Pro-Watch™

Security Management

Pro-Watch™ Installation and Functional Overview
Release Four
# Table of Contents

## Section 1  Introduction  
- Database Partitioning  
- Field Panel Deployment  
- Door Exception Lists  
- System Configuration & System Integration  
- Native AutoCAD Maps  
- OLE-DB Database Access  
- Download Monitor  
- Timed Clearance Codes  
- Custom Alarm Pages  
- Multiple Badge profile screens assigned by Operator  
- High-End Servers  

## Section 2  Architectural Overview  
- Pro-Watch User Interface  
- Pro-Watch Alarm Monitor  
- Pro-Watch Badge Builder  
- Pro-Watch Mao Builder  
- Pro-Watch Data Transfer Utility  
- Pro-Watch Database Manager  
- Pro-Watch Registry Editor  

### Access Control Features  
- Badge Profiles  
- Badge Range  
- Badge Status  
- Badge Types  
- Card Formats  
- Brass Keys  
- Companies  
- Reader/Door Configurations  
- Areas and Anti-Passback  
- Default Events  
- Event Procedures  
- Event Triggers  
- Event Types  
- Timezones and Holidays  
- Global Timezones and Daylight Savings Rules  

### Clearance Codes  
- User Information  
- Routing Groups  
- Database Partitions  
- Device Types  
- Hardware Classes  
- Hardware Templates  
- Logical Devices  
- Groups  
- Channels  
- CCTV Matrix Switchers
### Section 3  Installation Procedures

**Operating Systems**
- Installing Windows 2000 Server
- Member Server
- Domain Controller
- Configuring Network Adapters
- Installing a Loopback Adapter
- Assigning a Static IP Address
- Installing Windows 2000 Service Pack 2

**Accounts and Permissions**
- Creating a Pro-Watch User Group
- Creating a Pro-Watch Administrator Account
- Creating a Pro-Watch User Account

**Database Engine**
- Installing Microsoft Data Engine (MSDE)
- Installing SQL Server 2000
- Installing SQL Server Service Pack 1

**Pro-Watch Application**
- Installing the Pro-Watch Database
- Installing the Pro-Watch Application

### Section 4  User Operations

**Sites**
- Creating a Site
- Modifying a Site
- Deleting a Site

**Channels**
- Creating a Channel
- Modifying a Channel
- Deleting a Channel

**PW-5000 Panels**
- Creating a PW-5000 Panel

**Star 1 Panels**
- Creating a Star 1 Panel

**Clearance Codes**
- Creating a Clearance Code
- Modifying a Clearance Code
- Deleting a Clearance Code

**Badge Records**
- Creating a New Badge Record
- Modifying a Badge Record
- Deleting a Badge Record

**Card Records**
- Adding and Assigning Card Access

### Section 5  Access Control Glossary
Pro-Watch Security Management System

Overview

Introduction

Pro-Watch™, the premier NexWatch line of access control, alarm monitoring, video imaging, badging and CCTV control systems is designed to integrate seamlessly with virtually any organizational infrastructure. Initially created for the airport arena, Pro-Watch has since become the leader in the security industry successfully installed at facilities throughout the world.

Industry standards in networking, database engines, and the latest in information-management technologies; Pro-Watch becomes the most flexible and responsive Access Control System ready to be plugged into the enterprise network and ready to handle the most demanding enterprise applications.

With Windows® 2000 Server as the operating platform, Pro-Watch opens the door to a tightly integrated client/server database architecture that assures data integrity, reliable distributed transaction processing and optimal information sharing and maintenance.

Designed to meet the challenges of today’s growing business, Pro-Watch™ combines the flexibility, scalability, and power required for world-class security management without compromising the simplicity to make it work for you.

Pro-Watch offers the following benefits and features:

- Pro-Watch offers a non-proprietary Security Management System based on an open-architecture and made available through a network of certified NexWatch dealers.

- Pro-Watch leverages the existing network infrastructure by using standard network protocol to communicate to all system components.

- Pro-Watch leverages the stability and performance of Microsoft SQL Server 2000 as a database server.

- Pro-Watch provides a system, which is scalable from a localized single server installation with a few workstations to a global enterprise-wide solution involving regional servers and a virtually unlimited workstation and reader count.²


1 Pro-Watch is a trademark of NexWatch

2 Scalability involves the appropriate investment in hardware and network infrastructures.
Multiple reader technology support: Digital Prox, Weigand, Keypad, Magnetic stripe, Barcode, Biometrics.

CCTV control interfaces for VideoBlox, Pelco, Burle, Vicon, and others

'Generic Channel' functionality, which supports communication to third party devices via, customized interfaces.

Digital Video Storage control interface for NexWatch VAST™.

Unparalleled database-partitioning scheme allows for tremendous flexibility in managing operator permissions

Real-time status monitor provides “at a glance” status of the entire system and the ability to quickly evaluate the details of any entrance or alarm point

Report Manager provides customizable reports, savable report templates, an export option, and a report scheduler.

Database Import/Export Utility dynamically transfers Pro-Watch data to and from third party databases - a convenient customizable interface to Human-Resources database systems.

Global event processor links events on one field device to actions on many others.

Global area tracking and Anti-Passback processing enforces entry/exit and occupancy rules.

Visual hardware configuration ‘control panels’

Real-time Status monitors

History queries
Database Partitioning

Pro-Watch “partitions” provide the most flexible mechanism available for partitioning a database. System Resources such as cards, badge-holders, and field devices can be assigned to any number of partitions and so can the system operators: the need for special fixed ‘common partitions’ is removed.

Pro-Watch supports dynamic partitioning - administrators can assign partitions to resources at any time and the changes will take effect immediately. Administrators can assign partitions to groups of operators. Operators may view any item in their assigned partition (or group of partitions) as well as any global (unpartitioned) resource.

Field Panel Deployment

NexWatch PW-5000 series control panels are installed providing a two reader I/O module at each field location even if only one reader is required. This strategy will provide

- Plenty of ‘headroom’ leaving spare I/O resources available for future expansion. The goal will be to provide at least 25% headroom employing, on average, no more than 75% of the field panel resources in the initial installation.

- Standardized door installations.

- Simplified door installations: minimizes homerun wiring.

- Power monitoring and Tamper alarm monitoring at every location.

Pro-Watch supports “hardware templates” that capture hardware attributes across similar security devices. The operator can setup templates with the correct default programming and simply assign specific hardware devices using the template as a roadmap.

Door Exception Lists

Pro-Watch supports “precision access” through the use of exception lists. Pro-Watch knows when a door has been added or deleted from a cardholder; overriding any assigned clearance code. When downloading a card, Pro-Watch detects a custom door added or deleted to the card and sends the exception to the panel.

When a panel makes an access decision, it checks to see if the card has an exception assigned at the presented door. If so, the exception overrides any clearance codes; otherwise, processing continues with the assigned clearance codes. This feature eliminates excessive downloads by eliminating the door map; the panel uses only the memory required to hold the exceptions list.
System Configuration & System Integration

Pro-Watch provides seamless integration with other third party facility management subsystems like CCTV, Pagers, Intercoms, and Digital Storage Devices. Pro-Watch supports a “Generic Channel” capability, which allows customized interfaces to previously unsupported third party devices.

Native AutoCAD Maps

Pro-Watch uses native AutoCAD files allowing icons placed directly over the AutoCAD drawing without any conversion of the file. Operators can control zoom and layer visibility using simple right-clicks.

OLE-DB Database access

Pro-Watch uses Microsoft’s object-oriented database access called OLE-DB. The OLE-DB API replaces the older, less efficient ODBC standard. Microsoft has been migrating to the newer OLE-DB since the OLE-DB method is a better performer due to its support of not only relational databases, but also to “hierarchical data sets” such as Microsoft Exchange stores and XML recordsets. OLE-DB allows easier integration of disparate data sources. This technology lays some of the groundwork for a move to other database server vendors and web-based database access in the future.

Download Monitor

Pro-Watch has a download monitor displaying every queued download, the status of each, and errors encountered for every communication channel.

Timed clearance codes

Pro-Watch supports “timed clearance codes”. A timed clearance gets added, temporarily, to a card swiped at a special enrollment reader. Pro-Watch will then download the card to update the doors assigned in the timed clearance code. Later, when the card swipes at a special de-enrollment reader or after an operator defined time expires, Pro-Watch will remove the timed clearance and update the affected panels to restore the original clearance code rules.

Customized Alarm Pages, Toolbars, Keyboard accelerators

Pro-Watch uses the concept of “custom alarm pages” in the alarm monitor. The administrator defines which columns to display in the alarm monitor based on the type of event. For example, when a “Card Expired” alarm occurs, you would see the expiration date on the same line as the alarm itself because the first question will be “When did it expire?”
If an operator needs often to repeat a set of actions, a custom toolbar can be defined. The toolbar can be customized to perform Alarm Monitor built-in functions or run a macro using Pro-Watch procedures. The administrator controls the icon, placement, and help text of the button when building the toolbar.

Keyboard accelerators allow the operator to re-assign common functions to familiar keys. For example, if <CONTROL-A> was the old way of acknowledging an alarm, you can build a keyboard accelerator for <CONTROL-A> and assign any alarm monitor function or Pro-Watch procedure to be executed.

**Multiple Badge profile screens assigned by Operator**

Pro-Watch will support any number of badge profiles. The system administrator assigns the badge profiles to the appropriate class and/or user. If the operator has more than one profile assigned, Pro-Watch will ask which profile to use. For example, you may define profiles that handle visitor badges, contractor badges, employees, and others. The operator controls what and where shows up on each page.

**High-End Servers**

Server capacity and network bandwidth will, more than any other factors, govern the overall throughput and responsiveness of a Enterprise level access control system. For this reason, the Pro-Watch Servers are chosen from the Compaq ProLiant™ Server Line.

The ProLiant Servers will provide:

- **Fault Tolerance – System Level.** The two servers will operate in a hot redundant configuration; allowing the server operating in a secondary role to take over from the server operating in a primary role with minimal downtime.

- **Fault tolerance – Server Hardware Level.** Each server will support multiple processors with redundant power supplies and redundant fans.

- **Fault Tolerance – Data storage Level.** A RAID array built around the Compaq SmartArray controller will provide RAID Level 0+1 disk mirroring and striping for the ultimate in data redundancy and performance. Hot swap drives are supported and allow the system to replace a failed array drive automatically at the time of failure.

---

3 ProLiant is a trademark of Compaq Computers
Section 2

Architectural Overview

Pro-Watch™ uses a multi-tiered client server architecture employing industry-standard back-end in the form of Microsoft SQL Server 2000, a multi-threaded Pro-Watch™ server in the application logic tiers and an intuitive set of user interfaces which observes Microsoft User-Interface guidelines.

