events Tab".
  - Output Points
    - "Output Point Information Tab".
    - "Configuration Tab".
    - "Events Tab".
- "Default CCTV Tab".
- "Transactions Tab".

- "Partitions Tab".

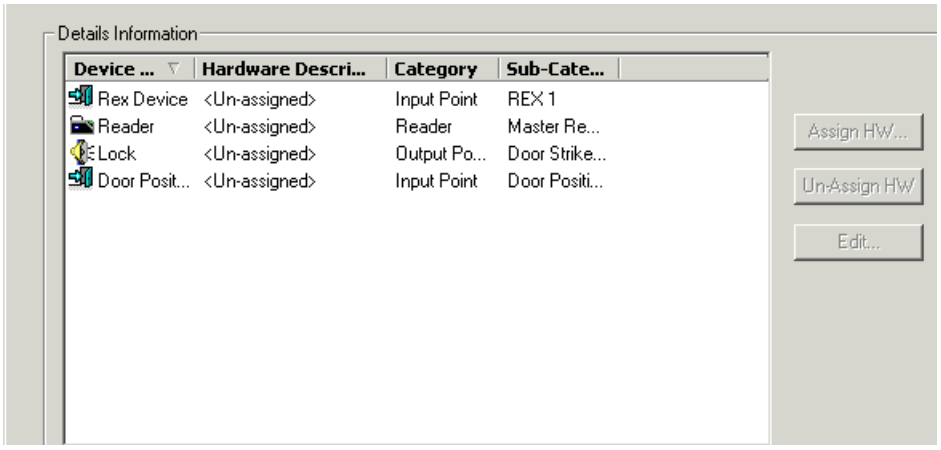
15.9.1 Define Logical Device Tab



Field	Description
Description	The description of the Logical Device as defined by the user.
Alt. Description	An alternate description of the Logical Device as defined by the user.
Location	Identifies the physical location of the Logical Device as defined by the user.
Hardware Template	Assigns a Hardware Template to the Logical Device. See Adding or Editing a Hardware Template, page 28.
Site	Identifies the Site in which the Logical Device is assigned
Hardware Class	Defines the hardware class in which the Logical Device resides. See Adding or Editing a Hardware Class, page 24.

Field	Description
Default Audio File	Defines the default audio file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default AVI File	Defines the default video file that initiates upon a specified event(s). See "HW Config - Edit Point" in Chapter 25.
Default Intercom	Assigns a default Intercom to the Logical Device. See "HW Config - Intercom" in Chapter 23for more information.
Default Pager	Defines the default pager number for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default E-mail	Defines the default e-mail for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Default Map ID	Defines the default map ID for the associated event(s). See "HW Config - Edit Point" in Chapter 25.
Elevator Unlock Clearance Code	When the Logical Device is part of an elevator configuration, defines and elevator unlock clearance code. For more information, see "DBC - Clearance Codes" in Chapter 37.

15.9.2 Logical Device Details Tab



To assign a sub-panel to a device type:

1. Click to select the device type and click **Assign HW ...** A list of all unused sub-panels appears.
2. Select the sub-panel you want, and click **OK**.

To un-assign a device type:

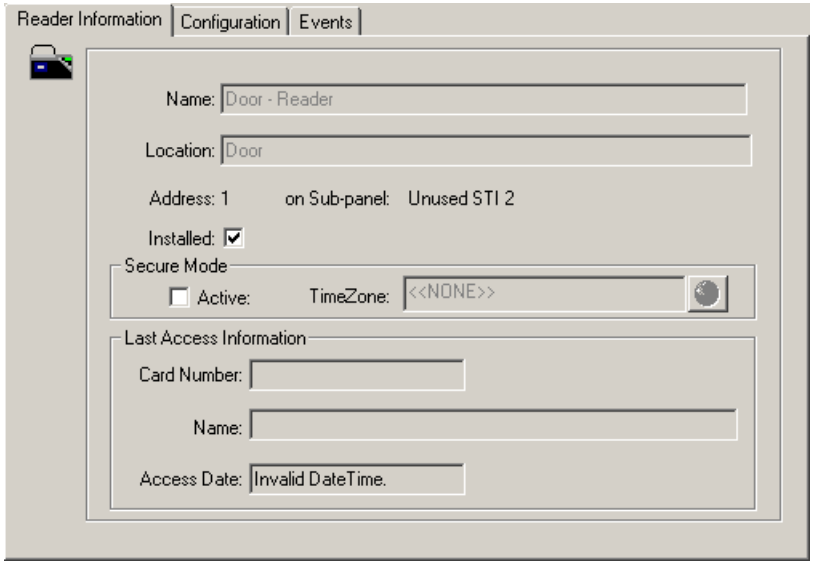
1. Click to select the device type and click **Un-Assign HW**.

To edit the current configuration of a device type:

1. Click to select the device type and click **Edit**. The Edit [device type] dialog box appears. The dialog box for each device type consists of information tabs, which you must complete.
2. Use the appropriate section below to edit or configure the device type you have selected.

15.9.3 Readers

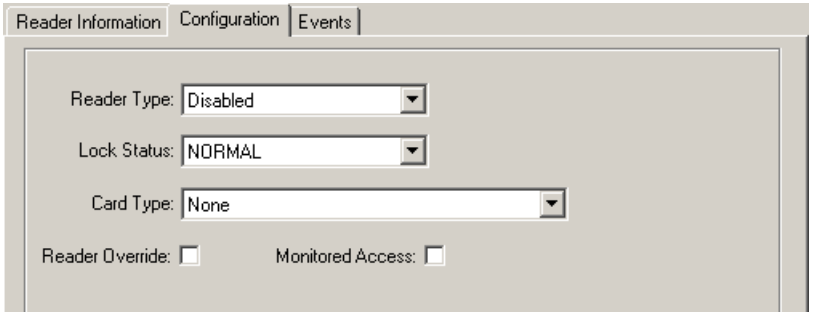
Reader Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.
Installed	Required for the Logical Device to be enabled and operational.

Field	Description
Active (Secure Mode)	Enables secure mode for a particular door. See Appendix A, Secure Mode Verification.
Time Zone (Secure Mode)	Defines the time zone during which the reader is in secure mode.
Card Number (Last Access)	Identifies the card number which accessed the Logical Device last.
Name (Last Access)	Identifies the name of the badgeholder who last accessed the Logical Device.
Access Date	Identifies the date of last access.

Configuration Tab



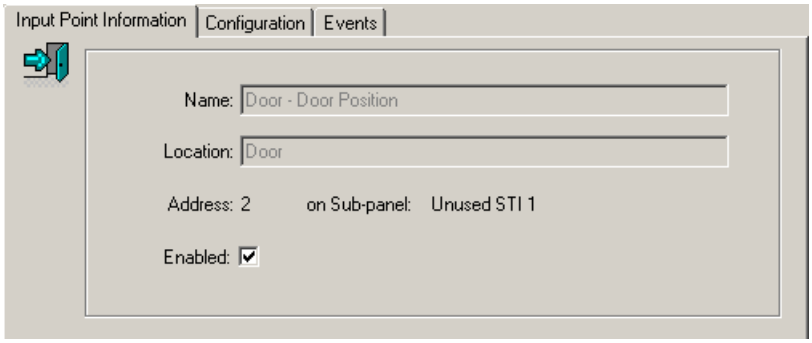
Field	Description
Reader Type	Defines the reader type (Disabled, Access, In In-X-It, Out In-X-It). In/Out In-X-It are used to designate the reader is part of an area, either as an in or an out reader. See "DBC - Area" in Chapter 29.
Lock Status	Defines the lock status of the reader. If the reader is locked, no cards gain access.
Card Type	Identifies the card type.
Reader Override	When enabled, the door remains unlocked indefinitely.
Monitored Access	Enables monitored access (card trace) on a reader.

Events Tab

To define an event, either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

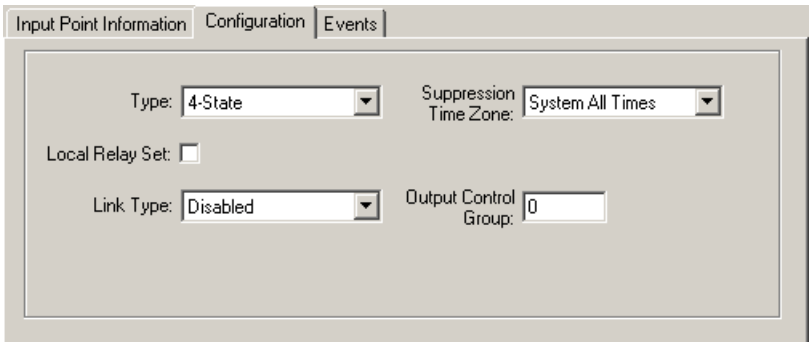
15.9.4 Input Points

Input Point Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.
Enabled	Required for the Logical Device to be operational.

Configuration Tab



Field	Description
Type	Defines the input type (2-State or 4-State).
Suppression Time Zone	Defines the time zone in which alarms associated with the input point are suppressed.
Local Relay Set	When enabled, upon the input point entering an alarm state, the panel relay activates. **Note:** This relay is the same relay as in Soft Alarms and Card Events.
Link Type (refers to output control group)	Defines the function of the associated output upon the input going into alarm. *Disabled* – The output point disables. *Active* – The output control group is activated when the input is in alarm. *Secure* – The output is not active when the input is secure (not in alarm). *Track* – The output is active when the input is in alarm but not in a trouble condition. *MIMIC* – The output is active when the input is in alarm, including a trouble condition. *Active Off* – The output is active when the input is secure (not in alarm). *Secure Off* – The output is inactive when the input is secure (not is alarm). *Reverse Trac* – The output is active when the input is secure; otherwise the output is inactive.
Output Control Group	Defines the output control group(1-600).

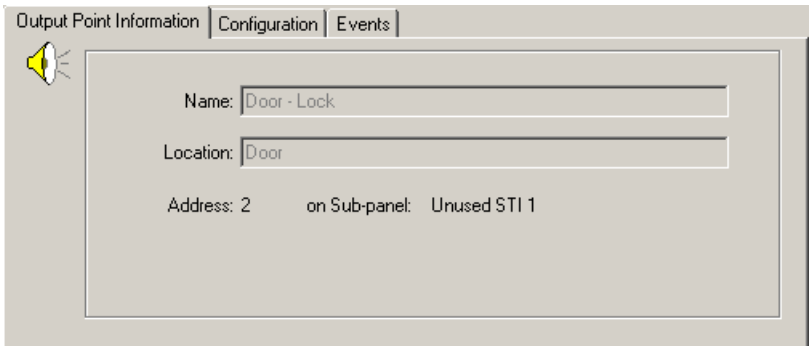
Events Tab

To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

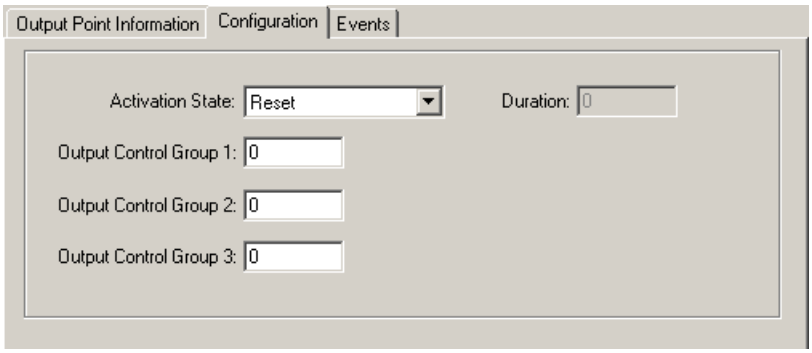
15.9.5 Output Points

Output Point Information Tab



Field	Description
Name	Identifies the name of the Logical Device.
Location	Identifies the location of the Logical Device as defined by the user.
Address_ on Sub-Panel_	Identifies the address of the Logical Device and the sub-panel in which it is assigned to.

Configuration Tab



Field	Description
Activation State	Defines the activation state of the output. When the output activate, this setting defines how the output is supposed to react. *Reset* - Turns the output off (inactive). *Set* - Turns the output on (activate). *Fast Flash* - Pulses the output every half second. *Slow Flash* - Pulses the output every second *Timed* - Pulses the output for a specified number of seconds up to 255 (defined in duration).
Duration	For a Timed activation state, specifies the number of seconds an output pulses.
Output Control Group 1	Designates the output is part of an output control group (1-600). An output can be a member of three groups.
Output Control Group 2	Designates the output is part of an output control group (1-600). An output can be a member of three groups.
Output Control Group 3	Designates the output is part of an output control group (1-600). An output can be a member of three groups.

Events Tab

To define an event:

Either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25.

15.9.6 Default CCTV Tab

If you added Logical Devices that included CCTV, the CCTV information you configured already appears on this tab. Click the appropriate icons to select the default auto CCTV command, select CCTV view, and select CCTV command for this device.

15.9.7 Transactions Tab

The Transactions tab displays all the transactions that have occurred at that particular reader. The number of records also appears, and you can print the list of transactions.

15.9.8 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

To assign a partition to an existing Logical Device:

1. Click the Partitions tab.
2. Click **Add**.
3. Select an available partition.
4. Click **OK**. See "DBC - Partitions" in Chapter 53 for more information about defining partitions.

15.10 Viewing and Editing Dependencies of a Vindicator V5 Logical Device

Please refer to How to View and Edit Dependencies of a Logical Device, page 53.

15.11 Deleting a Vindicator V5 Logical Device

Please refer to How to Delete a Logical Device, page 53.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config – VISTA

16

In this chapter ...

Overview

Adding a VISTA Channel

Viewing and Editing Dependencies of a VISTA Channel

Deleting a VISTA Channel

Adding a VISTA Panel

Editing a VISTA Panel

Viewing and Editing Dependencies of a VISTA Panel

Deleting a VISTA Panel

16.1 Overview

This chapter describes how to configure a site that uses a VISTA panel.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

16.1.1 Update Intervals

VISTA panel's Time/Date setting functionality works for a variety of on-the-hour time intervals other than just hourly updates. Here are the registry values and the updating options they represent:

-24 ==> every day at midnight

-23 ==> every day at 11PM

-22 ==> every day at 10PM

... (etc.)

-3 ==> every day at 3AM

-2 ==> every day at 2AM

-1 ==> every day at 1AM

0 ==> no updates

1 ==> hourly updates starting at midnight

2 ==> every two hours starting at midnight (midnight, 2AM, 4AM, etc.)

3 ==> every three hours, starting at midnight (midnight, 3Am, 6Am, etc.)

... (etc.)

10 ==> every 10 hours, starting at midnight (midnight, 10AM, 8PM)

11 ==> every 11 hours, starting at midnight (midnight, 11AM, 10PM)

12 ==> every 12 hours, starting at midnight (midnight and noon)

16.2 Adding a VISTA Channel

The Pro-Watch channel is the communications path between the host and the panel. You must identify the channel before adding a panel and Logical Device.

Note: The recommended maximum number of channels per site is 99.

To add a channel:

1. Select a Channel Type:
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.
   b. Select **Vista** from the drop-down list.
   c. Click **OK**. The Define Channel Information dialog box appears.
2. Define the Channel:
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
   c. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.
   d. In the Attempts field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.
   e. In the Poll Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds.
   f. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.
   g. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.
   h. Click **Next** to display the Communications Parameters dialog box.
3. Set Communications Parameters:
   - If you are using the COM port on the server:

     a. Set the port type to **Hardwired**.

     b. Set **Baud** to 1200. This field sets the speed (bits per second) at which communications will proceed.

c. Set **Word Size** to 8N1. This field indicates the number of bits the host computer can process at once (usually the same as the width of the CPU's external data bus). Leave the default value already entered in this field. The word size uses the following format:

[number of data bits][N (no), E (even), or O (odd) parity bits][number of stop bits]

d. Set **Poll Interval** to 40. This field sets the number of seconds that elapses between each poll by the host computer.

e. Set **Retry Time** to 20. This field sets the number of seconds that must elapse before a communications retry will be attempted.

f. Click **Next** to display the Partitions dialog box (proceed directly to step 4).

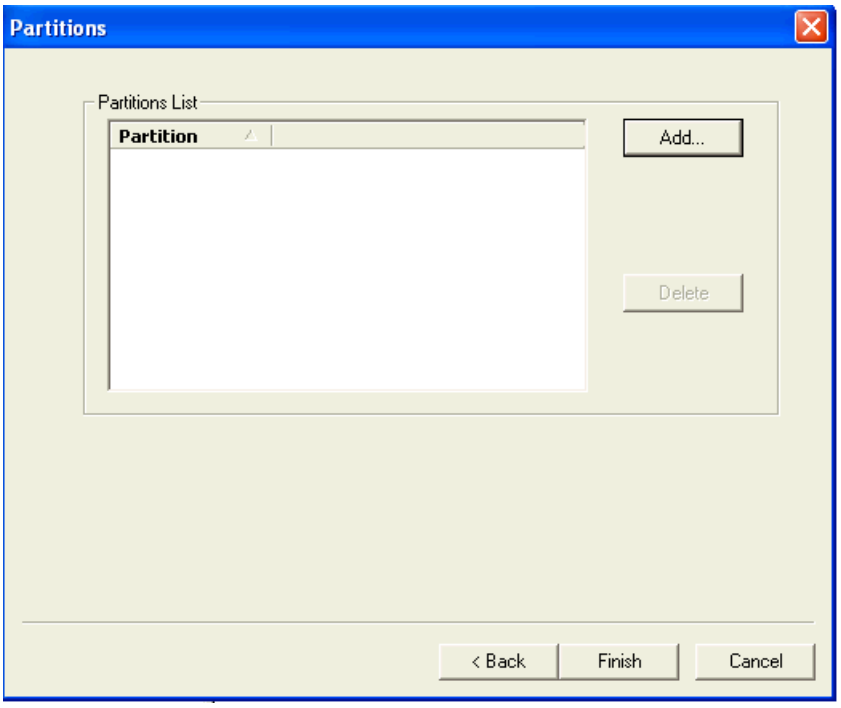
- If you are using a UDS device:

a. Set the port type to **TCP/IP**.

b. Enter the IP address of the UDS device in the left box.

c. Enter the device's port number to be used for communications in the right box.

d. Click **Next** to display the Partitions dialog box.



4. If you are using Pro-Watch partitions, click **Add** to add the partition to which the channel will be assigned. For information about adding partitions, see "DBC - Partitions" in Chapter 53. If you are not using Pro-Watch partitions, leave this box blank.
5. Click **Finish** to complete the channel configuration. A warning appears reminding you that no events on this channel can be reported until you add the channel to the appropriate Routing Group in Database Configuration. See "DBC - Routing Groups" in Chapter 55. If you are not using Routing Groups, Pro-Watch adds the channel to the default routing group automatically.



6. Click **OK**. The new channel is complete.

16.3 Viewing and Editing Dependencies of a VISTA Channel

Please refer to How to View and Edit Dependencies of a Channel, page 51.

16.4 Deleting a VISTA Channel

Please refer to How to Delete a Channel, page 51.

16.5 Viewing and Editing Dependencies of a VISTA Channel

Use this function to view and modify the Channel's dependencies. The Channel object depends upon the Site and Routing Group objects.

To view and modify a Channel's dependencies:

1. Right-click the icon of an existing Channel in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Channel's dependencies.
2. To modify or remove the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

16.6 Adding a VISTA Panel

To turn the User Wizard on and off, see *Turning the User Wizard On and Off*, page 4.

To set up a VISTA panel to be used by Pro-Watch using the keypad, enter Programming mode and set the following fields:

*05 = 1 (output all zone fault/restores)

*14 = 1 (use Home Facility Control instead of serial printer)

1*70 = 111111 (enter '1' six times - enable all event types)

1*71 = 1 (use 24 hour clock for event times)

1*72 = 0 (printer off line)

1*73 = 0 (1200 baud)

1*78 = 1 (extended event reports)

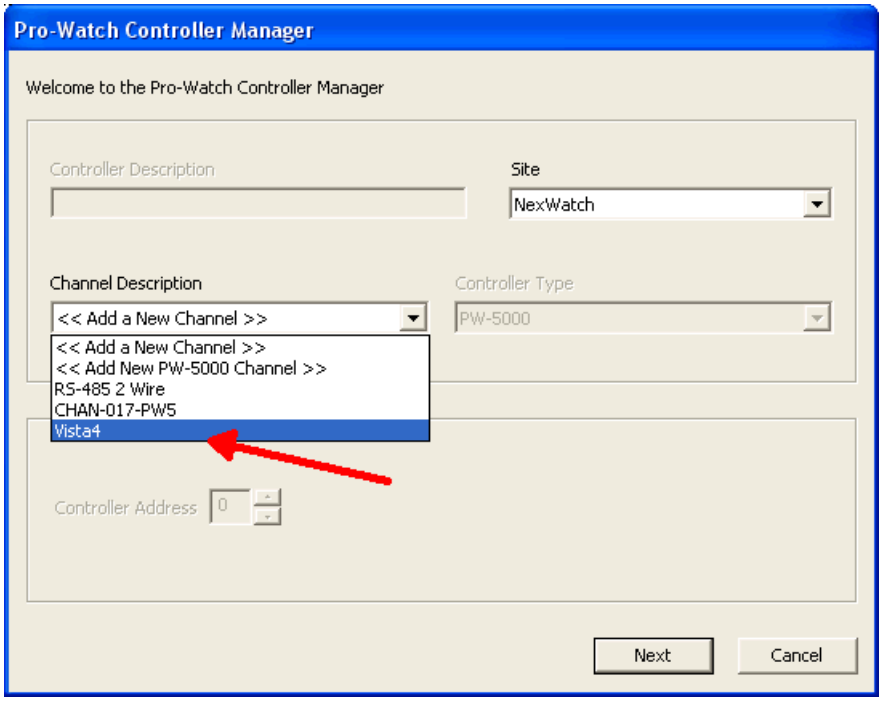
1*79 = 111111 (enter '1' six times - enable all event types)

2*30 = 0 (disable VA8201)

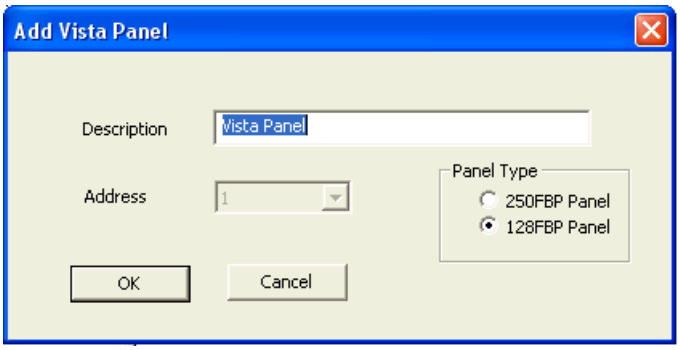
3*19 = 1 (enable 4100SM)

To add a VISTA panel:

1. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
2. Select **New > Panel** to display the Pro-Watch Controller Manager dialog box.
3. In the Channel Description field, select the VISTA channel you have created for the panel.



4. Click **Next**. The first Add Vista Panel dialog box appears.

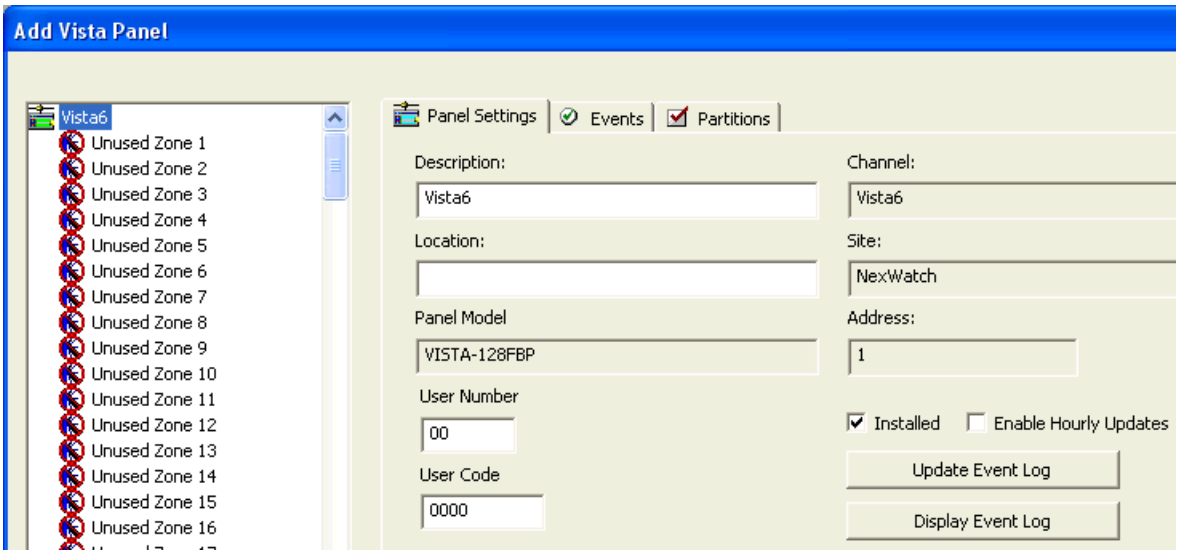


5. Perform the following:

   a. If you desire, revise the default description in the Description field.

   b. Select the model of the panel in the Panel Type field.

   c. Click **OK**. Pro-Watch creates the panel and the points table for this new device. It might require a few minutes to create the new tables. When the panel tables are created, the second Add Vista Panel screen appears, showing the panel's zones and properties.

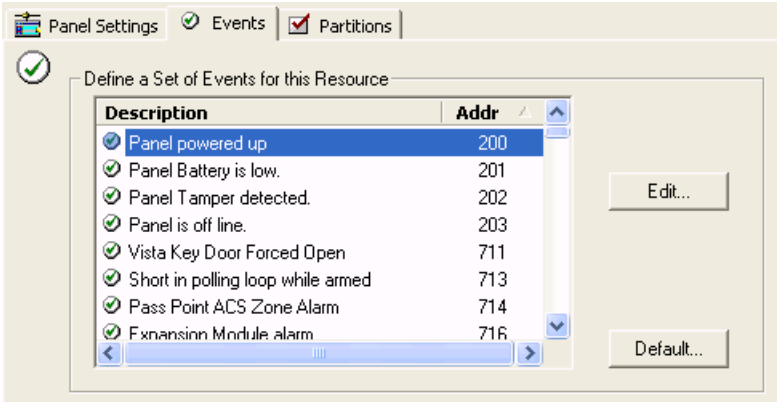


6. In the Location field on the Panels tab, enter a string that identifies the location of the panel. This field is not required, but it can help you to troubleshoot later if necessary.

Note: In the User Number field, enter a three-digit number that has already been programmed into the panel via the panel's keypad. Pro-Watch will use this number to access the panel. When a Pro-Watch user attempts to access the panel, he will be prompted to enter this number.

The three-digit user numbers, their associated user (security) codes, and their associated authority levels are all created via the panel's keypad. The panel installer has programmed one or more security codes by using the keypad, and the panel administrator adds users and associates them with authority levels and four-digit user (security) codes at the keypad. For more information about programming the security codes, see the *Partitioned Security System with Scheduling Installation and Setup Guide*. For more information about creating user numbers and assigning authority levels, see the *Partitioned Security System with Scheduling User Guide*.

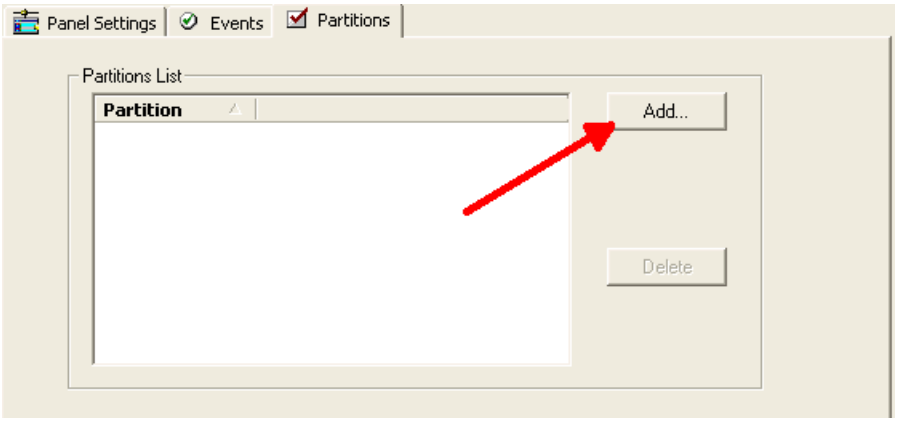
7. In the User Code field, enter the four-digit number that has already been assigned to the user number you entered in step 7.
8. Leave the Installed check box selected to have the panel installed and operational.
9. If you want the event log for this panel to be updated hourly, select the **Enable Hourly Updates** check box.
10. To view or edit the panel's events, click the **Events** tab.



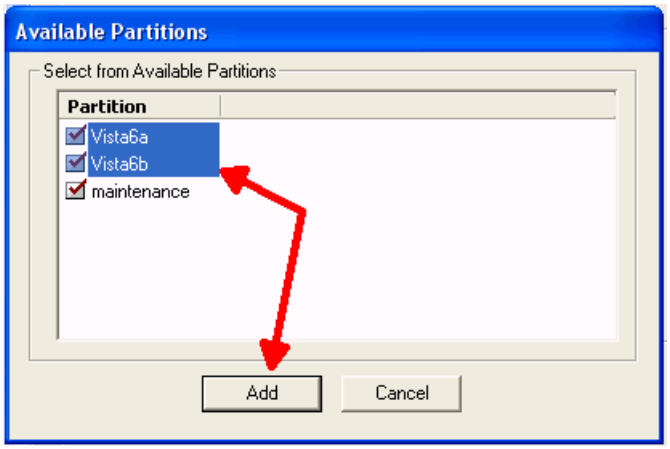
11. To edit an event, either double-click the event you want to define or select and click **Edit**. The Edit Point dialog box appears. For more information on editing events, see "HW Config - Edit Point" in Chapter 25. To re-set the event configuration to the default setting, click **Default**.
12. Click the **Partitions** tab to define any Pro-Watch partitions you may wish to assign to Pro-Watch users or classes. Note that there are two distinctly different types of partitions that control the use of the VISTA panel—VISTA partitions and Pro-Watch partitions. VISTA partitions are separate VISTA circuits on the panel to which you can assign zones of sensing devices. This enables you to physically restrict access to these devices among users. You can configure VISTA partitions only through the panel's keypad, not through Pro-Watch. This process includes assigning zones to partitions, setting zone types, and setting zone input types. A zone designates specific sensing devices. You assign devices to a zone. A zone type defines the way the system responds to faults in that zone. A zone input type defines where the system will look for status of the zone. For instructions, see the *Partitioned Security System with Scheduling Programming Guide*.

    A Pro-Watch partition is a logical division of access control that is assigned at the Pro-Watch User or Class level through the Pro-Watch Database Configuration application. The Pro-Watch partition determines the view of the resources within Pro-–Watch. See "DBC - Partitions" in Chapter 53for more details.

    To assign Pro-Watch partitions, select the Partitions tab and click **Add**:



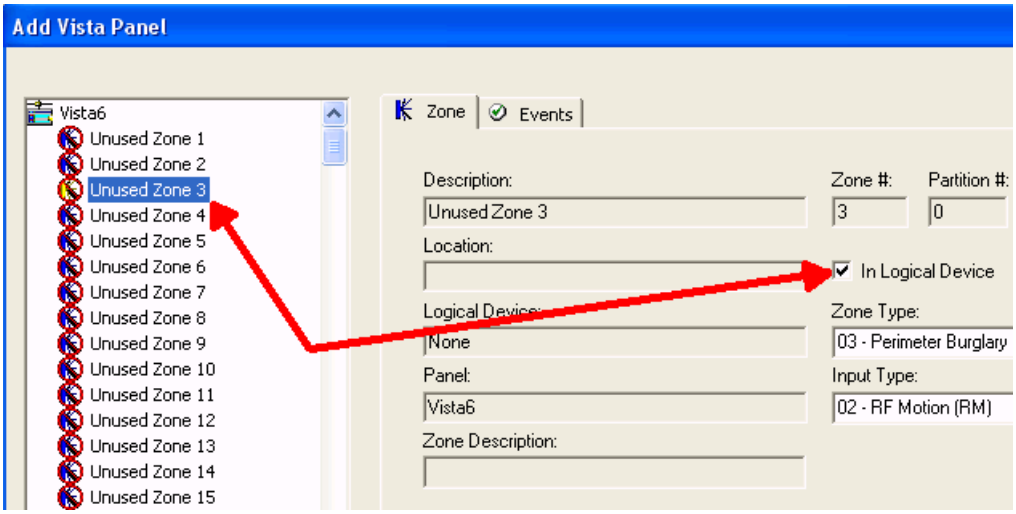
A list of the available partitions that have already been created in Pro-Watch (see "DBC - Partitions" in Chapter 53 for instructions) appears. Select the desired partitions and click **Add**: The added partitions are now available to be assigned to users and classes.



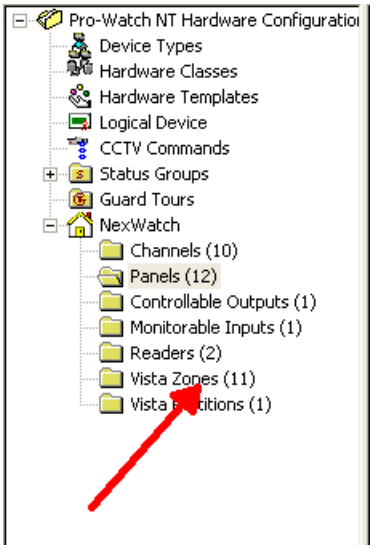
Note: Select the zone that you want to be viewed in Pro-Watch. Sensing devices are assigned to zones. Note that any zones you select from this list must first be configured from the panel keypad (see the *Partitioned Security System with Scheduling Installation and Setup Guide)*. To configure the zones in Pro-Watch, follow these steps:

– In the left window of the Add Vista Panel screen, click to select the first zone in the left
window. The Zone tab appears.

– Select the **In Logical Device** check box.



The zone you selected will appear in the Pro-Watch Hardware Configuration tree view after the panel is created, as shown below:



In the Zone tab, the Zone Type and Input Type fields appear to be active and configurable. However, this feature is not yet supported. If you select a zone type or input type in the Zone tab, the panel does not accept the selections. These values can only be programmed at the panel keypad.

13. Click **OK** to create the panel in Pro-Watch. The panel icon appears on the Pro-Watch Hardware Configuration screen in the **[site] > Panels** folder.

Note: Vista event times are provided in hours and minutes. The seconds will always show as :00, because the Vista panel does not support a time in seconds. Therefore, there will always be a small discrepancy of up to one minute in the reported event and system times.

16.7 Editing a VISTA Panel

To edit a VISTA panel's properties, you must use the panel's keypad. See the *Partitioned Security System with Scheduling Programming Guide* for instructions.

In Pro-Watch, you can only view the panel's properties. To view the panel's properties in Pro-Watch, right-click the panel you want to edit and select **Properties**. The Edit [panel name] Panel dialog box appears and displays the panel's properties that have been programmed at the panel keypad.

16.8 Viewing and Editing Dependencies of a VISTA Panel

Please refer to How to View and Edit Dependencies of a Panel, page 52.

16.9 Deleting a VISTA Panel

Please refer to How to Delete a Panel, page 53.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config – Generic Channels

17

In this chapter ...

Overview

Selecting a Channel Type

Setting Communications Parameters

SQL Stored Procedures for Generic Channels

Viewing and Editing Dependencies of a Generic Channel

Deleting a Generic Channel

17.1 Overview

Generic channels allow communication between devices which the Pro-Watch may not currently support.

Note: The procedures in this chapter assume that a site has already been created. For further information on site configuration, please refer to the following sections in this user guide:

- Add a Site, page 46.
- How to View and Edit Dependencies of a Site, page 48.
- How to Delete a Site, page 48.

17.2 Selecting a Channel Type

Note: The recommended maximum number of channels per site is 99.

1. In the Pro-Watch Hardware Configuration tree, right-click the site you have created, and select **New > Channel.** The Create a Channel dialog box appears.
2. Select the Generic channel type from the drop-down list.
3. Click **OK**. The Define Channel Information dialog box appears.
4. Define the Channel
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.
   c. From the Time Zone drop-down list, select the time zone that is appropriate for your site's geographic location.
   d. In the Attempts field, enter the maximum number times the Pro-Watch server will poll a panel before determining a panel timeout.
   e. In the Delay field, enter the Pro-Watch server-to-panel poll interval in milliseconds.
   f. In the Comm Break field, enter the number of panel timeouts that must occur before the Pro-Watch server determines that the panel is not operating.
   g. The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.
   h. Click **Next** to display the Communications Parameters dialog box.
5. The poll string is a string of characters that are sent every time the Pro-Watch performs a "Poll Delay" (see step 5).
   - To enter non-printable characters, use the hexadecimal value in the notation form of 0xFF where FF would be the hexadecimal value 0-255 (decimal).
   - If a poll string is not entered, the generic channel still receives characters and processes them but connectivity checks and poll-response protocols do not function.
6. Click **Next** to display the Communications Parameters dialog box.

17.3 Setting Communications Parameters

1. Select the port type from the following drop-down menu options:

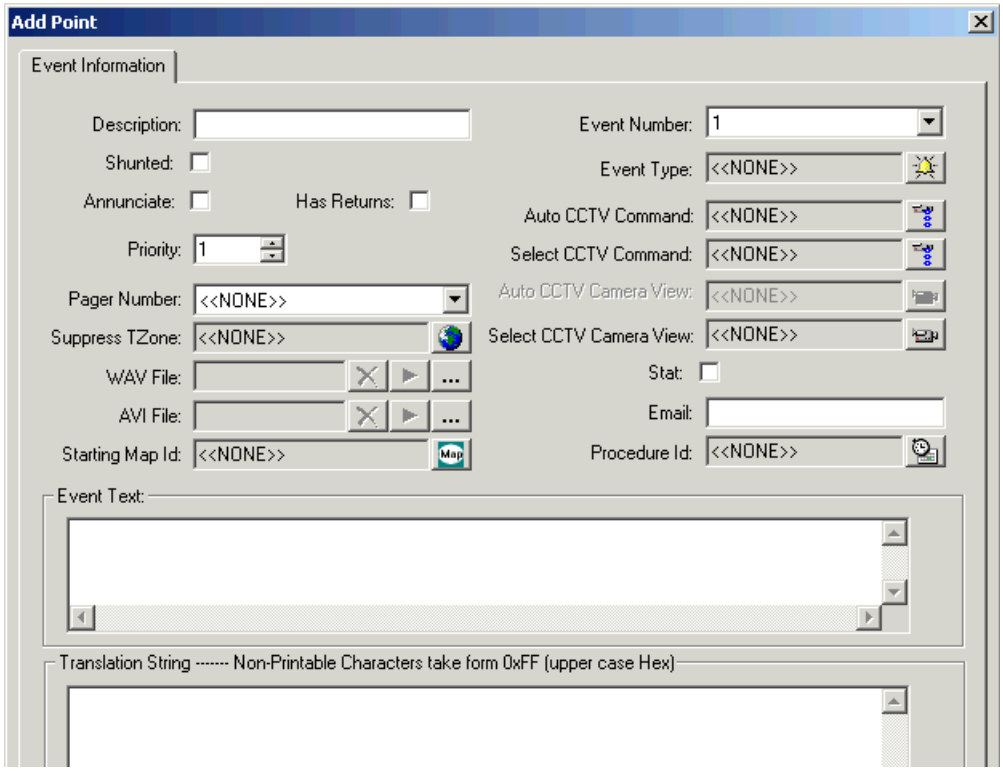
Option	Comments
Hardwired	Designates a serial port as the primary channel communication setting. Com Port—The com port on the host computer. Baud—The rate of communication between the host and the device. WordSize—Defines how many bits per communication channel. Flow Control—Starts and stops the transmission. Alarm Time—Sets the total time-out period for read operations, in milliseconds. Warning: You must set Alarm Time to a value greater than 0. Vtime—Sets the maximum time allowed to elapse between the arrival of two bytes on the communications line, in milliseconds. Warning: You must set VTime to a value greater than 0. Vmin—This parameter is not supported.
TCP/IP	Specifies that the channel is a network connection. IP Address – The IP address of the panel.

2. Click **Next** to display the Partitions dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.
3. Click **Finish** to complete the channel. A warning message appears reminding you that you must add the channel to the appropriate routing group before you can view any events using the channel. It is recommended that you assign the channel to a routing group after you plan and configure routing groups. See "DBC - Routing Groups" in Chapter 55.

To generate events for a generic channel:

Go to the Events tab of the generic channel and add a point. To access the Events tab, enter the edit mode of the Generic channel:

1. Select the channel and right-click.
2. Select **Properties** to display the Edit Channel dialog box.
3. Select the **Events** tab.
4. Click **Add** to display the Add Point dialog box.



5. Select a unique address from the Event Number drop-down list.
6. In the Translation String field, enter the text of the message to be received from the communication channel; this field is used to create a 'match' with the Generic channel. To enter non-printable characters, use the hexadecimal value in the notation form of 0xFF where FF would be the hexadecimal value 0-255 (decimal). When the Generic channel sees a match in the "translation string", the corresponding event is generated.

17.4 SQL Stored Procedures for Generic Channels

Generic channels may also use **SQL Stored Procedures** to process incoming messages and respond to those messages. This provides a very robust system to develop an interactive protocol without having to modify the Pro-Watch application. When a generic channel receives a matching string for an event, it attempts to call a SQL Stored procedure "GenericProcessReceive" with the following parameters:

- ChannelId NVARCHAR(64) - Channel the event was received.
- Address Integer - Address of the event matching the string.
- InputBuf VarBinary(200) - Actual contents of the receive buffer from the communication channel.
- OutputBuf VarVinary(200) - Contents to send back out the generic communication channel.
- OutputBufLen Integer - Length in bytes of the OutputBuf to transmit (0= Transmit nothing).

If the stored procedure does not exist, the Generic channel generates the event and waits to receive additional messages.

When a generic channel gets a request to transmit a message, it attempts to call a SQL Stored procedure "GenericProcessTransmit" with the following parameters:

- ChannelId NVARCHAR(64) - Channel the event was received.
- Address Integer - Address of the event matching the string.
- InputBuf VarBinary(200) - Actual contents of the receive buffer from the communication channel.
- OutputBuf VarVinary(200) - Contents to send back out the generic communication channel.
- OutputBufLen Integer - Length in bytes of the OutputBuf to transmit (0= Transmit nothing).

This stored procedure can act upon the incoming message in "InputBuf", perform any required calculations, such as a checksum, and place the result into the "OutputBuf" variable; the length to transmit in the "OutputBufLen" variable as well as the Generic channel transmits this message. This allows you to download messages and write code to compute any required message header information.

"This is A End-of-Line Marker" check box

If the check box, "This is A End-of-Line Marker", is selected when Pro-Watch 'matches' the received string with the event record, the following occurs:

1. The "GenericProcessReceive" stored procedure gets called.
2. An event is generated.
3. Pro-Watch calls the stored procedure discussed above.

For more information on configuring additional fields within the Add or Edit Point dialog boxes, see "HW Config - Edit Point" in Chapter 25.

17.5 Viewing and Editing Dependencies of a Generic Channel

Please refer to How to View and Edit Dependencies of a Channel, page 51.

17.6 Deleting a Generic Channel

Please refer to How to Delete a Channel, page 51.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Log Printers

18

In this chapter ...

Log Printers

18.1 Log Printers

Log Printers provide the ability to send particular system events to a line printer in real-time. This functionality is only available on the Pro-Watch server.

Note: The Channel icon for Log Printers always remains red.

Follow these steps:

1. Select a Channel Type:
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created and select **New > Channel**. The Create a Channel dialog box appears.
   b. Select the Log Printer channel type from the drop-down list.
   c. Click **OK**. The Define Channel Information dialog box appears.
2. Define the Channel:
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Select the **Installed** check box. This assures the channel is installed and operational.
   c. Select a time zone from the drop-down list.
   d. Enter the maximum number of poll attempts.
   e. Enter the poll delay interval between each polling. This number is in milliseconds.
   f. Enter the communications break; the host must receive communication from the device within the specified time or the host will determine the communication as broken.
   g. The spool directory is automatically created; this is where spool files temporarily reside during a download. The spool directory is created within the Pro-Watch directory.
   h. Click **Next** to display the Communications Parameters dialog box.

3. Set Communications Parameters:

   a. Select the port type from the following drop-down menu options:

Option...	Comments...
Hardwired	Designates a serial port as the primary channel communication setting. Com Port — the communication port on the host computer.
TCP/IP	Specifies that the channel is a network connection. IP Address — the IP address of the panel.

   b. Click **Next** to display the Routing Groups dialog box. Click **Add** to assign a routing group. Each printer resource can have one or more routing groups assigned to it. The routing group serves as a filter for the events that are sent to the printer.

   c. Click **Next** to display the Partitions dialog box. For information about adding partitions, see "DBC - Partitions" in Chapter 53.

   d. Click **Finish** to complete the channel.

Warning: Do not install the log printer on the Windows Operating System. The Log Printer does not function correctly if it has been installed.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Wireless Readers

19

In this chapter ...

Overview

Adding a Wireless Reader

Schlage AD-400 and AD-401

SALTO and ASSA ABLOY

Notes on SALTO Locks

Notes on ASSA ABLOY Locks

19.1 Overview

Pro-Watch 4.2 supports the following wireless readers and locks:

- Schlage model AD-400
- Schlage AD-401
- SALTO
- ASSA ABLOY

19.1.1 Panel Initialization and System Download

For wireless readers, after setting the port protocol and adding the subpanels, panel must be initialized and a system download must be performed for correct operation.

When changing the port protocols of the IC, the panel must be initialized and a system download must be performed.

19.2 Adding a Wireless Reader

19.2.1 STEP 1: Create a PW-5000 Channel

1. Launch the Pro-Watch.
2. On the left navigation panel, click and select **Hardware Configuration**.
3. Right-click and select **New > Channel** to display the **Create a Channel** dialog box.
4. From the **Channel Type** drop-down list, select PW-5000.Click **OK** to display the **Define Channel Information** dialog box.
5. Enter a **Description**. Select an appropriate **Time Zone**. Leave the default values for the **Attempts**, **Poll Delay**, and **Comm Break** fields.
6. Click **Next** to display the **Communications Parameters** dialog box.
7. Select the **Port Type** for the **primary** and **secondary** ports.
    a. If "**TCP/IP**" is selected as the Port Type in step 7, enter the **IP Address** of the PW-6000 (Honeywell Protocol) or EP-2500 (Mercury Protocol) for the primary port and the secondary port (if applicable).
8. Click **Next** to display the **PW-5000/6000 Parameters** dialog box.
9. Click **Next** to display the **Partitions** dialog box.
10. **Select** or **Add** a partition as appropriate.
11. Click **Finish** to finish setting up your channel.

Note: Before any events on this channel are reported, you must add it to the appropriate routing group(s).

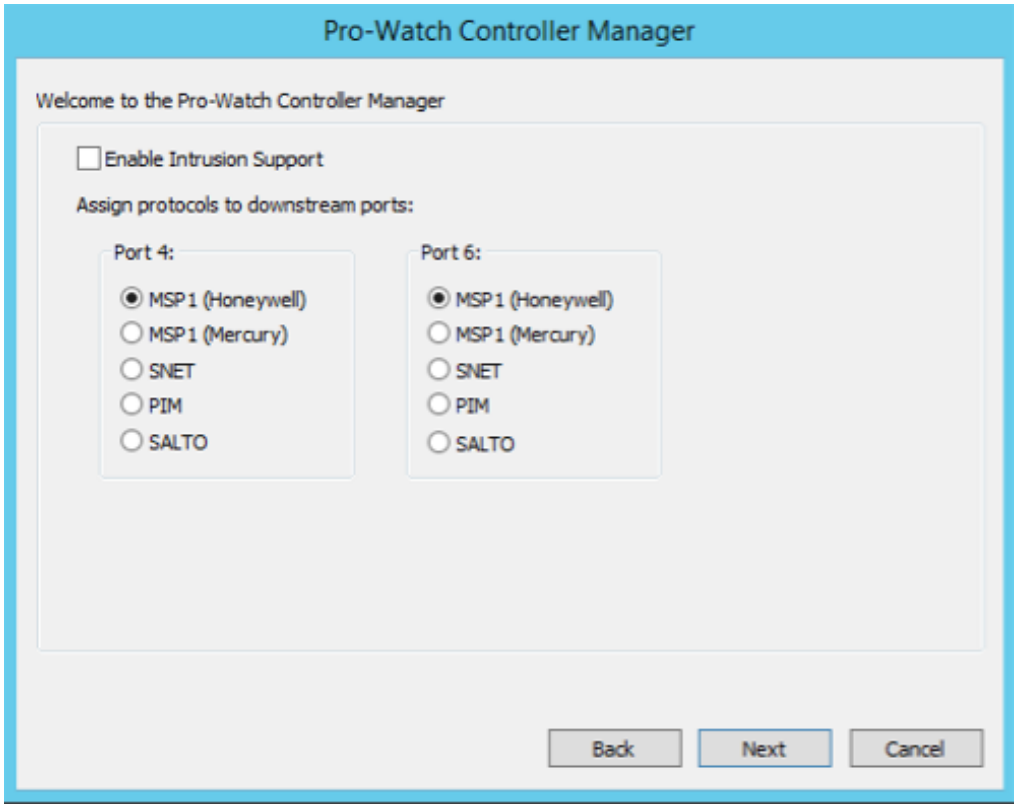
19.2.2 STEP 2: Add the Wireless Reader Panel

1. Right-click your Channel in the navigation pane and select **New > Panel** to display the **Pro-Watch Controller Manager** dialog box.
2. Select your site from the **Site** drop-down box.
3. Select the channel you've just created from the **Channel Description** drop-down box. This action will enable the **Controller Description** text field and dynamically display two new drop-down fields: **Channel Type** and **Controller Type.** Channel Type will be populated automatically.
4. Select “PW-6000” from the **Controller Type** drop-down list.
5. Enter a description in the **Controller Description** text field.
6. Leave the **Controller Address** field at its default value.
7. Click **Next** to display the **Downstream Port** dialog box.
8. For both **Port 4** and **Port 6**, select:

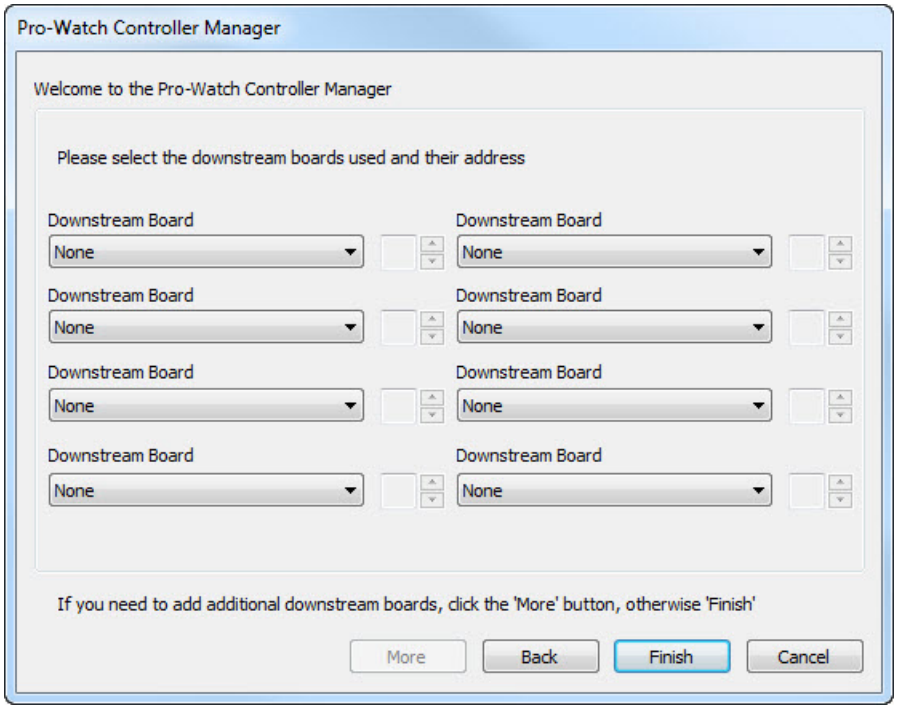
a. **MSP1** (Honeywell or Mercury to match the protocol for the ASSA ABLOY readers you have).

b. **PIM** if you are adding IR (Ingersoll Rand) reader.

c. **SALTO** if you are adding a SALTO reader.



9. Click **Next** to display the next dialog box displaying eight (8) **Downstream Board** drop-down fields:



10. Select the appropriate downstream board(s). If there are no downstream boards, select “None”.
11. Click **Finish**.

19.3 Schlage AD-400 and AD-401

Pro-Watch 4.2 supports the Schlage model AD-400 and Schlage AD-401 wireless readers/locks.

1. "Requirements"
2. "Step 1: Add the PW-6000 Panel"
3. "Step 2: Connect PW-6000 to PIM400-485 via RS-485 Port"
4. "Step 3: Configure PIM400-485 by using Schlage Hand Held Device (HHD)"
5. "Step 4: Connect the AD400/401 Door to the PIM400-485"
6. "Step 5a: Add the PIM400-485 Sub-Panel to PW-6000"
7. "Step 5b: Add the PIM400-485 Sub-Panel to PW-6000 via Wizard"
8. "Switching the Reader to PIN Mode"

Note: For more information on setting and registering these wireless readers/locks, see:

- Schlage *Networked Wireless Lock User Guide: Instructions for Adaptable Series Networked Wireless Locks*

- Ingersoll Rand *PIM400 and PIM401 User Guide: Installation and Operating Instructions for Panel Interface Modules PIM400-TD2, PIM401-TD2 and PIM400-485*

19.3.1 Requirements

PW-6000 is the only panel that supports the Schlage PIM400 and PIM401 wireless readers/locks.

Note: A single PW6000 will support up to 64 configured WAPM modules (wireless readers) across all its PIM modules. However, you can allocate 128 (8 PIMS X 16).

19.3.2 Step 1: Add the PW-6000 Panel

See Adding a PW-6000/5000/3000 Logical Device, page 35.

19.3.3 Step 2: Connect PW-6000 to PIM400-485 via RS-485 Port

All access to Schlage wireless readers/locks requires them to be attached to a PIM400-485 subpanel on a PW-6000.

Connect the PIM400-485 via the J5 Connector to the PW-6000 RS-485 port (Port 2).

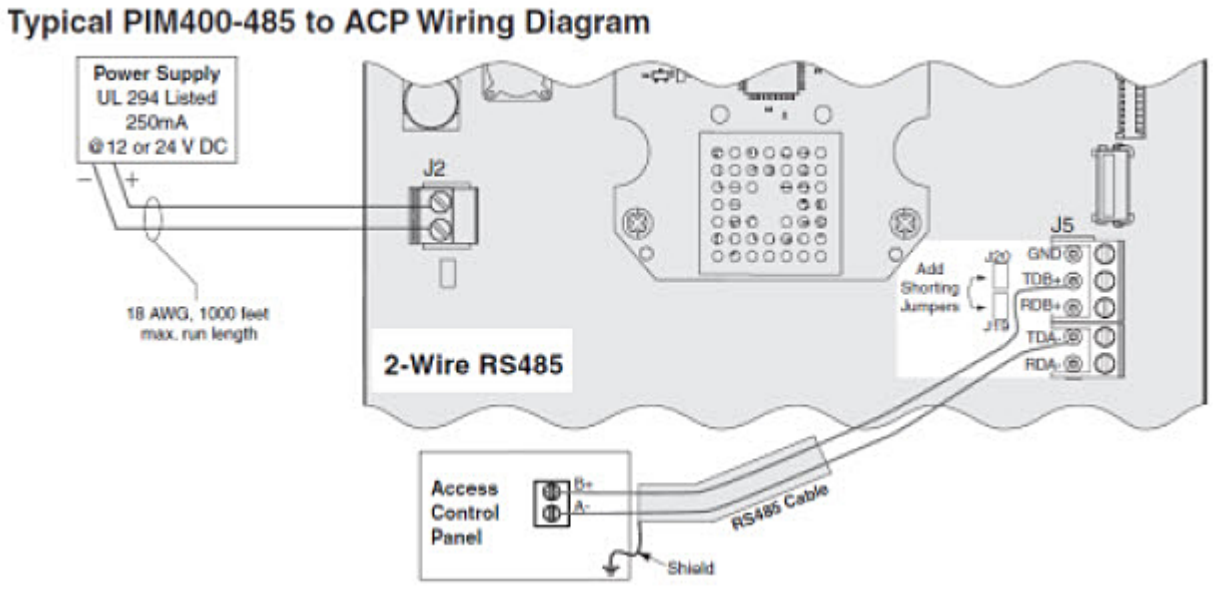


Figure 19-1 PIM400-485 to ACP Wiring Diagram

- PIM400-485 TB+ to PW-6000 TR-
- PIM400-485 TA- to PW-6000 TR+
- PIM400-485 GND to PW-6000 GND

Note: Reversing polarity will not damage either RS-485 device, it just won't communicate; if it doesn't work, switch the connections.

19.3.4 Step 3: Configure PIM400-485 by using Schlage Hand Held Device (HHD)

The wireless readers/locks communicate with the PIM sub-panel through RF (Radio Frequency). In addition to configuring the readers within Pro-Watch, you also have to configure the Schlage devices by using the **Hand Held Device (HHD)** made specifically for this purpose:

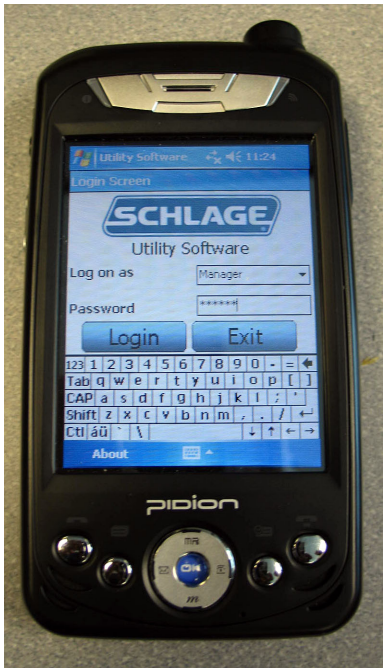


Figure 19-2 Schlage Hand Held Device (HHD)

1. Start the **Schlage Utility Software (SUS)** on the **Hand Held Device (HHD)**. The default username and password is “Manager” and “123456,” respectively.
2. Connect the HHD to the USB port of the PIM400-485. The SUS will display the PIM connection on the HHD.
3. Connect the HHD to the PIM400-485.

4. Set the PIM400-485 Address by selecting **PIM Properties > Edit > RS-485 Address**. You can also set the frequency channel in here.

19.3.5 Step 4: Connect the AD400/401 Door to the PIM400-485

1. Connect the HHD to the PIM400-485 via the USB port and start the SUS.
2. Select the PIM and click **PIM Properties > Link**:

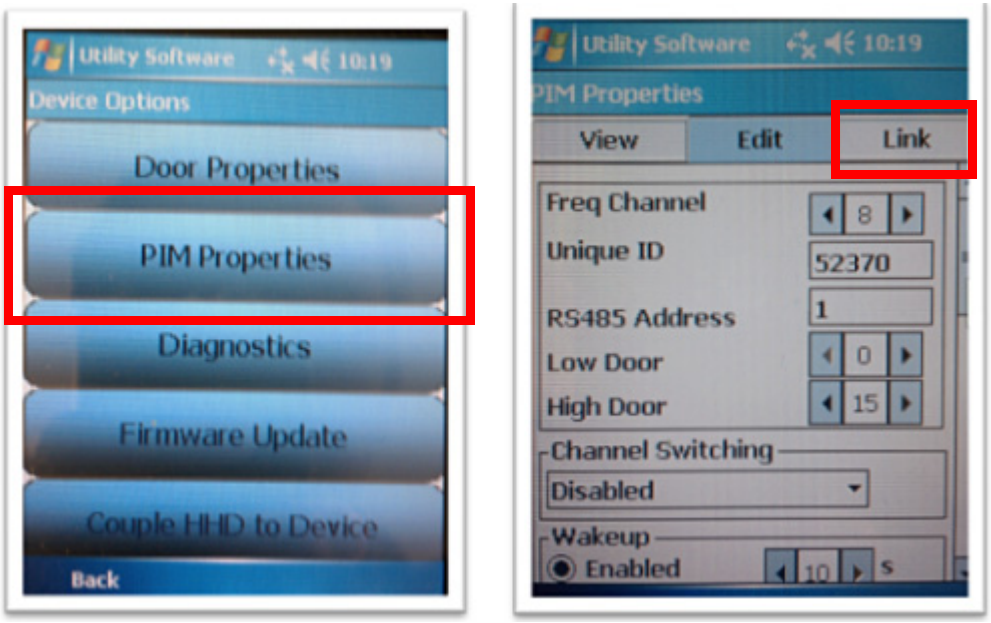


Figure 19-3 SUS PIM Properties Screen

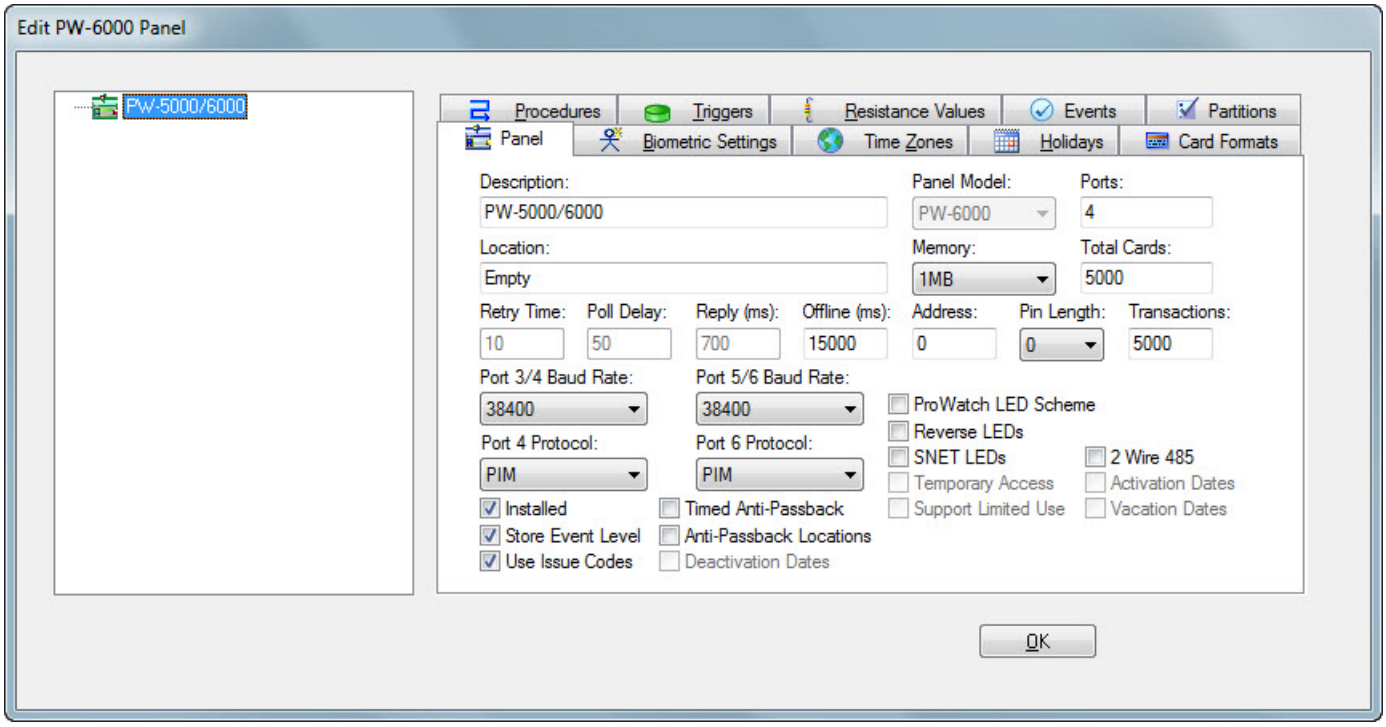
3. Select the desired Door Number (Address). The HHD will prompt you to link the door. Leave the HHD connected to the PIM while linking door.
4. On the AD400/401, hold down the inside lever (REX) and press the '#' button (or present a card to the reader). Continue to hold down the inside level until the Schlage button starts to blink green. This will be followed by a series of rapid green blinks while the AD400/401 is talking to the PIM. When linking is complete, the AD400/401 will beep; the number of beeps denotes the frequency channel it is communicating on.
5. Unplug the HHD from the PIM.

Note: You may want to connect the HHD to the AD400/401. To do this, connect to the AD400/401 via the USB port underneath the outside lock.

Press the “Schlage” button twice to link the AD400/401 to the HHD and connect the HHD to the door.

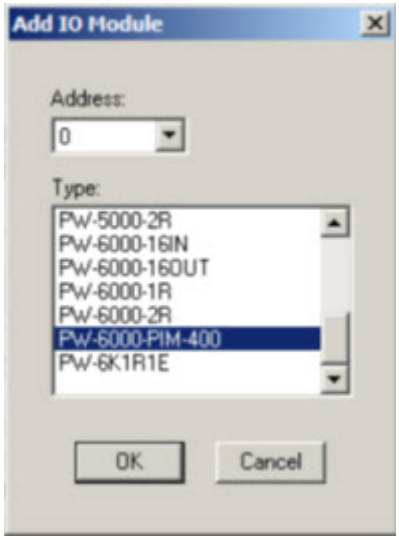
19.3.6 Step 5a: Add the PIM400-485 Sub-Panel to PW-6000

1. In Pro-Watch Hardware Configuration pane, select the PW-5000/6000 panel from the list of panels.
2. Right-click and select **Properties** to display the properties editing screen:

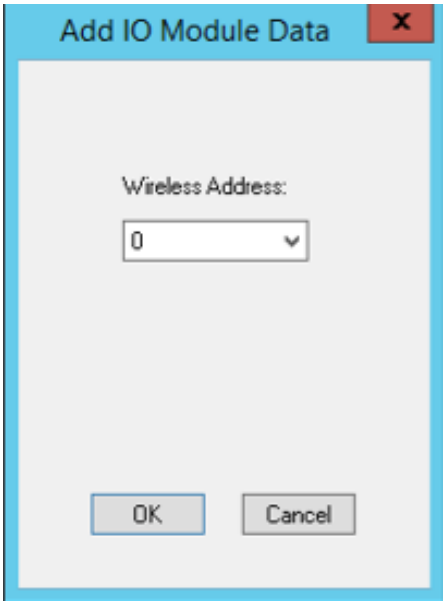


Note: **Port 4 Protocol** MUST be have been set to “**PIM**” when the panel was first created in order to add the PIM400-485 sub-panel.

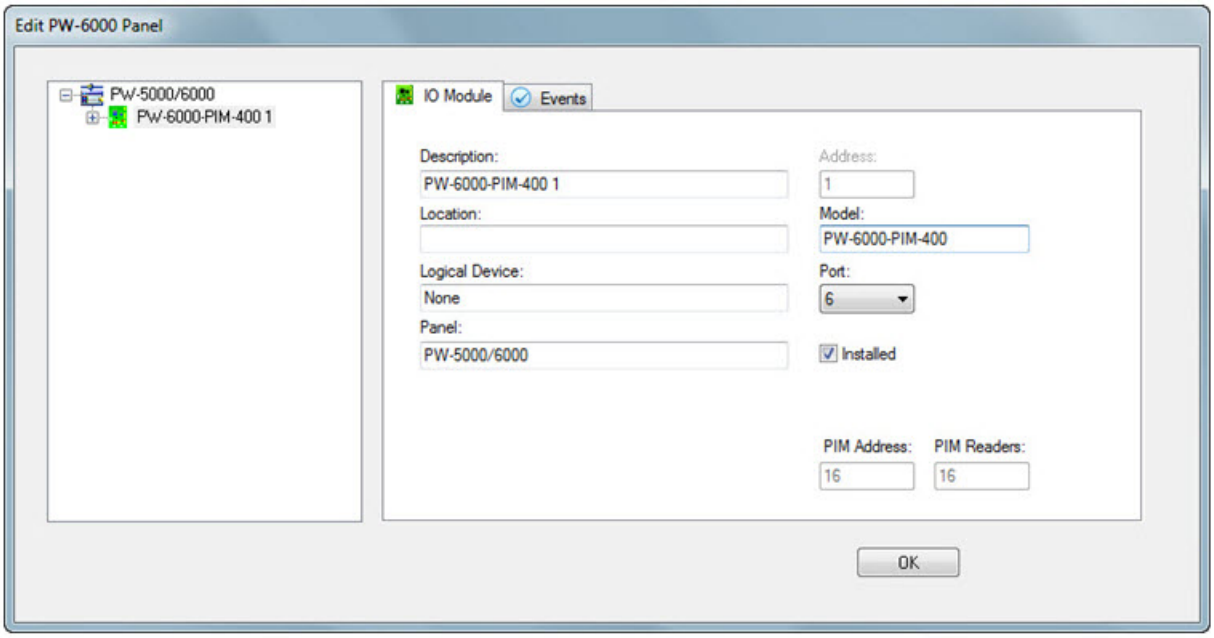
3. Right-click the panel icon on the left pane and select **Add IO Module** for the new sub-panel to display the respective list screen:



4. Select **PW-6000-PIM-400** for **Type** and **any available Address** and click **OK** to display the **PIM Address** screen:

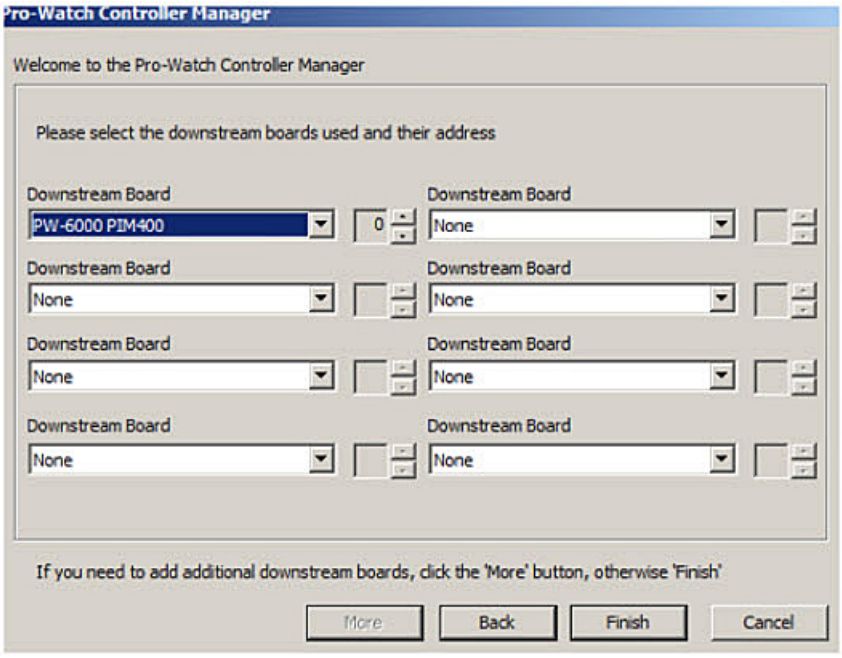


5. Select the base wireless address for the PIM and click OK. This address must match the base RS-485 Address in the PIM, which is set with the Hand Held Device. **Address 0** creates reader addresses 0 - 15. **Address 16** creates addresses 16 - 31. The address is limited to values in the range 0-240, and represents the address of the lowest WAPM on that PIM. Pro-Watch will display the IO Module configuration screen for the new sub-panel:


Edit PW-6000 Panel
PW-5000/6000
PW-6000-PIM-400 1
IO Module
Events
Description:
PW-6000-PIM-400 1
Location:
Logical Device:
None
Panel:
PW-5000/6000
Address:
1
Model:
PW-6000-PIM-400
Port:
6
Installed
PIM Address:
16
PIM Readers:
16
OK

19.3.7 Step 5b: Add the PIM400-485 Sub-Panel to PW-6000 via Wizard

1. Add PW-6000 channel and panel. See Adding a PW-6000/5000/3000 Logical Device, page 35.
2. When the Wizard prompts for downstream panels, select **PW-6000-PIM400** and the address. The address selected is NOT the RS-485 address of the PIM. The 485 address will be selected later. Click **Finish**:



19.4 SALTO and ASSA ABLOY

SALTO and ASSA ABLOY wireless locks are not connected to a Pro-Watch system directly but through control unit(s) and routers.

19.4.1 SALTO System Configuration

SALTO system configuration requires:

1. Either EP-2500 or PW-6000 controller
2. Sallis Router

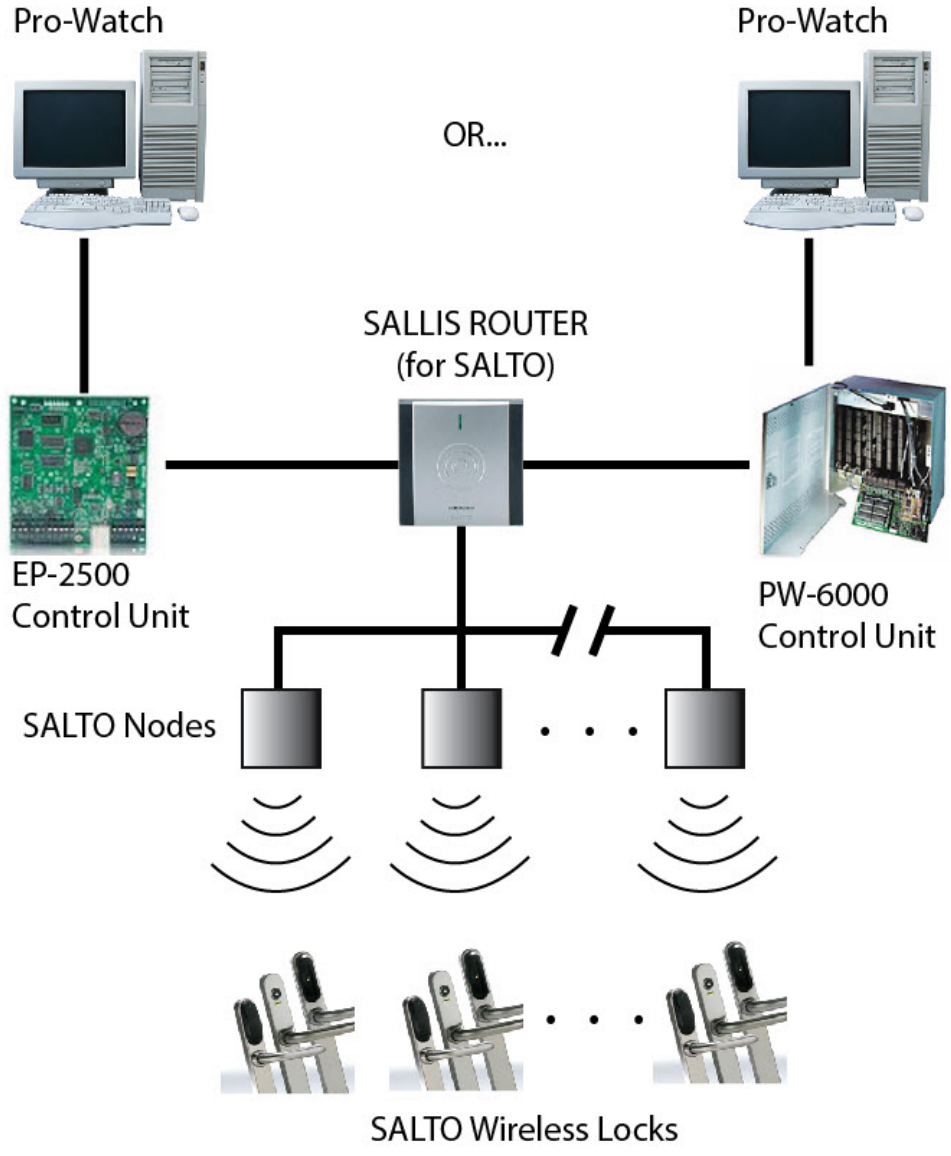


Figure 19-4 SALTO Wireless Reader System Configuration

19.4.2 ASSA ABLOY System Configuration

ASSA ABLOY system configuration requires:

1. PW-6000 (Honeywell Protocol) or EP-2500 (Mercury Protocol)
2. Aperio hub (Honeywell or Mercury Protocol)

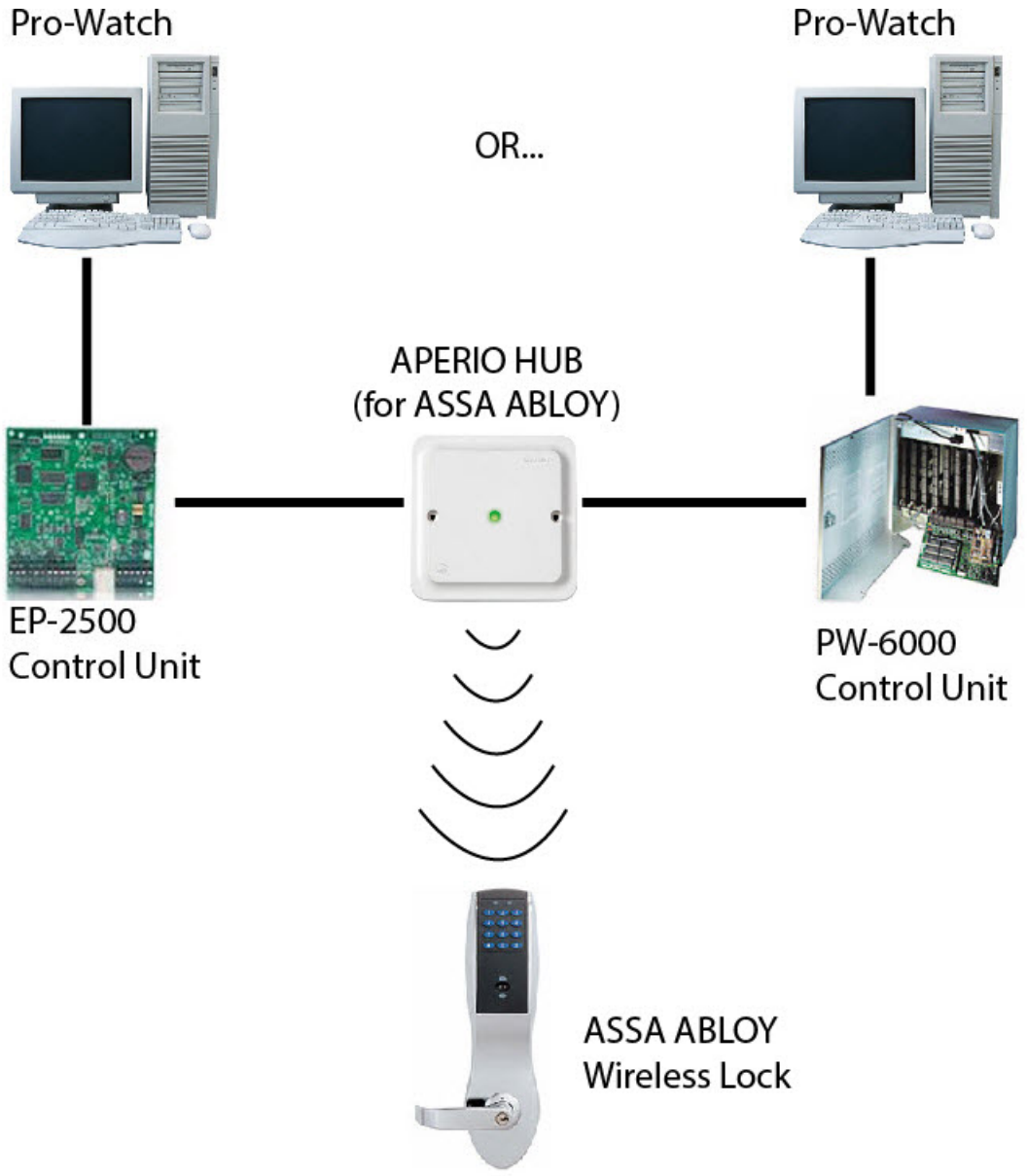


Figure 19-5 ASSA ABLOY Wireless Reader System Configuration

19.5 Notes on SALTO Locks

The SALTO locks will not report up individual door openings and closings. The reader should be setup to always assume that the door was used (unless an additional Mercury input is configured for the door contact). Due to this behavior, the lock should not be used in applications where it is necessary to know if the door was opened or not. This would include applications like strict anti-passback, two card control, man traps, etc.

19.5.1 Door Held Open Behavior

Since the SALTO locks due not report up the door opening and closing transactions the door held open processing cannot be handled by the EP. SALTO will report up the door held open event 40 seconds after the door was opened. When the door is closed the proper restored event will be reported. Pre-Alarm will not be able to be used due the EP not controlling when the door held open is generated. This functionality should not be used with these locks.

19.5.2 Request to Exit (REX) Behavior

If the REX is used multiple times within 10 seconds, only the first occurrence is reported. The additional uses of the REX will not be reported.

19.5.3 Door Forced Open Behavior

The door forced open transaction will be generated if the door is forced open and the proper restoring transaction will be generated after the door is closed. Multiple door forced occurrences within 10 seconds of the initial occurrence will not be reported by SALTO.

19.5.4 External Door Contact / REX

At this point in time an external door contact and REX located on another SIO is not supported. Please contact Mercury if you need more information regarding this type of configuration

19.5.5 No Host-Grants for SALTO Readers

19.5.5.1 Issue Description

Imagine a general situation in which a card is created in Pro-Watch's badging module but is not downloaded to the controller panel.

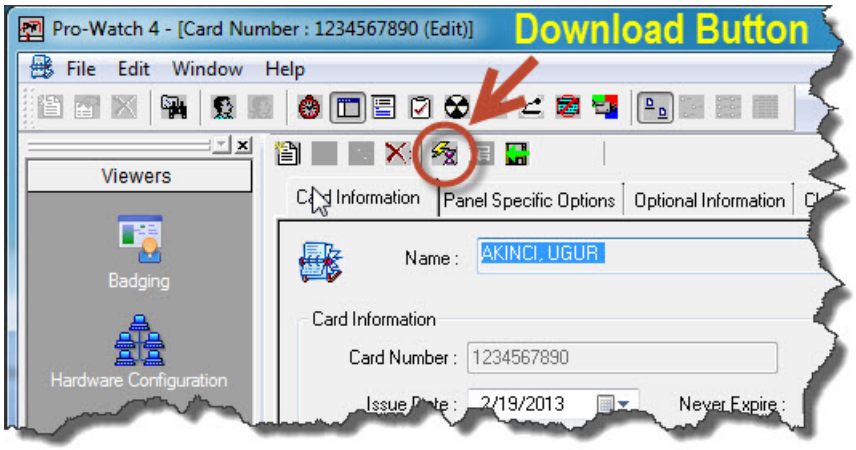
When such a card is presented at a reader, Pro-Watch sends a host-grant message to the controller. That will trigger a local-grant message and as a result the door will unlock.

This does not happen with SALTO wireless locks.

If a card is not downloaded to the controller panel after it is created in Pro-Watch, then the door will not unlock when the card is presented at a SALTO wireless reader.

19.5.5.2 Solution

After creating the card in the Pro-Watch's badging module, click the download button in the toolbar:



After the initial host-grant, Pro-Watch will download the card to the panel so that all subsequent card swipes should generate local-grants.

19.5.6 Number of SALTO readers

The number of SALTO readers configured for a SALTO subpanel must be at least as large as the highest lock number on the SALTO router.

19.6 Notes on ASSA ABLOY Locks

19.6.1 Unlock Operations Not Supported

ASSA ABLOY wireless locks do not support unlock operations.

19.6.2 Fixed-length PIN Codes

ASSA ABLOY locks have to be configured with fixed-length PIN codes. The length of the PIN code needs to match that for the control panel.

1. Enter the RS-485 address of the PIM.
2. Click **Finish**.

19.6.3 Switching the Reader to PIN Mode

Step 6: Switching the Reader to PIN Mode

1. Click the appropriate **Logical Device** folder in the **Hardware Configuration** screen to display the site's existing **Logical Devices**.
2. In the list of Logical Devices, right-click the Wireless Reader you want to configure, and select **Properties**. The **Edit Logical Devices** [Logical Device name] screen appears.
3. Select the **Logical Device Details tab** and click **Edit** to display the **Edit Reader** screen.
4. Click and select the **Reader Settings tab** to display the **Reader Settings** screen.
5. Select the **PIN Required** check box to put the reader into Card-and-PIN mode indefinitely.
6. Click **OK** to save the setting.

19.6.4 No Host-Grants for ASSA ABLOY Readers

19.6.4.1 Issue Description

Imagine a general situation in which a card is created in Pro-Watch's badging module but is not downloaded to the controller panel.

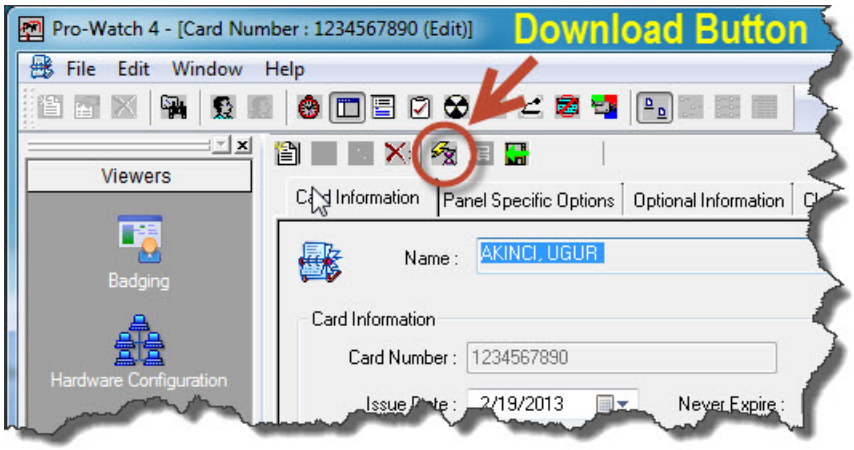
When such a card is presented at a reader, Pro-Watch sends a host-grant message to the controller. That will trigger a local-grant message and as a result the door will unlock.

This does not happen with ASSA ABLOY wireless locks.

If a card is not downloaded to the controller panel after it is created in Pro-Watch, then the door will not unlock when the card is presented at a ASSA ABLOY wireless reader.

19.6.4.2 Solution

After creating the card in the Pro-Watch's badging module, click the download button in the toolbar:



After the initial host-grant, Pro-Watch will download the card to the panel so that all subsequent card swipes should generate local-grants.

19.6.5 Mechanical Key May Generate “Forced Door” Message

If the ASSA ABLOY reader is not the L100 type, using a mechanical key will generate a “Forced Door” event message.

The users can add a second REX to ASSA ABLOY L100 readers and Pro-Watch will display a request to exit message. For such L100 readers, using a mechanical key (with a second REX) will not generate a “Forced Door” message.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config – Status & Panel Download

20

In this chapter ...

Overview
Channel Status
Panel Status
Panel Download

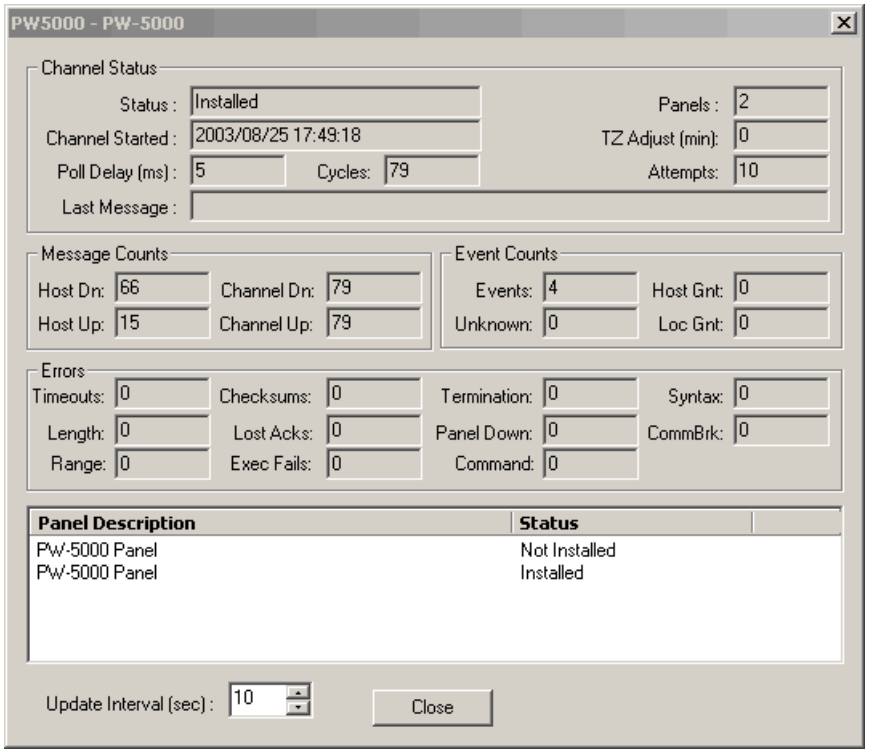
20.1 Overview

Pro-Watch allows the user to check channel as well as panel status.

20.2 Channel Status

To view channel status:

1. Select the channel and right-click.
2. Select **Status**. The Channel Status dialog box displays information regarding the channel and any panels attached to the channel, including any transactions that may have of occurred.



3. Click **Close** once you have completed examining the channel status.

20.3 Panel Status

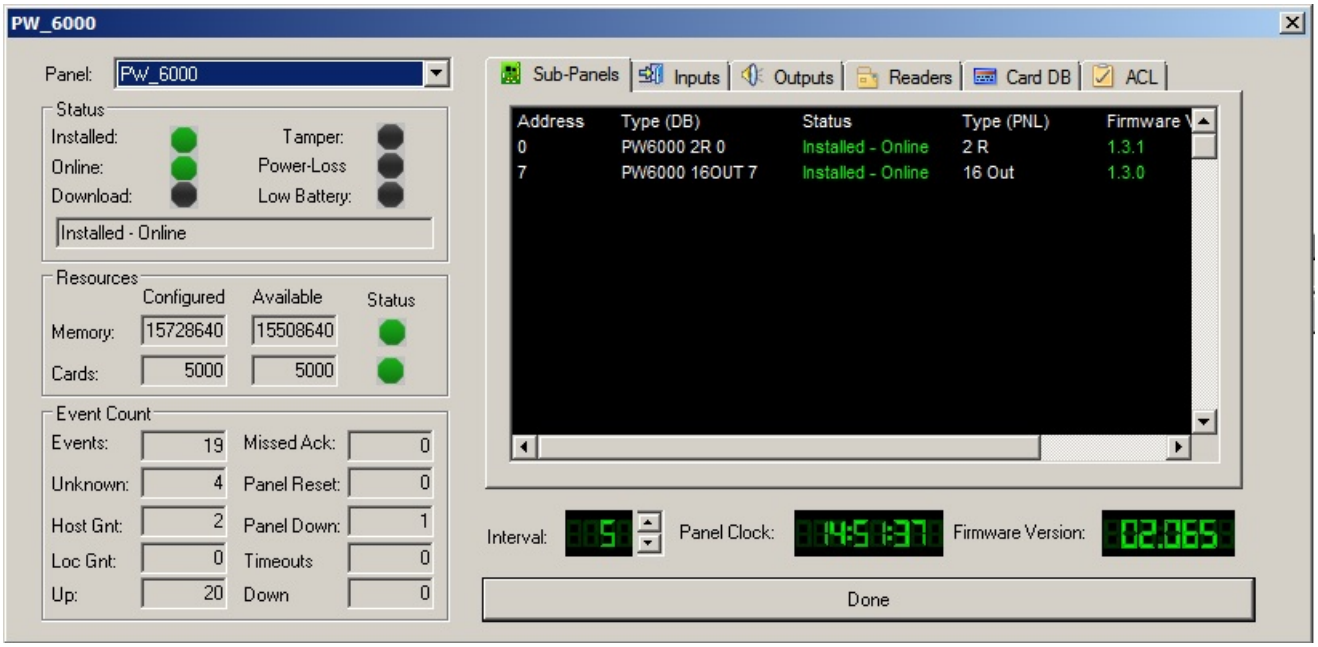
To view panel status (or Status Monitor):

1. Select the panel and right-click.

   Note: Select **Status**. The Panel Status dialog box appears. The Status Monitor allows you to view the status of the panel, sub-panels, and Logical Devices in real-time. For some panel types, the dialog box also displays the **Firmware Version**.

   Note: In addition, the **Subpanel tabs** of **PW-3000, PW-5000, PW-6000** and **Mercury** panels also display **subpanel firmwave versions** (see the screenshot below).

   Note: You can use the encrypted (E) version of firmware for both encrypted and nonencrypted communication.



2. Select the panel you want to view from the panel drop-down list. The panel status information automatically refreshes.The panel status dialog box shows when there is a download occurring, any alarm states such as Tamper, Power-Loss, and Low Battery, as well as the number of specific events that have occurred. If there are multiple panels attached to the channel, you may select each panel to view the status.
3. Select the applicable tab. Each Logical Device tab displays the status of each Logical Device.

4. The PW6K1ICE panels report additional status information. To view the PW6K1ICE reporting status, click the **Card DB** tab. The table below summarizes the PW6K1ICE panel reporting capabilities.

Parameter	Value
Number of Card Holders	Reports the number of cardholders the panel will support.
Number of ALVL per Card	Reports the number of access levels allowed per card. Note that a Clearance Code is correlated with an access level; therefore, you can set only 12 Clearance Codes per Card.
Number of PIN Digits	Reports the number of PIN digits the panel will support.
Issue Code	Reports the issue code.
Store Anti-passback location	Reports whether anti-passback locations are supported.
Store Activation Date	Reports whether the activation date is stored.
Store Deactivation Date	Reports whether the deactivation date is stored.
Store Vacation Date	Reports whether the vacation date is stored.
Store Temp ALVL Upgrade Date	Reports whether the temporary access level upgrade date is stored.
Store User Level	Reports whether the user level is stored. Note that this field corresponds to the Store Event Level check box on the panel tab.
Store Use Limit	Reports whether the use limit is stored.
Store Time of Last Entry	Reports whether the time of last entry is stored.
Precision Acc: Number of ACR to Save TZ	Reports the number of door time zones that is saved per card.
Enable Precision Access	Reports whether precision access is enabled.

Note: To refresh the panel reporting information, click **Card DB Info**. Note that the PW6K1ICE panel also reports access level status. To view which access levels are downloaded to the panel, click the **ACL** tab. To refresh the access level information, click **ACL Info**. The ACL Info list includes the Clearance Codes that are assigned to the Logical Devices configured for the panel. There can be a maximum of 128 (0-127) access levels (Clearance Codes) for a PW-5000 panel. ACL=0 is the default level and provides all access.

Within the status monitor, you can also perform "HW Config - Hardware Actions" in Chapter 24 for output and input points.

To initiate a hardware action for an output point:

1. Click the **Outputs** tab.
2. Select an output point. Note the output point must be a member of a Logical Device.
3. Click **Activate**, **Deactivate**, or **Pulse**. To refresh click **Output Info**.

To initiate a hardware action for an input point:

1. Click the **Inputs** tab.
2. Select an input point. Note the input point must be a member of a Logical Device
3. Click **Mask** to mask the action on the monitor, or **Unmask** to display the action on the monitor. To refresh, click **Input Info**.

To initiate a hardware action for a reader:

1. Click the **Readers** tab.
2. Select an reader. Note the reader must be a member of a Logical Device
3. Click **Re-enable**, **Lock**, or **Unlock**.To refresh, click **ACR Info**.

When you have completed viewing the status monitor, click **Done**.

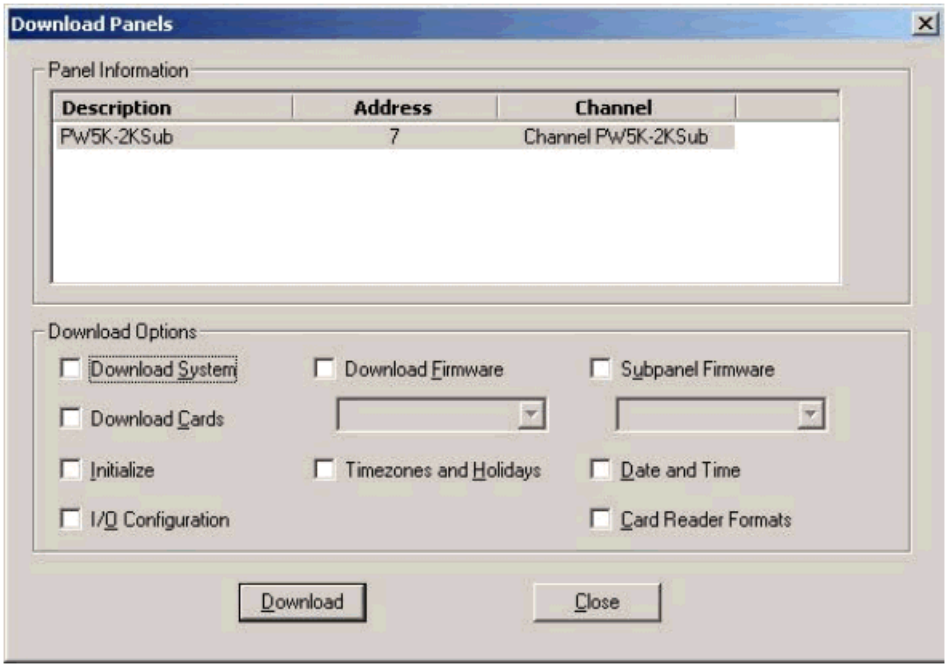
20.4 Panel Download

Pro-Watch allows the user to initialize and download the panel or particular resources to the panel.

Note: If you are downloading PW-3000 firmware to configure a panel for the Pro-Watch biometric hand geometry reader, use the downloading procedures given in Chapter 62, *Biometric Reader Configuration*.

Follow these steps:

1. Select the panel and right-click.
2. Select **Download**.



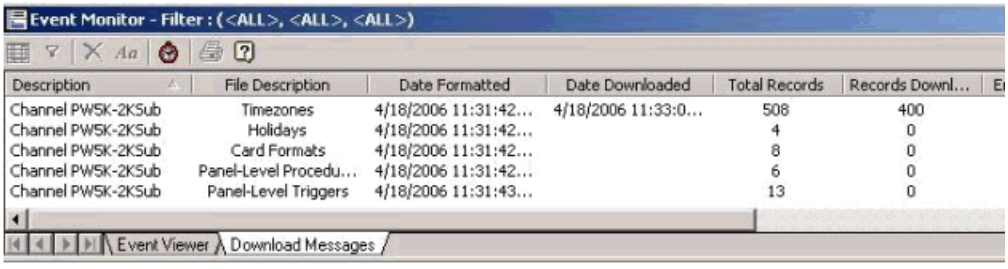
The following table describes the function of each check box:

Field	Description
Download System	Downloads everything to the panel except cards.
Download Cards	Downloads cards to the panel.
Initialize	Erases the panel's memory (PW2000); erases the cards from the panel. (PW6K1ICE and Cardkey).
I/O Configuration	Downloads the I/O configuration to the panel.
Download Firmware	Downloads the firmware of the panel (PW6K1ICE).

Field	Description
Timezones and Holidays	Downloads time zones and holidays to the panel.
Subpanel Firmware	Downloads the sub-panel's firmware to the panel (PW6K1ICE). Does not include PW2000 as a sub-panel.
Card Reader Formats	Downloads card reader formats to the panel.
Date and Time	Downloads the date and time to the panel.

3. Select the check boxes in which you want to download to the panel and click **Download** to accept the changes to the panel. Although this changes the panel's properties, you must still re-initialize and download the panel manually.
4. Click **Panels** under the appropriate Site folder in the Hardware Configuration tree to display the panel icon.
5. Right-click the panel's icon and select **Download**.
6. De-select **Download System**.
7. Select **Initialize**.
8. Click **Download** to re-initialize the panel. Note that this step only re-initializes the panel.
9. When the panel icon re-appears, right-click the icon and select **Download**.
10. Select **Download System** and **Download Cards**.

For more information on downloading panels, see "Panel Download". You can monitor the downloading status in the Download Messages tab in the Event Monitor, as shown below:



Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - CCTV

21

In this chapter ...

Overview
Configuring CCTV
Configuring Analog CCTV
Adding CCTV Monitors
Deleting CCTV Monitors
Adding CCTV Camera Views
Calling Up Camera Views
Using CCTV Commands
CCTV Controls

21.1 Overview

This chapter describes how to configure CCTV (Closed Caption TV) cameras, monitors and camera views for Pro-Watch.

21.2 Configuring CCTV

Pro-Watch CCTV controls allow you to perform these tasks:

- Select a surveillance camera associated with a monitor.
- Switch the video of the selected camera to the selected monitor.
- Set a preset, pan/tilt/zoom, and focus.
- Set the iris of the selected camera for the best video contrast.

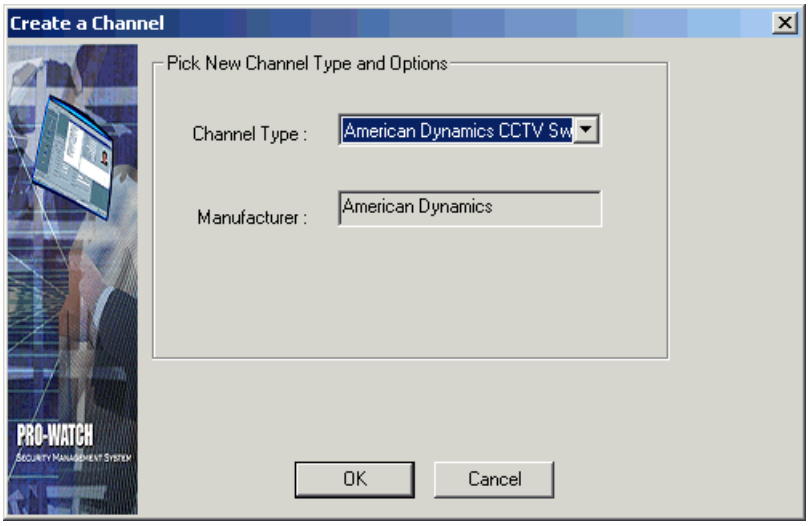
21.3 Configuring Analog CCTV

Pro-Watch supports these analog CCTV switchers:

- American Dynamics.
- VideoBlox.
- Pelco.
- Burle.
- MaxPro.

To configure CCTV:

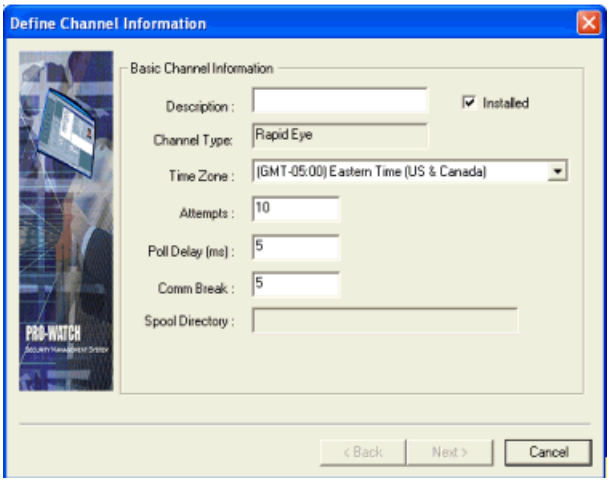
1. Select a channel type.
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel.** The Create a Channel dialog box appears.



   b. Select a channel type specific to your hardware manufacturer from the drop-down list.
   c. Click **OK**. The Define Channel Information dialog box appears.

2. Define the channel.

   a. In the Define Channel Information dialog box, enter an identifying channel description.



   b. Select the **Installed** check box. This assures the channel is installed and operational.

   c. Select a time zone from the drop-down list.

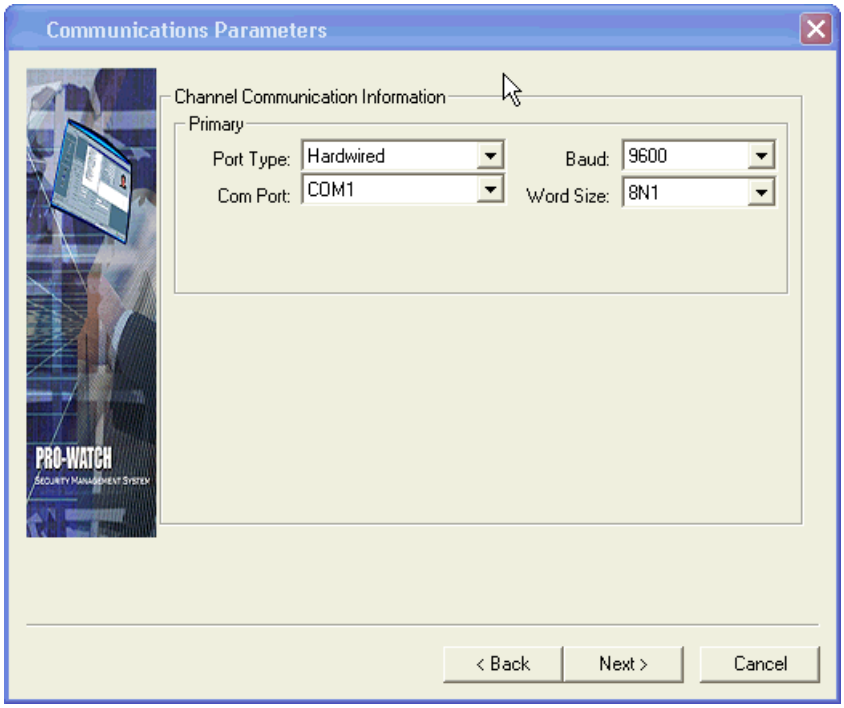
   d. Enter the maximum number of poll attempts.

   e. Enter the poll delay interval between each polling. This number is in milliseconds.

   f. Enter the communications break; the host must receive communication from the device within the specified time or the host determines the communication as broken.

   g. The spool directory is automatically created; this is where spool files temporarily reside during a download. The spool directory is created within the Pro-Watch directory.

h. Click **Next** to display the Communications Parameters dialog box.



3. Set communications parameters. Select the port type from the following drop- down list options:

Option	Comments
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. Com Port – the communication port on the host computer. Baud – the rate of communication.
TCP/IP	Specifies that the channel is a network connection. IP Address – the IP address of the CCTV switcher.

4. Click **Next** to display the Partitions dialog box. For more information, see "DBC - Partitions" in Chapter 53.
5. Click **Finish** on the Partitions dialog box to complete channel add. A warning message appears notifying you to add the channel to the appropriate routing group.

21.4 Adding CCTV Monitors

The next task in setting up CCTV is to add CCTV monitors. CCTV monitors are associated with workstations. After completing CCTV configuration, you must add the monitor to the workstation. For more information, see "DBC - Workstations" in Chapter 59.

To add a CCTV Monitor:

1. Select the **CCTV channel**, right-click, and select **New** > **CCTV Monitor** to display the CCTV Monitor View dialog box
2. Enter the **description** for the CCTV Monitor. The channel in which the monitor is assigned is identified.
3. Select the **port number** from the drop-down list. The port number corresponds to the physical port number on the back of the CCTV switcher. Each port number must be unique.
4. Enable Auto switch cameras. The Command ID does not function. The site in which the monitor is assigned is identified.
5. Click **OK.**

To edit a CCTV Monitor:

Select the monitor from the Hardware Configuration Window, right-click, and select **Properties**.

21.5 Deleting CCTV Monitors

Use this function to delete a CCTV Monitor from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the site icon to display the site's folder icons in the right pane.
2. Click the CCTV Monitors folder to display the icons of existing CCTV Monitors.

Note: Right-click the CCTV Monitor you want to delete and select **Delete**.

You cannot delete a CCTV Monitor that has dependencies. A dependency is another database object that includes the CCTV Monitor in its configuration. The CCTV Monitor object depends upon the Workstation object. If the CCTV Monitor has no current dependencies, you are prompted to confirm the deletion. However, if the CCTV Monitor does have current dependencies, the Dependencies dialog box appears.

3. If you still want to delete the CCTV Monitor:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
4. Repeat step 3 and click **Yes** at the prompt to delete the CCTV Monitor.

Viewing Dependencies of a CCTV Monitor

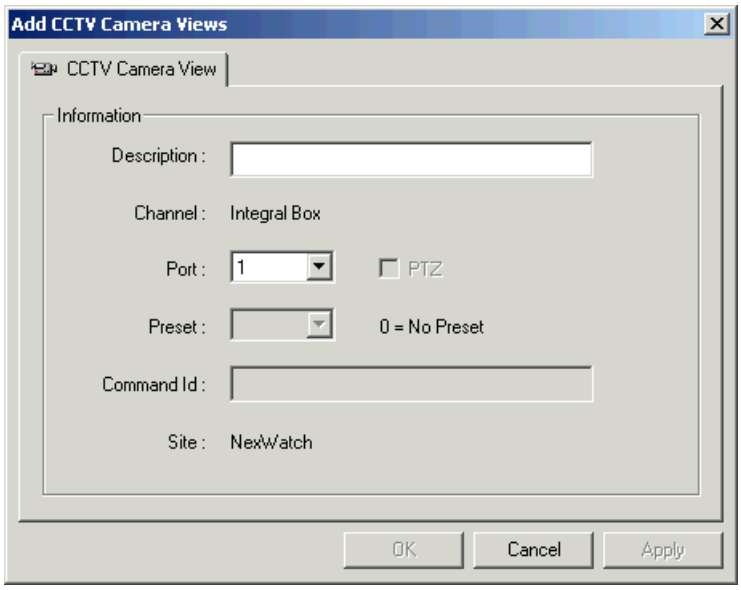
Use this function to view and modify the CCTV Monitor's dependencies. The CCTV Monitor object depends upon the Workstation object.

1. In the Pro-Watch Database Configuration tree list, click the site icon to display the site's folder icons in the right pane.
2. Click the CCTV Monitors folder to display the icons of existing CCTV Monitors.
3. Right-click the icon of an existing CCTV Monitor in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the CCTV Monitor's dependencies.
4. To modify or remove the dependency, click the specific dependency in the list to display its Edit dialog box.
5. After you finish viewing, click **OK** to close the dialog box.

21.6 Adding CCTV Camera Views

The next task in setting up CCTV is to add CCTV camera views.

1. In the Hardware Configuration tree view, click the Channels folder to display the channel icons.
2. Right click the appropriate channel icon and select **New** > **CCTV Camera View**. The Add CCTV Camera Views dialog box appears.



3. Enter the description for the CCTV Camera View.
4. Select the port number from the drop-down list. The port number corresponds to the physical port number on the back of the CCTV switcher. Each port number must be unique (that is, you can assign only one camera view to a port).
5. Select the **Preset** from the drop-down list. Preset is applicable to pan/tilt/zoom (PTZ) cameras only. The Command ID is not functional. The site in which the monitor is assigned is identified.
6. Click **OK.**

Camera views are associated with Logical Devices or event points. You may assign a CCTV camera view to either Logical Device, event point, or both. CCTVs assigned at the event level, when manually initiated, call up the assigned camera view for particular events. Similarly, CCTVs assigned to the Logical Device call up a camera view when manually invoked. (See your panel's Logical Device configuration instruction or "HW Config - Edit Point" in Chapter 25).

21.7 Calling Up Camera Views

To manually call-up a camera view assigned to a Logical Device, right-click the Logical Device icon and select **Show CCTV Camera View**.

You may also change the monitor in which the camera view is displayed.

To change the monitor display for a camera view:

1. Select the physical camera that was added and right-click.
2. Select **Show on Monitor 1** or **Show on Monitor 2** to receive a camera view.

To edit a CCTV Camera View:

Select the camera view from the Hardware Configuration Window, right-click, and select **Properties**.

21.8 Using CCTV Commands

CCTV commands allow you to send commands manually or automatically. You can assign CCTV commands to events or to Logical Devices. CCTVs assigned at the event level can initiate a command upon a certain event. A default auto CCTV command initiates at the time of the alarm, and there are no particular monitors associated with the command. A default select CCTV command is manually called up from the workstation.

Adding a CCTV Command

1. From the Hardware Configuration tree view, select CCTV Commands.
2. Right-click anywhere in the hardware configuration window and select **New CCTV Command** to display the Add CCTV Commands dialog box.
3. Enter the description of the CCTV Command and click **Add** to display the Define Command Detail dialog box.
4. Select the sequence number from the drop-down list.

5. Select the command from the drop-down list. Depending on the command chosen, only applicable fields will be enabled. Use the table below to complete command configuration.

Field	Description
CCTV Monitor	Defines the CCTV monitor that applies to the command.
CCTV Camera View	Defines the CCTV camera view that applies to the command.
PTZ Preset	Defines the PTZ preset that applies to the command.
CCTV Channel	Defines the CCTV channel that applies to the command.
Raw Command	Defines the raw command (as configured by the user) that applies to the command.

CCTV Camera Views can also be added to a map. A camera view can only be added to a single map. For further information, see Chapter 61, *Map Building*.

Deleting a CCTV Command

Use this function to delete a CCTV Command from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **CCTV Commands icon** to display the command icons in the right pane.
2. Right-click the CCTV Command you want to delete and select **Delete**. Note that you cannot delete a CCTV Command that has dependencies. A dependency is another database object that includes the CCTV Command in its configuration. The CCTV Command object depends upon the Event and Logical Device objects. If the CCTV Command has no current dependencies, you are prompted to confirm the deletion. However, if the CCTV Command does have current dependencies, the Dependencies dialog box appears.
3. If you still want to delete the CCTV Command:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
4. Repeat step 2 and click **Yes** at the prompt to delete the CCTV Command.

Viewing Dependencies of a CCTV Command

Use this function to view and modify the CCTV command's dependencies. The CCTV command object depends upon the Event and Logical Device objects.

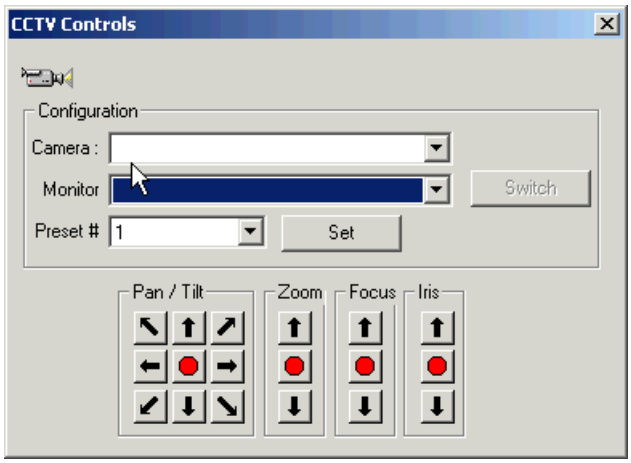
1. Right-click the icon of an existing CCTV command in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the CCTV Command's dependencies.
2. To modify or remove the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

21.9 CCTV Controls

CCTV Controls allow you to control the camera from the workstation. Use either of two methods to display the CCTV Controls:

Method 1

1. From the Hardware Configuration tree view, click the **Channel** folder to display the channel icons.
2. Right-click the appropriate CCTV channel icon and select **Actions > CCTV Controls** to display the CCTV Controls dialog box.



Method 2

You can also access CCTV Controls from the toolbar by selecting the camera icon. CCTV controls enable you to select a camera and monitor, switch the camera's video to the selected monitor, view presets, pan, tilt, zoom, focus, and change the iris of the selected camera.

1. Select the camera from the pull-down Camera menu.
2. To switch the camera's view to a monitor, select the monitor from the drop-down Monitor list and click **Switch**.
3. To set the camera and view to a preset position, select the position from the drop-down Preset # list.
4. Use the Pan/Tilt arrows to move the view to the desired spot. Clicking an arrow moves the camera view in the indicated direction until you click the red stop sign.
5. Use the Zoom arrows to zoom in (Up arrow) or zoom out (Down arrow).
6. Use the Focus arrows to adjust the proper focus.
7. Use the Iris arrows to adjust the view's area.
8. Click **Set** to set the configuration.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config – DVR

22

In this chapter ...

Configuring Digital Video Recording (DVR)
Configuring HVMS in Pro-Watch
Using HVMS in Pro-Watch
Configuring DVR

22.1 Configuring Digital Video Recording (DVR)

Pro-Watch supports Digital Video Recording (DVR), including Integral, Rapid Eye, VAST, Vicon, Honeywell Digital Video Manager (DVM), and Honeywell FUSION DVR. With Digital Video Recording, Integral, Rapid Eye, VAST, and Honeywell Digital Video Manager, you can associate a camera with a Pro-Watch Logical Device. Then, you can use the Pro-Watch Alarm Monitor or Event Viewer to display the video that occurred at the time of an alarm at that Logical Device by right-clicking the camera icon next to the alarm. With Integral DVR, Honeywell DVM, or Honeywell FUSION DVR, you can also search for and display video that occurred during any time you specify.

If you have purchased the Honeywell Video Management System (HVMS) option, you have additional tools that provide central control of any configured DVR package. For example, you can view and act upon any video device from within Pro-Watch and from a single system. See "Configuring HVMS in Pro-Watch" for more information about HVMS.

Notes**:**

- Pro-Watch Lite supports only Rapid Eye DVR.
- No Integral DVX video is accessible from the Event Viewer or the Alarm Monitor.
- When installing Honeywell DVM, make sure that the account under which Pro-Watch Service is started is included in the Oper and Oper Area tables of the DVM Database. If these tables do not include the Pro-Watch Service account, you will not get events in Pro-Watch.
- For FUSION, motion and the event must occur simultaneously to produce a video icon on the Event Viewer and Alarm Monitor.
- If you are using Integral or Honeywell FUSION, be sure that the time clocks for the video server and Pro-Watch server are synchronized. If the clocks are not synchronized, the search feature may not operate properly.
- VAST supports a maximum of seven live views; FUSION supports a maximum of 16 live views.
- Vicon supports one live video per camera at one time in the verification viewer. Although Pro-Watch does not prevent a user from starting a second live view from the same camera, the second video does not appear. Vicon also supports live video in the MUX Viewer. As in live video, however, only one live video is allowed per camera. MUX Viewer does prevent the user from starting the second live view from the same camera.
- Playback video in Vicon does not support clips.
- Vicon video supports only motion and video loss events. It does not yet support channel events.

Pro-Watch Software Suite, Release 3.71, supports the following DVR software versions:

DVR Software,	Versions Supported by Pro-Watch
Integral	Primary Control (for DVXi), version 4.1 SR2. DigitalSENTRY, version 2.1.0.
Rapid Eye	Versions 7; client builds 56.
VAST	Versions 1.9.3.b or 1.10.1.
Vicon	Version 3.2 (server), 3.2.3 (client)
Honeywell DVM	Version 200.2.5764.
Honeywell FUSION	Version 3.0

Caution: To configure DVR, you first must create a channel and at least one CCTV camera view.

Note: If you are configuring Integral, Rapid Eye DVR, Honeywell DVM, or Honeywell FUSION DVR, be sure the video server is already installed and configured. See the manufacturer's documentation for those instructions.

22.2 Configuring HVMS in Pro-Watch

HVMS (Honeywell Video Management System) is a video management system that connects to video recording subsystems such as Digital Video Recorders (Rapid Eye and Fusion, for example). The HVMS server collects information from the video subsystems, manages information in its Structured Query Language (SQL) 2005, and provides HVMS client systems with the gathered information.

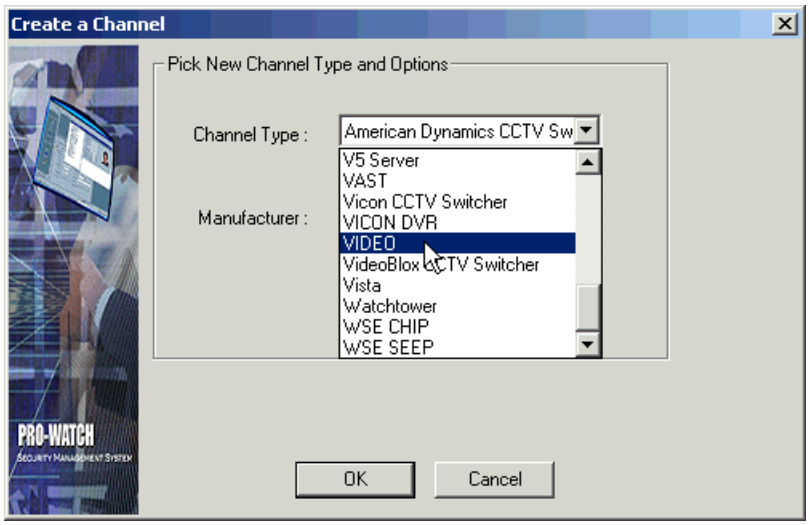
You install and configure the video subsystems independently as you normally would. Then, you install HVMS on top of these subsystems.

The integration of HVMS with Pro-Watch requires hardware configuration in both applications. The video devices (cameras, monitors, joystick controllers, switchers, and recorders) are configured in the HVMS application. The access devices (site, channel, and video server) are configured in Pro-Watch. When both configuration procedures are complete, all of the video devices configured in HVMS appear in the Pro-Watch Hardware Configuration tree under the new site. You can then control the video devices from Pro-Watch, using HVMS control tools.

This section provides the procedure for configuring the access devices in Pro-Watch. Follow these steps:

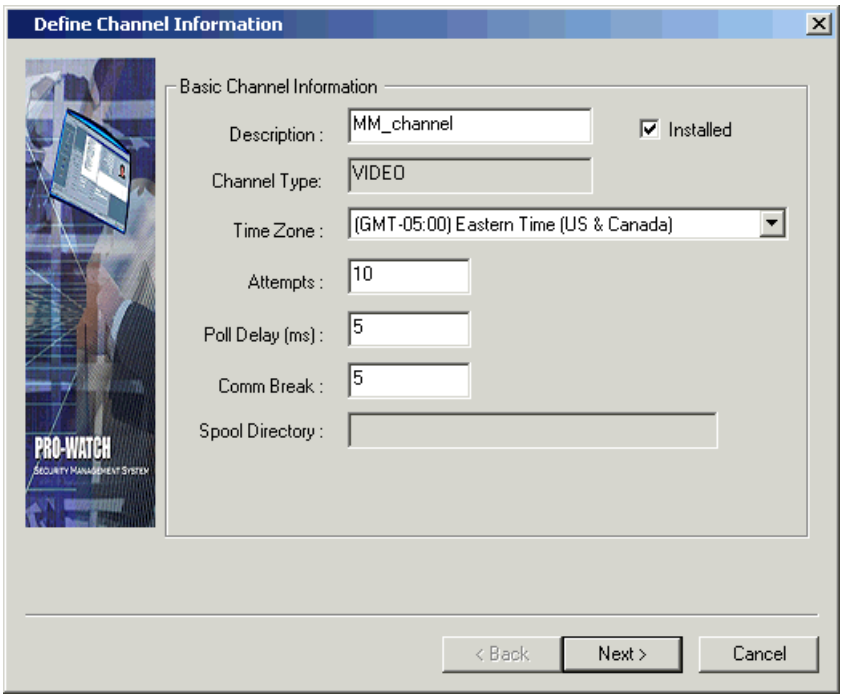
1. Verify that HVMS is installed on a server on a TCP/IP network, and that the video devices are configured in HVMS.
2. Start Pro-Watch and click **Hardware Configuration**.
3. Right click the **VIDEO** site in the Hardware Configuration tree, and select Properties. The Edit Site dialog box appears.
4. On the Site Record tab, click the icon next to the Primary Workstation field and select the machine on which Pro-Watch Server is installed. Click **OK** to complete the Site configuration.
5. Create a new channel on the VIDEO site:
    a. Right click the VIDEO site in the Hardware Configuration tree, and select **New > Channel** to display the Create a Channel dialog box.

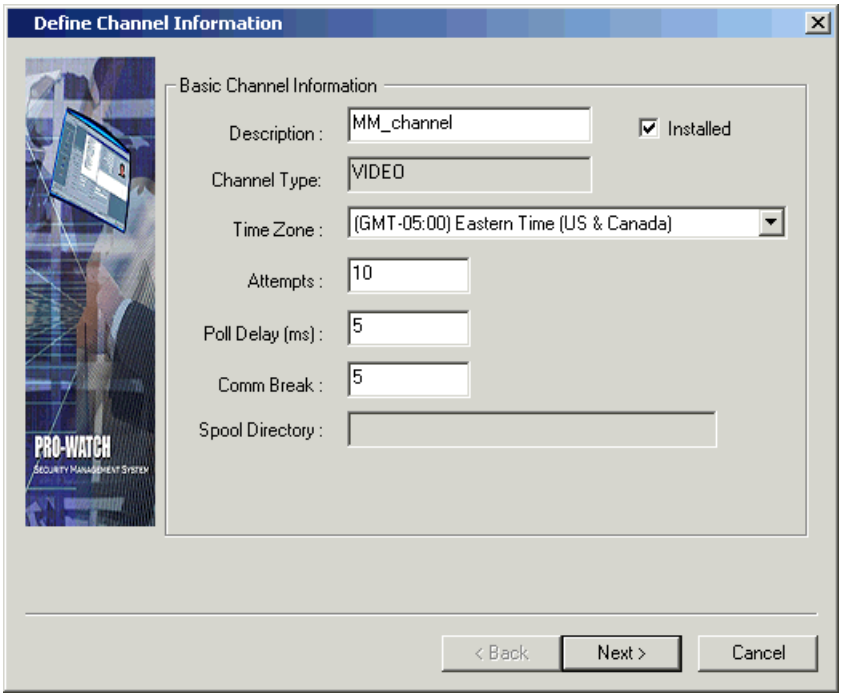
b. Select the **VIDEO** channel and click **OK**.



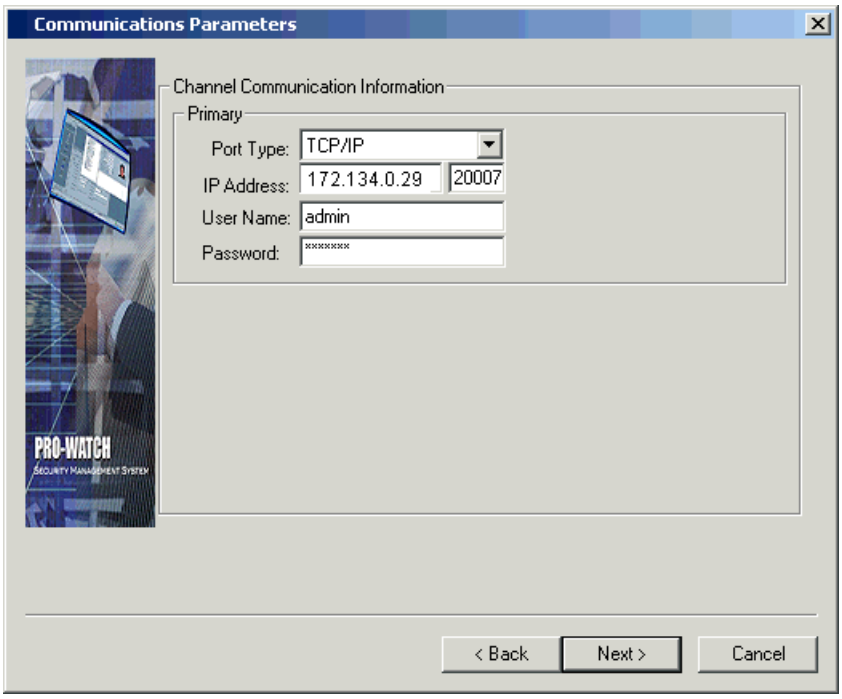
The Define Channel Information dialog box appears.

c. At the Define Channel Information dialog box, enter a channel description.





d. Click **Next**. The Communications Parameters dialog box appears.



Enter the following values in the Communications Parameters dialog box:

Field	Entry
Port Type	Select TCP/IP.
IP Address	Enter the IP address of the HVMS server machine. In the adjacent field, enter the port number.
User Name	Enter the administrator user name for the HVMS server machine.
Password	Enter the administrator password for the HVMS server machine.

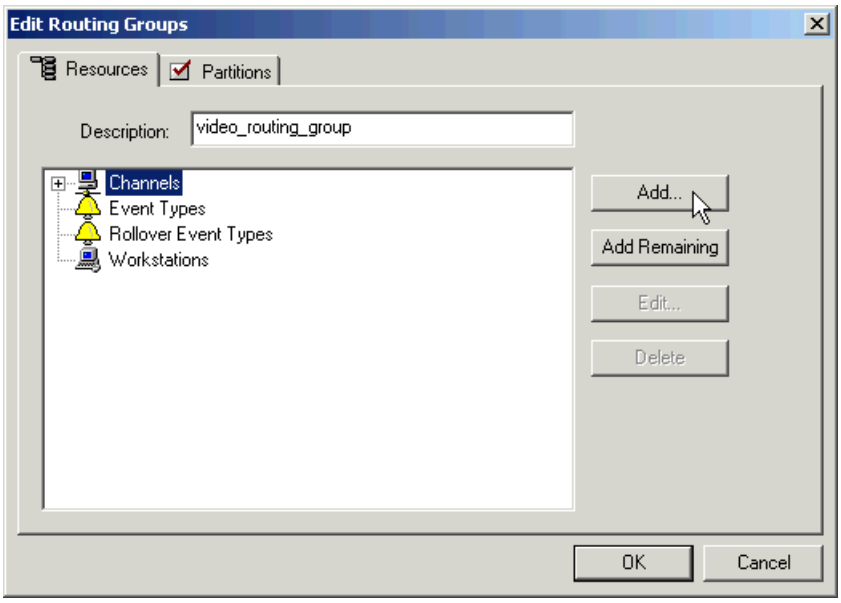
Click **Next** to display the Partitions dialog box.

e. If you want to create a partition for the channel, click **Add** and select the partition.

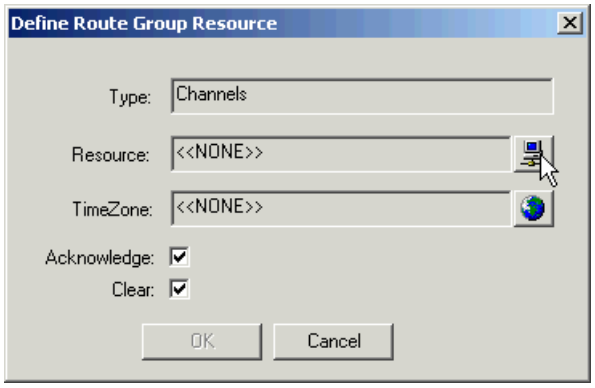
f. Click **Finish**. A message that reminds that you must add the channel to a Routing Group.

g. Add the new channel to the appropriate Routing Group by following these steps:

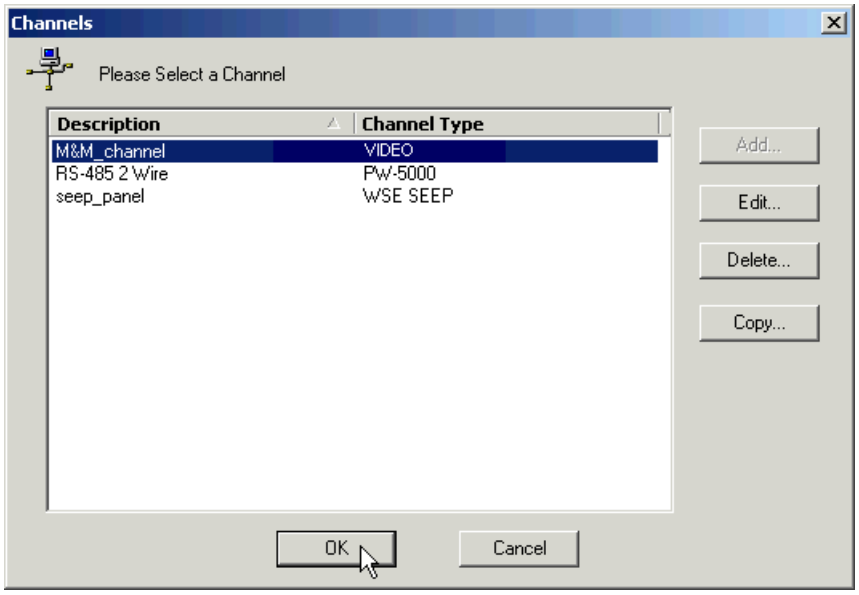
- Click **Database Configuration** to display the Database Configuration tree.
- Click **Routing Groups** in the tree to display all configured Routing Groups.
- Double-click the desired Routing Group to display the Edit Routing Groups dialog box.
- Click to highlight **Channels**, and click **Add**.



The Define Routing Group Resource dialog box appears.

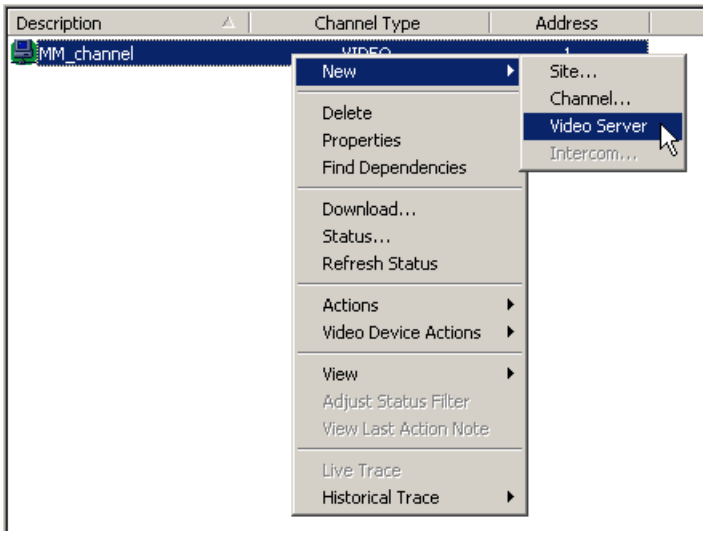


- Click the icon next to the Resource field and select **Define** to display the Channels dialog box.
- Highlight the VIDEO channel you created earlier in this procedure, and click **OK**.



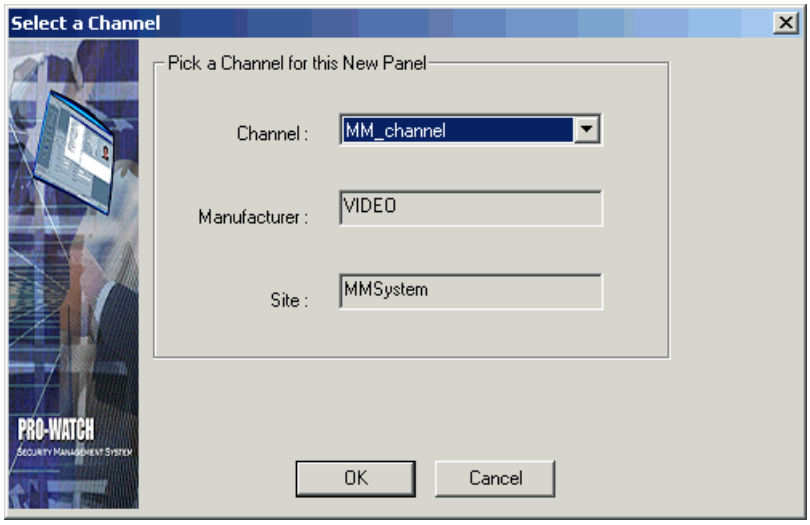
- The Define Routing Group Resource dialog box re-appears.
- Click the icon next to the TimeZone field and select **Define**. Then, select a Timezone for the channel and click **OK** to accept. The VIDEO channel is now added to the Routing Group.

6. Create a Video Server. To do this, right click the channel listing in the right pane of the Hardware Configuration screen, and select **New > Video Server**.



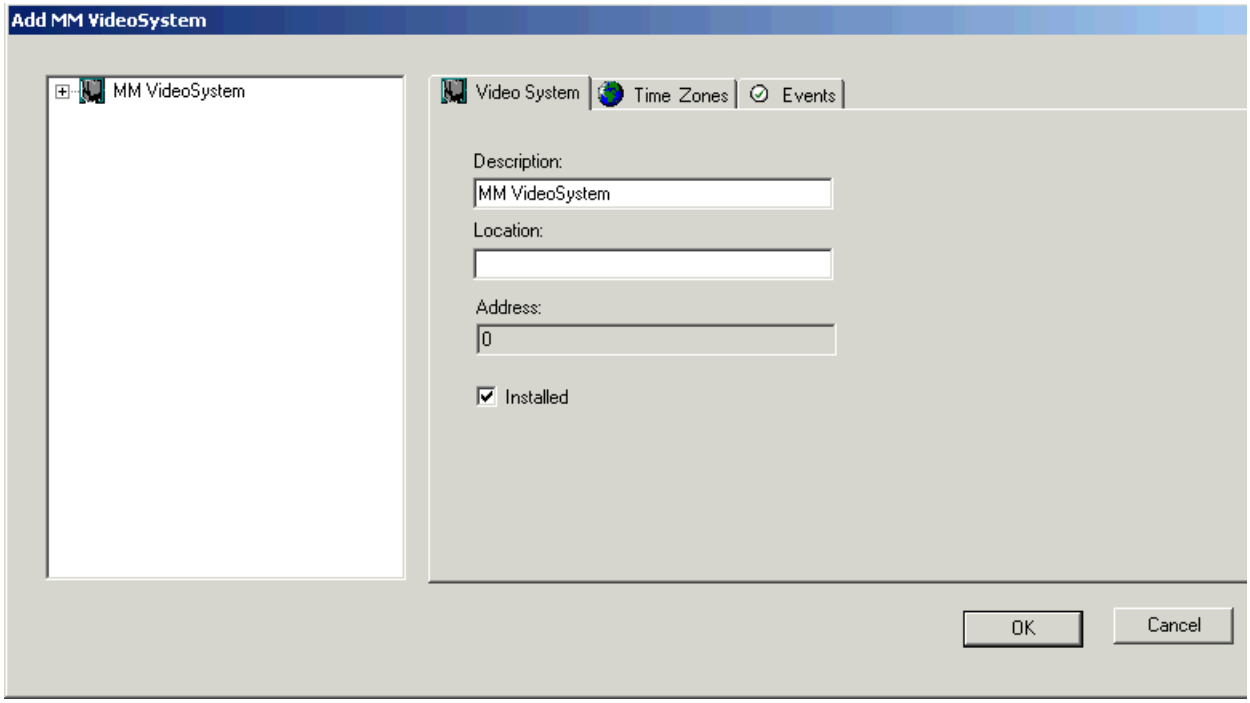
The Select a Channel dialog box appears.

7. In the Channel drop-down list, select the VIDEO channel you created in step 5.

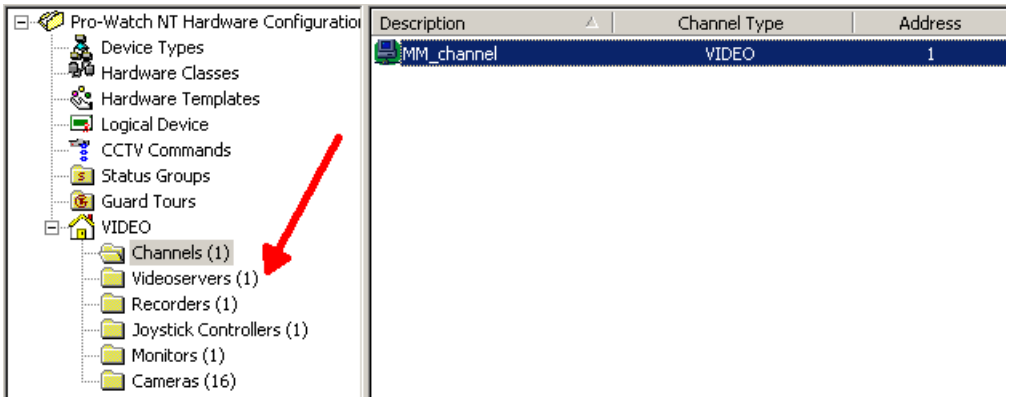


Click **OK**. The Add VideoSystem dialog box appears.

8. Click **OK** at the Add VideoSystem dialog box.



In the Pro-Watch Hardware Configuration tree, you will notice that all of the video devices configured in HVMS now are listed under the VIDEO site.



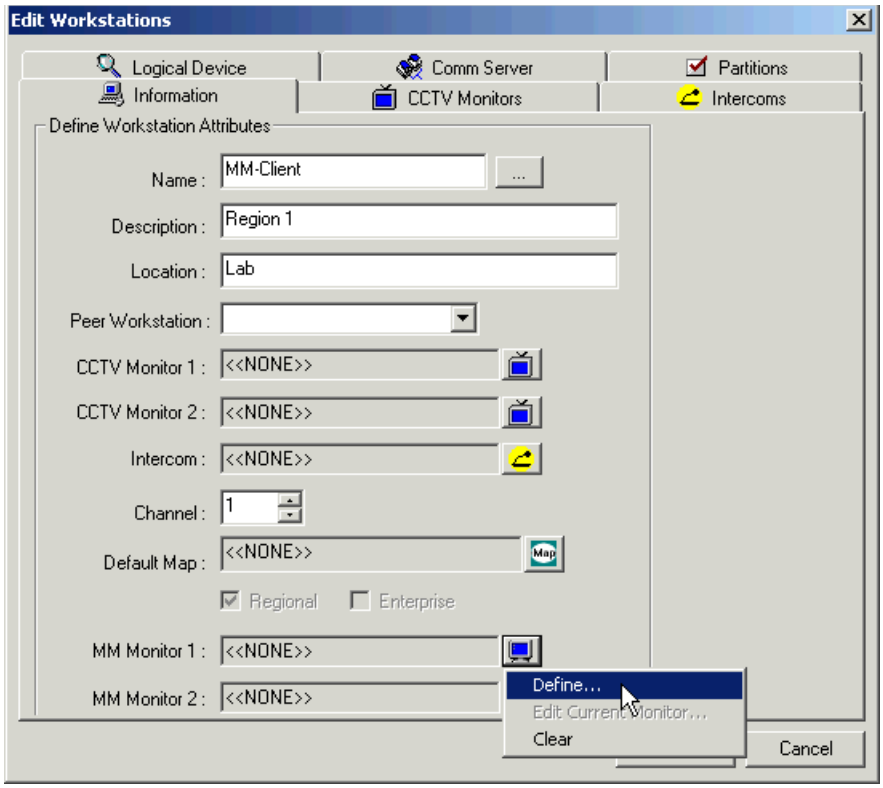
9. Configure the monitor. The monitors that were configured as a video device in HVMS must now be configured in Pro-Watch.

   a. Click Database Configuration in the main Pro-Watch tree.

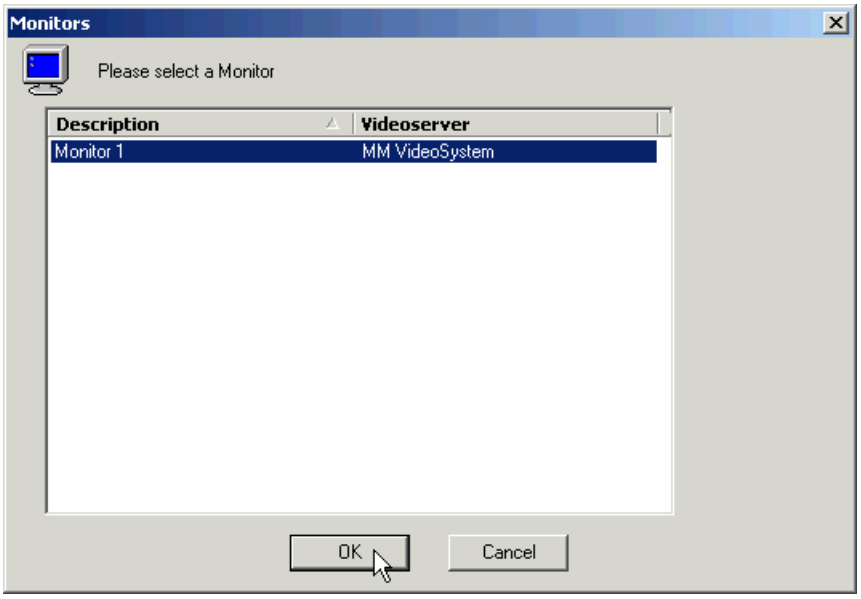
   b. Click Workstation to display the configured workstations.

   c. Double-click the workstation configured in HVMS to display the workstation's Information tab in the Edit Workstations dialog box.

   d. Click the icon next to the Monitor 1 field and select **Define**.



The Monitors dialog box appears.



e. Select the monitor configured in HVMS and click **OK**. The Edit Workstations dialog box re-appears.

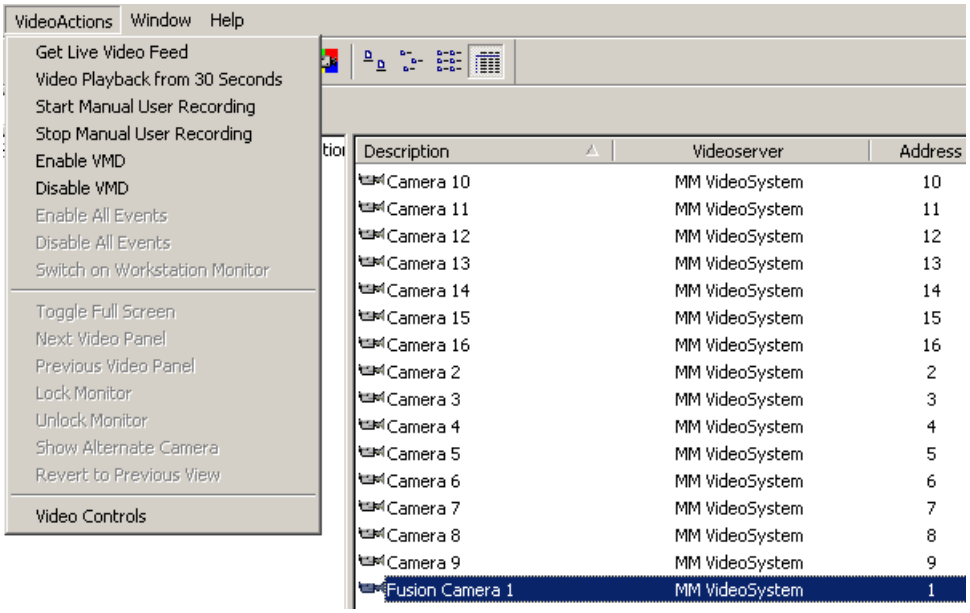
f. Repeat steps d and e if you want an additional workstation (Workstation 2).

g. At the Edit Workstations dialog box, click **OK**. The monitor are now configured in Pro-Watch.

The HVMS configuration in Pro-Watch is now complete.

22.3 Using HVMS in Pro-Watch

Click the VideoActions button on the Pro-Watch toolbar to display the following menu:



Select the desired camera and then select the desired operation from the menu list.

The following table describes the VideoActions:

Table 1 VideoActions

VideoAction	Description
Get Live Video Feed	Causes live video from the selected camera to be displayed in the HVMS viewer.
Video Playback from 30 Seconds	Re-plays the preceding 30 seconds of video recorded by the selected camera.
Start Manual User Recording	Starts the user video recording at the selected camera. The user video recording option is specific to the recorder (DVM, for example). The recorder is configured in HVMS.
Stop Manual User Recording	Stops the user video recording at the selected camera. The user video recording option is specific to the recorder.

Table 1 VideoActions

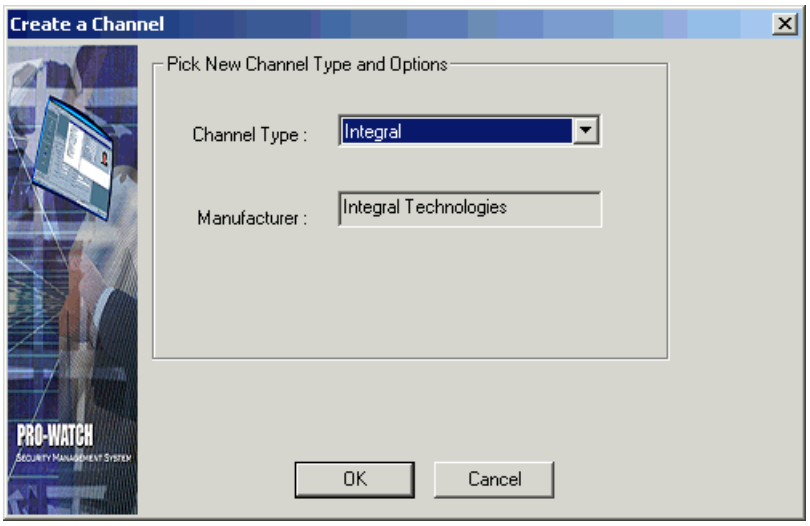
VideoAction	Description
Enable VMD	Enables Video Motion Detection (VMD) on the selected camera. VMD is specific to the recorder (DVM, for example). The recorder is configured in HVMS.
Disable VMD	Disables Video Motion Detection (VMD) on the selected camera. VMD is specific to the recorder (DVM, for example). The recorder is configured in HVMS.
Enable All Events	Enables all events at the selected camera to be reported in Pro-Watch.
Disable All Events	Disables all events at the selected camera to be reported in Pro-Watch.
Switch on Workstation Monitor	Displays the live video feed.
Toggle Full Screen	Toggles the HVMS Viewer between full screen and normal view.
Next Video Panel	Displays the HVMS Viewer's next video panel.
Previous Video Panel	Displays the HVMS Viewer's previous video panel.
Lock Monitor	Blocks access to the HVMS monitor by other users.
Unlock Monitor	Allows access to the HVMS monitor by other users.
Show Alternate Camera	Displays on the monitor the HVMS camera that is the alternate camera.
Revert to Previous View	Returns the display to the view produced by the previous user action.
Video Controls	Enables you to select a camera and monitor, switch the camera's video to the selected monitor, view presets, pan, tilt, zoom, focus, and change the iris of the selected camera.

22.4 Configuring DVR

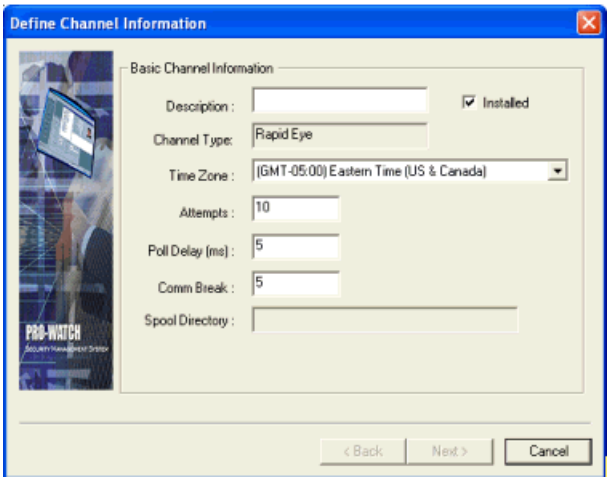
22.4.1 Creating a Channel

To create a channel:

1. Select a channel type.
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.



   b. If you are using the HVMS video system, select the VIDEO channel type from the drop-down list. Otherwise, select a channel type specific to your hardware manufacturer from the drop-down list.
   c. Click **OK**. The Define Channel Information dialog box appears.
2. Define the channel.
   a. In the Define Channel Information dialog box, enter an identifying channel description.



b. Leave the **Installed** check box selected if you want the configured channel to be installed and operational.

c. (Not active in this release). In the Time Zone field, select the time zone appropriate for your location from the drop-down list.

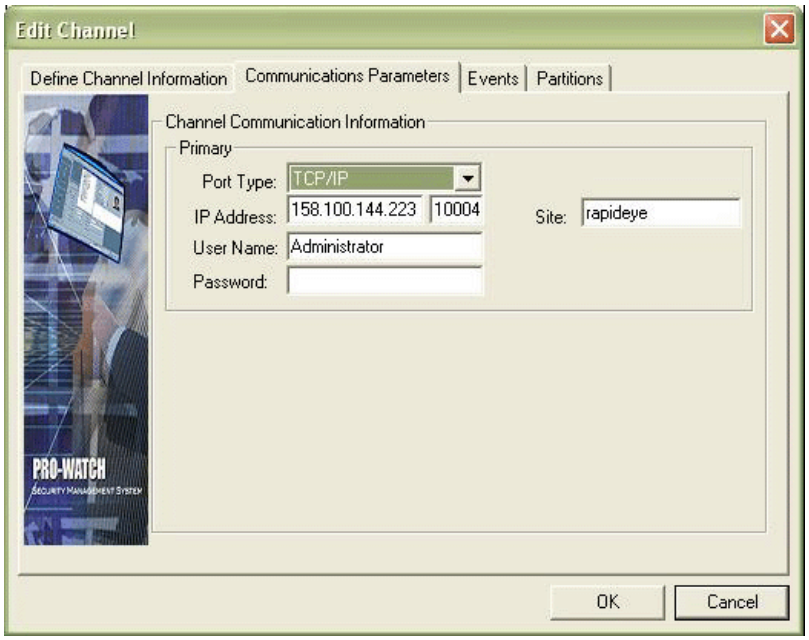
d. (Not active in this release). In the Attempts field, enter the maximum number of times the Pro-Watch server will poll a panel before determining a panel timeout.

e. (Not active in this release). Ignore the Delay field value, since the server-to-panel polling interval is not user-defined for DVR systems. The polling interval is fixed at one minute.

f. (Not active in this release). In the Comm Break field, enter the number of panel timeouts that will occur before the Pro-Watch server determines that the panel is not operating.

g. (Not active in this release). The communications spool directory is automatically created within the Pro-Watch directory. The spool files temporarily reside in this directory during a download.

h. Click **Next** to display the Communications Parameters dialog box. Note that Honeywell DVM displays a different dialog box. No port, user ID, or password fields appear for Honeywell DVM.



3. Set communications parameters.

   a. The port type is predefined as TCP/IP, since Integral, Rapid Eye, VAST, and Honeywell FUSION DVR use only a TCP/IP port.

   b. Enter the IP Address of the DVR device.

   c. Identify the Site (Rapid Eye only). The Site must be the same site that was configured during the manufacturer software setup.

   d. Define a Username and Password. For Rapid Eye, Integral, and Honeywell FUSION DVR, the username and password must be the same as the username and password configured during manufacturer software setup on the DVR device.

   e. For Rapid Eye only, enter the site name in the Site field.

4. Click **Next** to display the Partitions dialog box. See "DBC - Partitions" in Chapter 53.

5. Click **Finish** on the Partitions dialog box to finish adding the channel. A warning message appears notifying you to add the channel to the appropriate routing group. See "Adding or Modifying a Routing Group" in Chapter 55 for instructions. Note that the channel is not usable until you add it to a routing group.

Notes:

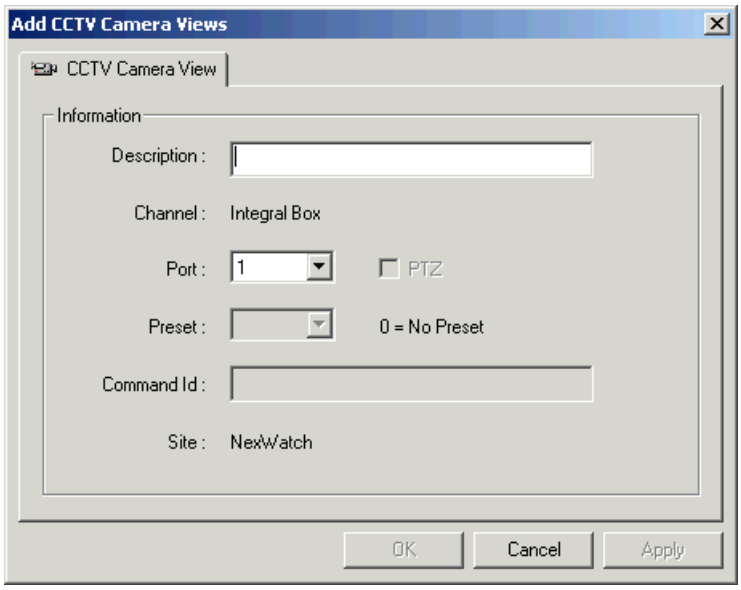
- Only the user ID and password for the first Vicon channel connection is required to connect to any channel in a ViconNet™ network.
- Pro-Watch supports only one ViconNet™ network (one Vicon nucleus) at a time.

22.4.2 Creating CCTV Camera Views

A camera view is the view that is captured by the camera and displayed on the monitor screen.

To add a CCTV camera view:

1. In the Hardware Configuration tree view, click the channel folder to display the channel icons.
2. Right-click the appropriate channel icon in the Hardware Configuration window and select **New** > **CCTV Camera View**. The Add CCTV Camera Views dialog box appears.



3. Enter a description that identifies, or locates, the CCTV camera view.
4. Select the port number from the drop-down list. The port number corresponds to the physical port number on the back of the switcher. Each port number will be unique. You can assign only one camera view to a port number.
5. Only if you will be using Rapid Eye, Integral, or FUSION equipment:
   a. Enable **PTZ** if you are using a pan/tilt/zoom (PTZ) camera.
   b. Select **Preset** from the drop-down list. Preset applies only to PTZ cameras. The Command ID is not functional. The site in which the DVR is assigned is identified.
6. Click **OK.**

Camera views are associated with Logical Devices or event points. You may assign a CCTV camera view to a Logical Device, an event point, or both. CCTVs assigned at the event level, when manually initiated, call up the assigned camera view for particular events. Similarly, CCTVs assigned to

the Logical Device call up a camera view when manually initiated (see your panel's Logical Device configuration instruction or "HW Config - Edit Point" in Chapter 25).

Note: Pro-Watch does not yet support the PTZ feature for Vicon DVR.

22.4.3 Calling Up a Camera View

You can call up a CCTV camera view by any of three methods:

- Right-click the icon of the Logical Device to which the camera view is assigned, and select **Show CCTV Camera View**.
- Right-click the camera view icon and select **Go Live**. See "Using "Go Live" to Search and Display Video" for instructions.
- Click the DVR toolbar icon  to display multiple camera views through the Digital Video Recording display utility. See "Displaying Multiple Camera Views".

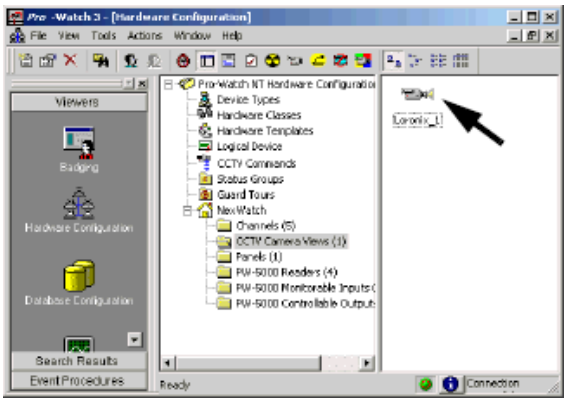
22.4.3.1 Using "Go Live" to Search and Display Video

The "Go Live" menu method of calling up CCTV camera views enables you to search for and display video clips recorded during a specified time.

Note: The Integral, Rapid Eye, and VAST video servers record a video clip for every event that is associated with a CCTV device. However, the Honeywell FUSION DVR system records video clips only when motion occurs simultaneously with the event. The Honeywell Digital Video Manager (DVM) does not require a simultaneous event to occur. A DVM motion alarm appears in the alarm and event log when a DVM motion alarm occurs.

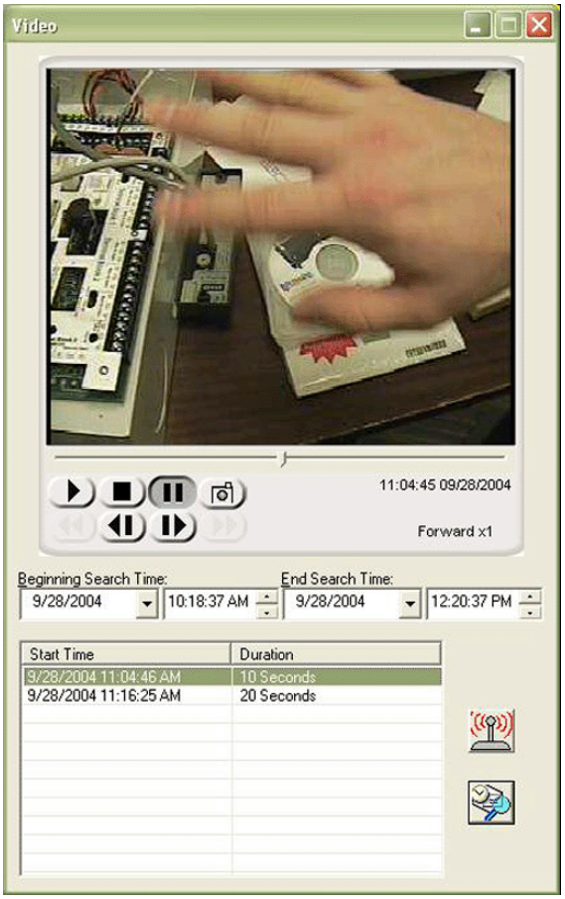
Follow these steps:

Note: Right click on the desired camera view icon in the Pro-Watch Hardware Configuration screen.



The Video screen for your DVR software appears.

Note: For example, the following is a Honeywell DVM Video screen:



The screens for the DVR software supported by Pro-Watch vary in their design, but they each provide search and display functions. Each also uses the following two function buttons:

	**Search** Executes the search for video clips within the specified time period, and displays a list of the clips retrieved.
	**Live** Displays the current camera view in real time.

Note that the Fusion Video screen also includes a Stop Search  icon. Also, if the camera is configured for Pan/Tilt/Zoom (PTZ) operation, a panel of PTZ navigation icons appears.

7. To play one of the retrieved video clips, double-click the desired clip from the list retrieved from the search.
8. To view the current camera view in real time, click the **Live** icon.

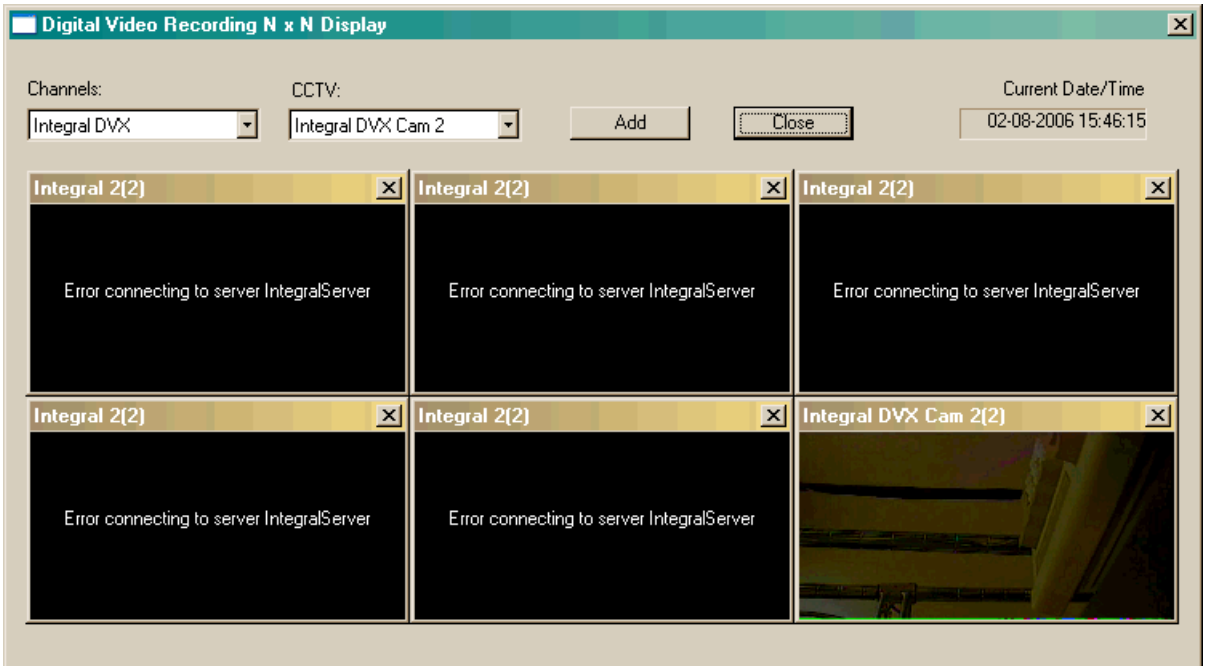
22.4.3.2 Playing Live and Captured Video from the Alarm Monitor

You can configure your Alarm Monitor to display maps by placing the map file in the /Maps folder of the Pro-Watch install directory (see "Adding a Map" on page 6). On the map, the Alarm Monitor displays camera icons that indicate the location of the configured cameras.

To display live video of a particular camera from the Alarm Monitor, right click the camera icon and select Actions > Go Live. To play back captured video, right click the camera icon and select Actions > Play Captured Video. This plays the last recording stored in the event log for this CCTV view. The playback can either be motion-generated recording or Pro-Watch-generated recording (events associated with a CCTV view).

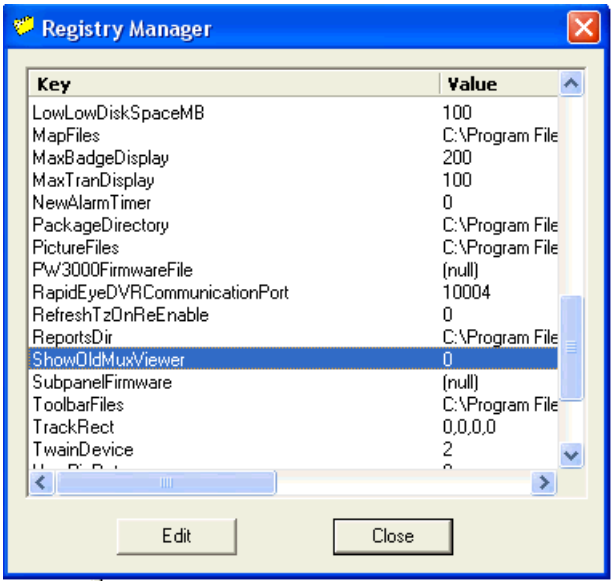
22.4.3.3 Displaying Multiple Camera Views

You can display multiple camera views simultaneously by clicking the DVR icon on the toolbar at the top of the Pro-Watch screen. Pro-Watch provides two formats in which to display the views. The following screen shows the default format of displaying all views of a selected camera.

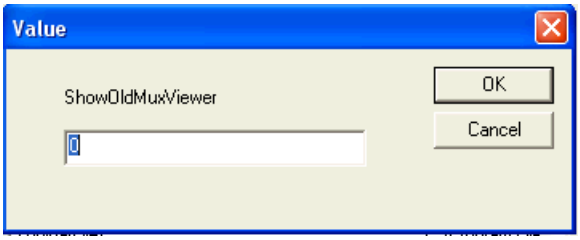


You can change the default format to display up to 16 views of a selected channel. To do this, perform the following steps:

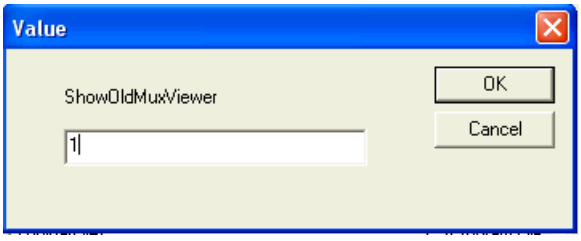
1. From the Pro-Watch Viewers window (left window of the Pro-Watch screen), click **Administration > Executables > Pro-Watch Registry Editor**. The Registry Manager box appears.



2. Click **ShowOldMuxViewer** (as shown) in the Registry Manager. The following Value box appears:

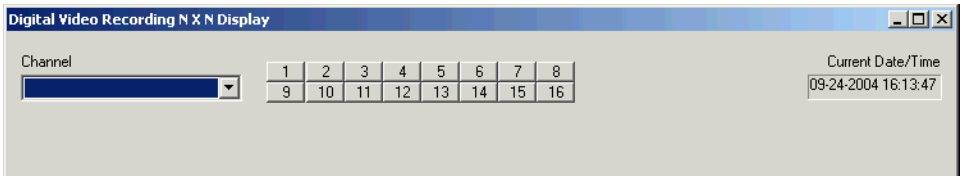


3. In the ShowOldMuxViewer field, change the value from 0 to 1.



4. Click **OK**.
5. Click the DVR icon  in the toolbar at the top of the Pro-Watch screen to display the alternative DVR viewer. The viewer includes a Channel

drop-down list and a panel of buttons with which you select camera views. The number of each button represents a camera view number.



6. Select the channel for which you want to display camera views from the Channel drop-down list.
7. From the panel of numbers next to the Channel field, click the number(s) of the camera views you want to display. That is, click 2 for camera view 2, click 7 for camera view 7, and so on. The maximum number of camera views you can show simultaneously is 16. Note that you can display views only for one channel at a time. When you select a new channel, all of the camera views of the previously-selected channel disappear.

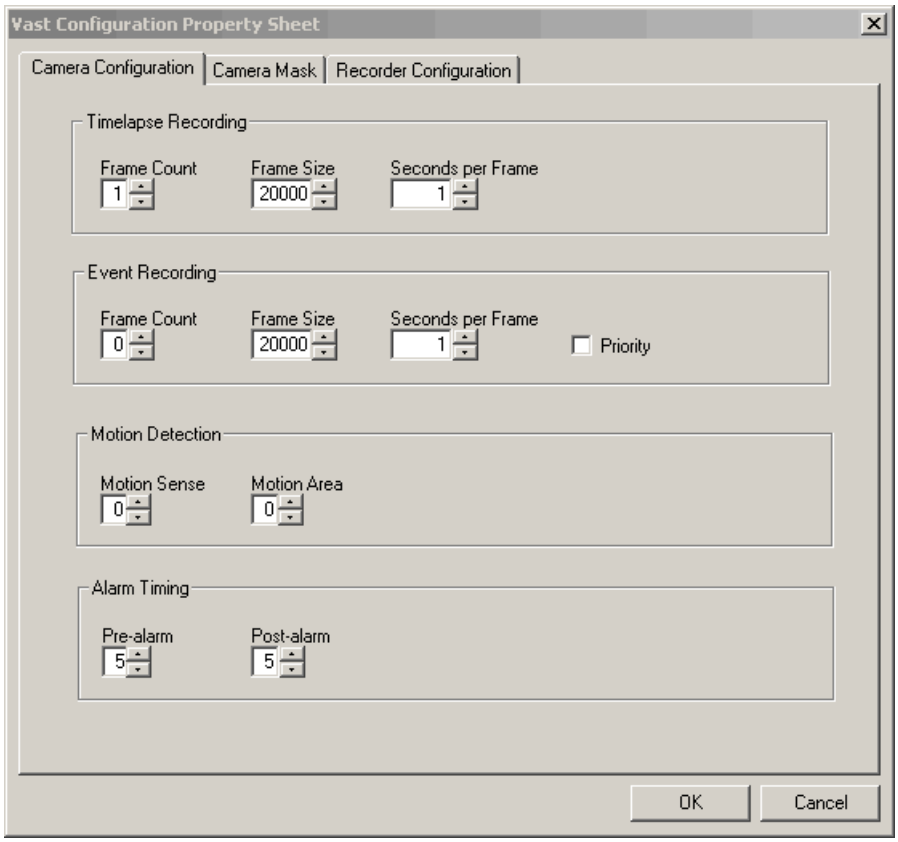
Note: An Integral system must be in Record mode before you call up its CCTV camera view.

22.4.4 Configuring VAST

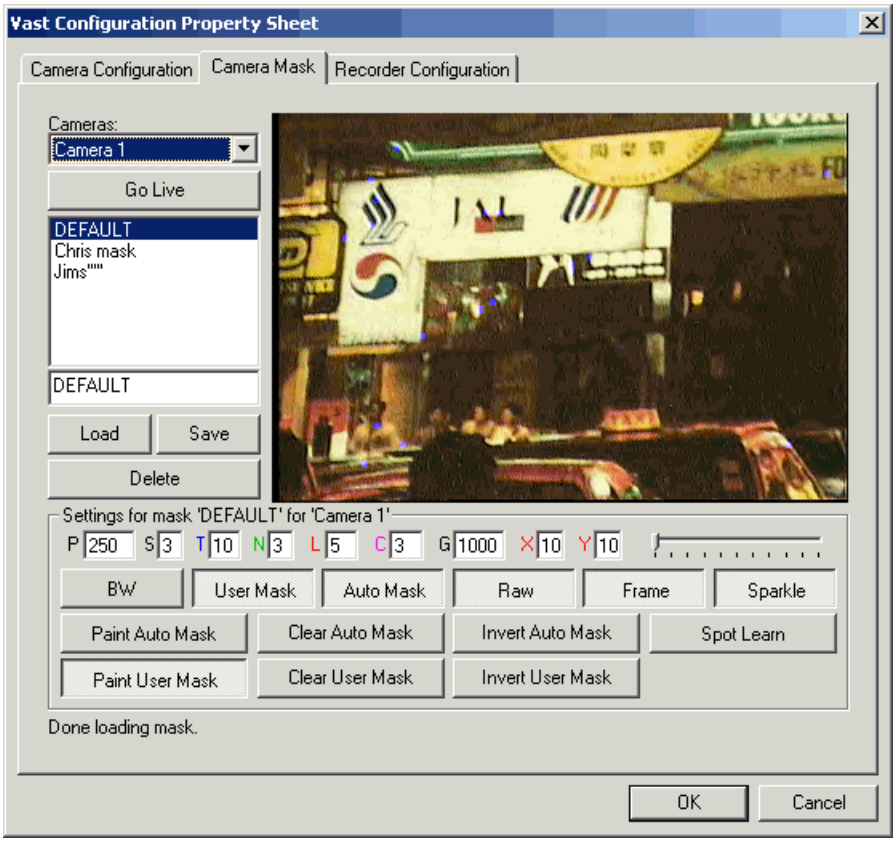
VAST software is configurable directly from Pro-Watch. For Integral and Rapid Eye software, you will need to use the manufacturer's configuration software.

To configure the VAST software from Pro-Watch:

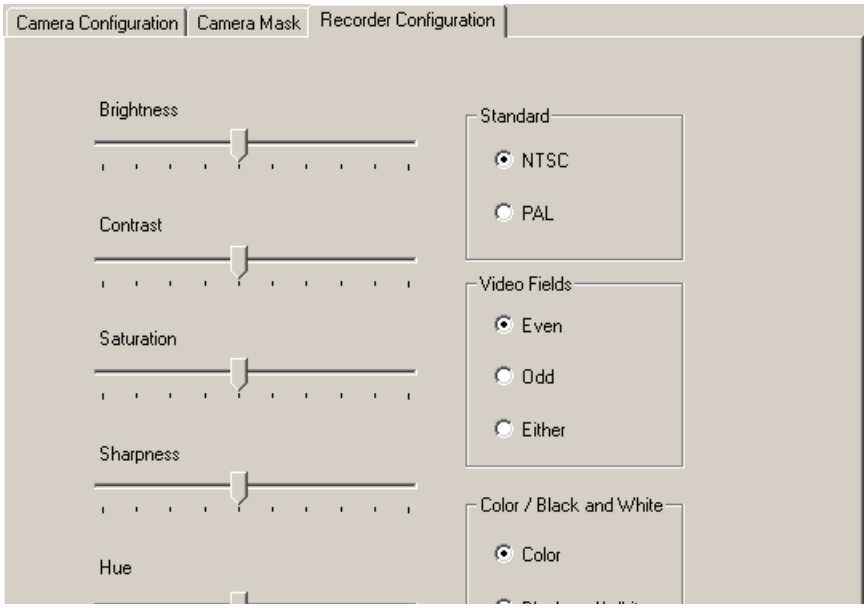
1. Right-click the VAST camera view and select **Configure**. The VAST Configuration Property Sheet dialog box appears.



2. We strongly recommend that you accept all default settings on the Camera Configuration tab.
3. Click the Camera Mask tab. The Camera Mask tab allows you to create and set masks, or shunts, for a specific camera and determine how sensitive the camera is to motion. Within this tab you can mask or shunt particular movement to avoid needless motion detection events. You can also place hotspots in particular regions in which a message is sent if movement occurs in that region.



4. Click the Recorder Configuration tab, which allows you to configure settings for the entire VAST box. It is strongly recommended that you accept the default settings. Any changes made to these settings affect all cameras associated with the box.



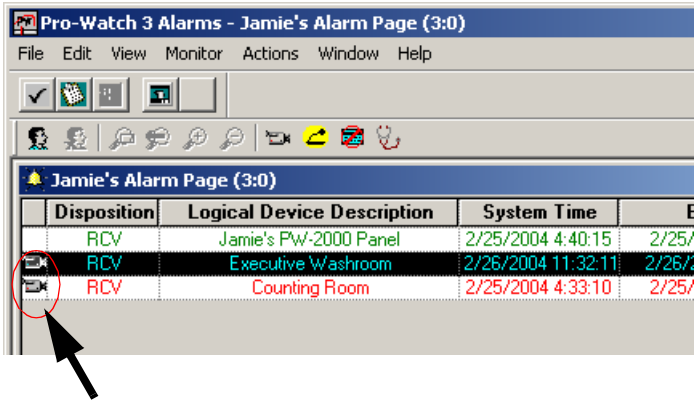
Note: The password for VAST video is case sensitive. The user ID is not case sensitive.

22.4.5 Associating a Camera with an Alarm

Associating a camera with an alarm enables you to capture the image of an intruder who attempts to open a locked door.

1. Click the **Hardware Configuration** icon in the left pane of the Pro-Watch main window.
2. Select and click a **Site** in the middle pane to display its associated Readers folder.
3. Click the **Readers** folder to display the icons of all the associated readers in the right pane.
4. Select a reader in the right pane and right-click to display the pop-up menu.
5. Select **Properties** to display the Edit Logical Device window for that specific Logical Device.
6. Click and select the **Default CCTV Information** tab.
7. Click the camera icon next to the **Default CCTV View** field to display the pop-up menu.
8. Select **Define** to display the CCTV Camera Views screen.
9. Select a camera from the list and click **OK** to associate the selected camera with the selected Logical Device. You'll revert to the Edit Logical Device window.
10. Click **OK** to complete the procedure.

When you return to the Alarm Monitor screen, you will see a camera icon next to a new instance of the associated event in the first column of the Unacknowledged Alarms Pane (see "Window Panes" on page 3-11):



Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Intercom

23

In this chapter ...

Overview
Adding an Intercom
Adding Intercom Stations

23.1 Overview

Intercoms consist of ‘primary’ stations, normally deployed in a dispatch center, and ‘remote’ stations also known as call boxes. Intercoms are often used to supplement an access control system by allowing a dispatcher to communicate with an individual at an access point. Intercoms can also be used as security devices, providing emergency call alarms, as seen on college campuses and parking garages.

Pro-Watch provides the ability to control audio connections between intercom stations, the processing of events from the intercom system, and the association of intercom stations with Logical Devices. Pro-Watch currently supports the Zenith1 (Stentofon) AlphaComm and the Commend Intercom product lines.

23.2 Adding an Intercom

Follow these steps:

1. Select a channel type.
   a. In the Pro-Watch Hardware Configuration tree view, right-click the site you have created, and select **New > Channel**. The Create a Channel dialog box appears.
   b. Select a channel type specific to your hardware manufacturer from the drop-down list (i.e., Stentofon or Commend).
   c. Click **OK**.
2. Define the channel.
   a. In the Define Channel Information dialog box, enter an identifying channel description.
   b. Select the **Installed** check box. This assures the channel is installed and operational.
   c. Select a time zone from the drop-down list.
   d. Enter the maximum number of poll attempts.
   e. Enter the poll delay interval between each polling. This number is in milliseconds.
   f. Enter the communications break; the host must receive communication from the device within the specified time or the host will determine the communication as broken.
   g. The spool directory is automatically created; this is where spool files temporarily reside during a download. The spool directory is created within the Pro-Watch directory.
   h. Click **Next** to display the Communications Parameters dialog box.

i. Set communications parameters. Select the port type from the following drop-down list options:

Option	Comments
None	Disables communications to all panels and hardware devices on a specific channel. To avoid wasting polling examples, use this option when you install or troubleshoot panels or other hardware on the channel. After you finish installing or troubleshooting, select another port type.
Hardwired	Designates a serial port as the primary channel communication setting. Com Port – The communication port on the host computer. Baud – The rate of communication.
TCP/IP	Specifies that the channel is a network connection. IP Address – The IP address of the panel.

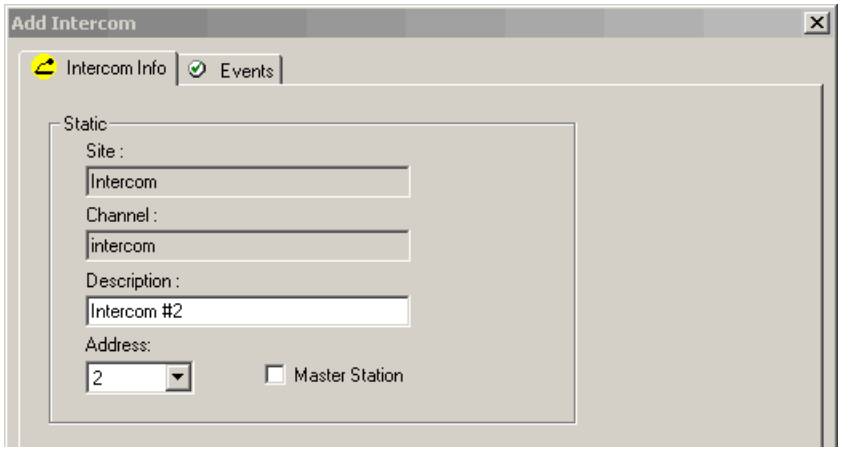
j. Click **Next** to display the Partitions dialog box. See "DBC - Partitions" in Chapter 53.

k. Click **Finish** on the Partitions dialog box to complete channel add. A warning message appears notifying you to add the channel to the appropriate routing group.

23.3 Adding Intercom Stations

Follow these steps:

1. From the hardware configuration window, right-click on the channel to display the add intercom dialog box. Note that the site and channel are static fields. These fields are populated automatically with the data assigned to both site and channel descriptions.
2. Enter the description of the intercom.
3. Set the address, or port, of the intercom, either by typing the number in the Address field or using the up and down buttons next to the field.
4. If the intercom is to be a primary station, enable the primary station check box and click **OK**.



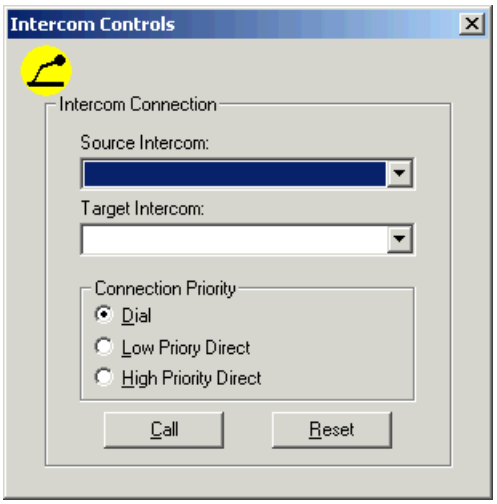
Intercoms are associated with workstations and Logical Devices. Primary intercoms should be assigned to the workstation and non-primary intercoms should be associated to Logical Devices. The primary intercom, assigned to a workstation, serves as the station from which calls are made. See "DBC - Workstations" in Chapter 59.

Note: Non-primary intercoms can be associated with Logical Devices under the Define Logical Device tab. See the Logical Device section corresponding to your hardware for more information.

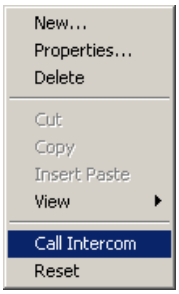
The Intercom Controls dialog box allows you to define a source and target intercom and initiate a connection between the two. Intercom controls also allow you to assign a connection priority.

1. To display the intercom control dialog box, click the intercom icon .
2. Select the source intercom. The source intercom must be a primary intercom. You must add the primary intercom to the workstation before the drop-down list will be populated.
3. Select the target intercom. The target intercom can be any other intercom in the system.

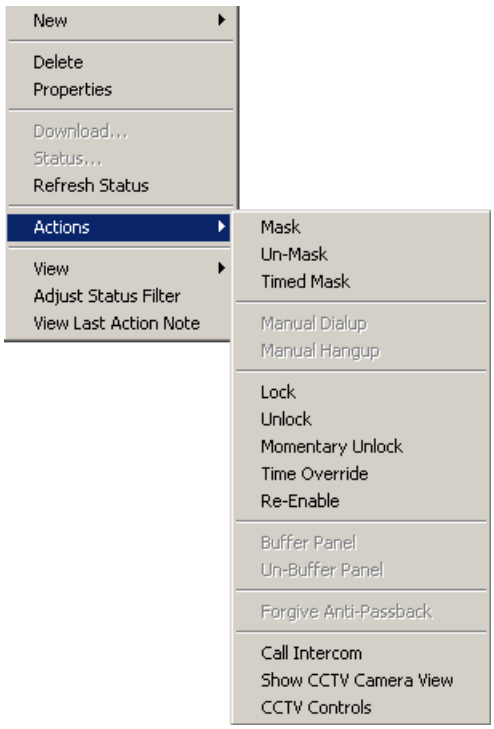
4. Select the connection priority. Dial priority is the standard priority of a call. Low Priority Direct and High Priority Direct can be used to override calls that are in progress, which are of lower priority.



- Intercom stations can also be called by right-clicking on an intercom station and selecting Call Intercom.



- If Call Intercom is used, the selected intercom station connects with the default primary station assigned to the workstation. Reset causes the intercom station to 'hang up' if it currently had an active connection.
- Intercoms that are associated to a Logical Device can also be called by right-clicking on the Logical Device, select **Actions > Call Intercom**.



Note: Intercoms may also be called from the Alarm Monitor. See Chapter 3, .

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Hardware Actions

24

In this chapter ...

Hardware Actions

24.1 Hardware Actions

Hardware Actions allow you to perform specific Logical Device functions. Hardware Actions can be performed from within Hardware Configuration

as well as within Alarm Monitor. For more information about the Alarm Monitor, see Chapter 3, .

The table below lists the hardware actions and the applicable panel types.

Hardware Actions	PW-6000/ 5000/3000	PW2000	Star II	SEEP	Cardkey
Mask (or shunt)	x	x	x	x	x
Un-Mask(or un-shunt)	x	x	x	x	x
Timed Mask	x	x	x	x	x
Activate	x	x	x	x	x
De-Activate	x	x	x	x	x
Pulse	x	x	x		x
Time Activate	x		x		x
Lock	x		x		x
Un-Lock	x	x	x	x	x
Momentaril y Unlock	x	x	x	x	x
Time Override	x				x
Re-Enable	x	x	x	x	x
Enter Cypher Mode	x				
Exit Cypher Mode	x				
Manual Dialup	x	x	x	x	x
Manual Hangup	x	x	x	x	x

Hardware Actions	PW-6000/ 5000/3000	PW2000	Star II	SEEP	Cardkey
Buffer Panel		x			
Un-Buffer Panel		x			
Forgive Anti-Passback	x	x	x	x	
Call Intercom	x	x	x	x	x
Show CCTV Camera View	x	x	x	x	x

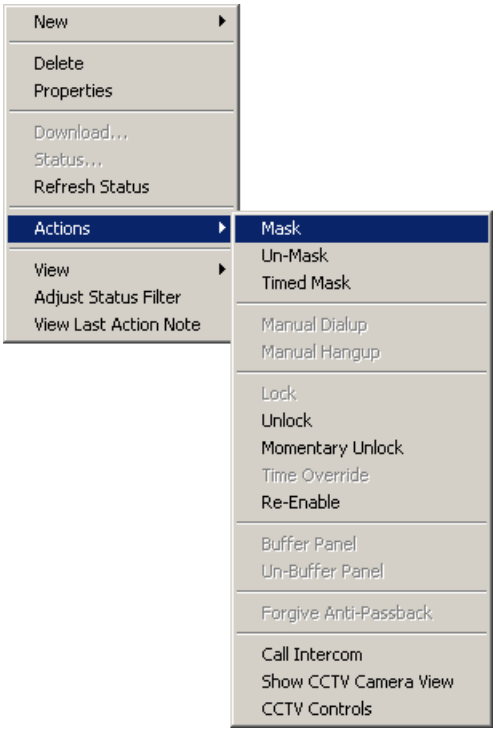
The functionality for each hardware action is defined below.

- Mask – masks the input point. This means that the input can cause no alarm.
- Un-Mask – unmasks the input point. This means that the input can cause an alarm.
- Timed-Mask – masks the input point for a specified amount of time.
- Activate – activates the output.
- De-Activate – deactivates the output.
- Pulse – pulses the output.
- Time Activate – activates the output for a specified amount of time.
- Lock – locks the door in which no cards can gain access.
- Un-Lock – unlocks the door.
- Momentary Unlock – momentarily unlocks the door.
- Time Override – for Cardkey, upon a door strike, the output remains energized for the specified amount of time. The door remains unlocked. For PW-5000, the output energizes for the 'normal' time; however, it remains shunted for the specified amount of time.
- Re-enable – re-enables the reader back to its 'normal' state.
- Enter Cypher Mode – causes the reader to enter cypher mode, in which a sequence of digits may be entered on the keypad that is interpreted as a card number. Cypher mode works differently on different panels. For example, on a PW6K1ICE panel, when you enter the card number on the keypad of the reader, you must start with an asterisk (*), then follow it with the card number, and finish with #. For

example, if the card number is 20418, you must enter *20418#. For a PW-6000, you must enclose the number with pound signs (#). For example, #12345#. Cypher mode is not an exclusive mode; cards may still be presented to the reader.

- Exit Cypher Mode – causes the reader to exit cypher mode.
- Manual Dial-up – enables a manual dial-up for a panel that is configured for dial-up.
- Manual Hangup – manually hangs-up the connection for a panel that is configured for dial-up.
- Buffer Panel – buffers the panel so that no events are received by Pro-Watch. When a panel is buffered, no events can be seen in the event viewer.
- Un-buffer Panel – un-buffers the panel so that events are received by Pro-Watch. When a panel is un-buffered the events can be seen in the event viewer.
- Forgive Anti-passback – forgives anti-passback for the reader if it is part of an anti-passback configuration.
- Call Intercom – calls the intercom associated with the reader.
- Show CCTV Camera View – shows the CCTV camera view associated with the reader. See "HW Config - CCTV" in Chapter 21.

You can initiate hardware actions from within Hardware Configuration by right-clicking the Logical Device and selecting **Actions > [the specific hardware action]**. Note that only the hardware actions that are supported by the panel type as well as applicable to the channel, panel, or Logical Device type will be available to initiate.



You can also initiate hardware actions by selecting **Actions** from the toolbar and selecting the specific hardware action.



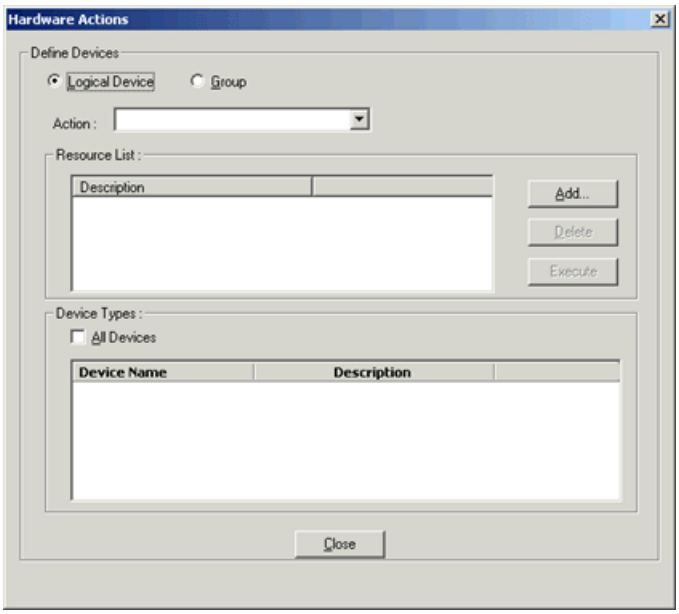
You may also perform a specific hardware action on multiple Logical Devices or a group consisting of Logical Devices.

1. Click on the Logical Device folder from the hardware configuration tree view.

2. From the toolbar select **Tools** > **Hardware Actions**. The Hardware Actions dialog box appears.
3. Select the option button for which you would like to initiate a hardware action.
4. Select an **Action**.
5. Click **Add.**
6. Select the specific groups or Logical Devices in which you would like to initiate the hardware action.

If you would like the hardware action to be initiated on all applicable device types:

1. Select the **All Devices** check box; otherwise,
2. Select the specific device type and click **Execute**.
3. Click **Close** to close the dialog box.



Note: If the Action Note (see "DBC - Classes" in Chapter 36) is required, you will need to enter an action note before executing a hardware action.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - Edit Point

25

In this chapter ...

Overview
Event Information
Adding an Instruction Set
Adding a New Instruction
Adding a Disposition

25.1 Overview

The Edit Point dialog box allows you to edit an event point. There may be multiple tabs to configure for specific events. Not all events contain an Instruction Set or Return to Normal tab. All event points require the Event Information tab to be configured.

25.2 Event Information

Use the following field definitions to complete the Event Information tab:

Field	Description
Description	Provides the description of the event as defined by the user.
Shunted	When enabled, the event is shunted.
Annunciate	When enabled, the event is annunciated.
Has Returns	When enabled, the event contains a Return to Normal tab for configurations.
Priority	Assigns the priority level of the event. The Alarm Monitor stacks alarms on the screen according to their priority. Priority 1 alarms appear at the top of the screen, priority 2 alarms appear below the priority alarms, and so on. This field supersedes the default priority level assigned in the Event Type dialog box.
Pager Number	Defines the default pager number for the event, which is assigned to a Logical Device. The default pager number was assigned while adding a Logical Devices. See your panel's Logical Device configuration instructions for more information
Suppress TZone	Defines the time zone in which the event is suppressed.
WAV File	Defines an audio file that initiates upon the event occurring. The default WAV file was assigned while adding a Logical Device. See your panel's Logical Device configuration instructions for more information.
AVI File	Defines a video file that initiates upon the event occurring. The default AVI file was assigned while adding a Logical Device. See your panel's Logical Device configuration instructions for more information.
Starting Map Id	Defines the map to call up for a particular edit point should the event occur.
Event Number	Identifies the event number or address.
Event Type	Defines the event type or the event that must occur.
Auto CCTV Command	Defines the auto CCTV command. See "HW Config - CCTV" in Chapter 21.

Field	Description
Select CCTV Command	Defines the select CCTV command. See "HW Config - CCTV" in Chapter 21.
Auto CCTV Camera View	Defines the auto CCTV camera view. See "HW Config - CCTV" in Chapter 21.
Select CCTV Camera View	Defines the select CCTV camera view. See "HW Config - CCTV" in Chapter 21.
E-mail	Defines the default e-mail address for the event, which is assigned to a Logical Device. The default e-mail address was assigned while adding a Logical Devices. See your panel's Logical Device configuration instructions for more information.
Procedure ID	Defines the event procedure. See "DBC - Event Procedures" in Chapter 43.
Event Text	Defines the text, if any, that appears in the window at the bottom of the Alarm Monitor, if the event occurs.

If applicable, click the **Return to Normal** tab. Use the field definitions given in step 2 to complete the applicable fields; use the table below to complete the additional fields:

Field	Description
Stat	This function is currently not supported.
Alarm Text	Defines the text, if any, that appears in the window at the bottom of the Alarm Monitor, if the event occurs.

If applicable, click the **Instruction Set** tab. The Instruction Set allows you to add instructions in the event an alarm occurs. Instructions are configured within Monitor. For more information, see "Instructions" in Chapter 3.

25.3 Adding an Instruction Set

Follow these steps:

1. In the Instruction Set dialog box, click **Add.**
2. Select an instruction from the Instruction dialog box and click **OK.**

Note: If you do not see an instruction you want to add within the dialog box, you can create a new instruction.

25.4 Adding a New Instruction

Follow these steps:

1. From the Instructions dialog box, click **Add.**
2. The Add Instructions dialog box will appear. For further information on configuring an Instruction, see "Instructions" in Chapter 3.

You may also add dispositions to the Instruction Set. Dispositions are configured within Monitor. See "Dispositions" in Chapter 3.

25.5 Adding a Disposition

Follow these steps:

1. Select the instruction from the instruction list within the Instruction Set dialog box and click **Set** to display the Dispositions dialog box.
2. Select the disposition you want to add and click **OK**.

Note: If you do not see a disposition you want to add within the dialog box, you can create a new disposition.

25.5.1 Adding a New Disposition

Follow these steps:

1. From the Dispositions dialog box, click **Add.**
2. The Add Dispositions dialog box appears. For further information on configuring a disposition, see "Dispositions" in Chapter 3.
3. After adding applicable instructions and dispositions, click **OK** at the Instruction Set dialog box to complete configuration.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

HW Config - MS-ICS

26

In this chapter ...

Overview

Board Properties

Configuration Limits

Typical Network Configuration

Configuring an MS-ICS Network for Pro-Watch

Creating a Site

Creating a Channel

Creating a Panel

Creating a Logical Device

26.1 Overview

The MS-ICS is part of Mercury Security's bridging hardware technology for replacing the Software House GCM module. The MS-ICS intelligent controller provides decision making, event reporting, and database storage for the Mercury hardware platform.

The MS-ICS communicates with the host via on-board 10-BaseT/100Base-TX Ethernet port. An alternate host 10-BaseT/100Base-TX communication connection is available by use of the optional Lantronix Micro125 interface daughter board.

The MS-ICS connects to the MS-ACS processor via a 34-pin ribbon cable, up to two MS-ACS are supported.

Standard Mercury remote serial I/O panels may be connected to the external 2-wire RS-485 multi-drop communication bus.

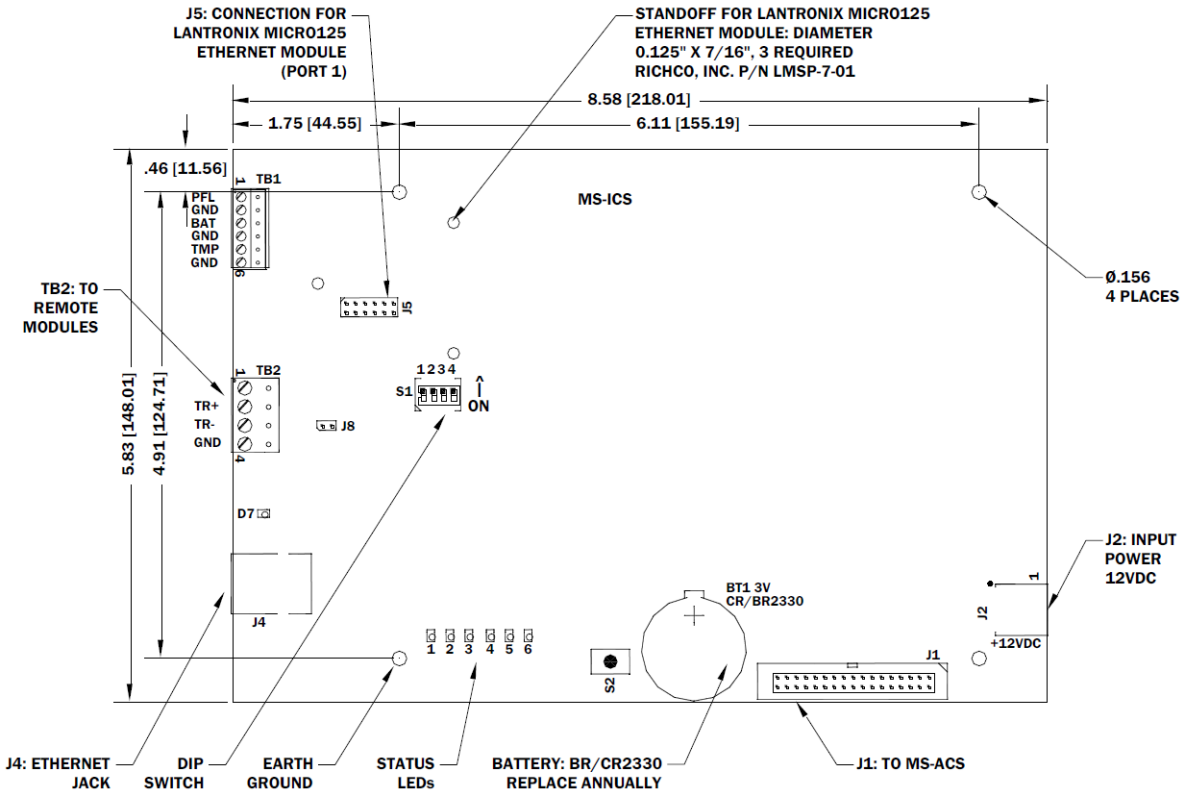


Figure 26-1 MS-ICS Panel Components

26.2 Typical Network Configuration

MS-ICS works with **MS-ACS** Reader Board, **MS-I8S** Input Board and **MS-R8S** Output Board.

Here is how, at a conceptual level, a typical MS-ICS network configuration would look like:

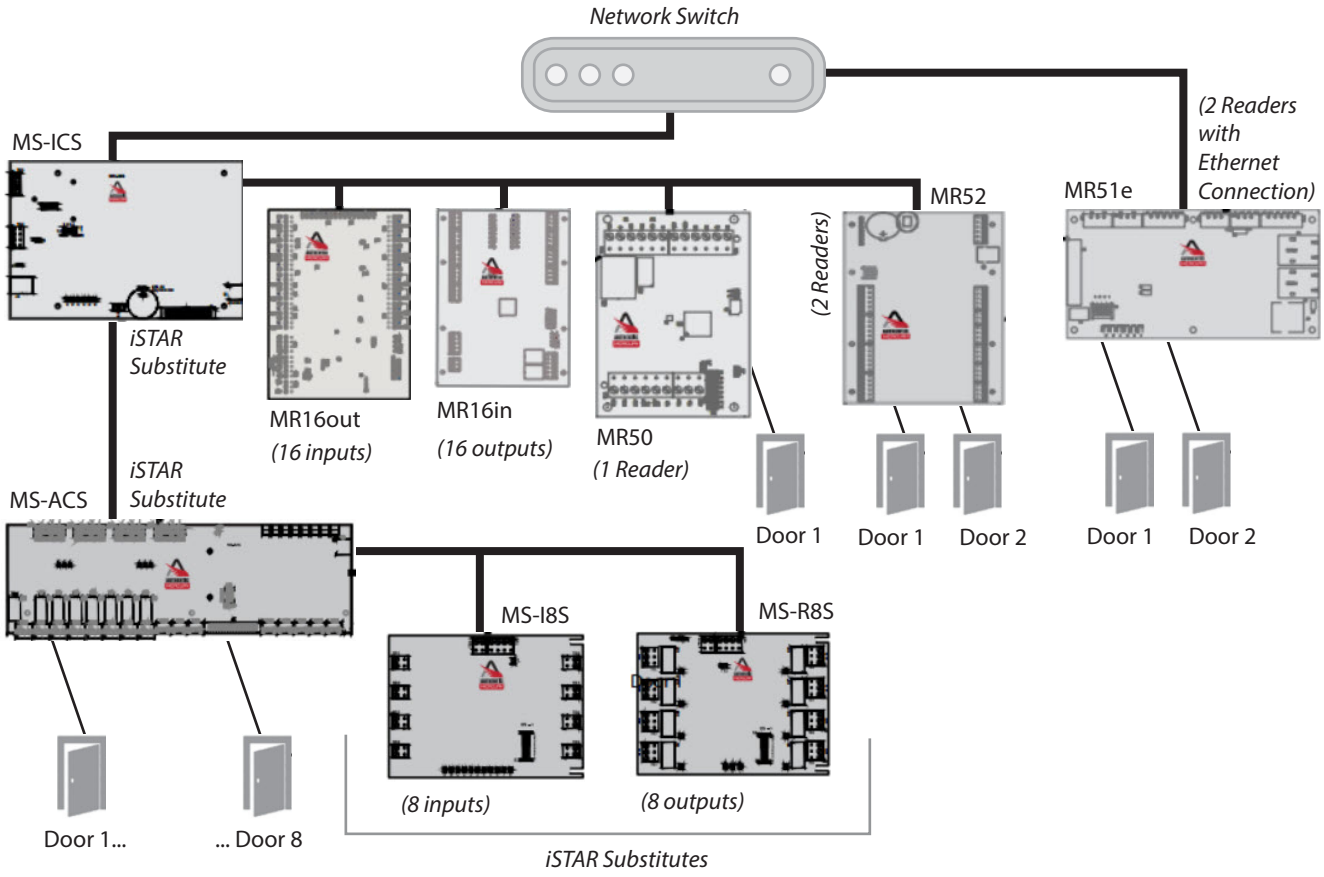


Figure 26-2 Typical MS-ICS Network Configuration

26.2.1 Board Properties

Table 26-1 Selected Properties of Boards in a MS-ICS Network

Board	Maximum Board Number in Network	# of Readers Supported by Each Board	# of Inputs per Board	# of Outputs per Board
MS-ICS	1	N/A	N/A	N/A
MS-ACS	2	8	16	8
MS-I8S	8	N/A	8	N/A
MS-R8S	8	N/A	N/A	8

26.2.2 Configuration Limits

You can connect up to two MS-ACS reader boards to one MS-ICS.

You can connect up to 8 MS-I8S input boards and 8 MS-R8S output boards to one MS-ACS.

26.2.3 Related Mercury Documentation

For more information on these panels, you can consult the following Mercury installation and wiring PDF manuals:

- MS-ICS Installation Manual Rev 1.02
- MS-ACS Installation Manual Rev 1.02
- MS-I8S Installation Manual Rev 1.01
- MS-R8S Installation Manual Rev 1.01

26.3 Configuring an MS-ICS Network for Pro-Watch

26.3.1 Creating a Site

In Pro-Watch, create an MS-ICS site just like you'd create a regular site.

26.3.2 Creating a Channel

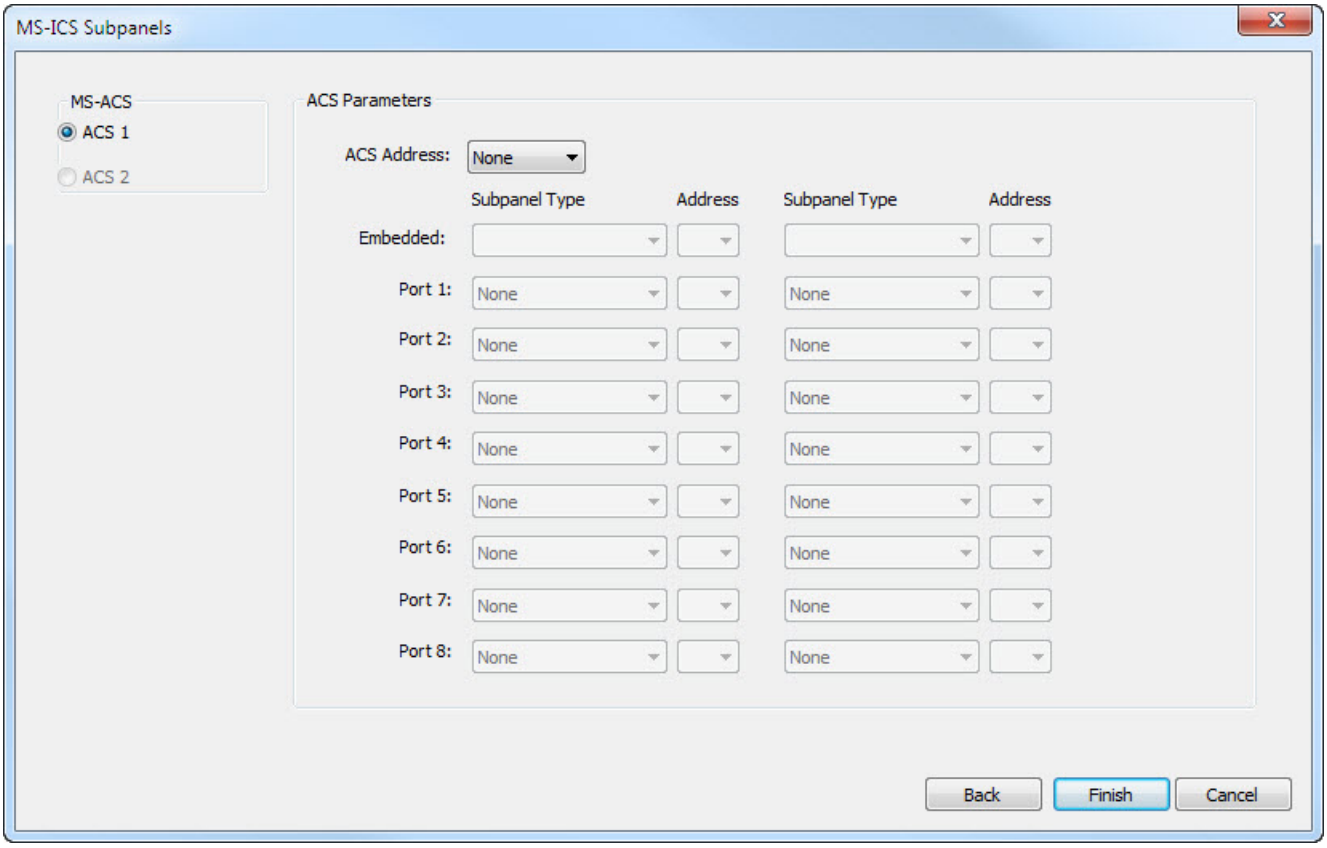
Create an MS-ICS channel just like you'd create a regular channel.

1. Right-click the **Site** and from the pop-up menu select **New > Channel** to display the **Create a Channel** screen.
2. For **Channel Type**, select **PW-5000/PW-6000/PW-6K1ICE** from the drop-down list.
3. Click **Next** to display the **Define Channel Information** dialog box.
4. Enter a **Description** and fill all the other fields as required.
5. Click **Next** to display the **Communication Parameters** dialog box.
6. For **Primary Port**, select **TCP/IP** from the drop-down list of available options.
7. Enter a user-defined **IP Address** and **port number**.
8. Leave the **Secondary Port** fields blank.
9. Click **Next** to display the **Encryption** screen. Select the **No Encryption** option-button.
10. If it is selected, clear (unselect) the **Honeywell Protocol** check-box.
11. Click Next to display the **Partitions** list. Add a partition if appropriate.
12. Click **Finish**.

26.3.3 Creating a Panel

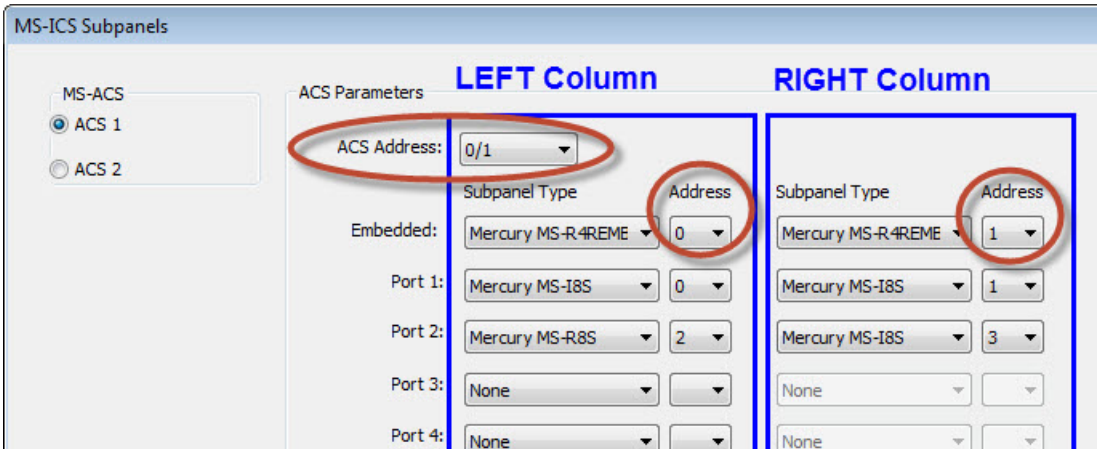
1. Right-click the **Channel** and from the pop-up menu select **New > Panel** to display the **Pro-Watch Controller Manager** screen.
2. Make sure the **Site** selected is the **MS-ICS site**.
3. Select the **Channel Description** of the MS-ICS channel that you've created earlier.
4. Enter a **Controller Description**.
5. For **Controller Type**, select **MS-ICS** from the drop-down menu of available Options
6. Enter **Controller Address** (Address is configured through the MS-ICS web server).

7. Click **Next** to display the **MS-ICS Subpanels** screen where you can add one or two MS-ACS subpanels:



Note: Pro-Watch will not allow you to add the second ACS subpanel before you add the first one.

8. For **ACS Address,** select "**0/1**" from the drop-down menu. These are the addresses Pro-Watch assigns to the two embedded 4-reader controllers on the MS-ACS subpanel:

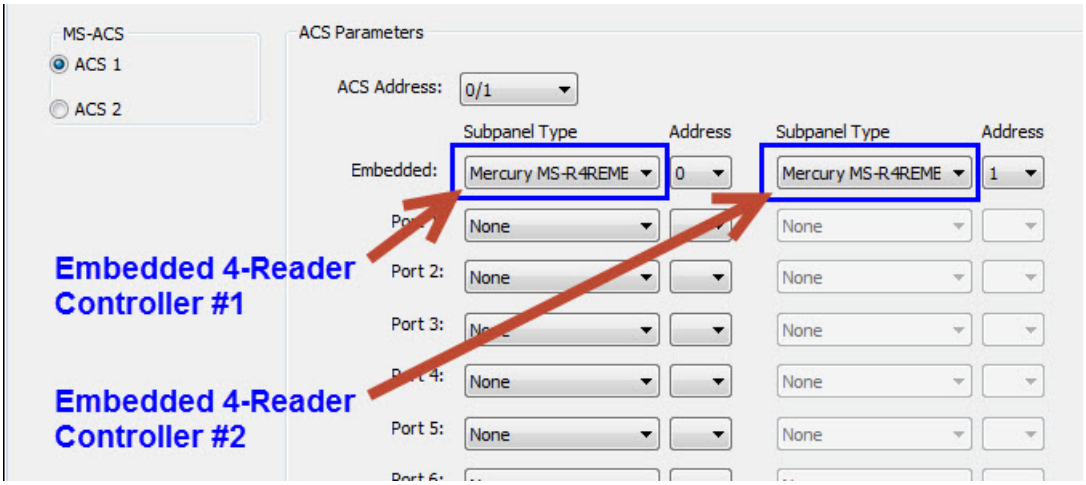


Note: For this selection to work you also need to configure the **DIP switches** on ACS correctly. For "**0/1**" ACS Address the **DIP DSwitch #1** must be set to **OFF**. For "**4/5**" ACS Address the **DIP DSwitch #1** must be set to **ON**.

Table 26-2 ACS Address and DIP Switch #1 Position

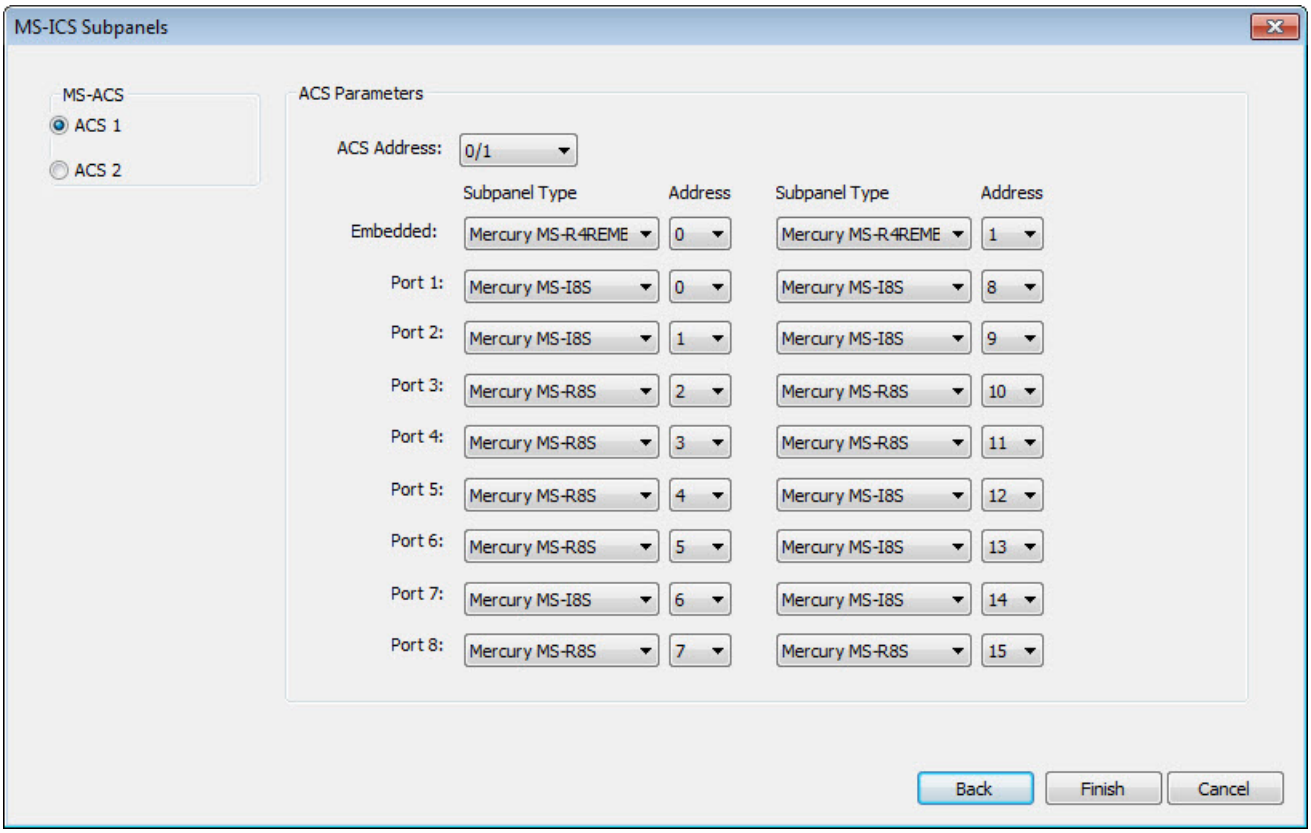
ACS #	ACS Address	DIP Switch #1
1	0/1	OFF
1	4/5	ON
2	2/3	OFF
2	6/7	ON

9. Selecting either "1/0" or "4/5" (depending on the position of DIP Switch #1) displays **two 4-reader Mercury controllers embedded into the ACS subpanel.** These are the same embedded controllers that display even if you select "4/5" as your ACS Address





10. You can assign a total of **16 MS-I8S (input) and MS-R8S (output) I/O boards (subpanels)**, with **a maximum of 8 of each.** The address of each board must be the address selected on the DIP switch on the I/O panel. The address of each board must be unique (0 - 31):



11. Repeat the same setup steps for ACS2 subpanel, if there is one.

Note: ACS2 subpanel is connected serially to ACS1 subpanel through a 34-pin cable.

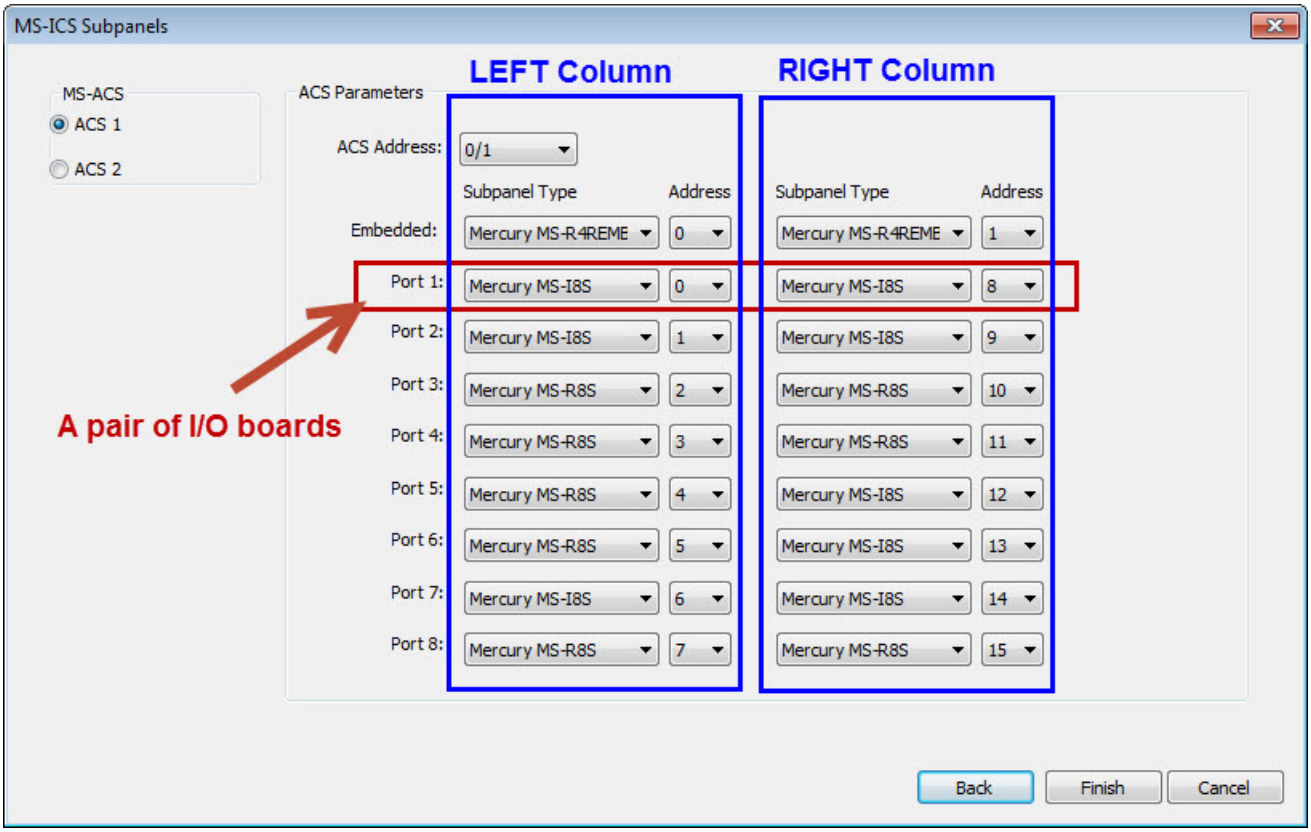
12. Click **Finish**.

26.3.3.1 The Order of Assigning I/O Boards

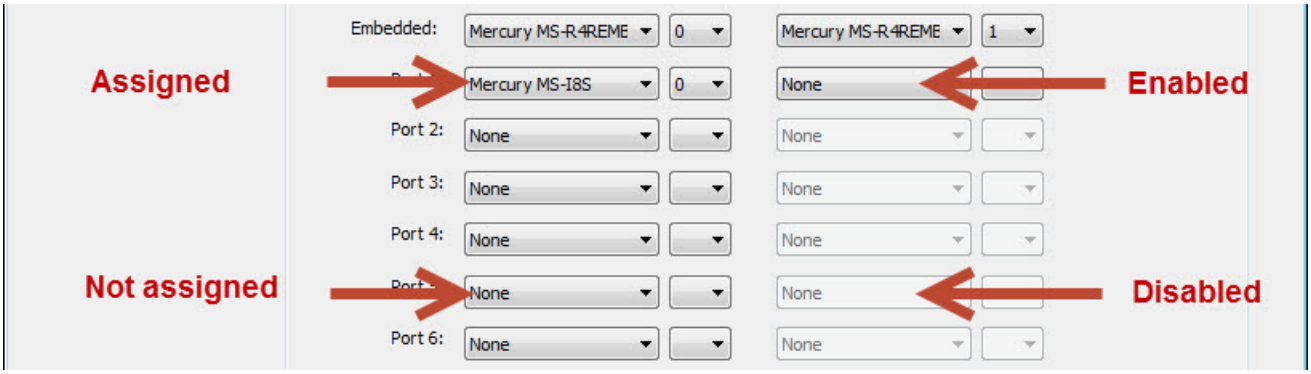
Pairs of I/O boards are connected to ACS and to each other through a **serial daisy-chain wiring**.

Due to this physical limitation, you can assign them in Pro-Watch GUI only in a particular manner and not in any way you like.

The I/O boards are assigned in pairs since they are physically daisy chained two boards at a time. That is, **you have to connect the first board of an I/O "pair" (in the LEFT Column) before you can serially connect the second member of the pair (in the RIGHT column)**:

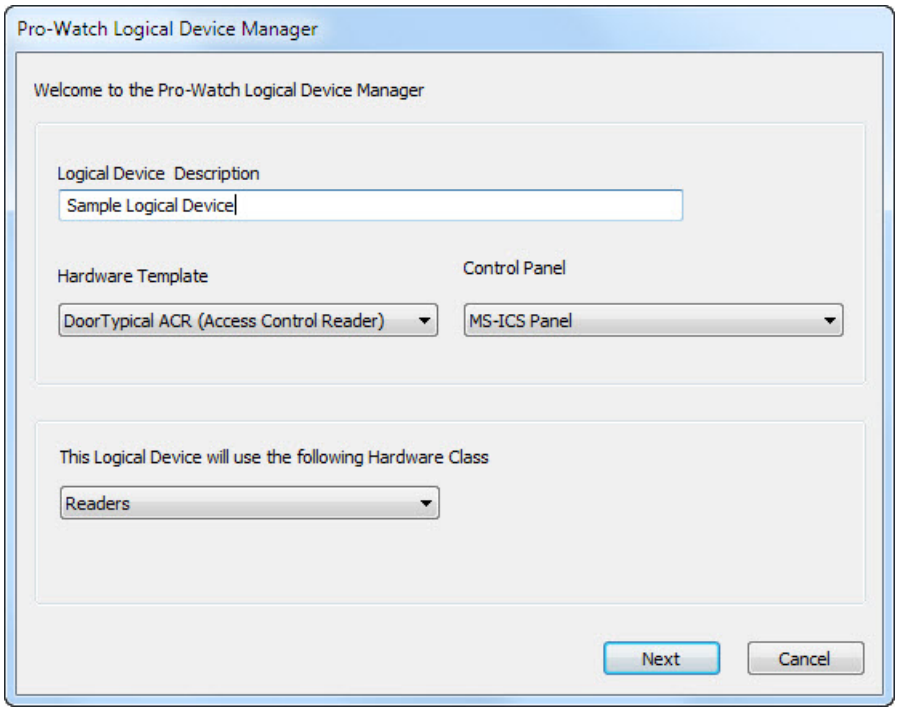


If the first I/O member of a pair is not assigned (LEFT column), Pro-Watch will NOT enable the assignment of the second I/O member (RIGHT column):



26.3.4 Creating a Logical Device

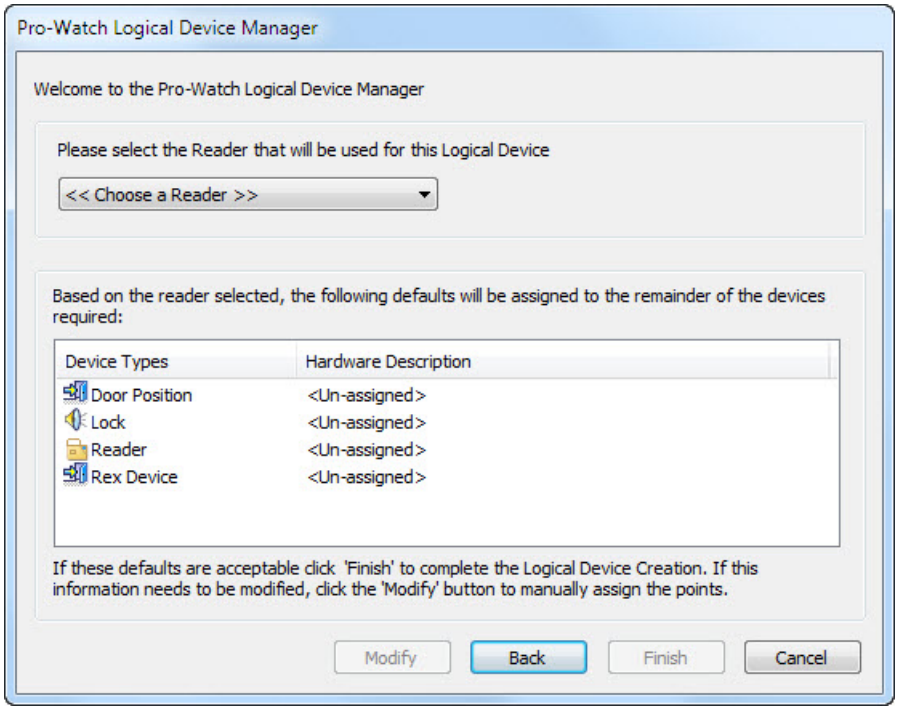
1. Right-click a channel or a panel and from the pop-up menu select **New > Logical Device** to display the **Pro-Watch Logical Device Manager** screen:



2. Enter a **Logical Device Description**.
3. Select an appropriate **Hardware Template**, depending on your specific setup. Some of the suggested ones are:
   - Controllable Output
   - Door Typical ACR (Access Control Reader)

- Monitorable Input

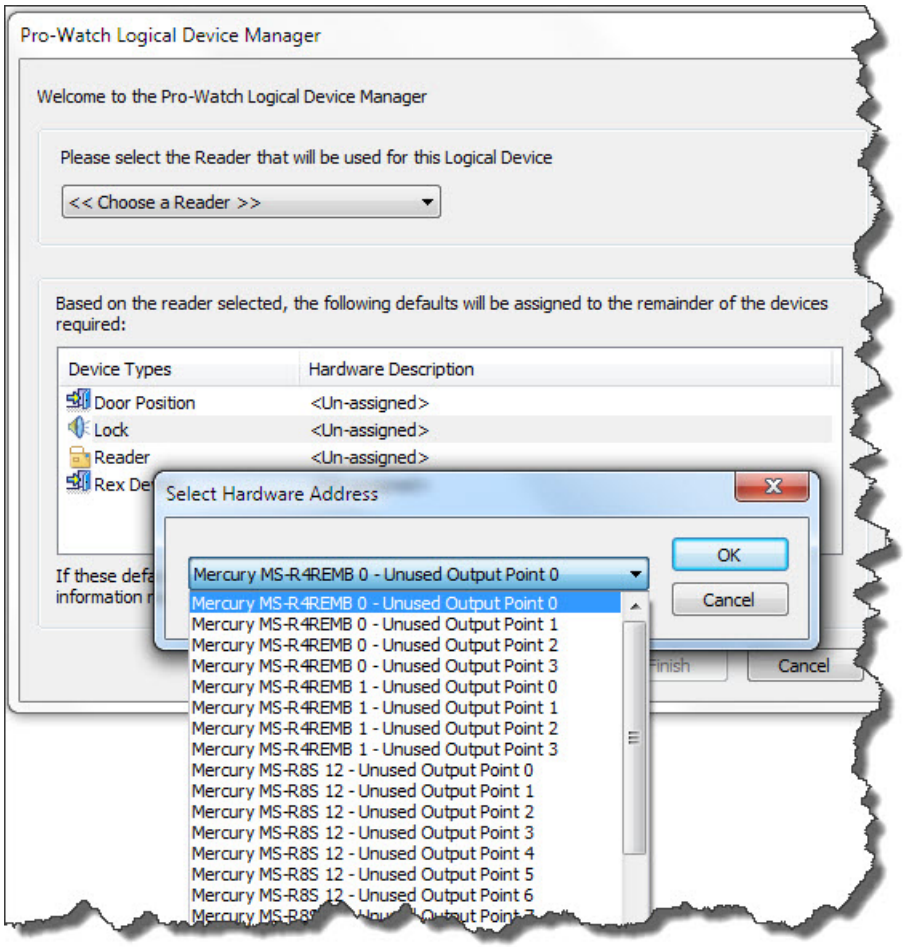
4. Select an appropriate **Hardware Class** from the drop-down list, depending on your specific setup, like “Monitorable Inputs” etc.
5. Select an appropriate **Control Panel** from the drop-down list.
6. Click **Next** to display the configuration screen that dynamically displays, depending on the selections you’ve made in the previous screen. For example, If you select “**Door Typical ACR (Access Control Reader)**” for **Hardware Template** and “**Readers**” for **Hardware Class**, and then click **Next**, this is the screen you will get:



7. Here you can choose a **Reader** from one of the eighth readers that embedded Mercury controllers have:



8. You can similarly click each **Device Type** listed and then select an available **Hardware Address** from the drop-down list:



9. Click **Finish** when you're done.

© Copyright Honeywell Inc. All Rights Reserved

Honeywell

Database Configuration (DBC) - Introduction

27

Chapters of Database Configuration (DBC)

Overview
DBC - Badge Profiles
DBC - Badge Statuses
DBC - Badge Types
DBC - BLOB Types
DBC - Brass Keys
DBC - Card Formats
DBC - Classes
DBC - Clearance Codes
DBC - Companies
DBC - Database Tables
DBC - Default Events
DBC - Deferred Access
DBC - Dial-Up Schedule
DBC - Event Procedures
DBC - Event Triggers
DBC - Event Types
DBC - Galaxy User Management
DBC - Groups
DBC - Guard Tours
DBC - Holidays
DBC - Keyboard Accelerator

27.1 Overview

The Database Configuration module enables you to configure the Pro-Watch database elements. Since these database elements will relate directly to the specific Pro-Watch hardware items you configure (see "" in Chapter 6), you should configure that hardware before following the procedures in this module.

