WIN-PAK SE/PE

The Complete Access Control Software

User's Guide

User Non-Disclosure and License Agreement

Important: This Agreement must be read before proceeding with any Honeywell Access Systems software. By installing this software you agree to the terms of this Agreement.

Important: This software is a proprietary product of Honeywell Access Systems. It is protected by copyright and trade secret laws. It is licensed [not sold] for use on a single computer system, and is licensed only on the condition that you agree to this User Non-Disclosure and License Agreement.

Please Read This Agreement Carefully.

If you do not agree to the terms contained in this Agreement, please return the sealed software **unopened** to your supplier, along with any associated manuals and/or other documentation. If you agree to the terms contained in this Agreement, proceed with the installation and registration of the software online at www.honeywellaccess.com or by calling (414) 766-1700 between 8:00 a.m. and 5:00 p.m. (CST).

In consideration of and upon receipt of payment of a license fee by you, Honeywell Access Systems grants to you a non-exclusive license to use this software and any associated manuals and/or other documentation furnished herewith (together referred to herein as "SOFTWARE") under the following terms and conditions.

Should you elect not to assume the obligations of this agreement, **do not break the seal on the SOFTWARE**. Return the SOFTWARE and any associated manuals and/or other documentation to the supplier for refund or credit. If you are unsuccessful in obtaining a refund or credit, please contact Honeywell Access Systems at 135 West Forest Hill Avenue, Oak Creek, WI 53154. **No refund or credit will be given on any SOFTWARE package on which the SOFTWARE seal has been broken.**

You shall not provide or disclose or otherwise make available the SOFTWARE or any portion thereof in any form to any third party. You shall be obligated to retain in confidence the SOFTWARE, except for any published user manual(s) you may have received from Honeywell Access Systems and except for SOFTWARE information which is publicly known, or lawfully received from a third party, or known by you prior to the date you received the SOFTWARE.

You shall not have the right to print, copy or reproduce, in whole, in part, or in any form whatsoever, the SOFTWARE, except that

two copies of the media may be made, in machine-readable form, for use by you for backup and/or archiving purposes on a single computer system. You may not transfer the SOFTWARE electronically from one computer to another or over a network.

You agree not to decompile, disassemble or otherwise reverse engineer the SOFTWARE. You may not modify the programs in any way without the prior written consent of Honeywell Access Systems.

The manuals and other documentation may not be copied for any purpose. The SOFTWARE may be removed from one computer system and transferred to a backup system, but shall not under any circumstances be used concurrently on more than one computer system, unless otherwise licensed to do so.

You agree to maintain full and complete records of the number and location of any such copies of the SOFTWARE which have been generated, and to reproduce on any such copies any and all copyright notices and other markings and notices present on the originals.

From time to time as they become available, Honeywell Access Systems may notify you of any enhancements or updates released by Honeywell Access Systems for SOFTWARE licensed hereunder. Any such updates offered would be subject to standard Honeywell Access Systems terms and charges if any. **Only registered licensees will be offered any such updates.** The license of the SOFTWARE provided by this Agreement shall not be assignable or otherwise transferable by you, except that, if you are a legally constituted organization, you may transfer the license as part of a transfer of your entire business or assets, or that portion of your business or assets to which the license of the SOFTWARE pertains.

NOTICE: This SOFTWARE is licensed [not sold]. It is licensed to licensees, including end-users, without either express or implied warranties of any kind on an "as is" basis. Honeywell Access Systems makes no express or implied warranties to licensees, including end-users, with regard to this SOFTWARE, including merchantability, fitness for any purpose or non-infringement of patents, copyrights, or other proprietary rights of others.

Honeywell Access Systems shall not have any liability or responsibility to licensees, including end-users, for damages of any kind, including special, indirect or consequential damages, arising out of or resulting from any programs, services or materials made available hereunder or the use or modification thereof.

NOTICE: Honeywell Access Systems makes no claim or warranty with respect to the fitness of any product or SOFTWARE for a specific application and assumes no responsibility for installation. This warranty is in lieu of all other warranties, express or implied. No representative or agent of Honeywell Access Systems may make any other claims to the fitness of any product for any application.

So long as the SOFTWARE licensed hereunder remains a part of Honeywell Access Systems, Honeywell intends to issue periodic enhancements and updates which will include corrections of programming errors discovered or brought to Honeywell's attention. However, Honeywell shall not be obligated to issue such enhancements or updates on any particular schedule.

NOTICE: The SOFTWARE contained herein is licensed as a "service only" for no particular application. It is not to be considered or construed as a "good" for product definition within the meaning of the uniform commercial code and applicable state law. Honeywell Access Systems makes no commitment to continue producing this or any other compatible SOFTWARE, nor makes any commitment as to marketing the SOFTWARE in any given territory.

NOTICE: This license Agreement is for Honeywell Access Systems SOFTWARE and/or documentation only. The SOFTWARE requires that the user obtain (either from Honeywell Access Systems or another supplier) additional SOFTWARE such as but not limited to operating systems and/or system utilities, compilers or computer languages. It will be the user's obligation to complete and register any other SOFTWARE agreements as required by the manufacturer. Honeywell Access Systems assumes no responsibility for any other manufacturer's SOFTWARE.

CONTENTS

About this Guide

Chapter 1 Introduction

Chapter 2 Installation

Chapter 3 User Interface

Chapter 4 Getting Started

Chapter 5 System Settings

Chapter 6 Quick Configuration

Chapter 7 Badge Layout

Chapter 8 Card Holders

Chapter 9 Time Management

Chapter 10 Device Map

Chapter 11 Defining Areas

Chapter 12 Floor Plan

Chapter 13 Command File

Chapter 14 Guard Tour

Chapter 15 Monitoring Actions

Chapter 16 Translation

Chapter 17 Reports

LIST OF TABLES

Chapter 8 Card Holders

Chapter 9 Time Management

Chapter 10 Device Map

Chapter 16 Translation

Chapter 17 Reports

Chapter 18 Appendix

About this Guide

Scope

The WIN-PAK User's Guide helps you in installing, configuring, and using the WIN-PAK access control software. In addition, this guide includes the **Special Applications** section, which describes the configuration of the several other applications to use WIN-PAK.

Intended Audience

This guide is intended for the WIN-PAK operators and Administrators.

Prerequisite Skills

Knowledge of Access Control System and its terminologies.

Document Structure

The guide is divided into several chapters for better organization. The following table describes the details of what is covered in each chapter:

Chapter	Description
Chapter 1, Introduction	Gives an overview of WIN-PAK and explains the key software concepts and features.
Chapter 2, Installation	Covers the system requirements, installation procedures, licensing and registration information.
Chapter 3, User Interface	Explains the basic convention used in the user interface of the WIN-PAK software. This chapter also includes the procedures to access the Help.
Chapter 4, Getting Started	Explains the basic configuration details of the client and server. This helps you to get started with the WIN-PAK software. It also includes the configuration details of WIN-PAK services.
Chapter 5, System Settings	Describes how to configure WIN-PAK users and to set or change the default settings of WIN-PAK.

Chapter	Description
Chapter 6, Quick Configuration	Comprises sections for configuring servers, panels, and readers using Quick Start wizard.
Chapter 7, Badging	Describes how to design a badge, configure the badge DLLs and the badge printer.
Chapter 8, Card Holders	Includes information on setting up the card holder template, card holders, cards, and assigning card holders to cards and badges. In addition, this chapter describes how to use the WIN-PAK Import Utility to import the card and card holder information to WIN-PAK from an Excel sheet.
Chapter 9, Time Management	Explains how to set time zones, schedule an event, and define holiday groups and daylight saving groups.
Chapter 10, Device Map	Comprises sections for configuring servers, panels, readers, and abstract devices and, in addition, includes instructions on how to monitor intrusions using the Galaxy and Vista Panels.
Chapter 11, Defining Areas	Describes how to define access areas, control areas and tracking and muster areas, control devices through the control map, and monitor card holder movement in the tracking and muster areas through the tracking and muster view.
Chapter 12, Floor Plan	Explains how to create floor plans and control devices from the floor plan view.
Chapter 13, Command File	Includes sections on defining commands, command files, and for controlling devices by executing the command files.
Chapter 14, Guard Tour	Describes how to define and run guard tours.
Chapter 15, Monitoring Actions	Explains the different ways available for tracking and monitoring events in the access control system.
Chapter 16, Translation	Describes how to translate the user interface using the language text file and on creating language files.
Chapter 17, Reports	Assists you in generating the variety of reports that can be exported, viewed, or printed.
Appendix	Includes a section on performing a cold restart of the access control panel in the event of the power surge.

Symbol Definition

The following table lists the symbols used in this document to denote certain conditions:

Symbol	Definition
	**Note:** Identifies information that requires special consideration.
	Tip: Identifies advice or hints for the user, often in terms of performing a task.
	Example: Identifies an example that complies with the concept.
	**Warning:** Indicates a potentially hazardous situation, which if not avoided, could result in serious injury or death.
	**Caution:** Indicates a situation which, if not avoided, may result in equipment or work (data) on the system being damaged or lost, or may result in the inability to properly operate the process.

Contacts

The contact details for Honeywell Access Systems are as follows:

Honeywell Access Systems

135 West Forest Hill Avenue

Oak Creek, WI 53154

U.S.A

OFFICE HOURS: 8 AM to 5 PM (CST)

PHONE: 414-766-1700

FAX: 414-766-1798

URL: http://www.honeywellaccess.com

Introduction

1

In this chapter...

Overview of WIN-PAK

WIN-PAK is a state-of-the-art access control software that is compatible with Windows XP operating system and Win2000 or Win2003 server-based operating systems. The WIN-PAK access control software uses access control mechanism to authenticate the employee access at security areas. Access is authenticated by way of access cards or key codes provided to the employees.

In addition, the access control tracks the employee access, controls the entry and exit details, and generates reports of all access cards and keycode activities.

Note: By default WIN-PAK supports the configuration and monitoring of the access control panels. If you want WIN-PAK to support intrusion panels, you must procure the additional license from Technical Support - Honeywell Access Systems.

WIN-PAK Components

The WIN-PAK application is divided into three components: Database Server, Communication Server, and User Interface. These components can run on a single computer or on multiple computers, allowing flexibility in configuring a networked system.

WIN-PAK Servers

Database Server

The database tables can store, organize, and retrieve data using the WIN-PAK Database Server. This data is accessible to Communication Server and User Interface for retrieving and generating the reports.

The Database Server can be installed on the client computer or any other computer connected to the network.

Communication Server

The Communication Server routes User Interface requests as well as the access transactions to the panel. The panel in turn processes the transactions and sends the information to the Database Server as well as responses to the User Interface through the Communication Server.

While the communication server is sending information to the database server, it can receive a request from the user interface. In such cases of conflict, the Communication Server considers the user request as a higher priority and stalls the panel-database server communication till the time the user request is processed.

The Communication Server can be installed on the client computer or any other computer connected to the network.

WIN-PAK Client

User Interface

The User Interface helps WIN-PAK operators to communicate with the access control system. The User Interface can be installed on the computer where the Database Server or the Communication Server is installed or any other computer connected to the network.

You can run several client computers and can access the single Database Server simultaneously. The number of client computers depend on the WIN-PAK license type.

WIN-PAK Features

- **Installation**: Handles large and complex installations including the configuration of the WIN-PAK environment.
- **Secured Environment**: Supports Tracking and Mustering reporting to indicate the location of people for enabling the secured environment. Additionally, intrusions at different areas can be monitored, if you have the license for the Galaxy and/or Vista features in WIN-PAK.
- **Live Monitor Display**: Provides CCTV control with live monitor display. The CCTV switchers are Burle, Dedicated Micros, Fusion, Geutebruck, Javelin, MaxCom, MaxPro, NCI CCTV, Panasonic, Pelco, Vicon, and VideoBlox.
- **WIN-PAK Services**: In addition to the database server and the communication server, WIN-PAK contains four other servers:
  - **Command File Server**: Text files containing device instructions are stored in the Command Files database. The commands in the command files can be sent to the devices automatically on receiving, acknowledging, or clearing an alarm. The command files can also be executed manually.
  - **Guard Tour server**: A Guard Tour is a defined series of check points a guard must activate within a given amount of time. The check points are readers or input points where the guard presents the card or presses the button.
  - **Muster Server**: A Muster Server is enabled in the event of an emergency and allows the card holders to swipe the readers. Muster areas are logical areas that contain readers to be used by the card holders, only if there is a call for muster (in the event of a disaster, for example).
  - **Schedule Server**: The Schedule server schedules the list of events to be performed at predetermined time and intervals such as hourly, daily, or monthly.

Note: The WIN-PAK services are installed while installing the Database Server or the complete WIN-PAK. They are started automatically after installation.

Software Concepts

Abstract Devices

An abstract device is a logical representation of a physical device. The ADVs can be associated with any hardware device, including communication interfaces, panels, alarm points, entrances, and CCTV equipment. The ADVs help in monitoring the device status and controlling the actions of a physical device through the Control Map, Floor Plan, or Alarm View.

Floor Plan View

The Floor Plan provides a graphical representation of a building which includes the placement of the physical devices such as doors, panels, inputs, outputs, and CCTV equipment. The floor plans can also be a loop wiring diagram, a simple grid, or a picture of an area where the device is located. The floor plan views can be tailored to the specific needs of your access control system.

Badge

Badge is a template or a design for creating a card. WIN-PAK includes a full-featured badge layout utility for designing, creating, and printing badges. Badge design includes magnetic stripe encoding, barcoding, signatures, and so on.

Card and Card Holder

A card is an identity proof of a person and a card holder is a person who holds the card. Multiple cards can be assigned to a single card holder to provide different access.

Intrusion Panels

Galaxy and Vista panels are intrusion panels that enable you to monitor and control intrusions in your organization. To enable this feature in WIN-PAK, procure the license for the Galaxy panel and/or Vista panel from Technical Support - Honeywell Access Systems.

Installation

2

In this chapter...

Introduction

Overview

The WIN-PAK installation chapter describes the step-by-step procedure for installing, uninstalling, and registering the WIN-PAK software. In addition, it provides the hardware and software requirements, and prerequisites for installing the WIN-PAK software.

The WIN-PAK installation setup installs the required components and programs depending on the type of installation. The WIN-PAK software is distributed on an auto-run CD, with release notes and other technical documents.

WIN-PAK Architecture

WIN-PAK is a multi-tier, client-server distributed application, consisting of three primary modules: the Database Server, Communication Server, and User Interface.

- The WIN-PAK modules installed on different computers are networked and connected through RPC and LPC. This allows extremely flexible WIN-PAK program components to run as full services in Windows XP.
- The WIN-PAK software is shipped with debug versions of the services, which provide a console output window. However, avoid daily usage of these versions, as they are reserved for error isolation.
- WIN-PAK provides the System Manager utility to configure connection information. The System Manager directs the User Interface and other remote servers to the Database Server.

Note: To optimize the resource usage, stop the unused services using System Manager. For example, stop the Guard Tour Server or the Muster Server, if not used.

System Requirements

Hardware Requirements

This section provides you the list of hardware requirements for installing WIN-PAK.

- If you want to install WIN-PAK in a stand-alone computer that supports 1 to 10 readers, 250 cards, and 2 communication ports, your computer must fulfill the **minimum** requirements.
- If you want to install WIN-PAK in a computer that supports 1 to 100 readers, 5,000 cards, and 8 communication ports, your computer must fulfill the **recommended** requirements.

- If you want to install WIN-PAK in a computer that supports more than 100 readers, 50,000 cards and 255 communication ports, your computer must fulfill the **performance** requirements.

Hardware Component	Minimum	Recommended	Performance
Processor	Intel Pentium III	Intel Pentium IV	Intel Xeon 4
CPU	1GHz CPU	2.8GHz CPU	3.0GHz CPU
RAM	256 megabytes (MB)	512 megabytes (MB)	8 Gigabytes
Hard Disk	2.1-GB with minimum free space	40-GB SATA or SCSI OR 36-GB 10k RPM SCSI	36-GB 15k RPM SCSI hard disk in a RAID 5 configuration
Serial communication ports	1	2	As per the requirement
Secondary Storage	Tape or CD burner	Tape or DVD burner	DLT or DAT tape
Printer port	1 (2 if badging)	1 (2 if badging)	1 (2 if badging)
Monitor Display	**Size**: 15 Inches SVGA **Resolution**: 1024 x 768 **Colors**: 256 color	**Size**: 17 Inches **Resolution**: 1024 x 768 **Colors**: True color	**Size**: 19 inch **Resolution**: 1280 x 1024 **Color**: True color
Pointing Device	Mouse (PS/2 mouse preferred)	Mouse (PS/2 mouse preferred)	Mouse

Video Capture Card

A video capture card is required for transmitting the analog signals to digital signals and to fed the source of video to a computer where WIN-PAK is installed. The source of video may be a CCTV switcher or any camera used for photo snapping. The video capture card can interact with the CCTV switcher and the video badge attached to the WIN-PAK software. However, a single computer supports only one video capture card.

Therefore, when both the CCTV switcher and video badging is used in a computer, the badging camera signal is routed to the CCTV switcher and back to the WIN-PAK software. Honeywell recommends PBVP15 video capture card.

Modems and Communication Ports

Modems and communication ports are required when the mode of communication between loop and server computer is dial-up. Modems and communication ports are supported by Windows XP operating system and Win2000 or Win2003 server-based operating system.

Badging Printers

The Windows Operating System supports any type of badge printer. However, for two-sided PVC encoding or magnetic stripe encoding, the PBVP35 series (Ultra Rio or Tango) printer is required.

Report Printers

The Windows Operating System supports any type of printer for printing the reports. However, for single-line printing a dot-matrix printer, such as the PB-PRINTER is sufficient.

Panel Firmware

The PW-2000 or N-1000 family of control panels must have firmware of version 8.02 or later. The NS2+ and P-Series panels must have firmware of version 1.04 or later.

Software Requirements

The following table describes the software requirements to install WIN-PAK on your computer:

Components	Minimum	Recommended	Performance
Operating System	Microsoft Windows XP Professional SP2	Microsoft Windows XP Professional SP2	Microsoft Windows 2003 Server SP1
Database Engine	MSDE 2000	MSDE 2000	Microsoft SQL Server 2000 OR Microsoft SQL Server 2005
Browser	Internet Explorer 5.5	Internet Explorer 5.5 or later	Internet Explorer 5.5 or later

System Prerequisites

Stand-alone Systems

Before installing WIN-PAK, ensure that the following prerequisites are met:

- Service Pack 2 is installed for Windows XP Professional.
- If the configuration is meant for Performance or Maximum, Microsoft SQL Server 2000 is installed on the Database Server computer.
- A video capture card is installed on the badging workstation.
- Printer and printer drivers are installed.
- The energy management from the BIOS and the Operation system is disabled. If not, it may affect the installation and operation of WIN-PAK.

- TCP/IP protocol is installed for the proper functioning of MSDE.
- Microsoft Loopback or Dial-up adapter is installed, if network card does not exist.

Note: WIN-PAK may not function properly with the earlier versions of Internet Explorer 5.5. Therefore, Honeywell recommends you to install IE 5.5 or later.

Before beginning the installation:

- Make a note of the CD Key, which is provided inside the WIN-PAK Quick Reference Guide cover. This is required while installing WIN-PAK.
- Read the release notes on the WIN-PAK CD for additional installation information and updates.

Networked Systems

Before installing WIN-PAK for the first time in the networked system, ensure that the following prerequisites are met in addition to the stand-alone systems prerequisites:

- Network cards are installed on a networked system. A standard Windows-compatible network card is adequate.
- Ensure that the client computer name is alphanumeric characters without spaces and the first character is always an alphabet (standard UNC connections).
- Ensure that an unrestricted, permanent path is established between the networked computers. Any firewalls, proxies, or routers between workstations must not restrict the communication.

Installation and Upgrades

Overview

The WIN-PAK installation setup installs the required components and programs depending on the type of installation. The WIN-PAK software is distributed on an auto-run CD, with release notes and other technical documents.

Note:

- Quit all the Windows applications running in the computer, before installing WIN-PAK on your computer.
- During installation, if you are prompted by the **Do you want to keep this file?** message, click **Yes**. If not, the existing .dll files are overwritten.

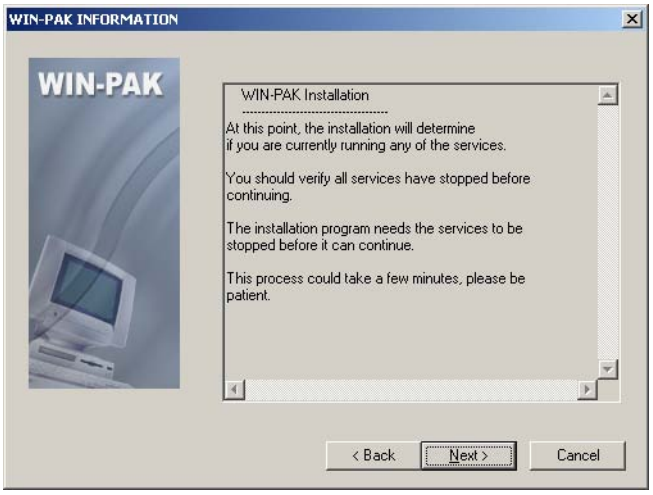
Installing WIN-PAK

To install WIN-PAK:

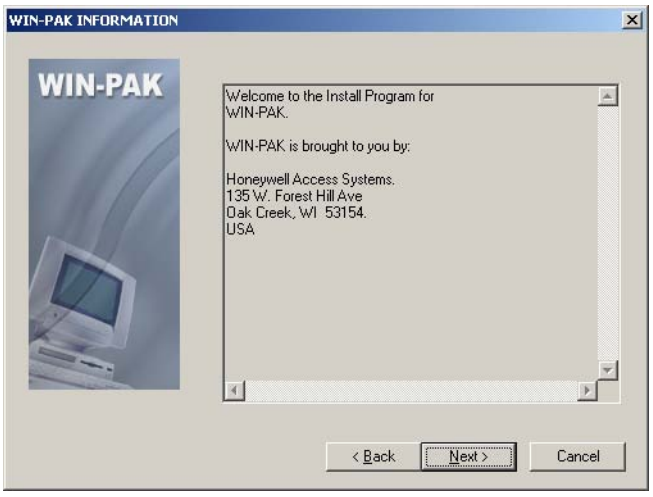
1. Insert the WIN-PAK CD into the CD drive. An installation browser opens. If the browser does not open, browse to the CD folder and run the Launch.exe file.
2. Navigate to the initial installation screens and click **Install Software** to display the next screen.
3. Click **Install/Upgrade WIN-PAK PE**. The **Welcome** screen appears.

Note: If an earlier version of Internet Explorer is found (earlier than IE 5.5), WIN-PAK prompts you to upgrade IE. Click **Yes** to upgrade IE.

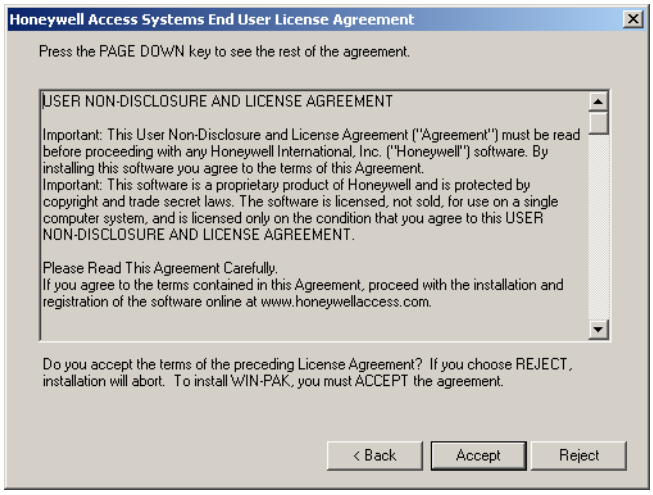
4. Click **Next** to continue installation. The **WIN-PAK Information** screen appears.



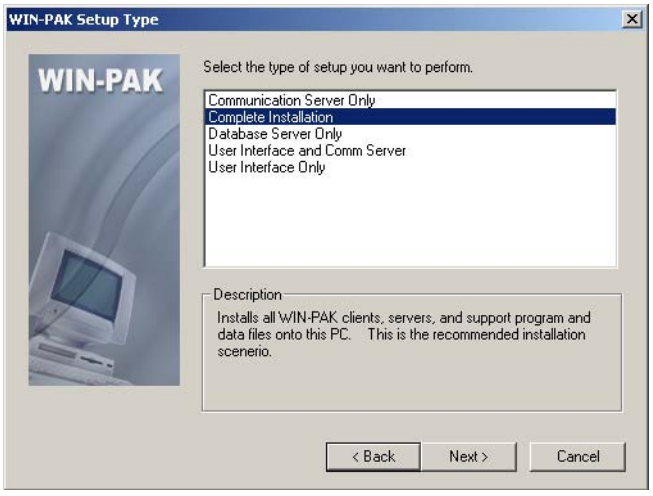
5. Click **Next** to verify that all the services are stopped. The **WIN-PAK Welcome** screen appears.



6. Click **Next**. The **End User License Agreement** screen appears.



7. Read the license agreement details and click **Accept** to accept the agreement. The **WIN-PAK Setup Type** screen appears.



8. Select the Type of Setup. The following table describes the available installation in WIN-PAK setup:

Type of Setup	Installs...	Suitable when...	Refer to...
If you are installing WIN-PAK in a stand-alone computer, you can select the setup type as Complete Installation:			
Complete Installation	All the WIN-PAK components such as client, server, support programs and so on.	– Setting up in a stand-alone computer. – Installing the Database Server for a networked system.	Installing Complete WIN-PAK
If you are installing WIN-PAK on a network environment, you can select any of the following setup types:			
Database Server Only	Only the Database Server and the related components.	Installing WIN-PAK in a networked computer	Installing Database Server
User Interface Only	Only the WIN-PAK User Interface.	Installing WIN-PAK on a client workstation in a networked computer.	Installing Complete WIN-PAK
User Interface and Comm Server	The User Interface and the Communication Server	Installing additional communication servers on a networked computer, where the networked computer is also used as a workstation.	Installing User Interface and Communication Server
Communication Server Only	Only the Communication Server and the related components.	Installing the communication server on a networked computer.	Installing Communication Server

Notes:

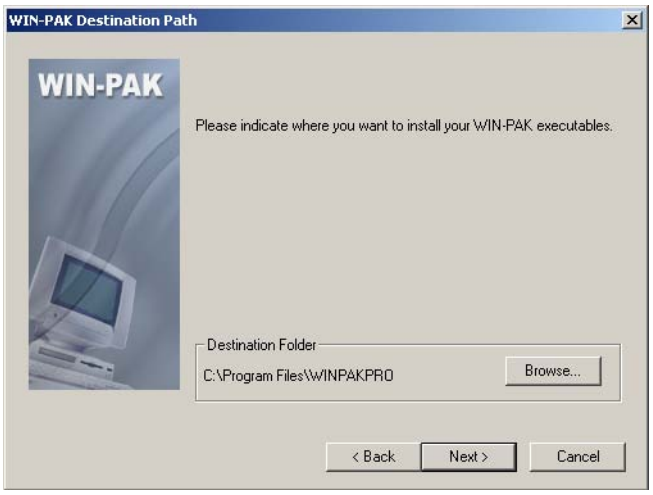
1. To protect the database files from the failure of the operating system, place them on a different drive partition.
2. To isolate the database files from the database server, place them on a separate hard drive.
3. Install the database file on the database server. This helps in effective usage of the WIN-PAK back up and restore option.

Installing Complete WIN-PAK

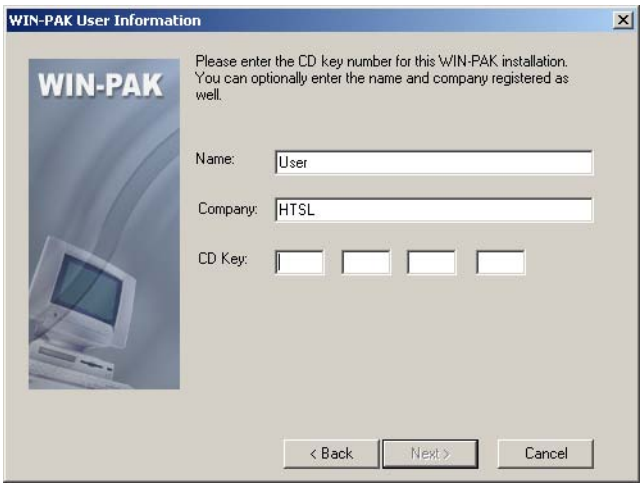
You can install complete WIN-PAK, if you are installing WIN-PAK on a stand-alone computer.

To install Complete WIN-PAK on your computer, perform the instructions given in "Installing WIN-PAK" on page 6 and follow these steps:

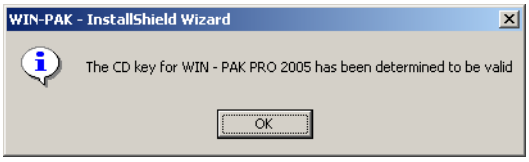
1. On the **WIN-PAK Setup Type** screen, select **Complete Installation** and click **Next**. The system checks for SQL Service status and displays the **WIN-PAK Destination Path** screen.



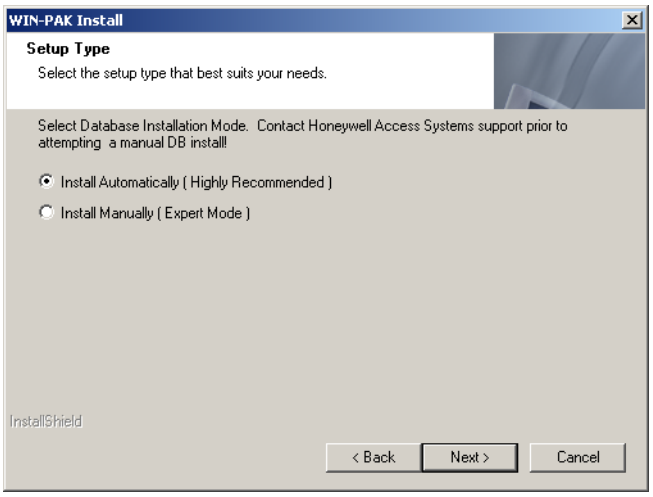
2. By default the installation path is C:\Program Files\WINPAKPRO. To change the path, click **Browse** and navigate to the destination folder.
3. Click **Next**. The **WIN-PAK Destination Path** screen appears displaying the WIN-PAK database file paths.
4. To change the path, click **Browse** and navigate to the destination folder for each database file.
5. Click **Next**. The **WIN-PAK User Information** screen appears.



6. Type your **Name**, **Company** and **CD Key** details. The CD Key is found in the front cover of the WIN-PAK Quick Reference Guide.
7. Click **Next**. The setup verifies the CD key and displays a message of its validity.



8. Click **OK**. The **WIN-PAK Setup Type** screen appears.

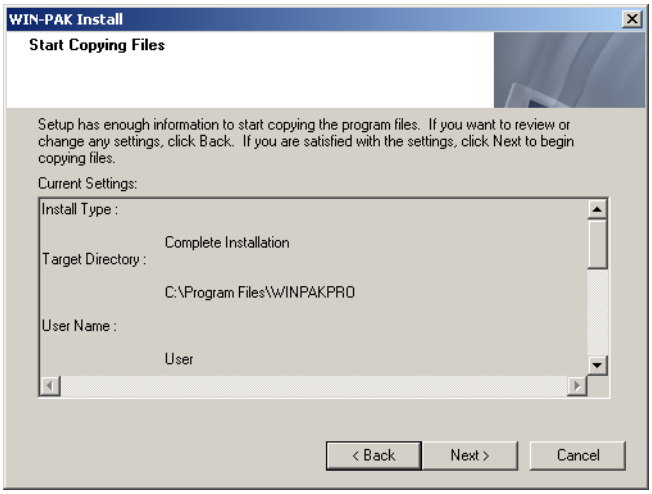


9. Select the Installation Mode as **Install Automatically** for auto-installation.

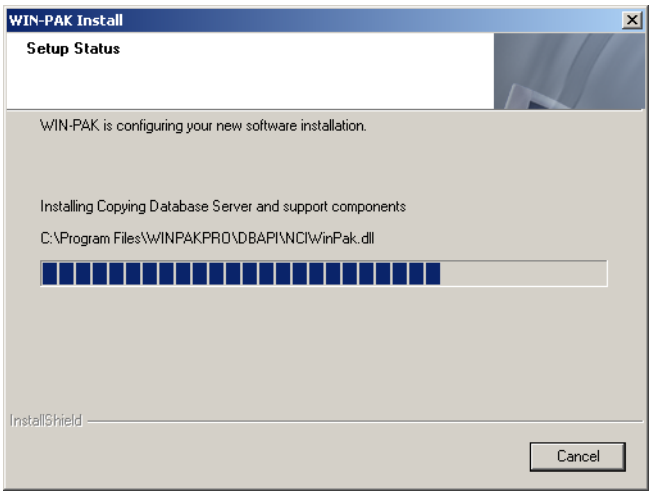
Note: You may need the support of Honeywell Access Systems for manual installation.

10. Click **Next**. A dialog box appears prompting you to create WIN-PAK shortcuts on your desktop.

11. Click **Yes** to place icons on your desktop. The **Start Copying Files** screen that summarizes the selected information is displayed.



12. If you want to change any setting, click **Back**. OR, click **Next** to start the installation.



13. After completing the installation, the **WIN-PAK Setup Complete** screen appears.

14. Click **Yes, I want to restart my computer now** to restart your computer after installation.

    OR

    Click **No, I will restart my computer later** to complete the installation without restarting your computer.

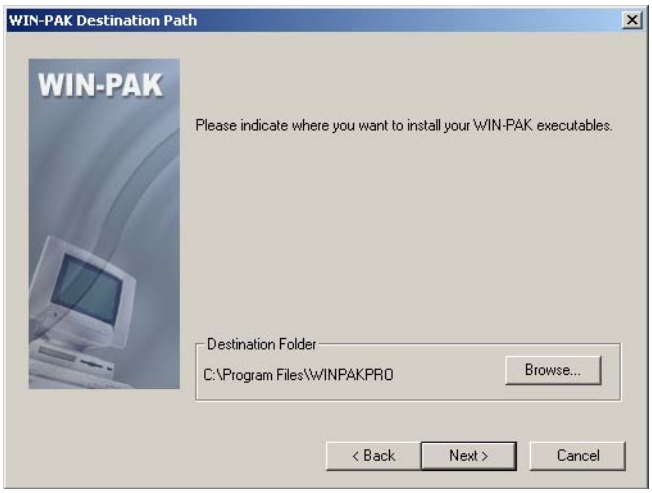
15. Click **Finish** to complete the installation.

Installing Database Server

You can install the database server on the computer connected to a network.

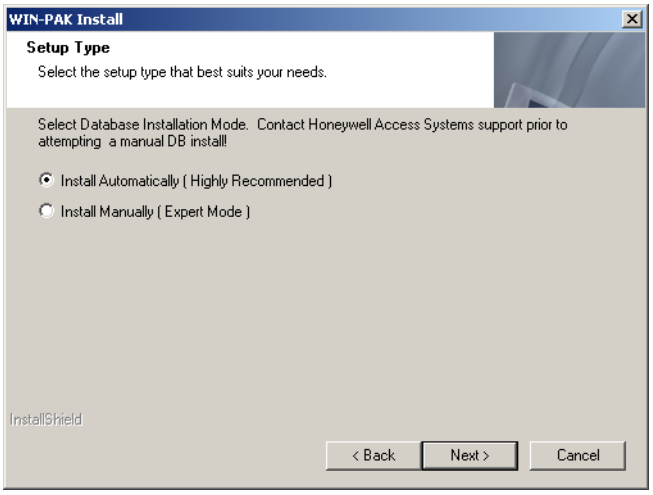
To install only the database server, perform the instructions given in "Installing WIN-PAK", and then follow these steps:

1. On the **WIN-PAK Setup Type** screen, select **Database Server Only** and click **Next**. The system checks for SQL Service status and displays the **WIN-PAK Destination Path** screen.



Note: In the following screens, the default path settings for installation, database, archive file, database file, and language file are displayed.

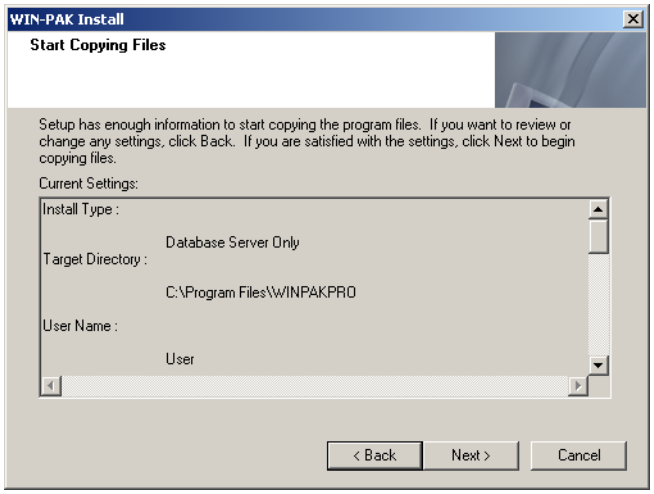
2. Click **Browse** to change the destination folder and click **Next** in each screen. The **WIN-PAK User Information** screen appears.
3. Type your **Name**, **Company** and **CD Key** details. The CD Key is found in the front cover of the WIN-PAK Quick Reference Guide.
4. Click **Next**. The setup verifies the CD key and displays the message for validity.
5. Click **OK**. The **WIN-PAK Setup Type** screen appears.



6. Select the Installation Mode as **Install Automatically** for auto installation.

Note: You may need the support of Honeywell Access Systems for manual installation.

7. Click **Next**. The dialog box appears prompting you to create icons on the desktop.
8. Click **Yes** to place the icons on your desktop. The summary of the selected information is displayed.



9. Click **Back** to change any installation settings, or click **Next**. The WIN-PAK software is installed and then **WIN-PAK Setup Complete** screen appears.
10. Click **Finish** to complete the installation.

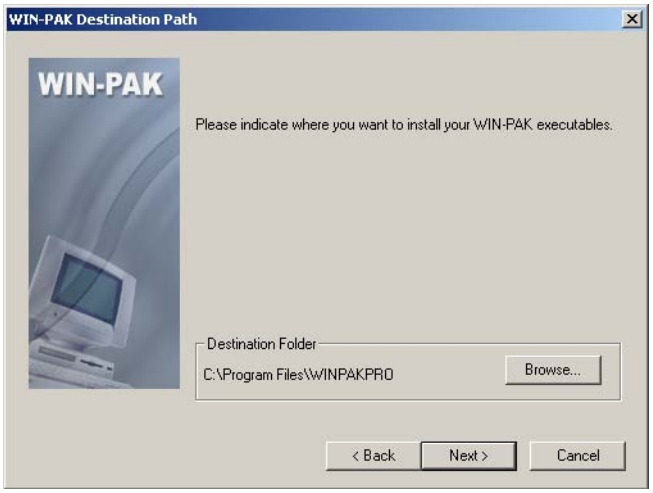
Installing User Interface

The User Interface is installed at each workstation across the Local Area Network (LAN).

Note: While installing at a workstation on a LAN, ensure that the installation directory resides on a shared drive mapped in the target system. If not, the installation fails when the system reboots and attempts to re-establish connection to the host directory.

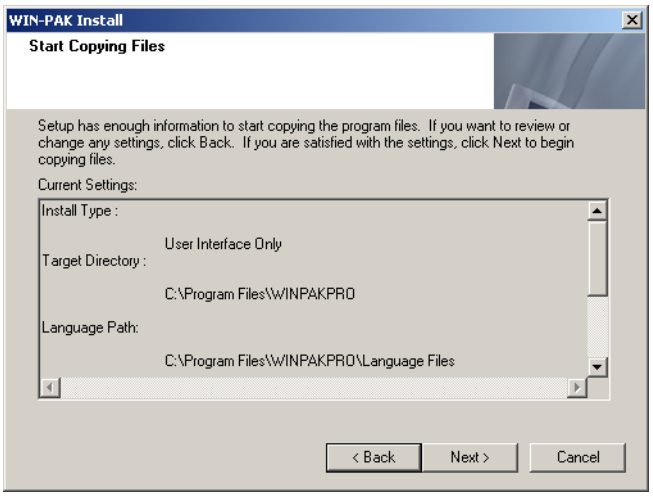
To install WIN-PAK User Interface only, perform the instructions given in "Installing WIN-PAK", and follow these steps:

1. On the **WIN-PAK Setup Type** screen, select **User Interface Only** and click **Next**. The system checks for SQL Service status and displays the **WIN-PAK Destination Path** screen.



Note: In the following screens, the default path settings for installation, database, archive file, database file, and language file are displayed.

2. Click **Browse** to change the destination folder and click **Next** in each screen. The dialog box appears prompting you to create icons on the desktop.
3. Click **Yes** to place the icons on your desktop. The summary of the selected information is displayed.
4. Click **Back** to change any installation settings, or click **Next**.
5. After the installation is complete, the **WIN-PAK Setup Complete** screen appears.

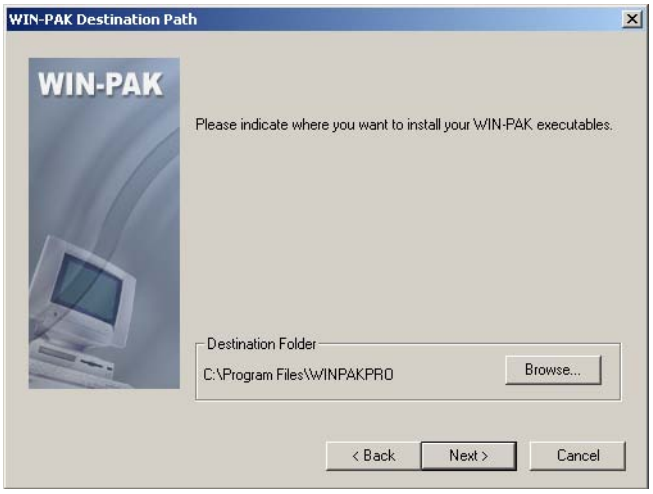


6. Click **Finish** to complete the installation.

Installing User Interface and Communication Server

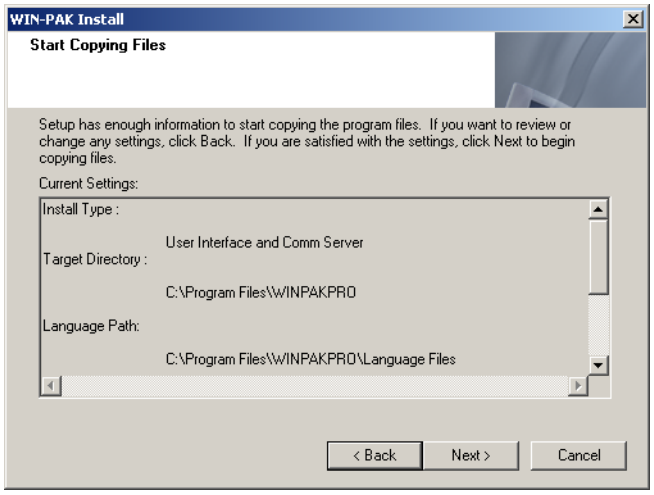
To install WIN-PAK User Interface and Communication Server, perform the instructions given in "Installing WIN-PAK", and follow these steps:

1. On the **WIN-PAK Setup Type** screen, select **User Interface and Comm Server** and click **Next**. The system checks for SQL Service status and displays the **WIN-PAK Destination Path** screen.



Note: In the following screens, the default path settings for installation, database, archive file, database file, and language file are displayed.

2. Click **Browse** to change the destination folder and click **Next** in each screen. The dialog box appears prompting you to create icons on the desktop.
3. Click **Yes** to place the icons on your desktop. The summary of the selected information is displayed.
4. Click **Back** to change any installation settings, or click **Next**.
5. After installation is complete, the **WIN-PAK Setup Complete** screen appears.



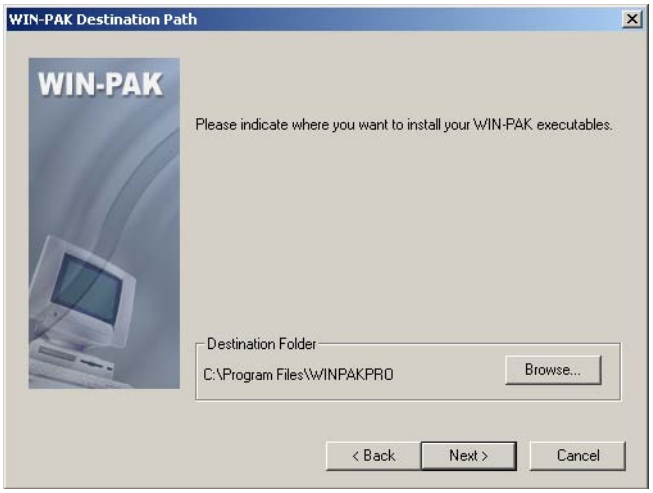
6. Click **Finish** to complete the installation and restart the computer.

Installing Communication Server

WIN-PAK supports installation of multiple communication servers across a network. After installing Database Server and User Interface, multiple communication servers can be installed depending on your licensing limit.

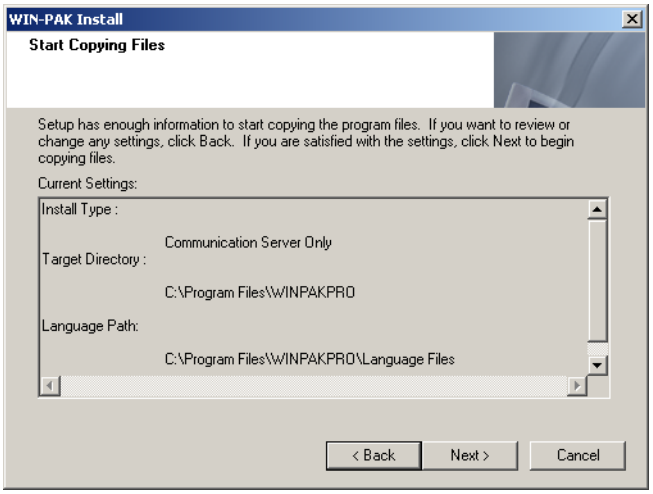
To install WIN-PAK Communication Server, perform the instructions given in "Installing WIN-PAK", and follow these steps:

1. On the **WIN-PAK Setup Type** screen, select **Communication Server** and click **Next**. The system checks for SQL Service status and displays the **WIN-PAK Destination Path** screen.



Note: In the following screens, the default path settings for installation, database, archive file, database file, and language file are displayed.

2. Click **Browse** to change the destination folder and click **Next** in each screen. The dialog box appears prompting you to create WIN-PAK icons on the desktop.
3. Click **Yes** to place the icons on your desktop. The summary of the selected information is displayed.
4. Click **Back** to change any installation settings, or click **Next**.
5. After the installation is complete, the **WIN-PAK Setup Complete** screen appears.



6. Click **Finish** to complete the installation and restart the computer.

Additional Installation Components

The WIN-PAK installation program installs several utilities during the normal installation process. These are supplied as re-distributable Microsoft packages and are deployed automatically based on the installed options. Each of these components is installed by a separate installation program that runs directly from the WIN-PAK CD.

Note: If prompted by the program, always keep the latest drivers.

While working with Windows XP operating systems, WIN-PAK installs the following external components:

External Components

The following is the list of external components that are installed during the WIN-PAK installation:

- Microsoft Data Access Components
- Sentinel Lock Drivers
- Crypkey Drivers

Microsoft Data Access Components

System Manager uses Microsoft Data Access Components (MDAC) for the DB server interface to the MDB file. Therefore, MDAC needs to be installed in your computer. However, MDAC is installed by default in all Operating Systems.

Note: The MDAC components are part of the operating system, and therefore it is not removed even after uninstalling WIN-PAK.

Sentinel: The Sentinel Hardware Lock Drivers

- Install the Sentinel Hardware Lock Drivers on the computer, where the Database Server is installed.

CrypKey: The CrypKey Licensing Drivers

- Install the CrypKey Licensing Drivers on the computer, where the Database Server is installed.

Foreign Language Installation

The WIN-PAK installation provides only the English version of these Microsoft modules. This may cause a problem, as the English version are not compatible with other language version of Windows operation system.

Note: Contact the Honeywell Technical Support team for the list of languages that are supported by the WIN-PAK system.

Upgrading WIN-PAK

WIN-PAK supports upgrading from WIN-PAK to WIN-PAK SE and WIN-PAK PRO to WIN-PAK PE.

Before upgrading WIN-PAK, make a backup copy of your database files. When prompted by the installation program, do not overwrite your existing database. In addition, make backup copies of your Floor Plan backgrounds, Card Holder photos, and signatures.

Also, before upgrading WIN-PAK, ensure to stop the WIN-PAK services and to quit all the Windows applications.

Note: When you reinstall WIN-PAK, it upgrades the existing WIN-PAK to the latest version.

Licensing and Registration

The WIN-PAK installation setup installs only the demo version. Though the demo version of WIN-PAK has no expiry date, it has the following limitations:

- Only a 10 card database can be maintained.
- You cannot import card and card holder information to WIN-PAK.
- You cannot add cards in bulk.
- You cannot print badges.

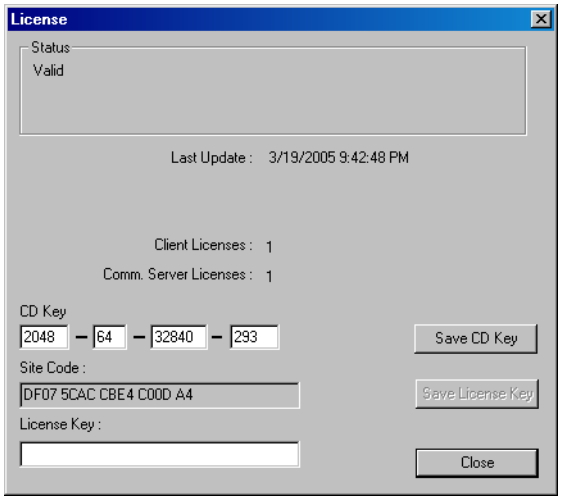
However, registering the software enables you to overcome the preceding limitations.

Registering WIN-PAK

Before you register the WIN-PAK software, make a note of the CD Key and Site Code. The CD Key number is located on the inner side of the front cover of the WIN-PAK Quick Reference Guide.

To view the Site Code:

1. Choose **Help > License**. The **License** window appears.



2. Make a note of the **Site Code**. This is a unique number that identifies your computer.

Registering WIN-PAK Online

You can register your WIN-PAK software online. The registration can be done using the Honeywell Access Systems web site.

To register WIN-PAK online:

1. Launch **Internet Explorer**, type www.honeywellaccess.com in the address bar, and then press ENTER.

   OR

   Choose **Help > Honeywell Access Systems > Registration**. The **Honeywell Access Systems** web page is displayed.

2. Choose **Support & Resources > Register Products**. The **Product Registration** page appears.
3. Click **Yes** to accept the License agreement. The **Site Information** page appears.
4. Enter the required details and click **Next**. The **Authorized Dealer Information** page appears.
5. Enter the dealer information and click **Next**. The **Enter the CD Key** page appears.
6. Select **WIN-PAK PRO** from the list of Honeywell products.
7. Type the **CD Key** in the provided box.
8. Click **Submit**. The **Site Key** is displayed.

   Note: If the CD Key is invalid, the system prompts you to provide the Site Code number.

9. Make a note of the **Site Key**. Close the browser and return to WIN-PAK.

10. In the **License** dialog box, type the **Site key** produced by the online registration.
11. Click **Save License Key**. This activates the license for WIN-PAK.

Note: The Site Key is sent you through e-mail.

Upgrading WIN-PAK License

You can upgrade your WIN-PAK license to overcome the limitations of the WIN-PAK software.

Example: You may need to upgrade your WIN-PAK license from single-user license to multi-user license.

Before upgrading the license, get the new CD Key from Honeywell Access System Support Service.

To upgrade your WIN-PAK license:

1. Choose **Help > Honeywell Access Systems > License**. The **License** dialog box appears.
2. Type the new **CD Key**.
3. Click **Save CD Key**. This upgrades your license.

Caution on License Files

The encryption software writes files to your hard drive as part of licensing. Do NOT move or damage these license files, as it invalidate the license.

Note: Honeywell recommends you to obtain a WIN-PAK hardware key (WP2KEY) for multi-drive RAID configuration computers. This avoids the licensing problems, if one of the drives needs to be replaced.

De-fragmenting Disk Drive

Any sort of moving or damaging license files, may invalidate your license. De-fragmentation is one of the actions that relocates the files.

Caution: Do not use Microsoft Disk Defragmenter for de-fragmenting.

Norton Speed Disk is used for de-fragmenting a hard drive so that it may be used more efficiently. In doing so, certain disk files may be physically moved. This may invalidate your license. However, if you de-fragment using Speed Disk after enabling the following options, the license file remains valid:

1. Open Norton Speed Disk, select **Options/Customize**, and select **Unmovable Files** from the **File** menu.
2. Enter the *.ent, *.key, and *.rst files under **Unmovable Files**.
3. Choose **Files > Options > Optimization > Save** to save the new profile.
4. Run the Speed Disk.

User Interface

3

In this chapter...

Introduction

The WIN-PAK PE User Interface enables you to configure, monitor, and control the entities in the Access Control System.

The User Interface can be installed on the computer in which the Database Server resides, or on one or more computers connected to the Database Server on a network. Closing or quitting the User Interface does not stop the WIN-PAK PE operations and the Database Server, Communication servers and the other services still continue to run.

This chapter describes how to log on to the WIN-PAK User Interface and about its various elements. Elements in the User Interface include windows, menus, toolbars, and status bar. In addition, you can learn how to gain access to the WIN-PAK help.

WIN-PAK User Interface Elements

The elements in the WIN-PAK User Interface are:

- Windows
- Menu bar
- Toolbar
- Status bar

Logging on to WIN-PAK

To log on to the WIN-PAK user interface:

1. Double-click the WIN-PAK PE User Interface icon on your desktop. The **Connect to Server** dialog box appears.
2. Type the **User Name** and **Password**.

Note: If the User Interface is not on the same computer as that of the Database Server, configure the details of the database server through the System Manager.

Refer to the section "Setting User Interface Workstation" in the Getting Started chapter for more details on setting the database server.

3. Click **Connect**.

Note: Administrator has privileges to access all Accounts whereas **Operator** has privileges to access only certain accounts. The title bar of the WIN-PAK Main window displays the name of the active account.

The **WIN-PAK PE - Account name - [Operator]** window appears after you have logged on to the WIN-PAK application.

Knowing more about the User Interface

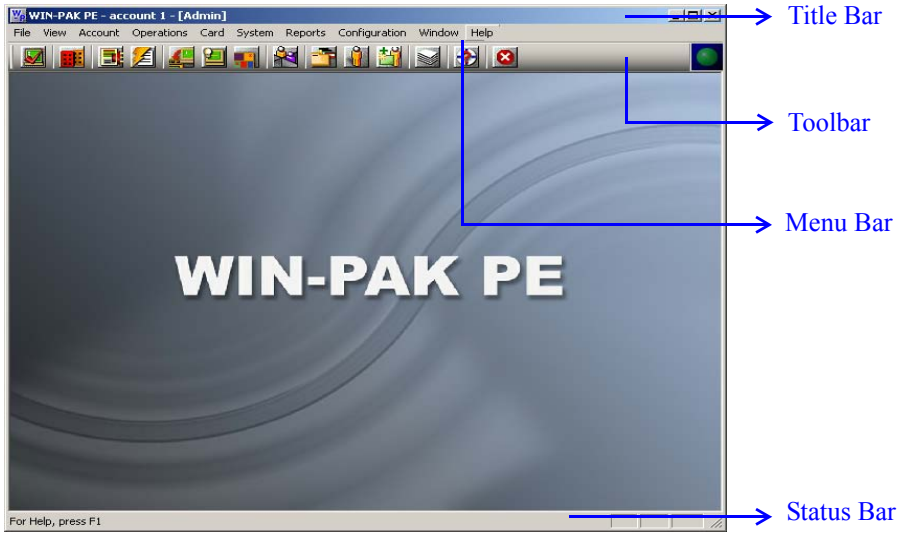


Figure 3-1 GUI Elements in the WIN-PAK User Interface

Note: If you have selected **All Accounts** using the **Select** option in the **Account** menu, the following toolbar icons and menu options appear disabled:

- Card and Cardholder icons in the toolbar.
- Sub-menu options in the **Card** menu.
- Options in the **Cardholder** sub-menu of the **Configuration** menu.

WIN-PAK Windows

The WIN-PAK user interface comprises a single Main window, multiple Maintenance windows, and Tree windows.

The Main window is started as soon as an Operator logs on to the WIN-PAK user interface. It comprises the options for performing various operations in WIN-PAK.

The Maintenance windows enable you to perform various operations for WIN-PAK entities.

The Tree windows enable you to view the details of devices, ADVs, areas, and operator levels and their relationship in a graphical tree.

The Main Window

The Main Window consists of a Title bar, Menu bar, Toolbar, and the Resize buttons.

The title bar displays the following details:

- **WIN-PAK** with the year of its release
- Account
- Operator

- Watchdog Timer

The Watchdog Timer is represented by the blinking green sphere icon  to the left of the Honeywell Access Systems logo on the toolbar. It sends continual pulses to the computer to verify that the connection to the server(s) is alive.

Toolbar

The toolbar appears below the menu bar in the Main window. The toolbar comprises the icons for the frequently used WIN-PAK operations.

The toolbar is displayed by default in the Main window. However, you can choose not to display the toolbar by clicking the **Tool** option in the **View** menu.

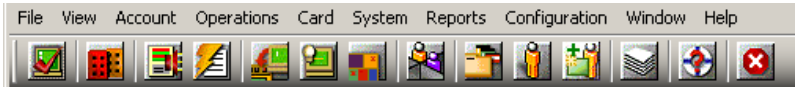


Table 3-1 Toolbar Buttons

Button	Button Name	Description
	**Log In**	Enables you to log on to WIN-PAK and connect to the WIN-PAK database server.
	**Select Account**	Displays the **Select Account** dialog box, allowing an authorized operator to select an account.
	**Dynamic Alarm View and Acknowledge**	Opens the **Alarm View** window, which allows incoming alarms to be viewed, acknowledged, and cleared.
	**View Events**	Opens the **Event View** window, which displays the current system activity in real time.
	**Control Map**	Opens the **Control Map** window, which can be used for controlling the devices and for providing an alternate means of acknowledging and clearing alarms.
	**Run Command File**	Displays the **Run a Command File** dialog box, enabling you to run command files containing device instructions.
	**Open Floor Plan**	Opens the **Open Floor Plan** window, enabling you to open floor plans.
	**Locate Last Card /Card Holder Transaction**	Opens the **Locate Card Holder** dialog box, enabling you to search for a card by card holder name or card number and view the time and place where the card was used.

Table 3-1 Toolbar Buttons

	**Card**	Opens the **Card** window, enabling you to search and sort the card list and to add, edit, or delete cards.
	**Card Holder**	Opens the **Card Holder** window, enabling you to search and sort the cardholder list and to add, edit, or delete card holders.
	**Add Card Holder**	Opens the **Card Holder** window enabling you to add card holders.
	**Run Report**	Opens the **Reports** window, enabling you to generate, view, and print reports.
	**Help Topics**	Opens the WIN-PAK Pro Help, the online help for WIN-PAK.
	**Auto-Logout from all servers**	Logs the operator out of the user interface and all the servers.

Menu Bar

The menu bar appears at the top of the Main window and comprises menus to carry out various WIN-PAK operations.

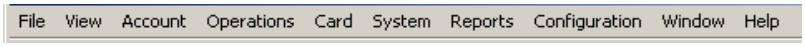


Table 3-2 Menu names and Shortcut Keys

Menu	Shortcut Key	Description
File	ALT + F	Contains options to configure printers, to log on and log off from the application, to quit from WIN-PAK, to view the reports window, and so on.
View	ALT + V	Enables you to disable or enable the toolbar and the status bar.
Account	ALT + A	Enables you to work with the accounts.
Operations	ALT + O	Enables you to perform various operations, such as viewing events, alarms, working with digital video, and so on.
Card	ALT + C	Contains options for working with access cards and access levels.
System	ALT + S	Contains options for setting system defaults.
Reports	ALT + R	Enables you to generate and view reports.

Table 3-2 Menu names and Shortcut Keys

Menu	Shortcut Key	Description
Configuration	ALT + N	Contains options for setting general hardware configuration before working with WIN-PAK.
Window	ALT + W	Enables you to toggle between the multiple open windows.
Help	ALT + H	Contains options to view the online help.

To access the options in the menu bar:

Using the pointing device (mouse),

1. Click the menu you want to access.
2. Click the required option. The corresponding window appears.

   Example: To gain access to the **Card Holder** menu, click **Card** and then click **Card Holder**. The **Card Holder** window appears.

Using the keyboard,

1. Press ALT combined with the short key for the menu you want to access.
2. Press the underlined alphabet of the option you require.

   Example: To gain access to the **Floor Plan** menu, press **<Alt>+O** and then press **F**. The **Open Floor Plan** window appears.

Status Bar

The Status Bar is displayed at the bottom of the Main window. By default, the status bar is displayed in the window. However, you can choose not to display the status bar by clicking the **Tool** option in the **View** menu.

The Status bar displays the following information:

- The message **For Help, press F1** at the left corner.
- A description of the option that you have highlighted in the menu or the toolbar.
- The messages for setting permissions and for establishing communication server connections when you log on to WIN-PAK.
- The message for disconnecting from the server when you log off from WIN-PAK.

Sub-menus and Pop-up menus on right-click

When you right-click inside certain dialog boxes, a pop-up menu appears displaying a set of options specific to the dialog boxes.

Example:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click **Devices** to display a sub-menu.
3. Move the mouse pointer on **Add** to display another sub menu.

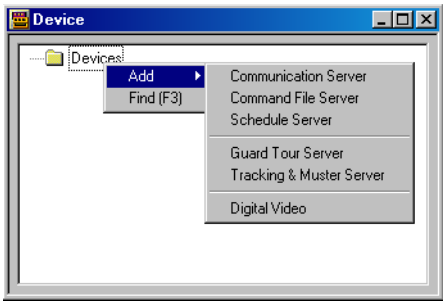


Figure 3-2 Sub-menus and Pop-up menus

Maintenance Window

The Maintenance windows enable you to perform the following operations on various WIN-PAK entities:

- Adding, editing, deleting, and printing data.
- Searching for and sorting data.
- Viewing the details of previously entered data.

Opening a Maintenance Window

To open a Maintenance Window, choose the menu option or click the icon in the toolbar for the operation you want to perform. The corresponding Maintenance window appears.

For example, if you want to configure the Card Holder Tab Layout, choose C**onfiguration > Card Holder > Card Holder Tab Layout**. The **Card Holder Tab Layout** window appears, which enables you to add, edit, delete, view card holders in addition to other card holder operations.

Viewing Information

You can view the details of previously entered information in a Maintenance Window. The information is listed in a table in the window.

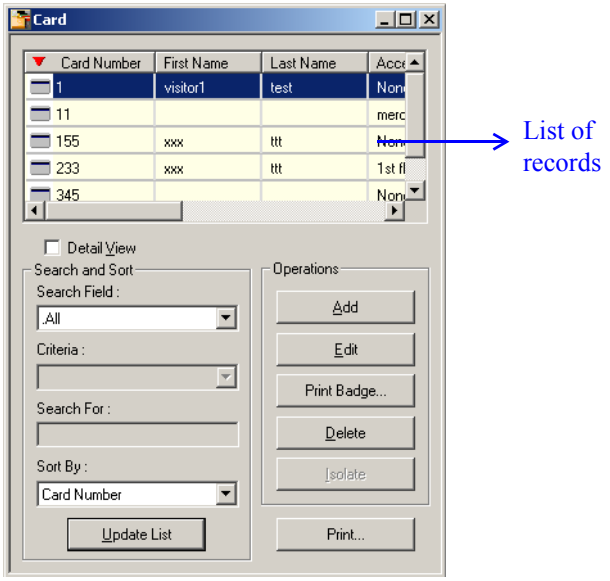


Figure 3-3 Viewing information

The following operations can be performed while viewing the list of records:

- To move through the list, use the scroll bars.
- To sort the list according to a particular column, click the column. The icon appears on the left of the column name and the list is sorted in the ascending order of the column.

  Example: If you want to sort the information based on **First Name**, click **First Name**. The icon appears on the left of **First Name** and the list is sorted in the ascending order, based on the column.
- To view the details of a specific record in the list, click the record and then select the **Detail View** check box. A dialog box displaying the details of the record appears towards the right of the **Card** dialog box. See Figure 3-4.
- To view the details of a specific record in the list,

  a. Click the entry and then select the **Detail View** check box or double-click the record. The following screen appears towards the right of the Maintenance window.

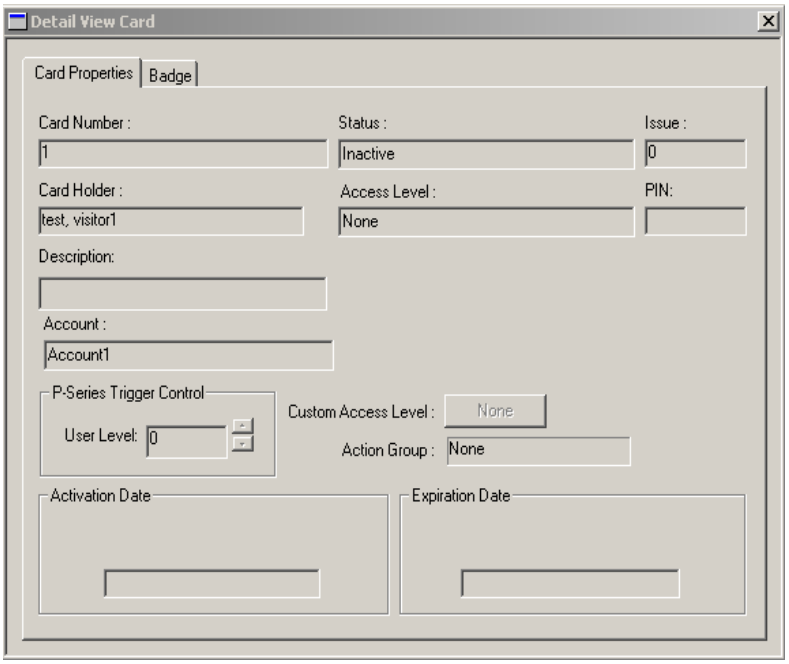


Figure 3-4 A detail view

b. Click **Close (X)** on the top-right corner of the screen or clear the **Detail View** check box in the Maintenance Window to close the **Detail View Card** dialog box.

Searching and Sorting

You can search for and sort the details displayed in the list in a specific order using **Search and Sort** option in the Maintenance window.

Note: The number of items returned as search result depends on the value set for the **Maximum Records returned from the Database for Find List** field in the Work Station Defaults. Set the value by choosing **System > Workstation Defaults** and clicking the **Defaults** tab.

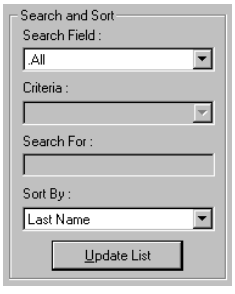


Table 3-3 Search and Sort Options and Actions

Options	Actions
Search	Select the item to be searched.
Criteria	Select the criteria for search.
Search For	Type a letter, word, phrase, or numeric expression that you want to search.
Sort By	Select the field based on which the records in the list must be sorted. In addition, it indicates the order in which the search results are displayed.
Update List	Click this button to perform the search. In addition, this button updates the list with the sorted information.

Adding, Editing, and Deleting records

The action buttons provided under the **Operations** area of the Maintenance window enables you to add, edit, and delete records.

Table 3-4 Buttons and Descriptions

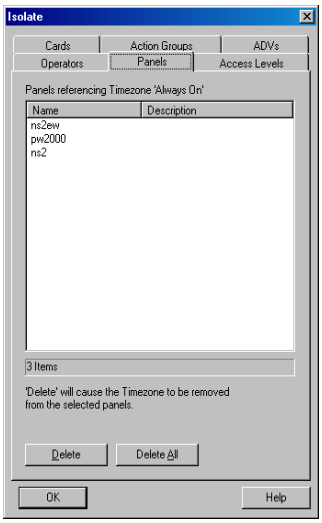
Button	Description
Add	Click this button to open a blank window for adding a new record.
Edit	Click this button to edit a selected record. An editable view of the selected record appears, where you can modify the details.
Delete	Click this button to delete a selected record. A message asking for confirmation appears. Click **Yes** to delete the record.

Isolating Records

Before deleting a record, it is essential to isolate it from all its associations.

Example: To delete a time zone you must first remove its association from the panels, access levels, cards, operators, ADVs, or action groups where it is used.

1. To isolate a record, select the record in the list and then click Isolate. The **Isolate** dialog box appears.



   The tabs in the **Isolate** dialog box indicate the various associations of the record that is deleted.

   Example: Time zones can be applied to Cards, Action Groups, ADVs, Operators, and Panels and therefore appear as tabs in the **Isolate** dialog box.

2. Click each tab and dissociate the record by clicking **Delete** or **Delete All**. A message asking for confirmation appears.
3. Click **Yes** to confirm the deletion.

Printing Details

You can print the record list using the **Print Report** option provided in the Maintenance window.

1. In the Maintenance window, click **Print Report**. A dialog box for specifying the print settings appears.
2. Specify the settings for previewing or printing the required information in the report.
3. Click **Print** on the window to print a report.

   Note: To view the report before printing, click **Print Preview**.

Toggle between Maintenance windows

You can open more than one Maintenance window at the same time.

1. Open two or more Maintenance windows.
2. Choose **Window** in the menu and click the appropriate window to activate it. A tick mark is displayed to the left of the window name in the menu and the corresponding window is activated.

Example:

a. Open the **Card** and the **Time Zone** windows by choosing **Card > Card** and **Configuration > Time Management > Time Zone** from the menu.

b. Choose **Windows** in the menu. The **Card** and **Time Zone** window names are listed in the menu.

c. To activate the **Card** window, click **Card**. Or to activate the **Time Zone** window, click **Time Zone**. A tick mark appears on the left of selected option in the menu indicating that the window is activated.

Tree Window

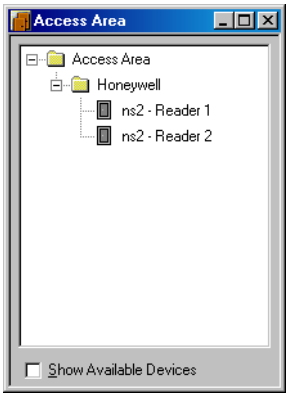
A Tree window enables you to view the details of devices, ADVs, areas, and operator levels and their relationship in a graphical tree. The tree organizes information into logical or geographical groups and is created as you program the access control system.

Six tree structures for Device Map, Control Map, Control Area, Access Area Map, Operator Level and Tracking Area Map are available in WIN-PAK. The tree structure for Device Map is defined, as and when devices are defined. The remaining tree structures define the hierarchy or relationship between the resources.

The status of the resources are indicated by Red and Green in the tree structure.

Example: In an access area, you can add entrances such as doors and readers to the tree structure.

- Choose **Configuration > Define > Access Areas**. The **Access Area** window appears.



- To expand the tree, click the plus sign (+) to the left of the folder. The branches corresponding to the selected folder are shown.
- To display only the top level information, collapse an opened tree by clicking the minus sign (-) to the left of a folder.

- The following colors indicate the access status of the entrances:

Color	Status
Green	Entrances having access in a selected access level.
Red	Entrances not having access.
Yellow	Entrances having limited access.

WIN-PAK Help

This section describes how to access the help topics of WIN-PAK as and when you are working with the user interface.

Accessing the Online Help

To access the WIN-PAK Pro Online Help, choose **Help > Help Topics** or press F1 on the keyboard.

Accessing Help on Web

You can access any information related to the Honeywell Access Systems from the web. Through the web site, you can view the Honeywell contact details and in addition, you can register WIN-PAK.

To access the Honeywell Access Systems website:

1. Choose **Help > Honeywell Access Systems > On the Web**. The **Honeywell Access Systems** website appears.

To view Honeywell contact details:

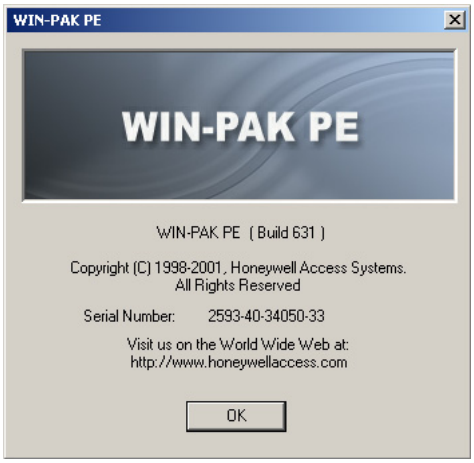
1. Choose **Help > Honeywell Access Systems >Contacts**. The **Honeywell Access Systems** website appears.
2. Click **Contact Us**. The contact details are displayed.
3. To obtain the contact details of a specific team, click the corresponding link.

   Example: If you want to obtain the contact details of technical support, click **Tech Support**.

Knowing more about WIN-PAK Pro

To know about the copyright, build, and serial number details of WIN-PAK Pro,

1. Choose **Help > About WIN-PAK PE**. The **WIN-PAK PE** dialog box appears with the details of the build number, copyright information, serial number, and URL of Honeywell Access Systems.



2. Click **OK** to close the window.

Getting Started

4

In this chapter...

Introduction

This chapter describes how to configure client and server, unblock firewall protections, start and stop the WIN-PAK services, and to log on and log off from WIN-PAK.

Note: Before you start working with WIN-PAK, make sure that you have configured the settings that are described in this chapter.

Remote Client Server Configuration

WIN-PAK works both in Domain and Workgroup environment. You can set the client-server communication as per the need. However, the domain environment is set by default.

After changing the settings, restart the servers and client for the changes to take effect.

Note: Ensure that the client-server communication setting matches across all the servers and client computers.

Domain Environment

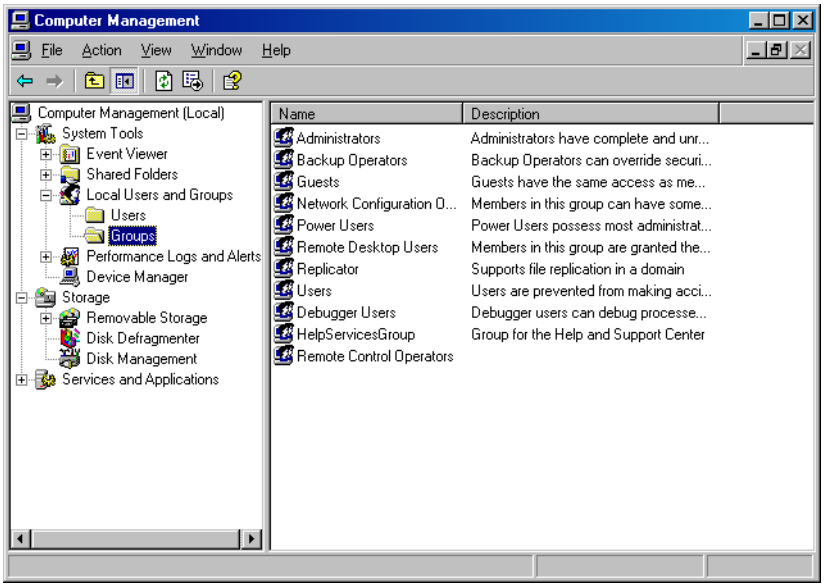
To work in a Domain Environment, you must add the domain users to the local System Administrator or Power Users Group and then unblock the WIN-PAK services from Firewall protection.

Adding Domain Users

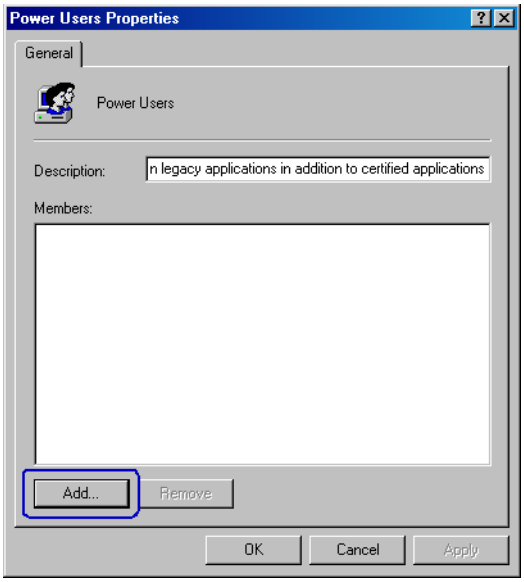
To add the domain users:

1. Log on to the system as Administrator where WIN-PAK Servers are installed.
2. Click **Start > Settings > Control Panel** and open **Administrative Tools > Computer Management**. The **Computer Management** window appears.

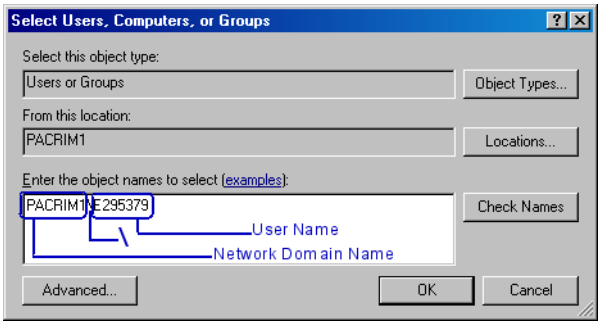
   Note: If Windows XP is installed on your computer, switch to Windows Classic view.
3. Choose **System Tools > Local Users and Groups** > **Groups**.



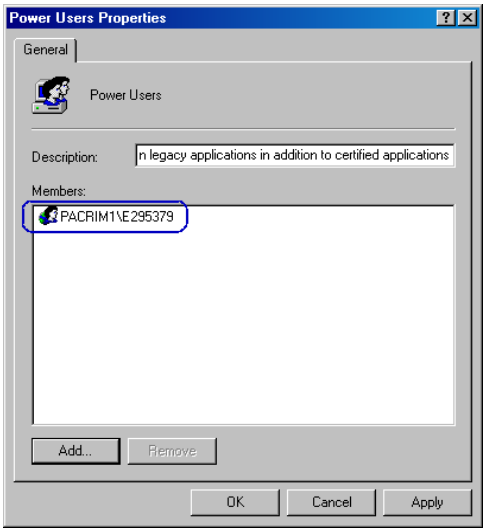
4. On the navigation pane, select and double-click **Power Users**. The **Power Users Properties** dialog box appears.



5. Click **Add** to add domain users to the group.
6. Type the network domain name and user name in the DOMAIN\USER NAME format.



7. Click **OK**. The user is added to the Power Users group.



8. Click **OK** to save the Power User Properties.

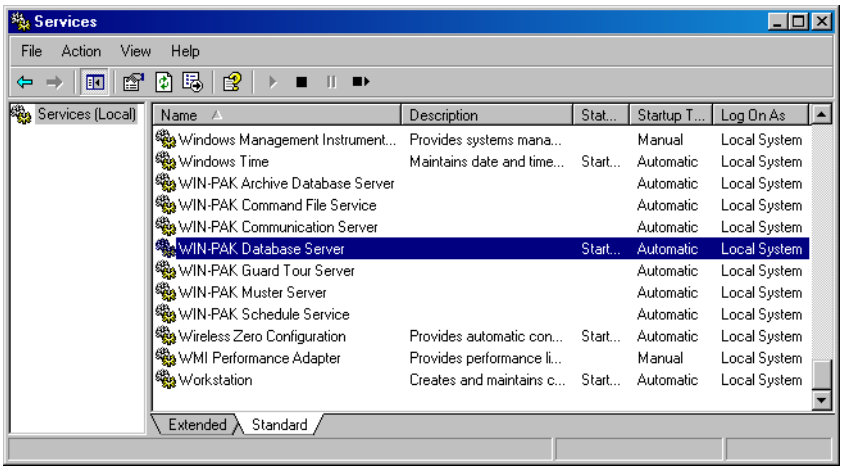
Configuring the Log On Property of WIN-PAK Servers

Before you configure the Log on property of WIN-PAK servers, add the domain user to the local System Administrator or Power Users Group.

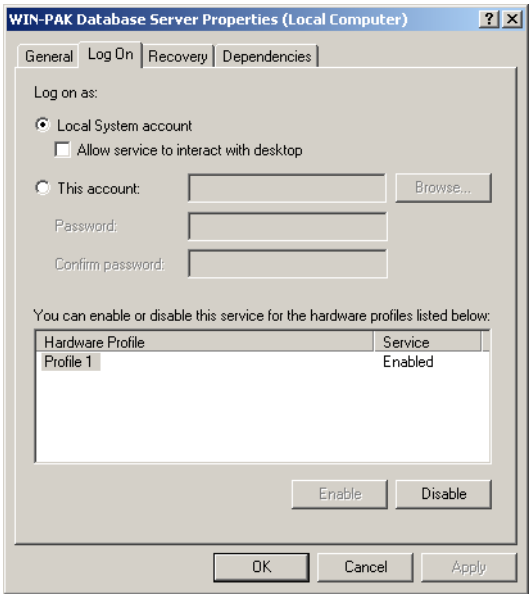
To configure the log on property of WIN-PAK Servers:

1. Click **Start > Settings > Control Panel** and open **Administrative Tools > Services**. The **Services** window appears.

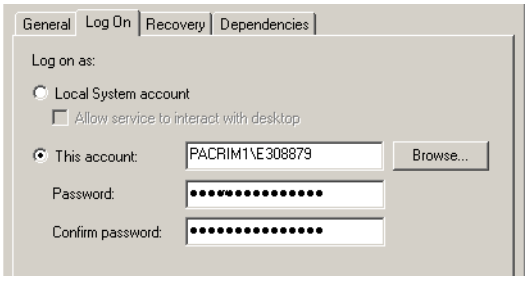
   By default, the **Log On As** property is **Local System** for all the WIN-PAK servers.



2. Select and double-click the required WIN-PAK Server from the right pane of the **Services** window. The **WIN-PAK Server Properties** window appears.



3. Click the **Log On** tab.
4. Click **This Account**. By default, **Local System account** is selected.
5. Enter the domain user account or click **Browse** to select the user account. The domain user account is added to the System Administrator or Power User group in the "Adding Domain Users" section in this chapter.
6. Type your **Password** and re-enter the password for confirmation in **Confirm password**.



7. Click **OK** to save the changes.

   Follow the same procedure for setting the **Log On As** property of all the other WIN-PAK Servers.

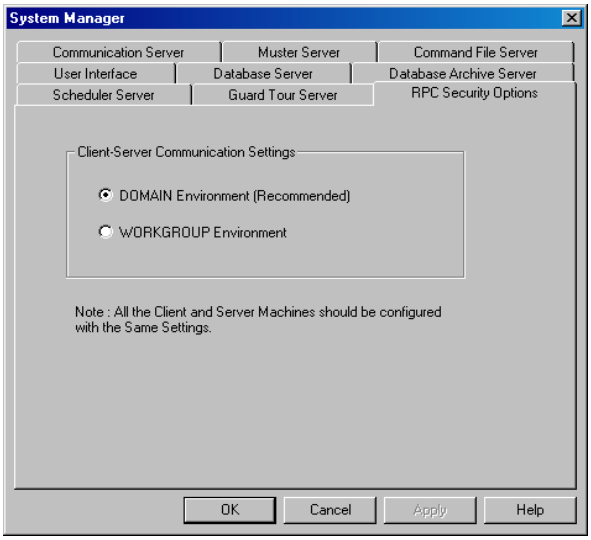
Notes:

- Restart the system to see the changes.
- Log on to WIN-PAK Server System using any account; local or domain. However, the client system must be logged on with the domain user account.

Setting Domain Environment

To set the domain environment:

1. Choose **Start > Programs > Honeywell Access Systems > System Manager**. The **System Manager** window appears.



2. Click **DOMAIN Environment (Recommended)** and click **OK**. This sets the Domain Environment.

Firewall Exception Settings

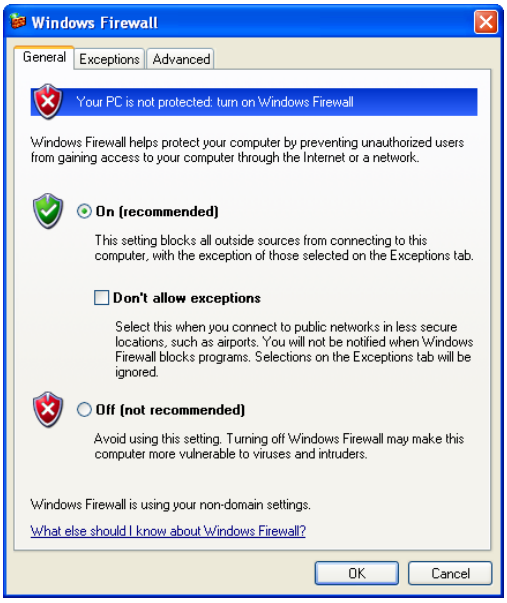
The Windows Firewall protection system blocks the WIN-PAK services in a networked system. Therefore, you must unblock the WIN-PAK services before using WIN-PAK.

Unblocking WIN-PAK Services on Windows XP SP2

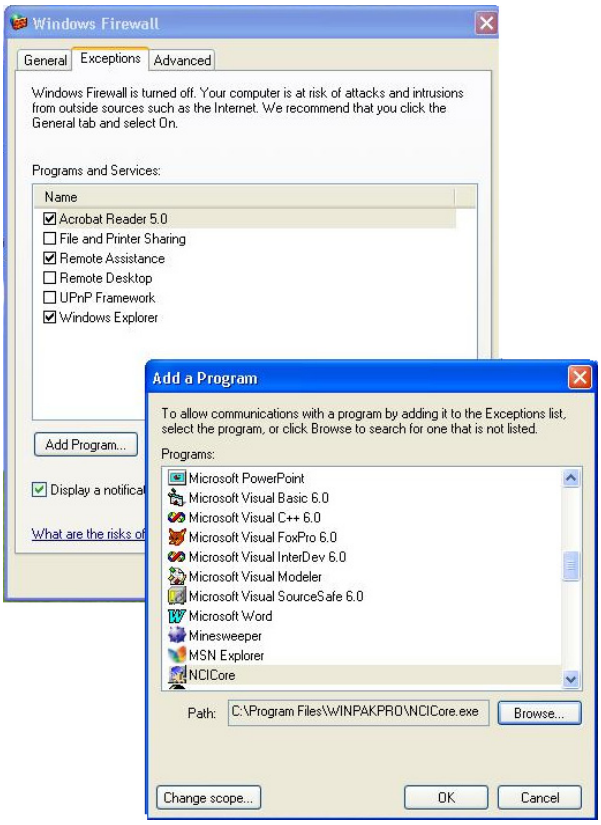
WIN-PAK services must be unblocked, only if the Windows Firewall status is set to **On**. Therefore, check the firewall status in the **Windows Firewall** dialog box.

To check Firewall Status and unblock WIN-PAK Services:

1. Click **Start > Settings > Control Panel** and open **Windows Firewall**. The **Windows Firewall** dialog box appears.
2. Check the status of Windows Firewall. If the option **Off (not recommended)** is set, no need of proceeding further.



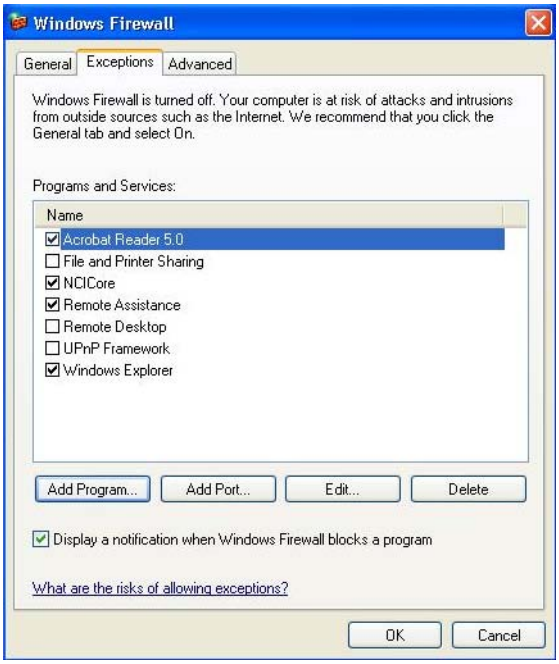
3. Click the **Exceptions** tab and click **Add Program…** to add the WIN-PAK services as exceptions from Windows Firewall protection. The **Add Program** dialog box appears.



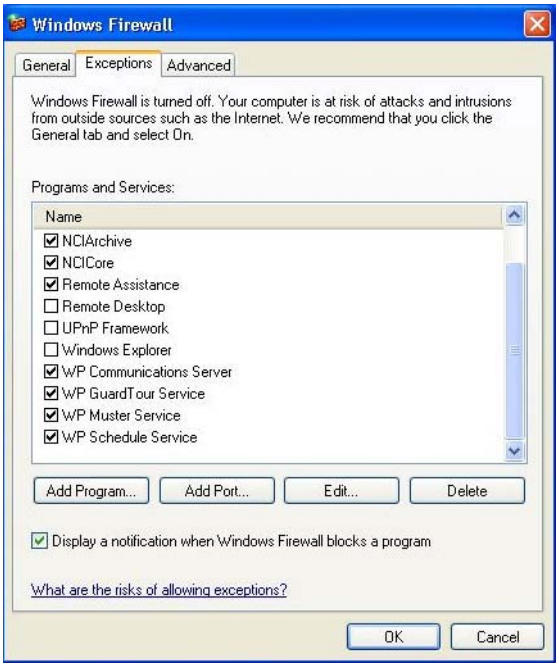
4. Select the following WIN-PAK services and click **OK**.
    - WIN-PAK User Interface
    - NCIArchive
    - NCICore
    - WP CmdFile Service
    - WP Communications Server
    - WP GuardTour Service
    - WP Muster Service
    - WP Schedule Service

    If you do not find the service in the **Programs** list, click **Browse** to locate the service.

Note: As multiple selections are not possible, select the services one at a time and add to the **Programs and Services** list for exceptions.



5. Click the **NCICore** check box to unblock the WIN-PAK Database Server.



6. Click **OK** to save the exceptions for Windows Firewall.

Note: Restart all the services.

Disabling Firewall in Windows 2003 Server

The Windows Firewall must be disabled to access the services. Therefore, check the firewall status in the **Windows Firewall** dialog box.

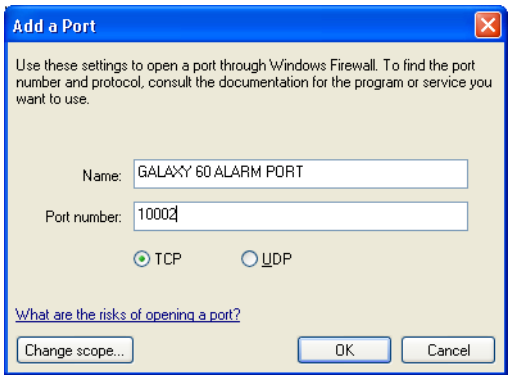
Note: You can disable the firewall status of Windows 2003 server in a similar way as you unblocked the firewall status in Windows XP.

Enabling Ports in Windows XP

Communication ports in a Windows XP operating system are disabled for security reasons by Windows Firewall. These ports must be enabled for remote communication to the Galaxy panel.

To enable ports in the Windows Firewall:

1. Click **Start > Settings > Control Panel** and open **Windows Firewall**. The **Windows Firewall** dialog box appears.
2. Click the **Exceptions** tab and click **Add Port**. The **Add a Port** dialog box appears.



3. Type the **Name** of the port and the **Port Number**.
4. Click **TCP** or **UDP** to select the type of port.
5. Click **OK** to open the port.

Notes:

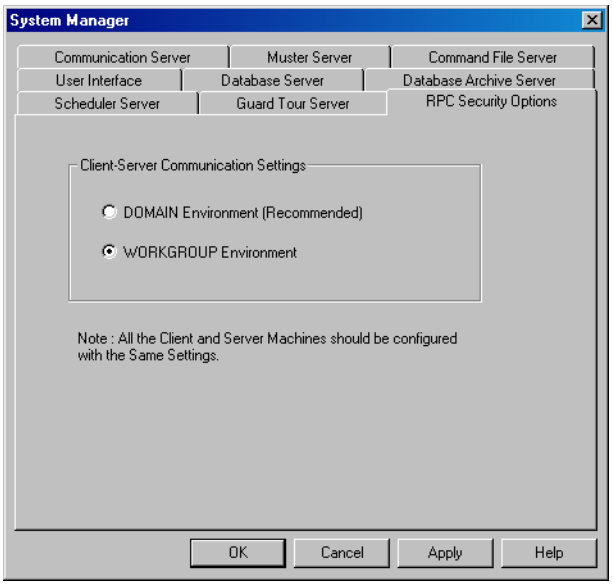
- Repeat the above procedure for enabling three ports in the system, where one port is used by Galaxy Gold and the remaining two ports are used by the Galaxy panel for reporting alarms and control commands.
- In the same way, the 3001 or 2101 ports must be enabled for the TCP/IP communication of the access panels.

WorkGroup Environment

To work in a Workgroup Environment, you must set the workgroup environment and then unblock the WIN-PAK services from Firewall protection.

To set the workgroup environment:

1. Click **Start > Programs > Honeywell Access Systems > System Manager**. The **System Manager** window appears.



2. Click the **RPC Security Options** tab.
3. Under **Client-Server Communication Settings**, click **WORKGROUP Environment** and click **OK**. The Workgroup Environment is set.

Note: WIN-PAK services must be unblocked before proceeding further.

Refer to the "Unblocking WIN-PAK Services on Windows XP SP2" or "Disabling Firewall in Windows 2003 Server" section in this chapter for unblocking firewall.

Comparison between Domain and Workgroup Environment

The following table compares the configuration between Domain Environment and Workgroup Environment:

Table 4-1 Comparing the configuration between Domain Environment and Workgroup Environment

Configuration Type	DOMAIN Environment	WORKGROUP Environment
Communication	The Servers and Clients communicate using the secure RPC connection.	The server and client communicate using an anonymous communication protocol.
Services Configuration	Requires Domain User and password for accessing Server Services.	Does not require Domain User and password for accessing Server Services.

Table 4-1 Comparing the configuration between Domain Environment and Workgroup Environment

Configuration Type	DOMAIN Environment	WORKGROUP Environment
Client Configuration	Requires Domain User Log On for running the UI client.	Does not require Domain User Log On for running the UI client.
Windows Firewall Configuration	Requires unblocking all the WIN-PAK services and client from Windows Firewall protection. **Note:** In Windows Server 2003, disable the Firewall protection to allow DOMAIN connectivity.	Requires unblocking all the WIN-PAK services and client from Windows Firewall protection. **Note:** In Windows Server 2003, disable the Firewall protection to allow WORKGROUP connectivity.

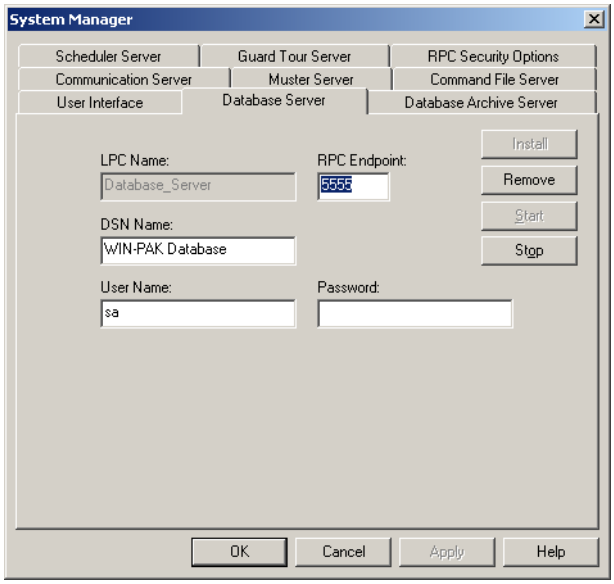
System Manager

The System Manager is a utility in WIN-PAK to locate its various software components. The machine name and protocol end point for each program component is displayed in the System Manager. Honeywell recommends you to retain the default settings.

Setting RPC Endpoints

To set the database server and database archive server RPC endpoints:

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK System Manager**. The **System Manager** window appears.



2. Click the **Database Server** tab.
3. Type the **RPC Endpoint** value. This is the same as TCP/IP port address, which is 5555.

Note: Do NOT change this number unless you have another service using TCP/IP port address 5555.

4. Click the **Database Archive Server** tab.
5. Type the **RPC Endpoint** value. This is the same as TCP/IP port address, which is 5556.

Note: Do NOT change this number unless you have another service using TCP/IP port address 5556.

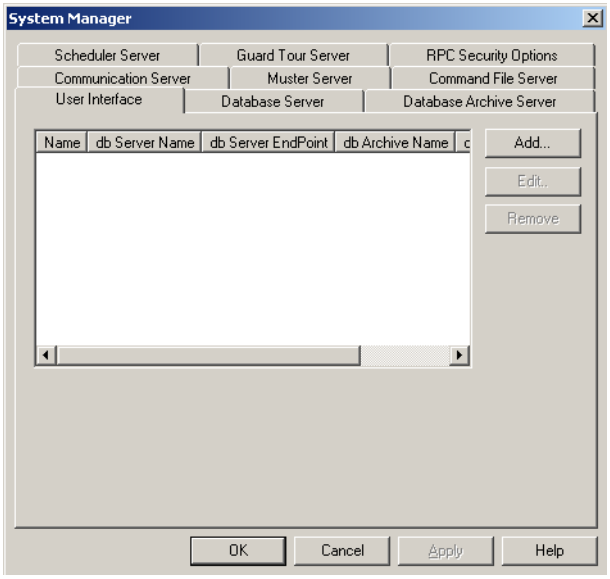
6. Click **OK** to save the changes.

Setting User Interface Workstation

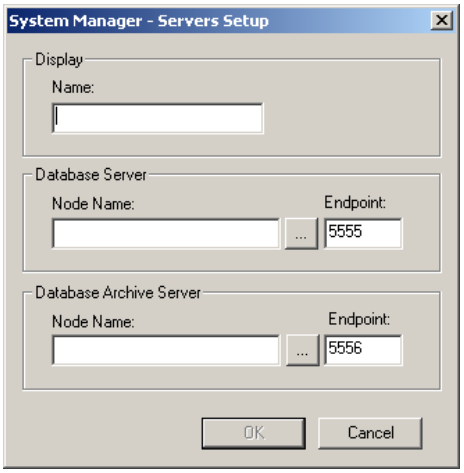
Ensure that you quit the WIN-PAK User Interface, before setting the User Interface workstation.

To set the user interface workstation,

1. Choose **Start > Programs > Honeywell Access Systems > WIN-PAK System Manager**. The **System Manager** window appears.
2. Click the **User Interface** tab.



3. Click **Add**. The **System Manager - Servers Setup** dialog box appears.



4. Enter a descriptive **Name** to identify the database server from the list.
5. Enter the computer name or IP address of the server in the **Node Name** field in the **Database Server** area.

   Ensure that the RPC **Endpoint** is the same as the value you set in "Setting RPC Endpoints" section in this chapter.
6. Under **Database Archive**, type the computer name or IP address of the server in the **Node Name** field.

   Ensure that the RPC **Endpoint** is the same as the value you set in "Setting RPC Endpoints" section in this chapter
7. Click **OK**. This enables you to start up the User Interface with the new database server.

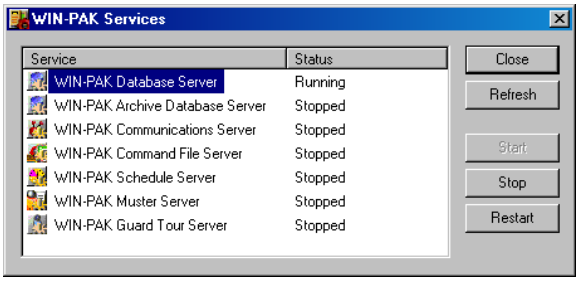
Service Manager

The WIN-PAK Service Manager enables you to start and stop the WIN-PAK services.

To start or stop the WIN-PAK services:

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK Service Manager**. The **WIN-PAK Services** window appears.

   Note: The **Service** column lists the installed components and the **Status** column displays the server status as running or stopped.



2. Select the **Service** to be started or stopped.
3. Click **Start** to start the server or click **Stop** to stop the server.
4. Click **Restart** to stop the service and start again.
5. Click **Refresh** to refresh the services.

User Interface

The WIN-PAK User Interface enables you to add, monitor and control devices, card holders, operators, and so on.

Logging On

Before logging on to WIN-PAK, ensure that all WIN-PAK services are running.

Refer to the "Service Manager" section in this chapter to start the services.

To log on to WIN-PAK:

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK User Interface**. The **Connect to Server** dialog box is displayed.

2. Type the **Name** of the user and the **Password**.

Note: By default, the user name "Admin" and a blank password are created by WIN-PAK for initial log on. However to ensure the security, you must add a password.

3. Click **Connect**. A message about the WIN-PAK demo version is displayed.

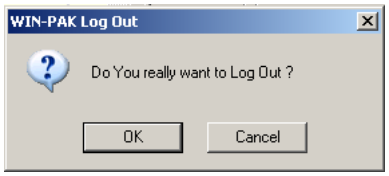
Note: The CD Key becomes invalid, when you uninstall the WIN-PAK system and install it again.

4. Click **OK**. The system connects to the servers and the WIN-PAK User Interface main window appears.

Logging Off

To log off from WIN-PAK:

1. In the WIN-PAK User Interface main window, choose **File > Log Out** or click from the toolbar. The confirmation dialog box appears.



2. Click **Yes** to confirm logging off from WIN-PAK.

Note: Logging Off from WIN-PAK does not automatically stop the WIN-PAK services.

Quitting WIN-PAK

To quit the WIN-PAK application:

1. Choose **File > Exit**. A message asking for confirmation appears.
2. Click **Yes** to quit the application.

System Settings

5

In this chapter...

Overview

This chapter describes how to configure WIN-PAK users and to set the default settings for WIN-PAK.

Accounts

This section Accounts describes to add, edit and delete an account. The card and card holder information in WIN-PAK are specific to an account. Therefore, you must select an account to enable card and card holder menu options.

WIN-PAK Users

This section WIN-PAK Users describes in detail about configuring the users and assigning privileges to them.

Users of WIN-PAK are of two types, namely, Administrators and Operators. An administrator has full privileges (view, change, and delete) to work in WIN-PAK whereas, an operator has restricted privileges, which are defined by the associated operator levels.

When you install WIN-PAK on your computer, a default user is created for logging on to WIN-PAK with administrator privileges. The default user name is **admin** with a blank password. However, to ensure security, you can change the user name and password.

Default Settings

This section describes how to change the default settings for WIN-PAK workstation and system settings. Defaults can be changed for alarm printer, sound files, e-mails for reporting alarms, auto log on, and so on.

In the WIN-PAK system, these settings are configured by default and WIN-PAK functions as per these settings. All the client systems of WIN-PAK would be affected by any changes made to the System Defaults settings. Whereas, only the computer where the settings are changed are affected by the Workstation Defaults settings.

Accounts

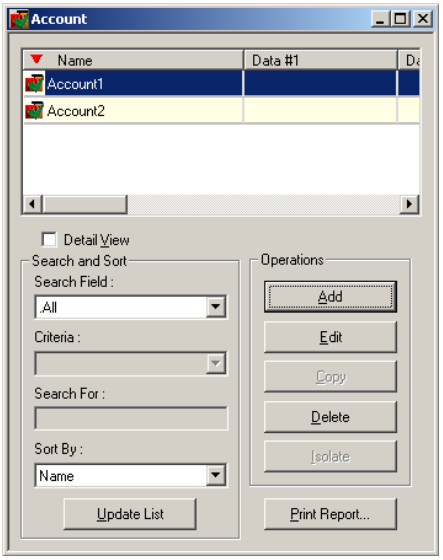
Using accounts in WIN-PAK, you can group cards and card holders, whose details can be modified by specific operators. An account can be created with an account name and mapped to the operators who can access the account.

Newly added cards and cardholders must be added to the specific account. Therefore, card holder tab menus in the WIN-PAK UI are available only when an account is selected.

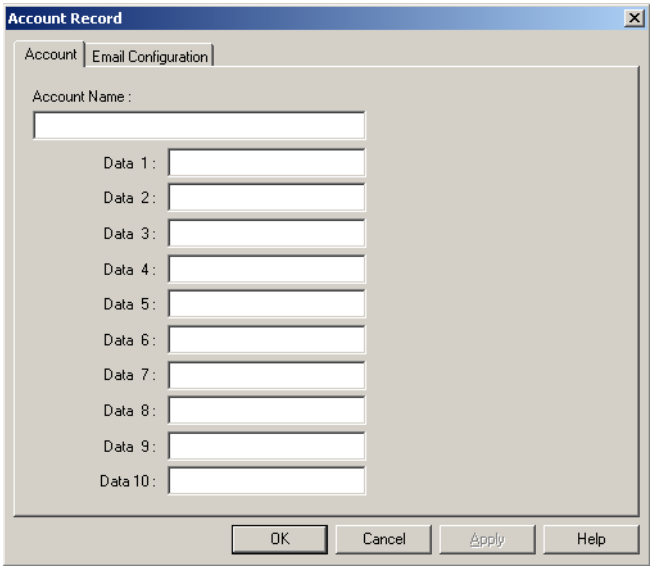
Adding an Account

To add an account:

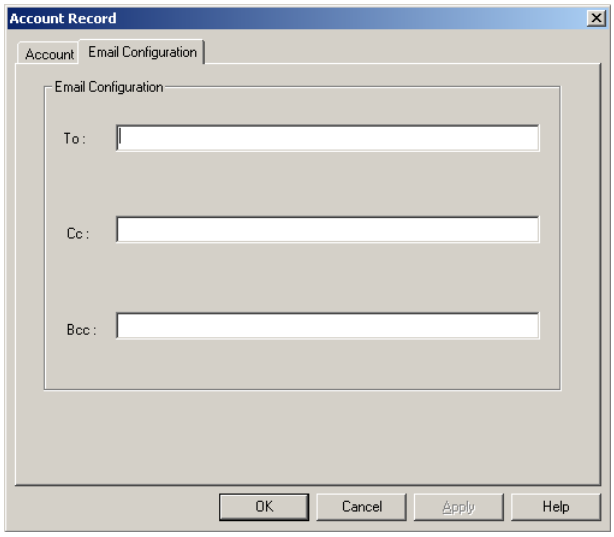
1. Choose **Account** > **Edit**. The **Account** window opens.



2. Click **Add** to add a new account. The **Account** dialog box opens.



3. In the **Account** tab, type the **Account Name**. The account name may include a maximum of 30 characters and is mandatory.
4. Enter the additional information about the account from **Data 1** to **Data 10**. For example, you can enter the category of the account, site name, and so on.
5. Click the **Email Configuration** tab to enter the e-mail Ids.



6. In the **To** box, type the e-mail ID of the user to whom the account-specific alarms must be reported.

Note: You can enter multiple e-mail IDs separated by semi-colons. In the Cc and Bcc fields, you can type the e-mail IDs of the users to whom the copy of the mails must be sent.

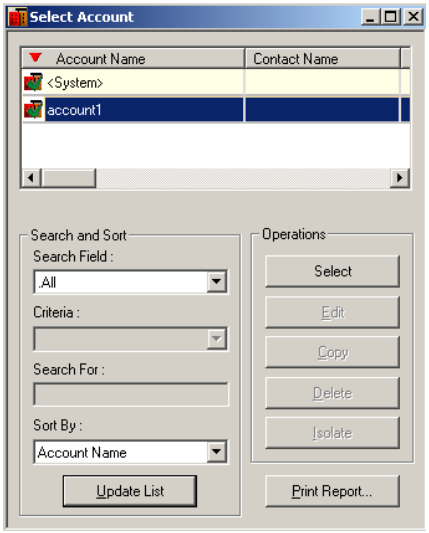
7. Click **OK** to save the account information.

Note: Select the required account before entering an account-sensitive information.

Selecting an Account

To select an account in WINPAK:

1. Choose **Account** > **Select** or press **F2**. The **Account** window opens.



2. In the **Account Name** list select the required account.
3. Click **Select**.

Note: Alternatively, double-click the required account to select it.

Editing an Account

To edit an account in WINPAK:

1. Choose **Account** > **Edit**. The **Account** window opens.
2. Click the required account to be edited and click the **Edit** button.

   Refer to the "Adding an Account" section in this chapter for more details on editing an account.

Deleting an Account

To delete an account that is not in use in WINPAK:

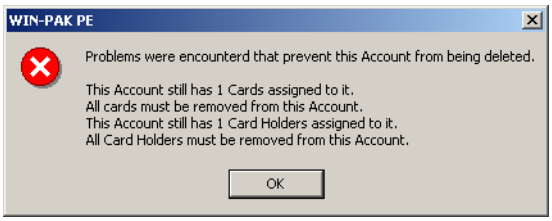
1. Choose **Account** > **Edit**. The **Account** window opens.
2. Click the account you want to delete and click the **Delete** button.

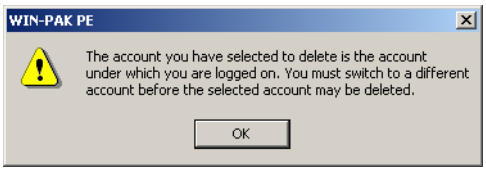
Note: A message box appears indicating that the account cannot be deleted, if the account you delete:

- is used by one or more entities in the system. (To delete this account, you must remove all the dependencies.)

  OR

- is active. (To delete this account, you must switch to a different account.)



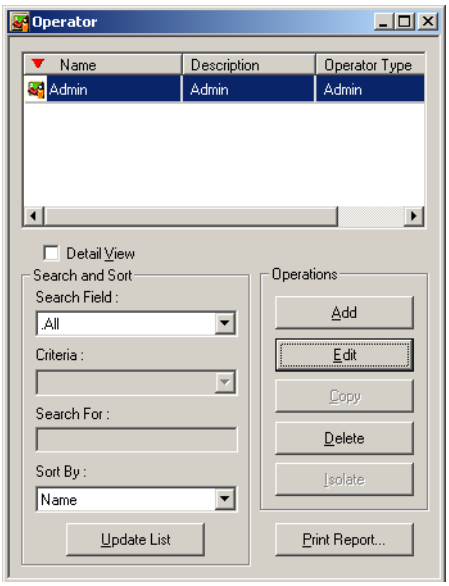


Administrators

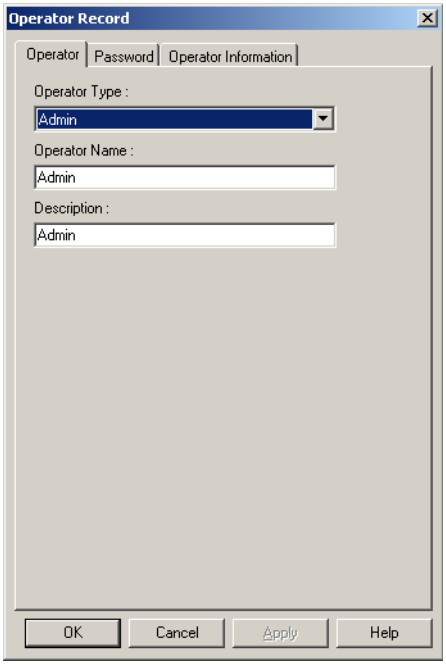
Administrator is created by default by WIN-PAK on installing the WIN-PAK User Interface. The user name is admin with no password. You can change the user name and password to ensure security.

To change the default settings for Administrator:

1. Choose **System > Operator**. The **Operator** window appears.

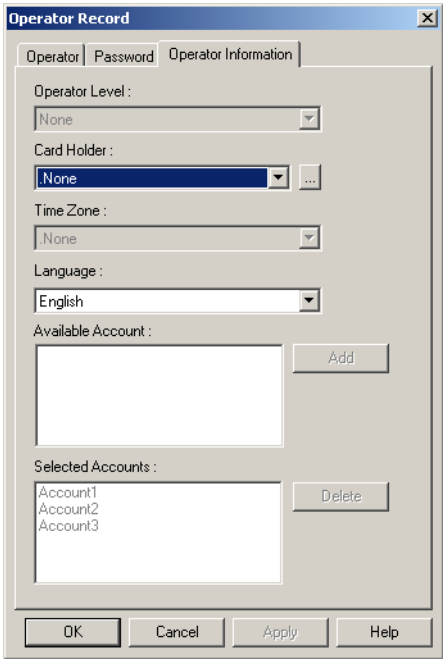


2. Select the **Admin** operator and click **Edit**.



3. In the **Operator** tab, change the **Operator Type**, **Operator Name** and **Description,** if required.
4. Click the **Password** tab to set the new password for the Administrator.
    a. Type the **New Password** for the Administrator to log on. This field is mandatory. Password is case-sensitive and you can enter maximum of 20 characters.
    b. Retype the password in **Confirm New Password**.

5. Click the **Operator Information** tab to set the operator details such as operator level, time zone during which the operator is provided access to work on WIN-PAK, the relevant accounts, and so on.



Note: The Operator Level, Time Zone, and Account options are enabled in the **Operator Information** tab only when you change the role (operator type) of the user from **Admin** to **Operator** in the Operator tab.

6. If the Administrator is a card holder, select the card holder in the **Card Holder** list or use the ellipsis button to locate the Administrator in the card holders list.
7. Select the **Language** of the Administrator.
8. Click **OK** to save the changes.

Note: If you select the operator type as **Operator**, you must select the following:

- **Operator Level** to be assigned to the operator.
- **Time Zone** during which the operator is given card access.
- **Accounts** that must be associated to the operator.

Operators

Operators are the individuals with a set of privileges to work with the WIN-PAK system. An operator can log on to WIN-PAK using a user name and password. Operators are assigned by operator levels, where the access rights are configured for the WIN-PAK system components.

Operator Levels

The operator level defines the privileges of the operator to work with WIN-PAK. When an operator is assigned to an operator level, the operator gains access for the system components that are configured in the operator level.

In an operator level, the rights are configured for the following system components:

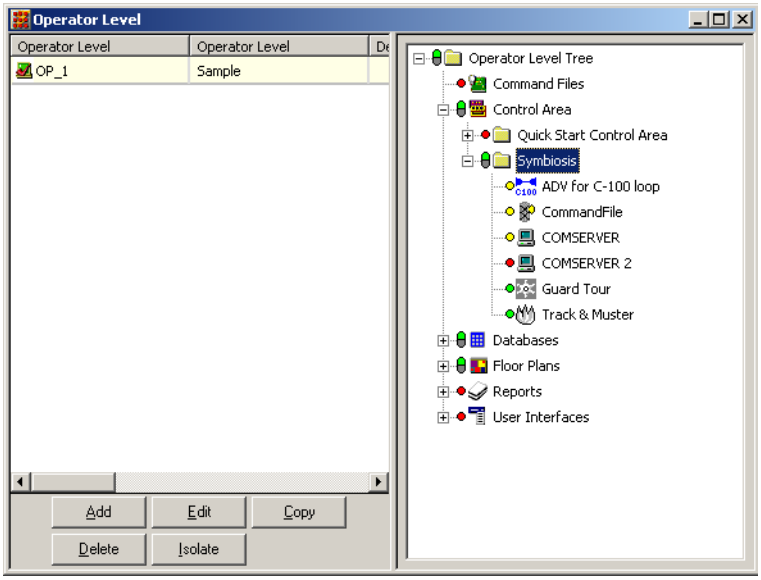
- **Command Files** - To run the command files.
- **Control Area** - To control devices in the control area through Control Map.
- **Databases** - To configure Card Holder, Cards, Floor Plan, and so on.
- **Floor Plans** - To open the floor plans.
- **Reports** - To run the reports.
- **User Interfaces** - To configure and operate on the WIN-PAK User Interface.

Note: Before you define the operator levels, ensure that you have defined the control areas for defining privileges for the areas in the Operator Level window.

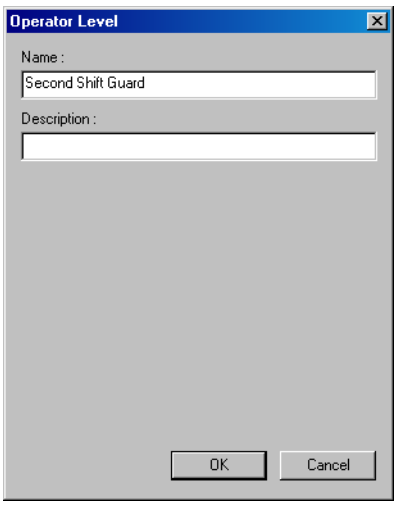
Adding an Operator Level

To add an operator level:

1. Choose **System > Operator Level**. The **Operator Level** window appears.



2. Click **Add** to add a new operator level. The **Operator Level** dialog box appears.



3. Type the **Name** for the operator level. This field is mandatory.
4. Type the **Description** for the operator level.
5. Click **OK** to save and return to the **Operator Level** window.

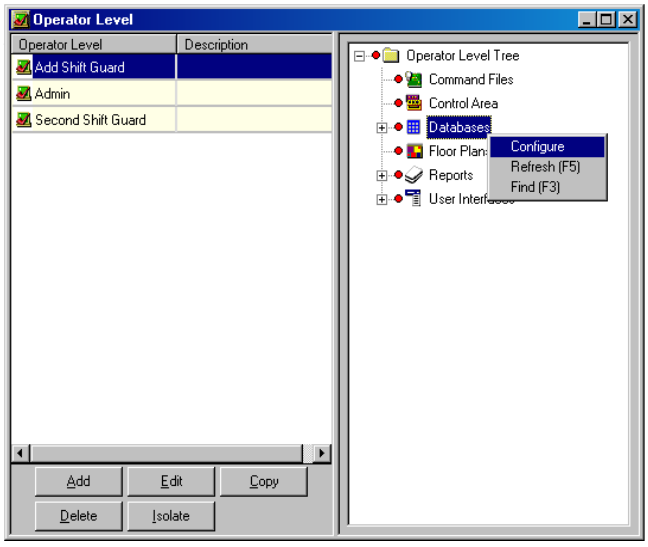
Configuring Operator Levels

You can configure the access rights to an operator level for the control area devices, databases, reports, user interface, and so on.

To configure access rights for an operator level:

1. Choose **System > Operator Level**. The **Operator Level** window appears.

Note: The Operator Level window is divided into two panes, the left-pane and the right-pane. The left-pane displays the list of operator levels and the right-pane displays the operator level tree in which you can set the access rights for the selected operator level.

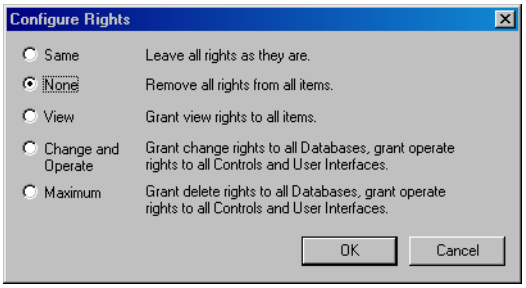


2. In the left-pane, select an operator level in the **Operator Level** list.
3. Right-click the control area device, database, or user interface to configure.
4. Configure rights for an entire branch, an individual device, database, report or user interface element.

Configuring rights for an entire branch

To configure access rights for an entire branch:

1. In the **Operator Level** window, right-click the main branch and select **Configure** to configure the rights for all the devices in one branch at once. The **Configure Rights** dialog box is displayed.

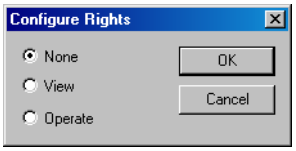


2. Select the appropriate rights configuration for the Operator Level and click **OK**.

Configuring rights for an individual device

To configure access rights at a device level:

1. In the **Operator Level** window, expand the branch and select a device.
2. Right-click the device and select **Configure**. The **Configure Rights** dialog box appears.

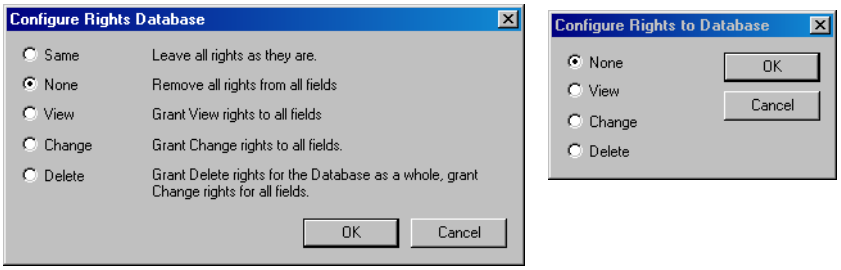


3. Select the appropriate rights configuration and click **OK**.

Configuring rights for databases

To configure rights for databases:

1. In the **Operator Level** window, expand the **Databases** branch and select a branch database or an individual database.
2. Right-click the database and select **Configure**. The **Configure Rights Database** dialog box appears for a branch database and the **Configure Rights to Database** dialog box appears for an individual database.

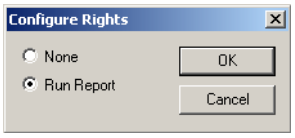


3. Select the appropriate option to set the rights for the database.

Configuring rights for reports

To assign rights to an individual report:

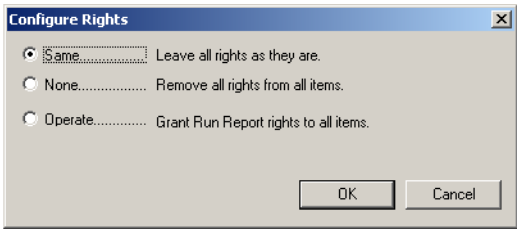
1. In the **Operator Level** window, expand the **Reports** branch and select a report.
2. Right-click the report and select **Configure**. The **Configure Rights** dialog box appears.



3. Click **None** to provide no access or click **Run Report** to provide rights for running the selected report.
4. Click **OK**.

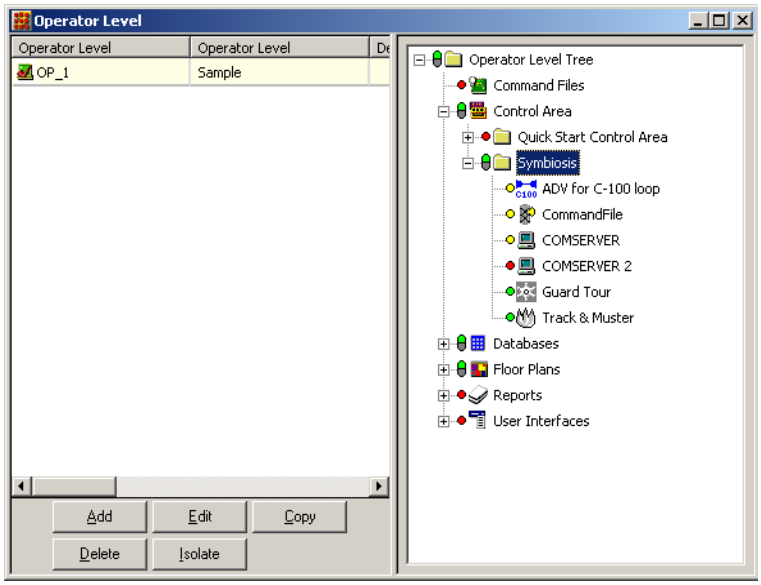
To assign the same rights to all the reports:

1. In the **Operator Level** window, select the **Reports** branch.
2. Right-click **Reports** and click **Configure**. The **Configure Rights** dialog box appears.



3. Select the appropriate option and click **OK**. The selected rights is assigned to all the reports.

Note: Each device, database, and user interface element in the control tree is color-coded, based on the rights assigned to it.



- Red indicates no rights
- Yellow indicates view rights
- Green indicates operate rights (view and edit)
- White indicates delete rights

Configuring rights summary chart

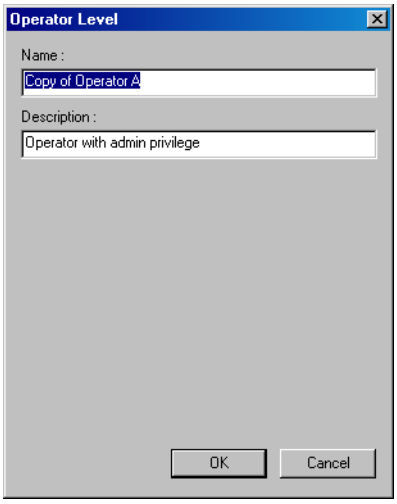
Branch, Database, Device	Change Operate	Delete	Max	None	Operate Specific	Same	View
Operator Level Tree	x		x	x		x	x
Command File Individual Command File				x x	x x	x	
Control Area Device-Control Area				x x	x x	x x	x x
Database Individual Database	x x	x x		x x		x	x x
Floor Plans Individual Floor Plans				x x	x x	x	
Reports Individual Reports				x x	x x	x	
User Interface Individual-User Interface				x x	x x	x	x x

Options	Description
Change & Operate	Grant change rights to all database. Grant operate rights to all controls and user interfaces.
Delete	Grant delete rights for all database as a whole. Grant change rights for all fields.
Maximum	Grant delete rights to all databases. Grant operate rights to all controls and user interfaces.
None	Remove all rights from all items.
Operate Specific	Grant operate rights to all items from branch or specific devices.
Same	Leave all rights as they are.
View	Grant view rights to all items.

Copying an Operator Level

To create operator levels that are similar to each other, but with a few minor differences, copy an existing operator level, and then make changes to the copy.

1. Choose **System > Operator Level**. The **Operator Level** window appears.
2. Select the operator level to be duplicated.
3. Click **Copy**. The **Operator Level** dialog box appears.



4. Type a new **Name** for the operator level.

   The default name of the copy is the same as the original with the prefix "Copy of..." and the default description is the same as the original.
5. Type a new **Description** for the operator level, if required.
6. Click **OK** to save a copy and return to the **Operator Level** window.

Note: The access rights for the copy is the same as the original. If you want to change the access rights, you can select the copied operator level and configure the new access rights.

Editing an Operator Level

To edit the name or description of an operator level:

1. Choose **System > Operator Level**. The **Operator Level** window appears.
2. Select the operator level and click **Edit**. The **Operator Level** dialog box appears.
3. Enter the new **Name** and/or **Description**, and click **OK**.

Note: To edit the access rights of an operator level, you can select the operator level and configure new access rights.

Refer to the "Configuring Operator Levels" section in this chapter for details on configuring access rights to an operator level.

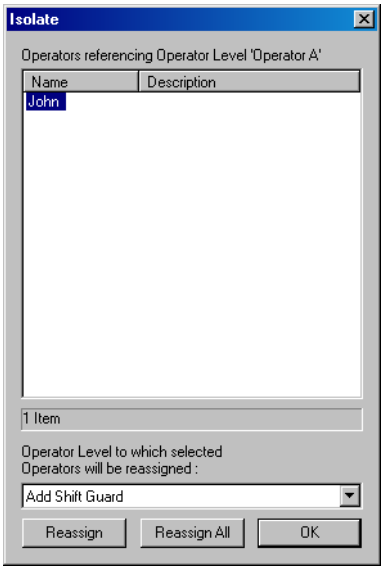
Isolating and Deleting an Operator Level

You cannot delete an operator level, if the operator level is already assigned to an operator. Therefore, before deleting an operator level, reassign the operator to a different operator level.

Isolating an operator level

To reassign operators to a different operator level and to isolate the operator level:

1. Choose **System > Operator Level**. The **Operator Level** window appears.
2. Select the operator level to be isolated and click **Isolate**. The **Isolate** dialog box appears.



3. Select the operator from the list. For multiple selections, press SHIFT or CTRL key while selecting the operators.
4. Select the different operator level to which the operators must be assigned.
5. Click **Reassign** to reassign the selected operators. A message asking for confirmation appears.

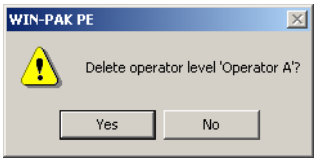
   OR

   Click **Reassign All** to reassign all the operators. A message asking for confirmation appears.
6. In the confirmation message, click **OK** to confirm the reassignment. The selected or all the operator levels are reassigned.
7. Click **OK** to return to the **Operator Level** window.

Deleting an operator level

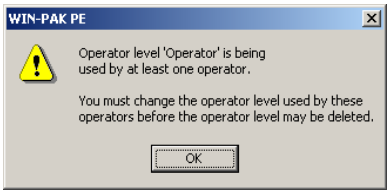
To delete an operator level:

1. Select an operator level from the database list and click **Delete**. A message asking for confirmation appears.



2. Click **Yes** to confirm the deletion. The operator level is deleted.

Note: If you attempt to delete an operator level that is used for defining an operator, the following warning message appears:



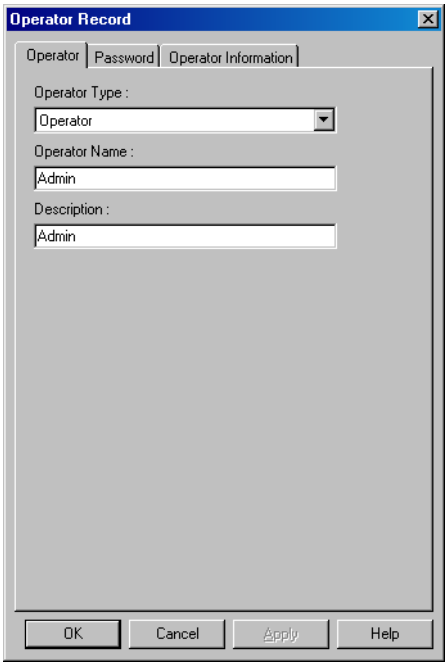
Defining Operators

The operators can gain access to various functions of WIN-PAK, based on the associated operator level and the rights assigned to that level.

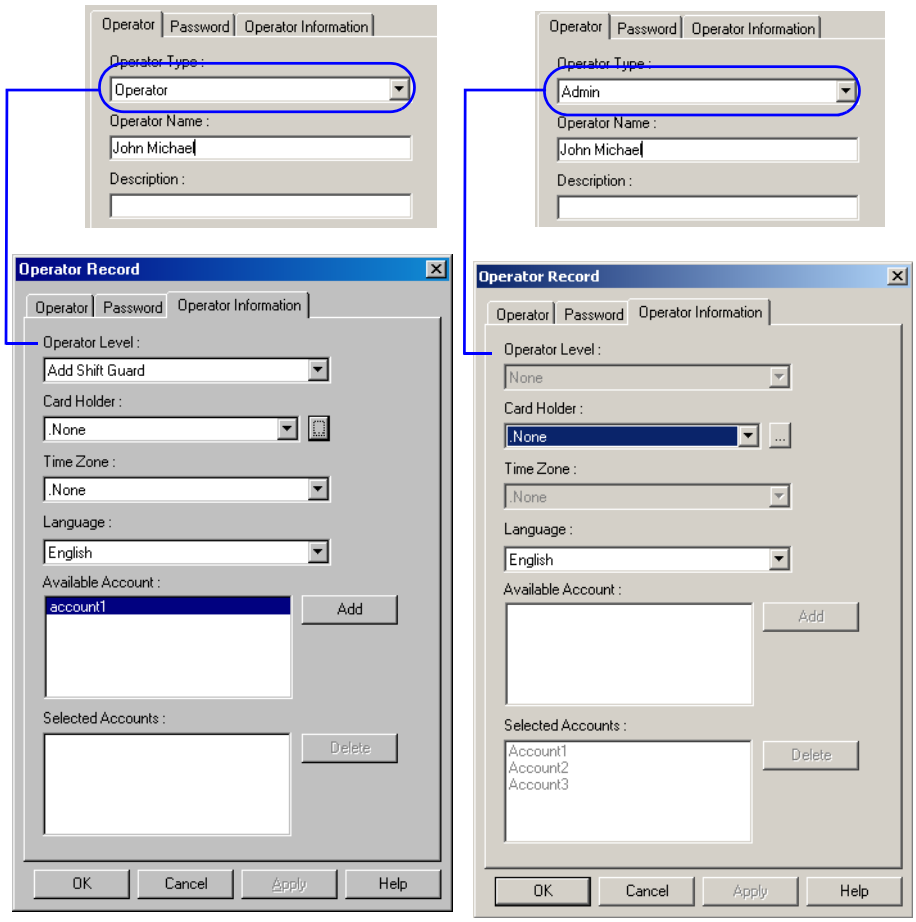
Adding an Operator

To add an operator:

1. Choose **System > Operator**. The **Operator** window appears.
2. Click **Add** to display the **Operator Record** dialog box.