All system components have been designed to operate under the control of the Windows 2000 operating system. Server components require Windows 2000 Server or Advanced Server while and the user interface can be loaded on any Windows 2000 platform.

Network and Interprocess communications depend on the TCP/IP protocol suite. Connections to the database are managed using the OLE-DB API; which ultimately utilizes network “pipes” to communicate with the SQL database engine.

Field panel and foreign-device communications are usually network-based. Serial device servers are employed to create connections to local and remote field devices. Local devices can also utilize direct serial port connections to the communications server.

Access Control to the operating system and Pro-Watch application is supervised through Windows 2000. Pro-Watch user-authentication is integrated with the operating system; a fact which avoids duplication of security functions and which enforces the strong rules established for Windows 2000. All operator access to the system can be audited.

User Interface Components

Pro-Watch User Interface

The Pro-Watch user Interface is the main control panel from which virtually all operator tasks are performed. Other user interface components or modules can be accessed from the main user interface.

The main features of the Pro-Watch user interface are:

- Integrated PhotoID and badging
- System Hardware Configuration
- System Database Configuration
- Monitoring

---

4 Windows NT 4.0 Operating Systems are also supported.
- Reports
- System Administration

**Pro-Watch Alarm Monitor**

The alarm monitor provides a user interface from which operators can monitor and manage alarm events that are routed by the server. Access to CCTV functions, Badgeholder Photos, and graphic maps are available when an associated condition occurs. Controls for acknowledging alarms, clearing alarms, silencing alarms, and logging comments are supported. Pre-programmed explanations of each alarm condition are displayed, in addition to operator instructions, and pre-programmed operator responses; which are used to help the operator respond quickly and clearly to alarms.

**Pro-Watch Badge Builder**

The Pro-Watch badge builder provides a way to define on-screen data entry forms to be used for creating Badgeholder records. A drag and drop utility allows an administrator to locate user-defined Badgeholder fields on one or more pages of a tabbed form. Each set of forms can be associated with Companies and badge types to customize data entry for different groups of Badgeholders in the system.

**Pro-Watch Map Builder**

The Pro-Watch Map Builder provides a way to define graphic maps for display by operators during alarm management and other monitoring duties. Graphic maps consist of scalable static backgrounds created from native DXF, DWG, and WMF graphic files with dynamic overlays of icons representing system resources such as readers, doors, and alarm points. The alarm monitor can cause one of these to be displayed and the icon overlay can be used to view resource status and to control individual resource points.

**Pro-Watch Data Transfer Utility**

The Pro-Watch Data Transfer Utility provides a way to create programmed data transfers for selected data moving in and out of the system. In this method, automated import or export of data can be scheduled or executed upon demand. Specifying the data source and destination through the use of ‘directors’ programs data transfers.

**Pro-Watch Database Manager**

The Pro-Watch Database manager is provided for senior operators and administrators who need help in managing system backups and database integrity checks. It provides access to the SQL Backup and restore functions, Backup device maintenance, Backup job scheduling, and a SQL query tool/analyzer.

**Pro-Watch Registry Editor**

The Pro-Watch Registry Editor is provided for installers or senior administrators for checking Pro-Watch registry keys.
Access Control Features

Badges and Cards

Pro-Watch stores Badgeholder information in a database table separate from the actual cards, which they are assigned for access.

Badge Profiles

A badge profile may be created for each different kind of badge being managed by the Pro-Watch system. The badge profile records properties related to Badgeholder data input form display options.

Badge Ranges

The Badge Range fields have been created as a means of ensuring that a specific data range is honored. This range can be assigned to any field that requires a user entry minimizing operator entry errors.

Badge Status

Badge Status items can be created to track special badge status not already incorporated in the system.

Badge Types

Badge types define the front and back badge designs for a type of badge. The badge layout design is created from this database.

Card Formats

Card Formats define the binary bit structure of the access control card used. Card formats are bound to certain readers to give them rules about parsing card reads.

Brass Keys

Brass Keys can be tracked by Pro-Watch. A brass key is created with a name and type and is assigned to a Badgeholder. Reports are available to track the keys.

Companies

The company defines a group of Badgeholders. A Company is assigned a group of access rules in the form of clearance codes. When a Badgeholder is issued a new card, the clearance codes assigned to the company are inherited by the new card saving the operator the trouble of having to repeat this operation for every Badgeholder in the group. The term “Companies” can be tailored to the customer needs such as Department, Tenant, Account, etc.
Readers and Doors

Reader/Door configurations

Reader controlled Doors are configured by giving the reader a description and assigning real resources to the resources specified by the Hardware Template they were created from. This might involve assigning real point addresses to the reader, the lock control output, the horn control output, the DPS, and the RTE input points.

Other default properties of the reader/door are:

- Default audio and AVI files.
- Default Email
- Default Map ID
- Default CCTV information (Auto and manual views and commands)
- Panel interlocks (reader related)

Anti-Passback and Areas

Areas and Anti-Passback

The installer or administrator can create ‘areas’ which in turn define area tracking zones, occupancy rules, and Anti-Passback rules.

Area properties include:

- Lock Status for this area
- Occupancy Count in this area– minimum and maximum allowed
- Passback Rules for this area: None, Soft, Hard
- Two person rule - Active Flag
- Triggers” Event triggers and procedures which are triggered in response to occupancy rule violations in this area.
- List of reader/doors assigned in this area
- List of occupants currently in this area.
Alarms and Events

Default Events

Defines a list of all events, which can be generated by various resources in the system: panels, sub-panels, readers, input points, and output points. For each resource type, the manufacturer of the device can be selected to view just the events from one specific device type such as PW5000 IC events.

Once a device type and a manufacturer is chosen, the resulting list of events shows the complete event repertoire for that event and, in each case, the display name of the event and its ‘address’ or event code.

Event Procedures

Event Procedures are created at the server level to program a series of control commands which can be activated on demand or automatically in response to various server-side events such as Event triggers or area control violations.

Event procedures can be programmed to control any resource, any resource group, or any clearance code.

Event Triggers

An Event Trigger can be created to establish a trigger for an automated event procedure (see above). A trigger can respond to any one of the following triggering events and/or event specifications:

- Events from a particular logical device such as a reader, a door, an alarm, etc
- Events from a particular device type (see above).
- Events of a particular type
- Events of a particular event number
- Events involving a particular card number
- Events on a particular date and/or time
- Events from resources in a particular group
- Events involving a particular clearance code.
- Events during a particular time-zone
- Events involving cards from Badgeholders in a particular company
- Events involving the use of a particular PIN code.
Event Types

Event Types are created to define the properties for all events. Default Events are defined to bind these event types to the actual event codes generated by the system resources.

Event properties can include:

- Re-Issue Time – 0 to 10 minutes
- Priority – 0 to 999
- Global Shunt Flag - shunt all occurrences of this event.
- Force Ack Note Flag – Check to force operators to make a note in the log
- No Log Event Flag
- Alarm Event Flag
- Auto Clear Flag
- Force Close Note Flag
- Rollup Events Flag
- Rollover Event settings: Time and procedure
- Passwords for Acknowledgments and/or Responses
- Default Message for this event
- Annunciation Settings: Colors, Flash flag, audio file with repeat flag and frequency.

Access Control Rules

Timezones and Holidays

Timezones define one or more time ranges each with a map of days of the week plus holidays type 1, 2, or 3.

A start-date plus duration define holidays in days. Holidays have a holiday type of 1, 2, or 3.

Timezones are used throughout the system to define time rules. They are essentially a weekly schedule, which repeats endlessly. The timezone is either active or inactive. Many server functions are controlled by timezones. They are assigned to panels to define the time and date rules for access by cards.
Global Timezones and Daylight-Savings Rules

Global Timezones are assigned to communication channels. All the panels on that channel are assumed to be in the same time zone. Daylight Savings rules are defined at the server.

Clearance Codes

Clearance codes define access rules for place and time. A clearance code defines a set of readers each with an associated time zone. The timezone defines when a person using this clearance code can access the reader. If a reader is not present on the list or if the time zone associated with it is never active, the clearance code will never provide access through that reader.

Clearance codes can be assigned to companies, from there to the cards held by Badgeholders assigned to that company. Clearance codes can also be assigned directly to cards. If a card is assigned more than one clearance code, the combination of clearance codes taken together is permissive: that is, if a given door is valid in any of the assigned clearance codes, the card will be granted access.

Users (Operators) and User Classes

Operators are called Users in Pro-Watch. A Pro-Watch user must be a defined operating system user (defined under Windows 2000) but not all Windows 2000 users need to be Pro-Watch users. Pro-Watch user authentication is integrated with Windows.

Users are organized in classes for ease of management. Both users and user classes have the roughly the same permissions. The following list of permissions applies to operator/users of the system whether the permission was granted to them because of their class or because the administrator granted permission directly to the user.

User information

Each user has a username/logon taken from Windows. In addition to assigning a user name, Pro-Watch allows for expiration dates, special PIN permissions, and badge information to be assigned to users.

Status Filtering

Device Status can be interpreted differently for different users if necessary. The device status filtering settings allow the administrator to define which kinds of device status are important for this operator in the device status display.

Program Access

Users can be assigned permissions to different system functions. A list of ‘programs’ – or system functions – contains sublists of subfunctions defining what functions an operator can do in the system.
Workstation access

Users can have access to different workstations in the Pro-Watch system. The Windows operating system will have controlled whether an operator is allowed to be logged in or not at specific workstations at specific times. Pro-Watch defines whether Pro-Watch itself can be used at a given workstation.

Routing groups

Routing groups determine what events/alarms will be routed to this operator at this workstation.

Event View Columns

Event View Columns define the layout of the event monitor for this operator/user.

Keystroke accelerators

The keystroke accelerators (defined elsewhere) are assigned to the operators here.

Event Toolbars

The event toolbar can be customized for this operator here.

Partitions

Any operator can be given access to any group of partitions. If no partitions are specified, the operator can have access without partition limitations – access to all partitions.

Alarm Pages

Alarm pages have been defined elsewhere. Here we assign which alarm pages this operator will view.

Badge Profiles

Badge profiles have been defined elsewhere. Here we assign which badge profiles this operator/user can use.

Event Procedures

Event Procedures have been defined elsewhere. Here we assign which group of procedures this operator can use.

Routing Groups

A routing group defines the group of events and routing rules, which the system uses to decide whether and where to route specific events. By assigning these to operator/users, the administrator can decide what, where, and when they can see specific events and alarms. Each item in the routing group defines a timezone, indicating when the rule is true,
and an ‘Ack’ flag and a ‘Clear’ flag for each item indicating whether this operator has the right to acknowledge or clear these events.

