WIN-PAK

The Complete Access Control Software

User's Guide

User Non-Disclosure and License Agreement

IMPORTANT-READ CAREFULLY: This Honeywell End-User License Agreement (this “Agreement”) is a legal agreement between you (either an individual or a single entity) and Honeywell International Inc. (including its subsidiaries) for the Honeywell software product identified above, which includes computer software and may include associated media, printed materials, and “online” or electronic documentation, and any future versions, releases, updates, patches, error fixes and bug fixes of the above identified Honeywell software product that is provided by Honeywell to you (“HONEYWELL SOFTWARE”).

By installing, copying, or otherwise using the HONEYWELL SOFTWARE, you agree to be bound by the terms and conditions in this Agreement. If you do not agree to the terms and conditions in this Agreement, do not install or use the HONEYWELL SOFTWARE; you may, however, return it to your place of purchase for a full refund.

Unregistered use of the HONEYWELL SOFTWARE is not authorized or permitted by Honeywell, and is in violation of U.S. and international copyright laws. Unauthorized reproduction, distribution or use is subject to civil and criminal penalties.

LICENSE: The HONEYWELL SOFTWARE includes software owned by Honeywell and software licensed to Honeywell, and is protected by United States' and international copyright laws and treaties, as well as other intellectual property laws and treaties. The HONEYWELL SOFTWARE is licensed to you, not sold.

Subject to the terms below, Honeywell grants you, under this Agreement, a limited, non-exclusive, non-transferable license (without the right to sublicense) to use one copy of the HONEYWELL SOFTWARE, on one computer or workstation, for your internal personal or commercial purposes, and not for re-sale or re-distribution.

You are specifically prohibited from making any additional copies of the HONEYWELL SOFTWARE, for charging for any copies, however made, and from distributing such copies with other products of any kind, commercial or otherwise, without prior written signed permission from Honeywell.

All rights of any kind in HONEYWELL SOFTWARE and all other rights of Honeywell, which are not expressly granted in this Agreement, are entirely and exclusively reserved to and by Honeywell. You may not rent, lease, copy, modify or translate HONEYWELL SOFTWARE, or create derivative works based on HONEYWELL SOFTWARE. You may not alter or remove any of Honeywell's or its licensor's copyright or proprietary rights notices or legends appearing on or in the HONEYWELL SOFTWARE. You may not reverse engineer, decompile or disassemble HONEYWELL SOFTWARE. You may not make access to HONEYWELL SOFTWARE available to any third party outside of your organization, nor are you authorized to make the output generated by HONEYWELL SOFTWARE available to others in connection with a service bureau, application service provider, or similar business. The HONEYWELL SOFTWARE is licensed as a single product. Its component parts may not be separated for use on more than one computer.

The HONEYWELL SOFTWARE may contain or be derived from materials of third party licensors. Such third party materials maybe subject to restrictions in addition to those listed in this Agreement, which restrictions, if any, are included in the documents accompanying such third party software. You agree that any third party supplier shall have the right to enforce this Agreement with respect to such third party's software.

Nothing in this Agreement shall restrict, limit or otherwise affect any rights or obligations you may have, or conditions to which you may be subject, under any applicable open source licenses to any open source code contained in the HONEYWELL SOFTWARE.

KEYS AND ACCESS: Honeywell shall provide you with any Software keys necessary to permit you to gain access to the HONEYWELL SOFTWARE contained on the media shipped or copy provided to you. You shall not disclose the Software keys to any other person or entity. You shall not circumvent, or attempt to circumvent, any license management, security devices, access logs, or other measures provided in connection with the HONEYWELL SOFTWARE, or permit or assist any other person or entity to do the same. You shall not attempt to modify, tamper with, reverse engineer, reverse compile or disassemble the keys. Upon your use of a new key for the HONEYWELL SOFTWARE, you represent and warrant that you will not use the superseded key to access the HONEYWELL SOFTWARE.

SUPPORT SERVICES: You may separately contract with Honeywell to receive support services related to the HONEYWELL SOFTWARE ("Support Services"), subject to and governed by the terms of a separate Support Services Agreement. Any supplemental

software code provided to you as part of the Support Services shall be considered part of the HONEYWELL SOFTWARE and subject to the terms and conditions of this Agreement. With respect to technical information you provide to Honeywell as part of the Support Services, Honeywell may use such information for its business purposes, including for product support and development. Honeywell will not utilize such technical information in a form that personally identifies you.

In any event, you shall promptly report to Honeywell any errors or bugs with respect to your evaluation and use of the HONEYWELL SOFTWARE. In any such report, you agree to designate no more than two contacts who shall be responsible for communicating with Honeywell.

WARRANTY DISCLAIMERS AND LIABILITY LIMITATIONS: HONEYWELL SOFTWARE, AND ANY AND ALL ACCOMPANYING SOFTWARE, FILES, DATA AND MATERIALS, ARE DISTRIBUTED AND PROVIDED AS IS AND WITH NO WARRANTIES OR REPRESENTATIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED. HONEYWELL EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. The entire risk arising out of use or performance of HONEYWELL SOFTWARE remains with you.

THE MAXIMUM AGGREGATE CUMULATIVE LIABILITY OF HONEYWELL ARISING OUT OF OR RELATING TO YOUR USE OF HONEYWELL SOFTWARE OR OTHERWISE ARISING OUT OF OR RELATING TO THE TRANSACTIONS CONTEMPLATED BY THIS AGREEMENT (REGARDLESS OF LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE) WILL BE THE AMOUNT THAT YOU PAID FOR THE HONEYWELL SOFTWARE. IN ADDITION, IN NO EVENT SHALL HONEYWELL, OR ITS PRINCIPALS, SHAREHOLDERS, OFFICERS, EMPLOYEES, AFFILIATES, CONTRACTORS, SUBSIDIARIES , OR PARENT ORGANIZATIONS, BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES WHATSOEVER RELATING TO THE USE OF HONEYWELL SOFTWARE, OR TO YOUR RELATIONSHIP WITH HONEYWELL, EVEN IF HONEYWELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TERMINATION: The license granted in this Agreement becomes effective on the date you legally acquire the HONEYWELL SOFTWARE and will automatically terminate if you breach any of its terms or conditions, without prejudice to any other rights or remedies available to Honeywell. If the HONEYWELL SOFTWARE is provided to you on a subscription basis, then your right to posses or use the HONEYWELL SOFTWARE will terminate at the end of the applicable subscription period. Immediately upon termination or expiration of the license granted in this Agreement, you must

destroy all copies of the HONEYWELL SOFTWARE and all of its component parts from your systems, and either return to Honeywell or destroy the original and any stand-alone copies of the HONEYWELL SOFTWARE and all of its component parts.

MISCELLANEOUS: You may not assign or transfer the license granted hereunder or the HONEYWELL SOFTWARE without Honeywell's prior written consent. Any assignment or transfer in contravention to the foregoing shall be null and void.

This Agreement is governed by the laws of the State of New York. Each of the parties hereto irrevocably consents to the jurisdiction of the Federal and state courts in New York, New York, to the exclusion of all other courts. If this product was acquired outside the United States, then local law may apply.

Honeywell has the right to audit your compliance with the terms and conditions of this Agreement, including without limitation, ensuring that you are not using more than one copy of the HONEYWELL SOFTWARE, or bypassing the software keys to engage in unauthorized, unlicensed use of the HONEYWELL SOFTWARE, and to immediately terminate your license in this Agreement if an audit shows that you are in breach with any of the terms and conditions of this Agreement, as well as to enforce all other rights and remedies available under this Agreement or otherwise under law or at equity.

The failure of Honeywell to enforce at any time any of the provisions of this Agreement shall not be construed to be a continuing waiver of any provisions hereunder nor shall any such failure prejudice the right of Honeywell to take any action in the future to enforce any provisions hereunder.

It is understood and agreed that, notwithstanding any other provisions of this Agreement, breach of any provision of this Agreement by you may cause Honeywell irreparable damage for which recovery of money damages would be inadequate, and that Honeywell shall therefore be entitled to obtain timely injunctive relief to protect Honeywell's rights under this Agreement in addition to any and all remedies available at law.

Nothing contained herein shall be construed as creating any agency, employment, relationship, partnership, principal-agent or other form of joint enterprise between the parties.

The section headings appearing in this Agreement are inserted only as a matter of convenience and in no way define, limit, construe, or describe the scope or extent of such section or in any way affect this Agreement.

Whenever possible, each provision of this Agreement shall be interpreted in such manner as to be effective and valid under applicable law. But, if any provision of this Agreement is held to be invalid, illegal or unenforceable in any respect under any applicable law or rule

in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other provision in that jurisdiction, but this Agreement shall be reformed, construed and enforced in such jurisdiction as if such invalid, illegal or unenforceable provision had never been contained herein. Further, such invalidity, illegality or unenforceability shall not affect any of the provisions in this Agreement in any other jurisdiction.

This Agreement constitutes the entire agreement between you and Honeywell and supersedes in their entirety any and all oral or written agreements previously existing between you and Honeywell with respect to the subject matter hereof. This Agreement may only be amended or supplemented by a writing that refers explicitly to this Agreement and that is signed by duly authorized representatives of you and Honeywell. The preprinted terms and conditions of any Purchase Order issued by you in connection with this Agreement shall not be binding to Honeywell and shall not be deemed to modify this Agreement.

Software and technical information delivered under this Agreement is subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to strictly comply with all such laws and regulations, and you shall be solely responsible for obtaining any import, export, re-export approvals and licenses required for such software any technical information, and retaining documentation to support compliance with those laws and regulations.

GDPR Privacy Statement

Please be aware that this product can store personal data.

Personal data is protected by the General Data Protection Regulation (2016/679) in Europe and therefore the owners of personal data have obtained certain rights thanks to this regulation.

We strongly advise you to be fully aware of these owner (“data subjects”) rights as well as which limitations you have to obey regarding the use and distribution of this data.

Further details can be found on the “https://eugdpr.org/” GDPR website of the EU.

CONTENTS

Chapter 1 Introduction

Chapter 2 Installation

Chapter 3 User Interface

Chapter 4 Getting Started

Chapter 5 System Settings

Chapter 6 Badge Layout

Chapter 7 Card Holders

Chapter 8 Time Management

Chapter 9 WIN-PAK CS/SE/PE Servers and Devices

Chapter 10 Defining Areas

Chapter 14 Monitoring Actions

Chapter 15 Translation

Chapter 20 Import Utility

Chapter 21 Troubleshooting

Chapter 22 Appendix

About this Guide

Scope

The WIN-PAK User's Guide helps you in installing, configuring, and using the WIN-PAK access control software.

Intended Audience

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

Prerequisite Skills

You need to have a knowledge of access control systems and their 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 user interface of the WIN-PAK software. This chapter also includes the procedure to access the Help.
Chapter 4, Getting Started	Explains the basic configuration details of the client and the 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 6, Badging	Describes how to design a badge, configure the badge DLLs and the badge printer.

Chapter	Description
Chapter 7, Card Holders	Includes information on setting up the card holder template, card holders, cards, and assigning card holders to cards and badges.
Chapter 8, Time Management	Explains how to set time zones, schedule an event, and define holiday groups and daylight saving groups.
Chapter 9, Device Map	Comprises sections for configuring servers, panels, readers, and abstract devices.
Chapter 10, Defining Areas	Describes how to • Define access areas, control areas, tracking and muster areas. • Control devices through the control map, and monitor card holder movement in the tracking and muster areas.
Chapter 11, Floor Plan	Explains how to create floor plans and control devices from the floor plan view.
Chapter 12, Command File	Includes sections on defining commands, command files, and controlling devices by executing the command files.
Chapter 13, Guard Tour	Describes how to define and run guard tours.
Chapter 14, Monitoring Actions	Explains the different ways available for tracking and monitoring events in the access control system.
Chapter 15, Translation	Describes how to translate the user interface using the language text file and on creating language files.
Chapter 16, Reports	Assists you in generating various 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 the advice or hint for the user, often in terms of performing a task.

Symbol	Definition
	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: 7 AM to 7 PM (CST)

PHONE: 800-323-4576

URL: http://www.honeywellaccess.com

EMAIL SUPPORT: HASsupport@honeywell.com

Honeywell Access Systems

Charles Avenue, Burgess Hill

West Sussex, RH15 9UF

U.K.

PHONE: +44 (0) 1444 251180

Introduction

1

In this chapter...

This chapter describes about the Overview, Components, Features and Software Concepts of WIN-PAK CS/SE/PE, and T&A.

Section	WIN-PAK CS	WIN-PAK SE/PE	WIN-PAK T&A
Overview: WIN-PAK CS, page 6	✓		
Overview: WIN-PAK SE/PE, T&A, page 7		✓	✓
Overview: WIN-PAK SE/PE, T&A, page 7	✓		
Components: WIN-PAK CS/SE/PE Servers, page 7	✓	✓	
Components: WIN-PAK CS/SE/PE Clients, page 8	✓	✓	
Features: WIN-PAK CS/SE/PE, page 9	✓	✓	
Features: WIN-PAK T&A, page 10			✓
Software Concepts: Abstract Devices, page 12	✓	✓	
Software Concepts: Floor Plan View, page 13	✓	✓	
Software Concepts: Badge, page 13	✓	✓	
Software Concepts: Card and Card Holder, page 13	✓	✓	
Software Concepts: Intrusion Panels, page 13	✓	✓	
Software Concepts: Video Management System, page 13	✓	✓	

Overview

WIN-PAK is a state-of-the-art access control software. It uses the access control mechanism to authenticate employee access at security areas.

The following table provides the list of compatible operating system for the access control software:

Variant	Compatible operating systems
WIN-PAK CS	Windows Server 2012 R2, Windows. Server 2016 and Windows 10 Operating Systems Windows 7 & Windows Server 2008 R2 is only supported as WIN-PAK Client machine.
WIN-PAK T&A	Windows Server 2012 R2, Windows Server 2016 and Windows 10 Operating Systems. Windows 7 & Windows Server 2008 R2 is only supported as WIN-PAK Client machine.
WIN-PAK SE/PE	Windows Server 2012 R2, Windows Server 2016 and Windows 10 Operating Systems Windows 7 & Windows Server 2008 R2 is only supported as WIN-PAK Client machine.

WIN-PAK CS

WIN-PAK CS is installed at the dealer's location. Access control panels that are installed at various customer locations are centrally monitored through the application.

Each customer of WIN-PAK CS is provided an account. Accounts are configured with the access related information of customers. The operators at the dealer's location monitor and track the access control activities of each customer, through the customer accounts.

In addition, WIN-PAK CS includes the Web Interface application which enables the customer to view reports and database information of their accounts.

WIN-PAK CS also supports Advanced Encryption Standard (AES). The AES encryption replaces the existing Two Fish encryption, which provides options for connecting to the N1000 series of products. The AES encryption provides the encryption support through the Lantronix SDS1101 serial-to- Ethernet converter and associated DLL obtained from Lantronix. AES Encryption support for N series panels is provided through SDS1101 Lantronix Device Server and for Direct P series panels, the encryption is supported via the panel.

WIN-PAK SE/PE, T&A

In WIN-PAK SE/PE, T&A, the access is authenticated using 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.

The WIN-PAK T&A Web interface enables an admin/operator at the customer location to perform certain basic operations such as managing employee time and attendance, approving leave requests, and generating reports. The main aim of developing the WIN-PAK T&A Web application is to minimize the dependency of admin/operators relying on WIN-PAK application for time and attendance configuration. The WIN-PAK T&A Web application is an extension of the WIN-PAK T&A with limited operations.

The employee list in WIN-PAK T&A is populated from the database server hosting the WIN-PAK T&A application.

Components

The WIN-PAK CS/SE/PE application has the following main components:

- Database Server
- Communication Server
- User Interface
- Web Interface (applicable only in WIN-PAK CS)

These components can run on a single computer or on multiple computers, allowing flexibility in configuring a networked system.

WIN-PAK CS/SE/PE Servers

Database Server

Data can be stored, organized and retrieved from database tables using the WIN-PAK CS/SE/PE Database Server. This data is accessible to the Communication Server, User Interface, and Web Interface for retrieving and generating reports.

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

Communication Server

The Communication Server sends the User Interface requests as well as the access transactions to the access control panel. The access control panel processes the transactions and sends the information to the Database Server and the response to the User Interface through the Communication Server.

When the communication server sends 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 until the user request is processed.

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

API Server

This component is installed by default only when Web CD Key is entered during installation, and is suitable for web installations.

Note: API Server is applicable only for WIN-PAK CS.

Video Management Server

The Video Management Server (VMS) is an enterprise-class video management and storage solution. It is a truly hybrid solution which, enables you to operate the traditional analog and the network and IP based video equipment in the same surveillance network. You can deploy thousands of cameras in number of locations, and add many video devices such as recorders and monitors.

Note: VMS is applicable only for WIN-PAK CS.

To set the VMS, you must perform the following tasks:

Task	Go To
Add or Edit Video Management Server	page 433, page 435
Connect the Video Management Server	page 435
Synchronize Video Management Server	page 436
Add Recorder	page 436, page 444, page 447, page 452
Delete Video Management Server	page 436

WIN-PAK CS/SE/PE Clients

User Interface

The User Interface helps WIN-PAK CS/SE/PE 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 access the single Database Server simultaneously. The number of client computers depend on the license type that you procure WIN-PAK.

Web Interface

Using the Web Interface, you can view, edit, and delete the database. You can also generate a report based on the privileges assigned to you. You can configure the privileges in the WIN-PAK CS User Interface.

Note: Web Interface is applicable only for WIN-PAK CS.

Features

WIN-PAK CS/SE/PE

- **Installation**: Handles large and complex installations including the configuration of the WIN-PAK CS/SE/PE 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 CS/SE/PE.
- **Digital Video**: Provides live display of Rapid Eye, MAXPRO NVR, and Fusion devices.
- **Encryption**: Provides the support for AES encryption
- **WIN-PAK Services**: In addition to the database server and the communication server, WIN-PAK CS/SE/PE contains the following 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 stipulated 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 card in Muster readers. Muster areas are logical areas that contain readers to be used by the card holders, only if there is a call for muster (For example, in the event of a disaster).
  - **Schedule Server**: This server schedules the list of events to be performed at predetermined time and intervals such as hourly, daily, or monthly.
  - **API Server**: The API server makes the WIN-PAK CS more robust, and serves as a message interface for the existing NCICore API Helper and COMAPI Helper components.

– **Video Management Server**: This server provides an interface to connect to the various Digital Video Recorders /Network Video Recorders (DVRs/NVRs). In addition, it also provides CCTV control with Live Monitor Display, PTZ control of cameras, Video Playback operations, and so on.

Notes:

- Digital Video, Encryption, and API Server features are available only in WIN-PAK CS.
- The WIN-PAK CS/SE/PE services are installed while installing the Database Server or the complete WIN-PAK CS/SE/PE application. They are started automatically after installation.

WIN-PAK T&A

Using the WIN-PAK T&A Web interface, any operator from any customer location can access the WIN-PAK T&A database server from any computer on the network.

The following are the features of WIN-PAK T&A:

- Supports shifts, holidays based on locations and mid-night cross over of shifts.
- Supports multiple locations.
- Supports unlimited cardholders.
- Supports leave / weekly offs / holiday definition, based on individual employee and also location.
- Supports manual update of attendance / leaves / out door duty.
- Supports shift allocation to employees.
- Supports shift allocation based on departments.
- Supports generating various reports.

Notes:

- An Operator can be classified either as a Super Administrator, Administrator, Supervisor, or a User.
- The Super Administrator can access only the WIN-PAK T&A Web application.

To know more about all the roles and the corresponding privileges, refer the following table:

Menu	Options	Admin	Supervisor	User
DashBoard	DashBoard	✓	✓	✓

Menu	Options	Admin	Supervisor	User
Configuration	Department	✓	✗	✗
	Designation	✓	✗	✗
	On Duty	✓	✗	✗
	Location	✓	✗	✗
	Employee Type	✓	✗	✗
	Correction	✓	✗	✗
	Holiday	✓	✓ (View only)	✗
	Leave	✓	✓ (View only)	✗
	Shift	✓	✓ (View only)	✗
Requisition	Leave Request	✓	✓	✓
	On Duty Request	✓	✓	✓
	Attendance Correction Request	✓	✓	✓
	Request Status	✓	✓	✓
	Approve Request	✓	✓	✗
Management	Shift Rotation	✓	✓	✗
	Update Supervisor	✓	✗	✗
	Report Schedule	✓	✗	✗
	Shift Allocation	✓	✓	✗

Menu	Options	Admin	Supervisor	User
Login	Login Page	✓	✓	✓
	Forgot Password	✓	✓	✓
	Change Password	✓	✓	✓
Employee	New Employees	✓	✗	✗
	All Employees	✓	✓ (View only)	✗
Report	Master Report	✓	✗	✗
	Shift Allocation	✓	✓	✗
	OverTime Report	✓	✓	✗
	Attendance Report	✓	✓	✓
	Attendance Correction Report	✓	✓	✓
	On Duty	✓	✓	✓
	Leave Report	✓	✓	✓
	Leave Balance Report	✓	✓	✓
Settings	Login and SMTP Configuration	✓	✗	✗

Software Concepts

Abstract Devices

An abstract device is a logical representation of a physical device. The Abstract Device Records (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 CS/SE/PE includes a full-featured badge layout utility for designing, creating, and printing the 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 access to different areas.

Intrusion Panels

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

Video Management System

The Video Management System (VMS) is an enterprise-class video management and storage solution. It is a hybrid solution which, enables you to operate the traditional analog and the network (IP) based video equipment in the same surveillance network. Through the user interface, you can easily add cameras, recorders, and other devices. Monitoring locations is more effective through features like color correction, digital zoom, and others. Event such as failure of camera or loss of video can be logged. You can retrieve and view the video pertaining to specific events. In addition, you can configure alarms to notify the operators when events occur.

Installation

2

In this chapter...

This chapter describes about the Introduction, System Requirements, Installation, and Licensing and Registration of WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
Installation: Installing UI and Communication Server for WIN-PAK CS/SE/PE, page 64	✓	✓
Installation: Installing Communication Server for WIN-PAK CS/SE/PE, page 68	✓	✓
Installation: Installing Video Management Server along with database server or complete installation for WIN-PAK CS, page 72	✓	
Installation: Installing Video Management Server along with communication server or user interface and comm server installation for WIN-PAK CS, page 81	✓	
Installation: Installing Video Management Server for WIN-PAK SE/PE, page 87		✓
Installation: Installing HON FIN4000 ENROLL Device Drivers for WIN-PAK SE/PE, page 89		✓
Installation: Additional Installation Components for WIN-PAK CS/SE/PE, page 89	✓	✓
Installation: Upgrading WIN-PAK SE/PE, page 90		✓
Licensing and Registration: Registering WIN-PAK CS/SE/PE, page 92	✓	✓
Licensing and Registration: Caution on License Files, page 94	✓	✓

Introduction

Overview

This 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 installation types available in WIN-PAK are:

- **Single Server Deployment (Default option)**: The Host and Web are installed on a single computer.
- **Dual server Deployment**: The Host and Web are installed on two different computers. Host is installed on Machine 1 and the Web is installed on Machine 2.
- **Custom/Classic Deployment**: Allows you to select the types of setup to be installed.

The WIN-PAK software is distributed on an auto-run CD, with release notes and other technical documents.

WIN-PAK Architecture

It is a multi-tier, client-server-distributed application, consisting of the following primary components:

- Database Server
- Communication Server
- User Interface
- Web Interface (applicable only in WIN-PAK XE/SE/PE/CS).

The WIN-PAK CS/SE/PE modules installed on different computers are networked and connected through RPC and Local Procedure Calls (LPC). This allows WIN-PAK CS/SE/PE program components to run as full services in their compatible operating system.

The WIN-PAK CS/SE/PE software is shipped with the debug versions of the services, which provide a console output window. However, avoid using these debug versions on a daily basis, as they are reserved for error isolation.

WIN-PAK CS/SE/PE provides the System Manager utility to configure connection information. The System Manager directs the User Interface and the other remote servers to the Database Server.

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

System Requirements

Hardware Requirements for WIN-PAK

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

Note: For maximum performance for Video integration applications, workstation must have Haswell i7 4770k class processor for GPU rendering (not applicable for WIN-PAK GX/XE).

Hardware Component	**Minimum - Single User standalone / Workstation**	**Recommended**	**Maximum/Performance**
Processor	Intel® Core i3 Desktop class machine	Intel® Quad Core Xeon® Server class machine	Intel® Quad Core Xeon® Server class machine
CPU	Dual Core, 3.30GHz	2.4GHz CPU	3.5GHz or more
RAM	8GB - 4GB Workstation	16GB - system server 8GB - Comserver/UI only	32GB
Hard Disk	120 GB with 60 GB free Workstation(s) 80 GB with 5 GB free	250 GB SATA or SCSI 7200 RPM min or Solid State drive 60GB Free space	1TB SATA 15k RPM or Solid State drive preferred
Serial communication ports	As per the requirement	As per the requirement	As per the requirement
Secondary Storage	Tape or DVD burner	Tape or DVD burner	Tape or DVD burner
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**: 1600 x 900 **Colors**: True color	**Size**: 19 inch **Resolution**: 1980 x 1200 **Color**: True color
Pointing Device	Mouse (USB mouse preferred)	Mouse (USB mouse preferred)	Mouse (USB mouse preferred)
Power Supply	UPS	Hot-swap, redundant with UPS	Hot-swap, redundant with UPS
Database Engine	SQL 2016 Express (64 Bit Only) **Note** Older SQL engines like MSDE, SQL2005 are strictly not supported.	SQL 2016 Standard (64 bit only)	SQL 2016 Standard (64 bit)

Note:

- If you want to install WIN-PAK in a stand-alone computer that supports 1 to 10 readers, 250 cards, or as a workstation, 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, or an additional communication server (PE/CS only),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, your computer must fulfill the **performance** requirements.

Badging Printers

The Windows Operating System supports any type of badge printer. However, for two-sided PVC encoding or magnetic stripe encoding, the 3652-0001 series (Ultra Rio Pro or Rio Pro Duplex) printer is required.

Note: The 2-side printing option is available in the printer setup only if the printer driver supports dual-side printing.

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 NS2+ must have firmware of version 1 or later (1.05.05 recommended) and the P-Series panels must have firmware version 1.04 or later. The NetAXS-123 and the NetAXS-4 panels must have a firmware of version 3.4 or later.

Panel	Recommended
PW-6000	V2.6.5
PRO 3200	2.7.8.480
N100IV X	V8.07
NetAXS-123	V6.0.10.5
NetAXS-4	V3.6.25
PRO 2200	P2E_2091.crc

Panel	Recommended
N1000 IV X	V8.02 - V8.07
NS2+	V1.05.05
Vista 128 BPT	Rev 10
Galaxy GD96	V6.50

Recorder Firmware

Recorder	Version
RapidEye	V10.0.30
MAXPRO NVR	V4.0 Build 87 Rev H
Fusion	V4.5.1513, 4.5.5300
HRDP H.264	V1.0.0.23, 1.0.0.37
HRDP MPEG4	V3.0.0.86_2.5.7.H53, 3.0.1.9

Galaxy

Intrusion Device/Panel	Version
Galaxy GD96	V6.50
Galaxy GD264	V6.8
Galaxy GD520	V6.75
Galaxy GD48	V6.8

Flex

Intrusion Device/Panel	Version
FX20	V3.18
FX50	V3.18
FX100	V3.18
FX20+	V3.35
FX100+	V3.35

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 the Windows 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 3652-0001 series (Ultra Rio Pro or Rio Pro Duplex) printer is required.

Software Requirements

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

Components	Supported	Recommended	Maximum/Performance
Operating Systems 64-bit only	Windows 8.1 Professional Windows 2012 Standard Windows Server 2012 R2 Server Standard Windows 10 Professional Windows Server 2016 **Note**: • ENGLISH OS alone with latest service pack. • Operating systems such as Windows Vista, Windows XP and Windows Server 2003 are NOT supported.	Windows 10 Professional (standalone system or Workstations) Windows Server 2012 R2 Standard when additional workstations and or communication servers are added. Also use for additional communication servers (PE/CS only).	Windows Server 2016
WIN-PAK CS/SE/PE Software	Direct upgrade supported from WIN-PAK 4.6 B1060.6 and WIN-PAK 4.6.1 B1060.22. Access only (no video integration), upgrade supported from WIN-PAK 4.4 GX/XE/SE and single account PE via restoring backup into an new 4.7 installation.		

Components	Supported	Recommended	Maximum/Performance
Panel Communication Types	*NetAXS 123/4* 1. TCP/IP with/without Encryption 2. Reverse IP with/without Encryption *PRO 2200/PRO 3200/PW 5000/PW 6000* 1. TCP/IP with/without Encryption 2. Reverse IP with/without Encryption *N1000 IV X f/w 8.07* 1. TCP/IP with/without Encryption 2. Reverse IP with/without Encryption 3. Using Lantronix and PCI3 *NS2+* TCP/IP using Lantronix		
Card Format	Corporate 1000 [35 bit] 34 bit proximity card		
Reader Types	OmniProx OP 10 OmniProx OP 30 OmniProx OP 40 HID Proximity Reader HID Card+PIN reader		
Browser	Internet Explorer 11 and later. Also, supports Google Chrome 40.0.2214.91, Mozilla Firefox 35.0, and Safari 5.1.7 (7534.57.2)	Internet Explorer 11	Internet Explorer 11

System Prerequisites

The following sections describe the list of system prerequisites to be carried before installing WIN-PAK CS/SE/PE/XE/GX.

WIN-PAK CS/SE/PE/XE/GX

Stand-alone Systems

Before installing WIN-PAK CS/SE/PE/XE/GX, ensure that the following prerequisites are met:

- You must verify and install .NET 3.5 SP1 and .NET 4.0.

- You must verify for the supported Operating systems and browser as described in the Software Requirements.
- You must verify for 80GB of free hard disk space.
- 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.

Before beginning the installation:

- Make a note of the CD Key, which is made available in the DVD case. This is required while installing WIN-PAK.
- Read the release notes on the WIN-PAK media for additional installation information and updates.

Networked Systems

Before installing WIN-PAK CS/SE/PE/XE/GX for the first time in the networked system, ensure that the following prerequisites are met in addition to the prerequisites applicable to the stand-alone systems.

- Network cards are installed on a networked system. A standard Windows-compatible network card is adequate.
- Ensure that the client computer name is alphanumeric, the characters are continuous (without any space), and the first character is 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

This section describes the procedures for installing WIN-PAK CS/SE/PE on your system.

Overview

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

Notes:

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

- During installation, the WIN-PAK opens the following ports in the firewall.