3. In the **Operator** tab, select the **Operator Type** as **Admin** or **Operator**.
4. Type the **Operator Name** and **Description**.
5. Click the **Password** tab to set the password.
    a. Type the **New Password** for the operator to log on. This field is mandatory. Password is case-sensitive and you can enter maximum of 20 characters.
    b. Retype the password in **Confirm New Password**.
6. Click the **Operator Information** tab. The field inside this tab varies according to the operator type.



Operator **Administrator**

7. Select an operator level in the **Operator Level** list to assign access rights to the operator.

   Note: The **Administrator** has rights to view, edit, and delete in WIN-PAK and so the Operator Level, Time Zone, and Accounts options are not applicable for the Administrator.

8. If the operator is also a card holder, select the **Card Holder** from the list or use the ellipsis [...] button to locate the operator in the card holder list.

9. Select the **Time Zone** during which the operator has to log on to the system.

   Note: If no time zone is assigned to an operator, the operator can log on to WIN-PAK any time.

10. Select the language of the operator in the **Language** list.

11. Under **Available Account**, select the list of accounts to which the operator can have access and then click **Add**. The accounts are moved to **Selected Accounts**.

12. If you want to remove an account from **Selected Accounts** list, select the account and click **Remove**. The selected account is moved to **Available Accounts**.

13. Click **OK** to add the operator.

Tips on Password

A good strategy for choosing a password is, it must be easy to remember, but hard to decode. The following list provides tips on choosing such a password:

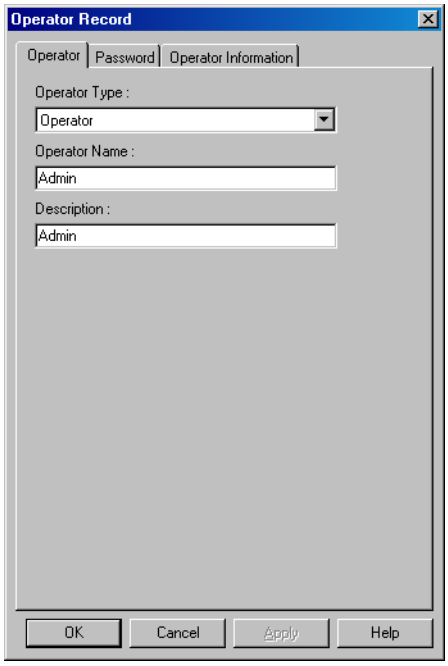
- Pick a simple phrase preceded or followed by one or more numbers.
- Use a password without spaces and capitalize each character. Such passwords cannot be easily decoded either by a random number generator or by a dictionary decoder.
- For tight security, use a combination of both letters and numbers. Avoid familiar terms such as your company name, initials, birth dates, and so on.

Caution: Passwords are case-sensitive.

Editing an Operator

To edit the operator details:

1. Choose **System > Operator**. The **Operator** window appears.
2. Select the operator to be edited and click **Edit**. The **Operator Record** dialog box appears.



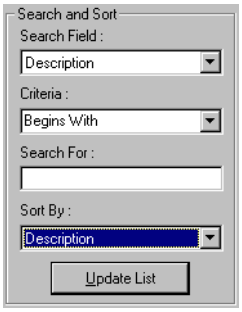
3. Edit the required details of an operator and click **OK**.

Refer to the "Adding an Operator" section in this chapter for details on adding an operator.

Searching and Sorting Operators

To search and sort the operator list:

1. Choose **System > Operator**. The **Operator** window appears.
2. Select an item in the **Search Field** list.



- **All** - Lists all the operators.
- **Description** - Searches for similar descriptions.
- **Last Log In** - Searches based on the last log on date and time.
- **Name** - Searches for similar operator names
- **Operator Type** - Searches based on the operator type.

3. If you have selected Description, Last Log In, Name or Operator in the Search Field, select the **Criteria**.
   - **Begins With** - Searches for an item that begins with the text in the **Search For** text box.
   - **Equals** - Searches for an item that exactly matches with the text in the **Search For** text box.
   - **Greater Than** - Searches for an item that is alphabetically or numerically greater than the text in the **Search For** text box.
   - **Less Than** - Searches for an item that is alphabetically or numerically less than the text in the **Search For** text box.
4. Type the text to be searched in the **Search For** text box.

Note: If you have selected **Last Log In** in the **Search Field** list, click the button below **Search For** and select the date.

5. Select an item in the **Sort By** list.
   - **.None** - No sorting required.
   - Other items - Sorts the list in the ascending order of the selected item.
6. Click **Update List** to list the searched items in the sorted order.

Tip:

- To sort the entire list:
  a. Click the column title. The list is sorted in the ascending order of the column.

     OR

Select **All** in the **Search Field** list.

Select an item in the **Sort By** list.

Click **Update List**. The entire list is sorted based on the selected item.

- To view the list of operators who have not yet logged on:
  a. Select **All** in the **Search Field** list and select **Last Log In** in the **Sort By** list.
  b. Click **Update List**. The **Not Yet Logged In** operators are displayed first in the list.

Deleting an Operator

To delete an operator:

1. Choose **System > Operator**. The **Operator** window appears.
2. Select the operator to be deleted and click **Delete**. The selected operator is deleted.

Default Settings

Defaults can be set for certain system functions in WIN-PAK. However, you can change these default settings. For example, you can set the deletion of a card without asking for a confirmation message.

WIN-PAK menus for configuring workstation and system settings are:

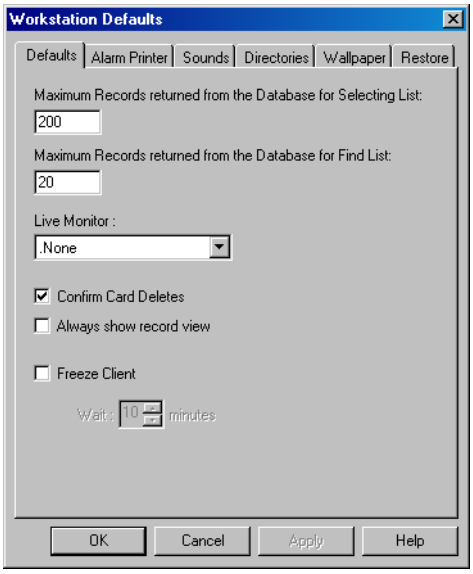
- Workstation Defaults
- System Defaults

Setting Workstation Defaults

Defaults can be set for alarm printer, sound files, paths, wallpapers and restore options.

To set the workstation defaults:

1. Choose **System > Workstation Defaults**. The **Workstation Defaults** dialog box appears.



2. Click each tab to configure or change the default settings.
3. Click **Apply** to save the settings.

Configuring default workstation settings

To configure the default workstation settings:

1. In the **Workstation Defaults** dialog box, click the **Defaults** tab.
2. Set the following settings:

Table 5-1 Describing options for setting defaults

Defaults Option	Description
Maximum Records returned from the Database for Selecting List	The maximum number of records to be displayed in the Maintenance window for Selection list. Enter a number between 20 and 200. Default value is 200.
Maximum Records returned from the Database for Find List	The maximum number of records to be displayed in the Maintenance window for Find list. Enter a number between 1 and 1000. Default value is 20
Live Monitor	From the defined list of CCTV monitors, the selected monitor output is connected to the video capture card. Therefore, the video signal from that monitor output is displayed in the Live Monitor view. Default is None.

Table 5-1 Describing options for setting defaults

Defaults Option	Description
Confirm Card Deletes	A message asking for confirmation appears, when you attempt to delete a card. By default, this check box appears selected.
Always Show Record View	When you open the Maintenance window, the Detail window for the selected item is opened simultaneously. By default, this check box appears cleared.
Freeze Client and Wait	If the operator leaves the WIN-PAK User Interface idle for a certain period, the session expires. Therefore, the operator must log on to the system again. By default, this check box appears cleared. The period for inactivity is set in the **Wait** box. The period ranges from 1 to 60 minutes. Default value is 10 minutes.

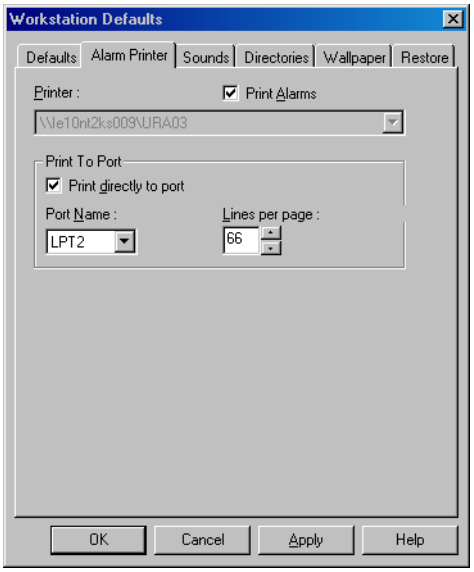
3. Click **Apply** to save the changes.

Setting defaults for alarm printers

By default, alarms are displayed only in the alarm view window and are not printed. If required, you can configure the settings in the alarm printer to print all alarms as soon as they are displayed in the alarm view window.

To configure alarm printer settings:

1. In the **Workstation Defaults** dialog box, click the **Alarm Printer** tab.



2. Select the **Print Alarms** check box to print the alarms.
3. To select a local printer:

    a. In the **Printer** list, select a printer from the list of printers installed in Windows.

    OR

    To select a printer in the network:

    a. Under **Print to Port**, select the **Print directly to port** check box.

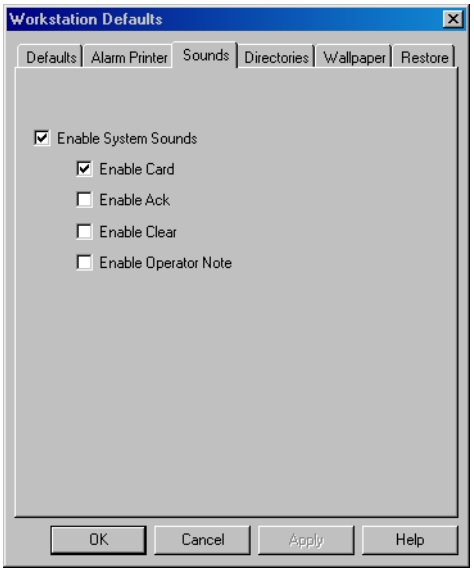
    b. In the **Port Name** list, select the name of the port connected to a printer.

    c. In the **Lines per page** box, enter the number of lines to be printed in a page. By default, it is 66.
4. Click **Apply** to save the changes.

Setting defaults sound settings

To activate sound files on certain instances:

1. In the **Workstation Defaults** dialog box, click the **Sounds** tab.



2. Select the **Enable System Sounds** check box.
3. Specify the instances during which sound files must be activated by selecting the following check boxes:

Table 5-2 Describing instances for activating a sound file

Instance	Activates a sound file...
Enable Card	During card reads.

Table 5-2 Describing instances for activating a sound file

Instance	Activates a sound file...
Enable Ack	When alarms are acknowledged.
Enable Clear	When alarms are cleared.
Enable Operator Note	When notes are added to alarms.

4. Click **Apply** to save the sound file settings.

Note: The sound card must be available in the operating system to enable the sound option.

Setting default paths for sound and language files

To define default paths for the sound files and language files:

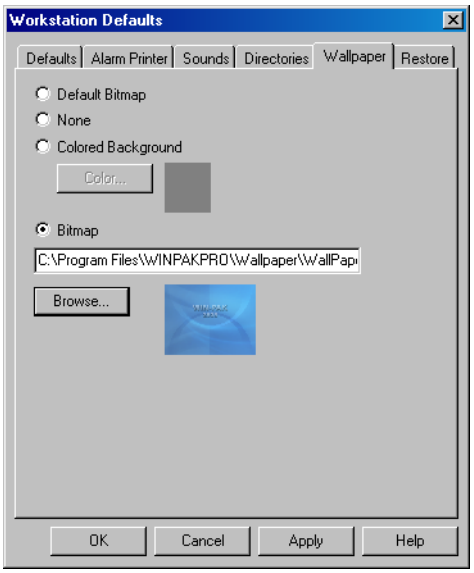
1. In the **Workstation Defaults** dialog box, click the **Directories** tab.

2. In **Path to Sound Files** text box, type the path for the sound files or click **Browse** to locate the sound files folder. By default the path is set to C:\Program Files\WINPAKPRO\Sound Files.
3. In **Path to Language Files** text box, type the path for the language files or click **Browse** to locate the language files folder. By default the path is set to C:\Program Files\WINPAKPRO\Language Files.
4. Click **Apply** to save the changes.

Setting the default wallpaper for WIN-PAK User Interface

To set the default wallpaper for WIN-PAK:

1. In the **Workstation Defaults** dialog box, click the **Wallpaper** tab.



2. Click any of the following options for setting wallpaper defaults:

Table 5-3 Describing options for setting wallpaper

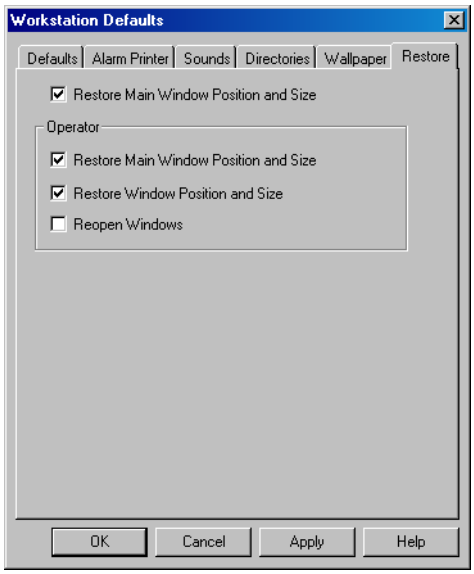
Wallpaper Option	Description
Default Bitmap	Retains the default bitmap set for the User Interface.
None	No wallpaper is set for the User Interface.
Colored Background	Sets a wallpaper color for the User Interface. Click **Color** and choose the background color.
Bitmap	Set a bitmap as a background for the User Interface. When you select this option, type the path of the image file, or click **Browse** to locate the image file.

3. Click **Apply** to save the wallpaper settings.

Setting defaults for Restore options

To configure the restore options in the WIN-PAK User Interface:

1. In the **Workstation Defaults** dialog box, click the **Restore** tab.



2. To set the restore option for the main window before logging on to the WIN-PAK system:
    a. Select the **Restore Main Window Position and Size** check box to retain the last size and position of the main window.
3. To set the restore options after logging on to the WIN-PAK system:
    a. Under **Operator**, select the following restore options:

Table 5-4 Describing restore options for operators

Restore Option	Description
Restore Main Window Position and Size	The position and size of the main window in the previous session are restored.
Restore Window Position and Size	The position and size of the secondary windows in the previous session are restored.
Reopen Window	The windows that were kept open in the previous session are re-opened.

4. Click **Apply** to save the restore settings.
5. Click **OK** to save the workstation settings and close the dialog box.

Setting System Defaults

Defaults can be set for certain functions in WIN-PAK. For example, you can configure system settings related to ADV access, card number length, alarm handling, e-mail configuration, and type of access levels.

To set the system defaults:

1. Choose **System > System Defaults**. The **System Config** dialog box appears.

2. Click each tab and configure the settings.
3. Click **OK** to save the system default settings.

Configuring default settings

To configure the defaults settings:

1. In the **System Config** dialog box, click the **Defaults** tab.
2. Set the following defaults options:

Table 5-5 Describing the options for setting the defaults

Defaults Option	Description
Grant all operators access to ADV not in Control Area	Select the check box to grant permission to all operators for accessing ADVs that are not in the Control Area
Maximum Length of Card Numbers	The maximum length for card numbers.

Table 5-5 Describing the options for setting the defaults

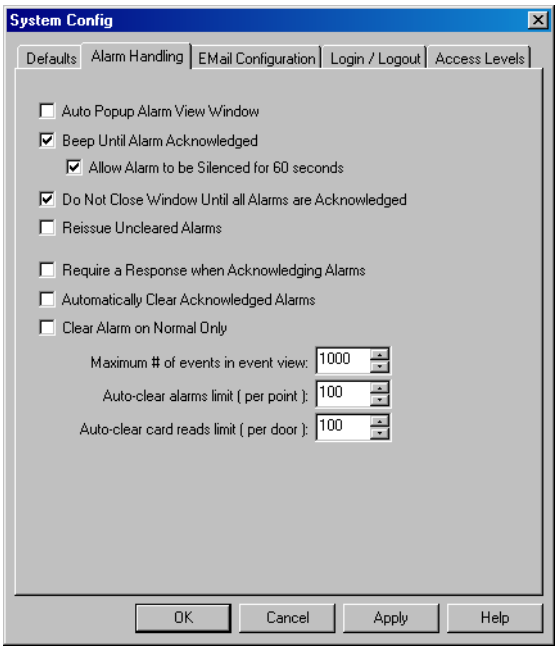
Defaults Option	Description
Allow only numeric Card Numbers	Card numbers can only be numbers.
Port Settings	
Port for TCP/IP Connection	The port number of the panels in the TCP/IP connection.
Port for TCP/IP Encrypted Connection	The port number of the panels in the TCP/IP encrypted connection.

3. Click **Apply** to save the defaults settings.

Setting defaults for alarm handling

To set defaults for alarm handling:

1. In the **System Config** dialog box, click the **Alarm Handling** tab.



2. Set the following alarm settings:

Table 5-6 Describing options for alarm settings

Alarm Options	Description
Auto Popup Alarm View Window	When a new alarm is received, the Alarm View window is opened, restored or continues its display. By default this check box appears selected.

Table 5-6 Describing options for alarm settings

Alarm Options	Description
Beep until Alarm Acknowledged	The alarm beeps continuously, until the alarm is acknowledged. By default it is selected.
Allow Alarm to be Silenced for 60 seconds	The Silence button appears enabled for an operator to stop the beep for 60 seconds even without acknowledging the alarm. By default it is selected.
Do Not Close Window Until all Alarms are Acknowledged	The Alarm View window cannot be closed, until all the alarms are acknowledged.
Reissue Uncleared Alarms	The acknowledged alarms are reissued if those alarms in the lower-pane returns to the alert state.
Require a Response when Acknowledging Alarms	A note must be provided when alarms are acknowledged.
Automatically Clear Acknowledged Alarms	Acknowledged alarms are automatically cleared.
Clear Alarm on Normal Only	The operator can clear an alarm, only if the device or or point on which the alarm is generated retains to the normal state.
Maximum # of events in event view	The maximum number of events to be displayed in the Event View.
Auto-clear alarms limit (per point)	The maximum number of recent alarms for a point (input or output) to be displayed in the Alarm View window. By default, the Alarm View window displays the 100 most recent alarms per point. This value can range from 10 through 500. **Note:** The alarm count (**Cnt**) shows the entire count of the alarms irrespective of the limit setting.
Auto-clear card reads limit (per door)	The maximum number of recent events per door to be displayed in the Alarm View window. By default, the Alarm View window displays the 100 most recent events per door. This value can range from 10 through 500.

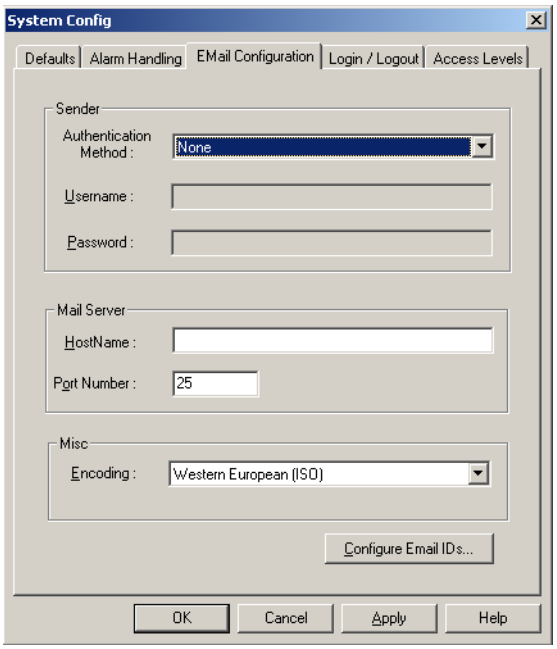
3. Click **Apply** to save the alarm handling settings.

Specifying default e-mail IDs for reporting alarms

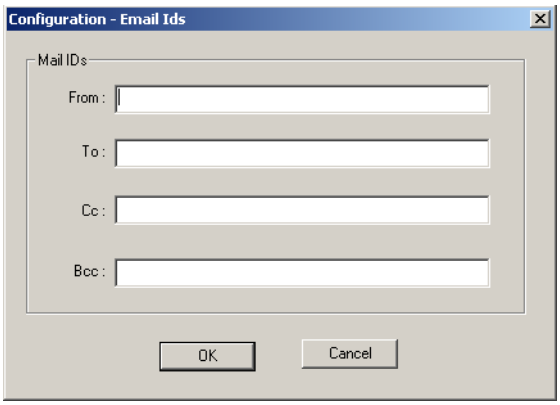
You can configure the e-mail IDs to whom the e-mails for alarms would be sent.

To specify default e-mail IDs for reporting alarms:

1. In the **System Config** dialog box, click the **Email Configuration** tab.



2. Under **Sender**, select the **Authentication Method** for sending the mail.
   - **AUTH LOGIN** - The password is encrypted while sending to the server. This ensures security.
   - **LOGIN PLAIN** - The password is sent to the server without encryption.
3. Type the **Username** and **Password** for the selected authentication method.
4. Under **Mail Server**, type the **HostName** or IP address of the mail server.
5. Type the **Port Number** of the mail server.
6. Under **Misc**, select the **Encoding** format.
7. Click **Configure E-mail IDs** to configure the e-mail IDs of the users to whom alarm reports must be sent. The **Configuration - Email Ids** dialog box appears.



8. Type the e-mail Ids in the **From**, **To**, **Cc**, and **Bcc** text boxes.

Tip: To enter multiple e-mail Ids, you can use the semicolon as a separator.

9. Click **OK** to save the e-mail details and return to the **System Config** dialog box.

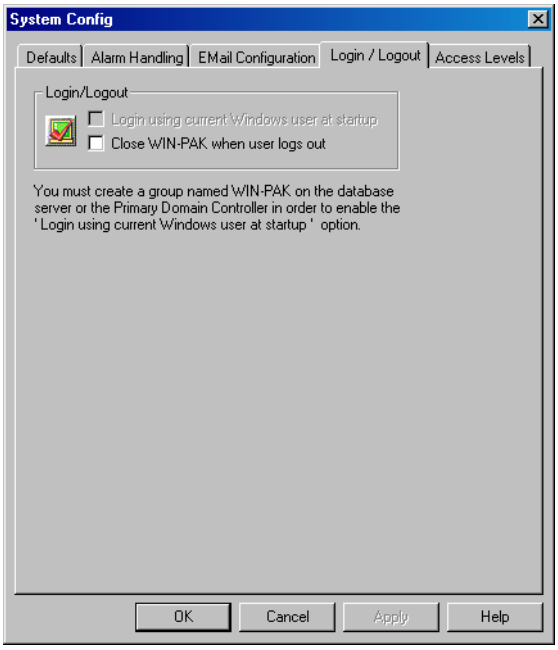
10. Click **Apply** to save the e-mail configuration details.

Configuring automatic log on and log off settings

You can set the WIN-PAK system to log on automatically, when you launch WIN-PAK. In addition, you can set to close the WIN-PAK User Interface when you log off from the system.

To configure the log on and log off settings:

1. In the **System Config** dialog box, click the **Login/Logout** tab.



2. Select the **Login using current Windows user at startup** check box, if you want the WIN-PAK system to log on automatically using Windows logon user name when you launch the application

Note: To enable this check box, you must create a group named WIN-PAK in the Windows User Group or in the Primary Domain Controller.

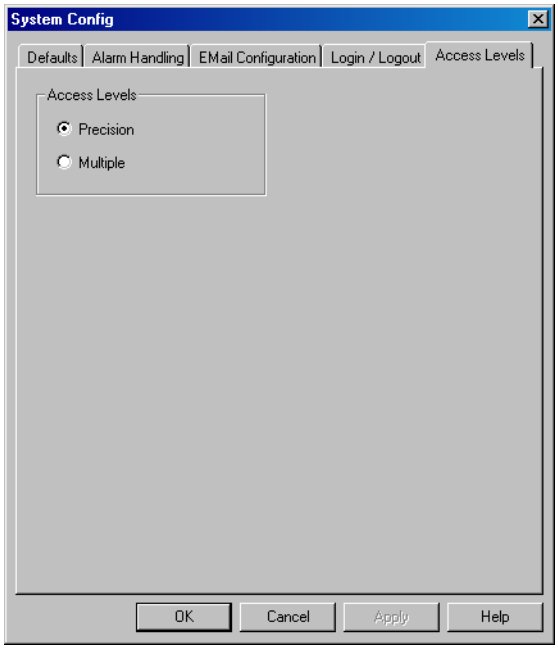
3. Select the **Close WIN-PAK when user logs out** check box, if you want to close the WIN-PAK system when you log off from WIN-PAK.

Configuring access levels for cards

You can configure the number of access levels that can be assigned to a card.

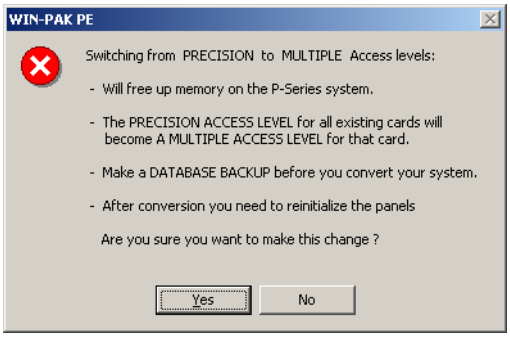
To configure the access levels for cards:

1. In the **System Config** dialog box, click the **Access Levels** tab.



2. Under **Access Levels**, click any of the following options:
   - **Precision**: Only one access level that must be assigned to a card. When this access level is selected, more memory is consumed.
   - **Multiple**: A maximum of six access levels can be assigned to a card.

Note: When you switch from **Precision** to **Multiple** access level, the following warning message appears:



A similar message is displayed when you switch from **Precision** to **Multiple** access level.

3. Click **Yes** to confirm the switching.
4. Click **Apply** to save the access level settings.
5. Click **OK** to save the changes and close the **System Config** dialog box.

Quick Configuration

6

In this chapter...

Quick Start Wizard

Overview

Quick Start Wizard (QSW) is an optional interface to configure the basic functionalities like creating an account, adding a new time zone, and so on with default settings. However, you can perform these operations using the WIN-PAK menus also.

- If you are new to WIN-PAK, you can quickly start with WIN-PAK for performing few basic operations using QSW.
- If you are already using WIN-PAK, you can still proceed with QSW for configuring the basic operations.

Configuration Options

Quick start wizard enables you to configure the following:

- Creating an Account
- Adding a Time Zone
- Adding Cards to an Account
- Adding a Site
- Adding Loops to a Site
- Adding a Panel
- Adding Readers to a P-Series Panel

Note: After configuring these options using QSW, you can edit the configuration settings using the corresponding WIN-PAK menu options.

Launching Quick Start Wizard

As QSW requires access to several WIN-PAK databases, you must log on with administrator privileges to access QSW. When you log on to WIN-PAK, Quick Start Wizard is automatically started.

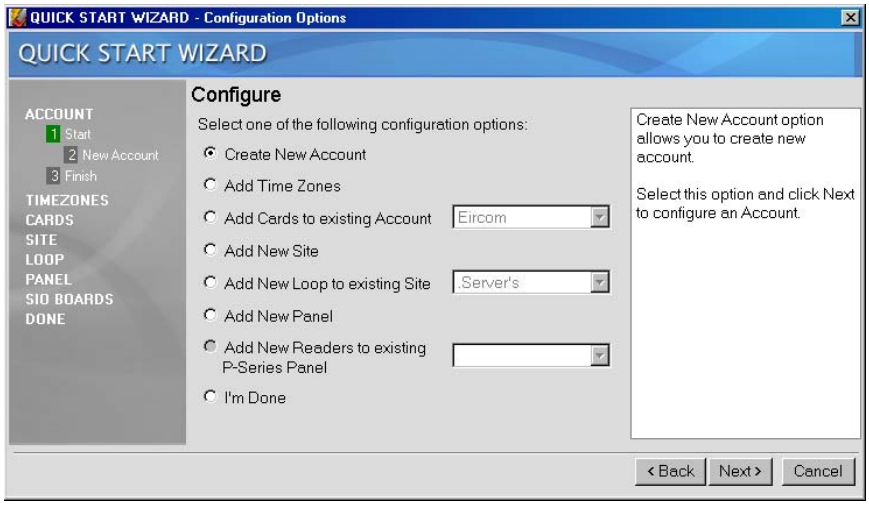
Notes:

- If you do not want QSW to start automatically,
  - Clear the **Show the Quick-Start Wizard after each Log-in** check box in the **Quick Start Wizard Configure** dialog box.
- To manually launch the quick start wizard,
  - Choose **Configuration > Quick-Start Wizard** from the main window of WIN-PAK. The **Quick Start Wizard Configure** dialog box appears.

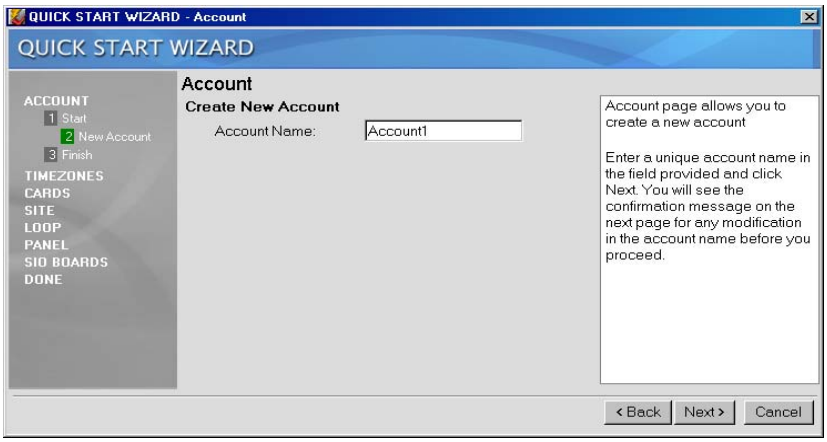
Creating an Account

To create a new account using QSW:

1. In the **Quick Start Wizard Welcome** dialog box, click **Create New Account** and click **Next**. The **Configure** dialog box appears.



2. Click **Create New Account** and then click **Next**. The **Account** dialog box appears.



3. Type a unique **Account Name** and click **Next**. A confirmation message appears for the account name.
4. Click **Next**. A new account is created and the **Configure** dialog box is displayed with the **Add Time Zones** option selected.

Note: The configuration details are NOT saved permanently, until you click **I'm Done** and perform the steps that follow.

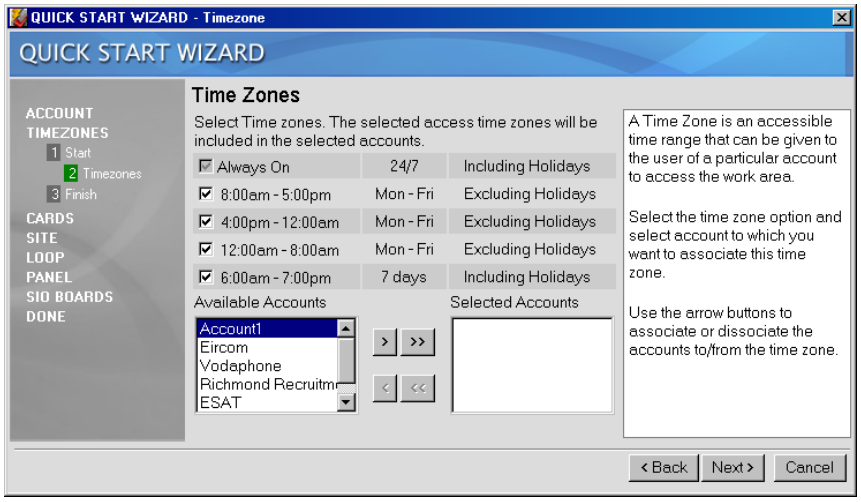
Associating Time Zones to Accounts

A time zone is the defined time interval for accessing the particular area. You must associate Time Zones to an account, as time zones are specific to an account.

To associate time zones to the accounts using QSW:

1. In the **Quick Start Wizard Configure** dialog box, click **Add Time Zones** and click **Next**. The **Time Zones** dialog box appears.

   The **Time Zone** dialog box displays the available time zones and accounts.



2. Select the time zones to be associated to an account.

Note: Using QSW, you cannot add a new time zone. Therefore, to add a new time zone, choose **Configuration > Time Management > Time Zone** on the WIN-PAK interface.

Refer to the "Adding a Time Zone" section in the chapter Time Management for details on adding a time zone.

3. In the **Available Accounts** list, click the account. For multiple account selection, use the SHIFT and CTRL keys.
4. Click > or >> to move the selected accounts or all accounts to the **Selected Accounts** list and then click **Next**. The **Continue?** dialog box appears.

5. Click **Back** to change the settings or click **Next**. The time zones are associated to the accounts and the **Configure** dialog box is displayed with the **Add Cards to existing Account** option selected.

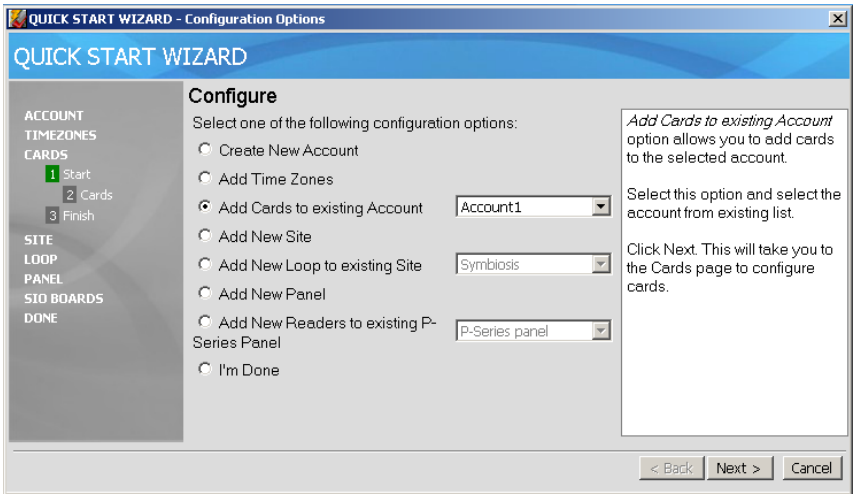
Note: The configuration details are NOT saved permanently, until you click **I'm Done** and perform the steps that follow.

Associating Cards to an Account

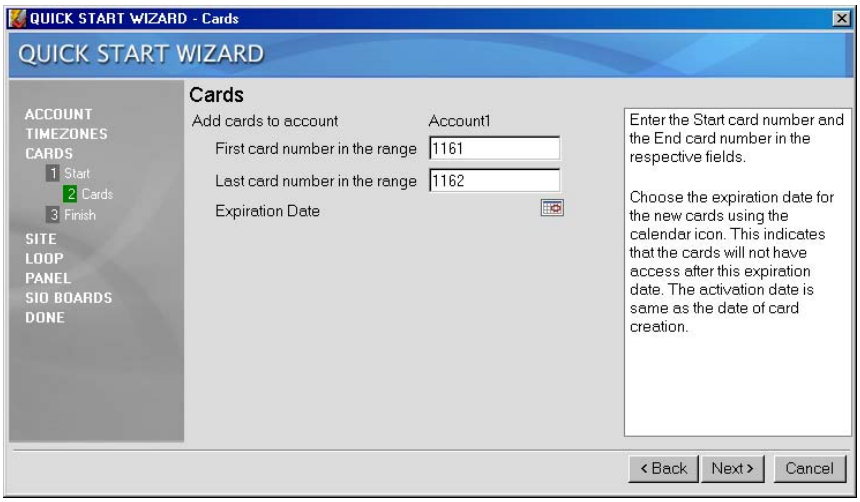
As the cards are specific to an account, they must be associated to an account before you create new cards.

To add new cards and associate them to an account:

1. In the **Quick Start Wizard Configure** dialog box, click to select **Add Cards to existing Account**.
2. In the **Account** list, select an account for associating cards to an account.



3. Click **Next**. The **Cards** dialog box appears.

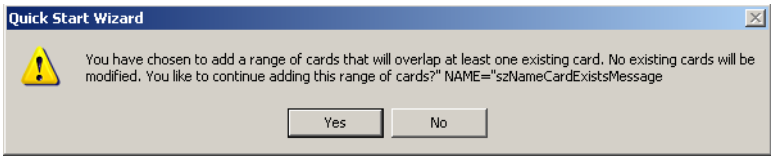


4. Type the **First card number in the range** and the **Last card number in the range**. For example, if you want to add the card numbers ranging from 100 to 150, enter 100 and 150 in the respective boxes. If you want to add a single card, enter the same number in both the boxes.

5. Select the **Expiration Date** using the icon. You can use the card to access only until the expiry date.

Note: The activation date is the same as the current date. In the demo version of WIN-PAK, the **Add Cards to existing Accounts** option is disabled.

6. Click **Next**. A warning message appears if you attempt to create the existing cards.



7. Click **Yes** to continue adding the new cards and to retain the existing cards. The **Continue?** dialog box appears.

   OR

   Click **No** to change the card range and then click **Next**. The **Continue?** dialog box appears.

8. Click **Back** to change the card settings or click **Next**. This associates the cards to an account and the **Configure** dialog box appears with the **Add New Site** option selected.

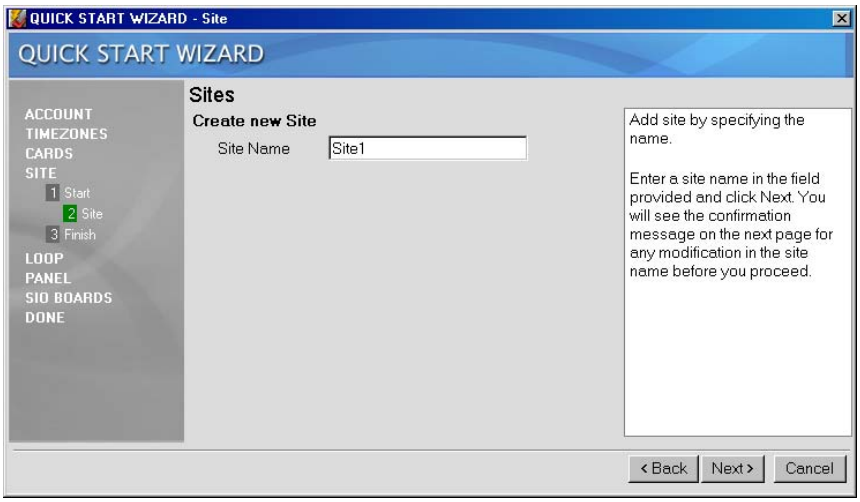
Note: The configuration details are NOT saved permanently, until you click **I'm Done** and perform the steps that follow.

Adding a New Site

Site is a logical representation of the physical location in WIN-PAK.

To add a new site:

1. In the **Quick Start Wizard Configure** dialog box, click to select **Add New Site** and then click **Next**. The **Sites** dialog box appears.



2. Type a unique **Site Name** and click **Next**. The **Continue?** dialog box appears.
3. Click **Back** to change the site name or click **Next**. A new site is created and the **Configure** dialog box is displayed with the **Add New Loop to existing Site** option selected.

Note: The configuration details are NOT saved permanently, until you click **I'm Done** and perform the steps that follow.

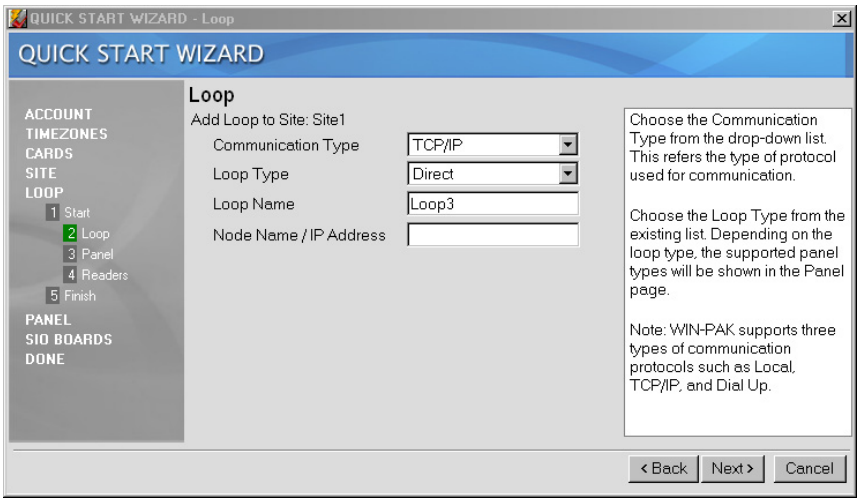
Adding a Loop to a Site

Loop refers to the communication method used for communicating between the workstation and the panel.

Adding a Loop to a Site process includes, adding a panel to a loop and adding readers to a panel.

To add a loop to a site:

1. In the **Quick Start Wizard Configure** dialog box, click **Add New Loop to existing Site**.
2. Click the **Site** to be associated with the loop and then click **Next**. The **Loop** dialog box appears.



3. Select the **Communication Type**. It determines the type of protocol used for communication.
4. Select the **Loop Type**. The available loop types are Direct and 485 ACK-NAK.
5. Type the **Loop Name**.

   WIN-PAK supports three types of communication protocols namely, Local, TCP/IP, and Dial Up. The loop configuration differs based on the protocol type selected for communication.
6. If you select **Local** as the **Communication Type**, select the **Communication Port** name connected to the panel.

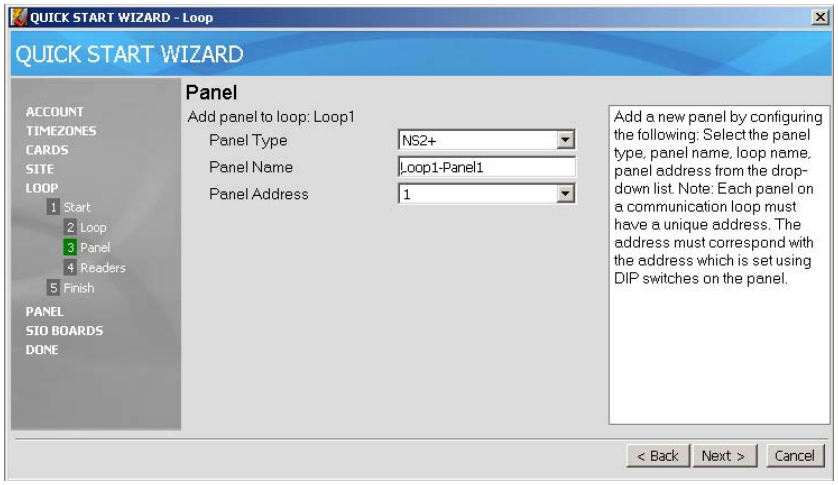
   OR

   If you select **TCP/IP** as the **Communication Type**, type the **Node Name or IP Address** of the loop.

   OR

   If you select **Dial Up** as the **Communication Type**,

   a. Select the **Communication Port** name.
   b. Type the **Modem Pool Name**.
   c. Type the **Modem Name**.
   d. Type the **Local Phone Number**.
   e. Type the **Remote Phone Number**.
   f. Type the **Password**.
7. Click **Next**. The **Panel** dialog box appears.



8. Select the **Panel Type**.

   WIN-PAK supports four types of panels such as N1000, PW2000, P-Series, and NS2+ panels to communicate with WIN-PAK.

9. Type the **Panel Name**.

10. Type the **Panel Address**.

Note: Each panel on a communication loop must have a unique address.

11. Click **Next**. The **Readers** dialog box appears to configure Reader details.

Note: The number of readers in the **Readers** dialog box depends on the panel type selected.

12. Type the **Name** of the reader.

13. Select the **Time Zone** during which the reader needs to be active.

14. Set the **Pulse time** for the reader. The WIN-PAK system sends pulses to the reader at a defined interval for checking the reader status.

15. Repeat steps 12 to 14 for each reader and click **Next**. The **Continue?** dialog box appears.

16. Click **Back**, if you want to change the settings or click **Next** to save and return to the **Configure** page.

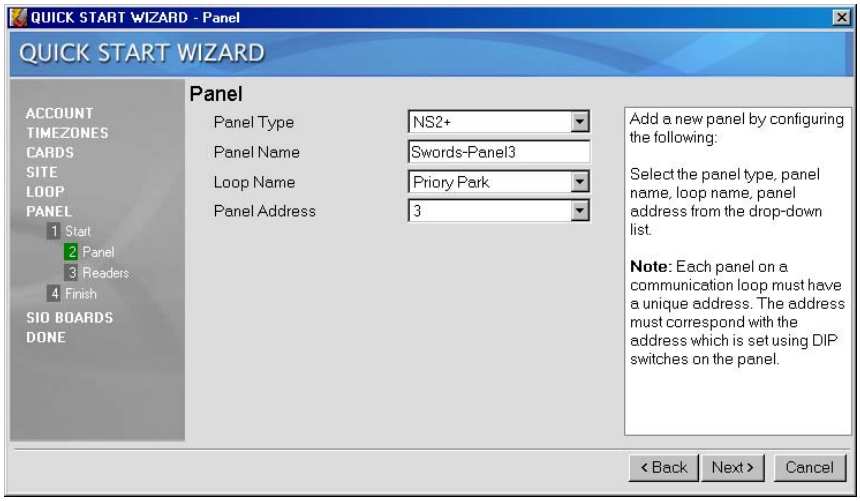
Note: The configuration details are NOT saved permanently, until you click **I'm Done** and perform the steps that follow.

Adding a Panel

A panel is a physical device in which the readers are connected through wires.

To create a new panel:

1. In the **Quick Start Wizard Configure** dialog box, click **Add New Panel** and click **Next**. The **Panel** dialog box appears.



2. Select the **Panel Type**.
3. Type a unique **Panel Name**.
4. If you select **P-Series (TCP/IP)** as the **Panel Type**,
    a. Type the **Node Name / IP Address** of the panel.
    b. Select a unique **Panel Address**.
    c. In the **Site Name**, select a site to which the panel must be associated.
    d. Click **Next** to add readers to a panel. The **Readers** dialog box appears.
    e. Select the **Reader Board Type** as 1 Reader Board or 2 Reader Board.
    f. Select the **Reader Board Address**.

    If you select any other **Panel Type**,
    a. In the **Loop Name**, select a loop to which the panel must be associated. The loops are displayed based on the selected panel type.
    b. Select a unique **Panel Address**.
    c. Click **Next** to add readers to a panel. The **Readers** dialog box appears.
5. Type the **Name** of the reader.
6. Select the **Time Zone** during which the reader needs to be active.
7. Specify the **Pulse time**. The WIN-PAK system sends pulses to the panel at a defined interval for checking the panel status.

8. Repeat steps 2 to 7 for each reader and click **Next**. The **Continue?** dialog box appears.
9. Click **Back**, if you want to change the settings or click **Next** to add a new panel and return to the **Configure** page.

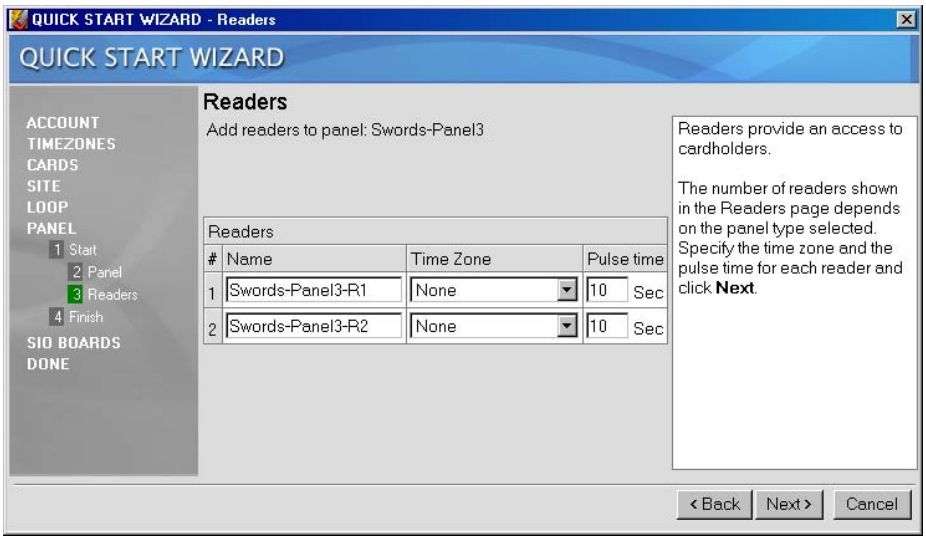
Note: The configuration details are NOT saved permanently, until you click **I'm Done** and perform the steps that follow.

Adding Readers to a P-Series Panel

This option is enabled only if a P-Series panel is added.

To add readers to a P-Series panel:

1. In the **Quick Start Wizard Configure** dialog box, click **Add Readers to a P-Series Panel** and click **Next**. The **Readers** dialog box appears.



2. Select the **Reader Board Type**. Depending on the type, the number of readers is displayed.
3. Select the **Reader Board Address**.
4. Type the **Name** of the reader.
5. Select the **Time Zone** for the reader during which the reader is active.
6. Set the **Pulse Time** for the reader.
7. Repeat steps 4 to 6 for each of the readers and click **Next**. The **Continue?** dialog box appears.
8. Click **Back**, if you want to change the settings or click **Next** to save and return to the **Configure** page.

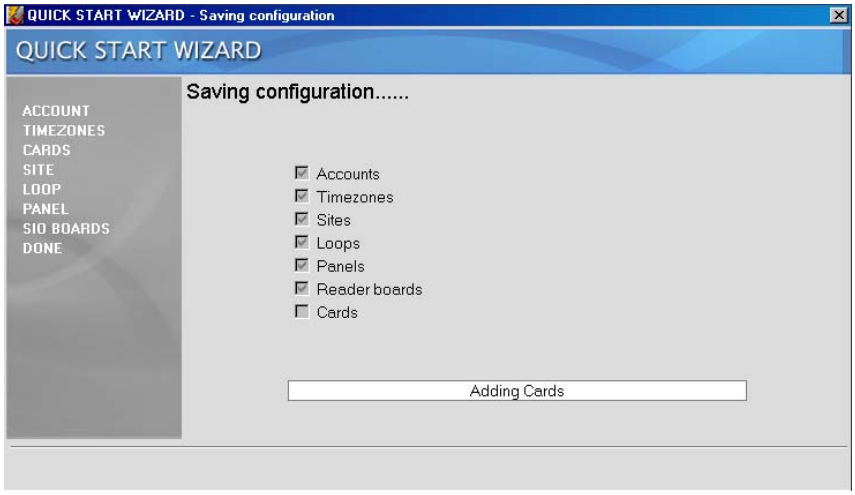
Note: The configuration details are NOT saved permanently, until you click **I'm Done** and perform the steps that follow.

Saving the Configuration

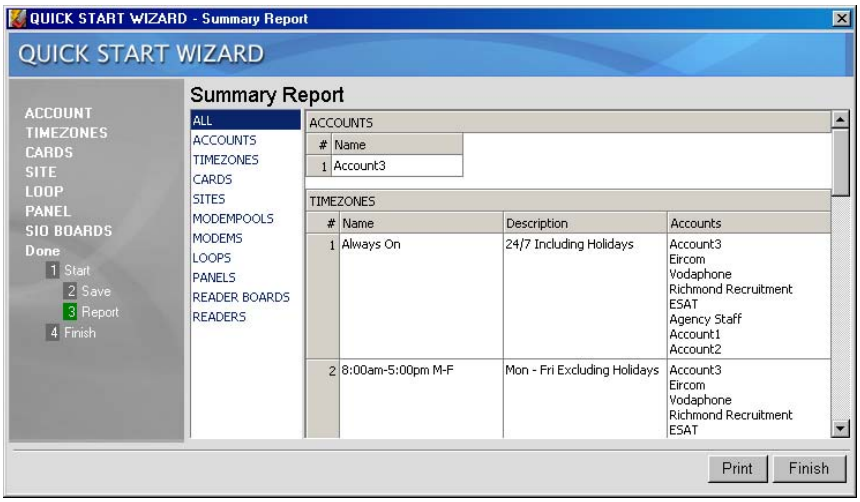
After completing the required configuration, you must save the configuration details using the **I'm Done** option. Note that the configuration details are NOT saved permanently, when you click the **Next** button after each configuration.

To save the configuration details and to generate the summary report:

1. In the **Quick Start Wizard Configure** dialog box, click **I'm Done** and click **Next**. The **Saving Configuration** dialog box appears.



After saving the configuration details, the **Summary Report** dialog box appears.



2. In the **Summary Report** dialog box, click **Print** to print the configuration details or click **Finish** to close the QSW dialog box.

Badge Layout

7

In this chapter...

Introduction

Badge layouts are templates that define the size, placement, and properties of a badge. Properties of a badge are its printable size, its background color, and the magnetic stripes used for encoding cardholder information. In addition, the badge layout is defined with placeholders for cardholder information such as photo, note fields, signatures, and bar codes.

When a badge layout is later associated with a card, the card holder information such as photo, signature, and any other note field information is automatically entered on the badge. This creates individual badges for every cardholder. These cards are used as photo IDs and access cards.

Badges can be displayed on the screen or printed on paper or on cards. Badges are printed on Technology or non-Technology cards. Any Windows-compatible printer, ink jet, laser, or PVC card printer can be used for printing badges. Special PVC card printers enable double-sided printing and magnetic stripe encoding.

Configuring a Badge Layout

Configuring a badge layout involves:

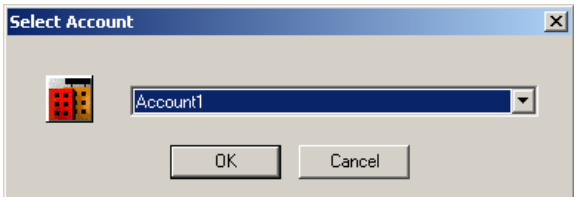
- **Selecting an account** - Select the individual account for which you want to create a badge layout or specify all accounts.
- **Adding a new badge layout** - Create a badge layout with a name and description.
- **Creating badge designs** - Place elements on the badge layout (bitmaps, placeholders for cardholder photo, bar codes and so on) and set various properties for the badge elements.

Selecting the Account

You can create badge layouts for a particular account or for all accounts.

To select an account:

1. Choose **Account > Select**. The **Select Account** dialog box appears.



2. To configure badge layouts for a particular account, select the account in the list.

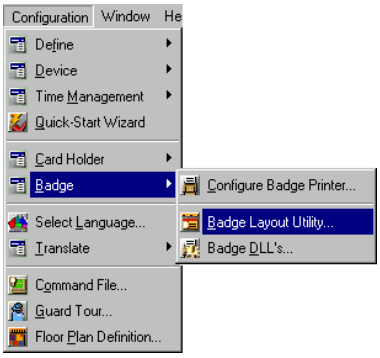
   OR

   To configure badge layouts for all accounts, select <All Accounts> in the list.

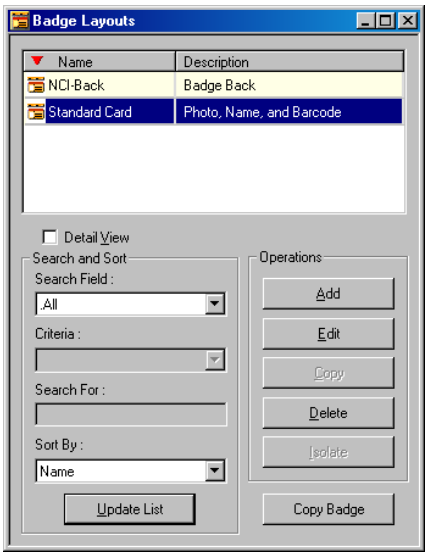
3. Click **OK** to save the account information for creating badge layouts and to exit from the **Select Account** dialog box.

Adding a New Badge Layout

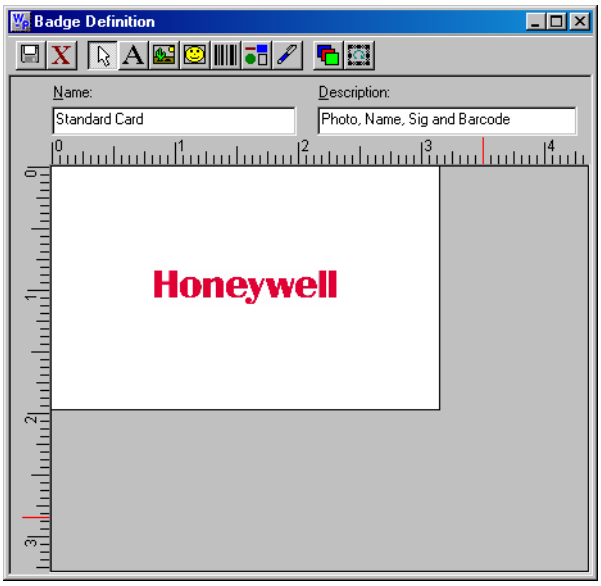
1. Choose **Configuration** > **Badge** > **Badge Layout Utility**.



The **Badge Layouts** window appears with a list of existing badges.



2. Click **Add** to add a new badge layout. The **Badge Definition** window appears.



3. Type a **Name** and **Description** for the badge layout.
4. Click the icon provided in the toolbar of the window. The new badge layout is saved and listed in the **Badge Layouts** window.

Searching and Sorting Badge Layouts

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select a search item in the **Search Field** list.
   - All - Lists all the badge layouts.
   - Description - Searches for similar badge layout descriptions.
   - Name - Searches for similar badge layout names.
3. If you have selected **Description** or **Name** in **Search Field**, select the criteria for search in the **Criteria** list.
   - Begins With
   - Equals
   - Greater than
   - Less than
4. Type the text you want to search in the **Search For** box.
5. To sort badge layouts based on badge name or description, select it from the **Sort By** list.
   - None - no sorting required.
   - Name - sorts badge layouts by the ascending order of badge name.

- Description - sorts badge layouts by the ascending order of badge description.

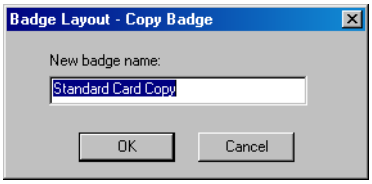
6. Click **Update List** to update the list of badge layouts based on the search criteria, sorted in the specified order.

Copying a Badge Layout

Copying a badge layout enables you to easily create several badges with the same basic layout, but with distinguishing features such as the background color.

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select the badge to be copied, and click **Copy Badge**.

   The **Badge Layout - Copy Badge** dialog box appears.



3. Type the name for the badge layout in the **New badge name** box.
4. Click **OK** to create a copy of the badge layout.

Editing a Badge Layout

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select the badge layout you want to edit and click **Edit**. The **Badge Definition** window appears.
3. Edit the **Name** and **Description** of the badge layout.
4. Click the  icon.

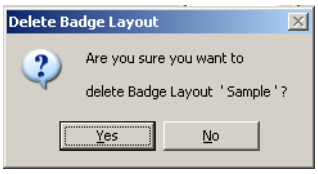
Viewing a Badge Layout

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select the badge layout you want to view and select the **Detail View** check box. The **Badge Definition** window appears, with the details of the selected badge layout.

Isolating and Deleting a Badge Layout

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.

2. Select a badge layout and click **Delete**. A dialog box appears, prompting you to confirm the deletion.



3. Click **Yes** to confirm the deletion of the badge layout. If cards are associated to the badge layout, the **Badge Layout Delete** dialog box appears with the list of linked cards.

4. Click **Delete** to remove the link between the badge layout and the linked cards, and to delete the badge layout.

Caution: Be cautious while deleting a badge layout as it could be attached to thousands of cards.

Creating Badge Designs

Overview

Designing badges involves:

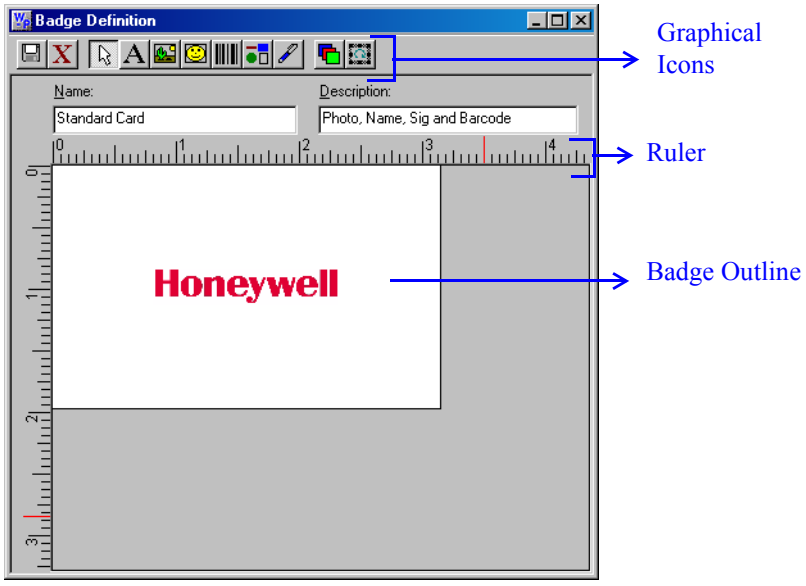
1. Setting the printable size of the badge.
2. Providing background color, graphics, and image for the badge.
3. Specifying blockout areas on the badge.
4. Placing the following badge elements and setting their properties:
    - Text
    - Bar Codes
    - Bitmap
    - Placeholder for card holder photo
    - Placeholder for signatures

Note: You can design a badge while adding a new badge layout or while editing an existing layout.

Know more about the Badge Definition window

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select a badge layout and click **Edit**.

   The **Badge Definition** window appears with the details of the selected badge layout.

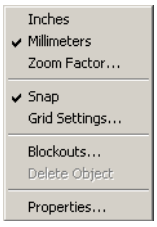


Changing the Ruler Measurement

You can set the ruler measurement of the badge outline as Inches or Millimeters.

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select a badge layout and click **Edit**. The **Badge Definition** window appears.
3. Right-click anywhere inside the badge outline and click **Inches** or **Millimeters**.

   A check mark indicates the option in use. To switch from one unit of measure to another, select the desired unit from the menu.

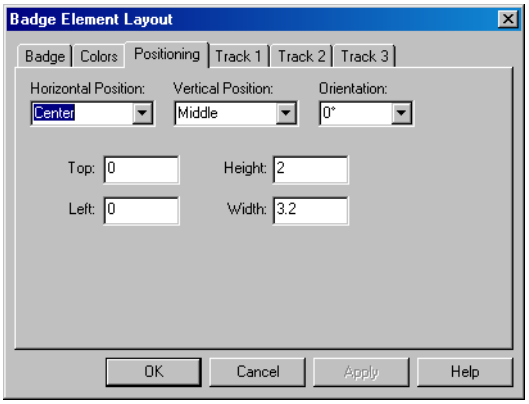


Setting the printable size of the badge

You can set the printable size of the badge by altering the height and width of the badge outline.

Note: The default badge size is 50 mm high by 80 mm wide and these dimensions are best suited for most PVC printers.

1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** dialog box appears.
2. Select a badge layout and click **Edit**. The **Badge Definition** dialog box appears.
3. Right-click anywhere inside the badge outline and click **Properties**. The **Badge Element Layout** dialog box appears.
4. Click the **Positioning** tab.



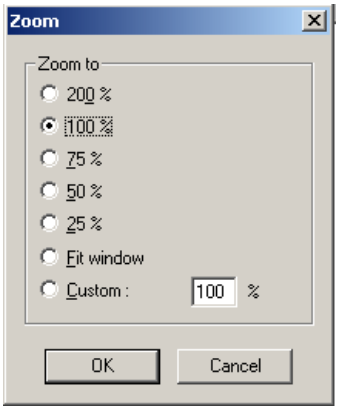
5. Select the **Horizontal Position** and the **Vertical Position** of the badge outline.
6. Select the degree of **Orientation**.
   - 0° - Places the object upright.
   - 90° - Rotates the object 90° clockwise.
   - 180° - Places the object upside-down.
   - 270° - Rotates the object 90° counterclockwise.
7. Type the **Top and Left** of the badge in millimeters or inches (0 for PVC printers.)
8. Type the **Height and Width** of the badge in millimeters or inches.
9. Click **Apply** to apply the dimensions to the badge outline.
10. Click **OK** to apply the dimensions to the badge outline and to return to the **Badge Definition** window.

Note: To change the badge orientation from landscape (horizontal) to portrait (vertical) enter a dimension in the **Height** box that is greater than the dimension in the **Width** box.

Adjusting the Zoom factor

The Zoom factor decides the view of the badge outline in the **Badge Definition** window.

1. Right-click in the **Badge Definition** window and select **Zoom Factor**. The **Zoom** dialog box is displayed.



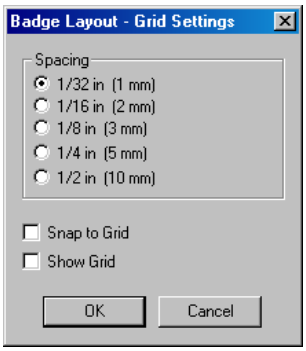
2. Select the required zoom factor, or click **Custom** and type the zoom percentage.
3. Click **OK**.

   The badge outline in the **Badge Definition** window enlarges or reduces by the selected zoom percentage.

Specifying Grid Settings

Grids are evenly spaced points on the badge layout area that assist in sizing and aligning items. You can use the grid as a visual aid for placing items on the badge layout. You can also enable the **Snap** setting for the grid, which pulls any item moving close to the grid mark.

1. Right-click in the **Badge Definition** window, and then click **Grid Settings**. The **Badge Layout - Grid Settings** dialog box appears.



2. Select one of the five spacing options in the **Spacing** list.

3. Select the **Snap to Grid** check box, if you want items to snap to the grid when they are moved or added.
4. Select the **Show Grid** check box, if you want the grid marks to be visible on the screen.
5. Click **OK** to save the settings and return to the **Badge Definition** window.

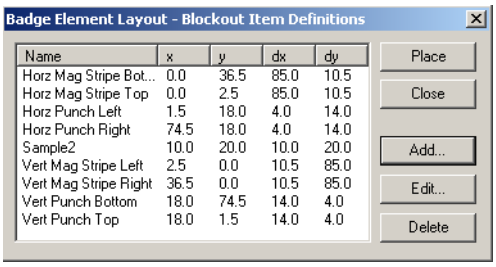
Setting Blockouts

You can set blockouts for reserving the non-printing area on a badge. This is useful to prevent instances like printing over a magnetic stripe or hole punch area in the card. Unlike other badge objects, the blockout has no properties and always remains on top in the item layering.

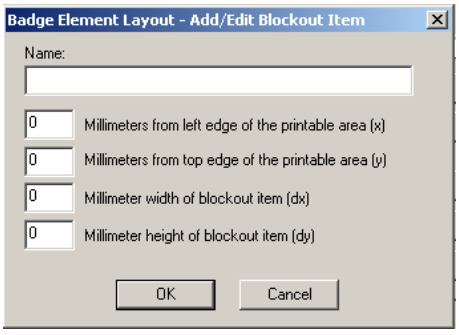
Though the blockout is generally effective in preventing overprinting of the Mag Stripe area, some card printers do print resin black over the blockout. To avoid this, ensure that no blockout is placed over the Mag Stripe area.

To add a new blockout to the badge layout:

1. Right-click within the badge outline, and then click **Blockouts**. The **Badge Element Layout - Blockout Item Definitions** dialog box appears.



2. Click **Add** (if you are creating a new blockout) or **Edit** (if you are making changes to an existing blockout). The **Badge Element Layout–Add/Edit Block Item** dialog box appears.



3. Type a **Name** for the blockout.
4. In the **Millimeters from left edge of the printable area (x)** box, type the distance of the blockout from the left edge of the badge printable area.
5. In the **Millimeters from top edge of the printable area (y)** box, type the distance of the blockout from the top edge of the badge printable area.

6. In the **Millimeter width of blockout item (dx)** box, type the width of the blockout.
7. In the **Millimeter height of blockout item (dy)** box, type the height of the blockout.

Note: You may have to measure an actual card and print a test card to determine the exact position for the blockout.

8. Click **OK**. The **Badge Layout - Blockout Item Definitions** dialog box appears with the blockout added in the list.
9. Select the blockout in the list and click **Place**. The blockout is placed on the badge layout in the **Badge Definition** window.

Note: A blockout once placed cannot be moved on the badge layout. However, you are provided with the option to edit its size and also to delete it.

To edit a blockout:

1. Right-click on the blockout on the badge layout, and then click **Blockouts**. The **Badge Element Layout - Blockout Item Definitions** dialog box appears.
2. Select the blockout in the list and click **Edit.** The **Badge Element Layout - Add/Edit Blockout Item** dialog box appears.

   You can edit the details of the blockout, such as, the Name, the distance of the blockout from the badge printable area, and the height and width of the blockout.

To delete a blockout:

1. To delete the blockout that is placed on the badge layout, right-click on the blockout on the badge layout, and then click **Delete Object**.

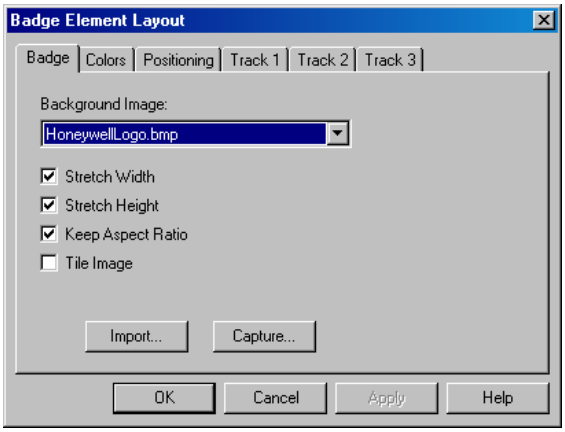
   OR

   To delete the blockout and its definition, right-click on the blockout on the badge layout, and then click **Blockouts**. The **Badge Element Layout - Blockout Item Definitions** dialog box appears. Select the blockout in the list and click **Delete**.

Setting a Badge Background

You can import or capture background images for the badge layouts. You can also set the width, height, aspect ratios, and the tiled appearance of the image.

1. Right-click anywhere on the badge outline and click **Properties**. The **Badge Element Layout** dialog box appears.
2. Click the **Badge** tab.



3. In the **Background Image** list, select the image that must be applied to the badge background.

Note: You can import an image from your computer to the **Background Image** list, or capture an image.

Refer to the "Setting a Badge Background" section in this chapter for more on importing and capturing images to the badge background.

4. Select the **Stretch Width** check box to stretch the width of the image.
5. Select the **Stretch Height** check box to stretch the height of the image.
6. Select the **Keep Aspect Ratio** check box to retain the existing aspect ratio of the image while stretching its height and width.
7. Select the **Tile Image** check box to enable a tiled appearance for the image.
8. Click **OK** to save the changes.

To import a background image:

1. On the **Badge** tab of the **Badge Element Layout** dialog box, click **Import**. The **Open** dialog box appears.
2. Locate for the image file or type the image **File Name**.

Note: BMP, JPG, PCX, or TGA images can be imported.

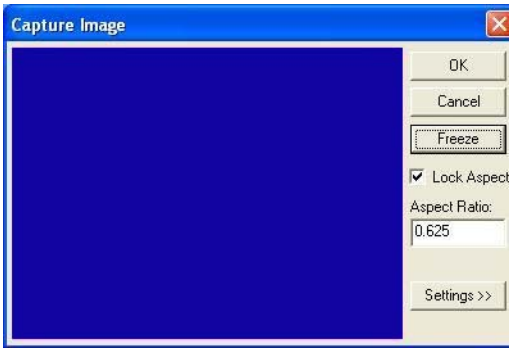
3. Click **Open**. The selected image file is listed in **Background Image**.
4. Click **Apply** to apply the image to the badge background or click **OK** to apply the image to the badge background and to close the **Badge Element Layout** dialog box.

To capture an image using a camera:

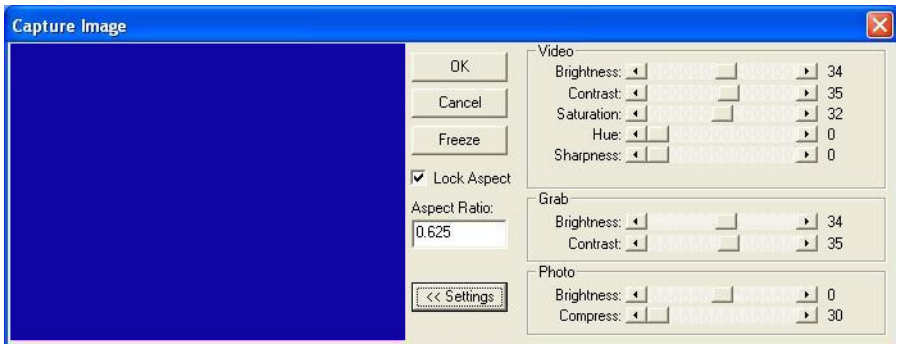
1. On the **Badge** tab of the **Badge Element Layout** dialog box, click **Capture**. The **Capture Image** dialog box opens displaying the live view from your video camera.

Note: Ensure that you have installed the necessary video equipment, including a supported video capture card, or a compatible TWAIN device.

Refer the "Configuring Badge DLLs" section in this chapter for details on configuring DLLs for Video Capture Cards.



2. Click **Settings** to expand the window and access the video settings.



3. Adjust the **Video**, and **Grab** settings for a satisfactory image.

Table 7-1 Live Screen Video Image Settings

Setting	Description
Brightness	Lightens or darkens the entire tonal range of the image.
Contrast	Expands or contracts the entire tonal range of the image. The difference in highlights and shadows is increased or decreased.
Saturation	Adjusts the vibrancy or the level of color in the image.
Hue	Adjusts the value of color in the image. This corrects incorrect coloring of images.
Sharpen	Sharpens blurry images by increasing the contrast of the adjacent pixels.

Table 7-2 Live Screen Grab Settings

Setting	Description
Brightness	Lightens or darkens the entire tonal range of the image.
Contrast	Expands or contracts the entire tonal range of the image. These settings are applied to the camera when an image is captured. If you are not using a flash, set the Contrast the same as the Video settings. If a flash is used, reduce the Contrast settings lower than the Video settings. This prevents overexposure of the picture. **Note:** The exact settings must be determined by experimentation, as they vary depending on the type of flash, distance from the subject, and other lighting being used.

Note: If you are not using a flash, set the Grab settings to the same values as the Video settings. If you are using a flash, reduce the **Grab Brightness** and **Contrast**. (The exact settings will vary depending on the type of flash and other lighting. The exact settings can only be determined by experimenting.)

4. Click **Freeze** to capture the image.
5. To crop the captured image, use the cropping frame or enter the image proportion in **Aspect Ratio,** and select the **Lock Aspect Ratio** check box.

   Tip: If you are using the default badge size, set the aspect ratio to **0.625**, to fill the entire badge outline.
6. Adjust the **Photo** settings of the captured image.

Table 7-3 Live Screen Photo Settings

Setting	Description
Brightness	Lightens or darkens the entire tonal range of the captured image.
Compress	The captured image is saved as a jpg file. If required, use the slider to adjust the compression of the saved image. The lower the number, the greater the compression. **Note:** Images lose quality as they are compressed, and thus it is recommended to avoid over-compressing. **Example:** A setting of 100 applies the least amount of compression and provides the best image quality. A setting of 30 applies the most compression, but provides lower image quality.

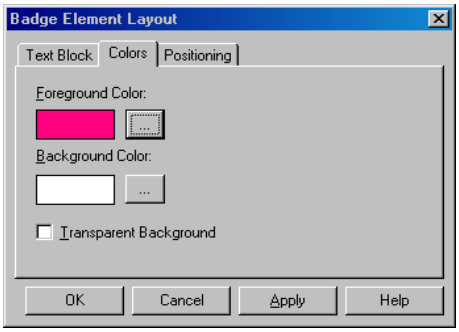
7. Click **OK** to save the image.

Setting a background color

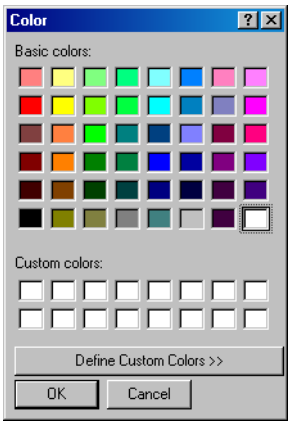
You can set a background color for a badge or for an item on the badge (for example, a bitmap, shape or signature.) The foreground color is not available unless an item is selected.

To select a color from the basic color palette:

1. Right-click on the badge outline and click **Properties**. The **Badge Element Layout** dialog box appears.
2. Click the **Colors** tab.



3. Click the ellipsis [...] provided near the **Background Color** box. The **Color** dialog box is displayed.

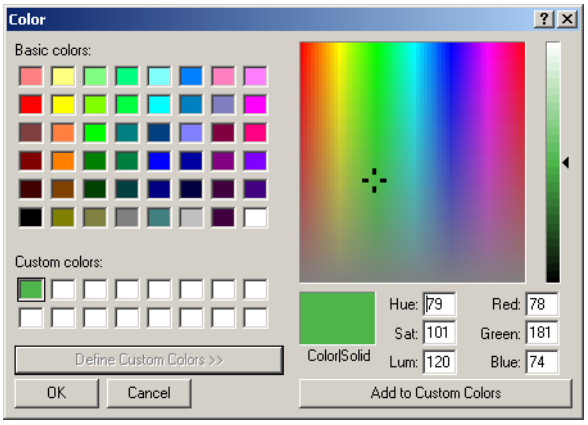


4. From the **Basic colors** palette, click the color swatch you want to use for a background.
5. Click **Apply** to apply the color to the badge background or click **OK** to apply the color and to exit from the **Color** dialog box.

To define a custom color:

1. Right-click on the badge outline and click **Properties**. The **Badge Element Layout** dialog box appears.
2. Click the **Colors** tab.
3. Click the ellipsis [...] button provided near the **Background Color** box. The **Color** dialog box is displayed.

4. Click **Define Custom Colors** to expand the **Color** dialog box.



5. If you know the Red, Green, Blue equivalents for a specific color, enter those values in the **Red**, **Green**, and **Blue** boxes.

   OR

   If you know the Hue, Saturation, Luminosity equivalents for a specific color, enter those values in the **Hue**, **Sat** and **Lum** boxes.

   OR

   Use the color selector to choose the color.

Table 7-4 Color Settings

Option	Description
Hue	Wave length of light reflected by an object. It is the characteristic commonly called color, and identified by color names such as yellow, green, or orange. Hue values range from 0 (red) through 239 (running through the spectrum and returning to red).
Saturation	Strength of the color. It indicates the amount of gray in the color. Saturation values range from 0 (gray with no trace of color) through 240 (fully saturated color with no gray).
Luminosity	Luminosity is the relative brightness or darkness of the color. Luminosity values range from 0 (black) through 240 (white) with the un-tinted color at about 120
Red Green Blue	The RGB model is based on the representation of the visible spectrum by mixing red, green, and blue light. Computer monitors are based on this model, creating colors by emitting light through red, green, and blue phosphors. The RGB model assigns a value for each pixel ranging from 0 (black) to 255 (white) for each color component. The red on the Basic color palette has a Red value of 255, a Green value of 0 and a Blue value of 6.

Table 7-4 Color Settings

Option	Description
Color Solid	The color swatch shows the color as it appears on the monitor, and also its approximate appearance when printed.

6. Click **OK**. The new custom color appears in the **Background Color** box of the **Badge Element Layout** dialog box.
7. Click **Apply** to apply the custom color to the badge background or click **OK** to apply the background color to the badge and to exit from the **Badge Element Layout** dialog box.

Note: Due to differences in monitors, printers, and the type of print media, there might be a difference in the color shade of the badge when it is printed as compared to its shade on the monitor.

Tip: Solid dark colors may not print evenly on all printers. Honeywell recommends that you use a light colored or a white background for the badge.

Setting Magnetic Stripe Encoding

Magnetic stripe data can be defined for all the three tracks.

Note: Certain encoders, and cards do not support Track 3. Check your printer and card supplier before setting magnetic stripe encoding.

For each track, specify the magnetic stripe format: IATA, ABA, or TTS. The industry standard for track/format assignment is Track 1 - IATA, Track 2 - ABA, Track 3 - TTS. (The NR-1-WR, and the NR-5-KP read ABA on Track 2, and the NR-2-WR reads ABA on Track 1.)

Each track can have a number of data items, which is limited by the amount of data that can fit on a given track. Only certain ASCII characters can be used, depending on the format selected for that track.

IATA supports alphanumeric characters 0-9, and A-Z, and various punctuation characters (ASCII 32-95). Lower-case letters are converted to upper-case as IATA does not support lowercase letters. Use a "^" character in the place of a field separator.

ABA supports only numeric characters 0-9 and various punctuation characters (ASCII 48-63).

TTS supports only numeric characters 0-9 and various punctuation characters (ASCII 48-63).

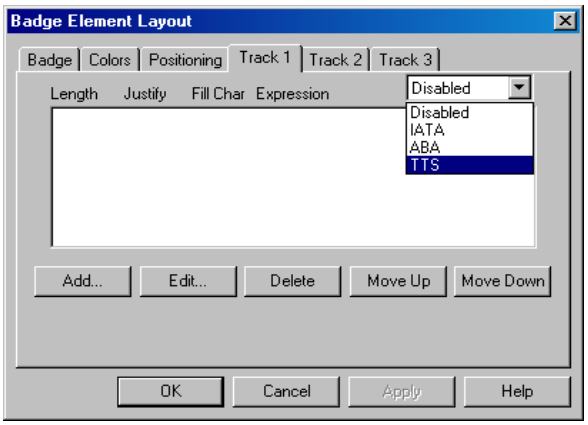
The following is a list of the maximum number of characters that can be printed using the Datacard IC III printer.

Table 7-5 Characters printed using Datacard IC III printer

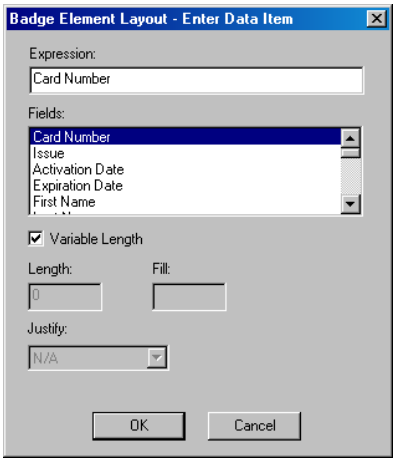
Track	Type of character	Maximum Characters	Bits per inch
1	Alphanumeric	76	210
2	Numeric	37	75
3	Numeric	104	210

To Enter Magnetic Stripe Data:

1. Right-click on the badge outline and click **Properties**. The **Badge Element Layout** dialog box appears.
2. Click the **Track X1**, **Track X2**, or the **Track X3** tab.



3. Select **Disabled, IATA, ABA**, or **TTS** from the list on the upper-right corner.
4. Click **Add** or **Edit** to define items to be added to the track. The **Badge Element Layout - Enter Data Item** dialog box appears.



5. Enter the following data items:

   - **Expression**: Any combination of text or database fields can be entered. Type the desired text or double-click the appropriate field in the Fields list to enter it in the Expression field. **The selected field appears within braces on the list.**
   - **Fields**: The list contains all the note fields defined for card and cardholder. Double-click to select a field and to add it to **Expression**.
   - **Variable Length**: Select the check box if the field length in the bar code must match the number of characters in the data item.
   - **Length**: The data item is truncated or padded so that it precisely matches the number of characters.

   Note: This option is not available, if the **Variable Length** check box is selected.

   - **Fill**: Enter the character to be used to pad the data to fit a fixed-length field.
   - **Justify**: If a data item is shorter than the number of characters allotted for it, it can be justified left, center, or right, within those characters. All other characters are set to the **Fill** character.

6. Click **OK** to save any changes and return to the **Badge Element Layout** dialog box.

   Note: Repeat the procedure until all the data items have been added.

7. To reorder the data items in a track, click **Move Up** and **Move Down**.
8. To remove a data item from the list, select it and click the **Delete** button.
9. On the **Badge Element Layout** dialog box, click **Apply** to save the data items for the tracks or click **OK** to save the data items for the tracks and to return to the **Badge Definition** window.

Placing Elements in the Badge Outline

After designing the badge outline, you can place items or elements on it to meet your specific needs. The badge holder's photo, name, card number, and other pertinent information can be included on the badge. A bar code can be added to the badge for system applications ranging from access control and payroll to resource checkout. Bitmaps such as logos can be added and colors can be applied to the items.

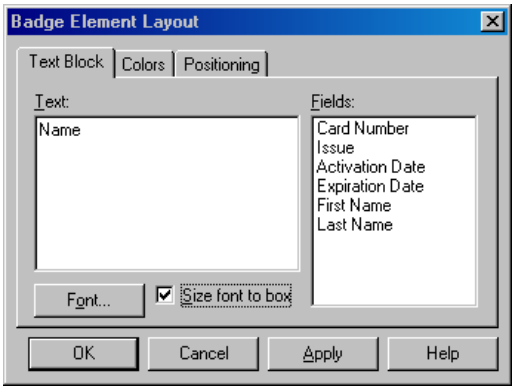
The following are the types of items that can be placed on a badge outline and their corresponding toolbar icons:

- Text
- Bitmap
- Photo
- Bar code
- Shape
- Signature

Placing a Text element

To place a text element on a badge, draw a text box, and then type the text and/or add card holder note fields. When you assign the badge to a card holder, the cardholder's data is automatically fill in the text.

- To add a text block on the badge outline:
    a. Click on the toolbar.
    b. Click and drag the mouse pointer on the badge outline to place the text. The text box is now placed on the badge outline.
- To add fields to the text area:
    a. Right-click on the text block and click **Properties**.
    b. Click the **Text Block** tab.



    c. Double-click the field that must appear in the text box in the **Fields** list. The field is now placed under **Text**.
    d. Type the field name within the parenthesis under **Text**.

e. Click **Font** to modify the font and color of the field name.

f. Select the **Size font to box** check box if you want to resize the font to fit the text block.

g. Click **Apply** to add the text box to the badge outline.

Placing a Photo

You can place a placeholder for the card holder's photo on the badge design. When the badge is assigned to a card and card holder, the card holder's photo is placed at the photo placeholder.

- To add a photo on the badge outline:

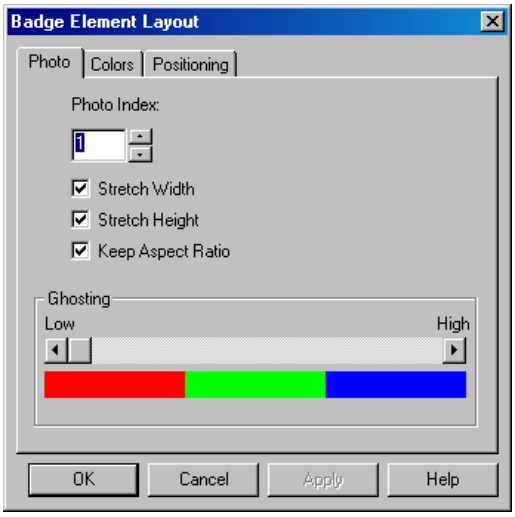
  a. Click  on the toolbar.

  b. Click and drag the mouse pointer on the badge outline to place the photo. The photo is now placed on the badge outline.

- To change the photo properties:

  a. Right-click on the photo and click **Properties**.

  b. Click the **Photo** tab.



c. Type or select the **Photo Index**.

Note: The **Photo Index** indicates which card holder picture must appear on the badge. The default is 1.

d. Select the **Stretch Width** check box to stretch the width of the photo.

e. Select the **Stretch Height** check box to stretch the height of the photo.

f. Select the **Keep Aspect Ratio** check box to retain the aspect ratio of the photo while stretching its height and width.

g. Increase or decrease the **Ghosting** option to set the degree of transparency for the photo.

Note: A ghosted photo is harder to photocopy and provides added security against unauthorized reproduction of ID badges.

h. Click **Apply** to place the photo in the badge outline.

Placing a Shape on the Badge outline

- To add a shape on the badge outline:

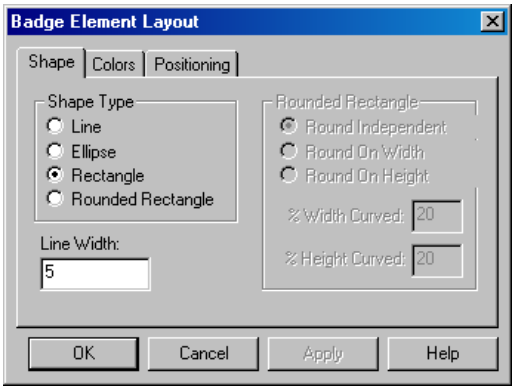
  a. Click  on the toolbar.

  b. Click and drag the mouse pointer on the badge outline to place the shape. The shape is now placed on the badge outline.

- To change the properties of the shape:

  a. Right-click on the shape and click **Properties**.

  b. Click the **Shape** tab.



  c. Under **Shape Type**, click to change the type of the shape. If you click **Rounded Rectangle**, set its properties in the options provided under **Rounded Rectangle** frame.

  d. In the **Line Width** box, type the width for the shape outline.

  e. Click **Apply** to place the shape in the badge outline.

Placing a Signature on the Badge outline

You can place Signature placeholders on the badge where you need the card holder's signature to appear. When the badge is assigned to a card holder, the card holder's signature is applied to the badge.

A signature pad (Honeywell Access Systems PB-SIG-CAP or PBSIGCAPLCD) must be connected to the computer to capture signatures. The captured signatures are saved in vector format and placed on the cards, stretching proportionally to fill the signature placeholder. The signature background is made transparent to be placed on top of any other object on the badge.

- To add a signature to the badge outline:

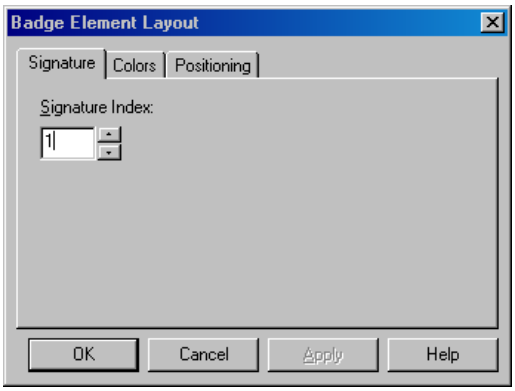
  a. Click  on the toolbar.

b. Click and drag the mouse pointer on the badge outline to place the signature. The signature is now placed on the badge outline.

- To change the signature index:

a. Right-click on the signature and click **Properties**.

b. Click the **Signature** tab.



c. Type or select the **Signature Index**.

Note: Signature Index indicates which card holder signature must appear on the card. The default is 1.

d. Click **Apply** to place the signature in the badge outline.

Placing a Bitmap on a badge

Graphic images such as a logo or symbol can be placed on the badge. You can either create or scan your image and save it as a bitmap graphic file. Windows Bitmap (*.bmp), JPEG (*.jpg), Targa (*.tga), or TIFF (*.tif) files are supported.

- To add a bitmap on the badge outline:

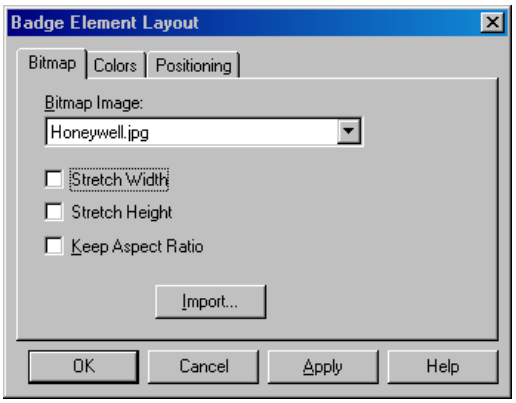
a. Click on the toolbar.

b. Click and drag the mouse pointer on the badge outline to place the bitmap. The bitmap is now placed on the badge outline.

- To change the bitmap properties:

a. Right-click on the bitmap and click **Properties**.

b. Click the **Bitmap** tab.



c. Select an image from the **Bitmap Image** list or click **Import** to import a bitmap.

d. Select the **Stretch Width** check box to stretch the width of the photo.

e. Select the **Stretch Height** check box to stretch the height of the photo.

f. Select the **Keep Aspect Ratio** check box to retain the aspect ratio of the photo while stretching its height and width.

g. Click **Apply** to place the bitmap in the badge outline.

Placing a Bar Code on the Badge

- To add a bar code on the badge outline:

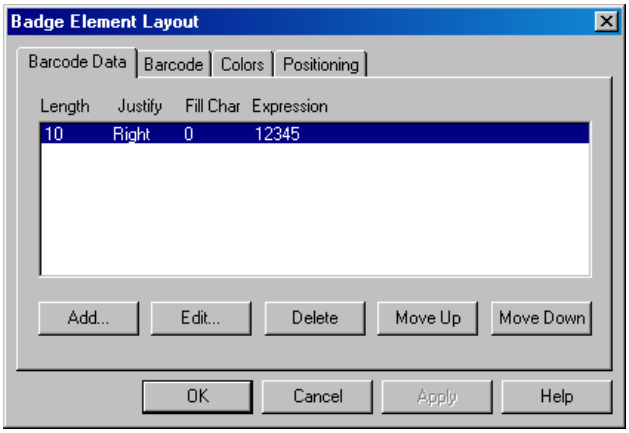
  a. Click on the toolbar. q

  b. Click and drag the mouse pointer on the badge outline to place the bar code. The bar code is now placed on the badge outline.

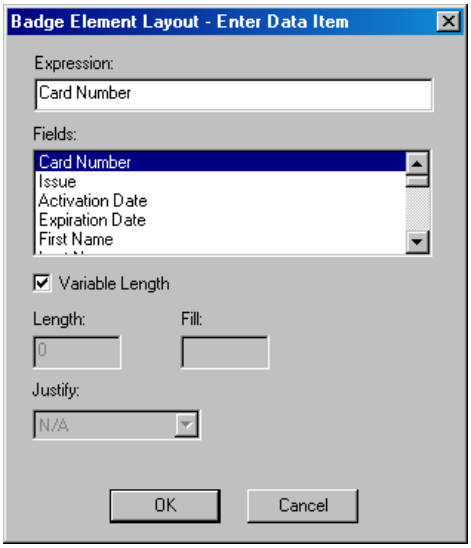
- To add bar code data items:

  a. Right-click on the bar code and click **Properties**.

  b. Click the **Barcode Data** tab.



c. Click **Add** to add a new barcode data or select an existing bar code and click **Edit**. The **Badge Element Layout - Enter Data Item** dialog box appears.



d. In the **Expression** box, enter the specific data to be contained in the bar code, or select an entry from the **Fields** list and double-click it to add the field to **Expression**.

e. If the field length of the bar code must be adjusted according to the number of characters in the data item, select the **Variable Length** check box.

Note: The **Length**, **Fill**, and **Justify** fields appear disabled.

f. If you want to set a fixed length for the bar code, clear the **Variable Length** check box and enter the following information:

- **Length** - The number of characters in the bar code. The data item is truncated or padded so that is has precisely the number of characters.
- **Fill** - The character used to pad the data in order to fit a fixed-length field.
- **Justify** - If a data item is shorter than the number of characters allotted for it, you can justify it to the left, center, or right, within those characters. The remaining characters are set to the character entered in the **Fill** box.

g. Click **OK** to save the bar code data items and to return to the **Badge Element Layout** dialog box.

Note: Repeat the procedure until all data items have been added.

h. To reorder the data items in a track, click **Move Up** and **Move Down**.

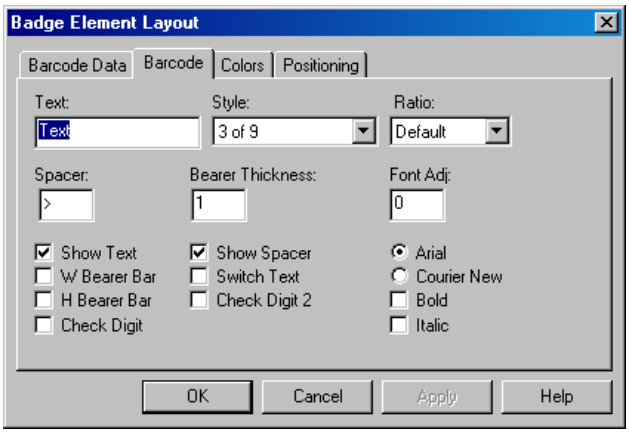
i. To remove a data item from the list, select it and click the **Delete** button.

j. On the **Badge Element Layout** dialog box, click **Apply** to save the data items for the tracks or click **OK** to save the data items for the tracks and to return to the **Badge Definition** window.

- To change the appearance of barcode data:

a. Right-click on the barcode and click **Properties**.

b. Click the **Barcode** tab.



c. Enter the following barcode options:

– **Text** - Text to be displayed above the bar code.

– **Style** - Style setting for the barcode characters.

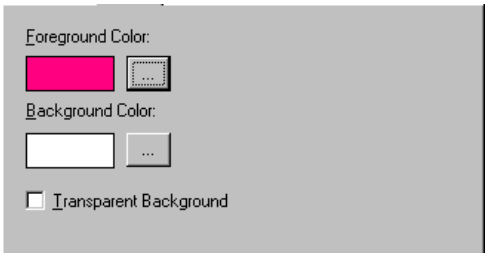
Table 7-6 Style for Bar Codes

Style	Bar Code
2 of 5	MSI
2 of 5 interleaved	ITF
3 of 9	Code 11
Codabar	Code B
Code 39	Telepen
Code 93	UPC A
Code 128	UPC E
EAN 128	Code 128 A
EAN 13	Code 128 B
EAN 8	Code 128 C

- **Ratio**: Determines the ratio of thickness of the thin bars to the thick bars in the bar code. For example, a ratio of 2.00 means that thick bars are twice the width of thin bars.
- **Spacer**: Adds space before and after the bar code when **Show Text** is enabled.
- **Bearer Thickness**: Thickness, in points, of the bearer bars.
- **Font Adj**: Adjusts the font size in relation to the bar code.
- **Show Text**: Displays the bar code data as text underneath the encoded information.
- **W Bearer Bar**: Displays the width bearer bars (top and bottom borders).
- **H Bearer**: Displays the height bearer bars (left and right borders).
- **Check Digit**: For error detection.
- **Show Spacer**: Displays space before and after the bar code data.
- **Switch Text**: Switches the top and bottom text. The bar code data displayed as text is placed above the bar code and the text entered into the **Text** field is displayed below the bar code.
- **Check Digit 2**: For error detection.
- **Arial**: Arial is the text font.
- **Courier New**: Courier New is the text font.
- **Bold**: Applies bolding to the text.
- **Italic**: Italicizes the text.

Common properties of elements

- To set the colors for the elements:
  a. Right-click on the element and click **Properties**.
  b. Click the **Colors** tab.



  c. Click the ellipsis button provided near the **Foreground Color** box to select a foreground color for the element.

d. Click the ellipsis button provided near the **Background Color** box to select a background color for the element.

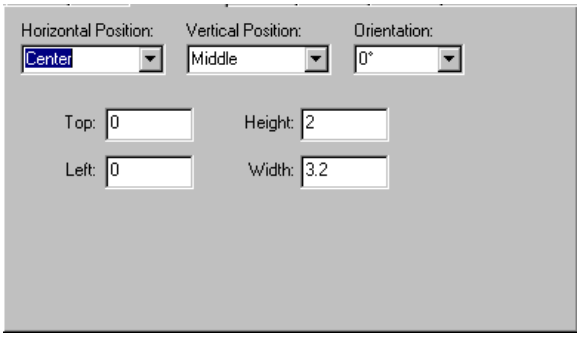
e. Select the **Transparent Background** check box to set a transparent background to the element.

f. Click **Apply** to set the common properties for the element.

- To position the element:

a. Right-click on the element and click **Properties**.

b. Click the **Positioning** tab.



c. Select the **Horizontal Position** of the element.

d. Select the **Vertical Position**.

e. Select the **Orientation**.

f. Type the **Top**, **Left**, **Height** and the **Width** of the badge in millimeters.

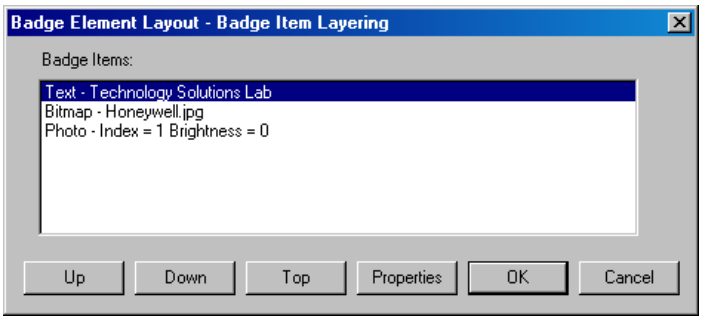
g. Click **Apply** to apply the badge outline.

Item layering order

Badge items are layered as they are placed. When an item is selected, it is brought to the top of the layering order. Layering can also be controlled using the Change Layering icon on the toolbar in the **Badge Definition** window.

- To change the items in the layering order:

a. Click on the toolbar in the **Badge Definition** window. The **Badge Element Layout - Badge Item Layering** dialog box appears, displaying the list of elements placed on the badge.



b. In the **Badge Items** list, select the item to be moved.

c. Click **Up** to move the item up or click **Down** to move the item down.

d. Click **Top** to bring the selected item to the upper layer of the badge.

e. Click **Properties** to open the **Badge Element Layout** dialog box for the selected item. The item's properties can be edited without changing its layering order.

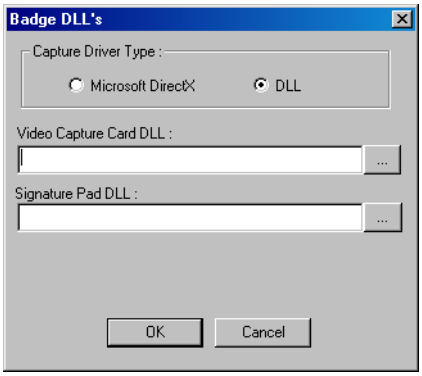
f. Click **OK** to save the changes.

- To select an item in the layering order, click the Select Next Item button. Each time you click the button, it moves to the next item. Continue clicking the button until the item you want is selected.

Configuring Badge DLLs

A specific dynamic-link library (dll) file is required for the video capture card, TWAIN device, and signature pad used with the WIN-PAK System. The DLLs for currently supported hardware are included in the WINPAK PRO directory and are installed from within WIN-PAK.

1. Choose **Configuration > Badge > Badge DLL's**. The **Badge DLL's** dialog box is displayed.



2. Select one of the following **Capture Driver Type** options:

   - **Microsoft DirectX** – Click this option if you want to capture the video using **DirectX** and no specific video capture card driver is required.

- **DLL** – Click this option if you have the access to Video Capture Card DLLs such as FlashBus.dll, FlashPoint.dll, TWAIN.dll and so on.

3. If you have selected **Microsoft DirectX**, select the video driver from the **DirectX Compatible Video Driver** list.
4. If you have selected **DLL**,
   a. Click the ellipsis button next to **Video Capture card DLL**. An **Open** dialog box appears with WIN-PAK PRO opened as the default directory.
   b. Select the appropriate .dll file, and click **Open**. The .dll file path is displayed in the **Video Capture Card DLL** box of the **Badge DLL's** dialog box.

Note: If no DLL is listed in the WIN-PAK PRO directory,

1. Open the **Windows Explorer**.
2. Choose **Tools > Folder Options**. The **Folder Options** dialog box appears.
3. Click the **View** tab.
4. Under Advanced settings, expand **Files and Folders** and then **Hidden files and folders.**
5. Click **Show hidden files and folders**.
6. Click **Apply** to apply the changes you have made and click **OK** to exit from the dialog box.

7. Click the ellipsis button next to **Signature Pad DLL**. An **Open** dialog box appears with WIN-PAK PRO opened as the default directory.
8. Select the appropriate .dll file and click **Open**. The path of the .dll file is displayed in the **Signature Pad DLL** box of the **Badge DLL's** dialog box.

Note: This DLL is applicable for the Signature Pad for both the **Capture Driver Types**.

9. Click **OK** to save the dll details and to close the **Badge DLL's** dialog box.

Setting up Badge Printers

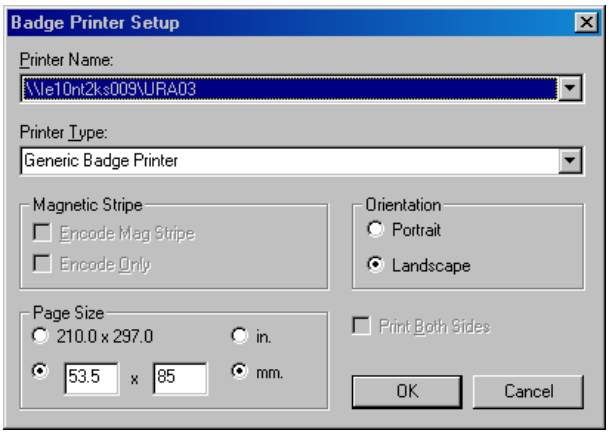
Overview

WIN-PAK PRO is compatible with many printers. Any printer that is supported by the Windows operating system can be used for printing badges. However, for two-sided PVC printing or magnetic stripe encoding, a Datacard IC III series or the Ultra Magicard Turbo series printer is required. In addition, Windows-compatible laser or other color printers can be used to print badges on paper.

Note: Install your printer(s) using the Windows Control Panel. (Refer Microsoft documentation for more information.)

Configuring Badge Printers

1. Choose **Configuration > Badge > Configure Badge Printer**. The **Badge Printer Setup** dialog box appears with the list of printers configured in your computer.



2. Select the printer required for badge printing in the **Printer Name** list.
3. Select the **Printer Type**.
4. Under **Magnetic Stripe**, select the **Encode Mag Stripe** check box if you want to encode magnetic stripe information.
5. Select **Encode Only** if you want to only encode the magnetic stripe information and not print it.
6. Under **Orientation**, click **Portrait** or **Landscape**. The default orientation for the badge is **Landscape**.
7. Under **Page Size**, select the page size in inches or millimeters. The default page size for the badge is 53.5 mm x 85 mm.
8. Click **OK** to save the badge printer settings and close the **Badge Printer Setup** dialog box.

Card Holders

8

In this chapter...

Overview

The chapter **Card Holders** describes how to configure card and card holders details and to assign cards to a card holder. In general, cards are added to WIN-PAK in large volume and later, they are assigned to the card holders as per the need.

A card holder can hold more than one valid card at the same time. These cards can be used by the card holder for access to multiple facilities. Multiple cards can also be issued to the family members of the card holder for using company facilities, such as gym, recreational center and so on.

The card and card holder information are defined for a specific account. Therefore, you must select an account to enable the card and card holder menu options.

Card

Cards are defined by card number, access level, and the status of the card whether Active or Inactive. Badge designs can be assigned to the cards and cards can be assigned with a PIN number for enabling high security. WIN-PAK enables you to add a single card or a bulk of cards. Later, the cards are associated to the employees, visitors, and so on.

In addition, you can define a card as a privileged card that can be used for setting the Galaxy group or arm the Vista partitions. However, you must procure the license for the Galaxy panel and/or Vista panel to avail this facility in WIN-PAK.

Card Holders

A Card Holder is a person who holds a card. Card Holders in WIN-PAK are defined by information such as First Name and Last Name and User-defined fields referred to as note fields. These fields are used for storing the additional information of a card holder such as qualification, passing year, employee number, and so on.

In addition, a card holder can be associated to user codes for accessing the Galaxy panel or Vista panel. However, you must procure the license for the Galaxy panel and/or Vista panel to avail this facility in WIN-PAK.

Note: Before you configure the card and card holder details, Honeywell recommends you to define the following:

- Time Zones
- Devices
- Access Areas
- Badge Design

Refer to the "Time Management", "Device Map", "Defining Areas", and "Badge Layout" chapters for more details on the above-mentioned sections.

Configuring Additional Information

As card holder information is specific to an account, you must select an account before you start working with card holders. If required, you can also configure the following additional information before you configure a card holder:

- Note fields
- Card holder tab layouts
- Access levels

Note field is a user-defined field for adding additional information to the card holder. These note fields are grouped together to form a card holder tab layout. Access level is a level of access provided to the Card Holders for various doors in the WIN-PAK system.

Note: The detailed information on note fields, card holder tab layouts and access levels are explained in the forth-coming sections.

Refer to the "Configuring Note Field Template", "Configuring Card Holder Tab Layout" and "Configuring Access Levels" sections in this chapter.

Therefore, configuring a Card Holder includes:

- **Selecting an Account** - You must select a specific account to enable the Card Holders menu options.
- **Configuring Note Field Template** - You can configure a note field template and associate it with the card holder tab layout.
- **Configuring Card Holder Tab Layout** - You can configure a card holder tab layout and associate it to card holders.
- **Configuring Access Levels** - You can configure various access levels and set the permissions for the access to doors based on the time zones.

Selecting an Account

Card holders are defined for a specific account.

To select an account, perform the following steps:

1. Choose **Account > Select**. The **Select Account** dialog box appears.
2. Select an account in the list.
3. Click **OK**. The account is selected and displayed in the Title bar.

Note: To enable the card holders menu options, you must select an account.

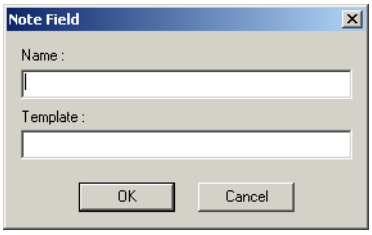
Configuring Note Field Template

Note field template is a field that is defined for recording card holders' additional information such as Gender, Date of Birth, College Studied, Passing Year, and so on. WIN-PAK enables you to define a maximum of 40 note fields.

Adding a Note Field Template

To add a note field template:

1. Choose **Configuration > Card Holder > Note Field Template**. The **Note Field Template** window appears.
2. Click **Add** to add a new note field template. The **Note Field** dialog box appears.



3. Type the **Name** of the note field. For example, Passing Year.
4. Type the format of the **Template**.

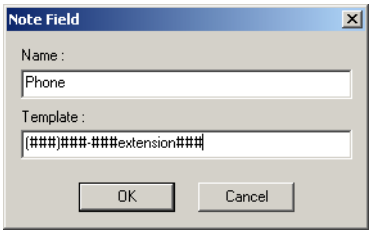
   The template defines the character type and the number of characters in the note field. Thus, it creates a mask for the note field for consistent and unambiguous usage. The following table describes the list of mask properties:

Table 8-1 Describing mask properties with examples

Input character	Mask Description	Example (Name, Template)
Nil	No mask is applied.	
#	Only numbers (0-9) are allowed.	DOB, ##/##/####
?	Only alphabets (a-z or A-Z) are allowed.	Name, ????????????
A	Only alphanumeric characters (0-9, a-z and A-Z) are allowed.	
U	Only upper-case alphabets (A-Z) are allowed.	Time, ##:## UU
L	Only lower-case alphabets (a-z) are allowed.	
&	Any characters are allowed including special characters.	

Table 8-1 Describing mask properties with examples

Input character	Mask Description	Example (Name, Template)
~	Defines the list of items.	Color, ~Red~Green~Blue~
\ (Escape Character)	Defines the character position in the note field.	



5. Click **OK** to create a new note field template.

Note: To use the note fields in the card holder, the note fields must be added to a card holder tab layout.

Searching and Sorting Note Field Templates

To search and sort a note field template:

1. Choose **Configuration > Card Holder > Note Field Template**. The **Note Field Template** window appears.
2. Select an item in the **Search Field** list.
   - **All** - Lists out all the note field templates.
   - **Name** - Searches for similar note field names.
   - **Template** - Searches for similar template names.
3. If you have selected **Name** or **Template** in the **Search Field**, select the **Criteria**.
   - **Begins With** - Searches for the name or template that begins with the text in the **Search For** text box.
   - **Equals** - Searches for the name or template that exactly matches with the text in the **Search For** text box.
   - **Greater Than** - Searches for the name or template that is alphabetically greater than the text in the **Search For** text box.
   - **Less Than** - Searches for the name or template that is alphabetically less than the text in the **Search For** text box.
4. Type the text to be searched in the **Search For** text box.
5. Select an item in the **Sort By** list.

- **None** - No sorting required.
- **Name** - Sorts the list in the ascending order of the names.
- **Template** - Sorts the list in the ascending order of the templates.

6. Click **Update List** to list the searched items in the sorted order.

Notes:

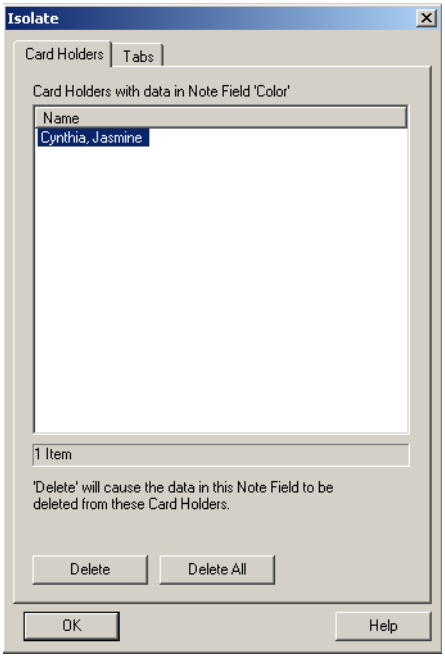
- If you want to sort the entire list, you can perform any of the following steps:
  a. Double-click the column title to be sorted out.
  b. Select **All** in the Search Field list, select the **Sort By** item and then click **Update List**.
- If you want to search without any sorting, you can perform the following steps:
  a. Enter the details to search.
  b. Select **None** in the **Sort By** list and then click **Update List**.

Isolating and Deleting a Note Field Template

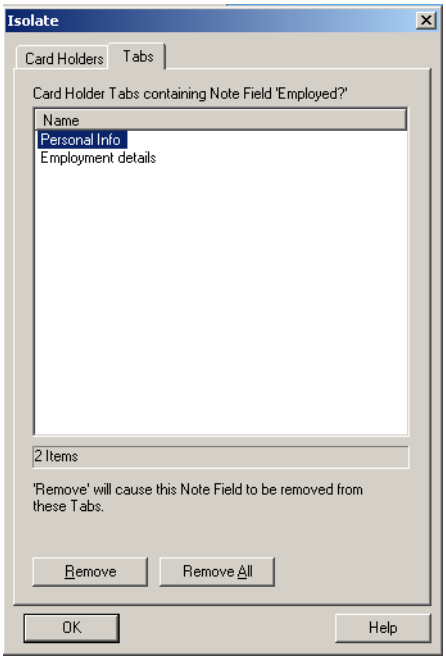
To delete a Note Field, it must be isolated from the card holder tab layouts and/or card holders.

To isolate a Note Field:

1. Choose **Configuration > Card Holder > Configure Note Field Template**. The **Note Field Template** window appears.
2. Select the note field to be isolated and/or deleted.
3. Click **Isolate**. The **Isolate** dialog box appears.
4. Click the **Card Holders** tab. It is selected by default.



5. Select the card holder in the **Name** list. You can also select multiple card holders by holding the SHIFT key or CTRL key while selecting.
6. Click **Delete** to remove the selected note field from the card holder details or click **Delete All** to remove all the note fields. A message for confirming the deletion appears.
7. Click **Yes** to delete.
8. Click the **Tabs** tab. The list of tabs associated with the note field is displayed.



9. Select the tab in the **Name** list. You can also select multiple tabs by holding the SHIFT key or CTRL key while selecting.
10. Click **Remove** to isolate the selected tabs from the tab note fields or click **Remove All** to isolate all the note fields. A confirmation for isolation appears.
11. Click **Yes** to confirm the isolation.

To delete a note field:

1. In the **Note Field Template** window, select the note field from the list.
2. Click **Delete**. A confirmation for deletion appears.
3. Click **Yes** to confirm the deletion.

Configuring Card Holder Tab Layout

A card holder tab layout is a collection of user-defined note fields. For example, Educational Info tab may contain the note fields such as College Name, Passing Year, Aggregate, and so on. This card holder tab layout will be displayed in the **Card Holder** window.

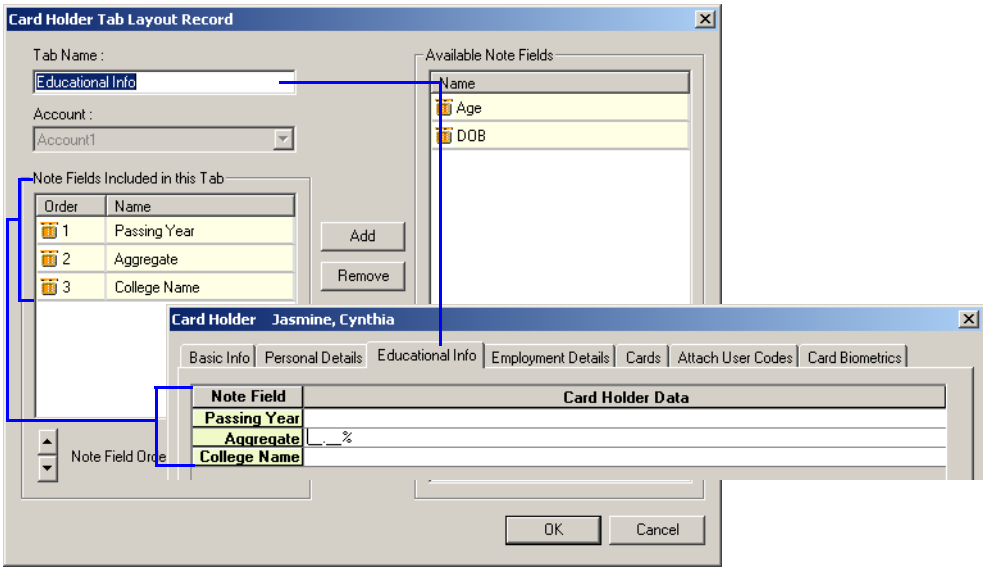


Figure 8-1 Customizing Card Holder information using Card Holder Tab Layout

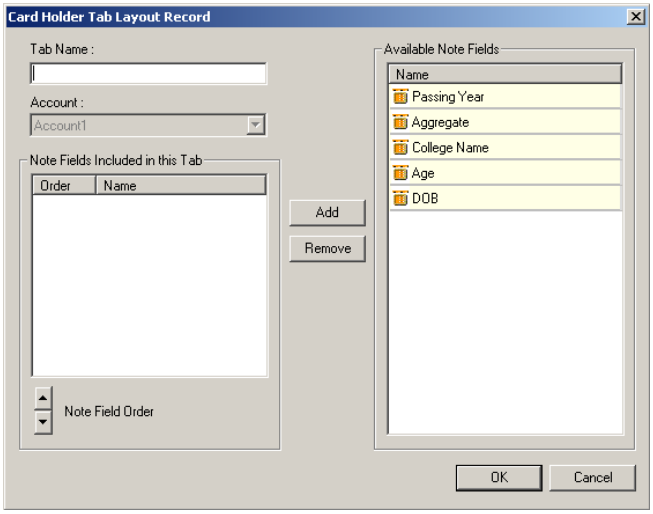
Adding a Card Holder Tab Layout

Before adding a card holder tab layout, ensure that the note field templates are added.

To add a card holder tab layout:

1. Choose **Account > Select** to select the account to which you want to add the card holder tab layout.
2. Choose **Configuration > Card Holder > Card Holder Tab Layout**. The **Card Holder Tab Layout** window appears.

3. Click **Add** to add a new card holder tab layout. The **Card Holder Tab Layout Record** window appears.



4. Type the **Tab Name**. For example, Educational Info.
5. In the **Available Note Fields**, select a relevant note field to be added to the card holder tab layout. For example, College Name.

Note: To select multiple note fields:

* In sequence: Hold the SHIFT key and select the note fields.
* At random: Hold the CTRL key and select the note fields.

6. Click **Add** to add the selected note fields to the card holder tab layout.
7. To remove a note field, select the note field and click **Remove**.
8. To change the order of note fields in the list, select the note field and click or .
9. Click **OK** to add a new card holder tab layout.

Rearranging the Card Holder Tab Layouts

You can rearrange the card holder tab layouts in a sequence that has to be displayed in the Card Holder window.

To rearrange the card holder tab layouts:

1. Choose **Configuration > Card Holder > Card Holder Tab Layout**. The **Card Holder Tab Layout** window appears.
2. Select the card holder tab layout to be rearranged.
3. Click or to move the selected tab up or down. The card holder tab layouts are rearranged accordingly.

Configuring Autocard Lookup

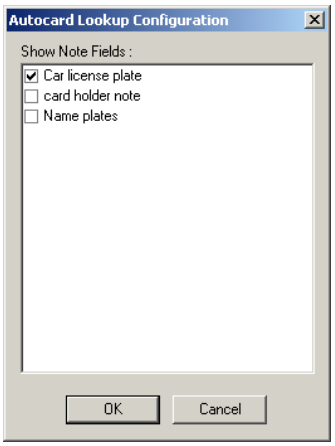
When a card is accessed, WIN-PAK identifies the card holder and displays the basic information in **AutoCard Lookup** by default.

Refer to the "Autocard Lookup" section in the chapter Monitoring Actions for more details on activating autocard lookup window and viewing the card holder details.

If you want to view additional information of the card holder in the Autocard Lookup window, you have to configure the settings using the **Autocard Lookup** option.

To include additional information (note fields) of the card holder:

1. Choose **Configuration > Card Holder > Configure Autocard Lookup**. The **Autocard Lookup Configuration** dialog box appears.



2. In the **Show Note Field** list, select the note fields that must be displayed in the Autocard Lookup window.
3. Click **OK** to save the configuration and close the dialog box.

Configuring Access Levels

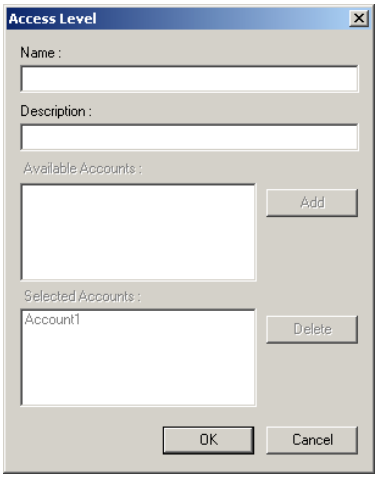
Access levels provide restricted access to the WIN-PAK users for various areas in the access control system. The **Access Level** window contains information of the existing access levels and the corresponding access areas.

Note: Before you configure the access levels, ensure that you have defined the access areas. Refer to the "Defining Access Areas" section in the chapter Defining Areas.

Adding a New Access Level

To add a new access level:

1. Choose **Card > Access Level**. The **Access Level** window appears. The existing access levels are displayed on the left and the Access Areas on the right.
2. Click **Add**. The **Access Level** dialog box appears. The access level is account specific and so the current account is listed in the **Selected Accounts** list.



3. Type the **Name** of the access level and the **Description**.
4. If the access level is specific to visitors, select the **Visitor** check box. The visitor check box is displayed, only if you have license for Visitor Management.

   Refer to the "Adding Access Level" section in the chapter Visitor Management System for more details.
5. If you want to assign the access level to the other accounts, select the account in the **Available Account** list and click **Add**. The account is moved to the **Selected Account** list.

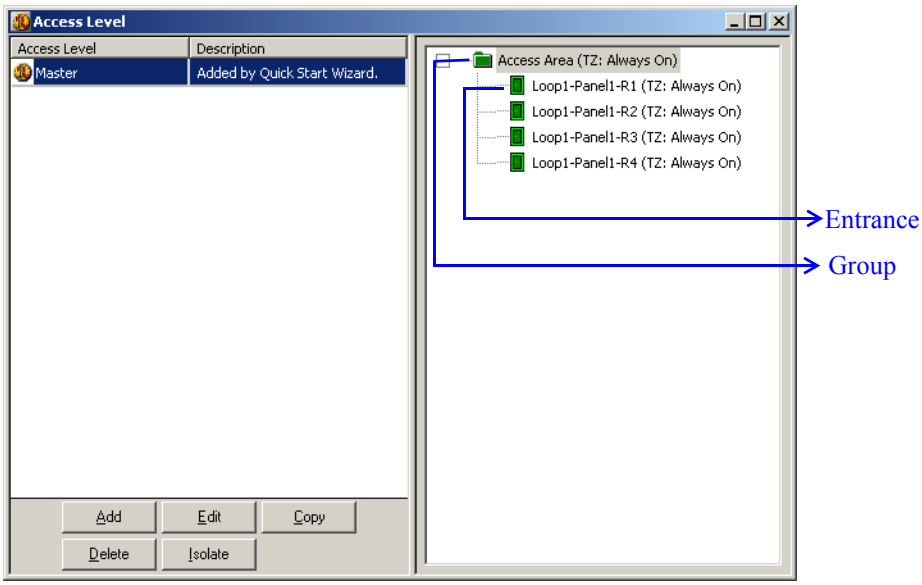
   Note: To remove the account from the **Selected Account** list, select the account and click **Remove**. It is moved to the **Available Account** list.
6. Click **OK** to save the details and close the dialog box.

   Note: The newly added access level has no rights assigned to it.

Configuring Access Area

To configure an access area:

1. Choose **Card > Access Level**. The **Access Level** window appears.



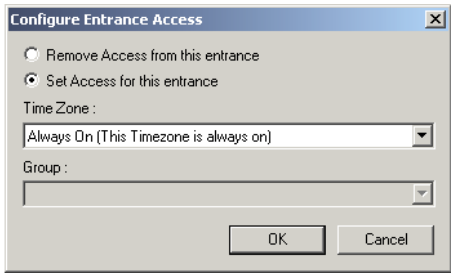
   The left-side of the window lists the access levels and the right-side of the window displays the access area tree.

2. Select the access level from the left-side to view the access areas of the selected level. The color of an icon defines the access permission of a group (folder) or an entrance.

   - **Red** - No access is permitted to any of the entrances in the area.
   - **Yellow** - Access permitted to some entrances in this area.
   - **Green** - Access permitted to all the entrances in this area during the assigned time zone.

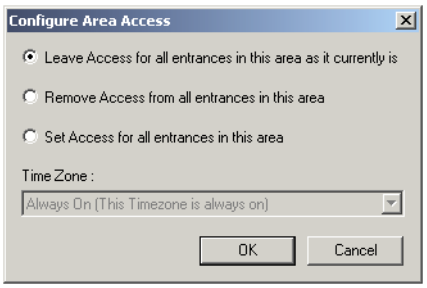
3. In the **Access Level** window, right-click the access area to which you want to set the access levels and select **Configure**. The **Configure Area Access** dialog box appears.

4. For an entrance, select one of the following:



- **Remove Access from all entrances in this area** to deny access through this entrance for this access level.
- **Set Access for all entrances in this area** to allow access through this entrance for a particular time zone. Select the time zone in the Time Zone list to determine periods of access.

For group entrance, select one of the following:



- **Leave Access for all entrances in this area as it currently is** to continue the same for each entrance in this group.
- **Remove Access from all entrances in this area** to deny access through these entrances for this access level.
- **Set Access for all entrances in this area** to allow access through these entrances for a particular time zone. Select the time zone in the Time Zone list to determine periods of access.

5. To search for a specific reader or device in a tree, right-click and select **Find**. Type the full text and click **OK**. The reader or device is selected.
6. To refresh the list, right-click and select **Refresh**.

Copying the access level

WIN-PAK enables you to create a copy of the existing access level with the same properties.

To create a copy of an access level:

1. Choose **Card > Access Level**. The **Access Level** window appears.
2. Select the access level to be copied and click **Copy**. The **Access Level** dialog box appears with the existing set up.
3. Type the new **Name** for the access level. By default, the name is prefixed by the word “Copy of”.
4. Change other settings if required and click **OK**. This duplicates the access level.

Isolating and deleting access levels

You cannot delete an access level, when it is associated to a card or card holder. In such a case, you must isolate the access level from the card and card holder and reassign it to an alternate access level.

To isolate the access level:

1. Choose **Card > Access Level**. The **Access Level** window appears.
2. Select the access level to be deleted and then click **Isolate**. The **Isolate** dialog box appears with a list of associated cards and card holders.
3. Select the card and the alternate access level.
4. Click **Reassign** to reassign the selected card.

   OR

   Click **Reassign All** to reassign all the associated cards.
5. Click **OK** to close the **Isolate** dialog box.

To delete the access level:

1. Choose **Card > Access Level**. The **Access Level** window appears.
2. Select the access level and click **Delete**. The access level is deleted.

Configuring Card and Card Holder Information

In WIN-PAK, you can configure card and card holder information by:

1. Adding a card and card holder in WIN-PAK manually.

   Refer to the "Adding a Card and Card Holder Information"section in this chapter for adding a card and card holder information in WIN-PAK manually.
2. Importing the card and card holder information from an Excel sheet to WIN-PAK.

   Refer to the "Importing from Excel Sheet" section in this chapter for importing a card and card holder information from an excel sheet.