Routing group properties are:

**Channels**

The channels of communication which this operator/user is permitted to monitor. If s/he is to monitor events from a certain door, the panel which services that door must be communicating through a channel to which the operator/user has access in one or more routing groups. For each channel, the associated timezone defines when this should be true.

**Generic Channels**

Pro-Watch supports the use of ‘Generic Channels’. A generic channel allows the installer to create a custom interface to any third-party device, which communicates using a published ASCII-based protocol. In this way, Pro-Watch can send commands to third party devices and can parse and respond to incoming messages from third-party devices.

**Event Types**

These are the events which should be displayed to this operator. For each event, the associated timezone defines when this should be true.

**Rollover Event Types**

These are the roll-over events which are displayed for this operator. For each roll-over event, the associated timezone defines when this should be true.

**Workstations**

Events can be displayed at these workstations. For each workstation, the associated timezone defines when this should be true.

**Database Partitions**

Pro-Watch has the most flexible database partitioning system available in access control today. Virtually every item in the database is already partitioned and those items, which are not, generally do not ever need to be. The partitioning capability can be turned on and off for some sections of the database such as Cards and Badgeholders.

Partitions control what system resources an operator can see.
Hardware Configuration and Status Monitoring

Device Types

Pro-Watch uses device types to define the fundamental uses of hardware resources. Example: A reader device can be a single reader, or it can be either a primary or secondary reader on a double reader door. The device type allows the installer to create a label on this type of hardware resource.

Hardware Classes

Pro-Watch uses hardware classes to organize groups of like hardware resources.

Hardware Templates

Pro-Watch uses hardware templates to organize aggregates of hardware device types which comprise one operating unit such as a reader controlled door consisting of a reader, lock relay, sounder relay, DPS input, and RTE input.

A hardware template defines

- A Description (a display name)
- All display icons for each resource states.
- Collection of device types
- Related Panel Interlocks

The ability to use the template saves time during the installation process.

Logical Devices

Pro-Watch defines logical devices, which represent single resource items or aggregates of real field equipment defined by hardware templates. The logical device properties vary depending on the actual resource created. In addition to the assignment of physical points, logical device properties include:

- Default audio file (WAV file)
- Default AVI file
- Default Email
- Default map ID
Groups

Pro-Watch allows the administrator to create groups of resources. This means that a group could consist purely of readers, or of output control points; or it could consist of a mixture of readers, outputs, inputs, or any logical device in the system.

Groups can be used for manual control purposes or can be used in automation procedures.

Channels

Each communication point in the system is called a channel. A channel can be a direct serial COM port connection to an access control panel or auxiliary device such as Pager, CCTV switcher, or Intercom controller.

Channel properties include:

- A channel type (defines protocol)
  - PW-5000 Channel
  - WSE SEEP Channel
  - CardKey Panel (Special Configuration Required)
  - Thorn Panel (Special Configuration Required)
  - Generic Channel
  - Log Printer Channel
  - CCTV Channel (various)
  - Pager Channel

- Global timezone –to localize time and date

- Primary and secondary port selection
  - Hardwired on COM
  - Dial In on COM
  - Dial Out on COM
  - Modem Pool
  - TCP/IP on IP address and IP port
CCTV matrix switchers

A Pro-Watch Channel is setup to communicate with each CCTV matrix switcher. CCTV command sequences are programmed with one or more of the following commands:

- Switch Monitor to Camera View
- Switch Camera to workstation Monitor 1
- Switch Camera to workstation Monitor 2
- Stop previous CCTV action
- Switch camera to preset
- Raw command to CCTV unit
- PTZ – Tilt camera Up, Down, Left, Right, Up+Left, Up+Right, Down+Left, Down+Right, Zoom In, Out, Focus Near, Focus Camera Far, Open Iris, Close Iris

CCTV commands can be associated with alarms to create automatic CCTV camera selection.
Installation Procedures

This section has been designed to assist in the installation of the Pro-Watch application as well as the operating system, SQL database engine, and associated system peripherals.

The Pro-Watch software suite is a very friendly application for whatever configuration needed. The following is a listing of basic software operating systems and database requirements:

**Pro-Watch Professional Edition**

- **Server Application Operating System**: Windows 2000 Server with SP2
- **Server Database Engine**: Microsoft Data Engine (MSDE)
- **Client Application Operating System**: Windows 2000 Professional with SP2

**Pro-Watch Corporate Edition**

- **Server Application Operating System**: Windows 2000 Server with SP2
- **Server Database Engine**: Microsoft SQL Server 2000 with SP1
- **Client Application Operating System**: Windows 2000 Professional with SP2

Setup and installation instructions for the above-mentioned are detailed in the sections following.

Operating Systems

The Pro-Watch software suite is designed and Certified for Windows 2000. Although the Actual Pro-Watch application will function on Windows NT Server and Workstation, this section will cover only the installation and setup procedures for a Windows 2000 based system.

**Installing Windows 2000 Server – Member Server Install**

1. Insert the Windows 2000 media CD into the CD Drive and turn on the machine.
2. You may be prompted to hit any key to boot from the CD, if this message appears, hit a key on the keyboard. Windows 2000 will load needed file to the hard disk for installation purposes, when setup screen appears press the ‘Enter’ key to continue.
3. The Windows 2000 licensing agreement will appear, hit the F8 key to accept the agreement.
4. Follow the instructions to delete all existing disk partitions. The exact steps will differ based on the number and type of partitions already on the computer. Continue to delete partitions until all disk space is labeled as ‘Unpartitioned Space’; press ‘C’ to create a partition in the unpartitioned space.
5. If your server has a single disk drive, split the disk space in half to create two equally sized partitions. Delete the total space default value, type in the value of half your total disk space at the ‘Create Partition’ of size (in MB) prompt, press ‘Enter’ when complete.

6. After the New (Unformatted) partition is created, press Enter.

7. Select ‘Format the partition using NTFS file system’ and press ‘Enter’.

8. Windows 2000 setup formats the partition and then copies the files from the Windows 2000 Server installation CD to the hard drive. The computer will restart after the initial setup is complete.

9. When the machine reboot has completed, the system will begin the graphical installation of Windows 2000 Server, do not let the system boot off of the CD for this portion of the setup.

10. The ‘Welcome to Windows 2000 Setup Wizard’ appears, click ‘Next’. Windows 2000 will now automatically detect and installed system devices, this process may take several minutes to complete.

11. In the ‘Regional Settings’ dialogue box, make the changes required for your locale, and then ‘Next’ to continue.

12. In the ‘Personalize Your Software’ dialogue box, type ‘Pro-Watch’ in the name box, and type ‘NexWatch’ in the organization box, click ‘Next’ to continue.

13. Type the ‘Product Key’ (found on the back of your Windows 2000 CD case) in the text boxes provided, click ‘Next’ to continue.

14. In the ‘Licensing Mode’ dialogue box, select the appropriate licensing mode for your organization and click the ‘Next’ button.

15. In the ‘Computer Name’ dialogue box type in ‘PWSERVER’ for the Administrator password boxes, they need to remain empty.


17. In the ‘Date and Time’ dialogue box, adjust the listed time and date if needed click ‘Next’ when complete.

18. Wait while networking components are installed, this may take a few minutes.

19. In the ‘Networking Settings’ dialogue box, make sure that ‘Typical Settings’ is selected and then click ‘Next’.

20. In the ‘Workgroups or Computer Domain’ dialogue, leave the defaulted ‘No’ and click ‘Next’ to continue. The computer will be configured as a domain controller late in this process.

21. Windows 2000 Server installation continues and configures the necessary components, this will take several minutes.

22. When you have reached the ‘Completing the Windows 2000 Setup Wizard’, remove the CD from the drive and click on ‘Finish’.

23. The server will reboot causing the final files to be automatically loaded upon completion. The remaining necessary files are sourced from the hard drive.

24. When the reboot has completed, logon to Windows 2000 using the default ‘Administrator’ account, leaving the password field blank.

25. When the ‘Windows 2000 Configure Your Server’ welcome dialogue box appears, select ‘One or more Servers are already running on my network’ and click ‘Next’.

26. De-select the box stating ‘Show this screen at startup’ and close out the window.

**Installing Windows 2000 Server – Domain Server Install**

1. Insert the Windows 2000 media CD into the CD Drive and turn on the machine.

2. You may be prompted to hit any key to boot from the CD, if this message appears, hit a key on the keyboard. Windows 2000 will load needed file to the hard disk for installation purposes, when setup screen appears press the ‘Enter’ key to continue.

3. The Windows 2000 licensing agreement will appear, hit the F8 key to accept the agreement.
4. Follow the instructions to delete all existing disk partitions. The exact steps will differ based on the number and type of partitions already on the computer. Continue to delete partitions until all disk space is labeled as ‘Unpartitioned Space’; press ‘C’ to create a partition in the unpartitioned space.

5. If your server has a single disk drive, split the disk space in half to create two equally sized partitions. Delete the total space default value, type in the value of half your total disk space at the ‘Create Partition’ of size (in MB) prompt, press ‘Enter’ when complete.

6. After the New (Unformatted) partition is created, press Enter.

7. Select ‘Format the partition using NTFS file system’ and press ‘Enter’

8. Windows 2000 setup formats the partition and then copies the files from the Windows 2000 Server installation CD to the hard drive. The computer will restart after the initial setup is complete.

9. When the machine reboot has completed, the system will begin the graphical installation of Windows 2000 Server, do not let the system boot off of the CD for this portion of the setup.

10. The ‘Welcome to Windows 2000 Setup Wizard’ appears, click ‘Next’. Windows 2000 will now automatically detect and installed system devices, this process may take several minutes to complete.

11. In the ‘Regional Settings’ dialogue box, make the changes required for your locale, and then ‘Next’ to continue.

12. In the ‘Personalize Your Software’ dialogue box, type ‘Pro-Watch’ in the name box, and type ‘NexWatch’ in the organization box, click ‘Next’ to continue.

13. Type the ‘Product Key’ (found on the back of your Windows 2000 CD case) in the text boxes provided, click ‘Next’ to continue.

14. In the ‘Licensing Mode’ dialogue box, select the appropriate licensing mode for your organization and click the ‘Next’ button.

15. In the ‘Computer Name’ dialogue box type in ‘PWSERVER’ for the Administrator password boxes, they need to remain empty.

16. In the ‘Date and Time’ dialogue box, adjust the listed time and date if needed click ‘Next’ when complete.

17. When the ‘Windows 2000 Components’ dialogue box appears, click next. Wait while networking components are installed, this may take a few minutes.