This chapter presents all of the Pro-Watch database elements in alphabetical order so you can reference them easier. There is a prescribed order, however, for configuring core database elements. The following chart illustrates the configuration task flow for core database elements.

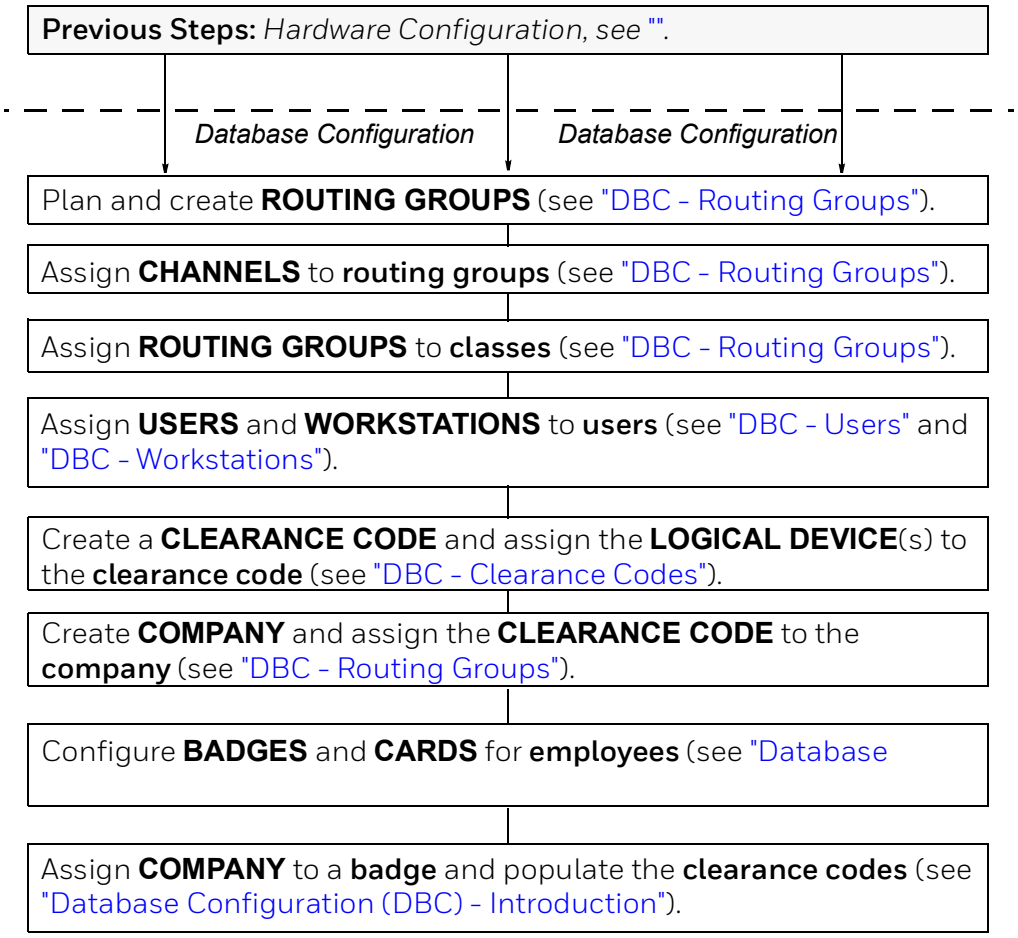
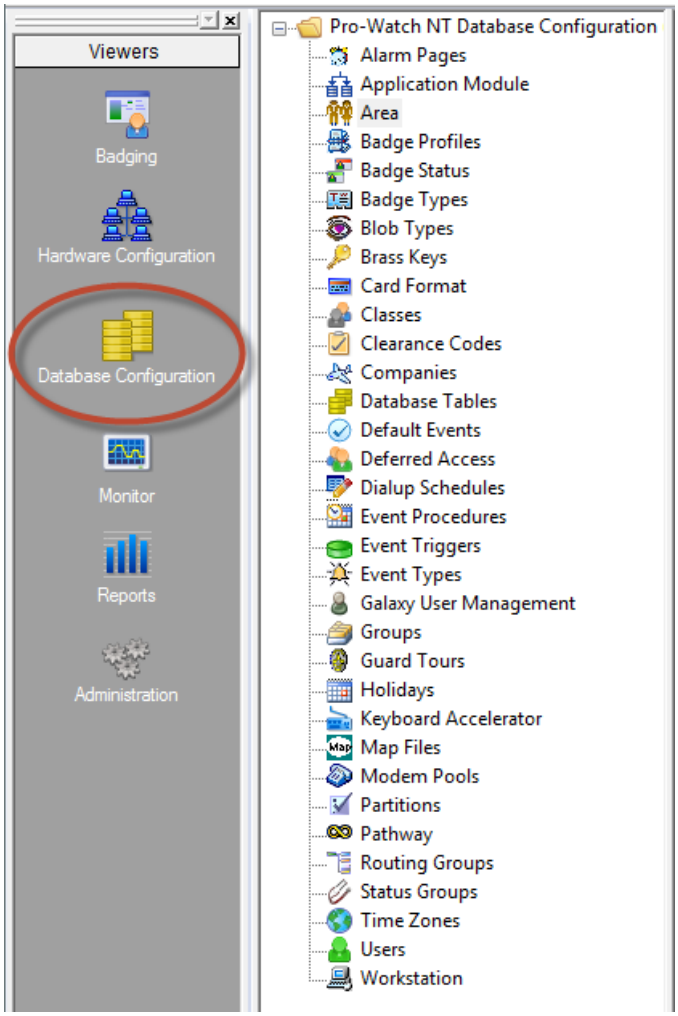


Figure 27-1 Database Configuration Task Flow

Click the **Database Configuration** link in the left navigation pane to display all the database configuration options, each represented by a different icon button:



27.2 Viewing the Icons

Use this function to change the visual display of the icons in the right pane of the Pro-Watch window.

1. Right-click anywhere in the right pane of the Pro-Watch window and select **View**.
2. Click one of the following four view options:
    - Large icons – enlarges the icon.
    - Small icons – displays smaller icons.
    - List – arranges the icons in a vertical list.
    - Details – lists the icons by system-configured details.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Alarm Page

28

In this chapter ...

Overview

Alarm Functions

Adding or Editing an Alarm Page

Viewing Alarm Page Dependencies

Copying an Alarm Page

Deleting an Alarm Page

28.1 Overview

An alarm page defines the Alarm Monitor display of incoming alarms. See Chapter 3, for details about alarm display. An alarm page defines the column layouts, lists the type of associated events, and specifies the maps a user will see when using the Pro-Watch Alarm Viewer. Alarm pages are assigned to classes or individual users.

You can also display the names of resources that depend on the alarm page, make a copy of the alarm page's configuration, and arrange the visual display of the alarm page icons in the Pro-Watch window. You can configure the alarm page, for example, to display the incoming alarm's event type as well as its associated logical device, group, or map resource.

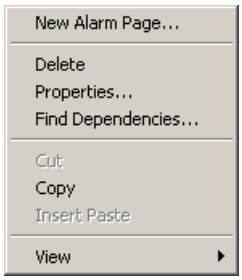
28.2 Alarm Functions

To access alarm page functions:

1. In the Pro-Watch Database Configuration tree list, click the **Alarm Pages** icon to display the currently-configured alarm pages in the right pane of the Pro-Watch window.

Note: Right-click any alarm page icon to display the pop-up menu (if no alarm pages have been created yet, right-click anywhere in the right pane).

If no alarm pages have been created yet, this pop-up menu only shows a subset of these functions.

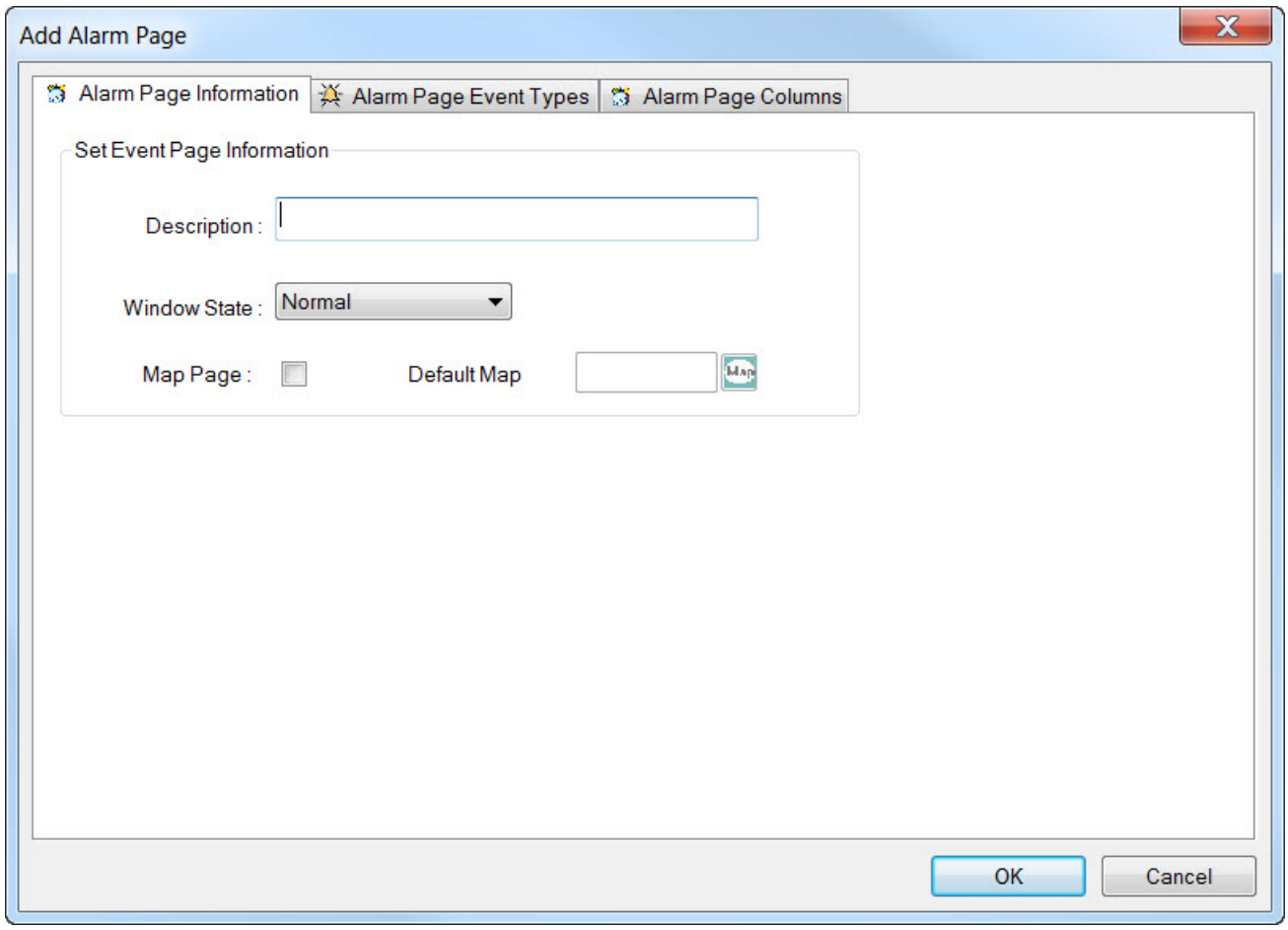


2. Use the following table to select a function:

Click ...	To ...
New Alarm Page...	Add a new alarm page. See "Adding or Editing an Alarm Page".
Delete	Delete a current alarm page. See "Viewing Alarm Page Dependencies".
Properties...	Edit a current alarm page. See "Adding or Editing an Alarm Page".
Find Dependencies...	Display the names of all resources that depend upon the alarm page. See "Viewing Alarm Page Dependencies".
Copy	Make a copy of the alarm page configuration. See "Copying an Alarm Page".
View	Change the way the icons are displayed in the Pro-Watch window.

28.3 Adding or Editing an Alarm Page

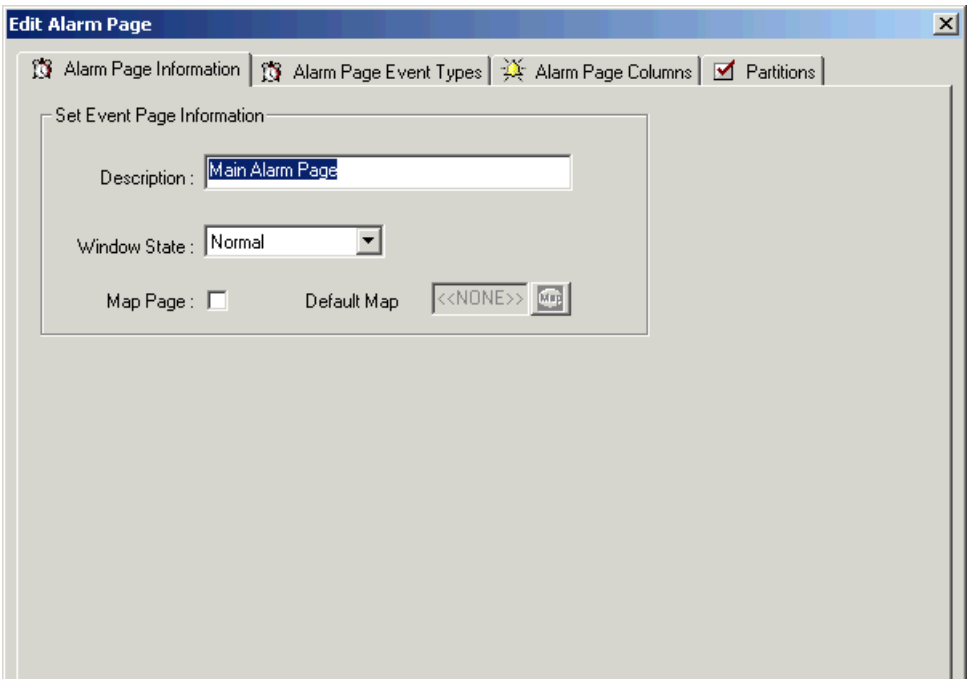
1. To add an alarm page, right-click the **Alarm Pages** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane of the Pro-Watch window).
2. Select **New Alarm Page** to display the **Add Alarm Page** dialog box:



There are **three tabs** on this page each of which is explained further down below in this chapter.

After you create an alarm page, you must assign it either to a class or to a user to make it operative. See Alarm Pages Tab, page 9 in "DBC - Classes" in Chapter 36 or Alarm Pages Tab, page 21 in "DBC - Users" in Chapter 58 for instructions.

3. To edit an existing alarm page, right-click the alarm page icon in the right pane of the Pro-Watch window and click **Properties**. The Edit Alarm Page dialog box appears.



4. Complete the following tab sections to add or edit alarm page information:

ALARM PAGE TABS LIST

- "Alarm Page Information Tab".
- "Alarm Page Event Types Tab".
- "Alarm Page Columns Tab".
- "Partitions Tab".

28.3.1 Alarm Page Information Tab

1. Enter a **Description** for the alarm page.
2. Select a window state:
   - **Normal** – places the window within the monitor screen.
   - **Maximized** – places the window to cover the entire screen.
   - **Minimized** – minimizes the window as a button at the screen's bottom.

3. Select or clear the **Map Page** check box if you do or do not want a map that shows the alarm location, respectively. To select a **Default Map**, click the  button and browse.

28.3.2 Alarm Page Event Types Tab

To add an event to the list:

Click **Add** to display the Event Types dialog box and select the event.

To add an event that is not on the Event Types list:

Click **Add** to display the Information dialog box and specify the event.

Click the **Annunciation** tab to specify the event's color and audio file.

Note: In the Alarm Page Event Types tab, click the values in the event's **Ack** and **Clear** columns to change those values, if you desire to change them.

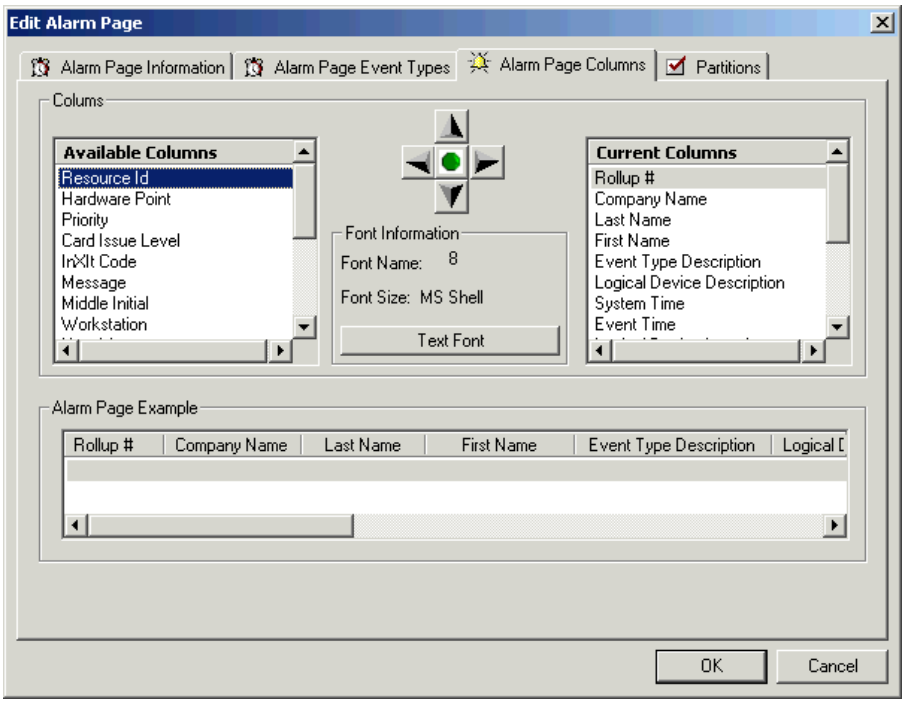
You can change a **Y** (yes) to **N** (no), and vice versa. If you specify Y, the Ack or Clear will appear on the alarm page.

To delete an event already on the list:

Select the event and click **Delete**.

28.3.3 Alarm Page Columns Tab

This tab defines the alarm page's columns, or the types of information provided for each event. The **Current Columns** box in the Alarm Page Columns tab shows the alarm page's current columns.



To add a new column to the alarm page:

Select the column in the Available Columns box and click the east arrow.

To delete a column in the Current Columns box:

Select the column and click the west arrow.

28.3.4 Partitions Tab

Partitions determine the view of the resources within Pro-Watch.

Example: In a building with multiple tenants, the tenants on floor one may not want to see the resources (users, sites, badges, etc.) of floor two and vice versa. To hide a floor's resources, you can partition them within Pro-Watch.

Note: If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition.

Use this function to create, assign or delete a partition:

To create a partition for the alarm page:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the alarm page:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

28.4 Viewing Alarm Page Dependencies

An alarm page can depend upon other database objects. The User and Class objects are dependencies of an Alarm Page.

To view an Alarm Page's dependencies:

1. In the Pro-Watch Database Configuration tree list, click the **Alarm Page** icon to display the currently-configured alarm pages in the right pane.
2. Right-click the icon of the alarm page for which you want to show dependencies, and select **Find Dependencies**. The Dependencies dialog box appears and lists the existing dependencies for the alarm page.
3. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
4. Click **OK** to close the dialog box.

28.5 Copying an Alarm Page

Copying an Alarm Page can be a fast way to create a new alarm page. If the original page will be similar to the new page, you can copy the original and change only a small number of its properties to create the new page.

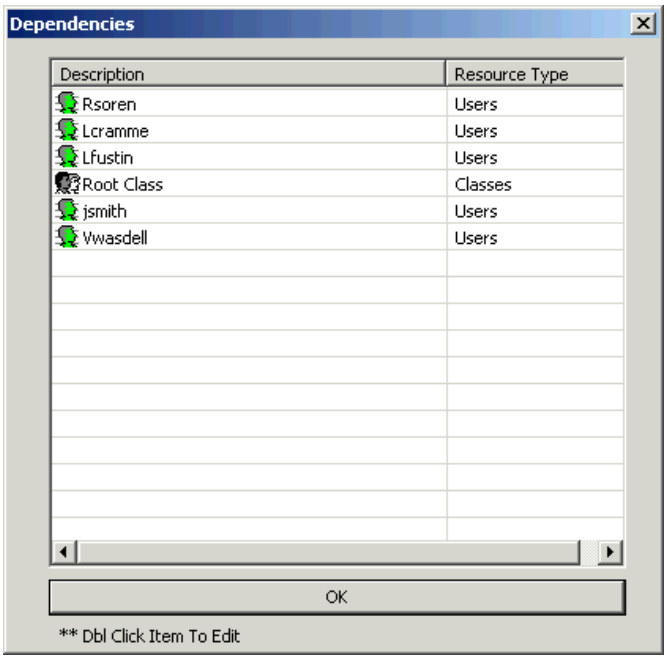
1. In the Pro-Watch Database Configuration tree list, click **Alarm Page** to display the currently-configured alarm pages in the right pane.
2. Right-click the icon of the alarm page you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original alarm page name]” appears in the right pane.

28.6 Deleting an Alarm Page

1. In the Pro-Watch Database Configuration tree list, click the **Alarm Pages** icon to display the currently-configured alarm pages in the right pane.

Note: Right-click the icon of the alarm page you want to delete, and select **Delete**.

You cannot delete an alarm page that has dependencies. A dependency is another database object that includes the Alarm Page in its configuration. The Class and User objects are Alarm Page dependencies. If the alarm page has no dependencies, it is deleted. However, if the alarm page does have dependencies, the **Dependencies** dialog box appears**.**



2. If you still want to delete the alarm page:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Click each dependency's Alarm Pages tab, and click to select the alarm page.
   c. Click **Delete/Revoke** to delete the alarm page from each dependency's configuration.
3. Repeat step 2 and click **Yes** at the prompt to delete the alarm page.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Area

29

In this chapter ...

Overview

Area Functions

Adding or Editing an Area

Deleting an Area

Locking or Unlocking an Area

Setting an Area's Zone Mode Properties

Anti-Pass-Back (APB) Update Limitations

29.1 Overview

A Pro-Watch area is a defined space for which you create a secure access plan. For a given area, you can define associated logical devices, lock and unlock capability, and zone mode attributes. This enables you to define how a badge holder enters and exits a secure area using designated In and Out readers.

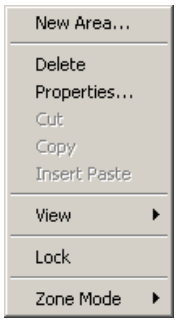
29.2 Area Functions

To access area functions:

1. In the Pro-Watch Database Configuration tree list, click the **Area** icon to display the currently-configured areas in the right pane of the Pro-Watch window.

Note: Right-click any area icon to display the pop-up menu. If no areas have been created yet, right-click anywhere in the right pane.

If no areas have been created yet, this pop-up menu only shows a subset (New Area, and, View) of these functions.



Use the following table to select a function:

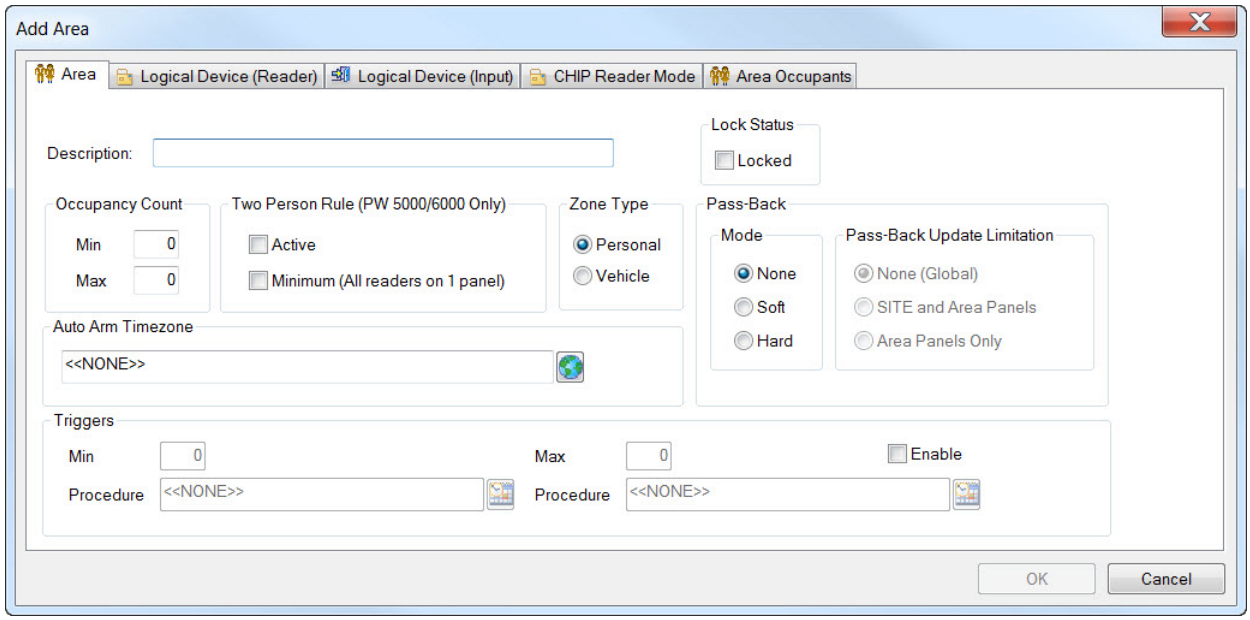
Click...	To...
New Area...	Create a new area. See "Adding or Editing an Area".
Delete	Delete a current area. See "Deleting an Area".
Properties...	Edit a current area configuration. See "Adding or Editing an Area".
View	Change the way the icons are displayed in the Pro-Watch window.
Lock	Lock and secure the area's entrances and exits. See "Locking or Unlocking an Area".
Zone Mode	Set the operational condition of the alarms in the area. See "Setting an Area's Zone Mode Properties".

29.3 Adding or Editing an Area

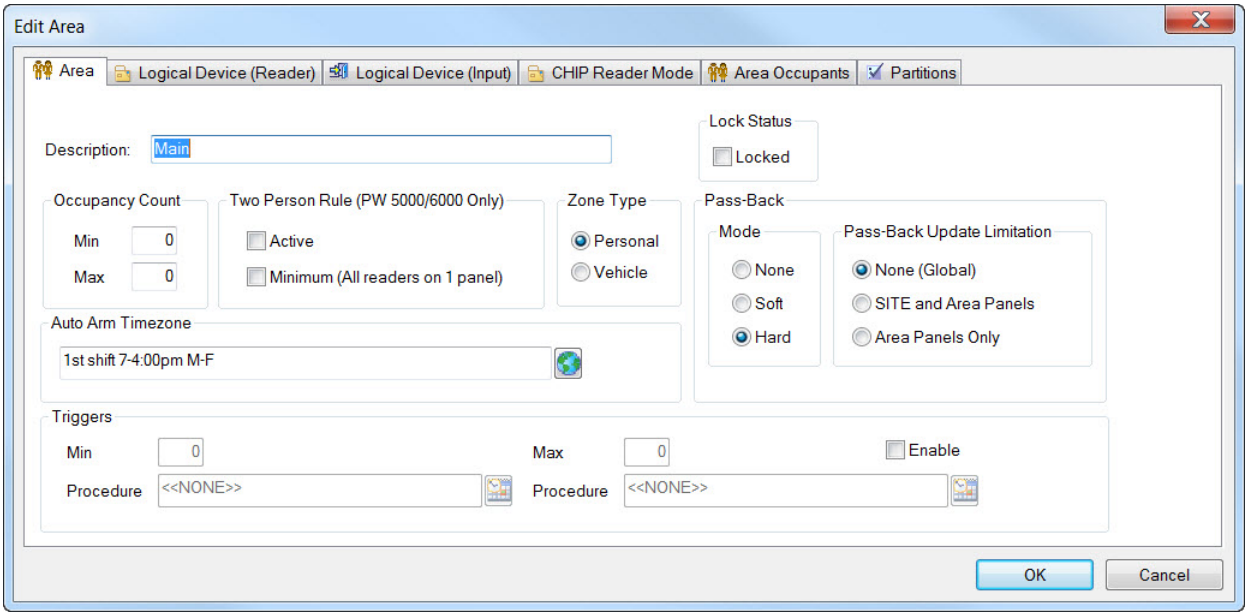
You can add or modify a new area, define the associated logical devices for an area, lock and unlock an area, and set area zone mode attributes.

*To **add** or edit an area:*

1. To add an area, right-click the **Area** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane of the Pro-Watch window), and select **New Area**. The **Add Area** dialog box appears:



2. To edit an area, right-click the area icon in the right pane of the Pro-Watch window and click **Properties**. The **Edit Area** dialog box, which looks just like the Add Area screen shot above, appears:

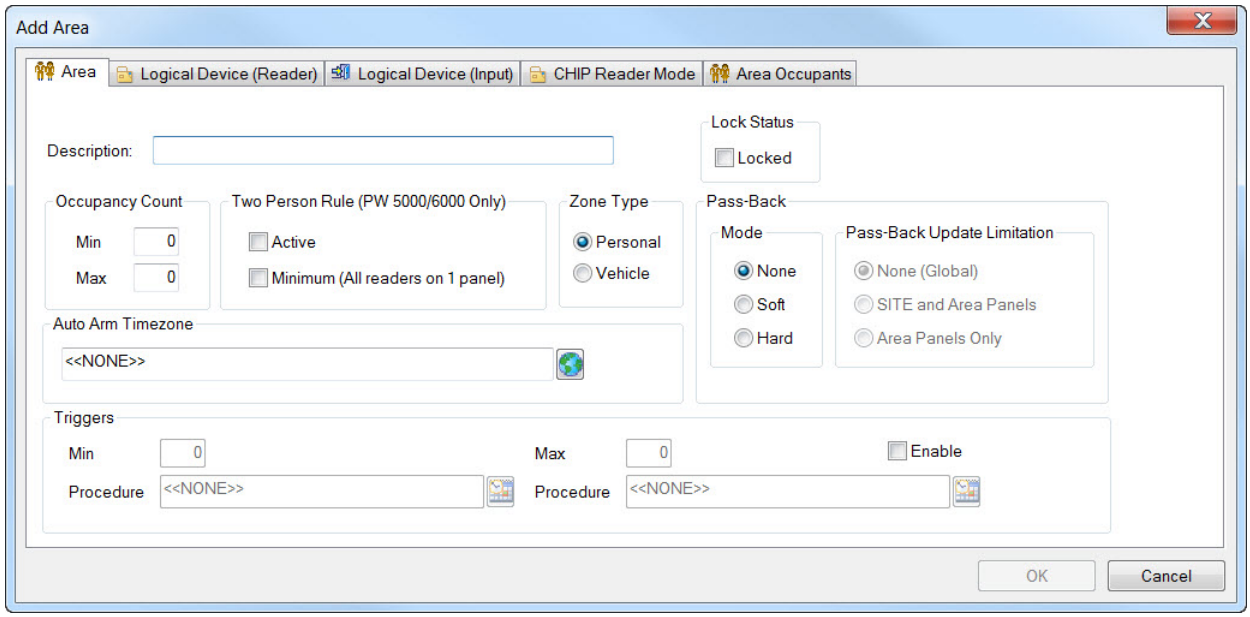


3. Complete the following tab sections to add or edit area information:

AREA TABS LIST

- "Area Tab"
- "Logical Device (Reader) Tab"
- "Logical Device (Input) Tab"
- "CHIP Reader Mode Tab"
- "Area Occupants Tab"
- "Partitions Tab"

29.3.1 Area Tab



Use the following field definitions to complete the **Area** tab in the **Add Area** dialog box:

Description -- The name of the area.

Lock Status -- Specifies whether the status is “locked” or “unlocked.” Select the check-box if the area is normally locked.

Occupancy Count -- Min (minimum) and Max (maximum) number of occupants allowed in the area.This feature is used only for the Two-Person Rule (See Appendix K).

Two-Person Rule -- Specifies the state of the two-person rule. The two-person rule requires at least two people in the area.

1) Select the **Active** to activate a two-person rule for an area. This means that the readers for the area will allow access only if two cards are pre-sented at once and people enter and exit the area only in pairs.

2) Select the **Minimum (all readers on 1 panel)** check-box **together with the Active check-box** to have PW-5000/6000 panel handle entry/exit on an area defined on the panel.

- **A minimum of two people must be present in the area at any given time. This means that the first two cards must be presented at an input reader at the same time before the door will open.**
- **Once those two enter, any number of others may enter, up to the maximum number set for the area.**
- **Any number can leave by the exit readers, as long as there are always at least two people left in the area. Those last two have to present their cards at an exit reader at the same time or the panel will not open the door.**

NOTE 1: Selecting **Minimum (all readers on 1 panel)** check-box alone has no effect on anything.
NOTE 2: The PW2000 panel does not support the two-person rule. Only PW-5000/6000 panels support this feature.
NOTE 3: ALL the input and output readers for an area must be on the SAME PW-5000/6000 panel. If the readers are on multiple PW-5000/6000 panels, this reverts to the existing two-person rule.
NOTE 4: The two-person minimum feature works only if anti-passback of some level is previously set, for both the hardware and the area.

NOTE 5: The maximum occupancy count needs to be set to at least 2 for two-person minimum to work, though such a setting is not useful. Anything greater than 2 is useful. Leaving it at 0 will not allow anyone access to the area.

Zone Type -- Specifies either "Personal" (for door access) or "Vehicle" (for parking lot or guard shack access). Note that this field is not available if you are using a PW-5000 panel.

Pass-Back Mode -- **None** means there is no pass-back rule applied. **Hard** means anti-passback rule is applied every time a user has a transaction at a reader. **Soft** means the anti-passback rule is not applied but the violation is reported to the operator without the user's knowledge. You have to select either **Soft** or **Hard** mode to enable the "**Pass-Back Update Limitation**" options.

Pass-Back Update Limitation -- Sometimes downloading pass-back updates tie up the network traffic and cause unexpected delays in processing. That's why Pro-Watch offers three different update limitation options:

- **None (Global) --** Select this option for no limitations on downloading any pass-back updates. All updates are downloaded to every site, area, or panel connected to the Pro-Watch server. This option would take the longest time to download the updates.
- **SITE and Area Panels --** Select this option to download the pass-back updates to the panels both in the area and the other panels in the same site.

- **Area Panels only --** Select this option to download the pass-back updates only to the panels in the area. This option would take the least time to download the updates.

See the section on "Anti-Pass-Back (APB) Update Limitations" further in this chapter for more detailed information on this topic.

Auto Arm Timezone -- Select a time zone during which the area is automatically armed. Click the browse button to either define a new time zone in the **Time Zones** screen or edit an existing one in the **Edit Time Zones** screen.

Triggers -- Select the Enable check-box to trigger a procedure when the minimum or the maximum threshold is violated. Enter the Min (minimum) and Max (maximum) occupancy count. Select a separate Procedure to triggered either when the occupancy count is equal to or less than the minimum threshold (except for 0), or when the count is equal to or more than the maximum threshold.

If there are no procedures listed in the drop-down list, select **Define** from the pop-up list to display the **Event Procedures** dialog box. Click **Add** to display the **Add Event Procedures** dialog box and add an event by filling all the required fields. Click **Add** to finish adding the event procedure.

Configuring an Area for Anti-Passback

The most effective anti-passback strategy is to configure an Area for either “hard” or “soft” anti-passback operation. As explained above, a “Hard” setting will not allow a second entry on the same card without an exit, and a “soft” setting does allow a second entry on the same card without an exit. The “soft” setting, however, generates an alarm upon the second and subsequent entries.

Notes:

- **If you set the Area to either a hard or soft anti-passback setting, you must also set the Panel for anti-passback operation.**
- **An Area’s anti-passback setting overrides any anti-passback setting for a Reader or Card in that Area.**

To configure an Area for either hard or soft anti-passback operation, select Anti-Passback Locations in the panel’s properties tab. See "Adding a PW-6000/5000/3000 Panel" in Chapter 9 for instructions.

29.3.1.1 Hard and Soft APB

Note: Anti-passback fails when Area APB In and Out readers are also used as Enrollment and De-enrollment for Timed Clearance codes.

The available anti-passback options within an Area are only **Hard**, **Soft**, or **None**.

Hard anti-passback will not allow anti-passback under any circumstances.

Soft anti-passback will allow a Logical Device within an Area to operate under timed anti-passback rules (when the panel and Logical Device are configured for anti-passback). This configuration, however, generates an alarm each time the reader reads a card.

29.3.1.2 No REX

If you set an anti-passback control for an area or zone, do not install REX (Request to Exit) devices at the doors between the zones.

Tip: For anti-passback zones, it is recommended that you use one physical door from zone A to zone B and another physical door from zone B to zone A. In this case, install door switches at both doors. Door switches are shunted by an access control unit (ACU) when a qualified card is read at a reader.

If an anti-passback-controlled door is not monitored by a door switch, then the ACU assumes that whenever a card is presented to a reader, the cardholder gains access through that door. If cardholder access is interrupted, the cardholder cannot present the card a second time.

Note: Using a door switch ensures that the ACU waits until the door opens before changing the cardholder status either from being in zone A to being in zone B, or from being in zone B to being in zone A. Therefore, door switches are recommended in Anti-Passback zones.

It is possible in Pro-Watch to allow exits but not allow double entries within the delay time. To do this:

1. Select "Timed by CARD HOLDER" APB mode for the ENTRY READER. Select a delay time that you like. (See the next section below: "***Timed by Reader vs. Card Holder***".)
2. Select "None" APB mode for the EXIT READER.

   Note: This configuration is not possible for an area since it does not support timed APB."

A PW2000 and PW-5000 panel can both participate in the same area and support Anti-Passback, when the PW2000 is participating only in that one area and the Anti-Passback function is set to "hard." All of the global Anti-Passback features apply when both panels are participating.

Example: If a card holder enters a PW-5000-controlled door, she cannot also enter a PW2000-controlled door in the same area.

Also, the PW2000 panel does not support the two-person rule. Therefore, in an area where both a PW2000 and PW-5000 are participating and supporting Anti-Passback, the two-person rule is not in effect.

Note: One area cannot be defined within another area for PW2000 and Cardkey panels. SEEP panels support multiple areas, but only through deferred mode. Other panels do support "internal areas."

29.3.1.3 Timed APB

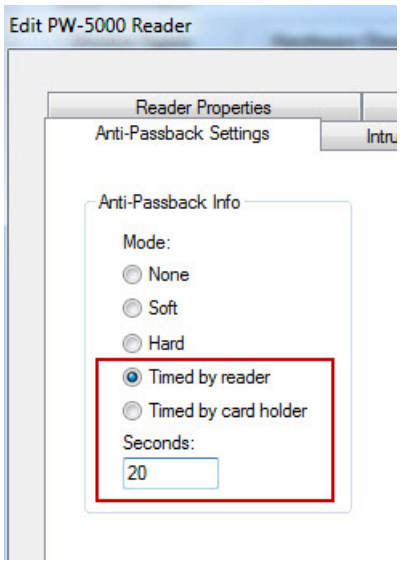
Another anti-passback strategy is timed anti-passback (APB).

When anti-passback is timed, Pro-Watch grants access by the same card (without an exit) for a second entry only after a specified time period has elapsed.

Note: Timed APB is not available for an area. It is available only at the reader level. Do not configure Logical Devices within a configured Area for timed anti-passback.

29.3.1.4 Timed by Reader vs. Card Holder

The user can select from two different APB timing options for a reader:

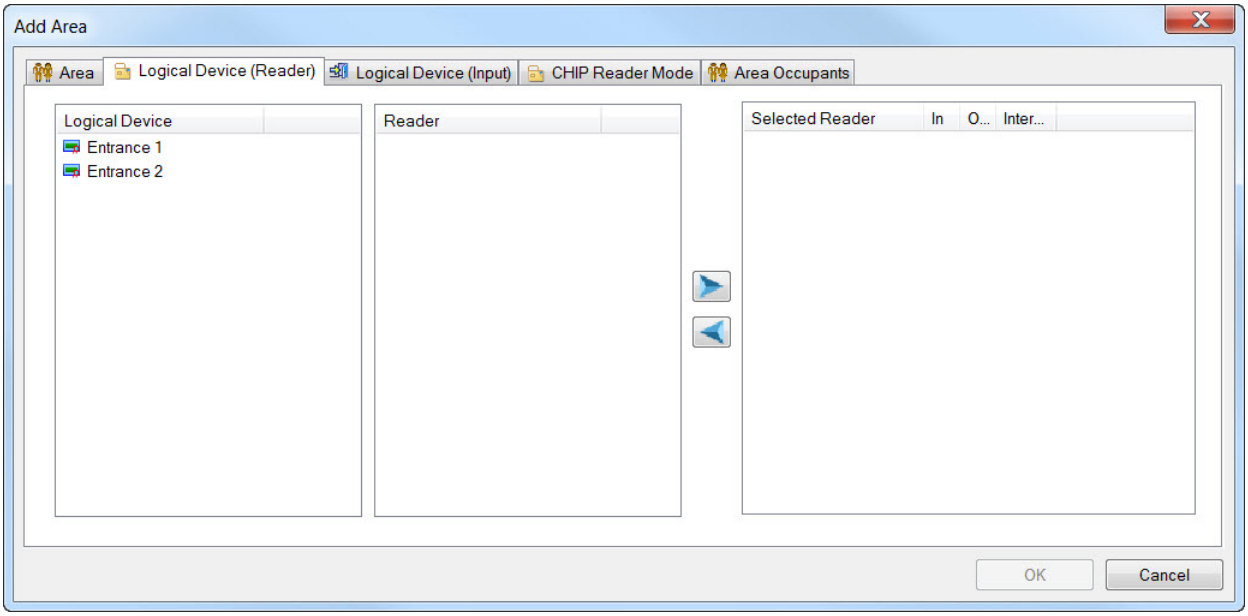


Note: Both of these APB modes work on a single panel. These options work only if the reader is not included in an Area. If the reader is included in an area, then the area setting will override the reader settings for anti-passback.

Timed By Reader - The reader keeps track of the cardholder and will not let the same card to be re-used within the delay period. Panel only keeps track of last card; so if another card is used on the same reader, then the panel stops keeping track of the previous card. Thus it is possible to use the same card multiple times within the delay period as long as other cards are used in between.

Timed By Card holder - The cardholder will not be allowed to re-use a card consecutively on the same reader within the delay period. Panel keeps track of each card's usage on a reader.

29.3.2 Logical Device (Reader) Tab

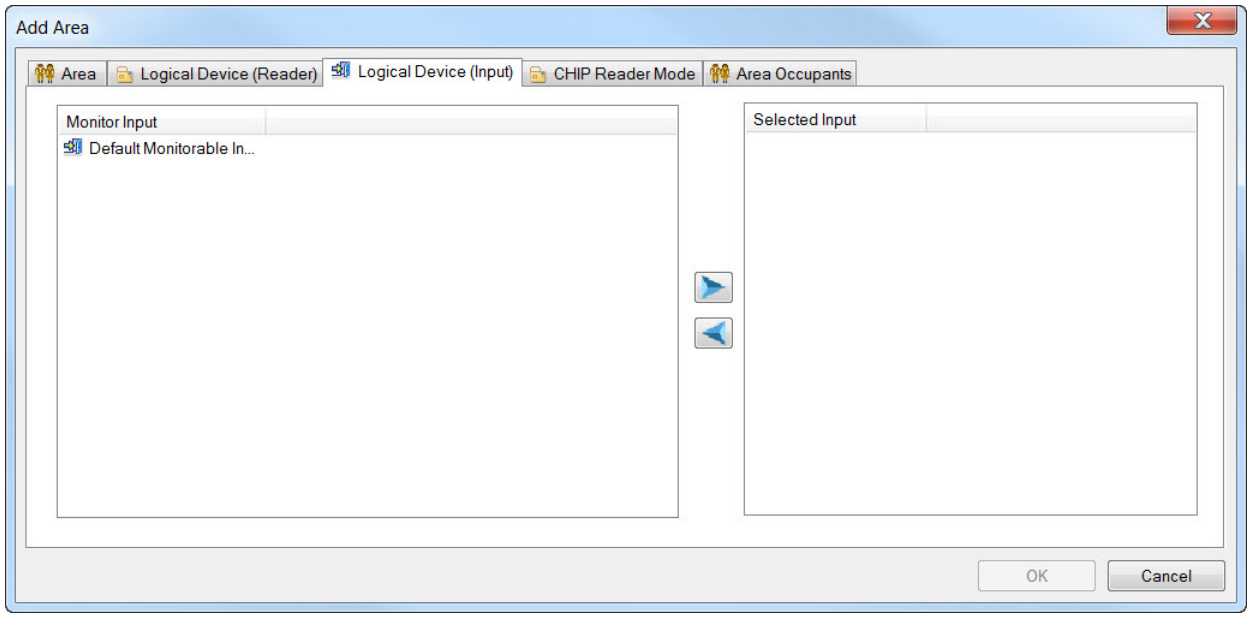


To select readers from the available logical devices:

1. Click a device in the **Logical Device** pane. The name of the reader assigned to the logical device appears in the Reader pane.
2. Click the entry under **Reader** to select it.
3. Click the right arrow button to list the device under **Selected Reader**.
4. Repeat steps 1–3 for all of the readers you want to be Selected Readers.
5. To delete a reader from the Selected Reader list, click the reader and click the left arrow button.

6. Click to designate the Selected Reader as one of the following (by placing an "X" mark under respective column):
   - **In** – designates this reader to allow entry into the area.
   - **Out** – designates this reader to allow exit from the area.
   - **Internal** – designates this reader to be used when the occupant remains in the area.
7. Click **OK** to save your settings.

29.3.3 Logical Device (Input) Tab



Use this function to designate a logical device as an input point in an area. Input points comprise the **PW-5000 Monitor Point Groups (MPG)** feature that supports anti-passback and burglar alarm functions.

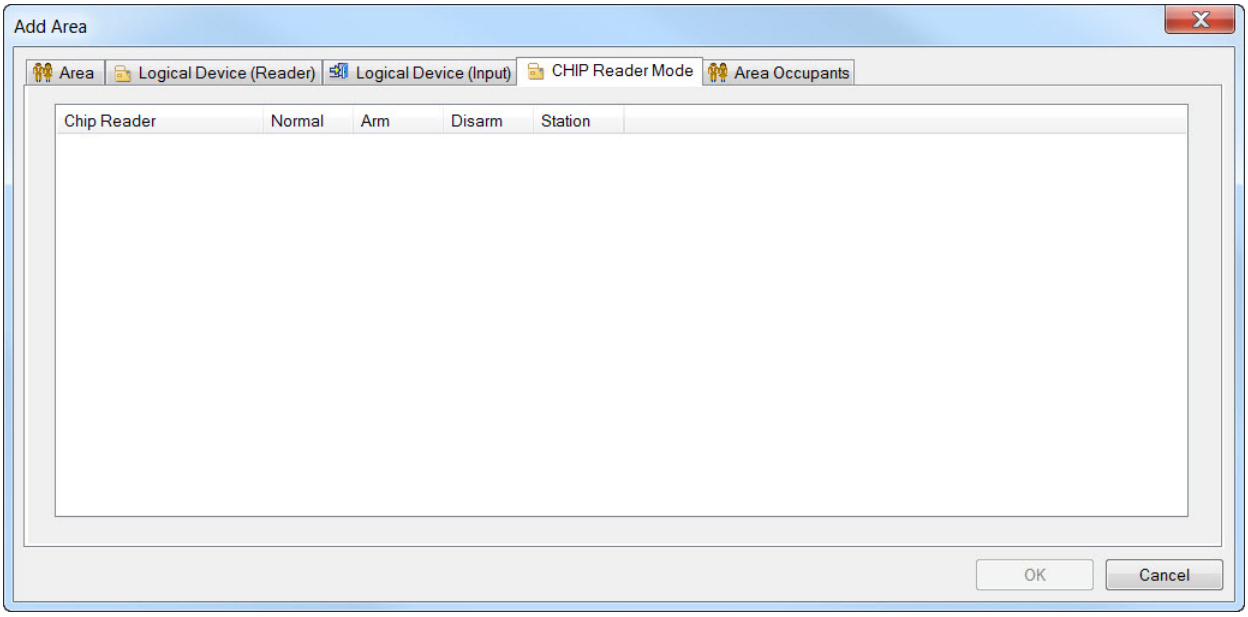
Example: An MPG system could be designed for a store. The system would consist of designated monitoring (or input) points. As the last person to leave the store at night, the manager would swipe a specially-coded card to activate the alarm system. The panel then determines whether all of the monitor input points are in a normal state. For example, if a door designated as an input point has been left ajar, the panel detects the "abnormal" status and does not allow the manager to activate the alarm.

In the Logical Device (Input) tab, designate a monitor input to be a Selected Input:

1. Select a Monitor Input entry in the **Monitor Input** pane.
2. Click the **right arrow button**. The monitor name appears in the **Selected Input** pane on the right.

3. To delete a selected input, select the input in the Selected Input pane and click the **left arrow button**.
4. Click **OK**.

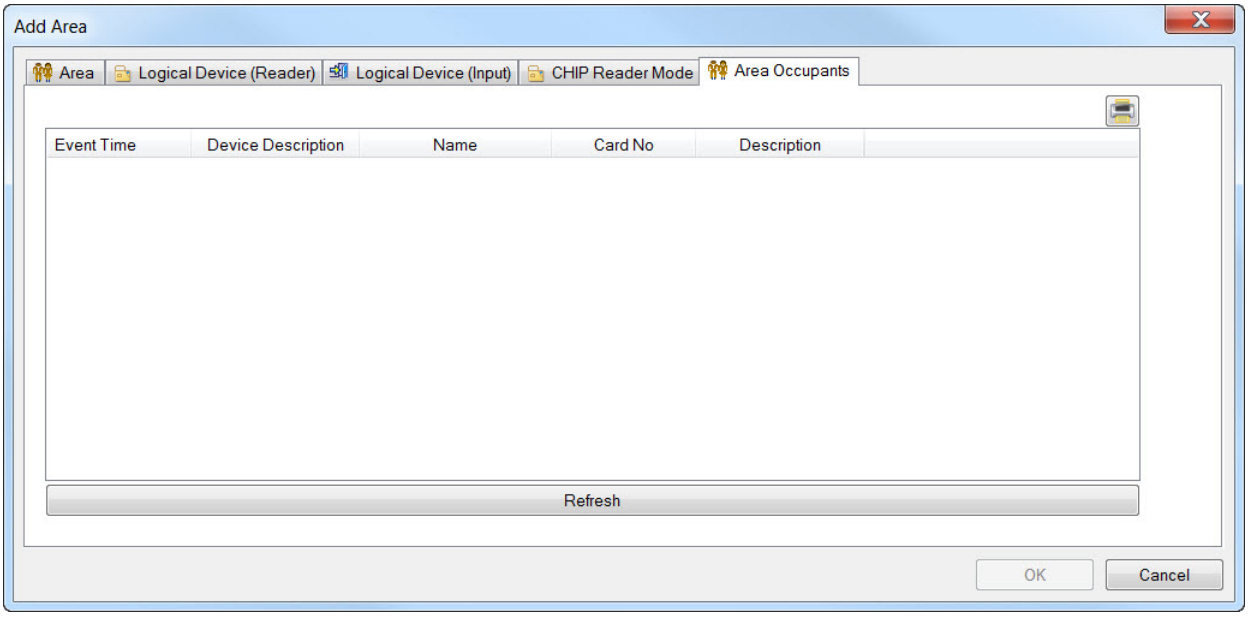
29.3.4 CHIP Reader Mode Tab



If you have designated a CHIP reader in the Logical Device (Reader) tab to be an “In” reader, set the CHIP reader mode in the **CHIP Reader Mode tab**. Use the following descriptions to set the CHIP reader mode.

Field	Description
Normal	Sets the reader and door to the default state.
Arm	Sets the reader and door to a locked state.
Disarm	Masks, or shunts, all input points in the area.
Station	Provides a privileged card holder the ability to change zone status. Can be performed via keypad reader or a reader and a station mode switch.

29.3.5 Area Occupants Tab



Monitor the occupancy of the area by viewing the event log in the Area Occupants tab. Click **Refresh** to display the most recent updates.

29.3.6 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the area:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the area:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

29.4 Deleting an Area

1. Right-click the icon of the area that you want to delete from Pro-Watch and select **Delete**.
2. Click **Yes** to confirm the deletion.

Caution: It is possible to delete an area and still leave an operating card reader at an access point at the deleted area. In this case, a card reader at a door to the deleted area would no longer restrict door access. Note, however, the behavior in the following unlikely sequence:

a. Set an area to soft anti-passback.

b. Delete the area.

c. Set “timed” anti-passback, and swipe the card once.

d. Swipe the card a second time after the time period lapses.

e. A message appears indicating that the card is already in the area, even though the area has been deleted.

If this occurs, re-start the Pro-Watch service.

29.5 Locking or Unlocking an Area

To lock or unlock the area's entrances and exits:

1. Click the **Area** icon in the Pro-Watch Database Configuration tree list.
2. In the right pane, right-click the icon of the area you want to lock. If the area is currently locked, a red "no entry" mark (a circle with a diagonal slash across) appears superimposed on the area icon. If the icon is not stamped with a red "no entry" mark, the area is unlocked.
3. Click **Lock** to lock an unlocked area, or click **Lock** to unlock a locked area and display the **Action Note** screen.
4. Enter an **Action Note** to record information relevant to the locking or unlocking. If locked, the area icon will change, displaying a lock:



5. Click **Done**.

29.6 Setting an Area's Zone Mode Properties

1. Click the **Area** icon in the Pro-Watch Database Configuration tree list.
2. In the right pane, right-click the icon of the area for which you want to set the zone mode.
3. Select from the **Zone Mode** submenu one of the following mode options:

Zone Mode	Description
Disarmed	Places the zone in its normal state, when the space within the zone is normally occupied. All readers work normally, and intrusion detectors are ignored.
Armed	Places the zone in an active state, when the zone is unoccupied. Some readers may be disabled or available only to privileged cards. The Monitor points are all active.
Shunt	Shunts, or removes from the circuit, all readers, input points, and output relays associated with the zone.
Disabled	Turns off all readers within the zone; also places all output relays in their non-energized state.
Monitor	Stops all input active or clear activity, but still allows open or short messages to pass through.

29.7 Anti-Pass-Back (APB) Update Limitations

Anti-Pass-Back (APB) update limitations are required because sometimes the updates take too long and/or the Pro-Watch server tries to download the updates to too many panels at the same time. To decrease the load on the system, the users now can select to limit their download options.

But first let's look at an example where we have two areas, each including panels from different sites:

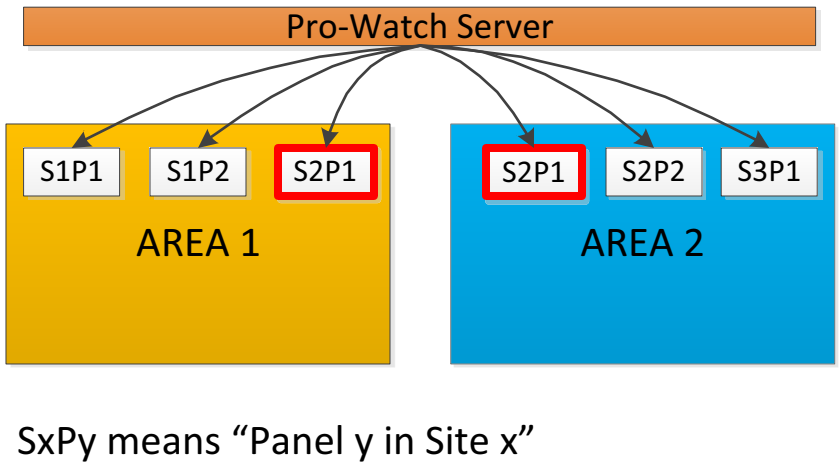


Figure 29-1 Areas connected to a Pro-Watch Server

In the above figure Figure 29-1, "S1P1" means "Panel 1 in Site 1" or "S3P1" means "Panel 1 in Site 3", etc.

As you can see:

- **An area may include multiple panels and panels from different sites.**
- **Areas 1 and 2 in the above example share the same panel S2P1 from Site 2.**

29.7.1 An Example

Now let's look at three different types of APB update options by taking Figure 29-1 as our reference.

ASSUMPTION: For the purposes of this illustration, we are assuming that the user creates a transaction by using her card at the panel **S1P1** in **Area 1**:

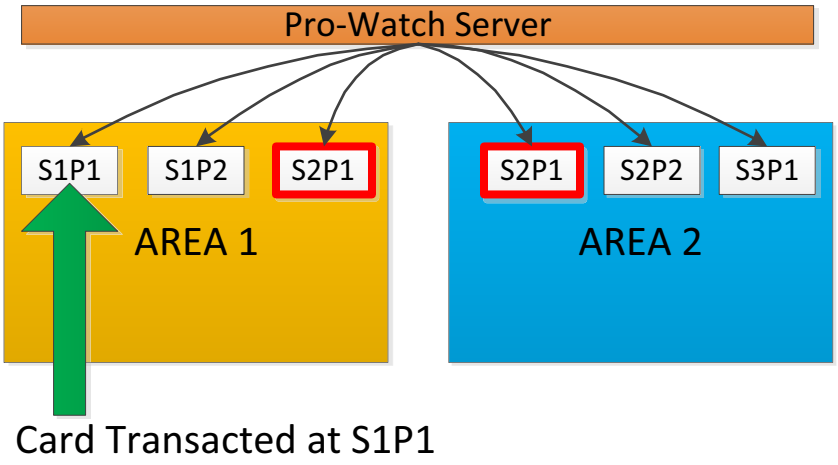


Figure 29-2 Card transacted at Panel 1 of Site 1 (S1P1)

Notes:

- **Update downloads are triggered by the reader where the card transaction takes place.**
- **Pro-Watch does not download any updates to the very same panel where the transaction has taken place. Such an update is performed locally and automatically at that local panel, without being pushed by the Pro-Watch server.**

Let's see how the selection of different APB update limitation options mean in terms of Pro-Watch server's downloads.

- **None (Global) --** Select this option for no limitations on downloading any pass-back updates. All updates are downloaded to every site, area, or panel connected to the Pro-Watch server. This option would take the longest time to download the updates.
  - In the above case (Figure 29-1), Pro-Watch downloads to the following **FOUR** panels: **S1P2, S2P1, S2P2, and S3P1**.
- **SITE and Area Panels --** Select this option to download the pass-back updates to the panels both in the area and the other panels in the same site.
  - In the above case (Figure 29-1), Pro-Watch downloads to the following **THREE** panels: **S1P2, S2P1, and S2P2**.
- **Area Panels only -- Select this option to download the pass-back updates only to the panels in the area. This option would take the least time to download the updates.**
  - In the above case (Figure 29-1), Pro-Watch downloads to the following **TWO** panels: **S1P2, and S2P1**.

29.7.1.1 Areas with Different APB Update Limitation Options

Sometimes the same panel will reference two or more areas with different APB update limitation options.

In such a case the least restrictive option takes precedence and the panel is assigned that less restrictive option.

- **None (Global) is the least restrictive option.**
- **SITE and Area Panels is the more restrictive option on the scale.**
- **Area Panels Only is the most restrictive option.**

An Example

If a panel refers to both an area with “None (Global)” option and another area with the “Area Panels Only” option, the panel is assigned the “None (Global)” APB download limitation option since it is the less restrictive of the two options.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Badge Profiles

30

In this chapter ...

Overview

Badge-System Implementation Steps

Adding or Editing a Badge Profile

Deleting a Badge Profile

Viewing Dependencies of a Badge Profile

Copying a Badge Profile

30.1 Overview

A badge profile is a collection of badge pages, and a badge page is a collection of badge fields. Use this function to define only the following elements of a badge profile:

- Badging screen tabs, such as the Access, Partition, Brass Keys, and Image Summary pages. If selected, these tabs appear on the badging screen.
- Auto Disable Cards function (turn on or off). When turned on, this function automatically disables a card after a specified number of inactive days.
- Searchable fields for the advanced and quick searches. You can specify the list of searchable fields that will appear when a user selects **Edit > Advanced Search** or **Edit > Quick Search** from the Badging menu bar.

30.2 Badge-System Implementation Steps

To create badge profiles, it is recommended that you begin with the Badge Builder utility (see "Adding a Badge Profile" in Chapter 60 for instructions). There, you can create the badge profile, the profile pages, and the page fields. Although you can use the Database Configuration component to create a badge profile in name, it is still necessary to create profile pages and page fields in Badge Builder before a user can use the profile.

After the complete badge profile (including its pages and fields) is created in Badge Builder, use the procedures in this section to add badging screen tabs, the Auto Disable function, and searchable fields.

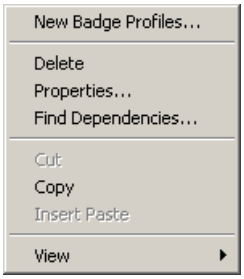
The following table lists the badge-building tasks in sequence and refers you to the appropriate chapter and section for instructions and information.

Task	Refer to ...
Create the badge profile.	"Adding or Editing a Badge Profile" in this chapter, or "Adding a Badge Profile" in Chapter 60
Create the badge profile pages.	"Adding Badge Profile Pages" in Chapter 60
Create the badge fields, if necessary.	"Adding a Badge Profile" in Chapter 60
Assign the badge fields.	"Adding a Badge Field to a Profile or Editing a Badge Field" in Chapter 60
Designate the badge types.	"DBC - Badge Types" in Chapter 32
Create badge statuses.	Adding a Badge Status, page 4
Assign cards to badges.	"Adding a Card" in Chapter 2.
Assign the badge profile to a class or user.	Badge Profiles Tab, page 10 in "DBC - Classes" in Chapter 36
Assign the badges to users.	"Adding a Card" in Chapter 2.

To access badge profiles functions:

1. In the Pro-Watch Database Configuration tree list in the center pane, click **Badge Profiles** to display the currently-configured Badge Profiles in the right pane of the Pro-Watch window.
2. Right-click a Badge Profile icon to display the pop-up menu. If no Badge Profiles have been created yet, right-click anywhere in the right pane.

Note: If no Badge Profiles have been created yet, this pop-up menu only shows a subset (New Badge Profiles and View) of these functions.



Use the following table to select a function:

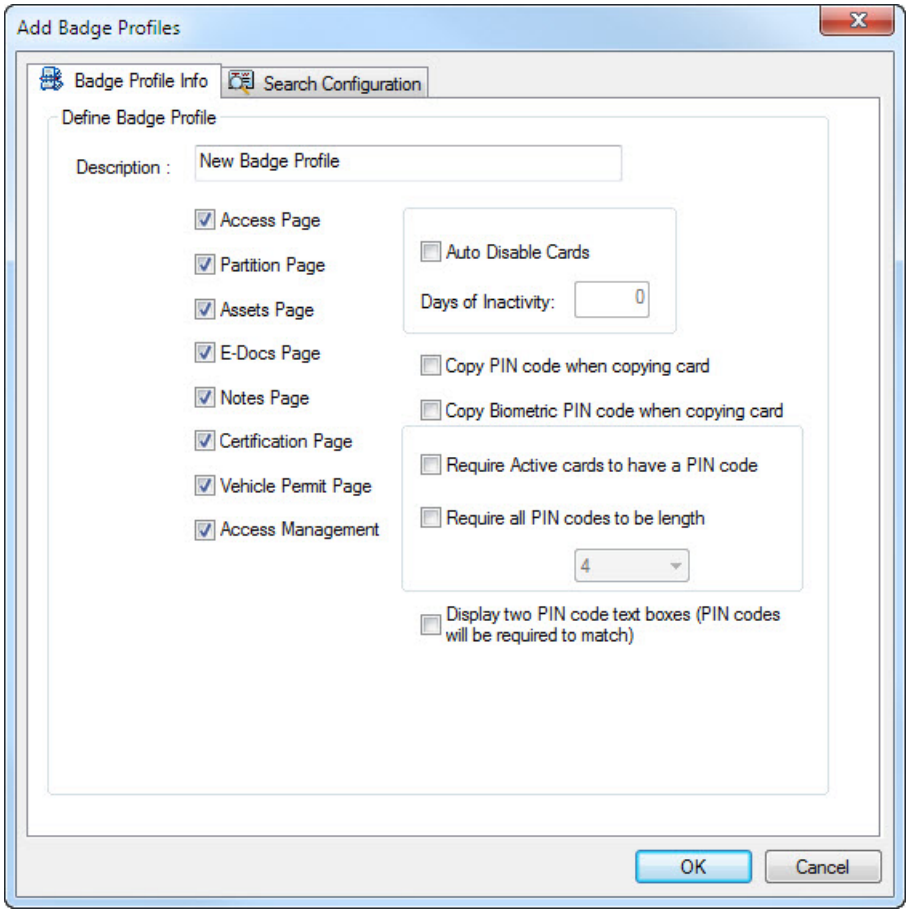
Click...	To...
New Badge Profiles...	Add a new badge profile. See "Adding or Editing a Badge Profile".
Delete	Delete a current badge profile. See "Deleting a Badge Profile".
Properties...	Edit a current badge profile configuration. See "Adding or Editing a Badge Profile".
Find Dependencies...	Display the names of all resources that depend upon the badge profile. See "Viewing Dependencies of a Badge Profile".
Copy	Make a copy of the badge profile configuration. See "Copying a Badge Profile".
View	Change the way the icons are displayed in the Pro-Watch window.

30.3 Adding or Editing a Badge Profile

You must assign the badge profile to either a class or a user before you can use the profile. See Badge Profiles Tab, page 10 in "DBC - Classes" in Chapter 36 or Badge Profiles Tab, page 22 in "DBC - Users" in Chapter 58 for instructions.

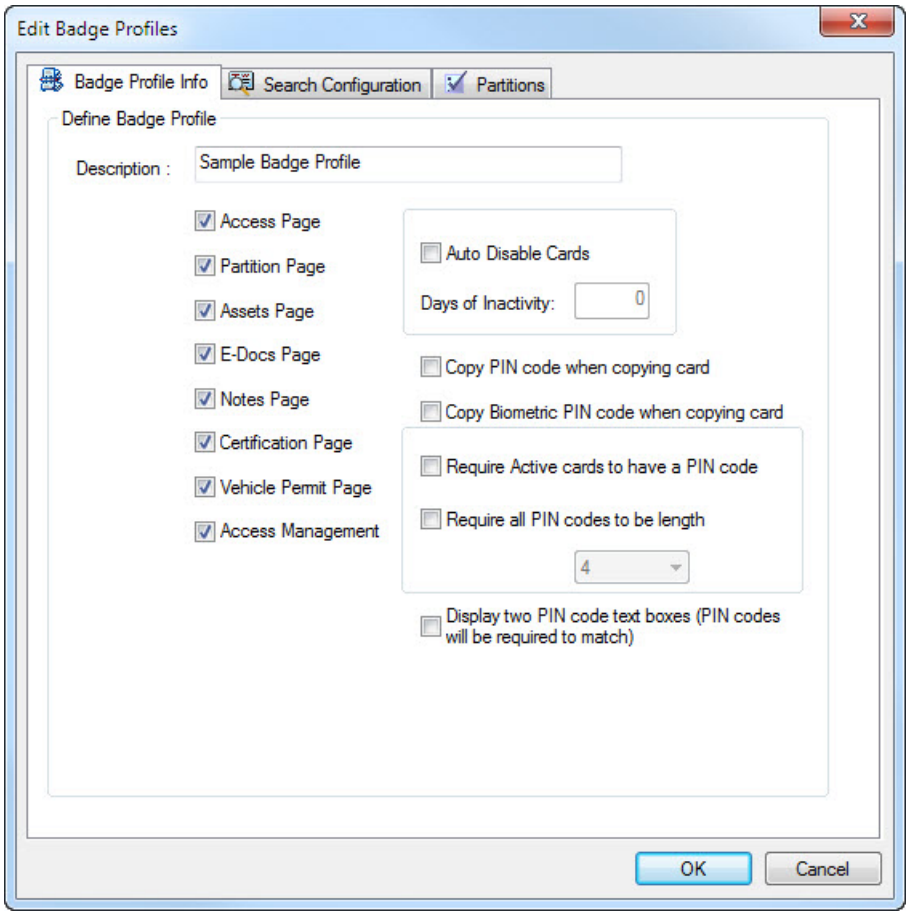
*To **add** or edit a badge profile:*

1. To **add** a badge profile, right-click the **Badge Profiles** icon in the Pro-Watch Database Configuration tree list (or anywhere in the right pane), and select **New Badge Profiles** from the pop-up menu to display the **Add Badge Profiles** dialog box:



2. To **edit** an existing badge profile, click the **Badge Profiles** icon to display the profiles in the right pane. Right-click on the badge you

want to display its pop-up menu and select **Properties** to display the **Edit Badge Profiles** dialog box:



3. Complete the following tab sections to add or edit badge profile information:

BADGE PROFILE TABS LIST

- "Badge Profile Info Tab"
- "Search Configuration Tab"
- "Partitions Tab"

30.3.1 Badge Profile Info Tab

Use the following field descriptions to complete the Badge Profile Info tab on either dialog box:

Description - The name that identifies the profile.

Access Page - When checked, provides information on cards assigned to the badge.

Partition Page - When checked, adds the Partitions tab to the Badging Screen display for users assigned this Badge Profile. Partitions determine

the view of the resources within Pro-Watch. See "DBC - Partitions" in Chapter 53 for more information.

Assets (previously called “Brass Keys”) Page - When checked, adds the Assets tab to the Badging Screen display for users assigned this Badge Profile. An “asset” is a physical object such as a brass key or a laptop assigned to a badge holder. See "DBC - Brass Keys" in Chapter 34 for more information.

E-docs Page -When checked, allows the user to attach scanned documents to the badge record.

Notes Page -When checked, allows the user to type in notes as a part of the badge record.

Certification Page -When checked, allows the user to save certification information as a part of the badge record.

Vehicle Permit Page -When checked, allows the user vehicle permission information as a part of the badge record.

Access Management Page - When checked, allows the user to record authorized clearance-code holders in the Access Management Tab of the Edit Clearance Code screen (both in the Clearance Code database module).

Auto Disable Cards and Days of Inactivity - When checked, automatically disables cards created under this profile after a specified number of inactive days.

Require all new cards to have a PIN code - This check-box is self-explanatory.

Copy PIN code when copying card - This check-box is self-explanatory.

Copy biometric PIN code when copying card - This check-box is self-explanatory.

Require all PIN codes to be length - Pick a number between 4 and 20 from the drop-down list.

Display two PIN code text boxes (PIN codes will be required to match) - This check-box is self-explanatory.

30.3.2 Search Configuration Tab

Use this function to create the list of card fields from which a user can perform a quick search. A **quick search** is a search on one field.

To move a field between the lists, select the field and click an arrow button.

To create the field list:

1. Click **Searchable Card Fields** or the **Quick Searchable Fields** list box.
2. By clicking the right arrows, move the fields that you want to be searchable from the **Unsearchable Card Fields** to the **Searchable Card Fields** list, and from **Quick Unsearchable Fields** to **Quick Searchable Fields** list.

3. By clicking the left arrows, move the fields that you want to be unsearchable from the **Searchable Card Fields** to the **Unsearchable Card Fields** list, and from **Quick Searchable Fields** to **Quick Unsearchable Fields** list.
4. Click **OK** when you're done.

30.3.3 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the badge profile:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the badge profile:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

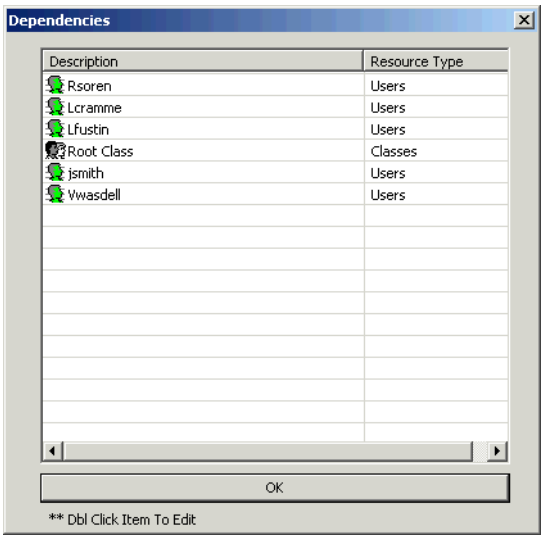
30.4 Deleting a Badge Profile

To delete a Badge Profile from the Pro-Watch database:

1. Click **Badge Profiles**. The existing Badge Profiles display in the main pane.

Note: Right-click the profile you want to delete, and select **Delete**.

You cannot delete a badge profile that has dependencies. A dependency is another database object that includes the Badge Profile in its configuration. The Class and User objects are Badge Profile dependencies. If the badge profile has no current dependencies, it is deleted. However, if the badge profile does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the badge profile:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Click each dependency's Badge Profile tab, and click to select the specific badge profile.
   c. Click **Delete/Revoke** to delete the badge profile from each dependency's configuration.
3. Repeat step 2 and click **Yes** at the prompt to delete the badge profile.

Note: Profiles that are in use cannot be deleted. To determine if an area is in use, see the next section, "Viewing Dependencies of a Badge Profile".

30.5 Viewing Dependencies of a Badge Profile

Use this function to view a list of the current dependencies for the selected Badge Profile. The Class and User objects are Badge Profile dependencies.

To view and edit a Badge Profile's dependencies:

1. In the Pro-Watch Database Configuration tree list, click the **Badge Profiles** icon to display the profiles in the right pane.
2. Right-click the profile you want, and select **Find Dependencies**. The Dependencies dialog box appears and lists the Badge Profile's dependencies.
3. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
4. After you finish viewing, click **OK** to close the dialog box.

30.6 Copying a Badge Profile

You can create a copy of a badge profile. For example, you may want to use this function to create a new profile quickly by copying and editing an existing badge profile.

1. In the Pro-Watch Database Configuration tree list, click the **Badge Profiles** icon to display the profiles in the right pane.
2. Right-click the profile you want and select **Copy**.
3. Right-click in a blank area of the main panel and select **Paste**. A new Badge Profile icon appears with the name “Copy of [Badge Profile name]”.
4. To rename and edit the new Badge Profile, see "Adding or Editing a Badge Profile".

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Badge Statuses

31

In this chapter ...

Overview
Badge Status Functions
Adding a Badge Status
Deleting a Badge Status

31.1 Overview

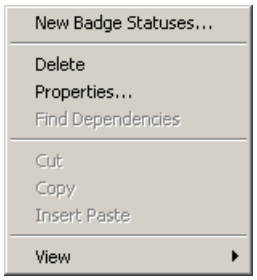
You can create, edit, or delete badge statuses. Categorizing badges by their status can be a useful way to organize them. For example, you might find it useful to maintain Active and Inactive badge statuses.

Note: Each badge can have one or more cards assigned. The status of a badge does not affect the status of its assigned cards.

31.2 Badge Status Functions

To access Badge Status functions:

1. In the Pro-Watch Database Configuration tree list, click the **Badge Statuses icon** to display the currently-configured Badge Statuses in the right pane of the Pro-Watch window.
2. Right-click a badge status icon to display the pop-up menu (if no Badge Statuses have been created yet, right-click anywhere in the right pane). Note that if no Badge Statuses have been created yet, this pop-up menu only shows a subset (New Badge Statuses and View) of these functions.



3. Use the following table to select a function:

Click...	To...
New Badge Statuses...	Add a new badge status. See "Adding a Badge Status".
Delete	Delete a current badge status. See "Deleting a Badge Status".
Properties...	Edit a current badge status configuration. See "Adding a Badge Status".
View	Change the way the icons are displayed in the Pro-Watch window.

31.3 Adding a Badge Status

1. To add a new badge status, right-click the **Badge Statuses** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Badge Statuses** to display the **Add Badge Statuses** dialog box.
2. Enter a **Description**.
3. In the **Status** field, enter any single-digit letter or number to identify the new badge status with.
4. Click the **Partitions** tab and select a partition to assign to the badge status.
5. Click **OK**.

31.4 Editing a Badge Status

1. To edit an existing badge status, click Badge Statuses to display the profiles in the right pane. Right-click on the badge you want and select **Properties** to display the Edit Badge Statuses dialog box.
2. Edit the **Description** and **Status** fields as you like.
3. Click the **Partitions** tab and edit the partition assignment as you like.
4. Click **OK**.

31.5 Deleting a Badge Status

1. In the Pro-Watch Database Configuration tree list, click the **Badge Status** icon to display all the current status icons in the right pane.
2. Right-click the status you want to delete, and select **Delete**.
3. Click **Yes** at the prompt to delete the badge status.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Badge Types

32

In this chapter ...

Overview

Badge Type Functions

Adding Types

Viewing Dependencies of a Badge Type

Copying Badge Types

Deleting Badge Types

32.1 Overview

A Pro-Watch badge type provides a way to organize your enterprise's badges. For example, you can create and design one type of badge for permanent employees and another type for contract workers.

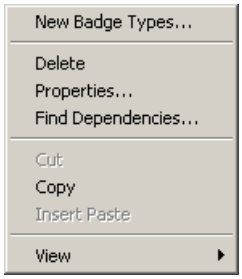
Use this function to:

- Create, delete, or modify badge types.
- Specify badge type partitions.
- Design the badge's front and back for each badge type.

32.2 Badge Type Functions

To access Badge Type functions:

1. In the Pro-Watch Database Configuration tree list, click the **Badge Types** icon to display the currently-configured Badge Types in the right pane of the Pro-Watch window.
2. Right-click a badge type icon to display the pop-up menu (if no Badge Types have been created yet, right-click anywhere in the right pane). Note that if no badge types have been created yet, this pop-up menu only shows a subset of these functions.

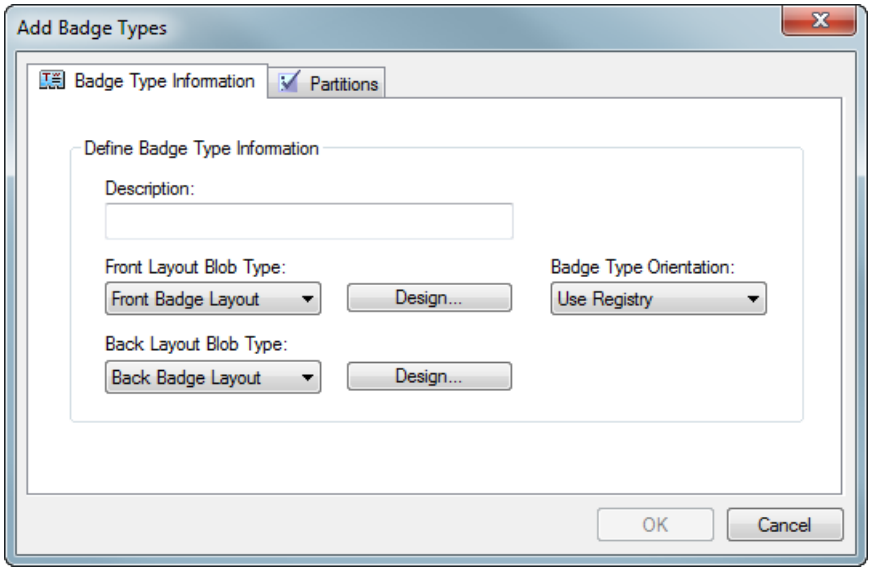


3. Use the following table to select a function :

Click...	To...
New Badge Types...	Add a new badge type. See "Adding Types".
Delete	Delete a current badge type. See "Viewing Dependencies of a Badge Type".
Properties...	Edit a current badge type configuration. See "Adding Types".
Find Dependencies...	Display the names of all resources that depend upon the badge type. See "Viewing Dependencies of a Badge Type"
Copy	Make a copy of the badge type configuration. See "Viewing Dependencies of a Badge Type".
View	Change the way the icons are displayed in the Pro-Watch window.

32.3 Adding Types

1. To add a new badge type, right-click the **Badge Types** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Badge Types** to display the Add Badge Types dialog box.



2. In the **Badge Type Information tab,** enter a **Description** of the badge type.
3. Design the front and back layout of the badge type:
   a. Click **Design** to display the BadgeDesigner. See Appendix G, Badging, for a description of Badge Designer tools.
   b. Use the **BadgeDesigner** tool bar to compose the badge layouts for front and back. To identify each icon in the toolbar, hold the cursor (without holding the mouse button down) over the icon until a text label appears over the icon. Each icon represents a graphic object; you can customize each object by adjusting its properties (see Appendix G, Badging).
   c. Select a badge orientation from the **Badge Type Orientation** drop-down list: Landscape, Portrait, or Use Registry.
   d. Click the **Partitions** tab and assign a partition if necessary.
   e. Click **OK** to accept the designs and create a new badge type.

32.4 Editing Badge Types

1. To edit an existing badge type, click **Badge Types** to display the profiles in the right pane.
2. Right-click on the badge you want and select **Properties** to display the **Edit Badge Types** dialog box, which is the same as the Add Badge Types dialog box.
3. Edit the **Description** if necessary.
4. Edit **Front Layout** and **Back Layout** design, if necessary.
5. Click the **Partitions** tab and edit the partition assignment if necessary.
6. Click **OK**.

32.5 Viewing Dependencies of a Badge Type

Use this function to view a list of the current dependencies for the selected Badge type. The Badge object is a dependency for a Badge Type.

To view and edit a Badge Type's dependencies:

1. Right-click the icon of an existing **Badge Type** in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** The Dependencies dialog box appears and lists the Badge Type's existing dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

32.6 Copying Badge Types

1. In the Pro-Watch Database Configuration tree list, click the **Badge Types** icon to display all the types in the right pane.
2. Right-click the badge type you want, and select **Copy**.
3. Right-click in a blank area of the main pane.
4. Select **Paste**. A new Badge Type icon appears with the name “Copy of [Badge Type name]”.
5. To rename and edit the new Badge Type, see "Adding Types".

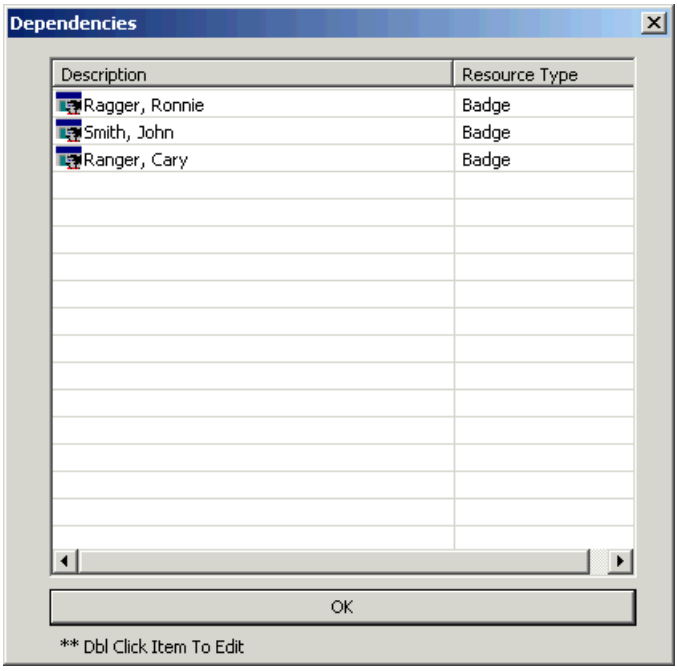
32.7 Deleting Badge Types

To delete a Badge Type from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Badge Types** icon to display all the current types in the right pane.

Note: Right-click the badge type you want to delete, and select **Delete**.

You cannot delete a badge type that has current dependencies. A dependency is another database object that includes the Badge Type in its configuration. The Badge object is a Badge Type dependency. If the badge type has no current dependencies, it is deleted. However, if the badge type does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the badge type:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Click each dependency's Badge Type tab, and click to select the badge type.
   c. Click **Delete/Revoke** to delete the badge type from each dependency's configuration.
3. Repeat step 2 and click **Yes** at the prompt to delete the badge type.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – BLOB Types

33

In this chapter ...

Overview
BLOB Type Functions
Adding or Editing BLOB Types
Viewing Dependencies of a BLOB Type
Partitions and BLOB Types
Viewing Dependencies of a BLOB Type

33.1 Overview

Use this function to define how graphic database items such as images, videos, sound, and even programs or fragments of code will be stored.

These objects are stored collectively as a single entity (a Binary Large Object, or BLOB) in the Pro-Watch database.

For example, a Pro-Watch BLOB can contain a badge type template, a badge picture, or a badge holder's file (job application, security clearance form, and so on).

33.1.1 BLOB Size Limit and Supported Formats

33.1.1.1 Maximum Size

Maximum BLOB size that Pro-Watch supports is approximately 878 KB or 900000 Bytes.

33.1.1.2 Supported Formats

For **Classical Badging**: JPEG, EMF, BMP

For **Advanced Badging**: JPG, PNG, TIF, TIFF, PCX, TGA, BMP, WMF, EMF, PSD, WBMP, GIF, TLA, PCD, JP2, J2K, JPF, JB2, CRW, DCR, NEF, SRF, ORF, PDF, DJVU, DJV

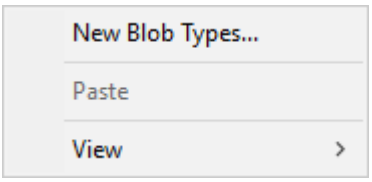
33.2 BLOB Type Functions

To access BLOB type functions:

1. In the Pro-Watch Database Configuration tree list, click the **BLOB Types** icon to display the currently-configured BLOB Types in the right pane of the Pro-Watch window.

Note: Right-click a BLOB type icon to display the pop-up menu. If no BLOB Types have been created yet, right-click anywhere in the right pane.

If no BLOB types have been created yet, this pop-up menu only shows a subset of these functions.



2. Use the following table to select a function
:

Click...	To...
New BLOB Types...	Add a new BLOB type. See "Adding or Editing BLOB Types".
View	Change the way the icons are displayed in the Pro-Watch window.

33.3 Adding or Editing BLOB Types

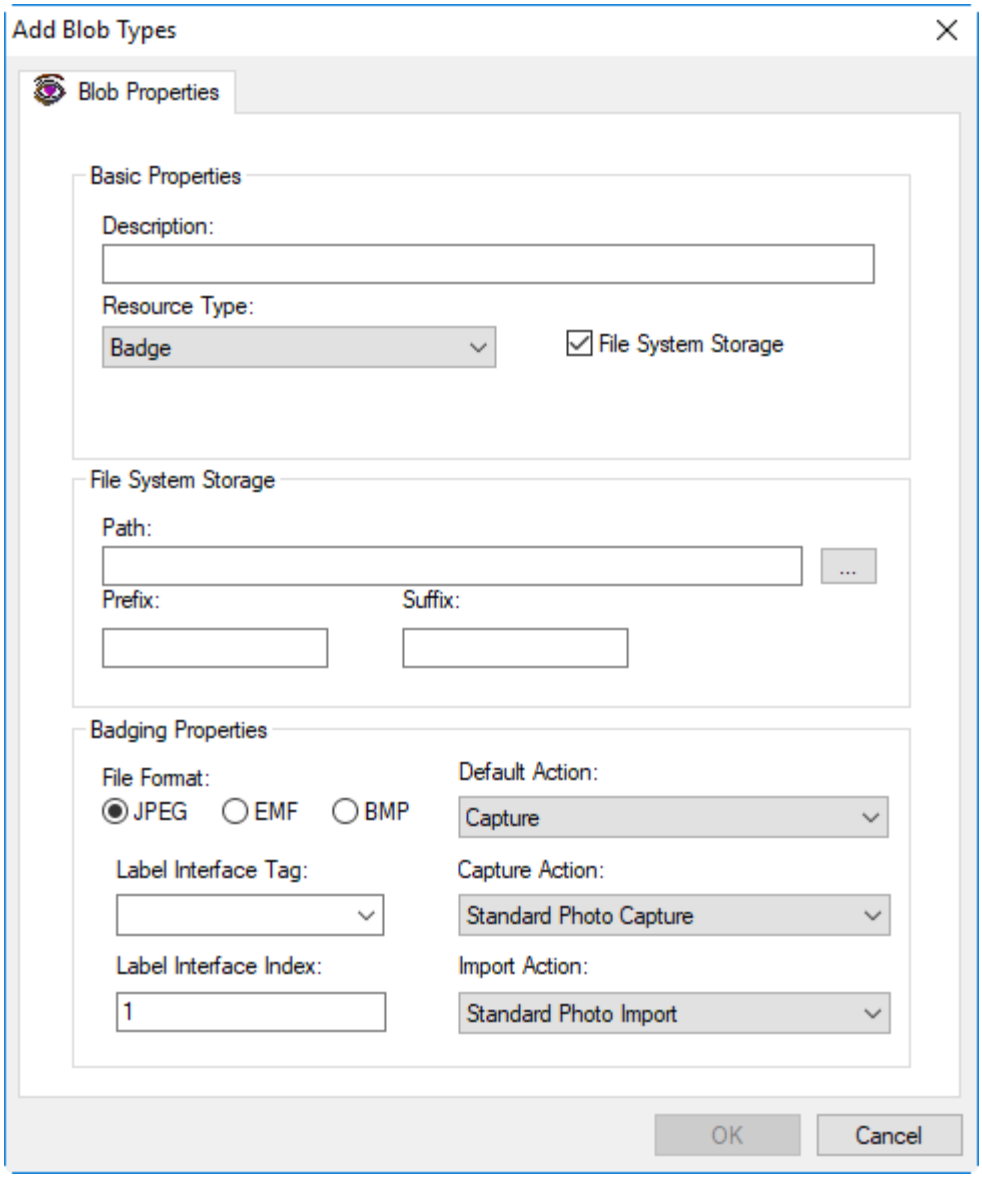
Note: You must first create a shared badges folder on the server for badge layouts, photos, and signatures. In the folder Properties tab, grant full control rights to all users. You may need to select users individually to grant them access. Then, you must be sure to change the path of each BLOB to point to this new folder.

1. To ***add*** a new BLOB type, right-click the **BLOB Types** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New BLOB Types** to display the Add BLOB Types dialog box.

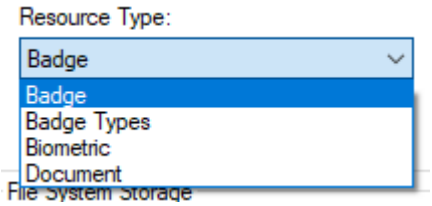
   To ***edit*** an existing BLOB type, click the **BLOB Types** icon to display all the profiles in the right pane. Right-click on the BLOB type you want and select **Properties** to display the Edit BLOB Types dialog box.

   The Add BLOB Types and Edit BLOB Types dialog boxes consist of three categories of information:

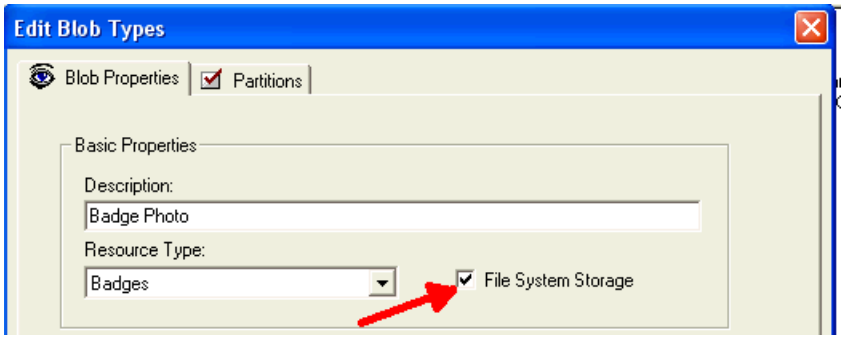
   - Basic properties.
   - File system storage path.
   - Badging properties.



2. Enter a **Description** that identifies the BLOB file.
3. From the **Resource Type** drop-down menu, select the type of resource that will be stored in the BLOB (badges, badge types, biometric, or document):



Note: In the File System Storage check box, indicate whether the BLOB will be stored internally in the Pro-Watch database or in a specified directory.



A badge type BLOB must use the File System Storage. However, you can store badge and document BLOBs in the Pro-Watch database as well as in a File System Storage directory. If you choose to use File System Storage, be sure the directory is accessible to all users with access rights to the BLOB directory.

To store the BLOB in the database, leave the box unchecked. To store the BLOB in a directory, select the box.

4. If you are storing the BLOB in a directory:

   a. Click the browse button (...) next to the Path field and select a path for your stored BLOB file.

   b. Enter a storage file prefix and suffix.

   - If the Resource Type is Badge Type, file prefixes are either front or back; suffixes are LYT. Note that LYT files, or layout files, are special files used by Badge Designer that cannot be stored in the Pro-Watch database.

Note: If the Resource Type is not Badge Type, enter a file prefix for the external storage file and enter the file's format for the suffix. Be sure to make the file name unique; file of the same name will overwrite each other. Alternatively, you can store BLOBs in different locations to avoid overwriting.

- If the Resource Type equals the Badge Type, the prefix is either Front or Back, and the suffix is LYT. Note that LYT files, or layout files, are special fields used by Badge Designer that cannot be stored in the Pro-Watch database.
- For other Resource Types, such as Badges, Documents, or Default Events, enter a file prefix that corresponds in some way to the BLOB description and distinguishes the file from others on the same badge. You can also organize files by specifying different locations for BLOBs stored externally. In this way, you can avoid having a badge's images overwrite each other.
- You can enter suffixes according to the file format for BLOBS other than Badge Types.

- If there is only one image to be stored in the file system storage folder to be placed on the badge, you can omit the prefix and suffix.
- Caution**:** Once you create a file system storage directory path, it is recommended that you do not change the path. A change in the path can cause the card file to lose its image.

5. If you selected either Badges or Document in Step 3, enter the following information in the Badging Properties section:
   - File format – JPEG is normally used for photographs, EMF is used for signatures, and BMP is typically used for graphic images.
   - Label interface tag – this field is used by the Pro-Watch Badge Designer to print photographs and signatures (stored in BLOBs) on cards. If the BLOB contains photograph images, enter Photos. If the BLOB contains signature images, enter Signatures. If you leave this field blank, the photograph or signature will not print onto the card.
   - Label interface index – this field assigns a unique number to identify the BLOB. Enter a unique number between 1 and 99. This number determines the Photo Index in the Photo Object Properties field when you use Badge Designer to design a badge layout.
6. Specify default actions, if you selected Badges for a resource type:
   - Default action – Specifying a default action can simplify the printing of photographs or signatures on a card. You can place images on a card either by capturing and printing the image of the person or by importing images that have already been captured.
     Example: Your enterprise might be set up with the proper camera equipment to capture an employee's photograph and place it in the BLOB when you are creating her card from the badge profile. In this case, select Capture as the default action. Or, if you plan to print images on cards by importing an already-taken photograph into the BLOB, select Import as the default action. Or, if you expect to use the BLOB for both capture or import, select None.
   - Capture action – If you specified a Capture default action, select Standard Photo Capture (if the file format is JPEG) or Standard Signature Capture (if the file format is EMF or BMP). Select **None** if you did not specify a Capture default action.
   - Import action – If you specified an Import default action, select Standard Photo Import (if the file format is JPEG) or Standard Signature Import (if the file format is EMF or BMP). Select None if you did not specify an Import default action.
7. Click **OK** to accept the BLOB file properties.

33.4 Viewing Dependencies of a BLOB Type

A BLOB Type can be dependent upon other resources. For example, a badge type could be a dependency on a BLOB Type.

To view and edit ***a BLOB Type's dependencies****:*

1. Right-click the icon of an existing BLOB type in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** The Dependencies dialog box appears and lists the BLOB Type's existing dependencies.
2. To edit or delete a dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

33.5 Partitions and BLOB Types

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition.

To assign or delete an already-created partition to the BLOB type:

1. To assign a partition to the BLOB type, click **Add** to display the Available Partitions dialog box.
2. Select the partition you want and click **Add**.

To delete a partition from the Partitions List dialog box, select the partition and click **Delete**.

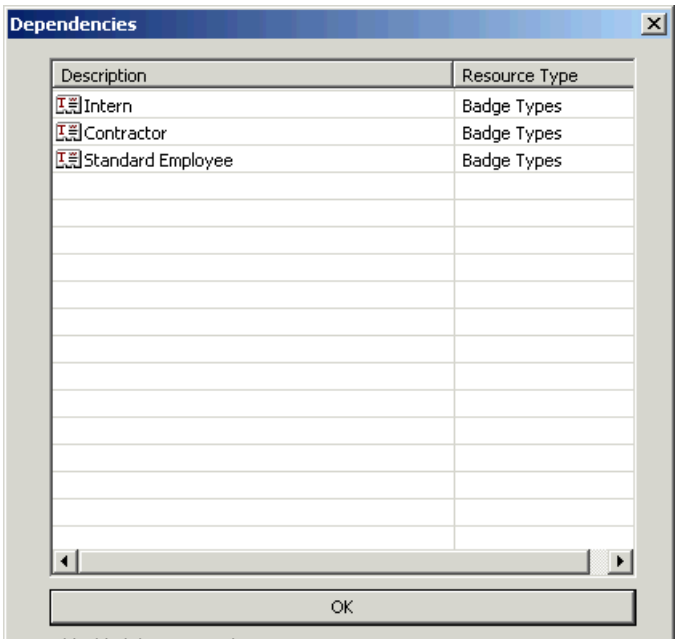
33.6 Deleting BLOB Types

To delete a BLOB Type from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **BLOB Types** icon to display all the current types in the right pane.

Note: Right-click the BLOB type you want to delete and select **Delete**.

You cannot delete a BLOB type that has current dependencies. A dependency is another database object that includes the BLOB Type in its configuration. The Badge Type object is a BLOB dependency. If the BLOB type has no current dependencies, you are prompted to confirm the deletion. However, if the BLOB type does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the BLOB type:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display the dependency's Edit [object name] dialog box.
   b. Use the drop-down lists to select either a different badge type or **None** for each BLOB type.
3. Repeat step 2 and click **Yes** at the prompt to delete the BLOB type.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Brass Keys

34

In this chapter ...

Overview

Brass Keys Functions

Adding or Editing Brass Keys

Viewing Dependencies of a Brass Key

Partitions and Brass Keys

Deleting a Brass Key

34.1 Overview

Use this function to monitor the assignments of physical keys. This function enters a key description into a form; once in the form, the key can be assigned to a badge holder.

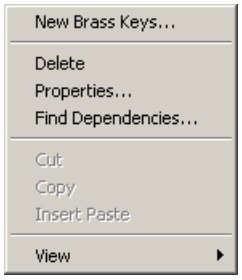
Tasks for this function include:

- Adding a brass key.
- Deleting a brass key.
- Modifying a brass key.

34.2 Brass Keys Functions

To access Brass Keys functions:

1. In the Pro-Watch Database Configuration tree list, click the **Brass Keys icon** to display the currently-configured Brass Keys in the right pane of the Pro-Watch window.
2. Right-click a brass key icon to display the pop-up menu (if no Brass Keys have been created yet, right-click anywhere in the right pane). Note that if no brass keys have been created yet, this pop-up menu only shows a subset of these functions.



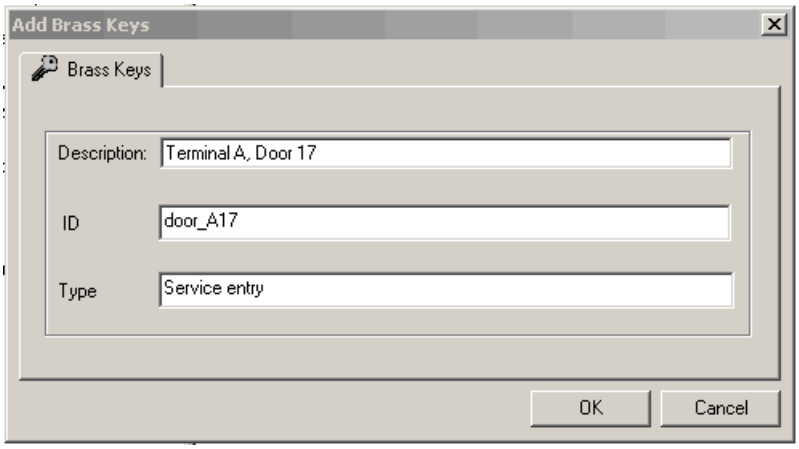
3. Use the following table to select a function:

Click...	To...
New Brass Keys...	Add a new brass key. See "Adding or Editing Brass Keys".
Delete	Delete a current brass key. See "Viewing Dependencies of a Brass Key".
Properties...	Edit a current brass key configuration. See "Adding or Editing Brass Keys".
Find Dependencies...	Display the names of all resources that depend upon or use the brass key. See "Viewing Dependencies of a Brass Key"
View	Change the way the icons are displayed in the Pro-Watch window.

34.3 Adding or Editing Brass Keys

1. To add a new brass key, right-click the **Brass Keys** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Brass Keys** to display the Add Brass Keys dialog box.

   To edit an existing brass key, click the **Brass Keys** icon to display all the profiles in the right pane. Right-click the brass key you want and select **Properties** to display the Edit Brass Keys dialog box.



2. In the **Description** field, enter a description that clearly identifies the key.
3. Enter a unique string that identifies the key.
4. Enter the type of entry point associated with the key.
5. Click **OK** to complete the new Brass Key.

34.4 Viewing Dependencies of a Brass Key

Use this function to view a list of the Brass Key dependencies. A brass key can be dependent upon other resources.

Example: A Badge object depends upon a Brass Key.

To view and edit ***a Brass Key's dependencies****:*

1. Right-click the icon of an existing **brass key** in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** The Dependencies dialog box appears and lists the Brass Key's current dependencies.
2. To edit or delete a dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

34.5 Partitions and Brass Keys

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition.

Use this function to create, assign or delete a partition:

To create a partition for the brass key:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want. See "DBC - Partitions" in Chapter 53 for an explanation of partitions.
3. Click **OK** to accept the partition.

To assign a partition to the brass key:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want.
3. Click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

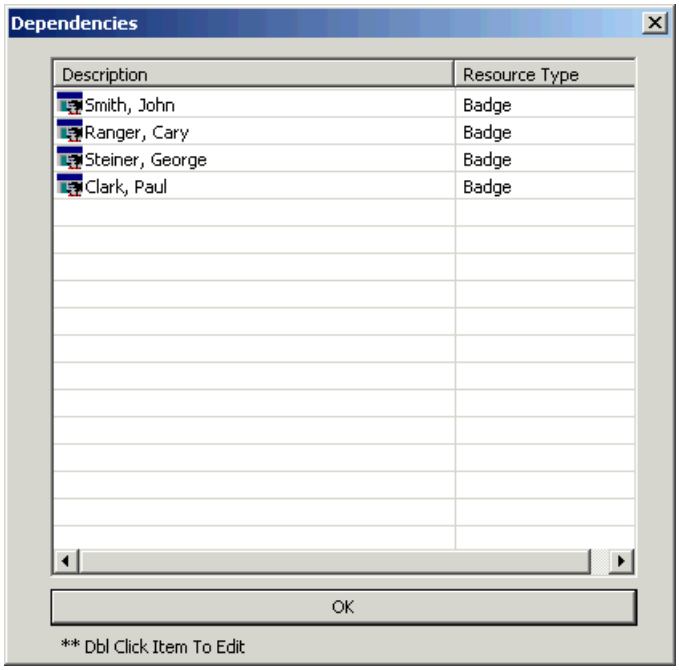
34.6 Deleting a Brass Key

To delete a Brass Key from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **brass keys** icon to display all the current Brass Keys in the right pane.

Note: Right-click the brass key you want to delete and select **Delete**.

You cannot delete a brass key that has current dependencies.A dependency is another database object that includes the Brass Key in its configuration. For example, the Badge object is the Brass Key dependency. If the brass key has no current dependencies, you are prompted to confirm the deletion. However, if the brass key does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the brass key:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the badge holders listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Brass Key.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Card Formats

35

In this chapter ...

Overview

Card Format Functions

Adding or Editing a Card Format

Viewing Dependencies of a Card Format

Copying a Card Format

Partitions and Card Formats

Deleting a Card Format

35.1 Overview

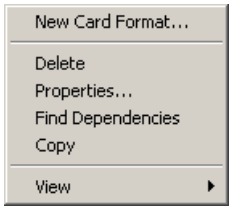
A Pro-Watch card defines specific access privileges for the badge holder. Use this function to configure the card formats that will be used to create your cards.

Card formats must be configured before cards can be read at card readers. The format of a card must match the format that is programmed into the Pro-Watch equipment. Pro-Watch supports a variety of card formats and comes preconfigured with four Weigand, two magnetic stripe card and an OmiSmart 64-bit card formats.

35.2 Card Format Functions

To access the card format functions:

1. In the Pro-Watch Database Configuration tree list, click the **Card Formats** icon to display the currently-configured Card Formats in the right pane of the Pro-Watch window.
2. Right-click a card format icon to display the pop-up menu (if no Card Formats have been created yet, right-click anywhere in the right pane). Note that if no card formats have been created yet, this pop-up menu only shows a subset of these functions.

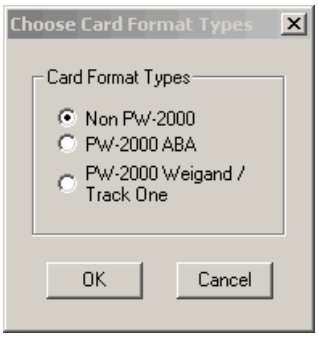


3. Use the following table to select a function:

Click...	To...
New Card Formats...	Add a new card format. See "Adding or Editing a Card Format".
Delete	Delete a current card format. See "Viewing Dependencies of a Card Format".
Properties...	Edit a current card format configuration. See "Adding or Editing a Card Format".
Find Dependencies...	Display the names of all resources that depend upon the card format. See "Viewing Dependencies of a Card Format".
Copy	Copies a card format. See "Copying a Card Format".
View	Change the way the icons are displayed in the Pro-Watch window.

35.3 Adding or Editing a Card Format

1. To **add** a new card format, right-click the **Card Formats icon** in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Card Formats** to display the Choose Card Format Types dialog box. Note that Pro-Watch comes with preconfigured Card Formats. If your installation requires a different Card Format, please consult with your installer for the proper settings.



2. Select the desired format, and click **OK** to display the Add Card Formats dialog box.
3. To **edit** an existing card format:
   a. Click **Card Formats** to display the profiles in the right pane.
   b. Right-click on the card format you want and click **Properties** to display the Edit Card Formats dialog box.

Note: There are three forms of the Add Card Formats dialog box and Edit Card Formats dialog box – one form for each of the possible different card formats.

CARD FORMATS TABS LIST

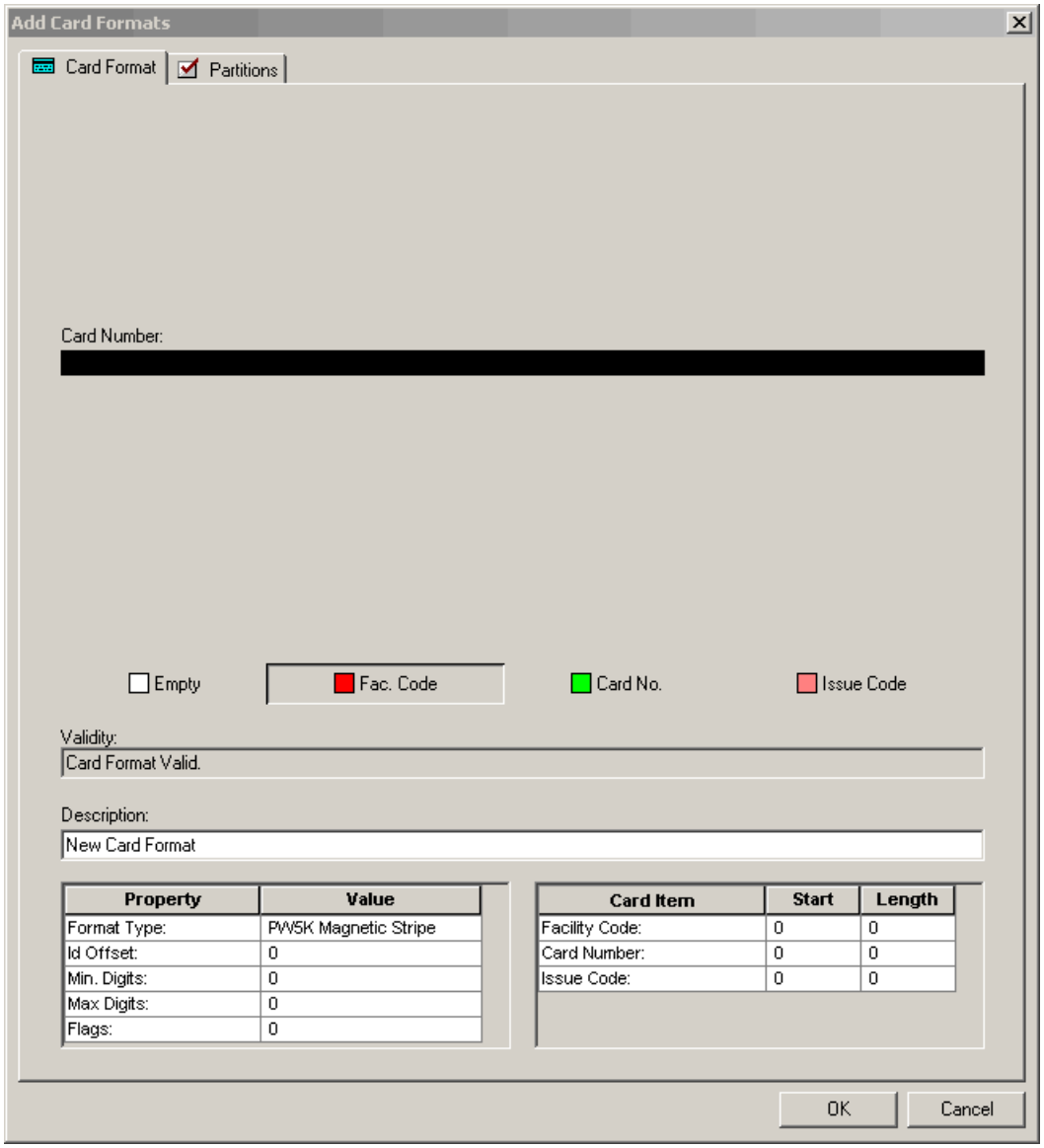
To complete the card format configuration, click the section header listed below that is appropriate for the particular panel you are using:

- "Adding or Editing a Non PW2000 Card Format".

- "Adding or Editing a PW2000 ABA Format".
- "Adding or Editing a PW2000 Weigand/Tack One Format".

35.3.1 Adding or Editing a Non PW2000 Card Format

1. Click the **Non PW2000** option button and **OK** to display the **Add Card Formats** screen:



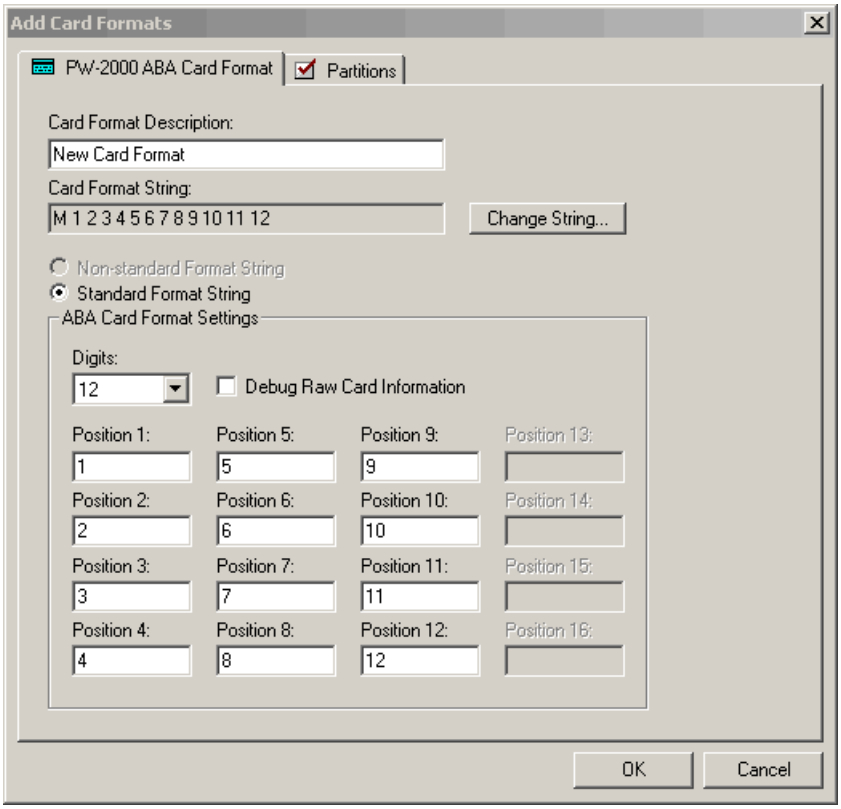
2. Use the following field descriptions to configure the card format:

Field	Description
Card Number	Displays a graphic representation of the bit layout of the Card Format you are configuring. You can change the values displayed by modifying the values in the Property and Value fields and the Card Item Start and Length fields.
Fac. Code	Identifies the facility where the card will be used.
Card No.	Specifies a unique card number.
Issue Code	Identifies the card's issue number. For example, if a badge holder loses his card and is reissued another, the second card's issue code indicates that it is the second issue. In this example, the first-issued card would no longer be valid.
Validity	Indicates whether the card format as designed is valid.
Description	Identifies the format for you and your organization.
Format Type	Specifies the format to be used for the card. Click in the Value field and select one of the following formats from the drop-down list: • PW5 Magnetic Stripe • PW5K Wiegand • SEEP ABA • CHIP ABA • CHIP Wiegand • CHIP Wiegand Raw The card format you select must match the format that is programmed into your hardware. Note that if you will be configuring a PW-6000 panel with S-Net readers, you must create a Card Format with the PW5K Wiegand format type. See "Reader Settings Tab" on page 41 for instructions.
ID Offset	Concatenates a number with the original card number to ensure the card number is unique. **Example:** An enterprise may have two facilities in different geographical locations. If their card numbering is local, duplicate card numbers are possible. This is a PW-5000 option only.

Field	Description
Min. Digits	Specifies the minimum number of digits in the magnetic stripe.
Max. Digits	Specifies the maximum number of digits in the magnetic stripe.
Flags	Specifies one of four possible forms of card number calculation. Enter a flag number 1, 2, 3, or 6: 1 – Uses two-bit parity calculation. 2 – Suppresses facility code checking. 3 – Combines flags 1 and 2. 6 – Uses the corporate card format. This option multiplies the ID offset by the facility code, and adds the sum to the read card number to produce the effective card number.

35.3.2 Adding or Editing a PW2000 ABA Format

1. Click the **PW2000 ABA option button** and **OK** to display the Add Card Formats screen:



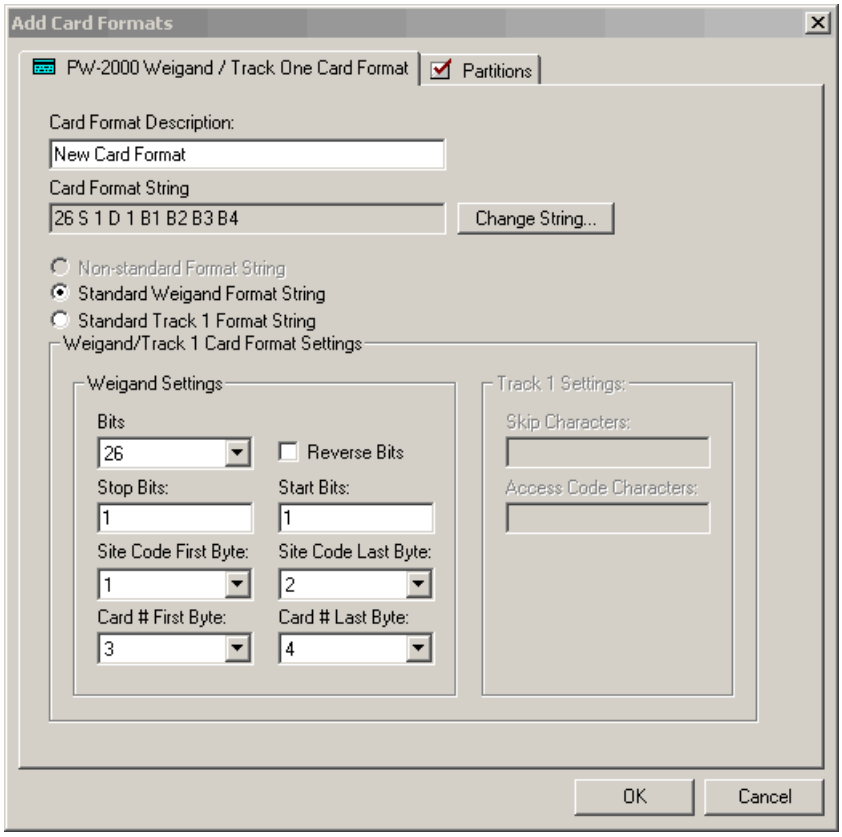
2. Use the following field descriptions to complete the card format:

Field	Description
Card Format Description	Names the card format.
Format String	Specifies PW2000 Mag Stripe.
Digits	Specifies the number of digits that will be in the format string.
Debug Raw Card Information	Outputs raw card data that can be used to program the card format.
Position	Specifies the numerical position of the digit in the format string.

3. Click to accept the new card format.

35.3.3 Adding or Editing a PW2000 Weigand/Tack One Format

1. Click the **PW2000 Weigand/Track One** option button and to display the Add Card Formats screen:


Add Card Formats
PW-2000 Weigand / Track One Card Format
Partitions
Card Format Description:
New Card Format
Card Format String
26 S 1 D 1 B1 B2 B3 B4
Change String...
Non-standard Format String
Standard Weigand Format String
Standard Track 1 Format String
Weigand/Track 1 Card Format Settings
Weigand Settings
Bits
26
Reverse Bits
Stop Bits:
1
Start Bits:
1
Site Code First Byte:
1
Site Code Last Byte:
2
Card # First Byte:
3
Card # Last Byte:
4
Track 1 Settings:
Skip Characters:
Access Code Characters:
OK
Cancel

2. Use the following field descriptions to complete the card format:

Field	Description
Card Format Description	Names the card format uniquely.
Format String	Specifies the PW2000 Weigand format.
Bits	Specifies the number of bits that will be read from the card.
Reverse Bits	Displays the read bits in reverse when reading.
Stop Bits	Specifies the number of stop bits.
Start Bits	Specifies the number of start bits.
Site Code First Byte	Specifies where the site code starts.
Site Code Last Byte	Specifies where the site code ends.
Card # First Byte	Specifies where the card number starts.
Card # Last Byte	Specifies where the card number ends.

3. Click to accept the new card format.

35.4 Viewing Dependencies of a Card Format

Use this function to view a list of a Card Format's dependencies. The Panel and Hardware Template objects are Card Format dependencies.

To view and edit ***a Card Format's dependencies****:*

1. Right-click the icon of an existing card format in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the existing dependencies for the Card Format.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click to close the dialog box.

35.5 Copying a Card Format

Use this function to copy the configuration of a card format and place the copy's icon in the right pane of the window.

1. In the Pro-Watch Database Configuration tree list, click the **Card Formats icon** to display the icons of all the current card formats in the right pane.
2. Right-click the format you want, and select **Copy**.
3. Right-click in a blank area of the main pane.
4. Select **Paste**. A new Card Format icon appears with the name "Copy of [Card Format name]".
5. To rename and edit the new Card Format, see "Adding or Editing a Card Format".

35.6 Partitions and Card Formats

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the card format:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want. See "DBC - Partitions" in Chapter 53 for an explanation of partitions.
3. Click to accept the partition.

To assign a partition to the card format:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click Delete.

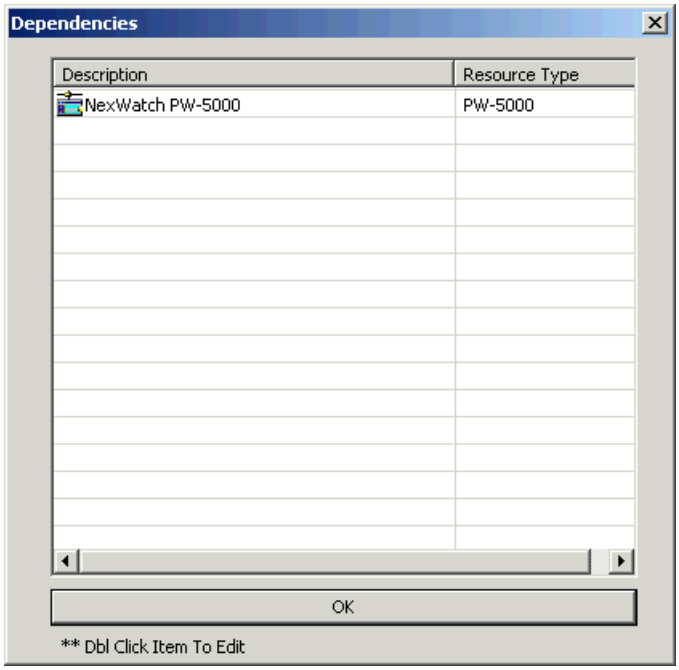
35.7 Deleting a Card Format

Use this function to delete a card format from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Card Formats** icon to display the icons of all the current formats in the right pane.

Note: Right-click the card format you want to delete and select **Delete**.

You cannot delete either a system card format or any card format that has current dependencies. A dependency is another database object that includes the Card Format in its configuration. The Panel and Hardware Template objects are Card Format dependencies. If the card format has no current dependencies, you are prompted to confirm the deletion. However, if the card format does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the card format:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the card format.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Classes

36

In this chapter ...

Overview

Class Functions

Adding or Editing a Class

Viewing Dependencies of a Class

Copying a Class

Deleting a Class

36.1 Overview

Use this function to create and maintain classes to which Pro-Watch privileges can be assigned.

Classes are defined in relation to the workstations as well as individuals. When you assign a class, any database entity assigned to that class receives the privileges configured for the class. You can assign the following database entities to a class:

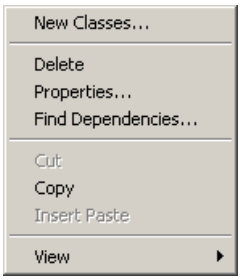
- Programs.
- Workstations.
- Routing groups.
- Alarm pages.
- Keystroke accelerators.
- Event toolbars.
- Partitions.
- Badge profiles.
- Event procedures.
- Eventview columns.

The user can add a new class or edit an existing one, delete a class, create a copy of a class, and view the class icons.

36.2 Class Functions

To access Classes functions:

1. In the Pro-Watch Database Configuration tree list, click the **Classes** icon to display the currently-configured areas in the right pane of the Pro-Watch window.
2. Right-click any area icon to display the pop-up menu:



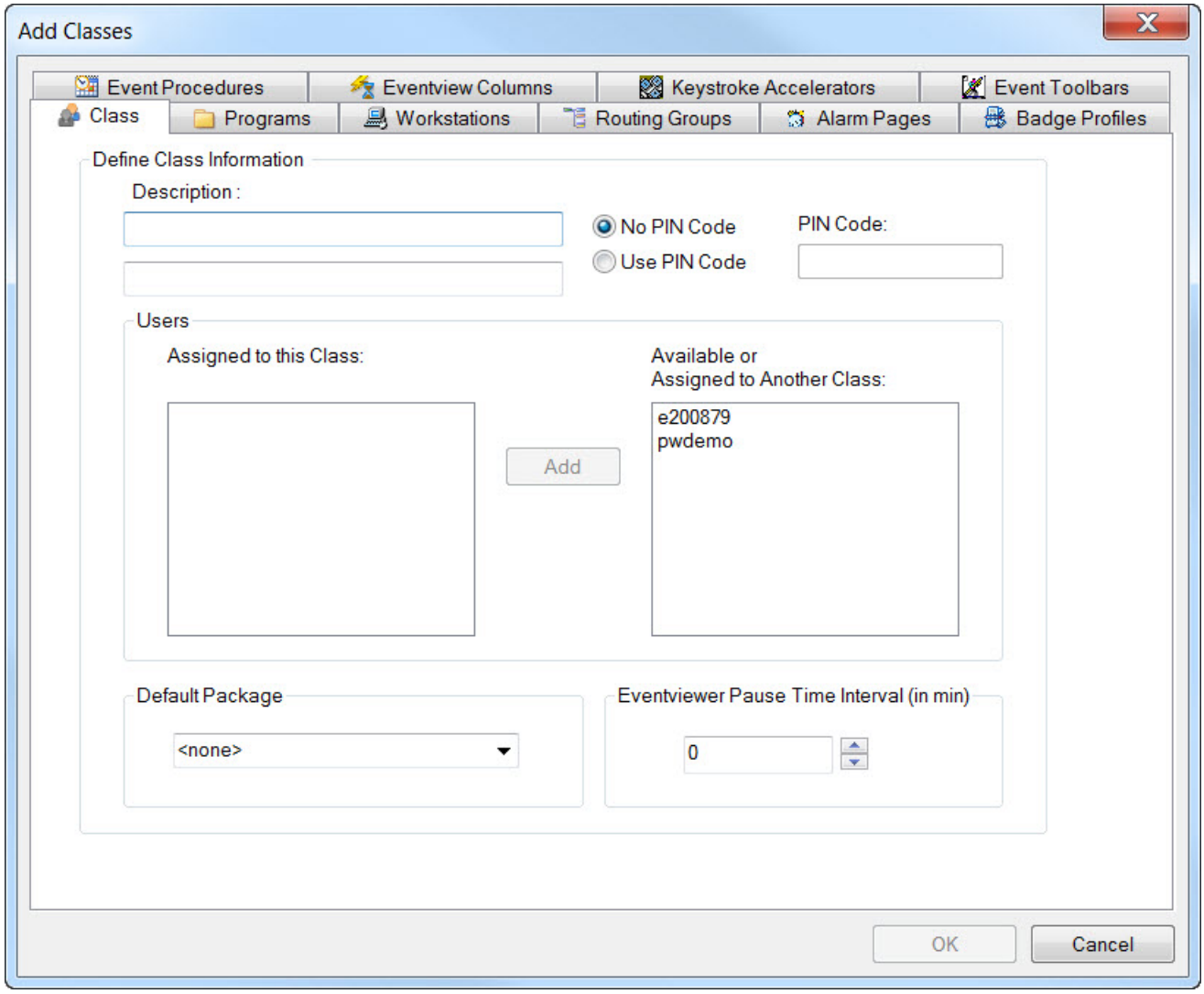
3. Use the following table to select a function:

Click...	To...
New Classes...	Add a new class. See "Adding or Editing a Class".
Delete	Delete a current class. See "Adding or Editing a Class".
Properties...	Edit a current class configuration. See "Adding or Editing a Class".
Find Dependencies...	Display the names of all resources that depend upon the class. See "Viewing Dependencies of a Class".
Copy	Create a copy of the class configuration and insert the new class icon in the right pane. See "Adding or Editing a Class".
View	Change the way the icons are displayed in the Pro-Watch window. See "Adding or Editing a Class".

36.3 Adding or Editing a Class

*To **add** or edit a class:*

1. To add a class, right-click the **Classes** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane of the Pro-Watch window), and select **New Classes**. The Add Classes dialog box appears:



2. To **edit** an existing class, right-click the class icon in the right pane of the Pro-Watch window and click **Properties**. The Edit Classes dialog box appears.
3. Complete the following tab sections to configure the class.

CLASS TABS LIST

- "Class Tab".
- "Programs Tab".
- "Workstations Tab".
- "Routing Groups Tab".
- "Alarm Pages Tab".
- "Badge Profiles Tab".
- "Event Procedures Tab".
- "Keystroke Accelerators Tab".
- "Eventview Columns Tab".
- "Event Toolbars Tab".
- "Partitions Tab".

36.3.1 Class Tab

Use the following field definitions to complete the Class tab in the Add Classes dialog box:

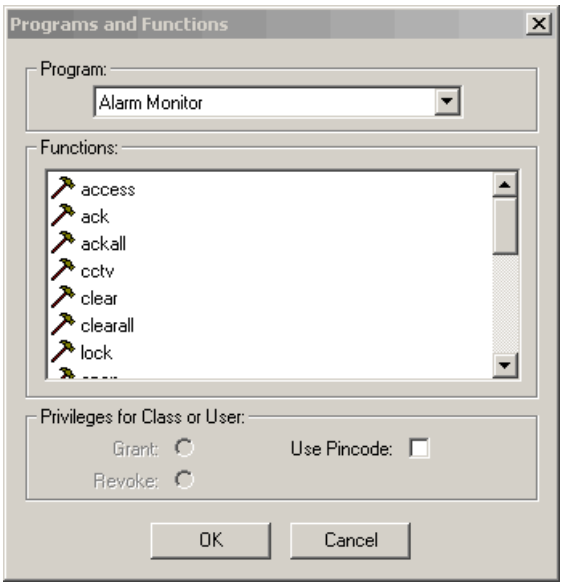
Field	Description
Description	Names the class you want to add or edit.
PIN Code	Specifies a PIN identification code for the class. Select either No PIN Code or Use PIN Code. If you select Use PIN Code, enter the code.
Users	Selects the users (by their system user ID) who will be assigned to the class. In the Available box, click to select the user(s) you want to assign to the selected class, then click **Add** to assign them.

36.3.2 Programs Tab

Click the **Programs** tab to display the Define User Programs and Functions dialog box. The Program folder displays the existing programs to which the class has access.

To add a program:

1. Click **Add Program** to display the Programs and Functions dialog box.



2. From the Program drop-down list, select the programs to which you want the class to have access. The available functions for the selected program appear in the Functions list box. See Appendix B, Assignable Programs, for a description of each program's available functions.
3. Click the functions for which you want to give the class access. Use **CTRL-click** to select more than one function.
4. Select the **Use Pincode** check box if you want the user to supply the class PIN code (if you created one on the Class tab) to access the command.
5. Click to set the Program property.

To edit a program:

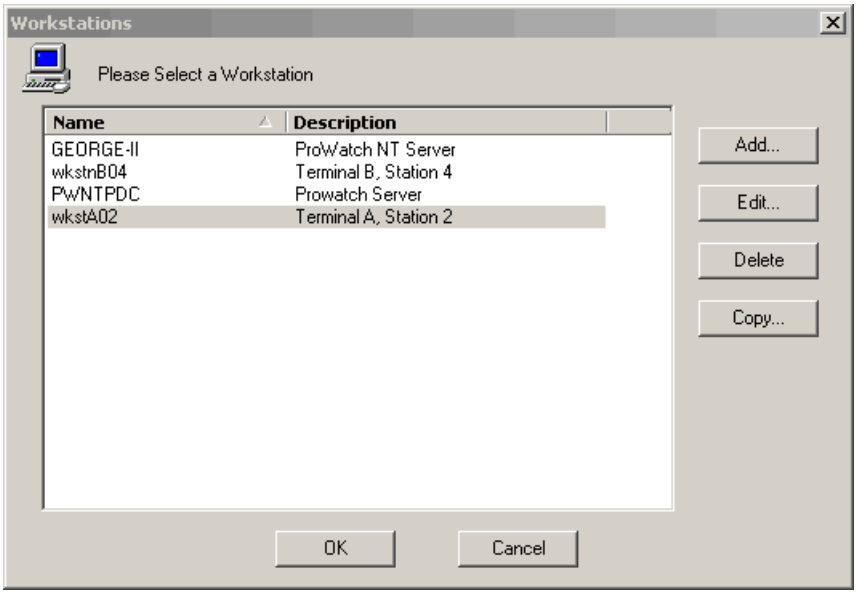
1. Select a program listed in the Define User Programs and Functions dialog box.
2. Click **Edit** to display the Programs and Functions dialog box.
3. Make the necessary changes and click **OK**.

36.3.3 Workstations Tab

Click the **Workstations** tab to display the Define User dialog box.

To add a workstation to a class:

1. Click **Add** to add class access to a workstation. The Workstations dialog box appears.



2. Click the workstation you want to add, and then click **OK**. The workstation is added to the class.

   If the workstation you want does not appear in the list of workstations, click **Add** on the Workstations dialog box to display the Add Workstations dialog box. See "DBC - Workstations" in Chapter 59 for instructions on completing the Add Workstations dialog box.

To edit a class's workstation configuration:

- Select the workstation in the Edit Workstations dialog box, and click **Edit** to display the Define User, Workstations, or Edit Workstations dialog box and modify the workstation's configuration. See "DBC - Workstations" in Chapter 59 for instructions on modifying the workstation's configuration.

To delete a workstation from the class:

1. Click **Delete** on the Define User or Workstations dialog boxes.
2. Click **OK** to complete the deletion.

36.3.4 Routing Groups Tab

A routing group is a group of defined resource types for which events are published. These resource types include channels, event types, rollover

event types, and workstations. When you assign a class of users to a routing group, the group's events are routed to all users in the class.

The routing groups listed in this tab are already assigned to the class. From here, you can either add new routing groups, modify current groups, or delete current groups.

1. To assign a new routing group to the class, click **Add** to display the Routing Groups dialog box. This dialog box lists all created routing groups available for assignment. From here you can:
   - Click a listed routing group and then click **OK** to assign the group to the class.
   - Create a new routing group. To create a new group, click **Add**, enter a routing group name in the Description field, and click **OK**. The new group is now available on the Routing Groups dialog box.
   - Assign the new group to the class by clicking the new group, and then clicking **OK**. Then, proceed with instructions to configure the routing group in step 2.
2. To edit a routing group already assigned to the class:
   a. Click to select the group and click **Edit** to display the Resources dialog box. The dialog box lists the four routing group resource types.
   b. Click the resource you want to define and click **Add**. The Define Route Group Resource dialog box appears.
   c. Click the button next to the Resource field, and then click **Define** to select a particular resource.
   d. Click **OK** to accept the resource as it is currently configured, or click **Edit** and re-configure the resource. Then, click **OK** to accept the resource.
   e. Click the button next to the TimeZone field, and then click **Define**. Select the time zone you want and click **OK**.
   f. Select **Acknowledge** and/or **Clear** to receive both acknowledge and clear alarms.
   g. Click **OK** to accept the resource definition. Select and configure another resource on the Resources dialog box, if you desire.

36.3.5 Alarm Pages Tab

The alarm page tab displays Pro-Watch alarm information that is assigned to the class, including alarm page names, default maps, associated events, categories (column heads) of the information displayed, and configured partitions.

Refer to "Overview" to complete the following alarm page format tabs:

- Alarm page information.

- Alarm page event types.
- Alarm page columns.
- Alarm page partitions.

36.3.6 Badge Profiles Tab

The Badge Profiles tab displays the badge profiles that are currently assigned to the current class. All badge profiles must be assigned to at least one class or user before you can use them to create badges.

To assign a badge profile to a class:

1. From the Badge Profiles tab, click **Add** to display the Badge Profiles dialog box.
2. Click to select a currently-configured badge profile, and then click **OK**. Or, optionally, create a new badge profile by clicking **Add** at the Badge Profiles dialog box, create the profile in the Add Badge Profiles dialog box and click **OK**. See "DBC - Badge Profiles" in Chapter 30 for more information about creating badge profiles.

Note: If you assign more than one badge profile to a class, the person who will be using the Badging utility to issue badges will choose from the list of badge profiles that you assign here.

36.3.7 Event Procedures Tab

The Event Procedures tab displays the event procedures that are already assigned to the current class. All event procedures must be assigned to at least one class or user before you can use them.

To assign an event procedure to a class, follow these steps:

1. From the Event Procedures tab, click **Add** to display the Event Procedures dialog box.
2. Click to select a currently-configured event procedure, and then click **OK**.
   Or, optionally, create a new event procedure by clicking **Add** at the Event Procedures dialog box. Then create an event procedure in the Add Event Procedures dialog box and click **OK**. See "DBC - Event Procedures" in Chapter 43 for more information about creating event procedures.

36.3.8 Keystroke Accelerators Tab

The Keystroke Accelerators tab displays the keystroke accelerators that are already assigned to the current class. All keystroke accelerators must be assigned to at least one class or user before you can use them.

To assign a keystroke accelerator to a class:

1. From the Keystroke Accelerator tab, click **Add** to display the Keystroke Accelerators dialog box.
2. Click to select a currently-configured keystroke accelerator, and then click **OK**. Or, optionally, create a new keystroke accelerator by clicking **Add** at the Keystroke Accelerators dialog box. Then create a keystroke accelerator in the Add Keystroke Accelerator dialog box and click **OK**. See "DBC - Keyboard Accelerator" in Chapter 50 for more information about creating keystroke accelerators.

36.3.9 Eventview Columns Tab

The Eventview Columns tab displays the event viewer columns that are already assigned to the current class. Event viewer columns customize the user's view of events. All event viewer columns must be assigned to at least one class before you can use them.

To assign an eventview column to a class:

1. In the Available Columns box on the Eventview Columns tab, click the column you want to assign to the current class.
2. Click the right (east) arrow to move the column to the Current Columns box.
3. Click **OK**.

To edit or delete an eventview column:

- Click to select the eventview column and click **Edit** or **Delete**.

36.3.10 Event Toolbars Tab

The Event Toolbars tab displays the event toolbars that are already configured for the current class. An event toolbar customizes the user's toolbar access to commands from inside of the event viewer window. All event toolbars must be assigned to at least one class or user before you can use them.

To assign a command or event to the toolbar for a class:

1. From the Event Toolbars tab, click **Add Command** or **Add Event** to display the Toolbar Maintenance dialog box.
2. Click the browse button next to the Command or Event field to select a command or event.
3. Select a bitmap icon file to represent the command or event on the toolbar. Note that the icon image appears next to the field after you select the file.

4. Click **OK**.

36.3.11 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the class:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want. See "DBC - Partitions" in Chapter 53 for an explanation of partitions.
3. Click **OK** to accept the partition.

To assign a partition to the class:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

36.4 Viewing Dependencies of a Class

Use this function to view a list of the Class's current dependencies. The User object is the Class's dependency.

To view and edit ***a Class's dependencies****:*

1. Right-click the icon of an existing class in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the existing dependencies for the Class.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

36.5 Copying a Class

Use this function to copy the configuration of a class and place the copy's icon in the right pane of the window.

1. In the Pro-Watch Database Configuration tree list, click the **Classes** icon to display the icons of all the current classes in the right pane.
2. Right-click the class you want, and select **Copy**.
3. Right-click in a blank area of the main pane.
4. Select **Paste**. A new class icon appears with the name "Copy of [class name]".
5. To rename and edit the new class, see "Adding or Editing a Class".

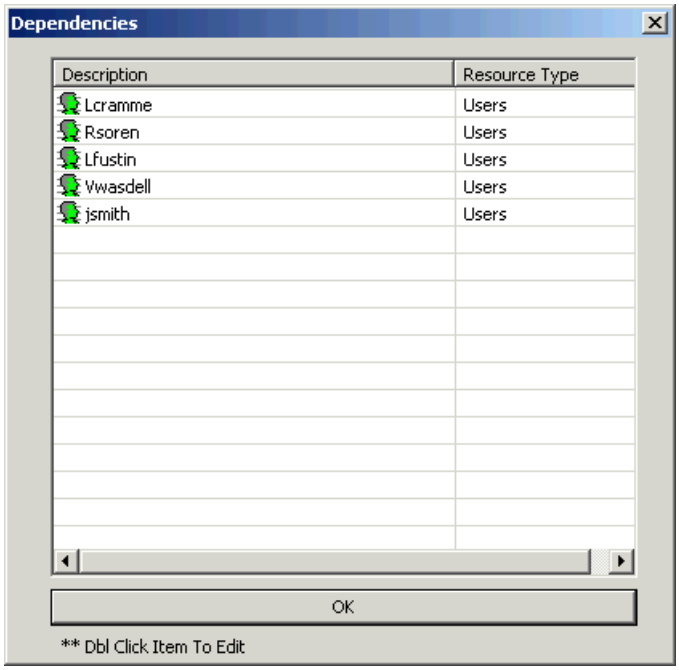
36.6 Deleting a Class

Use this function to delete a class from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Classes** icon to display the icons of all the current classes in the right pane.

Note: Right-click the class you want to delete and select **Delete**.

You cannot delete a class that has current dependencies. The User object is a Class dependency. If the class has no current dependencies, you are prompted to confirm the deletion. However, if the class does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the class:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the class.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Clearance Codes

37

In this chapter ...

Overview

Clearance Codes Functions

Adding or Editing Clearance Codes

Viewing Dependencies of a Clearance Code

Viewing Dependencies of a Clearance Code

Copying a Clearance Code

Clearance Codes and Code of Federal Regulations (21 CFR 11)

Deleting a Clearance Code

37.1 Overview

Clearance codes are tracked to comply with Title 21 of the **Code of Federal Regulations, Part 11** (21 CFR 11). See "Clearance Codes and Code of Federal Regulations (21 CFR 11)" for more information.

Use this function to create, edit, copy or delete a clearance code. A clearance code grants or denies badge holder access to certain enterprise doors and elevators. In addition, you can define temporary clearance codes that are valid for a given number of days to support contractor work at your facilities, for example.

Pro-Watch comes configured with a Primary clearance code**,** with which you can create as many clearance codes as your enterprise requires.

Note: 21 CFR 11 does not work with Application Login.

37.1.1 Limitation

A maximum of 300 clearance codes can be assigned to a single card. Going beyond this limit affects stability while selecting badge holder.

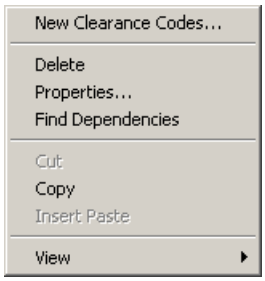
37.2 Clearance Codes Functions

To access Clearance Codes functions:

1. In the Pro-Watch Database Configuration tree list, click the **Clearance Codes icon** to display the currently-configured clearance codes in the right pane of the Pro-Watch window.

Note: Right-click a clearance code icon to display the pop-up menu (if no clearance codes have been created yet, right-click anywhere in the right pane).

If no clearance codes have been created yet, this pop-up menu only shows a subset of these functions:



2. Use the following table to select a function:

Click...	To...
New Clearance Codes...	Add a new clearance code. "Adding or Editing Clearance Codes".
Delete	Delete a current clearance code. "Viewing Dependencies of a Clearance Code".
Properties...	Edit a current clearance code configuration. "Adding or Editing Clearance Codes".
Find Dependencies...	Display the names of all resources that depend upon the clearance code. See "Viewing Dependencies of a Clearance Code".
Copy	Copy a clearance code and insert the new icon in the Pro-Watch window. "Copying a Clearance Code".
View	Change the way the icons are displayed in the Pro-Watch window.

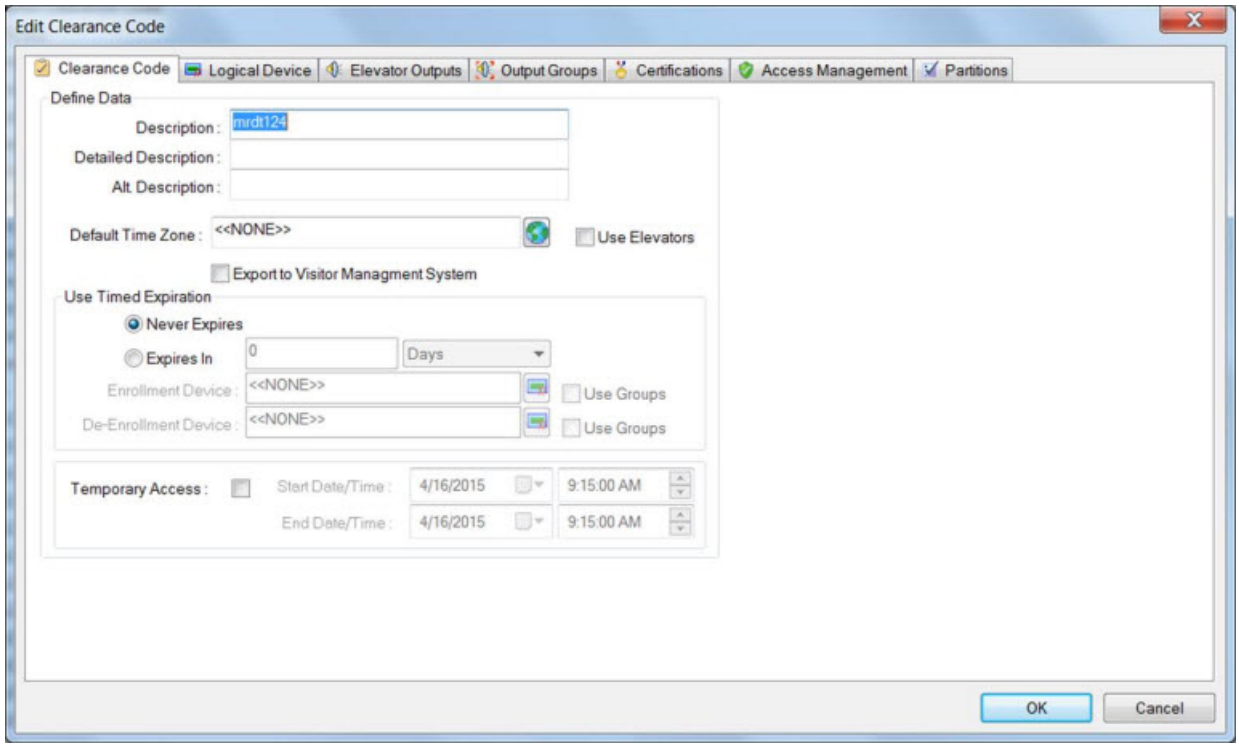
37.3 Adding or Editing Clearance Codes

Note: The Pro-Watch tracks the clearance codes during adding and editing to comply with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11). See "Clearance Codes and Code of Federal Regulations (21 CFR 11)" for more information.

Note: 21 CFR 11 does not work with Application Login.

1. To ***add*** a new clearance code, right-click the **Clearance Codes** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Clearance Codes** to display the Add Clearance Code dialog box.

   To ***edit*** an existing clearance code, click the **Clearance Codes** icon to display the profiles in the right pane. Right-click on the clearance code you want and select **Properties** to display the Edit Clearance Code dialog box.



2. Complete the following tab sections to configure the clearance code:

   CLEARANCE CODE TABS LIST

   - **"Clearance Code Tab".**
   - **"Logical Devices Tab".**
   - **"Elevator Outputs Tab".**

- "Output Groups Tab".
- "Certifications Tab"
- "Access Management Tab"
- "Certifications Tab".

37.3.1 Clearance Code Tab

Use the following field definitions to complete the Clearance Code tab in the Add Clearance Code or Edit Clearance code dialog box:

Field	Description
Description	Name the clearance code.
Detailed Description	Detailed description of the clearance code.
Alt Description	Alternative description of the clearance code.
Default Time Zone	Specifies the default time period during which this clearance code is operative. If the time zone is not available on that panel, Pro-Watch prompts you to select one that is available.
Use Elevators	Creates a clearance code for elevators. This option requires a PW2000, PW-5000, or CHIP panel. When you check the Use Elevators, the elevator readers are displayed in the Logical Devices tab.
Export to Visitor Management System	Exports the clearance code to the LobbyWorks visitor management system.

Field	Description
Use Timed Expiration	Specifies a timed clearance code (CC), which is most often used in cases where you want to force card holders to pass a checkpoint before their cards can be valid inside a facility. In this way, you can prevent people from tailgating into the facility, since they would be subject to the inconvenience of their cards not operating within the facility. **Note:** Area Anti-Passback fails when Timed CC Enrollment and De-enrollment readers are used as In and Out readers for a Area. A timed clearance code scenario involves three readers: swiping a card at the **enrollment reader** grants access to a **timed reader** for the time period you specify; the cardholder's access lasts until either the time period has elapsed or until the card is presented at the **de-enrollment reader**. Optionally, you can specify a group of readers for enrollment and de-enrollment, and you may use any reader in the specified group(s). See "Configuring Timed Access" for instructions. The timed clearance code requires the following: The cardholder already must have permanent access given to the enrollment and de-enrollment readers by some other clearance code. The timed reader must have a clearance code with a default time zone. All readers must be entered as logical devices (see "Logical Devices Tab"). All clearance codes must be assigned to the company or card. Note that you can also define a timed expiration by Group instead of device. This enables any reader belonging to a specified group to operate as an enrollment reader. To specify a group to use instead of an enrollment device or de-enrollment device, check the appropriate Use Groups check box, click the icon next to the box, and select the Group. Make sure that the readers defined in the specified Group are not added in the Logical Device tab of the Timed Clearance code. Add all readers belonging to the specified Group to the standard enrollment reader Clearance Code.
Temporary Access	Sets a time and date at which all cardholders having this clearance code are granted and denied access at a single reader.

Configuring Timed Access

Use this procedure to configure an enrollment reader for timed access.

1. Create a Reader logical device (or select an existing Reader) that will be used as the Enrollment Reader. If you create a new Reader, name the device Reader Logical Device Enrollment Reader.
2. Create or use existing Reader logical devices that will be added to the Timed Clearance Code.
3. Create a new Clearance Code, and name it Enrollment Reader Clearance Code. This Clearance Code will contain the Reader Logical Device that will be used as your Enrollment Reader.
4. Add the Reader Logical Device that will be used as your Enrollment Reader to the Logical Devices Tab. No other Reader Logical Devices will need to be added, except the Enrollment Reader.
5. Create a second Clearance Code, and name this Clearance Code Timed Enrollment Clearance Code. This Clearance Code will be programmed as a Timed Clearance Code that will contain all Reader Logical Devices to be used for timed access within the Logical Devices Tab.

   Do not add the Enrollment Reader to the Logical Devices tab of this Clearance Code. Use the following configuration when you create the Clearance Code:

   a. For the default time zone field, select System All Times.

   b. In the Use Timed Expiration box, select Expires In and select the unit of time you desire. For the Enrollment Device, select the Enrollment Reader Logical Device.

   c. In the Logical Device tab, add all Reader Logical Devices that will be used for timed access.

   Caution: Do not add the Enrollment Reader Logical Device to the Logical Devices tab of this Clearance Code. The Enrollment Reader will not grant access if it is added to the Enrollment Reader Clearance Code.

The swipe of a valid card at the enrollment reader results in a local grant. The local grant at the enrollment reader begins the timed countdown that is defined in the Timed Enrollment Clearance Code for all Reader Logical

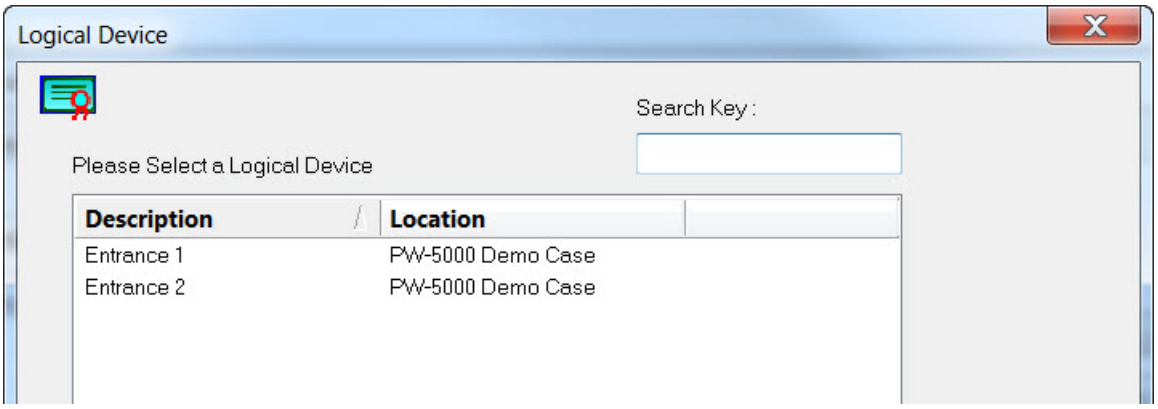
Devices configured in the Timed Enrollment Clearance Code's Logical Devices tab.

37.3.2 Logical Devices Tab

This tab displays the currently-configured logical devices assigned to this clearance code. You can add new logical devices, delete current logical devices, or change the default time zone for a logical device.

To add a new logical device:

1. Click **Add** to display the Logical Devices dialog box:



2. Select the logical device you want, and click **OK**. The device now appears in the Logical Devices tab.

Note: In the **Search Key** field, enter a search keyword to search progressively for logical devices. For example, the letters "ea" are sufficient to find a logical device named "East Door."

The returned logical devices are listed by their **Description** and **Location**. This is useful in sites with a large number of logical 'devices with similar names.

3. Click **OK** on the Logical Devices tab to assign the logical device to the clearance code.

To delete a logical device:

1. Click the logical device, and then click **Delete**. The prompt, "Are you sure you want to delete the selected resources?" appears.
2. Click **Yes**.

To change a logical device's time zone:

1. Click the logical device, and then click **Time Zone**. The Time Zones dialog box appears.

2. Click the time zone you want, and then click **OK**. The new time zone appears in the Logical Devices tab.

37.3.3 Elevator Outputs Tab

An elevator output, or output device, is wired to the elevator controller. The card holder can select the floor that corresponds to the output device.

1. Click the elevator output you want to assign to the clearance code.
2. Click **TimeZone** to change the elevator output's time zone, if you desire.

37.3.4 Output Groups Tab

An output group is a group of output devices. You assign output groups to the clearance code at this tab. You can assign a currently-configured output group listed on this tab, add an output group not on the tab, or delete an output group from the tab.

To assign a currently-listed output group:

Click the output group you want, and then click **OK**.

To add an output group:

1. Click **Add**. The Clearance Code - Add Output Groups dialog box appears.

Note: Click an output group, and then click **OK**.

The clearance code must contain a logical device with a reader at hardware address #1 on a PW2000 panel in order to show the output groups for that panel. Also, the list will not show output groups for a panel if the clearance code already has an output group from that panel.

2. Click **OK** at the Output Groups tab to assign the output group(s).

To delete an output group:

1. Click the output group, and then click **Delete**. The prompt, "Are you sure you want to delete the selected output group?" appears.
2. Click **Yes**.

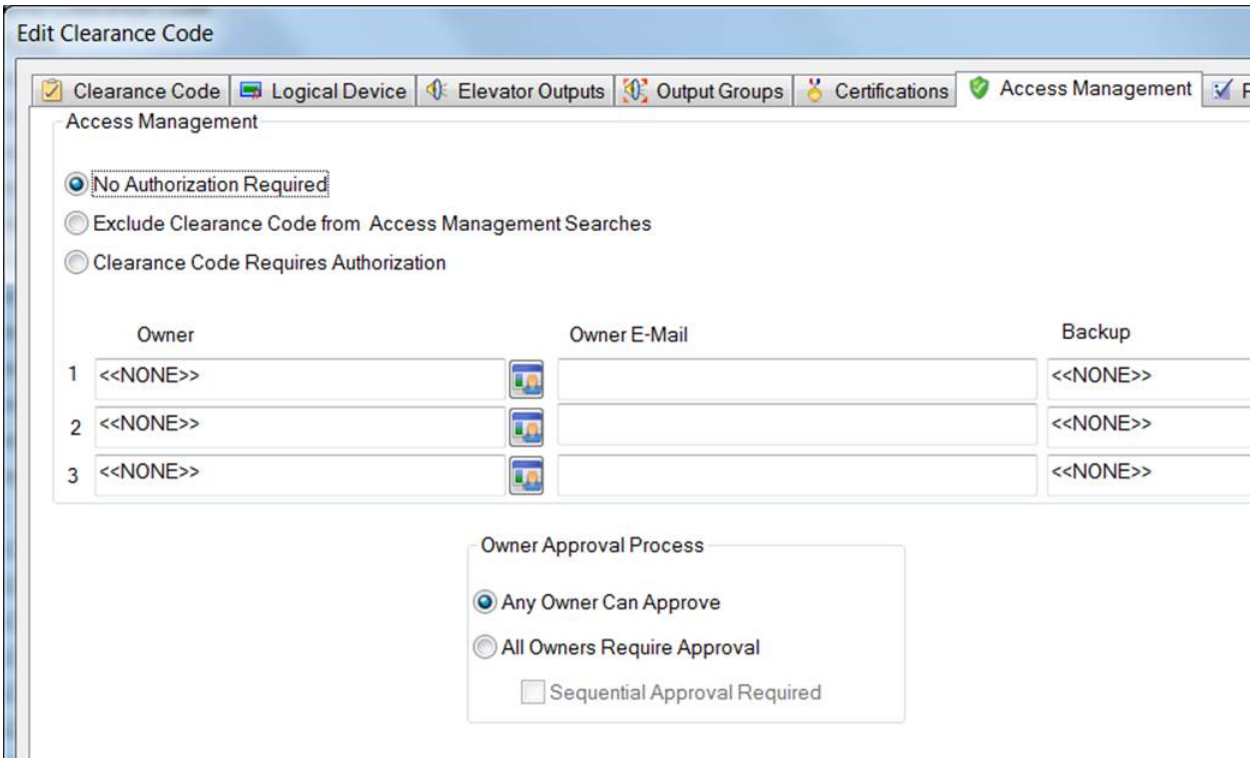
37.3.5 Certifications Tab

You can **add** and **delete** a clearance on this tab by using the respective command buttons on this screen. You can also select an existing clearance

code and tag it to be **removed when it expires**, again by using the respective command buttons on the certifications tab.

37.3.6 Access Management Tab

This is where you can enter and save the names of badge holders and their access authorization settings. You can save up to three badge holders and they can have backups. The radio buttons control how these badge IDs get used.



1. Select one of the following self-explanatory option-buttons:
   - **No authorization required**
   - **Exclude Clearance Code from Access Management Searches**
   - **Clearance Code Requires Authorization**
2. Enter the **Owner's Name** and **Backup**. The **Owner's E-Mail** address is a read-only field and displays the email address entered for the selected User ID.
3. Select one the following **Owner Approval Process** options:
   - **Any Owner Can Approve**
   - **All Owners Require Approval. If sequential approval is required, select the Sequential Approval Required check-box.**

4. Click **OK** when done.

37.3.7 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the clearance code:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the clearance code:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

37.4 Viewing Dependencies of a Clearance Code

Use this function to view a list of a Clearance Code's current dependencies. The Company object is the Clearance Code's dependency.

To view and edit ***a Clearance Code's dependencies****:*

1. Right-click the icon of an existing clearance code in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Clearance Code's current dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

37.5 Copying a Clearance Code

Use this function to copy the configuration of a clearance code and place the copy's icon in the right pane of the window.

1. In the Pro-Watch Database Configuration tree list, click the **Clearance Codes icon** to display the icons of all the current clearance codes in the right pane.
2. Right-click the clearance code you want, and select **Copy**.
3. Right-click in a blank area of the main pane.
4. Select **Paste**. A new clearance code icon appears with the name "Copy of [clearance code name]".
5. To rename and edit the new clearance code, see "Adding or Editing Clearance Codes".

37.6 Clearance Codes and Code of Federal Regulations (21 CFR 11)

Pro-Watch uses **digital signature technology** to verify that electronic records have not been altered subsequent to the last tracked modification, and that the authenticity of the user who is editing the records is affirmed.

By using digital signatures, Pro-Watch complies with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11).

Note: The term “digital signature” in this guide corresponds to the term “electronic signature” used in federal regulations.

Pro-Watch tracks the clearance codes for digital signature authorization, based on their underlying or potentially underlying logical devices.

Note: 21 CFR 11 does not work with Application Login.

37.6.1 Adding a Clearance Code and 21 CFR 11- No Signature Asked

Tracking begins when creating a new clearance code, or editing a logical device with no secured logical devices. In these cases, Pro-Watch does not prompt for any digital signatures.

37.6.2 Editing a Clearance Code and 21 CFR 11- Signature Asked

37.6.2.1 Adding Logical Device

If, while editing the clearance code, one or more logical devices from a secured area are added, then Pro-Watch asks for the appropriate **digital signatures**, logs that change under those signatures, and at the end saves the audited clearance code with all changes tied to the last received signature(s).

Pro-Watch displays the reason for change dialog box if any of the logical devices require it.

37.6.2.2 No Logical Devices Added

If no secured logical devices are added while editing the clearance code, Pro-Watch deletes the logging after the clearance code is saved.

37.6.2.3 Editing Clearance Code with Secured Logical Device

If the user edits a clearance code with secured logical device(s) present, Pro-Watch asks for signatures based on the most restrictive setting. All changes are logged, and are tied to that signature(s).

37.6.2.4 Adding, Deleting, Editing Secured Logical Device

Additionally if the user adds, deletes, or edits a secured logical device while editing the clearance code, Pro-Watch asks for the appropriate signatures, and logs that change under those signatures.

Pro-Watch displays the reason for change dialog box if any of the logical devices require it.

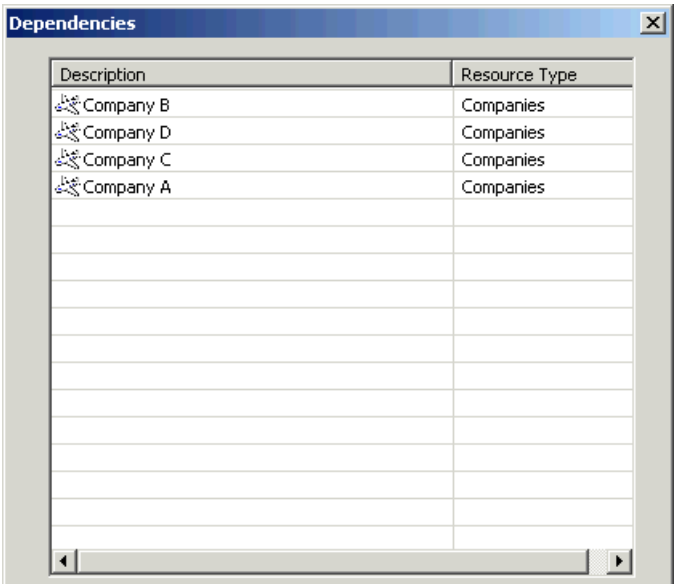
37.7 Deleting a Clearance Code

Use this function to delete a clearance code from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Clearance Codes** icon to display the icons of all the current clearance codes in the right pane.

Note: Right-click the clearance code you want to delete and select **Delete**.

You cannot delete either a system clearance code or a clearance code that has current dependencies. A dependency is another database object that includes Clearance Code object in its configuration. For example, the Company object is the Clearance Code's dependency. If the clearance code has no current dependencies, you are prompted to confirm the deletion. However, if the clearance code does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the clearance code:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the clearance code.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Companies

38

In this chapter ...

Overview

Companies Functions

Adding or Editing Companies

Viewing Dependencies of a Company

Copying a Company

Deleting a Company

38.1 Overview

Use this function to set privileges on a company-wide basis.

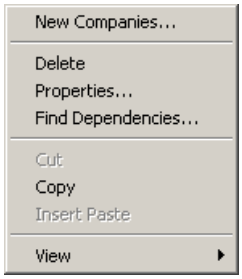
Note: Pro-Watch records database changes associated with **clearance code assignment to a company**, clearance code assignment to a card, logical device assignment to a card, and **company assignment to a card** in order to comply with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11), and for compliance tracking. The compliance tracking requirements use the aggregated logical devices' most restrictive settings.

After you set the privileges on a company level, you can refine access to doors and database information by assigning Clearance Codes and Partitions. You can also delete a company from the system if necessary, or limit access to a facility for a specific number of days by using temporary Clearance Codes. When you assign a company to a card, the company clearance codes become the default clearance codes for that card.

38.2 Companies Functions

To access Companies functions:

1. In the Pro-Watch Database Configuration tree list, click the **Companies** icon to display the currently-configured companies in the right pane of the Pro-Watch window.
2. Right-click a company icon to display the pop-up menu (if no company has been created yet, right-click anywhere in the right pane). If no companies have been created yet, this pop-up menu only shows a subset of these functions:



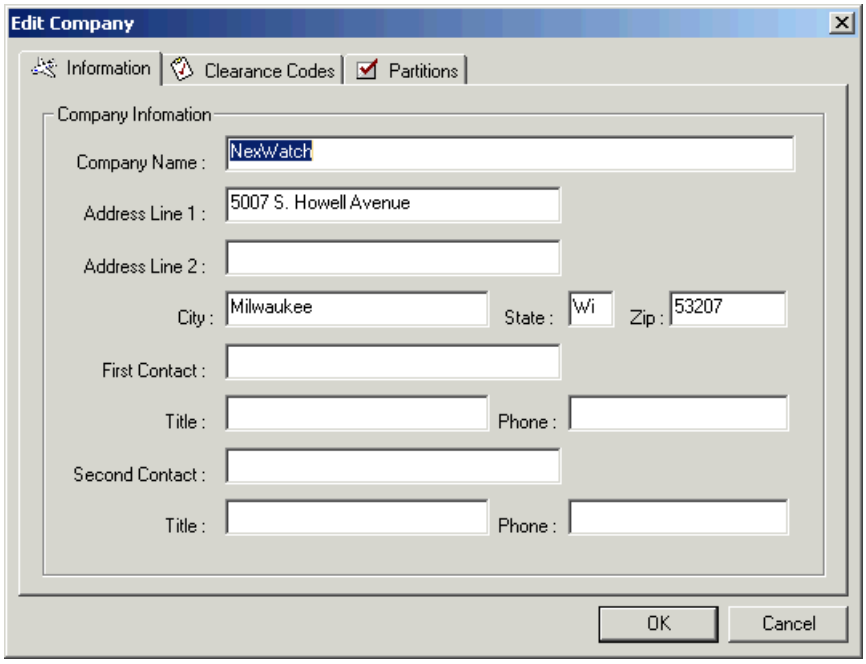
3. Use the following table to select a function:

Click...	To...
New Companies...	Add a new company. See "Adding or Editing Companies".
Delete	Delete a current company. See "Viewing Dependencies of a Company".
Properties...	Edit a current company configuration. See "Adding or Editing Companies".
Find Dependencies...	Display the names of all resources that depend upon the company. See "Viewing Dependencies of a Company".
Copy	Copy a company configuration and insert the copy's icon in the Pro-Watch window. See "Copying a Company".

38.3 Adding or Editing Companies

1. To ***add*** a new company, right-click the **Companies icon** in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Companies** to display the Add Company dialog box.

   To ***edit*** an existing company, click the **Companies icon** to display the profiles in the right pane. Right-click on the company you want and select **Properties** to display the Edit Company dialog box.



2. Complete the following tab sections to configure the company:

   COMPANIES TABS LIST

   - "Information Tab".
   - "Clearance Codes Tab".

- "Partitions Tab".

38.3.1 Information Tab

Use the following field definitions to complete the Information tab in the Add Company or Edit Company dialog box:

Field	Description
Company Name	Specifies the name of the company.
Address Line 1 Address Line 2 City State Zip	Specifies the company address.
First Contact Title Phone	Specifies the company's access control manager.
Second Contact Title Phone	Specifies a second employee who is responsible for the company's access control system.

38.3.2 Clearance Codes Tab

A clearance code grants or denies badge holder access to certain doors and elevators within the company (see "DBC - Clearance Codes" in Chapter 37 for more information). At this tab, you can assign or delete a currently-defined clearance code or define and assign a new clearance code.

Note: Clearance codes are assigned to the Company database element. Badge holders within an enterprise are often assigned access privileges that are defined at the Company level. Therefore, changing the company's clearance code broadly impacts access privileges across the company.

To assign a currently-defined clearance code:

- Click the clearance code you want, and then click **OK**.

To delete a currently-defined clearance code:

- Click the clearance code you want do delete, and then click **Delete**.

To define and assign a new clearance code:

1. Click **Add** to display the Clearance Codes dialog box.
2. Click the clearance code you want to add, and click **OK**.

38.3.3 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the company:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the company:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

38.4 Viewing Dependencies of a Company

Use this function to view a list of a Company's current dependencies. The Badge and Event Trigger objects are Company dependencies.

To view and edit ***a Company's dependencies****:*

1. Right-click the icon of an existing company in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the company's current dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

38.5 Copying a Company

Use this function to copy the configuration of a company and place the company's icon in the right pane of the window.

1. In the Pro-Watch Database Configuration tree list, click the **Companies** icon to display the current companies in the right pane.
2. Right-click the company you want, and select **Copy**.
3. Right-click in a blank area of the main pane.
4. Select **Paste**. A new company icon appears with the name "Copy of [company name]".
5. To rename and edit the new company, see "Adding or Editing Companies".

38.6 Deleting a Company

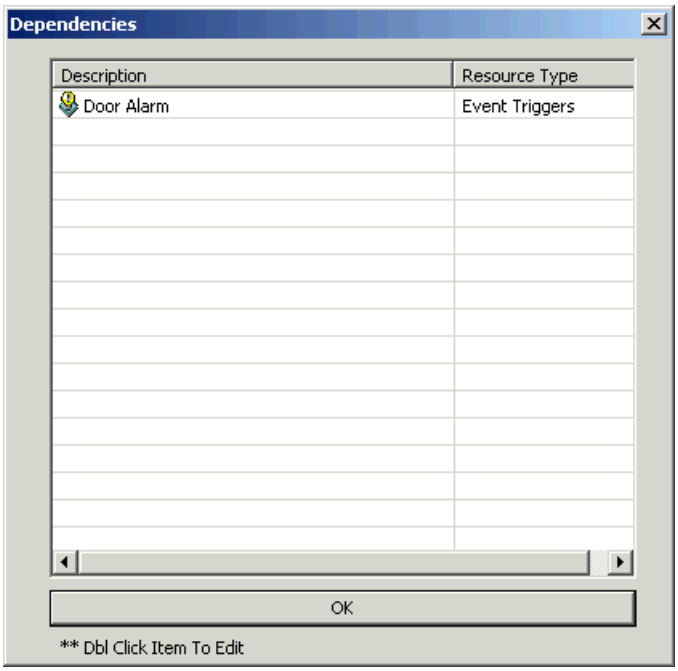
Use this function to delete a Company from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Companies icon** to display the current companies in the right pane.

Note: Right-click the company you want to delete and select **Delete**.

You cannot delete a company that has current dependencies. A dependency is another database object that includes the Company object in its configuration.

Example: The Badge and Event Trigger objects are the Company dependencies. If the company has no current dependencies, you are prompted to confirm the deletion. However, if the company does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the company:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the company.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Database Tables

39

In this chapter ...

Overview
Database Table Functions
Adding or Editing Database Tables
Deleting a Database Table

39.1 Overview

Use this feature to specify which database tables will be available to users, and which tables can be partitioned and audited.

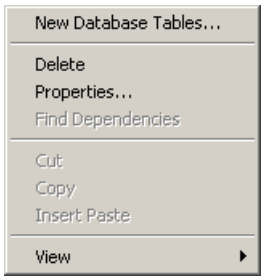
Partitioned tables require more system resources than non-partitioned tables. Therefore, it is important to partition selectively.

Note: Normally, it is not necessary to add a new database table. If you should consider adding a new table, remember that enabling audit logging consumes resources and may affect Pro-Watch performance.

39.2 Database Table Functions

To access Database Tables functions:

1. In the Pro-Watch Database Configuration tree list, click the **Database Tables** icon to display the currently-configured tables in the right pane of the Pro-Watch window.
2. Right-click a database table icon to display the pop-up menu:



3. Use the following table to select a function:

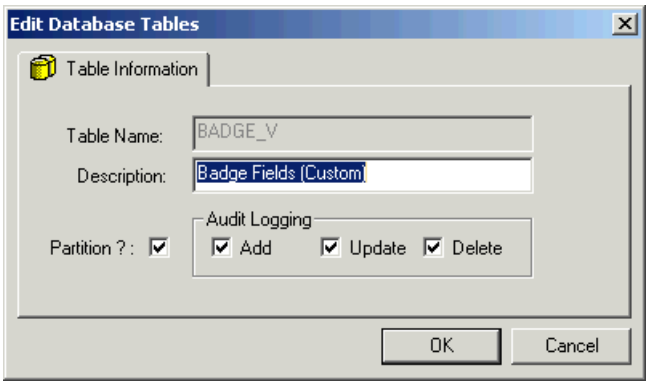
Click...	To...
New Database Tables...	Add a new database table. See "Adding or Editing Database Tables".
Delete	Delete a current database table. See "Deleting a Database Table".
Properties...	Edit a current database table configuration. See "Adding or Editing Database Tables".
Find Dependencies...	Display the names of all resources that depend upon the database table.
View	Change the way the icons are displayed in the Pro-Watch window.

39.3 Adding or Editing Database Tables

*To **add** or edit a database table:*

1. To *add* a new database table, right-click the **Database Tables icon** in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Database Table** to display the Add Database Table dialog box.

   To ***edit*** an existing database table, click the **Database Tables** icon to display the profiles in the right pane. Right-click on the database table you want and select **Properties** to display the Edit Database Tables dialog box.



2. Complete the tab sections below to configure the database table:

39.3.1 Table Information

Use the following field definitions to complete the Table Information tab in the Add Database Table or Edit Database Table dialog boxes, and then click **OK** to accept the entries:

Field	Description
Table Name	Names the database table. If you are adding a new table, you must enter a table name. If you editing an existing table, the name already appears in the field, and it is recommended that you do not change it.
Description	Identifies the table uniquely. If you are adding a new table, you must enter a unique description. If you editing an existing table, the description already appears in the field, and it is recommended that you do not change it.
Partition	Specifies whether or not the table will be partitioned.

Field	Description
Audit Logging	Captures changes to a Pro-Watch table. Add – when a record is added to a table, this function inserts a copy of the record (with audit information) in the audit log. Update — when a record is updated, this function writes for each modified column a before value, an after value, and audit information in the audit log. Delete — when a record is deleted from a table, this function inserts an audit log record with audit information. **Warning: It is EXTREMELY IMPORTANT to be sure you are NOT deleting a table record required by your enterprise!!!**

39.4 Deleting a Database Table

Use this function to delete a database table.

Warning: Before deleting a Pro-Watch database table, you should be completely certain that your enterprise does not need this data.

1. In the Pro-Watch Database Configuration tree list, click the **Database Tables** icon to display the profiles in the right pane. Right-click on the database table you want to delete and select **Properties** to display the Edit Database Tables dialog box.
2. Click **Delete**. The prompt, "Delete Table [table name]?" appears.
3. If you are sure you want to delete the table, click **Yes**.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC - Default Events

40

In this chapter ...

Overview

40.1 Overview

For every possible occurrence on a hardware device, Pro-Watch requires a defined event to process that occurrence. The Default Events utility enables you to change the absolute defaults for these events when the hardware is first added. Default Events also changes defaults for events in logical device templates, which overwrite a hardware device's events when the hardware is assigned to a logical device.

It is very unlikely that you would need to use the Default Events utility, unless you are creating large number of templates or configuring a large amount of hardware that is not assigned to any logical device. Therefore, it is strongly suggested that you modify event points at the template or logical device levels. Refer to "Configuring Hardware Templates" in Chapter 6 for instructions and information.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Deferred Access

41

In this chapter ...

Overview

Considerations and Limitations of Deferred Access

Starting and Ending a Deferred Access Project

Accessing the Deferred Access Functions

Adding or Editing a Deferred Access Project

Viewing Dependencies of a Deferred Access Project

Copying a Deferred Access Project

Deleting a Deferred Access Project

41.1 Overview

The Deferred Access functionality enables the user to quickly shun a selected group of access holders from a specified area. Deferred Access is designed to take effect immediately.

The Deferred Access functionality employs host-based access because, in critical situations, it may take just too long to re-download all the cards affected by a Group. An example would be the need to immediately deny access to all but a small group of flight engineers on the launch pad of a space rocket just before the launch.

When a Deferred Access project is active, the access decisions for the associated doors are made by the Communications Server, not locally by the individual panels and ACUs.

Note: Despite what its name may suggest, the Deferred Access is actually a filter that **takes away access** which has already been assigned to the cards via other means (e.g., Clearance Codes and Logical Device Grants).

The user can activate or deactivate the Deferred Access on a specified date and time, or by an Event Trigger.

The Deferred Access functionality enables the user to:

- Configure a start and stop date and time, or a trigger event, for activation and deactivation.
- Assign one or more multiple clearance codes (for Device Access Selection) and companies (for badgeholder selection) to an event or project as defined by the user.

41.2 Considerations and Limitations of Deferred Access

- The user can set the Deferred Access Project start and stop times only to whole minutes.
- A Deferred Access project can be started and ended through setting a specific date and time, and specifying an Event Trigger. This topic is explained in detail in "Starting and Ending a Deferred Access Project".
- The Communications Server is required to download commands to the associated panels in order set Host Access Mode upon activation, and during the deactivation of the Deferred Access Projects. If a panel is offline when this occurs, its Host Access Mode does not change until it comes back online.
- When a panel is disconnected from the Server during an active Deferred Access Project, different panel types may behave in different ways. The SEEP panels may revert to normal access, while the Cardkey panels may deny all access altogether. A panel's offline behavior must be taken into consideration when setting up Deferred Access Projects and system maintenance procedures.
- Deferred Access is designed primarily for use with the SEEP panels. However, PW-5000 series and Cardkey panels are also supported. At the time of this writing, Star II and PW2000 panels do not properly function if assigned to a Group.
- If the same SEEP panel is referenced by both a Deferred Access Project and an anti-passback Area with "hard" enforcement, the panel is always in Host Access mode when connected to the Server. This must be taken into consideration if Deferred Access is planned in conjunction with Anti-Passback.
- Host Grants and Denials for cards at the readers on panels currently in Host Access Mode do not queue a corrective card download since it would result in redundant information.

41.3 Starting and Ending a Deferred Access Project

A Deferred Access project can be started and ended in two different ways:

- Through setting a definite Start and Stop date and time. These dates and times are processed using the local time of the Database Server.
- Through setting an Event Trigger.

The following table summarizes the **four combinations** in which date/time and an event trigger can be configured to start and stop a Deferred Access project:

	STARTS ON Date and Time	**STARTS ON Event Trigger**
STOPS ON Date and Time	(Cell 1) 1 year maximum default	(Cell 2) 1 year maximum default
STOPS ON Event Trigger	(Cell 3) 1 year maximum default	(Cell 4) 1 year maximum default

1. **(Cell 1)** The project starts on a specific date+time and ends on a specific date+time. The end date+time is by default set at 1 year, maximum.

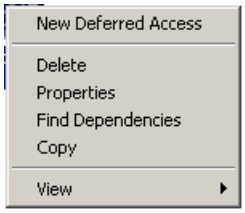
Note: **(Cell 2)** The project starts when a specific alarm event is triggered and ends at a specific date+time.

If the Event Trigger occurs not before but after the pre-set ending date+time, the project is deactivated after the maximum default date+time interval of 1 year.

2. **(Cell 3)** The project starts on a specific date+time and ends when a specific alarm event is triggered. If the ending Event Trigger fails to occur, then the project is deactivated after the maximum default date+time interval of 1 year.
3. **(Cell 4)** The project starts when a specific alarm event is triggered and ends again when a specific alarm event is triggered. If the ending Event Trigger fails to occur, then the project is deactivated after the maximum default date+time interval of 1 year.

41.4 Accessing the Deferred Access Functions

1. In the Pro-Watch Database Configuration tree list, click the **Deferred Access** icon to display the currently-configured groups (if there are any) in the right pane of the Pro-Watch window.
2. Right-click on the icon of an existing Deferred Access project to display the pop-up menu:



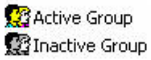
3. Use the following table to select a function:

Click...	To...
New Deferred Access	Add a new Deferred Access project. See "Adding or Editing a Deferred Access Project".
Delete	Delete a current Deferred Access project. See "Viewing Dependencies of a Deferred Access Project".
Properties	Edit a current Deferred Access project. See "Adding or Editing a Deferred Access Project".
Find Dependencies	Display the names of all resources that depend upon the Deferred Access project. See "Viewing Dependencies of a Deferred Access Project".
Copy	Copy a Deferred Access project and insert the copy's icon in the Pro-Watch window. See "Copying a Deferred Access Project".
View	Change the way the icons are displayed in the Pro-Watch window.

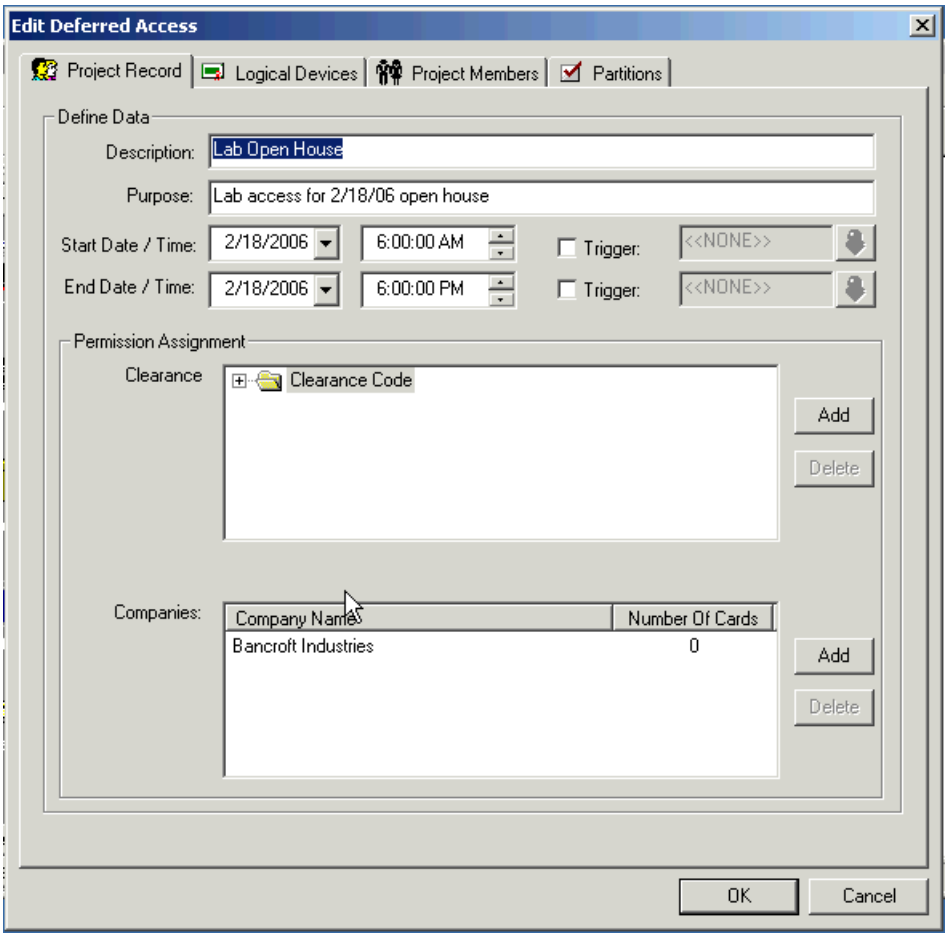
41.5 Adding or Editing a Deferred Access Project

Note: To ***add*** a new Deferred Access project, right-click the **Deferred Access** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Deferred Access from the pop-up menu** to display the **Add Deferred Access** dialog box. Follow the steps and field descriptions given below for editing Deferred Access.

Active Deferred Access projects are represented by color icons. The inactive groups have gray icons:



To ***edit*** an existing group, click the **Deferred Access** icon to display the existing Deferred Access projects in the right pane. Right-click the icon of the Deferred Access project you want and select **Properties** to display the **Edit Deferred Access** dialog box:



4. Complete the tab sections below to configure the new or existing Deferred Access project.

5. After filling in all the tabs, click **OK** to finish configuring the Deferred Access.

41.5.1 Project Record Tab

1. Enter a **Description** (32 characters maximum) of the Deferred Access project.
2. Enter the **Purpose** (32 characters maximum) of the Deferred Access project.

Note: Select a **Start Data/Time** and **End Date/Time** from the respective drop-down list boxes (for dates) and spin boxes (for times).

The start date and time must be a minimum of three minutes before the designated stop date and time.

3. If the project can be started and/or ended by a trigger event, do the following:
    - Select the respective start Trigger and/or end Trigger **check-box**.

Note: Select the start and/or end **trigger event** from the respective drop-down list box(es).

Date/time and trigger event selections are mutually exclusive. When you select a Trigger check box, the related Data and Time fields are disabled.

4. In the Clearance Codes list box, select the **clearance code(s)** needed for the event.
    - To *add* new clearance codes for this group project, click **Add**.
    - To *delete* a clearance code displayed for this group project, select it and click **Delete**.

Note: You can assign one or more **badge holders** to the group project by clicking the browser button next to the Badgeholder field and making the appropriate selection(s).

Click and select the **Project Members tab** to see a list of all the individuals assigned to the group project through this badgeholder field.

Note: You can assign a **company** to the group project by clicking the browser button next to the Company field and making the appropriate selection.

All the individuals assigned to this company become the members of the

group project. Click and select the **Project Members tab** to see a list of all the individuals assigned to the group project through the company code.

41.5.2 Logical Devices Tab

Click and select the **Logical Devices tab** to manually change the existing readers and/or timezones assigned to the group project. This tab enables the user to grant access to specific areas without creating new clearance codes.

Notes:

- Logical devices are part of a Deferred Access project only if they are added directly on the Logical Devices tab, or if they are added through a clearance code on the Projected Tab, and not revoked on the Logical Devices tab.
- Any panel with a logical device that is added to a Deferred Access project is in the host mode while the project is in progress.

To grant access to an existing logical device that has a revoke status:

Select the device and click **Grant**.

Note: Access for logical devices in a Deferred Access project is affected only while that project is in progress.

To deny access to an existing logical device that has a grant status:

Select the device and click **Revoke**.

To edit the time zone of an existing logical device:

Select the device and click **Time Zone**.

To delete an existing logical device:

Select the device and click **Delete**.

41.5.3 Project Members Tab

Click and select the **Project Members tab** to display a list of all the individuals assigned to the group project.

All the individuals that are added to the group project through the company you have selected earlier in the Project Record tab have an asterisk (“*”) after their names.

Note: Cards are part of a project only if they are added directly on the Project Members tab, or if they are added through a company on the Project record tab, and not revoked on the Logical Devices tab

To display the company-member project members:

Select the **Include Company Members** check box.

To add company-non-member cardholders to the project:

1. Enter either the full name of a cardholder or the first few letters of his name into the Card Holder search field.
2. The name(s) of the cardholder(s) matching the search letter/word are listed in the Card Holder list box.
3. Select a cardholder and click **Add**.

To change the grant/revoke status of a project member:

Select the member's name from the Project Members list box and click **Grant** or **Revoke**.

To delete a member from the Deferred Access project:

Select the member's name from the Project Members list box and click **Delete**.

41.5.4 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for more information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the Deferred Access project:

1. In the Partitions tab, select the partition you want.
2. Click **OK** to assign the partition to the project.

To assign a partition to the Deferred Access project:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

41.6 Viewing Dependencies of a Deferred Access Project

Use this function to view a list of a Deferred Access project's current dependencies.

To view and edit ***a Deferred Access Project's dependencies:***

1. Right-click the icon of an existing Deferred Access project in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Deferred Access project's current dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

41.7 Copying a Deferred Access Project

Use this function to create a copy of a group project. This is a fast way to create a new type of group project.

If the original project is similar to the new one, you can copy the original and change only a small number of its properties to create the new group project.

1. In the Pro-Watch Database Configuration tree list, click the **Deferred Access** icon to display the currently-configured Deferred Access projects in the right pane.
2. Right-click the icon of the Deferred Access you want to copy, and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original group name]” appears in the right pane.

41.8 Deleting a Deferred Access Project

Use this function to delete a Deferred Access project from the Pro-Watch database:

1. In the Pro-Watch Database Configuration tree list, click the **Deferred Access** icon to display the currently-configured groups in the right pane of the Pro-Watch window.

Note: Right-click the Deferred Access you want to delete and select **Delete**.

You cannot delete a Deferred Access project until you delete its current dependencies. A dependency is another database object that includes the Deferred Access object in its configuration. If the Deferred Access has no current dependencies, you are prompted to confirm the deletion. However, if the Deferred Access does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Deferred Access:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the group.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC - Dial-Up Schedule

42

In this chapter ...

Overview

Dial-Up Schedule Functions

Adding or Editing Dial-up Schedules

Viewing Dependencies of a Dial-up Schedule

Copying a Dial-up Schedule

Deleting a Dial-up Schedule

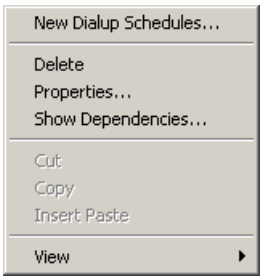
42.1 Overview

Use this function to establish the frequency and time of day when the server uploads or downloads data to or from a remote panel via a dial-up modem. This function is also used in conjunction with the Modem Pools and Dial-ups functions.

42.2 Dial-Up Schedule Functions

To access Dial-up Schedule functions:

1. In the Pro-Watch Database Configuration tree list, click the **Database Tables** icon to display the currently-configured tables in the right pane of the Pro-Watch window.
2. Right-click a database table icon to display the pop-up menu:



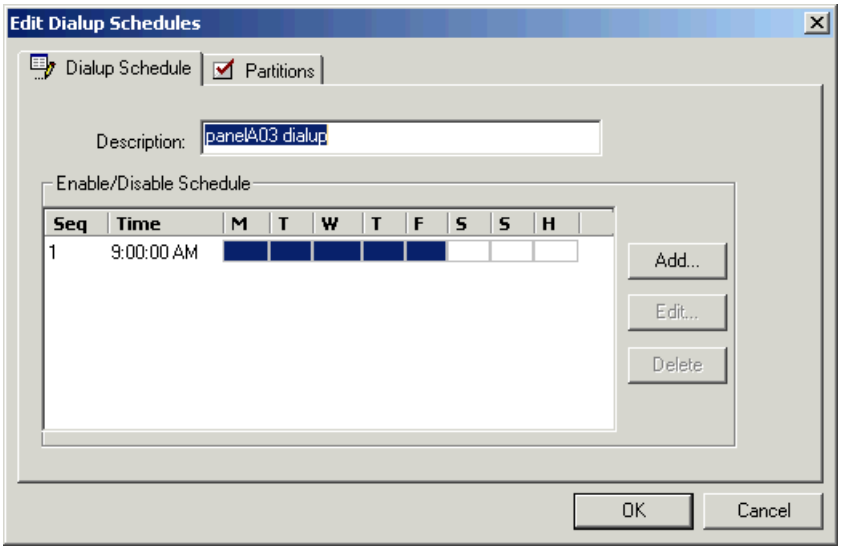
3. Use the following table to select a function:

Click...	To...
New Dial-up Schedules...	Add a new dial-up schedule. See "Adding or Editing Dial-up Schedules".
Delete	Delete a current dial-up schedule. See "Adding or Editing Dial-up Schedules".
Properties...	Edit a current dial-up schedule. See "Adding or Editing Dial-up Schedules".
Show Dependencies...	Display the names of all resources that depend upon the Dial-up schedule.
Copy	Copy a dial-up schedule and insert the copy's icon in the Pro-Watch window. See "Adding or Editing Dial-up Schedules".
View	Change the way the icons are displayed in the Pro-Watch window. See "Adding or Editing Dial-up Schedules".

42.3 Adding or Editing Dial-up Schedules

1. To ***add*** a new dial-up schedule, right-click the **Dial-up Schedules** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Dial-up Schedule** to display the Add Dial-up Schedule dialog box.

   To ***edit*** an existing dial-up schedule, click the **Dial-up Schedules** icon to display the schedules in the right pane. Right-click on the dial-up schedule you want and select **Properties** to display the Edit Dial-up Schedule dialog box.



2. Complete the tab sections below to configure the database table:

42.3.1 Dial-up Schedule Tab

1. Enter a unique description of the dial-up schedule. For example, you can include the name of the panel.
2. If you are adding a new dial-up schedule, click **Add**. The Enable/Disable Time dialog box appears. If you are editing an existing dialog box schedule, click the schedule row you want to edit and click **Edit**. Or, double-click the schedule row you want to edit. The Enable/Disable Time dialog box appears.
3. Set the days and times you want the server and the panel to exchange information during the week.
4. Click **OK** to accept the schedule.

42.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no

partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the dial-up schedule:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the dial-up schedule:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

42.4 Viewing Dependencies of a Dial-up Schedule

Use this function to view and edit the Dial-up Schedule's dependencies. The Dial-up Schedule object depends upon the Channel object.

To view and edit ***a Dial-up Schedule's dependencies****:*

1. Right-click the icon of an existing Dial-up Schedule in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Dial-up Schedule's current dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

42.5 Copying a Dial-up Schedule

Use this function to copy the configuration of a dial-up schedule and place the copy's icon in the right pane of the window.

1. In the Pro-Watch Database Configuration tree list, click the **Dial-up Schedules** icon to display the current dial-up schedule in the right pane.
2. Right-click the dial-up schedule you want, and select **Copy**.
3. Right-click in a blank area of the main pane.
4. Select **Paste**. A new dial-up schedule icon appears with the name "Copy of [dial-up schedule name]".
5. To rename and edit the new dial-up schedule, see "Adding or Editing Dial-up Schedules".

42.6 Deleting a Dial-up Schedule

Use this function to delete a Dial-up Schedule from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Dial-up Schedules** icon to display the procedures in the right pane.

Note: Right-click the Dial-up Schedule you want to delete and select **Delete**.

You cannot delete a Dial-up Schedule that has current dependencies. A dependency is another database object that includes the Dial-up Schedule in its configuration.

Example: The Channel object is the Dial-up Schedule's dependency. If the Dial-up Schedule has no current dependencies, you are prompted to confirm the deletion. However, if the Dial-up Schedule does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Dial-up Schedule:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Dial-up Schedule.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Event Procedures

43

In this chapter ...

Overview

Event Procedure Functions

Adding or Editing Event Procedures

Viewing Dependencies of an Event Procedure

Copying an Event Procedure

Running an Event Procedure

Deleting an Event Procedure

43.1 Overview

Use this function to create an execution sequence of one or more commands. For example, an event procedure might open a door when an operator pushes a button. The execution of an event procedure, however, requires an event trigger (see "DBC - Event Triggers" in Chapter 44). The event procedure does not execute by itself.

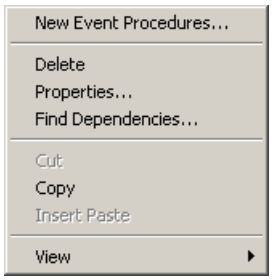
You can create an event procedure that executes on a logical device, with a CCTV command, or with a change the state of a Reader. The commands do not have to be executed on the same device, CCTV command, or Reader.

Example: An event procedure can execute multiple tasks on different devices throughout the network. Something that occurs to an input on a PW2000 panel could cause a door to unlock on a PW-5000 panel.

43.2 Event Procedure Functions

To access Event Procedures functions:

1. In the Pro-Watch Database Configuration tree list, click the **Event Procedures** icon to display the currently-configured procedures in the right pane of the Pro-Watch window.
2. Right-click a database table icon to display the pop-up menu:



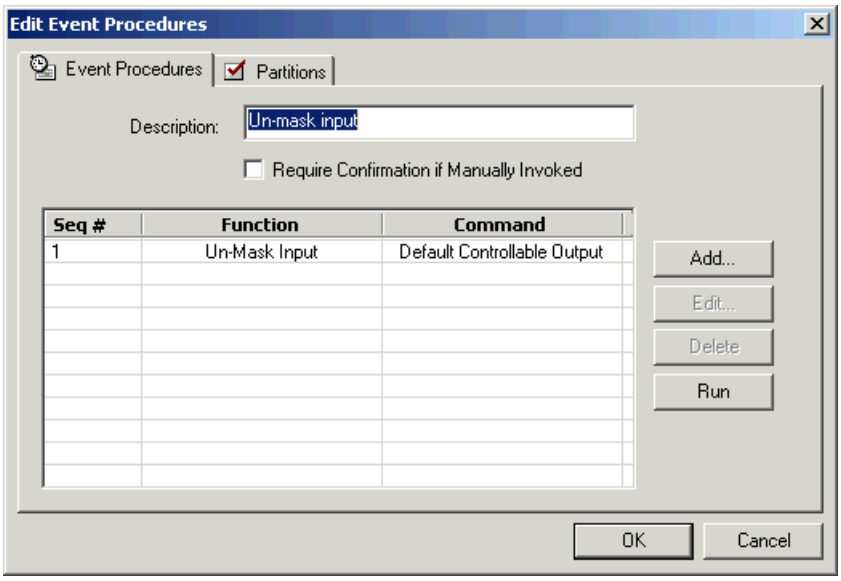
3. Use the following table to select a function:

Click...	To...
New Event Procedures...	Add a new event procedure. See "Adding or Editing Event Procedures".
Delete	Delete a current event procedure. See "Viewing Dependencies of an Event Procedure".
Properties...	Edit a current event procedure. See "Adding or Editing Event Procedures".
Find Dependencies...	Display the names of all resources that depend upon the event procedure. See "Viewing Dependencies of an Event Procedure"
Copy	Copy an event procedure and insert the copy's icon in the Pro-Watch window. See "Copying an Event Procedure".
View	Change the way the icons are displayed in the Pro-Watch window.
Execute	Runs the event procedure to verify that the settings are correct. See "Running an Event Procedure".

43.3 Adding or Editing Event Procedures

1. To ***add*** a new event procedure, right-click the **Event Procedures** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Event Procedures** to display the Add Event Procedures dialog box.

   To ***edit*** an existing event procedure, click the **Event Procedures** icon to display the event procedures in the right pane. Right-click on the event procedure you want and select **Properties** to display the Edit Event Procedures dialog box.



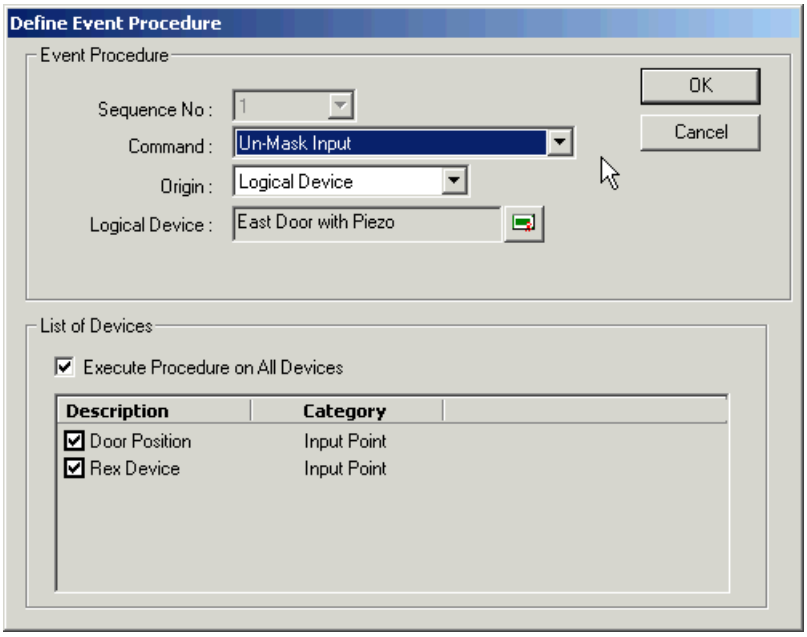
2. Complete the tab sections below to configure the event procedure:

Note: After you create an event procedure, you must assign it to either a class or to a user to make it operative. See Event Procedures Tab, page 10 in "DBC - Classes" in Chapter 36 or Event Procedures Tab, page 23 in "DBC - Users" in Chapter 58 for instructions.

43.3.1 Event Procedures Tab

1. To *add* a new event procedure at the Add Event Procedures dialog box, select **Require Confirmation** if you want the user to be prompted before the procedure is run. Then, click **Add**. The Define Event Procedure dialog box appears.

   Or, to *edit* an existing event procedure at the Edit Event Procedures dialog box, click the procedure you want to edit and then click **Edit**. The Define Event Procedure dialog box appears.



2. Whether you are adding a new event procedure or editing an existing one, use the following field descriptions to complete the Define Event Procedure dialog box:

Field	Description
Sequence No.	Specifies the order you want the event procedure to occur. The number range is 1-99; 1 is the highest priority, 99 is the lowest. **Example:** Select 1 if you want this procedure to occur before all other assigned event procedures. **Note:** An event procedure can consist of multiple commands that run sequentially each time the procedure executes.
Command	Lists the commands that are available for the event procedure to perform. Click the drop-down box to display the available commands. See Appendix B, Assignable Programs for descriptions of the commands.
Origin	Specifies from where the command executes. Possible origins are a logical device, group, clearance code, or CCTV command.

Field	Description
Logical Device	Specifies the device against which the originating device executes the command.
List of Devices	Lists the available device types that are capable of executing the defined event procedure.
Execute Procedure on All Devices	Specifies that all device types in the selected logical device will be capable of executing the defined event procedure.

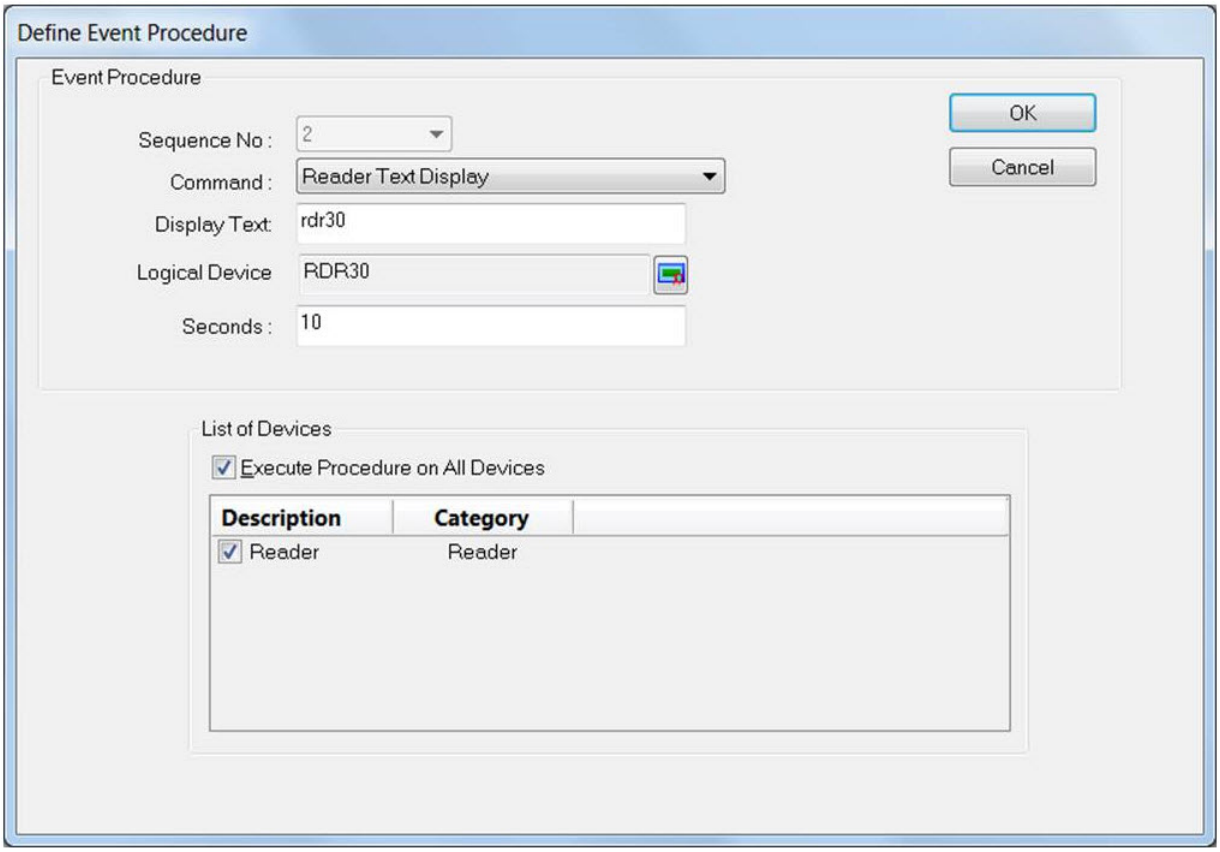
3. Click **OK** to return to the Add Event Procedures or Edit Event Procedures dialog box with the new procedure included. If you have added a new event procedure, enter a description.
4. Either create additional event procedures using the previous steps or click **OK** to close the dialog box.

43.3.1.1 Reader Text Display

"**Reader Text Display**" is a new action that sends a text string down to a reader. The display text can be up to 16 characters, must be ASCII characters, and will appear on the first line of the reader's display for the specified number of seconds.

1. Select an event procedure in the **Event Procedures** database module..
2. Double-click the icon (or right click and from the pop-up menu select **Properties**) to display the **Edit Event Procedures** screen.

3. Click **Add** to display the **Define Event Procedure** screen:



4. From the **Command** drop-down menu, select **Reader Text Display**.
5. Select a **Logical Device**.
6. Enter the number of **Seconds** to define the display duration.
7. When done, click **OK**.

43.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the event procedure:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the event procedure:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

43.4 Viewing Dependencies of an Event Procedure

Use this function to view a list of an Event Procedure's current dependencies. An Event Procedure is dependent upon the Event Trigger object.

To view and edit ***an Event Procedure's dependencies****:*

1. Right-click the icon of an existing event procedure in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the event procedure's current dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

43.5 Copying an Event Procedure

Use this function to create a copy of an event procedure. This can be a fast way to create a new procedure. If the original procedure will be similar to the new one, you can copy the original and change only a small number of its properties to create the new event procedure.

1. In the Pro-Watch Database Configuration tree list, click the **Event Procedure** icon to display the currently-configured event procedures in the right pane.
2. Right-click the icon of the event procedure you want to copy, and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original event procedure name]” appears in the right pane.

43.6 Running an Event Procedure

To test the procedure.

1. In the Pro-Watch Database Configuration tree list, click the **Event Procedure** icon to display the currently-configured event procedures in the right pane.
2. Right-click the icon of the event procedure you want to run, and select **Execute**. The command sequence runs.

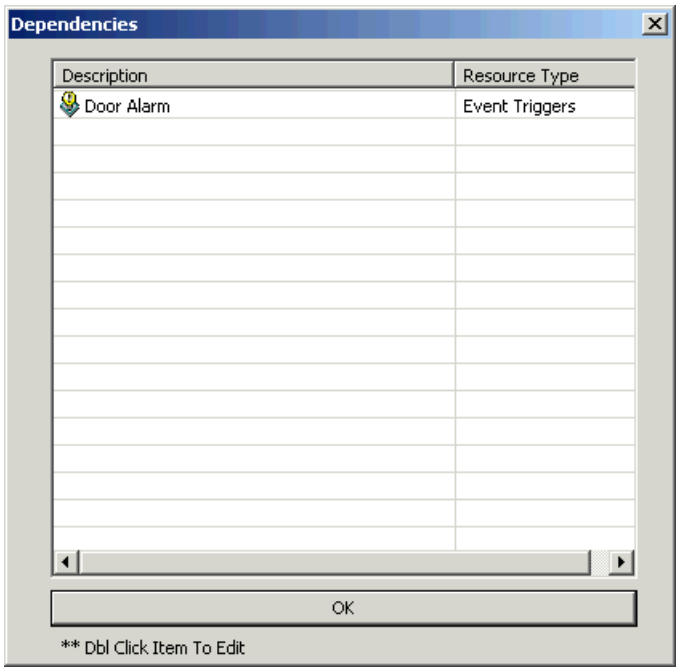
43.7 Deleting an Event Procedure

1. In the Pro-Watch Database Configuration tree list, click the **Event Procedures icon** to display the procedures in the right pane.

Note: Right-click the event procedure you want to delete and select **Delete**.

You cannot delete an Event Procedure until you delete its current dependencies. A dependency is another database object that includes the Event Procedure in its configuration.

Example: The Event Trigger object is the Event Procedure's dependency. If the event procedure has no dependencies, you are prompted to confirm the deletion. However, if the event procedure does have dependencies, the Dependencies dialog box appears.



2. If you still want to delete the event procedure:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the event procedure.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Event Triggers

44

In this chapter ...

Overview
Event Trigger Functions
Adding or Editing Event Triggers
Copying an Event Trigger
Deleting an Event Trigger

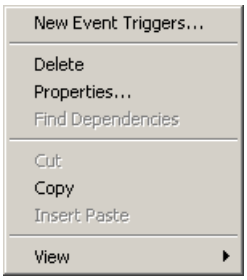
44.1 Overview

Use this function to trigger an event procedure when the conditions of the trigger are met. An event procedure is a sequence of commands. For example, you can configure a trigger to execute an event procedure that turns an alarm off after the alarm occurs.

44.2 Event Trigger Functions

To access Event Trigger functions:

1. In the Pro-Watch Database Configuration tree list, click the Event Triggers icon to display the currently-configured triggers in the right pane of the Pro-Watch window.
2. Right-click an event trigger icon to display the pop-up menu:



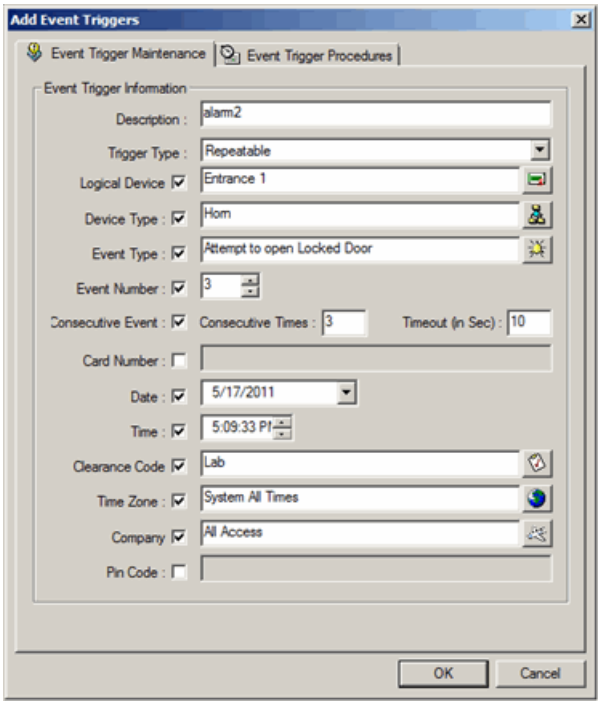
3. Use the following table to select a function:

Click...	To...
New Event Triggers...	Add a new event trigger. See "Adding or Editing Event Triggers".
Delete	Delete a current event trigger. See "Deleting an Event Trigger".
Properties...	Edit a current event trigger. See "Adding or Editing Event Triggers".
Copy	Copy an event trigger and insert the copy's icon in the Pro-Watch window. See "Copying an Event Trigger".
View	Change the way the icons are displayed in the Pro-Watch window.

44.3 Adding or Editing Event Triggers

1. To ***add*** a new event trigger, right-click the Event Triggers icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select New Event Triggers to display the Add Event Triggers dialog box.

   To ***edit*** an existing event trigger, click the Event Triggers icon to display the triggers in the right pane. Right-click on the event trigger you want and select Properties to display the Edit Event Triggers dialog box.



2. Complete the following tab sections to configure the event trigger:

   EVENT TRIGGER TABS LIST

   - "Event Trigger Maintenance Tab".
   - "Event Trigger Procedures Tab".

- "Partitions Tab".

44.3.1 Event Trigger Maintenance Tab

1. Use the following field descriptions to complete the Define Event Trigger dialog box:

Field	Description
Description	Names the trigger.
Trigger Type	Specifies one of the following three trigger types: Repeatable – trigger activates whenever the defining criteria are met. Once only – trigger activates only the first time the defining criteria are met. Disable – trigger is disabled.
Logical Device	Specifies the logical device that will be the source of the event.
Device Type	Specifies the device type of the logical device that the trigger will use.
Event Type	Specifies the type of event that will activate the trigger. See "DBC - Event Types" in Chapter 45 for more information about event types.
Event Number	Specifies the number of the event that will activate the trigger. This is optional.
Consecutive Event	When selected, it requires the event to occur multiple times within a specified time interval to execute as a trigger. Consecutive Times—Specifies the number of times the event must occur. Timeout (In Sec)—Specifies, in seconds, the time interval within which the multiple events must occur.
Card Number	Permits a card number to activate a trigger. Only one card number per trigger is allowed. Click the box and enter the number.
Date	Specifies the date the event trigger will start.
Time	Specifies the hour and minute the event trigger will start.

Field	Description
Clearance Code	Indicates that you want an event assigned to a reader with a special clearance code to trigger the procedure. Click the box and select the clearance code. See "Overview" for more information about clearance codes.
Time Zone	Specifies the time interval during which the event trigger starts the procedure. Click the button and select a time zone. See "DBC - Time Zones" in Chapter 57 for more information about time zones.
Company Code	Indicates that you want an event assigned to a specific company card to trigger the procedure. Click the box and select the company code. Use the Key field to search; enter the first letter of the company you want to select.
Pin Code	Indicates that you want a PIN code to activate an event trigger at a specific reader.

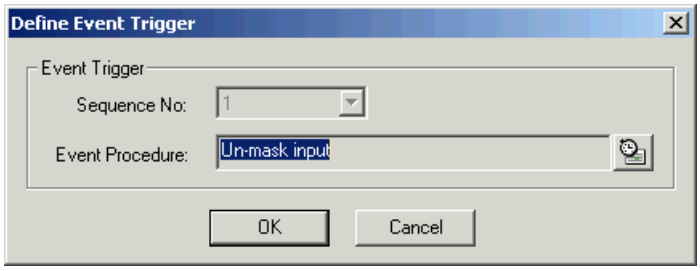
2. Click **OK** to return to the Add Event Trigger Procedures or Edit Event Trigger Procedures dialog box.

44.3.2 Event Trigger Procedures Tab

Use this function to add or edit the procedure that will execute when the alarm occurs.

Follow these steps:

1. To assign, or add, a procedure to an alarm, click Add. To edit a procedure already assigned to an alarm, click the procedure and then click Edit. In both cases, the Define Event Trigger dialog box appears.



2. Enter the sequence number for this procedure. The sequence number specifies the order in which the procedure is executed. For example, a procedure with a sequence number of 2 executes after the procedure

with a sequence number of 1 and before the procedure with a sequence number of 3.

3. Click the icon next to the Event Procedure field, then click **Define.** The Event Procedures dialog box appears.
4. Click the procedure you want, and then click **OK** to return to the Define Event Trigger dialog box.
5. Click **OK** to assign the procedure to the alarm trigger.

44.3.3 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information. Use this function to create, assign or delete a partition:

To create a partition for the event trigger:

1. Click Partitions.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the event trigger:

1. Click Add to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

44.4 Copying an Event Trigger

Use this function to create a copy of an event trigger. This can be a fast way to create a new trigger. If the original trigger will be similar to the new one, you can copy the original and change only a small number of its properties to create the new event trigger.

1. In the Pro-Watch Database Configuration tree list, click the Event Triggers icon to display the currently-configured event triggers in the right pane.
2. Right-click the icon of the event trigger you want to copy, and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original event trigger name]” appears in the right pane.

44.5 Deleting an Event Trigger

1. From the Pro-Watch Pro-Watch Database Configuration tree list, click the Event Triggers icon to display the triggers in the right pane.
2. Right-click the event trigger you want to delete and select **Delete.** The prompt, “Delete the Event Procedure [trigger name]?” appears.
3. Click **Yes**.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Event Types

45

In this chapter ...

Overview

Event Type Functions

Adding or Editing Event Types

Viewing Dependencies of an Event Type

Copying an Event Type

Deleting an Event Type

45.1 Overview

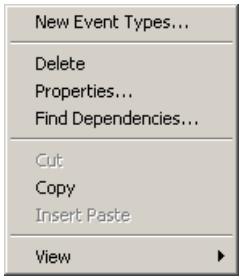
Event types provide instructions on how to handle an event generated in Pro-Watch.

For example, you can create an event type that displays color-coded event message text on the event viewer and plays a sound file on the alarm monitor. Or, you can instruct that the event should “roll over”, or forward, to another workstation.

45.2 Event Type Functions

To access Event Type functions:

1. From the Pro-Watch Database Configuration tree list, click the **Event Types** icon to display the currently-configured types in the right pane of the Pro-Watch window.
2. Right-click an event type icon to display the pop-up menu:



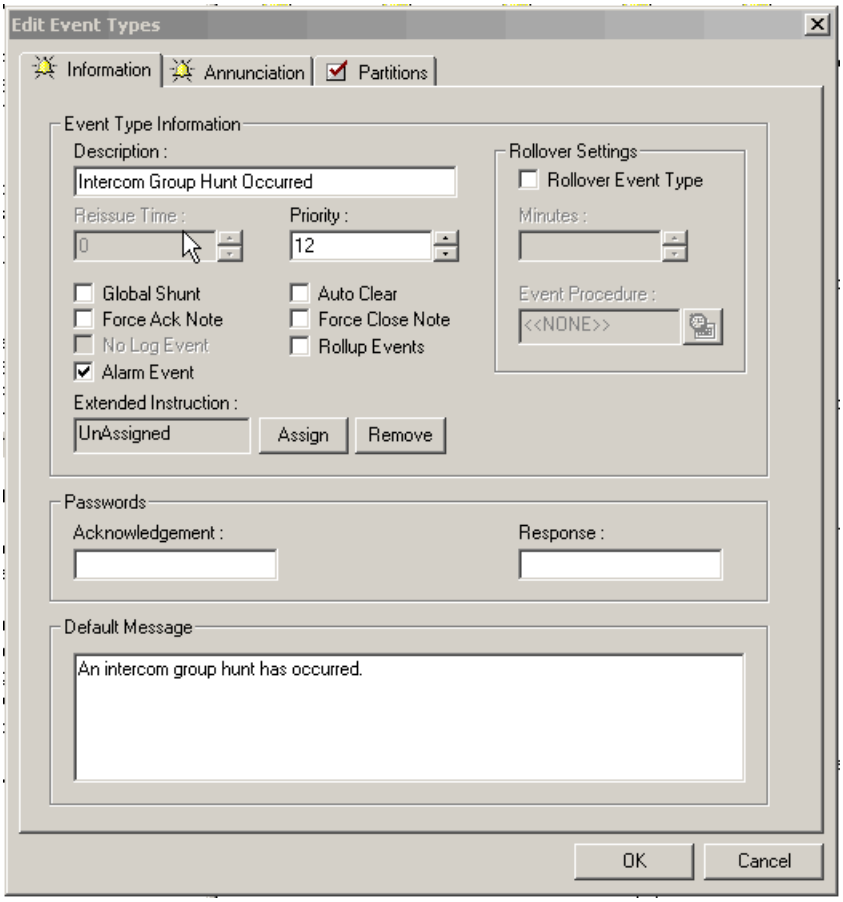
3. Use the following table to select a function:

Click...	To...
New Event Types...	Add a new event type. See "Adding or Editing Event Types".
Delete	Delete a current event type. See "Viewing Dependencies of an Event Type".
Properties...	Edit a current event type. See "Adding or Editing Event Types".
Find Dependencies...	Display the names of all resources that depend upon the event type. See "Viewing Dependencies of an Event Type"
Copy	Copy an event type and insert the copy's icon in the Pro-Watch window. See "Copying an Event Type".
View	Change the way the icons are displayed in the Pro-Watch window.

45.3 Adding or Editing Event Types

1. To ***add*** a new event type, right-click the **Event Types** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select the **New Event Types** icon to display the Add Event Types dialog box.

   To ***edit*** an existing event type, click the **Event Types** icon to display the event types in the right pane. Right-click on the event type you want and select **Properties** to display the Edit Event Types dialog box:



2. Complete the following tab sections to configure the event type:

   EVENT TYPE TABS LIST

   - "Information Tab".

- "Annunciation Tab".
- "Partitions Tab".

45.3.1 Information Tab

1. Use the following field descriptions to complete the Edit Event Types dialog box:

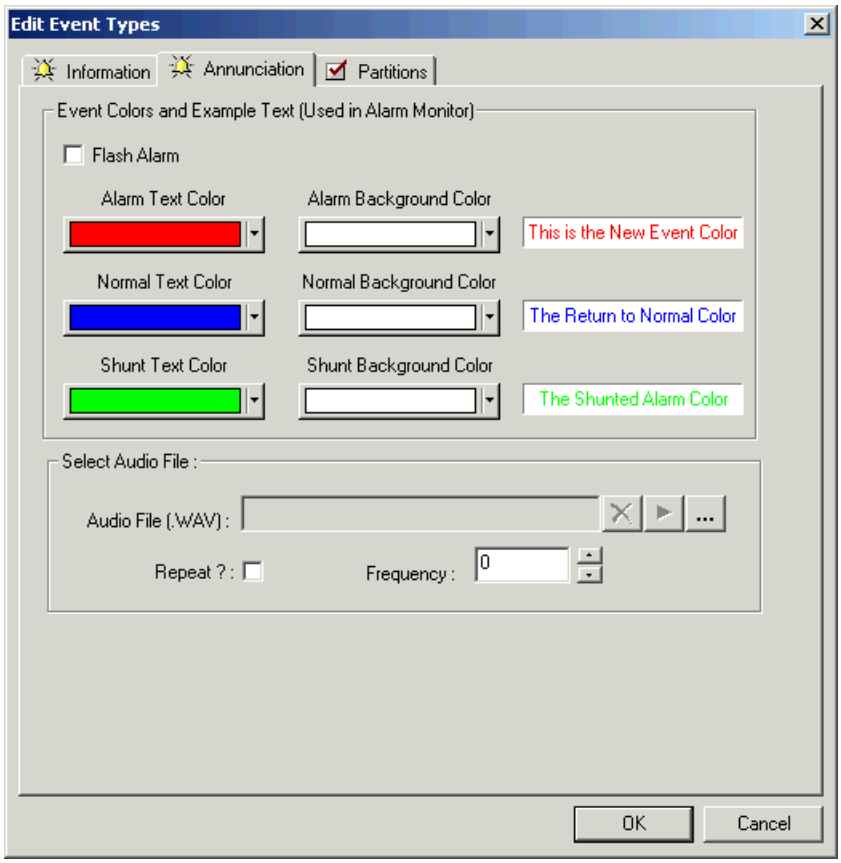
Field	Description
Description	Names the event type.
Reissue Time	This field is not supported in Pro-Watch, Release 3.71.
Priority	Specifies the default alarm priority number. The Alarm Monitor stacks alarms on the screen according to their priority. Priority 1 alarms appear at the top of the screen, priority 2 alarms appear below the priority alarms, and so on. Note that this field only sets the default; the priority assigned in the Edit Point dialog box supersedes the default (see "HW Config - Edit Point" in Chapter 25).
Global Shunt	Prevents any event of this type from being displayed by the Alarm Monitor. It also prevents execution of Event Triggers for this event type.
Force Ack Note	Forces an operator to enter response text before the alarm can be acknowledged in the Alarm Monitor.
No Log Event	Prevents events from being logged.
Alarm Event	Displays the event as an alarm in the Alarm Monitor.
Auto Clear	Automatically clears the alarm from the Alarm Monitor as soon as it is acknowledged.
Force Close Note	Forces an operator to enter response text before the alarm can be cleared in the Alarm Monitor.
Rollup Events	Rolls up multiple events from the same logical device into a single line on the Alarm Monitor.

Field	Description
Extended Instruction	Associates a file of instructions with the event. You can view the instructions from the Alarm Monitor. When the event is viewed on the Alarm Monitor, a link to the instruction file also appears. You can open and view the extended instructions from the Alarm Monitor. To create an extended instruction file: 1. Create a Blob Type. It must be a "Default Events" resource type. De-select "File System Storage." 2. On the Information tab in the Edit Event Types dialog box, click Assign in the Extended Instructions field. Browse for and select the extended instruction file. The file must be either an .html or an .htm file with no embedded images. 3. Open the Alarm Monitor and double-click the alarm event with the extended instructions to display the instructions. If a "Page cannot be displayed" message appears, the file probably contains an image. To disassociate an already-assigned instruction file, click **Remove** at the Extended Instructions field.
Rollover Settings	Instructs Pro-Watch to run the event procedure when the specified event type occurs after the specified amount of time.
Passwords	Requires a password to generate an acknowledgement or response.
Default Message	Displays a message in the Alarm Monitor that describes what has occurred. This message can be overridden on a logical device level.

4. Click the Annunciation tab, and proceed to the next section, Annunciation.

45.3.2 Annunciation Tab

Use this tab to assign colors and audio files to an event type. Colors distinguish alarm, normal, and shunt text and background color, and audio files are available to play in association with an event.



Use the following field descriptions to complete the Annunciation tab:

Field	Description
Flash Alarm	Sets the alarm to flash in the Alarm Monitor.
Alarm Text Color/Alarm Background Color	Sets the color of the alarm text in the Alarm Monitor.
Normal Text Color/Normal Background Color	Sets the color of the regular text in the Alarm Monitor.

Field	Description
Shunt Text Color/Shunt Background Color	Sets the color of the background text.
Audio File (.WAV)	Selects an audio file you specify and enables you to delete or play it. The browse button enables you to search for the file.
Repeat	Sets the Alarm Monitor to repeat the play of the audio file.
Frequency	Sets the frequency of the Alarm Monitor for a playback of the audio file.

To assign partitions to your event types:

Click the **Partitions** tab and proceed to the next section.

If you do not want to assign partitions:

Click **OK** on the Annunciation tab to accept the event type configuration.

45.3.3 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the event type:

1. Click **Partitions**:
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the event type:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

45.4 Viewing Dependencies of an Event Type

Use this function to view a list of an Event Type's current dependencies.

To view and edit ***an Event Type's dependencies****:*

1. Right-click the icon of an existing event type in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Event Type's current dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

45.5 Copying an Event Type

Use this function to create a copy of an event type. This can be a fast way to create a new type. If the original type will be similar to the new one, you can copy the original and change only a small number of its properties to create the new event type.

1. In the Pro-Watch Database Configuration tree list, click the **Event Types** icon to display the currently-configured event types in the right pane.
2. Right-click the icon of the event type you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original event type name]” appears in the right pane.

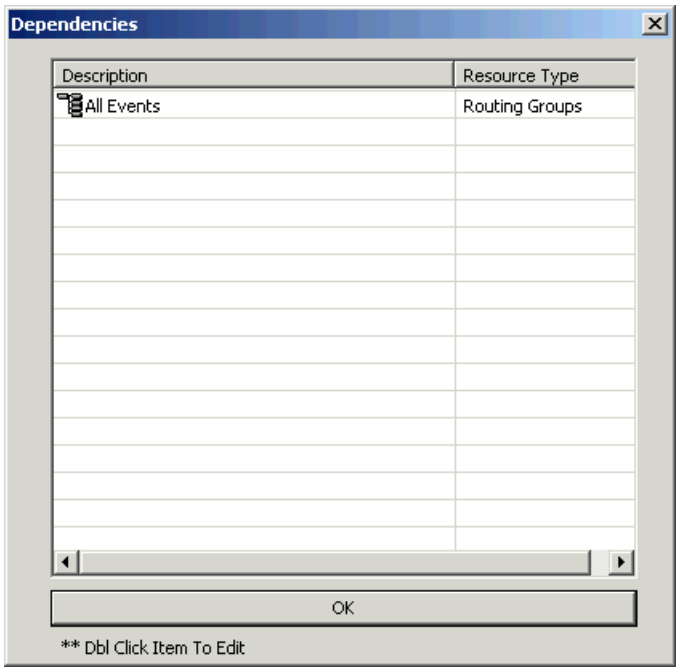
45.6 Deleting an Event Type

To delete an Event Type from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Event Types** icon to display the procedures in the right pane.

Note: Right-click the event type you want to delete and select **Delete**.

You cannot delete a event type until you delete its current dependencies. A dependency is another database object that includes the Event Type in its configuration. For example, the Event Type's dependencies are the Class, User, Routing Group, and Event Trigger objects. If the event type has no current dependencies, you are prompted to confirm the deletion. However, if the event type does have current dependencies, the Dependencies dialog box appears.



2. If you still want to delete the event type:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the event type.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Galaxy User Management

46

In this chapter ...

Overview
Configuration Steps

46.1 Overview

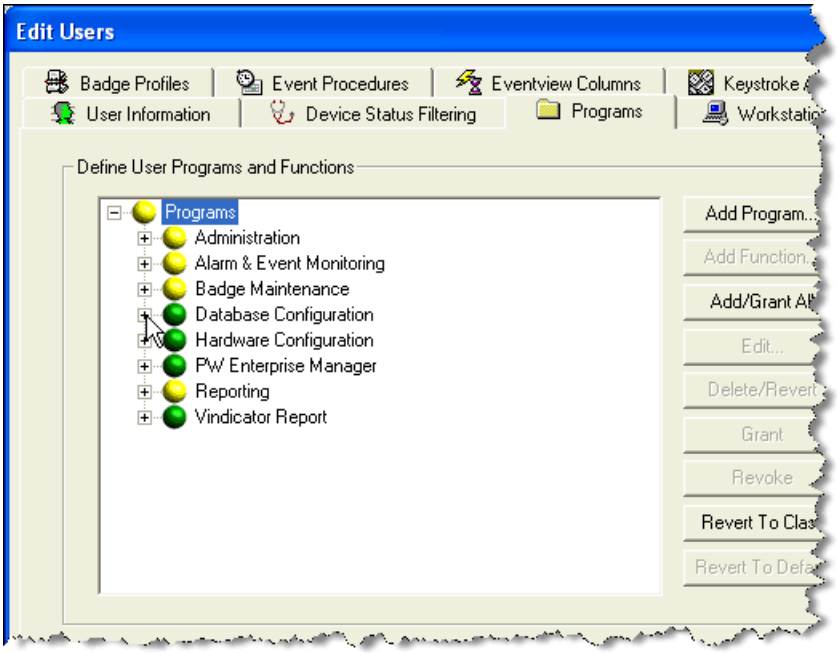
You can configure Galaxy panel users in **Pro-Watch > Database Configuration > Galaxy User Management** as well as in **Pro-Watch > Hardware Configuration** (see "Editing a Galaxy Panel" on page 7). You can change the following Galaxy User tab fields: Menu Access, PIN, Menu Option, Keypad, User Level, Arm/Disarm Group, Card Number, Toggle Action Privileges, Group Choice, and Badge Profiles. All field entry changes are downloaded to the Galaxy panel.