Adding a Card and Card Holder Information

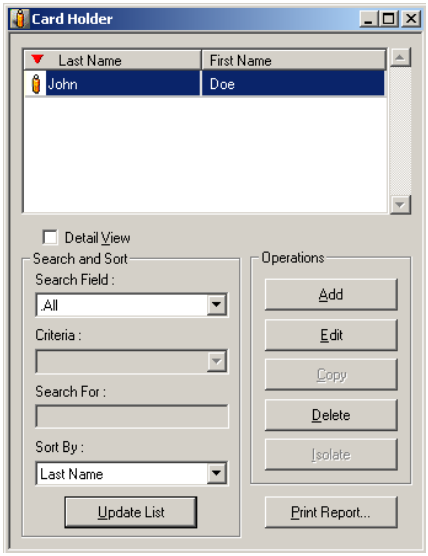
Adding a Card Holder

Adding a card holder involves:

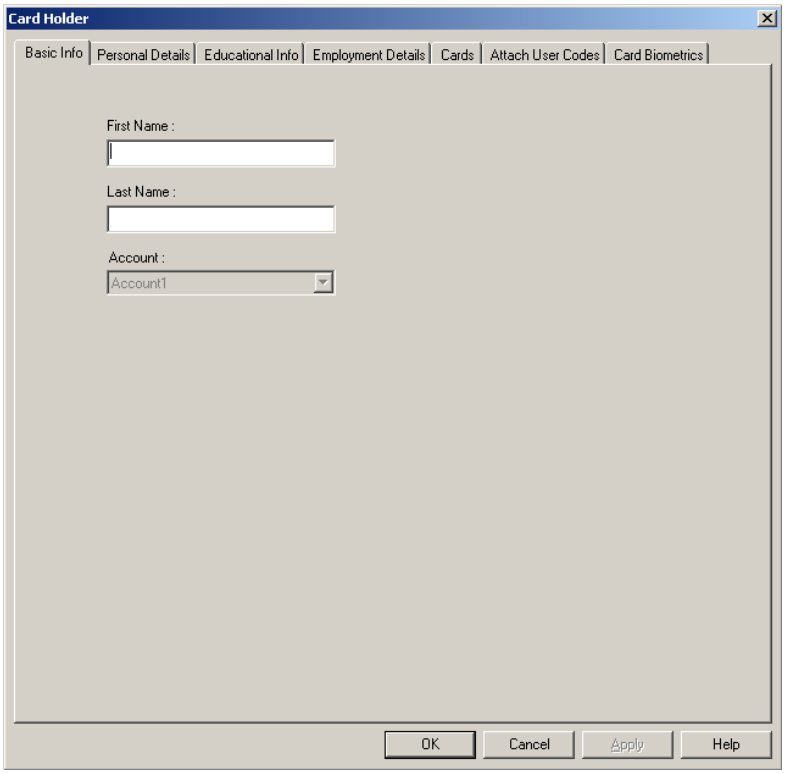
- Providing card holder basic information
- Providing card holder additional information
- Adding a new card and attaching the card to the card holder

Providing card holder basic information

1. Choose **Card > Card Holder** or click in the toolbar. The **Card Holder** window appears.



2. Click **Add** or click in the toolbar. The **Card Holder** dialog box appears.



3. In the **Basic Info** tab, type the **First Name** and **Last Name** of the card holder. These fields are mandatory.

Note: The card holder details are specific to an account. Therefore, select an account before adding a card holder. You cannot change the account while adding the card holder details.

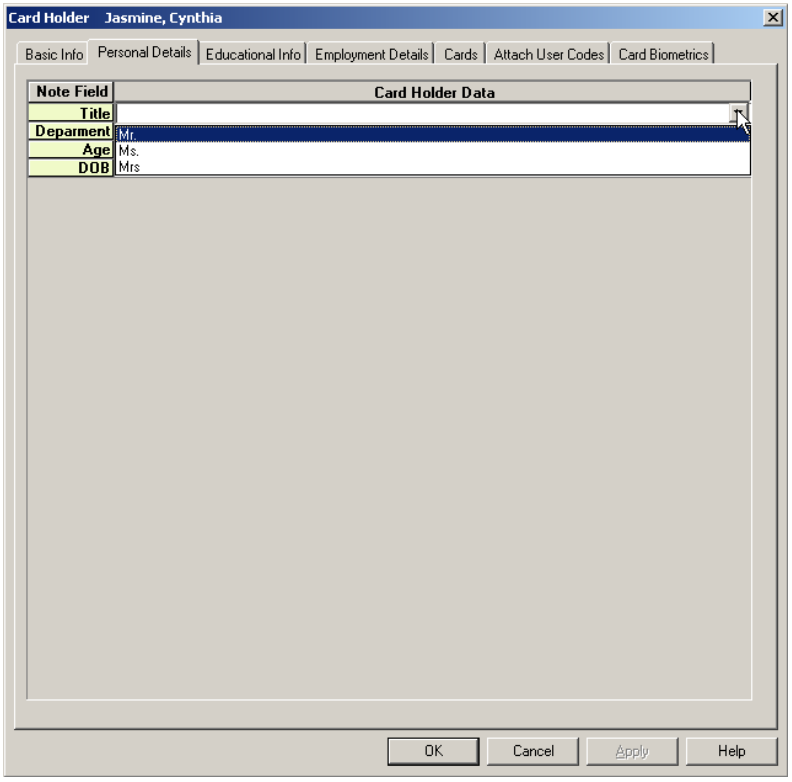
4. Click **OK**. The basic information is saved.

Providing card holder additional information

Using the user-defined tabs, you can add the additional information of the card holder.

1. Choose **Card > Card Holder**. The **Card Holder** window appears.
2. Click **Add**. The **Card Holder** dialog box appears.
3. Select the user-defined tab to add the additional information of the card holder.

Note: The user-defined tabs are displayed in the **Card Holder** dialog box, only if you have already defined these tabs in **Card Holder Tab Layout**.

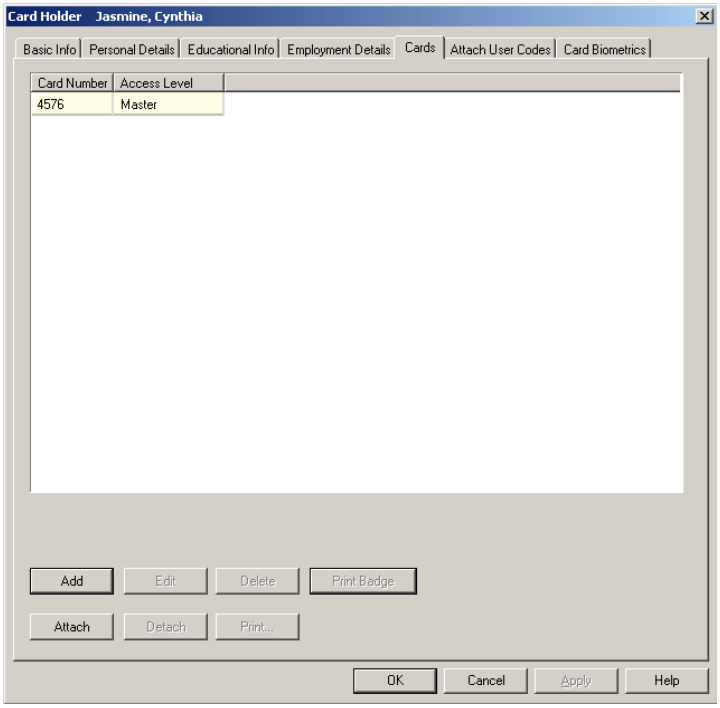


4. Enter the additional information of the card holder in the fields under the **Card Holder Data** column.
5. Repeat steps 3 and 4 for the remaining user-defined tabs.
6. Click **Apply**. The additional information is saved.

Adding and attaching a card to a card holder

Using the Cards tab, you can attach a new card or an existing card to a card holder. In addition, you can print a badge associated to it or you can print the card reports.

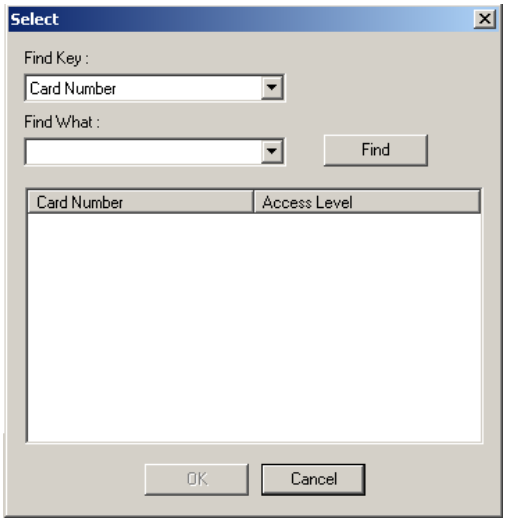
1. In the **Card Holder** dialog box, click the **Cards** tab.



2. Click **Add** to add a new card. The **Card Record** dialog box appears.

   Refer to the "Adding a Card" section in this chapter for details on adding cards. The new card is automatically attached to the card holder, after adding it here.

3. Click **Attach** to attach an existing card to the card holder. The **Select** dialog box appears.



4. Select **Card Number** or **Access Level** in the **Find Key** list.
5. Enter the keyword in the **Find What** list and click **Find**. The cards that match the criteria are displayed.
6. Select the card and click **OK**. The selected card is attached to the card holder.

To edit the card details:

a. Select the card from the list of cards and click **Edit**. The **Card Record** dialog box appears.

b. Change the required card details and click **OK**.

To delete a card:

a. Select the card from the list of cards and click **Delete**. A confirmation message appears for deletion.

b. Click **OK**. The card is deleted from the database.

To detach a card:

a. Select the card from the list and click **Detach**. The card is detached from the card holder.

Note: If you detach a card, it is dissociated from the card holder and not deleted from the card list.

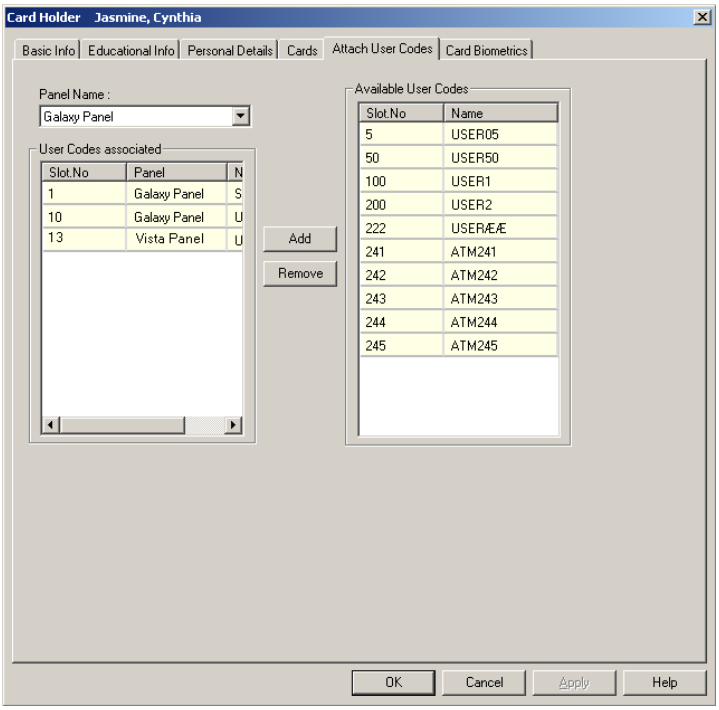
Attaching user codes to a card holder

A card holder can be attached to the user codes for accessing and working on the Galaxy panel or Vista panel.

To attach user codes to the card holder:

1. In the **Card Holder** dialog box, click the **Attach User Codes** tab.

Note: The **Attach User Codes** tab is displayed in the **Card holder** dialog box, only if you procure the license for the Galaxy panel and/or Vista panel features in WIN-PAK.



2. In the **Panel Name** list, select the panel to which you want to associate the user codes. The user codes that are configured for the selected panel are listed out.

   The **Panel Name** list contains the Galaxy and Vista panels that are configured in the Device Map.

   Refer to the "Adding a Galaxy Panel" or "Adding a Vista Panel" section in the chapter Device Map for configuring panels in WIN-PAK.

3. In the **Available User Codes** list, select the user codes to be associated to the card holder.

4. Click **Add**. The selected user codes are moved to the **User Codes associated** list.

   Tip: If you want to remove the associated user codes, select the user codes from the User Codes associated list and click **Remove**.

Printing a badge and card report

To print a badge associated with the card,

1. Select the card from the list and click **Print Badge**. The badge is printed.

   OR

   Perform the following steps:

   a. Select the card from the list and click **Print**. The **Select Printed Output** dialog box appears.

b. Click **Print Cards**. The **Print Badge Preview** of the badge associated to the selected card appears.

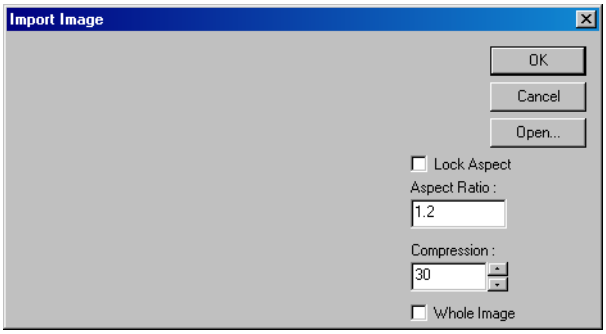
c. Click **Print**. The badge is printed.

Note: Use the **Previous** and **Next** buttons to move to the rest of the badges associated to the card and click **Print**.

Attaching a photo or badge to a card holder

To attach a photo:

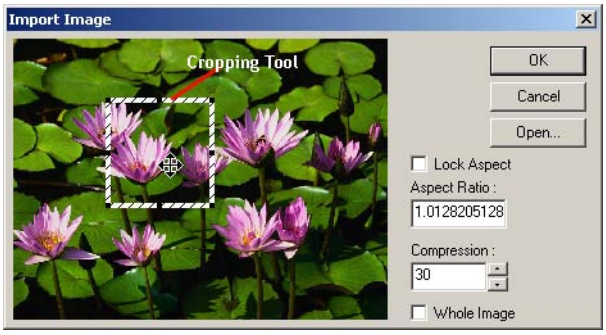
1. In the **Card Holder** dialog box, click the **Card Biometrics** tab.
2. In the **Frame Selected** list, select **Photo** to attach a photo or badge to the card holder. The **Photo** frame is highlighted.
3. Under **Badge Layout**, click **Photo** to attach a photo.
4. To import an image file for the photo:
   a. Click **Import**. The **Import Image** dialog box appears.



   b. Click **Open** and browse through the required folder.
   c. Select the image file and click **Open**. The selected photo appears in the display area.

d. Select the **Whole Image** check box to import the photo without cropping.

e. To crop the photo, clear the **Whole Image** check box. The cropping tool appears on the photo.



f. To increase the grid size, click the corners of the grid and drag it to the required size.

g. To maintain the consistent height and width, enter the **Aspect Ratio** value.

h. To maintain the same ratio of height and width, select the **Lock Aspect** check box.

i. Adjust the **Compression** setting at this point, if required.

Note: 100 is the least compression and the best quality. 30 is the highest compression and the lowest quality.

j. Click **OK** to close the dialog box and import the photo.

5. To capture a photo using a camera:

a. Click **Capture**. The **Capture Image** window appears with the live show from your video camera.

b. Click **Settings** to expand the window and access the video settings.

c. Adjust the **Video** settings for a satisfactory image.

Table 8-2 Live Screen Video Image Settings

Setting	Description
Brightness	Lightens or darkens the entire tonal range of the image.
Contrast	Expands or contracts the entire tonal range of the image.
Saturation	Adjusts the vibrancy or the level of color in the image.
Hue	Adjusts the value of color in the image. This corrects the incorrect coloring of images.
Sharpen	Sharpens blurry images by increasing the contrast of the adjacent pixels.

Table 8-3 Live Screen Grab Settings

Setting	Description
Brightness	Lightens or darkens the entire tonal range of the image.
Contrast	Expands or contracts the entire tonal range of the image. These settings are applied to the camera when an image is captured. If you are not using a flash, set the Contrast to the same as the Video settings. If a flash is used, reduce the Contrast settings to lower than the Video settings. This prevents overexposure of the picture. **Note**: The exact settings must be determined by experimentation, as they vary depending on the type of flash, distance from the subject, and other lighting being used.

Note: If you are not using a flash, set the Grab settings to the same values as the Video settings. If you are using a flash, reduce the Grab Brightness and Contrast. (The exact settings may vary depending on the type of flash and other lighting. The exact settings can be determined only by experimenting.)

d. Click **Freeze** to capture the image.

e. To crop the captured image, use the cropping frame or enter the image proportion in **Aspect Ratio**, and select the **Lock Aspect Ratio** check box.

Tip: If you are using the default badge size, set the aspect ratio to 625, to fill the entire badge outline.

f. Adjust the **Photo settings** of the captured image.

Table 8-4 Live Screen Photo Settings

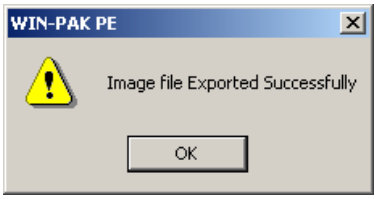
Setting	Description
Photo Brightness	Lightens or darkens the entire tonal range of the captured image.
Compress	The captured image is saved as a .jpg file. If required, use the slider to adjust the compression of the saved image. The lower the number, the greater the compression. **Note:** Images lose quality as they are compressed, and thus it is recommended to avoid over-compressing. **Example:** A setting of 100 applies the least amount of compression and provides the best image quality. A setting of 30 applies the most compression, but provides lower image quality.

g. Click **OK** to save the photo and close the **Capture Image** window.

Note: A camera (Web camera, Analog camera, or USB camera) must be connected to the system for capturing an image. If you are using an analog camera, use the Frame Grabber to convert analog signals to digital signals for the system to understand the signals.

6. To export the captured image into a file:

   a. Click **Export**. A confirmation message appears indicating that the image is exported.



   The image is exported to a file and the file is stored in the **Database\Exported Files** folder in the WIN-PAK installation path. The format of the file is <First Name>b<Last Name>b<index of the photo>.jpg, where b indicates blank.

   b. Click **OK**.

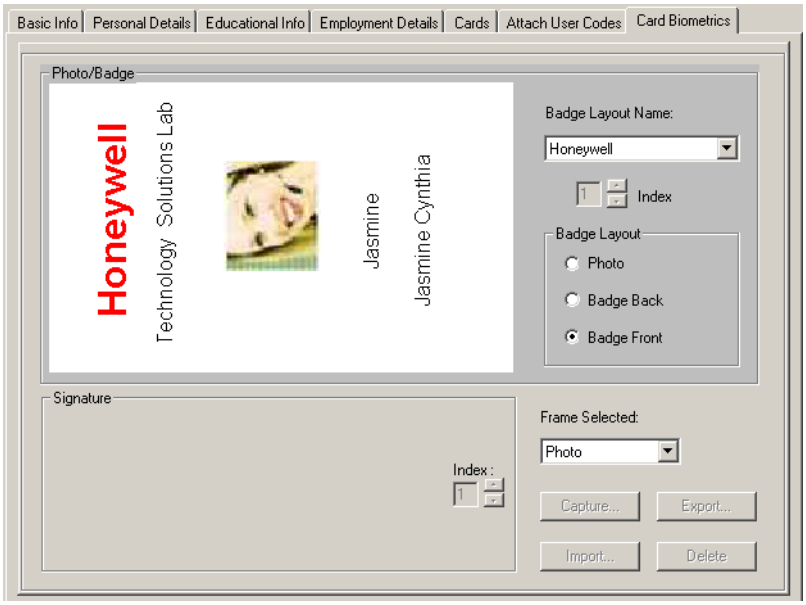
To capture additional card holder photos:

- Follow the same procedure of capturing a card holder's photo.
- Change or increase the **Index** number.

Caution: If you capture a different image with the same index number, the new photo replaces the existing photo.

To attach a badge to a card holder:

1. In the **Card Holder** dialog box, click the **Card Biometrics** tab.
2. In the **Frame Selected** list, select **Photo** to attach a photo or badge to the card holder. The **Photo** frame is highlighted and the attached photo is displayed in the preview area.
3. Under **Badge Layout**, select **Badge Back** or **Badge Front** to attach a badge to a card holder at the back or front.

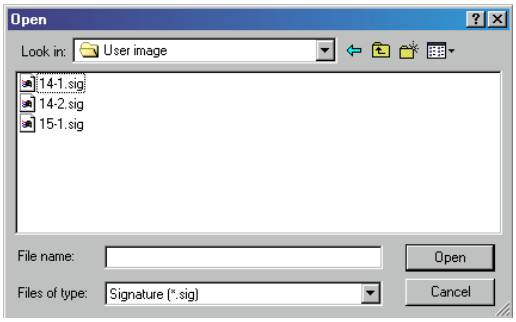


4. Select the badge design in the **Badge Layout Name** list. The selected badge design is displayed in the preview area.

Tip: To detach a badge, select None in the **Badge Layout Name** list.

Attaching a signature to a card holder

1. In the **Card Holder** dialog box, click the **Card Biometrics** tab.
2. In the **Frame Selected** list, select **Signature** to attach a signature to the card holder. The **Signature** frame is highlighted.
3. To import an existing signature file:
    a. Click **Import**. The **Open** dialog box appears.



b. Select the signature file (.sig or .emp file) and click **Open**. The signature is displayed in the preview area.

OR

To capture the signature, click **Capture**. The **Enter Signature** dialog box is displayed.

Note: Ensure that a digital writing pad is connected to the system, before capturing the signature.

a. Select the **Signature Width** as Thin, Bold, Thick.

b. Click **OK** to close the dialog box and display the signature on the **Card Biometrics** tab.

4. To delete the signature, click **Delete**.

To capture additional card holder signatures:

- Follow the same procedure of capturing card holder signature.
- Change or increase the **Index** number.

Caution: If you capture a different image with the same index number, the new signature replaces the existing signature.

Adding a new card and attaching it to a card holder

The Card Biometrics tab enables you to add a new card (with basic details like card number and access level) and attach it to the card holder.

To add a new card:

1. In the **Card Holder** dialog box, click the **Card Biometrics** tab.
2. At the bottom, click **New** next to **Card Number**.
3. Type a unique **Card Number** and press ENTER.
4. Select the **Access Level** of the new card. The new card is added and attached to the card holder.

   Tip: To verify the card attachment, click the **Card** tab and view the new card in the card list.
5. To print the badge design attached to the card, click **Print Badge**.

   Note: After printing the badge, the **Status** of printed is automatically changed to **Printed**. However, you are provided with an option to change.
6. Click **OK** to save and close the **Card Holder** dialog box.

Editing Card Holder Information

To edit the card holder details:

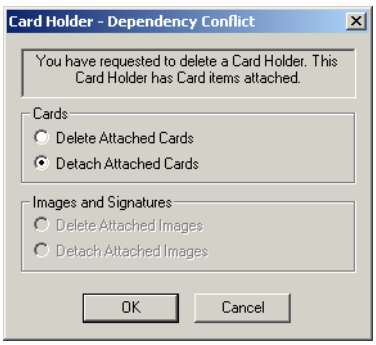
1. Choose **Card > Card Holder**. The **Card Holder** window appears.
2. Select the card holder from the list and click **Edit**. The **Card Holder** dialog box appears.

   Refer to the "Adding a Card Holder" section in this chapter for information on editing card holder details.

Deleting a Card Holder

To delete a card holder:

1. Choose **Card > Card Holder**. The **Card Holder** window appears.
2. Select the card holder to be deleted from the list and click **Delete**. The **Card Holder - Dependency Conflict** dialog box appears.



3. Select **Delete Attached Cards** to delete the cards attached to the card holder.

   OR

   Select **Detach Attached Cards** to detach the cards from the card holder.
4. Click **OK**. A confirmation for deletion or detachment appears.
5. Click **Yes** to confirm the deletion or detachment.

Note: You can also delete or detach the images or signatures attached to the card holder.

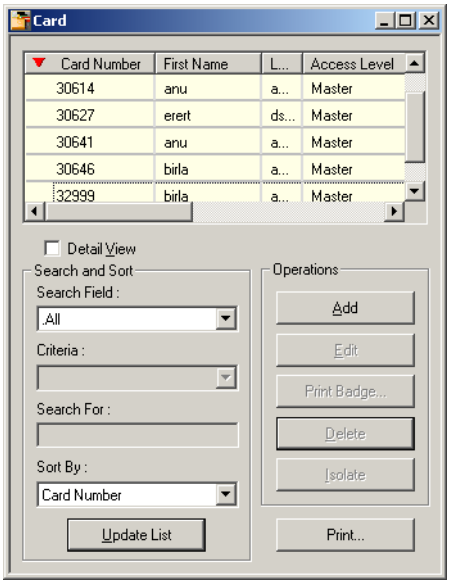
6. Select the appropriate option to delete or detach the attached images or signatures and click **OK**.
7. Click **Yes** to confirm the deletion or detachment.

Adding a Card

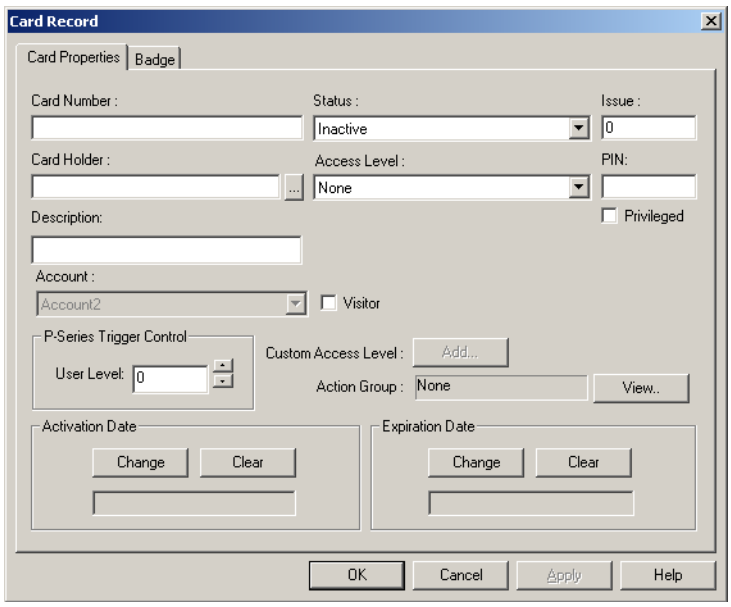
A card holder is uniquely identified by the card. The access levels can be defined for the cards. When a card is attached to a card holder, the card holder has access only to those areas of the access level.

To add a card:

1. Choose **Card > Card** or click  in the toolbar. The **Card** window is displayed.



2. Click **Add** to add a new card. The **Card Record** dialog box appears.



3. Click the **Card Properties** tab. It is selected by default.
4. Type a unique **Card Number**.
5. Click the ellipsis [...] button to select the **Card Holder**. The **Select** dialog box appears.
6. Select the **First Name** or **Last Name** in the **Find Key** list.
7. Enter the keyword in the **Find What** box and then click **Find**. A list of card holders that matches the criteria is displayed.

Note: To list all the card holders, click **Find** without entering the keyword.

8. Select the card holder and click **OK**. The **Select** dialog box is closed and returned to the **Card Record** dialog box.
9. Select the **Status** of the card:
   - **Active**: The card is ready for access. It is selected by default.
   - **Inactive**: The card is on hold for access.
   - **Lost or Stolen**: The card is lost or stolen and the access is restricted.
   - **Trace**: The card is ready for access and given special attention while accessing. The card details are displayed in Alarm View while accessing the card.
10. Select the access level of the card in the **Access Level** list. You must assign an access level, if you have selected the **Status** as **Active** or **Trace**.
11. Type the **Issue** number to trace the number of times the card is issued.
12. Type the unique **PIN** number. The PIN number adds more security to the card.
13. Select the **Privileged** check box if the card must be assigned as a privileged card. The card holder can set or unset the galaxy groups associated to the

reader on which the card is presented. If the Vista feature is enabled, the card holder can or arm or disarm the vista partitions.

Refer to the "Configuring a reader to the panel" section in the chapter Device Map for more details on associating galaxy groups or vista partitions to the reader.

Note: This option is available only if you avail a license for the Galaxy panel and/or Vista panel in WIN-PAK.

14. Describe the card details in **Description**.
15. Select the **Visitor** check box if the card holder is a visitor.

Note: This option is available only if you avail a special license for integrating WIN-PAK with LobbyWorks.

16. Under **P-Series Trigger Control**, type the **User Level** number to trigger certain controls when this card is used. You can use ▲ or ▼ buttons to increase or decrease the current index number.

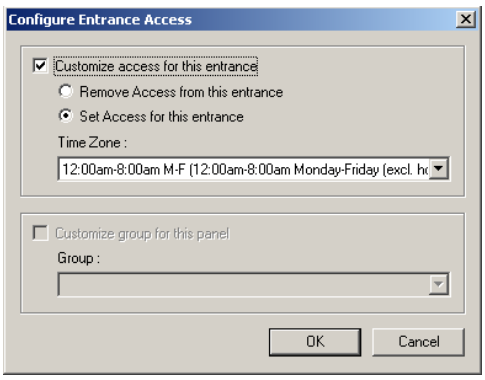
Refer to the "Configuring triggers and procedures" section in the chapter Device Map for more details on triggers and controls.

Defining a custom access level

1. In the **Card Properties tab**, next to **Custom Access Level**, click **Add** (if you are defining newly) or **Edit** (if you have defined already). The **Custom Access Level** dialog box appears.

Note: The Custom Access level is disabled, if you select the **Access Level** as None.

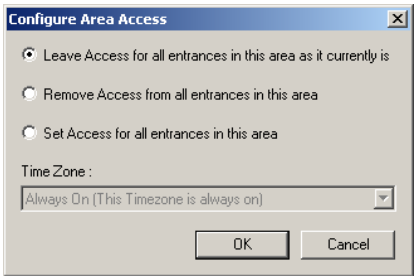
2. Right-click and select configure area access or double-click the area where you want to provide access. The **Configure Entrance Access** or **Configure Area Access** dialog box appears based on the selected area; Entrance or Area.
3. For one entrance, select one of the following:



- **Remove Access from all entrances in this area** to deny access through this entrance for this access level.

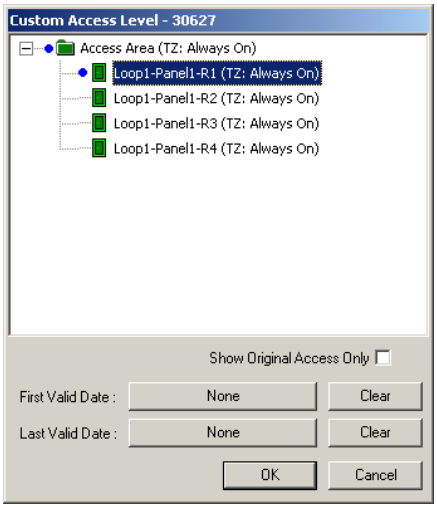
- **Set Access for all entrances in this area** to allow access through this entrance for a particular time zone. Select the time zone in the Time Zone list to determine periods of access.

For group entrance, select one of the following:



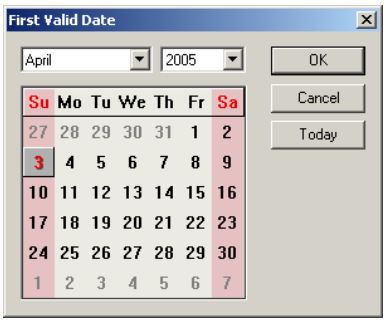
- **Leave Access for all entrances in this area as it currently is** to continue the same for each entrance in this group.
- **Remove Access from all entrances in this area** to deny access through these entrances for this access level.
- **Set Access for all entrances in this area** to allow access through these entrances for a particular time zone. Select the time zone in the Time Zone list to determine periods of access.

4. Click **OK** to set the access for the selected area and return to the **Custom Access Level** dialog box.



Note: The Blue dot indicates that the access area is customized for this card. If you want to restore the original access level for a group or entrance, right-click the customized group or entrance and click **Restore Original Access**.

5. To set the start date for the customized access level, click **None** in **First Valid Date**. The **First Valid Date** calendar appears.



6. Select the **Month, Year** and then select the date.
7. To select the current date, click **Today** and then click **OK** to return to the **Custom Access Level** dialog box.
8. To set the end date for the customized access, click **None** in **Last Valid Date**. The **Last Valid Date** dialog box appears.
9. Select the date in the same way that you have selected for **First Valid Date** and click **OK**.

Note: If you want to clear the dates, click **Clear** next to **First Valid Date** and/or **Last Valid Date**.

10. Select the **Show Original Access only** check box to view the original access levels of the areas.
11. Click **OK** to save the access levels and return to the **Card Record** dialog box.

Defining an action group for the card

1. In the **Card Properties** tab, click **View** next to **Action Group**. The **Abstract Device Record** dialog box appears.
2. Select the **Name** of the action group and click **OK**. The **Abstract Device Record** dialog box is closed.

Defining an activation and expiry date

1. In the **Card Properties** tab, click **Change** under **Activation Date** to define or change the activation date (the date on which the card is activated). The **Select Activation Date** calendar appears.

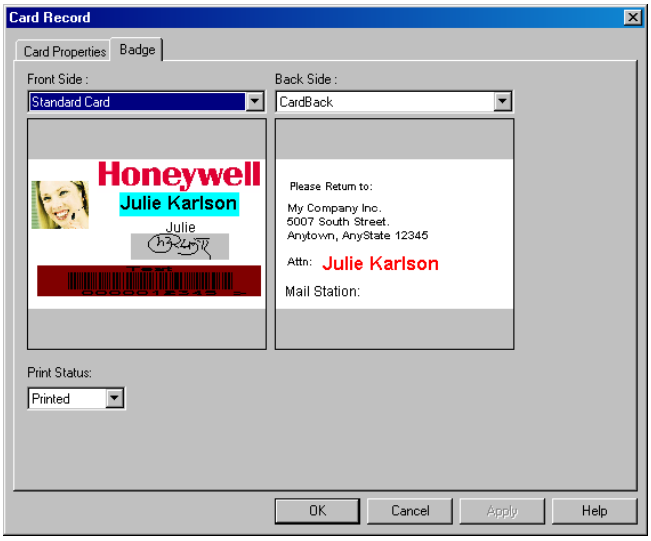
Note: The Activation Date is enabled only if you select the **Status** as Inactive.

2. Select the activation date and click **OK** to return to the **Card Record** dialog box.
3. Click **Clear** to clear the activation date.
4. To define or change the expiration date (the date on which the card access is expired), click **Change** under **Expiration Date**. The **Select Expiration Date** calender appears.

5. Select the expiry date and click **OK** to return to the **Card Record** dialog box.
6. Click **Apply** to save the card properties.

Assigning a badge to a card

1. In the **Card** dialog box, click the **Badge** tab.
2. Select the badge design in the **Front Side** list for the front side design of the card. The preview is displayed at the preview area.
3. Select the badge design in the **Back Side** list for the back side design of the card. The preview is displayed at the preview area.



4. After printing the card, the **Print Status** automatically changes to **Printed**. However, you are provided with an option to change the print status.
5. Click **OK** to save the card details.

Editing a Card

To edit a card:

1. Choose **Card > Card** or click  in the toolbar. The **Card** window appears.
2. Select the card to be edited from the list and click **Edit**. The **Card Record** dialog box appears.

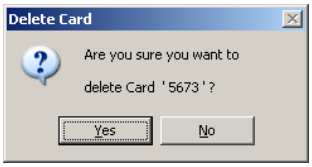
   Refer to the "Adding a Card" section in this chapter for information on editing the card.

Deleting a Card

To delete a card:

1. Choose **Card > Card** or click  in the toolbar. The **Card** window appears.

2. Select the card to be deleted from the list and click **Delete**. A message asking for confirmation appears, if you have set to confirm the card deletion in the Workstation Defaults setting.

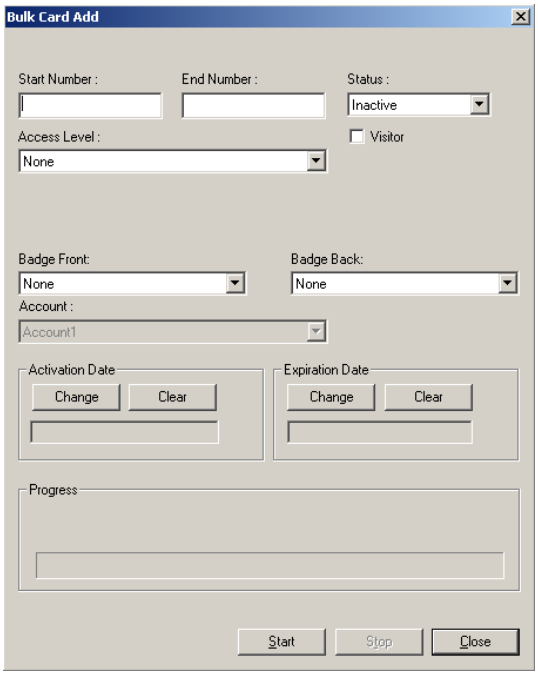


3. Click **Yes** to confirm the deletion. The card is deleted.

Adding Bulk Cards

To add cards in bulk:

1. Choose **Card > Bulk Card Add**. The **Bulk Card Add** dialog box appears.



2. Type the **Start Number** and the **End Number** of the card series. For example, type 100 and 200 to add 100 cards starting with the card number 100.
3. Select the **Status** of the cards.
4. Select the **Access Level** of the cards.
5. Select the **Visitor** check box, if the cards are for visitors.
6. Select the front and back badge designs of the cards in **Badge Front** and **Badge Back**.
7. Select the **Activation Date** and **Expiration Date**.
8. Click **Start** to add the cards. The progress bar displays the progress of adding bulk of cards.

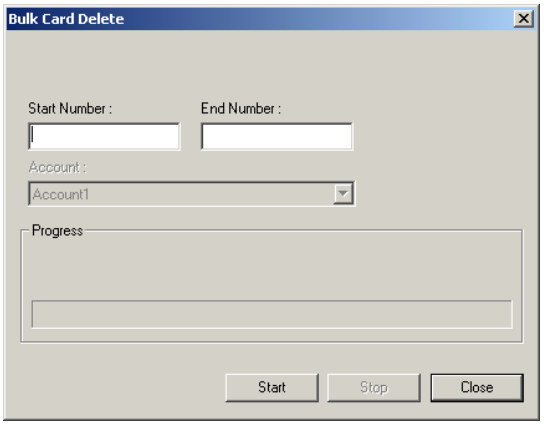
Caution: Do NOT close any WINPAK services or turn-off the computer while the Bulk Card Add is in progress.

9. Click **Stop**, if you want to cancel generating cards in bulk.
10. Click **Close** to close the **Bulk Card Add** dialog box.

Deleting Cards in Bulk

To delete a bulk of cards,

1. Choose **Card > Bulk Card Delete**. The **Bulk Card Delete** dialog box appears.



2. Type the **Start Number** and the **End Number** of the card series to be deleted.
3. Click **Start** to delete the bulk of cards. The progress bar displays the deletion progress.

Note: If you want to cancel bulk deletion, click **Stop**.

4. Click **Close** to close the **Bulk Card Delete** dialog box.

Assigning a Card to a Card Holder

You can assign a card to a card holder in two different ways:

- **While adding a card**: Select the card holder name while defining the card properties.

  Refer to the "Adding a Card" section for more details on adding cards.
- **While adding a card holder**: Create a new card or attach the existing card while adding cards to a card holder.

  Refer to the "Adding a Card Holder" section for more details on adding card holders.

Importing Card and Card Holder Information

The WIN-PAK Import Utility is used for importing the card and card holder details into WIN-PAK from an excel sheet. When you import these details into WIN-PAK, cards are assigned to the card holders accordingly.

Importing card and card holder details to WIN-PAK involves:

1. Defining note fields and card holder tab layouts, and configuring access levels.

   Refer to the "Configuring Additional Information" section in this chapter for more details on defining note fields, card holder tab layouts and access levels.

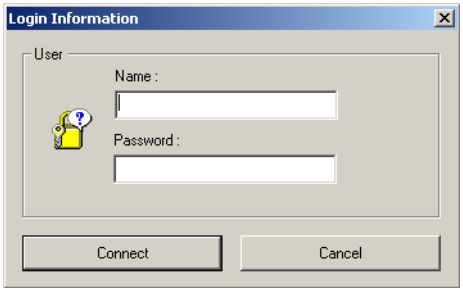
2. Defining the order of the fields.
3. Entering card and card holder details in an excel sheet.
4. Assigning default values to certain fields like Activation Date, Expiration Date and User-defined fields.
5. Importing the excel sheet into WIN-PAK.

Note: Ensure that you logged on to WIN-PAK client system, before using Import Utility.

Logging on to Import Utility

To log on to WIN-PAK Import Utility:

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK Import Utility**. The **Login Information** dialog box appears.



2. Type the **Name** of the user and the **Password**.

Note: Only the Administrator can log on to WIN-PAK Import Utility.

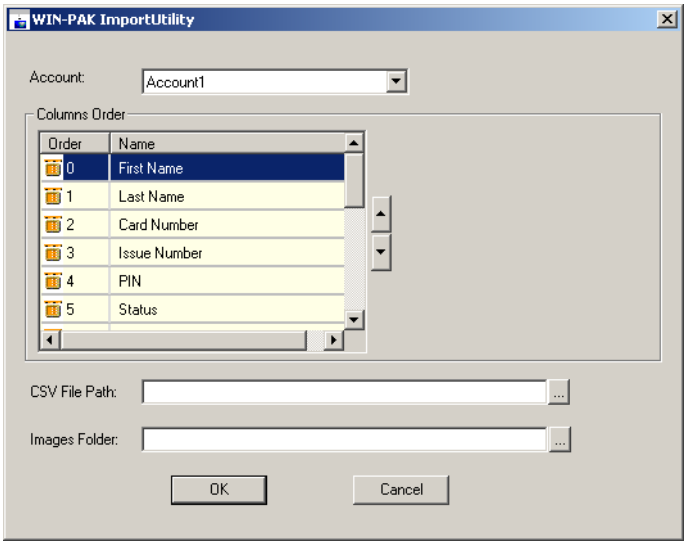
3. Click **Connect**. The system retrieves the data from database and displays the **WIN-PAK ImportUtility** dialog box.

Defining Order of Fields

After you define the note fields and card holder tabs, you must define the order of the card and card holder fields.

To define the order of the fields:

1. Log on to the WIN-PAK Import Utility. The **WIN-PAK ImportUtility** dialog box appears.



2. Select the **Account** to which the order is to be defined. The card holder fields for the selected account are listed in **Columns Order**.
3. To change the order of a row, select the row in the list and click the up button and/or down button.

Note: Ensure that you enter card holder information in the excel sheet in the order specified under Column Order. For example, Row 0 in the Columns Order becomes Column 1 in the excel sheet and Row 1 in the Columns Order becomes Column 2 in the excel sheet.

Entering Card and Card Holder Information in an Excel Sheet

Before you create the excel sheet, make a note of the column order in which the fields must be entered.

To enter the card and card holder information in the excel sheet:

1. Open Microsoft Excel.
2. Enter the card and card holder information as in the order you defined in the WIN-PAK Import Utility. The name of the this sheet must be “Sheet1”.
3. Save the excel sheet in the .xls or .csv format.

Note: When you import an excel sheet to WIN-PAK, cards are assigned to the respective card holders, as a row in the excel sheet contains complete information of a card and card holder. The following image depicts the typical excel sheet that contains the card and card holder information:

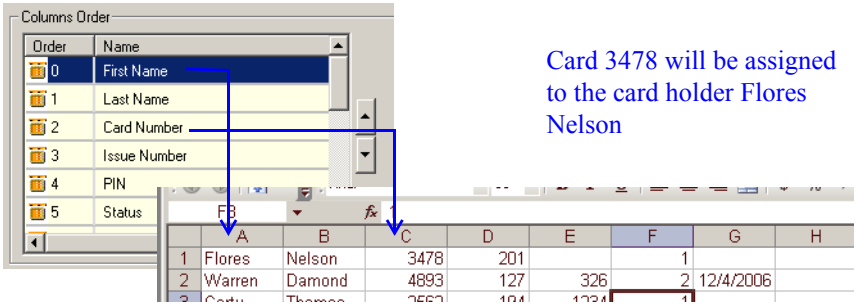


Figure 8-2 Entering card holder data in the excel sheet

Tips:

- Do not enter the field names in the first row. If you enter the field names to identify the columns, delete it before you import the data into WIN-PAK.
- For the Status field, type 1, 2, or 4 to indicate the card status as Active, Inactive, or Trace.

Note: Leave the Activation Date field blank, if you specify the card status as Active or Trace.

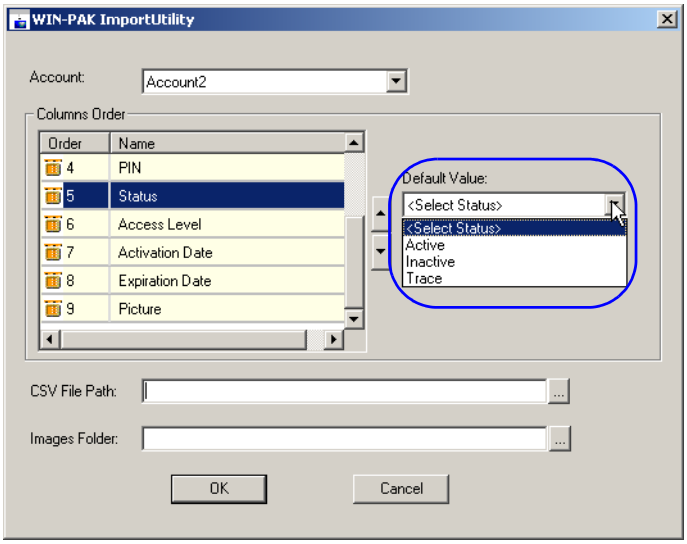
- Ensure that access levels are configured in WIN-PAK for the respective account, before you enter the name of the access levels.
- Avoid duplication of card numbers.
- To assign default values for fields, leave the fields blank. You can assign default value to the Issue Number, Status, Access Level, Activation Date, and Expiry Date fields and the user-defined fields.
- Use the format for note field templates for the user-defined fields.
- To assign the photo of the card holder, enter the name of the photo image file in the Photo column.

Assigning Default Values

You can assign the default values to certain fields like Issue Number, Status, Access Level, Activation Date, and Expiration Date. You can also assign default values for user-defined fields.

To assign the default values to certain fields:

1. Log on to the WIN-PAK Import Utility. The **WIN-PAK ImportUtility** window appears.
2. Select the **Account** for assigning the default values. The fields for the selected account are displayed in **Columns Order**.
3. Under **Columns Order**, select the field to which the default value must be assigned. The **Default Value** box appears on the right.



4. Type or select the default value that must be assigned to all the card holders belonging to the selected account.

   Tip: To set the current dates for Activation Date or Expiration Date, select the check box. To set different dates, click the drop-down list and select the required date in the calendar.

   Note: Ensure that the Expiration Date is later than the Activation Date.

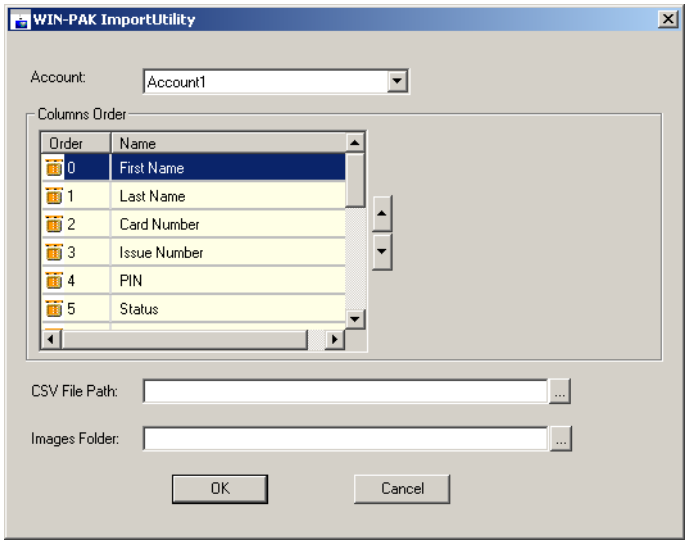
Importing from Excel Sheet

You can import the card and card holder information from the excel sheet in which the card and card holder information is entered.

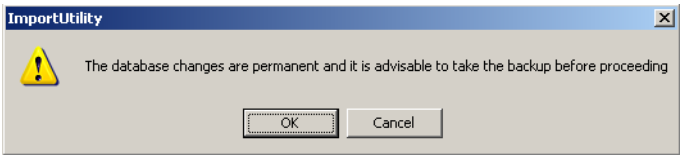
Note: Honeywell recommends you to take a backup of the current WIN-PAK database, before importing the data to WIN-PAK.

To import the card and card holder information from an excel sheet:

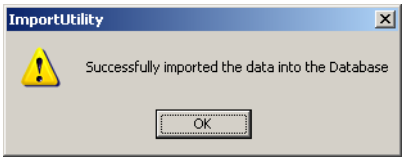
1. Log on to WIN-PAK Import Utility. The **WIN-PAK ImportUtility** dialog box appears.



2. Select the **Account** to which the card and card holder information must be imported. The corresponding fields are displayed in **Columns Order**.
3. In **CSV File Path**, specify the path of the excel sheet or click the ellipsis button and select the path.
4. In **Images Folder**, select the folder in which the photo images are stored.
5. Click **OK**. A message asking for confirmation appears.



6. Click **OK** to import the data. A message appears indicating that import is successful.

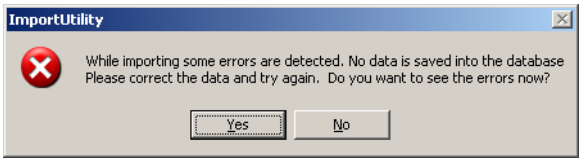


Correcting Errors in Excel Sheet

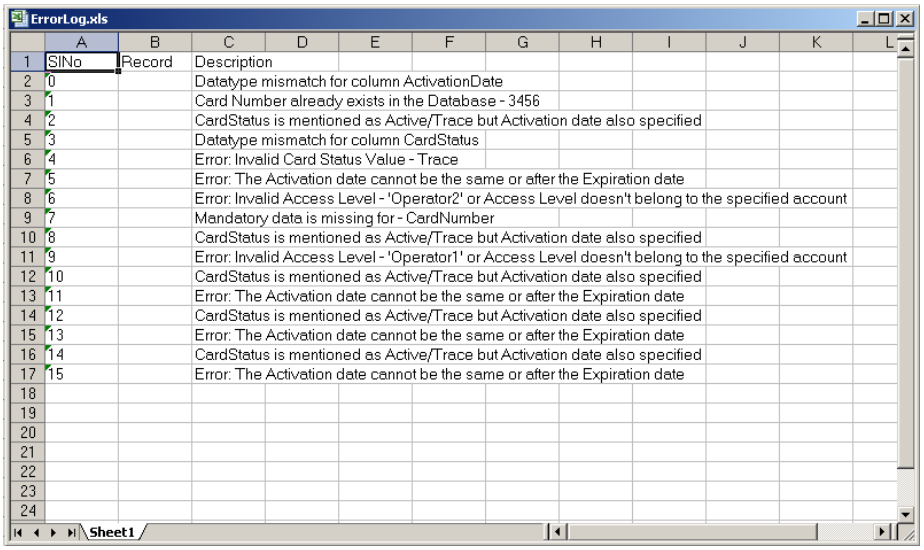
Errors might occur while importing the data from the excel sheet. You cannot import the card and card holder information to WIN-PAK until you correct these errors.

To view and correct the errors:

1. In case of errors during an import, the following dialog box appears prompting you to open and view the error list.



2. Click **Yes** to view the errors. The **ErrorLog.xls** file is opened.



SINo	Record	Description
0		Datatype mismatch for column ActivationDate
1		Card Number already exists in the Database - 3456
2		CardStatus is mentioned as Active/Trace but Activation date also specified
3		Datatype mismatch for column CardStatus
4		Error: Invalid Card Status Value - Trace
5		Error: The Activation date cannot be the same or after the Expiration date
6		Error: Invalid Access Level - 'Operator2' or Access Level doesn't belong to the specified account
7		Mandatory data is missing for - CardNumber
8		CardStatus is mentioned as Active/Trace but Activation date also specified
9		Error: Invalid Access Level - 'Operator1' or Access Level doesn't belong to the specified account
10		CardStatus is mentioned as Active/Trace but Activation date also specified
11		Error: The Activation date cannot be the same or after the Expiration date
12		CardStatus is mentioned as Active/Trace but Activation date also specified
13		Error: The Activation date cannot be the same or after the Expiration date
14		CardStatus is mentioned as Active/Trace but Activation date also specified
15		Error: The Activation date cannot be the same or after the Expiration date

3. Review and correct the errors in the source file.

The following table lists the possible errors and provides the corrective action to resolve them:

Table 8-5 Error types and Corrective Actions

Error Type	Corrective Action
Datatype mismatch	This error may occur if you have entered alphabets for numeric datatype and vice-versa. Check the datatype and enter the correct data.
Card Number already exists in the Database	Avoid duplicate card numbers.
Card Status is mentioned as Active/Trace but Activation date also specified.	The activation date is not applicable for the card status of Active or Trace. Therefore, if you have entered 1 or 4 in the card status column, leave the Activation Date column empty.
Invalid Card Status Value	Ensure that you select only 1, 2, or 4 for Active, Inactive or Trace status. Any other number will lead to such error.

Table 8-5 Error types and Corrective Actions

Error Type	Corrective Action
The Activation date cannot be the same or after the Expiration date	The Expiration date must be later than Activation Date.
Mandatory data is missing	Card Number is a mandatory field.
Invalid Access Level	Enter the correct name of the access level and ensure that it belongs to the account to which the data must be imported.

Visitor Management

LobbyWorks, a Visitor Management system that tracks the movement of visitors, assets, and deliveries, can be intergrated with WIN-PAK. By doing this, the access cards that are created for visitors in LobbyWorks can be used in WIN-PAK as access cards. After the access cards are copied from LobbyWorks to WIN-PAK, they are provided with the necessary access levels for allowing or restricting visitors to the different areas in the premises.

Integrating LobbyWorks

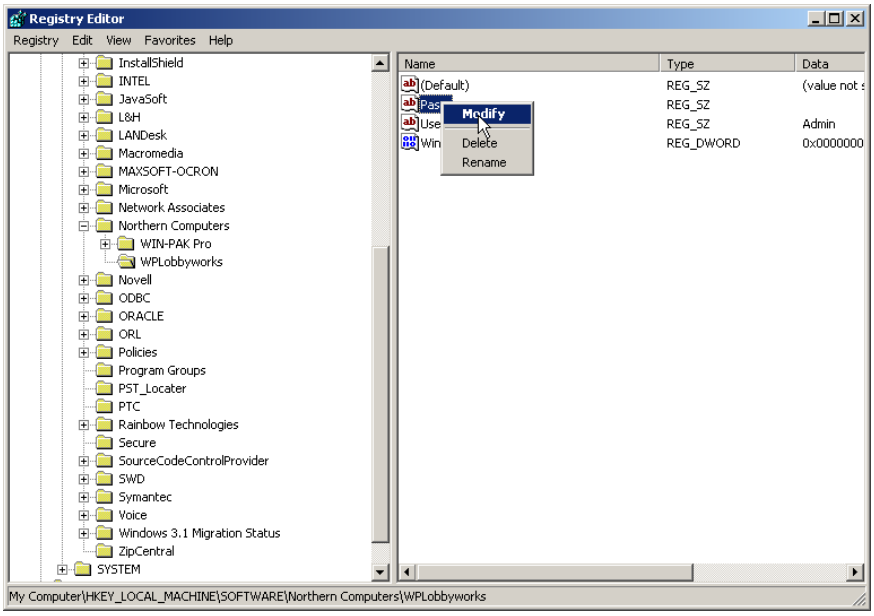
Before you begin:

- Ensure to install WIN-PAK and LobbyWorks on the same network.
- Procure the license for integrating LobbyWorks with WIN-PAK.

Setting Key Values

To integrate LobbyWorks with WIN-PAK:

1. Choose **Start > Run**, and then type regedit. The **Registry Editor** window appears.
2. In the left pane, expand **HKEY_LOCAL_MACHINE**, **Software**, and then **Northern Computers**.
3. Select **WPLobbyWorks**. The relevant keys are displayed in the right-pane.



4. Edit the values of the **Pass** and **User** keys.

    a. Right-click the **Pass** key and click **Modify**. The **Edit String** dialog box appears.

    b. Enter the password in the **Value Data** box.

    c. Right-click the **User** key and click **Modify**. The **Edit String** dialog box appears.

    d. Enter the user name in the **Value Data** box.

5. Set the **Value data** of WinAuth as **0**, if you are logging on to WIN-PAK in the WIN-PAK authentication mode.

    OR

    Set the **Value data** of WinAuth as **1**, if you are logging on to WIN-PAK in the Windows authentication mode.

    Note: In the Windows Authentication mode, the values for Pass and User are considered by default and so setting these key values can be ignored.

6. Close the **Registry Editor** window.

Time Management

9

In this chapter...

Introduction

The chapter **Time Management** describes how to configure a time zone, holiday group, daylight saving group, and to schedule a task.

Time Zone

A time zone is a group of time slots that define the access of the associated item. For example, the time zone can be mapped to an access level. When a card holder is associated to an access level, the card holder's access is allowed or denied depending on the time zone associated to the access level.

You can create any number of Time Zones. However, a maximum of 63 time slots can be downloaded to a PW-2000 series panel and 255 time slots can be downloaded to a PRO-2200 Intelligent Controller.

Refer to the "Time Zone" section in this chapter for configuring a time zone.

Schedule

A schedule is planned task that must be performed at the defined time periods. In WIN-PAK, a task includes running a command file, guard tour, or generating a report, and so on.

Refer to the "Schedule" section in this chapter for scheduling a task.

Holiday Group

A holiday group is a set of holidays. The access decision is based on the time zone that you associate to an entrance in the access level and the holiday group you associate while configuring panels.

Refer to the "Holiday Group" section in this chapter for configuring a holiday group.

Daylight Saving Group

Daylight saving group is a set of daylight saving time slots. Daylight Saving Time is the time during which clocks are set one hour ahead of local standard time.

Refer to the "Daylight Saving Group" section in this chapter for configuring a daylight saving group.

Time Zone

Time Zones can be assigned to cards, action groups, ADVs, operators, panels, and access levels. Therefore, ensure that you define the time zone first, before defining these items.

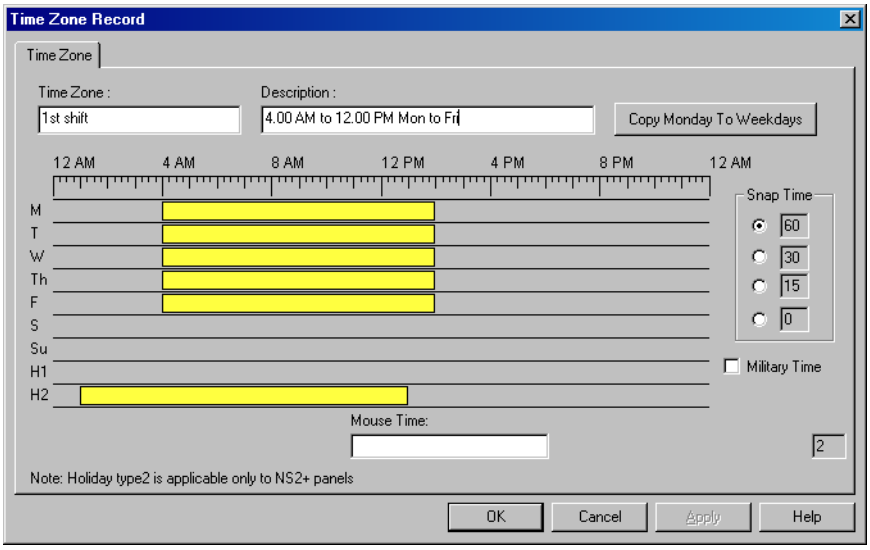
Always On and **Never On** are the system-generated time zones that are available in WIN-PAK by default.

- **Always On** - This time zone allows full-time access to the card holder assigned to it.
- **Never On** - This time zone restricts the access of the card holder assigned to it.

Adding a Time Zone

To add a new time zone:

1. Choose **Configuration > Time Management > Time Zone**. The **Time Zone** window appears.
2. Click **Add**. The **Time Zone Record** dialog box appears to add a new time zone.

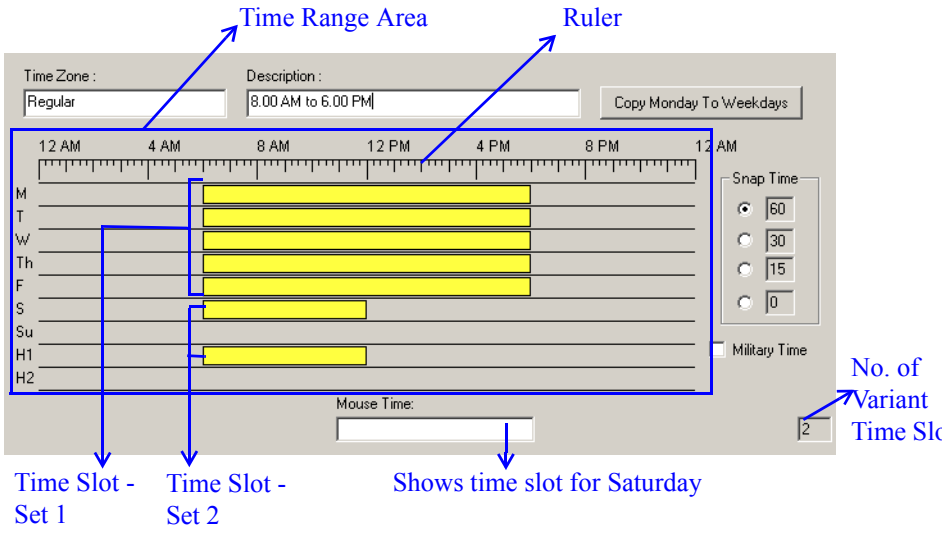


3. Type the name of the **Time Zone** and a brief **Description**.
4. Select the corresponding **Snap Time**. The Snap Time option enables you to set the time slot according to the selected snap time.

   Example: If you set a **Snap Time** of 60 minutes, you can only define time slots with a minimum of 1 hour interval. This time slot must start and end as a whole hour and would not include any minutes or seconds. For example, you can set time slots of 8 AM to 9 AM, or 3 PM to 4 PM. However, you cannot set a time slot of 4:30 to 5:30 or 1:15 to 2:15.

   Time slots including minutes and seconds as interval can be set by selecting 30 and 15 snap time options.

Time slot with an interval of a minute can be set by selecting the snap time of 0.

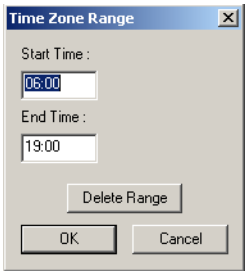


5. To define a time slot:

   a. Click any of the weekdays and drag the mouse pointer to reach the end time of the time slot.

      OR

      Right-click any of the weekday to display the **Time Zone Range** dialog box. Enter the **Start Time** and **End Time** and click **OK** to set the time slot.



Note: The **Mouse Time** box indicates the time at the mouse pointer.

- When you hover the mouse pointer over the time range area, the time at the mouse pointer is displayed in the **Mouse Time** box.
- When you define a time slot, the start and the end time is displayed in the **Mouse Time** box when you click and drag the mouse pointer.
- For an already defined time slot, the start and the end time is displayed in the **Mouse Time** box when you hover the mouse pointer over the time slot.

Tip: It is sufficient to define the time slot for Monday, so that you can copy the time slot for the rest of the weekdays using the **Copy Monday to Weekdays** option.

6. If you want to set the hour format of the ruler as 24 hours, select the **Military Time** check box.
7. After you set the time range for Monday, click **Copy Monday to Weekdays** to copy it to the other weekdays.

   Tip: If you want to delete the time slot, place the cursor over the time slot and right-click to display the **Time Zone Range** dialog box. Click **Delete Range**.
8. Follow the same procedure to set the time slot for Saturday and Sunday.
9. Set the time slots for holidays in **H1** and **H2**.

Note: When time zones and holiday group are assigned to a panel, the time slots defined for the holidays H1 and H2 are applied to the holiday group.

10. Click the **Accounts** tab to associate accounts to the time zone.

Note: You must assign an account to a time zone, after setting the time slots.

11. Under **Available Accounts**, select an account and then click **Add**. For multiple selections, use the SHIFT or CTRL key while selecting the accounts.
12. To remove an account from the selected account list, select an account and click **Delete**. The selected accounts are moved to the **Available Accounts** list.
13. Click **OK** to save the Time Zone.

Editing a Time Zone

To edit a Time Zone:

1. Choose **Configuration > Time Management > Time Zone**. The **Time Zone** window appears.
2. Select a time zone and then click **Edit**. The **Time Zone Record** dialog box appears.
3. Make the required changes and then click **OK** to save the changes and to close the **Time Zone Record** dialog box.

Note: You cannot edit the **Always On** and **Never On** time zones, as these are generated by WIN-PAK.

Isolating and Deleting a Time Zone

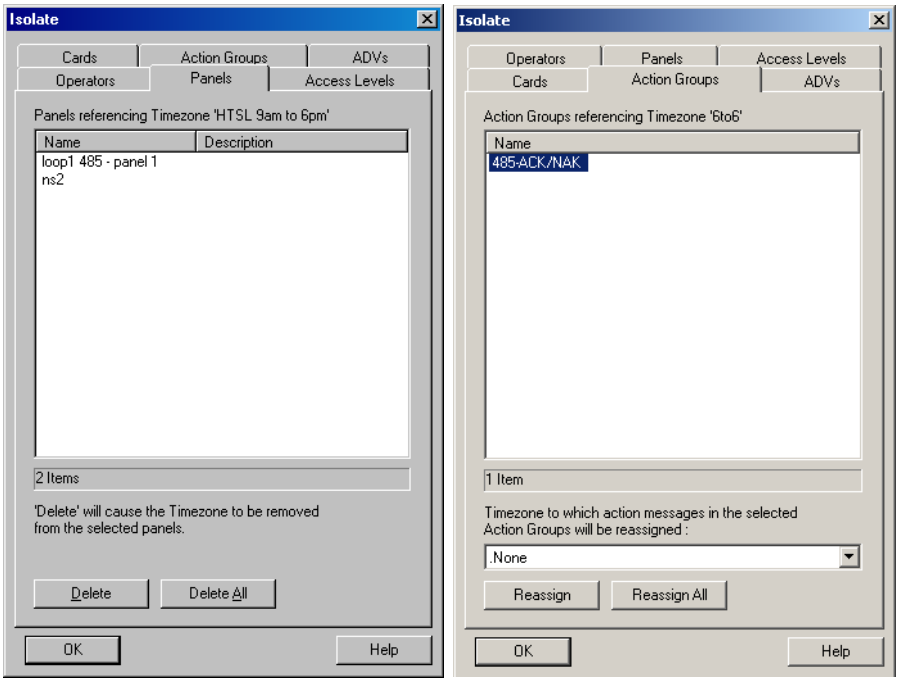
Time Zones are used in many places throughout the access control system. Therefore, to delete a time zone, you must isolate the time zone if it is assigned to any panel, operator, or access level.

Isolating a Time Zone

To isolate a time zone:

1. Choose **Configuration > Time Management > Time Zone**. The **Time Zone** window appears.
2. Select a time zone and then click **Isolate**. The **Isolate** dialog box appears.

   The Cards, Action Groups, ADVs, Operators, Panels, and Access Levels associated to the time zone are displayed in the relevant tabs.



3. Click each tab to view the list of associated items.
4. To dissociate a panel from the time zone, select the panel in the list and click **Delete** or to dissociate all the panels from the time zone click **Delete All**. However, you cannot assign a panel to a different time zone.

   OR

   To reassign a time zone for other devices:

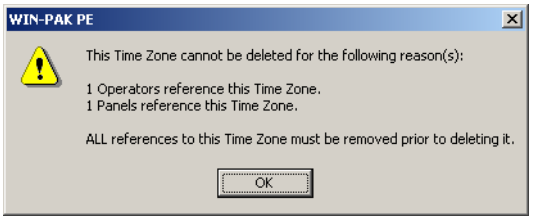
   a. Select the device from the list of devices

   b. Select the alternate time zone from the drop-down list.

c. Click **Reassign** to reassign the selected devices or click **Reassign All** to reassign all the devices to the selected time zone.

5. Click **OK**. The time zone is isolated from the selected device and is assigned to the different time zone.

Note: A warning message is displayed, if you attempt to delete a Time Zone that is referenced to other devices.



Click **OK** to close the message box.

Deleting a Time Zone

After you have isolated a time zone, you can delete the time zone.

To delete a time zone:

1. In the **Time Zone** window, select the time zone from the list of time zones.
2. Click **Delete**. The time zone is deleted.

Schedule

You can schedule tasks so that they run automatically at a defined time.

Scheduling a Task

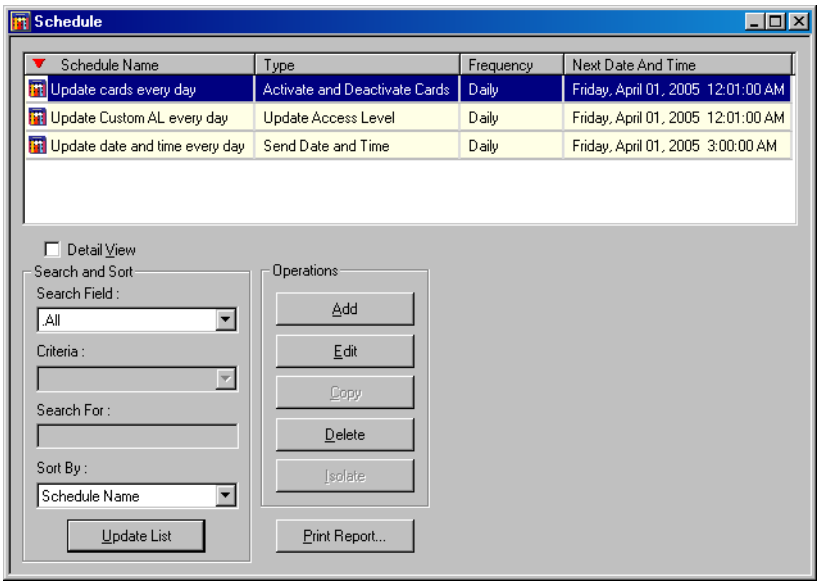
To schedule a task:

1. Choose **Configuration > Time Management > Schedule**. The **Schedule** window appears with the list of the following system-generated schedules:

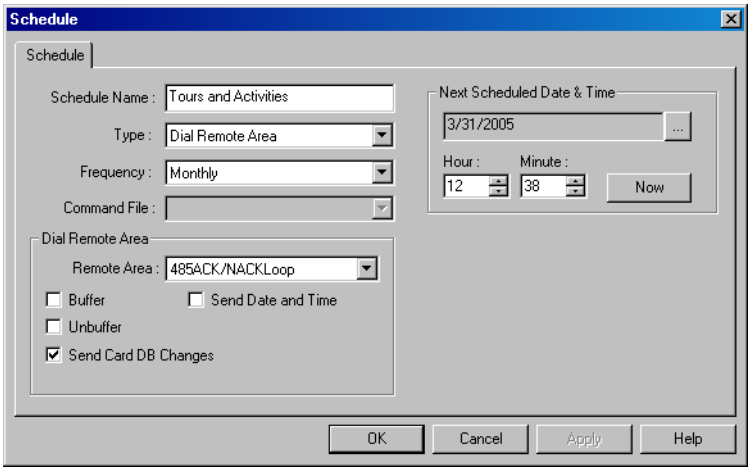
   Update cards every day - Updates the card details every day in the panel. If this schedule is not generated, the panel will allow the card access of the inactivated or expired card also.

   Update Custom AL every day - Updates the custom access level start date and expiry date in the panel. If this schedule is not generated, the panel will still consider the global access level of an operator.

   Update date and time every day - Updates the date and time in the panel every day. If this schedule is not generated, the panel does not sync with the system time and it may cause in outdated data in the panel.



2. Click **Add**. The **Schedule Record** dialog box is displayed.



3. Type the **Schedule Name** for the task.
4. Select a task **Type**. Based on the selected task type, other options on the dialog box may be activated.

   Task types include:

   - **Activate and Deactivate Cards**: Activates or deactivates cards depending on the card activation and deactivation dates. This helps to update the card details in the panel.
   - **Card Frequency Report**: Generates the card frequency report in a defined interval.
   - **Dial Remote Area**: Establishes the dial-up connection between WIN-PAK systems and sends the command to the panel.

- **Run Command File**: This schedule runs a command file at a specific time in a defined frequency.
- **Run Guard Tour**: This schedule runs the guard tour in a defined interval.
- **Run Report**: Generates the report at a defined interval.
- **Send Date and Time**: Sends the system date and time to all the panels attached to WIN-PAK.
- **Update Custom Access Level**: Updates custom access level of cards in the panels at a defined frequency.

Refer to the "Task Type" section in this chapter, for more details on task types and scheduling a task.

5. In the **Frequency** list, select how often the task is to be performed.
6. Under **Next Scheduled Date and Time**, select the date and enter the time (in hours and minutes) for the task to be performed.

Notes:

- To select the date, click the ellipsis button and select the date in the calendar.
- To enter the time, type the **Hour** and **Minute**. The hour ranges from 0 to 23 and minute ranges from 0 to 59.
- To enter the current date and time, click **Now**.

Task Type

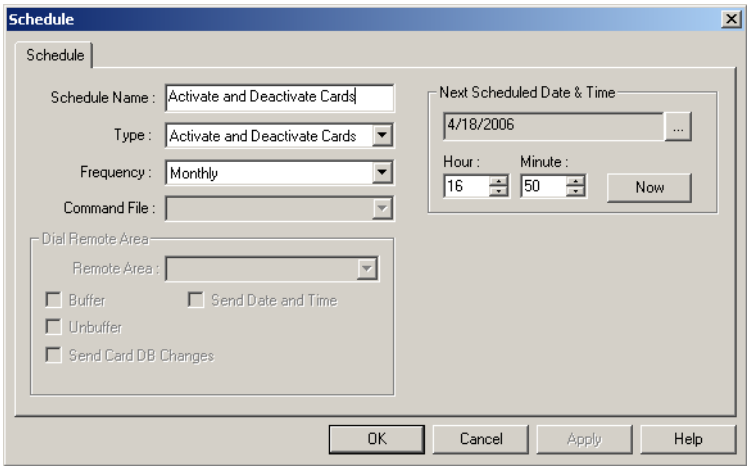
For every Task type that you select in the **Schedule** dialog box, a different set of options appears. This section describes the task types and guides you how to schedule a task for the various task types.

Activate and Deactivate Cards

Select this task type to schedule a task for activating and deactivating the cards, depending on the card activation and deactivation dates. However, this task is scheduled by default.

If you select this type, perform the following steps:

1. In the **Schedule** dialog box, select how often the task is to be performed in the **Frequency** list.



2. Under **Next Scheduled Date and Time**, select the date and enter the time (in hours and minutes) for the task to be performed.

Notes:

- To select the date, click the ellipsis button and select the date in the calendar.
- To enter the time, type the **Hour** and **Minute**. The hour ranges from 0 to 23 and minute ranges from 0 to 59.
- To enter the current date and time, click **Now**.

3. Click **OK** to save the schedule.

Card Frequency Report

Select this task type, if you want to generate the Card Frequency Report at the defined intervals. If you select this type, the **Card Frequency Report Configuration** form appears on the lower-left corner of the **Schedule** dialog box.

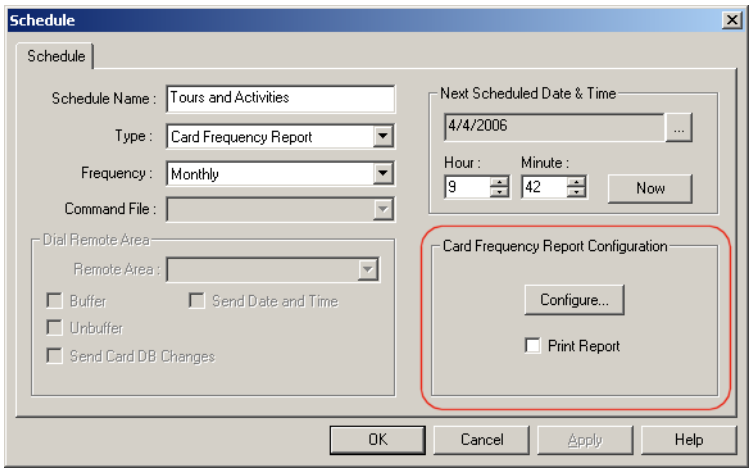
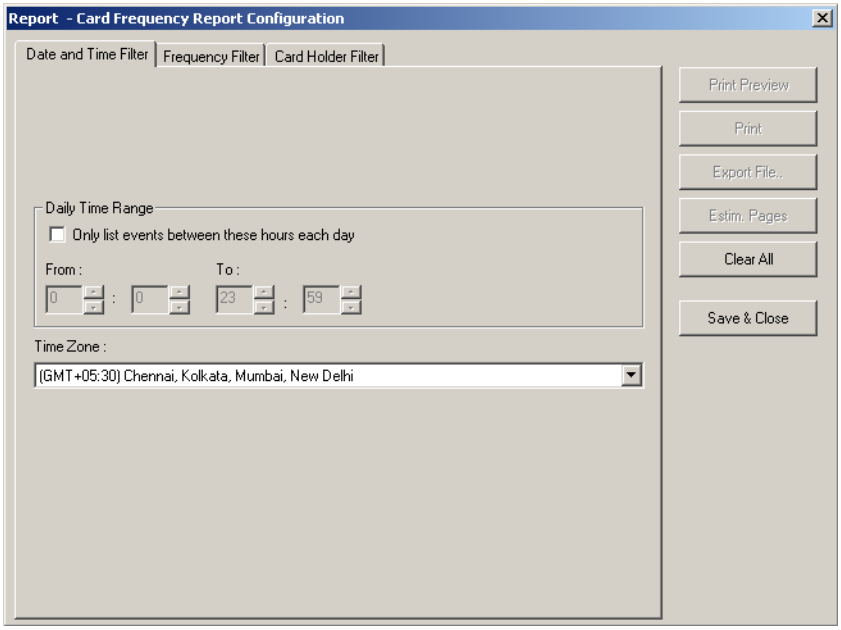


Figure 9-1 Scheduling a task for the "Card Frequency Report" task type

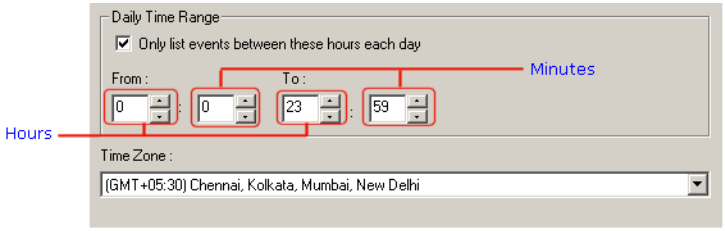
In addition to the basic steps, perform the following steps for scheduling a task:

1. In the **Schedule** dialog box, under **Card Frequency Report Configuration**, click **Configure**. The **Report - Card Frequency Report Configuration** dialog box appears.



2. To set the date and time range for generating the card frequency report, click the **Date and Time Filter** tab.

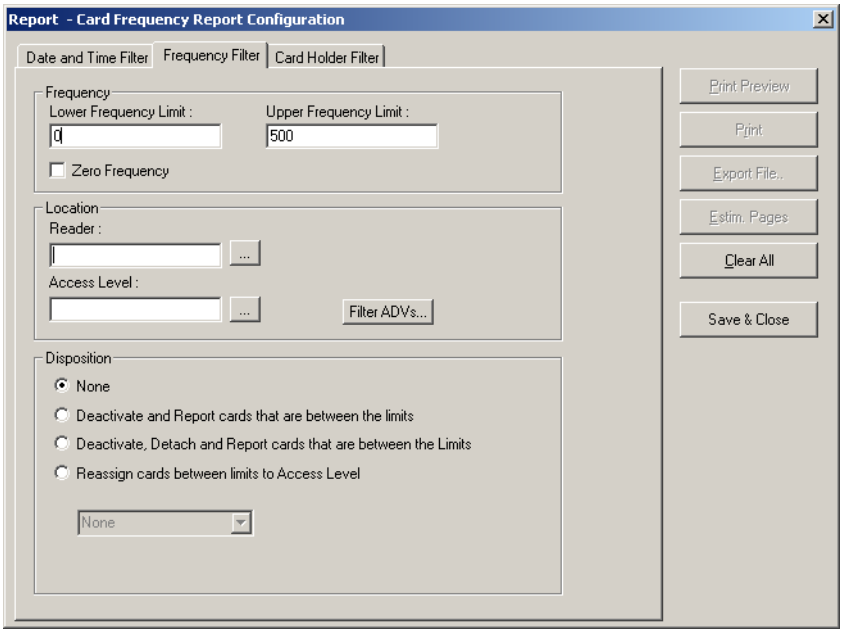
    a. To generate reports for events occurring during the specified period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The **From** and **To** text boxes are enabled.



    b. In the **From** and **To** boxes, select the time range (in hours and minutes).

    c. Select the standard time zone in the **Time Zone** list.

3. To set the card frequency limits for generating reports on card frequency, click the **Frequency Filter** tab.



Note: Frequency Filter is used for finding the reader or the access area in which the cards are less-frequently accessed. This helps to take some action on the particular reader or the access area like unlocking the reader always.

4. Under **Frequency**, type the **Lower Frequency Limit** and **Higher Frequency Limit** to filter the cards between these limits.

   Note: If you want to generate a report of cards that are not used, select the **Zero Frequency** check box.

5. To generate the card frequency reports by filtering the readers, type the **Reader** name under **Location** or select the reader by clicking the ellipsis button.

6. To generate the frequency filter reports for access areas, type the **Access Area** name under **Location** or select the access area by clicking the ellipsis button.

7. To include only certain devices, click **Filter ADVs** to select the ADVs. In the **Filter Devices** dialog box, select the appropriate ADV or ADV type from the tree and click **OK**.

8. Under **Disposition**, select one of the following actions that must be performed on the cards after you have filtered for frequency report:

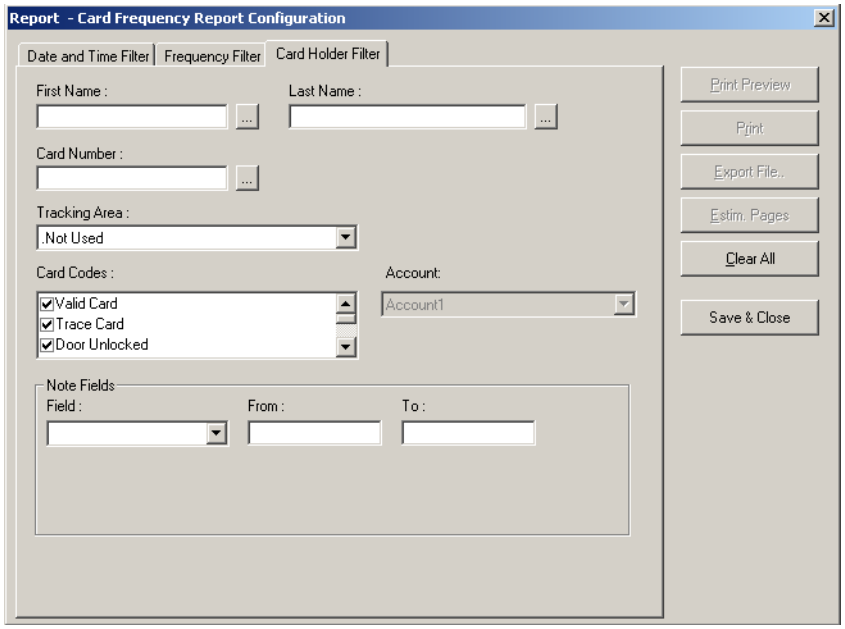
   a. **None**: Perform no action on the cards.

   b. **Deactivate and Report cards that are between the limits**: Deactivate and generate a report for the cards whose access frequency falls between the frequency limits.

   c. **Deactivate, Detach and Report cards that are between the limits**: Deactivate, detach and generate a report for the cards whose access frequency falls between the frequency limits.

d. **Reassign cards between limits to Access Level**: Reassign and generate a report for the cards whose access frequency falls between the frequency limits.

9. To filter the card holders for generating the card frequency report, click the **Card Holder Filter** tab.



10. Type the **First Name** and **Last Name** of the card holder, or select them by clicking the ellipsis button.
11. Type the **Card Number** of the card holder or select it by clicking the ellipsis button.
12. To generate the card frequency reports of the card holders accessing a specific area, select one of the options from the **Tracking Area** list.
    - **Exit Area: Card reads not shown**: To generate the reports of the cards accessed in the Exit area.
    - **Tracking and Mustering Area**: To generate the reports of the cards accessed only in the Tracking and Mustering Area.
13. Select one or more **Card Codes** which define the card transaction.
14. Select the **Note Fields** to be displayed in the report. You can also specify the range if you select the numerical note field.
15. Click **Save & Close** to save the configuration details and close the dialog box.
16. Click **OK** to save the schedule.

Dial Remote Area

Select **Dial Remote Area** as the task type, if you want the WIN-PAK system to send the commands to the panel connected through modem.

If you select this type, the **Dial Remote Area** box is enabled on the lower-right corner of the **Schedule** dialog box.

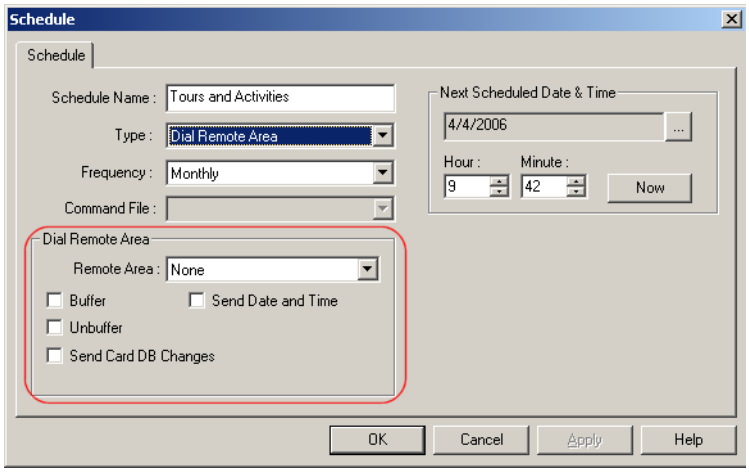


Figure 9-2 Scheduling a task for the "Dial Remote Area" task type

In addition to the basic steps, perform the following steps for scheduling a task:

1. In the **Schedule** dialog box, select a remote area in the **Remote Area** list.
2. Select the following commands to be sent to the panel:

Table 9-1 Describing Dial Remote Area commands

Option	Description
Buffer	Select this option, if you want the panel to store the task data in the panel buffer.
Unbuffer	Select this option, if you want the panel to send the stored data to the WIN-PAK system.
Send Card DB Changes	Select this option, if you want the WIN-PAK system to send the updated card details to the panel.
Send Date and Time	Select this option, if you want the WIN-PAK system to send the system date and time to the panel.

3. Click **OK** to save the changes.

Run Command File

Select **Run Command File** as a task type, if you want to run the command files in a defined frequency.

When you select this task type, the Command File list is enabled in the **Schedule** dialog box.

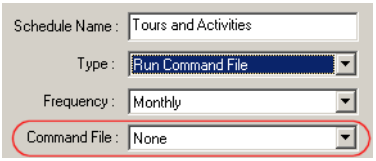


Figure 9-3 Scheduling a task for the "Run Command File" task type

In addition to the basic steps, perform the following steps for scheduling a task:

1. In the **Schedule** dialog box, select a command file in the **Command File** list. The command files available in WIN-PAK are listed.
2. Click **OK** to save the schedule.

Run Guard Tour

Select **Run Guard Tour** as a task type, if you want to run a guard tour at a defined interval.

Refer to the "Adding a Guard Tour" section in the chapter Guard Tour for more details on defining the guard tour.

When you select this task type, the **Guard Tour Configuration** frame appears on the lower-right corner of the **Schedule** dialog box.

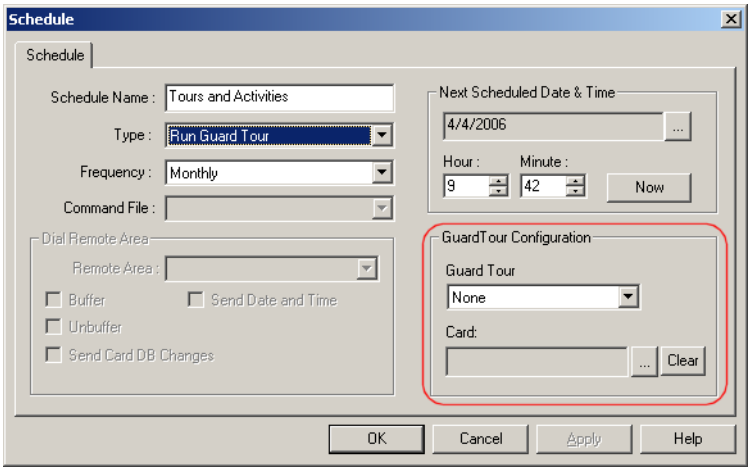


Figure 9-4 Scheduling a task for the "Run Guard Tour" task type

In addition to the basic steps, perform the following steps for scheduling a task:

3. In the **Schedule** dialog box, under **GuardTour Configuration**, select the guard tour in the **Guard Tour** list.
4. To select the card attached to the card holder (guard), click the ellipsis button and select the card.

   If you want to remove the card, click **Clear**.
5. Click **OK** to save the schedule.

Run Report

Select **Run Report** as a task type, if you want to generate card holders report or history report at a defined interval. In addition, the reports that are configured in Report Templates can be executed.

When you select this task type, the **Configure Reports** frame appears on the lower-right corner of the **Schedule** dialog box.

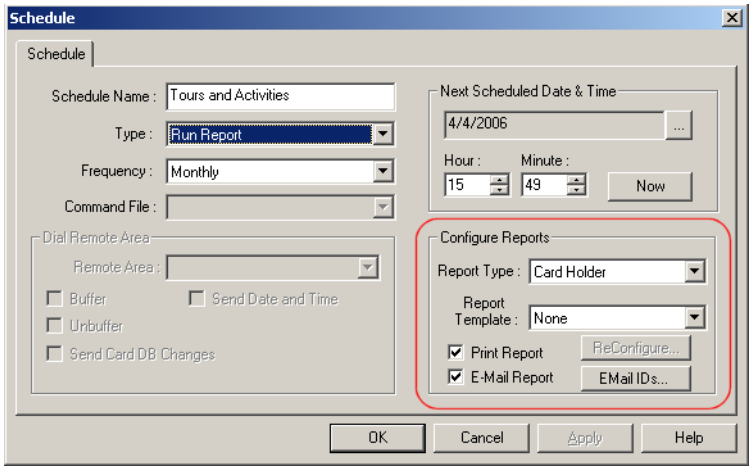
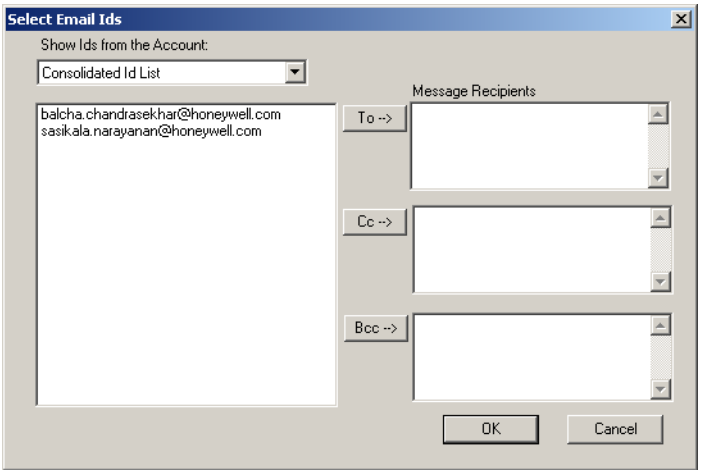


Figure 9-5 Scheduling a task for the "Run Report" task type

In addition to the basic steps, perform the following steps for scheduling a task:

1. Select the type of the report to be generated in the **Report Type** list.
   - **Card Holder** - To generate the report for card holders.
   - **History** - To generate the report of the history.
2. Select the template for the report in the **Report Template** list. The templates are listed for the selected report type. You must have created the templates using the **Report Template** menu option.
3. Click **Reconfigure** to edit the report template configuration. The **Report - Card Holder** or **Report - History** dialog box appears.

   Refer to the "Report Templates" section in the chapter Reports for adding or editing a report template.
4. Select the **Print Report** check box to print the report immediately after the configuration.
5. Select the **E-Mail Report** check box to send the report to the selected e-mail Ids after the configuration.
6. Click **EMail IDs** to select the e-mail Ids for sending the report. The **Select Email Ids** dialog box appears.



7. Select the Id type in the **Show Ids from the Account** list. The available Id list types are Consolidated Id List, To Id List, Cc Id List, and Bcc Id List. The e-mail Ids of the selected ID type are listed.
8. Select the Id from the list and click **To** or **Cc** or **Bcc** to move it to the corresponding recipients list.

   OR

   Type the e-mail Ids in the corresponding **Message Recipients** boxes.

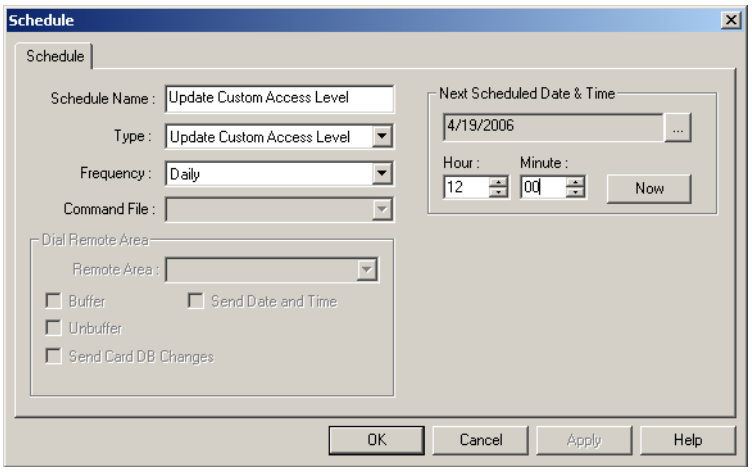
   Note: To remove an Id from the recipients list, select the Id and press DELETE.
9. Click **OK** to save the e-mail Ids and close the dialog box.

Send Date and Time

Select **Send Date and Time** task type to update the panel date and time with the system timing. However, this task is scheduled by default.

If you select this type, perform the following steps:

1. In the **Schedule** dialog box, select how often the task is to be performed in the **Frequency** list.



2. Under **Next Scheduled Date and Time**, select the date and enter the time (in hours and minutes) for the task to be performed.

Notes:

- To select the date, click the ellipsis button and the calendar appears.
- To enter the time, type the **Hour** and **Minute**. The hour ranges from 0 to 23 and minute ranges from 0 to 59.
- To enter the current date and time, click **Now**.

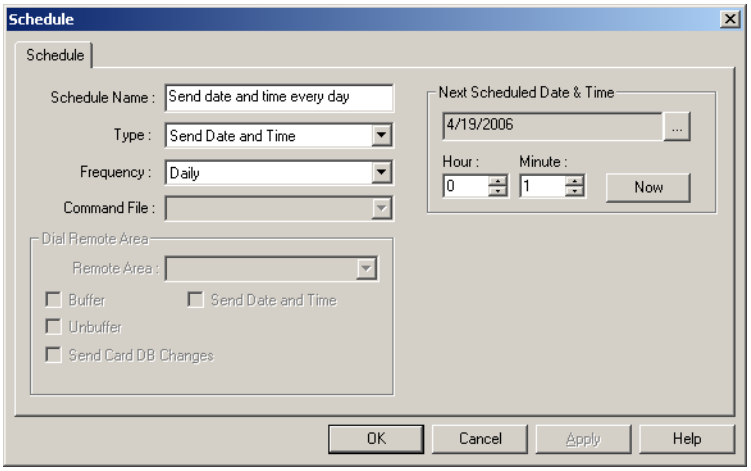
3. Click **OK** to save the schedule.

Update Custom Access Level

Select **Custom Access Level** task type to send the card details with the custom access level to the panel at a scheduled time. However, this task is scheduled by default.

If you select this type, perform the following steps:

1. In the **Schedule** dialog box, select how often the task is to be performed in the **Frequency** list.



2. Under **Next Scheduled Date and Time**, select the date and enter the time (in hours and minutes) for the task to be performed.

Notes:

- To select the date, click the ellipsis button select the date in the calendar.
- To enter the time, type the **Hour** and **Minute**. The hour ranges from 0 to 23 and minute ranges from 0 to 59.
- To enter the current date and time, click **Now**.

3. Click **OK** to save the schedule.

Editing a Schedule

To edit the schedule:

1. Choose **Configuration > Time Management > Schedule**. The **Schedule** window appears.
2. Select the schedule to be edited and click **Edit**. You can also edit the default schedule generated by WIN-PAK.
3. Change the required details and click **OK** to save the changes.

Deleting a Schedule

To delete a schedule:

1. Choose **Configuration > Time Management > Schedule**. The **Schedule** window appears.
2. Select the schedule to be deleted and click **Delete**. You can also delete the default schedule generated by WIN-PAK.
3. Click **Delete**. The selected schedule is deleted.

Holiday Group

Holiday group is a set of holidays. For example, you can group the holidays like Christmas, Thanks Giving Day, and Independence Day as a Government Holiday group. Holiday Groups are useful for grouping the departments that would close on holidays and the departments that would remain open on holidays.

Associating Holiday Groups to Panels

A holiday group can be associated to a panel to control or restrict the panel access on holidays. For example, the access of the doors attached to the panel can be restricted on holidays.

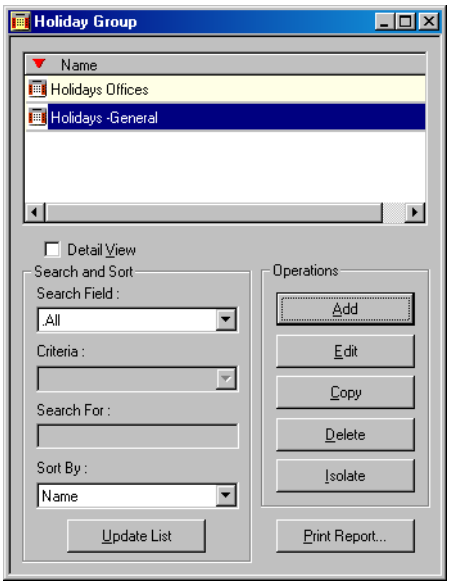
Associating Holiday Groups and Time Zones

When Time Zones and a Holiday Group are assigned to a panel, the start and end times for the H1 and H2 time slots are applicable to the Holiday Group.

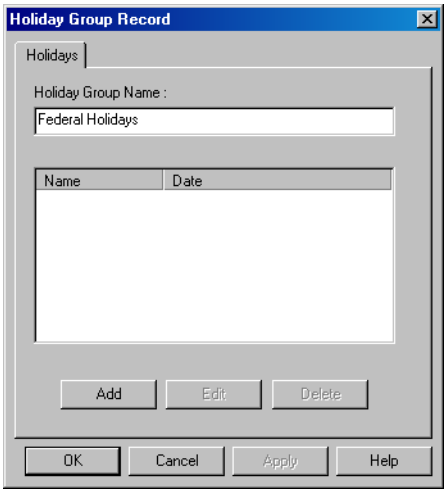
Adding a Holiday Group

To add a holiday group:

1. Choose **Configuration > Time Management > Holiday Group**. The **Holiday Group** window appears.

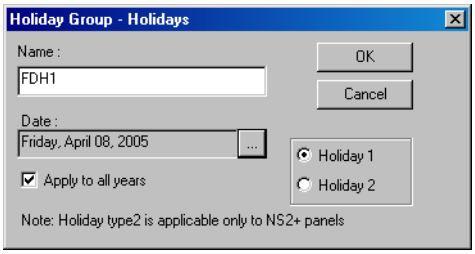


2. Click **Add** to add holidays to the holiday group. The **Holiday Group Record** dialog box appears.



3. Type the **Holiday Group Name**. For example, Federal Holidays.

4. Click **Add**. The **Holiday Group - Holidays** dialog box appears to add a list of holidays in the holiday group.



5. Type the **Name** of the holiday.
6. Click the ellipsis button to select the date.
7. Select the **Apply to all years** check box, if the holiday must recur every year.
8. Select the holiday category as **Holiday 1** or **Holiday 2**. The holiday groups are grouped into two major categories as Holiday 1 and Holiday 2. You can use these categories to group the mandatory holidays and optional holidays.

   Note: Holiday 2 category is applicable only for NS2+ panel types, as other panels do not support the holiday categories.
9. Click **OK** to save the holiday.
10. Repeat steps 4 to 9 for adding more holidays to the holiday group.
11. After adding the required holidays, click **OK**.

Editing a Holiday Group

To edit a holiday group:

1. Choose **Configuration > Time Management > Holiday Group**. The **Holiday Group** window appears with the list of existing holiday groups.
2. Select a holiday group from the list.
3. Click **Edit**. The **Holiday Group Record** dialog box appears.
4. Change the required details.
5. If you want to add a holiday to a holiday group, click **Add** and follow the same procedure as in "Adding a Holiday Group" .
6. Click **OK** to save the changes.

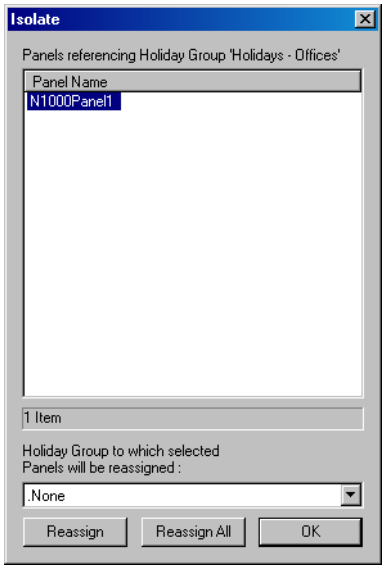
Isolating and Deleting a Holiday Group

If a holiday group is associated to a panel, you cannot delete the holiday group until you isolate it from the panel.

To isolate a holiday group:

1. Choose **Configuration > Time Management > Holiday Group**. The **Holiday Group** window appears with the list of existing holiday groups.

2. Select a holiday group from the list.
3. Click **Isolate**. The **Isolate** dialog box appears with the list of associated panels.



4. Select a panel and reassign it to a different holiday group.
5. Click **Reassign** to reassign the selected panel to a different holiday group. A confirmation message appears.

   OR

   If you want to reassign all the panels to the selected holiday group, click **Reassign All**. A confirmation message appears.
6. Click **OK** to confirm reassignment.
7. Repeat steps 4 to 6 to isolate the holiday groups from the panels.
8. Click **OK** to close the dialog box.

To delete a holiday group:

1. Choose **Configuration > Time Management > Holiday Group**. The **Holiday Group** window appears with the list of existing holiday groups.
2. Select a holiday group from the list.
3. Click **Delete**. The selected holiday group is deleted.

Daylight Saving Group

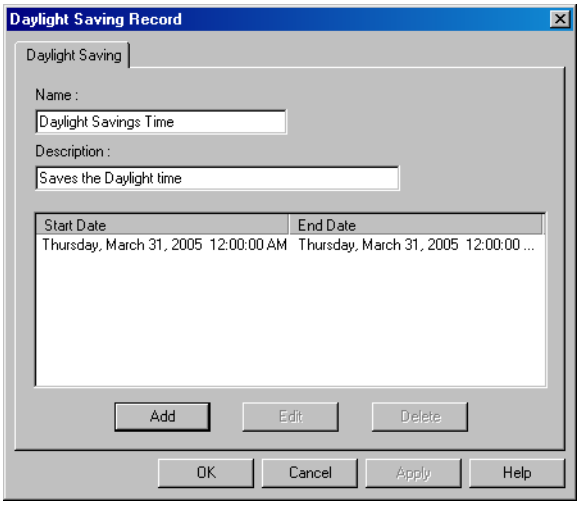
You can create a custom daylight saving group for the locations where the standard daylight saving group is not used. These daylight saving groups are attached to the panels for using the custom timings.

Note: The Daylight Saving Group is applicable only to P-Series Panels (PRO-2000 Intelligent Controller).

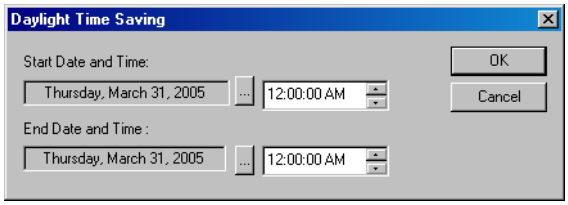
Adding a Daylight Saving Group

To add a daylight saving group:

1. Choose **Configuration > Time Management > Daylight Saving Group**. The **Daylight Saving Group** window appears.
2. Click **Add**. The **Daylight Saving Record** dialog box appears.



3. Type a **Name** for the daylight saving group and a **Description**.
4. Click **Add** to add daylight savings to a daylight saving group. The **Daylight Time Saving** dialog box appears.



5. To set the **Start Date and Time**:
   a. Click the ellipsis button to open the calendar.
   b. In the calendar, select the month, year and date or click **Today**, if you want to select the current date.
   c. Click **OK**. The date is selected and the calendar is closed.
   d. Type the start time. You can use or arrow to increase or decrease the current time.
6. To set the **End Date and Time**:
   a. Click the ellipsis button to open the calendar.
   b. In the calendar, select the month, year and date or click **Today**, if you want to select the current date.
   c. Click **OK**. The date is selected and the calendar is closed.

d. Type the end time. You can use ▲ or ▼ arrow to increase or decrease the current time.

7. Click **OK** to add the daylight time saving.

Editing a Daylight Saving Group

To edit a daylight saving group:

1. Choose **Configuration > Time Management > Daylight Saving Group**. The **Daylight Saving Group** window appears with the list of existing daylight saving groups.
2. Click **Edit**. The **Daylight Saving Record** dialog box appears with the details.
3. Change the details of the daylight saving group.
4. If you want to add new daylight timing to a daylight saving group, click **Add** and follow the same procedure of adding daylight timing as in "Adding a Daylight Saving Group" .
5. Click **OK** to save the changes.

Deleting a Daylight Saving Group

If a daylight saving group is associated to a panel, you cannot delete the daylight saving group.

To delete a daylight saving group:

1. Choose **Configuration > Time Management > Daylight Saving Group**. The **Daylight Saving Group** window appears with the list of existing groups.
2. Select a daylight saving group from the list.
3. Click **Delete**. The selected Daylight Saving Group is deleted.

Note: If you attempt to delete a daylight saving group that is associated to a panel, the following warning message appears:

Click **OK** to close the message box.

Device Map

11

In this chapter...

Introduction

The chapter **Device Map** describes how to configure servers, loops, panels, modem pools, and so on, which includes adding abstract devices and action groups.

Device Map Structure

The Device Map in WIN-PAK is a graphical tree structure that represents the physical connections of the devices. Devices include communication hardware, servers, panels, readers, and CCTV equipment. The following is the list of device types that can be added to the Device Map:

- Servers
- Communication Servers
- Communication Loops
- Panels
- Abstract Devices

In the Device Map tree structure, under the Devices folder, Servers and CCTV Switcher form the high level nodes of the tree. Communication Server is one of the servers added to the Devices folder, where you can add loops, modem pools and also direct connections to the P-Series panels. Physical devices such as card readers, keypads, input points, and output points are defined while configuring panels. The following picture depicts the structure of the Device Map tree:

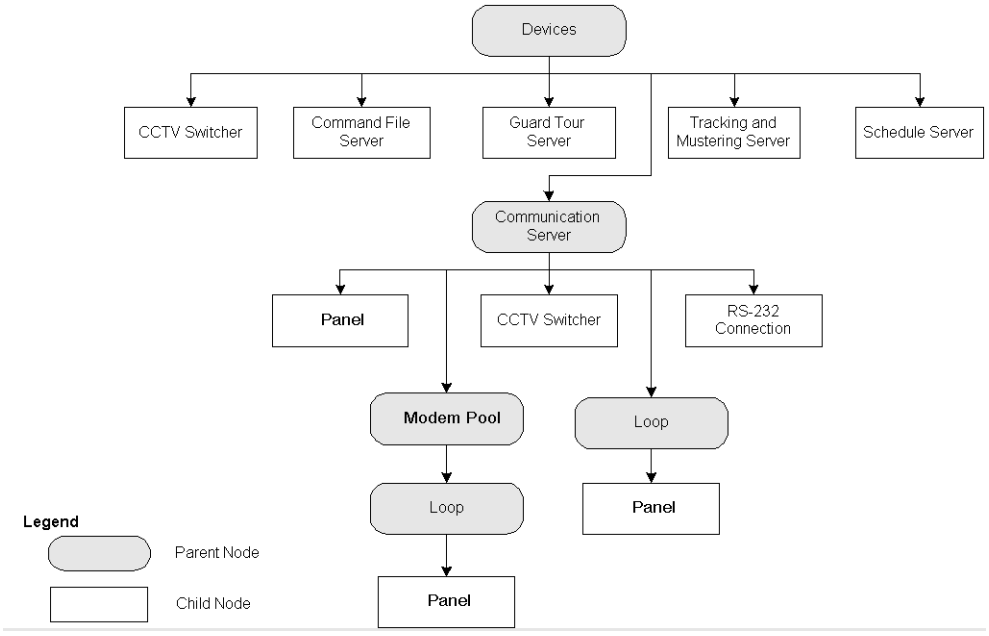


Figure 11-1 Graphical representation of the Device Map tree structure

Physical Devices and Abstract Devices

Abstract Devices logically represent physical devices in the access control system. Physical devices and connections must be configured as ADVs in WIN-PAK.

Servers and Devices

WIN-PAK has different servers to perform different tasks. The following is the list of servers in WIN-PAK for handling different functions:

Database Server

The WIN-PAK User Interface and other servers must request the Database Server to fetch the data from the SQL database. In addition, whenever the data is updated in the WIN-PAK UI, it is sent to the Database server to update the data in the SQL database.

Archive Database Server

The WIN-PAK user has an option to restore the backed up data and view the reports from the Archive Database Server.

Communication Server

The communication server establishes the connection between panels and WIN-PAK or other servers. Therefore, the servers must request the communication server to interact with panels.

Command File Server

The WIN-PAK User Interface and other servers must communicate with the Command File Server to execute the command file. In turn, the Command File server communicates with the communication server to send the commands to the hardware that are configured in Command File server.

Schedule Server

The Schedule Server communicates with the Database Server to configure the schedules and it communicates with other servers to run the schedules.

Guard Tour Server

The WIN-PAK User Interface and other servers must communicate with the Guard Tour Server to run the guard tour. In turn, the Guard Tour server communicates with the communication server to interact with panels or communicates with the database server to retrieve data in the SQL server.

Tracking and Muster Server

The WIN-PAK User Interface and other servers must communicate with the Tracking and Muster Server to monitor the tracking and mustering area. In turn, the Tracking and Muster server communicates with the communication server to interact with panels for retrieving the up-to-data on card reads.

Interacting with Intrusion Panels

In WIN-PAK, the intrusions happening in the premises of the access control system are monitored using the Galaxy and Vista panels. To monitor intrusions of a particular area in the access control system, the Galaxy panel groups or the Vista panel partitions in that area must be activated.

To set the Galaxy groups or arm the Vista partitions, you must:

1. Associate Galaxy groups or Vista partitions to the readers and the input points.

   Refer to the "Configuring a reader to the panel" section in this chapter for associating Galaxy groups or Vista partitions to the reader and the input point.

2. Add these readers and input points to the access area.

   Refer to the "Adding a Device" section in the chapter Defining Areas for adding readers to the access area.

3. Assign access levels for these readers and input points.

   Refer to the "Configuring Access Area" section in the chapter Card Holders for configuring readers in the access level.

4. Add privileged cards.

   Refer to the "Adding a Card" section in the chapter Card Holder for adding privileged cards.

The Galaxy Groups are set or Vista partitions are armed when a privileged card is swiped and the input button is pressed within 15 seconds.

Note: The Galaxy groups or Vista partitions are unset or disarmed:

- If the input button is not pressed after swiping the privileged card.
- A non-privileged card is swiped.

Server Configuration

Servers are configured in the Device Map for every WIN-PAK service. In addition, the servers can be placed on the floor plans and the server access can be assigned in the control area.

Servers establish the communication between various WIN-PAK devices and databases. This section explains how to set up the Communication Server, Command File Server, Guard Tour Server, Schedule Server, Tracking and Muster Server and Digital Video.

Communication Server

The Communication Server establishes the connection between WIN-PAK and the panels that are physically located in the access control system. The communication server must be available on the WIN-PAK Device tree for the WIN-PAK system to communicate with the system devices including the P-Series Intelligent Controller.

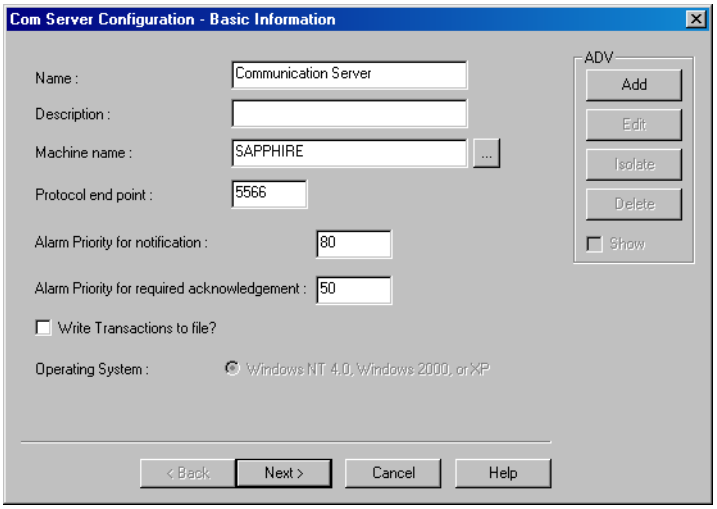
Multiple communication servers can be configured in WIN-PAK in a networked environment. This speeds up the communication when there are many devices in the communication. However, it depends on the type of WIN-PAK license that you availed.

Adding a Communication Server

To communicate with system devices such as panels, readers, inputs, or outputs, you must configure the Communication Server for your access control system. The Communication Server can be installed on the same machine as the Database Server or on another computer in a networked system.

To add a communication server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder and choose **Add** > **Communication Server**. The **Com Server Configuration - Basic Information** dialog box appears.



3. Type a **Name** for the communication server. It can be up to 30 characters.
4. Type the **Description** for the communication server. It can be up to 60 characters.
5. Click **Add** under **ADV** to create an ADV for the communication server. The **Abstract Device Record - Server** dialog box appears.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

6. After adding an ADV, click **OK** to return to the **Com Server Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Select the **Show** check box to view the ADV details.

7. Enter the **Machine Name** for the communication server. By default, it is the name of the local computer.

Tip: To find the machine name:

a. Right-click the **My Computer** icon on your desktop and click **Properties**. The **System Properties** dialog box appears.

b. Click the **Computer Name** tab. The machine name is displayed in the **Full computer name** field.

c. Note down the machine name and click **OK**.

8. Type a **Protocol end point** number that is not used by any other application or service on that computer.

Note: Each server must have a unique **Protocol end point** that can range from 1024 to 9999. The default number of **Protocol end point** need not be changed. However, you can change the number, if any other application uses the same port number.

9. Enter a value for the **Alarm Priority for notification**. An action with lower priority than this value is displayed as an event in the Event view.

Note: Ensure that this number is higher than the "Alarm Priority for required acknowledgement**"** value.

10. Set the **Alarm Priority for required acknowledgement** value. An action with higher priority than this value and with lower priority than "Alarm Priority for notification" value is displayed as an alarm in the Alarm View.

Note: Ensure that this value is higher than the priority number set in the Action Group while adding an ADV for the communication server. If you enter lower value than the priority number, the action is not displayed in Alarm View or in Event View. Rather, it is stored in the history of events.

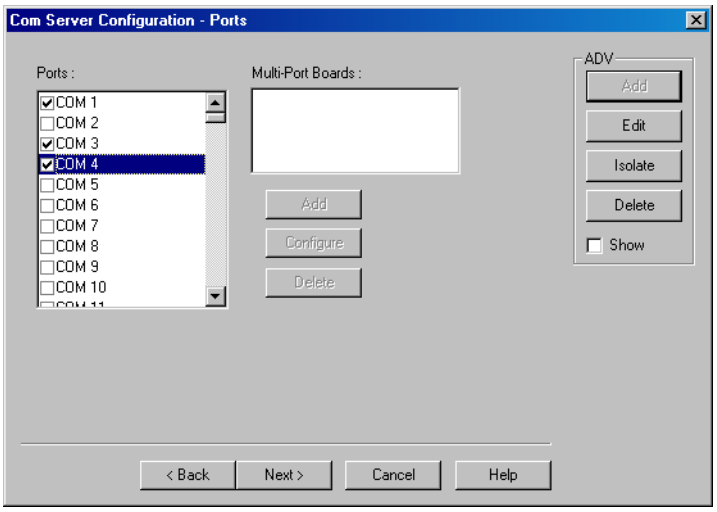
11. Select the **Write Transactions to file?** check box to write a record of the server transactions, message exchanges between communication server and panels into a text file. This file is used for debugging purposes.

Notes:

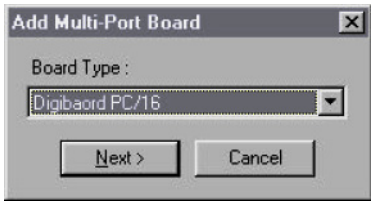
- For N-1000/PW-2000 panel types, the text file is generated every hour with the name of the file that indicates the date and time of the file generation. This file is stored in the RSDUMP folder where the WIN-PAK system is installed.

- For P-Series panel types, the transactions are written in the MCBdebug.txt file. Here the same file is updated every time the file is generated. This file is stored in C:\Windows\System32 or C:\Winnt\System32 folder based on the operating system used in the computer.

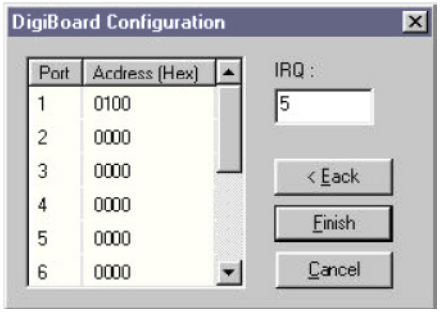
12. In the **Operating System** area, the OS of the WIN-PAK system is displayed.
13. Click **Next**. The **Com Server Configuration - Ports** dialog box appears.



14. In the **Ports** list, select the required check boxes for the COM port that are used on this server for the access control equipment.
15. If the server has a Multi-Port board,
    a. Click **Add** under **Multi-Port Boards**. The **Add Multi-Port Board** dialog box appears with a list of compatible multi-port boards.



    b. Select a multi-port board in the **Board Type** list. The available board types are Boca BB1004, Boca BB1008, Boca BB2016, Digiboard PC/4, Digiboard PC/8, and Digiboard PC/16.
    c. Click **Next**. The **DigiBoard Configuration** dialog box appears.



d. For each port, set a unique address and IRQ value.

   Consult the board manufacturer's documentation for further information.

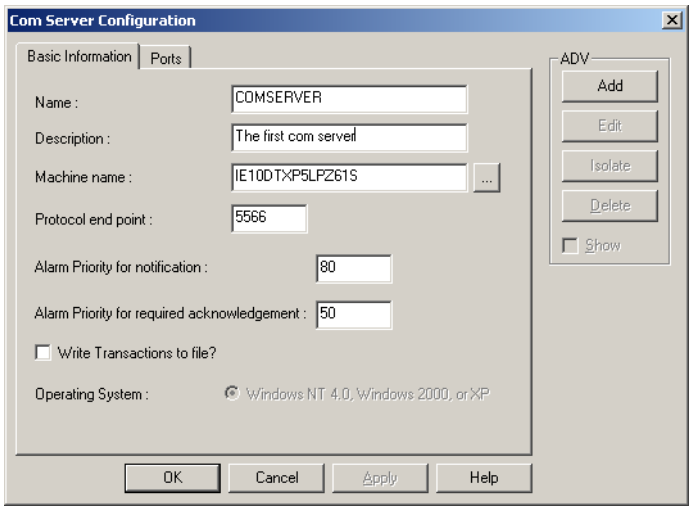
e. Click **Finish** to close the **Add Multi-Port Board** dialog box.

16. Click **Next** and then click **Finish** to add the communication server to the Device Map.

Editing a Communication Server

To edit the communication server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the communication server and click **Configure**. The **Com Server Configuration** dialog box appears.



4. Edit the required details of the communication server.

   Refer to the "Adding a Communication Server" section in this chapter for field description.

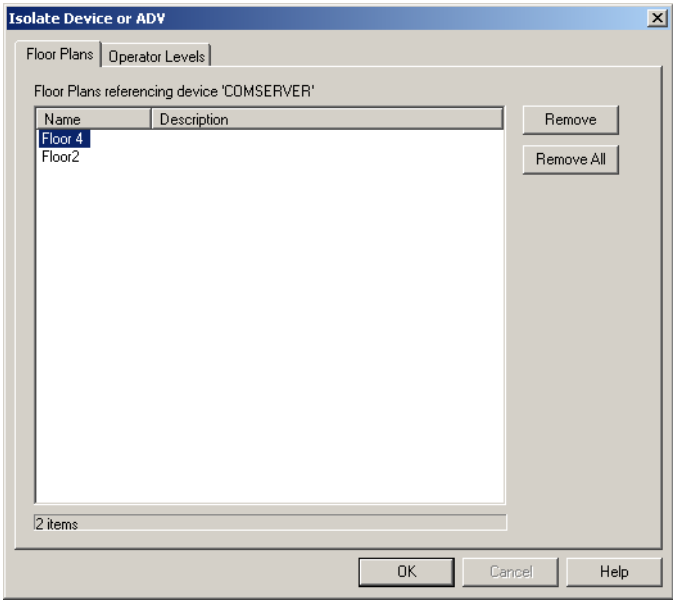
Isolating and Deleting a Communication Server

You can delete a communication server only if you delete the devices attached to the communication server. In addition, you must isolate an ADV of the communication server from floor plans and operator levels.

Isolating a communication server

To isolate a communication server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the communication server and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate floor plans from an ADV of communication server:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the communication server is displayed.
    b. Select the floor plans to be isolated from the communication server and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the communication server.
5. To isolate operator levels from an ADV of the communication server:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the communication server is displayed.

b. Select the operator levels that must be isolated from the communication server and click **Remove**. The selected operator levels are dissociated from the communication server.

   OR

   Click **Remove all** to isolate all the operator levels from the communication server.

c. To remove the communication server from the control area, clear the presence of an ADV of the communication server in the control area by clearing the **Present in Control Area** check box.

6. Click **OK**.

Deleting a communication server

After deleting or moving the devices and isolating the associated floor plans and operator levels, you can delete the communication server.

To delete a communication server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the communication server and click **Delete**. A message asking for confirmation appears.

4. Click **OK** to confirm the deletion. The communication server is deleted from the device map.

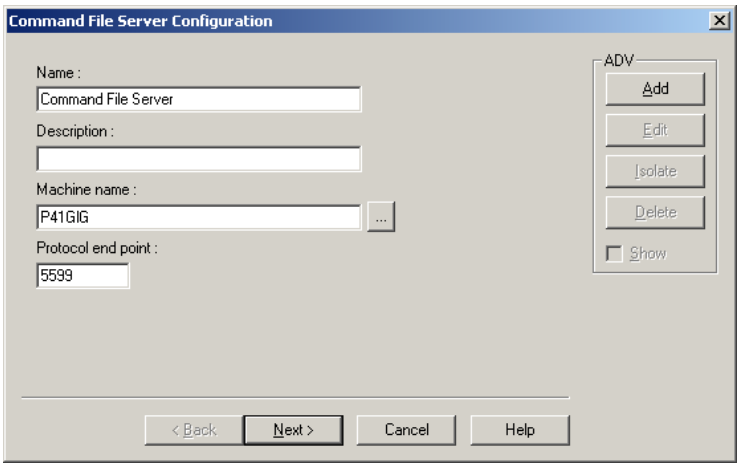
Command File Server

Before using the Command File functions, you must configure the Command File Server. Normally this server is located on the same machine as the Database Server.

Adding a Command File Server

To add a command file server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder and choose **Add** > **Command File Server**. The **Command File Server Configuration** dialog box appears.



3. Type a **Name** for the command file server.
4. Type the **Description** for the command file server.
5. Click **Add** under **ADV** to create an ADV for the command file server. The **Abstract Device Record - Server** dialog box appears.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
6. After adding an ADV, click **OK** to return to the **Communication Server Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Click the **Show** check box to view the ADV details.

7. Enter the **Machine Name** for the communication server.

   Tip: To find the machine name:

   a. Right-click the **My Computer** icon on your desktop and click **Properties**. The **System Properties** dialog box appears.

   b. Click the **Computer Name** tab. The machine name is displayed in the **Full computer name** field.

   c. Note down the machine name and click **OK**.
8. Type a **Protocol end point** number that is not used by any another device on the network.

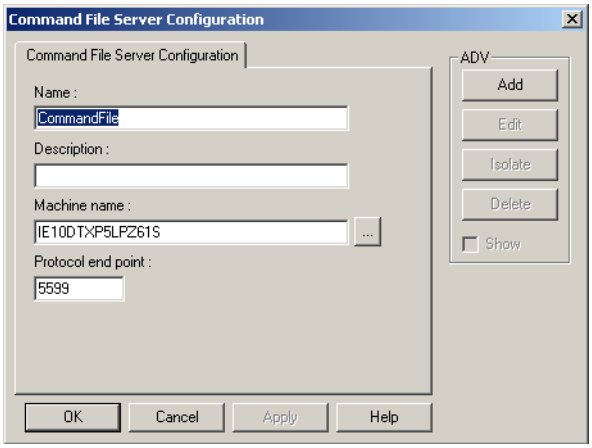
Note: Each server must have a unique **Protocol end point** that can range from 1024 to 9999. The default number of **Protocol end point** need not be changed. However, you can change the number, if you have multiple servers in your device map.

9. Click **Next** to proceed to the final dialog box for the Command File Server Configuration.
10. Click **Finish** to add the server to the Device Map.

Editing a Command File Server

To edit a command file server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the command file server and click **Configure**. The **Command File Server Configuration** dialog box appears.



4. Edit the required details of the command file server.

   Refer to the "Adding a Command File Server" section in this chapter for configuring a command file server.

5. Click **OK** to configure the command file server.

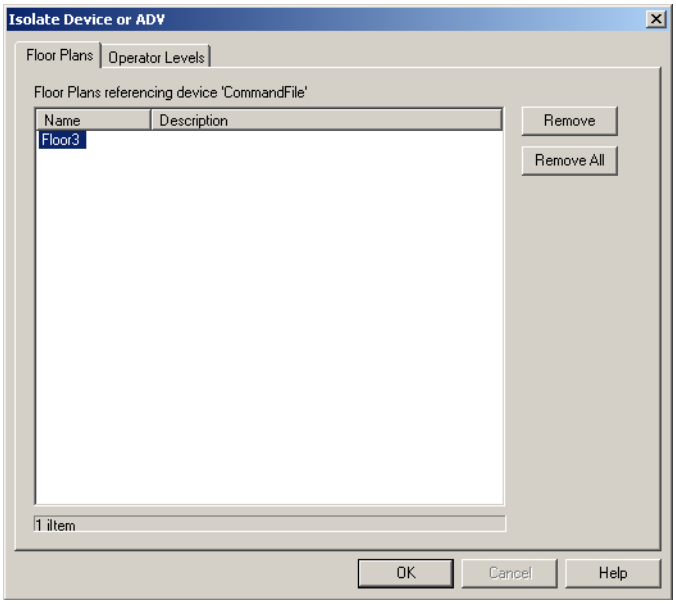
Isolating and Deleting a Command File Server

You can delete a command file server, only if you isolate an ADV of the command file server from floor plans and operator levels.

Isolating a command file server

To isolate a command file server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the command file server and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate floor plans from an ADV of the command file server:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the command file server is displayed.
    b. Select the floor plans to be isolated from the command file server and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the command file server.
5. To isolate operator levels from a device or an ADV of the command file server:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the command file server is displayed.
    b. Select the operator levels to be isolated from the command file server and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the command file server.
    c. To remove the command file server from the control area, clear the presence of an ADV of the command file server in the control area by clearing the **Present in Control Area** check box.
6. Click **OK**.

Deleting a command file server

After isolating the associated floor plans and operator levels, you can delete the command file server.

To delete a command file server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display servers and devices added to the device map.
3. Right-click the command file server and click **Delete**. A message asking for confirmation appears.
4. Click **OK** to confirm the deletion. The command file server is deleted from the device map.

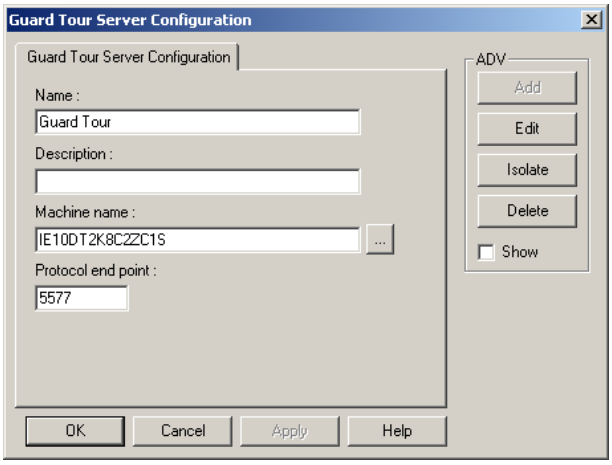
Guard Tour Server

Before using the Guard Tour functions, you must configure the Guard Tour Server. Normally this server is located on the same machine as the Database Server.

Adding a Guard Tour Server

To add a guard tour server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder and choose **Add > Guard Tour Server**. The **Guard Tour Server Configuration** window appears.



3. Type the **Name** of the schedule server and the **Description** for guard tour server.
4. Create an ADV for the guard tour server. Click **Add** under **ADV** to display the **Abstract Device Record - Server** dialog box.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

5. After adding an ADV, click **OK** to return to the **Guard Tour Server Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate** and **Delete** buttons to edit, isolate and delete the ADV.
- Click the **Show** check box to view the ADV details.

6. Enter the **Machine Name** for the guard tour server.

Tip: To find the machine name:

a. Right-click the **My Computer** icon on your desktop and click **Properties**. The **System Properties** dialog box appears.

b. Click the **Computer Name** tab.

c. Look for **Full computer name** field. This is the machine name of your computer.

d. Note down the machine name and click **OK**.

7. Type a **Protocol end point** number that is not used by any other device on the network.

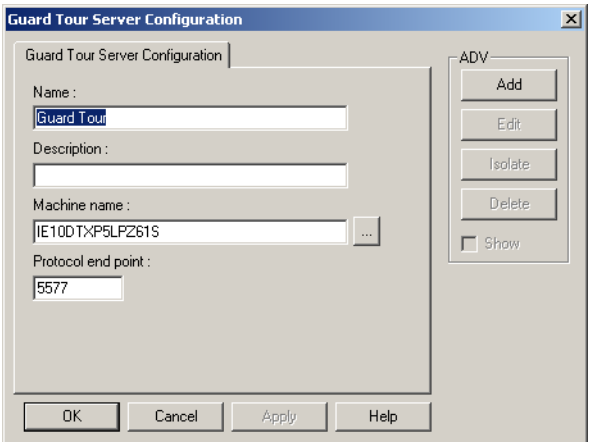
Note: Each server must have a unique **Protocol end point** that can range from 1024 to 9999. The default number of **Protocol end point** need not be changed. However, you can change the number, if you have multiple servers in your device map.

8. Click **Next** to proceed to the final dialog box for the Guard Tour Server Configuration.
9. Click **Finish** to add the server.

Editing a Guard Tour Server

To edit a guard tour server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the guard tour server and click **Configure**. The **Guard Tour Server Configuration** dialog box appears.



4. Make the required changes of the guard tour server.

   Refer to the "Adding a Guard Tour Server" section in this chapter for configuring guard tour server.