Port	Type	Used for...
135	TCP	DCOM components
1433, 1434, 2383, 2380, 49373	TCP	MSSQL
1434	UDP	MSSQL
5544	TCP	WIN-PAK API Server
80	HTTP	Web application
445	TCP	Microsoft-ds
5555	TCP	WIN-PAK Database Server
5556	TCP	WIN-PAK Archive Server
5500	TCP	WIN-PAK Muster Server
5577	TCP	WIN-PAK Guardtour Server
5599	TCP	WIN-PAK Commandfile Server
5588	TCP	WIN-PAK Schedule Server
3001	TCP	WIN-PAK Panel communication
2101	TCP	WIN-PAK Panel communication
5566	TCP	WIN-PAK Communication server
443	HTTPS	Web application
6000-6200	TCP	RPC Random ports

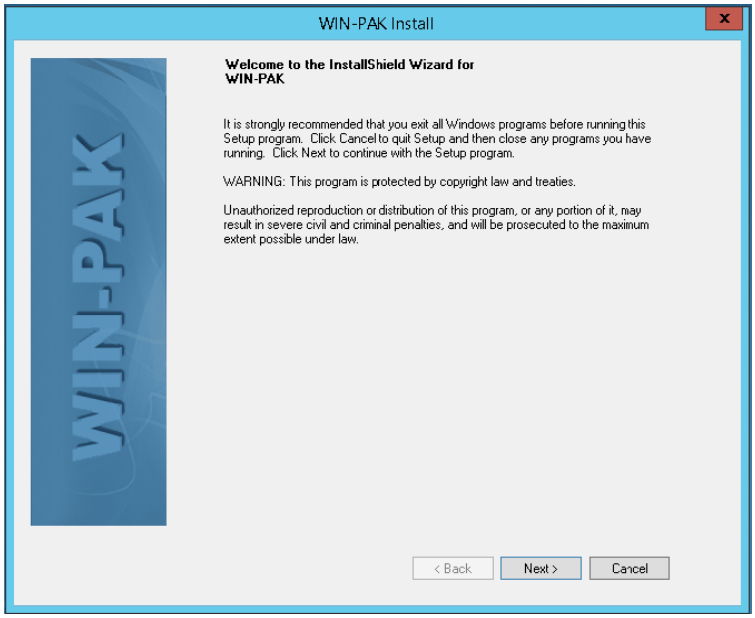
Also, the following ports must be manually opened.

- WIN-PAK CS Comserver ports
- RIP panel ports

To install WIN-PAK CS/SE/PE

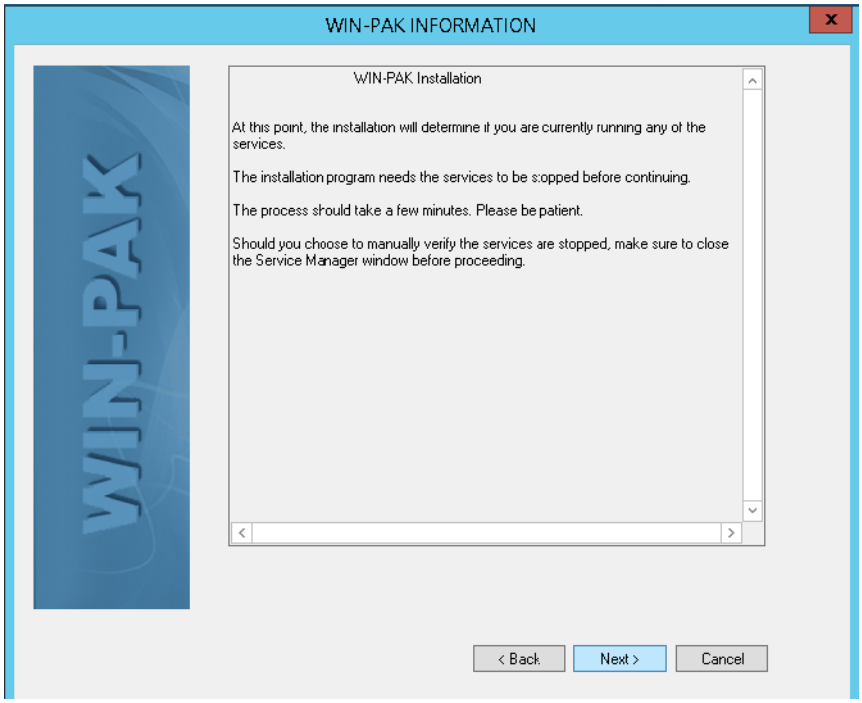
1. Insert the WIN-PAK CS/SE/PE CD/DVD into the CD/DVD-ROM drive. An installation browser opens. If the browser does not open, browse to the CD/DVD folder and run the **Setup.exe** file. The **Welcome** screen appears.

Note: WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

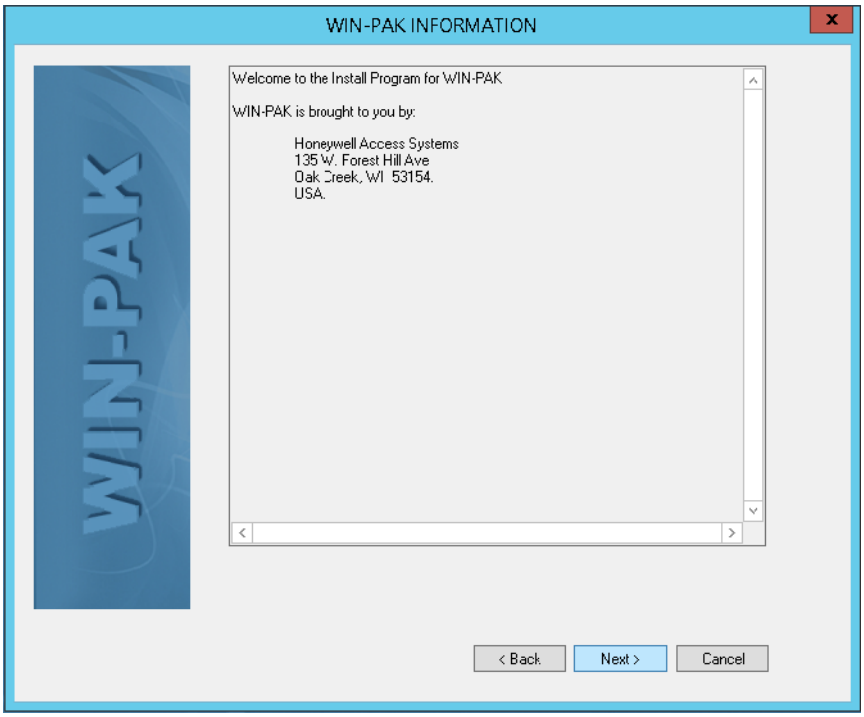


Note: If an earlier version of Internet Explorer is found (earlier than IE 6), WIN-PAK CS/SE/PE prompts you to upgrade the IE. Click **Yes** to upgrade.

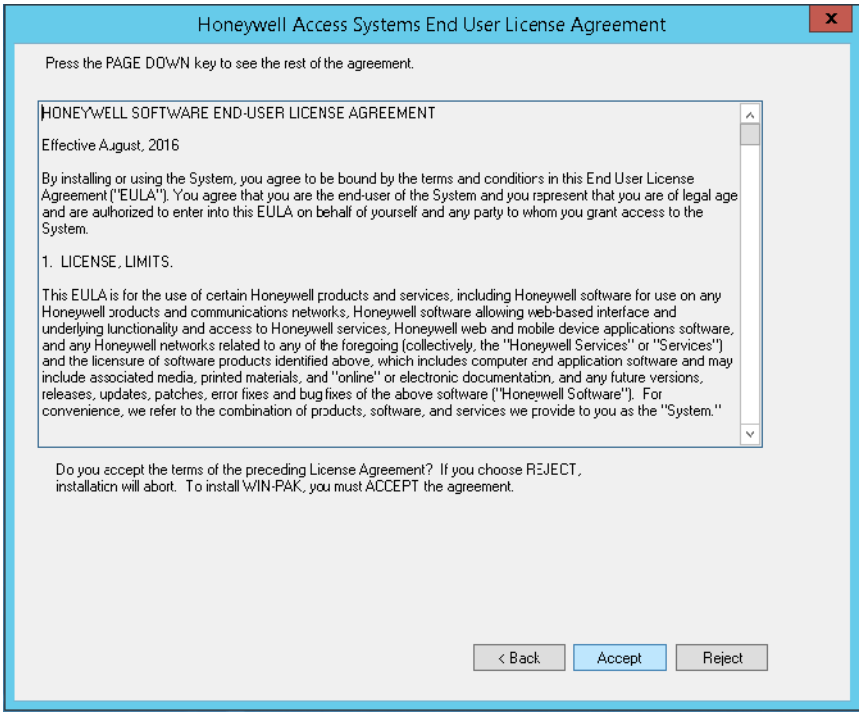
2. Click **Next** to continue the installation. The **WIN-PAK CS/SE/PE Information** screen appears.



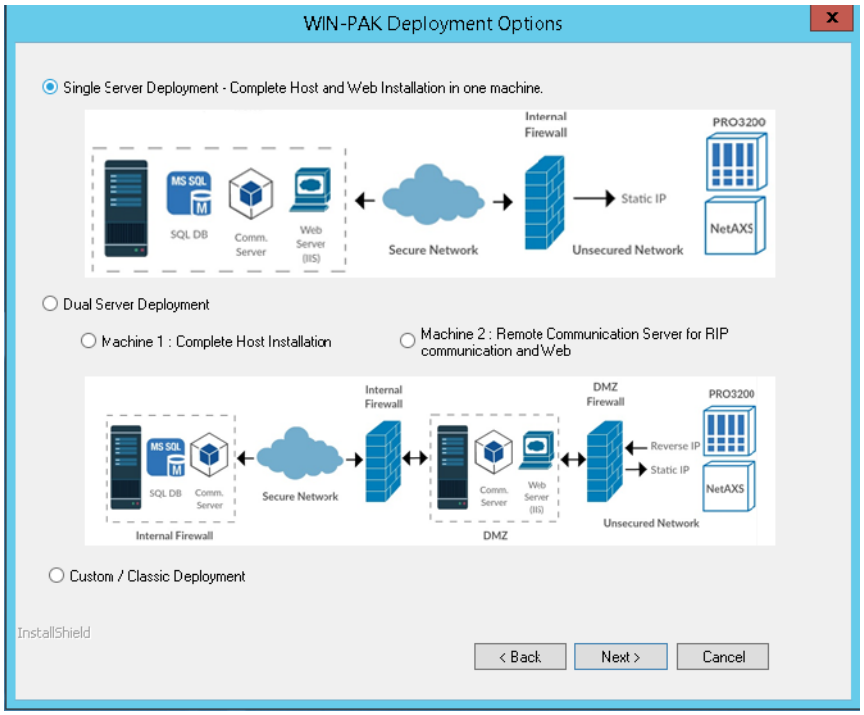
3. Click **Next** to verify that all the services are stopped.



4. Click **Next**. The **Honeywell Access Systems End User License Agreement** screen appears.



5. Read the license agreement details and click **Accept**. The **WIN-PAK CS/SE/PE Deployment Options** screen appears.



6. Select the Deployment Type. The following table describes the setup types available in WIN-PAK CS/SE/PE:

Deployment Type	Installs...	Suitable when...	See...
If you are installing WIN-PAK CS on a stand-alone computer, you can select the deployment type as Single Server Deployment:			
Single Server Deployment - Complete Host and Web Installation in one machine	All the WIN-PAK CS components such as client, server, and support programs.	Setting up in a stand-alone computer.	Installing Complete WIN-PAK CS/SE/PE, page 29
If you are installing WIN-PAK CS on two different computers, you can select the deployment type as Dual Server Deployment:			
Machine 1: Complete Host Installation	All the WIN-PAK CS host components.		Installing Complete Host on Machine 1, page 38
Machine 2: Remote Communication Server for RIP communication and Web	The remote server and web.		Installing Remote Communication Server and Web on Machine 2, page 46
If you are installing WIN-PAK CS/SE/PE in a custom environment, you can select the deployment type as Custom/Classic Deployment where the web is not installed:			

Deployment Type	Installs...	Suitable when...	See...
Database Server Only	Only the Database Server and the related components.	Installing WIN-PAK CS/SE/PE in a networked computer	Installing Database Server for WIN-PAK CS/SE/PE, page 52
User Interface Only	Only the WIN-PAK CS/SE/PE User Interface.	Installing WIN-PAK CS/SE/PE on a client workstation in a networked computer.	Installing User Interface for WIN-PAK CS/SE/PE, page 59
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 UI and Communication Server for WIN-PAK CS/SE/PE, page 64
Communication Server Only	Only the Communication Server and the related components.	Installing the communication server on a networked computer.	Installing Communication Server for WIN-PAK CS/SE/PE, page 68
Video Management Server selected along with database server or complete installation	Video Management Server.	Installing WIN-PAK in a networked computer.	Installing Video Management Server along with database server or complete installation for WIN-PAK CS, page 72
Video Management Server, selected along with User Interface only/User Interface and Communication Server only	Only Video Management with client components.	Installing WIN-PAK CS/SE/PE on a client workstation in a networked computer.	Installing Video Management Server along with communication server or user interface and comm server installation for WIN-PAK CS, page 81
API Server (applicable only for WIN-PAK CS)	This component is installed by default only when the Web option is selected during installation, and is suitable for web installations.	Web installations	
If you are installing WIN-PAK SE/PE in a stand-alone computer, you can select the setup type as Complete Installation:			

Deployment Type	Installs...	Suitable when...	See...
Complete Installation	All the WIN-PAK SE/PE 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 User Interface for WIN-PAK CS/SE/PE, page 59

Notes:

- To protect the database files from the failure of the operating system, place them on a different drive partition.
- To isolate the database files from the database server, place them on a separate hard drive.
- Install the database file on the database server. This helps in effective usage of the WIN-PAK CS/SE/PE back up and restore option.
- To complete WIN-PAK SE/PE, install SQL Express 2012. For installation visit the website at: http://msdn.microsoft.com/en-us/library/ms143219.aspx

Installing Complete WIN-PAK CS/SE/PE

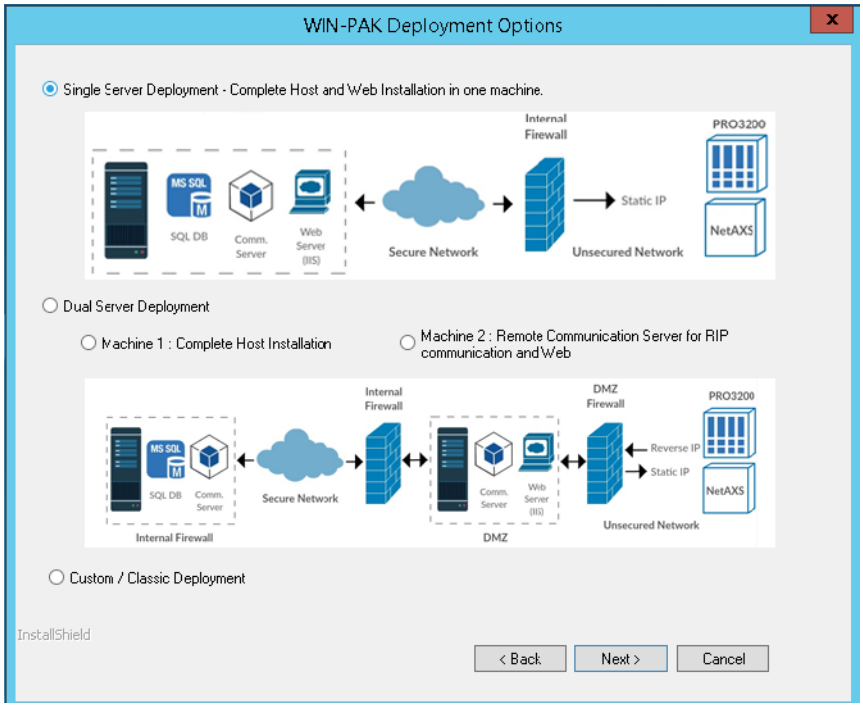
You can install complete WIN-PAK CS/SE/PE, if you are installing on a stand-alone computer.

To install complete WIN-PAK CS/SE/PE on your computer, perform the instructions given in "To install WIN-PAK CS/SE/PE" and follow these steps:

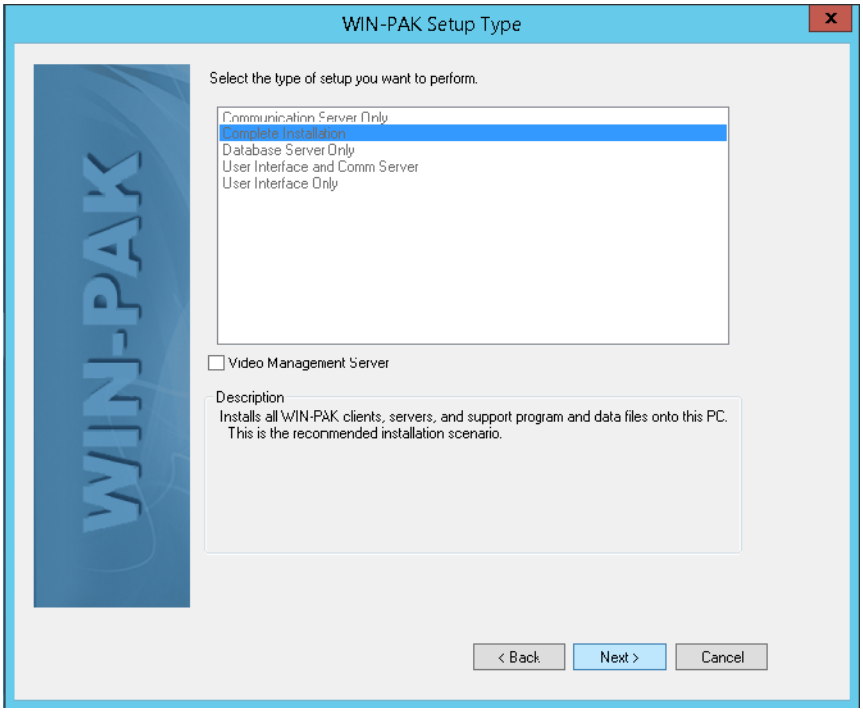
Notes:

- To install Complete WIN-PAK CS, follow steps from 1 to 22.
- To install complete WIN-PAK SE/PE, follow steps from 8 to 22.
- WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

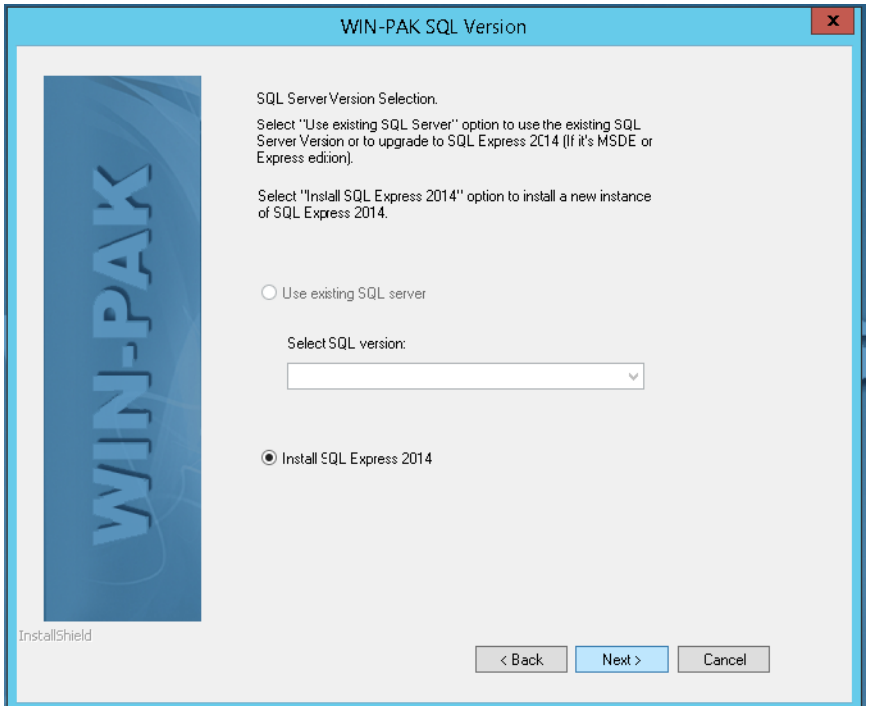
1. In the **WIN-PAK CS Deployment Options** screen, select **Single Server Deployment - Complete Host and Web Installation in one machine**.



2. Click **Next**. The **WIN-PAK CS Setup Type** screen appears.



3. By default, the **Complete Installation** is selected. Click **Next**. The system checks for SQL Service status and displays the **WIN-PAK CS SQL Version** screen.



4. You can select:
    - **Use existing SQL server** to use the existing SQL Server version or to upgrade to the SQL Express 2012 (if it is MSDE or Express Edition). You must **Select SQL Version** from the drop-down list.
    - **Install SQL Express 2012** to install a new instance of the SQL Express.
5. In the **WIN-PAK CS SQL Version** screen, click **Next**. The **WIN-PAK CS SQL Server Authentication Dialog** box appears.

6. If you are logging on with **SQL Server Authentication**, provide the following details.
    a. **Instance Name** - The name of the SQL server.
    b. **User Name** - The user name which is used for accessing the SQL Server present in the database server. Using the user name 'sa' is not allowed. If you have already installed SQL server with username 'sa', then, the following message appears. **Username 'sa' is not allowed. New SQL server user named 'WPUSER' will be created to connect to SQL Server? Do you want to proceed?**
    c. **Password** - The password which is used for accessing the SQL Server present in the database server.
7. If you are logging on with **Windows Authentication**, then, the system automatically logs on using the Windows user name and password.

Note: If the previously installed SQL server is installed with connection type as **Windows Authentication only**, then, after the installation of WIN-PAK CS, it is changed to **Mixed Mode**.

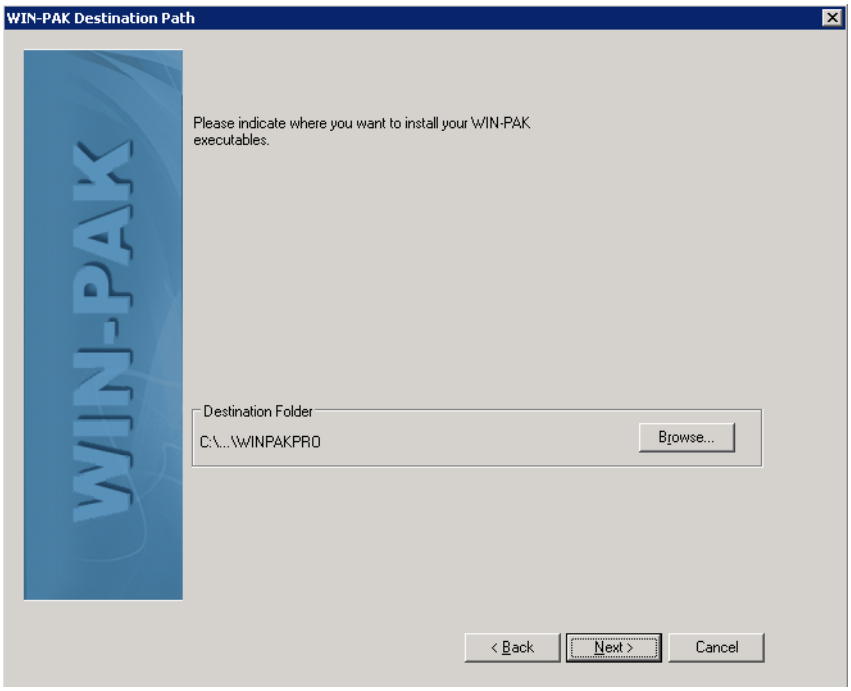
	Pre-installed SQL server (Windows authentication only)	**Pre-installed SQL server (Mixed mode)**	**SQL server Installation from WP (Mixed mode)**	**SQL server Installation from WP (Windows authentication only)**
Domain	X	✓	✓	✓
Work group	X	✓	✓	X **Note**: This works only on single server deployment.

X: Will work for the current setup.

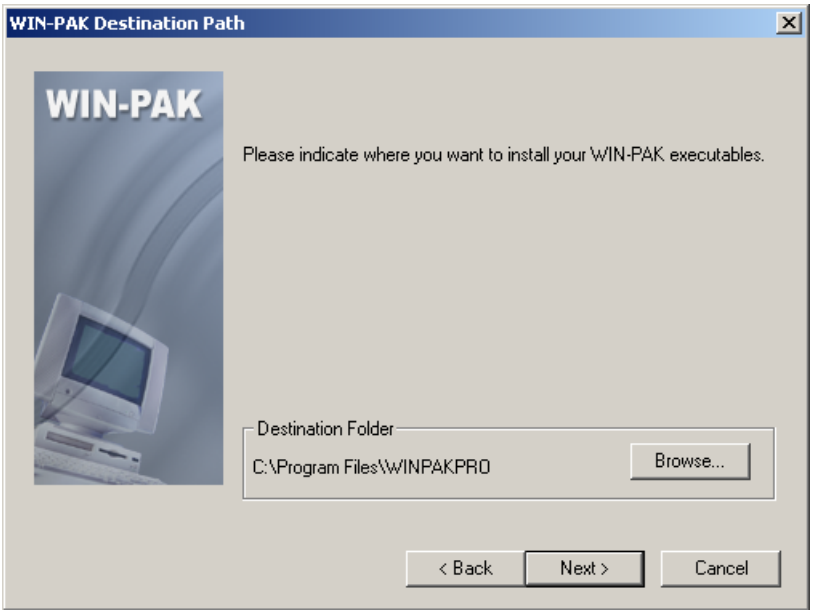
✓: Will not work for the current setup.

8. Follow the below given step for installing Complete WIN-PAK CS/SE/PE:

- **WIN-PAK CS:** Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file path.

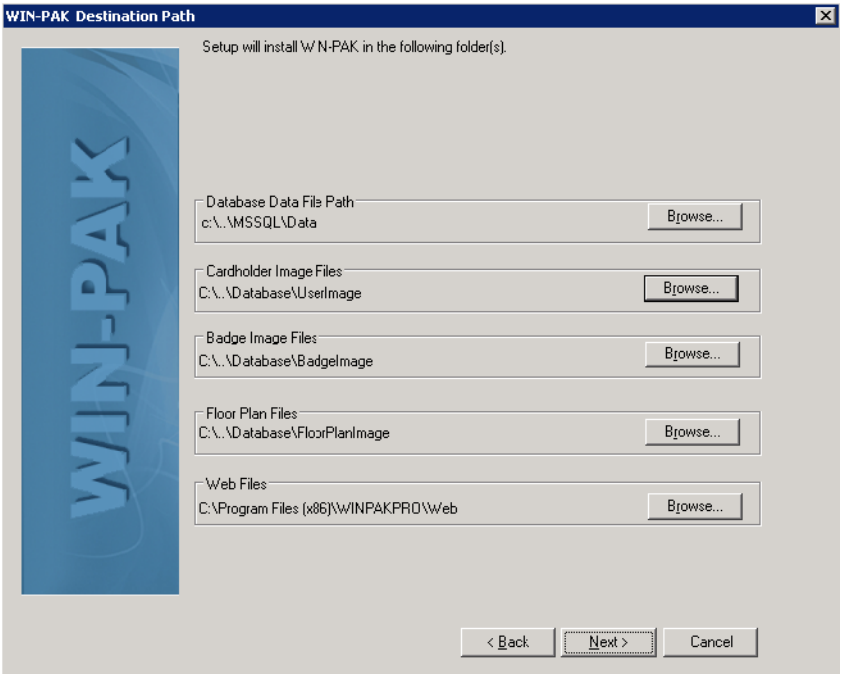


- **WIN-PAK SE/PE:** After performing instructions given in "To install WIN-PAK CS/SE/PE". On the **WIN-PAK SE/PE Setup Type** screen, select **Complete Installation** and click **Next**. The system checks for SQL Service status and display the following screen.



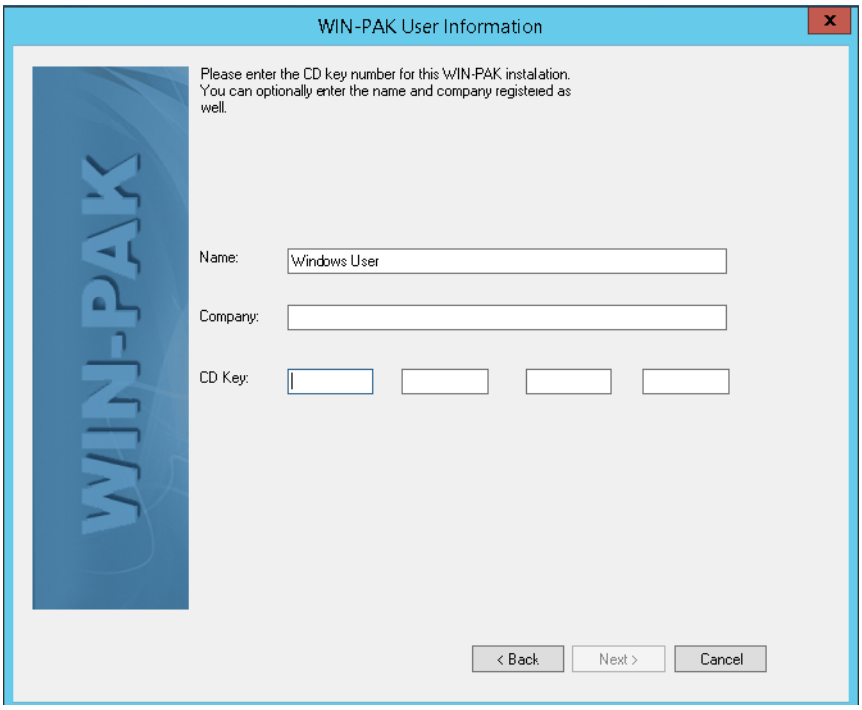
9. By default, the WIN-PAK CS/SE/PE application is installed in the C drive. To change the path, click **Browse** and navigate to the destination folder.

10. Click **Next**. The screen displays the WIN-PAK CS/SE/PE database file path.



11. To change the path, click **Browse** and navigate to the destination folder for each file.

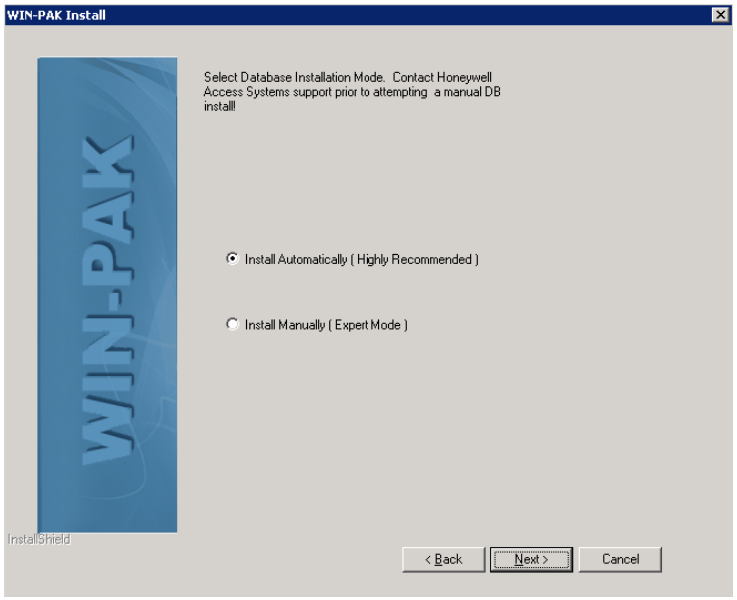
12. Click **Next**. The **User Information** screen appears.



13. Type your **Name**, **Company** and **CD Key** details. The CD Key is available on the front cover of the WIN-PAK CS/SE/PE Quick Reference Guide/DVD case.