46.2 Configuration Steps

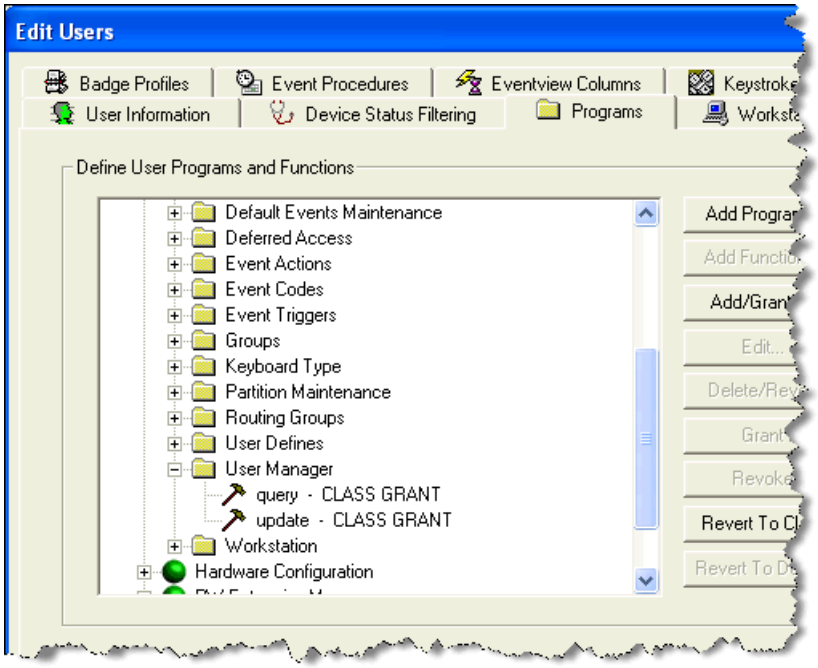
1. Be sure that you have query and update permissions granted:

   a. Go to **Database Configuration > Users**.

   b. Right click the selected user in the right-hand pane, and select **Properties** to display the **Edit Users** screen. Select the **Programs** tab:

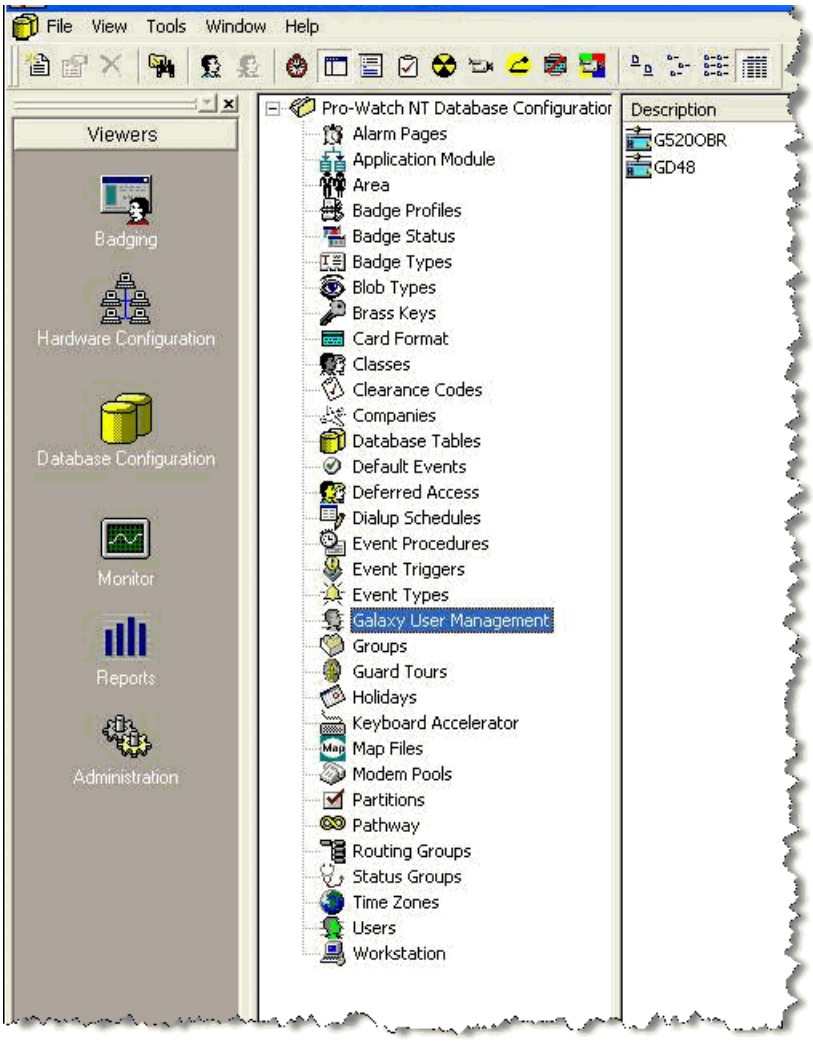


c. Select **Database Configuration**, then click **User Manager**.

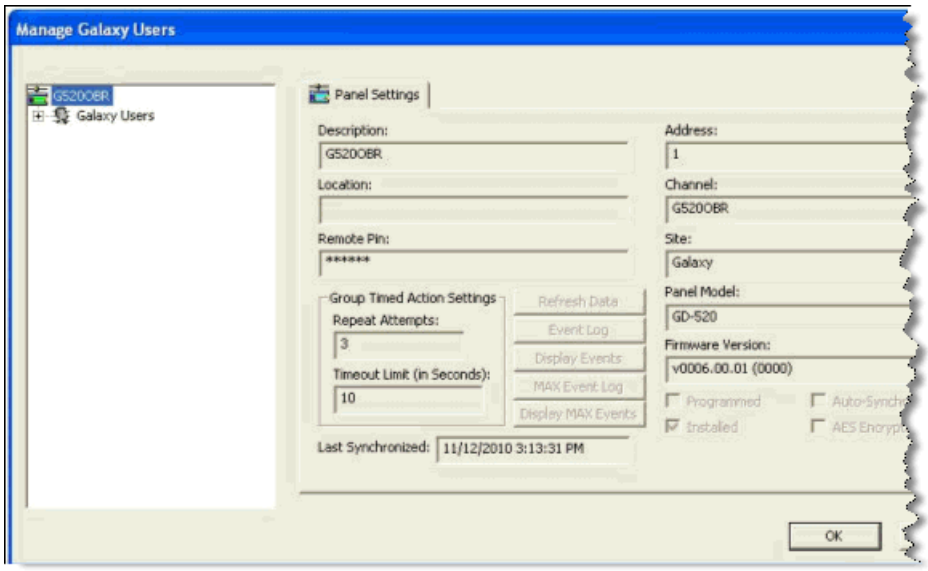


d. Be sure that the query and update permissions are granted, and click **OK**.

2. Return to **Pro-Watch > Database Configuration**.

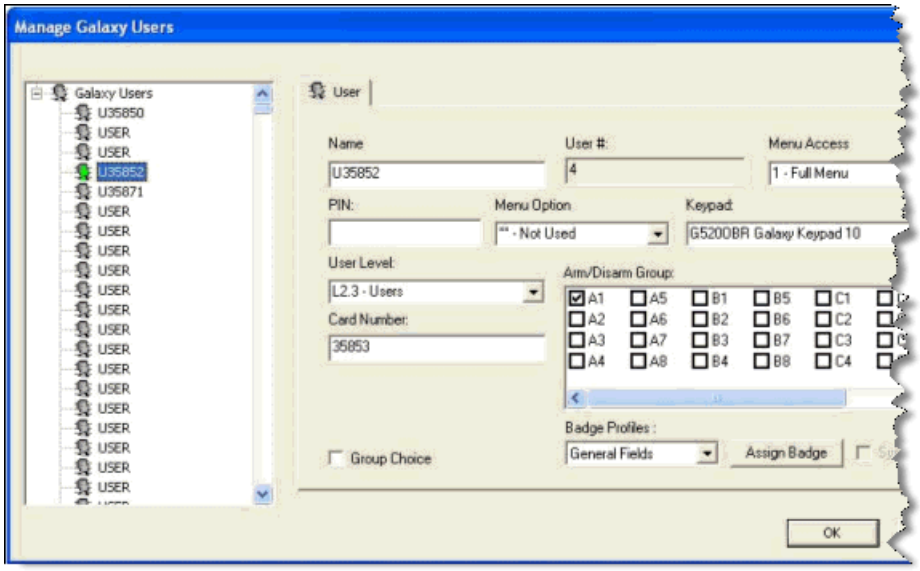


3. Click **Galaxy User Management** to display the **Manage Galaxy Users** screen.



In the left pane of the Manage Galaxy Users screen, each of the configured Galaxy panels is listed, along with a drop-down list of the users of that panel.

4. For the desired panel, click the **Galaxy Users** drop-down list to display the panel's users.



5. Select the appropriate user and either create or edit the user's configuration.
6. Click **OK** to accept the user entries.

Note: Clicking the Assign Badge button creates a link between the user and an existing Pro-Watch card, if there is a number in the Galaxy Card Number field. If there is no number in the Galaxy Card Number field, no link is

created. If there is no existing Pro-Watch card that matches the number in the Galaxy Card Number field, then clicking Assign Badge creates a Pro-Watch badge holder and a Pro-Watch card.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Groups

47

In this chapter ...

Overview

Groups Functions

Adding or Editing Groups

Viewing Dependencies of a Group

Copying a Group

Deleting a Group

47.1 Overview

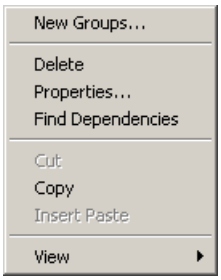
Use this function to group hardware and logical devices together as a single entity.

Example: You can group all outputs to control all enterprise doors for an open house at your enterprise. Or, you can create group that makes it convenient to conduct monthly checks of enterprise hardware categories.

47.2 Groups Functions

To access Groups functions:

1. In the Pro-Watch Database Configuration tree list, click the **Groups icon** to display the currently-configured groups (if there are any) in the right pane of the Pro-Watch window.
2. Right-click an event type icon to display the pop-up menu:



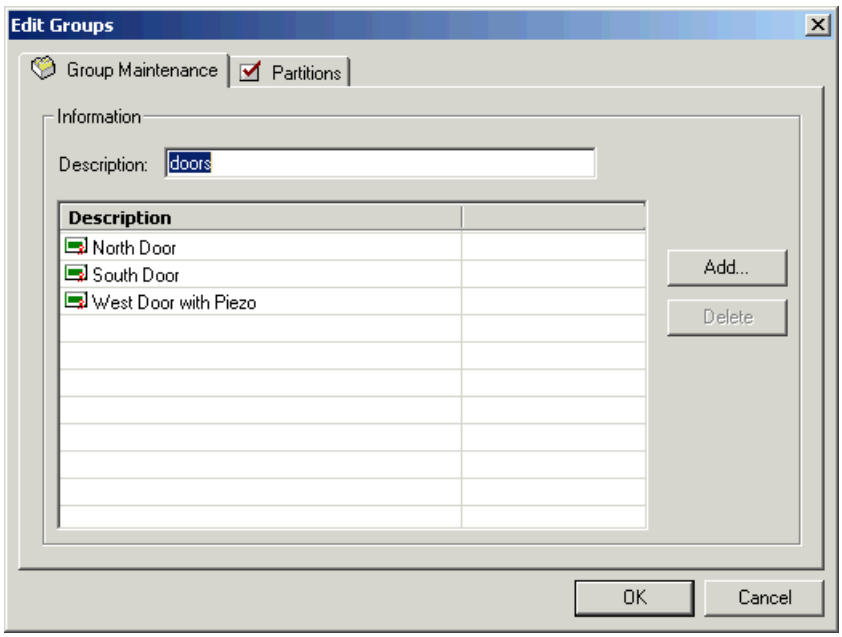
3. Use the following table to select a function:

Click...	To...
New Groups...	Add a new group. See "Adding or Editing Groups".
Delete	Delete a current group. See "Viewing Dependencies of a Group".
Properties...	Edit a current group. See "Adding or Editing Groups".
Find Dependencies	Display the names of all resources that depend upon the group. See "Viewing Dependencies of a Group".
Copy	Copy a group and insert the copy's icon in the Pro-Watch window. See "Copying a Group".
View	Change the way the icons are displayed in the Pro-Watch window.

47.3 Adding or Editing Groups

1. To ***add*** a new group, right-click the **Groups icon** in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Groups** to display the Add Groups dialog box.

   To ***edit*** an existing group, click the **Groups** icon to display the groups in the right pane. Right-click on the group you want and select **Properties** to display the Edit Groups dialog box.



2. Complete the tab sections below to configure the group.

47.3.1 Group Maintenance Tab

1. Enter a description (or edit the current description) that identifies the group in the Description field.
2. To add a logical device to the group, click **Add**. The Logical Devices dialog box appears.
3. Click the logical device you want to add, and click **OK**. The logical device appears on the Group Maintenance tab.
4. To delete a logical device currently in the group, click the device and then click **Delete**. The prompt, “Are you sure you want to delete the selected resources?” appears.
5. Click **Yes** to delete the device.

6. Click **OK** to accept the new group configuration.

47.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for more information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the group:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the group:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

47.4 Viewing Dependencies of a Group

Use this function to view a list of a Group's current dependencies. The Group object depends upon the Clearance Code and Event Procedure objects.

To view and edit ***a Group's dependencies:***

1. Right-click the icon of an existing group in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Group's current dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

47.5 Copying a Group

Use this function to create a copy of an group. This can be a fast way to create a new group. If the original group will be similar to the new one, you can copy the original and change only a small number of its properties to create the new group.

1. In the Pro-Watch Database Configuration tree list, click the **Groups** icon to display the currently-configured groups in the right pane.
2. Right-click the icon of the group you want to copy, and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original group name]” appears in the right pane.

47.6 Deleting a Group

Use this function to delete a Group from the Pro-Watch database:

1. In the Pro-Watch Database Configuration tree list, click the **Groups** icon to display the procedures in the right pane.

Note: Right-click the group you want to delete and select **Delete**.

You cannot delete a group until you delete its current dependencies. A dependency is another database object that includes the Group object in its configuration. For example, a Group object depends upon the Clearance Code and Event Procedure objects. If the group has no current dependencies, you are prompted to confirm the deletion. However, if the group does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the group:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the group.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Guard Tours

48

In this chapter ...

Overview

Guard Tour Functions

Adding or Editing Guard Tours

Viewing Dependencies of a Guard Tour

Copying a Guard Tour

Deleting a Guard Tour

48.1 Overview

A Pro-Watch guard tour creates a facility walk-through that is defined by a series of reader checkpoints. The cardholder, or guard, walks through the facility and presents his card at predefined readers within time windows. Failure to arrive at a checkpoint within the window generates notification to those who must respond.

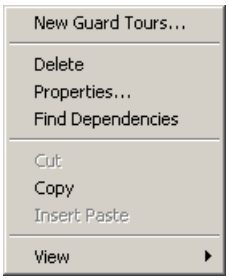
Example: A prison warden follows a guard tour through his cell blocks. If he arrives early or late at a reader, an event is logged to the database and sent to operators who view this information. The operators then takes the appropriate action.

Real-time status of the tour, as indicated by the arrival state of the cardholder at particular points, is also available. Each of the guard tours allows only one cardholder to walk the tour at one time. Also, only cards that are marked “Guard” (see Badging) are eligible to participate.

48.2 Guard Tour Functions

To access Guard Tour functions:

1. In the Pro-Watch Database Configuration tree list, click the **Guard Tours** icon to display the currently-configured tours (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a guard tour icon to display the pop-up menu:



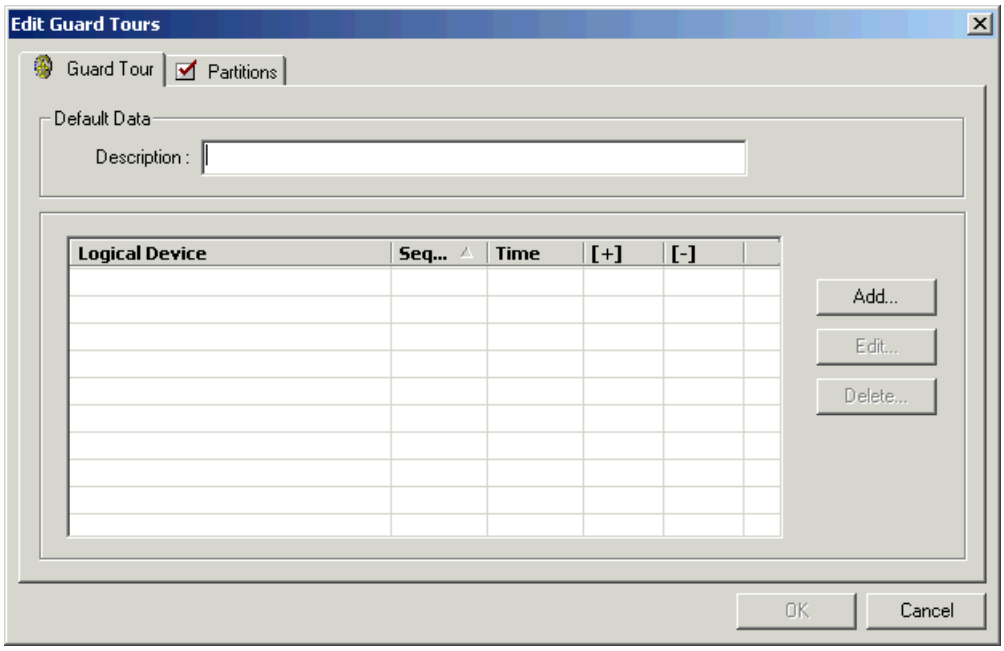
3. Use the following table to select a function:

Click...	To...
New Guard Tours...	Add a new guard tour. See "Adding or Editing Guard Tours".
Delete	Delete a current guard tour. See "Viewing Dependencies of a Guard Tour".
Properties...	Edit a current guard tour. See "Adding or Editing Guard Tours".
Find Dependencies...	Display the names of all resources that depend upon the guard tour. See "Viewing Dependencies of a Guard Tour"
Copy	Copy a guard tour and insert the copy's icon in the Pro-Watch window. See "Copying a Guard Tour".
View	Change the way the icons are displayed in the Pro-Watch window.

48.3 Adding or Editing Guard Tours

1. To ***add*** a new guard tour, right-click the **Guard Tours** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Guard Tours** to display the Add Guard Tours dialog box.

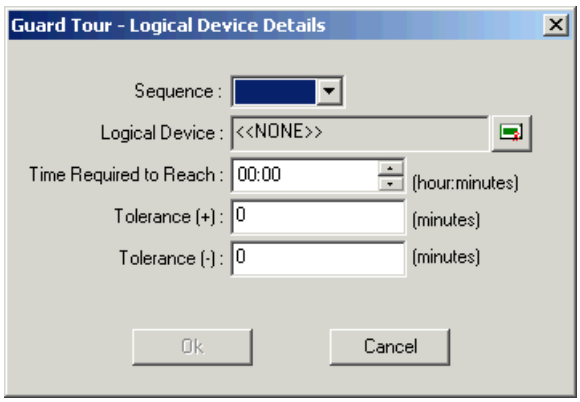
   To ***edit*** an existing guard tour, click the **Guard Tours** icon to display the guard tours in the right pane. Right-click on the guard tour you want and select **Properties** to display the Edit Guard Tours dialog box.



2. Complete the tab sections below to configure the guard tour.

48.3.1 Guard Tour Tab

1. Enter a description (or edit the current description) that identifies the guard tour in the Description field.
2. To add a logical device to the guard tour, click **Add**. The Logical Device Details dialog box appears.



3. Enter a sequence from the Sequence drop-down box. The sequence number specifies the order in which the device is visited during the tour. For example, sequence 1 means the device is visited first, sequence 2 means the device is visited second, and so on.
4. Click the button next to the Logical Device field, and then click **Define**, to select the device(s) for the tour. The Logical Devices dialog box appears.

Note: Click the device you want and click OK. The device name appears in the Logical Device Details dialog box.

If you want to edit the configuration of the logical device you have selected, click the button next to the Logical Device field again, and click Edit Current Logical Devices. See "HW Config - PW-6000/5000/3000" in Chapter 9 for information about completing the Edit Logical Devices dialog box.

5. Enter the time required for the guard to reach the logical device from the previous device checkpoint. Note that the time does not need to be exact. In the next steps, you can specify plus and minus tolerances.
6. Enter a plus tolerance in minutes. This is the number of minutes by which the guard can exceed the time you specified in the “Time Required to Reach,” field in the previous step. If the guard exceeds the tolerance number you enter here, someone is notified.
7. Enter a minus tolerance in minutes. This is the number of minutes by which the guard can precede the time you specified in the “Time

Required to Reach," field. If the guard arrives at the device earlier than the minus tolerance, someone is notified.

8. Click **OK** at the Logical Device Details dialog box. The device appears in the Add/Edit Guard Tours dialog box as a guard checkpoint.

48.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the guard tour:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the guard tour:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

48.4 Viewing Dependencies of a Guard Tour

In Pro-Watch, the Guard Tour object depends upon the Event Trigger object.

To view and edit ***a Guard Tour's dependencies:***

1. Right-click the icon of an existing Guard Tour in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Guard Tour's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

48.5 Copying a Guard Tour

Use this function to create a copy of a guard tour. This can be a fast way to create a new tour. If the original guard tour will be similar to the new one, you can copy the original and change only a small number of its properties to create the new tour.

1. In the Pro-Watch Database Configuration tree list, click the **Guard Tours** icon to display the currently-configured tours in the right pane.
2. Right-click the icon of the guard tour you want to copy, and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original tour name]” appears in the right pane.

48.6 Deleting a Guard Tour

Use this function to delete a Guard Tour object from the Pro-Watch database:

1. In the Pro-Watch Database Configuration tree list, click the **Guard Tours** icon to display the procedures in the right pane.

Note: Right-click the Guard Tour you want to delete and select Delete.

You cannot delete a Guard Tour until you delete its current dependencies. A dependency is another database object that includes the Guard Tour object in its configuration. For example, the Guard Tour object depends upon the Event Trigger object. If the Guard Tour has no dependencies, you are prompted to confirm the deletion. However, if the Guard Tour does have dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Guard Tour:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Guard Tour.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Holidays

49

In this chapter ...

Overview

Holiday Functions

Adding or Editing Holidays

Viewing Dependencies of a Holiday

Copying a Holiday

Deleting a Holiday

49.1 Overview

Use this function to modify normal Time Zone behavior on a particular day. You can define related holiday information to enable the connected panels to modify access for the day(s) on which the holiday falls.

Example: If your enterprise is scheduled to restrict access into the building on Christmas, you can apply the holiday to a unique time zone to accommodate the modified schedule.

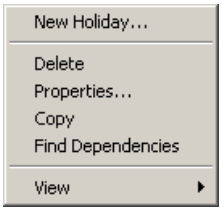
49.1.1 A Note on Holiday Icons

Note: Holiday icons appear in either green or red. A green icon indicates a holiday date that has not yet arrived. A red icon indicates a holiday date that has expired.

49.2 Holiday Functions

To access Holiday functions:

1. In the Pro-Watch Database Configuration tree list, click the **Holidays** icon to display the currently-configured holidays (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a holiday icon to display the pop-up menu:



3. Use the following table to select a function:

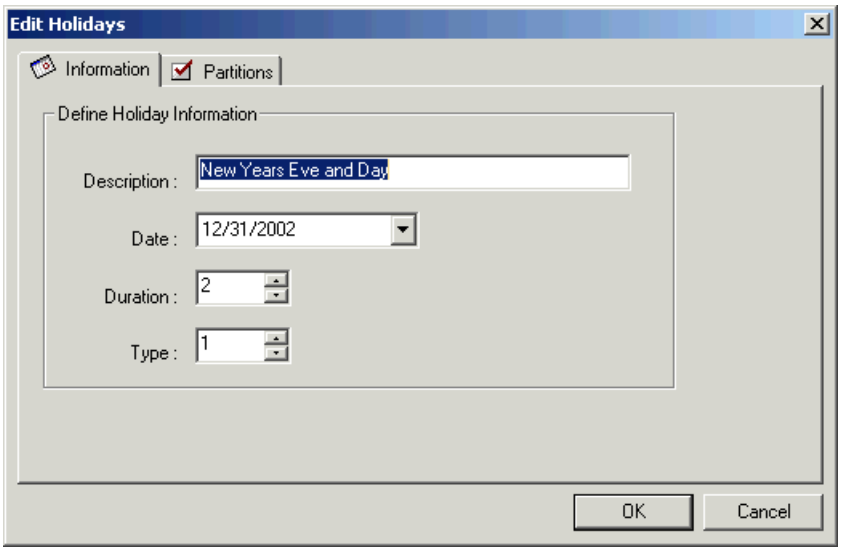
Click...	To...
New Holidays...	Add a new holiday. See "Adding or Editing Holidays".
Delete	Delete a current holiday. See "Viewing Dependencies of a Holiday".
Properties...	Edit a current holiday. See "Adding or Editing Holidays".
Find Dependencies	Display the names of all resources that depend upon the holiday.
Copy	Copy a holiday and insert the copy's icon in the Pro-Watch window. See "Copying a Holiday".
View	Change the way the icons are displayed in the Pro-Watch window.

49.3 Adding or Editing Holidays

Note: When editing a holiday, the Pro-Watch prompts for the appropriate digital signature(s) and the appropriate information post-edit, if the holiday is a member of a secured panel. Holidays tied to more than one secure panel uses the aggregated panels's most restrictive settings.

1. To ***add*** a new holiday, right-click the **Holidays** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Holidays** to display the Add Holidays dialog box.

   To ***edit*** an existing holiday, click the **Holidays** icon to display the holidays in the right pane. Right-click on the holiday you want and select **Properties** to display the Edit Holidays dialog box.



2. Complete the tab sections below to configure the holiday:

49.3.1 Information Tab

1. Enter a description (or edit the current description) that identifies the holiday in the Description field.
2. Enter the date of the holiday in the Date field. Note that at the start of each new year, you must update the year in the Date field.
3. Enter the duration of the holiday as a number of days.
4. Enter the holiday type. The holiday type is a numeric, 1-3. The type is for operator information only and has no effect on the operation of the

panel. That is, you can define three different holiday types (such as government, cultural, company, etc.) and designate a number to each.

49.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the holiday:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want. See "DBC - Partitions" in Chapter 53 for an explanation of partitions.
3. Click **OK** to accept the partition.

To assign a partition to the holiday:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

49.4 Viewing Dependencies of a Holiday

Use this function to view and edit the Pro-Watch object dependencies upon the Holiday object. The Holiday object depends upon the Panel object.

*To view and edit **a Holiday's dependencies**:*

1. Right-click the icon of an existing holiday in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the holiday's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

49.5 Copying a Holiday

Use this function to create a copy of a holiday. This can be a fast way to create a new holiday. If the original holiday will be similar to the new one, you can copy the original and change only a small number of its properties to create the new holiday.

1. In the Pro-Watch Database Configuration tree list, click the **Holidays** icon to display the currently-configured holidays in the right pane.
2. Right-click the icon of the holiday you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original holiday name]” appears in the right pane.

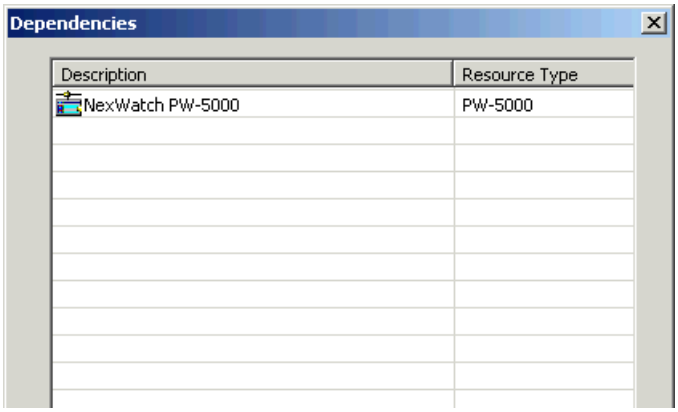
49.6 Deleting a Holiday

Use this function to delete a Holiday from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Holidays** icon to display the procedures in the right pane.

Note: Right-click the holiday you want to delete and select **Delete**.

You cannot delete a holiday that has dependencies. A dependency is another database object that includes the holiday in its configuration. The Holiday object depends up on the Panel object. If the holiday has no dependencies, you are prompted to confirm the deletion. However, if the holiday does have dependencies, the Dependencies dialog box appears.



2. If you still want to delete the holiday:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the holiday.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Keyboard Accelerator

50

In this chapter ...

Overview

Keyboard Accelerator Functions

Adding or Editing Keyboard Accelerators

Viewing Dependencies of a Keyboard Accelerator

Copying a Keyboard Accelerator

Deleting a Keyboard Accelerator

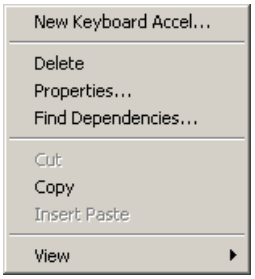
50.1 Overview

Use this function to configure a shortcut key, or a hot-key combination, that executes commands and event procedures. These keyboard accelerators execute only in the Alarm Monitor.

50.2 Keyboard Accelerator Functions

To access Keyboard Accelerator functions:

1. From the Pro-Watch Database Configuration tree list, click the **Keyboard Accelerator** icon to display the currently-configured keyboard accelerators (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a keyboard accelerator icon to display the pop-up menu:



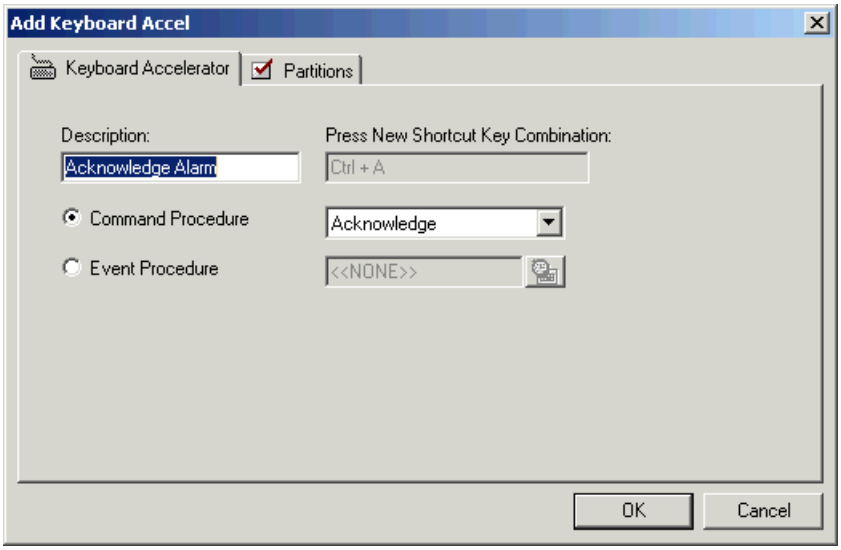
3. Use the following table to select a function:

Click...	To...
New Keyboard Accelerator...	Add a new keyboard accelerator. See "Adding or Editing Keyboard Accelerators".
Delete	Delete a current keyboard accelerator. See "Viewing Dependencies of a Keyboard Accelerator".
Properties...	Edit a current keyboard accelerator. See "Adding or Editing Keyboard Accelerators".
Find Dependencies...	Display the names of all resources that depend upon the keyboard accelerator. See "Viewing Dependencies of a Keyboard Accelerator".
Copy	Copy a keyboard accelerator and insert the copy's icon in the Pro-Watch window. See "Copying a Keyboard Accelerator".
View	Change the way the icons are displayed in the Pro-Watch window.

50.3 Adding or Editing Keyboard Accelerators

1. To ***add*** a new keyboard accelerator, right-click the **Keyboard Accelerator** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Keyboard Accelerator** to display the Add Keyboard Accelerator dialog box.

   To ***edit*** an existing keyboard accelerator, click the **Keyboard Accelerator** icon to display the keyboard accelerators in the right pane. Right-click on the keyboard accelerator you want and select **Properties** to display the Edit Keyboard Accelerator dialog box.



2. Complete the tab sections below to configure the keyboard accelerator:

50.3.1 Keyboard Accelerator Tab

1. Enter a description (or edit the current description) that uniquely identifies the keyboard accelerator in the Description field.
2. Enter the key combination you want to use. Hold down the SHIFT, CTRL, or ALT key and press a second key.
3. Select either Command Procedure or Event Procedure and enter the key combination that will launch one of the following:
   - Acknowledge – acknowledges the selected alarm.
   - Alarm Respond – produces a dialog box with alarm response options.
   - Alarm Text – displays message text associated with the alarm.
   - Clear Alarm – clears the alarm.

- Picture – displays a photograph of the card holder (if any) associated with the alarm.
- Pop Door Dialog – produces a dialog box from which you can open a door of your choice.
- Pop Selected Door – opens the currently-selected door.
- Silence – silences the selected alarm signal.
- Void Card Dialog – opens a dialog box that enables you to void the card.

4. If you selected Command Procedure, select the procedure from the drop-down box. If you selected Event Procedure, click the icon and then click **Define** to display a list of available procedures. Either:
   - Click an available procedure and click **OK** to accept.
   - Click **Add**, and then click **Add** again to create a new procedure.
   - Click an available procedure and click **Edit** to re-configure the procedure.
   - Click an available procedure and click **Delete** to delete the procedure from the availability list.
   - Click an available procedure and click **Copy** to make a copy of the procedure.
5. If you either added a new procedure or modified an existing procedure, select the procedure you want from the Event Procedures dialog box, and click **OK**. The Add Keyboard Accelerator dialog box appears.
6. Click **OK** to create the keyboard accelerator.
7. Assign the keyboard accelerator to either a class or a user.

Note: After you create a keyboard accelerator, you must assign it to either a class or to a user to make it operative. See "Keystroke Accelerators Tab" in "DBC - Classes" in Chapter 36 or "Keystroke Accelerators Tab" in "DBC - Users" in Chapter 58 for instructions.

50.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition.

Use this function to create, assign or delete a partition:

To create a partition for the keyboard accelerator:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the keyboard accelerator:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

50.4 Viewing Dependencies of a Keyboard Accelerator

Use this function to view and edit the Keyboard Accelerator's dependencies. The Keyboard Accelerator object depends upon the Class and User objects.

*To view and edit **a** Keyboard Accelerator's **dependencies**:*

1. Right-click the icon of an existing keyboard accelerator in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the keyboard accelerator's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

50.5 Copying a Keyboard Accelerator

Use this function to create a copy of a keyboard accelerator. This can be a fast way to create a new keyboard accelerator. If the original accelerator will be similar to the new one, you can copy the original and change only a small number of its properties to create the new accelerator.

1. In the Pro-Watch Database Configuration tree list, click the **Keyboard Accel** icon to display the currently-configured keyboard accelerators in the right pane.
2. Right-click the icon of the accelerator you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original accelerator name]” appears in the right pane.

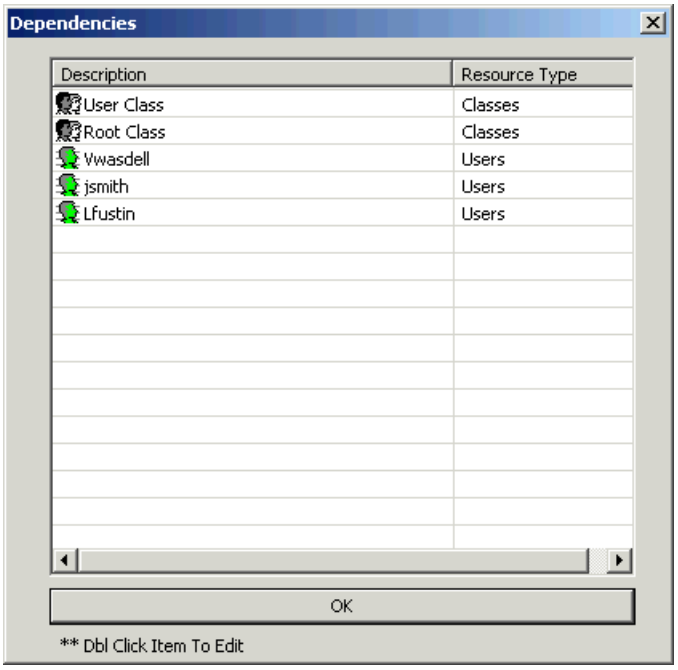
50.6 Deleting a Keyboard Accelerator

Use this function to delete a Keyboard Accelerator from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Keyboard Accelerator** icon to display the icons of the existing keyboard accelerators in the right pane.

Note: Right-click the keyboard accelerator you want to delete and select **Delete**.

You cannot delete a keyboard accelerator that has dependencies. A dependency is another database object that includes the keyboard accelerator in its configuration. The Keyboard Accelerator object depends upon the Class and User objects. If the keyboard accelerator has no dependencies, you are prompted to confirm the deletion. However, if the keyboard accelerator does have dependencies, the Dependencies dialog box appears.



2. If you still want to delete the keyboard accelerator:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the keyboard accelerator.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Maps

51

In this chapter ...

Overview

Maps Functions

Adding or Editing Maps

Viewing Dependencies of a Map

Copying a Map

Deleting a Map

51.1 Overview

Use this function to view maps that display the location of channels, panels, input/output points, readers, or cameras installed in the enterprise. The maps also display the state and condition of alarm points in the enterprise.

Notes:

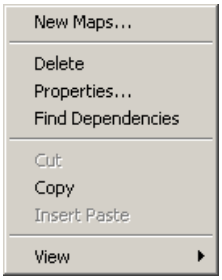
- You must first create a shared Map file folder on the server. In the folder **Properties** tab, grant full control rights to all users. You may need to select users individually to grant them access. Then, you must be sure to change the path of each BLOB to point to this new folder.
- Maps can be created in the Map Builder utility as well. See Chapter 61, *Map Building* for instructions and information about creating maps. A list of all existing maps, whether they are created in the Database Configuration module or through the Map Builder utility, will be displayed both in the Database Configuration and the Map Builder screens.

Tip: You can attach and detach logical devices to and from a map only in the Map Builder utility.

51.2 Maps Functions

To access the Maps functions:

1. In the Pro-Watch Database Configuration tree list, click the **Maps** icon to display the currently-configured maps (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a map icon to display the pop-up menu:



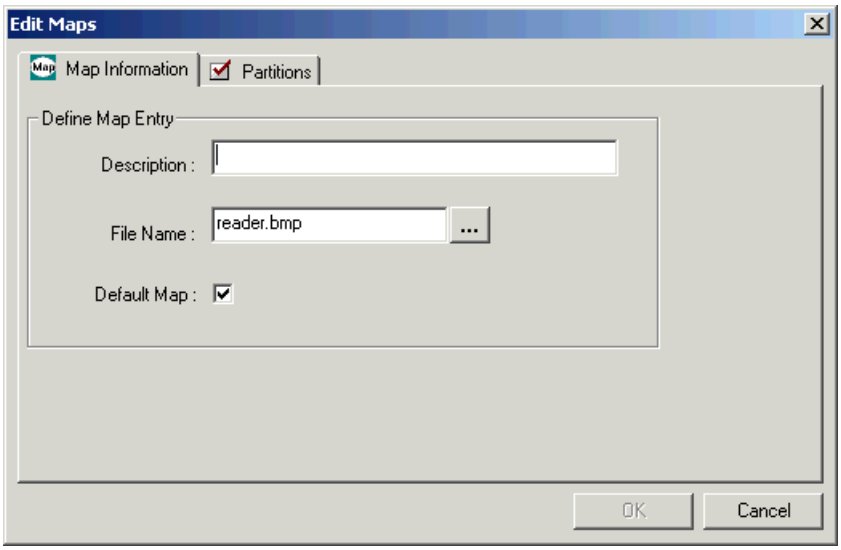
3. Use the following table to select a function:

Click...	To...
New Map...	Add a new map. See "Adding or Editing Maps".
Delete	Delete a current map. See "Viewing Dependencies of a Map".
Properties...	Edit a current map. See "Adding or Editing Maps".
Find Dependencies	Display the names of all resources that depend upon the map. See "Viewing Dependencies of a Map".
Copy	Copy a map and insert the copy's icon in the Pro-Watch window. See "Copying a Map".
View	Change the way the icons are displayed in the Pro-Watch window.

51.3 Adding or Editing Maps

1. To add a new map, right-click the **Maps** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Map** to display the Add Maps dialog box.

   To edit an existing map, click the **Maps** icon to display the maps in the right pane. Right-click on the map you want and select **Properties** to display the **Edit Maps** dialog box.



2. Complete the tab sections below to configure the map:

51.3.1 Map Information Tab

1. On the Add Maps or Edit Maps dialog box, enter a description (or edit the current description) that identifies the map. For example, “Terminal A” would identify a map of that terminal’s access configuration.
2. Enter the name of the map file. To browse for the file, click the button to display the Select Image File dialog box. Select a file from the default directory, and then click **Open** to display the Add Maps dialog box or Edit Maps dialog box. Or, browse for the file from the drop-down list.
3. Click the **Default Map** check box to produce a check mark in the box if you want this map to be used as the default map for your facility’s Pro-Watch configuration. Leave the box unchecked if this map should not be the default map.

4. Click **OK** on the Add Maps or Edit Maps dialog box to accept the map configuration.

51.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the map:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the map:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

51.4 Viewing Dependencies of a Map

Use this function to view and edit the map's dependencies. The Map object depends upon the Alarm Page object.

*To view and edit **a Map's dependencies**:*

1. Right-click the icon of an existing map in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the map's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

51.5 Copying a Map

Use this function to create a copy of a map. This can be a fast way to create a new map.

If the original map will be similar to the new one, you can copy the original and change only a small number of its properties to create the new map.

1. In the Pro-Watch Database Configuration tree list, click the **Maps** icon to display the currently-configured maps in the right pane.
2. Right-click the icon of the map you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original map name]” appears in the right pane.

51.6 Deleting a Map

Use this function to delete a Map from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click **Maps** to display the Map icons in the right pane.
2. Right-click the map you want to delete and select **Delete**. Note that you cannot delete a map that has dependencies. A dependency is another database object that includes the map in its configuration. The Map object depends upon the Alarm Page object. If the map has no dependencies, you are prompted to confirm the deletion. However, if the map does have dependencies, the Dependencies dialog box appears.
3. If you still want to delete the map:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
4. Repeat step 2 and click **Yes** at the prompt to delete the map.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Modem Pools

52

In this chapter ...

Overview

Modem Pools Functions

Adding or Editing Modem Pools

Copying a Modem Pool

Viewing Dependencies of a Modem Pool

Deleting a Modem Pool

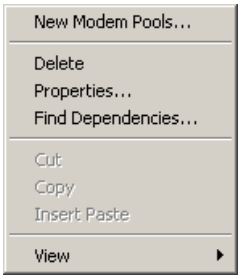
52.1 Overview

Use this function to create collections of modems (that is, “modem pools”) from which Pro-Watch chooses to dial out to remote panels.

52.2 Modem Pools Functions

To access the Modem Pools functions:

1. In the Pro-Watch Database Configuration tree list, click the **Modem Pools** icon to display the currently-configured modem pools (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a modem pool icon to display the pop-up menu:



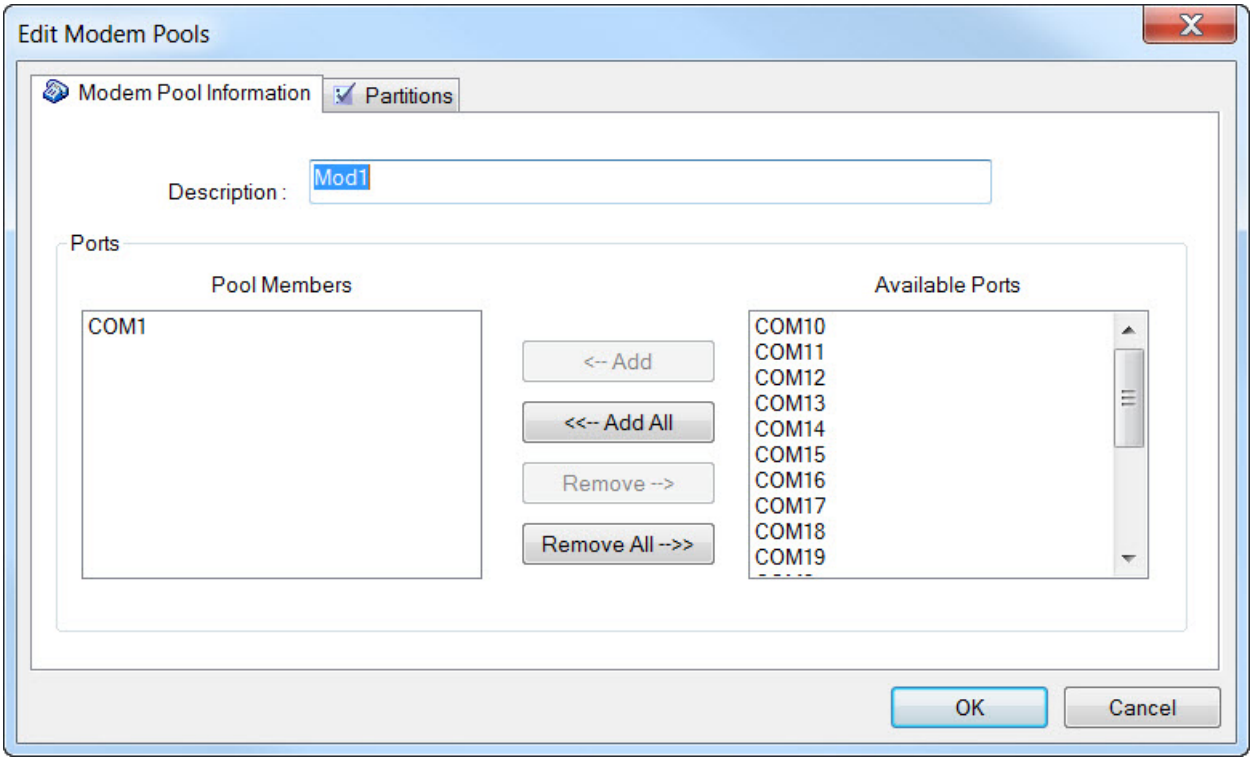
3. Use the following table to select a function:

Click...	To...
New Modem Pools...	Add a new modem pool. See "Adding or Editing Modem Pools".
Delete	Delete a current modem pool. See "Copying a Modem Pool".
Properties...	Edit a current modem pool. See "Adding or Editing Modem Pools".
Find Dependencies...	Display the names of all resources that depend upon the modem pool. See "Viewing Dependencies of a Modem Pool".
Copy	Copy a modem pool and insert the copy's icon in the Pro-Watch window. See "Copying a Modem Pool".
View	Change the way the icons are displayed in the Pro-Watch window.

52.3 Adding or Editing Modem Pools

1. To add a new modem pool, right-click the **Modem Pools** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Modem Pools** to display the Add Modem Pools dialog box.

   To edit an existing modem pool, click the **Modem Pools** icon to display the modem pools in the right pane. Right-click on the modem pool you want and select **Properties** to display the Edit Modem Pools dialog box:



2. Complete the tab sections below to configure the modem pool.

52.3.1 Modem Pool Information Tab

1. On the Add Modem Pools or Edit Modem Pools dialog box, enter a description (or edit the current description) that identifies the modem pool.
2. Add the desired ports to the Pool Members window by selecting the available ports from the Available Ports window and clicking **Add** or **Add All**. To remove ports from the Pool Members window, click the ports and then click **Remove** or **Remove All**.

3. Click **OK** to accept the modem pool.

52.3.2 Partitions Tab

Partitions determine the view of the resources within Pro-Watch. If a resource is not partitioned, all users can view it. If a user or class has no partition assigned, the user or class can view all resources, regardless of whether the resource is partitioned.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the modem pool:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the modem pool:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

52.4 Copying a Modem Pool

Use this function to create a copy of a modem pool. This can be a fast way to create a new modem pool. If the original modem pool will be similar to the new one, you can copy the original and change only a small number of its properties to create the new modem pool.

1. In the Pro-Watch Database Configuration tree list, click the **Modem Pools** icon to display the currently-configured modem pools in the right pane.
2. Right-click the icon of the modem pool you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original modem pool name]” appears in the right pane.

52.5 Viewing Dependencies of a Modem Pool

A Modem Pool can be dependent upon other resources. For example, a user class and its access limits could be a dependency on a Modem Pool.

To view and edit ***a Modem Pool's dependencies***

1. To view the system components (i.e. "dependencies") that depend on a Modem Pool, right-click the icon of an existing Modem Pool in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Modem Pool's dependencies.

   This is a view-only screen that gives you an idea about the system components that you may need to go back and re-configure if you, for example, decide to delete that specific Modem Pool.

2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.

3. After you finish viewing, click **OK** to close the dialog box.

52.6 Deleting a Modem Pool

Use this function to delete a Modem Pool from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click **Modem Pools** to display the Modem Pool icons in the right pane.

Note: Right-click the Modem Pool you want to delete and select **Delete**.

You cannot delete a Modem Pool that has dependencies. A dependency is another database object that includes the Modem Pool in its configuration. The Modem Pool object depends upon the Channel object. If the Modem Pool has no dependencies, you are prompted to confirm the deletion. However, if the Modem Pool does have dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Modem Pool:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Modem Pool.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC - Partitions

53

In this chapter ...

Overview

Partitions Functions

Adding or Editing Partitions

Viewing Dependencies of a Partition

Copying a Partition

Deleting a Partition

53.1 Overview

Use this function to create a partition, which restricts user and class access to database resources that you designate.

Note: If a resource is not partitioned, all users can access it.

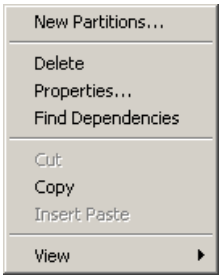
Example: In a building with multiple tenants, you may not want the tenants on floor 1 to have access to the resources (users, sites, badges, etc.) of floor 2 and vice versa.

Before the partition can effectively restrict access to a particular database resource (such as a workstation), however, you must assign the partition to either a class or a user after you create the partition. See "Partitions Tab" in "DBC - Classes" in Chapter 36 or "Partitions Tab" in "DBC - Users" in Chapter 58 for instructions.

53.2 Partitions Functions

To access Partitions functions:

1. In the Pro-Watch Database Configuration tree list, click the **Partitions** icon to display the currently-configured partitions (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a partition icon to display the pop-up menu:



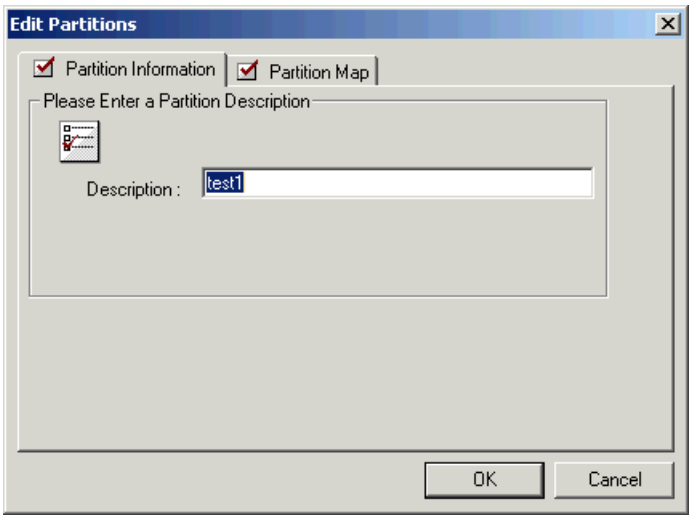
3. Use the following table to select a function:

Click...	To...
New Partitions...	Add a new partition. See "Adding or Editing Partitions".
Delete	Delete a current partition. See "Viewing Dependencies of a Partition".
Properties...	Edit a current partition. See "Adding or Editing Partitions".
Find Dependencies	Display the names of all resources that depend upon the partition. See "Viewing Dependencies of a Partition".
Copy	Copy a partition and insert the copy's icon in the Pro-Watch window. See "Copying a Partition".
View	Change the way the icons are displayed in the Pro-Watch window.

53.3 Adding or Editing Partitions

1. To ***add*** a new partition, right-click the **Partitions** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Partitions** to display the Add Partitions dialog box.

   To ***edit*** an existing partition, click the **Partitions** icon to display the partitions in the right pane. Right-click on the partition you want and select **Properties** to display the Edit Partitions dialog box:



2. Complete the tab sections below to configure the partition:

53.3.1 Partition Information Tab

1. On the Add Partitions or Edit Partitions dialog box, enter a unique description (or edit the current description) that identifies the partition.
2. Click **OK** to create the partition. You can now assign resources to this partition in the resource's own dialog box.

53.3.2 Partition Map Tab

This tab lists all of the resources included in this partition.

To delete a resource from the partition:

1. Click the resource.
2. Click **Delete**.
3. Click **OK**.

53.4 Viewing Dependencies of a Partition

Use this function to view and edit the Partition's dependencies. The Partition object depends upon most Pro-Watch objects.

To view and edit ***a Partition's dependencies****:*

1. Right-click the icon of an existing Partition in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Partition's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

53.5 Copying a Partition

Use this function to create a copy of a partition. This can be a fast way to create a new partition. If the original partition will be similar to the new one, you can copy the original and change only a small number of its properties to create the new partition.

1. In the Pro-Watch Database Configuration tree list, click the **Partitions** icon to display the currently-configured partitions in the right pane.
2. Right-click the icon of the partition you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original partition name]” appears in the right pane.

53.6 Deleting a Partition

Use this function to delete a Partition from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click **Partitions** to display the Partition icons in the right pane.

Note: Right-click the Partition you want to delete and select **Delete**.

You cannot delete a Partition that has dependencies. A dependency is another database object that includes the Partition in its configuration. The Partition object depends upon most Pro-Watch objects. If the Partition has no current dependencies, you are prompted to confirm the deletion. However, if the Partition does have dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Partition:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Partition.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC - Pathways

54

In this chapter ...

Overview

Pathway Functions

Adding or Editing Pathways

Viewing Dependencies of a Pathway

Deleting a Pathway

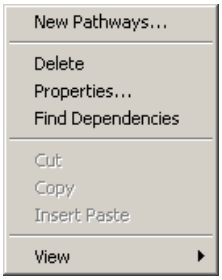
54.1 Overview

Use this function to enable personnel to bypass designated security checkpoints after gaining initial access. The card holder inserts her card upon entering the building and enjoys unchecked access at designated access points (a pathway) until exiting the building.

54.2 Pathway Functions

Follow these steps:

1. In the Pro-Watch Database Configuration tree list, click the **Pathways** icon to display the currently-configured pathways (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a pathway icon to display the pop-up menu:



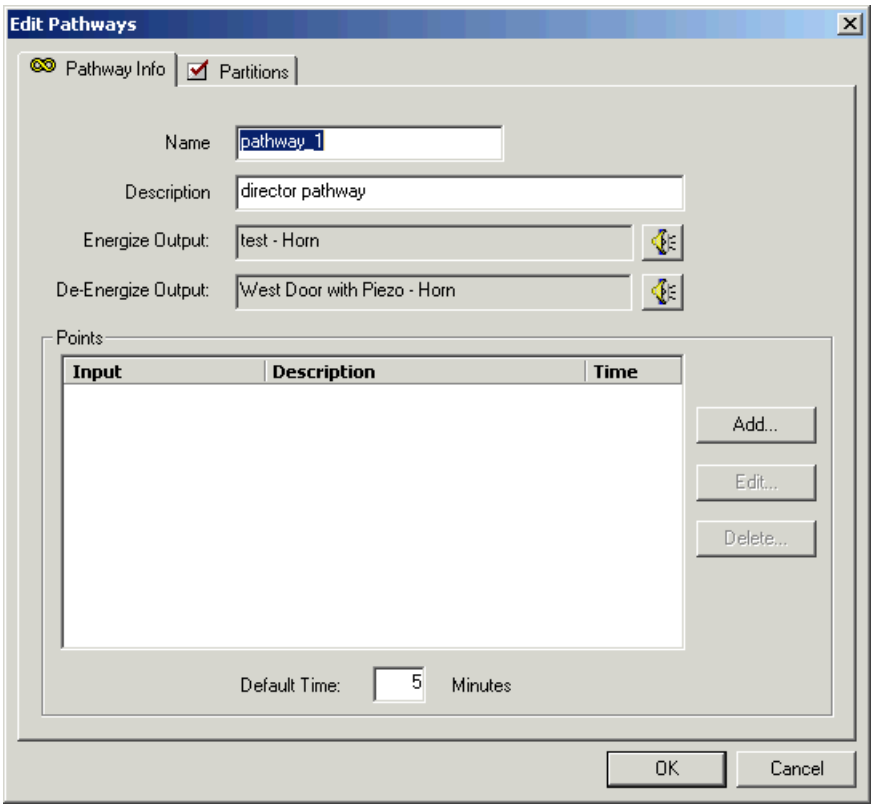
3. Use the following table to select a function:

Click...	To...
New Pathways...	Add a new pathway. See "Adding or Editing Pathways".
Delete	Delete a current pathway. See "Viewing Dependencies of a Pathway".
Properties...	Edit a current pathway. See "Adding or Editing Pathways".
Find Dependencies	Display the names of all resources that depend upon the pathway. See "Viewing Dependencies of a Pathway".
View	Change the way the icons are displayed in the Pro-Watch window.

54.3 Adding or Editing Pathways

1. To add a new pathway, right-click the **Pathways** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane), and select **New Pathways** to display the Add Pathway dialog box.

   To edit an existing pathway, click the **Pathways** icon to display the pathways in the right pane. Right-click on the pathway you want and select **Properties** to display the Edit Pathways dialog box.



2. Use the following field definitions to complete the Pathway Info tab:

Field	Description
Name	Specifies a unique name.
Description	Identifies the pathway beyond the name; for example, the description might identify the pathway's location.
Energize Output	Energizes, or activates, the specified output device when the specified pathway is active.

Field	Description
De-Energize Output	De-energizes, or de-activates, the specified output device when the specified pathway is active.
Points	Specifies the checkpoints that are bypassed along the pathway. The checkpoints are defined by logical devices.
Default Time	Specifies the number of minutes the pathway can be used as configured before access expires. The range is 1-999.

3. Complete the tab sections below to configure the pathway:

54.3.1 Pathway Info Tab

1. On the Add Pathways or Edit Pathways dialog box, enter or modify a unique name for the pathway.
2. On the Add Pathways or Edit Pathways dialog box, enter or modify a description of the pathway.
3. Click Add to display the Desired Inputs dialog box.
4. Click the button next to the Description field, and then click Define. The Logical Devices dialog box appears.
5. Click the device you want to include in the pathway, and then click **OK**.
6. Select the Energize Output device for each device you have added to the pathway. Click the button sequence, and then click Define, and select the device you want to energize.
7. Select the De-Energize Output device for each device you have added to the pathway. Click the button sequence, and then click Define, and select the device you want to de-energize.
8. Specify a default time. The default time is the number of minutes (range 1 to 999) the pathway access will be in effect.

54.3.2 Partitions Tab

Partitions restrict user and class access to database resources that you designate.

See "Overview" for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the pathway:

1. Click **Partitions**.

2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the pathway:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

54.4 Viewing Dependencies of a Pathway

Use this function to view and edit the Pathway's dependencies. The Pathway object depends upon the Badge object.

To view and edit ***a Pathway's dependencies****:*

1. Right-click the icon of an existing Pathway in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Pathway's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

54.5 Deleting a Pathway

Use this function to delete a Pathway from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click **Pathways** to display the Pathway icons in the right pane.
2. Right-click the Pathway you want to delete and select **Delete**. Note that you cannot delete a Pathway that has dependencies. A dependency is another database object that includes the Pathway in its configuration. The Pathway object depends upon the Badge object. If the Pathway has no current dependencies, you are prompted to confirm the deletion. However, if the Pathway does have current dependencies, the Dependencies dialog box appears.
3. If you still want to delete the Pathway:
   a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
   b. Either change or delete each of the objects listed as dependencies.
4. Repeat step 2 and click **Yes** at the prompt to delete the Pathway.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Routing Groups

55

In this chapter ...

Overview

Routing Group Functions

Adding or Modifying a Routing Group

Viewing Dependencies of a Routing Group

Copying a Routing Group

Deleting a Routing Group

55.1 Overview

A routing group determines which events will appear on a given user's Alarm Monitor. Before a user is notified of an event, the event must be validated by passing through at least one of the routing groups assigned to that user or user's class.

Example: As an administrator of a two-building access security system, you may not want the security guard for Building 1 to be viewing the events associated with Building 2. Therefore, you would create a routing group that would route only Building 1 events to the Building 1 security guard.

Tip: The user can be assigned a routing group individually or through the user's class.

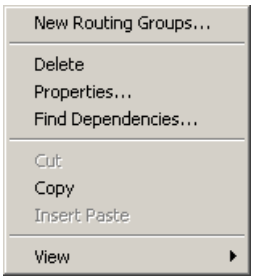
To create a new routing group, you define associated channels and event types. An event must originate from one of the associated routing group channels and be of one of the associated event types. Also, the user must be logged in at one of the associated routing group workstations in order for the event to "pass through" the associated routing group.

Pro-Watch routing groups include Alarm Rollover capability, which forwards (or rolls over) an alarm to another workstation if it has not been acknowledged within a defined time period. If the time period elapses without an acknowledgment from the user, the Alarm Monitor transmits the event to all users that have routing groups with the event type listed in the "Rollover" branch.

55.2 Routing Group Functions

To access Routing Group functions:

1. In the Pro-Watch Database Configuration tree list, click the **Routing Groups** icon to display the currently-configured routing groups in the right pane of the Pro-Watch window.
2. Right-click any routing group icon to display the pop-up menu:



3. Use the following table to select a function:

Click...	**To...**
New Routing Groups...	Add a new routing group. See "Adding or Modifying a Routing Group".
Delete	Delete a current routing group. See "Viewing Dependencies of a Routing Group".
Properties...	Edit a current routing group configuration. See "Adding or Modifying a Routing Group".
Find Dependencies...	Display the type and name of every resource dependency upon the routing group. See "Viewing Dependencies of a Routing Group".
Copy	Create a copy of a routing group's configuration and display its icon in the right pane. See "Copying a Routing Group".
View	Change the way the icons are displayed in the Pro-Watch window.

55.3 Adding or Modifying a Routing Group

To ***add*** a routing group, right-click anywhere in the right pane of the Pro-Watch window and click **New Routing Groups**. The Resources tab in the Add Routing Groups dialog box appears.

To ***edit*** an existing routing group, right-click the Routing Groups icon in the right pane of the Pro-Watch window and click **Properties**. The Resources tab in the Edit Routing Groups dialog box appears.

Note: After you create a routing group, you must assign it either to a class or to a user before it becomes operative. See "Routing Groups Tab" in "DBC - Classes" in Chapter 36 or "Routing Groups Tab" in "DBC - Users" in Chapter 58 for instructions.

Complete the sections below to configure the resources on the Resources tab for a new or existing routing group.

55.3.1 Configuring Channels

To configure a channel, you assign the channel to a routing group. See Chapter 6, for the channel configuration instructions that are specific to your panel.

55.3.2 Configuring Event Types

Use this function to define valid event types for the routing group. For an alarm event to pass through the routing group to the user, the event must belong to one of the event types you select here.

1. From the Resources tab, click **Event Types** to display the tree of available event types.
2. Click the event type you want to assign to the routing group, and click **OK**.

If you want to edit the event type's configuration before assigning it to the routing group:

1. Click the event type and then click **Edit**.
2. Modify the event type on the Define Route Group Resource dialog box, and click **OK**.
3. Then click the event type on the Resources tab and click **OK**.

55.3.3 Configuring Rollover Event Types

Use this function to define which event types will "roll over," or forward, the alarm event to another workstation if the event is not acknowledged within a specified time period.

1. From the Resources tab, click **Rollover Event Types** to display the tree of available rollover event types.
2. Click the event type you want to assign to the routing group as a rollover event type, and click **OK**.

55.3.4 A Special Routing Group: "All System Events"

The Routing Group "All System Events," which used to be called "All Events" in the earlier versions of Pro-Watch, has the following special properties:

- "All System Events" cannot be deleted or edited.
- All users or classes to whom this routing group is assigned get all events from every current and future channel, of any current or future event type, routed to them at any current and future workstation.

This special routing group is a filterless route to which you never need to add any new channels, event types, and workstations.

Note: Do not copy the Routing Group "All System Events" to create a customized routing group. The Routing Group "All System Events" has a unique identifier and specific default configuration (channels, workstations, event types) which are not retained in a duplicate version. A copy would not have the same function.

55.3.5 Configuring Workstations

Use this function to define which workstations the routing group will allow to receive the passed-through alarm events.

1. From the Resources tab, click Workstations and then click **Add**. The Define Route Group Resource dialog box appears.
2. Click the button next to the Resource field to display the list of available workstations.
3. Click the workstation you want to assign to the routing group and click **OK**. Note that if you want to edit the configuration of the workstation you want to select, click the workstation, click **Edit**, modify the workstation settings, and click **OK**.
4. On the Define Route Group Resource dialog box, select the time zone, or time period during which the workstation can be sent events.
5. Click the Acknowledge check box if you want to allow the operator to acknowledge the event.
6. Select the Clear check box if you want to allow the operator to clear the event.
7. Click **OK** to assign the workstations to the routing group; click **Add Remaining** to add all of the remaining workstations.

8. Click **OK** to accept the resource definition. Select and configure another resource on the Resources dialog box, if you desire.

55.3.6 Assigning a Routing Group to a User

Note: Before you perform this task you have to first assign Channels, Events Types, Rollover Event Types, and Workstations to a routing group.

1. In the main Pro-Watch window, click the **Database Configuration** module icon to display the database options in the middle pane.
2. Click the **Users** icon to display the existing users in the right pane.
3. Select a user and right-click its icon to display the pop-up menu.
4. Select **Properties** to display the Edit Users screen.
5. Click and select the **Routing Groups** tab.

Note: If the routing group that you want to assign to the user is not already listed in the list box, click **Add** to display the Routing Groups screen and proceed with
step 7.

Once you add a routing group to this tab you can revoke and disable but not delete it. See step b below.

a. If the correct routing group is displayed in the list box and has a Grant status, then you do not need to add it since it is already assigned to the user and enabled.

b. If an incorrect routing group is displayed in the list box and has a Grant status, select it and click **Revoke**. Then proceed to add the routing group that you want as described in step 6 above.

c. If the correct routing group is already listed in the listed box but has a Revoke status, select it and click **Grant**.

d. To assign a routing group the same privileges as the class to which the user belongs, select it and click **Delete/Revert**. The status of the routing group toggles to “Class Grant.”

e. You can still revert and reassign user-level privileges to this routing group by clicking **Grant**, or conversely, revoke the user-level privileges by clicking **Revoke**. Compare this with the note for step e below.

Note: To permanently assign a routing group the same privileges as the class to which the user belongs, select it and click **Revert to Class**. A warning message will display, asking for your confirmation. Click **Yes**.

This action is not reversible. Once a routing group is assigned class-level privileges through the Revert to Class button, you cannot reassign user-level privileges. Compare this with the note for step d above.

6. In the Routing Groups screen, select a routing group from the list box and click **OK** to return to the Edit Users screen.
7. Click **OK** to close the Edit Users screen.

55.3.7 Assigning a Routing Group to a Class

Before you perform this task you must first assign Channels, Events Types, Rollover Event Types, and Workstations to a routing group.

1. In the main Pro-Watch window, click the **Database Configuration** module icon to display the database options in the middle pane.
2. Click the **Class** icon to display the existing classes in the right pane.
3. Select a class and right-click its icon to display the pop-up menu.
4. Select **Properties** to display the Edit Classes screen.
5. Click and select the **Routing Groups** tab.
6. Click **Add** to display the Routing Groups screen.
7. Select a routing group from the list box and click **OK** to return to the Edit Classes screen.
8. Click **OK** to close the Edit Classes screen.

55.3.8 Applying a Routing Group Filter

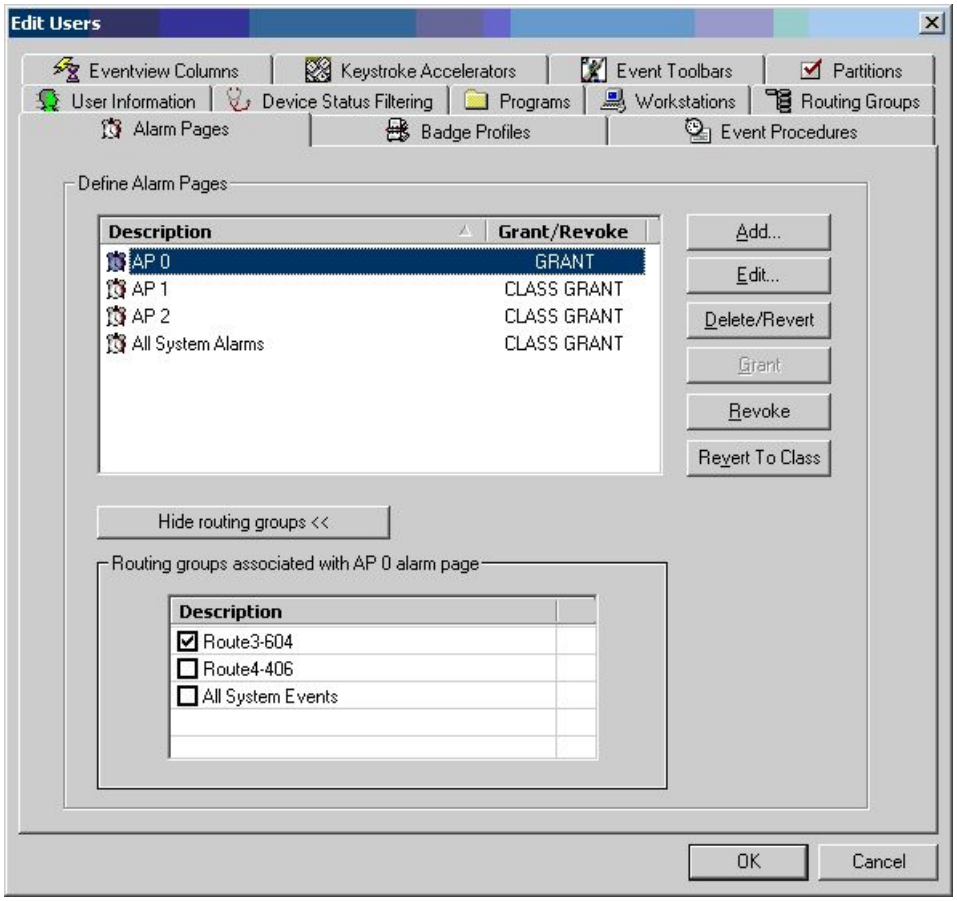
Note: Before you perform this task, you must first assign Channels, Event Types, Rollover Event Types, and Workstations to a routing group.

You can apply a filter to associate Alarm pages and routing groups so that only certain events display on an Alarm page.

To associate alarm pages and routing groups:

1. In the main Pro-Watch window, click the **Database Configuration** module icon to display a list of database options in the left pane.
2. In the left pane, click the **Users** icon to display the existing users in the display pane.
3. Select a user and right-click its icon to display the pop-up menu.
4. Select **Properties** to display the Edit Users screen.

5. Click and select the Alarm Pages tab.

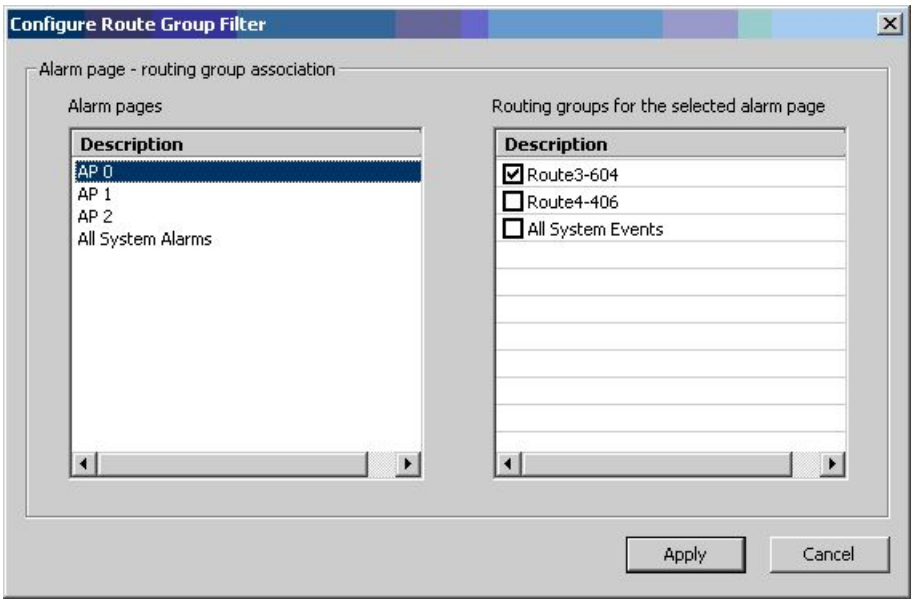


6. In the Define Alarm Pages box, select an alarm to display the Routing Groups box.
7. Click on one of the routing groups listed in the Routing groups box (if you cannot see the routing groups, click **Show Routing Groups**) and click **OK**.

Note: Only users with appropriate permissions can change the alarm page/routing association. Once the association is set, all events that can appear on an alarm page are filtered based on the routing groups.

To temporarily change the alarm page routing group:

1. In the main Pro-Watch window, click the **Monitor** module icon to display the Monitor icon in the middle pane.
2. Click the **Alarm Monitor** icon to display the current alarms.
3. Select an alarm and right-click to display the pop-up menu.
4. Click **View > Configure Route Group Filter** to display the Configure Route Group Filter dialog box.



5. Click an alarm page to display the routing groups associated with it.
6. Select the check box(es) for any other routing groups you want to associate with this alarm page.
7. Click **Apply**.

After the changes are applied, events are displayed on a page based on this association. Events are displayed on all alarm monitors that run on this machine at this time. When all the alarm monitors in the workstation are closed and another instance is run, the default alarm page-routing group association for that user is reinstated.

Once the routing association is set, all the events that can appear on an alarm page are filtered based on the routing groups.

Note: Only users with appropriate permissions can change the alarm page/routing association. Once the association is set, all events that can appear on an alarm page are filtered based on the routing groups.

55.3.9 Partitions

Partitions restrict user and class access to database resources that you designate.

See "Overview" for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the routing group:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the routing group:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

55.4 Viewing Dependencies of a Routing Group

Use this function to view and edit the Routing Group's dependencies. The Routing Group object depends upon the Badge object.

To view and edit ***a Routing Group's dependencies****:*

1. Right-click the icon of an existing Routing Group in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Routing Group's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

55.5 Copying a Routing Group

Use this function to create a copy of a routing group. This can be a fast way to create a new routing group. If the original routing group will be similar to the new one, you can copy the original and change only a small number of its properties to create the new routing group.

1. In the Pro-Watch Database Configuration tree list, click the **Routing Groups** icon to display the currently-configured routing groups in the right pane.
2. Right-click the icon of the routing group you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original routing group name]” appears in the right pane.

55.6 Deleting a Routing Group

Use this function to delete a Routing Group from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click **Routing Groups** to display the Routing Group icons in the right pane.

Note: Right-click the Routing Group you want to delete and select **Delete**.

You cannot delete a Routing Group that has dependencies. A dependency is another database object that includes the Routing Group in its configuration. The Routing Group object depends upon the Class and User objects. If the Routing Group has no current dependencies, you are prompted to confirm the deletion. However, if the Routing Group does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Routing Group:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Routing Group.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Status Groups

56

In this chapter ...

Overview
Status Group Functions
Adding a User-Defined Status Group
Editing a User-Defined Status Group
Copying a Status Group
Deleting a User-Defined Status Group
System All Installed Status Groups
System All Installed Channels
System All Installed Panels

56.1 Overview

Use this function to

1. add a user-defined status group of logical devices, channels and/or panels, or
2. to automatically see a list of all installed channels and panels. See System All Installed Channels and System All Installed Panels.

For example, security personnel can conduct monthly checks of enterprise hardware categories. The status consists of events associated with the logical devices.

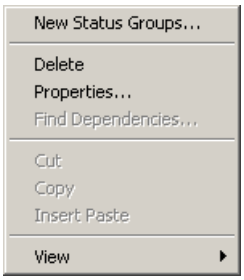
These status groups can be automatically updated or updated on-demand whenever new panels and channels are added into the system.

Status groups are not defined by geography or function. However, all physical devices in the logical devices must be polled by the same Pro-Watch server.

56.2 Status Group Functions

To access Status Groups functions:

1. In the Pro-Watch Database Configuration tree list, click the **Status Groups** icon to display the currently-configured status groups in the right pane of the Pro-Watch window.
2. Right-click any status group icon to display the pop-up menu:

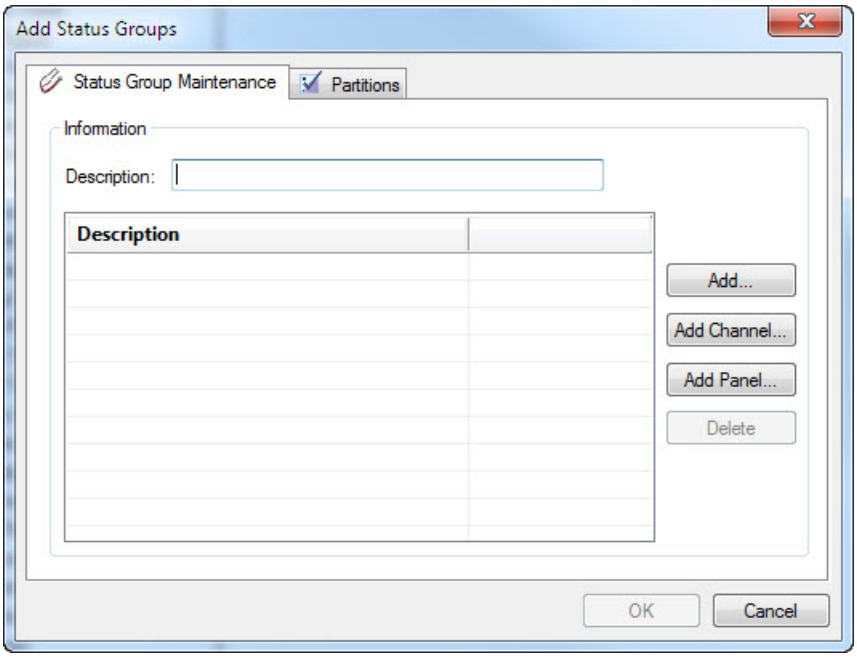


3. Use the following table to select a function:

Click...	To...
New Status Groups...	Add a new status group. See "Adding a User-Defined Status Group".
Delete	Delete a current status group. See "Copying a Status Group".
Properties...	Edit a current status group configuration. See "Adding a User-Defined Status Group".
Copy	Create a copy of a status group's configuration and display its icon in the right pane. See "Copying a Status Group".
View	Change the way the icons are displayed in the Pro-Watch window.

56.3 Adding a User-Defined Status Group

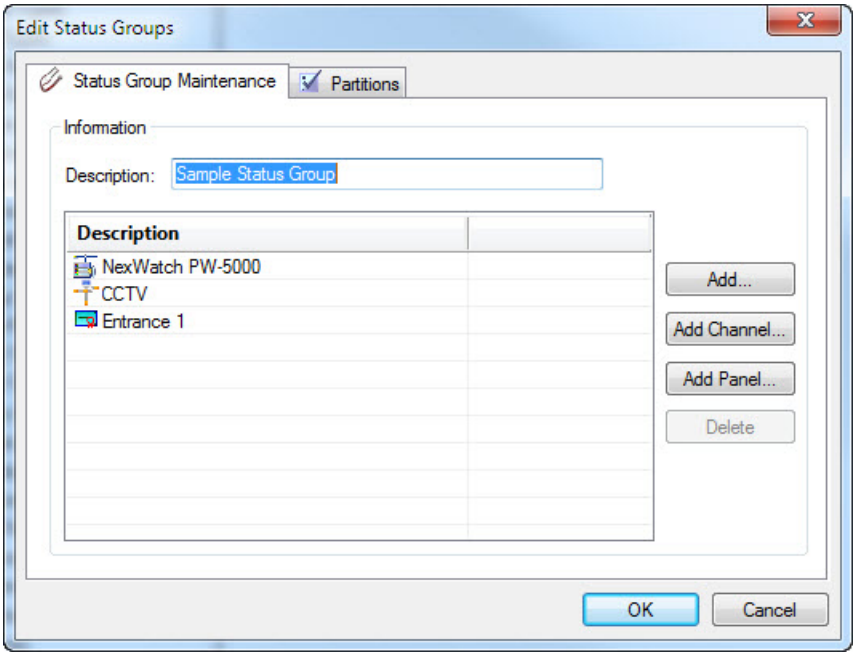
1. To **add** a user-defined status group, right-click the **Status Groups** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane of the Pro-Watch window), and select **New Status Groups.** The **Status Group Maintenance** tab in the **Add Status Groups** dialog box appears:



2. Enter a **Description**.
3. Click **Add** to add a logical device.
4. Click **Add Channel** to add a channel.
5. Click **Add Panel** to add a panel.
6. To delete a status group, select it from the list and click **Delete**.
7. Click the **Partitions** tab to add a partition.

56.4 Editing a User-Defined Status Group

1. To **edit** an existing status group, right-click the Status Groups icon in the right pane of the Pro-Watch window and select **Properties**. The **Status Group Maintenance** tab in the **Edit Status Groups** dialog box appears:



2. Complete the sections below to configure a status group:

56.4.1 Status Group Maintenance Tab

1. Edit the **Description**.
2. Click **Add** to edit a logical device.
3. Click **Add Channel** to edit a channel.
4. Click **Add Panel** to edit a panel.
5. To delete a status group, select it from the list and click **Delete**.
6. Click **OK**.

56.4.2 Partitions Tab

Partitions restrict user and class access to database resources that you designate.

See "Overview" for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the status group:

1. Click **Partitions**.
2. Click **Add**, and select the partition you want.
3. Click **OK** to accept the partition.

To assign a partition to the status group:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

56.5 Copying a Status Group

Use this function to create a copy of a status group. This can be a fast way to create a new status group. If the original status group will be similar to the new one, you can copy the original and change only a small number of its properties to create the new status group.

1. In the Pro-Watch Database Configuration tree list, click the **Status Groups** icon to display the currently-configured status groups in the right pane.
2. Right-click the icon of the status group you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original status group name]” appears in the right pane.

56.6 Deleting a User-Defined Status Group

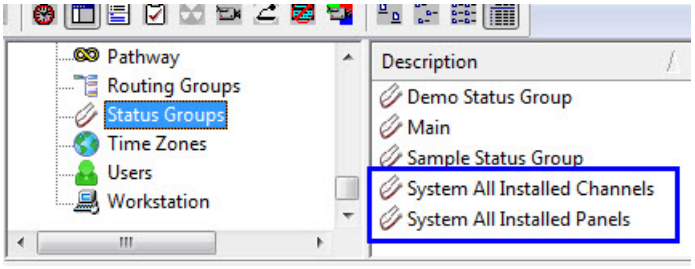
Use this function to delete a Status Group from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click **Status Groups** to display the Status Group icons in the right pane.
2. Right-click the Status Group you want to delete and select **Delete**.
3. Click **Yes** at the prompt to delete the Status Group.

56.7 System All Installed Status Groups

There are two types of "System All Installed Status Groups" that are installed by default when you install Pro-Watch on your system:

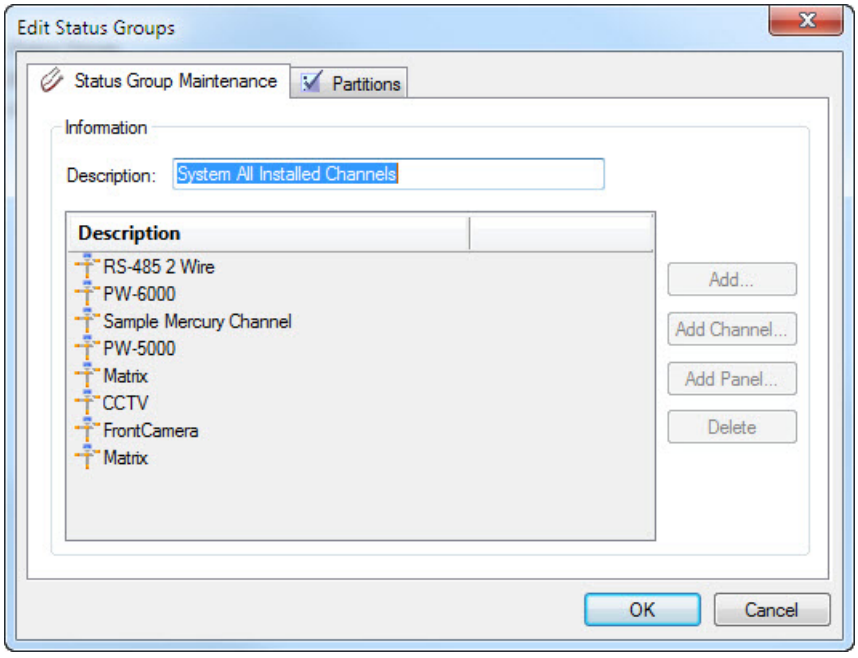
1. System All Installed Channels
2. System All Installed Panels



56.7.1 System All Installed Channels

Adding a new installed channel in Pro-Watch will automatically add it to this status group. Similarly, uninstalling or deleting the channel will automatically remove it from this status group.

Double-click the **System All Installed Channels** link to display all the existing channels installed in the system:

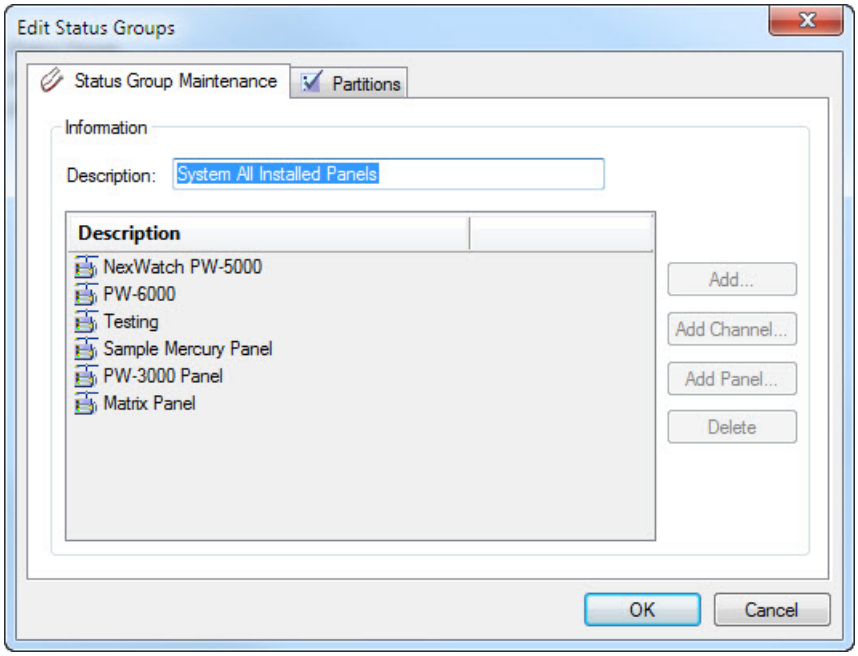


This is a view-only information screen that does not allow adding, editing, or deleting any channels.

56.7.2 System All Installed Panels

A new installed panel will automatically show up in this status group. In addition, the channel corresponding to this panel must also be installed to show up in this status group. Uninstalling a channel, panel or deleting the panel will remove it automatically from this status group.

Double-click the **System All Installed Panels** link to display all the existing panels installed in the system:



This is a view-only information screen that does not allow adding, editing, or deleting any panels.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Time Zones

57

In this chapter ...

Overview

Time Zone Functions

Adding or Editing a Time Zone

Viewing Dependencies of a Time Zone

Copying a Time Zone

Deleting a Time Zone

57.1 Overview

Use this function to specify time periods for which access is allowed.

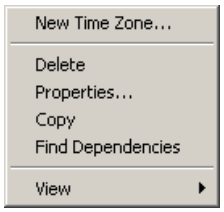
Example: You can specify 6:00 a.m. to 6:00 p.m., Monday through Friday, as the time zone for a PW-5000 panel that controls the elevators of a 128-story building. This time zone allows the elevators to be used during working hours, but not otherwise.

Note: The end time for a time zone ends at the END of the last specified minute. For example: a time zone running from 16:00 to 23:59 starts at 4 PM and ends at midnight, not at 11:59 PM. Another example: an 8-hour time zone running from 10:00 to 18:00 starts at 10 AM and ends at 6:01 PM.

57.2 Time Zone Functions

To access Time Zone functions:

1. In the Pro-Watch Database Configuration tree list, click the **Time Zones** icon to display the currently-configured time zones in the right pane of the Pro-Watch window.
2. Right-click any time zone icon to display the pop-up menu:



3. Use the following table to select a function:

Click...	To...
New Time Zones...	Add a new time zone. See "Adding or Editing a Time Zone".
Delete	Delete a current time zone. See "Viewing Dependencies of a Time Zone".
Properties...	Edit a current time zone configuration. See "Adding or Editing a Time Zone".
Copy	Create a copy of a time zone's configuration and display its icon in the right pane. See "Copying a Time Zone".
Find Dependencies	Display the names of all resources that depend upon the time zone.
View	Change the way the icons are displayed in the Pro-Watch window.

57.3 Adding or Editing a Time Zone

Note: When editing a time zone, the Pro-Watch prompts for the appropriate digital signature(s) and the appropriate information post-edit, if the time zone is a member of a secured panel, or is a member of a clearance code with secured logical devices. Time zones tied to more than one secure resource use the aggregated resources's most restrictive settings.

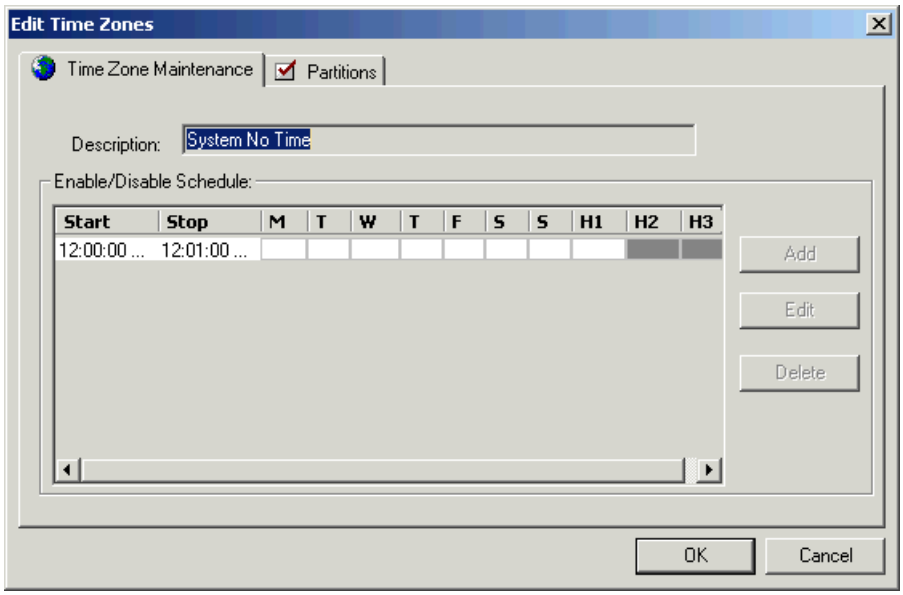
Note: To add a time zone, right-click the **Time Zones** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane of the Pro-Watch window), and select **New Time Zones**. The Resources tab in the Add Time Zones dialog box appears.

To edit an existing time zone, right-click the Time Zones icon in the right pane of the Pro-Watch window and click **Properties**. The Resources tab in the Edit Time Zones dialog box appears.

The grayed-out fields in the Add Time Zones and Edit Time Zones dialog boxes are not downloaded to the panel.

Examples:

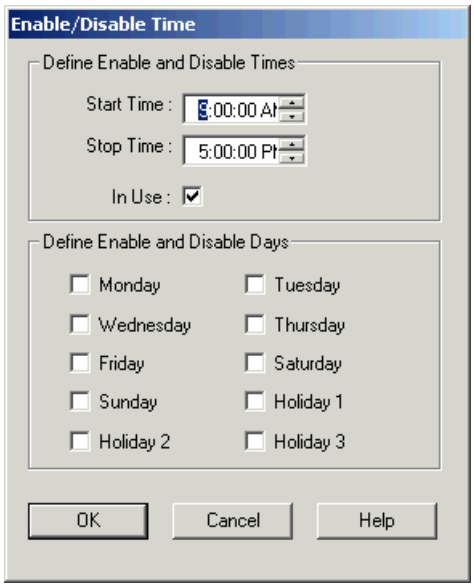
- The H2 (Holiday 2) and H3 (Holiday 3) fields are not supported on the panel configured in the dialog box above. If your panel(s) allows holiday settings within the Time Zone function, you can configure H1-H3 to modify normal Time Zone behavior on a particular day.
- If your enterprise is scheduled to restrict access into the building on Christmas, you can apply the holiday to a unique time zone to accommodate the modified schedule.



4. Complete the sections below to configure a time zone:

57.3.1 Time Zone Maintenance Tab

1. From the Add Time Zones dialog box or Edit Time Zones dialog box, enter or modify a description that uniquely identifies the time zone.
2. Click **Add** to display the Enable/Disable Time dialog box:



3. Specify a start time and stop time for each time zone you want, and check the In Use box to activate this time zone setting. You can specify multiple time zones for each day and for the entire week.

   Notes:

   - The maximum number of multiple time zones depends upon the panel type. See the appropriate panel section in Chapter 6, "". [See "DBC - Holidays" in Chapter 49 "DBC - Holidays" for an explanation of Holidays 1-3.

- Blue boxes in the time zone schedule indicate when the devices are enabled, and the white boxes indicate when the devices are disabled.

57.3.2 Partitions Tab

Partitions restrict user and class access to database resources that you designate.

See "Overview" for information about creating a partition. Use this function to create, assign or delete a partition:

To create a partition for the time zone:

1. Click **Partitions**, click **Add**, and select the partition you want.
2. Click **OK** to accept the partition.

To assign a partition to the time zone:

1. Click **Add** to display the Available Partitions dialog box.
2. Select the partition you want, and click **Add**.

To delete a partition from the Partitions List dialog box:

Select the partition and click **Delete**.

57.4 Viewing Dependencies of a Time Zone

Use this function to view and edit the Time Zone's dependencies. The Time Zone object depends upon the Panel, Clearance Code, and Routing Group objects.

*To view and edit **a Time Zone's dependencies**:*

1. Right-click the icon of an existing Time Zone in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Time Zone's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

57.5 Copying a Time Zone

Use this function to create a copy of a time zone. This can be a fast way to create a new time zone. If the original time zone will be similar to the new one, you can copy the original and change only a small number of its properties to create the new time zone.

1. In the Pro-Watch Database Configuration tree list, click the **Time Zones** icon to display the currently-configured time zones in the right pane.
2. Right-click the icon of the time zone you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original time zone name]” appears in the right pane.

57.6 Deleting a Time Zone

Use this function to delete a Time Zone from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click **Time Zones** to display the Time Zone icons in the right pane.

Note: Right-click the Time Zone you want to delete and select **Delete**.

You cannot delete a Time Zone that has dependencies. A dependency is another database object that includes the Time Zone in its configuration. The Time Zone object depends upon the Panel, Clearance Code, and Routing Group objects. If the Time Zone has no current dependencies, you are prompted to confirm the deletion. However, if the Time Zone does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Time Zone:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Time Zone.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC - Users

58

In this chapter ...

Overview

User Functions

Adding a User

Editing a User

Copying a User

Types of User Icons

Deleting a User

58.1 Overview

Use this set of functions to set up user access accounts. For each user, you specify a class. When you assign a user to a class, he or she automatically receives the Pro-Watch privileges that are assigned to the class.

Additionally, however, you can customize the user's class rights by changing his access to any of the following:

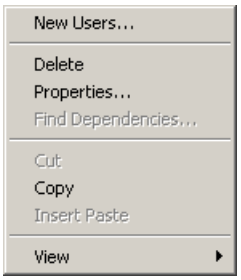
- Pro-Watch programs, or functions.
- Workstations the user can access.
- Routing groups.
- Alarm pages.
- Keystroke accelerators.
- Event toolbars.
- Partitions.
- Badge profiles.
- Event procedures.
- Eventview columns.

Note: Since all users must be assigned to a class, at least one class must be created before you add users.

58.2 User Functions

Follow these steps:

1. In the Pro-Watch Database Configuration tree list, click the **Users** icon to display the currently-configured users in the right pane of the Pro-Watch window.
2. Right-click any user icon to display the pop-up menu:



3. Use the following table to select a function:

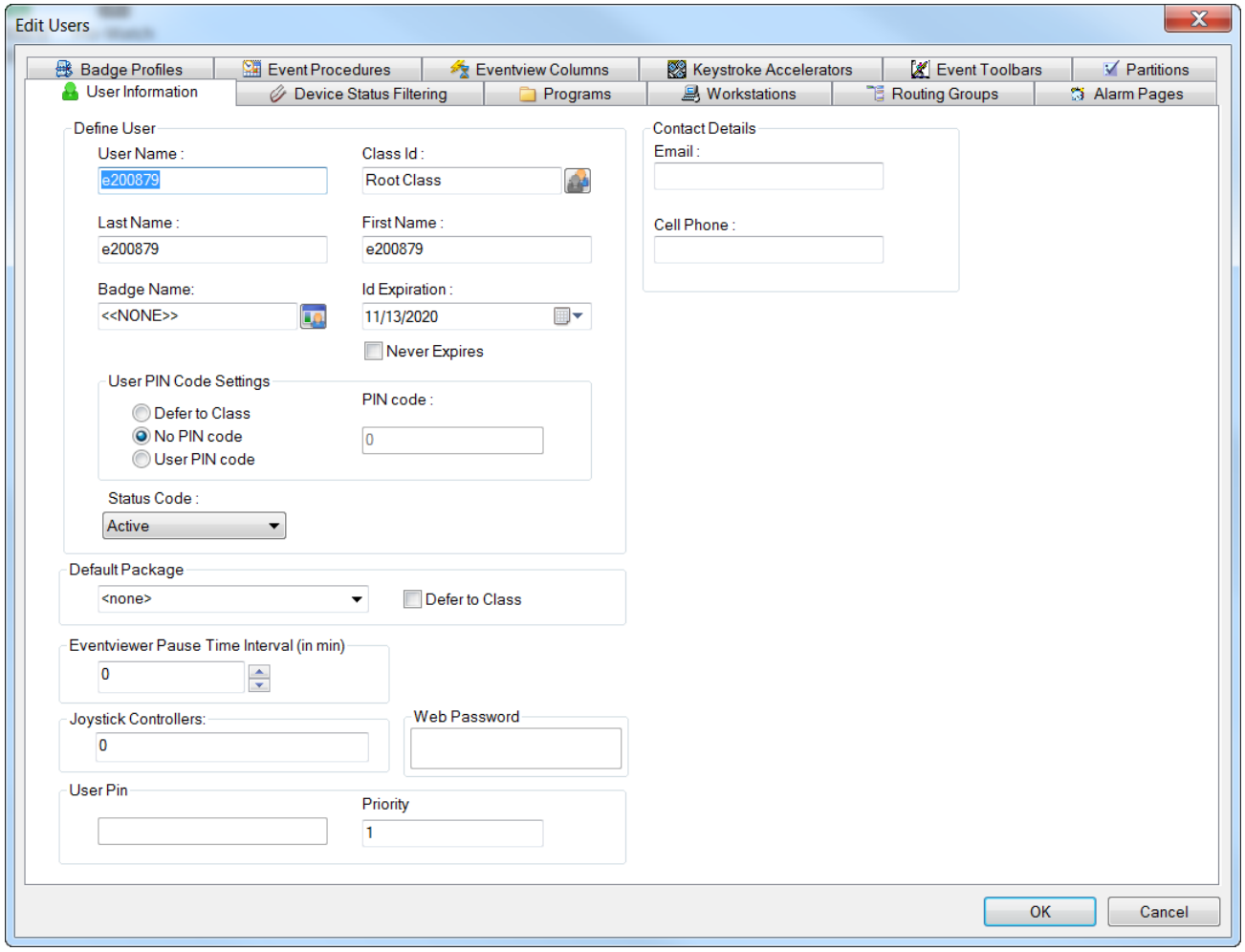
Click...	To...
New Users...	Add a new user. See "Adding a User".
Delete	Delete a current user. See "Copying a User".
Properties...	Edit a current user configuration. See "Adding a User".
Copy	Create a copy of a user's configuration and display its icon in the right pane. See "Copying a User".
View	Change the way the icons are displayed in the Pro-Watch window.

58.3 Adding a User

To add a user, right-click the **Users** icon in the Pro-Watch Database Configuration tree list (or right-click anywhere in the right pane of the Pro-Watch window), and select **New Users**. The Pro-Watch User Manager (New Wizard) dialog box appears. See "Adding a System User" in Chapter 6 for the Pro-Watch User Manager instructions.

58.4 Editing a User

To edit an existing user, right-click the **Users** icon in the right pane of the Pro-Watch window and select **Properties** to display the **Edit Users** dialog box:



Complete the following tab sections to configure a new or existing user.

USER TABS LIST

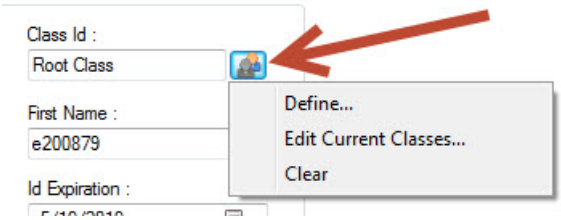
- "User Information Tab".
- "Device Status Filtering Tab".
- "Programs Tab".
- "Workstations Tab".
- "Routing Groups Tab".
- "Eventview Columns Tab".
- "Keystroke Accelerators Tab".

- "Event Toolbars Tab".
- "Partitions Tab".
- "Alarm Pages Tab".
- "Badge Profiles Tab".
- "Event Procedures Tab".

58.4.1 User Information Tab

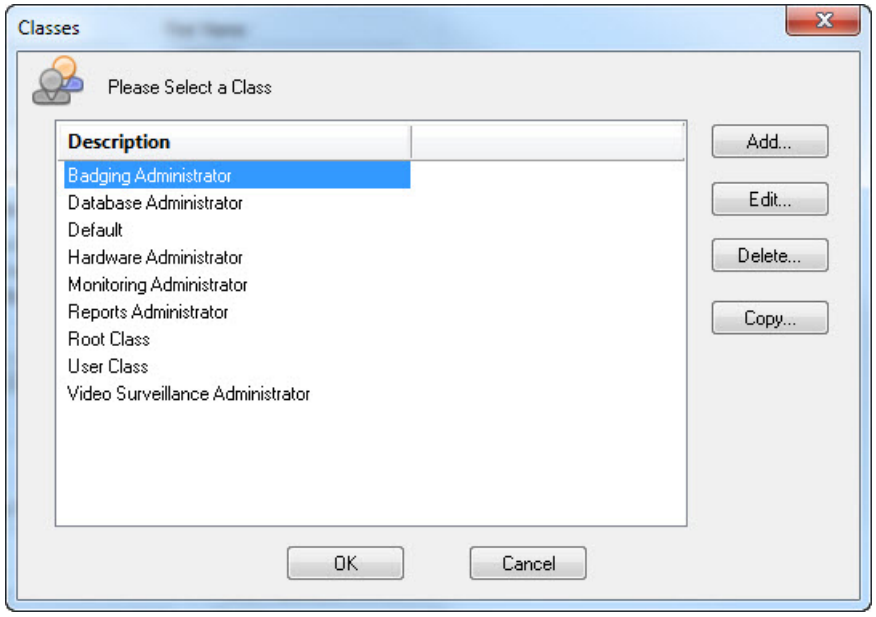
1. Enter a user ID into the **User Name** field.
2. Enter a **Last Name** and a **First Name** for the user.
3. Enter a **Class ID**. Note that the user's workstation, as well as the user himself, must be assigned to the same classes. The workstation will be disabled if the user and the workstation are assigned to different classes. See "DBC - Workstations" in Chapter 59 for information about assigning workstations to classes.

   a. To add, edit, or delete a class, left-click the associated field icon to display the pop-up menu:



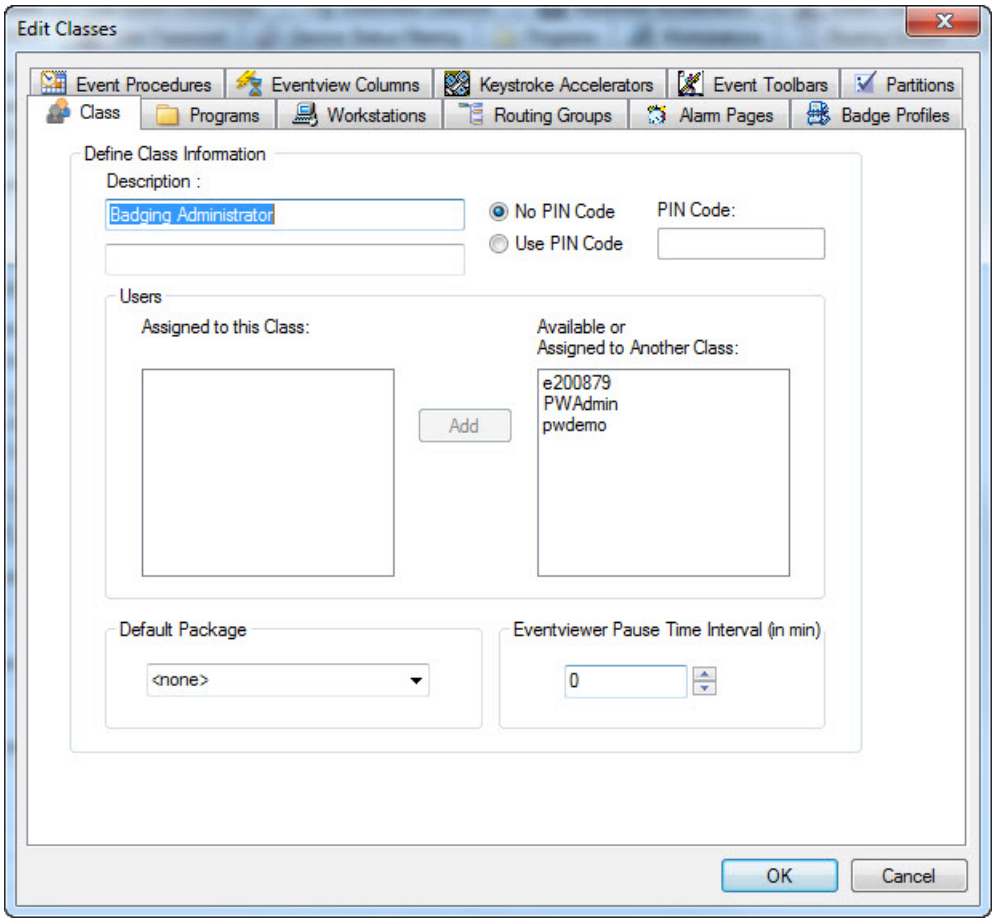
   b. To clear the **Class ID** (with the intention of adding a new one from the list of classes) select **Clear** from the pop-up menu.

c. Select **Define** from the pop-up menu to display the **Classes** dialog box:

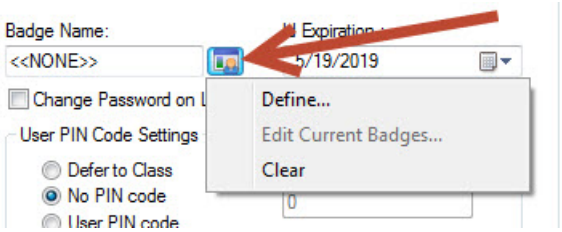


d. To add a class, select one from the **Description** list and click **Add**. To delete a class, click **Delete**. To copy a class, click **Copy**.

e. To edit a class, click the **Edit** button to display the **Edit Classes** dialog box. Make the necessary changes and click **OK** to close it:



4. Enter a **Badge Name**. Left-click the associated field icon to display the pop-up menu:



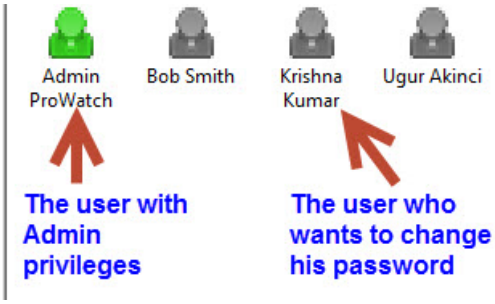
   a. Click **Define** to display badge names. Select the user's badge name.

   b. Select **Clear** from the pop-up menu to clear the **Badge Name** (with the intention of adding a new one from the list of classes).

   c. Select **Edit Current Badges...** to edit the badge name selected.

5. Select the **Change Password on Login** check-box to enable the users change their passwords at the application login screen.

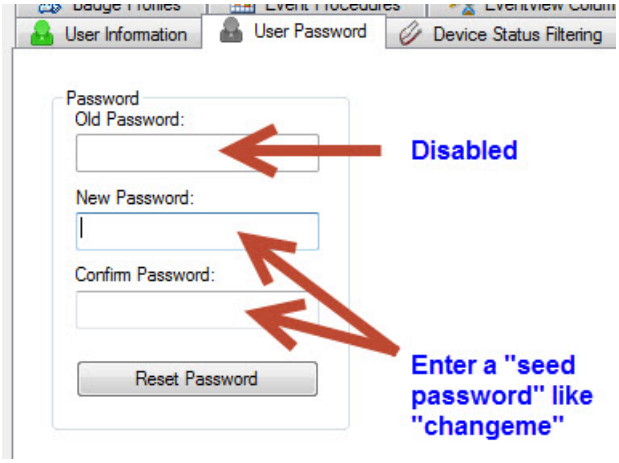
a. As an Administrator, select the user who asked his or her password to be changed. **For example**, in the below example, you are logged in as **Admin ProWatch** (GREEN). We will assume that the user **Krishna Kumar** (GRAY) has requested to change his password since he cannot remember it:



b. Double-click and display Krishna Kumar's "Edit User" screen.

c. Select Krishna Kumar's "**Change Password on Login**" check-box.

d. Click and select Krishna Kumar's "**User Password**" tab. Note that the "**Old Password**" field is disabled since the Administrator cannot know an individual user's password:



e. Enter a temporary "**seed password**" like "**changeme**" so that the user can log in to Pro-Watch to change his password even though he lost the last password. Send the seed password to the user.

f. When the user logs in to the Pro-Watch by using the seed password, **a second login screen** will display where the user can change the temporary password to any new alphanumeric string he likes, provided it is at least 8 digits in length.

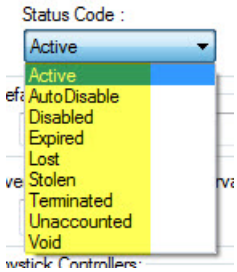
6. Select the **Never Expires** check-box to make sure the User ID will never expire.

7. Select a personal identification number (**PIN**) code setting:

   - Defer to Class – defers to the generic class PIN setting.

- No PIN code – assigns no PIN code to the user.
- User PIN code – assigns a unique PIN code to a user who needs access rights that are not included in his class rights.

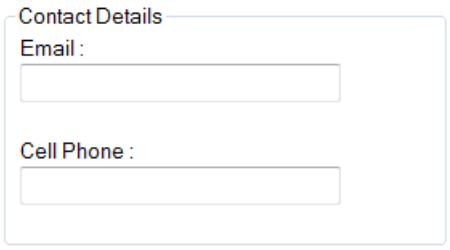
8. Select a **Default Package** setting by clicking and displaying the drop-down list shells. Select a shell for the user to access at login. For example, if the user will typically be using the hardware configuration functions, you might select the **Hardware Configuration Shell** to save the user a few "clicks" to access the functions he needs. Other two options are **Database Configuration Shell** and **Event Viewer Shell.**
9. Select the **Defer to Class** check-box to defer to the generic class setting.
10. Select an appropriate **Status Code** from the respective drop-down menu:



Note that status code applies only to Application Login.

11. Set the **Event Viewer Pause Time Interval**, in minutes.
12. Enter the address of **Joystick Controllers**.
13. Enter a **Web Password**.
14. Enter a **User Pin** and **Priority** for the user.
15. In the **Enhanced Privilege Setting** box, select the **Restrict User Privilege** checkbox only if you are configuring this user to be a "restricted user." A restricted user is a user who has privileges to create other users and grant them with the same privileges he (the restricted user) has. Any other privileges the user might have been granted by class are revoked. This is not the only step required, however, to create a sub-administrator. See "Setting Privilege Management" in Chapter 5 for details and additional instructions.

16. In the **Contact Details** group of fields, enter the **Email** address and **Cell Phone** number associated with the user of this account:

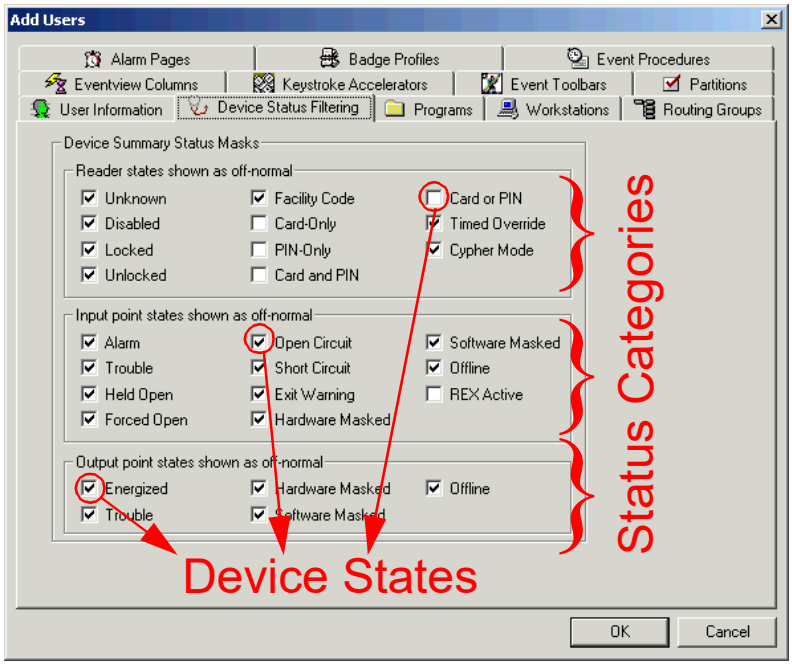


58.4.2 Device Status Filtering Tab

Use this function to create masks that filter device status. You can create a mask for reader states, input point states, and output point states.

Example: You can create a mask for a device that blocks all reader state status except card-only, PIN-only, and cipher mode status.

1. Click the Device Status Filtering tab.
2. For any or all of the three status categories, click the device states for which you want to display status:

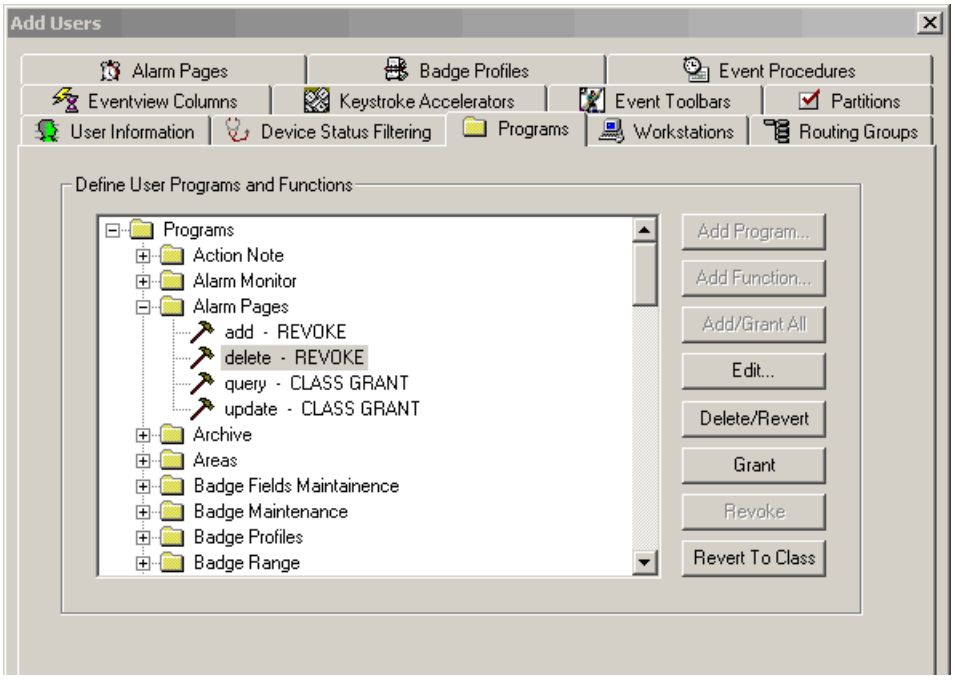


58.4.3 Programs Tab

In the Programs tab, you can customize the user's program access if you want his program access to be different from his class program access.

To customize a user's program access:

1. Click the Programs tab to display the tree list of the Programs directory. See Appendix B, Assignable Programs for a complete list of programs and descriptions of their functions.

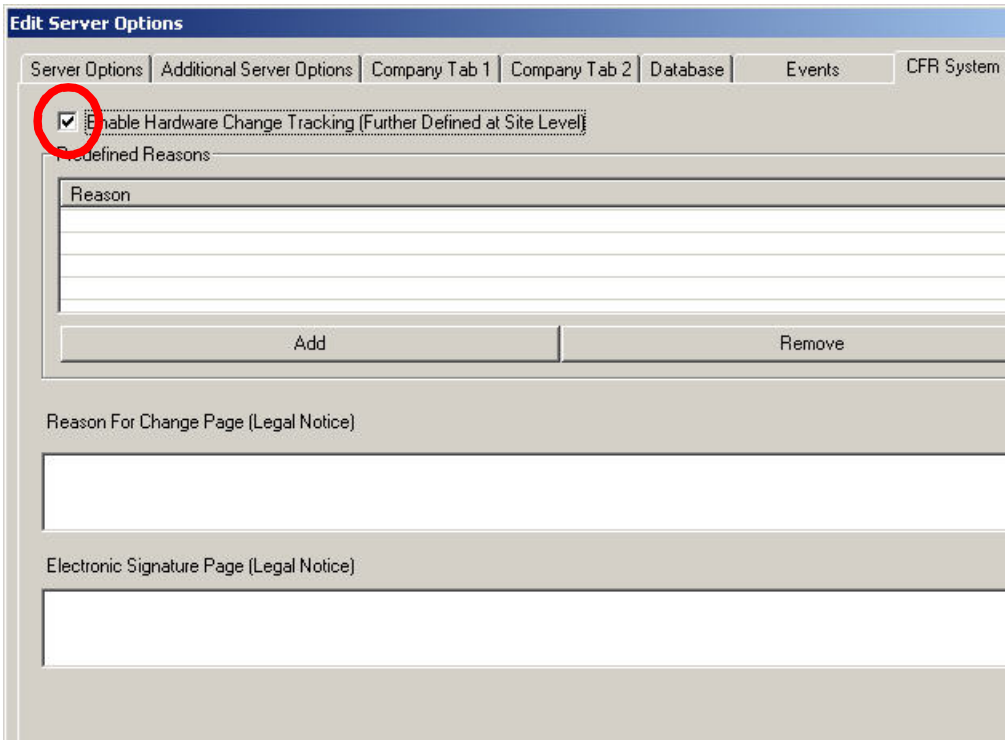


2. Use the following list of task definitions to create or change the user's access to one of the programs:
    - Add Program – adds a program to the program directory.
    - Add Function – makes an additional function of the program available to the user.
    - Add/Grant All – enables you to add and provide class access to all programs.
    - Edit – edits the current access to a program; you can either grant or revoke a program's access, or you can require the user to provide a PIN code for access.
    - Delete/Revert – deletes the user's unique access to a program and reverts to the user's class access.
    - Grant – grants individual, not class, access to the program.
    - Revoke – revokes individual access to the program.
    - Revert to Class – revokes any individual access the user has to a program, and reverts to the user's class privileges.

To add compliance with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11):

1. In the Programs tab, select **Administration**.
2. Click **Add Program** to display the Programs and Functions dialog box.
3. Select **CFR Maintenance** from the Program drop-down menu.

4. Select the **Grant** option button for Privileges for Class or User.
5. Click **OK** to add the functionality to the Administration program.
6. Click **OK** to close the Edit Users window.
7. Select **File > Server Options** from the main menu to display the Edit Server Options screen.
8. Select the **CFR System Setting** tab.



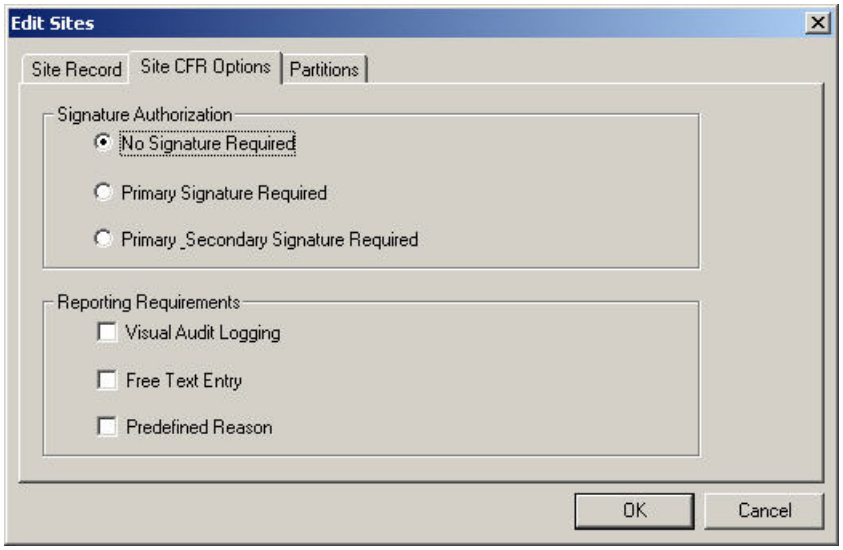
9. Select the **Enable Hardware Change Tracking (Further Defined at Site Level)** check box.

Note: Click **Add** and type in one or more reasons why the 21 CFR 11 tracking is enabled. The reason(s) are now listed in the list box.

The user must enter at least one reason. The default is “Unknown Reason.”

10. Select a reason and click **Remove** to remove it from the Predefined Reasons list box.
11. Enter a text for the **Reason For Change Page (Legal Notice)** text box. For example: “Pursuant to Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11), all changes must be recorded with a reason for that change.”

12. Enter a text for the **Electronic Signature Page (Legal Notice)** text box. For example: "Pursuant to Section 11.100 of title 21 of the Code of Federal Regulations, this is to certify that (Name of the Company) intends that all electronic/digital signatures executed by our employees, agents or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures."
13. Click **OK** to close the Edit Server Options screen.
14. Click **Hardware Configuration** function icon to display the existing sites in the middle pane.
15. Select a **site** and right-click its **name** to display the pop-up menu.
16. Select **Properties** to display the Edit Sites screen.
17. Click the **Site CFR Options tab**.



18. Select one of the following **Signature Authorization** option buttons:
    - No Signature Required.
    - Primary Signature Required.
    - Primary and Secondary Signature Required.
19. Select one of the following **Reporting Requirements** check boxes:
    - Visual Audit Logging.
    - Free Text Entry.
    - Predefined Reason.

20. Click **OK** to save and close the Edit Sites screen.

58.4.4 Workstations Tab

The Workstations tab (the Define User dialog box) shows the workstations to which the user has access. Access to these workstations has already been granted either by the user's class or by one of the custom functions in the Workstations dialog box.

From here, you can add more workstations, remove workstations, edit the workstations' current configurations, grant or revoke access, or delete the user's custom configuration and revert to class access. Refer to "DBC - Workstations" in Chapter 59 for instructions.

58.4.5 Routing Groups Tab

Use this function to assign an existing routing group to an individual user. A routing group is a path through which an alarm event must pass before it displays in the Alarm Monitor.

Example: Before a user is notified of an event, the event must be validated by passing through at least one of the routing groups assigned to that user. The user can be assigned a routing group individually or through the user's class.

Note: A routing group must already be created before you can assign it to a user. For information about creating routing groups, see "DBC - Routing Groups" in Chapter 55.

To assign or edit a routing group for an individual user:

1. Click **Add** to display the Routing Groups dialog box.
2. If the group you want already appears in the displayed list, select the desired group and click **OK** to add it.

   If the group you want appears in the list and you would like to edit the group configuration, select the group and click **Edit**. Add, edit, or delete group items on the Edit Routing Groups dialog box and click **OK**.
3. If the group you want does not appear in the displayed list, click **Add** to display the Add Routing Groups dialog box. Enter a group description and add, edit, or delete group items on the Add Routing Groups dialog box. Click **OK**.

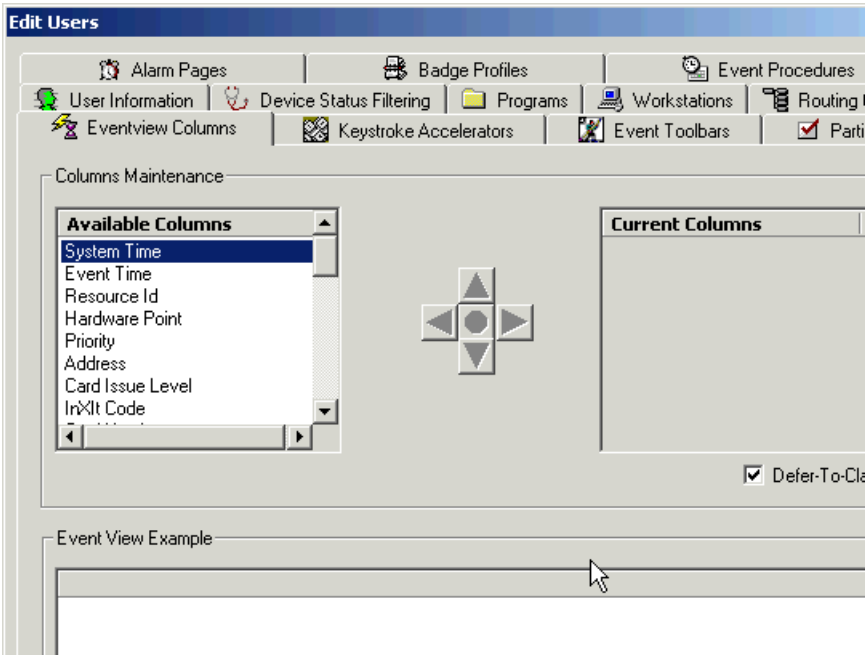
To delete a routing group from the user:

1. In the Pro-Watch Database Configuration tree list, click the **Routing Groups icon** to display the group icons in the right pane.

2. Right-click the icon of the group you want to delete, and select **Delete**.

58.4.6 Eventview Columns Tab

Use this function to customize the user's view of events. The Eventview Columns tab displays the column heads, or event categories, that are available to include in the user's view of events.



1. Click the **Defer-to-Class** check box to de-select the class default settings for Eventview Columns.
2. Click the first column, or event category, you want included in the user's event view, and then click the right arrow. The column head moves to the Current Columns box.
3. Repeat step 2 for all additional column heads.
4. Click **OK**.

58.4.7 Keystroke Accelerators Tab

Use this function to assign shortcut keys that execute **Commands** and **Event Procedures**. Keyboard Accelerators are sometimes called "hot keys."

Example: You can use a Keyboard Accelerator to modify normal Time Zone behavior on specific days. You can enable connected panels to modify access, in all time zones or only in specific ones.

Note: A keystroke accelerator must already be created before you can assign it to a user. For information about creating keyboard accelerators, see "DBC - Keyboard Accelerator" in Chapter 50.

Follow these steps to create a keyboard accelerator:

1. Click **Add** to display a list of available keyboard accelerators on the Keystroke Accelerators dialog box.
2. Click the accelerator you want and then click **OK**. The accelerator appears on the Keystroke Accelerators tab as an assigned accelerator.
3. If you want to edit the keystroke accelerator (change the name, keystroke sequence, or called procedure) before assigning it to the user, click **Edit** and modify before clicking **OK**.
4. If you want to create a new keyboard accelerator, click **Add** on the Keystroke Accelerators dialog box and see "Adding or Editing Keyboard Accelerators" for instructions.
5. At the Keystroke Accelerators tab you can also edit or delete accelerators, grant or revoke the user's access to them, or restrict the user's access to the class default.
    - To edit a keyboard accelerator on this tab, click the accelerator and then click **Edit**. See "Adding or Editing Keyboard Accelerators" for instructions.
    - To delete a keyboard accelerator from the user's access list, click the accelerator in the Define User dialog box and click **Delete/Revert**.
    - To grant or revoke keyboard accelerator access on a custom basis (supersede class rights), select the keyboard accelerator and click either **Grant** (Return to give access) or **Revoke (Return to remove access)**.
    - To remove any customized access created for a listed keyboard accelerator, select the workstation and click **Revert To Class.**
6. Click **OK** to accept the user's keyboard accelerator assignments.

58.4.8 Event Toolbars Tab

Use this function to give the user customized toolbar access to commands and events. You can perform any hardware action on a logical device, execute a CCTV command, or change the state of a Reader.

To assign or edit a user's access to toolbar commands:

1. In the Database Configuration tree list, click the **Users** icon to display the user icons in the right pane.
2. Right-click the user's icon, and select Properties to display the Edit Users dialog box.
3. Click **Event Toolbars** to display the Define Toolbar Buttons dialog box.

4. Click the **Defer-To-Class** check box to un-check the box and disable the default toolbar settings. This activates the Define Toolbar Buttons dialog box.
5. Click **Add Command** to display the Toolbar Maintenance dialog box.
6. From the Command drop-down list, select the command for which you want to create toolbar access.
7. From the Bitmap File drop-down list, select the bitmap image file that you want to represent the command on the toolbar.
8. In the Status Text field, enter text that will appear in the status line of the Alarm Monitor.
9. In the Balloon Text field, enter the text that will appear over the program button in the Alarm Monitor.
10. Click **OK**.

To assign or edit a user's toolbar access to event procedures:

1. In the Database Configuration tree list, click the **Users** icon to display the user icons in the right pane.
2. Right-click the user's icon and select **Properties** to display the Edit User's dialog box.
3. Click **Event Toolbars** to display the Define Toolbar Buttons dialog box.
4. Select the **Defer-to-Class** check box to un-check the box and disable the default toolbar settings. This activates the Define Toolbar Buttons dialog box.
5. Click **Add Event** to display the Toolbar Maintenance dialog box.
6. Click the button next to the Event field, and click **Define** to display the Event Procedures dialog box.
7. To select a procedure that is already defined in the dialog box, select the event and click **OK**. To define a new event, refer to "Overview" for instructions.
   Click **Add** to display the Define Event Procedure dialog box.
8. Click the button next to the Logical Device field, and select the logical device on which you want to execute the command. The devices associated with this logical device appear in the List of Devices box.
9. To execute the command on all of the listed devices, click the **Execute Procedure on All Devices** check box and click **OK**. To execute the

command only on some of the devices, click those devices and then click **OK**.

58.4.9 Partitions Tab

Use this function to assign, delete, grant or revoke a user's access to partitions. See "Overview" for an explanation of the use of partitions.

To assign a partition to a user:

1. Click **Add** to display the Partition Maintenance dialog box.
2. Select one or more of the listed partitions and click **OK**.
3. If the partition you want is not listed on the Partition Maintenance dialog box, click **Add** on this dialog box.
4. Enter the description of the new partition and click **OK** to return to the Build Partition List.
5. Select the new partition and click **OK**.

To delete a partition from a user:

1. In the Build Partitions List, select the partition you want to delete and click **Delete**.
2. Click **Yes** to confirm the deletion.

To grant or revoke partitions to or from a user:

The partition must have grant status to be active. A partition with a revoke status remains on the list but does not function as a partition for the user. Therefore, assign Grant status to the partitions you want to be active, and Revoke status to the partitions you want to be inactive.

1. On the Build Partition List, select the partitions you want to be active in the user's profile, and click **Grant** (if it is not already set to Grant).
2. Select the partitions you want to be inactive in the user's profile, and click **Revoke**.

58.4.10 Alarm Pages Tab

Use this function to assign alarm pages to a user. An alarm page configures the Alarm Monitor display of incoming alarms. See "Overview" for more information about alarm pages.

Note: An alarm page must already be created before you can assign it to a user. For information about creating alarm pages, see "Overview".

1. Click **Add** to display a list of available alarm pages on the Alarm Page dialog box.

2. Click the alarm page you want and then click **OK**. The alarm page appears on the Alarm Pages tab as an assigned alarm page. Note that if you want to edit the alarm page before assigning it to the user, click **Edit** and modify before clicking **OK**. See "Adding or Editing an Alarm Page" for editing instructions.
3. If you want to create a new alarm page, click **Add** on the Alarm Page dialog box and see "Adding or Editing an Alarm Page" for instructions.
4. At the Alarm Pages tab you can also edit or delete alarm pages, grant or revoke the user's access to them, or restrict the user's access to the class default.
    - To edit an alarm page on this tab, click the alarm page and then click **Edit**. See "Adding or Editing an Alarm Page" for instructions.
    - To delete an alarm page from the user's access list, click the alarm page in the Alarm Pages tab and click **Delete/Revert**.
    - To grant or revoke alarm page access on a custom basis (supersede class rights), select the alarm page and click either **Grant** (Return to give access) or **Revoke** (Return to remove access).
    - To remove any customized access created for a listed alarm page, select the workstation and click **Revert To Class**.
5. Click **OK** to accept the user's alarm page assignments.

58.4.11 Badge Profiles Tab

Use this function to assign a badge profile to a user, edit the badge profile for the user, or remove the profile from the user. A user badge profile defines the tabs presented in the badging application, turns on or off the Auto Disable Cards function, and defines which card fields will be searchable.

Note: A badge profile must already be created before you can assign it to a user. For information about creating badge profiles, see "DBC - Badge Profiles" in Chapter 30.

1. Click **Add** to display a list of available badge profiles on the Badge Profiles dialog box.
2. Click the badge profile you want and then click **OK**. The badge profile appears on the Badge Profiles tab as an assigned accelerator. Note that if you want to edit the badge profile before assigning it to the user, click **Edit** and modify before clicking **OK**. See "Adding or Editing a Badge Profile" for editing instructions.
3. If you want to create a new badge profile, click **Add** on the Badge Profiles dialog box and see "Adding or Editing a Badge Profile" for instructions.

4. At the Badge Profiles tab you can also edit or delete accelerators, grant or revoke the user's access to them, or restrict the user's access to the class default.
    - To edit a badge profile on this tab, click the profile and then click **Edit**. See "Adding or Editing a Badge Profile" for instructions.
    - To delete a badge profile from the user's access list, click the profile in the Badge Profiles tab and click **Delete/Revert**.
    - To grant or revoke badge profile access on a custom basis (supersede class rights), select the badge profile and click either **Grant** (Return to give access) or **Revoke** (Return to remove access).
    - To remove any customized access created for a listed badge profile, select the workstation and click **Revert To Class.**
5. Click **OK** to accept the user's badge profile assignments.

58.4.12 Event Procedures Tab

Use this function to assign event procedures to a user, edit or delete a user's event procedures, and grant or revoke a user's access to event procedures.

An event procedure is an event-triggered execution of one or more commands. You can create an event procedure for a user that executes on a logical device, with a CCTV command, or with a change the state of a Reader. The commands do not have to be executed on the same device, CCTV command, or Reader.

Note: An event procedure must already be created before you can assign it to a user. For information about creating event procedures, see "Overview".

1. Click **Add** to display a list of available event procedures on the Event Procedures dialog box.
2. Click the event procedure you want and then click **OK**. The badge procedure appears on the Event Procedures tab as an assigned procedure. Note that if you want to edit the event procedure before assigning it to the user, click **Edit** and modify before clicking **OK**. See "Overview" for editing instructions.
3. If you want to create a new event procedure, click **Add** on the Event Procedures dialog box and see "Adding or Editing Event Procedures" for instructions.
4. At the Event Procedures tab you can also edit or delete procedures, grant or revoke the user's access to them, or restrict the user's access to the class default.
    - To edit an event procedure on this tab, click the procedure and then click **Edit**. See "Adding or Editing Event Procedures" for instructions.

- To delete an event procedure from the user's access list, click the procedure in the Event Procedures tab and click **Delete/Revert**.
- To grant or revoke event procedure access on a custom basis (supersede class rights), select the event procedure and click either **Grant** (Return to give access) or **Revoke** (Return to remove access).
- To remove any customized access created for a listed event procedure, select the workstation and click **Revert To Class.**

5. Click **OK** to accept the user's event procedure assignments.

58.5 Copying a User

Use this function to create a copy of a user. This can be a fast way to create a new user. If the original user will be similar to the new one, you can copy the original and change only a small number of its properties to create the new user.

Note: This method does not copy the device status filtering configuration.

1. In the Pro-Watch Database Configuration tree list, click the **Users** icon to display the currently-configured users in the right pane.
2. Right-click the icon of the user you want to copy and select **Copy**.
3. Right-click again anywhere in the right pane and select **Paste**. A new icon with “Copy of [original user name]” appears in the right pane.

58.6 Types of User Icons

In Pro-Watch there are three main types of users represented by the following three icons:

Icon	Description
 e200879 User	Regular user signing in with a regular user license.
 Jay Krandal	Administrative user signing in with administrative access rights.
 e200879 User	User signing in with a badging license.

58.7 Deleting a User

1. In the Pro-Watch Database Configuration tree list, click the **Users** icon to display the users in the right pane.
2. Right-click the user you want to delete and select **Delete.** The prompt, “Delete the user [user name]?” appears.
3. Click **Yes**.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

DBC – Workstations

59

In this chapter ...

Overview

Workstation Functions

Adding Workstations

Editing a Workstation

Viewing Dependencies of a Workstation

Types of Workstation icons

Code of Federal Regulations (21 CFR 11) Functionality

Deleting a Workstation

59.1 Overview

Use this function to add workstations to the Pro-Watch network, delete the workstations, or modify their configurations.

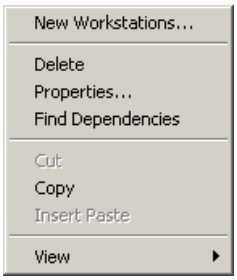
Note: Simply adding a workstation from this tab is only the first step in making the workstation an active network device. The workstation must also be assigned to a routing group to receive events (see "DBC - Routing Groups" in Chapter 55), and assigned to either a class or to a user to receive access privileges (see "DBC - Classes" in Chapter 36 or "DBC - Users" in Chapter 58). Also, the workstation user must be assigned to the workstation (see "Workstations Tab").

Warning: Both the user's workstation and the user must be assigned to the same class. The workstation will be disabled if the user and the workstation are assigned to different classes.

59.2 Workstation Functions

To access workstation functions:

1. In the Pro-Watch Database Configuration tree list, click the **Workstations** icon to display the currently-configured workstations (if there are any) in the right pane of the Pro-Watch window.
2. Right-click a workstation icon to display the pop-up menu:

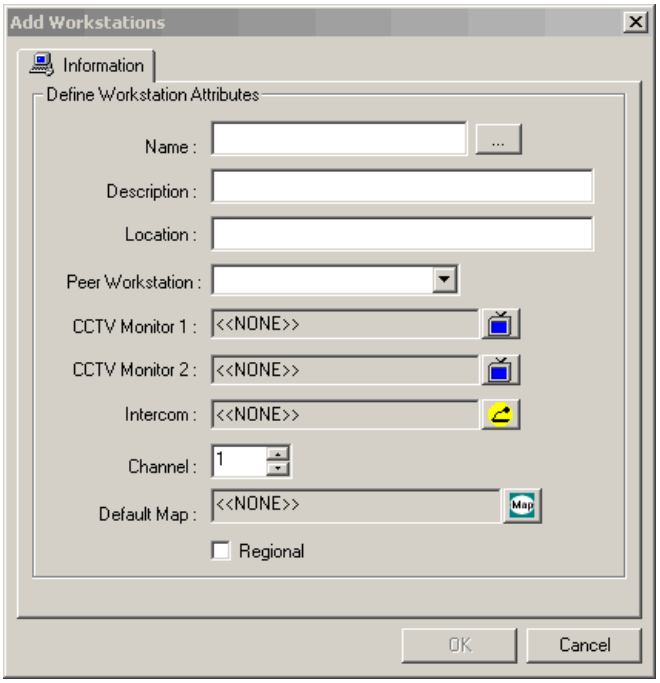


3. Use the following table to select a function:

Click...	To...
New Workstations...	Add a new workstation. See "Adding Workstations".
Delete	Delete a workstation. See "Viewing Dependencies of a Workstation".
Properties...	Edit a current workstation. See "Adding or Editing Partitions".
Find Dependencies	Display the names of all resources that depend upon the partition. See "Viewing Dependencies of a Workstation".
Copy	Copy a partition and insert the copy's icon in the Pro-Watch window. See "Copying a Partition" in Chapter 53.
View	Change the way the icons are displayed in the Pro-Watch window.

59.3 Adding Workstations

1. In the Pro-Watch Database Configuration tree list, right-click **Workstations** to display a pop-up menu.
2. Select **New Workstations** to display the Add Workstations dialog box:



3. Click the button next to the Name field and select a workstation from the tree list.
4. Enter text in the Description field that will identify the workstation.
5. Enter text in the Location field that will identify the workstation's location in the enterprise.

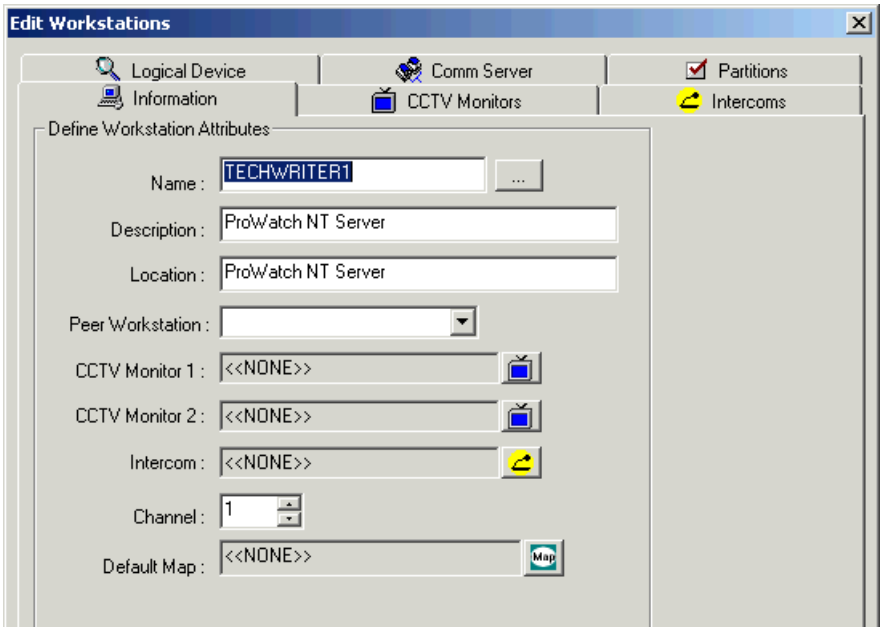
Note: Select up to two configured CCTV monitors and one intercom to which this workstation will connect.

You must first configure names and ports for CCTV Monitors and Intercoms before you can assign them to a workstation. See "HW Config - CCTV" in Chapter 21 for instructions.

6. Select the channel (1 to 100) this workstation will use.
7. Click the button next to the Default Map field to select a configured map that locates the workstation.
8. Click **OK** to accept the workstation configuration.

59.4 Editing a Workstation

1. In the Pro-Watch Database Configuration tree list, click **Workstations** to display in the right pane the icons of currently-configured workstations.
2. Right-click the workstation you want to edit, and select **Properties**. The Edit Workstations dialog box appears.



3. Finish the workstation's configuration by completing the Edit Workstation information tabs described in the following sections.

59.4.1 Information Tab

Use this tab to enter basic workstation information.

1. Enter text in the Description field that will identify the workstation.
2. Enter text in the Location field that will identify the workstation's location in the enterprise.

Note: Select up to two configured CCTV monitors and one intercom to which this workstation will connect.

You must first configure names and ports for CCTV Monitors and Intercoms before you can assign them to a workstation. See "HW Config - CCTV" in Chapter 21 for instructions.

3. Select the channel (1 to 100) this workstation will use.
4. Click the button next to the Default Map field to select a configured map that locates the workstation.

5. Click **OK** to accept the workstation configuration.

59.4.2 CCTV Monitors Tab

Use this tab to assign CCTV monitors to the workstation. Note that a monitor must be configured in the network before it can be assigned to a workstation. See "HW Config - CCTV" in Chapter 21 for instructions on configuring a monitor in the network.

1. In the Pro-Watch Database Configuration tree list, click the **Workstations** icon to display the configured workstations in the right pane.
2. Right-click the icon representing the workstation to which you want to assign the CCTV monitor and select **Properties**.
3. Click **CCTV Monitors** to display the Define Workstation CCTV Monitors dialog box. The monitors currently assigned to this workstation (if any) appear in this dialog box.
4. To assign a new CCTV monitor to the workstation, click **Add** to display the CCTV Monitors dialog box. This dialog box shows all of the currently-configured CCTV monitors in the Pro-Watch network. Select the monitor you want, and click **OK**. The monitor is assigned to the workstation.
5. To delete a monitor from the workstation's monitor list, select the monitor on the Define Workstation CCTV Monitors dialog box and click **Delete**.

59.4.3 Intercoms Tab

Use this tab to assign an intercom to a workstation. Intercoms are often used to supplement an access control system by allowing a dispatcher to communicate with an individual at an access point. Intercoms can also be used as security devices, providing emergency call alarms, as seen on college campuses and parking garages.

Note: An intercom cannot be assigned to a workstation until it is first configured in the network. See "HW Config - Intercom" in Chapter 23 for instructions on configuring an intercom in the network.

1. In the Database Configuration menu, click **Workstations** to display the configured workstations in the right pane.
2. Right-click the icon representing the workstation to which you want to assign the intercom and select **Properties**.
3. Click **Intercoms** to display the Define Workstation Intercoms dialog box. The intercom currently assigned to this workstation (if any) appears in this dialog box.
4. To assign a new intercom to the workstation, click **Add** to display the Intercoms dialog box with currently-configured intercoms. Select the

intercom you want, and click **OK**. The intercom is assigned to the workstation.

5. To delete an intercom from the workstation's monitor list, select the intercom on the Define Workstation Intercoms dialog box and click **Delete**.

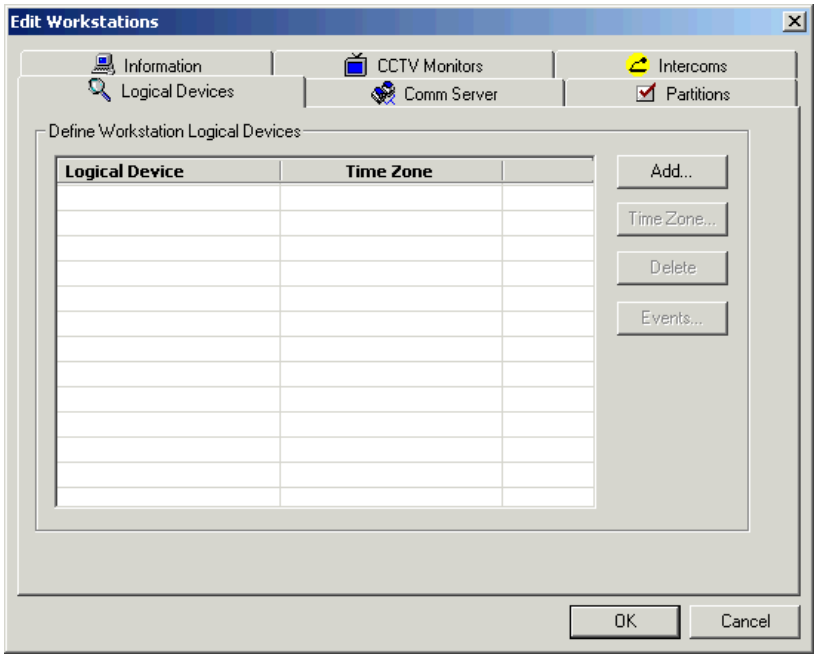
59.4.4 Logical Devices Tab

Use this tab to assign logical devices to a workstation, or to edit logical devices already assigned to a workstation.

1. In the Pro-Watch Database Configuration tree list, click the **Workstations** icon to display in the right pane all the icons representing the currently-configured workstations.
2. Right-click the icon representing the workstation to which you want to assign the logical device and select **Properties**.

Note: Click **Logical Devices** to display the Define Workstation Logical Devices dialog box.

You can view the workstation's Logical Devices in the Verification Window by clicking the Logical Device icon in the Hardware Configuration Tree. Up to eight Logical Devices per workstation can be viewed in the Verification Window. See "Logical Device Icon" in Chapter 6 for more information about the use of the Logical Device icon.



3. Click **Add** to display currently-configured logical devices in the Logical Devices dialog box.

4. Select one or more logical device and click **OK**. The Time Zones dialog box appears.
5. Select the time period during which the workstation will monitor the device(s) and click **OK**. The devices are assigned to the workstation.
6. To delete a logical device from a workstation:
   a. Click the logical device and then click **Delete**. The prompt, "Are you sure you want to delete the selected resource?" appears.
   b. Click **Yes**.
7. Click **Events** to assign events to the logical devices assigned to the workstation. The Verification Window Popup - Events dialog box appears.
8. Click to select the first event you want to assign to the logical device in the Available Events box, then click the left-arrow button to transfer the event to the Selected Events box.
9. Repeat step 4 for other events you want to assign to the logical device.
10. Click **OK**.

59.4.5 Communications Server Tab

Use this tab to identify a workstation as the communications server and to allow the workstation to communicate with the hardware.

If the current workstation is a communications server, check the Communications Server check box. Then, indicate with the Communications Server Type option button whether the workstation is a Remote or the Primary server.

59.4.6 Partitions Tab

You can add or delete partitions for workstations. See "DBC - Partitions" in Chapter 53 for an explanation of the use of partitions.

To add a partition to a workstation:

1. In the Partitions Tab, click the **Add** button to display the Available Partitions dialog box.
2. Select one or more of the listed partitions and click **OK**.
3. If the partition you want is not listed on the Available Partitions dialog box, click **Add** on this dialog box.
4. Enter the description of the new partition and click **OK** to return to the Build Partition List.
5. Select the new partition and click **OK**.

To delete a partition from a workstation:

1. In the Partitions Tab, click to select the partition you want to delete and click **Delete**.
2. Click **Yes** to confirm the deletion.

59.5 Viewing Dependencies of a Workstation

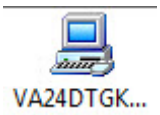
Use this function to view and edit the Workstation's dependencies. The **Workstation** object depends upon the Site, Class, User, and Routing Group objects.

*To view and edit **a Workstation's dependencies**:*

1. Right-click the icon of an existing Workstation in the right pane of the Pro-Watch Database Configuration window, and select **Find Dependencies...** to display the Dependencies dialog box. The Dependencies dialog box appears and lists the Workstation's dependencies.
2. To edit or delete the dependency, click the specific dependency in the list to display its Edit dialog box.
3. After you finish viewing, click **OK** to close the dialog box.

59.6 Types of Workstation icons

In Pro-Watch there are two main types of workstations represented by the following two icons:

Icon	Description
	Wokstation currently logged ON (LIGHT BLUE).
	Workstation currently logged OFF (DARK BLUE).

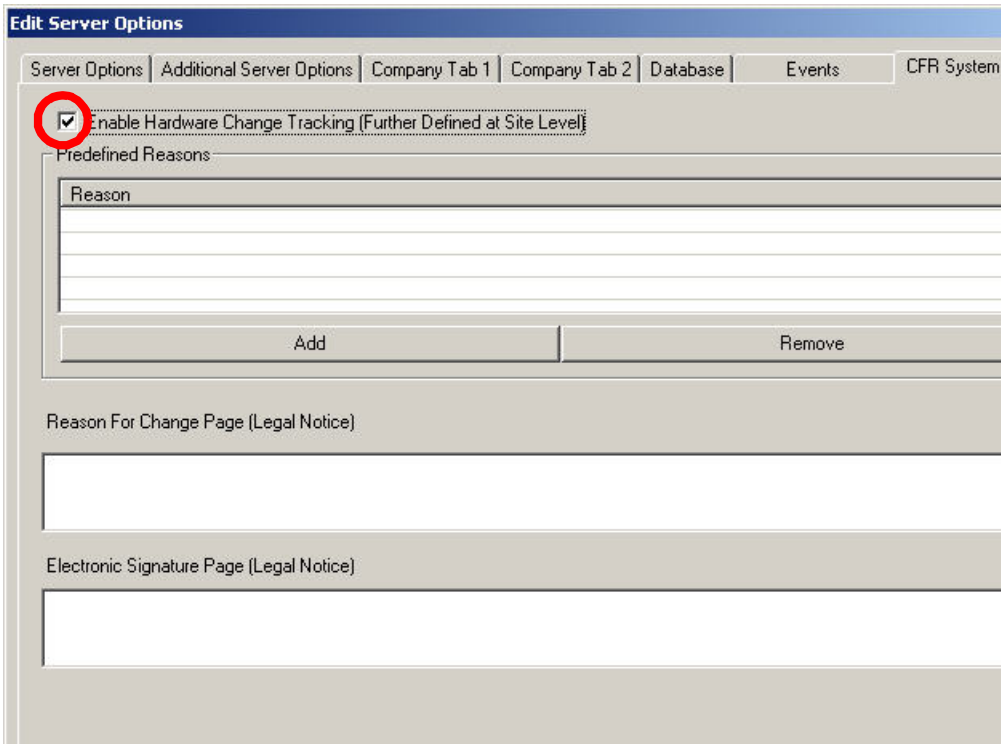
59.7 Code of Federal Regulations (21 CFR 11) Functionality

The Pro-Watch supports digital signature tracking functionality required by Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11).

Note: The 21 CFR 11 setup requires the user to configure more than one Pro-Watch module, including the Administration, Database and Hardware configuration modules. This multi-module process is described here below, with the appropriate links provided to this section in the appropriate chapters of this User's Guide.

To add compliance with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11):

1. In the Programs tab, select **Administration**.
2. Click **Add Program** to display the Programs and Functions dialog box.
3. Select **CFR Maintenance** from the Program drop-down menu.
4. Select the **Grant** option button for Privileges for Class or User.
5. Click **OK** to add the functionality to the Administration program.
6. Click **OK** to close the Edit Users window.
7. Select **File > Server Options** from the main menu to display the Edit Server Options screen.
8. Select the **CFR System Setting** tab.

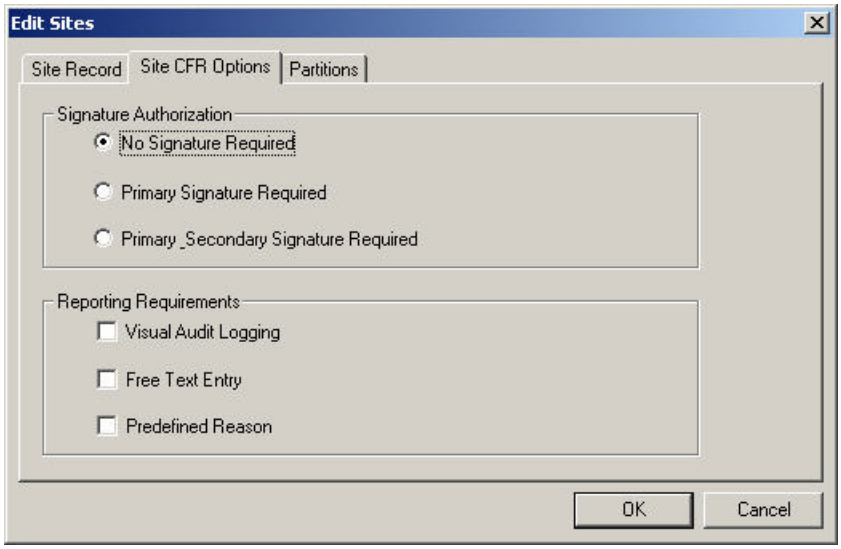


9. Select the **Enable Hardware Change Tracking (Further Defined at Site Level)** check box.

Note: Click **Add** and type in one or more reasons why the 21 CFR 11 tracking is enabled. The reason(s) are now listed in the list box.

The user must enter at least one reason. The default is "Unknown Reason."

10. Select a reason and click **Remove** to remove it from the Predefined Reasons list box.
11. Enter a text for the **Reason For Change Page (Legal Notice)** text box. For example: "Pursuant to Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11), all changes must be recorded with a reason for that change."
12. Enter a text for the **Electronic Signature Page (Legal Notice)** text box. For example: "Pursuant to Section 11.100 of title 21 of the Code of Federal Regulations, this is to certify that (Name of the Company) intends that all electronic/digital signatures executed by our employees, agents or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures."
13. Click **OK** to close the Edit Server Options screen.
14. Click **Hardware Configuration** function icon to display the existing sites in the middle pane.
15. Select a **site** and right-click its **name** to display the pop-up menu.
16. Select **Properties** to display the Edit Sites screen.
17. Click the **Site CFR Options tab**.



18. Select one of the following **Signature Authorization** option buttons:
    - No Signature Required.
    - Primary Signature Required.
    - Primary and Secondary Signature Required.
19. Select one of the following **Reporting Requirements** check boxes:
    - Visual Audit Logging.
    - Free Text Entry.
    - Predefined Reason.

Note: Click **OK** to save and close the Edit Sites screen.

If Primary or Primary-and-Secondary signature options are selected, the Pro-Watch displays an electronic signature verification dialog box when editing a device type.

59.8 Deleting a Workstation

Use this function to delete a Workstation from the Pro-Watch database.

1. In the Pro-Watch Database Configuration tree list, click the **Workstations icon** to display the procedures in the right pane.

Note: Right-click the Workstation you want to delete and select **Delete**.

You cannot delete a Workstation that has dependencies. A dependency is another database object that includes the Workstation in its configuration. The Workstation object depends upon the Site, Class, User, and Routing Group objects. If the Workstation has no current dependencies, you are prompted to confirm the deletion. However, if the Workstation does have current dependencies, the Dependencies dialog box appears.

2. If you still want to delete the Workstation:
    a. Click on each of the dependencies listed in the Dependencies dialog box to display each dependency's Edit [object name] dialog box.
    b. Either change or delete each of the objects listed as dependencies.
3. Repeat step 2 and click **Yes** at the prompt to delete the Workstation.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Badge Building

60

In this chapter ...

Overview

Adding a Badge Profile

Editing a Badge Profile

Using Badge Builder Layout Options

Badge Utilities

60.1 Overview

Use the Pro-Watch Badge Builder to create a complete badge profile. The badge profile is used by the Badging component of Pro-Watch to create badges for those using the access control system in your enterprise.

A Pro-Watch badge profile is a collection of profile pages, and a profile page is a collection of badge fields (see the following figure).

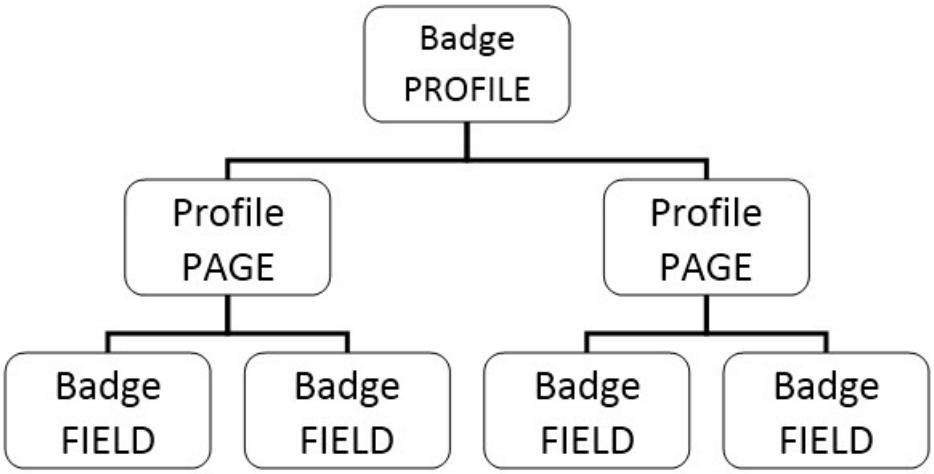


Figure 60-1 Badge Profile Components

Creating badge profiles, profile pages, and badge fields is only the first step in implementing a badging system for your enterprise. You need to use the Database Configuration component (see Chapter 27, *Database Configuration (DBC)*) and the Badging component (see Chapter 2,) in addition to this Badge Builder utility to implement the enterprise's entire badging system.

The table below lists the badge-building tasks in sequence and refers you to the appropriate chapter and section for instructions and information:

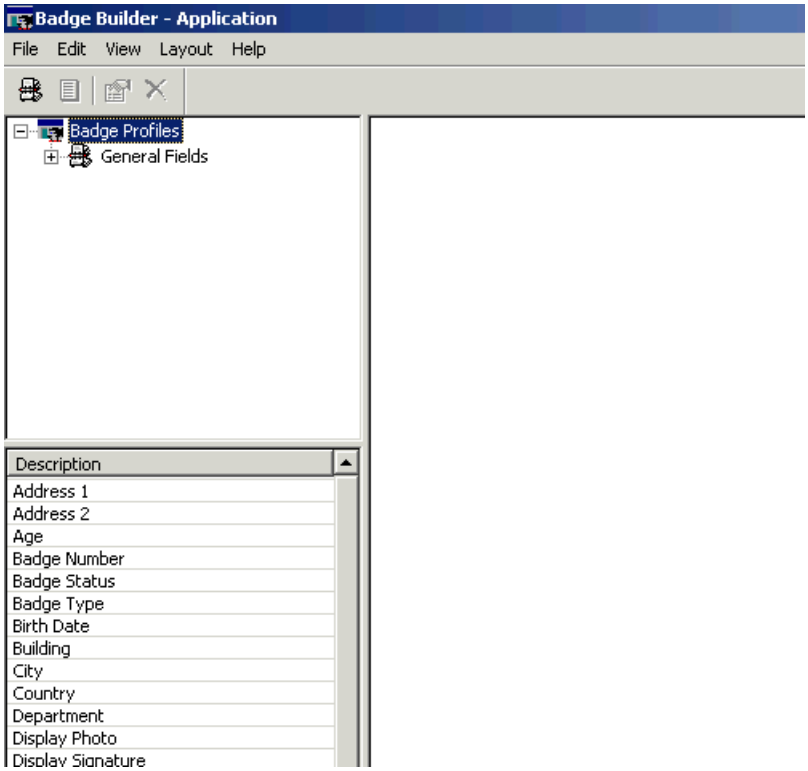
Step #	Task	Refer to ...
1	Create the badge profile.	"Adding a Badge Profile" in this chapter.
2	Create the badge profile pages.	"Adding Badge Profile Pages" in this chapter.
3	Create the badge fields, if necessary.	"Adding a Badge Profile" in this chapter.
4	Assign the badge fields.	"Adding a Badge Field to a Profile or Editing a Badge Field" in this chapter.

Step #	Task	Refer to ...
5	Designate the badge types.	"DBC - Badge Types" in Chapter 32.
6	Create badge statuses.	"DBC - Badge Statuses" in Chapter 31.
7	Assign cards to the badge.	"Adding a Card" in Chapter 2.
8	Assign the badge profile to a class or user.	"DBC - Badge Profiles" in Chapter 30.
9	Assign the badges to a class or user.	"" in Chapter 2.
11	Assign the badges to users.	"Adding a Badge" in Chapter 2.

To access Badge Builder, follow these steps:

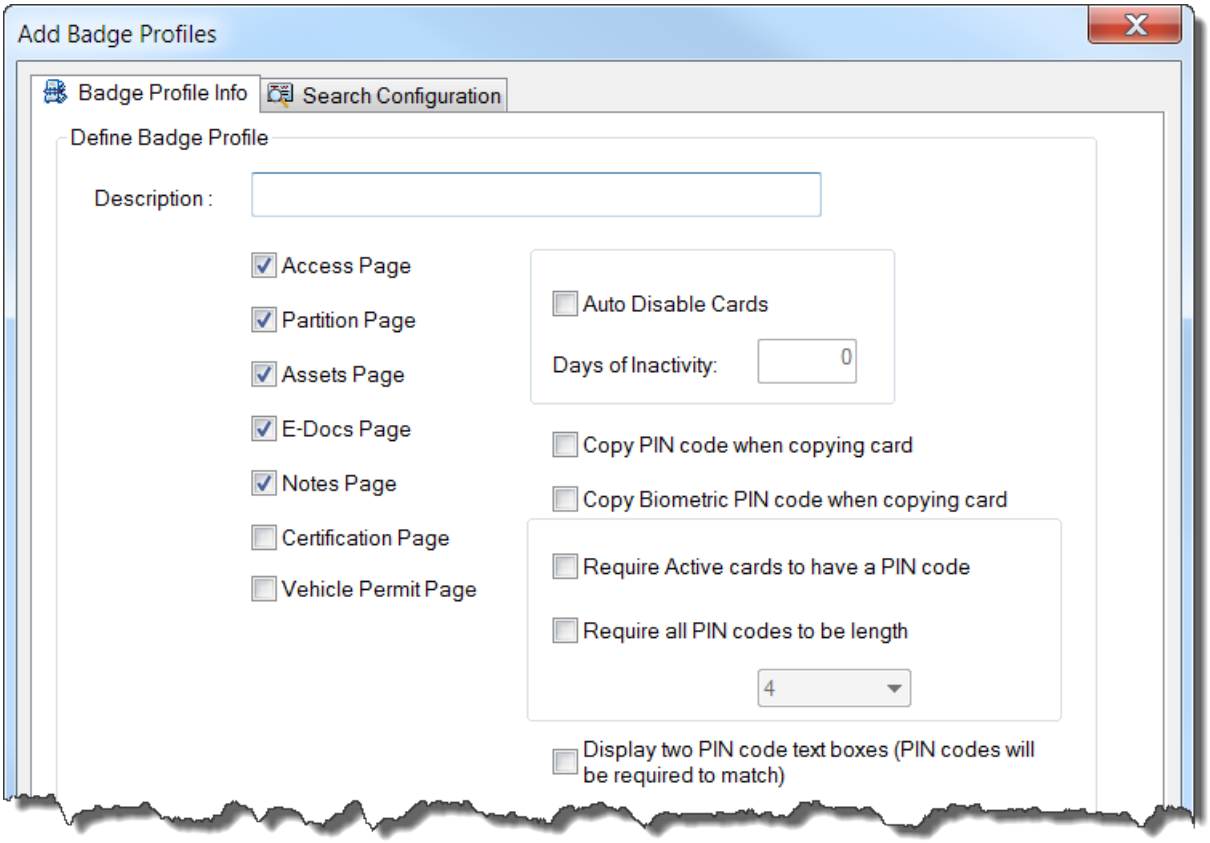
1. From the left Pro-Watch pane, click **Administration**.

2. Click the **"+" sign** next to the **Executables** folder to expand it.
3. Double-click the **Badge Builder** icon to launch the Pro-Watch Badge Builder application and display the Badge Builder-Application dialog box in a new window:



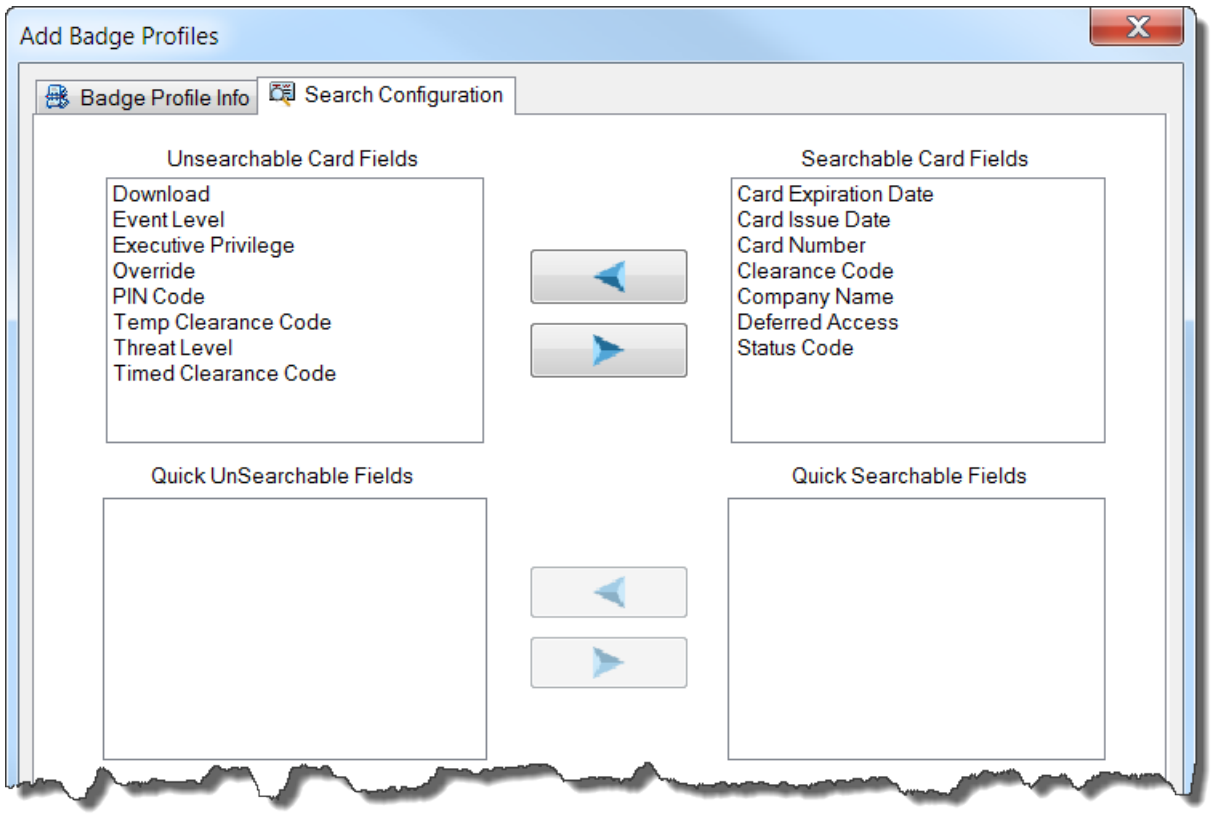
60.2 Adding a Badge Profile

1. From the Badge Builder menu bar, select **File > New Profile**. The B**adge Profile Info** tab of the **Add Badge Profiles** dialog box appears.



2. Enter a profile description in the **Description** field.
3. To add an **Access Page, Partition Page, Assets** (used to be called "Brass Key") **Page, E-Docs Page, Notes Page, Certification Page**, or **Vehicle Permit Page** to the profile, select the appropriate page check box. These pages enable you to assign access, partitions, assets, e-docs, notes, certifications, and vehicle permits to a badge. Note that these privileges can also be assigned in other ways, such as by user or class. See Chapter 27, *Database Configuration (DBC)* for more information.
4. Select the **Auto Disable Cards** check box and enter the number of days of inactivity to disable a badge's cards (see "Adding a Card" in Chapter 2 for an explanation of cards) after a specific number of days of inactivity. After Auto Disable Cards check box is selected and a value is entered for the number of days of inactivity, this number becomes the default value when adding a new card for a badge.
5. Select **Copy PIN code when copying card** check box to copy PIN code when copying card.

6. Select **Copy Biometric PIN code when copying card** check box to copy Biometric PIN code when copying card.
7. Select **Require Active cards to have a PIN code** check box to require active cards to have a PIN code.
8. Select **Require all PIN codes to be length** check box and then select a number from the **drop-down menu** to require all PIN codes to have a specific number of digits.
9. Select **Display two PIN code text boxes (PIN codes will be required to match)** check box to require PIN codes to match.
10. Select and display the **Search Configuration** tab of the **Add Badge Profiles** screen:



Note: The Searchable card fields list created here is used in **Advanced Search** to search by card fields.

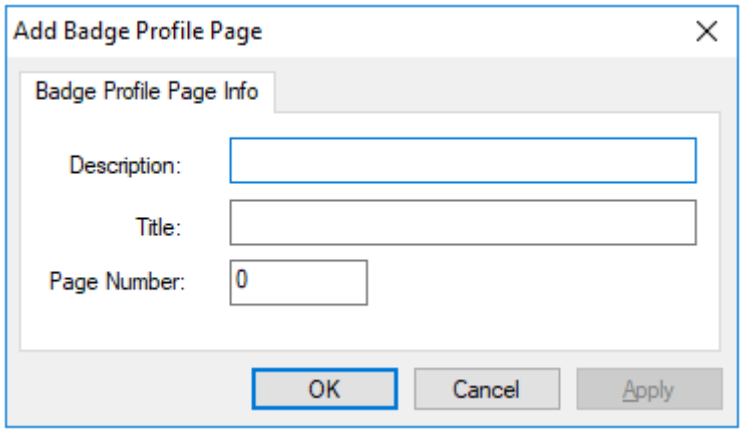
11. Select the card fields that you want to be searchable in the **Searchable Card Fields** text list and then click the LEFT arrow to shift them to the **Unsearchable Card Fields**.
12. Select the card fields that you want to be unsearchable in the **Unsearchable Card Fields t**ext list and then click the RIGHT arrow to shift them to the **Searchable Card Fields**.

13. Repeat the above two steps for the **Quick Searchable Fields** and **Quick Unsearchable Fields**.
14. Click **OK** to accept the new badge profile. Notice that the new profile now appears in the **Badge Profiles** tree in the **Badge Builder** dialog box.

60.2.1 Adding Badge Profile Pages

The Pro-Watch default badge profile ships with two standard profile pages: Badge Information and Employee Information. If these pages suit your needs, you should not create a new profile page.

1. From the Badge Builder menu bar, select **File > New Page**. The Add Profile Page dialog box appears.

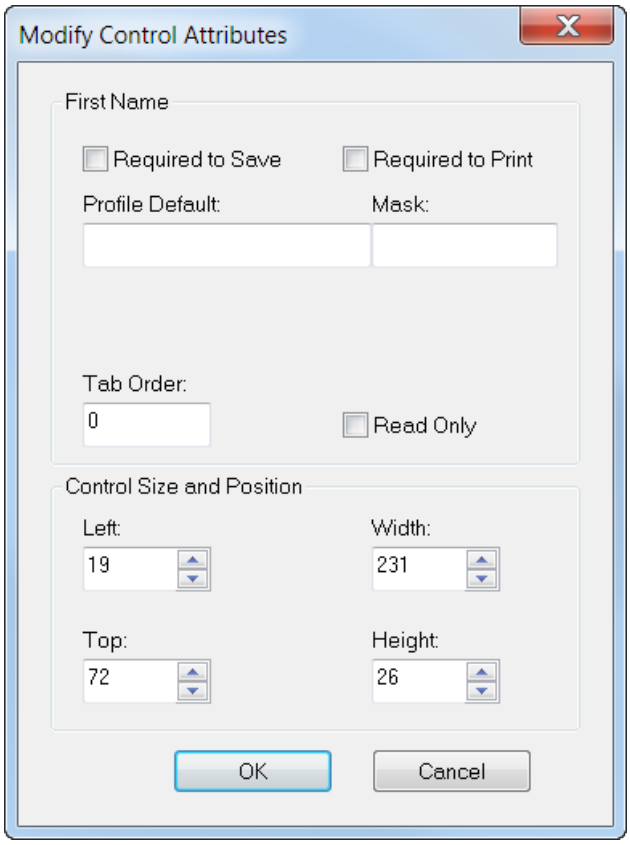


2. Enter a short description that identifies the page's content. This entry is the page name that will appear in the Badge Profile tree menu.
3. Enter a page title. This title shows up on the tab in Badging module.
4. Enter a page number. This number determines the order in which the Badge Profiles tree menu lists the pages for this profile and the tab order of folders in Badging.
5. Click **OK** to display the newly created page in the left pane, under the badge profile it belongs to.
6. Double-click the page icon to display the blank page on the right pane. The title bar of the page will look grayed out.
7. Drag and drop any of the fields from the Description box in the left corner of the dialog box to the page. Arrange the field layout on the page to suit your needs by selecting one or more of the alignment options from the Layout menu item. See "Aligning Badge Fields".

60.2.2 Modifying Control Attributes

Note: You can define and edit the data type of any badge field in **Administration > Badge Utilities > Badge Fields** window.

1. Select **Administration > Executables > Badge Builder** to launch the **Badge Builder** module.
2. From the **Badge Profiles** tree-view, select a **Badge Field** to modify.
3. To modify the control attributes of the individual badge fields, either select the field and press **Enter**, or double-click the field to display the **Modify Control Attributes** dialog box for that specific badge field:



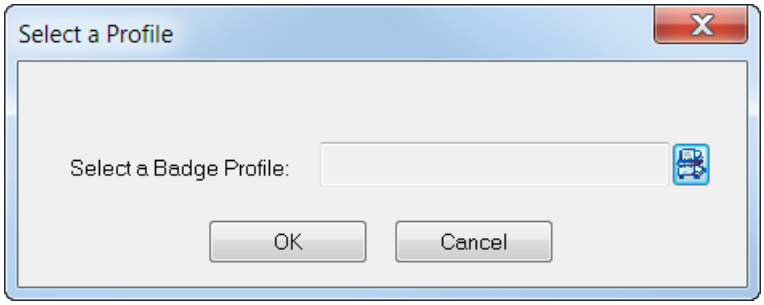
4. When you select the **Required to Save** check box, the badge field becomes a mandatory field for saving the badge record (designated with an asterisk (*) appearing before it). If you do not enter a value into this field you will not be able to save the badge record.
5. When you select the **Required to Print** check box, the badge field becomes a mandatory field for printing the badge record. If you do not enter a value into this field you will not be able to print the badge record.
6. The **Profile Default** field will appear only for fields that are of the following data type: short, int, varchar, money, datetime, float. You can populate the **Profile Default** field in two ways.

a. The system will display a **drop-down menu** when you can assign one of the pre-existing list of values as the field's default value. For example, if you have a Badge Type field, then the drop-down menu might display pre-populated values like "Contractor" or "Standard Employee"." In those cases, select an item from the drop-down menu to assign it as the field's **Profile Default** value.

b. If there are no pre-existing list of values for the field, then enter an appropriate value as the **Profile Default** value. For example, for First Name or Last Name fields, you can type in the name of the person into the field.

7. Enter a **Mask** if you would like the entered value to have a specific format, like for example a phone number or a social security number. Use the following characters for your mask:
   - # = number
   - L = letter
   - A = number or letter
   - & = any character
   - For example, for a phone number, you may enter the following mask: "(###) ###-####" (quotation marks not included).
8. Enter a numeric value (integer) into the **Tab Order** field to determine the path and order in which the cursor will navigate to this badge field when you press the Tab key (on the keyboard). Default value is zero ("0").
   - For example, if the tab order value for your badge field is zero, then it will either be the very first field reached by the tab key or it will be among the first group of fields navigated to by the tab key. This means tab order values do not have to be unique; there can be more than one badge field sharing the same tab order value.
9. Select the **Read Only** check box to render the field read-only.
10. To control the precise dimensions and coordinates of the field, enter the appropriate numeric pixel values into the **Left** (defines the distance of the field in pixels from the left edge of the page), **Top** (defines the distance of the field in pixels from the top edge of the page), **Width** (defines the width of the field in pixels), and **Height** (defines the height of the field in pixels) fields.
11. Click **OK** to close the **Modify Control Attributes** dialog box and return to the **Badge Information** screen.

12. Click to select the new page in the **Badge Profiles** dialog box, then select **Edit > Assign to Profile**. The **Select a Profile** dialog box appears:



13. Click the browse button to select the profile to which you want to assign the new page. Select **Define** from the pop-up menu to display the list of existing badge profiles. Either select one and click **OK**.
14. Select an existing badge profile from the Badge Profiles dialog box and click **OK** to place the new page in the selected profile.
15. If none of the existing badge profiles are appropriate, click **Add** in the Badge Profiles dialog box and proceed to add a new badge profile for the new page. Once the new profile is added, select it in the Badge Profiles dialog box and click **OK** to place the new page in the selected profile.

60.2.3 Adding a Badge Field to a Profile or Editing a Badge Field

Use this function to add, edit, or arrange the fields that will appear on the badge pages.

To add or edit a badge field:

Double-click the badge page icon in the left pane to display the appropriate badge page in the right pane of the Badge Builder screen.

To add a field:

1. Drag and drop any of the fields from the Description box in the left pane of the Badge Builder dialog box to the page.
2. Arrange the field layout on the page to suit your needs.

Note: This procedure only adds badge fields that are already defined and displayed in the Description box. To define a new badge field that will appear in the Description box, use Badge Utilities. See "Badge Utilities" for instructions and information.

To edit a field:

Either select the field and press **Enter** or double-click the field to display the Modify Control Attributes dialog box. See "Modifying Control Attributes".

Note: Badge profile changes have no effect on the actual badge fields in the database.

60.2.4 Deleting a Badge Field from a Profile

Follow these steps:

1. From the Badge Builder dialog box, click to select an existing profile page so it is displayed in the right pane of the Badge Builder window.
2. Click to select the badge field you want to remove.
3. Either select **Edit > Delete** from the menu bar, or press the **Delete** key on your keyboard.

60.3 Editing a Badge Profile

Follow these steps:

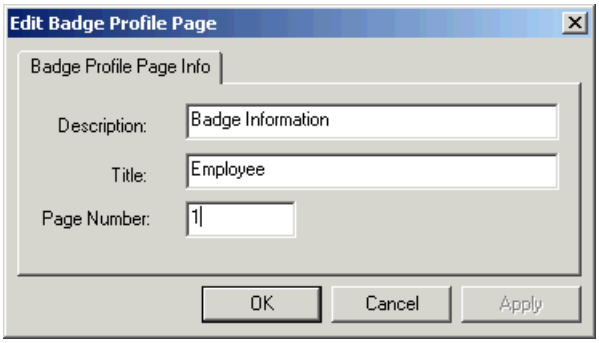
1. In the Badge Builder application, double-click **Badge Profiles** to display the list of available fields:



2. Double-click the **fields list** to reveal the list of badge profile pages:



3. Select **a page** from the list and right-click to display the pop-up menu.
4. Select **Properties** to display the Edit Badge Profile Page related to that specific badge profile page. For example:



5. Edit the **description** that identifies the page's content. This entry is the page name that appears in the Badge Profile tree menu.
6. Edit the **page title**. This title shows up on the tab in Badging module.
7. Edit the **page number**. This number determines the order in which the Badge Profiles tree menu lists the pages for this profile and the tab order of folders in Badging.
8. Click **OK** to display the edited page in the left pane, under the badge profile it belongs to.

60.4 Using Badge Builder Layout Options

Use the Badge Builder layout options to align, size, and list the badge fields for a new and existing badge profile. Either access these options from the Layout menu or from the Status menu bar at the bottom of the Badge Builder window.

60.4.1 Aligning Badge Fields

Follow these steps:

1. Create a new profile, or click to select an existing profile to display it in the right pane of the Badge Builder window.
2. Select two or more badge fields by holding down the SHIFT key while clicking each item, or by dragging the pointer around each field.
3. Select **Layout > Align**. Select one of the following:
    - Left – Aligns the left edges of the selected fields.
    - Right – Aligns the right edges of the selected fields.
    - Top – Aligns the top edges of the selected fields.
    - Bottom – Aligns the bottom edges of the selected fields.

60.4.2 Spacing Badge Fields

Follow these steps:

1. Create a new profile or click to select an existing profile to display it in the right pane of the Badge Builder window.
2. Select two or more badge fields by holding down the SHIFT key while clicking each item, or by dragging the pointer around each field.
3. Select **Layout > Space Evenly**.
4. Select one of the following:
    - Across – Evenly spaces the selected fields horizontally.
    - Down – Evenly spaces the selected controls vertically.

60.4.3 Sizing Badge Fields

Follow these steps:

1. Create a new profile or click to select an existing profile to display it in the right pane of the Badge Builder window.
2. Select two or more badge fields by holding down the SHIFT key while clicking each item, or by dragging the pointer around each field.

3. Select **Layout > Make Same Size**.
4. Select one of the following:
    - Width – Resizes the selected controls to the same width.
    - Height – Resizes the selected controls to the same height.
    - Both – Resizes the selected controls to the same size.

60.4.4 Centering a Badge Field

Follow these steps:

1. Create a new profile or click to select an existing profile to display it in the right pane of the Badge Builder window.
2. Select two or more badge fields by holding down the SHIFT key while clicking each item, or by dragging the pointer around each field.
3. Select **Layout > Center on Dialog**.
4. Select one of the following:
    - Vertical – Centers the fields vertically in the dialog box.
    - Horizontal – Centers the controls horizontally in the dialog box.

60.4.5 Using Badge Builder Status Bar

Use the following Badge Builder status bar at the bottom of the dialog box to access the same layout options available from the menu bar.



The following table identifies the status bar icons with their respective functions:

Icon	Function	Description
	Test	Calls the profile to test the profile pages' appearance and behavior.
	Align Left	Aligns the left edges of the selected fields.
	Align Right	Aligns the right edges of the selected fields.
	Align Top	Aligns the top edges of the selected fields.
	Align Bottom	Aligns the bottom edges of the selected fields.

Icon	Function	Description
	Center Vertical	Centers the fields vertically within the dialog box.
	Center Horizontal	Centers the fields horizontally within the dialog box.
	Space Across	Evenly spaces the selected fields horizontally.
	Space Down	Evenly spaces the selected fields vertically.
	Make Same Width	Resizes the selected fields to the same width.
	Make Same Height	Resizes the selected fields to the same height.
	Make Same Size	Resizes the selected fields to the same size.

60.4.6 Assigning a Badge Profile to a Class or a User

Note: Profiles and privileges assigned to individual users always take precedence over profiles and privileges assigned to classes.

Follow these steps:

1. To assign the profile to a **class**, right-click a badge profile from the left pane of the Badge Builder window and select **Edit > Assign Profile to ... > Class**. The Select a Class dialog box appears.

   To assign the profile to a **user**, right-click a badge profile from the left pane of the Badge Builder window and select **Assign Profile to... > User**. The Select a User dialog box appears.
2. Select the **Grant** check box to assign a badge profile to a user. Clear it to revoke the badge profile for a user.
3. Click the browse button to find and select the class or the user to whom you want to assign the profile.
4. Click **OK** to assign the profile to the class or user.

For further information about assigning privileges to a class or to a user, see "DBC - Classes" in Chapter 36 or "DBC - Users" in Chapter 58.

60.4.7 Testing a Badge Builder Layout

Use this function to call the badge profile and display the badge layout.

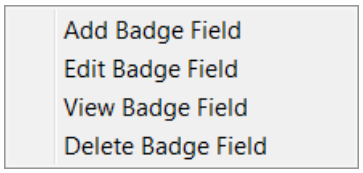
1. Create a new profile, or click to select an existing profile and display it in the right pane of the Badge Builder window.
2. Select **Layout > Test**. The profile pages appear.

60.5 Badge Utilities

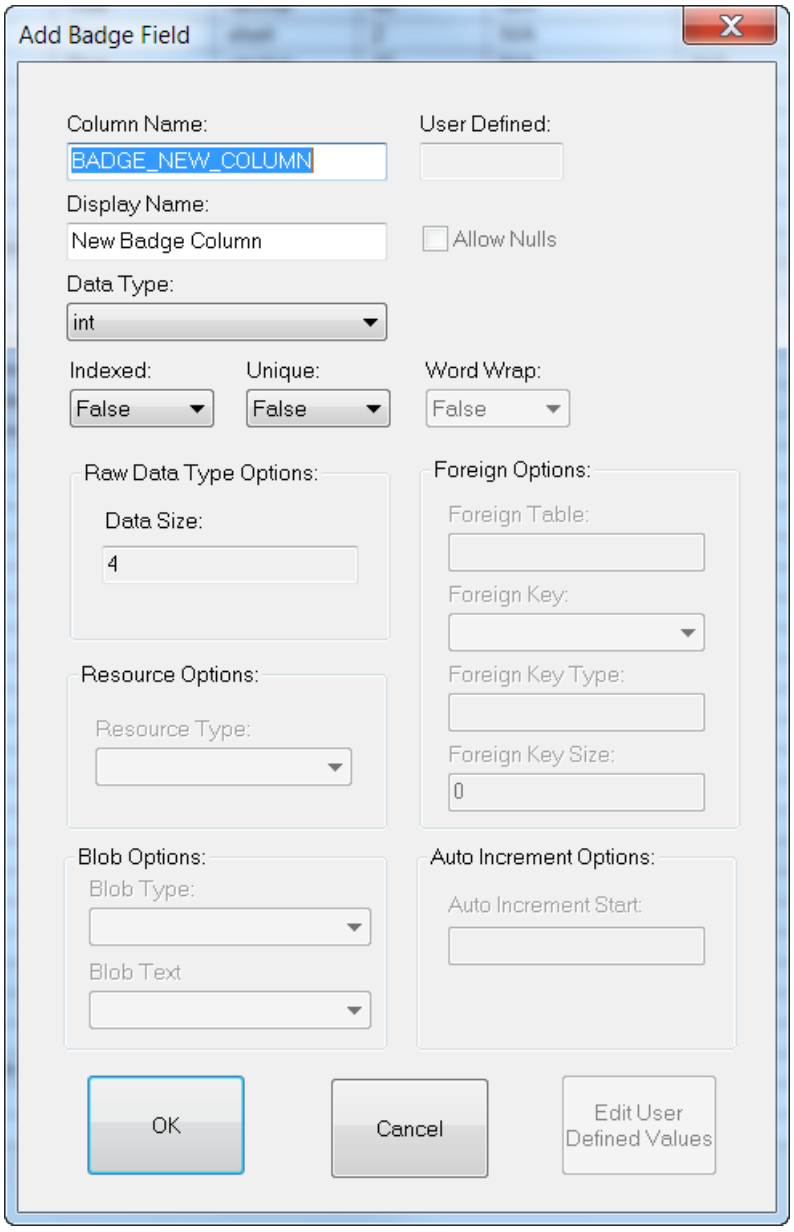
Use the Badge Utilities module to add a new badge field that will appear in the Description box in the left pane of the Badge Builder screen.

To add a new badge field:

1. Click the **Administration** icon in the left pane of the Pro-Watch screen.
2. Double-click the **Badge Utilities** folder in the middle pane to reveal its contents.
3. Click the **Badge Fields** to display all the available badge fields in the right pane.
4. Right-click the first column of a badge field that you want to add. A pop-up menu will display:



5. Select **Add Badge Field** to display the **Add Badge Field** dialog box:



6. Enter a **Column Name** without any spaces. Underscore is accepted. Note that preceding numbers are not permitted in a Badge Fields column name.
7. Enter a Display Name which will display on the badge screen.
8. The values of the **User Defined** field, True and False, is determined by the following:
    - If the variable is in the static BADGE data table, the value of the User Defined field is FALSE.

- If the variable is in the BADGE_V data table, the value of the User Defined field is TRUE.

  Select a **Data Type** from the drop-down list. Note that if you select "**user defined**" for data type, the **Edit User Defined Values** button at bottom right will be enabled. To add or edit any user defined variables click this button to display the **User Defined Data** dialog box and enter/change the appropriate values.

9. For the **Indexed** field, select a value (TRUE or FALSE) from the drop-down list.
   - Select TRUE for variables with wide-ranging unique values (e.g. Social Security Numbers, or First and Last Names) and on which you perform searches frequently. Variables that have an index value can be searched faster.
   - Select FALSE for variables with only a few values (e.g. only TRUE or FALSE) or those variables that you search only occasionally. Indexing facilitates searching but indexed tables take up more memory space.
10. For the **Word Wrap** field, select a value (TRUE or FALSE) from the drop-down list.
11. **Foreign Options** group of fields is not operational in Pro-Watch Release 4.3.5.

Note: **Data Size** is a read-only field (with one exception described below) filled in automatically depending on the **Data Type** you select.

Example: If the Data Type is "**int** (integer)" then the Data Size automatically displays "**4** (bytes)". If you select "**bool** (boolean)" for Data Type, then Data Size displays "**1** (byte)," etc.

If you select "**varchar** (variable character)" for Data Type, then the Data Size field is enabled for you to enter an appropriate byte size.

12. **Resource Type** drop-down list is enabled when you select **Resource** for **Data Type**. Select a resource type value from the list.

Note: **BLOB Options** fields are enabled when you select **BLOB Types** for **Resource Type**. Select a **BLOB Type** and **BLOB Text** from the respective drop-down lists.

BLOB Type and BLOB Text (i.e., BLOB description) must be entered earlier in the Database Configuration > BLOB Types module in order to appear in these drop-down lists.

13. **Auto Increment Start** field is enabled when you select "**auto increment**" for data type. Enter a numeric value to be used as a starting value for the auto increment field. Auto increment fields are always incremented by 1.

To edit a badge field:

1. Click the **Administration** icon in the left pane of the Pro-Watch screen.
2. Double-click the **Badge Utilities** folder in the middle pane to reveal its contents.
3. Click the **Badge Fields** to display in the right pane all the badge fields available
4. Right-click the first column of a badge field that you want to edit. A pop-up menu will display.
5. Select **Edit Badge Field** to display the Edit Badge Field dialog box.
6. Make the necessary changes and click **OK**.

To delete a badge field:

1. Click the **Administration** icon in the left pane of the Pro-Watch screen.
2. Double-click the **Badge Utilities** folder in the middle pane to reveal its contents.
3. Click the **Badge Fields** to display in the right pane all the badge fields available
4. Right-click the first column of a badge field that you want to delete. A pop-up menu will display.
5. Select **Delete Badge Field** to display the **Delete Badge Field** warning message: “This action will delete information for every badge! Are you absolutely sure you want to do this?”
6. Click **Yes**.

To view the properties of a badge field:

1. Click the **Administration** icon in the left pane of the Pro-Watch screen.
2. Double-click the **Badge Utilities** folder in the middle pane to reveal its contents.
3. Click the **Badge Fields** to display in the right pane all the badge fields available
4. Right-click the first column of a badge field when you want to view its properties. A pop-up menu will display.
5. Select **View Badge Field** to display the **View Badge Field** dialog box displaying the read-only properties of the badge field.
6. When you are done, click **OK** to close the dialog box.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Map Building

61

In this chapter...

Overview

Creating Maps

Map Builder Tool Bar

Map Building Functions

Adding, Editing, or Deleting Resources

Editing Resource Properties

Locating a Resource

Cleaning Up a Resource

Show Resource Text

Linking Maps to Alarms

Linking Multiple Maps

61.1 Overview

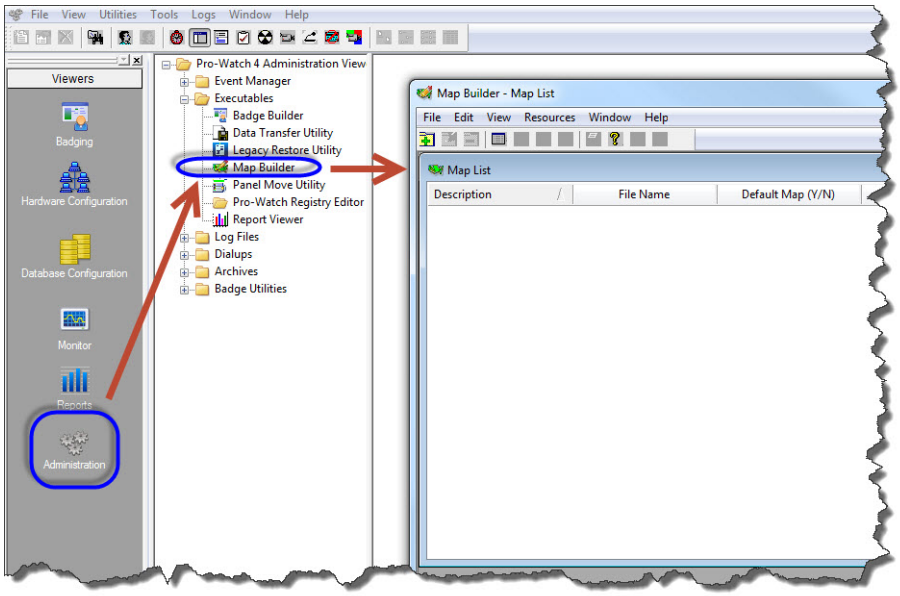
This chapter describes the Pro-Watch Map Builder utility. You can use this tool to add, edit, view, or remove maps from your Pro-Watch system. A map helps you to locate the position of the object with which it is associated.

Note: Maps can be created in the Database Configuration module as well. See Chapter 27, *Database Configuration (DBC)* for instructions and information about creating maps. A list of all existing maps, whether they are created in the Database Configuration module or through the Map Builder utility, will be displayed both in the Database Configuration and the Map Builder screens.

Tip: You can attach and detach logical devices to and from a map only in the Map Builder utility.

61.1.1 To Launch the Map Builder

1. In the main Pro-Watch window, double-click the **Administration** module icon in the left navigation panel to display the Administration options in the middle tree-view panel.
2. In the tree-view pane in the middle, click the **plus (+) sign** next to the **Executables** directory icon to display all the subdirectories underneath it.
3. Double-click the **Map Builder** icon to launch the Map Builder application in a separate window:



61.2 Creating Maps

A map, a site, or a floor-plan drawing can be created by any image editor (e.g., Adobe Illustrator, Adobe Photoshop) or CAD (Computer-Aided Design) program that creates and saves images in one of the following file formats acceptable by the Pro-Watch Map Builder:

- .DWG
- .DXF
- .PCX
- .BMP

61.3 Map Builder Tool Bar

You can use the following buttons on the tool bar to perform various map functions:



You can add, edit and delete maps in Pro-Watch's map building module:

Button	Description
	Adds a new map.
	Edit a selected map.
	Deletes a selected map.
	Reveals the list of existing maps, if it is not displayed by default.
	Views a selected map.
	Zooms the selected area of the map.
	Restores the previous view setting. This function is available only with Auto-CAD maps.
	Prints a selected map.
	Launches "About Pro-Watch" help.

Button	Description
	Zooms in on a selected map.
	Zooms out on a selected map.

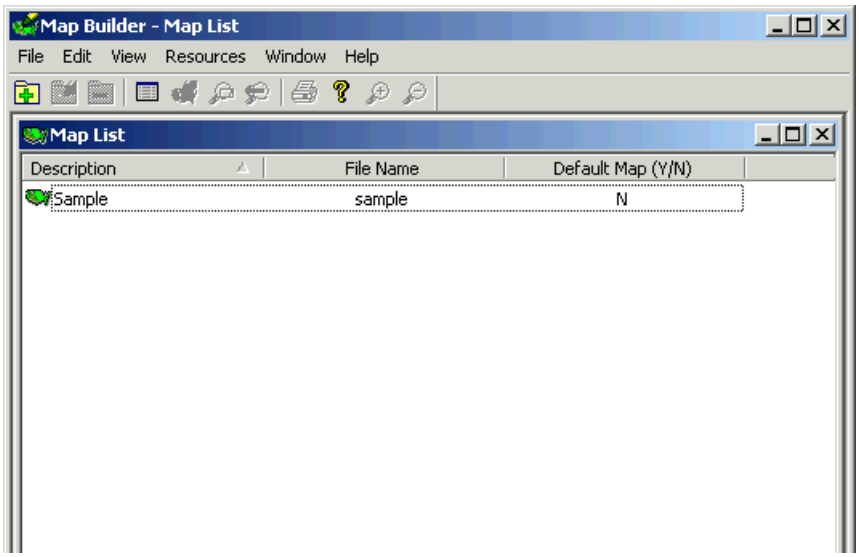
61.4 Map Building Functions

61.4.1 Adding a Map

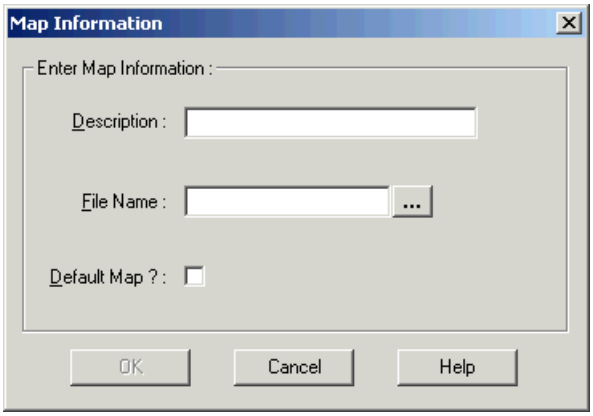
Note: Maps must not exceed 300-350KB. Maps larger than this cannot be saved. If you try to save the larger map, the map will not appear when you open the display.

Note: The map images must be in one of the following file formats:.**DWG,.DXF,.DWFX,.PCX,.XPS.,** or.**BMP.**

1. Launch the **Map Builder**:

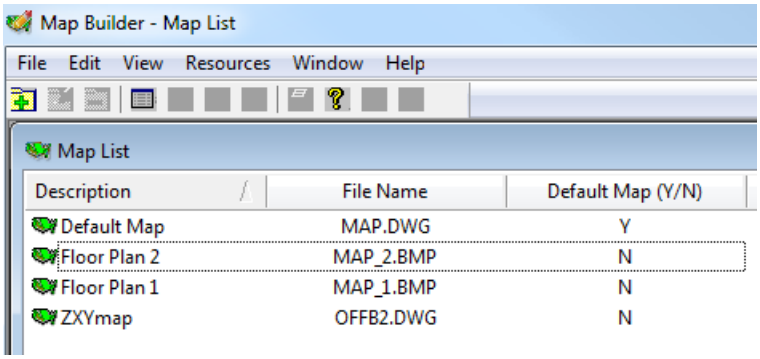


2. Select **Edit > Add Map** from the menu to display the **Map Information** dialog box:



Note: Enter a **Description** for the map you are adding. You cannot use a description if it is the name of a map image saved into the **Database Configuration > Map Files** database.

3. Enter a **File Name** or click the ellipsis button (...) and browse for the appropriate file.
4. Select the **Default Map** check-box if you want to designate it as a default map.



5. Click **OK** to close the dialog box.
6. Click **Help** for more information.

Note: The Alarm Monitor can display maps. To configure this feature, place the map file in the /Maps folder of the Pro-Watch install directory on each workstation on which you want the map to appear.

61.4.2 Editing a Map

The Edit menu on the Map Builder toolbar provides the following options:

- Add Map
- Edit Map
- Delete Map
- Selected Map
- Layers
- Blocks

1. In the Map Builder screen, select a map from the list displayed in the grid.
2. Select **Edit > Edit Map** from the menu to display the Map Information dialog box.
3. Edit the **Description** of the map, if appropriate.
4. Edit the **File Name** or click the ellipsis button (...) and browse for the appropriate file.
5. Select or unselect the **Default Map?** check-box as appropriate.
6. Click **OK** to close the dialog box.

61.4.3 Deleting a Map

1. In the Map Builder screen, select a map from the list displayed in the grid.
2. Select **Edit > Delete Map** from the menu to display the "Delete this map?" warning message.
3. Click **Yes**.

61.4.4 Displaying the Selected Map

1. In the Map Builder screen, select a map from the list displayed in the grid.
2. Select **Edit > Selected** from the menu to display the selected map.

61.4.5 Displaying the Layers of the Map

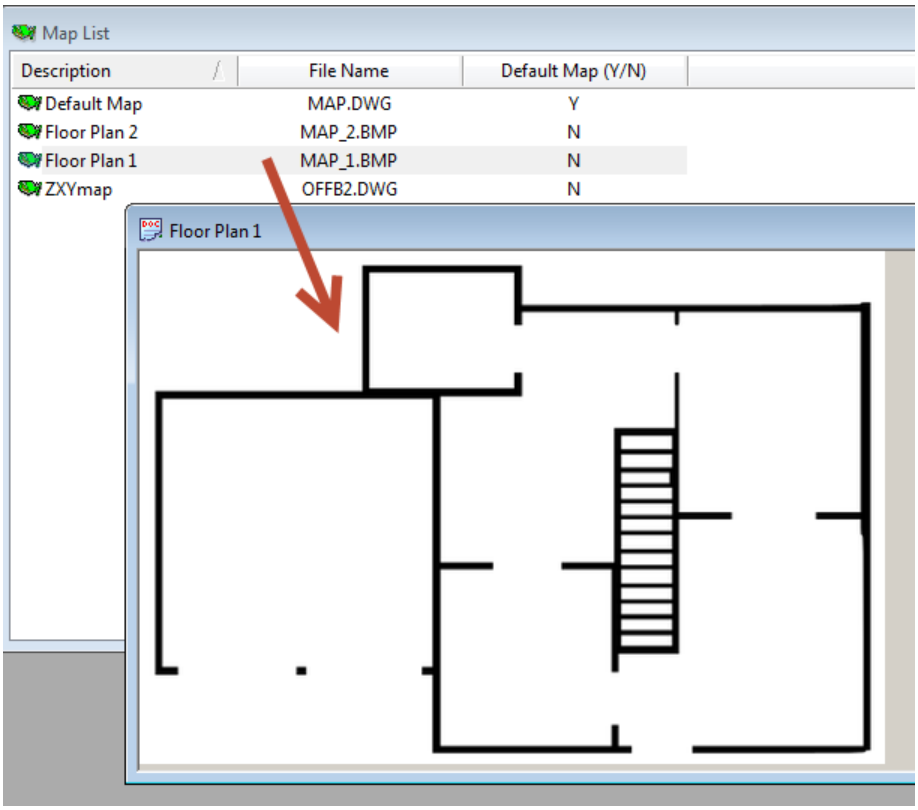
This feature is not yet implemented in Pro-Watch.

61.4.6 Displaying the Blocks in the Map

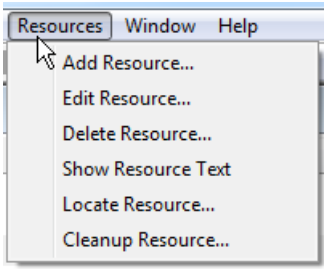
This feature is not yet implemented in Pro-Watch.

61.5 Adding, Editing, or Deleting Resources

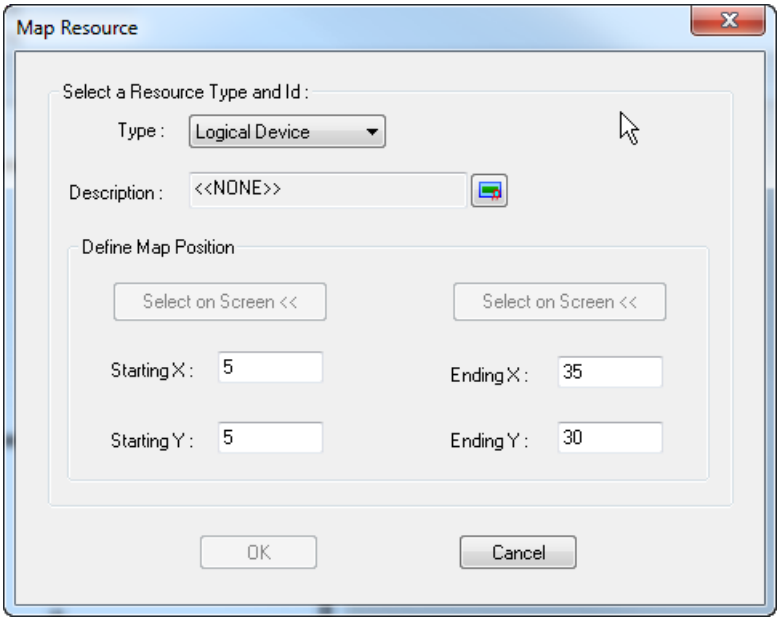
1. To add resources to a map, double click its description the Map List screen to display it in its own new screen:



2. Click the Resources menu to select one of the options available:



3. Select the **Add Resource** option to display the **Map Resource** dialog box:

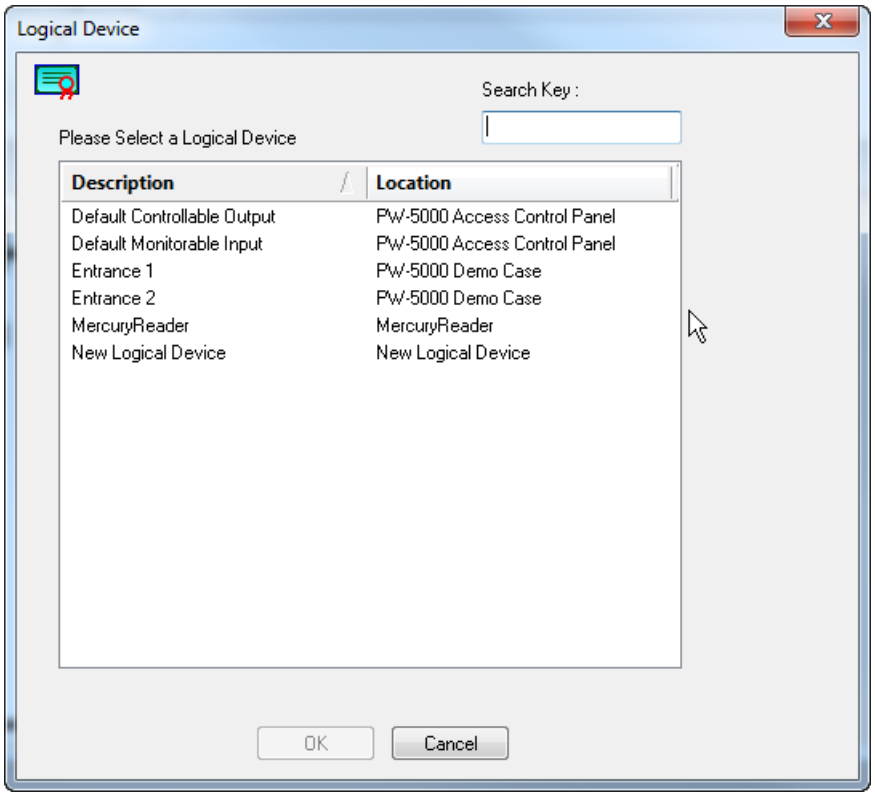


4. Follow one of the procedures described below to add, edit or delete any particular resource.

61.5.1 Adding, Editing or Deleting a Logical Device

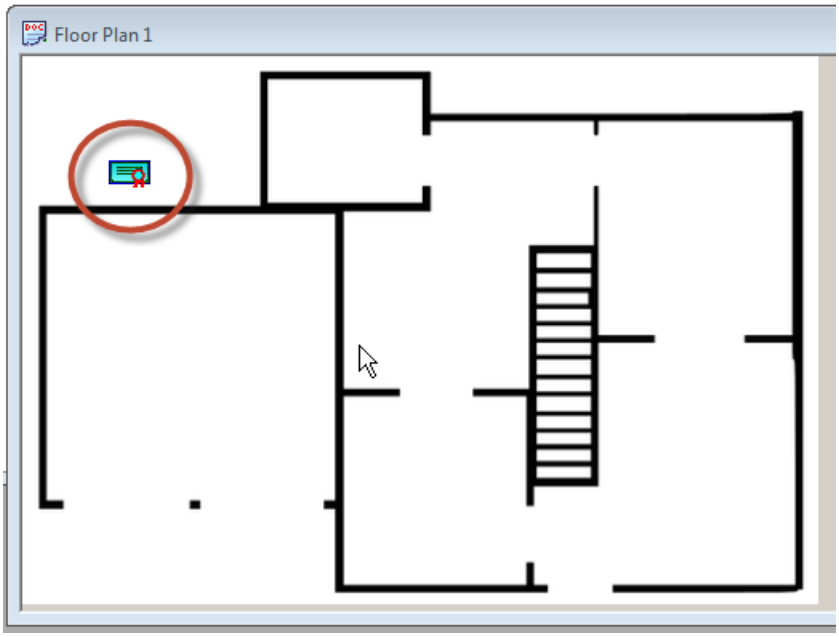
1. In the M**ap Resource** dialog box, select **Logical Device** from the **Type** drop-down list.

2. Click the **Description** button and then select **Define** from the pop-up menu to display the **Logical Device** selection screen:



3. If there is a long list of devices, search for them by entering a search string into the **Search Key** field.

Note: Select a logical device from the list and click **OK** to insert its icon into the map. If you select more than one device by pressing the **Ctrl** key, only the first-selected device will be inserted into the map.



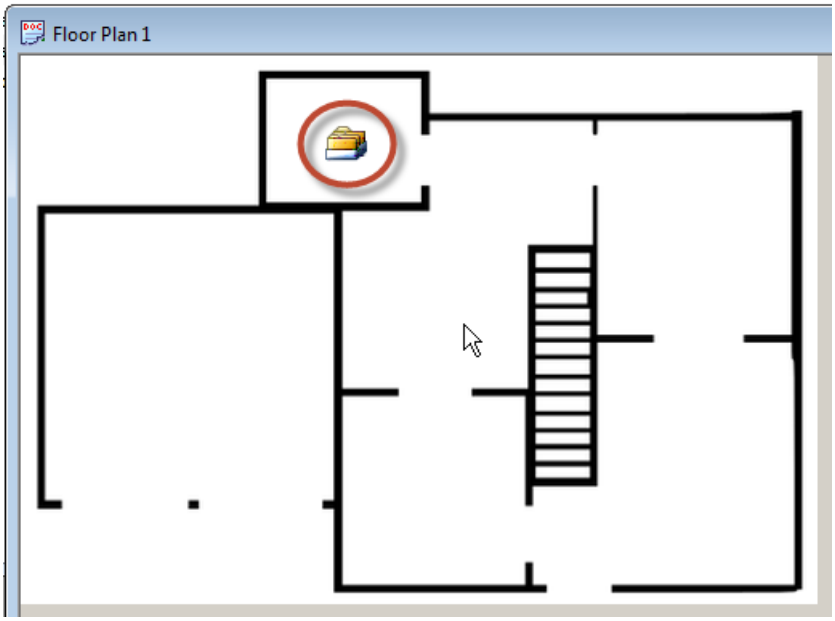
4. Click and drag the icon to any new position you like.
5. To edit the attributes of the logical device icon, right-click on it and select **Properties** from the pop-up menu or select **Resources > Edit Resource** from the main menu to display the **Map Resource** screen. Make the necessary changes and click **OK**.
6. Define the map position of the icon by entering new X and Y coordinates.
7. To delete a logical device, right click on its icon and select **Delete**, or select **Resources > Delete Resource** from the main menu.

61.5.2 Adding, Editing or Deleting Groups

Note: Groups and maps cannot be represented on a map without having a minimum of once device in those.

1. In the **Map Resource** dialog box, select **Groups** from the **Type** drop-down list.
2. Click the **Description** button and then select **Define** from the pop-up menu to display the **Groups** selection screen.

3. Select a group and click **OK**. If there are no groups or you'd like to add a new group, click **Add**:



4. To edit the attributes of the group icon, right-click on it and select **Properties** from the pop-up menu or select **Resources > Edit Resource** from the main menu to display the **Map Resource** screen. Make the necessary changes and click **OK**.
5. To delete a group, right click on its icon and select **Delete**, or select **Resources > Delete Resource** from the main menu.

61.5.3 Adding, Editing or Deleting Map Files

Note: Groups and maps cannot be represented on a map without having a minimum of once device in those.

1. In the **Map Resource** dialog box, select **Map Files** from the **Type** drop-down list.
2. Click the **Description** button and then select **Define** from the pop-up menu to display the **Map Dialog** selection screen.
3. Select a map and click **OK**. If there are no maps or you'd like to add a new map, click **Add.**
4. To edit the attributes of the map file, right-click on it and select **Properties** from the pop-up menu or select **Resources > Edit Resource** from the main menu to display the **Map Resource** screen. Make the necessary changes and click **OK**.

5. To delete a map file, right click on its icon and select **Delete**, or select **Resources > Delete Resource** from the main menu.

61.5.4 Adding, Editing or Deleting a CCTV Camera View

1. In the **Map Resource** dialog box, select **CCTV Camera View** from the **Type** drop-down list.
2. Click the **Description** button and then select **Define** from the pop-up menu to display the **CCTV Camera Views** selection screen.
3. Select a CCTV camera view and click **OK**. If there are no views or you'd like to add a new view, click **Add.**
4. To edit the attributes of the CCTV camera view icon, right-click on it and select **Properties** from the pop-up menu or select **Resources > Edit Resource** from the main menu to display the **Map Resource** screen. Make the necessary changes and click **OK**.
5. To delete a CCTV camera view, right click on its icon and select **Delete**, or select **Resources > Delete Resource** from the main menu.

61.5.5 Adding, Editing or Deleting a Camera

Note: You need to have access to a MAXPRO server for this option.

1. In the **Map Resource** dialog box, select **Camera** from the **Type** drop-down list.
2. Click the **Description** button and then select **Define** from the pop-up menu to display the **Cameras** selection screen.
3. Select a camera and click **OK**. If there are no cameras or you'd like to add a new camera, click **Add.**
4. Back in the Map Resource screen, select an appropriate **Angle** for the camera from the respective drop-down list.
5. To edit the attributes of the camera icon, right-click on it and select **Properties** from the pop-up menu or select **Resources > Edit Resource** from the main menu to display the **Map Resource** screen. Make the necessary changes and click **OK**.
6. To delete a camera right click on its icon and select **Delete**, or select **Resources > Delete Resource** from the main menu.

61.5.6 Adding, Editing or Deleting a Monitor

1. In the **Map Resource** dialog box, select **Monitor** from the **Type** drop-down list.
2. Click the **Description** button and then select **Define** from the pop-up menu to display the **Monitors** selection screen.
3. Select a monitor and click **OK**.

4. To edit the attributes of the monitor icon, right-click on it and select **Properties** from the pop-up menu or select **Resources > Edit Resource** from the main menu to display the **Map Resource** screen. Make the necessary changes and click **OK**.
5. To delete a monitor, right click on its icon and select **Delete**, or select **Resources > Delete Resource** from the main menu.

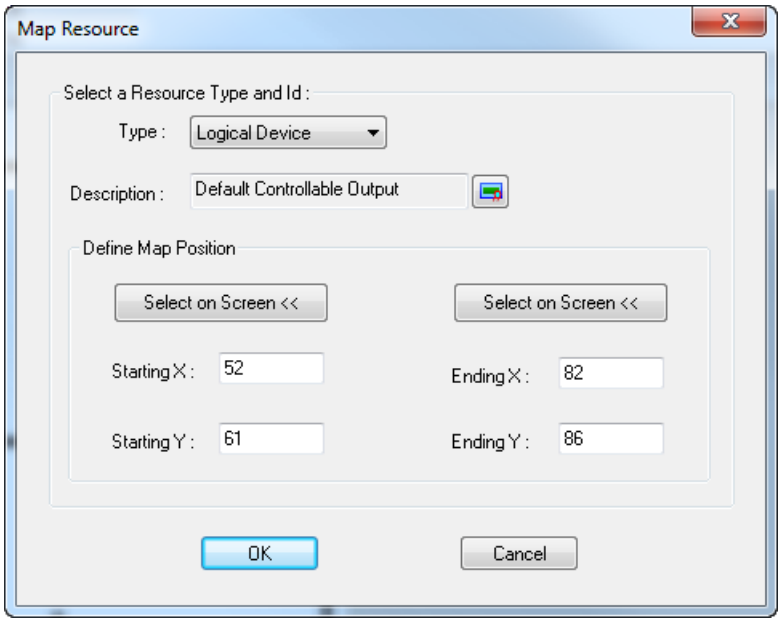
61.5.7 Adding, Editing or Deleting an Intercom

1. In the **Map Resource** dialog box, select **Intercom** from the **Type** drop-down list.
2. Click the **Description** button and then select **Define** from the pop-up menu to display the **Intercoms** selection screen.
3. Select an intercom and click **OK**.
4. To edit the attributes of the icon, right-click on it and select **Properties** from the pop-up menu or select **Resources > Edit Resource** from the main menu to display the **Map Resource** screen. Make the necessary changes and click **OK**.
5. To delete an intercom, right click on its icon and select **Delete**, or select **Resources > Delete Resource** from the main menu.

61.6 Editing Resource Properties

Caution: When editing the properties of a resources like a Logical Device you need to be careful in changing the X and Y coordinate values. A good practice is to record the original coordinates before you start to change them.

For example, right-click on a logical device icon and from the pop-up menu select **Properties** to display the **Map Resource** screen:



To move the icon on the X axis add the same number of pixels to both "Starting X" and "Ending X" fields. Otherwise, you will distort the look of the icon.

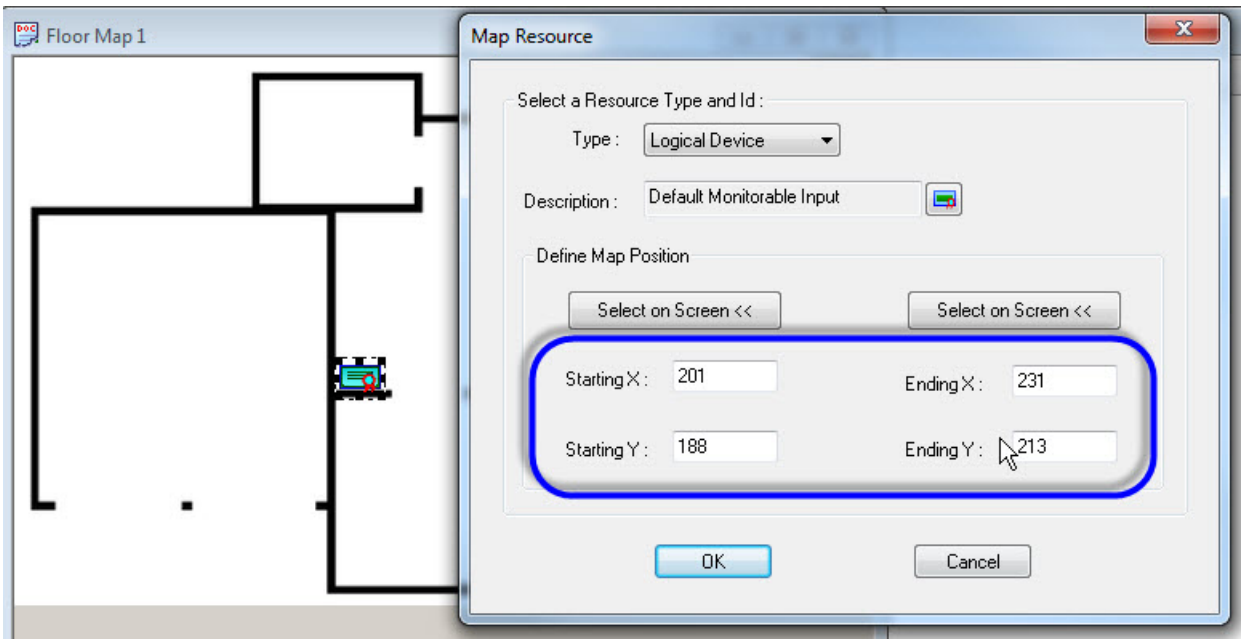
To move the icon on the Y axis add the same number of pixels to both "Starting Y" and "Ending Y" fields. Otherwise, you will distort the look of the icon.

Caution: **You need to add exactly the same number of pixels to the X and Y coordinate fields** in order not to distort the icon image while moving it. Thus it's good practice to **write down the original beginning coordinates** somewhere before you change them. The only way to reset the icon is by

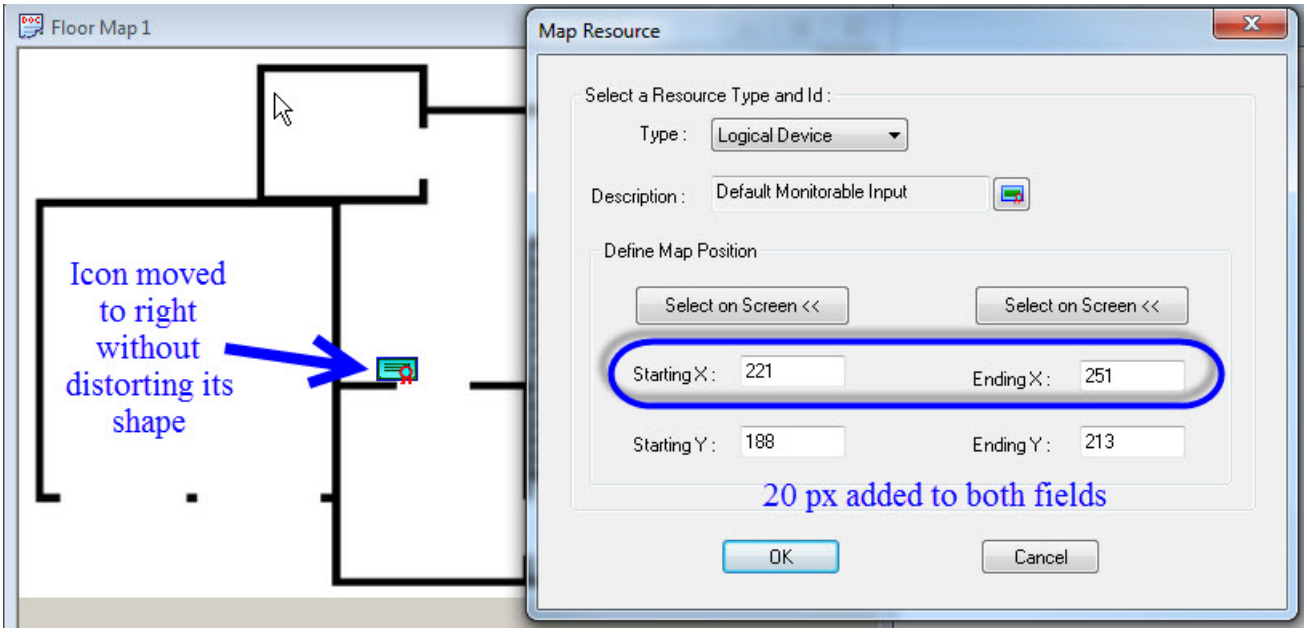
entering its original coordinates manually into the X and Y coordinate fields.

61.6.1 An Example

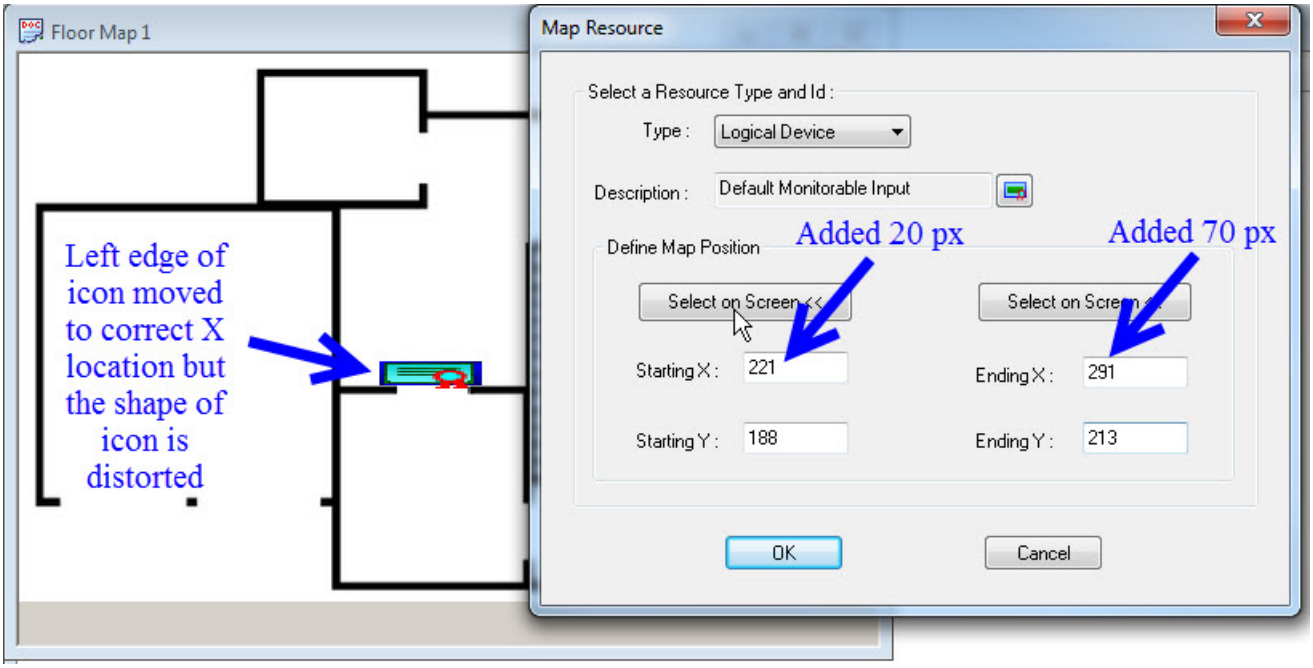
Here is an example of the original coordinates of a resource (logical device, in this case):



We added 20 pixels to both X fields to move the icon 20 pixels to the right:



However, if we add unequal number of pixels to these fields, the icon will be distorted even when its left edge is still moved to the correct location:



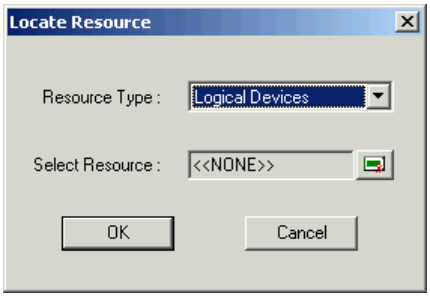
61.6.1.1 "Select on Screen" Buttons

You can also try to make a manual location selection by clicking the "**Select on Screen**" buttons but sometimes the results could be hard to control. Be cautious when you are using these buttons.

61.7 Locating a Resource

Follow these steps to add a resource and establish its association with a map:

1. Select **Resources > Locate Resource** from the Map Builder menu. The Locate Resources dialog box will display:



2. Select a **Resource Type** from the drop-down list.
3. Select a resource by clicking the button next to the **Select Resource** field.
4. Select **Define** from the pop-up menu to display the selection screen for the resource selected.
5. Select a resource and click **OK** to return to the **Locate Resource** dialog box.
6. Click **OK** once again to return to the **Map Builder** screen.

61.8 Cleaning Up a Resource

Follow these steps to delete a resource and break its association with a map, or "clean up" the resource:

1. Select **Resources > Cleanup Resource** from the Map Builder menu. The **Cleanup Resources** dialog box will display.
2. Select a **Resource Type** from the drop-down list.
3. Select a resource by clicking the button next to the **Select Resource** field.
4. Select **Define** from the pop-up menu to display the selection screen for the resource selected.
5. Select a resource and click **OK** to return to the **Cleanup Resources** dialog box.
6. Click **OK** once again to return to the **Map Builder** screen.

61.9 Show Resource Text

When this option is selected from the **Resources** menu, the **Map Builder** displays the name of the individual resources (e.g., readers) when the user zooms into the map.

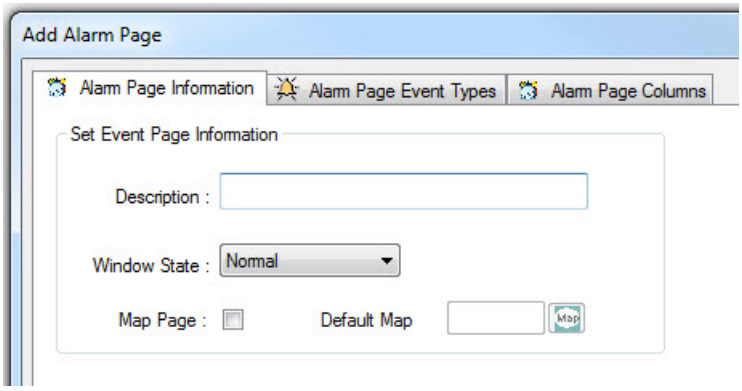
61.10 Linking Maps to Alarms

61.10.1 Add a Map with Resource(s)

1. Select **Database Configuration > Map Files** and add one or more map images.
2. Add resources as explained in section "Adding, Editing, or Deleting Resources".