5. Click **OK** to save the changes.

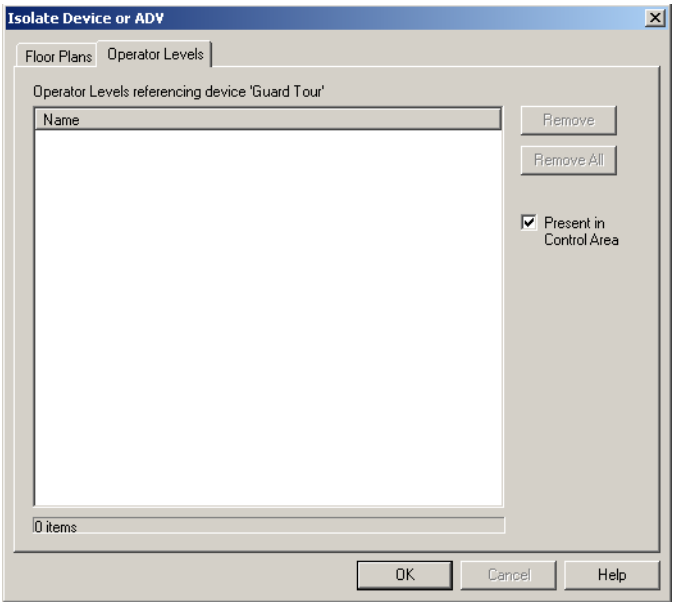
Isolating and Deleting a Guard Tour Server

You can delete a guard tour server, only if you isolate an ADV of the guard tour server from floor plans and operator levels.

Isolating a guard tour server

To isolate a guard tour server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the guard tour server and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate floor plans from an ADV of the guard tour server:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the guard tour server is displayed.
    b. Select the floor plans to be isolated from the guard tour server and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the guard tour server.
5. To isolate operator levels from an ADV of the guard tour server:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the guard tour server is displayed.
    b. Select the operator levels to be isolated from the guard tour server and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels.
    c. To remove a guard tour server from the control area, clear the presence of guard tour server by clearing the **Present in Control Area** check box.
6. Click **OK**.

Deleting a guard tour server

After deleting the child nodes and isolating the associated floor plans and operator levels, you can delete the guard tour server.

To delete a guard tour server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the guard tour server and click **Delete**. A message asking for confirmation appears.
4. Click **OK** to confirm the deletion. The guard tour server is deleted from the device map.

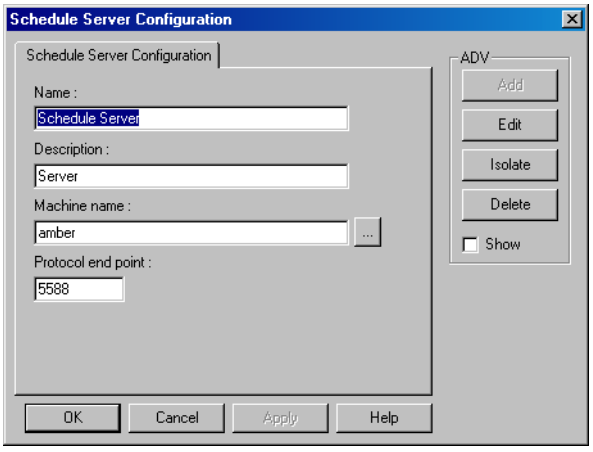
Schedule Server

Before using the Scheduling functions, you must configure a Schedule Server. Normally the Schedule Server is located on the same machine as the Database Server.

Adding a Schedule Server

To add a schedule server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder and choose **Add** > **Schedule Server**. The **Schedule Server Configuration** window appears.



3. Type the **Name** of the schedule server.
4. Type the **Description** for the schedule server.
5. Click **Add** under **ADV** to create an ADV for the schedule server. The **Abstract Device Record - Server** dialog box appears.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

6. After adding an ADV, click **OK** to return to the **Schedule Server Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Click the **Show** check box to view the ADV details.

7. Enter the **Machine Name** for the schedule server.

Tip: To find the machine name:

a. Right-click the **My Computer** icon on your desktop and click **Properties**. The **System Properties** dialog box appears.

b. Click the **Computer Name** tab.

c. Look for **Full computer name** field. This is the machine name of your computer.

d. Note down the machine name and click **OK**.

8. Type a **Protocol end point** number that is not used by any another device on the network.

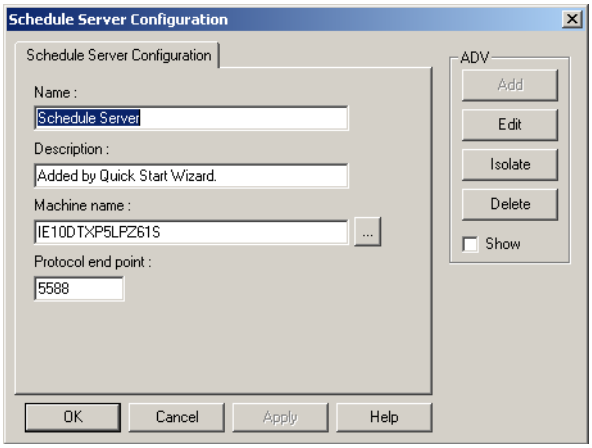
Note: Each server must have a unique **Protocol end point** that can range from 1024 to 9999. The default number of **Protocol end point** need not be changed. However, you can change the number, if you have multiple servers in your device map.

9. Click **Next** to proceed to the final dialog box for the Schedule Server Configuration.
10. Click **Finish** to add the server to the Device Map.

Editing a Schedule Server

To edit a schedule server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the schedule server and click **Configure**. The **Schedule Server Configuration** dialog box appears.



4. Edit the required details of the schedule server.

   Refer to the "Adding a Schedule Server" section in this chapter for configuring guard tour server.

5. Click **OK** to configure the schedule server.

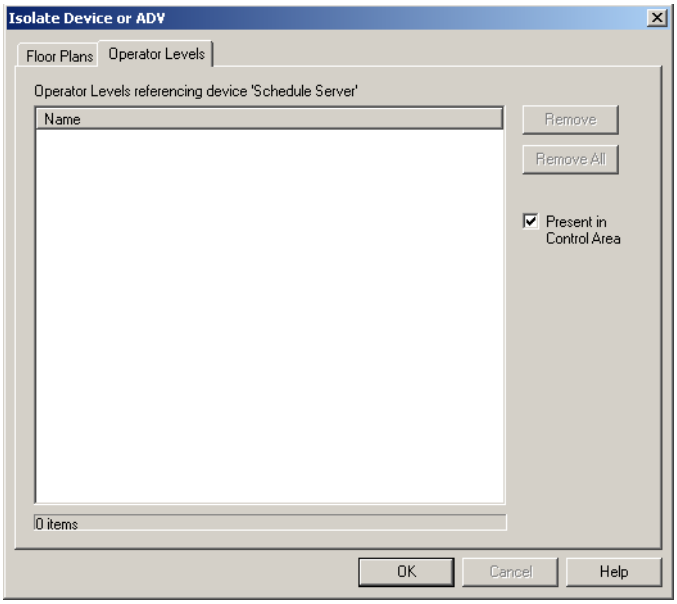
Isolating and Deleting a Schedule Server

You can delete a schedule server, only if you isolate the device or an ADV of schedule server from floor plans and operator levels.

Isolating a schedule server

To isolate a schedule server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the schedule server and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate floor plans from an ADV of the schedule server:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the schedule server is displayed.
    b. Select the floor plans to be isolated from the schedule server and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans.
5. To isolate operator levels from a device or an ADV of schedule server:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the schedule server is displayed.
    b. Select the operator levels to be isolated from the schedule server and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels.
    c. To remove the schedule server from the control area, clear the presence of an ADV of the schedule server in the control area, clear the **Present in Control Area** check box.
6. Click **OK**.

Deleting a schedule server

After isolating the associated floor plans and operator levels, you can delete the schedule server.

To delete a schedule server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the schedule server and click **Delete**. A message asking for confirmation appears for deleting the server.
4. Click **OK** to confirm the deletion. The schedule server is deleted from the device map.

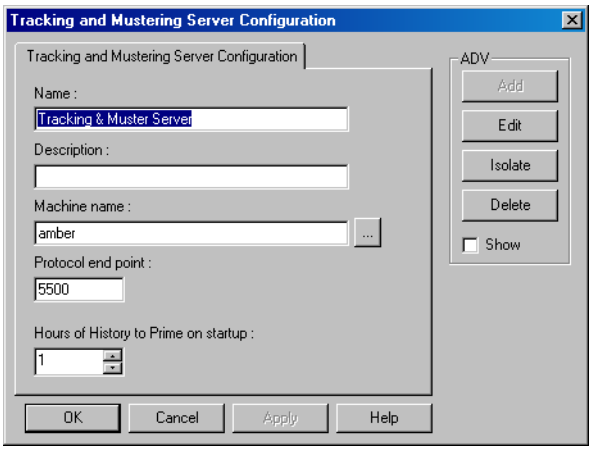
Tracking and Muster Server

Before using the Tracking and Muster functions, you must configure a Tracking and Muster Server. Normally the server is located on the same machine as the Database Server.

Adding a Tracking and Muster Server

To add a tracking and muster server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder at the top of the tree, choose **Add**, then click **Tracking and Muster Server**. The **Tracking and Mustering Server Configuration** dialog box appears.



3. Type a unique **Name** of the tracking and muster server and the **Description** for tracking and muster server.
4. Click **Add** under **ADV** to create an ADV for the tracking and muster server. The **Abstract Device Record - Server** dialog box appears.

Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

5. After adding an ADV, click **OK** to return to the **Tracking and Mustering Server Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Click the **Show** check box to view the ADV details.

6. Enter the **Machine Name** where the tracking and muster server is located.

Tip: To find the machine name:

a. Right-click the **My Computer** icon on your desktop and click **Properties**. The **System Properties** dialog box appears.

b. Click the **Computer Name** tab.

c. Look for **Full computer name** field. This is the machine name of your computer.

d. Note down the machine name and click **OK**.

7. Type a **Protocol end point** number that is not used by any other device on the network.

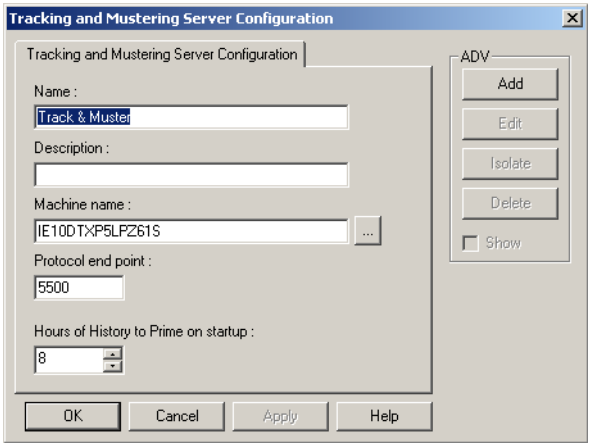
Note: Each server must have a unique **Protocol end point** that can range from 1024 to 9999. The default number of **Protocol end point** need not be changed. However, you can change the number, if you have multiple servers in your device map.

8. In **Hours of History to Prime on startup**, increase or decrease the number of hours the tracking history is processed and displayed when the Muster View is opened. The hours can range from 0 to 99. By default, it is set to 8 hours.
9. Click **Next** to proceed to the final dialog box for the Tracking and Muster Server configuration.
10. Click **Finish** to add the server to the Device Map.

Editing a Tracking and Muster Server

To edit a tracking and muster server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the tracking and muster server and click **Configure**. The **Tracking and Mustering Server Configuration** dialog box appears.



4. Edit the required details of the tracking and muster server.

   Refer to the "Adding a Tracking and Muster Server" section in this chapter for configuring the tracking and muster server.

5. Click **OK** to configure the tracking and muster server.

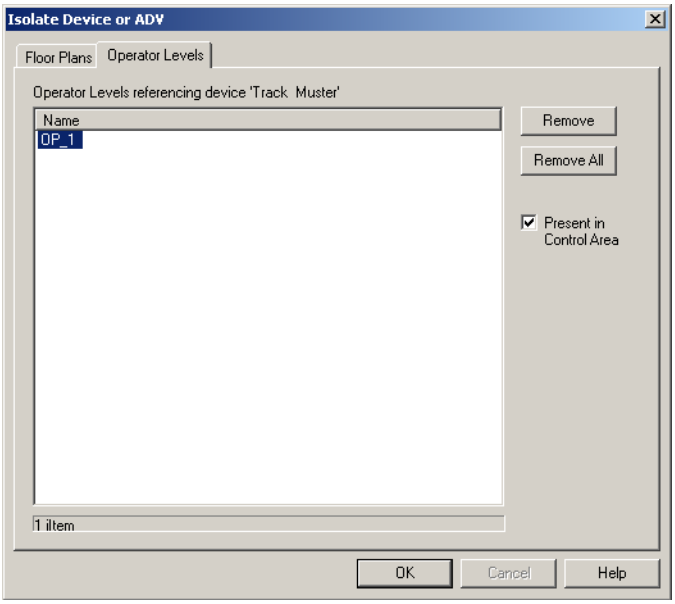
Isolating and Deleting a Tracking and Muster Server

You can delete a tracking and muster server, if only you isolate an ADV of tracking and muster server from floor plans and operator levels.

Isolating a tracking and muster server

To isolate a tracking and muster server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the tracking and muster server and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate floor plans from an ADV of tracking and muster server:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the tracking and muster server is displayed.
    b. Select the floor plans to be isolated from the tracking and muster server and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the tracking and muster server.
5. To isolate operator levels from an ADV of tracking and muster server:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the command file server is displayed.
    b. Select the operator levels to be isolated from the command file server and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels.
    c. To remove the tracking and muster server from the control area, clear the presence of an ADV of the tracking and muster server in the control area, clear the **Present in Control Area** check box.
6. Click **OK**.

Deleting a tracking and muster server

After isolating the associated floor plans and operator levels, you can delete the tracking and muster server.

To delete a tracking and muster server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the tracking and muster server and click **Delete**. A message asking for confirmation appears for deleting the server.
4. Click **OK** to confirm the deletion. The tracking and muster server is deleted from the device map.

Digital Video

Digital Video is defined as a digital video recorder system. In WIN-PAK, the video is viewed using the Digital Video Display window. This window can also be triggered by an action of the panel. To do that, you must select a camera for the panel action in ADV configuration.

As panels, the digital video configuration does not have a defined set of action groups. Therefore, if you want to set an action group to the ADV, you must add a custom action group.

The digital videos supported by WIN-PAK are RapidEye, Fusion and Dedicated Micros.

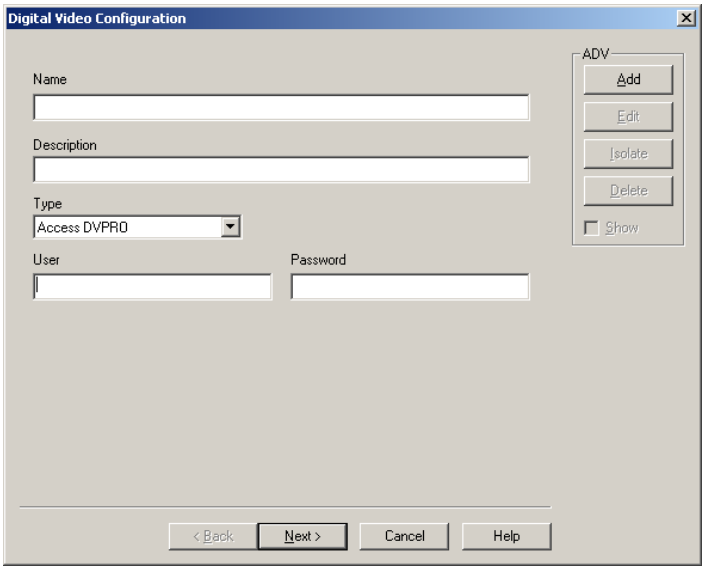
Configuring an Access DVPRO Digital Video

Ensure that you configure the Digital Video, before using the Access DVPRO functions.

Note: For Access DVPRO, RapidEye Software needs to be installed on the computer from where it has to be viewed.

To add a new Access DVPRO:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder and choose **Add** > **Digital Video**. The **Digital Video Configuration** window appears.



3. Select the **Type** of digital video as **Access DVPRO**.
4. Type a **Name** and the brief **Description** for the Access DVPRO.
5. Type the **User** name and **Password**. These fields are mandatory.

Note: The Access DVPRO name is identical to the RapidEye Site name. The User name and Password are used for controlling the digital video device and they must be identical to the User name and Password defined in the RapidEye software.

6. Click **Add** under **ADV** to create an ADV for the Access DVPRO digital video. The **Abstract Device Record - Access DVPRO DVSS** dialog box appears.

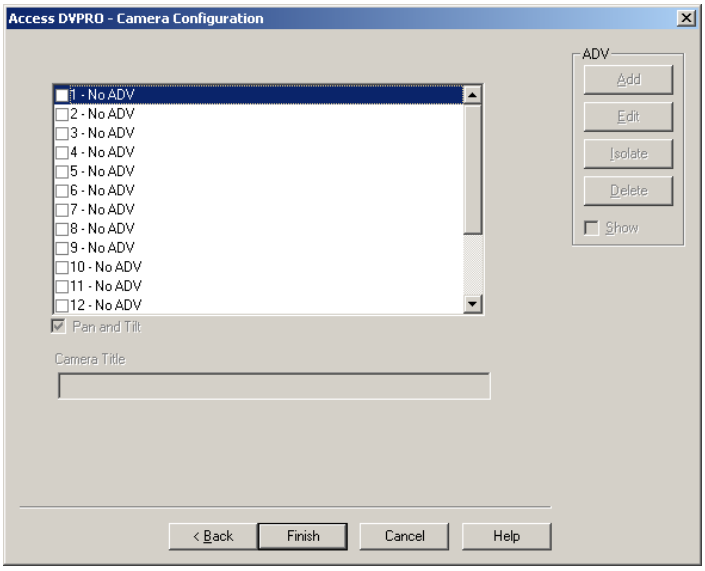
   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

7. After adding an ADV, click **OK** to return to the **Digital Video Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Click the **Show** check box to view the ADV details.

8. Click **Next** to add ADVs to the digital video cameras. The **Access DVPRO - Camera Configuration** dialog box appears.

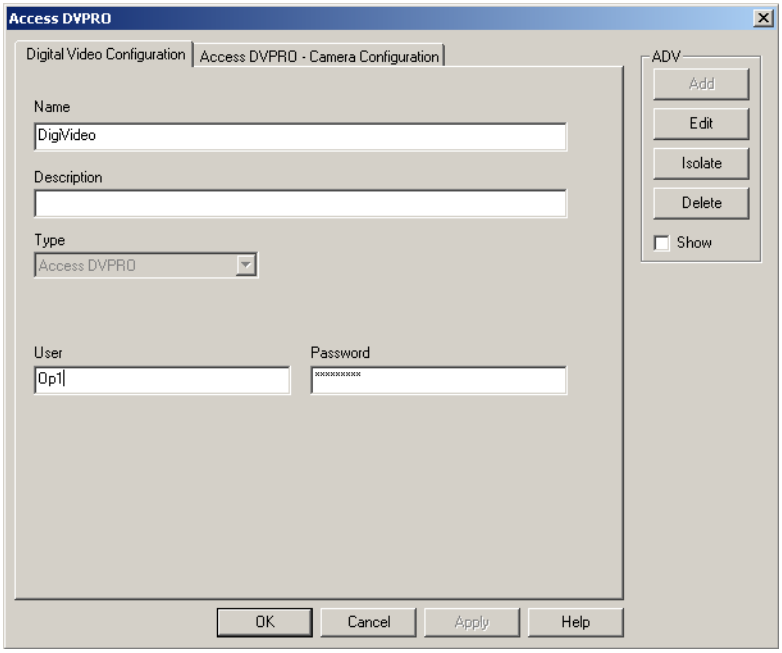


9. Configure an ADV for each camera attached to the digital video. Select an ADV, double-click to enter a name and press ENTER or click **Add** under **ADV** and enter the ADV properties and click **OK**.
10. Select or clear the **Pan and Tilt** check box to define a camera as a PTZ (Pan Tilt Zoom) camera or as a stationary camera.
11. Type the title for the camera in **Camera Title**.
12. Click **Finish** to save the digital video.

Editing an Access DVPRO

To edit an Access DVPRO digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the access DVPRO and click **Configure**. The **Access DVPRO** dialog box appears.



4. Click the corresponding tab and make the required changes.

   Refer to the "Configuring an Access DVPRO Digital Video" section in this chapter for configuring Access DVPRO digital video.

5. Click **OK** to save the changes.

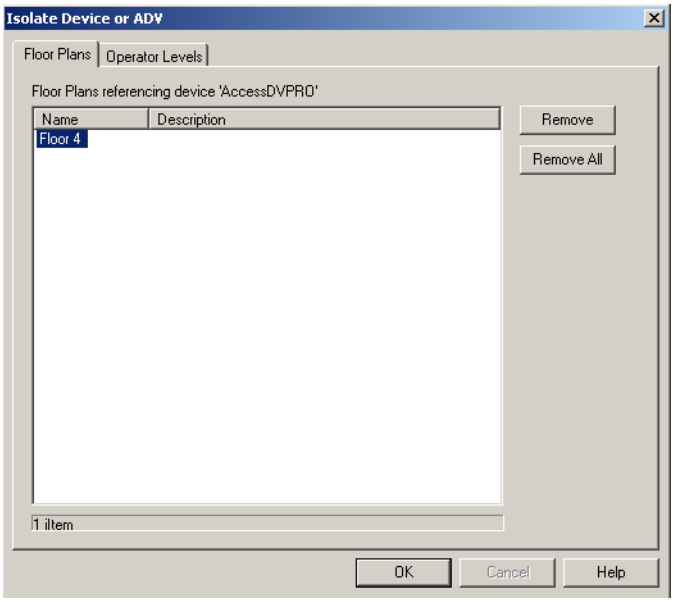
Isolating and Deleting an Access DVPRO

You can delete an access DVPRO digital video only if you isolate an ADV of the access DVPRO digital video from floor plans and operator levels.

Isolating an access DVPRO digital video

To isolate an access DVPRO digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the access DVPRO digital video and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



3. To isolate floor plans from an ADV of the access DVPRO digital video:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the access DVPRO digital video is displayed.
    b. Select the floor plans to be isolated from the access DVPRO digital video and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the access DVPRO digital video.
4. To isolate operator levels from an ADV of access DVPRO digital video:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the access DVPRO digital video is displayed.
    b. Select the operator levels to be isolated from the access DVPRO digital video and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the access DVPRO digital video.
    c. To remove the access DVPRO digital video from the control area, clear the presence of an ADV of the access DVPRO digital video in the control area by clearing the **Present in Control Area** check box.
5. Click **OK**.

Deleting an access DVPRO digital video

After deleting the child nodes and isolating the associated floor plans and operator levels, you can delete the access DVPRO digital video.

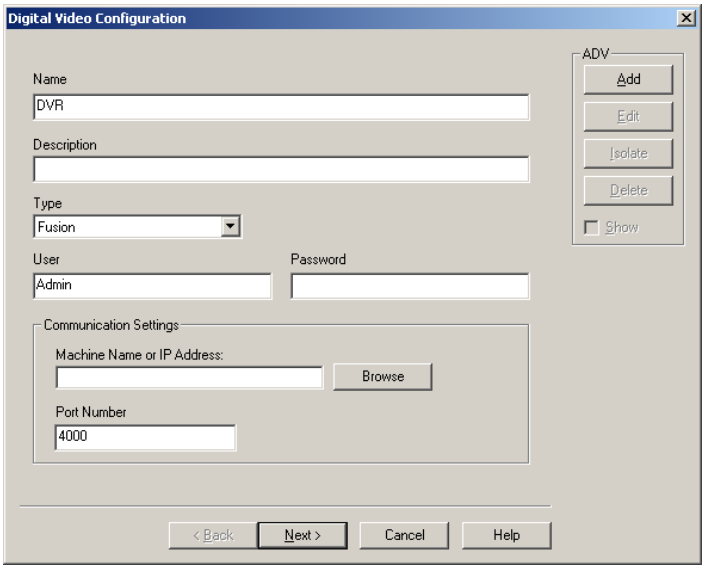
To delete an access DVPRO digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices that are added to the device map.
3. Right-click the access DVPRO digital video and click **Delete**. A message asking for confirmation appears for deleting the digital video.
4. Click **OK** to confirm the deletion. The access DVPRO digital video is deleted from the device map.

Configuring a Fusion Digital Video

To add a Fusion digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder and choose **Add** > **Digital Video**. The **Digital Video Configuration** dialog box appears.



3. Select the **Type** of digital video as **Fusion**.
4. Type the **Name** and the brief **Description** for the Fusion DVR.
5. Type the **User** name and **Password**. The User and Password fields are mandatory.
6. Under **Communication Settings**, type the **Machine Name or IP Address** of the Fusion DVR. You can use the **Browse** button to select the machine name.

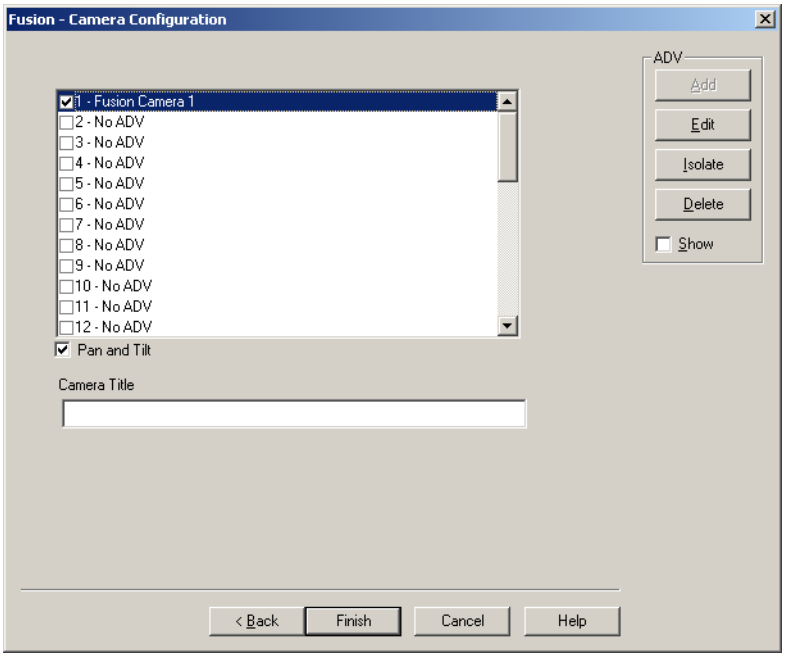
7. Enter the **Port Number** which is the same as the port number configured in Fusion DVR. However, Honeywell recommends the default port number.
8. Click **Add** under **ADV** to create an ADV for the digital video. The **Abstract Device Record** dialog box appears.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
9. After adding an ADV, click **OK** to return to the **Digital Video Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Click the **Show** check box to view the ADV details.

10. Click **Next** to add ADVs to the fusion cameras. The **Fusion - Camera Configuration** dialog box appears.

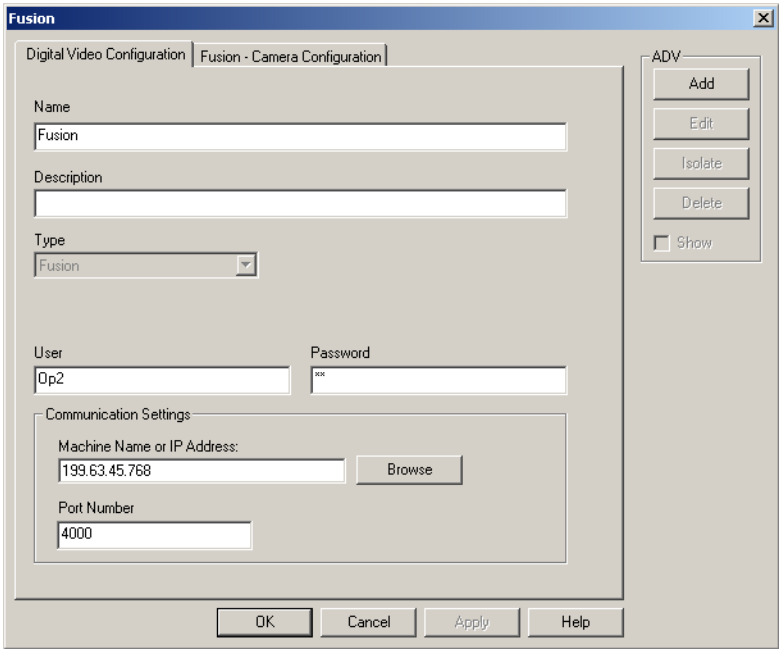


11. Create an ADV for each camera attached to the digital video. Select an ADV, double-click to enter a name and press ENTER or click **Add** under **ADV** and set the ADV properties and click **OK**.
12. Select or clear the **Pan and Tilt** check box to define the fusion camera as a PTZ (Pan Tilt Zoom) camera or as a stationary camera.
13. Type the title for the camera in **Camera Title**.
14. Click **Finish** to save the digital video.

Editing a Fusion Digital Video

To edit a Fusion digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the Fusion and click **Configure**. The **Fusion** dialog box appears.



3. Click the corresponding tab and make the required changes.

   Refer to the "Configuring a Fusion Digital Video" section in this chapter for configuring Fusion digital video.

4. Click **OK** to save the changes.

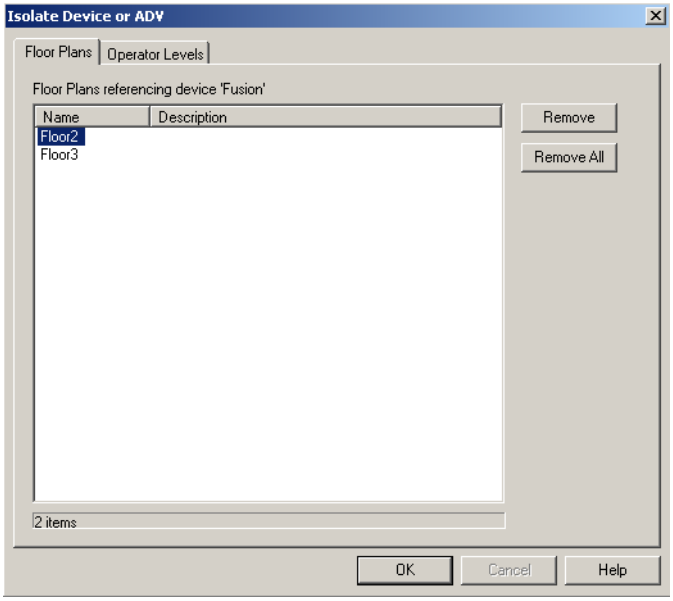
Isolating and Deleting a Fusion Digital Video

You can delete a fusion digital video, only if you isolate an ADV of fusion digital video from floor plans and operator levels.

Isolating a fusion digital video

To isolate a fusion digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices.
3. Right-click the fusion video and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate floor plans from an ADV of the fusion digital video:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the fusion digital video is displayed.
    b. Select the floor plans to be isolated from the fusion digital video and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the fusion digital video.
5. To isolate operator levels from an ADV of the fusion digital video:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the fusion digital video is displayed.
    b. Select the operator levels to be isolated from the fusion digital video and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the fusion digital video.
    c. To remove the fusion digital video from the control area, clear the presence of an ADV of the fusion digital video in the control area, clear the **Present in Control Area** check box.
6. Click **OK**.

Deleting a fusion digital video

After deleting the child nodes and isolating the associated floor plans and operator levels, you can delete the fusion digital video.

To delete a fusion digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the fusion digital video and click **Delete**. A message asking for confirmation appears.
3. Click **OK** to confirm the deletion. The fusion digital video is deleted from the device map.

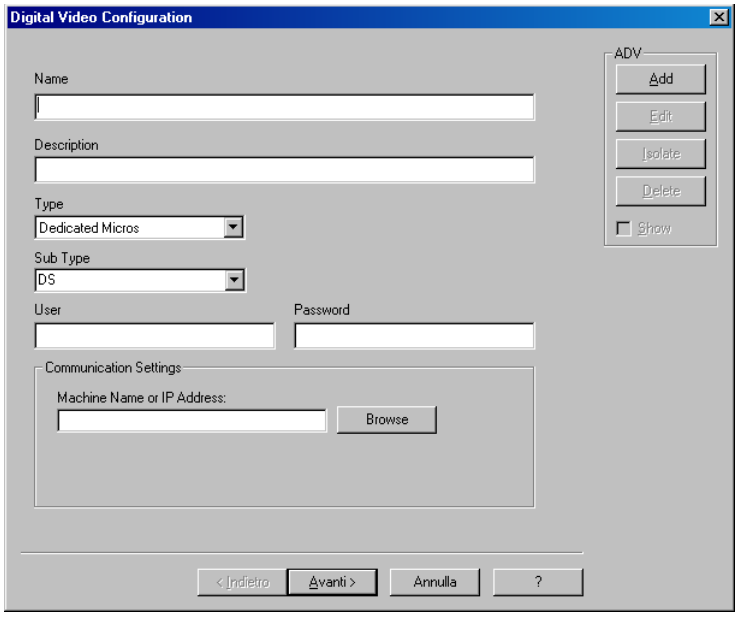
Configuring a Dedicated Micros Digital Video

Ensure that you configure the Digital Video, before using the Dedicated Micros functions.

Note: You must procure the license for dedicated micros for enabling this feature in WIN-PAK.

To add a new Dedicated Micros:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder and choose **Add** > **Digital Video**. The **Digital Video Configuration** dialog box appears.



3. Select the digital video **Type** as **Dedicated Micros**. The relevant fields are enabled.
4. Select the **Sub Type** of the dedicated micros. The available sub types are **DS** and **DVIP**.

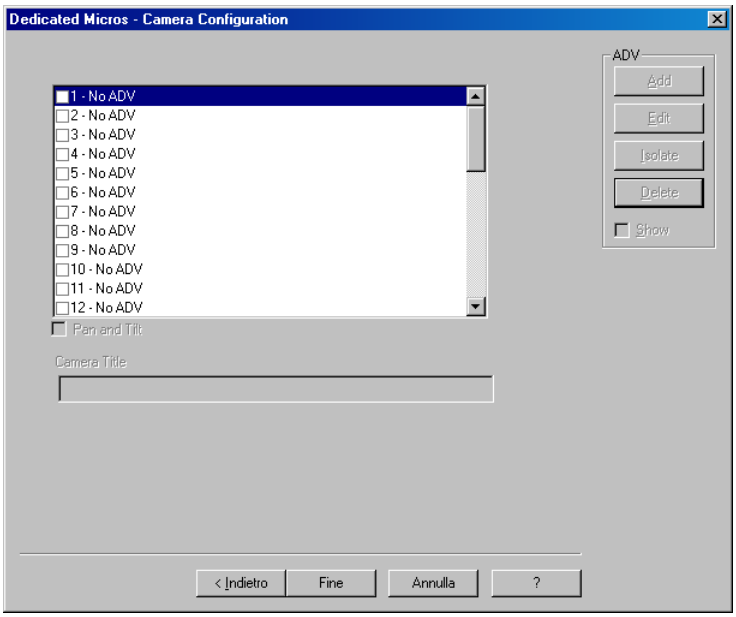
5. Type a **Name** and the brief **Description** for the dedicated micros.
6. Type the **User** name and **Password**. These fields are mandatory.
7. Under **Communication Settings**, type the **Machine Name or IP Address** of the Dedicated Micros. You can use the **Browse** button to select the machine name.
8. Click **Add** under **ADV** to create an ADV for the Access DVPRO digital video. The **Abstract Device Record - Access DVPRO DVSS** dialog box appears.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
9. After adding an ADV, click **OK** to return to the **Digital Video Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Select the **Show** check box to view the ADV details.

10. Click **Next** to add ADVs to the digital video cameras. The **Dedicated Micros-Camera Configuration** dialog box appears.



11. Configure ADVs for every camera that is attached to the digital video. To configure an ADV:
    a. Select and double-click the ADV.
    b. Enter a name and press ENTER

    OR

    a. Click **Add** under **ADV**. The ADV dialog box appears.

b. Enter the ADV properties and click **OK**.

12. Select or clear the **Pan and Tilt** check box to define a camera as a PTZ (Pan Tilt Zoom) camera or as a stationary camera.
13. Type the title for the camera in **Camera Title**.
14. Click **Finish** to save the digital video.

Editing a Dedicated Micros

To edit a Dedicated Micros digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the dedicated micros and click **Configure**. The **Dedicated Micros** dialog box appears.
4. Click the desired tab and make the required changes.

   Refer to the "Configuring an Access DVPRO Digital Video" section in this chapter for configuring Access DVPRO digital video.
5. Click **OK** to save the changes.

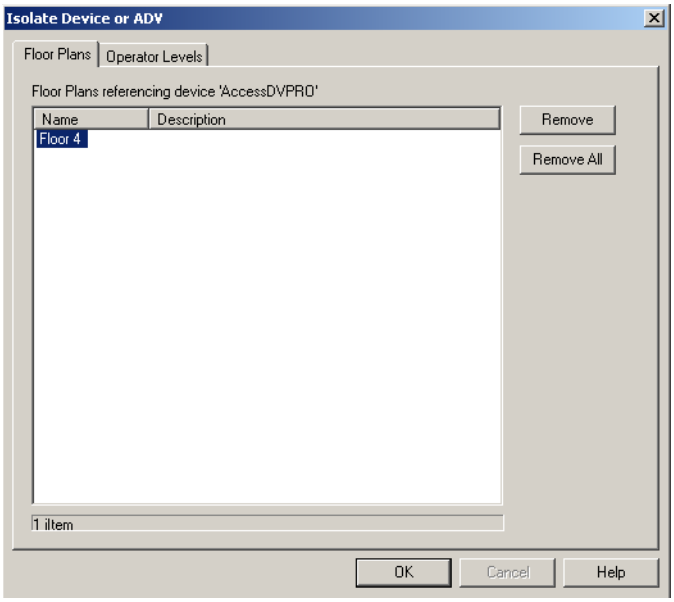
Isolating and Deleting an Access DVPRO

You can delete a dedicated micros digital video only after you isolate its ADV from floor plans and operator levels.

Isolating a dedicated micros digital video

To isolate a dedicated micros digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the dedicated micros digital video and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



3. To isolate floor plans from an ADV of the dedicated micros digital video:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the dedicated micros digital video is displayed.
    b. Select the floor plans to be isolated from the dedicated micros digital video and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the dedicated micros digital video.
4. To isolate operator levels from an ADV of the dedicated micros digital video:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the dedicated micros digital video is displayed.
    b. Select the operator levels to be isolated from the dedicated micros digital video and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the dedicated micros digital video.
    c. To remove the access DVPRO digital video from the control area, clear the presence of an ADV of the dedicated micros digital video in the control area by clearing the **Present in Control Area** check box.
5. Click **OK**.

Deleting a dedicated micros digital video

After deleting the child nodes and isolating the associated floor plans and operator levels, you can delete the dedicated micros digital video.

To delete a dedicated micros digital video:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices that are added to the device map.
3. Right-click the dedicated micros digital video and click **Delete**. A message asking for confirmation appears.
4. Click **OK** to confirm the deletion. The dedicated micros digital video is deleted from the device map.

Communication Loops

A communication loop is an interface between the panels and the communication server. It must be added to an existing communication server on the Device Map. You must have an available communication port, for each panel or a communication loop to be added to a loop.

Note: You must create an ADV for each loop, panel, and other communication interfaces while configuring them.

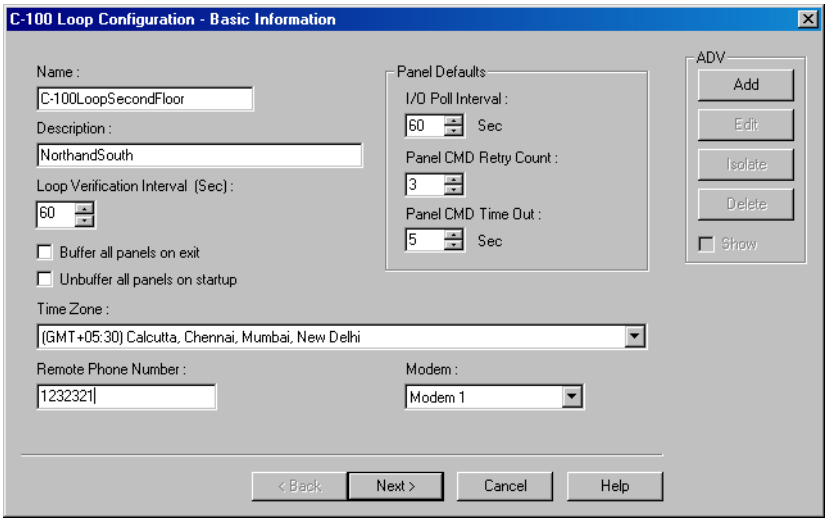
C-100 Panel Loop

Panels using 20-milliamp communications can be connected to the WIN-PAK system by a C-100 communication adaptor. The C-100 connection is defined by adding it to the Device Map.

Adding a C-100 Panel Loop

To add a C-100 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and then right-click the communication server and click **Panel Loop (C-100)**. The **C-100 Loop Configuration - Basic Information** dialog box appears.



3. Type a unique **Name** for the panel loop. This field is mandatory.
4. Type a **Description** for the panel loop.
5. Create an ADV for the communication loop. Click **Add** under **ADV** to display the **Abstract Device Record - Server** dialog box.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
6. After adding an ADV, click **OK** to return to the **Communication Server Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate** and **Delete** buttons to edit, isolate and delete the ADV.
- Select the **Show** check box to view the ADV details.

7. Increase or decrease the **Loop Verification Interval (Sec)** to verify whether the loop is responding when a signal is send from WIN-PAK to the C-100 loop.

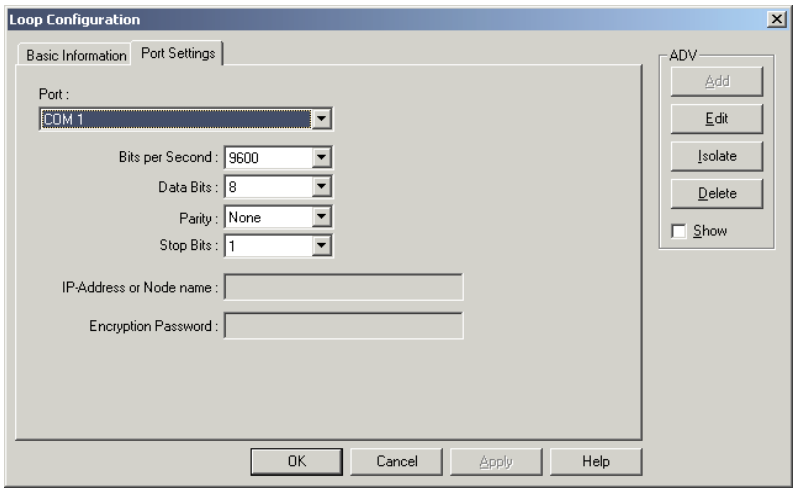
   Increasing the interval improves the bandwidth. The default interval is set to 60 seconds as it is an optimal value.
8. Select **Buffer all panels on exit** to buffer the events on all the panels when the communication server is stopped.
9. Select **Unbuffer all panels on startup** to unbuffer all the panel events when the communication server is started.
10. Select the standard **Time Zone** based on the loop location.
11. Set the **Panel Defaults** for the panel loop.

a. **I/O Poll Interval**: Select the interval at which the signal must be sent to the panel to verify the communication and check the panel's input and output states. By default, the frequency interval is 60 seconds.

b. **Panel CMD Retry Count**: Specify the number of times a command must be resent to the panel, if the event of the panel not responding to the command. By default, the command is resent 3 times.

c. **Panel CMD Time Out**: Specify the waiting time for receiving a response from the panel and for time out the command. By default, the loop waits for 5 seconds.

12. Click **Next** to set the port for the loop.



13. In the **Port** list, select a port of the communication server to which the loop is to be connected. The ports that are selected for the communication server and not used for other loops are listed.

14. If you select a port,

a. Select the communication baud rate for the loop in **Bits per second**.

b. Select the number of bytes that can be transferred in **Data Bits.** Select a number between 4 and 8. By default, it is set to **8**.

c. Select the type of **Parity** for the error detecting procedure. By default, it is set to **None**. The available parity types are **Even**, **Odd**, **Mark**, and **Space**.

d. Select the **Stop Bits** value. By default, it is 1. In serial communications, a stop bit is an extra bit transmitted after each unit of information (usually a byte) to indicate that transmission of that unit is complete.

15. If you select a **TCP/IP Connection** port,

a. Type the **TCP/IP IP-Address or Node name** of the computer where the loop is connected. The corresponding **Port No.** is displayed.

16. If you select a **TCP/IP Encrypted Connection** port,

a. Type the **TCP/IP IP-Address or Node name** and the **Encryption Password** of the computer where the loop is connected. The corresponding **Port No.** is displayed.

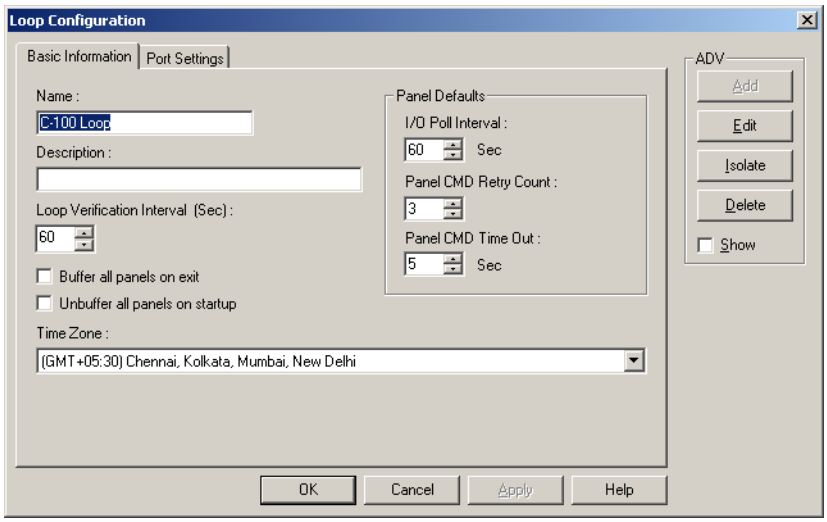
17. Click **Next** to display the **C-100 Loop Configuration - Finish** dialog box.
18. Click **Finish** to add the C-100 panel loop and return to the **Device** window.

The corresponding loop icon is displayed for the panel loop in the **Device** tree structure. For the communication port loop the  icon is displayed. For the TCP/IP port loop the  icon is displayed.

Editing a C-100 Panel Loop

To edit a C-100 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the C-100 loop and click **Configure**. The **Loop Configuration** dialog box appears.



4. Configure the loop using the Basic Information and Port Settings tabs.

Refer to the "Adding a C-100 Panel Loop" section in this chapter for configuring C-100 panel loop.

5. Click **OK** to configure the loop.

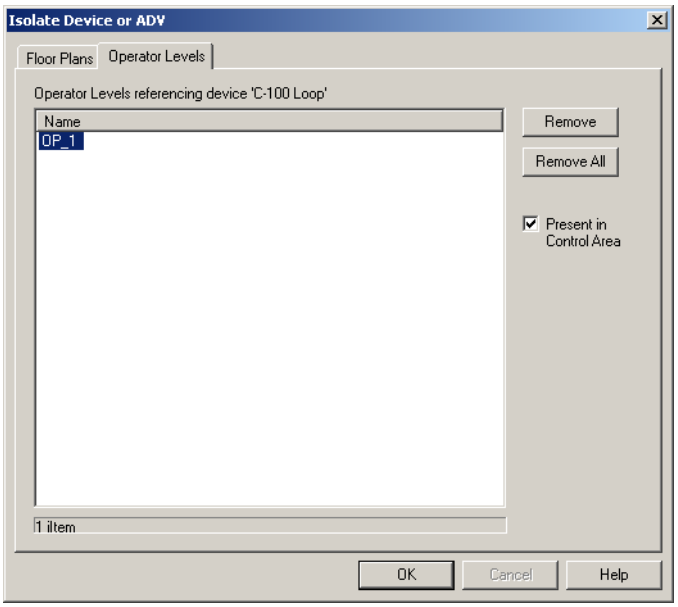
Isolating and Deleting a C-100 Panel Loop

You cannot delete a C-100 panel loop, until you delete the panels attached to it and remove all references to the C-100 Panel Loop from floor plans and operator levels.

Isolating a C-100 panel loop

To isolate a C-100 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the C-100 panel loop and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



3. To isolate floor plans from an ADV of C-100 panel loop:
   a. Click the **Floor Plans** tab. The floor plans associated to the C-100 panel loop are listed.
   b. Select the floor plans to be isolated from the C-100 panel loop and click **Remove**. The selected floor plans are dissociated from the C-100 loop.

      OR

      Click **Remove all** to isolate floor plans from the panel loop.
4. To isolate operator levels from an ADV of C-100 panel loop:
   a. Click the **Operator Levels** tab. The operator levels associated to the C-100 panel loop are listed.
   b. Select the operator levels to be isolated from the C-100 panel loop and click **Remove**. The selected operator levels are dissociated.

      OR

      Click **Remove all** to isolate all the operator levels from the panel loop.
   c. To remove the panel loop from the control area, clear the presence of an ADV of C-100 panel loop in the control area by clearing the **Present in Control Area** check box.
5. Click **OK**.

Deleting a C-100 panel loop

After deleting the panels attached to a panel loop and isolating the associated floor plans and operator levels, you can delete the C-100 panel loop.

To delete a C-100 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the C-100 panel loop and click **Delete**. A message asking for confirmation appears for deleting the panel loop.
4. Click **OK** to delete. The C-100 panel loop is deleted from the device map.

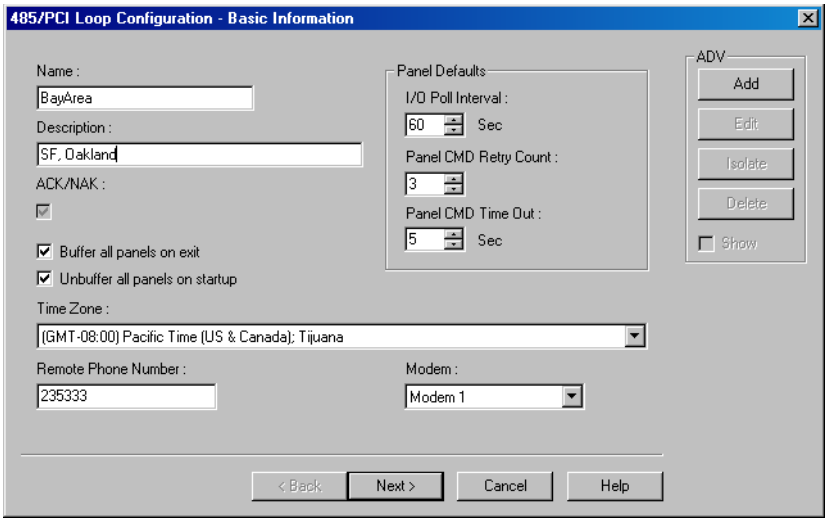
485/PCI Panel Loop

Panels using the RS-485 communication protocol can be connected to the WIN-PAK system by the N-485-PCI-2 communication adaptor. The 485 communication protocol offers better data supervision and increased system performance compared to the 20-milliamp communication protocol. A 485 PCI (with or without ACK/NAK) connection is defined by adding it to the Device Map.

Adding a 485/PCI Panel Loop

To add a 485/PCI panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder, right-click the communication server and then click **Panel Loop** dialog box appears.



3. Type a unique **Name** for the 485/PCI panel loop. This field is mandatory.
4. Type a **Description** of the 485/PCI panel loop.
5. Create an ADV for the 485/PCI panel loop. Click **Add** under **ADV** to display the **Abstract Device Record - Server** dialog box.

Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

6. After adding an ADV, click **OK** to return to the **Communication Server Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Click the **Show** check box to view the ADV details.

7. Select the **ACK/NAK** check box, if you are using a ACK/NAK protocol. ACK/NAK protocol requires acknowledgement, which can be positive (ack) or negative (nak). ACK indicates a successful message receipt, while nak indicates an invalid message.
8. Select **Buffer all panels on exit** to buffer the events in the respective panels when the communication server stops.
9. Select **Unbuffer all panels on startup** to unbuffer all the panel events when the communication server restarts.
10. Select the standard **Time Zone** based on the loop location.
11. Set the **Panel Defaults** for the panel loop.
    a. **I/O Poll Interval**: Select the interval at which the signal must be sent to the panel to verify the communication and check the panel's input and output states. By default, the frequency interval is 60 seconds.
    b. **Panel CMD Retry Count**: Specify the number of times a command must be resent to the panel, if the event of the panel not responding to the command. By default, the command is resent 3 times.
    c. **Panel CMD Time Out**: Specify the waiting time for receiving a response from the panel and for time out of the command. By default, the loop waits for 5 seconds.
12. Click **Next** to set the port for the loop.
13. In the **Port** list, select a port of the communication server to which the loop is to be connected. The ports that are selected for the communication server and not used for other loops are listed.
14. If you select a port,
    a. Select the transmission baud rate for the loop in **Bits per second**.
    b. Select the number of bytes that can be transferred in **Data Bits**. Select a number between 4 and 8. By default, it is set to **8**.
    c. Select the type of **Parity** for error detecting procedure. By default, it is set to **None**. The available parity types are **Even, Odd, Mark,** and **Space**.

d. Select the **Stop Bits** value. By default, it is 1. In serial communications, a stop bit is an extra bit transmitted after each unit of information (usually a byte) to indicate that transmission of that unit is complete.

15. If you select the **TCP/IP Connection** port,

    a. Type the **TCP/IP IP-Address or Node name** of the computer where the 485/PCI loop is configured. The corresponding port number is displayed in **Port No**.

16. If you select the **TCP/IP Encrypted Connection** port,

    a. Type the **TCP/IP IP-Address or Node name** and the **Encryption Password** of the computer where the 485/PCI loop is configured. The corresponding port number is displayed in **Port No**.

17. Click **Next** to display the **485/PCI Loop Configuration - Finish** dialog box.

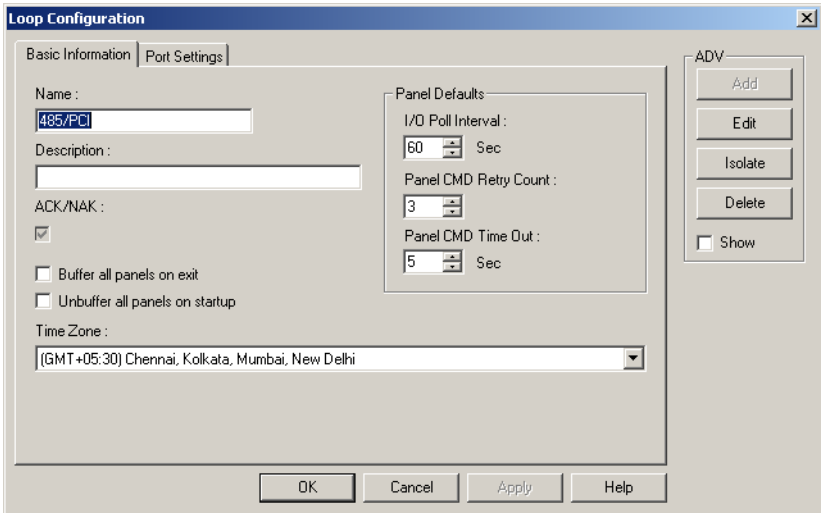
18. Click **Finish** to add the 485/PCI panel loop and return to the **Device** window.

    The corresponding loop icon is displayed for the panel loop in the **Device** tree structure. For the communication port loop the  icon is displayed. For the TCP/IP port loop the  icon displayed.

Editing a 485/PCI Panel Loop

To edit a 485/PCI panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the 485/PCI loop and click **Configure**. The **Loop Configuration** dialog box appears.



4. Configure the loop using the Basic Information and Port Settings tabs.

Refer to the "Adding a 485/PCI Panel Loop" section in this chapter for configuring 485/PCI panel loop.

5. Click **OK** to save the changes.

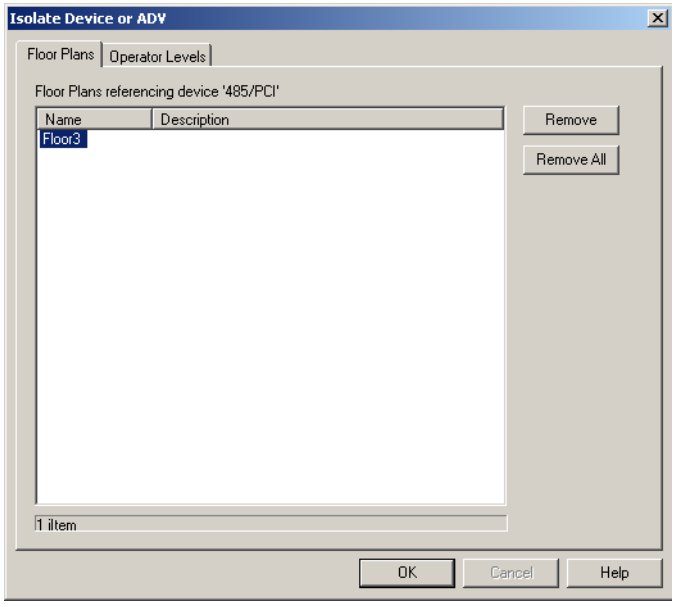
Isolating and Deleting a 485/PCI Panel Loop

You cannot delete a 485/PCI panel loop, until you delete the panels attached to it and remove all references to the 485/PCI panel loop from floor plans and operator levels.

Isolating a 485/PCI panel loop

To isolate 485/PCI panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the 485/PCI panel loop and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate floor plans from an ADV of 485/PCI panel loop:
   a. Click the **Floor Plans** tab. The floor plans associated to the 485/PCI panel loop are listed.
   b. Select the floor plans to be isolated from the 485/PCI panel loop and click **Remove**. The selected floor plans are dissociated.

      OR

      Click **Remove all** to isolate all the floor plans from the panel loop.
5. To isolate operator levels from an ADV of 485/PCI panel loop:

a. Click the **Operator Levels** tab. The operator levels associated to the 485/PCI panel loop are listed.

b. Select the operator levels to be isolated from the 485/PCI panel loop and click **Remove**. The selected operator levels are dissociated.

   OR

   Click **Remove all** to isolate all the operator levels from the loop.

c. To remove the panel loop from the control area, clear the presence of an ADV of 485/PCI panel loop in the control area by clearing the **Present in Control Area** check box.

6. Click **OK**.

Deleting a 485/PCI panel loop

After deleting the panel attached to it and isolating the assiocated floor plans and operator levels, you can delete the 485/PCI panel loop.

To delete a 485/PCI panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the 485/PCI panel loop and click **Delete**. A message asking for confirmation appears for deleting the panel loop.
4. Click **OK** to delete. The 485/PCI panel loop is deleted from the device map.

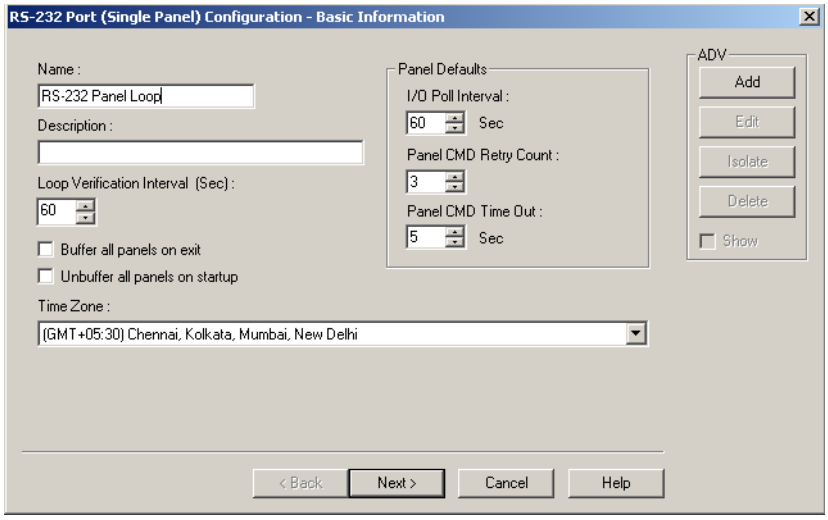
RS-232 Panel Loop

The RS-232 loop is an interface between the computer or communication server and a panel using serial binary data interchange.

Adding an RS-232 Panel Loop

To add an RS-232 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the communication server and click **RS-232 Port (Single Panel)**. The **RS-232 Port (Single Panel) Configuration - Basic Information** dialog box appears.



4. Type a unique **Name** for the panel. This field is mandatory.
5. Type a **Description** of the panel.
6. Create an ADV for the RS-323 loop. Click **Add** under **ADV** to display the **Abstract Device Record - Server** dialog box.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
7. After adding an ADV, click **OK** to return to the **RS-232 Port (Single Panel) Configuration** dialog box.

Notes:

- Under **ADV**, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate, and delete the ADV.
- Select the **Show** check box to view the ADV details.

8. Increase or decrease the **Loop Verification Interval (Sec)** to verify whether the loop is responding when a signal is send from WIN-PAK to the C-100 loop.

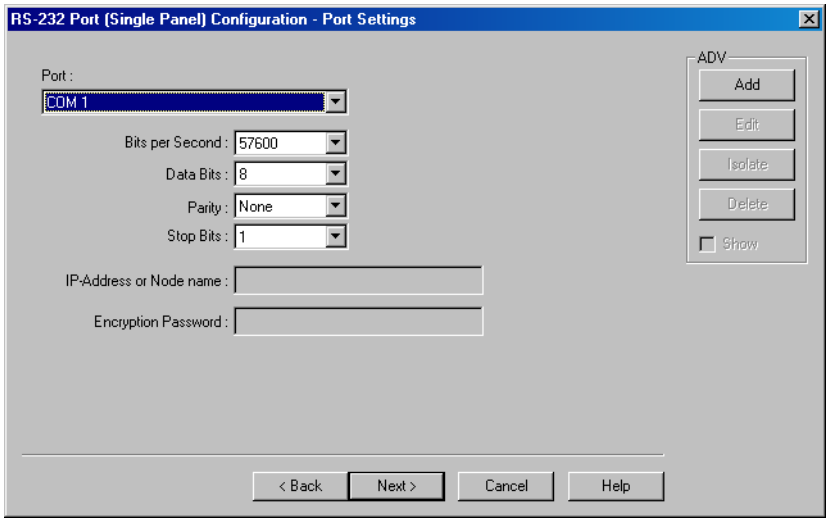
   Increasing the interval improves the bandwidth. The default interval is set to 60 seconds as it is an optimal value.
9. Select **Buffer all panels on exit** to buffer the events in all the panels when the communication server stops.
10. Select **Unbuffer all panels on startup** to automatically unbuffer all panel events to WIN-PAK when the communication server restarts.
11. Select the standard **Time Zone** based on the loop location.
12. Set the **Panel Defaults** for the panel loop.

a. **I/O Poll Interval**: Select the interval at which the signal must be sent to the panel to verify the communication and check the panel's input and output states. By default, the frequency interval is 60 seconds.

b. **Panel CMD Retry Count**: Specify the number of times a command must be resent to the panel, if the event of the panel is not responding to the command. By default, the command is resent 3 times.

c. **Panel CMD Time Out**: Specify the waiting time for receiving a response from the panel and for time out the command. By default, the loop waits for 5 seconds.

13. Click **Next** to set the port for the loop.



14. In the **Port** list, select a port of the communication server to which the loop is to be connected. The ports that are selected for the communication server and not used for other loops are listed.

15. If you select a port,

a. Select the transmission baud rate for the loop in **Bits per second**.

b. Select the number of bytes that can be transferred in **Data Bits**. Select a number between 4 and 8. By default, it is set to **8**.

c. Select the type of **Parity** for the error detecting procedure. By default, it is set to **None**. The available parity types are **Even, Odd, Mark**, and **Space**.

d. Select the **Stop Bits** value. By default, it is 1. In serial communications, a stop bit is an extra bit transmitted after each unit of information (usually a byte) to indicate that transmission of that unit is complete.

16. If you select **TCP/IP Connection** port,

a. Type the **TCP/IP IP-Address or Node name** of the computer where the panel is connected. The corresponding **Port No.** is displayed.

17. If you select **TCP/IP Encrypted Connection** port,

a. Type the **TCP/IP IP-Address or Node name** and the **Encryption Password** of the computer where the panel is connected. The corresponding **Port No.** is displayed.

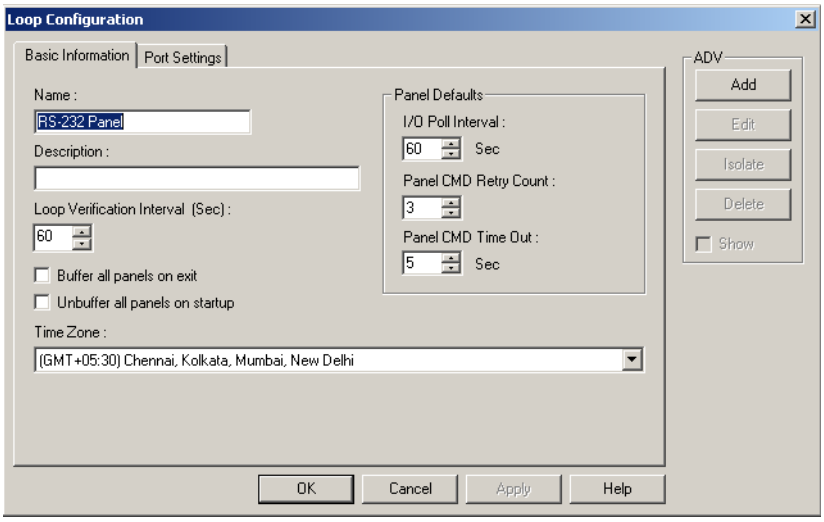
18. Click **Next** to display the **Finish** dialog box.
19. Click **Finish** to add the RS-232 panel loop and return to the **Device** window.

The corresponding loop icon is displayed for the panel loop in the **Device** tree structure. For the communication port loop the icon is displayed. For the TCP/IP port loop the icon is displayed.

Editing an RS-232 Panel Loop

To edit an RS-232 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the RS-232 loop and click **Configure**. The **Loop Configuration** dialog box appears.



4. Configure the loop using the Basic Information and Port Settings tabs.

   Refer to the "Adding an RS-232 Panel Loop" section in this chapter for configuring the RS-232 panel loop.

5. Click **OK** to save the changes.

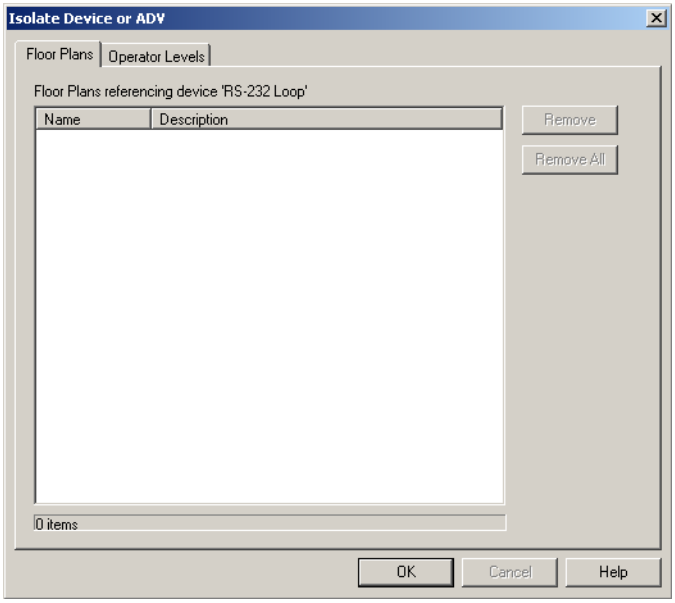
Isolating and Deleting an RS-232 Panel Loop

You cannot delete an RS-232 panel loop, until you delete the panels attached to it and remove all the references to the RS-232 panel loop from floor plans and operator levels.

Isolating an RS-232 panel loop

To isolate RS-232 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the RS-232 panel loop and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



3. To isolate floor plans from an ADV of RS-232 panel loop:
   a. Click the **Floor Plans** tab. The list of floor plans associated to the RS-232 panel loop is displayed.
   b. Select the floor plans to be isolated from the RS-232 panel loop and click **Remove**. The selected floor plans are dissociated.

      OR

      Click **Remove all** to isolate all the floor plans from the panel loop.
4. To isolate operator levels from an ADV of RS-232 panel loop:
   a. Click the **Operator Levels** tab. The list of operator levels associated to the 485/PCI panel loop is displayed.
   b. Select the operator levels to be isolated from the RS-232 panel loop and click **Remove**. The selected operator levels are dissociated.

      OR

      Click **Remove all** to isolate all the operator levels from the panel loop.
   c. To remove the panel loop from the control area, clear the presence of an ADV of RS-232 panel loop in the control area by clearing the **Present in Control Area** check box.
5. Click **OK**.

Deleting an RS-232 panel loop

After deleting the panels attached to the panel loop and isolating the assiocated floor plans and operator levels, you can delete the RS-232 panel loop.

To delete an RS-232 panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the RS-232 panel loop and click **Delete**. A message asking for confirmation appears for deleting the panel loop.
3. Click **OK** to delete. The RS-232 panel loop is deleted from the device map.

P-Series Panel Loop

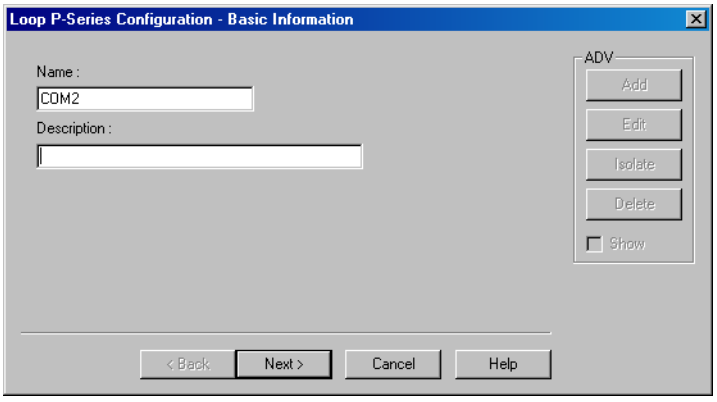
A P-Series panel loop represents a configuration of more than one P-Series Intelligent Controller panel board. A loop requires only one com port on a communication server, and there can be up to eight Intelligent Controllers per loop, and up to 32 SIO Boards per Intelligent Controller.

Note: Be aware, when using a panel loop, that the traffic on the com port increases with each Intelligent Controller and SIO Board added to the loop.

Adding a P-Series Panel Loop

To add a P-Series panel loop:

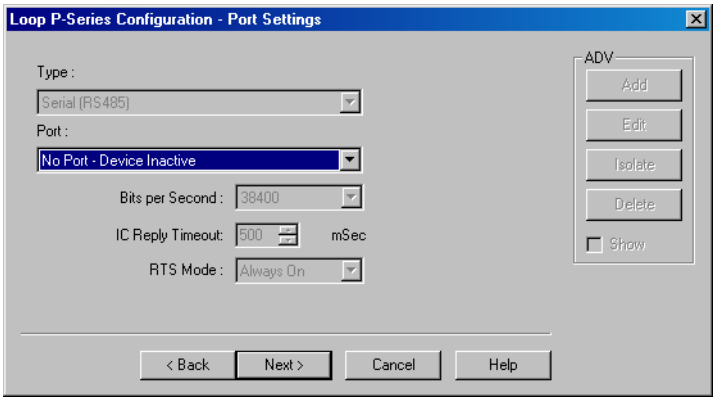
1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and then right-click the communication server and click **Panel Loop (P-Series)**. The **Loop P-Series Configuration - Basic Information** dialog box appears.



3. Type a unique **Name** for the P-Series panel loop. This field is mandatory.
4. Type a **Description** of the panel loop.

Note: An ADV cannot be created for the P-Series panel loops, as the panel is directly connected to the WIN-PAK system.

5. Click **Next** to include port details.



In the **Type** list, **Serial (RS485)** is displayed by default. When you establish a PRO-2200 panel loop, the only applicable type is RS485.

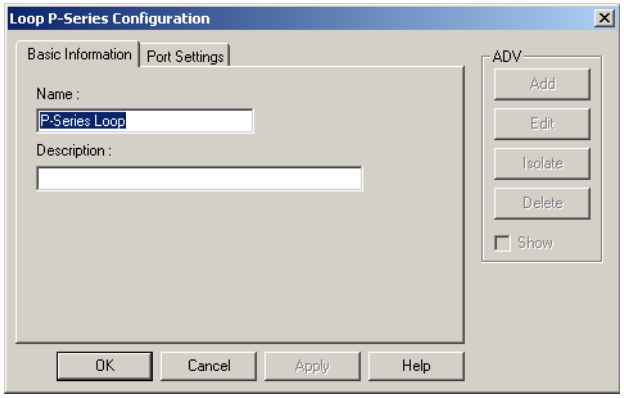
6. In the **Port** list, select a port of the communication server to which the loop is to be connected. The ports that are added to the communication server and are not used by any other device are listed.
7. Enter the following port details:
   - **Bits per Second**: The transmission baud rate of the communication port. The default baud rate is 38400. It can be set to 9600 or 19200 when the RS-485 communication port is used.
   - **IC Reply Timeout**: The duration the Host PC waits for an acknowledgment after it has sent an outgoing packet. If acknowledgment is not received within the specified time, the Host PC re-sends the packet. The host retries according to the Host Retry Count set in the panel.
   - **RTS Mode**: The Request to Send mode that enables the host PC to know that the Intelligent Controller is ready to send information. The RTS Mode defaults to **Always On**.

     The **Toggle** RTS Mode applies when there is an RS-485 to RS-232 converter that requires a handshake. The RS-485 converter needs to know when it is sending and when it is receiving. Toggle enables you to control the direction on an external converter. The converter specified by Honeywell Access Systems has handshaking turned off and therefore, do not set the RTS Mode to Toggle.
8. Click **Next** to display the **Loop P-Series Configuration - Finish** dialog box.
9. Click **Finish** to add a P-Series panel loop.

Editing a P-Series Panel Loop

To edit a P-series panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the P-series loop and click **Configure**. The **Loop P-Series Configuration** dialog box appears.



4. Configure the loop using the Basic Information and Port Settings tabs.

   Refer to the "Adding a P-Series Panel Loop" section in this chapter for configuring P-series panel loop.

5. Click **OK** to configure the loop.

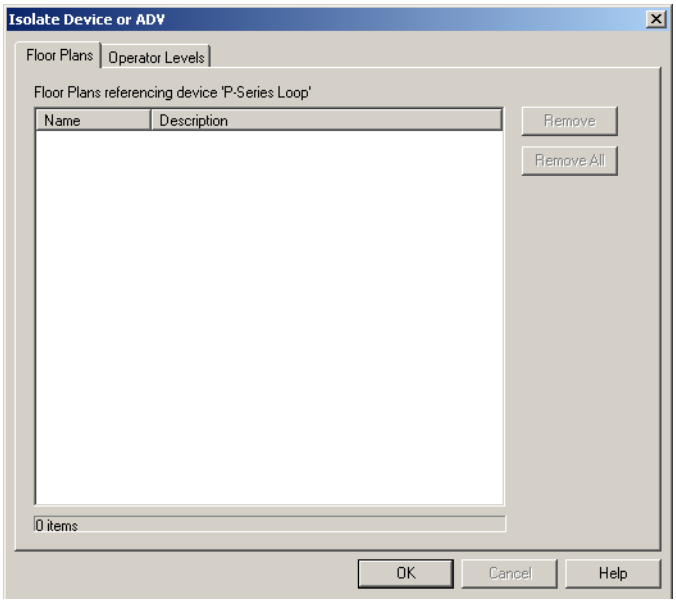
Isolating and Deleting a P-Series Panel Loop

You cannot delete a P-Series panel loop, until you delete the P-series panels attached to it and remove all the references of a P-series panel loop from floor plans and operator levels.

Isolating a P-series panel loop

To isolate a P-series panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the P-series panel loop and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



3. To isolate floor plans from an ADV of P-series panel loop:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the P-series panel loop is displayed.
    b. Select the floor plans to be isolated from the P-series panel loop and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the panel loop.
4. To isolate operator levels from an ADV of P-series panel loop:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the P-series panel loop is displayed.
    b. Select the operator levels to be isolated from the P-series panel loop and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the panel loop.
    c. To remove the P-series panel loop from the control area, clear the presence of an ADV of P-series panel loop in the control area by clearing the **Present in Control Area** check box.
5. Click **OK**.

Deleting a P-series panel loop

After deleting the panels attached to the panel loop and isolating the assiocated floor plans and operator levels, you can delete the P-series panel loop.

To delete a P-series panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the P-series panel loop and click **Delete**. A message asking for confirmation appears for deleting the panel loop.
3. Click **OK** to delete. The P-series panel loop is deleted from the device map.

Modem Pools

Modem can be used for enabling the communication between panel loops at remote sites. Modems are defined in the modem pool and then added to the communication loop. Modems enable communication between WIN-PAK User Interface and panels. The C-100, 485 with a HUB (non ACK/NAK), 485 with a HUB (ACK/NAK), and P-Series panel loops can communicate to the modems. The procedure for configuring these panel loops is similar to the procedure for configuring local panel loops.

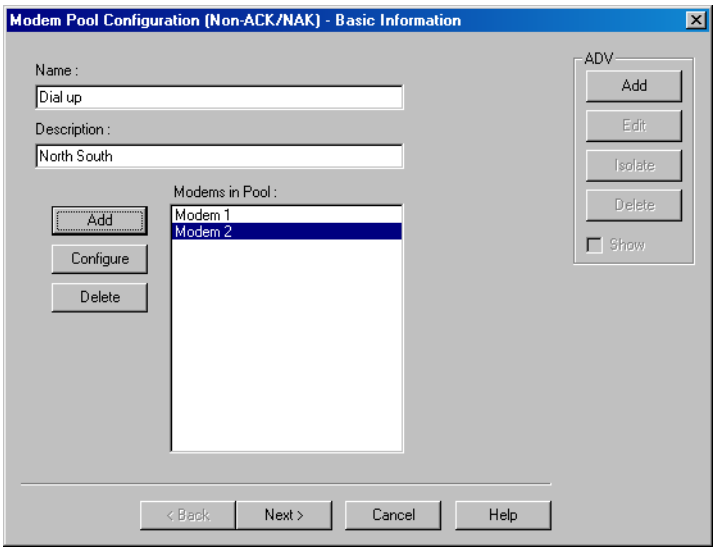
Modem pools are defined by adding them to the Device Map. You must have a communication server with an available com port for each modem. Once the pool is defined, the panel loops are added to the modem pool, rather than adding them directly to the communication server, as is the case with local loops.

Note: Any modem that is supported by the Windows operating system can be used for panel communication.

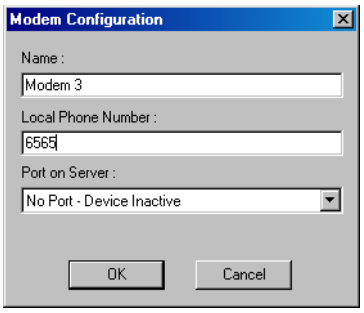
Adding a Modem Pool

To add a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click communication server and select the type of modem pool connection. The **Modem Pool Configuration - Basic Information** dialog box for the selected modem pool type appears.



4. Type a unique **Name** for the modem pool. This field is mandatory.
5. Enter a **Description** for the modem pool.
6. Click **Add** on the left of the dialog box to add the modems to the pool. The **Modem Configuration** dialog box appears.



7. Type a unique Modem **Name** and the **Local Phone Number** for the modem. These fields are mandatory.
8. In the **Port on Server** list, select the port on the communication server to which the modem must be connected. The list of ports on the communication server and are not used in any modem pool or loop is displayed.

Note: You cannot add a modem to a modem pool without having a specific port to the modem. However, you can define a modem pool without adding a modem to it and you can add modems later.

9. Click **OK** to close the **Modem Configuration** dialog box and return to **Modem Pool Configuration** dialog box.
10. Create an ADV for the modem pool. Click **Add** under **ADV**, enter the ADV properties and click **OK**.

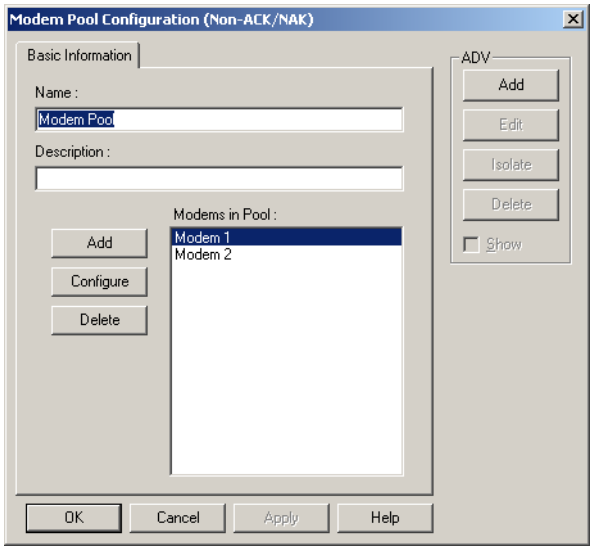
    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

11. Click **Next** and in the next dialog box click **Finish**. The modem pool is added to the Communication Server.

Editing a Modem Pool

To edit a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the modem pool (ACK/NAK or non ACK/NCK) and click **Configure**. The **Modem Pool Configuration** dialog box appears for the ACK/NAK or non-ACK/NAK modem pool.



3. Configure the modem pool using the **Basic Information** tab. You can also add, edit, or delete the modems to the modem pool.

   Refer to the "Adding a Modem Pool" section in this chapter for configuring modem pool.

4. Click **OK** to configure a modem.

Isolating and Deleting a Modem Pool

You cannot delete a modem pool, until you delete the loops added to it and remove all the references of the modem pool ADV from floor plans and operator levels.

Isolating a Modem Pool

To isolate a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the modem pool and click **Isolate**. The **Isolate Device or ADV** dialog box appears.

4. To isolate floor plans from a modem pool ADV:
    a. Click the **Floor Plans** tab. The floor plans associated to the modem pool are listed.
    b. Select the floor plans to be isolated from the modem pool and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the modem pool.
5. To isolate operator levels from a modem pool ADV:
    a. Click the **Operator Levels** tab. The operator levels associated to the modem pool are listed.
    b. Select the operator levels to be isolated from the modem pool and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the modem pool.
    c. To remove the modem pool from the control area, clear the presence of an ADV of the modem pool in the control area by clearing the **Present in Control Area** check box.
6. Click **OK**.

Deleting a Modem Pool

After isolating the panel loops attached to the modem and the associated floor plans and operator levels, you can delete the modem pool.

To delete a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the modem pool and click **Delete**. A message asking for confirmation appears.
4. Click **OK** to confirm the deletion. The modem pool is deleted from the device map.

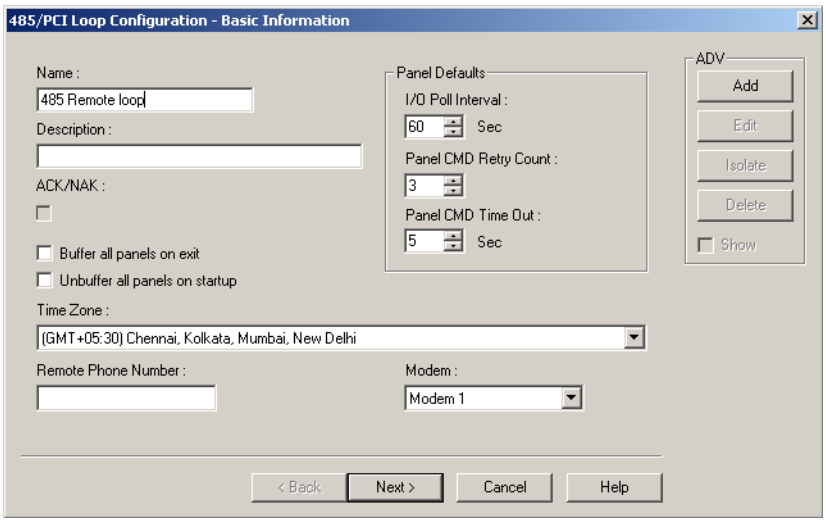
C-100 or 485 (non-ACK/NAK) Remote Communication Loop

You can add C-100 or 485 (non-ACK/NAK) remote communication loops only to the modem pools defined as non-ACK/NAK hub.

Adding a C-100 or 485 (non-ACK/NAK) Remote Communication Loop

To add a C-100 loop or 485 (non-ACK/NAK) to a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server.
3. Right-click the non-ACK/NAK modem pool and click **Add New C-100 Loop** or **Add New 485 Loop**. The **Loop Configuration - Basic Information** dialog box appears for the selected loop type (C-100 or 485/PCI).



4. Type a unique **Name** of the remote communication loop. This field is mandatory.
5. Type a **Description** for the C-100 or 485 (non-ACK/NAK) loop.
6. Create an ADV for the communication loop. (Click **Add** under **ADV**, set the ADV properties and click **OK**.)

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

   Note: The ACK/NAK box appears disabled. You cannot select this check box, as you are adding the non-ACK/NAK loop.

7. Increase or decrease the **Loop Verification Interval (Sec)** to verify whether the loop is responding to a signal that is sent from WIN-PAK to the C-100 loop or 485/PCI panel loop.

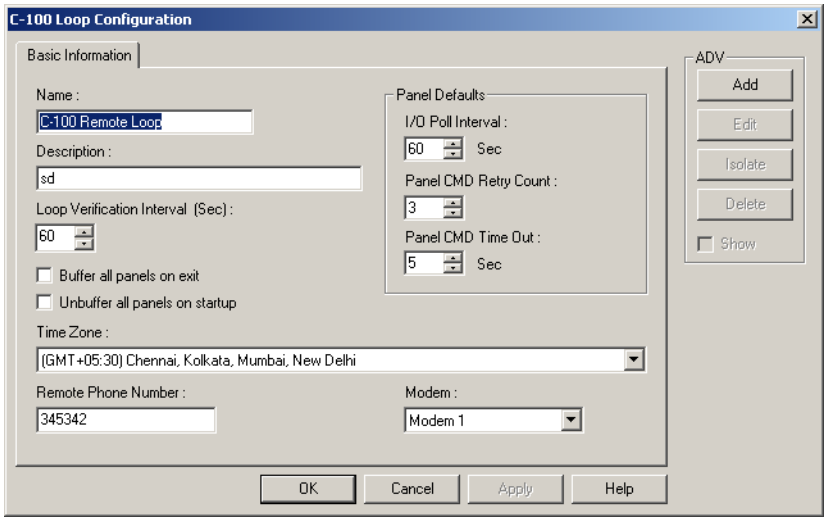
Note: Increasing the interval improves the bandwidth. The default interval is set to 60 seconds as it is an optimal value.

8. Select **Buffer all panels on exit** to buffer the events on all the panels when the communication server stops.
9. Select **Unbuffer all panels on startup** to unbuffer all panel events when the communication server restarts.
10. Select the standard **Time Zone** based on the loop location.
11. Set the **Panel Defaults** for the remote communication loop.
    a. **I/O Poll Interval**: Select the interval at which the signal must be sent to the panel to verify the communication and check the panel's input and output states. By default, the frequency interval is 60 seconds.
    b. **Panel CMD Retry Count**: Specify the number of times a command must be resent to the panel, if the panel event is not responding to the command. By default, the command is resent 3 times.
    c. **Panel CMD Time Out**: Specify the waiting time for receiving a response from the panel and for time out of the command. By default, the loop waits for 5 seconds.
12. In **Remote Phone Number,** type the phone number of the modem in the remote site. Include the area code and dialing prefix, if they are needed to dial in from the remote site like 3125551212. This field is mandatory.
13. Select the **Modem** of the remote site.
14. Click **Next** to display the **Finish** dialog box.
15. Click **Finish**. The C-100 or 485 (non-ACK/NAK) remote communication loop is added to the modem pool.

Editing a C-100 or 485 (non-ACK/NAK) Remote Communication Loop

To edit a non-ACK/NAK remote communication loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the C-100 or 485 non-ACK/NCK remote communication loop and click **Configure**. The **Loop Configuration** dialog box appears for the selected loop type.



4. Configure the loop using the Basic Information tab.

   Refer to the "Adding a C-100 or 485 (non-ACK/NAK) Remote Communication Loop" section in this chapter for configuring the non-ACK/NAK remote communication loop.

5. Click **OK** to configure the panel loop.

Isolating and Deleting a non-ACK/NAK Remote Communication Loop

You cannot delete a non-ACK/NAK remote communication loop, until you delete the panels attached to it and remove all the references of an ADV of a non-ACK/NAK remote communication loop from floor plans and operator levels.

Isolating a non-ACK/NAK remote communication loop

To isolate a non-ACK/NAK remote communication loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.
3. Right-click the non-ACK/NAK remote communication loop and click **Isolate**. The **Isolate Device or ADV** dialog box appears.
4. To isolate floor plans from an ADV of non-ACK/NAK remote communication loop:

   a. Click the **Floor Plans** tab. The list of floor plans associated to the non-ACK/NAK remote communication loop is displayed.

   b. Select the floor plans to be isolated from the non-ACK/NAK remote communication loop and click **Remove**. The selected floor plans are dissociated.

      OR

Click **Remove all** to isolate all the floor plans from the panel loop.

5. To isolate operator levels from an ADV of non-ACK/NAK remote communication loop:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the non-ACK/NAK remote communication loop is displayed.
    b. Select the operator levels to be isolated from the non-ACK/NAK remote communication loop and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the panel loop.
    c. To remove the panel loop from the control area, clear the presence of an ADV of non-ACK/NAK remote communication loop in the control area by clearing the **Present in Control Area** check box.
6. Click **OK**.

Deleting a non-ACK/NAK remote communication loop

After deleting the panels attached to the panel loops and isolating the associated floor plans and operator levels, you can delete the non-ACK/NAK remote communication loop.

To delete a non-ACK/NAK remote communication loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the non-ACK/NAK remote communication loop and click **Delete**. A message asking for confirmation appears.
3. Click **OK** to delete. The non-ACK/NAK remote communication loop is deleted from the device map.

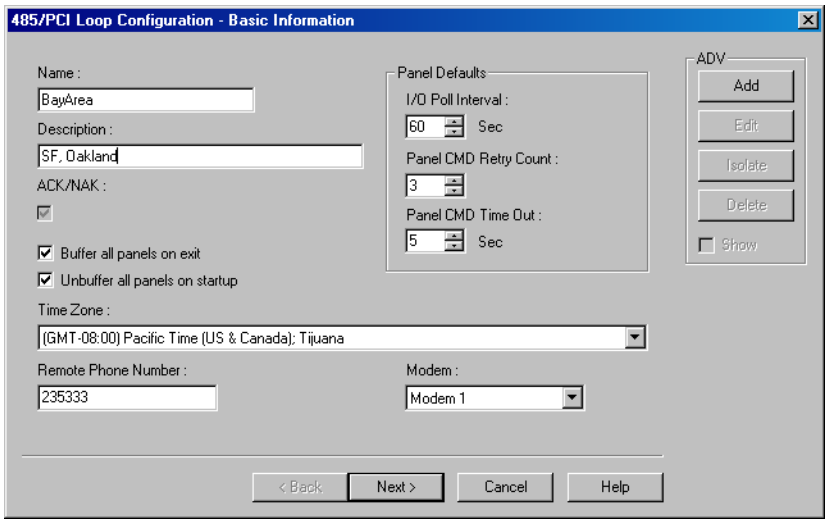
485 ACK-NAK Remote Communication Loop

You can add a 485 ACK-NAK remote communication loop only to a modem pool with ACK-NAK Hub.

Adding a 485 ACK-NAK Remote Communication Loop

To add 485 remote connection (with ACK/NAK) to a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server.
3. Right-click the ACK/NAK modem pool and click **Add New 485 ACK/NAK Loop**. The **485/PCI Loop Configuration - Basic Information** dialog box for appears.



4. Type a unique **Name** of the remote communication loop. This field is mandatory.
5. Type the **Description** for the 485 (ACK/NAK) loop.
6. Create an ADV for your communication loop. (Click **Add** under **ADV**, set the ADV properties and click **OK**.)

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

   Note: The ACK/NAK check box is disabled. You cannot clear this check box, as you are adding the ACK/NAK loop.

7. Increase or decrease the **Loop Verification Interval (Sec)** to verify whether the loop is responding to a signal that is sent from WIN-PAK to the C-100 loop.

   Note: Increasing the interval improves the bandwidth. The default interval is set to 60 seconds as it is an optimal value.

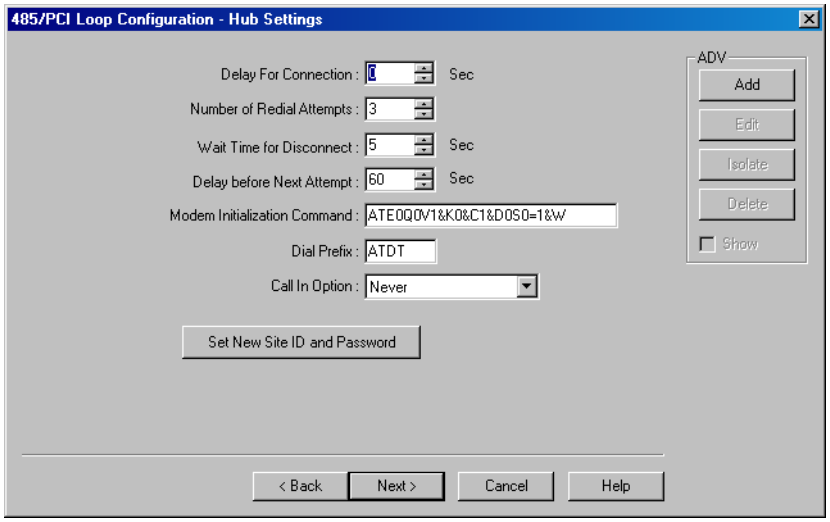
8. Select **Buffer all panels on exit** to buffer the events on all the panels when the communication server stops.
9. Select **Unbuffer all panels on startup** to unbuffer all panel events when the communication server restarts.
10. Select the standard **Time Zone** based on the loop location.
11. Set the **Panel Defaults** for the remote communication loop.
    a. **I/O Poll Interval**: Select the interval at which the signal must be sent to the panel to verify the communication and check the panel's input and output states. By default, the frequency interval is 60 seconds.
    b. **Panel CMD Retry Count**: Specify the number of times a command must be resent to the panel, if the panel event is not responding to the command. By default, the command is resent 3 times.

c. **Panel CMD Time Out**: Specify the waiting time for receiving a response from the panel and for time out of the command. By default, the loop waits for 5 seconds.

12. In **Remote Phone Number**, type the phone number of the modem in the remote site. Include the area code and dialing prefix, if they are needed to dial in from the remote site like 3125551212. This field is mandatory.

13. Select the **Modem** of the remote site.

14. Click **Next** to configure the hub settings. The **485/PCI Loop Configuration - Hub Settings** dialog box appears.



15. Set the following hub settings:

- **Delay for Connection**: The duration (in seconds) to pause between the dialing prefix and dialing phone number. Enter a number between 0 and 120 seconds.
- **Number of Redial Attempts**: The number of redial attempts to make. Enter a number between 0 and 50 times. The default is 3 times.
- **Wait Time for Disconnect**: The wait time allowed before disconnect. Enter a number between 1 and 999 seconds. The default is 5 seconds.
- **Delay before Next Attempt**: The wait time allowed between two dialings. Enter a number between 1 and 999 seconds. The default is 60 sec.
- **Modem Initialization String**: Enter the remote initialization string as: ATEØQØV1&KØ&C1&DØSØ+1&W.

  Refer to the modem documentation for further details.
- **Dial Prefix**: The command prefix for dial. In most cases it is ATDT, which is set as the default.
- **Call In Option**: Select the call in option as **On Invalid Transaction** or **Never** for the panel to dial-up in case an alarm is raised.

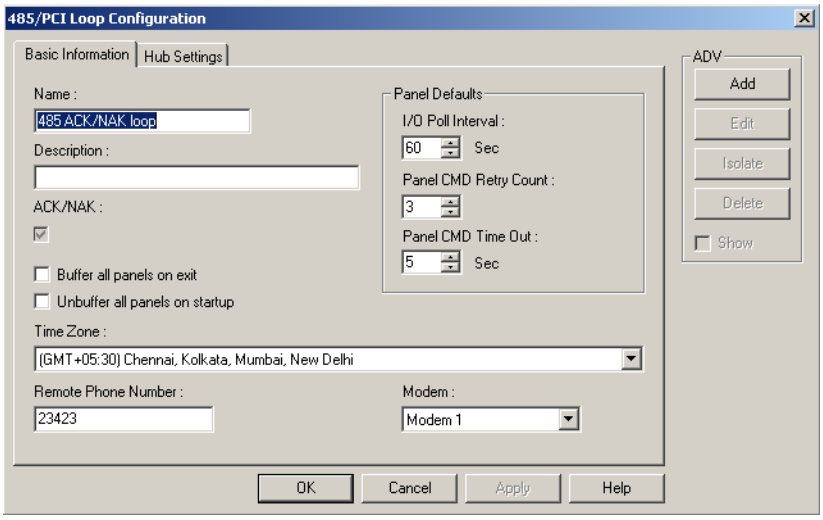
Note: Honeywell recommends to retain the default settings.

16. To set a new site ID and password, click **Set New Site ID and Password**. The **Site - Password** dialog box appears. The Site ID and password must be given while dialing-up the modem.
17. Type a **New Password**. This field is mandatory and it can be up to 20 characters.
18. Retype the password in **Confirm Password**.
19. In the **Site ID** field, enter the site ID in **@A** [unique 4-digit number for area], **S** [unique 4-digit number for site] format. For example **@A0002, S0003** is area 2 site 3.
20. Click **OK** to return to the **Hub Settings** dialog box.
21. Click **Next** and then click **Finish** in the next dialog box.

Editing a 485 ACK/NAK Remote Communication Loop

To edit a 485 ACK/NAK remote communication loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and communication server.
3. Right-click the 485 ACK/NAK remote communication loop and click **Configure**. The **485/PCI Loop Configuration** dialog box appears.



4. Configure the panel loop using Basic Information and Port Settings tabs.

   Refer to the "Adding a 485 ACK-NAK Remote Communication Loop" section in this chapter for configuring the 485 ACK/NAK remote communication loop.

5. Click **OK** to save the changes.

Isolating and Deleting a 485 ACK/NAK Remote Communication Loop

You cannot delete a 485 ACK/NAK remote communication loop, until you delete the panels attached to it and remove all the references of an ADV of a 485 ACK/NAK remote communication loop from floor plans and operator levels.

Isolating a 485 ACK/NAK remote communication loop

To isolate a 485 ACK/NAK remote communication loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the 485 ACK/NAK remote communication loop and click **Isolate**. The **Isolate Device or ADV** dialog box appears.
3. To isolate floor plans from an ADV of 485 ACK/NAK remote communication loop:
    a. Click the **Floor Plans** tab. The floor plans associated to the 485 ACK/NAK remote communication loop are listed.
    b. Select the floor plans to be isolated from the 485 ACK/NAK remote communication loop and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the panel loop.
4. To isolate operator levels from or an ADV of 485 ACK/NAK remote communication loop:
    a. Click the **Operator Levels** tab. The operator levels associated to the 485 ACK/NAK remote communication loop are listed.
    b. Select the operator levels to be isolated from the 485 ACK/NAK remote communication loop and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the panel loop.
    c. To remove the panel loop from the control area, clear the presence of an ADV of 485 ACK/NAK remote communication loop in the control area by clearing the **Present in Control Area** check box.
5. Click **OK**.

Deleting a 485 ACK/NAK remote communication loop

After deleting the panels in the panel loop and isolating the associated floor plans and operator levels, you can delete the 485 ACK/NAK remote communication loop.

To delete a 485 ACK/NAK remote communication loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the 485 ACK/NAK remote communication loop and click **Delete**. A message asking for confirmation appears for deleting the 485 ACK/NAK remote communication loop.
3. Click **OK** to delete. The 485 ACK/NAK remote communication loop is deleted from the device map.

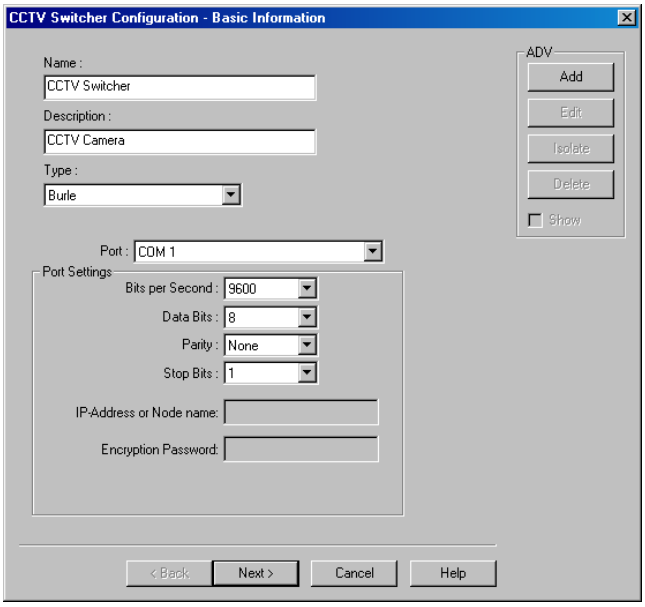
CCTV Switcher

In addition to the local or remote panel loops, CCTV networks can be connected to the WIN-PAK system using CCTV Switchers. A CCTV Switcher is defined by adding it to a communication server on the Device Map. You must have an available communication port for each Switcher.

Adding a CCTV Switcher

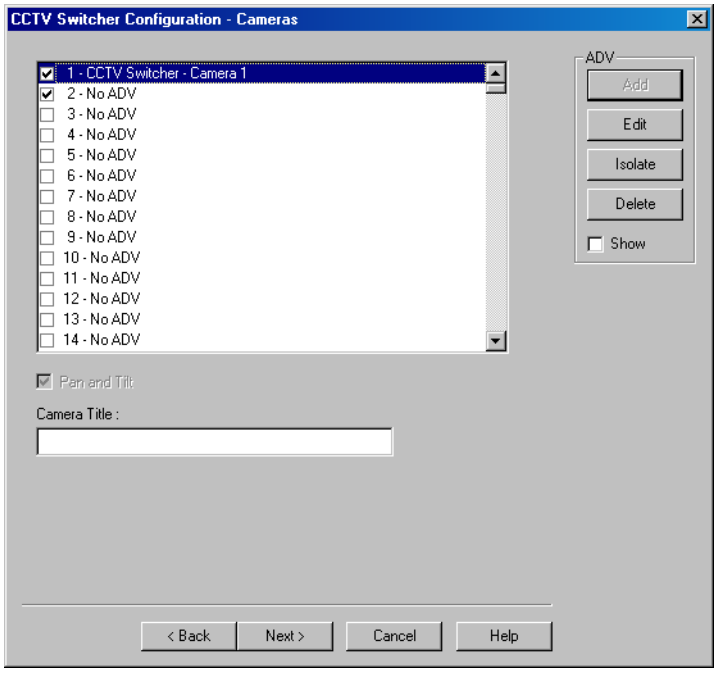
To add a CCTV Switcher:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder, right-click the communication server and click **CCTV Switcher**. The **CCTV Switcher Configuration - Basic Information** dialog box appears.

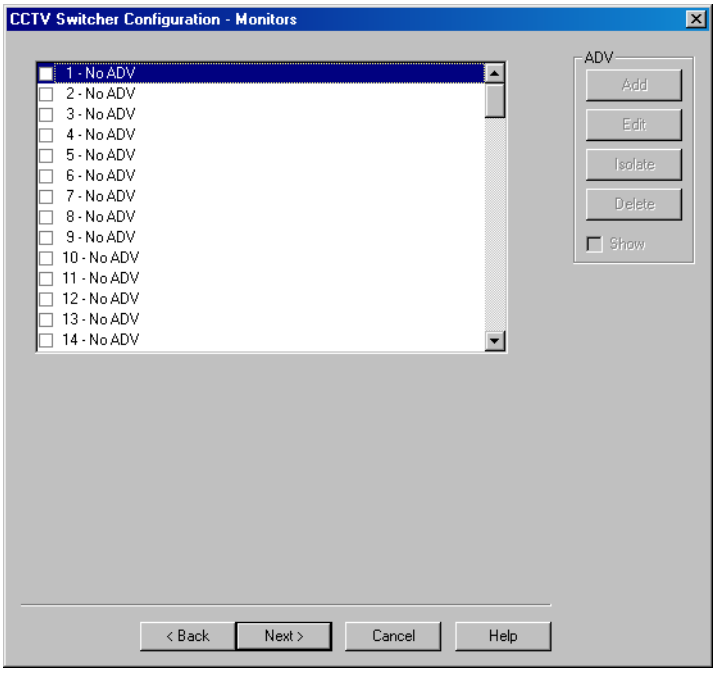


3. Type a **Name** for the CCTV switcher. This field is mandatory.

4. Type a **Description** for the CCTV switcher.
5. Select the manufacturer of the CCTV switcher in the **Type** list.
6. In the **Port** list, select a port of the communication server to which the CCTV Switcher is to be connected. The ports that are selected for the communication server and not used for other loops are listed.
7. If you select a port:
    a. Select the transmission baud rate for the switcher in **Bits per second**.
    b. Select the number of bytes that can be transferred in **Data Bits**. Select a number between 4 and 8. By default, it is set to **8**.
    c. Select the type of **Parity** for the error detecting procedure. By default, it is set to **None**. The available parity types are **Even**, **Odd**, **Mark** and **Space**.
    d. Select the **Stop Bits** value. By default, it is 1. In serial communications, a stop bit is an extra bit transmitted after each unit of information (usually a byte) to indicate that transmission of that unit is complete.
8. If you select a TCP/IP connection:
    a. Type the **TCP/IP IP-Address or Node name** of the computer where the CCTV switcher is connected. The corresponding **Port No.** is displayed.
9. If you select a TCP/IP encrypted connection:
    a. Type the **TCP/IP IP-Address or Node name** and the **Encryption Password** of the computer where the CCTV switcher is connected. The corresponding **Port No.** is displayed.
10. Click **Next** to configure cameras to the CCTV switcher. The **CCTV Switcher Configuration - Cameras** dialog box appears.



11. Select the check box to select the camera to be controlled by this switcher.
12. Type the **Camera Title** and create an **ADV** for the camera.
13. Click **Next** to configure the monitors of the CCTV switcher. The **CCTV Switcher Configuration - Monitors** dialog box appears.



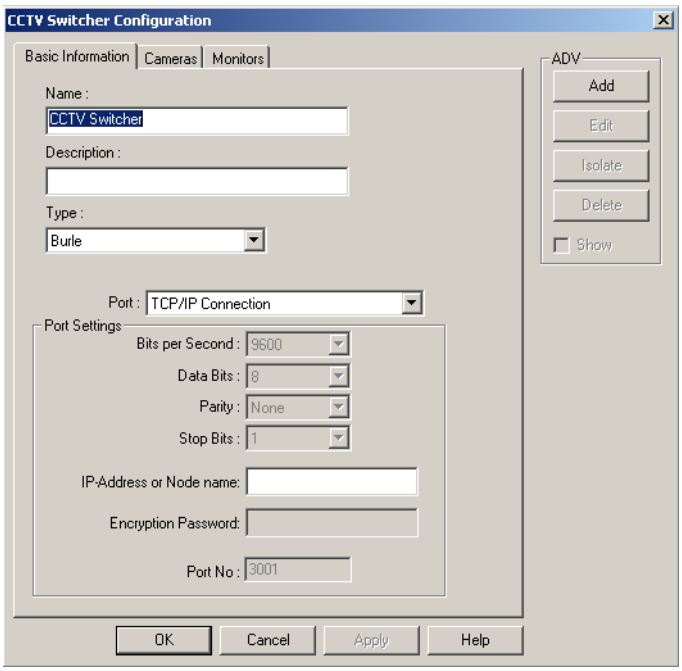
14. Select the check box to select the monitor to be controlled by this switcher.
15. Create an **ADV** for the monitor.

16. Click **Next** and in the next dialog box click **Finish**. The CCTV switcher is configured.

Editing a CCTV Switcher

To edit a CCTV switcher:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the CCTV switcher and click **Configure**. The **CCTV Switcher Configuration** dialog box appears.



3. Configure the CCTV Switcher using the Basic Information, Cameras, and Monitors tabs.

   Refer to the "Adding a CCTV Switcher" section in this chapter for configuring the CCTV switcher.

4. Click **OK** to save the changes.

Isolating and Deleting a CCTV Switcher

You cannot delete a CCTV switcher until you isolate CCTV switcher ADV from floor plans, operator levels, action groups, and ADVs.

Isolating a CCTV switcher

To isolate a CCTV switcher:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server.
3. Right-click the CCTV switcher and click **Isolate**. The **Isolate Device or ADV** dialog box appears.
4. To isolate floor plans from a CCTV switcher ADV:
    a. Click the **Floor Plans** tab. The floor plans associated to the CCTV switcher are listed.
    b. Select the floor plans to be isolated from the CCTV switcher and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the floor plans from the CCTV switcher.
5. To isolate operator levels from a CCTV switcher ADV:
    a. Click the **Operator Levels** tab. The operator levels associated to the CCTV switcher are listed.
    b. Select the operator levels to be isolated from the CCTV switcher and click **Remove**. The selected operator levels are dissociated.

       OR

       Click **Remove all** to isolate all the operator levels from the CCTV switcher.
    c. To remove the CCTV Switcher from the control area, clear the presence of a CCTV switcher ADV in the control area by clearing the **Present in Control Area** check box.
6. To isolate action group from a CCTV switcher ADV:
    a. Click the **Action Groups** tab. The action groups associated to the CCTV switcher are listed.
    b. Select the action groups to be isolated from the CCTV switcher and click **Remove**. The selected action groups are dissociated.

       OR

       Click **Remove all** to isolate all the action groups from the CCTV switcher.
7. To isolate ADV from a CCTV switcher ADV:
    a. Click the **Action Groups** tab. The ADVs associated to the CCTV switcher are listed.

b. Select the ADVs to be isolated from the CCTV switcher and click **Remove**. The selected ADVs are dissociated.

OR

Click **Remove all** to isolate all the ADVs from the CCTV switcher.

8. Click **OK**.

Deleting a CCTV switcher

Isolate the floor plans and operator levels associated to a CCTV switcher, before delete the CCTV switcher.

To delete a CCTV switcher:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server.
3. Right-click the CCTV switcher and click **Delete**. A message asking for confirmation appears.
4. Click **OK** to delete. The CCTV switcher is deleted from the device map.

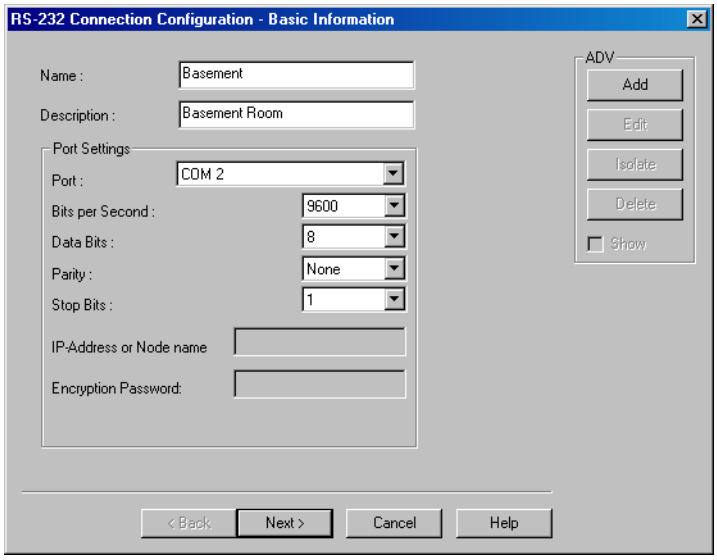
RS-232 Connection

RS-232 connection settings are used for the debugging purpose. An RS-232 connection is defined by adding it to the Device Map. The communication server must have a port available for each communication interface in your system.

Adding an RS-232 Connection

To add an RS-232 connection:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder, right-click the communication server and click **Add > RS-232 Connection**. The **RS-232 Connection Configuration - Basic Information** dialog box appears.



3. Type a **Name** for the RS-232 connection. This field is mandatory.
4. Type a **Description** for the RS-232 connection.
5. Under **Port Settings**, select a **Port** for the RS-232 Connection.
6. If you select a port,
    a. Select the transmission baud rate for the switcher in **Bits per second**.
    b. Select the number of bytes that can be transferred in **Data Bits**. Select a number between 4 and 8. By default, it is set to **8**.
    c. Select the type of **Parity** for the error detecting procedure. By default, it is set to **None**. The available parity types are **Even**, **Odd**, **Mark**, and **Space**.
    d. Select the **Stop Bits** value. By default, it is 1. In serial communications, a stop bit is an extra bit transmitted after each unit of information (usually a byte) to indicate that transmission of that unit is complete.
7. If you select a TCP/IP connection,
    a. Type the **TCP/IP IP-Address or Node name** of the computer where the RS-232 protocol is connected. The corresponding **Port No.** is displayed.
8. If you select a TCP/IP encrypted connection:
    a. Type the **TCP/IP IP-Address or Node name** and the **Encryption Password** of the computer where the RS-232 protocol is connected. The corresponding **Port No.** is displayed.
9. Create an ADV for the RS-232 Connection. Click **Add** under **ADV**, set the ADV properties and click **OK**.

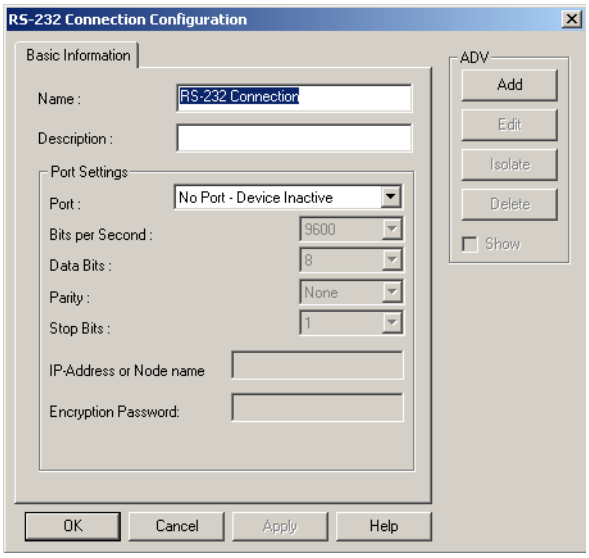
    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

10. Click **Next** and in the next dialog box click **Finish**. The RS-232 Connection is configured.

Editing an RS-232 Connection

To edit an RS-232 connection:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server.
3. Right-click the RS-232 connection and click **Configure**. The **RS-232 Connection Configuration** dialog box appears.



4. Configure the RS-232 connection using the Basic Information tab.

   Refer to the "Adding an RS-232 Connection" section in this chapter for configuring the RS-232 connection.

5. Click **OK** to save the changes.

Isolating and Deleting an RS-232 Connection

You cannot delete an RS-232 until you isolate RS-232 connection from floor plans and operator levels.

Isolating an RS-232 connection

To isolate an RS-232 connection:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the RS-232 connection and click **Isolate**. The **Isolate Device or ADV** dialog box appears.
3. To isolate floor plans from an ADV of RS-232 connection:

a. Click the **Floor Plans** tab. The list of floor plans associated to the RS-232 connection is displayed.

b. Select the floor plans to be isolated from the RS-232 connection and click **Remove**. The selected floor plans are dissociated.

OR

Click **Remove all** to isolate all the floor plans from the RS-232 connection.

4. To isolate operator levels from an ADV of RS-232 connection:

a. Click the **Operator Levels** tab. The list of operator levels associated to the RS-232 connection is displayed.

b. Select the operator levels to be isolated from the RS-232 connection and click **Remove**. The selected operator levels are dissociated.

OR

Click **Remove all** to isolate all the operator levels from the RS-232 connection.

c. To clear the presence of an ADV of RS-232 connection in the control area, clear the **Present in Control Area** check box.

5. Click **OK**.

Deleting an RS-232 Connection

Isolate the associated floor plans and operator levels from RS-232 connection to delete the RS-232 connection.

To delete an RS-232 connection:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server.
3. Right-click the RS-232 connection and click **Delete**. A message asking for confirmation appears for deleting the RS-232 connection.
4. Click **OK** to delete. The RS-232 connection is deleted from the device map.

Ethernet Module (Galaxy Panel)

Galaxy panel helps you to monitor and track intrusion happening at different zones in the access control system. Zones are areas monitored by a device in the galaxy panel. Galaxy panel is configured in the Galaxy Gold User Interface application and then downloaded to WIN-PAK. However, the virtual keypad provided on WIN-PAK enables you to configure certain features in the Galaxy panel.

Note: You must have a unique user name and password to operate on the virtual keypad.

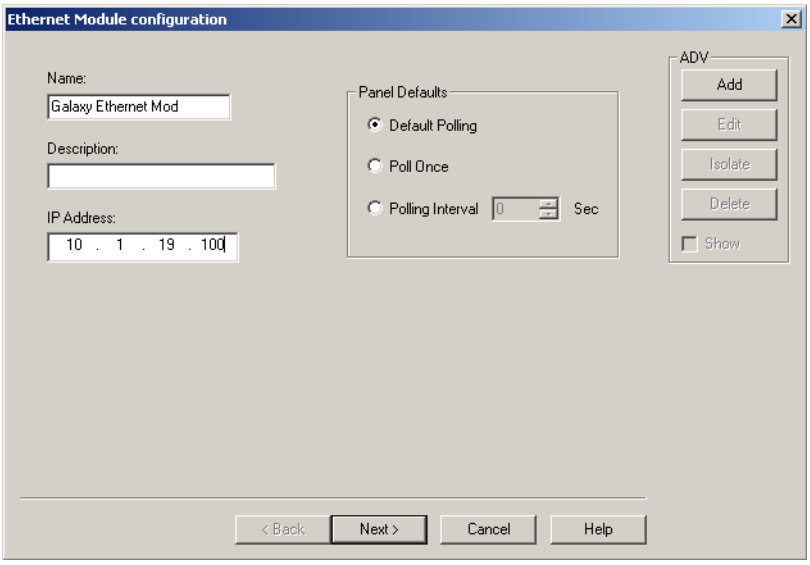
WIN-PAK communicates with the Galaxy panel through the Galaxy Ethernet module. Therefore, you must configure Galaxy Ethernet Module in the communication server

to add the Galaxy panel in WIN-PAK. When you add the galaxy panel, its connection with WIN-PAK is established and the panel configuration details are downloaded to WIN-PAK.

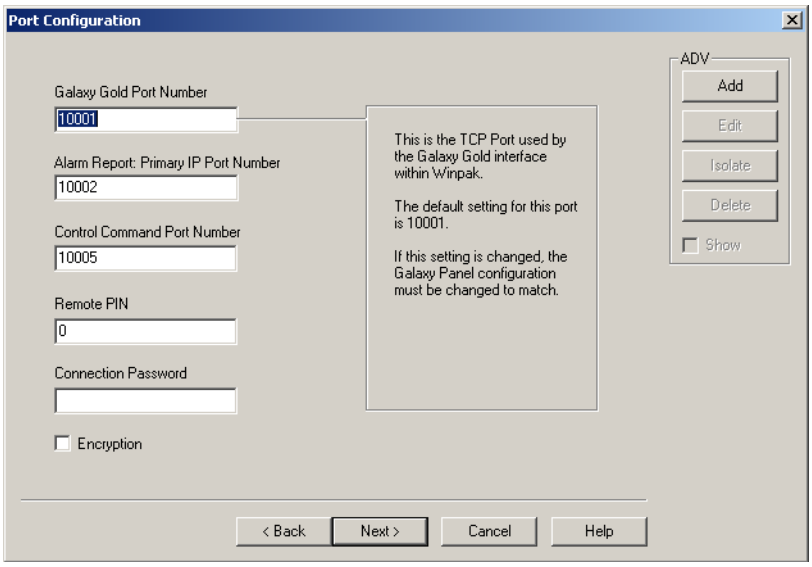
Adding a Galaxy Ethernet Module

To add a galaxy Ethernet module:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the communication server and choose **Add > Ethernet Module (Galaxy Single Panel)**. The **Ethernet Module configuration** dialog box appears.



3. Type a **Name** and a **Description** for the Ethernet module.
4. Type the **IP address** of the Galaxy Panel. This field is mandatory.
5. Under **Panel Defaults**, select the frequency at which the Galaxy panel is polled to know the status of the panel. The available polling options are:
    a. **Default Polling**: Select this option to poll continuously at the interval of 2 seconds.
    b. **Poll Once**: Select this option to poll only once after the Communication server is started.
    c. **Polling Interval**: Select this option to set the interval for polling. If you select this option, specify the interval in seconds for polling.
6. Click **Next** to configure the Galaxy port. The **Port Configuration** dialog box appears.



Note: When you click the text box, the corresponding help is displayed on the right of the dialog box.

7. In the **Galaxy Gold Port Number** box, type the TCP IP port number used by the Galaxy Gold User Interface in WIN-PAK. By default, it is set to 10001. If you change the port number, the configuration of the Galaxy Gold UI must be changed accordingly.
8. In the **Alarm Report: Primary IP Port Number** box, type the TCP IP port number used by the Galaxy Gold UI for reporting alarms in WIN-PAK. By default, it is set to 10002.
9. In the **Control Command Port Number** box, type the TCP port used for Control Commands. By default, it is set to 10005.
10. In the **Remote PIN** box, type a PIN number to remotely access the Galaxy panel. The default PIN number for the panel is 543210.
11. In the **Connection Password** box, type the password to connect WIN-PAK to Galaxy panel. The connection password is configured in the Galaxy Gold UI.
12. Select or clear the **Encryption** check box to enable encryption of password when an alarm is sent to WIN-PAK from the Galaxy panel.
13. Under **ADV**, click **Add** to create an ADV for the Ethernet module (E080) of Galaxy.

    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
14. Click **Next** to advance to the Finish dialog box.
15. Click **Next** to configure the Ethernet module for Galaxy. The Ethernet module (E080) for Galaxy panel is configured.

Refer to the "Adding a Galaxy Panel" section in this chapter for configuring the galaxy panel.

Vista Panel Port (Home Automation Mode)

The Vista panel helps you to monitor and track intrusion happening at different zones in the access control system. Zones are areas monitored by a device in the vista panel. The Vista panel is configured separately and then it is added in WIN-PAK with its configuration settings.

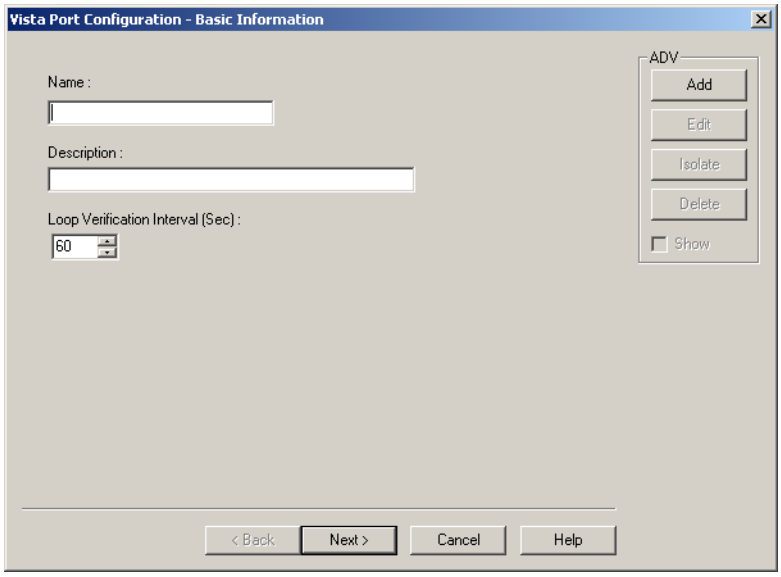
WIN-PAK communicates with the Vista panel through the Vista Panel Port. Therefore, you must configure the Vista Panel Port in the communication server to add the Vista panel in WIN-PAK.

Note: The virtual keypad is provided in WIN-PAK that enables you to work in the Vista panel.You need to have a master code to operate on the virtual keypad.

Adding a Vista Panel Port

To add a vista panel port:

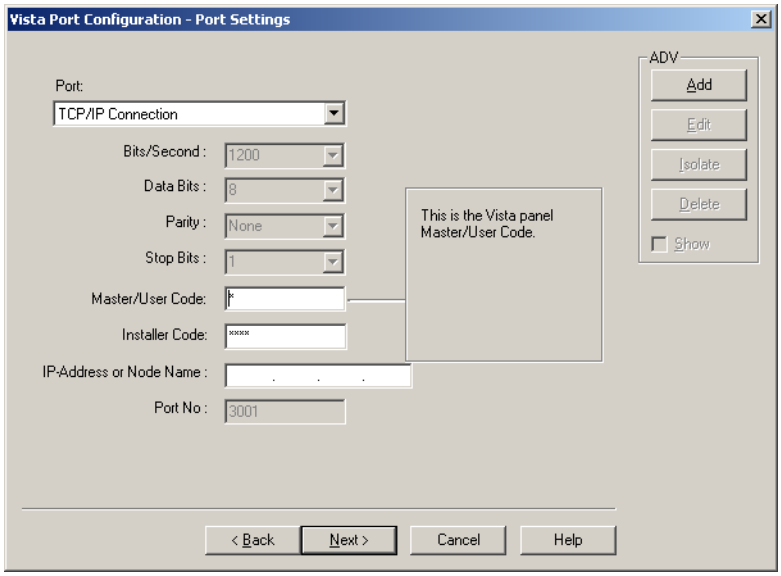
1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the communication server and choose **Add > Vista Panel Port (Home Automation Mode)**. The **Vista Port Configuration - Basic Information** dialog box appears.



3. Type a **Name** and **Description** for the Vista panel port.
4. Set the **Loop Verification Interval (Sec)** in seconds to verify the connection between WIN-PAK and the Vista panel.
5. Create an ADV for the Vista Port. Click **Add** under **ADV**, set the ADV properties and click **OK**.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

6. Click **Next** to configure the Vista port. The **Vista Port Configuration - Port Settings** dialog box appears.
7. Select the **Port** for communication. You can select the TCP/IP Connection, if you use the Micro Cobox converter for converting RS-232 to TCP/IP.



Note: When you click the text box, the corresponding help is displayed on the right of the dialog box.

8. Type the **Master/User Code** of the Vista panel. This enables you to operate on the Vista panel in WIN-PAK.
9. Type the **Installer Code** of the Vista panel. This enables you to change the Vista panel settings in WIN-PAK.
10. If you select the **TCP/IP Connection**, type the **IP-Address or Node Name** of the Micro Cobox converter.

    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
11. Click **Next** to advance to the Finish dialog box.
12. Click **Next** to configure the vista panel port. The Vista Panel Port for vista panel is configured.

Refer to the "Adding a Vista Panel" section in this chapter for configuring the galaxy panel.

Panel Configuration

The panel configuration is required in setting up your access control system. Configuring panels include:

- Setting up card formats
- Configuring different types of readers and keypads
- Configuring input and output points with numerous options.

As the number of options to set up the panel is too high, adding panels to a large system can be a time consuming job. To reduce the time effort:

- Define a panel and make a copy of it to create panels
- Define templates for action groups and use it to define ADVs of the same action type
- Copy an action group and edit. This enables you to create a variety of action groups quickly.

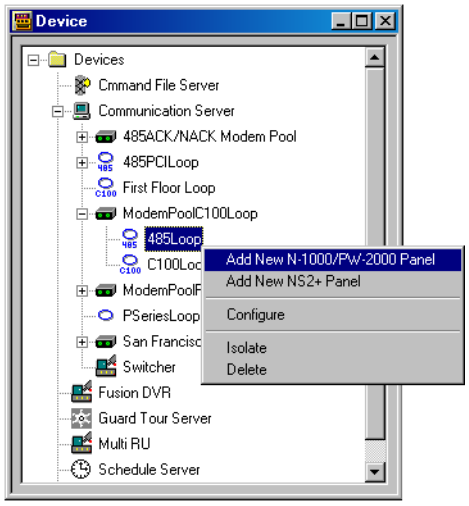
Panels are configured in WIN-PAK by adding them to the Device Map.

Adding an N-1000/PW-2000 Panel

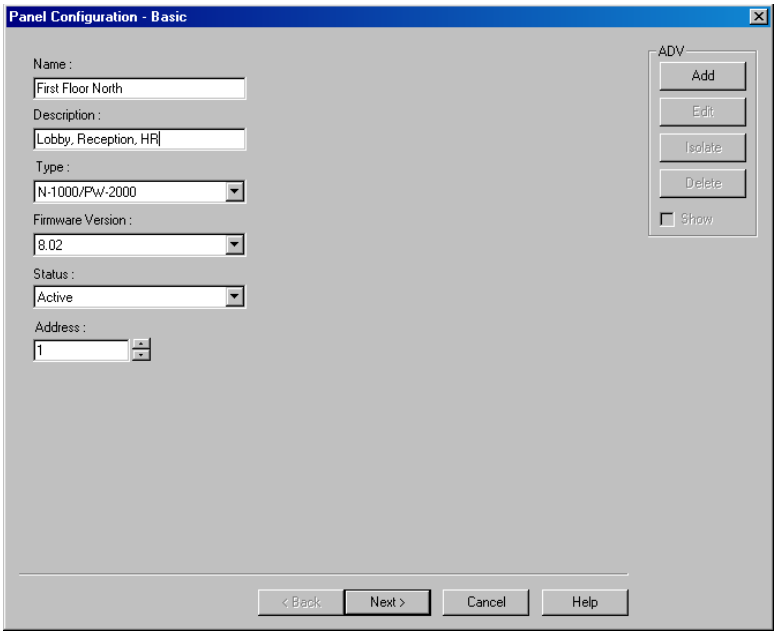
A N-1000 or PW-2000 panel can be added to C-100 and 485/PCI panel loops.

To add an N-1000/PW-2000 panel:

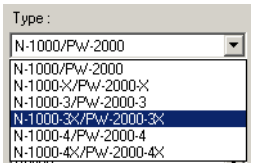
1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server folder.



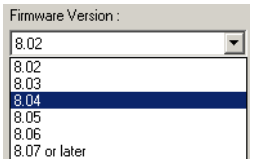
3. Right click the 485/PCI Loop or C-100 Loop and select **Add New N-1000/PW-2000 Panel**. The **Panel Configuration - Basic** dialog box appears.



4. Type a unique **Name** for the panel. This field is mandatory.
5. Type a **Description** for the panel.



6. Select the type of panel in the **Type** list. The number suffixed in the panel type indicates the number of readers, inputs, or outputs that can be connected to a panel.



7. Select the firmware version number of your panel in the **Firmware Version** list.

Note: This refers to the version of firmware of the PROM chip in your PW-2000 panel. The default is 8.2. Different panel options are available, depending on the selected firmware version.

8. Select the **Status** of the panel.
   - **Active** - The panel is configured and currently connected to the WIN-PAK system.

- **Inactive** - The panel is configured but temporarily disconnected for maintenance purpose. When you add or delete a card to an inactive panel, the card details are simply saved.
- **Not Present** - To define the panel before completing the panel installation. If the panel is marked as **Not Present**, no card transactions are saved.

9. Enter the unique **Address** for the panel from 1 through 31. The address corresponds to the DIP Switches setting on the panel.

   Consult the NS2+ installation manual for further information.