18. In the ‘Networking Settings’ dialogue box, make sure that ‘Typical Settings’ is selected and then click ‘Next’.

19. In the ‘Workgroups or Computer Domain’ dialogue, leave the defaulted ‘No’ and click ‘Next’ to continue. The computer will be configured as a domain controller late in this process.

20. Windows 2000 Server installation continues and configures the necessary components, this will take several minutes.

21. When you have reached the ‘Completing the Windows 2000 Setup Wizard’, remove the CD from the drive and click on ‘Finish’.

22. The server will reboot causing the final files to be automatically loaded upon completion. The remaining necessary files are sourced from the hard drive.

**Configuring Your Server as a Domain Controller**

1. Log into Windows 2000 using the default Administrator logon (no password).

2. When the ‘Windows 2000 Configure Your Server’ page appears, select ‘One of more servers are already running on my network’.

3. From the menu listing on the left side of the screen, select ‘Active Directory’.

4. Scroll to the bottom of the Active Directory screen, and select ‘Start Active Directory Wizard’.

5. When the ‘Active Directory Installation Wizard’ appears click on ‘Next’ to begin the process.
7. On this screen select ‘Create a new domain tree’ followed again by the ‘Next’ button.
8. Select ‘Create a new forest of domain trees’, and click on the ‘Next’ key.
9. In the ‘Full DNS Name’ for a new domain box, type in ‘NexWatch’, then ‘Next’. A message box will appear stating that DNS names will typically have a .com extension. When asked if you are sure if you want to use the name “NexWatch” answer ‘Yes’.
10. When the NetBIOS Domain name dialogue appears, the default should be ‘NEXWATCH’, click ‘Next’ to accept the default value.
11. Accept the default values for on the ‘Database and Log Locations’ screen, and the ‘Shared System Volume’ screens by click on ‘Next’
12. A message stating ‘The wizard cannot contact the DNS Server that handles the name “NexWatch” to determine if it supports dynamic update. Confirm your DNS configuration, or install and configure a DNS Server on this computer.’ Click on ‘Ok’ to acknowledge this message.
13. When the ‘Configure DNS’ box appears, accept the default value ‘Yes, Install and configure DNS on this computer’. Click on ‘Next’ to begin the DNS installation.
14. On the permission screen leave the default ‘Permissions with Pre-Windows 2000 Servers’ and click on ‘Next’ to continue.
15. Leave the password boxes blank on the Administrator Password screen; click on ‘Next’ to continue.
16. On the ‘Summary Screen’; click on ‘Next’ to begin the ‘Active Directory Configuration’. This process may take several minutes, when prompted insert the Windows 2000 Server CD into the CD drive and click on ‘Ok’.
17. When the ‘Active Directory Installation Wizard’ completes; click ‘Finish’. You will be prompted to reboot the machine, remove the Windows 2000 Server CD from the drive and click on ‘Restart Now’.

Configuring Network Adapters

If your machine has a network adapter (NIC) installed and it is speaking on the network using a static IP address, this section can be skipped. This section is for users that have a network card installed and does not have it physically speaking to the network using a static IP address, or users that do not any NIC installed.

If the computer you are using does not have a physical network card a ‘Loopback Adapter’ will need to be installed. If there is an existing network card and it is speaking on the network using a DHCP address, this will need to be changed to a static IP address.

Installing a Loopback Adapter

1. To install a Loopback Adapter, right-click on the ‘My Computer’ icon located on the desktop of the computer and select ‘Properties’.
2. When the computer properties are open, go to the tab labeled ‘Hardware’, and click on the box marked ‘Hardware Wizard’.
3. When the ‘Add/Remove Hardware Wizard’ appears, click ‘Next’ to begin.
4. Select ‘Add/Troubleshoot a device’ from the ‘Choose a Hardware Task’ screen, and click ‘Next’ to continue.
5. When Windows completes its initial hardware query, the ‘Choose a Hardware Device’ dialogue box will appear. From this box, highlight the first entry (Add a new device), and click ‘Next’.
6. When the ‘Hardware Type’ dialogue screen appears, scroll down the list of hardware and highlight ‘Microsoft’ from the list of manufacturers.
7. When 'Microsoft' has been selected, the 'Microsoft Loopback Adapter' will be made available for selection on the adapter portion of the menu. Select 'Microsoft Loopback Adapter' and click on the 'Next' button.

8. Click on the 'Next' button once again when the 'Start Hardware Installation' screen and click 'Finish' when the installation complete dialogue appears.

9. Although the adapter has been installed, Microsoft defaults network properties to DHCP for addressing purposes. Please refer to the next section, ‘Assigning a Static IP Address’ for instruction on changing the address scheme.

**Assigning a Static IP Address**

1. Although a NIC may be installed, if it is configured to utilize DCHP for addressing purposes, it will need to be reconfigured for a static IP address in order for Pro-Watch to function correctly.

2. To configure a network adapter for Static IP address connectivity, right-click on the ‘My Network Places’ icon on the computers desktop and select ‘Properties’.

3. When the ‘Network and Dial-up Connections’ dialogue has been opened, right click on the adapter that needs to be changed and select ”Properties”

4. When the ‘Local Area Connections Properties’ screen appears, go to the section labeled ‘Components checked are used by this connection:’ and scroll down to ‘Internet Protocol (TCP/IP)’ and click on the ‘Properties’ button.

5. When the TCP/IP properties appear, click on the box labeled ‘Use the following IP address’.

6. Enter the IP address supplied by the customers IT department or use the NexWatch default of **192.168.100.100** when you hit tab after the last digit has been entered, the Subnet Mask value of 255.255.255.0 will automatically appear.

7. Leave the section on the DNS Server Address blank and click on ‘Ok’ to save the changes.

8. Click ‘Ok’ on the ‘Local Area Connection Properties’ page to save the record.

**Installing Windows 2000 Service Pack 2**

1. After the appropriate changes to the system have been made, log onto the system using the default Administrator logon.

2. Insert the media CD that contains the Windows 2000 Service Pack. Locate the Windows 2000 Service Pack 2 folder and execute the application (typically named w2ksp2.exe).

3. Windows will extract the necessary files and verify system information at this time. When the initial setup screen appears select both boxes I order to backup the necessary files and to accept the terms of the licensing agreement; click ‘Install’ to begin.

4. When the installation has completed, you will be prompted to restart the computer.

**Accounts and Permissions**

This section deals with assigning general operator user permissions for the operating system and database. Please check with your organizations local Information Technology Administrator prior to creating or modifying any system permissions.
Creating a Pro-Watch User Group

1. After the reboot has completed, log onto the system using the default Administrator logon.
2. To create a new user group, go to ‘Computer Management’ 
   ('\Start\Programs\Administrative Tools\Computer Management')
3. When the directory opens, expand the ‘Local Users and Groups’ icon; then click on the ‘Groups’ folder.
5. Enter ‘PW_User’ in both the ‘Group Name’ and ‘Description’ dialogue box; click on ‘Ok’ to save.
6. After the record has been saved close out the ‘Computer Management’ screen.
7. User Rights (permissions) must now be assigned to the class. To assign Rights, proceed to the ‘Local Security Policy’ (‘\Start\Programs\Administrative Tools\Local Security Policy’)
8. When the ‘Security Settings’ dialogue opens, click on the plus (+) sign next to ‘Local Policies’.
9. After the ‘Local Policies’ has been expanded, click on the ‘User Rights Assignment’.
10. A listing of user permissions should now be present on the right side of the screen, double-click on ‘Log on as a Service’.
11. Click the ‘Add’ button, and select ‘PW_User’ from the list. Highlight the group and click ‘Add’; this will bring the group to the lower portion of the screen.
12. After the group has been and is present in the lower in the lower box, click on ‘Ok’ to save the record.
13. In the ‘Local Security Policy Settings’ box for the right ‘Log on as a Service’, the assignment should state that the right is assigned to ‘PWSERVER\PW_User’.
14. Make sure that both ‘Local’ and ‘Effective’ are selected, and click ‘Ok’ to save the record.
15. On the main screen, double-click on ‘Load and Unload Device Drivers’.
16. Click the ‘Add’ button, and select ‘PW_User’ from the list. Highlight the group and click ‘Add’; this will bring the group to the lower portion of the screen.
17. After the group has been and is present in the lower in the lower box, click on ‘Ok’ to save the record.
18. In the ‘Local Security Policy Settings’ box for the right ‘Load and Unload Device Drivers’, the assignment should state that the right is assigned to ‘PWSERVER\PW_User’.
19. Make sure that both ‘Local’ and ‘Effective’ are selected, and click ‘Ok’ to save the record.
20. Click on ‘Ok’ to save the record.

Creating a Pro-Watch Administrator Account

2. To create a Pro-Watch Administrator Account right click on the ‘Users’ folder on the left side of the screen, then select ‘New User’.
3. For the ‘User Name’ type in ‘PWCE’, for the ‘Full Name’ and ‘Description’ type in ‘Pro-Watch Admin’.
4. For the ‘Password’ box, type in ‘nexwatch’ (all lower case) and confirm the entry in the confirm box.
5. Deselect the checkbox stating ‘User must change password at next logon’. Check the boxes labeled ‘User can not change password’ and ‘Password never expires’.
6. Click on ‘Create’ to save the record, and then ‘Close’ to exit the ‘Add New User’ dialogue.
7. After the user record has been created, double-click on the record and proceed to the ‘Member Of’ tab. Click on ‘Add’ and select ‘Administrators’, then click on ‘Add’. The ‘Member Of’ box should now list ‘Users’ and ‘Administrators’.
8. Click on ‘Ok’ to save the record.
Creating a Pro-Watch User Account

2. To create a Pro-Watch User Account right click on the ‘Users’ folder on the left side of the screen, then select ‘New User’.
3. Enter the ‘User Name’, ‘Full Name’, and ‘Description’ information.
4. Deselect the checkbox stating ‘User must change password at next logon’. Check the boxes labeled ‘User can not change password’ and ‘Password never expires’.
5. Click on ‘Create’ to save the user record, and then ‘Close’ to exit the ‘Add New User’ dialogue.
6. After the user record has been created, double-click on the record and proceed to the ‘Member Of’ tab. Click on ‘Add’ and select ‘PW_User’, then click on ‘Add’. The ‘Member Of’ box should now list ‘Users’ and ‘PW_User’.
7. Click on ‘Ok’ to save the record.