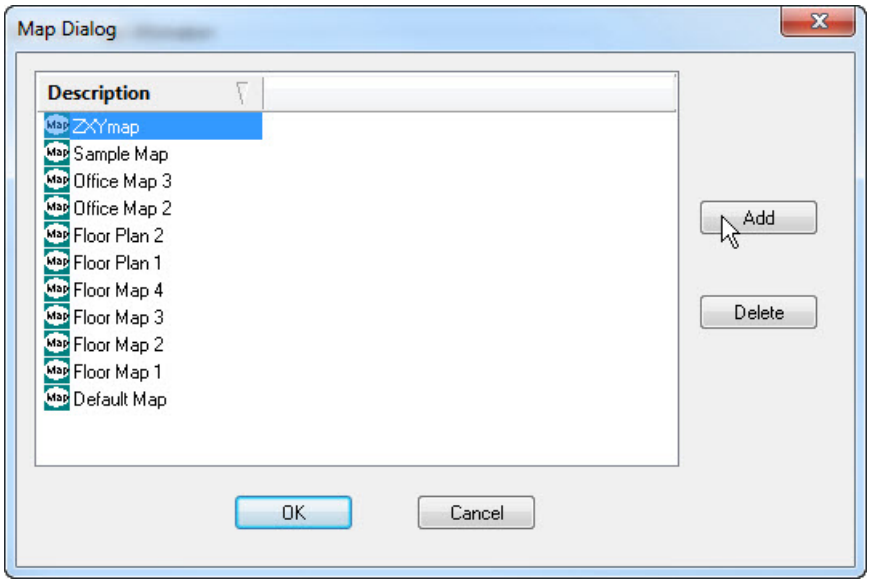
61.10.2 Add an Alarm Map Page

3. Select **Database Configuration > Alarm Pages.**
4. Right click and select **New Alarm Page** to display the **Add Alarm Page** screen:



5. Enter a **Description**.
6. **Select the Map Page** check-box since you are creating a special kind of alarm page: a map page.

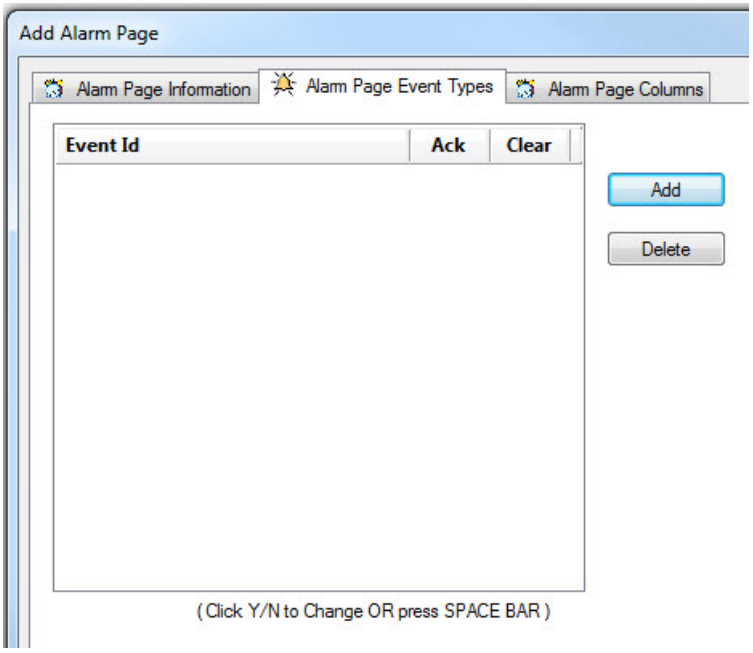
7. Click the **MAP** button next to the **Default Map** field and select **Define** from the pop-up menu to display the **Map Dialog** screen:



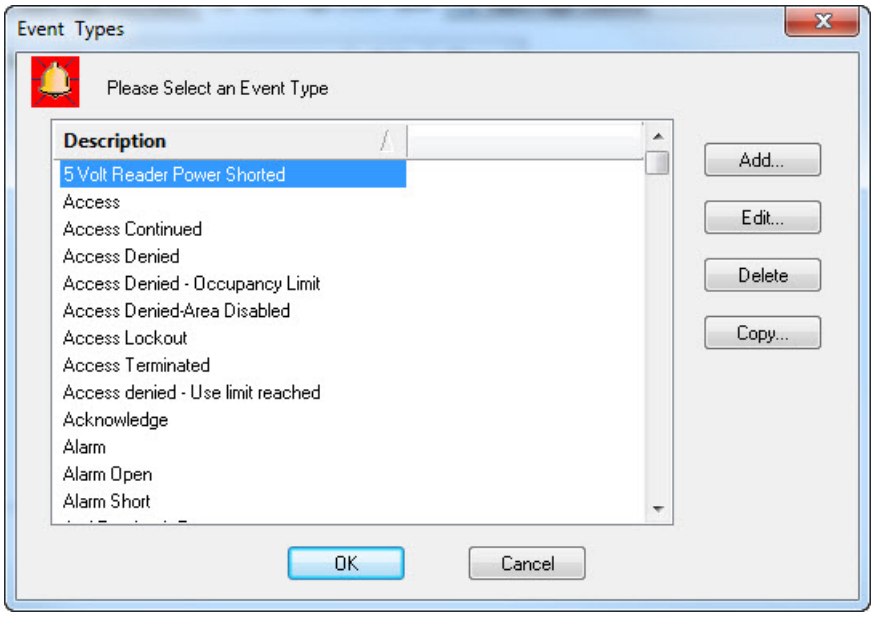
8. Select a map and click **OK** to display the **Add Alarm Page** screen. If you'd like to add a new map click **Add** to display the **Add Maps** screen and follow the prompts.

61.10.3 Add Alarm Event Types

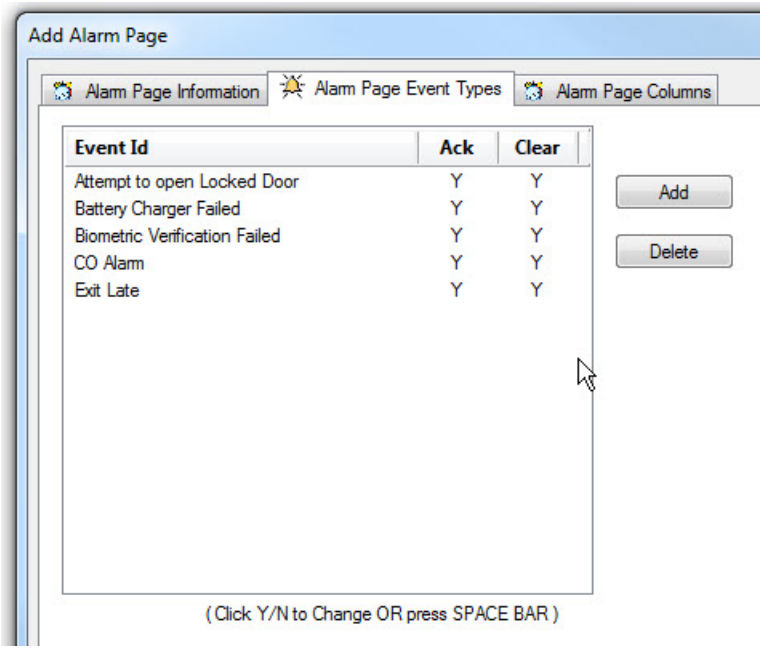
9. Back in the **Add Alarm Page** screen, select the **Alarm Page Event Types**:



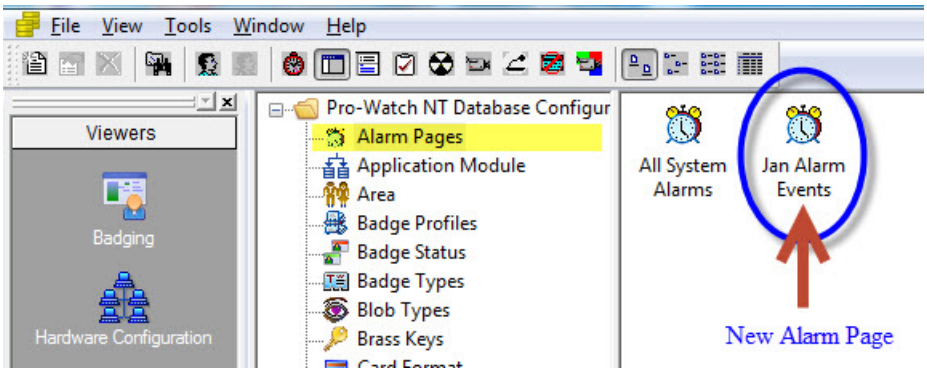
10. Click **Add** to display the **Event Types** screen:



11. Select all the alarm events that you'd like to associate with the selected map by pressing the **Ctrl** key. If you'd like to add a new event type click **Add** to display the **Add Even Types** screen and follow the prompts.
12. Click **OK** to return to the **Alarm Page Event Types** tab, now displaying all the selected alarm events:

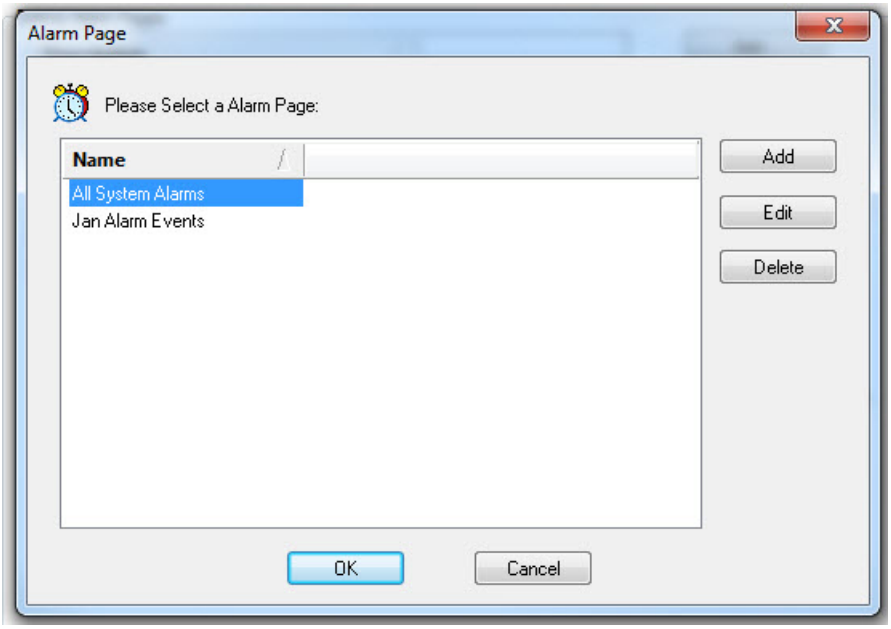


13. Click **OK** to close the **Add Alarm Page** screen and return to the **Database Configuration** screen where the new alarm page displayed:



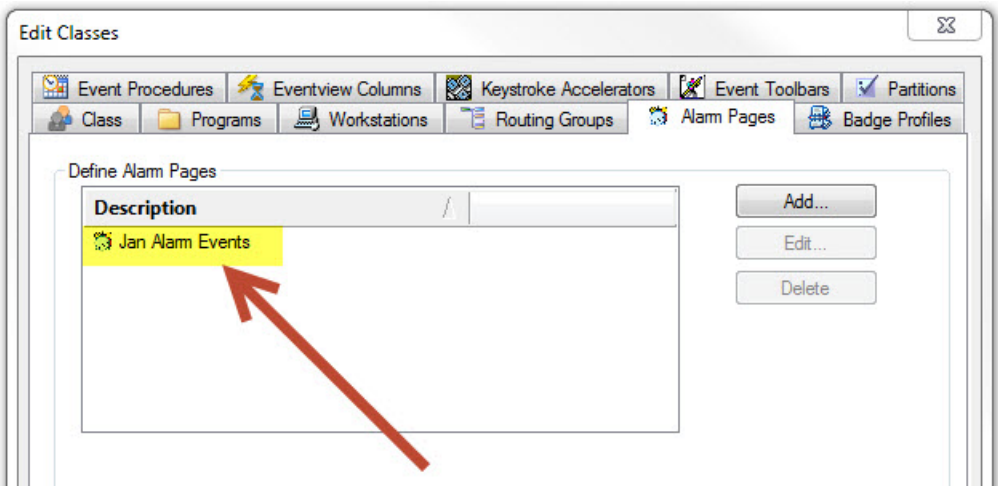
61.10.4 Add User Class or Individual User(s)

14. Select **Classes** (or **Users**) from the **Database Configuration** navigation list.
15. Select a class. Right click and select **Properties** from the pop-up menu to display the editing screen of that class (or user).
16. Click and select the **Alarm Pages** tab.
17. Click **Add** to display the **Alarm Page** screen:



18. Select the alarm map-page that you've created earlier. See "Add an Alarm Map Page".

19. Click **OK** to close that screen and have the map page listed in the **Alarm Pages tab** list:



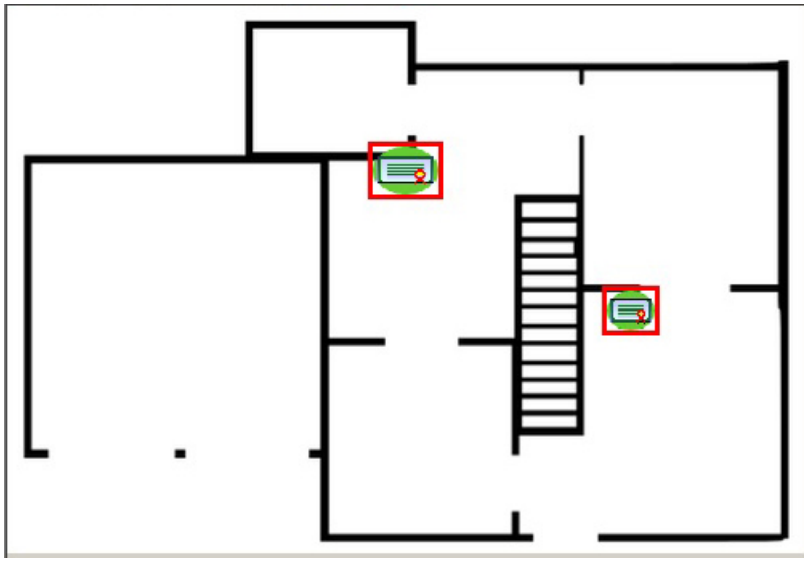
20. Click **OK** to close the editing screen of the class or user you have chosen.

61.10.5 Display the Alarm Monitor

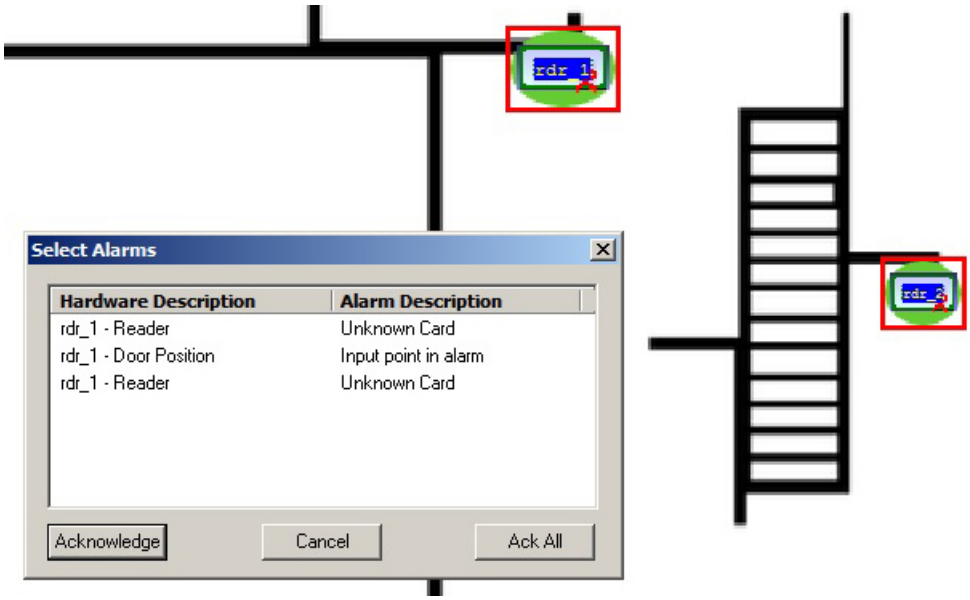
Note: **Select Monitor > Alarm Monitor** from the Pro-Watch navigation pane to display the alarm monitor. Your map page will be displayed along side the regular alarm events page. This assumes that you are either an individual user or belong to the class of users to whom the alarm map page is assigned. See "Add User Class or Individual User(s)".

61.10.5.1 Alarm Events on the Map

This is how the alarm events will look like on the map -- RED rectangles around resources (e.g., readers):



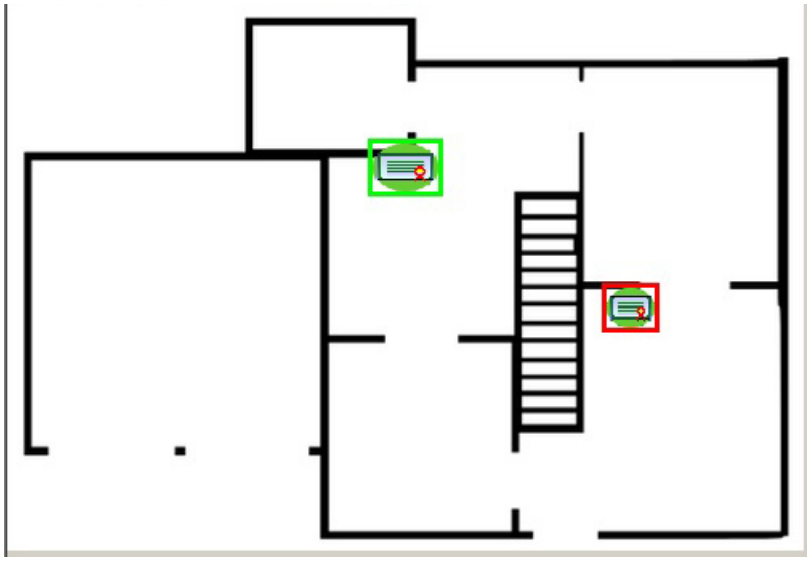
To see all the alarms associated with a particular resource, right-click on it and from the pop-up menu select **Select Alarms**:



In this particular example, the first reader (rdr_1) has three different alarm events associated with it. You can select and click **Acknowledge** button to acknowledge any single alarm or click **Ack All** to acknowledge all of them.

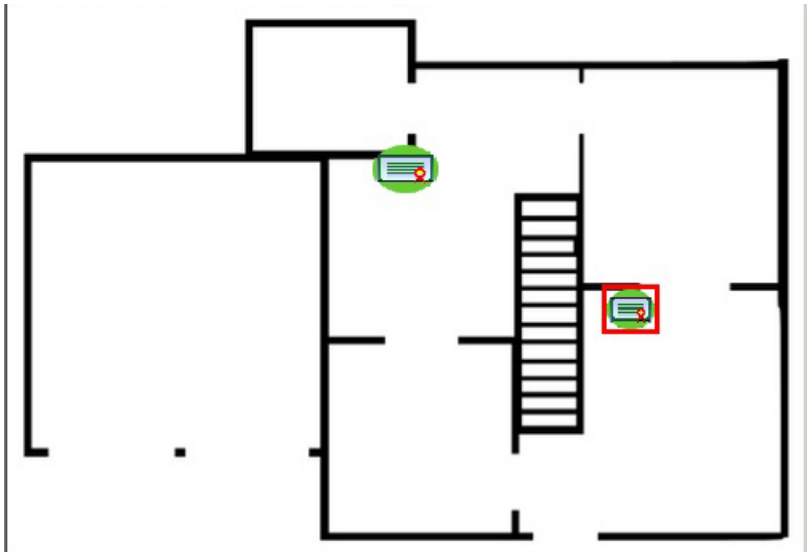
61.10.5.2 Acknowledge Alarm Events

To acknowledge an alarm event, right-click on the resource and from the pop-up menu select **Ack Alarm**. The acknowledged alarm will be represented by a GREEN rectangle:



61.10.5.3 Clear the Alarm Events

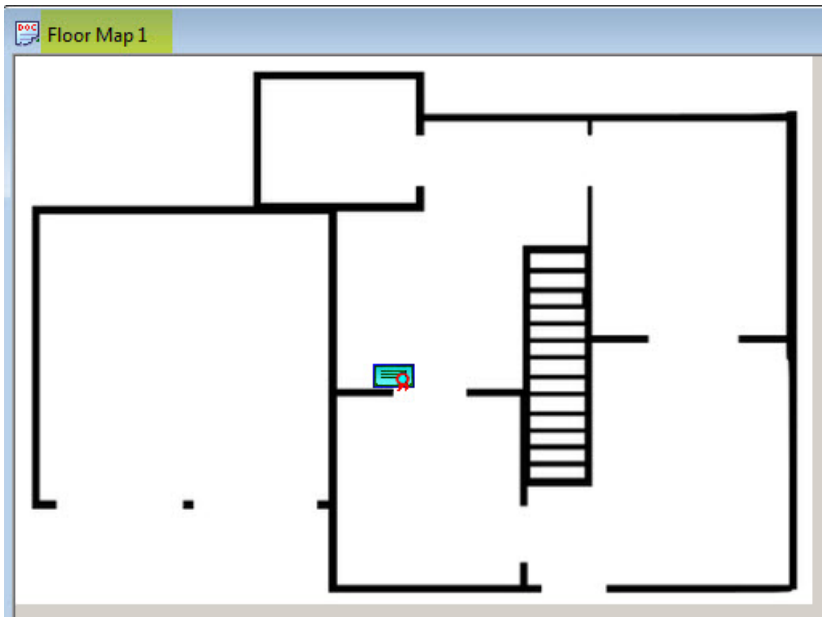
To clear an alarm event, right-click on the resource and from the pop-up menu select **Clear Alarm**. The cleared alarm will be represented by a GREEN CIRCLE:



61.11 Linking Multiple Maps

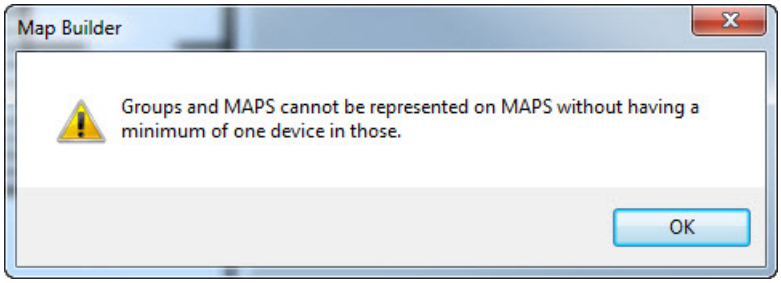
Map Builder offers a map linking feature that is sometimes also referred to as creating “Parent-and-Child Maps.”

1. Open a map with at least one resource attached to it:

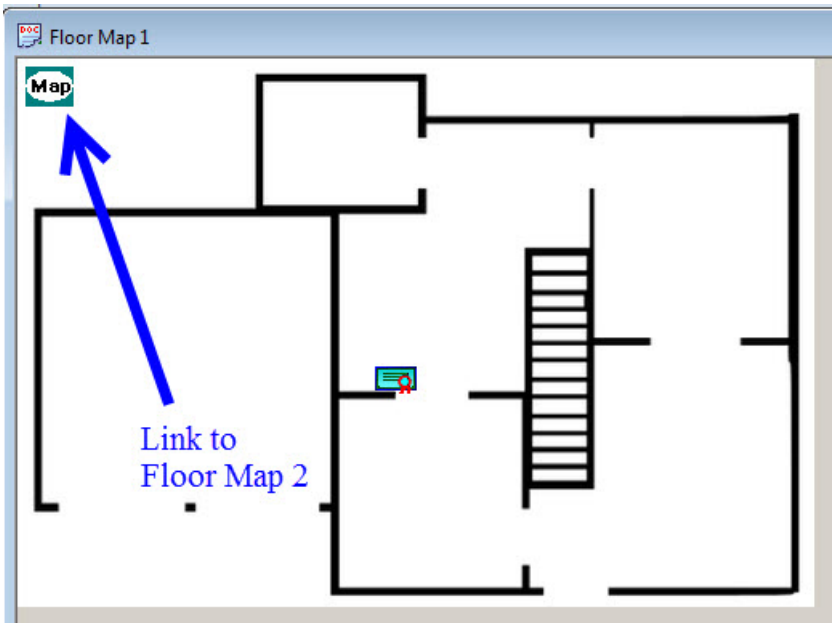


2. Select **Resources > Add Resource** to display the **Map Resource** screen.
3. Select **Map Files** from the **Type** drop-down list.
4. Click the **Map** button next to the **Description** field to display the pop-up menu. Select **Define** to display the **Map Dialog** screen.
5. Select a map from the list and click **OK** to return to the **Map Resource** screen. You can edit the default coordinates of the map link by paying attention to the cautionary remarks in section "Editing Resource Properties".

Note: If the map you are trying to add does not have at least one resource attached to it, the system will display the following warning message:



6. The link to the new map, also known as a “child” map, will display on your map:



Now whenever in Floor Map 1 you click this link, the system will automatically display the second map as well, complete with all the related alarm events.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Biometric Reader Configuration

62

In this chapter...

Overview
Setting Up the Hardware to Run with Pro-Watch
Configuring Pro-Watch to Support the Reader

62.1 Overview

The Pro-Watch biometric hand geometry reader controls access by reading the dimensions of an individual's hand as well as by keypad entry.

Pro-Watch supports three hand geometry reader configurations:

- Standalone reader – operates as the only reader device at the access point. The badge holder must initiate access by entering a PIN code on the reader's keypad as well as by having his hand read. The reader connects to a PW-3000 configured as an RSI board in a PW-5000 panel, as shown in the following figure.

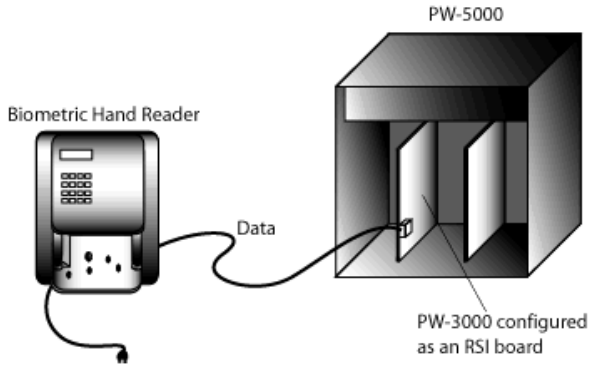
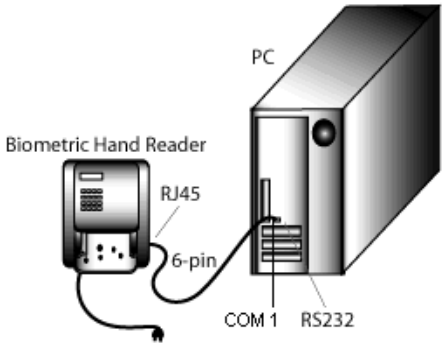


Figure 62-1 Biometric Hand Reader, Standalone Configuration

- Complementary reader – operates as a second reader for additional security at an access point equipped with both the hand geometry reader and a standard card reader. As it does in the standalone configuration, the biometric hand reader connects to a PW-3000 configured as an RSI board in a PW-5000 panel.

- Enrollment reader – operates as a reader at which badge holders enroll their hands in the Pro-Watch database. The reader connects directly to a PC running Pro-Watch, as shown in the following figure.

Figure 62-2 Biometric Hand Reader, Enrollment Configuration



This chapter explains the reader's physical setup and the configuration of the reader in Pro-Watch.

Note: To set up the biometric hand reader to operate with Pro-Watch, see the *Biometric Hand Reader Pro-Watch Setup Guide*.

62.2 Setting Up the Hardware to Run with Pro-Watch

62.2.1 Wiring the PW-3000 RSI Board to the PW-5000 IC

The PW-3000 RSI board and the PW-5000 IC must be wired together for data and power transmissions and grounding:

Table 62-1 RSI Board-to-PW-5000 IC Wiring

Wire	Device	Port
Data (white)	RSI board	Port 2, TR+
	PW-5000 IC	Port 6, TR+
Data (green)	RSI board	Port 2, TR-
	PW-5000 IC	Port 6, TR-
Power (red and black)	RSI board	Power port beneath Port 3
Common	RSI board	Port 1
	PW-5000 IC	Port 6, Com-RTS

62.2.2 Wiring the Readers

The following figure illustrates the power and data wire connections for a standalone reader configuration. The reader connects to a PW-3000 board that is configured to be an RSI board in a PW-5000 panel.

Note: A biometric hand reader in a complementary reader configuration is wired the same way as it is in the standalone configuration.

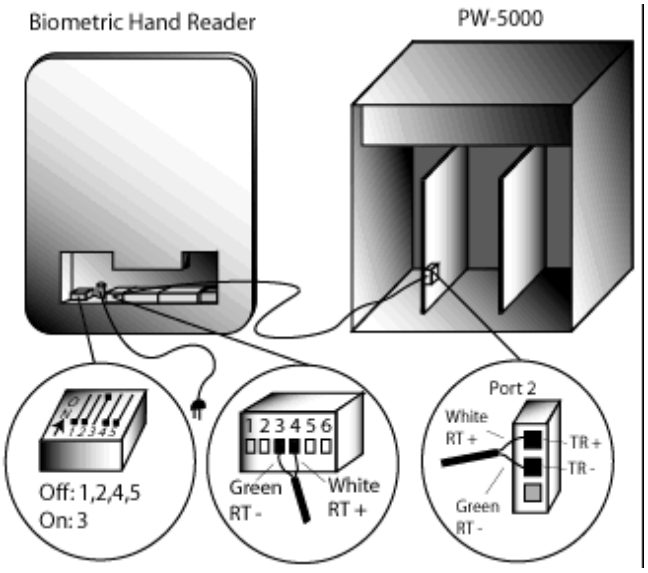


Figure 62-3 Wiring the Biometric Hand Reader, Standalone Configuration

Table 62-2 repeats the port and pin numbers for each connection in the Standalone configuration.

Table 62-2 Standalone Reader Wiring

Device	Power	Data
Reader	AC barrel connector	TR+ (white wire) connects to RT+ at PJ1, Pin 4 TR- (green wire) connects to RT- at PJ1, Pin 3
PW-3000 RSI Board	N/A	Port 2, TR+ (white wire), TR- (green wire)

The following figure shows the power and PC connections for an enrollment reader configuration. The reader connects to a PC that is running Pro-Watch, and it is used to enroll badge holders' hands in the Pro-Watch database.

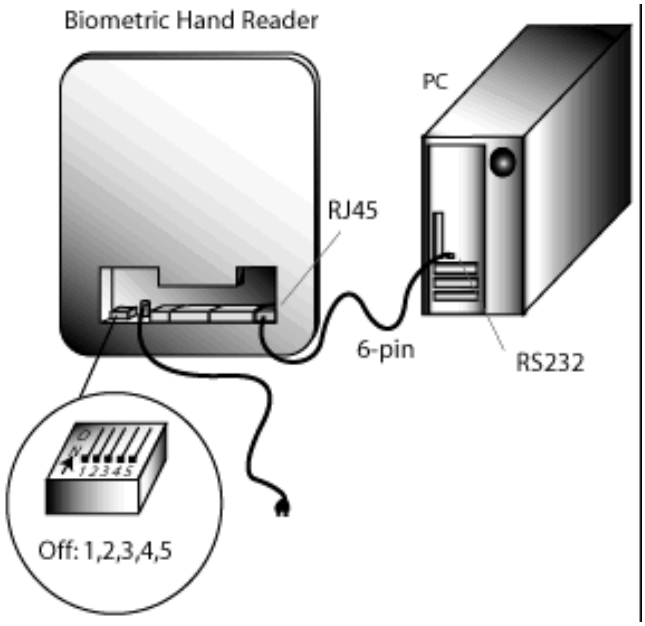


Figure 62-4 Biometric Hand Reader, Enrollment Configuration

Table 62-3 repeats the port and pin numbers for each connection in the Enrollment configuration.

Table 62-3 Enrollment Reader Wiring

Device	Power	Communications
Reader	AC barrel connector	RJ45 adapter
PC	N/A	RS-232 port

62.2.3 Setting the DIP Switches

62.2.3.1 Standalone Reader

For the standalone reader configuration, Pro-Watch requires DIP switch 3 to be set to “ON;” switches 1, 2, 4, and 5 are set to “OFF” (Figure 62-3).

62.2.3.2 Enrollment Reader

For the enrollment reader configuration, Pro-Watch requires all DIP switches on the reader to be set to “OFF” (Figure 62-4).

62.2.3.3 PW-3000 RSI Board

Use the following table to set the DIP switches on the RSI board:

S8	S7	S6	S5	S4	S3	S2	S1	Selection
				OFF	OFF	OFF	OFF	Address 32 (OFF = 0)
				OFF	OFF	OFF	ON	Address 1[1] (OFF = 0)
				OFF	OFF	ON	OFF	Address 2 (OFF = 0)
				OFF	OFF	ON	ON	Address 3 (OFF = 0)
				OFF	ON	OFF	OFF	Address 4 (OFF = 0)
				OFF	ON	OFF	ON	Address 5 (OFF = 0)
				OFF	ON	ON	OFF	Address 6 (OFF = 0)
				OFF	ON	ON	ON	Address 7 (OFF = 0)
			OFF					No Hardware Handshake[1]
			ON					TX Enabled by CTS[2]
	OFF	OFF						Reserved
	OFF	ON						9,600 BPS
	ON	OFF						19,200 BPS
	ON	ON						38,400 BPS[1]
OFF								19,200 BPS
ON								9,600 BPS

1Default
2Required for PW-5KxEN

62.2.4 Setting the Reader Menus

1. Press **CLEAR** and **ENTER**. The Enter Password prompt appears.
2. Press 2 to begin the Setup menu. The “Set Language” prompt appears.
3. Click *** (YES)** to display the prompt “Set Date Format.”
4. Click **# (YES)** to display the first date format. If the displayed format is not the one you want to use, click *** (NO)** to display the next format, and so on, until the format you want appears.
5. Click **# (YES)** to accept the desired date format. The “Set Date Format” prompt reappears. Click *** (NO)** to display the “Set Time and Date” prompt.
6. Click **# (YES)** to display the first time-and-date format. If the displayed format is not the one you want to use, click *** (NO)** to display the next format, and so on, until the format you want appears.
7. Click **# (YES)** to accept the desired time-and-date format. The “Set Time and Date” prompt reappears. Click *** (NO)** to display the “Set Address” prompt.
8. Enter one of the following addresses:
   a. If the hand reader is configured as an enrollment reader (connected to a PC via RS232 connection), set the address to 0.
   b. If the hand reader is configured as a standalone reader (connected directly to a PW-3000 RSI board in a PW-5000 panel), set the address to the address of the Primary Biometric Reader. You can find the Primary Biometric Reader address in the Logical Device Details tab.
9. Click **ENTER**. The “Set Address” prompt reappears. Click *** (NO)** to display the “Set ID Length” prompt.
10. Click *** (NO)** to display the “Set Output Mode” prompt. Click **# (YES)** to display the “For Lock & Aux.” prompt.
11. Click **# (YES)** to accept “For Lock & Aux.” Click *** (NO)** to display the “Facility” prompt. Click *** (NO)** to display the “Lock/Shunt Time” prompt.
12. Click *** (NO)** to display the “Set Aux Out Control” prompt. Click *** (NO)** to display the “Set Reader Mode” prompt.
13. Click **# (YES)** to display the “To Primary” prompt. Click ***(NO)** to display the “To Remote” prompt, and click **# (YES)**.
14. Click *** (NO)** to display the “Set Serial” prompt. Click **# (YES)** to display the “Set RS-485/422” prompt.
15. Click **# (YES)** to display the “9600 baud” prompt. Note that the baud rate you select here must be the same baud rate configured on the PW-3000 RSI gateway board. DIP switches 6 and 7 on the RSI board

set the baud rate. Look at the RSI board to determine the ON or OFF settings of switches 6 and 7, and then refer to the DIP switch table in the "PW-3000 RSI Board" section in this chapter to determine the board's baud rate. If the RSI board's rate is 9,600 BPS, click **# (YES)** to accept 9,600 BPS for the reader. If the RSI board's rate is 19,200 BPS, click *** (NO)** to display the "19,200 baud" prompt, and then **# (YES)** to accept 19,200 BPS for the reader. The "Set RS-232?" prompt appears.

16. Click *** (YES)** to display the "Set Duress Code" prompt. Click *** (NO)** to display the "Set Print Options" prompt.
17. Click *** (YES)** to display the "Set Beeper" prompt. Click *** (NO)** to return to the top of the menu.

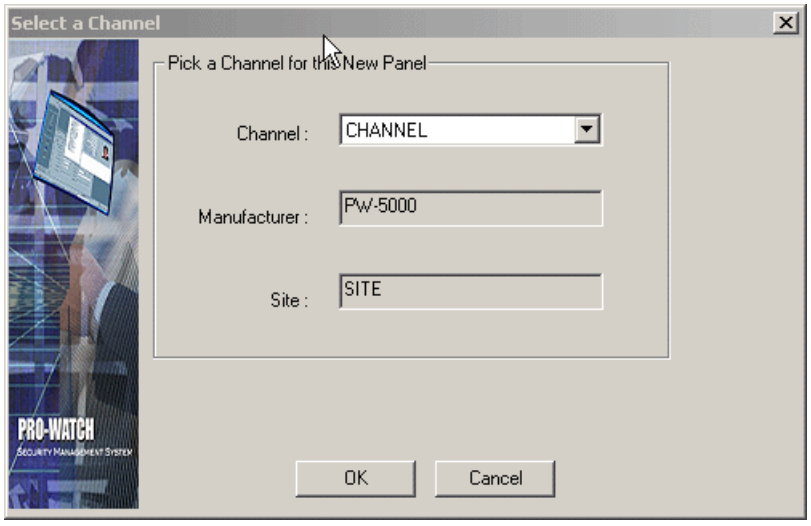
62.3 Configuring Pro-Watch to Support the Reader

62.3.1 Converting a PW-3000 Panel to an RSI Board

Biometric hand geometry readers are configured on RSI boards, which are converted from PW-3000 panels. Before you configure the hand geometry reader, you must configure the RSI boards.

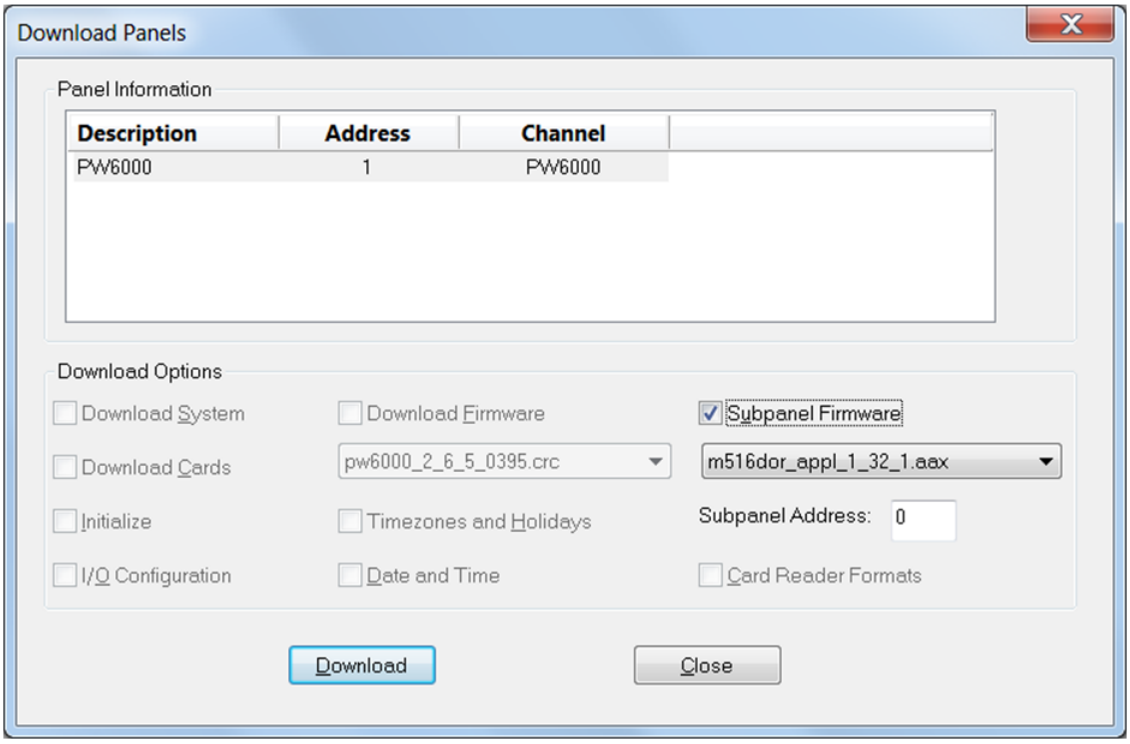
Follow these steps:

1. Convert a PW-3000 I/O to a PW-3000 RSI:
   a. Click **Start > Programs > Pro-Watch > Registry Manager** to display the Registry Manager dialog box.
   b. Set the PW300Firmware File registry key to the following: C:\Program File\ProWatch\FirmWare\NGwRsi.crc.
2. Add a PW-3000 panel:
   a. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.
   b. Add a PW-5000 Channel. Select **New > Panel** to display the Select a Channel dialog box:



3. Add a PW-3000 panel using the PW-5000 Channel you created:
   a. In the Add Panel dialog box, select PW-3000.
   b. Click **Add**. The Add PW-3000 Panel dialog box appears.
   c. Click **OK** to add the panel.

4. On the Pro-Watch Hardware Configuration screen, right-click the icon of the new panel and select **Download**. The **Download Panels** dialog box appears:



   a. In the Download Options box, click to de-select **Download System**.

   b. In the Download Options box, click to select **Download Firmware** and **Subpanel Firmware** (if applicable).

   c. Click **Download**. When the firmware is downloaded, the panel goes off-line. This indicates that the firmware successfully downloaded and that the board has been converted to an RSI board.

62.3.2 Configuring the Biometric Hand Geometry Reader

The biometric hand geometry reader is configured with the same general procedure used for any PW-5000/3000 device (see ""). However, the procedure in this section includes necessary information that is unique to the hand geometry reader.

Note: Pro-Watch Software Suite includes two new device types to support the biometric hand geometry reader. These device types are the Primary Biometric Reader and Secondary Biometric Reader.

1. Create a Hardware Class:

   a. In the Pro-Watch Hardware Configuration tree view, right-click Hardware Classes to display the Add Hardware Classes dialog box.

b. Enter a name for the new Hardware Class, such as Biometric Readers.

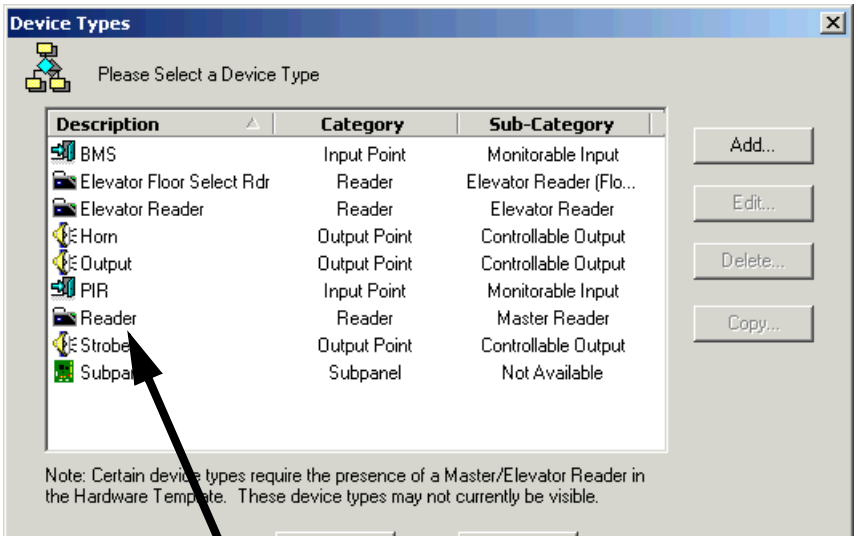
c. Click **OK**.

2. Create a Hardware Template. Note in this step that you must first add a Primary Reader Device Type before you can add the Primary Biometric Reader Device Type. This is similar to adding a Primary Reader Device Type before adding a Secondary Reader Device Type.

   a. Right-click Hardware Templates in the Pro-Watch Hardware Configuration tree view and select **New**. The Add Hardware Templates dialog box appears.

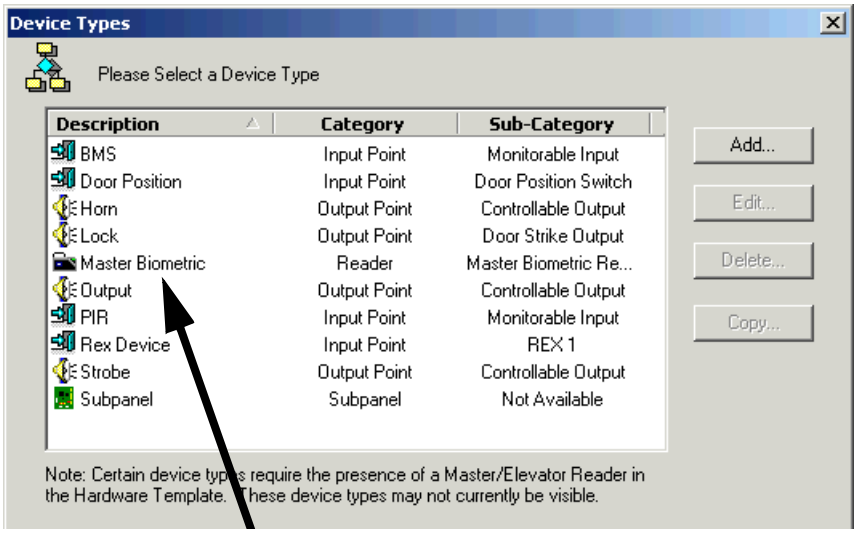
   b. Enter a description for the Hardware Template. See "Adding or Editing a Hardware Template" in Chapter 6 to complete the dialog box.

   c. Click the Device Types tab to display the Define Types box, and click **Add**. The Device Types dialog box displays device types, including Reader.



   d. Click to select **Reader** and click **OK**.

   e. In the Add Hardware Templates dialog box, click **Add**. The Add Device Types dialog box appears.



f. Click to select **Primary Biometric**, and click **OK**. The Device Types folder returns with the Primary Biometric reader entered.

g. Add a door position switch and a door lock to the Hardware Template.

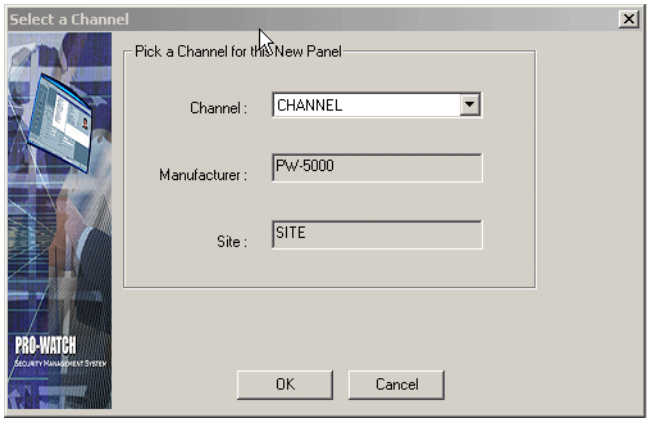
h. Click **OK** to accept the hand geometry reader Hardware Template.

3. Create a Channel for a PW-5000 panel. See "HW Config - PW-6000/5000/3000" in Chapter 9 for instructions.

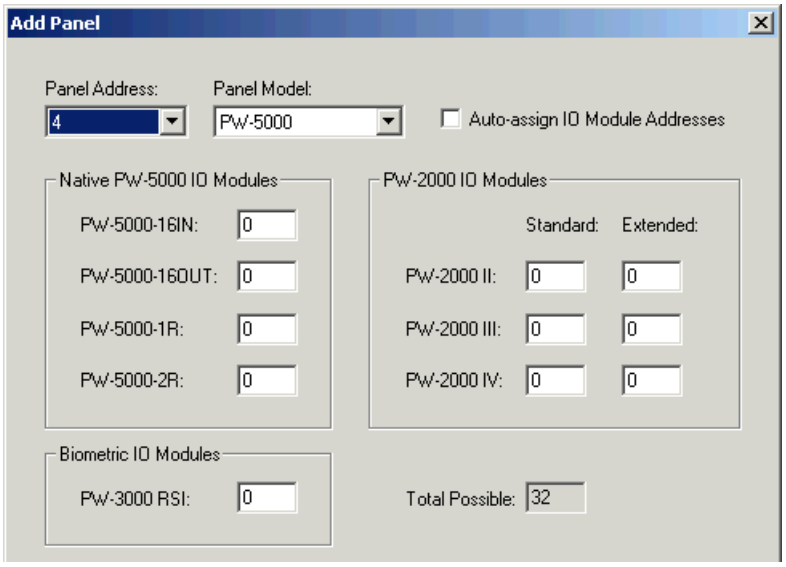
4. Add a PW-5000 panel:

   a. In the Pro-Watch Hardware tree view, right-click the site you have created for this panel.

   b. Select **New > Panel** to display the Select a Channel dialog box:



   c. Select the PW-5000 channel you want to use for the biometric hand geometry reader, and click **OK** twice to display the Add Panel dialog box:



Note: In the Biometric I/O Modules field, enter the number of PW-3000 RSIs you want to configure.
If you are configuring standalone hand geometry readers, you can configure a maximum of four hand geometry readers per RSI. If you are configuring complementary hand geometry readers, you can configure a maximum of eight readers per RSI. See "Overview" for an explanation of standalone and complementary reader configurations.

d. Click **Add**. The Assign I/O Modules dialog box appears. Enter an address number (0-31) for each module.

e. Click **OK**. The Add PW-5000 Panel dialog box appears.

f. Click the **Biometric Settings** tab. Use the following field descriptions to complete the Biometric Settings tab:

Field	Description
RSI Handkey	Indicates that the panel will support a biometric hand geometry reader.
Default Passing Score	Indicates the score a hand reading must receive before the biometric hand geometry reader grants access. It is recommended that you leave the number at 100.
Identix	N/A.
Bioscript	N/A.
Iridian	N/A.

g. Click each module to display the I/O Module tab, and click **Installed** for each module. This installs the module.

h. Click and complete the **Card Format** tab, and any other tabs in the Add PW-5000 Panel dialog box that you may require. See "HW Config - PW-6000/5000/3000" in Chapter 9 for more information about each tab.

i. Click **OK** to accept the panel.

5. Proceed to the following sections to complete the configuration of the biometric hand geometry reader:
   - Either "Configuring a Standalone Hand Geometry Reader" or "Configuring a Complementary Hand Geometry Reader".
   - "Configuring the Badge Profile for Hand Enrollment".
   - "Enrolling the Badgeholders' Hands".

62.3.2.1 Configuring a Standalone Hand Geometry Reader

1. Add a Logical Device:

   a. On the Pro-Watch Hardware Configuration tree view, right-click in the right pane and select **New > Logical Device**.

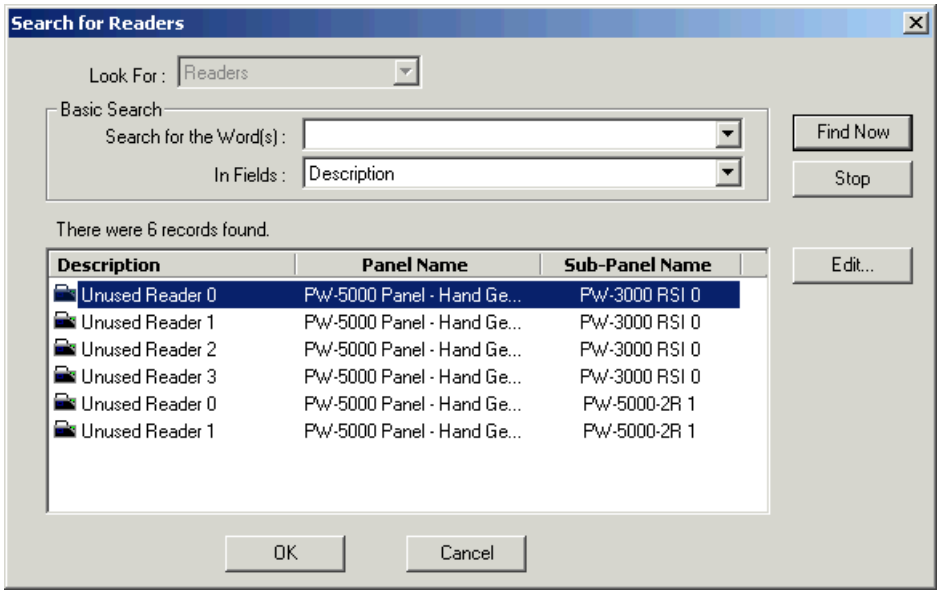
   b. Click to select the hand geometry reader Hardware Template, and click **Next**.

   c. Enter a description, alternate description, and location. Also, select a Hardware Class, and click **Next**.

Note: Click to select the **Reader** Device Type (Primary Reader in Sub-Category).

Do not select the Primary Biometric Device Type for a standalone hand geometry reader.

   d. Click **Assign HW...** The Search for Readers dialog box appears:



e. Click to select one of the unused readers on an RSI board, and click **OK** to assign it to the reader. The Logical Device Details dialog box appears and displays the assigned hardware. Note that you can identify RSI boards by the sub-panel names. For example, PW-3000 RSI 2 would be an RSI board.

f. At the Logical Device Details dialog box, click to select the Primary Reader and click **Edit**. The Edit PW-5000 Reader dialog box appears.

g. Click the **Reader Settings** tab and set the following: Default Mode = PIN only, Card Format = 26 Bit No Facility, Wiegand Pulse is selected, and Keypad Mode = None. Click **OK**. Also, assign hardware to the door position switch and the door lock. Note that the PIN number is either auto-generated or hand-generated in the Pro-Watch Badging component. Click the **Badging** icon to display a badge holder's badge, click in the Cards box to display the Card Information tab. The PIN Code field is on this tab. Note that the badge holder will be prompted to present his hand the reader when he enters this PIN code and then presses the pound (#) key.

h. Click **Next** twice, and then click **Finish** to add the Logical Device.

62.3.2.2 Configuring a Complementary Hand Geometry Reader

1. Add a Logical Device:

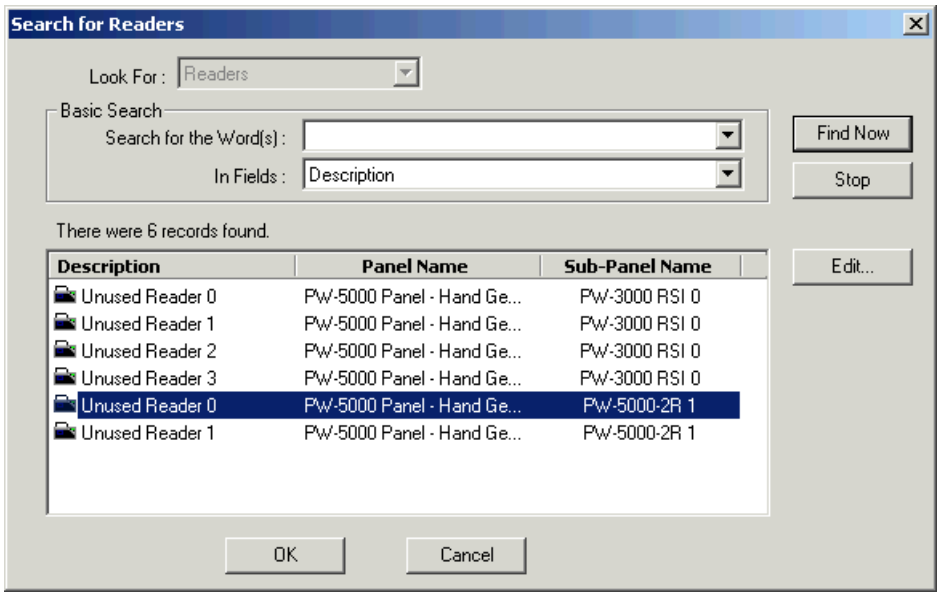
   a. On the Pro-Watch Hardware Configuration tree view, right-click in the right pane and select **New > Logical Device**.

   b. Click to select the hand geometry reader Hardware Template, and click **Next**.

c. Enter a description, alternate description, and location. Also, select a Hardware Class, and click **Next**.

d. Click to select the **Reader** Device Type (Primary Reader in Sub-Category).

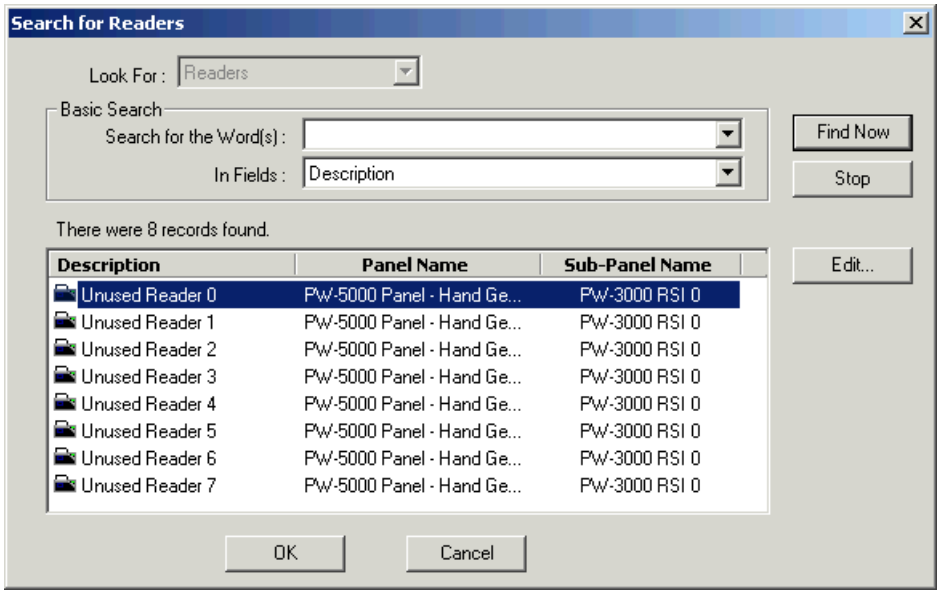
e. Click **Assign HW...** The Search for Readers dialog box appears:



f. Click to select one of the unused readers on a PW-5000 two-reader board, and click **OK** to assign it to the reader. The Logical Device Details dialog box appears and displays the assigned hardware. Edit and configure the reader to conform to your equipment. If you select Card and PIN, Card or PIN, or PIN only as the default mode, you can use the PIN key pad on the standard reader or the hand geometry reader.

g. Click to select the **Primary Biometric** Device Type (Primary Biometric Reader in Sub-Category).

h. Click **Assign HW...** The Search for Readers dialog box appears:



i. Click to select one of the unused readers on an RSI board, and click **OK** to assign it to the reader. The Logical Device Details dialog box appears and displays the assigned hardware.

j. Assign hardware to the door position switch and the door lock.

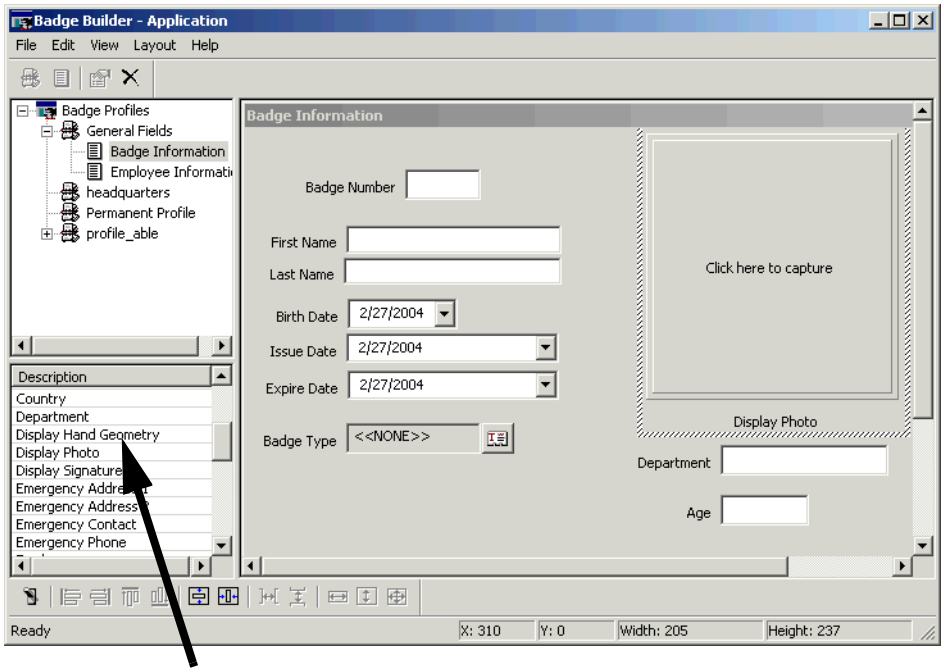
k. Click **Next** twice, and then click **Finish** to add the Logical Device.

62.3.2.3 Configuring the Badge Profile for Hand Enrollment

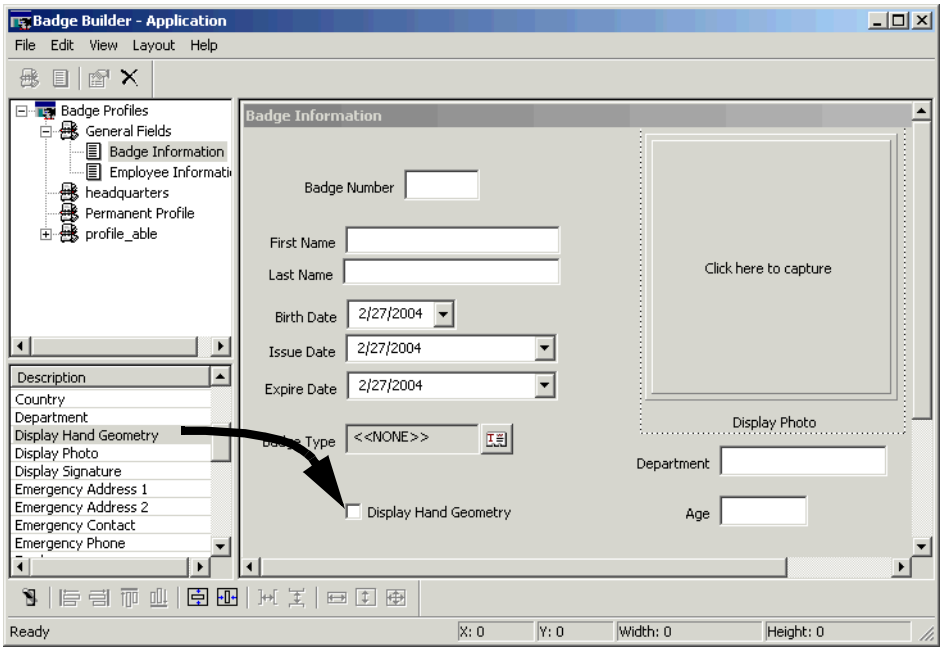
You must enroll the hand of each individual for whom you want to grant hand reader access. To do this, you must add a field to the Badge Profile.

Follow these steps:

1. On the Pro-Watch main screen, click the **Administration** icon to display the Pro-Watch Administration Viewer.
2. Click **Executables > Badge Builder** to display the Badge Builder Application screen.
3. Click **Badge Profiles > General Fields > Badge Information**. The Badge Information dialog box and a list of available badge fields appear. One of these fields is the Display Hand Geometry field.



4. Click to select the **Display Hand Geometry** field, and drag the field onto the Badge Information window, to the exact spot you want.

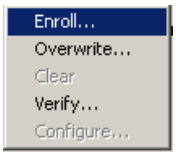


62.3.2.4 Enrolling the Badgeholders' Hands

After you add the Display Hand Geometry field to the Badge Profile, you can enroll the hands of your badgeholders.

Follow these steps:

1. On the Pro-Watch main screen, click the **Badging** icon to display the Pro-Watch Badging screen.
2. Click to select the name of the badge holder you want to enroll.
3. Click the Display Hand Geometry field to display a pop-up menu:



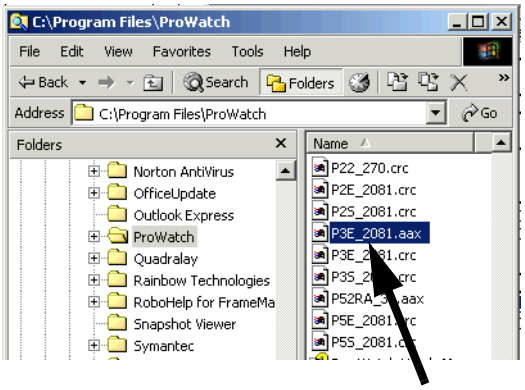
4. Click **Enroll** to activate the hand geometry reader and switch on the device's red lights.
5. Place the badge holder's hand on the device. When the badge holder squeezes his or her fingers into the reader's pins, the red lights go out. When all the red lights go out, the badge holder's hand measurements are stored in the Pro-Watch database as a Hand Key Geometry BLOB.
6. Repeat steps 2 through 5 for each badge holder.

62.3.3 Converting an RSI Board Back to a PW-3000 Panel

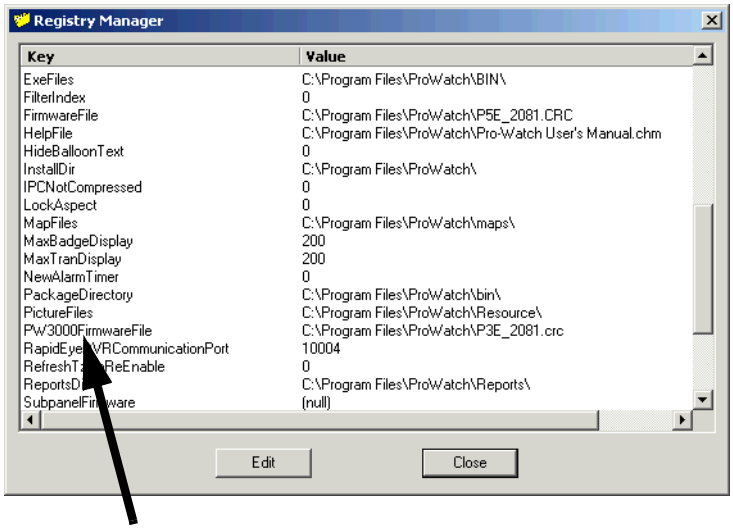
Use this procedure to convert an RSI board configured for the biometric hand geometry reader back to a PW-3000 panel. The procedure downloads the PW-3000 firmware.

Follow these steps:

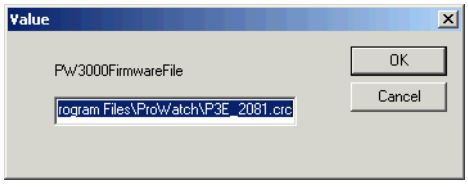
1. Copy the file name of the current Pro-Watch PW-3000 firmware to the Pro-Watch registry:
   a. Find the firmware file name at this path: Program Files\ProWatch\P3E_[version number].aax:



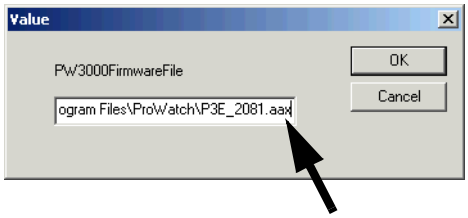
b. Click **Start > Programs > Pro-Watch > Registry Manager** to open the Pro-Watch registry. Locate the PW3000FirmwareFile registry key:



c. Click the PW3000FirmwareFile registry key value (or select the key and click **Edit**).The Value dialog box appears, enabling you to change the firmware file name:



d. Enter the current firmware file name located in step 1a. The extension of this file name must be .aax:



e. Click **OK**, and click **Close** to close the Registry Manager.

2. In the Pro-Watch Hardware Configuration tree view, click the **Panels** folder for the appropriate Site. The panel icons appear.
3. Right-click the icon of the panel you are downloading to, and select **Download**. The Download Panels dialog box appears.
4. Click to select the PW-3000 panel.
5. Click to select the **Subpanel Firmware** check box.
6. Click **Download** to download the firmware.
7. If you are downloading the firmware to a panel you are configuring for the first time, you should repeat the download process to download the system and card firmware. That is, in step 5 above, you would select **Download System** and **Download Cards** before clicking **Download**.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Data Management

63

In this chapter ...

Overview
Database Manager
Moving the Database to Another Drive

63.1 Overview

This chapter describes data management utilities that will help you perform the following:

- Database management – backing up and restoring the Pro-Watch database.
- Database moving – moving the database to another drive.
- Data archiving – moving transaction data (event and audit logs) to offline storage.
- Data transferring – importing data from an external database to synchronize Pro-Watch with the other systems that interact with it, and exporting Pro-Watch data.

63.2 Database Manager

The Pro-Watch Database Manager enables you to back up and restore databases as well as to maintain devices and backup/restore schedules.

Note: The default location of the PWNT database is

`C:\Program Files\Prowatch\Database\PWNT_Data.MDF.`

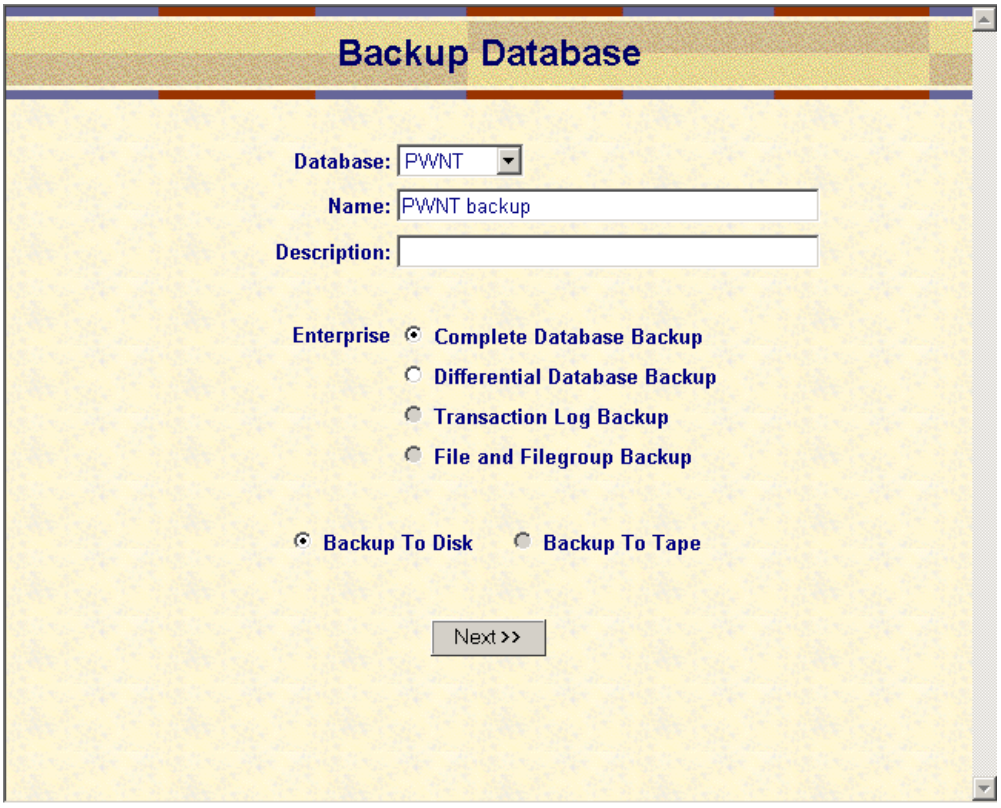
63.2.1 Backup Database

Use this function to perform any of the following types of Pro-Watch database backup:

- Complete database backup.
- Differential database backup.
- Transaction log backup.
- File and file group backup.

Follow these steps:

1. From the Windows menu bar, click **Start > Pro-Watch > Pro-Watch Enterprise Manager**. The Pro-Watch Database Manager dialog box appears.
2. Click the plus sign “+” in front of the appropriate database folder to expand it and then click **Backup Database**. The Backup Database dialog box appears in the right pane:

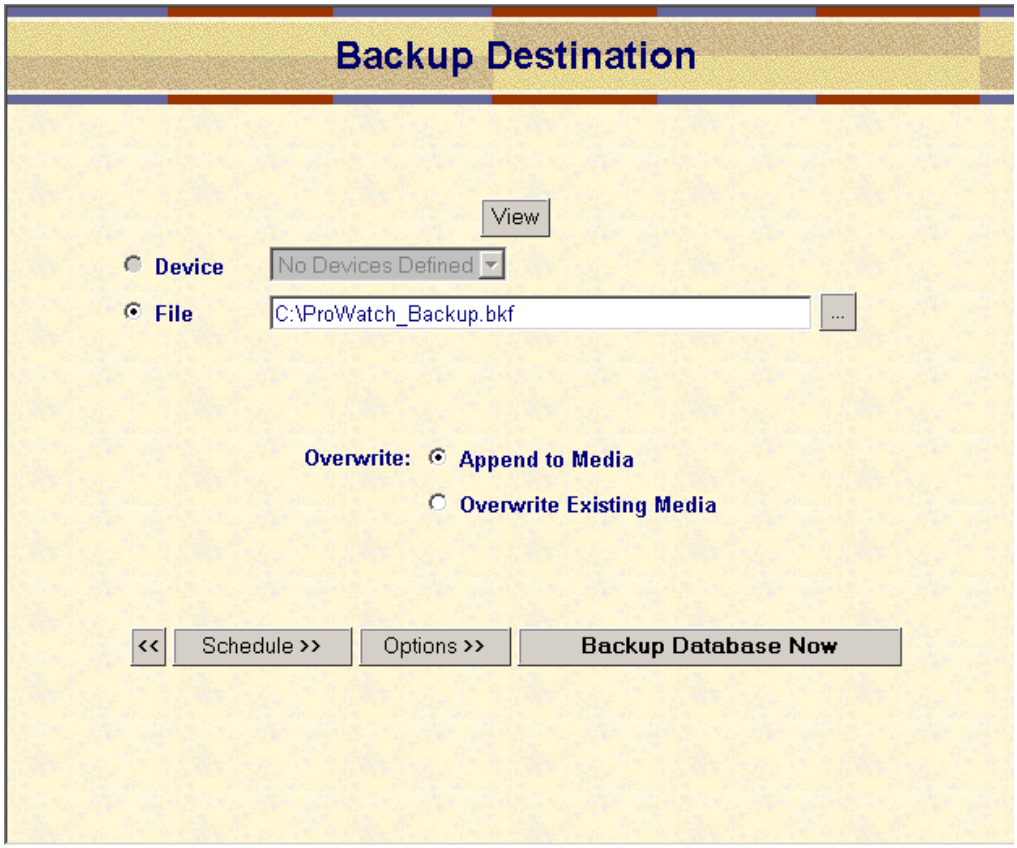


3. Use the following field descriptions to complete the Backup Database dialog box:

Field	Function
Database	Lists all databases in the SQL server.
Name	Specifies the name of the backup you will create.
Description	Describes and more fully identifies the contents of the backup.
Complete Database Backup	Creates a duplicate of the data that is in the source database. A full backup uses more storage space than differential and transaction log backups, and it takes more time.
Differential Database Backup	Records only the data that has changed since the last database backup. Since differential database backups are smaller and faster than full backups, they can be performed more frequently. More frequent backups decrease the risk of losing data. Use a differential database backup when a small amount of data has changed since the last database backup.

Field	Function
Transaction Log Backup	Restores a serial record of all the transactions that have been performed against the database since the transaction log was last backed up.
File and Filegroup Backup	Described in SQL server books on line.
Backup to Disk	Specifies that you will backup the database to a hard disk.
Backup to Tape	Specifies that you will backup the database to a tape drive.

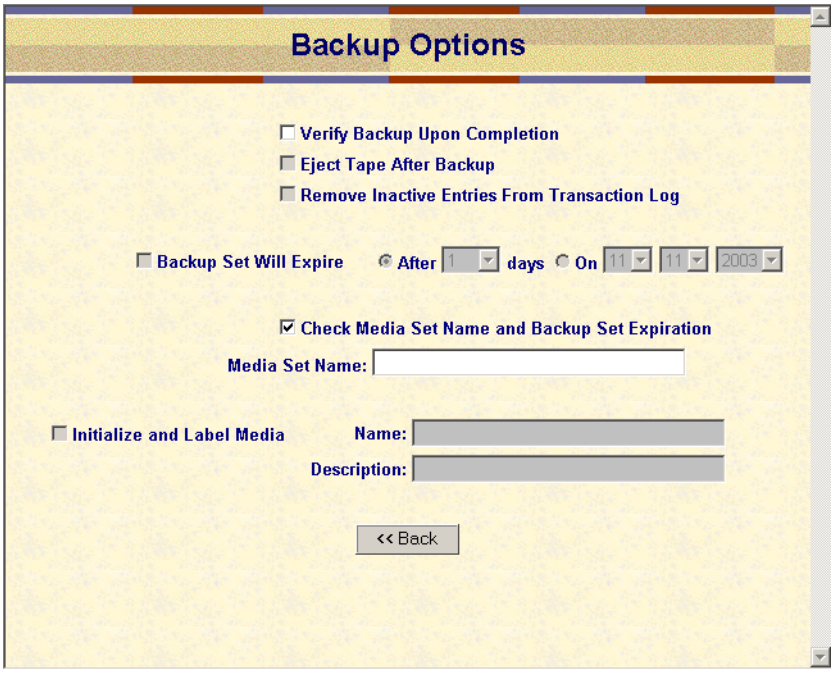
4. Click **Next** to display the Backup Destination dialog box.



5. Use the following field descriptions to complete the Backup Destination dialog box:

Field	Description
Device	Select this option button to specify a device as the destination of the backup. You can view the available devices by clicking the View button which displays the View Backup Contents screen. Click Back to return to the Backup Destination screen.
File	Enter the path of the destination file that you want to use for the backup. You can click the ellipsis (...) button to search for an appropriate directory.
Append to Media	Adds the backed-up data to any existing data on the destination file.
Overwrite Existing Media	Replaces any existing data on the destination file with the backed-up data.

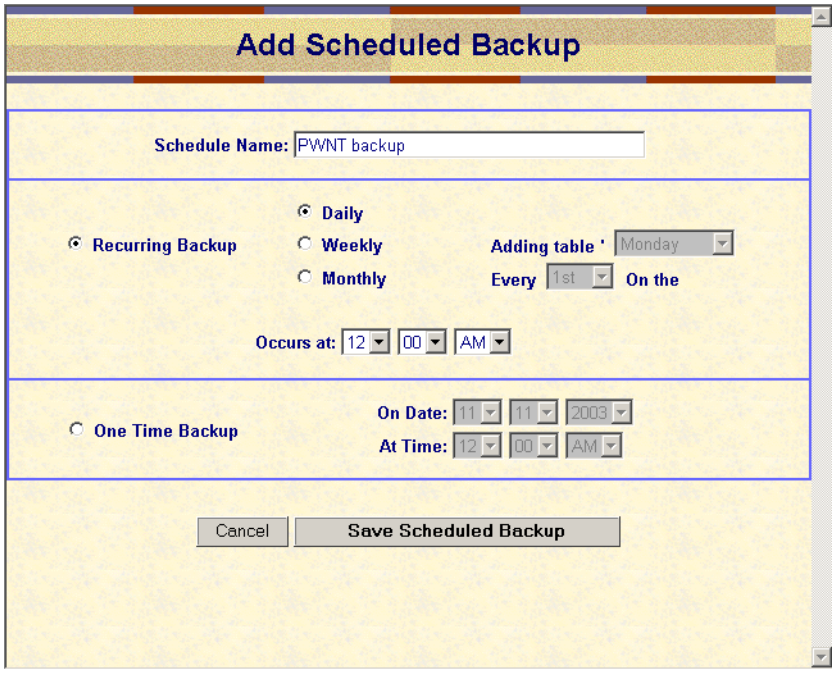
6. Click **Options** to refine the backup. The Backup Options dialog box appears:



7. Use the following field descriptions to select options:

Field	Description
Verify Backup Upon Completion	It verifies that the backup matches the source data.
Eject Tape After Backup	Ejects the tape from the tape drive after the backup completes.
Remove Inactive Entries from Transaction Log	Deletes the inactive entries from the transaction log.
Backup Set Will Expire	Select this check box to make sure that the scheduled back up will expire either: after a specific number of days (select from the drop-down list), or on a given date (select from the drop-down lists).
Check Media Set Name and Backup Set Expiration	When restoring, these will be checked to verify that the backup is a valid one.
Initialize and Label Media	Erase the tape/disk file before using it.
Name	Backup label.
Description	Description of the backup.

8. Click **Back** to return to the Backup Destination dialog box.
9. Either click **Schedule** to schedule one or more backups in the future (see Step 10 below), or click **Backup Database Now** to begin the backup immediately.
10. To schedule a backup, click **Schedule** to display the Add Scheduled Backup dialog box:



11. Enter a **Schedule Name**.
12. For recurring backups, select either the **Daily**, **Weekly** (enables the week day field on the right) or **Monthly** (enables the date field on the right) option button. For recurring weekly backups select a day of the week from the drop-down list. For recurring monthly backups select a day of the month from the drop-down list.
13. Enter a time for the backup by selecting an appropriate hour, minute, and AM/PM designation from the three drop-down lists below.
14. For one time backups, select an appropriate date and time from the respective drop-down lists.
15. Click **Save Scheduled Backup**.

Note: If you schedule one or more future backups, you can view the schedule by using the Schedule Maintenance tool on the Pro-Watch Database Manager menu tree. There you can view, disable/enable, or delete scheduled backups.

63.2.2 Restore Database

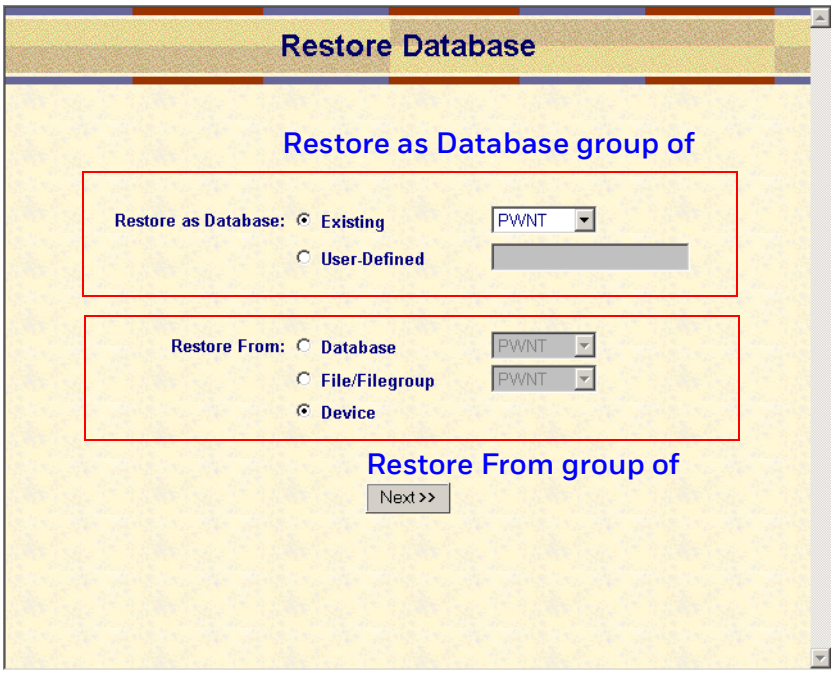
Use this function to restore a database from one of the following sources:

- Backed-up database.
- File or file group.
- Device.

For each type of restore, you can restore either to a database already defined in Pro-Watch, or you can restore to a database file that you have defined.

Follow these steps:

1. Stop the Pro-Watch Server service **(Start > Settings > Control Panel > Administrative Tools > Services)** before proceeding to restore the database.
2. From the Windows menu bar, click **Start > Programs > Pro-Watch > Pro-Watch Enterprise Manager**. The Pro-Watch Database Manager dialog box appears.
3. Click the plus sign "+" in front of the appropriate database folder to expand it and then click the **Restore Database** icon. The Restore Database dialog box appears in the right pane:



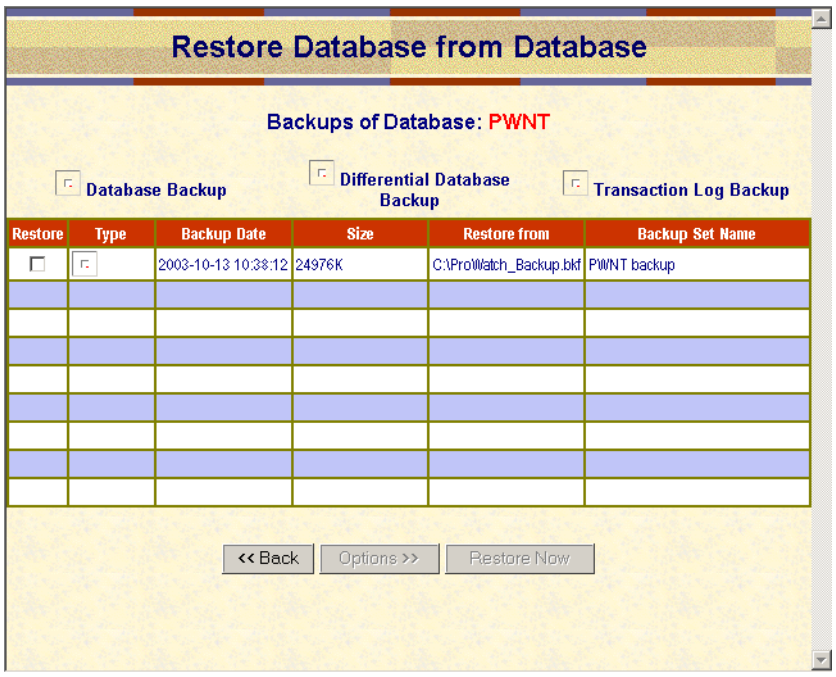
4. Choose among the types of backup restore below, and follow the steps given.

63.2.2.1 Restoring from a Backed-up Database

Use the Restore Database dialog box to restore a full database, differential database, or transaction log database.

Follow these steps:

1. In the Restore As Database group of fields, select from one of the following source database options by selecting the respective option button: an **Existing** database (select from the pull-down list) or a **User-Defined** database that you can specify in the text field. You can backup and then restore to a new database name to create a copy.
2. In the Restore From group of fields, click **Database, select a database from the drop-down list** and then click **Next**. The Restore Database from Database dialog box appears:



3. Click one of the following types of restore:
   - Database backup – restores a complete database. The restore process either overwrites the existing database or creates a new database if one does not exist.
   - Differential database backup – restores only the data that has changed since the last database backup.
   - Transaction log backup – restores a serial record of all the transactions that have been performed against the database since the transaction log was last backed up.

4. To view further restore options, click **Options**. The Restore Options dialog box appears.
5. Click **Restore Now** to restore the database according to your specifications.

63.2.2.2 Restoring from a File or File Group

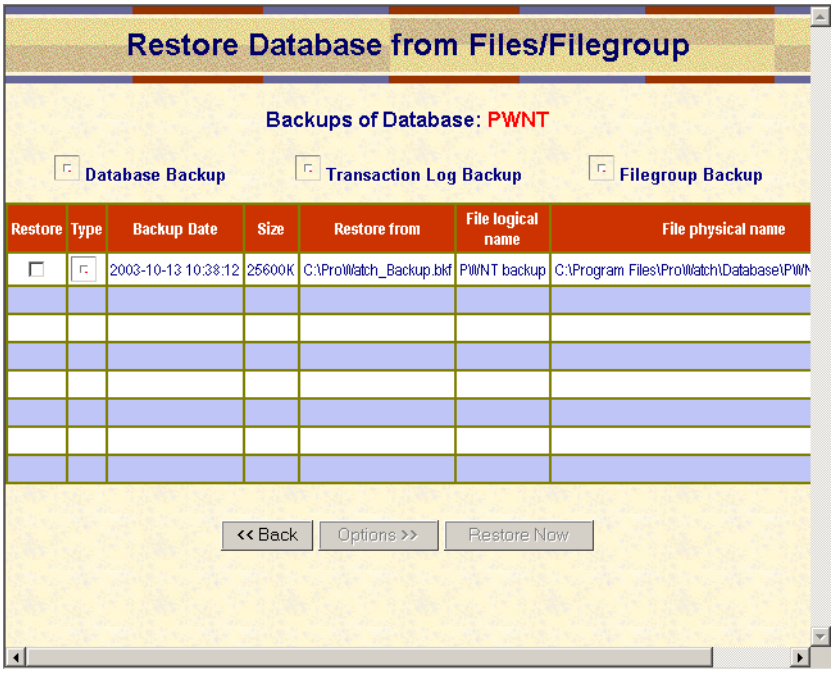
Use this function to restore a database from an existing file or group of files.

The files in a database can be backed up and restored individually. Doing this can increase the speed of recovery by allowing you to restore only damaged files without restoring the rest of the database.

Examples: If a database is comprised of several files physically located on different disks and one disk fails, only the file on the failed disk needs to be restored.

Follow these steps:

1. In the Restore As Database group of fields, select from one of the following source database options by selecting the respective option button: an **Existing** database (select from the pull-down list) or a **User-Defined** database that you can specify in the text field.
2. In the Restore From group of fields, click **File/Filegroup**, select a database from the drop-down list, and then click **Next**. The Restore Database from File/Filegroup dialog box appears:



3. Select one of the following types of restore:

- **Database backup** – restores a complete database. The restore process either overwrites the existing database or creates a new database if one does not exist.
- **Transaction log backup** – restores a serial record of all the transactions that have been performed against the database since the transaction log was last backed up.
- **File group backup** – is a single backup of all files in the filegroup and is equivalent to explicitly listing all files in the filegroup when creating the backup. Files in a filegroup backup can be restored individually or as a group.

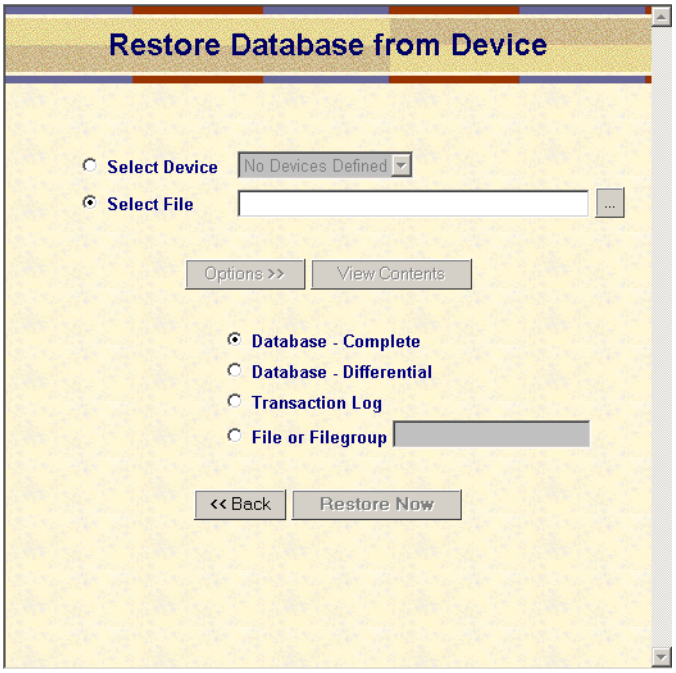
4. To view further restore options, click **Options**. The Restore Options dialog box appears.
5. Click **Restore Now** to restore the database according to your specifications.

63.2.2.3 Restoring from a Device

Use this function to restore a database from a device such as a tape drive.

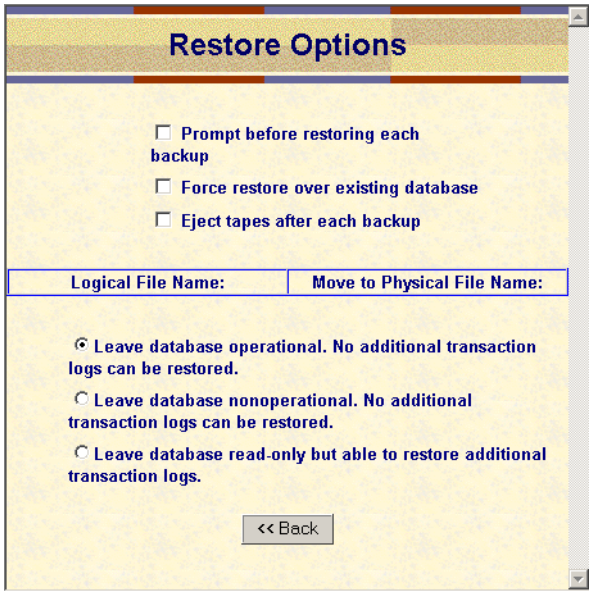
Follow these steps:

1. In the Restore As Database group of fields, select from one of the following source database options by selecting the respective option button: an **Existing** database (select from the pull-down list) or a **User-Defined** database that you can specify in the text field.
2. In the Restore From group of fields, click **Device** and then click **Next**. The Restore Database from Device dialog box appears:



3. Either:
   - Click the **Select Device** option button and select a tape drive from the drop-down menu, or
   - Click the **Select File** option button, then click the ellipsis button next to the field and browse for a disk file.

     Tip: A tape drive will allow you to work offsite and not rely on sufficient disk space. It protects you against disk crashes as well. The advantage of working from a disk, on the other hand, is that it is quicker and more convenient.
4. Click **View Contents** to retrieve backup labels like date and time of backup (see Initialize Label Backup).
5. Click **Options** to refine the restoration procedure. The Restore Options dialog box appears:



6. Use the following field descriptions to select options:

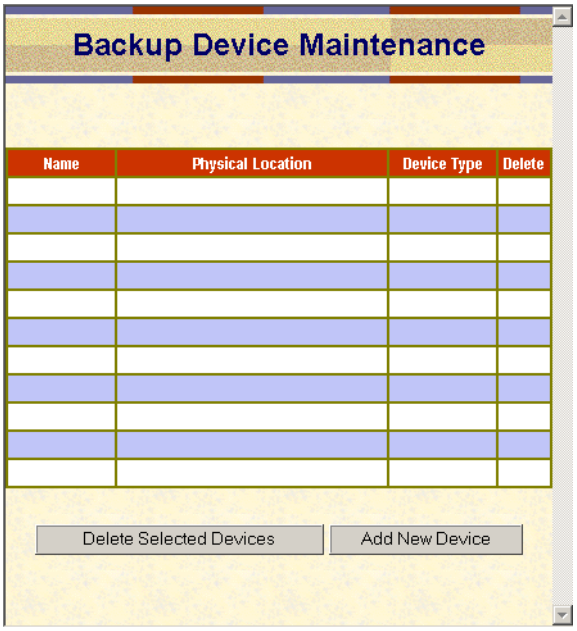
Field	Description
Prompt before restoring each backup.	A warning prompt requires your confirmation before the restore proceeds.
Force restore over existing database.	Causes the restore to proceed without prompts and to automatically write over any existing database.
Eject tapes after each backup.	Ejects the tape from the device when the restore completes.
Leave database operational. No additional transactions logs can be restored.	Leaves the restored database in an operational state and incapable of being changed by future transaction log restorations.
Leave database non-operational. No additional transactions logs can be restored.	Leaves the restored database in a non-operational state and incapable of being changed by future transaction log restorations.
Leave database read-only, but able to restore additional transaction logs.	Leaves the restored database in an unchangeable state, except for changes caused by future transaction log restorations.

7. Select one of the following four restore options:
   - **Database Complete** – restores a complete database. The restore process either overwrites the existing database or creates a new database if one does not exist.
   - **Database Differential** – restores only the data that has changed since the last database backup.
   - **Transaction Log** – restores a serial record of all the transactions that have been performed against the database since the transaction log was last backed up.
   - **File or File Group** – The files in a database can be backed up and restored individually. Doing this can increase the speed of recovery by allowing you to restore only damaged files without restoring the rest of the database. For example, if a database is comprised of several files physically located on different disks and one disk fails, only the file on the failed disk needs to be restored.
8. Click **Restore Now** to restore the database according to your specifications.

63.2.3 Backup Device Maintenance

Follow these steps:

1. From the Windows menu bar, click **Start > Programs > Pro-Watch > Pro-Watch Enterprise Manager**. The Pro-Watch Database Manager dialog box appears.
2. Click the plus sign "+" in front of the appropriate database folder to expand it and then click the **Device Maintenance** icon. The Backup Device Maintenance dialog box appears in the right pane:



Use the following field descriptions to complete the Add Backup Device dialog box.

Field	Description
Name	The name of the device used for backup.
Physical Location	The address of the physical location where the backup device is kept.
Device Type	The kind of backup device used. For example, a Tape drive.
Delete	This column identifies the devices you want to delete.

To add a device:

1. Click **Add New Device**. The **Add Backup Device** dialog box will display.
2. Enter a **Device Name**.
3. If the device you are adding is a tape drive, select the **Tape** option button and then select one from the drop-down list.
4. If the backup will be restored from a file, select the **File** option button and then click the ellipsis button to browse to the appropriate file.
5. After completing either step 3 or 4, click **Add Device** to add the device.

To delete a device:

1. Select the respective check box under the Delete column to select the device you want to delete.
2. Click the **Delete Selected Devices** button.

63.2.4 Scheduled Maintenance

Use this function to view all scheduled maintenance tasks and either modify, disable, or delete any of the tasks.

Follow these steps:

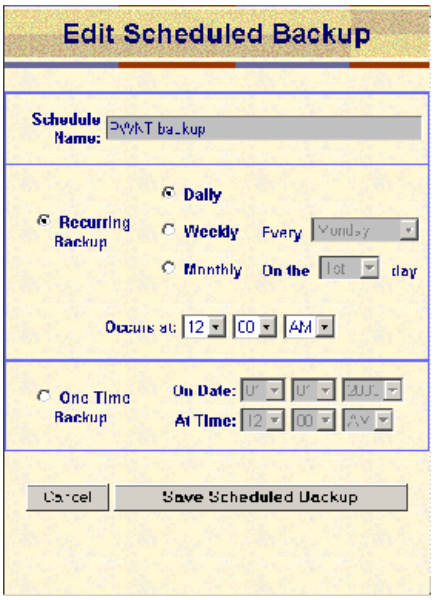
1. From the Windows menu bar, click **Start > Programs > Pro-Watch > Pro-Watch Enterprise Manager**. The Pro-Watch Database Manager dialog box appears.
2. Click the plus sign "+" in front of the appropriate database folder to expand it and then click the **Schedule Maintenance icon**. The Schedule Job Maintenance dialog box appears in the right pane:



63.2.4.1 Editing Scheduled Maintenance Jobs

Use this function to change the schedule of a listed maintenance job.

1. Click the job name in the Job Name column. The Edit Scheduled Backup dialog box appears.



2. Edit the schedule settings as you desire and click **Save Scheduled Backup**.

63.2.4.2 Disabling and Enabling Scheduled Maintenance Jobs

Use this function to quickly disable or enable a scheduled job on the Schedule Job Maintenance dialog box. Disabling the job does not delete the job or the job schedule. The job and schedule remain listed in the dialog box and require only a click to be re-enabled.

To disable a job:

Click to remove the check mark in the **Enabled?** column next to the job listing in the Schedule Job Maintenance dialog box.

To re-enable the job:

Simply click the same box to re-produce the check mark.

63.2.4.3 Deleting Scheduled Maintenance Jobs

Use this function to delete scheduled jobs when you no longer want them to continue.

Note: If you want to resume a deleted job at any time, you will need to re-create the job and schedule with the Backup Database function.

1. Click the **Delete** box next to the job(s) you want to delete on the Scheduled Job Maintenance dialog box.
2. Click **Delete Scheduled Jobs**.

63.3 Moving the Database to Another Drive

Use this procedure to move the Pro-Watch database from one drive to another using OSQL. You might want to do this, for example, if the database was installed on the C drive. The C drive is often reserved for application programs. The Pro-Watch database could potentially consume enough space to cause memory problems.

To move the Pro-Watch database from drive C to drive D using OSQL:

1. Back up the Pro-watch database to a safe location. See "Backup Database" for backup instructions.
2. Stop the Pro-watch service (you might need to stop and restart the SQL server if you receive an error that the PWNT database is in use).
3. In OSQL:
   a. Change directory to program files.
   b. Pro-Watch folder.
   c. Enter `OSQL -E`.
   d. Press **Enter**. The prompt 1> should appear.
4. Run the detach script:
   1>sp_detach_db @dbname = 'PWNT'
   2>Go (If successful, the 1> prompt returns; otherwise, you will receive an error.)
5. Create a new folder on the D drive and name the folder Prowatch_db.
6. On the C drive, rename PWNT_LOG.ldf to PWNT_LOG.
7. Copy PWNT_DATA.mdf to the \Prowatch_db folder on the D drive.
8. Run the attach script:
   1>sp_attach_single_file_db @dbname = 'PWNT', @physname = 'd:\Prowatch_db\pwnt_data.mdf '
   2>Go (If successful, you will receive a device activation error on the old log file and a message that a new log file was created on the D drive and go back to the 1> prompt.)

9. Run the following to verify that the database attached successfully:
   1>Use PWNT
   2>Select * from UID
   3>Go (If successful, you will see data scroll across the screen. The data will contain a list of all the Pro-Watch users.)
10. Start the Pro-Watch service. If you can log into the Pro-Watch application, it is now safe to delete the PWNT_DATA.mdf and PWNT_LOG files from the C drive.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Data Transfer Utility (DTU)

64

In this chapter ...

Overview
Installing Real Time DTU
Log File
Data Transfer Interfaces
Data Transfer Steps
Adding a DTU Import or Export Profile
Editing a DTU Profile
ODBC Import Mapping Rules
ODBC Export Mapping Rules
Transferring the Data
LDAP/Active Directory Integration

64.1 Overview

You can import data from an external data source to synchronize Pro-Watch with the other systems that interact with it. Mapping of data from an external data source to Pro-Watch is accomplished using the **Data Transfer Utility (DTU)**.

Loading the data can be done manually as well. DTU is also used for database table migrations from one version of Pro-Watch NT to a newer version of Pro-Watch NT.

Companies often wish to integrate their human resource data with the security/access control system, especially when an employee has been terminated. The Pro-Watch Data Transfer Utility (DTU), using a variety of data transfer interfaces, provides the means to insert and update Pro-Watch badging data as often as needed.

Examples:

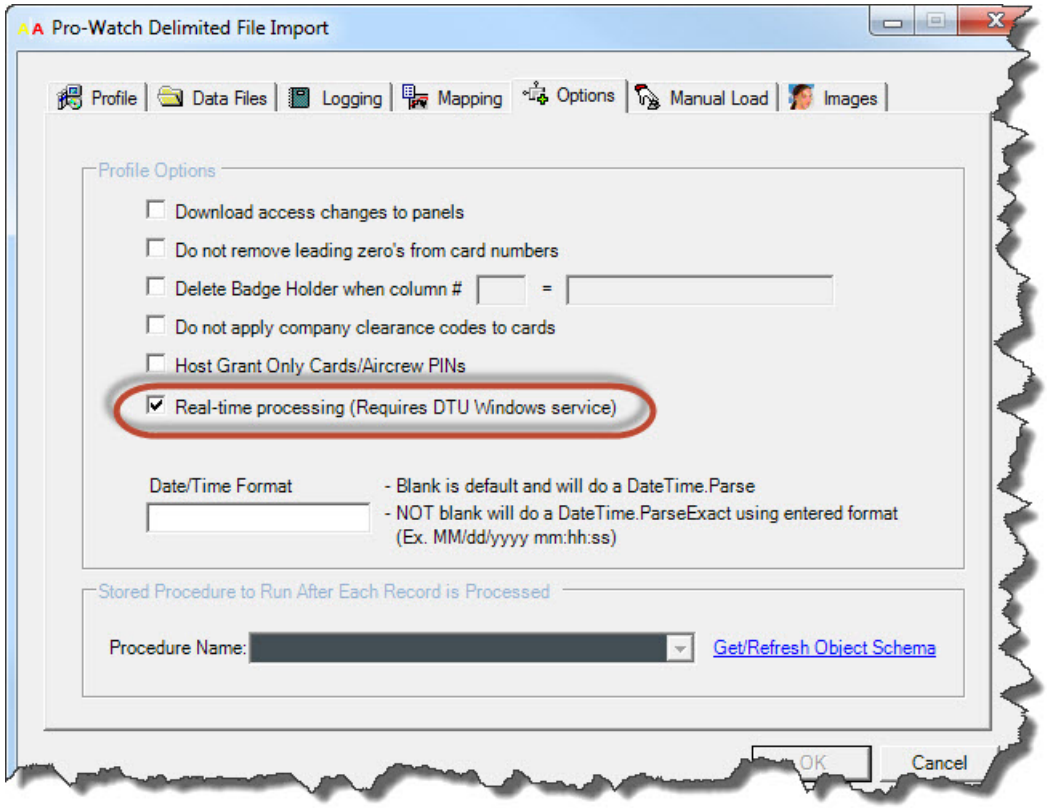
- You may want any changes in the human resources data reflected in the Pro-Watch data as well so that the personnel who leave the company do not have access to the premises, or, you may want to issue access codes and cards for the new hires. You can accomplish such necessary synchronization by importing the HR data into Pro-Watch. Many companies use data exports to synchronize Pro-Watch with the other systems that interact with it.
- A university may use the same card both to grant physical access to the campus buildings and provide meal services at the cafeteria. When such a multi-purpose card gets lost and a new one is issued, you have to make the necessary deletions and additions both in the physical access (Pro-Watch) and the dining services databases. Such synchronization is easily accomplished by making the necessary edits in Pro-Watch and then exporting the edited data to the external database (for example, dining services).
- When a company is publishing a web directory of employees, they may want to include only those employees with specific access profiles. This can be accomplished easily by exporting the Pro-Watch data to the web directory

64.2 Installing Real Time DTU

Note: The Real Time DTU must be installed in the ProWatch\DTU folder. DTU is now in its own folder. It is no longer in the ProWatch\bin folder.

1. Copy **HoneywellAccess.ProWatch.RealDTU.exe**, **HoneywellAccess.ProWatch.RealDTU.exe.config**, **Install_RealTime_DTU_Service.bat** and **Uninstall_RealTime_DTU_Service.bat** in the ProWatch\DTU directory.
2. Double click on **Install_RealTime_DTU_Service.bat** to install the service.
3. Go to the **Windows Services**.
   a. Select the **Pro-Watch Real Time DTU Service.** Double-click it to display its properties screen.
   b. Click and select the **Logon tab.**
   c. Enter valid values for the **Account Logon Name** and **Password** fields.
4. Start the R**eal Time DTU Service**.
5. In Pro-Watch, select **Administration > Executables > Data Transfer Utility** to display the DTU profiles. Double click the respective DTU

profile to display its properties screen. Click and select the **Options** tab. Then select the "**Real-time processing**" check-box:



6. Drop the data file in the DTU directory to process it. If there is an error in the data transfer process, it will be logged in the user-defined **DTU Log file** configured in the **Logging** tab of the respective **DTU profile**. See the section "Log File" below.

64.2.1 Configuring Real Time DTU

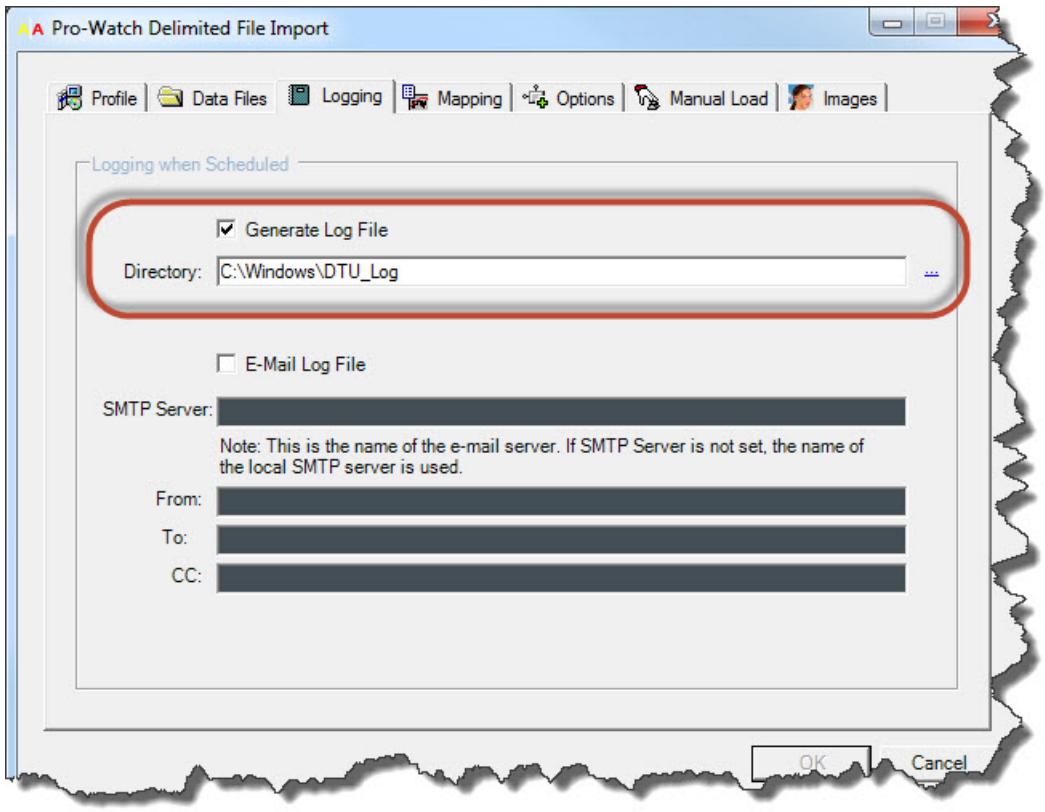
In the configuration file for Real Time DTU, a forward slash ("/") needs to be placed at the end of the file location:

```
<add key="PWIFaceXmlLocation" value="C:\Users\super\Desktop\" />
```

If the forward slash is missing, the Real Time DTU service will not start and the event viewer message will warn that the PWIFace.xml file cannot be found.

64.3 Log File

All data loaded to Pro-Watch using the DTU can produce a log file that displays the number of records inserted, updated, and if an error occurs, the location in the data file that produced the error. You can configure the directory address of the log file in the **Logging** tab of the respective **DTU profile**



64.4 Data Transfer Interfaces

The Pro-Watch Data Transfer Utility (DTU) enables you to import and export data by utilizing the following interfaces:

- Delimited text files.
- Fixed-length data.
- SQL/Microsoft Access databases.
- ODBC (Open Data Base Connectivity) databases.
- LDAP (Lightweight Direct Access Protocol) databases.
- Images.

64.5 Data Transfer Steps

A Pro-Watch data transfer requires two steps:

1. Add an import or export profile. A profile is a file that identifies a transfer source and destination. Pro-Watch ensures that the source and destination have matching schemes, which is a must for a successful transfer.
2. Transfer the data. See "Transferring the Data".

64.5.1 Importing PINs and Duress Digit

When the duress functionality is enabled, the duress digit must be different than the last digit of PIN.

In cases where PINs are imported through DTU, the duress digit is not checked against the last digit of the imported PINs. Therefore, in such cases it is the user's responsibility to make sure that none of the imported PINs have a last digit that is equal to the duress digit.

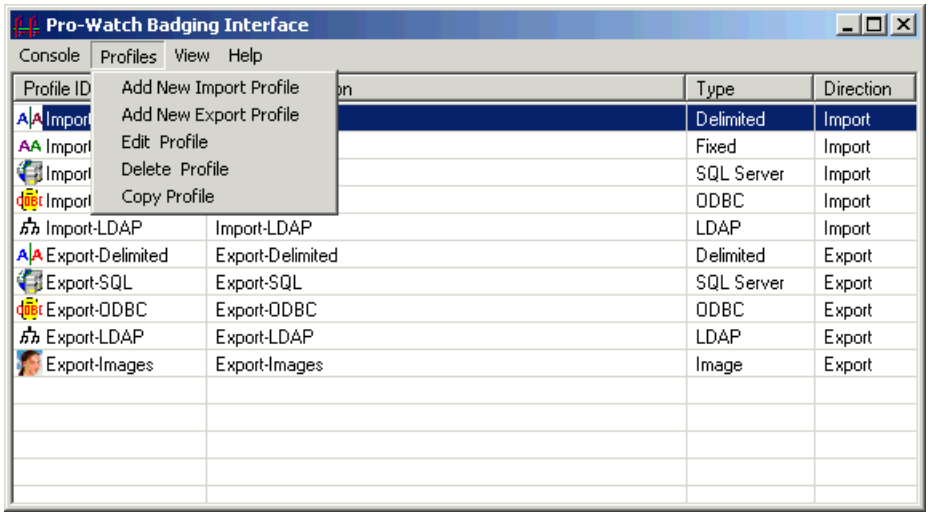
64.6 Adding a DTU Import or Export Profile

You need to create an import and export profile first in order to be able to transfer data.

Each data source is defined as a profile in the DTU. A profile defines all aspects regarding how the data will be loaded to Pro-Watch, including the type of data load, where the data comes from, the type of logging, and the mapping between Pro-Watch and the data source.

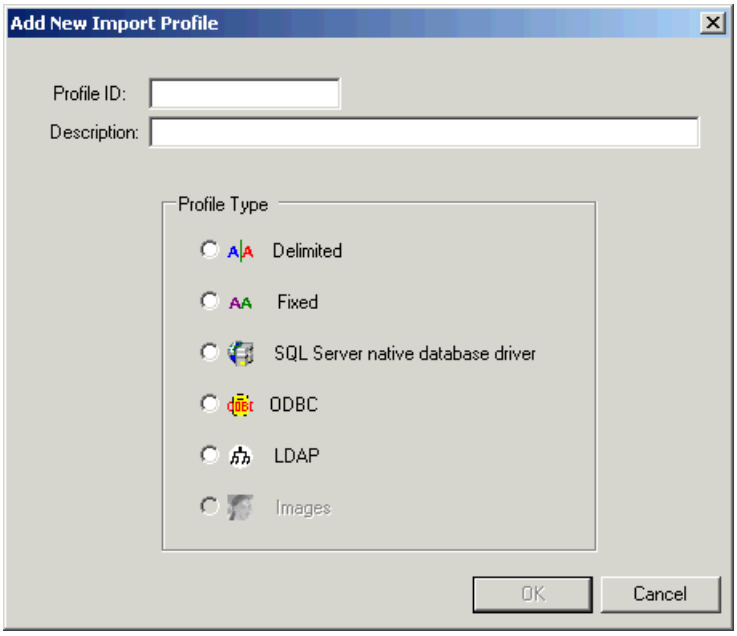
Follow these steps:

1. Double-click **Pro-Watch Administration Viewer > Executables > Data Transfer Utility** in the center pane to display the Pro-Watch Data Transfer Utility screen in a separate window:



2. Click **Profiles** and select **Add New Import Profile** or **Add New Export Profile** to display either the Add New Import Profile or the Add New Export Profile dialog box, which look almost identical.

Here is the Add New Import Profile dialog box:



3. Enter a **Profile ID** and **Description**.
4. Select one of the following option buttons to specify a data source:
    - **Delimited** - data in a text file, individual fields separated by |-vertical bars, commas or tabs.
    - **Fixed** - data with a fixed length. You can import but cannot export fixed length data.
    - **SQL server native database driver**.
    - **ODBC** (Open Data Base Connectivity) - an Application Programming Interface (API) that allows you to import from and export to a database.
    - **LDAP** (Lightweight Direct Access Protocol) - an Internet protocol that allows you to import from and export to a database.
    - **Images** - you can export but cannot import images as data.
5. Click **OK** to save the new profile.

64.7 Editing a DTU Profile

In the Pro-Watch Data Transfer Utility screen, right-click the icon of the profile you want to edit and select **Edit Profile**. The editing screen for the data profile selected appears.

Editing tabs and fields for each data source is explained in separate sections. Click one of the following links to go directly to the relevant section:

- "Why Import Pro-Watch Data?"
- "Editing a Delimited Database Import Profile"
- "Editing a Fixed-Length Data Import Profile"
- "Editing an SQL Database Import Profile"
- "Editing an ODBC Database Import Profile"
- "Editing an LDAP Database Import Profile"
- "Why Export Pro-Watch Data?"
- "Editing a Delimited Data Export Profile"
- "Editing an ODBC Database Export Profile"
- "Editing an Image Export Profile"

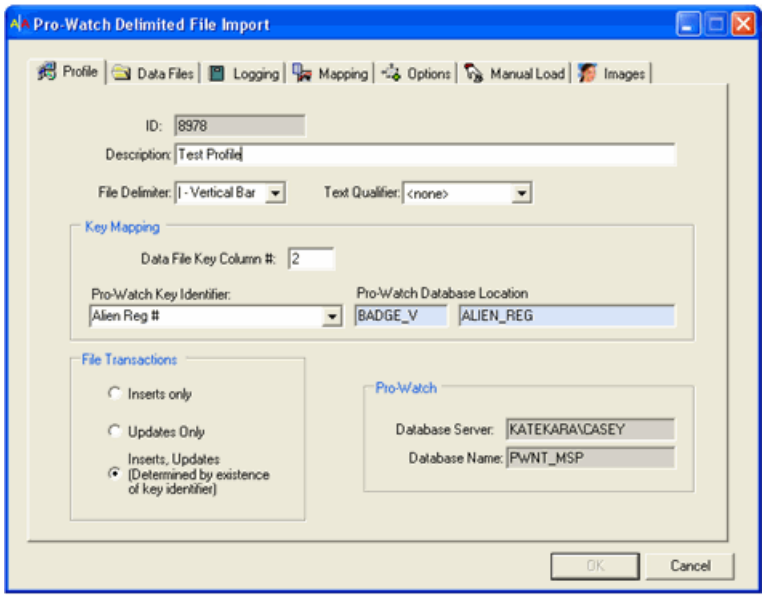
64.7.1 Why Import Pro-Watch Data?

You may want to import data from an external database to synchronize Pro-Watch with the other systems that interact with it.

Example: You may want any changes in the human resources data reflected in the Pro-Watch data as well so that the personnel who leave the company do not have access to the premises, or, you may want to issue

access codes and cards for the new hires. You can accomplish such necessary synchronization by importing the HR data into Pro-Watch.

64.7.2 Editing a Delimited Database Import Profile



Edit the following Delimited Database Import fields as appropriate.

TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile tab".
- "Data files tab".
- "Logging tab".
- "Mapping tab".
- "Options tab".
- "Manual Load tab".
- "Images tab".

Tab	Field	Comments
Profile tab (Return to Delimited "TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.
	Description	Description of the profile. Required field.

Tab	Field	Comments
	File Delimiter	The text character that separates the data fields in the data file. Required field. Select one from the drop-down list: I-Vertical Bar. Comma. Tab.
	Text Qualifier	Select one from the drop-down list: <none>. Double Quote {"}. Single Quote {'}.
	Data File Key Column #	This is the delimited field number in the delimited file that is used to determine whether a record will be an Update or an Insertion. This is the unique key in the data file that identifies individuals in the external system. Required if transactions are "Updates Only" or "Updates, Inserts Only."
	Pro-Watch Key Identifier	This is the Pro-Watch data field that maintains the keys of the external system. This is used to determine if a record is an Update or Insertion.
	Pro-Watch Database Location	Read-only fields that are enabled when a Pro-Watch Key Identifier is entered. The first field displays the name of the database table and the second field displays the name of the database column in that table to which the data will be transferred by DTU.
	File Transactions	The type of transactions this profile contains. Required field. Select one of the following option buttons: Inserts Only—If a "Data File Key Column #" is provided, the DTU will only insert a new badge record if the key column value is not found. An error will be displayed in the log file if an existing badge record is found. If no "Data File Key Column #" is provided, every record will be inserted into Pro-Watch. Updates Only—The DTU will use the "Data File Key Column #" to look for the matching Pro-Watch record. An error will be logged in the log file if the badge holder is not already in the Pro-Watch database. Inserts, Updates—The DTU will use the "Data File Key Column #" to look for the matching Pro-Watch record. If a matching record is not found, the DTU will insert the data. If a matching record is found, the record will be updated.
	Database Server	The name of the Pro-Watch database to which the data will be loaded.
	Database Name	Name of the database.
Data files tab (Return to Delimited "TAB LIST")	Directory	Location of the delimited data source file. Required field. Click the ellipsis (...) button to browse for a directory.

Tab	Field	Comments
	Option Buttons	Select one: Load all files in Directory—Loads all files specified in the data directory. Load only the file with the following name—Loads a single file with the name specified. Load all files that match the following naming pattern—Loads all the files that match the specified naming pattern. Wildcard "*" and single character wildcard "?" can be used to specify a naming pattern.
	Archive file when finished processing	The directory where the file that was processed will be archived after the file has been loaded.
	Directory	Location of the archived file. Click the ellipsis (...) button to browse for a directory.
Logging tab (Return to Delimited "TAB LIST")	Generate Log File	Select this check box to generate a log file for scheduled data transfer sessions.
	Directory	Location of the log file. Click the ellipsis (...) button to browse for a directory.
	E-Mail Log File	Select this check box to e-mail the generated log file.
	SMTP Server	The name of the e-mail server which will e-mail the log file. Enabled if the e-mail check box is selected.
	From, To, CC	Enter the From, To and Copy e-mail addresses to be used when the log file is e-mailed. Enabled if the e-mail check box is selected.
Mapping tab (Return to Delimited "TAB LIST")	Pro-Watch Badging Field	Select a badge field from the drop-down list. Required field.
	Pro-Watch Database Mapping	Read-only fields that are enabled when a Pro-Watch Badging Field is selected from the drop-down list. The first field displays the name of the database table and the second field displays the name of the database column in that table to which the Badging Field selected will be transferred by DTU.
	Default Value	If no data is supplied in the file, this value will be used to update or insert the badging record for the mapping value. If no "Delimited Field #" is defined, this value will always update the defined mapping value unless the "Apply Default to Inserts Only" is checked.
	Apply Default to Inserts Only	Select this check box to apply the "Default Value" when the transaction is an insert. This option will not overwrite the existing value by inserting the default value when updating a record.
	Delimited Field #	The delimited field number in the data file. Note: If using the GetDate() (or GetDate() + x days) function in the "Default Value" field, please leave the delimited field # empty.
	Add	Click this button to add the data to the grid below.

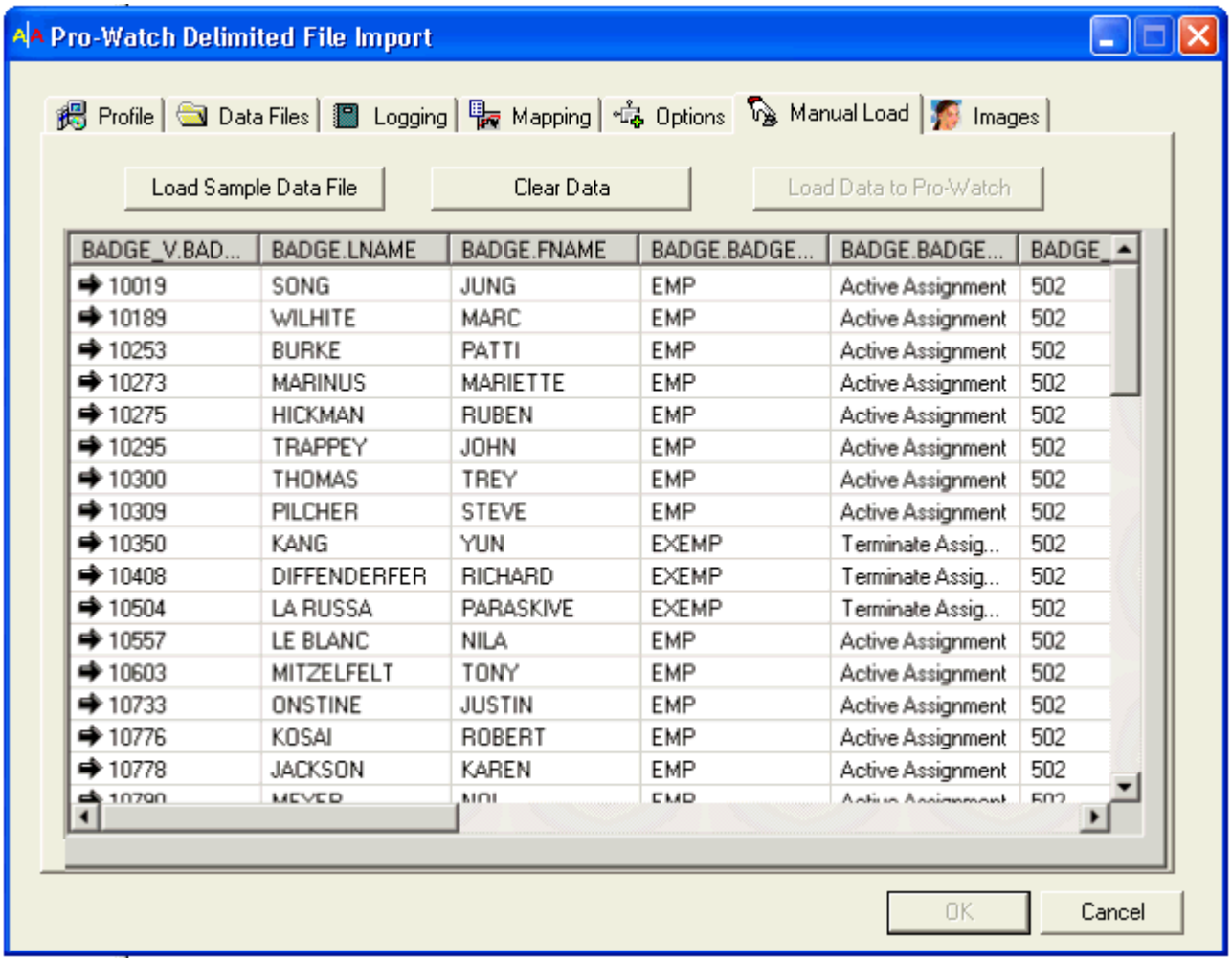
Tab	Field	Comments
Options tab (Return to Delimited "TAB LIST")	Profile Options	Download access changes to panels—Downloads card access changes to the panels when a new card is created, and when any of the following is changed on an existing card: card status, card company, expiration date, PIN code, issue level, or Clearance Code. Do not remove leading zeros from card numbers—Card numbers, by default in Pro-Watch, are stripped of their leading zeros. Checking this option preserves the leading zeros. Delete Badge Holder when column # ____ - _____ — Deletes a badge record when the value of column # "X" equals the value entered. This applies only to delimited profiles. For example, column #6 - DELETE in a delimited file removes the badge holder from the Pro-Watch database. This deletion is logged in the Pro-Watch Audit Log. Do not apply company Clearance Codes to cards—All cards are required to have a company, which is used to group multiple Clearance Codes. The default of the DTU is to apply all Clearance Codes of that company to the card. Checking this option prevents this default when a new card is added or an existing card company is modified. Host Grant Only Cards/Aircrew PINS—Applies to cards that do not get downloaded to the panel. Real-time processing (requires DTU Windows service)—Applies only to delimited profiles. Selecting this option instantly starts a DTU job whenever a file is dropped in a drop directory. If this Real Time DTU option is not selected, jobs are started at a specified scheduled time. Note that the Real Time DTU option requires the Pro-Watch DTU Windows service to be installed and running. To obtain this service, see your Honeywell representative.

Tab	Field	Comments
Options tab, continued	Date/Time Format	Specifies the format of the date and time. A blank field invokes a DateTimeParse, which is the default. Specifying a date invokes a DateTimeParseExact that uses the date/time given. Note that the Pro-Watch DTU requires dates to be specified in the mm/dd/yyyy format and hh:mm:ss formats. For example, enter “mm/dd/yyyy hh:mm:ss” if you want to export a date and time like “09/03/2003 12:45:03”. d—day of the month. Single-digit days have no leading zero. dd—day of the month. Single-digit days have a leading zero. ddd—abbreviated name of the day of the week, for example: "Sun.” dddd—full name of the day of the week, for example: "Sunday." M—numeric month. Single-digit months have no leading zero. MM—numeric month. Single-digit months have a leading zero. MMM—abbreviated name of the month, for example: "Jan." MMMM—full name of the month, for example: "January." y— year without the century. If the year is < 10, it has no leading zero. yy—year without the century. If the year is < 10, it has leading zero yyyy—year in four digits, including the century. gg— period or era. This pattern is ignored if the date to be formatted does not have an associated period or era string. h—hour in a 12-hour clock. Single-digit hours: no leading zero. hh—hour in a 12-hour clock. Single-digit hours: leading zero. H—hour in a 24-hour clock. Single-digit hours: no leading zero. HH—hour in a 24-hour clock. Single-digit hours: leading zero. m—minute. Single-digit minutes: no leading zero. mm— minute. Single-digit minutes: leading zero. s—second. Single-digit seconds: no leading zero. ss—second. Single-digit seconds: leading zero. f— fraction of a second, single-digit precision. Remaining digits cut. ff—fraction of a second, double-digit precision. Remaining digits cut. fff—fraction of a second, three-digit precision. Remaining digits cut. ffff—fraction of a second, four-digit precision. Remaining digits cut fffff—fraction of a second, five-digit precision. Remaining digits cut. ffffff—fraction of a second, six-digit precision. Remaining digits cut. fffffff—fraction of a second, seven-digit precision. Remaining digits cut. t—first character in the AM/PM designator defined in AMDesignator or PMDesignator, if any. tt—AM/PM designator defined in AMDesignator or PMDesignator. z—time zone offset ("+" or "-" followed by the hour only). Single-digit hours have no leading zero (e.g., Pacific Standard Time is "-8". zz—time zone offset ("+" or "-" followed by the hour only). Single-digit hours will have a leading zero (e.g., Pacific Standard Time is "-08"). zzz—full time zone offset ("+" or "-" followed by the hour and minutes). Single-digit hours and minutes have leading zeros. For example, Pacific Standard Time is "-08:00". :—default time separator defined in TimeSeparator. /—default date separator defined in DateSeparator.
Options tab, continued	Procedure Name	Specifies the name of the stored procedure that will run after each record is processed.

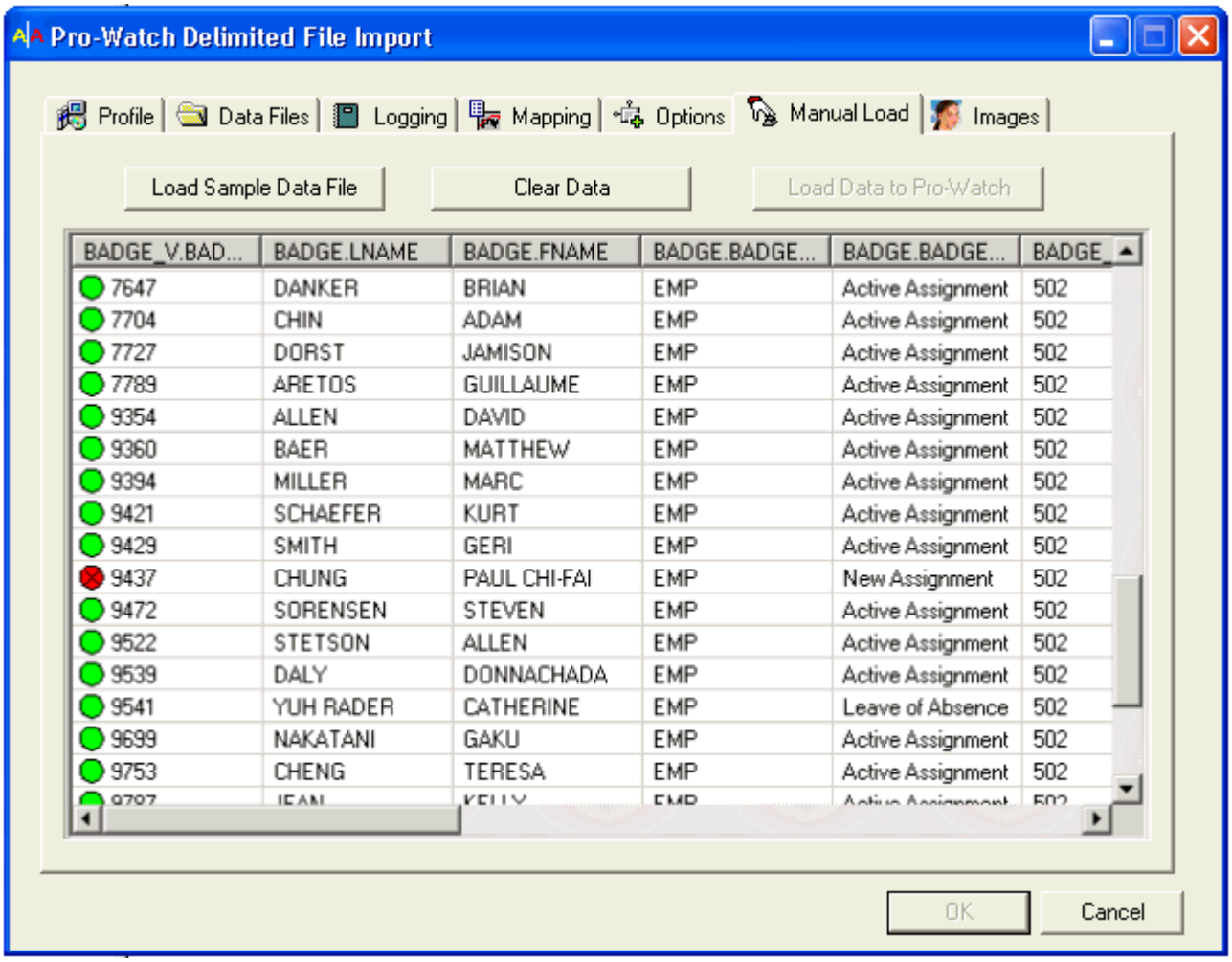
Tab	Field	Comments
Manual Load tab (Return to Delimited "TAB LIST")	Load Sample Data File	Click this button to load a sample data file manually. See "Manual Load Tab - Additional Information".
	Clear Data	Click this button to clear all the loaded sample data.
	Load Data to Pro-Watch	Click this button to load the sample data file to Pro-Watch. See "Manual Load Tab - Additional Information".
Images tab (Return to Delimited "TAB LIST")	Import Photos	Select this check box to import photos.
	Naming Column #	The column number in the delimited file that is used to name the images. Required field.
	Photo Import Extension	Select the image-file extension of the files you want to import.
	Import Directory	The directory address from which the image will be imported. Required field. Click the ellipsis (...) button to browse for a directory.
	Pro-Watch BLOB	Select a Pro-Watch BLOB from the drop-down list that will be used to import image to Pro-Watch. Required field.

Manual Load Tab - Additional Information

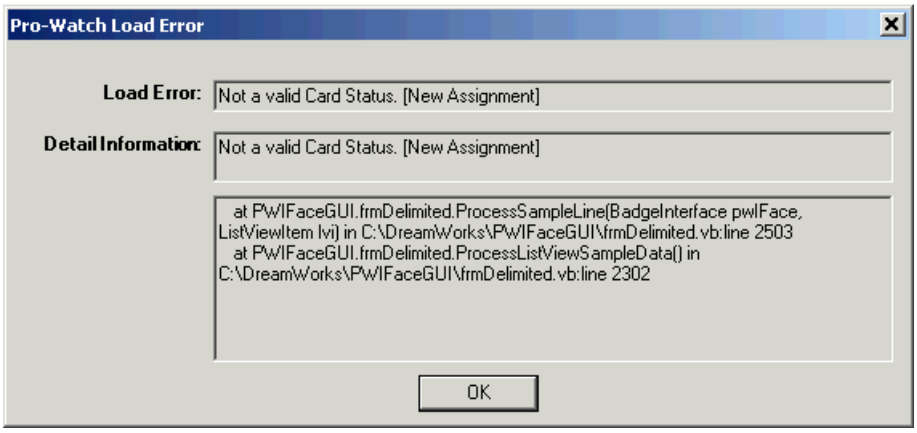
The Manual Load tab allows you to load a sample data file to Pro-Watch. After a sample data file is loaded, the icon for all rows appears as a black arrow:



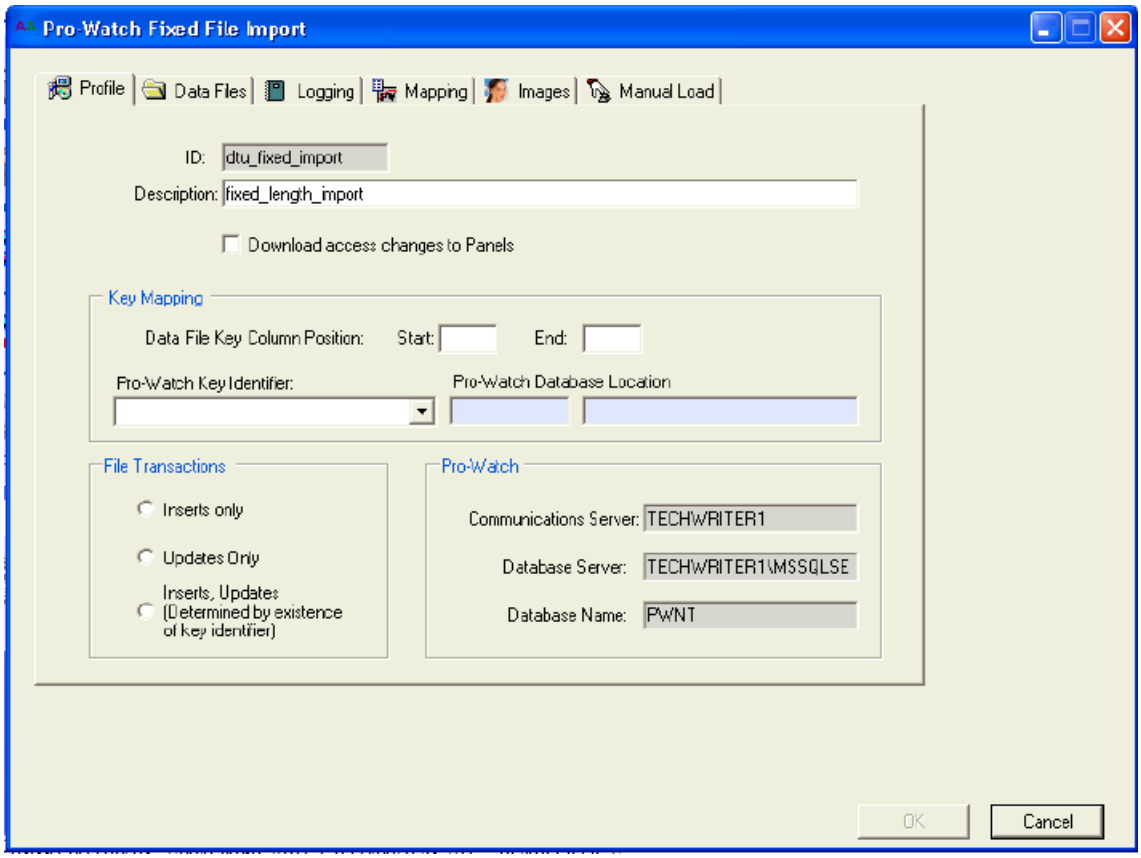
After the data is loaded, the icons change to a green circle if the sample data is loaded successfully to Pro-Watch, or a red circle if there was an error in loading the data:



Double-click on a row with a red circle that was not loaded to display the reason for the failure:



64.7.3 Editing a Fixed-Length Data Import Profile



Edit the following Fixed-Length Data Import fields as appropriate.

TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile".
- "Data files tab".

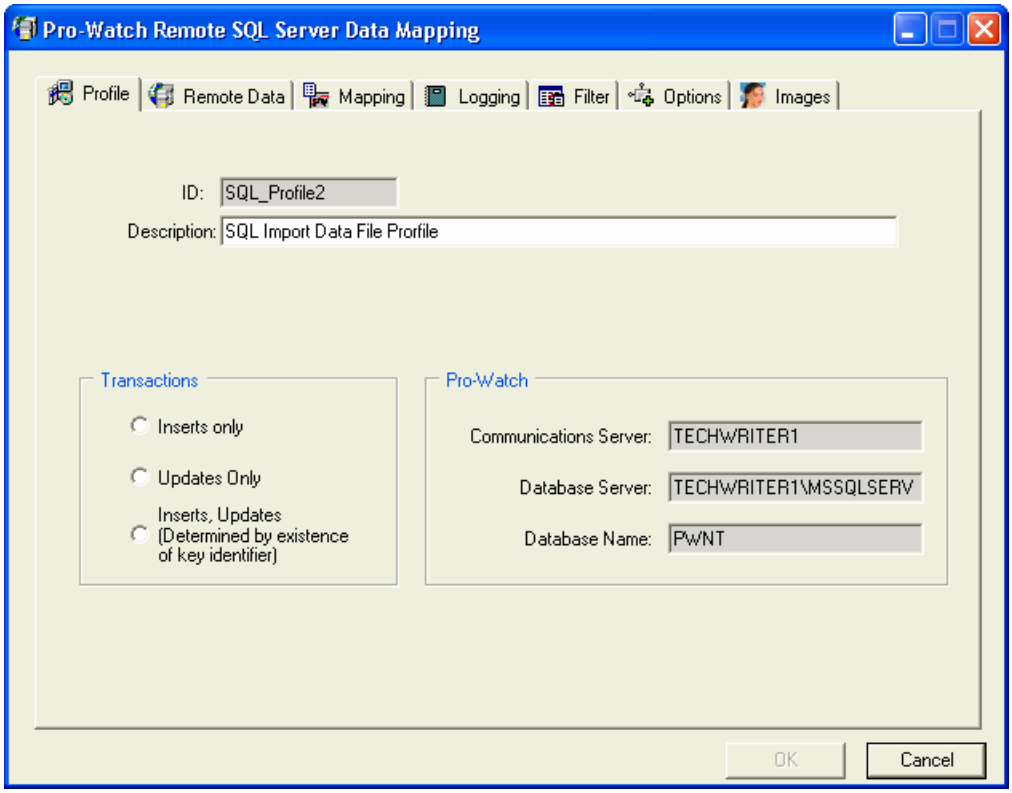
- "Logging tab".
- "Mapping tab".
- "Images tab".
- "Manual Load tab".

Tab	Field	Comments
Profile tab (Return to Fixed "TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.
	Description	Description of the profile. Required field.
	Download access changes to Panels	Select this check box to download the changes to the respective panels, only if access has changed.
	Data File Key Column Position	Enter the Start and End column numbers of the fixed-length key field. This is the unique key in the data file that identifies individuals in the external system. Required if transactions are “Updates Only” or “Updates, Inserts Only.”
	Pro-Watch Key Identifier	This is the Pro-Watch badging field that maintains the keys of the external system. This is used to determine if a record is an Update or Insertion.
	Pro-Watch Database Location	Read-only fields that are enabled when a Pro-Watch Key Identifier is entered. The first field displays the name of the database table and the second field displays the name of the database column in that table to which the data will be transferred by DTU.
	File Transactions	The type of transactions this profile contains. Required field. Select one of the following option buttons: Insert Only—If a “Data File Key Column #” is provided, the DTU will only insert a new badge record if the key column value is not found. An error will be displayed in the log file if an existing badge record is found. If no “Data File Key Column #” is provided, every record will be inserted into Pro-Watch. Updates Only—The DTU will use the “Data File Key Column #” to look for the matching Pro-Watch record. An error will be logged in the log file if the badge holder is not already in the Pro-Watch database. Inserts, Updates—The DTU will use the “Data File Key Column #” to look for the matching Pro-Watch record. If a matching record is not found, the DTU will insert the data. If a matching record is found, the record will be updated.
	Pro-Watch	Communications Server—The name of the Pro-Watch server to which the data will be loaded. Database Server—The name of the Pro-Watch database to which the data will be loaded. Database Name—Name of the database.

Tab	Field	Comments
Data files tab (Return to Fixed "TAB LIST")	Directory	Location of the fixed-length data source file. Required field. Click the ellipsis (...) button to browse for a directory.
	Option Buttons	Select one: Load all files in Directory—selecting this option will load all files specified in the data directory. Load only the file with the following name—selecting option will load a single file with the name specified. Load all files that match the following naming pattern—selecting this option will load all the files that match the specified naming pattern. Wildcard "*" and single character wildcard "?" can be used to specify a naming pattern.
	Archive file when finished processing	The directory where the file that was processed will be archived after the file has been loaded.
	Directory	Location of the archived file. Click the ellipsis (...) button to browse for a directory.
Logging tab (Return to Fixed "TAB LIST")	Generate Log File	Select this check box to generate a log file for scheduled data transfer sessions.
	Directory	Location of the log file. Click the ellipsis (...) button to browse for a directory.
	E-Mail Log File	Select this check box to e-mail the generated log file.
	SMTP Server	The name of the e-mail server which will e-mail the log file. Enabled if the e-mail check box is selected.
	From, To, CC	Enter the From, To and Copy e-mail addresses to be used when the log file is e-mailed. Enabled if the e-mail check box is selected.
Mapping tab (Return to Fixed "TAB LIST")	Pro-Watch Badging Field	Select a badge field from the drop-down list. Required field.

Tab	Field	Comments
	Pro-Watch Database Mapping	Read-only fields that are enabled when a Pro-Watch Badging Field is selected from the drop-down list. The first field displays the name of the database table and the second field displays the name of the database column in that table to which the Badging Field selected will be transferred by DTU.
	Default Value	If no data is supplied in the file, this value will be used to update or insert the badging record for the mapping value. If no “Delimited Field #” is defined, this value will always update the defined mapping value unless the “Apply Default to Inserts Only” is checked.
	Apply Default to Inserts Only	Select this check box to apply the “Default Value” when the transaction is an insert. This option will not overwrite the existing value by inserting the default value when updating a record.
	Fixed file position	The Start and End positions of the fixed-length record in the data file. Required field only if the “Default Value” is blank.
	Add	Click this button to add the data to the grid below.
Images tab (Return to Fixed "TAB LIST")	Import Photos	Select this check box to import JPG photos.
	Naming Column	The Start and End positions of the fixed-length image name in the data file. Required field.
	Import Directory	The directory address from which the image will be imported. Required field. Click the ellipsis (...) button to browse for a directory.
	Pro-Watch BLOB	Select a Pro-Watch BLOB from the drop-down list that will be used to import image to Pro-Watch. Required field.
Manual Load tab (Return to Fixed "TAB LIST")	Load Sample Data File	Click this button to load a sample data file manually. See "Manual Load Tab - Additional Information".
	Clear Data	Click this button to clear all the loaded sample data.
	Load Data to Pro-Watch	Click this button to load the sample data file to Pro-Watch. See "Manual Load Tab - Additional Information".

64.7.4 Editing an SQL Database Import Profile



Edit the following SQL Database Import fields as appropriate.

TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile Definition tab".
- "Remote Data Tab".
- "Data Mapping tab".
- "Logging tab".
- "Filter tab".
- "Options tab".
- "Images tab".

Tab	Field	Comments
Profile Definition tab (Return to SQL "TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.
	Description	Description of the profile. Required field.
	Transactions	The type of transactions this profile contains. Required field. Select one of the following option buttons: Insert Only—The DTU will only insert a new data record. Updates Only—The DTU will update the data record. An error will be logged in the log file if the record is not already in the Pro-Watch database. Inserts, Updates—The DTU will use the "Data File Key Column #" to look for the matching Pro-Watch record. If a matching record is not found, the DTU will insert the data. If a matching record is found, the record will be updated.
	Pro-Watch	Communications Server—The name of the Pro-Watch server to which the data will be loaded. Database Server—The name of the Pro-Watch database to which the data will be loaded. Database Name—Name of the database.
Remote Data Tab (Return to SQL "TAB LIST")	SQL Server Name	The name of the SQL server. After entering this and the Database Name, click Test Connection to make sure Pro-Watch is able to connect to the specified SQL database.
	Database Name	The name of the SQL database on the specified server. After entering this and the SQL Server Name, click Test Connection to make sure Pro-Watch is able to connect to the specified SQL database.
	Windows or SQL Server authentication	Select the Windows option button if the database is on your local machine. Select the SQL Server authentication option button if the database is on an external server. Then enter your Login Name and Password.
	Login Name	Your user ID required to connect to an external SQL database.

Tab	Field	Comments
	Password	Your password required to connect to an external SQL database.
	Table/View	Select a table or database view from the drop-down list. A view is a “virtual table” that is generated on the fly by pulling data from one or more tables when a user demands it.
	Get/Refresh Object Schema	Click this link to view the list of tables and views for the selected server and database.
	Remote Key Column	The key column in the remote data table that identifies each record uniquely. Select the name of this column from the drop-down list. When updating records, you need to set the remote key because Pro-Watch needs to know what field to use to determine if the importing data record is a new record or an existing record. The columns listed in the drop-down list are populated automatically from the table/view that is selected in a previous step from the database.
	Data Type/ Size	When you select a remote key column, its data type and size are displayed automatically in these view-only fields.
	Pro-Watch Key Identifier	This is the Pro-Watch data field that corresponds to the key column of the database from which you are importing records. Select one from the drop-down list. This is used to determine if a record is an Update or Insertion.
	Pro-Watch Database Location	Read-only fields that are enabled when a Pro-Watch Key Identifier is selected. The first field displays the name of the database table and the second field displays the name of the database column in that table to which the data will be transferred by DTU.
Data Mapping tab (Return to SQL "TAB LIST")	Pro-Watch Badging Field	Select a badge field from the drop-down list. Required field.
	Default Value	If no data is supplied in the file, this value will be used to update or insert the badging record for the mapping value. If no “Delimited Field #” is defined, this value will always update the defined mapping value unless the “Apply Default to Inserts Only” is checked.

Tab	Field	Comments
	Apply Default to Inserts Only	Select this check box to apply the “Default Value” when the transaction is an insert. This option will not overwrite the existing value by inserting the default value when updating a record.
	Table Column Data Type Size	Read-only SQL data import fields that are enabled and automatically populated when a Pro-Watch Badging Field is selected from the drop-down list. Table displays the name of the SQL database table. Column displays the database column in that table. Data Type and Size fields display the type and size of the data imported by DTU.
	Remote Column	The key column in the remote data table that identifies each record uniquely. Select the name of this column from the drop-down list.
	Data Type Size	The data type and size of the remote key column is populated automatically in these two fields.
	Add	Click this button to add the data record to the grid below under the following columns: Remote Column - The key column in the remote data table that identifies each record uniquely. Pro-Watch Description - The description of the column in Pro-Watch. Pro-Watch Table - The Pro-Watch table to which the record is imported. Pro-Watch Column - The name given to the same column in Pro-Watch. Default - The default value which, if no data is supplied, will be used to update or insert the badging record. Mapping Rules - See "Mapping Rules".
Logging tab (Return to SQL "TAB LIST")	Generate Log File	Select this check box to generate a log file for scheduled data transfer sessions.
	Directory	Location of the log file. Click the ellipsis (...) button to browse for a directory.
	E-Mail Log File	Select this check box to e-mail the generated log file.
	SMTP Server	The name of the e-mail server which will e-mail the log file. Enabled if the e-mail check box is selected.

Tab	Field	Comments
	From, To, CC	Enter the From, To and Copy e-mail addresses to be used when the log file is e-mailed. Enabled if the e-mail check box is selected.
Filter tab (Return to SQL "TAB LIST")	Remote Column	Click the drop-down list arrow to select a column to import from the remote database.
	Comparison	Click the drop-down list arrow to select a logical operator for comparing the value of the column to the selection criterion entered into the “Value” field (see below).
	Value	Enter the alphanumeric value that the Pro-Watch will use to compare and filter the remote column according to the logical operator selected in the Comparison field (see above).
	Add/Delete	Adds or deletes the filters highlighted in the window.
Options tab (Return to SQL "TAB LIST")	Download access changes to panels	Downloads card access changes to the panels when a new card is created, and when any of the following is changed on an existing card: card status, card company, expiration date, PIN code, issue level, or Clearance Code.
	Procedure Name	Specifies the name of the stored procedure that will run after each record is processed.
Images tab (Return to SQL "TAB LIST")	Import Photos	Select this check box to import photos.
	Photo Import Extension	Select the image-file extension of the files you want to import.
	Naming Column	Select from the drop-down list the name (the badge field) you want to assign to the imported photo.
	Import Directory	The directory address from which the image will be imported. Required field. Click the ellipsis (...) button to browse for a directory.
	Pro-Watch BLOB	Select a Pro-Watch BLOB from the drop-down list that will be used to import image to Pro-Watch. Required field.
	Import Signatures	Select this checkbox to import signatures.

Tab	Field	Comments
	Signature Import Extension	Select the image-file extension of the signature files you want to import.
	Naming Column	Select from the drop-down list the name (the badge field) you want to assign to the imported photo.
	Import Directory	The directory address from which the image will be imported. Required field. Click the ellipsis (...) button to browse for a directory.
	Pro-Watch BLOB	Select a Pro-Watch BLOB from the drop-down list that will be used to import image to Pro-Watch. Required field.

Mapping Rules

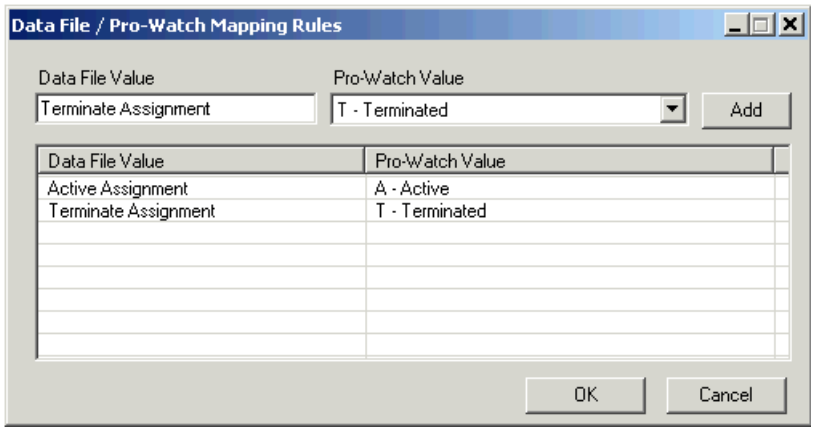
Mapping rules determine how each column value in the external database will be converted into a Pro-Watch column value.

Examples:

- One mapping rule could be "whenever you see the value '123' for Department_ID, map it as 'Human Resources' when importing the record into Pro-Watch."
- Another mapping rule could be: "whenever you see the value 'Terminated' for Employee-Status, map it as 'T' when importing the record into Pro-Watch."

To define a mapping rule:

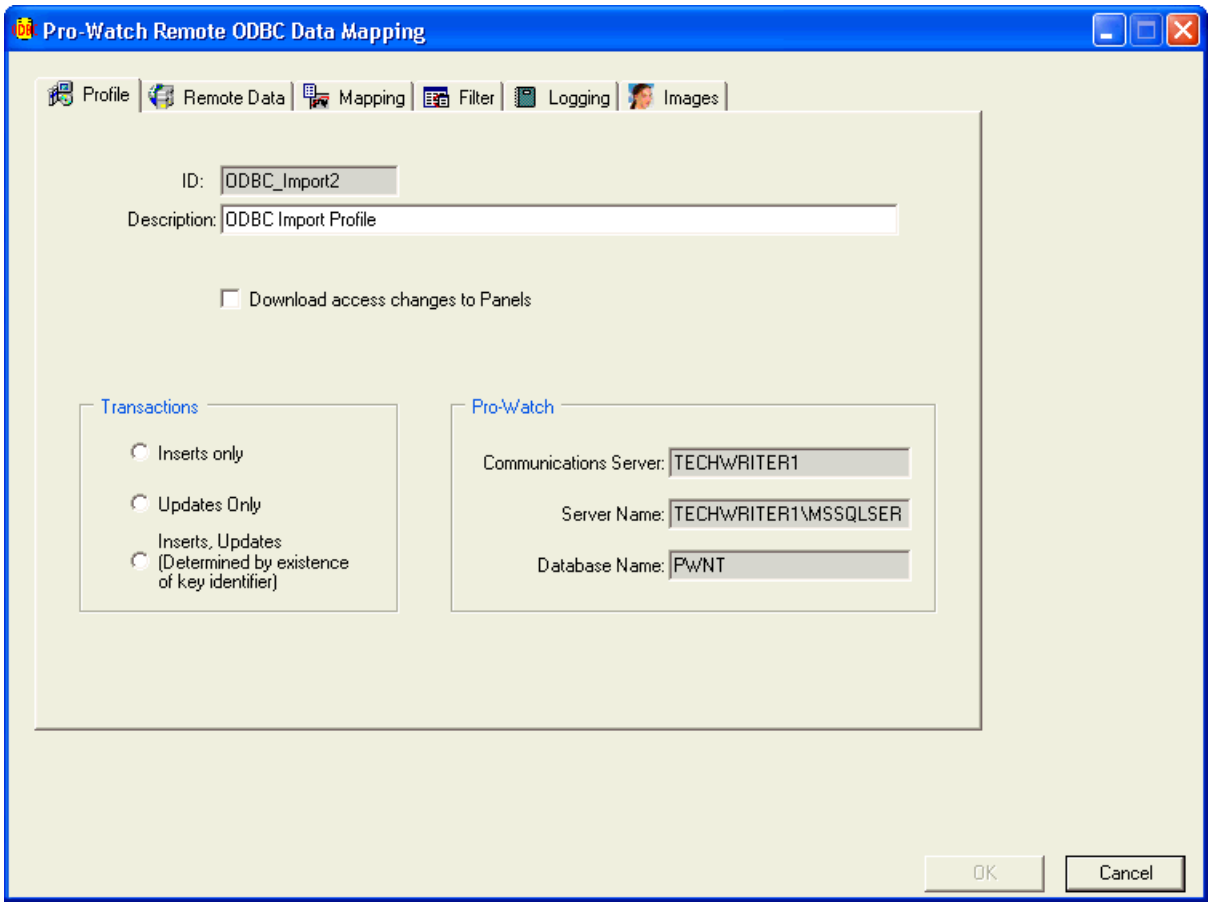
1. In the Data Mapping tab grid, right-click **a mapping row**.
2. Select **Edit Mapping Rules** from the pop-up menu to display Data File/Pro-Watch Mapping Rules dialog box:



3. Enter each **Data File Value** (the value of the variable in the external database) with its corresponding **Pro-Watch Value**.
4. After you have entered all the corresponding mapping pairs, click **OK** to return to the Data Mapping tag.

   The Mapping Rules column will display the number of rules you have defined, e.g., “1 rule,” “2 rules” etc.

64.7.5 Editing an ODBC Database Import Profile



Edit the following ODBC Database Import fields as appropriate.

TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile tab".
- "Remote Data Tab".
- "Data Mapping tab".
- "Filter tab".
- "Logging tab".

- "Images tab".

Tab	Field	Comments
Profile tab (Return to ODBC Import "TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.
	Description	Description of the profile. Required field.
	Download access changes to Panels	Select this check box to download the changes to the respective panels, only if access has changed.
	Transactions	The type of file transactions this profile contains. Required field. Select one of the following option buttons: Insert Only—The DTU will only insert a new data record. Updates Only—The DTU will update the data record. An error will be logged in the log file if the record is not already in the Pro-Watch database. Inserts, Updates—The DTU will use the "Data File Key Column #" to look for the matching Pro-Watch record. If a matching record is not found, the DTU will insert the data. If a matching record is found, the record will be updated.
	Communications Server	The name of the Pro-Watch server to which the data will be loaded.
	Server Name	The name of the Pro-Watch database to which the data will be loaded.
	Database Name	Name of the database.
Remote Data Tab (Return to ODBC Import "TAB LIST")	Data Source Name (DSN)	The name of the ODBC data server. Select one from the drop-down list. server. After making your selection, click Test Connection to make sure Pro-Watch is able to connect to the specified ODBC data source.
	User ID	ID of the user.
	Password	Password of the user.

Tab	Field	Comments
	Remote Table/View	The name of the ODBC database table or view on the specified server. A view is a "virtual table" that is generated on the fly by pulling data from one or more tables when a user demands it.
	Get/Refesh Object Schema	Click this link to view the list of tables and views for the selected server and database.
	Remote Key Column	The key column in the remote data table that identifies each record uniquely. Select the name of this column from the drop-down list. When updating records, you need to set the remote key because Pro-Watch needs to know what field to use to determine if the importing data record is a new record or an existing record. The columns listed in the drop-down list are populated automatically from the table/view that is selected in a previous step from the database.
	Data Type Size	When you select a remote key column, its data type and size are displayed automatically in these view-only fields.
	Pro-Watch Key Identifier	This is the Pro-Watch data field that maintains the keys of the external system. Select one from the drop-down list. This is used to determine if a record is an Update or Insertion.
	Pro-Watch Database Location	Read-only fields that are enabled when a Pro-Watch Key Identifier is selected. The first field displays the name of the database table and the second field displays the name of the database column in that table to which the data will be transferred by DTU.
Data Mapping tab (Return to ODBC Import "TAB LIST")	Pro-Watch Badging Field	Select a badge field from the drop-down list. Required field.
	Default	If no data is supplied in the file, this value will be used to update or insert the badging record for the mapping value. If no "Delimited Field #" is defined, this value will always update the defined mapping value unless the "Apply Default to Inserts Only" is checked.

Tab	Field	Comments
	Apply Default to Inserts Only	Select this check box to apply the “Default Value” when the transaction is an insert. This option will not overwrite the existing value by inserting the default value when updating a record.
	Table Column Data Type Size	Read-only SQL data import fields that are enabled and automatically populated when a Pro-Watch Badging Field is selected from the drop-down list. Table displays the name of the SQL database table. Column displays the database column in that table. Data Type and Size fields display the type and size of the data imported by DTU.
	Remote Column	Name of the badging column on the remote database table. Select one from the drop-down menu.
	Data Type Size	When you select a remote badging column, its data type and size are displayed automatically in these view-only fields.
	Add	Click this button to add the data mapping statement to the grid below under the following columns: Remote Column—The key column in the remote data table that identifies each record uniquely. Pro-Watch Description—The description of the column in Pro-Watch. Pro-Watch Table—The Pro-Watch table to which the record is imported. Pro-Watch Column—The name given to the same column in Pro-Watch. Default—The default value which, if no data is supplied, will be used to update or insert the badging record. Mapping Rules—See "ODBC Import Mapping Rules".
	Delete	Click Delete to delete the selected data mapping statement from the grid below.
Filter tab (Return to ODBC Import "TAB LIST")	Remote Column	Click the drop-down list arrow to select a column to import from the remote database.
	Comparison	Click the drop-down list arrow to select a logical operator for comparing the value of the column to the selection criterion entered into the “Value” field (see below).

Tab	Field	Comments
	Value	Enter the alphanumeric value that the Pro-Watch will use to compare and filter the remote column according to the logical operator selected in the Comparison field (see above).
	And / Or	Select either the And or the Or option button to combine multiple filtering statements to filter a remote column.
	Add	Click Add to add the filtering statements to the grid under the following columns: Remote Column - The key column in the remote data table that identifies each record uniquely. Comparison - The logical operator used to filter the data record from the remote data table. Value - The value according to which the data record will be filtered from the remote data table and imported into Pro-Watch. And/Or - The logical operator that concatenates multiple filtering statements.
	Delete	Click Delete to delete a selected filtering statement from the grid.
Logging tab (Return to ODBC Import "TAB LIST")	Generate Log File	Select this check box to generate a log file for scheduled data transfer sessions.
	Directory	Location of the log file. Click the ellipsis (...) button to browse for a directory.
	E-Mail Log File	Select this check box to e-mail the generated log file.
	SMTP Server	The name of the e-mail server which will e-mail the log file. Enabled if the e-mail check box is selected.
	From, To, CC	Enter the From, To and Copy e-mail addresses to be used when the log file is e-mailed. Enabled if the e-mail check box is selected.
Images tab (Return to ODBC Import "TAB LIST")	Import Photos	Select this check box to import photos.
	Photo Import Extension	Select the image-file extension by which you want to filter.

Tab	Field	Comments
	Naming Column	Select from the drop-down list the name (the badge field) you want to assign to the imported photo.
	Import Directory	The directory address from which the image will be imported. Required field. Click the ellipsis (...) button to browse for a directory.
	Pro-Watch BLOB	Select a Pro-Watch BLOB from the drop-down list that will be used to import image to Pro-Watch. Required field.

64.8 ODBC Import Mapping Rules

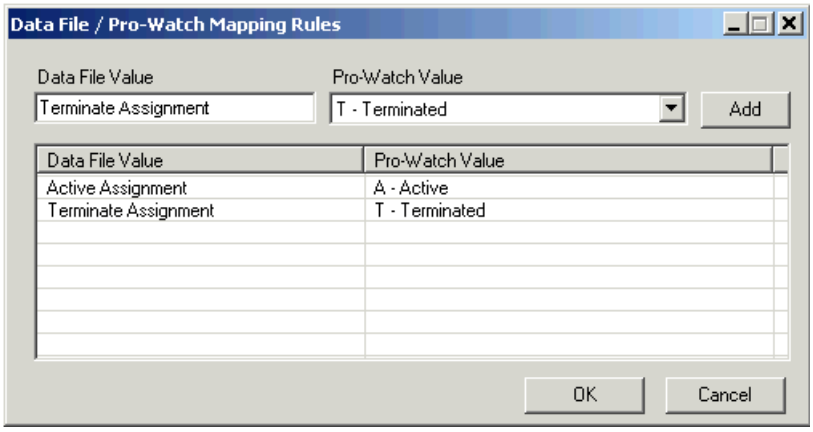
Mapping rules in this context determine how each column value in the external database will be converted into a Pro-Watch column value.

Examples:

- One mapping rule could be "whenever you see the value '123' for Department_ID, map it as 'Human Resources' when importing the record into Pro-Watch."
- Another mapping rule could be: "whenever you see the value 'Terminated' for Employee-Status, map it as 'T' when importing the record into Pro-Watch."

To define a mapping rule:

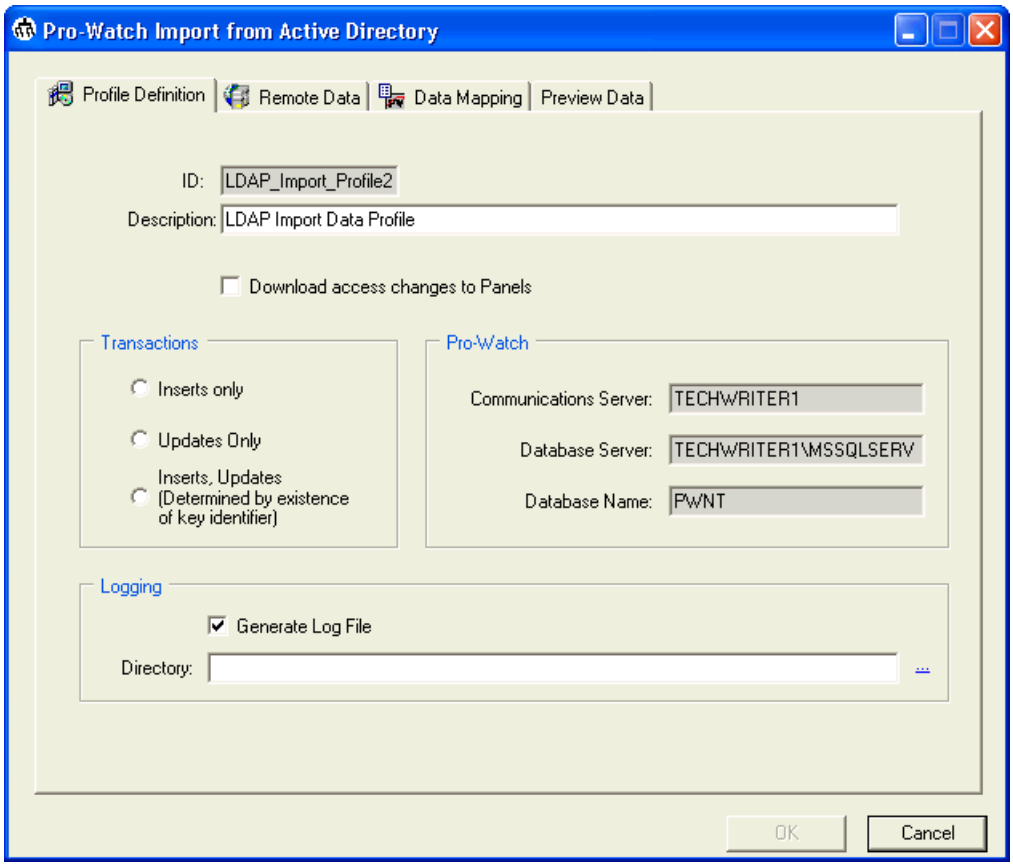
1. In the Data Mapping tab grid, right-click **a mapping row**.
2. Select **Edit Mapping Rules** from the po-up menu to display Data File/Pro-Watch Mapping Rules dialog box:



3. Enter each **Data File Value** (the value of the variable in the external database) with its corresponding **Pro-Watch Value**.
4. After you have entered all the corresponding mapping pairs, click OK to return to the Data Mapping tag.

The Mapping Rules column will display the number of rules you have defined, e.g., “1 rule,” “2 rules” etc.

64.8.1 Editing an LDAP Database Import Profile



Edit the following LDAP Database Import fields as appropriate.

LDAP TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile Definition tab".
- "Remote Data Tab".
- "Data Mapping tab".
- "Preview Data tab".

Tab	Field	Comments
Profile Definition tab (Return to "LDAP TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.
	Description	Description of the profile. Required field.
	Download access changes to Panels	Select this check box to download the changes to the respective panels, only if access has changed.
	Transactions	The type of file transactions this profile contains. Required field. Select one of the following option buttons: Inserts Only—The DTU will only insert a new data record. Updates Only—The DTU will update the data record. An error will be logged in the log file if the record is not already in the Pro-Watch database. Inserts, Updates—The DTU will use the “Data File Key Column #” to look for the matching Pro-Watch record. If a matching record is not found, the DTU will insert the data. If a matching record is found, the record will be updated.
	Communications Server	The name of the Pro-Watch server to which the data will be loaded.
	Database Server	The name of the Pro-Watch database to which the data will be loaded.
	Database Name	Name of the database.
	Generate Log File	Select this check box to generate a log file for scheduled data transfer sessions.
	Directory	Location of the log file. Click the ellipsis (...) button to browse for a directory.
Remote Data Tab (Return to "LDAP TAB LIST")	LDAP Server Name	Name of the LDAP server machine.

Tab	Field	Comments
	Login Name	Enter a valid login ID for the LDAP server machine.
	Password	Enter a valid password for the login ID entered.
	Test Connection	Click to test a successful login to the server machine.
	LDAP Class	Select the LDAP class of the remote object.
	LADP Container	Select one from the drop-down list. All the “children” of an “entry” (i.e. stored LDAP object) are siblings and are said to reside in the same container.
	Remote Key Column	The key column in the remote data table is the column that identifies each record uniquely. Select the name of this column from the drop-down list. When updating records, you need to set the remote key because Pro-Watch needs to know what field to use to determine if the importing data record is a new record or an existing record. The columns listed in the drop-down list are populated automatically from the table/view that is selected in a previous step from the database.
	Data Type Size	When you select a remote key column, its data type and size are displayed automatically in these view-only fields.
	Pro-Watch Key Identifier	This is the Pro-Watch data field that maintains the keys of the external system. Select one from the drop-down list. This is used to determine if a record is an Update or Insertion.
	Pro-Watch Database Location	Read-only fields that are enabled when a Pro-Watch Key Identifier is selected. The first field displays the name of the database table and the second field displays the name of the database column in that table to which the data will be transferred by DTU.
Data Mapping tab (Return to "LDAP TAB LIST")	Pro-Watch Badging Field	Select a badge field from the drop-down list. Required field.

Tab	Field	Comments
	Default	If no data is supplied in the file, this default value will be used to update or insert the badging record for the mapping value. If no "Delimited Field #" is defined, this value will always update the defined mapping value unless the "Apply Default to Inserts Only" is checked.
	Apply Default to Inserts Only	Select this check box to apply the "Default Value" when the transaction is an insert. This option will not overwrite the existing value by inserting the default value when updating a record.
	Table Column Data Type Size	Read-only SQL data import fields that are enabled and automatically populated when a Pro-Watch Badging Field is selected from the drop-down list. Table displays the name of the SQL database table. Column displays the database column in that table. Data Type and Size fields display the type and size of the data imported by DTU.
	Remote Column	Name of the badging column on the remote database table. Select one from the drop-down menu.
	Data Type Size	When you select a remote badging column, its data type and size are displayed automatically in these view-only fields.
	Add	Click this button to add the data record to the grid below under the following columns: Remote Column—The key column in the remote data table that identifies each record uniquely. Pro-Watch Description—The description of the column in Pro-Watch. Pro-Watch Table—The Pro-Watch table to which the record is imported. Pro-Watch Column—The name given to the same column in Pro-Watch. Default—The default value which, if no data is supplied, will be used to update or insert the badging record. Mapping Rules—See "Mapping Rules".
Preview Data tab (Return to "LDAP TAB LIST")	Load Sample LDAP Data	Loads the selected data in the window.
	Clear Data	Clears the desired data.

Tab	Field	Comments
	Rows to Display	Specifies the number of rows of data to display in the window.

Mapping Rules

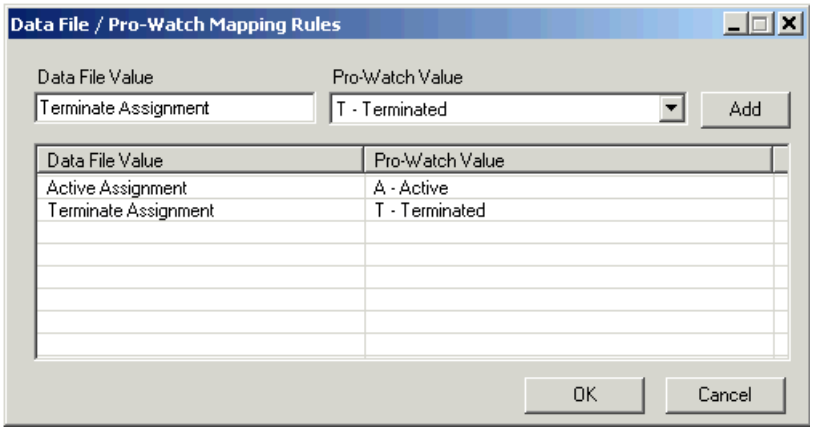
Mapping rules determine how each column value in the external database will be converted into a Pro-Watch column value.

Examples:

- One mapping rule could be "whenever you see the value '123' for Department_ID, map it as 'Human Resources' when importing the record into Pro-Watch."
- Another mapping rule could be: "whenever you see the value 'Terminated' for Employee-Status, map it as 'T' when importing the record into Pro-Watch."

To define a mapping rule:

1. In the Data Mapping tab grid, right-click **a mapping row**.
2. Select **Edit Mapping Rules** from the po-up menu to display Data File/Pro-Watch Mapping Rules dialog box:



3. Enter each **Data File Value** (the value of the variable in the external database) with its corresponding **Pro-Watch Value**.
4. After you have entered all the corresponding mapping pairs, click OK to return to the Data Mapping tag.

The Mapping Rules column will display the number of rules you have defined, e.g., “1 rule,” “2 rules,” etc.

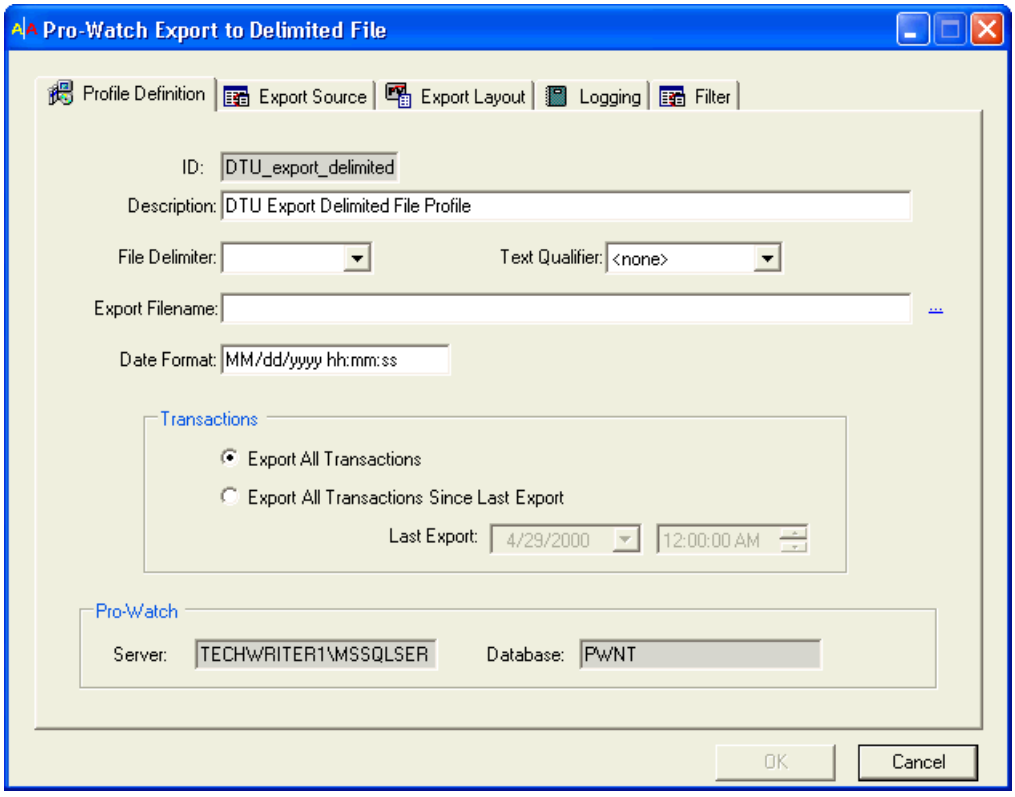
64.8.2 Why Export Pro-Watch Data?

Many companies use data exports to synchronize Pro-Watch with other systems that interact with Pro-Watch.

Examples:

- A university may use the same card both to grant physical access to the campus buildings and provide meal services at the cafeteria. When such a multi-purpose card gets lost and a new one is issued, you have to make the necessary deletions and additions both in the physical access (Pro-Watch) and the meal/cafeteria databases. Such synchronization is easily accomplished by making the necessary edits in Pro-Watch and then exporting the edited data to the external database (e.g., meal/cafeteria).
- When a company is publishing a web directory of employees, they may want to include only those employees with specific access profiles. This can be accomplished easily by exporting the Pro-Watch data to the web directory database.

64.8.3 Editing a Delimited Data Export Profile



Edit the following Delimited Database Export fields as appropriate.

TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile Definition tab".
- "Export Source tab".
- "Export Layout tab".
- "Logging tab".
- "Filter tab".

Tab	Field	Comments
Profile Definition tab (Return to Delimited Export "TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.
	Description	Description of the profile. Required field.
	File Delimiter	The text character that separates the data fields in the data file. Required field. Either enter one or more alphanumeric characters as a delimiter or click the down arrow and select one of the following delimiters from the drop-down menu: I-Vertical Bar. Comma. Tab.
	Export Filename	Enter the name of the file to be exported. Click the ellipsis (...) button to browse for the file.

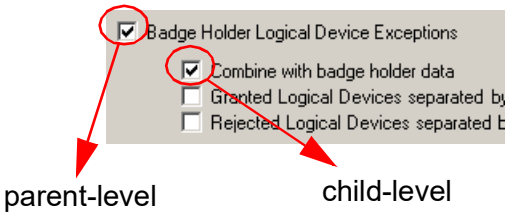
Tab	Field	Comments
Profile Definition tab, continued	Date Format	Enter the format in which you want to export date data. For example, enter “mm/dd/yyyy hh:mm:ss” if you want to export a date and time like “09/03/2003 12:45:03”. Note that the Pro-Watch DTU requires dates to be specified in the mm/dd/yyyy format, and time in the hh:mm:ss format. d—day of the month. Single-digit days have no leading zero. dd—day of the month. Single-digit days have a leading zero. ddd—abbreviated name of the day of the week, for example: "Sun.” dddd—full name of the day of the week, for example: "Sunday." M—numeric month. Single-digit months have no leading zero. MM—numeric month. Single-digit months have a leading zero. MMM—abbreviated name of the month, for example: "Jan." MMMM—full name of the month, for example: "January." y— year without the century. If the year is < 10, it has no leading zero. yy—year without the century. If the year is < 10, it has leading zero yyyy—year in four digits, including the century. gg— period or era. This pattern is ignored if the date to be formatted does not have an associated period or era string. h—hour in a 12-hour clock. Single-digit hours: no leading zero. hh—hour in a 12-hour clock. Single-digit hours: leading zero. H—hour in a 24-hour clock. Single-digit hours: no leading zero. HH—hour in a 24-hour clock. Single-digit hours: leading zero. m—minute. Single-digit minutes: no leading zero. mm— minute. Single-digit minutes: leading zero. s—second. Single-digit seconds: no leading zero. ss—second. Single-digit seconds: leading zero. f— fraction of a second, single-digit precision. Remaining digits cut. ff—fraction of a second, double-digit precision. Remaining digits cut. fff—fraction of a second, three-digit precision. Remaining digits cut. ffff—fraction of a second, four-digit precision. Remaining digits cut fffff—fraction of a second, five-digit precision. Remaining digits cut. ffffff—fraction of a second, six-digit precision. Remaining digits cut. fffffff—fraction of a second, seven-digit precision. Remaining digits cut. t—first character in the AM/PM designator defined in AMDesignator or PMDesignator, if any. tt—AM/PM designator defined in AMDesignator or PMDesignator. z—time zone offset ("+" or "-" followed by the hour only). Single-digit hours have no leading zero (e.g., Pacific Standard Time is "-8". zz—time zone offset ("+" or "-" followed by the hour only). Single-digit hours will have a leading zero (e.g., Pacific Standard Time is "-08"). zzz—full time zone offset ("+" or "-" followed by the hour and minutes). Single-digit hours and minutes have leading zeros. For example, Pacific Standard Time is "-08:00". :—default time separator defined in TimeSeparator. /—default date separator defined in DateSeparator.

Tab	Field	Comments
	Transactions	Export All Transactions—Exports all transactions defined in the profile. Export All Transactions Since Last Export—Exports only the transactions defined in the profile that occurred since the last transaction export.
	Pro-Watch Server	The name of the Pro-Watch server from which you want to export.
	Pro-Watch Database	The name of the Pro-Watch database from which you want to export.
Export Source tab (Return to Delimited Export "TAB LIST")	Badge Holder Data	Select this check box to export the fields of the badging profile data, separated by delimiters. **Note:** This check box is always selected by default and cannot be cleared.
	Badge Holder Card Data	Select this check box to export the badge holder card data. Select one of the associated options buttons to either: combine this data with the badge holder data, or add the clearance code data after the badge data and separate the two by a delimiter. **Note:** If a user has more than one card, then there will be a separate data group exported per card, for the same user.
	Badge Holder Clearance Codes	Select this check box if you want to export the badge holder clearance codes together with the badge profile data, separated by delimiters. **Note:** Selecting this check box **disables** the Badge Holder Events check box since it is not possible to determine a unique clearance code from event data (i.e. the data from the doors and the readers with which the user interacts). That would be possible only if every card was assigned a single clearance code but that is not the case. In Pro-Watch you can assign multiple clearance codes to a single card.
	Badge Holder Logical Device Exceptions	See "Logical Device Data check Boxes". **Note:** Selecting this check box **enables** the child-level check boxes and **disables** the Badge Holder Events check box.
	Badge Holder Events	Select this check box to export the badge holder events (i.e., door and reader) data. **Note:** Selecting this check box **disables** the Badge Holder Clearance Codes and Badge Holder Logical Device Exceptions check boxes, and **selects** the Badge Holder Card Data check box.
	Minutes Back From Date	If you selected “Export All Transactions Since Last Export” in the Profile Definition tab, you have also entered the date and time of the last export. To avoid missing the export of any transactions that might have occurred during the exact time the DTU was running the last export, enter in the Minutes Back From Date toggle box a number of minutes preceding the date and time you entered in the Profile Definition tab. This instructs the DTU to export the transactions that occurred during those minutes, including the exact time the DTU was running during the last export.

Tab	Field	Comments
Export Layout tab (Return to Delimited Export "TAB LIST")		This is the tab where the user can specify the exact order in which the data fields will be exported. **Note:** The categories in the left pane are determined by the choices you make in the **Export Source tab**. For example, the "Transaction Data" category will appear here only if you have selected the "Badge Holder Events" check box in the Export Source tab. Click the plus "+" signs next to the category headings in the left pane. Select the individual fields you want by clicking on them. Click the Right arrow to move the selected field(s) to the right pane. Use the Up and Move arrows to change the field(s)'s relative position in the data line. Top fields are exported first. To delete an expression from the right pane, right-click on its row and then select "Delete Definition" from the pop-up menu.
Logging tab (Return to Delimited Export "TAB LIST")	Generate Log File	Select this check box to generate a log file for the data export procedure.
	Directory	Enter a directory path for the log file or click the "..." button to browse for a directory.
	E-Mail Log File	Select this check box to e-mail the log file.
	SMTP Server	Enter the name of the e-mail server. If the SMTP Server is not set, enter the name of the local SMTP server.
	From/To/CC	Enter: Your e-mail address (From). The e-mail address of the log file's recipient (To). The e-mail address of the party who will receive a copy of the log file (CC).
Filter tab (Return to Delimited Export "TAB LIST")	Pro-Watch Badging Field	Click the drop-down list arrow to select a badging field to filter from the Pro-Watch database.
	Comparison	Click the drop-down list arrow to select a logical operator for comparing the value of the Pro-Watch field to the selection criterion entered into in the "Value" field (see below).
	Value	Enter the alphanumeric value that the Pro-Watch will use to compare and filter the remote column according to the logical operator selected in the Comparison field (see above).
	And/Or	Select either the And or the Or option button to combine multiple filtering statements to filter a Pro-Watch column.

Tab	Field	Comments
	Add	Click Add to add the filtering statements to the grid under the following columns: Pro-Watch Column - The key column in the Pro-Watch data table that identifies each record uniquely. Comparison - The logical operator used to filter the data record from the remote data table. Value - The value according to which the data record will be filtered from the Pro-Watch data table and exported to the remote database. And/Or - The logical operator that concatenates multiple filtering statements.
	Delete	Click Delete to delete a selected filtering statement from the grid.

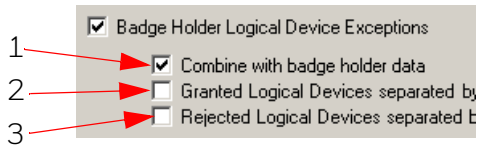
64.8.4 Logical Device Data check Boxes



1. Select the parent-level check box “Badge Holder Logical Device Exceptions” to enable the three child-level check boxes within this group:
   - Combine with badge holder data.
   - Granted Logical Devices separated by delimiter on line after badge data.

Note: Rejected Logical Devices separated by delimiter on line after badge data.

The first child-level check box and the other two are mutually exclusive.



- If you select 1, you cannot select 2 or 3 (although both look enabled).
- If you select either 2 or 3, you cannot select 1 (although it looks enabled).

2. Select the first child-level check box, “Combine with badge holder data,” to combine the badge holder data with both the “granted” and “rejected” logical device data, separated by delimiters.

   Example:

Joe Brown | Door 1 | R | 1234 | Building 1 | etc.

Joe Brown | Door 2 | G | 1234 | Building 1 | etc.

Carol May | Door 1 | G | 468 | Building 2 | etc.

Roy Smith | Door 2 | R | 345 | Building 3 | etc.

3. Select the second child-level check box, **"**Granted Logical Devices separated by delimiter on line after badge data," to combine the badge holder data with the "granted" logical device data on different lines, separated by delimiters.

   Example:

   Joe Brown | 1234

   Building 1 | Building 2

   Door 1 | Door 2 | etc.

   Carol May | 258

   Building 1 | Building 3

   Door 1 | Door 2 | Door 3 | etc.

4. Select the third child-level check box, **"**Rejected Logical Devices separated by delimiter on line after badge data," to combine the badge holder data with the "rejected" logical device data on different lines, separated by delimiters.

   Example:

   Joe Brown | 1234

   Building 1 | Building 2

   Door 1 | Door 2 | etc.

   Carol May | 258

   Building 1 | Building 3

   Door 1 | Door 2 | Door 3 | etc.

5. If you select both the second and third child-level check boxes the granted data will be on the second line and the rejected data on the third line.

Example:

Joe Brown | 1234

Door 1 | Door 2 ... [Granted data]

Door 4 | Door 5 ... [Rejected data]

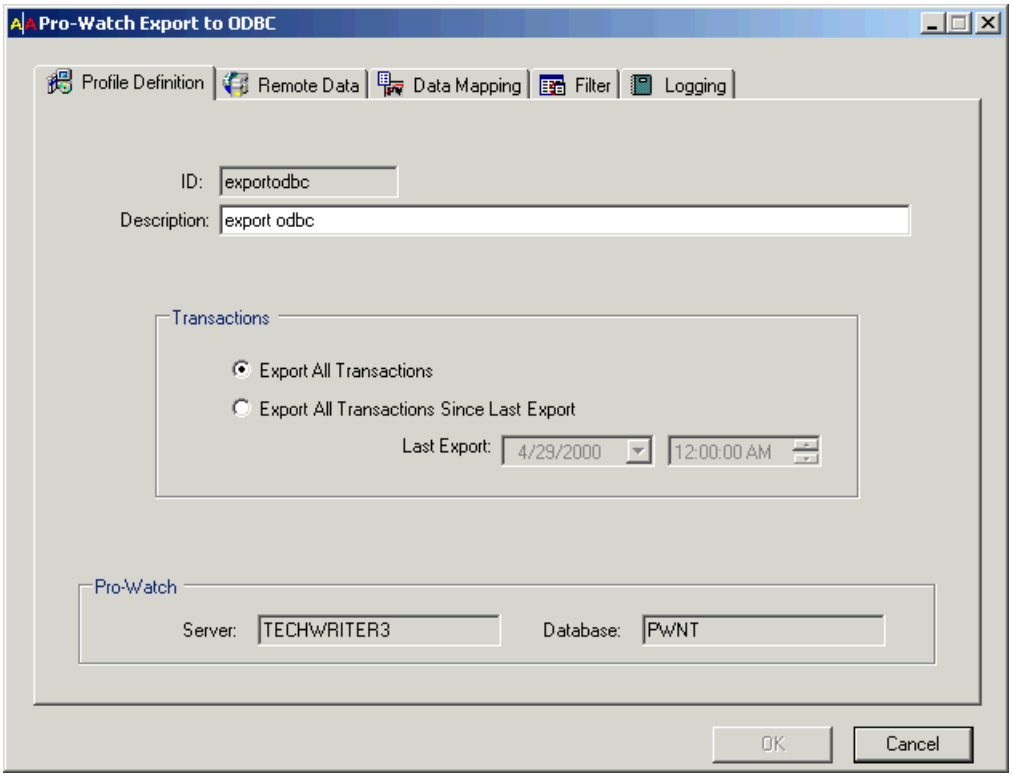
Carol May | 258

Door 8 ... [Granted data]

Door 1 | Door 2 | Door 3 ... [Rejected data]

Note: Exporting data through selecting the first child-level check box is the fastest method. Exporting through checking the second, third or both child-level check boxes will take longer due to the longer database search involved.

64.8.5 Editing an ODBC Database Export Profile



Edit the following ODBC Database Export fields as appropriate.

TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile Definition tab".
- "Remote Data tab".
- "Data Mapping tab".
- "Filter tab".
- "Logging tab".

Tab	Field	Comments
Profile Definition tab (Return to ODBC Export "TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.
	Description	Description of the profile. Required field.
	Export All Transactions	Select this option box to export all Pro-Watch records that satisfy the filtering criteria.
	Export All Transactions Since Last Export	Select this option box to export all updated Pro-Watch records that satisfy the filtering criteria and were not exported during the last exporting session. **Note:** You must have Audit Log In feature turned on to export the updated records. See "Audit Log In".
	Last Export	Select from the drop-down lists the date and time of the last exporting session.
	Pro-Watch Server	The name of the Pro-Watch server from which you want to export.
	Pro-Watch Database	The name of the Pro-Watch database from which you want to export.
Remote Data tab (Return to ODBC Export "TAB LIST")	Data Source Name (DSN)	Enter the name of the export data source or select one from the drop-down list. Click Test Connection to verify the connection.
	User ID	Enter your user ID.
	Password	Enter your password.
	Remote Table/View	The name of the ODBC database table or view on the specified server. A view is a "virtual table" that is generated on the fly by pulling data from one or more tables when a user demands it.
	Get Object Schema	Click this link to view the list of tables and views for the selected server and database.

Tab	Field	Comments
	Badge Holder Data	Select this check box to export the fields of the badging profile data. **Note:** This check box is always selected by default and cannot be cleared. **Note:** In order to be able to export badge holder data the **Audit Log In** check boxes must be selected for the **Badges** and **Badge Fields Custom** data tables. See "Audit Log In".
	Badge Holder Card Data	Select this check box to export the badge holder card data. Select one of the associated options buttons to either: combine this data with the badge holder data, or add the clearance code and logical device exceptions data after the badge data. **Note:** If a user has more than one card, then there will be a separate data group exported per card, for the same user. **Note:** In order to be able to export badge holder card data the **Audit Log In** check boxes must be selected for the **Badge Cards** data table. See "Audit Log In".
	Badge Holder Clearance Codes	Select this check box if you want to export the badge holder clearance codes together with the badge profile data, separated by delimiters. **Note:** In order to be able to export badge holder clearance codes data the **Audit Log In** check boxes must be selected for the **Card Door Exceptions** data table. See "Audit Log In".
	Badge Holder Logical Device Exceptions	Select this check box if you want to export the badge holder Logical Device exceptions
	Badge Holder Events	Select this check box to export the badge holder events (i.e. door and reader) data. **Note:** Selecting this check box **disables** the Badge Holder Clearance Codes and Badge Holder Logical Device Exceptions check boxes, and **selects** the Badge Holder Card Data check box.

Tab	Field	Comments
Data Mapping tab (Return to ODBC Export "TAB LIST")	Pro-Watch Badging Field	Select a badge field from the drop-down list. Required field.
	Default	If no data is supplied in the file, this value will be used to update or insert the badging record for the mapping value. If no “Delimited Field #” is defined, this value will always update the defined mapping value unless the “Apply Default to Inserts Only” is checked.
	Table Column Data Type Size	Read-only SQL data import fields that are enabled and automatically populated when a Pro-Watch Badging Field is selected from the drop-down list. Table displays the name of the SQL database table. Column displays the database column in that table. Data Type and Size fields display the type and size of the data imported by DTU.
	Remote Column	Name of the badging column on the remote database table. Select one from the drop-down menu.
	Data Type Size	When you select a remote badging column, its data type and size are displayed automatically in these view-only fields.
	Add	Click this button to add the data mapping statement to the grid below under the following columns: Remote Column—The key column in the remote data table that identifies each record uniquely. Pro-Watch Description—The description of the column in Pro-Watch. Pro-Watch Table—The Pro-Watch table from which the record is exported. Pro-Watch Column—The name given to the same column in Pro-Watch. Default—The default value which, if no data is supplied, will be used to update or insert the badging record. Mapping Rules—See "ODBC Export Mapping Rules".
	Delete	Click this button to delete the selected data mapping statement from the grid below.

Tab	Field	Comments
Filter tab (Return to ODBC Export "TAB LIST")	Pro-Watch Badging Field	Click the drop-down list arrow to select a badging field to filter from the Pro-Watch database.
	Comparison	Click the drop-down list arrow to select a logical operator for comparing the value of the Pro-Watch field to the selection criterion entered into in the “Value” field (see below).
	Value	Enter the alphanumeric value that the Pro-Watch will use to compare and filter the remote column according to the logical operator selected in the Comparison field (see above).
	And/Or	Select either the And or the Or option button to combine multiple filtering statements to filter a Pro-Watch column.
	Add	Click Add to add the filtering statements to the grid under the following columns: Remote Column - The key column in the external data table that identifies each record uniquely. Comparison - The logical operator used to filter the data record from the remote data table. Value - The value according to which the data record will be filtered from the Pro-Watch data table and exported to the remote database. And/Or - The logical operator that concatenates multiple filtering statements.
	Delete	Click Delete to delete a selected filtering statement from the grid.
Logging tab (Return to ODBC Export "TAB LIST")	Generate Log File	Select this check box to generate a log file for the data export procedure.
	Directory	Enter a directory path for the log file or click the “...” button to browse for a directory.
	E-Mail Log File	Select this check box to e-mail the log file.
	SMTP Server	Enter the name of the e-mail server. If the SMTP Server is not set, enter the name of the local SMTP server.

Tab	Field	Comments
	From/To/CC	Enter: Your e-mail address (From). The e-mail address of the log file's recipient (To). The e-mail address of the party who will receive a copy of the log file (CC).

64.8.6 Audit Log In

The below example demonstrates how you can turn on the **Audit Log In check boxes** for the **Badges data table**. All the other relevant tables can be edited similarly:

1. Double-click the **Database Configuration** icon in the left pane to display in the middle pane the icons for all Pro-Watch data modules.
2. Double-click the **Database Tables** icon in the middle pane to display in the right pane the icons for all Pro-Watch database tables.
3. Select the **Badges** table by clicking its icon once.
4. Right click to display the pop-up menu and select **Properties**. The Edit Database Tables dialog box will display.
5. In the **Audit Logging** information group, select the **Add**, **Update** and **Delete** check boxes.
6. Click **OK** to close the dialog box.

64.9 ODBC Export Mapping Rules

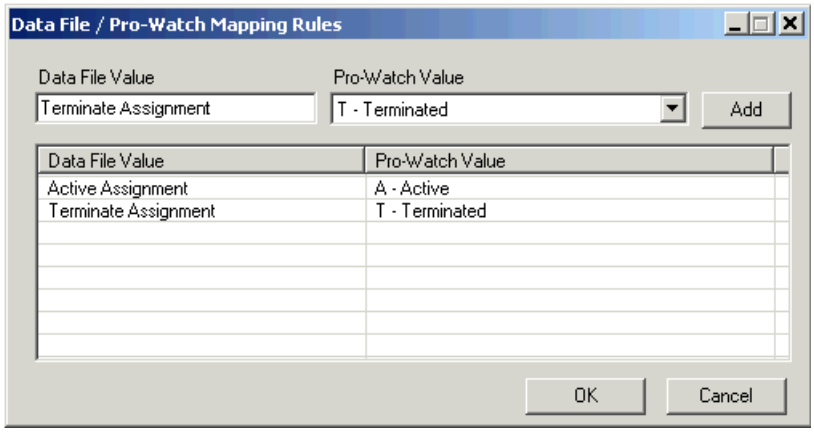
Mapping rules in this context determine how each column value in the Pro-Watch database will be converted into an external database column value.

Examples:

- One mapping rule could be "whenever you see the value 'Human Resources' for Department_ID in a Pro-Watch data table, map it as '123' when exporting the record into an external data table."
- Another mapping rule could be: "whenever you see the value 'T' in a Pro-Watch data table, map it as 'Terminated' for Employee-Status when exporting the record into an external data table."

To define a mapping rule:

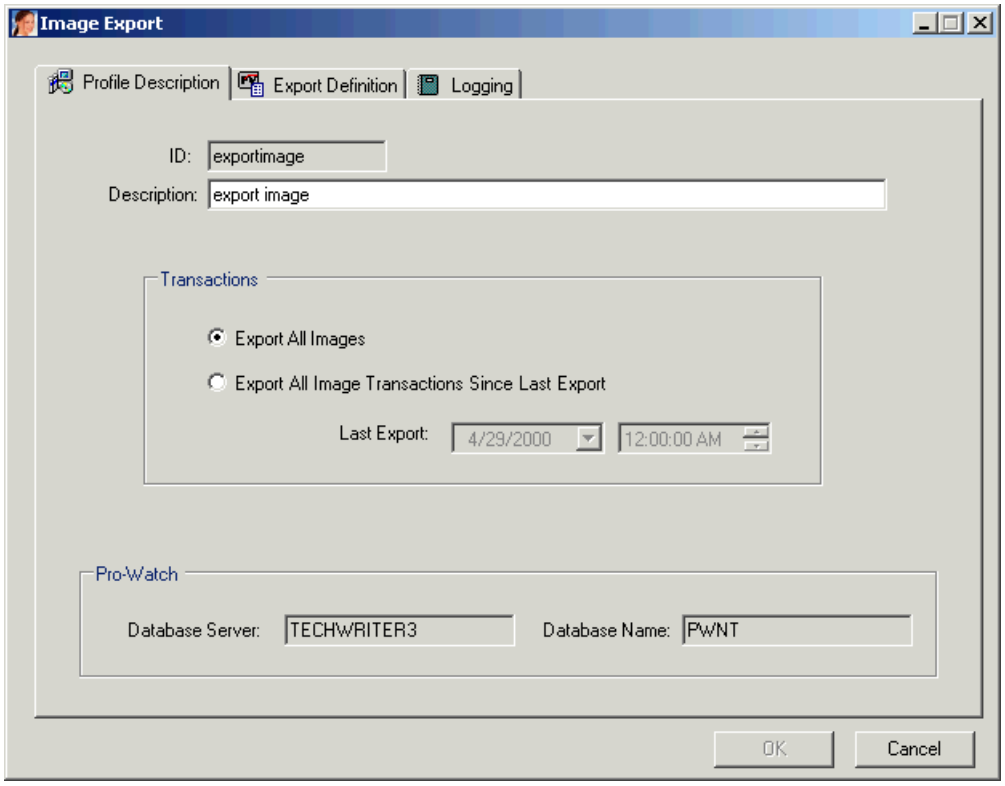
1. In the Data Mapping tab grid, right-click **a mapping row**.
2. Select **Edit Mapping Rules** from the po-up menu to display Data File/Pro-Watch Mapping Rules dialog box:



3. Enter each **Data File Value** (the value of the variable in the external database) with its corresponding **Pro-Watch Value**.
4. After you have entered all the corresponding mapping pairs, click OK to return to the Data Mapping tag.

The Mapping Rules column will display the number of rules you have defined, e.g., “1 rule,” “2 rules,” etc.

64.9.1 Editing an Image Export Profile



Edit the following ODBC Image Export fields as appropriate.

TAB LIST

Click one of the links below for the definitions of fields in different tabs:

- "Profile Description tab".
- "Export Definition tab".
- "Logging tab".

Tab	Field	Comments
Profile Description tab (Return to ODBC Image Export "TAB LIST")	ID	Unique profile ID used to identify the profile. Required field.

Tab	Field	Comments
	Description	Description of the profile. Required field.
	Export All Images	Select this option box to export all Pro-Watch images that satisfy the conditions set in the Export Definition tab (see below).
	Export All Image Transactions Since Last Export	Select this option box to export all updated Pro-Watch images that satisfy the filtering criteria and were not exported during the last exporting session. **Note:** You must have Audit Log In feature turned on to export the images stored in the BLOB data table. See "Export Definition tab".
	Last Export	Select from the drop-down lists the date and time of the last exporting session.
	Database Server	The name of the Pro-Watch database server from which the images will be exported.
	Database Name	The name of the Pro-Watch database from which the images will be exported.
Export Definition tab (Return to ODBC Image Export "TAB LIST")	Export Blob	Select a BLOB to export from the drop-down list. If the image is stored in a database the "Database Image Storage" text will be highlighted. For such images you have to enable the Audit Log In in the BLOBS table in order to track image transactions. See "Audit Log In". If the image is stored in a file on your hard drive the "File System Image Storage" text will be highlighted. Tracking of image transactions will be based on the file system date and time of the image file.
	Export Directory	Enter the path of the directory to which you want to export the image or click the ellipsis (...) button to browse for a directory.
	Export File Name	Enter a Prefix and a Postfix to lead and follow the file name of your exported image. The pre- and postfix may contain an underscore or a hyphen. Select a Naming Column from the drop-down list for the middle components of the export file name. For example, if you select "last name," the real last name in that column will be inserted into the file name. Select an Image Type from the drop-down list. Your choices are .JPG, .BMP, .TIF, .GIF, .PNG.

Tab	Field	Comments
Logging tab (Return to ODBC Image Export "TAB LIST")	Generate Log File	Select this check box to generate a log file for scheduled image export sessions.
	Directory	Enter the path of the directory to which you want to save the log file or click the ellipsis (...) button to browse for a directory.
	E-Mail Log File	Select this check box to e-mail the generated log file.
	SMTP Server	The name of the e-mail server which will e-mail the log file. Enabled if the e-mail check box is selected.
	From, To, CC	Enter the From, To and Copy e-mail addresses to be used when the log file is e-mailed. Enabled if the e-mail check box is selected.

64.10 Transferring the Data

To execute the data transfer, go to the command prompt at the Pro-Watch server and execute the following commands from the default directory:

```
cd:\Program Files (x86)\prowatch\DTU
pwbadgeload.exe [profile name]
```

64.11 LDAP/Active Directory Integration

Pro-Watch DTU integration with LDAP allows insert/update of Pro-Watch badge records based on Active Directory settings for the user.

This allows the ability to:

- Automatically create new Pro-Watch badges and cards for new Active Directory users
- Update of Pro-Watch badge information based on Active Directory user account
- Deletion of Pro-Watch badge based on Active Directory account attribute
- Disable on Pro-Watch card based on Active Directory account setting
- etc.

Note: Legacy DTU LDAP jobs will no longer work with PW 4.4 DTU. Existing DTU LDAP jobs will need to be modified to work with the new functionality.

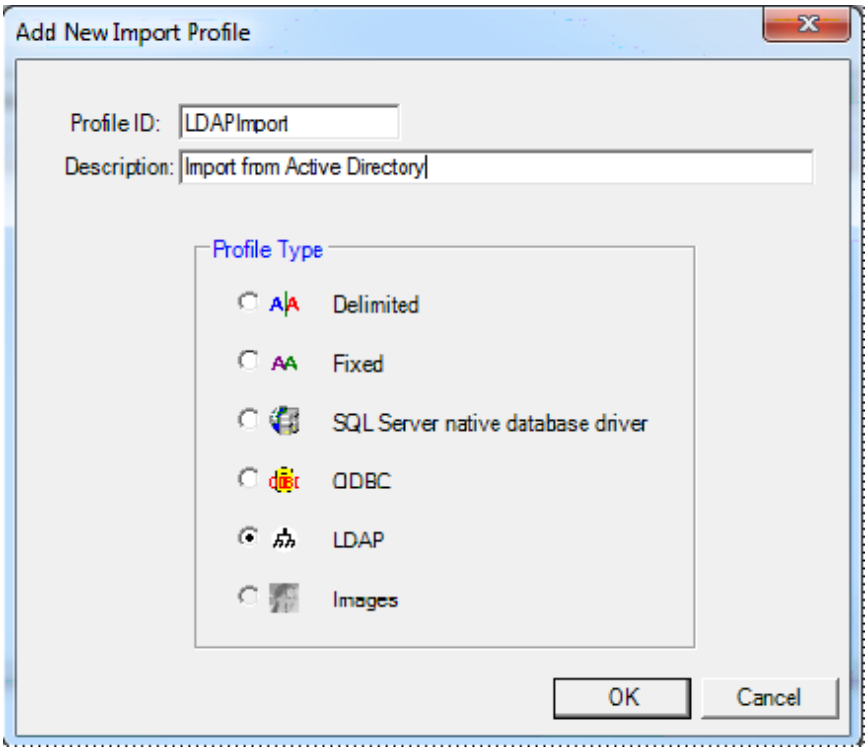
Note: After entering remote connection settings for the domain controller, there will be a brief delay in opening up the import profile. This delay is due to Pro-Watch establishing a connection to the active directory server.

64.11.1 Creating DTU LDAP Import Profile

To create a LDAP import profile for the DTU:

1. Run the Data Transfer Utility from **Pro-Watch > Administration > Executables**.

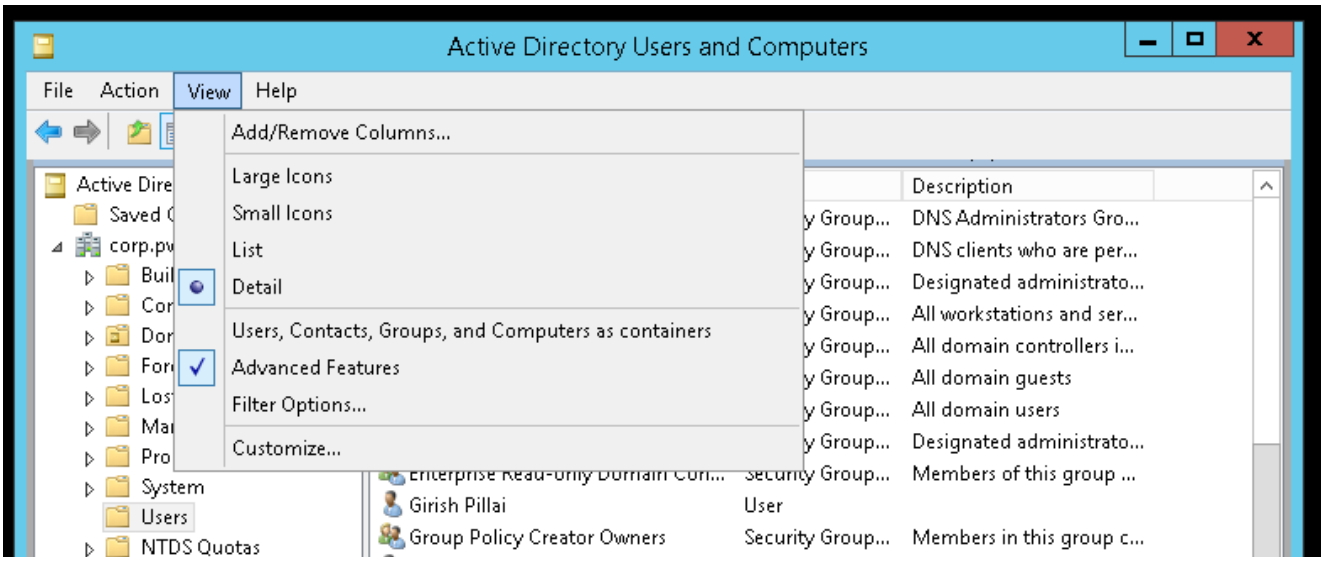
2. Create a new import profile with **Profile Type** of **LDAP**:

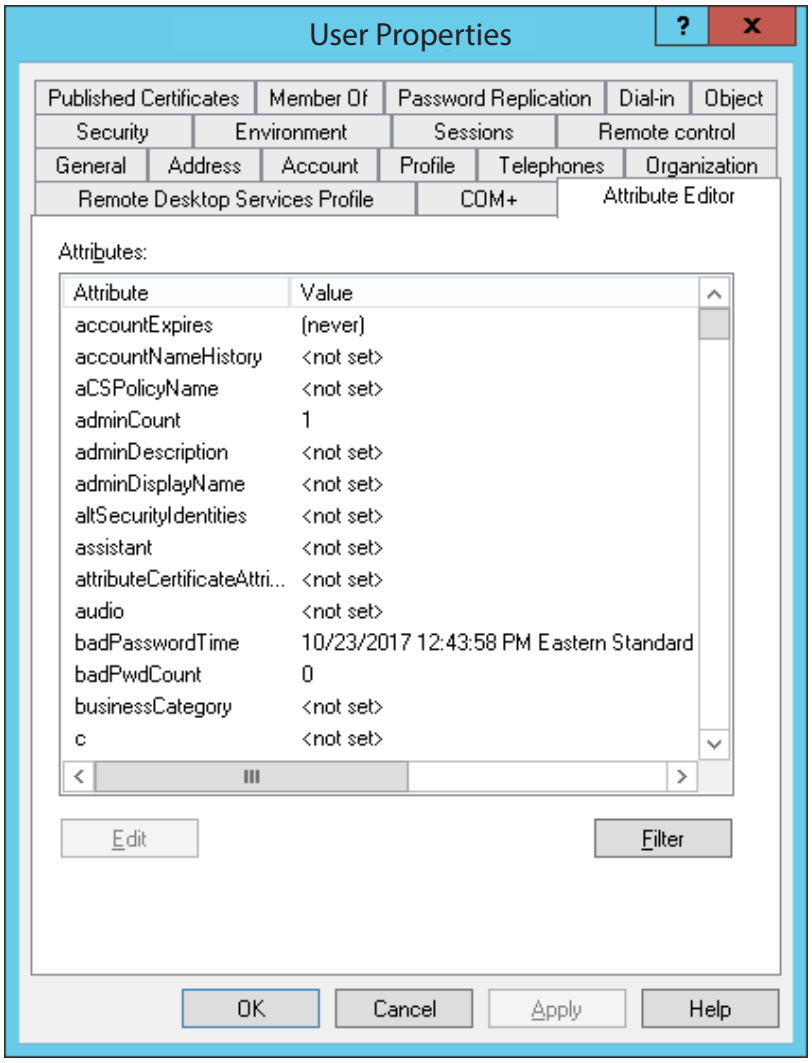


64.11.2 Editing Active Directory User Attributes

The Active Directory user account settings can be edited on the domain controller where the Active Directory Users and Trusts are installed.

To enable view/edit of the user account attributes, select **Active Directory Users** and **Computers > View > Advanced Features**:



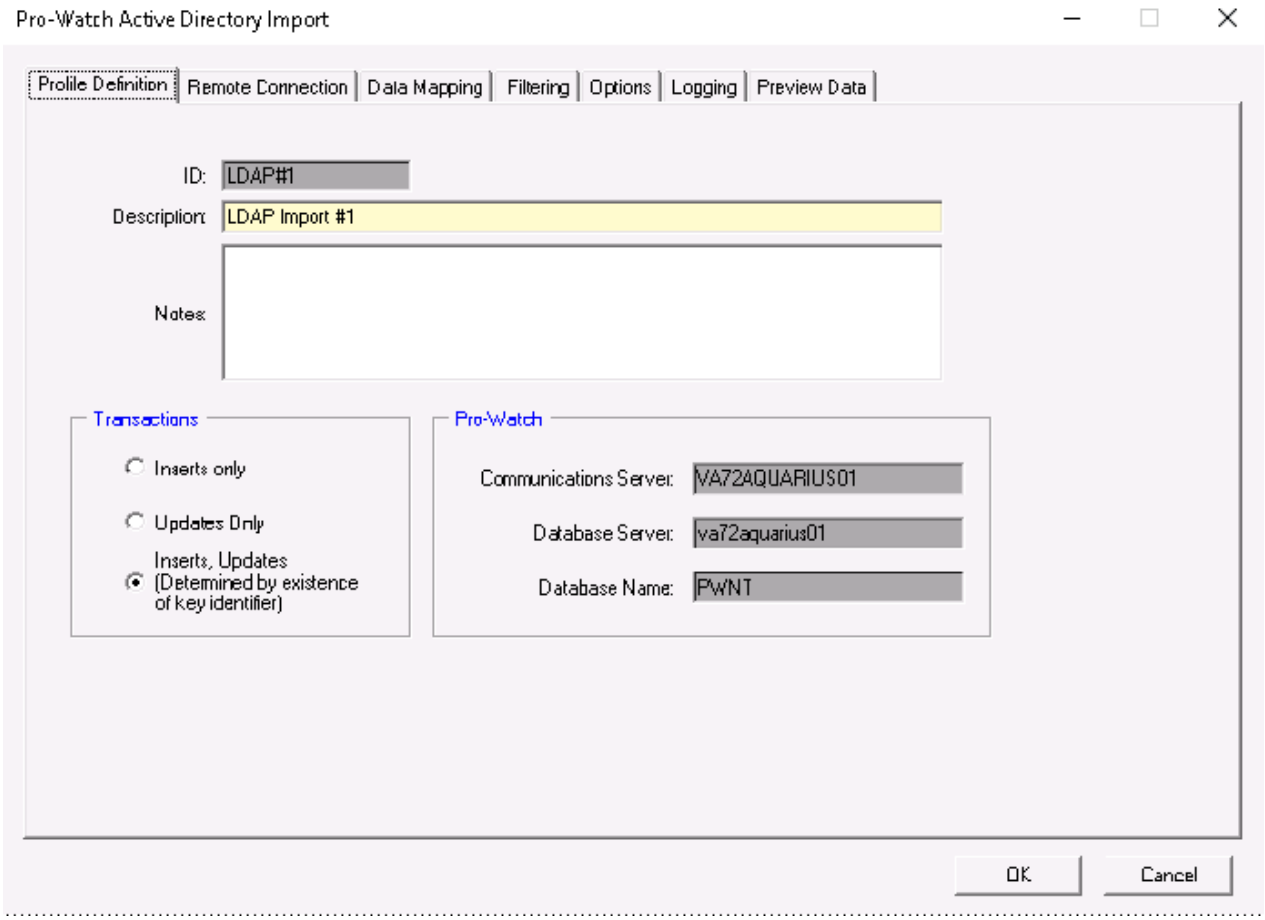


These user fields can be mapped to Pro-Watch fields through the DTU.

64.11.3 DTU Import Profile General

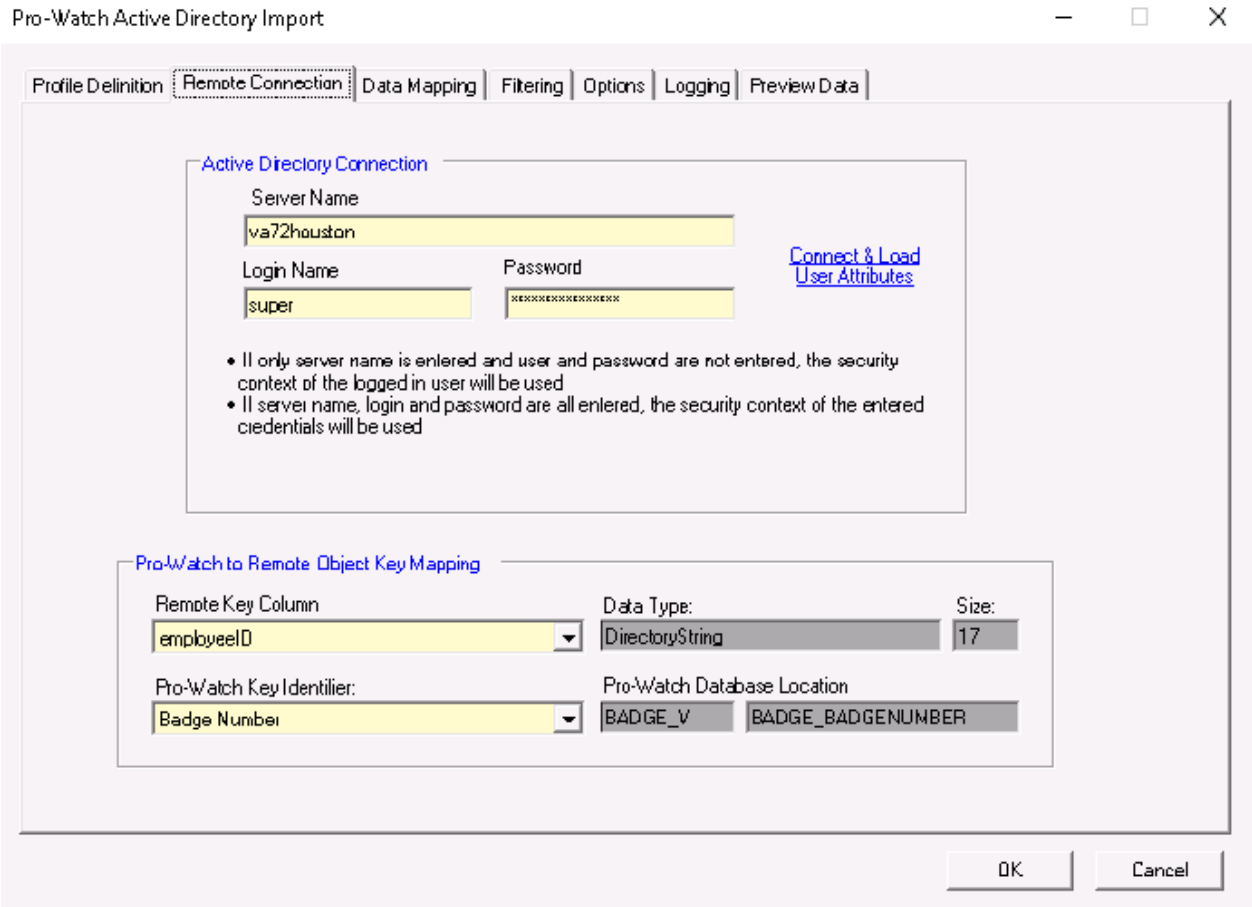
The DTU Import profile has several tabs to govern the general settings and connection to active directory.

64.11.3.1 Profile Definition Tab



Field	Required	Notes
ID	Yes	ID of the DTU import profile. This is set on creation of the import profile and cannot be changed. The ID is what is used to run the DTU profile through PWBadgeLoad.
Description	Yes	Description of the profile. This is a required field.
Notes	No	Notes regarding the import profile.
Transactions	Yes	Indicates if the pull will be for inserts, updates, or both.
Pro-Watch	N/A	This is information only documenting the Pro-Watch Comm Server, Pro-Watch Database Server, and Pro-Watch Database.

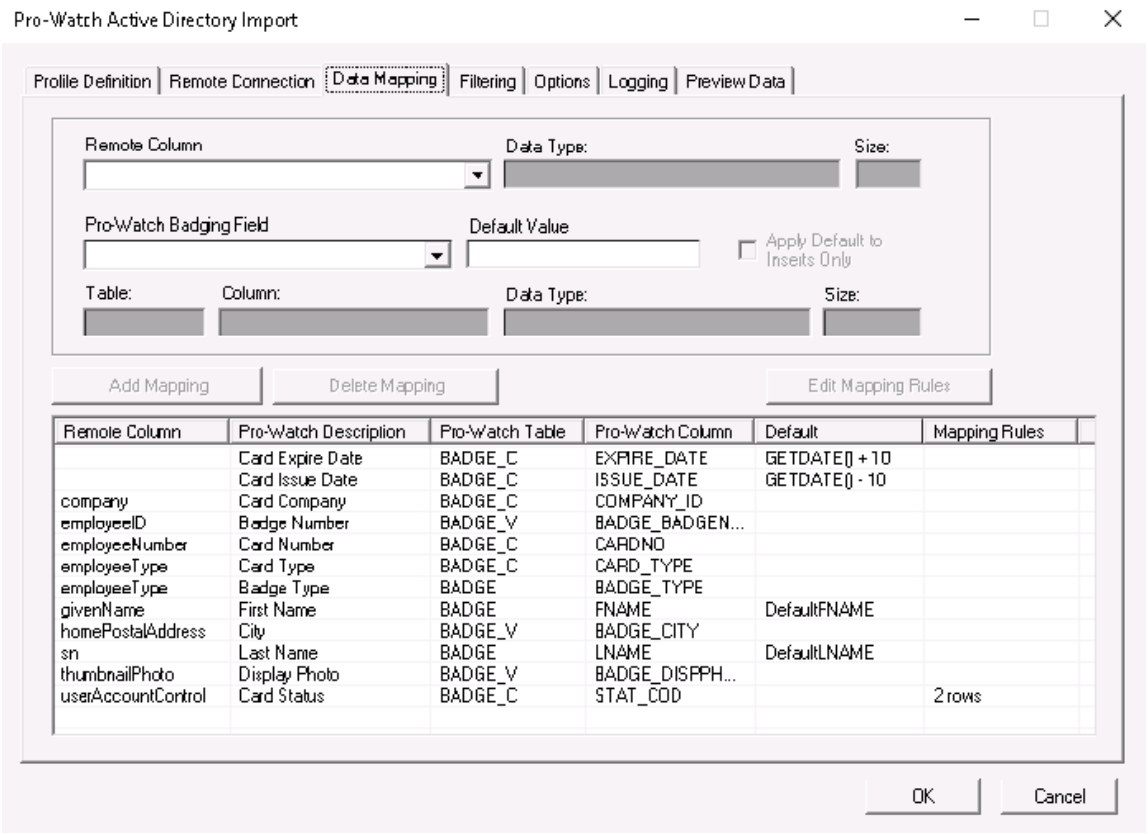
64.11.3.2 Remote Connection Tab



Field	Required	Notes
Active Directory Connection	Yes	Connection information for the active directory server (domain controller).
Pro-Watch to Remote Object Key Mapping	Yes	The key mapping between active directory and Pro-Watch. This needs to be an unique identifier.

Once the active directory server information is entered, press the **Connect & Load User Attributes** to check connection to the active directory server and to populate the **Remote Key Column** under the **Pro-Watch to Remote Object Key Mapping** section.

64.11.3.3 Data Mapping Tab



Field	Notes
Remote Column	Active Directory Field
Pro-Watch Badging Field	Pro-Watch Badging Field that the Active Directory Field links to.
Default Value	Default value to be used if there is no associated remote column value.
Add Mapping	Add the mapping
Delete Mapping	This is information only documenting the Pro-Watch Comm Server, Pro-Watch Database Server, and Pro-Watch Database.
Edit Mapping Rules	Edit the mapping rules for values imported from the remote column.

Note: To guarantee correct operation, the **Remote Key to Pro-Watch Key Identifier** set during **Profile Definition** must be a part of the mapping.

Note: If importing data to a Pro-Watch primary key field, there has to be a corresponding value for the **Active Directory** record. Otherwise, the import will generate errors.

64.11.3.4 userAccountControl values

In Active Directory, the **userAccountControl** value governs the status of the user account. This value in Active Directory follows the following value settings:

- **512** = Account is Enabled
- **514** = Account is Disabled
- **66048** = Account is Enabled, password never expires
- **66050** = Account is Disabled, password never expires

64.12 LDAP Filtering

64.12.1 Active Directory Filtering

The filters for active directory will allow filtering of active directory records based on desired values. The filter syntax follows standard active directory filter syntax (see reference/resource links above for examples).

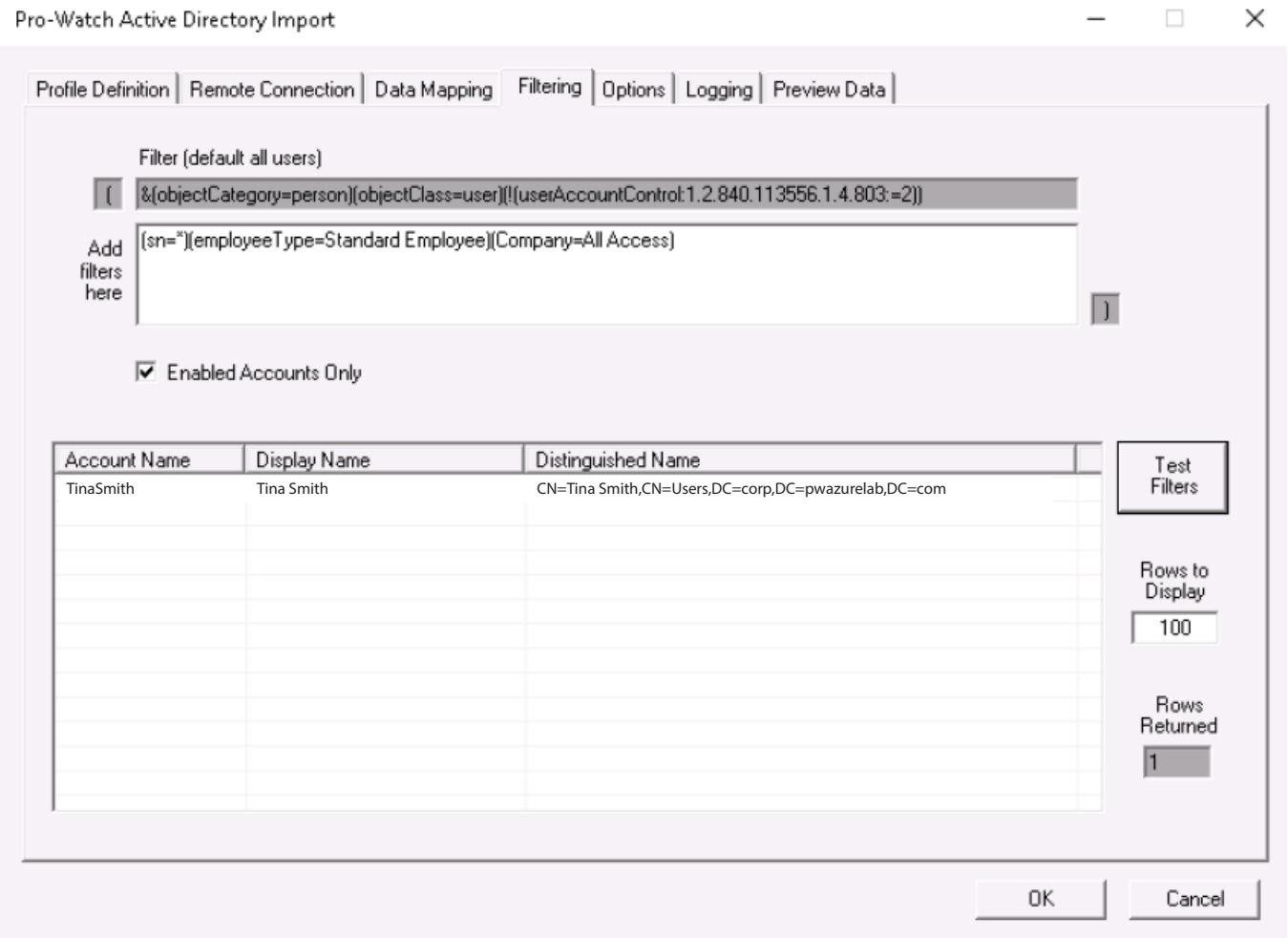
The filters in the screenshot below:

- Looks for active directory users with a value in the last name (build in AD user accounts will have first and last name values blank)
- Looks for active directory users with attribute **employeeType** set to **Standard Employee**.
- Looks for active directory users with attribute **Company** set to **All Access.**

The **Enabled Accounts Only** check-box will only pull enabled accounts from Active Directory. While this is useful to screen out disable accounts on the initial pull, this will also screen out accounts that recently underwent a change from active to disabled and may affect the desired operation.

For example, if the DTU profile is set to either (1) delete the badgeholder for a given field or (2) change the card status for a given field and the

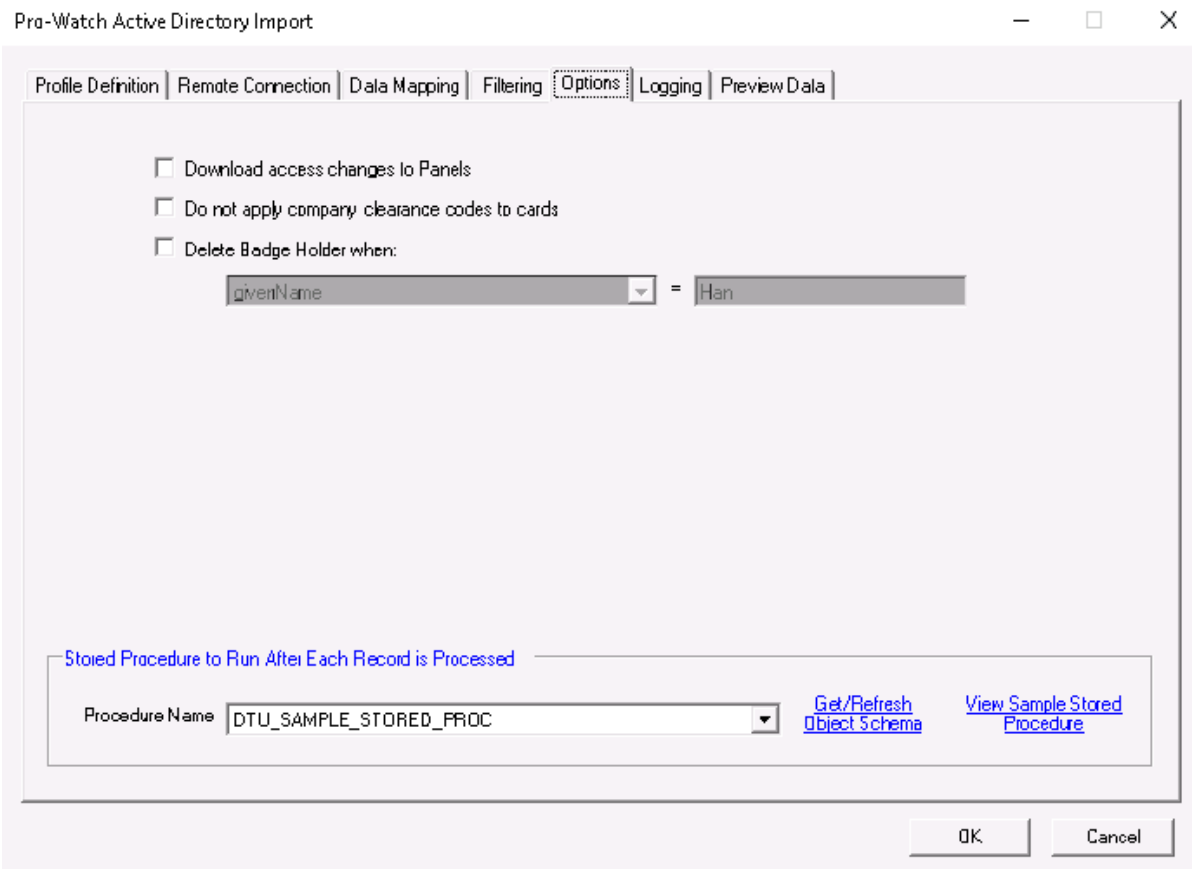
Active Directory user is disabled, this will screen out that user from being pulled by the DTU so no changes will be made in Pro-Watch for that record.