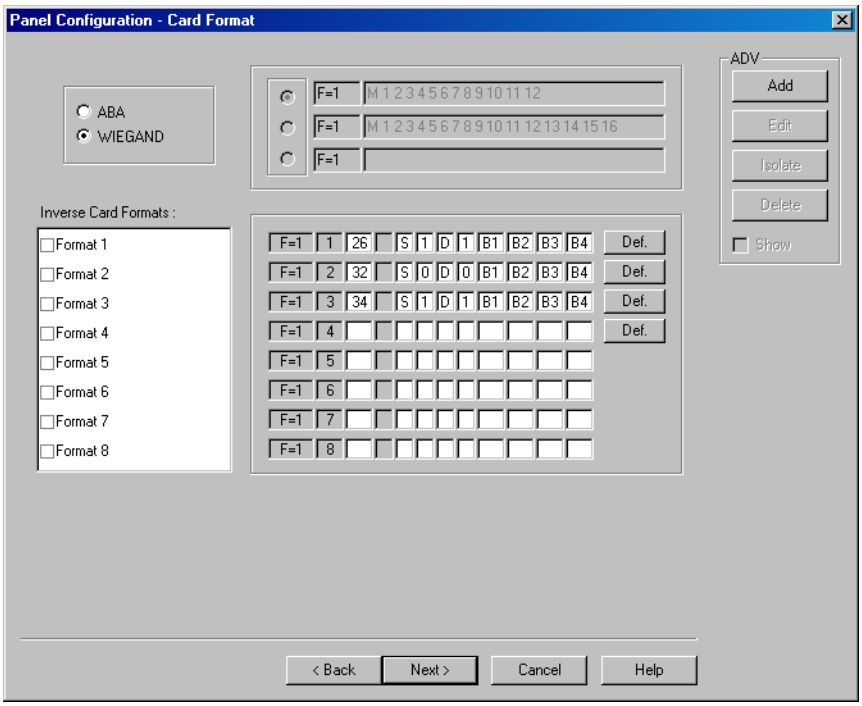
10. Click **Add** under **ADV** and set the ADV properties to create an ADV for the panel.

    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

11. Click **Next** to specify the Card Format. The **Panel Configuration - Card Format** dialog box appears.

Setting the card format for the panel

1. In the **Panel Configuration - Card Format** dialog box, select the card format type as **ABA** or **WIEGEND**. The card formats are displayed, based on the selected card format type.



2. If you select **ABA**, select one of the following card formats:
   - 12-digit card format

- 16-digit card format
- User-defined card format and type the format value.

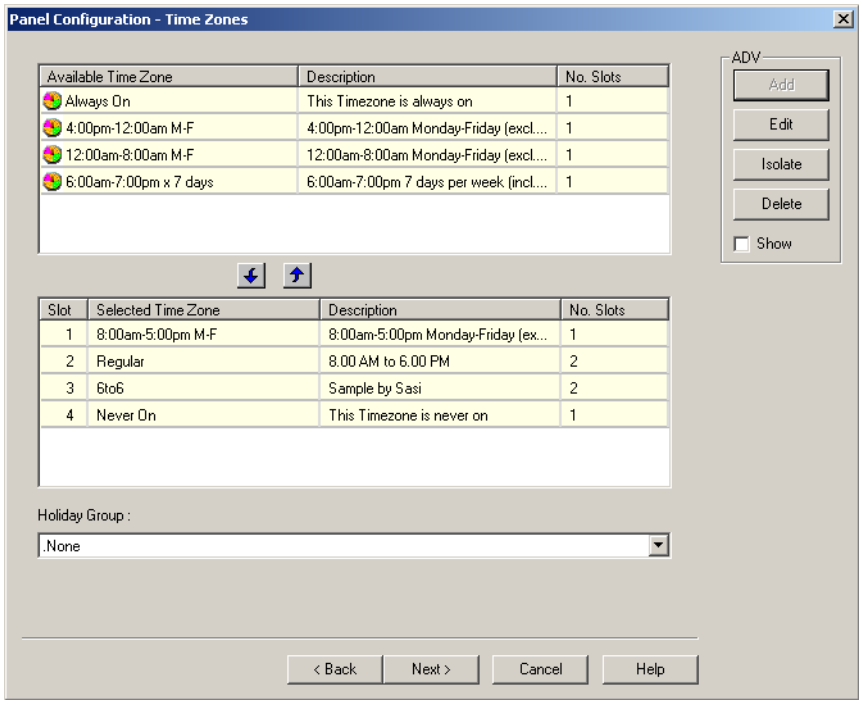
3. If you select **WIEGAND**, Honeywell recommends you to retain the default card format values.

Note: Default formats for slots 1, 2, and 3 are CR-1 Wiegand Card Swipe Reader, NR-1 Magstripe Swipe Reader, and PR-2 Hughes/IDI Proximity Reader. You can edit the default card format values and in addition, you can enter the card formats for other WIEGAND card format.

4. Click **Next** to assign time zones and holiday group to this panel. The **Panel Configuration - Time Zones** dialog box appears.

Assigning time zones and holiday group to a panel

1. In the **Panel Configuration - Time Zones** dialog box, select the time zones from the **Available Time Zone** list and click . The time zones are moved to the **Selected Time Zone** list. For multiple selections, use the SHIFT and CTRL keys.



Tip: If you want to remove a time zone from the **Selected Time Zone** list, select the time zone and click .

Only the time zones that are listed in **Selected Time Zone** are available for readers, input points and output points of this panel.

2. Select the holiday group in the **Holiday Group** list.

3. Click **Next** to set the panel options. The **Panel Configuration - Options** dialog box appears.

Setting the panel options

You can set certain panel options such as anti-passback, groups, key pads for providing access for the readers, input points, and output points attached to the panel.

- **Anti-passback**

  Anti-Passback discourages card holders to enter without using their cards. Anti-passback violation occurs at the following scenarios:

  a. If you have entered the building without using the card and exited from the building using your card. And then, if you try to enter the building the access is denied.

  b. If you have entered the building using the card and exited from the building without using the card. And then, if you try to enter the building the access is denied.

Notes:

- Anti-passback requires a reader on each side of the door. If anti-passback is selected for a panel in the Options tab, the anti-passback is locally implemented.
- In the two readers panels such as PW-2000-II and PW-2000-III, the reader 1 is used as in-reader and reader 2 is used as out-reader.
- In the four readers panels such as PW-2000-IV (X), the readers 1 and 3 are used as in-readers and the readers 2 and 4 are used as out-readers.

- **Groups**

  Output groups enable a card read to activate more than one output points for the applications such as elevator control. For example, when Reader 1 is associated to a group, a valid card read on Reader 1 pulses all points in the group. Groups must be selected to access the AEP-3 in Hardware Options.

- **Forgiveness**

  Anti-passback violation can be forgiven by selecting the **Forgiveness** option. When this option is selected, all cards are reset during midnight. Therefore, the cardholders who have violated the anti-passback option can now access their cards to enter the building.

Note: If the anti-passback option is not selected, WIN-PAK defaults to a free egress configuration. In this case, the door can be activated by a button, motion detector, or other devices. For example, with an PW-2000-II panel, card reader 1 activates one door, and card reader 2 activates a different door. Inputs 3 and 4 are reserved for the exit devices for these two doors which release locks just like a valid card read.

- **Keypads**

  Indicates that the panel is using matrix style (11-wire) keypads. If Wiegand style (5-wire) keypads are used, the keypad is treated as a reader and this option must be cleared.

- **PIN and Time Zone for PIN**

  The PIN number must be entered in the keypad during a particular time zone, before presenting a card to gain access in an entrance.

- **Continuous Card Reads**

  Card readers do not recognize valid cards while the corresponding output is energized. Continuous Card Reads enables card readers to read cards continuously, independent of output pulse time.

  Example: When Output 1 is assigned a 10 second pulse time, a valid card read at Reader 1 causes Output 1 to energize for 10 seconds. During this time the card reader does not recognize any other valid cards, if the Continuous Card Reads option is not selected.

- **Reverse Read LEDs**

  This option reverses the standard LED operation of the reader. If this option is selected, a reader that normally changes from green to red on a valid card read, changes from red to green.

- **Host Grant**

  Host Grant option provides the fault tolerance even if the card is not found in the panel. Host Grant options are used when, for example, a number of cards have been entered in the database, but have not yet been downloaded to the panel.

- **Site Codes**

  Site codes ensure that the card belongs to the facility where the card is used for gaining access. The site code is encoded with a card number on cards.

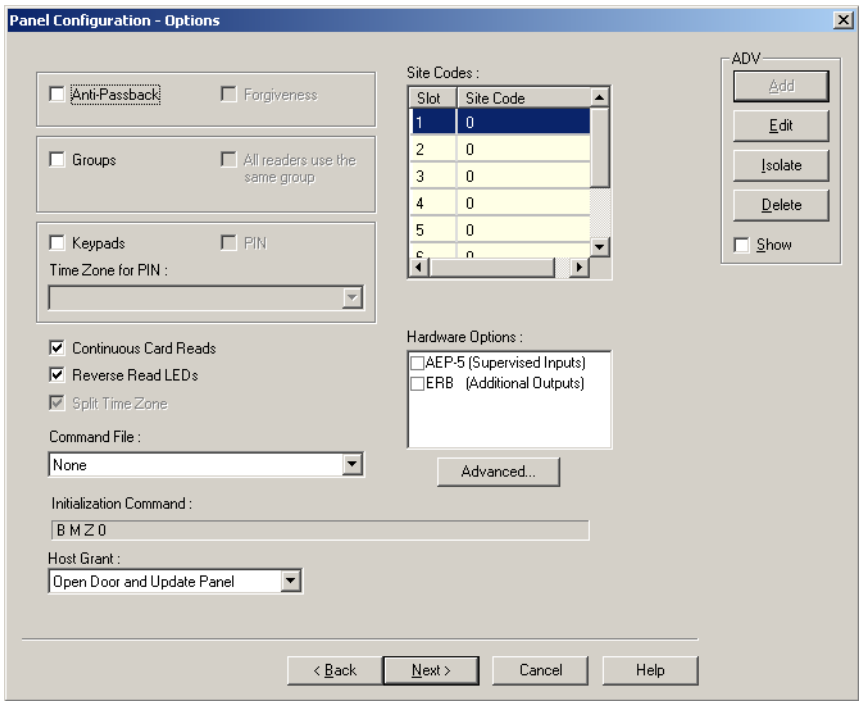
- **Hardware Options**

  Hardware Options enable you to include additional input and output points to the panel using the extendable boards. The available hardware options vary depending on the type of panel selected. The AEP-5 (supervised input board) and ERB (Expanded Relay Board) are only used with PW-2000-II panels.

  If the Groups option is selected in this dialog box, you can select one or two AEP-3 Output Expansion Boards. Each board adds eight output relays to a panel.

To set the panel options:

1. In the **Panel Configuration - Options** dialog box, select the **Anti-passback** check box to ensure that the card holders present the cards while entering and exiting a building.



2. Select the **Groups** check box to create output relay groups.
3. Select the **All readers use the same group** check box to pulse the group when a valid card is presented on any reader to pulse the group.
4. Select the **Keypads** check box if matrix style (11-wire) keypads are used in the panel. If you are using Wiegand style (5-wire) keypads, the keypad is treated as a reader and this option must be cleared.
5. Select the **PIN** check box, if a keycode must be entered before presenting a card to gain access.

Note: Do not select this check box if the door is using keypads without readers.

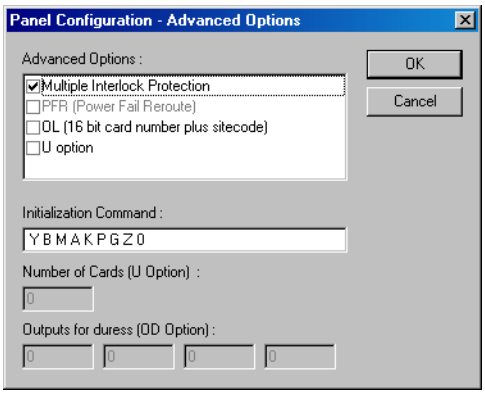
6. Select a time zone in the **Time Zone** list during which a PIN is required for card access.
7. Select the **Continuous Card Reads** check box to enable card readers to read cards continuously, independent of output pulse time.
8. Select the **Reverse Read LEDs** check box to reverse the standard LED operation of the reader. If this check box is selected, a reader that normally changes from green to red on a valid card read, changes from red to green.
9. In the **Command File** list, select a command file that is applicable to a panel.

10. Select the following **Host Grant** options to grant the permission for the card holders, even if the card is not found in the panel:
    - **Disable** - Denies access to the card holders whose card details are not present in the panel.
    - **Open Door** - Enables the door to open, even if the card is not found in the panel.
    - **Open Door and Update Panel** - Enables the door to open and also to download the card details to the panel. Therefore, the panel is updated.
11. Enter a **Site Code** to ensure that cards belong to the facility where access is attempted. You can enter up to eight site codes.

    Tip: To enter a site code, double-click any cell in the table, type the site code and press ENTER. If no site code is defined, the reader does not check for site codes to enable card access.

    Note: When the card formats for the panel is ABA card formats, site codes cannot be entered.
12. Under **Hardware Options**, select the required hardware expandable boards check boxes for including the additional input or output points.

    Note: If the Groups option is selected in this dialog box, you can select one or two AEP-3 Output Expansion Boards. Each board adds eight output relays to a panel.
13. To configure the Advanced options:
    a. Click **Advanced**. The **Panel Configuration - Advanced Options** dialog box appears.



    b. Select the **Multiple Interlock Protection (MIP)** check box to return all input points tied to a single output to a normal state before the output is de-energized. Without MIP, just one input returning to the normal state de-energizes the output. This is available with all the PW-2000 series panels.
    c. Select the **PFR (Power Fail Reroute)** check box to allow Input 8 (Primary Power) to be re-routed to Input 9 (Primary Power–System

Alarm), freeing up Input 8 on the AEP-5 to be used as a standard/supervised input point. This is available only with the PW-2000-II using AEP-5.

d. Select the **OL (16 bit card number plus site code)** check box to create WIEGAND card numbers by concatenating the site code and the card numbers. The result is transmitted as a 12-digit number. This is available with all PW-2000 series panels. Do not add site codes to the panel with this option.

e. Select the **OJ (20 bit card number plus site code)** check box to set the format for 20-bit card numbers. This is only available with firmware 8.03 version or later. The first 12 bits are interpreted as the site code and the last 8 as the card number. The card number is sent to the head end software as a 12-digit number.

f. Select the **OH (25-bit card number plus site code)** check box to enable special card format applications. This is available for use with firmware later than 8.03.

Note: The **OJ**, **OL** or **OH** option cannot be used at the same time.

g. Select the **U Option** check box to change the number of cards the panel can support. This option is available only for PW-2000 panel series. It enables the user to change the number of cards the panel supports. Selecting more cards reduces the number of buffers available to store events when the panel is not on-line with the computer or when heavy traffic prevents immediate transmission of all events.

h. Select the **OD (Duress Option)** check box to activate the pulse action for the output defined in the Outputs for Duress, when the PIN is used one value low or high in case of emergencies like threatening. When configured with firmware later than 8.03, two outputs can be selected. This is only available with the PW-2000 with firmware 8.03 version.

i. In the **Initialization Command** box the command string that is sent to the panel at initialization is displayed.

j. In the **Number of cards for U option** box, enter the number of cards for the panel. This option is enabled only if the U option is selected.

k. In the **Outputs for duress (OD Option)** box, enter the value for Outputs for duress. This option is enabled only if the OD option is selected.

l. Click **OK** to configure the advanced options.

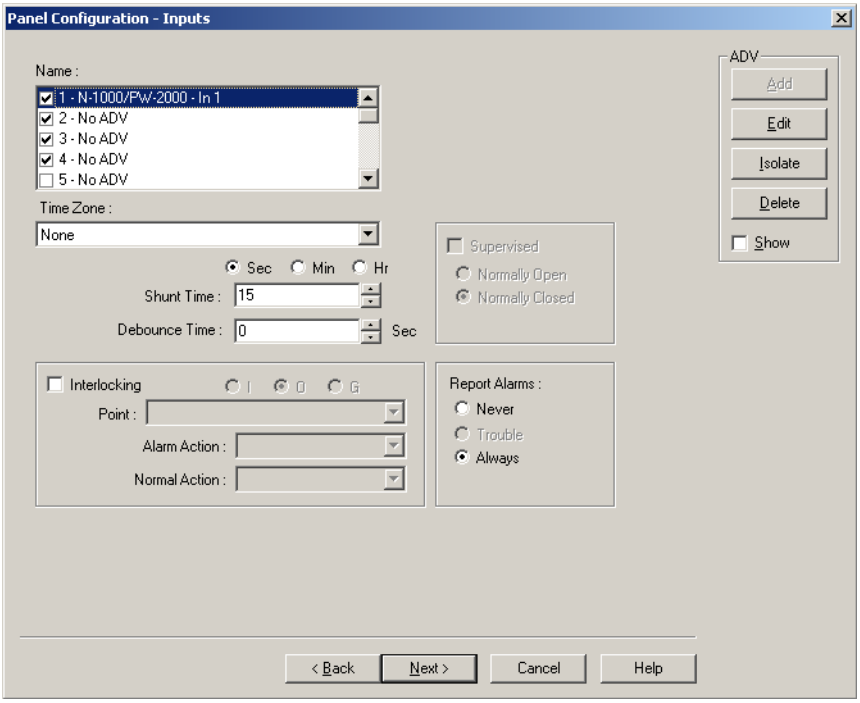
Note: The Advanced Options are available depending on the PW-2000 series panel and the version of firmware that is used.

14. Click **Next** to configure the Input points to the panel.

Configuring input points to the panel

To configure input points to the panel:

1. In the **Panel Configuration - Inputs** dialog box, select an input point check box under **Name**. The other settings in the dialog box are available only for the selected input point.



Notes:

- WIN-PAK sets some input points as active and may assign them an interlock value. These default settings vary depending on the type of panel.
- The settings of these input points can be changed, but you cannot make it inactive if it is interlocked with an output point.

2. Click **Add** under **ADV**, set the ADV properties and click **OK** to define an ADV for each input point.
3. Select a **Time Zone** during which an input point must be deactivated.
4. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the maximum time allowed for the door to close after it has been unlocked. If the time taken to close the door exceeds the shunt time, an alarm is raised.
5. Enter the **Debounce Time** in seconds. Debounce time is the maximum time allowed for the door to close after the shunt time is exceeded. If the time taken to close the door exceeds the debounce time, an alarm is raised. This debounce time is meant for the doors that swing often due to wind.

For example, consider the following scenarios:

Table 11-1 Explaining Shunt Time and Debounce Time

Scenario	Shunt Time	Debounce Time	Alarm raised at...
1	15 sec	0 sec	16th sec
2	15 sec	10 sec	25th sec

6. Enter the time interval after which the changed state of an input point is reported.

   Example: An input point with a debounce time of 5 can be in active condition for five seconds before it is reported as an alarm. The same is true when returning to normal condition. The input point would not report as normal until it was in the normal state for five seconds.

   Note: If the value is set to zero, the debounce time is a minimum of .33 seconds on events going to normal, but alarms are reported immediately. The debounce time is 0 seconds on alarm.

7. Select the **Supervised** check box to report the troubles when there is a change in the state of input points.
8. Select **Normally Closed** or **Normally Opened** to specify the normal state of the door.

   Note: All N-1000/PW-2000 alarm input points and N-1000/PW-2000 with an AEP-5 default to **Normally Closed**. N-1000/PW-2000-III/IV inputs can be configured for **Normally Open** circuits and 3-state supervised circuits.

9. Under **Report Alarms**, select the following:
   - **Never**: To prevent from reporting the alarms.
   - **Always**: To report alarms.
   - **Trouble**: To report the trouble conditions. This is typically used for egress devices to detect tampering. This option is enabled only for supervised input point.
10. Set the **Interlocking** option for the input point.

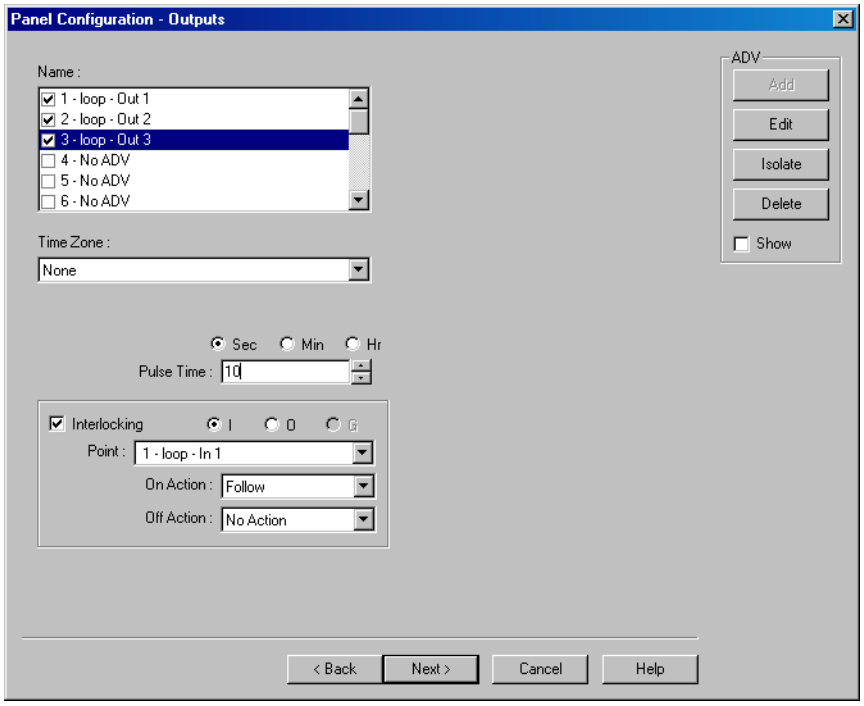
    Refer to the "Interlocking" section in this chapter for more details on interlocking.

11. Click **Next** to configure the output points to the panel. The **Panel Configuration - Outputs** dialog box appears.

Configuring output points to the panel

To configure output points to the panel:

1. In the **Panel Configuration - Outputs** dialog box, select an output point check box under **Name**. The other settings in the dialog box are applicable only for the selected output point.



Notes:

- WIN-PAK sets some output points as active and may assign them an interlock value. These default settings vary depending on the type of panel.
- The settings of these output points can be changed, but you cannot make it inactive if it is interlocked with an input point.

2. Click **Add** under **ADV**, set the ADV properties and click **OK**, define an ADV for each output point.

   Note: In the ADV definition, three actions are listed for an output point: Energized, De-Energized, and Trouble. In an output point, Trouble means that WIN-PAK cannot determine if the output is energized or de-energized.

3. Select a **Time Zone** during which the output point must be turned on.
4. Select **Sec**, **Min**, or **Hrs** and enter the **Pulse Time** to set the period during which the output point must be energized when triggered.
5. Set the **Interlocking** for the output point.

   Refer to the "Interlocking" section in this chapter for more details on interlocking.

6. Click **Next** to set the group properties. The **Panel Configuration - Group** dialog box appears.

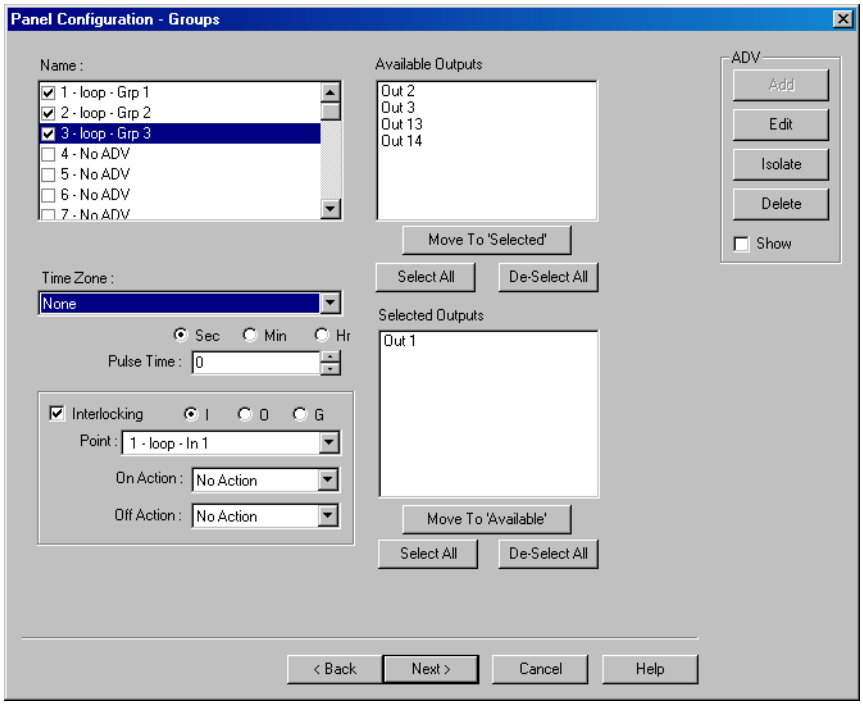
Note: This dialog box appears only if you have opted for Group option in the **Panel Configuration - Options** dialog box.

Configuring groups to the panel

A group is one or more active output points that are grouped together. Output relay groups enable a card read to activate more than one output relay for applications such as elevator control. As many as 32 groups can be defined per panel.

To define an output group:

1. In the **Panel Configuration - Groups** dialog box, select a group under **Name**. The output points belonging to the selected groups are listed in **Available Outputs**.



2. Select the output points under **Available Groups** and click **Move to "Selected"**. Alternatively, click **Select All** to select all outputs points. The output points are moved under the **Selected Outputs** list.
3. Select a **Time Zone** during which the output group must be turned on.
4. Select the required time unit for the pulse time and then set the **Pulse Time** for the output group to stay energized when it is triggered.
5. Set the interlocking for the output group.

   Refer to the "Interlocking" section in this chapter for more details on interlocking.

6. Define ADV for each group. Click **Add** under **ADV**, set the ADV properties and click **OK**.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

7. Click **Next** to configure readers to the panel. The **Panel Configuration - Readers** dialog box appears.

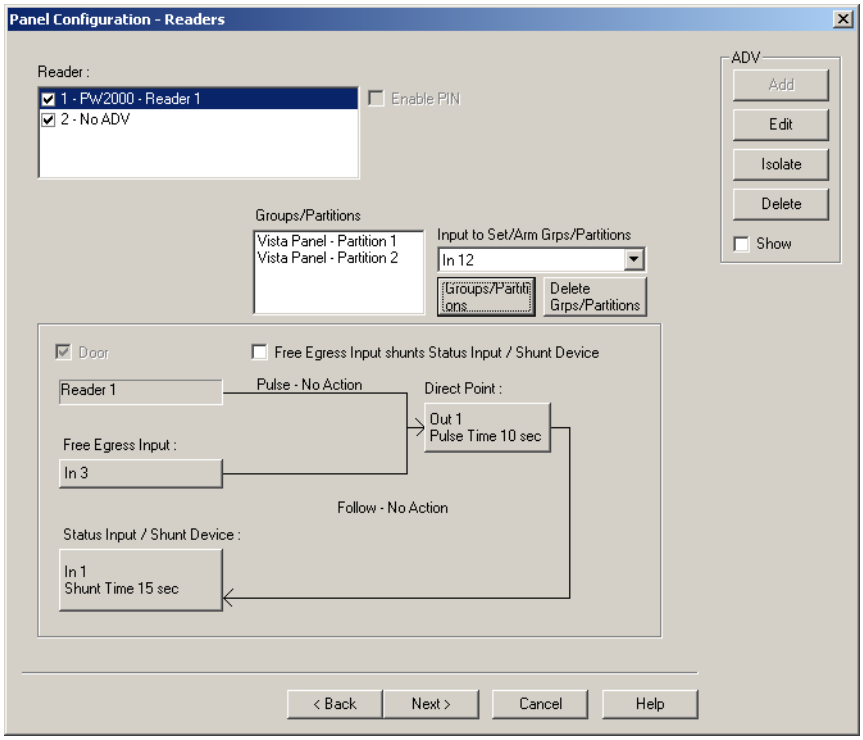
Configuring a reader to the panel

The number of readers available for the panel depends on the type of panel being configured. The WIN-PAK system automatically adds readers to the panel. By default, all available readers are active and are defined as doors. If the anti-passback option is not set, the readers are set for a free egress configuration.

In addition, you can associate galaxy groups or vista partitions to the reader and the input point. After the association you can set/unset galaxy groups or arm/disarm vista partitions using the privileged card. Present the privileged card to the reader and press the input button to unset the galaxy groups or disarm the vista partitions. However, present the privileged card to the reader to set the galaxy groups or arm the vista partitions.

To define a reader:

1. In the **Panel Configuration - Readers** dialog box, select a reader from the list to view its settings. The panel configuration is depicted on the lower-half of the dialog box.



Note: The Direct Point (the point that is pulsed on a valid card read), Pulse Time, Status Input and Shunt Time, and Free Egress Input are displayed.

2. Select a reader from the **Reader** list.
3. To detach a reader from the door, clear the **Door** check box. For example, a reader used in the muster area can be used without a door.
4. Click **Add** under **ADV** and set the ADV properties to create an ADV for the reader.

Caution: Once a reader is added to the device map, you cannot attach the reader to a door or detach it from the door. Therefore, confirm the reader's usage, before adding it to the device map.

If a reader is not attached to a door, it remains as a reader without any door properties.

If a reader is attached to a door, the graphical form depicts the way the door is configured.

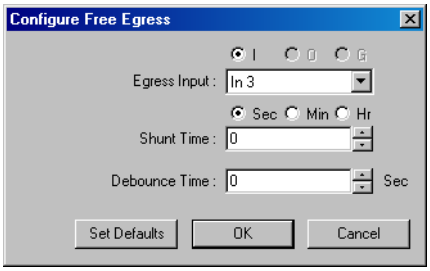
5. To associate galaxy groups or vista partitions to this reader, click **Groups/Partitions** and select the groups from the list.

Note: To dissociate the galaxy group or vista partition from the reader, select the galaxy group or vista partition and click **Delete Grps/Partitions**.

6. To associate galaxy groups or vista partitions to the input point, select the input point from the **Input to Set/Arm Galaxy Grps/Partitions** list.

Note: Only the input points that are configured in this panel and not interlocked are listed in the **Input to Set/Arm Galaxy Grps/Partitions** list.

7. To change the input point used as a free egress input:
    a. Click **Free Egress** in the graphical form. The **Configure Free Egress** dialog box appears.



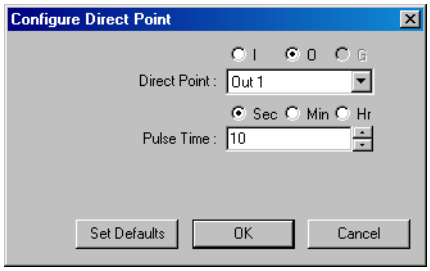
    b. Select the **Egress Input** from the list.
    c. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the maximum time allowed for the door to close after it has been unlocked. If the time taken to close the door exceeds the shunt time, an alarm is raised.
    d. Enter the **Debounce Time** in seconds. Debounce time is the maximum time allowed for the door to close after the shunt time is exceeded. If the

time taken to close the door exceeds the debounce time, an alarm is raised. This debounce time is meant for the doors that swing often due to wind. See Table 11-1 for examples.

e. Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

8. To change the output pulsed on a valid card read:

   a. Click **Direct Point** in the graphical form. The **Configure Direct Point** dialog box appears.



   b. Select **I**, **O** or **G** to indicate Input Point, Output Point, or Group. The corresponding points are enabled in Direct Point.

   c. Select the **Direct Point** from the list.

   d. Select **Sec**, **Min** or **Hr** and change the **Pulse Time**.

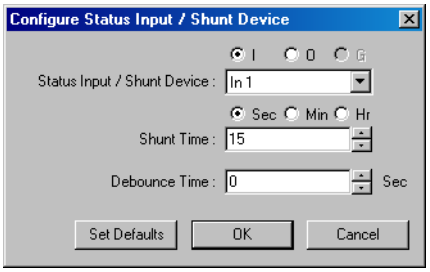
   e. Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

   The changes to the pulse time are automatically reflected in the appropriate input, output, or group.

9. Select the **Free Egress Input shunts Status Input / Shunt Device** check box to follow no action on the direct point when a **Free Egress Input** is activated.

10. To trigger an action in another input, output or group as a series action of direct point:

   a. Click **Status Input / Shunt Device** in the graphical form. The **Configure Status Input / Shunt Device** dialog box appears.



   b. Select **I**, **O** or **G** to indicate Input Point, Output Point, or Group. The corresponding points are enabled in **Status Input / Shunt Device**.

   c. Select the **Status Input / Shunt Device** from the list.

d. Select the unit of time as **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the maximum time allowed for the door to close after it has been unlocked. If the time taken to close the door exceeds the shunt time, an alarm is raised.

e. Enter the **Debounce Time** in seconds. Debounce time is the maximum time allowed for the door to close after the shunt time is exceeded. If the time taken to close the door exceeds the debounce time, an alarm is raised. The debounce time is meant for the doors that swing often due to the wind. See Table 11-1 for examples.

f. Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

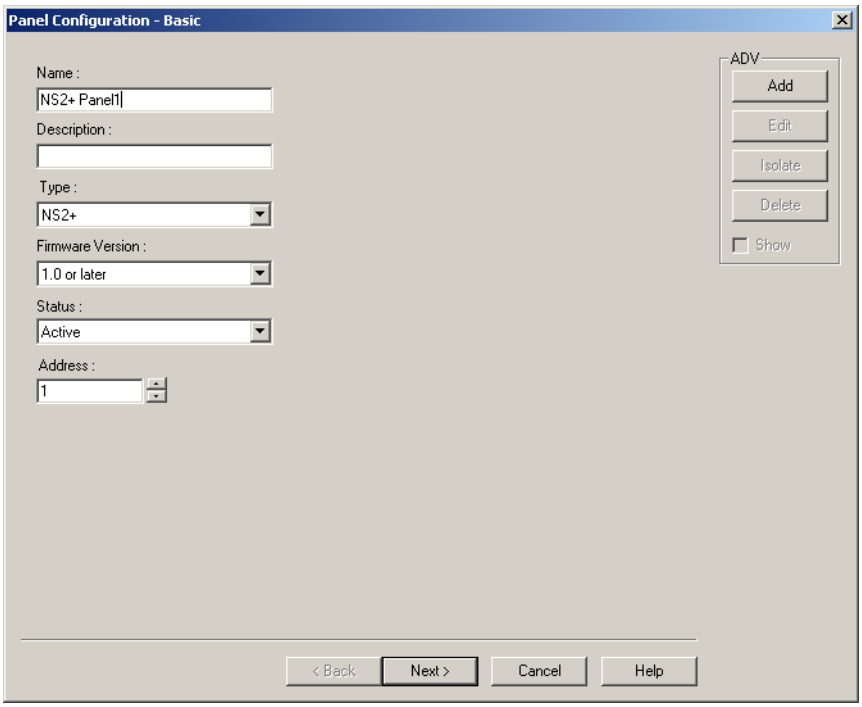
11. Click **OK** to save the panel configuration.

Adding a NS2+ Panel

A NS2+ panel can be added to an RS-232 (single panel) and 485/PCI panel loops.

To add a NS2+ panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server folder.
3. Right click the RS-232 Loop or 485/PCI Loop and select **Add New NS2+ Panel**. The **Panel Configuration - Basic** dialog box appears.



4. Type a unique **Name** for the panel. This field is mandatory.
5. Type a **Description** for the NS2+ panel.

6. Select the type of panel in the **Type** list. The only available type is NS2+.
7. Select the firmware version number of your panel in the **Firmware Version** list. This refers to the version of firmware of the PROM chip in your NS2_ panel. The default is 1.0 or later.
8. Select the **Status** of the panel:
    - **Active** - If the panel is configured and presently connected to the WIN-PAK system.
    - **Inactive** - If the panel is configured but temporarily disconnected for maintenance purpose. When you add or delete a card to an inactive panel, the card details are simply saved.
    - **Not Present** - If you want to configure the panel in WIN-PAK before completing the panel installation. If the panel is marked **Not Present**, no transactions are saved.
9. Enter a unique panel **Address**. The address corresponds to the DIP Switches setting on the panel and ranges from 1 through 31.

    Consult the NS2+ installation manual for further information.
10. Click **Add** under **ADV** and set the ADV properties to create an ADV for the panel.

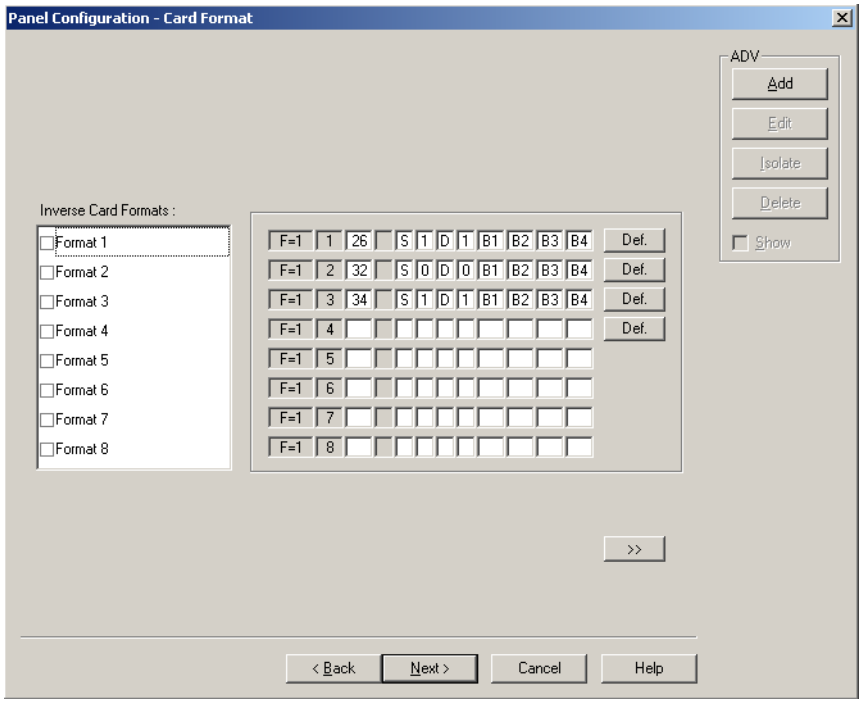
    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
11. Click **Next** to set the Card Format. The **Panel-Configuration - Card Format** dialog box appears.

Setting the card format for the panel

WIEGEND is the only card format type available for NS2+ panels. It supports 32 card formats to be used.

1. In the **Panel-Configuration - Card Format** dialog box set the WIEGEND card format values.

    Honeywell recommends you to retain the default card format values.



Reader/Card	Format
CR-1 Wiegand Card Swipe/26 bit-generic	_F=*pn_fsn*_26_S_1_D_1_B1_B2_B3_B4
NR-1 Magstripe Swipe, NR5/32 bit	_F=*pn_fsn*_32_S_Ø_D_Ø_B1_B2_B3_B4
HID/34 bit	_F=*pn_fsn*_34_S_1_D_1_B1_B2_B3_B4
CI-1 Wiegand Card Insert/26 bit	_F=*pn_fsn*_26_I_1_D_1_B1_B2_B3_B4
PR-1-280 Cotag Proximity/32 bit	_F=*pn_fsn*_32_S_Ø_D_Ø_B1_B2_B3_B4
HG-1 Hand Geometry/32 bit	_F=*pn_fsn*_32_S_Ø_D_Ø_B1_B2_B3_B4
5 Conductor Keypad/32 bit	_F=*pn_fsn*_32_S_Ø_D_Ø_B1_B2_B3_B4
Dorado Magstripe Cards/34 bit	_F=*pn_fsn*_34_S_1_D_Ø_B1_B2_B3_B4
Sielox Wiegand Cards/34 bit	_F=*pn_fsn*_34_S_1_D_1_B1_B2_B3_B4
Sielox Proximity Cards/32 bit	_F=*pn_fsn*_32_S_Ø_D_Ø_B1_B2_B3_B4

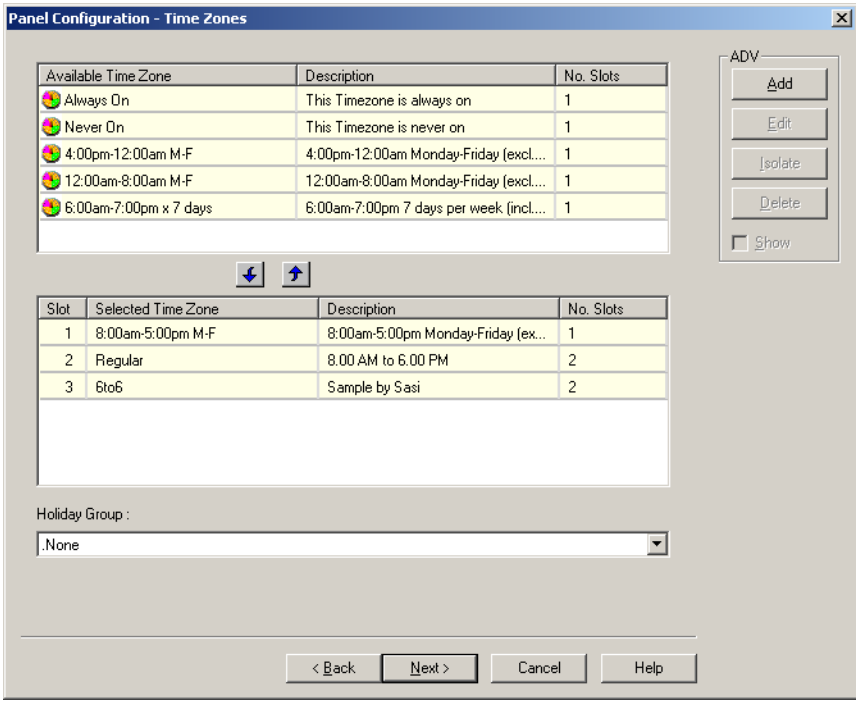
Where *pn* = panel address number and *fsn* = format slot number.

Note: Default formats for slots 1, 2, and 3 are CR-1 Wiegand Card Swipe Reader, NR-1 Magstripe Swipe Reader, and PR-2 Hughes/IDI Proximity Reader. You can edit the default card format values and also you can enter the card formats for other WIEGAND card format.

2. Click **Next** to assign time zones and holiday group to this panel. The **Panel Configuration - Time Zones** dialog box appears.

Assigning time zones and holiday group to a panel

1. In the **Panel Configuration - Time Zones** dialog box, select the time zones from the **Available Time Zone** list and click . The time zones are moved to the **Selected Time Zone** list. For multiple selections use the SHIFT and CTRL keys.



Tip: If you want to remove a time zone from the Selected Time Zone list, select the time zone and click .

The time zones that are listed in Selected Time Zone are available for readers, inputs and outputs of this panel.

Note: The NS2+ panel has 63 time zone slots, in a very large system, the number of time zones might be higher than the number of available slots. In that case, it would be necessary to select only the time zones that apply to a given panel. To help you determine the number of slots available, only the number of slots used is displayed for each time zone.

2. If you are using holiday overrides, select the holiday group in the **Holiday Group** list.
3. Click **Next** to set the panel options. The **Panel Configuration - Options** dialog box appears.

Setting the panel options

- **Global Anti-passback**

  An Anti-passback violation occurs when a card holder does not access the card at a reader while entering or exiting a building.

  Anti-passback violation occurs at the following two scenarios:

  - **In-Out-In**: If you have entered the building using the card and exited from the building without using the card. And then, if you try to enter the building the access is denied.

- **Out-In-Out**: If you have entered the building without using the card and exited from the building using your card. And then, if you try to enter the building the access is denied.

Notes:

- Anti-passback requires a reader on each side of the door. If anti-passback is selected for a panel in a given area, the anti-passback is globally implemented.

- **Forgiveness**

  Anti-passback violation can be forgiven by selecting the **Forgiveness** option. When this option is selected, all cards are reset during midnight. Therefore, the cardholders who have violated the anti-passback option can now access their cards to enter the building. This option is enabled only if Global Anti-passback is selected.

Note: If the anti-passback option is not selected, WIN-PAK defaults to a free egress configuration. In this case, the door can be activated by a button, motion detector, or other devices. For example, with a NS2+ panel, card reader 1 activates one door, and card reader 2 activates a different door. Inputs 3 and 4 are reserved for the exit devices for these two doors which release locks just like a valid card read.

- **Keypads**

  Indicates that the panel is using matrix style (11-wire) keypads. If Wiegand style (5-wire) keypads are used, the keypad is treated as a reader and this option must be cleared.

- **PIN**

  The PIN number must be entered in the keypad, before presenting a card to gain access at an entrance. This option is disabled and it is selected when the Keypad option is selected.

- **Continuous Card Reads**

  Card readers do not recognize valid cards while the corresponding output is energized. Continuous Card Reads allow card readers to read cards continuously, independent of output pulse time.

  Example: When Output 1 is assigned a 10 second pulse time, a valid card read at Reader 1 causes Output 1 to energize for 10 seconds. During this time the card reader does not recognize any other valid cards, if the Continuous Card Reads option is not selected.

- **Reverse Read LEDs**

  This option reverses the standard LED operation of the reader. If this option is selected, a reader that normally changes from green to red on a valid card read changes from red to green.

- **Host Grant**

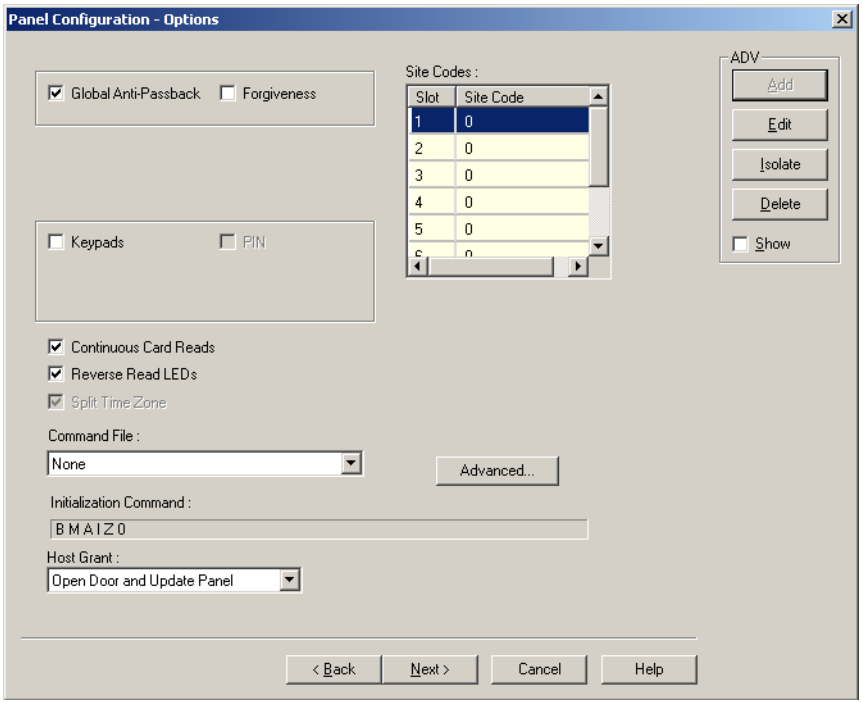
The Host Grant option provides the fault tolerance even if the card is not found in the panel. Host Grant options are used when, for example, a number of cards have been entered in the database, but have not yet been downloaded to the panel.

- **Site Codes**

  Site codes ensure that the card belongs to the facility where the card is used for gaining access. The site code is encoded with a card number on cards.

To configure the panel options for the NS2+ panel:

1. In the **Panel Configuration - Options** dialog box, select the following options:



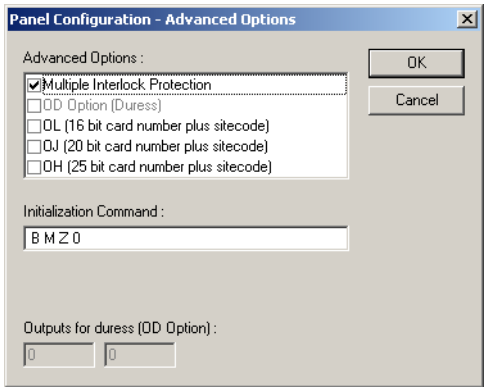
1. Select the **Global Anti-passback** check box to ensure that the card holders present the cards while entering and exiting a building. When you select this option, the anti-passback is globally implemented.
2. Select the **Forgiveness** check box to allow the door to open but to report the anti-passback violation. This check box is enabled only if Global Anti-passback is selected.
3. Select the **Keypads** check box if matrix style (11-wire) keypads are used in the panel. If you are using Wiegand style (5-wire) keypads, the keypad is treated as a reader and this option must be cleared.
4. Select the **Continuous Card Reads** check box to allow card readers to read cards continuously, independent of output pulse time.
5. Select the **Reverse Read LEDs** check box to reverse the standard LED operation of the reader. If this check box is selected, a reader that normally changes from green to red on a valid card read changes from red to green.

6. In the **Command File** list, select a command file that is applicable to a panel.
7. Select the following **Host Grant** options to grant the permission for the card holders, even if the card is not found in the panel:
   - **Disable** - Deny access to the card holders whose card details are not present in the panel.
   - **Open Door** - Enables the door to open, even if the card is not found in the panel.
   - **Open Door and Update Panel** - Enables the door to open and also to download the card details to the panel. Therefore, the panel is updated.
8. Enter a **Site Code** to ensure that cards belong to the facility where access is attempted. You can enter up to 8 site codes.

   Tip: To enter a site code, double-click any cell in the table, type the site code and press ENTER. You can press the ESC key to cancel the site code entry. If no site code is defined, the reader does not check for site codes to enable card access.

   Note: When the card formats for the panel is ABA card formats, site codes cannot be entered.

9. To configure the Advanced options,
   a. Click **Advanced**. The **Panel Configuration - Advanced Options** dialog box appears.



   b. Select the **Multiple Interlock Protection (MIP)** check box if you want all input points tied to a single output return to a normal state before the output is de-energized. Without MIP, just one input returning to the normal state de-energizes the output.
   c. Select the **OD (Duress Option) check box** to activate the pulse action for the output defined in the Outputs for Duress, when the PIN is used one value low or high in case of emergencies like threatening. This check box is enabled only when the PIN option is selected.
   d. Select the **OL (16 bit card number plus site code)** check box to create WIEGAND card numbers by concatenating the site code and the card

numbers. The result is transmitted as a 12-digit number. Do not add site codes to the panel with this option.

e. Select the **OJ (20 bit card number plus site code)** to set the format for 20-bit card numbers. The first 12 bits are interpreted as the site code and the last 8 as the card number. The card number is sent to the head end software as a 12-digit number.

f. Select the **OH (25-bit card number plus site code)** check box to set the special card format applications.

Note: The OJ, OL or OH option cannot be used at the same time.

g. In the **Initialization Command** box, the command string that is sent to the panel at initialization is displayed.

h. In the **Number of cards for U option** box, enter the number of cards for the panel. This option is enabled only if the U option is selected.

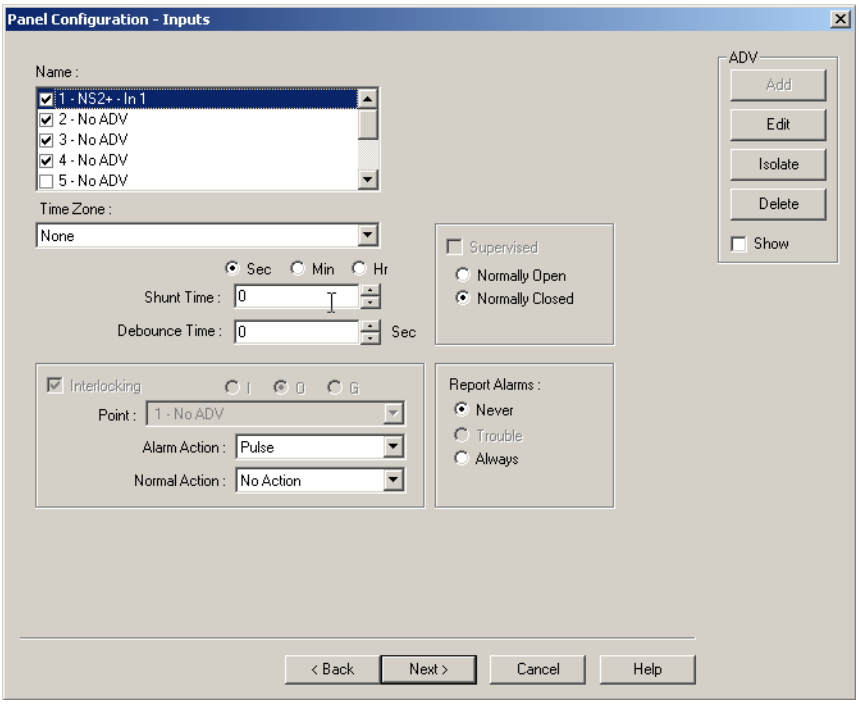
i. In the **Outputs for duress (OD Option)** box, enter the value for Outputs for duress. This option is enabled only if the OD option is selected.

10. Click **Next** to configure the Input points to the panel.

Configuring input points to the panel

To configure input points to the panel:

1. In the **Panel Configuration - Inputs** dialog box, select an input point check box under **Name**. The other settings in the dialog box are applicable only for the selected input point.



Note:

- WIN-PAK sets some input points as active and may assign them an interlock value. These default settings vary depending on the type of panel.
- The settings of these input points can be changed, but you cannot make it inactive if it is interlocked with an output point.

2. Click **Add** under **ADV**, set the ADV properties and click **OK** to define an ADV for each input point.
3. Select the **Time Zone** during which the input point must be activated.
4. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the maximum time allowed for the door to close after it is unlocked. If the time taken to close the door exceeds the shunt time, an alarm is raised.
5. Enter the **Debounce Time** in seconds. Debounce time is the maximum time allowed for the door to close after the shunt time is exceeded. If the time taken to close the door exceeds the debounce time, an alarm is raised. This debounce time is meant for the doors that swing often due to wind.

Note: If the value is set to zero, the debounce time is a minimum of .33 seconds on events going to normal, but alarms are reported immediately. The debounce time is 0 seconds on alarm. See Table 11-1 for examples.

6. Select the **Supervised** check box to report the troubles when there is a change in state of input points.
7. Select **Normally Closed** or **Normally Opened** to specify the normal state of the door.

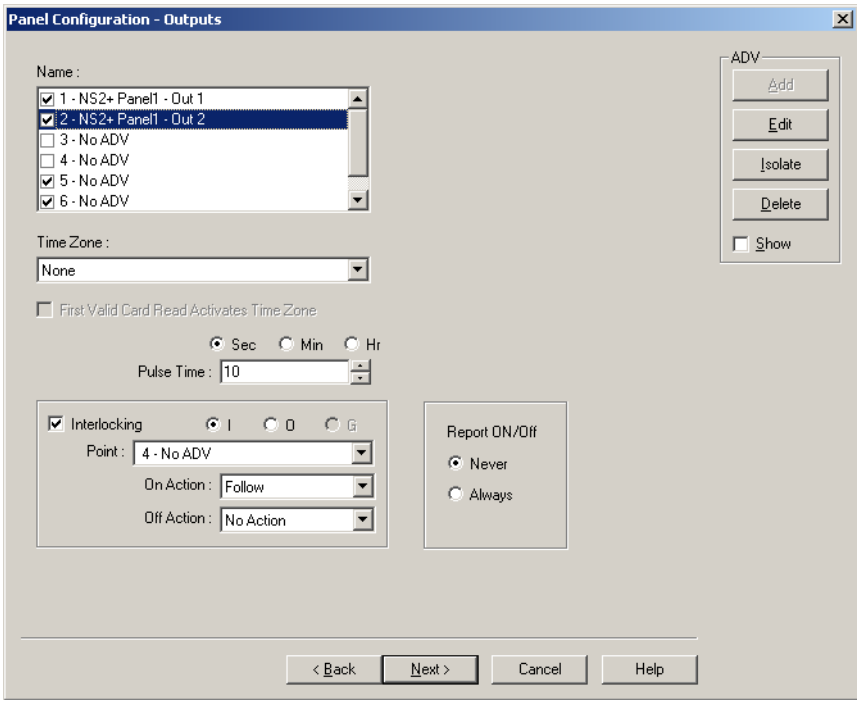
8. Under **Report Alarms**, select one of the following options:
   - **Never**: Never report an alarm on this input point.
   - **Always**: Report an alarm always.
   - **Trouble**: Report only the trouble conditions of the input point. This is typically used for egress devices to detect tampering. This option is enabled only if the input point is supervised.
9. Set the **Interlocking** for the input point.

   Refer to the "Interlocking" section in this chapter for more details on interlocking.
10. Click **Next** to configure the output points to the panel. The **Panel Configuration - Outputs** dialog box appears.

Configuring output points to the panel

To configure output points to the panel:

1. In the **Panel Configuration - Outputs** dialog box, select an output point check box under **Name**. The other settings in the dialog box are applicable only for the selected output point.



Note: WIN-PAK sets some output points as active and may assign an interlock value. These default settings vary depending on the type of panel and whether or not you have chosen the anti-passback option. The settings of these output points can be changed, but you cannot make it inactive if it is interlocked with an input point.

2. Define an ADV for each output point. Click **Add** under **ADV**, set the ADV properties and click **OK**.

Note: In the ADV definition, three actions are listed for an output point: Energized, De-Energized, and Trouble. In a output point, Trouble means that WIN-PAK cannot determine if the output is energized or de-energized.

3. Select a **Time Zone** during which the output point must be activated.
4. Select the **First Valid Read Activates Time Zone** check box to activate the output point only when a valid card is read, though the time zone is set for the output point. And then at the end of the Time Zone, the output is turned off automatically.

Note: To enable this option, you must have selected the time zone.

5. Select the time unit for the pulse time, and then select the **Pulse Time** to set the maximum time required for the output to be energized when it is triggered.
6. Select the **Interlocking** check box to interlock the points.

   Refer to the "Interlocking" section in this chapter for more details on interlocking.
7. Select the required **Report ON/OFF** option.
8. Click **Next** to configure the reader of the panel. The **Panel Configuration - Readers** dialog box appears.

Configuring a reader to the panel

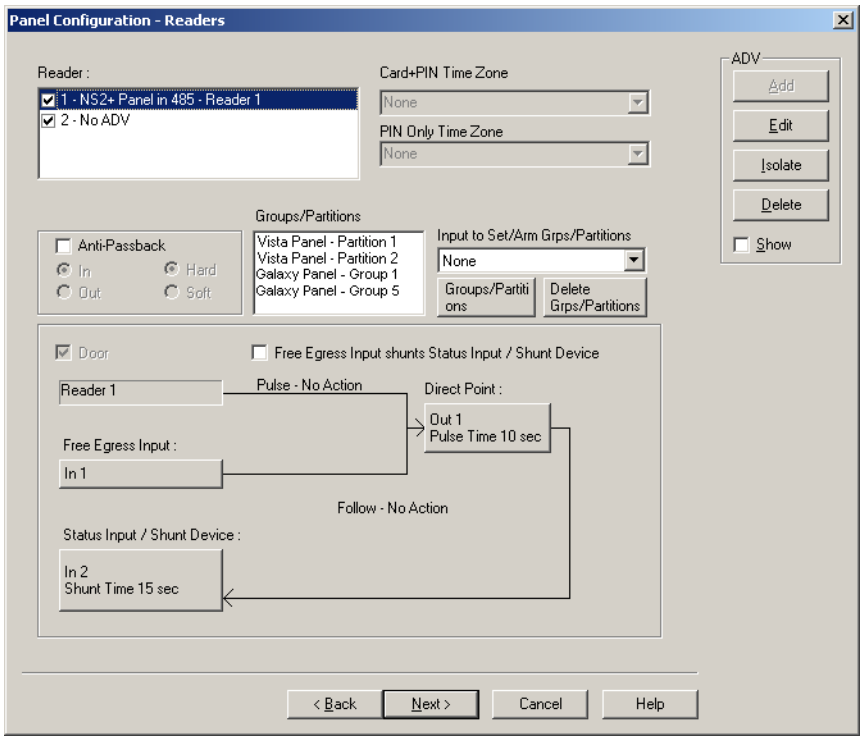
The number of readers available for the panel depends on the type of panel being configured. The WIN-PAK system automatically adds readers to the panel. By default, all available readers are active and are defined as doors.

If you have not set the anti-passback option, the readers are set for a free egress configuration. If the anti-passback option is set, the reader settings are changed to anti-passback settings.

In addition, you can associate galaxy groups or vista partitions to the reader and the input point. After the association you can set/unset galaxy groups or arm/disarm vista partitions using the privileged card. Present the privileged card to the reader and press the input button to unset the galaxy groups or disarm the vista partitions. However, Present the privileged card to the reader to set the galaxy groups or arm the vista partitions associated to the reader.

To define a reader:

1. In the **Panel Configuration - Readers** dialog box, select a reader from the list to view its settings. The dialog box displays the panel configuration in a graphical form.



Note: The Direct Point (the point that is pulsed on a valid card read), Pulse Time, Status Input and Shunt Time, and Free Egress Input are displayed.

2. Select a reader from the **Reader** list.
3. Select the **Anti-Passback** check box to set the anti-passback and implement it locally.
4. Select one of the following options to set the reader as IN or OUT and set anti-passback properties:

Table 11-2 Describing the anti-passback options

Option	Description
In	The reader is considered as IN-Reader. The anti-passback violation occurs, when the In-Out-In link is broken while accessing the readers.
Out	The reader is considered as OUT-Reader. The anti-passback violation occurs, when the Out-In-Out link is broken while accessing the readers.
Hard	When an anti-passback violation occurs, the reader strictly restricts the access.
Soft	When an anti-passback violation occurs, the reader allows the access but sends a report on anti-passback violation.

5. In the **Card+PIN Time Zone**, select a time zone for the reader during which the access is allowed only when both card and PIN number are used.
6. In the **PIN Only Time Zone**, select a time zone for the reader during which the access is allowed only by using the PIN number. In this duration, the access is denied on the reader even for the valid card read.

Note: The **Card+PIN Time Zone** and **PIN Only Time Zone** are enabled, only if you opt for the Keypad option.

7. To use the reader without attaching it to a door, clear the **Door** check box. For example, a reader used in the muster area can be used without a door.
8. Click **Add** under **ADV** and set the ADV properties to create an ADV for the reader.

Note: Once a reader is added to the device map, you cannot attach the reader to a door or detach it from the door. Therefore, ensure the reader's usage, before adding it to the Device Map.

If a reader is not attached to a door, it remains as just a reader without any door properties.

If a reader is attached to a door, the graphical form depicts the way the door is configured.

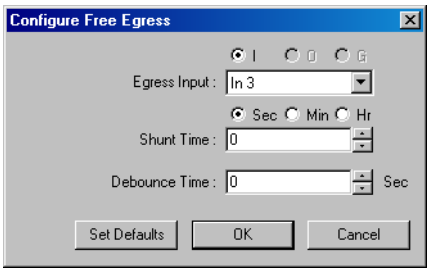
9. To associate galaxy groups or vista partitions to this reader, click **Groups/Partitions** and select the groups from the list.

Note: To dissociate the galaxy group or vista partition from the reader, select the galaxy group or vista partition and click **Delete Grps/Partitions**.

10. To associate galaxy groups to the input point, select the input point from the **Input to Set/Arm Galaxy Grps/Partitions** list.

Note: Only the input points that are configured in this panel and not interlocked are listed in the **Input to Set/Arm Galaxy Grps/Partitions** list.

11. To change the input point used as a free egress input:
    a. Click **Free Egress** in the graphical form. The **Configure Free Egress** dialog box appears.



    b. Select the **Egress Input** from the list.

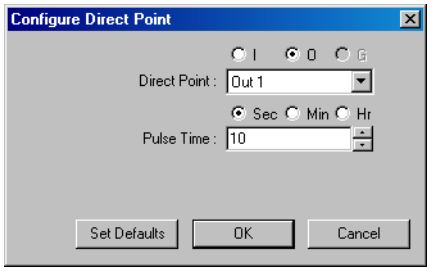
c. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the duration allowed for the door kept unlocked. If the door remains in the unlocked state even after the shunt time, the alarm is raised.

d. Enter the **Debounce Time** in seconds. Debounce time is the duration allowed after shunt time for the door to remain in the unlock status. If the door remains in the unlocked state even after the debounce time, the alarm is raised. This duration is meant for the doors that swing often due to wind.

e. Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

12. To change the output pulsed on a valid card read:

a. Click **Direct Point** in the graphical form. The **Configure Direct Point** dialog box appears.



b. Select **I**, or **O** to indicate Input Point or Output Point. The corresponding points are enabled in Direct Point.

c. Select the **Direct Point** from the list.

d. Select **Sec**, **Min** or **Hr** and change the **Pulse Time**.

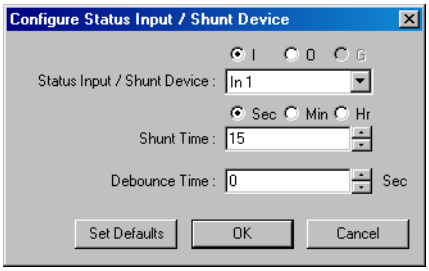
e. Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

The changes to the pulse time are automatically reflected in the appropriate input, output or group.

13. Select the **Free Egress Input shunts Status Input / Shunt Device** check box to follow no action on the direct point when a **Free Egress Input** is activated.

14. To trigger an action in another input or output as a series action of direct point:

a. Click **Status Input / Shunt Device** in the graphical form. The **Configure Status Input / Shunt Device** dialog box appears.



b. Select **I** or **O** to indicate Input Point or Output Point. The corresponding points are enabled in **Status Input / Shunt Device**.

c. Select the **Status Input / Shunt Device** from the list.

d. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the duration allowed for the door to be kept unlocked. If the door remains in the unlocked state even after the shunt time, the alarm is raised.

e. Enter the **Debounce Time** in seconds. Debounce time is the duration allowed for the door to remain in unlock status after the shunt time. If the door remains in the unlocked state even after the debounce time, the alarm is raised. This duration is meant for the doors that swing often due to wind.

f. Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

15. Click **OK** to configure the NS2+ panel.

Interlocking

The interlocking feature enables an input point or output point to take a specified action based on the change of state of another input point or output point. In an interlock sequence, an action on one point causes a reaction from a second point.

To enable Interlocking:

1. In the **Panel Configuration** dialog box, select the interlocked point (input point, output point, or group - let it be considered as Component A) under **Name**, and then select the **Interlocking** check box.
2. Select **I**, **O** or **G** option to indicate Input Point, Output Point, or Group.
3. Select the interlocking point in the **Point** list (let it be considered as Component B). Only input points, output points or groups that have already been activated, are listed out. If the required point is not listed, go to the appropriate dialog box and activate the point, then return to this dialog box.
4. If the interlocked point is an input point,
   a. Select **Alarm Action** to be taken by Component B when Component A goes to the Alert state.
   b. Select **Normal Action** to be taken by Component B when Component A returns to the normal state.

5. If the interlocked point is an output point or a group:
    a. Select the **On Action** that has to be taken by Component B when Component A is on.
    b. Select the **Off Action** that has to be taken by Component B when Component A is off.

Table 11-3 Describing the available actions for points

Action	Description
Energize	Turns the point on
De-Energize	Turns the point off
Pulse	Energize the point for a set time.
Pulse Off	Turn off a point currently pulsed. When relay is energized, it does Pulse Off and then return to Energized state. (This is rarely used and is used in addition to a command file.)
No Action	No change of state
Component A	Output 1, door strike relay
Component B	Input 1, door status switch
Action 1	Follow
Action 2	No Action

Interlocking Examples

Example 1:

Component A: Input 5, motion detector

Component B: Output 3, siren

Action 1: Energize

Action 2: De-energize

When the motion detector is triggered, input 5 goes into active state, output 3 energizes, turning on the siren. When input 5 returns to normal state, output 3 de-energizes, turning off the siren.

Example 2:

Component A: Input 6, door status switch

Component B: Output 4, bell

Action 1: Pulse

Action 2: No Action

When the door status switch is opened illegally, input 6goes into active state, output 4 pulses based on the pulse time set, The pulse time is set in the Output Point dialog box.

Adding a P-Series Panel

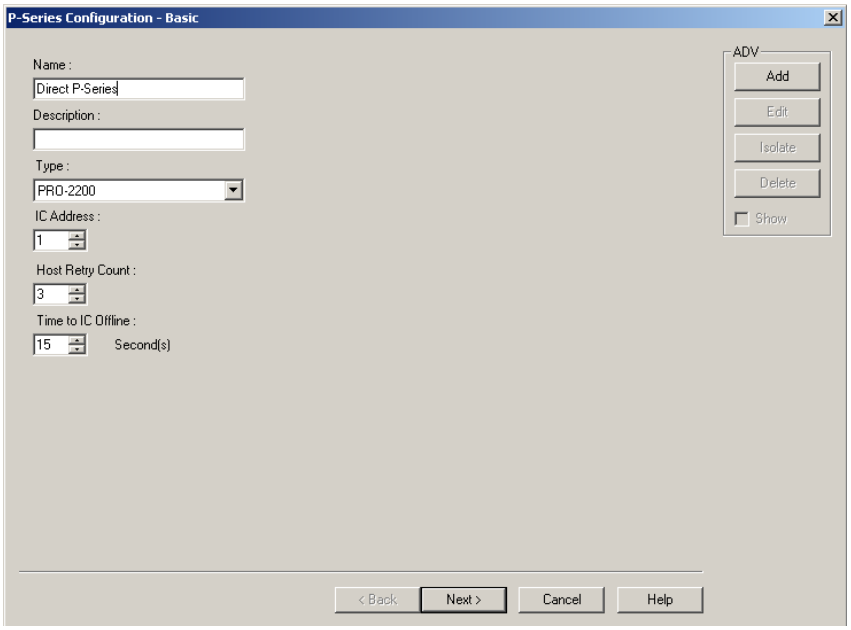
A P-Series panel is added to a P-Series Loop, a P-Series Modem Pool, or directly to a Communication Server. A direct connection to the Intelligent Controller enables the Host PC to communicate directly with the P-Series panel through RS-232 connection or through TCP/IP on the P-Series panel.

P-Series panel types available in WIN-PAK are PRO-2000 and PW-5000. Eight SIO Boards can be included in the PRO-2000 panel and 32 SIO Boards can be included in the PW-5000 panel.

Setting Up a Direct Connection

To set up a direct connection of P-Series panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the communication server folder and select **Direct P-Series Panel**. The **Panel Configuration - Basic** dialog box appears.



3. Type a unique **Name** for the panel. This field is mandatory.
4. Type the **Description** of the panel.
5. Select the type of panel in the **Type** list. The available P-Series panel types are PRO-2000 and PW-5000.
6. In the **IC Address**, enter a unique address of the Intelligent Controller board. It must be uniquely defined for each panel.

   Refer to the ***PRO-2200 Intelligent Controller Installation Manual*** for details.
7. Enter the value for **Host Retry Count**. The Host Retry Count is the number of times the Host computer has to send a command packet to the Intelligent Controller, if the Host computer receives:
   - A bad command packet from the Intelligent Controller.
   - No response from the Intelligent Controller for the command packet sent from the Host computer.

Note: Host Retry Count can be set from 2 to 10 (with 3 as the default). A range of 2 to 4 is recommended for most applications; retry counts above 4 would be used in extreme circumstances, such as in a “noisy” environment.

8. Enter the value for **Time to IC Offline**. This is the maximum time allowed for the software to declare the panel as offline, when there is no response from the Intelligent Controller.

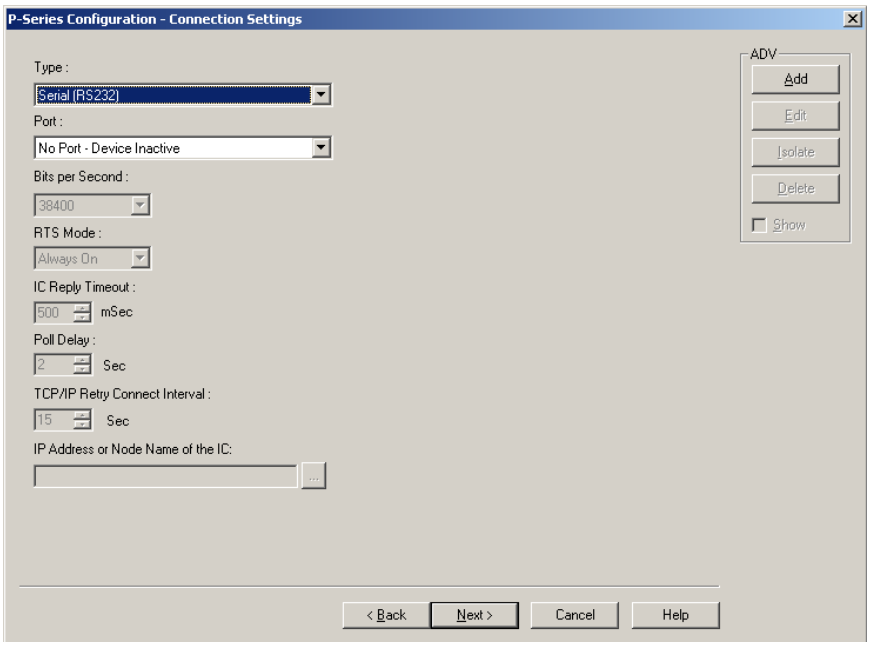
Note: The Time to IC Offline can be set from 10 to 65 seconds (with 15 seconds as the default). A range of 10 to 30 seconds is recommended for most applications.

9. Click **Add** under **ADV** and set the ADV properties to create an ADV for the P-Series panel.
10. Click **Next** to configure the connection settings.

Configuring the connection settings

To configure the connection settings of the direct P-Series panel:

1. In the **P-Series Configuration - Connection Settings** dialog box, select the **Type** of connection (Serial RS-232 or TCP/IP) used for connecting the P-Series directly to the Host computer.



2. If you select the connection type as **Serial RS-232**, enter the following:

   a. **Port**: The port in which the panel is connected to the communication server.

   b. **Bits per Second**: The communication rate for the panel. This field defaults to 38400, but can be set at 9600 or 19200 as well, depending on the baud rate set on the Intelligent Controller.

   c. **RTS Mode**: The **RTS Mode** (Request to Send) enables the Host PC to know that the Intelligent Controller is ready to send information. The RTS Mode defaults to **Always On.**

   The **Toggle** RTS Mode applies when there is an RS-485 to RS-232 converter that requires a handshake. The Toggle option is never used for a direct connection.

3. If a network card is installed on the computer and the PRO-Intelligent Controller is configured for a **TCP/IP** connection, enter the following:

   a. **IC Reply Timeout**: It is the duration the Host computer waits for an acknowledgment after it has sent an outgoing packet.

   Note: If acknowledgment is not received within the specified time, the Host PC resends the packet. The host retries according to the **Host Retry Count** set in the panel. The timeout defaults to 500 mSec but can be set from 200 to

1500 mSec. The reasonable setting for network connections is 400 to 600 mSec. The setting is higher for a WAN.

b. **Poll Delay**: This enables the system to delay polling to avoid loading down the network, if there is no activity. The default for the Poll Delay is 2 seconds, but can range from zero to 5.

Note: No delay is applied, if there is something to be sent from the software, or if the panel has more to report. For example:

- Outgoing commands posted by the application are not delayed.
- No delay is applied if the panel signals, through a reply, that it has unreported transactions. Reply headers include a "poll-me" flag.

c. **TCP/IP Retry Connect Interval**: This is the time the system waits to reopen a socket after a connection to the network is lost and the socket is closed. The system waits for this time and then tries to determine if there is a device at the other end of the socket. If a device is found, a new socket is opened. The default for this interval is 15 seconds, but it can be set from 5 to 30 seconds.

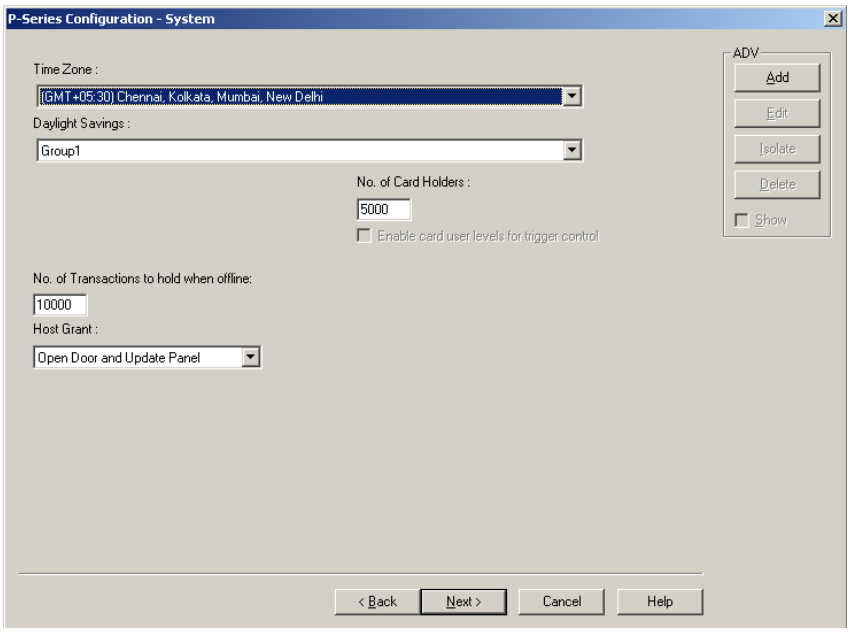
d. **IP Address or Node Name of the IC**: The IP address configured for the LAN card or the node name of the Intelligent Controller.

4. Click **Next** to set the system configuration.

Configuring the system settings

To configure the system settings:

1. In the **P-Series Configuration - System** dialog box, select the standard **Time Zone** for setting the time zone for the PRO-2000 Intelligent Controller.



2. Select the **Daylight Savings** group for setting the daylight saving option in the P-Series Intelligent Controller.

   Refer to the "Daylight Saving Group" section in the chapter Time Management for more details on configuring daylight saving groups.

3. In the **No. of Card Holders** text box, specify the maximum number of card holders details to be stored based on the memory available in the board. By default, you can store details of 5000 card holders in controller.

4. Select the **Enable card user levels for trigger control** to trigger certain controls on the usage of specific cards.

5. In the **No. of Transactions to hold when offline** text box, specify the number of transactions to be buffered in the controller. By default, you can store 10000 transactions in a buffer storage. This number is decreased or increased to provide more or less memory for cards if necessary.

   1 transaction = 16 bytes (so 100,000 transactions takes up 1.6 MB of memory)

   1 card record = within 20 to 80 bytes. This depends upon the use of precision access levels versus multiple access levels, and the number of card readers per Intelligent Controller.

   Tip: Adding an extended memory board to the Intelligent Controller provides more memory to work with.

6. Select the **Host Grant** option to provide fault tolerance, even if the card is not found in the panel device.

   - Host Grant options are used when, for example, a number of cards are entered in the database, but not yet downloaded to the panel.
   - The available options are:
     - **Disable** - Does not allow the card holder, if the card is not found in the panel.
     - **Open Door** - Enables the door to open, even if the card is not found in the panel.
     - **Open Door and Update Panel** - Enables the door to open and also to download the card details to the panel. Therefore, the panel is updated.

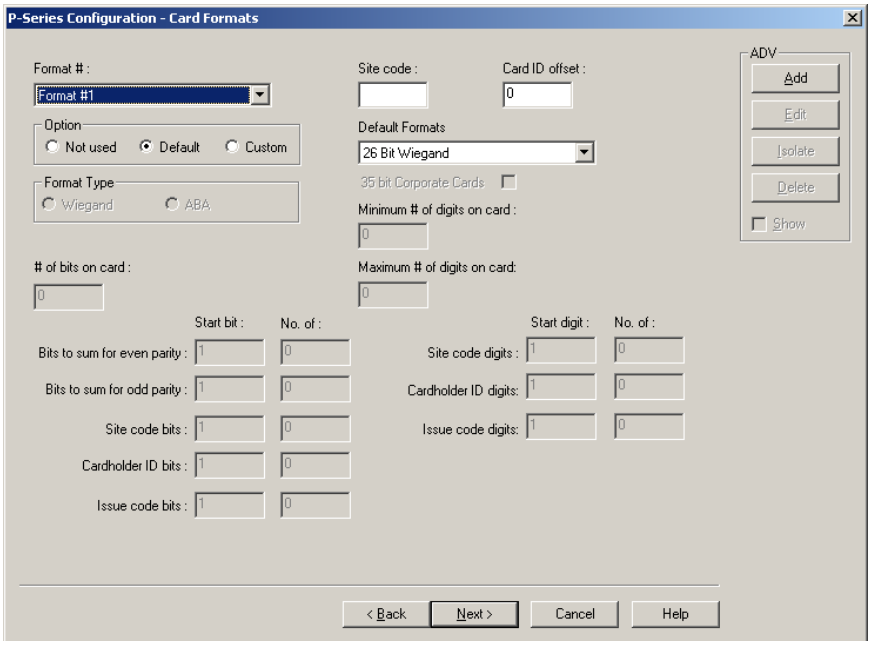
7. Click **Next** to set the card formats for the P-Series panel.

Configuring card formats

The available card format types for P-Series panels are Wiegand and ABA. The first three formats are set by default, however, you can set the other card formats using the Custom option.

To configure the card format:

1. In the **P-Series Configuration - Card Formats** dialog box, select a card format to be used for the panel, in the **Format #** list. The format number ranges from 1 through 8.



2. Under **Option**, select the following options:
    a. **Default**: To view the default settings for the card format. Selecting this option enables you to set the **Site Code**, **Card ID offset**, and the **Default Formats**.
    b. **Custom**: To define the customized settings for the card format. Selecting this option enables you to set Format Type of the card and other properties of the card like site code, number of bits on card, and so on.
    c. **Not Used**: To prevent the usage of card formats for the P-Series panel. If you select this option, all the fields are disabled.
3. Click **Next** to configure time zones for the panel.

Configuring ABA card format

This section helps you to configure the 12-digit ABA card format for the P-Series Intelligent Controller.

To configure the 12-digit ABA card format:

1. In the **P-Series Configuration - Card Formats** dialog box, select the default card formats (Format #1, Format #2 and Format #3) and set each format as **Not Used**.
2. Then select **Format #4** and set the **Custom** option to set the ABA card format.
3. Select the **Format Type** as **ABA** and set the following:

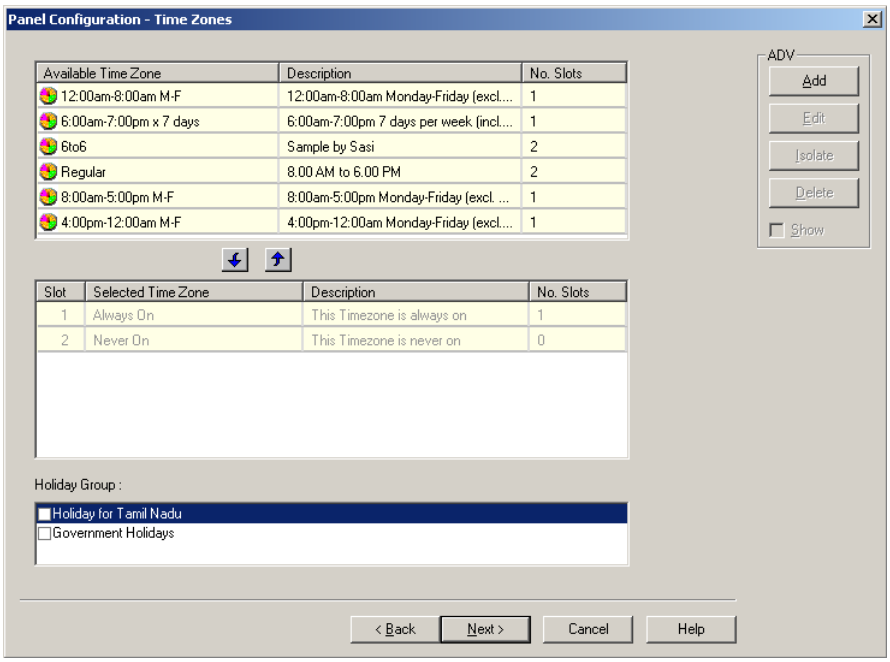
Site Code	No value
Card ID Offset	0
35 bit Corporate Cards	Cleared
Minimum # of digits on card	1
Maximum # of digits on card	12
Site code digits	**Start digit**: 1 **No of**: 0
Cardholder ID digits	**Start digit**: 1 **No of**: 12
Issue code digits	**Start digit**: 1 **No of**: 0

4. Click **OK** to save the ABA format configuration details.

Assigning time zones and holiday groups to a panel

To assign time zones and holiday groups:

1. In the **Panel Configuration - Time Zones** dialog box, select the time zones from the **Available Time Zone** list and click . The time zones are moved to the **Selected Time Zone** list. For multiple selections use the SHIFT and CTRL keys.



Tip: If you want to remove a time zone from the Selected Time Zone list, select the time zone and click .

The time zones that are listed in Selected Time Zone are available for readers, inputs and outputs of this panel.

2. If you are using holiday overrides, select the holiday group in the **Holiday Group** list.
3. Click **Next** to set the panel options. The **Panel Configuration - Options** dialog box appears.

Adding SIO boards to Intelligent Controller

The number of readers, inputs, and outputs that can be connected to the controller is based on the type of SIO Board that is added to the Intelligent Controller. The available SIO Board types are:

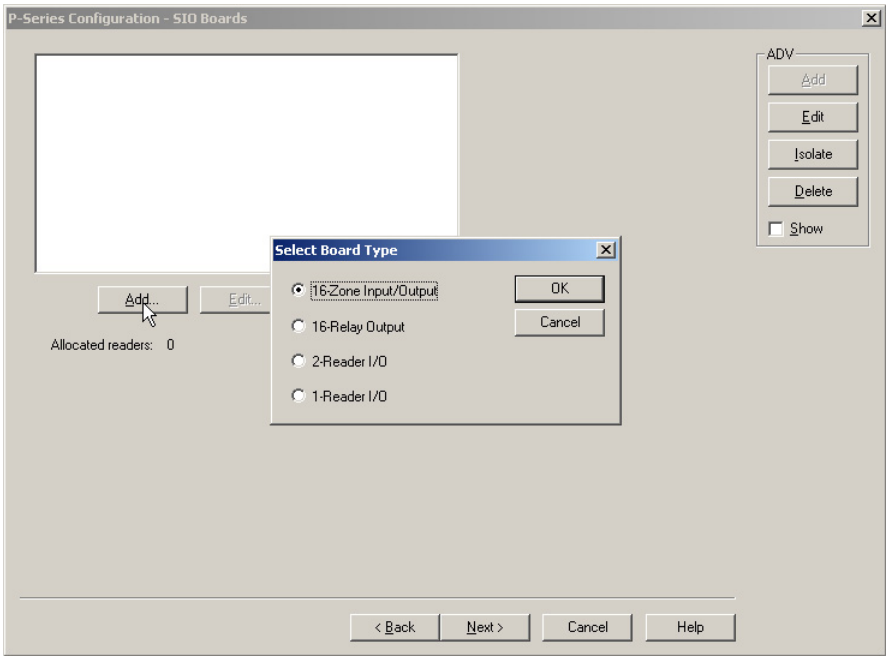
SIO Board Type	Maximum Inputs	Maximum Outputs	Maximum Readers
16-Zone Input/Output	16	2	0

SIO Board Type	Maximum Inputs	Maximum Outputs	Maximum Readers
16-Relay Output	0	16	0
2-Reader I/O	2	8	6
1-Reader I/O	1	2	2

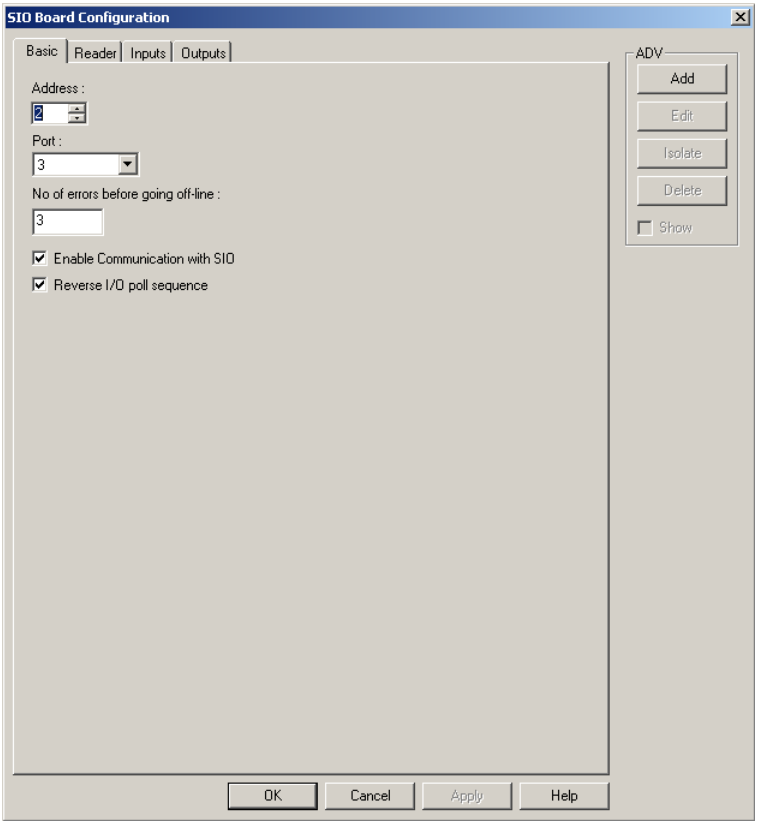
This section explains how to add an SIO board of 2-Reader I/O board type. You can use the same procedure for adding other types of SIO board.

To add an SIO board of 2-Reader IO board type:

1. In the **P-Series Configuration - SIO Boards** dialog box, click **Add**. The **Select Board Type** dialog box appears for you to select the SIO board type.

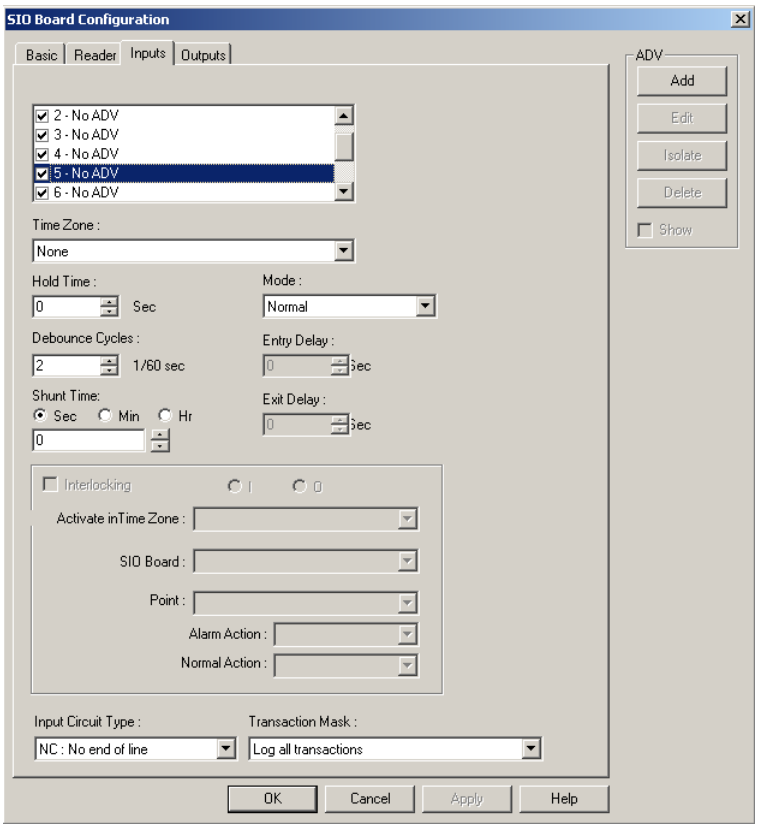


2. In the **Select Board Type** dialog box, select the **2-Reader I/O** board type.
3. Click **OK** to configure the basic information of SIO Board. The **SIO Board Configuration** dialog box appears.
4. Click the **Basic** tab. It is displayed by default.



5. Type a unique **Address** for the SIO Board.
6. In the **Port** list, select the port from which the board communicates with the Intelligent Controller.
7. In the **Number of Errors before Going Off-Line** field, type a number of attempts the panel must make to communicate with the communication server before tripping the offline trigger. This field defaults to 3.
8. Select the **Enable Communication with SIO** check box for enabling connection with the SIO Board. Select this check box, only if the board is installed.
9. Select the **Reverse I/O poll sequence** check box to reverse the sequence in which the inputs and outputs are polled.
10. Create an ADV for the selected board type. Click **Add** under **ADV** and set the ADV properties.

    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
11. Click the **Input** tab to configure the input point details of SIO Board.



12. Select the check box to select an input point and create an ADV. Here you can decide on the alarm or trouble condition of an input point.

    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

Note: You cannot disable or deactivate the status input or the free egress input of the reader. If you still want to disable these inputs, you must change the status input or free egress input of the reader before disabling.

For 2 readers SIO board, In 1 and In 3 are status inputs and In 2 and In 4 are free egress inputs. Whereas for 1 reader SIO board, In 1 is the status input and In 2 is the free egress input.

Refer to the "Free egress input" and "Status input" sections in this chapter for more details on free egress input and status input.

13. In the **Time Zone** list, select a time zone during which input point must be shunt or deactivated.

14. Type the **Hold Time** to report the Normal state of the input point only after a specified duration. By default, it is set to zero.

Note: The reporting of the Input point Normal state is delayed for a period (hold time), when the input returns to normal condition from the alarm or trouble condition.

15. Enter the debounce cycle time in **Debounce Cycles**. If an input point state changes before the debounce time, the change is not reported. Debounce time can be set from 2/60 through 15/60 of a second.

    Example: If the debounce time is set to 4 and if the Alert state of the input point changes to the Normal state before the debounce time, the Alert state is not reported.

16. In **Shunt Time**, select **Sec**, **Min**, or **Hr** and specify the shunt time. By default, the field is set to zero, but can be set from 0 through 32400 seconds, 0 through 540 minutes, 0 through 9 hours.

17. In the **Mode** list, select the mode of input point.

Table 11-4 Describing the modes of input point

Mode	Description
Normal	The input acts normal reporting alert, normal and troubled states.
Non-Latching	**Entry**: A door is set up as an input point, with an entry delay of 10 seconds. If the door remains open more than 10 seconds, it is reported. **Exit**: The exit delay is the amount of time a contact can be unshunted (unmasked) before being reported.
Latching	**Entry**: If a door-set up as an input point, with an entry delay of 10 seconds, the card holder has 10 seconds to shunt the point, otherwise it reports as an alarm. Even if the point returns to normal before the entry delay time, if the point has not been shunted (masked), it reports as an alarm. **Exit**: The exit delay is the amount of time a contact can be unshunted (unmasked) before being reported.

18. Enter the entry delay time in **Entry Delay**. This is the duration an input point can remain open before an alarm is activated. This field defaults to zero seconds, but can be set up to 255 seconds.

19. Enter the exit delay time in **Exit Delay**. This is the duration a point can be unshunted (unmasked) before being reported as an alarm. This field defaults to zero seconds, but can be set up to 255 seconds.

Note: The **Entry Delay** and **Exit Delay** fields are enabled only for Latching and Non-Latching mode of input points.

20. Select the **Interlocking** check box to activate the interlocking for a particular input point.

    Refer to the "Interlocking Points on SIO Board" section in this chapter for more details on interlocking.

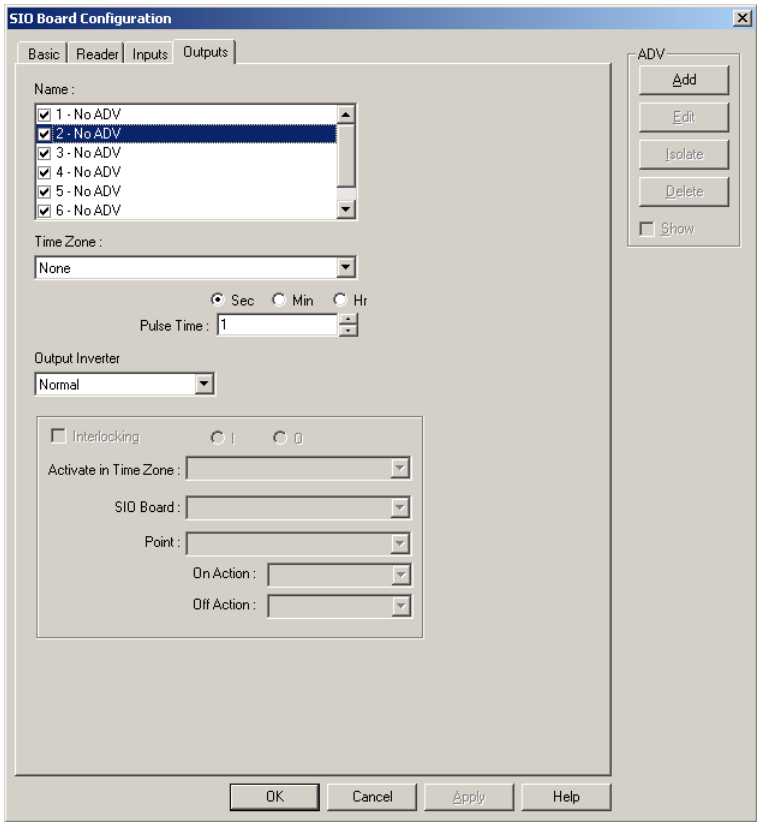
21. Select the **Input Circuit Type** for specifying whether a point is supervised or unsupervised. The available types are:

Table 11-5 Describing Input Circuit Types

Input Circuit Type	Description
NC: No end of line Normally Closed	Refers to contact points that always touch when a device is in its normal position. A normally closed device, such as most door contacts, complete a circuit when they are in their normal, at rest condition.
NO: No end of line Normally Opened	Refers to contact points that do not touch when a device is in its normal position. A normally open device, such as most REX switches, complete the circuit when pushed.
NC: Std end of line Normally Closed	Refers to a three-state circuit (Alert, Normal, or Trouble) in a normally closed contact points.
NO: Std end of line Normally Opened	Refers to a three-state circuit (Alert, Normal, or Trouble) in a normally opened contact points.

22. In the **Transaction Mask** list, select the type of transaction mask that enables masking for the log of transaction information related to input points. By default, it is **Log all Transactions**, indicating that all input points are monitored and all transaction is logged to WIN-PAK.

23. Click the **Output** tab to configure the output point details of SIO Board:



24. Select the check box to select an output point and create an ADV.

    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

25. In the **Time Zone** list, select a time zone during which the output point must be shunt or deactivated.

26. Select **Sec**, **Min**, or **Hr** and enter a value in the **Pulse Time** field to set the amount of time that the output point is energized when triggered. By default, the field is set to zero, but can be set from 0 through 32400 seconds, 0 through 540 minutes, 0 through 9 hours.

27. In the **Output Inverter** list, select a default setting for the output:

Table 11-6 Describing the Output Inverter settings

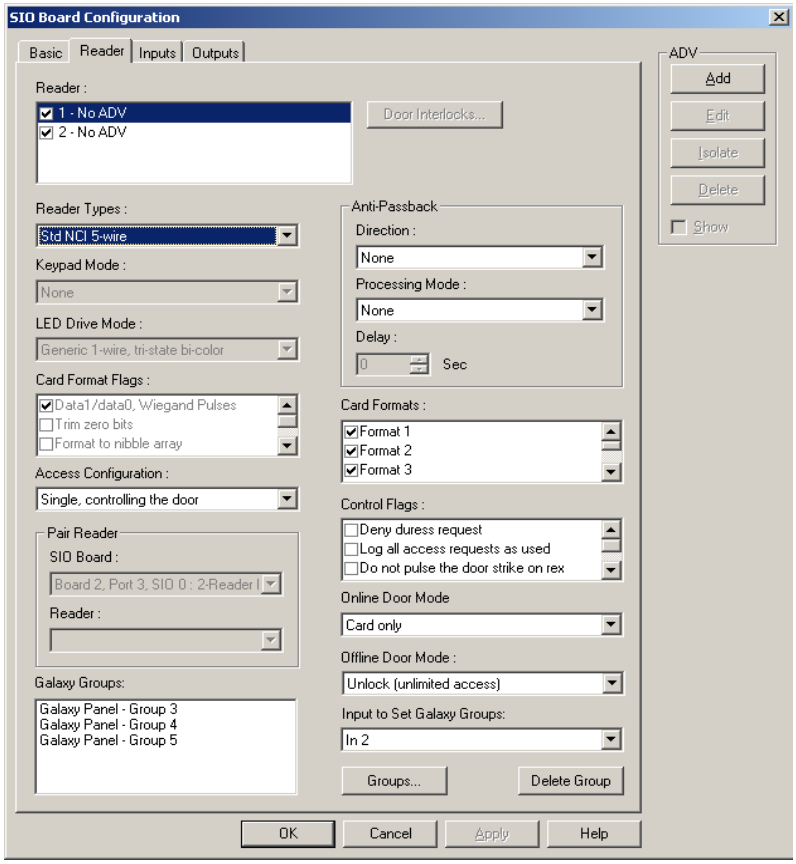
Output	Setting
Normal	• Relay defaults to a de-energized state. • Pulsing the output energizes it for its designated pulse time (or pulses the output on). At the end of the pulse time, the output de-energizes. (The output responds the same upon a valid egress, a valid card read, and/or a manual pulse command.) • Energizing a relay turns the relay on (LED on). • De-energizing a relay turns the relay off (LED off). • Normally Open circuit acts as a NO circuit; Normally Closed circuit acts as an NC circuit.
Inverted	• Relay defaults to an energized state. • Pulsing the output de-energizes it for its designated pulse time (or pulses the output off). At the end of the pulse time, the output re-energizes. (The output responds the same upon a valid egress, a valid card read, and/or a manual pulse command. • Energizing a relay turns the relay off (LED off). • De-energizing a relay turns the relay on (LED on). • Normally Open circuit acts as a Normally Closed circuit; Normally Closed circuit acts as a Normally Open circuit.

28. Select the **Interlocking** check box to activate the interlocking for a particular output point.

    Refer to the "Interlocking Points on SIO Board" section in this chapter for more details on interlocking.

29. Click the **Reader** tab to configure readers for SIO board.

Note: While configuring readers, you can associate galaxy groups or vista partitions to the reader and the input point. If you associate galaxy groups or vista partitions, after the association you can set or unset galaxy groups or arm or disarm vista partitions using the privileged card. To set the galaxy groups or arm the vista partitions associated to the reader, you must present the privileged card to the reader and press the input button. However, to unset the galaxy groups or disarm the vista partitions, you must present the privileged card to the reader.



30. Select a reader and create an ADV for the reader.

    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

31. In the **Reader Types** list, select the type of reader.

Note: The available reader types are Std NCI 5-Wire, Std Motorola, Std Mercury, and Std HID. If you select these types, the Keypad Mode, LED Drive Mode, and Card Format Flags default to pre-defined settings. However, if you want to set the reader settings, select **Custom** in the list.

32. If **Custom** is selected as the reader type, select a **Keypad Mode**. This keypad mode includes the following:

    - **MR-20 8-bit** with (or without) tamper support, which represents a Mercury Magstripe reader with keypad attached
    - **Hughes ID 4-bit**
    - **Motorola/Indala** which sends an 8-bit key code)

33. Select the **LED Drive Mode** for the reader. The default is **Generic 1-wire, tri-state bi-color**. Alternatively, you can select **Separate red and green, no buzzer** dependent on the physical reader.

34. Select the **Card Format Flags**, which represent how the reader must interpret the access card to be used.
35. Select the **Access Configuration** option to define the reader access in a door.
    - **Single, controlling the door**: The door is defined by only one reader.
    - **Paired, primary reader**: The door is defined by two readers in which this reader becomes a primary reader.
    - **Paired, secondary reader**: The door is defined by two readers in which this reader becomes a secondary reader. Selecting this option disables the **Door Interlocks** button.
36. Under **Pair Reader**, select the SIO Board and the corresponding reader which pairs with this for defining a door. Pair Reader is enabled, only if you define a door by two readers. In that case, you must select the other reader.
37. Click **Door Interlocks** for configuring door interlock. The Door Interlocks dialog box appears.

    Refer to the "Door Interlocks" section in this chapter for more details on door interlock.
38. Anti-Passback discourages card holders to enter without using their cards. Under **Anti-Passback**, select the Direction and Processing Mode for the anti-passback.
    - Direction enables you to specify if the reader is in or out. (It is None by default.)
    - Processing Mode enables you to specify the processing mode of the reader:
        - **Hard**: When an anti-passback violation occurs, the reader strictly restricts the access.
        - **Soft**: When an anti-passback violation occurs, the reader allows the access but sends a report on anti-passback violation.
        - **Reader Based Timed APB**: A card cannot be swiped twice at the same Anti-Passback reader, before the time specified for the delay.
        - **Card Based Timed APB**: A card cannot be swiped twice anywhere in the system, before the time specified for the delay.
        - **Panel Based Timed APB**: A card cannot be swiped twice at the same panel, before the time specified for the delay.

39. Select the following **Control Flags**:

Table 11-7 Describing Control Flags

Control Flag	Description
Deny a duress request	Works in a card and PIN mode only. Unless this option is selected, duress is always enabled. Notify the monitoring station you are under duress. Always one number higher than the PIN code.
Log all access requests as used	If selected, logs all card reads as “door used”, without actually determining if the door is used. If unchecked, logs all card reads, but waits until the door times out, or the door is opened, to report. Cancel this option when using anti-passback.
Do not pulse the door strike on rex	Door strike does not pulse upon free egress, however, door contact still gets shunted.
Filter CosDoor transaction	Throughout the door cycle the IC generates about 4 to 5 messages (door strike relay on, door strike relay off, door opening, and son.). If more message are needed, this feature can be disabled.
Require two-card control at this reader	Needs 2 valid cards within a 20 second window to grant access. Used in vaults, high security areas.

40. Select the following **Online Door Mode** that indicates the mode in which the Intelligent Controller is operating:

Table 11-8 Describing Online Door Mode options

Online Door Mode	Description
Card Only	The card is sufficient for door access.
PIN Only	The PIN number is sufficient for door access.
Card and PIN	Both card access and PIN are required for door access.
Card or PIN	Either card or PIN is sufficient for door access

41. Select an **Offline Door Mode** that indicates the mode in which the SIO Reader board will run if the system goes offline. The available options are Disable the reader, Unlock, Locked, and Facility code only.

42. To associate galaxy groups or vista partitions to this reader, click **Groups/Partitions** and select the groups from the list.

Note: To dissociate the galaxy group or vista partition from the reader, select the galaxy group or vista partition and click **Delete Grps/Partitions**.

43. To associate galaxy groups or vista partitions to the input point, select the input point from the **Input to Set/Arm Galaxy Grps/Partitions** list.

Note: Only the input points that are configured in this panel and not interlocked are listed in the **Input to Set/Arm Galaxy Grps/Partitions** list.

44. Click **OK** to configure the SIO Board.

45. Click **Next** to configure triggers and procedures.

    Refer to the "Configuring triggers and procedures" section in this chapter for details on triggers and procedures.

Interlocking Points on SIO Board

Interlocking enables you to interlock an input or output point within the SIO Board points or across other SIO Board points.

To interlock an input or output point:

1. In the **SIO Board Configuration** dialog box, click the **Inputs** or **Outputs** tab.
2. Select an **Input point** or **Output point**.
3. Select the **Interlocking** check box to activate the interlocking for a particular input point.
4. Select **I** (input point) or **O** (output point) to interlock the input point with an input point or output point of the SIO Board.
5. In the **Activate a Time Zone** list, select a time zone during which the interlock must be active.
6. Select the **SIO Board** in which you want the input or output point to be interlocked.
7. In the **Point** list, select the interlocking input point, output point, or reader, of the selected SIO Board.
8. In the **Alarm Action** (for an input point) or **On Action** list, select an action to be taken when the interlocked point raises an alarm (Alert state) or becomes active. The actions include:
   - **No Action** - Take no action
   - **Energize** - Turn the point on
   - **De-Energize** - Turn the point off
   - **Pulse On** - Energize the point for a particular period
   - **Pulse Off** - De-energize the point for a particular period.
9. In the **Normal Action** (for input point) or **Off Action** list, select an action to be taken when the interlocked point becomes Normal state or becomes inactive.

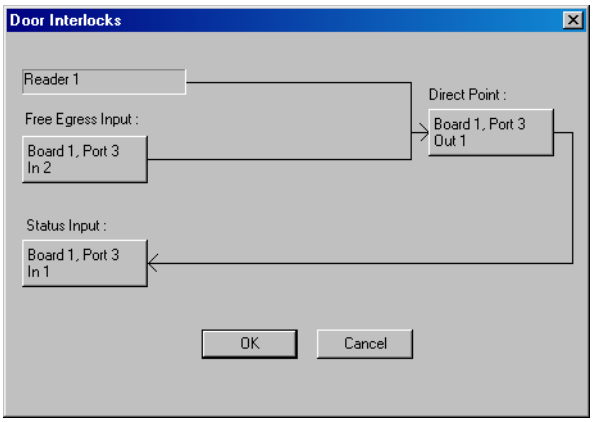
Door Interlocks

Door Interlocks show input and output relationships available for the reader. Two types of locking devices can be configured with WIN-PAK PE:

- Magnetic Locks - which require power for the door to be closed.
- Door Strikes - which require power for the door to be opened.

To configure door interlock:

1. In the **SIO Board Configuration** dialog box, click the **Reader** tab.
2. Click **Door Interlocks** to display the **Door Interlocks** dialog box.



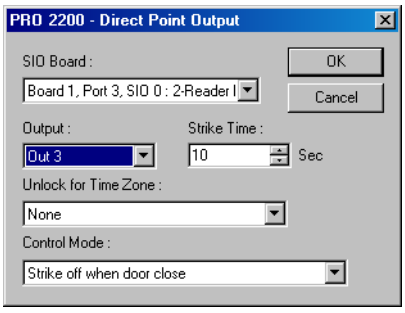
3. Use this dialog box to edit the default settings of the Direct Point, Free Egress Input, and Status Input as desired.

Note: When you click **Door Interlocks**, WIN-PAK automatically determines the appropriate inputs for status and REX devices.

Direct point

The Direct Point indicates the output that will be directly controlled by the reader.

1. In the **Door Interlocks** dialog box, click **Direct Point** to display the **Direct Point Output** dialog box.



2. Select an **SIO Board** with which you configure the direct point.
3. Select an **Output** that has to be used as the door output or door lock.

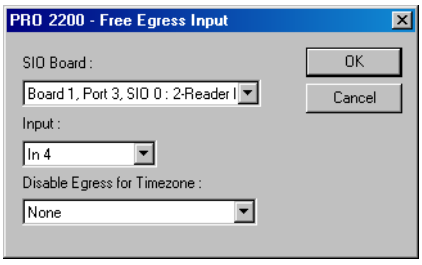
Note: The **Output** list contains, only active output points that have not been added as ADVs. The contents of the list depend on the SIO Board selected.

4. Specify the **Strike Time**. This is the amount of time the direct point relay is pulsed or interlocked. The default for this field is ten seconds, but can be set up to 60 seconds.
5. In **Unlock for Time Zone** list, select a Time Zone during which the door must be kept unlocked.
6. Select the **Control Mode**. This is an auto-relock function. By default, the field is set to **Strike off when door closed**, but can be set to strike off when door is opened.
7. Click **OK** to return to Direct Interlocks dialog box.

Free egress input

Free Egress Input is used for indicating which input must be used for the Free Egress device, and for configuring a door's free egress point. Free Egress Input can only be linked to an input point.

1. In the **Direct Interlocks** dialog box, click **Free Egress** Input. The **PRO 2200 - Free Egress Input** dialog box appears.



2. Select the **SIO Board** with which you want to configure the free egress point.
3. Select the **Input** that you want to use as the Free Egress Input.

Note: The **Input** list contains only active input points that are not added as ADVs. The contents of the list are dependent upon the SIO Board selected.

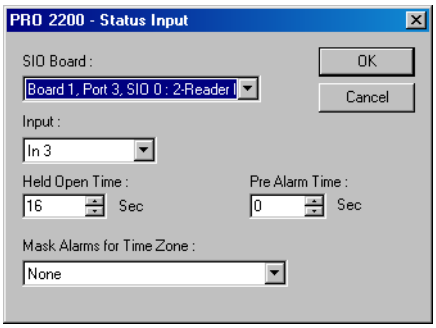
4. In the **Disable Egress for Time Zone** list, select a time zone during which the Egress is disabled.
5. Click **OK** to return to Door Interlocks dialog box.

Status input

Status Input indicates the status of the door such as normal, closed, forced open, ajar, and so on. The Status Input may only be linked to an input. It is normally connected to a door position sensor, such as a magnetic door contact to detect the status of the door (open, closed, and so on.).

Note: Input 1 (with Inputs 2, 3, and 4) is reserved by WIN-PAK for use in controlling doors.

1. In the **Door Interlocks** dialog box, click **Status Input** to display the **Status Input** dialog box.



2. Select an **SIO Board** with which you want to configure the status point.
3. In the **Input** list, select an input used as the door status input. Only active input points that have not been added as ADVs appear on this list. The contents of the list depend on the SIO Board selected.
4. Select the **Held Open Time**. This is the time that elapses after the door is opened, before the door is reported as ajar. By default, this field is set to 16 seconds.
5. Specify the **Pre Alarm Time** if required. Pre Alarm Time is the time that elapses after the door is opened, before a warning (typically a beeping sound) indicates that the alarm is activated.

   Note: Consider a door with a **Held Open Time** set at 30 seconds and a Pre Alarm Time also set at 30 seconds. As soon as the door opens on a valid card read, a beeping sound is emitted (the Pre Alarm) indicating that an alarm is imminent. At the end of the 30 second **Held Open Time**, the alarm is activated.
6. In the **Mask Alarms for Time Zone** list, select a time zone during which the alarms must be masked.
7. Click **OK** to return to the Door Interlocks dialog box.
8. Click **OK** to save door interlocks.

Configuring triggers and procedures

In response to a panel event (trigger), define a set of actions a panel must carry out. The occurrence of the event triggers the execution of the procedure.

- Triggers and procedures are used to define interlocks (an action on a point triggered by an action on a different point).
- Assigning points and readers to time zones can also be done through triggers and procedures on the P-Series Intelligent Controller.
- User triggers are those defined for site-specific events and actions.

- User triggers are added, edited, or deleted at any time from the Triggers and Procedures dialog boxes of the P-Series Configuration dialog boxes.
- System triggers are those created when points are assigned to interlock definitions. System triggers can only be viewed and cannot be edited in Triggers and Procedures dialog box.

System Triggers and Procedures

System triggers and procedures are created as a result of an interlock defined on one of the P-Series Configuration SIO Board Inputs or Outputs tabs. After an action is assigned to an interlock point, two system triggers and procedures are created to correspond to the interlock. One trigger and procedure set deals with the “On” action, and the other deals with the “Off” action.

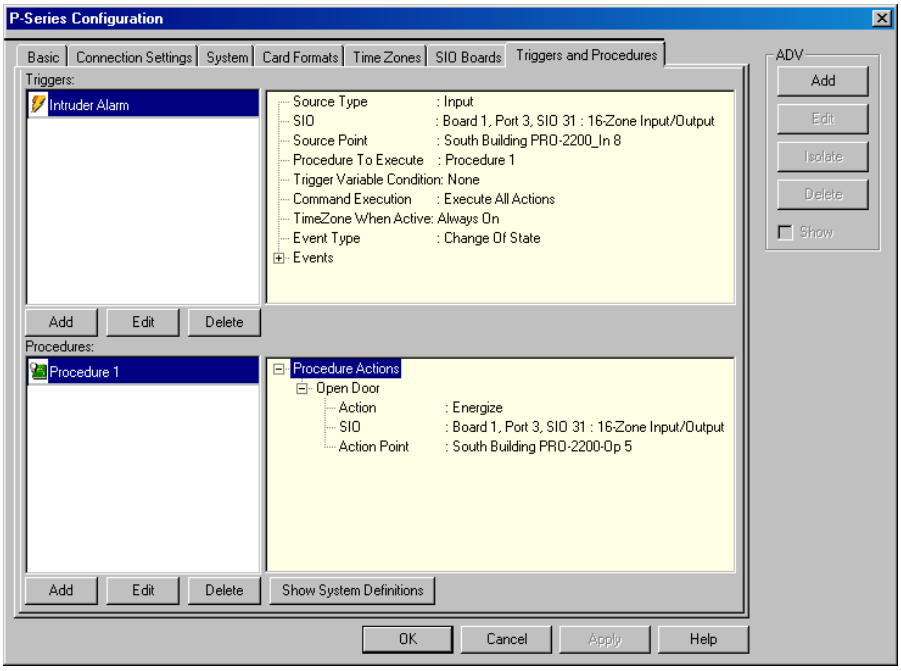
Note: To view the system-defined triggers and procedures, click the **Show System Definitions** button. After you this button, it changes to **Hide System Definitions**, which hides the system-defined triggers and procedures when you click it.

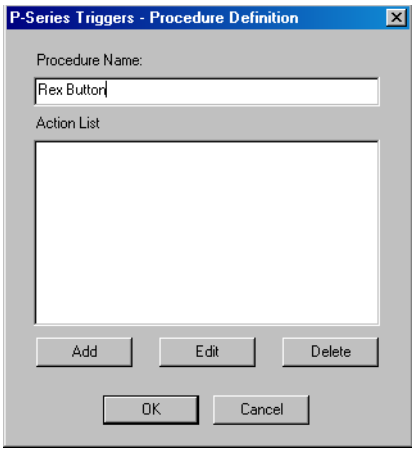
Adding a new procedure

Procedures are assigned to triggers, and therefore, are defined first. Use the Procedure Definition dialog boxes to build a script of actions that take place based on the event (trigger) to which the procedure is linked. Procedures are limited by the type of device or point defined.

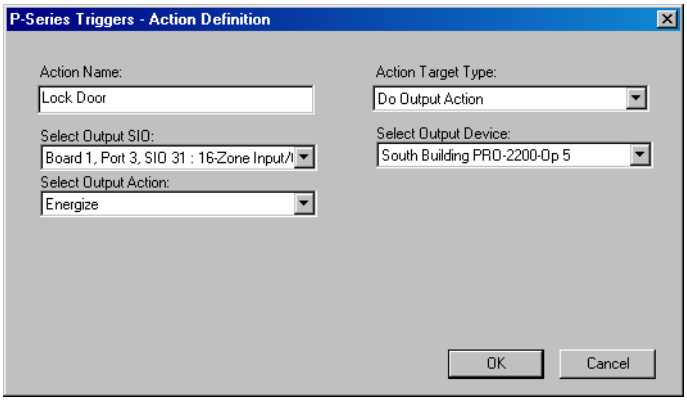
To add a new procedure:

1. In the **Triggers and Procedures** dialog box, click **Add** at the bottom of the Procedures section. The **Procedure Definition** dialog box appears.





2. Enter a **Procedure Name**. This name is unique and descriptive for easy reference.
3. To define a new action for the procedure, click **Add** at the bottom of the **Action List** box. The **Action Definition** dialog box appears.



4. Type an **Action Name**.
5. In the **Action Target Type** list, select the target of the action: Reader, Output, Input, Delay.

   The remaining fields in the dialog box are activated, based on the selected action target type.
6. If you select **Do Output Action** as an Action Target Type, perform the following steps:

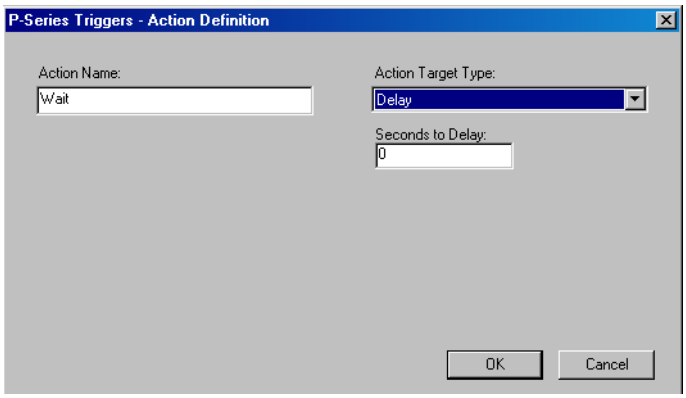
   a. In the **Select Output SIO** list, select the SIO board on which the output action must occur.

   b. In the **Select Output Device** list, select a point on which the output action must occur.

   c. In the **Select Output Action** list, select an action to be performed.

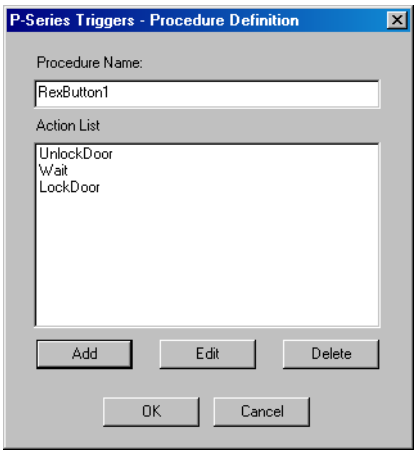
   d. Click **OK** to return to the Procedure Definition dialog box.

7. If you select **Delay** as an Action Target type, perform the following steps:
   a. In **Seconds to Delay** box, type the number of seconds to delay for proceeding to the next action.

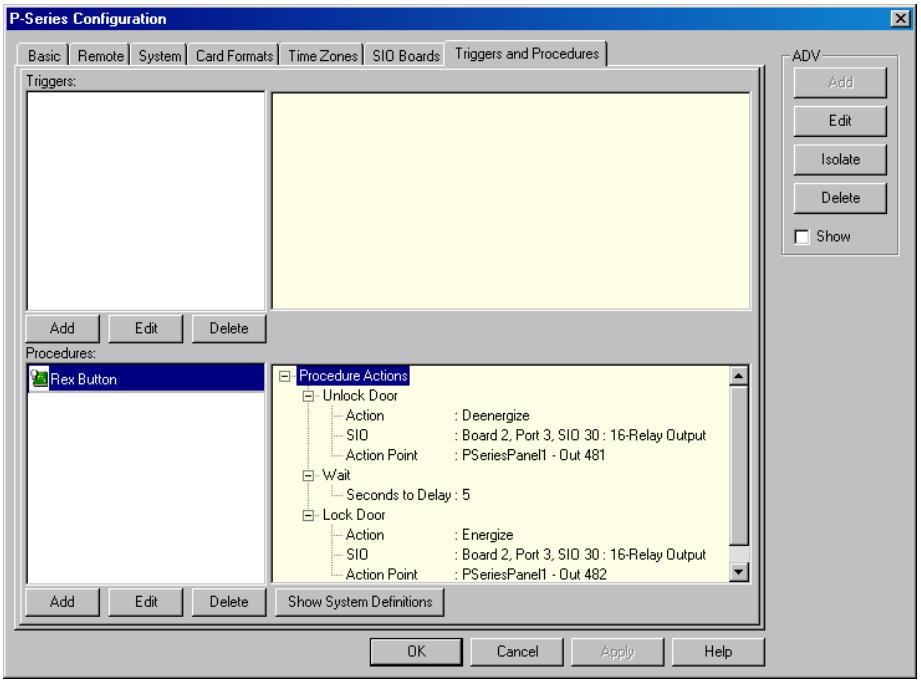


   b. Click **OK** to return to **Procedure Definition** dialog box.

After you define the procedures, the actions are listed in the **Procedure Definition** dialog box.



8. Click **OK** to return to the **Triggers and Procedures** dialog box.



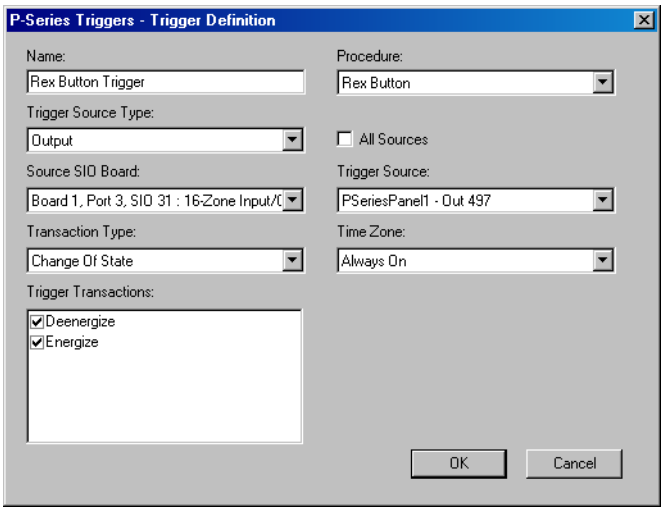
Tip: The newly-defined procedure is shown in the Procedures list. To look at the detailed view of each action defined for this procedure, expand the **Procedure Actions** tree.

Adding a new trigger

After defining the procedures, it must be associated to a trigger for triggering an action.

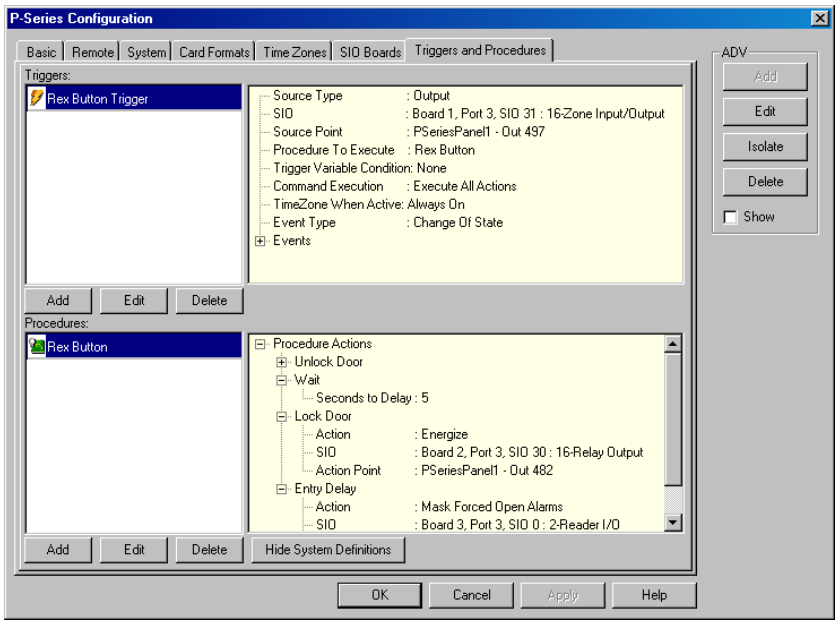
To add a new trigger:

1. Click **Add** at the bottom of the Triggers section of the Triggers and Procedures dialog box. The **Trigger Definition** dialog box appears.



2. Enter a **Name** for the trigger. This name relates to its corresponding procedure.
3. Select a **Procedure** in the list. Only user-defined procedures (as opposed to system procedures) are displayed in this list.
4. In the **Trigger Source Type** list, select the type of trigger point defined (Input, Output, Reader, or Time Zone).
5. Select the **All Sources** check box if you want the trigger to apply to all inputs, outputs, and readers.
6. Select a **Source SIO Board**. Only the boards configured for this panel are displayed in the list.
7. Select a **Source SIO Board** to select the SIO Board in which you want to select a trigger point.
8. In the **Trigger Source** list, select the exact point on the SIO Board that you want to use as the trigger point. The Trigger Source field is activated only if Source SIO Board is selected.
9. Select a **Time Zone** during which the trigger is active. This field defaults to **Always On**.
10. In the **Transaction Type** list, select the type of transaction.
11. In the **Trigger Transactions** list, select the events to associate with the trigger.
12. Click **OK** to save the definition and return to the Triggers and Procedures dialog box.

Note: In the Triggers and Procedures dialog box, you can view the list triggers and procedures. Select the trigger to see its definition on the right side of the window. Click the plus sign (+) to expand the Events view.



13. After you complete adding Triggers and Procedures, click **Next** to advance to the Finish dialog box.
14. Click **Finish** to complete the direct P-Series panel configuration.

Adding P-Series Panel in Modem Pool

The procedures for adding a P-Series panel in a Modem Pool is similar to adding a Direct P-Series panel. When you add a P-Series panel in the Modem Pool, you must provide Remote details of the panel and more details on System settings.

Refer to the "Adding a P-Series Panel" section in this chapter for more details on panel configuration.

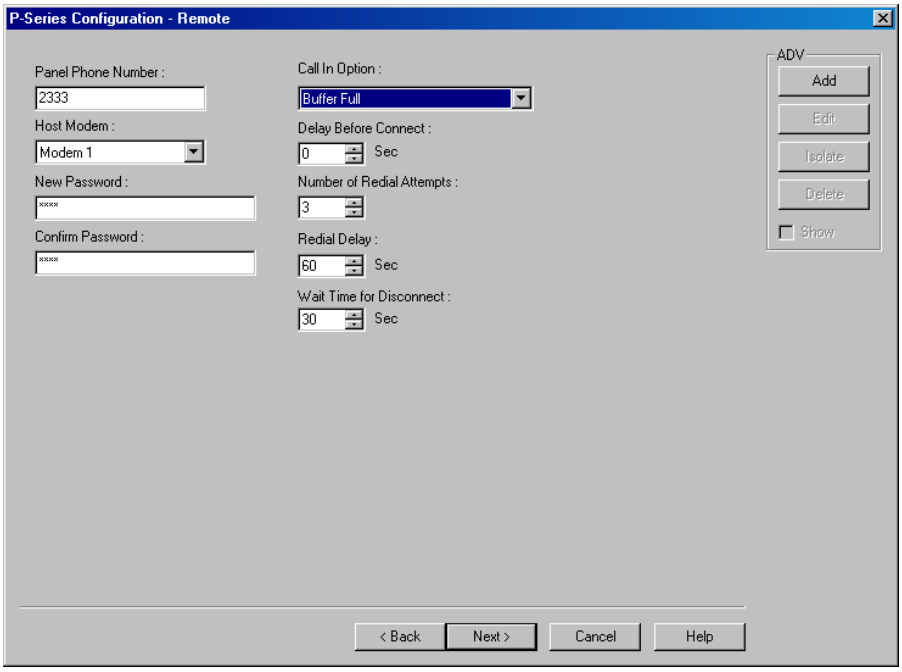
This section helps you in detailing procedures for providing Remote details and System settings.

Configuring remote details

When configuring a P-Series panel on a Modem Pool, the Remote dialog box appears next to the Basic dialog box.

To configure the remote:

1. In the **P-Series Configuration** dialog box, enter the **Panel Phone Number** for the remote site. Enter the number as it would be dialed, including any required prefix or area code. This is the phone number the system uses to connect to the panel.



2. Select a **Host Modem**. The options in this field are those previously entered in the Modem Pool when the interface was set up.

3. In the **New Password** text box, enter a password and re-enter the password in the **Confirm Password** field. WIN-PAK requires a password for remote dial-ups. The password can be up to 16 alphanumeric characters in length.

   Refer to the ***PRO-2200 Intelligent Controller Installation Manual*** for details on setting the password switch.