Database Engine

Installing Microsoft© Data Engine (MSDE)

1. Log into Windows 2000 using the PWPE account.
2. Insert the Pro-Watch Demo CD into the CD drive. Browse the contents of the disk and execute the application (Pro-Watch Demonstration Edition.exe).
3. Before the installation of MSDE can begin, the system will load the data tools MDAC. A message box stating that MDAC will need to be installed will appear, click ‘Ok’ to begin.
4. The system will automatically load configure the tools. When the installation is complete, click ‘Ok’ to allow the system to reboot.
5. When the reboot has completed, log into Windows using the PWPE account. The system will automatically bring you to the Pro-Watch welcome screen.
7. Click ‘Next’ to accept the default database directory. The system will automatically load configure the tools. When the installation is complete, click ‘Yes’ to complete the installation and allow the system to reboot.

Installing SQL Server 2000

1. Log into Windows 2000 using the newly created PWCE account.
2. Insert the SQL Server 2000 CD into the drive. The auto-start will activate the setup menu.
4. On the ‘Welcome’ screen click ‘Next’ to begin the setup.
5. The ‘Computer Name’ screen should have ‘PWSERVER’ listed as the default, accept the local computer default and click on ‘Next’.
6. On the ‘Installation Section’ screen click on ‘Next’ to accept the default ‘Create a new instance of SQL Server’.
7. Click ‘Next’ on the User Information screen to accept the defaulted ‘Pro-Watch\NEXXWATCH’ information.
8. On the ‘Licensing Agreement’ screen, click ‘Yes’ to accept the terms.
9. Enter the 25-digit CD key number located on the CD case of the SQL Server media, click ‘Next’ after entering the information.
10. On the ‘Installation Definition’ screen, click ‘Next’ to accept the defaulted ‘Server and client tools’.
11. For the ‘Instance Name’, accept the default by clicking ‘Next’
12. Select ‘Typical Installation’ for the installation type, and click ‘Next’ to proceed.
13. For the ‘Services Account’ screen, enter in the password (nexwatch) for the listed PWCE User and click on ‘Next’.
15. Click ‘Next’ on the ‘Start Copying Files’ screen to begin the installation.
16. When the installation has completed, click on the ‘Finish’ button.
17. Remove the CD from the drive and reboot the computer.

Installing SQL Server 2000 Service Pack 1

1. Log into Windows 2000 using the PWCE account.
2. Insert the media CD that contains the SQL Server 2000 Service Pack. Locate the SQL 2000 Service Pack 1 folder and execute the application (typically named sql2ksp1.exe).
3. Accept the default path and click ‘Finish’. A dialogue box stating that the directory does not exist will ask if you would like to create it; answer ‘yes’ to continue.
4. SQL will deliver the package, when this process is complete; click ‘Ok’ to continue.
5. Browse the computer and execute the service pack application (setup.bat), this file will be located in the directory created in step 3.
6. Click ‘Next’ to accept the defaults on the first two screens (Welcome and Computer Name).
7. Answer ‘Yes’ to agree to the licensing agreement terms.
8. Accept the default for the ‘Instance Name’ by clicking ‘Next’.
9. For the ‘Connecting to Server’ (Authentication Mode) screen, click ‘Next’ to continue.
10. SQL Server will now verify the files configured in the existing installation, when it has completed its evaluation; click ‘Next’ to begin copying files.
11. When the installation is complete a message stating that you should back up your master and msdb files will appear, click ‘Ok’ to acknowledge the message. Click on ‘Finish’ to complete the installation, reboot the computer.

Pro-Watch Application

Installing the Pro-Watch Database

1. Log into Windows 2000 using the PWCE account.
2. Insert the Pro-Watch Media CD into the CD drive. Browse the contents of the disk execute the application.
3. When the Pro-Watch ‘Welcome’ screen appears, select ‘Install Pro-Watch Database’ and click ‘Next’.
4. On the ‘Database Directory’ screen, click ‘Browse’ and select the path ‘\Program Files\Microsoft SQL Server\MSSQL\Data’. Do not accept the default path. Click ‘Next’ when ready to proceed.
5. On the ‘Domain Identification’ screen, enter the domain name hit the period key (.), click ‘Next’ to install the database.
6. When the database installation is complete, click on ‘Finish’ to exit to the desktop.
Installing the Pro-Watch Application

1. Log into Windows 2000 using the PWCE account.
2. Insert the Pro-Watch Media Demo CD into the CD drive. Browse the contents of the disk and execute the application.
3. When the Pro-Watch ‘Welcome’ screen appears, select ‘Install Pro-Watch’ and click ‘Next’.
4. Select ‘Server’ (the client entry will automatically be selected whenever server is selected), then click ‘Next’.
5. Accept the defaulted destination path by click ‘Next’.
6. The ‘Choose Servers’ screen will automatically default to the name of the local machine, click on ‘Next’ to continue.
7. On the ‘Service Account’ screen enter ‘PWCE’ in the ‘Administrator ID’ box, and ‘nexwatch’ in the password box. This login and password entry is used for registering the service as a startup in Windows.
8. In the box asking for the ‘User ID’ for the application, enter ‘PWCE’.
9. For the ‘Domain’ information, hot the period key (.), click on ‘Next’ to continue.
10. When the ‘Ready to Install’ screen appears, click ‘Next’ to begin the installation.
11. When the installation has completed, click ‘Finish’.
12. When prompted to reboot the machine, answer ‘Yes’.
13. Before the reboot has completed, place the security key (Dongle) on the LPT port of the computer. This Dongle is required for full service functionality. If a Dongle is not placed on the LPT port of the computer, the software will run in a ‘Demo’ mode of
This section has been design to assist Pro-Watch Users administer the key elements of the application.

This section will cover the basic concepts of Sites, Channels, Logical Devices, Clearance Codes, Badgeholders, and Cardholders.

Sites

Creating a Site

From the main application window, click on the ‘Hardware Configuration’ icon located in the viewer’s tab on the left side of the screen. Clicking this icon will open the main Hardware control window.

Pro-Watch comes preconfigured with a default Site known as ‘NexWatch, which includes a PW-5000 Channel, Panel, Reader, Input, and Output Points.

The purpose of the ‘NexWatch’ site is to support a hands-on training course and to allow a trainee to practice editing the default hardware functions at his/her facility.

**Warning**: If you have no prior experience with Pro-Watch, NEVER add sites nor edit sites, channels, panels, etc. that were configured specifically for your facility.

During the hardware configuration process you will encounter dialog boxes and settings that will require you to enter and select the correct options specific to your system. As each hardware component is configured, another level is added to the configuration list. For example, adding a Site is the first step you take to configuring the system hardware.

From this window, the ‘Hardware Tree’ will show a listing of system hardware installed. Viewing the tree the will show the template and controls of the Hardware screen on the upper most section of the tree. The ‘Site’ is identifiable as the icon, which resembles a house. An arrow should appear next to any ‘Site’ that has already been created and that has hardware associated to it.
To create a new Site, right click on the default NexWatch site, and select ‘New’, followed by ‘Site’. When the ‘Add Sites’ dialogue box screen appears, enter in a name for the ‘Site ID’. The Site ID entry cannot contain any spaces. This entry is used by SQL Server for referencing, and is not shown in the general view.

After the Site ID has been entered, enter a description for the Site. This description is what the user will physically see on the screen when this site is referenced. There are no character type restrictions on this field, with the exception of 32 characters in length.

When the description has been entered, the workstation field needs to be populated. This field represents the actual computer that the hardware in this site will use to speak to. Typically this will be the name of the server, click on the resource box next to the dialogue and click on ‘Define’. From the listing of computers in the list select the appropriate computer and click ‘OK’. If the computer you are looking for is not in this listing, you can click on the ‘Add’ button and add the computer to the list. After this field has been entered, click on the ‘OK’ button to save the record.

Modifying a Site

Making a change to an existing ‘Site’ is done in a fashion similar to that of creating a new Site. From the Hardware Configuration screen, right click on the site that needs to be modified. From the options available, select ‘Properties’ from the list, this will put the record in a modify mode. The ‘Site ID’ field will be grayed out and not available for editing. Make the changes needed to either the ‘Description’ or the ‘Workstation’ fields, and click ‘OK’ to save the changes.

**Warning**: Changing the workstation entry can result in hardware communications failure if incorrectly assigned. The system administrator should only do changes to the ‘Workstation’ field when the machine has physically been replaced or renamed.

Deleting a Site

If the situation occurs that requires a sit to be deleted from a system, make sure that all hardware and devices associated to this site are deleted. A site cannot be removed until this has occurred.

From the Hardware Configuration screen, right click on the site that needs to be deleted. From the options available, select ‘Delete’ from the list; this will prompt a verification box. Acknowledge the deletion in the verification box to completely remove the record from the system.
Creating a Channel

From the main application window, click on the ‘Hardware Configuration’ icon located in the viewer’s tab on the left side of the screen. Clicking this icon will open the main Hardware control window.

A channel is the method in which your hardware speaks to the host computer. Each site in your system can have one or more channels that the server uses to communicate with panels and other devices. You must first decide upon which site to install a new channel, create the site if it does not exist, and then configure the associated channel before you can add new panels or other hardware to the system.

Although every type of hardware device/panel (PW-5000, Star I, etc.) embeds its own communications protocol in its firmware, Pro-Watch is able to communicate with each device’s unique/proprietary communications protocol. However, because each device/panel protocol is different, each device/panel type must be configured on the same channel with other devices/panels of the same type (e.g., D600AP).

Configuring a mixture of various device/panel types (e.g., PW-5000 and D600AP) on the same Channel may cause communication failures or unexpected results with the associated devices/panels.

To create a new Channel, right click on the associated site, and select ‘New’, followed by ‘Channel’. When the ‘Create a Channel’ dialogue box screen appears, select the device you are wishing to program from the available entries in the drop down list. The items in the list are controlled by the security key used on the server and may vary from installation to installation based on the features ordered.

After the appropriate channel type has been select, the ‘Basic Channel Information’ screen will appear. On this screen a ‘Description’ will need to be given to this channel. This description will be used throughout the software, so using a naming convention that is familiar will simplify things later on in programming.

If hardware is installed, check (default) ‘Installed’ box, if hardware is not installed, uncheck box to save polling cycles until the hardware is installed.

**Warning:** If “Installed box” is unchecked, hardware installed on the channel will not communicate with server!
Click on the arrow for the Time Zone selection; select the Geographic Time Zone where the hardware on this channel will be physically located.

Accept the default of 10 in the ‘Attempts’ dialogue box. The value in the ‘Attempts’ box represents the number of times the server will try to communicate with this channel before an alarm is generated.

Accept the default of 5 in the ‘Poll Delay’ (ms) dialogue box. This value represents the number of milliseconds between each poll cycle; this value should only be changed if recommended in hardware manual.