After entering the desired filters, click on the Test Filters button to test the filters and to see the returned values from active directory.

64.13 LDAP Options

64.13.1 Active Directory Import Options



Option	Notes
Download access changes to Panels.	If a change is made (access given/removed), download the corresponding changes to panels so that the panel database is up to date. Entries will be made to the HI_QUEUE table.
Do not apply company clearance codes to cards	When creating a new card with a company, do not apply the clearance codes associated with that company to the card.
Delete Badge Holder when (mapping and value must be provided)	Deletes the corresponding badge in Pro-Watch if an Active Directory field matches the desired value.

Option	Notes
Delete Mapping	This is information only documenting the Pro-Watch Comm Server, Pro-Watch Database Server, and Pro-Watch Database.
Edit Mapping Rules	Edit the mapping rules for values imported from the remote column.

64.13.2 Stored Procedure to Execute

The DTU will allow execution of a stored procedure following each import record. View the provided sample stored procedure by clicking on **View Sample Stored Procedure** to see the format. The stored procedure must take in two (2) parameters in order to be executed corrected.

See below for a sample stored procedure that will be executed following each record:

Sample Code

```
USE [PWNT]
GO

SET ANSI_NULLS ON
GO

SET QUOTED_IDENTIFIER ON
GO

-- This sample stored procedure assumes there is a column in BADGE_V called
EMPLOYEE_ID


ALTER PROCEDURE [dbo].[DTU_SAMPLE_STORED_PROC]
(
-- DTU key value of data loaded
-- This could be an nvarchar or an integer depending on the key type
@keyID nvarchar(50),
-- Status from DTU of data loaded. 1 = data loaded, 0 = data not loaded
-- Use this value if you need to update the status of a row being loaded or
not
@status integer
)

AS

BEGIN
       SET NOCOUNT ON;
       -- add stored procedure code here
       -- declare @badgeID varbinary(18);

       -- get Pro-Watch unique ID using key passed in from DTU
       -- select @badgeID = id from dbo.badge_v where employee_id = @keyID;


    -- update dbo.badge set last_change_date = getdate() where id =
@badgeID

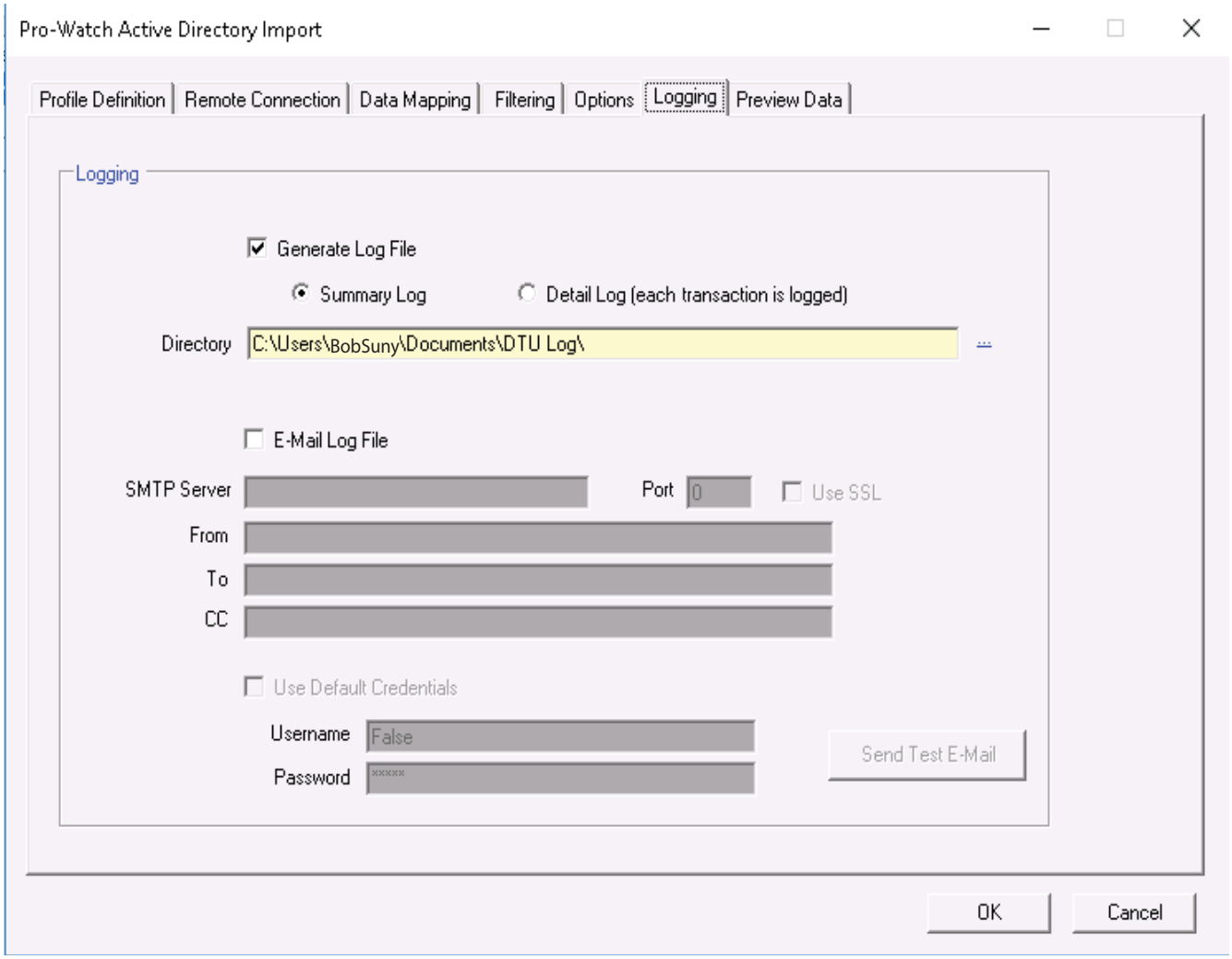
    insert into dbo.TempTable (ID, EventDate) values (@keyID,
CURRENT_TIMESTAMP);
END
```

This stored procedure inserts the ID (card number) of the record along with the date of insert into a created **TempTable** table in SQL.

64.14 DTU Logging and Preview

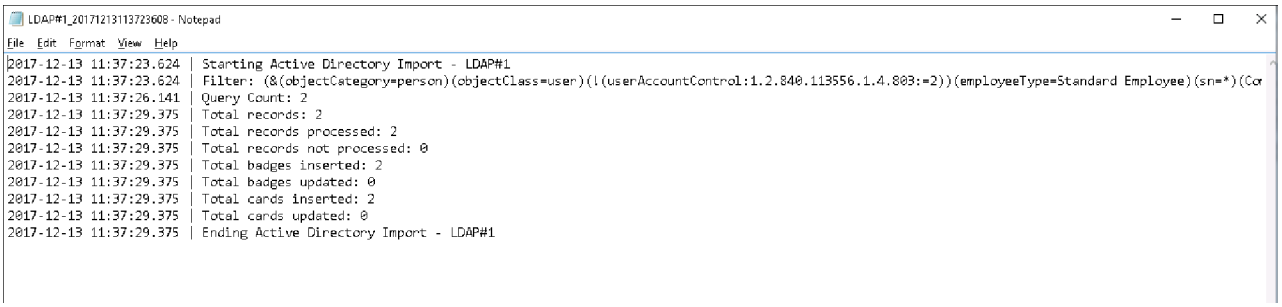
64.14.1 DTU Logging

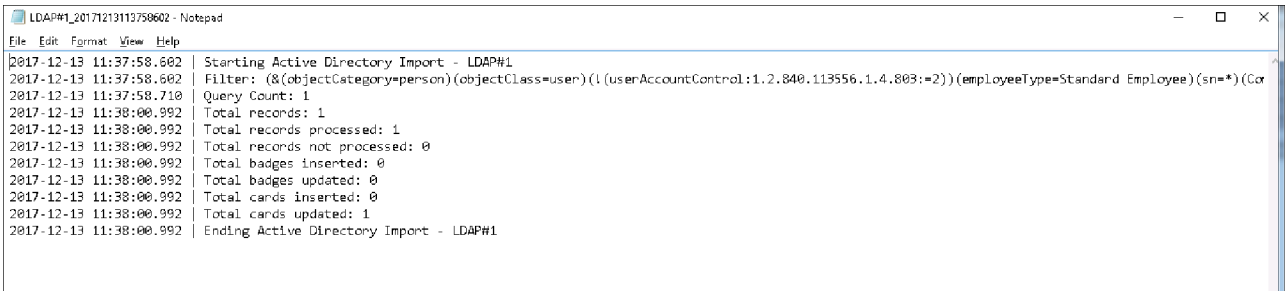
The Logging tab governs the logging functionality of the DTU. Generating a log file is not required, but is recommended for troubleshooting purposes. The DTU offers the ability to generate a summary log or detailed log and also to e-mail the log file by using SMTP to a desired recipient.



The log names created will contain the DTU profile name and the date/time of run.

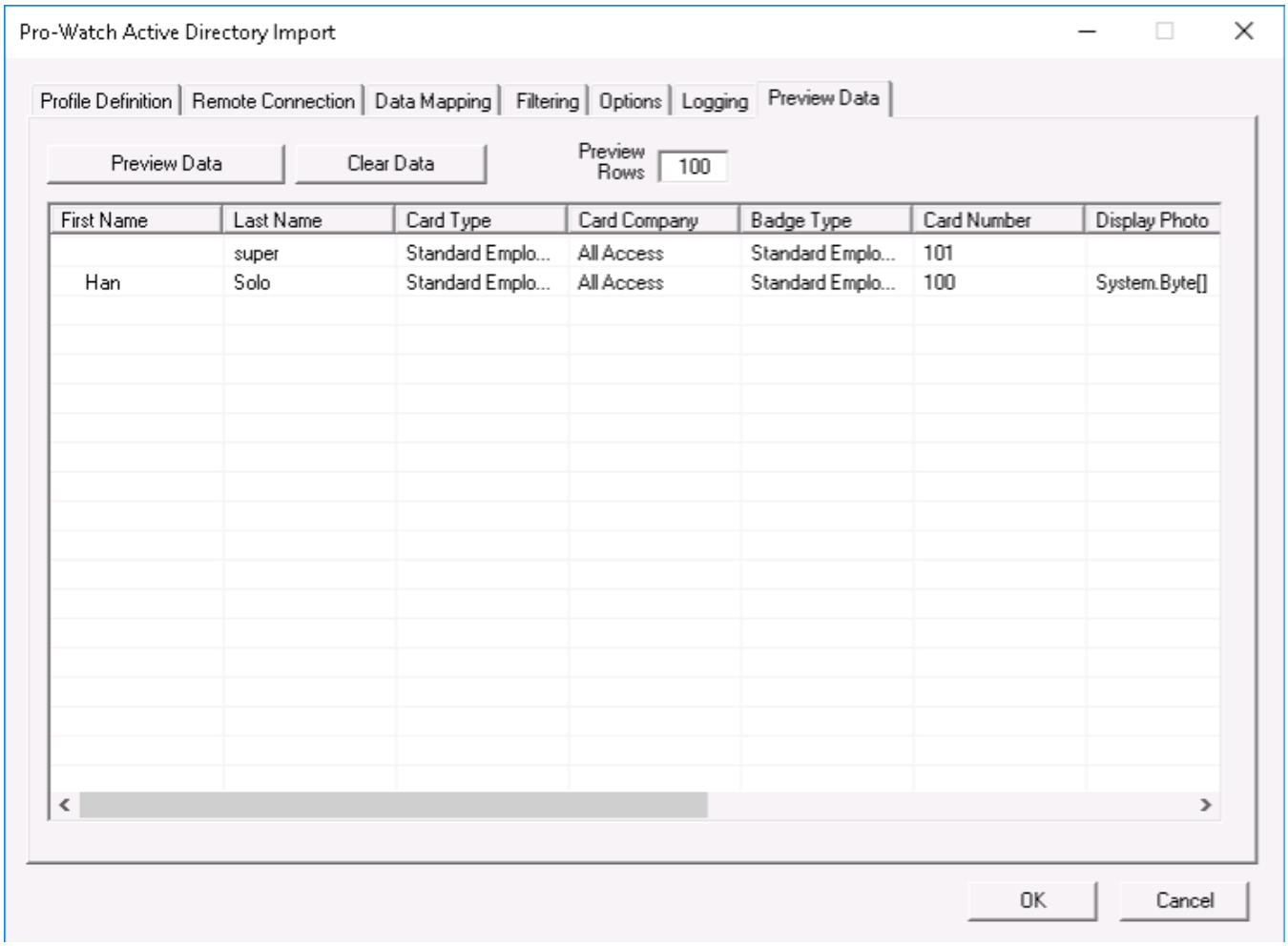
64.14.2 Sample Log Files





64.14.3 DTU Preview

The **Preview Data** tab allows preview of the data, fields, and field values that will be imported through the profile. Click on **Preview Data** to view the list of records that will be imported.



Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Archiving

65

In this chapter ...

Overview
Event History
Archiving and Purging Event History
Adding or Editing an Archive
Using the Pro-Watch Query Analyzer
Deleting an Archive

65.1 Overview

Use this function to move transaction data (event and audit logs) to offline storage. Archiving reduces the size of the database, allowing Pro-Watch to maintain optimal performance.

Note: For information on defining log thresholds, see "Setting Event Log Thresholds" in Chapter 5 . See also "Setting Database Limits" in Chapter 5 and "Setting the Log Size" in Chapter 5.

Caution: If your Pro-Watch system uses Microsoft SQL Server, the database can grow to a size that will consume the entire drive space. If your Pro-Watch system uses MSDE, the database size is limited to 2 GB. Transaction history (card reads, alarms, and so on) uses most of this space. Therefore, whether your Pro-Watch system is using Microsoft SQL Server or MSDE, it is necessary that you monitor and manage the database size.

65.1.1 Discontinued Support

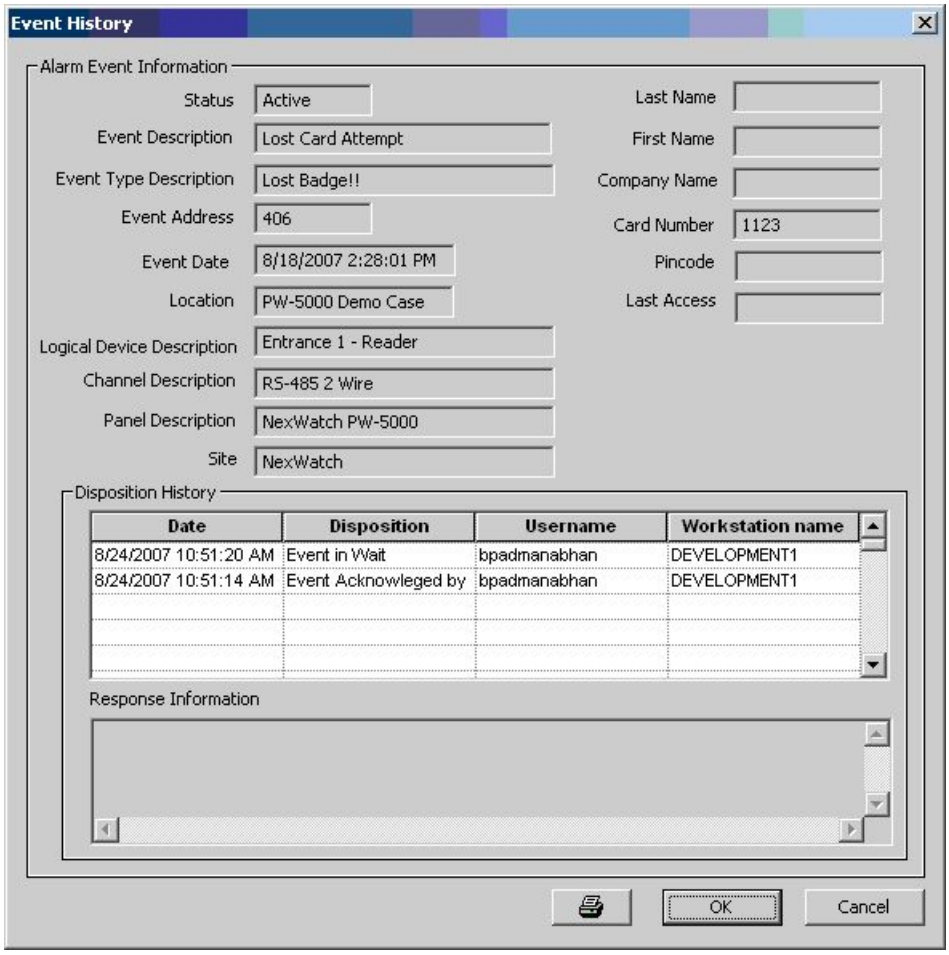
The “Legacy Restore” function is no longer supported.

65.1.2 Format of the Archives

CSV (Comma Separated Value) is the format of the archives.

65.2 Event History

You can view an event history from the **Alarm monitor** or from the **Transactions** tab in the properties of a card, logical device, or site. To view an event history from either the Alarm monitor or the Transactions tab of card, logical device, or site properties, right-click on the event and select **View Event History** to display the history of the selected event.



Click the print button to print a hard copy of the history report.

65.3 Archiving and Purging Event History

Each site has different requirements on how much current history must be kept in the database. A good rule of thumb is to keep three months of active history. This means that every month you should archive and purge history for one month, three months back.

Example: On January 1, archive and purge the entire month of September of the previous year. Then, on February 1, archive and purge the entire month of October of the previous year.

It is generally recommended that you archive monthly to avoid archiving more than one month's history at a time. This will keep the database and the archives well organized in the event you need to restore them. However, your site may have specific needs that require you to use a different archiving practice.

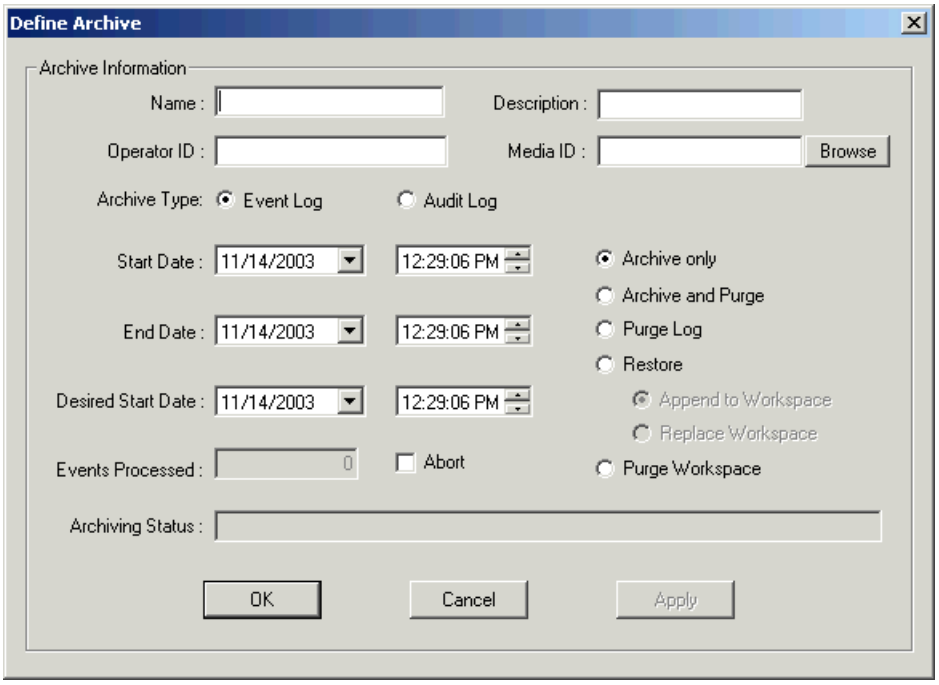
See "Setting Event Log Thresholds" in Chapter 5 for more information on purging.

65.4 Adding or Editing an Archive

Follow these steps:

1. In the left Pro-Watch navigation pane, click **Administration**.
2. Double-click the **Archives** folder. The Archives folder expands, and icons for any existing archives display in the right pane.
3. If you are creating a new archive, right-click anywhere in the right pane and select **New**. The **Define Archive** dialog box appears.

   If you are editing an existing archive, right-click the selected archive and select **Properties**. The **Define Archive** dialog box appears:



4. Use the following table to complete the dialog box fields:

Field	Description
Name	Specifies an archive name, such as Audit Nov-25-02.
Description	Specifies an archive label such as Audit Nov-25-02. Pro-Watch uses this field as a label for your Archive icon. Because you may eventually fill up the right pane with Archive icons, it is recommended that you make each label both log-name and date-specific.

Field	Description
Operator ID	ID of "SysOp," system operator, or the user who created the archive.
Media ID	Specifies the name of your backup/restore file. You can enter the media ID (the folder and name of your file), or click the Browse button to search for the appropriate directory.
Archive Type	Specifies one of the following archive types: Event Log—Uses an event log for processing. Audit Log—Uses an audit log for processing.
Activity	Selects the tasks you want the archive to perform: Archive Only—Archives designated log records defined by start and end times. Archive and Purge—Archives designated log records and then purges them from the system. **Note: Purge Log—**Removes log records from the system. You cannot undo a purge, so you should only select this option if you are certain you will not need to archive these records again. Restore—Restores previously-archived log records. Select Append to Workspace option button if you want to add these records to the ones in the workspace. Select Replace Workspace option button if you want these records to replace the current ones in the workspace. Purge Workspace—Deletes the contents of the workspace.
Events Process	The number of events processed.
Start Date/End Date	Specifies the start and end dates and time of the alarm-event records to be archived. You can select the start and end dates interactively by using the Archive Calendar.
Abort (Check Box)	Aborts an archive. You can select this check box at any time during the archive to abort.
Desired Start Date	Specifies the date and time when you want the archiving to begin. This field defaults to the current date and time. If you accept the current time, Pro-Watch begins the archive as soon as you click **Apply**.
Archiving Status	Indicates the archive's processing progress.

5. Enter the information for the new archive.

6. Click **Apply** to save the settings of the new Archive and keep the Define Archive dialog box open. The **Apply** button enables you to run an archive and view its progress.
7. Click **OK** to save the archive and finish.

65.4.1 Beware of "11:59:00 p.m." and "11:59:59 p.m." End Times

Most users define a "day" as one that starts at midnight and runs 24 hours through to the next midnight.

Thus there is a tendency to define the ending time of the alarm events to be archived as "11:59:00 p.m." or "11:59:59 p.m."

65.4.1.1 Problem

The not-so-obvious problem is this:

- If you define the end time as "11:59:00 p.m.", then the Pro-Watch will not archive the alarm events occurring in the last minute of the day.
- If you define the end time as "11:59:59 p.m.", then the Pro-Watch will not archive the alarm events occurring in the last second of the day.

65.4.1.2 Solution: "12:00:00 a.m." Next Day

There is a very easy solution to this problem: enter "12:00:00 a.m." for the **next day** for ending day and time. That way you will never miss any alarm events taking place within the last minute or second of the day.

65.4.1.3 Caution about "Desired Start Time"

Caution: If the "Desired Start Time" (i.e., the day and hour when you want the archiving to begin) is **earlier than** the end day and time of the alarm events, you will miss some of the archiving data.

For example: let's say your **Start Date** is January 1, 2014 11:00 a.m. and your **End Date** is January 31, 2014 11:00 a.m. If your **"Desired Start Time"** is January 15, 2014 12:00 p.m., then you will miss archiving all the alarm events that occurred between that date (Jan 15) and the end of the month (Jan 31).

So make sure your "Desired Start Time" always comes **after** the end date of the last archiving event you want to archive.

65.4.1.4 FAQ

Q: "What if I need to archive the alarm events starting on 01/01/2014 (dd:mm:yyyy**) at 3:38 p.m. and ending three days later (04/01/2014) on 11:06 a.m.? What start and end days and times I should enter to make sure all alarm events occurring between those two dates and times (inclusive) are archived?**

A: Enter

- "1/1/2014" and "3:38 p.m." for start day and time
- "4/1/2014" and "11:06 a.m." for end day and time

65.5 Using the Pro-Watch Query Analyzer

If your site is not concerned with history and the database is nearing capacity, archiving and purging the history is not the only option in maintaining the database size. To avoid the processing time it takes to perform an archive and purge you can use the Pro-Watch Query Analyzer to completely remove all of the history from the PWNT database.

To completely remove all of the history from the PWNT database:

Warning: This operation is irreversible! Make sure use have the proper authority to make the decision before deleting all history from the PWNY database.

1. Select **Start > Programs > Pro-Watch > Pro-Watch Enterprise Manager**. The Pro-Watch Database Manager screen appears.
2. Select **Tools > Query Analyzer** from the tool bar. The Pro-Watch Query Analyzer opens.
3. In the Database To Query drop-down box, select PWNT. This should already be selected by default.
4. In the Upper Pane text box, type: `Truncate Table EV_LOG`
5. Click **Execute Query** to run the query. This may take up to several minutes.
6. When the query completes, the message “The Command(s) Completed Successfully” appears in the lower pane.

Another helpful query to use at this time clears all unacknowledged alarms from the Alarm Monitor.

Follow these steps:

1. Select **Start > Programs > Pro-Watch > Pro-Watch Enterprise Manager**. The Pro-Watch Database Manager screen appears.
2. Select **Tools > Query Analyzer** from the tool bar. The Pro-Watch Query Analyzer opens.
3. In the Database To Query drop-down box, select PWNT. This should already be selected by default.
4. In the Upper Pane white space, type: `Truncate Table UNACK_AL`
5. Click **Execute Query** to run the query. This may take up to several minutes.
6. When the query finishes, the message “The Command(s) Completed Successfully” appears in the lower pane.

65.6 Deleting an Archive

Follow these steps:

1. In the left Pro-Watch pane, click **Administration**.
2. Click **Archive**. The Archives folder expands, and icons for the existing Archives appear in the right pane.
3. Right-click the selected archive. Select **Delete**.

Copyright © Honeywell Inc. All Rights Reserved

Secure Mode Verification

A

In this appendix ...

Overview
Considerations and Limitations
Implementation
How Secure Mode Verification Works
Badge-Holder Photo Display

A.1 Overview

The Secure Mode feature is an extension of the Verification Viewer, which provides operator-validated access for particular access points. The purpose of the secure mode is to allow operator controlled acceptance or denial for access. Only if the reader is in secure mode will the host, through operator intervention (as opposed to field controller) will make all the access decisions.

When you open a verification window for a door within the specified Time Zone, the door becomes locked down.

When you set a Time Zone for secure mode, and the verification window is closed, the doors will not lock until you open the verification window even if you've rolled into the Time Zone you've set previously. For the doors to lock, you must open a verification window.

If you open the verification window before the Time Zone begins, then the doors will not automatically go into secure mode/lock even if you roll into the Time Zone set for the secure mode.

For a door to lock in secure mode, you must open a verification window within the specific Time Zone assigned to that reader, but not before.

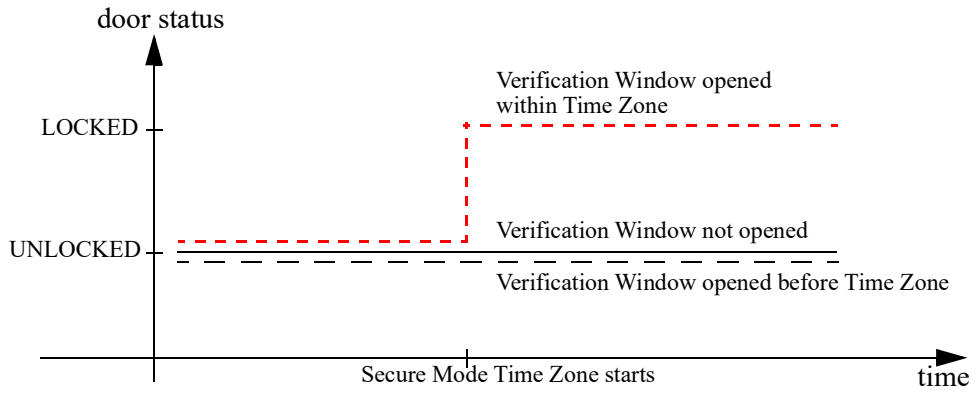


Figure A-1 Secure Mode Time Zone v.s. Verification Window Interaction

Cards presented to the reader will cause an "Access Attempt at Locked Door" (PW-5000) or "Invalid Reader Time Zone" (Cardkey) message, and the corresponding badge information and photo will appear in the verification window.

You can then grant or deny access to the individual by clicking **Accept** or **Deny**.

- Click **Accept** to open the door and log a host grant message.
- Click **Deny** to deny door access and log a host denial message.

When you close the Verification window, or at client disconnection, the door returns to its default operational state.

A.2 Considerations and Limitations

The Secure Mode feature is available only on panel technologies that support "Lock" functionality. "Lock" is defined in this context as a state in which a reader physically denies access yet still reads card presentations. At this time of writing, SEEP, CHIP and PW2000 are excluded for this reason.

Note: Cardkey and Mercury series are the only two panels that support Secure Mode.

The Accept and Deny buttons appear only after card events indicate that there is an access attempt at a locked door. Therefore, doors that are merely locked, but not necessarily in an explicit secure mode, may cause these buttons to appear.

The physical state of a secure mode-enabled door depends on whether you as an operator are currently viewing it in a verification window. That's why the server maintains information regarding who is viewing which doors.

It is the server that locks and re-enables the secure mode doors. Therefore a door is properly re-enabled only after *all* the operators have closed windows viewing that door.

If a door is in a "locked" mode before it is viewed by an operator in the secure mode, it will be re-enabled and reverted to its default mode of

operation, and not remain “locked,” after all operators have closed their verification viewers.

A.3 Implementation

You have to first configure a logical device before switching it to the Secure Mode.

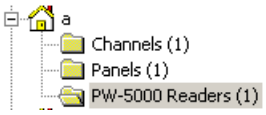
You may configure the individual readers within a logical device so that the readers may or may not to support the Secure Mode feature. For example, on a dual-reader door, the “in” reader may support the Secure Mode, but the “out” reader is not required to support it also.

To set the secure mode:

1. On any particular reader screen, whether in the Logical Device, Panel or Hardware Template setups, select the **Secure Mode** check-box to enable the secure mode for that reader.

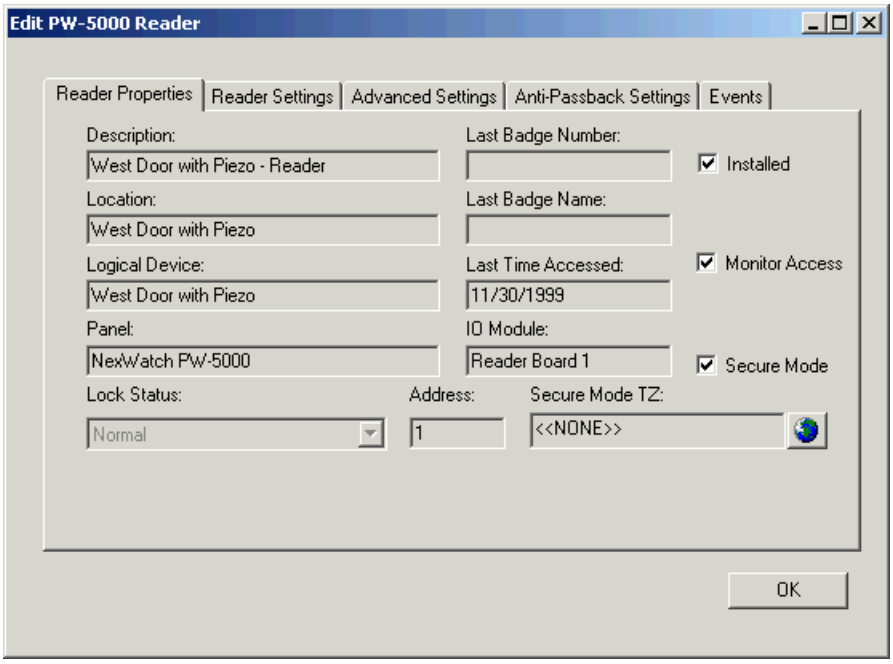
   For example, here is how you would do it from scratch in the Hardware module:

   - Create a **Site**, a **Channel**, a **Panel**, and a **Reader**, in that order. For example, the tree-diagram for the sample site “a” should look like the following:



   - Click the Reader (in the above example, “PW-5000 Readers(1)”) to display its icon in the right pane.
   - In the right pane, double-click the reader icon to display the Edit Logical Devices dialog box.
   - Select the Logical Device Details tab.

- Select a Reader and then click **Edit** to display the reader edit dialog box like the one below:



- Check the Secure Mode check-box.

2. In the Secure Mode TZ field, click the icon and select a Secure Mode time zone. This is the time zone, as processed in the server's local geographical time zone, during which the reader will go into the secure mode *if* an operator opens a verification window for the door.
3. If an operator opens a verification window for that door *before* the start of the time zone, the door will not automatically go into the Secure Mode when the time zone becomes enabled. Similarly, the doors that are in Secure Mode when their corresponding time zones end will remain in the Secure Mode until the last operator stops viewing the door in a verification window.

A.4 How Secure Mode Verification Works

When you open a verification window for a Secure Mode-enabled door, the door will "lock" during the appropriate time zone. Subsequent access attempts by cardholders will cause either an "Access Attempt at Locked Door" event (for PW-5000 series panels) or an "Invalid Reader Time Zone" event (for Cardkey series panels) to be reported.

Figure A-2 A badge photo



The receipt of either of these events will display the Accept and Deny buttons in the verification window.

- If you click **Accept**, you will momentarily unlock the door and log an "Operator Host Grant" message to the event log.
- If you click **Deny**, the door will remain locked but an "Operator Host Deny" message will be logged to the event log.

Note that you can display live video in the secure verification window along with the photo ID associated with the card that was presented to the reader. A camera view must be assigned to the reader logical device. By clicking the blue icon (with the right-directional arrow) in the tool bar of the secure verification mode screen, you can display the live video from the assigned camera view.

The receipt of other events at the door besides "Access Attempt at Locked Door" or "Invalid Reader Time Zone" will cause the Accept and Deny buttons to disappear, so that the operator may only make an access decision in response to those events.

A.5 Badge-Holder Photo Display

On top of the events window, Pro-Watch displays the photos of the latest badge-holders who present their cards to the reader.

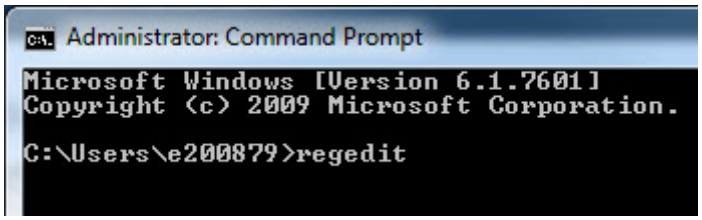
The photos of the badge holders are displayed horizontally, with the most recent badge-holder's photo displayed in the upper-left corner of the image area, and the oldest badge-holder's photo displayed in the lower-right corner of the image area.

The total number of badge-holder photos that the Pro-Watch can display is configured in the Registry. The default is 100 badge-holder photos.

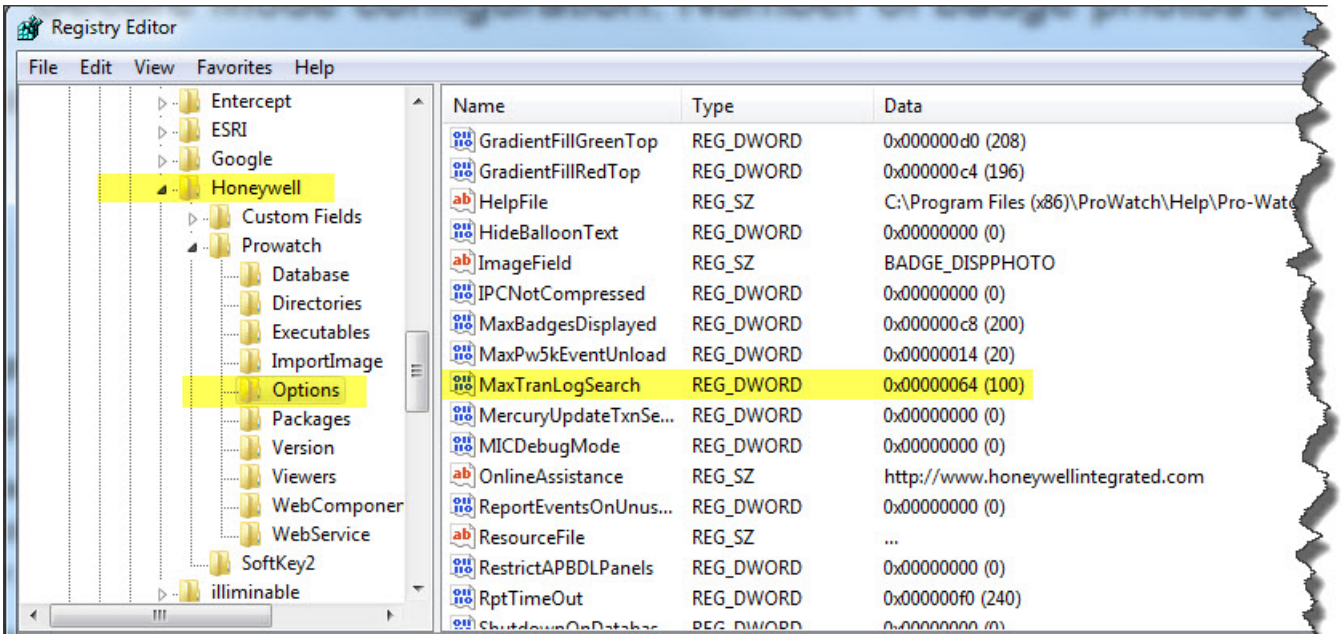
A.5.1 Editing MaxTranLogSearch Registry Key

You can change the maximum number of badge-holder photos displayed by editing the **MaxTranLogSearch** registry key.

1. From the Start menu, find and select the Command Prompt.
2. Type "**regedit**":

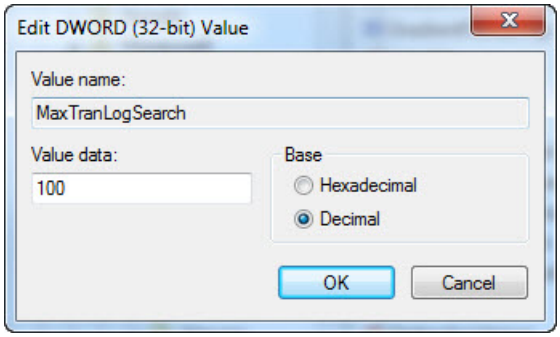


3. Press **Enter** to display the **Registry Editor**:



4. Select **Honeywell > Prowatch > Options > MaxTranLogSearch** which defaults to 100 (64hex).

5. To change that value, right click **MaxTranLogSearch.** From the pop-up menu select **Modify** to display the **Edit DWORD** dialog box:



6. Change the **Value Data** and click **OK**.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Assignable Programs

B

In this appendix ...

Programs Assignable to Classes and Users
Commands Assignable to Event Procedures

B.1 Programs Assignable to Classes and Users

The table below lists and describes the programs you can assign to classes and users. See the "DBC - Classes" and "DBC - Users" for information about how to assign these programs.

Note: If you do not assign the Query function to a program, the program will not be accessible to users from the Pro-Watch main screen.

Table B-1 Programs Assignable to Classes and Users

Program	Description and Available Program Functions
Action Note	User defined text or note that is required before an action can be initiated. Allows the user to initiate an action on a specific logical device or all applicable logical devices. Enforce – requires users to input a comment/note whenever they perform a manual function/action.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Administrative Viewer	Controls a user's access to and ability to launch the following applications listed in the Administrative Viewer: Archive – Moves transaction data (event and audit logs) to offline storage. Badge Builder – Creates a complete badge profile of users accessing the control system in your enterprise. Badge Fields – Creates fields that appear on the badge pages. Control Record – Defines the following server settings within the Pro-Watch shell: event log threshold, logical device tags, alternative names for "clearance code" and "logical device," and company tab labels. You can also set the card number seed and create additional tabs for the Companies dialog box in Database Configuration. Data Fields – Creates fields for use on forms. Dial-Up – Enables dial-up access to the Internet. Legacy Files – Moves files offline for archiving. Log Files – Creates a detailed list of system's activities. Map Builder – Creates drawings or floor plans of a facility for use in planning access control. Registry Editor – Edits Pro-Watch registry key values. Report Viewer – Creates and displays customized reports.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Alarm Monitor	Enables you to see and act upon the real-time status of alarms as they occur. See "". Access – allows access to Alarm Monitor. Ack – changes the status of an unacknowledged event to "acknowledged." Ackall – changes the status of all unacknowledged events to "acknowledged." CCTV – displays the Select CCTV view defined for the alarm on the alarm grid. Clear – clears the selected alarm from the Alarm Monitor. Clearall – clears all alarms from the Alarm Monitor. Lock – locks a reader in a logical device that is associated with the selected alarm. Open – momentarily unlocks a door. Output – activates, de-activates, pulses, or time activates an output. Quiet – silences the beeper. Reenable – returns the hardware associated with the alarm to normal operations. Response – adds an event response/instruction for an alarm. Rtnclear – clears an alarm that has not returned to normal. Secure – masks an input point. Sizegrid – resizes columns in the alarm page. Timed – initiates a timed override on a door. Unlock – unlocks the door associated with the alarm. View_picture – displays the photograph of the card holder. Void – voids a card.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Alarm Pages	Defines the Alarm Monitor display of incoming alarms. Add – adds an alarm page. Delete – deletes an alarm page. Query – queries for and displays an alarm page; provides program access. Update – edits an alarm page.
Archive	Moves transaction data (event and audit logs) to offline storage. Add – defines an archive. Archive – archives data. Delete – deletes an archive definition. Purge – deletes archived data. Query – queries for and displays an archive icon/entity; provides program access from the Pro-Watch screen. Restore – restores previously-archived data. Update – edits previously-archived data.
Areas	Defines a space for which you create an access control plan. For a given area, you can define associated logical devices, lock and unlock capability, and zone mode attributes. See "DBC - Area". Add – creates an area. Delete – deletes an area. Query – queries for and displays an area resource; provides program access from the Pro-Watch screen. Update – edits an area.
Badge Fields Maintenance	Provides the ability to add, edit, or delete custom badge fields or to edit or delete default badge fields. See "Badge Building" in Chapter 60. Add – adds a badge field. Delete – deletes a badge field. Query – queries for and displays badge fields; provides program access from the Pro-Watch screen. Update – edits a badge field.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Badge Maintenance	Provides the ability to configure badges and cards for access. See "" in Chapter 2. Add – creates a badge. AddBrassKey – assigns a physical key to the card holder. Batch_update – performs an edit on a group of badges. Biometric – this function is not supported in Pro-Watch, Release 5.0. Clearance – adds clearance codes to a badge. DelBrassKey – deletes a card holder's physical key privileges. Delete – deletes a badge. EditBrassKey – edits a card holder's physical key privileges. Image_export – exports images. Print – prints a badge. Query – queries for and displays a badge; provides program access from the Pro-Watch screen. Update – updates a badge. Void – voids a badge.
Badge Profiles	Provides the ability to create profiles in which the user can define fields and pages. These profiles make up the dialog where a user would configure badges and populate data for those badges for access. See "Badge Building" in Chapter 60. Add – adds a badge profile resource. Delete – deletes a badge profile resource. Query – queries for and displays a badge profile resource; provides program access from the Pro-Watch screen. Update – updates a badge profile resource.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Badge Status	Defines badge statuses (for example, “active,” “inactive,” and so on). See "Registry Management". Add – adds a badge status resource. Delete – deletes a badge status resource. Query – queries for and displays a badge status resource; provides program access from the Pro-Watch screen. Update – updates a badge status resource.
Badge Toolbar	Adds permissions for individual badge-in toolbar items.
Badge Type Maintenance	Defines badge types (for example, “contractor,” “standard employee,” and so on). See "DBC - Badge Types" in Chapter 32. Add – adds a badge type resource. Delete –deletes a badge type resource. Query – queries for and displays a badge type resource; provides program access from the Pro-Watch screen. Update – updates a badge type resource.
Badges	Provides the ability to query for badges. Query – queries for and displays badges
BLOB Type	Defines objects that contain graphic database items such as images, videos, sound, and even programs or fragments of code. These objects are called Binary Large Objects, or BLOBs. See "DBC - BLOB Types" in Chapter 33. Add – adds a BLOB type resource. Delete – deletes a BLOB type resource. Query – queries for and displays a BLOB type resource; provides program access from the Pro-Watch screen. Update – updates a BLOB type resource.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Brass Keys	Issues physical keys to doors. See "DBC - Brass Keys" in Chapter 34. Add – adds a brass key resource. Delete – deletes a brass key resource. Query – queries for and displays a brass key resource; provides program access from the Pro-Watch screen. Update – updates a brass key resource.
Card Format	Configures card formats, which define specific access privileges for the badge holder. See "DBC - Card Formats" in Chapter 35. Add – adds a card format resource. Delete – deletes a card format resource. Query – queries for and displays a card format resource; provides program access from the Pro-Watch screen. Update – updates a card format resource.
CCTV	Defines and configures CCTV channels. Add – adds a CCTV channel. Delete –deletes a CCTV channel. Query – queries for and displays a CCTV channel. Update – updates a CCTV channel.
CCTV Cameras	Defines and configures CCTV camera views. These camera views can be associated with logical devices or events. See "HW Config - CCTV" in Chapter 21. Add – adds a CCTV camera view. Delete – deletes a CCTV camera view. Query – queries for and displays a CCTV camera view; provides program access from the Pro-Watch screen. Update – updates a CCTV camera view.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
CCTV Commands	Defines and configures CCTV commands. These commands can be associated with logical devices or events. See "HW Config - CCTV" in Chapter 21. Add – adds a CCTV command. Delete – deletes a CCTV command. Query – queries for and displays a CCTV command; provides program access from the Pro-Watch screen. Update – updates a CCTV command.
CCTV Monitors	Defines and configures CCTV monitors. See "HW Config - CCTV" in Chapter 21. Add – adds a CCTV monitor. Delete – deletes a CCTV monitor. Query – queries for and displays a CCTV monitor; provides program access from the Pro-Watch screen. Update – updates a CCTV monitor.
CFR Maintenance	Provides update and signature functions.
Channel Maintenance	Provides the ability to add and configure channel types within hardware configuration. See "" in Chapter 6 for more about your specific hardware type. Add – adds a channel type. Delete – deletes a channel type. Dial – initiates dialup communication on a channel type. Hangup – hangs up a connection for a new dialup. Query – queries for and displays a channel type; provides program access from the Pro-Watch screen. Update – updates a channel type.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Class	Creates and maintains classes to which Pro-Watch privileges are assigned. See "DBC - Classes" in Chapter 36. Add – to adds a class. Delete –deletes a class. Query – queries for and displays a class; provides program access from the Pro-Watch screen. Update – updates a class.
Clearance Codes	Assigns access privileges company-wide. See "DBC - Clearance Codes" in Chapter 37. Add – adds a clearance code resource. Delete – deletes a clearance code resource. Query – queries for and displays a clearance code resource; provides program access from the Pro-Watch screen. Update – updates a clearance code resource.
Companies	Creates a company database element for which access privileges are granted. See "DBC - Companies" in Chapter 38. Add – adds a company resource. Delete – deletes a company. Query – queries for and displays a company resource; provides program access from the Pro-Watch screen. Update – updates a company resource.
Control Record	Defines the following server settings within the Pro-Watch shell: event log threshold, logical device tags, alternative names for “clearance code” and “logical device,” and company tab labels. You can also set the card number seed and create additional tabs for the Companies dialog box in Database Configuration. See "Server Options" in Chapter 5. Update - updates server options from the Pro-Watch shell.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Data Transfer Utility	Provides the ability to transfer large amounts of data from a source to a destination. See "Data Transfer Utility (DTU)". Run - opens the data transfer utility executable.
Default Events Maintenance	Defines the default events associated with various hardware. See "DBC - Default Events" in Chapter 40. Add – adds a default event. Query – queries for and displays a default event; provides program access from the Pro-Watch screen. Update – updates a default event.
Deferred Access	Restricts user access.
Device Types	Defines and configures the device types, which, in turn, are used to create logical devices. See "Configuring Device Types" in Chapter 6. Add – adds a device type. Delete – deletes a device type. Query – queries for and displays a device type; provides program access from the Pro-Watch screen. Update – updates a device type.
Dialup Schedule Maintenance	Establishes the frequency and time of day when the server uploads or downloads data to or from a remote panel via a dialup modem. See "DBC - Dial-Up Schedule" in Chapter 42. Add – adds a dialup schedule. Delete – deletes a dialup schedule. Query – queries for and displays a dialup schedule; provides program access from the Pro-Watch screen. Update – updates a dialup schedule.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Enable Codes	Enable Codes are codes that allow for feature add-ons. See "" in Chapter 6. Add – adds an enable code. Delete – deletes an enable code. Query – queries for and displays an enable code; provides program access from the Pro-Watch screen. Update – updates an enable code.
Event Actions	Event actions are the event procedures, which provide execution sequence of one or more commands. See "DBC - Event Procedures" in Chapter 43. Add – adds an event procedure. Delete – deletes an event procedure. Query – queries for and displays an event procedure; provides program access from the Pro-Watch screen. Update – updates an event procedure.
Event Codes	Add – adds an event code. Delete – deletes an event code. Query – queries for and displays an event code. Update – updates an event code.
Event Log	Logs all events that occur up to the maximum configured in server options. See "Tool Bar" in Chapter 1. View – queries within event log.
Event Log Manager	Clears event entries from the following logs: Unack Log - Clear All – Clears all entries in the Unacknowledged Log.
Event Monitor	Displays the events as they occur in the event viewer. See "Tool Bar" in Chapter 1. View – displays the event viewer.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Event Triggers	Trigger an event procedure when the conditions of the trigger are met.See "DBC - Event Triggers" in Chapter 44. Add – adds an event trigger. Delete – deletes an event trigger. Query – queries for and displays an event trigger; provides program access from the Pro-Watch screen. Update – updates an event trigger.
Event Types	Provides instructions on how to handle an event generated in Pro-Watch. See "DBC - Event Types" in Chapter 45. Add – adds an event type. Delete – deletes an event type. Query – queries for and displays an event type; provides program access from the Pro-Watch screen. Update – updates an event type.
Groups	Groups hardware or logical devices together as a single entity. See "DBC - Groups" in Chapter 47. Add – adds a group resource. Delete – deletes a group resource. Query – queries for and displays a group resource; provides program access from the Pro-Watch screen. Update – updates a group resource.
Guard Tours	Creates a facility walk-through that is defined by a series of reader checkpoints. See "DBC - Guard Tours" in Chapter 48. Add – adds a guard tour resource. Delete – deletes a guard tour resource. Query – queries for and displays a guard tour resource; provides program access from the Pro-Watch screen. Update – updates a guard tour resource.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Hardware Classes	Groups the system hardware into different hardware classes for organizational purposes; categorizes associated logical devices. See "Configuring Hardware Classes" in Chapter 6. Add – adds a hardware class. Delete – deletes a hardware class. Query – queries for and displays a hardware class; provides program access from the Pro-Watch screen. Update – updates a hardware class.
Hardware Templates	Determines the related template information. See "Configuring Hardware Templates" in Chapter 6. Add – adds a hardware template. Delete – deletes a hardware template. Query – queries for and displays a hardware template; provides program access from the Pro-Watch screen. Update – updates a hardware template.
Holidays	Modifies normal time zone behavior on a particular day. See "DBC - Holidays" in Chapter 49. Add – adds a CCTV monitor. Delete – deletes a CCTV monitor. Query – queries for and displays a CCTV monitor; provides program access from the Pro-Watch screen. Update – updates a CCTV monitor.
Input Point Maintenance	A logical device, configurable as monitorable input or as part of a door configuration. See "Configuring Device Types" in Chapter 6. Query – queries for and displays an input point; provides program access from the Pro-Watch screen. Update – updates an input point.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Intercoms	Supplement an access control system by allowing a dispatcher to communicate with an individual at an access point. See "HW Config - Intercom" in Chapter 23. Add – adds an intercom. Delete – deletes an intercom. Query – queries for and displays an intercom; provides program access from the Pro-Watch screen. Update – updates an intercom.
Keyboard Type	Configures a shortcut key, or a hot-key combination, that executes commands and event procedures. See "DBC - Keyboard Accelerator" in Chapter 50. Add – adds a keyboard accelerator. Delete – deletes a keyboard accelerator. Query – queries for and displays a keyboard accelerator; provides program access from the Pro-Watch screen. Update – updates a keyboard accelerator.
Logical Devices	Defines a single physical device or group of selected physical devices. See Adding a logical device corresponding to your specific hardware in "" in Chapter 6. Add – adds a logical device. Delete – deletes a logical device. Query – queries for and displays a logical device; provides program access from the Pro-Watch screen. Update – updates a logical device.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Map Build	Defines an engineering drawing, or floor plan, for your facility and enables you to add resources such as logical devices to the map. See "Map Building" in Chapter 61 or "DBC - Maps" in Chapter 51. Add – adds a map. AddResource – adds a resource to a map. CleanUp – refreshes a resource's data on a map. Delete – deletes a map. DelResource – deletes a resource on a map. EditResource – edits a resource on a map. Locate – locates a resource on a map. Query – queries for and displays map builder executable; provides program access from the Pro-Watch screen. Update – updates a map.
Modem Pool Maintenance	Creates a collection of modems from which Pro-Watch chooses to dial out to remote panels. See "DBC - Modem Pools" in Chapter 52. Add – adds a modem pool. Delete – deletes a modem pool. Query – queries for and displays a modem pool; provides program access from the Pro-Watch screen. Update – updates a modem pool.
Output Point Maintenance	A logical device, configurable as a controllable output or as part of a door configuration. See "Configuring Device Types" in Chapter 6. Query – queries for and displays an output point; provides program access from the Pro-Watch screen. Update – updates an output point.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Panel Maintenance	Panels can be added and configured to control hardware and access settings. See "" in Chapter 6 to learn more about your specific hardware type. Add – adds a panel. Delete – deletes a panel. Query – queries for and displays a panel; provides program access from the Pro-Watch screen. Update – updates a panel.
Partition Maintenance	Restricts user and class access to database resources. See "DBC - Partitions" in Chapter 53. Add – adds a partition. Delete – deletes a partition. Query – queries for and displays a partition; provides program access from the Pro-Watch screen. Update – updates a partition.
Pathway	Enables personnel to bypass designated security checkpoints after gaining initial access. See "DBC - Pathways" in Chapter 54. Add – adds a pathway. Delete – deletes a pathway. Query – queries for and displays a pathway; provides program access from the Pro-Watch screen. Update – updates a pathway.
Port Maintenance	Add – adds a port. Delete – deletes a port. Query – queries for and displays a port. Update – updates a port.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Reader Maintenance	A logical device configurable as a stand-alone reader, part of a door configuration, or part of an elevator configuration. See "Configuring Device Types" in Chapter 6. Query – queries for and displays a reader; provides program access from the Pro-Watch screen. Update – updates a reader.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Reports	Provides a comprehensive report of any Pro-Watch data group. See "" in Chapter 4. Area Attendance Report – displays the area attendance report. AuditLog – displays the audit log report. BadgeProfile – displays the badge profile report. BadgeTypes – displays the badge types report. BdgAccess – displays the badge holder access to a logical device report. BdgDetail – displays the badge holder detail report. BdgSumm – displays the badge holder summary report. CardStatus – displays the card status report. Channel – displays the channel configuration report. CHIP Panel Configuration – displays the CHIP panel configuration report. Class – displays the classes report. ClearBadge – displays the clearance code/badge access report. ClearCode – displays the clearance codes report. CompClear – displays the company clearance codes report. CompDetail – displays the company detail report. CompSumm – displays the company summary report. D600AP_Panel – displays the D600AP panel configuration report. DataTables – displays the database tables report. Design – designs a report.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Reports (continued)	DeviceTypes – displays the device types report. Dialup – displays the dialup schedules report. EventPoints – displays the event points report. EventProc – displays the event procedures report. EventTypes – displays the event types report. EvLog – displays the event log report. Guard Tour Configurations – displays the guard tours report. HWClass – displays the hardware classes report. HWTemplate – displays the hardware templates report. KeyAssign – displays the key assignment list report. KeyList – displays the brass key list report. LastAccess – displays the last access by a badge holder report. LastReader – displays the last access at a logical device report. LDAccess – displays the logical device access by a badge holder report. LogicalDev – displays the logical devices report. ModemPool – displays the modem pools report. Muster – displays the mustering report. OpLog – displays the operator log report. PanelTypes – displays the panel types report. Partitions – displays the partitions report.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Reports (continued)	Printers – displays the printers report. PW2000Panel – displays the PW2000 panel configuration report. PW5000Panel – displays the PW-5000 panel configuration report. RespCodes – displays the response codes report. RouteGroups – displays the routing groups report. SEEPPanel – displays the SEEP panel configuration report. TimeZones – displays the time zones report. UIDSumm – displays the user summary report. UserDetail – displays the user detail report. Workstations – displays the workstations report.
Response Codes	Provides a prepared response that can be used reply to an alarm. See "Response Codes" in Chapter 3. Add – adds a response code. Delete – deletes a response code. Query – queries for and displays a response code; provides program access from the Pro-Watch screen. Update – updates a response code.
Routing Groups	Determines which events will appear on a user's Alarm Monitor. See "DBC - Routing Groups" in Chapter 55. Add – adds a routing group. Delete – deletes a routing group. Query – queries for and displays a routing group; provides program access from the Pro-Watch screen. Update – updates a routing group.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Site Maintenance	A site refers to the area of controlled access. You must configure a site before adding a channel, panel, and any logical devices. See "" in Chapter 6 to learn more about your hardware type. Add – adds a site. Delete – deletes a site. Query – queries for and displays a site; provides program access from the Pro-Watch screen. Update – updates a site.
Status Groups	Provides the ability to group logical devices for which real-time status is displayed. See "DBC - Status Groups" in Chapter 56. Add – adds status group. Delete – deletes a status group. Query – queries for and displays a status group; provides program access from the Pro-Watch screen. Update – updates a status group.
Subpanel Maintenance	Provides the ability to add inputs, outputs, or readers. Subpanels are attached to panels. See "" in Chapter 6 to learn more about your hardware type. Add – adds a subpanel. Delete – deletes a subpanel. Query – queries for and displays a subpanel; provides program access from the Pro-Watch screen. Update – updates a subpanel.
System Toolbar	Adds permissions for individual system toolbar items.

Table B-1 Programs Assignable to Classes and Users (continued)

Program	Description and Available Program Functions
Table Maintenance	Add – adds to a table. Delete – deletes from a table. Log_ctrl – enables logging on a table. Query – queries for and displays a table; provides program access from the Pro-Watch screen. Update – updates a table.
Time Zone Def	Provides the ability to specify time periods for which access is allowed. See "DBC - Time Zones" in Chapter 57. Add – adds a time zone. Delete – deletes a time zone. Query – queries for and displays a time zone; provides program access from the Pro-Watch screen. Update – updates a time zone.
User Defines	Provides the ability to set up user access accounts. See "DBC - Users" in Chapter 58. Add – adds a user. Delete – deletes a user. Query – queries for and displays a user; provides program access from the Pro-Watch screen. Update – updates a user.
Workstation	Provides the ability to add workstations to the Pro-Watch network, delete the workstations, or modify their configurations. See "DBC - Workstations" in Chapter 59. Add – adds a workstation. Delete – deletes a workstation. Query – queries for and displays a workstation; provides program access from the Pro-Watch screen. Update – updates a workstation.

B.2 Commands Assignable to Event Procedures

The table below lists the commands that are available for an event procedure to execute. See "DBC - Event Procedures" in Chapter 43, for information about executing these commands in event procedures.

Table B-2 Commands Assignable to Event Procedures

Program	Description
Unmask Input	Unmasks the input point.
Mask Input	Masks the input point.
Software Unmask Input	Unmasks events at the software level.
Software Mask Input	Masks events at the software level.
Activate Output	Activates the output device.
Deactivate Output	Deactivates the output device.
Pulse Output	Momentarily activates the output device.
Unlock Doors	Unlocks the doors.
Lock Doors	Locks the doors.
Re-enable Doors	Returns the doors to normal operation.
Momentary Unlock	Unlocks the door momentarily.
Change Reader Threat Level	Changes the door access threat level. If the threat level of the card is not equal to or greater than the threat level assigned to the reader, then that card will not have access.
Timed Override	Sets up an override of a reader's timed unlock.
Enable Reader Cypher Mode	Activates an entry keypad at the reader.
Disable Reader Cypher Mode	Deactivates an entry keypad at the reader.
Download Date and Time to Panels	Downloads the current date and time to the active panels.
Send Message to a Channel	Sends a hardware-defined text message to a channel.

Table B-2 Commands Assignable to Event Procedures (continued)

Program	Description
Run Stored Procedure	Runs a designated stored procedure. Note that you do not precede the stored procedure name with the word “exec” in the Stored Procedure field on the Define Event Procedure dialog box.
Run an Executable	Not supported in Pro-Watch Release 5.0.
Run a Report	Runs the specified report.
Issue an Event	Issues an event for a specified logical device.
External Table Entry	Not supported in Pro-Watch Release 5.0.
Download a Clearance Code	Downloads a clearance code to the panel.
Execute CCTV Command	Executes a CCTV command.
Set Reader to Card Only	Sets a specified reader to card only, in which only a card will be needed to gain access.
Set Reader to Card and PIN	Sets a specified reader to card and PIN, in which a card and a PIN will be needed to gain access.
Set Reader to Card or PIN	Sets a specified reader to card or PIN, in which a card or a PIN can be used to gain access.
Set Reader to PIN Only	Sets a specified reader to PIN only, in which only a PIN will be needed to gain access.
Set Reader to Facility Mode	Sets a specified reader to facility mode.
Forgive Anti-passback	Forgives anti-passback on a an applicable logical device associated with a specified channel.
Timed Masked Input	Masks an input point for a specified amount of time.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Dial-Up Configuration

C

In this appendix ...

Overview

PW-5000/3000 Dial-up Configuration

PW2000 Dial-Up Configuration

CHIP (Star II) Dial-up Configuration

SEEP Dial-up Configuration

Cardkey Dial-up Configuration

C.1 Overview

This appendix explains how to set up and connect a Dial-up channel for the following panels using Pro-Watch software:

- PW-5000/3000
- PW2000
- CHIP (Star II)
- SEEP
- Cardkey

This guide assumes that you are familiar with the basic principles of configuring your Operating System and Pro-Watch. The manual also assumes that you have Administrator privileges for both your Operating System and Pro-Watch software.

C.2 PW-5000/3000 Dial-up Configuration

C.2.1 PW-5000/3000 Dial-In

To configure Dial-In for the PW-5000/3000 panel:

1. Connect the serial cable from the host modem to the communication port on the host. The modem connects to the PC using a standard modem cable. In most cases, the cable will be a DB25 (modem) to DB9 (serial COM port). The remote modem requires a custom cable to be manufactured. This cable will be a DB25 (modem) and terminate to the PW-5000 IC Port 1 Terminal Block. Note that the IC port must be Port 1. See the diagram below for connection details.

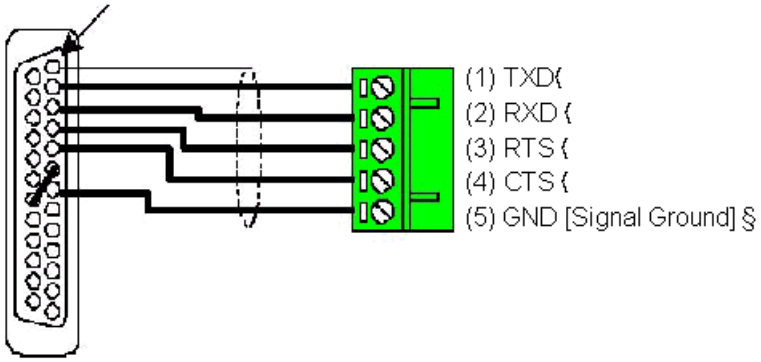


Figure C-1 PW-5000/3000 Connections

2. In Pro-Watch, open *the Hardware Configuration* window by clicking on the Hardware Configuration Icon in the Viewer window.

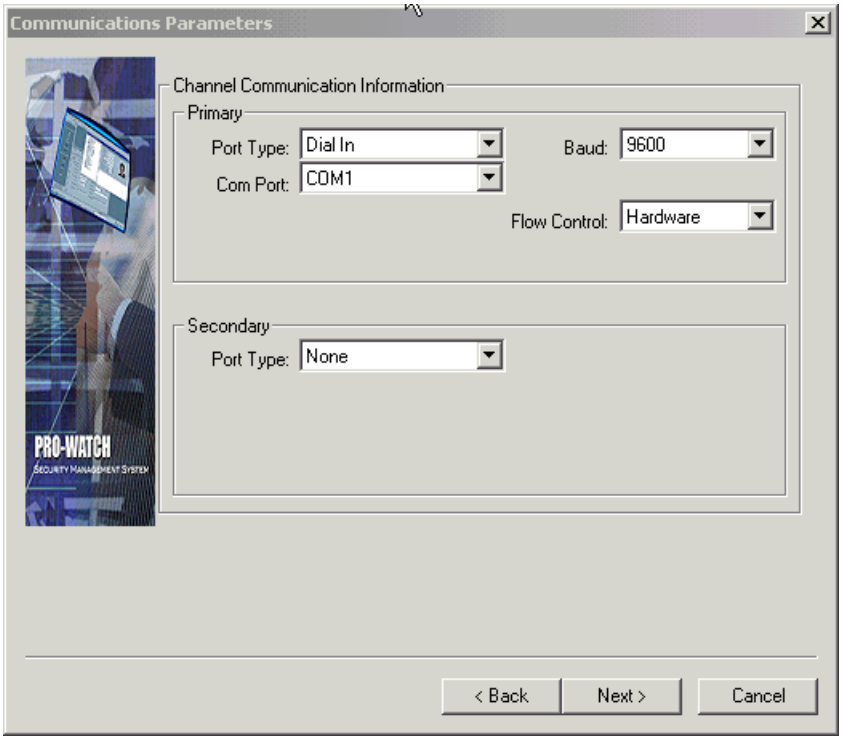
3. Create a new site. Right click in the window and select **New > Site** to display the **Site Record tab** of the **Edit Sites** screen.
4. In the **Site Record tab** of the **Edit Sites** screen, enter the **Site ID**, a **Description**, and the communication server for the **Workstation**. Click **OK** to continue.
5. Create a **Dial-In** channel in Pro-Watch. See "HW Config - PW-6000/5000/3000" in Chapter 9. At the Communications Parameters dialog box:

   a. Select Dial-In as the Port Type.

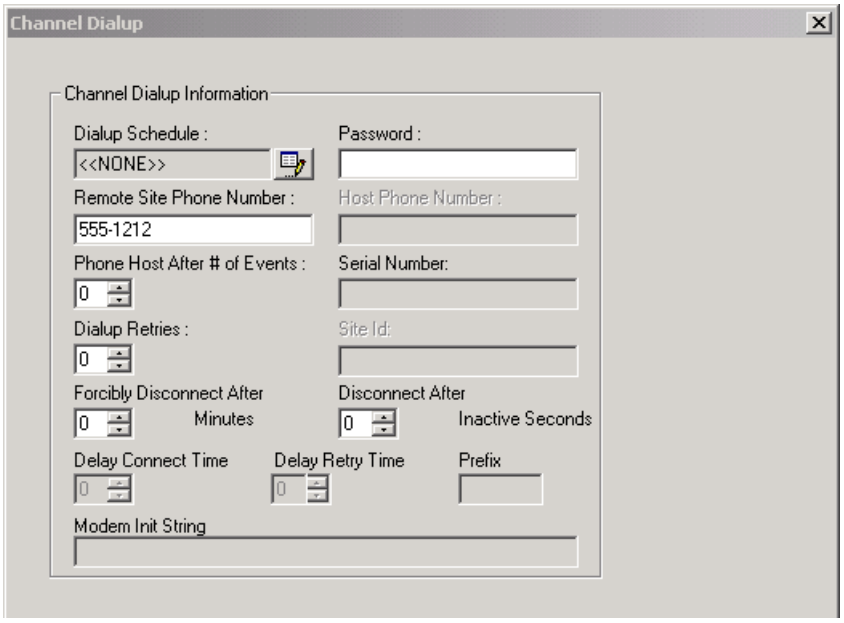
   b. Select the communication port to which the modem is connected.

   c. Select the Baud Rate at which to connect.

d. Select **Hardware** from the Flow Control drop-down list:



Note: Configure the Channel Dial-up information. See "HW Config - PW-6000/5000/3000" in Chapter 9. At the Channel Dialup dialog box, enter the remote site phone number. You cannot enter a Host Phone Number in this dialog box. This information is accessed at the panel level.



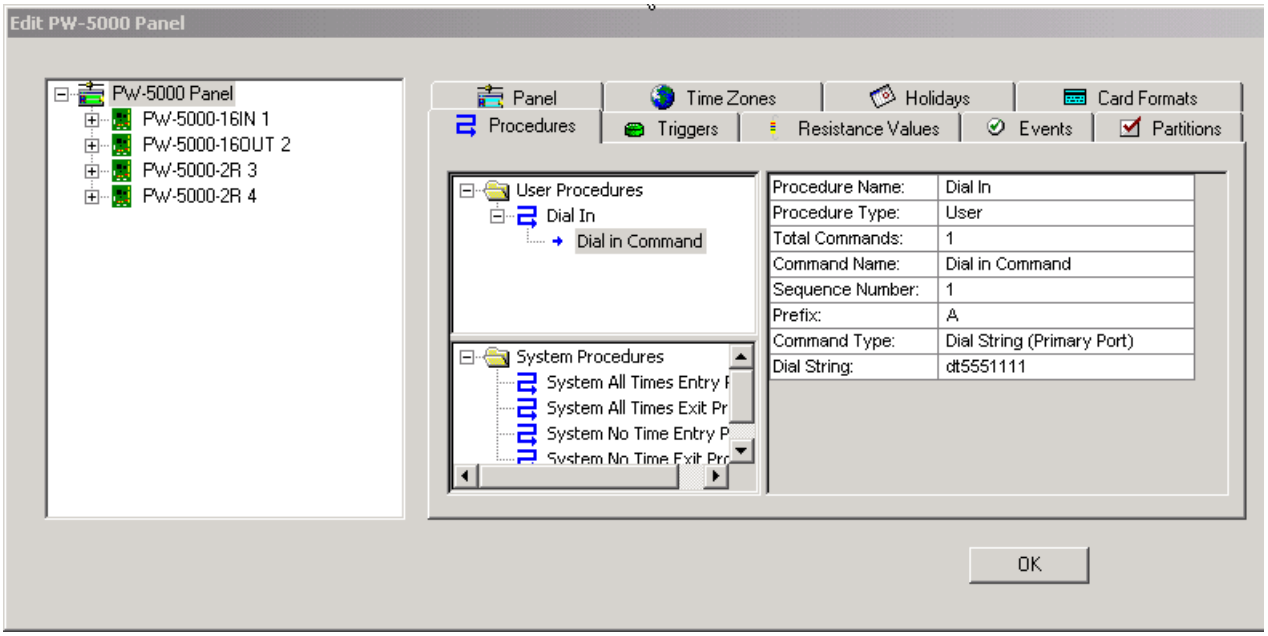
6. After the site, channel, panel, and logical devices are added, edit the panel and create a panel trigger and procedure to initiate dial-in.

To create a panel procedure:

1. From the Edit [Panel Name] Panel dialog box, select the **Procedures** tab.
2. In the User Procedures window, right click and select **Add Procedure**.
3. In the Procedure Name field, enter the Procedure Name.
4. In the tree of user procedures, right click the procedure name and select **Add Command**.
5. Enter the Command Name.
6. Right-click the prefix field, and select the prefix from the drop-down list.
7. Right-click the Command Type field and select **Dial String (Primary Port)** from the drop-down list.
8. Enter the Dial String, and precede it with "dt." For example, "dt5551234." Note that in the dial string, the AT command is omitted.

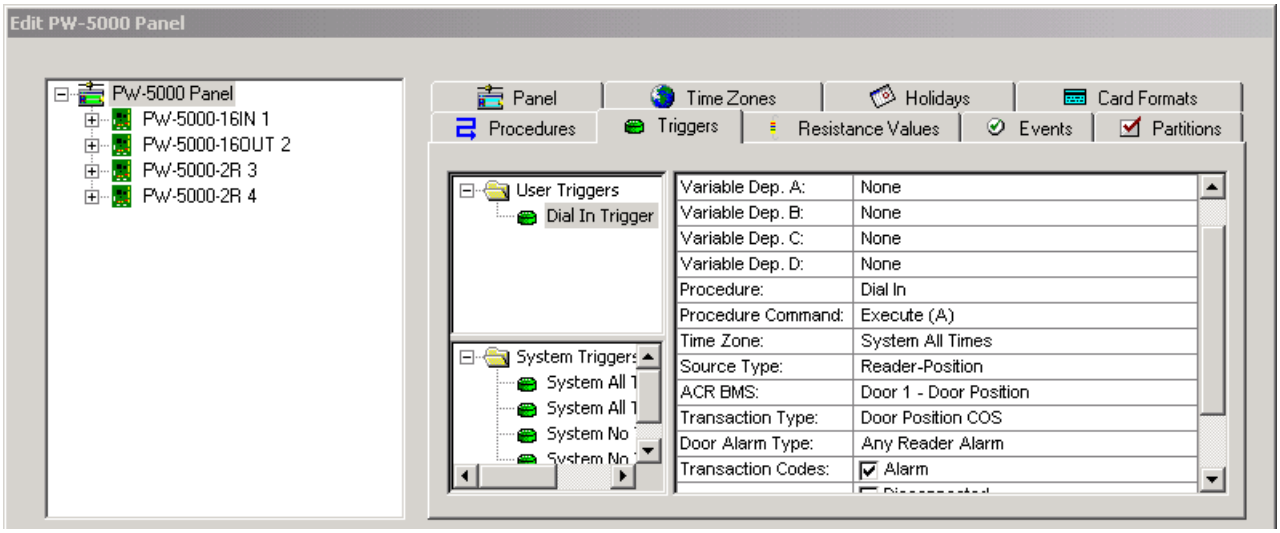
To create a panel trigger:

1. Display the Edit [panel name] Panel dialog box:



2. Select the **Triggers** tab.
3. Enter the Description.
4. Select the procedure created for dial-in.
5. Select the Procedure Command. For example, if you selected **A** for the Prefix in the procedure, then you would select **Execute (A)** in the trigger.

6. Select the Time Zone from the drop-down list.
7. Select the Source Type from the drop-down list. The example provided shows a source type of Reader-Position.
8. Select the Transaction Type. The example provided shows a transaction type of Door Position COS or change of state. To complete the example, the **Alarm** checkbox is selected for the Transaction Code.
9. Click **OK** to save the panel trigger and procedure configuration.



10. Set the DIP switches for the Server (host). The settings in this table assume the use of external US Robotics modems for both the Server (host) and the PW-5000 controller (remote modem).

Table C-1 Server (Host) Modem DIP Switch Settings

Switch	Position	Description
1	Up	DTR provided by PC
2	Up	Verbal result codes
3	Down	Result codes displayed
4	Down	Echo offline commands disable
5	Down	Auto Answer off
6	Up	Carrier detect normal
7	Up	Loads NVRAM defaults
8	Down	Smart mode

11. Set the DIP switches for the PW-5000 controller (remote) modem according to the following table. The settings in this table assume the use of external US Robotics modems for both the Server (host) and the PW-5000 controller (remote modem).

Table C-2 PW-5000 Controller (Remote) Modem DIP Switch Settings

Switch	Position	Description
1	Down	DTR provided by PC
2	Up	Verbal result codes
3	Down	Result codes displayed
4	Down	Echo offline commands disable
5	Down	Auto Answer off
6	Up	Carrier detect normal
7	Up	Loads NVRAM defaults
8	Down	Smart mode

12. Connect the PC modem to the host computer.
13. Install the US Robotics 56K FAX EXTERNAL driver (Not the US Robotics 56K FAX EXTERNAL PnP driver). Use the Universal INF file (mdmusr01.inf) supplied by US Robotics at the following web address: http://www.usrobotics.com/support/driverstemplate.asp?prod=s-modem - 568603 .
14. Enter "**Phone and Modem Options**" by clicking on **Start> Settings> Control Panel> Phone and Modem Options**.
15. Click the **Modem** tab and go into the properties of the **US Robotics** modem.
16. Set the **Maximum Port Speed** to **9600** baud.
17. Click the **Advanced** tab and enter the following string in **the Extra Initialization Commands**: **ATX4&A3&B1&H1&N0&P0&R2&W0&W1**

    Note: On Windows 2008 R2 x64 installations, under **Phone and Modem Options**, let Windows search for new hardware and install the modem driver but DO NOT enter the initialization string. Leave the field blank.
18. Click the **Diagnostics** tab and select **Query Modem**.

19. Check the modem strings and verify that they match the PC modem string below. If not make the appropriate changes.

PC Modem Strings	Remote Modem Strings
AT&R2&W0&W1	AT&R2&W0&W1
ATI4 Report in Hyper Terminal	ATI4 Report in Hyper Terminal
B0 E0 F1 M1 Q0 V1 X4 Y0 Baud=9600 Parity=N Worlen=8 Dial=Tone On Hook CID=0	B0 E0 F1 M1 Q0 V1 X4 Y0 Baud=9600 Parity=N Worlen=8 Dial=Tone On Hook CID=0
&A3 &B1 &C1 &D2 &G0 &H1 &I0 &K1 &M4 &N0 &P0 &R2 &S0 &T5 &U0 &Y1	&A3 &B1 &C1 &D2 &G0 &H1 &I0 &K1 &M4 &N0 &P0 &R2 &S0 &T5 &U0 &Y1

20. Repeat steps 13-19 for the remote modem.

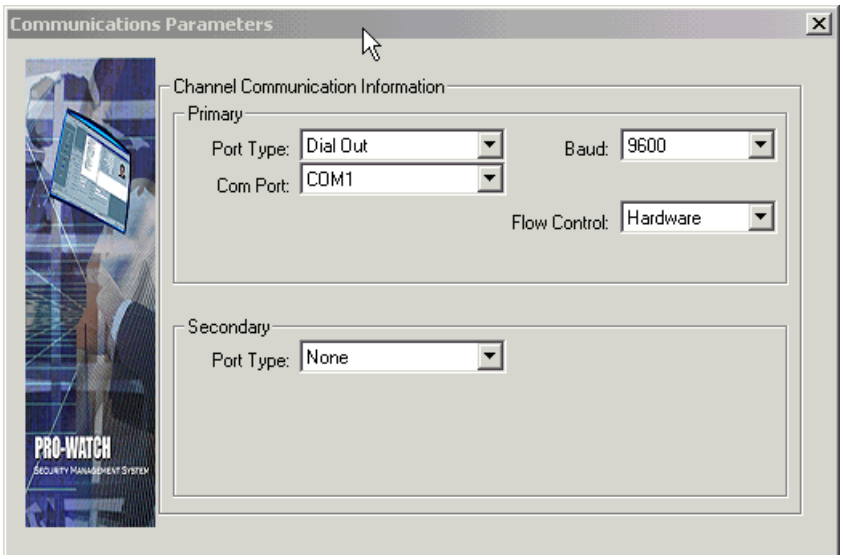
Notes:

- The PW-5000/3000 panels cannot have a daughter board connected while trying to connect via modems.
- When using the PW-3000 panel, jumper 14 needs to be on. (on= direct RS232 or RS485 / off = Ethernet).
- When using modems for redundant communications (port 2), DIP switch 4 on the IC needs to be set “ON”.
- When using the Digi Boards, you will need the 25 pin CAN (part number NTEXPC25), not the 9 pin CAN.

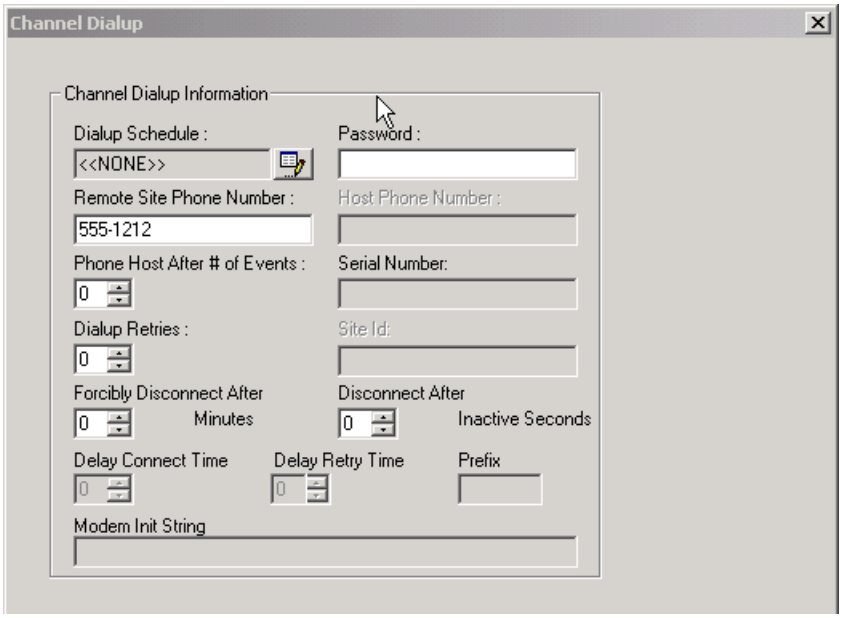
C.2.2 PW-5000/3000 Dial-Out

To configure dial-out for the PW-5000/3000 panel:

1. Connect the serial cable from the host modem to the communication port on the host.
2. The remote modem requires a custom cable to be manufactured. This cable will be a DB25 (modem) and terminate to the PW-5000 IC Port 1 Terminal Block.
3. Create a **Dial-Out** Channel in Pro-Watch. See "HW Config - PW-6000/5000/3000" in Chapter 9. At the Communications Parameters dialog box:
   a. Select Dial Out for the primary port type.
   b. Select the Comm Port being used for this connection.
   c. Select 9600 from the Baud Rate drop-down list.
   d. Select **Hardware** from the Flow Control drop-down list.



4. Configure the Channel Dial-up Information. See "Set CHIP Communications Parameters" in Chapter 10 for field descriptions. At the Channel Dialup dialog box, enter the remote site phone number.



5. After the channel, panel, and logical devices are configured, right-click the channel and select **Actions** > **Manual Dialup**.
6. Use the following DIP switch settings to configure the host modem. Note that the settings are based on the use of an external US Robotics modem.

DIP Switch	Setting
Sw.1	Up - DTR provided by PC.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Down - Auto answer off.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down - Smart Mode.

7. Use the following DIP switch settings to configure the remote modem. Note that the settings are based on the use of an external US Robotics modem.

DIP Switch	Setting
Sw.1	Down - DTR provided by modem.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Down - Auto answer off.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down

8. If you are using a modem, configure the following DIP switches and jumpers:

DIP Switch	Setting	Description
Sw.1	On*	Switches 1 - 4 are used for addressing the IC. Set the switches to the required address. (* The example provided is for address 1.)
Sw.2	Off*	
Sw.3	Off*	
Sw.4	Off*	
Sw.5	On	TX enabled by CTS.
Sw.6	On	Baud rate 9600.
Sw.7	Off	Baud rate 9600.
Sw.8	Off	No password required.

Jumper	Position	Description
Port 1		
J4	2-3	Port 1 RS232.
J5	2-3	
J6	2-3	
Port 2 (if used)		
J13	2-3	Port 1 RS232.
J14	2-3	
J15	2-3	

Consider these points when you configure dial-up for the PW-5000/3000 panels:

- The PW-5000/3000 panels cannot have a daughter board connected while trying to connect via modems.
- When using the PW-3000 panel, jumper 14 (J14) needs to be on. On = direct RS232 or RS485. Off = Ethernet.
- When using modems for redundant communications (Port 2), DIP switch 4 on the IC needs to be set to "on."
- When using the Digi Boards, you will need the 25-pin CAN (part number NTEXPC25), instead of the 9-pin CAN.

C.3 PW2000 Dial-Up Configuration

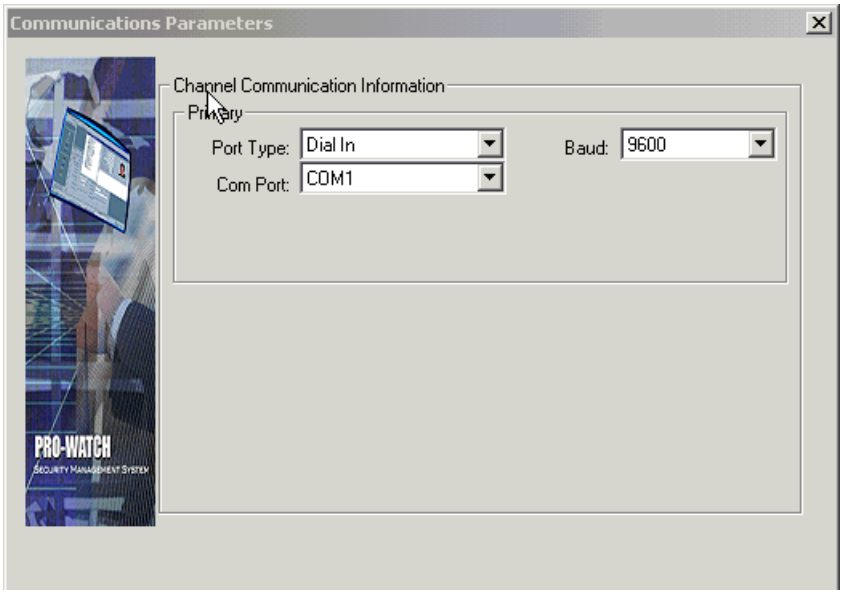
C.3.1 PW2000 Dial-In

To configure dial-in for the PW2000 panel:

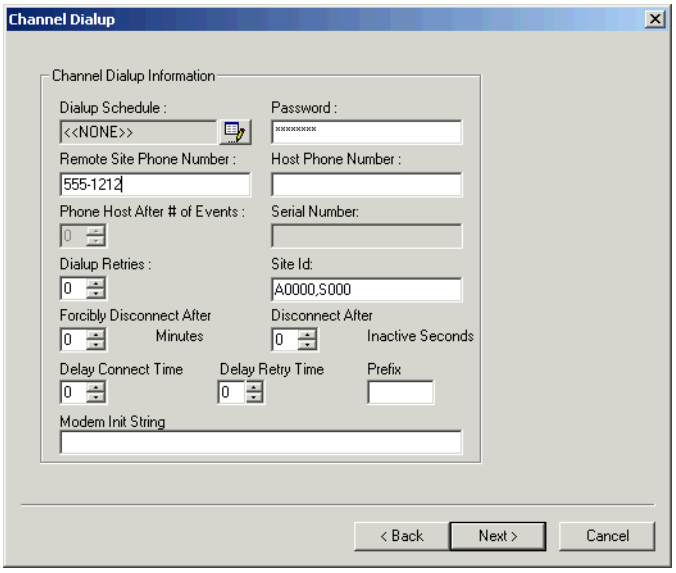
1. Connect the serial cable from the host modem to the communication port on the host.
2. Connect the serial cable from the host port of the ACU to the remote modem.
3. Create a **Dial-In** Channel in Pro-Watch. See "Adding a PW2000 Channel" in Chapter 7. At the Communications Parameters dialog box:

   a. Select the communication port to which the modem is connected.

   b. Select the Baud Rate at which to connect.



4. Configure the Channel Dial-up Information. See "Adding a PW2000 Channel" in Chapter 7. At the Channel Dialup dialog box:
   a. Enter the remote site phone number.
   b. Ignore the Phone Host After # of Events field, since this feature is not supported on the PW2000 panel.
5. After the channel, panel, and logical devices are configured at the panel, initiate events until you exceed the threshold (maximum number of events). The panel will attempt to dial-in to the host.
6. Use the following table to configure the host modem DIP switch. Note that the settings are based on the use of an external US Robotics modem.



DIP Switch	Setting
Sw.1	Up - DTR provided by PC.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Down - Auto answer off.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down - Modem smart mode.

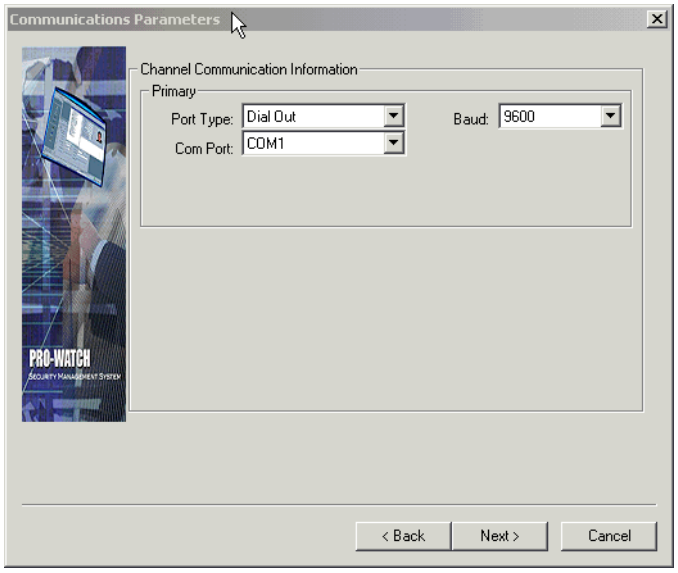
7. Use the following table to configure the remote modem DIP switch. Note that the settings are based on the use of an external US Robotics modem.

DIP Switch	Setting
Sw.1	Down - DTR provided by modem.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Down - Auto answer off.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down - Modem smart mode.

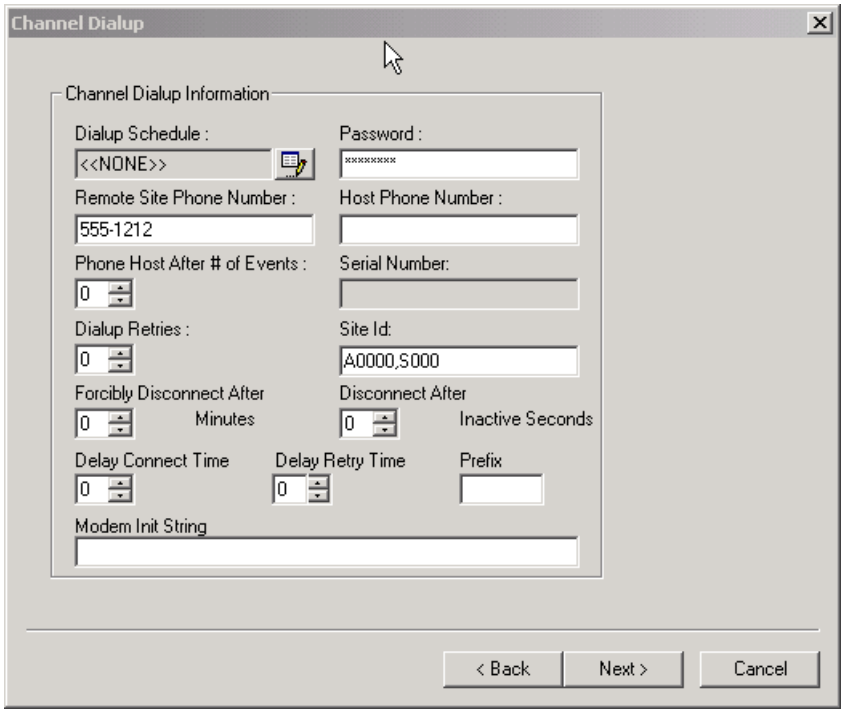
C.3.2 PW2000 Dial-Out

To configure dial-out for the PW2000 panel:

1. Connect the serial cable from the host modem to the communication port on the host.
2. Connect the serial cable from the host port of the ACU to the remote modem.
3. Create a **Dial-Out** Channel in Pro-Watch. See "Adding a CHIP Channel" in Chapter 10. At the Communications Parameters dialog box:
   a. Select the communication port to which the modem is connected.
   b. Select the Baud Rate at which to connect.



4. Configure the Channel Dial-up Information. See "Adding a CHIP Channel" in Chapter 10. At the Channel Dialup dialog box, enter the remote site phone number.



5. After the channel, panel, and logical devices are configured, right-click the channel and select **Actions** > **Manual Dialup**.

Note: Use the following table to configure the Host Modem DIP switch.

The DIP switch settings are based on the use of an external US Robotics modem. Also note that the host modem baud rate and connection should be set no higher than 9600.

DIP Switch	Setting
Sw.1	Up - DTR provided by PC.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Down - Auto answer off.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down - Modem smart mode.

6. Use the following table to configure the Remote Modem DIP switch. Note that the DIP switch settings are based on the use of an external US Robotics modem. Also note that auto answer must be "on."

DIP Switch	Setting
Sw.1	Down - DTR provided by modem.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Up - Auto answer on.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down - Modem smart mode.

Note: To dial out successfully on a PW2000 panel, the following must be true:

- The PCI requires a HUB chip to be inserted into the U1 socket.
- DIP switches 5 (HUB) and 6 (ACK/Nack) must be in the off position.
- Reset the PCI. See your PW2000 panel installation guide for more information.

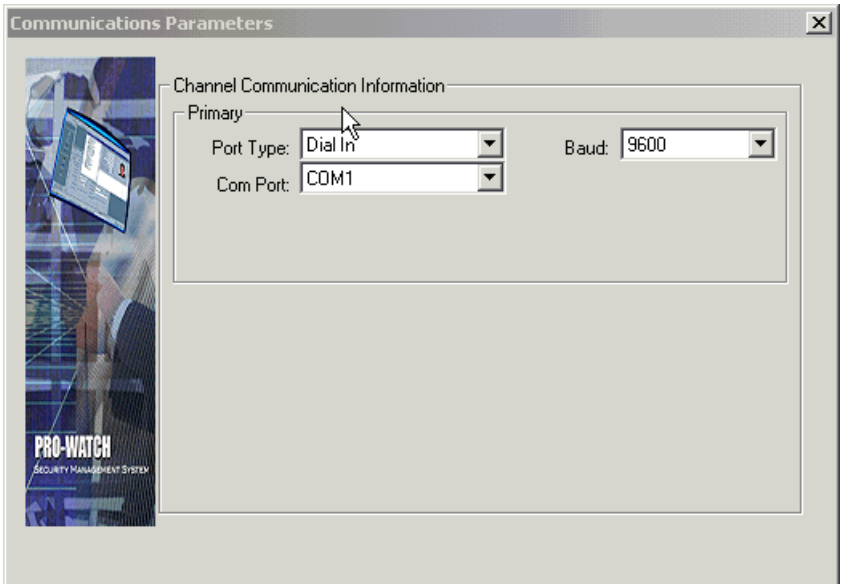
C.4 CHIP (Star II) Dial-up Configuration

C.4.1 CHIP (Star II) Dial-In

To configure dial-in for the Star II panel:

1. Open the Hyperterminal application.
   a. Select the Bits per Second from the drop-down list.
   b. Select **8** from the Data Bits drop-down list.
   c. Select **None** from the Parity drop-down list.
   d. Select **1** from the Stop Bits drop-down list.
   e. Select **None** from the Flow Control drop-down list.
   f. Click **OK**.

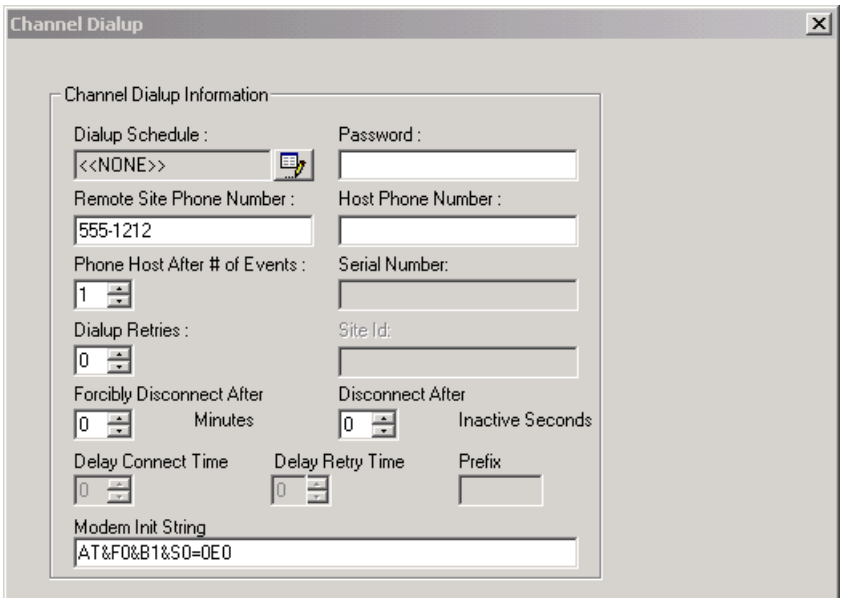
2. Press the **ESC** Key.
3. Enter the logon name.
4. Enter the password.
5. Select the **Modem Configuration Menu** (Choice 3).
   a. Select **Enable/Disable Modem** (Choice 1) and Enter **Y** (Yes).
   b. Select **Enable/Disable Callback** (Choice 2) and Enter **N** (No).
   c. Select **Set Telephone Number**. This is number for the Host.
   d. Select **Set Number of Retries**. This defines how many times the modem will try to connect.
   e. Select **Set Modem Initialization String**. Enter **AT&F0&B1&S0=0E0**.
   f. Select **Set Record Event Threshold**. This is the number of events in the Buffer.
6. Connect the serial cable from the host modem to the communication port on the host.
7. Connect the serial cable from the host port of the ACU to the remote modem.
8. Create a **Dial-In** Channel in Pro-Watch. See "Adding a CHIP Channel" in Chapter 10. At the Communications Parameters dialog box:
   a. Select the communication port to which the modem is connected.
   b. Select the Baud Rate at which to connect.
   c. Set the panel address to **1,** either via terminal or DIP switches.



9. Configure the Channel Dial-up Information. See "Set CHIP Communications Parameters" in Chapter 10. At the Channel Dialup dialog box:

   a. Set the Phone Host After # of Events to a minimum of **1.**

   b. Enter the Modem Init String as **AT&F0&B1&S0=0E0**.



10. After the channel, panel, and logical devices are configured (see "HW Config - CHIP" in Chapter 10), at the panel, initiate events until you exceed the threshold (maximum number of events). The panel will attempt to dial in to the host.

11. Use the following table to configure the DIP switch settings for the Star II (CHIP) ACU Modems. Note that these setting are for use with

the external US Robotics 56k V.90 modems for both the host and remote modem.

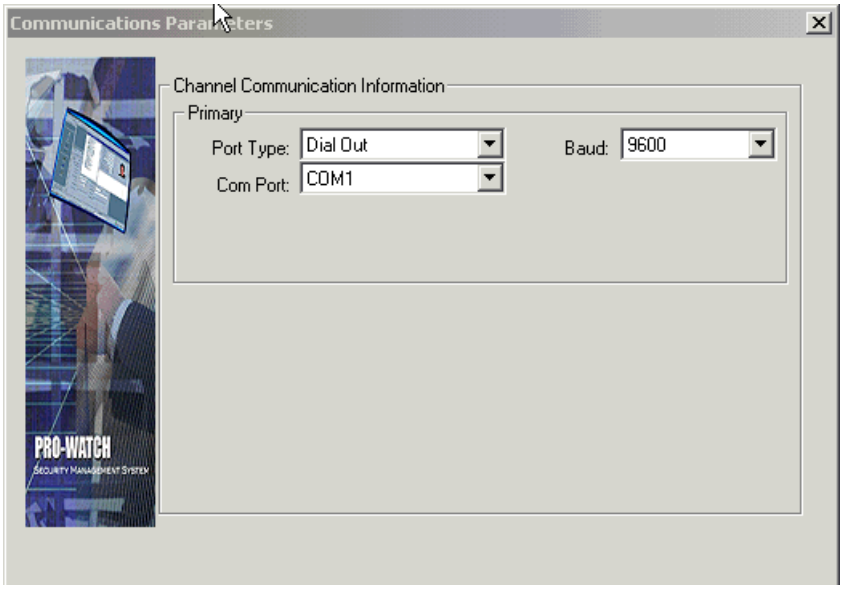
DIP Switch	Setting
Sw.1	On (down) - Ignore DTR.
Sw.2	Off (up) - Verbal result codes.
Sw.3	On (down) - Display result codes.
Sw.4	On (down) - No Echo, offline commands.
Sw.5	On (down) - Answer on ACU command.
Sw.6	Off (up) - Carrier detect normal.
Sw.7	Off (up) - Load NVRAM defaults.
Sw.8	On (down) Modem smart mode.

C.4.2 CHIP (Star II) Dial-Out

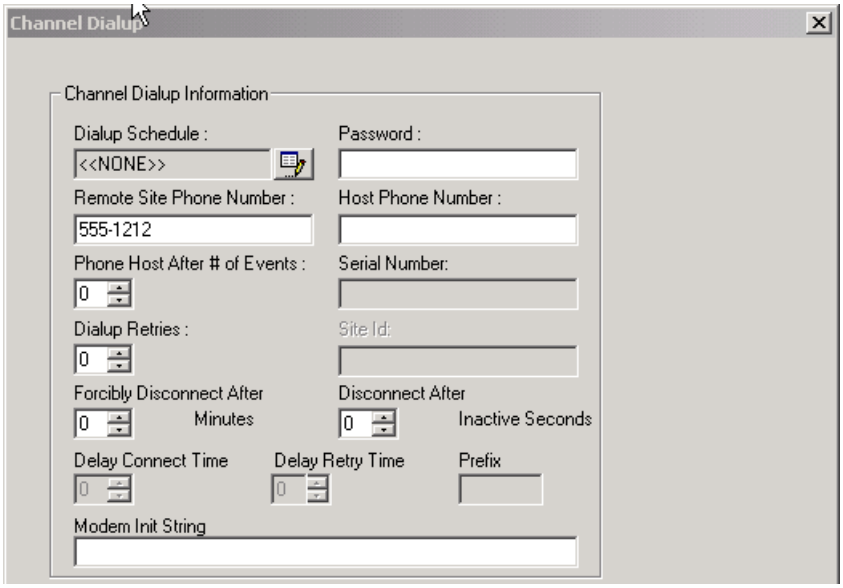
To configure dial-out capability for the Star II (CHIP) panel:

1. Open the Hyperterminal application.
   a. Select the Bits per Second from the drop-down list.
   b. Select **8** from the Data Bits drop-down list.
   c. Select **None** from the Parity drop-down list.
   d. Select **1** from the Stop Bits drop-down list.
   e. Select **None** from the Flow Control drop-down list.
   f. Click **OK**.
2. Press the **ESC** Key.
3. Enter the logon name.
4. Enter the password.
5. Select the **Modem Configuration Menu** (Choice 3)
6. Select **Enable/Disable Modem** (Choice 1), and Enter **Y** (Yes).
7. Return to the **Modem Configuration Menu.**
   a. Select choice 2.
   b. Select choice 12 to reset the panel.

8. Connect the serial cable from the host modem to the communication port on the host.
9. Connect the serial cable from the host port of the ACU to the remote modem.
10. Create a **Dial-Out** Channel in Pro-Watch. See "Adding a PW-6000/5000/3000 Channel" in Chapter 9. At the Communications Parameters dialog box:
    a. Select the communication port to which the modem is connected.
    b. Select the Baud Rate at which to connect.



11. Configure the Channel Dial-up Information. See "Set CHIP Communications Parameters" in Chapter 10.



12. After the channel, panel, and logical devices are configured (see "" in Chapter 6), right click the channel and select **Actions** > **Manual Dialup**.
13. Use the following table to configure the DIP switch settings for the Star II (CHIP) ACU Modems. Note that these settings are for use with the external US Robotics 56k V.90 modems for both the host and remote modem.

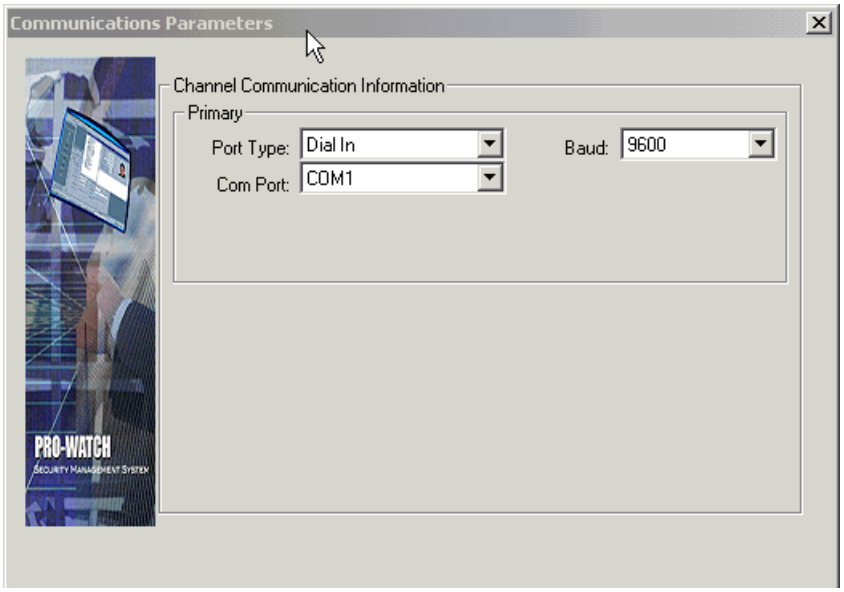
DIP Switch	Setting
Sw.1	On (down) - Ignore DTR.
Sw.2	Off (up) - Verbal result codes.
Sw.3	On (down) - Display result codes.
Sw.4	On (down) - No Echo, offline commands.
Sw.5	On (down) - Answer on ACU command.
Sw.6	Off (up) - Carrier detect normal.
Sw.7	Off (up) - Load NVRAM default.
Sw.8	On (down) Modem smart mode.

C.5 SEEP Dial-up Configuration

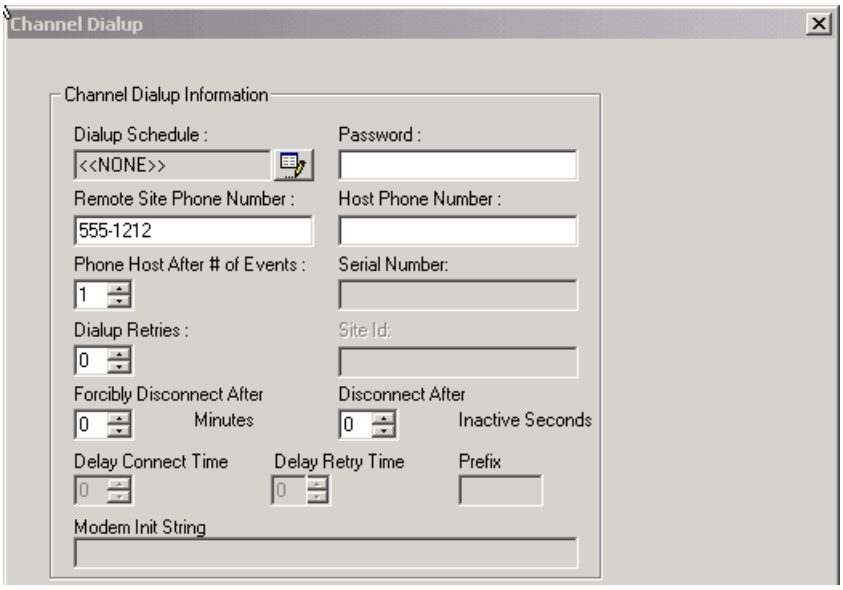
C.5.1 SEEP Dial-In

To configure dial-in for the SEEP panels:

1. Open the Hyperterminal application.
   a. Select Bits per Second from the drop-down list.
   b. Select **7** from the Data Bits drop-down list.
   c. Select **Odd** from the Parity drop-down list.
   d. Select **1** from the Stop Bits drop-down list.
   e. Select **None** from the Flow Control drop-down list.
   f. Click **OK**.
2. Press the **Space Bar** key.
3. Enter the password and press the **Enter** key.
4. Enter **Modem** and press the **Enter** key.
   a. Select **Enable/Disable Modem** (Choice 1) and Enter **Y** (Yes).
   b. Select **Enable/Disable Callback** (Choice 2) and Enter **N** (No).
   c. Select **Set Telephone Number**. This is number for the host.
   d. Select **Set Number of Retries**. This defines how many times the modem will try to connect.
   e. Select **Set Record Event Threshold**. This is the number of events in the buffer.
5. Connect the serial cable from the host modem to the communication port on the host.
6. Connect the serial cable from the host port of the ACU to the remote modem.
7. Create a **Dial-In** Channel in Pro-Watch. See "Adding a SEEP Channel" in Chapter 13. At the Communications Parameters dialog box:
   a. Select the communication port to which the modem is connected.
   b. Select the Baud Rate at which to connect.
   c. Set the panel address to **1** either via terminal or DIP switches.



8. Configure the Channel Dial-up Information. See "Set Communications Parameters" in Chapter 13. The Phone Host After # of Events must be set to a minimum of **1**.



9. After the channel, panel, and logical devices are configured (see "HW Config - SEEP" in Chapter 13), initiate events at the panel until you exceed the threshold (maximum number of events). The panel will attempt to dial in to the host.

10. Use the following table to configure the DIP switch for the SEEP ACU Modems. Note that these settings are for use with the external US Robotics 56k V.90 modems for both the host and remote modem.

DIP Switch	Setting
Sw.1	Off (up) - DTR normal.
Sw.2	Off (up) - Verbal result codes.
Sw.3	On (down) - Display result codes.
Sw.4	On (down) - No Echo, offline commands.
Sw.5	Off (up) - Auto-answer on first ring.
Sw.6	Off (up) - Carrier detect normal.
Sw.7	Off (up) - Load NVRAM default.
Sw.8	On (down) Modem smart mode.

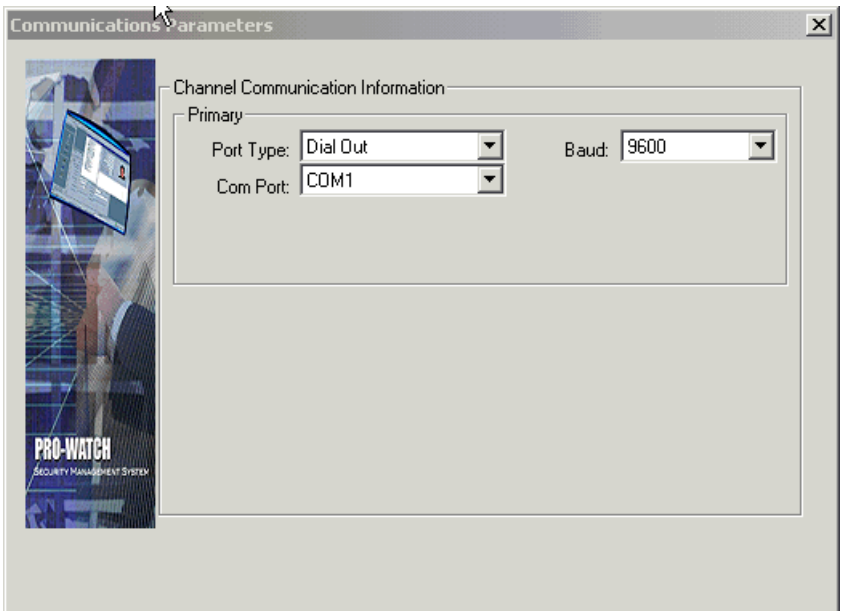
Note: Auto Answer should be activated on the modem.

C.5.2 SEEP Dial-Out

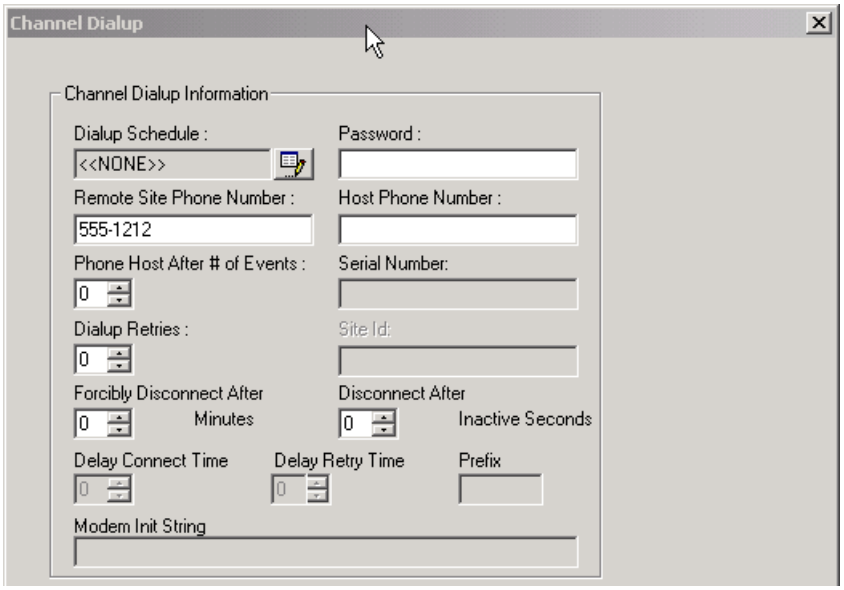
To configure dial-out for the SEEP panels:

1. Open the Hyperterminal application.
   a. Select the Bits per Second from the drop-down list.
   b. Select **7** from the Data Bits drop-down list.
   c. Select **Odd** from the Parity drop-down list.
   d. Select **1** from the Stop Bits drop-down list.
   e. Select **None** from the Flow Control drop-down list.
   f. Click **OK**.
2. Press the **Space bar** key.
3. Enter the password.
4. Enter **Modem** and press the **Enter** key.
5. Select **Enable/Disable Modem** (Choice 1) and Enter **Y** (Yes).
6. Select the **Modem Configuration Menu** (Choice 3).

7. Connect the serial cable from the host modem to the communication port on the host.
8. Connect the serial cable from the host port of the ACU to the remote modem.
9. Create a **Dial-Out** Channel in Pro-Watch. See "Adding a SEEP Channel" in Chapter 13. At the Communications Parameters dialog box:
   a. Select the communication port to which the modem is connected.
   b. Select the baud rate at which to connect.



10. Configure the Channel Dial-up Information. See "Set Communications Parameters" in Chapter 13.



11. After the channel, panel, and logical devices are configured (See "HW Config - SEEP" in Chapter 13), right-click the channel and select **Actions** > **Manual Dialup**.
12. Use the following table to configure the DIP switch for the SEEP ACU Modems. Note that these settings are for use with the external US Robotics 56k V.90 modems for both the host and remote modem.

DIP Switch	Setting
Sw.1	Off (up) - DTR normal
Sw.2	Off (up) - Verbal result codes
Sw.3	On (down) - Display result codes
Sw.4	On (down) - No Echo, offline commands
Sw.5	Off (up) - Auto-answer on first ring
Sw.6	Off (up) - Carrier detect normal
Sw.7	Off (up) - Load NVRAM defaults
Sw.8	On (down) Modem smart mode

C.6 Cardkey Dial-up Configuration

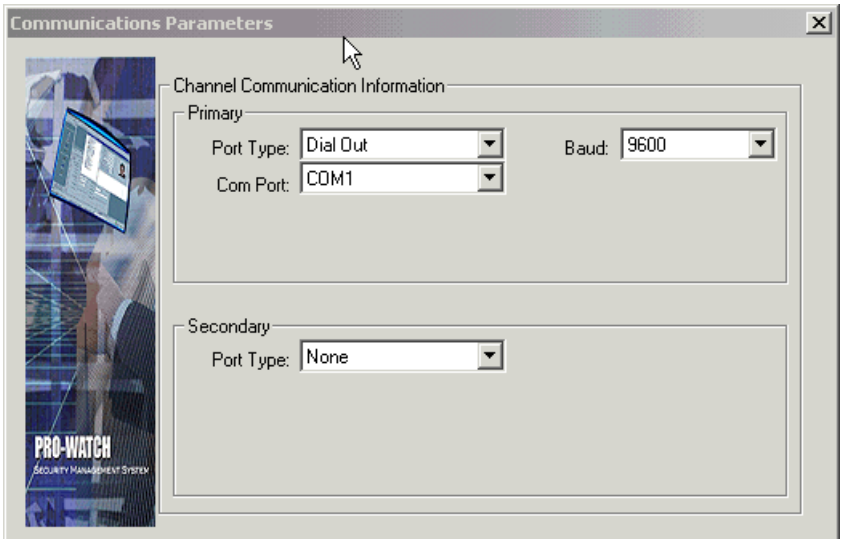
C.6.1 Cardkey Dial-In

Pro-Watch does not support Cardkey dial-in.

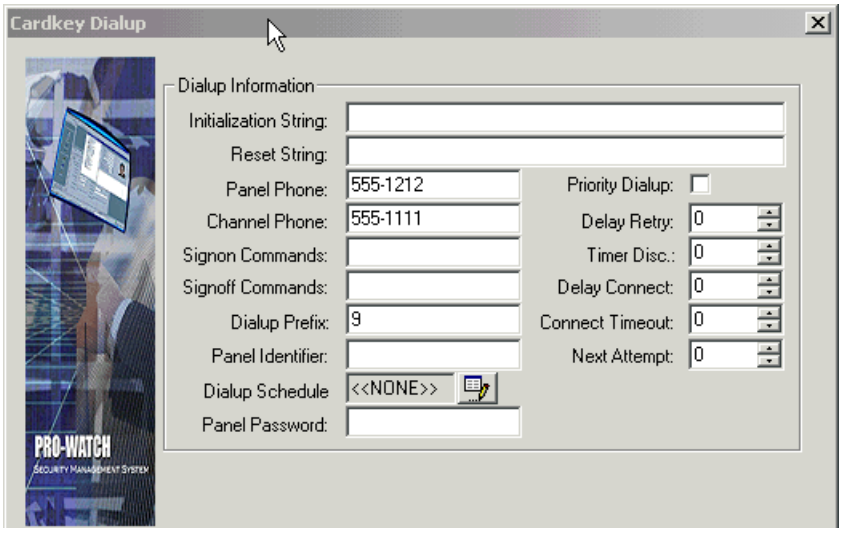
C.6.2 Cardkey Dial-Out

To configure dial-out for the Cardkey panels:

1. Connect the serial cable from the host modem to the communication port on the host.
2. Connect the serial cable from the RS232/485 Converter, which is connected to the Nodal Port J3 on the ACU, to the remote modem.
3. Create a **Dial-Out** Channel in Pro-Watch. See "Adding a Cardkey Channel" in Chapter 9. At the Communications Parameters dialog box:
   a. Select the communication port to which the modem is connected.
   b. Select the baud rate at which to connect.



4. Configure the Channel Dial-up information. See "Adding a Cardkey Channel" in Chapter 9. At the Channel Dialup dialog box:
   a. Enter the Panel Phone Number or the remote site phone number.
   b. Enter the Channel Phone Number or the host phone number.



5. After the channel, panel, and logical devices are configured (See "HW Config - Vindicator V5" in Chapter 15), right-click the channel and select **Actions** > **Manual Dialup**.
6. Use the following table to configure the Host Modem DIP switch. Note that the DIP switch settings are based on the use of an external US Robotics modem.

DIP Switch	Setting
Sw.1	Up - DTR provided by PC.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Down - Auto answer off.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down - Modem smart mode.

7. Use the following table to configure the Remote Modem DIP switch. Note that the DIP switch settings are based on the use of an external US Robotics modem. Also note that auto answer must be “on.”

DIP Switch	Setting
Sw.1	Down - DTR provided by modem.
Sw.2	Up - Verbal result codes.
Sw.3	Down - Display result codes.
Sw.4	Down - Echo offline commands disabled.
Sw.5	Up - Auto answer on.
Sw.6	Up - Carrier detect normal.
Sw.7	Up - Load NVRAM defaults.
Sw.8	Down - Modem smart mode.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Remote Terminal Services

D

In this appendix ...

Overview
Setting Up Terminal Services
Before Badging from the Terminal Client

D.1 Overview

This appendix describes how to set up Remote Terminal Services in a Pro-Watch configuration for a Pro-Watch client-server configuration.

The legacy Remote Terminal Service enables you to perform administrative functions on Pro-Watch systems from a remote site over firewalls. Using this package is very different from using a remote-control product. You are not manipulating the keyboard, mouse, and screen at the server. Instead, you log on to the computer and create a new session. However, this session is displayed remotely over Remote Terminal Services, rather than locally at the computer. You still have full access to the computer's programs just as if you were working at its local console.

D.2 Setting Up Terminal Services

Use this procedure if you have installed Pro-Watch on a Windows platform.

D.2.1 Installing Terminal Services

Use this procedure to install Terminal Services in Remote Administration mode. Remote administration mode allows two low-resource simultaneous connections that are ideally suited for remote administration. No additional licenses are necessary, and the limit cannot be increased.

D.2.2 Connecting to Terminal Services

To connect to Terminal Services running on a server, you must use a Terminal Services client. The client is available at the following location on the server on which you installed Terminal Services:

```
%SystemRoot%\System32\Clients\Tsclient\Net\Win32
```

Next, create a share on your server so that you can easily install the client on any computer.

D.2.3 Creating a Share on the Server

To create a share on the server:

1. Use Windows Explorer to locate the %SystemRoot%\System32\Clients\Tsclient\Net\Win32 folder. Note that %SystemRoot% may be the C:\Winnt folder.
2. Right-click the Win32 folder, and then click **Sharing**.
3. On the **Sharing** tab, click **Share this folder**.
4. Change the share name to TSClient.
5. Click **Permissions**.
6. Click to clear the **Full control** and **Change** check boxes. Only the Read permission should be selected.

7. Click **OK**, and then click **OK** again.

D.2.4 Installing the Terminal Services on the Client

Use this procedure to install Terminal Services on the computer from which you want to perform remote administration.

Connect to the share you created earlier on the server (see "Creating a Share on the Server". The share is named *Servername*\TSClient, where *Servername* is the name of the computer on which you installed Terminal Services.

Tip: It is not necessary to follow the uppercase and lowercase convention that is used in this procedure.

To install Terminal Services on the client:

1. Connect to the *Servername*\TSClient share that you created in the section "Creating a Share on the Server".
2. Double-click **Setup.exe**.
3. Click **Continue** in the dialog box that appears, and then type your name and organization in the next dialog box.
4. Click **I agree** (if you agree) when you see the license agreement.
5. Click the large button in the next dialog box. You can change the installation path first, if you desire.
6. Click **Yes** when you are prompted whether you want all users to have the same initial settings.

D.2.5 Using the Terminal Services Client

To use the Terminal Services client, perform these tasks:

1. Create a connection to the Terminal Services server.
2. Specify Pro-Watch as the application using Terminal Services.
3. Connect to the Terminal Services server.

D.2.5.1 Creating a Connection to the Terminal Services Server

Use this procedure to create icons with which to connect to the Terminal Services server.

1. Click **Start > Programs > Terminal Services Client > Client Connection Manager**.
2. When the Client Connection Manager opens, select **File** > **New Connection**.
3. When the Client Connection Manager Wizard starts, click **Next.**

4. In the **Connection name** box, enter a name that will identify the connection.
5. In the Server Name or IP Address box, enter the server's name or IP address, or click **Browse** to search for the server. When you are done, click **Next**.
6. Leave all automatic logon information blank. Using automatic logon information might present a security problem if a non-administrator has access to the computer from which you run the client. Click **Next**.
7. Click a screen resolution that is appropriate for you.

   Tip: It is best to use the largest area you can select (the client does not let you select an area larger than your local screen can display). Do not select **Full screen** at this time; you can toggle between windowed and full screen modes later. Also, if you leave the initial connection in the window, the screen will remind you that you are working on a remote computer rather than your local workstation.
8. Click **Next**.
9. Leave the Enable Data Compression and Cache Bitmaps check boxes cleared. They are useful only if you are working over a slow dial-up link. Click **Next**.
10. Leave the Start the Following Program check box cleared if you want the client to display the server's desktop. Click **Next**. Change the icons if you desire. Click **Next**, and then click **Finish** to complete the wizard.

D.2.5.2 Creating a Shortcut

Follow these steps to create a shortcut:

1. Select **Start > Programs** > **Terminal Services Client** > **Client Connection Manager**.
2. Right-click the connection you would like to use for Pro-Watch and select **Properties.**
3. Click the **Connection Options** tab and set Connection startup to **Full screen.**
4. Click the **Program** tab and select **Start the following program.**
5. In **Program path and file name**, type the path and file name of the program that you want to start on the server when the user logs on to the Terminal Server. For example: C:\Program Files\ProWatch\bin|MICShell.exe.
6. To change the program icon to match that of a typical Pro-Watch installation, copy and paste the **idr_prow.ico** file from the Pro-Watch Server (located in the ProWatch\bin directory) to the client machine.

7. Click the **Change Icon** button, Browse to idr_prow.ico file, and click **OK.**
8. Click **OK** to save the settings.
9. Right-click the connection and select **Create Shortcut on Desktop.**

D.2.5.3 Connecting to the Terminal Services Server

Follow these steps to connect to the Terminal Services server:

1. Double-click the connection shortcut for Pro-Watch (or the server icon in Client Connection Manager if a shortcut wasn't created). The Terminal Services client window appears and displays the server's logon dialog box. You might need to double-click the window's title bar to see it all.
2. Type an appropriate set of credentials to log on to the server. Typically, you will log on as some kind of administrator (local, domain, or enterprise).

If you use correct credentials, you will log into Pro-Watch (or see the server's desktop if Pro-Watch was not specified as the application).

D.3 Before Badging from the Terminal Client

Before attempting to perform badging functions at the Pro-Watch Terminal Client, be sure that the following tasks have been completed:

- Install the TWAIN camera drivers.
- Install the appropriate printer drivers.
- Install Windows Terminal Server.
- Place the **TermServ./dll** file in the application server's **\system32** directory.
- Place the **TermClient.dll** file in each terminal client's **\system32** directory.
- Ensure that badging functions operate correctly on the server machine before attempting them from the client.
- Ensure that the non-administrator accounts have "Full Control" permissions for the **\ProWatch** directory.

Copyright © Honeywell Inc. All Rights Reserved

Magicard Prima Printer Installation

E

In this appendix ...

Overview

Installing Magicard Prima Printer

E.1 Overview

This appendix describes how to install and configure the Magicard Prima printer and to make it work with Pro-Watch.

E.2 Installing Magicard Prima Printer

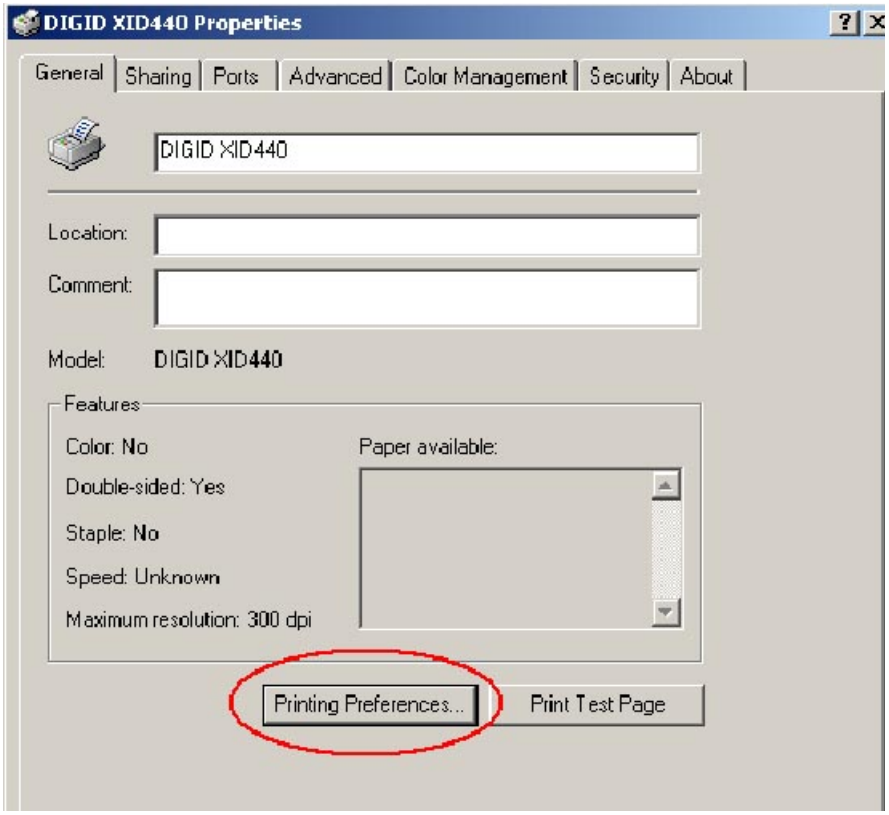
Note: Before installing the Magicard Prima driver software, you must install the USB-to-SCSI adapter driver. Without this driver in place, the Magicard driver will not work properly. Reboot the system before continuing.

These instructions are based on the **Prima driver, v3.0.6.0 (or later)**. Screens may appear slightly different for other versions of the driver. Use the **DIGID XID440** printer when installing the driver.

Once the driver is installed and the computer has been rebooted, the following steps are needed to ensure that the printer works properly with Pro-Watch.

E.2.1 Printer Configuration

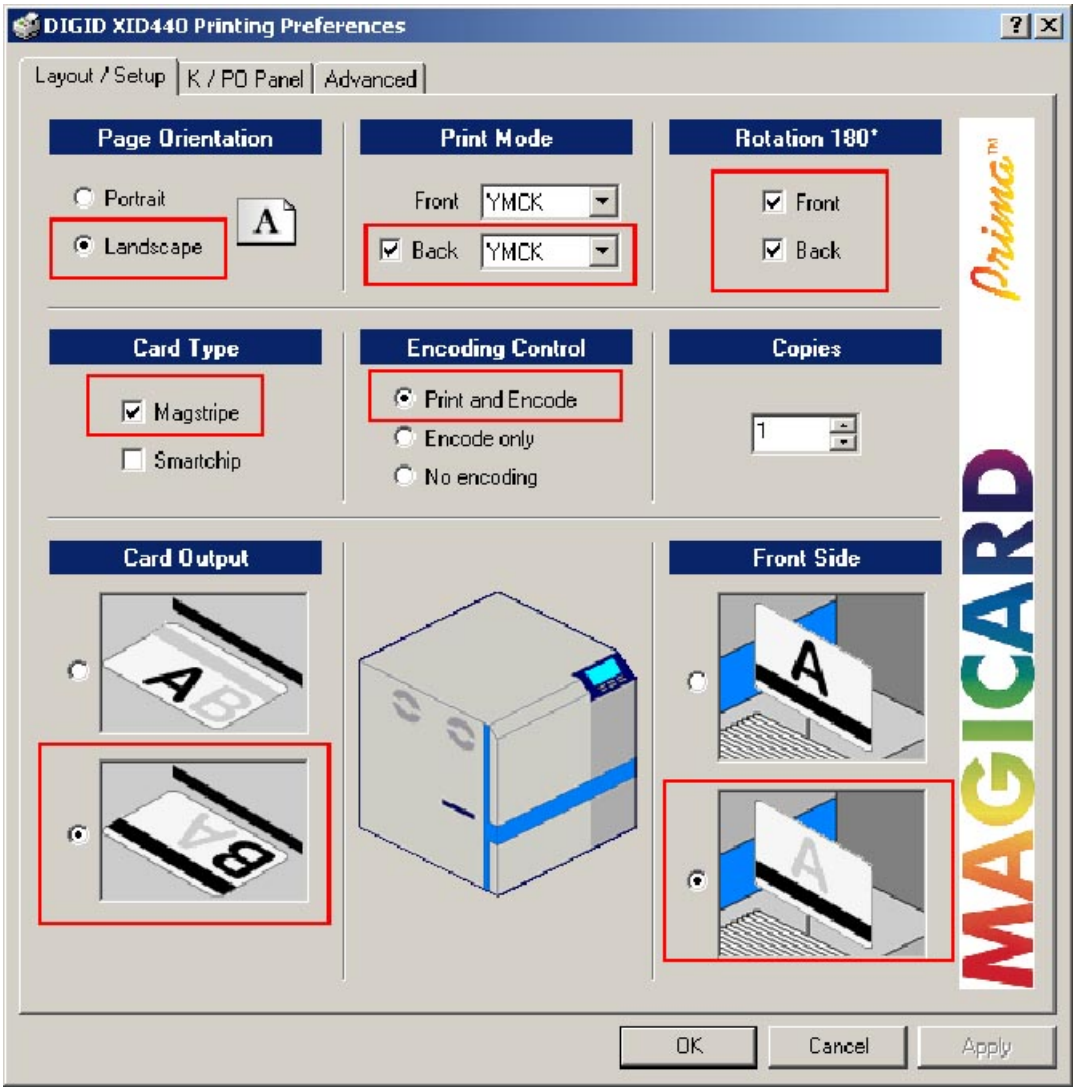
1. Select one of the following to open the printers folder:
   - **Start > Printers and Faxes**, or
   - **Start > Settings > Printers**
2. Right-click the **DIGID XID440** printer and select **Properties**:



3. At the DIGID XID440 Printer Preferences dialog box, use the following table to select the proper settings:

Table E-1 DIGID XID440 Printer Preferences

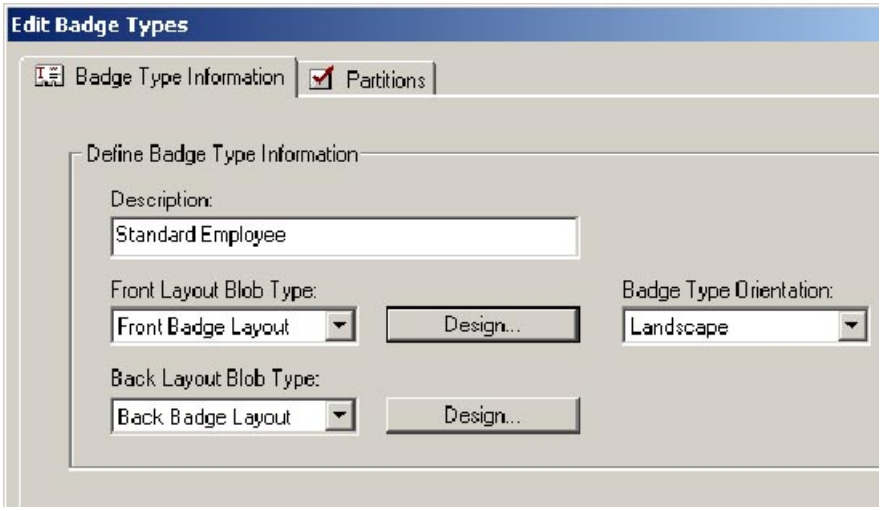
Category	Proper Setting
Page Orientation	Landscape.
Print Mode	Both YMCK, Back check box is checked.
Rotation 180°	Both Front and Back are checked.
Card Type	Magstripe is checked.
Encoding Control	Select Print and Encode.
Card Output	Bottom radio button is selected.
Front Side	Bottom radio button is selected.



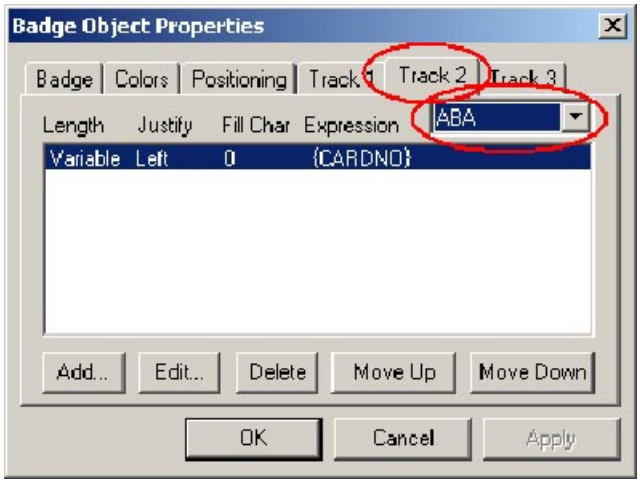
Note: Launch the **Badge Designer** application to create your badge that contains the magstripe.

The card should be configured so that the magstripe is the first page. If you are creating a card layout that has the stripe on the back of the card, you must create the back of the card as the “Front Badge Layout” and the front of the

card as the “Back Badge Layout”.

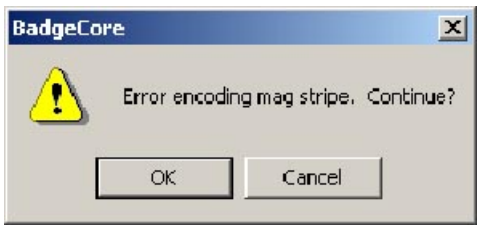


4. In the Badge Designer, Right-Click on the badge design, and select **Properties**.
5. Select the **Track 2** tab and set it for **ABA** format.
6. Click **Add** to select the fields that should be encoded into the card. Select the “CARDNO” as one of the fields.



E.2.2 Printing and Encoding Within Pro-Watch

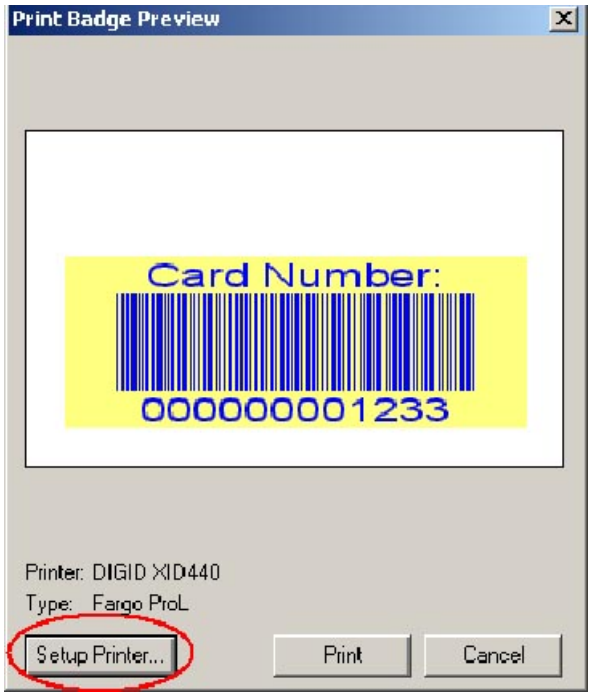
1. In order to properly encode a card within Pro-Watch, the printer type Fargo ProL must be selected. This printer type uses “generic” codes to print the badge with the encoding information.
2. Selecting “Generic Badge Printer” or “Ultra Magicard” will result in the following error within Pro-Watch:



To select the Fargo ProL printer type:

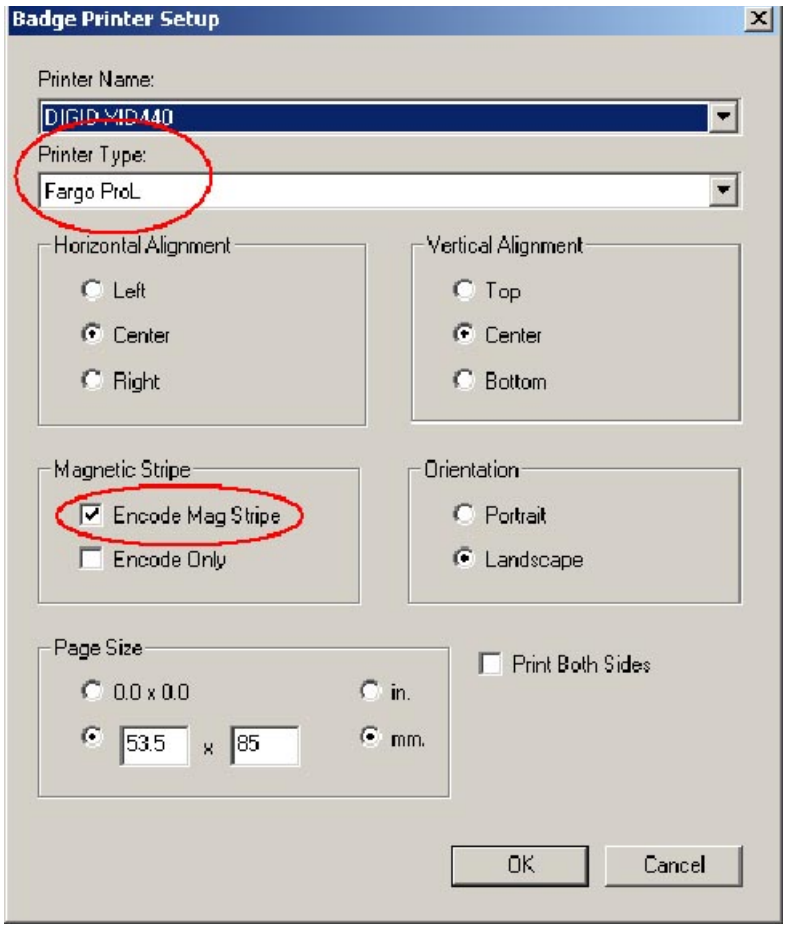
Note: When printing a badge, click the **Setup Printer** from the Print Badge Preview screen.

This should only need to be done the first time a badge is printed.



3. From the Printer Type drop-down list, select **Fargo ProL**.

4. Verify that the **Encode Mag Stripe** check box is selected.



Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Moving Panels

F

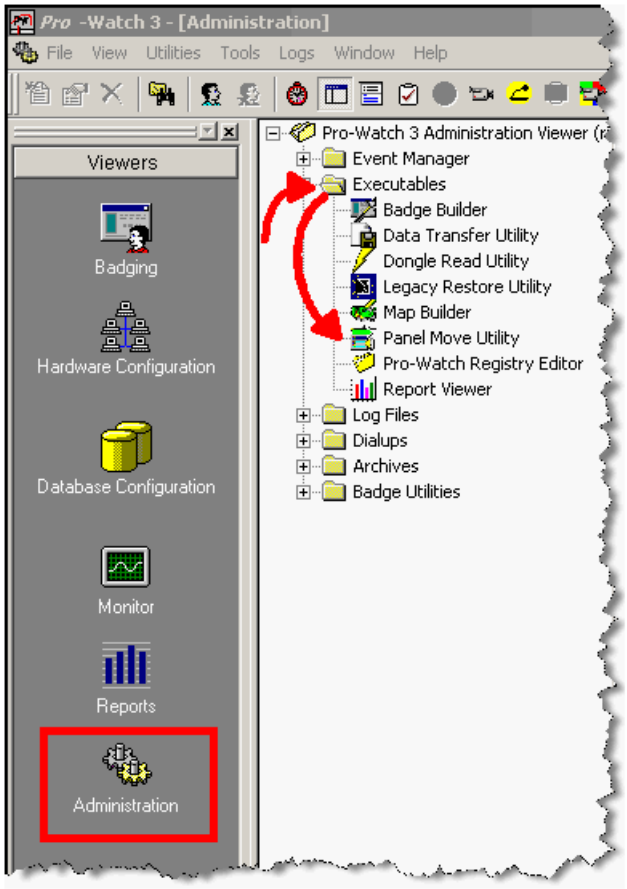
In this appendix ...

Overview
Moving the Panel

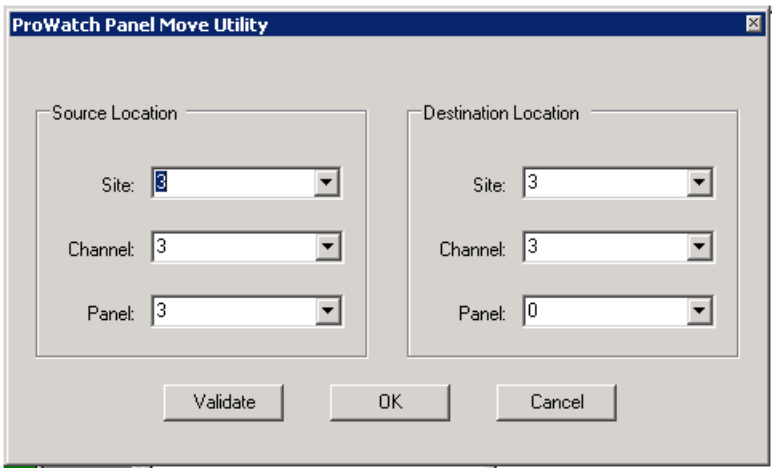
F.1 Overview

This appendix describes how to move a Pro-Watch Panel from its current Site/Channel/Address to another location, without having to reconfigure the Panel's Logical Devices.

To access the Panel Move utility from the Pro-Watch main screen, double-click and select **Administration > Executables > Panel Move Utility:**



The Pro-Watch Panel Move Utility dialog box appears:



Note: By default, all Pro-Watch users are configured with a Class grant, which enables them to use the Panel Move Utility. If for some reason access is denied, go to **Database Configuration > Users**, right-click the user, and select **Properties**. Then, select **Programs > Administration > Administration Viewer**, and apply the Grant setting to the Panel Move Utility.

F.2 Moving the Panel

Follow these steps to move a Panel in Pro-Watch:

1. In the Source Location box, specify the Channel's current location. Use the drop-down lists in the Site, Channel, and Panel fields to select the Panel's Site, Channel, and Panel address.

Note: In the Destination Location box, specify a new Site, Channel, or Panel address. All values that appear in the drop-down lists are available. For example, if the Panel field lists "2" and "4," this means that addresses 2 and 4 are available, but address 3 is already taken.

you can "relocate" the Panel to any or all of the available values listed in the Destination Location box. For example, you may wish to move the Panel to a different Site. In this case, you would also specify a new Channel and Panel address. Or, you may wish to keep the Panel at the same Site but move the Panel only to a different Channel and Panel address in that Site. Likewise, you may wish to keep the same Site and Channel but change only the Panel's address.

2. After making your Site, Channel, and Panel selections, click **Validate** to be sure that the source and destination specifications are still available to complete the move. This is advisable because the Pro-Watch Panel Move Utility dialog box does not automatically refresh itself after it is first opened. When multiple users are using the same Pro-Watch server, it is possible that the locations that appear in

the drop-down lists may no longer be available.

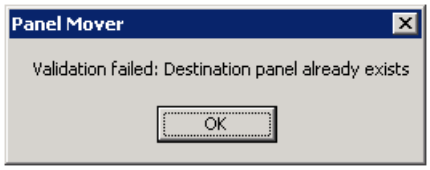
When you click **Validate**, all of the selected values are still available if the following message appears:



If, since the Pro-Watch Panel Move Utility dialog box was first opened, the Panel specified in the Source Location box has become unavailable, the following message appears after you click **Validate**:



If, since the Pro-Watch Panel Move Utility dialog box was first opened, the Panel specified in the Destination Location box has become unavailable, the following message appears after you click **Validate**:



Click **OK** to acknowledge the Validate message. If the validation failed, you will need to repeat steps 1 and 2 to specify another source or destination Panel.

3. At the Pro-Watch Panel Move Utility dialog box, click **OK** to execute the Panel's move. At the prompt, click **OK** to confirm the move. The moved Panel now operates in the new location with all of its original Logical Devices.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Badging

G

In this appendix ...

Overview
Badges
Cards
Badge Designer
Exiting the Badge Designer

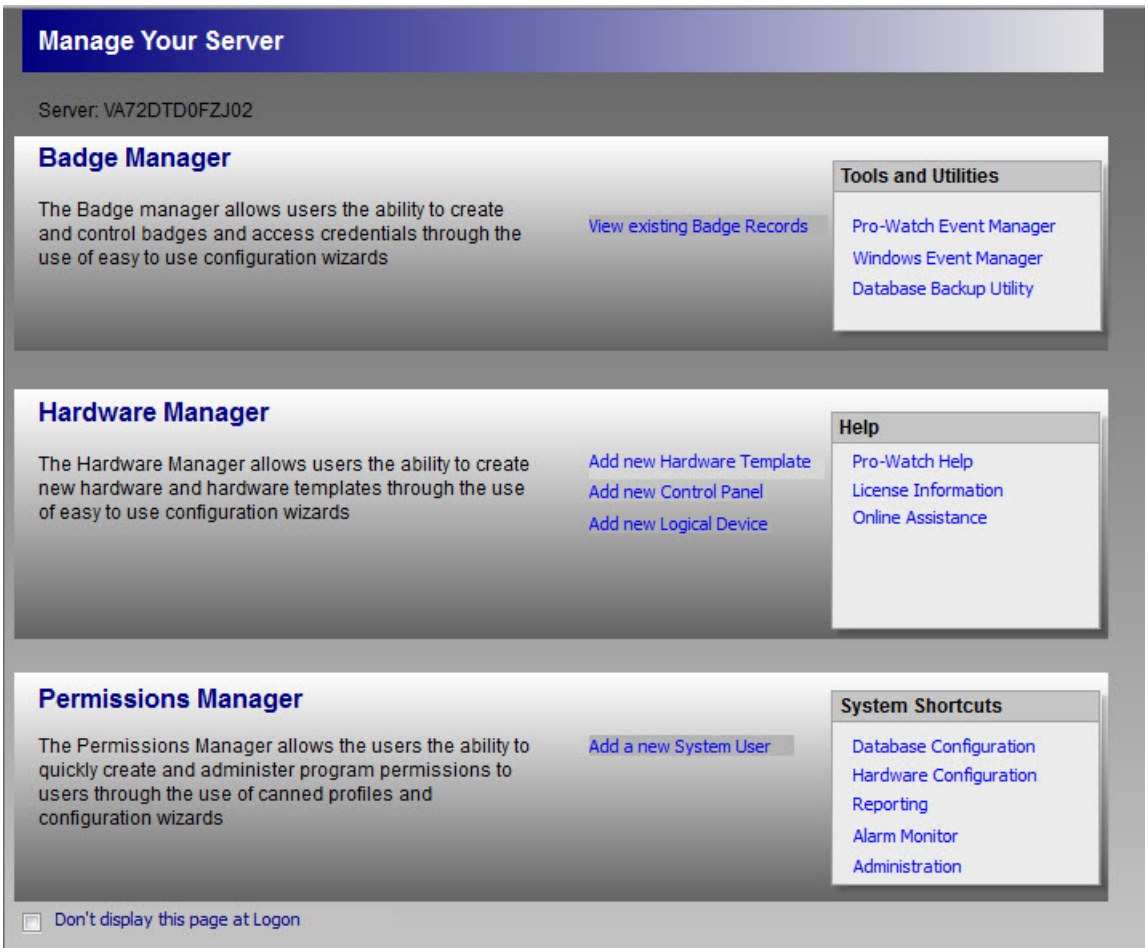
G.1 Overview

The Pro-Watch Badging module creates badges and assigns card access privileges within your enterprise. This chapter describes how to design and create badges and how to assign privileges to cards.

The complete badging process, however, includes other tasks not described in this chapter. For example, you must first create badge profiles in the Badge Builder utility described in Chapter 60, Badge Building. Other tasks, as well, must be completed within the Database Configuration component (see Chapter 27, Database Configuration (DBC)).

The easier and faster way to complete the badging process is to use the Badge Manager wizard from the Manage Your Server window.

Figure G-1 Selecting Badge Manager Wizard



It is also possible to accomplish the badging by completing the steps manually. For manual badging, use the table below to identify the required sequence of badging tasks and to find the tools and instructions to complete them.

Step	Task	Refer to ...
1	Create the badge profile.	"Adding a Badge Profile" in Chapter 60.
2	Create the badge profile pages.	"Adding Badge Profile Pages" in Chapter 60.
3	Create the badge fields, if necessary.	"Adding a Badge Profile" in Chapter 60.
4	Assign the badge fields.	"Adding a Badge Field to a Profile or Editing a Badge Field" in Chapter 60.
5	Assign the badge profile to a class.	"DBC - Badge Profiles" in Chapter 30.
6	Designate the badge types.	"DBC - Badge Types" in Chapter 32.
7	Create badge statuses.	"Adding a Badge Status" in Chapter 31.
8	Design the badge.	"Designing the Badge Layout" in this chapter, and Chapter 60, Badge Building .
9	Assign the badges to users.	"Badges" in this chapter.
10	Assign cards to badges.	"Cards" in this chapter.

Note: The Pro-Watch Badge Manager application also supports badging for Honeywell's Vindicator access control system.To configure Pro-Watch for Vindicator badging support, you must reset the badging key in the registry. In the Key Default section of the registry, replace **`Badging MICBadgeViewer.pkg`** with **`PWVinLauncher.exe`**.

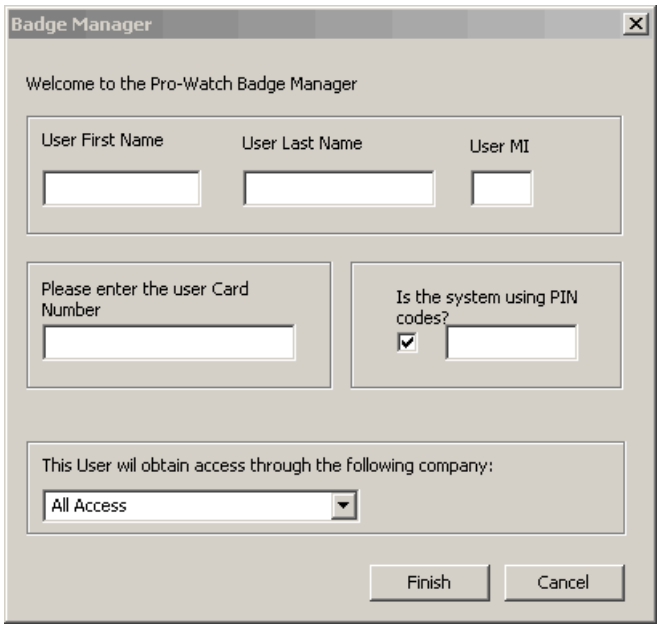
G.2 Badges

This section explains how to add new badges, edit existing badges, assign cards to badges, partition badges, assign brass keys, and print badges.

Note: The views of the badge screens change from site to site and from profile to profile**.** The screen shots presented in this guide are for illustration purposes only.

G.2.1 Adding and Editing a Badge

1. To add a new badge, select **Badge > New** from the menu bar. Note that if the Server Manager is turned on (the default condition), the following Badge Manager dialog box appears. However, if the Server Manager is turned off, the dialog box in step 3 appears, and you should proceed directly to that step.



2. Use the following field descriptions to complete the Badge Manager dialog box:

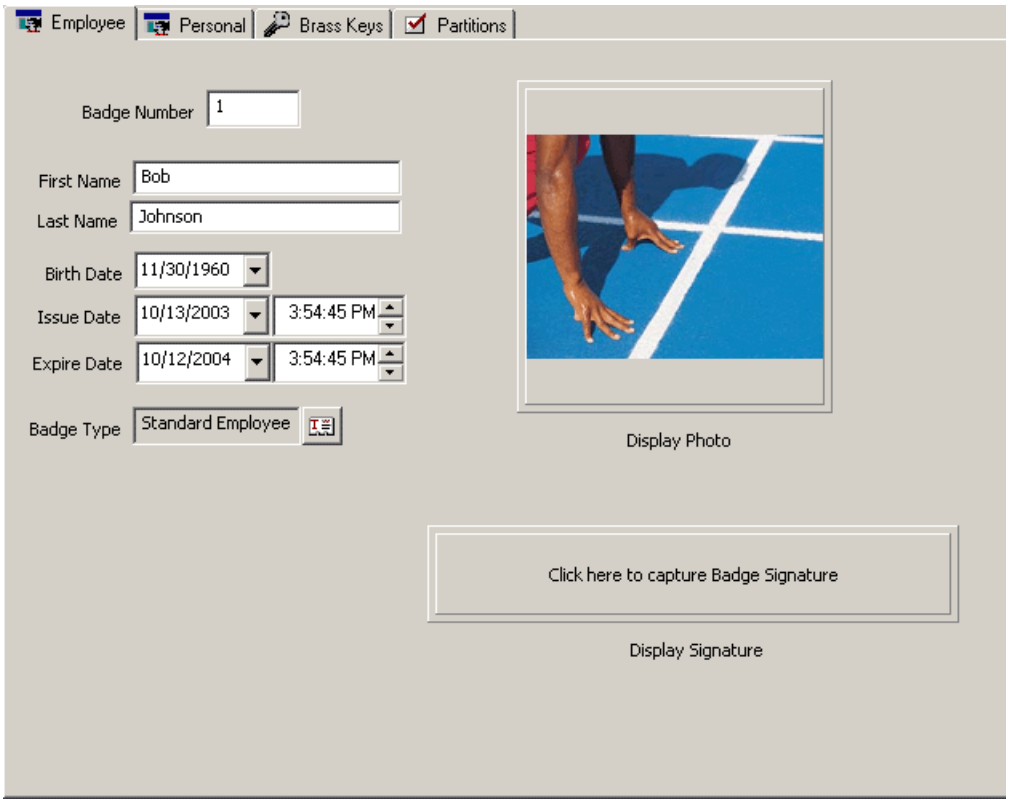
Field	Description
Name fields	Enter the first and last names and middle initial.
Card number	Enter a unique number that will identify the user.

Field	Description
PIN codes	If your enterprise uses Personal Identification Numbers (PINs) to identify staff, select the check box and enter the user's PIN code.
Access	**All Access** – this card provides access at every point. **Company name** – this limits the card access to the clearance codes associated with the Company name you select.

3. Click **Finish** to display the user's badge record dialog box.
   Notes:
   - The required fields are configured in the Modifying Control Attributes dialog box of the Badge Builder module. See "Modifying Control Attributes" in Chapter 60.
   - All the fields in all the badging tabs may display a **default value** if they have been configured to display a default value in the Modifying Control Attributes dialog box of the Badge Builder module. See "Modifying Control Attributes" in Chapter 60.
   - The specific tabs that display on the right pane depend on the badge profile configuration choices made in the **Badge Profile > General Fields** section of the Badge Builder utility. You can access the Badge Builder utility by clicking the Administration icon in the left pane of the Pro-Watch screen and then double-clicking the Executables folder. See Chapter 60, Badge Building.

     Badge Builder is where you can select all, some, or none of the following tabs before they display in the main badging screen:
   - Any user-defined tab.
   - Access Page (the card information pane at the bottom of the screen).
   - Partition Page (tab).
   - Brass Keys Page (tab).
   - Image Summary Page (tab).

     Also, see "DBC - Badge Profiles" in Chapter 30.
4. To edit an existing badge, click the desired badge name in the center pane. The associated badging tabs will display in the right pane:



5. Complete the following tabs to either add or edit the badge:

   BADGE TABS LIST

   - "Employee Tab".
   - "Personal Tab".
   - "Brass Keys Tab".
   - "Image Summary Tab".
   - "Partitions Tab".

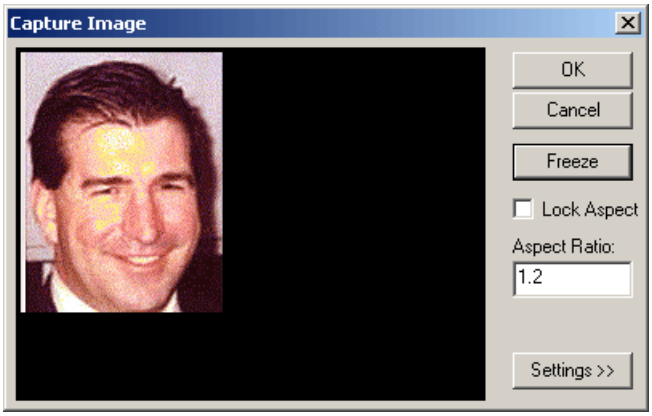
G.2.1.1 Employee Tab

(Return to "BADGE TABS LIST")

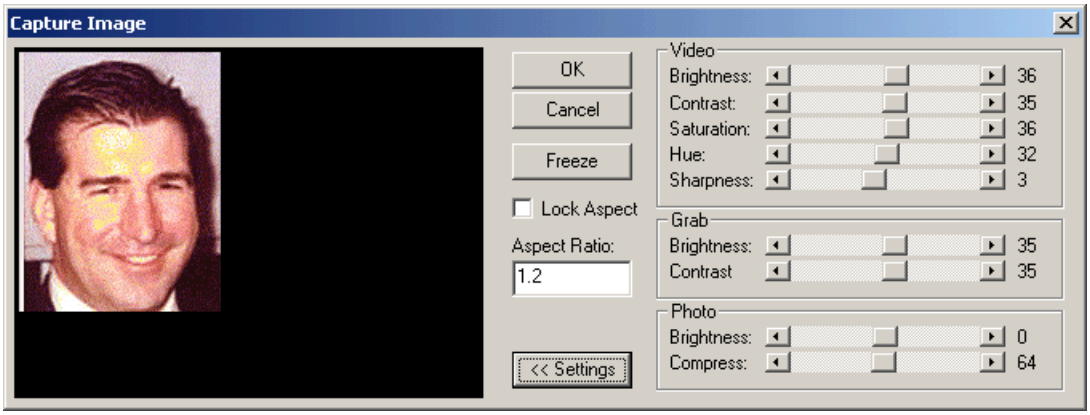
1. Enter a unique badge number.
2. Enter the last name and first name of the new badge holder.
3. Enter a Birth Date in the Issue Date box, or select the correct date from the calendar, which displays when you click the corresponding down arrow.



4. Enter an Issue Date and Time in the issue date and time fields. You can select the correct date from the calendar, which displays when you click the corresponding down arrow.
5. Enter the Expiration Date and Time in the expiration date and time fields. You can select the correct date from the calendar, which displays when you click the corresponding down arrow.
6. In the Badge Type field, enter a badge type, click the  icon to display a pop-up menu, and then select **Define** to display the list of currently-defined badge types. Then, perform one of the following two options (note that you can also edit an existing badge type by clicking the  icon, and then clicking **Edit Current Badge Types**):
   - Click one of the currently-defined badge types and click **OK**. Add a new badge type by clicking **Add** and then filling in the appropriate fields in the next Add Badge Types dialog box. Then click **OK**.
   - Click one of the currently-defined badge types and click **Edit** to change the badge's configuration. Make the desired edits on the Edit Badge Types dialog, click **OK**, and then select the badge type at the Badge Types dialog.
7. To capture a badge photograph, click **Click here to capture Badge Photo**. The Capture Image dialog box appears. Note that to capture a badge photo, you need an imaging device like a digital camera, a video camera, a scanner, a web cam, etc. that is compatible with TWAIN, Flashpoint, or Canon. See "Setting the Capture Device".



8. Click **Freeze** to fix the live video picture, or click **Freeze** again to go back to live video.
9. Click **Lock Aspect** to keep the ratio of the width of an image to its height, avoiding distortions. The aspect ratio is listed in the Aspect Ratio box.
10. To change the image quality settings and compression rates for the captured image, click **Settings**. The Capture Image dialog box displays additional fields.



11. Define the Video, Grab, Photo settings by moving the corresponding sliders to achieve the desired effect.
12. Once you determine the image settings, click **Settings** to return to the normal capture window.
13. When you have the desired image, click **OK**. This image is now linked to the badge holder's record, for display on the badge profile and badge layout.
14. To import an existing photo:
    - Select **Badge > Import Photo** from the menu bar or click the Import Photo icon on the tool bar. Import Image dialog box displays.
    - Click **Open** and browse to the photo file you want. Select it and click **Open** to have the photo display in the Import Image dialog box.
    - If you select the **Whole Image** check box the image will be inserted into the badge as is, in its original size. If you would like to change the image's size, unselect the check box, select either the **Coordinates** or the **Aspect** option button and enter the appropriate values.
    - Click **OK** to insert the photo into your badge.

Note: You can also set compression and intensity parameters for photos on badges. See "Setting Badge Photo Compression and Intensity" in Chapter 5 for more information.

G.2.1.2 Personal Tab

1. Enter the badge holder's street address, home phone number, and Social Security number.
2. Enter the badge holder's employer. Click the  icon to display the pop-up menu, and then select **Define** to display the list of currently-defined companies. Perform one of the following options:
    - Click one of the currently-defined companies and click **OK**.
    - Click one of the currently-defined companies and click **Edit** to change the company's configuration. Make the desired edits in the Edit Company dialog box, click **OK**, and then select the company at the Companies dialog. You can also edit an existing company by clicking the  icon, and then selecting **Edit Current Companies**.
    - To search for a specific company, enter one or more letters into the **Key** field. Pro-Watch will display only those companies the names of which start with the letter(s) you have entered into the Key field.
    - Click **Add** to add a new company. The Add Company dialog box will display. Enter the appropriate values and click **OK**. Once you are back in the Companies dialog box select the company that you have added and then click **OK**.
    - To delete a company, select it in the Companies dialog box and click **Delete**.
3. Enter the badge holder's department, the supervisor, office phone, and extension.

G.2.1.3 Brass Keys Tab

In this tab you can assign new brass (i.e. physical) keys to the badge holder and edit or delete the existing brass keys. Through this functionality you can set the key status, issue date, issue time, due date, due time, return date, and return time as well.

To add a brass key:

1. Click **Add** to display the Add Brass Key dialog.
2. Click the key icon next to the Brass Key field to display the pop-up menu. Select **Define** to display the Brass Key list.
3. Perform one of the following options:
    - Select one of the currently-defined brass keys, and then click **OK** to assign it to the badge. You will return to the Add Brass Key dialog box where the name of the brass key is inserted in the Brass Key field.

- Click **Add** to create a new brass key. The Add Brass Key dialog box will display. Enter the description of the brass key in the Description field. Click **OK** to To the Brass Keys dialog box. Select the new brass key that you have just added and click **OK**. You will return to the Add Brass Key dialog box where the name of the brass key is inserted in the Brass Key field.
- To edit an existing brass key, select it from the list and click **Edit** to display the Edit Brass Key dialog box. Edit its description and its partition (if any). Click **OK** to return to the Brass Keys dialog box. Select the edited brass key and click **OK**. You will return to the Add Brass Key dialog box where the name of the brass key is inserted in the Brass Key field.
- To delete a brass key, select it in the Brass Key List dialog box and click **Delete**.

4. Select the **Issued** check box in the Add Brass Key dialog box to enable the Issue Date and Issue Time fields. Enter the appropriate values. You can also select an issued date by clicking on the down arrow and displaying the issue date calendar.
5. Select the **Due** check box to enable the Due Date and Due Time fields. The due date and due time specify when the badge holder is expected to return the key. You can also select a due date by clicking on the down arrow and displaying the due date calendar.
6. Select the **Returned** check box and enable the Returned Date and Returned Time fields when the badge holder returns the brass key. Enter the appropriate values. You can also select a returned date by clicking on the down arrow and displaying the returned date calendar.
7. Click **OK** to complete the key assignment.

G.2.1.4 Image Summary Tab

The Image Summary tab displays any captured images assigned to and all the archived images for a selected badge. You may print or delete an image from the Image Summary tab.

Left-click on the image to zoom-in. Right-click to zoom-out.

To print an image:

1. Right-click on the **Display Photo** text.
2. Select **Print Image** to display the Image Printing dialog box. Click **Zoom In** or **Zoom Out** to view the image at the desired size. To revert to its original size, click **Normal**.
3. Click **Print**.
4. Click **Close** to exit the Image Printing dialog box.

To delete an image:

1. Right-click on the **Display Photo** text.
2. Select **Delete Image**. A message box will appear confirming if the user wants to delete the image.
3. Click **Yes**.

G.2.1.5 Partitions Tab

Partitions restrict user and class access to database resources that you designate.

See "DBC - Partitions" in Chapter 53 for information about creating a partition. Use this function to assign or delete an already-created partition to the badge:

1. To assign a partition to a badge, select one from the Partitions List.
2. To add a new partition, click **Add** to display the Available Partitions dialog box. Select the partition you want, and click **Add**.
3. To delete a partition from the Partitions List, select the partition and click **Delete**.

G.2.1.6 Saving a Badge

The badges you have created are saved automatically to the database when you exit out of the badging module or perform various other actions like print previewing, creating another badge, clicking to view another badge listed in the center pane, performing a badge search, and so on.

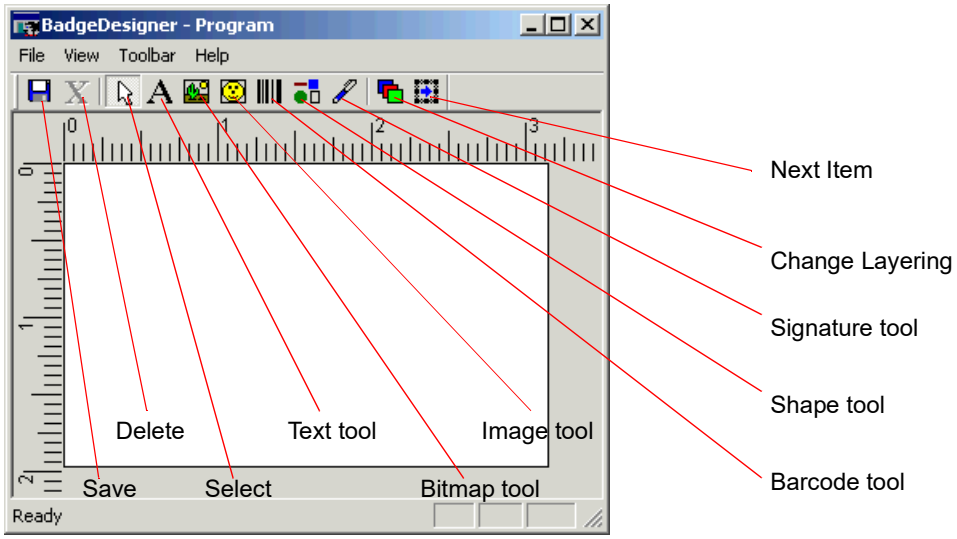
Selecting **Badge > Save** from the menu bar also saves the additions or edits into the database.

Note: The badges that are saved will not be immediately displayed in the badge list in the center pane unless you exit the Badging module and then re-enter it by clicking the Badging module icon in the first pane. You can also refresh the badge list in the center pane by performing a search by either clicking the **Quick Search button** on the tool bar or selecting **Edit > Quick Search** or **Edit > Advanced Search** from the menu bar.

G.2.1.7 Designing the Badge Layout

Use this function to design the front and back layout of a badge from the Badging window.

1. Select **Edit > Badge Layout > Front** or **Edit > Badge Layout > Back** from the menu bar to display the window:



2. From **Toolbar** menu item, select among the following options to design the layout:

   - Select **Keyboard Placement** to place objects inside the design window by using the keyboard and without using the mouse.
   - Select **Place Text** to enter text (see "Placing Text"). Click and drag to define the text area. Right-click and select **Properties** to set the Badge Text Object properties.
   - Select **Place Bitmap** to place a bitmap picture (see "Placing a Bitmap"). Click and drag to define the bitmap picture area. Right-click and select **Properties** to set the Badge Bitmap Object properties.
   - Select **Place Photo** to place a photo (see "Placing a Photo"). Click and drag to define the photo area. Right-click and select **Properties** to set the Badge Photo Object properties.
   - Select **Place Barcode** to place a barcode (see "Placing a Barcode"). Click and drag to define the barcode area. Right-click and select **Properties** to set the Badge Barcode Object properties.
   - Select **Place Shape** to draw a shape (see "Placing a Shape"). Click and drag to define the shape area. Right-click and select **Properties** to set the Badge Shape Object properties.
   - Select **Place Signature** to place a signature (see "Placing a Signature"). Click and drag to define the signature area. Right-click and select **Properties** to set the Badge Signature Object properties.
   - Select **Change Layering** to set badge object layering properties (see "Layering Badge Items").

Note: Click **Select Next Item** to select different badge objects.

All the above functions can be selected by clicking the corresponding button on the tool bar as well.

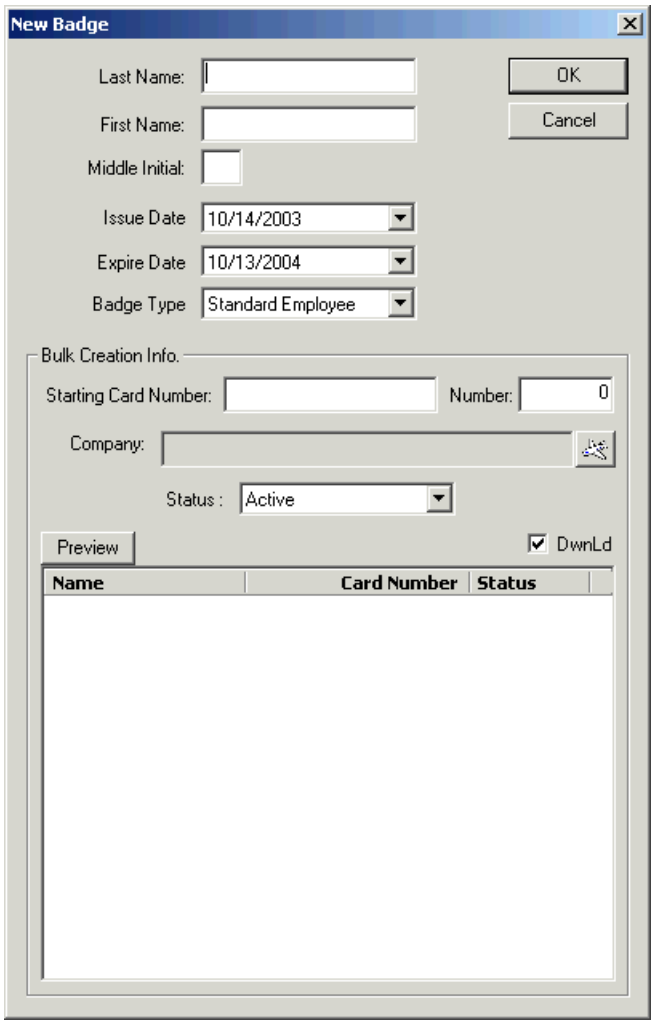
3. Select **File > Save** from the menu bar to save the edits to the badge layout.
4. To delete any layout object, right-click on the object and select **Delete Object** from the pop-up menu.
5. Select **File > Print** to print the badge.

G.2.1.8 Adding Badges in Bulk

Use this function to create multiple cards for multiple badge holders who share the same access profile, or badge.

Note: Click the **Multiple New Badge** icon  on the tool bar or select **Badge > Multiple New Badge** from the main menu to display the New Badge dialog box:

If a badge field has a default value assigned to its badge profile in the Badge Builder, then that field will automatically display the default value. If an auto increment default value is assigned to the badge profile, card numbers are incremented automatically with that preconfigured value. Enter a **Last Name**, **First Name**, and a **Middle Initial**, if any.



6. Enter an **Issue Date** or click the down arrow and select one from the calendar. This is the date on which the cards are issued.
7. Enter an **Expire Date** or click the down arrow and select one from the calendar. This is the date on which the cards will expire.
8. Select a **Badge Type** from the drop-down menu.
9. In the **Starting Card Number** field, enter the first card number.
10. In the **Number** field, enter the number of consecutively numbered cards you want to create.
11. In the **Company** field, enter a company name or click the browse button to display the pop-up menu.
12. Select **Define** to display the Companies dialog.
13. Select a **company**, and click **OK**. You will return to the New Badge dialog box.
14. Select the status of the bulk cards from the **Status** drop-down list.

15. Click **Preview** to see an example of your bulk card numbering in the lower portion of the dialog box. Note that cards with duplicate numbers will not be created.
16. Select the **Dwnld** check box to download the card information to all system panels. Each new card created will be displayed in the center pane of the Badging window under a separate but identical badge.
17. Click **OK**.

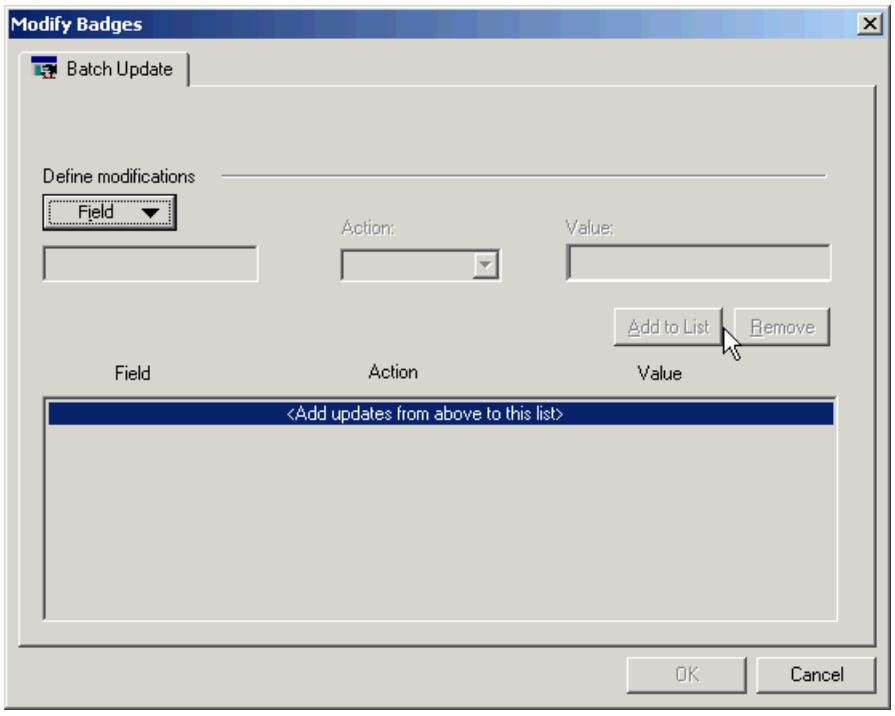
G.2.1.9 Editing Badges in Bulk

This function enables you to edit badge fields for multiple badge holders at once.

Note: Bulk edit is always performed on the badges that were searched and selected by Advanced Search (see "Advanced Search") or (see "Quick Search") functions.

Specify the field, the action to be performed on the field, and the edited value for the field.

1. Select **Edit > Batch Modify** from the menu bar to display the Modify Badges dialog box:



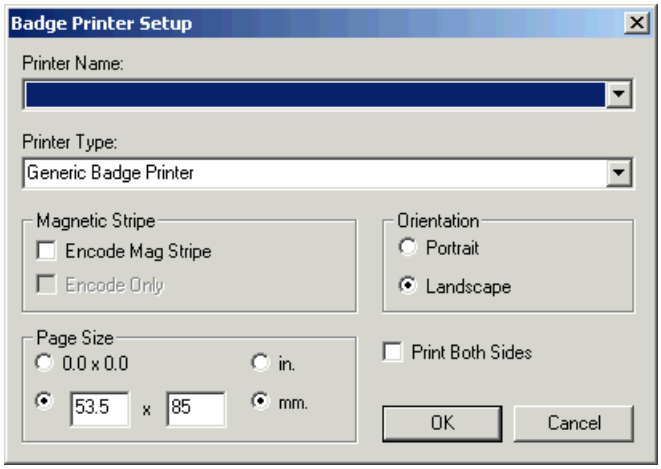
2. Select the badge field you want to edit from the **Field** drop-down list and the three sub-lists provided: Standard, Custom, and Card Fields.
3. From the **Action** drop-down list, select the action you want to perform on the selected field.
4. Enter the new value for the field in the **Value** field.

5. Click **Add to List** to add this edit to the list of edits you are creating.
6. Repeat steps 2-5 for each batch edit you want to perform.
7. Click **OK** to save the edits.

G.2.1.10 Printing a Badge

Note: This feature is not supported in Pro-Watch Lite.

1. Select **Badge > Print** from the menu bar. The Print Badge Preview screen appears and displays the front and back sides of the badge.
2. If you need to adjust your printer settings, click **Setup Printer** and proceed to step 3. Otherwise, click **Print** to print the front and back sides of the badge.
3. Click **Setup Printer** to open the Badge Printer Setup dialog, if required.



4. Select a **Printer Name** from the drop-down list.
5. Select a **Printer Type** from the drop-down list. Your choices include: DataCard ImageCard HIFX, DataCard ImageCard II+/III, DataCard ImageCard IV, Fargo ProL, Nisca, and Ultra Magicard.
6. If your printer supports encoding and you are using magnetic stripe cards, select the **Encode Magstripe** check box to automatically encode a magnetic stripe as the card prints.
7. Select the **Encode Only** check box if you wish to encode the magnetic stripe only, without printing any other information on the badge.
8. Select either the **in.** or **mm.** option button to select either inches or millimeters as the measuring unit for the card size.
9. Select the **0.0 x 0.0** option button for a the default card size, or select the other option button and enter the width and height values for a custom card size.
10. For layout orientation of the card, select either the **Portrait** or the **Landscape** option button.

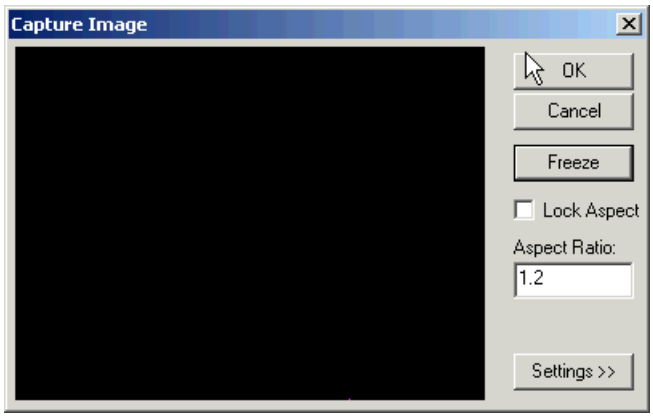
11. Select the **Print Both Sides** check box if your printer supports duplex printing (printing on both sides of the card).
12. Click **OK** to save your settings.
13. Select **Print** to print the card. Click **Cancel** to cancel the printing.

G.2.1.11 Capturing a Photo

1. Click a badge name from the Badging window.

Note: Select **Badge > Take Photo** from the menu bar, or click the **Take Photo** icon on the tool bar, or click the **Click here to capture Badge Photo** square within the Employee tab to display the Capture Image dialog box.

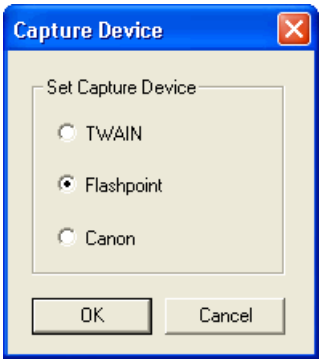
The way this dialog box looks on your screen will depend on the way you have configured your specific image capturing device. Follow the directions either for capturing a flash-point image or capturing a TWAIN image, as explained below.



Capturing a FlashPoint Image

Note: This section describes a specific instance of image capturing by using Pro-Watch. You may see a different screen depending on the specific image capturing hardware and software configured on your system.

1. Select **Badge > Set Capture Device** from the menu bar to display the Capture Device dialog box.

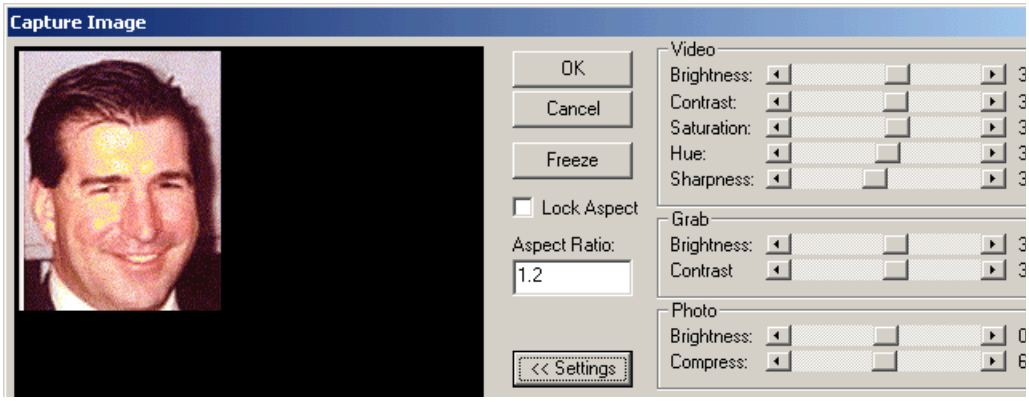


2. Select the **Flashpoint** (not TWAIN) option button to set your capture device and click **OK**. Note that it is necessary at this time to select **Flashpoint** (not TWAIN) in this dialog box to successfully capture a Flashpoint image. your capture device to TWAIN when using the FlashBusMV or Flashpoint 3Dx Lite PCI card
3. Select **Badge > Take Photo** from the menu bar, or click the **Take Photo** icon on the tool bar, or click the **Click here to capture Badge Photo** square within the Employee tab to display the Capture Image dialog box.
4. Click **Freeze** to fix the live video picture, or click **Freeze** again to return to the live video:



5. Click **Lock Aspect** to keep the ratio of the width of an image to its height, avoiding distortions. The aspect ratio is listed in the Aspect Ratio box.

6. To change the image quality settings and compression rates for the captured image, click **Settings**. The **Capture Image** dialog box displays additional fields:



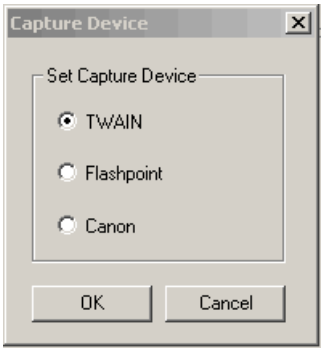
7. Define the Video, Grab, Photo settings by moving the corresponding sliders until the desired effect is attained.
8. Once you determine the image settings, click **<< Settings** again to return to the normal capture window.
9. When you have the desired image, click **OK**. This image is now linked to the badge holder's record, for display on the badge profile and badge layout.

Capturing a TWAIN Image

Note: This section describes a specific instance of image capturing by using Pro-Watch. You may see a different screen depending on the specific image capturing hardware and software configured on your system.

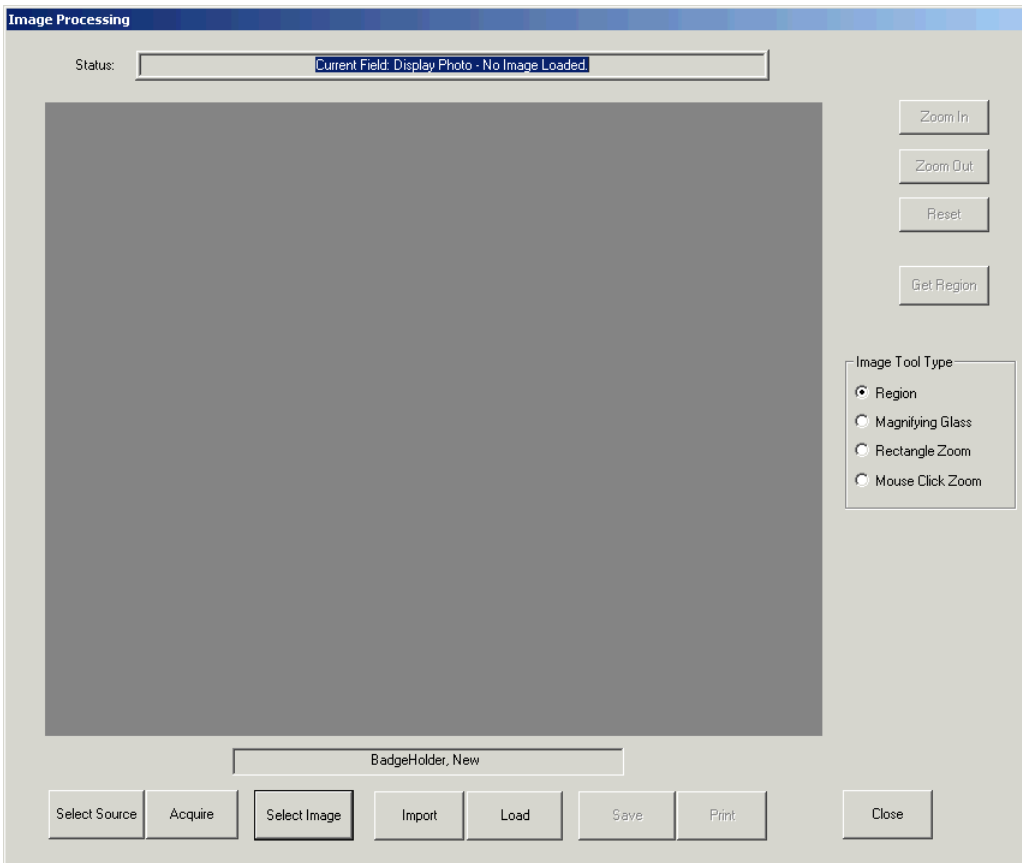
To capture a TWAIN image:

1. Select **Badge > Set Capture Device** from the menu bar to display the Capture Device dialog box with three options buttons:



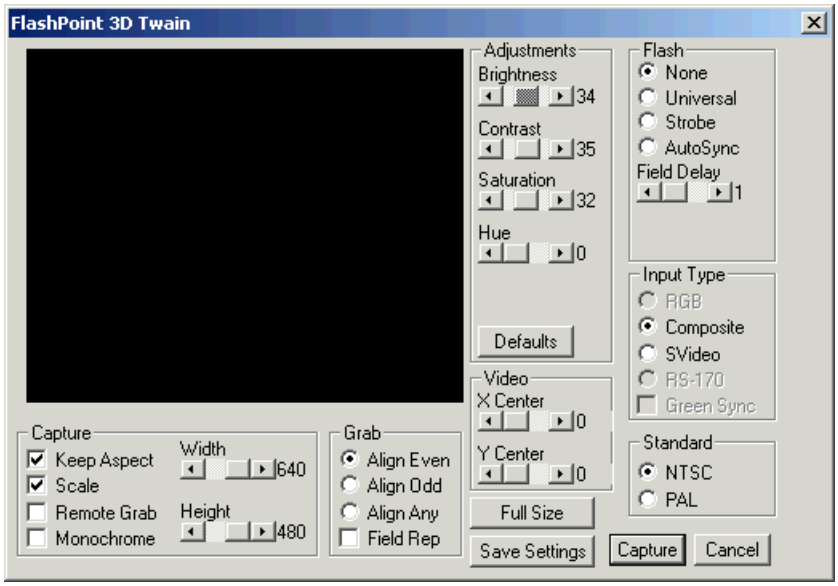
2. Select the **TWAIN** option button to set your capture device and click **OK**. Note that FlashBusMV uses the TWAIN device.

3. Select **Badge > Take Photo** from the menu bar, or click the **Take Photo** icon on the tool bar, or click the **Click here to capture Badge Photo** square within the Employee tab to display the Capture Image dialog box:



Note: Click **Select Source** and select **FlashBus TWAIN32** or **FlashPoint3D TWAIN32** as your source.
The content of the Select Source list will vary depending on the TWAIN-supporting camera devices installed on the Pro-Watch system.

4. Click **Select Image** to display the Select Document dialog box. Select **Display Photo** and click **OK**.
5. Click **Acquire** to display the **FlashPoint 3D Twain** screen:



6. Set the **Adjustment** controls for Brightness, Contrast, Saturation and Hue until you are satisfied with the image color and quality. Click **Defaults** to assign the default values.
7. Set the **Flash** controls by selecting None for no flash, or one of the following flash options: Universal, Strobe, or AutoSync. Use the slider control to set the desired value for Field Delay.
8. Set the **Capture** controls for Width and Height until you are satisfied with the image size and quality.
    - Click **Keep Aspect** to keep the ratio of the width of an image to its height, avoiding distortions. To change the ratio of the width of an image to its height and render it disproportionate, clear the Keep Aspect check box and then move the Width and Height sliders to the desired values.
    - Click **Scale** to create a thumbnail version that would still have proportionate Width and Height if Keep Aspect is checked. The scaled picture can have disproportionate width and height if Keep Aspect is not checked.
    - Click **Remote Grab** to capture a picture from a remote address.
    - Click **Monochrome** to capture a black and white image.
9. Set the **Grab** controls for Align Even, Align Odd, Align Any, and Field Rep to align the image.
10. Set the **Video** controls for X Center and Y Center to nudge the picture along the X and Y axes, respectively.
11. Set the **Input Type** controls by selecting either a Composite or SVideo type of image-input plug.

12. Select either NTSC (for United States) or PAL (for European) video **Standard**.
13. Click **Full Size** to view a larger image. Click **Settings** to revert to the original size picture.
14. Click **Save Settings** to save the current image settings to the registry so that they would be used the next time the dialog is initiated.
15. Click **Capture** to capture the image and revert to the **Image Processing** screen.
16. Use **Image Tool Type** controls to select a different part of the captured image.
    - Select the **Region** option button. Then click and drag the mouse to create a selection marquee on any part of the image. Click **Get Region** to capture only the selected region. Note that once you select a region, you cannot revert to the original picture by clicking **Reset**. The selection is not reversible.
    - Select the **Magnifying Glass** option button. The cursor transforms into a square magnifying glass. Click the mouse to magnify temporarily any section of the captured picture to view the details.
    - Select the **Rectangle Zoom** option button. The cursor transforms into a round magnifying glass with a plus (+) sign. Click and drag to magnify any section of the captured picture to view the details. Click **Reset** to revert to the original picture.
    - Click **Zoom In** as many times as necessary to zoom into the picture from its center. Click **Reset** to revert to the original picture.
    - Click **Zoom Out** as many times as necessary to zoom out of the picture from its center. Click **Reset** to revert to the original picture.
17. When you are satisfied with the final image, click **Save** to save the picture. Click **Close** to close the Image Processing screen, and To the original badge editing window. The Employee Tab will now be displaying the final saved image.

Capturing a Canon Image

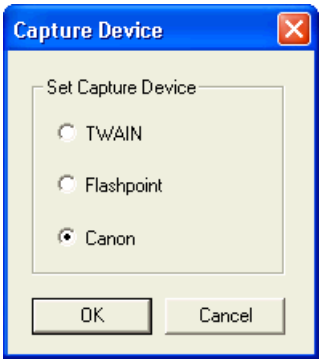
Before you can use a Canon camera to capture an image, you must ensure the following:

- You have the correct drivers. If you do not have the correct drivers, see your system administrator.
- The camera is attached via a USB port.

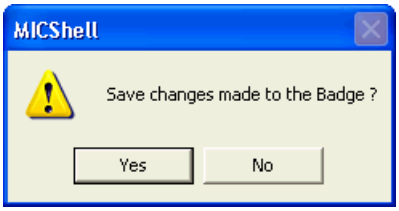
Note: This section describes a specific instance of image capturing with Pro-Watch. You may see a different screen depending on the specific image capturing hardware and software configured on your system.

To capture a Canon image:

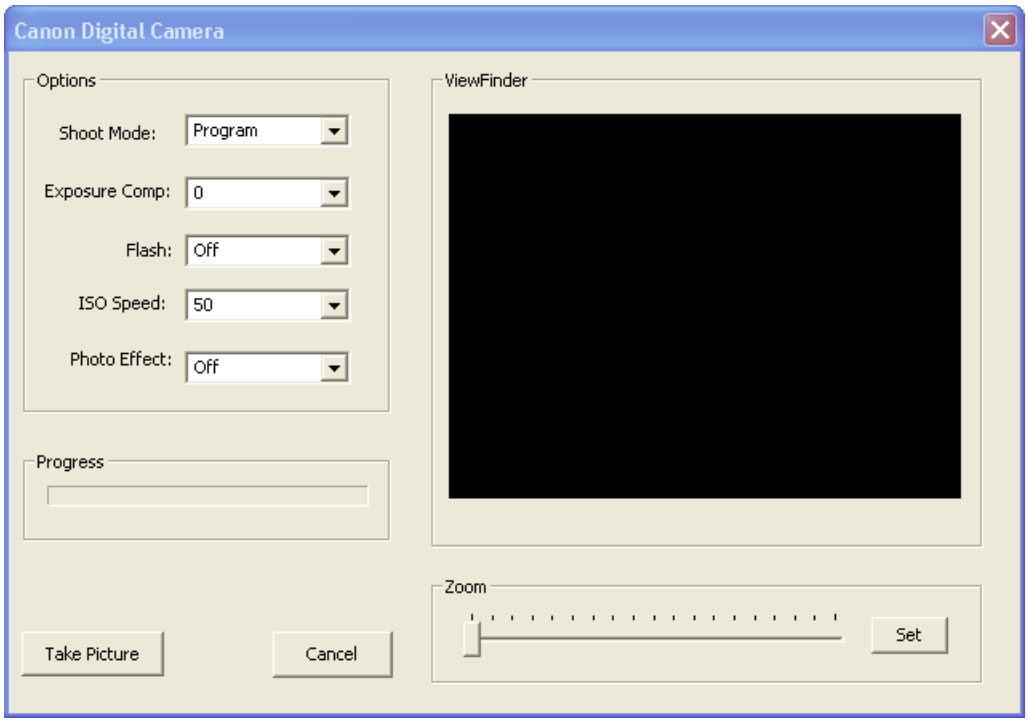
1. Select **Badge > Set Capture Device** from the menu bar to display the Capture Device dialog box with three option buttons:



2. Click the **Canon** option button to set your capture device and click **OK**.
3. Select **Badge > Take Photo** from the menu bar, or click the **Take Photo** icon on the tool bar, or click the **Click here to capture Badge Photo** square within the Employee tab. You may see the following dialog box:

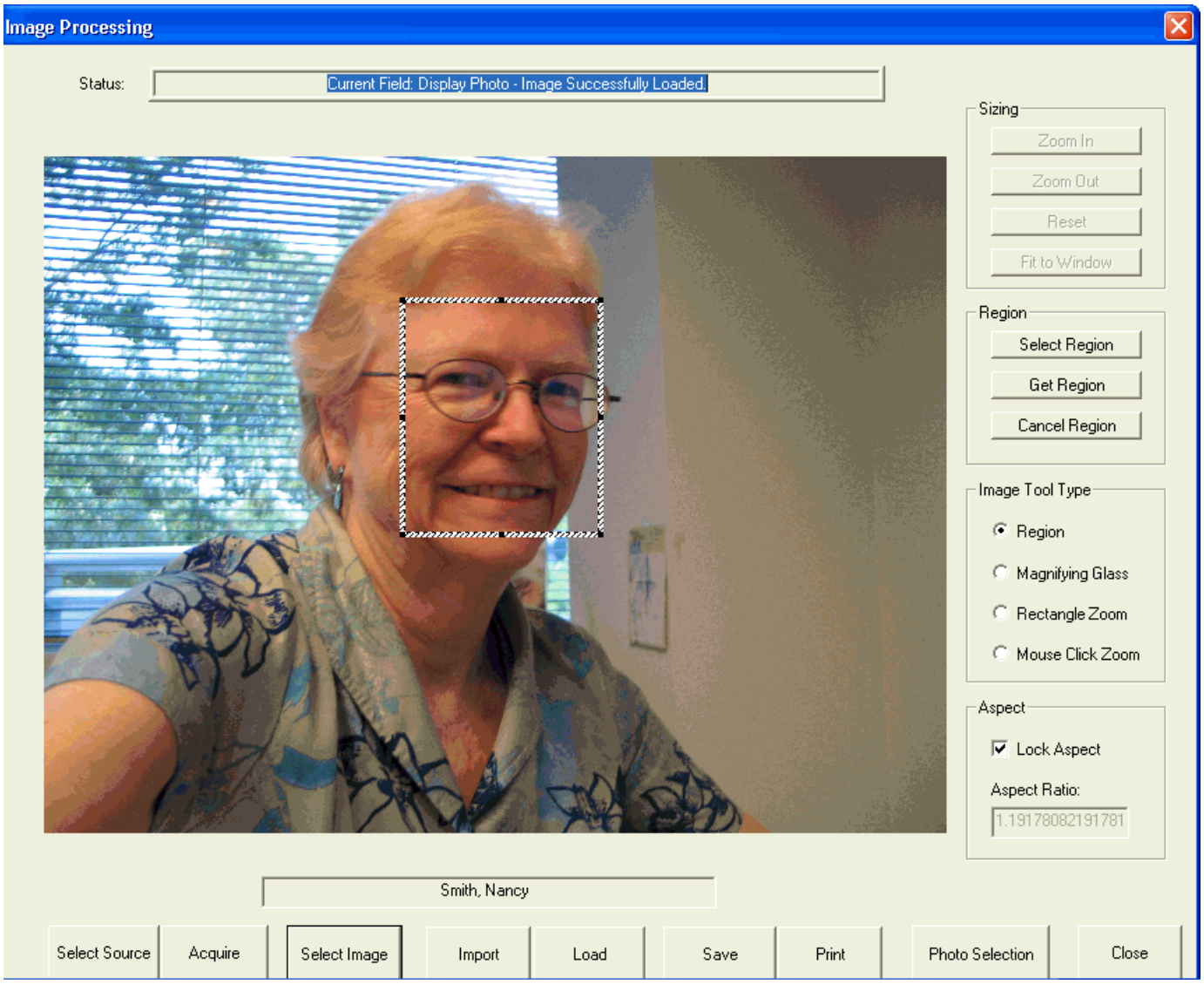


Click **Yes**.The Canon Digital Camera dialog box appears. Whatever is in the camera's viewfinder appears in the ViewFinder on this dialog box. The image is still dynamic.



In the Options section you can select your preferences for Shoot Mode, Exposure, Comp, Flash, ISO Speed, and Photo Effect. For more information on these options see the Canon documentation available at www.canon.com.

4. Click **Take Picture**. The Progress bar indicates the status of the picture being developed. When it is ready, the photo appears on the Image Processing screen.



Note: On the Image Processing screen you can focus the image as you want it. The marquee box has handles on the corners and sides that you can use to frame the precise image you want.
The Lock Aspect check box must be unchecked for this operation. If the box is checked you cannot alter the size of the marquee box at all. Check this box only when you have sized the image to your satisfaction. In addition, tools are provided on the left to help you refine the image. In the **Sizing** section, you can specify size controls. Options include:

- Zoom In/Out—Zoom in or out of the picture from its center. Click Reset to revert to the original image.
- Reset—Click to revert the image to its original size.

- Fit to Window—Fit the photo to fill up the window. In the **Region** section, you can Select Region or Get Region to view a specific area of a picture. You can also Cancel Region. Note that once you select a region, you cannot revert to the original picture by clicking **Reset**. The selection is not reversible. In the **Aspect** section, you can Lock Aspect when you are ready to keep the ratio of the width of an image to its height, thus avoiding distortion. You can also type in a custom aspect ratio. In the **Image Tool Type** section, you can focus on a special part of the captured image. Options include:
  - Region—Enables you to move the marquee box around the screen.
  - Magnifying Glass—The cursor transforms into a square magnifying glass. Click the mouse to magnify temporarily any section of the captured picture to view the details.
  - Rectangle Zoom—The cursor transforms into a round magnifying glass with a plus (+) sign. Click and drag to magnify any section of the captured picture to view the details. Click Reset to revert to the original image.
  - Mouse Click Zoom—The cursor becomes a round empty magnifying class. Click anywhere to enlarge the entire image.

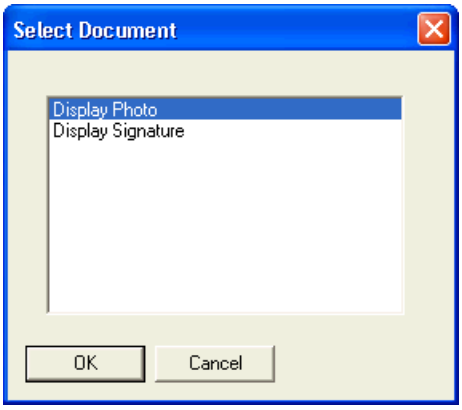
5. The command buttons enable you to perform several functions.

- If you are going to use a different camera model than the one already used, click **Select Source** to view a list of available camera models, select the model of the new camera, and click **OK**.



- Click **Acquire** to return to the Canon Digital Camera dialog box described above.

- Click **Select Image** to display the Select Document dialog box where you can specify the display. Select **Display Photo** and click **OK**.

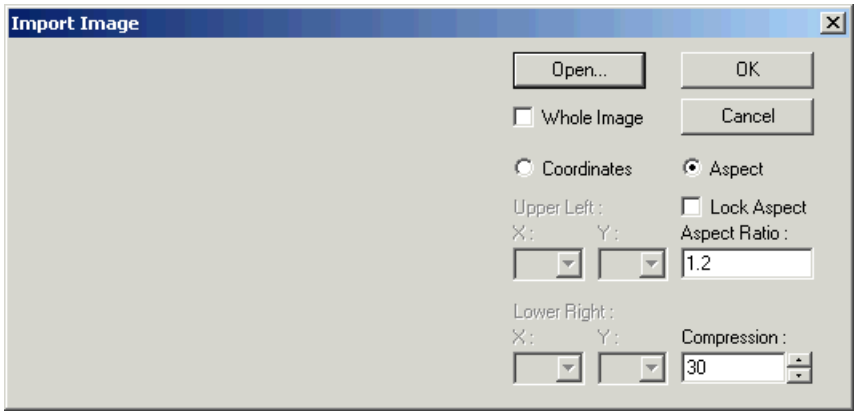


- Click **Import** to import another photo.
- Click **Load** to load another photo.
- Click **Save** to save the image. When you return to the Employee tab, the photo appears in the Display Photo box.
- Click **Print** to print the image.
- Click **Photo Selection** to display a panel of shots you can choose from to decide which one will be the final shot. Each shot varies in its intensity level. Highlight the photo with the desired intensity level and click **OK**. See "Setting Badge Photo Compression and Intensity" in Chapter 5 for information about setting the intensity levels that will appear on this screen.
- Click **Close** to return to the Employees tab.

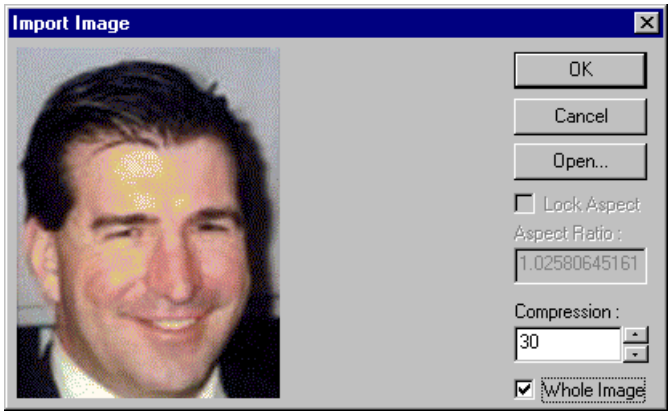
6. When you are satisfied with the final image, click **Save** to save it. Click **Close** to close the Image Processing screen and return to the original badge editing window. The Employee Tab now displays the final saved image.

G.2.1.12 Importing a Photo

1. Select a badge name from the center pane of the Badging window.
2. Select **Edit > Modify** from the menu bar, or click **Modify** button on the tool bar.
3. Select **Badge > Import Photo** from the menu bar or click the **Import Photo** icon on the tool bar to display the Import Image dialog box:



4. Click **Open**. Locate the image you want to import from the resulting Windows Open dialog.
5. Click **Open** to display the selected image in the Import Image dialog box:

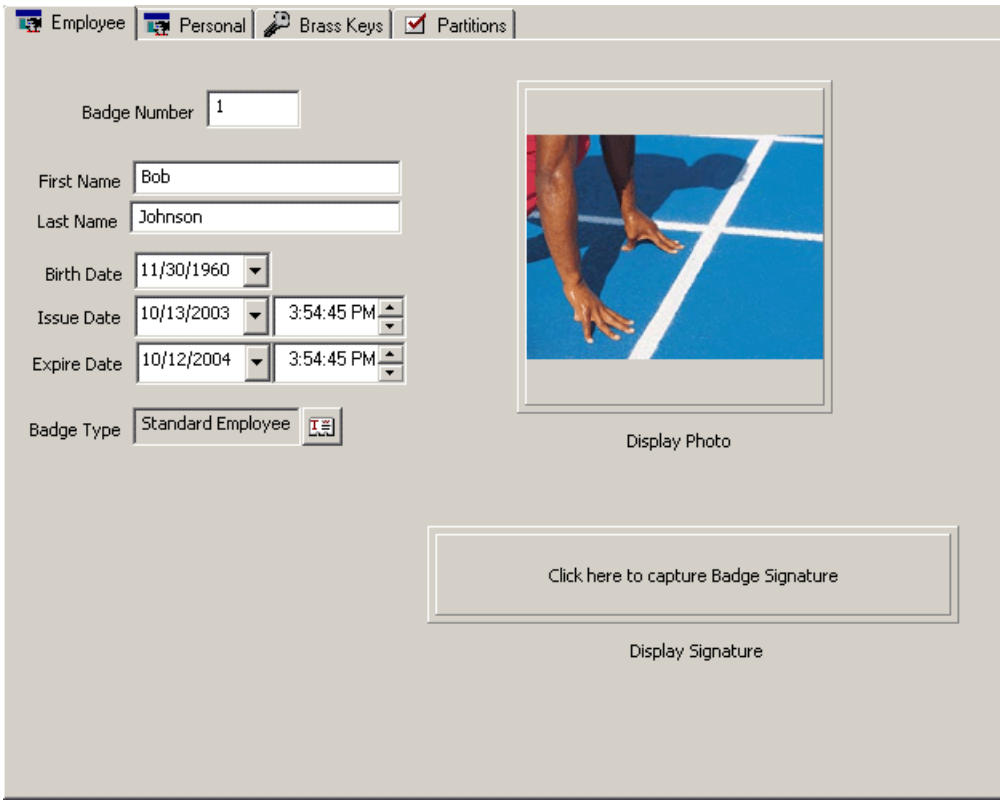


6. Select **Lock Aspect** to keep the ratio of the width of an image to its height; thus, avoiding distortions, or type in a custom aspect ratio.
7. Use the **Compression** box to set the compression level used to save the image file. The higher the number, the more compressed the file will be. Higher compression will save disk space when storing large numbers of image files.
8. Select **Whole Image** to capture the entire image, or deselect **Whole Image** to use the image crop tool for selecting only a portion of the captured image.

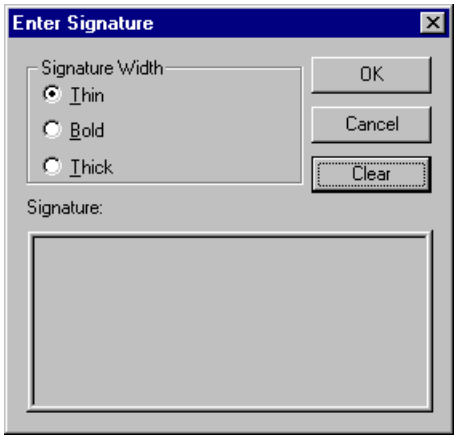
9. Click **OK**.

G.2.1.13 Capturing a Signature

1. Select a badge name from the Badging window to display the badging tabs:



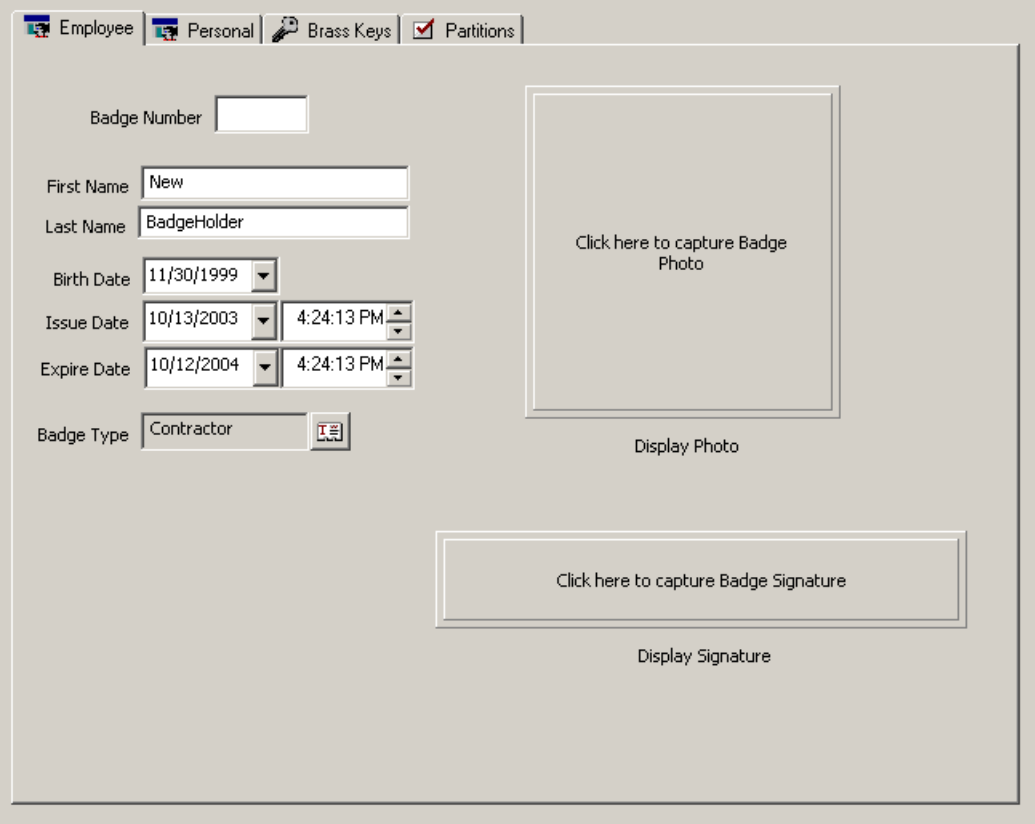
2. To capture a badge signature, click the **Capture Signature** icon, or click Click here to capture Badge Signature. The **Enter Signature** dialog box appears:



3. Go to the Signature Width section of the dialog box if your signature capture pad supports different line styles. Click **Thin**, **Bold**, or **Thick** line style.
4. Have the badge holder sign the signature capture pad.
5. Click **OK**. The captured signature is linked to the badge holder's record, and displays on the profile and badge layout.

G.2.1.14 Importing a Signature

1. Select a badge name from the Badging window to display the badging tabs:



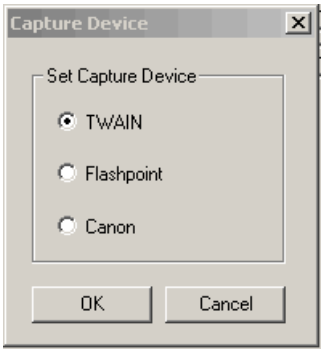
2. Click the **Import Signature** button on the tool bar, or select **Badge > Import Signature** from the menu bar.
3. Using the Windows Open file dialog, navigate to the location of the file that you want to import. The file must be in BMP or EMF (Enhanced Metafile) format.
4. Click Open. If a signature file for this badge holder already exists, the system prompts for overwrite. Click **Yes** or **No**. The new signature displays on the badge holder record. The actual location of the signature file is based on the configuration for the Signature BLOB type.

G.2.1.15 Setting the Capture Device

The capture device must either be a TWAIN or Flashpoint device. Specify the format that matches your photo capture device.

To set the capture device:

1. Select **Badge > Set Capture Device** from the menu bar to display the set capture device dialog box:



2. Select either **Twain** or **Flashpoint** as your image capturing device. Then click **OK** to close the dialog box and go back to the editing window.

G.2.1.16 Exporting an Image

The image export functionality exports images to the file system since some users want to use the images in other applications. The export facility allows users to export the photos, whether they are stored in a directory or in the database, and annotate them such that they can identify and use the images when needed.

G.2.1.17 Deleting a Badge

1. In the Badging window, select the badge(s) you want to delete.
2. Select **Edit > Delete** from the menu bar or click the delete icon on the tool bar. The prompt “You have selected [number] badges for deletion. Continue?” appears.
3. Click **OK** to delete the badge(s).

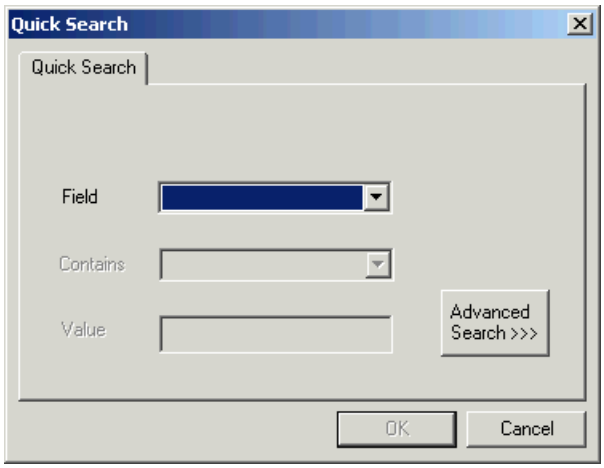
G.2.1.18 Searching for Badges

You have two search options to find a specific badge:

- "Quick Search" – searches on one field.
- "Advanced Search" – searches on multiple fields and sorts the results.

Quick Search

1. Select **Edit > Quick Search** from the menu bar or click the **Quick Search** icon on the screen. The Quick Search dialog box appears. Note that you can also conduct a search by using the quick search fields configured in the Badge Builder utility when you have created the badge profile (see Chapter 60, Badge Building). These search fields are displayed in the center pane, on top of the badge list.



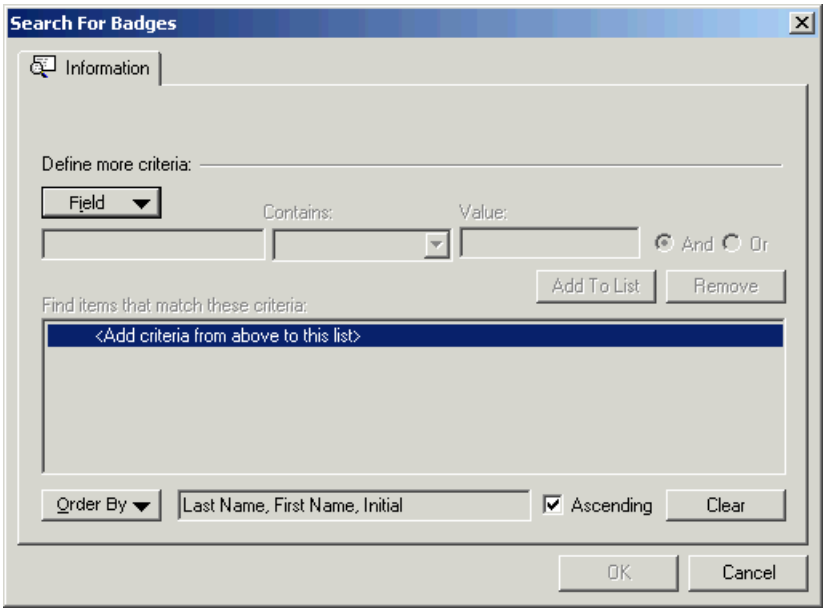
2. Select field criteria:

Field	Description
Field	Select a field name from the drop-down list.
Contains	Select a qualifier from the drop-down list.
Value	Enter a value for the field you selected.

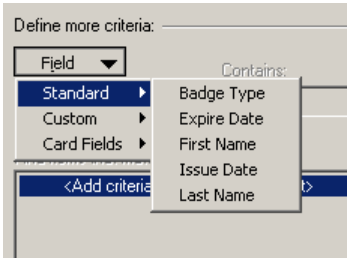
3. Click **OK.**

Advanced Search

1. Select **Edit > Advanced Search** from the menu bar or click **Advanced Search** in the Quick Search screen. The advanced search screen appears:



2. Select your search field:

Field	Description
Field	Select a field type from the drop-down list. Click the **Field** drop-down list to display three options: **Standard**, **Custom**, and **Card Fields:**.  • **Standard** fields: Badge Type, Expire Date, First Name, Issue Date, Last name. • **Custom** fields: Address 1, Address 2, Badge Number, Birth Date, City, Department, Employer, Extension, Home Phone, Office Phone, Social Security, State, Supervisor. • **Card Fields**: Card Number, Card Expiration Date, Card Issue Date, Clearance Code, Company Name, Status Code.

Field	Description
Contains	Select a search criterion from the context-sensitive drop-down list. These criteria change depending on the **Field** selected: • Example criteria for **Standard** fields: Equal To, Not Equal To. • Example criteria for **Custom** fields: Begins With, Contains, Ends With, Equal To, Not Equal To, Is Empty. • Example criteria for **Card Fields**: Begins With, Contains, Ends With, Equal To, Not Equal To, Is Empty. **Note:** The criteria is not fixed for Standard, Custom and Card Fields. The criteria is based on the type of field selected. • For example: • The Resource field type will contain “Equal To” and “Not Equal To.” • Date field type will contain “Equal To,” “Not Equal To,” “Greater Than,” “Less Than,” “Is Empty.” • Etc.

Field	Description
Value	Enter a value for the field you selected. The Value field will display a context-sensitive **browsing button** for your convenience when you select the following search **Fields**: • Standard > Badge Type. • Standard > Expire Date. • Standard > Issue Date. • Custom > Birth Date. • Custom > Employer. • Card Fields > Card Expiration Date. • Card Fields > Card Issue Date. • Card Fields > Clearance Code. • Card Fields > Company Name. **Note:** You can also use this field to reset the search criteria and display all badges in the list by entering the percentage symbol (%) in the field.

3. Select **And** to include additional search criteria to the previously designated search criteria, or select **Or** to search for an alternative criteria. Use both of these options when you have more than one criterion you want to use.
4. Click **Add to List** to add the defined criteria to the search requirements. Any items that match your search criteria are listed in the lower portion of the dialog box.
5. If you need to remove a search criteria, select it from the criteria list and click **Remove**.
6. Select the field for ordering search results
7. Select ascending order in the check box, if required.
8. Click **OK**.

G.2.2 Concurrency Check

When more than one users are trying to change the same badging fields simultaneously, Pro-Watch performs a “concurrency check” to make sure that a user does not change the value of a field without first viewing the value entered and saved by another user. This functionality prevents changing the field values by inadvertently deleting the work of others.

The badging actions listed below will trigger a concurrency violation message. These are exactly the same actions that trigger checks to see if required badging fields are filled in.

If you leave a “required field” blank, you cannot execute any of the following:

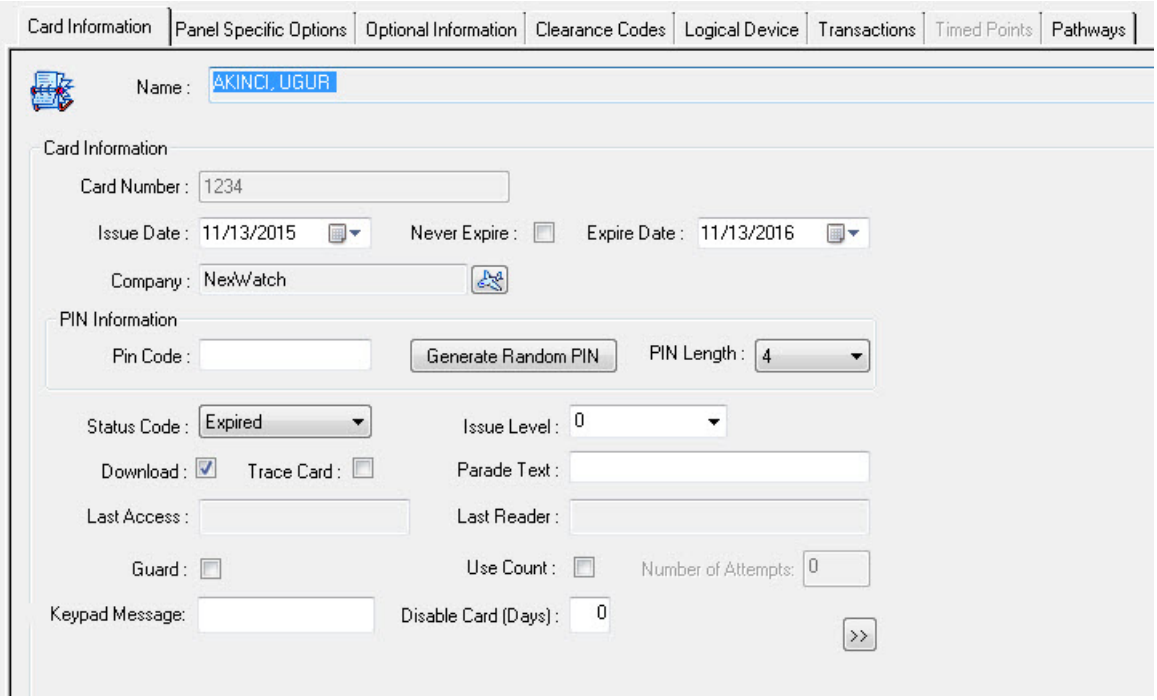
- Bulk adding badges.
- Adding a single badge.
- Explicitly saving a badge from the menu.
- Advanced find.
- Next badge.
- Previous badge.
- Adding a new card.
- Pasting a card.
- Adding a biometric card.
- Editing front or back card layouts.
- Print previewing a card.
- Printing a card.
- Exiting badge viewer, or Pro-Watch. (The application will allow the user to exit. The error message will appear, but Pro-Watch will not save the user's changes.)
- Batch modify.
- Badge quick search.
- Badge progressive search.
- Selecting another badge with the mouse or arrow keys.
- Calculate expire date. (Detroit functionality)
- Calculate badge number. (Detroit functionality)
- Select last badge.
- Select first badge.
- Edit card.
- Delete card.
- Import signature.
- Capture signature.
- Import photo.
- Take photo.
- Delete badge.
- Image export.
- Process image.
- Profile image action. (For example, capturing a signature by clicking on it.)
- Downloading a card by clicking the “lightning button”  on the tool bar.

G.3 Cards

Each badge can be assigned multiple cards. Each card defines specific access privileges for the badge holder. For example, a card defines card number and PIN information, panel-related information, optional information, clearance codes, logical devices, transactions, and pathways.

G.3.1 Adding or Editing a Card

1. To add a new card to a badge, select the badge in the center pane. Then select **Cards > New Card** from the menu bar or click the **New Card** icon on the toolbar to display the card tabs window:



2. To edit an existing card, select it from the bottom of the Badging window. Then either double-click the card or click the **Card Properties** icon on the tool bar to display the same card tabs window shown above.
3. Complete the following tabs to add or edit a card.

CARD TABS LIST

- "Card Information Tab".
- "Panel-Specific Options Tab".
- "Optional Information Tab".
- "Clearance Codes Tab".
- "Logical Devices Tab".

- "Transactions Tab".
- "Timed Points Tab".
- "Pathways Tab".

G.3.1.1 Card Information Tab

Use the following field definitions to complete this tab:

Field	Description
Name	First name and last name of the cardholder.
Card Number	A unique number assigned to the card. **Note:** This is a required field that you need to fill to save a card. To assign an automatically incremented card number to a new card: Close all open screens in Pro-Watch. Select File > System Options from the main menu. Click and select the Additional Server Options tab. In the Card Seed field enter the number which will be defaulted for the card number whenever a new card is added or copied and pasted. The card number gets incremented by "1" after every attempt. Click OK. Caution: Do not include leading zeros in the card number. For example, to create card number 89, enter "89" instead of "00089." Use of leading zeros can cause errors when the cards are downloaded to the panel.
Issue Date	The date on which the card is issued. You can type in the date directly or select one from the drop-down calendar.
Never Expire	When checked, the card never expires.
Expire Date	The date on which the card will expire. You can type in the date directly or select one from the drop-down calendar.

Field	Description
Company	The company name. This is a required field. Click the Company icon to display the pop-up menu. All clearance codes that you assign to the company while configuring the database (see "Adding or Editing Companies" in Chapter 38) are shared by all the cardholders in that company. Select Define to display the Companies dialog box where you can select, add, edit or delete a company. **Note:** When you modify a company for a card, only company-level clearance codes get replaced with the new company clearance codes. However all clearance codes that were added directly from the clearance code tab remain unchanged. **Note:** Pro-Watch records database changes associated with clearance code assignment to a company, clearance code assignment to a card, logical device assignment to a card, and company assignment to a card in order to comply with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11), and for compliance tracking. The compliance tracking requirements use the aggregated logical devices's most restrictive settings.
PIN Information	Enter a Pin Code or click Generate Random PIN to have Pro-Watch generate a random PIN for you. PIN Length determines the length (number of characters) of the PIN number. This length should be the same length that is specified when configuring a panel (see "Panel Tab" in Chapter 9). For the PW-5000 panel, for example, the full PIN specified for a Card will not be operative unless the PIN specified for the panel is at least equal in length. Note that when a Matrix panel is configured, select "Matrix Pin" from the PIN length drop-down list. The "Generate Random PIN" button then changes to "Set Matrix PIN: [number]. Press this button to set the number. If you are using Matrix and non-Matrix panels and want the card to have the same PIN code for all panels, use the displayed Matrix number.
Status Code	Select a card status from the drop-down list: Active, Disabled, Expired, Lost, Stolen, Terminated, Unaccounted and Void.

Field	Description
Issue Level	The issue level is used to differentiate between one or more cards with the same card number. Select from the drop-down list a value between 0 (zero) and 10. A level of "0" (zero) means that either the issue levels are not being used, or the card has not ever been re-issued. Pro-Watch supports up to 10 re-issues of the same card. The issue level is nearly always used in situations where a cardholder loses his card and needs to have one re-issued at a time when issuing a new card number is not feasible. For example, this is the case when the social security number is used as the card number. The newly re-printed card has a different issue level. Thus, the old card, if found, does not work.
Download	Select this check box to allow the downloading of card information to a panel.
Trace Card	Select this check box to allow a trace and create visible transactions in Transactions tab.
Parade Text	Enter a message to display on the card reader when the card is swiped. The reader must support this function.
Guard	Select this check box to enable the cardholder to participate in the Guard Tour.
Use Count	Select this check box to make it possible to set the number of times a specific card/PIN can be used to gain access. See Number of Attempts (below).
Number of Attempts	Enter the maximum number of times a card/PIN can be used to gain access. For instance, if the number is set to 3, that particular card/PIN will be granted access three times. After that, access will be denied and the card will be disabled/deactivated.
Disable Card (Days)	Enter the number of days of a card's inactivity, after which the card will be automatically disabled. The period of days begins on the day the card was last used, and it expires at midnight of the last day in the period.

Field	Description
Keypad Message	Enter the text that will be displayed on the first line of the keypad's LCD display when a user uses that specific card. The text is restricted to 16 characters.