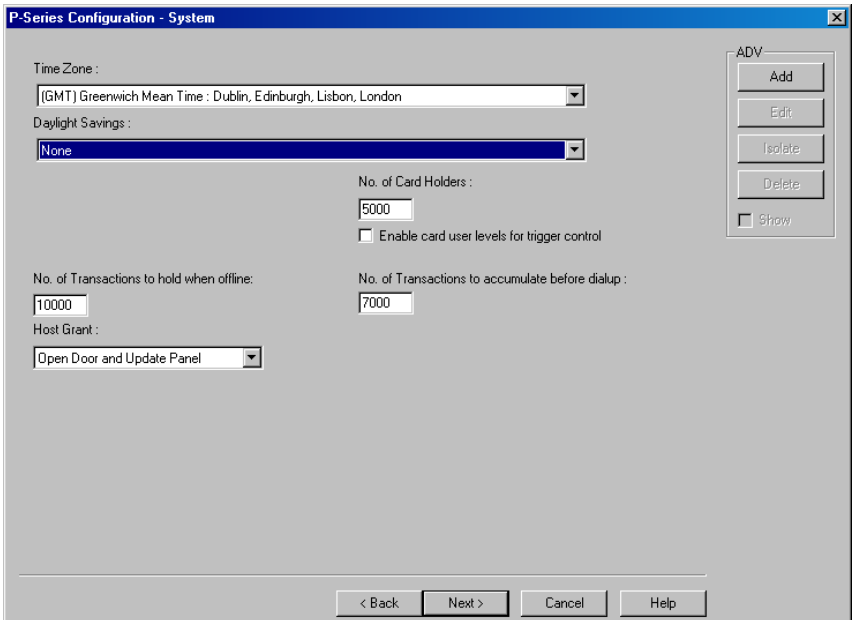
4. In the **Call In Option** list, select an event that determines when the remote panel calls in to the communication server.
5. Enter a value in the **Delay Before Connect** text box, if a pause is required between the dialing prefix and the phone number.
6. Enter the value in the **Number of Redial Attempts** text box. By default, it is set to 3 but can be up to 50.
7. In the **Redial Delay** text box, enter the time allowed between dial attempts. This field defaults to 60 seconds, but you can enter between 5 to 120 seconds.
8. In the **Wait Time for Disconnect** text box, enter the time allowed before disconnecting. By default, it is set to 30 seconds but can be from 1 through 30 seconds.
9. Click **Next** to save the panel remote configuration.

Configuring system settings

Several broad operating parameters are set up using the System dialog box, including those dealing with the PRO-2200 Intelligent Controller board capabilities, as well as the Time Zone in which it operates.

To configure the system settings:

1. In the **P-Series Panel Configuration - Remote** dialog box, click **Next**. The **P-Series Configuration - System** dialog box appears.



2. In the **Time Zone** list, select a standard time zone which indicates the panel location. The default time zone depends on the time set in the local system.
3. In the **Daylight Saving Group** list, select a daylight saving group for this panel. This field defaults to None.
4. In the **No. of Card Holders** field, specify the maximum number of card holders details to be stored based on the memory available in the board. By default, you can store 5000 card holders details in the controller.
5. Select the **Enable card user levels for trigger control** to trigger certain controls on the usage of specific cards.
6. In the **No. of Transactions to hold when offline** text box, specify the number of transactions to be buffered in the controller. By default, you can store 10000 transactions in a buffer storage. This number is decreased or increased to provide more or less memory for cards if necessary.

   1 transaction = 16 bytes (so 100,000 transactions takes up 1.6 MB of memory)

   1 card record = within 20 to 80 bytes. This depends upon the use of precision access levels versus multiple access levels, and the number of card readers per Intelligent Controller.

   Tip: Adding an extended memory board to the Intelligent Controller provides more memory to work with.
7. In the **No. of Transactions to accumulate before dialup** text box, specify the number of transactions to be accumulated in the memory before dialing up.
8. Select the **Host Grant** option to provide fault tolerance, even if the card is not found in the panel device.
   - Host Grant options are used when, for example, a number of cards have been entered in the database, but have not yet been downloaded to the panel.
   - The available options are:
     - **Disable** - Do not allow the card holder, if the card is not found in the panel.
     - **Open Door** - Enables the door to open, even if the card is not found in the panel.
     - **Open Door and Update Panel** - Enables the door to open and also to download the card details to the panel. Therefore, the panel is updated.
9. Click **Next** to set the card formats for the P-Series panel.

   Refer to the "Setting the card format for the panel" section and the following section in this chapter for more details on configuring the P-Series panel.

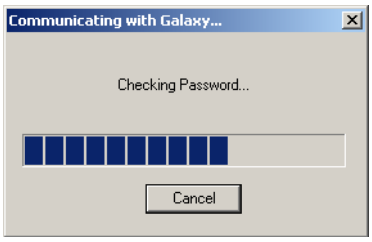
Adding a Galaxy Panel

WIN-PAK monitors and controls the Galaxy panel through the Galaxy panel you add to the Galaxy Ethernet module. When you add a Galaxy panel to WIN-PAK, the Galaxy panel configuration details are downloaded to WIN-PAK.

Note: While downloading configuration details from the panel, ensure that the connection between the panel and WIN-PAK is established. When you download Galaxy panel configuration details to WIN-PAK, the abstract devices for groups, zones, outputs, RIO boards are automatically created. However, you can change the ADV configuration details in the WIN-PAK system.

To add a Galaxy panel:

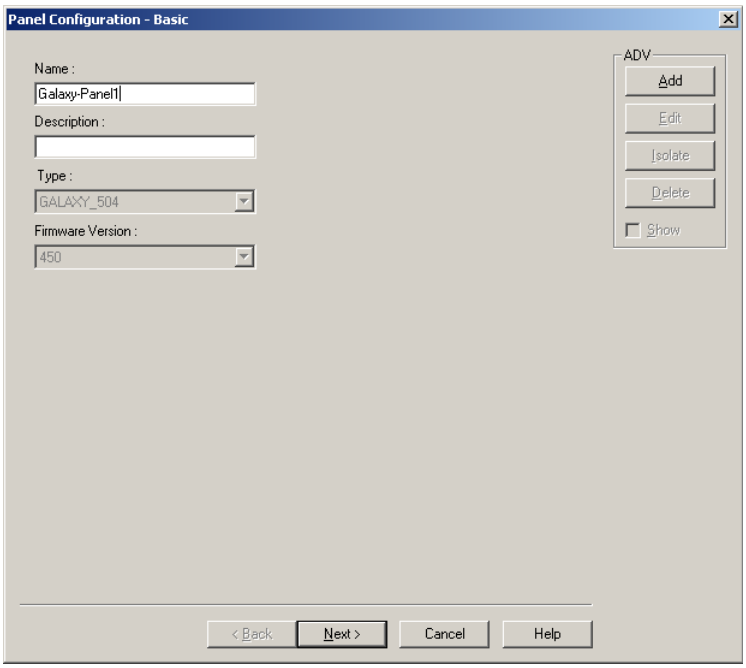
1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the communication server.
3. Right-click the **Ethernet Module Galaxy (Single Panel)** and select **Add New Galaxy Panel**. The WIN-PAK system starts communicating with the Galaxy panel to establish the connection and download configuration details to WIN-PAK.



4. After the panel configuration details are downloaded, the **Panel Configuration - Basic** dialog box appears. Enter the basic details of the panel such as Name and Description.

Entering basic details

1. In the **Panel Configuration - Basic** dialog box, type a **Name** and a **Description** for the Galaxy panel.

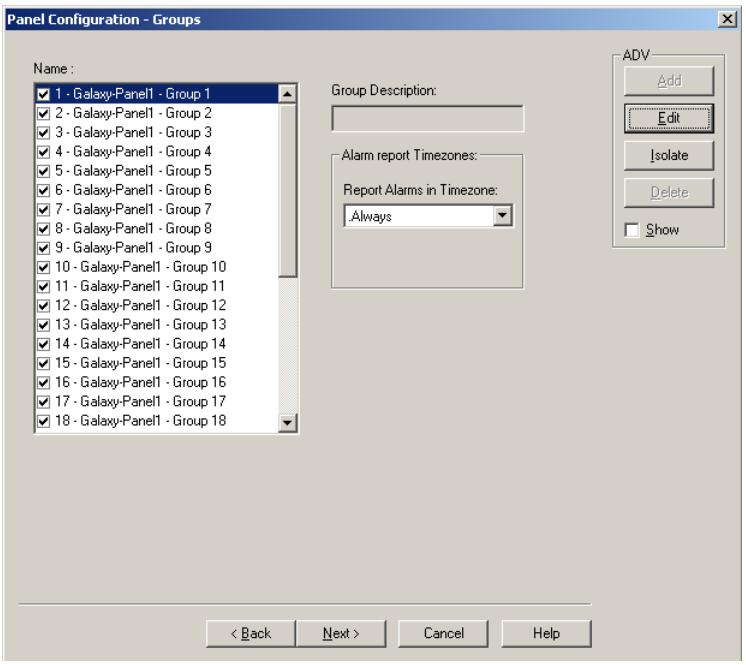


2. Details for **Type** and **Firmware Version** are automatically downloaded from the panel to WIN-PAK.
3. Click **Next** to view the groups in the panel. The **Panel Configuration - Groups** dialog box appears.

Setting panel groups

A set of zones can be grouped in the Galaxy panel and called as groups. A zone is an area covered by the input device in the Galaxy panel. By default, all the zones are grouped under one group and later various groups are configured using the Galaxy Gold User Interface.

1. In the **Panel Configuration - Groups** dialog box, double-click a group in the **Name** list to rename it.



2. Under **Alarm report Timezones**, select a time zone during which the alarms generated from a group must be reported.
3. To edit the group ADV configuration, click **Edit** under **ADV** and edit ADV and action groups.

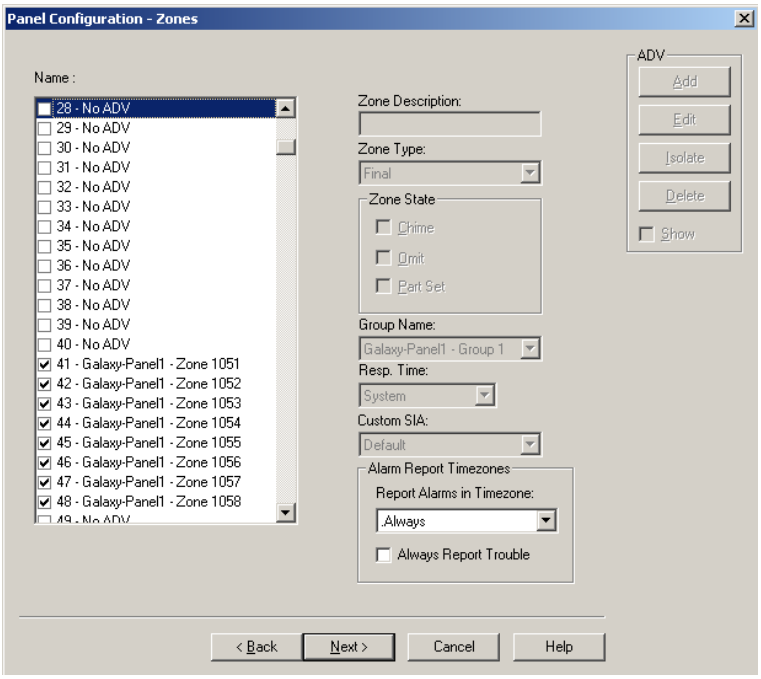
Note: If you want to assign zones to different groups, you must do it in the Galaxy panel and then download it to WIN-PAK.

4. Click **Next** to view the zone configuration details.

Setting panel zones

A zone is the area covered by an input device in the Galaxy panel that monitors intrusions and creates alarms.

1. In the **Panel Configuration - Zone** dialog box, double-click a zone in the **Name** list to rename it.



Note: The Zone Type, Zone State, Group of the zone and other details are displayed on the right. These fields are non-editable.

Table 11-9 Describing Zone properties

Property	Description
Zone Type	The type of the device used in the zone such as Fire, Intruder.
Zone State	The property set for the zone.
	• If **Chime** is selected, the control over this zone from WIN-PAK UI is restricted.
	• If **Omit** is selected, the alarm from this zone is not reported.
	• If **Part Set** is selected, the zone is set as Part Set Zone. In the floor plan or control map, you can set all the zones that are Part Set without setting other zones.
Group Name	The name of the group to which the zone belongs.
Resp. Time	Indicates how quick the panel has to respond to the device. It can be **Slow**, **Fast**, or **System**.
Custom SIA	Custom SIA is a zone type that is used for customizing the user-defined zone types.

2. Under **Alarm Report Timezones**, select a time zone during which the alarms generated from this zone must be reported.

3. Select the **Always Report Trouble** check box to report troubles irrespective of the selected time zone.
4. To edit the zone ADV configuration, click **Edit** under **ADV**.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
5. Click **Next** to view the output configuration details. The **Panel Configuration - Output** dialog box appears.

Setting panel outputs

An output is a device triggered by the input device to indicate a change in the device status. The indication could be an alarm, or an action that normalizes the situation.

For example, in case of glass break, the output device could be a Siren that beeps the alarm sound. In case of fire indication, the output device could be a Sprinkler which sprinkles the water to set off the fire.

1. In the **Panel Configuration - Output** dialog box, double-click an output in the **Name** list to rename it.

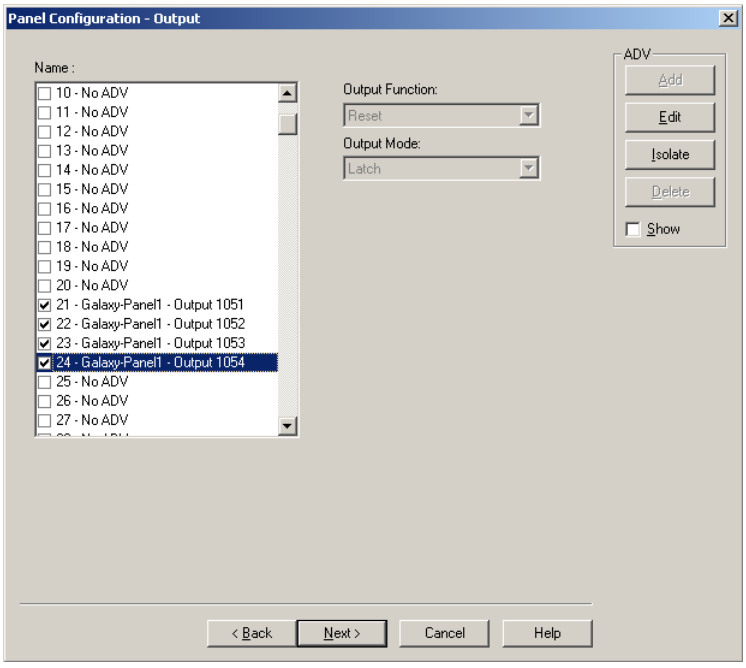


Table 11-10 Describing Output Properties

Property	Description
Output Function	The function to be performed by the output device like beep an alarm.

Table 11-10 Describing Output Properties

Property	Description
Output Mode	The mode in which the output operates such as Latch, Reflex, and Pulse.

2. To edit the output ADV configuration, click **Edit** under **ADV** and edit ADV and action groups.

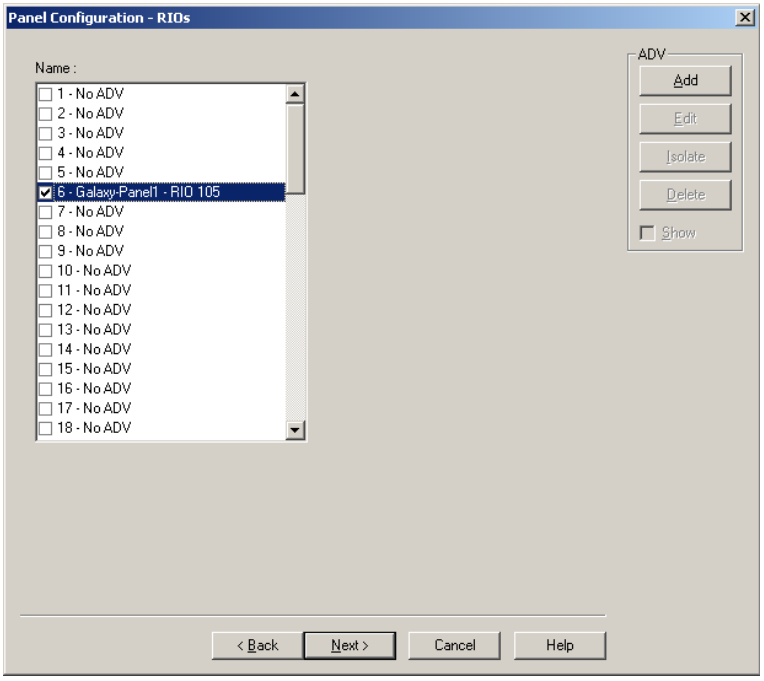
   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

3. Click **Next** to view the RIO board configuration details.

Setting the RIO board

The Relay Input Output (RIO) board is the extendable board used for extending the number of zones or outputs that can be plugged in to the Galaxy panel.

1. In the **Panel Configuration - RIO** dialog box, double-click an RIO board in the **Name** list to rename it.



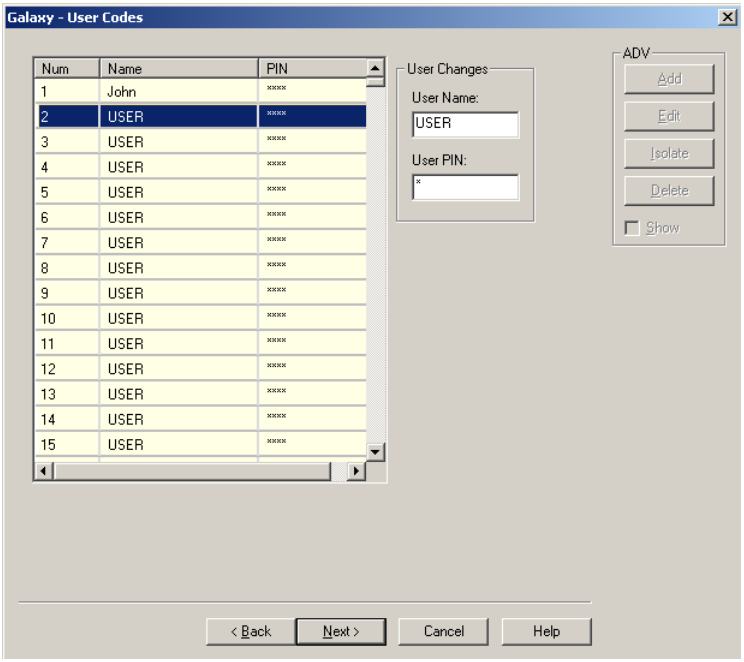
2. Click **Next** to define the user codes. The **Galaxy - User Codes** dialog box appears.

Defining user codes

User code is a unique code with a set of privileges for the user to work on the Galaxy panel keypad. The number of user codes that can be set in the panel can vary based on the Galaxy panel type. These user codes are associated to the card holder for the card holder to access the Galaxy panel.

In WIN-PAK UI, you can set the user name and password for the user code. However, the privileges for the user are set in the panel and cannot be modified in WIN-PAK UI.

1. In the **Galaxy - User Codes** dialog box, to change the user name and password, select a USER in the list and type the **User Name** and **User PIN** under **User Changes**.

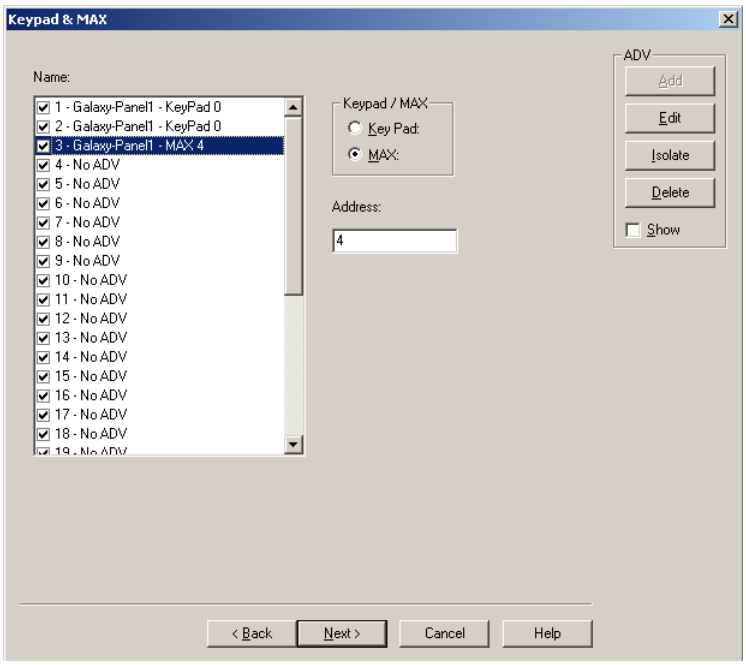


2. Click **Next** for setting the keypad or Max for configuring Galaxy panel. The **Keypad & MAX** dialog box appears.

Defining a keypad and MAX

A keypad is a data input device for the Galaxy panel. WIN-PAK enables you to work on keypad from WIN-PAK using the virtual keypad. MAX is the reader that helps the WIN-PAK users to gain access to a particular area and WIN-PAK enables you to set the MAX. You can define ADVs for the various keypads and MAX that are connected to the Galaxy panel.

1. In the **Keypad & MAX** dialog box, select a keypad or MAX in the **Name** list.



2. Select the type of keypad under **Keypad / Max**.
3. Set a unique address for the keypad or MAX.
4. In the **Name** list, double-click a name and press ENTER to create an ADV for the keypad.
5. Click **Next** to finish the Galaxy panel configuration.
6. Click **Finish**. The Galaxy panel is configured.

Right-Click Menu Options

The following options are available, when you right-click the Galaxy panel:

- Synchronize
- Edit Configuration
- Download Log Data
- Upload User Code
- Upload Date and Time
- Work on Virtual Keypad

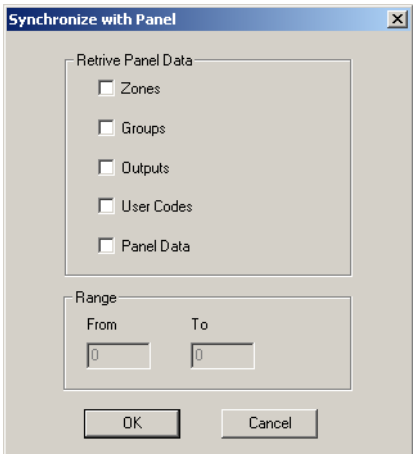
Note: WIN-PAK enables Galaxy to stop polling at communication server, when you perform any of these options except for editing the configuration details.

Synchronizing with Galaxy Panel

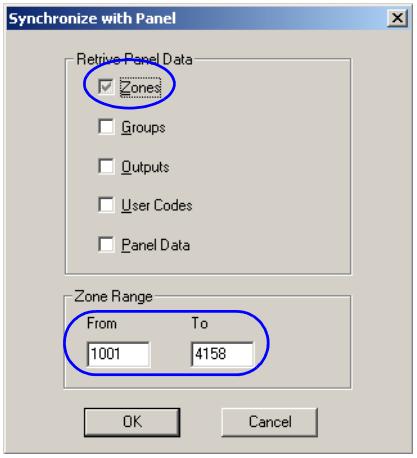
Synchronizing the data in the Galaxy panel with WIN-PAK ensures that the data in WIN-PAK is updated with the latest data in Galaxy. In addition, any changes made in the Galaxy panel after it was downloaded to WIN-PAK are also updated in WIN-PAK.

To synchronize WIN-PAK data with the Galaxy panel:

1. Right-click the Galaxy panel and select **Synchronize**. The **Synchronize with Panel** dialog box appears.



2. Under **Retrieve Panel Data**, select the required check boxes such as Zones, Groups, Outputs, and so on.
3. To specify the range of data to be retrieved, select the required check box again. The selection is grayed and the **From** and **To** boxes are enabled.



4. Change the data range in the **From** and **To** boxes.
5. Click **OK**. A message asking for confirmation to stop polling at the Communication server appears.
6. Click **Yes** to stop polling and start downloading data from the Galaxy panel to WIN-PAK.

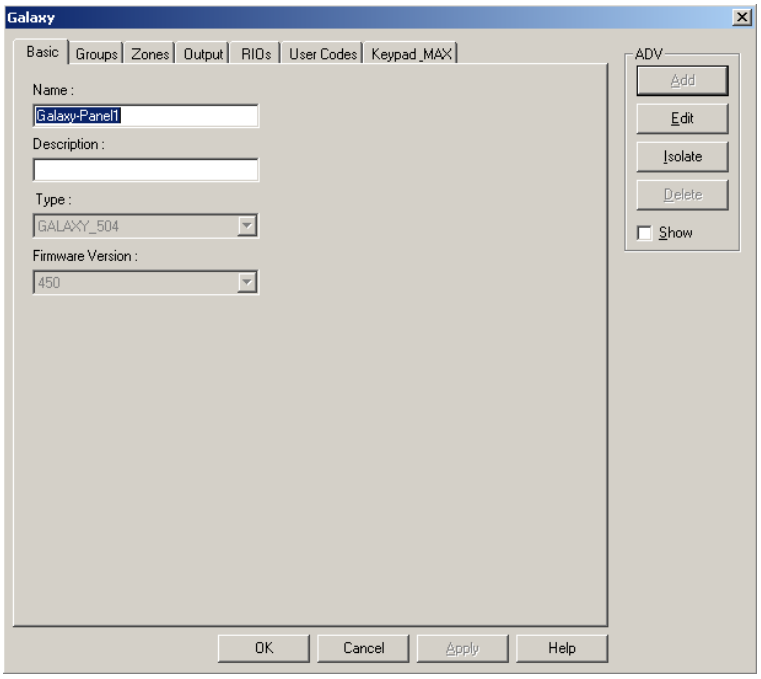
Note: When you upload the data to the panel, the panel data is overwritten with the uploaded data.

Viewing Panel Configuration Details

You can view the latest configuration details of the Galaxy panel that were downloaded to WIN-PAK.

To view the panel configuration details:

1. Right-click the Galaxy panel and select **Configure**. The **Galaxy** dialog box appears.



2. Click the required tab to view and edit the ADV details.

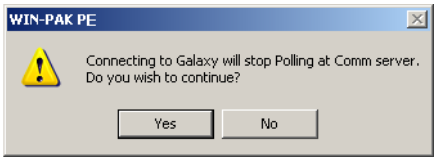
   Refer to the "Adding a Galaxy Panel" section in this chapter for more details on editing Galaxy Panel configuration details.

Downloading Log Data

You can download the log information of the Galaxy panel into WIN-PAK.

To download the log data to WIN-PAK:

1. Right-click the Galaxy panel and select **Download log data**. A confirmation message asking to stop the communication server appears.



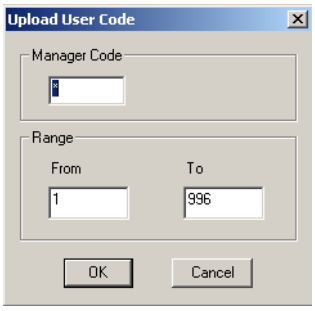
2. Click **Yes** to stop the communication server and download the log data to WIN-PAK. If you click **No**, you cannot download log data to WIN-PAK.

Uploading User Code

You can upload a range of user code details that are configured in WIN-PAK to the Galaxy panel.

To upload the user code to the Galaxy panel:

1. Right-click the Galaxy panel and select **Upload User Code**. The **Upload User Code** dialog box appears.



2. Type the **Manager Code**. If the manager code is invalid, you cannot upload the user code.
3. Under **Range**, type the **From** and **To** values.
4. Click **OK** to upload the user code details to the Galaxy panel.

Uploading Date and Time

You can upload the current date and time of the WIN-PAK system to the Galaxy panel.

To upload the current date and time:

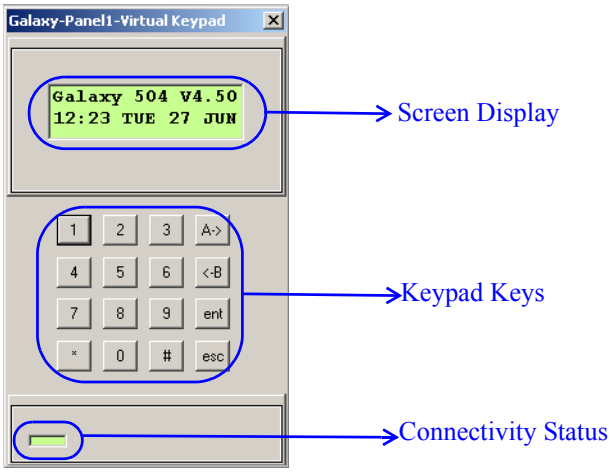
1. Right-click the Galaxy panel and select **Upload date and time** for uploading the current date and time. A confirmation message to stop the polling appears.
2. Click **Yes** to stop polling at communication server and upload the current date and time to the panel.

Working on Virtual Keypad

The virtual keypad is displayed in WIN-PAK for the user to change the Galaxy panel configuration details.

To view and operate on virtual keypad:

1. Right-click the Galaxy panel and select **Virtual Keypad**. The **Galaxy Panel - Virtual Keypad** appears.



2. Use the keys on your keyboard to operate on keypad. The connectivity status is shown at the bottom of the keypad. When the connectivity is lost, the connectivity status color changes to red.
3. Click the button to close the keypad.

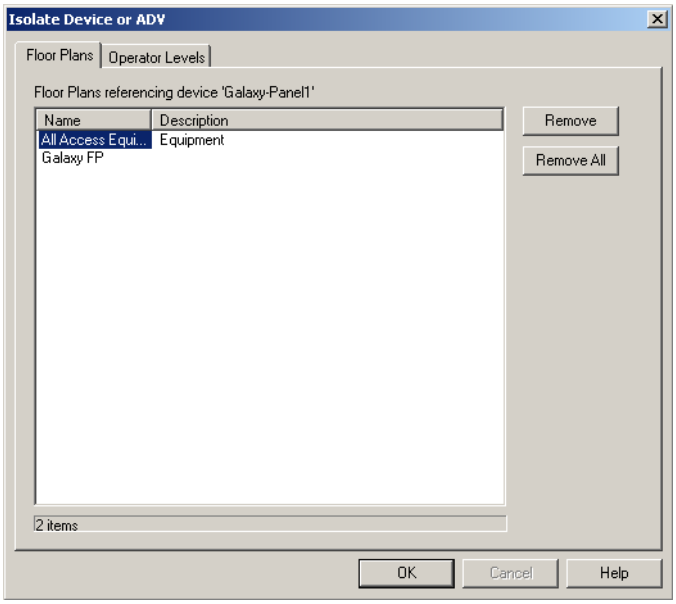
Isolating and Deleting a Galaxy Panel

You can delete the configuration details of the Galaxy panel from WIN-PAK. However, the panel ADVs must be isolated from the floor plans and the operator levels.

Isolating a Galaxy panel

To isolate a Galaxy panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the Galaxy panel and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate ADVs of the Galaxy panel from the floor panel:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the panel is displayed.
    b. Select the floor plans and click **Remove**. The selected floor plans are dissociated.

       OR

       Click **Remove all** to isolate all the ADVs of Galaxy panel from the floor plan.
5. To isolate operator levels from an ADV of the Galaxy panel:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the panel is displayed.
    b. Select the operator levels that must be isolated from the communication server and click **Remove**. The selected operator levels are dissociated from the communication server.

       OR

       Click **Remove all** to isolate all the operator levels from the communication server.
    c. To remove the communication server from the control area, clear the presence of an ADV of the panel in the control area by clearing the **Present in Control Area** check box.
6. Click **OK**.

Deleting a Galaxy panel

After isolating the associated floor plans and operator levels, you can delete the Galaxy panel.

To delete a Galaxy panel:

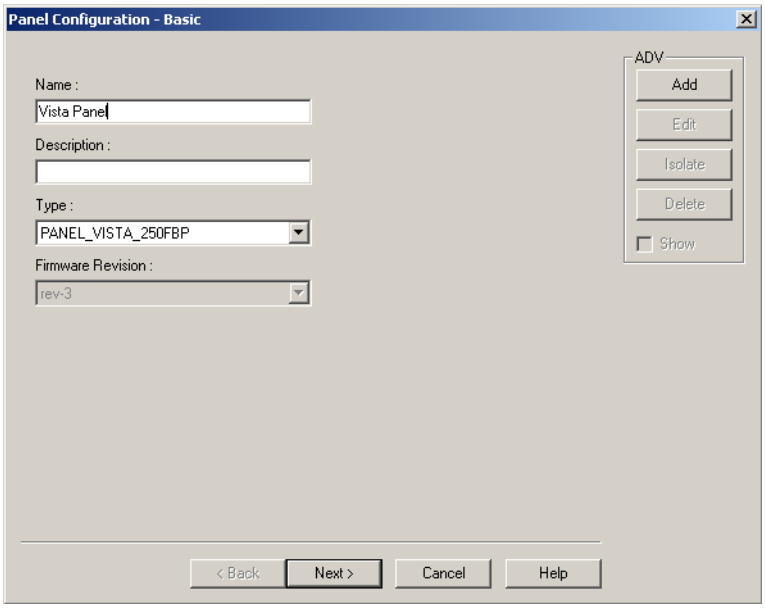
1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the Galaxy panel and click **Delete**. A message asking for confirmation appears.
4. Click **OK** to confirm the deletion. The Galaxy panel is deleted from the device map.

Adding a Vista Panel

You can monitor and control intrusions using the Vista panel in WIN-PAK. In the Vista Panel Port, you can add only one Vista panel. To add multiple vista panels to the communication server, you must add multiple Vista Panel Ports.

To add a Vista panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the communication server.
3. Right-click the **Vista Panel Port** and select **Add New Vista Panel**. The **Panel Configuration - Basic** dialog box appears.



4. Type the **Name** and **Description** of the Vista panel.
5. Select the **Type** of the vista panel. WIN-PAK supports two types of Fire Burglary Panels: **PANEL VISTA 250FBP** and **PANEL VISTA 128FBP**.

Note: The number (250, 128) in the panel types indicates the maximum number of zones that a panel can support and the FBP indicates that the panel is a Fire Burglary Panel.

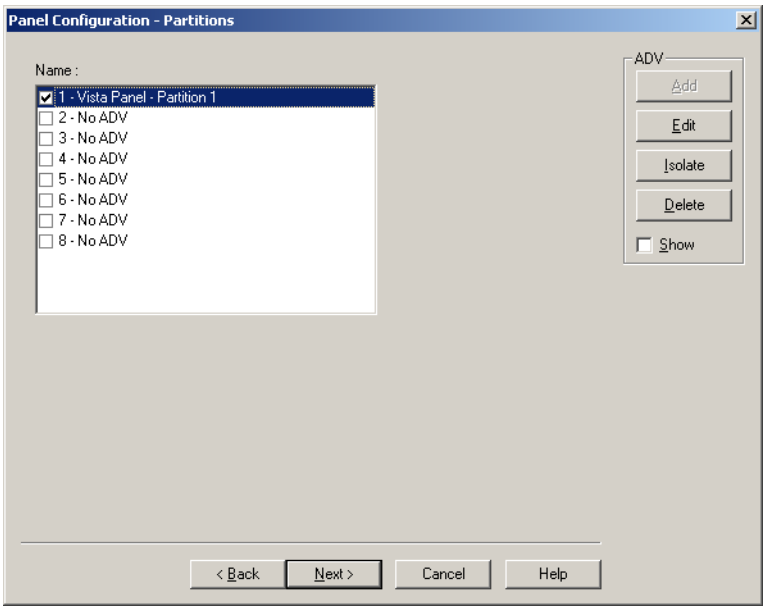
6. Click **Next** to configure the vista partitions. The **Panel Configuration - Partitions** dialog box appears.

Configuring the vista panel partitions

In the Vista panel, a set of zones can be grouped and called as partitions.

Note: Honeywell recommends you to partition by grouping zones based on your building structure.

1. In the **Panel Configuration - Partition** dialog box, create an ADV for the partition.



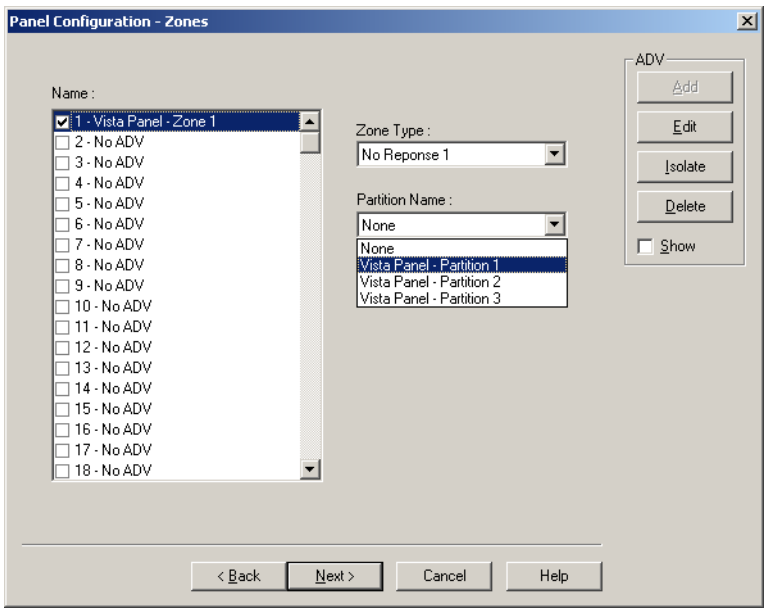
2. Click **Next** to configure the vista panel zones. The **Panel Configuration - Zones** dialog box appears.

Configuring vista panel zones

A zone is the area covered by an input device in the Vista panel that monitors intrusions and creates alarms.

1. In the **Panel Configuration - Zones** dialog box, select the panel zone and create an ADV.

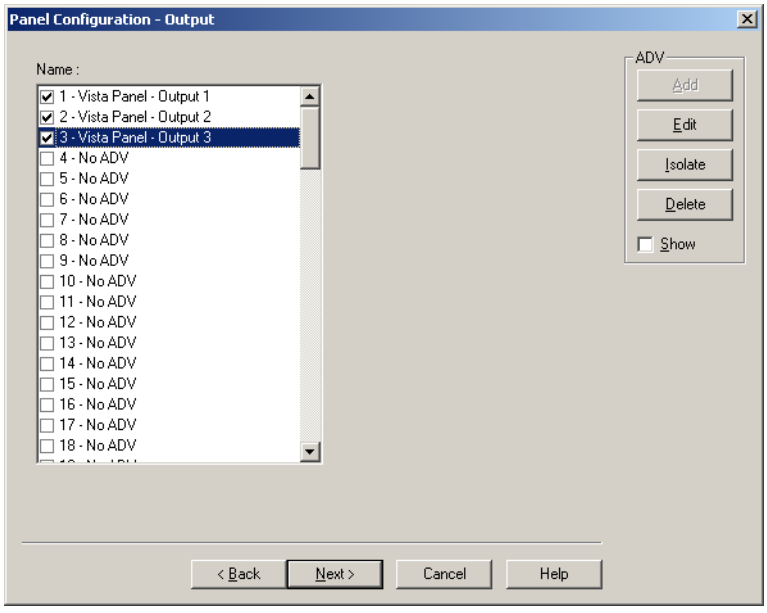
Note: The number of zones in the Name list depends on the selected panel type. In addition, the list contains three more zones for you to define the custom zone types.



2. In the **Zone Type** list, select the type of the zone.
3. In the **Partition Name** list, select the partition to which the zone belongs.
4. Click **Next** to configure the vista panel outputs. The **Panel Configuration - Output** dialog box appears.

Configuring the vista panel outputs

1. In the **Panel Configuration - Output** dialog box, select an output and create an ADV for the output.



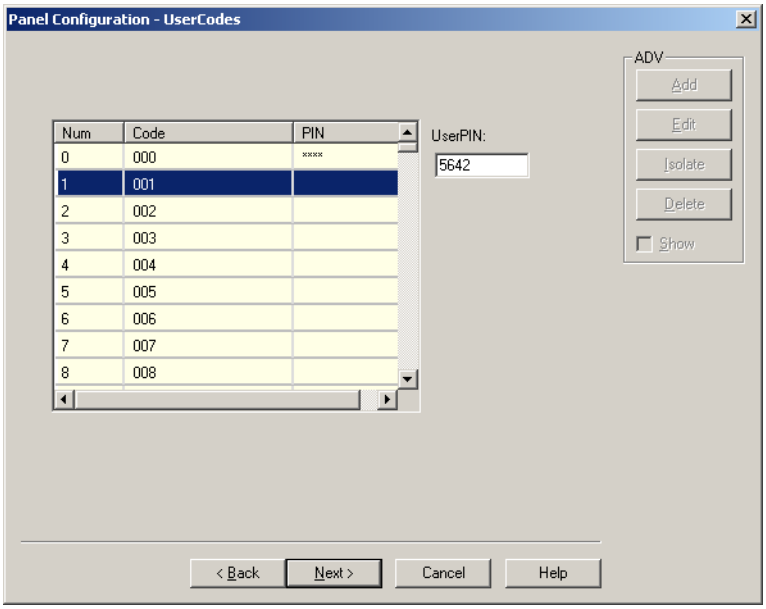
2. Click **Next** to define the user codes. The **Panel Configuration - User Codes** dialog box appears.

Defining user codes

The user code is a unique code with a set of privileges for the user to work on the Vista panel keypad. These user codes are associated to the card holder for the card holder to access the Vista panel. In the WIN-PAK UI, you can set the password for the user code.

To set the password for the user code:

1. In the **Panel Configuration - User Codes** dialog box, select a code.

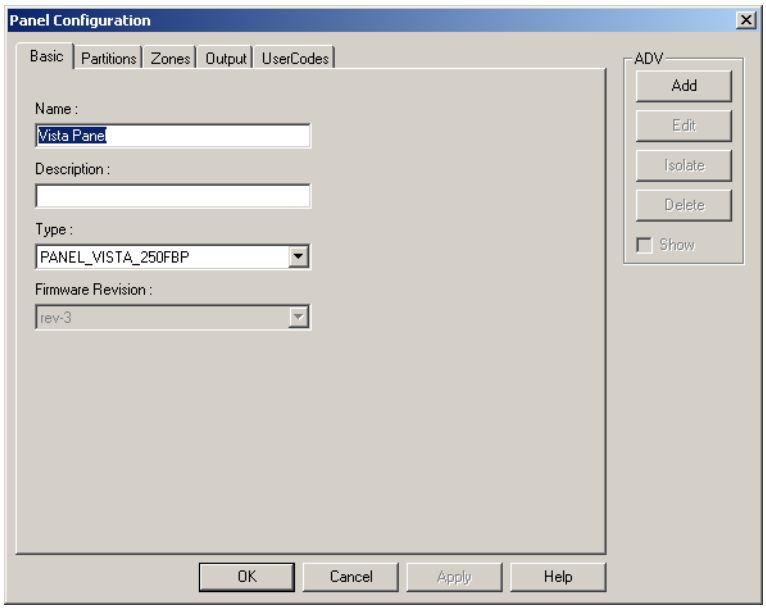


2. In the **UserPIN** box, type the password for the selected user code.
3. Click **Next** to finish the vista panel configuration. The **Panel Configuration - Finish** dialog box appears.
4. Click **Next** to configure the Vista panel.

Editing a Vista Panel

To edit the vista panel configuration details:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and the communication server to display the loops and devices added to the communication server.
3. Expand the Vista Port and select the Vista panel.
4. Right-click the Vista panel and click **Configure**. The **Panel Configuration** dialog box appears.



5. Edit the details of the vista panel, as required.

   Refer to the "Adding a Vista Panel" section in this chapter for editing vista panel configuration details.

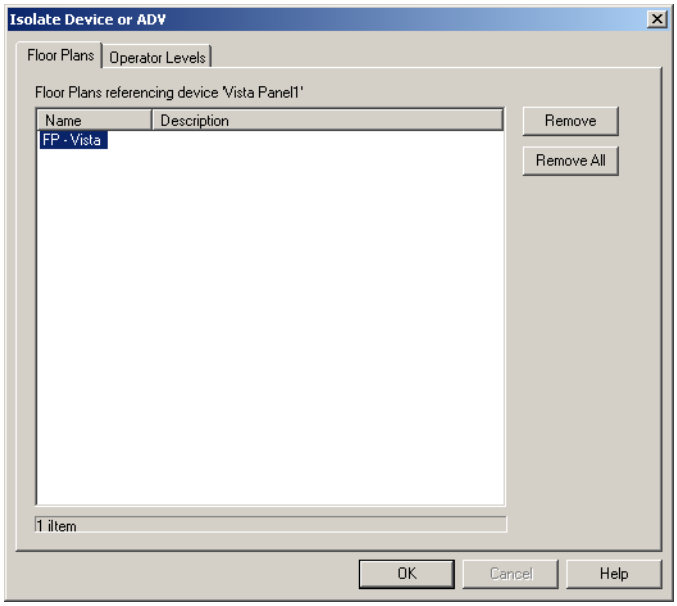
Isolating and Deleting a Vista Panel

You can delete the configuration details of the Vista panel. However, the panel ADVs must be isolated from the floor plans and the operator levels.

Isolating a Vista panel

To isolate a vista panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the Galaxy panel and click **Isolate**. The **Isolate Device or ADV** dialog box appears.



4. To isolate the ADVs of the Vista panel from the floor panel:
    a. Click the **Floor Plans** tab. The list of floor plans associated to the panel is displayed.
    b. Select the floor plans and click **Remove**. The selected floor plans are dissociated from the floor plan.

       OR

       Click **Remove all** to isolate all the ADVs of the Vista panel from the floor plan.
5. To isolate operator levels from an ADV of the Vista panel:
    a. Click the **Operator Levels** tab. The list of operator levels associated to the panel is displayed.
    b. Select the operator levels that must be isolated from the communication server and click **Remove**. The selected operator levels are dissociated from the communication server.

       OR

       Click **Remove all** to isolate all the operator levels from the communication server.
    c. To remove the communication server from the control area, clear the presence of an ADV of the panel in the control area by clearing the **Present in Control Area** check box.
6. Click **OK**.

Deleting a Vista panel

After isolating the associated floor plans and operator levels, you can delete the Vista panel.

To delete a Vista panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder to display the servers and devices added to the device map.
3. Right-click the Vista panel and click **Delete**. A message asking for confirmation appears.
4. Click **OK** to confirm the deletion. The Vista panel is deleted from the device map.

Abstract Device

An Abstract Device (ADV) is a logical representation of a physical device. An ADV is associated to an actual device in your access control system such as a panel or alarm. Therefore, ADVs must be configured for every device mapped to the Device tree structure. ADVs provide an interface for monitoring the device status and controlling the actions of a physical device.

Each ADV is associated to an Action Group. An Action Group defines the priority of a given event related to the device, as well as any actions that take place in response to an event. When you edit an Action Group, all ADVs associated to the action group are updated.

Configuring an Abstract Device

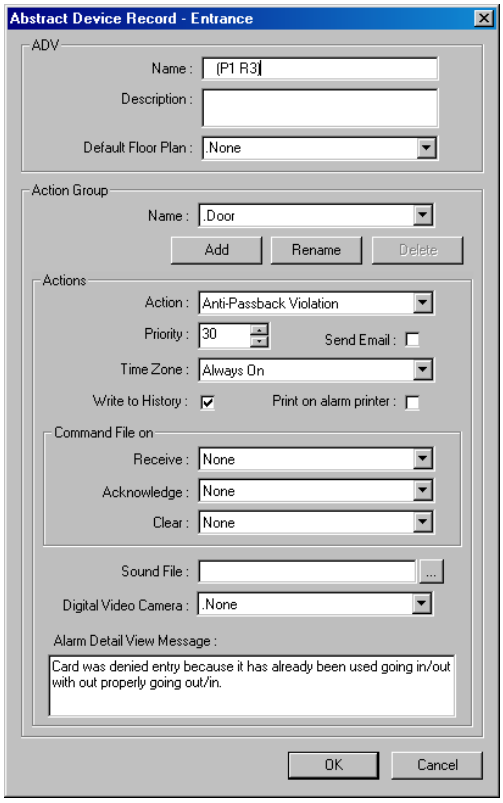
This section describes how to add, edit, delete an abstract device.

Adding an Abstract Device

You can add an abstract device only while configuring the device map. However, you can edit or delete an ADV using the **Abstract Device** window.

To configure an ADV:

1. Open the **Abstract Device Record Configuration** window. You can open this window by clicking **Add** under **ADV** in any device configuration dialog box.



2. The ADV **Name**, by default, is based on the name of device configured. However, you can change the name if required.
3. Enter the **Description** for ADV. The description enables you in selecting the ADV when setting up other aspects of the access control system.
4. In the **Default Floor Plan** list, select a floor plan in which the device is logically located. This floor plan can be opened in an **Alarm View** window, by right-clicking an alarm message and selecting **Floor Plan**. This helps you in locating the place from where the alarm is triggered.
5. Select an existing **Action Group** from the drop-down list and set the action properties. Each action group contains a group of actions.

   Note: If you want to define a unique action group for this ADV, select **.Custom** for the **Action Group** and define the priorities, command files, and other properties.
6. To add a new action group, click **Add**. The **Name** drop-down list changes to a text box. Type a name of the action group and press ENTER. The **Rename** and **Delete** buttons helps you in renaming and deleting the action group.
7. Select an **Action** from the list. This list varies depending on the type of device configured and the selected action group.

   Refer to the "ADV Action Groups" section in this chapter for examples.

8. Enter a **Priority** for the action. By default, the priority assigned is 20. The maximum value you can specify is 99.

Notes:

- Each action must be set with a priority for considering the action as an alarm or an event. When an action is triggered, the action priority is compared with the values set for **Alarm Priority for notification** and **Alarm Priority for required acknowledgement** fields that are configured in the Communication Server.
- The action is considered as an alarm, if the action priority is less than the value in the **Alarm Priority for required acknowledgement** field.
- The action is considered as an event, if the action priority is greater than the value in the **Alarm Priority for required acknowledgement**.

Example: Alarm Priority for notification is set as 20 and Alarm Priority for required acknowledgement is set as 50 in the Com Server Configuration window. If you set 15 as the action priority, it is considered as an alarm. If you set 35 as the action priority, it is considered as an alarm and event.

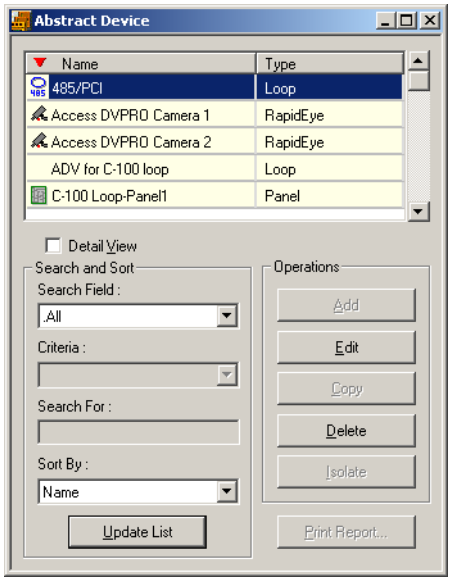
9. Select the **Send Email** check box, if e-mails must be sent to the configured e-mail ids when the action takes place.
10. Select the **Time Zone** for the action. The default setting is **.Always**, as the defined actions take effect regardless of the time.
11. Select the **Write to History** check box to write the event into the log file.
12. Select the **Print on alarm printer** check box to print the action details on the alarm printer.
13. Under **Command Files on**, select a **Command File** to be executed for the action.
    - In the **Receive** list, select the command file that must be executed when an alarm or an event for this action is received.
    - In the **Acknowledge** list, select the command file that must be executed when the alarm for the action is acknowledged.
    - In the **Clear** list, select the command file that must be executed when the alarm for the action is cleared.
14. To play a sound file when an action takes place, type the name of the **Sound File**, or select a sound file by clicking the ellipsis button.
15. To view a live video of the action, select the camera in the **Digital Video Camera** list. When the action has taken place, the **Digital Video - Display** window is displayed showing the live video from the selected camera.
16. Type a detail message for the alarm in **Alarm Detail View Message**.
17. Click **OK** to save the details.

Note: The action properties set in one place are globally defined for the particular Action Group. Therefore, any changes made to this Action Group are applied to all the associated ADVs using this Action Group name.

Editing an Abstract Device

To edit an abstract device:

1. Choose **Configuration > Abstract Device (ADV)**. The **Abstract Device** window appears with the list of ADVs added through device map.



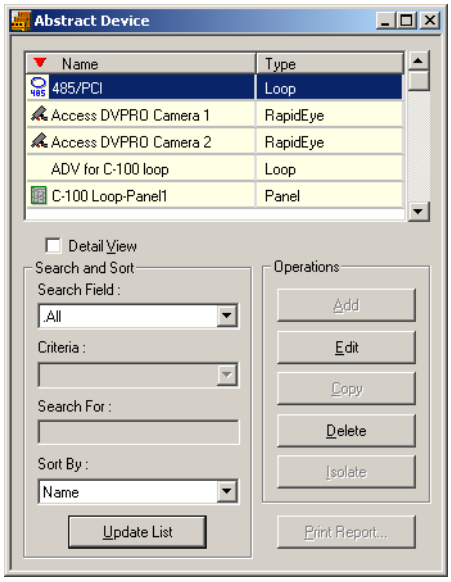
2. Select an abstract device and click **Edit**. The **Abstract Device Record** dialog box for the selected ADV appears.
3. Edit the required details of an ADV.

   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

Deleting an ADV

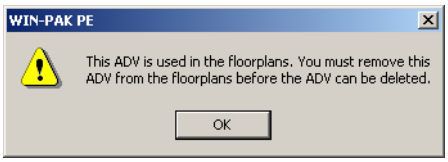
To delete an ADV not in use:

1. Choose **Configuration > Abstract Device (ADV)**. The **Abstract Device** window appears with the list of ADVs added through device map.



2. Select an abstract device and click **Delete**. The Abstract Device is deleted.

Note: If an ADV is associated to a floor plan or control area the following warning message appears.



Action Group

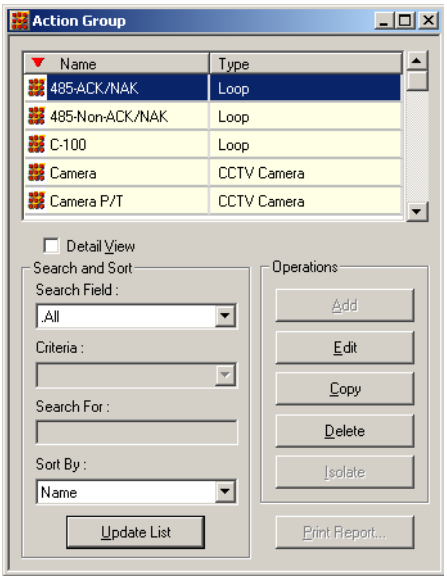
An Action Group is a set of actions assigned to a device when its ADV is defined. All the actions in the action group are set with the list of properties for a response to an action. Responses include executing a command file, activating a sound file, viewing a live video, and so on.

Note: Action groups are added to an ADV while configuring ADVs. However, you are provided with an option to view, edit, copy, and delete action groups individually.

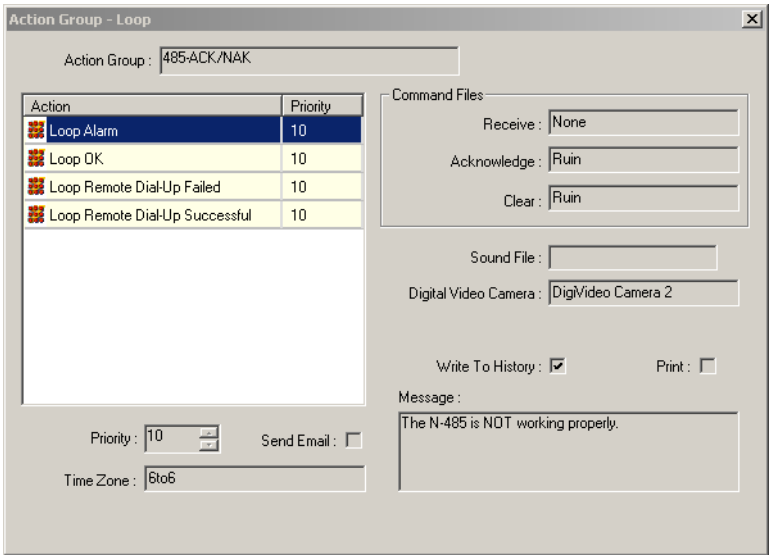
Viewing Action Group Details

To edit details of an action:

1. Choose **Configuration > Device > Action Group**. The **Action Group** window appears.



2. Select the action group and select the **Detail View** check box. The **Action Group** dialog box for the selected action group appears.



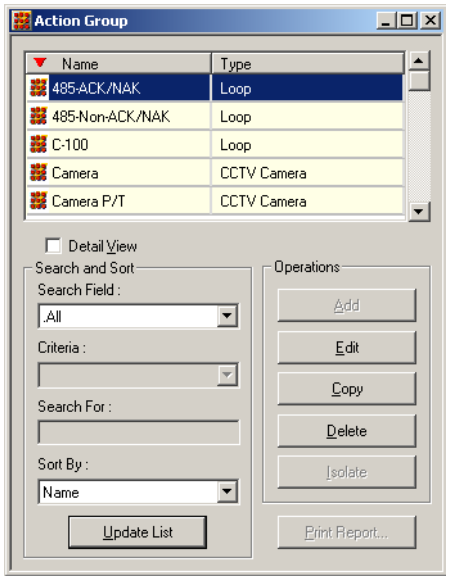
3. View the details of the action group. The priority of the action, time zone, command files and other details are displayed.
4. Select a different action from the list to view the related details.
5. Clear the **Detail View** check box in the Action Group window to close the dialog box.

Editing an Action Group

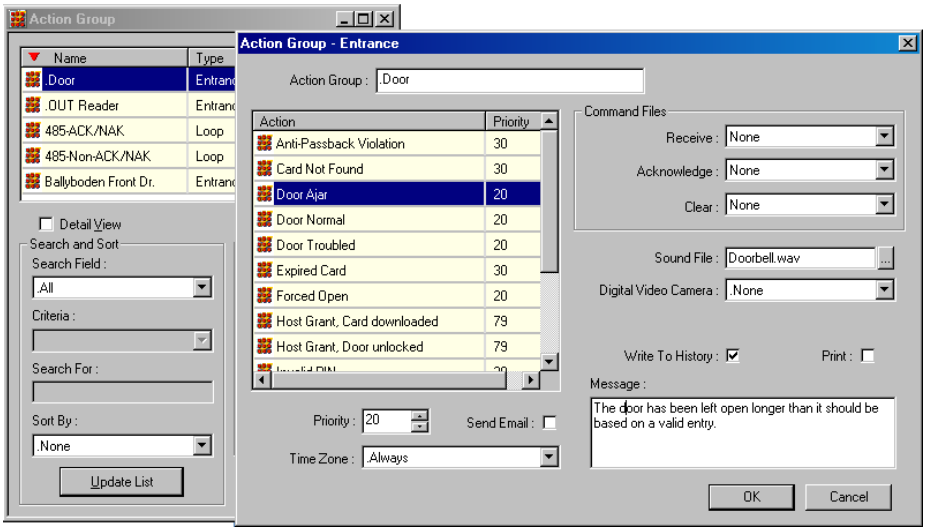
You can edit an Action Group from the Action Group window to make global changes to all ADVs associated with a particular Action Group.

To edit an action group:

1. Choose **Configuration > Device > Action Group**. The **Action Group** window appears.



2. Select the action group and click **Edit**. The **Action Group** dialog box for the selected action group appears.



3. Edit the required details and click **OK**. The action group for the selected device is changed globally.

   Refer to steps 8 to 16 of the "Adding an Abstract Device" section in this chapter for more details on setting the action group properties.

Note: After you create the Action Group (except ".Custom"), it can be used as a template for other devices of the same type.

Copying an Action Group

You can create a copy of an Action Group with the same set of properties and then you can define a different set of properties.

To create a copy:

1. Select the action group and click **Copy**. The selected action group is duplicated.
2. Select the copied action group and click **Edit** to change the settings.

Deleting an Action Group

If an action group associated to an ADV is still in use, reassign the ADV associated to it to a different action group, before deleting the action group. Otherwise the warning message appears showing that the action group is in use.

To delete an action group:

1. Select the action group and click **Delete**. The selected action group is deleted.

ADV Action Groups

The following list of tables that describe you the types of actions defined for different ADVs used in WIN-PAK.

Table 11-11 Describing 485 ACK/NAK and 485 non-ACK/NAK (loop) Actions

Action	Message/Description
Loop OK	The N-485 is working properly.
Loop Remote Dial-up Failed	The host computer was not able to connect through dialup to the panel.
Loop Remote Dial-up Successful	The host computer was able to connect through dialup to the control panel.
Loop Alarm	The N-485 is NOT working properly.

Table 11-12 Describing C-100 (loop) Actions

Action	Message/Description
Loop OK	The C-100 is working properly.
Loop Remote Dial-up Failed	The host computer was unable to connect through dial-up to the control panel.

Table 11-12 Describing C-100 (loop) Actions

Action	Message/Description
Loop Remote Dial-up Successful	The host computer was able to connect through dialup to the control panel.
Loop Alarm	The C-100 is NOT working properly.

Table 11-13 Describing Camera (CCTV camera) Actions

Action	Message/Description
CCTV Camera OK	The camera is working properly.
CCTV Camera Trouble	The camera is NOT working properly.

Table 11-14 Describing Camera PTZ (CCTV camera) Actions

Action	Message/Description
CCTV Camera OK	The pan tilt camera is working properly.
CCTV Camera Trouble	The pan tilt camera is NOT working properly.

Table 11-15 Describing Cards (Entrance Reader) Actions

Action	Message/Description
Anti-Passback Violation	A card was denied entry because it has already been used going in/out without properly going in/out.
Card Not Found	A card was denied entry because it was unknown to the reader.
Expired Card	A card was denied entry because it has been expired by date or number of uses.
Host Grant Card downloaded	Access was granted to the user, if the event is downloaded within two minutes of computer time. The control panel was updated with valid card information.
Host Grant Door unlocked	Access was granted to the user, if the event is unlocked within two minutes of computer time. The control panel was not updated with valid card information.
Invalid PIN	A card was denied entry because of an invalid PIN.

Table 11-15 Describing Cards (Entrance Reader) Actions

Action	Message/Description
Invalid Site Code	A card was denied entry because of an improper site code.
Invalid Time Zone	A card was denied entry because it was used outside its time period.
Trace Card	A card that is being traced was used and entry was granted.
Valid Card	A valid card had been used and entry was granted.

Table 11-16 Describing Command File Server Actions

Action	Message/Description
Server OK	The command file server is working properly.
Server Trouble	The command file server is NOT working properly. Verify that the "WIN-PAK Command File Server" is running in the WIN-PAK Service Manager.

Table 11-17 Describing Communication Server Actions

Action	Message/Description
Server OK	The communication server is working properly.
Server Trouble	The communication server is NOT working properly. Verify that "WIN-PAK Communication Server" is running in the WIN-PAK Service Manager.

Table 11-18 Describing Door (Entrance) Actions

Action	Message/Description
Anti-Passback Violation	A card was denied entry because it has already been used - going in/out without properly going out/in.
Card Not Found	A card was denied entry because it was unknown to the reader.
Door Ajar	The door has been left open longer than it must be based on a valid entry.
Door Normal	The door is now closed.
Door Troubled	The door status can not be accurately displayed due to tampering.
Expired Card	A card was denied entry because it was expired by date.

Table 11-18 Describing Door (Entrance) Actions

Action	Message/Description
Forced Open	The door is in the alarm mode due to invalid entry.
Host Grant Card downloaded	Access was granted to the user, if event is downloaded within two minutes downloaded of computer time. The control panel was updated with valid card information.
Host Grant Door unlocked	Access was granted to the user, if the event is unlocked within two minutes unlocked of computer time. The control panel was not updated with valid card information.
Invalid PIN	A card was denied entry because it was used with an invalid PIN.
Invalid Site Code	A card was denied entry because it did not have a proper site code.
Invalid Time Zone	A card was denied entry because it was used outside its time period.
Trace Card	A card being traced was used and entry was granted.
Valid Card	A valid card has been used and entry was granted.

Table 11-19 Describing Door Output Actions

Action	Message/Description
De-energized	The output of the door is not energized.
Energized	The output of the door is energized.
Trouble	The output of the door is not responding.

Table 11-20 Describing Group Actions

Action	Message/Description
De-energized	The group of relays is not energized.
Energized	The group of relays is energized.

Table 11-21 Describing Guard Tour Sequenced Group Actions

Action	Message/Description
Early Arrival	The guard arrived early at the designated check point reader.
Late Arrival	The guard arrived late at the designated check point reader.

Table 11-21 Describing Guard Tour Sequenced Group Actions

Action	Message/Description
Missed	The guard missed the designated check point reader.
Out of Sequence	The guard is out of sequence.

Table 11-22 Describing Guard Tour Server Group Actions

Action	Message/Description
Server OK	The Guard Tour server is working properly.
Server Trouble	The Guard Tour server is NOT working properly. Verify that "WIN-PAK Guard Tour Server" is running in the WIN-PAK Service Manager.

Table 11-23 Describing Guard Tour Unsequenced Actions

Action	Message/Description
Checked	The guard has checked the required input/reader.

Table 11-24 Describing Input Alarm Point (Input Supervised) Actions

Action	Message/Description
Input Active	The input is in the alarm state.
Input Normal	The input is in the normal state.
Input Trouble	The status can not be accurately displayed due to tampering. **Note:** This action is included only if the input is Supervised.

Table 11-25 Describing Modem Pool ACK/NAK Actions

Action	Message/Description
Modem Pool OK	Modem pool is working properly.
Modem Pool Trouble	Modem pool is NOT working properly.

Table 11-26 Describing Modem Pool non ACK/NAK Actions

Action	Message/Description
Modem Pool OK	Modem pool is working properly.
Modem Pool Trouble	Modem pool is NOT working properly.

Table 11-27 Describing Monitor (CCTV Monitor) Actions

Action	Message/Description
CCTV Monitor OK	Monitor is working properly.
CCTV Monitor Trouble	Monitor is NOT working properly.

Table 11-28 Describing NS2+ Panel Actions

Action	Message/Description
Auxiliary Port Failure	The auxiliary communication port is not working.
Auxiliary Port Normal	The auxiliary communication port is working.
External 5 Volt Normal	The 5 Volt reader power is normal.
External 5 Volt Alarm	The 5 Volt reader power is shorted.
Ground Fault Alarm	An input point or reader is shorted to earth ground causing a ground fault.
Ground Fault Normal	An input point or reader that caused the ground fault has returned to normal.
Low Voltage Alarm	Battery voltage is low.
Low Voltage Normal	Battery voltage is normal.

Table 11-28 Describing NS2+ Panel Actions

Action	Message/Description
Panel Communication Alarm	Communication with the control panel has been lost.
Panel Communication Normal	Communication with the control panel has been restored.
Panel Reset	The control panel has been reset.
Poll Response Alarm	The control panel is NOT responding to computer polling.
Poll Response Normal	The control panel is responding normally to computer polling.
Primary Power Failure	Control panel primary power has been lost.
Primary Power Normal	Control panel primary power has been restored.
Tamper Switch Alarm	The control panel service door is open.
Tamper Switch Normal	The control panel service door is closed.

Table 11-29 Describing N-1000-II/PW-2000-II Panel Actions

Action	Message/Description
Auxiliary Port Failure	The auxiliary communication port is not working.
Auxiliary Port Normal	The auxiliary communication port is working.
Panel Communication Alarm	Communication with the control panel has been lost.
Panel Communication Normal	Communication with the control panel has been restored.
Panel Reset	The control panel has been reset.

Table 11-29 Describing N-1000-II/PW-2000-II Panel Actions

Action	Message/Description
Poll Response Alarm	The control panel is NOT responding to computer polling.
Poll Response Normal	The control panel is responding normally to computer polling.
Primary Power Failure	Control panel primary power has been lost.
Primary Power Normal	Control panel primary power has been restored.

Table 11-30 Describing N-1000-III/PW-2000-IV Panel Actions

Action	Message/Description
Auxiliary Port Failure	The auxiliary communication port is not working properly.
Auxiliary Port Normal	The auxiliary communication port is working properly.
External 5 Volt Alarm	The 5 volt reader power is shorted.
External 5 Volt Normal	The 5 volt reader power is normal.
Ground Fault Alarm	An input point is shorted to earth ground causing a ground fault.
Ground Fault Normal	An input point that caused the ground fault has returned to normal.
Low Voltage Alarm	Battery voltage is low.
Low Voltage Normal	Battery voltage is normal.
Panel Communication Alarm	Communication with the control panel has been lost.
Panel Communication Normal	Communication with the control panel has been restored.
Panel Reset	The control panel has been reset.

Table 11-30 Describing N-1000-III/PW-2000-IV Panel Actions

Action	Message/Description
Poll Response Alarm	The control panel is not responding to computer polling.
Poll Response Normal	The control panel is responding normally to computer polling.
Primary Power Failure	Control panel primary power has been lost.
Primary Power Normal	Control panel primary power has been restored.
Tamper Switch Alarm	The control panel service door is open.
Tamper Switch Normal	The control panel service door is closed.

Table 11-31 Describing P-Series SIO Board Actions

Action	Message/Description
Poll Response Alarm	The SIO Board is NOT responding to polling.
Poll Response Normal	The SIO Board is responding to polling.
Primary Power Failure	Primary power is down. Make a service call.
Primary Power Normal	You have about 2 hours of backup power.
Tamper Switch Alarm	The PRO-2200 enclosure is open. Check to see if service is done or dispatch security as needed. The tamper switch is a Norther Computers switch. When the door to the enclosure is opened (switch open), the firmware reports a Tamper Switch Alarm immediately, which is also shown at the same time as a Tamper Switch Alarm in the Alarm View of WIN-PAK.
Tamper Switch Normal	The PRO-2200 enclosure is now closed. When the door to the enclosure is closed (switch closed), the firmware reports a Tamper Switch Normal after approximately 3 seconds, which is also shown at that time as a Tamper Switch Normal in the Alarm View of WIN-PAK.

Table 11-32 Describing P-Series Dial-Up Actions

Action	Message/Description
Incorrect Password	An incorrect password attempt was made to access the controller.
Panel Configuration Error	An error was generated by an incorrect panel configuration.
Panel Remote Dial-Up Failed	The N-485 remote dial-up is NOT Working properly.
Panel Remote Dial-Up Successful	The N-485 remote dial-up is working properly.
Poll Response Alarm	The P-Series Intelligent Controller is NOT responding to computer polling.
Poll Response Normal	The P-Series Intelligent Controller is responding to computer polling.
Primary Power Failure	P-Series Intelligent Controller primary power has been lost.
Primary Power Normal	P-Series Intelligent Controller primary power has been restored.
Tamper Switch Alarm	The P-Series Intelligent Controller service door is open.
Tamper Switch Normal	The P-Series Intelligent Controller service door is closed
Unsupported Panel	

Table 11-33 Describing P-Series Reader Actions

Action	Message/Description
Anti-Passback Violation	A card was denied entry because it has already been used going in/out without properly going out/in.
Anti-Passback Violation, door not used	A soft Anti-Passback violation has occurred. The door was not opened by the card holder.
Anti-Passback Violation, door used	A soft Anti-Passback violation has occurred. The door was opened by the card holder.

Table 11-33 Describing P-Series Reader Actions

Action	Message/Description
Card Not Found	A card was denied entry because it was unknown to the reader.
Door Ajar	The door has been left open longer than it should be based on a valid entry.
Door Locked	Door is in a “Locked” mode of operation. No card access granted, free egress is allowed.
Door Normal	The door position is now closed.
Door Troubled	The door status can not be accurately displayed due to tampering.
Door Unlocked	A card was presented to the reader while the door was unlocked.
Duress, request denied	A duress code was entered. Access was denied.
Duress, door not used	A duress code was entered. Access was granted. Door was not opened.
Duress, door used	A duress code was entered. Access was granted. Door was opened.
Forced Open	The door is in the alarm mode due to invalid entry.
Free Egress, door not used	Free egress request was granted. Door was not opened.
Free Egress, door not verified	Free egress request was granted. Door is not monitored.
Free Egress, door used	Free egress request was granted. Door was opened.
Host Grant, card downloaded	Access was granted to the user. The P-Series Intelligent Controller was updated with valid card information.
Host Grant, door unlocked	Access was granted to the user. The P-Series Intelligent Controller was NOT updated with valid card information.
Invalid Format	The P-Series Intelligent Controller detected an invalid card format.
Invalid Format, reverse read	The P-Series Intelligent Controller detected a card swiped backwards. Invalid card format.
Invalid PIN	A card was denied entry because it was used with an invalid PIN.
Invalid Site Code	A card was denied entry because it did not have a proper facility code.
Invalid Time Zone	A card was denied entry because it was used outside its time report.

Table 11-33 Describing P-Series Reader Actions

Action	Message/Description
Issue Code	An invalid issue code was presented to the reader.
Never allowed at this door	This card is never allowed at this door even if Host Grant is enabled.
No second card presented	This door is using the two man rule. A second valid card was not presented to the reader.
Site Code Verified, door not used	Door is in the facility or site code mode. A valid facility or site code was presented. The door was not opened by card holder.
Site Code Verified, door used	Door is in the facility or site code mode. A valid facility or site code was presented. The door was opened by card holder.
Trace Card	A card that is traced was used and entry was granted.
Valid Card, door not used	A valid card was presented to the reader but the door was not opened during its pulse time.
Valid Card, door used	A valid card was presented to the reader and the door was opened.

Table 11-34 Describing P-Series Input-Generic (Input P-Series Supervised) Actions

Action	Message/Description
Input Active	The input is in the alarm state.
Input Normal	The input is in the normal state.
Input Troubled	The status can not be accurately displayed because of tampering.

Table 11-35 Describing P-Series Output (Output P-Series) Actions

Action	Message/Description
De-energized	The output is not energized.
Energized	The output is energized.
Trouble	The output is not responding.

Table 11-36 Describing Galaxy Panel Action Groups

Action	Message/Description
Alarm Cancel	
Alarm Reset	
Automatic Test	
Battery Restore	The Module Battery which was low is restored.
Battery Trouble	The Module Battery is low.
Code Tamper	Wrong code alarm act.
Comm Fail	The communication between module and RS485 is lost.
Comm Restore	The communication between module and RS485 is restored.
Control Unit Fuse Restore	The control unit fuse is restored.
Control Unit Fuse Trouble	The control unit fuse is in trouble.
Local Program End	Engineer mode exited.
Manual Test	Engineer test
Module AC Fail Restore	Module AC Fail is restored.
Module AC Fail Trouble	Module AC Fail is in trouble.
Module Removed	Module Removed
Panel Cold Start	Power Up Panel.
Power Up	Warm start of panel.
Program Begin	Engineer mode entered.
Recent Close	Panel Full Set
Remote Call End	Remote Call End
Remote Call Start	Remote Call is complete.
RF Jam	RF signal is jammed.
RF Jam Restore	RF signal which was jammed is restored.s

Table 11-36 Describing Galaxy Panel Action Groups

Action	Message/Description
RF NVM RAM Fail	RF NVM RAM Fail
Standby Battery Low	Standby Battery is low
Standby Battery OK	Standby Battery is OK.
Tamper Alarm	Module is tampered.
Tamper Restore	Module tampered is restored.
Tel. Line Fail Restore	Module telephone line fail is restored.
Tel. Line Fail Trouble	Module telephone line fail is in trouble.
Time/Date changed	The time and date of the panel is changed.
Unset Early	Panel is unset.
Walk Test End	Walk Test is finished.
Walk Test Start	Walk Test is started.

Table 11-37 Describing RS-232 Action Groups

Action	Message/Description
RS-232 Link OK	The RS-232 port is communicating properly.
RS-232 Link Trouble	The RS-232 port is NOT communicating properly.

Table 11-38 Describing RS-232 Port (Single Panel) Action Groups

Action	Message/Description
Loop Alarm	The RS-232 Port (Single Panel) is NOT working properly.
Loop OK	The RS-232 Port (Single Panel) is working properly.

Table 11-39 Describing Schedule Server Action Groups

Action	Message/Description
Server OK	The Schedule Server is operating normally.
Server Trouble	The Schedule Server is not operating properly. Verify that the "WIN-PAK Schedule Server" is running in the WIN-PAK Service Manager.

Table 11-40 Describing Tracking Server Action Groups

Action	Message/Description
Server OK	The Tracking Server is working.
Server Trouble	The Tracking and Muster Server is not operating properly. Verify that the WIN-PAK Muster Server is running in the WIN-PAK Service Manager.

Table 11-41 Describing Video Switcher (CCTV Switcher) Action Groups

Action	Message/Description
CCTV Switcher OK	The video switcher is working properly.
CCTV Switcher Trouble	The video switcher is NOT working properly.

Table 11-42 Describing Galaxy Communication Actions

Action	Message/Description
Galaxy Communication Alarm	Galaxy Communication is in trouble.
Galaxy Communication Ok	Galaxy Communication is working properly.
Galaxy Polling Started	Galaxy is started polling.

Table 11-42 Describing Galaxy Communication Actions

Action	Message/Description
Galaxy Polling Started	Galaxy is stopped polling.

Table 11-43 Describing Galaxy Group Actions

Action	Message/Description
Group Alarm Cancel	Galaxy Group alarm is cancelled.
Group Alarm Confirm	Galaxy Group alarm is confirmed.
Group Alarm Reset	Galaxy Group alarm is reset.
Group Automatic Set	Galaxy Group is automatically set.
Group Bypass	Galaxy Group is bypassed
Group Closing Extend	The Galaxy group auto-arm extend is delayed.
Group Early Unset	The Galaxy group is unset early.
Group Fail to Set	The Galaxy group is fail to set.
Group Full Set	The Galaxy group is set.
Group in Alarm	Group in Alarm
Group Late to Open	
Group Late to Set	
Group Normal	Group returned to Normal.
Group Part Set	
Group Part Unset	
Group Rearm after alarm	Rearm after alarm.
Group Recent Close	Previous alarm was within 5 mins of set.

Table 11-43 Describing Galaxy Group Actions

Action	Message/Description
Group Reset Required	Reset is required to do any operation at the Group.
Group Unbypass	Group is unbypassed.
Group Unset	Group is unset.
Group Walk Test End	Group walk test is finished.
Group Walk Test Start	Group walk test is started.
Lid Tamper	Lid is tampered.
Lid Tamper Restore	Lid tamper is restored.

Table 11-44 Describing Galaxy Keypad Actions

Action	Message/Description
Keypad Alarm	Keypad raised an alarm.
Keypad Communication Loss	The communication with keypad is lost.
Keypad OK	Keypad is working properly.
Keypad Tamper	Keypad is tampered.
Keypad Tamper Restore	Keypad tamper is restored.

Table 11-45 Describing Galaxy Keyprox Actions

Action	Message/Description
Door Forced	
Door Propped	The door is supported with a prop.
Invalid Card	The accessed card is invalid.
Keyprox Alarm	

Table 11-45 Describing Galaxy Keyprox Actions

Action	Message/Description
Keyprox Communication Loss	The communication with keyprox is lost.
Keyprox OK	Keyprox is working properly.
Keyprox Tamper	Keyprox is tampered.
Keyprox Tamper Restore	Keyprox tamper is restored.
Rejected Card	The accessed card is the rejected card.
Valid Card	The accessed card is the valid card.

Copying and Moving Loops and Panels

The following functions can be performed across communication servers:

- Move an existing panel from one communication server to the other.
- Copy an existing panel to create a new panel with same settings in other communication server.

Moving Loops and Panels

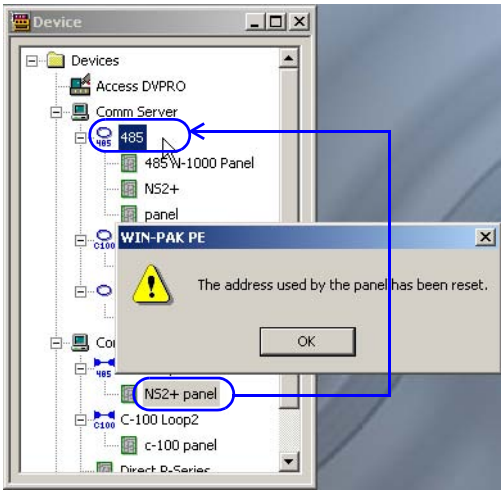
You can move loops and panels across communication servers if the following conditions are met:

1. Ports are available in the destination communication server.
2. The same type of loops are available in the destination communication server, while moving panels attached to loops. For example, when you move a panel attached to a P-Series loop, the destination communication server must have a P-Series Loop.

Moving loops across communication servers

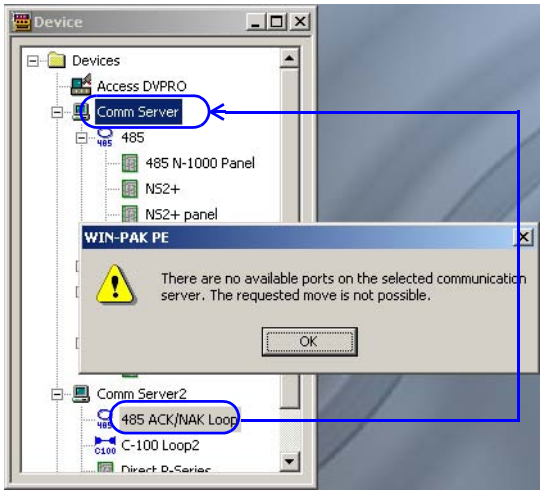
To move a loop across communication servers:

1. Select a loop to be moved in the source communication server.
2. Drag and drop the loop onto the destination communication server. A message appears indicating that the port is reset for the loop.



3. Click **OK**. The loop is moved to the destination communication server.

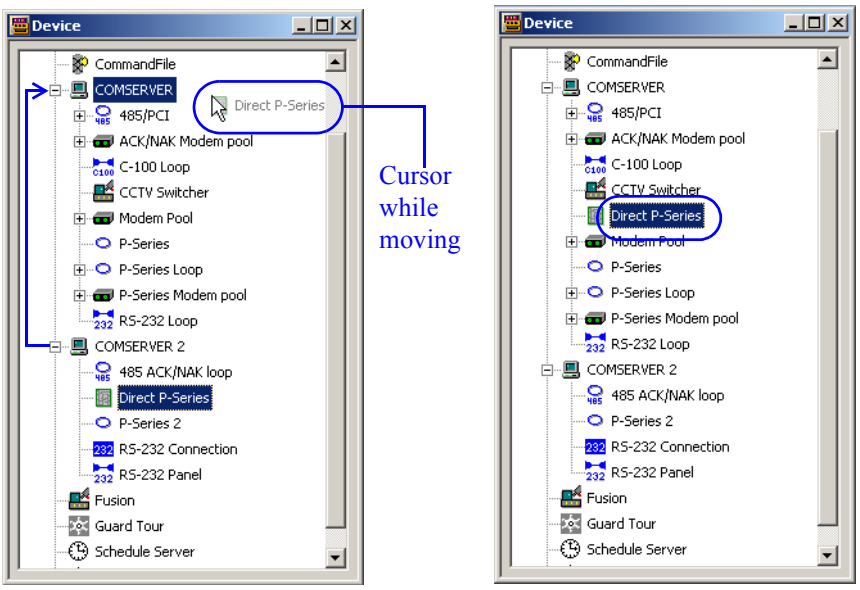
Note: If the destination communication server does not contain a port and if you attempt to move a loop, the following message appears:



Moving direct panels across communication servers

To move a direct panel across communication servers:

1. Select a direct panel (not attached to a loop) in the source communication server.
2. Drag and drop the direct panel onto the destination communication server.

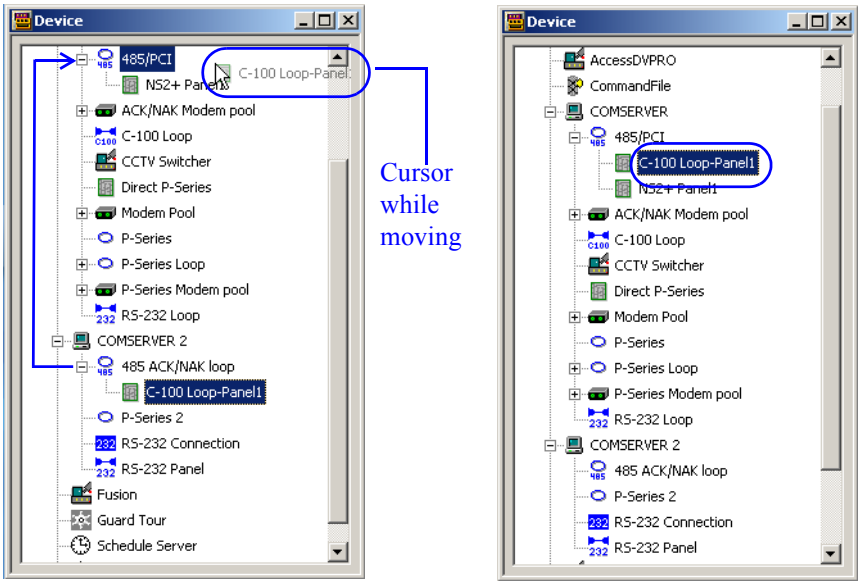


3. Release the mouse button at the destination communication server. The direct panel is moved.

Moving panels across communication servers

To move a panel attached to a loop:

1. Select a panel (attached to a loop) in the source communication server.
2. Drag and drop the panel onto the destination communication server.



3. Release the mouse button at the same type loop of the destination communication server. The panel is moved.

Copying Loops and Panels

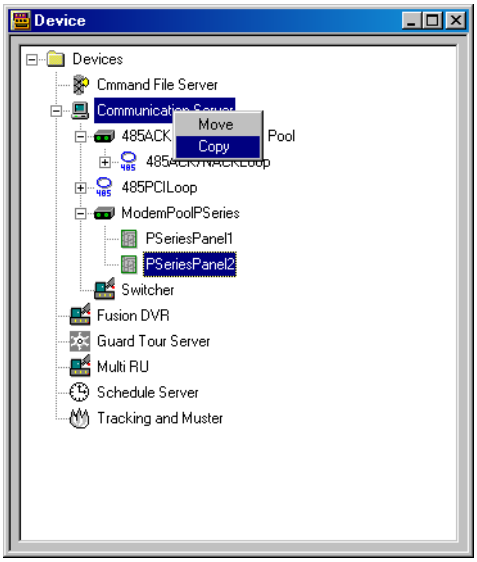
You can create a copy of loops and panels onto another communication servers if the following conditions are met:

1. Ports are available in the destination communication server.
2. The same type of loops are available in the destination communication server, while creating a copy of panels attached to loops. For example, you can create a copy of direct panel onto another communication server, but not onto a Modem Pool or a Loop on the communication server.

Copying a direct panel

To create a copy of a panel to other communication server:

1. Right-click the panel icon, hold and drag the panel icon to the Communication Server onto which you want it to be copied. When you release the mouse button, the pop-up (Move or Copy) menu is displayed, enabling you to select the desired action.



2. Click **Copy** to create a copy of it. The **Copying Device** dialog box appears, with an incremental number appended onto the device name.

3. Rename the device, or accept the default name.
4. Click **OK**. A message appears indicating that the loop or port has been reset.

5. Click **OK**. The device is copied to the other communication server.

Note: When you create a copy of a loop or modem pool, only the loop or modem pool is copied and not the panels attached to it.

Initializing Panels

Programming information entered into the WIN-PAK System is sent to the panels before it takes effect.

- When panels are first added to the system, they are initialized so that the information entered during panel configuration is sent to the panels.
- Likewise, whenever there is a change in the panel configuration, the new information is sent to the panels.
- The only exceptions to this are changes to individual cards and card holders, which are automatically sent to the panels.
- Panels are initialized from the Floor Plan view (the background) or from the Control Map.

Note: Panel Configuration Options reset all of your panel's programming. Honeywell recommends that you select all options (select the "Select All" check box) when sending the Panel Configuration Options.

Refer to the "Initializing Panels from Floor Plan" section in the chapter Floor Plan for details on panel initializing on floor plans.

Refer to the "Initializing a Panel from Control Map" section in the chapter Defining Areas for details on panel initializing on floor plans.

Defining Areas

11

In this chapter...

Introduction

Areas in WIN-PAK are classified as Access Areas, Control Areas, Tracking Areas, and Muster Areas.

Access Areas are a logical grouping of doors and readers to which card holders can gain access. After the access areas are defined, they are mapped to access levels. When card holders are assigned to an access level, they can gain access to the access area for the time zone and access permissions set for the access level.

Example: An access area A can be defined with doors D1, D2 and readers R1 and R2, and a card holder C1 can be assigned to an access level AL1. When the access area A is mapped to the access level AL1, the card holder C1 can gain access to D1, D2, R1, and R2.

Control areas are logical areas containing devices such as communication servers, loops, panels, input points, output points, groups, and readers. Operators who are assigned to a control area, can view the status of the devices in the control areas and their relationship using a Control Map. In addition, an operator can control the devices from the control map.

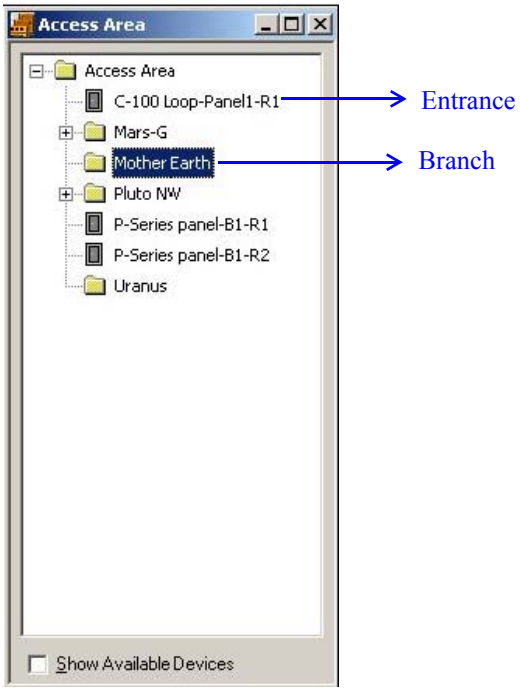
Tracking Areas are used for tracking card holder movements and Mustering areas are used for tracking card holder movements in the event of emergency situations such as fire.

This chapter describes how to configure access areas, configure control areas and view control maps, define tracking and mustering areas.

Defining Access Areas

Access Areas are the logical areas in the Access Control System, in which entrances such as doors and readers are placed. The access area definition in WIN-PAK appears as a tree, to which branches and entrances can be added. The access areas are represented as branches, and panels, readers, and doors are represented as entrances by which you can gain access to the areas. An entrance can be added to the **Access Area** folder or it can be added to a branch inside the **Access Area** folder.

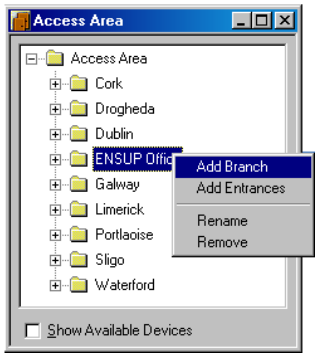
Example: If a reader R1 is located in the first floor of a building, you can define “First Floor” as the branch and R1 as the entrance within “First Floor.”

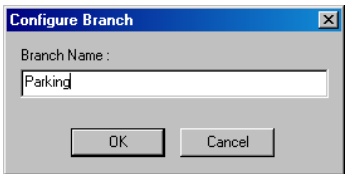


Readers, loops and doors that are already defined in the device map can be added to the access areas. The access areas are later mapped to access levels. The card holders who are associated with the access levels can gain access to the entrances in the access areas.

Adding a Branch

1. Choose **Configuration > Define > Access Areas**. The **Access Area** window appears.
2. Right-click the **Access Area** folder or branch and select **Add Branch**. The **Configure Branch** dialog box appears.





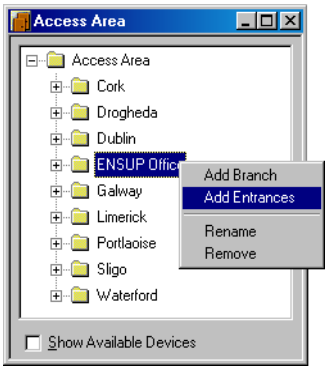
3. Type the **Branch Name**.
4. Click **OK**. The new branch is listed below the **Access Area** folder.

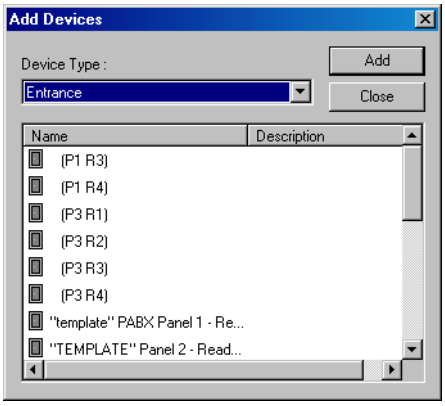
Note: If you are adding a branch inside another branch, the new branch appears below the selected branch.

Adding an Entrance

You can add entrances as an access area or you can group one or more entrances and add them under a branch in the access area.

1. Choose **Configuration > Define > Access Areas**. The **Access Area** window appears.
2. To add entrances as access areas, right-click the **Access Area** folder or to add entrances to a branch, right-click the branch and click **Add Entrances**. The **Add Devices** dialog box appears.
3. Alternatively, select the **Show Available Devices** check box. The **Add Devices** dialog box appears.





4. Select the entrance and click **Add**.

Note: To select the multiple entrances, press and hold down the CTRL key and click each entrance.

5. Click **Close** to close the **Add Devices** dialog box. Alternatively, clear the **Show Available Devices** check box. The newly added entrance(s) are displayed in the **Access Area** window.

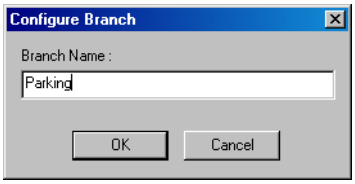
Moving an Entrance

To move an entrance from the access area to a branch or from one branch to another:

1. Choose **Configuration > Define > Access Areas**. The **Access Area** window appears.
2. Click the entrance that you want to move.
3. Drag and place the entrance on the branch to which you want to move.

Renaming a Branch

1. Choose **Configuration > Define > Access Areas**. The **Access Area** window appears.
2. Right-click the branch you want to rename.
3. Click **Rename**. The **Configure Branch** dialog box appears.



4. Type the new **Branch Name**.
5. Click **OK** to rename the branch.

Removing a Branch or Entrance

1. Choose **Configuration > Define > Access Areas**. The **Access Area** window appears.
2. Right-click the branch or the entrance you want to remove.
3. Click **Remove**. A message asking for confirmation appears.
4. Click **OK** to confirm the deletion.

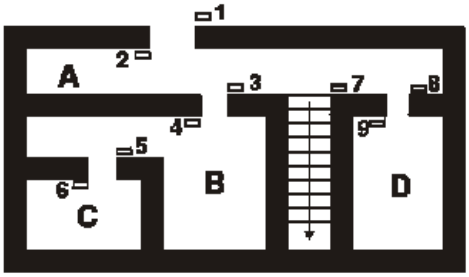
Note: You cannot remove an entrance if it is assigned to an access level.

Defining Tracking and Mustering Areas

Tracking and Mustering areas in WIN-PAK are logical areas consisting of entrances, and are used for tracking cardholder movements.

Tracking Areas

A tracking area is an area defined for tracking cardholder movements. When a cardholder presents a card in the tracking area, a read event is recorded along with the card-read details.



In the preceding diagram, A, B, C, and D are Tracking Areas. Readers 1, 4, and 9 allow access to Tracking Area A. Readers 3 and 6 allow access to Tracking Area B. Reader 5 allows access to Tracking Area C and Reader 8 allows access to Tracking Area D.

The first time a card holder presents a card at one of these readers, the details of the read event are recorded, and displayed in the **Tracking and Mustering View** window of the User Interface. Each time that card is presented at one of the readers in that same area, the details of the latest card-read is displayed in the user interface. When the card holder moves to a different tracking area, the card-read details for the new area is displayed. When the card holder moves out of the tracking area to a non-tracking area, the last card-read details of the card holder are removed from the user interface.

One tracking area can be nested inside the other. This enables better tracking of card holders in a specific area. For example, if “Building1” is created as a tracking area, then “Floor 1” and “Floor 2” can be created as nested areas in “Building1”. When a card holder enters “Building1”, the card-read details are recorded and displayed in the user interface. When the card holder moves to “Floor1”, the card-read details are displayed for “Floor1”.

Mustering Areas

Mustering areas are logical areas defined with readers, used for tracking card holder movements in the case of emergency situations like fire. Muster readers are placed in the mustering areas, which must be accessed by the card holders who are moving from the tracking areas into the mustering area. The details of the card holders moving into the mustering areas are recorded and, in addition, displayed in the **Tracking and Mustering View** window of the user interface.

Tracking and Mustering tree

In the **Tracking and Mustering** tree of the User Interface, the tracking and mustering areas are configured as **Branches** and the readers are configured as **Entrances**.

Exit Areas

The entrances that are not defined as a part of the tracking and the mustering areas are considered as exit areas. During WIN-PAK installation, a branch “Exit Area” is created by default. Card holders quitting the tracking areas present their cards to the readers in the exit area.

Nested Areas

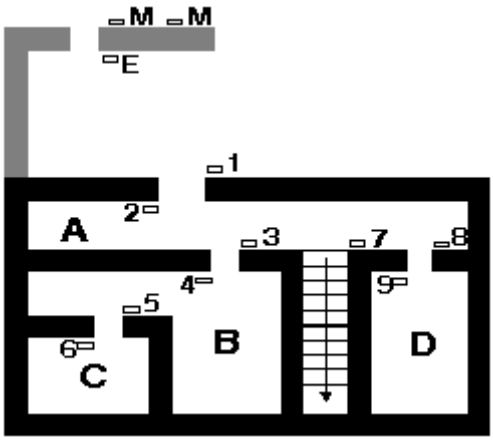
Nested areas are created when a tracking area is defined inside another tracking area and when a mustering area is defined under another mustering area. However, tracking areas cannot be nested inside mustering areas and vice versa.

When a area “A” is defined under area “B”, it indicates that the area “A” is nested under “B”. All the readers added under “A” belong to “B”.

Example:

- In a hospital, one branch can be defined as “Hospital” and another branch “Laboratory” can be added inside the “Hospital” branch. The “Laboratory” branch is nested inside the “Hospital” branch. When a card holder enters the laboratory, the card holder is seen as present in both the hospital and in the branch.
- If the “Laboratory” is not nested within the “Hospital” building, the card holder is seen as present only in the laboratory and not in the hospital.

Consider the following figure:



- **1-9** are Tracking Readers
- **A**, **B**, **C**, **D** are Tracking Areas,
- **M** is the Muster Reader
- **E** is the Exit Reader

The difference between nested and non-nested areas is explained in the following scenarios, for the areas B and C:

In case of Nested area,

- C is defined inside B. If you are in area C, then you are in area B.

- The readers 3, 6 are defined in B because both the readers are used for entering into B. Reader 3 is used for entering into B, and reader 6 is used for quitting C, and entering into B.
- The reader 5 is defined in C as it is used for entering into C. In addition, this is included in B because C is defined within B.

In case of Non-nested area,

- The areas B and C are defined separately.
- The readers 3, 6 are defined in B because both the readers are used for entering into B. Reader 3 is used for entering into B, and reader 6 is used for quitting C, and entering into B.
- The reader 5 is defined in C as it is used for entering into C.

Muster System Precautions

While creating mustering areas in WIN-PAK, keep the following precautions in mind:

1. Use a separate dropline (communication port) to isolate muster readers from tracking units.

   An alternate/additional communication path from the N-1000 to the computer is achieved by using the N485DRLA (Digital Redundant Loop Adapter).

   Note: Muster readers are not used for controlling a door.

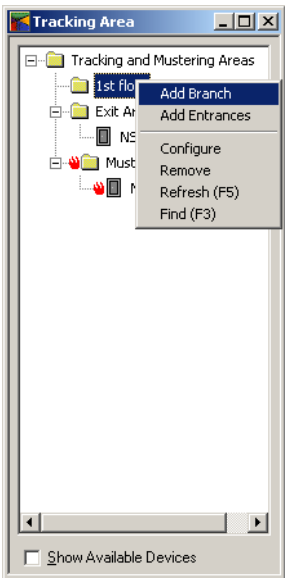
2. Run a special line for the muster units to provide a unique data path, even if the wiring from the main facility is damaged. The tracking units also have a unique data path.
3. Use 485 communications with ACK-NAK enabled. A battery backup power supply is required for the 485-API-2 on any N-1000 or NS2+ or P-Series panel.
4. Provide a UPS or other backup power source for the WIN-PAK computer and any other associated communication devices.
5. Provide a safe location for the computer and communication.
6. Keep the muster system on-line (not buffered) to ensure timely and complete information.
7. Perform regular checks to ensure that the muster system is functioning properly.
8. Check that all panels are maintaining the correct time and date. It is critical that the time and date be correct on card reads at the muster readers. If the time and/or date are earlier than that of other reads in the system they are ignored.
9. Program the scheduler to update the panel time and date at least once a day.
10. Create a check list for muster procedures.
11. Test the Muster Report printer.

Configuring Tracking Areas

Tracking areas can be defined as branches inside the Tracking and Mustering area tree in the WIN-PAK User Interface. Nested tracking areas can be created by defining branches one inside the other. After adding the branches for the tracking areas, you can add the readers in the tracking areas as entrances.

Adding a Tracking Area Branch

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.



2. Right-click the **Tracking and Mustering Areas** folder or the branch where you want to add the new branch, and select **Add Branch**. The **Tracking and Mustering Area Configuration** dialog box is displayed.

Note: You can add only entrances and not branches to the “Exit Area” branch that is created by default.

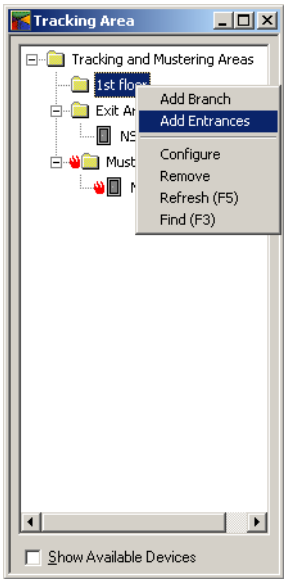
3. Type a name for the tracking area in **Name**.
4. Select the **Mustering** check box to define the area specified in **Name** as mustering area.

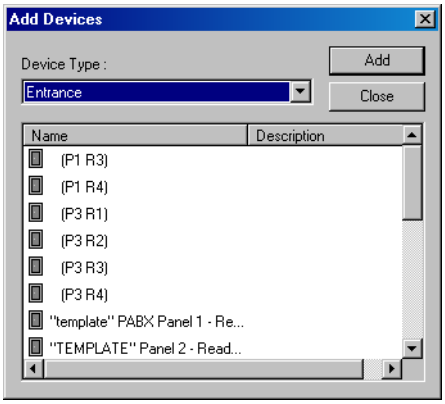
Note: This check box is disabled if you are defining an area inside another mustering area.

5. Click **OK**. The new branch is listed below the **Tracking and Mustering Areas** folder in the **Tracking Area** window.

Adding an Entrance to the Tracking Area

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click the branch to which you want to add an entrance and click **Add Entrances**. The **Add Devices** dialog box appears with the list of all entrances.
3. Alternatively, select the **Show Available Devices** check box. The **Add Devices** window appears with the list of all entrances.





4. Select the entrance to be added to the branch and click **Add**.

Note: To select the multiple entrances, press and hold down CTRL and click each of the required entrance.

5. Click **Close** or clear the **Show Available Devices** check box to close the window. The entrances are in the **Tracking Area** window.

Moving an Entrance

To move an entrance from one branch to another:

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Select the entrance you want to move.
3. Drag and place the entrance on the branch to which you want to move.

Notes:

- You cannot move an entrance from and to the "Exit Area" branch.
- You cannot move an entrance from a tracking area branch to a mustering area branch, and vice versa.

Renaming a Branch

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click the branch you want to rename.
3. Click **Configure**. The **Tracking and Mustering Area Configuration** dialog box appears.

4. Type the new branch name in the **Name** box.
5. Click **OK** to rename the branch.

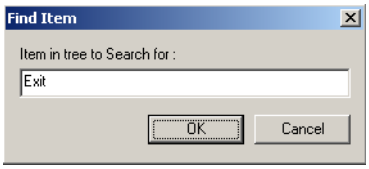
Removing a Branch or an Entrance

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click the branch or the entrance you want to remove.
3. Click **Remove**. A message asking for confirmation appears.
4. Click **OK** to remove the selected branch or entrance.

Note: You cannot remove the "Exit Area" branch.

Finding an Item in the tree

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click on a branch or entrance, and click **Find**. The **Find Item** dialog box appears.



3. Type the item you want to search in the tree, in the **Item in tree to Search for** box.
4. Click **OK**. The item, if found, is highlighted in the tree.

Notes:

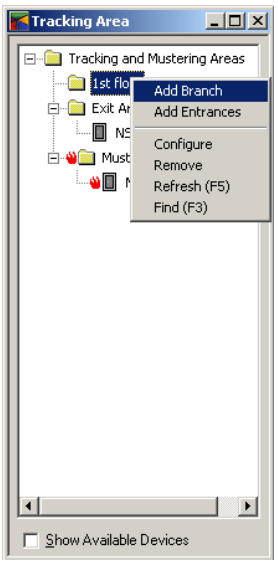
- From a tracking area you cannot search for a branch or an entrance in the mustering area.
- Right-click on a branch, and click **Refresh** to refresh the items in the tree.

Configuring Mustering Areas

Mustering areas are defined as branches of the **Tracking and Mustering** area tree of the WIN-PAK User Interface. Nested mustering areas can be created by defining branches one inside the other. After adding the branches, you can add the readers in the mustering areas as entrances.

Adding a Mustering Area Branch

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.



2. Right-click the **Tracking and Mustering Areas** folder or the branch where you want to add the new branch, and select **Add Branch**. The **Tracking and Mustering Area Configuration** window is displayed.

Note: You cannot add mustering area branches to the “Exit Area” branch.

3. Type a name for the mustering area in **Name**.
4. Select the **Mustering** check box to define the area as a mustering area.

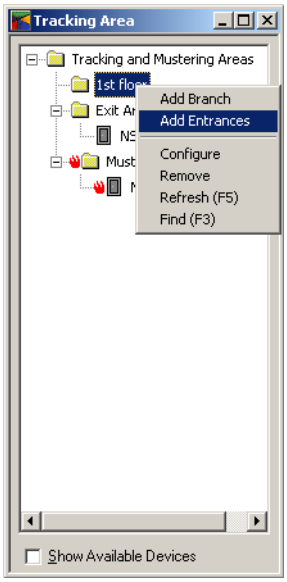
Note: The check box appears disabled if you are defining an area inside another mustering area.

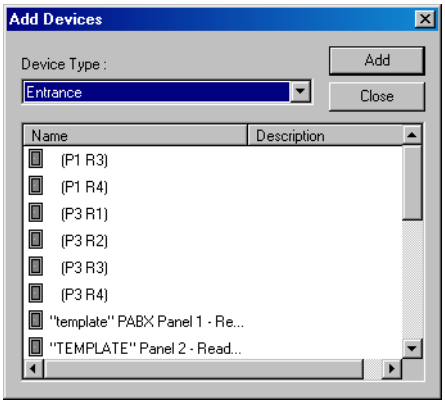
5. Click **OK**. The new branch is displayed in the **Tracking Area** window.

Note: The icon for the branches defined as mustering area appears as .

Adding an Entrance to the Mustering Area

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click the **Tracking and Mustering Areas** folder or the mustering area branch to which you want to add an entrance and click **Add Entrances**. The **Add Devices** dialog box appears with the list of all entrances.
3. Alternatively, select the **Show Available Devices** check box. The **Add Devices** window appears with the list of all entrances.





4. Select the entrance to be added to the branch and click **Add**.

Note: To select the multiple entrances, press and hold down CTRL and click each of the required entrances.

5. Click **Close** or clear the **Show Available Devices** check box to close the window. The entrances are in the **Tracking Area** window.

Moving an Entrance

To move an entrance from one branch to another:

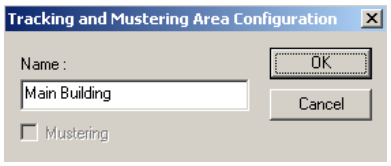
1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Under a mustering area branch, select the entrance you want to move.
3. Drag and place the entrance on the mustering area branch to which you want to move.

Notes:

- You cannot move an entrance from and to the "Exit Area" branch.
- You cannot move an entrance from a mustering area branch to a tracking area branch.

Renaming a Branch

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click the branch you want to rename.
3. Click **Configure**. The **Tracking and Mustering Area Configuration** dialog box appears.



4. Type the new branch name in the **Name** box.
5. Click **OK** to rename the branch.

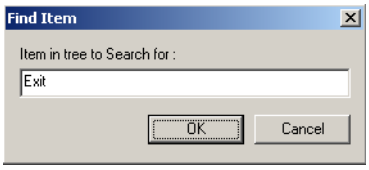
Removing a Branch or an Entrance

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click the branch or the entrance you want to remove.
3. Click **Remove**. A message asking for confirmation appears.
4. Click **OK** to remove the selected branch or entrance.

Note: You cannot remove the "Exit Area" branch.

Finding an Item in the tree

1. Choose **Configuration > Define > Tracking Areas**. The **Tracking Area** window appears.
2. Right-click the mustering area branch or entrance, and click **Find**. The **Find Item** dialog box appears.



3. Type the item you want to search in the **Item in tree to Search for** box.
4. Click **OK**. The item, if found, is highlighted in the tree.

Notes:

- From a tracking area you cannot search for a branch or an entrance in the mustering area.
- Right-click on a branch, and click **Refresh** to refresh the items in the tree.

Tracking and Muster View

The tracking and muster view enables you to view the details of the card holders who are present in the tracking and the mustering areas.

The tracking and the muster areas are displayed in a tree in the **Tracking and Muster View** window. Select the tracking or muster area in the tree, to view the details of the card holders present in the area.

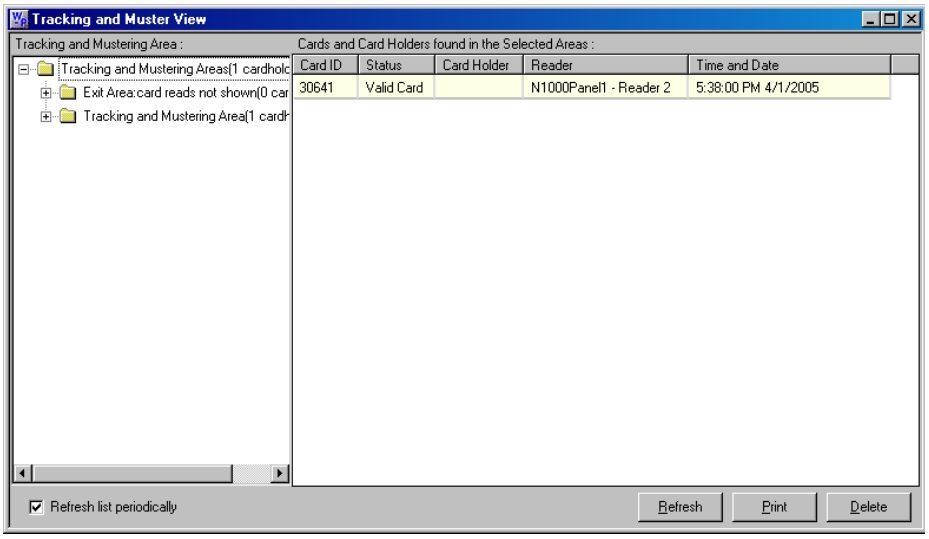
Before viewing the muster information, ensure the following:

1. Verify that muster reads from the panel have the correct time and date.
2. If the date and time are wrong, stop the presentation of cards and send the time and date to the panel.
3. Test the correction.
4. Repeat all card presentations. Multiple presentations of the same card at the muster reader do not adversely affect the result of the muster as the most recent time and date stamp is displayed.

Viewing the Tracking and Mustering details

To view the details of card holders in tracking or mustering areas:

1. Choose **Operations > Tracking and Mustering**. The **Tracking and Muster View** window appears.

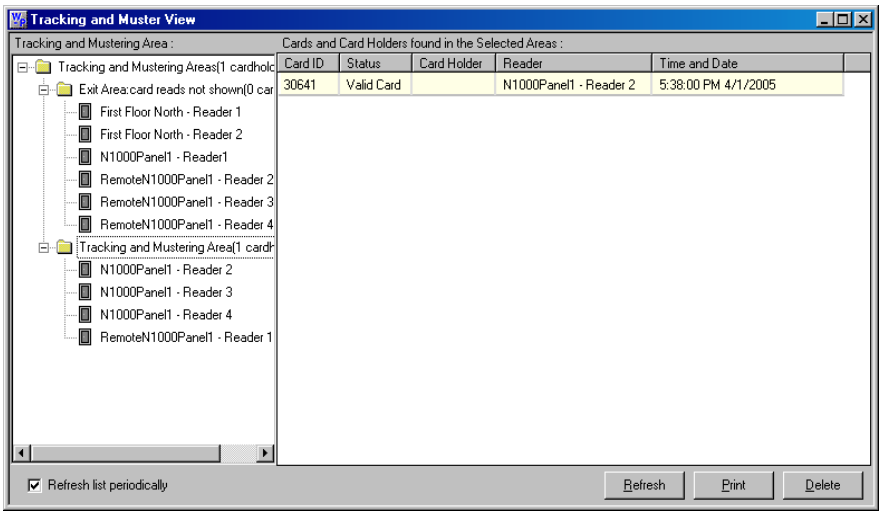


2. Expand the **Tracking and Mustering Areas** folder to list the branches and the entrances belonging to the selected branch.

Note: The branches and entrances with on the left indicate muster areas and muster readers.

3. Select the branch for which you want to view the card holder information.
   - Select a muster area branch to view the details of card holders who have accessed the readers in the mustering area.
   - Select a tracking area branch to view the details of card holders who have accessed the readers in the tracking area.
   - Select "Exit Area" branch to view the details of card holders who have accessed the readers in the exit area.

   The details of the card holders who have accessed the entrances in the selected branch are listed in the right pane of the **Tracking and Muster View** window.



4. Select the **Refresh List periodically** check box to automatically update the list of card holders every few seconds. Alternatively, click **Refresh** to refresh the list of card holders.
5. Click **Close (X)** on top of the window to close the window.

Deleting a Card holder from the Tracking and Muster View

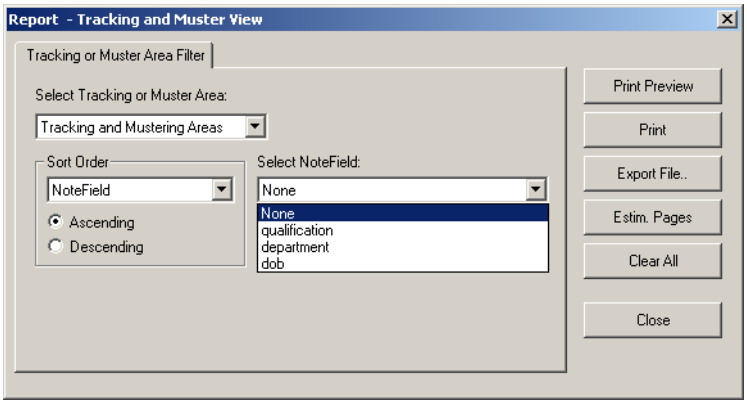
When a card holder has moved out of the tracking area without accessing the reader in the area, you can delete the card holder details from the **Tracking and Muster View** window.

To delete the details of a card holder:

1. In the **Tracking and Muster View** window, select the card holder detail from the list on the left pane.
2. Click **Delete** to delete the card holder detail.

Printing Tracking and Mustering details

1. In the **Tracking and Muster View** window, click **Print**. The **Report - Tracking and Muster View** dialog box appears.



2. In the **Select Tracking or Muster Area** list, select the tracking or mustering area for which you want to print the card holder details.
3. To print the card holder information in a sorted order, select the option for sorting in the **Sort Order** list.
    - Select **Time and Date** to sort the card holder details in a chronological order.
    - Select **Card Number** to sort the card holder details based on the card number.
    - Select **Card Holder** to sort the card holder details based on the card holder number.
    - Select **Note Fields** to sort the card holder details based on the Note field value. When you select this option, the **Select NoteField** list is enabled.

Notes:

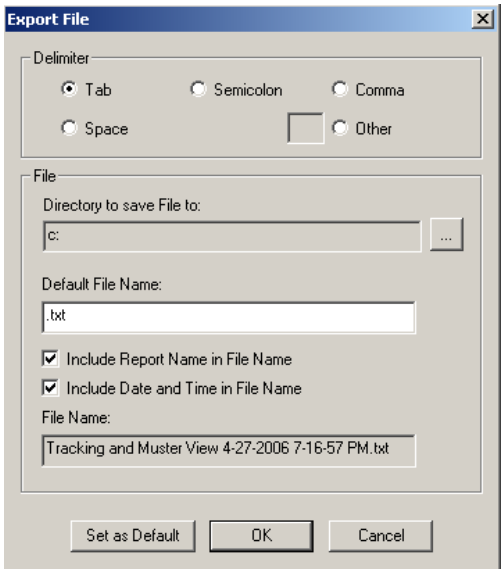
- If you do not have a privilege to create a note field template, the **Note Fields** option will not be listed in **Sort Order**.
- If you do not have the privilege for viewing or changing a note field, the note field will not be listed in **Select NoteField**.
- The **Select NoteField** list contains the note fields that are specific to the selected account. If **<All Accounts>** is selected, the note fields that are common to all the accounts are listed. You can create a common note field by creating a note field in each account with the same name.

4. To sort the card holder details in the ascending order, click **Ascending**.

   OR

   To sort the card holder details in the descending order, click **Descending**.

5. To preview the report before printing, click **Print Preview**.
6. To print the card holder report, click **Print**.
7. To export the card holder details into a text file, click **Export File**. The **Export File** dialog box appears.



   a. Under **Delimiter**, click the required delimiter character or click **Other** and enter the character.

   b. Under **File**, enter the following details:

   c. Click the ellipsis button in the **Directory to Save File to** box to select the folder in which the text file must be saved.

   d. Type the name of the text file in the **Default File Name** box.

e. To append the report name to the file name, select the **Include Report Name in File Name** check box.

f. To append the date and time to the file name, select the **Include Date and Time in File Name** check box.

g. To set the delimiter and file name information as default for all text files, click **Set as Default**.

h. Click **OK** to export card holder details to the file.

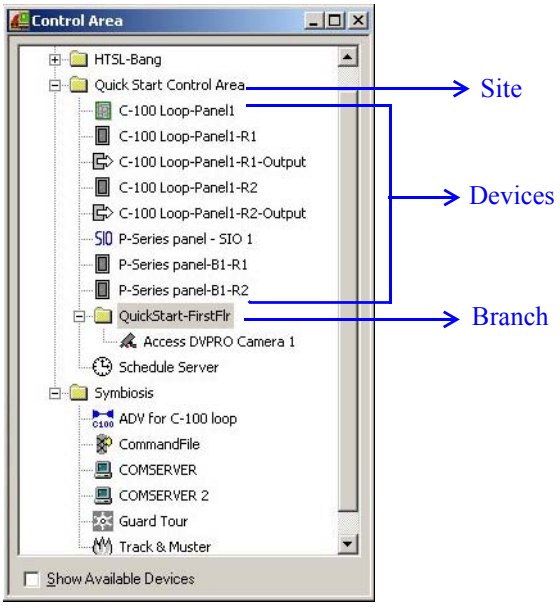
8. To know about the number of pages that would be printed, click **Estim Pages**.
9. To clear the filter criteria, click **Clear All**.
10. To close the **Report-Tracking and Muster View** dialog box, click **Close**.

Defining Control Areas

Control areas are logical areas containing devices such as communication servers, loops, panels, input points, output points, groups, and readers.

Control Areas are defined by creating a Control Map of the devices and adding them to a tree structure. This map shows the status of each device, the set of actions to be performed for the device when an event takes place, and the relationship between the various devices.

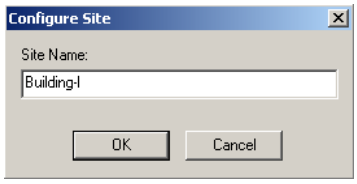
Control Maps are defined by adding a site, adding branches to the site and then adding devices to the branches. The devices can also be added directly to a site.



Adding a Site

To add a new site:

1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Right-click **Control Area** folder and then click **Add Site**. The **Configure Site** dialog box appears.

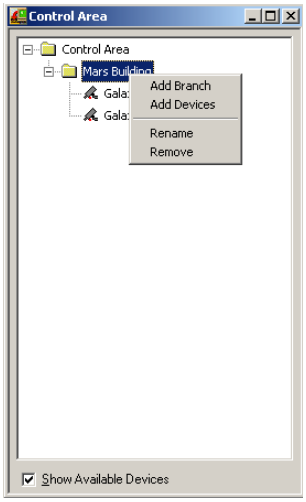


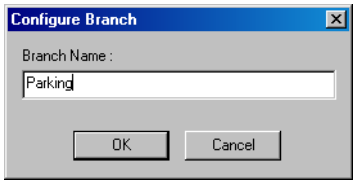
3. Enter the **Site Name**.
4. Click **OK** to add the site as a control area.

Adding a Branch to a Site

1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Right-click the site to which you want to add the branch and click **Add Branch**. The **Configure Branch** dialog box appears.

Note: You can add a branch under another branch. In such case, right-click the branch and click **Add Branch**.

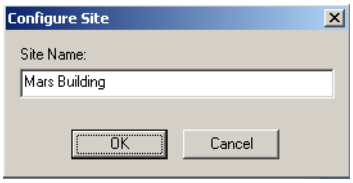




3. Type the **Branch Name**.
4. Click **OK**. The branch is listed under the site or the branch in the **Control Area** window.

Renaming a Site or a Branch

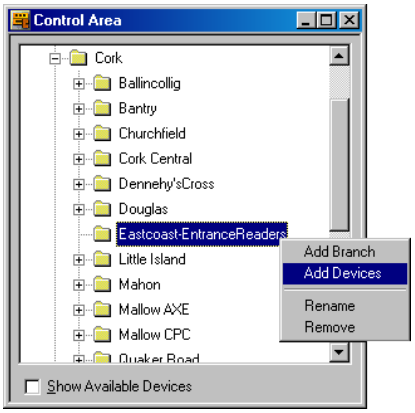
1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Right-click the branch or the site you want to rename.
3. Click **Rename**. The dialog box for renaming the branch or site appears.

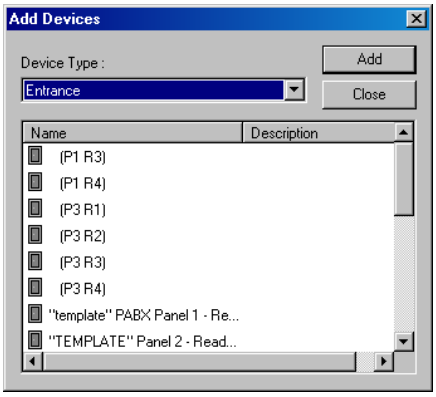


4. Type the site or the branch name.
5. Click **OK** to save the change.

Adding a Device

1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Right-click the site or branch to which you want to add the device and click **Add Devices**. Alternatively, select the **Show Available Devices** check box. The **Add Devices** dialog box appears.





3. Select the **Device Type**. The devices belonging to the selected device type are listed.

Note: The device type includes devices of intrusion panel too, if the license for the Galaxy panel and/or the Vista panel is procured.

4. Select the device to be added and click **Add**.

Note: To select the multiple devices, press and hold down CTRL and click each entrance.

5. Click **Close** or clear the **Show Available Devices** check box to close the **Add Devices** dialog box. The device(s) are displayed in the **Control Area** window.

Moving a Device

To move a device from one branch to another:

1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Click the device you want to move.
3. Drag and place the device on the branch or the site to which you want to move.

Removing a Site, Branch or Device

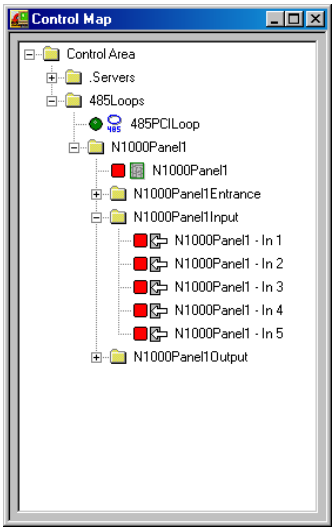
1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Right-click the branch, site or device you want to remove.
3. Click **Remove**. A message asking for confirmation appears.
4. Click **OK** to remove the selected site, branch or device. The site, branch or device is removed from the control map.

Viewing Control Maps

Control Map enables you to view and control the devices belonging to the control area. In addition, you can view the status, acknowledge and clear alarms, and run various commands for each device.

Controlling Devices from a Control Map

1. Choose **Operations > Control Map**. The **Control Map** window appears.



2. Expand the control area to view the details of its branches and devices.

   The status of each device is indicated by the following icons to the left of the device name:

   - Normal status

   - Alarm condition

   ? - Unknown status

The icons for the Galaxy devices and Vista devices vary depending on the action that is set on them. In addition, the icon color changes for various device status. The following table provides you various icons that are displayed for different status:

Device Types	Action	Icon	Status	Description
Group/Partition Zone	Set/Arm Reset/Disarm Unbypassed		Normal	No alarm in the Alarm View window (Alarm is acknowledged and cleared)
			Normal	Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)
			Alarm	No alarm in the Alarm View window (Alarm is acknowledged and cleared)
			Alarm	Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)
Group/Partition Zone	Unset Bypassed		Normal	No Alarm in the Alarm View window (Alarm is acknowledged and cleared)
			Normal	Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)
			Alarm	No Alarm in the Alarm View window (Alarm is acknowledged and cleared)
			Alarm	Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)
Zone	Tamper		Alarm	No Alarm in the Alarm View window (Alarm is acknowledged or cleared)
			Alarm	Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)

Device Types	Action	Icon	Status	Description
Zone	Tamper Bypassed		Alarm	No Alarm in the Alarm View window (Alarm is acknowledged and cleared)
			Alarm	Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)
Output	Activated		Normal	Normal - No Alarm in the Alarm View window (Alarm is acknowledged and cleared)
			Normal	Normal - Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)
Output	Deactivated		Normal	Normal - No Alarm in the Alarm View window (Alarm is acknowledged and cleared)
			Normal	Normal - Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)
All types	Any action	?	Unknown	No Alarm in the Alarm View window (Alarm is acknowledged and cleared)
		?	Unknown	Alarm in the Alarm View window (Alarm waiting to be acknowledged or cleared)

Move the mouse over the icons to view a textual description of each device status.

3. To control a device, right-click the device and select the command.

The commands available for each ADV control are listed in the following table:

Table 11-1 Typical ADVs and Control Functions

ADV	Control Functions
Alarm View	Open Click **Open** to open the **Alarm View** window through the floor plan.
CCTV Switcher	Send Time & Date, Send Camera Titles, Camera to Monitor Switch, Acknowledge All Alarms, Clear All Alarms
Comm Server	Acknowledge All Alarms, Clear All Alarms

Table 11-1 Typical ADVs and Control Functions

ADV	Control Functions
Command File Server	Run Command File
C-100 Local Connection	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms
C-100 Remote Connection	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms, Connect Remote, Disconnect Remote
Doors	Unlock, Lock, Shunt, Unshunt, Pulse, Timed Pulse, Restore to Time Zone, Acknowledge All Alarms, Clear All Alarms
Event View	Open Click **Open** to open the **Event View** window through the floor plan.
Input Points	Acknowledge all Alarms, Clear all Alarms, Shunt, Unshunt, Restore to Time Zone
Links	Open Click **Open** to open the floor plan to which this floor plan is linked. This device is relevant only for the Floor Plan.
Modem Pool	Hang-Up Modem, Reset Modem, Acknowledge All Alarms, Clear All Alarms
CCTV Monitor	Acknowledge All Alarms, Clear All Alarms
N-485 Remote Dialup	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Connect, Remote, Disconnect Remote, Acknowledge All Alarms, Clear All Alarms
N-485 Local Connection	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms
Output Points & Groups	Energize, De-energize, Pulse, Timed Pulse, Restore to Time Zone, Acknowledge All Alarms, Clear All Alarms
Panel	Initialize, Cancel Initialization, Buffer, UnBuffer, Acknowledge All Alarms, Clear All Alarms Refer to the "Initializing a Panel from Control Map" section in this chapter for initializing a panel
Pan / Tilt Camera	Acknowledge All Alarms, Clear All Alarms
Readers	Acknowledge All Alarms, Clear All Alarms
SIO Boards	Acknowledge All Alarms, Clear All Alarms

Table 11-1 Typical ADVs and Control Functions

ADV	Control Functions
Static Camera	Acknowledge All Alarms, Clear All Alarms
Galaxy Communication	Acknowledge All Alarms, Clear All Alarms
Galaxy Panel	Acknowledge All Alarms, Clear All Alarm **Set All Groups** - Panel sets all the groups associated to the panel. **Unset All Groups** - Panel unsets all the groups associated to the panel. **Reset Panel** - Resets the panel. **Bypass Zones** - Panel bypasses alarms from the selected zone types. **Unbypass Zones** - Panel stops bypassing alarms the selected zone types. **Activate Output** - Activates the selected output. **Deactivate Output** - Deactivates the selected output. To select a zone type or output type, right-click the Galaxy panel and select the appropriate action, and then select the zone type or output type.
Galaxy Group	Acknowledge All Alarms, Clear All Alarms **Set Group** - Panel sets the selected group. **Unset Group** - Panel unsets the selected group. **Part Set** - Panel sets all the zones for which the Zone State (attribute) is set as Part Set. **Timed Set** - Panel sets all the zones after a specific time. **Group Bypass** - Panel bypasses alarms from all the zones in the group. **Group Unbypass** - Panel stops bypassing alarms from all the zones in the group. **Refresh** - Refreshes the latest status of a group. Acknowledge All Alarms, Clear All Alarms
Galaxy Zone	Acknowledge All Alarms, Clear All Alarms **Bypass Zone** - Panel bypasses alarms from the zone. **Unbypass Zone** - Panel stops bypassing alarms from the selected zones. **Force bypass Zone** - Forcefully bypasses the zones which cannot be bypassed using the Bypass Zone option. For example, Fire. **Refresh** - Refreshes the latest status of a zone.

Table 11-1 Typical ADVs and Control Functions

ADV	Control Functions
Galaxy Output	Acknowledge All Alarms, Clear All Alarms **Activate** - Activates the output. **Deactivate** - Deactivates the output. **Refresh** - Refreshes the latest status of an output.
Galaxy Keypad	Acknowledge All Alarms, Clear All Alarms
Galaxy MAX	Acknowledge All Alarms, Clear All Alarms
Galaxy RIOs	Acknowledge All Alarms, Clear All Alarms
Vista Panel	Acknowledge All Alarms, Clear All Alarms **Arm Away** - The panel completely arms the selected perimeter and interior burglary partitions by sensing the intruder's movements. This option enables you to select multiple partitions of the panel. **Arm Stay** - Arms only the perimeter burglary protection, guarding protected doors, windows, and other perimeter protection points in the selected partitions. This enables automatic bypassing of certain areas that allows movement on those areas without causing an alarm. **Note:** To define the perimeter area, the zone type of the zones must be defined as Perimeter while configuring the Vista Panel. **Disarm** - The panel disarms the selected burglary partitions, silences alarms and audible trouble indicators. This option enables you to select multiple burglary partitions in the panel. **Panel Reset** - Resets the panel. **Refresh** - Refreshes the latest status of the vista panel.
Vista Partition	Acknowledge All Alarms, Clear All Alarms **Arm Away** - The panel completely arms the perimeter and interior burglary partition by sensing the intruder's movements. **Arm Stay** - Arms only the perimeter burglary protection, guarding protected doors, windows, and other perimeter protection points in the partition. This enables automatic bypassing of certain areas that allows movement on those areas without causing an alarm. **Note:** To define the perimeter area, the zone type of the zones must be defined as Perimeter while configuring the Vista Panel. **Disarm** - The panel disarms the selected burglary partition, silences alarms and audible trouble indicators.