14. Click **Next**. The setup verifies the CD key and displays a message of its validity.

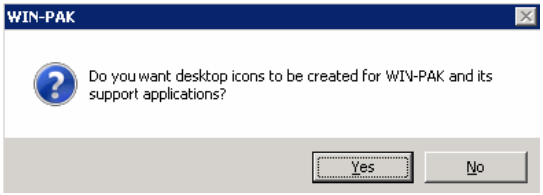
15. Click **OK.** The **Install** screen appears.



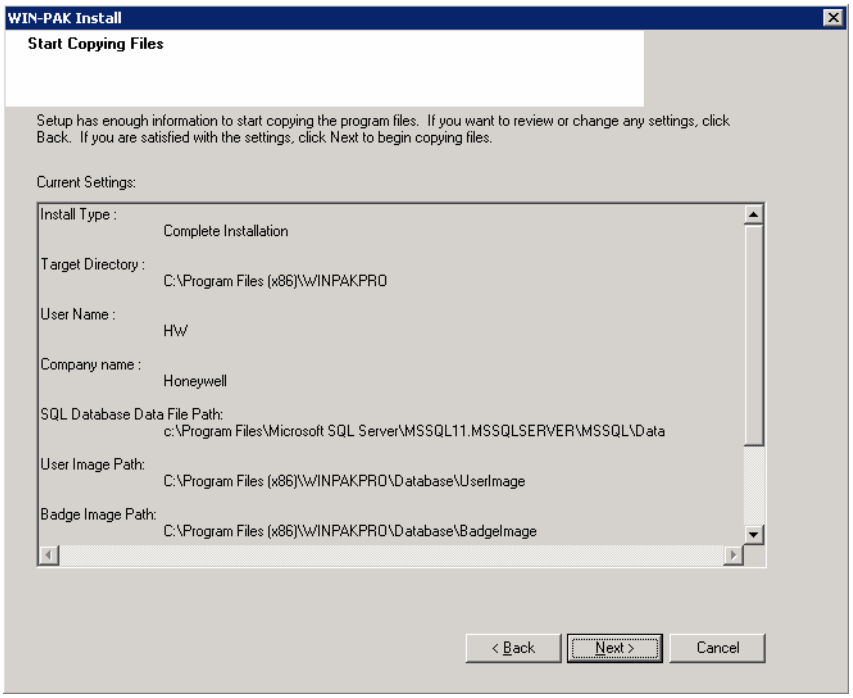
16. Select the installation mode as **Install Automatically** for an automatic installation.

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

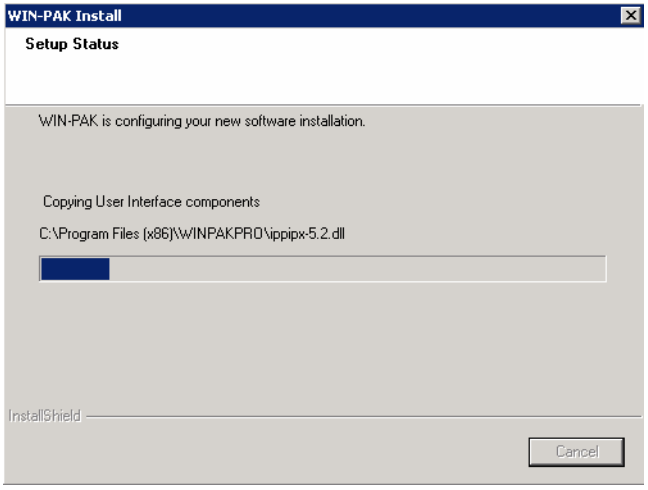
17. Click **Next**. A dialog box appears prompting you to create WIN-PAK CS/SE/PE shortcuts on your desktop.



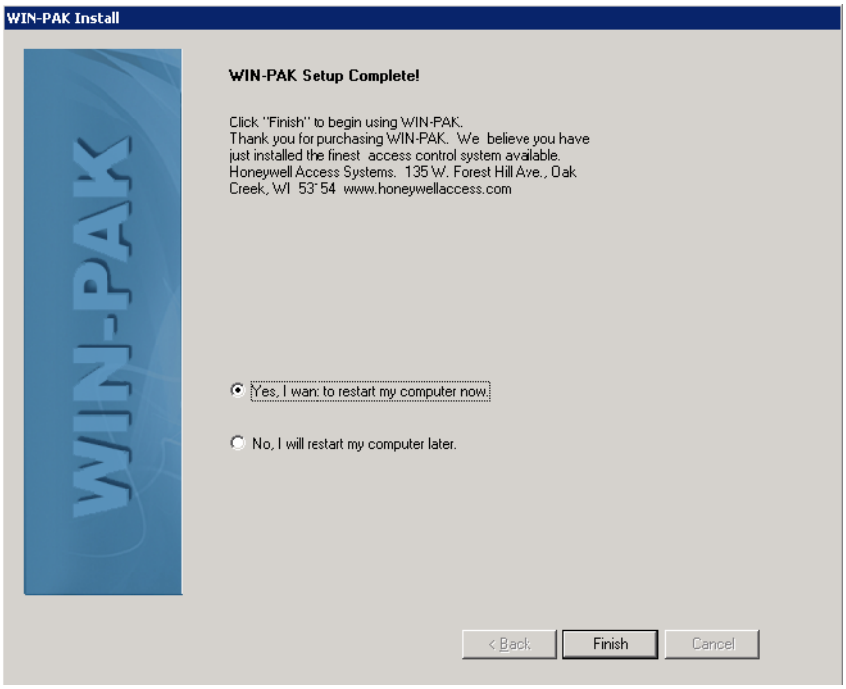
18. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



19. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



20. After completing the installation, the following screen appears.



21. 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.

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

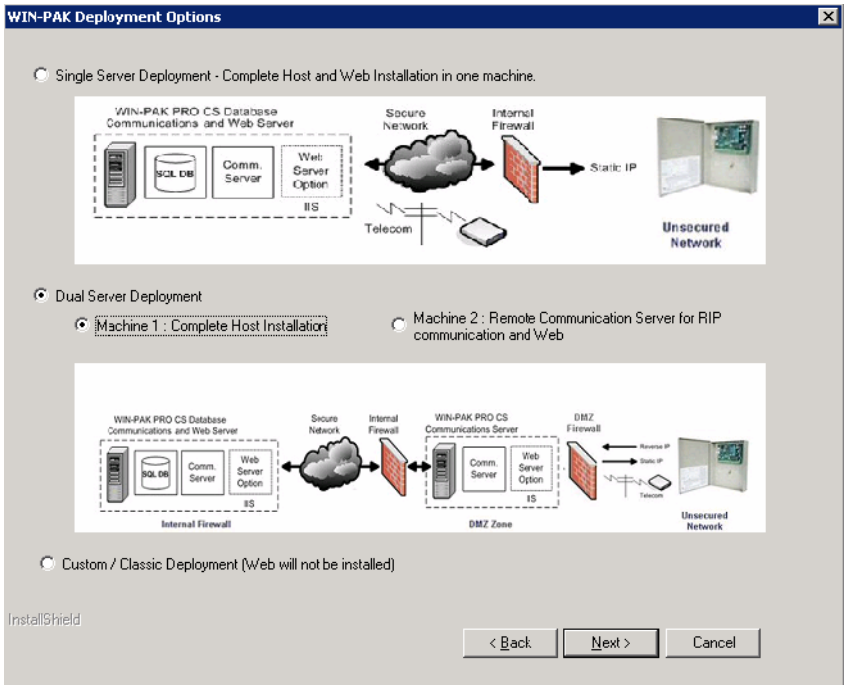
Installing Complete Host on Machine 1

You can install complete host on a single computer, that is, Machine 1.

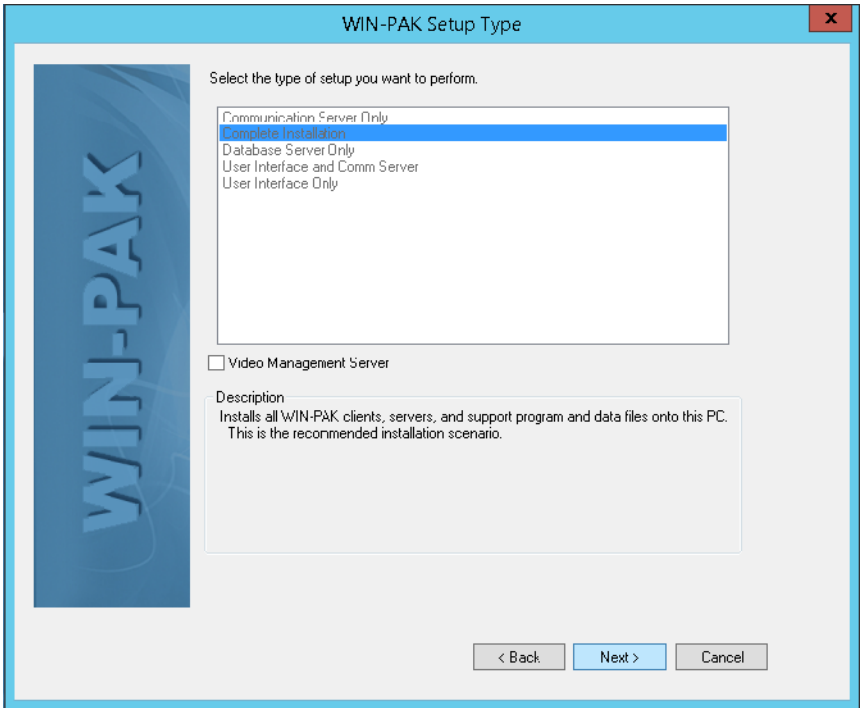
Notes:

- **Installing Complete Host on Machine 1** is applicable only for WIN-PAK CS.
- To install complete host on your computer, perform the instructions given in "To install WIN-PAK CS/SE/PE" and follow these steps:

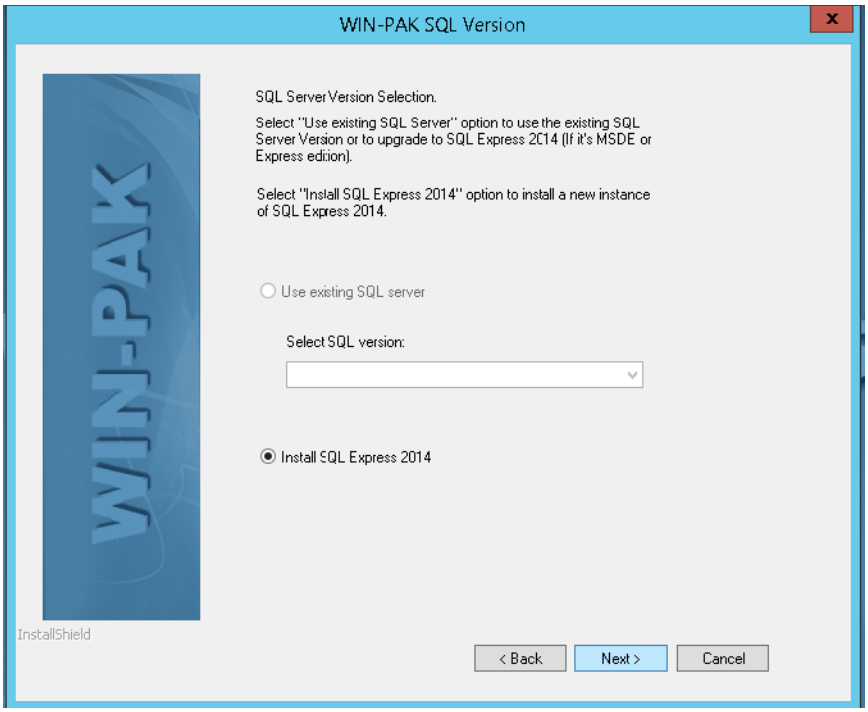
1. In the **WIN-PAK CS Deployment Options** screen, select **Dual Server Deployment - Machine 1 : Complete Host Installation**.



2. Click **Next**. The **WIN-PAK CS Setup Type** screen appears.



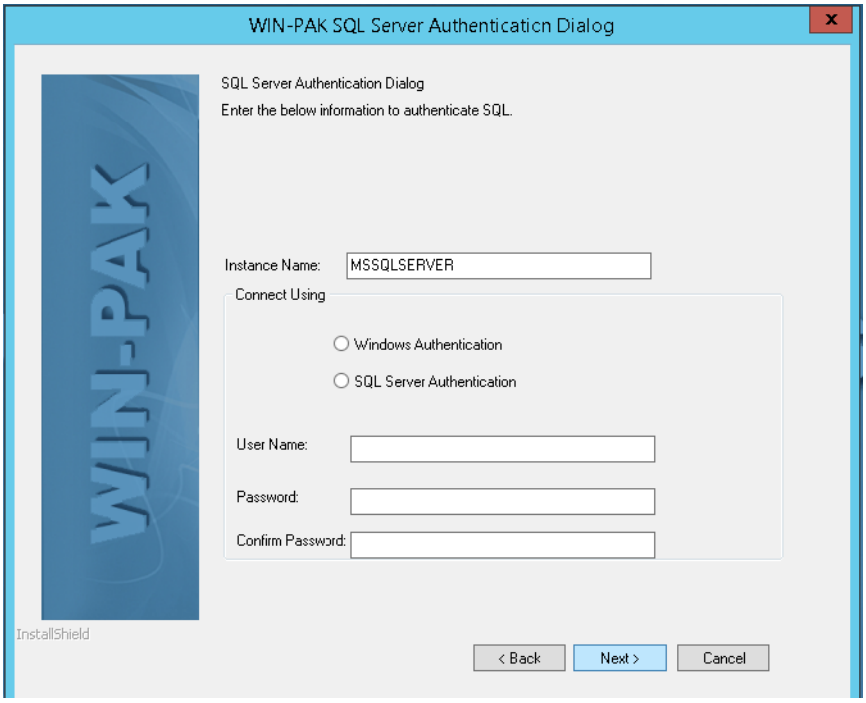
3. By default, the **Complete Installation** is selected. Click **Next**. The system checks for SQL Service status and displays the **WIN-PAK CS SQL Version** screen.



4. You can select:

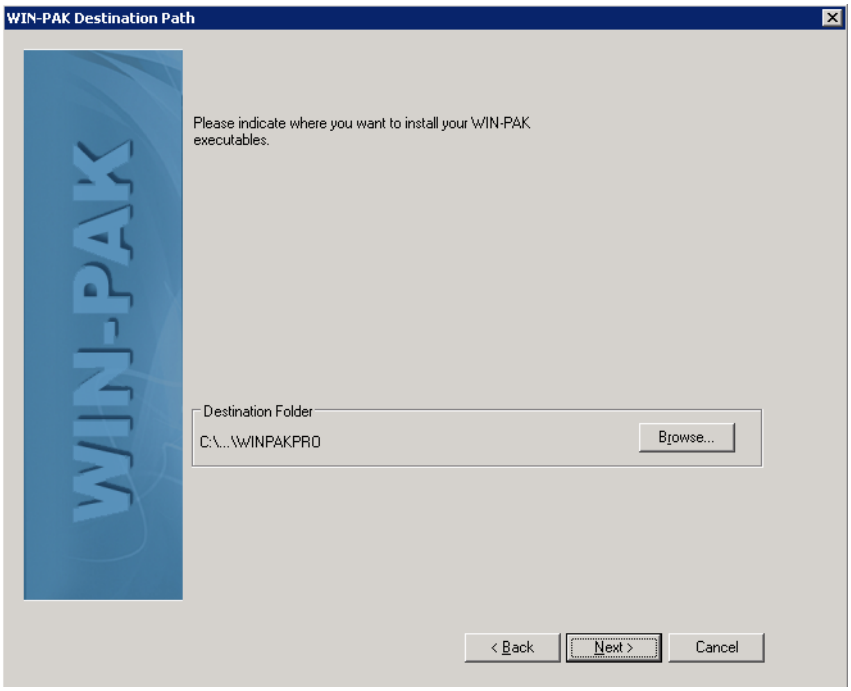
   - **Use existing SQL server** to use the existing SQL Server version or to upgrade to the SQL Express 2012 (if it is MSDE or Express Edition). You must **Select SQL Version** from the drop-down list.
   - **Install SQL Express 2012** to install a new instance of the SQL Express.

5. In the **WIN-PAK CS SQL Version** screen, click **Next**. The **WIN-PAK CS SQL Server Authentication Dialog** box appears.



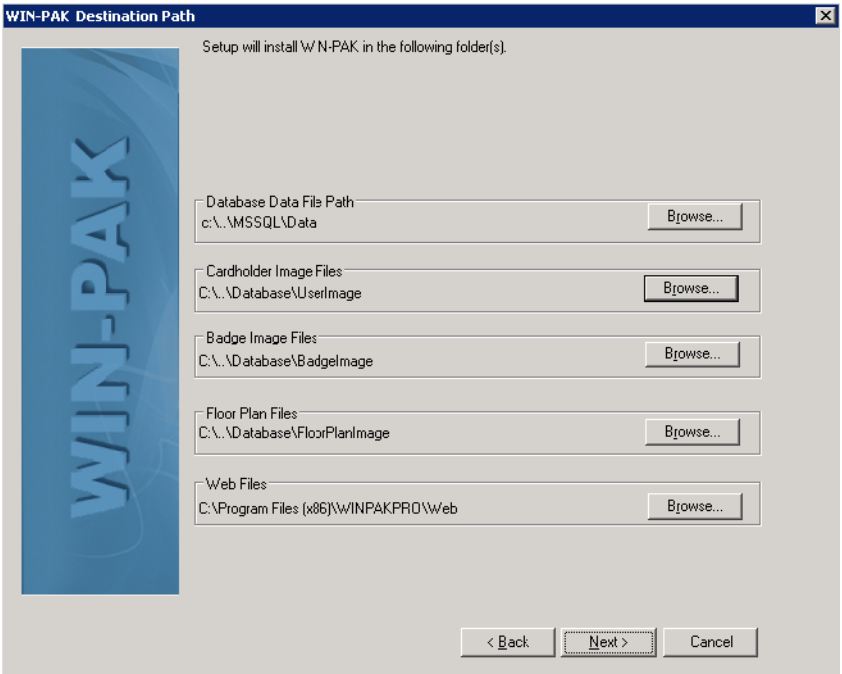
6. Provide the following details about the SQL server:
    a. **Instance Name** - The name of the SQL server.
    b. **User Name** - The user name which is used for accessing the SQL Server present in the database server.
    c. **Password** - The password which is used for accessing the SQL Server present in the database server.

7. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file path.

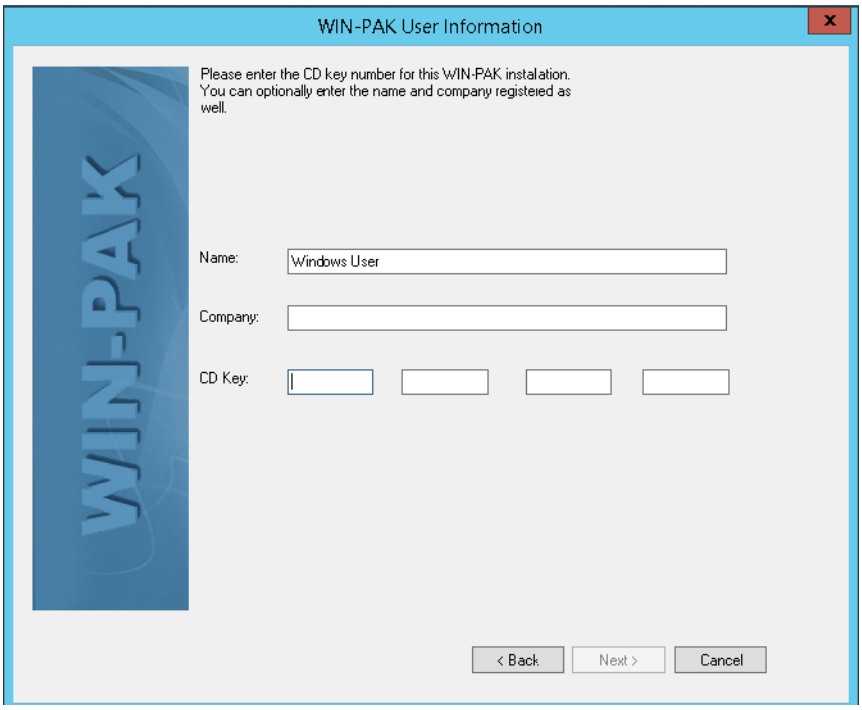


8. By default, the WIN-PAK CS application is installed in the C drive. If you want to change the installation folder, click **Browse** and specify a different destination folder.

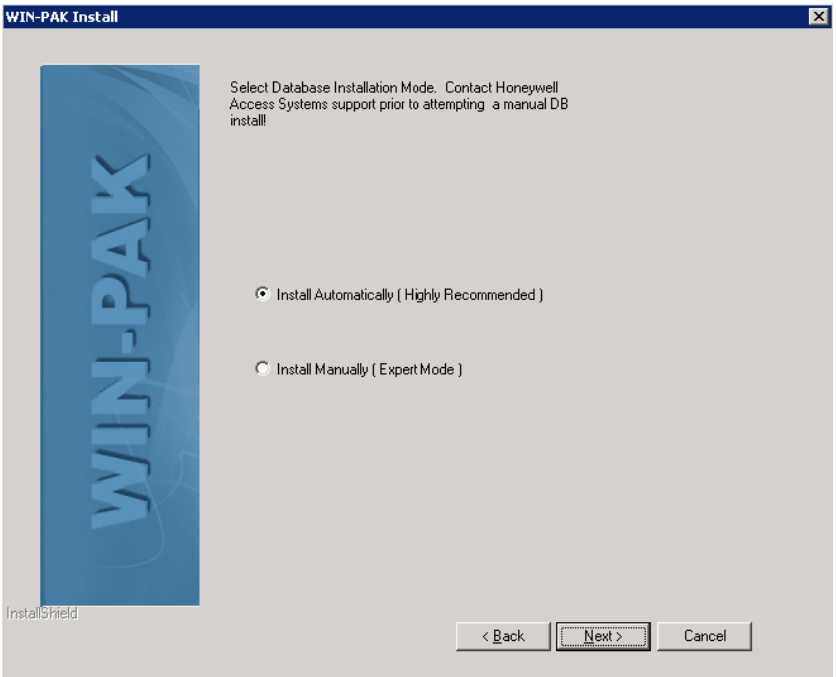
9. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file paths.



10. To change the path, click **Browse** and navigate to the destination folder for each file.
11. Click **Next**. The **WIN-PAK CS User Information** screen appears.



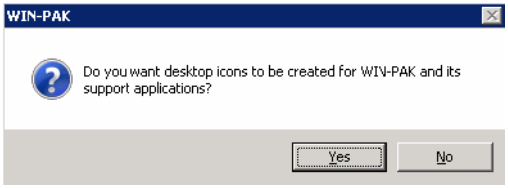
12. Type your **Name**, **Company** and **CD Key** details. The CD Key is found in the front cover of the WIN-PAK CS Quick Reference Guide.
13. Click **Next**. The **WIN-PAK CS Install** screen appears.



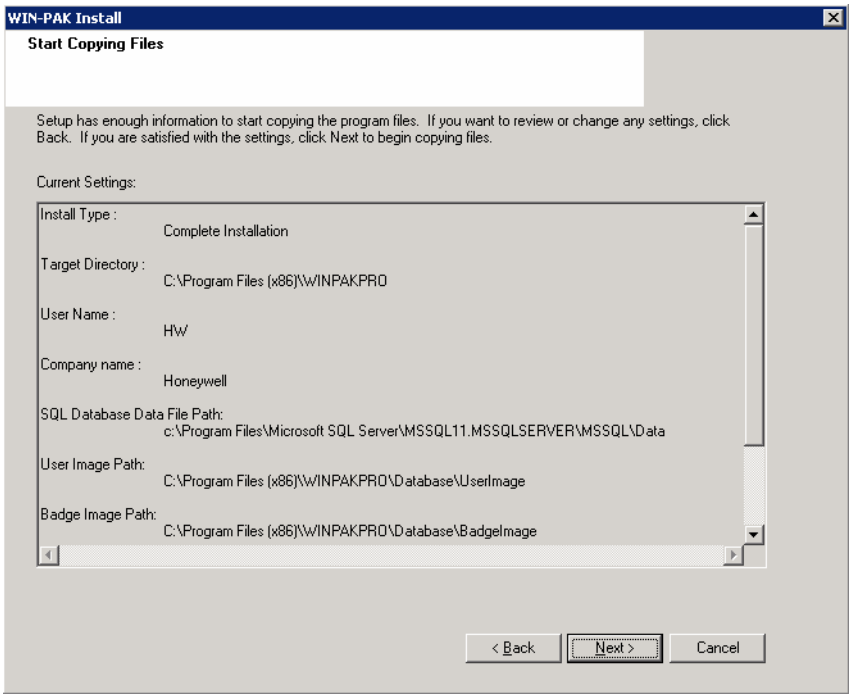
14. Select the installation mode as **Install Automatically** for an automatic installation.

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

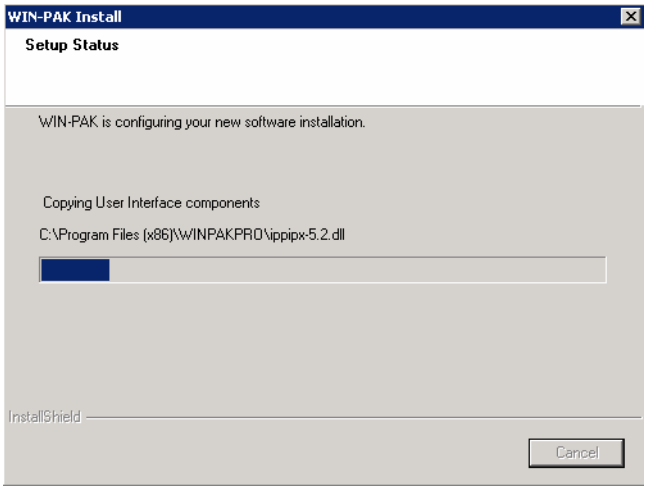
15. Click **Next**. A dialog box appears prompting you to create WIN-PAK CS shortcuts on your desktop.



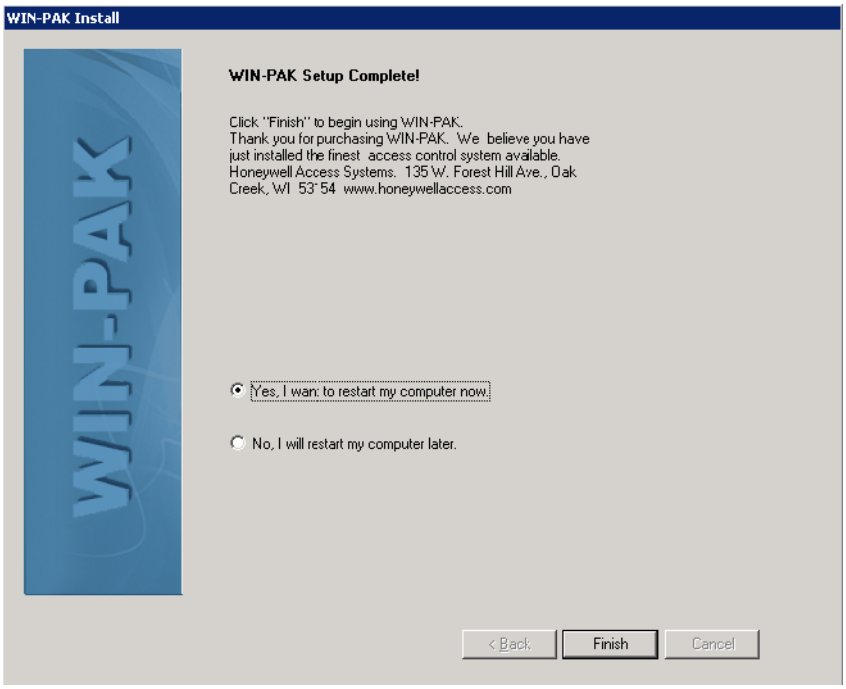
16. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



17. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



18. After completing the installation, the following screen appears.



19. 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.

20. Click **Finish**.

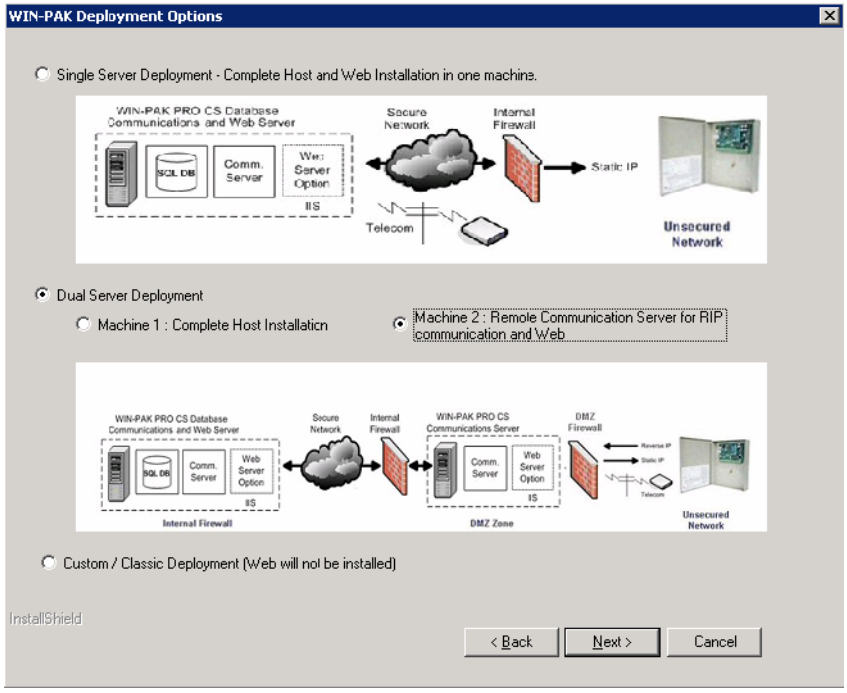
Installing Remote Communication Server and Web on Machine 2

You can install the remote communication server and web installation on a single computer, that is, Machine 2.