G.3.1.2 Requiring a Supervisor PIN to Activate

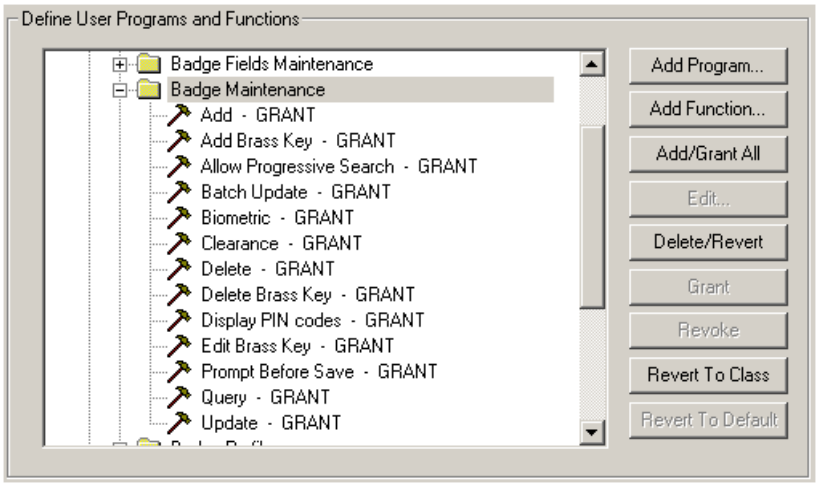
Selecting the "Active" status code for the card activates the card. There may be some circumstances when you would prefer to have a card activated by a supervisor rather than by the staff member who normally enters the card information. Pro-Watch provides two permissions functions that work together to accomplish this. Note that you can assign these permissions either to a user or to a class. To find the functions, go to **Database Configuration > [Users or Class] > Programs > Badge Maintenance > Badge Maintenance**.

- Display Supervisor PIN—Designates the user as a supervisor, and enables you to create a supervisor PIN for her in the **Database Configuration > User Properties > User Information** tab. This supervisor PIN, or another supervisor PIN, will be required by any user who has been assigned the Require Supervisor PIN function that is described below).
- Require Supervisor PIN—Displays a supervisor PIN prompt when a non-supervisor user tries to save a created or edited card in Badging with an Active card status. This requires the user to either obtain the supervisor PIN from a supervisor or have the supervisor enter the supervisor PIN to complete the card activation.

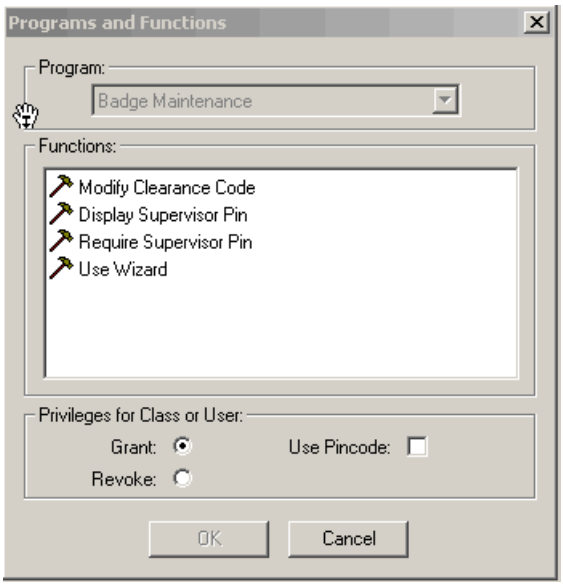
Note: The Supervisor PIN feature is not operational for a User or a Class by default; you must manually follow the procedure given below.

Follow these steps to designate a user as a supervisor and assign a supervisor PIN:

1. At the Pro-Watch main screen, select **Database Configuration > [Users or Class]**. Double-click the user's icon to display the user properties.
2. Select **Programs > Badge Maintenance > Badge Maintenance**.

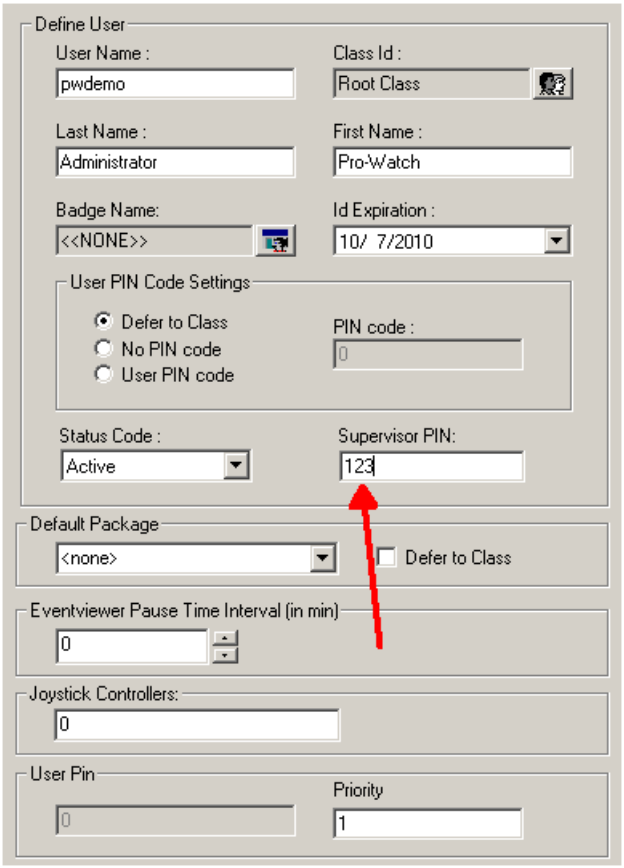


3. Click **Add Function** to display the Programs and Functions dialog box.



4. Select Display Supervisor Pin, be sure that **Grant** is selected in the Privileges for Class or User box, and then click **OK**.
5. In Database Configuration, go to **Users** and click the user's icon to display the User Information tab in the user properties. Find the newly

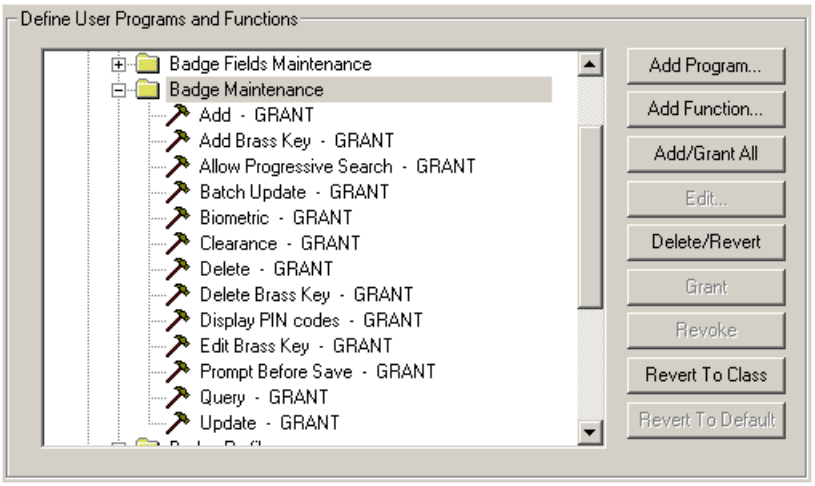
created Supervisor PIN field in the Define User block, and enter a PIN for the supervisor.



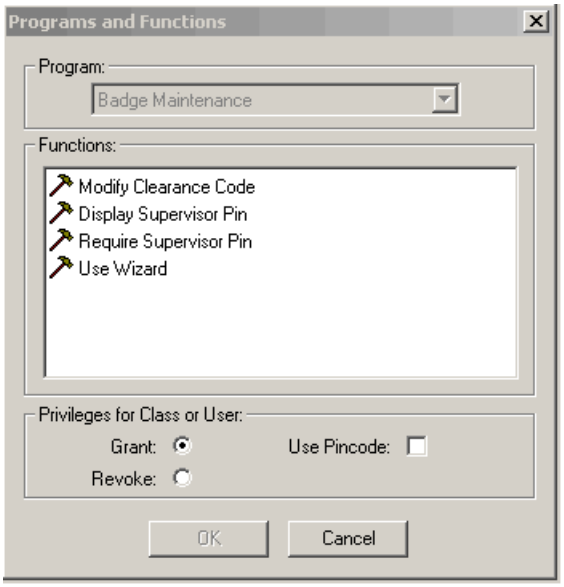
Next, follow these steps to prevent a non-supervisory user from saving a created or edited card without a supervisor entering her PIN:

1. At the Pro-Watch main screen, select **Database Configuration > [Users or Class]**. Double-click the user's (or class's) icon to display the user (or class) properties.

2. Select **Programs > Badge Maintenance > Badge Maintenance**.



3. Click **Add Function** to display the Programs and Functions dialog box.



4. Select **Require Supervisor Pin**, be sure that **Grant** is selected in the Privileges for Class or User box, and then click **OK**. This user now cannot save a created or edited card without having a supervisor enter her PIN in a prompt box that appears when the user clicks **Save** to save the card.

Note: To restore a user's permission to save a created or edited card without a supervisor PIN, return to the Define User Programs and Functions dialog box (**Database Configuration > [Users or Class] > Programs > Badge Maintenance > Badge Maintenance**), select the **Require Supervisor PIN** function, click **Revoke**, and then click **OK**.

G.3.1.3 Panel-Specific Options Tab

The specific options appearing in this tab will depend on the specific channel (PW-5000, CHIP, SEEP, Cardkey, or Matrix). Only these four panels have specific options. Use the following field definitions to complete this tab:

Panel	Option	Description
PW-5000	ADA	ADA refers to "Americans with Disabilities Act." Select this check box to allow for extended shunt time on a door so that someone in a wheelchair, for example, has enough time to get through the door without generating an alarm. The "extended shunt time" needed is set up on the PW-5000 door configuration.
	PIN Exempt	Select this check box to make sure that if a door requires both a card and a PIN, a PIN-exempt cardholder will not need to enter a PIN.
	User Level	The user level is often used to make some cards accomplish special tasks. For example, a manager may want to use such a card to automatically unlock the lobby doors at the beginning of a shift. Panel-level triggers and procedures can be written to trigger only on valid card accesses where the cardholder user level is equal to the user level set in the trigger. Allowed user level values range between 0 (zero) and 255. If a user enters anything out of this range Pro-Watch displays a validation error message and prompts the user to enter a proper value.
	VIP	Select this check box to exempt the cardholder from anti-passback restrictions. A cardholder with VIP privileges can pass his/her card to the next person to swipe and pass through a reader. Note that selecting this check box automatically selects the Executive Priv. check box for the Cardkey panel.

Panel	Option	Description
SEEP	Privilege	Select this check box to allow a cardholder to open/limit/close a building by use of a station reader keypad or a station reader and input point button. Note that selecting this check box automatically selects the Privilege check box for the CHIP panel.
	1030/1040	1030/1040 denotes a combination of different card types. Select this check box to allow cards to be downloaded correctly when there is a mixture of cards, such as 1030/1040/1050.
	Use Alternate Fac Code	Enabled only when 1030/1040 is selected. Select this check box to have Pro-Watch use an alternative facility code to allow the cardholder enter a facility even when the main facility code does not match.
CHIP	Privilege	Select this check box to allow a cardholder to open/limit/close a building by using a station reader keypad or a station reader and input point button. Note that selecting this check box automatically selects the Privilege check box for the SEEP panel.
	Visitor	Select this check box to confirm the user as a valid visitor as required by some event actions.
	Escort	Select this check box to confirm the user as a valid escort as required by some event actions.

Panel	Option	Description
Cardkey	Threat Level	In the Cardkey panel, doors and cards can be assigned a numerical "threat" level. These levels are arbitrary, except that the threat level of the card must be greater than or equal to the threat level of the door to gain access. Valid threat level values range between 0 (zero) and 99. If a user enters anything out of this range Pro-Watch displays a validation error message and prompts the user to enter a proper value. In general practice most users are assigned a threat level of zero. A few users get a higher level. During an emergency event, the system administrator increases the threat level for all doors. During this time of "increased threat," only those few individuals will be able to go through those doors.
	Event Level	In Cardkey panel, a card with an event level "n," upon a valid access, will cause all card events of level "n" or less to be executed at the panel which controls the card reader. Valid event level values range between 0 (zero) and 7. If a user enters anything out of this range Pro-Watch displays a validation error message and prompts the user to enter a proper value. Card events are defined on a tab on channel maintenance (for Cardkey channels only). Typical uses for this include elevator control, as well as local silencing of horns and sirens associated with doors.
	Timed Override	Select this check box to enable a door stay open for a specified amount of time.
	Executive Privilege	Select this check box to allow a cardholder to open/limit/close a building by use of a station reader keypad or a station reader and an input point button. Note that selecting this check box automatically selects the VIP check box for the PW-5000 panel.
	STI Download	STI stands for a specific type of sub-panel (others are OCT, AMT). Select this check box to download the card information to an STI sub-panel. STI's memory capacity is much more limited than that of the Cardkey. But STI can grant access to a door for those cards the information of which is downloaded.

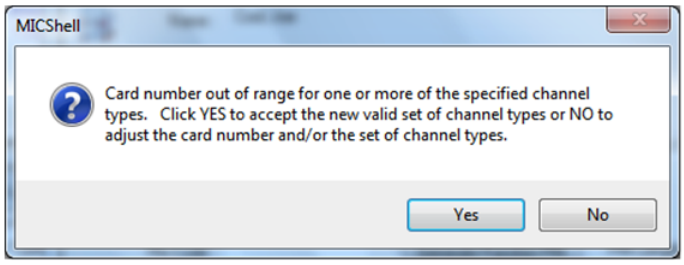
Panel	Option	Description
Matrix	Arm	Indicates that the cardholder is authorized to use the “A” and “D” keypad keys to arm and disarm a reader and/or zone.
	Guard	Indicates that the cardholder is authorized to clear local alarms by using the “C” keypad key.

G.3.1.4 Optional Information Tab

Use the following field definitions to complete this tab:

Field	Description
None	Specifies that you do not want to set any optional information.
Timed Points	Activates the Disarm Logical Device and Arm Logical Device fields and enables you to select and edit Logical Devices for these fields. If you select a Logical Device for the Disarm Logical Device field, a user’s valid card read at that device masks or shunts the Monitorable Inputs specified in the Timed Points tab. The mask or shunt lasts (is “timed”) for 180 minutes. The 180-minute period renews with each valid card read. Conversely, if you select a Logical Device for the Arm Logical Device field, a user’s valid card read at that device unmasks the Monitorable Inputs specified in the Timed Points tab.
Default Company	Enabled only when Timed Points option button is selected. Click this button to set the Disarm and Arm Readers to the Enrollment and De-Enrollment Readers on the First Timed Clearance Code from the Company, if applicable.
Default Card	Enabled only when Timed Points option button is selected. Click this button to set the Disarm and Arm Readers to the Enrollment and De-Enrollment Readers on the First Timed Clearance Code from the current Card, if applicable.
Start Pathway	Activates a configured pathway. A pathway allows a badge holder to follow a clear path through a building without setting off alarms (see "Pathways Tab").

Field	Description
Stop Pathway	De-activates a configured pathway. A pathway allows a badge holder to follow a clear path through a building without setting off alarms (see "Pathways Tab").
Disarm Logical Device	Requires Timed Points to be selected. When you select a Logical Device for the Disarm Logical Device field, a user's valid card read masks or shunts the Monitorable Inputs specified in the Timed Points tab. The mask or shunt lasts (is "timed") for 180 minutes. The 180-minute period renews with each valid card read.
Arm Logical Device	Requires Timed Points to be selected. When you select a Logical Device for the Arm Logical Device field, a user's valid card read unmasks the Monitorable Inputs specified in the Timed Points tab.

Field	Description
Valid Card/Channel Types	 Select the card/channel type(s) appropriate for your card. This selection will determine the maximum number of digits you can enter for your card number. If the number is greater than what is allowed by the data limit of the panel selected, you'll get the following error message:  Click YES to accept the new valid set of channel types or NO to adjust the card number and/or the set of channel types. CAUTION: If you click YES, Pro-Watch may truncate the card number to a length permitted by the channel type(s) you've selected. Also see: Section 5.3.8, Setting Database Limits, in Chapter 5, "Overview" in Chapter 5.

G.3.1.5 Clearance Codes Tab

Note: The Pro-Watch records database changes associated with clearance code assignment to a company, **clearance code assignment to a card**, logical device assignment to a card, and company assignment to a card in order to comply with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11), and for compliance tracking. The compliance tracking requirements use the aggregated logical devices's most restrictive settings.

This tab enables you to add, edit and delete clearance codes for a card.

A clearance code grants or denies badge holder access to enterprise doors and elevators.

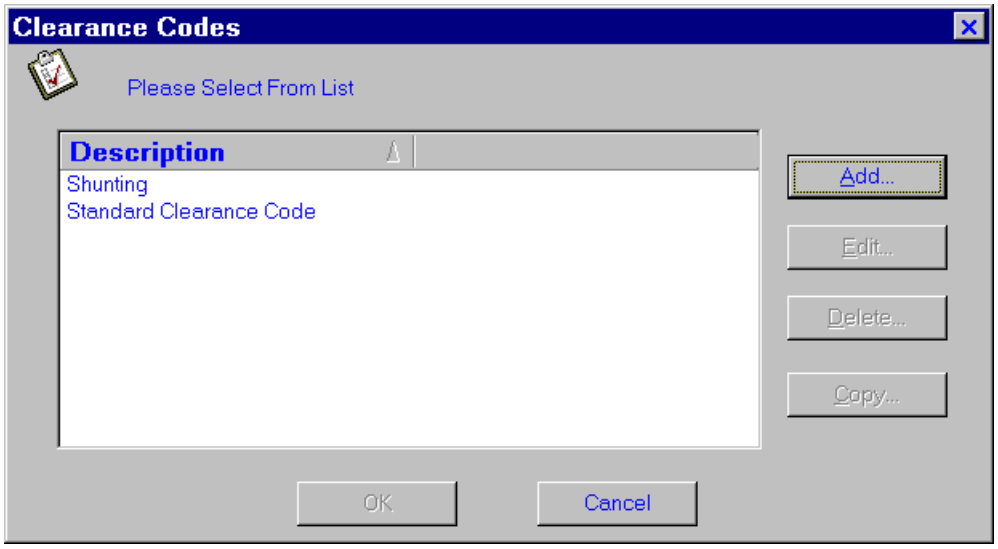
A clearance code set at the company level applies to everyone working for that company. However, you can assign to individual users clearance codes that override company-level clearance codes.

Notes:

- Logical Device access assigned at the card level (PW-5000/3000/2000 only) overrides company-level clearance codes.
- Clearance codes can be created, edited and deleted through the Database module as well. See "DBC - Clearance Codes" in Chapter 37.

To add an existing clearance code to a card:

1. In the Clearance Code tab, within the Current Clearance Codes Assigned to Card dialog box, select **Clearance Codes**.
2. Click **Add**. The Clearance Code dialog box appears.

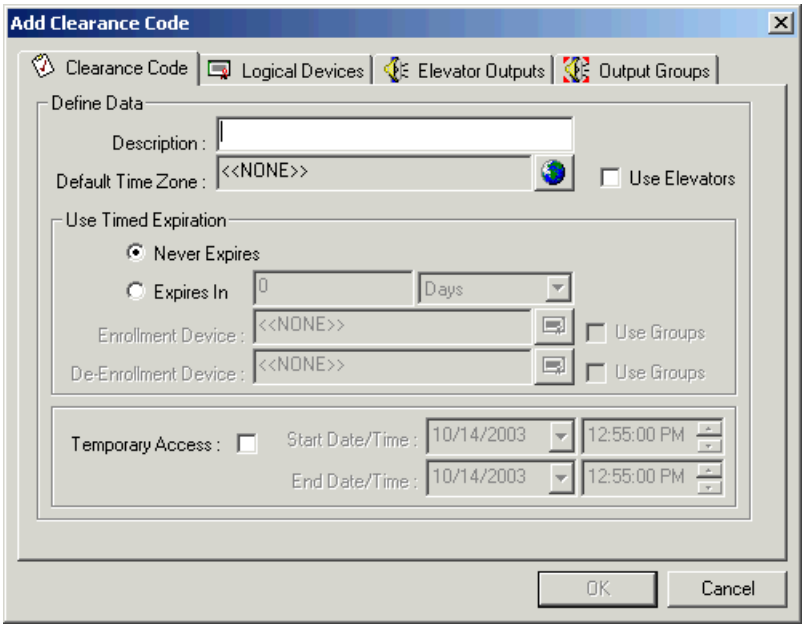


3. Select a clearance code description.
4. Click **OK**.

To add a new clearance code to the list of clearance codes:

Note: The new clearance codes configured as a Timed or Temporary code are automatically saved in their respective Timed Clearance Codes and Temporary Clearance Codes folders.

1. In the Clearance Code tab (within the Current Clearance Codes Assigned to Card dialog box) select **Clearance Codes**.
2. Click **Add**. The Clearance Code dialog box appears.
3. Click **Add** again to display the Add Clearance Code dialog box.



4. Select the **Clearance Code** tab of the Add Clearance Code dialog box to enter the following information on your new clearance code:
    - **Description**. A description of the clearance code you are creating.
    - **Default Time Zone**. If "None," click the icon and select **Define** from the pop-up menu. Time Zones dialog box displays. Select a **time zone** and click **OK**. To add, edit or delete a time zone click **Add**, **Edit** or **Delete**, respectively. Note that the default Time Zone for any clearance code (temporary, timed, or regular) is the time zone that is initially assigned to a logical device when the logical device is assigned to a specific clearance code. It has no relevance to the day-to-day functioning of the clearance code, but valid only during the initial assignment of the logical devices to it. That's why changing the Default Time Zone changes nothing about the logical devices already assigned to the clearance code.
    - Use Elevators. Select this check box if the card will be used in operating elevators. If this checkbox is unchecked then all elevator-type logical devices will not be displayed in the Select Logical Device screen when adding a logical device to a clearance code. Note that if an elevator has already been added in the Logical Device tab, then this check box will not be enabled in the Clearance Code tab.

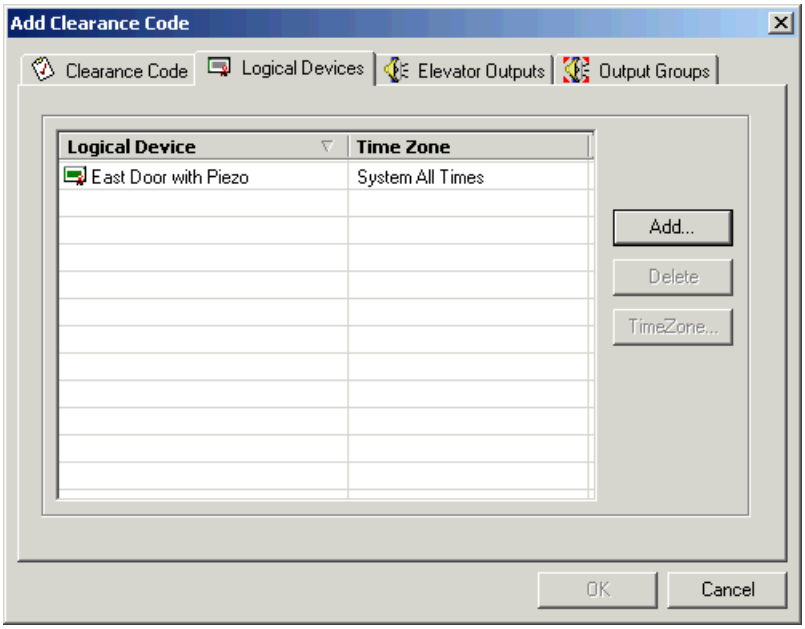
- **Use Timed Expiration**. Select the **Never Expires** option button if you want the clearance code never to expire. If you, however, want the code to expire after a specific time period, then select the **Expires In** option button to enable the related fields. Select a time unit (Days/Hours/Minutes) from the drop-down list and enter a numeric value into the first field.
- Select an **Enrollment Device** and **De-Enrollment Device** for timed clearance codes. Click the icon and select **Define** from the pop-up menu. Logical Devices dialog box displays. Select a logical device and click **OK**.
- Select Use Groups to select a group of logical devices for enrollment or de-enrollment for a timed clearance code. If "None," click the icon and select **Define** from the pop-up menu. Groups dialog box displays. Select a group and click **OK**.

  To add a new use group, click **Add** in the Add Groups dialog box. Logical Devices screen will display. Select one of the listed logical devices and click **OK**. Repeat the same for all the logical devices you want to add to the user group. Once you are done, enter a Description to identify your new user group. Click **OK**. The new use group will now be listed in the Groups screen.

  To edit or delete a use group click **Edit** or **Delete**, respectively.

  Select **Temporary Access** to grant temporary access privileges to the card and thus create a Temporary Clearance Code. Select **Start** and **End Date** and **Time** from the drop-down lists.

5. Select the **Logical Devices** tab to add or delete a logical device, or to edit the timezone for the logical device:



- To add a logical device, click **Add**. Logical Devices screen will display. Select a logical device and click **OK**. The Time Zones dialog box will display. Select a time zone and click **OK** to revert to the Logical Devices tab.
- To edit the time zone of a logical devices, select it and click **Time Zone** to display the Time Zones dialog box. Select a time zone and click OK.
- To delete a logical device, select it and click **Delete**.

Note: Select the **Elevator Outputs tab** to set an elevator output. Elevators (or more specifically, the "Floor-Only Method" of operating an elevator through Pro-Watch) are applicable to PW-5000, PW-3000, and Star II panels.
Elevator outputs will be displayed on this screen only if there are elevator-type logical devices included in the logical devices screen. Also, elevator outputs will be visible only if there is hardware assigned to it. Only the timezone associated with an elevator output or a floor can be changed in this screen.

6. Select the **Output Groups tab** (specific to PW2000 panel) to select an output group.

To add an output group:

1. Click Add to display the Clearance Code - Add Output Groups dialog box.
2. Select an output group and click **OK**.

To edit a clearance code:

1. To edit a code listed in the Current Clearance Codes Assigned to Card screen, select it and click Delete. This will not actually delete the code from the database but only from the GUI. Then select the respective folder and click **Add** to display the Clearance Codes dialog box. Then follow Step 3 (below).
2. To edit a code not listed in the Current Clearance Codes Assigned to Card screen, select a folder and then click **Add** to display the Clearance Codes dialog box.
3. To edit a code listed in the Clearance Codes dialog box, select the code and click **Edit** to display the Edit Clearance Code screen. Make the necessary edits in the respective tabs. Click **OK** to To the Clearance Codes dialog box. To re-assign the edited code back to the card, select it and click **OK**.

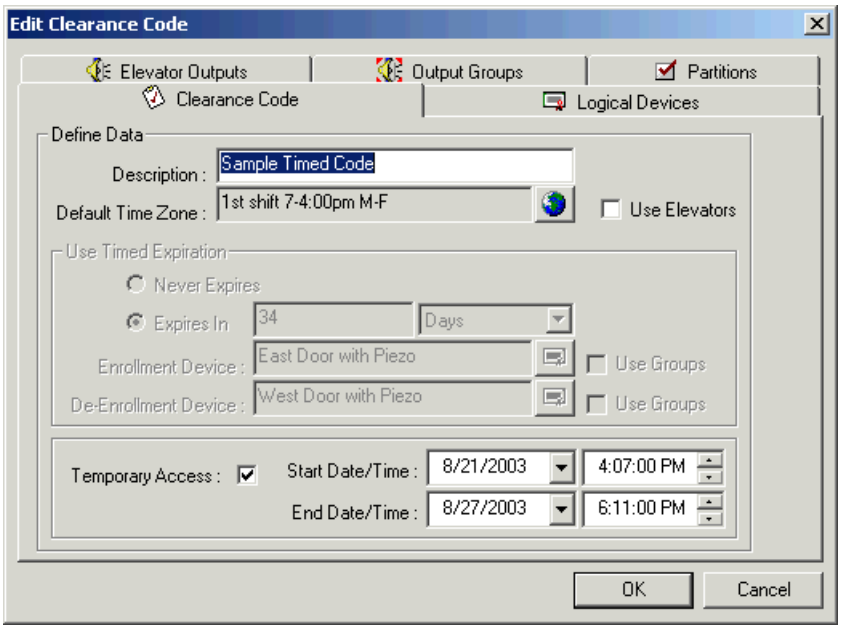
To delete a clearance code:

1. In the Clearance Codes dialog box, select the code you want to delete.
2. Click **Delete**. When prompted for verification, click **Yes**.

To add a logical device to a clearance code:

1. Select a clearance code in the Clearance Codes dialog box.
2. Click **Delete**. This will not actually delete the code from the database but only from the GUI. Click **Add** to display the Clearance Codes dialog box.

3. Select in the Clearance Codes dialog box the same code that you have deleted earlier. Click **Edit** to display Edit Clearance Code dialog box:



4. Select Logical Devices tab to view the list of devices already assigned to the code.
5. Click **Add** to display Logical Devices dialog box.
6. Select the new device you want to add and click **OK**.

G.3.1.6 Timed Clearance Codes

A timed clearance code grants a specified time access at a specified reader. It is most often used in cases where you want to force card holders to pass a checkpoint before their cards become invalid inside a facility. In this way, you can prevent people from tailgating into the facility since their cards would not operate inside.

A timed clearance code scenario involves **three readers**: swiping a card at the enrollment reader grants access to a timed reader for the time period you specify; the cardholder's access lasts until either the time period has elapsed or until the card is presented at the de-enrollment reader.

Optionally, you can specify a group of readers for enrollment and de-enrollment, and you may use any reader in the specified group(s).

The timed clearance code requires the following:

- The cardholder already must have permanent access given to the enrollment and de-enrollment readers by some other clearance code.
- The timed reader must have a clearance code with a default time zone.
- All readers must be entered as logical devices.

Timed Clearance Codes work just like Temporary Clearance Codes, except that they are activated by a valid card presentation (swipe) at the enrollment Logical Device, and are de-activated by a valid card swipe at a de-enrollment Logical Device (or by a certain amount of time elapsing).

The cardholder must already have valid access to a Timed Clearance Code's enrollment reader in order to activate the Timed Clearance Code. This means access to the enrollment reader must have already been granted to the cardholder, via a “permanent” (regular) Clearance Code or an already-active Timed or Temporary Clearance Code, at the time of the card swipe at the enrollment reader.

A common mistake some users make is that they include a Timed Clearance Code's enrollment reader in the Timed Clearance Code's own access list. Unless the cardholder has access to the reader by some other clearance code, the Timed Clearance Code will not activate.

G.3.1.7 Temporary Clearance Codes

These are clearance codes that are valid for only a specified time period and do not require setting of Enrollment and De-Enrollment devices. The temporary time period is set by selecting the **Temporary Access** check box and selecting the **Start** and **End dates and times** in the same Add Clearance Code dialog box used to assign a clearance code to a card.

Temporary clearance codes will not work for a cardholder before the start date-time nor after the end date-time. However, between those date-times, a cardholder's access depends on the timezones assigned to the Logical Devices (for example, doors) in the Clearance Codes.

Example: A temporary clearance code grants 9-5, Mon-Fri access to the front door. The temporary clearance code on the card starts at Tuesday at noon, and ends Friday at noon. The user is not able to use the front door before noon on Tuesday, nor after noon on Friday. But between those two distinct points in time, the user can open the door only between 9-5 hours.

Note: Outside the temporary access, if the user has another way (by another permanent or timed clearance) to get through the door before noon on Tuesday and after noon on Friday, then the user will be able to gain access.

G.3.1.8 Precedence Rules

If multiple types of clearance codes give access to the same doors but different time zones, here are the precedence rules:

First of all, if the Temporary or Timed Clearance Codes are not active, it is as if they don't exist; access is determined by the “permanent” Clearance Codes.

Next, assuming timed and temporary clearance codes are active, the precedence rule is as follows (highest priority first):

- Individual Logical Device Grants and Revokes (from the Logical Device tab on the keycard screen),
- Temporary Clearance Codes, Timed Clearance Codes,

- Permanent (regular) Clearance Codes.

G.3.1.9 Logical Devices Tab

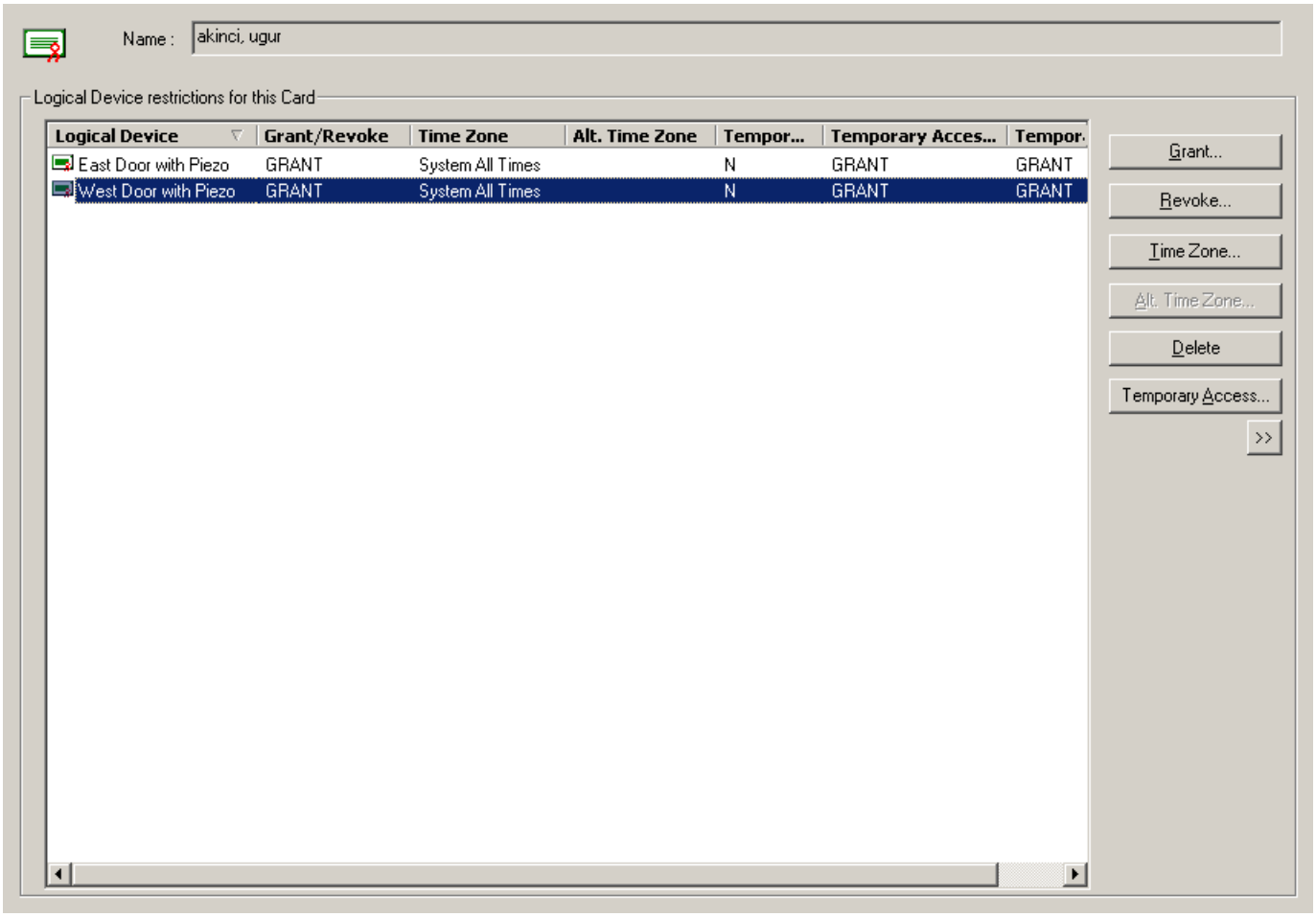
This tab allows users to grant and revoke access to logical devices for a card.

However, it cannot grant or revoke access for:

- Elevator (both floor select and non-floor select) doors.
- Doors on Star I or Star II panels.

All logical devices for the card display in an edit window, and may be deleted by highlighting the logical device name, and clicking Delete.

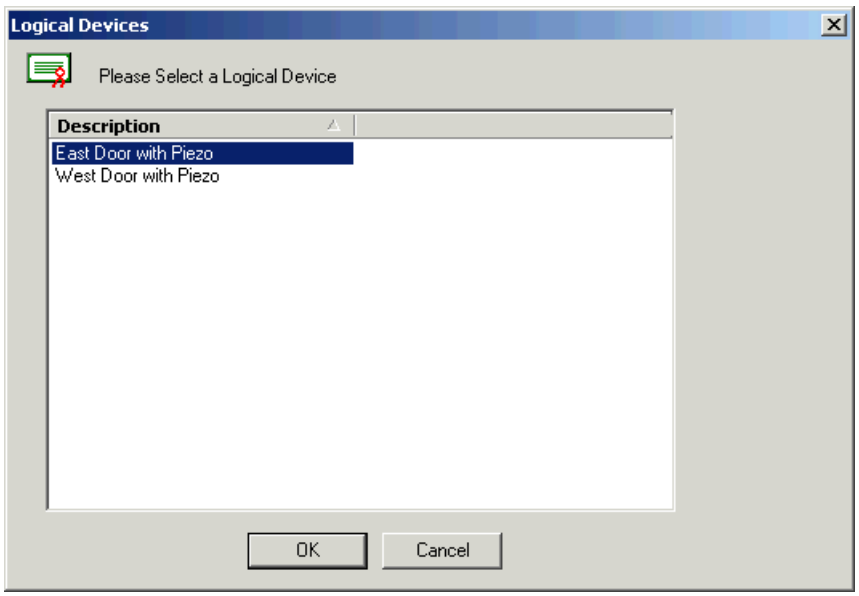
Deleting a logical device from a card removes that card from the access exceptions for that card. The access rights for that logical device will now be set back to the access (if any) set in the Clearance Codes assigned to that card.



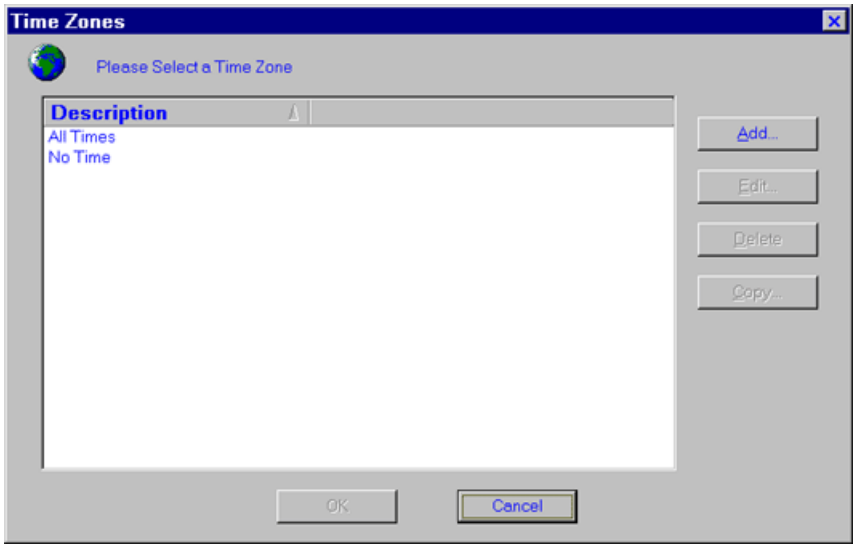
To grant card access to a logical device:

Note: The Pro-Watch records database changes associated with clearance code assignment to a company, clearance code assignment to a card, **logical device assignment to a card**, and company assignment to a card in order to comply with Title 21 of the Code of Federal Regulations, Part 11 (21 CFR 11), and for compliance tracking. The compliance tracking requirements use the aggregated logical devices's most restrictive settings.

1. Click **Grant**. The Logical Devices dialog box appears:



2. Select a logical device description.
3. Click **OK** to display the Time Zones dialog box. Select a time zone and then click **OK** to grant access to the logical device selected.



To revoke card access:

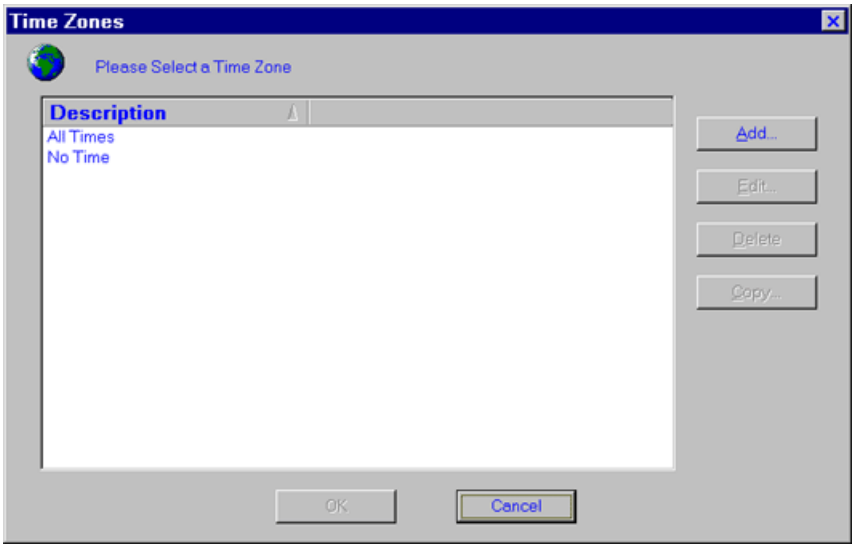
1. Click **Revoke**. The Logical Devices dialog box appears.
2. Select a logical device description.
3. Click **OK.**

Notes:

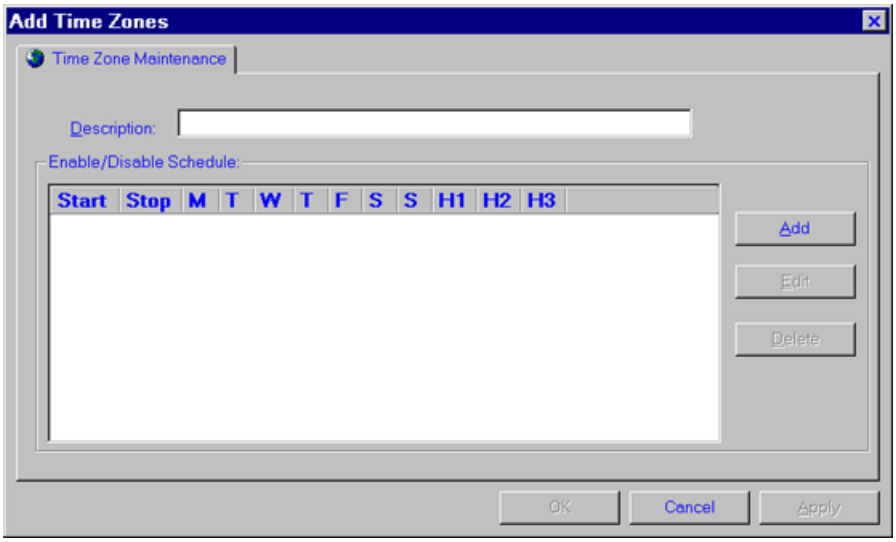
- Revoking a logical device set with a temporary access will only revoke that logical device during the set temporary access time. If there is a clearance code set to system all times for the same logical device, the card will have access after the temporary access time for the revoke expires.
- Temporary Clearance Code takes precedence. For example, if you have a clearance code set to system no times for a logical device as well as a temporary clearance code for the same door, access will be granted during the temporary access time.

To add a new time zone:

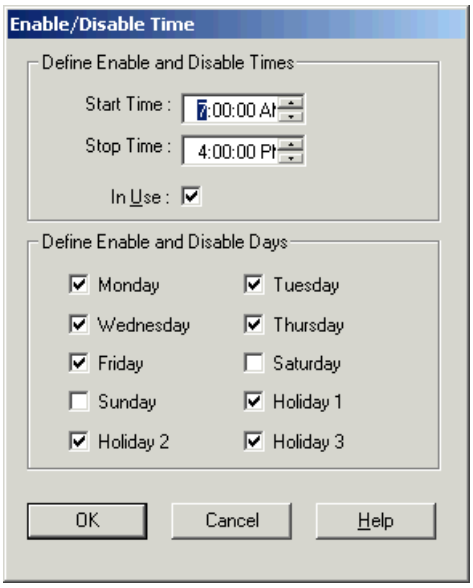
1. Click the **Time Zone**. Time Zones dialog box appears:



2. Click **Add** to display the Add Time Zones dialog box:



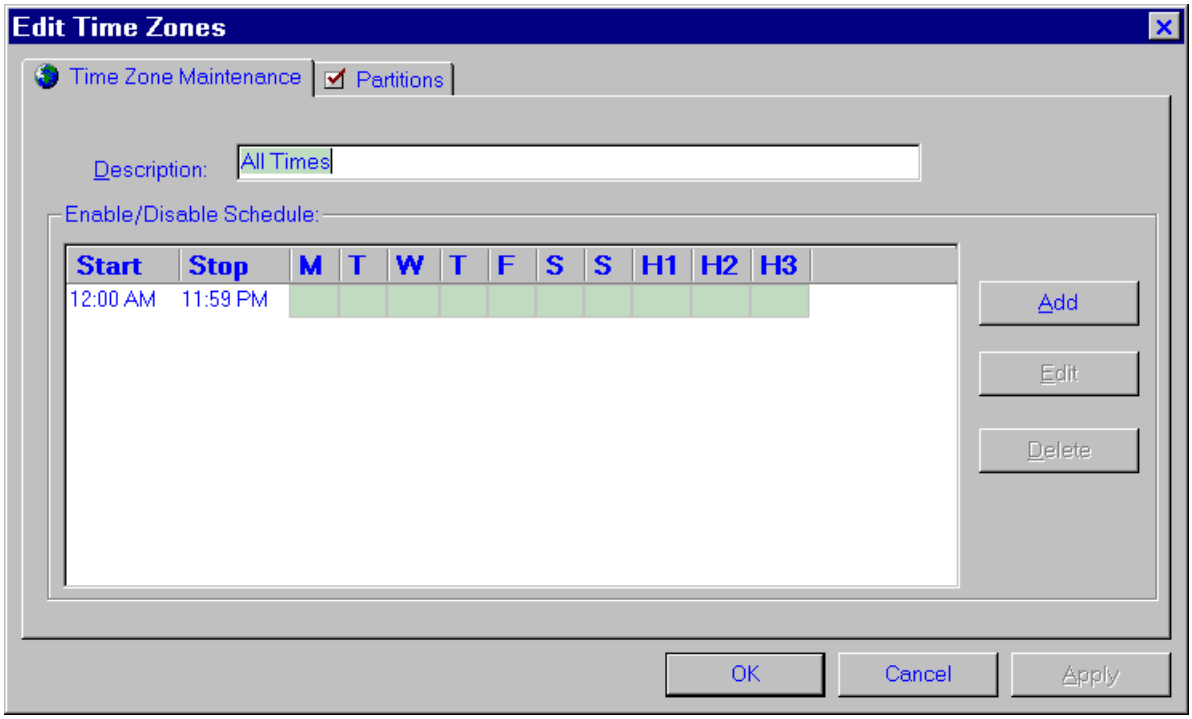
3. Enter a Description and then click **Add** to display the Enable/Disable Time dialog box:



4. Select the desired values and then click **OK** to display the Add Time Zones screen.
5. Select the newly created time zone and click **OK** to have it added to the Time Zones list.

To edit an existing time zone:

1. Click the **Time Zone**. Time Zones dialog box will display.
2. Select a time zone and then click **Edit** to display the Edit Time Zones dialog box:



3. Select a time zone listed in the Enable/Disable Schedule and then click **Edit**. Enable/Disable Time dialog box will display.
4. Make the necessary edits and then click **OK** to revert to the Logical Devices tab. Note that the logical device time zone must match the temporary access time zone in order to gain access. For example, if you set the temporary access time zone from 9-to-5, and the logical device time zone is set from 6-to-10, you will not gain access. If your logical device time zone is set to system all times, then you will gain access only during the time determined by the temporary access time zone.

To delete an existing time zone:

1. Click **Time Zone**. Time Zones dialog box will display.
2. Select the time zone you want to delete and then click **Delete**.

To grant temporary access:

1. Select the logical device from the list and click **Temporary Access**. Temporary Access dialog box displays.

2. Select the **Temporary Access** check box.
3. Set the proper Start and End access days and hours.
4. Click **OK**.

G.3.1.10 Alternative Time Zone

When you have multiple readers assigned to the same logical device you can assign an alternative time zone to one or more of the readers.

For example, if there are two readers controlling two doors in a room, you may want to let people in through Door 1 only between 9-11 a.m. hours but allow them to leave the room from Door 2 any time they want. You can accomplish this by assigning “9-11 a.m.” time zone to Door 1 and “System All Times” alternative time zone to Door 2.

To assign an alternative time zone:

1. Select a **reader** from the list in the Logical Devices tab.
2. Click the **Alt. Time Zone button** and follow the instructions for assigning an alternative time zone (see "To add a new time zone:") to the selected reader.

G.3.1.11 Transactions Tab

This tab displays a report of every event for this card, listing the description, event date, event description, location, channel description, panel description, last access and PIN code for each event. Click the **printer** icon to print the list of transactions.

G.3.1.12 Timed Points Tab

This tab lists the Logical Devices that are also specified in the Disarm Logical Device/Arm Logical Device fields of the Optional Information tab (see "Optional Information Tab"). The monitorable inputs of the specified Logical Devices are masked or unmasked upon granted access for a timed period of 180 minutes.

Note: This tab is enabled only when the Timed Points feature is selected in the Optional Information tab.

To add a Logical Device:

1. Click **Add** to display the Logical Input Selection dialog box.
2. Select a description for the logical device. Click the icon and select **Define** from the pop-up menu. The Logical Devices dialog box appears.
3. Select a logical device from the list and click **OK**.
4. Select a device from the list and click **OK** to revert to the Timed Points tab.

G.3.1.13 Pathways Tab

Pathways allow a badge holder to follow a clear path through a building without setting off alarms. This tab displays a report listing the name and description of each pathway taken for the card.

Note: This monitoring is activated only when the Start Pathways feature is selected in the Optional Information tab (see "Optional Information Tab").

G.3.2 Exiting out of Card View Screen

When you finish adding or editing a card you can exit the card view section and return to the main badging window by clicking the exit button  on the card editing tool bar.

G.3.3 Downloading a Card

After you create a card, you have to download the information to its respective panel in order to grant access to card users. You can download a card by clicking the “lightning button”  on the tool bar of the badging screen.

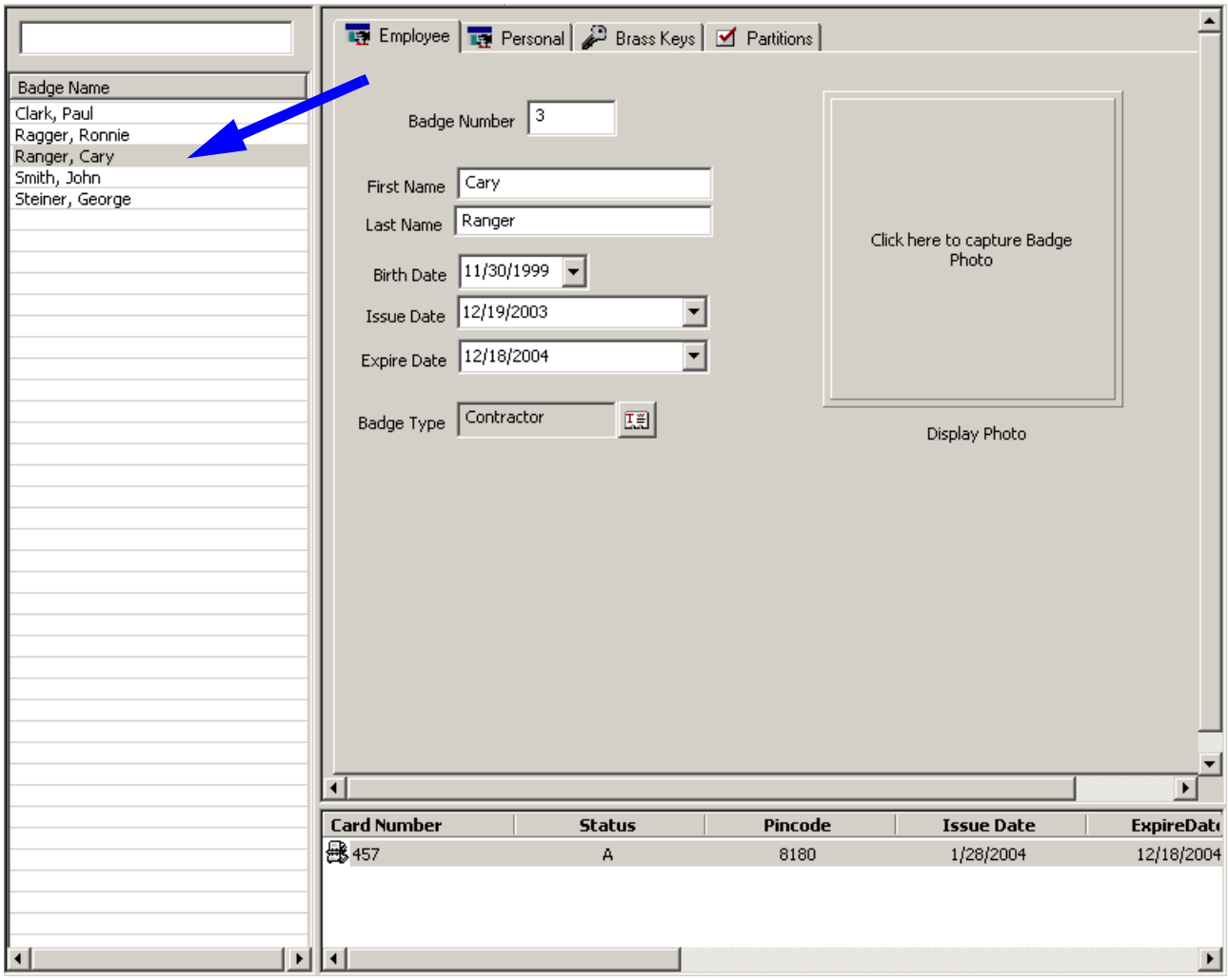
G.3.4 Copying and Pasting a Card

Copying and pasting a single card can be a fast method of either creating the same card for another employee or creating a new card that will have a similar configuration.

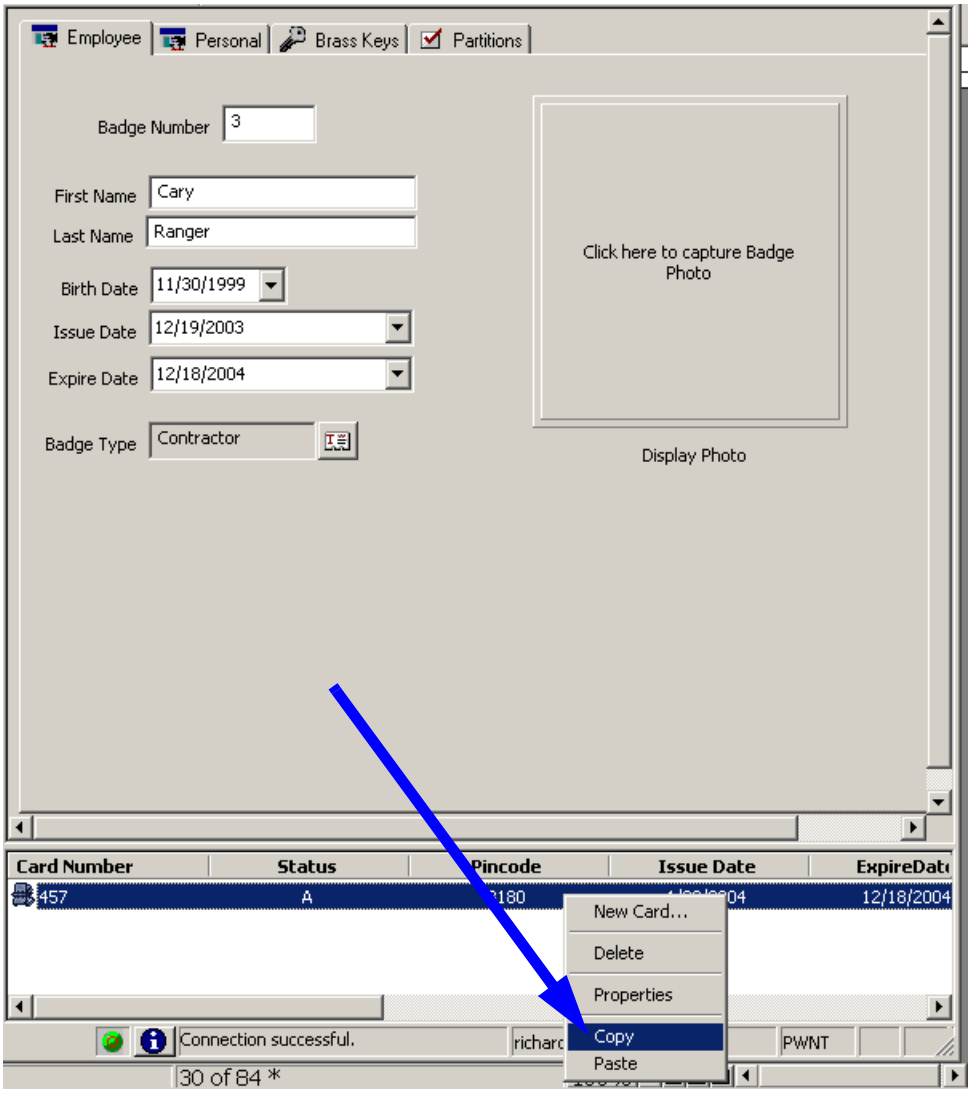
Note: The Copy function is enabled only when a single card is selected.

To copy and paste a card:

1. From the list of badgeholders in the main Badging screen, click to select the badgeholder whose card you want to copy.


Badge Name
Clark, Paul
Ragger, Ronnie
Ranger, Cary
Smith, John
Steiner, George
Employee
Personal
Brass Keys
Partitions
Badge Number
3
First Name
Cary
Last Name
Ranger
Birth Date
11/30/1999
Issue Date
12/19/2003
Expire Date
12/18/2004
Badge Type
Contractor
Click here to capture Badge Photo
Display Photo
Card Number
Status
Pincode
Issue Date
ExpireDat
457
A
8180
1/28/2004
12/18/2004

2. Right-click the card from the card list at the bottom of the Employee tab to display a pop-up menu.



3. Select **Copy**.
4. Right click in the card view section of the badgeholder for whom you want to create the copy of the card. A pop-up menu appears.
5. Select **Paste** to paste the copy of the card.

Note: On the Card Information tab, enter new values in the Card Number, Last Access, and Last Reader fields. The card number must be unique. When you save the pasted card, Pro-Watch determines whether the card number is unique. If you try to exit without saving the pasted card, Pro-Watch will prompt you to save it first.
If you have configured the Pro-Watch to assign automatically incremented

card numbers, the pasted card will automatically be assigned the incremented value. See "Card Information Tab".

6. Review and edit any of the information that was automatically populated from the original card. All the fields in the Panel Specific, Optional Information, Clearance Codes, Logical Devices, Timed Points, and Pathways tabs of the copied card will be included in the newly pasted card. See "Adding or Editing a Card".

G.3.5 Deleting a Card

1. Select a badge holder name from the left pane of the Badging window.
2. In the list at the bottom of the right pane, right-click the card assigned to the badge.
3. Select **Delete**.
4. Follow the on-screen directions. Click **Yes**.

G.3.6 Voiding a Card

Note: You can void a card even if the Badging module is not open.

1. Select a badge holder name from the left pane of the Badging window.
2. In the list at the bottom of the right pane, select the card assigned to the badge.
3. Select **File > Void Card** from the menu bar to display the Void Card dialog box.
4. Search for the card to void or select one of the cards listed in the dialog box.
5. Click **Void Card**. Then, click **OK**.

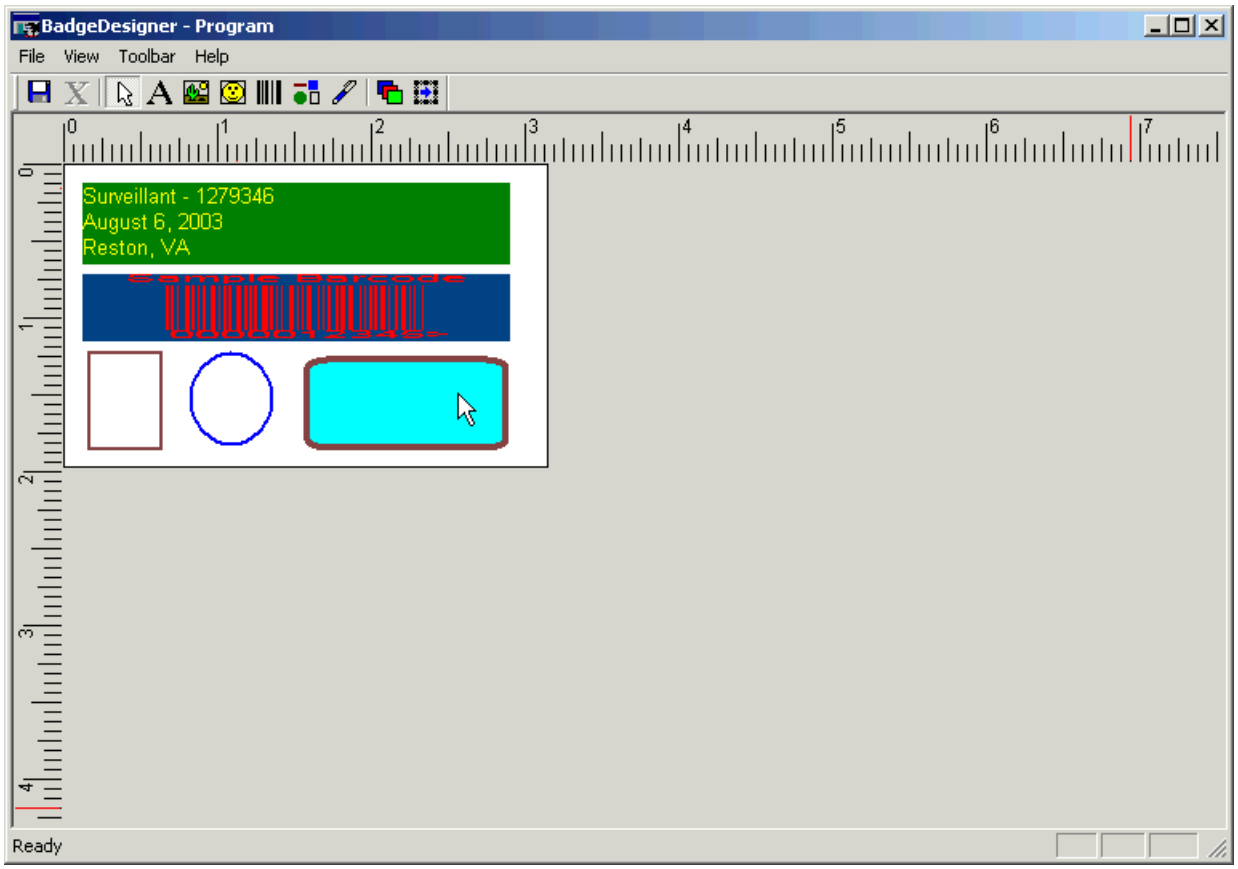
G.4 Badge Designer

Use the Badge Designer to create or edit the front and back sides of a badge. You can create different badge designs, in addition to the “Contractor” or “Standard Employee” badge designs that come configured with Pro-Watch.

Note: If you never intend to capture a badge holder photograph or print a badge, then you will not need to create a badge layout.

Select either **Edit > Badge Layout > Front**, or **Edit > Badge Layout > Back** from the menu bar. The Badge Designer - Program layout window appears:

Figure G-2 Badge Designer Screen



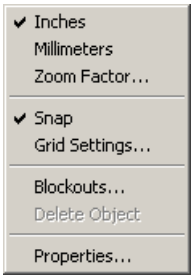
The Badge Designer interface consists of an active layout design sheet, a badge format properties menu, a menu bar and a tool bar.

G.4.1 Badge Format Properties

The badge format properties include:

- Measurement units.
- Zoom factor.
- Snap and grid settings.
- Blockouts.
- Image placement.
- Magnetic stripe encoding.

1. Right-click in the layout design sheet space to display the properties menu:



2. Use the following property descriptions to select the appropriate property dialog:

Property	Description
Inches	Sets layout design sheet unit of measurement to inches. See "Using Inches or Millimeters".
Millimeters	Sets layout design sheet unit of measurement to millimeters. See "Using Inches or Millimeters".
Zoom Factor	Sets the percentage by which the badge image is enlarged or reduced. See "Setting the Zoom Factor".
Snap	Aligns a selected badge object to a grid. See "Setting Snap and Grid Properties".
Grid Settings	Defines the density of the badge design grid, by which you can align selected badge objects. See "Setting Snap and Grid Properties".
Blockouts	Defines a badge area which cannot be printed upon. See "Adding Blockouts".
Delete object	Deletes the selected object on the badge.
Properties	Edits badge, color, positioning and track object properties.

Complete the steps in the following tabs to set the properties.

G.4.1.1 Using Inches or Millimeters

Use this function to define the unit of measurement for the Badge Designer ruler.

To set inches or millimeters as unit of measurement:

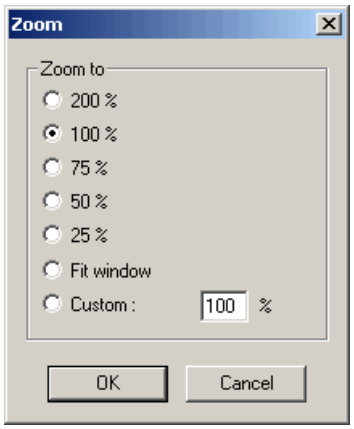
1. Right-click the specific Badge Designer item.
2. Click **Inches** or **Millimeters**.

G.4.1.2 Setting the Zoom Factor

Use this function to enlarge or reduce the object's size on the badge.

To set the zoom factor:

1. Right-click the specific Badge Designer item and then click **Zoom Factor** to display the Zoom dialog box:



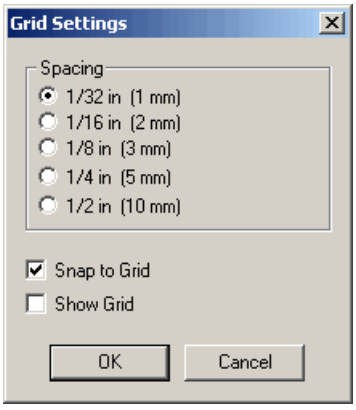
2. Select the zoom percentage that will correctly magnify or shrink the selected Badge Designer item.
3. Click **OK**.

G.4.1.3 Setting Snap and Grid Properties

Use this function to display a grid on any badge design, determine the grid density, and align badge objects on the grid. This makes it easy to align objects such as photographs and signatures.

To set the snap and grid properties:

1. Right-click anywhere in the Badge Designer and select **Grid Settings** to display the Grid Setting dialog box:



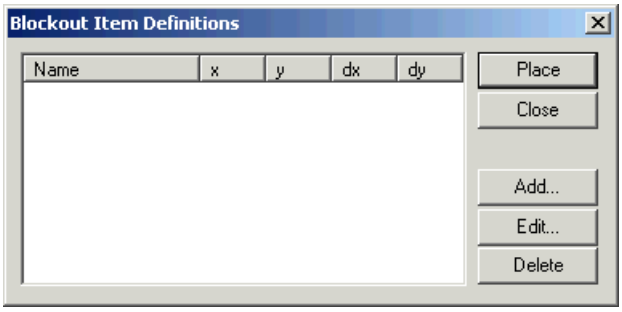
2. In the Spacing section of the dialog, select the grid density. Be sure the dialog box displays the percentages in the unit of measurement (inches or millimeters) you want. See "Using Inches or Millimeters".
3. Click **Snap to Grid** if you want to align the object to the grid. Optionally, click the Badge Designer item, and then click **Snap**.
4. Click **Show Grid** to display the grid in the Badge Designer.
5. Click **OK**.

G.4.1.4 Adding Blockouts

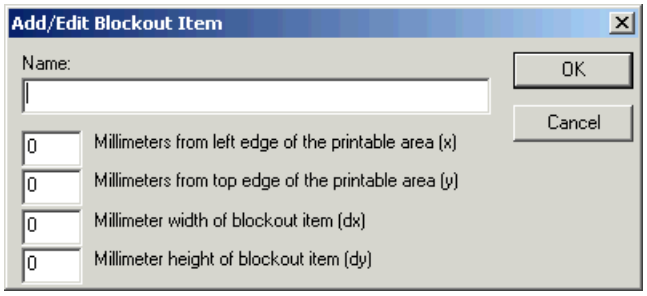
Use this function to block out an area on the card so that it cannot be printed on by mistake. For example, you may want to prevent printing on the area where the magnetic stripe or holographic picture will be. A blockout area will not print or preview on the badge layout.

Adding and Editing Blockouts

1. To *create* a new blockout area, right-click anywhere in the Badge Designer and select **Blockouts**.The Blockout Item Definitions dialog box appears. To *modify* an existing blockout area, select **Edit > Blockouts** from the menu bar. The same Blockout Item Definitions dialog box appears:



2. If you are creating a new blockout, click **Add** to open the Add/Edit Blockout Item dialog box. If you are editing an existing blockout, click the blockout you want to edit and then click **Edit** to display the Add/Edit Blockout Item dialog box:



3. Enter the name of the blockout in the Name box.

4. Enter the distance from the blockout area to the left edge of the printable area.
5. Enter the distance from the blockout area to the top edge of the printable area.
6. Enter the width of blockout area.
7. Enter the height of the blockout area.
8. Click **OK** to save your settings and To the Blockout Item Definitions dialog.
9. Select the blockout you just defined, and click **Place**.

Deleting Blockouts

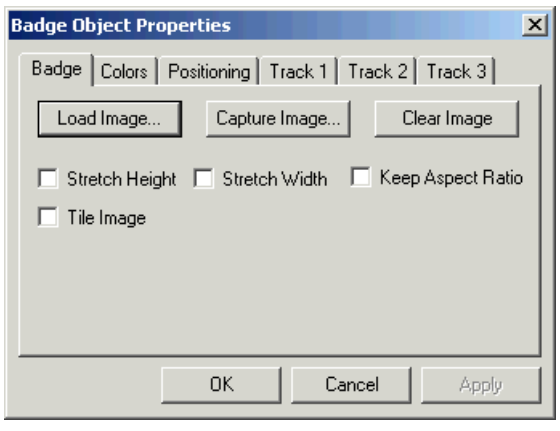
1. Right-click the blockout you want to remove from the Badge Designer.
2. Click Blockouts.
3. From the Blockout Item Definitions dialog, select the blockout you want to remove and click **Delete**.
4. Click **Yes** at the prompt.
5. Click **Close**.

G.4.1.5 Setting Image and Magnetic Stripe Properties

Use this function to capture, load, color, and position images on the badge. Also, you can encode the magnetic stripe.

To set the image and magnetic stripe properties:

1. Right-click in the design layout sheet and select **Properties**. The Badge Object Properties dialog box appears:



2. Complete the following tabs to set the image or magnetic stripe properties.

Badge Tab

This tab creates, loads, and fits an image on the badge. Use the following field definitions to complete the tab:

Field	Description
Load Image	Places the image you specify onto the badge.
Capture Image	Creates a digital photograph.
Clear Image	Deletes the image from the database.
Stretch Height	Extends the top border of the image to the top of the frame.
Stretch Width	Extends the side border of the image to the side of the frame.
Keep Aspect Ratio	Maintains the object placement on the badge as the badge adjusts in size.
Tile Image	Repeats the image in adjacent tiles until the picture area is filled.

Colors Tab

This function sets the background color of the badge. Click the browse button next to the Background Color field and select the color you want. Click **OK** to To the Colors tab. Then, click **Apply** to set the background color to the badge.

Positioning Tab

This function positions the image on the badge. Use the following field definitions to position the image:

Field	Description
Horizontal Position	Right-justifies, left-justifies, or centers the image on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").

Field	Description
Vertical position	Top-justifies, bottom-justifies, or centers the image on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Orientation	Rotates the image on the badge in multiples of ninety degrees.
Top	The distance in inches or millimeters from the top of the design screen. You can enter a value but this field is not applicable. It does not affect how the card will look when it is printed. Leave it blank.
Height	Sets the height of the badge in inches or millimeters.
Left	The distance in inches or millimeters from the left of the design screen. You can enter a value but this field is not applicable. It does not effect how the card will look when it is printed. Leave it blank.
Width	Sets the width of the badge in inches or millimeters.

Track 1, 2, and 3 Tabs

Select a **status** from the drop-down menu:

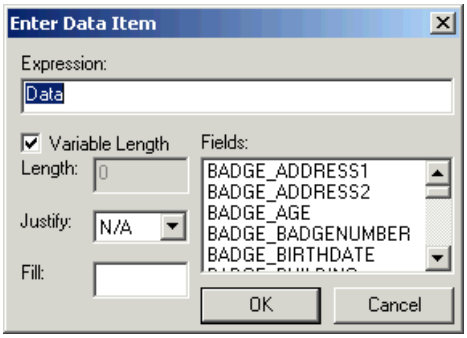
- Disabled means the track is disabled.
- IATA stands for the International Air Transport Association standards.
- ABA stands for American Bankers Association standards.
- TTS stands for Think Tank Session standards.

These tabs are used to encode the card's magnetic stripe. The magnetic stripe consists of three tracks, each represented by a separate tab. Each track is defined by the field's type, expression, length, justification, and fill.

Note: The magnetic stripe encoding information should be placed only on the front badge layout. The magnetic stripe will not work if it is placed on the back of the card.

The information that should be entered into these tabs, such as which data fields to include on what tab and in what order, is determined by the specific configuration of the magnetic stripe reader hardware that will be used with the cards. Therefore please make sure you understand the requirements of the magnetic stripe reader hardware that will be used with the Pro-Watch system before you enter any information into these tabs.

1. Click **Add** to display the Enter Data Item dialog box:

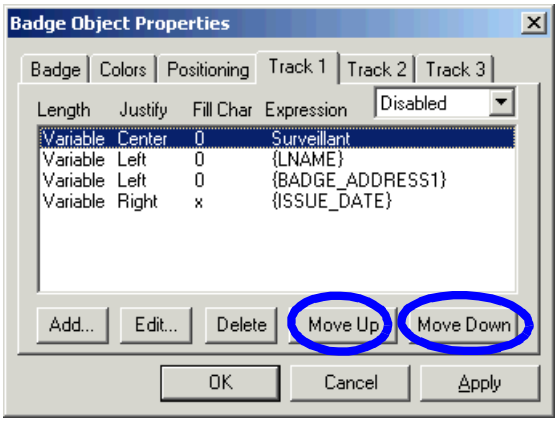


2. Enter a value in the Expression field either by double-clicking on a variable name listed in the Fields list box or by manually typing it into the text field provided. The variables listed in the Fields list box are populated from either a default database or from the values entered in the badging screen while creating a badge.
3. Set the field's length by doing one of the following:
   - If the variable has a fixed length, then enter a number into the **Length** field. Fixed length variables are strings of fixed length, made up of any printable alphanumeric characters. For example, "1234" has a fixed length of four digits. The variable "a98wwBB33" has a fixed length of nine digits.
   - If the variable has a variable length select the **Variable Length** check box. The Length field will be disabled. Variable length variables are strings of variable length, made up of any printable alphanumeric characters.

Note: From the Justify drop-down list, select the **field's justification** (N/A, left, center, or right).
Left-justified strings align on a field's left edge. Right-justified strings align on a field's right edge. Center-justified strings are centered in the field.

4. Go to the **Fill box** and enter the fill characters if the fixed Length setting exceeds the length of the magnetic stripe data. For example: your data would be 0000012345 if your fixed data length is 10, your data to code is 12345, and your Fill is set at 0.
5. Click **OK** to accept the encoding for this track. Repeat the procedure for the other two tracks, if necessary.
6. In the Track tabs of the Badge Object Properties dialog box you can configure the order in which the entered variables will be displayed by

clicking the **Move Up** and **Move Down** buttons.

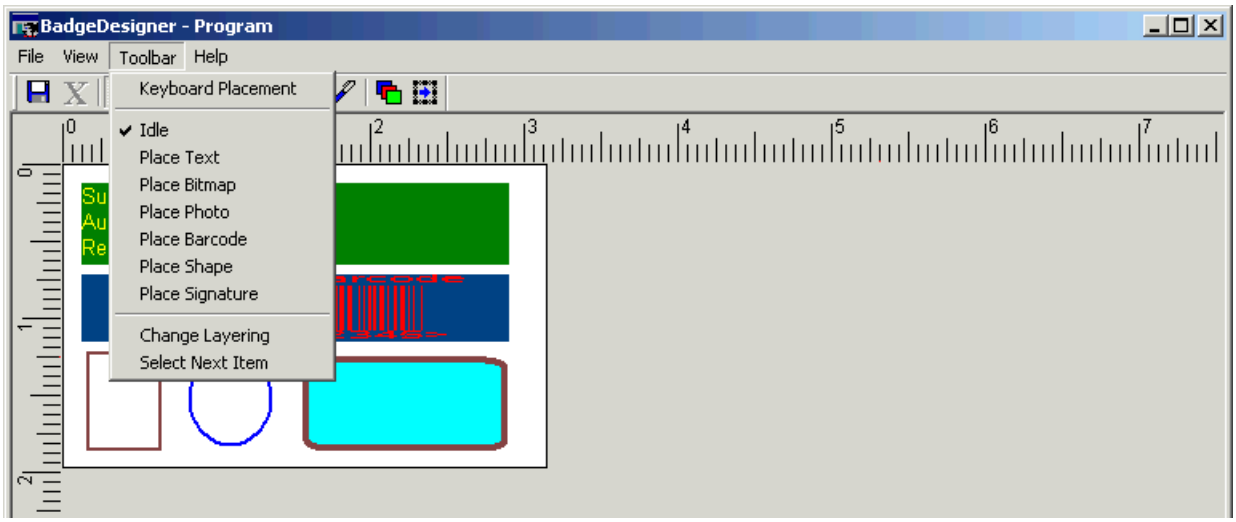


As a rule, the variable displayed on top of the grid is read first on a magnetic stripe, and it is followed by the other variables in descending order. The last variable displayed at the bottom of the grid is read last on a magnetic stripe. This is the reason the exact order in which the track variables should be displayed in the grid depends on the way the card reader hardware is configured to read such variables.

G.4.2 Badge Designer Tool Bar

You can place several types of Badge Designer objects onto the layout design sheet in one of the following three ways:

- You can click the Badge Designer **Toolbar** menu item to display the following drop-down menu list:



- You can click the appropriate icon from the Badge Designer tool bar:



Use the following table to identify the tool bar buttons, or rest the cursor over the button to display the button's description.

Button	Description
Save	Saves Badge Designer settings.
Exit	Exits from Badge Designer.
Idle	Selects one or more Badge Designer items.
Place Text	Inserts text into Badge Designer.
Place Bitmap	Inserts bitmap image into Badge Designer.
Place Photo	Inserts photograph into Badge Designer.
Place Barcode	Inserts barcode into Badge Designer.
Place Shape	Places shape into Badge Designer layout. The system places a rectangle by default until it is modified.
Place Signature	Places a signature into the Badge Designer layout.
Change Layering	Opens the Badge Item Layering dialog. You use this dialog box to properly layer the items within a selected layout.
Select Next Item	Selects the next Badge Designer item Badge Designer layout.

You can also place the badge fields on the badge design screen by using your keyboard only, without touching the mouse. Select the **Toolbar > Keyboard Placement** menu option to enable this function.

G.4.2.1 Placing Text

1. Either select **Toolbar > Place Text** from the menu bar or click the **Place Text** icon on the tool bar.

2. Click and drag the cursor on the layout design sheet to define the size you want for the text block.
3. Right-click the text area and select **Properties**. The Badge Text Object Properties dialog box appears.

Complete the following tabs to finish placing the text on the badge.

Text Block Tab

1. In the **Text** box, enter the text you want in the selected area.
2. In the **Fields** box, select the field type that is appropriate for the text entry.
3. Click **Font** to select the font properties for the text
4. If you want the text block to be sized to fit the text area you created, select **Size font to box** check box.

Colors Tab

1. Click the browse button next to the **Foreground Color** field to display the foreground color options.
2. Click the color you want for the foreground, and click **OK**.
3. Click the browse button next to the **Background Color** field to display the background color options.
4. Click the color you want for the background, and click **OK**. If the badge's background is to be transparent, click the **Transparent Background** box.

Positioning Tab

This function positions the text on the badge. Use the following field definitions to position the image:

Field	Description
Horizontal Position	Right-justifies, left-justifies, or centers the text on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Vertical position	Top-justifies, bottom-justifies, or centers the text on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Orientation	Rotates the text on the badge by multiples of ninety degrees.

Field	Description
Top	Sets the text distance from the top of the badge in inches or millimeters.
Height	Sets the text height in inches or millimeters.
Left	Sets the text distance from the left border of the badge in inches or millimeters.
Width	Sets the text width in inches or millimeters.

Conditional Display Value Tab

This tab enables you to display or hide a badge object depending on the conditions you define in the Field and Value fields.

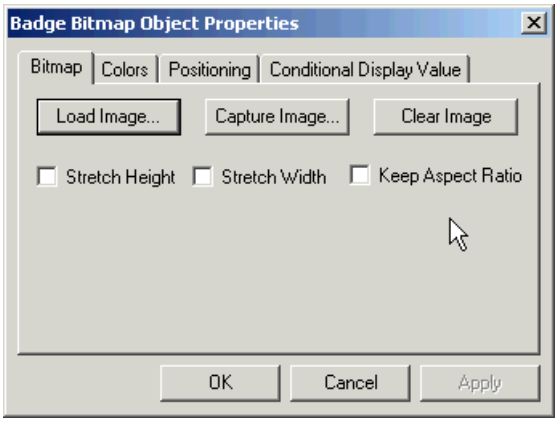
1. Select a display condition from the Field drop-down list. For example, you may select BADGE_CITY.
2. Enter a corresponding value into the Value field. For example, you may enter Baltimore. Note that if the Field is a Boolean field, then the acceptable values are “TRUE” and “FALSE.”

In this example, the specific badge object will be displayed only if the “Badge City” variable has a value of “Baltimore.” For all other cities, the badge object will not be displayed.

G.4.2.2 Placing a Bitmap

Note: Background badge images must not exceed 300-350KB. Images larger than this cannot be saved when you save the badge design. If you try to save the larger image when you close the badge design, the image will not appear when you open the design.

1. Either select **Toolbar > Place Bitmap** from the menu bar or click the **Place Bitmap** icon on the tool bar.
2. Click and drag on the layout design sheet to define the size you want for the bitmap block.
3. Right-click the bitmap area and select **Properties**. The Badge Bitmap Object Properties dialog box appears:



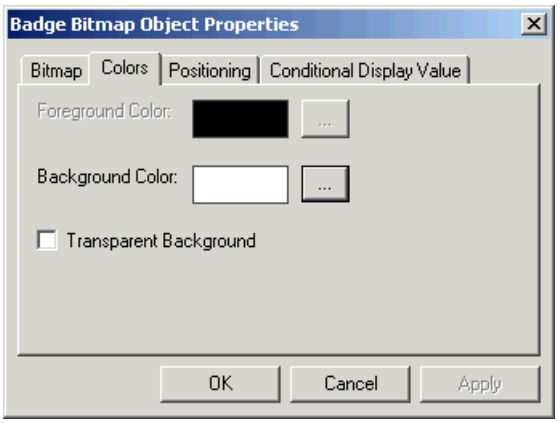
4. Complete the following tabs to finish placing the text on the badge.

Bitmap Tab

1. Click **Load Image** to place an existing bitmap that you locate from a Windows Open dialog.
2. Select **Capture Image** to all or part of an on-screen image and convert it to a graphics file format for insertion onto the selected badge layout. To do this, you will need to select from the displayed dialog box the .dll file that supports the image capture software you are using. For example, if you are using Flashpoint software, select the flashpoint.dll file.
3. Select **Clear Image** to remove an image.
4. Select **Stretch Width** to automatically stretch the width of the photograph to fill the display box on the badge.
5. Click **Stretch Height** to automatically stretch the height of the photograph to fill the display box on the badge.
6. When changing the size of a graphic, select **Keep Aspect Ratio** to keep the ratio of the width of an image to its height. This avoids image distortions. From here you can access other bitmap properties by clicking the appropriate tab, or you can click **Apply** to assign the settings to the selected bitmap.
7. Click **OK** to save the settings and close the dialog.

Color Tab

1. Go to **Background Color** box and select the associated browse button:



2. Click a basic color from the Color dialog or click **Define Custom Colors** to create a more desirable color.
3. Click **OK** to assign the color. From here you can access other bitmap properties by clicking the correct tab, or you can click **Apply** to assign the settings to the selected bitmap.
4. Click **OK** to save the settings and close the dialog box.

Positioning Tab

This function positions the bitmap on the badge. Use the following field definitions to position the bitmap:

Field	Description
Horizontal Position	Right-justifies, left-justifies, or centers the bitmap on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Vertical position	Top-justifies, bottom-justifies, or centers the bitmap on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Orientation	Rotates the bitmap on the badge by a specified number of degrees.
Top	Sets the bitmap distance from the top of the badge in inches or millimeters.

Field	Description
Height	Sets the bitmap height in inches or millimeters.
Left	Sets the bitmap distance from the left border of the badge in inches or millimeters.
Width	Sets the bitmap width in inches or millimeters.

Conditional Display Value Tab

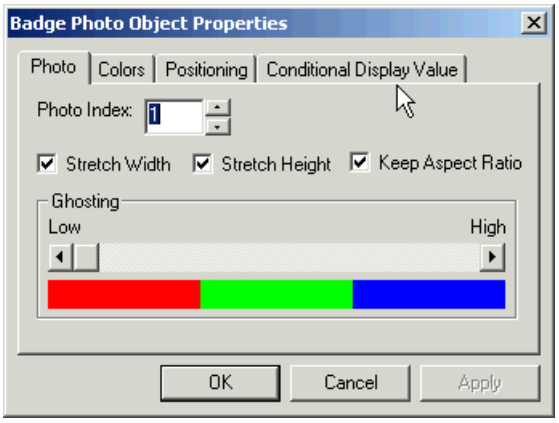
This tab enables you to display or hide a badge object depending on the conditions you define in the Field and Value fields.

1. Select a display condition from the Field drop-down list. For example, BADGE_CITY is a valid entry.
2. Enter a corresponding value into the Value field. For example, Baltimore is a valid entry. Note that if the Field is a Boolean field, then the acceptable values are “TRUE” and “FALSE.”

In this example, the specific badge object will be displayed only if the “Badge City” variable has a value of “Baltimore.” For all other cities, the badge object will NOT be displayed.

G.4.2.3 Placing a Photo

1. Either select **Toolbar > Place Photo** from the menu bar or click the **Place Photo** icon on the tool bar.
2. Click and drag on the layout design sheet to define the size you want for the photo.
3. Right-click the photo area and select **Properties**. The Badge Photo Object Properties dialog box appears:



4. Complete the following tabs to finish placing the bitmap on the badge.

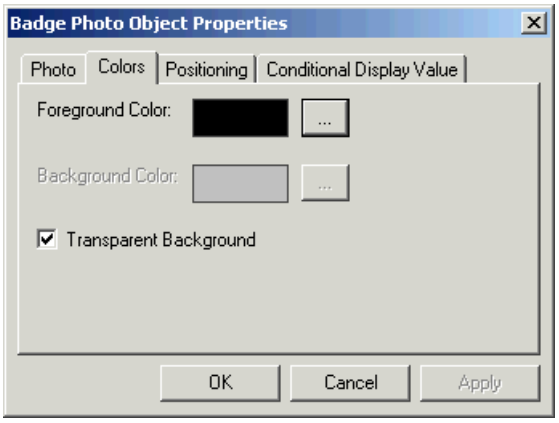
Photo Tab

1. Go to the **Photo Index** and enter a value between 1 and 99. This value corresponds to the index setting of the photograph BLOB type. If the badge holder has more than one photograph associated with his or her record, this value determines which photograph will print on the badge.
2. Select **Stretch Width** to automatically stretch the width of the photograph to fill the display box on the badge.
3. Click **Stretch Height** to automatically stretch the height of the photograph to fill the display box on the badge.
4. When changing the size of a graphic, select **Keep Aspect Ratio** to keep the ratio of the width of an image to its height; thus, avoiding distortions.
5. Locate the **Ghosting** section of the dialog and move the scroll bar indicator to the desired effect. Ghosting is the degree of transparency of the image. The higher the setting, the greater you can see through the image.

   From here you can access other photograph properties by clicking the correct tab or you can click **Apply** to assign the settings.
6. Click **OK** to save the settings and close the dialog.

Color Tab

1. Go to **Foreground Color** box and select the associated browse button:



2. Click a basic color from the Color dialog or click **Define Custom Colors** to create a more desirable color.
3. Click **OK** to assign the color.
4. Locate the **Background Color** box and follow the same instructions listed above. From here you can access other barcode properties by clicking the correct tab, or click **Apply** to assign the settings to the

selected photograph. Note that the Background Color box will be disabled if you select a **Transparent Background**.

5. Click **OK** to save the settings and close the dialog box.

Positioning Tab

This function positions the photo on the badge. Use the following field definitions to position the image:

Field	Description
Horizontal Position	Right-justifies, left-justifies, or centers the photo on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Vertical position	Top-justifies, bottom-justifies, or centers the photo on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Orientation	Rotates the photo on the badge by a specified number of degrees.
Top	Sets the photo distance from the top of the badge in inches or millimeters.
Height	Sets the photo height in inches or millimeters.
Left	Sets the photo distance from the left border of the badge in inches or millimeters.
Width	Sets the photo width in inches or millimeters.

Conditional Display Value Tab

This tab enables you to display or hide a badge object depending on the conditions you define in the Field and Value fields.

1. Select a display condition from the Field drop-down list. For example, a valid value is BADGE_CITY.
2. Enter a corresponding value into the Value field. For example, a valid value is Baltimore. Note that if the Field is a Boolean field, then the acceptable values are “TRUE” and “FALSE.”

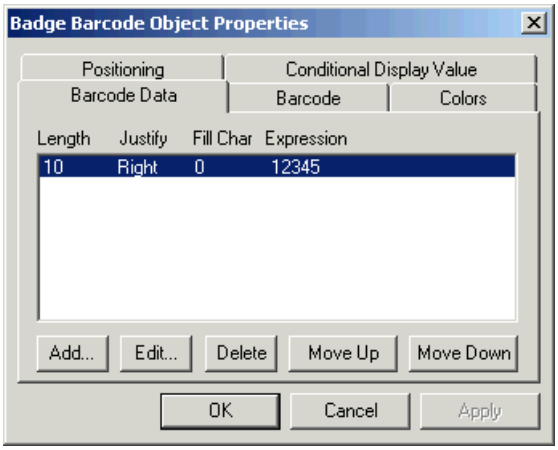
In this example, the specific badge object will be displayed only if the “Badge City” variable has a value of “Baltimore.” For all other cities, the badge object will NOT be displayed.

G.4.2.4 Placing a Barcode

Barcodes are machine-readable symbols that are made of patterns of black and white bars, or in some cases checkerboard-like grids. There are different styles of barcodes, called symbologies. Code 39, UPC, and Code 128 are examples of different symbologies.

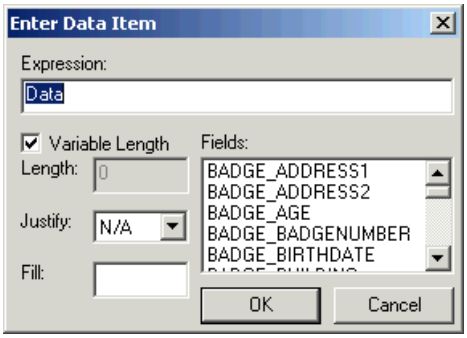
Bits of information are encoded within bar codes. The data is read by a barcode scanner and is often used in conjunction with databases. Barcodes do not require human input, they can be read by automated machines.

1. Either select **Toolbar > Place Barcode** from the menu bar or click the Place Barcode icon on the tool bar.
2. Click and drag the cursor on the layout design sheet to define the size you want for the barcode.
3. Right-click the barcode area and select Properties. The Badge Barcode Object Properties dialog box appears:



Barcode Data Tab

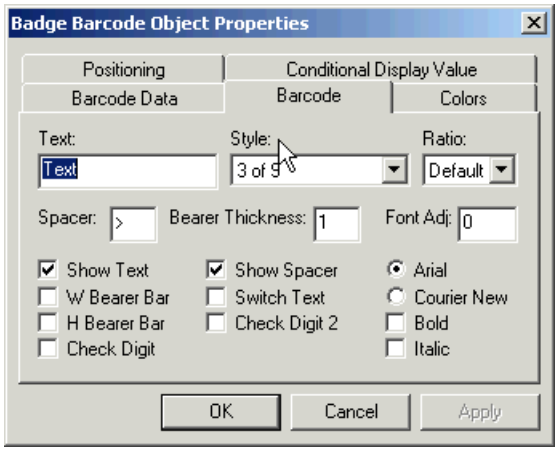
1. Click **Add** to display the Enter Data Item dialog box where you can define each line within the selected barcode:



2. Go to the Expression box and define the type of barcode line you are adding. For example, enter Data or Value for line of text or numbers.
3. Click **Variable Length** if the number of characters within the barcode will periodically change. Do not click this option if the number of characters will remain constant. Then, go to the Length box and enter the number of characters.
4. To align or "justify" the barcode line, locate the Justify box and select **N/A** (meaning "not applicable"), **Left**, **Center**, or **Right**.
5. Go to the **Fill** box and enter the fill characters if the fixed Length setting exceeds the length of the data in the barcode. For example: your barcode would be 0000012345 if your fixed data length is 10, your data to code is 12345, and your Fill is set at 0.
6. Locate the **Fields** box and select the type of barcode field you are adding.
7. Click **OK** to save your settings and To the Badge Barcode Object Properties dialog box.
8. To reposition one or more barcode lines, select each line and click **Move Up** or **Move Down**. To modify or remove a barcode line, select it and click **Edit** or **Delete**.
9. From here you can access other barcode properties by clicking the correct tab, or you can click **Apply** to assign the settings to the selected barcode.
10. Click **OK** to close the dialog box.

Barcode Tab

1. Go to the **Text** box and enter the name of the barcode.

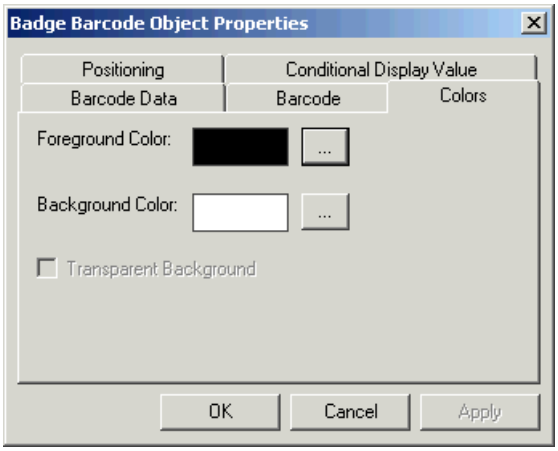


2. Find the **Style** drop-down box and select the correct barcode format that you want to use. Consult your card reader documentation for specific details.

3. Go to the **Ratio** drop-down box and select the width ratio between the thick and thin bars within the barcode.
4. Find the **Spacer** box and enter the space before and after the barcode on the badge layout.
5. In the **Bearer Thickness** box, enter an integer between 1 and 30 for the correct thickness of the bearer bars in Points (72 points to an inch).
6. In the **Font Adj** box, enter the correct font size in relation to the barcode if text is displayed.
7. In the lower portion of the dialog, select all that apply:
    - Show Text – shows the barcode data in text, below the barcode.
    - **W Bearer Bar –** displays the width bearer bars (top and bottom borders).
    - **H Bearer Bar –** displays the height bearer bars (left and right borders).
    - **Check Digit –** enables error checking.
    - **Show Spacer –** displays the space before and after the barcode data.
    - **Switch Text –** switches the top and bottom text. Barcode data is displayed as text and is placed above the barcode; the text entered into the Text field is displayed below the barcode.
    - **Check Digit 2 –** enables error checking.
    - **Arial –** designates the text font type.
    - **Courier New –** designates the text font type.
    - **Bold –** designates the text font weight.
    - **Italic –** designates the text font style. From here you can access other barcode properties by clicking the correct tab, or you can click **Apply** to assign the settings to the selected barcode.
8. Click **OK** to close the dialog box.

Colors Tab

1. Go to **Foreground Color** box and select the associated browse button.



2. Click a basic color from the Color dialog, or click **Define Custom Colors** to create a more desirable color.
3. Click **OK** to assign the color.
4. Locate the **Background Color** box and follow the same instructions listed above.
5. The system returns to the Badge Barcode Object Properties dialog box. From here you can access other barcode properties by clicking the correct tab, or you can **Apply** to assign the settings.
6. Click **OK** to save the settings and close the dialog.

Positioning Tab

This function positions the barcode on the badge. Use the following field definitions to position the barcode:

Field	Description
Horizontal Position	Right-justifies, left-justifies, or centers the barcode on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Vertical position	Top-justifies, bottom-justifies, or centers the barcode on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Orientation	Rotates the barcode on the badge by multiples of ninety degrees.
Top	Sets the barcode distance from the top of the badge in inches or millimeters.
Height	Sets the barcode height in inches or millimeters.
Left	Sets the barcode distance from the left border of the badge in inches or millimeters.
Width	Sets the barcode width in inches or millimeters.

Conditional Display Value Tab

This tab enables you to display or hide a badge object depending on the conditions you define in the Field and Value fields.

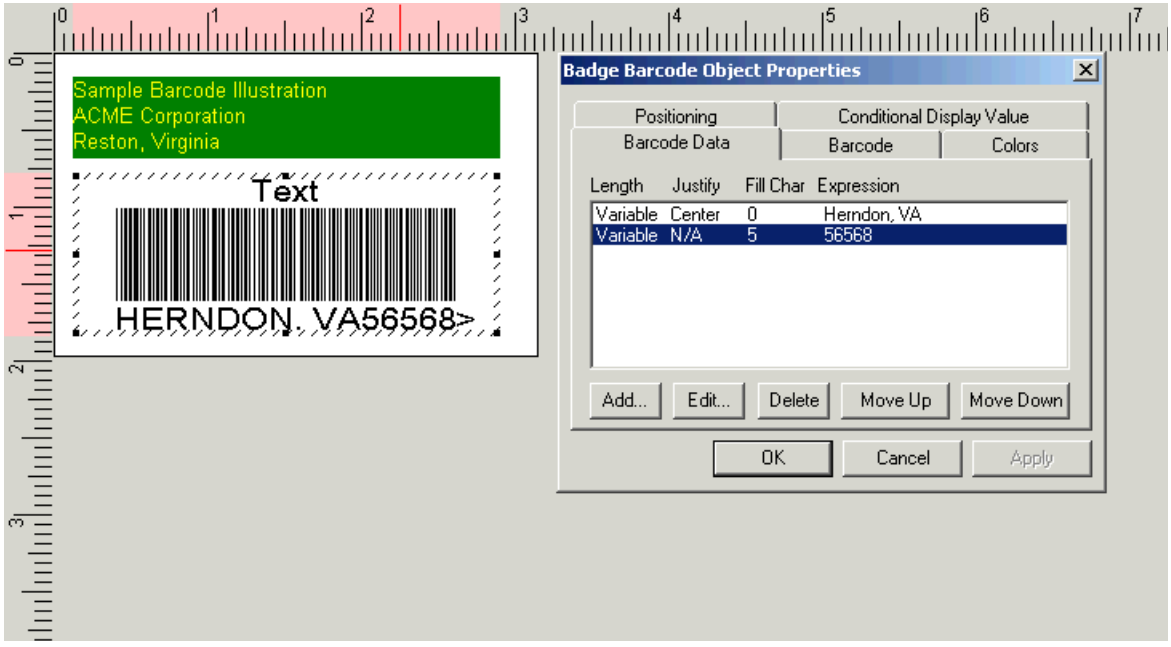
1. Select a display condition from the Field drop-down list. For example, a valid value is BADGE_CITY.
2. Enter a corresponding value into the Value field. For example, a valid value is Baltimore. Note that if the Field is a Boolean field, then the acceptable values are “TRUE” and “FALSE.”

In this example, the specific badge object will be displayed only if the “Badge City” variable has a value of “Baltimore.” For all other cities, the badge object will NOT be displayed.

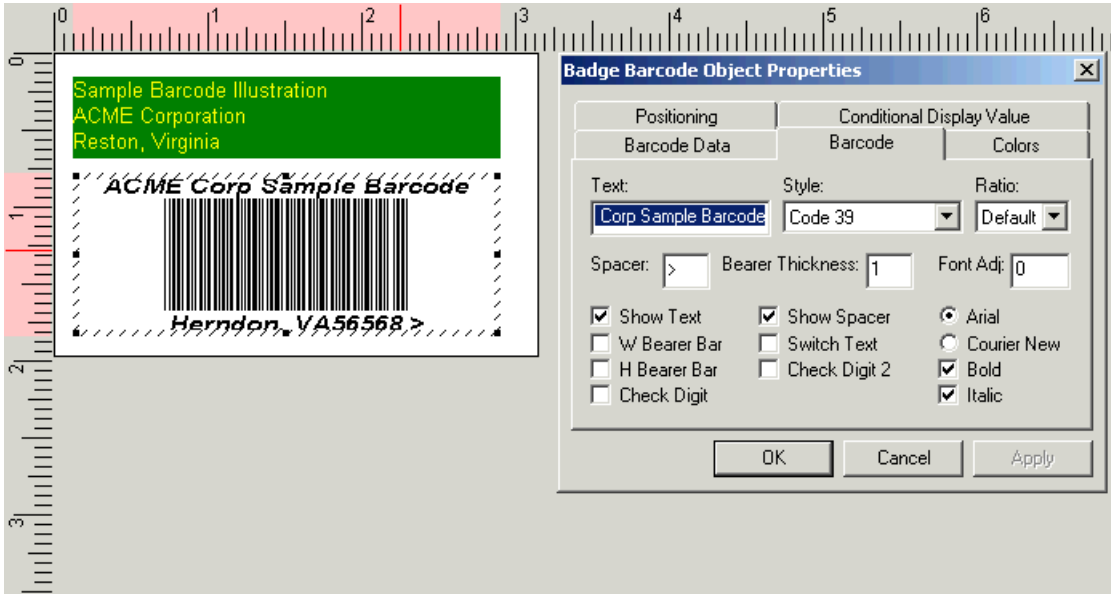
Example: Designing a Barcode

Here is how you can design a sample barcode from scratch:

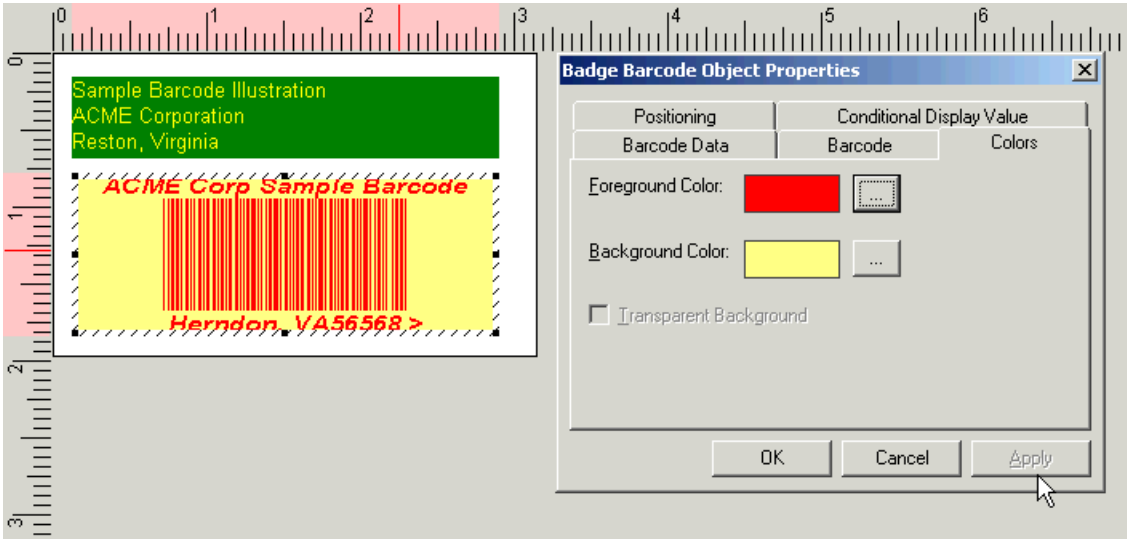
1. Select **Edit >Badge Layout > Front** (or **> Back**) from the main Badging menu bar to launch the BadgeDesigner program in its own separate window.
2. Select **Tool bar > Place Barcode** from the menu bar. The cursor changes to a barcode icon.
3. Click and drag your cursor on the badge image to define the size of the barcode area. When you let go, the program will automatically place a barcode place-holder image.
4. Right-click on the barcode image and select **Properties** from the pop-up menu to display the Badge Barcode Object Properties screen.
5. In the Barcode Data tab, delete all the displayed data by selecting each row and then clicking **Delete**.
6. Click **Add**, and add the following data rows:
   - BADGE_ADDRESS1: Herndon, VA, Center justified, no fill.
   - BADGE_BADGENUMBER: 56568, justification N/A, 5 digits in length.
7. Click **Apply**. The barcode now looks like this:



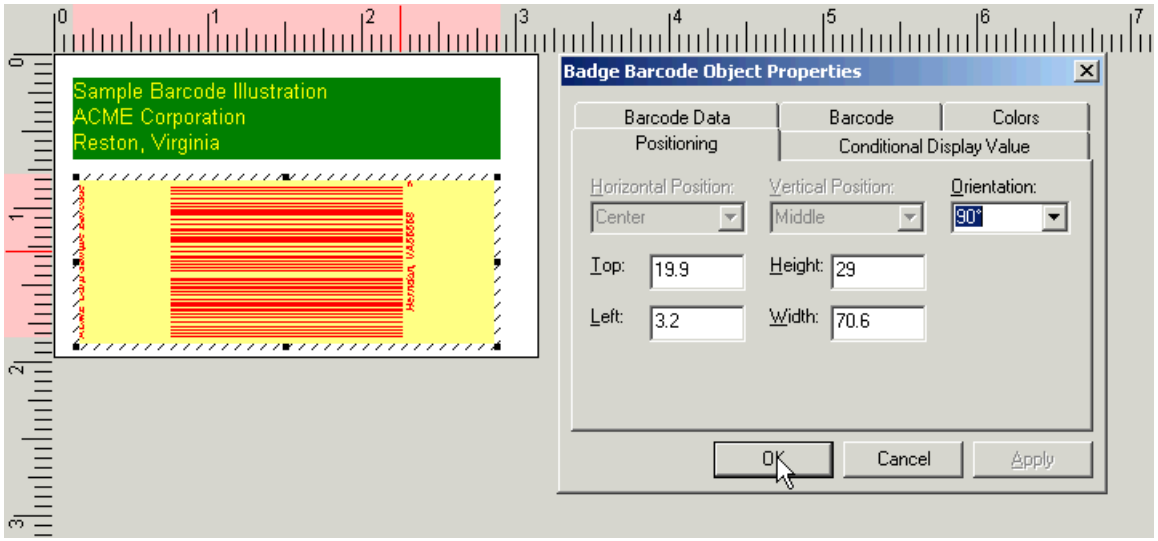
8. Select the **Barcode** tab and enter the "ACME Corp Sample Barcode" for Text and select **Bold** and **Italic** as font style, and "**Code 39**" as general barcode style, and click **Apply**.



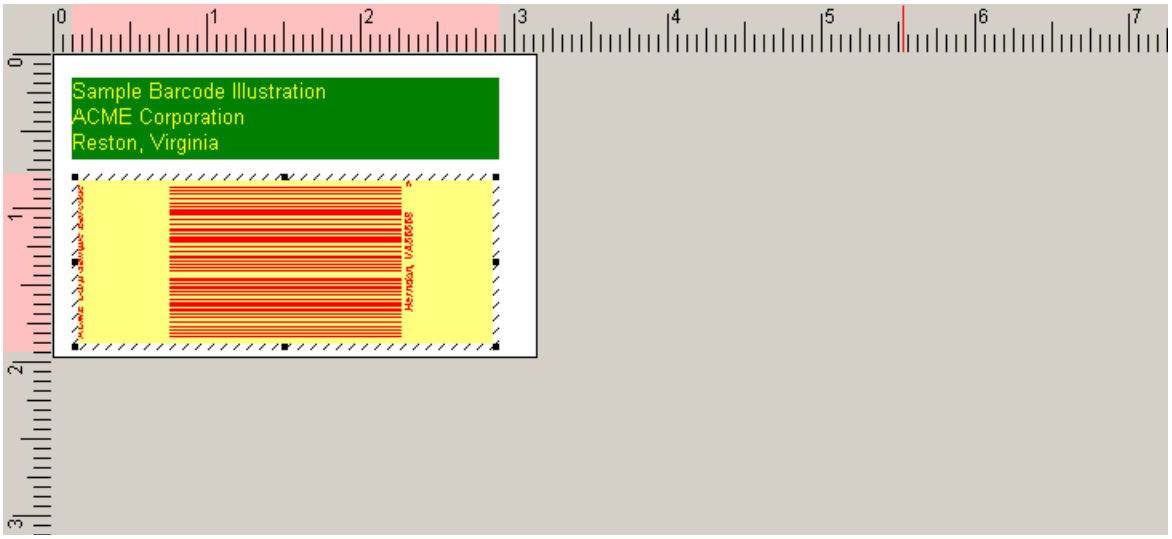
9. Select the **Colors** tab and click the buttons next to the foreground and background color fields, respectively. Select a yellow background and a red foreground, and click **Apply**.



10. Select the **Positioning** tab and enter “29” for Height, “90” for Orientation, and click **Apply**.



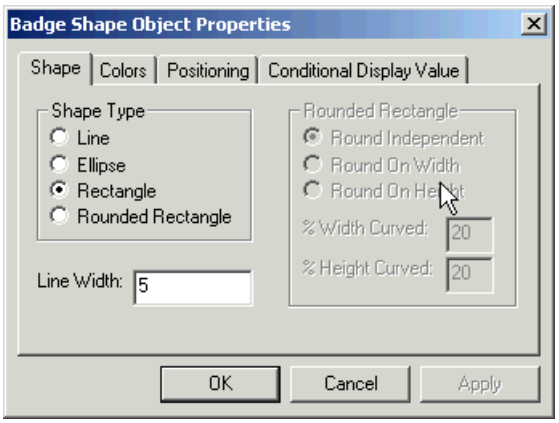
11. Don’t enter anything into the Conditional Display Value tab. Click **OK** to finish designing the barcode.



G.4.2.5 Placing a Shape

Use this function to place a shape, such as a line, ellipse, rectangle, or rounded rectangle.

1. Either select **Toolbar > Place Shape** from the menu bar or click the **Place Shape** icon on the tool bar.
2. Click and drag the cursor on the layout design sheet to define the size you want for the shape.
3. Right-click the shape area and select **Properties**. The Badge Shape Object Properties dialog box appears:



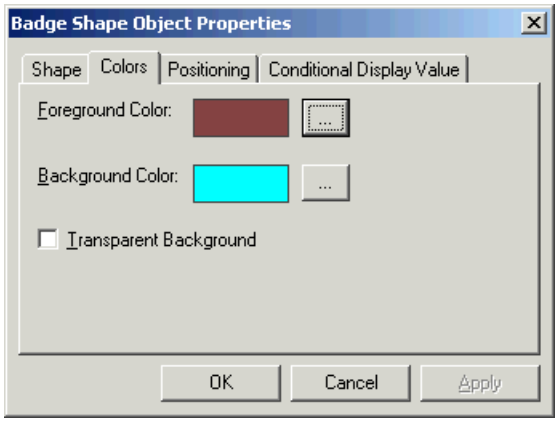
4. Complete the following tabs to set the shape, colors, and positioning properties.

Shape Tab

1. Select the shape type. If you select **Rounded Rectangle**, the system enables the following Rounded Rectangle options in the right portion of the dialog box:
   - **Round Independent:** if you select this option, be sure to go to the **% Width Curved** and the **% Height Curved** boxes and enter the curve percentages.
   - **Round on Width:** if you select this option, be sure to find the **% Width Curved** box and enter the curve percentage.
   - **Round on Height:** if you select this option, locate the **% Height Curved** box and enter the curve percentage.
2. Locate the **Line Width** box and enter an integer between 1 and 100 for width of the selected line in Points (72 points to an inch). From here you can access other badge shape properties by clicking the appropriate tab, or you can click **Apply** to assign the settings to the selected shape.
3. Click **OK** to close the dialog.

Color Tab

1. Go to **Foreground Color** box and select the associated browse button.



2. Click a basic color from the Color dialog or click **Define Custom Colors** to create a more desirable color.
3. Click **OK** to assign the color.
4. Locate the **Background Color** box and follow the same instructions listed above. The Badge Shape Object Properties dialog box appears.

   From here you can access other badge shape properties by clicking the correct tab, or you can click **Apply** to assign the settings to the selected shape.
5. Click **OK** to close the dialog.

Positioning Tab

This function positions the shape on the badge. Use the following field definitions to position the shape:

Field	Description
Horizontal Position	Right-justifies, left-justifies, or centers the shape on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Vertical Position	Top-justifies, bottom-justifies, or centers the shape on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Orientation	Rotates the shape on the badge by a specified number of degrees.

Field	Description
Top	Sets the distance of the shape from the top of the badge in inches or millimeters.
Height	Sets the height of the shape in inches or millimeters.
Left	Sets the distance of the shape from the left border of the badge in inches or millimeters.
Width	Sets the width of the shape in inches or millimeters.

Conditional Display Value Tab

This tab enables you to display or hide a badge object depending on the conditions you define in the Field and Value fields.

1. Select a display condition from the Field drop-down list. For example, a valid value is BADGE_CITY.
2. Enter a corresponding value into the Value field. For example, a valid value is Baltimore. Note that if the Field is a Boolean field, then the acceptable values are “TRUE” and “FALSE.”

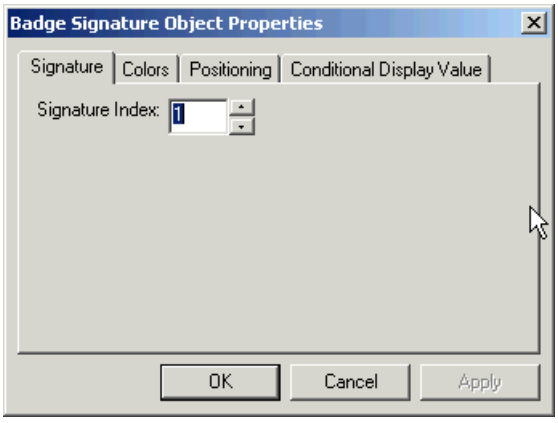
In this example, the specific badge object will be displayed only if the “Badge City” variable has a value of “Baltimore.” For all other cities, the badge object will NOT be displayed.

G.4.2.6 Placing a Signature

Use this function to place a signature on the card.

1. Either select **Toolbar > Place Signature** from the menu bar or click the icon on the tool bar.
2. Click and drag the cursor on the layout design sheet to define the size you want for the signature.

3. Right-click the signature area and select **Properties**. The Badge Signature Object Properties dialog box appears:



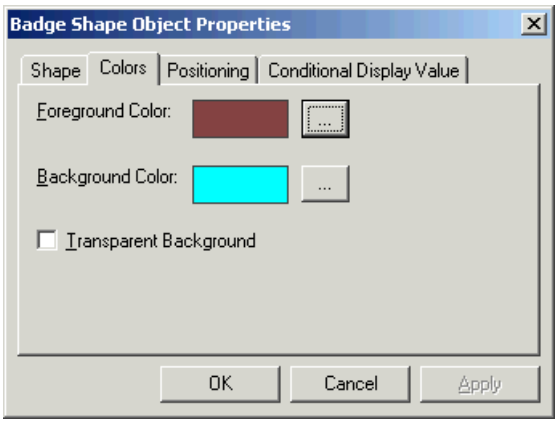
Complete the following tabs to set the signature, colors, and positioning properties.

Signature Tab

1. Enter or select the correct signature index from the Signature Index box.
2. You can access other signature properties by clicking the correct tab, or you can click **OK** to save the index setting and close the dialog.

Colors Tab

1. Locate the **Background Color** box and click the associated browse button.



2. Click a basic color from the Color dialog box or click **Define Custom Colors** to create a more desirable color.
3. Click **OK** to assign the color.

4. Select Transparent Background if you want the assigned background color to be transparent.
5. From here you can access other signature properties by clicking the correct tab, or you can **Assign** to apply the settings to the selected signature.
6. Click **OK** to save the index setting and close the dialog.

Positioning Tab

This function positions the signature on the badge. Use the following field definitions to position the signature:

Field	Description
Horizontal Position	Right-justifies, left-justifies, or centers the signature on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Vertical Position	Top-justifies, bottom-justifies, or centers the signature on the badge. The value is measured in the unit specified for the layout design sheet (see "Using Inches or Millimeters").
Orientation	Rotates the signature on the badge by a specified number of degrees.
Top	Sets the distance of the signature from the top of the badge in inches or millimeters.
Height	Sets the height of the signature in inches or millimeters.
Left	Sets the distance of the signature from the left border of the badge in inches or millimeters.
Width	Sets the width of the signature in inches or millimeters.

Conditional Display Value

This tab enables you to display or hide a badge object depending on the conditions you define in the Field and Value fields.

1. Select a display condition from the Field drop-down list. For example, a valid value is BADGE_CITY.
2. Enter a corresponding value into the Value field. For example, a valid value is Baltimore. Note that if the Field is a Boolean field, then the acceptable values are “TRUE” and “FALSE.”

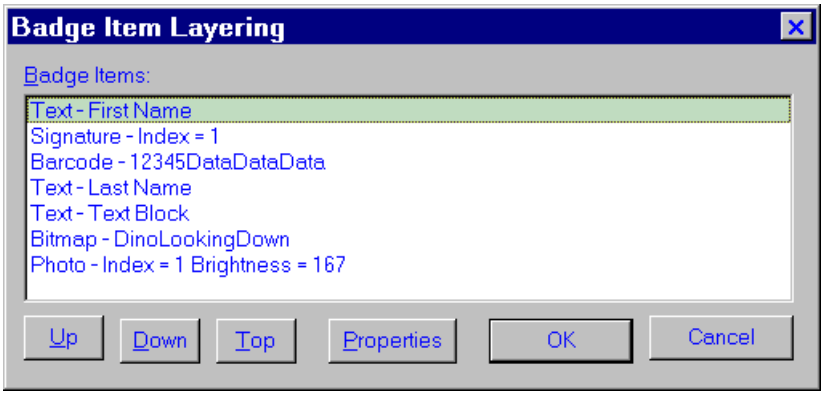
In this example, the specific badge object will be displayed only if the “Badge City” variable has a value of “Baltimore.” For all other cities, the badge object will NOT be displayed.

G.4.2.7 Layering Badge Items

Use this function to layer badge layout items in order to decide which layers to display.

Badge items are layered in the order you place them on the design layout. When you select a badge item, it is brought to the top of the layering order. Layering can also be controlled using the Badge Item Layering dialog, from which you can edit the item properties without changing their layering order.

1. In the Badge Designer, either select **Toolbar > Change Layering** from the menu bar or click the **Change Layering** button ( ) on the tool bar to display the Badge Item Layering dialog box:



2. Select the badge item(s) you want to layer and click **Up**, **Down**, or **Top** until the desired location is achieved. Please note that you can also access the select item's properties from this dialog by selecting the item and clicking **Properties**.
3. Click **OK** to save your settings and close the dialog.

G.5 Exiting the Badge Designer

Do one of the following to exit the Badge Designer:

- Select **File > Exit** from the menu bar.
- Click **Close** within the Badge Designer window.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Reports

H

In this appendix ...

Overview
Creating Reports
Using Reports
Report Designer

H.1 Overview

This appendix describes how to use the Classic Reports module. For Compliance Reports see the chapter on "".

You can produce a comprehensive report of any Pro-Watch data group of your choice in a few keystrokes. You can select data to match specified criteria, sort the data by specified fields, and partition the report. You can preview, print, or export the report. These are the general categories of reports you can generate:

- Access reports.
- Badge holder reports.
- Company reports.
- Configuration reports.
- Logging reports.
- User reports.
- Vindicator reports.

You can also design your own report. See "Report Designer".

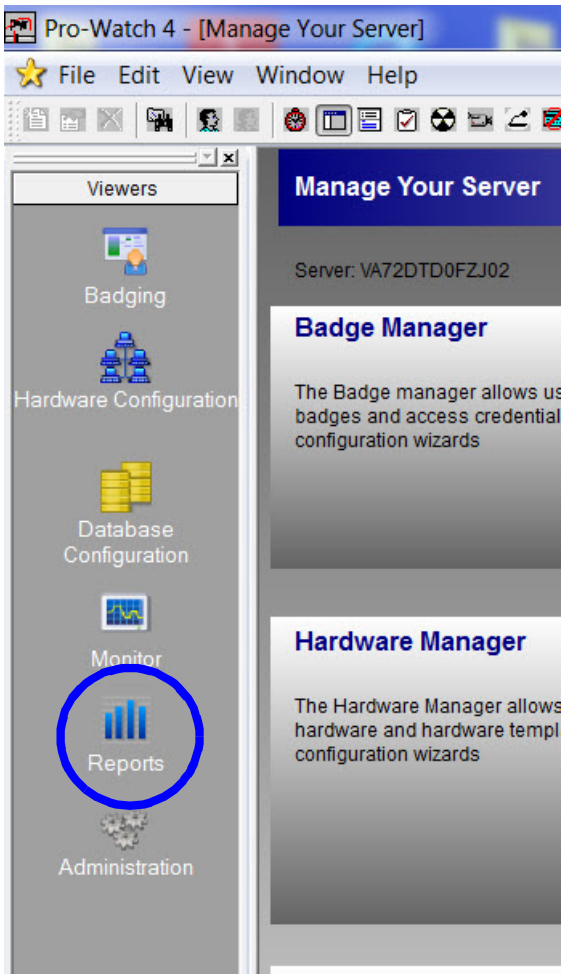
H.1.1 To switch from one module to another

To switch from one report module to another please see "To switch from classic reports to compliance reports".

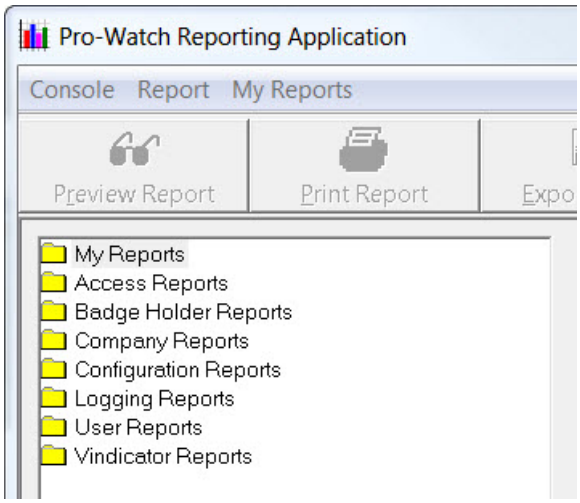
H.2 Creating Reports

Follow these steps to create and use reports:

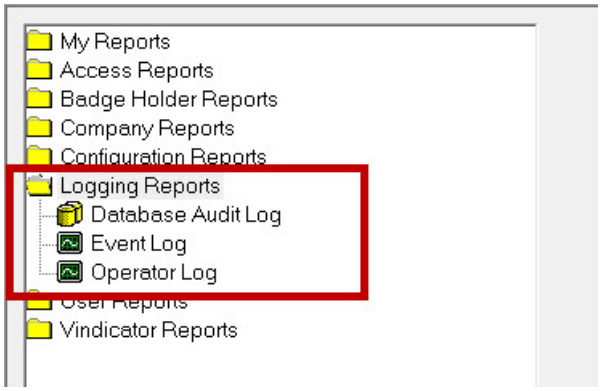
1. Click the **Reports** icon in the navigation pane of the Pro-Watch main screen:



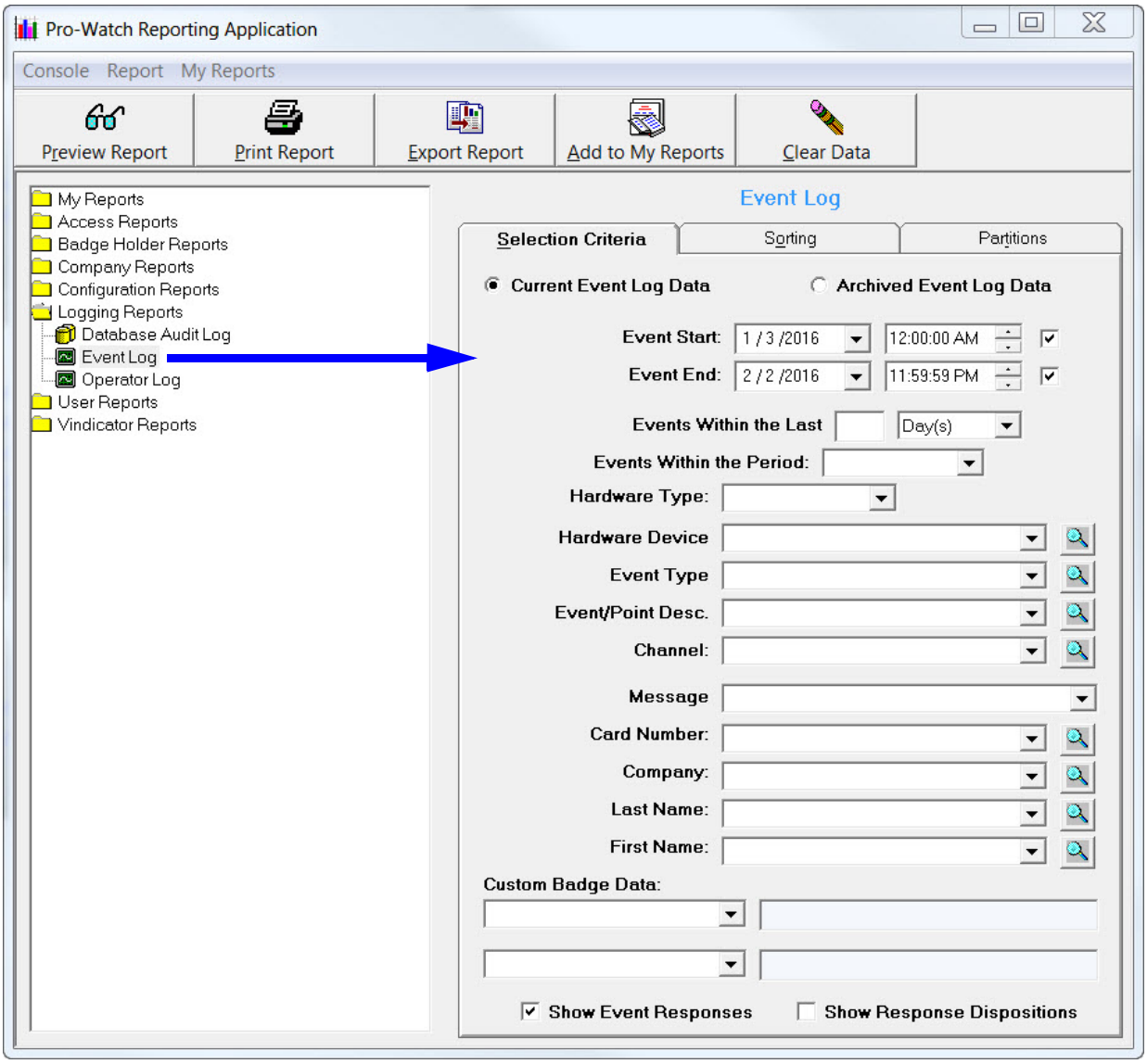
The **Pro-Watch Reporting Application** starts and displays the list of reporting applications available:



2. Click to select the application you want (for example, “Logging Report” selected below):

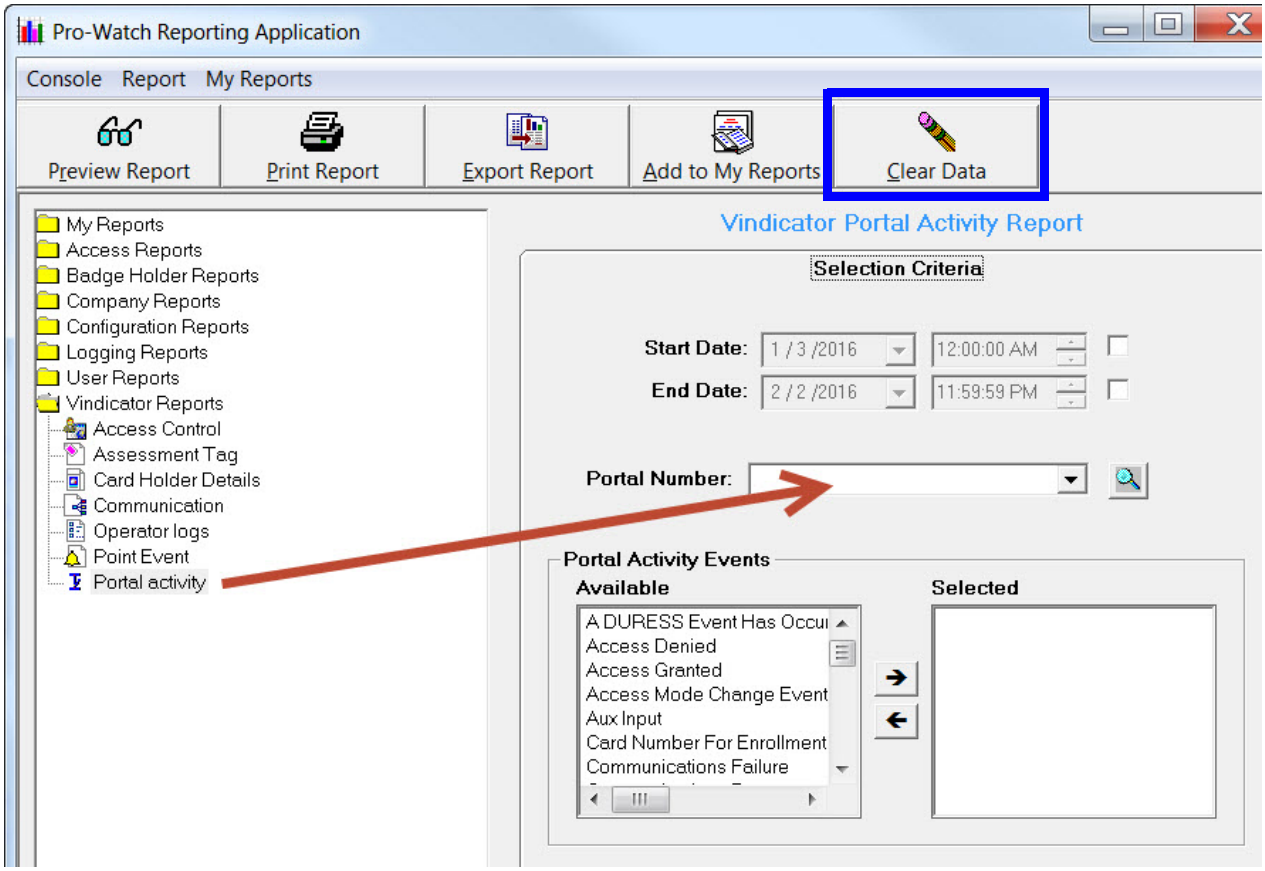


3. Click to select the type of report you want to create (for example, “Event Log” selected below):



4. Enter all appropriate field values in the criteria tabs displayed for the report you have selected.

Note: When you run a Vindicator Portal Activity report, one criterion you need to enter is the portal number (see below):



Be sure that when you enter a portal number and create the report, you click the Clear Data button at the top of the screen before you enter another portal number to create another portal activity report.

H.2.1 Vista Commercial Panels

Vista panels generate Alarm Only reports or Zone Alarm Restore Reports. These modes are mutually exclusive.

To activate Alarm Only Reports (turns off Zone Restore Reports):

1. Enter Panel Program Mode by entering “Installer Code” + 8000 at the keypad. The keypad will show:

   PROGRAM MODE
   * FILL # VIEW-00

2. Press *89. The keypad will show:

   RESTORE REPORTING TIMING -89

3. Press 2. Keypad will beep 3 times and show

   2ND SUBS. ACCOUNT # -90

4. Press *99 to exit Program Mode. Keypad will show

   VISTA-XXX SYSTEM RESET

5. Wait 2 minutes for the panel to reset, or press Code +1 twice to bypass this wait time.

Zone Alarm Restore Reports will not be held until Disarm.

To reactivate Zone Restore Reports:

1. To enable Panel Program Mode, enter “Installer Code” + 8000 at the keypad. The keypad will show:

   PROGRAM MODE
   * FILL # VIEW-00

2. Press *89. The keypad will show:

   RESTORE REPORTING TIMING -89

3. Press 0. The keypad will beep 3 times and show

   2ND SUBS. ACCOUNT # -90

4. Press *99 to exit Program Mode. The keypad will show

   VISTA-XXX SYSTEM RESET

5. Wait 2 minutes for the panel to reset, or press Code +1 twice to bypass this wait time.

Zone Alarm Restore Reports will now be sent as soon as the zone is restored.

H.3 Using Reports

After you have completed the criteria tabs to generate a report, you can print, export, or clear the data of the report. You can also save the report configuration in your My Reports folder for future use.

H.3.1 Printing a Report

You can print a report from either the Report menu or the icon toolbar:

1. From the report generation screen, click the **Print Report** icon on the tool bar. Or, select **Report > Print Report** from the menu bar. The Print dialog box appears.
2. Complete the General, Layout, and Paper Quality tabs in the Print dialog box to configure the printout as you want it.
3. Click **Print**.

Alternatively, you can print reports from the Preview Report display. Select either Report > Print Preview from the Report menu or click the Preview Report icon on the toolbar to print the report.

H.3.2 Exporting a Report

Pro-Watch allows you to export a report to a file and to design the export file's format.

To access the Export Report wizard:

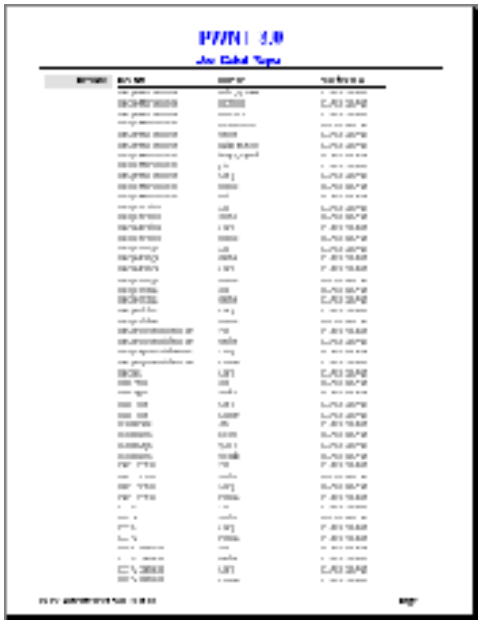
- From the Pro-Watch Reporting Application screen, select **Report > Export Report** from the main menu.
- From the Pro-Watch Reporting Application screen, click the **Export Report** icon on the tool bar.
- From the previewed report display, click the **Export** menu bar button.

Complete the steps in the following sections to finish the wizard.

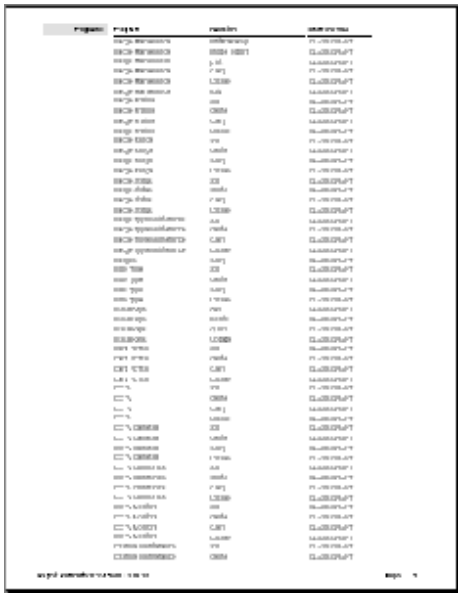
H.3.2.1 Headers and Footers

Click Yes to place the report title at the top of each page. Click No for no report title. The following sample report shows the two options:

With headers and footers ...



Without headers and footers ...



H.3.2.2 Report File Formats

Pro-Watch offers the following report formats to best match your needs:

- De-limited text (.txt).
- Excel spreadsheet (.xls).
- Adobe Acrobat Portable Document Format (.pdf).
- Microsoft Word Rich Text Format (.rtf).
- Hypertext Markup (.htm).

Click the format you want and click **Next to choose from different sets of parameters**.

H.3.2.3 Format Parameters

The .txt, .xls, and .pdf formats offer different parameter options:

Format	Parameter	Description
Delimited text	Text delimiter	Format parameter that defines the end of each column of data in the report display. Use any of the following: Semi-colon (;). Comma (,). Vertical bar (/). Colon (:). Tab.
	Page delimiter	Format parameter that defines the end of each page in the text of the report display. Use any of the following: Carriage return. Line feed. New line. Horizontal tab. Vertical tab. Form feed. Null character.
	Suppress empty lines	Determines whether empty lines will or will not be inserted for layout purposes.
	Unicode	Determines whether the text will be saved as a UNICODE text file. UNICODE provides a unique number for every character, regardless of the platform, program or the language.
Excel spreadsheet	Auto Row Height	When set to true, Excel will correct for the size of the line by resizing the line to the largest object on the line.
	Double Boundaries	Places columns on both the left and right sides of a field.
	Generate page breaks	Determines if the export method will generate page breaks automatically in the exported file.

Format	Parameter	Description
Excel spreadsheet (continued)	Multi-sheet	Determines if the report will be generated as a single Excel sheet, or as a multiple sheet workbook.
	Show margin space	Specifies whether the space between the report elements and the margin will display. Default is False.
	Border space	Amount of vertical space added to the lines in twips (1/1440th of an inch).
	Minimum column width	Minimum column width in twips (1/1440th of an inch). Larger values reduce number of columns in a sheet.
	Minimum row height	Minimum row height in twips (1/1440th of an inch). Larger values force the export to place more controls on a single line.
	Excel version	The version number of the Excel you are using. Versions 2, 3, 4, 5, 7, and 8 are supported.
	Trim empty space	Determines if the exported report outputs runs of vertical empty spaces, or if they are eliminated.
Adobe Acrobat PDF	Acrobat version	The version number of the Acrobat you are using. Versions 2.1, 3.0 and 4.0 are supported.
	JPEG Quality	Image resolution quality, range 1-100.

H.3.2.4 Export File Path

Specify the export file path. The export file does not need to exist before exporting. The wizard creates a new file. You can export to an existing file of the same format. However, this overwrites the existing file contents. An export file contains only one report and does not append multiple reports.

H.3.3 Saving Report Configurations to My Reports Folder

You can add frequently-used report configurations to the My Reports folder. This way, you can

- Generate an updated report without having to re-enter the selection criteria and sorting parameters.
- Schedule the exact times to run the report.

For example, if you create a Badge Holder Access to a Logical Device report for July, you can save the report configuration in the My Reports folder and simply click the report the next month to produce the same report with August data.

Follow these steps:

1. In the Reports window, double-click **Logging Reports** folder.
2. Select a report. Define or edit your selection criteria, sorting options, and partition information.
3. Click the **Add to My Reports** icon on the tool bar, or select **My Reports > Add to My Reports** from the main menu to launch the **Add To My Reports Wizard**.
4. Enter a **report name** and select **Add for User** if this report is only for the user defining it, or **Add for Class** to make it available to all users for a class. Click **Next** to display the printer dialog screen.
5. If you would like to print this report, select the **Yes** option button and select a printer from the drop-down list. If printing the report is not necessary select the **No** option button. Click **Next** to display the “Will you be scheduling this report for Export?” screen.
6. Select the **Yes** option button to export the report on a scheduled basis. See "Exporting a Report" for details on configuring this option. Click **Next**.
7. Select the **Yes** option to export Headers and Footers as well. Click **Next**.
8. Select one of the following option buttons to set the export format: Delimited Text (.txt), Excel Spreadsheet (.xls), Adobe Acrobat (.pdf), Rich text Format (.rtf), and HTML (.htm).
9. In the next dialog box, set the proper options for the format you have selected in the previous screen. Click **Next**.
10. Click **Browse** and select the file to export. The next screen will confirm that you have successfully added the selected report to your My Reports folder.

11. Click **Finished** to return to the Reports window.

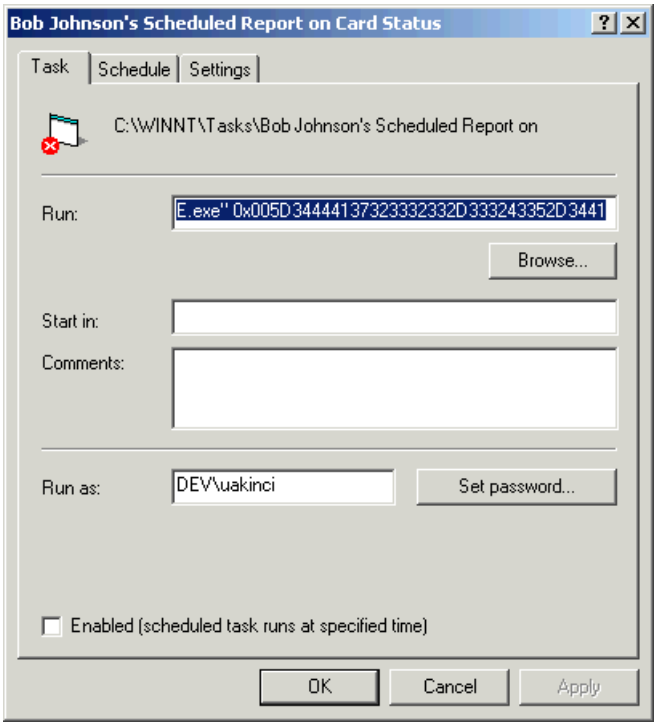
H.3.4 Scheduling a Report

You can schedule reports saved in the My Reports folder to run and export automatically.

Follow these steps:

1. Select **My Reports > Schedule Reports** from the main menu to display the Schedule Reports dialog box.
2. Click **Add New** to display the Add Scheduled Report dialog box.

   Note: If the report name already appears in the Schedule Reports dialog box, click the name to select it and click **Properties** and proceed to Step 7, Task tab.
3. Click the report you want to schedule for export, and click **Next**.
4. Enter a name that will identify a schedule, and click **Next**. The schedule configuration dialog box appears with three tabs, Task, Schedule, and Settings. The focus is on the Task tab by default:



5. Complete each of the following tabs to schedule the report.

H.3.4.1 Task Tab

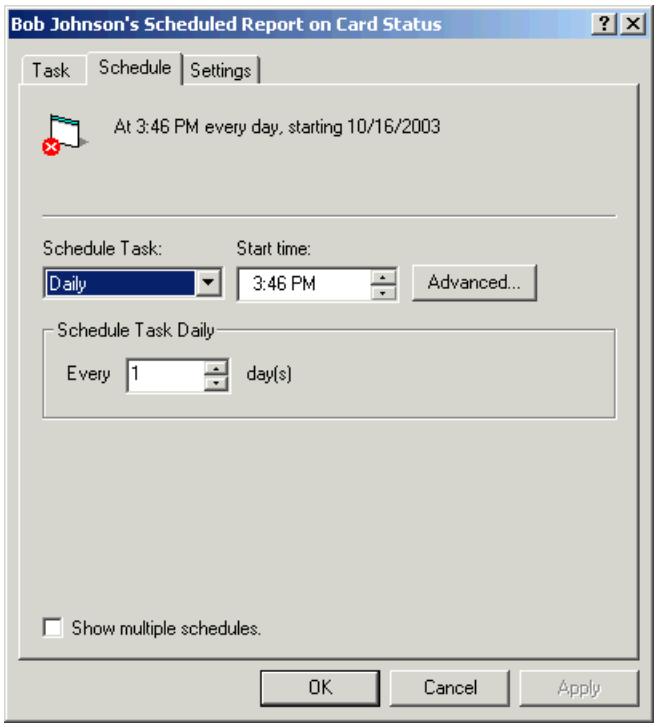
Use the following field descriptions to complete the tab:

Field	Description
Run	Executable program that will generate and export the report. Pro-Watch automatically enters the executable name in the field.
Start in	User should not enter anything here and must leave it blank.
Comments	Comments about the task.
Run as	Domain name and user ID.
Set Password	Click to display the Set Password dialog box where you can set a password for running the scheduled report. You have to enter a password so that the report will run at the scheduled time.
Enabled check-box	Select this check-box to enable the executable to run at the specified time.

H.3.4.2 Schedule Tab

Schedule the start time and the frequency for a report generation on the Schedule tab. By default, these schedules run indefinitely. You can set one or multiple schedules for a report. For example, you may want to schedule a

daily report generation and export as well as a weekly or monthly generation.

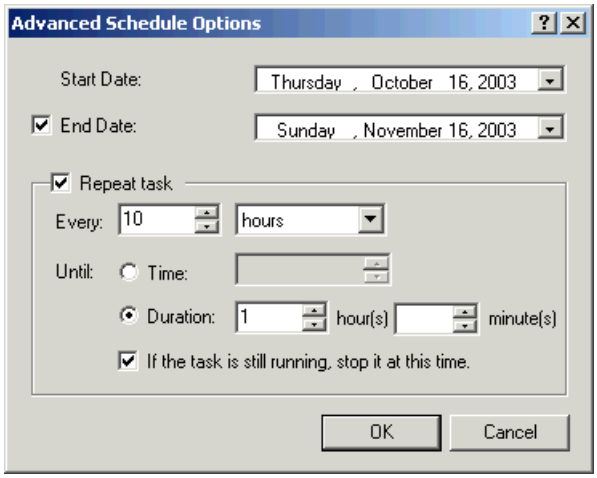


To set multiple schedules, follow these steps:

1. Click **Show multiple schedules** at the bottom of the dialog box. A new field appears at the top of the dialog box.
2. Click **New** to create an additional schedule, and enter the values you want in the Schedule Task and Start Time fields.
3. Click **Apply**.
4. Click **Advanced** for advanced scheduling.

   You can schedule a report to run and export at specified intervals during a fixed period of time. For example, you can schedule a report to run every hour until 6:00 p.m. from July 1 to August 1.

   On the Schedule tab, click **Advanced**. The Advanced Schedule Options dialog box appears.



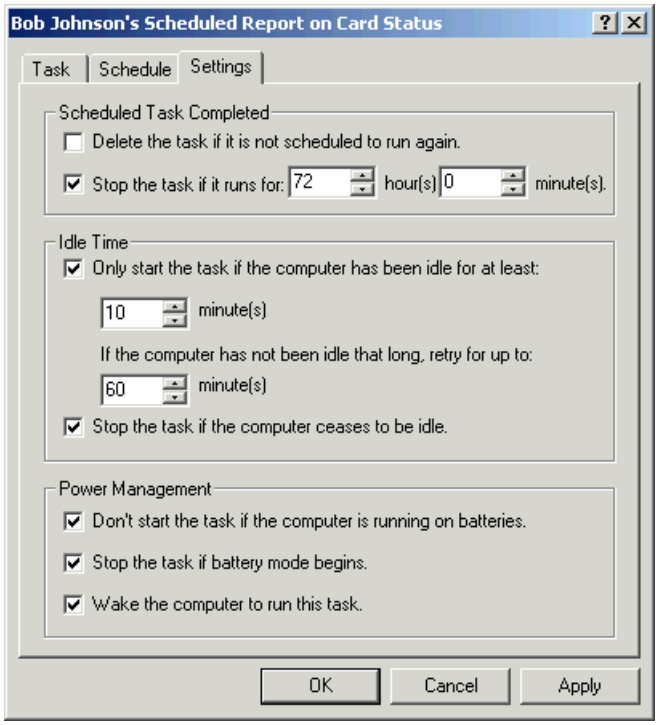
5. Specify the time periods you desire and click **OK**.

H.3.4.3 Testing the scheduled report

1. Verify that the report schedule was created under Windows Control panel and Scheduled Tasks. Also verify that the Enable check box is selected.
2. Verify that a report scheduled to export is working properly by checking the modified date and time under the file properties.
3. In the Schedule Reports window, highlight the report you have created and click **Run Now!**
4. Close the window by clicking the "**X**" in the upper right corner.
5. Verify that the report ran successfully by either checking the file location that you specified during the report creation or check the printer to which you specified the report to print.

H.3.4.4 Settings Tab

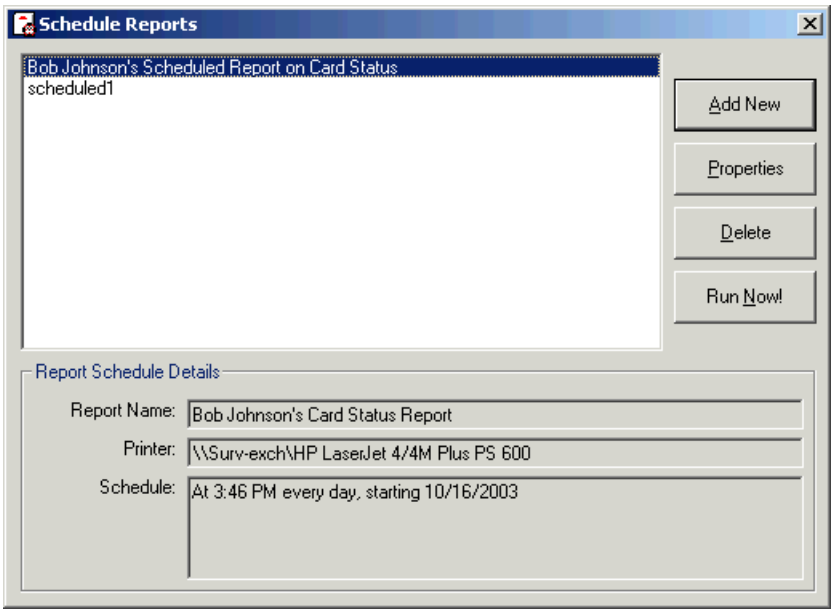
For every report schedule, you can provide instructions for idled or stopped tasks on the Settings tab. You can also provide starting and stopping instructions that relate to the computer's power source condition.



H.3.4.5 Editing/Deleting/Executing a Scheduled Report

To edit, delete or immediately run an existing scheduled report:

1. Select the My Reports menu item.
2. Select **My Reports > Schedule Reports** from the main menu. The Schedule Reports dialog box displays, listing all the schedules which you have created.



3. Click a schedule name from the display list.
4. Click **Run Now!** to run the report, **Delete** to delete the schedule, or click **Properties** to edit the schedule. The edit steps are identical to those for adding a schedule. See "Scheduling a Report" for details.

H.3.5 Access Reports

H.3.5.1 Badge Holder Access To A Logical Device

This report lists all badge holders who have access to a logical device, grouped by badge holder. The selection criteria are:

- Last Name.
- First Name.
- Custom Badge Data.
- Card Number.
- Company.
- Badge or Card Issue Start and End dates, Expiration Start and End dates.
- Logical Device.
- Clearance Code.

H.3.5.2 Card Status

This report lists cards by status (Active, Disabled, Lost, Expired, Lost, Stolen, Terminated, Unaccounted for, and Void) and associated card data. The selection criteria are:

- Last Name.
- First Name.
- Custom Badge Data.
- Card Number.
- Company.
- Card Issue Start and End dates, Expiration Start and End dates.
- Card Status.
- Clearance Code.

H.3.5.3 Clearance Code/Badge Access

This report lists all badge holders with access to a selected clearance code. Report data is grouped by clearance code. The selection criteria are:

- Clearance Code.
- Last Name.
- First Name.
- Custom Badge Data.
- Card Number.
- Company.
- Card Status.
- Badge or Card Issue Start and End dates, Expiration Start and End dates.

H.3.5.4 Last Access at Logical Device

This report lists the last badge holder to present their badge at a logical device. The selection criteria are:

- Logical Device.
- Last Access Start and End dates and times.
- Card Number.
- Company.

H.3.5.5 Last Access by a Badge Holder

This report lists the last logical device at which a badge holder presented a badge. The selection criteria are:

- Last Name.
- First Name.
- Custom Badge Data.
- Logical Device.
- Last Access Start and End dates and times.
- Card Number.
- Company.
- Badge or Card Issue Start and End dates, Expiration Start and End dates.

H.3.5.6 Logical Device Access by a Badge Holder

This report lists all badge holders with access to a logical device. Access may be granted by a clearance code or an individual logical device. A “G” at the end of a report line indicates individual, rather than clearance code, access. Report data is grouped by logical device. The selection criteria are:

- Logical Device.
- Clearance Code.
- Last Name.
- First Name.
- Custom Badge Data.
- Card Number.
- Company.
- Badge or Card Issue Start and End dates, Expiration Start and End dates.

H.3.5.7 Mustering

This report lists all users in a muster area at the time when the report is run, grouped by area. The selection criteria are:

- Area.
- Card Number.

H.3.6 Badge Holder Reports

H.3.6.1 Area Attendance

This report lists the entrance and exit times of badge holders to predefined areas. Report data is grouped by area. The selection criteria are:

- Start Date.
- End Date.
- Area.
- Last Name.
- First Name.
- Custom Badge Data.
- Card Number.
- Company.

H.3.6.2 Badge Holder Detail

This report lists available data for all badge holders. Any picture or signature for a badge holder also appears in the report. The selection criteria are:

- Last Name.
- First Name.
- Custom Badge Data.
- Logical Device.
- Card Number.
- Company.
- Card Status.
- Badge Type.
- Badge or Card Issue Start and End dates, Expiration Start and End dates.
- Logical Device.
- Clearance Code.

H.3.6.3 Badge Holder Summary

This report lists the summary data for selected badge holders. The selection criteria are:

- Last Name.
- First Name.
- Custom Badge Data.
- Badge or Card Issue Start and End dates, Expiration Start and End dates.
- Card Number.
- Card Status.
- Badge Type.
- Company.
- Logical Device.
- Clearance Code.

H.3.6.4 Key Assignment List

For sites using the Brass Keys feature of Pro-Watch, this report lists all keys issued to a badge holder. The selection criteria are:

- Key.
- Last Name.
- First Name.
- Custom Badge Data.
- Card Number.
- Company.
- Badge Expiration dates.
- Key Issue dates.
- Key Due dates.
- Key Return dates.

H.3.7 Company Reports

H.3.7.1 Company Clearance Codes

This report lists all the clearance codes assigned to a company. The selection criteria are:

- Company Name.
- Clearance Codes.

Company Summary

This report provides summary data for all companies set up within the system. The selection criteria are:

- Company Name.
- Contact 1 ~ Name, Title, Phone.
- Contact 2 ~ Name, Title, Phone.

H.3.8 Configuration Reports

H.3.8.1 Badge Profiles

This report provides summary information on badge profiles. The selection criterion is Badge Profile.

H.3.8.2 Badge Types

This report provides summary data on badge types. The selection criterion is Badge Type.

H.3.8.3 Brass Key List

This report lists the physical keys tracked by the system. The selection criterion is Key Description.

H.3.8.4 Channel Configuration

This report provides a summary of the selected channel's configuration. This report is useful for documenting preconfigured settings. The selection criteria are:

- Channel.
- Site.

H.3.8.5 CHIP Panel Configuration

This report provides a summary of the selected CHIP Panel configuration. This report is useful for documenting preconfigured settings. The selection criteria are:

- Panel Name.

- Site.
- Information to Display (Actions, Basic Information, Event Actions, Events, Hardware Tree, Holidays, Site Codes, Sub Panels, Terminal Users, Time Zones, and Zones).

H.3.8.6 Classes

This report provides summary of the users, program assignments, workstations, routing groups and event columns which make up a class. The selection criteria are:

- Class.
- Information to Display (Users, Programs, Work Stations, Routing Groups, Event Pages, Badge Profiles, Event Procedures, Eventview Columns, Keystroke Accelerators, Event Toolbars, and Assign Partitions).

H.3.8.7 Clearance Codes

This report lists all logical devices associated with a clearance code, grouped by clearance code. The selection criteria are:

- Clearance Codes.
- Logical Device.
- Elevator Output.

H.3.8.8 D600AP Panel Configuration

This report provides a summary of the selected D600AP Panel configuration. The selection criteria are:

- Panel.
- Site.
- Information to Display (Basic Information, Sub Panels, Setup, Soft Alarms, Mag Stripe, Time Zones, Holidays, Enable Codes, Card Events, Events and Hardware Tree).

H.3.8.9 Database Tables

This report provides information on the tables used by the system. The selection criterion is Table Name.

H.3.8.10 Device Types

This report lists the device types defined on the system. The selection criterion is Device Name.

H.3.8.11 Dialup Schedules

This report provides summary information on the Dialup Schedules used by the system. The selection criterion is Dialup Schedule.

H.3.8.12 Event Points

This report lists the configuration of selected event points. The selection criteria are:

- Event Description.
- Hardware Type (Channel, Input, Output, Panel, Reader, Subpanel).
- Hardware Description.

H.3.8.13 Event Procedures

This report provides information on configured events procedures, and is useful for documenting the settings at a site. The selection criteria are:

- Event Procedure.
- Display Devices.

H.3.8.14 Event Type

This report lists the configuration of event types used by the system. The selection criteria are:

- Event Type.
- Shunt (Yes/No).
- Auto Clear (Yes/No).

H.3.8.15 Guard Tours

This report provides configuration information on guard tours. The selection criterion is Guard Tour.

H.3.8.16 Hardware Classes

This report lists the hardware classes and any associated partitions. The selection criterion is Hardware Class.

H.3.8.17 Hardware Templates

This report provides comprehensive information on the configuration and settings of hardware templates. The selection criteria are:

- Hardware Template.
- Information to Display (Device Types, PW5000 - Interlocks, Partitions).

H.3.8.18 Logical Devices

This report displays logical device configuration data. The selection criteria are:

- Logical Device.
- Information to Display (Basic Information, Logical Device Details).

H.3.8.19 Modem Pools

This report lists the modem pools and the communication ports assigned to each pool. The selection criteria are:

- Modem Pool.
- Port.

H.3.8.20 Panel Types

This report lists all Panel Types available on the system which are supported by the software key in use. The selection criteria are:

- Panel Name.
- Manufacturer.

H.3.8.21 Partitions

This report lists the partitioned resources on the system, grouped by partition. The selection criteria are:

- Partition ID.
- Resource.

H.3.8.22 Printers

This report displays the configuration settings for log printers. The selection criteria are:

- Printer.
- Site.

H.3.8.23 PW2000 Panel Configuration

This report lists the complete configuration of the selected PW2000 panel(s). The selection criteria are:

- Panel Name.
- Site.
- Information to Display (Basic Information, Card Formats, Events, Facility Codes, Hardware Tree, Holidays, Interlocks, Output Groups, Time Zones).

H.3.8.24 PW5000 Panel Configuration

This report lists the complete configuration of the selected PW5000 panel(s). The selection criteria are:

- Panel Name.
- Site.
- Information to Display (Basic Information, Card Formats, Events, Hardware Tree, Holidays, Sub Panels, System Procedures, System Triggers, Time Zones, User Procedures, User Triggers).

H.3.8.25 Response Codes

This report lists the response codes in use on the system. The selection criterion is Response Code.

H.3.8.26 Routing Groups

This report provides information on the resources assigned to a routing group. The selection criterion is Routing Group.

H.3.8.27 SEEP Panel Configuration

This report lists the complete configuration of the selected SEEP panel(s). The selection criteria are:

- Panel.
- Site.
- Information to Display (Basic Information, Events, Hardware Tree, Holidays, Reports, Site Codes, Time Zones).

H.3.8.28 Time Zones

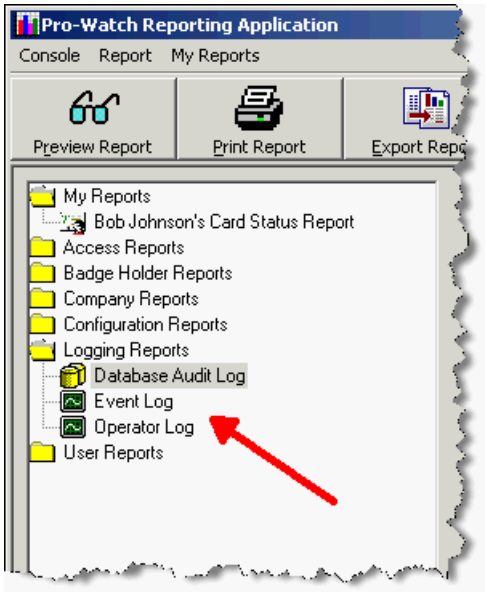
This report provides data on configured time zones. The selection criterion is Time Zone.

H.3.8.29 Workstations

This report provides data on configured workstations. The selection criterion is Workstation Name.

H.3.9 Logging Reports

Use the report tree on the Pro-Watch Reporting Application screen to display the Database Audit Log, Event Log, and Operator Log report query dialog boxes.



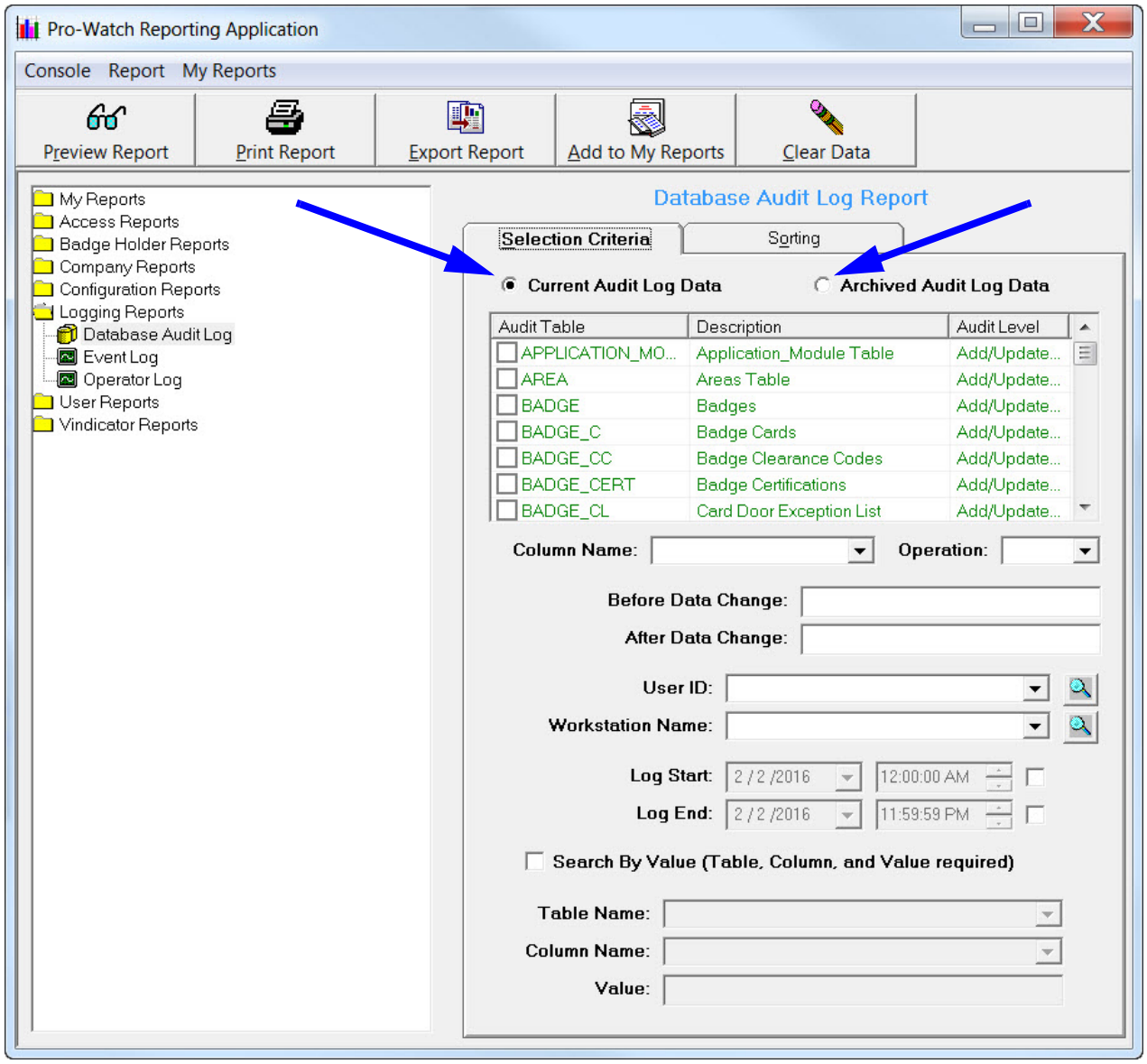
H.3.9.1 Database Audit Log

This report displays auditing information. Use of this report presumes auditing has been activated on the desired database tables (auditing can be activated through the Database Tables feature).

The radio buttons near the top of the database audit log query box enable you to query a database audit log report either from the current audit log data or from archived audit log data.

To create a report, select either the Current Audit Log Data or Archived Audit Log Data radio button and complete the rest of the report screen.

Note that if you are creating a report from archived data, you must first restore the desired archived data to the audit log workspace:



Within the Selection Criteria Tab, only those tables shown in green have auditing enabled. Apart from this restriction, the report generation procedure is identical to all Pro-Watch reports.

H.3.9.2 Event Log

This report provides a concise listing of Pro-Watch events. Monitor, alarm, card transaction, and related events are listed. The selection criteria are:

- Event Start and End dates and times.
- Events Within the Last (Days/Hours/Minutes).

- Events Within the Period (Month to Date/Year to Date).
- Hardware Type (Panel, Subpanel, Reader, Input, Output).
- Hardware Device.
- Event Type.
- Event/Point Description.
- Message.
- Card Number.
- Company.
- Last Name.
- First Name.
- Show Events Responses.
- Show Response Dispositions.

The radio buttons near the top of the database event log query box enable you to query a database event log report either from the current event log data or from archived event log data.

To create a report, select either the Current Event Log Data or Archived Event Log Data radio button and complete the rest of the report screen. Note that if you are creating a report from archived data, you must first restore the desired archived data to the event log workspace.

H.3.9.3 Operator Log

This report lists actions taken by system operators. The selection criteria are:

- Start and End dates and times.
- Logged Within the Last (Days).
- Logged Within the Period (Month to Date/Year to Date).
- Workstation.
- User Name.
- Log Action (Alarm response has been entered, Archive has completed, Archive start, Arm an alarm point, CCTV command has been requested, Database queryset, Database record add, Database record deleted, Database record updated, Door in access mode, Door locked, Door unlocked, Download request, Event log is filling up, Exceeded your concurrent license, Invalid operator class, Invalid operator ID, Invalid password, Invalid workstation, Maps have been rebuilt, Mask an alarm point, Momentary unlock, Operator has logged in, Operator has logged off, Operator ID has expired, Operator log is filling up, Output activate request, Output deactivate request, Output

momentary pulse, Page has been issued, Report has been requested, Restore has completed, Restore has started, System procedure has been executed, Threat level change request, Timed override issue, Void card request).

H.3.10 User Reports

H.3.10.1 User Detail

This report provides detailed information on the configuration of users within the system. The selection criteria are:

- User name.
- Class.
- Last name.
- First name.
- Expiration Start and End dates.
- Information to display (Programs, Workstations, Routing groups, Alarm pages, Badge profiles, Event procedures, Eventview columns, Keystroke accelerators, Event toolbars, Assigned partitions).

H.3.10.2 User Summary

This report provides summary data of system users. It is useful for quickly determining the class and expiration dates of users. The selection criteria are:

- User ID.
- Class.
- Last name.
- First name.
- Expiration Start and End dates.

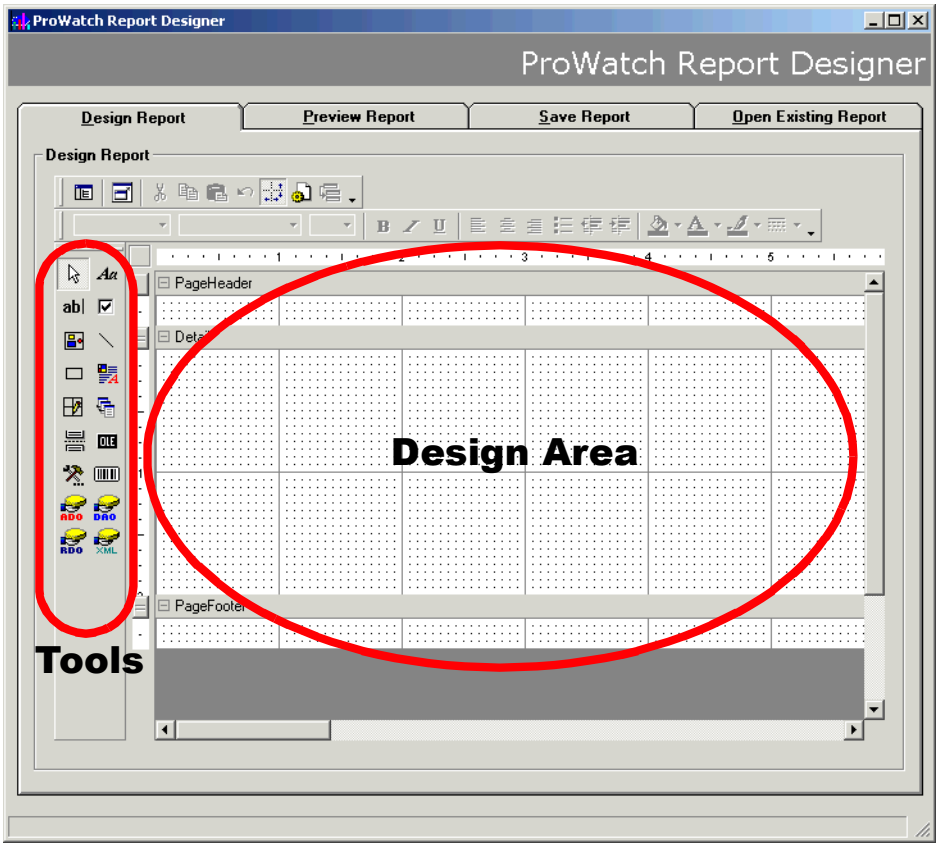
H.4 Report Designer

Pro-Watch allows you to design your own reports from scratch.

To launch the Pro-Watch Report Designer application, right-click the My Reports folder, and from the pop-up menu select Design New Report.

The Pro-Watch Report Designer screen appears:

Figure H-1 Report Designer Screen



H.4.1 Design Report Tab

The Design Report Tab is where you can draw each field that you want to see on your report, including the header and footer sections, by using the graphic and text tools provided on the left side of the screen:

The tool set includes an ActiveX Control, Barcode Control and OLE Object tools as well.

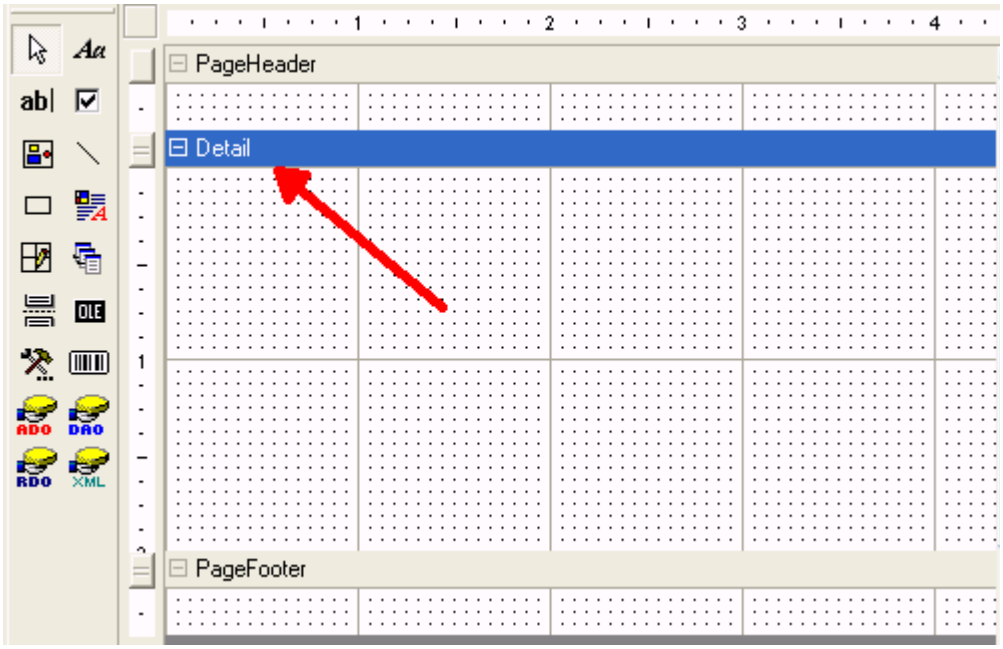
You can attach individual fields to your database by using one of the four database connection tools (ADO, DAO, RDO, XML) provided.

To design the header, main body and footer of your report, click the PageHeader, Detail, and PageFooter title bars, respectively. Then enter the

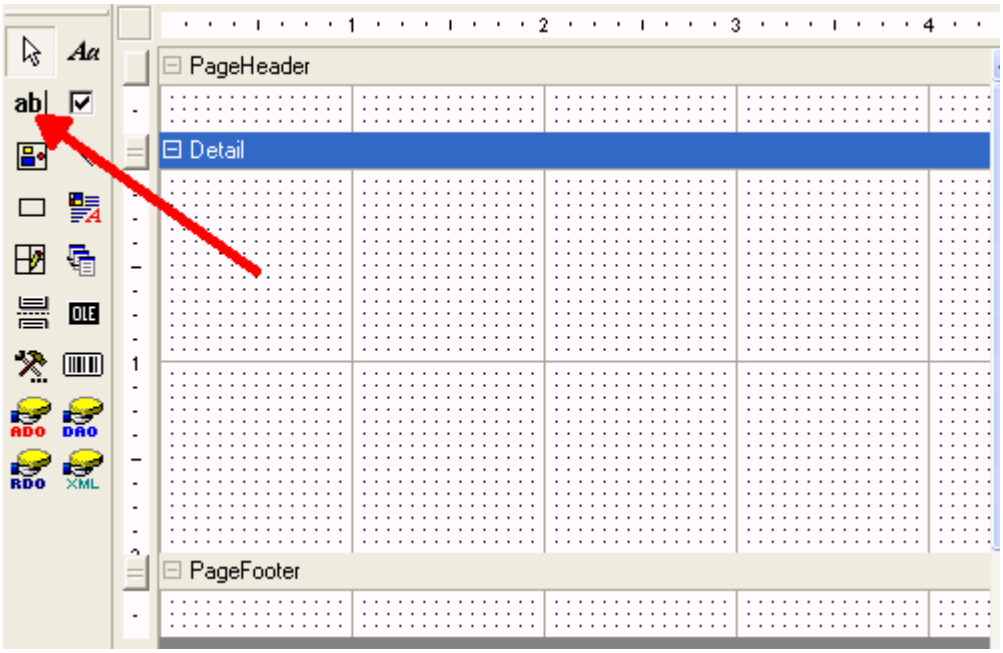
design elements you want by selecting the appropriate tools from the left pane.

For example, to include a text field in the main body of your report:

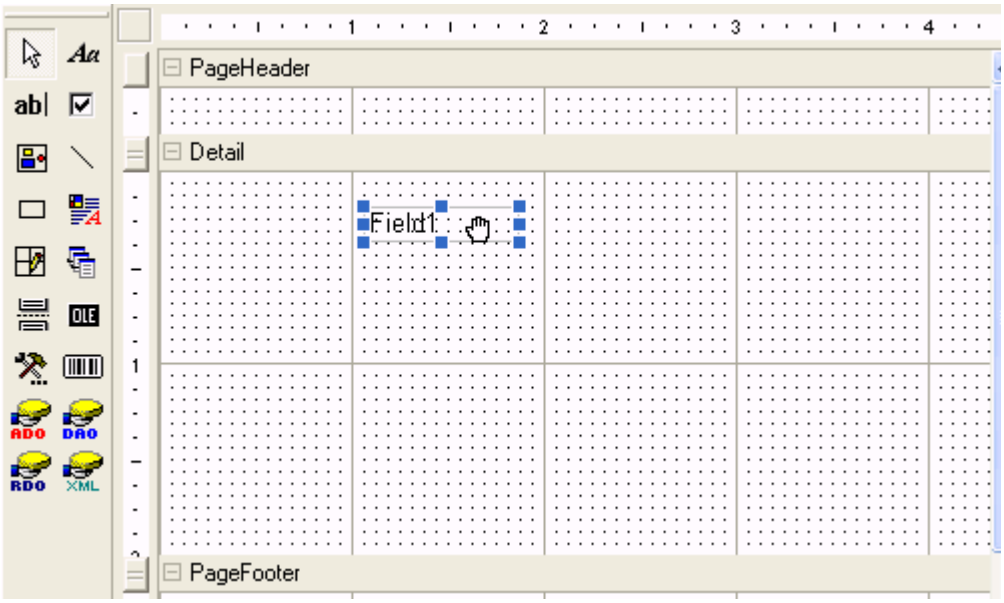
1. Click the **Detail** titlebar. The color of the bar will turn from gray to dark blue.



2. Click and select the **Textbox** tool (second from top-left).


PageHeader
Detail
PageFooter
ADO
DAO
RDO
XML

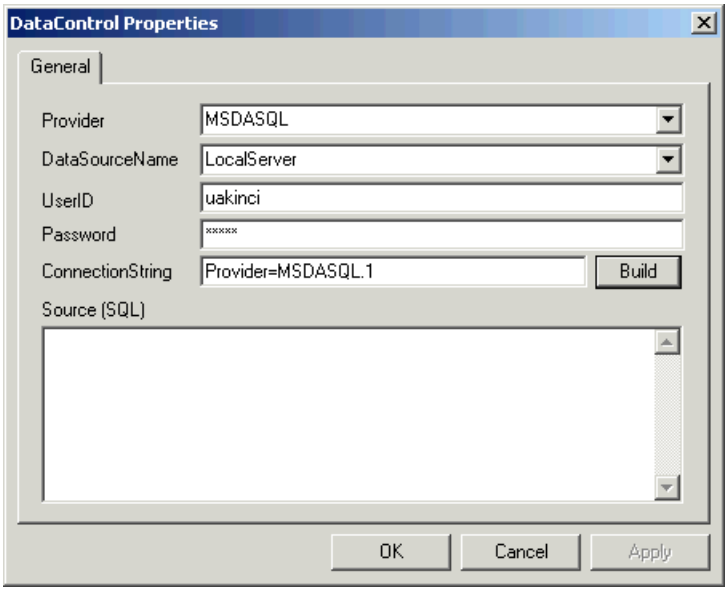
3. Click in the design area and drag to the desired size of the text field, which is automatically named Field1 (since it is the first field you have created). Click to drag the text field to the desired position.



Additional fields are automatically named Field2, Field3, etc. You can change everything about these fields, including their name, from the Property toolbox that you can access by right-clicking the field, and then selecting **Properties** from the pop-up menu.

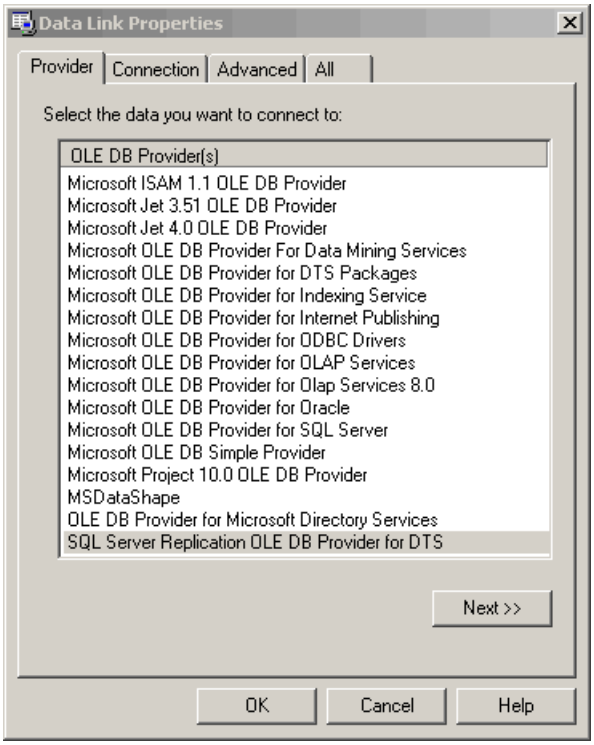
H.4.1.1 Connecting a database to the report:

1. Click and select a **database tool**, for example, the ADO Data Control Tool.
2. Click and drag the tool on the design area to create an ADO placeholder icon.
3. Right-click and select **Properties** from the pop-up menu to display the ADO properties dialog box:



4. Select a **Provider** from the drop-down menu.
5. Select the **name of your data source** from the DataSourceName drop-down menu.
6. Enter your **User ID**.
7. Enter your **Password**.

8. Build a data connection string by clicking on the **Build** button next to the ConnectionString field. Data Link Properties screen appears:



9. In the Provider tab, select the data you want to connect to.
10. In the Connection tab, enter:
    - Data source and location.
    - Any specific user name and/or password you need to access the data.
    - Any initial catalog that you may want to use.
11. Click the **Test Connection** button to make sure you have established a successful connection to the database.
12. In the Advanced tab, select any **Network Settings**, and/or enter a time-out value and select an access permission as appropriate.
13. In the All tab, edit any initialization property as appropriate through the following steps:
    - Select an initialization value from the list.
    - Click the **Edit Value** button to display the Edit Property Value dialog box.
    - Select the appropriate values in the Edit Property Value dialog box.
    - Click the **Reset Value** button.
14. Click **OK** to close the Data Link Properties screen and return to the Properties screen.
15. Click **Apply**.

16. Click **OK** to close the Properties screen.

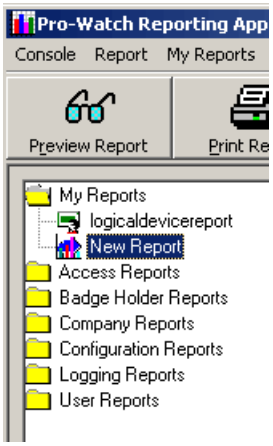
H.4.2 Preview Report Tab

Click this tab to preview the finished form of your report.

H.4.3 Save Report Tab

To save your report, follow these steps:

1. Enter a **Report Name**.
2. Click either the **Add for User** or the **Add for Class** radio-button.
3. Click either the **File** or **Database** radio-button to select a Destination.
4. Enter a **Report Description** if you'd like to.
5. Click **Save** to save the new report and have it listed in the My Reports directory:



H.4.4 Open Existing Report Tab

To open an existing report, follow these steps:

1. Click either the **File** or **Database** radio-button to select a Report Source.
2. Select a report from the list at the bottom of the screen.
3. Click **Open**.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Pro-Watch Biometric Service

In this appendix ...

Overview
Pro-Watch/Morpho Process Diagram
Pro-Watch/Morpho Biometrics Setup
General Notes
Pro-Watch Advanced Badging
Morpho Reader Network Configuration
Pro-Watch/Morpho Template Download Windows Service
DESFire Smart Card Key Management
Morpho Reader Smart Card Key Management
Pro-Watch Panel Configuration
Version Information
Required Licensing
Included Morpho Documentation & Software
Add Biometric Field to Pro-Watch Advanced Badging
Morpho Indoor 500 Series Reader
Morpho Outdoor 500 Series Reader
MSO300 Finger Enroller
MorphoWave Reader

I.1 Overview

This document describes the integration between Pro-Watch Access Control and Morpho biometric readers.

This document applies for storing templates in the Morpho readers (1-to-many matching) and/or storing the templates on a DESFire smart card (1-to-1 matching).

Biometric templates stored in the Morpho readers require a TCP/IP connection to every reader. Templates are downloaded to the readers via a Windows service as cards are granted and revoked access to the readers in Pro-Watch Advanced Badging.

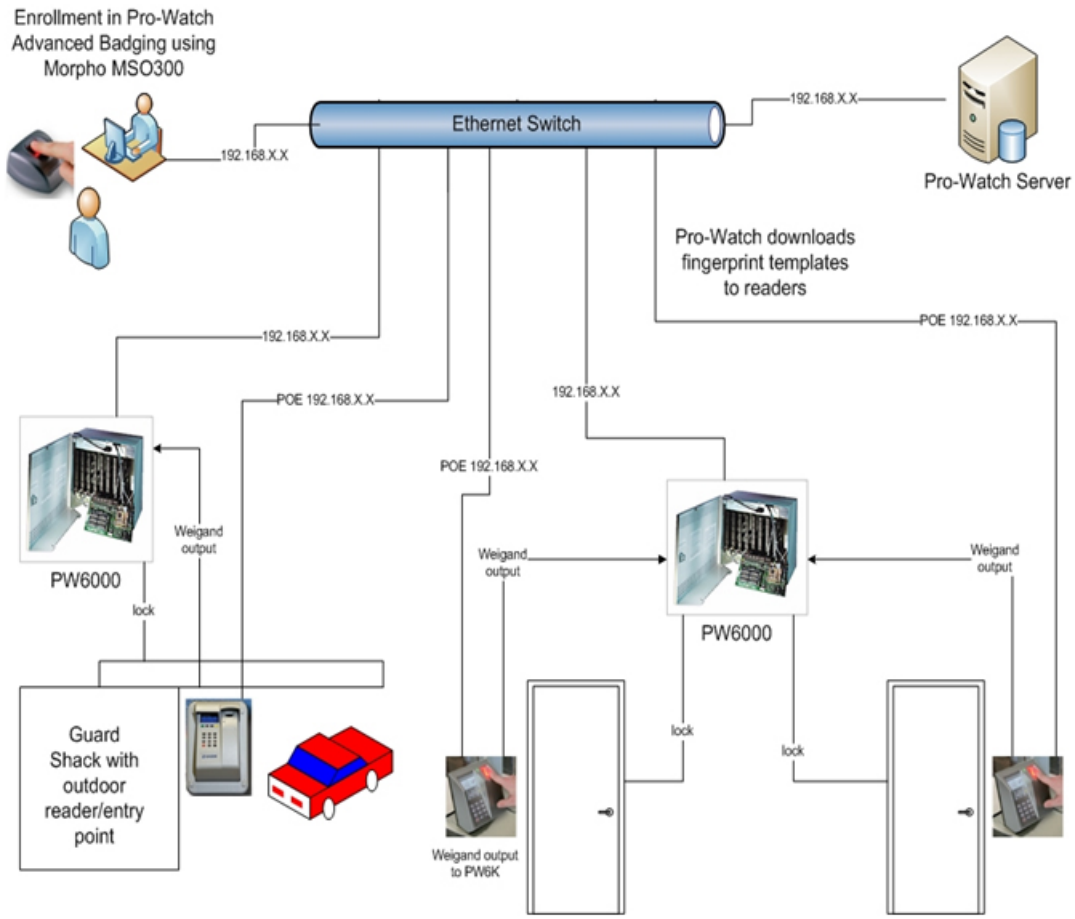
Biometrics stored on a DESFire card are encoded to the smart card using a contactless smart card encoder. The DESFire cards are secured using secret keys encoded to the smart card and those same keys are stored in the Morpho readers for validation.

Note: Advanced Badging UI operations making card inactive turns the Wave reader to go idle and reader does not come back to active mode until the user touches LCD.

I.2 Pro-Watch/Morpho Process Diagram

This graphic applies to storing fingerprint templates in the Morpho readers via TCP/IP. For templates stored on a DESFire smart card, there is no need for a TCP/IP connection from the server to the readers.

Figure I-1 Pro-Watch/Morpho Process Diagram



I.3 Pro-Watch/Morpho Biometrics Setup

Recommended steps to begin using Biometrics:

1. Advance Badging Installation

   a. Go to the **Program Files** on your local disk (C:). Select **Pro-Watch > Advanced Badging > Morpho > MorphoLicense** subdirectory. Run the **SagemSecurite_License_Protection_Installer.msi.** This installs the Morpho licensing software. The Morpho licenses are stored in the MSO300 enroller.

   b. In the same Morpho subdirectory (see the above step), install the 32 or 64 bit USB driver for the MSO300 enroller.

   c. Plug in the MSO300 finger enroller. Go to **Start > All Programs > Sagem Sécurité Licence Management 4.3.1** and then run **Sagem Sécurité Licence Manager 4.3.1**. You should see a VERIF license to enrollment fingerprints.

   d. **TROUBLESHOOTING:** If you do not see the license information display in Windows Services, try stopping the **Sagem License Service** and **Sagem MorphoSmart Service Provider Usb Server**. Then, in the following order, start the **Sagem MorphoSmart Service Provider Usb Server** and then the **Sagem License Service**.

2. Enrollment

   a. Add six new badge fields in Pro-Watch:

   - Two blobs fields to store the enrolled templates
   - Two dropdowns fields for enrolled finger text, and
   - Two short fields for enrolled finger scores. Make the enrolled finger text and finger score fields read-only in Pro-Watch Badge Builder.

     Drop down values for finger text are: Left Index, Left Middle, Left Pinky, Left Ring, Left Thumb, Right Index, Right Middle, Right Pinky, Right Ring, Right Thumb.

   b. In Pro-Watch Badge Builder, add the six new badge fields to a badging profile and tab page. Finger field drop down and finger score fields should be read-only.

   c. **Restart Pro-Watch Advanced Badging** and now you should see the **Biometric Settings** module.

   d. In the **Biometric Settings** module, setup the **Morpho Configuration and Morpho Fingerprint Configuration tabs** and save.

   e. **Start the Pro-Watch Advanced Badging profile** that the six badge fields were added to and edit a badge. Click on the first biometric and the Morpho MSO300 enrollment screen should display.

f. Enroll the fingerprint and then enroll the second fingerprint.

3. Determine how biometrics will be used. Will it be TCP/IP based fingerprint templates stored in the readers for a one-to-many match, or will it be fingerprint templates written to a DESFire smart card (no need for TCP/IP) for a one-to-one match. It can also be a combination of both modes.

4. **For Templates stored in the Reader. 1-to-Many Matching**

   a. In the Biometrics Setting module, select the **Morpho Configuration tab**. Select either

   - Download Biometric Template to Reader, or
   - Non Database Smart Card Biometric encoding -- iClass..

   b. **Morpho Configuration tab**.

      a. The **Daily Full Load Time** is the once-a-day or once-a-week time when all readers will be refreshed with Pro-Watch with the current card holder access.

      b. The **Daily Date/Time Synchronization** value is the once a day time when all readers clocks will be synchronized.

   c. In **Biometric Terminals** tab, all readers that will store templates in the reader need to be entered as terminals. Associate the Pro-Watch logical device to the TCP/IP address of the reader. Validate readers as they are added so it looks like the readers are getting downloaded properly.

   d. In the Advanced Badging installation directory, run the **Install_PW_Morpho_Service.bat** file. This will install the Pro-Watch Morpho Service in Windows Services. Make sure after running the Install_PW_Morpho_Service.bat file, you see commit phase completed successfully.

   e. Edit the **PWMorphoService.exe.config** file and set the ProWatchDatabaseServer and ProWatchDatabase settings.

   f. Go to **Windows Services** and check the credentials of the service. Make sure the credentials have access to the Pro-Watch SQL Server database. Run the service.

   g. In **Advanced Badging**, give access to the reader either through a clearance code or a logical device exception. Looking at the reader, in 10 seconds or less, you should see the template get downloaded to the reader.

5. **Templates stored on a DESFire smart card. 1-to-1 Matching**

These steps are for a first time brand new installation.

Note: Morpho biometric and card data is written to the smart card and secured with DESFire keys. In order to write biometrics to the smart card, a DESFire encoder is required. A USB Omnikey 5x21 encoder is the

recommended encoder to use. If printing and encoding smart cards is a requirement, the Magicard Prima4 is required with the Omnikey encoder. If using Windows 7, there may be issues with Windows and the smart card certificates, so turn off the 'Certificate Propagation' Windows service.

h. In the **Biometric Settings** module, select the **Morpho Configuration tab**. Select either

- Download Biometric Templates to Reader, or
- Non Database Smart Card Biometric Encoding -- iClass.

Note: Morpho allows three keys (16 bytes each) to be used to secure the card, the card master key, an application read/write key and an application read key. If the smart card will be used by other applications, do not change the card master key (recommended). This is the default for Pro-Watch Advanced Badging and the Morpho reader. At a minimum, the application keys need to be set.

i. To change the keys that will be written to the card by the Pro-Watch Advanced Badging application click the **Change Smart Card Encryption Keys button**. This should only be done once. Select the first-time check box and enter key values (16 hex bytes) for the application read/write and read keys.

j. Click the **Save** button to save the keys and encrypt them in the database.

k. Now, set the same keys for the reader by making a **Reader Admin Card**. The Reader Admin Card will encode the encryption keys to the reader. This is a one-time only process for each reader, so the one admin card can flash all the readers, but you cannot use the same card to flash the same reader more than once. A blank DESFire card and an encoder is required to make an **Admin Card**.

l. Click the **Create Reader Admin Card button** and if the reader is right out of the box, check the **New Reader check box**. Enter your encryption keys for the application read/write and read keys.

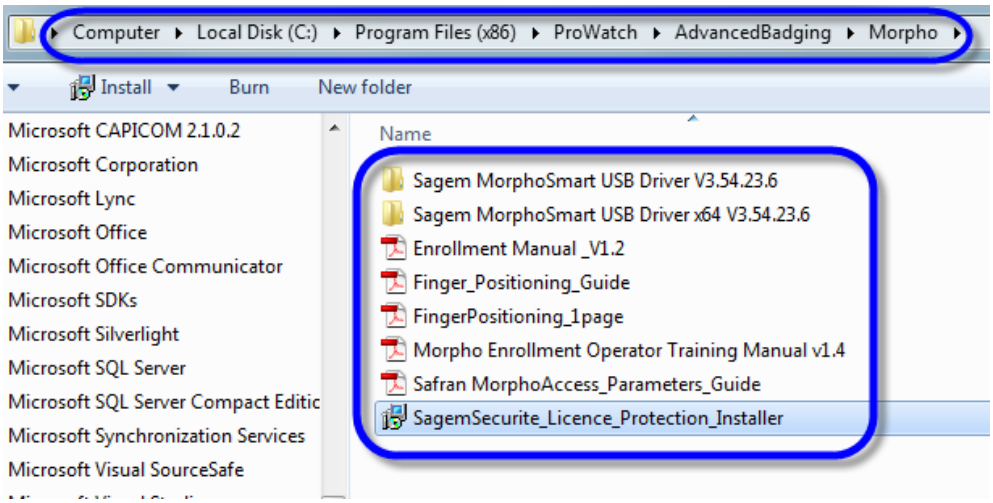
m. Make sure your encoder is set in the **Console**, **Options** settings. Place DESFire card on Omnikey encoder and click the **Encode Admin Card button**.

n. Take card to brand new/factory reset reader and place card up to reader. The reader will beep several times and be finished.

o. Create a smart card in Pro-Advanced Badging and test the card.

I.4 General Notes

Note 1: The Morpho license software, MSO300 USB driver and enrollment documentation is located in a folder called Morpho below the Pro-Watch Advanced Badging installation directory:

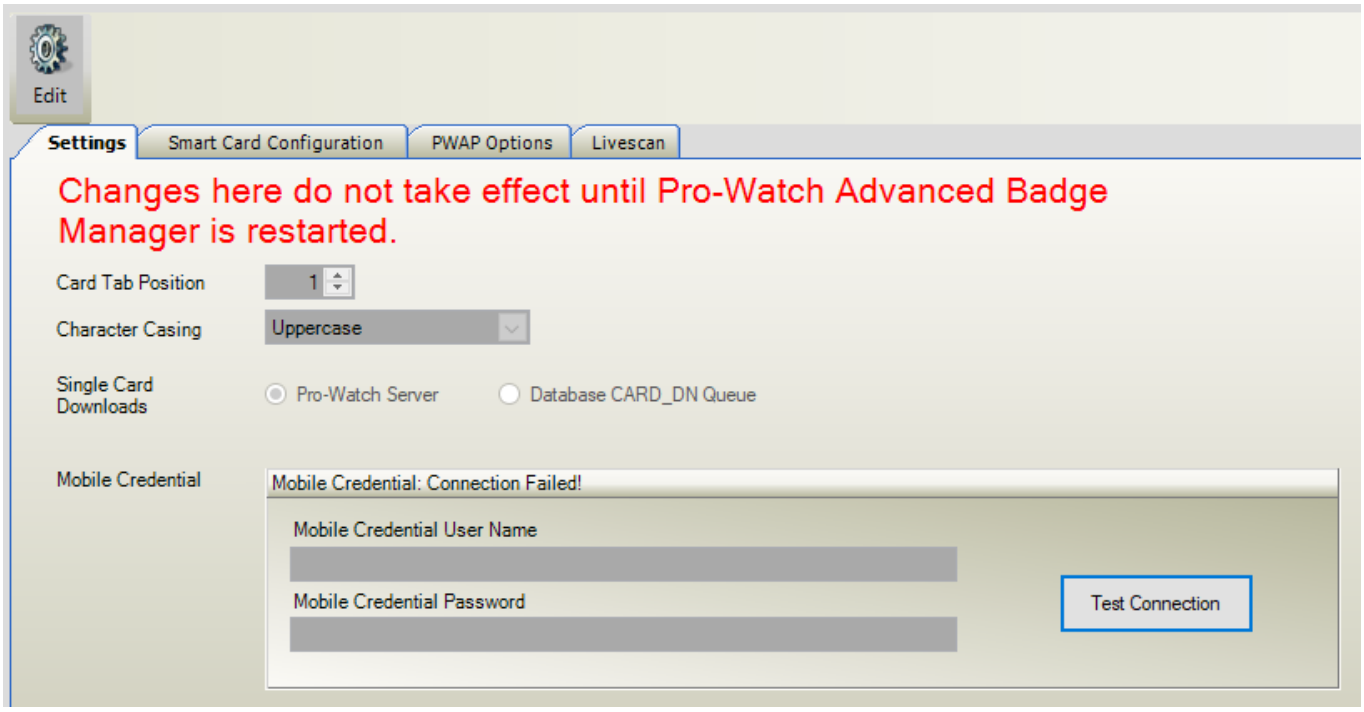


I.5 Pro-Watch Advanced Badging

I.5.1 Enabling Morpho Biometrics

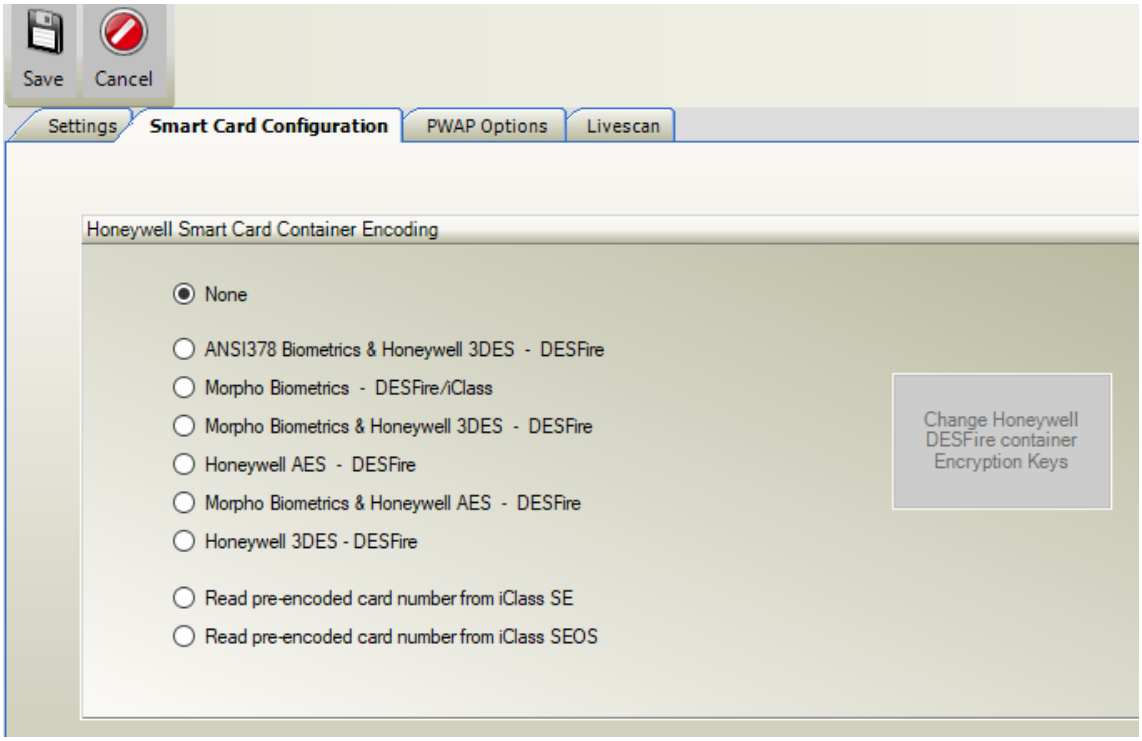
To enable Pro-Watch/Morpho biometrics:

1. Click **Badging** in the left navigation pane and launch the **Advanced Badging** module. If you're not in Advanced Badging, see Opening Multiple Instances of Advanced Badging, page 2-95
2. Click the **Application Settings** link in the left navigation pane to display the screen below:

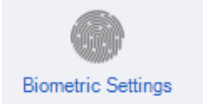


3. Click **Edit**.

4. Select the **Smart Card Configuration** tab:



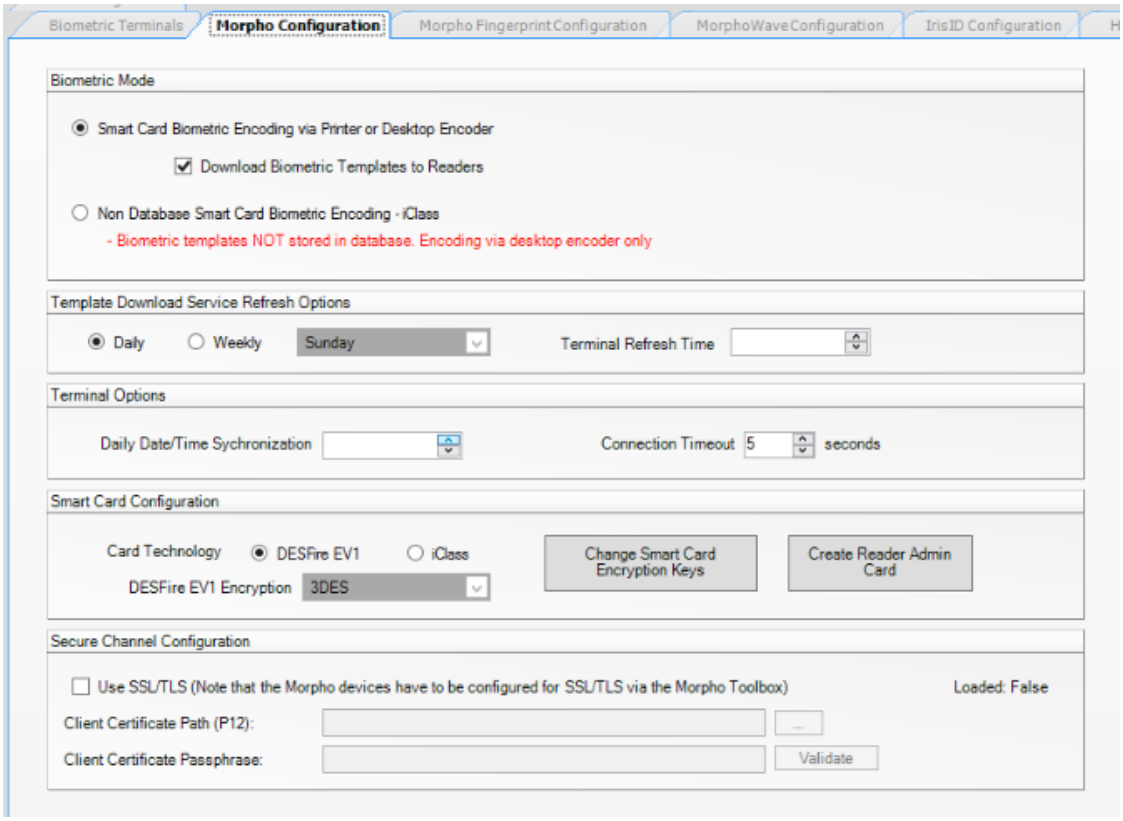
5. Select the 3rd, 4th, or 6th radio button.
6. Click **Save**.
7. **Close** and **re-start** the Advanced Badging module. Now the navigation pane will display the **Biometric Settings** icon and link:



Note: The **Application Settings** link and module displays only for users who are in the Pro-Watch Root class

I.5.2 Morpho Template Configuration

1. Click the **Biometrics Settings** icon in the left navigation pane to display the below screen:



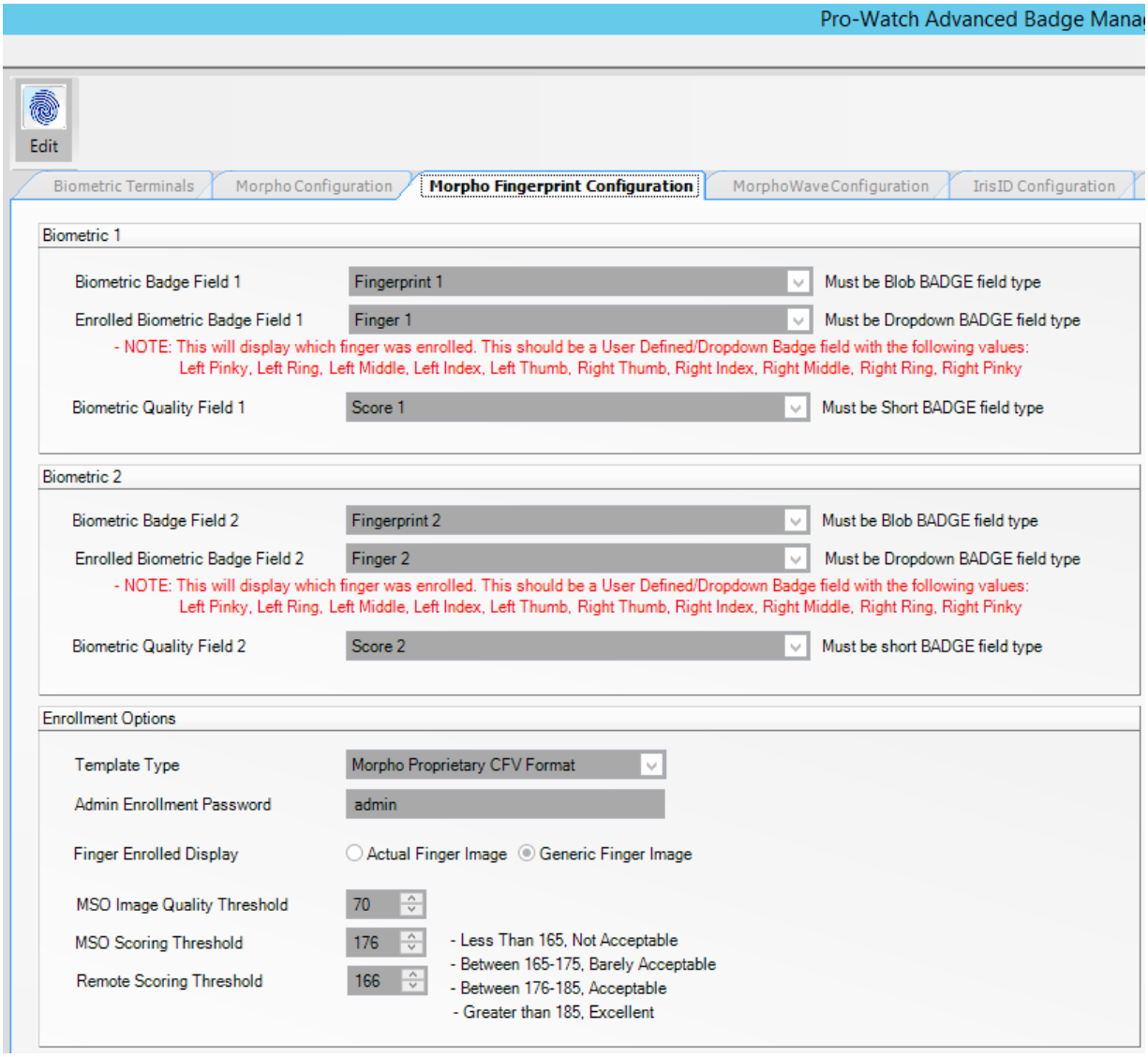
2. Click and select the **Morpho Configuration tab**. Morpho templates are stored at the reader or on the DESFire smart card, or both.

Field Name	Description
Smart Card Biometric Encoding via Printer or Desktop Encoder	Select this option button when biometric templates will only be stored in the smart card. Templates will not be store in the reader.
Download Biometric Templates to Readers	Select this option button when biometric templates will be downloaded and stored to the Morpho readers. Templates will not be stored on a smart card.

Non-database Smart Card Biometric Encoding	Select this option button when storing biometric templates to a smart card. Templates will be downloaded and stored in the Morpho readers.
Template Download Service	This applies to templates stored in the reader. Once a day or weekly, all Morpho readers are refreshed with the Pro-Watch database to make sure the templates and badge data in the Morpho reader is accurate with the correct badge holders who have access to the reader in Pro-Watch.
Daily Date/Time Synchronization	This applies to templates stored in the reader. Once a day, all Morpho readers are refreshed with the date/time from the Pro-Watch server.
Smart Card Configuration	This is for templates stored on a smart card. Currently only the smart card encryption is supported when programming to the smart card.
Change Smart Card Encryption Keys	Use this option to change the encryption keys that will be written to the smart card. This should be a one-time only use. These are the keys that secure each smart card. These keys are encrypted and stored in the Pro-Watch database.
Create Reader Admin Card	Use this option to create an admin card to program the Morpho readers. The keys written to the admin card need to be the same keys written to the smart card.

I.5.3 Morpho Fingerprint Configuration

Click and select the Morpho Fingerprint Configuration tab to configure fingerprint enrollment and badging parameters. Two fingers must be enrolled for a valid biometric template to be downloaded to the Morpho readers or stored on a DESFire card. To enroll two fingers, six badge fields must be created to store the fingerprint image/ templates, the enrolled finger text and the enrolled finger quality. See Add Biometric Field to Pro-Watch Advanced Badging, page I-33 to create badge fields.



Field Name	Description
Biometric Badge Field 1	This is the first Pro-Watch Blob badge field used to enroll one of the biometric fingers in the Badging module. See section titled Add Biometric Field to Pro-Watch Advanced Badging, page I-33 to create badge field.
Biometric Badge Field 2	This is the second Pro-Watch Blob badge field used to enroll one of the biometric fingers in the Badging module. See section titled Add Biometric Field to Pro-Watch Advanced Badging, page I-33 to create badge field.
Enrolled Biometric Badge Field 1	This drop-down badge field is auto filled after a finger is enrolled with the selected finger that was enrolled. Valid values are: Left Pinky, Left Ring, Left Middle, Left Index, left Thumb, Right Thumb, Right Index, Right Middle, Right Ring and Right Thumb.
Enrolled Biometric Badge Field 2	This drop-down badge field is auto filled after a finger is enrolled with the selected finger that was enrolled. Valid values are: Left Pinky, Left Ring, Left Middle, Left Index, left Thumb, Right Thumb, Right Index, Right Middle, Right Ring and Right Thumb.
Biometric Quality Field 1	This short badge field is auto filled with quality score of the enrolled finger.
Biometric Quality Field 2	This field will be auto filled with quality score of the enrolled finger. This must be a Pro-Watch short badge field.
Template Type	This is the type of biometric template created during the enrollment process. Morpho Proprietary CFV: This is the default Morpho proprietary template format. ANSI INCITS378: This is an international standardized template format. This format can be used with other manufacturer readers, but the matching and verification quality will not be as good as the Morpho format.
Admin Enrollment Password	This is the password to be used by an Admin to allow enrollment settings to be changed. This functionality will typically be used for troublesome enrollments.
Finger Enrolled Display	This is the image of the finger in badging. You can store the actual picture of the finger or a fake image of the finger.

Default Image Quality Threshold	This is the default image quality used to determine acceptance of an enrolled fingerprint. This setting can be lowered by and admin user during enrollment to accept poor quality fingerprints.
Default Scoring Threshold	This is the default fingerprint template quality score. The enrollment process scores the captured fingerprint template and compares the captured template score with this value. If the captured fingerprint template score is below this value, the prints must be re-enrolled. If template score is less than 165, the template is not acceptable and the finger must be re-enrolled. If the score is between 165-175, the template is barely acceptable. Anything greater than 176 is acceptable. The greater the scoring threshold, the better the overall biometric verification will be at the readers.

I.5.4 MSO300 Biometric Enrollment

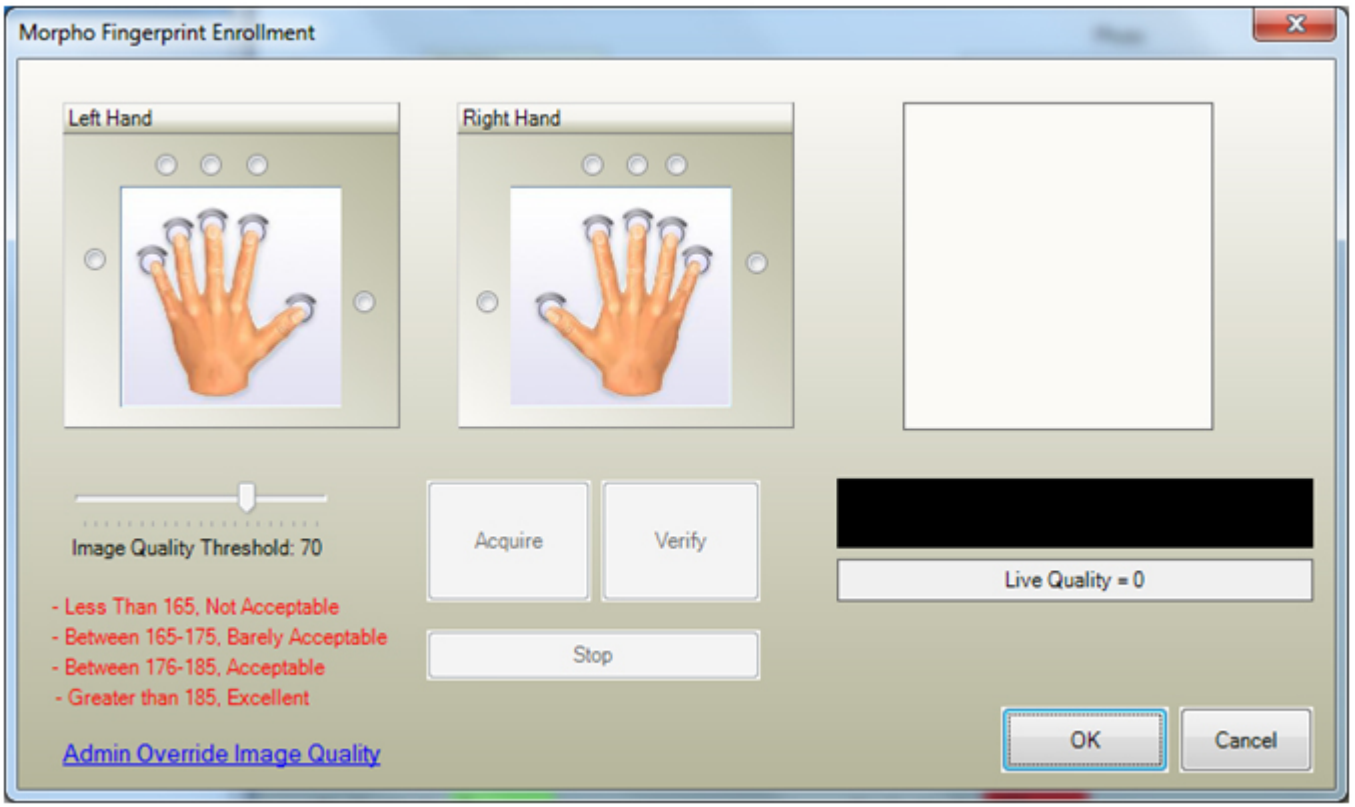
From the Badging module, badge holders are enrolled one finger at a time by clicking on a biometric enrollment field. To enroll a fingerprint, select the radio button of the finger to enroll and then click the Acquire button.

During the acquisition process, the badge holder will have to place and remove their finger on the MSO300 three times. Enrolling the finger three times, using the fingerprint and placement, allows the process to generate a template of the badge holder for better verification in the field.

Note: See Add Biometric Field to Pro-Watch Advanced Badging, page I-33 to create badge field.



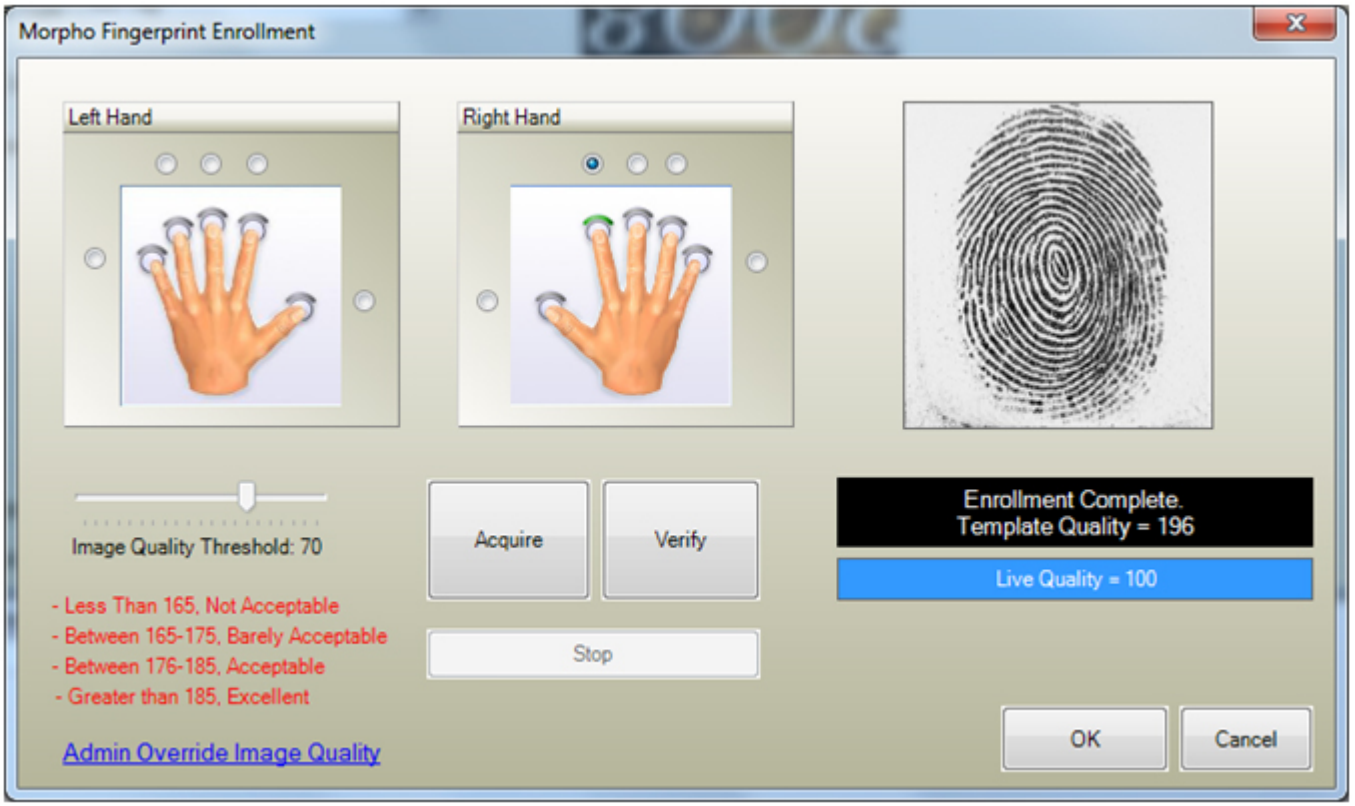
I.5.4.1 Start of Enrollment



Field Name	Description
Left Hand	If enrolling a finger on the left hand, select the appropriate finger radio button.
Right Hand	If enrolling a finger on the right hand, select the appropriate finger radio button.
Image Quality Threshold	This is the image quality value that must be met in order for the acquisition of the finger to be completed. This slider is disabled and can be enabled by selecting the Admin Override Image Quality button. A password must be entered to override the image quality. Use this slider for fingerprints that are difficult to capture.
Acquire	Start the acquire process of capturing and removing the finger three times.
Verify	Start the verification process of the captured fingerprint.

Stop	Stop the acquisition or verification process
Enrollment Status (Black Control)	This is the real time status of the enrollment process. During enrollment, the status will inform the badge holder when to place their finger on the MSO300 enroller and when the remove it. When the enrollment is complete, the template quality score will display.
Live Quality	This is the image quality score. The operator can use this value to tell the badge holder to move the finger or rotate it or press harder or press less.
Admin Override Image Quality	Use this when having difficulty getting fingerprints that have a quality that is equal or greater than the Image Quality Threshold. Select this to enable the Image Quality Slider to lower the quality of prints enrolled.
OK	Save the fingerprint.
Cancel	Do not save the fingerprint.

I.5.4.2 End of Enrollment



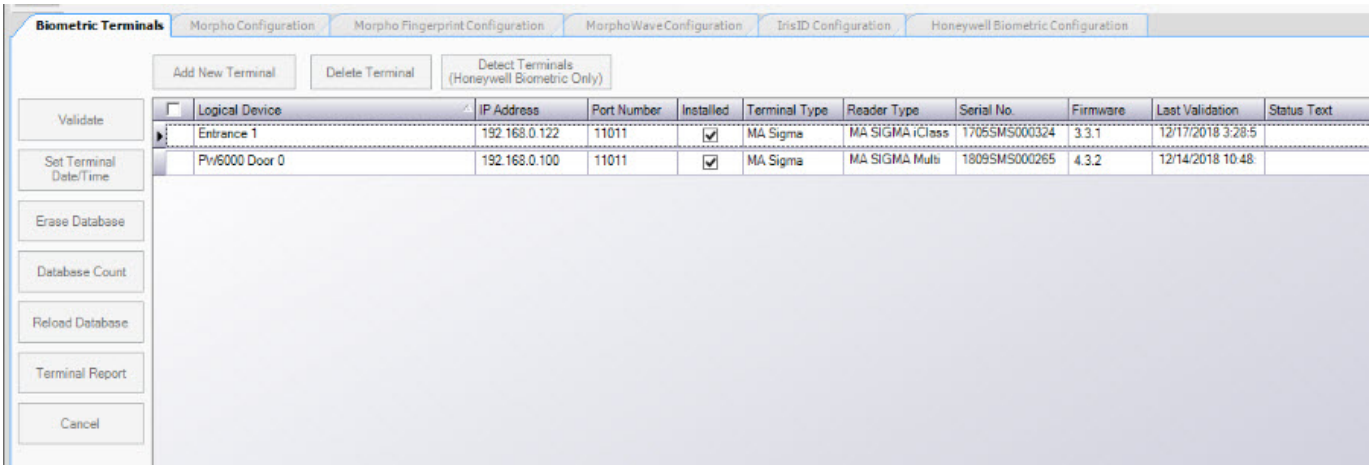
I.5.4.3 Enrollment Troubleshooting

Error Message/Problem	Tip
Morpho MSO300 Enrollment device not found.	Make sure the MSO300 is USB connected and the 'Sagem License Service' is running and the 'Sagem MorphoSmart Service Provider Usb Server'.
Finger X and X do not match.	When the finger is placed on the MSO300 enroller three times, one of the fingers did not match one of the other fingers. Re-enroll.
Score is too low. Score [XXX] must be greater than threshold [176].	The template quality score is below the threshold set in the Morpho system configuration. Try re-enrolling the fingerprints to get a score above the default value. The default value is set in the Morpho configuration screens.
Can't enroll fingerprint because of poor quality.	Try numerous times and if all else fails, lower the image quality value. See Morpho enrollment manuals located in the morpho directory below the Advanced Badging install directory. These manuals will help with difficult prints.
Acquisition Time Out	The enroller did not detect a finger in a sufficient amount of time.

I.6 Morpho Reader Network Configuration

Sometimes the templates are stored in the reader and not on a DESFire card. Use this screen to associate a Morpho reader to a Pro-Watch Logical device as well as assign an IP address to the Morpho reader so that the fingerprint templates can be downloaded over TCP/IP. All command actions can be done on all readers or individual readers.

Note: This screen only needs to be populated if templates are to be downloaded and stored in the reader.

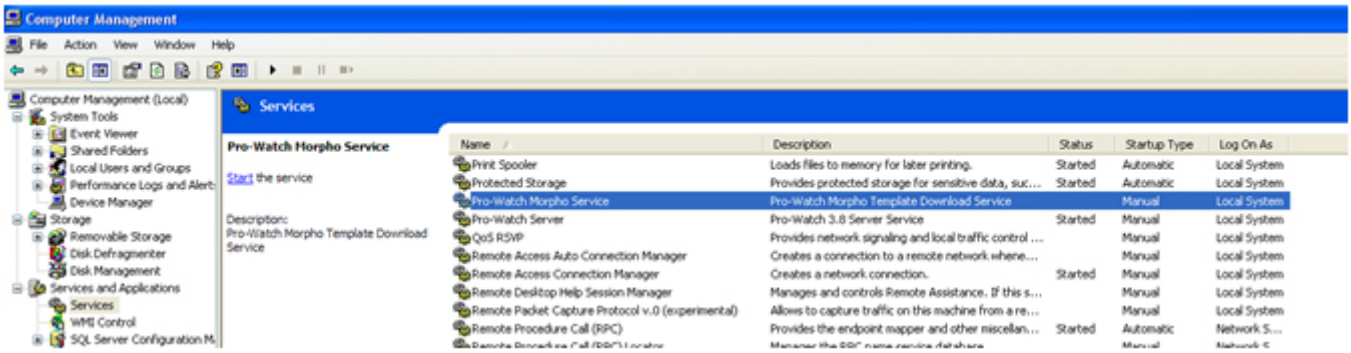


Button Action	Description
Validate	This command validates the terminal IP address. Upon successful validation, the terminal type, serial number, firmware and last validation date will be updated.
Set Terminal Date/Time	This command sets the date and time for the terminal.
Erase Database	This command resets the terminal and wipes out any templates stored in the terminal. After this command no one can use this reader.
Database Count	This command will display the number of records in the Morpho reader.
Reload Database	This command will re-load all templates from the Pro-Watch database that should be loaded to this reader.
Terminal Report	This command will list the Card Numbers and Name of the cards that are in the selected Morpho reader.
Cancel	This command cancels a command in progress.

I.7 Pro-Watch/Morpho Template Download Windows Service

A separate Windows service downloads biometric templates to the Morpho readers via TCP/IP. The service will poll a download queue every X-number of seconds and then download the templates to the readers. Every 24 hours, this service will do a reset and full download of templates to all the readers.

Note: The **Download Templates to Morpho Readers** check-box must be selected in the Morpho Biometrics module



I.7.1 Pro-Watch/Morpho Windows Service Configuration

```
<appSettings>
  <add key="ProWatchDatabaseServer" value="PWServer"/>
  <add key="ProWatchDatabase" value="PWNT"/>
  <add key="LogLevel" value="2"/>
  <add key="DownloadQueueInterval" value="10"/>
  <add key="DownloadThreads" value="5"/>
 </appSettings>
```

Key	Description
ProWatchDatabaseServer	The Pro-Watch database server
ProWatchDatabase	There Pro-Watch database name

LogLevel	Log Nothing = 0 Log Errors = 1 Log Everything = 2 **Note:** All logging goes to database table SAGEM_LOG
DownloadQueueInterval	This is the number of seconds the service will look in the SAGEM_DOWNLOAD table for records to download to a reader.
DownloadThreads	This is the number of threads used to download data to the Morpho readers at the same time. If set to 5, this means there are 5 processes sending data to the terminals. One process per terminal. When one process finishes with a terminal it moves on to the next terminal to download.

I.7.2 Pro-Watch/Morpho Windows Service Installation

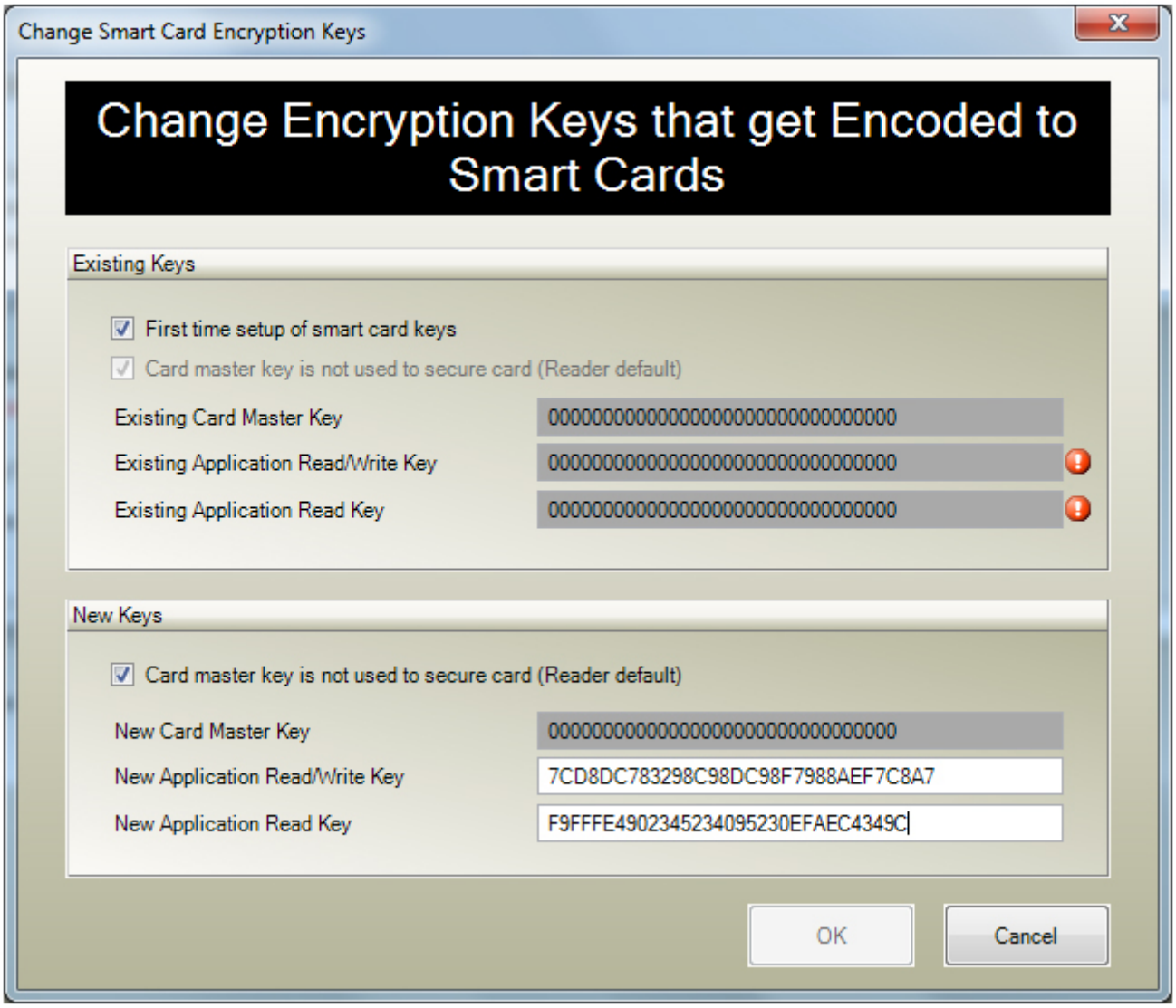
To install the windows service, execute the Install_PW_Morpho_Service.bat file

To uninstall the windows service, execute the Uninstall_PW_Morpho_Service.bat file

I.8 DESFire Smart Card Key Management

To secure DESFire smart cards with encryption keys, use the functionality below from the Morpho Configuration module.