Accept the default of 5 in the ‘Comm Break’ dialogue box. This value represents the number of poll cycles that will occur between each communication break test. A communication break is a random sequence of characters sent across the channel to test the line connecting the device and the server; this value should only be changed if recommended in hardware manual. Once these values have been verified (modified) click on the ‘Next’ button to proceed.

The ‘Channel Communication Information’ screen is where the actual method of communications to the field device gets defined. All controllers will utilize the ‘Primary’ section, where only the PW-5000 can utilize both the ‘Primary’ and ‘Secondary’ ports.

Select the ‘Port Type’ from the drop down list of available communication protocols. The standard ‘Port Types’ are as follows:

**None**—disables the channel by disabling the text boxes in the Primary section, and designating no primary channel communication settings.

**Dial In**—designates a modem port as the primary channel communication setting and enables each text box in the Primary section.

**Dial Out**—defines a modem port as the primary mode of communication for the selected channel and enables all the text boxes in the Primary section.

**Hardwired**—designates a serial port as the primary channel communication setting and enables each text box in the Primary section.

**TCP/IP**—disables the Baud, Word Size, and Flow Control boxes. Selecting this option also adds an IP Address text field to the Primary section, into which you enter the IP address that is assigned to the network interface device for the channel.

**Modem Pool**—designates a bank of modems as the primary channel communication setting. Choosing this option disables the Baud, Word Size, and Flow Control boxes. This option also adds the Modem Pool text field to the dialog box, from which you select the
corresponding browse button and click **Define**. The system then opens the Modem Pools dialog box. Select an available modem pool and click **OK**.

When the appropriate port type has been identified, continue entering the associated information for that port. When complete, click on ‘Next’ to continue. Continue clicking ‘Next’ throughout the ‘Channel Dialup’ and ‘Partitions’ screen. After the ‘Partitions’ screen, the channel will be complete.

### Modifying a Channel

Making a change to an existing ‘Channel’ is done in a fashion similar to that of creating a new Channel. From the Hardware Configuration screen, right click on the channel that needs to be modified. From the options available, select ‘Properties’ from the list, this will put the record in a modify mode. All fields in the ‘Channel’ screen can be modified. Make the changes needed and click ‘OK’ to save the changes.

### Deleting a Channel

If the situation occurs that requires a Channel to be deleted from a system, make sure that all hardware and devices associated to this channel are deleted. A channel cannot be removed until this has occurred. If attempting to delete a Channel and a warning appears stating that it is in use, verify that the channel is not in an existing ‘Routing Group’, or associated to and ‘Host Level Procedures’.

From the Hardware Configuration screen, right click on the Channel that needs to be deleted. From the options available, select ‘Delete’ from the list; this will prompt a verification box. Acknowledge the deletion in the verification box to completely remove the record from the system.

### PW-5000 Panels

#### Creating a PW-5000 Panel

To create a new Panel proceed to the Hardware Configuration screen, and right-click the site that will include the new PW-5000 panel. Right click on the newly created channel and click ‘New’, and select ‘Panel’. From the Select a Panel dialog box, choose the channel that this new panel will be based off of in the Channel dialog box. Click ‘OK’ to save your settings and to open the Add Panel dialog box.

The first ‘Add Panel’ dialogue box that will appear will allow for the panel selection. The default will be PW-5000, but the PW-3000 can be selected by scrolling the drop down menu.

After selecting the correct controller type (we will use the PW-5000 for this example), click on the ‘OK’ button to proceed to the second ‘Add Panel’ dialogue box.

The next ‘Add Panel’ box that appears will be used for
the panel address and selection of the downstream modules. The downstream modules off of a PW-5000 controller include the following:

- PW-2000-II series controllers, both standard and expanded relay
- PW-2000-III/IV series controllers, both standard and expanded relay
- PW-5000 Single Reader Module
- PW-5000 Dual Reader Module
- PW-5000 16 Input Module
- PW-5000 16 Output Module

The ‘Panel Address’ box is a drop down list used to signify the physical address on the PW_5000 controller. The dialogue boxes next to the downstream devices (defaulted at zero (0)) represent the number of downstream devices that are present on this controller.

Selecting ‘Auto-assign IO Module Addresses’ will cause the system to automatically give each IO module its own address. Then, click Add for the system to briefly display the Add Panel Progress dialog box in which the system monitors the loading of the associated IO modules, inputs, outputs, readers, and events.

Not selecting Auto-assign IO Module Addresses will not automatically assign the address scheme to the downstream devices. A new dialogue box will appear asking for the addresses of the devices. Clicking the IO address box next to each IO module and selecting the correct address do assigning the addresses. When complete click ‘OK’. The system briefly displays the Add Panel Progress dialog box in which the system monitors the loading of the associated IO modules, inputs, outputs, readers, and events. After these points have been created, the system opens the ‘Edit PW-5000’ dialogue box.

The ‘Description’ dialogue box is used to assign a name that will be represented throughout the application. Use a unique name that easily is identifiable, as most systems will utilize several controllers. For the ‘Location’ dialogue box enter where
the panel is physically located at your facility. The ‘Memory’ dialogue box is used to select how many megabytes of RAM the new panel contains. This value is dependant as to the amount of RAM physically on the controller.

The ‘Total Cards’ dialogue box is the total amount of different types of ID badges the panel will contain. This value can be increased with additional RAM. The ‘Poll Delay’ dialogue box is used to identify the time delay between polling cycles. This value is based in milliseconds.

The ‘Reply’ dialogue box allows the user to alter the time (ms) that the panel will have to reply to the server after a poll cycle. The ‘Offline’ dialogue box denotes the amount of milliseconds the panel will have to remain off-line until the next poll.

The ‘Pin Length’ dialogue box is designed for systems that will utilize a reader in conjunction with a keypad. The PIN value is defaulted at 0 and can be up to 8 indicating how many characters are included in each Personal Identification Number that the panel recognizes.

Similar in logic to that of the ‘Total Cards’, the ‘Transactions’ dialogue box is used to enter a value that represents the total number of history transactions that can be stored in memory. This value will be dependant on the amount of RAM that the controller contains.

The lower half of the main panel screen contains a series of check boxes, these boxes are defined as follows:

- **Installed**—choose this option if the panel is currently installed in the system.
- **Stored Event Level**—click this option if the panel will store event levels.
- **2 Wire 485**—click this option to designate the panel is connected to the host using a 2 wire 485 communication.
- **Use Issue Codes**—choose this option if the panel will recognize issue codes.
- **Timed Anti-Passback**—select this option if the panel contains readers that refuse access to cards used to gain entrance a second time within a specified period and after a valid card read.
- **Anti-Passback Locations**—select this option if the panel contains an in/out reader that the cardholder must swipe in sequence in order to enter and exit a secure area.

When the appropriate controller selections have been made, click ‘OK’ to save the panel, or select another programming tab to program, Time zones, Holidays, and Card Formats.
Star 1 Controllers

Creating a Star 1 Panel

To create a new Panel proceed to the Hardware Configuration screen, and right-click the site that will include the new Star 1 panel. Right click on the newly created channel and click ‘New’, and select ‘Panel’. From the Select a Panel dialog box, choose the channel that this new panel will be based off of in the Channel dialog box. Click ‘OK’ to save your settings and to open the Add Panel dialog box.

The first ‘Add Panel’ dialogue box that will appear will allow for the panel selection. The Default will be 804S, the Star 1 can be selected by scrolling the drop down menu.

After selecting the correct controller type, click on the ‘OK’ button to proceed to the second proceed to the ‘Add Star 1 Panel’ dialogue box.

When the ‘Add Star 1 Panel’ dialogue box appears, the ‘Description’ dialogue box is used to assign a name that will be represented throughout the application. Use a unique name that easily is identifiable, as most systems will utilize several controllers. For the ‘Location’ dialogue box enter where the panel is physically located at your facility.

Modify the data on these tabs as needed. Please note that all 'Reports' are defaulted as ‘Default Send Host Report’. When the appropriate selections have been made, click 'OK' to save the panel, or select another tab to program Time Zones, Holidays, Reports, or Site Codes.
More Panel Settings Tab

Click to check (enable) or uncheck (disable) **Duress Enabled**

Systems with Keypads have the ability to generate a special Duress Report if a Cardholder is being forced to enter through a door with a Keypad. The Cardholder will enter a “Shifted” version of their PIN Number to cause the Duress. The altered PIN will have the first digit moved to the last position. For example, if the regular PIN is 12345, the Duress version is 23451. Typically, a special Report will be created for Duress. It might actuate a strobe light at the Guard post or some other unique alerting device.

If Keypads are being used WITH Readers, then the system can be set to use 4, 5 or 6 digit PIN Numbers. With Star I controllers, each Cardholder may choose their own PIN #. In addition, the controller can generate a table of PIN numbers to be assigned to the Cardholders. Anyone who chooses their own PIN will be skipped by the PIN generator.

If Keypads are being used WITHOUT Readers, then the system can be set to use 4, 5, 6, 7 or 8 digit PIN Numbers. Since there are no Readers, there are obviously no Cards. In this case, each person will choose a unique PIN number of the specified length. This number will be entered in the Cardholder command as if it were a Card Number.

A Keypad automatically allows ONE attempt to enter a correct PIN number. Retries are ADDITIONAL attempts to get a correct PIN entry. NOTE: If you intend to use Keypads to set Building Mode changes, Retries MUST be set to 1 or greater.

The Grace Period is the number of seconds that a Cardholder has to complete the required Access Sequence. This will include one or more PIN attempts PLUS a card read if a reader is included.

The PIN Seed is used when the controller is generating the PIN Numbers. It applies only to applications with a Keypad PLUS a reader. An internal algorithm calculates each Cardholder’s PIN based on the actual Card number AND the PIN seed. If you change the PIN seed, the controller will recompile all PIN numbers (except those that have been selected by the Cardholders). This is typically used in applications where a relatively small number of people use PINs that must be changed every 30 days or so. The System Administrator will change the Seed, print out the new PINs and assign them to the Cardholders.
The vast majority of existing 4100 Family controllers should be set to Native SE 4100. A very small number of existing installations will have 4100 controllers emulating 818SC units for the sake of uniformity.

Verification Sweeps default values are fixed and should not be changed unless you are instructed to do so by NexWatch Tech Support or Engineering personnel.

If you have selected a “Building Should Be Closed” Time Zone above, this value is the interval that the ACU will wait before repeating a “Building Should Be Closed” message to the operator(s). The message will continue to be repeated at the specified interval until either the ACU is placed in the Closed Mode, or the Time Zone expires.

Select an Output Relay to be used to power a visual indicator that the controller is in the LIMITED Mode.

The vast majority of existing 4100 Family controllers should be set to Native SE 4100. A very small number of existing installations will have 4100 controllers emulating 818SC units for the sake of uniformity.