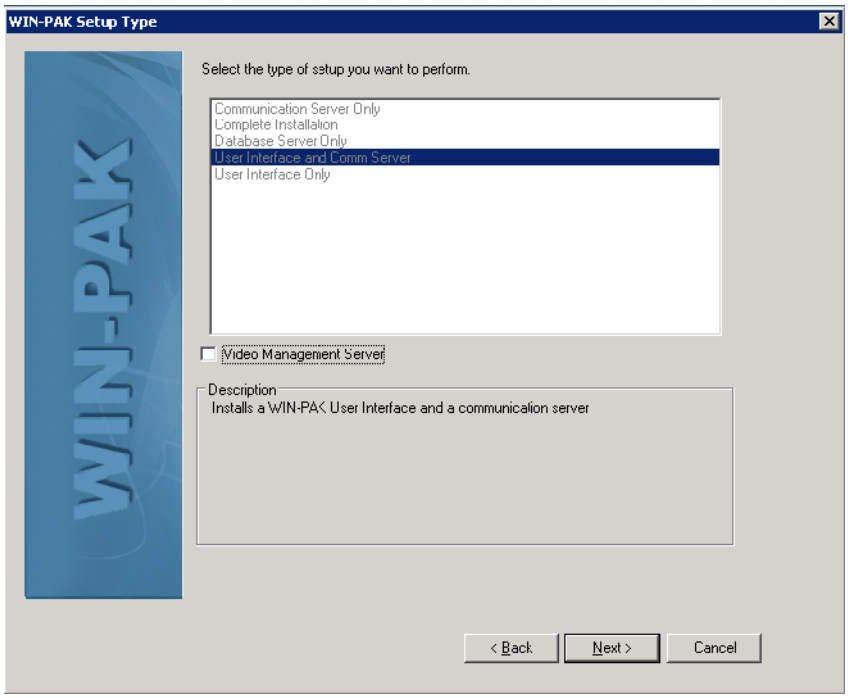
Notes:

- **Installing Remote Communication Server and Web on Machine 2** is applicable only for WIN-PAK CS.
- To install the remote communication server and web on your computer, perform the instructions given in "To install WIN-PAK CS/SE/PE" and follow these steps:

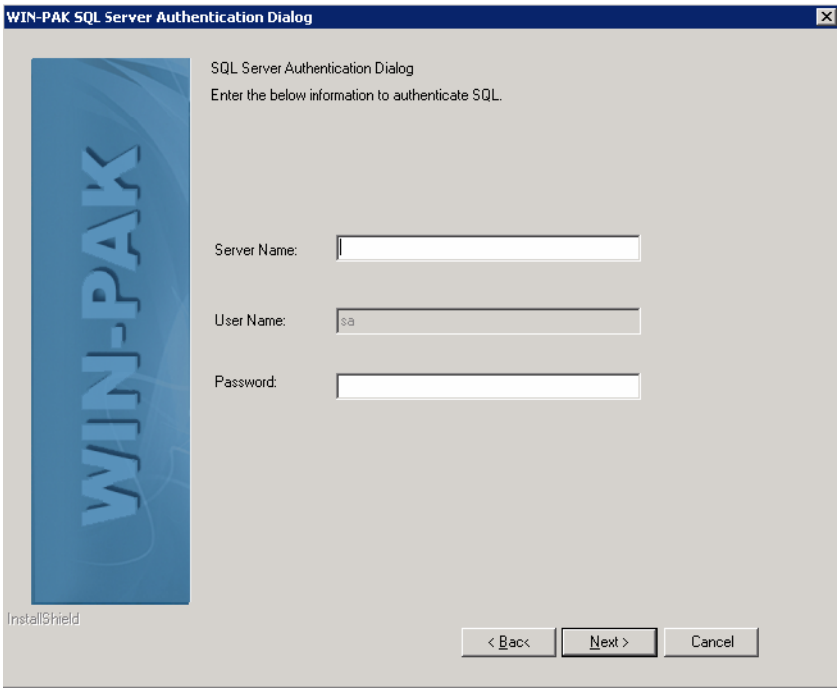
1. In the **WIN-PAK CS Deployment Options** screen, select **Dual Server Deployment - Machine 2 : Remote Communication Server for RIP communication and Web**.



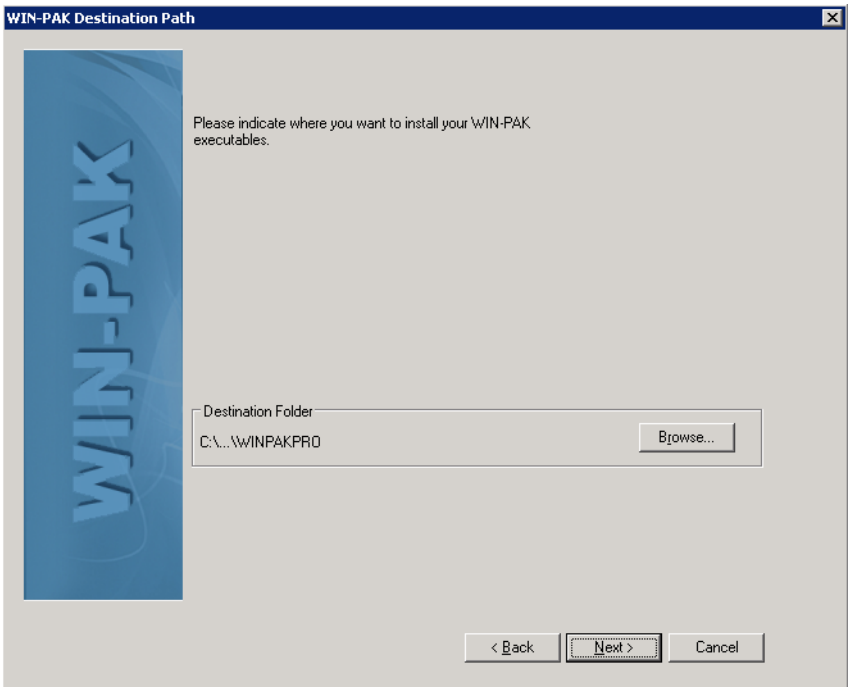
2. Click **Next**. The **WIN-PAK CS Setup Type** screen appears.



3. By default, the **User Interface and Comm Server** is selected. Click **Next**. The system checks for SQL Service status and displays the **WIN-PAK CS SQL Server Authentication Dialog** screen.

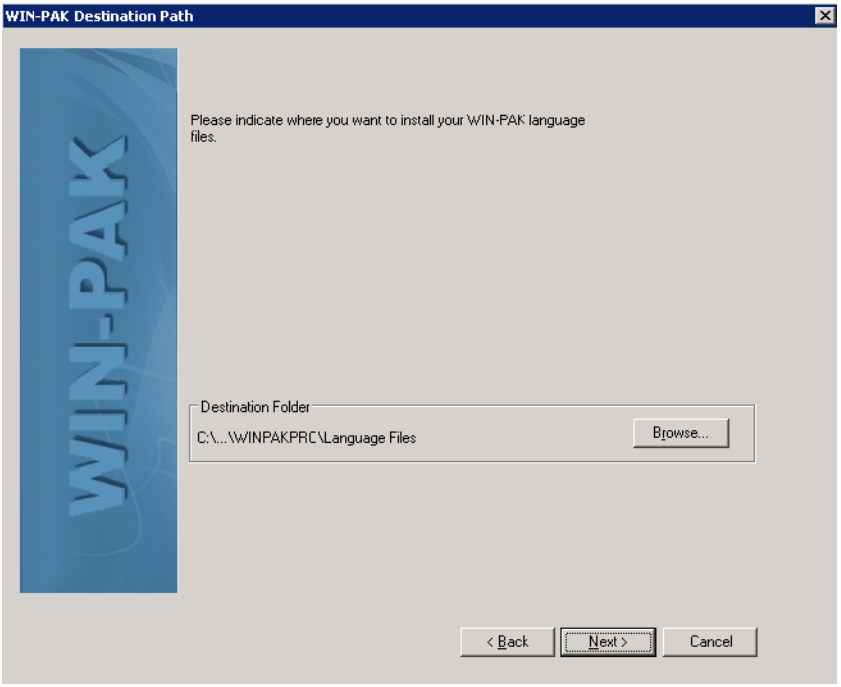


4. Provide the following details about the SQL server in Machine 1:
    a. **Server Name** - The the server name of the SQL server which is installed in Machine 1. You can also provide the IP address of Machine 1.
    b. **User Name** - The user name which is used for accessing the SQL Server present in Machine 1.
    c. **Password** - The password which is used for accessing the SQL Server present in Machine 1.
5. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file path.



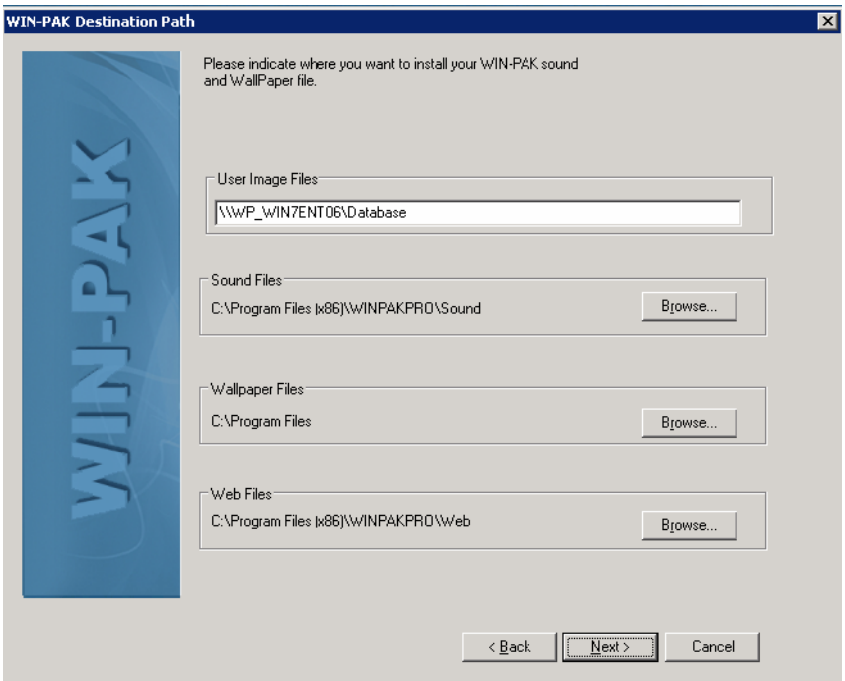
6. By default, the WIN-PAK CS application is installed in the C drive. If you want to change the installation folder, click **Browse** and specify a different destination folder.

7. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS language file path.



8. By default, the WIN-PAK CS language files are installed in the C drive. If you want to change the installation folder, click **Browse** and specify a different destination folder.

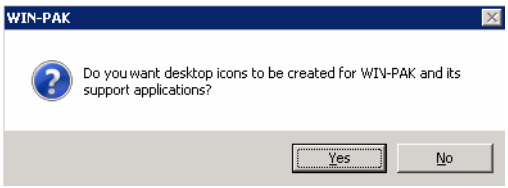
9. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS sound and wallpaper file paths.



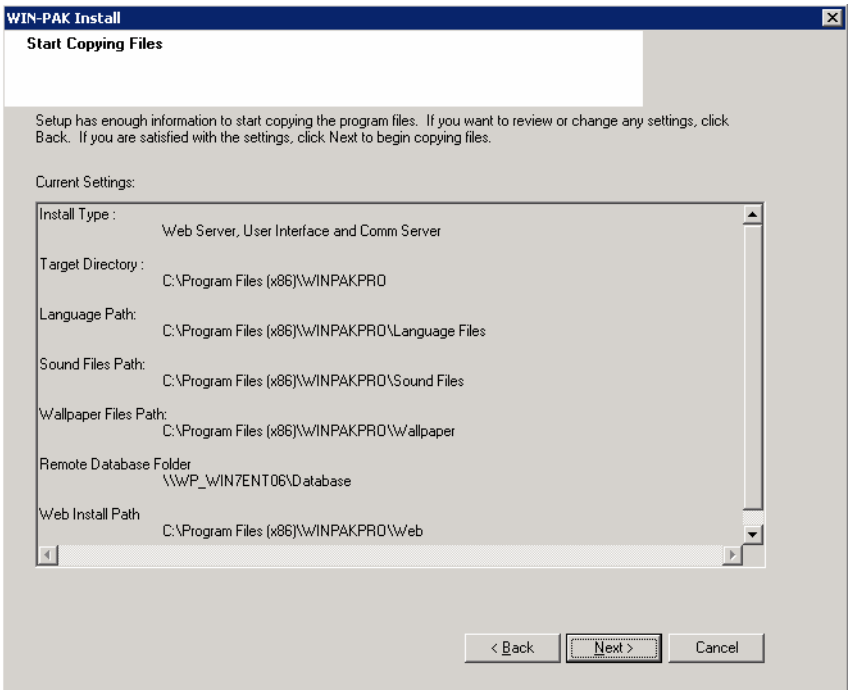
10. To change the path, click **Browse** and navigate to the destination folder for each file.

Note: The **User Image Files** path must match the IP address of Machine 1.

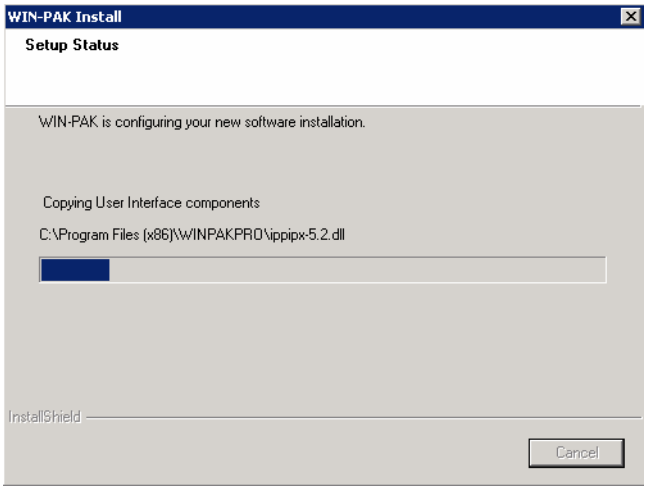
11. Click **Next**. A dialog box appears prompting you to create WIN-PAK CS shortcuts on your desktop.



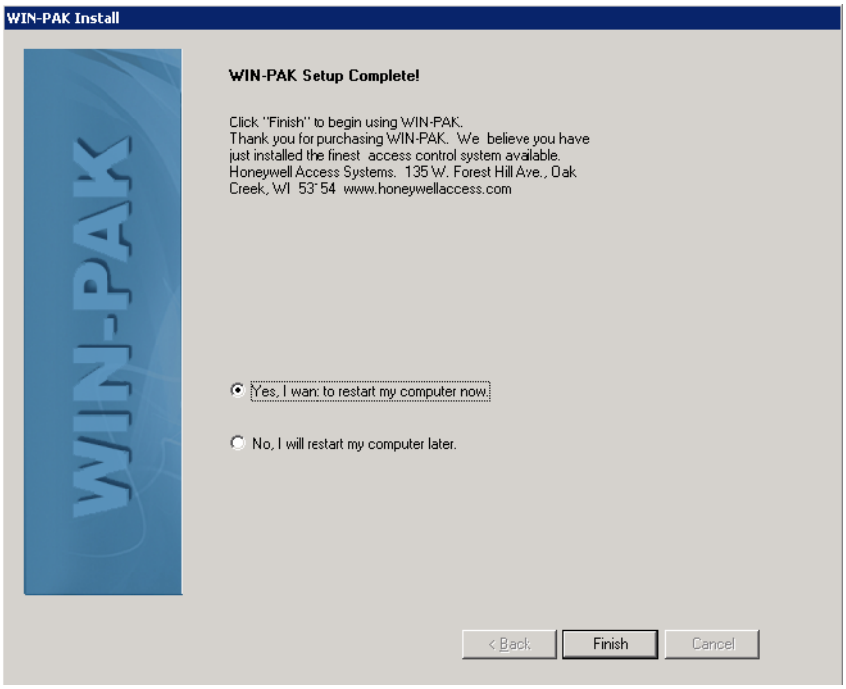
12. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



13. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



14. After completing the installation, the following screen appears.



15. 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.

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

Installing Database Server for WIN-PAK CS/SE/PE

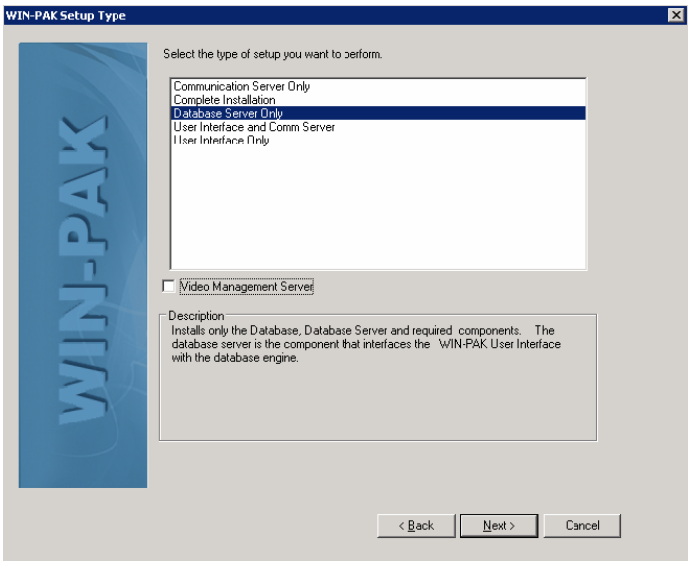
You can install the database server on a computer connected to a network.

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

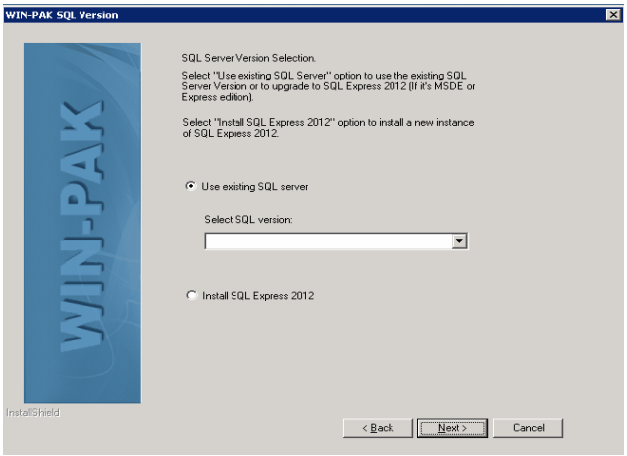
Notes:

- To install Complete WIN-PAK CS, follow steps from 1 to 23.
- To install Complete WIN-PAK SE/PE, follow steps from 12 to 23.
- WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

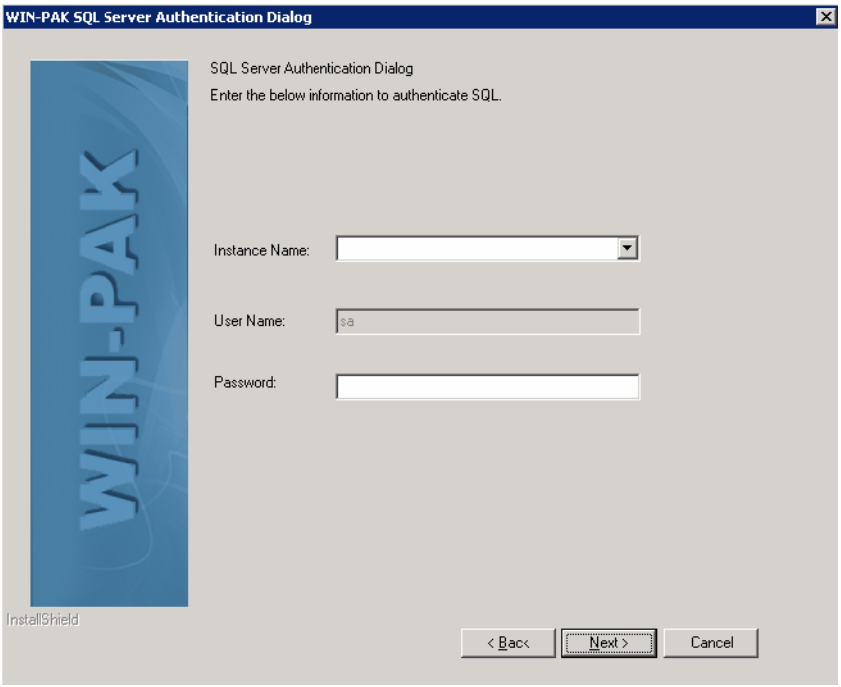
1. On the **WIN-PAK CS Setup Type** screen, select **Database Server Only** and click **Next**.



2. The system checks for SQL Service status and displays the **WIN-PAK CS SQL Version** screen.

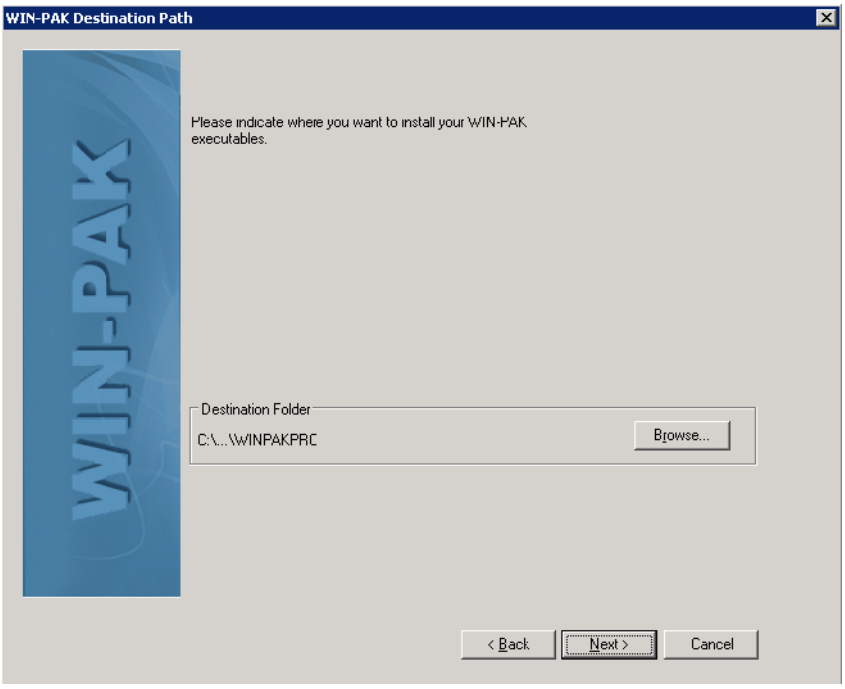


3. You can select:
    - **Use existing SQL server** to use the existing SQL Server version or to upgrade to the SQL Express 2012 (if it is MSDE or Express Edition). You must **Select SQL Version** from the drop-down list.
    - **Install SQL Express 2012** to install a new instance of the SQL Express.
4. In the **WIN-PAK CS SQL Version** screen, click **Next**. The **WIN-PAK CS SQL Server Authentication Dialog** box appears.



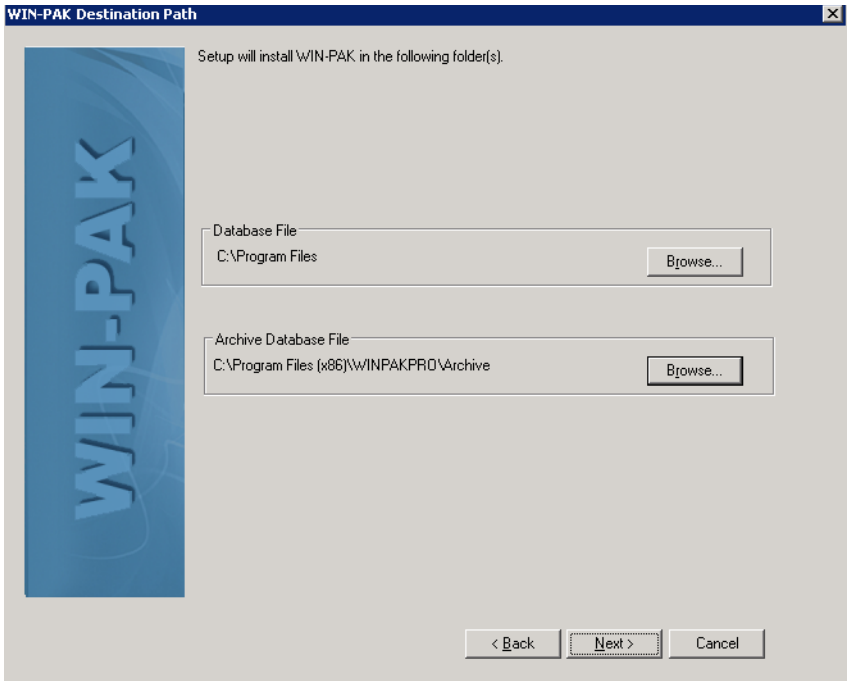
5. Provide the following details about the SQL server:
    a. **Instance Name** - The name of the SQL server.
    b. **User Name** - The user name which is used for accessing the SQL Server present in the database server.
    c. **Password** - The password which is used for accessing the SQL Server present in the database server.

6. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file path.

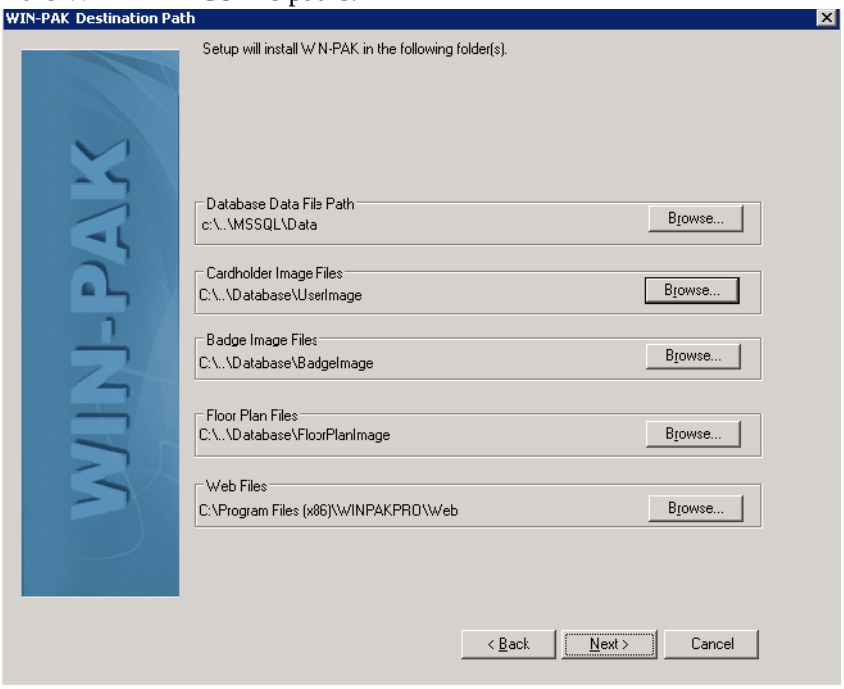


7. By default, the WIN-PAK CS application is installed in the C drive. If you want to change the installation folder, click **Browse** and specify a different destination folder.

8. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS database and archive database file paths.

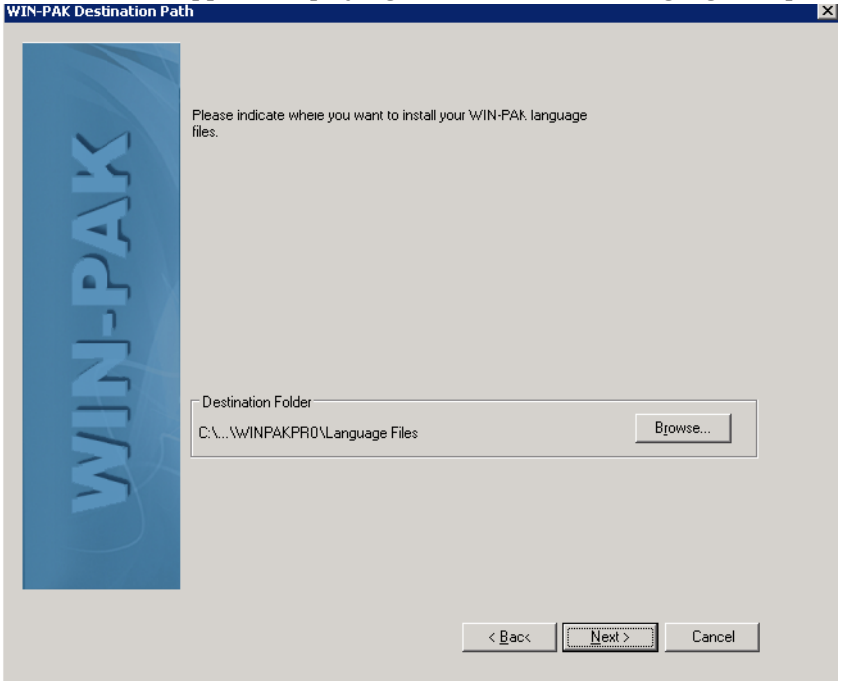


9. To change the path, click **Browse** and navigate to the destination folder for each file.
10. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file paths.

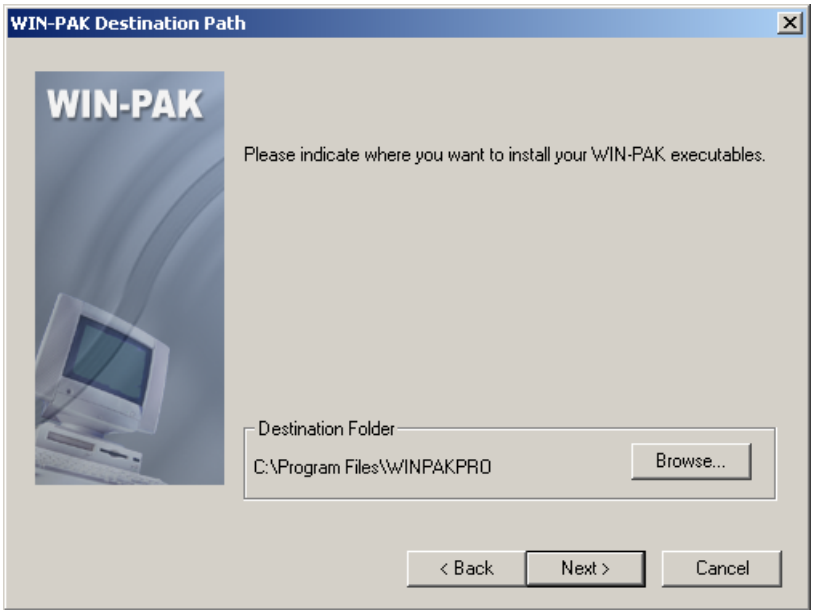


11. To change the path, click **Browse** and navigate to the destination folder for each file.
12. Follow the below given step for installing database server for WIN-PAK CS/SE/PE:

- **WIN-PAK CS:** Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS language file path.

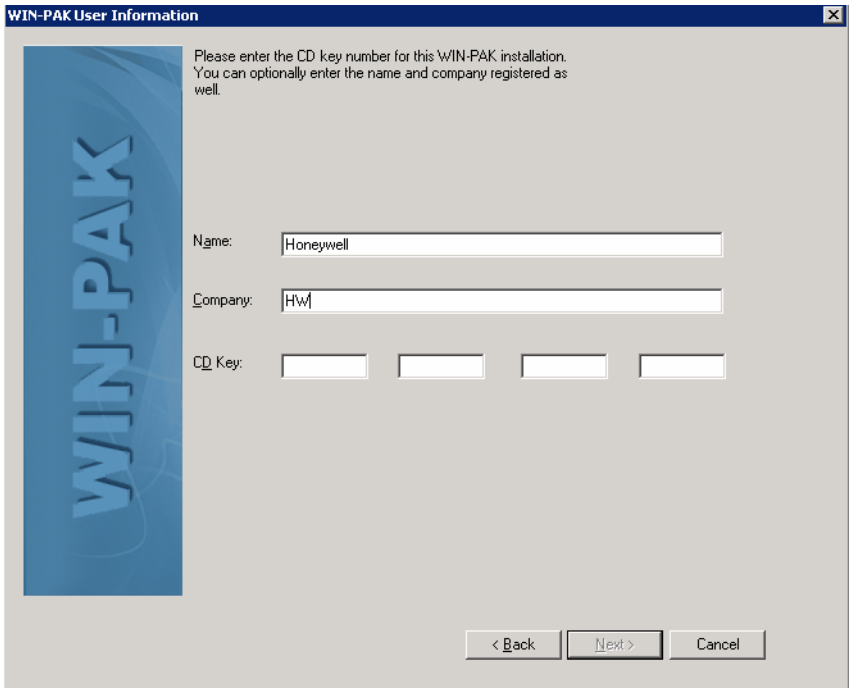


- **WIN-PAK SE/PE:** After performing instructions given in "To install WIN-PAK CS/SE/PE". On the WIN-PAK SE/PE Setup Type screen, select Database Server Only and click Next. The system checks for SQL Service status and displays the below screen.