This screen will save the encryption keys to the database for the encoding and printing of smart cards. Keys are encrypted to the Pro-Watch database.



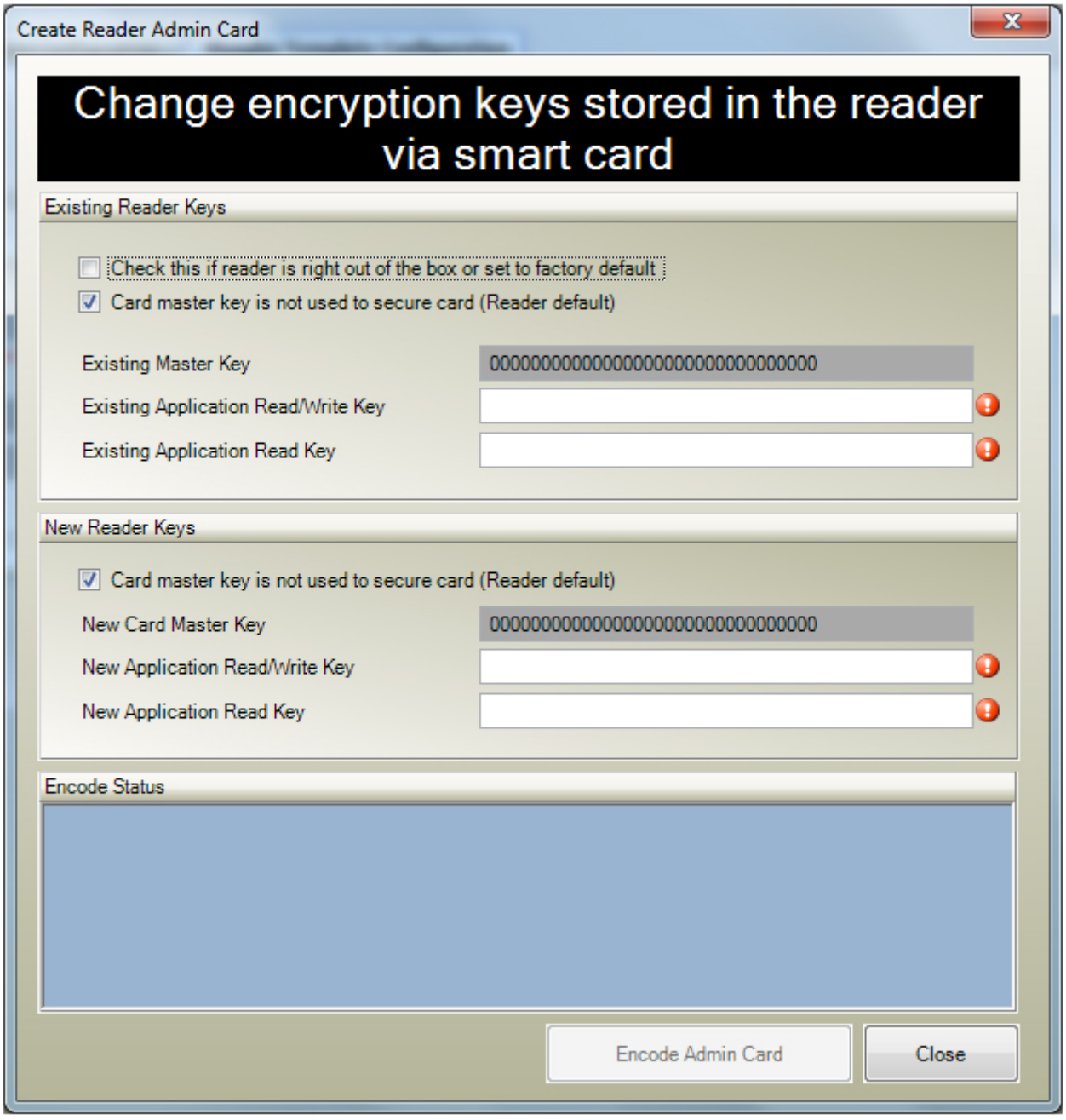
Field Name	Description
First time setup of smart card keys	If this is the first time encryption keys are setup, check this box as it will set the default existing keys to all zeros.
Card master key is not used to secure card	Check this box if the DESFire master key will not be encrypted and is used by other applications. This is the default for the Morpho reader. Warning: If the card master key is changed and secured, the multi-applicative mode in the reader must be modified. See reader documention.
Existing Card Master Key	This is the existing master key that secures the card.
Existing Application Read/Write Key	This is the existing encryption read/write key that secures the Morpho data on the DESFire card.
Existing Application Read Key	This is the existing encryption read key that secures the Morpho data on the DESFire card.
New Card Master Key	This is the new master key that secures the card.
New Application Read/Write Key	This is the new encryption read/write key that secures the Morpho data on the DESFire card.
New Application Read Key	This is the new encryption read key that secures the Morpho data on the DESFire card.

I.9 Morpho Reader Smart Card Key Management

To set the encryption keys for the Morpho readers, an Admin Card must be created. An Admin Card is a DESFire card that replaces existing encryption keys with new encryption keys.

An Admin Card works one-time for each reader, but can be used on multiple readers.

To create an Admin Card, enter in the existing and new keys, create the DEFire card and then hold the card to a reader. The reader will beep numerous times indicating the reader has the new keys.



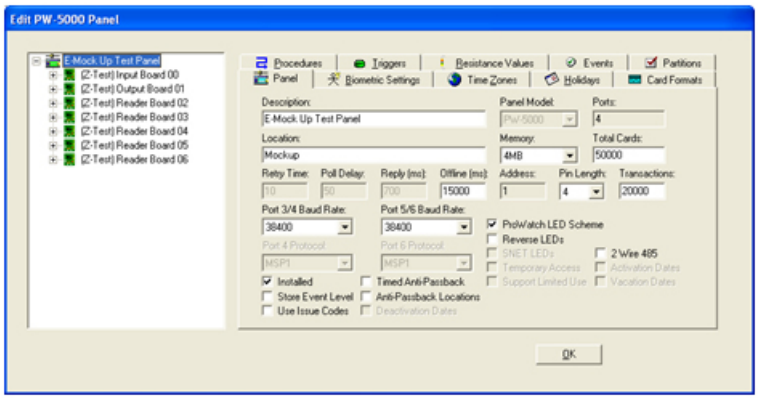
Field Name	Description
New or Factory Default	Check this if it is a new reader or the reader has been reset to its factory default settings.

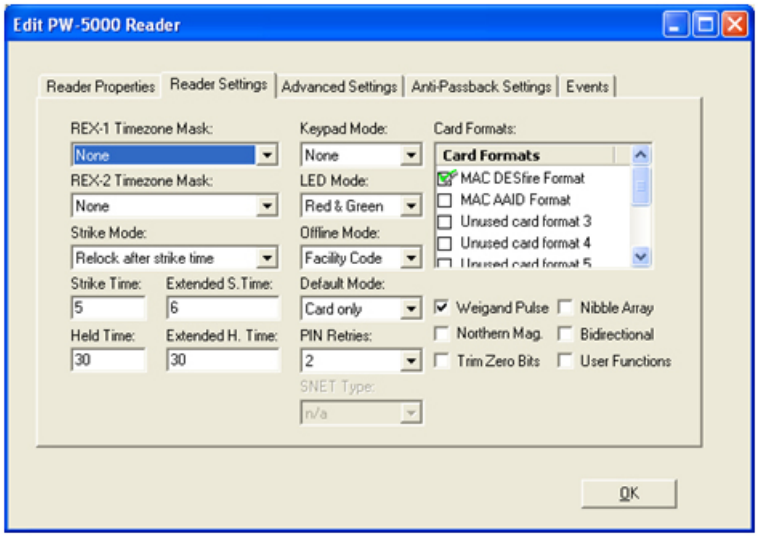
Card master key is not used to secure card	Check this box if the DESFire master key will not be encrypted and is used by other applications. This is the default for the Morpho reader. Warning: If the card master key is changed and secured, the multi-applicative mode in the reader must be modified. See reader documention.
Existing Card Master Key	This is the existing master key that is used to read the card.
Existing Application Read/Write Key	This is the existing encryption read/write key that is used to read/write the Morpho data on the DESFire card.
Existing Application Read Key	This is the existing encryption read key that is used to read the Morpho data on the DESFire card.
New Card Master Key	This is the new master key that will be used to read the DESFire card.
New Application Read/Write Key	This is the new encryption read/write key that will be used to read/write the DESFire card.
New Application Read Key	This is the new encryption read key that will be used to read the DESFire card.
Encode Admin Card	Using a new DESFire card, this will encode a new Admin card with the keys entered. Make sure encoder is set in the drop down menus, Console, Options.

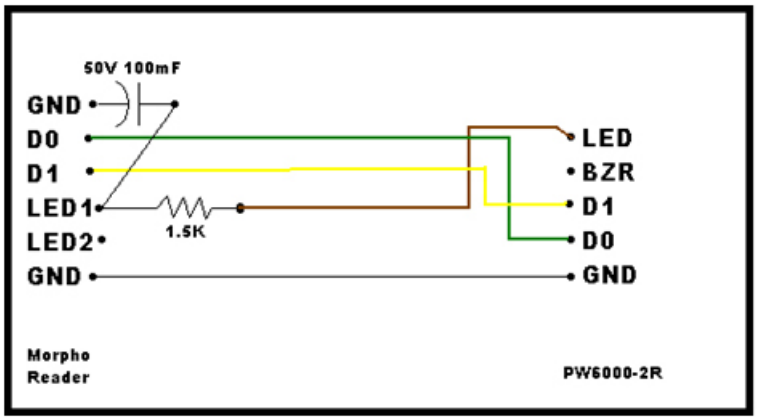
I.10 Pro-Watch Panel Configuration

To get the Pro-Watch 6000 panel to give a valid denial when access is denied, add a 1.5K ohm resistor and 100microfarad capacitor to filter out the brief LED pulse that the Pro-Watch board sends even on an Access Denied.

Usage: Especially with smart cards, the Morpho reader validates the fingerprint, but the user does not have access to the door, the reader needs to give an access denied.






50V 100mF
GND
D0
D1
LED1
LED2
GND
1.5K
LED
BZR
D1
D0
GND
Morpho
Reader
PW6000-2R

I.11 Version Information

- Pro-Watch 4.5
- MorphoKit 5.13.0
- Microsoft .NET 4.5 and .NET 2.0
- MACI Version 6.1.13

I.12 Required Licensing

The following licensing is required for a Pro-Watch/Morpho Biometric solution

- License to run Pro-Watch
- License to run Pro-Watch Advanced Badging with Biometrics and Smart Cards enabled
- A 'VERIF' license from Morpho to enroll fingerprints. This license will be embedded in the MSO300 enroller device
- If 'Pro-Watch Morpho Template Download Service' runs on the enrollment station, the 'MACI' license can be embedded in the MSO300 enroller. If the 'Pro-Watch Morpho Template Download Service' will run on the Pro-Watsch server, then a USB dongle license must be on the server.

I.13 Included Morpho Documentation & Software

This documentation and installers are located in the 'morpho' directory under the AdvancedBadging install directory.

Documentation/Software	Description
Enrollment Manual v1.2	This manual is intended to provide information and assistance to anyone who is involved in the capturing of fingerprint templates (fingerprint enroller) using a Sagem fingerprint device.
Finger Position Guide	This manual is intended to assist the badge operator with the process of enrollment, specifically the placement and position of the finger on the MSO300 enroller.
Finger Positioning Summary	Summary page for the position the finger on the MSO300 enroller
Sagem Securite License Protection Installer	This Sagem/Morpho software is required for license validation of enrollment and template downloading to the Morpho readers.
MorphoSmart USB Driver	This is the installer for the USB driver for the MSO300 enroller device.

I.14 Add Biometric Field to Pro-Watch Advanced Badging

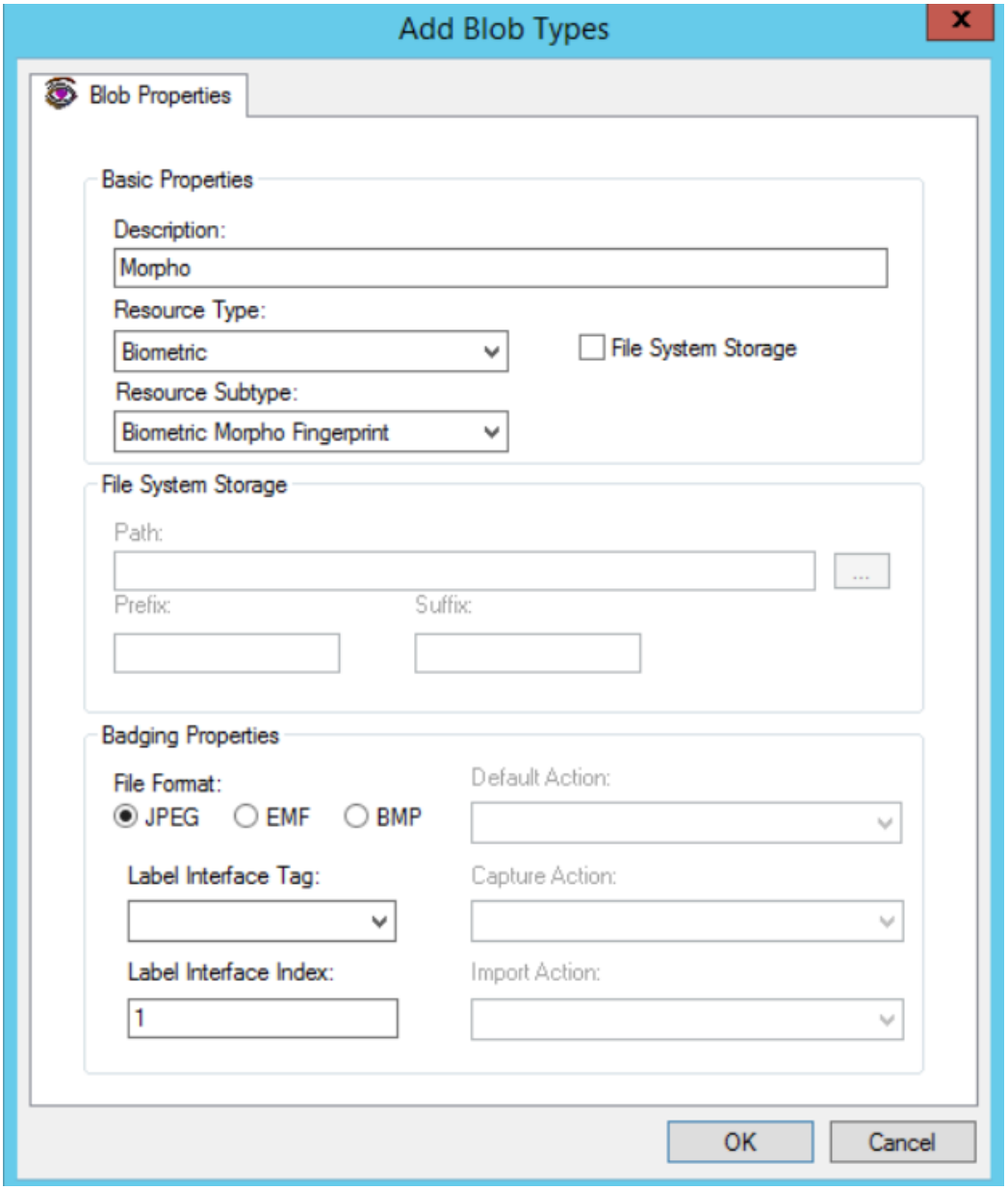
The following will provide a step by step guide to adding a biometric field to Pro-Watch Advanced Badging.

I.14.1 Step 1: Add two Pro-Watch Blob Types

In Pro-Watch:

1. Click and select **Administration** in the left navigation pane.
2. Select **Database Configuration**, then select **Blob Types to display the Blob Properties tab.**
3. Add two new blob types, one for each finger to be enrolled. Make sure the **Resource Type** is set to **"Biometric"**. **Resource Subtype** is set to **"Biometric Morpho Fingerprint."** This blob type will store the finger graphic and it does not matter if it is stored in the database or in the file system. The Morpho fingerprint template will be stored in the database.

Note: Honeywell recommends saving the fingerprint image to the database.

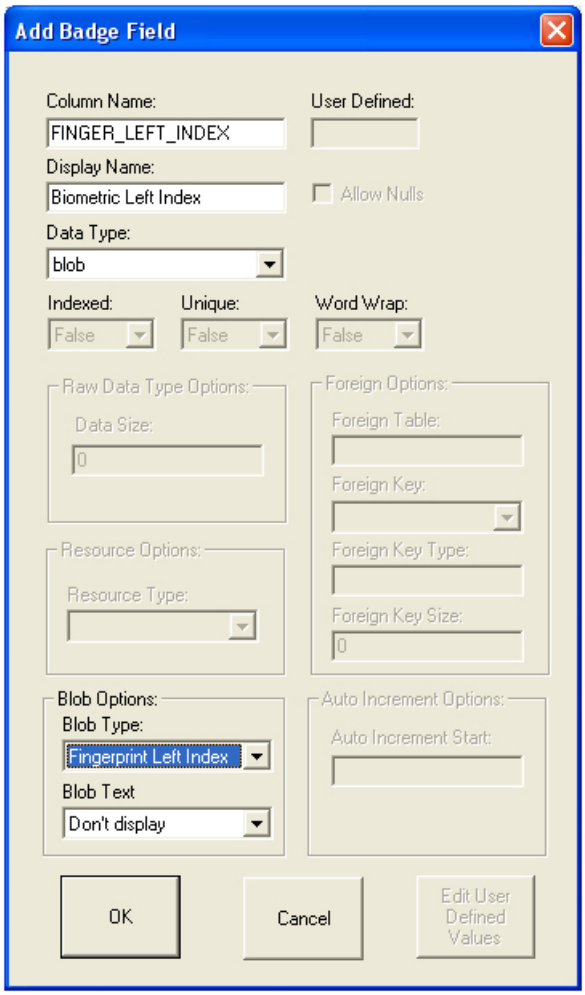


I.14.2 Step 2: Add two Pro-Watch Blob Fields

In Pro-Watch:

1. Click and select **Administration** in the left navigation pane.
2. Expand **Badge Utilities** and select **Badge Fields**.
3. Add a new badge field.

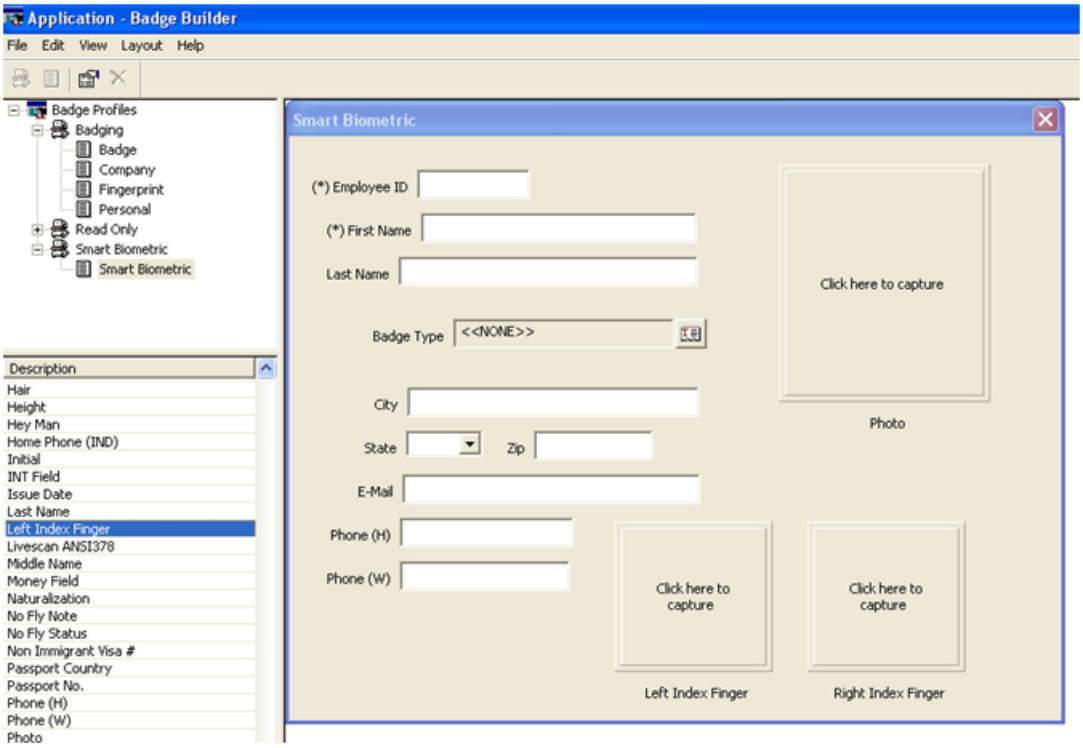
4. Set the **Data Type** to "**Blob**" and then at the bottom of the dialog box make sure the **Blob Type** is set to the blob type created in step 1. Do this for both biometric fields.



I.14.3 Step 3: Add New Badge Fields to Badging Forms

In Pro-Watch:

1. Click and select **Administration** in the left navigation pane.
2. Expand **Executables** and then double-click on **Badge Builder** to launch the Badge Builder application.
3. Select the Pro-Watch profile.
4. Then select the badge tab to add the biometrics fields to. Drag the two biometric field names from the left onto the badge form.
5. **Save** the profile and exit.
6. Now run **Pro-Watch Advanced Badging**, **edit** a badge record and select the biometric field to start the enrollment process.


Application - Badge Builder
File Edit View Layout Help
Badge Profiles
Badging
Badge
Company
Fingerprint
Personal
Read Only
Smart Biometric
Smart Biometric
Description
Hair
Height
Hey Man
Home Phone (IND)
Initial
INT Field
Issue Date
Last Name
Left Index Finger
Livescan ANSI378
Middle Name
Money Field
Naturalization
No Fly Note
No Fly Status
Non Immigrant Visa #
Passport Country
Passport No.
Phone (H)
Phone (W)
Photo
Smart Biometric
(*) Employee ID
(*) First Name
Last Name
Badge Type
<<NONE>>
City
State
Zip
E-Mail
Phone (H)
Phone (W)
Click here to capture
Photo
Click here to capture
Left Index Finger
Click here to capture
Right Index Finger

I.15 Morpho Indoor 500 Series Reader

Figure I-2 Morpho Indoor 500 Series Reader



I.16 Morpho Outdoor 500 Series Reader

Figure I-3 Morpho Outdoor 500 Series Reader



I.17 MSO300 Finger Enroller

Figure I-4 MSO300 Enroller



Copyright © Honeywell Inc. All Rights Reserved

I.18 MorphoWave Reader

I.18.1 Introduction



MorphoWave (formerly called Finger-on-the-Fly) is a technology by IDEMIA (previously Safran) Morpho that allows quick acquisition of 4 fingers in a single swipe of the hand.

The technology is contactless and accurate, allowing capture of wet or dry fingers.

The MorphoWave creates a 3D model of the finger shape using structured light technology, which creates an interoperable 2D image by unwrapping the texture image using the 3D model. The high-speed capture is less than a second and provides increased throughput and efficiency without sacrificing accuracy, which in turn decreases bottlenecks in high-traffic areas.

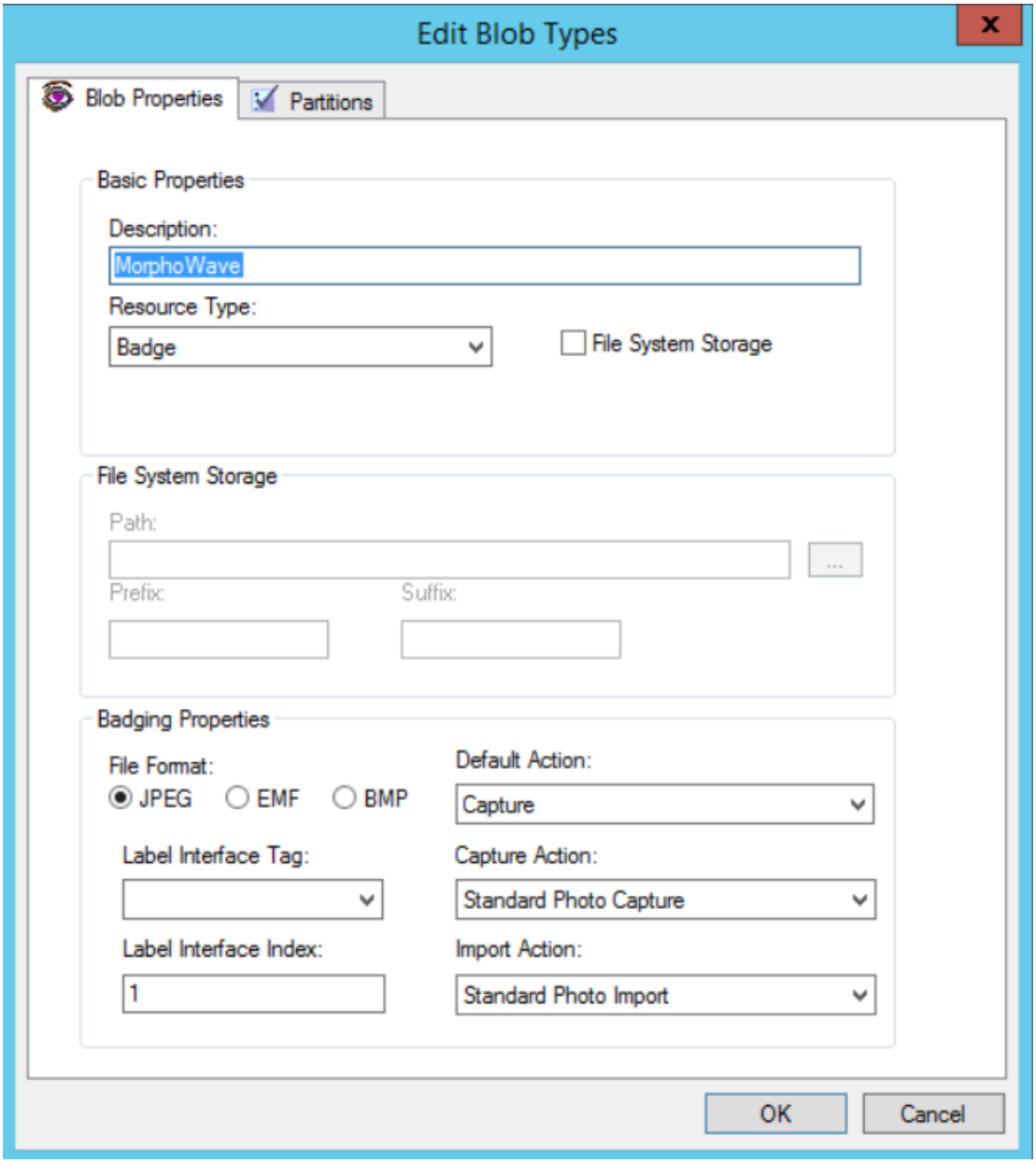
The MorphoWave integration consists of 2 pieces of hardware: the MorphoWave enrollment device and the MorphoWave Tower. The MorphoWave Tower is built up of several components: a Morpho Sigma reader, the Wave reader, the Wave PC, and a network switch.

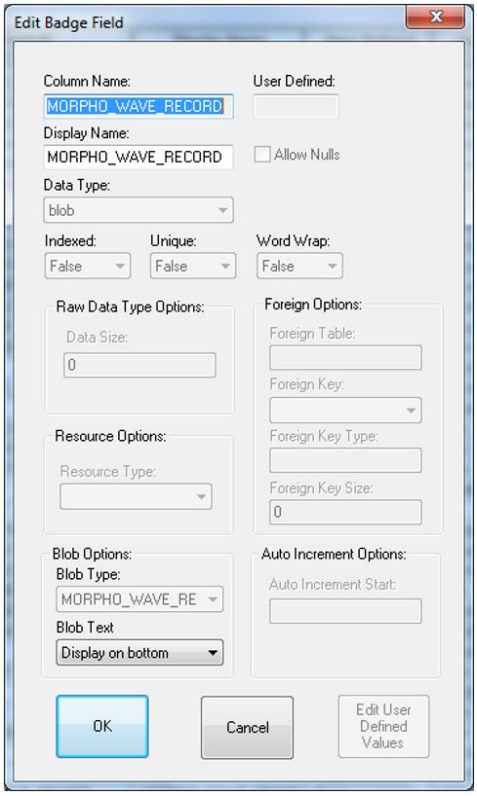
I.18.2 Requirements

- Enrollment reader requires a FiOTF license dongle
- VC++ 2013 64-bit needed
- The enrollment reader requires a USB 3.0 port to the host
- Pro-Watch Software License should have the **Smart Card and Biometrics** option enabled under **Pro-Watch AP options**.

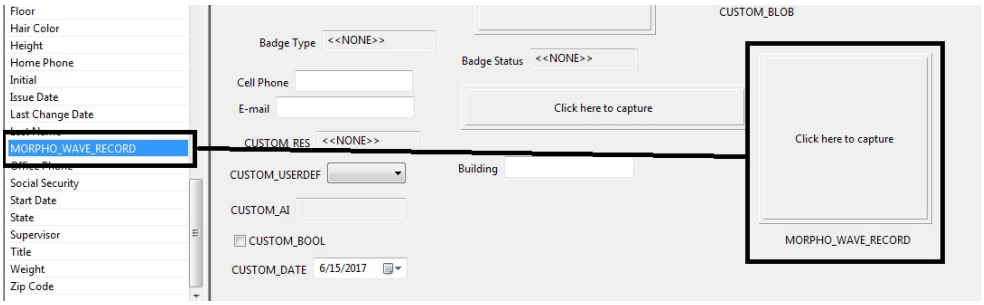
I.18.3 Setup for Enrollment

1. Create a new **BLOB type** and corresponding **badge field**:





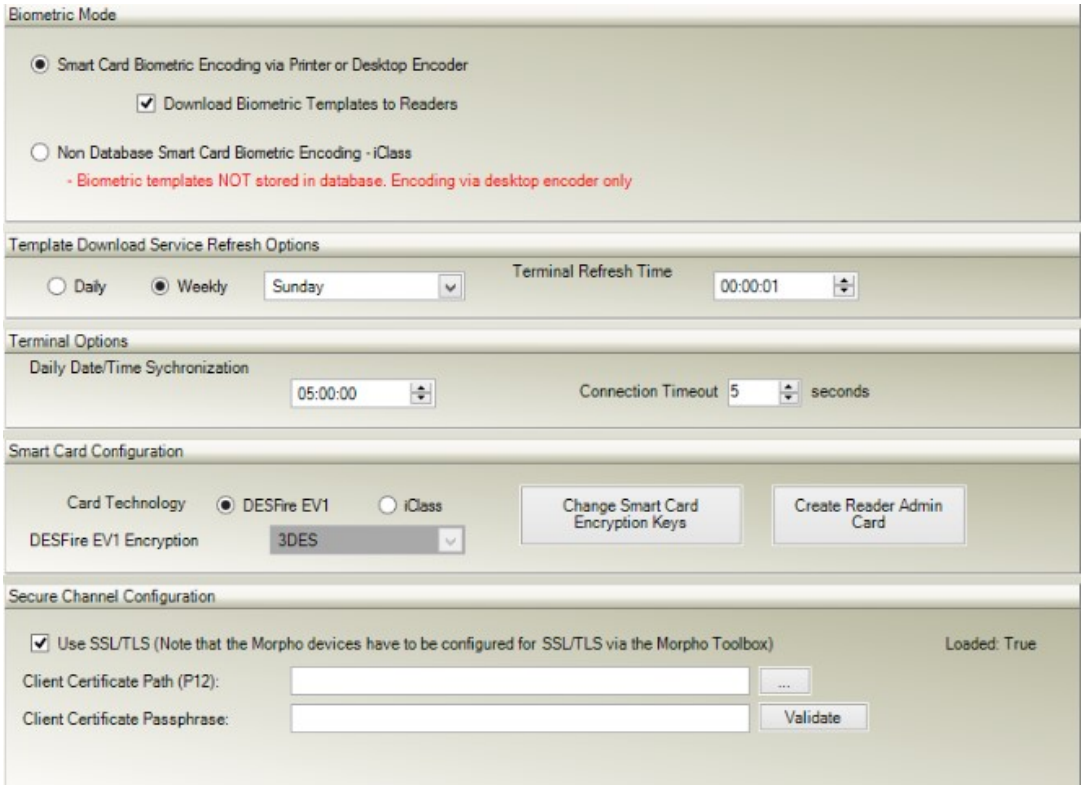
2. The new badge field can then be added to the badge profile through badge builder:



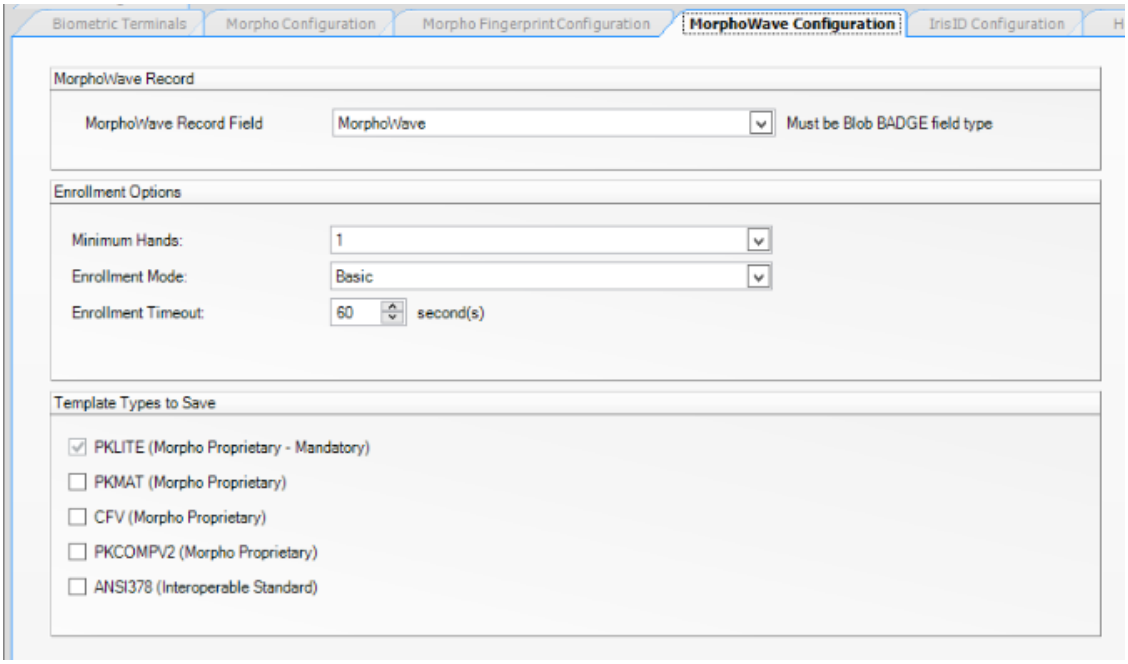
I.18.4 Morpho Biometrics Setup in Advanced Badging

Under the Morpho Biometrics module of Advanced Badging, there are 2 new tabs, Morpho Configuration and MorphoWave Configuration, that govern the functionality of enrollment through the Wave device.

Morpho Configuration:



Option Name	Description
Biometric Mode	Select Encoding and option to download Biometric Templates to readers.
Template Download Service Refresh Option	Option to refresh/reload terminals.
Terminal Options	Set time-of-day to synchronize date and time with terminals.
Smart Card Configuration	Select card technology and DESFire encryption.
Secure Channel Configuration	Enable SSL/TLS with Morpho devices that have been configure via the Morpho Toolbox. See Section Quick Start for SSL.



Option Name	Description
MorphoWave Record Field	The badge field that is used to store the MorphoWave template.
Enrollment Options	Set the number of required hands for enrollment, enrollment type, and the enrollment timeout values.
Template Types to Save	Sets the format of the saved template type.

The Minimum Hands option can be set for 1 or 2. If 1 is set, then only 1 hand is required for enrollment. If 2 is set, then both hands are required for enrollment.

The Enrollment Mode allows toggle between the Basic and Advanced enrollment:

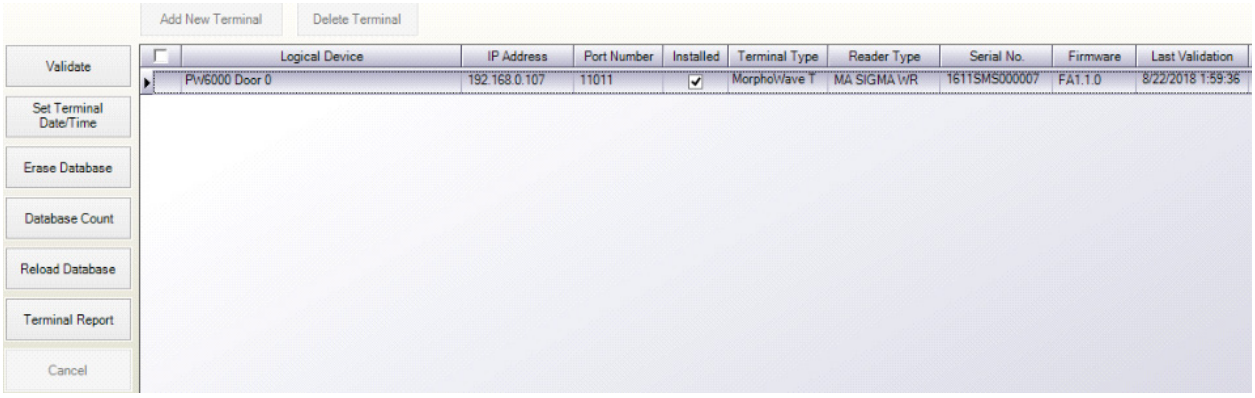
- **Basic Enrollment:** 2 captures are done and the best capture is saved as the template.
- **Advanced Enrollment:** Up to 10 captures are done and the best finger scan is saved.

A template type must be selected, otherwise the enrollment will not save. It is recommended that CFV, PKLITE, PKCOMPV2 and ANSI378 are checked by default.

A third tab under the Biometric Settings module of Advanced Badging,

Morpho Terminal Configuration is used to configure the terminals used for biometric terminals.

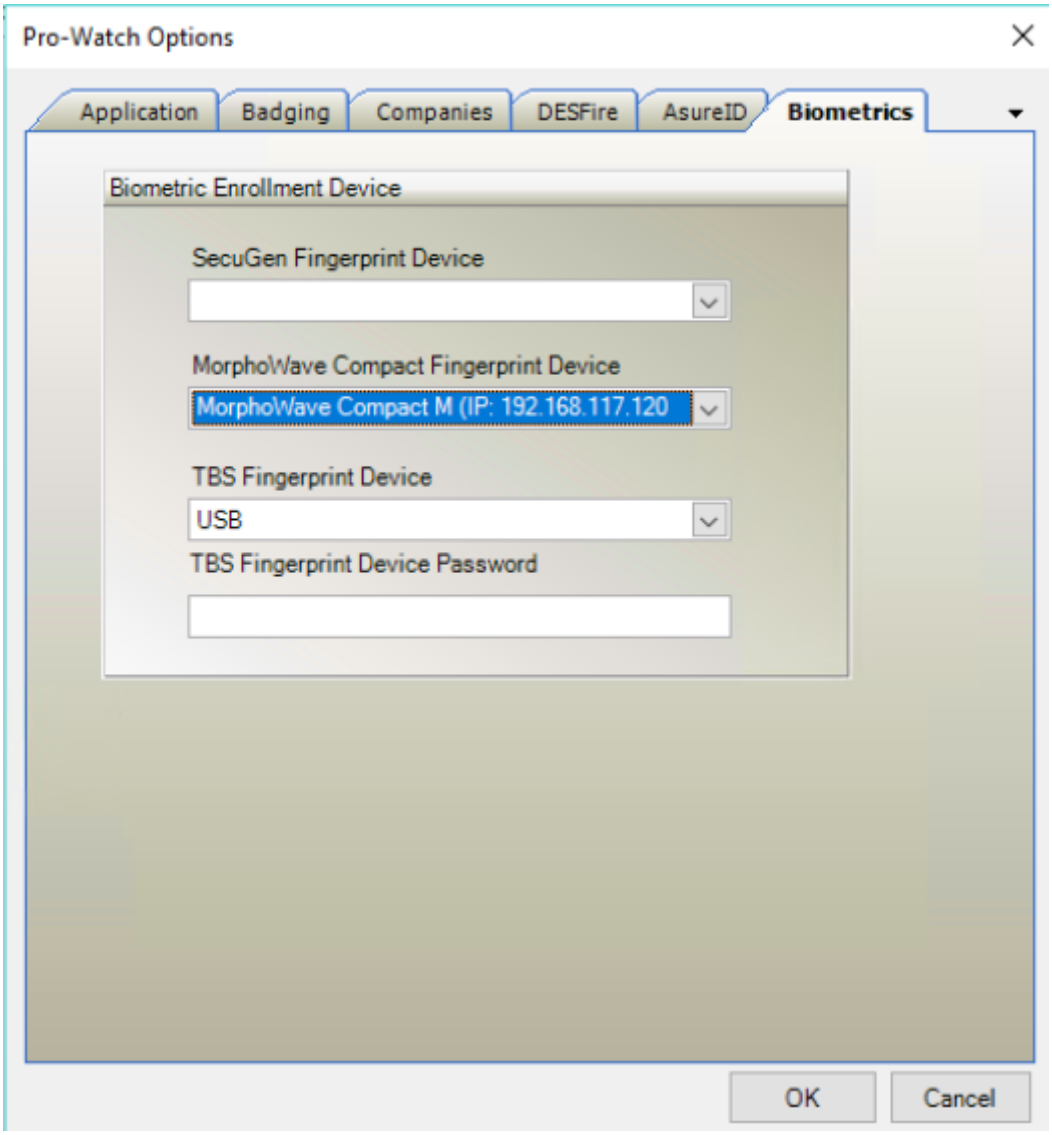
Morpho Terminal Configuration:



This tab is used to configure each Morpho terminal that will be used for access control. Logical Device, IP Address, Port Number, Installed and terminal type must be entered. The remaining fields are filled in by Advanced Badge during a Validate command.

The Terminal Types supported are: Sigma MA, MorphoWave Tower and MA5xx M1xx MJ. MorphoWave Tower must be selected.

MorphoWave Compact Towermust be associated as an enrollment device in Console > Options > Biometrics Tab from the MorphoWave Compact Fingerprint Device drop-down list as shown below:



I.18.5 MorphoWave Tower Connection/Setup

Download the Morpho Bio Toolbox from the Morpho Support Site (http://service.morphotrak.com/software-links.html). This will allow configuration of the Sigma reader to setup Wiegand output.

The MorphoWave Tower is an all-in-one unit which consists of a Sigma display, the Wave reader, an onboard PC to store template DBs, and a network switch. The switch must be connected to the network for the Morpho Bio Toolbox and Pro-Watch Client to communicate with the device.

In addition, the Tower is capable of outputting Wiegand through the Wiegand Out 0, Wiegand Out 1, and Ground to a reader port to pass events into Pro-Watch.

I.18.6 Quick Start for SSL

I.18.6.1 MA Sigma Setup

Certificates

This section requires the generation of certificates using OpenSSL. In this example, we will use the same self-signed authority for MA and PC, without intermediate authority.

1. **Example certificates:**
   a. MA_full.p12 to be loaded to MA SIGMA, this file uses passphrase 'morpho'. It contains MA certificate and private key, and trusted authority when receiving connections.
   b. PC.p12 is the certificate for the PC, this file uses passphrase 'maci'. It will be used by MACI.
   c. ca.pem is the authority certificate. It will be used by MACI.

MA SIGMA configuration

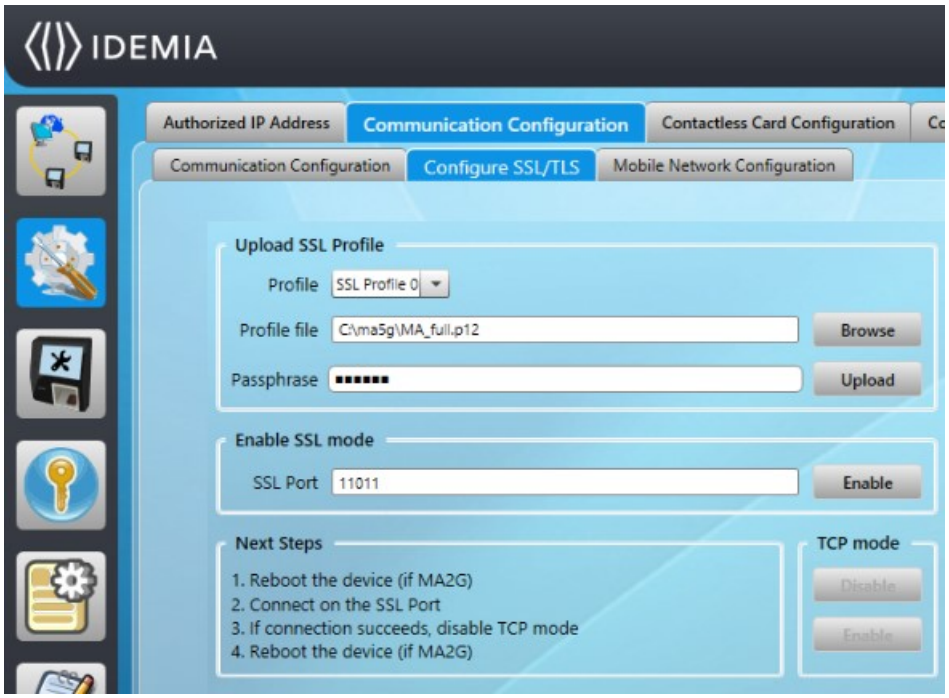
This section describes how to configure a MA SIGMA. Using MBTB, Morpho Bio ToolBox,

1. Connect to the MA SIGMA using default port (11010):



2. Load MA_full.p12 file: using MBTB (see below) or using file_load Thrift command, type = ssl_component, sub_type = SSL_profile_0
3. Enter 'morpho' passphrase (without the '): using MBTB (see below) or using passphrase_set. Thrift command, ID = SSL_profile_0
4. Set configuration parameter in_channel.SSL_conn_mode configuration to 1: using MBTB or config_set_params Thrift

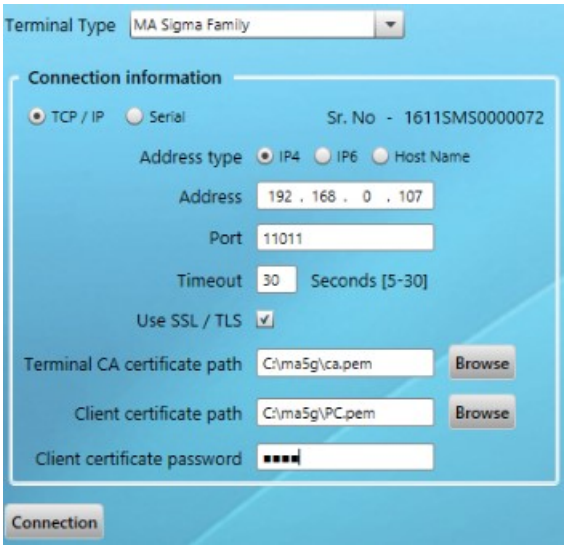
command.



Secure communication with MBTB

1. Connect to the MA SIGMA using SSL port (11011 by default):
   a. Using MBTB: see below
   b. Using OpenSSL (only to test the communication can be established): openssl s_client - connect your.masigma.ip.address:11011 -cert ma5g\PC.pem -CAfile ma5g\ca.pem

2. If it succeeds, you can disable clear TCP communication by setting in_channel.primary_port to 11011 (same value as in_channel.secondary_port)



Copyright © Honeywell Inc. All Rights Reserved.

Honeywell

Mercury M5 Bridge

J

In this appendix ...

Overview

Equivalences

Installation - General

Installation Steps (Without Wizard)

Installation Steps (With Wizard)

Adding Subpanels through Panel Properties

Mercury M5 Port Assignments

Default Assignments for REX and DPOS

M5-MUX8

M5-2K

Test Your Knowledge

J.1 Overview

Mercury Micro 5 Bridge (a.k.a. **M5 Bridge**) is Honeywell's hardware solution for those existing GE CASI-RUSCO clients who would like to continue to use the CASI enclosure with Mercury panels and Pro-Watch software.

Mercury's M5 Bridge is a replacement for the Micro 5 hardware enclosure which utilizes the existing wiring and downstream hardware at the CASI sites and does not require a screwdriver for installation.

The Mercury IC and IO boards provided for its Micro 5 solution are equivalent to existing Mercury hardware, but have been modified to fit into the physical slots of a standard Micro 5 enclosure. This allows users to convert from non-Mercury panels to Mercury panels without the expense

of rewiring everything. Since these are Mercury equivalents, Pro-Watch can be used as part of any such conversion.

J.2 Equivalences

The following M5 and Mercury boards are equivalents:

M5 Board	Its Mercury Equivalent
M5-IC (CPU Board)	EP2500
M5-COM (Communication board, providing communication between multiple panel enclosures)	N/A
M5-2RP/M5-2SRP (2-reader boards)	MR52
M5-20IN (20 input board)	Two MR16IN subpanels with 10 inputs each
M5-16DO/M5-16DOR (16 output boards)	MR16OUT
M5-8RP (8 reader board)	MR52 extended to support 8 readers

J.3 Installation - General

The installation consist of taking a Mercury EP2500 (M5-IC and M5-COM) and placing it on a board that fits into an existing GE hardware enclosure, a.k.a. Micro5. M5-IC or M5-COM is always installed in the seventh slot (J7) (see the illustrations below).

The installer then mates six different kinds of sub-panels which also fit into the enclosures (M5-16DO, M5-16DOR, M5-20IN, M5-2RP, M5-2SRP and M5-8RP).

There is also a communication board (M5-COM) for connecting multiple enclosures together. M5-COM is always installed in the seventh slot (J7) (see the illustrations below).

However the M5-IC and M5-COM boards cannot be both used in the same Micro5 enclosure. The user must choose one or the other in the seventh slot (J7).

Here is a typical M5-IC installation:

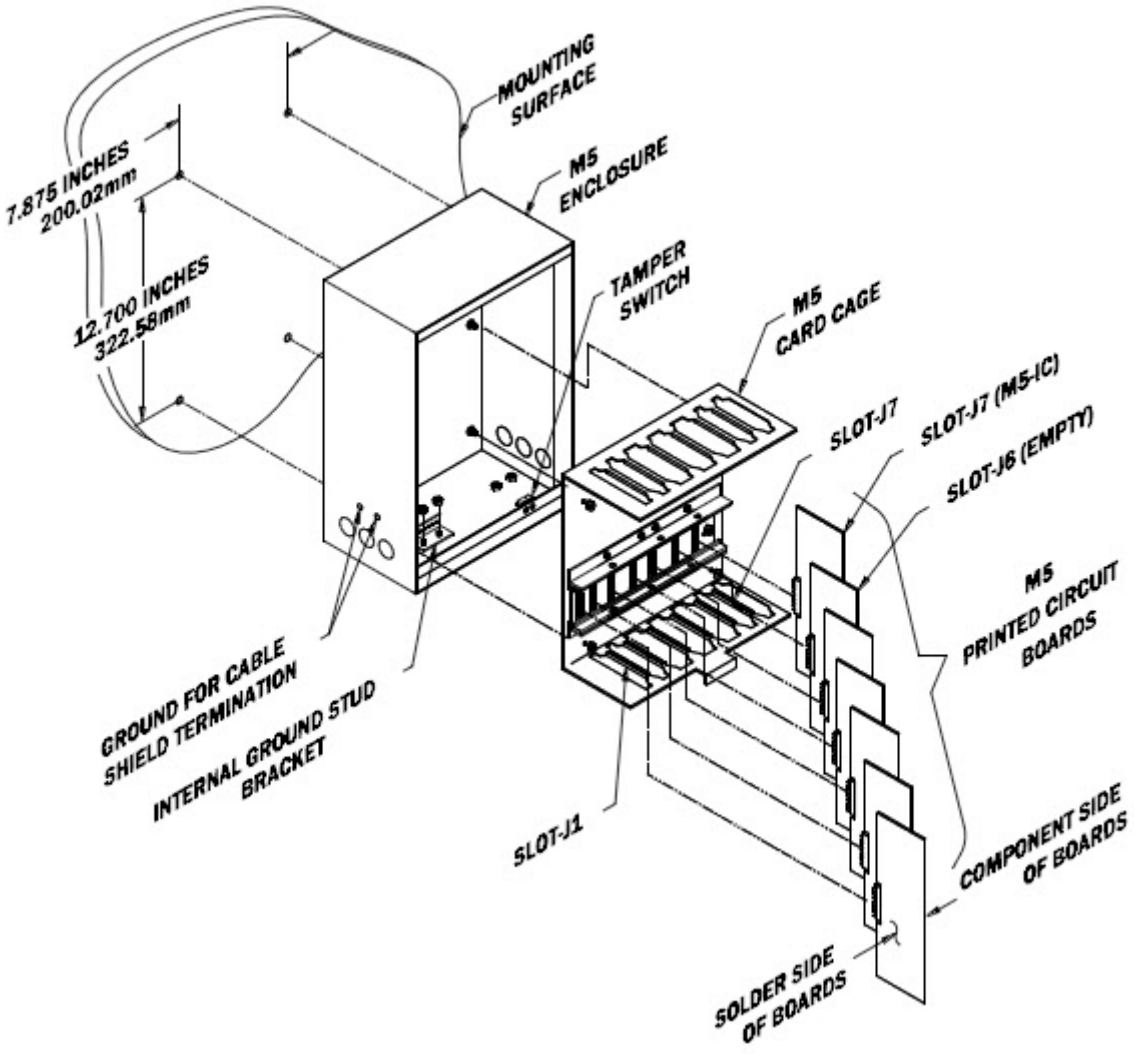


Figure J-1 Typical M5-IC Installation

Here is a typical M5-COM installation:

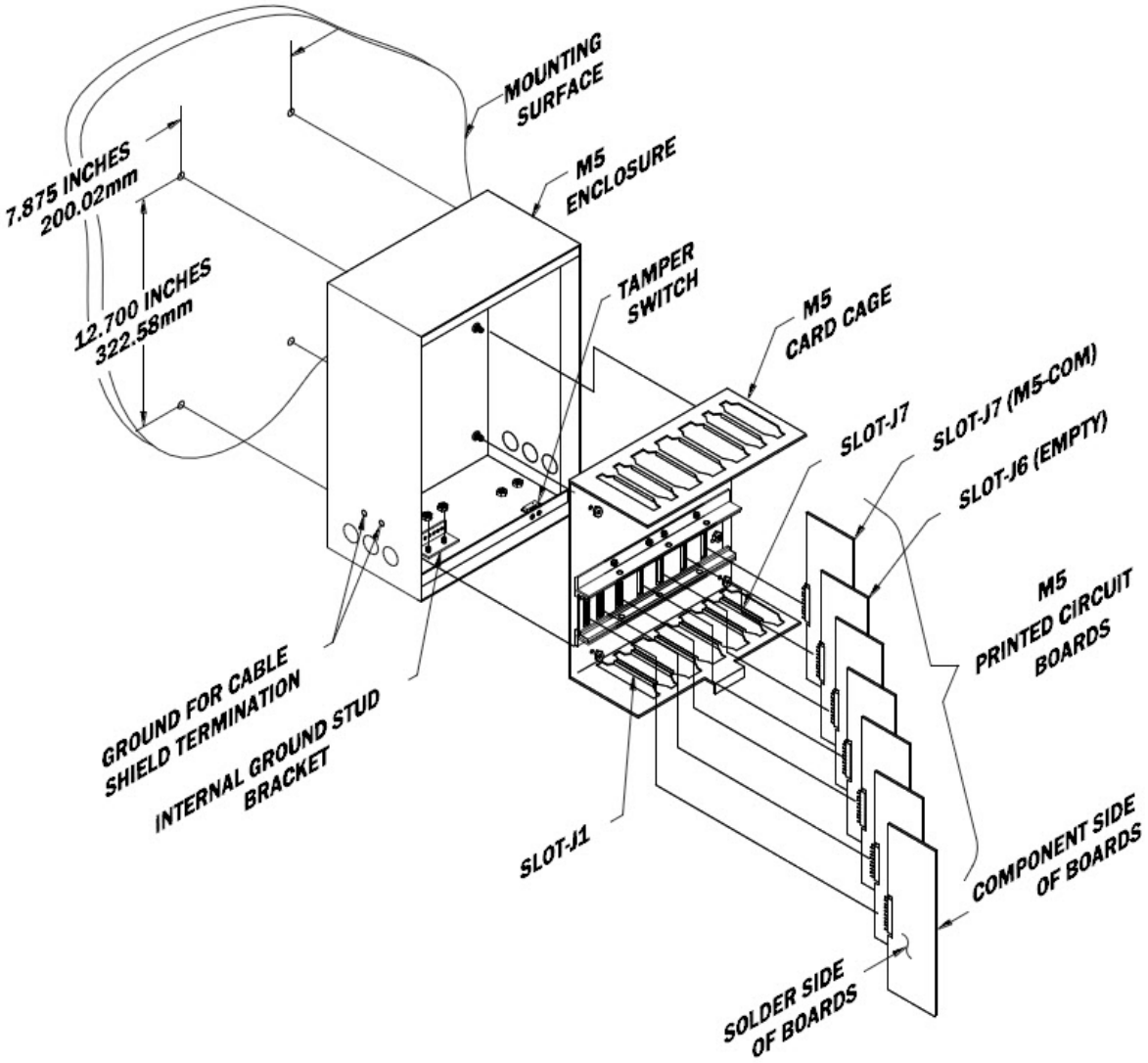


Figure J-2 Typical M5-COM Installation

Note: In all installations, the sixth slot (J6) is always left empty.

J.4 Installation Steps (Without Wizard)

To turn off the wizard, see Turning the User Wizard On and Off, page 4.

J.4.1 STEP1: Create a Site

See Add a Site in Chapter 6,

J.4.2 STEP 2: Create a Channel

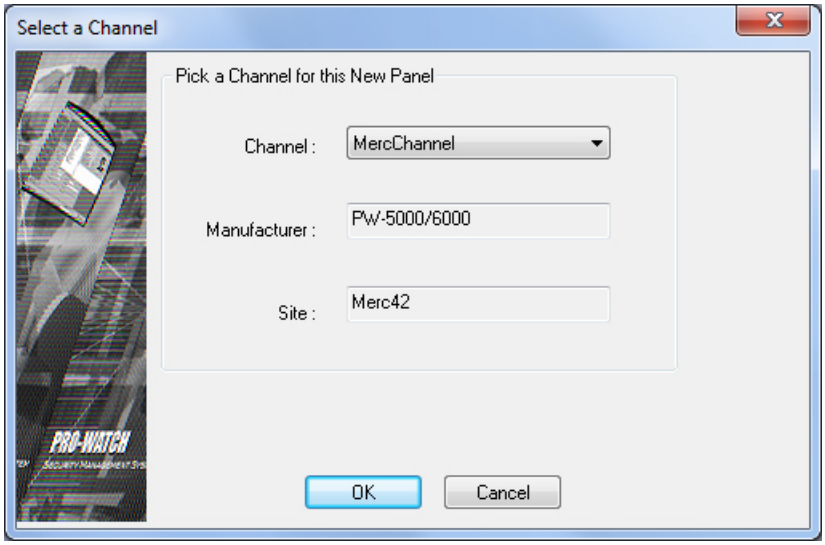
See How to Add a Channel in Chapter 6,

When creating a Channel for the M5 IC, there is a check-box on the on the PW5000/PW6000 Parameters dialog that selects Honeywell Protocol.

Uncheck this check-box because the M5 IC uses Mercury Protocol, not Honeywell.

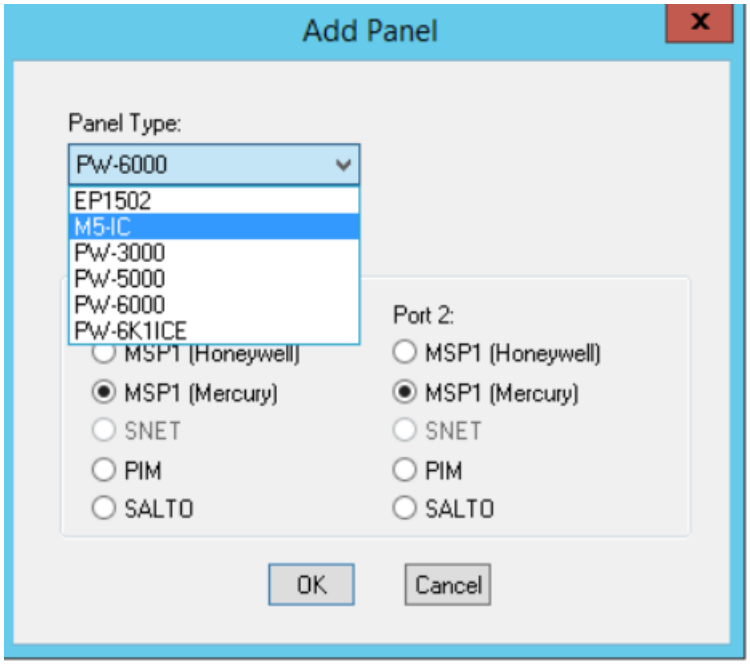
J.4.3 STEP 3: Create a Panel

Right-click on the channel created in Step 2 and from the pop-up menu select **New > Panel** to display the **Select a Channel** dialog box:



J.4.4 STEP 4: Select the Panel Type

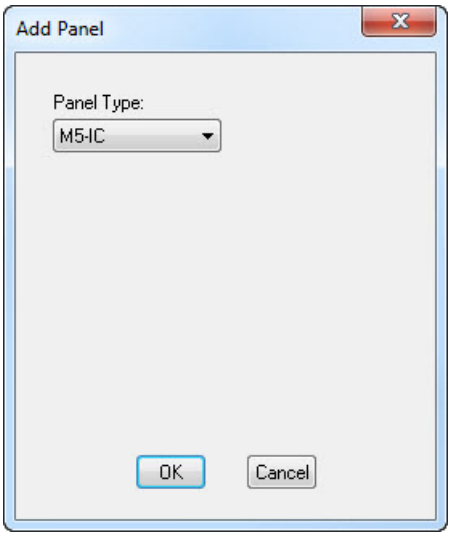
1. Click **OK** to display the **Add a Panel** dialog box:



Note: "M5-IC" is one of the panel type choices. M5-IC will only appear if the "Micro/5 Bridge" license feature is enabled when creating a license.

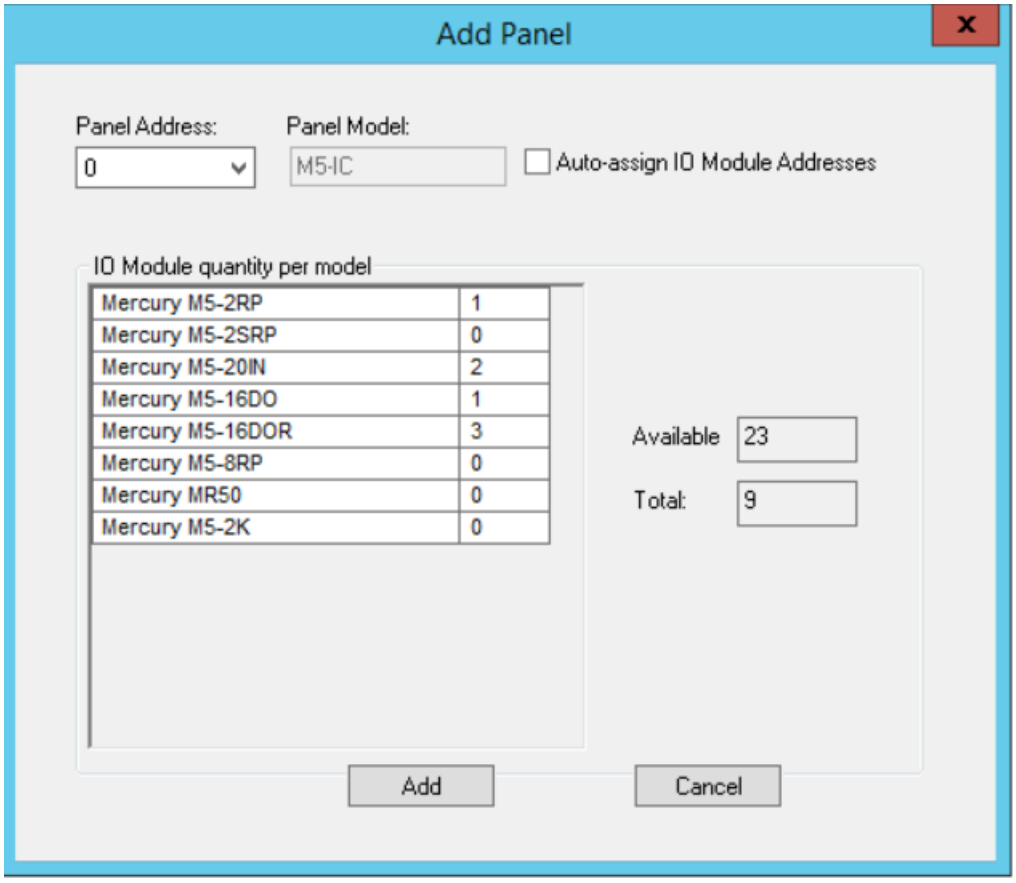
Note: Since M5-IC and PW6K1ICE must be the only panels on their channel, these panel-type selections will not appear for any channel which already has panels configured on it.

2. Select **M5-IC** panel type to change the appearance of the dialog box:



J.4.5 STEP 5: Allocate subpanels

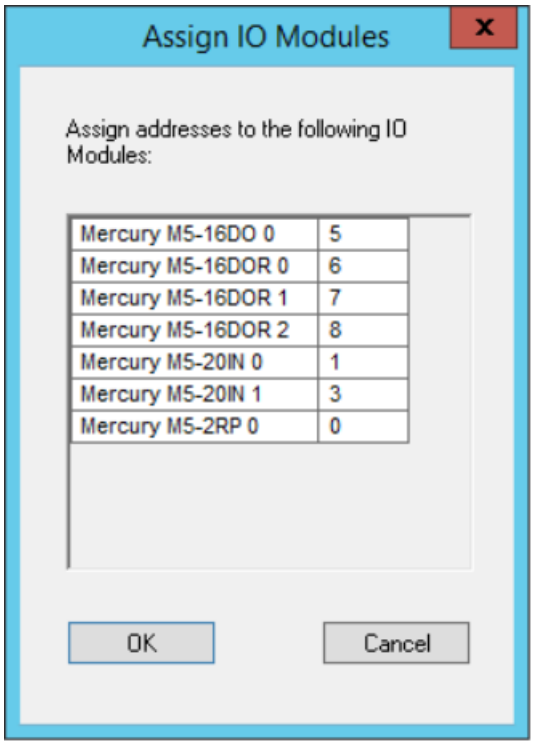
3. Click **OK** to display the **Add Panel** screen. Select all the appropriate numbers from the respective drop-down panels. The Pro-Watch will display the number of **Available** and current **Total** subpanels.



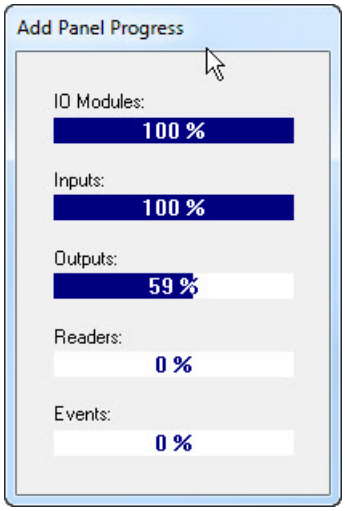
Selecting the panel type and port configuration controls the set of possible sub-panel types. This is displayed in a common dialog, with one line per sub-panel type, and a drop-down consisting of the possible number of subpanels of that type which can be added.

Selecting “M5-IC” for panel type allows selection from among six possible sub-panel types. The restriction of a single reader sub-panel type is enforced by restricting the drop-down value to 0 for the two reader types not already allocated.

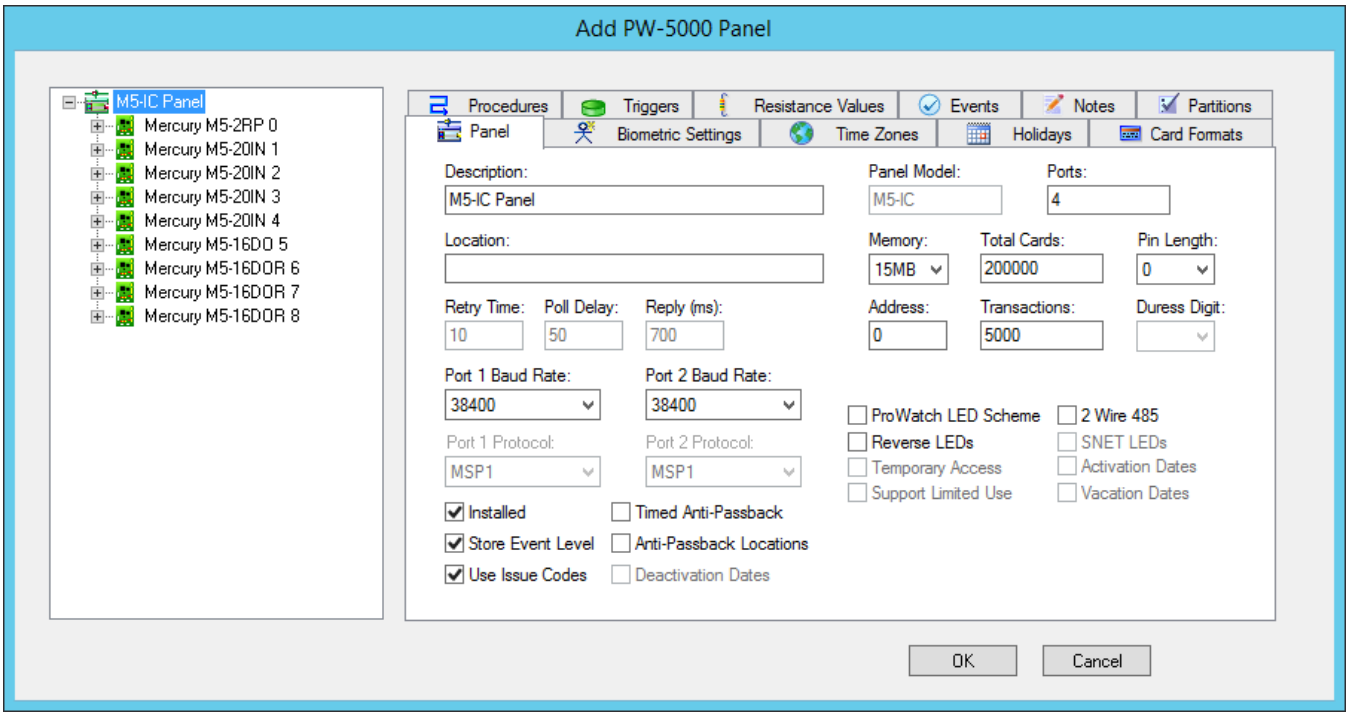
4. Assign addresses to the following IO modules:



5. Click **Add** to display the Progress Bars:



6. When all the panel components are added, the system displays the **Panel Properties** screen:



J.5 Installation Steps (With Wizard)

To turn on the wizard, see Turning the User Wizard On and Off, page 4.

J.5.1 STEP1: Create a Site

See Add a Site in Chapter 6, .

J.5.2 STEP 2: Create a Channel

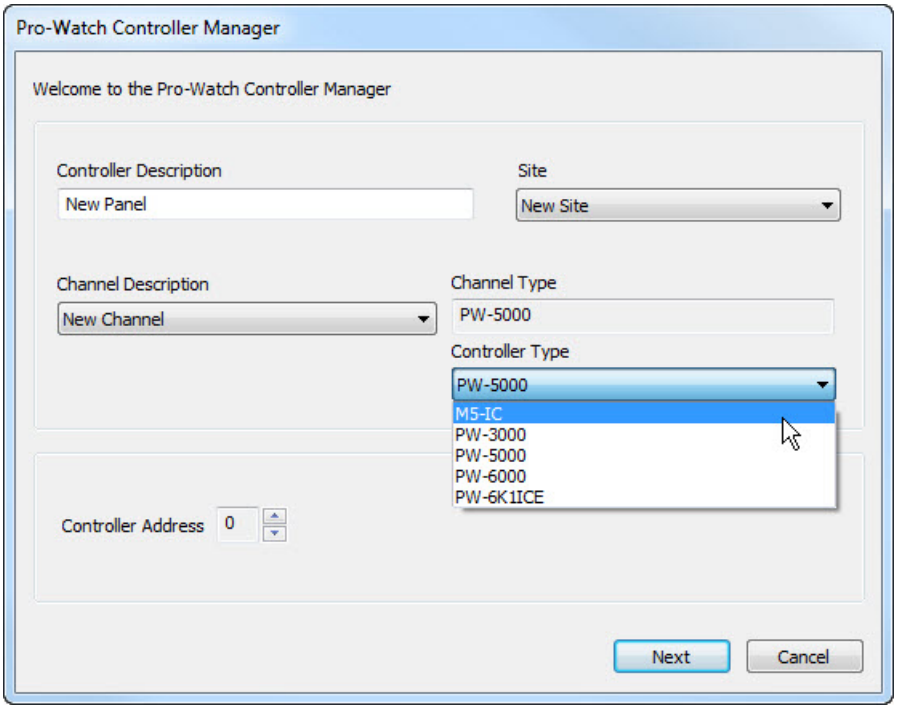
See How to Add a Channel in Chapter 6, .

When creating a Channel for the M5 IC, there is a check-box on the on the PW5000/PW6000 Parameters dialog that selects Honeywell Protocol.

Uncheck this check-box because the M5 IC uses Mercury Protocol, not Honeywell.

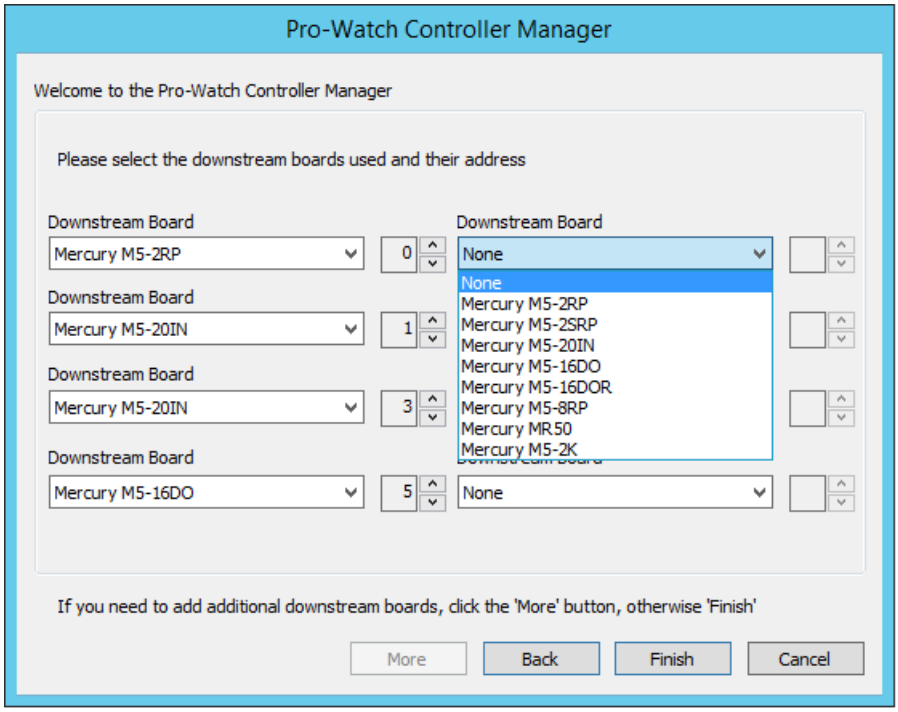
J.5.3 STEP 3: Define the panel

The users can select the new panel type of M5-IC, which is available if licensed and if the channel has no other panels on it.



J.5.4 STEP 4: Adding subpanels

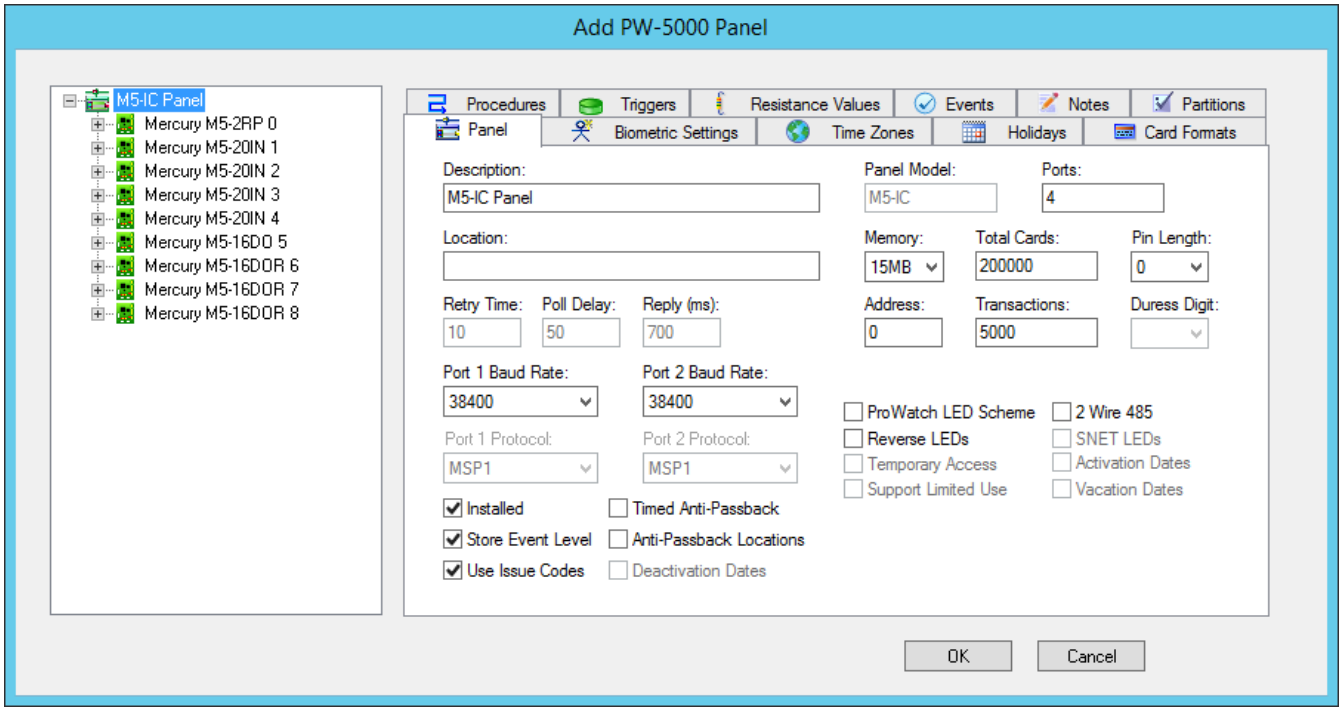
1. Click **Next** to display the downstream board selection screen:



The lists of valid sub-panel types in the “Downstream Board” dropdowns take into account the panel type, the configured downstream protocols, and the subpanels already allocated.

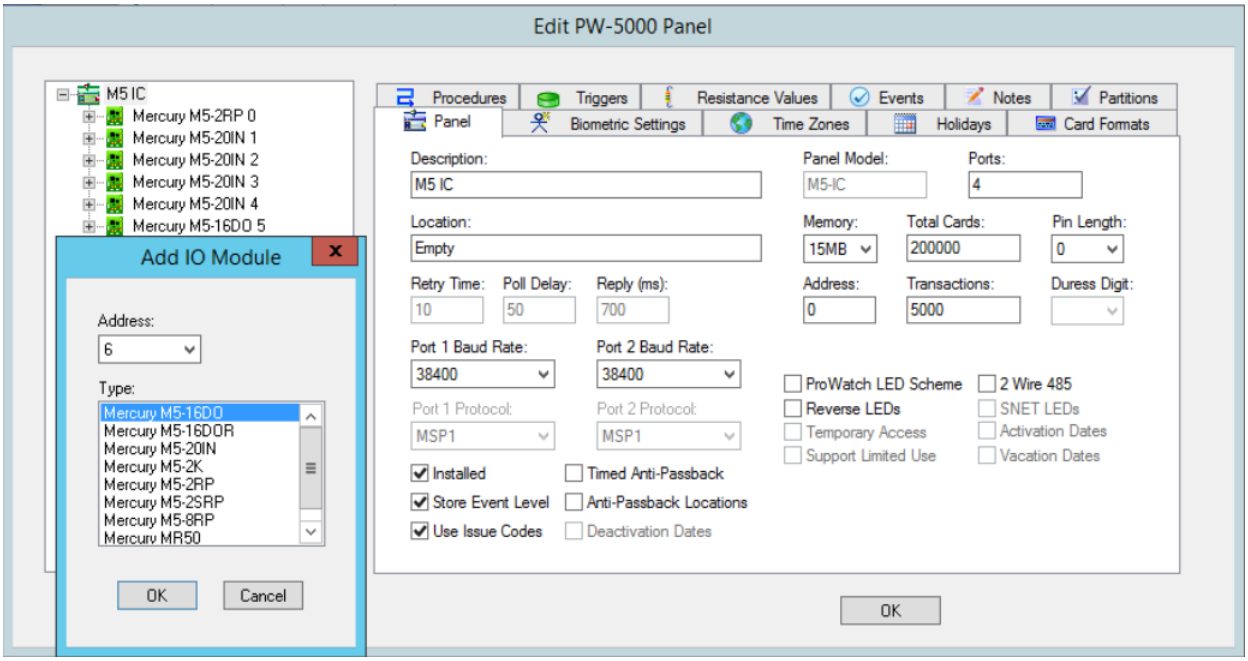
2. Click **Finish** to create the new panel.

3. To edit the newly created panel or add subpanels or I/O modules, double-click the panel's icon and display the **Panel Properties** screen. Here is an example:

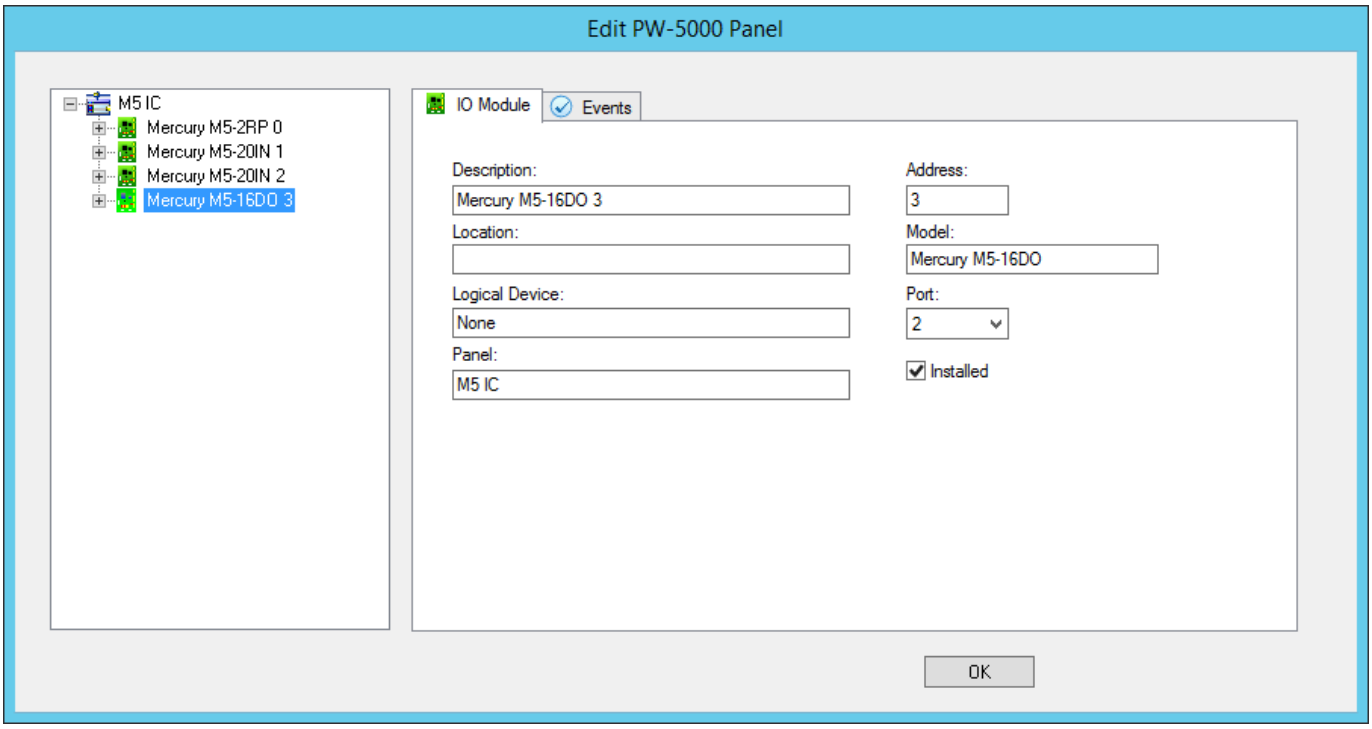


J.6 Adding Subpanels through Panel Properties

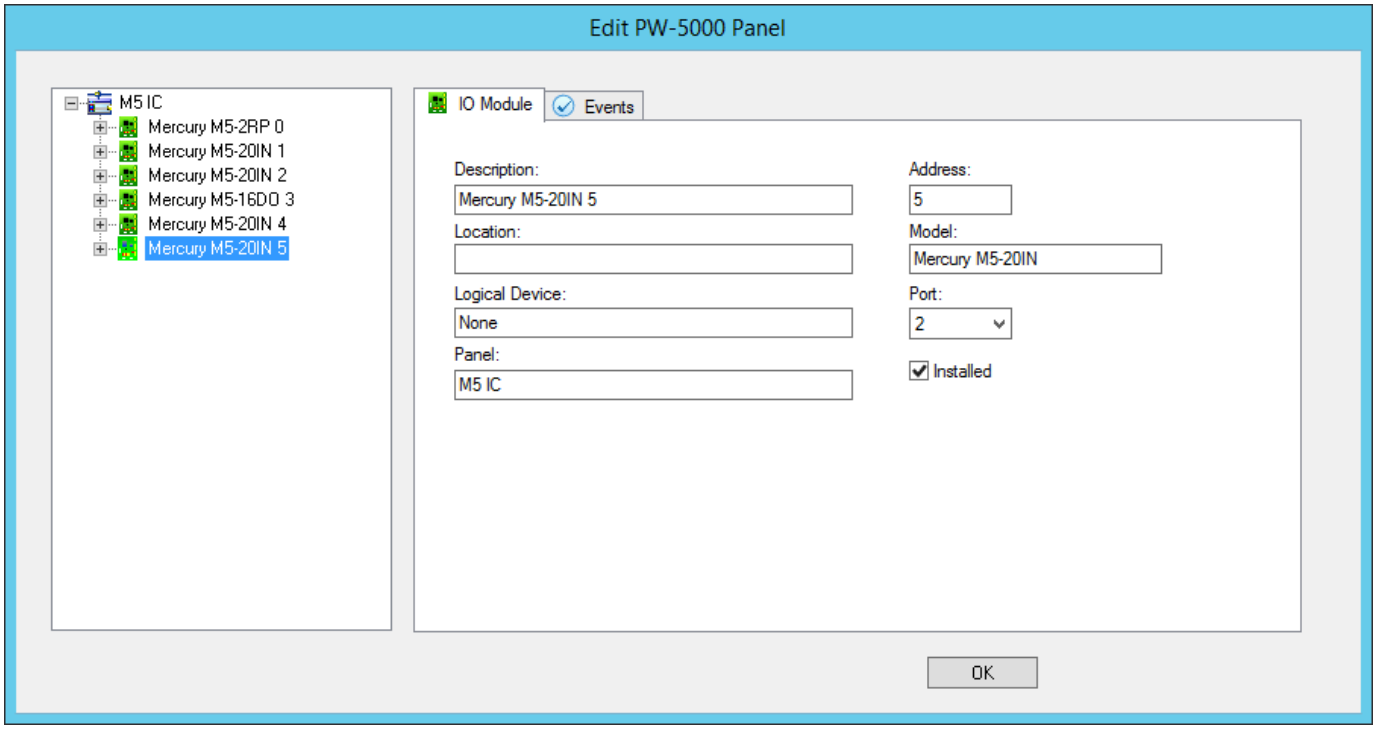
When adding subpanels to an existing panel, the contents of the drop-down are populated according to the port protocol configuration and the existing set of subpanels.



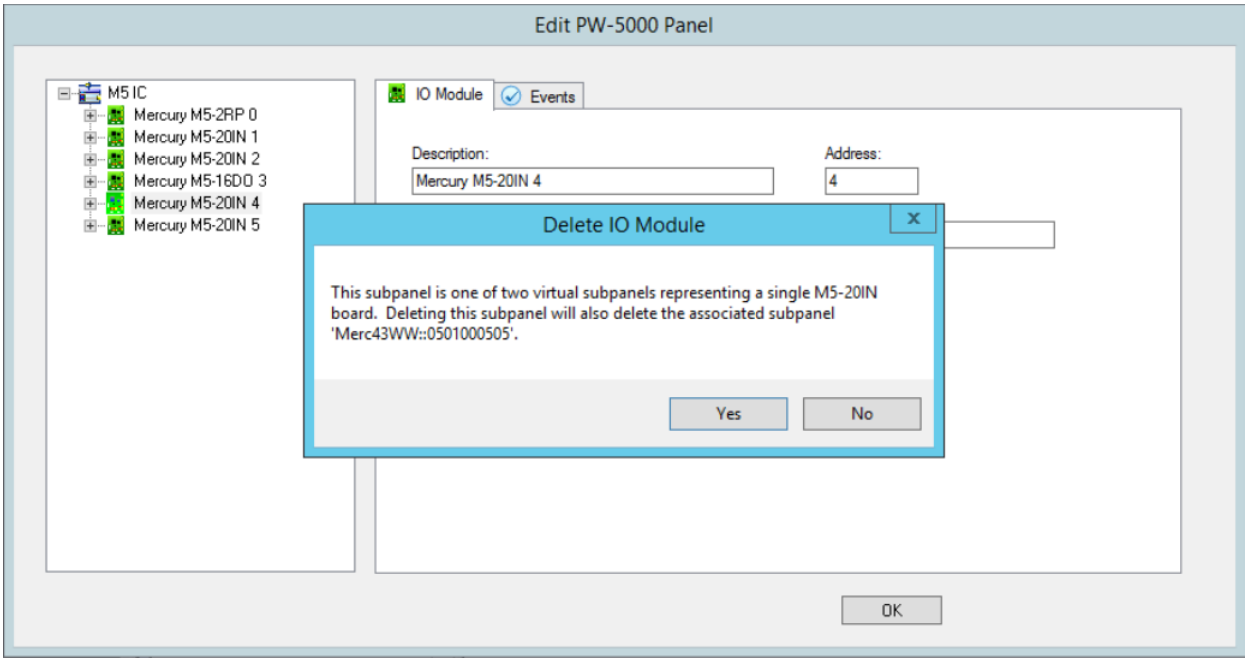
Here is another example that shows the division of an M5-20DI into two 10 input subpanels. The first display below shows an M5-IC with a 2 reader board (“M5-2RP 0"), two 10 input boards resulting from adding a single M5-20DI (“M5-20DI 1" and “M5-20DI 2"), and a single M5-16DO (“M5-16DO 3").

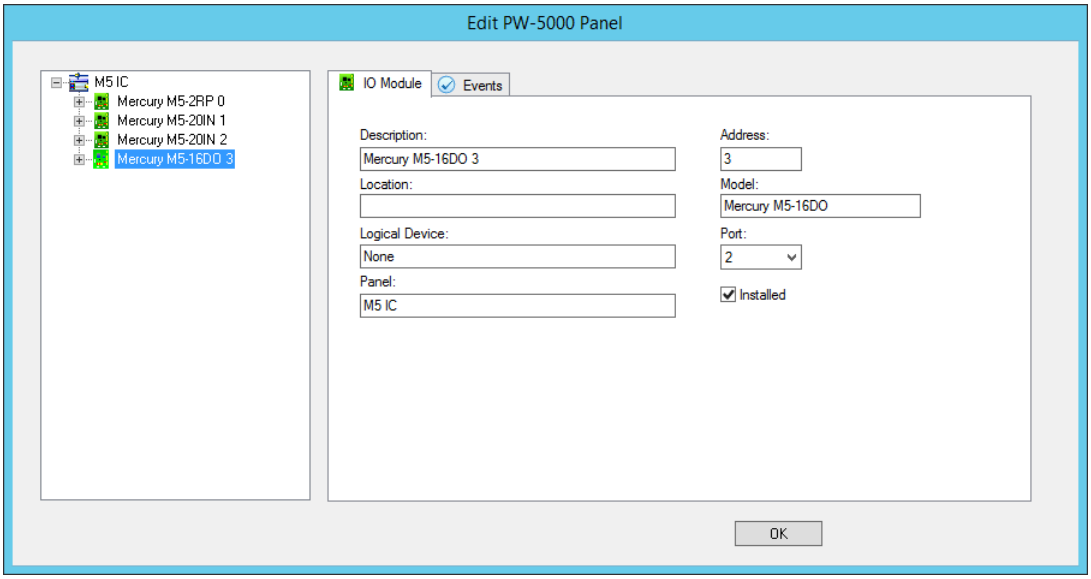


This second display shows the results of adding another M5-20DI.

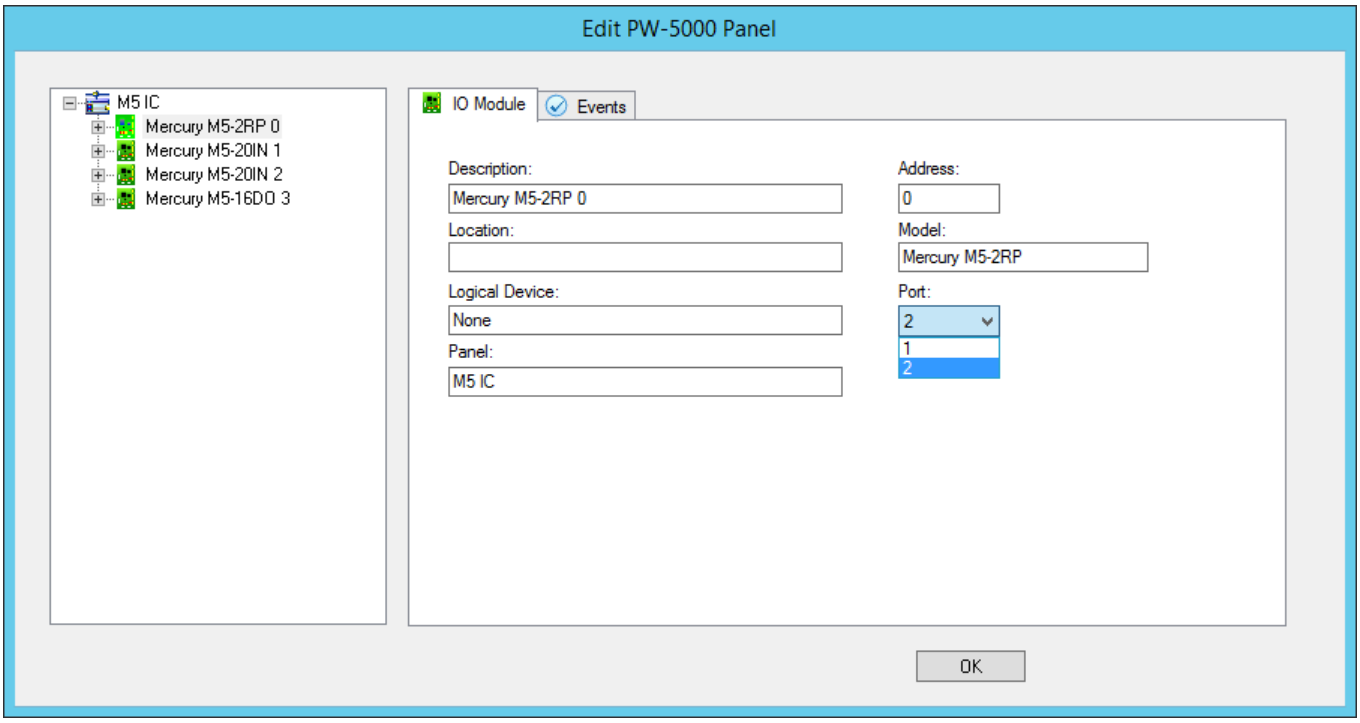


Deleting either of the two newly added “virtual” subpanels results in the popup warning that both will be removed. The final display shows the results after deleting one of the virtual subpanels. Note that both are now gone.





J.7 Mercury M5 Port Assignments



The Mercury M5-COM board provides interface to downstream M5 enclosures.

In Pro-Watch:

- Subpanels that are installed in the same enclosure as the **M5-IC** should be installed under **Port 1** in the IO Module tab of the sub-panel properties.

- Subpanels that are installed in downstream **M5-COM** enclosures should be installed under **Port 2**.

J.8 Default Assignments for REX and DPOS

The default assignments for the REX and DPOS are determined in two ways:

1.For **F/2F readers on an M5-8RP board**, the inputs, outputs and readers are hard coded in groups, but with only two inputs instead of three for each reader. For the M5-8RP, the first input is always the REX and the second is always the DPOS. A database view groups and arranges the hardware accordingly.

3.For **all other hardware**, if there are two inputs, the first is always the DPOS and the second is always the REX. The order in which the inputs are listed in the hardware template doesn't matter. This is currently hard coded.

This means, when doing the default assignments for a F/2F reader, the inputs will be backwards for M5-2RP and M5-2SRP boards. Thus they must be reassigned.

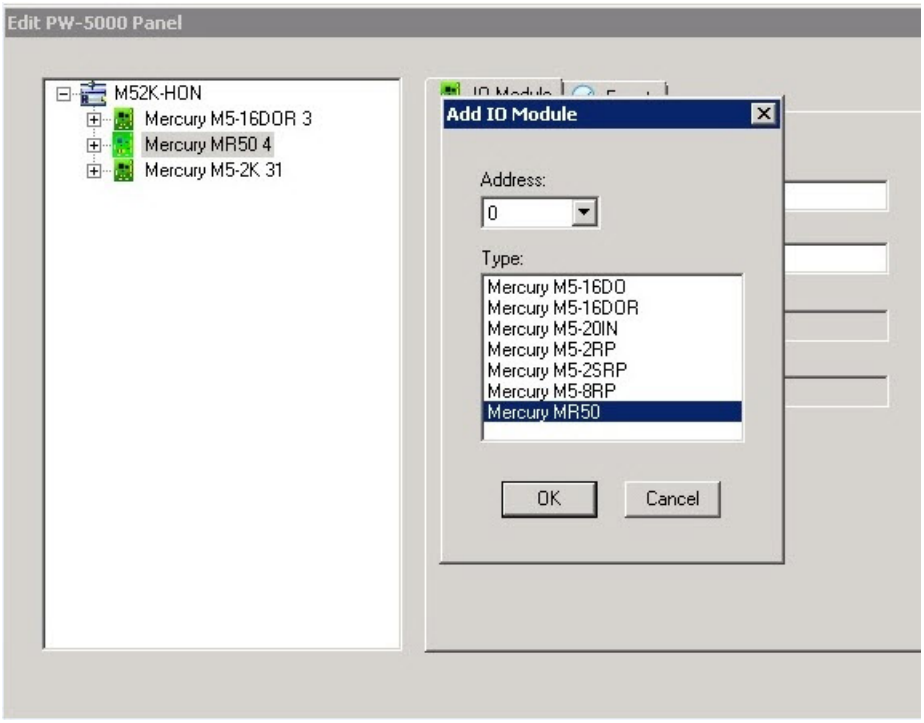
J.9 M5-MUX8

The M5-MUX8 device is a multiplexer designed to a replace an 8RP board to a single communications port that supports up to eight (8) external, two wire RS-485 based IOs.

The M5-MUX8 will allow F/2F readers or Wiegand Interface Units (WIU) to be replaced with up to eight (8) MR50 reader interface boards.

J.9.1 Installing the M5-MUX8

The M5-MUX8 replaces the 8RP board. Plug the M5-MUX8 directly in the M5 back plane.



J.9.2 Programming in Pro-Watch

The M5-MUX8 is a hardware device that extends the RS-485 port to allow users to connect MR50 subpanels to the M5-IC. In Pro-Watch, the MR50 subpanel type is now enabled for the M5 controller type. Each MR50 must have an unique RS-485 address.

Note: Adding a MR50 subpanel must be used in conjunction with the M5-MUX8 in order for correct operation.

J.10 M5-2K

The M5-2K is a subpanel for the M5-IC that provides support for:

- Four (4) F/2F protocol based readers,
- Ten (10) on-board inputs with Addresses 8 to 17, and
- Eight (8) on-board outputs with Addresses 4 to 11 for non-reader logical devices.

Only one (1) M5-2K subpanel can be added to a M5-IC installation.

J.10.1 Virtual Inputs and Outputs

In Pro-Watch, hardware allocations for the M5-2K contain **virtual inputs and outputs** that are located through the reader using F/2F protocol.

The first eight (8) inputs with Addresses from 0 to 7 and first four (4) outputs with Addresses from 0 to 3 are virtual and should be associated with the logical devices for the F/2F reader. Although it is possible in Pro-Watch to assign non-reader logical devices to these hardware points, these hardware addresses cannot be used for non-reader logical devices.

For input and output needs, the M5-2K provides an additional ten (10) on-board inputs (Input Addresses 8 to 17) and eight (8) on-board outputs (Output Addresses 4 to 11).

J.10.2 Reserved Inputs and Outputs

In Pro-Watch, hardware allocations for the M5-2K contain **reserved inputs and outputs** that are located through the reader using F/2F protocol.

The first eight (8) inputs with Addresses from 0 to 7 and first four (4) outputs with Address 0-3 are reserved to be used with the M5-2K readers. Although non-reader logical devices can be assigned to these hardware points, these hardware addresses should not be used for non-reader logical devices.

Note: For additional information on the M5-2K, please refer to the *M5-2K Application Note* document from Mercury.

J.11 Restrictions

A Pro-Watch PW channel can support **only one M5-IC**, and that has to be the only panel on that channel.

A new Pro-Watch license flag will allow or disallow access to the M5-IC. In addition to this flag, the license will also limit the maximum number of M5-IC panels supported by a Pro-Watch installation.

J.12 Test Your Knowledge

(Answers provided in the next section.)

1) In which slot of the Micro5 enclosure should you install M5-IC or M5-COM board?

A. First slot (J1)

B. Seventh slot (J7)

C. Third slot (J3)

D. Fifth slot (J5)

2) Which slot of the CASE Micro 5 enclosure should always be left empty?

A. First slot (J1)

B.Seventh slot (J7)

C.Third slot (J3)

D.Sixth slot (J6)

3) What is the maximum number of readers one enclosure can control?

A. 6

B. 8

C. 64

D. 32

4) One can install both M5-IC and M5-COM boards to the same enclosure.

A. True

B. False

J.12.1 ANSWERS to "Test Your Knowledge" Quiz

1) B

2) D

3) C

4) B

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Two-Person Rule

K

In this appendix ...

Overview
Mercury Panel Area Support
Activating the Two-Person Rule
The Minimum Option
FAQ
Test Your Understanding

K.1 Overview

The Two-Person Rule is a Pro-Watch security feature supported only by PW-5000 or PW-6000 panels.

When activated, the Two-Person Rule requires two persons to present their cards to a reader in order to enter or exit an area. The "minimum" option of this rule circumvents the two-person requirement as long as there are a minimum of two persons still present in a given area (see the section on "The Minimum Option" below).

After the user activates the rule (see the section on "Activating the Two-Person Rule" below), the rule is enforced by allowing only two persons enter or leave the area if they present their cards to the reader one after the

other within 15 seconds. The door will not open until after the second card swipe.

K.2 Mercury Panel Area Support

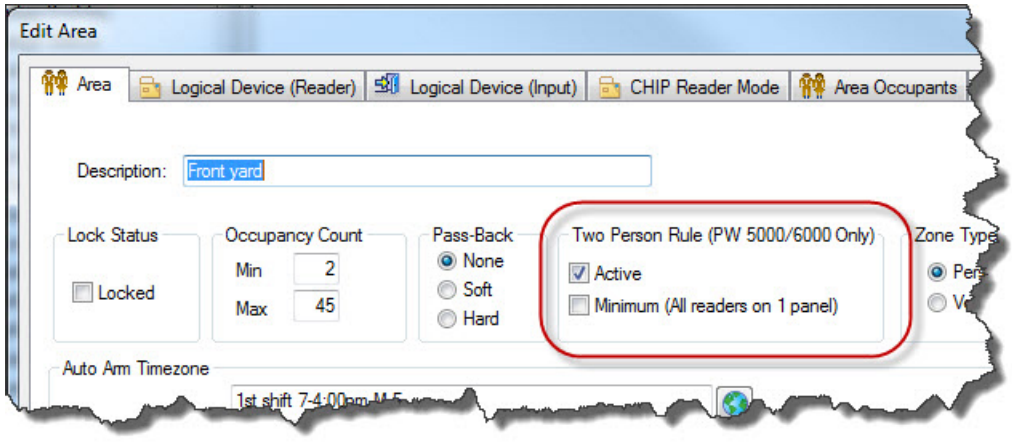
Where possible, Pro-Watch can take advantage of Mercury area support. In order for the "minimum" functionality to work, all the readers in the area must be controlled by the same Mercury panel.

Mercury supports the two-person-minimum feature in areas completely defined within one Mercury panel. If all the entry and exit readers for an area are on a single panel, then the area can be configured on the panel, and the panel can keep track of the number of cards in that area.

If the area spans more than one panel, no single Mercury panel can keep track of the area. The multiple Mercury panels cannot collectively keep track of the total card usage in the area either since the Mercury panels do not communicate directly with each other.

K.3 Activating the Two-Person Rule

1. Launch the Pro-Watch.
2. Click the Database Configuration link on the Navigation pane on the left.
3. Select an Area. Right click and select Properties option from the pop-up menu to display the Edit Area dialog box
4. Click and select the Area tab which displays two Two-Person check-boxes:



5. Select Active to activate the Two-Person rule. Either select or skip the Minimum check-box after reading the next section, "The Minimum Condition."
6. Click OK when you're done.

K.4 The Minimum Option

The user can select from one of the following three combinations by selecting or clearing the "Active" and "Minimum" check-boxes in various combinations:

Here are the combinations:

	Active CHECKED	**Active UNCHECKED**
Minimum CHECKED	There can be any number of persons in the area greater than one (1), i.e**., there should be a minimum of TWO (2) persons.** The first two must enter as a pair, and the last two must exit as a pair. But as long as there are at least 2 persons in the area, any number can enter singly, and as long as there are three or more in the area, any number can exit singly. The key for the MINIMUM mode is that there must be a minimum of 2 in the area.	N/A
Minimum UNCHECKED	If the minimum is NOT selected, then people can only pass through the door(s) in pairs, but any number of pairs can go though.	Two-Person Rule is not in effect. Any number of persons can enter or leave an area at any time.

K.5 FAQ

Q: Both Active and Minimum is checked. Can a third person enter a Two-Person area when it is already populated by two persons?

A: Yes.

Q: Both Active and Minimum is checked. Can one person leave a Two-Person area when it is populated by three or more persons?

A: Yes.

Q: Both Active and Minimum is checked. Can two persons leave a Two-Person area when it is populated by three persons?

A: No. In such a situation, there needs to be a minimum of two persons (or no persons at all) in the area at all times. Only a single person will not be allowed in such an area.

Q: Both Active and Minimum is checked. Can one person leave a Two-Person area when it is populated by two persons?

A; No. In such a situation, there needs to be a minimum of two persons (or no persons at all) in the area at all times. Only a single person will not be allowed in such an area.

Q: When both Active and Minimum is checked, how can the two persons in a Two-Person area leave the area?

A: They can leave together; only by presenting their cards to the door reader within a fixed default time period of 15 seconds.

Q: When Active is checked but Minimum is not checked, can a single person enter or leave the area even when there are three or more persons present?

A: No. In that situation, people can only pass through the door in pairs even though any number of pairs can go in or out of the area.

Q: Can persons enter an area from one door and leave it from another? In such a situation, will the Two-Person Rule still be enforced?

A: Yes because the cards in an area are tracked not by the door(s) or the reader(s) but by the panel that controls the area.

Q: What happens when a third person slips out of an area, walking right behind the pair of persons that leave it?

A: Since the third person did not swipe the card at the reader, the controller will think that person is still inside the area. Thus when that person tries to

present his card at another reader and enter a second area, he will be denied access since the controller will think he is still inside the first area.

K.6 Test Your Understanding

(Answers are at the end of this quiz section.)

1. For the Two-Person rule to work, how many Mercury panels should be controlling all the readers in the area?

    a. 1

    b. 2

    c. 4

    d. 8

2. Imagine both Active and Minimum is checked. Can two persons leave a Two-Person area when it is populated by three persons?

    a. Yes

    b. No

3. The Two-Person rule applies to which of the following data objects?

    a. Company

    b. Class

    c. Partition

    d. Area

4. For the Two-Person rule to work, what is the time period during which two persons must present their cards to a reader?

    a. 5 second

    b. 15 seconds

    c. 45 seconds

    d. 120 seconds

5. Imagine both Active and Minimum is checked. Can a third person enter a Two-Person area when it is already populated by two persons?

    a. Yes

    b. No

6. For the Two-Person Rule to work, there needs to be only a single door leading in and out of the area.

    a. True

b. False

K.6.1 Answers to “Test Your Knowledge” Quiz

1. A
2. B
3. D
4. B
5. A
6. B

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

PW5K Conversion Utility

L

In this appendix...

Overview
Adding “PW5K Conversion Utility” Registry Key
Granting the Functionality

L.1 Overview

"**PW5K Conversion Utility**” tool enables the user to preserve all reader settings and other configuration information when the PW-5000 panel is replaced by a PW-6000 panel.

Without this utility, the user would have to delete and rebuild all readers together with their respective clearance codes and other related configuration information.

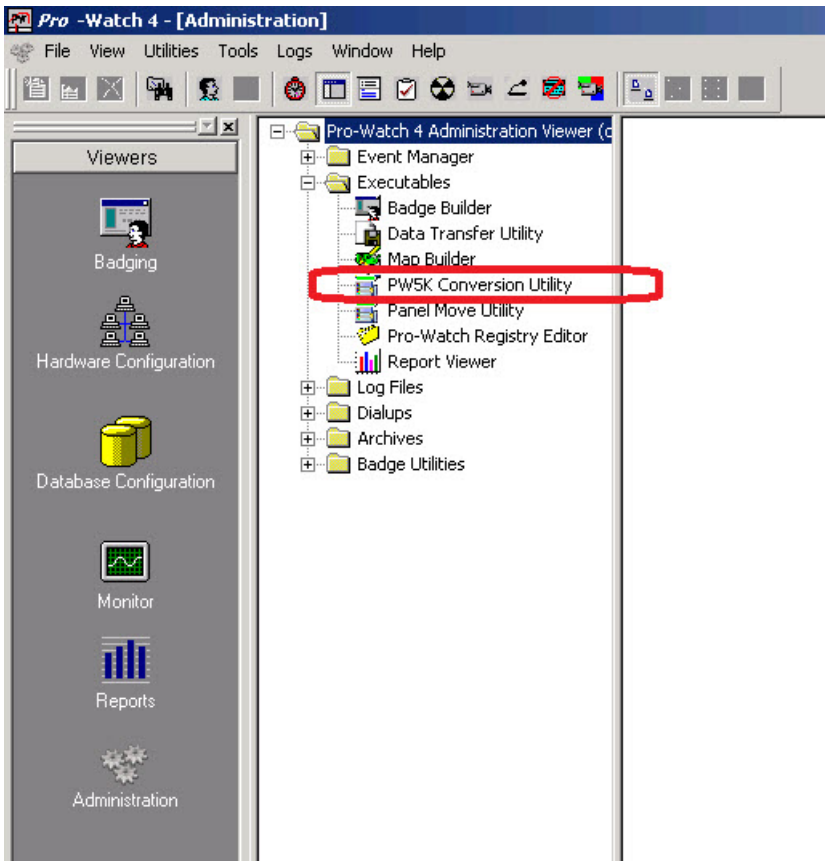
When the user runs this utility, Pro-Watch recognizes the new PW-6000 panel with all the configuration settings that existed before. This saves the user from many hours of repeated effort that would be necessary to enter the site's configuration information from scratch.

To enable and use this utility, you need to perform two separate actions, which are explained in the rest of this appendix:

1. Add the “PW5K Conversion Utility” key to the MICUtils subdirectory in Registery to make the utility visible.
2. Grant the functionality in the Pro-Watch User Edit screen.

L.2 Adding "PW5K Conversion Utility" Registry Key

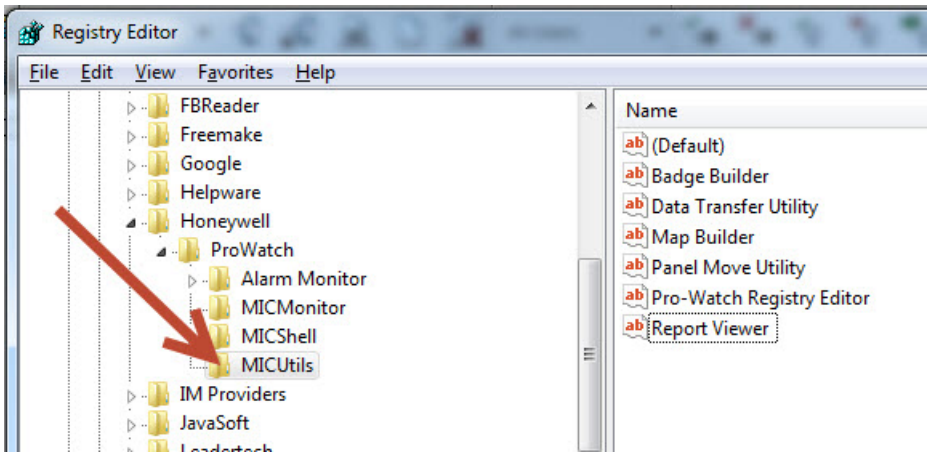
The "**PW5K Conversion Utility**" should be visible in Pro-Watch's **Administration** module, under the **Executables** directory, as follows:



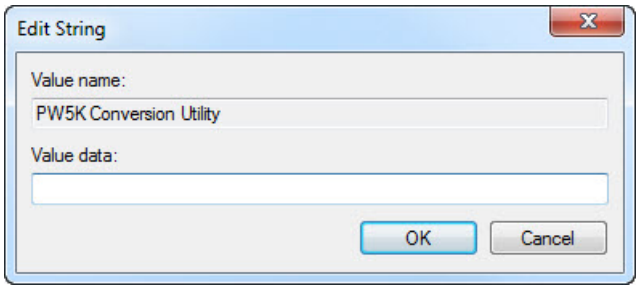
If the utility is not visible, follow these steps to add the "PW5K Conversion Utility" key to the MICUtils subdirectory in the Registry:

1. Go to **Start > Run**.
2. Type "**regedit**" and click **OK** in the Run dialog to display the **Registry Editor** screen.
3. In the Registry Editor, go to "**Software**" under HKEY_CURRENT_USER.
4. Under "Software," go to "**Honeywell**."
5. Under "Honeywell," find "**Pro-Watch**."

6. In Pro-Watch, go to the **MICUtils subdirectory** as shown below:



7. On the right pane, right-click and from the pop-up menu select **New > String Value**. A new key with temporary name "**New Value #1**" is created.
8. Right-click on "**New Value #1**" and from the pop-up menu select **Rename**. Type in "**PW5K Conversion Utility**".
9. Double click "**PW5K Conversion Utility"** to display the **Edit** screen:



10. In the **Value data** field enter "**PW5KConverter.exe**". Click **OK**.
11. Close the **Registry Editor.**
12. Close and re-launch the **Pro-Watch**.

L.3 Granting the Functionality

1. In Pro-Watch, select the **Database Configuration** module.
2. Click the **Users**. Then double-click the icon of your preferred user to display the **Edit Users** screen.
3. Click and select the **Programs** tab.
4. In the **Programs** tab, click and expand the **Administration** sub-directory.
5. Under the **Administration** sub-directory, click and expand the **Administrative Viewer** sub-subdirectory.

6. Under the **Administrative Viewer** sub-subdirectory, if the "PW5K to PW6K Conversion Utility" is there, click and select the **PW5K Utility**. If it is not in the list, you have to select the **Add Function** button and add the "PW5K to PW6K Conversion Utility".
7. Click the **GRANT** button on the right sidebar to grant the functionality.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Partition Manager

M

In this appendix...

Overview
Running the Partition Manager
Partition Management Layout
Assigning Partitions
Unassigning Partitions and Objects

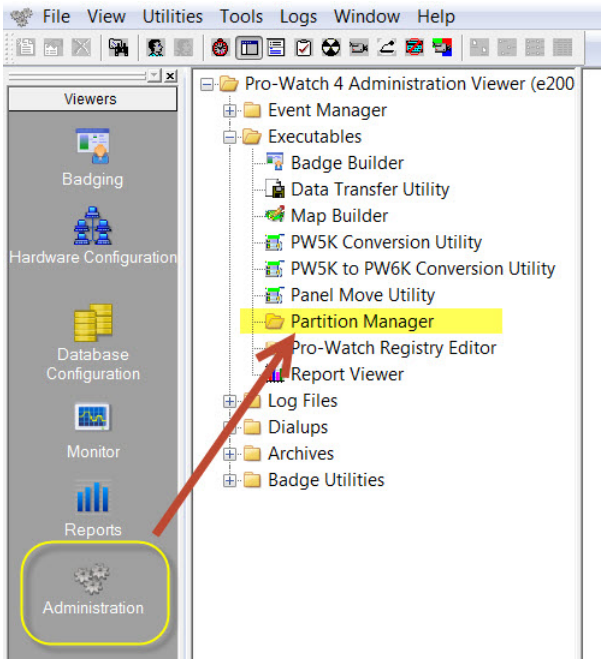
M.1 Overview

The Partition Manager utility is used to assign partitions to and unassign partitions from Pro-Watch database configuration objects or selected site hardware. This tool will allow users to bulk-load objects into partitions as well as bulk-remove objects from partitions.

The users cannot create brand new partitions, or edit and delete them from Pro-Watch by using this utility; they can only assign and unassign the existing partitions. To create, edit or delete partitions see Chapter 53, DBC - Partitions.

M.2 Running the Partition Manager

Users can run the Partition Manager by starting the **Partition Manager executable** from the **Executables** list in the **Administration** pane:



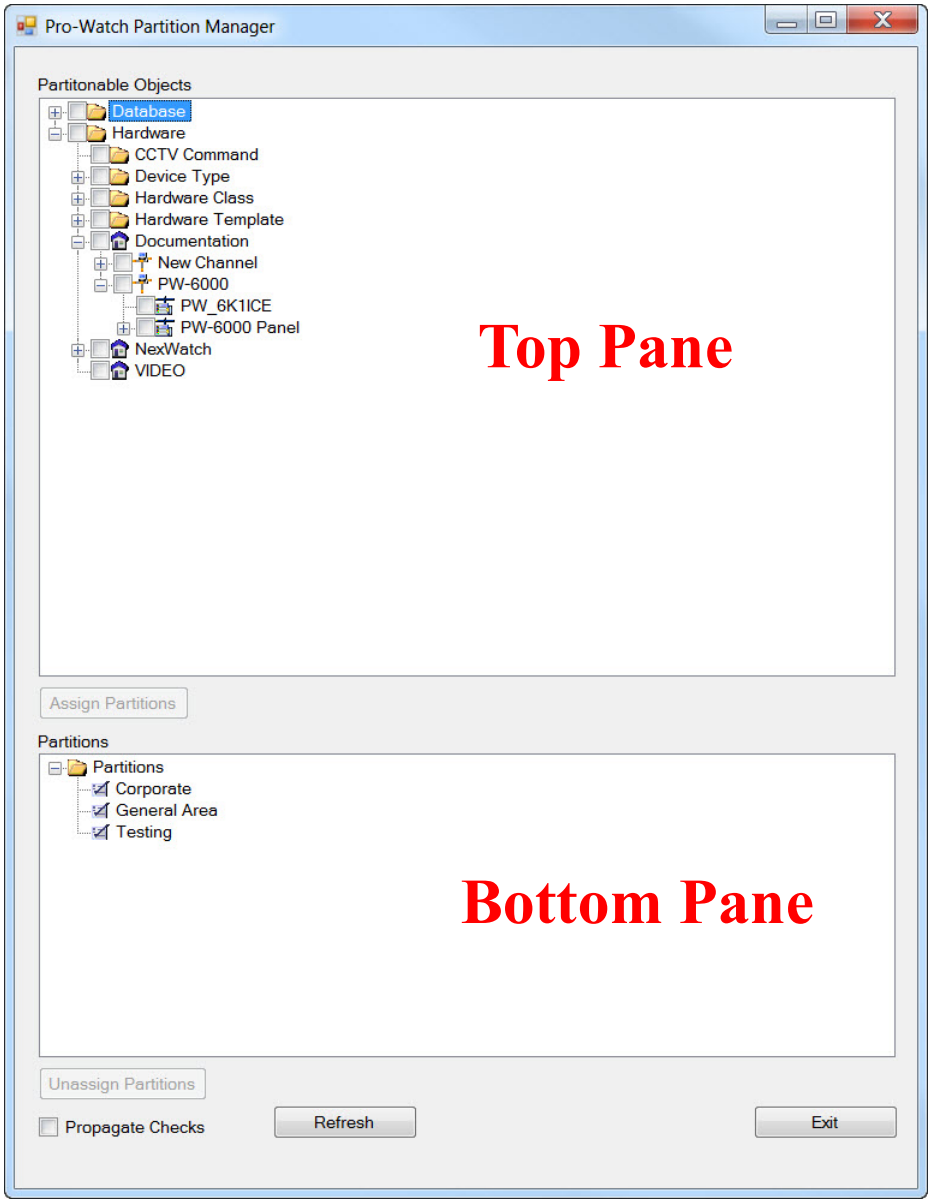
If the Partition Manager executable is missing from the Executables list, then it may need to be added manually. To add the Partition Manager manually:

1. Right-click on the **Executables** node.
2. Select **Add**. Type "**Partition Manager**" for the description and "PartitionManager.exe" for the **Command**.

Note: The tool can also be used by invoking **PartitionManager.exe** from the Pro-Watch bin directory.

M.3 Partition Management Layout

The Partition Manager is split into two panes.



The **top pane** displays the partitionable objects. It displays the database and hardware objects in a tree-view format.

The **bottom pane** is for unassigning partitions. Users can select a partition, click "**Unassign Partitions**" to display the objects assigned to that partition and pick and choose what objects to remove from that partition.

The "**Propogate Checks**" checkbox will only display when the user selects a partitionable object. This checkbox will fill in the check or uncheck action for all child nodes of the node being checked or unchecked.

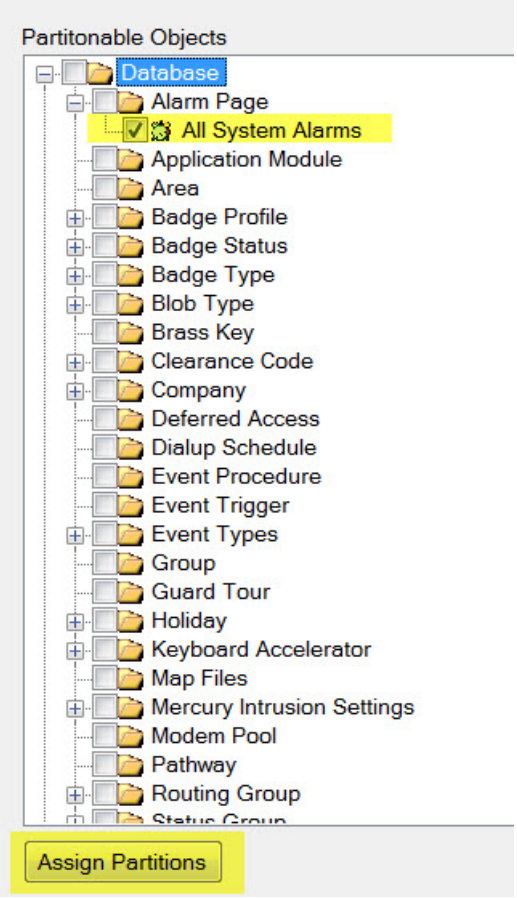
The "**Refresh**" button will refresh the tool and any changes made to the database since the Partition Manager was started via other means (i.e., Pro-Watch client).

The "**Exit**" button will exit out of the tool.

M.4 Assigning Partitions

To assign a partition to an object (or objects), select or deselect "**Propagate Checks**" check-box and select any elements that will be partitioned.

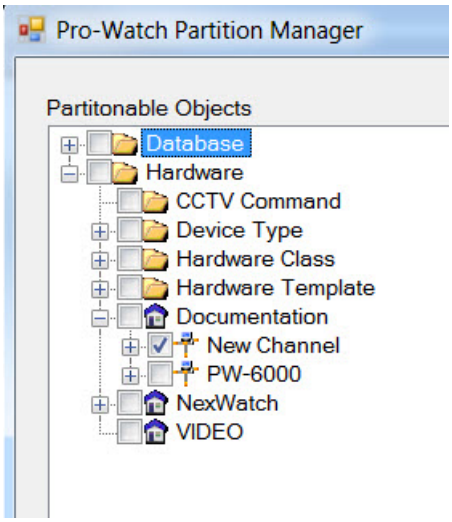
Note: The user must select a valid object for the "**Assign Partitions**" button to be enabled, as shown below:



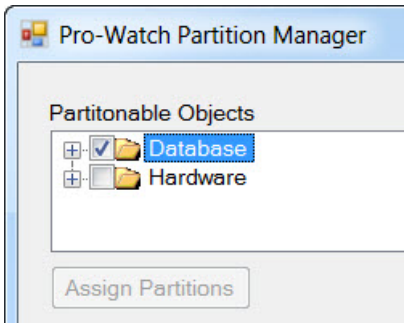
Follow these steps:

1. Run the **Partition Manager** executable from the Executables list under the Pro-Watch **Administration** pane.

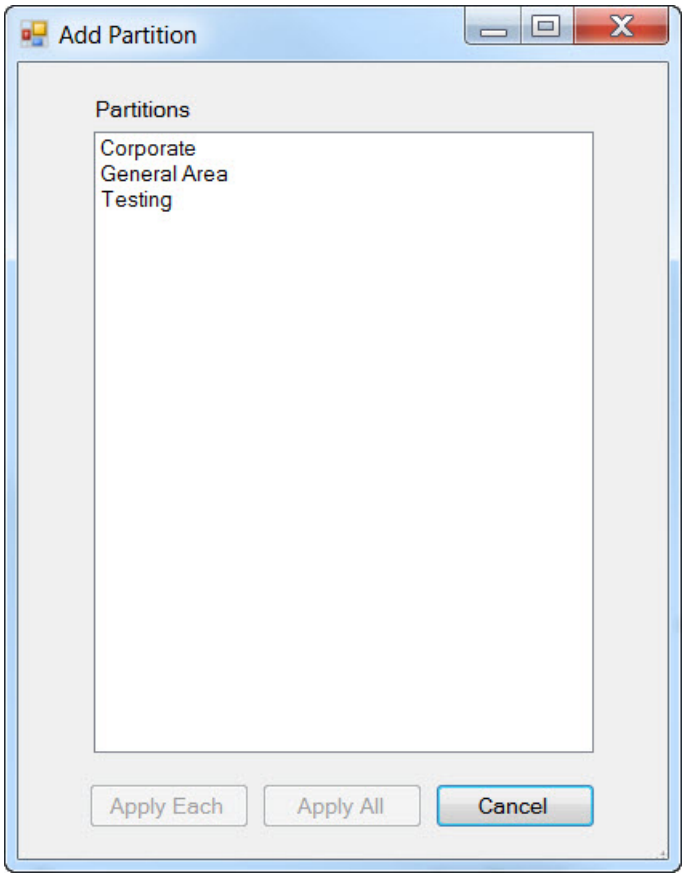
2. Click and display the **Database** or **Hardware** tree-view and select the objects to assign to a partition(s) by selecting its check box:



Note: If "**Propagate Checks**" check-box is unchecked, the user will still be able to select folders. This is inconsequential because the "**Assign Partitions**" check-box will not be enabled until a valid object is selected, as shown below:

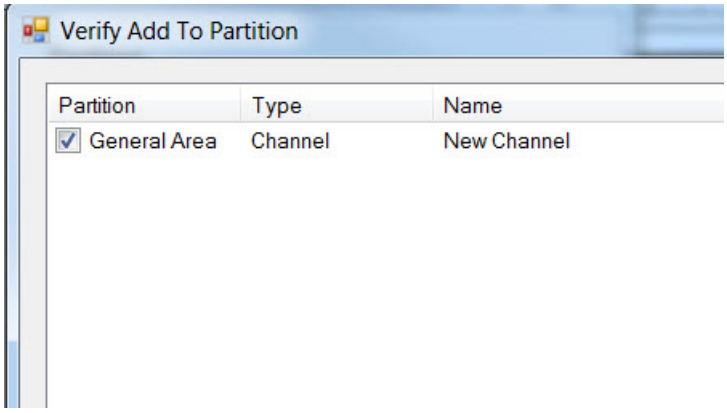


3. Click **Assign Partitions** button to display the **Add Partition** page:

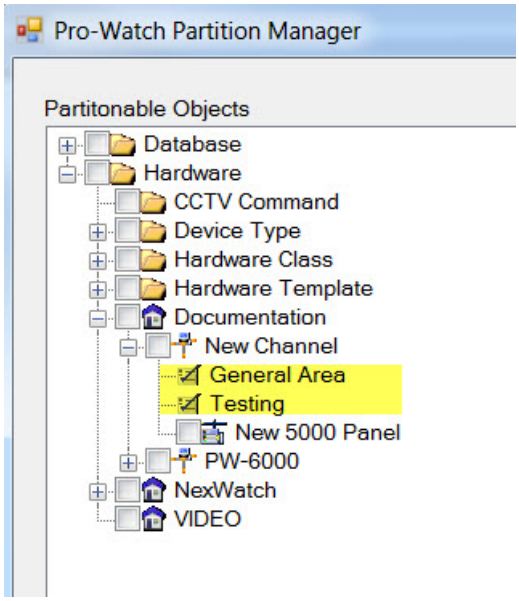


Note: **Multiple partitions** can be selected by using **Ctrl+select** or **Shift+select** method.

4. Select the Partition(s) to assign and click either **Apply Each** (for a single selected partition) or **Apply All** (for multiple selected partitions) button to display the **Verify Add to Partition** page:



5. Click **Add** to assign the partition(s) to the desired objects. In Partition Manager, the assigned partitions for an object will be displayed under the object in the tree-view:



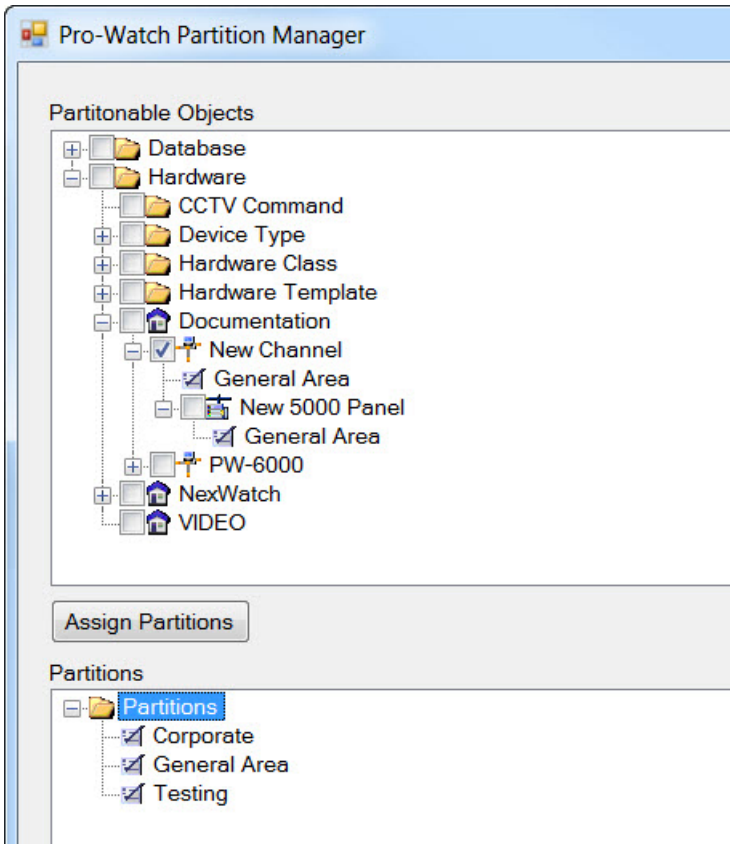
M.4.1 Already Assigned Partitions

M.4.1.1 Case 1: Single Partition Selected

If a partition is already assigned to an object, the user will still see the assigned partition when selecting "**Assign Partitions**."

However, if the already assigned partition is selected to be added again, the Partition Manager will display an error message "Partition is already assigned to an object."

For example, let's assume that the partition "**General Area**" is already assigned to **Documentation > New Channel** object, as shown below:



If the user tires to assign the same partition (General Area) to the same object (New Channel), Pro-Watch will issue the following error screen:



M.4.1.2 Case 2: Multiple Partitions Selected

If the user selects multiple partitions and only some of them have been assigned to the object, the Partition Manager will display an error message for each occurrence of the duplicate partition.

However, partitions included that are not assigned to the object will be added to the object.

For example: If partitions P1 and P2 are assigned to MyBadgeProfile and user adds partitions P1, P2, P3, and P4 to MyBadgeProfile, two things will happen:

1. Partition Manager will display 2 error messages for duplicate partitions P1 and P2.
2. Partition Manager will assign partitions P3 and P4 to MyBadgeProfile.

M.5 Unassigning Partitions and Objects

M.5.1 Unassigning Partitions Directly from the Object

If the user expands the Database or Hardware node tree-view, the assigned partitions for an object will be displayed under the object.

1. Click on that single partition to unassign the single partition from the object.
2. Click the **Unassign Partitions** button to display the **Remove from Partitions** screen.
3. Verify removal selection and click the **Remove** button. Partition Manager will refresh and the partition will be removed from the object.

M.5.2 Unassigning Objects from the Partition

If the user goes into the bottom pane and directly selects a partition, clicking on the **Unassign Partitions** button will bring up all the database or hardware objects assigned to that partition in the **Remove from Partition** page.

Select the objects to remove from the partition and click the **Remove** button. Partition Manager will refresh and the partition will be removed from the object(s).

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Registry Management

N

In this appendix...

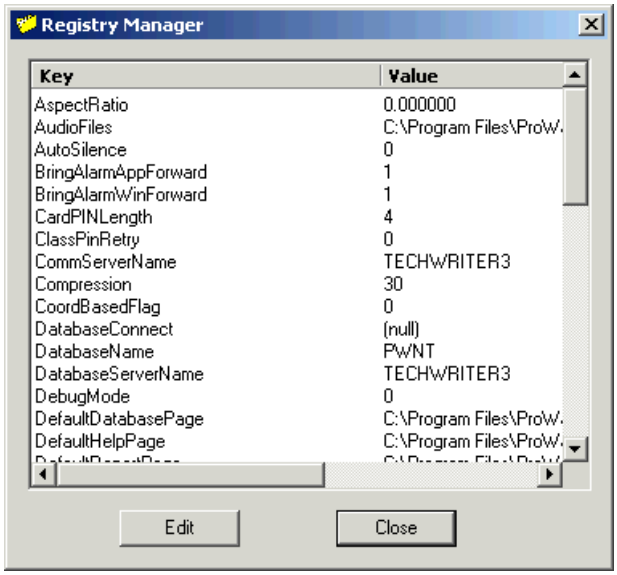
Overview
Editing the Registry Manager

N.1 Overview

Use the Registry Manager to edit Pro-Watch's registry key values.

To access the Registry Manager:

1. From the left Pro-Watch pane, click **Administration**.
2. Click the plus mark "**+**" in front of the **Executables** folder to expand it.
3. Double-click the **Pro-Watch Registry Editor** icon to display the Registry Manager dialog box:



Note: Only users with administrative privileges can access the Registry Editor through Pro-Watch. Non-administrative users cannot access the Registry Editor through Pro-Watch.

N.2 Editing the Registry Manager

Follow these steps:

1. Click to select a key name, and click **Edit**. Or, double-click the key name. The Value dialog box appears.
2. Enter a value for the key field.
3. Click **OK** to save.
4. Click **Close** in the Registry Manager dialog box.

Warning: Before you make any changes in the Registry Manager, it is strongly recommended that you make a handwritten note of the value you intend to change for a given registry key. Then, you can restore that value if necessary.

The below table lists the key and value entries contained in the Registry Manager:

Table N-1 Registry Manager Fields, Functions and Sample Values

Field	Function	Sample Value
AudioFiles	Specifies the default auto file directory for Alarm Monitor.	C:\Program Files\Pro-Watch\audio\
AutoSilence	Deactivates outputs linked to alarms.	0 Only values 0, 1, and 2 are valid: 0 = disabled, 1 = deactivate a linked output on an ACK of an input alarm event, and 2 = deactivate a linked output on a CLEAR.
BringAlarmAppForward	Brings the Alarm Monitor application forward on a new alarm.	0 0 = Not, 1 = Bring forward.
BringAlarmWinForward	Brings the Alarm Monitor window forward on a new alarm.	0 0 = Not, 1 = Bring forward.
CardPINLength	Indicates the number of PIN digits; defaults to 4 when Pro-Watch is installed. The value of this registry key is then set in the Badge Profile screen under Badging. It is strongly recommended that you NEVER manually change this value within this Registry, and that you always set it using the Card Information Page.	4 The range is 4-20. Use the Card Information Page to set this value.

Table N-1 Registry Manager Fields, Functions and Sample Values

Field	Function	Sample Value
ClassPinRetry	Indicates the number of PIN retries. The PIN code is checked per class setting if the user PIN code checking is deferred to Class.	1 0 = no PIN code checking dialog box, 1 = one retry, and so on.
CommServerName	Specifies the PC name of the machine running as the Pro-Watch server.	In a redundant server architecture[a], this is the name of the Primary Server, even if the PC name is a remote server as well as a client.
DataBaseConnect	Specifies the name of resource configuration table.	[Null] If the value is null, then CONFIGTYPE is used. This is only used by developers when adding new resources.
DatabaseName	Specifies the name of the Pro-Watch database.	PWNT You can switch between two or more Pro-Watch databases with different names.
DatabaseServerName	Specifies the PC name of the Pro-Watch database server.	Any valid name that is the name for the PC on which the Pro-Watch database server resides.
DebugMode	Specifies a key that can enable the PW-5000 debug file and the *.adm log files. A value greater than 0 enables the files. Only programmers should use this key.	0

Table N-1 Registry Manager Fields, Functions and Sample Values

Field	Function	Sample Value
DefaultDatabasePage	Displays the URL of a web page or file in the Database Viewer when the top level of the tree is selected.	C:\Program Files\Pro-Watch\bin\Pro-Watch NT.htm
DefaultHelpPage	Displays the URL of a web page or file in the Help Viewer when the top level of the tree is selected.	C:\Program Files\Pro-Watch\help\Pro-Watch NT Help.htm
DefaultReportPage	Displays the URL of a web page or file in the Reports Viewer when the top level of the tree is selected.	C:\Program Files\Pro-Watch\bin\index.html
DefaultViewerList	Indicates how the list is to be displayed in the Viewer.	3 0 = Large Icons, 1 = Details, 2 = Small Icons, 3 = List
DefaultZoomAll	Sets an AutoCAD image to zoom to fit in the Map page of the Alarm Monitor and Map Builder during startup.	0 0 = no zoom, 1 = zoom to fit
Display Splash	Displays or does not display the splash screen on debug build.	0 0 = no, 1 = yes
ExeFiles	Specifies the Pro-Watch executable directory.	C:\Program Files\Pro-Watch\bin\
FirmwareFile	Specifies the PW-5000 firmware file name.	C:\Program Files\ProWatch\Firmware\ PW_5K\

Table N-1 Registry Manager Fields, Functions and Sample Values

Field	Function	Sample Value
Helpfile	Specifies the help file name for displaying help.	C:\Program Files\ProWatch\Help\
InstallDir	Specifies the main application install directory.	C:\Program Files\Pro-Watch\
MapFiles	Specifies the default directory for alarm maps.	C:\Program Files\PW-5000\maps\
MaxBadgeDisplay	Specifies the maximum number of badges to display on default initial search when the user opens the badge module.	200 0 = disabled; numbers over 200 will cause increasing delays in Pro-Watch throughput.
MaxTranDisplay	Specifies the maximum number of events to display in the Event Viewer.	200 0 = disabled; numbers over 200 will cause increasing delays in Pro-Watch throughput.
New Alarm Timer	Sets the number of seconds between beeps on the Alarm Monitor when there are unacknowledged alarms.	0 0 = constant beeping, 1 = beep once per second, etc.
Package Directory	Specifies the package file (*.pkg) install directory. Usually this is the InstallDir.	C:\Program Files\Pro-Watch\bin\
PictureFiles	Specifies the status icon default directory.	c:\BADGES\

Table N-1 Registry Manager Fields, Functions and Sample Values

Field	Function	Sample Value
PW-3000 firmware file	Specifies the PW-3000 firmware file name (applies only to Pro-Watch Version 3, Release 5).	[null]
RefreshTzOnReEnable	When its value is "1", this registry key re-enables the override time zone for a door (in which the door unlocks). The specific value of this time zone is configured in the Advanced Settings sub-tab, reached through the Logical Device Details tab of the PW-5000 panel editing screen. To toggle between (the default value) "0" and "1," select the RefreshTzOnReEnable key in the Registry Manager screen and click Edit to display the Value screen. Enter "1" and click OK.	0

Table N-1 Registry Manager Fields, Functions and Sample Values

Field	Function	Sample Value
ReportEventsOnUnusedHardware	Pro-Watch, by default, will not report events on unused Input, Output and Reader hardware - unless they are a part of a logical device. Sub-panel events, as well as the events on any other hardware type, are reported regardless of logical device membership. However, some sites may need event reporting on the unused hardware for a variety of reasons. A user can do so by configuring this registry setting (under Options).	When the (default) value of this numeric field is 0 (zero), the events on the unused hardware will not be reported. To report the events on the unused hardware, change the value to 1 (one). **Note:** You do not need to restart the Pro-Watch for this registry change to take effect.
SubpanelFirmware	Names the subpanelFirmware file.	C:\Program Files\ProWatch\Firmware\ PW_SubPanel\
Toolbar file	Names the toolbar file default directory.	C:\Program Files\Pro-Watch\resource\
User PIN Retry	Indicates the allowable number of PIN retries. This PIN is based on the User settings.	1 0 = no PIN code checking dialog box, 1 = one retry, and so on.
Video Player	Names the video player for AVI or other video files.	mplay3P1.2.exe

a. Redundancy is not supported in Pro-Watch Lite.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Galaxy Dimension Integration Guide

O

In this appendix...

Overview
Required Galaxy Configuration parameters
Configuring Pro-Watch
Creating the Galaxy Dimension Panel
Uploading the Galaxy Configuration Into Pro-Watch
Create Event Procedures
Enabling Galaxy Components
Badgeholder Operation Permissions
Managing Galaxy Users
The Arm/Disarm Mechanism
New Trigger Options
New Pro-Watch Registry Keys
Process Flowchart
Pro-Watch Icons
Backup and Restoring a Galaxy Database Using RSS
Functional Testing

O.1 Overview

This appendix describes the steps needed to successfully configure Pro-Watch® to support Galaxy Dimension Intrusion panels. It does not detail the full setup for Galaxy Dimension panels, but provides information for the setup of the communication parameters within the Galaxy panel.

O.1.1 Audience

This appendix is intended for qualified Pro-Watch engineers, with in-depth knowledge of the Galaxy Dimension series intrusion panels.

O.1.2 Installation Pre-requisites

The following components as a minimum are required for the integration:

- Operational Pro-Watch® PE or CE Suite 3.81 build 8359 or higher
- The "Galaxy" option must be supported by the Pro-Watch license.
- A Galaxy Dimension GD-XXX Panel (minimum firmware 6.01 or higher)
- A Galaxy Dimension E080 Ethernet card (minimum firmware 2.08 or higher)
- A Galaxy Dimension E080-4 Ethernet card (from initial released firmware)
- Functional TCP/IP network.

Caution: For an updated list of minimum required firmware please consult “Pro-Watch Eco-System Compatibility Matrix and System Dependencies” document (800-07545V10).

O.1.3 Integration Overview

With the Pro-Watch - Galaxy Dimension integration, Pro-Watch user are able to control and monitor Group and zone status using the Pro-Watch client, and control the individual Galaxy Zones and Groups using Pro-Watch Access control credentials. Depending on the combined Galaxy user profiles and access permissions defined in Pro-Watch, a Pro-Watch cardholder is allowed or denied permission to arm/disarm zones and groups.

The Access control functionality of the Galaxy panel is disabled when the integration is operational.

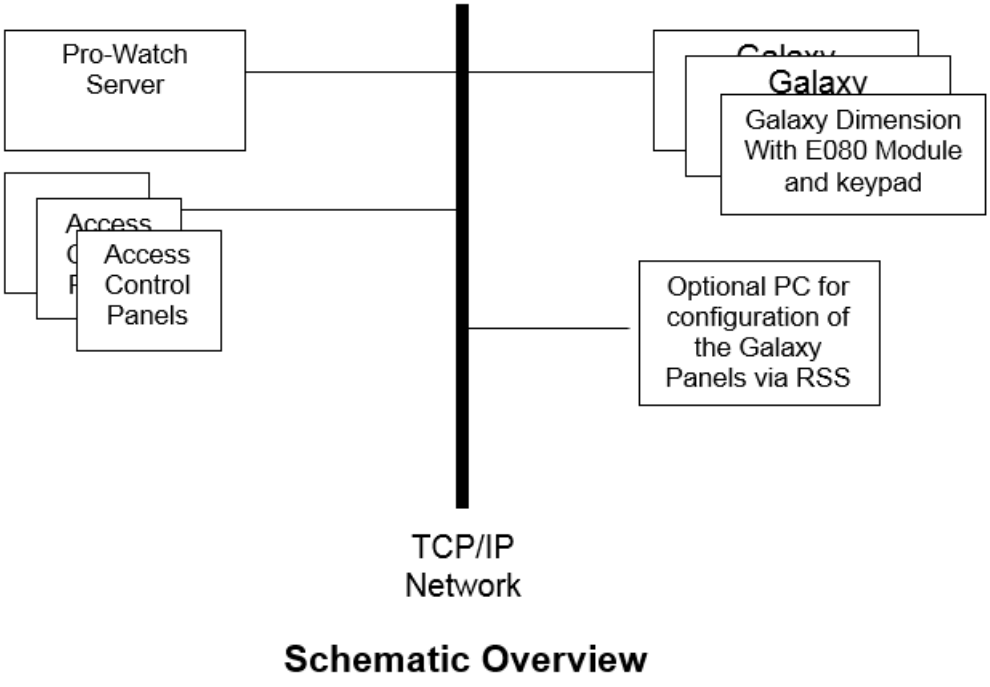


Figure O-1 Schematic Overview

O.2 Required Galaxy Configuration parameters

In order to program the Galaxy Dimension panel for communication with the Pro-Watch channel, the following parameters must be set;

To do this, enter the Galaxy Dimension panel programming interface using the engineer's code, and select and edit the following menu items;

Menu #	Description	Sub-menu	Value
56-04-01	Module Config	-01 IP Address	Enter IP address of the GD080 module.
		-02 Site name	Enter a description for this panel
		-03 Gateway IP	Enter the IP address of the gateway if needed.
		-04 Subnet mask	Enter the subnet mask to be used.
56-04-02	Alarm Report	-01 Format	Select SIA 4 *
		-02.01 Primary IP	Enter IP address of the Pro-Watch server.
		-04 Client number	Enter a value example “543210”
		-06.04 Port Number	Default 10002 **
		-08 Protocol	SIA Control, Change to “TCP”
56-04-03	Remote access	-01 Access Period	Select “Any time”
		-02 Mode	Select “Direct”
56-04-08	SIA Control		Enter Pro-Watch Server IP address

This concludes the setup of the communication parameters for the Galaxy Dimension panel.

*** Note:** As the SIA4 Protocol is used to retrieve the hardware status from the panel. Status changes on the panel will display delayed in Pro-Watch when the panel groups are in disarmed state. When armed, the panel will initiate transmission of the alarm event immediately to Pro-Watch.

**** Note:** The default port number 10002 must be changed when more than 1 Galaxy panel is to be

connected. Each Galaxy Dimension Panel must communicate on a dedicated

"Default Alarm" TCP/IP port.

Tip: As TCP/IP ports are usually governed by a firewall product, and exclusion must be added to the firewall filter setup to allow the Galaxy panel to communicate to Pro-Watch.

Tip: To access the "Engineers Mode" use code "112233" <Enter>. In case this login is denied, then change the value under menu 48-01-01 and change engineer access to "1".

O.3 Configuring Pro-Watch

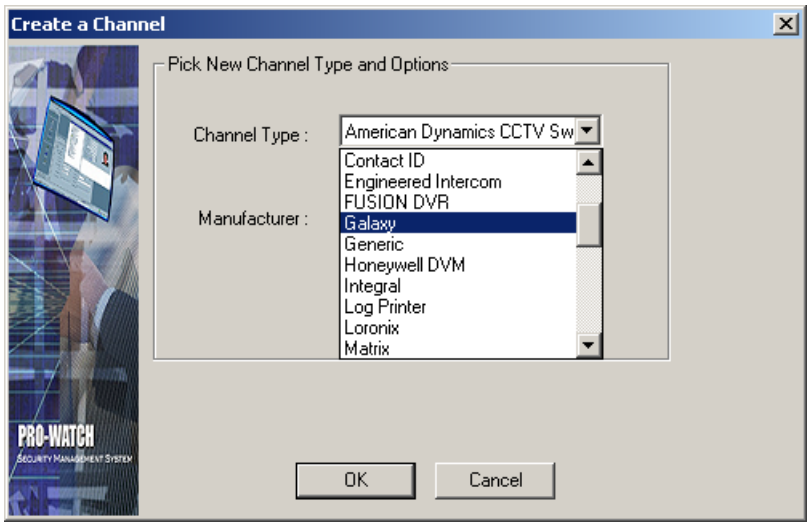
The configuration of Pro-Watch to integrate a Galaxy Dimension panel consists of the following steps:

1. Create the Galaxy Channel
2. Create the Galaxy Panel
3. Upload the configuration information into Pro-Watch
4. Create Event Procedures on Reader event #500 "Access Granted".

Additional steps for combining Pro-Watch functions with Galaxy functions are explained later in this document.

O.3.1 Creating a Galaxy Channel

1. From the Pro-Watch hardware configuration tree view, right-click and select "**New**" > "**Channel**" to display the "**Create a Channel**" dialog screen:

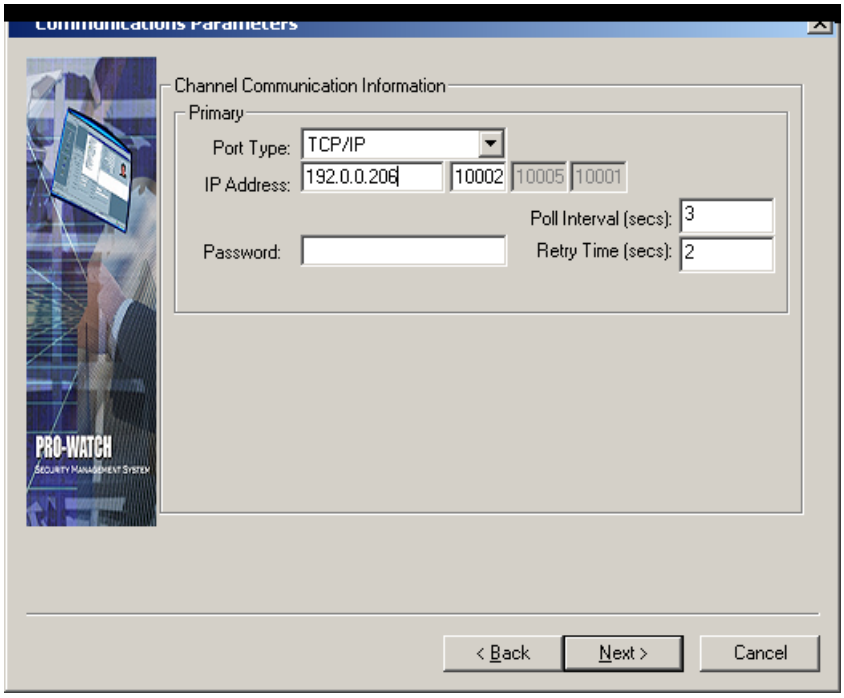


2. Select "**Galaxy**" from the channel type dropdown list.
3. Click "**OK**" to store the record, next the "**Define Channel Information**" screen will open. Enter an appropriate name for this channel. Click "**Next**" to configure the Communication Parameters.

*** Note:** If "Galaxy" is not shown in the "channel type" selection, the systems license dongle must be updated.

4. Select Port type: **TCP/IP**
5. Enter the IP address of the panels Ethernet interface.

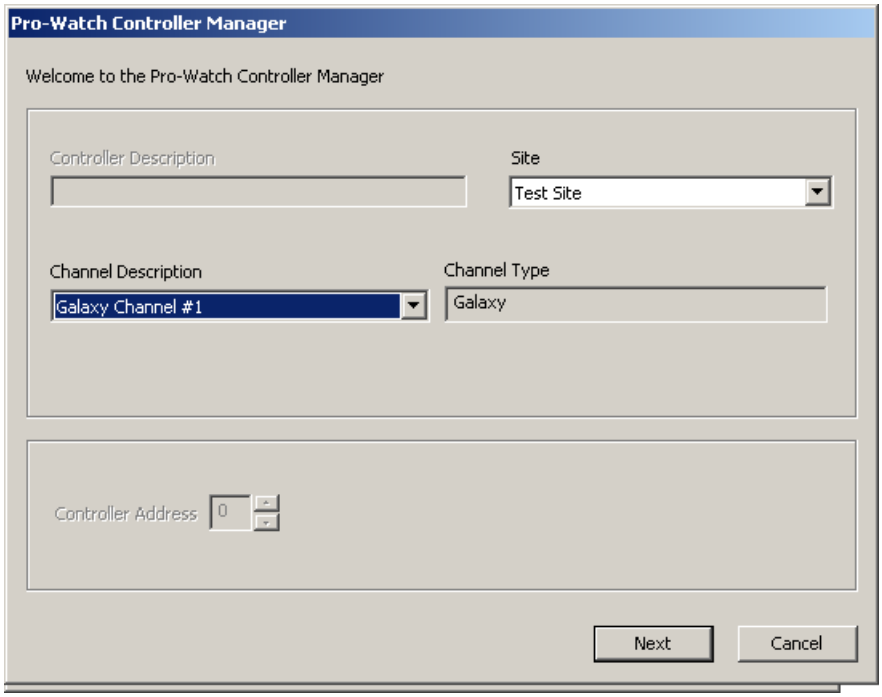
Caution: Leave the default IP port values as presented. Use the Pro-Watch registry editor for changing the Basic and alarm monitor ports (10001 and 10005)



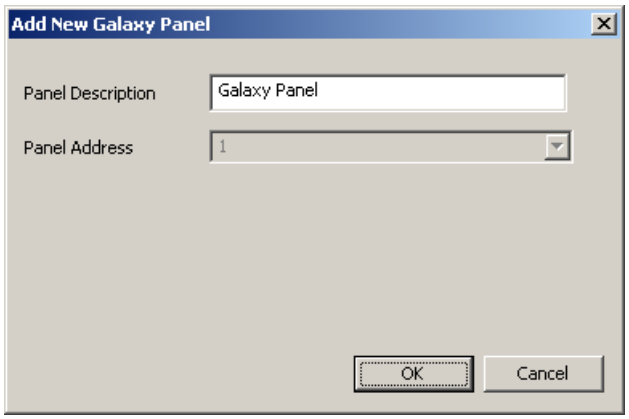
6. Click "**Next**" to save and close the record.

O.4 Creating the Galaxy Dimension Panel

1. From the Pro-Watch hardware configuration tree view, right-click and select "**New**" > "**Panel**" to display the "**Pro-Watch Controller Manager**" wizard:



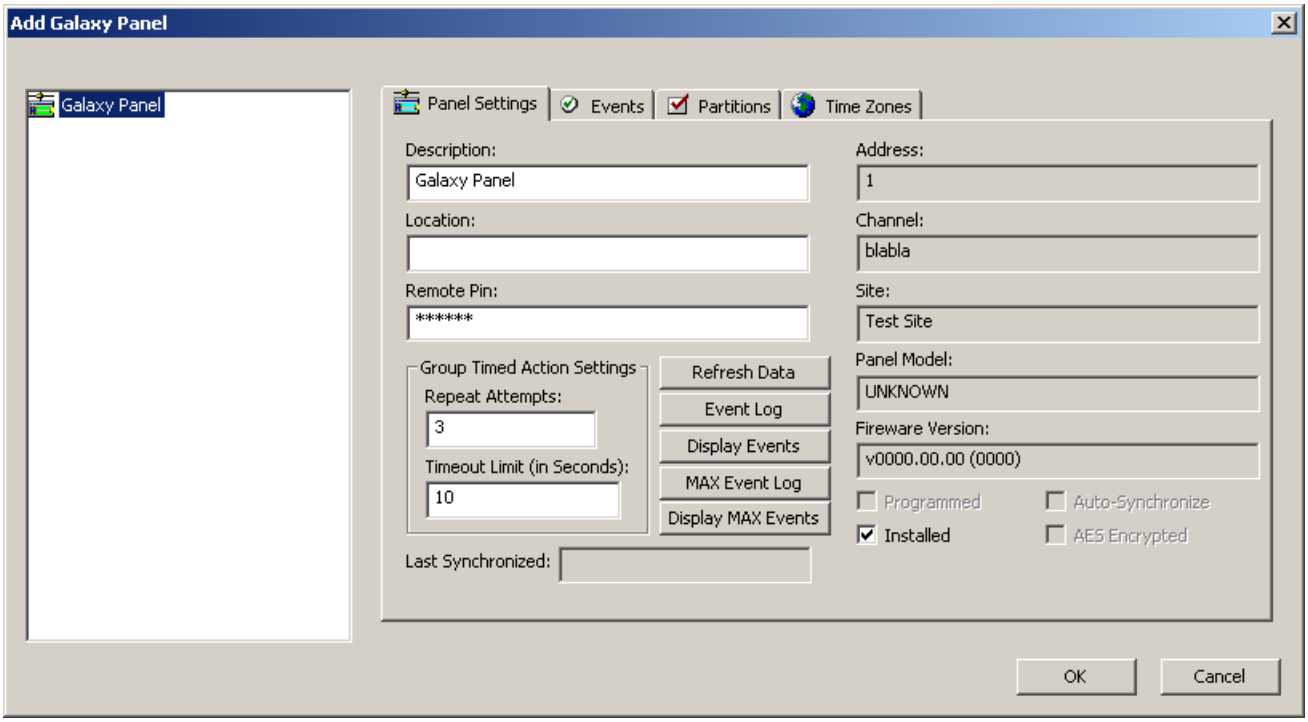
2. Select the **Galaxy channel** which was just created and select the "**Site**" this panel must be added to. The "**Add New Galaxy Panel**" screen will display:



3. Enter an appropriate description for this panel:

*** Note:** It is not possible to alter the panels address. As the Channel <> Panel communication is a Peer-to-Peer connection, no other address than "1" is needed.

4. Click "**OK**" to store the record. Next the "**Add Galaxy Panel**" screen will open. Make sure the "**Installed**" check-box is selected:



*** Note:** Do not change the "Remote Pin" code as this code can only be changed using RSS software connected to the panel. (Default 54321)

5. Click "**OK**" to store the record.

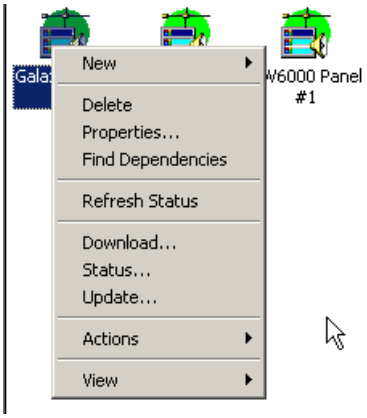
At this stage the necessary panel programming is completed. The remaining action is to upload the configuration from the panel into Pro-Watch.

*** Note:** Both the Channel and the Panel should now indicate "**Online**" status, indicated by the green icons. Do not proceed before the panel is online. Make sure not to leave the Galaxy panel in "**Engineer's mode**" before continuing with the next integration steps.

O.5 Uploading the Galaxy Configuration Into Pro-Watch

This step will upload all configuration information as programmed by the Galaxy engineer directly into the Galaxy Dimension panel. Once uploaded, the Pro-Watch user is capable to control the elements however it is not possible to change any programming from Pro-Watch.

1. Right click on the Galaxy Panel Icon and select "**Update**":



The "**Upload Galaxy Information**" screen will display.

2. Select the "**Update All**" check-box.

3. Click "**Send Upload request**".

The upload will start immediately, but will take considerable time to complete. The upload progress can be observed using the Pro-Watch event viewer's "**Download/upload messages**" tab.

Caution: The Panel should not be in engineer's mode, and no zones should be armed when attempting the upload. A warning will be displayed to the Pro-Watch user.

Once the panel upload finishes, all peripheral boards as programmed in the Galaxy panel will show in the "**Properties**" screen of the Panel.

Other information such as Users and permission will also be available in Pro-Watch.

Here are the Before-Upload and After-Upload screen-shots for your comparison:

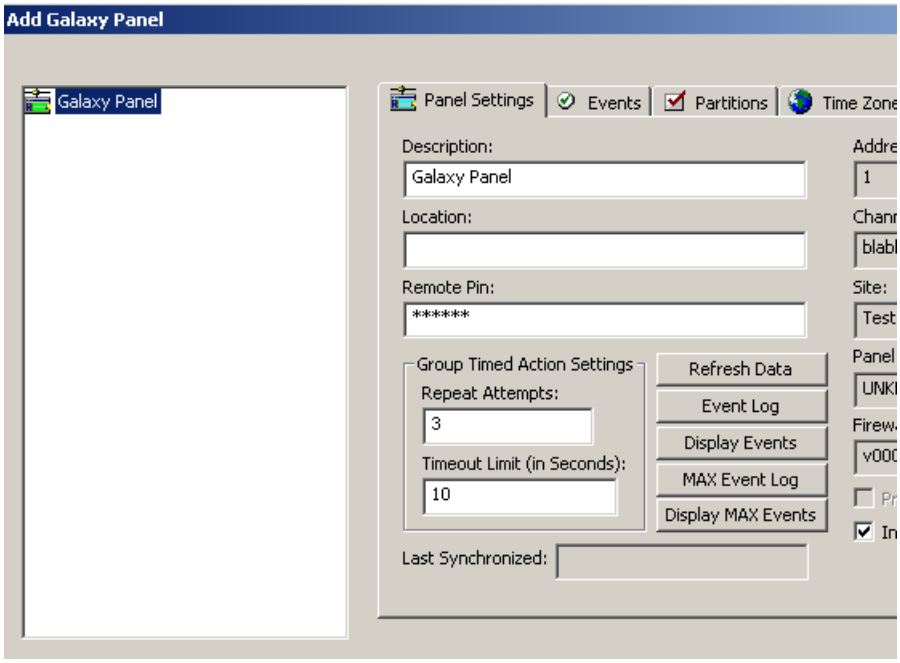


Figure O-2 Before Galaxy Upload

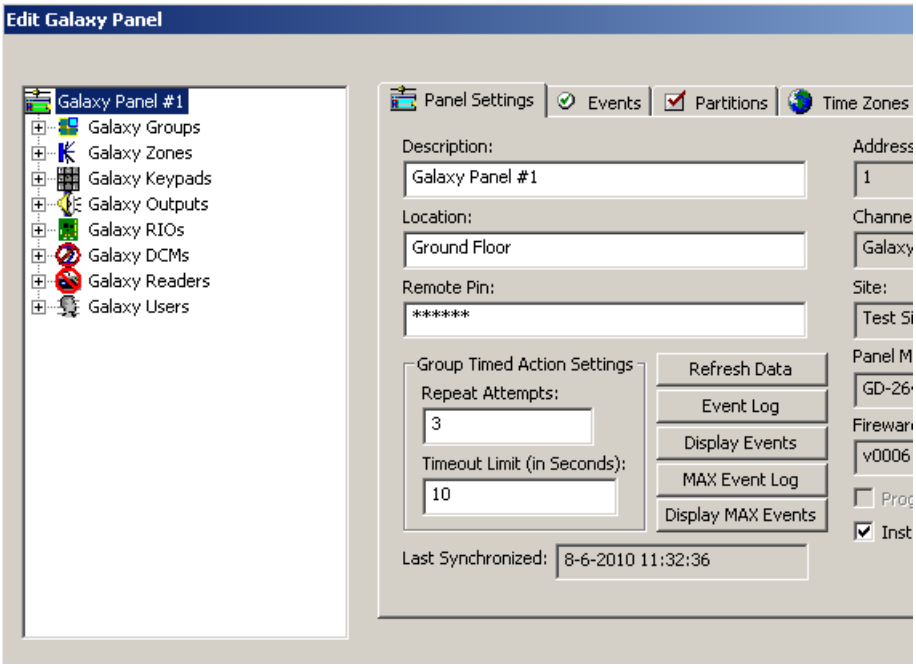


Figure O-3 After Galaxy Upload

This concludes step 3 in the integration process.

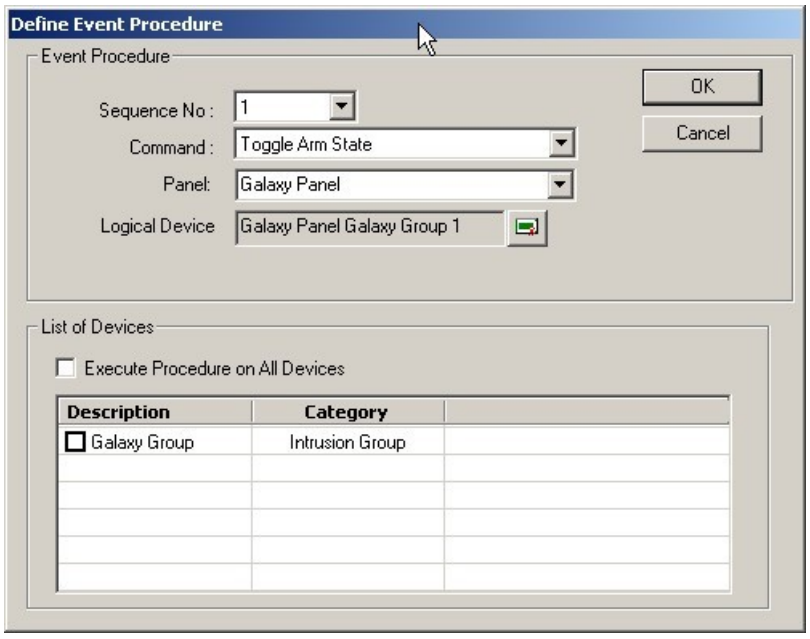
O.6 Create Event Procedures

In his step a procedure is created to allow Arming / Disarming Galaxy zones from Access control readers.

Each reader that will be used to perform arm/disarm tasks needs to trigger the Galaxy panel each time a specific transaction occurs, such as "Access Granted", or "Host Grant".

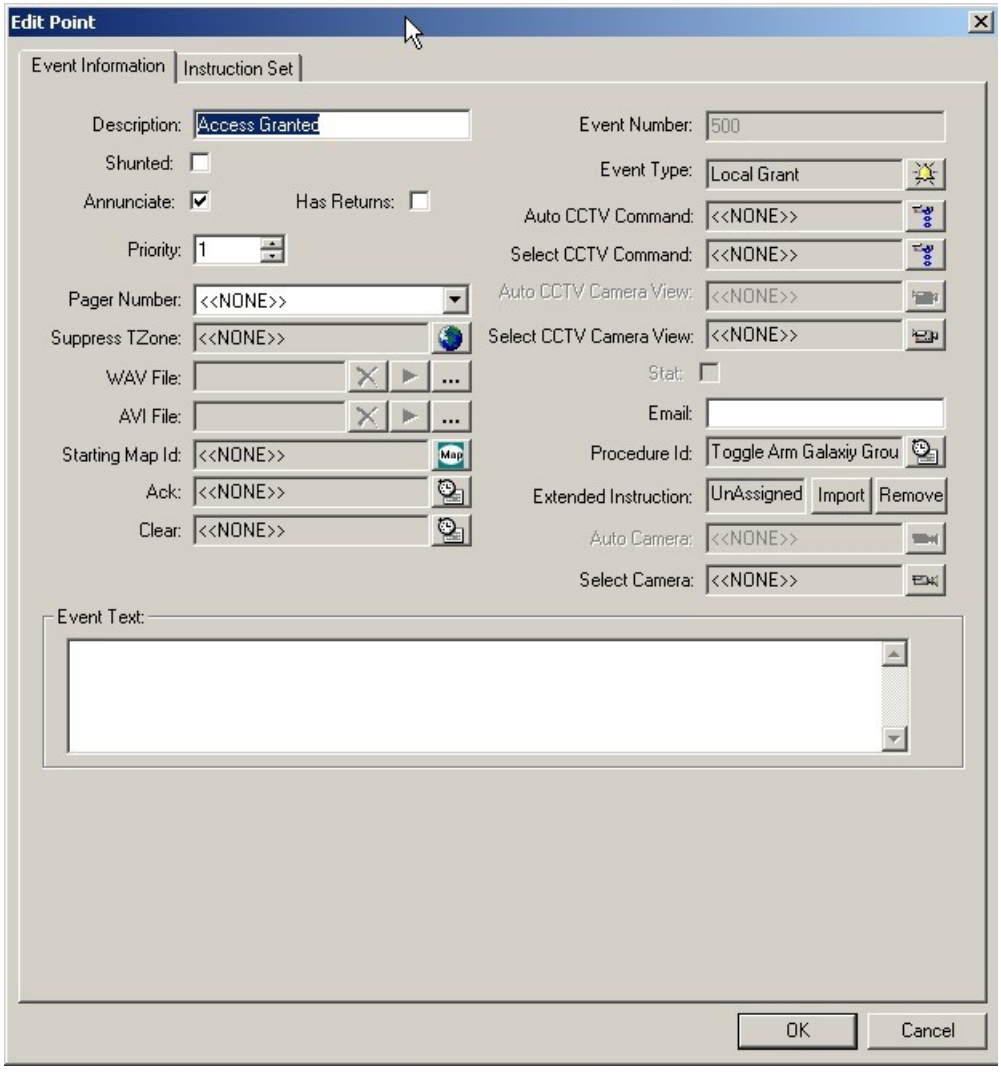
This requires the use of Procedures.

1. In Pro-Watch open "**Database Configuration**" and select "**Procedures**".
2. Click "**New Procedure**" to display the "**Define Event Procedure**" screen:



3. For the **Command** field, select "**Toggle Arm State**" from the drop-down menu.
4. For the **Panel** field, select the **Galaxy Dimension panel** of your choice from the drop-down menu.
5. Select the Galaxy group or Zone you wish to control. Multiple groups or zones can be programmed into the procedure.

6. Open the "**Logical Device**" tab of the reader to control the zone from and open "Events":



7. Select the events which will trigger the Arm/Disarm action. Logically "**Local Grant**" or "**Access Granted**" and "**Host Grant**" are available for use.
8. Add the new Procedure in the corresponding "**Procedure ID**" box.

In this example we used the "**Access Granted**" event. (Event code #500)

Repeat this action for as many Logical devices as needed.

This concludes the Pro-Watch Configuration

O.7 Enabling Galaxy Components

After the upload is finished all Galaxy system components such as RIO's, Zones, Keypads, Outputs, DCM's, Reader, and Users will show in the panel properties.

To be able to control and manipulate the Galaxy hardware components, it is essential to individually select which component will be available in the various logical device selection screens in Pro-Watch.

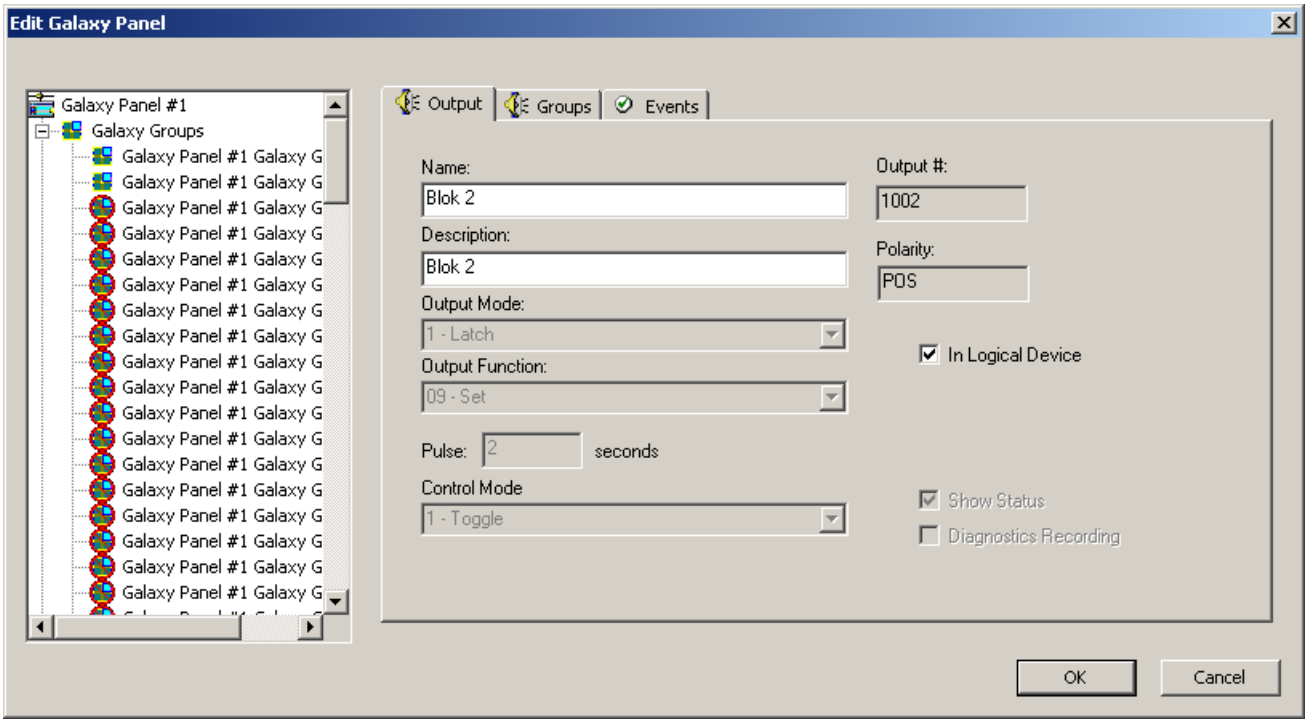


Figure O-4 Galaxy Panel Properties

For each individual hardware component the check mark "In logical Device" must be checked. This will cause this element to be available in all Logical Device look-up fields or selection menus in the Pro-Watch suite.

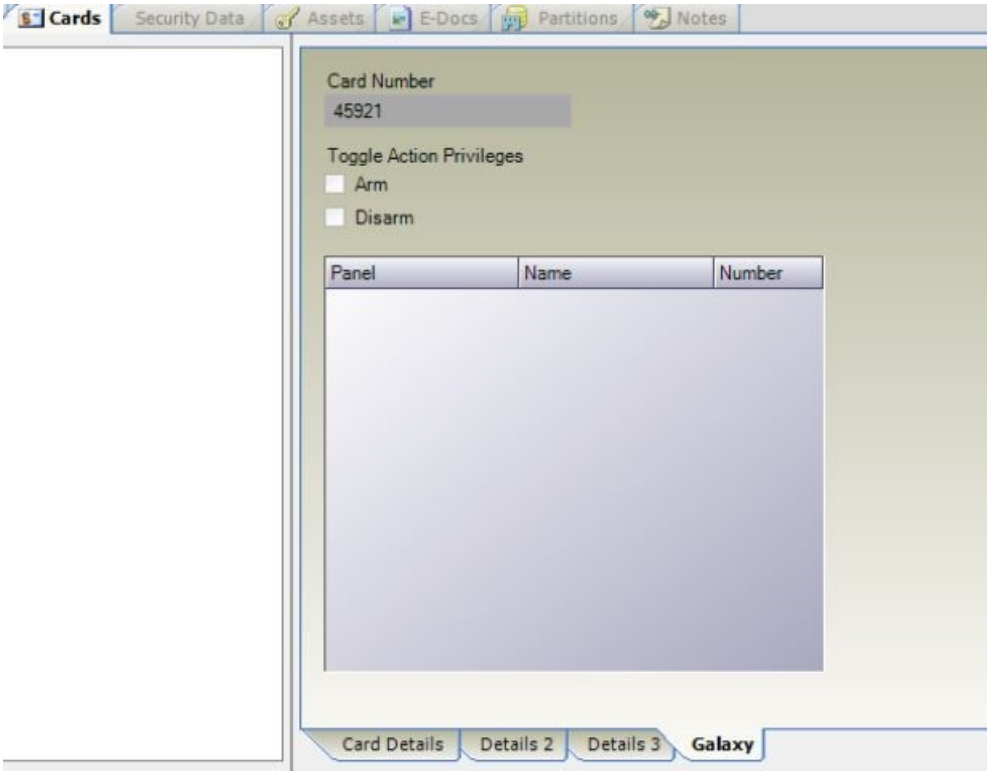
*** Note:** The **Database Configuration > Users > "Device Filter"** tab provides filter settings for Galaxy Zone and Group off-normal status. Do not forget to adjust these items to suit your preference.

*** Note:** Although visible, Galaxy Readers and DCM cannot be controlled from Pro-Watch.

O.8 Badgeholder Operation Permissions

Each access control card supplied to a badgeholder can be allowed or denied to control the Galaxy Intrusion system using that credential.

The new variables under the "**Galaxy**" tab of the badgeholder screen include permissions to:

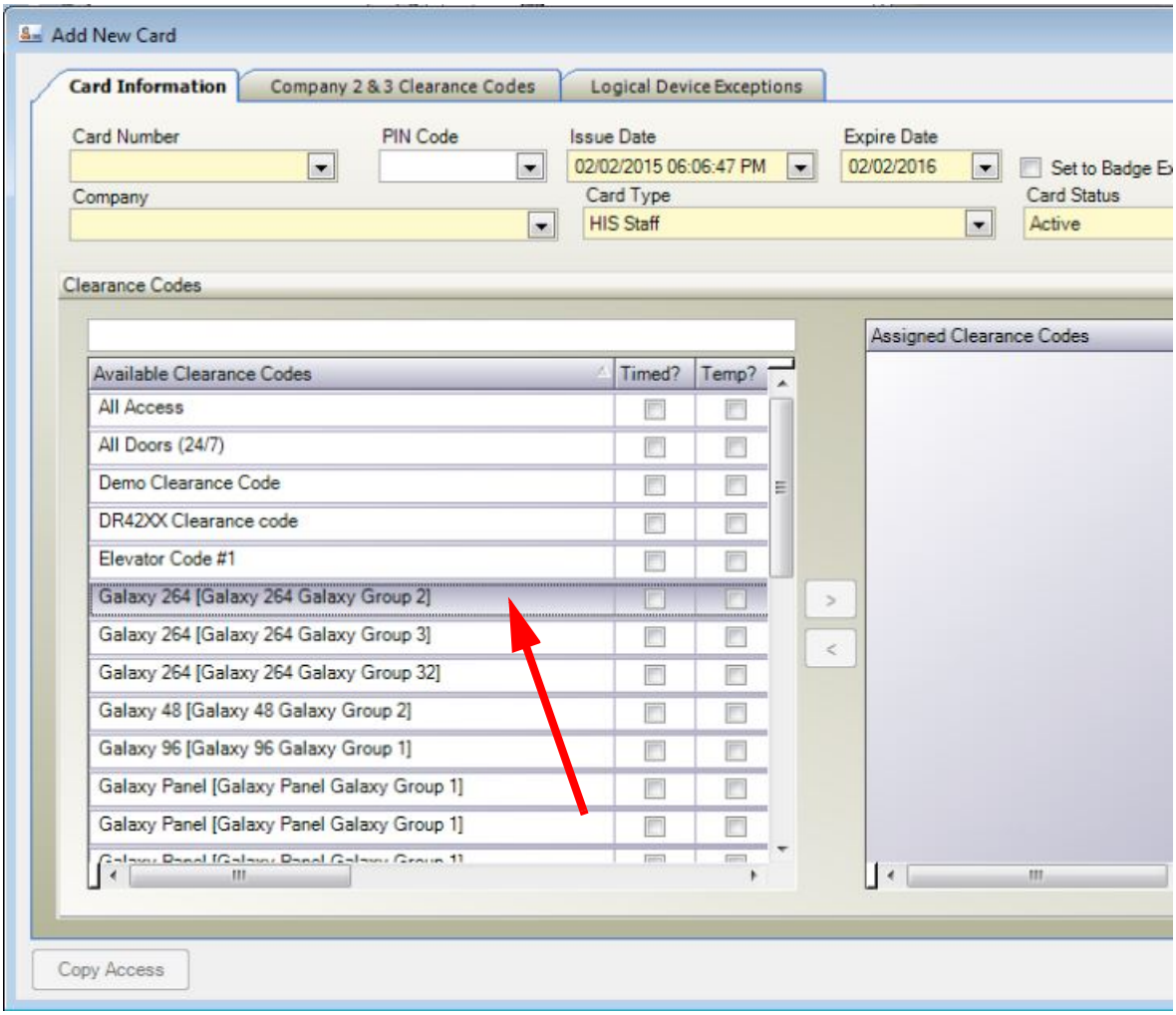


- Only allow Toggle Arm (Arm zone or Group)
- Only allow Toggle Disarm (Disarm Zone or group)
- Allow Toggle Arm and Disarm (Full control)
- No options set (No control)

A list of panels where this cardholder's card is valid is shown in the separate panel.

Pro-Watch user permissions set in this option are independent to the users and permissions programmable in the Galaxy panel. All Pro-Watch cardholders are eligible to arm/disarm any integrated Galaxy intrusion panel.

All Galaxy zones and groups which are imported during the initial upload are added as clearance code to the Pro-Watch database.

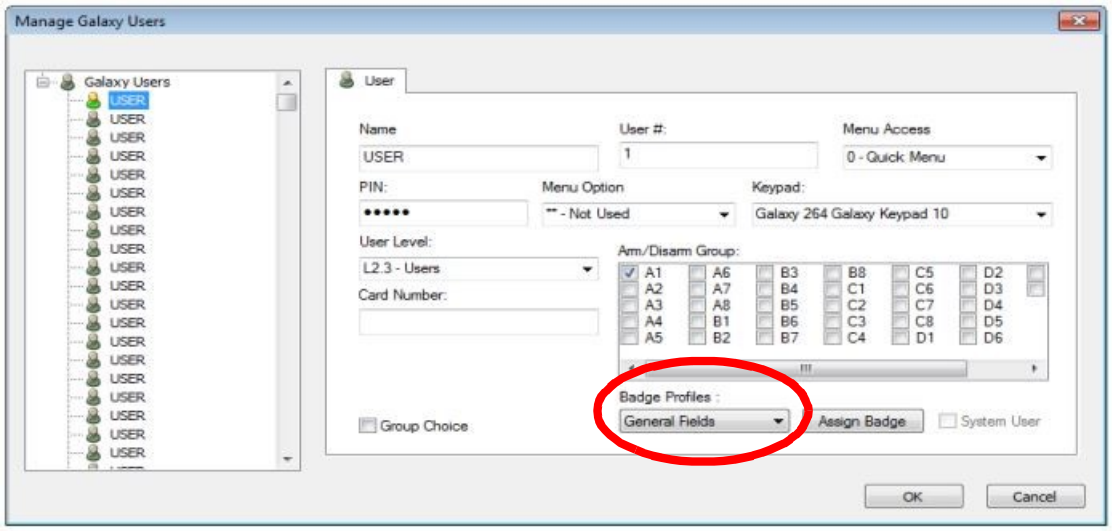


By assigning one or more Galaxy clearance code(s) to a badgeholder, this badgeholder will be able to arm/disarm the respective zone(s) and with respect to the "Arm/Disarm" Operation permissions set to the card.

O.9 Managing Galaxy Users

Each Galaxy Dimension panel supports a number of system users. Depending on the type of panel this number will be 100 (GD48), 250 (GD96), 999 (GD264/520) users.

These users can be controlled from Pro-Watch through the Panel Properties, or from "Database Configuration" > "Galaxy User Management".



It is possible to modify existing Galaxy users from this screen, as well as merging Galaxy Users with the Pro-Watch badgeholder database.

The "**Assign Badge**" option can be used to add an existing Galaxy user to Pro-Watch, where the card is assigned to the new added company "**No Access**".

If the added card already exists in the Pro-Watch database the cardholder will be merged to the Pro-Watch cardholder database, including the operator's clearances to zones,

Caution: A Galaxy user without a unique card number will not be added as a Pro-Watch badgeholder.

*** Note:** Control through Pro-Watch of Galaxy functions is limited to the essentials for combining Pro-Watch badgeholders with Galaxy functionality, and interaction between the 2 systems. Galaxy system programming can only be done using the standard Galaxy keyboard or RSS software options.

The Galaxy Dimension panel users are still able to control the intrusion panel functions.

Through the Pro-Watch integration however, badgeholders are also be allowed to arm and disarming Galaxy Zones and groups using their regular access control card presented to a regular access control reader.

Direct control over alarm inputs and outputs can be granted to Pro-Watch system operators through the normal Pro-Watch user or class security options.

The way badgeholders can arm and disarm is arranged through a set of new features in Pro-Watch.

O.9.1 Creation of Galaxy users

Galaxy panel users can be created on the panel or in Pro-Watch. The following conditons must be taken into account.

O.9.1.1 A User created on the Panel:

Use command 42 to create a user in the Panel. The Pro-Watch database will not be updated.

Once an upload (Users) from the Panel is initiated and completed, the User account is present in Pro-Watch.

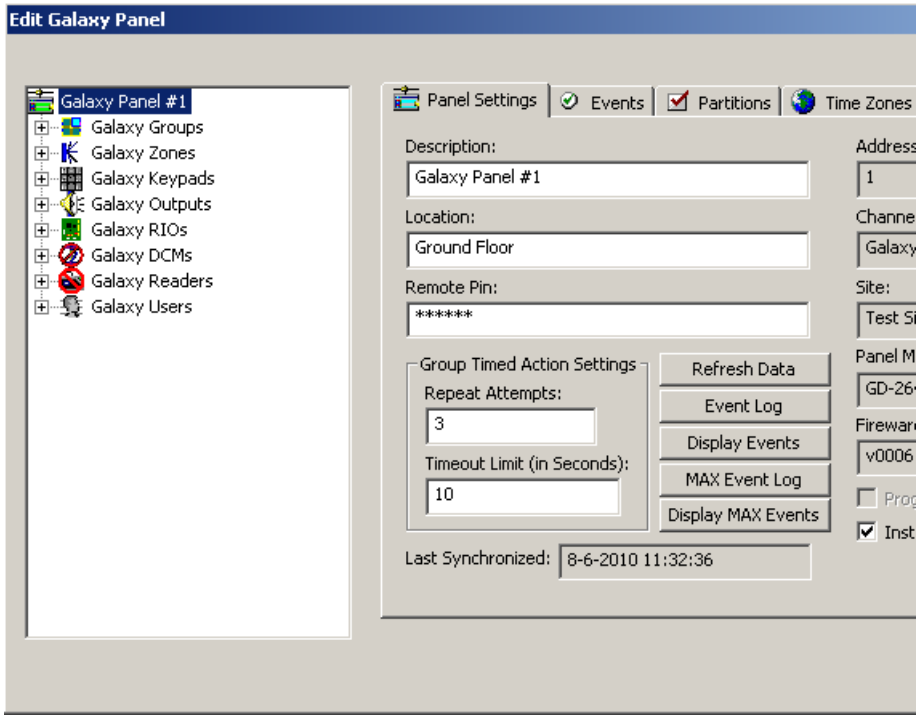
O.9.1.2 A User created in Pro-Watch:

The user is immediately downloaded into the panel.

O.10 The Arm/Disarm Mechanism

A badgeholder can present his/her credential for a predefined number of times to an access control reader for Arming/Disarming one or more Galaxy zone(s) or group(s).

This is defined through a Galaxy panel parameter in combination with the operation permissions set in Pro-Watch for the used card. (See previous page)



O.10.1 Arming Zone(s)

The new procedure which was added to the Reader Event will signal the Galaxy channel as many times the card is presented.

Based upon;

A)The reader triggered procedure pointing to a Galaxy group or zone,

B)The cardholder's permission to Arm/Disarm,

C)The badgeholders Access permission to the Galaxy Zone

D)The number of consecutive events within the number of seconds,

The Galaxy panel will arm the selected Zone(s).

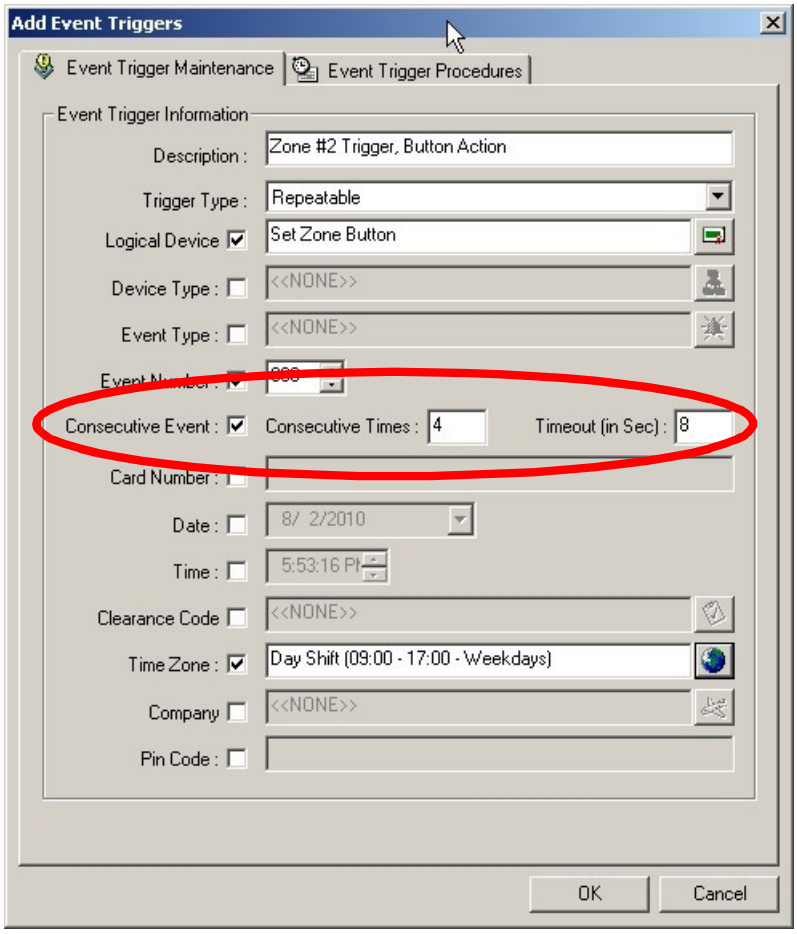
O.10.2 Disarming Zone(s)

The Galaxy panel will disarm zones/groups again, when the first valid card is presented to the reader and complies with the set access and operation permissions.

See "Process Flowchart" for detailed overview of the process.

O.11 New Trigger Options

It is possible to program a Pro-Watch trigger to react only when a predefined event has occurred a consecutive number of times. (See the red circle in the below screen-shot). This new trigger function allows for any event generated by any logical device, use of card, or use of clearance permissions to execute procedures.



In this example, the trigger is set to execute a procedure when;

- "A specific button is pressed
- "and is pressed 4 times within 8 seconds.
- "and event 900 Is generated (Input point active),
- "and during a specific time zone.

Using the various variables available in the Trigger feature, a flexible Security control can easily be configured and maintained.

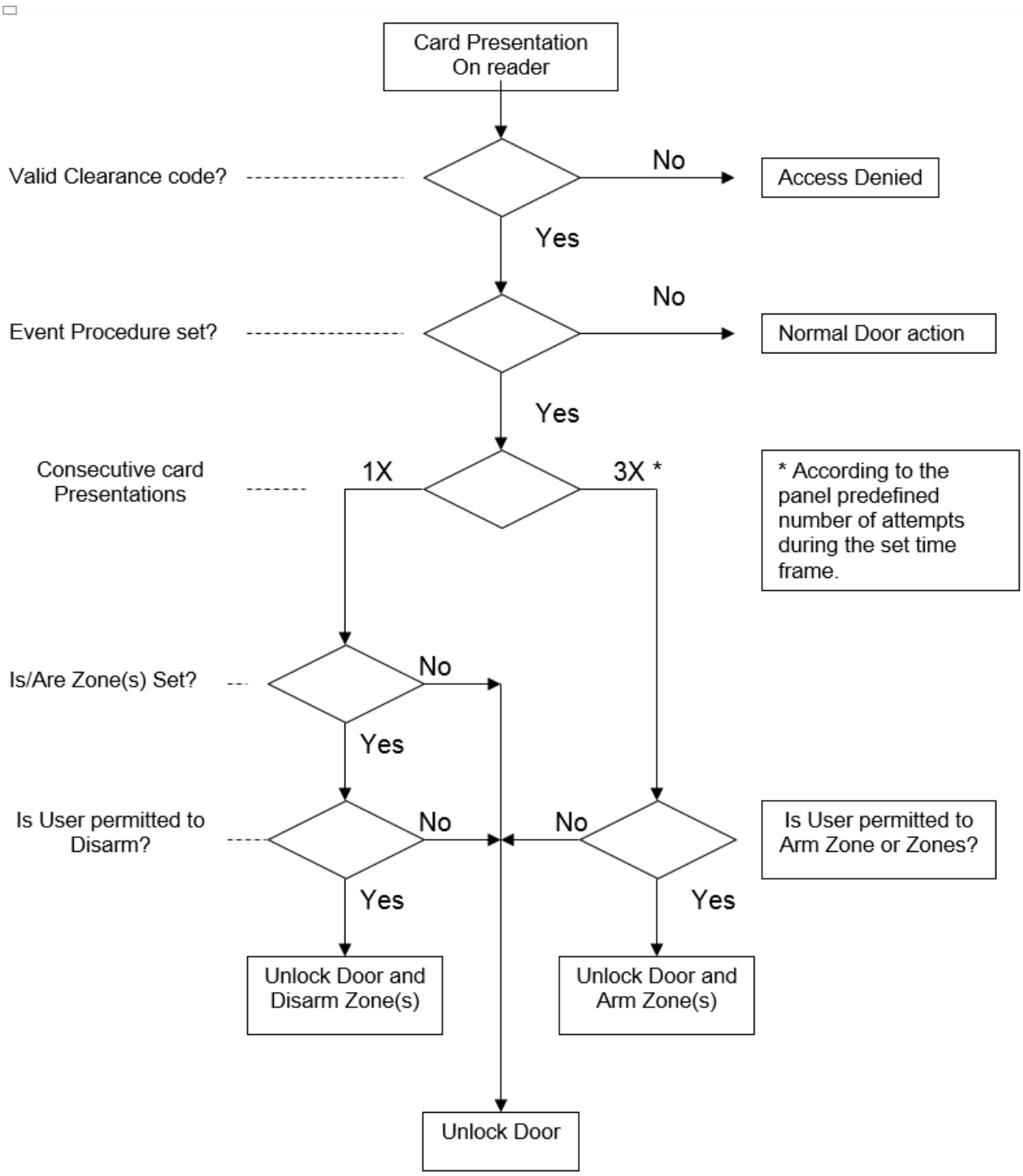
O.12 New Pro-Watch Registry Keys

A set of entries are added to the Pro-Watch registry defining default values for the Galaxy Panel Programming in Pro-Watch. All registry keys are to be found under HKLM_Software\Wow6432Node\Honeywell\Prowatch\Options\

Registry Key	Value	Description
GalaxyCommlossPort	Default value 30	Time in seconds Pro-Watch buffers commands for the Galaxy panel in case of a communication interruption
GalaxyDefaultAlarmPort	Default value 10002	Default Alarm TCP/IP Port
GalaxyDefaultBasicPort	Default value 10005	Default Basic TCP/IP Port
GalaxyDefaultConfigPort	Default value 10001	Default Configuration Port
GalaxyScanFlags48	Default 0x180A40	Internal function. Do not change.
GalaxyFlags	Default value 0	For engineering purpose only. Creates log files as C:\Galaxytrace_xx.txt for each active Galaxy channel on C:\
	FFFF	Trace function is activated.
	80000100	Activates Process Debugging
NoGalaxyDTUpdate	Default 0	turns time sync messages OFF if value is changed from the default “0” to “1”

*** Note:** Use of the Windows registry editor to modify the registry keys. Be careful not to alter any other registry key than instructed in this manual.

O.13 Process Flowchart



O.14 Pro-Watch Icons

The representation in Pro-Watch of status changes of Groups and Zones is represented by Icons. Below tables show the relevant default icons for the various status situations.

The Icons shown on this page are used in "Hardware Configuration" and "Status groups".

Table O-1 Pro-Watch Icons

Element	State	Device Status	Icon Change	Icon	Event text description
Zones	Cleared	Normal			Normal cleared
Zones	Active / Alarm	Open	Y		GeneralZoneOpened General Zone Opened – RTN
Zones	Masked	Masked	Y		Maskanalarmpoint Arm an alarm point (unmask)
Zones	Bypassed		Y		ZoneisOmitted Zone is Omitted – RTN
Zones	Bypassed	Bypassed Open	Y		Zone is Omitted, and zoneisactive Zone is Omitted – RTN
Group	Normal	Disarmed			Group is Unset
Group	Armed	Armed	Y		Group is Set
Group	In Alarm	Armed in Alarm	Y		Group is in Alarm State Group is Unset (After reset)
Output	De-Activated	Normal			No transaction (It's the way it works)
Output	Activated	Energized	Y		No transaction (It's the way it works)

Below are the Icons as shown in the Maps option in the Alarm monitor.

Table O-2 Pro-Watch Icons - Maps

Zones	Cleared	Normal			N/A
Zones	Active / Alarm	Open	Y		N/A
Zones	Masked	Masked	Y		N/A
Zones	Bypassed	Bypasseed	Y		N/A
Zones	Un-Bypassed	Normal	Y		N/A
Group	Normal	Disarmed			N/A
Group	Armed	Armed	Y		N/A
Group	In Alarm	Armed in Alarm	Y		N/A
Output	De-Activated	Normal			N/A
Output	Activated	Energized	Y		N/A

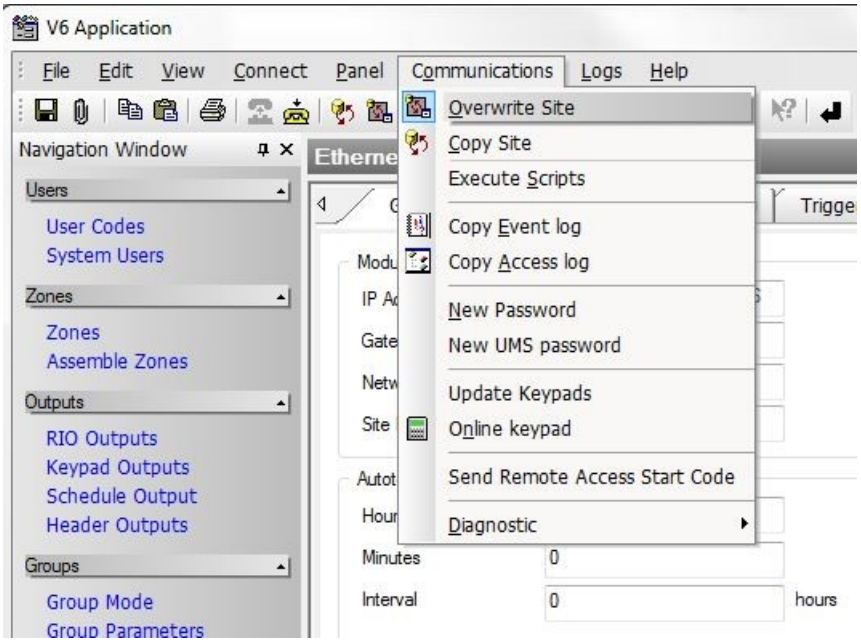
O.15 Backup and Restoring a Galaxy Database Using RSS

Once a Galaxy Panel is configured and functions as desired it is advised to create database backup of the Galaxy's database on a safe media.

*** Note:** Although Pro-Watch will show the complete panel configuration, this cannot be downloaded into the panel in case of a mishap with the panel's database. For the management of the Galaxy database Honeywell's Remote Service Suite (RSS) is required. Download the RSS application from the URL at the end of this chapter and install the product. For the purpose of this manual we only describe the steps necessary to create and restore a database. The default Login name is "manager" with password "password". Consult the PSS manual for detailed setup information to establish communication with the Galaxy Panel.

*** Note:** At no moment RSS and Pro-Watch GD channel should be simultaneously active. Alarm monitoring in Pro-Watch will be erratic and event history collection will be incomplete..

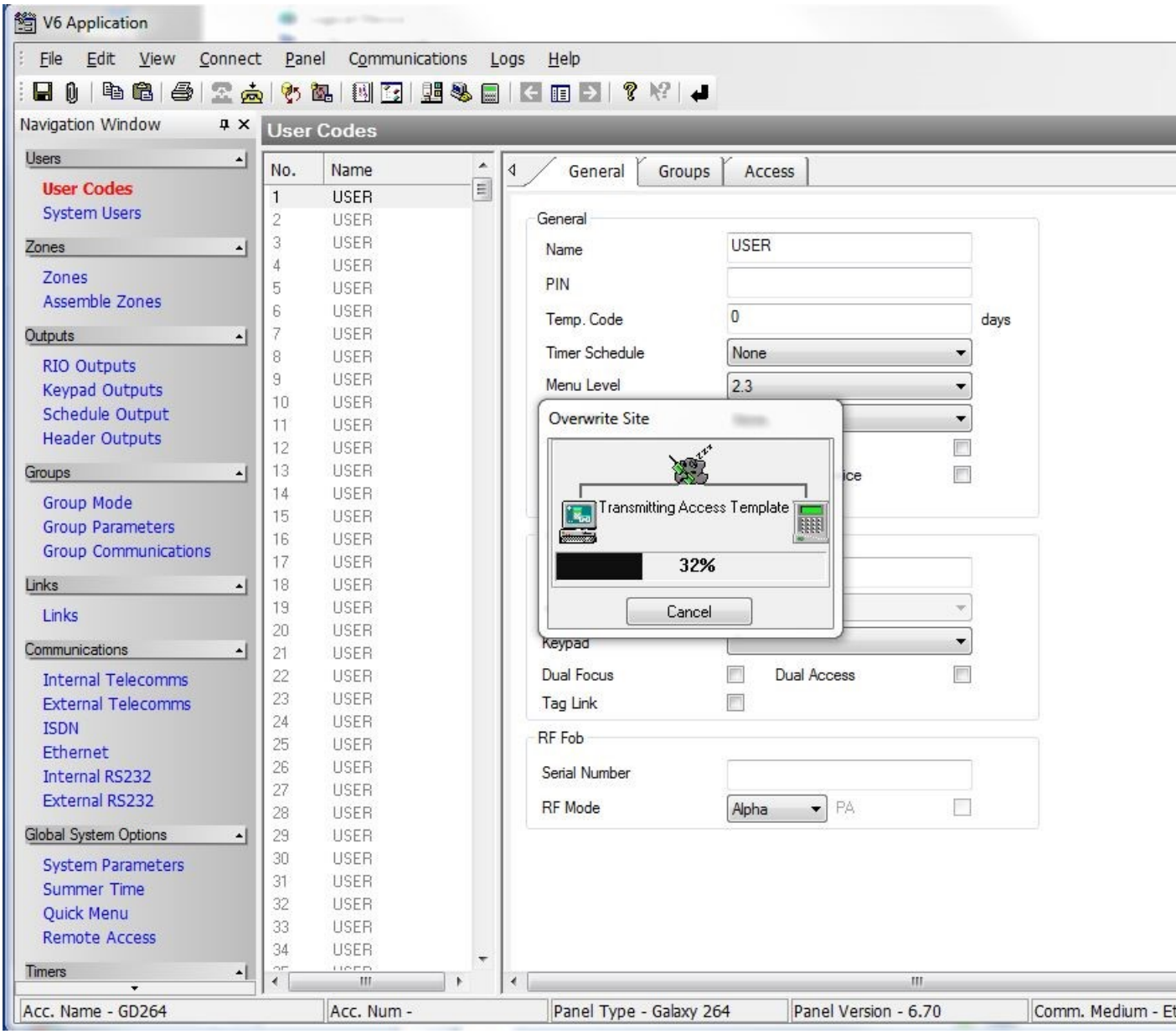
O.15.1 Backup of the Galaxy Database



1. Open "**Communications**" and select TCP/IP, leave encryption as set. Open the site and open communication again and connect to the Panel.
2. Answer "**NO**" if a message appears "The data on the panel has changed. Do you want to copy the changed data?
3. Next select "**Copy site**" and select "**Set All**" and click **OK** to start the download process.

This concludes the Backup process

O.15.2 Restoring a Galaxy Database Backup



The **Download Select** screen will open.

1. Click the "**Select All**" button to select all items that are to be overwritten from the saved DB or select individual items if desired.
2. "Open "**Communications**" and select TCP/IP, leave encryption as set.
3. "Open the site and open communication again and select "**overwrite site**". The password for the download is the default 12345, unless changed.

4. "Answer "**NO**" if a message appears "The data on the panel has changed. Do you want to copy the changed data?
5. "Click **OK** to start the transfer.

*** Note:** The Database Restore option allows for uploading a database that is created on another panel type. The restore process will inform that the database you are restoring does not match the present panel type.

You can choose to overwrite the connected panel's database. Example: A GD264 database can be restored onto a GD96 panel.

URL to the RSS Software.

http://www.security.honeywell.com/uk/products/intruder/control-panels/accessories/programming/index.html

O.16 Functional Testing

When a Galaxy Dimension panel is successfully connected and uploaded in Pro-Watch for the 1st time, execute following tests to verify functionality.

- Arm / Disarm a zone from the Panels keypad.
  - Observe incoming events in the Pro-Watch event viewer
- Activate / De-Activate an output from the keypad
  - Observe incoming events in the Pro-Watch event viewer
- Activate / De-Activate an Input on a RIO.
  - Observe incoming events in the Pro-Watch Event viewer.
- Execute same actions from the Pro-Watch hardware configuration by right clicking on the Galaxy object and select the appropriate control option from the context menu.

If the above does not show events, check and verify the panel setup against the configuration items as shown in section "Configuring Pro-Watch".

O.16.1 Test Arm / Disarm by Card

Configure the necessary procedures to toggle Arm / Disarm as described on page 8 and 11 and test by presenting a valid card with the correct Galaxy group added to the clearance code.

- **Present card 3 times** on designated reader, panel should **arm** the group.
- **Present card 1 time** to designated reader, the panel should **disarm** the group.

TIP: In case the panel does not arm/disarm it is needed to Stop / Restart the Pro-Watch server service and restart the Galaxy panel using the menu option 51 - 17.

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Extended Card Number Support

P

In this appendix...

Overview
Prerequisites
Setup

P.1 Overview

P.1.1 Extended Card number support (up to 128 bits)

Mercury panels (PW-6000, PW-6101, and EP-1502) can support card numbers up to 128 bit in length. Card download commands include an extended card number portion where a hexadecimal value representing a long card number can be added in addition to smaller card number. Through server options in Pro-Watch, we can now configure and setup Mercury panel to expect longer card numbers.

P.2 Prerequisites

Please install the following version or higher:

Pro-Watch version	4.3.5
PW-6000 Firmware	2.7.3
PW-6000 2R Firmware	1.6.0
PW-6101 Firmware	1.20.1
PW-6101 2R Firmware	1.4.8
EP-1502	1.229

P.3 Setup

P.3.1 Configuring Pro-Watch

1. Select **File > Server Options** to display the **Server Options** page.
2. Turn on support for 128bit credential number by selecting "**Support up to 128 bit credential number on PW-6000/6101"** check-box.
3. Enter an appropriate number for number of bits in the **Credential Length field** (for example, "92" as shown in the below screen-shot):

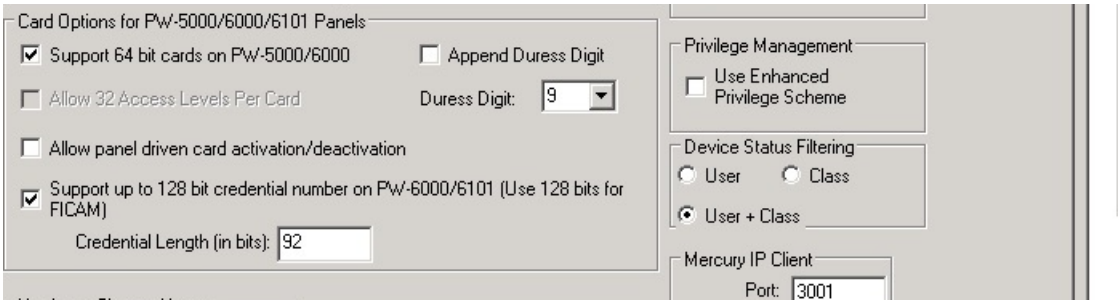


Figure P-1 Server Options in Pro-Watch

4. Restart Pro-Watch service.
5. Add required card formats to the panel. Make sure the readers have the required card formats selected.

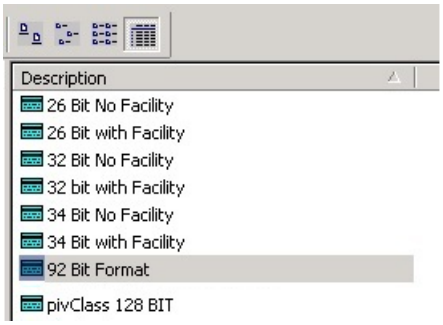


Figure P-2 Card Formats in Database Configuration

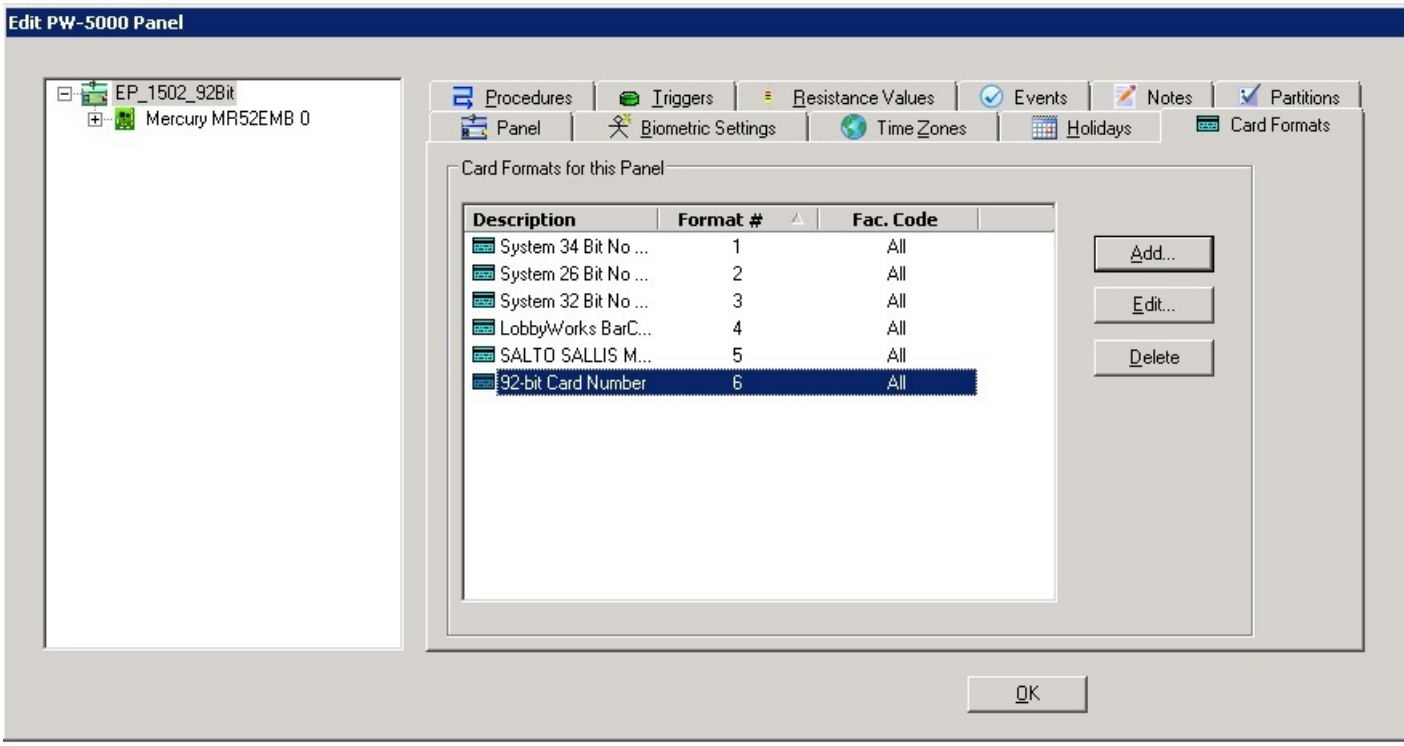


Figure P-3 Panel Properties in Pro-Watch

Note: Make sure that the Panels/Subpanels are running the latest firmware. Refer to Prerequisites for more information.