Table 11-1 Typical ADVs and Control Functions

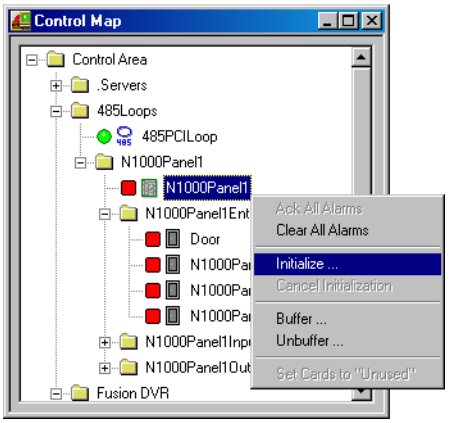
ADV	Control Functions
Vista Zone	Acknowledge All Alarms, Clear All Alarms **Bypass Zone** - The panel bypasses alarms from the zone. This allows movement on the bypassed area without causing an alarm. **Unbypass Zone** - The panel stops bypassing alarms from the selected zone.
Vista Output	Acknowledge All Alarms, Clear All Alarms **Activate** - Activates the output. **Deactivate** - Deactivates the output. **Refresh** - Refreshes the latest status of an output.

Initializing a Panel from Control Map

When panels are added to the WIN-PAK system, they are initialized so that the information entered during panel configuration is sent to the panels. Panels are initialized from the Floor Plan view or from the Control Map.

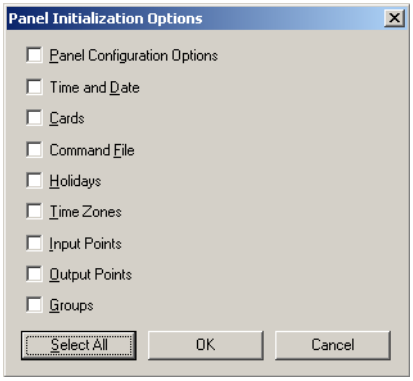
To initialize panels from the control map:

1. Choose **Operations > Control Map**. The **Control Map** dialog box appears.



2. Right-click the desired panel in the Control Map tree, and select **Initialize**. The **Panel Initialization Options** dialog box appears.

Note: The options available on the Panel Configuration Options dialog box are device-dependent.



Refer to the "Panel Initialization Options" section in this chapter to know the description for initialization options.

3. To send all types of information, click **Select All**.

   OR

   To update only the selected information, select the corresponding check boxes.

4. Click **OK** to update the panel details.

Refer to the "Initializing Status" section in this chapter for details on status of the initialization.

Panel Initialization Options

Table 11-2 Describing panel initialization options

Panel Initialization Options	**Description**
Panel Configuration Options	Sends all panel configuration information. This resets your panel programming. It is recommended that you use the "Select All" feature (button) when the Panel Configuration Options are to be sent.
Time & Date	Updates panel time and date with the network time and date. You may notice a pause for up to 50 seconds when the time and date are sent because the time is sent at the top of the computer minute up to + 10 seconds. Closed circuit acts as a NC circuit.
Cards	Sends card information to the panel. When sending cards, it is recommended that you re-initialize the panel by choosing **Select All**. This ensures that old card information is removed when the new card information is added. When cards with an Active or Trace status are added, edited, or deleted from the card or card holder database, this information is automatically sent to the panels. All other card information changes are sent using this command.

Additionally, new or updated information on the following features, functions, and panel elements are sent to the panel:

- Access Levels
- Access Control Areas
- Card Formats
- Command File
- Conversion Tables
- Groups
- Holidays
- Inputs
- IC Configuration
- Input Groups
- Input Scan
- Outputs
- Procedures/Actions
- SIO Boards
- Triggers
- Reader LED/Buzzer specs
- Time Zones

Initializing Status

As the panel initializes, a status window indicates the status of sending the information. If an error occurs, the status window indicates which command caused the error.

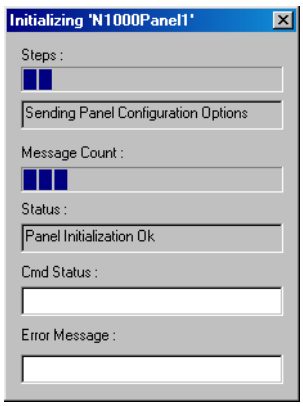


Figure 11-1 Showing the status of initialization

Table 11-3 Describing fields in the Status dialog box

Field name	Description
Steps	Indicates what information is sent.
Message Count	Indicates the progress of messages sent.
Status	Indicates whether the proceeding initialization is successful or has failed.
Cmd Status	Indicates if a command has timed out.
Error Message	Indicates if any errors occurred while transmitting information to the panel.

Floor Plan

12

In this chapter...

Introduction

A floor plan is a map or plan of a building, used for viewing, monitoring, and controlling devices in the Access Control System.

This chapter describes how to create floor plans and to control system devices using floor plan views.

A floor plan comprises a floor plan background on which ADVs, links, and text blocks are placed. Images, photos, and simple graphs can be imported into the floor plan background. These images are imported as graphic files (Windows Metafile) and are stored in the **WINPAK PRO\Database\ FloorPlanImage** folder.

ADVs, representing devices in the Access System, can be added to a floor plan. These ADVs can be monitored and controlled from the floor plan. Different objects (for example, a door, a panel or a C-100 loop) are available in the toolbox for the types of ADVs.

Links to other floor plans can be added to a floor plan. These links enable you to view other floor plans from the currently open floor plan.

Links to Alarm View and Event View of devices can be added to a floor plan. These links enable you to view the alarm and the event views of devices from the floor plan.

Text blocks can be added to the floor plan for adding additional information in the floor plan. For example, you can add a text block for creating a legend, explaining the color codes of the ADVs, or special instructions for the operator for viewing a particular floor plan.

After the floor plan is created with ADVs, links, and text blocks, you can view it through a floor plan view to monitor the status of the ADVs, and to control the ADVs by commands.

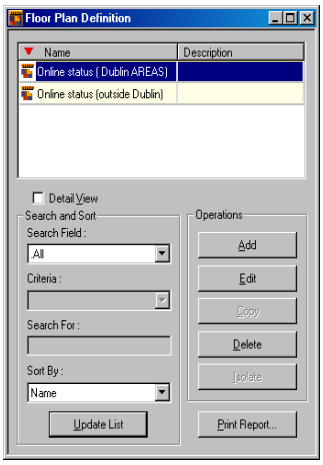
Floor Plan Definition

Defining a floor plan involves:

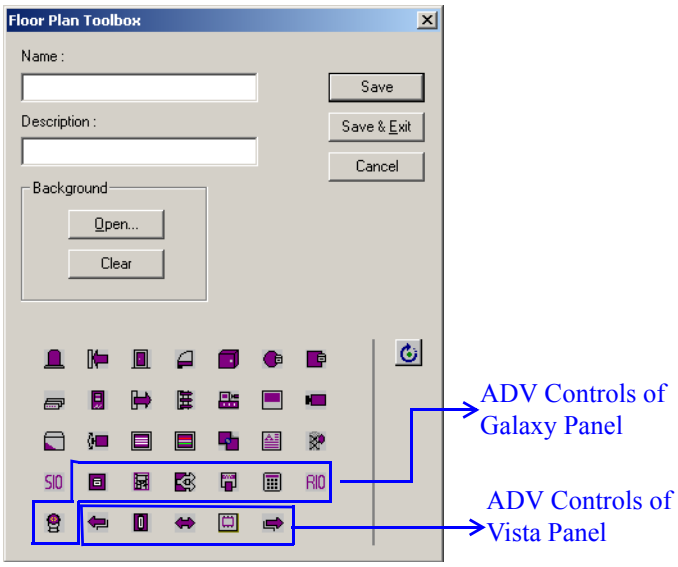
1. Adding a floor plan.
2. Creating floor plan designs, which involves placing ADVs on the floor plan, providing links to other floor plans, and links to alarm and event views.
3. Adjusting the size of the floor plan and previewing it.
4. Editing and deleting a floor plan.

Adding a Floor Plan

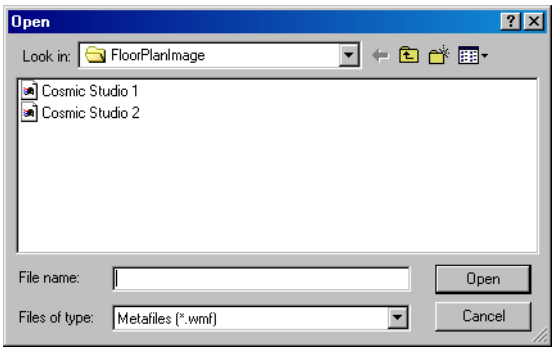
1. Choose **Configuration > Floor Plan Definition**. The **Floor Plan Definition** window appears.



2. Click **Add**. The **Floor Plan Toolbox** dialog box together with a blank window for creating a floor plan design appear.



3. Type a name for the floor plan in **Name**. The name can be up to 30 alphanumeric characters in length.
4. Type a **Description** for the floor plan. The description can be up to 60 alphanumeric characters in length.
5. Click **Open** in the **Background** area. The **Open** dialog box appears.



6. Browse to the location of the image file and click **Open**. The selected graphic file opens in the window behind the **Floor Plan Toolbox** window and is also saved in the **WINPAK PRO\Database\ FloorPlanImage** folder.
7. Add ADVs, links, and text objects to the background.

   Refer to the "Creating Floor Plan Design" section in this chapter for more details on adding ADVs, links, and text objects to the floor plan.
8. In the **Floor Plan Toolbox** dialog box, click **Save & Exit** to save the floor plan and return to the **Floor Plan Definition** window.
9. Click **Close (X)** to close the **Floor Plan Definition** window.

Note: The ADV controls of the Galaxy panel and/or Vista panel are available only if the license for the Galaxy and/or Vista panel is procured.

Creating Floor Plan Design

Designing a floor plan involves:

- Placing ADVs that must be monitored and controlled from the floor plan.
- Adding text blocks and links to other floor plans.
- Adding Event View and Alarm View links to the floor plan.

To create a floor plan design:

1. Choose **Configuration > Floor Plan Definition**. The **Floor Plan Definition** window appears.
2. Click **Add** to add a new floor plan or highlight a floor plan from the database list and click **Edit** to modify the selected floor plan. The **Floor Plan Toolbox** window together with the floor plan design window appear.
3. Add ADVs, Floor Plan links, Alarm View and Event View Links, and Text Blocks to the floor plan.

   Refer to the sections "Adding an ADV to the Floor Plan", "Adding Links to other Floor Plans", "Adding Alarm View and Event View links to the Floor Plan" and "Adding a Text Box to the Floor Plan" for information on adding ADVs, links, or text objects to the floor plan.

Adding an ADV to the Floor Plan

ADVs that must be monitored and controlled from the floor plan are added to the floor plan design.

After adding ADVs to the floor plan, you can set the control properties for each of them. The control properties vary for each ADV control.

The following are the common control properties that can be set for an ADV:

General Configuration

- Enter the ADV name.
- Link the ADV control to the ADV.
- Set the rotation angle of the ADV.
- Specify whether the ADV name must appear with the ADV control in the floor plan.
- Specify whether a tool tip for the ADV must appear when you move the mouse over the ADV.

Status Configuration

- **Color**: A color swatch appears next to the various states for the selected ADV (the states vary depending on the type of device). Change the color scheme by selecting new colors for the three conditions (no alarms, alarms, alarms acknowledged) for each state.
- **Blink**: Set the blink settings for the various ADV states.

To add an ADV to the floor plan:

1. In the **Floor Plan Toolbox** window, drag and drop an ADV into the floor plan background.

   Refer to the following table for information on ADV icons, ADV names, and description:.

   Table 12-1 ADV Icons and Description

Icon	Name	Description
	**Input**	Signals an alarm condition.
	**Input II**	Signals an input condition or state that is not associated with an alarm condition.
	**Door**	Used with Entrance ADV.
	**Door II**	Used with Entrance ADV for configuring four different types of doors, namely, left, right, double, or garage. Each door type displays an open or closed animation.
	**Panel**	Used with all control panels.

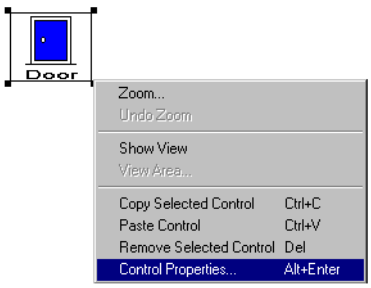
Table 12-1 ADV Icons and Description

	**Loop C-100**	Used with C-100 ADV.
	**Loop PCI**	Used with N-485-PCI ADV.
	**Modem Pool**	Used with Modem Pool ADV.
	**Communication Server**	Used with the communication server ADV.
	**Output**	Used with relay output ADV.
	**Group**	Used with relay group ADV.
	**Switcher**	Used with the CCTV switcher ADV.
	**Monitor**	Used with the monitor ADV.
	**Stationary Camera**	Used with the stationary camera ADV.
	**Reader**	Used with the reader ADV.
	**Pan/Tilt Camera**	Used with pan/tilt camera ADV.
	**Text**	Used for providing any additional information in the floor plan.
	**Command File Server**	Used with the command server ADV. Enables you to select and run a command file.
	**SIO Board**	Used with the SIO Board ADV. Provides tamper and power status of the PRO-2200 SIO boards.
	**Galaxy Communication**	Used with Galaxy Ethernet module (E080) ADV.
	**Galaxy Panel**	Used with Galaxy panel ADV.

Table 12-1 ADV Icons and Description

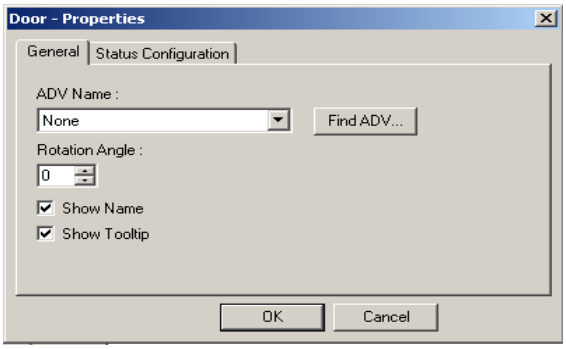
	Galaxy Group	Used with Galaxy group ADV.
	Galaxy MAX	Used with Galaxy MAX ADV.
	Galaxy Keypad	Used with Galaxy keypad ADV.
	RIO Control	Used with Galaxy RIO control ADV.
	Galaxy Output	Used with Galaxy output ADV.
	Galaxy Zone	Used with Galaxy zone ADV.
	ADV Rotation Tool	Used for rotating the ADV object.
	Vista Panel	Used with Vista panel ADV.
	Vista Partition	Used with Vista partition ADV.
	Vista Zone	Used with Vista zone ADV.
	Vista Output	Used with Vista output ADV.
	Vista Comm	Used with the Vista panel port ADV.

2. Right-click the object and select **Control Properties**.



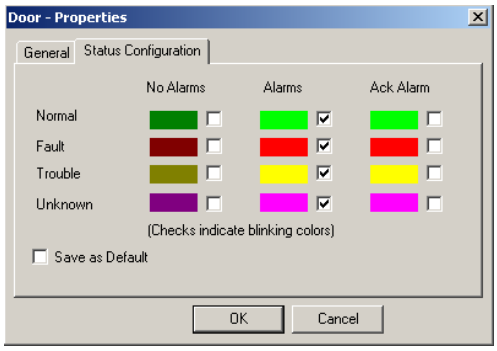
The **Control Properties** dialog box appears for the ADV object.

Example: If you have selected a door, then the **Door - Properties** dialog box appears.



3. To set the general properties of the ADV, click the **General** tab.
    a. Select the **ADV Name** or click **Find ADV** to locate the ADV to be associated to the object. The **Find ADV** dialog box appears.

    b. Type or select the name of the ADV in the **Name** list and click **Find Now**. A list of ADVs with similar names are retrieved in the list.
    c. Select an ADV from the list and click **OK** to return to the properties dialog box.
    d. Enter the angle at which the ADV must be rotated in **Rotation Angle**. By default, the rotation angle is set as zero.
    e. Select the **Show Name** check box to display the name of the ADV below the image in the floor plan design window.
    f. Select the **Show Tooltip** check box display the ADV name as a tool tip.
4. To set the color, blink, and default options for the ADVs, click the **Status Configuration** tab.



a. To change the colors for each state (Normal, Fault, Trouble, and Unknown), double-click the color swatch to open the **Color** dialog box.

b. Select a standard color or create a custom color and then click **OK**. The selected color appears in the swatch.

c. Repeat this for every color you want to change.

d. To set the blink option for a state-condition combination, select the check box provided next to the color swatch. Clear the check box to remove the blink option.

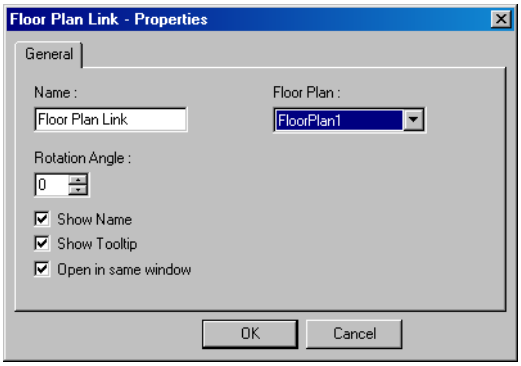
5. Select the **Save as Default** check box to set the configuration details as default.
6. Click **OK** to save the ADV properties and to return to the **Floor Plan Toolbox** window.

Adding Links to other Floor Plans

A floor plan link object enables you to open another floor plan within the current floor plan. You can view the floor plan that you open and control the devices that are placed on it. However, you cannot add new or remove the existing objects from the floor plan.

To add a floor plan link:

1. In the **Floor Plan Toolbox** window, drag and place it into the floor plan background.
2. Right-click the object and select **Control Properties**. The **Floor Plan Link - Properties** dialog box appears.



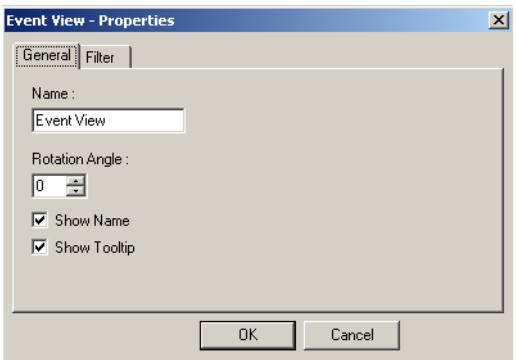
3. Type a name for the floor plan link in **Name**. By default, the link appears with **Floor Plan Link** as its name.
4. Select the name of the floor plan to be linked in the **Floor Plan** list.
5. To rotate the ADV control, enter the **Rotation Angle** or use the scroll bars to select an angle from the list.
6. Select the **Show Name** check box to display the name of the floor plan link below the ADV in the floor plan.
7. Select the **Show Tooltip** check box to display the ADV name as a tool tip.
8. Select the **Open in same window** check box to replace the original floor plan with the target floor plan in the floor plan view. Clear this check box to open the target floor plan in a new window.
9. Click **OK**.

Adding Alarm View and Event View links to the Floor Plan

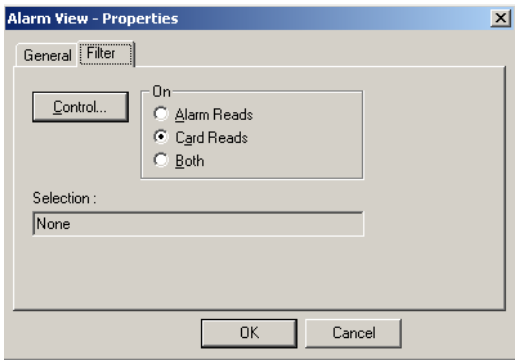
Alarm View and Event View links enable you to view the alarms and events occurring for a device from the floor plan.

To add an Alarm View or an Event View link to the floor plan:

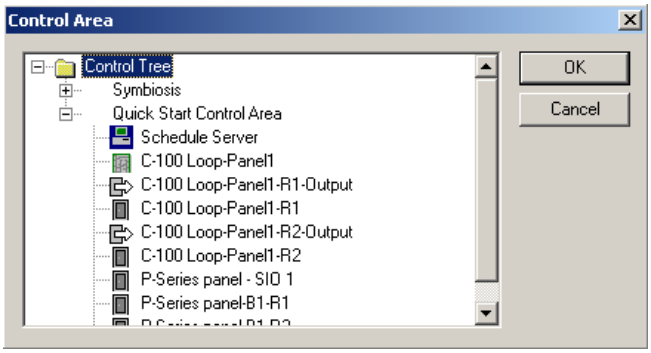
1. In the **Floor Plan Toolbox** dialog box, select the for Alarm View or for Event View and drag it to the floor plan design.
2. Right-click the link object and click **Control Properties.** A properties dialog box appears.



3. To set the general properties for the view link, click the **General** tab.
    a. Type a **Name** for the link.
    b. To rotate the ADV control, enter the **Rotation Angle** or use the scroll bars to select an angle from the list.
    c. Select the **Show Name** check box to display the **Name** below the ADV in the floor plan.
    d. Select the **Show Tooltip** check box to display the ADV name as a tool tip.
4. To select the device for which event or alarm views must be displayed in the floor plan, click the **Filter** tab.



    a. Click **Control** to open the Control Map.
    b. Expand the Control Map by clicking the [+] sign.



    c. Right-click the device and click **Select**. The icon for the selected device appears in red.

Note: You can select multiple devices in the control map.

    d. Click **OK** to close the **Control Area** dialog box and to return to the **Filter** tab of the properties dialog box.

Note: The **Selection** field displays the name of the selected device or displays **Multiple** if more than one device has been selected.

    e. Under **On**, select **Alarm Reads**, **Card Reads**, or **Both**.

f. Click **OK**.

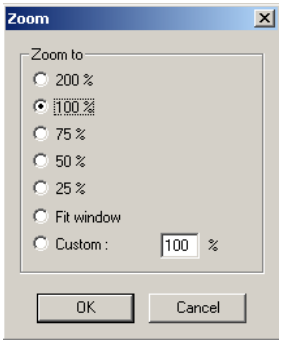
Adding a Text Box to the Floor Plan

You can add a text box to a floor plan for creating legends, or to give special instructions to the Operator viewing the floor plan.

After you drag and drop the text box to the floor plan background, enter the text, and resize or reposition the text box to accommodate the text. The Text box has no **Control Properties** to configure.

To add a text box to the floor plan:

1. In the **Floor Plan Toolbox** dialog box, drag and place it in the floor plan design window.
2. Enter the required text inside the text box.
3. Adjust the zoom percentage of the text box.
    a. Right-click the text box and select **Zoom** to adjust the Zoom percentage of the text box. The **Zoom** dialog box appears.



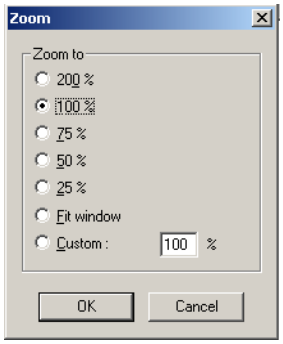
    b. Select the zoom percentage or enter the percentage in **Custom**.
    c. Click **OK** to save the zoom percentage and to close the **Zoom** dialog box.

Adjusting the Size of the Floor Plan

The zoom factor enables you to enlarge or reduce the size of the floor plan for a specified percentage.

To set the zoom factor:

1. Right-click anywhere inside the floor plan design.
2. Select **Zoom** from the pop-up menu. The **Zoom** dialog box appears.



3. Under **Zoom to**, click the required percentage for enlarging or reducing the floor plan, or click **Custom** and type the required percentage.
4. Click **OK** to save the changes.

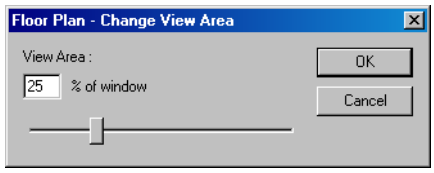
Note: Right-click anywhere inside the floor plan design and select **Undo Zoom** to display the floor plan in its previous size.

Previewing the Floor Plan

You can preview the floor plan and customize the preview area.

To preview the floor plan:

1. Right-click anywhere inside the floor plan design.
2. Select **Show View** from the pop-up menu. A preview of the floor plan is displayed.
3. Right-click anywhere in the floor plan preview and select **View Area**. The **Floor Plan - Change View Area** dialog box appears.



4. In **View Area**, type the percentage or use the slider at the bottom of the window for enlarging the floor plan preview.
5. Click **OK** to save the changes made.

Working with Floor Plan Controls

The following functions can be performed with the floor plan controls:

- Copy an already existing control to create new controls in the floor plan.
- Remove a control from the floor plan.
- Resize and re-arrange the controls in the floor plan.

Copying and Pasting a Control

1. In the floor plan design, right-click the object that you want to copy.
2. Select **Copy Selected Control** from the pop-up menu to copy the control.
3. Right-click the control and select **Paste Control** to paste the control in the floor plan design window.

Removing a Control from the Floor Plan

1. In the floor plan design, right-click the object you want to remove.
2. Select **Remove Selected Control** from the pop-up menu to delete the selected object from the floor plan.

Resizing, Rotating, and Re-arranging Objects

To resize an object:

1. In the floor plan design, select the object you want to resize.
2. Drag the corners of the object until the object is of the required size.

To rotate an object:

1. In the floor plan design, select the object you want to rotate.
2. Click  in the **Floor Plan Toolbox** dialog box.
3. Place the mouse pointer on one of the corners of the object you want to rotate.
4. Click and drag the mouse pointer to rotate the object.

Note: In addition, you can rotate an object by setting the Rotation Angle in the object Control Properties.

To re-arrange the object:

1. In the floor plan design, select the object you want to re-arrange.
2. Drag the object and place it where you require in the floor plan.

Note: Save the changes made to the floor plan controls by clicking Save in the **Floor Plan Toolbox** dialog box.

Editing a Floor Plan

To edit a floor plan:

1. Choose **Configuration > Floor Plan Definition**. The **Floor Plan Definition** window appears.
2. Highlight the floor plan you want to edit from the list of floor plans.
3. Click **Edit**. The **Floor Plan Toolbox** dialog box and the floor plan design appear.

4. Change the name or description of the floor plan, add or delete objects, or edit the properties of existing objects.
5. Click **Save and Exit** to save the changes made to the floor plan and return to the **Floor Plan Definition** window.
6. Click **Close (X)** to close the **Floor Plan Definition** window.

Deleting a Floor Plan

To delete a floor plan:

1. Choose **Configuration > Floor Plan Definition**. The **Floor Plan Definition** window appears.
2. Select the floor plan you want to delete, from the list of floor plans.
3. Click **Delete**.

Floor Plan Operations

After defining floor plans, you can use floor plan views for monitoring and controlling the devices in the Access Control System. Monitoring and controlling of devices can be done by executing commands from floor plan views for each ADV in the floor plan. For example, a door can be locked by performing the **Lock** command on the door that is added as an ADV in the floor plan.

In addition, you can view the statuses of the ADVs, which is indicated by different colors.

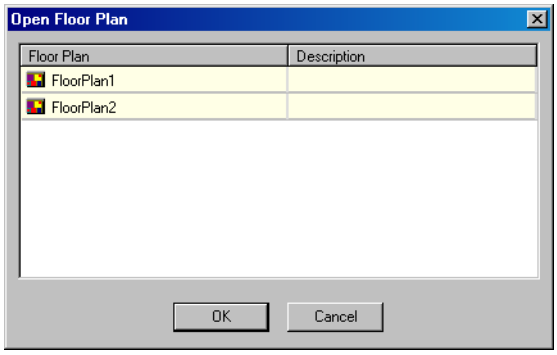
Note: Ensure that you have defined the color-coding for the various ADV statuses while designing the floor plan.

Refer to the "Adding an ADV to the Floor Plan" section of this chapter for information on setting the status colors for ADVs.

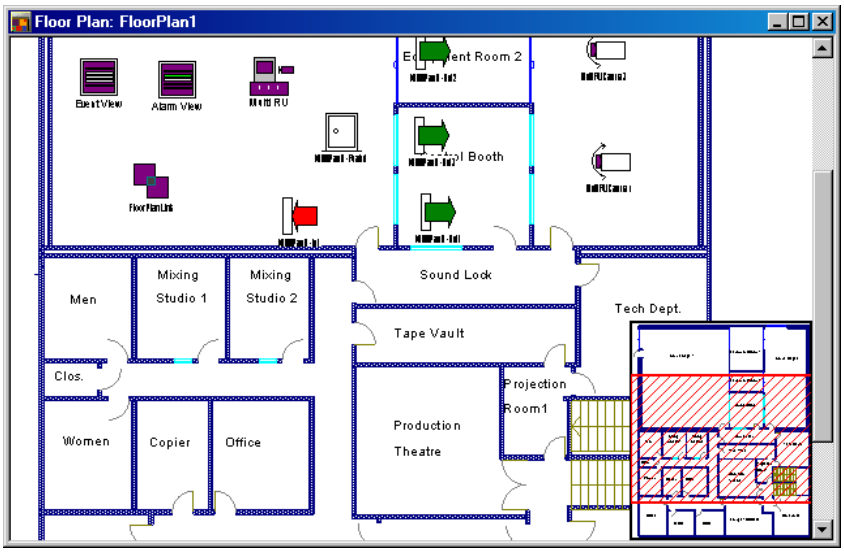
Working with Floor Plan Views

Opening a Floor Plan View

1. Choose **Operations > Floor Plan** or click  in the tool bar. The **Open Floor Plan** dialog box appears.



2. Click to select the floor plan you want to view.
3. Click **OK**. The floor plan is displayed in a floor plan view window.



Resizing and Previewing Floor Plan Views

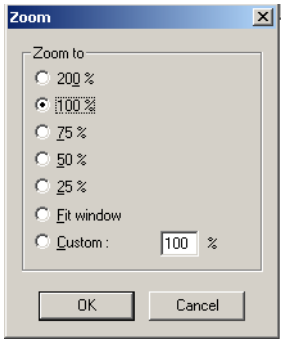
You can resize a floor plan view by adjusting the zoom percentage. In addition, you can preview the floor plan view to view the entire floor plan as a snap shot inside the floor plan view window.

Resize the floor plan view

Using the Zoom factor you can enlarge or reduce the size of the floor plan to a specific percentage.

To set the zoom factor:

1. Right-click anywhere in the floor plan view.
2. Select **Zoom** from the pop-up menu. The **Zoom** dialog box appears.



3. Select the zoom percentage for enlarging or reducing the size of the floor plan view or click **Custom** and type the required percentage.
4. Click **OK** to save the zoom percentage.

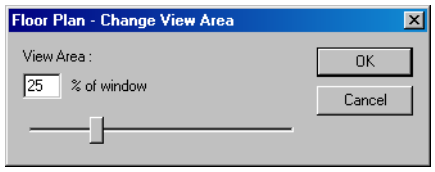
Note: Right-click anywhere in the floor plan view and select **Undo Zoom** to view the floor plan in its original size.

Previewing floor plan view

You can preview the floor plan view and customize the preview area.

To preview the floor plan:

1. Right-click anywhere in the floor plan view.
2. Select **Show View** from the pop-up menu. A preview of the floor plan view is displayed.
3. Right-click anywhere in the floor plan preview and select **View Area**. The **Floor Plan - Change View Area** dialog box appears.



4. In **View Area**, type the percentage for reducing or enlarging the view area or use the slider at the bottom of the window.
5. Click **OK**. A preview of the floor plan is displayed.

Controlling System Devices from the Floor Plan

You can control system devices by executing commands from the floor plan view. In addition, you can view and control other floor plans by clicking the floor plan link and view the alarms and events for a specific device by clicking the alarm and the event view links.

To run commands for ADVs from a floor plan view:

1. Right-click an ADV on the floor plan view to open its control menu. Commands for performing actions on the ADV are displayed in the menu.

Note: The commands vary based on the selected device.

2. Select the required command from the menu.

Note: To select more than one ADV of the same type, press and hold down CTRL and click each ADV. Right-click any one of the ADVs in the selected group, and then select the required control function.

See Table 12-2 in this section, for information on ADVs and their control functions.

To open other floor plans:

- Right-click in the floor plan view and click **Open**. The floor plan linked to the source floor plan is displayed.

To open event view and alarm view:

- Right-click for event view or for alarm view in the floor plan view and click **Open**. The event view or the alarm view window appears.

Table 12-2 ADV Control Functions from Floor Plan

ADV	Control Functions
CCTV Switcher	Send Time & Date, Send Camera Titles, Camera to Monitor Switch, Acknowledge All Alarms, Clear All Alarms
Comm Server	Acknowledge All Alarms, Clear All Alarms
Command File Server	Run Command File
C-100 Local Connection	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms
C-100 Remote Connection	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms, Connect Remote, Disconnect Remote
Doors	Unlock, Lock, Shunt, Unshunt, Pulse, Timed Pulse, Restore to Time Zone, Acknowledge All Alarms, Clear All Alarms
Input Points	Acknowledge all Alarms, Clear all Alarms, Shunt, Unshunt, Restore to Time Zone
Modem Pool	Hang-Up Modem, Reset Modem, Acknowledge All Alarms, Clear All Alarms
CCTV Monitor	Acknowledge All Alarms, Clear All Alarms
N-485 Remote Dialup	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Connect, Remote, Disconnect Remote, Acknowledge All Alarms, Clear All Alarms

Table 12-2 ADV Control Functions from Floor Plan

ADV	Control Functions
N-485 Local Connection	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms
Output Points & Groups	Energize, De-energize, Pulse, Timed Pulse, Restore to Time Zone, Acknowledge All Alarms, Clear All Alarms
Panel	Initialize, Cancel Initialization, Buffer, UnBuffer, Acknowledge All Alarms, Clear All Alarms
Pan / Tilt Camera	Acknowledge All Alarms, Clear All Alarms
Readers	Acknowledge All Alarms, Clear All Alarms
SIO Boards	Acknowledge All Alarms, Clear All Alarms
Static Camera	Acknowledge All Alarms, Clear All Alarms
Galaxy Communication	Acknowledge All Alarms, Clear All Alarms
Galaxy Panel	Acknowledge All Alarms, Clear All Alarm **Set All Groups** - Panel sets all the groups associated to the panel. **Unset All Groups** - Panel unsets all the groups associated to the panel. **Reset Panel** - Resets the panel. **Bypass Zones** - Panel bypasses alarms from the selected zone types. **Unbypass Zones** - Panel stops bypassing alarms from the selected zone types. **Activate Output** - Activates the selected output. **Deactivate Output** - Deactivates the selected output. To select a zone type or output type, right-click the Galaxy panel and select the appropriate action, and then select the zone type or output type.
Galaxy Group	Acknowledge All Alarms, Clear All Alarms **Set Group** - Panel sets the selected group. **Unset Group** - Panel unsets the selected group. **Part Set** - Panel sets all the zones for which the Zone State (attribute) is set as Part Set. **Timed Set** - Panel sets all the zones after a specific time. **Group Bypass** - Panel bypasses alarms from all the zones in the group. **Group Unbypass** - Panel stops bypassing alarms from all the zones in the group. **Refresh** - Refreshes the latest status of a group.

Table 12-2 ADV Control Functions from Floor Plan

ADV	Control Functions
Galaxy Zone	Acknowledge All Alarms, Clear All Alarms **Bypass Zone** - Panel bypasses alarms from the zone. **Unbypass Zone** - Panel stops bypassing alarms from the selected zones. **Force bypass Zone** - Forcefully bypasses the zones which cannot be bypassed using the Bypass Zone option. For example, Fire. **Refresh** - Refreshes the latest status of a zone.
Galaxy Output	Acknowledge All Alarms, Clear All Alarms **Activate** - Activates the output. **Deactivate** - Deactivates the output. **Refresh** - Refreshes the latest status of an output.
Galaxy Keypad	Acknowledge All Alarms, Clear All Alarms
Galaxy MAX	Acknowledge All Alarms, Clear All Alarms
Galaxy RIOs	Acknowledge All Alarms, Clear All Alarms
Vista Partition	Acknowledge All Alarms, Clear All Alarms **Arm Away** - The panel completely arms the perimeter and interior burglary partition by sensing the intruder's movements. **Arm Stay** - Arms only the perimeter burglary protection, guarding protected doors, windows, and other perimeter protection points in the partition. This enables automatic bypassing of certain areas that allows movement on those areas without causing an alarm. **Note:** To define the perimeter area, the zone type of the zones must be defined as Perimeter while configuring the Vista panel. **Disarm** - The panel disarms the selected burglary partition, silences alarms and audible trouble indicators.
Vista Zone	Acknowledge All Alarms, Clear All Alarms **Bypass Zone** - The panel bypasses alarms from the zone. This allows movement on the bypassed area without causing an alarm. **Unbypass Zone** - The panel stops bypassing alarms from the selected zone.

Table 12-2 ADV Control Functions from Floor Plan

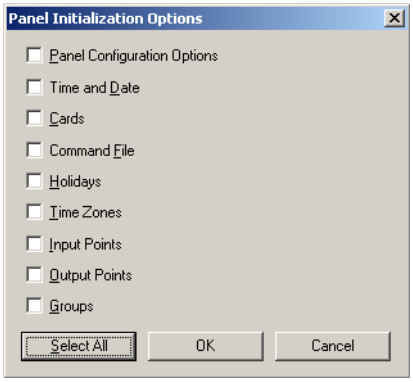
ADV	Control Functions
Vista Panel	Acknowledge All Alarms, Clear All Alarms **Arm Away** - The panel completely arms the selected perimeter and interior burglary partitions by sensing the intruder's movements. This option enables you to select multiple partitions of the panel. **Arm Stay** - Arms only the perimeter burglary protection, guarding protected doors, windows, and other perimeter protection points in the selected partitions. This enables automatic bypassing of certain areas that allows movement on those areas without causing an alarm. **Note:** To define the perimeter area, the zone type of the zones must be defined as Perimeter while configuring the Vista panel. **Disarm** - The panel disarms the selected burglary partitions, silences alarms and audible trouble indicators. This option enables you to select multiple burglary partitions in the panel. **Panel Reset** - Resets the panel. **Refresh** - Refreshes the latest status of the vista panel.
Vista Output	Acknowledge All Alarms, Clear All Alarms **Activate** - Activates the output. **Deactivate** - Deactivates the output. **Refresh** - Refreshes the latest status of an output.

Initializing Panels from Floor Plan

When panels are added to the WIN-PAK system, they are initialized so that the information entered during panel configuration is sent to the panels. Panels are initialized from the Floor Plan view or from the Control Map.

To initialize a panel from floor plan:

1. Choose **Operations > Floor Plan** and open the Floor Plan view that contains the panel to be initialized.
2. Right-click the panel, and select **Initialize** from the subsequent menu. The **Panel Initialization Options** dialog box appears.



Refer to the "Panel Initialization Options" section in this chapter to know the description for initialization options.

3. To update all information in the panel, click **Select All**.

   OR

   To update only the selected information, select the corresponding check boxes.

4. Click **OK** to update the panel details.

Refer to the "Initializing Status" section in this chapter for details on status of the initialization.

Panel Initialization Options

Table 12-3 Describing panel initialization options

Panel Initialization Options	**Description**
Panel Configuration Options	Sends all panel configuration information. This resets your panel programming. It is recommended that you use the "Select All" feature (button) when the Panel Configuration Options are to be sent.
Time & Date	Updates panel time and date with the network time and date. You may notice a pause for up to 50 seconds when the time and date are sent because the time is sent at the top of the computer minute up to + 10 seconds. Closed circuit acts as a NC circuit.
Cards	Sends card information to the panel. When sending cards, it is recommended that you re-initialize the panel by choosing **Select All**. This ensures that old card information is removed when the new card information is added. When cards with an Active or Trace status are added, edited, or deleted from the card or card holder database, this information is automatically sent to the panels. All other card information changes are sent using this command.

Additionally, new or updated information on the following features, functions, and panel elements are sent to the panel:

- Access Levels
- Access Control Areas
- Card Formats
- Command File
- Conversion Tables
- Groups
- Holidays
- Inputs
- IC Configuration
- Input Groups
- Input Scan
- Outputs
- Procedures/Actions
- SIO Boards
- Triggers
- Reader LED/Buzzer specs
- Time Zones

Initializing Status

As the panel initializes, a status window indicates the status of sending the information. If an error occurs, the status window indicates which command caused the error.

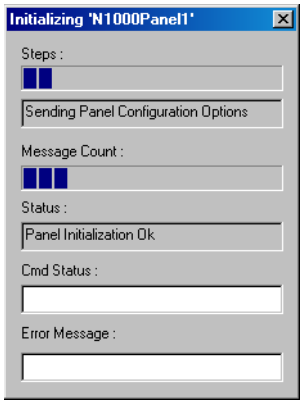


Figure 12-1 Showing the status of initialization

Table 12-4 Describing fields in the Status dialog box

Field name	Description
Steps	Indicates what information is sent.
Message Count	Indicates the progress of messages sent.
Status	Indicates whether the proceeding initialization is successful or has failed.
Cmd Status	Indicates if a command has timed out.
Error Message	Indicates if any errors occurred while transmitting information to the panel.

Command File

13

In this chapter...

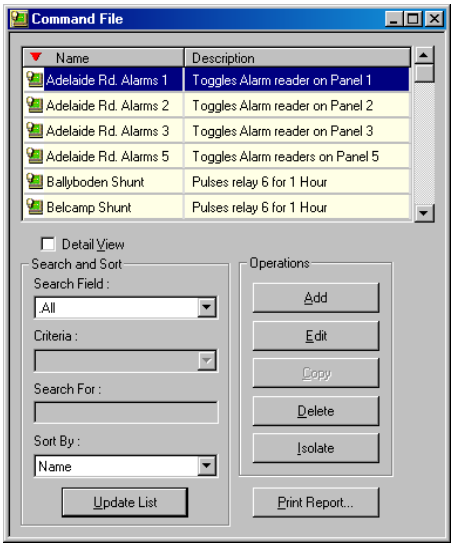
Command File Configuration

A Command file contains a set of commands that can be executed manually or automatically when an event or alarm occurs on an ADV. Commands to be performed on different ADVs can be included in the same command file. When a command file is run, all the commands in the file are carried out at the same time.

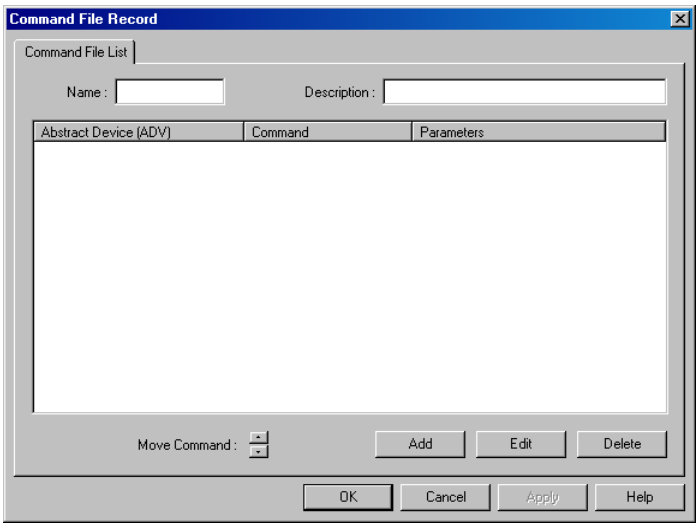
For example, when fire is detected in a building, the doors must be automatically unlocked. A command file can be defined containing the commands to Unlock and Pulse the two ADVs, Doors and Outputs.

Adding a Command File

1. Choose **Configuration > Command File**. The **Command File** window appears.



2. Click **Add**. The **Command File Record** dialog box appears.

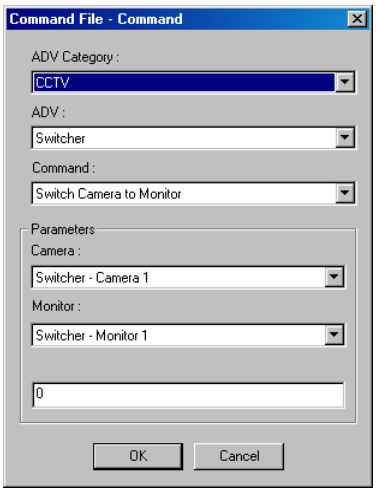


3. Type the name of the command file in the **Name** box.
4. Type a **Description** for the command file.
5. To add commands to the command file, click **Add**.

   Refer to the "Adding Commands to the Command File" section in this chapter for more information on adding commands to the command file.

Adding Commands to the Command File

1. In the **Command File Record** dialog box, click **Add**. The **Command File - Command** dialog box appears.



2. Select an **ADV Category** for the command file. The ADVs belonging to the selected category are retrieved in the **ADV** list.
3. Select the **ADV** on which the command must be run. The commands that can be run on the ADV are retrieved in the **Command** list.
4. Select the required command from the **Command** list.

   See Table 13-1 for the commands available for the ADV controls.

5. To define custom commands for the ADV, select **Custom Command** from the **Command** list and enter the action parameters in the fields provided under **Parameters**.

   Note: The fields displayed under **Parameters** vary based on the command that is selected.

   Refer to the "Running a Command File" section in this chapter for more details on adding a custom command.

   See Table 13-1 for the parameters fields displayed for the ADV controls.

6. Click **OK** to add the command to the command file and to return to the **Command File Record** dialog box. The newly added command is appended to the command list in the **Command File Record** dialog box.

7. To move a command in the command list, click any of the following buttons provided next to **Move Command**:
   - Select a command in the list and click  to move the selected command on top of the previous one.
   - Select a command in the list and click to move the selected command to the bottom of the list.
8. To delete a command from the command file, click **Delete**.
9. Click **OK** to save the command file and return to the **Command File** window.

Adding a Custom Command

You can add customized commands for ADVs such as CCTVs, Panels, and RS232 Connections.

To add custom commands:

1. Select an **ADV Category** for the command file. The ADVs belonging to the selected category are retrieved in the **ADV** list.
2. Select the **ADV** on which the custom command must be run. The commands that can be run on the ADV are retrieved in the **Command** list.
3. Select **Custom Command** in the **Command** list.
4. Under **Parameters**, define the custom command.

Note: The fields displayed under **Parameters** vary based on the command that is selected.

See Table 13-1 for the parameters fields displayed for the ADV controls.

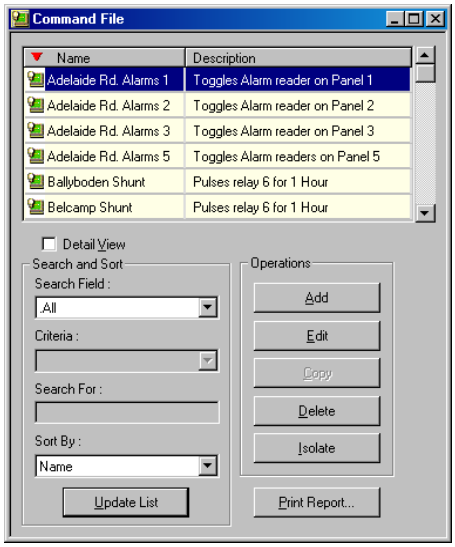
5. Click **OK** to save the changes.

Editing a Command in the Command File

1. In the **Command File Record** dialog box, click **Edit**. The **Command File - Command** dialog box appears.
2. Edit the required details of the command and click **OK**.

Editing a Command File

1. Choose **Configuration > Command File**. The **Command File** window appears.



2. Click **Edit**. The **Command File Record** dialog box appears.
3. To edit the command file name, type the name of the command file in the **Name** box.
4. Type a **Description** for the command file.
5. Click **Apply** to save the changes to the command file or click **OK** to save the changes and to close the **Command File Record** dialog box.

   Refer to the "Adding Commands to the Command File" and "Editing a Command in the Command File" sections in this chapter to add or edit commands to the command file.

List of Commands

The following list shows standard commands available when defining Command Files:

Table 13-1 Command and Parameter list for ADVs

ADV	Commands	Parameters
CCTV	Camera	Go Home
	Go to Preset	Preset #
	Iris Open	
	Iris close	
	Pan Left	
	Pan Right	
	Refresh	
	Stop	
	Tilt Down	
	Tilt Up	
	Zoom In	
	Zoom Out	
CCTV Switcher	Custom Command	Custom Command
	Switch Camera to Monitor	
	Camera ID	Camera ADV
	Monitor ID	Monitor ADV
CCTV Monitor	Refresh	DoorLock
	Switch Camera (Camera ID)	Camera ADV
Door	Lock	
	Pulse	
	Timed Pulse	0 - 65, 335 sec.
	Unlock	

Table 13-1 Command and Parameter list for ADVs

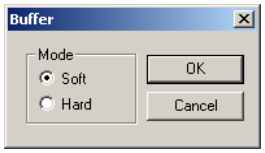
ADV	Commands	Parameters
Galaxy Group	Part Set	
	Set	
	Timed Set	Set Time(in Sec) = 0 to 180 sec.
	Unset	
Galaxy Output	Activate	
	Deactivate	
Galaxy Panel	Reset	
	Set Panel	
	Unset Panel	
Galaxy Zone	Bypass	
	Force Bypass	
	Unbypass	
Input	Shunt	
	Switch To Time Zone Control	
	Unshunt	
Loop	Buffer All Panels	
	Unbuffer All Panels	0 = Hard, 1=Soft
Output & Group	De-energize	
	Energize	
	Pulse	
	Switch to TimeZone Control	
	Timed Pulse	0 - 65, 335 sec.
Panel	Buffer	
	Unbuffer	
	Custom Command	

Table 13-1 Command and Parameter list for ADVs

ADV	Commands	Parameters
Server (All)	Refresh	
RS232 Connection	Custom Command	
Vista Output	Activate	
	Deactivate	
Vista Panel	ArmAway Partitions	In the **Partition** list, select the partitions to be armed.
	ArmStay Partitions	In the **Partition** list, select the partitions to be armed.
	DisArm Partitions	In the **Partition** list, select the partitions to be disarmed.
	Reset Panel	
Vista Partition	ArmAway	
	ArmStay	
	DisArm	
	Send Keypress	Key entries - 0 to 9, A to D, *, #
Vista Zone	Bypass	
	Unbypass	

Note: Consider the following if you are selecting the **Buffer** or **Unbuffer** command for panels.

- When you select a **Buffer** command, all the events are stored in the panel. The events are stored in the panel buffer and cannot be viewed in the **Event view** and **Alarm view** windows in the WIN-PAK User Interface.
- When you select an **Unbuffer** command, the event details that are buffered in the panel are transmitted to the WIN-PAK User Interface and can be viewed through the **Event View** and **Alarm View** windows.
- **Buffer** command can be either hard or soft. The following window appears when you select the **Buffer** command for panels.



The Hard and Soft buffer options are explained in the following table as scenarios:

Table 13-2 Scenario 1

Action	Result
Buffer Command at 1 P.M.	Events buffered in the panel from 1 P.M.
Buffer Command at 2 P.M.	Events continue to be buffered in the panel even after 2 P.M.
Mode	**Soft**
Unbuffer Command at 3 P.M.	Events buffered after the last buffer command are sent to WIN-PAK. Therefore, the events buffered only between 2 to 3 P.M. are sent to WIN-PAK.
Second **Unbuffer** Command at 3 P.M.	Events buffered between the first and the second buffer commands are sent to WIN-PAK. Therefore, the events buffered between 1to 2 P.M. are sent to WIN-PAK.

Table 13-3 Scenario 2

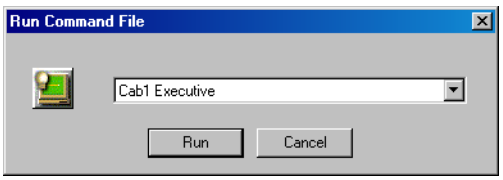
Action	Result
Buffer Command at 1 P.M.	Events buffered in the panel from 1 P.M.
Buffer Command at 2 P.M.	Events continue to be buffered in the panel even after 2 P.M.
Mode	**Hard**
Single **Unbuffer** Command at 3 P.M.	All the buffered events (from 1 P.M. to 3 P.M.) are sent to WIN-PAK.

Running a Command File

Commands that are configured in a command file can be run for performing actions on ADVs.

To run a command file:

1. Choose **Operations > Command File**. The **Run Command File** dialog box appears.



2. Select the command file to be run from the drop-down list.
3. Click **Run** to start running the command file. The commands in the command file are run on the ADVs.

Guard Tour

14

In this chapter...

Introduction

A Guard Tour is defined as a series of check points a guard must activate within a given time. The check points are either readers, at which the guard presents the card, or input points, such as egress buttons.

The check points can be sequenced (to be activated in the specified order) or un-sequenced (can be activated in any order.) A sequenced check point is defined with the time at which the guard must access the check point and the grace period allowed for early arrival and late arrival of the guard at the check point. An unsequenced check point can be accessed by the guard at any order.

In addition, the validity of cards that can be accessed at the reader check points is specified (sequenced and un-sequenced.)

Alarms for the various check point states are defined by associating an action group to each check point and by specifying the action priority. Based on the priority, an event is displayed or an alarm is triggered for the specific action. For example, if an alarm must be triggered when a guard misses a check point, it can be configured by setting the priority for the **Missed** action state for the check point. When the guard tour is run and if the guard misses the check point, an alarm is triggered based on the action priority.

After a guard tour is configured, it can be run to monitor the guard's movements at the various check points. As the guard tour progresses, alarms and events are displayed in the Alarm or the Event window for the various action states of a check point.

Configuring Guard Tours

Configuring guard tours involves:

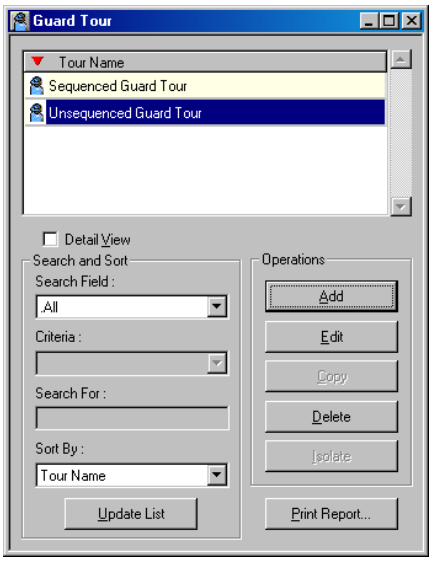
- Adding a guard tour.
- Defining readers and input points as a part of sequenced and unsequenced check points.
- Associating action groups to check points and specifying priority for each state together with the command file to be executed when the action occurs.

Adding a Guard Tour

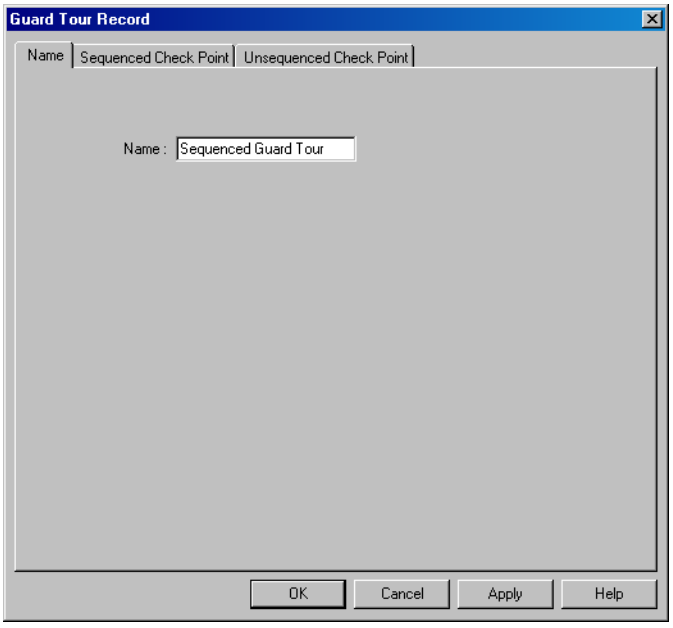
Adding a guard tour involves defining a name for the guard tour and specifying at least one check point for the guard tour.

To add a guard tour:

1. Choose **Configuration > Guard Tour**. The **Guard Tour** window appears.



2. Click **Add**. The **Guard Tour Record** dialog box appears.



3. Type a **Name** for the guard tour.
4. Click the **Sequenced Check Point** and the **Unsequenced Check Point** tabs to enter the checkpoint details for the guard tour.

   Refer to the "Adding Unsequenced Check Points" and "Adding Sequenced Check Points" sections in this chapter, for information on defining sequenced and unsequenced check points for the guard tour.
5. Click **Apply** to create the guard tour.
6. Click **OK** to create the guard tour and to close the **Guard Tour Record** dialog box.

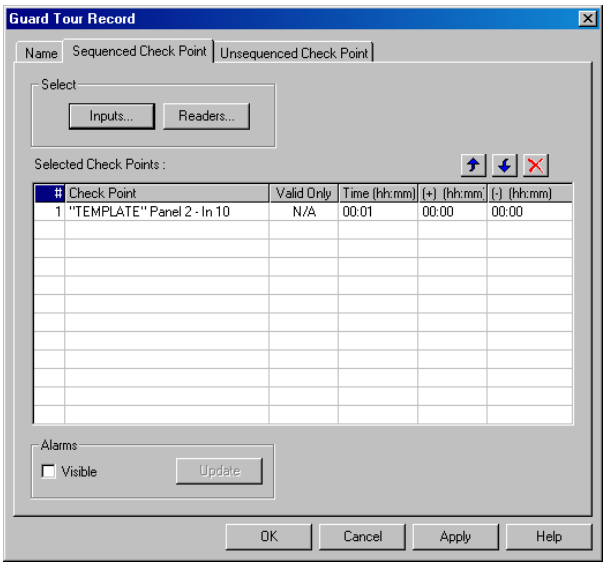
Adding Check Points

Readers and Input points can be added as sequenced and un-sequenced check points to the guard tour.

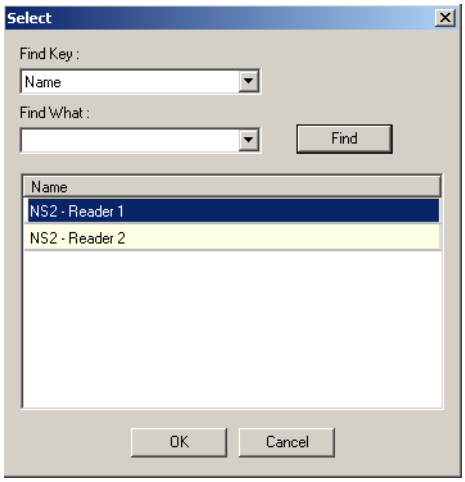
Note: It is mandatory to add at least one check point to the guard tour.

Adding Sequenced Check Points

1. In the **Guard Tour Record** dialog box, click the **Sequenced Check Point** tab.



2. Under **Select**, click **Inputs** to assign input points or click **Readers** to assign readers as checkpoints to the guard tour. The **Select** dialog box appears.



3. Type the first few letters of the reader or the input point name in **Find What**.
4. Click **Find**. A list of readers or input points with similar names, are retrieved in the **Name** list.

Note: Leave the **Find What** field blank to retrieve all input points or readers in the **Name** list.

5. In the **Name** list, select the input point or reader to be added to the guard tour, and click **OK**.

   Note: To select multiple input points or readers, press and hold down the SHIFT key for contiguous selection or press and hold down the CTRL key for non-contiguous selection.

   The selected input point or reader is displayed in **Selected Check Points** list in the **Guard Tour Record** dialog box.

6. Under the **Valid Only** column in the **Selected Check Points** list, specify the validity requirement of cards that must be accessed at readers.
   - Type **Y** if only a valid card must be accessed at a reader.
   - Type **N** if a valid and an invalid card can be accessed at a reader. (Invalid cards do not have access rights on a specific reader.)

     Note: N/A is displayed for input points.

7. Type the **Time(hh:mm)** at which the guard must present the card at the checkpoints (in hours and minutes.)
8. In **(+) (hh:mm)**, type the grace period in hours and minutes allowed for presenting the card, later than the time specified in **Time(hh:mm)**.
9. In **(-) (hh:mm)**, type the grace period in hours and minutes allowed for presenting the card, earlier than the time specified in **Time(hh:mm)**.
10. To add check point alarms to the reader or the input point, select the reader or input device and click **Update** under **Alarms.**

    Refer to the "Setting Check Point Alarms" section in this chapter for information on setting check point alarms.

11. To view the check point alarms that are already set for the input point or reader, select the **Visible** check box under **Alarms.** The alarms set for the check point is displayed in the **Abstract Device Record** dialog box.

    Note: Clear the **Visible** check box to close the **Abstract Device Record** dialog box.

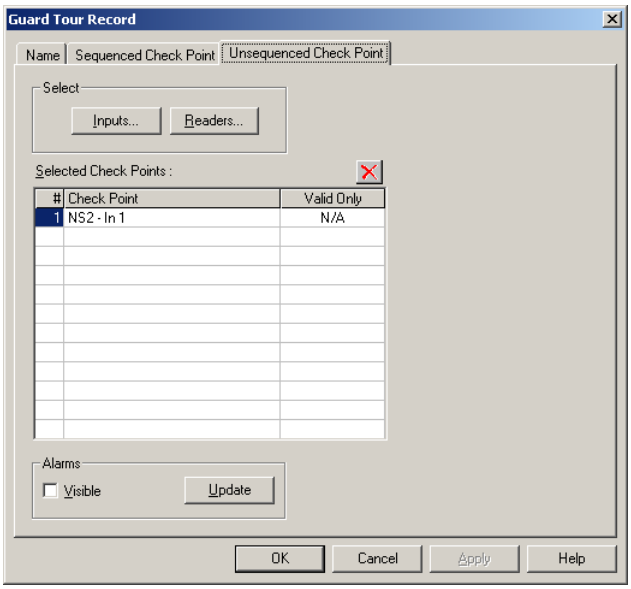
12. To change the display order of the checkpoints:
    - Select a reader or input point in the **Selected Check Points** list, and click  to shift it to the top of the list.
    - Select a reader or input point in the **Selected Check Points** list, and click  to shift it to the bottom of the list.

      Note: Changing the display order of the check points does not affect the sequence in which the check points are accessed. The check points are accessed only at the time entered in the **Time (hh:mm)** box and after considering the grace periods.

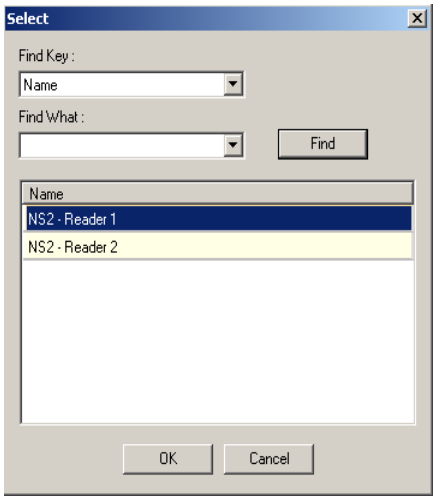
13. To remove a reader or an input point from the list of check points, select the reader or input point in **Selected Check Points** and click .

Adding Unsequenced Check Points

1. In the **Guard Tour Record** dialog box, click the **Unsequenced Check Point** tab.



2. Under **Select**, click **Inputs** to assign inputs points or click **Readers** to assign readers as checkpoints to the guard tour. The **Select** dialog box appears.



3. Type the first few letters of the reader or the input point name in **Find What**.
4. Click **Find**. A list of readers or input points with similar names, are retrieved in the **Name** list.

Note: Leave the **Find What** field blank to retrieve all input points or readers in the **Name** list.

5. In the **Name** list, select the input point or reader to be added to the guard tour, and click **OK**.

Note: To select multiple input points or readers, hold down the SHIFT key for contiguous selection or hold down the CTRL key for non-contiguous selection.

The selected input point or reader is displayed in **Selected Check Points** list in the **Guard Tour Record** dialog box.

6. Under the **Valid Only** column in the **Selected Check Points** list, specify the validity requirement of cards that must be accessed at readers.
   - Type **Y** if only a valid card must be accessed at a reader.
   - Type **N** if a valid or an invalid card can be accessed at a reader. (Invalid cards are cards that do not have access rights on a specific reader.)

     Note: N/A is displayed for input points.
7. To add check point alarms to the reader or the input point, select the reader or input device and click **Update** under **Alarms.**

   Refer to the "Setting Check Point Alarms" section in this chapter for information on setting check point alarms.
8. To view the check point alarms that are already set for the input point or reader, select the **Visible** check box under **Alarms.** The alarms set for the check point is displayed in the **Abstract Device Record** dialog box.

Note: Clear the **Visible** check box to close the **Abstract Device Record** dialog box.

9. To remove a reader or an input point from the list of check points, select the reader or input point in **Selected Check Points** and click .

Setting Check Point Alarms

You can track the movements of a guard by setting check point alarms.

For example, alarms can be configured to track the various actions of the guard, such as missing a check point, visiting a check point at a time earlier than the stipulated time, or visiting the check point at a time later than the stipulated time.

Alarms can be set for the following four states of a Sequenced checkpoint: Early Arrival, Late Arrival, Missed, and Out of Sequence. Alarms can be set only for the **Checked** state of Unsequenced check points.

Check point alarms are defined in the following manner:

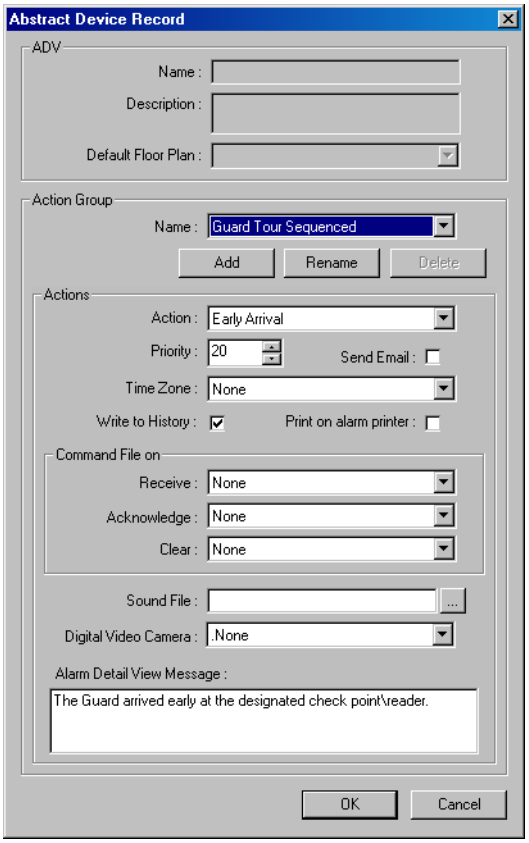
a. An action group is associated to a sequenced or unsequenced check point.

b. Priority for triggering off an event or an alarm is specified for each action in the action group.

c. The Command files to be executed for each action are selected.

To set check point alarms:

1. In the **Guard Tour Record** dialog box, click the **Sequenced Check Point** or the **Unsequenced Check Point** tab.
2. Click **Update** under **Alarms**. The **Abstract Device Record** dialog box appears.



Refer to the "Configuring an Abstract Device" section in the Device Map chapter for details on configuring action groups.

3. Click **OK** to save the details of check point alarms and return to the **Guard Tour Record** dialog box.

Running Guard Tours

Guard tours are run to monitor and track the movements of guards. You need to configure the guard tour server for running guard tours.

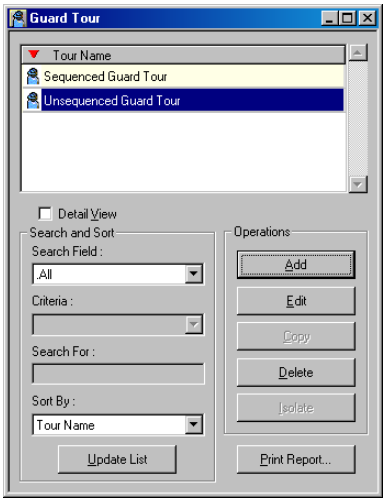
Refer to the "Adding a Guard Tour Server" section of the Device Map chapter for information on configuring a guard tour.

Running a guard tour involves:

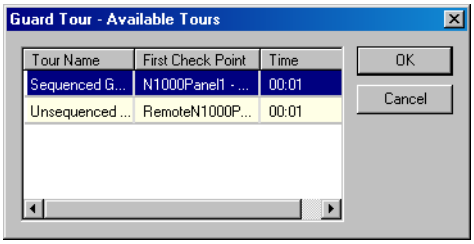
- Selecting the guard tour you want to run.
- Specifying the card that is used by the guard for accessing various check points.
- Starting the guard tour.
- Viewing the status of the sequenced and unsequenced check points that the guard accesses while the guard tour progresses.
- Viewing the alarms and events generated for the actions configured for the various check point states in the guard tour.

Starting a Guard Tour

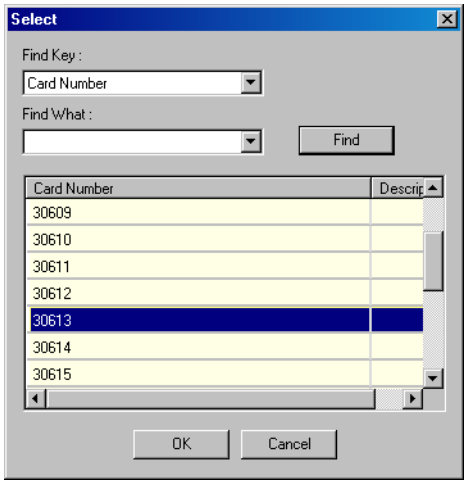
1. Choose **Operations > Guard Tour**. The **Guard Tour** window appears.



2. Click **Start**. The **Guard Tour - Available Tours** dialog box appears with the list of configured guard tours.



3. Select the guard tour to be started and click **OK**. The **Select** window appears.



4. Select the card that is being used to validate the reader check points.

    a. In the **Find Key** list, select **Card Number** to search for cards based on card numbers, or select **Description** to search for cards based on the card description.

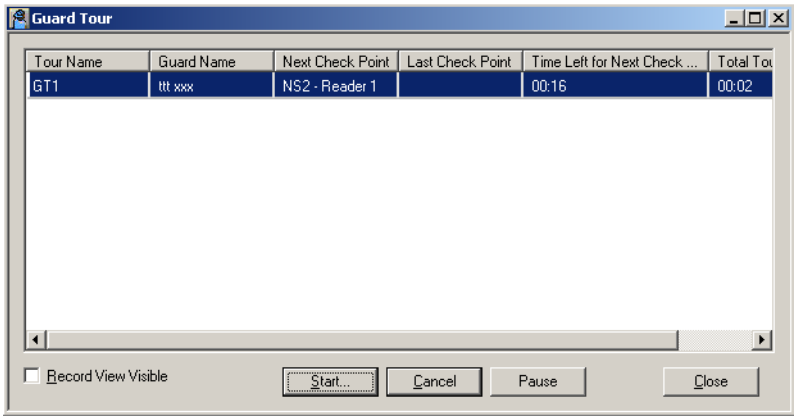
    b. In the **Find What** list, enter all or a part of the card number or description.

    c. Click **Find**. The cards matching the search criteria are retrieved in the list.

    d. Select a card number from the list and click **OK** to associate the card to the guard tour and to close the Select dialog box.

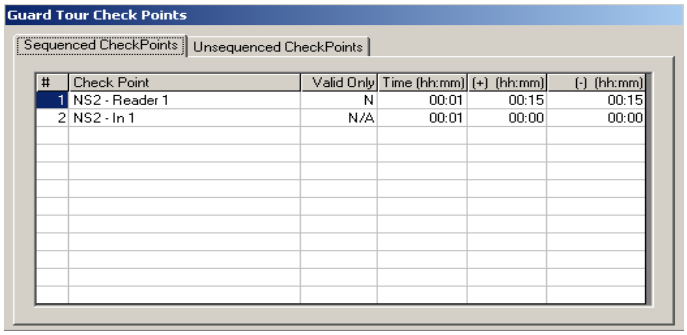
Note: Cards need not be added to a guard tour, having only input points as its checkpoints.

The details of the selected guard tour are displayed in the **Guard Tour** window.



5. Select a guard tour and select the **Record View Visible** check box to view the sequenced and unsequenced checkpoints for the guard tour. The **Guard Tour Check Points** dialog box appears.

6. To start the guard tour, click **Start**. The guard tour starts and the **Next Check Point**, **Last Check Point**, **Time Left for Next Check Point**, **Total Tour Time Left** details are updated as the guard tour proceeds.
7. To view the status of the checkpoints as the guard tour proceeds, select the **Record View Visible** check box. The **Guard Tour Check Points** dialog box appears.



   a. To view the status of sequenced checkpoints, click the **Sequenced CheckPoints** tab.

      Note: Alarms are displayed in the **Alarm View** window and Events are displayed in the **Event View** window according to the check point alarms configured for various action states.

   b. To view the status of unsequenced checkpoints, click the **Unsequenced CheckPoints** tab. The checkpoints the guard has visited is displayed in Red color.

   c. To close the **Guard Tour Check Points** dialog box, clear the **Record View Visible** check box in the **Guard Tour** window.

8. To pause the guard tour, click **Pause**. The button name changes to **Resume**.
9. Click **Resume** to restart the tour.
10. Click **Cancel** to stop the guard tour.

Monitoring Actions

15

In this chapter...

Introduction

In the WIN-PAK system, the actions of card holders, guards, devices can be monitored and controlled with various methods. An action might be a card read, change in the state of input, server trouble, or even an attempt made to open a door without using a card. These actions are categorized into Events, which are regular occurrences and Alarms that require special attention.

Actions to be performed on servers, devices, and digital video are specified while defining ADVs to represent them in WIN-PAK.

Different ways of monitoring the actions:

Locate Card Holder

- Displays the card holder details such as card number, account, time and location where the card is read by the card holder, and so on.

System Events

- Displays summary of the WIN-PAK system activities such as successful and unsuccessful server connections, log on details and server disconnections.

Event View

- Displays list of currently occurring events.

Alarm View

- Pops up on the User Interface with a beep sound as soon as an alarm occurs. Continues beeping till the alarm is acknowledged.

Autocard Lookup

- The Autocard Lookup window displays the card holder details of all the card transactions. However, the option is provided to filter the devices or cards.

Live Monitor

- The Live Monitor window displays the live video from the CCTV camera.

Digital Video

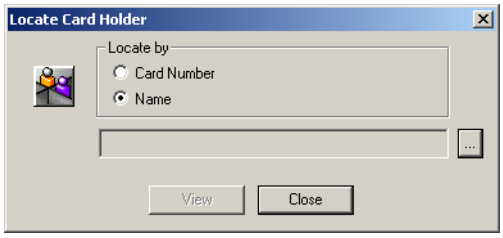
- The Digital Video Display window displays the live video or the recorded video from the DVRs.

Locate Card Holder

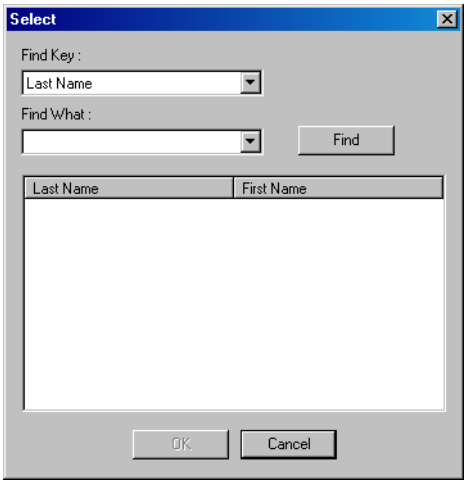
The Locate Card Holder option reports the card holder details, time and location of the cards that are used by the card holder.

To locate a card holder by a card number or a card holder name:

1. Choose **Operations > Locate** or click on the toolbar. The **Locate Card Holder** dialog box appears.



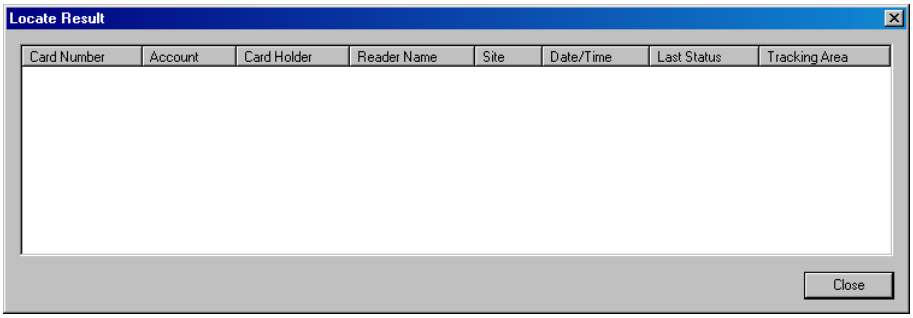
2. Under **Locate by**, click **Card Number** or card holder **Name**.
3. Click the ellipsis button to search for the card holder. The **Select** dialog box appears.



4. Select an item in **Find Key** and enter the keyword in the **Find What** box.
5. Click **Find**. The card holders that match the criteria are listed.

Note: If you want to list all the card holders, leave the **Find What** box empty and click **Find**.

6. Select the card holder and click **OK**. The dialog box is closed and the selected card holder name is displayed in the **Locate Card Holder** dialog box.
7. Click **View** to view the card holder details. The **Locate Result** dialog box appears.



8. Click **Close** to close the **Locate Result** dialog box.
9. Click **Close** to close the Locate Card Holder dialog box.

System Events

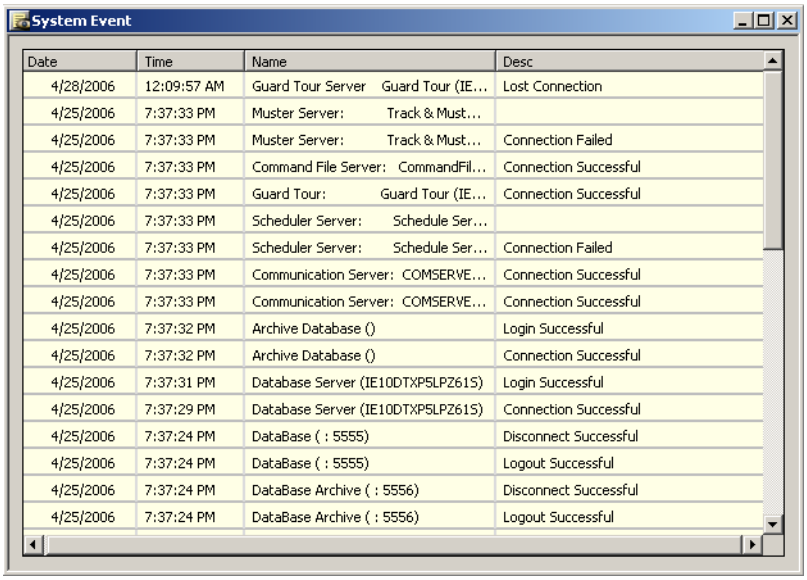
The System Event window displays the details of WIN-PAK system activities, such as successful and unsuccessful server connections, log on details, and server disconnections. Details such as the name, time, and date of the activity are displayed. This enables easier identification of the problem sources during server communications.

Viewing System Events

The WIN-PAK system provides an option to the user to view the history of WIN-PAK system activities.

To view the system events:

1. Choose **Operations > System Events**. The **System Event** window appears.



2. Click ☒ to close the window. You can also keep the window open always.

Note: Event View is different from System Events. Event View displays the access control activity, including card reads, alarms, and operator activity such as acknowledging and clearing of alarms.

Event View

An event is an access control activity such as a card read, change in the state of input, and so on. The Event View window displays the details of access control activities as and when they occur. The number of events displayed in the Event View depends on the setting made for the maximum number of events in the System Defaults option. When the number of events exceeds this number, the oldest entries are replaced by the new entries.

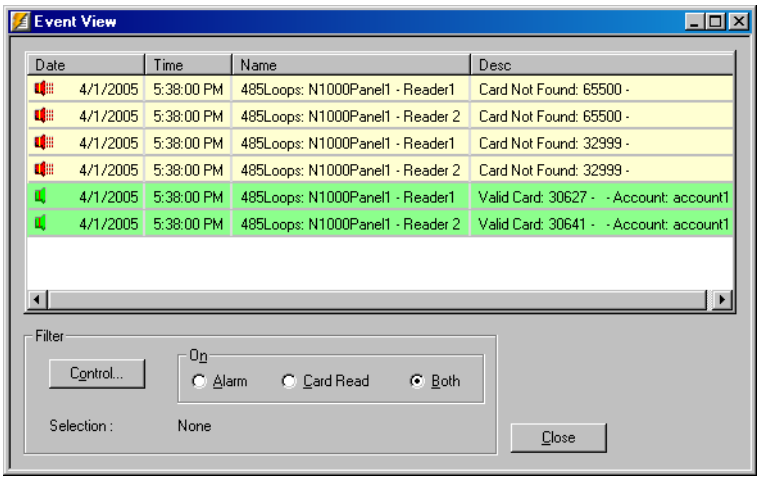
In addition, you can filter the areas or devices to show the events that occur only in the filtered areas or devices. When the window is closed, the displayed events are lost in the Event View window. However, the history of events is maintained in the WIN-PAK system.

Note: If you have procured the license for the Galaxy panel and/or Vista panel, the events occurring in the Galaxy panel and/or Vista panel are displayed in the **Event View** window.

Opening an Event View window

To open the Event View window:

1. Click **Operations > Events** or click the View Events icon on the tool bar. The **Event View** window appears showing the list of events.



2. Click **Close** to close the **Event View** window.

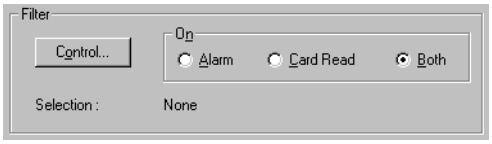
Note: The Digital Video Display window appears, when an alarm is raised from a reader or point to which attached the camera is associated. This helps you to view and monitor the area from where the alarm is raised. This alarm is prefixed by the icon.

Filtering Event Views

The WIN-PAK system is provided with an option to filter the events that must be displayed in the Event View window. These filter selections are cleared, after you close the Event View window.

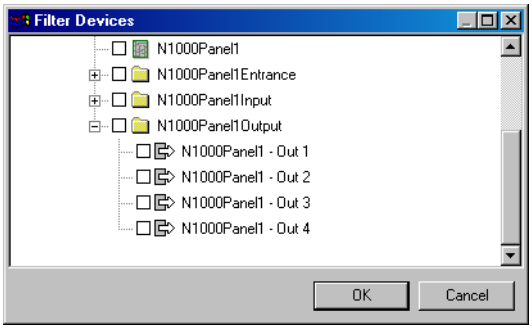
To filter the events:

1. Click **Operations > Events** or click the View Events icon on the tool bar. The **Event View** window is displayed.
2. Select one of the following options under **On**:

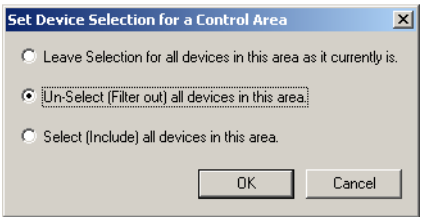


   - **Alarm** - To display only alarms in the Event View window.
   - **Card Read** - To display only card read events in the Event View window.
   - **Both** - To display all alarm and card read events in the Event View window.

3. To filter the events that occur in the specific areas and devices, click **Control** under **Filter**. The **Filter Devices** window appears.



4. Expand the tree by clicking the plus [+] symbol.
5. Select a branch or an individual device to be filtered for monitoring.
6. To filter a branch, right-click the branch and select **Configure**. The **Set Device Selection for a Control Area** dialog box appears.



Note: You can also double-click the branch to display the S**et Device Selection for a Control Area** dialog box.

7. Select one of the following options:
   - **Leave Selection for all devices in this area as it currently is**: To retain the existing filters set for the devices in this branch.
   - **Un-Select (Filter out) all devices in this area**: To clear the selection of all the devices in this branch. The devices in this branch are not monitored.
   - **Select (Include) all devices in this area**: To select all the devices in this branch. All the devices in this branch are monitored.
8. To filter a device, right-click the device and select **Invert Selection Status** to select the device or clear the selection.
9. Click **OK** to return to the **Filter Devices** dialog box.

   Tip:

   - To search for a branch or device:
     a. Right-click the branch or device and select **Find**. The **Find** dialog box appears.
     b. Type the item to be searched and click **Find**. The first item in the tree that matches the criteria is highlighted.
   - To refresh the tree, right click the branch or device and select **Refresh**.
10. Click **OK** to save the filter selection. Only the events that occur in the selected area and device are displayed in the **Event View** window.

Note: The filter settings are lost after you close the Event View window. Therefore, to view the floor plan with filter settings, you can open the Event View window from the Floor Plan.

Refer to the "Adding Alarm View and Event View links to the Floor Plan" section in the chapter Floor Plan, for details on creating an Event View in the Floor Plan.

Alarm View

An alarm is an event or an access control activity that must be acted upon as soon as it has occurred. The Alarm View window displays alarms when they occur and continuous to beep the sound until it is acknowledged. The Alarm View window is divided into two horizontal panes. Incoming alarms are displayed in the upper pane according to priority and time. The color of an alarm indicates the state of an alarm.

Various states of alarms are:

Table 15-1 Describing various states of alarm and the relevant colors

Alarm State	Description	Color
Alert State	The initial state of an alarm is Alert state. When an alarm is in this state, the immediate action must be taken. **Example:** A person tries to open the door forcefully. This is an alarm in the Alert state.	Red
Normal State	When the access control activity becomes normal, the alarm in Alert state goes to Normal state. **Example:** When the forced open door is closed.	Green
Trouble State	Any problem that occurs in the device is reported as an alarm in Trouble state. **Example:** A reader is tampered. **Note:** An N-1000/PW-2000 panel can only detect a trouble condition when an AEP-5 board is used.	Yellow

The **Cnt** (Count) column on the **Alarm View** window shows the number of state changes in a point. After the message is acknowledged, the new messages of Normal state are displayed in green.

The **Details** check box enables you to open the **Alarm Details** dialog box. In the Alarm Details dialog box, you can view the details of the state changes indicated by **Cnt** (Count) and write a note for an alarm in **Operator Messages**.

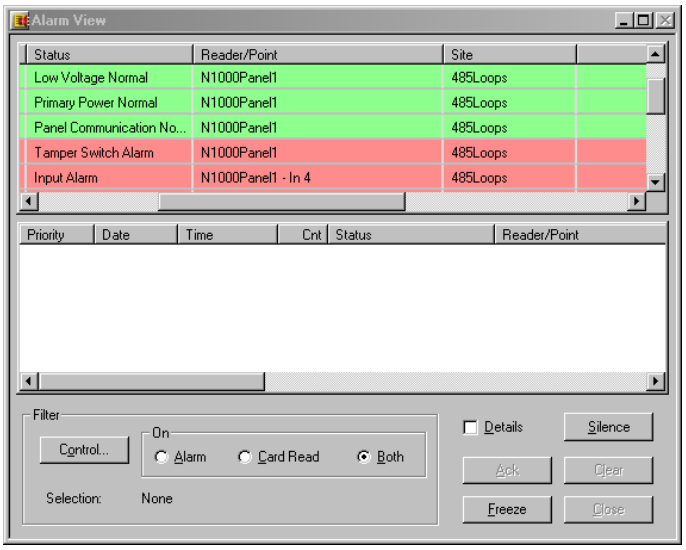
Note: If you have procured the license for the Galaxy panel and/or Vista panel, the alarms triggered on the Galaxy panel and/or Vista panel devices are displayed in the **Alarm View** window.

Opening an Alarm View Window

The **Alarm View** window automatically opens when an alarm is triggered at a reader, door, input point, or output point. You can also manually open the Alarm View window.

To open the Alarm View window:

1. Choose **Operations > Alarms**. The **Alarm View** window appears.



The details of an alarm is displayed in the Alarm View window such as date and time, alarm status, the reader or point from where the alarm is raised, and so on.

The **Cnt** (Count) column on the **Alarm View** window shows the number of state changes in a point.

2. Click **Close** to close the Alarm View window.

Note: By default, alarms that are displayed in the alarm view window beep until they are acknowledged. This default setting can be changed in System Defaults.

Refer to the "Setting defaults for alarm handling" section in the chapter System Settings for changing the default settings for handling the alarms.

Handling Alarms using the right-click menu options

When you right-click the alarm, it enables the list of options to handle the alarm tasks. Based on the selected alarm type, the list of menu options differs.

Control Functions

The control functions pop-up on right-click menu options differ based on the alarm type:

- **Input** alarms: Acknowledge, Clear, Open Default Floor Plan, Add Note, Shunt, Unshunt, and Restore to Time Zone.
- **Door** alarms: Acknowledge, Clear, Open Default Floor Plan, Add Note, Unlock, Lock, Pulse, Timed Pulse, and Restore to Time Zone.
- **Reader** alarms: Acknowledge, Clear, Open Default Floor Plan, and Add Note.
- **Reader or Point** alarm which is attached to a camera: Acknowledge, Clear, Open Default Floor Plan, Add Note, Digital Video Live, and Digital Video Retrieval.

- **Panel System** alarms: Acknowledge, Clear, Open Default Floor Plan, Add Note, Buffer, and Unbuffer.

Table 15-2 Describing the basic right-click menu options for handling alarms

Menu options	Description
Acknowledge	This is to acknowledge an alarm. When an alarm is acknowledged, it is moved to the lower pane of the Alarm View window. The message remains in the lower-pane, until it is cleared. **Note:** If the **Automatically Clear Acknowledged Alarms** option is selected in System Defaults, it is not moved to the lower pane of the Alarm View window, when you acknowledge an alarm.
Open Default Floor Plan	This enables you to open the default floor plan associated to the device from where the alarm is triggered. Refer to the "Configuring an Abstract Device" section in the chapter Device Map, for defining the default floor plan for an ADV.
Add Note	This enables you to provide comments on acknowledging the alarm. When you click this option, the **Add Operator Note** dialog box is opened.

Handling Alarms using the Command buttons

A set of buttons on the Alarm View window enables you to easily handle basic, routine alarm tasks.

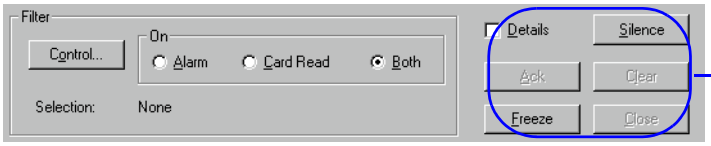


Table 15-3 Describing command buttons in the Alarm View window

Option	Description
Acknowledge (Ack)	To acknowledge an alarm, select it from the list of incoming alarms and click **Ack**. When the alarm is acknowledged, it moves to the list in the lower pane of the Alarm View window. However, if the **Automatically Clear Acknowledged Alarms** option is selected in System Defaults, the alarm is cleared as soon as it is acknowledged. The background color of the acknowledged alarm changes to grey and the text color changes to green (normal), yellow (trouble) and red (alert) depending on the state of the device. It remains in the lower pane of the window until it is cleared.

Table 15-3 Describing command buttons in the Alarm View window

Option	Description
Silence	This enables you to silence the alarm for 60 seconds without actually acknowledging it. This feature is enabled in the Alarms Handling section of the System Default Configuration.
Clear	To clear one or more transactions, select them from the list and click **Clear**.
Freeze	To temporarily stop the display of incoming messages, click **Freeze.** When you click **Freeze**, the button toggles to **Release**. Freezing stops the screen from scrolling as new information appears. Click **Release** to return the Alarm View to its normal functions.
Close	To quit Alarm View, click **Close**.

Note: While acknowledging or clearing alarms, to select multiple alarms:

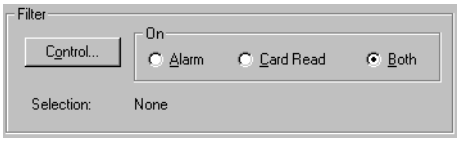
- In sequence: Press and hold the SHIFT key and click the first and last alarms in the range.
- At random: Press and hold the CTRL key and click each alarm.

Filtering Alarm Views

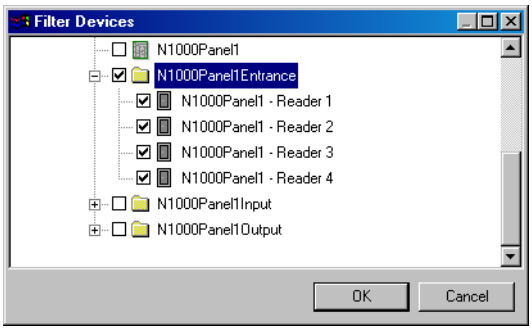
The Alarm View is provided with an option to filter areas and devices for monitoring card reads or alarms on a particular area or device. Filtering could be very useful for instances, such as, a particular guard station needs to monitor the loading dock. An Alarm View can be defined to receive messages only from the loading dock doors.

To filter the alarms:

1. Click **Operations > Alarms** or click the Dynamic Alarm View icon on the tool bar. The **Alarm View** window is displayed.
2. Under **On**, click **Alarm**, **Card Read** or **Both** to view only the alarms, card reads or both respectively.



3. To filter the branches and devices, click **Control** under **Filter**. The **Filter Devices** window appears.



4. Expand the tree by clicking the plus [+] symbol.
5. Select a branch or an individual device to be filtered for monitoring.
6. To filter an branch, right-click the branch and select **Configure**. The **Set Device Selection for a Control Area** dialog box appears.

Note: You can also double-click the branch to display the S**et Device Selection for a Control Area** dialog box.

7. Select one of the following options:
   - **Leave Selection for all devices in this area as it currently is**: To leave the devices in this branch as it is - selected or cleared.
   - **Un-Select (Filter out) all devices in this area**: To clear the selection of all the devices in this branch. The devices in this branch are not monitored.
   - **Select (Include) all devices in this area**: To select all the devices in this branch. All the devices in this branch are monitored.
8. To filter a device, right-click the device and select **Invert Selection Status** to select the device or clear the selection.
9. Click **OK** to return to the **Filter Devices** dialog box.
10. Click **OK** to save the filter selection. Only the alarms that occur in the selected area and device are displayed in the **Alarm View** window.

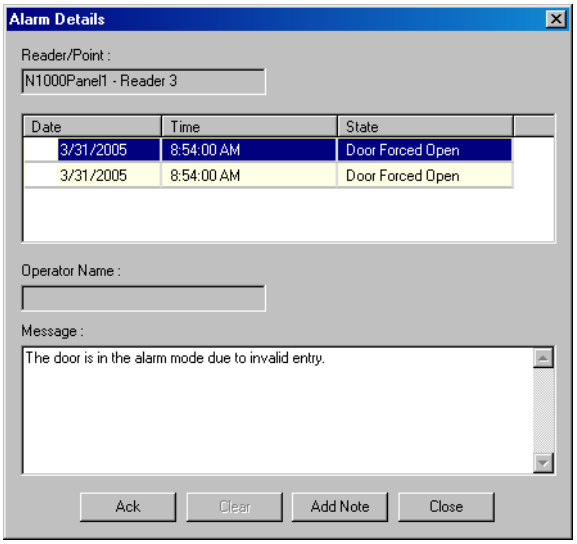
Note: The filter settings are lost after you close the Alarm View window. Therefore, to view the floor plan with filter settings, you can open the Alarm View window from the Floor Plan.

Refer to the "Adding Alarm View and Event View links to the Floor Plan" section in the chapter Floor Plan, for details on creating an Alarm View in the Floor Plan.

Viewing Alarm Details

To view the details of an alarm:

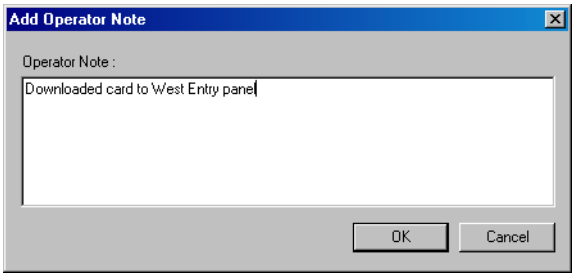
1. Choose **Operations > Alarms** or double-click an alarm to open an **Alarm View** dialog box.
2. Select the **Details** check box. The **Alarm Details** window is displayed.



The **Alarm Details** window displays the following information:

- Name of the reader, input or output point from where the alarm is triggered
- The date and time of the alarm and the state of the reader or point
- Indication of whether the alarm has been acknowledged or cleared
- The name of the operator who has acknowledged or cleared the alarm.
- The message box to display the note added by the operator while acknowledging or clearing the alarm.

3. To acknowledge the alarm, select the alarm and click **Ack**.
4. To clear the alarm, select the alarm and click **Clear**.
5. To add a note to an alarm while acknowledging or clearing, click **Add Note**. The **Add Operator Note** dialog box appears.



6. Type a message in the **Operator Note** and click **OK**.

Note: The operator notes are included in history and can be printed using the **History** report.

Autocard Lookup

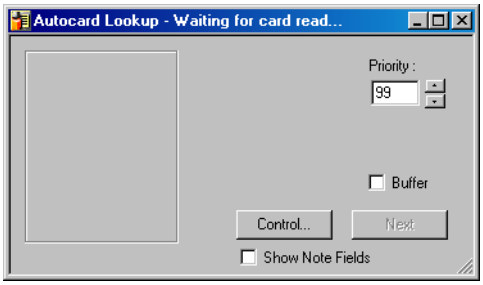
The Autocard Lookup feature enables you to view the card holders details from the designated readers or card reads that have a status priority higher than a designated threshold. If the Autocard Lookup window is minimized and a card read is received, the window will pop-up automatically.

The Autocard Lookup window displays the card holder picture (if available), name of the card holder, card number, time, date, reader name, and the status of the card read.

Activating Autocard Lookup

To activate an Autocard Lookup window:

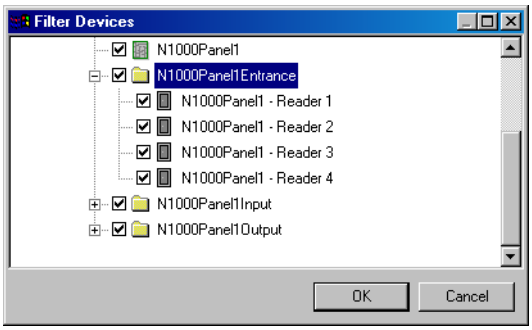
1. Choose **Operations > AutoCard Lookup**. The **AutoCard Lookup - Waiting for card read...** window appears.



2. Set the **Priority** of card read. The card holder details of all card reads having a higher priority (lower number) than this priority is displayed in Autocard lookup. The priority of a given card read event is set in the reader's Action Group.

   Refer to the "Configuring an Abstract Device" section in the chapter Device Map for details on setting the priority for an action.

3. To specify the areas and panels of card reads, click **Control**. The **Filter Devices** window appears.



4. Expand the panel by clicking on the plus signs [+].
5. Right-click the readers that you want to monitor through Autocard Lookup and select **Invert Selection Status**.
6. Click **OK** to return to the **AutoCard Lookup - Waiting for Card Read...** window. When a card from the filtered area and device is presented to the reader, the card information is displayed.

7. Select the **Buffer** check box to freeze the current card information on the lookup screen, while saving any subsequent card reads in the panel memory.
8. Click **Next** to display the next card read results, while remaining in the buffer mode.

Note: The **Next** button is enabled only when you have the sequence card reads in the panel memory.

9. Clear the **Buffer** check box to remove all stored information and continue with the next card presented.
10. Click the **Show Note Fields** check box to display the additional information of the card holder defined in the note fields.

    Refer to the "Configuring Autocard Lookup" section in the chapter Card Holders for enabling note fields to be displayed in the Autocard Lookup window.

Note: Multiple lookup windows can be opened at the same time, and each can have its own filter selections.

Live Monitor View

The Live Monitor view displays information from a selected CCTV camera in real-time. You can adjust the video display using the Iris, Zoom, Focus, Pan and Tilt controls that are located to the right of the viewing screen. In addition, you can capture and save individual frames.

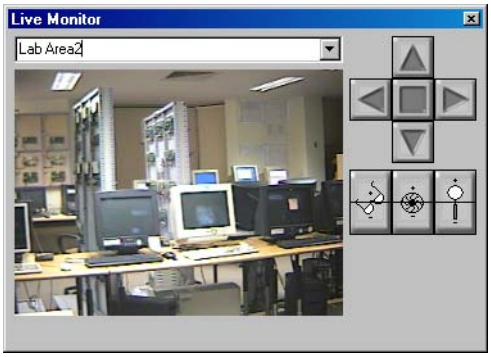
For Live Monitor view, you must:

- Equip your computer with a video capture card.
- Connect the CCTV Switcher to the video capture card.
- Define cameras and monitors on the Device Map.
- Select the CCTV Switcher monitor for Live Monitor view while setting the Workstation Defaults.

Opening a Live Monitor View

To open the Live Monitor view:

1. Choose **Operations > Live Monitor**. The **Live Monitor** dialog box appears.



2. To enlarge the size of the **Live Monitor** view, click and drag the corners of the dialog box.
3. To view a different area from a different camera, select the camera in the drop-down list.

Capturing a Frame from the Live Monitor View

To capture a frame from the Live Monitor view, freeze the live view and then save the frame.

1. To freeze a view, right-click anywhere in the live area and select **Live**.
2. To save the frame, right-click the frozen video and select **Save**.
3. Select a path, enter a filename and click **Save** to save the image as a .jpg file.
4. Click **OK**.

Controlling the Camera

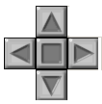
You can control the focus, aperture adjustment, zoom, pan and tilt, and homing presets of switchers and cameras remotely through WIN-PAK.

Note: Ensure that the above-mentioned features are supported by the switchers and cameras.

1. To view the title of the camera that is monitored, right-click in the live view area and select **Send Camera Titles**.
2. To view the time and date, right-click in the live view area and select **Send Time and Date**.

   Refer to the ***CCTV equipment manual*** to ensure that title, time and date features are supported.

Table 15-4 Describing control buttons on the Live Monitor window

Button	Control Button	Description
	Adjusting Focus	Click and hold the upper half of **Focus In/Focus Out** to slowly focus on closer objects. Click and hold the lower half of the button to slowly focus on distant objects.
	Adjusting Iris	Click and hold the top half of **Iris In/Iris Out** to slowly increase the aperture (opening) of the camera iris, allowing more light in. Click and hold the bottom half of the button to slowly decrease the aperture of the camera iris, letting in less light.
	Adjusting Zoom	Click and hold the upper half of **Zoom In/Zoom Out** to slowly zoom the camera in. Click and hold the lower half of the button to slowly zoom the camera out.
	Adjusting Pan/Tilt	The control arrows on the **Live Monitor** window pan the camera left and right, and tilt it up and down. Click and hold the camera control arrows to move the camera. The left arrow pans to the left. The right arrow pans to the right. The up arrow tilts the camera up, while the down arrow tilts the camera down. If the cursor is moved over the live viewing area, arrows appear. Clicking these cursor arrows has the same effect as the control arrow buttons.

Setting Pan and Tilt Limits

Panning and tilting limits are set for each camera to ensure that the camera does not pan or tilt to a point that is stressful on the camera.

Perform the following steps to set the upward tilt limit for a camera. Repeat these steps for downward tilt, left pan, and right pan on each camera.

1. Using the upward and downward arrows, tilt the camera to the highest required point.
2. Right-click the upward arrow and select **Set Limit** from the control menu displayed.

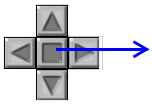
Clearing Limits

To clear the pan and tilt limits:

1. Right-click the arrow for which you want to clear limits, and select **Clear Limit** from the control menu.

Setting Home Position

Home Position is the camera view set for each camera to bring back its home position with the current focus, aperture, and zoom settings. This is the most utilized camera view.



To set the home position:

- On the **Live Monitor** window, click the square button, located among the pan/tilt arrows.

The following steps outline setting a home position:

1. Adjust the pan, tilt, and aperture settings for the view that you want to make your home position.
2. Right-click **Home** and click **Set Home**.

   The camera returns to this view anytime you click **Home**.

WIN-PAK CCTV Options

Brand	Switch	Camera Title	Time Date	Pan Tilt	Zoom	Iris	Pan Tilt Limit	Zoom Limit	Focus Limit	Iris Limit	Seek Home	Set Home	Select Monitor
Burle	x	x	x	x	x	x	o	o	o	o	x	x	o
Dedicated Micros	x	x	x	x	x	o	o	o	o	o	o	o	o
Geutebruk	x	o	x	x	x	x	o	o	o	o	x	x	o
Javelin	x	x	x	x	x	x	x	x	x	x	x	x	o
NCI CCTV	x	x	x	x	x	x	x	x	x	x	x	x	o
Panasonic	x	o	o	x	x	x	o	o	o	o	x	o	o
Pelco	x	o	o	x	x	x	o	o	o	o	x	x	x
Vicon	x	o	x	x	x	x	o	o	o	o	x	x	x

X = option is available and usable through WIN-PAK
O = option either not available or not supported by WIN-PAK

Digital Video

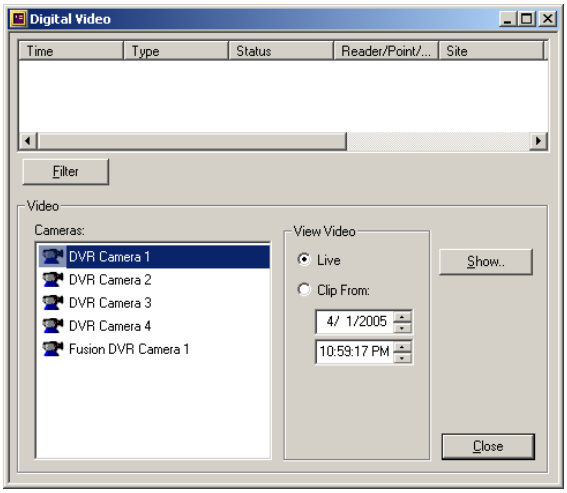
The Digital Video Display shows the live video or the recorded video from the selected DVRs. At the maximum, it can display videos from 16 cameras.

Opening the Digital Video Display

The Digital Video Display window opens automatically, when an action triggers this window to open. However, you can open the video display window manually.

To open the digital video display:

1. Choose **Operations > Digital Video**. The **Digital Video** window is displayed.

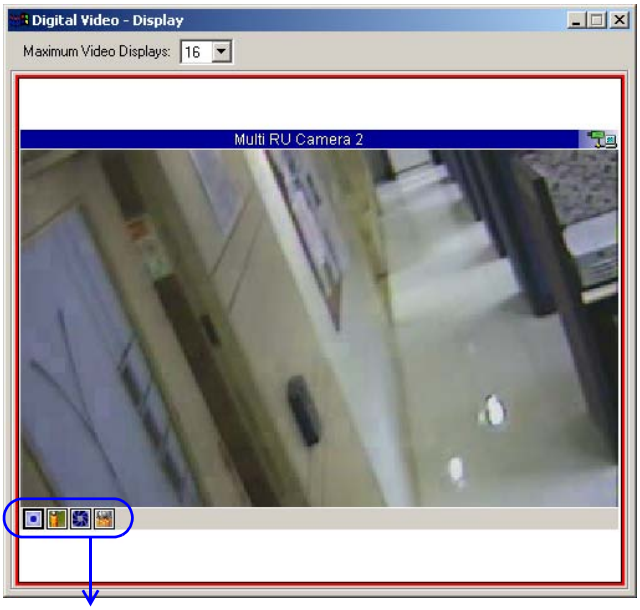


2. Select the cameras in the **Cameras** list. For multiple selections, use the SHIFT or CTRL key.
3. To view live video, click **Live**.

   OR

   To view the recorded clip, click **Clip From** and enter the date and time from when you want to view the clip.
4. If you want to filter the events to be displayed in the Digital Video display, click **Filter**.

   Refer to the "Filtering Events" section in this chapter for details on filtering the events.
5. Click **Show** to view the live video or the recorded video. The **Digital Video Display** window appears.



Camera Controls for live video

6. Use the camera controls in the lower-left corner of the **Digital Video Display** window to adjust the camera as required.

Note: The Digital Camera controls placed on the lower-left corner of the live video display helps to adjust the camera Focus, Iris, Zoom, and Pan and Tilt.

Controlling live video display

You can control the focus, iris, zoom, and pan and tilt of the cameras using the camera control available at the bottom of the live video display.

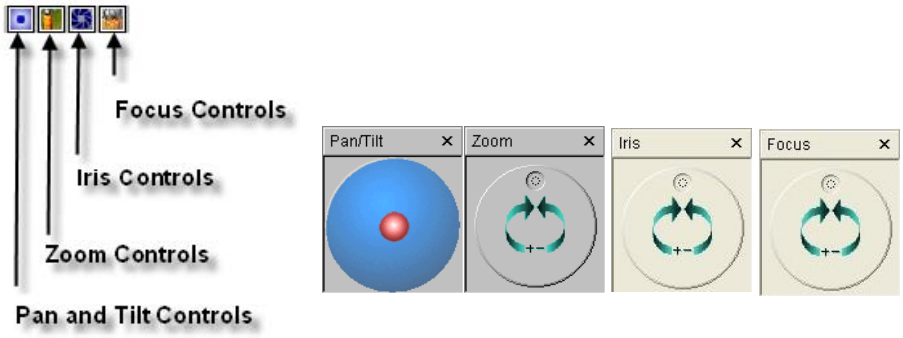
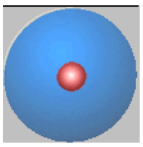


Figure 15-1 Depicting camera controls on the live digital video display

The following table describes the control buttons on the live digital video display:

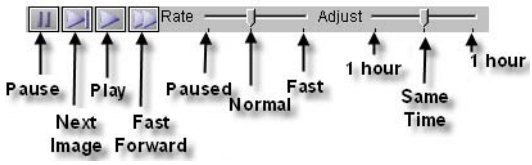
Table 15-5 Describing control buttons on the Live Monitor window

Button	Control Button	Description
	Pan/Tilt	Click the Pan and Tilt icon to display the Pan/Tilt adjustment box. Click and drag the red dot left or right to pan camera left or right. Click and drag the red dot up or down to tilt the camera up or down.
	Zoom	Click the Zoom icon to display the Zoom adjustment box. Click the drag the Zoom dot towards right to zoom the camera in. Click and drag the dot towards left to zoom the camera out.
	Iris	Click the Iris icon to display Iris adjustment box. Click and drag the Iris dot towards right to increase the aperture of the camera iris. Click and drag the Iris dot towards left to decrease the aperture of the camera iris.
	Focus	Click the Focus icon to display the Focus adjustment box. Click and drag the Focus dot towards right to focus on closer objects. Click and drag the Focus dot towards left to focus on distant objects.

Controlling the recorded video display

In the recorded video window, controls are provided to pause, play, fast forward, adjust time, and so on.

1. Click **Pause** to stop the video and click **Play** to restart the video display.



2. Adjust the **Rate** control to adjust the video play-back speed.
3. Adjust the **Adjust** control to adjust the time of the recorded video maximum to an hour before or after the current time being viewed.

Right-Click Menu Options

When you right-click in the live video display, few control options are provided to customize the video display and adjust the camera controls.

Table 15-6 Describing the Live Video Display control options

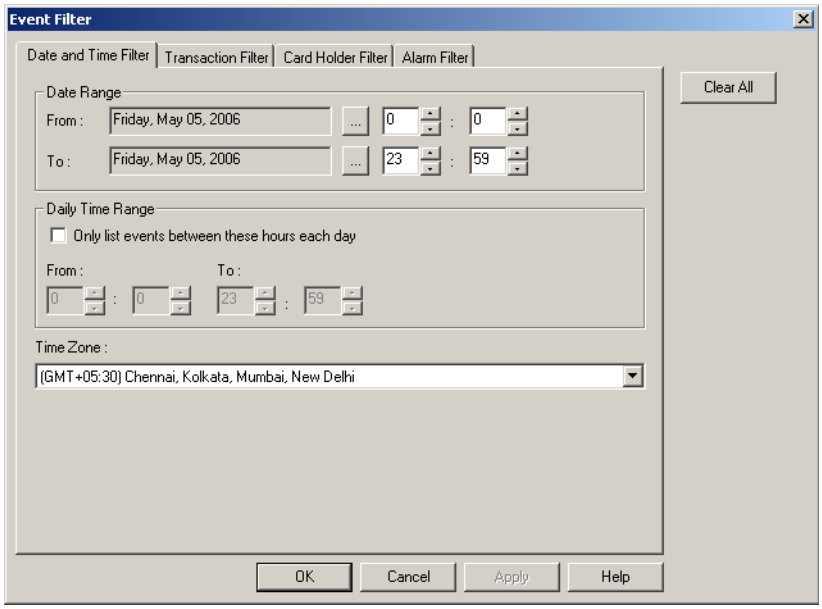
Control Option	Description
Show Title	The title bar displays the ADV name and the status icon. By default it is selected.
Show Controls	The camera controls are available in the live video display. By default it is selected.
Auto Focus	Camera automatically focuses on subject, provided it is an auto-focus camera. By default it is cleared.
Auto Iris	Camera automatically adjusts for brightness, provided the camera has an automatic-iris control. By default it is cleared.
Pan/Tilt speed	Controls speed at which the camera pans and tilts. Three speed options are available: Slow, Medium, and Fast. By default it is Medium.
Network speed	Controls speed at which pan/tilt command is sent to the camera. Three speed options are available: Dial-up connection, Slow LAN, and Fast LAN. By default it is Fast LAN.
Set Preset	Enables the operator to set maximum of eight preset controls for a PTZ camera.
Go to Preset	Enables the operator to select from eight previously defined preset PTZ camera controls.
Close	Enables the operator to close an individual camera display without closing the camera display window. By default it is cleared.

Filtering Events

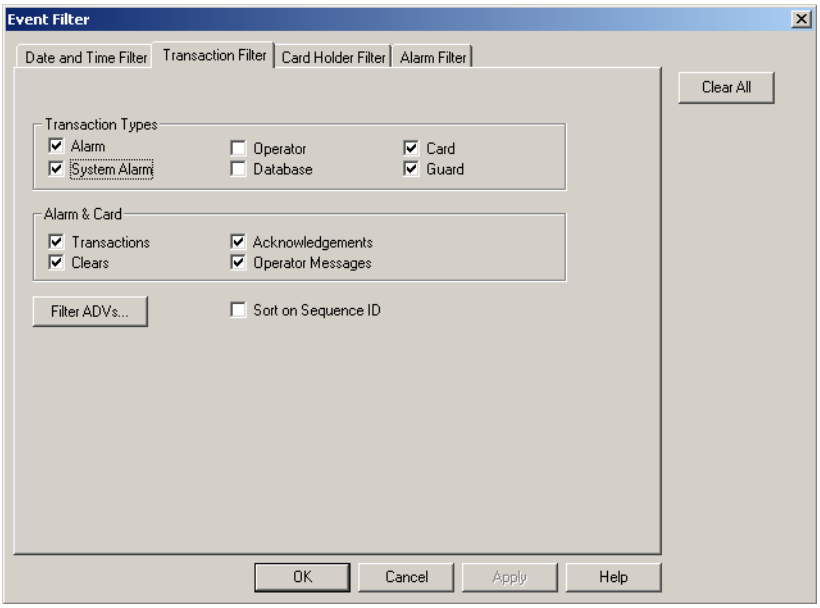
The filter option in the Digital Video window helps you to view the events for a specific period. Therefore, it enables you to retrieve the digital video that is associated to an ADV, which is configured for an auto pop-up display. For example, you may want to view the events from March 15, 2005 to April 30, 2005.

To filter the events of the recorded video display:

1. In the **Digital Video** window, click **Filter**. The **Event Filter** dialog box appears.



2. To select the associated camera and recorded video clip based on the specific date and time ranges:
    a. Click the **Date and Time Filter** tab.
    b. Under **Date Range**, select the **From** and **To** dates using the ellipsis button.
    c. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.
    d. To display video for events that occurred during a particular period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The From and To text boxes are enabled.
    e. In the **From** and **To** boxes, enter the time range (in hours and minutes).
    f. Select the standard time zone in the **Time Zone** list.
3. To select the associated camera and recorded video clip based on the type of card events:
    a. Click the **Transaction Filter** tab.



b. To filter the video display based on the transaction types, select the following options under **Transaction Types**:

Table 15-7 Describing the transaction types for filtering video display

Card Option	Description
Alarm	Includes alarms in Alert and Normal states.
System Alarm	Includes events of system type alarms (not wired points) such as Poll Response alarms.
Operator	Includes events of operator activities, such as log on and log off.
Database	Includes events of basic database activities, such as time, date, operator, update, delete or add action to a particular database.
Card	Includes all card events.
Guard	Includes all guard tour events.

c. To select the camera display based on the alarm and card behaviors, select the following options under **Alarm & Card**:

Table 15-8 Describing the alarm and card options for filtering video display

Card Option	Description
Transactions	Includes card events of all transactions such as normal, alarm, or host grant.
Clears	Includes the card alarm events that were cleared by the operator.
Acknowledgements	Includes the card alarm events that were acknowledged by the operator.
Operator Messages	Includes the card alarm events that were provided with the operator messages.

d. To filter the transactions performed on specific ADVs (devices), click **Filter ADVs**. The **Filter Devices** dialog box appears.

e. Double-click the branch (folder) to select all the devices in the branch

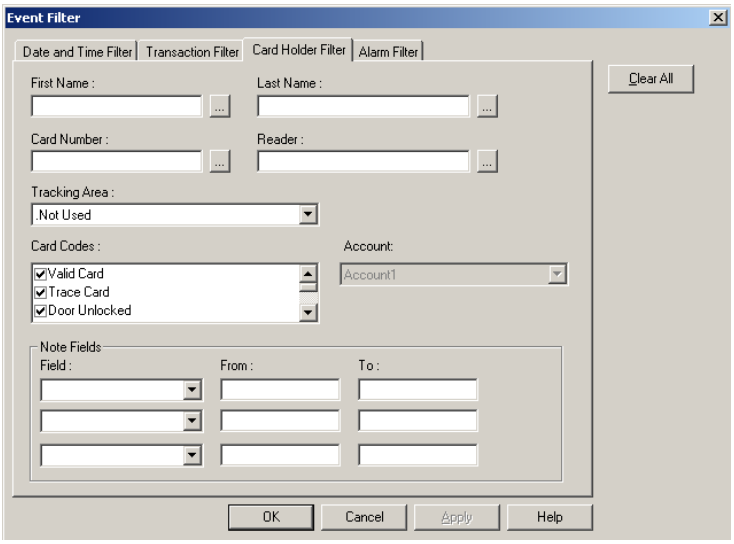
OR

Expand the branch (folder) and double-click a device to select the particular device.

f. Click **OK** to return to the **Event Filter** dialog box.

4. To filter the card holders:

a. Click the **Card Holder Filter** tab.



b. Type the **First Name** and **Last Name** of the card holder, or select them by clicking the ellipsis button.

c. Type the **Card Number** of the card holder or select it by clicking the ellipsis button.

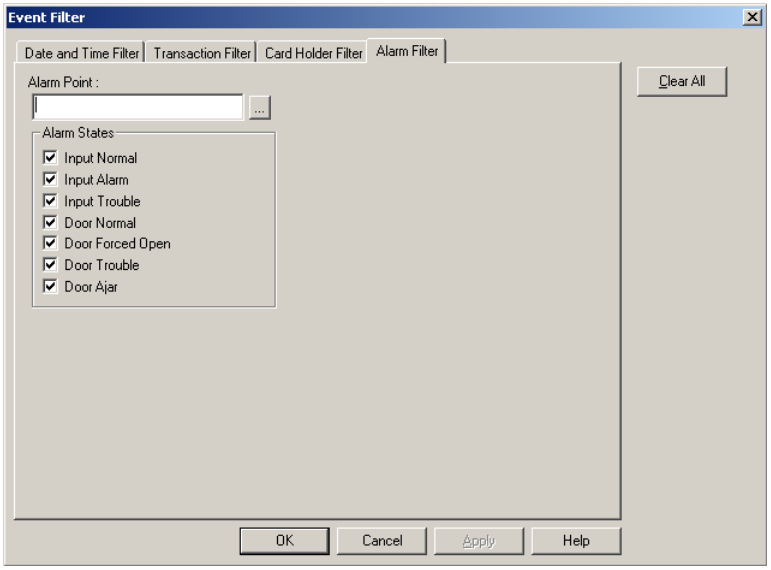
d. To display the video of the card holders accessing a specific area, select an area in the **Tracking Area** list that is configured in Tracking and Mustering Area.

e. Select one or more **Card Codes** which define the card transaction.

f. Select the **Note Fields** to be displayed. You can also specify the range if you select the numerical note field.

5. To filter further on alarm events:

a. Click the **Alarm Filter** tab.



b. Enter the alarm point name or use the ellipsis button to find an alarm point.

c. Select the **Alarm States** that must be included in the report.

6. Click **OK** to save the filtering settings and return to **Digital Video** window.

Events associated with a digital camera are displayed with either a fixed camera icon or a PTZ (Pan Tilt Zoom) camera icon, represented with a zoom lens.

Translation

16

In this chapter...

Introduction

WIN-PAK allows you to translate the language of its user interface to languages other than English. The User Interface is translated based on the entries in language text files. A language text file contains entries in English and the corresponding entries in the language to be translated for the captions in the dialog boxes, menus, and other text in the WIN-PAK user interface. The text files for French, German, Dutch, Italian, English, Simplified Chinese, and Traditional Chinese languages are available by default in the **WINPAKPRO\Language Files** folder of WIN-PAK.

Translating WIN-PAK User Interface involves:

1. Adding a new language with its text and help files into the **WINPAKPRO\Language Files** folder.
2. Selecting the language for translation.
3. Modifying the translated text (if required) for the dialog box captions, menus, and the other text in the User Interface.

By default, WIN-PAK is designed to work with U.S. English operating systems. Therefore, a special version of WIN-PAK is required to work with the operating systems of other languages. Contact the technical support of Honeywell Access Systems for support on international operating systems.

Language Configuration

Configuring language details involves:

1. Adding a new language with its text and help files.

   OR

   Editing existing language information.

2. Selecting a language for translation.

If a language text file is present, the user interface is translated based on the information present in the text file. In case of a new language, the text file would initially be empty. You are provided with the option of entering the translated text for the captions in the dialog boxes, menus, and the other text present in the user interface. These entries are updated in the language text file and are used for translation.

Note: **English, United States** is the default language used for WIN-PAK and its details cannot be edited.

Adding or Editing Language Information

You can add a new language for translation by providing the following information:

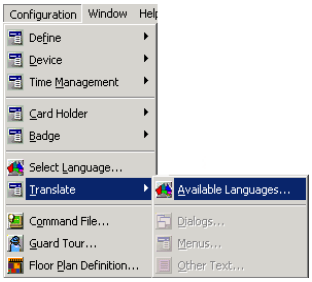
- the language name
- the language text file
- the language help file

Note: Before adding a language, ensure that the language text file and help file (chm) are present in the **WINPAKPRO\Language Files** folder.

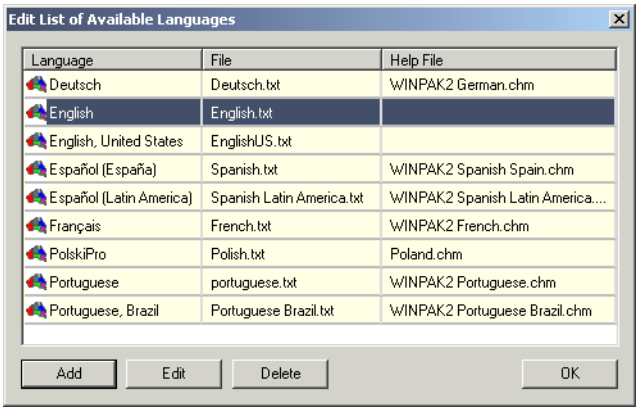
Adding a New Language

Note: Honeywell recommends you to contact its support center for creating language text files.

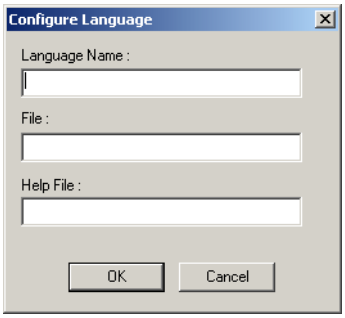
1. Choose **Configuration > Translate > Available Languages**.



The **Edit List of Available Languages** dialog box appears with a list of existing language files.



2. Click **Add**. The **Configure Language** dialog box appears.



3. Type the **Language Name**.
4. Type a name for the text file in **File**.

   Note: If the new language refers to a text file available in the **WINPAKPRO\Language Files** folder, type the respective text file name.

5. Type the name of the **Help File** for this language. By default, the American English help file is used.

   Note: The newly added text and help files are saved in the **WINPAKPRO\Language Files** folder.

6. Click **OK** to save the language information, and return to the **Edit List of Available Languages** dialog box. The details of the newly added language are listed.
7. Click **OK** to close the window.

Editing a Language

1. Choose **Configuration > Translate > Available Languages**. The **Edit List of Available Languages** dialog box appears.
2. Select the language you want to edit and then click **Edit**. The **Configure Language** dialog box appears.
3. Edit the **Language Name**, **File**, and **Help File**.
4. Click **OK** to save the changes and return to the **Edit List of Available Languages** dialog box.

   Note: The text file for the language **English, United States** cannot be edited.

Deleting a Language

1. Choose **Configuration > Translate > Available Languages**. The **Edit List of Available Languages** dialog box appears.
2. Select the language you want to delete and then click **Delete**. A message asking for confirmation appears.
3. Click **Yes** to confirm the deletion.

Selecting a language for translation

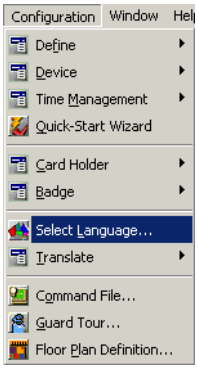
You can select a language for translating the WIN-PAK user interface. When a language is selected, the WIN-PAK user interface is translated based on the entries in the language text file.

In addition, you can set the language for operators using the **Operator** option in the **System** menu. The WIN-PAK user interface is translated to the language of the operator who logs on to WIN-PAK.

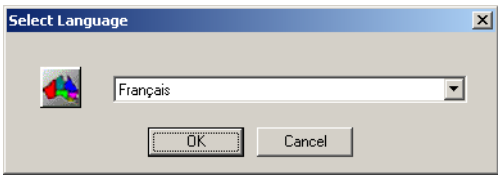
Refer to the "Defining Operators" section in the chapter System Settings for more details on setting language for operators.

To select a language:

1. Choose **Configuration > Select Language**.



The **Select Language** dialog box appears.



2. Select a language for translation from the list.
3. Click **OK**.

Note: The sub-menu options **Dialogs**, **Menus**, and **Other Text** are enabled in the **Configuration > Translate** menu. You can edit the entries for dialog boxes, menus, and the other text. However, you cannot edit the user interface entries, if you have selected the language as **English, United States**.

Adding or editing entries for translating Dialogs, Menus, and Other Text

On selecting a language, the WIN-PAK user interface is translated based on the entries in the language text file. In case of a new language, the text file would initially be empty. In such a case, you can translate the captions for all the dialogs, menus, and other text present in the user interface. The translated captions are entered in the language text file. In addition, you can edit the translated captions for all dialogs, menu, and the other text in the user interface. The language text file is updated with the modified entries.

Note: You can add or edit the translated captions for dialogs, menus, and other text only after selecting a language for translation.

Refer the to "Selecting a language for translation" section in this chapter, for more details on selecting a language for translation.

Adding or Editing entries for dialog boxes

1. Choose **Configuration > Translate > Dialogs**. The **Edit Dialog Text** dialog box appears.

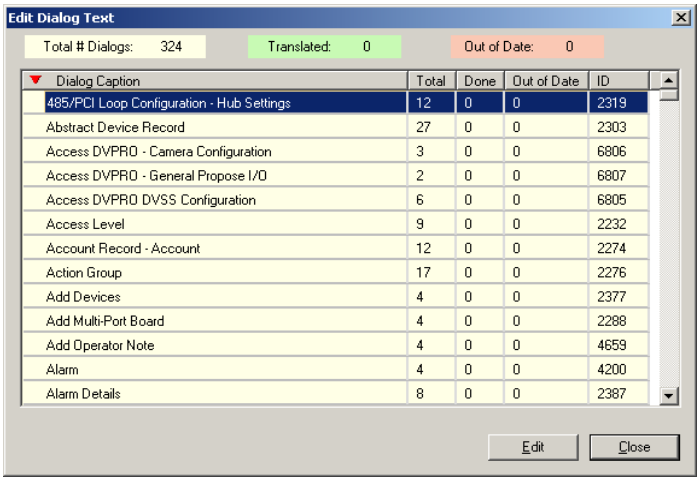


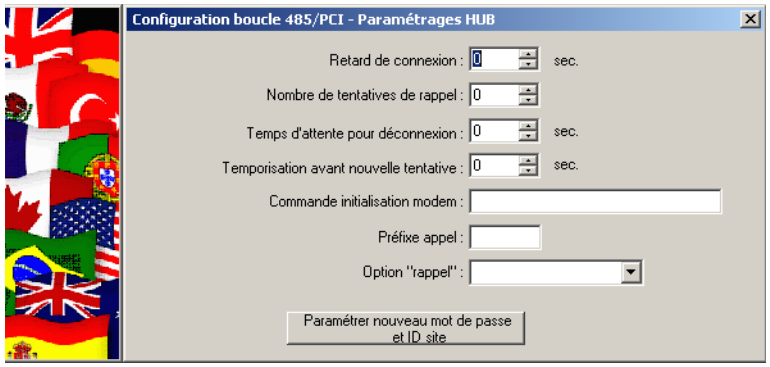
Table 16-1 Edit Dialog Text - Elements and Descriptions

Field/Column	Description
Total # Dialogs	The total number of dialog boxes for translation.
Translated	The total number of fields in the dialog box that has been translated.
Out of Date	The number of dialog boxes that were translated in the previous version of WIN-PAK (applies only to a WIN-PAK upgrade.)

Table 16-1 Edit Dialog Text - Elements and Descriptions

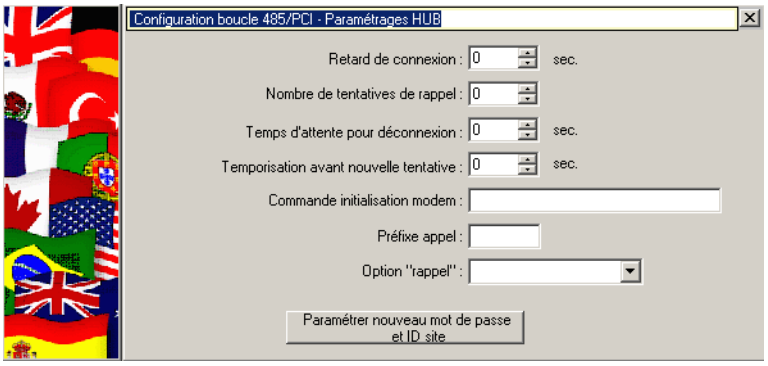
Field/Column	Description
Dialog Caption	The caption of the dialog box.
Total	The total number of fields in the dialog box.
Done	The number of fields that has been translated in the dialog box.
Out of Date	The number of fields that were translated in this dialog box in the previous version of WIN-PAK (applies only to a WIN-PAK upgrade.)
ID	The dialog ID used in the application resource file.