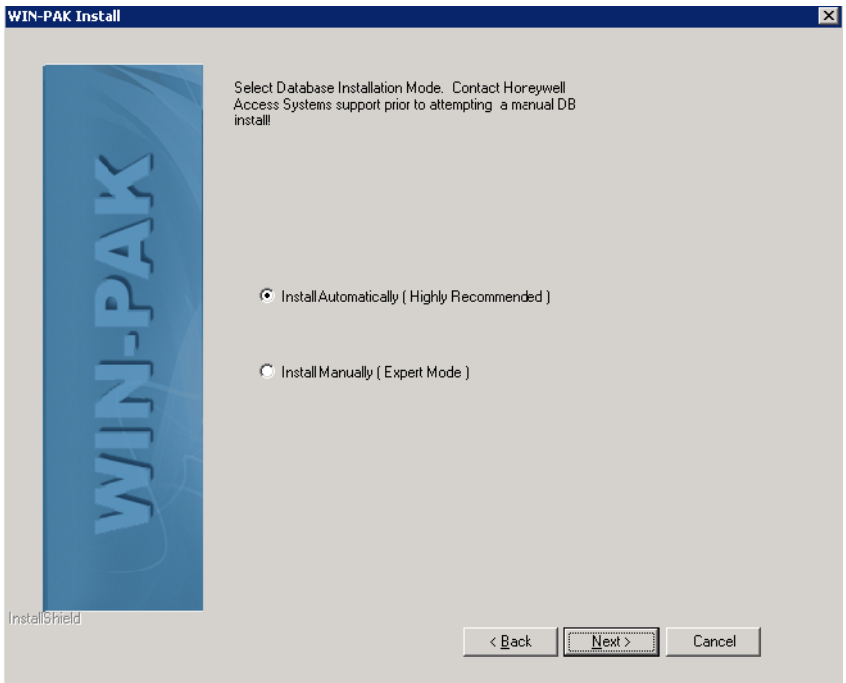


13. To change the path, click **Browse** and navigate to the destination folder for the file.

14. Click **Next**. The **User Information** screen appears.



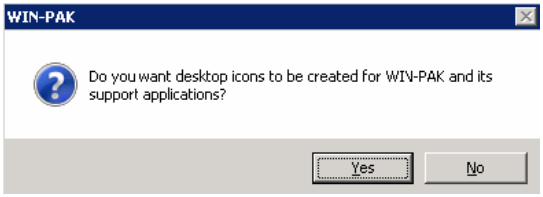
15. Type your **Name**, **Company** and **CD Key** details. The CD Key is found in the front cover of the Quick Reference Guide/DVD case.
16. Click **Next**. The setup verifies the CD key and displays the message for validity.
17. Click **OK**. The **WIN-PAK CS/SE/PE Install** screen appears.



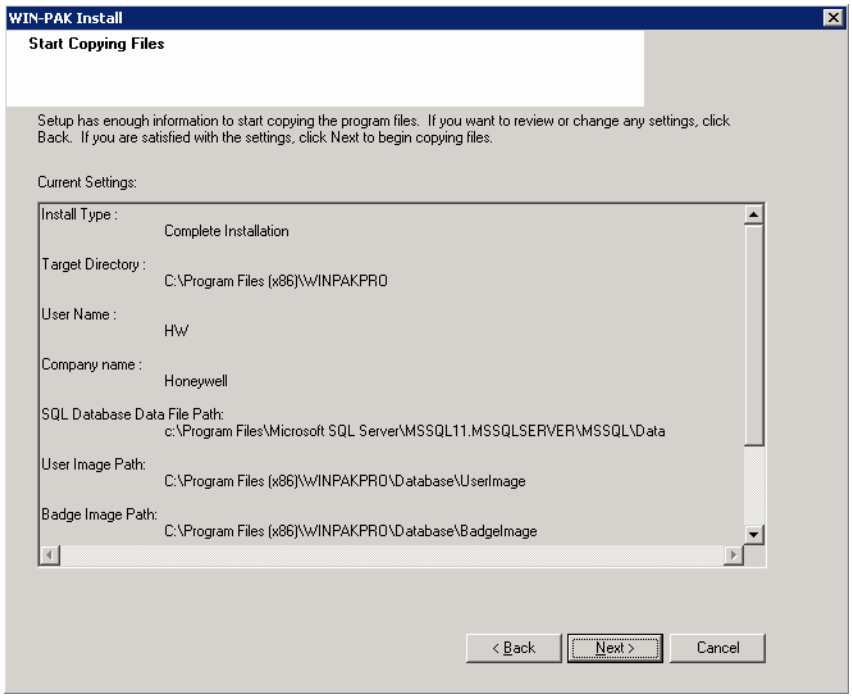
18. Select the installation mode as **Install Automatically** for an automatic installation.

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

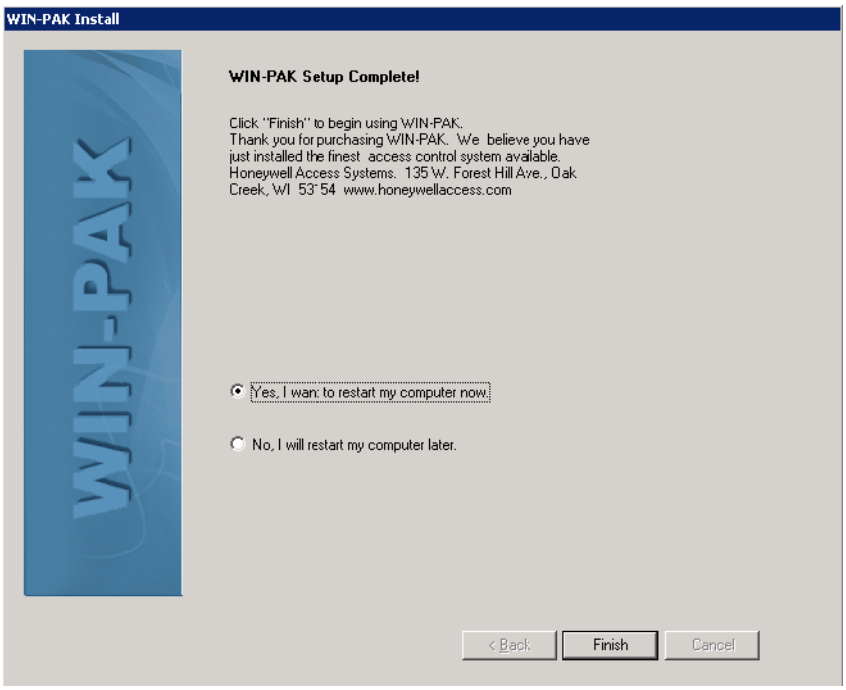
19. Click **Next**. A dialog box appears prompting you to create shortcuts on your desktop.



20. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



21. Click **Back** to change any installation settings, or click **Next**. The software is installed and then **WIN-PAK CS/SE/PE** dialog box appears.



22. 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.

23. Click **Finish**.

Installing User Interface for WIN-PAK CS/SE/PE

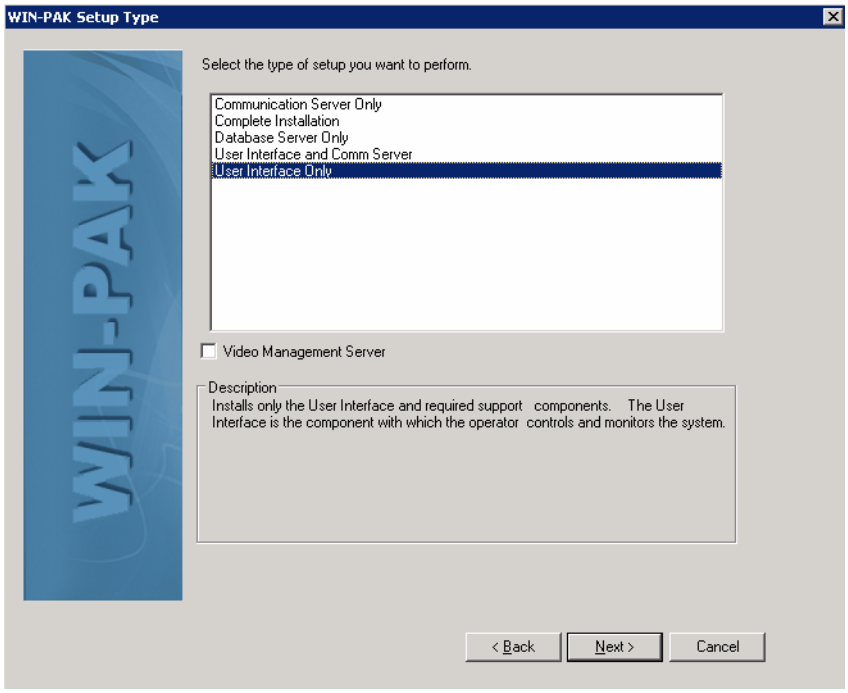
The User Interface is installed at each workstation across the Local Area Network (LAN).

Notes:

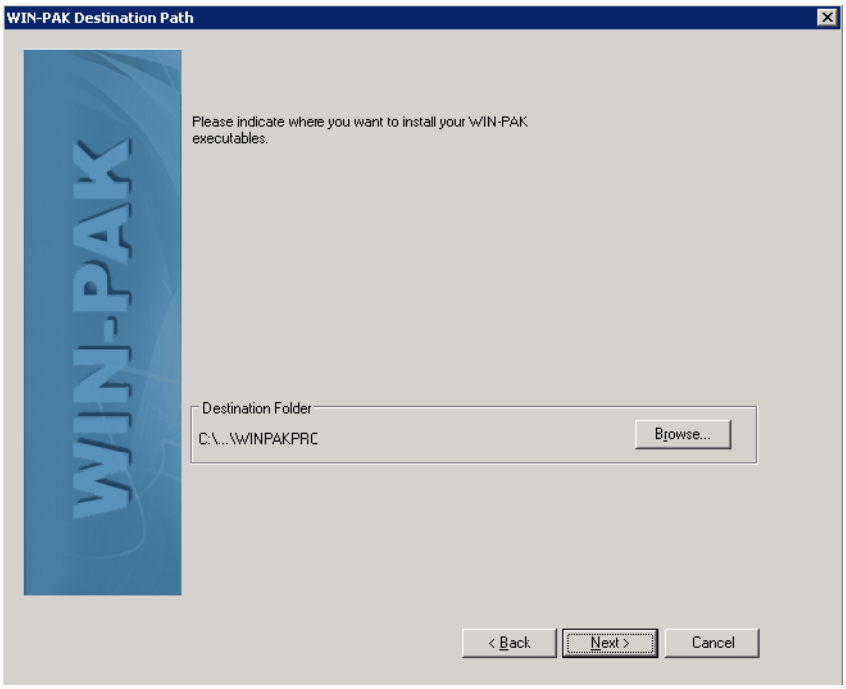
- While installing the User Interface at a workstation on a LAN, ensure that the installation directory resides on a shared drive mapped in the target system. If not, the installation fails, when the system reboots and attempts to re-establish connection with the host directory.
- WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

To install only the WIN-PAK CS/SE/PE User Interface, perform the instructions given in "To install WIN-PAK CS/SE/PE", and then follow these steps:

1. On the **WIN-PAK CS/SE/PE Setup Type** screen, select **User Interface Only** and click **Next**.

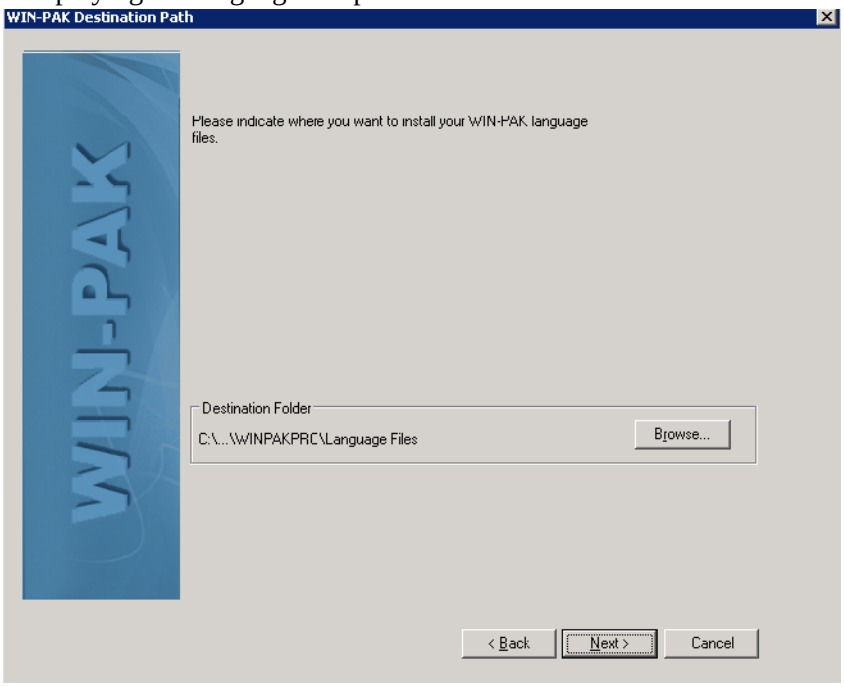


2. The system displays the **WIN-PAK CS/SE/PE Destination Path** screen.



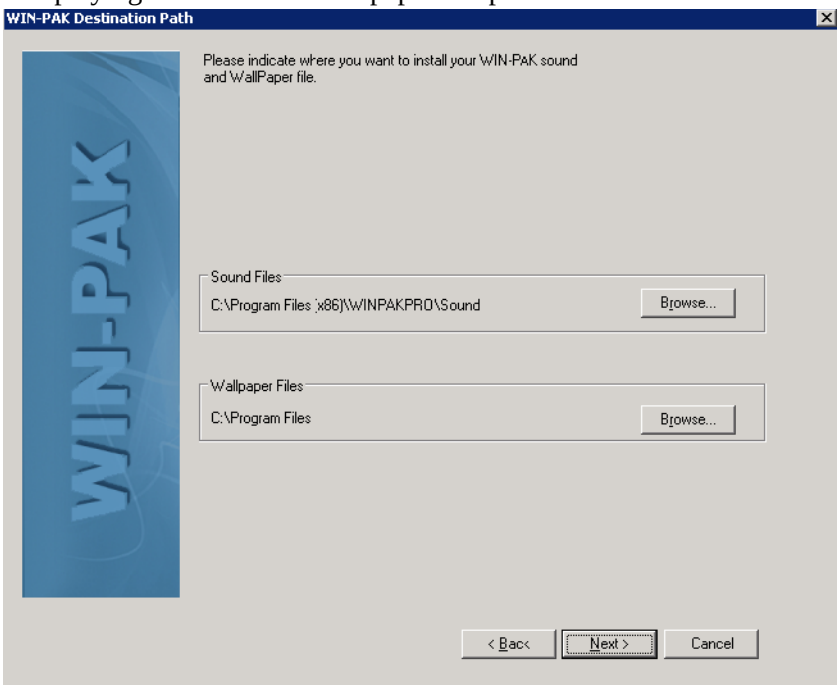
3. To change the path, click **Browse** and navigate to the destination folder for the application.

4. Click **Next**. The **WIN-PAK CS/SE/PE Destination Path** screen appears displaying the language file path.



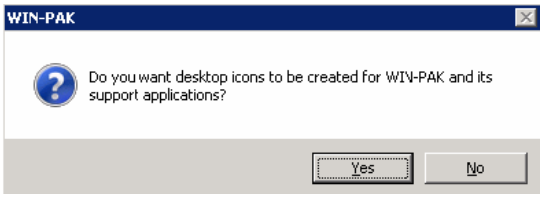
5. To change the path, click **Browse** and navigate to the destination folder for the file.

6. Click **Next**. The **WIN-PAK CS/SE/PE Destination Path** screen appears displaying the sound and wallpaper file paths.

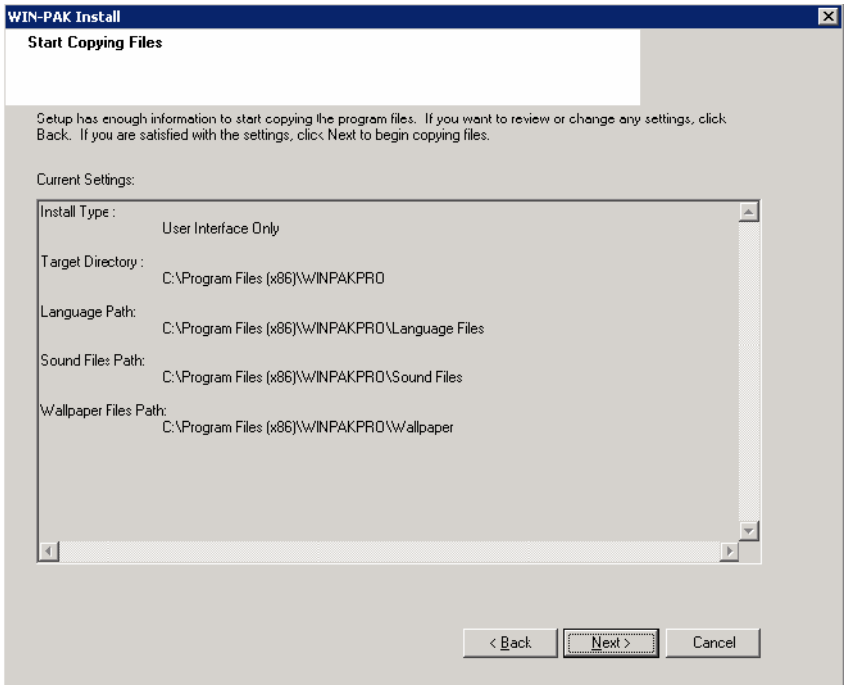


7. To change the path, click **Browse** and navigate to the destination folder for each file.

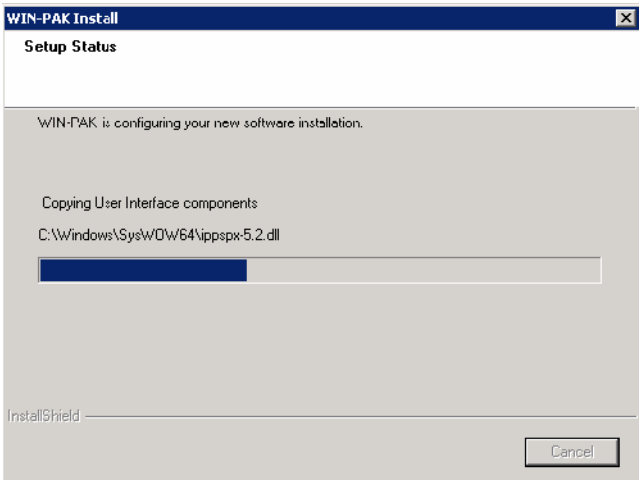
8. Click **Next**. A dialog box appears prompting you to create shortcuts on your desktop.



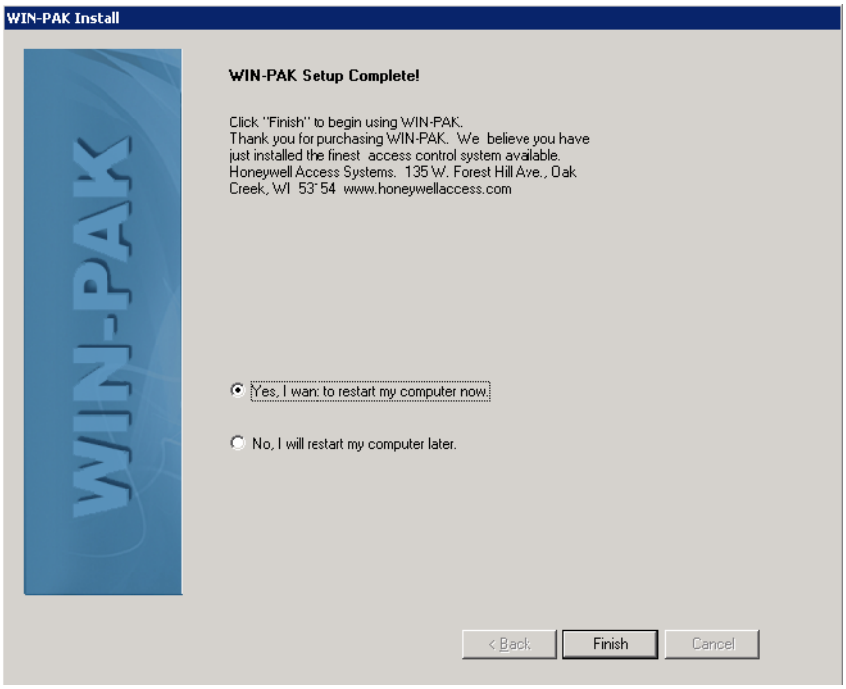
9. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



10. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



11. After completing the installation, the following screen appears.



12. 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.

13. Click **Finish**.

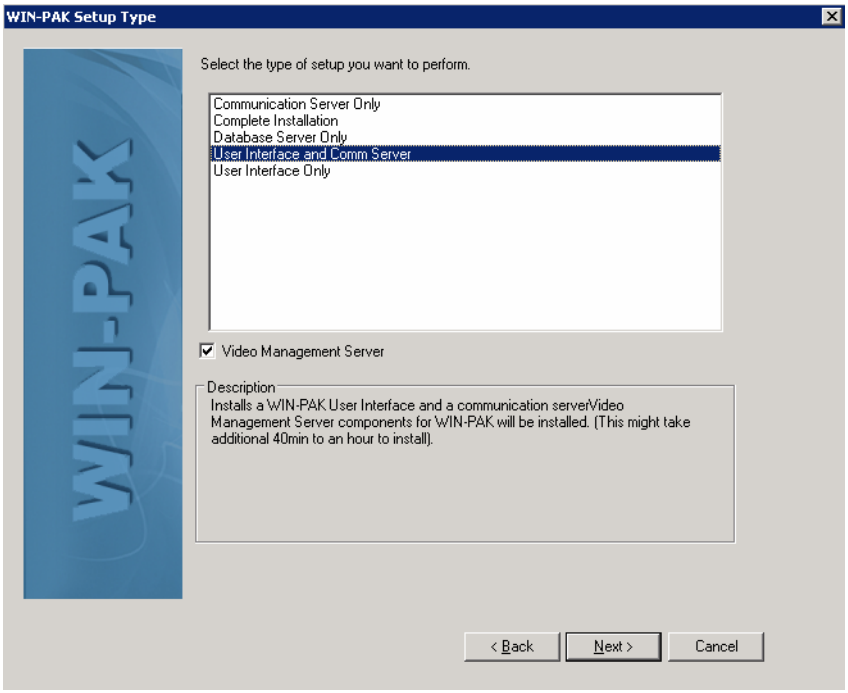
Installing UI and Communication Server for WIN-PAK CS/SE/PE

To install WIN-PAK CS/SE/PE UI and Communication Server, perform the instructions given in "To install WIN-PAK CS/SE/PE", and follow these steps:

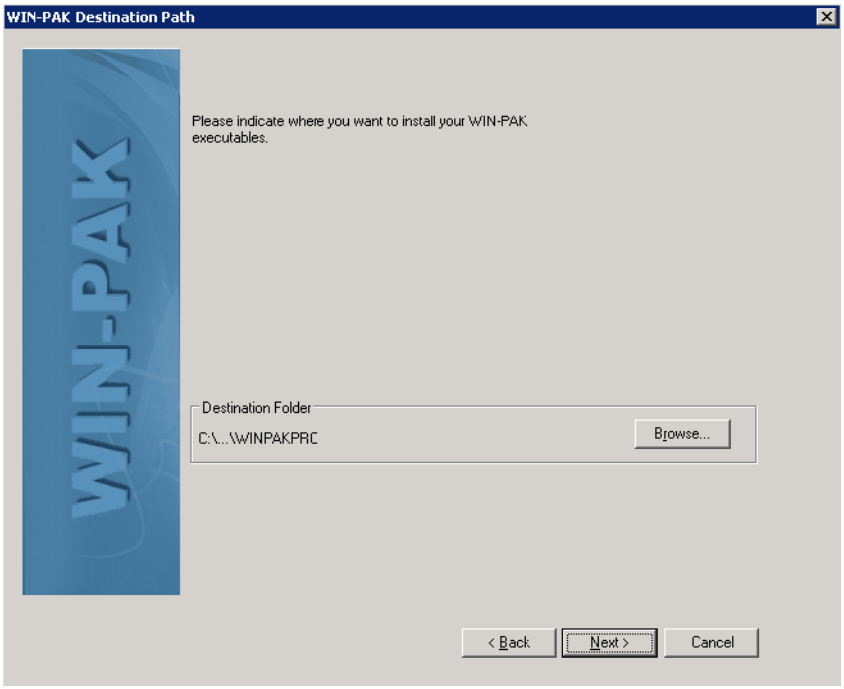
Note:

WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

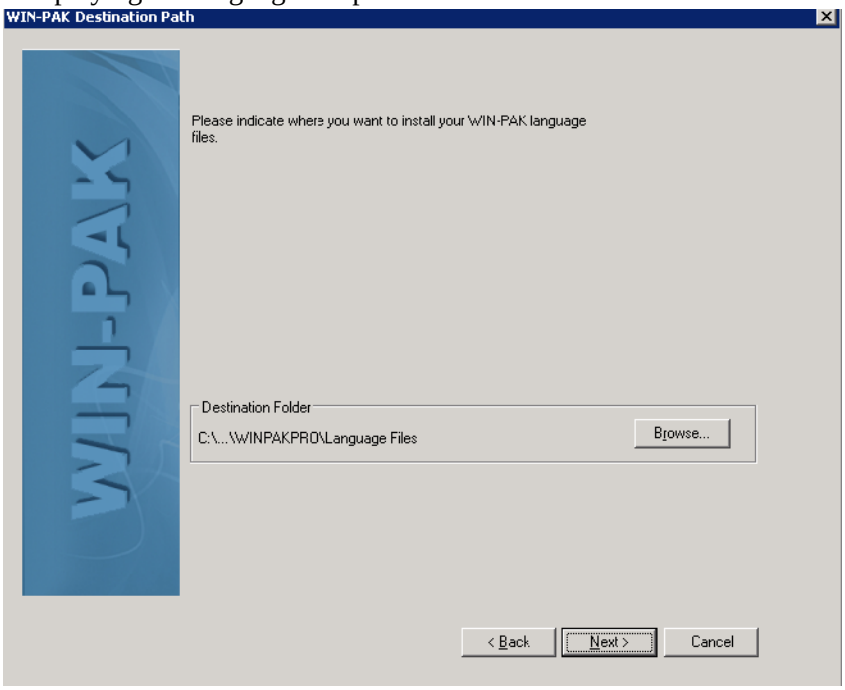
1. On the **WIN-PAK CS/SE/PE Setup Type** screen, select **User Interface and Comm Server** and click **Next**.



2. The system displays the **WIN-PAK CS/SE/PE Destination Path** screen.

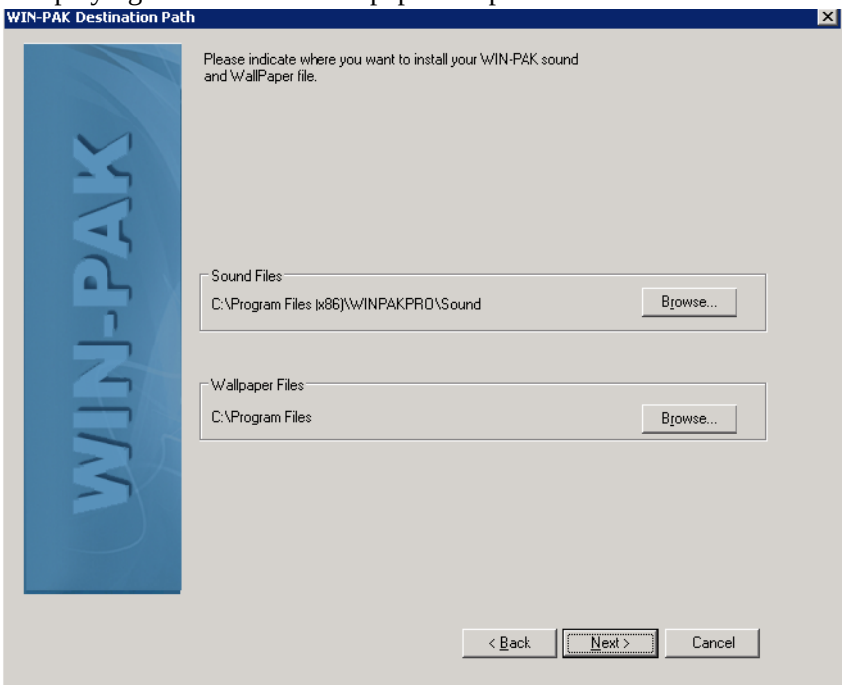


3. To change the path, click **Browse** and navigate to the destination folder for the application.
4. Click **Next**. The **WIN-PAK CS/SE/PE Destination Path** screen appears displaying the language file path.

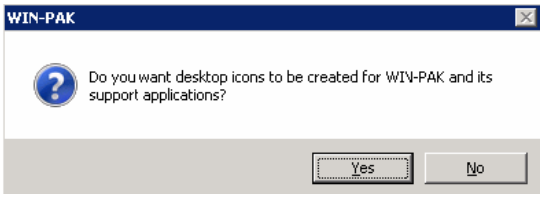


5. To change the path, click **Browse** and navigate to the destination folder for the file.

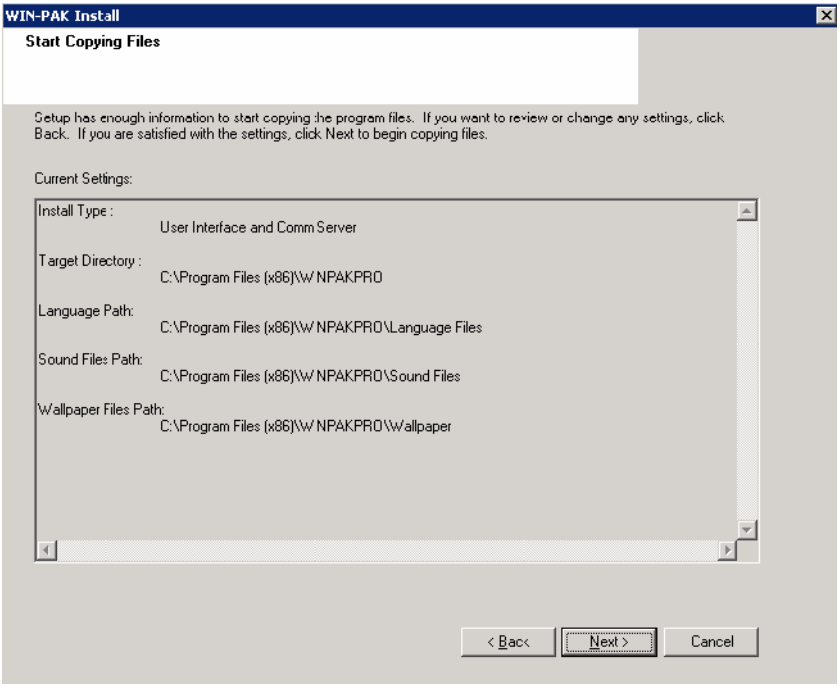
6. Click **Next**. The **WIN-PAK CS/SE/PE Destination Path** screen appears displaying the sound and wallpaper file paths.