Verification Sweeps default values are fixed and should not be changed unless you are instructed to do so by NexWatch Tech Support or Engineering personnel.
Clearance Codes

Creating Clearance Codes

From the main application window, click on the ‘Database Configuration’ icon located in the viewer's tab on the left side of the screen. Clicking this icon will open the main database control window.

From this window, select ‘Clearance Code’ icon. The listing of available databases should be listed in alphabetical order for convenience.

Once the ‘Clearance Code’ icon has been selected, a list of existing clearance codes should appear on the right hand portion of the screen.

Right-click anywhere on the right side of the screen and select ‘New Clearance Code’.

The ‘Add New Clearance Code’ dialogue box should appear. Enter a description in the dialogue box, this entry will serve as the name used to identify the clearance code. The ‘Default Time Zone’ box will require a defaulted timezone entry. Click on the icon next to this box and browse the listing of existing Time Zones in the database.

The checkbox labeled ‘Use Elevators’ should only be selected when using the elevator control module with the PW-5000 series controllers.

When ready to assign access, click on the ‘Logical Device’ tab. This screen allows the programming of logical devices for access and the time schedule for valid access.

Clicking on the ‘Add’ button on the right hand side of the screen will produce a list of configured logical devices. From the listing of logical devices, select the appropriate devices that this clearance code will have access privileges for. A dialogue box will appear asking when the clearance code should be active from. The timezones listed in this dialogue are pulled directly from the controller programming. If the timezone required is not listed in this selection, you will need to add it to the controller.

When all appropriate logical devices have been assigned to the clearance code, click on the ‘OK’ button to save the clearance code into the database.
Modifying a Clearance Code

If the need to alter the structure of an existing clearance code becomes necessary, it can be done quickly and easily. Follow the steps listed above in order to access the clearance code database.

When the listing of programmed clearance codes is viewable on the right hand side of the screen, double-click on the clearance code that requires modification. Alter the data as needed. Logical devices can be added, removed, and timezones can be adjusted to fit the needs of the system. When complete with the modifications, click on the ‘OK’ button to save the changes.

If the clearance code that has been modified has valid cards assigned to it, a dialogue box will appear asking the user how to download the changes. Depending on the needs of the system, several options are available for downloading. The changes can be downloaded immediately by selecting the ‘Download Now’ button. If there is no need to download the changes the ‘Never Download’ button should be selected (this option should be used when connecting to field controllers via dial-up modem). If the download should occur at a specific time, the user can program the time and date for the download to occur by selecting the ‘Download Later’ option. When the required method of downloading has been selected, click on the ‘OK’ button to continue.

Deleting a Clearance Code

If the need to delete an existing clearance code exists, follow the steps listed above to access the clearance code database. Locate the clearance code that is to be removed from the listing on the right hand side of the screen. Right-click on the clearance code and select ‘Delete’.

If a warning dialogue box appears stating that the clearance code is in use, that means that the clearance code is currently assigned to a cardholder record. Either the cardholder record or the clearance code on the record needs to be removed.

When the record is available for removal, a confirmation box will appear after the ‘Delete’ option is selected on the clearance code. Confirm the removal by click on the ‘Yes’ button.
Creating a New Badge Record

From the main application window, click on the ‘Badging’ icon located in the viewer’s tab on the left side of the screen. Clicking this icon will open either the main badge control window, or a select badge profile screen. If the select badge profile screen appears, this option will allow the user to select which badge profile to view. Select the appropriate view and click ‘OK’.

When the selected view is available, the badge operations are defaulted into a ‘Info Mode’, this mode allows for read-only operation of the badgeholder database.

When there is a need to create a new badge record, click on the ‘New Badge’ icon on the upper toolbar of the badge module. Clicking on this icon will open the ‘New Badge dialogue box. This box will require that the Last and First name of the user be entered in order for this record to be created. In addition to the first and last name entries, the user has the ability to enter in the users middle initial, badge issue date, badge expiration date, and the badge type that this user will have assigned. The badge type is the layout of the data including photo used in the imaging process of credential printing.

After the initial data has been entered into the dialogue box, the information will be populated into the badge profile that has been defaulted for the profile. The information required can be any selection of fields, and images as defined in the badge profile.

When the record information entry has been completed, the record can be saved by either saving the individual record, or by creating another new record. In order to save the individual record, click on the ‘Modify Badge’ icon located on the upper toolbar of the badging module. This will prompt the user to save the badge and will revert the badge module into the ‘Info Mode’.

Modifying a Badge Record

If the need to alter an existing badge record, it can be done in a manner similar to that of creation. Click on the ‘Badging’ icon located in the viewer’s tab on the left side of the screen. Clicking this icon will open either the main badge control window, or a select badge profile screen. If the select badge profile screen appears, this option will allow the user to select which badge profile to view. Select the appropriate view and click ‘OK’.

When the selected view is available, the badge operations are defaulted into a ‘Info Mode’, this mode allows for read-only operation of the badgeholder database. Locate the badge that needs to be modified, and click on the ‘Modify Badge’ icon on the upper toolbar of the
module. This will open the individual record, and allow for the required changes to be made.

When all required modifications have been completed, again click on the ‘Modify Badge’ icon and acknowledge the badge record to be saved.

Deleting a Badge Record

If the need to delete an existing badge record, it can be done from the main toolbar in the badging module. From the toolbar in the upper section of the module, select the ‘Delete’ icon. When the delete confirmation box appears, confirm the deletion. The record will be removed from the database, and the badge module will return to the ‘Info Mode’.

Card Records

Adding and Assigning Card Access

One a new Badge Record has been created, a card record can be assigned to the record. Please note that a card cannot be added unless the record is in the ‘Modify Mode’.

Click on the ‘White Section’ on the lower portion of the module, the card number needs to be entered into the ‘Card Number’ dialogue box. This is a required field, as no access privileges can be assigned without the card number.

In addition to the card number, the ‘Company’ field needs to be applied as well. From the resource box next to the Company box, select a company to assign the card record to.

When a company has been assigned, the ability to add a clearance code will be made available. Click on the ‘Clearance Code’ tab from the badge menu. If a clearance code is already listed in the listing of assigned clearance codes, this is because the permissions have been assigned to the company assigned to the card.

If the clearance codes listed are not appropriate additional clearance privileges can be added to the users permissions by clicking on the ‘Add’ button on the right side of the screen. A dialogue of predefined clearance codes will be listed, select the appropriate clearance code and click ‘OK’ to register the clearance code.

When ready to save the record, click on save icon on the upper toolbar. The save icon will be the diskette icon. When the record has been saved, the record can be immediately sent to the appropriate controllers by clicking on the newly illuminated ‘Download’ icon. When ready to close the record, click on the close icon (diskette with a green arrow).

The record should now be saved with the badge record.
Access Control Glossary

**Access Point** - Point of entry or exit (e.g., door or gate) that can be controlled by the Pro-Watch system via the host computer and its peripheral devices.

**ADA Held Time** - The number of seconds a door is held open after a card read. This is an extended time in addition to the standard “held” time.

**ADA Strike Time** - The number of seconds the door strike is energized after a card read. This is an extended time in addition to the standard "strike" time.

**Alarm** - The activation of an alarm device that causes a message to be sent to the alarm monitor, which displays the alarm information and then creates the alarm monitor terminal to beep. An open switch causes alarms. Alarms, for example, can occur as a result of a forced entry into an access point or a door being held open beyond its shunt time.

**Alarm Input** - The physical connection of an alarm circuit to the interface panel controller.

**Alarm Time** - This is how long (in minutes) the failed attempts at connection will occur before an alarm is generated.

**Alarm Monitor** - The user interface in the Pro-Watch system that monitors activated alarms and allows them to be acted upon.

**Alarm Priority** - Alarm priority level; the lower the number, the higher the priority.

**AMT** - Alarm Monitor Terminal. This type of terminal is equipped to monitor input points only.

**Annunciate** - The system to sounds the alarm (with visual alarm notification) on the alarm monitor whenever the alarm on a designated piece of hardware occurs.

**Anti-Passback Reader** - A reader that will refuse access to cards which attempt access for a second time within a specified period of time after a valid card read.

**Area** - Refers to a secure area for which you define the related “in readers” and “out readers”.

**Arm** - Enable, to make a Pro-Watch system function usable.

**Attempts** - The amount of times the channel will try to connect to the system before an alarm is generated. The system default is ten attempts.

**Auto Clear** - When you want the system to clear the selected event type from the alarm monitor after the user has acknowledged the event and the event status has returned to normal.

**AVI File** - Audio Video Interleave. This is a file format for storing audio and video information.
**B**

**Badge Profile** - These relate to the internal badging system. When determining these you specify which users can view Access, Partition, and Brass Keys page, as well as which fields will appear on the profile pages.

**Badge Ranges** - When you set a range of badges in the Pro-Watch system, you determine the first and last number in a range for use with a particular badge field, on your profile pages.

**Badge Type** - This is a type of badge. When you create a badge type you set the name of a badge type, as well as the front and back badge layouts.

**Baud** - This is the baud rate reflecting the maximum number of changes occurring per second in the electrical state of the communications circuit.

**Bi-directional** - Bi-directional card reading (i.e., backward and forward card swipes).

**Blob Types** - These are commonly known as Binary Large Objects, which are a collection of binary data stored as a single entities in a database management system such as Pro-Watch.

**Brass Keys** - Brass keys are facility keys that can be issued to a badge holder. Pro-Watch allows you add these using the Brass Keys options within the Database Configuration window and the Badging window.

**C**

**Card Event** - An action that the panel is programmed to execute after a valid access is registered at a door. Specifically reading a card into a card reader triggers this event.

**Card Formats** - These define system card formats and must be configured prior to adding badge holders to the system.

**Channel** - A communication path or link to system hardware including communication parameters, events, and partitions.

**Class** - A group of users that is defined to possess the same access privileges of the system software and hardware within the facility. Classes are configured through a series of dialog boxes and property sheets, all of which are accessed from the Edit Classes dialog box.

**Clearance Code** - Defining clearance codes establishes which Groups of logical devices will grant or deny access to certain badge holders.

**Closed-Supervised** - An input point that is normally closed and is in a forced state; designates the panel to report electrical trouble alarms on the input.

**Closed-Unsupervised** - Input type that is normally closed and designates the panel not to report electrical trouble alarms on the input.

**Comm Break** - The number of polling cycles that will occur between each Comm break test. A Comm break is a random sequence of characters sent across the channel to test the line connecting the device and the server. The system default is five poll cycles.