6. Initialize the panel(s) and Download System.
7. If the panel setup was successful you will see something similar in the mercury SCPLOG file:

```
enNCcMcbAdbSpec: 1103 0 25 5000 12 16 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 12 1 12 0 0 0 0 0 0 0 0 0 0 0 0 0 0
enNCcMcbCfmt: 1105 0 25 0 -1 0 1 512 34 0 0 0 0 0 0 16 17 0 0
enNCcAdbCard: 5304 0 25 3 38450 0 "" 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

- 0x99950001000001010000000001300031 is the extended card number.

P.3.2 Configure Advanced Badging

Set the **enrollment reader** in **Options** under **Badging** tab.

Note: The enrollment reader will be used to pull up last unknown card read in the **Add Card** dialog in **Advanced Badging**.

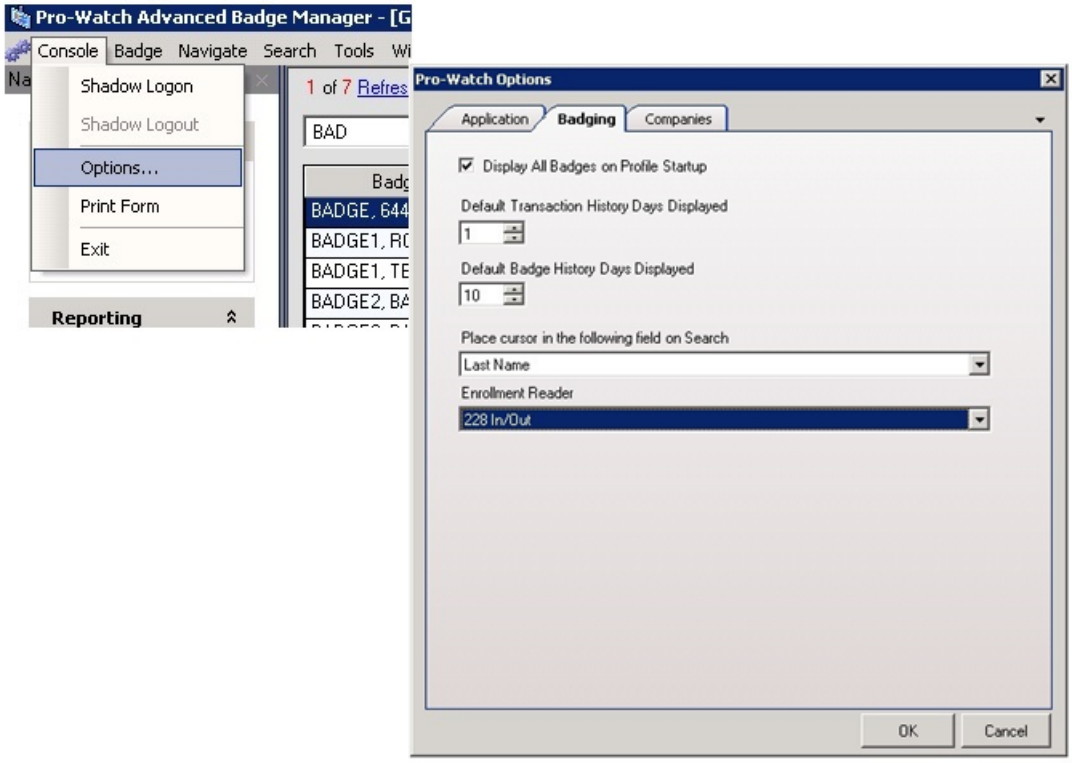


Figure P-5 Pro-Watch Options in Advanced Badging

P.3.3 Adding Card in Pro-Watch

The simplest way to add a card in Pro-Watch is to swipe the card at the enrollment reader. This generates an Unknown badge event in Pro-Watch that is used by the "last read" feature, in Add new card dialog in advanced badging, to pull up the new card.

1. Swipe the new card at the enrollment reader:

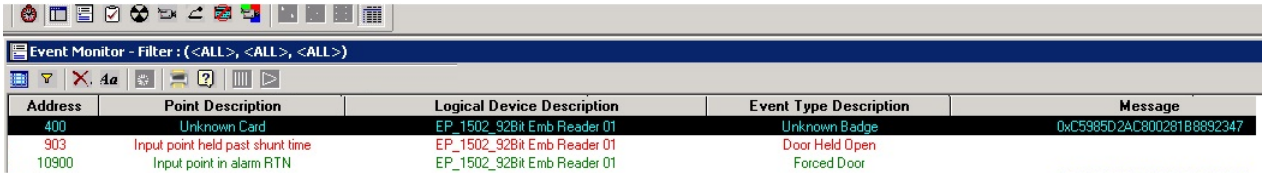


Figure P-6 Unknown Badge Event in Pro-Watch Event Viewer

2. In the **Add New Card** dialog screen in Advanced Badging, pull the drop-down for **Extended** card number and click "**Last Read"** button. This will pull the last **Unknown Badge** read at the **Enrollment Reader.** Make sure to also fill Card number with unique value and other required fields. Click the **Add Card** button to add the card to the badge:

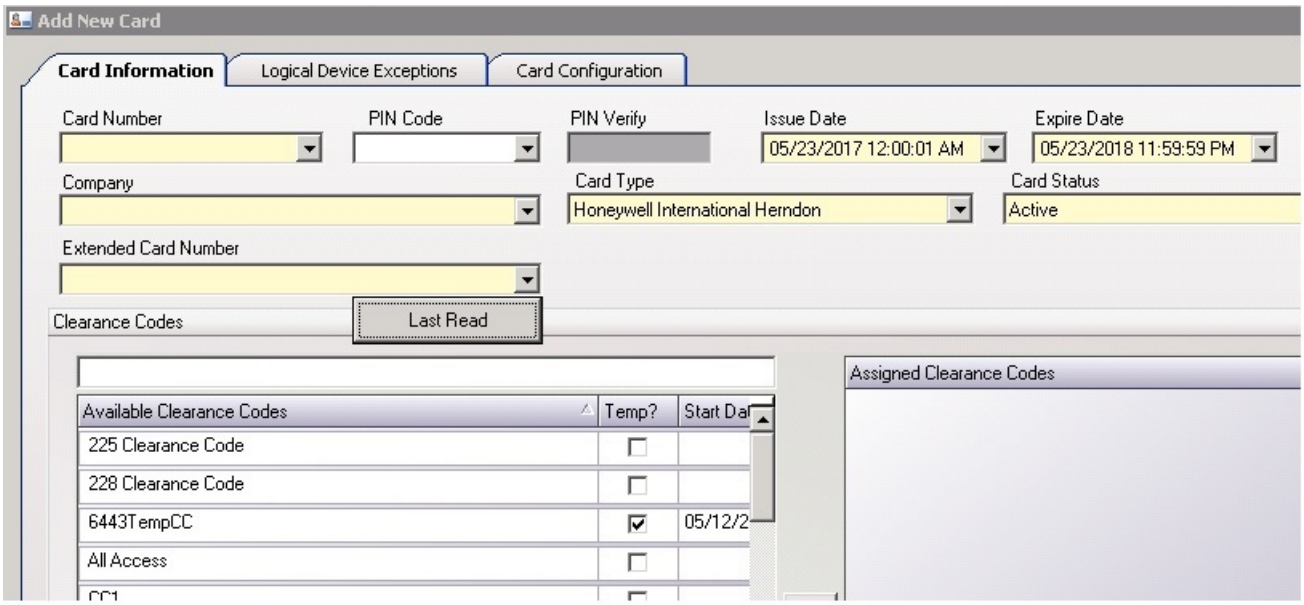


Figure P-7 Last Read Feature Drop-Down

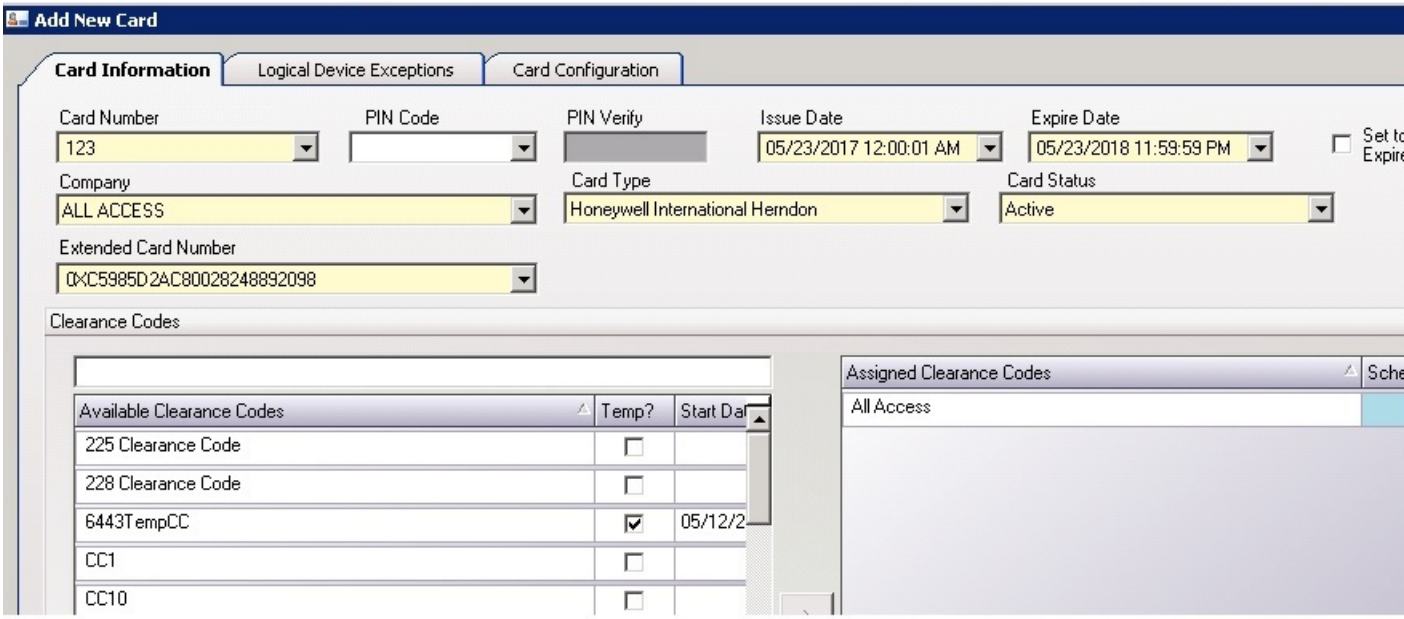


Figure P-8 Add New Card Screen

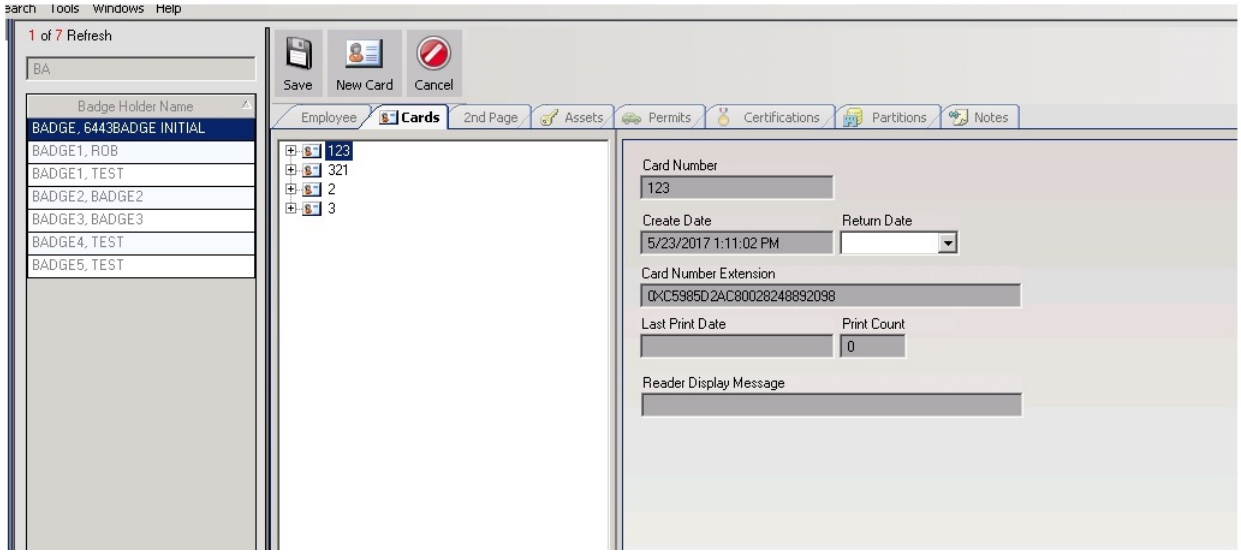
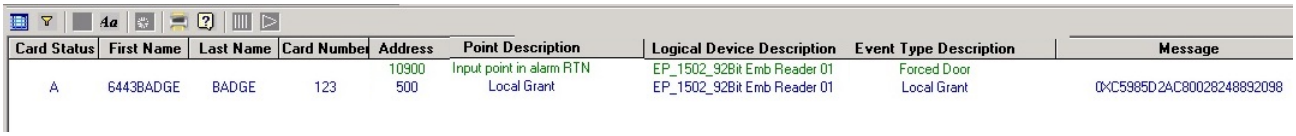


Figure P-9 Card Showing the Extended Card Number

3. All card events that are displayed in the **Event Viewer** in Pro-Watch will also show the extended card number in the **Message** column:



Card Status	First Name	Last Name	Card Number	Address	Point Description	Logical Device Description	Event Type Description	Message
				10900	Input point in alarm RTN	EP_1502_92Bit Emb Reader 01	Forced Door	
A	6443BADGE	BADGE	123	500	Local Grant	EP_1502_92Bit Emb Reader 01	Local Grant	0XC5985D2AC80028248892098

Figure P-10 Card Events with Extended Card Number in Event Viewer

Copyright © Honeywell Inc. All Rights Reserved

Honeywell

IRIS ID Integration

Q

In this appendix...

Overview
General System Architecture
General Operation
Iris ID EAC Components
EAC Components Required for Pro-Watch Integration
Installation Prerequisites
Installation Notes
Creating the IrisServer Database
Configuring the IrisServer
Configuring the IrisManager
Starting the IrisManager
Creating the Remote Unit Connection
Creating the IrisEnroll Connection
Creating the Iris Manager Connection
Creating the Iris Monitor Connection
Using Iris Monitor
Using Iris Enroll
Connecting to the iCAM Web Configuration
Configuring the IP Address of the iCAM
Changing the Operational Mode of the iCAM
Security and Ports
Pro-Watch Configuration

Q.1 Overview

IRIS ID is an identity authentication software supported by Pro-Watch. It works in One to Many, One to One, Wiegand and Token environments. It can handle applications requiring management of large user groups, such as a National Documentation application might require.

IRIS recognition works by taking a digital picture of the eye's iris pattern and recreating an encrypted digital template of that pattern. 512-byte IRIS templates are encrypted and cannot be re-engineered or reconstituted to produce any sort of visual image. In a few instances even blind persons have used iris recognition successfully, as the technology is iris pattern-dependent, not sight dependent.

Installation of the software through the setup.exe for IRIS ID will install the following EAC (Entry Access Control) components:

Q.2 General System Architecture

The general architecture of the IrisAccess system EAC (Entry Access Control) consists of an IrisServer computer, an Ethernet network, and "Remote Units" used for identification/verification which will output Wiegand to an Access Control Panel or Relay outputs to door control devices.

A dedicated iCAM for enrollment is recommended for systems where users are added frequently. A fully expanded system can include up to 128 remote units (consisting of iCAM7000S, iCAM7000, ICU7000, iCAM4000, ICU4000, ROU3000, and ICU3000 units).

Q.3 General Operation

Through the enrollment software and hardware, a series of digital images of the users' irises are captured. The best images from this series of images are determined by the software and then converted into a 512 byte biometric record. This biometric record is then encrypted and sorted in the IrisAccess database along with the other user information collected during the enrollment process.

Q.4 Iris ID EAC Components

Installation of the software through the setup.exe for Iris ID will install the following EAC components:

Component	Description
IrisServer	Controls the IrisAccess database and communications to and from the ICU(s) and IrisAccess system. Only one IrisServer application per network is needed.
IrisManager	Manages the system configuration, system permissions, and user database. Up to 10 IrisManager applications can be placed on one network, however only one can be active at any time.
IrisMonitor	Allows for real-time monitoring of system status and user activities with optional audio alerts. Up to 10 IrisMonitor applications can be placed on one network
IrisEnroll4000	Used with the IrisAccess 4000, 7000, and 7000S series iris cameras for user enrollment. Up to 32 enrollment stations per network. (Combined stations of IrisEnroll4000 and IrisEnroll TD100)
IrisEnroll TD100	Used with the iCAM TD100 iris cameras for user enrollment. Up to 32 enrollment stations per network. (Combined stations of IrisEnroll4000 and IrisEnroll TD100)
IrisDBAdmin	Provides backup and other database utilities. For use with the IrisServer Only.
iCAM7000Update	Used to perform a new installation or update of the iCAM7000 Series device software/firmware.
iCAM7000SUpdate	Used to perform a new installation or update of the iCAM7000S Series device software/firmware.
IrisICUAdmin7000	Used to perform a new installation or update of the ICU7000 device software/firmware.

IrisICUAdmin7000-2	Used to perform a new installation or update of the ICU7000 device software /firmware.
Option3 Admin	Used to perform the change of the IrisServer IP Address and Security IDs for multiple devices which are using Option 3 mode.
IrisICUAdmin4000	Used to configure the setting of the ICU4000 device IP Address and Security IDs (New Installation), upgrade of the ICU software, and to make changes to the ICU4000 configuration.
ImportUserDataToEAC	An off-line utility to import a list of users which are in a .CSV file into the EAC database.
ClientCertMgr	A management utility for the Client Certificates issued to the iCAM7000 Series and iCAM7000S Series units in high security applications.

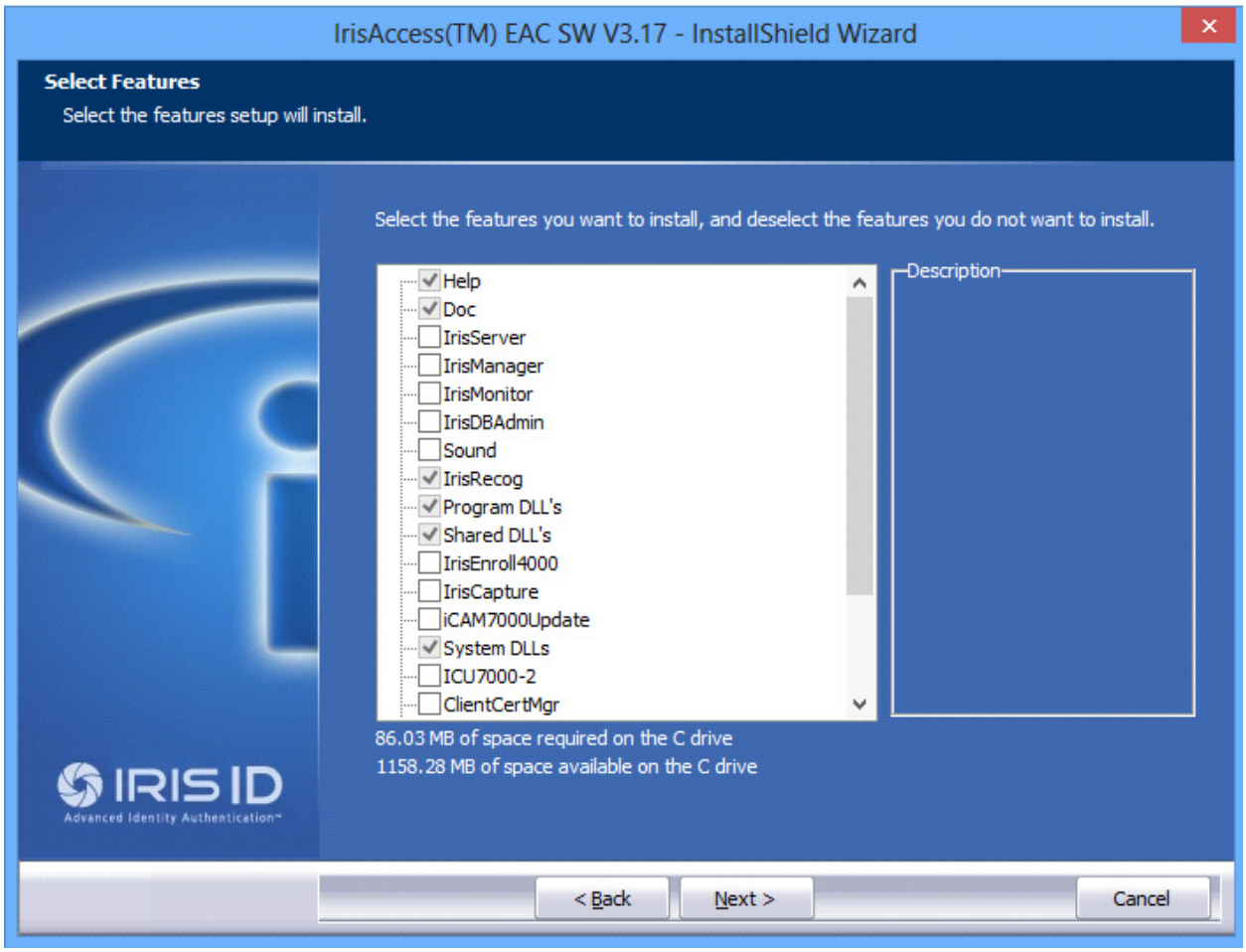
Q.5 EAC Components Required for Pro-Watch Integration

For the Pro-Watch Integration with Iris ID, the following 4 components will be used:

- IrisManager
- IrisServer
- IrisDBAdmin
- IrisEnroll4000

Q.6 Installation Prerequisites

- Microsoft Access is the standard database type used in the IrisAccess system. Microsoft SQL Server 2000 (or above) including express versions, or Oracle 9i (or higher) can also be used. It is recommended that SQL Server be used. If using SQL Server, an admin SQL Login needs to be created.
- SQL Server should already be installed prior to installing the EAC software.
- The IrisServer computer with the Iris ID EAC administrative software should be placed within the protected area and in a location that is not accessible by the general staff or public.
- Each device on the network must have a unique statically-assigned IP address. IrisEnroll4000 and IrisEnroll TD100 will not function simultaneously on the same computer.
- The Enrollment computer requires a sub-set of the Iris ID software, which is used by Pro-Watch to connect to the IrisServer and the Iris ID camera. The required IRIS EAC software is:

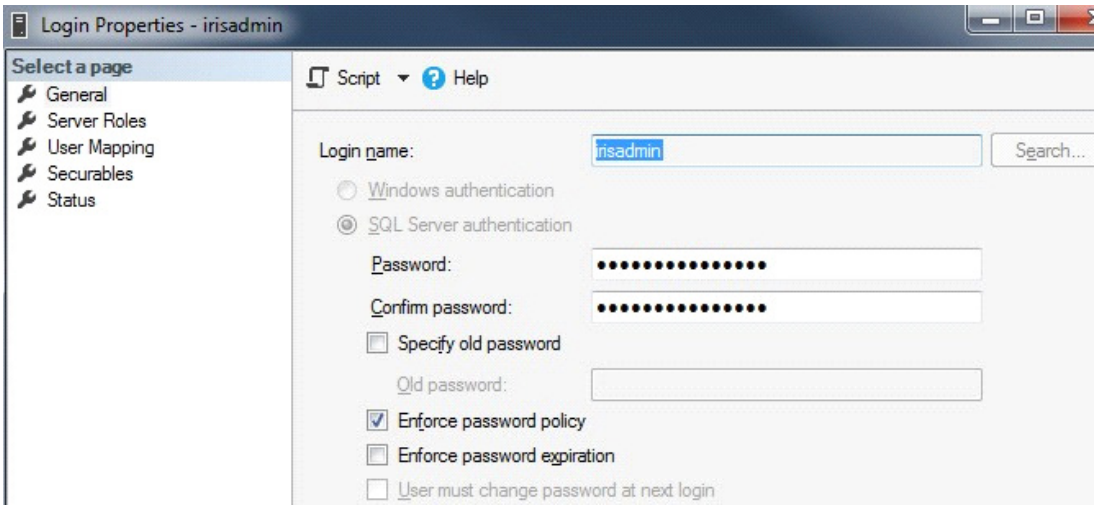


Q.7 Installation Notes

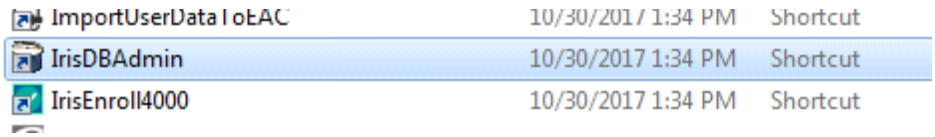
- Run the setup.exe executable file located within the Setup folder of the Iris ID disk. This will install all of the components listed in the EAC Suite Applications tab.
- When selecting Customer Information, it is highly recommended that the default selection of "Anyone who uses this computer (all users)." is kept.
- When installing the EAC IrisService, it is recommended during the initial setup of the EAC System that the IrisService is set to manually start. The IrisServer when run as an application (not a service) can provide very useful troubleshooting information. The IrisServer Service starting mode can be changed later within the Windows Services settings.
- When selecting database type, select Microsoft SQL Server. Verify that the appropriate DBMS (i.e., SSMS) is installed on the machine. The database selection cannot be changed without uninstalling and re-installing the EAC software.
- If running a software or hardware firewall product, disable and/or allow all access of the IrisAccess EAC application and installation.

Q.8 Creating the IrisServer Database

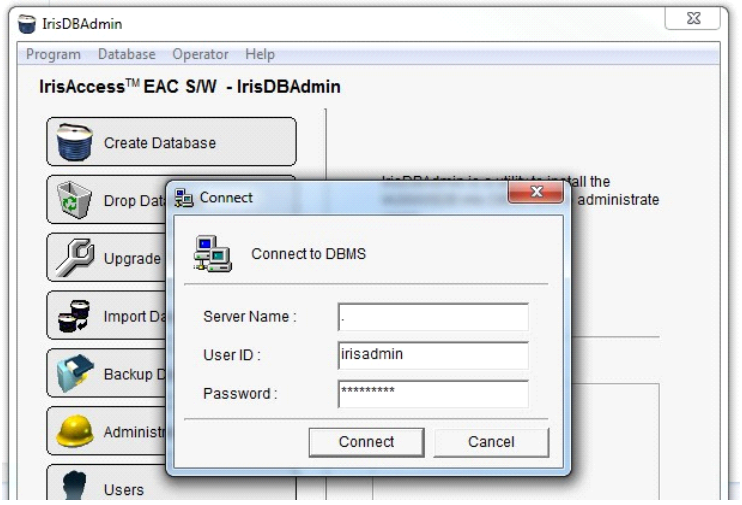
1. Verify that an administrator SQL Login exists ('sa' can be used).



2. Open IrisDBAdmin from the list of installation application modules:



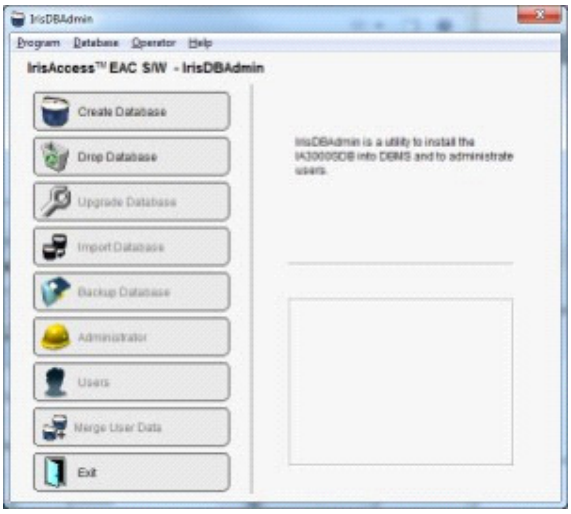
3. Enter the Server Name, the SQL User ID, and the User Password:



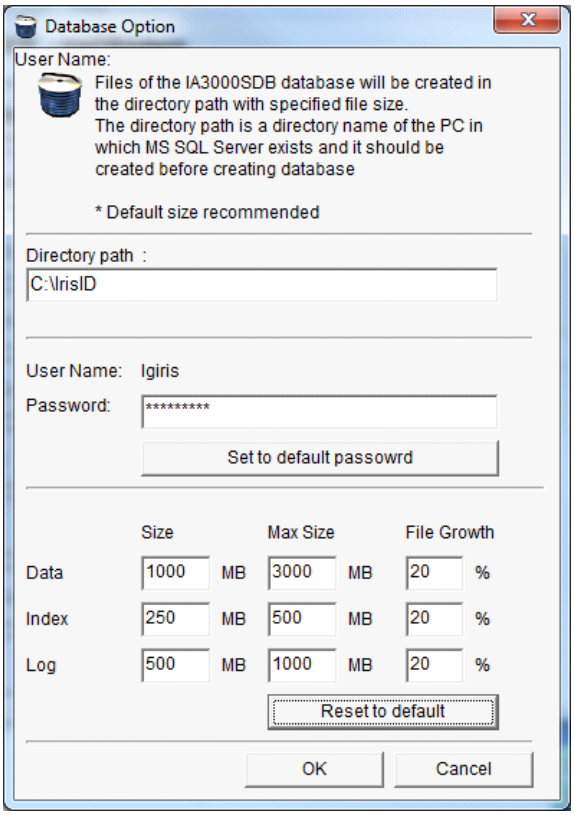
4. If IrisDBAdmin cannot connect to the MS SQL Server, the following message will appear: "Cannot connect to server. Check if User ID, Password or Server Name is invalid."

- This message is also displayed if SQL Server is not configured for SQL Server Authentication. To turn on SQL Server Authentication for SQL Server, right-click on the SQL Server in SSMS and select Properties >> Security >> SQL Server and Windows Authentication Mode. SQL Server will need to be restarted in order for the changes to take effect.
- The SQL User created must be an administrator. If the user is not an administrator (grant db_owner on the master database for this user), the following message will appear: "Administrator can only use IrisDBAdmin."

5. After successfully connecting to SQL Server, the IrisDBAdmin main window will be displayed:

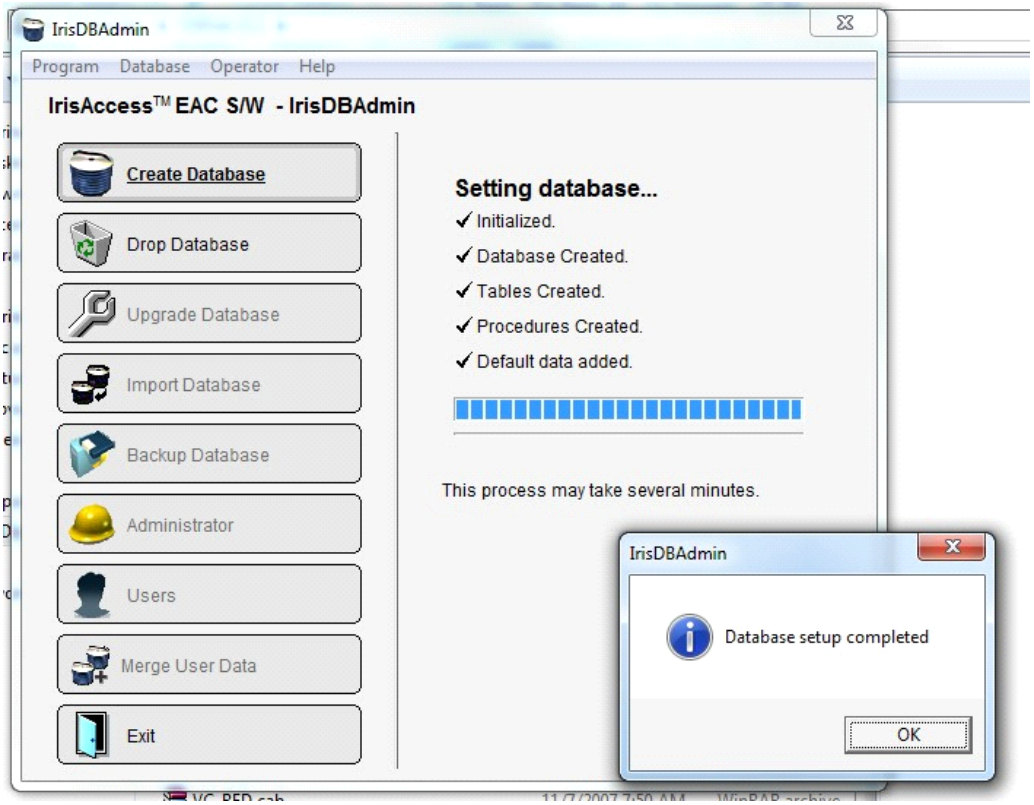


6. Click on Create Database to create a new Iris ID database:

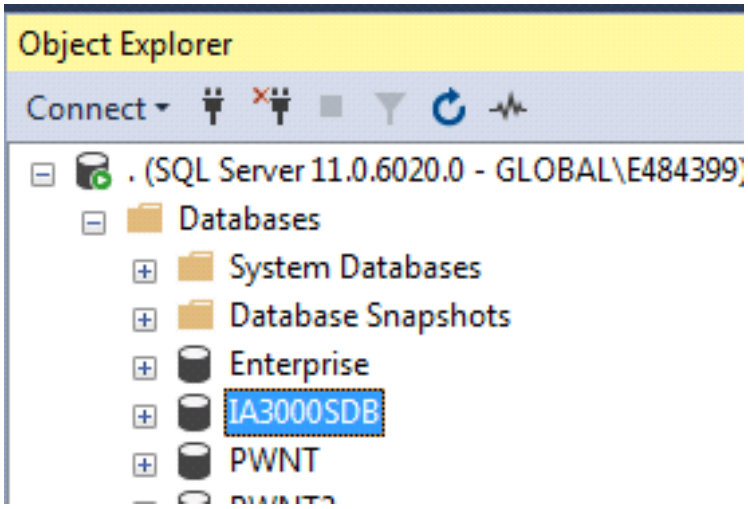


- Size: This option specifies the size of the file in megabytes. The minimum value is 1 MB. The default value is 1000 MB for the primary file. The default value is 250 MB for the index and log files. (Note: If intending on capturing face images during enrollment, it is suggested to use a higher value than the default).
- Max Size: This option specifies he maximum size to which the file can grow in megabytes. The minimum value is 1 MB. The default value is 3000 MB for the primary file. The default value is 500 MB for the index and log files. (Note: If intending on capturing face images during enrollment, it is suggested to use a higher value than the default).
- File Growth: This option specifies the growth increment of the file. The File Growth setting for a file cannot exceed the Max Size setting. A value of 0 indicates no growth. The value is specified as a percentage (%). The minimum value is 0% and the maximum value is 100%. The default value is 20 percent.

7. After specifying the path and options for all 3 files, click on the OK button. The following window will be displayed with the status of the setup:



8. The IA3000SDB database will be created in SQL and accessible via SSMS:

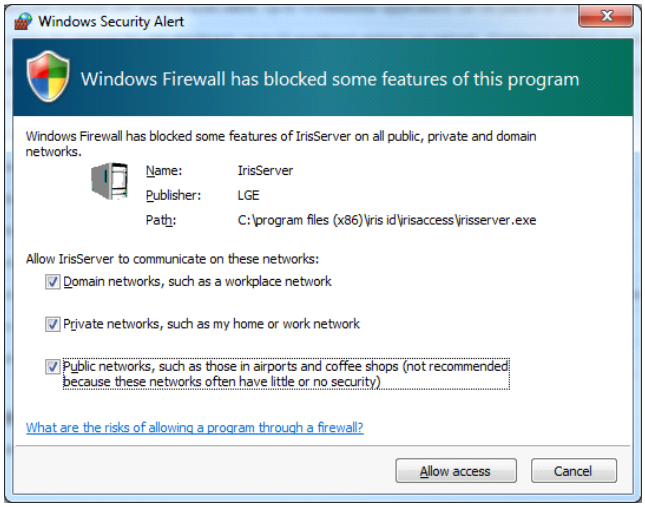


Q.9 Configuring the IrisServer

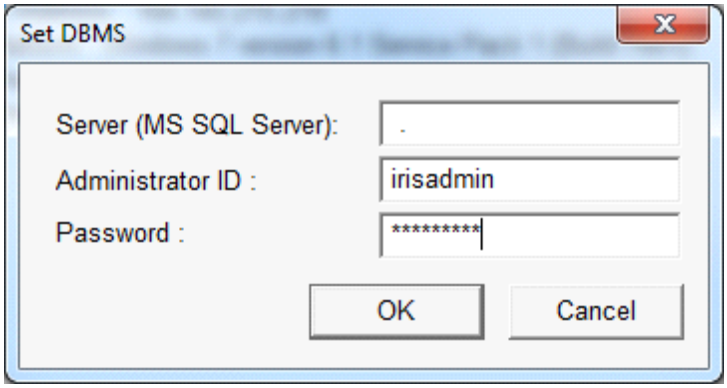
Make sure that the EAC IrisServer Windows Service is set to Manual and the service is not started. Start the IrisServer executable to start the Iris Server.

Note: The following steps apply only if the IrisServer is run manually.

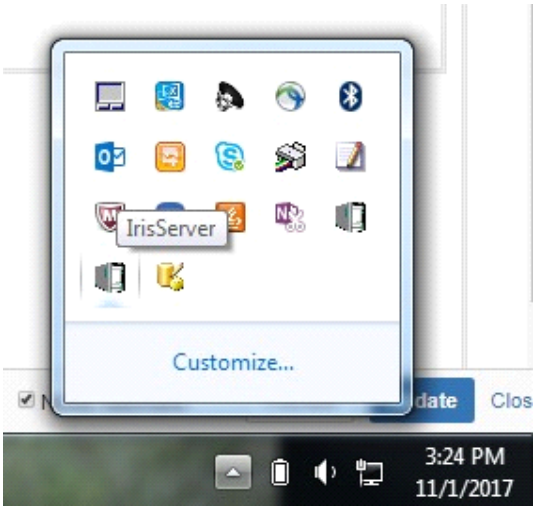
1. When starting IrisServer for the first time, Windows Firewall may pop up a message prompting the user to unblock the program. Select "Unblock" to ensure that the firewall does not block functionality of the IrisServer.



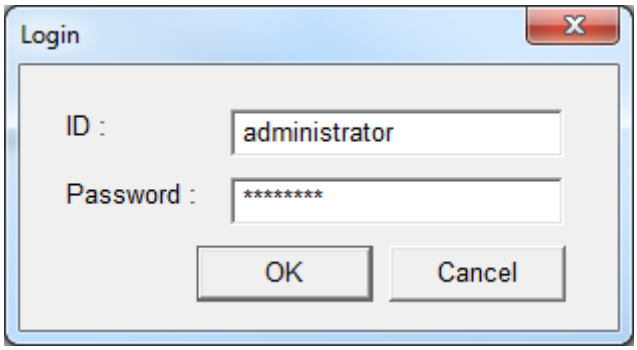
2. On initial start, the IrisServer will ask for the for the DBMS information in order to connect to the database. After this is set initially, it will not be asked for again. The values here can be changed by going into the IrisServer >> Option >> Set DBMS.



3. Once the application is launched, find the application (which will automatically minimize) in the system tray and double-click on the IrisServer.exe icon.

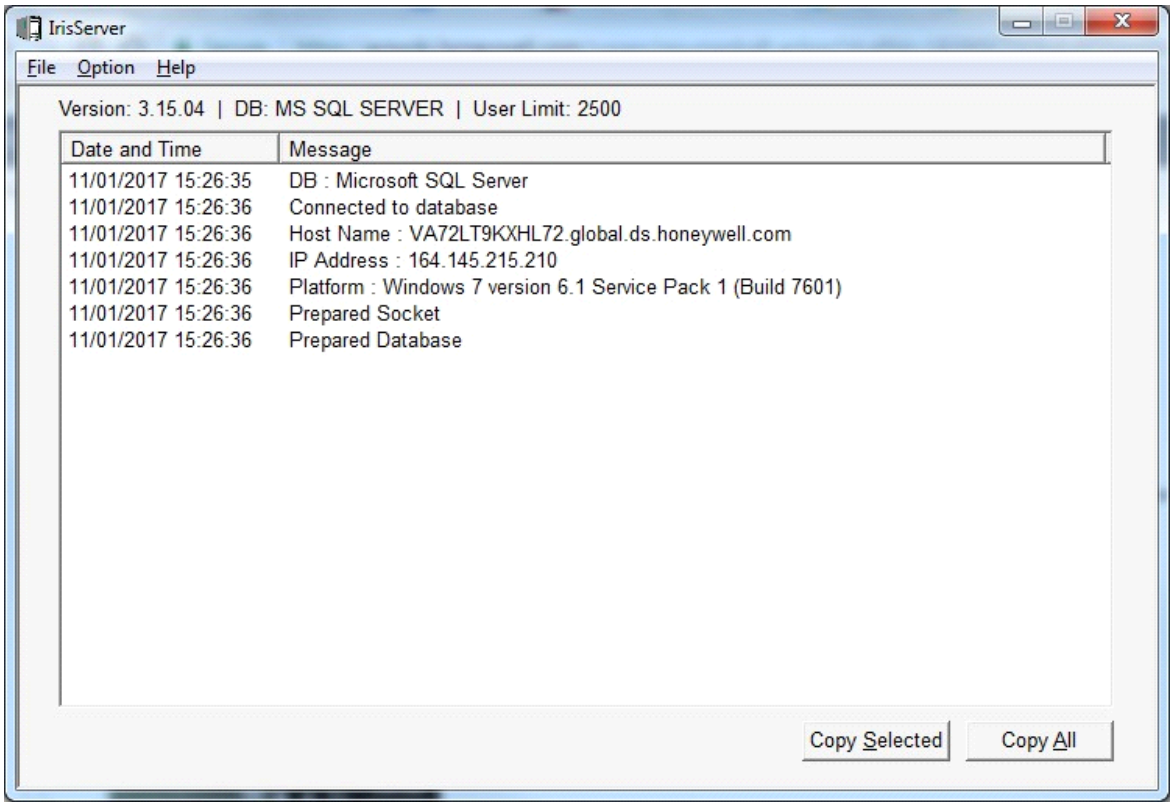


4. Enter the administrator password of iris3000 (this is case sensitive) and press OK. Every time the IrisServer is started from the minimized state, the user will be prompted for the administrator password. **Note:** This is different than the DBMS username and password.



5. The IrisServer dialog box will then be displayed. **Note:** If the IrisServer dialog box is closed, then the service will be stopped. If the IrisServer

dialog box is minimized, it will disappear and go back into the system tray.

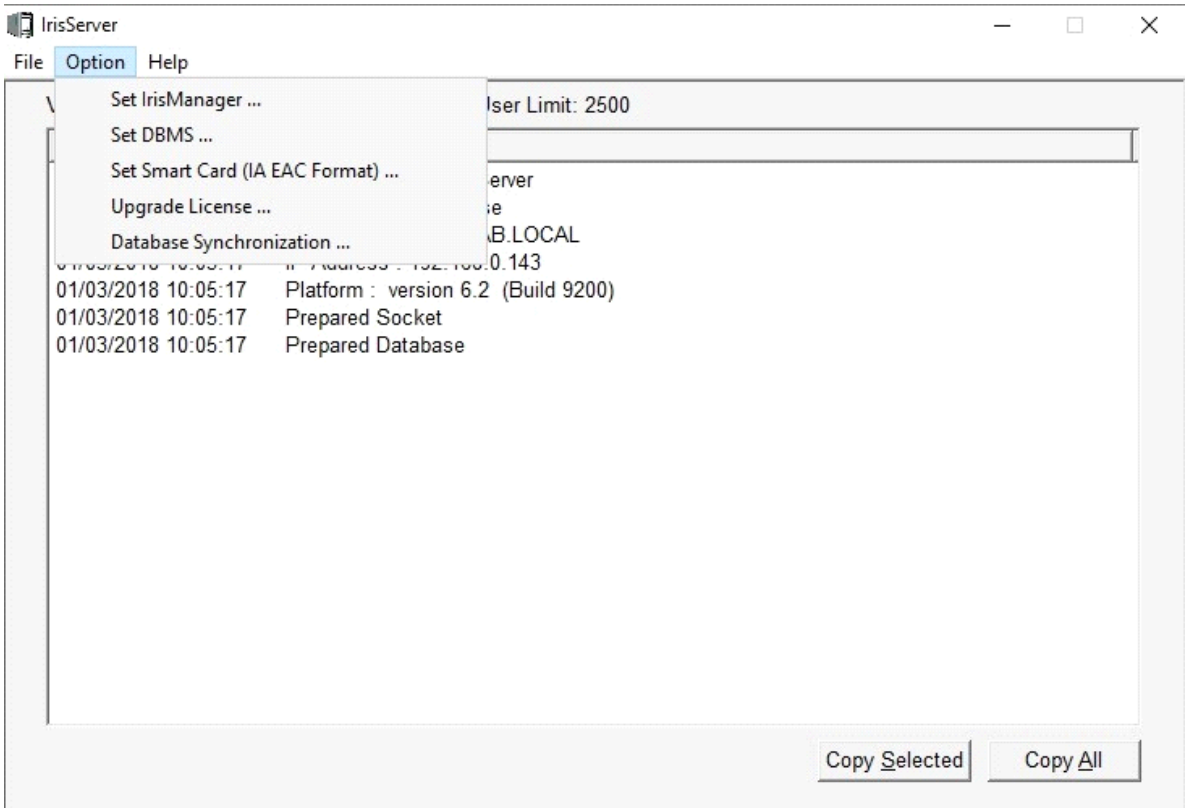


The IrisServer will display important troubleshooting information such as client connections and disconnections as well as connections between the server and the IrisID cameras.

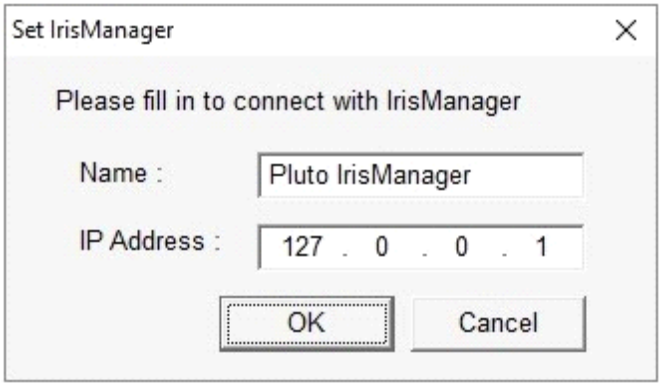
Q.10 Configuring the IrisManager

Initial configuration or modification of the IrisManager can be done through the IrisServer.

1. In IrisServer, select Option > Set IrisManager to display the Set IrisManager dialog box.

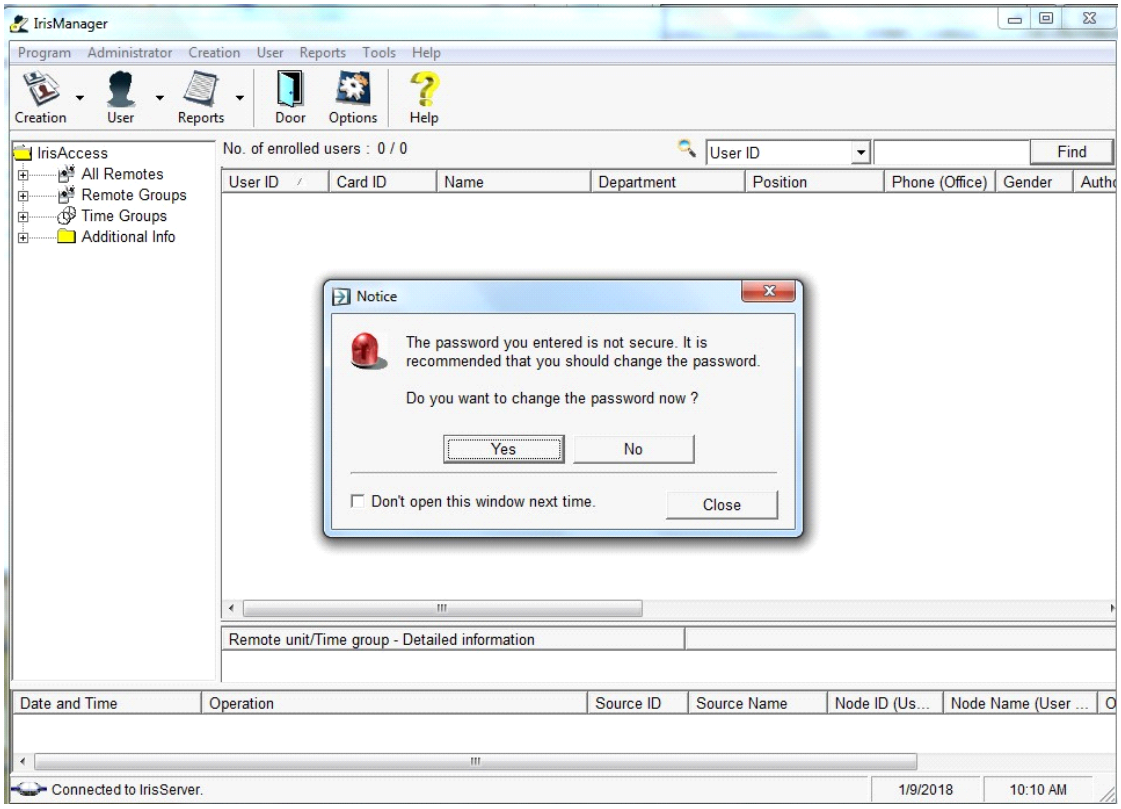


2. Enter the IrisManager name (name can be anything greater than 1 character and not more than 20 characters) and the IP address of the IrisManager. If the IrisManager will be located on the same computer as IrisServer, then the loopback address of 127.0.0.1 is highly recommended as the IP Address. Click OK to confirm the settings.

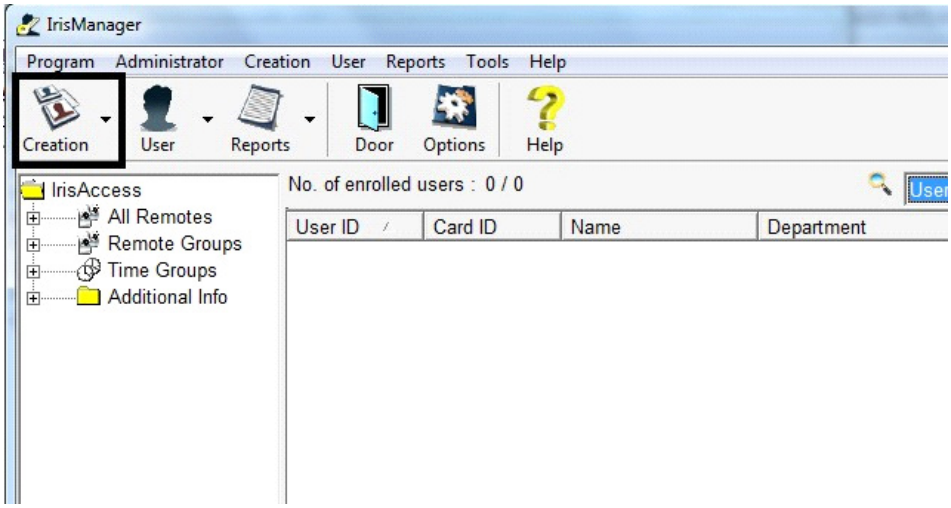


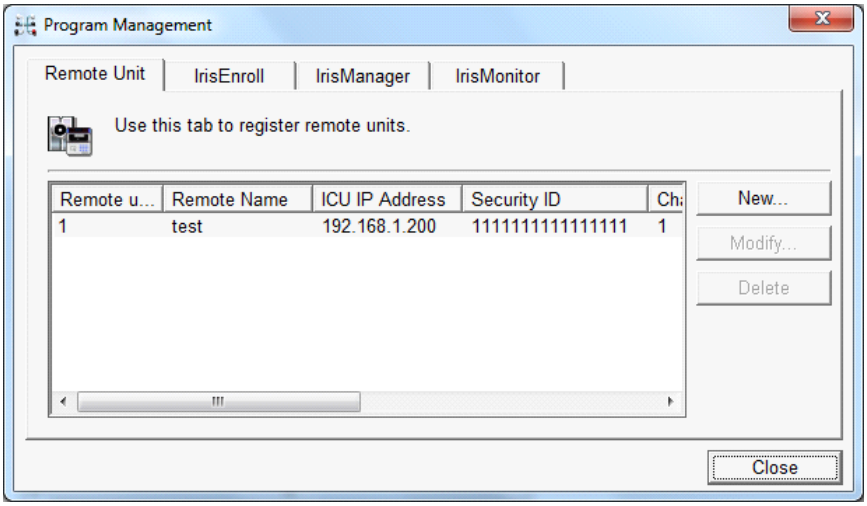
Q.11 Starting the IrisManager

1. Start the IrisManager executable and use the default password of administrator and iris3000. On initial logon, IrisManager will ask the user to change the default password; changing the default password is not required.



2. To setup the connections for the Remote Units, IrisEnroll, IrisManager, and IrisMonitor, click on the Creation button to open up the Program Management dialog box.

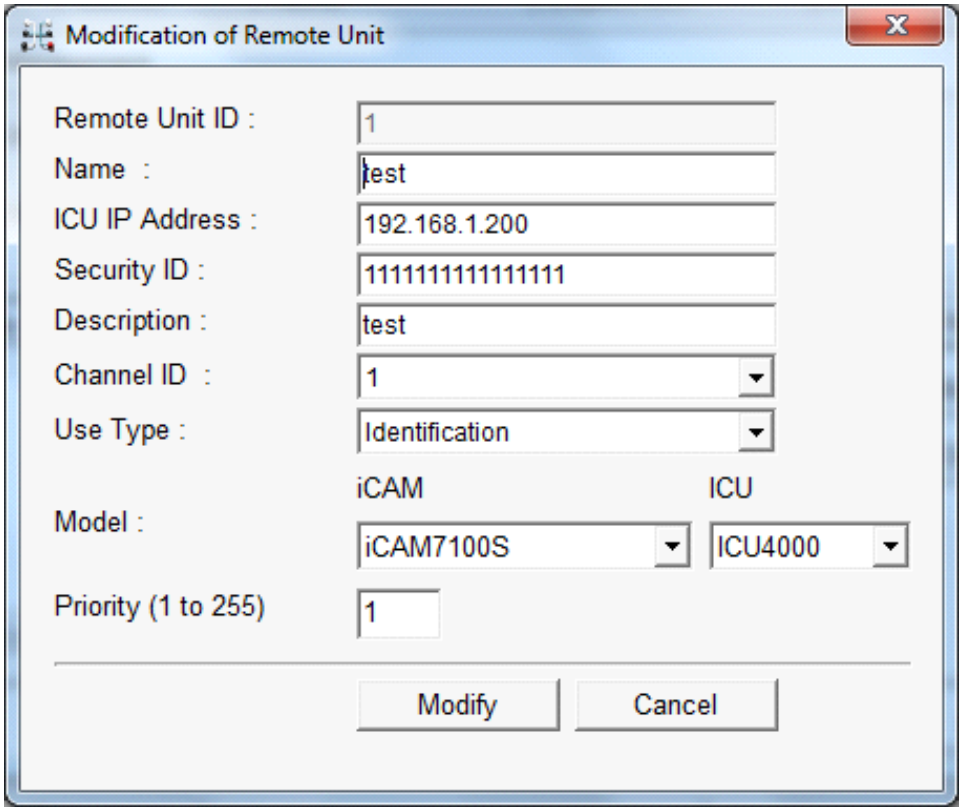




Q.12 Creating the Remote Unit Connection

The Iris camera can be in 2 modes: enrollment or remote. Enrollment means that the camera will be used for enrollment of iris information. Remote means that the camera is in production and used for standard operational scanning.

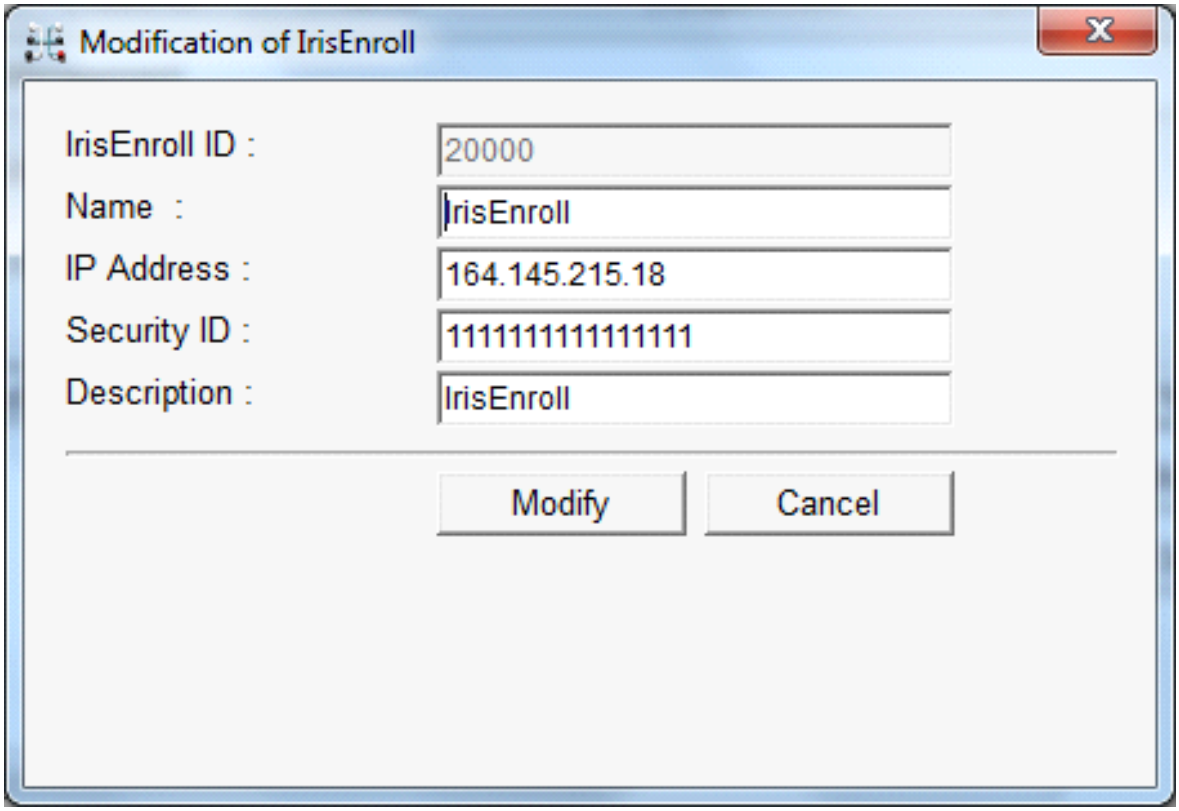
For testing purposes, a remote unit must be configured in software. It can be a dummy connection (meaning the reader does not actually exist), but if there is no remote unit in this list, enrollment in Pro-Watch will error out.



When adding an operational remote unit, verify that the Security ID matches what is programmed in the camera through the web server.

Q.13 Creating the IrisEnroll Connection

Register a new instance of IrisEnroll from this tab. This is the software will be handle the actual enrollment.



The Security ID here must match what is configured in Pro-Watch in Advanced Badging. This Security ID should not be confused with the security ID set during the Remote Unit step.

- **If Pro-Watch is installed on the same computer as the IrisServer,** the Iris ID documentation recommends using the standard loopback IP address of 127.0.0.1 for the IrisEnroll.
- **If Pro-Watch is not installed on the IrisServer computer**, you must use the IP address of the IrisServer computer.

During testing, it was found that there was an issue when connecting using the loopback address. This is because there is a limit of connections on a single machine using the idatatoolkit SDK for Pro-Watch. As a result, it is recommended that the actual IP address be used for this step. In Pro-Watch, when setting up the connection to the Iris application, either the IP address or loopback address can be used.

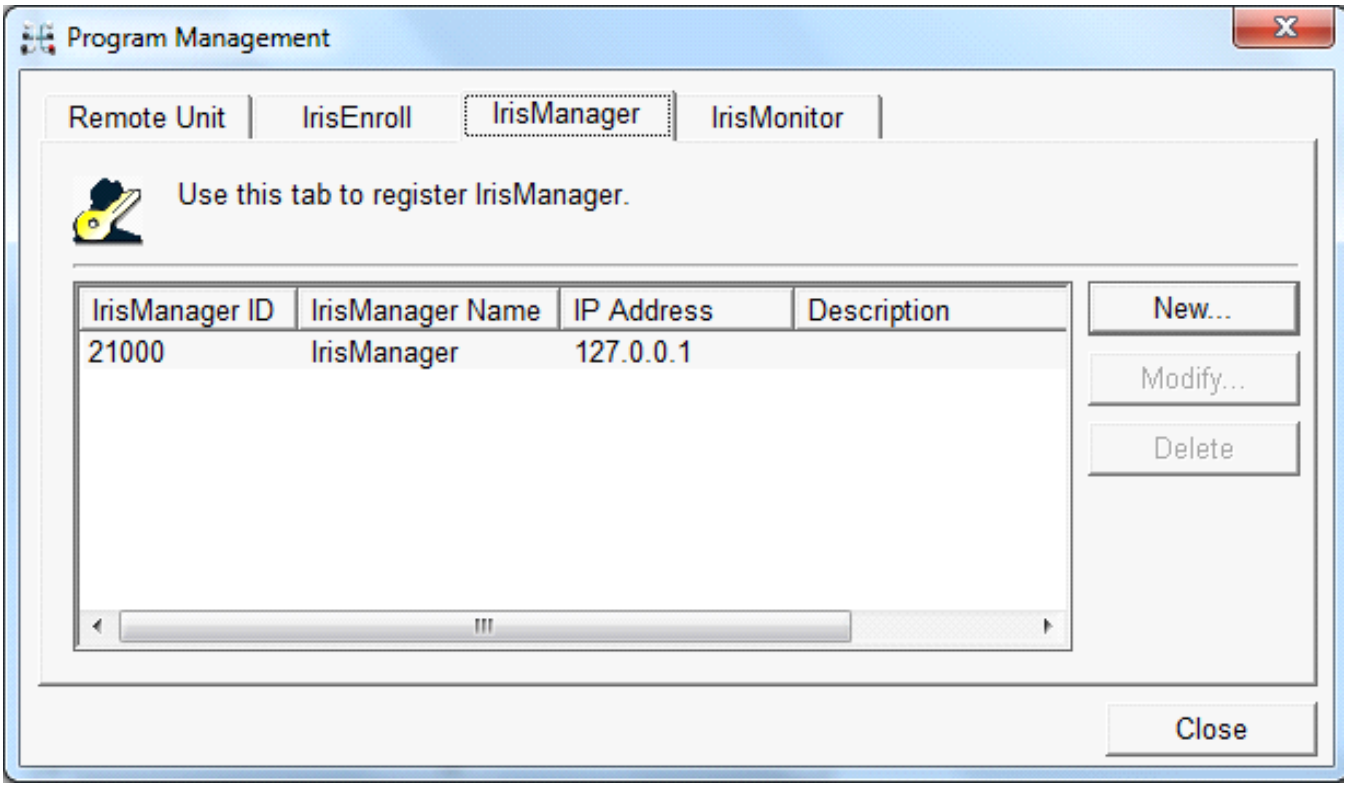
For example:

Iris Enroll IP	Pro-Watch Connection IP (In Advanced Badging)

Actual IP (e.g. 192.168.0.10)	192.168.0.10 or 127.0.0.1 (if Pro-Watch is on the same server)
Loopback IP (127.0.0.1)	Do not use. Pro-Watch will not connect.

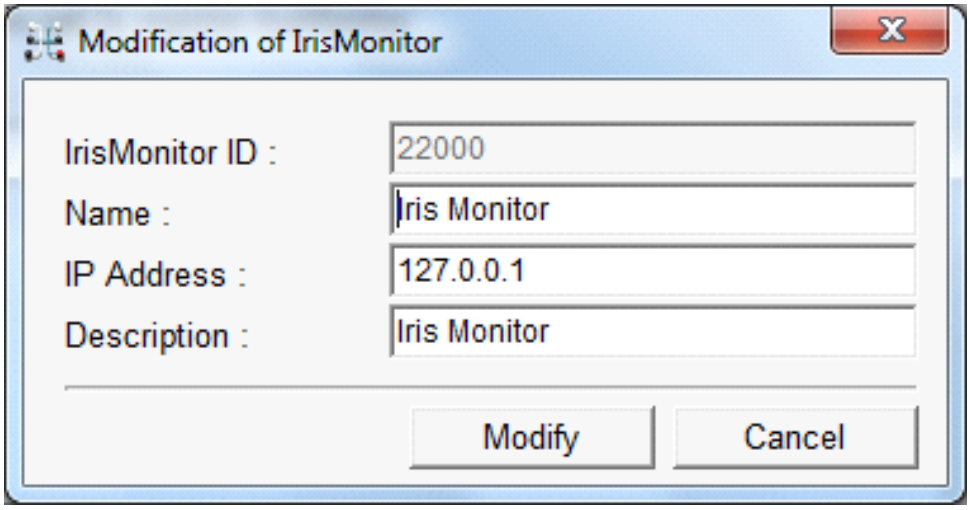
Q.14 Creating the Iris Manager Connection

The connection information for Iris Manager should already be set:



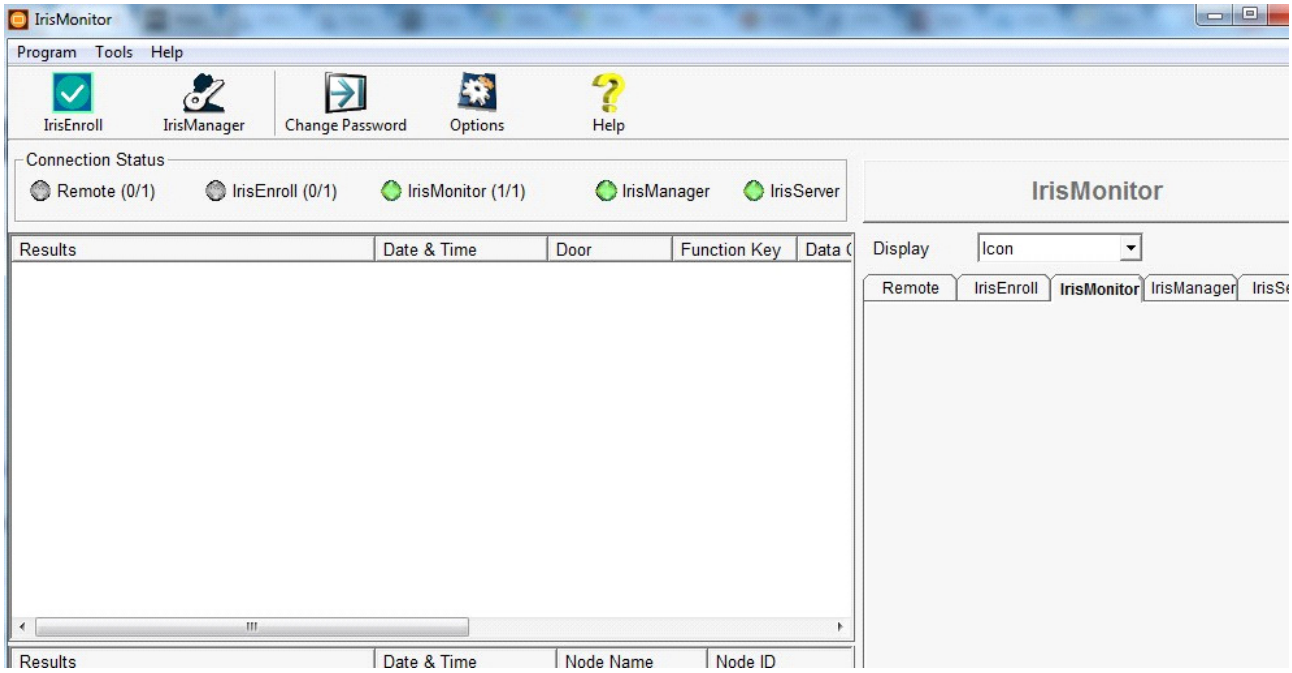
Q.15 Creating the Iris Monitor Connection

IrisMonitor is used to monitor connections to the different components in the Iris System.



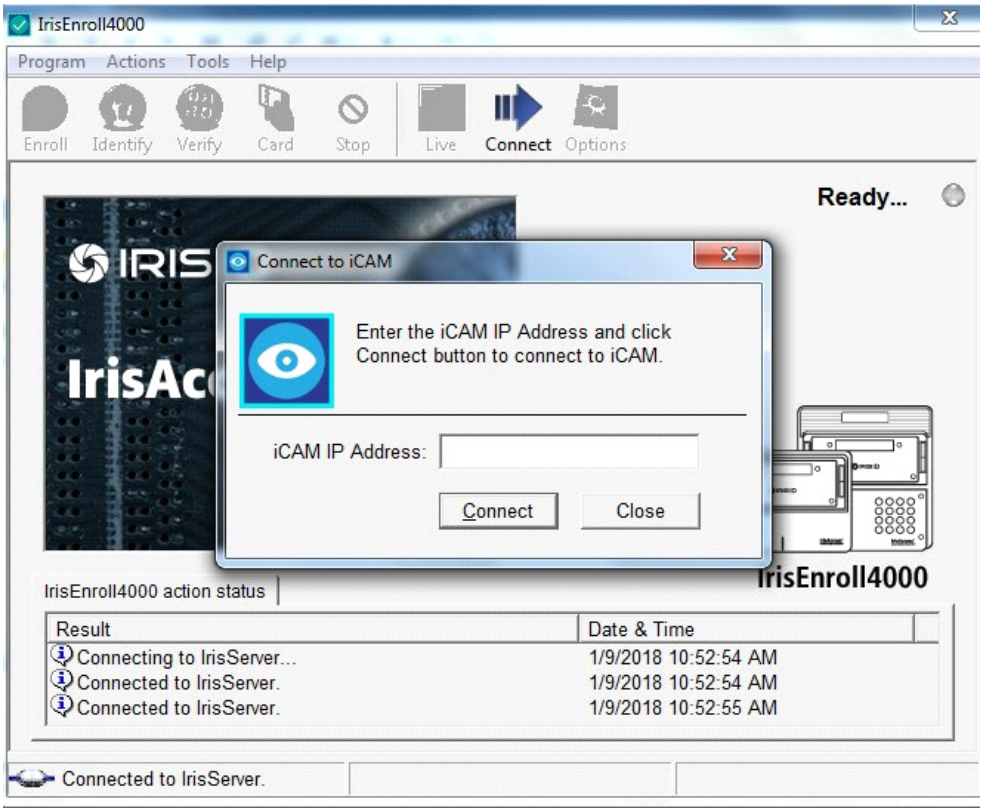
Q.16 Using Iris Monitor

Start the IrisMonitor application and login using the default username of administrator and password of iris3000. The IrisMonitor can be used to monitor active connections to the Iris system (in addition to IrisServer).



Q.17 Using Iris Enroll

Start the IrisEnroll4000 application, set the IP address of IrisEnroll and login using the default username of administrator and password of iris3000. Enter the IP address of the enrollment camera and IrisEnroll will connect to the camera. This can be used to check the connection to the camera as a form of troubleshooting.



Only one IrisEnroll connection can be active at one time. If IrisEnroll4000 is running and connected, then Pro-Watch will be unable to connect.

Q.18 Connecting to the iCAM Web Configuration

Each device on the IrisAccess system requires a unique static IP Address on the network. It is recommended configuring each device with this unique IP Address before connecting the devices to the network. The IP address of the iCAM can be changed by using the iCAM Configuration Interface (web configuration), which is accessed through a web browser.

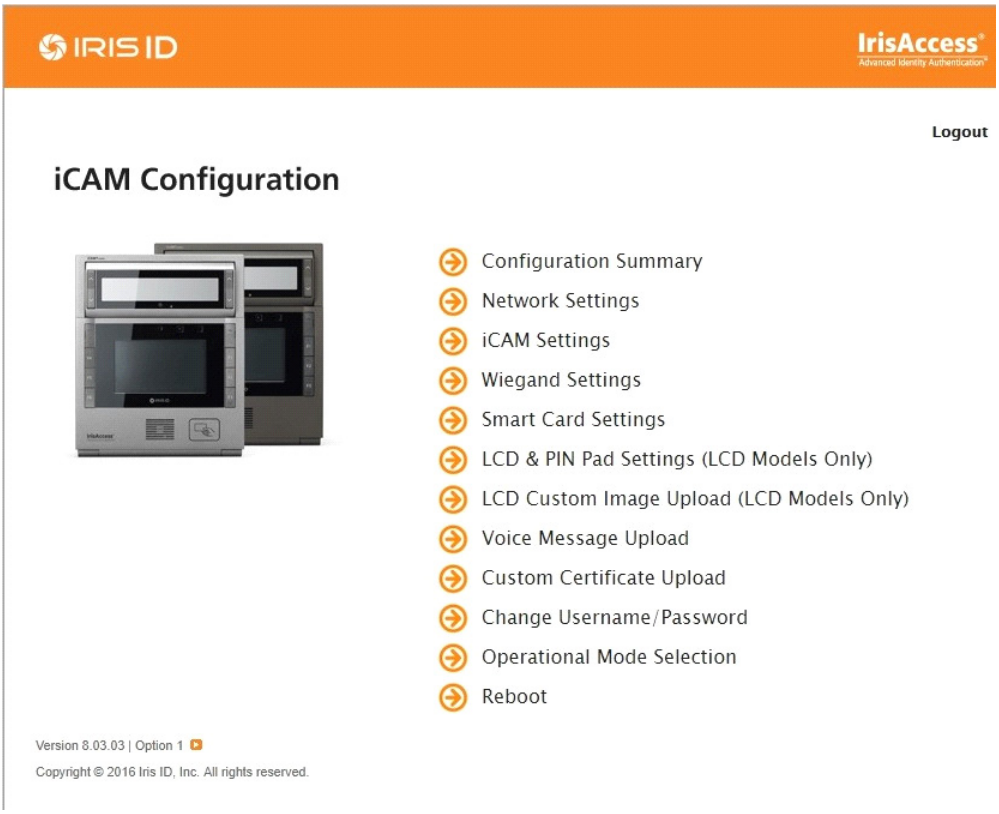
Note: If the IP Address of the iCAM is not known, it can be determined by pressing and holding the up tilt button of the iCAM for at least 10 seconds. The IP Address will be announced from the iCAM speaker.

In order to access the iCAM Configuration Interface, the computer must be on the same network subnet as the iCAM's default IP Address of 192.

168.5.100. To change these settings on the computer, change the adapter settings of the network device and use the 192.168.5.250 (if available) IP Address along with the 255.255.255.0 subnet and 192.168.5.1 gateway.

An Internet connection is not required to access or use the iCAM web configuration. Only a network connection between the computer and the iCAM is required. Use a web browser to navigate to the iCAM using the default IP address: https://192.168.5.100. To login, the username is iCA M7000 and the password is iris7000. The login credentials entry for both username and password are case sensitive.

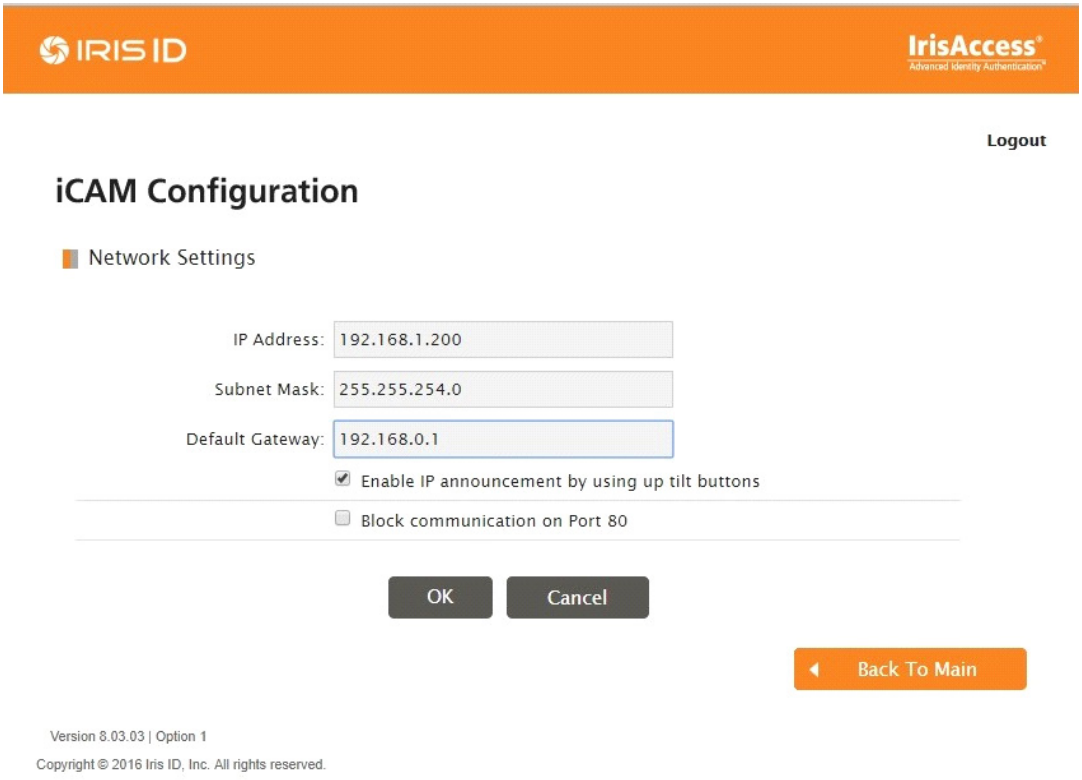
After logging in, the main configuration page is displayed:

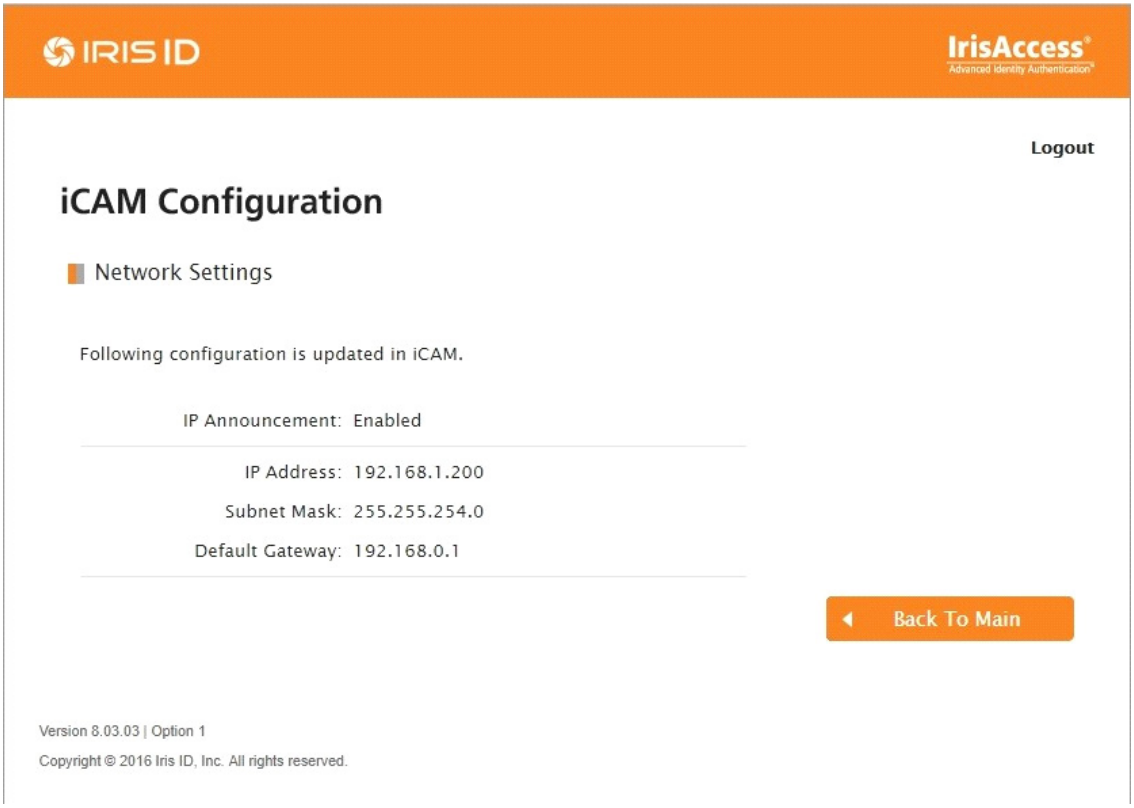


Q.19 Configuring the IP Address of the iCAM

From the main configuration page, select Network Settings to be taken to the iCAM Configuration page for the network settings. Here, enter the desired IP address, the subnet mask, and the default gateway. There are also options here to Enable IP announcement by using up/down tilt buttons and Block communication on Port 80.

Enter the desired values and click OK to confirm the changes.

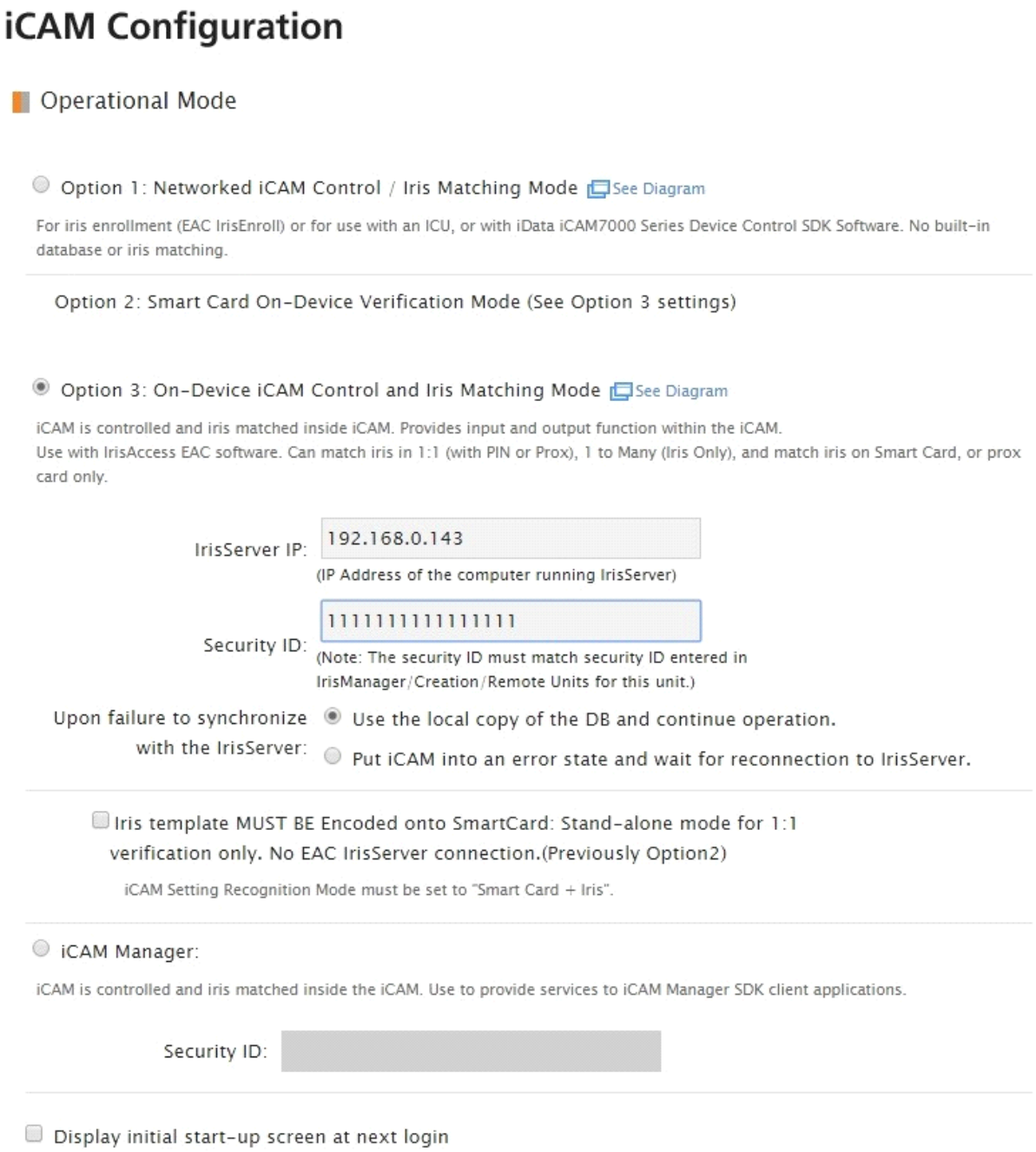

IRIS ID
IrisAccess
Advanced Identity Authentication
Logout
iCAM Configuration
Network Settings
IP Address: 192.168.1.200
Subnet Mask: 255.255.254.0
Default Gateway: 192.168.0.1
Enable IP announcement by using up tilt buttons
Block communication on Port 80
OK
Cancel
Back To Main
Version 8.03.03 | Option 1
Copyright © 2016 Iris ID, Inc. All rights reserved.


IRIS ID
IrisAccess
Advanced Identity Authentication
Logout
iCAM Configuration
Network Settings
Following configuration is updated in iCAM.
IP Announcement: Enabled
IP Address: 192.168.1.200
Subnet Mask: 255.255.254.0
Default Gateway: 192.168.0.1
Back To Main
Version 8.03.03 | Option 1
Copyright © 2016 Iris ID, Inc. All rights reserved.

Q.20 Changing the Operational Mode of the iCAM

To change the operational mode of the iCAM from enrollment to a remote unit, click on Operational Mode Selection from the main configuration menu.

Here, change the operational mode from Option 1, which is used for iris enrollment to Option 3, which is used for remote operation. If Option 3 is selected, enter the IP address of the IrisServer and the security ID. Click OK to confirm the changes. The iCAM should now reboot.



Q.21 Security and Ports

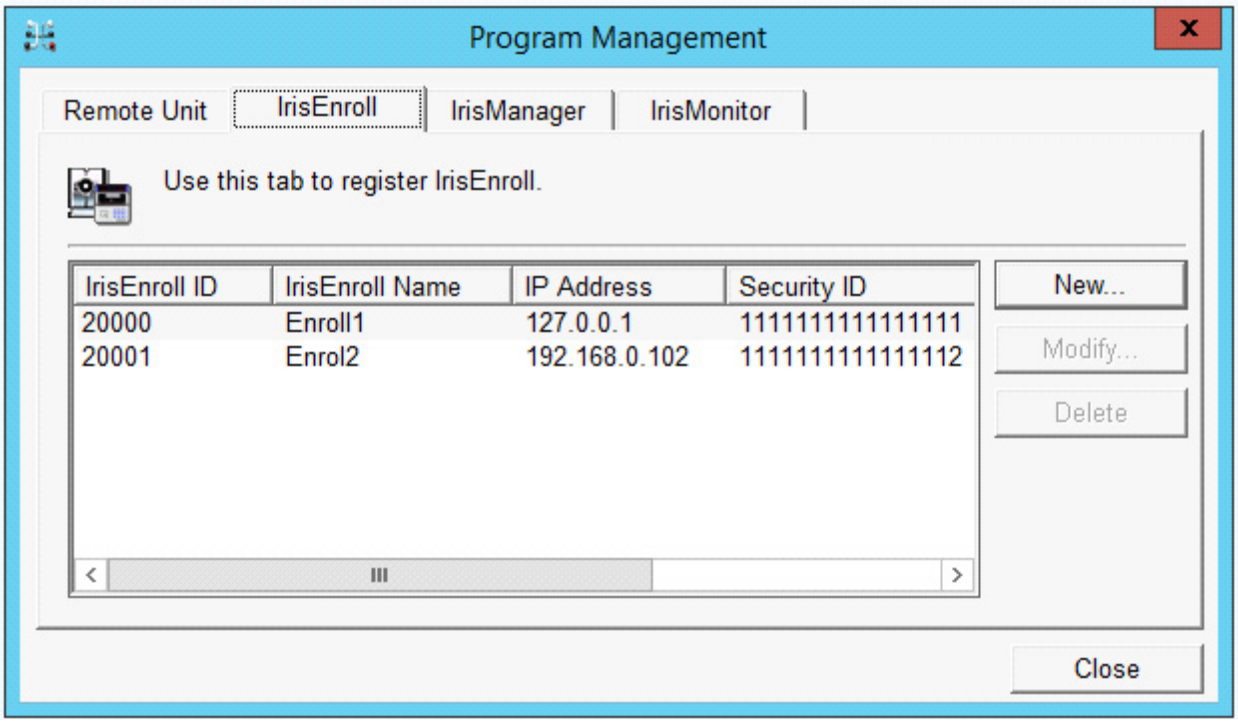
The following network ports is used and needs to be opened in the firewall for Iris operation:

Server	Client(s) Features	Port Number	Remarks
IrisServer	IrisEnroll Application	15000	
IrisServer	IrisManager Application	15001	
IrisServer	IrisMonitor Application	15002	
IrisServer	Remote Unit (Non-SSL) ICU or iCAM7000/7000s Option 3	15003	
IrisServer	Remote Unit (SSL) iCAM7000 Option 3 iCAM7000s Option 3 ICU7000-2	15004	SSL communication is configurable (if disabled, non-SSL will be used). SSL is supported in iCAM7000-Option 3 from EAC v3.13 onwards. SSL is supported in iCAM7000S-Option 3 & ICU7000-2 from EAC v.3.15 onwards.
iCAM7000 ICUs	Firmware install application iCAM7000: iCAM7000Update ICUs: IrisICUAdminX000	23 (Telnet) 21 (FTP)	iCAM7000: Up to EAC v3.13 only. ICU7000: Up to EAC v3.14 only.
iCAM7000 iCAM7000s ICU7000-2	Firmware install application	22 (SSH)	iCAM7000: since EAC v3.14. ICU7000: Since EAC v3.15. iCAM7000S: Always, included in EAC since EAC v3.14. ICU7000-2: always, supported in EAC since EAC v3.12.
iCAM (Option 1)	iCAM Device Control SDK client	16000	
iCAM (Option 1)	iCAM Smartcard SDK client	15999	

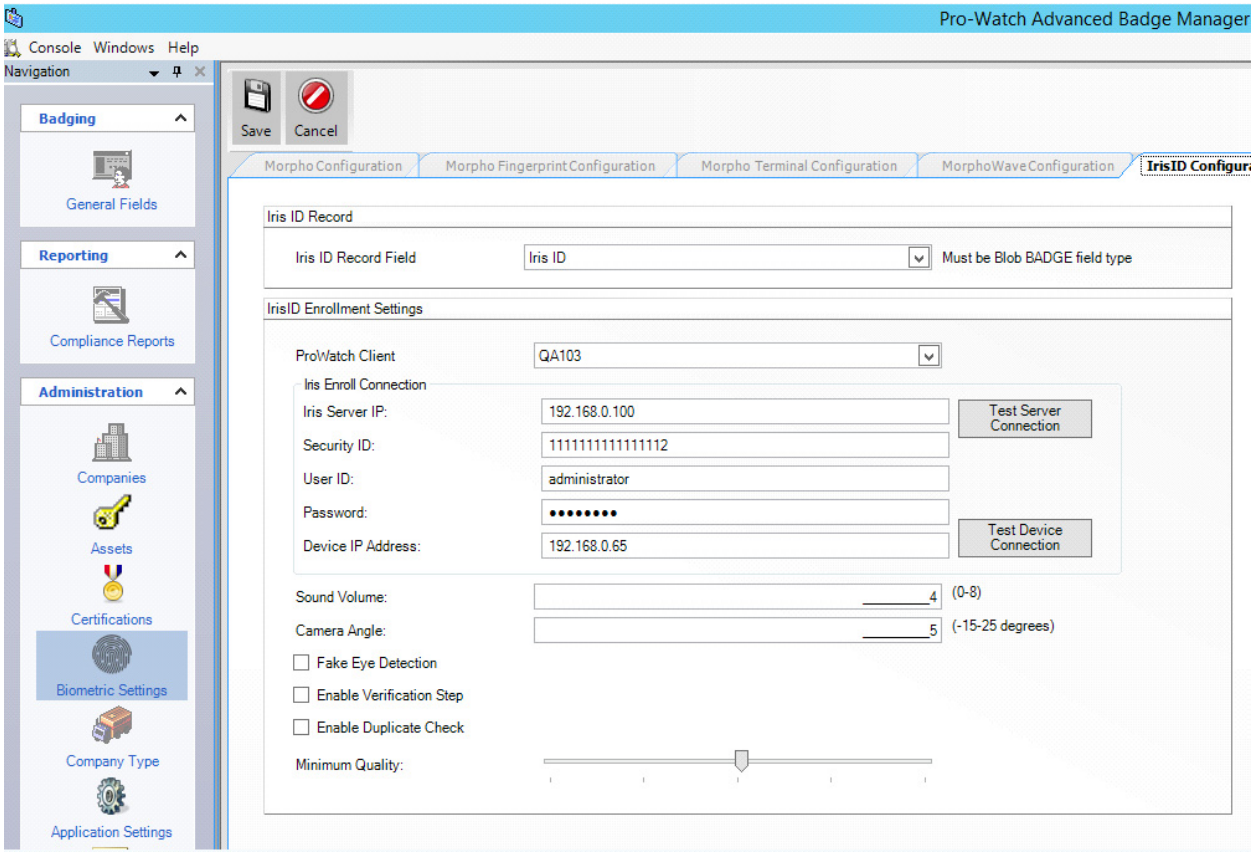
Server	Client(s) Features	Port Number	Remarks
iCAM4000 iCAM7000 ICU7000 iCAM7000S ICU7000-2	iCAM4000: Firmware install acpplication. iCAM7000, ICU7000, iCAM7000S & ICU7000-2: Not used	16061	Not used so far in iCAM7000, ICU7000, iCAM7000s & ICU7000-2.
iCAM4000 iCAM7000 ICU7000 iCAM7000S ICU7000-2	Find iCAM / Find ICU7000 / Find ICU7000-2 Locate iCAM (beep from iCAM's speaker)	55555 (UDP)	
iCAM4000 iCAM7000 (prior to https support) ICU7000 (prior to https support)	Web Configuration via browser	80 (http)	
iCAM7000 ICU7000 iCAM7000S ICU7000-2	Web Configuration via browser	443 (https)	

Q.22 Pro-Watch Configuration

Iris Remote Units must be configured in IrisManager prior to enrollment in Pro-Watch:

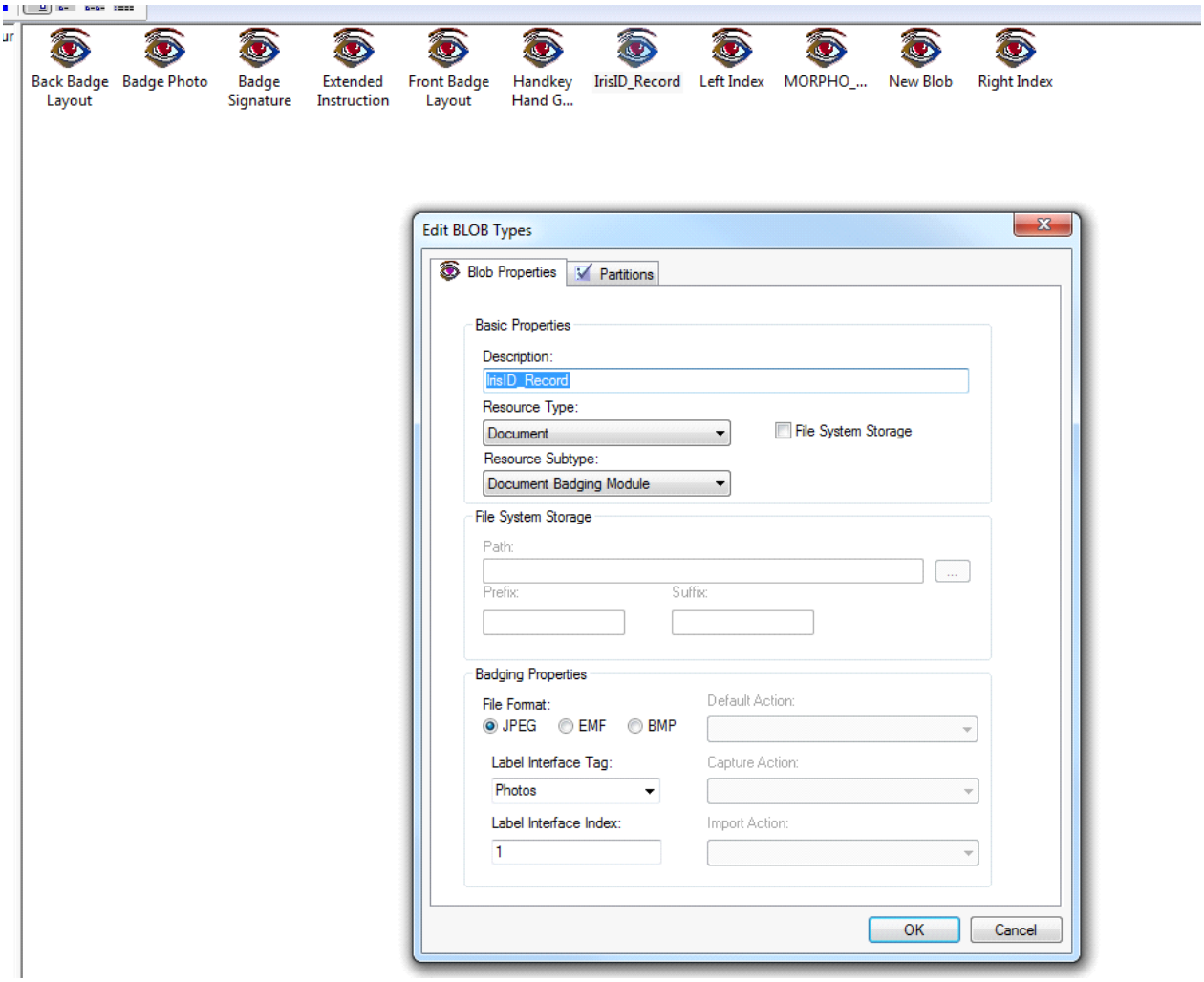


Each Pro-Watch badge client must be configured in IrisManager. In the example above, there are 2 enrollment clients. Each must have its own Security ID that must match the Biometric setting in Advanced Badge.

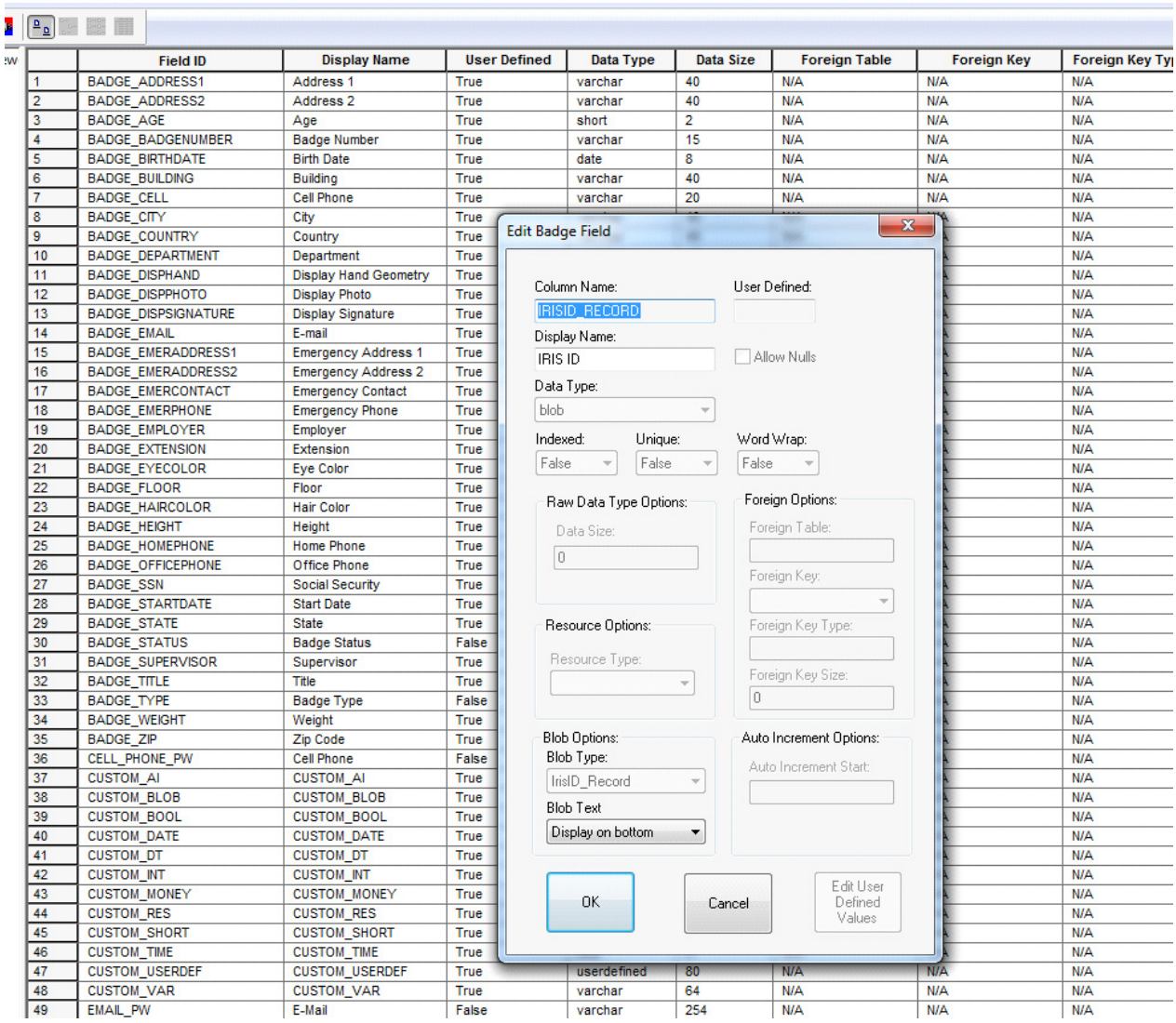


Q.22.1 Iris ID Badge Field

1. Go to Pro-Watch **Database > BLOB Type** and create a new BLOB type of Resource Type Document.

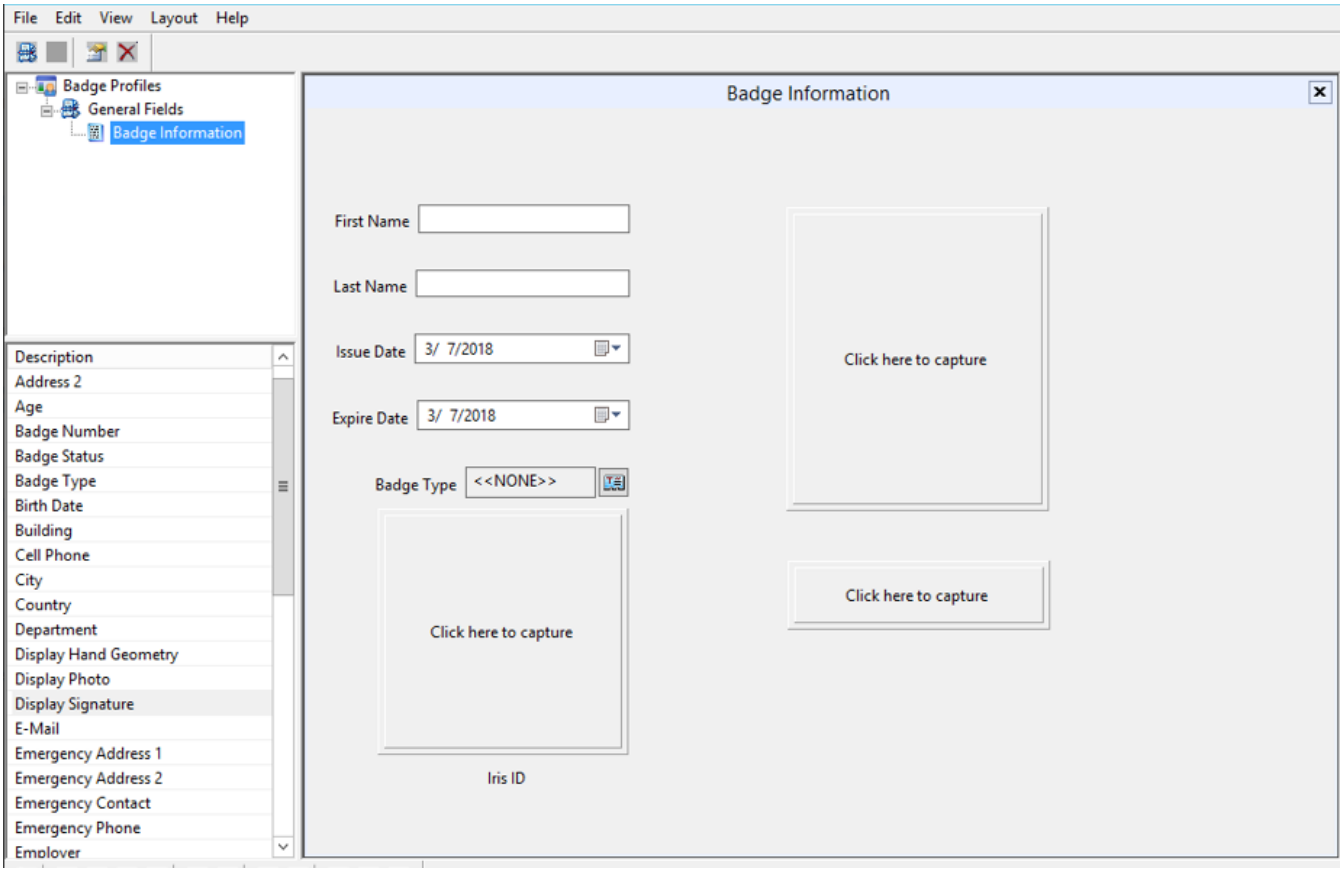


2. Go to Pro-Watch **Administration >> Badge Utilities >> Badge Fields** and create a new badge field of data type BLOB and set it to the BLOB type that was created in the previous step.



	Field ID	Display Name	User Defined	Data Type	Data Size	Foreign Table	Foreign Key	Foreign Key Ty
1	BADGE_ADDRESS1	Address 1	True	varchar	40	N/A	N/A	N/A
2	BADGE_ADDRESS2	Address 2	True	varchar	40	N/A	N/A	N/A
3	BADGE_AGE	Age	True	short	2	N/A	N/A	N/A
4	BADGE_BADGENUMBER	Badge Number	True	varchar	15	N/A	N/A	N/A
5	BADGE_BIRTHDATE	Birth Date	True	date	8	N/A	N/A	N/A
6	BADGE_BUILDING	Building	True	varchar	40	N/A	N/A	N/A
7	BADGE_CELL	Cell Phone	True	varchar	20	N/A	N/A	N/A
8	BADGE_CITY	City	True					N/A
9	BADGE_COUNTRY	Country	True					N/A
10	BADGE_DEPARTMENT	Department	True					N/A
11	BADGE_DISPHAND	Display Hand Geometry	True					N/A
12	BADGE_DISPPHOTO	Display Photo	True					N/A
13	BADGE_DISPSIGNATURE	Display Signature	True					N/A
14	BADGE_EMAIL	E-mail	True					N/A
15	BADGE_EMERADDRESS1	Emergency Address 1	True					N/A
16	BADGE_EMERADDRESS2	Emergency Address 2	True					N/A
17	BADGE_EMERCONTACT	Emergency Contact	True					N/A
18	BADGE_EMERPHONE	Emergency Phone	True					N/A
19	BADGE_EMPLOYER	Employer	True					N/A
20	BADGE_EXTENSION	Extension	True					N/A
21	BADGE_EYECOLOR	Eye Color	True					N/A
22	BADGE_FLOOR	Floor	True					N/A
23	BADGE_HAIRCOLOR	Hair Color	True					N/A
24	BADGE_HEIGHT	Height	True					N/A
25	BADGE_HOMEPHONE	Home Phone	True					N/A
26	BADGE_OFFICEPHONE	Office Phone	True					N/A
27	BADGE_SSN	Social Security	True					N/A
28	BADGE_STARTDATE	Start Date	True					N/A
29	BADGE_STATE	State	True					N/A
30	BADGE_STATUS	Badge Status	False					N/A
31	BADGE_SUPERVISOR	Supervisor	True					N/A
32	BADGE_TITLE	Title	True					N/A
33	BADGE_TYPE	Badge Type	False					N/A
34	BADGE_WEIGHT	Weight	True					N/A
35	BADGE_ZIP	Zip Code	True					N/A
36	CELL_PHONE_PW	Cell Phone	False					N/A
37	CUSTOM_AI	CUSTOM_AI	True					N/A
38	CUSTOM_BLOB	CUSTOM_BLOB	True					N/A
39	CUSTOM_BOOL	CUSTOM_BOOL	True					N/A
40	CUSTOM_DATE	CUSTOM_DATE	True					N/A
41	CUSTOM_DT	CUSTOM_DT	True					N/A
42	CUSTOM_INT	CUSTOM_INT	True					N/A
43	CUSTOM_MONEY	CUSTOM_MONEY	True					N/A
44	CUSTOM_RES	CUSTOM_RES	True					N/A
45	CUSTOM_SHORT	CUSTOM_SHORT	True					N/A
46	CUSTOM_TIME	CUSTOM_TIME	True					N/A
47	CUSTOM_USERDEF	CUSTOM_USERDEF	True	userdefined	80	N/A	N/A	N/A
48	CUSTOM_VAR	CUSTOM_VAR	True	varchar	64	N/A	N/A	N/A
49	EMAIL_PW	E-Mail	False	varchar	254	N/A	N/A	N/A

3. In the **Badge Builder** module, add this new badge field to the Pro-Watch badge profile by dragging and dropping it from the left-hand list to the Badge Information pane.



Copyright © Honeywell Inc. All Rights Reserved

Honeywell

Software Keys Licensing

R

In this appendix ...

Overview
Quick Start
How to View License Information
How to Supersede a License
How to Transfer the License to Another Machine
How to Terminate a License
Cut-over/Migration Licenses

R.1 Overview

Pro-Watch Software Keys is the new secure licensing system that replaces the dongle for Honeywell's Pro-Watch family of security access products.

Software Keys application:

- Reads the License information from the Server.
- Displays the grace period and thus lets the user know when Pro-Watch has to be licensed to remain operational.

1.2 Quick Start

1.2.1 Two Options to Install a License Certificate

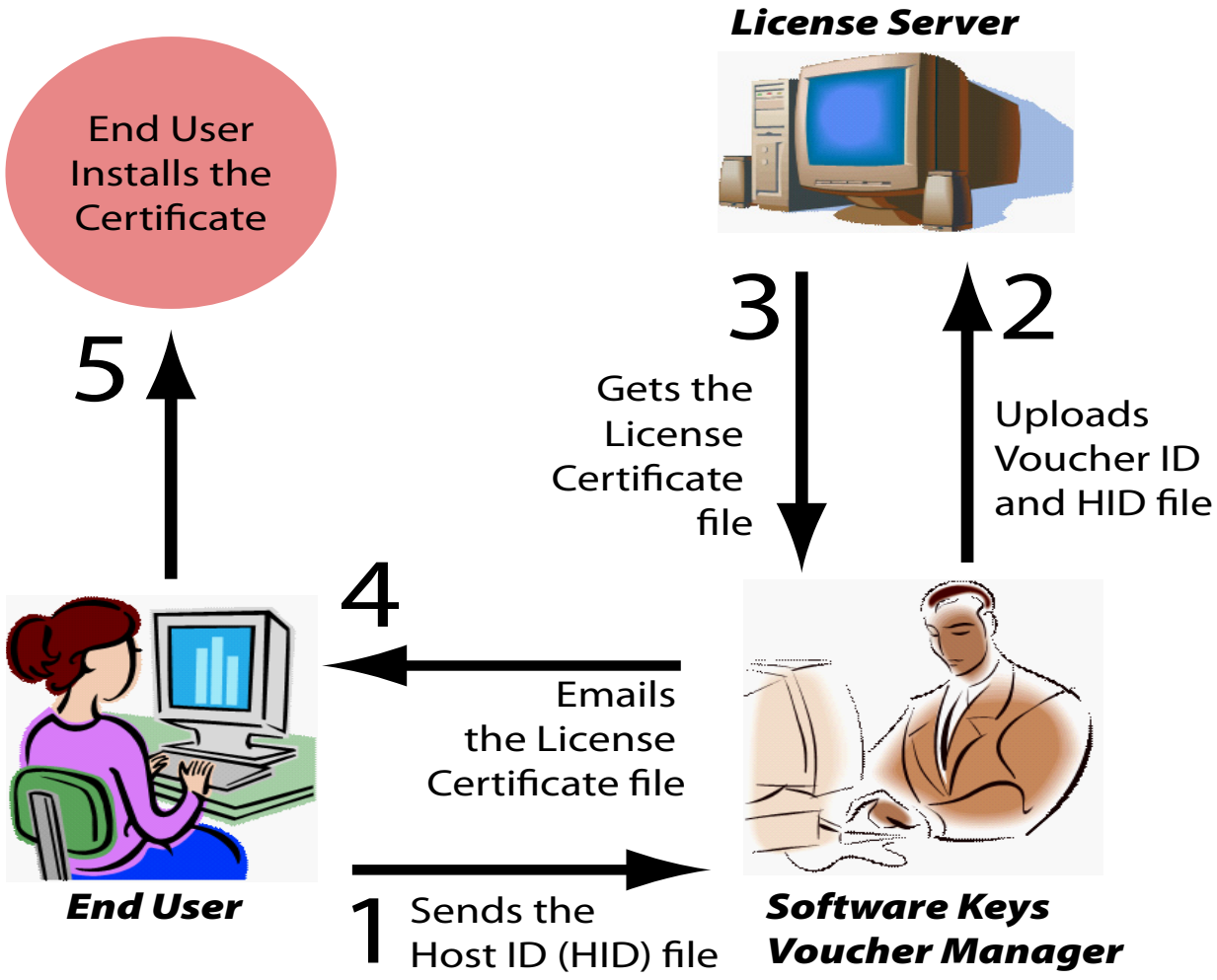
You have two options to install a Pro-Watch license:

1. **Regular License.** This is generated by the Software Keys Voucher Manager.
2. **Default Demo License.** This is a one-time-only demo license that's shipped with Pro-Watch and is good for 30 days. It is the easiest and preferred method to try out Pro-Watch with limited functionalities.

Each option is explained below.

1.2.2 How to Install a Regular License

The end user can generate a regular license by following these steps:



STEP 1: The User Contacts Pro-Watch Inside Sales Dept.

The integrator or the end-user (from now on referred to simply as the "user") starts the process by calling Pro-Watch Inside Sales department and placing an order for the Pro-Watch.

The Inside Sales gathers the necessary information and starts the Pro-Watch license certificate acquisition process.

STEP 2: Inside Sales Contacts the User

The Pro-Watch Inside Sales department emails the SoftKey.zip file and the Pro-Watch License Certificate (PDF) to the user.

Note: The **Pro-Watch License Certificate (PDF)** includes the user's **Voucher Number**.

The user unzips the Software Keys file and saves the Pro-Watch Software Keys Automated Server software on to the user machine.

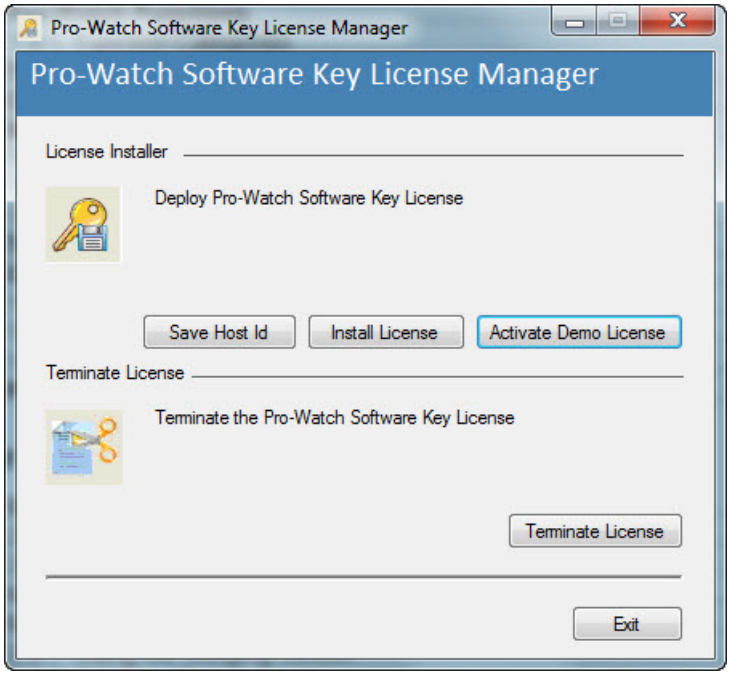
STEP 3a: The User Generates the *HID file

If Pro-Watch is not installed:

1. Unzip the SoftKeys.zip and start the ProWatchSoftwareKeyUtility.exe installation.
2. After installation, double-click **Pro-Watch SoftwareKey Utility** (located on the Windows Desktop).
3. Click **Generate Machine HID Pro-Watch**.
4. Browse and save the automatically generated *.HID file to where you like on your machine.

If Pro-Watch is already installed:

1. Select **Start > All Programs > Pro-Watch > Pro-Watch Software Keys Manager** from the Windows Start menu. Right-click and select "**Run as Administrator**" to launch the **Pro-Watch Software Keys Manager**:



Note: Your screen may look slightly different depending on the Windows version you are using.

2. Click **Save Host ID** to automatically generate an *.HID file. This will open your Windows browser screen.
3. Browse and save the automatically generated *.HID file to where you like on your machine.

STEP 3b: The User Contacts SK Automated Server

1. Browse and find the *.HID file on your machine.
2. Attach the *.HID file to an email with the following:
    - Mail subject = VOUCHID: Vouchernumber (e.g., VOUCHID:PW-123420120101-P-1) **Do not use any spaces and be sure to type out the preceding text properly.**
3. Email the ***.HID file** together with the **Voucher Number** to the **Software Keys Automated Server** at **License.Server@honeywell.com** with a request for a new license.

STEP 4: SK Automated Server Contacts the User

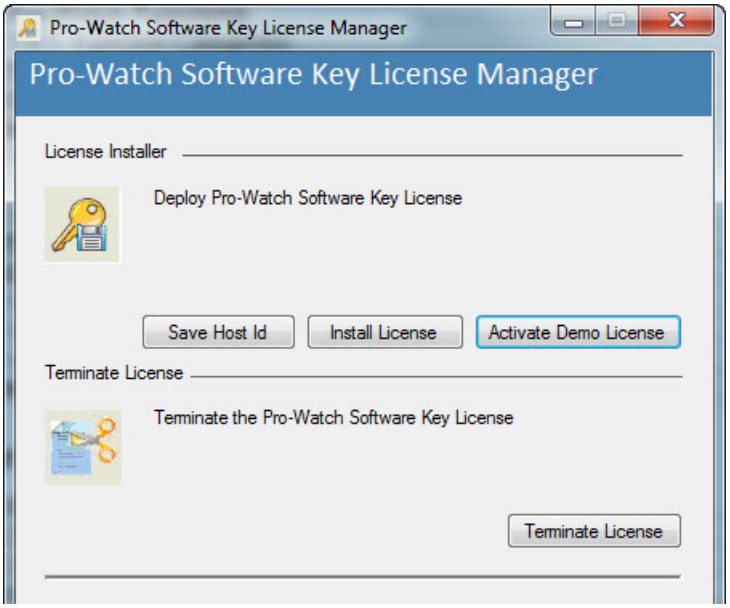
The Software Keys Automated Server generates the license and emails it to the user.

STEP 5: The User Installs the License Certificate

The user installs the Pro-Watch license certificate by following these steps:

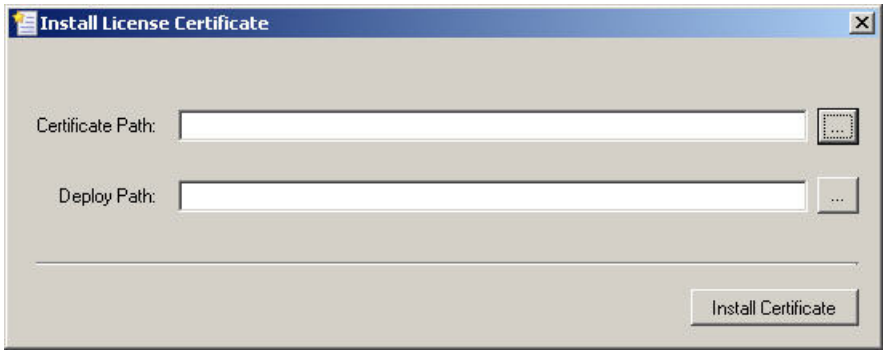
1. Stop the **Pro-Watch** and **SQL** services BEFORE you install the certificate file.
2. Select **Start > All Programs > Pro-Watch > Pro-Watch Software Keys Manager** from the Windows Start menu. Right-click and select

"**Run as Administrator**" to launch the **Pro-Watch Software Keys Manager**:



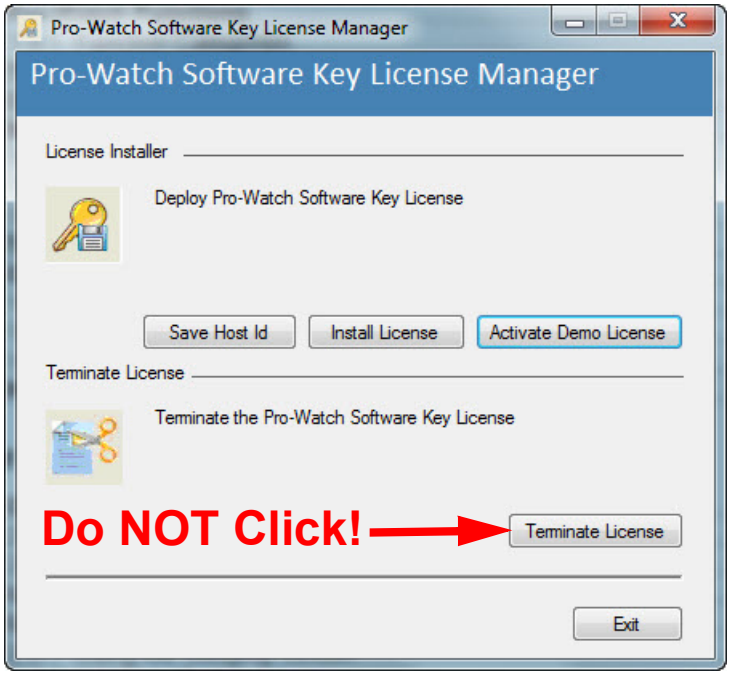
Note: Your screen may look slightly different depending on the Windows version you are using.

3. Click **Install License** to display the **Install License Certificate** dialog box:



4. To fill the **Certificate Path** field, click the browse button on the right and browse back to the location where you've saved the certificate in an earlier step. Select the certificate file and click **OK** to close the browser and enter the path into the **Certificate Path** field.
5. Click **Install Certificate**.
6. Select **Administrative Tools > Services > SQL Server.** Click the **Start Service** button on the tool-bar to restart the **SQL** service. Then select **Administrative Tools > Services > Pro-Watch Server**. Click the **Start Service** button on the tool-bar to restart the **Pro-Watch** service for the license to take effect.

Caution: After installing a license, the **Terminate License button** will be enabled. **Do not click this button** unless you want to terminate the license:

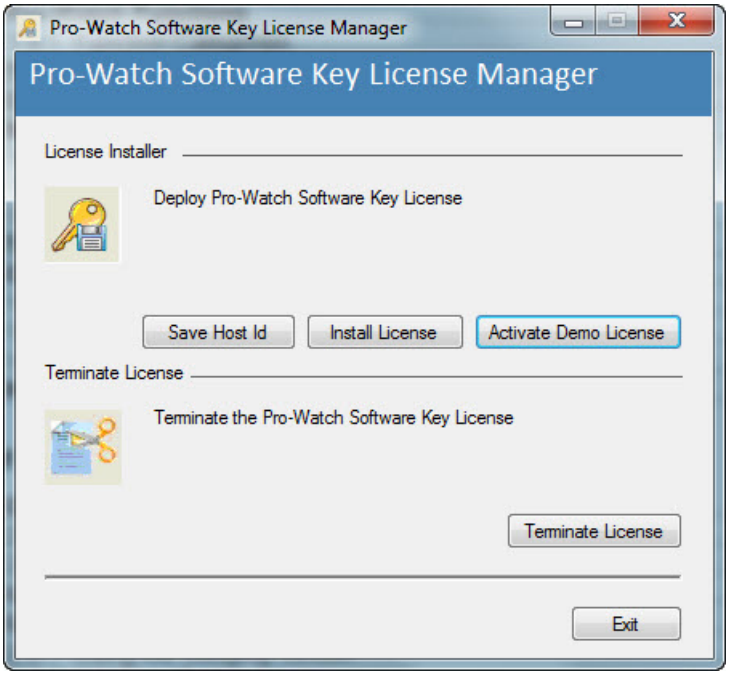


1.2.3 How to Activate a Demo License

The end user can activate a default 30-day demo license after installing Pro-Watch by following these steps:

1. Select **Start > All Programs > Pro-Watch > Pro-Watch Software Keys Manager** from the Windows Start menu. Right-click and select

"**Run as Administrator**" to launch the **Pro-Watch Software Keys Manager**:



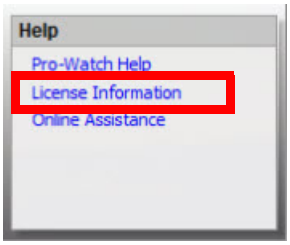
Note: Your screen may look slightly different depending on the Windows version you are using.

2. Click **Activate Demo License**.
3. Start or restart **Pro-Watch Server service**:
    a. If the Pro-Watch Server service is already started, restart it for the demo license to take effect.
    b. Otherwise, start the Pro-Watch Server service for the demo license to take effect. The Pro-Watch Server service can be found in the Windows Services by launching "**Services**" from the **Windows Control Panel > Administrative Tools** or typing "Services.msc" in the **Run** command on the **Start** menu.

1.3 How to View License Information

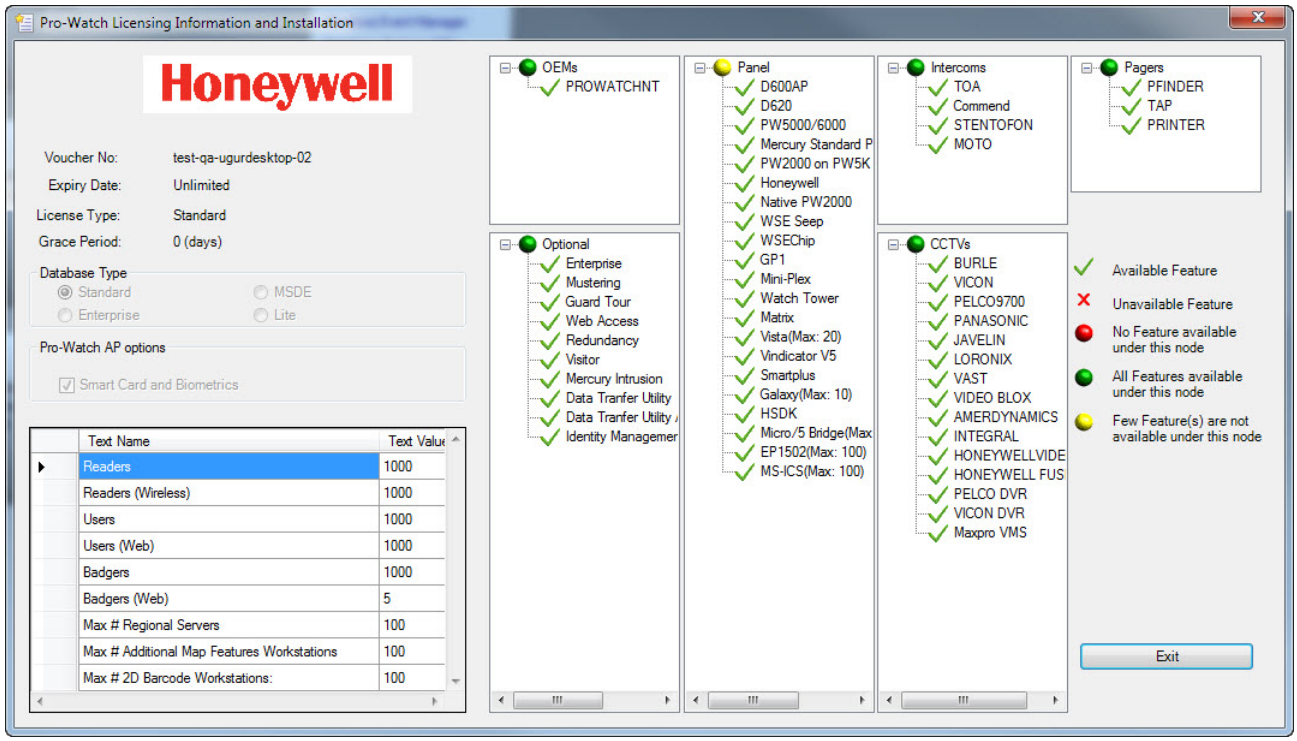
You can access important Pro-Watch Software Keys licensing information through the Pro-Watch Licensing Information and Installation screen.

1. Launch Pro-Watch.
2. On the home page, click **License Information** in the **Help** group of links:



3. View the license related information in the **Pro-Watch Licensing Information and Installation** screen:

Figure R-1: Licensing Information Screen



This screen displays the following licensing information:

- Voucher Number
- Expiry Date (Day, Month, Year in the dd/mm/yyyy format). Unlimited licenses do not have an expiry date.

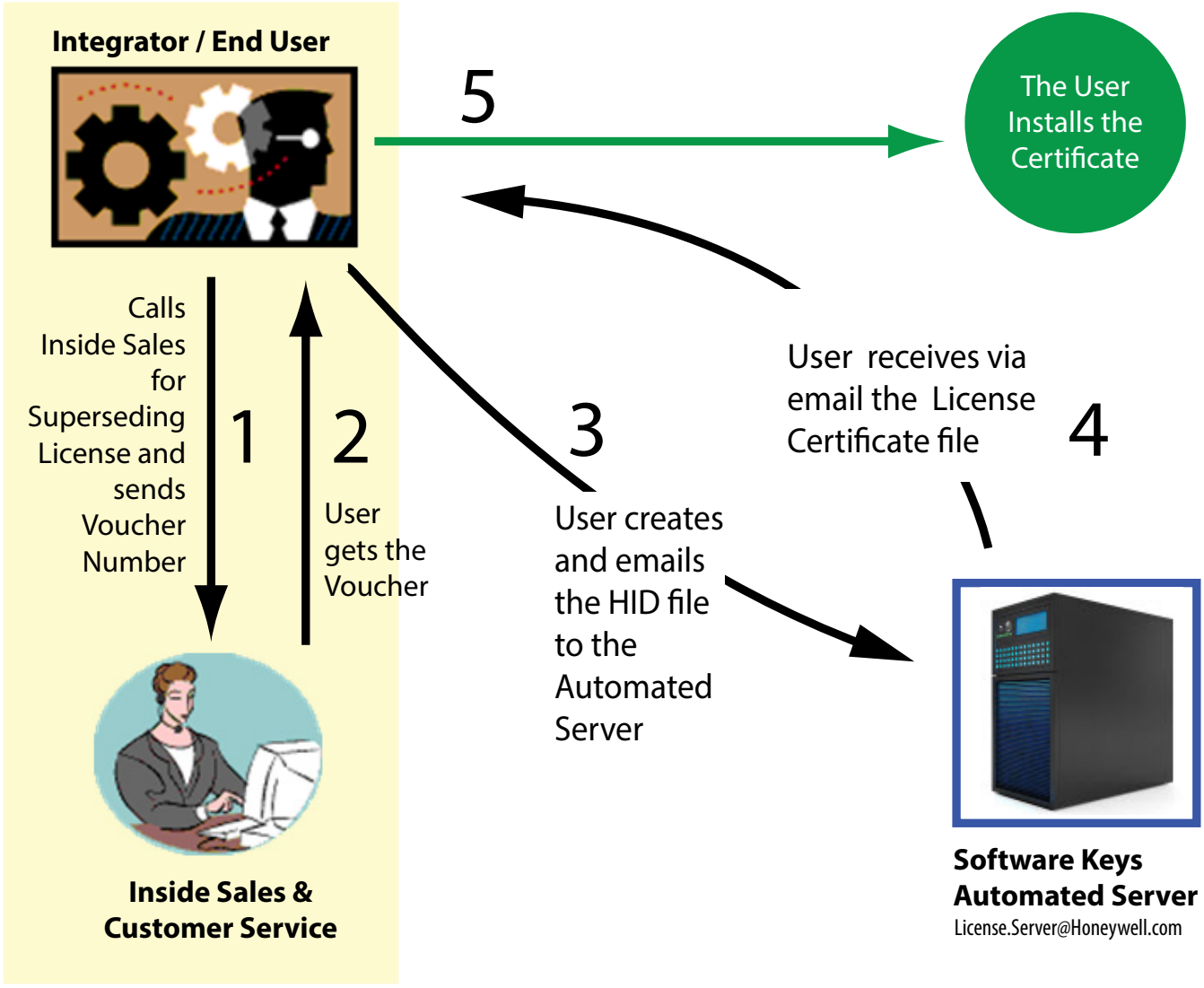
Note: **Grace period** is included in the **Expiry Date**.
(Expiry date = Expiry date + Grace period)

- License Type
- Grace Period (Number of days).

The pane in the middle of Figure R-1 on page 10 displays all the panels with software keys.

If the software keys come with a maximum licensing limit, it will be displayed as a number right after the panel name. For example, “Vista (Max. 20)”.

1.4 How to Supersede a License



1.4.1 STEP 1: The User Contacts Pro-Watch Inside Sales Dept.

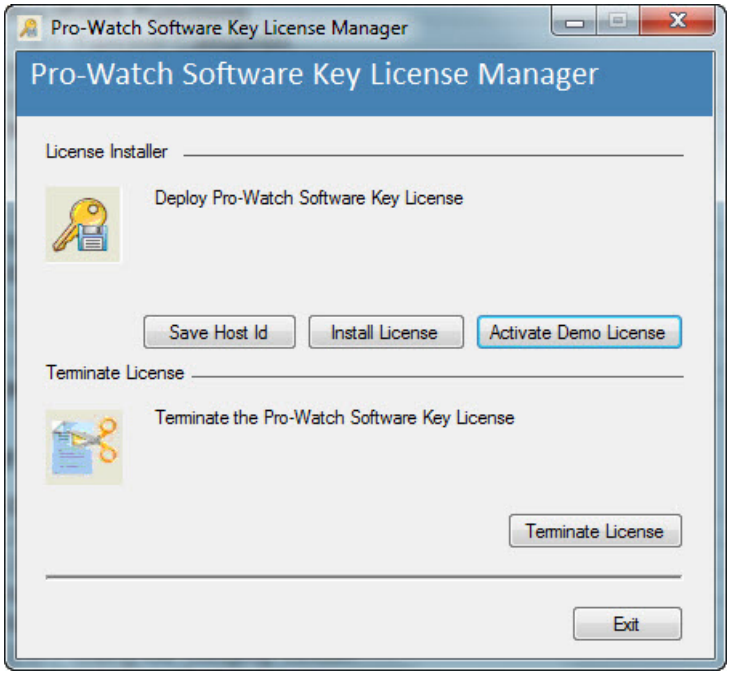
The integrator or the end-user (simply referred to as the "user") starts the process by calling Pro-Watch Inside Sales department and placing an order to supersede the Pro-Watch license and sends the existing Voucher Number.

The Inside Sales gathers the necessary information and starts the Pro-Watch license certificate superseding process.

1.4.2 STEP 2a: The User Generates the *HID file

1. Select **Start > All Programs > Pro-Watch > Pro-Watch Software Keys Manager** from the Windows Start menu. Right-click and select

"**Run as Administrator**" to launch the **Pro-Watch Software Keys Manager**:



Note: Your screen may look slightly different depending on the Windows version you are using.

2. Click **Save Host ID** to automatically generate an *.HID file. This will open your Windows browser screen.
3. Browse and save the automatically generated *.HID file to where you like on your machine.

1.4.3 STEP 2b: The User Contacts SK Automated Server

1. Browse and find the *.HID file on your machine.
2. Attach the *.HID file to an email with the following:
   - Mail subject = VOUCHID: Vouchernumber (e.g., VOUCHID:PW-123420120101-P-1) **Do not use any spaces and be sure to type out the preceding text properly.**
3. Email the ***.HID file** together with the **Voucher Number** to the **Software Keys Automated Server** at **License.Server@honeywell.com** with a request for a new license.

1.4.4 STEP 3: SK Automated Server Mails the User

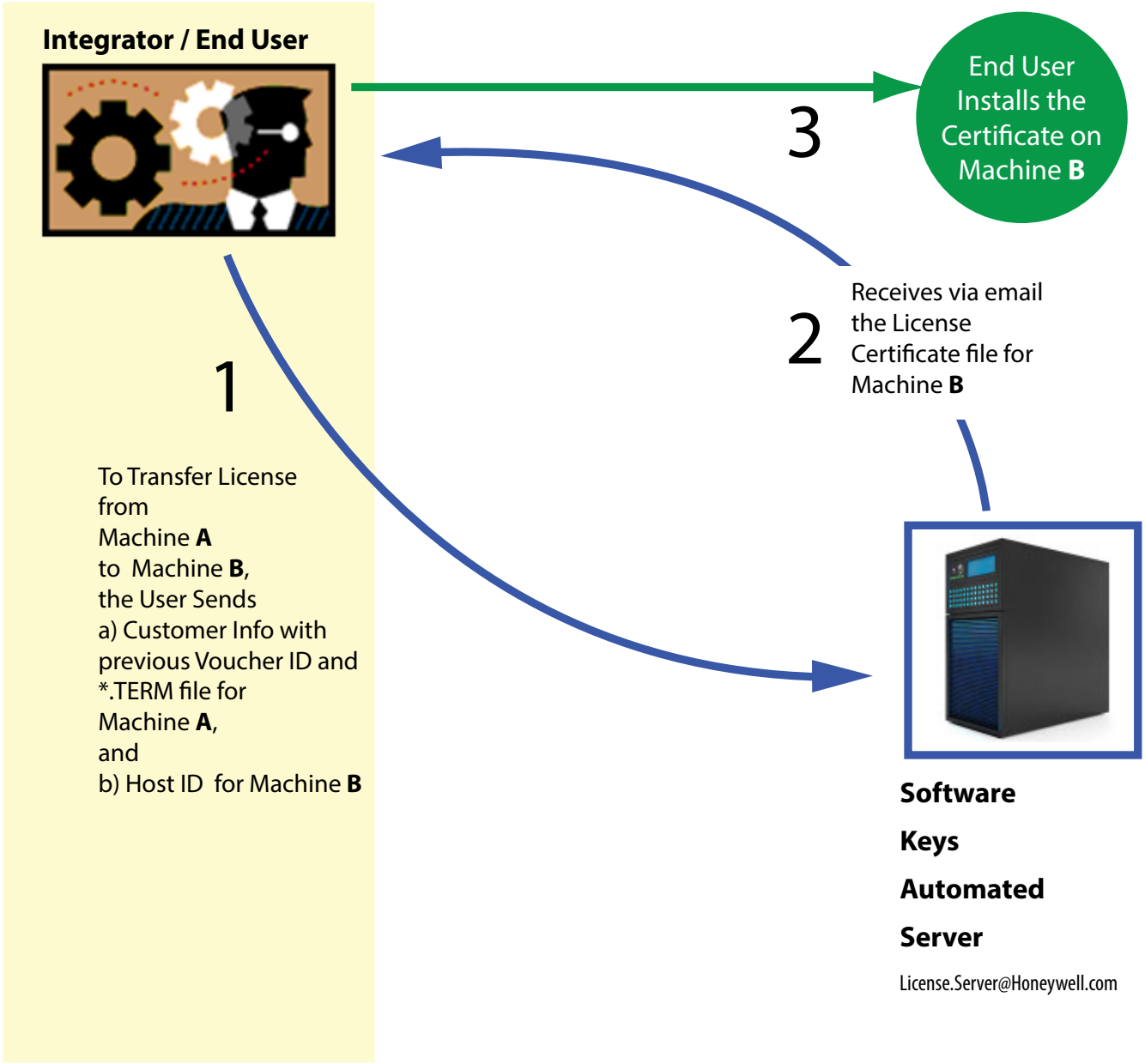
The Software Keys Automated Server generates the superseded license and emails it to the user with a new .CERT file.

1.4.5 STEP 4: The User Installs the License Certificate

Save the .CERT file on your machine.

Follow the instructions at STEP 5: The User Installs the License Certificate, page R-6.

1.5 How to Transfer the License to Another Machine



1.5.1 STEP 1: The User Contacts Software Keys Automated Server and/or the Voucher Manager

The integrator or the end-user (simply referred to as the "user") starts the process by emailing Software Keys Automated Server at license.server@honeywell.com to transfer the Pro-Watch license from Machine A to Machine B.

1. Attach the *.HID file from MACHINE B and the *.TERM file from MACHINE A to an email with the following:

Mail subject = VOUCHID: Vouchernumber (e.g., VOUCHID:PW-123420120101-P-1) Do not use any spaces and be sure to type out the preceding text properly.

2. Email the ***.HID file and *.TERM file** together with the **Voucher Number** to the **Software Keys Automated Server** at **License.Server@honeywell.com** to request a Transfer license.

1.5.2 STEP 2: SK Automated Server Emails the User

The Software Keys Automated Server generates the license certificate file for Machine B and emails it to the user with a new .CERT file.

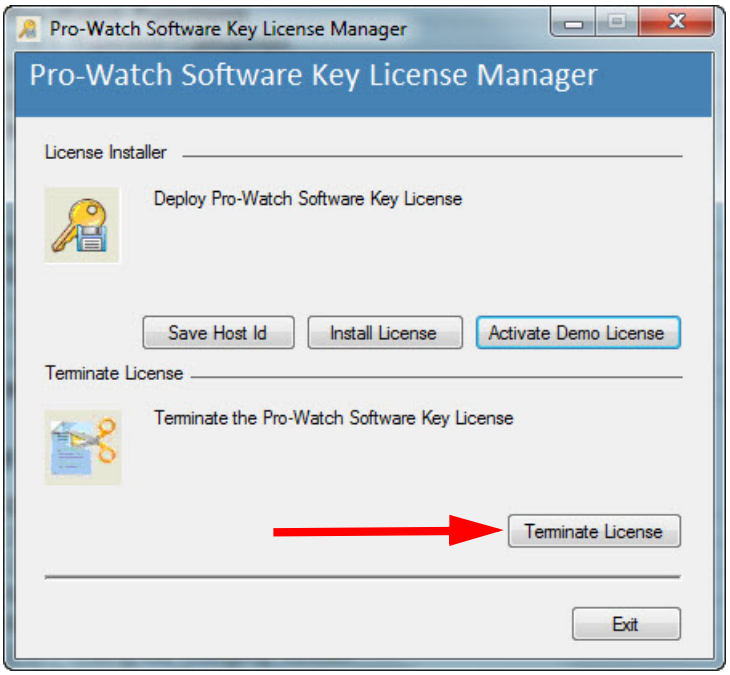
1.5.3 STEP 3: The User Installs the License Certificate

Save the new license on your machine (Machine B).

Follow the instructions at STEP 5: The User Installs the License Certificate, page R-6.

1.6 How to Terminate a License

1. Select **Start > All Programs > Pro-Watch > Pro-Watch Software Keys Manager** from the Windows Start menu. Right-click and select "**Run as Administrator**" to lunch the **Pro-Watch Software Keys Manager**:



2. Click **Terminate License** to terminate the license. This action automatically creates the *.TERM file in the following directory:
   - For 32-bit Machines:
     Local Disk (C:) > Program Files (x86) > Pro-Watch
   - For 64-bit Machines:
     Local Disk (C:) > Program Files > Pro-Watch

1.7 Cut-over/Migration Licenses

1.7.1 Definition

A Cut-over/Migration License is a special situation license that is created by the Honeywell License team to accommodate certain high-availability sites that, for various reasons, would need to migrate their Pro-Watch server over an extended period as opposed to using the normal transfer method. See How to Transfer the License to Another Machine, page R-15.

1.7.2 Examples

What kind of situations demand a cut-over license?

Situations that might require a cut-over license would include sites that must remain up and live due to regulations in their particular industry. Examples would be Banking, Utility industry sites, Government sites and large corporations.

Also any larger or at-risk site that is making a significant upgrade in their Pro-Watch system may want to keep their current system Live, while being able to setup and test their new hardware and any upgrades that accompany that new server.

1.7.3 Why needed?

Why is the cut-over license needed?

For any site, the Pro-Watch License they have legally entitles that site to run one (1) server with that license concurrently.

If a site were to try to copy or clone that server into a migration where they intend to run both the old and the new for any real length of time, they would be violating the Software License Agreement, and thus could put themselves at legal and financial risk.

In addition, the cut-over license allows for the registration and License history of a site to remain intact through the whole process and beyond. This reduces the amount of time needed to accommodate what can be a longer process, saving on-site time while still satisfying all the legal requirements involved.

1.7.4 How Does It Work?

For a site that feels that they need this kind of an option there are some basic guidelines and steps that need to be followed.

1. Contact the sales person for your account and or Honeywell's customer service team so that they can start the process on Honeywell's end. Waiting to do it until you are ready to start and or on-site means you are now at the mercy of just how busy the license team is at that given point in time. Calling a day or two in advance on the request can save you a lot of time.

2. Cut-over licenses are valid for a **maximum of 90 days**. If you are planning to add to the site's license package features or additional items, AND you require them to be on the old server as well as the server you are migrating to, then get those ordered before you start this process. Once the cut-over period starts, the License on the old/current server is considered to be "**Locked**" and no changes can be made to it. All changes would be made to the license that will be active on the new server that is being migrated to.
3. When the cut-over license is ready for activation, a copy of the voucher would be sent to the dealer. The on-site installer or technician would send that voucher number in with a fresh HID file from the new server that is being cut-over/ migrated to. The request should be sent to **VoucherManager@Honeywell.com** One of our Voucher Managers will process the request and send back the cert file for the cut-over license.
4. Dealer/ installer installs that license cert file just like any other Pro-Watch New license install. See How to Install a Regular License, page R-4.
5. **CRITICAL ITEMS:** Once the site is satisfied with their new server setup, and are ready to convert their cut-over license to a permanent one and complete the migration, they will need to supply 2 key things BEFORE the 90 days Cut-over license expires.
    a. **The TERM (termination) file from the old server.** This allows Honeywell to Log that in fact that server is no longer active and thus removes a Red Flag for potential software audit.
    b. **A Current/ freshly generated HID file from the new server** that is running the cut-over license. The Dealer/ Installer DOES NOT terminate the cut-over license. This is simply a freshly generated HID that will be needed for the Voucher Manager to convert that 90 day limited life License into a permanent one. The license server will check the security Data on the HID file to make sure it's the same and is able to supersede it.
6. The Dealer/ Installer sends the Term file and the HID file along with the Cut-over Licenser Voucher Number to **VoucherManager@Honeywell.com** They should include a brief note stating "Ready to Convert cut-over to permanent" or a similar message.
7. The Voucher Manager team will email back with a **New Voucher Number** (PDF) and the **cert file** that when applied will supersede the installed cut-over license and covert it to a Permanent one. Standard Installation process is to be followed. See How to Install a Regular License, page R-4.

Note: For more information about softwarekeys licensing and error codes, see Pro-Watch 5.0 Softwarekeys User Guide, Document 800-08123V17.

Copyright Honeywell | All Rights Reserved

Honeywell

TBS and Pro-Watch Integration

S

In this appendix ...

Overview
Prerequisites
Limitations of Pro-Watch-TBS Integration
Manual Configuring on TBS Side
WebEdition
NETSDK100
TBS EnrollClient
Pro-Watch Configuration
TBS Configuration of Biometrics Settings
Configuring the Badge Field for TBS Enrollment
Configuring TBS Terminal and Validating the Logical Device
Enrolling the Badgeholder Fingerprint

S.1 Overview

This appendix describes the integration between Pro-Watch Access Control and TBS (Touchless Biometric Systems) readers.

Integration with TBS biometric reader allows user to add cutting-edge biometric identification to their security portfolio without having to managing the security badging module.

Utilizing TBS biometric technology, the users are able to enroll and manage biometric templates within Pro-Watch, providing an integrated user experience.

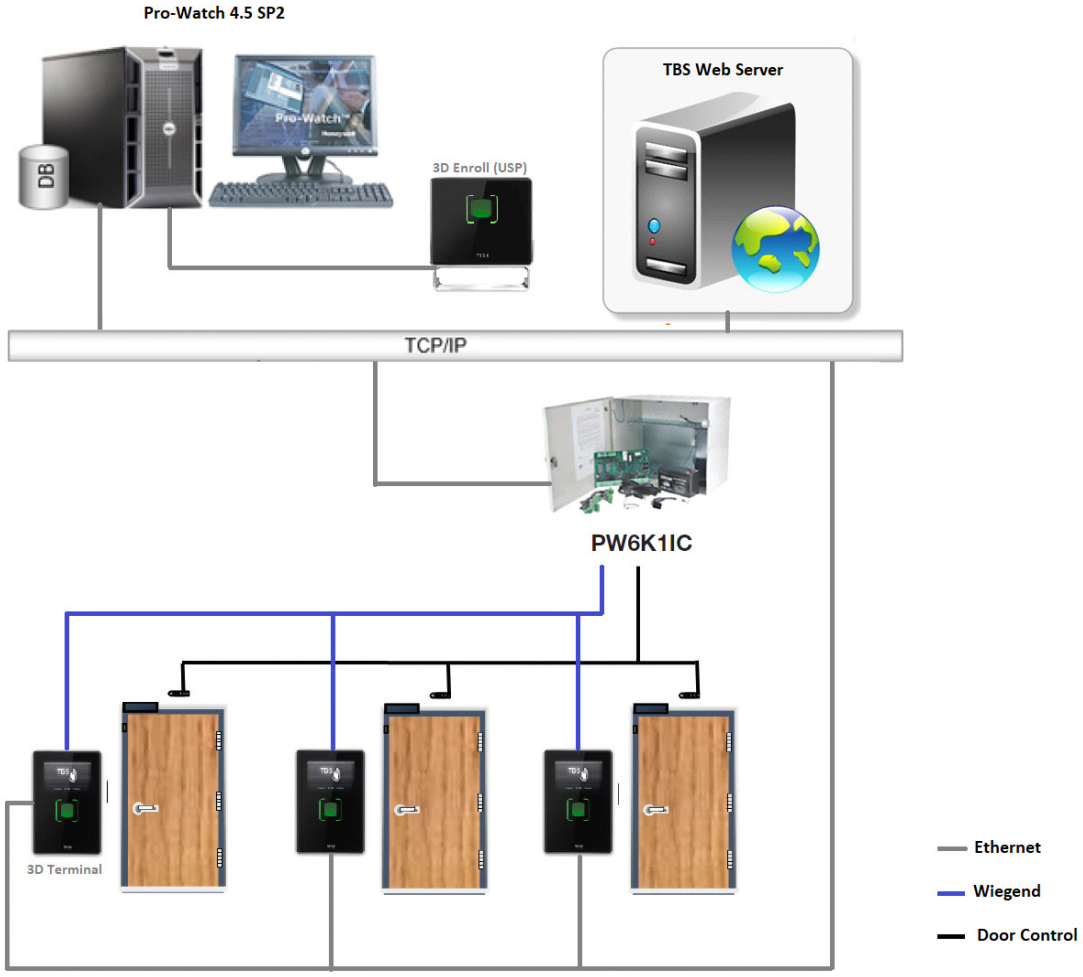
S.1.1 TBS 3D Terminal



S.1.2 TBS 3D Enrollment Device



S.1.3 Typical Network Configuration



S.2 Prerequisites

1. Pro-Watch 4.5 SP2 supports the TBS integration. Pro-Watch 4.5 SP2 or higher should be installed (Refer to Pro-Watch Installation Guide).
2. The installers should familiarize themselves with the TBS System before starting the Pro-Watch -TBS integration
3. The following TBS components will be used for Pro-Watch-TBS Integration:
   - TBS WebEdition (R10.1 or higher)
   - TBS EnrollClient (v4)
   - NETSDK(10.0.1)
4. Please refer to TBS installation guides to install TBS Applications (WebEdition, NETSDK and EnrollClient).

S.3 Limitations of Pro-Watch-TBS Integration

S.3.1 Badge/Card download

There is no Clearance Code validation for Pro-Watch-TBS integration.

Irrespective of Clearance Code or TimeZone validation, all cards will be downloaded to all TBS readers by the below logic.

S.3.1.1 Badge Only

- If a badge does not have TBS biometric enrollment, it will not be downloaded to TBS system.
- The badge which have TBS biometric enrollment will be downloaded to TBS system

S.3.1.2 Badge with a single card

- If a badge does not have TBS biometric enrollment but has a card, it will not be downloaded to TBS system until "**Biometric Card Selected**" option is selected on the card.
- If a badge has TBS biometric enrollment and a card, then it will be downloaded to TBS system whether the "**Biometric Card Selected**" option is selected or not in the card.

S.3.1.3 Badge with more than one card

- If a badge does not have TBS biometric enrollment but has cards, these cards will not be downloaded to TBS system until "**Biometric Card Selected**" option is selected on any one of the cards.
- If a badge has TBS biometric enrollment and multiple cards, first created active card will be downloaded to TBS system until the "**Biometric Card Selected**" option is selected for one of the cards. If the user selects of the cards as “Biometric Card Selected,” then only the particular selected card will be downloaded to all the TBS readers.

S.3.2 Unique PIN

Unique PIN should be enabled on the Pro-Watch Server option, The card which is saved with Duplicate PIN will not be download to the TBS system.

S.3.3 Primary Field Mapping

Advance badge Card number is mapped with flex ID in TBS system. Thus, Flex ID must be mapped as Primary field in TBS terminal configuration (TBS terminal web page).

S.3.4 Pro-Watch Badge Holder Image

Pro-Watch badge holder image will not be updated to TBS system. Thus, badge holder photo will not display in TBS terminal while the user accesses the TBS terminals.

S.3.5 Integration Validation

Pro-Watch-TBS integration is validated with 3D Enroll and 3D Terminals with Smart mode (PIN, Primary ID, Bio).

S.3.6 Authentication and Authorization

	Not Supported	Supported
Authentication	RFID RFID+Bio RFID+PIN PIN + Bio Primary ID (Card Number) + Bio Template on Card	Bio PIN Primary ID (Card Number)
Authorization	Rights Check	Basic (Card and Validity)
Badge Record	Badge Holder Photo	

S.4 Manual Configuring on TBS Side

S.4.1 WebEdition

1. After the TBS WebEdition installation, make the below changes to TBS web configuration file to enable the below TBS API services:
   - RemoteDevice
   - RemoteSync
   - RemoteClient
2. Open the WebConfig from below path in notepad with administrator permission

   TBS_Installedpath\TBS\BioAdmin Web Edition\Core
3. In WebConfig, go to **AppSettings xml** node and add the below line after **cfgVerion** (if authRPKey is available already, update only the value):

```
        <add key="authRPKey"
value="AA5990D3CD7146B7BDF3D47BE5FA056B" />
```

4. Add following line (xml node) under "**serviceActivations**" xml node:

```
        <add relativeAddress="RemoteDevice.svc"
service="TBS.Services.PublicSvc.SvcRemoteBioClient"/>

        <add relativeAddress="RemoteZone.svc"
service="TBS.Services.PublicSvc.SvcRemoteZone"/>
```

5. Add following lines ("service" xml node) under "**services**" xml node:

```
        <!-- Remote Device (public service) -->


        <service
name="TBS.Services.PublicSvc.SvcRemoteBioClient">

        <endpoint address="BasicSecure"
name="epBasicHttpSecure" binding="basicHttpBinding"

        bindingConfiguration="cfgBasicHttpSecure"

        bindingNamespace="http://api.tbsinc.com/Services/Rem
oteDevice/BasicSecure"

        contract="TBS.Services.PublicSvc.ISvcRemoteBioClient
" />

        <endpoint address="Basic" name="epBasicHttp"
binding="basicHttpBinding"

        bindingConfiguration=""

        bindingNamespace="http://api.tbsinc.com/Services/Rem
oteDevice/Basic"

        contract="TBS.Services.PublicSvc.ISvcRemoteBioClient
" />
```

```
        <endpoint address="mex" binding="mexHttpBinding"
bindingConfiguration=""

        contract="IMetadataExchange" />

        </service>


        <!-- Remote Zone (public RemoteSync) -->


        <service name="TBS.Services.PublicSvc.SvcRemoteSync">

        <endpoint address="BasicSecure"
binding="basicHttpBinding"
bindingConfiguration="cfgBasicHttpSecure"

        name="epBasicHttpSecure"
bindingNamespace="http://api.tbsinc.com/Services/RemoteSync/
BasicSecure"

        contract="TBS.Services.PublicSvc.ISvcRemoteSync" />

        <endpoint address="Basic" binding="basicHttpBinding"
bindingConfiguration="cfgBasicHttp"

        name=""
bindingNamespace="http://api.tbsinc.com/Services/RemoteSync/
Basic"

        contract="TBS.Services.PublicSvc.ISvcRemoteSync" />

        </service>


        <!-- Remote Zone (public service) -->


        <service name="TBS.Services.PublicSvc.SvcRemoteZone">

        <endpoint address="Basic" name="epBasicHttp"
binding="basicHttpBinding"

        bindingConfiguration=""

        bindingNamespace="http://api.tbsinc.com/Services/Rem
oteZone/Basic"

        contract="TBS.Services.PublicSvc.ISvcRemoteZone" />

        <endpoint address="mex" binding="mexHttpBinding"
bindingConfiguration=""

        contract="IMetadataExchange" />

        </service>
```

6. Please ensure that **svcBehaviorDefaultMeta** is enabled on Remote Sync (public service), Go to services and search for Remote sync service (by default it should be enabled in WebEdition R10.1).

svcBehaviorDefaultMeta is enabled	svcBehaviorDefaultMeta is not enabled
<service name="TBS.Services.PublicSvc.SvcRemoteSync" behaviorConfiguration="svcBehaviorDefaultMetaON">	<service name="TBS.Services.PublicSvc.SvcRemoteSync" >

7. In this WebConfig Search for **<serviceMetadata httpGetEnabled="** and set <serviceMetadata httpGetEnabled="true" as below,

```
<behaviors>
  <serviceBehaviors>
    <behavior>
      <dataContractSerializer
maxItemsInObjectGraph="2147483647" />
    <!-- To avoid disclosing metadata information,
set the value below to false and remove the metadata endpoint
above before deployment -->
      <serviceMetadata httpGetEnabled="true"
httpsGetEnabled="false" />
    <!-- To receive exception details in faults
for debugging purposes, set the value below to true.
      Set to false before deployment to avoid
disclosing exception information -->
      <serviceDebug
includeExceptionDetailInFaults="false" />
    </behavior>
    <behavior name="svcBehaviorDefaultMetaON">
      <dataContractSerializer
maxItemsInObjectGraph="2147483647" />
      <serviceMetadata httpGetEnabled="true"
httpsGetEnabled="false" />
      <serviceDebug
includeExceptionDetailInFaults="false" />
    </behavior>
  </serviceBehaviors>
</behaviors>
```

S.4.2 NETSDK100

After the NETSDK100 installation, please verify that “TBS biometric client” Windows service is getting installed. If this Windows service is not available, then below configurations need to be done to install the "TBS biometric client service”.

1. App poll which are running with "BAWebClient' application need to be stopped. Usually these are the below-listed app poll items:

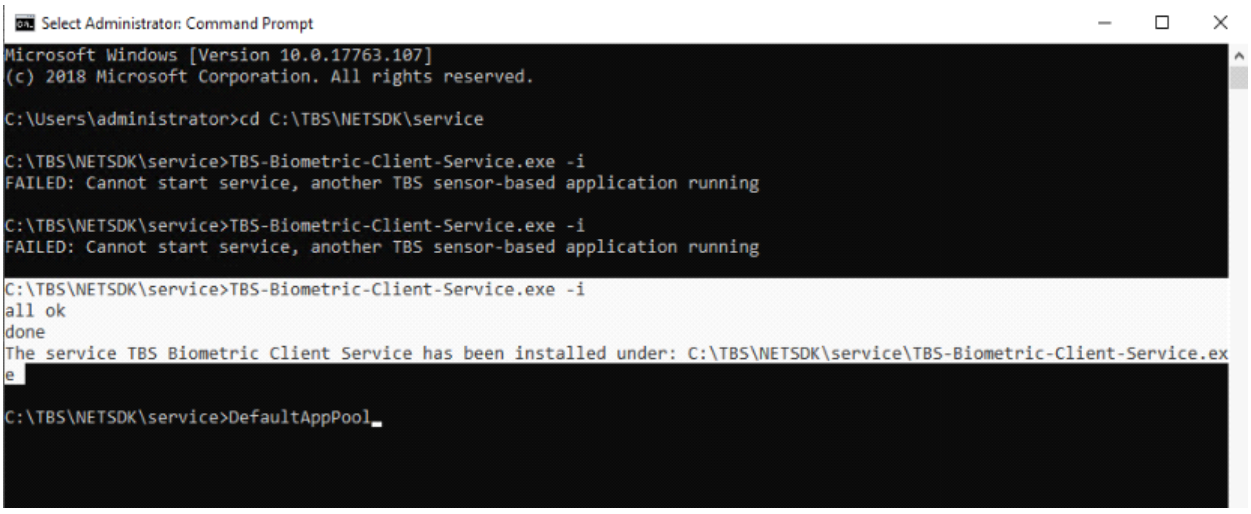
   TBS BAIPCamService AppPool

   .NET v4.5

   DefaultAppPool

2. Run the below command in CMD to install the "TBS biometric client service"

   C:\>TBS\NETSDK\service\TBS-Biometric-Client-Service.exe -i



3. TBS biometric client service will be installed in windows service.
4. Change the Service account type to administrator (Domain or Workgroup based BA installation).
5. Start the TBS biometric client service.
6. Start the app pools which you stopped during step 1.
7. Once done above, ensure that TBS biometric client service is running as windows service.
8. Then the www folder needs to be copied from NETSDK-installed path (Source) to Advance badging folder (Destination):

   SOURCE: ...\TBS\NETSDK\sdk\bin

   DESTINATION: ...\Program Files(x86)\ProWatch\AdvancedBadging

S.4.3 TBS EnrollClient

After installing the “TBS EnrollClient” do the following:

1. Open EnrollClient and see the system status, Server should be connected as below.
2. EnrollClient has to be validated to get it enabled the Client status.
3. Launch BioManger from IIS (Site name: BAWebClient) to validate the EnrollClient.
4. Default login credentials of BioManger is below:

   ```
   Username: Sysadmin

   Password: 12345678
   ```

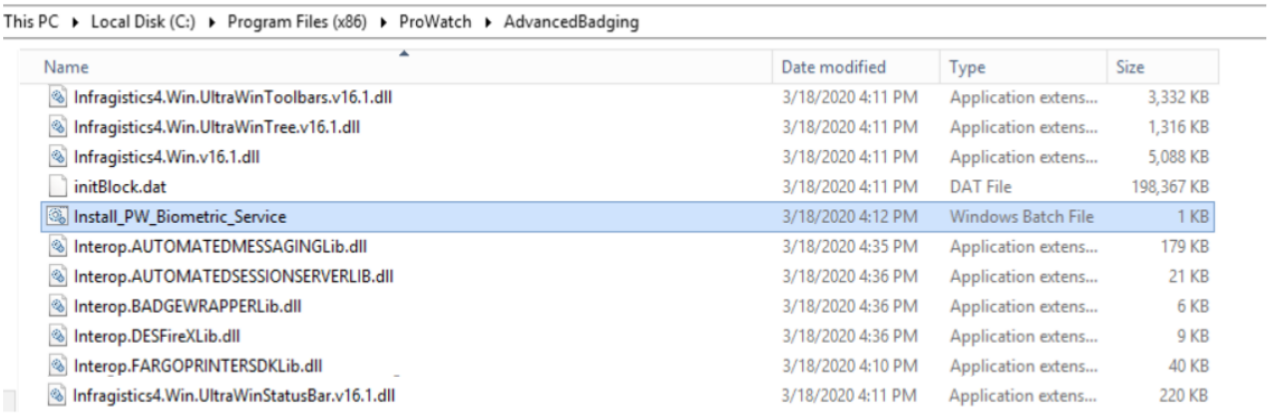
5. Open the BioManger. Go to Clients menu , EnrollClient should be listed in this list , Validate this client using "Validate client option".
6. Now Client status should be green for "Valid", "Active", "Enroll"and "Sync" in EnrollClient system status.
7. Now connect the USP entrollment device via USP port and ensure the that Senor status is connected in " in EnrollClient system status.

S.5 Pro-Watch Configuration

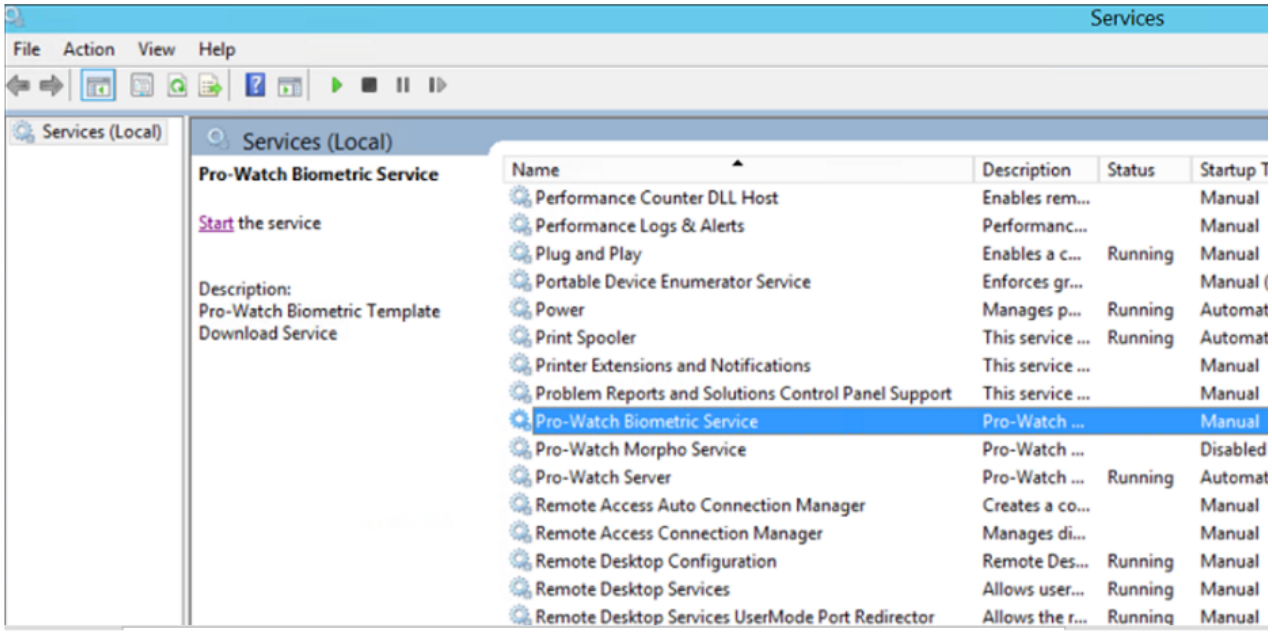
S.5.0.1 Installing Pro-Watch Biometric Service

Pro-Watch Biometric Service must be installed on the server.

1. To Install the Pro-Watch biometric service go to Pro-Watch installed path and open advance folder and find "**Install_PW_Biometric_Service**" bat file:



2. Right-click the bat file and run it as an Administrator. After the installation, it should look like this:



S.5.1 TBS Configuration of Biometrics Settings

1. Start **Advanced Badge Manager.**

   a. Select the **Biometrics Settings** icon and select the T**BS Configuration** tab.

   b. Enter the TBS web service address for the following 3 services:

   - **Service communicated via http**

     `http://localhost/BACore/RemoteDevice.svc/Basic`

     `http://localhost/BACore/RemoteSync.svc/Basic`

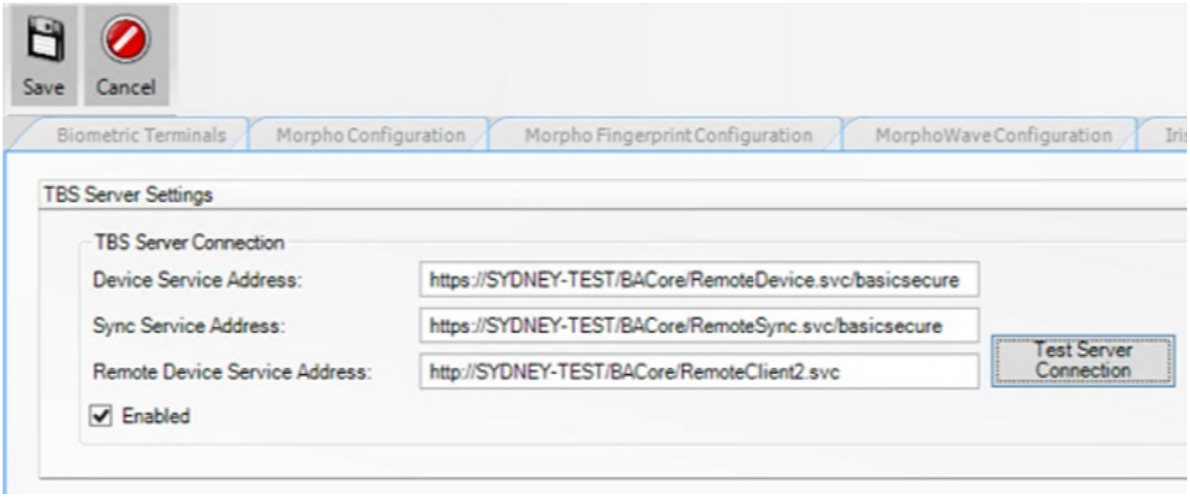
     `http://localhost/BACore/RemoteClient2.svc`

   - **Service communicated via https**

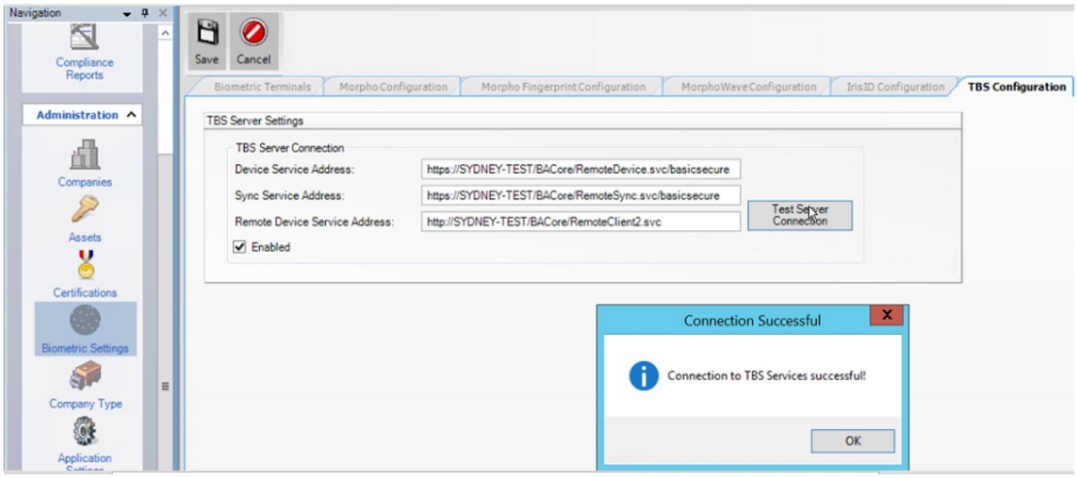
     `https://localhost/BACore/RemoteDevice.svc/BasicSecure`

     `https://localhost/BACore/RemoteSync.svc/BasicSecure`

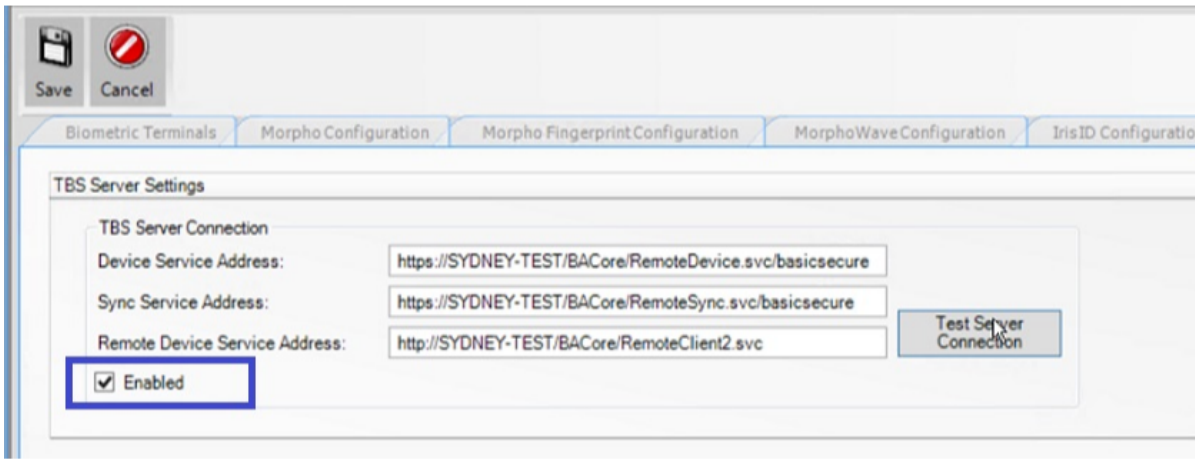
     `https://localhost/BACore/RemoteClient2.svc`



2. Click the **Test Server Connection** button. If it is okay, select **OK**:

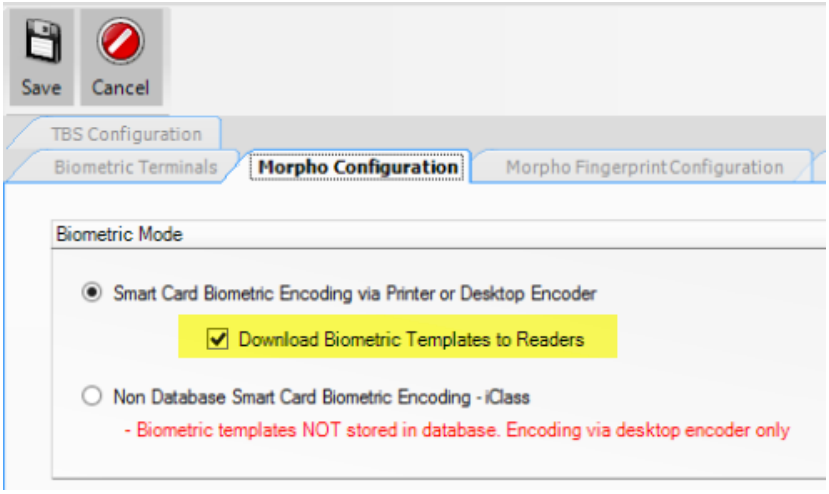


3. The **Enabled checkbox** will be selected:



a. Click **Save**.

4. Then go to biometric settings and, on the **Morpho Configuration tab**, select **Edit** and then select the **Download Biometric Templates to Readers** check-box:



5. Click **Save**.

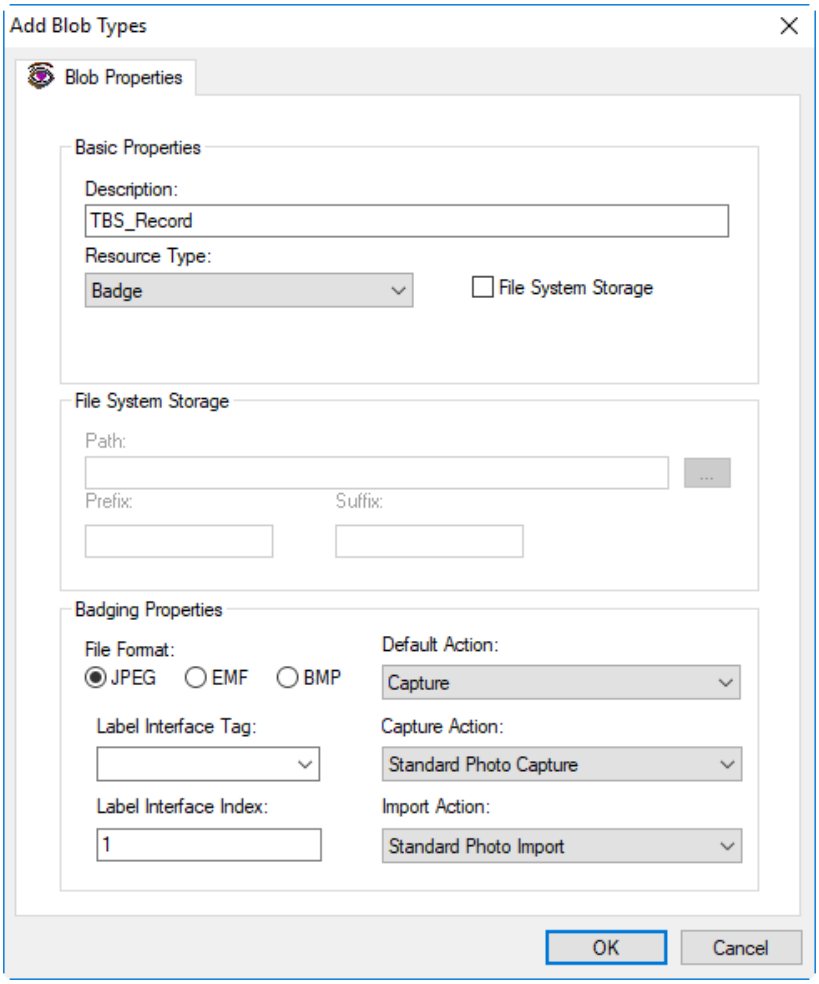
S.5.2 Configuring the Badge Field for TBS Enrollment

S.5.2.1 Creating the TBS BLOB

Create a BLOB by following these steps:

1. In Pro-Watch, go to **Database Configuration > BLOB Types**.
2. Right-click to display the pop-up menu. Select "**New BLOB Types...**" to display the "**Add BLOB Types**" screen.

3. Enter a meaningful **Description** like "TBS_Record." Select "**Badge**" for **Resource Type**. Do NOT select "File System Storage" check-box to make sure the BLOB will be saved in the database.

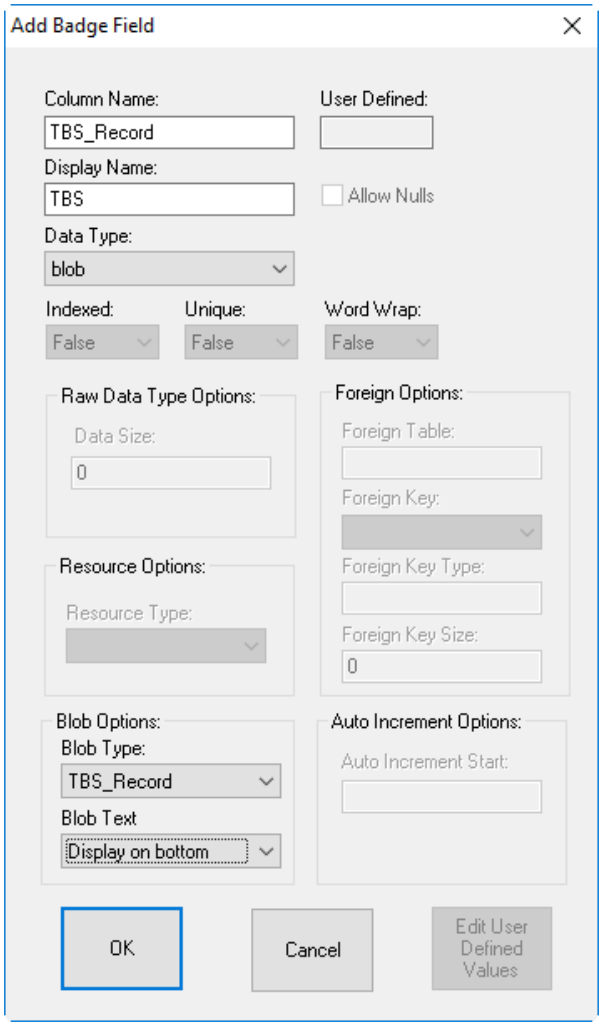


4. Click **OK**.

S.5.2.2 Adding the TBS BLOB Field to Badge Fields

1. In Pro-Watch, go to **Administration > Badge Utilities**. Expand the tree-view and double click the **Badge Fields.**
2. Right-click on the badge field table and from the pop-up menu, select "**Add Badge Field**" to display the Add Badge Field screen.

3. Enter **Column Name** as "TBS_Record." Enter a meaningful Display name like "TBS." Select "BLOB" for **Data Type**. Select "TBS_Record" for **BLOB Type** and "Display at Bottom" for **BLOB Text**:



4. Click **OK** when done.

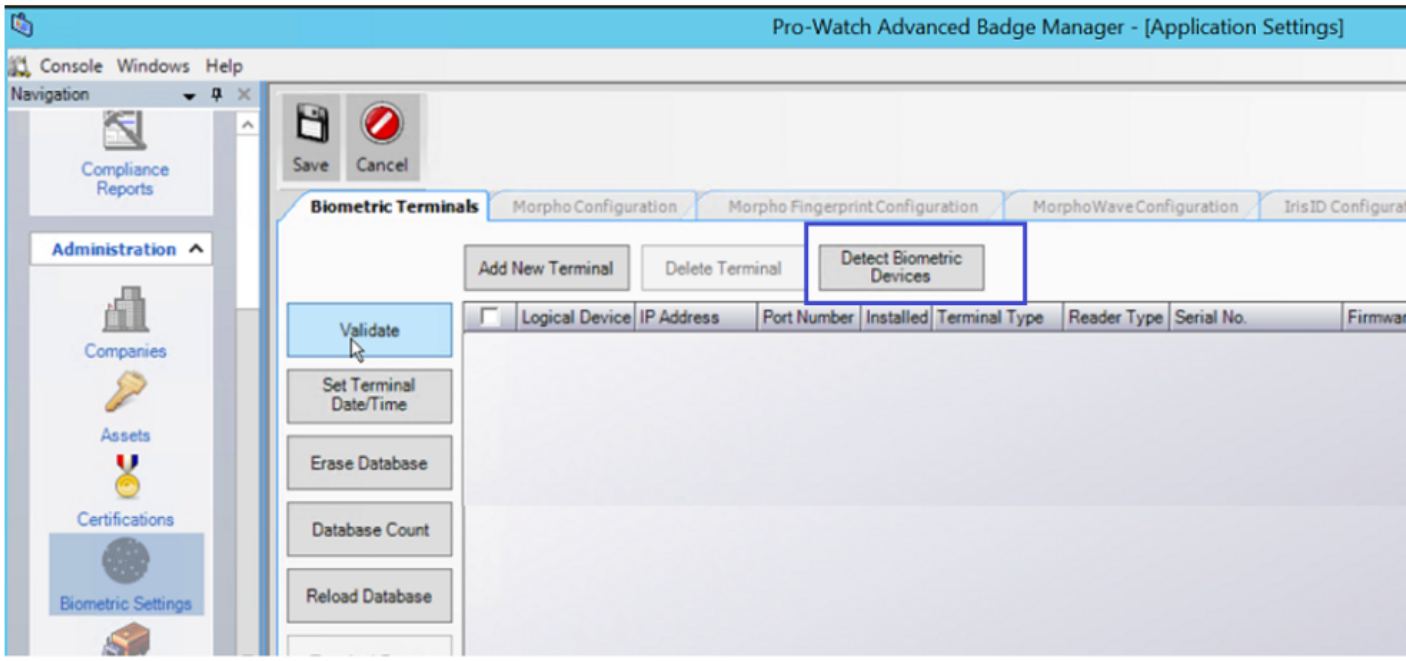
S.5.2.3 Adding the TBS BLOB Field to Badge Record Template

1. Go to **Administration > Executables > Badge Builder**.
2. Drag and drop the "TBS_Record" field to the badge template.

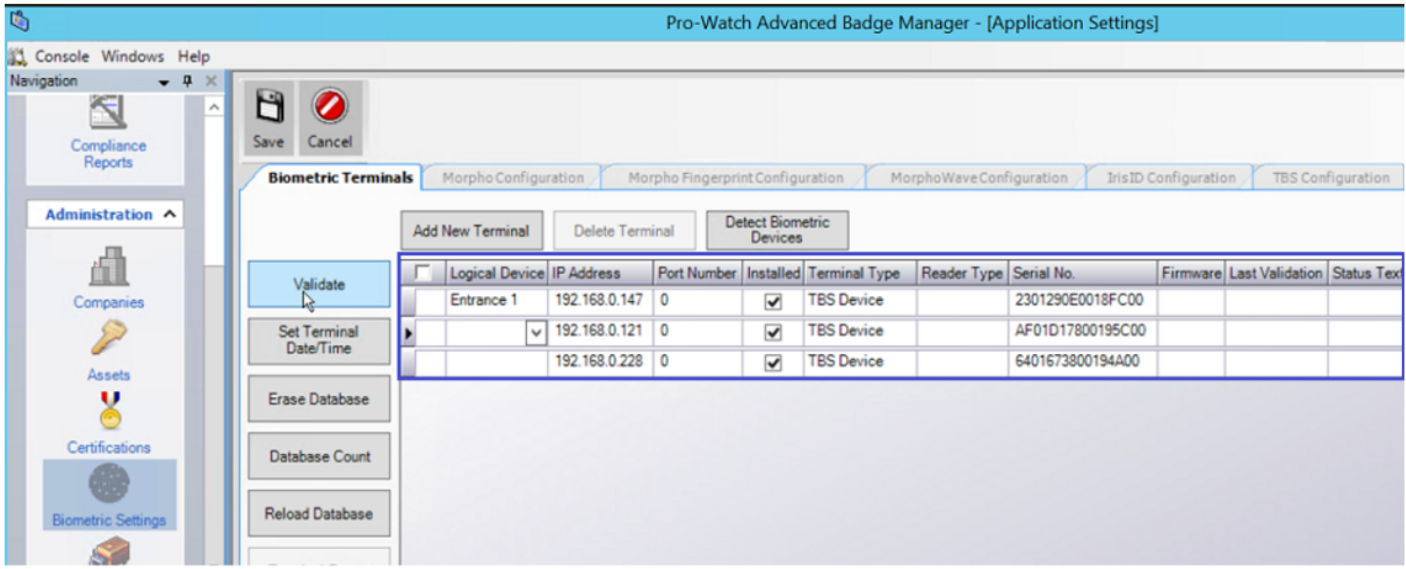
S.5.3 Configuring TBS Terminal and Validating the Logical Device

1. Launch the **Advanced Badging** module.
2. Select **Biometric Settings > Edit > Bio Terminals tab**.

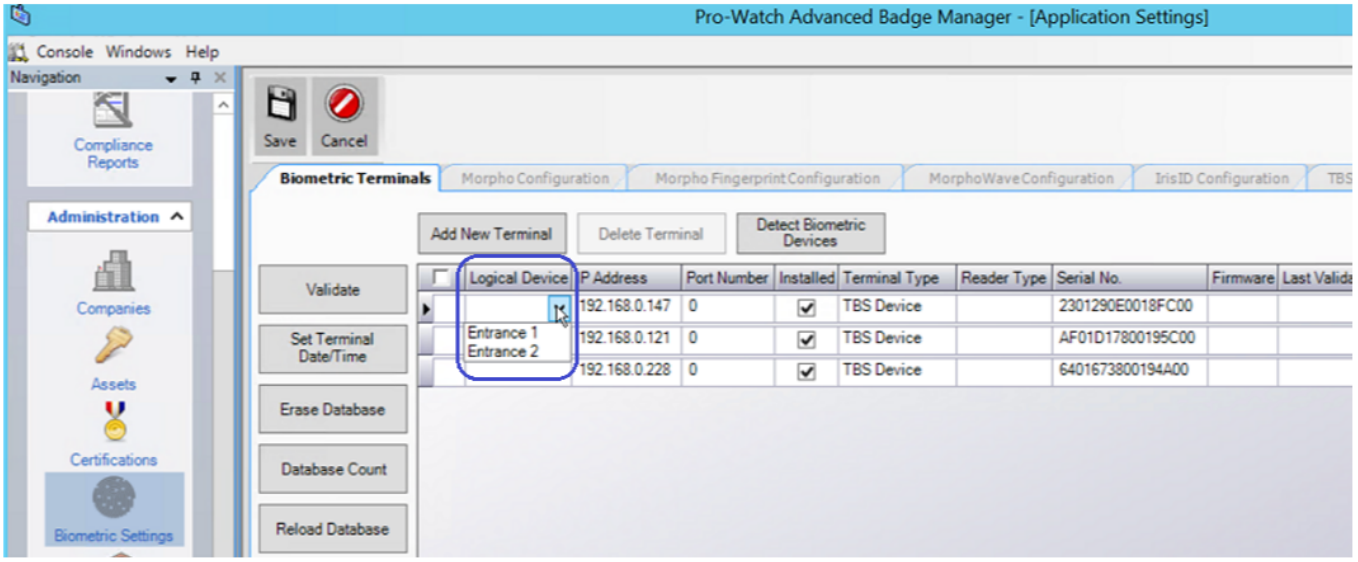
3. Click the "**Detect TBS Devices**" button to retrieve the unassigned TBS readers from the TBS database:



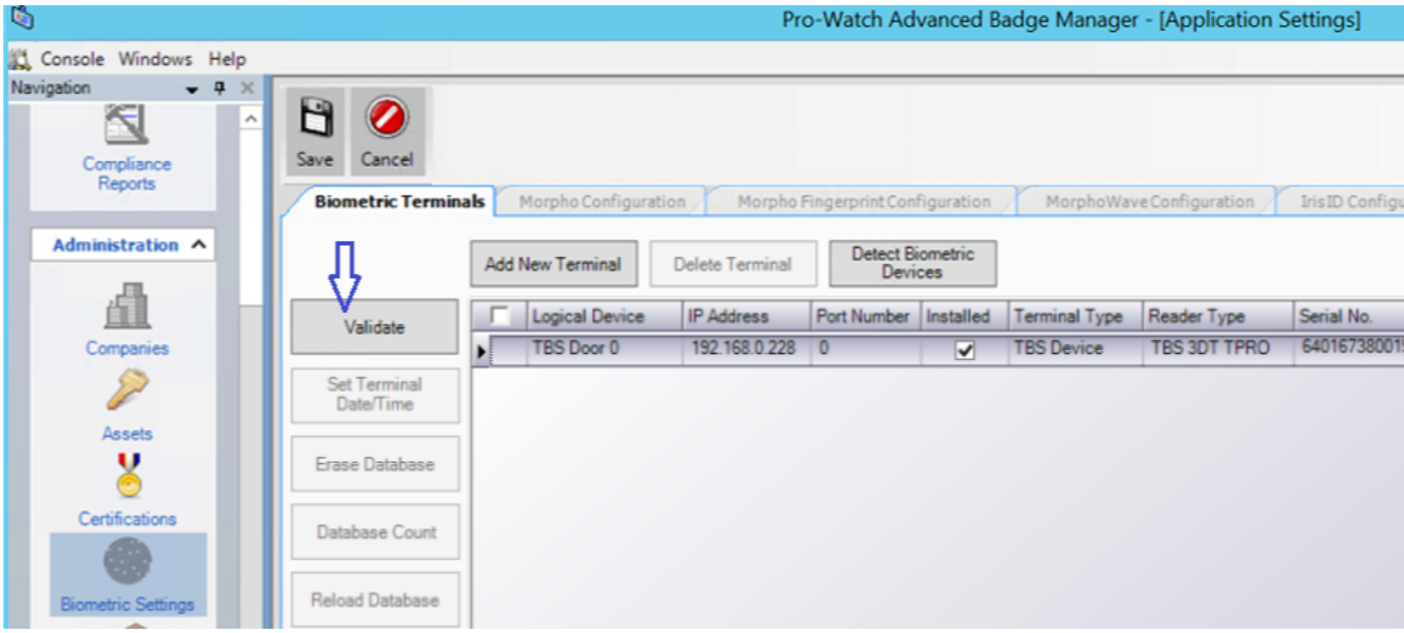
4. After clicking the "Detect Biometric Devices," the Unassigned TBS terminals will be listed as below:



5. Assign a **Logical Device** from the drop-down menu and click **Save**:



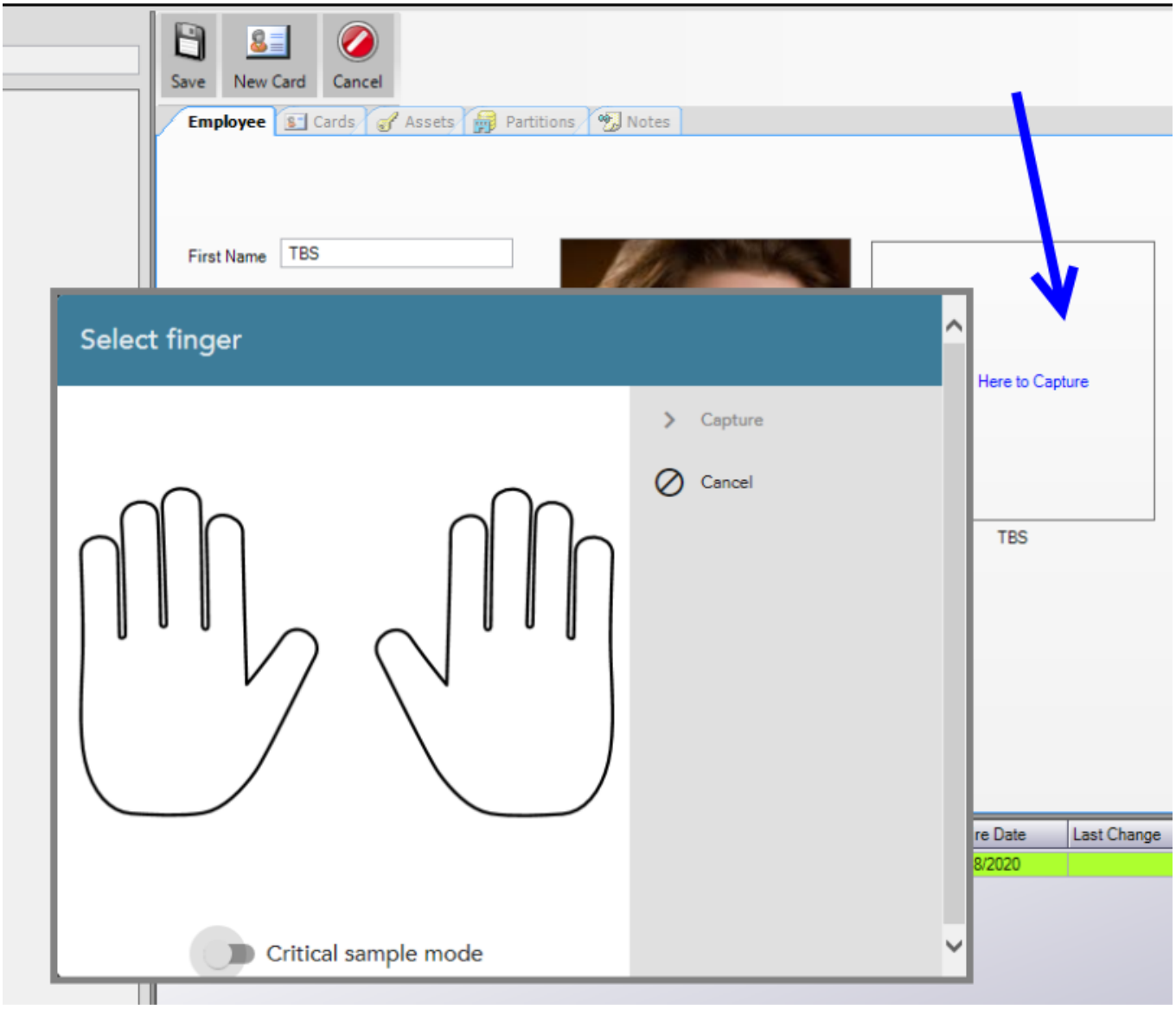
6. Select a **Logical Device** from the drop-down list and click the **Validate** button (the only control enabled) to fill in the fields:



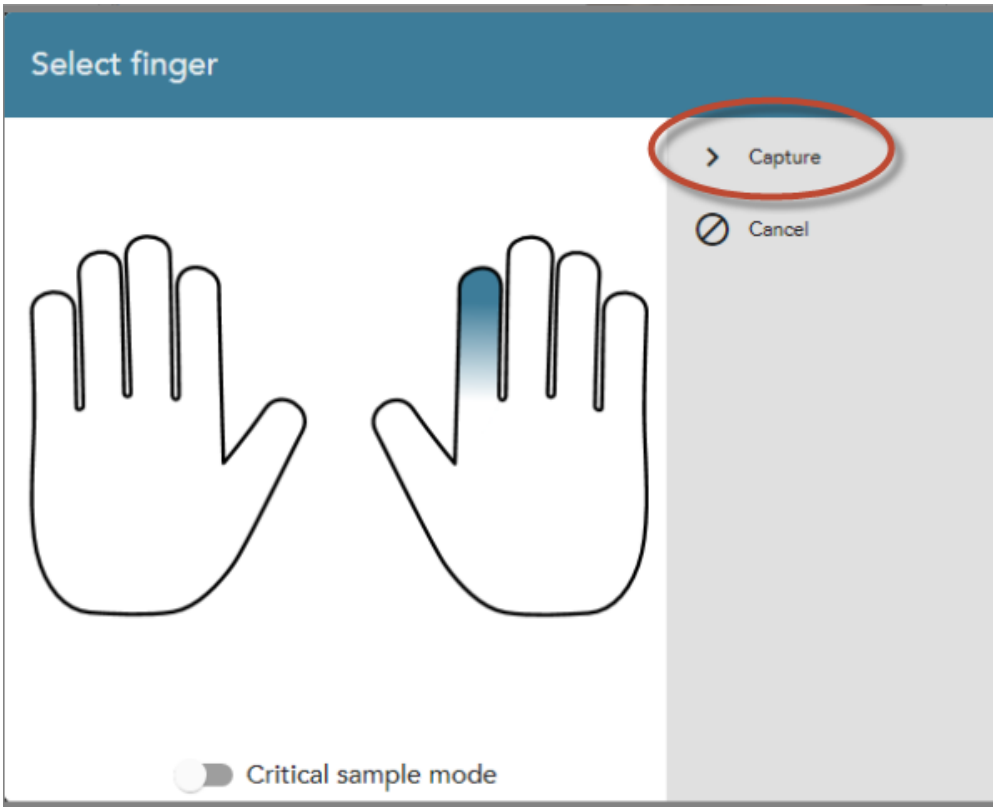
7. Go to **Database Configuration > Clearance Codes** to create TBS clearance code which is assigned to the logical device you've selected.
8. Assign a **Company** to TBS with the respective clearance codes.
9. In the **Advanced Badging** module, go to the **General Fields** and create a new **Badge Holder**. Add a **Card** for the appropriate TBS company.

S.6 Enrolling the Badgeholder Fingerprint

1. Go to the **Advanced Badging** module and create a new badge header with card.
2. In the **Badge record**, click the **TBS "Click Here to Capture" place-holder square** and start the finger enrollment utility:

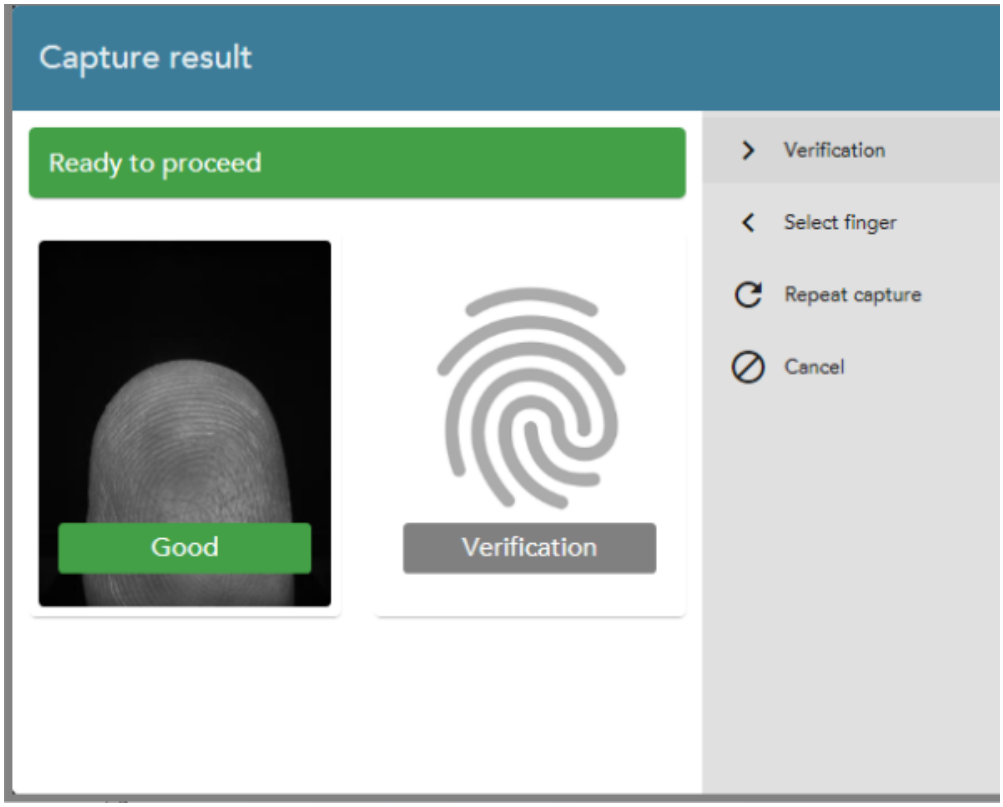


3. Click and **select a finger**:

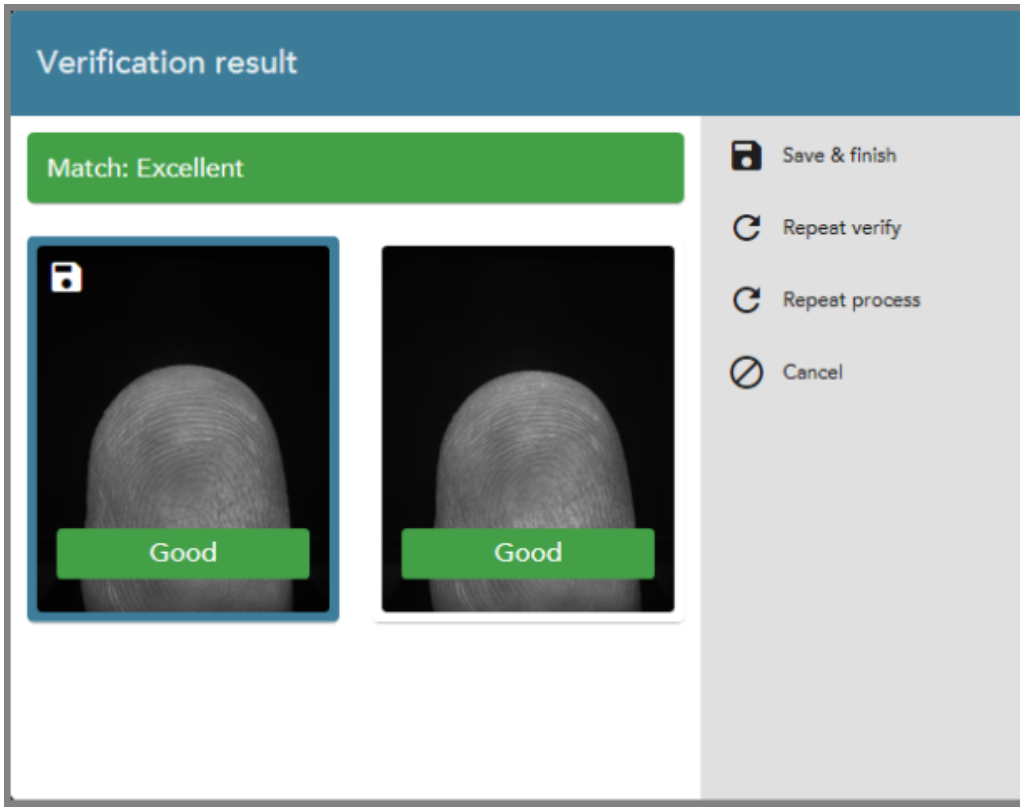


4. Click **Capture**.

5. Insert the selected finger into the 3D reader hole and follow the instructions on the enrollment device. If the fingerprint quality is good, TBS will display a "Good" feedback:

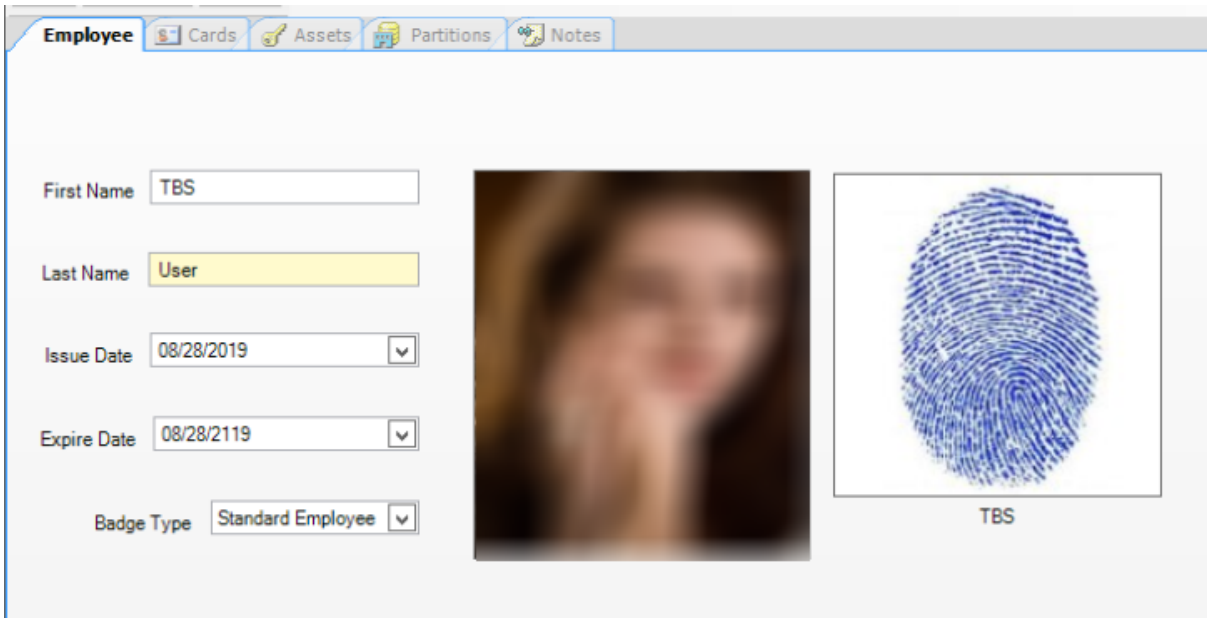


6. Select **Verification** and then insert the same finger for a second time for verification. When the fingerprint is verified, the TBS will display a green "**Good**" label under both fingerprints. That means the two fingerprints match:



7. At this point you can also choose from one of the following options:
   a. Repeat Verify
   b. Repeat Process
   c. Cancel

8. Click **Save and Finish**. The fingerprint that is saved in the TBS database is represented in the badge record with a fingerprint icon:



9. Click **Save**. Now, the Badge has been saved with user biometric data and card. It will be downloaded to all TBS terminals irrespective of clearance code.

S.6.1 Door Strike Activated for Unauthorized Users when TBS Reader is Configured with Multi-factor Authentication

S.6.1.1 Scenario 1: TBS reader configured with PIN+Bio

Enter valid PIN on reader then show invalid bio, TBS reader display shows "Verification failed" but it send the wiegened output for Valid PIN. Hence the panel Provides Access and the door opens.

S.6.1.2 Scenario 2: TBS reader configured with CardNumber+ Bio

Enter valid Card number on reader then show invalid bio, TBS reader display shows "Verification failed" but it send the wiegened output for valid card number. Hence the panel Provides Access and the door has opens.

S.6.1.3 Cause of the Issue

TBS Reader sends the wiegened output for verification failed scenarios. Hence access is granted by the P-Series panel.

Copyright © Honeywell Inc. All Rights Reserved.

Honeywell

INDEX

Numerics

128-bit encryption 8-11
256-bit encryption 8-11

A

access levels
    See Clearance Codes
access management 30-7, 37-10
access report H-19
accounts
    login 1-8
Active Directory 64-61
adding
    alarms 3-8
    badge field 60-17
    badge profile 60-5
    badges G-4
        in bulk G-13
    cards G-37
    channel
        Cardkey 9-3
        CHIP 10-3
        Matrix 11-3
        PW-2000 7-3
        PW-5000 8-4
        PW-6000 8-4
        PW-6K1ICE 8-4
        SEEP 13-3
        SmartPlus Mobile 14-3
        Vindicator V5 15-3
        VISTA 16-3
    Intercom 23-3
    logical device
        Matrix 11-16
        PW-2000 7-29
        PW-6000/5000/3000 8-42, 8-133
    time zone G-61

administration
overview 1-11, 5-6
administrator functions 5-1
advanced badging
navigating 2-2
alarm monitor
associating a camera with 22-26
card voiding 3-28
disposition 3-3
adding, editing 3-4
deleting 3-6
file menu 3-25
CCTV controls 3-25
comm status 3-25
intercom controls 3-27
reconnect 3-28
status groups 3-28
void card 3-28
historical trace 3-15
instruction 3-7
adding, editing 3-8
deleting 3-9
invoking actions
devices associated with alarms 3-22
devices not associated with alarms 3-23
live trace 3-15
logical devices, acting on 3-22
monitoring alarms 3-14
play video 22-21
processing events
layers map function 3-30
map view 3-29
response code 3-9
adding, editing 3-10
deleting 3-10
toolbar 3-12
using 3-14
window pane 3-11
alarms
adding, editing 3-8
associating a camera with 22-26
deleting 3-9
dispositions 3-3
instructions 3-7
anti-passback
hard 29-8
load balancing 5-12
soft 29-8
timed 29-9
by card holder 29-10
by reader 29-10
Anti-Pass-Back update limitations 29-19
APB
See anti-passback
APB Update Limitations 29-19
appendix
(A) secure mode verification A-1
(B) assignable programs B-1
(C) dial-up configuration C-1
(D) remote terminal services D-1
(E) Magicard Prima printer installation E-1
(F) moving panels F-1
(G) badging G-1
(H) reports H-1
(I) Morpho biometric integration I-1
(J) Mercury M5 Bridge J-1
(K) two-person rule K-1
(L) PW5K conversion utility L-1
(M) partition manager M-1
(N) registry management N-1
(O) Galaxy Dimension O-1
(P) extended card number support P-1
(Q) IRIS ID integration Q-1
(R) Software Key Licensing R-1
(S) TBS-PW Integration S-1
(S) TBS-PW integration S-1
application login 1-3
archiving
adding, editing 65-5
deleting 65-10
Query Analyzer 65-9
area 29-1
adding 29-4
APB update limitations 29-19
editing 29-4
functions 29-3
mustering 5-32
passback 29-7
triggers 29-8
two-person rule 29-6
areas
mustering 1-16, 1-17
ASSA ABLOY
system configuration 19-15
assignable programs B-1
audit log in 64-56
autoCAD map 3-30
Azure 1-37

B

badge builder
See also badge designer and badge utilities
badge field
adding, editing 60-10
deleting 60-11
badge layout
aligning fields 60-13
centering a field 60-14
layout options 60-13
sizing a field 60-13
spacing fields 60-13
status bar 60-14
testing layout 60-16
badge profile 60-13
adding 60-5
adding profile pages 60-7
assigning to class or user 60-15
editing 60-12
badge designer
See also badge builder and badge utilities
badge barcode
barcode G-89
barcode data G-88
colors G-90
conditional display value G-92
placement G-88
positioning G-92
badge bitmap
bitmap G-83
color G-84
conditional display value G-85
placing G-82
positioning G-84
badge image
badge G-75
colors G-75
positioning G-75
track G-76
badge items
layering G-102
badge photo
color G-86
compression 5-32
conditional display value G-87
intensity 5-32
photo G-86
placing G-85
positioning G-87
badge shape
color G-97
conditional display value G-98
placing G-96
positioning G-97
shape G-96
badge signature
colors G-99
conditional display value G-101
placing G-98
positioning G-101
signature G-99
badge text G-80
colors G-81
conditional display value G-82
positioning G-81
text block G-81
blockout
adding, editing G-73
deleting G-74
exiting G-102
format, properties G-70
grid and snap properties G-72
image and magnetic stripe properties G-74
snap and grid properties G-72
tool bar G-79
using inches or millimeters G-71
zoom factor G-72
badge field
adding 60-17
deleting 60-20
editing 60-20
viewing 60-20
badge holder report H-21
badge photo intensity 5-32
badge profile
badge builder 60-13
configuration report H-23
info tab 30-6
badge shape
conditional display G-98
placement G-96
positioning G-97
tab G-96
badge type
configuration report H-23
badge utilities 60-17
See also badge builder and badge designer

badges
adding
in bulk G-13
adding, editing G-4
brass key G-9
deleting G-31
editing
in bulk G-15
employee G-6
image
exporting G-31
setting compression and intensity 5-32
summary G-10
layout
designing G-11
multiple new G-13
partitions G-11
personal G-9
photo
importing G-28
taking G-17
printing G-16
saving G-11
searching
advanced G-32
quick G-32
searching for G-32
signature
capture device G-31
capturing G-29
importing G-30
task steps G-3
badging G-1
overview
Part I 1-9
advanced
adding a badge 2-35
adding a card 2-40
administration 2-88
assigning assets 2-77
assigning notes 2-84
assigning partitions 2-83
copying a card 2-60
deleting a card 2-64
downloading a card 2-61
editing a badge 2-36
editing a card 2-62
navigation pane 2-30
preview badge record 2-86
printing badge record 2-87
screen 2-32
toolbar 2-8
using e-docs 2-78
classic G-1
overview
Part II 5-4
balanced magnetic switch 6-31
barcode
color G-90
conditional display G-92
data G-88
how to example G-93
placement G-88
positioning G-92
tab G-89
biometrics I-1
adding biometric field to PW AB I-33
configuration I-12
enabling I-8
enrollment troubleshooting I-19
Morpho 2-50
override 2-50
PIN 2-50
TBS S-1
use mode I-10
bitmap
badge G-83
color G-84
conditional display G-85
placement G-82
placing G-82
positioning G-84
BLOB
adding or editing 33-4
deleting 33-10
partitions 33-9
size limit 33-2
supported formats 33-2
type functions 33-3
types 33-1
blockout G-73
BMS
See balanced magnetic switch
brass key G-9
configuration report H-23
bulk
adding in
badges G-13
editing in
badges G-15
buttons
CCTV controls 1-18

delete 1-12
details 1-21
digital video recording 1-20
find 1-12
intercom controls 1-19
large icons 1-21
list 1-21
logoff shadow user 1-14
mustering 1-16
new 1-12
properties 1-12
shadow user 1-13
small icons 1-21
toggle event 1-14
verification 1-15
view event log 1-14
viewer bar 1-14

C

capturing
photo G-17
signature G-29, G-31
card
activating G-42
adding, editing G-37
auto incrementing card number G-38
card information G-38
clearance codes G-51
deleting G-68
deleting from area 1-17
download verification 5-36
downloading 5-32, G-65
expiration date G-38
extended number P-1
issue date G-38
logical devices G-59
moving from area 1-16
mustering areas 1-16, 1-17
never expire checkbox G-38
numbers 5-30
optional info G-49
panel specific options G-46
pathways G-65
revoking access G-61
supervisor PIN G-42
timed points G-64
transactions G-64
voiding
Part I 1-19
Part II 5-56
voiding, steps G-68
card download
tracking 5-32
verification 5-36
card options
PW-5000, PW-6000, PW-6101
PW-5000
card options 5-14
CardKey
adding
channel 9-3
logical device 9-36
panel 9-12
site 9-3
subpanels 9-13
card event 9-22
duress 9-16
editing
communication port 9-33
elevator 9-53
enable codes 9-21
event level G-48
holiday 9-20
information 9-14
input point 9-46
mag stripe 9-19
output point 9-48
setup 9-15
soft alarms 9-17
STI download G-48
threat level G-48
time zone 9-19
timed override G-48
CASI J-1
channel J-6
installation J-2
MUX8 J-18
quiz J-21
restrictions J-21
subpanel J-8
subpanels J-14
wizard panel creation J-10
CCTV
associating with an alarm 22-26
configuring 21-3
controls
Part I 1-18
Part II 5-55
steps 3-25
CCTV controls button 1-18

CFR
See Code of Federal Regulations 37-14
channel
adding
CardKey 9-3
CHIP 10-3
Matrix 11-3
PW-2000 7-3
SEEP 13-3
SmartPlus Mobile 14-3
Vindicator V5 15-3
VISTA 16-3
configuration report H-23
deleting
Matrix 11-7
PW-2000 6-51
PW-5000/3000 16-7
PW-6000/5000/3000 8-15
SmartPlus Mobile 14-7
Vindicator V5 15-7
VISTA 16-7
dependencies
Matrix 11-6
SmartPlus Mobile 14-6
Vindicator V5 15-6
VISTA 16-8
limit per site 5-2
CHIP
adding
actions 10-22
advanced 10-15
channel 10-3
event actions 10-24
events 10-29
holidays 10-18
logical device 10-34
MIRO board 10-11
panel 10-9
partitions 10-29
site 10-3
site codes 10-19
terminal users 10-28
time zones 10-17
zones 10-21
channel
configuring 10-10
editing
actions 10-22
advanced 10-15
event actions 10-24
events 10-29
holidays 10-18
logical device 10-39
panel 10-30
partitions 10-29
site codes 10-19
terminal users 10-28
time zones 10-17
zones 10-21
logical device
actions/digital 10-48
define logical device 10-40
events 10-52
input 10-52
keypad 10-46
logical device details 10-41
reader (advanced) 10-44
reader (general) 10-43
SNET/LED 10-47
Weigand Raw 10-51
Weigand/ABA 10-50
panel configuration report H-23
Star II elevators 10-58
two-man rule 10-24
Weigand Raw card format 10-51
class
configuration report H-24
classic badging G-1
clearance code
scheduled 2-53
temporary 2-53
clearance codes 37-1
Code of Federal Regulations 37-14, G-51
configuration report H-24
digital signature 37-14
memory warning 8-41
setting 5-29
tab G-51
cloud 1-37
Code of Federal Regulations
clearance code assignment to card G-51
clearance codes 37-14
company assignment to card 38-2
logical device assigned to card G-60
color
badge shape G-97
badge signature G-99
barcode G-90
bitmap G-84
coding 1-29

photo G-86
text G-81
communication status
alarm monitor 3-25
company
clearance code report H-23
Code of Federal Regulations 38-2
summary report H-23
tabs 5-38
setting 5-29
Compliance Report Manager 4-2
concurrency G-35
conditional display
badge shape G-98
barcode G-92
bitmap G-85
signature G-101
text G-82
configuration
CCTV 21-3
dial-up C-1
DVR 22-2, 22-15
HVMS 22-4
logical device 8-134
PW2000 7-12
PW-6K1ICE 8-56
tabs
PW-6000/5000/3000 8-24
configuration report H-23
panel type H-26
partition H-26
printer H-26
workstation H-27
configuring
dashboard 2-5
credentials
mobile 2-65

D

D600AP
panel configuration report H-24
dashboard 2-3, 2-4
configuring 2-5
data management
moving the database to another drive 63-21
data mapping rules
defining, in general 64-29
ODBC export 64-57
ODBC import 64-37
data transfer utility
audit log in 64-56
data transfer steps 64-7, 64-61
editing DTU profile 64-10
exporting
delimited data 64-43
images 64-58
ODBC data 64-50
import/export profile 64-8
importing
delimited data 64-11
fixed-length data 64-19
LDAP data 64-38
ODBC data 64-30
SQL data 64-24
log file 64-5
logical device data 64-48
manual load tab 64-17
mapping rules
LDAP import 64-42
ODBC export 64-57
ODBC import 64-37
transferring the data 64-61
types of interface 64-6
why export data? 64-43
why import data? 64-10
database
audit log report H-28
connecting to report H-35
limits
setting 5-39
moving the database to another drive 63-21
sizing 5-39
table H-24
database configuration
overview
Part I 1-10
Part II 5-5
alarm page
adding, editing 28-4
columns 28-7
copying 28-10
deleting 28-11
dependencies 28-9
event types 28-6
information tab 28-5
partitions 28-7
area 29-2–29-18
adding, editing 29-4
area occupants 29-15

CHIP reader mode 29-14
deleting 29-16
locking, unlocking 29-17
logical device input 29-12
logical device reader 29-11
partitions 29-15
zone mode properties 29-18
badge profile
adding, editing 30-5
badge profile info 30-6
copying 30-11
deleting 30-9
dependencies 30-10, 32-6
partitions 30-8
quick search configuration 30-7
badge status
adding, editing 31-4, 31-5
deleting 31-6
badge type
adding, editing 32-4
copying 32-7
deleting 32-8
BLOB type
adding or editing 33-4
deleting 33-10
dependencies 33-8
partitions 33-9
brass key
adding or editing 34-4
deleting 34-7
dependencies 34-5
partition 34-6
card format
adding, editing 35-4
copying 35-12
deleting 35-14
dependencies 35-11
non PW-2000 card format 35-5
partitions 35-13
PW-2000 ABA card format 35-7
PW-2000 Weigand/Tack One format 35-8
channel dependencies
generic 17-8
Matrix 11-6, 16-8
PW-2000 7-27
SEEP 13-6
SmartPlus Mobile 14-6
Vindicator V5 15-6
class
adding, editing 36-5
alarm pages tab 36-9
class tab 36-6
copying 36-14
deleting 36-15
dependencies 36-13
programs tab 36-6
routing groups tab 36-8
workstations tab 36-7
clearance code 37-5
adding, editing 37-4
copying 37-13
deleting 37-16
dependencies 37-12
elevator outputs 37-9
logical devices 37-8
output groups 37-9
partitions 37-11
company 38-2–38-8
adding, editing 38-4
clearance codes 38-5
copying 38-8
deleting 38-9
dependencies 38-7
information 38-5
partitions 38-6
database table
adding, editing 39-4
deleting 39-6
table information 39-4
deleting, workstation 59-9
device types
deleting 6-20
dependencies 6-21
dialup schedule
adding, editing 42-4
copying 42-7
deleting 42-8
dependencies 42-6
dialup schedule 42-4
partitions 42-4
event procedure
adding, editing 43-4
copying 43-10
deleting 43-12
dependencies 43-9
partitions 43-7
running 43-11
event trigger
adding, editing 44-4
copying 44-8

deleting 44-9
maintenance 44-5
partitions 44-7
procedures 44-6
event type
adding, editing 45-4
annunciation 45-7
copying 45-10
deleting 45-11
dependencies 45-9
information 45-5
partitions 45-8
group
adding, editing 47-4
copying 47-7
deleting 47-8
dependencies 47-6
maintenance 47-4
partitions 47-5
guard tour 48-5
adding, editing 48-4
copying 48-8
deleting 48-9
dependencies 48-7
partitions 48-6
hardware classes
deleting 6-25
dependencies 6-25
hardware templates
deleting 6-43
dependencies 6-43
holiday
adding, editing 49-4
copying 49-7
deleting 49-8
dependencies 49-6
information 49-4
partitions 49-5
keyboard accelerator
adding, editing 50-4
copying 50-8
deleting 50-9
dependencies 50-7
partitions 50-5
map
adding, editing 51-4
copying 51-7
deleting 51-8
dependencies 51-6
map information 51-4
partitions 51-5
modem pool
adding, editing 52-4
copying 52-6
deleting 52-8
dependencies 52-7
modem pool information 52-4
partitions 52-5
overview 27-2–31-2
partition
adding, editing 53-4
copying 53-6
deleting 53-7
dependencies 53-5
partition information 53-4
partition map 53-4
pathway
adding, editing 54-4
deleting 54-8
dependencies 54-7
partitions 54-5
pathway info 54-5
routing group
adding, editing 55-5
all system events 55-6
assigning to a class 55-8
assigning to a user 55-7
configuring
channels 55-5
event types 55-5
rollover event type 55-5
workstation 55-6
copying 55-13
deleting 55-14
dependencies 55-12
partitions 55-11
sizing 5-39
status group
copying 56-7
deleting 56-8
maintenance tab 56-5
partitions tab 56-5
time zone
adding, editing 57-4
copying 57-8
deleting 57-9
dependencies 57-7
maintenance tab 57-5
partitions tab 57-6
user
adding, editing 58-5
alarm pages 58-21
badge profiles 58-22
copying 58-25
deleting 58-27

device status filtering 58-12
event procedures 58-23
event toolbar 58-19
eventview column 58-18
keystroke accelerator 58-18
partitions 58-21
programs 58-13
routing group 58-17
user information 58-7
workstations 58-17
workstation
adding 59-4
CCTV monitors 59-6
communications server 59-8
dependencies 59-10
information 59-5
intercom 59-6
logical devices 59-7
partitions 59-8
database limits 5-39
database manager
See enterprise database manager
database size
archiving, purging 65-4
defining 5-39
query analyzer 65-9
deferred access 41-2
delete button 1-12
deleting
alarms 3-9
badge field 60-20
badges G-31
cards G-68
channel
Matrix 11-7
PW-2000 6-51
PW-6000/5000/3000 8-15
SmartPlus Mobile 14-7
Vindicator V5 15-7
VISTA 16-7
time zone G-63
DESFire Smart Card Key I-23
DESFire smart card Key Management I-23
details button 1-21
device type
adding, editing 6-16
balanced magnetic switch 6-31
configuring 6-14
copying 6-21
deleting 6-20
dependencies 6-21
door position switch 6-31
elevator
door select reader 6-31
input 6-31
output 6-32
reader 6-32
horn 6-32
lock 6-32
overview 6-2, 19-2, 26-2
PIR 6-32
reader 6-32
REX device 6-32
strobe 6-32
sub-panels 6-32
dial-up C-1
configuration C-1
dialup schedule
configuration report H-24
digital signature
CFR 37-14
clearance codes 37-14
digital video recording 1-20
associating with an alarm 22-26
configuring 22-2
digital video recording button 1-20
door position switch 6-31
download
cards G-65
tracking 5-32
verification 5-36
DTU
real time 64-3, 64-14
See data transfer utility
duress
CardKey 9-16
PW-6000/5000 8-143
duress signal
"Appended Digit" 5-40
Appended Duress Digit Q & A 5-42
setting the PIN length 5-41
DVR
See digital video recording
DVR, see digital video recording 22-2

E

editing
alarms 3-8
badge field 60-20
badge profile 60-12

badges G-4
in bulk G-15
cards G-37
logical device 7-31
registry manager N-2
time zone G-63
elevator
floor, select reader 6-31
input 6-31
output 6-32
reader 6-32
e-mail 5-30
protocols 5-30
employee G-6
encryption
128-bit 8-11
256-bit 8-11
icons 8-11
PW-5000 8-4
PW-6000 8-4
PW-6K1ICE 8-4
enhanced PIN mode 5-11
enhanced privileges
granting Privilege Restrict program access 5-23
scheme 5-24
setting Server Options 5-21
the Enhanced Privilege setting 5-26, 58-11
enterprise database manager 63-3
backup device maintenance 63-16
database
backup 63-3
restore database 63-9
from a device 63-13
from backed-up database 63-11
from file or file group 63-12
scheduled maintenance 63-18
deleting 63-20
disabling and enabling 63-19
editing 63-19
event
level G-48
managing 5-8
procedure H-25
type H-25
event log
report H-29
setting thresholds 5-8
sizing 5-45
viewing 1-14
Part II 5-52
exporting
See also data transfer utility
delimited data 64-43
export profile 64-8
images 64-58, G-31
mapping rules, ODBC 64-57
ODBC data 64-50
reports H-8
why export data? 64-43
extended card number P-1
extended instructions 5-13

F

Fargo ProL E-5
file menu
alarm monitor 3-25
find button 1-12
FlashPoint image G-17

G

Galaxy
configuration 2-51
Galaxy Dimension O-1
generic channels 17-2
grid G-72
group events
Mercury Intrusion 8-121
guard tour 6-40
configuration report H-25

H

hardware
channel
adding
CardKey 9-3
CHIP 10-3
Matrix 11-3
PW-2000 7-3
PW-6000/5000/3000 8-4
SEEP 13-3
SmartPlus Mobile 14-3
Vindicator V5 15-3
VISTA 16-3

CCTV 21-4
DVR 22-15
log printers 18-2
status 6-55, 20-2
class H-25
adding, editing 6-24
configuring 6-23
copying 6-26
device type
adding, editing 6-16
configuring 6-14
copying 6-21
overview 6-2, 19-2, 26-2
device type tab 6-31
DVR
CCTV camera views 22-18
configuring 22-2
hardware template
configuring 6-27
information tab 6-30
logical device
CardKey 9-40
CHIP 10-39
editing
PW-2000 7-31
SEEP 13-30
SmartPlus Mobile 14-17
Vindicator V5 15-18
panel
adding
CardKey 9-12
CHIP 10-9
Matrix 11-8
PW-2000 7-10
PW-6000/5000/3000 8-16
SEEP 13-8
SmartPlus Mobile 14-8
Vindicator V5 15-8
VISTA 16-9
buffer 24-4, 24-5
CardKey
communication port 9-33
configuring
CardKey 9-13
CHIP 10-10
PW-2000 7-12
SEEP 13-9
download 6-59, 20-7
editing
CHIP 10-30
PW-2000 7-24
PW-6000/5000/3000 8-36
PW-6K1ICE 8-68
SEEP 13-20
un-buffer 24-4, 24-5
template H-25
hardware classes
deleting 6-25
dependencies 6-25
hardware configuration
overview 1-10
CCTV commands
dependencies 21-13
CCTV monitor
dependencies 21-8
overview 5-4
hardware notes 5-15, 5-17
hardware templates
adding, editing 6-28
deleting 6-43
dependencies 6-43
HID 2-65
historical trace 3-15
Honeywell
DVM 22-2, 22-3
FUSION 22-2, 22-3
protocol
unselecting 8-83
Video Management System (HVMS) 22-2
configuring 22-4
using 22-13
horn 6-32
HVMS 22-2
configuring 22-4
using 22-13

I

icon color coding 1-29
image
exporting G-31
summary G-10
TWAIN G-19, G-22
importing
See also data transfer utility
delimited data 64-11
fixed-length data 64-19
import profile 64-8
LDAP data 64-38
mapping rules
LDAP 64-42
ODBC 64-37
ODBC data 64-30

signature G-30
SQL data 64-24
why import data? 64-10
installation
Magicard Prima printer E-1
instructions
extended 5-13
Integral 22-2, 22-3
intercom controls
alarm monitor 3-27
button 1-19
Part I 1-19
Part II 5-56
IRIS ID Q-1

K

key
brass G-9
keyboard accelerator
tab 50-4
keypad message G-41

L

large icons button 1-21
layer
badge items G-102
map function 3-30
layout
badge G-11
LDAP, Active Directory 64-61
licensing R-1
certificate R-3
cut-over & migration licenses R-18
demo R-8
how to supercede R-12
how to terminate R-17
how to transfer R-15
how to view R-10
regular R-4
licensing information 1-34
list button 1-21
live trace 3-15
lock 6-32
log files
sizing 5-45
log printers 18-2
log size 5-45
logging in to the Pro-Watch Server 1-5
logging reports H-27
logical device
adding
CHIP 10-34
Matrix 11-16
PW-2000 7-29
PW-6000/5000/3000 8-42
alarm monitor actions 3-22
assignment to card G-60
CardKey 9-36
cards G-59
Code of Federal Regulations G-60
configuration report H-25
configuring
advanced settings for PW-6000/5000/3000 8-143
anti-passback settings for PW-6000/5000/3000 8-145
define logical device for PW-6000/5000/3000 8-135
define Matrix logical device 11-21
events for PW-6000/5000/3000 8-146
input point events for PW-6000/5000/3000 8-147
input point for PW-6000/5000/3000 8-146
logical device details for PW-6000/5000/3000 8-136
Matrix advanced settings 11-26
Matrix logical device details 11-22
Matrix reader properties 11-23
Matrix reader settings 11-24
output events for PW-6000/5000/3000 8-149
output for PW-6000/5000/3000 8-148
reader properties for

PW-6000/5000/3000 8-138
reader settings for PW-6000/5000/3000 8-139
configuring for PW-6000/5000/3000 8-134
editing 7-31
actions/digital 10-48
define logical device 10-40
events 10-52
keypad 10-46
logical device details 10-41
reader (advanced) 10-44
reader (general) 10-43
SNET/LED 10-47
Weigand Raw 10-51
Weigand/ABA 10-50
icon 6-61
labels 5-29
Matrix
configuring 11-20
SEEP 13-25
server options 5-12
SmartPlus Mobile 14-12
status report 5-12
tags 5-10
template 6-27, 6-31
Vindicator V5 15-14
login 1-3
login accounts 1-8
logoff shadow user button 1-14
Loronix 22-2, 22-3

M

M5
MUX8 J-18
Magicard Prima
configuring E-1
Fargo ProL E-5
installing E-1
printer installation E-1
Pro-Watch E-5
magnetic stripe G-74, G-76
mail options 5-30
map view 3-29
MAPI mail option 5-30
mapping rules
data transfer utility 64-29
ODBC export 64-57
ODBC import 64-37
Matrix
adding
channel 11-3
panel 11-8, 16-9
site 11-3
deleting
channel 11-7
dependencies 11-6
Mercury
intrusion 8-90
LCD terminal 8-81
M5 bridge J-1
protocol 8-83
text output 8-81
Mercury Intrusion
command codes 8-103
configuring PW-6000 8-100
group events 8-121
intrusion groups
adding 8-110, 8-116
creating 8-116
intrusion zones
adding 8-110, 8-116
creating 8-103, 8-105
MRDT
display settings 8-126
terminal 8-121, 8-122
wiring 8-128, 8-130
panel tabs 8-92
reader tabs 8-94
settings 8-98
terminal command maps 8-128
Mercury intrusion 8-90
Mercury IP Client 5-18
Mercury M5 J-1
Mercury panel
adding 8-73
creating third-party panel 8-74
with User Wizard 8-75
without User Wizard 8-77
unselecting Honeywell Protocol 8-73
Mercury Protocol
third-party panel creating
with wizard 8-84
without wizard 8-87
merge replication 5-46
message
keypad G-41

Microsoft Azure 1-37
mobile credentials 2-65
modem pool
configuration report H-26
Morpho 2-50, I-1, R-1, S-1
adding biometric field to Pro-Watch Advanced Badging I-33
biometric integration I-1
DESFire Smart Card Key I-23
documentation & software I-32
enabling biometrics I-8
fingerprint configuration I-12
Indoor 500 Series Reader I-37
licensing I-31
MSO300 I-15
network configuration I-20
Outdoor 500 Series Reader I-38
Pro-Watch Advanced Badging I-8
Pro-Watch panel configuration I-28
Pro-Watch process diagram I-3
Pro-Watch setup I-4
Pro-Watch, adding biometric field to Advanced Badging I-33
Reader network configuration I-20
Reader smart card Key Management I-25
Smart Card Key I-25
template configuration I-10
template download Windows service I-21
version info I-30
MorphoWave
reader I-40
Quick Start for SSL I-47
requirements I-40
setup for enrollment I-41
setup in Advanced Badging I-42
Tower connection I-46
moving a panel F-2
MRDT
display settings 8-126
Mercury Intrusion 8-121, 8-122
wiring 8-128, 8-130
MS Azure 1-37
MSO300
Biometric Enrollment I-15
biometric enrollment I-15
multiple new badges G-13
mustering 1-16, 1-17
areas 1-16, 1-17
button 1-16
bell
Part I 1-16
Part II 5-55
freeze
Part I 1-16
Part II 5-55
print
Part I 1-16
Part II 5-55
deleting cards 1-17
moving cards 1-16
MUX8 J-18

N

new button 1-12

O

OmniSmart card reader
configuring 6-33
encryption enable/disable 6-34
supervision enable/disable 6-34
tamper enable/disable 6-34
operator log report H-30

P

panel
adding
CardKey 9-12
CHIP 10-9
Matrix 11-8
PW-2000 7-10
PW-6000/5000/3000 8-16
SEEP 13-8
SmartPlus Mobile 14-8
Vindicator V5 15-8
VISTA 16-9
configuring
CardKey 9-40
CHIP 10-10
PW-2000 7-12
PW-5000/3000 7-24
SEEP 13-30

SmartPlus Mobile 14-17
editing
CHIP 10-30
logical device
CHIP 10-39
PW-2000 7-24
PW-6000/5000/3000 8-36
SEEP 13-20
VISTA 16-15
moving F-1, F-2
panel configuration report
PW-2000 H-26
PW-5000/3000 H-26
Panel Move Utility F-2
panel type
configuration report H-26
partition
badge G-11
Cardkey 9-23
configuration report H-26
manager M-1
SEEP 13-19
pathways
card G-65
photo
capturing G-17
color G-86
compression 5-32, 5-39, 5-45
conditional display G-87
intensity 5-32, 5-39, 5-45
placing G-85
positioning G-87
PIN
biometric 2-50
enhanced PIN mode 5-11
PIN seed numbers 5-30
PIR 6-32
placing
photo G-85
play video
alarm monitor 22-21
positioning
barcode G-92
bitmap G-84
photo G-87
shape G-97
signature G-101
text G-81
printer
configuration report H-26
DIGID XID440 E-1
Fargo ProL E-5
Magicard Prima E-1
Magicard Prima installation E-1
printing
badges G-16
reports H-8
privilege management
granting Privilege Restrict program access 5-23
setting Server Options 5-21
the Enhanced Privilege setting 5-26, 58-11
program
assignable B-1
properties button 1-12
Pro-Watch
configuration chart 5-50
tool bar 5-51
Pro-Watch application login 1-3
Pro-Watch database
moving the database to another drive 63-21
Pro-Watch functions
administration
Part I 1-11
Part II 5-6
alarm monitor
Part I 1-10
Part II 5-5
badging
Part I 1-9
Part II 5-4
database configuration
Part I 1-10
Part II 5-5
hardware configuration
Part I 1-10
Part II 5-4
reports
Part I 1-10
Part II 5-5
Pro-Watch Panel configuration I-28
Pro-Watch Server login 1-5
Pro-Watch tool bar
button
delete 1-12
details 1-21
digital video recording 1-20
find 1-12
intercom controls 1-19
large icons 1-21
list 1-21
logoff shadow user 1-14

new 1-12
properties 1-12
shadow user 1-13
small icons 1-21
toggle event 1-14
verification 1-15
view event log 1-14
viewer bar 1-14
void card 1-19
CCTV controls 1-18
mustering 1-16
Pro-Watch/Morpho
biometrics setup I-4
process I-3
template download I-21
Windows service
configuration I-21
installation I-22
PW-2000
adding
channel 7-3
panel 7-10
site 7-3
configuring
advanced 7-14
card formats 7-18
events 7-22
facility codes 7-17
general 7-12
holidays 7-20
interlocks 7-15
output groups 7-16
panel 7-12
partitions 7-22
time zones 7-19
editing
default CCTV 7-38
define logical device 7-32
input 7-35
input events 7-37
logical device details 7-33
output 7-37
output events 7-38
panel 7-24
partitions 7-38
reader 7-34
reader events 7-35
transactions 7-38
input point 7-35
interlock 6-39
output point 7-37
panel configuration report H-26
PW-5000/3000
event 7-22, 9-23, 10-29, 13-19
interlock 6-34
interlocks tab 6-34
options G-46
panel configuration report H-26
PW5K conversion L-1
PW-6000
card options 5-14
memory warning 8-41
Mercury Intrusion 8-100
PW-6000/5000/3000
adding
channel 8-4
panel 8-16
configuring
biometric settings 8-28
card formats 8-30
events 8-34
holidays 8-29
panel 8-25
partitions 8-35
procedures 8-31
resistance values 8-33
time zones 8-29
triggers 8-32
deleting
channel 8-15
dependencies 8-10, 8-15
duress 8-143
editing
biometric settings 8-28
card formats 8-30
events 8-34
holidays 8-29
panel 8-25, 8-36
partitions 8-35
procedures 8-31
resistance values 8-33
time zones 8-29
triggers 8-32
elevator 8-43
input point 8-146
output point 8-148
PW-6101
card options 5-14
PW-6K1ICE
configuring
biometric settings 8-59
card formats 8-61
events 8-67
holidays 8-61

panel 8-56
partitions 8-67
procedures 8-63
resistance values 8-65
time zones 8-60
triggers 8-64
editing
biometric settings 8-59
card formats 8-61
events 8-67
holidays 8-61
panel 8-56, 8-68
partitions 8-67
procedures 8-63
resistance values 8-65
time zones 8-60
triggers 8-64
PW6K1ICE
RS-485 Downstream 8-50
PW6K1ICE DS 8-50

Q

Query Analyzer 65-9

R

Rapid Eye 22-2, 22-3
reader 6-32
adding 19-3
wireless 19-6
real time DTU 64-3, 64-14
reconnect
alarm monitor 3-28
registry manager
overview N-1
audio files N-3
autosilence N-3
bringalarmappforward N-3
bringalarmwinforward N-3
cardPINlength N-3
classPINretry N-4
commservername N-4
databaseconnect N-4
databasename N-4
databaseservername N-4
debugmode N-4
defaultdatabasepage N-5
defaulthelppage N-5
defaultreportpage N-5
defaultviewerlist N-5
defaultzoomall N-5
displaysplash N-5
editing N-2
exefiles N-5
firmwarefile N-5
helpfile N-6
installdir N-6
mapfiles N-6
maxbadgedisplay N-6
maxtrandisplay N-6
newalarmtimer N-6
packagedirectory N-6
picturefiles N-6
PW-3000firmwarefile N-7
reporteventsonunusedhardware N-8
subpanelfirmware N-8
toolbarfile N-8
userPINtry N-8
videoplayers N-8
remote
server topology 5-47
terminal services D-1
replication 5-46
merge 5-46
report designer
overview H-32
connecting database H-35
design report tab H-32
open existing report tab H-38
preview report tab H-38
save report tab H-38
text field H-33
reports H-1
overview 1-10
access H-19
badge holder access to a logical device H-19
card status H-19
clearance code/badge access H-19
last access at logical device H-20
last access by a badge holder H-20
logical device access by a badge holder H-20
mustering H-21
badge holder H-21
area attendance H-21

badge holder detail H-21
badge holder summary H-22
key assignment list H-22
company H-23
clearance code H-23
summary H-23
configuration H-23
badge profile H-23
badge type H-23
brass key list H-23
channel H-23
CHIP panel H-23
class H-24
clearance code H-24
D600AP panel H-24
database table H-24
device type H-24
dialup schedule H-24
event point H-25
event procedure H-25
event type H-25
guard tours H-25
hardware class H-25
hardware template H-25
logical device H-25
modem pool H-26
panel type H-26
partition H-26
printer H-26
PW2000 panel H-26
PW5000 panel H-26
response code H-27
routing group H-27
SEEP panel H-27
time zones H-27
workstation H-27
creating H-3
database connecting H-35
exporting H-8
export file path H-11
file format H-9
format parameter H-10
header and footer H-9
logging H-27
database audit log H-28
event log H-29
operator log H-30
logical device status 5-12
overview 5-5
printing H-8
saving
configuration H-12
scheduling H-13
deleting H-18
editing H-18
executing H-18
settings tab H-17
task H-14
time H-14
user H-31
user detail H-31
user summary H-31
using H-8
response code
alarm monitor 3-9
report H-27
restrict user privilege 5-25
revoking access
cards G-61
revoking card G-61
REX device 6-32
routing group
configuration report H-27
RS-485
PW6K1ICE 8-50

S

SALTO
REX 19-16
system configuration 19-14
scheduling
a report H-13
clearance codes 2-53
time
frequency H-14
searching
advanced G-32
quick G-32
secure mode verification A-1
considerations, limitations A-2
how it works A-4
implementation A-3
overview A-1
See badging
advanced 2-2
SEEP
adding 13-25
channel 13-3
panel 13-8
site 13-3
configuring 13-30

editing
panel 13-20
events 13-19
holiday 13-14
input point 13-39
interlock 6-36
output point 13-40
panel configuration report H-27
report 13-15
terminal user 13-18
time zone 13-13
transactions 13-18
server
remote, topology 5-47
server options 5-7, 5-8
additional 5-29
assigning extended instructions 5-13
hardware notes 5-15, 5-17
setting a Clearance Code 5-29
setting a Company 5-29
setting badge photo compression 5-32
setting badge photo intensity 5-32
setting card download verification 5-36
setting company tabs 5-38
setting database limits 5-39
setting download tracking 5-32
setting event log thresholds 5-8
setting logical device status reporting 5-12
setting Logical Device tags 5-10
setting Logical Devices 5-29
setting mustering 5-32
setting the card and PIN numbers 5-30
setting the log size 5-45
shadow user 1-13, 5-52
logoff 5-52
shadow user button 1-13
shape
badge G-96
color G-97
conditional display G-98
positioning G-97
signature
capturing G-29, G-31
color G-99
conditional display G-101
importing G-30
placement G-98
positioning G-101
tab G-99
site
channel limit 5-2
small icons button 1-21
SmartPlus Mobile
adding
channel 14-3
logical device 14-12
panel 14-8
site 14-3
deleting
channel 14-7
dependencies 14-6
input point 14-23
output point 14-25
SMTP mail option 5-30
snap G-72
SNET
Card Format 8-140
CHIP panel 10-47
configuring the panel
Port 3/4 baud rate 8-26
PW-6000 panel baud rate 8-26
PW-6000 panel LEDs 8-27
SNET LED 8-27
configuring the reader
add I/O module 8-38
configuring the I/O module 8-37
Default mode 8-141
LED mode 8-140
SNET reader type 8-142
specifying SNET reader type 8-142
PW-6000 panel LEDs 8-27
SEEP panel 13-37, 13-38
software keys R-1
status group
adding, editing 56-4
alarm monitor 3-28
STI download G-48
strobe 6-32
sub-administrator
granting Privilege Restrict program access 5-23
setting Server Options 5-21
the Enhanced Privilege setting 5-26, 58-11
sub-panels 6-32
CardKey 9-13

supervisor PIN G-42

T

tabs
biometric settings 8-28
card formats 8-30
events 8-34
holidays 8-29
panel 8-25
partitions 8-35
procedures 8-31
resistance values 8-33
time zones 8-29
triggers 8-32
TBS S-1
enroll fingerprints S-21
limitations S-6
manual configuration S-8
prerequisites S-5
terminal
remote control D-1
terminal services
client D-3
creating shortcut to D-4
installing on D-3
server
connecting to D-5
creating a share on D-2
text
badge G-80
block G-81
color G-81
conditional display G-82
positioning G-81
report designer H-33
threat level G-48
thresholds 5-8
time zone
alternative G-64
configuration report H-27
deleting G-63
editing G-63
timed override G-48
timed points
card G-64
toggle event button 1-14, 5-53
tool bar
alarm monitor 3-12
badge designer G-79
button
delete 5-51
digital video recording 5-57
find 5-51
intercom controls 5-56
logoff shadow user 5-52
new 5-51
properties 5-51
shadow user 5-52
toggle event 5-53
verification 5-54
view event log 5-52
viewer bar 5-52
void card 5-56
CCTV controls 5-55
mustering 5-55
trace 3-15
track G-76
transaction
cards G-64
transactional replication 5-46
transferring data 64-61
TWAIN image G-19
Two-Person Rule 29-6, K-1
"Minimum" option K-3
activate K-2
FAQ K-4
Mercury panel support K-2
Quiz K-5

U

unit
inch G-71
millimeter G-71
user
detail report H-31
functions 1-1
login accounts 1-8
privilege 5-25
report H-31
summary report H-31

V

VAST 22-2, 22-3, 22-24
verification
button
cascade

Part I 1-15
Part II 5-54
erase all
Part II 5-54
freeze
Part I 1-15
Part II 5-54
live video window
Part I 1-15
Part II 5-54
print area members
Part II 5-54
show pictures denied access
Part I 1-16
Part II 5-54
show pictures given access
Part I 1-16
Part II 5-54
sound bell on grant transaction
Part I 1-16
Part II 5-54
new button
Part I 1-15
Part II 5-54
secure mode A-1
verification button 1-15
video
play, alarm monitor 22-21
video recording 1-20, 22-2
view event log button 1-14
viewer bar button 1-14
Part II 5-52
Vindicator V5
adding
channel 15-3
logical device 15-14
panel 15-8
site 15-3
deleting
channel 15-7
dependencies 15-6
input point 15-23
output point 15-25
VISTA
adding
channel 16-3
panel 16-9
site 16-3
deleting
channel 16-7
dependencies 16-8
editing panel 16-15
VMS 3-2
voiding
cards G-68
button 1-19

W

window pane
alarm monitor 3-11
wireless
reader 19-6
adding 19-3
workstation
configuration report H-27

Z

zoom factor G-72

Honeywell Integrated Security
135 W. Forest Hill Avenue
Oak Creek, WI 53154
United States
800-323-4576
414-766-1798 Fax
www.honeywellintegrated.com

Specifications subject to change without notice.

© 2020 Honeywell, Inc.
Document 7-901071V19

Honeywell