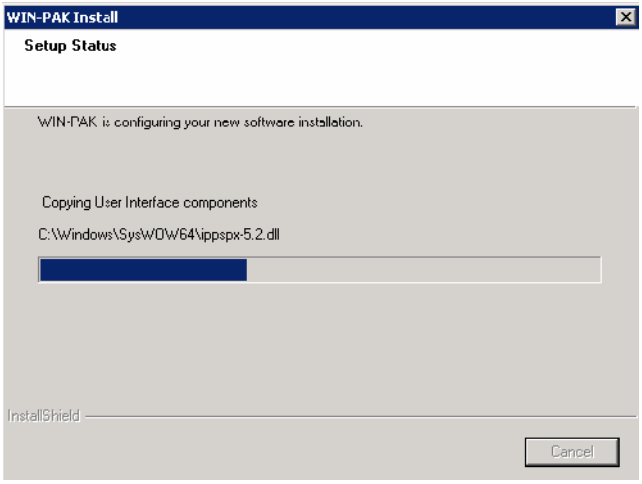
7. To change the path, click **Browse** and navigate to the destination folder for each file.
8. Click **Next**. A dialog box appears prompting you to create shortcuts on your desktop.



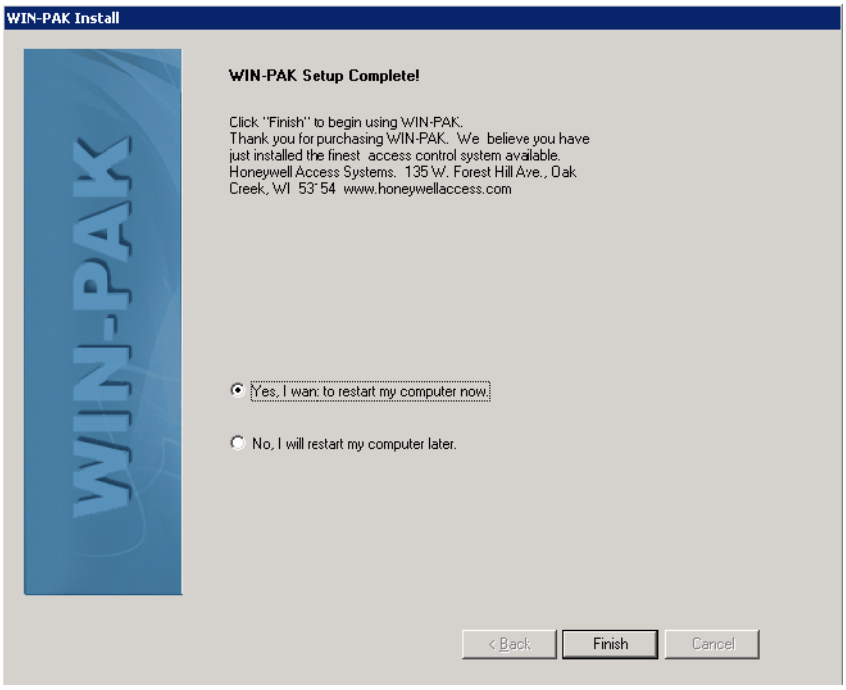
9. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



10. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



11. After completing the installation, the following screen appears.



12. 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.

13. Click **Finish**.

Installing Communication Server for WIN-PAK CS/SE/PE

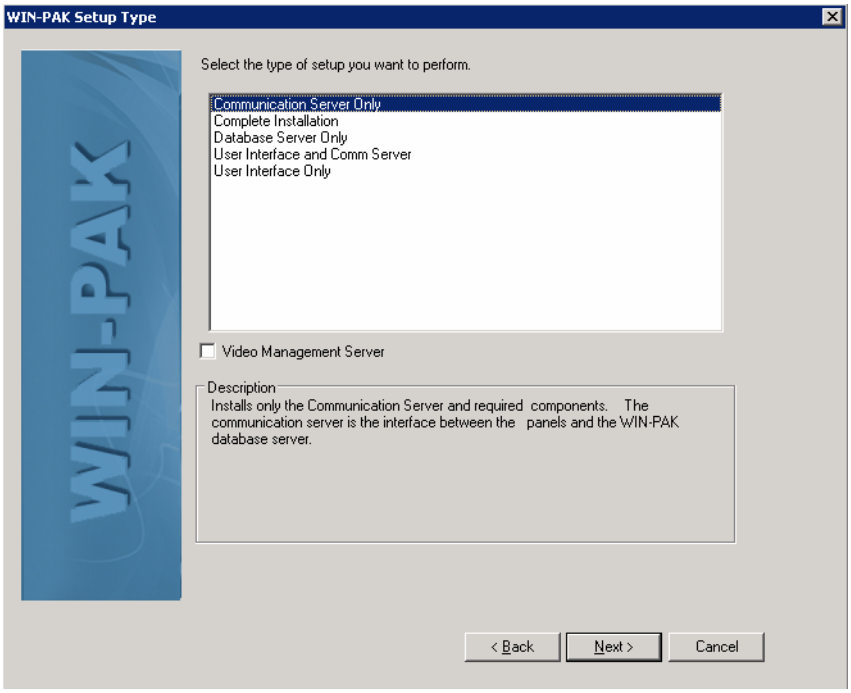
WIN-PAK CS/SE/PE supports installation of multiple communication servers across a network. After installing Database Server and User Interface, multiple communication servers can be installed depending on your licensing limit.

To install WIN-PAK CS/SE/PE Communication Server, perform the instructions given in "To install WIN-PAK CS/SE/PE", and follow these steps:

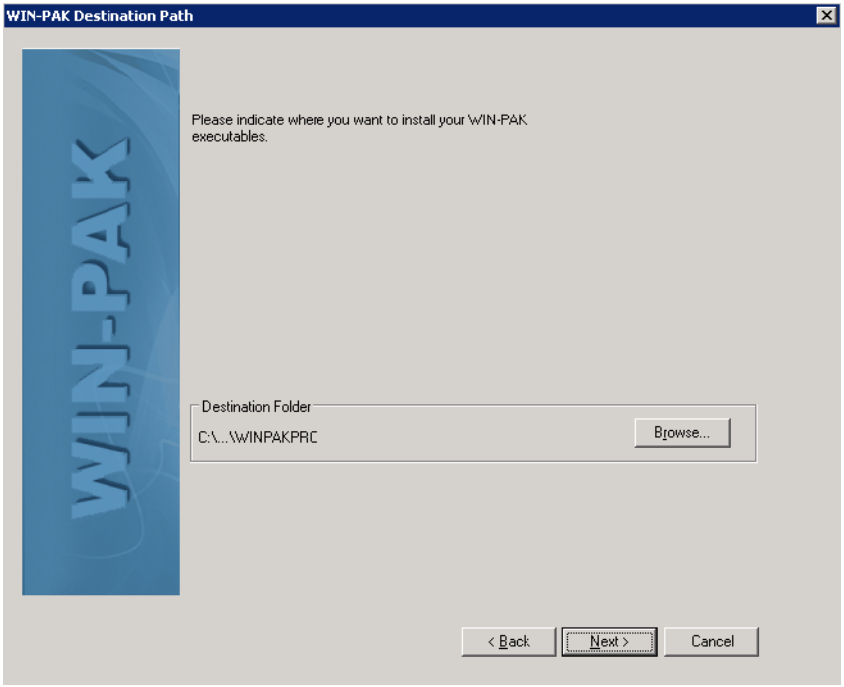
Note:

WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

1. On the **WIN-PAK CS/SE/PE Setup Type** screen, select **Communication Server Only** and click **Next**.

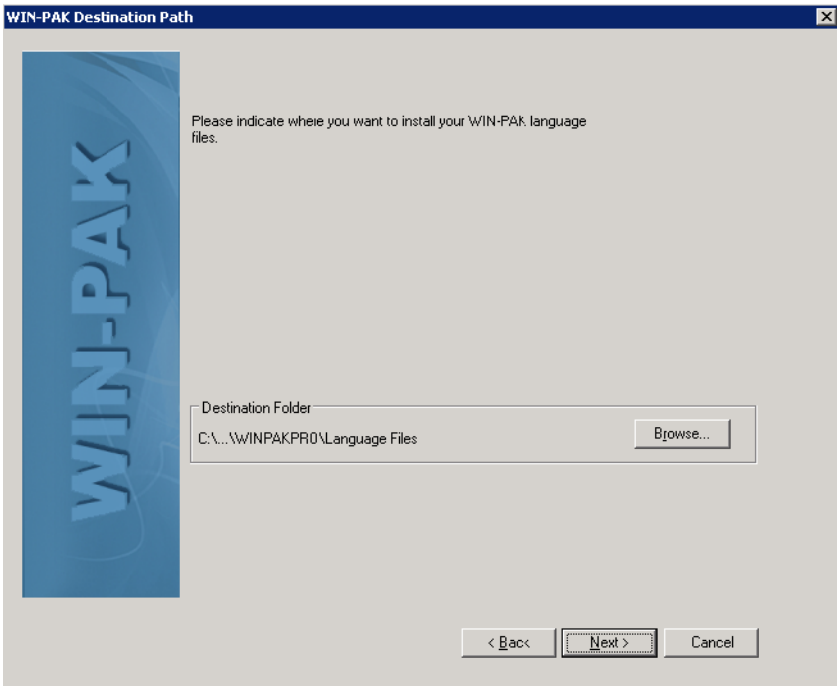


2. The system displays the **WIN-PAK CS/SE/PE Destination Path** screen.

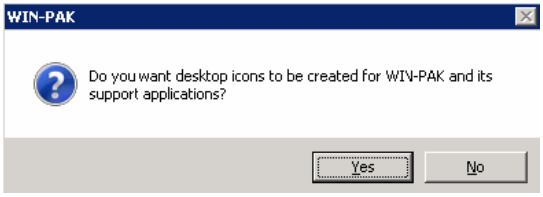


3. To change the path, click **Browse** and navigate to the destination folder for the application.

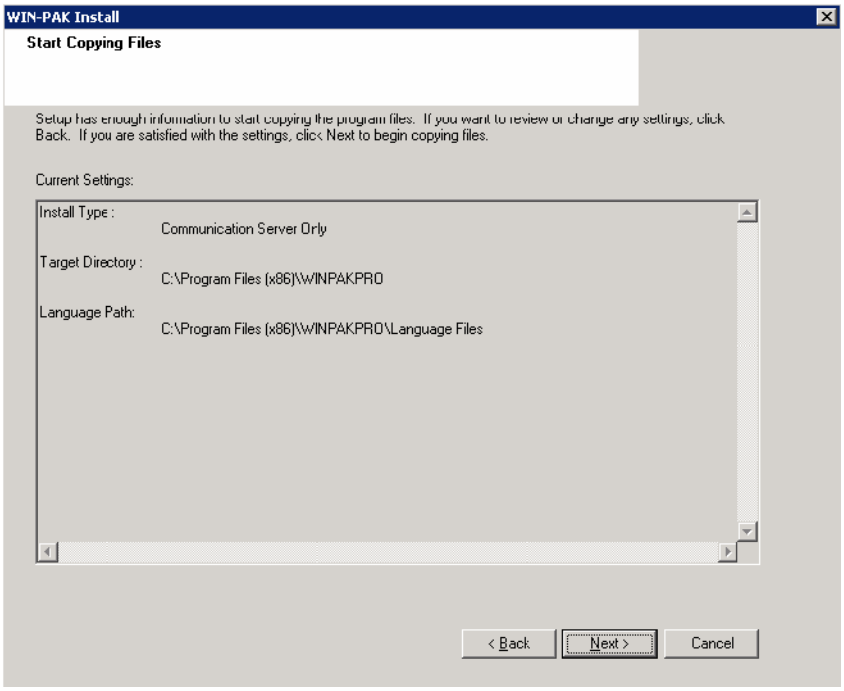
4. Click **Next**. The **WIN-PAK CS/SE/PE Destination Path** screen appears displaying the language file path.



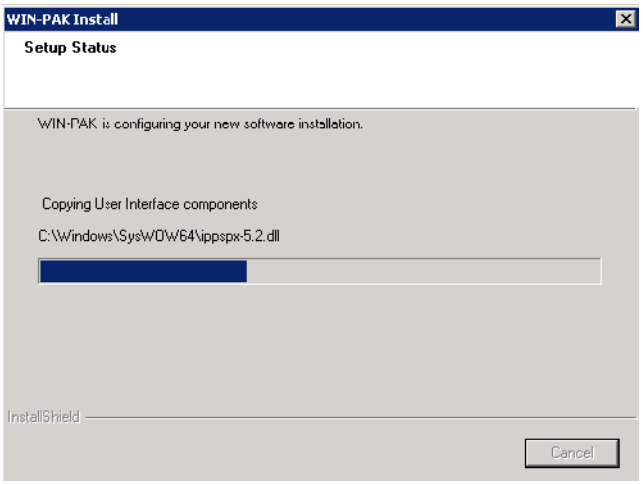
5. To change the path, click **Browse** and navigate to the destination folder for the file.
6. Click **Next**. A dialog box appears prompting you to create shortcuts on your desktop.



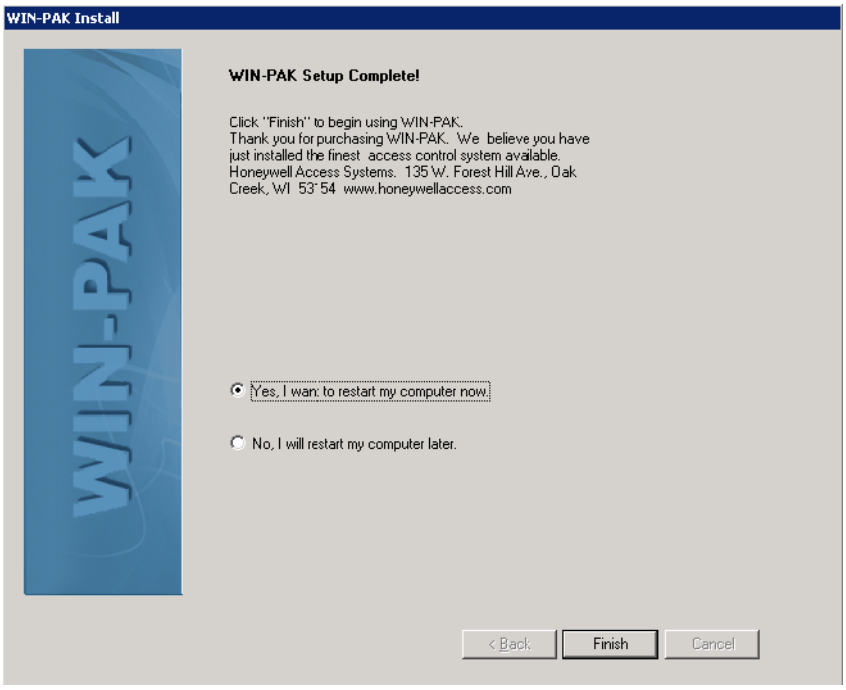
7. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



8. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



9. After completing the installation, the following screen appears.



10. 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.

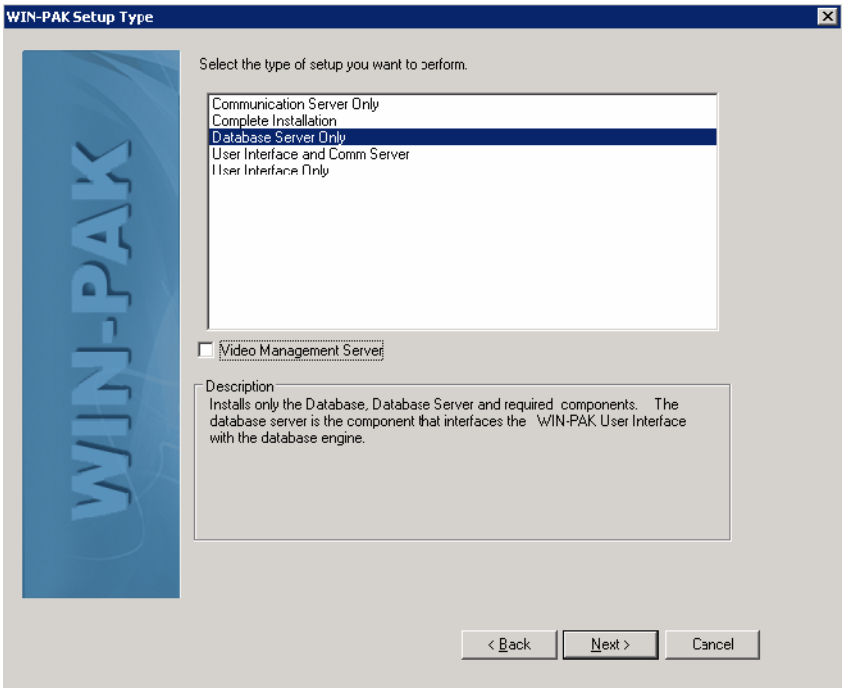
11. Click **Finish**.

Installing Video Management Server along with database server or complete installation for WIN-PAK CS

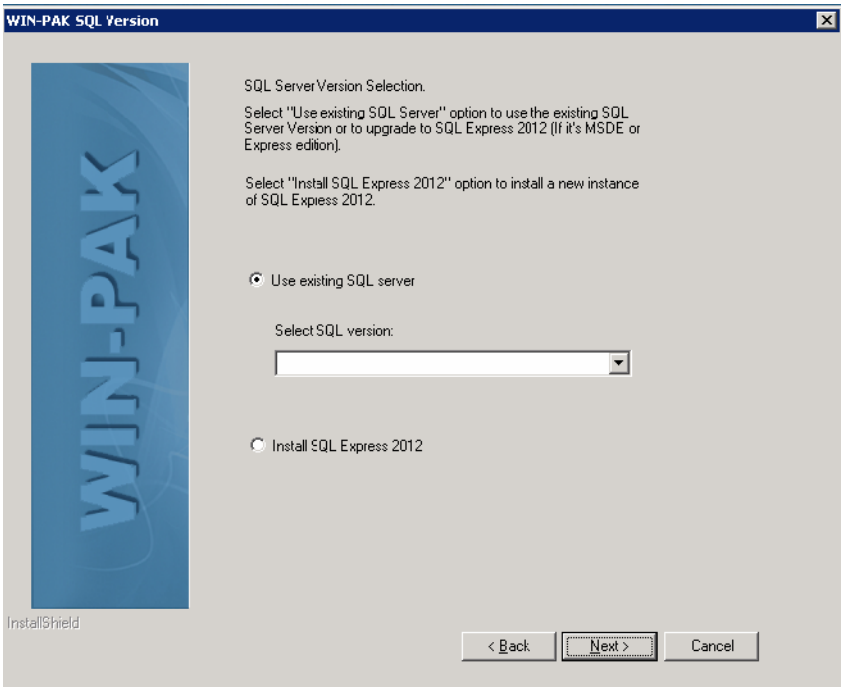
You can install the Video Management Server (VMS) along with database server or complete installation, on a computer connected to a network.

To install the video management server along with database server or complete installation, perform the instructions given in "To install WIN-PAK CS/SE/PE", and then follow these steps:

1. On the **WIN-PAK CS Setup Type** screen, select **Complete Installation** and **Video Management Server** and then click **Next**.



2. The system checks the prerequisite for installing VMS, lists the available domains, and displays the **WIN-PAK CS Install** screen.



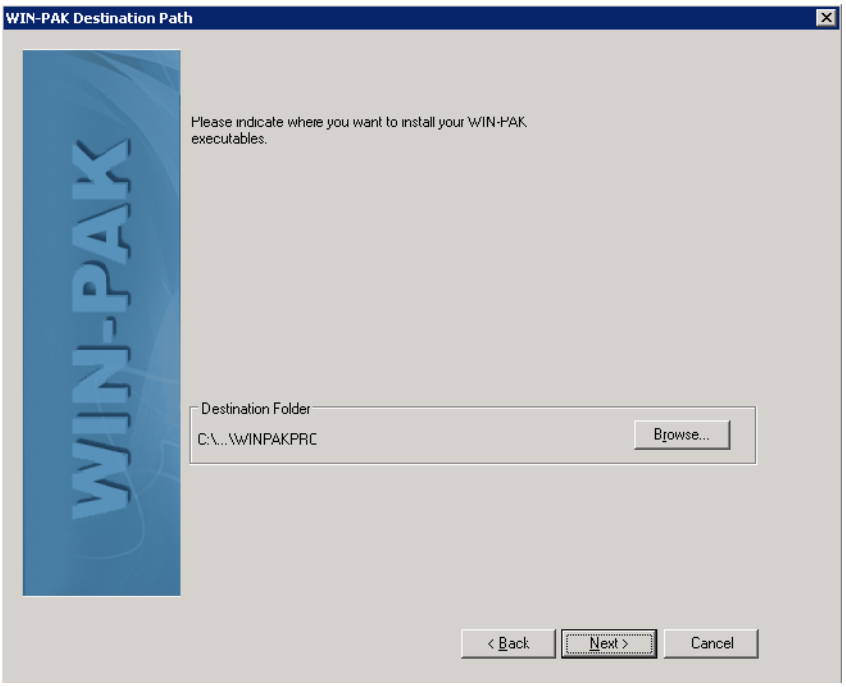
3. Provide the following details to validate the user credentials:

    a. **Domain Name/Host Name** - The name of the domain to which the user is associated to.

b. **User Name** - The user name which is used for accessing the video management server.

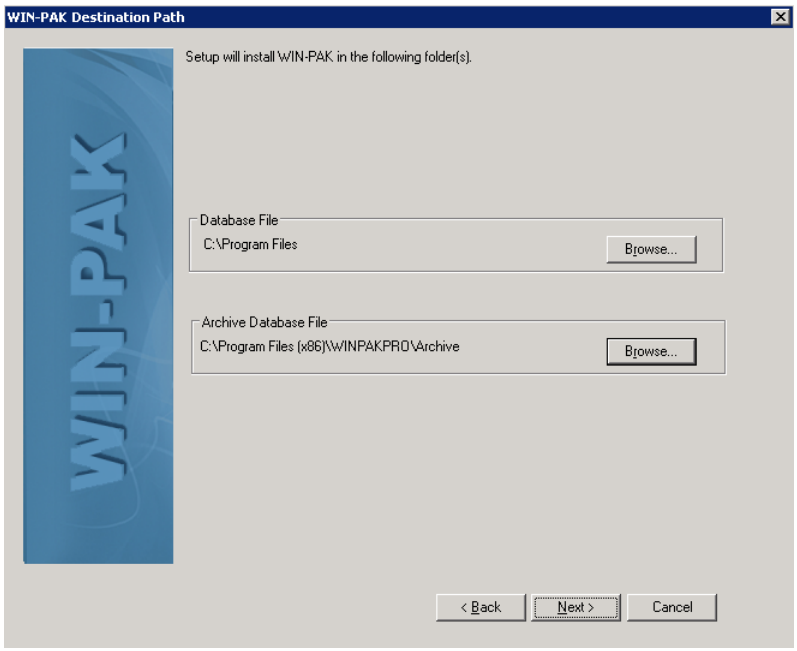
c. **Password** - The password which is used for accessing the video management server.

4. Click **Next**. The **WIN-PAK CS Install** screen appears.

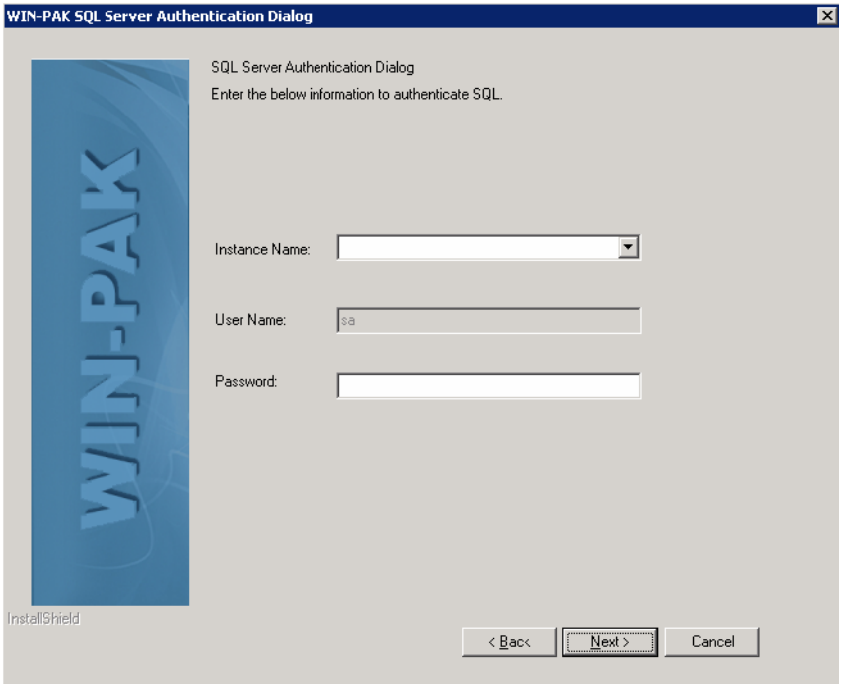


5. Under **Device Drivers**, you can select the VMS drivers which must be installed.

6. In the **WIN-PAK CS Install** screen, click **Next** to view the **WIN-PAK CS SQL Version** screen.

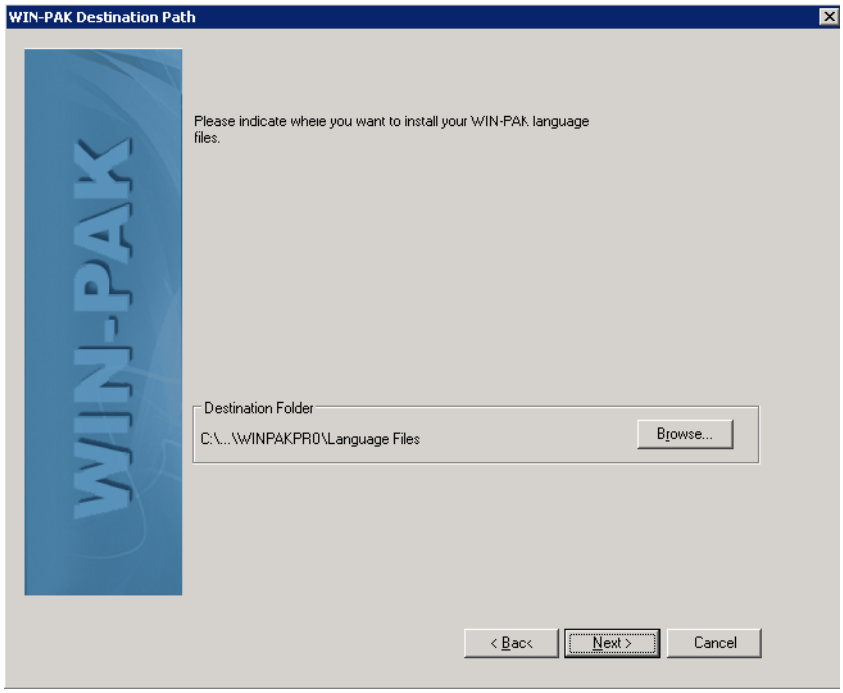

WIN-PAK Destination Path
WIN-PAK
Setup will install WIN-PAK in the following folder(s).
Database File
C:\Program Files
Browse...
Archive Database File
C:\Program Files (x86)\WINPAKPRO\Archive
Browse...
< Back
Next >
Cancel

7. You can select:
    - **Use existing SQL server** to use the existing SQL Server version or to upgrade to the SQL Express 2012 (if it is MSDE or Express Edition). You must **Select SQL Version** from the drop-down list.
    - **Install SQL Express 2012** to install a new instance of the SQL Express.
8. In the **WIN-PAK CS SQL Version** screen, click **Next**. The **WIN-PAK CS SQL Server Authentication Dialog** box appears.



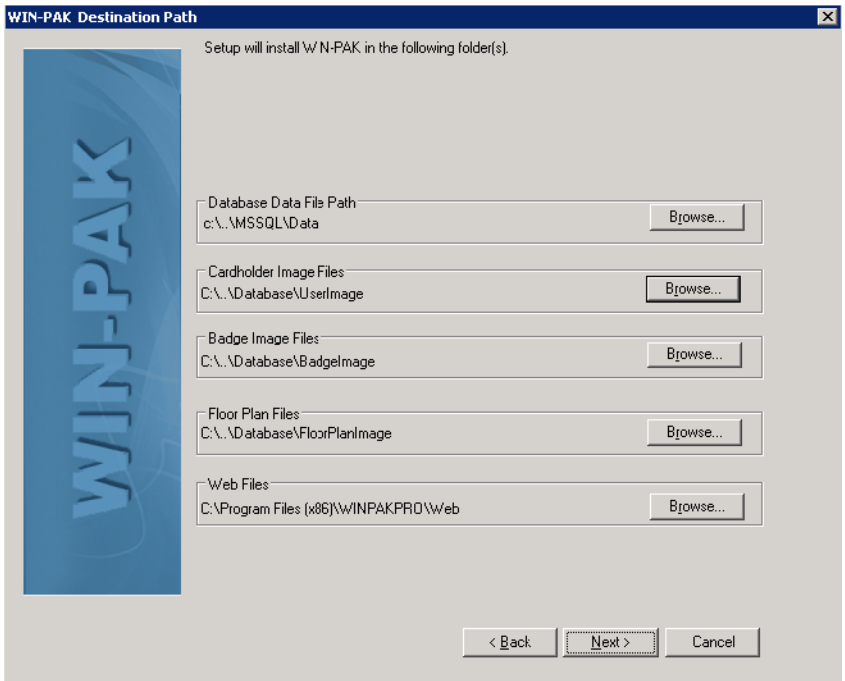
9. Provide the following details about the SQL server:
    a. **Instance Name** - The name of the SQL server.
    b. **User Name** - The user name which is used for accessing the SQL Server present in the database server.
    c. **Password** - The password which is used for accessing the SQL Server present in the database server.

10. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file path.