**Com Port** - This is the communications port (or serial port) to which the channel is connected.
Database Tables - Use these options to define which database tables are partitionable. Because partitioning uses more resources than not partitioning, it is helpful to define the tables that you do not want to partition.

Debounce - A numerical value that represents the period of time (in tenths of a second) the input point must remain in alarm before an alarm message is sent.

De-energize - A relay that is not in a active state.

Default Events - These connect an event type from a selected device to the alarm monitor. When you configure these, you actually configure the alarm and its return to a normal status.

Dial In - This is a communication parameter option that designates a modem port as the primary channel communication setting.

Dial Out - This is a communication parameter option that defines a modem port as the primary mode of communication for the selected channel.

Duress - A state in which a badge holder is forced to provide unauthorized entry into a secured area at the facility.

Duress Alarm - An alarm that is functional with keypad card readers; a duress alarm is activated by a badge holder by pressing the digit “9” in place of one of the PIN digits when entering the normal PIN code into the card reader.

Energize - A relay that is in a active state.

Enrollment and De-enrollment Devices - Enrollment and de-enrollment readers are used at sites where you want to force people to enter and exit through a particular point and allow only so much time inside. If you swipe your card at the de-enrollment reader before the time is up, your access is removed.

Entry Delay - The amount of seconds after a valid card swipe that the green access light is on, during which access can be made.

Event Procedure - An event procedure is an order to execute a command. For example, you can assign an event procedure to a specific class and user once configured.

Event Trigger - This option allows you to specify what events are used to trigger event procedures, as well as determine which event procedures will occur once a trigger happens.

Event Type - Use this option to configure the types of alarms in your system. Event types include relevant information, visual and audio display settings, and associated partitions.

Executive Privilege - Allows the card to obtain a valid access at any reader on the panel, and also allows the card to obtain a valid access regardless of any other privileges assigned to the card or any time zones assigned to any readers on the panel.
**Exit Delay** - The amount of seconds after a valid card swipe. This option represents how long the cardholder has to exit from a secure area through an open door.

**Extended H. Time** - The extra amount of time, in seconds, the system will allow the access door to be held open before an alarm occurs.

**Extended S. Time** - The extended card strike time in seconds.

**F**

**Fast Poll** - The server updates the status of the hardware on the channel as fast as it can. This option is not recommended for CCTV channels, but good for busy card access channels.

**Firmware Revision** - Refers to information related to the panel's own software.

**Freeze** - AutoCAD term indicating layers in a drawing that is to be hidden from view.

**G**

**Global Shunt** - This causes the system to shut down all events of a certain event type when they occur. Then, override any individual alarm shunt status. This option also prevents any events of this type from displaying in the alarm monitor.

**Groups of Logical Devices** - This Pro-Watch feature allows a group logical devices to categorize similar alarms. These Groups can be acted upon as a single device.

**H**

**Hardwired** - This communication parameter option designates a serial port as the primary channel communication setting.

**Has Returns** - Indicates an alarm has a corresponding “return to normal” event.

**Held Time** - The amount of time in seconds the system will allow the access door to be held open before an alarm occurs.

**Holiday** - This option in Pro-Watch allows you to define specific holiday information used with specific timezones.

**I**

**Input Point** - Electrical contacts that open and close when there is a changed in the system. Input points are always designated as odd numbers. Input points consist of two types: a) 2-state (on/off) and b) 4-state (on/off/open/short).

**Interface Panel Controller** - The physical device for controlling the behavior of the interface panels.

**Interface Panel** - The physical device for controlling access through an access point or connecting an alarm input or connecting a digital output. There are three types of interface panels.
that can be defined in the system; STI's (Smart Terminal Interface), AMT's (Alarm Monitor Terminal, and OCT's (Output Control Terminal).

**L**

**Latching Type** - The type of latching mechanism of the monitored door.

**LED Mode** - Light-emitting diode. A semiconductor device that converts electrical energy into light. For example, on a reader.

**Local Relay** - The communication occurring between the doors (interface panels) and the interface panel controller (panel).

**Loop** - An optical fiber or wire network by which each panel is connected to other panels and communicates with the host.

**M**

**Mask During Timezone** - Determines when the input point is disabled during a designated time; thus, disabling alarm from this input point.

**Mask Forced Open** - A time zone when force open door alarm is suppressed.

**Mask Held Open** - A time zone when the held open door alarm is suppressed.

**Modem Pool** - Modem pools are banks of identical modems from which the system chooses to dial out to a remote panel.

**O**

**OCT** - Output Control Terminal. A type of interface panel which contains relays that can turn on or off field equipment via instructions received from the main server or a user in the system.

**Offline** - The number of milliseconds the panel will have to remain off-line until the next poll.

**Open-Supervised** - Input point that is normally open, in a forced state; designates the panel to report electrical trouble alarms on this input.

**Open-Unsupervised** - Input point that is normally open; designates the panel not to report electrical trouble alarms on this input.

**Output Control Group** - A numbered group of output points that can be activated when the status of an input point (assigned to the output group) changes.

**Output Point** - Contact point on the interface panel controller that can be opened or closed by the system to turn something on or off. These are always numbered sequentially.

**Override** - Used in relation to card readers and doors; a door that is overridden is unlocked, the reader shows a valid access (green light), and an “access granted” condition is enabled.
Panel - A system panel is a small computer that must control readers, input points, output points, and subpanels. Each panel manages a database of cards, as well as registers all interface panel alarms and card transactions. This information is sent via a loop to the main server. Each system panel is capable of maintaining security even when communication with the main server is lost.

Panel Download - This process involves downloading panel parameters and card information from the server. Anytime you add hardware to the system during setup, you can automatically download all panel information on a channel. Furthermore, individual card information is automatically updated every time a card is updated or added to the system. Panel configuration is automatically downloaded when panel information also is updated.

Partitions - Partitioning the database restricts the information your classes and individual users can view.

Pathways - Pathways allow a badge holder to have a clear path through a building without setting off alarms.

PIN - Personal Identification Number.

PIN Suppression - A time zone during which the cardholder does not need a Personal Identification Number to gain access.

Poll Delay - The number of milliseconds between each poll cycle. The system default is five milliseconds.

Polling - Sending of information from one device to another that indicates or determines the status of the device.

Precision Access - Instructs the panel to not use downloadable access levels.

PTZ - Refers to Pan/Tilt/Zoom cameras.

Pulse Time (sec) - The amount of time (in seconds) that the output will remain activated when pulsed.

Reader - An electric device that absorbs information from an input/output device.

Real Time - Data processing concerning events occurring in current time.

Redundant - Having a forward and reverse channel.

Re-enable - Return to normal operation; in reference to doors, reverses the effect of a “Lock” or “Unlock” command, and returns the doors to normal operation.

Refresh - Update, as in update a file or report.

Relay - An electrically operated device that is activated by a change in conditions in an electrical circuit and which may actuate other devices in the same or another electric circuit.

Reply - The number of milliseconds the panel will have to reply to the server after being polled.
Retry Time - How many poll requests must fail before the system will register the panel as 
“down”.

Return to Normal - The Return to Normal status advises the operator that an alarm condition no 
longer exists, but a horn may still be sounding and the security in an area may be still 
compromised. An alarm may return to a normal state before it is acknowledged and may be 
cleared before it has returned to a normal status. The ability to clear alarms that have not 
returned to normal is a privilege that may be granted to or revoked from users. Alarms that return 
to a normal status (for example, a door that was forced open then later closed) will appear as an 
icon on the alarm monitor in a specific “return to normal” color.

REX - Request to Exit.

Routing Groups - These are paths through which event types must travel before the system 
displays them on the designated alarm monitor. They also control who, what, where, and when 
alarms and events display on the alarm monitor.

RTN Separate Alarm - To treat the designated event type’s “return to normal” status as a 
separate alarm.

Secured Access Area - An area in the facility protected by a door (or gate) that may only be 
opened by use of a card or by a PIN number and card combination.

Server - The host computer. The host computer is the computer that maintains the Pro-Watch 
database.

Shadow Login - This option hides the login identity of a user.

Shunt Point - Prevents the notification of a selected event to anyone viewing an alarm monitor or 
alarm viewer. However, selecting this option does not prevent the event from being logged into 
the database.

Shunt Time - The length of time a door open alarm is suppressed (shunted) after a valid card 
access request. Enough shunt time should be set to allow the cardholder to open the door or 
gate, pass through the doorway, and close the door.

Shunt - Disable; to make a function of Pro-Watch unusable.

STI - Smart Terminal Interface. This type of terminal interfaces with one of a wide selection of 
card readers. In a system like Pro-Watch, STI's are set up to maintain a relay used to unlock the 
door adjacent to the card reader. The STI interfaces to and receives it's access control 
instructions from the host computer, and has the ability to make access control decisions based 
on valid card access requests should communications be lost with the host computer.

Strike Time - The correct amount of seconds for a card strike.

Subpanel - A device that is connected to a panel; used to control system hardware such as 
readers, inputs, and outputs.

System Administrator - The system administrator is a user who maintains full privileges to all
applications that are part of the Pro-Watch system. This person is familiar with the hardware components that make up the security system at the facility, as well as the software that controls it. The system administrator also is responsible for assigning passwords and privileges to users within the Pro-Watch system.

TCP/IP - This communication parameter option disables the Baud, Word Size, and Flow Control boxes within the Communications Parameters dialog box. Selecting this option also adds an IP Address text field to the Primary section, into which you enter the IP address that a modem dials to contact the main server.

Thaw - AutoCAD terminology that indicates the layers in a drawing to be included for viewing and editing.

Timezones - The system uses start and stop times for scheduling a number of program functions during specific days of the week and holidays. These affect such system features as clearance codes, company codes, and logical devices.

Timed Override - A period of time during which a door is unlocked and the green lamp on the card reader is on, indicating an “access granted” condition.

Transaction - A transaction is an event that occurs as a result of a card access attempt or a timed override being issued for an interface panel in the system. Transactions are recorded in the real-time Transaction History log.

Trigger - An input or condition that initiates a set response (i.e., output or action). In a database, an action that causes a procedure to be carried out automatically when a user attempts to modify data. A trigger can instruct the database system to take a specific action, depending on the particular change attempted. Incorrect, unwanted, or unauthorized changes can thereby be prevented, helping to maintain the integrity in the database.

Two Card Control - Requires two valid consecutive cardholders to gain entry through an access door.

Two Person Rule - This rule requires two valid code entries to obtain access into a secured area.

User - A person who is allowed access to the Pro-Watch system's database. A User ID identifies users in the Pro-Watch system. The system administrator assigns the User ID and a password.

V

Vmin - The minimum number of bytes in a message.

Vtime - The time the system will wait for a message.

WAV File - Sound file stored in waveform (WAV) audio format.