2. Select a dialog caption from the **Dialog Caption** list and click **Edit**. The dialog box of the selected dialog caption appears.

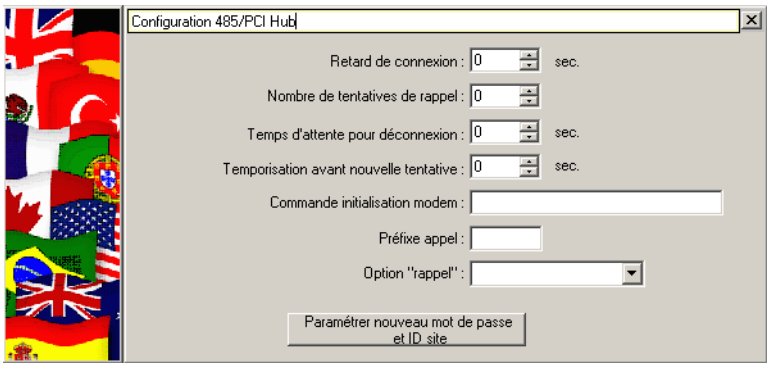


3. Click the field you want to edit. The field name is highlighted.

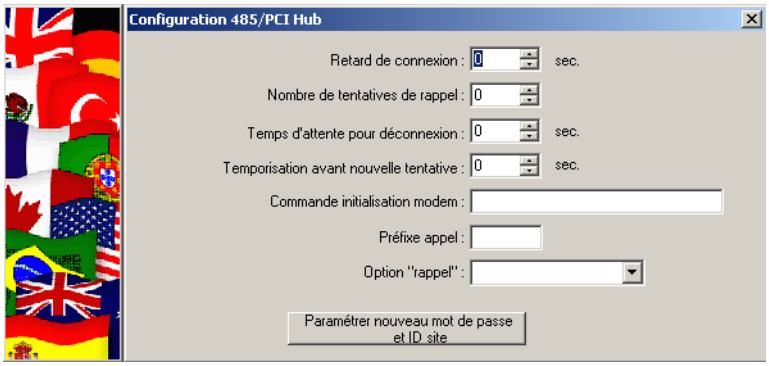
Note: To change the title of the dialog box, click the title and edit the dialog box.



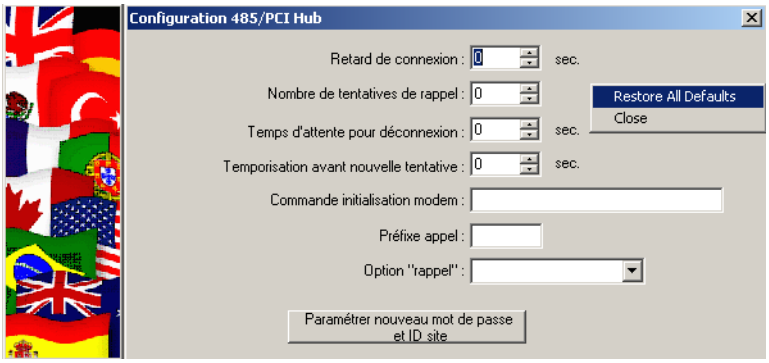
4. Type the text in the highlighted area.



5. Press ENTER to save the change.



Note: To restore the default button or field names, right-click the dialog box and click **Restore All Defaults**.



6. Repeat steps 3 to 5 of the procedure to edit the remaining field names in the dialog box.
7. Click the **Close (X)** icon in the dialog box to save the changes and to close the dialog box.

   The changes are updated in the language text file. The values in **Total Line of Text**, **Translated**, **Out of Date, Total**, **Done**, and **Out of date** columns in the **Edit Dialog Text** are updated with the number of fields that are translated.

Adding or editing entries for menus

1. Choose **Configuration > Translate > Menus**. The **Translate Menu Text** window appears.

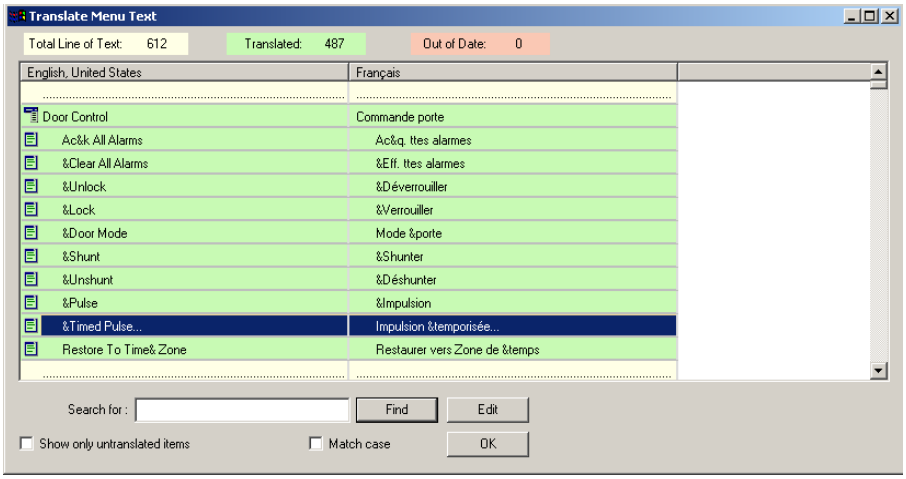


Table 16-2 Translate Menu Text - Elements and Description

Field/Column	Description
Total Line of Text	The total text lines to be translated.
Translated	The total number of text lines that have been translated.
Out of Date	The number of menus that were translated in the previous version of WIN-PAK (applies only to a WIN-PAK upgrade.)
English, United States	The menu captions in the original language of WIN-PAK
Language (the language selected for translation is displayed as the column name.)	The menu text in the translated language.

2. Double-click the menu item that must be translated from the list, or right-click the menu item and then click **Edit**. The **Translate Text** dialog box appears.

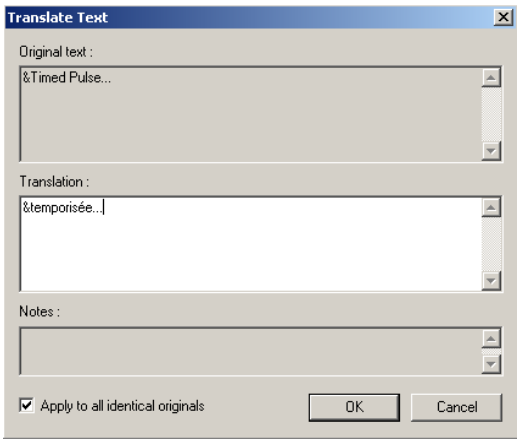
Note: To search for the menu item in a scrolling list:

a. Type a part or the whole text in the **Search** box.

b. Select the **Match Case** check box to match case while searching.

c. Select the **Show only untranslated items** check box to search only for menu items that are not translated.

d. Click **Find**. The first instance of the menu item is highlighted in the list. Clicking **Find** repeatedly highlights the remaining instances of the text in the list.



The current menu caption is displayed under **Original text**.

3. Type the translated caption for the menu under **Translation**.

Note: Use the "&" symbol in the menu caption to indicate that the character immediately following the "&" must appear with an underscore and can be used as a hot key (accessed by pressing ALT + Key entry.)

4. Select the **Apply to all identical originals** check box to apply the translation for all instances of **Original text** in the User Interface.

Note: The translation entry is applied only to the exact instances of **Original text**, matching the case.

5. Click **OK** to save the entry and return to the **Translate Menu Text** window.

The changes are updated in the language text file. The values in **Total Line of Text**, **Translated**, and **Out of Date** columns in the **Edit Dialog Text** are updated with the number of fields that are translated.

Adding or Entering Entries for other Text

Other text refers to the text other than the dialog box or menu captions, such as examples, warnings, prompts, messages, and so on.

1. Choose **Configuration > Translate > Other Text**. The **Translate Other Text** window appears.

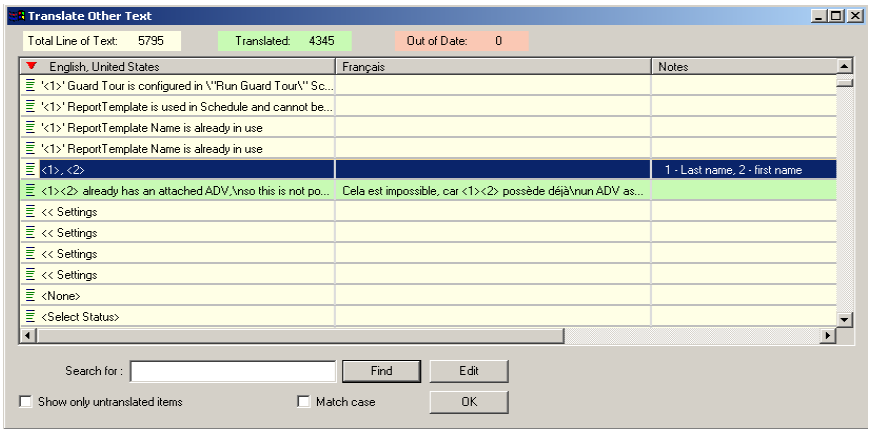


Table 16-3 Translate Other Text Options

Field/Column	Description
Total Line of Text	The total number of lines of text to be translated.
Translated	The total number of lines of a text that have been translated.
Out of Date	The number of miscellaneous text entries that were translated in the previous version of WIN-PAK (applies only to a WIN-PAK upgrade.)
English, United States	The text in the original language of WIN-PAK
Language (the language selected for translation is displayed as the column name.)	The text in the translated language.
Notes	The instructions used for performing the translation. This is included in the text file.
In File	This is significant only for the maintenance people.

2. Double-click the text that must be translated from the list, or right-click the text and then click **Edit**. The **Translate Text** dialog box appears.

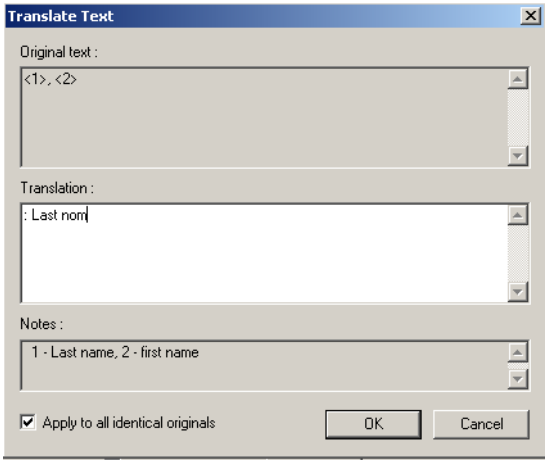
Note: To search for the text item in a scrolling list:

a. Type a part or the whole text in the **Search** box.

b. Select the **Match Case** check box to match case while searching.

c. Select the **Show only untranslated items** check box to search only for text items that are not translated.

d. Click **Find**. The first instance of the text item is highlighted in the list. Clicking **Find** repeatedly highlights the remaining instances of the text in the list.



The current line of text is displayed under **Original text**.

3. Type the translated text under **Translation**.
4. Select the **Apply to all identical originals** check box to apply the translation to all instances of the **Original text** in the user interface.

   Note: The translation entry is applied only to the exact instances of the **Original text**, matching the case.

5. Click **OK** to save the entry and return to the **Translate Other Text** window.

   The changes are updated in the language text file. The values in **Total Line of Text**, **Translated**, and **Out of Date** columns in the **Edit Dialog Text** are updated with the number of field names that are translated.

Reports

17

In this chapter...

Introduction

You can generate a number of reports using WIN-PAK. These reports can be generated based on the filter criteria. Reports can be sorted in an ascending or descending order and can be previewed and printed.

The following is the list of reports that can be generated in WIN-PAK:

- Access Area
- Access Level
- Account
- Attendance
- Card
- Card Frequency
- Card History
- Card Holder
- Card Holder Tab Layout
- Command File
- Control Area
- Device Map
- Floor Plan
- Galaxy Panel Log
- Guard Tour
- History
- Holiday Group
- Note Field Template
- Operator
- Operator Actions
- Operator Level
- Schedule
- Time Zone
- Tracking and Mustering Area

In addition, WIN-PAK provides an option to define the templates for the Card Holder report and the History report.

Report Templates

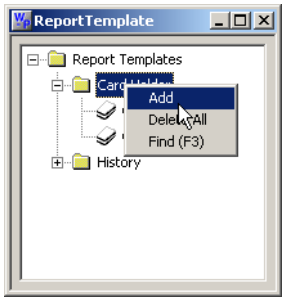
In WIN-PAK, you can define the report templates for the frequently-generated reports; Card Holder report and History report.

Defining Card Holder Report Templates

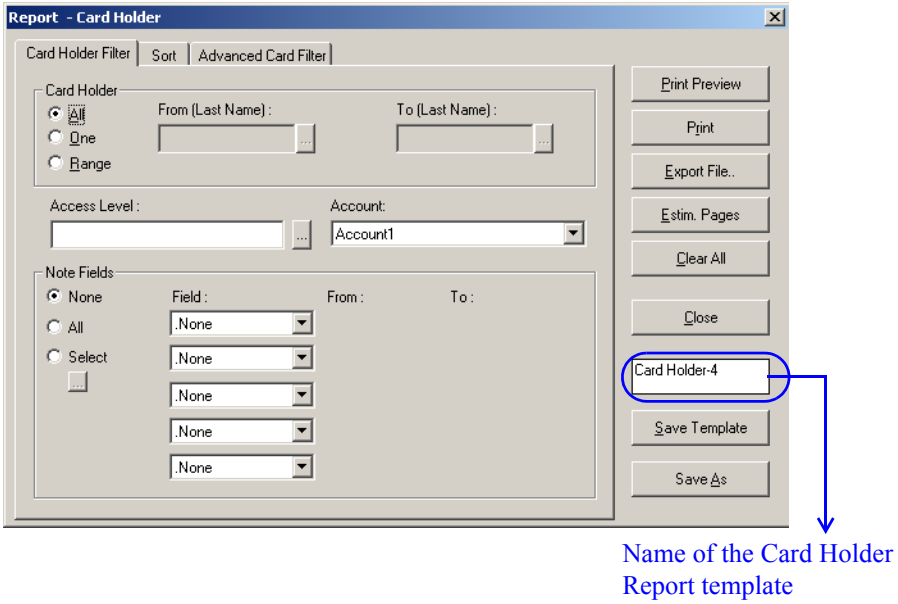
Adding a Card Holder Report Template

To define the Card Holder report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the Card Holder and History folders.

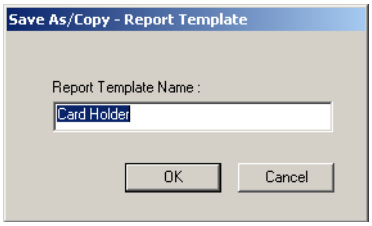


3. Right-click the **Card Holder** folder and click **Add**. The **Report - Card Holder** dialog box appears.



Refer to the "Card Holder Report" section in this chapter for more on defining the filter options for the card holder report.

4. Type the name of the Card Holder Report template in the text box on the right.
5. Click **Save** Template to save the template.
6. To create a copy of the template, click **Save As**. The **Save As/Copy - Report Template** dialog box appears.



7. Type a new name for the template and click **OK** to create a copy of template and return to **Report - Card Holder** dialog box.
8. Click **Close** to close the dialog box.

Editing a Card Holder Report Template

To edit the Card Holder Report template:

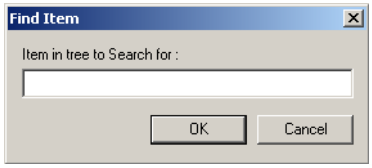
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card Holder** folder.
3. Right-click the report template and click **Edit**. The **Report - Card Holder** dialog box appears.

   Refer to the "Adding a Card Holder Report Template" section in this chapter for details on editing the template.

Searching a Card Holder Report Template

To search a Card Holder Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card Holder** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.

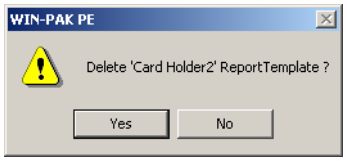


4. Type the name of the template to be searched and click **OK**. The template starts with the specified name is highlighted.

Deleting a Card Holder Report Template

To delete a Card Holder Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card Holder** folder.
3. Right-click the report template and click **Delete**. A message asking for confirmation appears.



4. Click **Yes** to confirm the deletion. The selected report template is deleted.

To delete all the card holder report templates:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and
3. Right-click the **Card Holder** folder and click **Delete All**. A message asking for confirmation appears.
4. Click **Yes** to confirm the deletion.

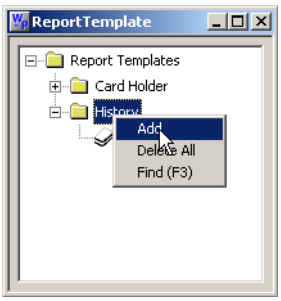
Note: All the card holder report templates are deleted except for the templates that are used in the schedule.

Defining History Report Templates

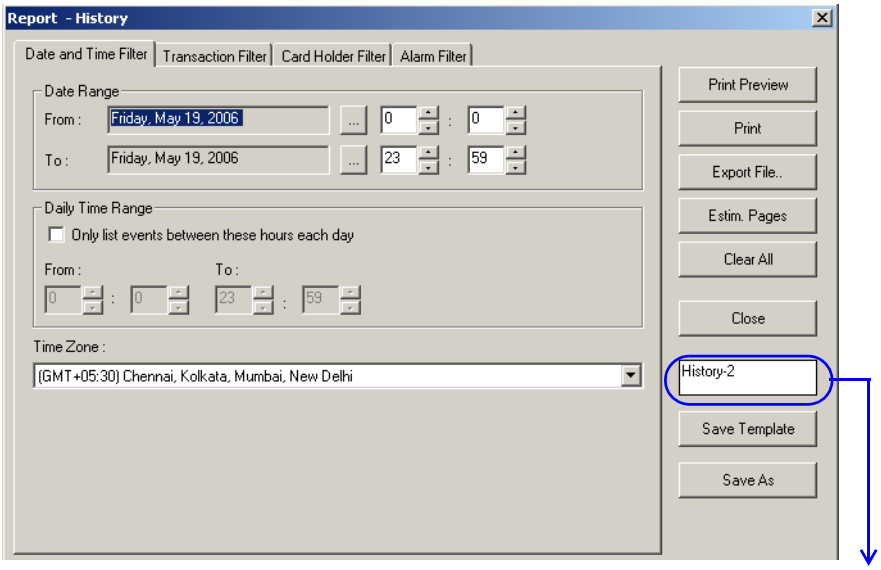
Adding a History Report Template

To define the History report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the Card Holder and History folders.



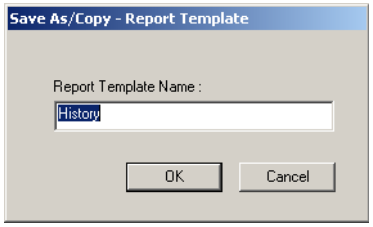
3. Right-click the **History** folder and click **Add**. The **Report - History** dialog box appears.



Name of the History Report template

Refer to the "History Report" section in this chapter for more on defining the filter options for the generating history report.

4. Type the name of the History Report template in the text box on the right.
5. Click **Save** Template to save the template.
6. To create a copy of the template, click **Save As**. The **Save As/Copy - Report Template** dialog box appears.



7. Type a new name for the template and click **OK** to create a copy of template and return to **Report - History** dialog box.
8. Click **Close** to close the dialog box.

Editing a History Report Template

To edit the History Report template:

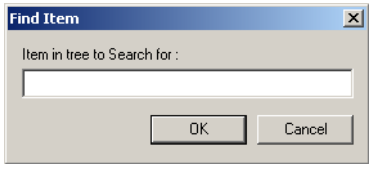
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **History** folder.
3. Right-click the report template and click **Edit**. The **Report - History** dialog box appears.

   Refer to the "Adding a History Report Template" section in this chapter for details on editing the template.

Searching a History Report Template

To search a History Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **History** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.



4. Type the name of the template to be searched and click **OK**. The template starts with the specified name is highlighted.

Deleting a History Report Template

To delete a History Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **History** folder.
3. Right-click the report template and click **Delete**. A message asking for confirmation appears.
4. Click **Yes** to confirm the deletion. The selected report template is deleted.

To delete all the History Report templates:

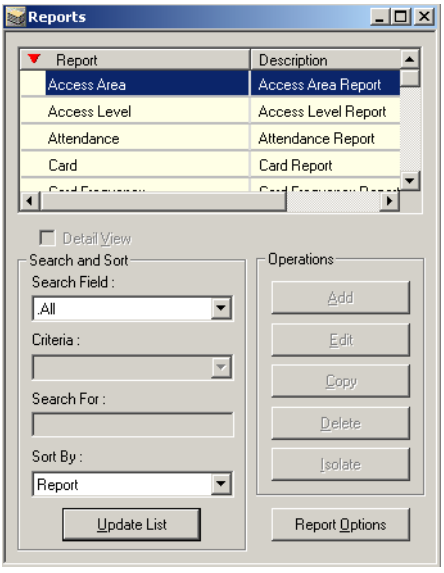
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and
3. Right-click the **History** folder and click **Delete All**. A message asking for confirmation appears.
4. Click **Yes** to confirm the deletion.

Note: All the report templates are deleted except for the templates that are used in the schedule.

Generating and Printing a Report

To generate a report:

1. Choose **Reports > Reports** or click the Reports icon on the toolbar. The **Reports** window appears.



2. To generate a report based on the filtering parameters, select and double-click a report from the list.

   OR

   Select a report from the list and click **Report Options**. The corresponding **Report** dialog box appears.

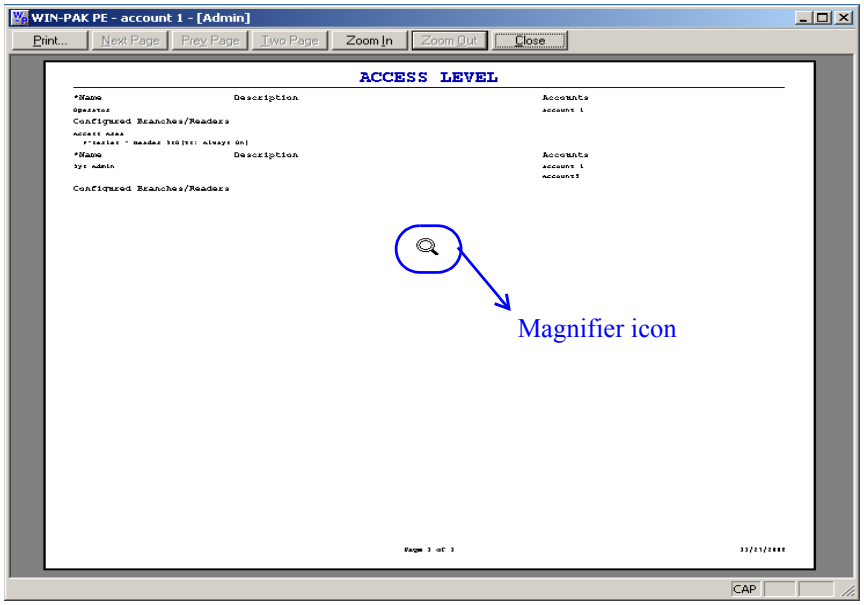
3. Set the filtering parameters for generating the report.

Refer to the corresponding report section in this chapter for setting the filter parameters

Previewing a report

To see the preview of a report, before printing the report:

1. In the **Report** dialog box, click **Print Preview**. The preview of the corresponding report is displayed.



   If you place the cursor on the preview area, the pointer changes to a magnifier icon.

2. To enlarge the preview size:

   a. Click **Zoom In**.

      OR

      Click anywhere on the preview area using the magnifier icon. Ensure that the **Zoom In** button is enabled before clicking.

3. To reduce the preview size,

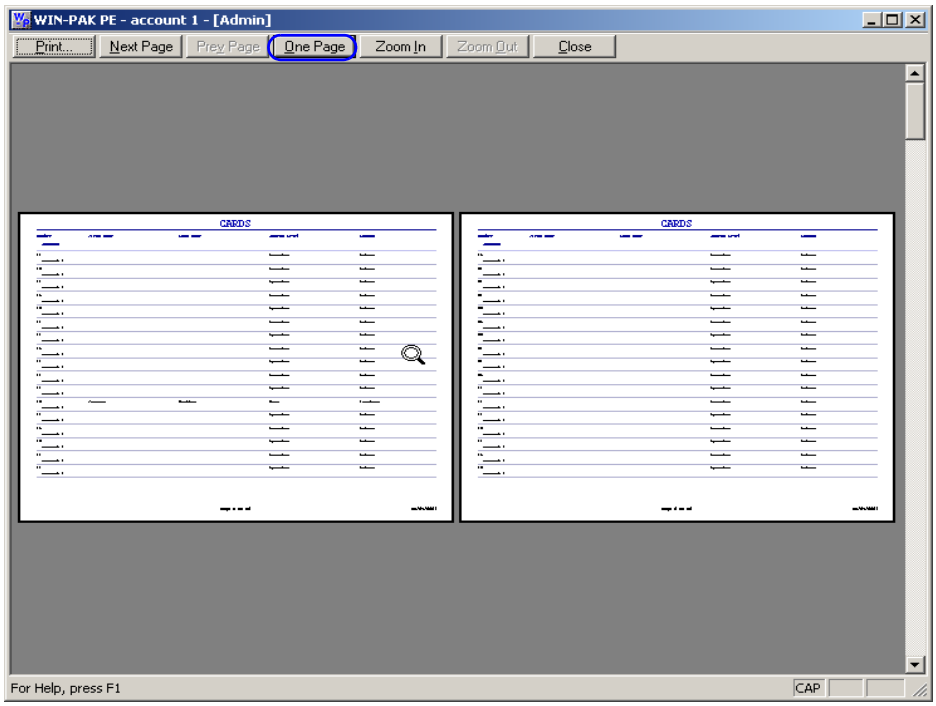
   a. Click **Zoom Out**.

      OR

      Click anywhere on the preview area using the magnifier icon. Ensure that the **Zoom Out** button is enabled before clicking.

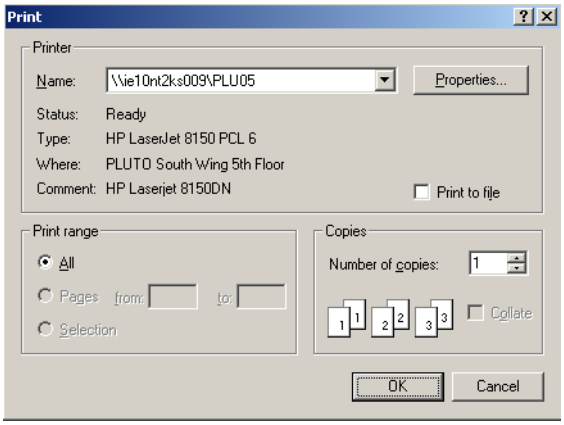
4. If the report runs to more than a page, click **Next Page** or **Prev Page** to move to the next and previous pages of the report.

5. If you want to preview the report on two pages, click **Two Page**.



Note: The **Two Page** button toggles between **Two Page** and **One Page**. If you want to restore the single page display, click **One Page**.

6. To close the preview window and print the report:
   a. Click **Print**. The **Print** dialog box appears.

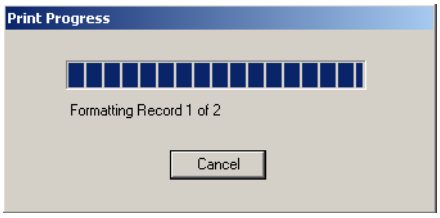


   b. Select the printer in the **Name** list and set the print properties.
   c. Click **OK**. The report is printed to the selected printer.
7. To close the preview window without printing the report, click **Close**.

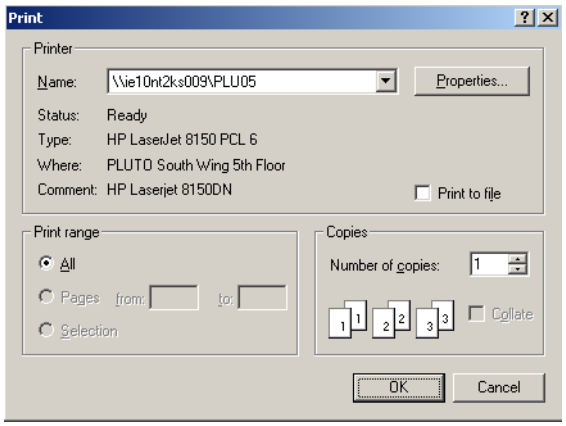
Printing the report

To print the report:

1. Click Print in the **Report** dialog box. The **Print Progress** dialog box appears showing the formatting status.



Then, the **Print** dialog box appears.



2. Select the printer in the **Name** list. The corresponding printer details are displayed.
3. Click **Properties** to set the printer properties.
4. Select the **Print to File** check box to save the report as a file.

Note: The report is saved as **.prn** file in the WIN-PAK installed path with the default name **Output**. However, you can change the path and the file name.

5. Under **Print Range**, select **All** to print all the pages.
6. Click **OK**. The report is printed to the selected printer.

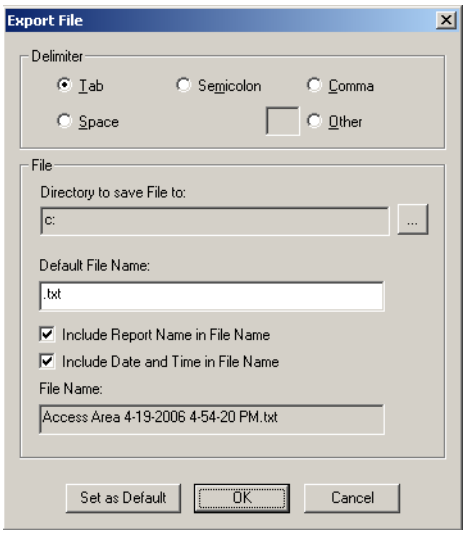
Note: If you have selected the **Print to file** check box, the **Print to File** dialog box appears. Change the path and file name, if required, and click **OK**.

Exporting the report to a file

You can export the reports to a file. The available file formats are .txt and .csv.

To export a report into a file:

1. In the **Report** dialog box, click **Export File**. The **Export File** dialog box appears.



2. Under **Delimiter**, select the separator to separate columns of the report in the report file.

   Tip: If you want to set your own delimiter, click **Other** and type the separator in the provided text box.

3. To set or change the default path of the report file, click the ellipsis button next to **Directory to save File to** and browse through the folder. The selected path is displayed in the **Directory to save File to** box.

4. To set the parameters for the file name:

   a. In **Default File Name**, type the name of the file and the file format. For example, Report.txt.

   b. Select the **Include Report name in File name** check box to include the name of the report in the file name mentioned in the **Default File Name** box.

   c. Select the **Include Date and Time in File name** check box to include the current date and time of the report generation in the file name mentioned in Default File Name.

   After setting these parameters the name of the file is displayed in **File Name**.

   Example: When you generate a card report, if you type **Sample.txt** in Default File Name and select the **Include Report Name in File Name** check box, the name of the file would be **SampleCard.txt**. The name of the report file is Report.txt, if you do not set any of these parameters.

5. To set the default parameters, click **Set as Default**.
6. Click **OK** to export the report to a file at the specified location.

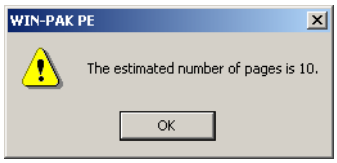
   Tip: To open and view the report file, browse through the specified location and open it.

Estimating the number of pages in the report

To estimate the number of pages in the report:

1. In the **Report** dialog box, click **Estim. Pages**. The **Print Progress** dialog box appears showing the formatting status.

   Then, the message box appears showing the number of estimated pages.



2. Click **OK** to return to the **Report** dialog box.

Clearing the filter options

To clear all the filter options set for generating the report:

1. Click **Clear All**. The user-defined filter options are cleared in the **Report** dialog box.

Note: The sorting options for the report are not cleared.

Reporting from Archive Database

When you restore a backup file, you can either overwrite the information in the current database or you can restore to the Archive Database.

To view the reports from the Archive Database:

1. Select the **Run from Archive Database** check box in the report window. You can view the report from the archived database.

Closing the dialog box

To close the Report dialog box:

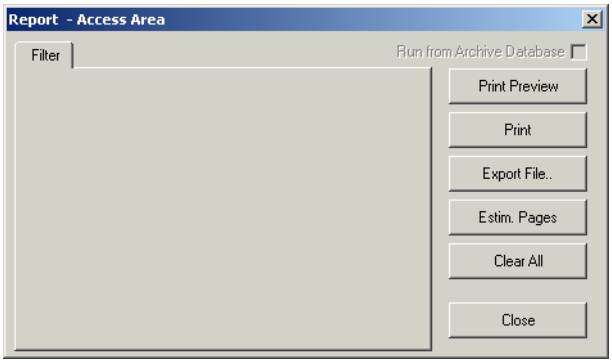
1. Click **Close**. The dialog box is closed.

Access Area Report

The Access Area report displays the branches and entrances or readers that are configured in Access Area.

To generate an access area report:

1. In the **Reports** window, select the **Access Area** report and click **Report Options**. The **Report - Access Area** dialog box appears.



   No filter or sorting options are provided for the access area report.

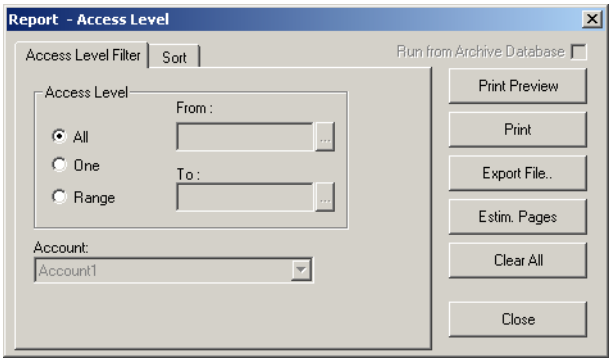
2. Click **Print Preview** to view the Access Area Report prior to printing.
3. Click **Print** to send the report to your printer.
4. Click **Close** to return to the **Reports** window.

Access Level Report

The Access Level report contains the available access levels and the corresponding branches or readers that are configured in Access Level.

To generate the access level report:

1. In the **Reports** window, select the **Access Level** report and click **Report Options**. The **Report - Access Level** dialog box appears.



2. To generate reports for the specific access levels and account:
   a. Click the **Access Level Filter** tab.

b. Under **Access Level**, select one of the following options:

Table 17-1 Describing the filter options for Access Level report

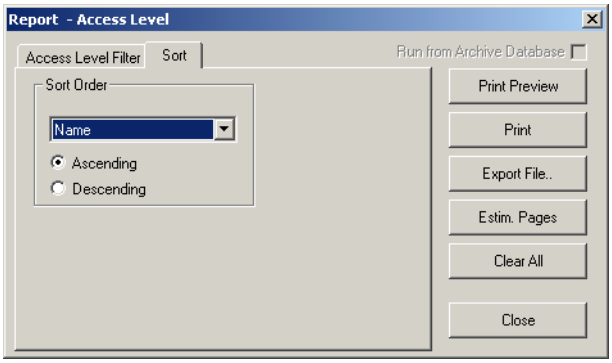
Filter Option	Action
All	Generates the report for all the access levels.
One	Generates the report for only one access level. When you select this option, the **From** field is enabled. Enter the name of the access level to generate the report. You can use the ellipsis button to find the access level.
Range	Generates the report for the range of access levels. When you select this option the **From** and **To** fields are enabled. To specify the range, enter the starting access level name in **From** and the ending access level name in **To**. You can use the ellipsis button to find the access level.

c. Select the **Account** on which the access levels are configured.

Note: By default, the current account is selected. To generate the reports of the access levels configured in all the accounts, select **Available Account**.

3. To sort the report by access level name:

a. In the **Report - Access Level** dialog box, click the **Sort** tab.



b. Under **Sort Order**, select the field (**Name**) by which the list must be sorted. If you select **Not Sorted**, the list is sorted in any order.

c. Click **Ascending** or **Descending** to sort the list in the ascending or descending order.

4. Click **Print Preview** to view the Access Level Report prior to printing.
5. Click **Print** to send the report to your printer.
6. Click **Close** to return to the **Report** window.

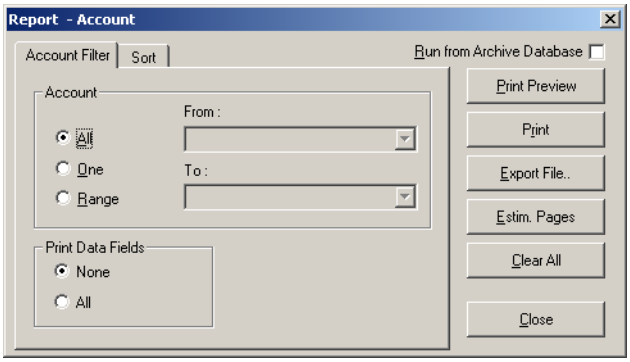
Note: In the report, some access levels are identified by numbers instead of the name. This indicates that these access levels are the custom access levels for the cards.

Account Report

The Account report contains the available accounts that are configured in Account.

To generate the account report:

1. In the **Reports** window, select the **Account** report and click **Report Options**. The **Report - Account** dialog box appears.



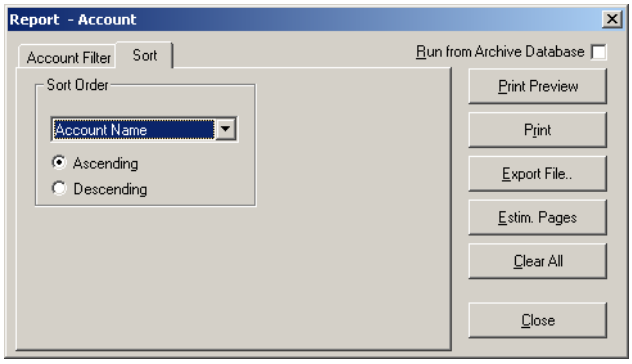
2. To filter the accounts:
   a. Click the **Account Filter** tab.
   b. Under **Accounts**, select one of the following options

Table 17-2 Describing the filter options for Account report

Filter Option	Description
All	Generates the report for all the accounts.
One	Generates the report for a single account. When you select this option, the **From** field is enabled. Enter the name of the account to generate the report. You can use the ellipsis button to find the access level.
Range	Generates the report for the range of accounts. When you select this option, the **From** and **To** fields are enabled. Enter the name of the accounts to generate the report. You can use the ellipsis button to find the access level.

   c. Under **Print Data Fields**, click **None** to exclude the data fields or click **All** to include all the data fields of the account in the report.

3. To sort the account list in the report:
    a. In the **Report - Account** dialog box, click the **Sort** tab.



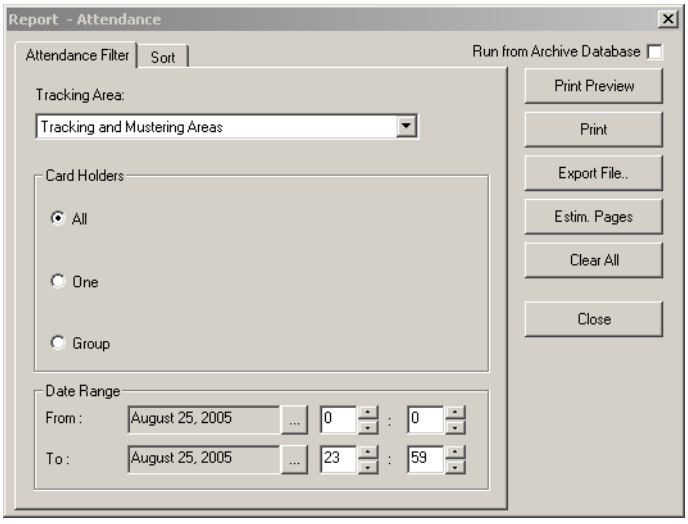
    b. Under **Sort Order**, select the field on which the report must be sorted.
    c. Click **Ascending** or **Descending** to sort the accounts in the ascending or descending order.
4. Click **Print Preview** to view the Account Report prior to printing.
5. Click **Print** to send the report to your printer.
6. Click **Close** to return to the **Reports** window.

Attendance Report

The Attendance Report helps to know the entry and exit details of the card holders who have presented their card in the reader of the tracking area. The Administrator required this report for audit.

To generate the attendance report:

1. In the **Reports** window, select the **Attendance** report and click **Report Options**. The **Report - Attendance** dialog box appears.



2. To filter the tracking area, card holder, and date:

    a. Click the **Attendance Filter** tab.

    b. Select an area in the **Tracking Area** list. The areas or branches configured in Tracking Area are listed.

    Tip: To include all the areas, select **Tracking and Mustering Areas** in the **Tracking** list.

    c. Select one of the following options for filtering the card holders under **Card Holders**:

    Table 17-3 Describing the card holder filter options for Attendance report

Filter Option	Description
All	Generates the report for all the card holders in the specified area.
One	Generates the report for a single card holder. When you select this option, the **Card Number** and **Name** fields are enabled. Enter the card number or name of the card holder to generate the report. You can use the ellipsis button to find the card holder.
Group	Generates the report for a particular group. When you select this option, the **Access Level** and **Note Field** fields are enabled. Enter the access level and select the note field to generate the report. If you select a note field, the text box appears next to it and enables you to enter the value for the note field. You can use the ellipsis button to find the access level.

    d. To filter the report for a specific period, under **Date Range**, click the ellipsis button next to the **From** or **To** fields and select the date in the calendar.

    e. To specify the time range, enter the time in hours and minutes for the From and To fields.

3. To sort the attendance report:

    a. Click the **Sort** tab.

    b. Under **Sort Order 1**, select the field by which the report must be sorted.

    c. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

    d. Under **Sort Order 2**, select the field by which the report must be sorted in the second level.

e. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

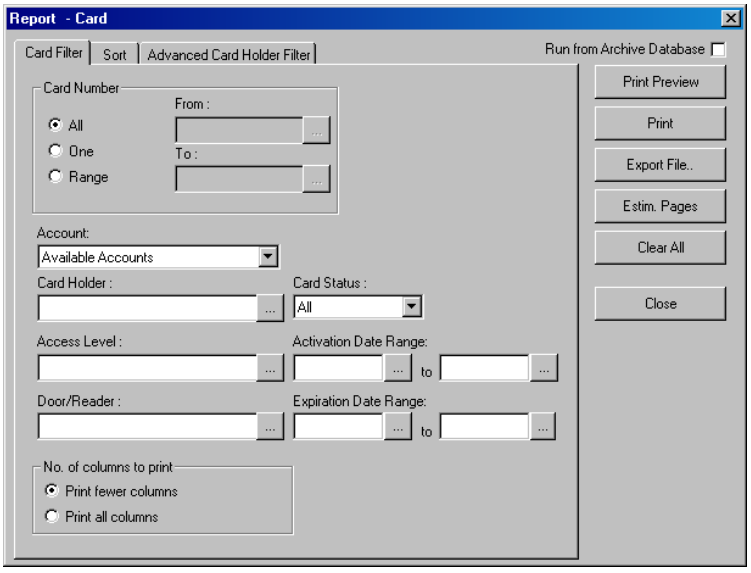
4. Click **Print Preview** to view the report prior to printing it.
5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

Card Report

The Card Report is generated based on the selected account or on the all the accounts that are available for the operator. This report enables you to obtain the details of card holders holding a card, the card status and access level.

To generate the attendance report:

1. In the **Reports** window, select the **Card** report and click **Report Options**. The **Report - Card** dialog box appears.



2. To filter the card details:
   a. Click the **Card Filter** tab.
   b. Select one of the following options for filtering the cards, under **Card Number**:

Table 17-4 Describing the options for filtering the card number

Filter Option	Description
All	Generates a report for all cards.

Table 17-4 Describing the options for filtering the card number

Filter Option	Description
One	Generates a report for a single card. When you select this option, the **From** field is enabled. Enter the card number to generate the report. You can use the ellipsis button to find the card number.
Group	Generates the report for a range of cards. When you select this option, the **From** and **To** fields are enabled. Enter the first card number of the range in **From** and last card number of the range in **To**. You can use the ellipsis button to find the card number.

c. Select any of the following options, to filter the cards further based on the selected option:

- Account
- Card Holder
- Access Level
- Door/Reader
- Card Status
- Activation Date Range
- Expiration Date Range

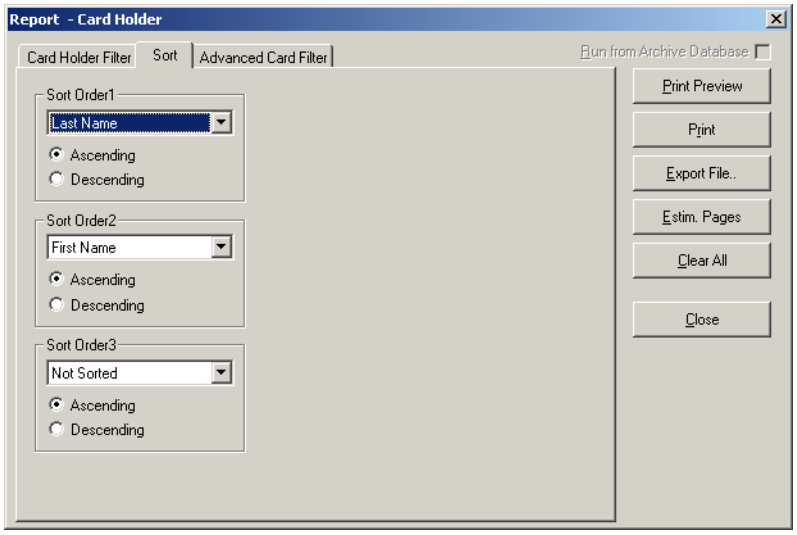
Note: You can use the ellipsis button to search for these options.

d. Under **No. of columns to print**,

- Select **Print fewer columns** if you want the report to contain only basic details of the card such as account, first name, last name, access level, and status.
- Select **Print all columns** if you want the report to contain all the details of the card.

3. To sort the card report:

a. Click the **Sort** tab.



b. Under **Sort Order 1**, select the field by which the report must be sorted in the first level.

c. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

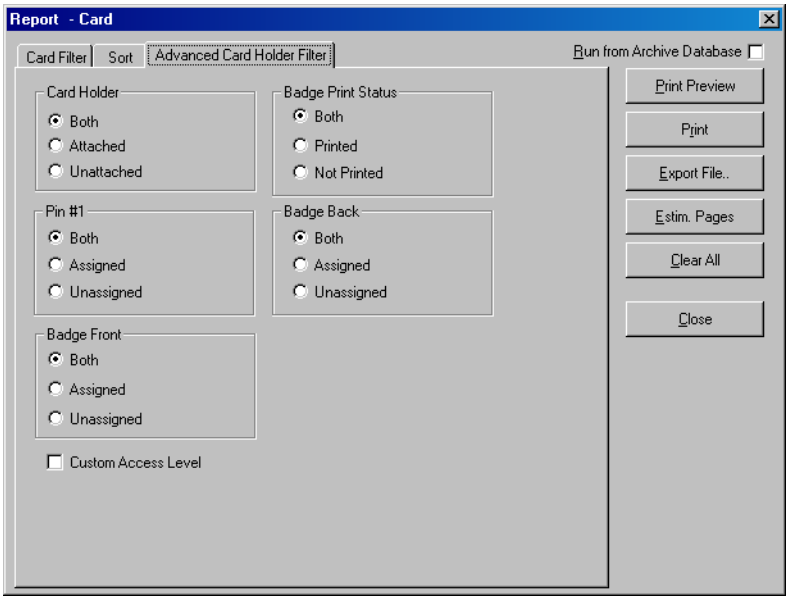
d. Under **Sort Order 2**, select the field by which the report must be sorted in the second level. If you select **Not Sorted** the report is sorted on the basis of the field selected in Sort Order 1.

e. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

f. Under **Sort Order 3**, select the field by which the report must be sorted in the third level. If you select **Not Sorted**, the report is sorted on the basis of the field selected in Sort Order 1 and/or Sort Order 2.

g. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

4. To filter cards based on card holder categories, click the **Advanced Card Holder Filter** tab.



The Card Report is filtered according to the status of:

- **Card Holder** - Attached (to the card), Unattached, or Both.
- **PIN #1** (number) - Assigned (to the card), Unassigned, or Both.
- **Badge Front** and/or **Badge Back** - Assigned (to the card), Unassigned, or Both.
- **Badge Print Status** - Printed, Not Printed, or Both.

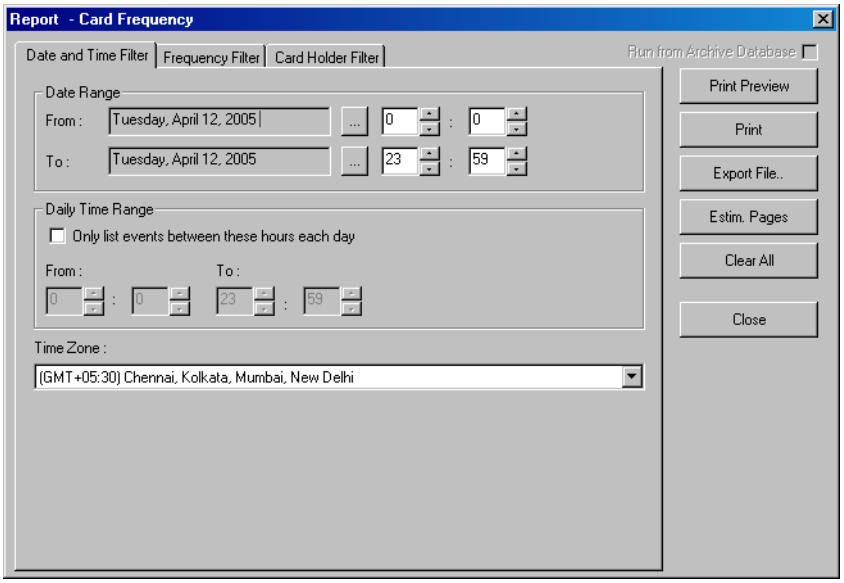
5. Select the **Custom Access Level** check box to include all cards that have custom access levels assigned to them.
6. Click **Print Preview** to view the report prior to printing it.
7. Click **Print** to send a copy of the report to your printer.
8. Click **Close** to return to the **Reports** window.

Card Frequency Report

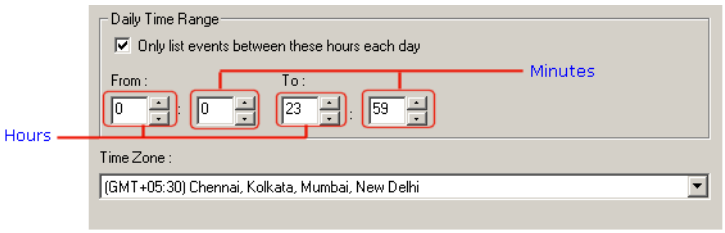
The Card Frequency Report enables you to generate a report to know the number of times a card holder has accessed a particular reader using the card. This report also helps the user to obtain the details of the unused cards and to prevent any misuse of the card.

To generate a card frequency report:

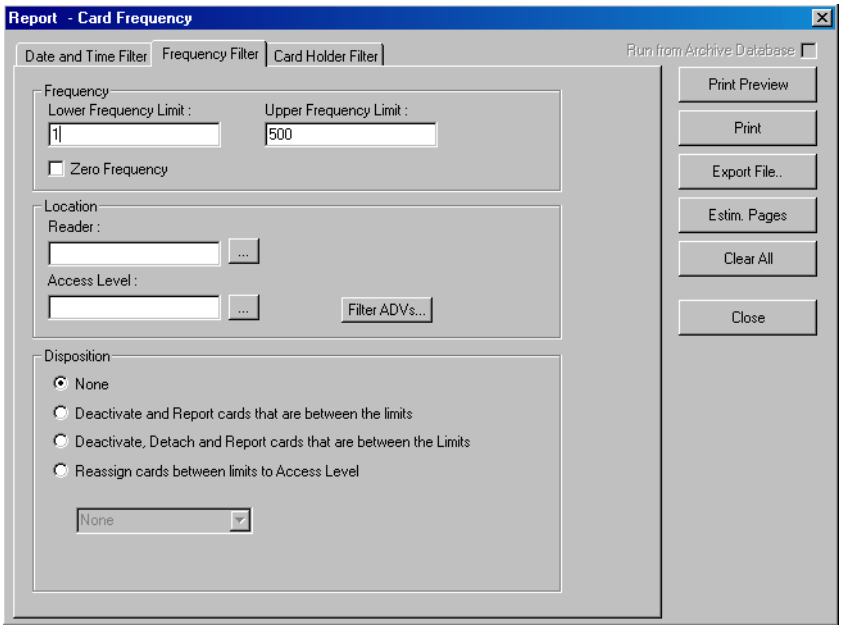
1. In the **Reports** window, select the **Card Frequency** report and click **Report Options**. The **Report - Card Frequency** dialog box appears.



2. To filter the records based on the specific date and time ranges:
    a. Click the **Date and Time Filter** tab.
    b. Under **Date Range**, select the **From** and **To** dates using the ellipsis button.
    c. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.
    d. To generate reports for events that occurred during the specified period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The From and To text boxes are enabled.



    e. In the **From** and **To** boxes, enter the time range (in hours and minutes).
    f. Select the standard time zone in the **Time Zone** list.
3. To set the card frequency limits:
    a. Click the **Frequency Filter** tab.



Note: Frequency Filter is used for finding the reader or the access area in which cards are less-frequently accessed. This helps you to take some action on the particular reader or the access area like unlocking the reader always.

b. Under **Frequency**, type the **Lower Frequency Limit** and **Higher Frequency Limit** to filter cards between these limits.

Note: If you want to generate a report on cards that are not used, select the **Zero Frequency** check box.

c. To generate the card frequency reports by filtering the readers, type the **Reader** name under **Location** or select the reader by clicking the ellipsis [...] button.

d. To generate the frequency filter reports for access areas, type the **Access Area** name under **Location** or select the access area by clicking the ellipsis [...] button.

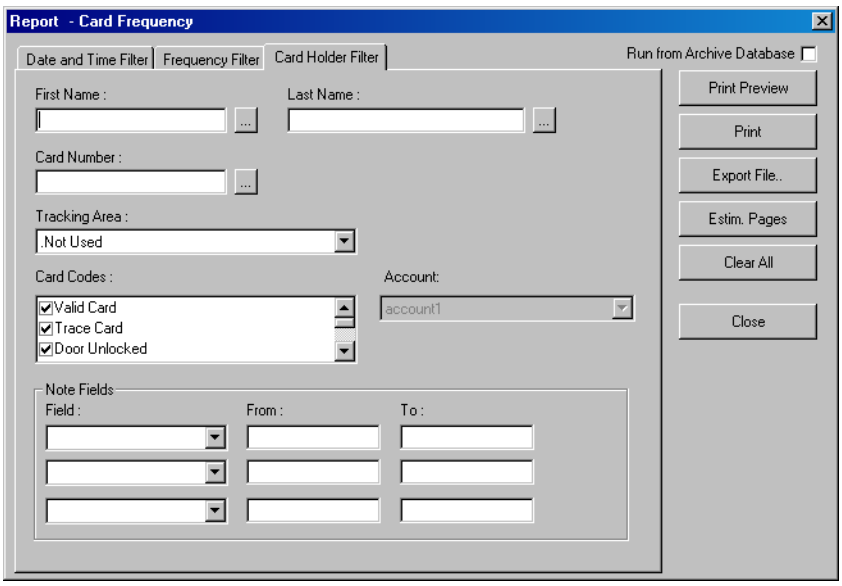
e. To include only certain devices, click **Filter ADVs** to select the ADVs. In the **Filter Devices** dialog box, select the appropriate ADV or ADV type from the tree and click **OK**.

f. Under **Disposition**, select one of the following actions that must be performed on the cards that are filtered for frequency report:

- **None**: Perform no action on the cards.
- **Deactivate and Report cards that are between the limits**: Deactivate and generate a report for the cards whose access frequency falls between the frequency limits.
- **Deactivate, Detach and Report cards that are between the limits**: Deactivate, detach and generate the report for the cards whose access frequency falls between the frequency limits.

- **Reassign cards between limits to Access Level**: Reassign and generate the report for the cards whose access frequency falls between the frequency limits.

4. To generate card frequency report based on the card holders:
   a. Click the **Card Holder Filter** tab.



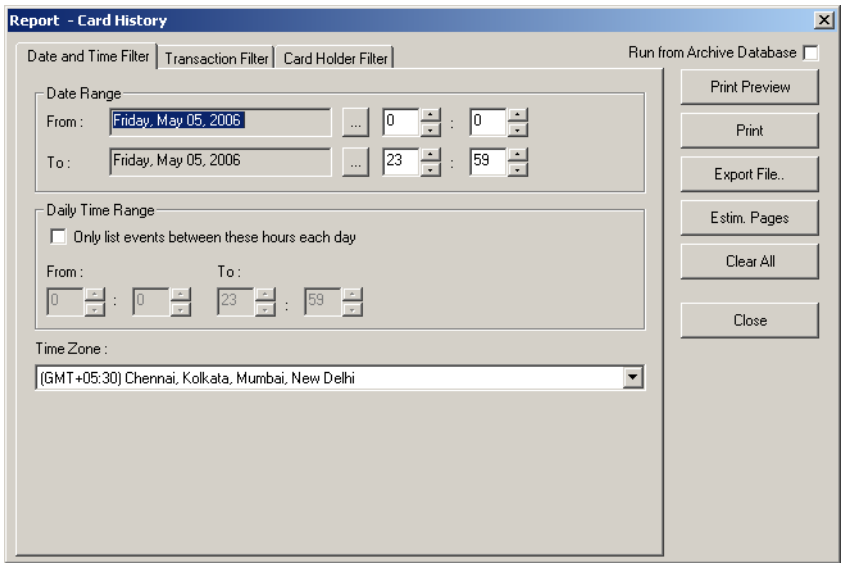
   b. Type the **First Name** and **Last Name** of the card holder, or select them by clicking the ellipsis button.
   c. Type the **Card Number** of the card holder or select it by clicking the ellipsis button.
   d. To generate the card frequency reports of the card holders accessing a specific area, select an area in the **Tracking Area** list that are configured in Tracking and Mustering Area.
   e. Select one or more **Card Codes** which define the card transaction.
   f. Select the **Note Fields** to be displayed in the report. You can also specify the range if you select the numerical note field.
5. Click **Print Preview** to view the report prior to printing.
6. Click **Print** to print the card frequency report.
7. Click **Close** to return to the Reports window.

Card History Report

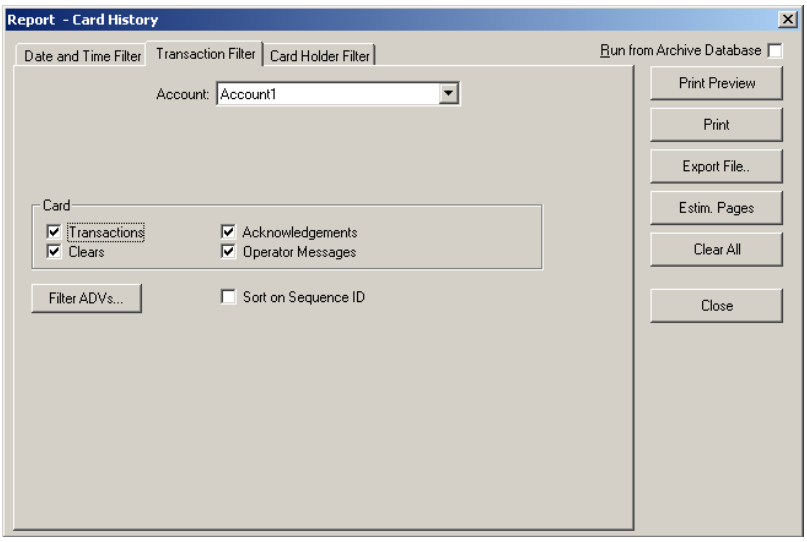
The Card History report contains the history of card transactions and events.

To generate a card history report:

1. In the **Reports** window, select the **Card History** report and click **Report Options**. The **Report - Card History** dialog box appears.



2. To filter records based on the specific date and time ranges:
    a. Click the **Date and Time Filter** tab.
    b. Under **Date Range**, select the **From** and **To** dates using the ellipsis button.
    c. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.
    d. To generate reports for events occurring during a particular period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The From and To text boxes are enabled.
    e. In the **From** and **To** boxes, enter the time range (in hours and minutes).
    f. Select the standard time zone in the **Time Zone** list.
3. To filter the report based on the type of card events:
    a. Click the **Transaction Filter** tab.



b. Select an account in the **Account** list.

c. To filter the report based on the card behaviors, select the following options, under **Card**:

Table 17-5 Describing the card options for filtering card events

Card Option	Description
Transactions	Reports card events of all transactions such as normal, alarm, or host grant.
Clears	Reports the card alarm events that were cleared by the operator.
Acknowledgements	Reports the card alarm events that were acknowledged by the operator.
Operator Messages	Reports the card alarm events that were provided with an operator message.

d. To filter the transactions performed on specific ADVs (devices), click **Filter ADVs**. The **Filter Devices** dialog box appears.

e. Double-click the branch (folder) to select a all the devices in the branch.

OR

Expand the branch and double-click a device to select the particular device of the branch.

f. Click **OK** to return to the **Report - History** dialog box.

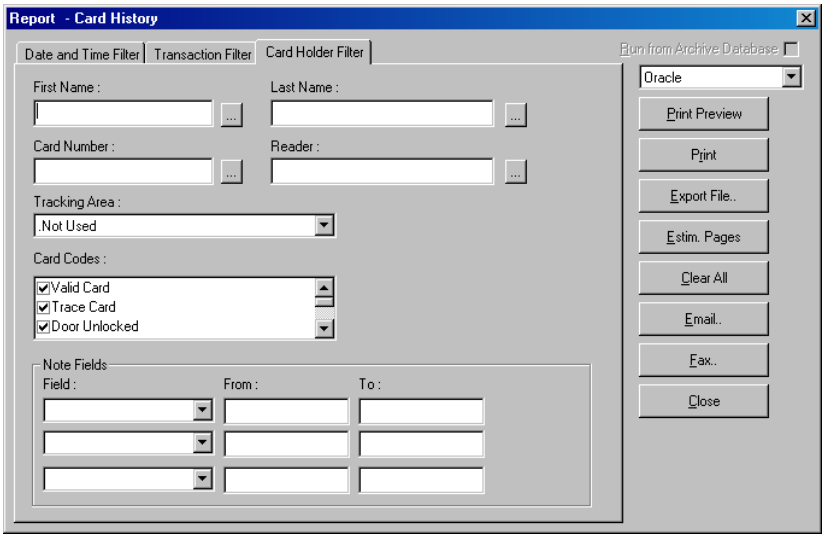
g. Click the **Sort on Sequence ID** check box to sort the report by the sequence number of each action.

When a new event is identified, it is given a sequence ID and any change in the event carries a new sequence ID.

When a report is sorted by the Sequence ID, the events of the specific ID are grouped together in a chronological order. This makes it easier to view relative to other system-wide events.

4. To filter card events based on the card holders:
   a. Click the **Card Holder Filter** tab.

Caution: Do not select too many options for selection criteria, as it may result in not finding records meeting the selected criteria.



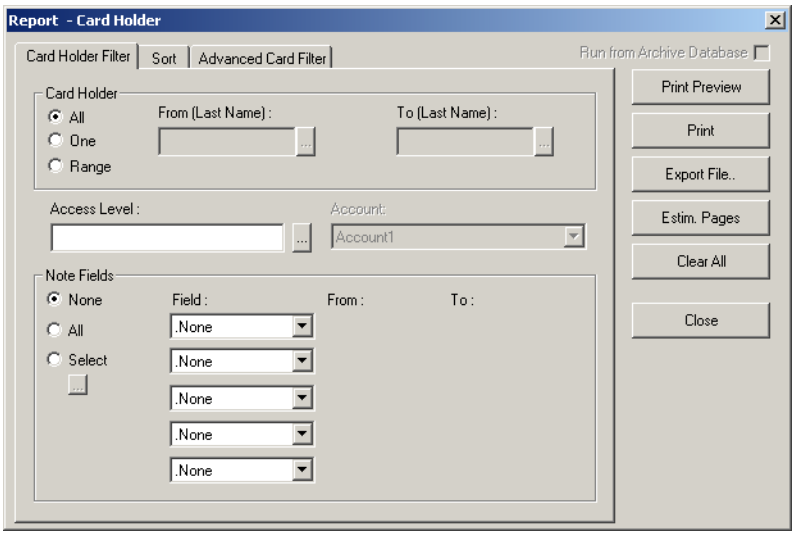
   b. Type the **First Name** and **Last Name** of the card holder, or select them by clicking the ellipsis button.
   c. Type the **Card Number** of the card holder or select it by clicking the ellipsis button.
   d. To generate the card history reports of the card holders accessing a specific area, select an area in the **Tracking Area** list that are configured in Tracking and Mustering Area.
   e. Select one or more **Card Codes** which define the card transaction.
   f. Select the **Note Fields** to be displayed in the report. You can also specify the range if you select the numerical note field.
5. Click **Print Preview** to view the report prior to printing.
6. Click **Print** to print the card history report.
7. Click **Close** to return to the **Reports** window.

Card Holder Report

The Card Holder report displays the list of card holder details.

To generate a card holder report:

1. In the **Reports** window, select the **Card History** report and click **Report Options**. The **Report - Card Holder** dialog box appears.



2. To filter the card holders based on card holder name, access level:
   a. Click the **Card Holder Filter** tab.
   b. Under **Card Holder**, select the following options to filter card holders based on last name:

Table 17-6 Describing the options for filtering card holders

Option	Description
All	Generates the report that includes all the card holders.
One	Generates the report for a single card holder detail. When you select this option, the **First (Last Name)** is enabled. Enter the last name of the card holder in **First (Last Name)** to generate a report for this card holder.
Range	Generates the report for a range of card holders. When you select this option, the **First (Last Name)** and **Last (Last Name)** are enabled. To specify the range, enter the starting last name of the card holder in **First (Last Name)** and ending last name in the **Last (Last Name)**.

   c. To filter the report based on the card holders' access level, select it in the **Access Level** list.

d. To filter the report based on the card holders' account, select it in the **Account** list. To include all the accounts, select **Available Accounts**.

e. To include the note fields in the report, select the following options under **Note Fields**.

Table 17-7 Describing the options for filtering note fields

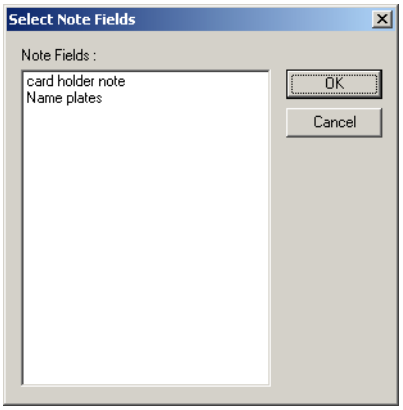
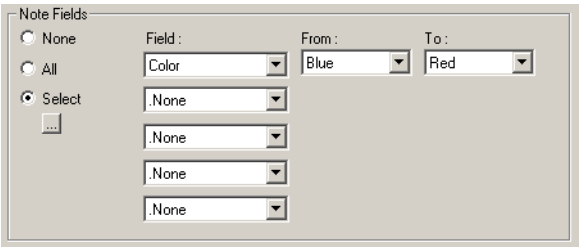
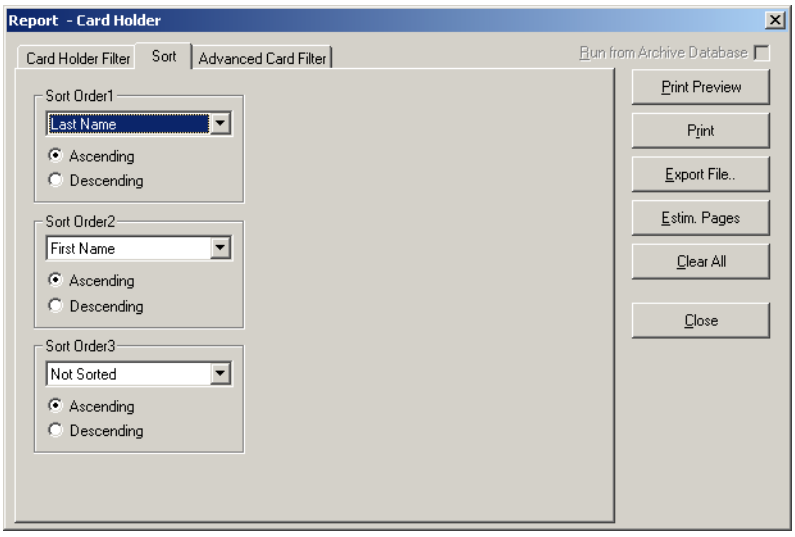
Option	Description
None	To include NO note fields in the report.
All	To include all the note fields in the report.
Select	To select a specific note field that must be included in the report. When you select this option, the ellipsis button beneath the **Select** option is enabled. 1. Click the ellipsis button to display the **Select Note Fields** dialog box.  2. Select the note fields that must be included in the report. 3. Click **OK** to return to the Report - Card Holder dialog box.

Table 17-7 Describing the options for filtering note fields

Option	Description
Field	To filter the note fields information that must be displayed in the report. The number of drop-down lists depend on the number of available note fields. When you select a note field, the **From** and **To** fields are enabled.  1. Enter the corresponding information in the **From** and **To** fields. These fields are case-sensitive, if the note field template is defined for a note field. **Example:** If you select **Color** in **Field** and you select **Blue** in **From** and **Red** in **To**, the card holder details that contain **Blue** through **Red** colors are included in the report.

3. To sort the report in the ascending or descending order of a specific field:
   a. Click the **Sort** tab.



   b. Under **Sort Order 1**, select the field by which the report must be sorted in the first level.
   c. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

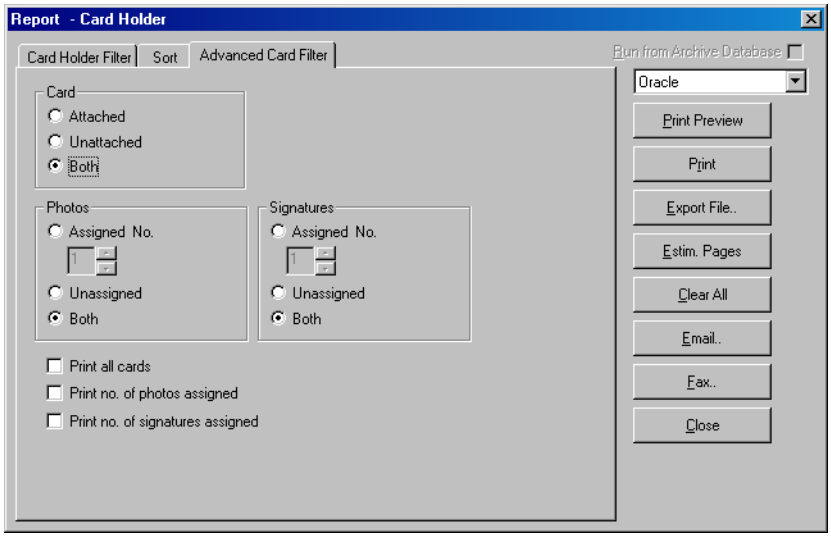
d. Under **Sort Order 2**, select the field by which the report must be sorted in the second level. If you select **Not Sorted** the report is sorted on the basis of the field selected in Sort Order 1.

e. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

f. Under **Sort Order 3**, select the field by which the report must be sorted in the third level. If you select **Not Sorted** the report is sorted based on the field selected in Sort Order 1 and/or Sort Order 2.

g. Click **Ascending** or **Descending** to sort the list in the ascending or descending order of the selected field.

4. To filter the cards based on the card details, click the **Advanced Card Filter** tab.



The Card Holder report is filtered according to the status of:

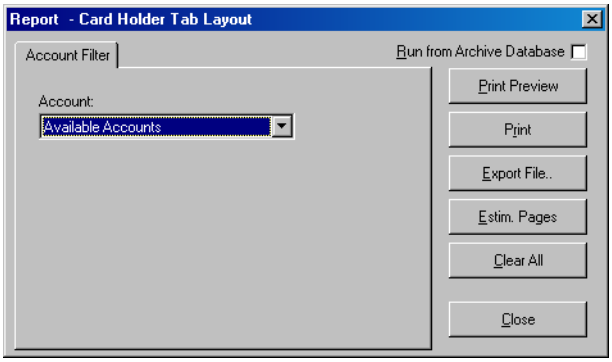
- **Card** - Attached (to the card holder), Unattached, or Both.
- Number of **Photos** or **Signatures** - Assigned (to the card), Unassigned, or Both.

5. Select the following check boxes to set global parameters for information to be included in the report:
   - **Print all cards** (assigned to the card holder)
   - **Print no. of photos assigned**
   - **Print no.of signatures assigned**
6. Click **Print Preview** to view the report prior to printing it.
7. Click **Print** to send a copy of the report to your printer.
8. Click **Close** to return to the **Reports** window.

Card Holder Tab Layout Report

To generate the card holder tab layout report:

1. In the **Reports** window, select the **Card Holder Tab Layout** report and click **Report Options**. The **Report - Card Holder Tab Layout** dialog box appears.



2. To filter the card holder tab layout by an account, select it in the **Account** list. If you want to include card holder tab layouts of all the account, select **Available Accounts** in the **Account** list.

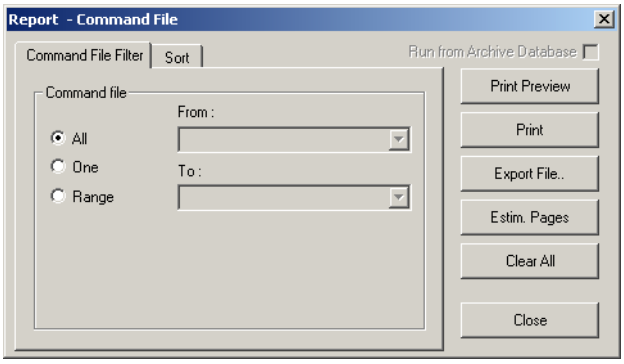
Note: The Card Holder Tab Layout report shows the "Note Fields" associated with each Tab on the Card Holder Layout.

3. Click **Print Preview** to view the report prior to printing it.
4. Click **Print** to send a copy of the report to your printer.
5. Click **Close** to return to the **Reports** window.

Command File Report

To generate a command file report:

1. In the **Reports** window, select the **Command File** report and click **Report Options**. The **Report - Command File** dialog box appears.



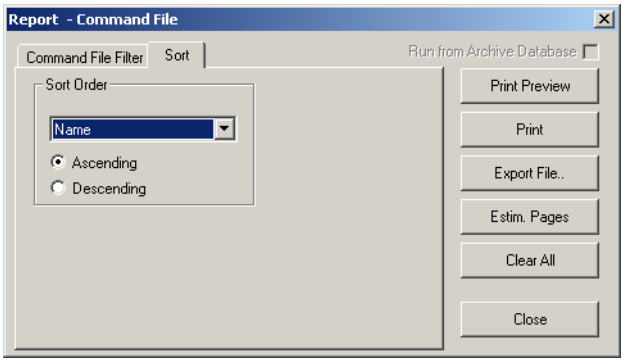
2. To filter command files to be included in the report,
   a. Click the **Command File Filter** tab.

b. Under **Command File**, select one of the following options:

Table 17-8 Describing the options for filtering card holders

Option	Description
All	Generates the report that includes all the command files.
One	Generates the report for a single command file. When you select this option, the **From** field is enabled. Enter the name of the command file to generate the report. You can use the ellipsis button to find the access level.
Range	Generates the report for the range of command files. When you select this option, the **From** and **To** fields are enabled. To specify the range, enter the starting command file name in **From** and the ending command file name in **To**. You can use the ellipsis button to find the command files.

3. To sort the list in the report in the ascending or descending order:
   a. Click the **Sort** tab.



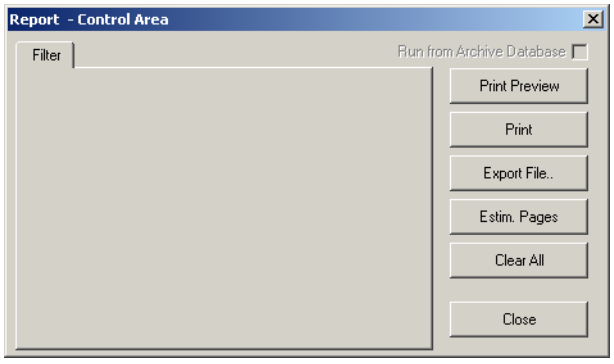
   b. Under **Sort Order**, select the field by which the list in the report must be sorted.
   c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.
4. Click **Print Preview** to view the report prior to printing it.
5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

Control Area Report

The Control Area report displays the branches or devices that are configured in Control Area.

To generate a control area report:

1. In the **Reports** window, select the **Control Area** report and click **Report Options**. The **Report - Control Area** dialog box appears.



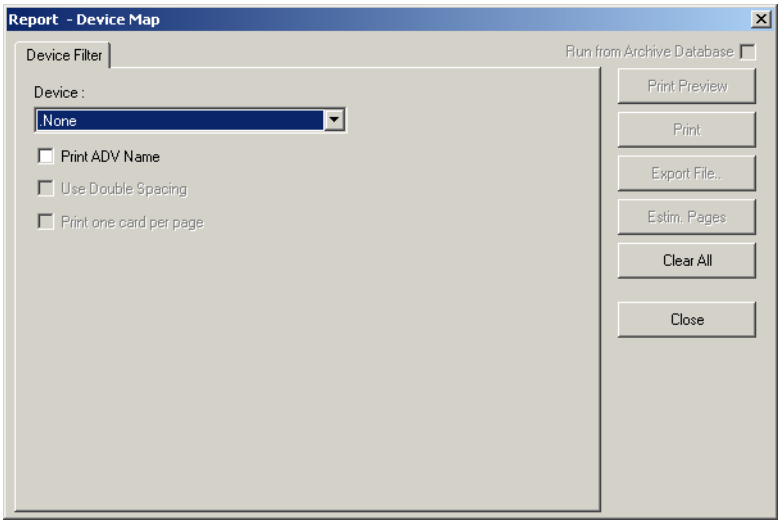
   No filter or sort options are provided for the control area report.

2. Click **Print Preview** to view the Access Area Report prior to printing.
3. Click **Print** to send the report to your printer.
4. Click **Close** to return to the **Reports** window.

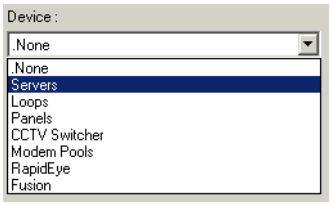
Device Map Report

To generate a device map report:

1. In the **Reports** window, select the **Device Map** report and click **Report Options**. The **Report - Device Map** dialog box appears.



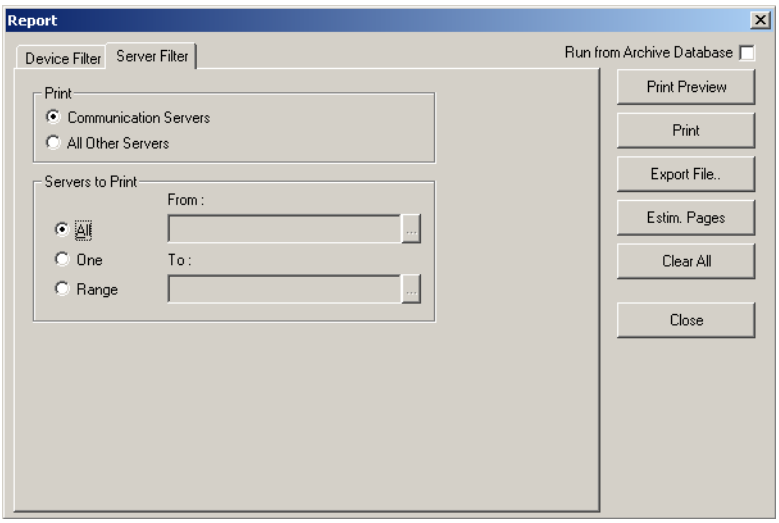
2. Under **Device Filter**, select the **Print ADV Name** check box to include the abstract device names in the report.
3. To filter the devices to be included in the report, select a device in the **Device** list.



A corresponding tab with additional filter options is added to the dialog box.

Servers:

– The **Device Map Report** can include communication servers or all other servers. You are also provided with an option to display all or a range of servers.



– To select the type of server:

a. Click the **Server Filter** tab. It is displayed by default when you select the device as **Servers**.

b. Under **Print**, select the type of server; **Communication Servers** or **All Other Servers**.

– To select the range of servers:

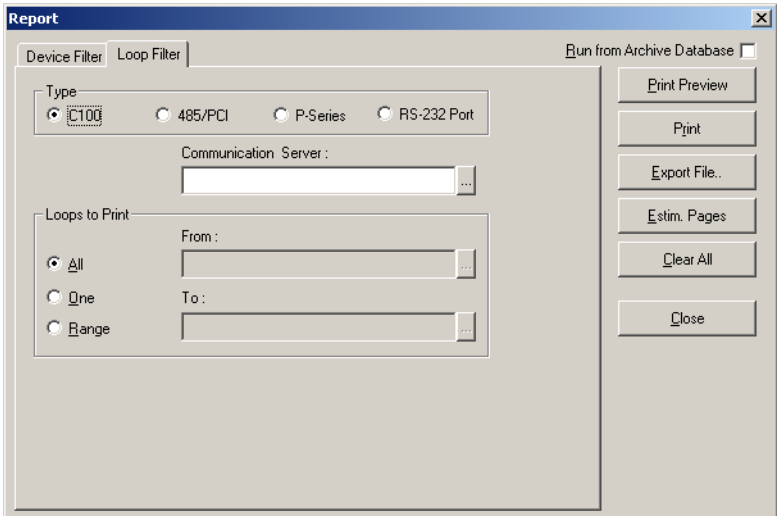
a. Under **Servers to Print**, select one of the following options:

- **All** - to include all the servers
- **One** - to include a single server that you select in the **From** field.
- **Range** - to include a range of servers that you select in the **From** and **To** fields.

- You can use the ellipsis button to select a server.

Loops

– The **Device Map Report** displays the details of a single loop like C-100, 485/PCI of all or the selected communication server. You are also provided with an option to display the details of all or a range of loops.



– To select the type of loop:

a. Click the **Loop Filter** tab. It is displayed by default when you select the device as **Loops**.

b. Under **Type**, select the type of loop; **C100, 485/PCI, P-Series** or **RS-232 Port**.

c. Enter the name of the **Communication Server** to include only the loops that are available in the selected communication server. You can use the ellipsis button to select the communication server.

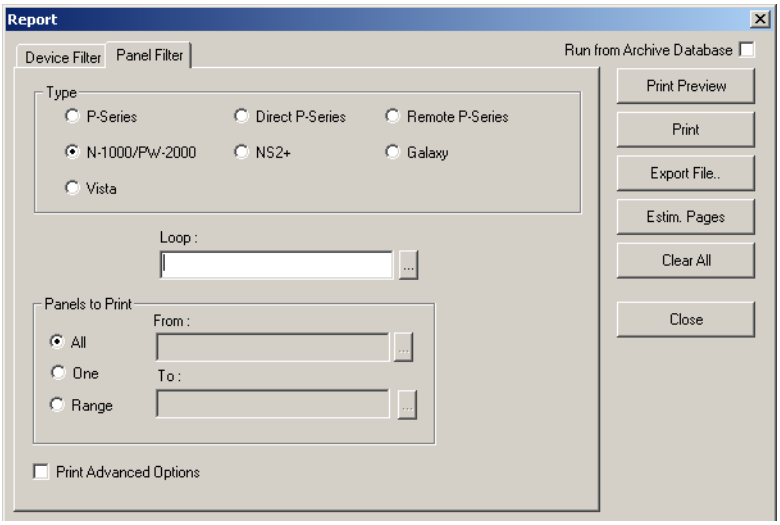
– To select the range of loops:

a. Under **Loops to Print**, select one of the following options:

- **All** - to include all the loops.
- **One** - to include a single loop that you select in the **From** field.
- **Range** - to include a range of loops that you select in the **From** and **To** fields.
- You can use the ellipsis button to select a loop.

Panels

– The **Device Map Report** can display the details of a single panel like P-Series, NS2+ of all or the selected loop. You are also provided with an option to display the details of all or a range of loops.



– To select the type of loop:

  a. Click the **Panel Filter** tab. It is displayed by default when you select the device as **Panels**.

  b. Under **Type**, select the type of panel; **P-Series, Direct P-Series, Remote P-Series, N-1000/PW-2000, NS2+** or **Galaxy**.

  c. Enter the name of the **Loop** to include the panel of this loop. You can use the ellipsis button to select the communication server.

Note:

* The Loop option is disabled, if the Galaxy, Vista, or Direct P-Series panel type is selected.
* The Loop option changes to Modem Pool, if the Remote P-Series panel type is selected.

– To select the range of panels:

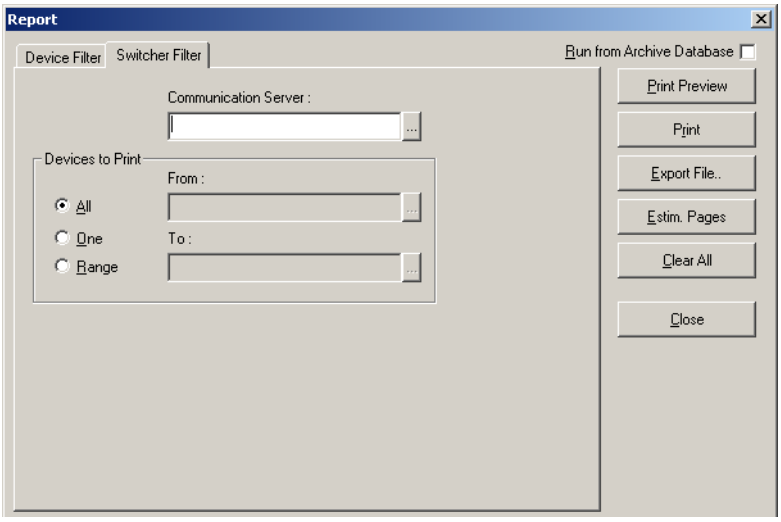
  a. Under **Panels to Print**, select one of the following options:

  - **All** - to include all the panels.
  - **One** - to include a single panel that you select in the **From** field.
  - **Range** - to include a range of panels that you select in the **From** and **To** fields.
  - You can use ellipsis button to select a loop.

– To include the advanced option details of a panel, select the **Print Advanced Options**. This option is enabled only for the N-1000/PW-2000 panel type.

CCTV Switcher

– The **Device Map Report** can display the details of a CCTV Switcher of all or the selected communication server. You are also provided with an option to display the details of all or a range of CCTV switchers.



– To select the communication server:

  a. Enter the name of the **Communication Server** to include the CCTV Switcher of this loop. You can use the ellipsis button to select the communication server.

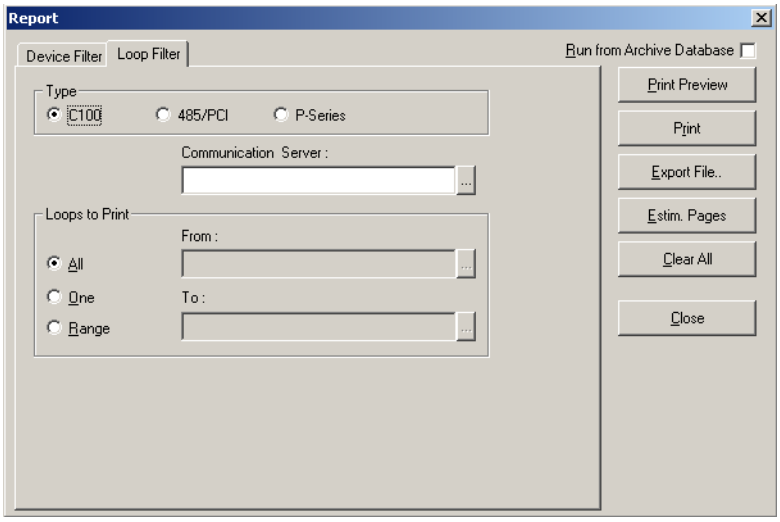
– To select the range of switchers:

  a. Under **Devices to Print**, select one of the following options:

  - **All** - to include all the CCTV switchers.
  - **One** - to include a single CCTV switcher that you select in the **From** field.
  - **Range** - to include a range of CCTV switchers that you select in the **From** and **To** fields.
  - You can use ellipsis button to select a loop.

Modem Pool

– The **Device Map Report** can display the details of a single loop like C-100, 485/PCI of all or the selected communication server in the modem pool. You are also provided with an option to display the details of all or a range of loops.



– To select the type of loop:

  a. Click the **Loop Filter** tab. It is displayed by default when you select the device as **Modem Pools**.

  b. Under **Type**, select the type of loop; **C100, 485/PCI,** or **P-Series**.

  c. Enter the name of the **Communication Server** to include the loop of this server. You can use the ellipsis button to select the communication server.

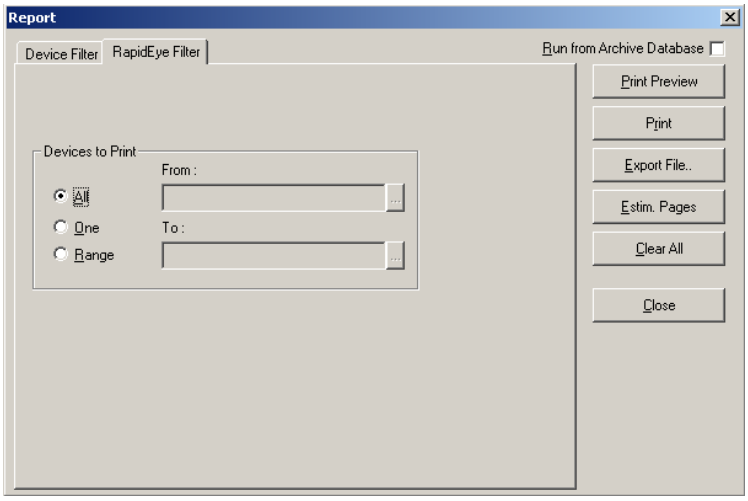
– To select the range of loops:

  a. Under **Loops to Print**, select one of the following options:

  - **All** - to include all the loops.
  - **One** - to include a single loop that you select in the **From** field.
  - **Range** - to include a range of loops that you select in the **From** and **To** fields.
  - You can use the ellipsis button to select a loop.

RapidEye

– The **Device Map Report** can display the details all or a range of access DVPROs.



– To select the range of access DVPROs:

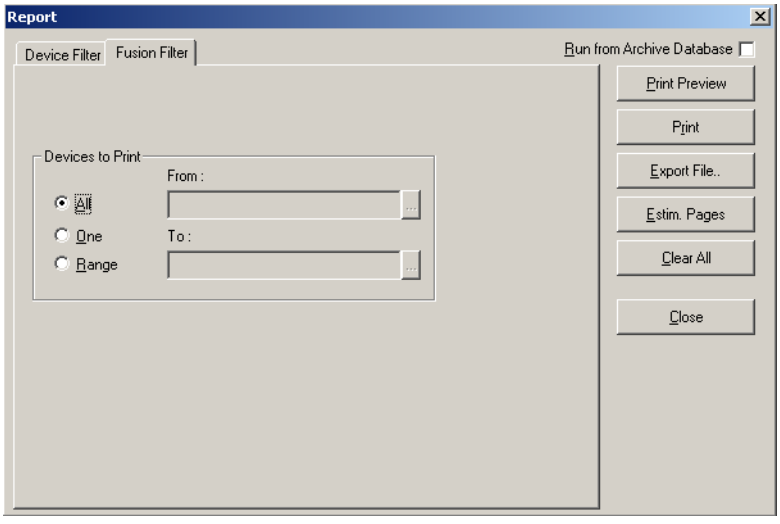
  a. Click the **RapidEye Filter** tab. It is displayed by default when you select the device as **RapidEye**.

  b. Under **Devices to Print**, select one of the following options:

  - **All** - to include all the access DVPRO servers.
  - **One** - to include a single access DVPRO server that you select in the **From** field.
  - **Range** - to include a range of access DVPRO servers that you select in the **From** and **To** fields.
  - You can use the ellipsis button to select an access DVPRO server.

Fusion

– The **Device Map Report** can display the details all or a range of Fusion DVR devices.



– To select the range of Fusion DVR servers:

a. Click the **Fusion Filter** tab. It is displayed by default when you select the device as **Fusion**.

b. Under **Devices to Print**, select one of the following options:

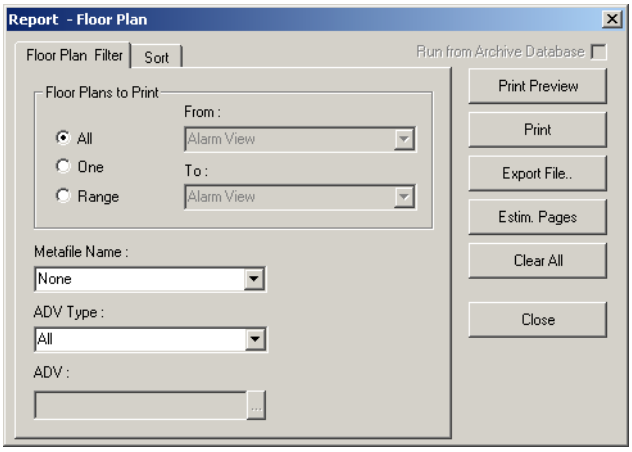
- **All** - to include all the Fusion DVR servers.
- **One** - to include a single Fusion DVR server that you select in the **From** field.
- **Range** - to include a range of Fusion DVR servers that you select in the **From** and **To** fields.
- You can use the ellipsis button to select a loop.

4. Click **Print Preview** to view the report prior to printing it.
5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

Floor Plan Report

To generate a floor plan report:

1. In the **Reports** window, select the **Floor Plan** report and click **Report Options**. The **Report - Floor Plan** dialog box appears.



2. To filter floor plans to be included in the report,

a. Click the **Floor Plan Filter** tab.

b. Select one of the following options under **Floor Plans to Print**:

Table 17-9 Describing the options for filtering floor plans

Option	Description
All	Generates the report that includes all the floor plans.

Table 17-9 Describing the options for filtering floor plans

Option	Description
One	Generates the report for a single floor plan. When you select this option, the **From** field is enabled. Enter the name of the floor plan to generate the report. You can use the ellipsis button to find the floor plan.
Range	Generates the report for the range of floor plans. When you select this option, the **From** and **To** fields are enabled. To specify the range, enter the starting floor plan name in **From** and the ending floor plan in **To**. You can use the ellipsis button to find the floor plan.

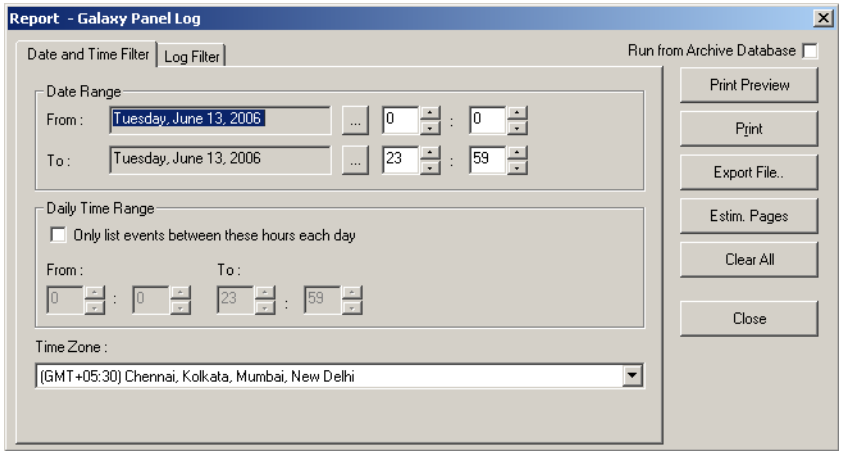
3. To filter floor plans based on metafiles, select the **Metafile Name** in the list.
4. To filter a specific ADV, select an **ADV Type** in the list and enter the name of the **ADV**. Use the ellipsis button to find an ADV.
5. To sort the list in the report in the ascending or descending order:
    a. Click the **Sort** tab.
    b. Under **Sort Order**, select the field by which the list in the report must be sorted.
    c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.
6. Click **Print Preview** to view the report prior to printing it.
7. Click **Print** to send a copy of the report to your printer.
8. Click **Close** to return to the **Reports** window.

Galaxy Panel Log Report

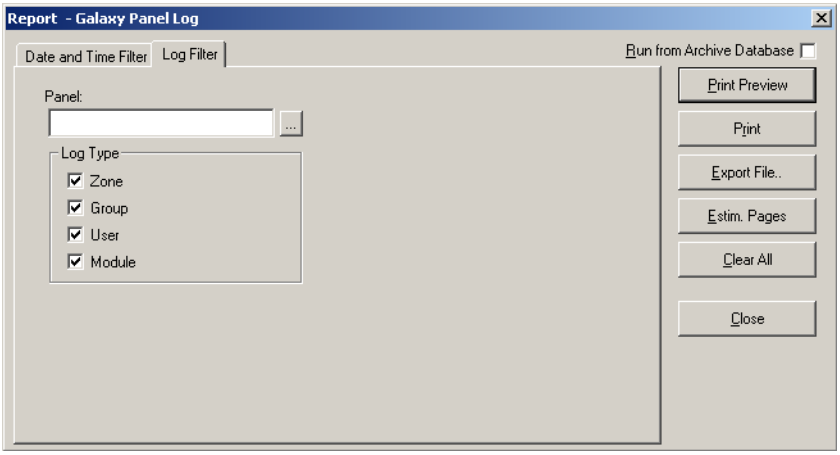
Galaxy Panel Log report is used for tracking the events happening at the Galaxy panel. This report can be generated if you procured license for the Galaxy feature in WIN-PAK.

To generate a Galaxy Panel Log report:

1. In the **Reports** window, select the **Galaxy Panel Log** report and click **Report Options**. The **Report - Galaxy Panel Log** dialog box appears.



2. To filter date and time of the log events to be included in the report:
    a. Click the **Date and Time Filter** tab.
    b. Under **Date Range**, select the **From** and **To** dates using the ellipsis button.
    c. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.
    d. To generate reports for messages sent and received during a particular period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The **From** and **To** text boxes are enabled.
    e. In the **From** and **To** boxes, enter the time range (in hours and minutes).
    f. Select the standard time zone in the **Time Zone** list.
3. To filter log type of the log events to be included in the report:
    a. Click the **Log Filter** tab.



    b. Click the ellipsis button next to **Panel** to open **Select** dialog box.
    c. Search for the panel and click **OK**.

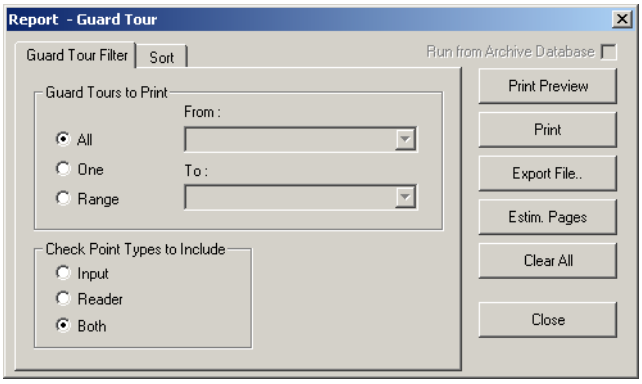
d. Under **Log Type**, select the log types such as Zone, Group, User, or Module.

4. Click **Print Preview** to view the report prior to printing it.
5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

Guard Tour Report

To generate a guard tour report:

1. In the **Reports** window, select the **Floor Plan** report and click **Report Options**. The **Report - Guard Tour** dialog box appears.



2. To filter guard tours that must be included in the report,
   a. Click the **Guard Tour Filter** tab.
   b. Under **Guard Tours to Print**, select one of the following options:

Table 17-10 Describing the options for filtering guard tours

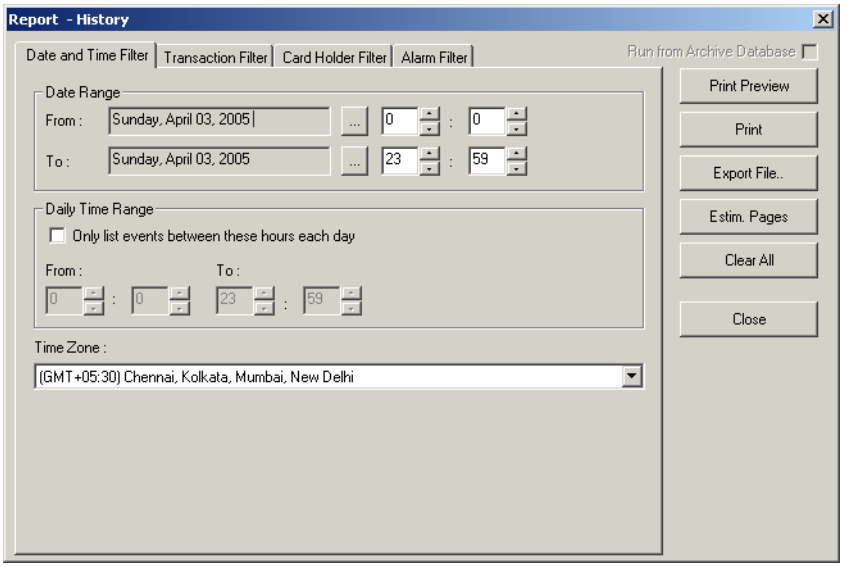
Option	Description
All	Generates the report that includes all the guard tours.
One	Generates the report for a single guard tour. When you select this option, the **From** field is enabled. Enter the name of the guard tour to generate the report. You can use the ellipsis button to find a guard tour.
Range	Generates the report for the range of guard tours. When you select this option, the **From** and **To** fields are enabled. To specify the range, enter the starting guard tour name in **From** and the ending guard tour in **To**. You can use the ellipsis button to find a guard tour.

3. To filter the check point types, select one of the **Check Point Type to Include** options.
4. To sort the list in the report in the ascending or descending order:
    a. Click the **Sort** tab.
    b. Under **Sort Order**, select the field by which the list in the report must be sorted.
    c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.
5. Click **Print Preview** to view the report prior to printing it.
6. Click **Print** to send a copy of the report to your printer.
7. Click **Close** to return to the **Reports** window.

History Report

To generate a history report:

1. In the **Reports** window, select the **History** report and click **Report Options**. The **Report - History** dialog box appears.



2. To filter the records based on the specific date and time ranges:
    a. Click the **Date and Time Filter** tab.
    b. Under **Date Range**, select the **From** and **To** dates using the ellipsis button.
    c. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.

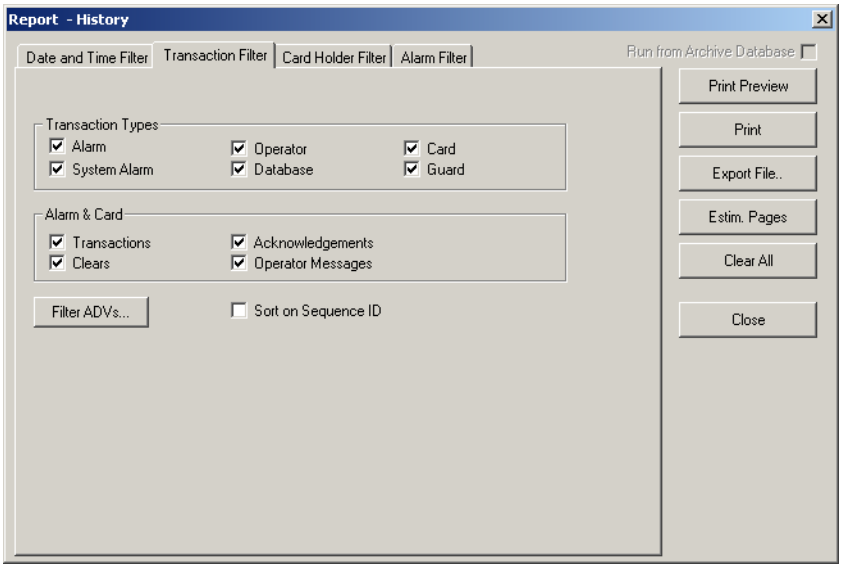
d. To generate reports for events occurring during a particular period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The From and To text boxes are enabled.

e. In the **From** and **To** boxes, enter the time range (in hours and minutes).

f. Select the standard time zone in the **Time Zone** list.

3. To filter the report based on the type of card events:

a. Click the **Transaction Filter** tab.



b. To filter the report based on the transaction types, select the following options, under **Transaction Types**:

Table 17-11 Describing the transaction types for filtering history details

Card Option	Description
Alarm	Reports transactions of type alarms.
System Alarm	Reports system type alarms (not wired points) such as Poll Response alarms.
Operator	Reports operator activities, such as log on and log off.
Database	Reports basic database activities, such as update, delete or add action to a particular database.
Card	Reports all card events.
Guard	Reports all guard tour events.

c. To filter the options based on the alarm and card behaviors, select the following options, under **Alarm & Card**:

Table 17-12 Describing the Alarm & Card options for filtering history details

Card Option	Description
Transactions	Reports card events of all transactions such as normal, alarm, or host grant.
Clears	Reports the card alarm events that were cleared by the operator.
Acknowledgements	Reports the card alarm events that were acknowledged by the operator.
Operator Messages	Reports the card alarm events that were provided with an operator message.

d. To filter the transactions performed on specific ADVs (devices), click **Filter ADVs**. The **Filter Devices** dialog box appears.

e. To select a device, expand the corresponding folder and double-click a device.

Note: The devices of the Galaxy panel and/or Vista panel are also displayed, if you have procured the license for the Galaxy panel and/or Vista panel features in WIN-PAK.

f. To select all the devices in a folder:

- Double-click the corresponding folder. The **Set Device Selection for a Control Area** dialog box appears.
- Click an appropriate option and click **OK**. The dialog box is closed.

g. After selecting the required devices, click **OK** in the **Filter Devices** dialog box to return to the **Report - History** dialog box.

h. Click the **Sort on Sequence ID** check box, if you want the report to be sorted by the sequence number given to each action in the data base.

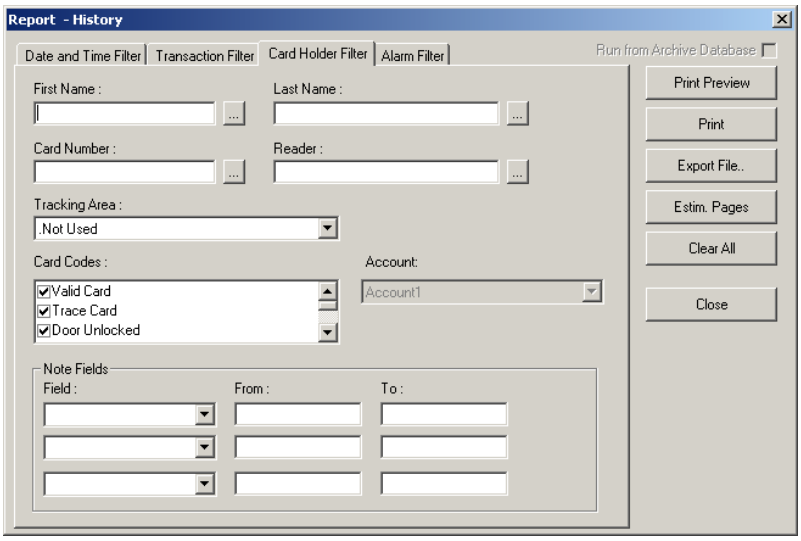
When a new event is identified, it is given a sequence ID and any change carries a new sequence ID.

When a report is sorted by the Sequence ID, the ID number groups the events together in chronological order. This makes it easier to view information relative to other system-wide events.

4. To filter the card events based on the card holders:

a. Click the **Card Holder Filter** tab.

Caution: Do not select too many options for the selection criteria, as it may result in not finding records meeting the selected criteria.



b. Type the **First Name** and **Last Name** of the card holder, or select them by clicking the ellipsis button.

c. Type the **Card Number** of the card holder or select it by clicking the ellipsis button.

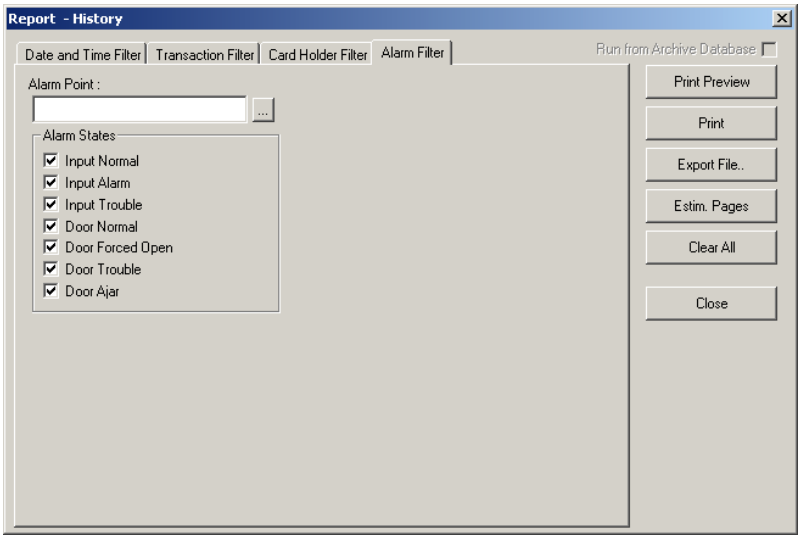
d. To generate the card history reports of the card holders accessing a specific area, select an area in the **Tracking Area** list that are configured in Tracking and Mustering Area.

e. Select one or more **Card Codes** which define the card transaction.

f. Select the **Note Fields** to be displayed in the report. You can also specify the range if you select the numerical note field.

5. To filter further on alarm events:

   a. Click the **Alarm Filter** tab.



b. In the **Alarm Point** text box, enter the device or point name. You can also use the ellipsis [...] button to find the device or point on which the alarms to be viewed.

c. Select the **Alarm States** that must be included in the report.

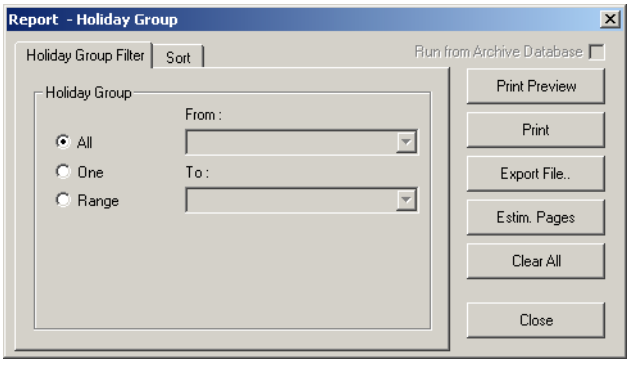
Note: The options in **Alarm Filter** tab are enabled, only if you have selected **Alarms** transaction type in the **Transaction Filter** tab.

6. Click **Print Preview** to view the report prior to printing.
7. Click **Print** to print the card history report.
8. Click **Close** to return to the **Reports** window.

Holiday Group Report

To generate a holiday group report:

1. In the **Reports** window, select the **Holiday Group** report and click **Report Options**. The **Report - Holiday Group** dialog box appears.



2. To filter the holiday groups to be included in the report,

a. Click the **Holiday Group Filter** tab.

b. Under **Holiday Group**, select one of the following options:

Table 17-13 Describing the options for filtering holiday groups

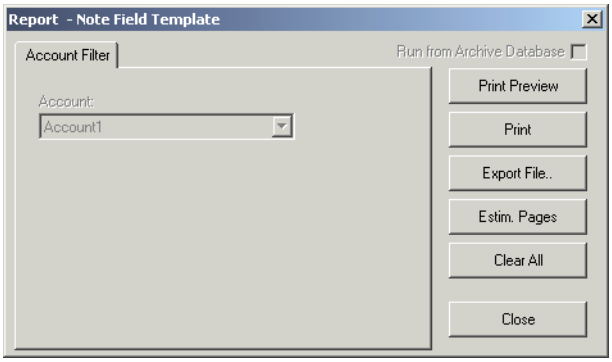
Option	Description
All	Generates the report that includes all the holiday groups.
One	Generates the report for a single holiday group. When you select this option, the **From** field is enabled. Enter the name of the holiday group to generate the report. You can use the ellipsis button to find the holiday group.
Range	Generates the report for the range of holiday groups. When you select this option, the **From** and **To** fields are enabled. To specify the range, enter the starting holiday group name in **From** and the ending holiday group in **To**. You can use the ellipsis button to find the holiday group.

3. To sort the list in the report in the ascending or descending order:
   a. Click the **Sort** tab.
   b. Under **Sort Order**, select the field by which the list in the report must be sorted.
   c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.
4. Click **Print Preview** to view the report prior to printing it.
5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

Note Field Template Report

To generate an access area report:

1. In the **Reports** window, select the **Access Area** report and click **Report Options**. The **Report - Note Field Template** dialog box appears.

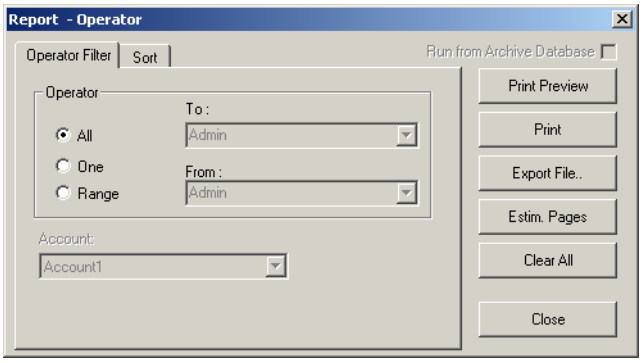


2. To filter the note field templates based on an account, select an **Account** under Account Filter.
3. Click **Print Preview** to view the report prior to printing.
4. Click **Print** to send the report to your printer.
5. Click **Close** to return to the **Reports** window.

Operator Report

To generate a report on operators:

1. In the **Reports** window, select the **Operator** report and click **Report Options**. The **Report - Operator** dialog box appears.



2. To filter the operators to be included in the report,
   a. Click the **Operator Filter** tab.
   b. Under **Operator**, select one of the following options:

Table 17-14 Describing the options for filtering operators

Option	Description
All	Generates the report that includes all the operators.
One	Generates the report for a single operator. When you select this option, the **From** field is enabled. Enter the name of the operator to generate the report. You can use the ellipsis button to find an operator.
Range	Generates the report for the range of operators. When you select this option, the **From** and **To** fields are enabled. To specify the range, enter the first operator name in **From** and the last operator name in **To**. You can use the ellipsis button to find an operator.

3. To sort the list in the report in the ascending or descending order:
   a. Click the **Sort** tab.

b. Under **Sort Order**, select the field by which the list in the report must be sorted.

c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.

4. Click **Print Preview** to view the report prior to printing it.
5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

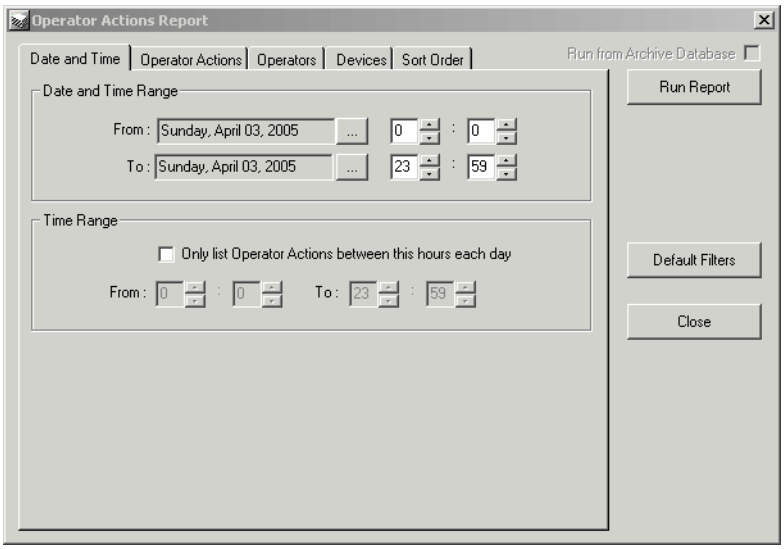
Operator Actions Report

The Operator Actions report is an Audit Report for the Administrator to monitor the actions performed by the operator using WIN-PAK User Interface. This report can be generated based on the operator levels, devices, and operator actions.

To generate an operator actions report:

1. In the **Reports** window, select the **Operator Actions** report and click **Report Options**. The **Operator Actions Report** dialog box appears.
2. To filter the operator actions based on the date and time range:

a. Click the **Date and Time** tab.



b. Under **Date and Time Range**, select the **From** and **To** dates using the ellipsis [...] button.

c. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.

d. To generate reports for actions occurring during the specified period, select the **Only list operator actions between this hours each day** check box, under **Time Range**. The From and To text boxes are enabled.

e. In the **From** and **To** boxes, enter the time range (in hours and minutes).

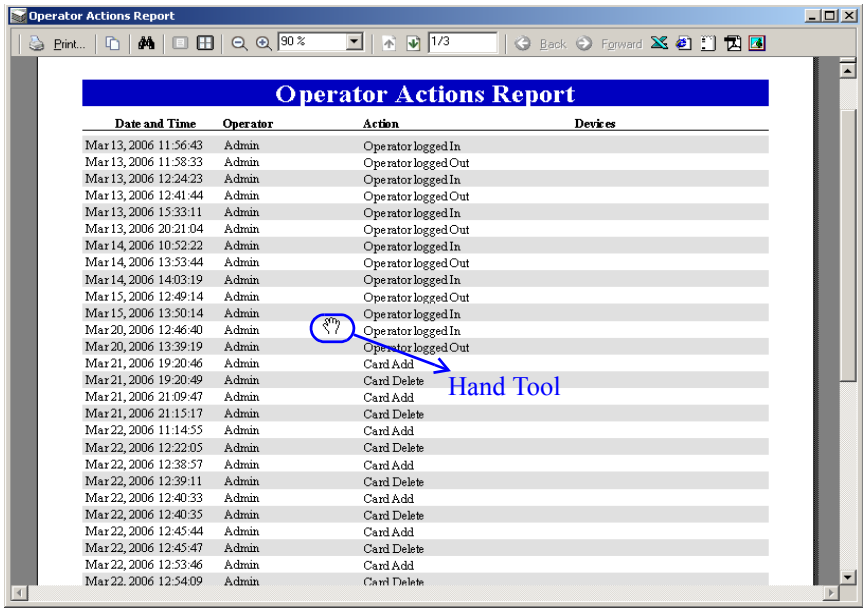
3. To filter only the specific operator actions:
   a. Click the **Operator Actions** tab.
   b. Under **Operator Actions**, select or clear the operator actions to be included or excluded. By default all the actions are selected.

      Tip: Click **Select All** to select all the actions or click **Deselect All** to clear all the actions.
4. To filter the list of operators to monitor their actions:
   a. Click the **Operators** tab.
   b. Under **Operators**, select or clear the operators to be included or excluded. By default all the operators are selected.

      Tip: Click **Select All** to select all the operators or click **Deselect All** to clear all the operators.
5. To filter the devices on which the actions are performed:
   a. Click the **Devices** tab.
   b. Under **Devices**, select or clear the devices to be included or excluded. By default all the devices are selected.

      Tip: Click **Select All** to select all the devices or click **Deselect All** to clear all the devices.
6. To sort the report based on report columns:
   a. Click the **Sort Order** tab.
   b. Under **Sort Field**, in **First Sort**, select the field in the list by which the report must be sorted.
   c. In the adjacent list, select the sort order; **Ascending** or **Descending**.
   d. Repeat steps b and c for defining **Second Sort**, **Third Sort** and **Fourth Sort**.

      Note: To define the $n+1^{th}$ sort, you must have defined n^{th} sort. For example, to define Third Sort, you must have defined Second Sort.
7. To set the default filter criteria, click **Default Filters.**
8. Click **Run Report** to generate the report. The **Operator Actions Report** window is displayed in a separate window.



Toolbar buttons on the report

You can perform additional operations on this report using the toolbar available on the top of the Operator Actions Report window.

The following image illustrates the toolbar buttons:

Table 17-15 Defining toolbar buttons

Toolbar button	Description
Print	Sends the report to the printer.
Copy	Copies the content of the report and it can be pasted in any of the text applications like Word, Excel, Notepad.
Find	Searches for a particular text in the report. When you click this button, the **Find** dialog box appears. Enter the text and click **Find Next**.
Single Page	Changes the view of the report to a single page. This button is enabled, only when you view the report in multiple pages.
Multiple Pages	Changes the view of the report to multiple pages. To view multiple pages, click and select the number of pages in the drop-down list box.
Zoom Out	Reduces the size of the page display. This button is disabled, when the page size is less than or equal to the window size.

Table 17-15 Defining toolbar buttons

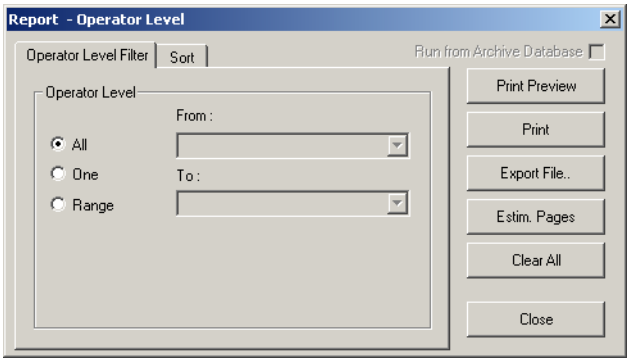
Toolbar button	Description
Zoom In	Enlarges the size of the page display.
Zoom	Reduces or enlarges the size of the page display based on the selected percentage.
Previous Page	Displays the previous page of the report. This button is disabled, if you are in the first page.
Next Page	Displays the next page of the report. This button is enabled, if you are in the last page.
Page No./Total no. of pages	Displays the "page number of the current page/total number of pages". To move to the desired page, type the page number in the text box and press ENTER.
Move Backward	Displays the previously viewed page. Note that it is not the previous page.
Move Forward	Functions reverse to the Move Backward button.
Export Buttons	
Excel	Exports the report to the excel sheet.
HTML	Exports the report to the html page.
ASCII Text	Exports the report to the text file.
PDF	Exports the report to the PDF file.
TIFF	Exports the report to the image file in TIFF format.
Note: When you click the Export button, **Save Report to**... dialog box appears. Browse through the desired folder, change the file name and click **Save**. By default the file is saved in **My Documents** folder with the name **Operator Action Report**.	

9. Click **Close** to close **Operator Actions Report dialog** box.

Operator Level Report

To generate a report on operator levels:

1. In the **Reports** window, select the **Operator Levels** report and click **Report Options**. The **Report - Operator Level** dialog box appears.



2. To filter the operator levels to be included in the report:
   a. Click the **Operator Level Filter** tab.
   b. Under **Operator Level**, select one of the following options:

Table 17-16 Describing the options for filtering operator levels

Option	Description
All	Generates the report that includes all the operator levels.
One	Generates the report for a single operator level. When you select this option, the **From** field is enabled. Enter the name of the operator level to generate the report. You can use the ellipsis button to find an operator level.
Range	Generates the report for the range of operator levels. When you select this option, the **From** and **To** fields are enabled. To specify the range, enter the first operator level name in **From** and the last operator level name in **To**. You can use the ellipsis button to find an operator level.

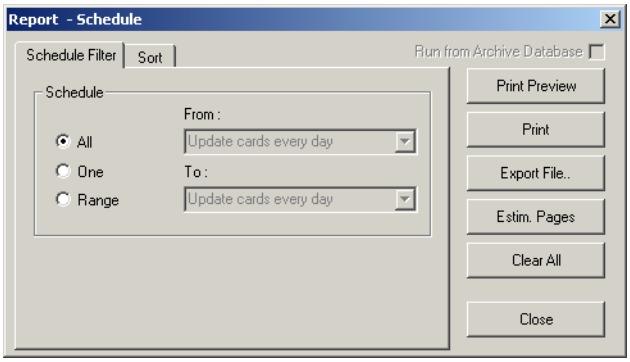
3. To sort the list in the report in the ascending or descending order:
   a. Click the **Sort** tab.
   b. Under **Sort Order**, select the field by which the list in the report must be sorted.
   c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.
4. Click **Print Preview** to view the report prior to printing it.

5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

Schedule Report

To generate a schedule report:

1. In the **Reports** window, select the **Schedule** report and click **Report Options**. The **Report - Schedule** dialog box appears.



2. To filter the schedules to be included in the report,
   a. Click the **Schedule Filter** tab.
   b. Under **Schedule**, select one of the following options:

Table 17-17 Describing the options for filtering schedules

Option	Description
All	Generates the report that includes all the schedules.
One	Generates the report for a single schedule. When you select this option, the **From** field is enabled. Enter the name of the schedule to generate the report. You can use the ellipsis button to find a schedule.
Range	Generates the report for the range of schedules. When you select this option, the **From** and **To** fields are enabled. To specify the range, enter the first schedule name in **From** and the last schedule name in **To**. You can use the ellipsis button to find a schedule.

3. To sort the list in the report in the ascending or descending order:
   a. Click the **Sort** tab.
   b. Under **Sort Order**, select the field by which the list in the report must be sorted.

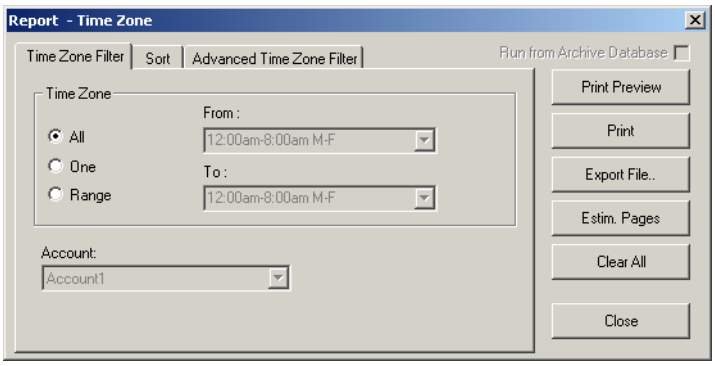
c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.

4. Click **Print Preview** to view the report prior to printing it.
5. Click **Print** to send a copy of the report to your printer.
6. Click **Close** to return to the **Reports** window.

Time Zone Report

To generate a time zone report:

1. In the **Reports** window, select the **Time Zone** report and click **Report Options**. The **Report - Time Zone** dialog box appears.



2. To filter the time zones to be included in the report,
   a. Click the **Time Zone Filter** tab.
   b. Under **Time Zone**, select one of the following options:

Table 17-18 Describing the options for filtering time zones

Option	Description
All	Generates the report that includes all the time zones.
One	Generates the report for a single time zone. When you select this option, the **From** field is enabled. Enter the name of the time zone to generate the report. You can use the ellipsis button to find a time zone.
Range	Generates the report for the range of time zones. When you select this option the **From** and **To** fields are enabled. To specify the range, enter the first time zone name in **From** and the last time zone name in **To**. You can use the ellipsis button to find a time zone.

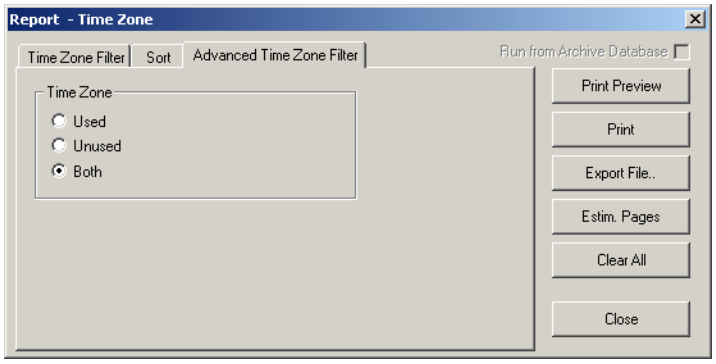
3. To sort the list in the report in the ascending or descending order:
   a. Click the **Sort** tab.

b. Under **Sort Order**, select the field by which the list in the report must be sorted.

c. Click **Ascending** or **Descending** to sort the list in chronological order or reverse order.

4. To perform advanced filter on time zones:

a. Click the **Advanced Time Zone Filter** tab.



b. Under **Time Zone**, select one of the following options:

Table 17-19 Describing the time zone options

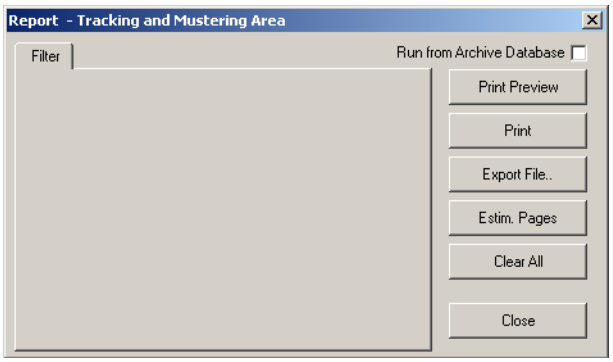
Option	Description
Used	Generates the report only on the used time zones.
Unused	Generates the report only on the unused time zones.
Both	Generates the report on the used and unused time zones.

5. Click **Print Preview** to view the report prior to printing it.
6. Click **Print** to send a copy of the report to your printer.
7. Click **Close** to return to the **Reports** window.

Tracking and Mustering Area Report

To generate a tracking and mustering area report:

1. In the **Reports** window, select the **Tracking and Mustering Area** report and click **Report Options**. The **Report - Tracking and Mustering Area** dialog box appears.



   No filter or sorting options are provided for the access area report.

2. Click **Print Preview** to view the Access Area Report prior to printing.
3. Click **Print** to send the report to your printer.
4. Click **Close** to return to the **Reports** window.

Appendix

Cold Restart on Power-surge

Caution: A cold restart of the access control panel sometimes occurs if there is a serious power surge on the power or communication lines. This causes corruption of the panel's database and time functions.

- The PW-2000 panels address the time problem by generating a system alarm 99 (Panel Database, System Alarms, Panel Reset Alarm) when the panel experiences a cold restart.
- WIN-PAK then sends the current Time and Date to the panel within 60 seconds of receiving this alarm. The default time and date after a cold restart is January 1st, Monday at 12:00 a.m. This time stamp appears on activities in the Event view and History report.
- Panel Time is critical to the proper operation of the muster function as the most recent event is used to determine the tracking or muster status of a card holder.
- If a card is presented to the Muster reader and the time and date stamp is earlier than the stamp from another reader location, there is no change of status to the Muster (safe) location.
- In the event that the card database is lost or corrupted at the muster reader, WIN-PAK recognizes all read-types (Not Found, Time Zone, Normal, Trace, PIN Violation, and Expired) as valid muster reads, provided that the time is later than the previous card read as described above.

This function eliminates the need to reload cards or to have host grant enabled to a muster panel during a muster event. Only Valid and Trace card reads count at a Tracking reader.

Note: Honeywell recommends that the muster panel has the host grant feature set to disabled to optimize system communication in the event the panel would go through a cold restart.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Honeywell

Honeywell Access Systems
135 West Forest Hill Avenue
Oak Creek, WI 53154
(414) 766-1700 Ph
(414) 766-1798 Fax
www.honeywellaccess.com

NexWatch – Europe
Boblingerstrasse 17
71101 Schonaich
Germany
Tel +49 7031637784
Fax +49 7031637786

Document 7-901032, Revision 02