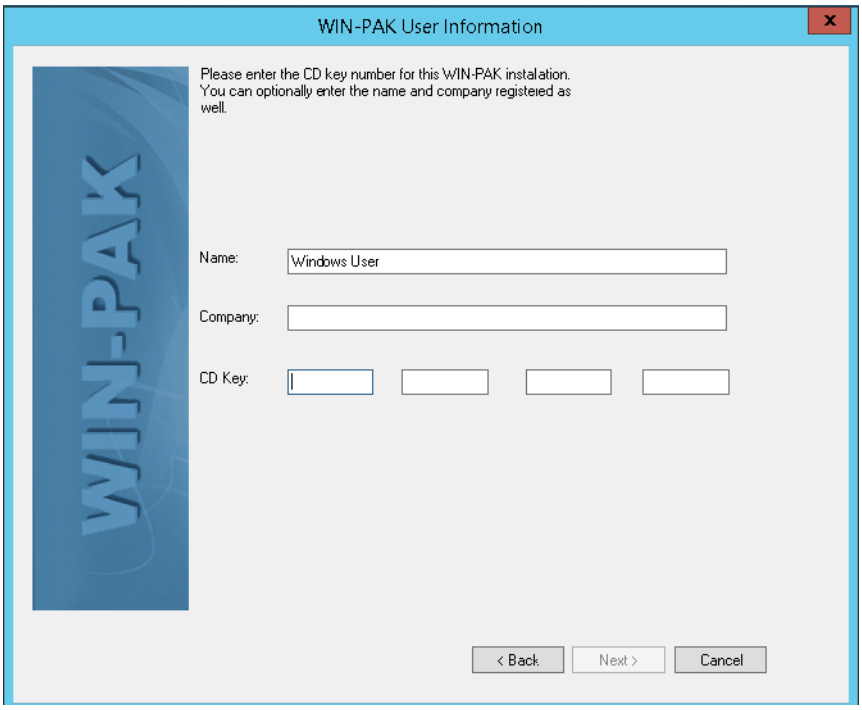


11. By default, the WIN-PAK CS application is installed in the C drive. If you want to change the installation folder, click **Browse** and specify a different destination folder.

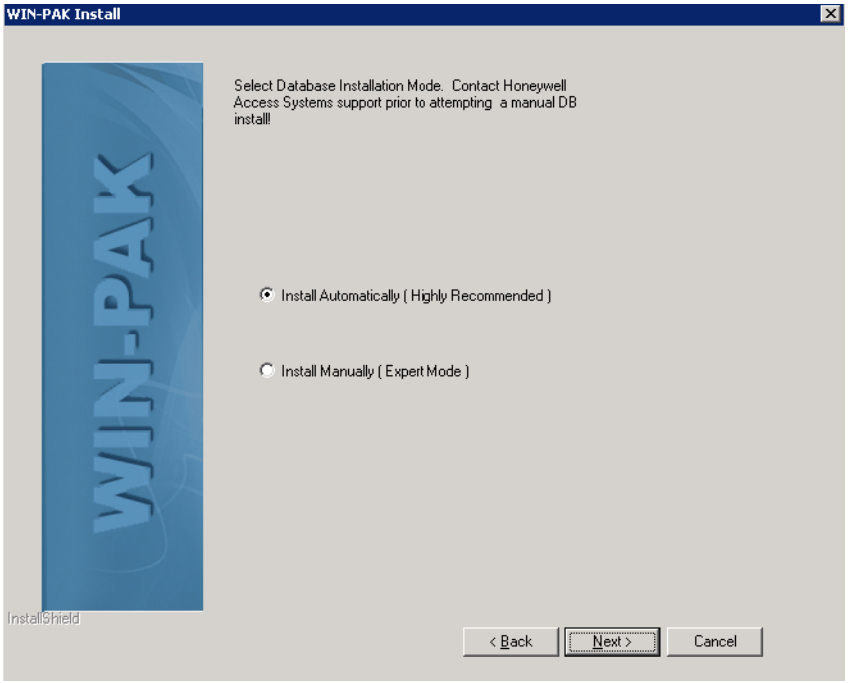
12. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file paths.



13. To change the path, click **Browse** and navigate to the destination folder for each file.
14. Click **Next**. The **WIN-PAK CS User Information** screen appears.



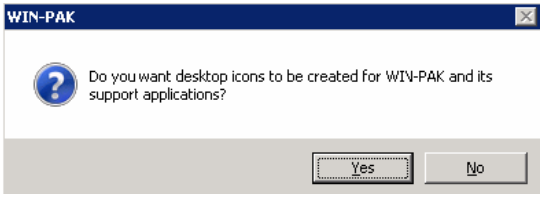
15. Type your **Name**, **Company** and **CD Key** details. The CD Key is found in the front cover of the WIN-PAK CS Quick Reference Guide.
16. Click **Next**. The **WIN-PAK CS Install** screen appears.



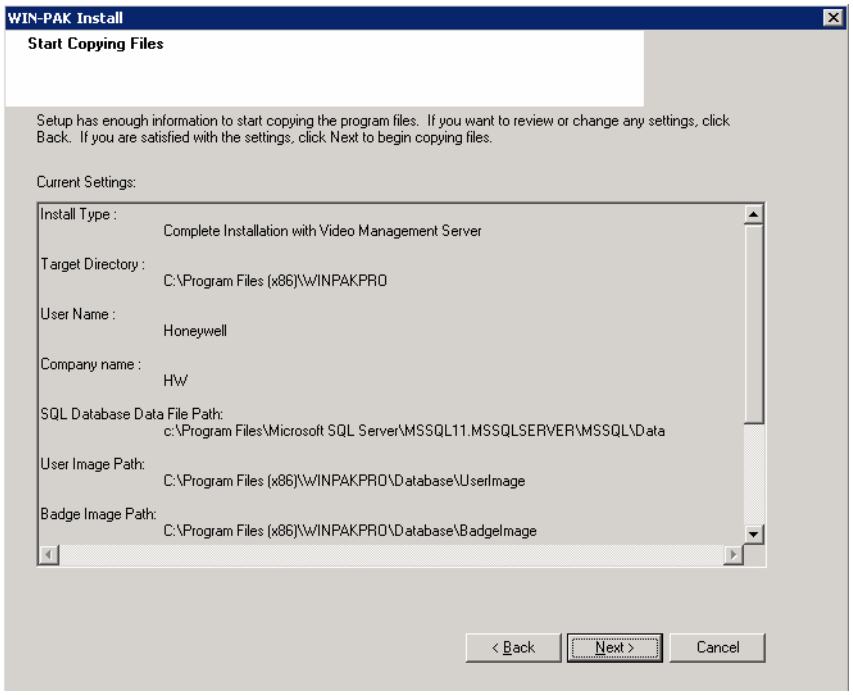
17. Select the installation mode as **Install Automatically** for an automatic installation.

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

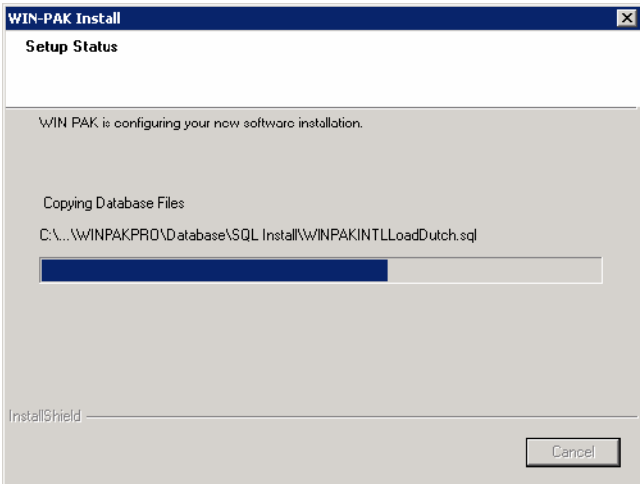
18. Click **Next**. A dialog box appears prompting you to create WIN-PAK CS shortcuts on your desktop.



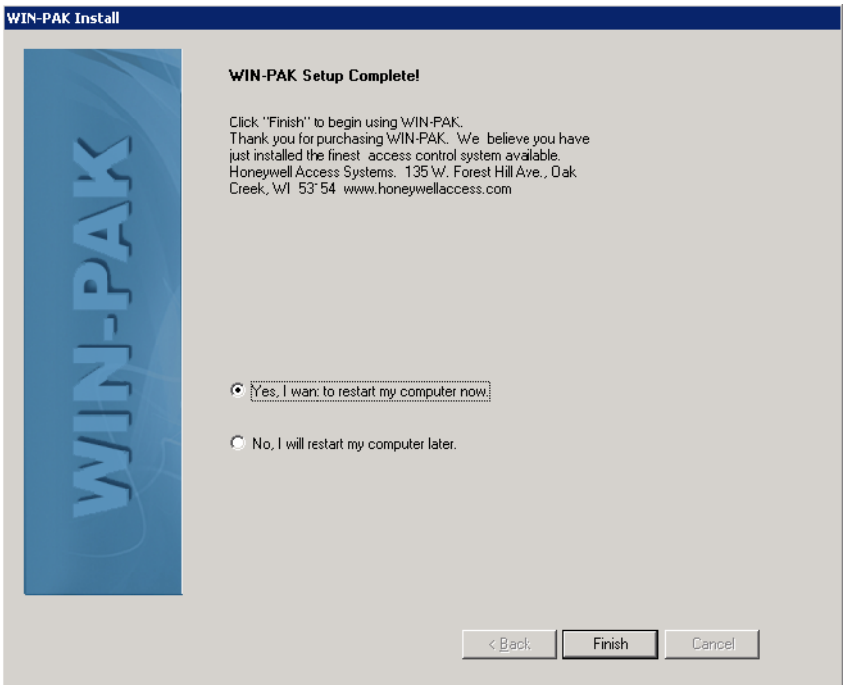
19. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



20. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



21. After completing the installation, the following screen appears.



22. 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.

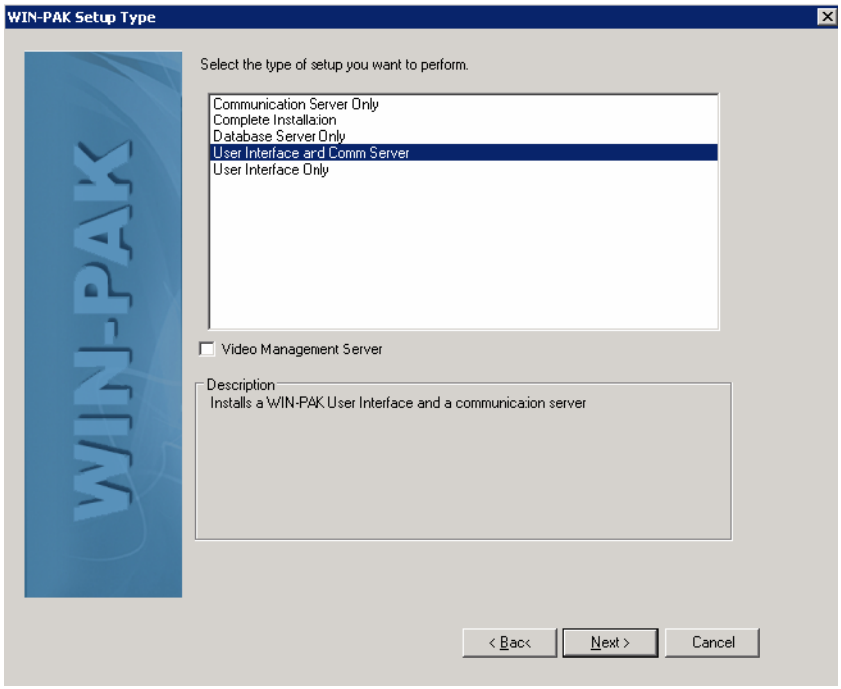
23. Click **Finish**.

Installing Video Management Server along with communication server or user interface and comm server installation for WIN-PAK CS

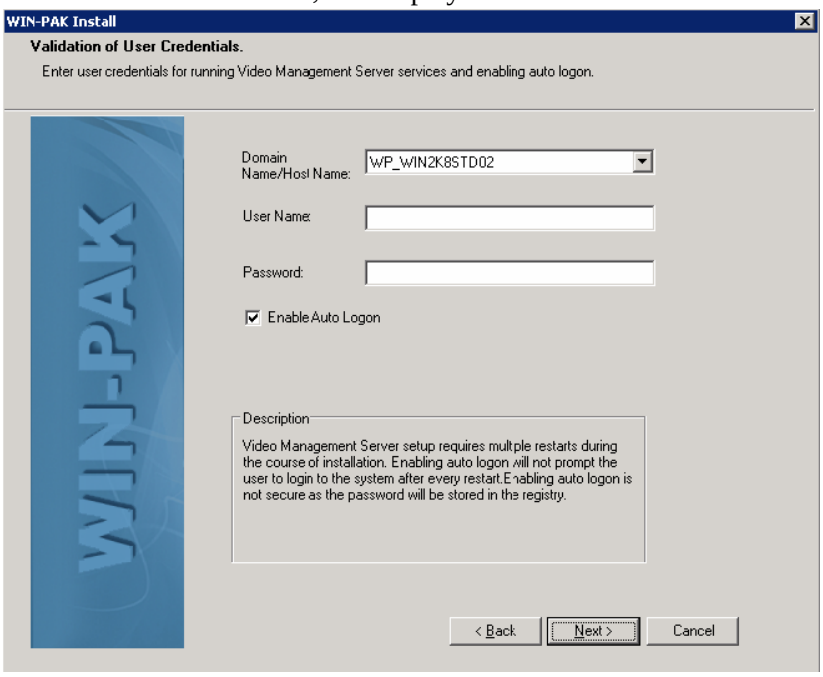
You can install the Video Management Server (VMS) along with communication server or user interface and comm server installation, on a computer connected to a network.

To install the video management server along with communication server or user interface and comm server installation, perform the instructions given in "To install WIN-PAK CS/SE/PE", and then follow these steps:

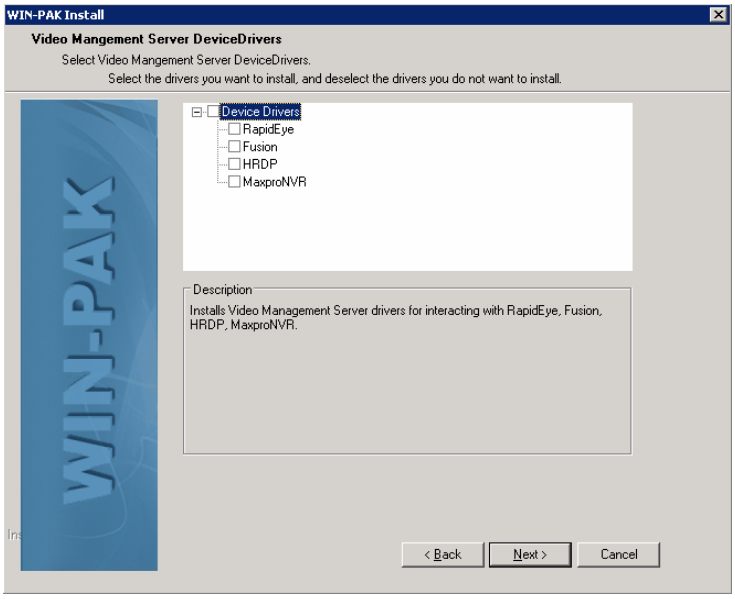
1. On the **WIN-PAK CS Setup Type** screen, select **User Interface and Comm Server** and **Video Management Server** and then click **Next**.



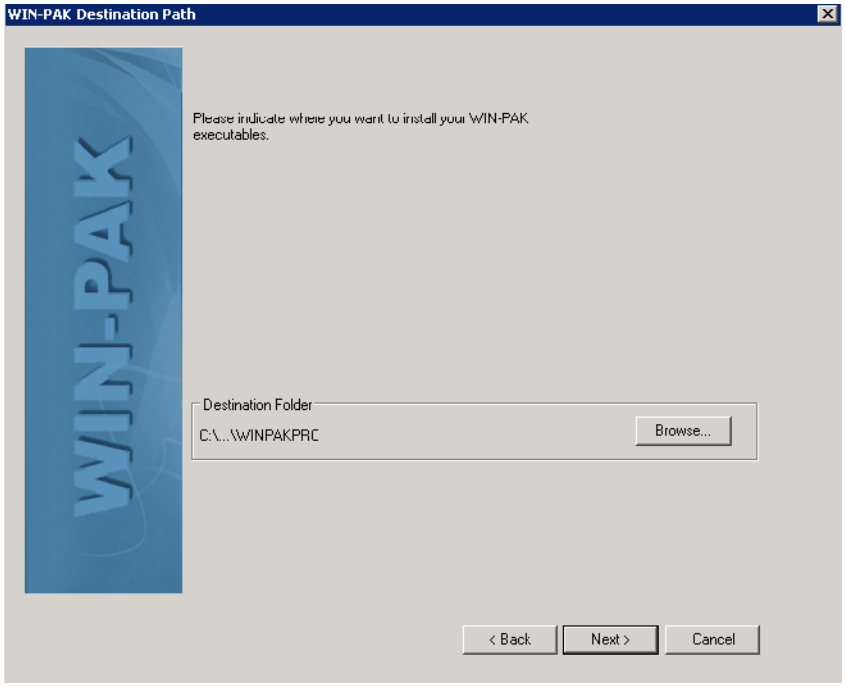
2. The system checks the prerequisite for installing video management server, lists the available domains, and displays the **WIN-PAK CS Install** screen.



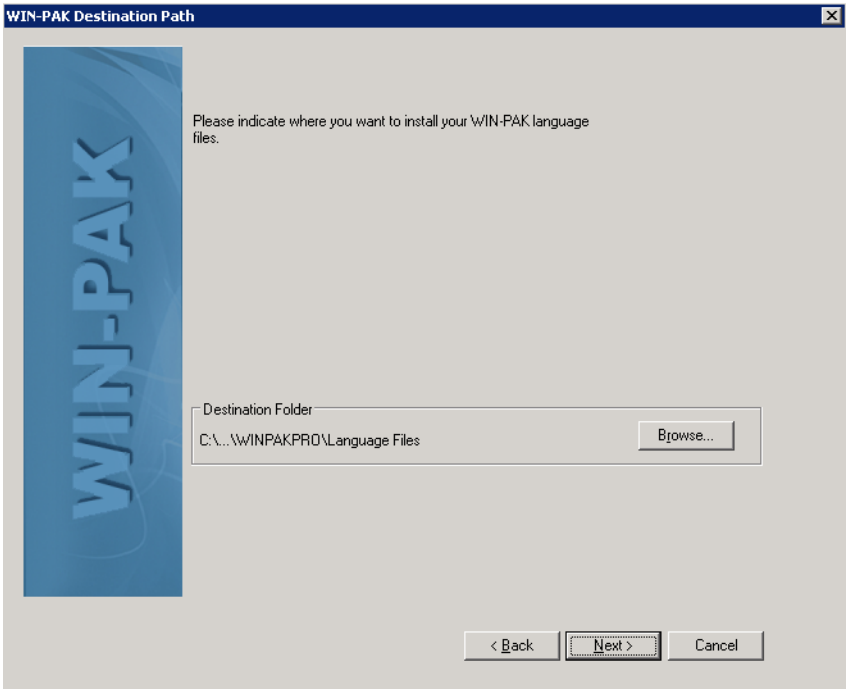
3. Provide the following details to validate the user credentials:
    a. **Domain Name/Host Name** - The name of the domain to which the user is associated to.
    b. **User Name** - The user name which is used for accessing the video management server.
    c. **Password** - The password which is used for accessing the video management server.
4. Click **Next**. The **WIN-PAK CS Install** screen appears.



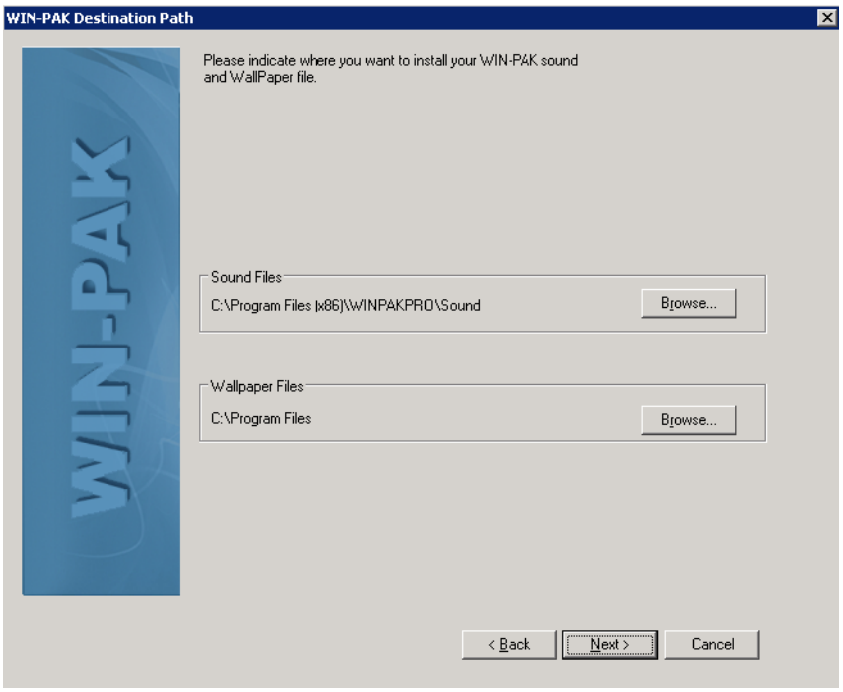
5. Under **Device Drivers**, you can select the VMS drivers which must be installed.
6. In the **WIN-PAK CS Install** screen, click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file path.



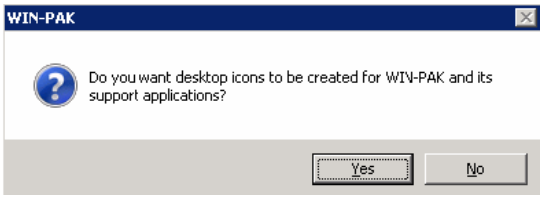
7. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS file path.



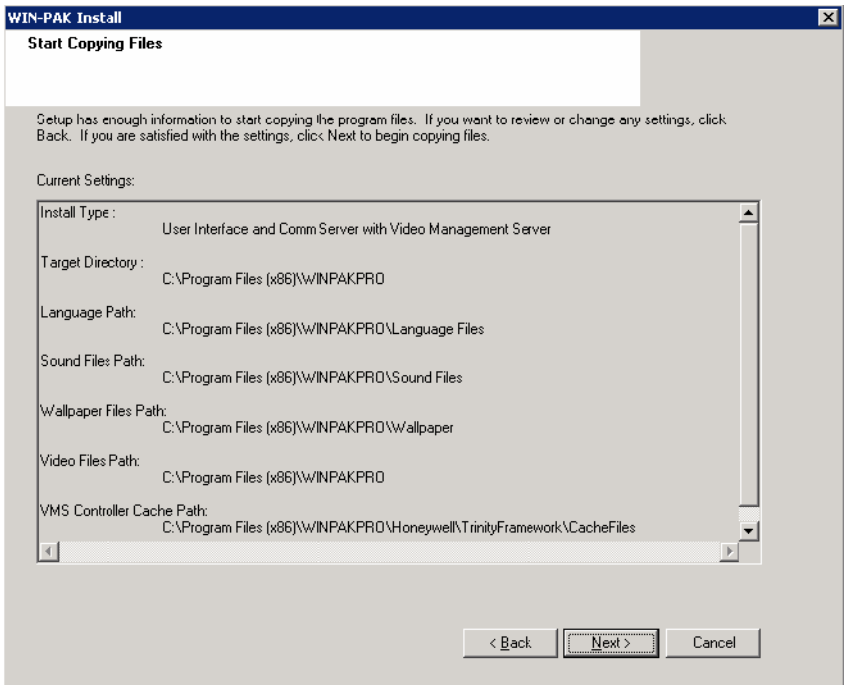
8. By default, the WIN-PAK CS application is installed in the C drive. If you want to change the installation folder, click **Browse** and specify a different destination folder.
9. Click **Next**. The **WIN-PAK CS Destination Path** screen appears displaying the WIN-PAK CS sound and wallpaper file paths.



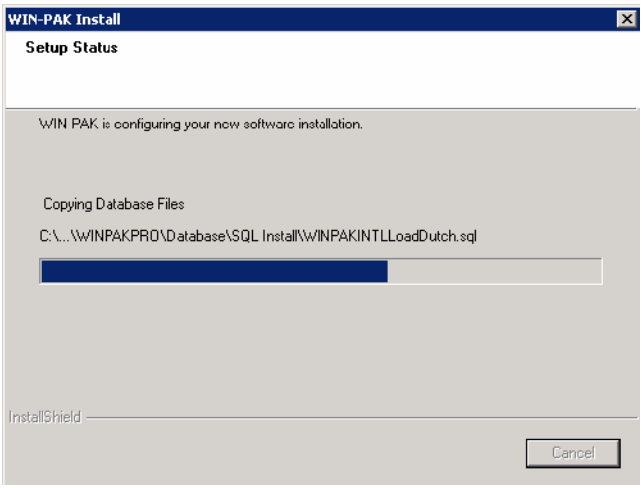
10. To change the path, click **Browse** and navigate to the destination folder for each file.
11. Click **Next**. A dialog box appears prompting you to create WIN-PAK CS shortcuts on your desktop.



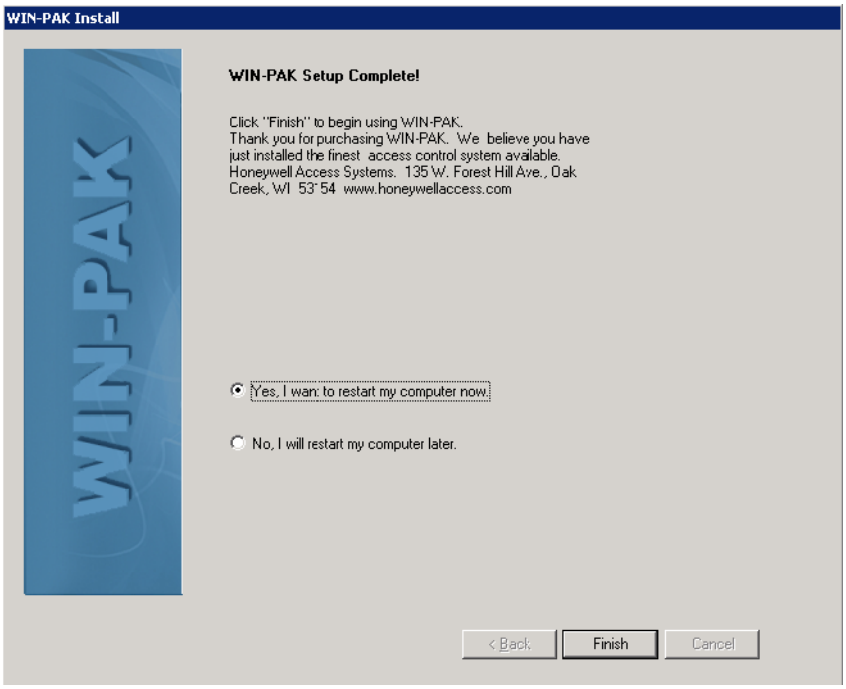
12. Click **Yes** to place icons on your desktop. The following screen is displayed with a summary of the installation information.



13. If you want to change any setting, click **Back**, or else, click **Next** to start the installation.



14. After completing the installation, the following screen appears.



15. 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.

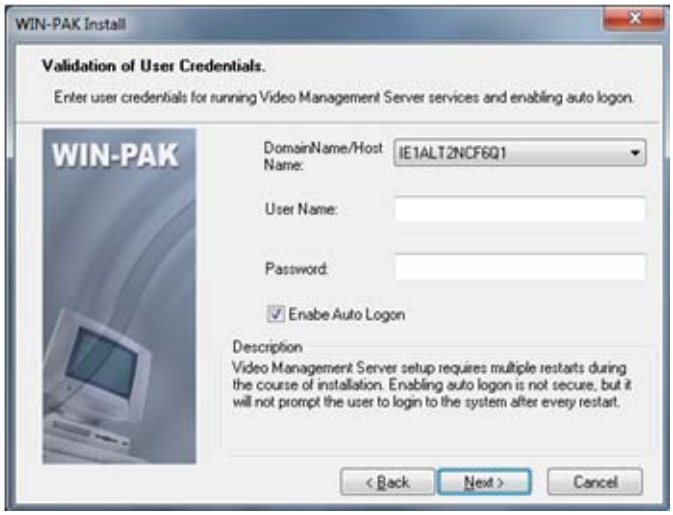
16. Click **Finish**.

Note: After the WIN-PAK CS installation is complete, the WIN-PAK CS services will run with the user name **winpakuser**.

Installing Video Management Server for WIN-PAK SE/PE

The complete installation installs the Video Management Server by default. However, clear the Video Management Server check box if you do not want to install the Video Management Server.

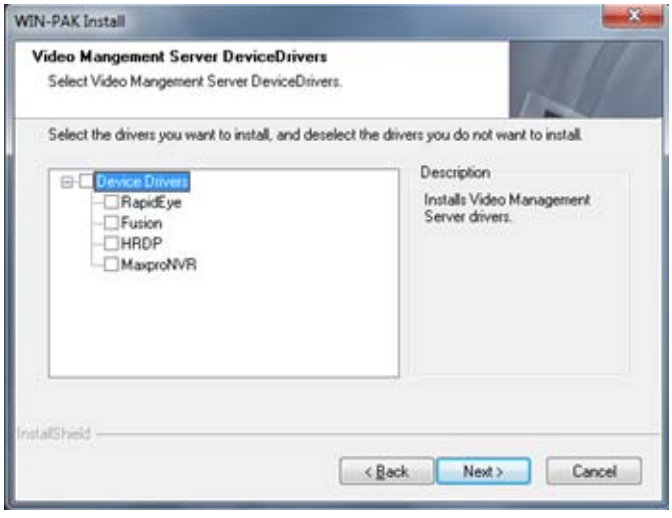
1. On the **WIN-PAK SE/PE Setup Type** screen, select the **Video Management Server** check box and click **Next**. The system check for SQL Service status and displays the screen shown below.



2. From the **Domain Name/Host Name** list, select the domain name/host name of the video management server.
3. Type the **User Name** to access the video management server.
4. Type the **Password** to access the video management server.
5. Select the **Enable Auto Logon** check box to enable the system to auto logon each time the system restarts.

Note: The system reboots several times to complete the Video Management Server installation.

6. Click **Next**.



7. Select the check boxes corresponding to DVRs under **Device Drivers** as applicable.

8. Click Next. Follow the steps from "Installing Complete WIN-PAK CS/SE/PE" section to complete the installation.

Installing HON FIN4000 ENROLL Device Drivers for WIN-PAK SE/PE

Before you plug-in the HON FIN4000 ENROLL device, you must:

1. Browse to the destination folder which has WIN-PAK installed.
2. Double-click the **HON-FIN4000-ENROLL Driver.exe**.
3. Follow the on screen instructions.

Additional Installation Components for WIN-PAK CS/SE/PE

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

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

While working with Windows 2008 R2 or Windows 7 operating systems, WIN-PAK CS/SE/PE installs the following external components.

External Components

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

- Microsoft Data Access Components
- Sentinel Lock Drivers
- Crypkey Drivers
- Microsoft .NET FrameWork
- Active Reports
- Topaz Signature pad
- Videology drives for Badge print

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 CS/SE/PE.

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 CS/SE/PE installation provides only the English version of these Microsoft modules. This may cause a problem, as the English version is not compatible with other language versions of the Windows operating system.

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

Upgrading WIN-PAK SE/PE

Honeywell recommends you to select direct upgrade. WIN-PAK SE/PE supports direct upgrade from WIN-PAK SE/PE 3.2 and above only.

You must use the Backup and Restore Utility option to upgrade any older versions of WIN-PAK SE/PE installed on your computer.

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

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

Migration Utility

Note: Migration is not applicable if you are installing WIN-PAK SE/PE for the first time or for a site that does not have video devices.

Migration tool is installed on the computer that has the WIN-PAK SE/PE Database when you have opted to Install Video Management server during Installation.

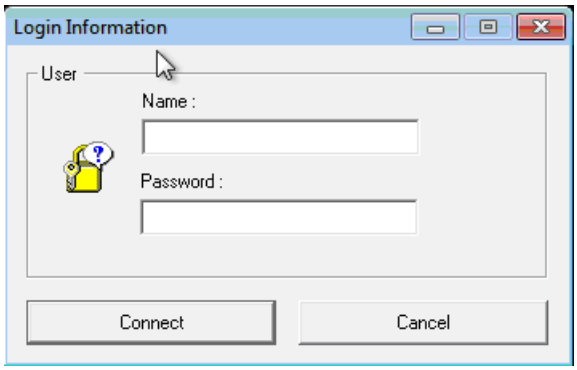
Migration tool is needed when you upgrade from previous SE/PE versions of WINPAK SE/PE, that is, Build 633.2 to 645.3 which has Video Devices to the latest WIN-PAK SE/PE 3.2 Build. This tool helps you to migrate any legacy video devices which were configured from Builds 633.2 onwards to the latest WIN-PAK SE/PE 3.2 Build.

Steps to run the Migration Tool: (Applicable when video devices are configured in legacy builds)

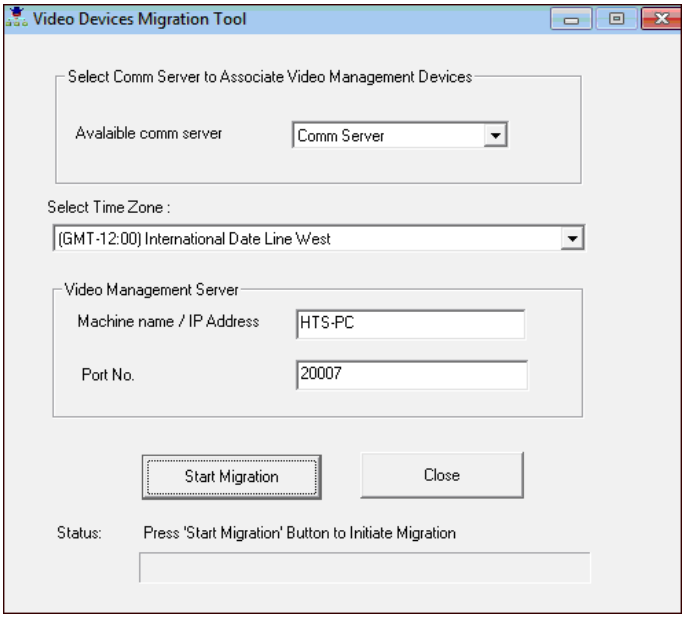
Scenario1: Directly upgrading from Builds 633.2 onwards to Release 3 builds

1. While upgrading to Release 3 build, choose the **Video Management Server** option.
2. After the installation is finished, the WIN-PAK Migration Tool icon 

appears on your desktop.
3. Click the Migration Tool icon, The **Login Information** dialog box appears



4. Type your user **Name** and **Password** (WIN-PAK SE/PE user credentials) to open the tool. The following image appears listing all the communication servers available in WIN-PAK SE/PE.



5. In the **Available comm server** list, select the communication server to which you want to associate all the video devices.
6. In the **Select Time Zone** list, select the time zone in which the recorders are available. By default the local time zone displays.
7. Click **Start Migration**. A progress bar appears displaying the status of migration. The “Migration Completed” message appears after the migration is successfully finished.
8. Close the Migration Tool and restart all WIN-PAK SE/PE Services using the WIN-PAK SE/PE Service Manager.

Scenario 2: Upgrade through Backup & Restore Utility

1. If you take a backup of the old database then, uninstall the old build and install the Release 3 build.
2. After restoring the old database into the Release 3 build, you must manually run the Migration tool to migrate the legacy video devices.

Scenario 3: Upgrading from Builds older than 633.2

- You must first upgrade the older build to build 633.2, and follow the procedure listed in Scenario 1.

Licensing and Registration

By default, the WIN-PAK CS installation setup installs the trial version which expires in 30 days. All the features of WIN-PAK CS are available in the trial version. Whereas for WIN-PAK SE/PE the installation setup installs only the demo version that has no expiry date. However it has following limitations:

• Only a 10 card database can be maintained.

• You cannot add cards in bulk.

• You cannot print badges.

However, registering the software enables you to overcome the preceding limitations and use it beyond the 30 day trial period in case of WIN-PAK CS.

Registering WIN-PAK CS/SE/PE

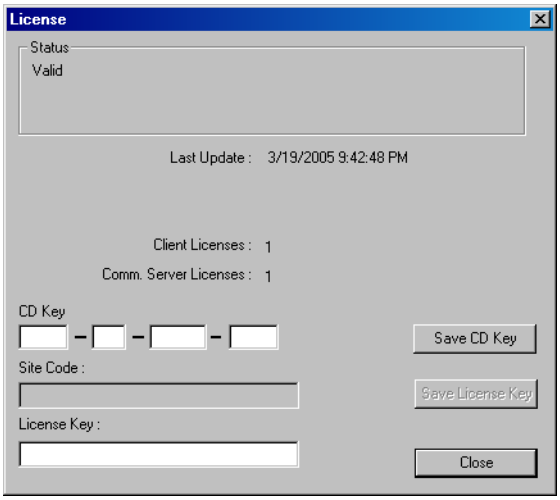
Before you register the WIN-PAK CS/SE/PE software, make a note of the CD Key and the Site Code. The CD Key number is located on the inner portion of the front cover of the Quick Reference Guide/DVD case.

Note:

WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

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.

You can register the WIN-PAK CS/SE/PE software over the telephone, with the Honeywell Access Systems Technical Support, or registration can be done online using the Honeywell Access System web site.

To register the software over the telephone:

1. Contact the Honeywell Access Systems Technical Support and provide the CD Key and the Site Code.
2. Type the License Key provided in the **License Key** box.
3. Click **Save License Key**. This enables you to use WIN-PAK CS beyond the 30 day trial period.

To register the software online:

1. Open **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 appears.

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

Upgrading WIN-PAK SE/PE License

You can upgrade your WIN-PAK SE/PE license to overcome the limitations of the WIN-PAK SE/PE 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 SE/PE 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, which invalidates the license.

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

De-fragmenting Disk Drive

Any movement or damage to the license files, may invalidate your license. De-fragmentation is one of the actions that relocate the files.

Caution: Do not use Microsoft Disk Defragmenter for De-fragmenting. If used, some disk files may be physically moved and this results in invalidating the license.

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...

This chapter describes about the Introduction, User Interface Elements, and the Help topics of WIN-PAK CS/SE/PE, and T&A User Account.

Section	WIN-PAK CS	WIN-PAK SE/PE	WIN-PAK T&A
User Account: Requests Raised, page 118			✓
User Account: Log Out, page 118			✓

Introduction

The WIN-PAK CS/SE/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 CS/SE/PE operations.The Database Server, Communication servers and the other services continue to run.

This chapter describes how to log on to the WIN-PAK CS/SE/PE User Interface and use the various elements present in the interface. Elements in the User Interface include windows, menus, tool bars, and status bars. In addition, you can learn how to gain access to the WIN-PAK CS/SE/PE help.

WIN-PAK CS/SE/PE User Interface Elements

The elements in the WIN-PAK CS/SE/PE User Interface are:

- Windows
- Menu bar
- Tool bar
- Status bar

Logging on to WIN-PAK CS/SE/PE

To log on to the WIN-PAK CS/SE/PE User Interface:

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

Notes:

- When you first log on to the WIN-PAK CS/SE/PE User Interface, by default, the user credentials are ‘admin’ and blank password. However, to ensure security you must set the password during the first login.
- 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:

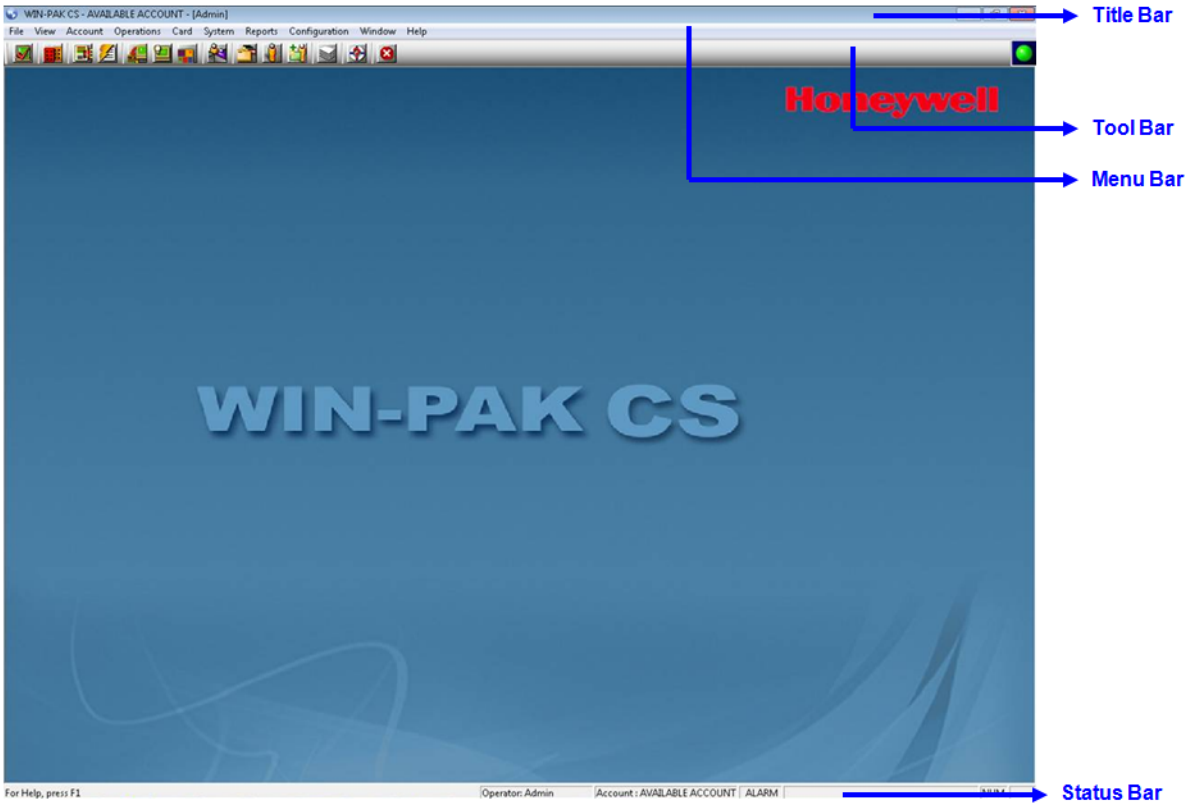
The Administrator has the privilege to log on to all the accounts. Operators can log on to those accounts for which they have the privilege. The title bar of the WIN-PAK CS/SE/PE main window displays the name of the active account.

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

Knowing more about the User Interface

The section describes about the UI screen of WIN-PAK CS, and SE/PE.

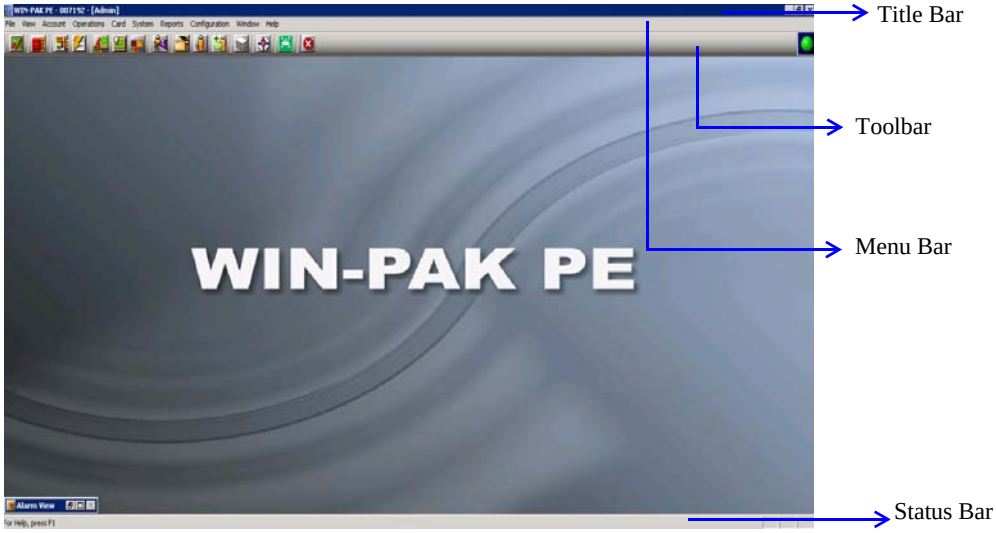
WIN-PAK CS



Note: For the System account, the following tool bar icons and menu options are disabled:

- **Locate Last Card/Card Holder Transaction** , **Card** , **Cardholder** , and **Add Cardholder** icons in the toolbar.
- **Card**, **Card Holder**, and **Access Level** sub-menu options in the **Card** menu.
- Options in the **Define**, **Device,** and **Cardholder** sub-menus of the **Configuration** menu.

WIN-PAK SE/PE



- 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 CS/SE/PE Windows

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

The Main window is started as soon as you log on to the WIN-PAK CS/SE/PE user interface. It comprises the options for performing various operations in WIN-PAK CS/SE/PE.

The Maintenance windows enable you to perform various operations for WIN-PAK CS/SE/PE 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, Tool bar, and the Resize buttons.

The title bar displays the following details:

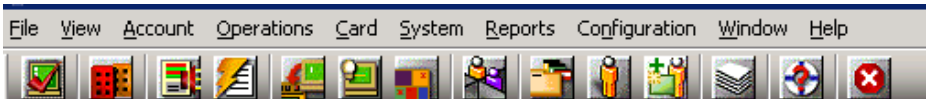
- WIN-PAK CS/SE/PE
- Account
- Operator
- Watchdog Timer

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.

Tool Bar

The toolbar appears below the menu bar in the Main window. The tool bar consists of icons that are frequently used in WIN-PAK CS/SE/PE operations.

By default, the tool bar is displayed in the Main window. However, you can change the display settings by clicking the **Tool** option in the **View** menu.



Note:

Print the Muster Report button is available only in WIN-PAK SE/PE.

Button	Button Name	Description
	**Log In**	Enables you to log on to WIN-PAK CS/SE/PE and connect to the WIN-PAK CS/SE/PE 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**	Enables you to open the floor plans.

Button	Button Name	Description
	**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.
	**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 online help for WIN-PAK CS/SE/PE.
	**Print the Muster Report**	Opens the **Print** window, enabling you to print the mustering report. **Note:** You can also click the shortcut key **Alt** + **Ctrl** + **P** to directly open the Print window and print the muster report.
	**Auto-Logout from all servers**	Enables you to log off the user interface and all the servers.

Menu Bar

The menu bar appears at the top of the Main window and contains commands menus to carry out various WIN-PAK CS/SE/PE operations.

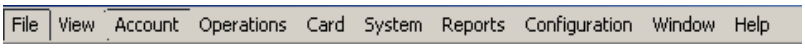


Table 3-1 Menu names and Short Keys

Menu	Shortcut Key	Description
File	ALT + F	Contains commands to configure printers, to log on and log off from the application, to quit from WIN-PAK CS/SE/PE, to view the reports window, and so on.
View	ALT + V	Enables you to disable or enable the tool bar 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 the commands to work with access cards and access levels.
System	ALT + S	Contains the commands for setting the system defaults.
Reports	ALT + R	Enables you to generate and view reports.
Configuration	ALT + N	Contains the commands for configuring the general hardware.
Window	ALT + W	Enables you to toggle between the multiple open windows.
Help	ALT + H	Enables you to view the online help.

To access the commands in the menu bar:

Using the pointing device (mouse),

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

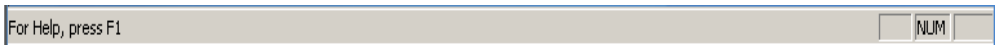
   Example: To gain access to the **Card Holder** window, on the **Card** menu, click **Card Holder.** The **Card Holder** window appears.

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** command, press **<Alt>+O** and then press **F**. The **Open Floor Plan** window appears.

Status Bar



By default, the Status Bar is displayed at the lower portion of the Main 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:

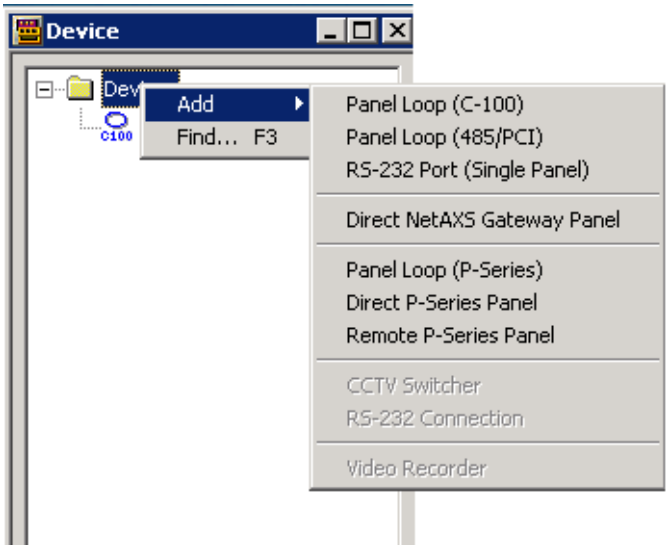
- The message **For Help, press F1** at the left corner.
- A description of the option that you have highlighted in the menu or the tool bar.
- The messages for setting permissions and for establishing communication server connections when you log on to WIN-PAK CS/SE/PE.
- The message for disconnecting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

Sub-menus and shortcut menus on right-click

When you are in a menu, click the right mouse button, a pop-up menu appears displaying a set of options specific to the dialog boxes.

Example:

1. Select an account.
2. Choose **Configuration > Device > Device Map**. The **Device** window appears.
3. Right-click **Devices**. A sub-menu is displayed.
4. Point to **Add** and click the required command.



Maintenance Window

The Maintenance window enables you to perform the following operations on various WIN-PAK CS entities:

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

Note: Maintenance window is available only in WIN-PAK CS.

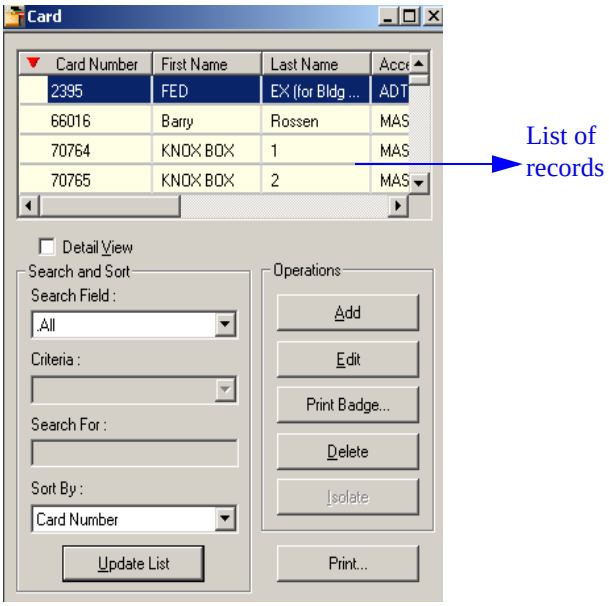
Opening a Maintenance Window

To open a Maintenance Window, select the menu and choose the required command from the menu or click the icon in the Tool bar. The corresponding Maintenance window appears.

For example, if you want to configure the Card Holder Tab Layout, select **Configuration > 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.



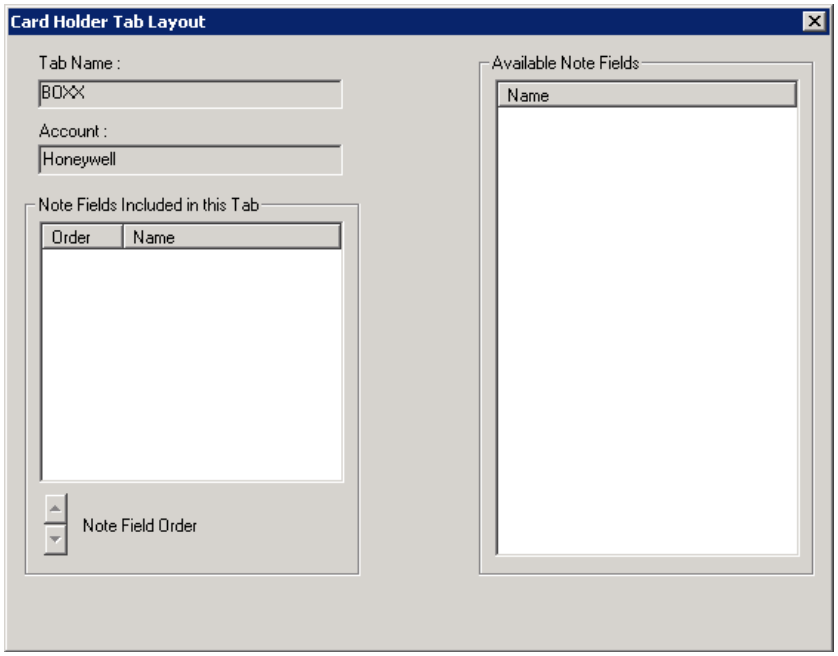
The following operations can be performed while viewing the list of records:

- 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.

- 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.
- 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.

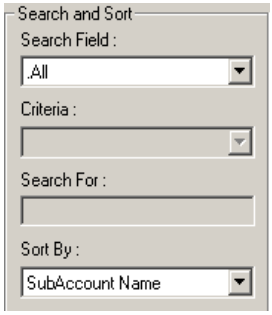


  b. Click **Close (X)** on the top-right corner of the screen or clear the **Detail View** check box in the Maintenance Window to close the **Detail View Card** dialog box.

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 records in the search result depends on the value set for the field **Maximum Records returned from the Database for Find List**. You can set the value by pointing to **System > Workstation Defaults** and clicking the **Defaults** tab.



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 3-2 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.

Button	Description
Delete	Click this button to delete a selected record. A message asking for confirmation appears. Click **Yes** to delete the record.

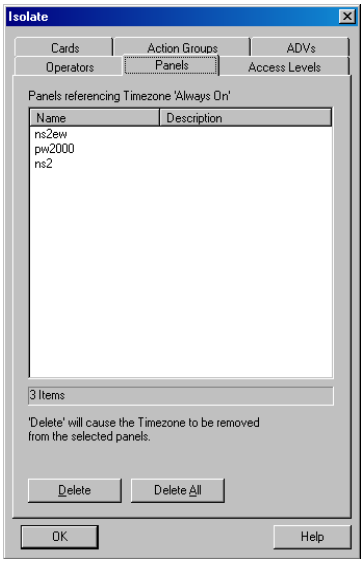
Isolating Records

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.

To isolate a record:

1. 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.

   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. Point to **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 selecting **Card > Card** and **Configuration > Time Management > Time Zone** from the menu.

   b. Select **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.

Eight tree structures are available in WIN-PAK CS, and six tree structures are available for WIN-PAK SE/PE as follows:

- Server Configuration
- Device Map
- Control Map
- Control Area
- Access Area Map
- Operator Level
- Customer Level
- Tracking Area Map

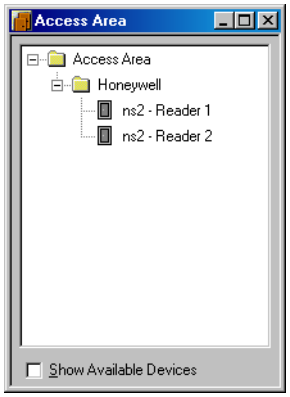
Note: The tree structure **Server Configuration** and **Customer Level** is not applicable for WIN-PAK SE/PE.

The tree structure for Device Map is defined, as and when the 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.

- Select **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 at a selected access level.
Red	Entrances not having access.
Yellow	Entrances having limited access.

Dialog Boxes

Note: The **Dialog Boxes** is available only in WIN-PAK CS.

Select

The **Select** dialog box enables you to locate a specific record in the list of records. The following table describes the action to be performed on the **Select** dialog box option.

Option	Action
Find key	Select the item to be searched

Option	Action
Find what	Type a letter, word, phrase, or numeric expression that you want to search.
Find	Click this button to display the search result.
OK	From the list of items, select the relevant item and click this button.
Cancel	Click this button to close the dialog box without selecting an item.

Zoom

The **Zoom** factor decides the view of the current window.

1. Right-click in the 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**.

Note: The current window enlarges or reduces according to the selected zoom percentage.

Calendar

The **Calendar** can be used for the scheduler, card activation, deactivation, holidays, Time Zones, and so on.

To select a date:

1. Click **Today** to select the current date.
2. For any other date, select the **Month** and **Year** from the list.
3. Click the appropriate day and then click **OK**.

Add Devices

The **Add Devices** dialog box enables you to select a device or entrance and add it to a branch.

1. Right-click a site or branch and click **Add Device** or **Add Entrance**. The **Add Devices** window appears.
2. If you have clicked **Add Device**, select the **Device Type**. The devices of the selected type are listed.
3. Select the device or entrance to be added to the branch and click **Add**.

Note: To select multiple devices, press and hold down CTRL and click each of the required devices.

Filter Devices

To filter the events that occur in the specific areas and devices, click **Control** under **Filter**. The **Filter Devices** window appears.

1. Expand the tree by clicking the plus [+] symbol.
2. Select a branch or an individual device to be filtered for monitoring.
3. To filter a branch, right-click the branch and select **Configure**. The **Set Device Selection for a Control Area** dialog box appears.

Tip: You can also double-click the branch to display the **Set Device Selection** for a **Control Area** dialog box.

4. 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.
   - **Clear selection (Filter out) for 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.
5. To filter a device, right-click the device and select **Invert Selection Status** to select the device or clear the selection.
6. 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**.

7. Click **OK** to save the filter selection.

Note: The filter settings are lost when 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**.

Find an Item

The **Find** Item dialog box enables you to search for an item in a tree-structured list.

To find an item:

1. Right-click a branch or entrance, and click **Find**.

   OR

   Press F3. The **Find** Item dialog box appears.
2. Type the item you want to search in the **Item in tree to Search** for box.
3. Click **OK**. The item, if found, is highlighted in the tree.

Note: Right-click a branch, and click **Refresh** to refresh the items in the tree.

WIN-PAK T&A User Interface Elements

This section describes the basic Web operations that are performed using the Requisition link, Setting link, Configuration link, Employee link, Management link, and Reports link.

Configure the Requisition link

You can place the following request in the Requisition link.

- Leave Request
- On Duty Request
- Attendance Correction Request
- Request Status
- Approve Request

Configure the Settings link

You can modify the user settings in the **Settings** link.

Configure the Configuration link

You can configure the following in the **Configuration** link.

- Department
- Designation
- On Duty
- Location
- Employee Type
- Correction
- Holiday
- Leave
- Shift

Configure the Employee link

You can view the following in the **Employee** link.

- New Employee(s)
- All Employees

Configure the Management link

You can manage the following operations in the **Management** link.

- Shift Rotation
- Update Supervisor
- Report Schedule
- Shift Allocation

Configure the Reports link

You can generate various reports in the **Reports** link.

- Master Report
- Shift Allocation Report
- OverTime Report
- Attendance Report
- Attendance Correction Report
- On Duty Report
- Leave Report
- Leave Balance Report

WIN-PAK CS/SE/PE Help

This section describes how to access the help topics of WIN-PAK CS/SE/PE when you are working with the user interface.

Note: WIN-PAK CS help screens are shown in this section as an example. The screens would change based on the variant selected.

Accessing the Online Help

To access the WIN-PAK CS/SE/PE Online Help, click **Help > Help Topics** or press F1 on the keyboard.

Accessing Help on Web

WIN-PAK CS/SE/PE

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 CS/SE/PE.

To access the Honeywell Access Systems website:

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

To view Honeywell contact details:

1. Click **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**.

WIN-PAK T&A

You can access any informations related to the Time and Attendance from the web.

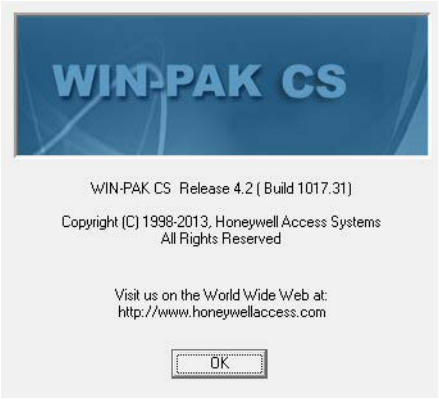
To access help in the Time and Attendance website:

1. Click **Help** at the top right corner. The **Time and Attendance User's Guide** appears.

About WIN-PAK CS

For information about the copyright, build, and serial number details of WIN-PAK CS:

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



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

WIN-PAK T&A User Account

The user account option enables you to perform the following:

- Change Password
- Approvals
- Request Raised
- Log Out

Change Password

To change the User Account password:

1. Click the **User Name** (based on the login type) displayed at the top right corner and then click **Change Password**. The **Change Password** dialog box appears.
2. Enter the following details.
    a. **Current Password**: Type the existing password which is used for accessing the Web interface.
    b. **New Password**: Type a new password for accessing the Web interface.
    c. **Confirm Password**: Repeat the password for accessing the Web interface.
3. Click **Save**. The new password for accessing the Web interface is set.

Approvals

To view approvals:

1. Click **User Name** (based on the login type) at the top right corner and then click **Approvals**.

    The list of all the approvals appears.

Requests Raised

To view the list of requests raised:

1. Click **User Name** (based on the login type) at the top right corner and then click **Request Raised**.

   The list of all the requests appears.

Log Out

To Log Out of the system:

1. Click the **User Name** (for example, super administrator, administrator, supervisor, or user) at the top right corner and then click **Log Out**.

   You are successfully logged out from the Web interface.

Getting Started

4

In this chapter...

This chapter describes about the Introduction, Client Server Configuration, System Manager, Service Manager, and User Interface of WIN-PAK CS/SE/PE, and T&A.

Section	WIN-PAK CS	WIN-PAK SE/PE	WIN-PAK T&A
Client Server Configuration: Domain Environment**, page 121**	✓	✓	
System Manager: Setting RPC Endpoints, page 126	✓	✓	
System Manager: Setting User Interface Workstation, page 127	✓	✓	
System Manager: Setting WorkGroup Environment, page 128	✓	✓	
System Manager: Comparison between Domain and Workgroup Environment of WIN-PAK CS/SE/PE, page 129	✓	✓	
System Manager: Setting Server Location in WIN-PAK CS, page 129	✓		
System Manager: Firewall Exception Settings for WIN-PAK SE/PE, page 130		✓	
User Interface: Logging on to WIN-PAK CS/SE/PE, page 138	✓	✓	
User Interface: Logging on to WIN-PAK T&A, page 139			✓
User Interface: Logging off from WIN-PAK CS/SE/PE, page 140	✓	✓	
User Interface: Logging off from WIN-PAK T&A, page 140			✓

Section	WIN-PAK CS	WIN-PAK SE/PE	WIN-PAK T&A
User Interface: WIN-PAK T&A Wed interface, page 140			✓
User Interface: Quitting WIN-PAK CS/SE/PE, page 140	✓	✓	

Introduction

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

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

Client Server Configuration

WIN-PAK CS/SE/PE 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 all the servers and the 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 allow the WIN-PAK CS/SE/PE services from Firewall protection.

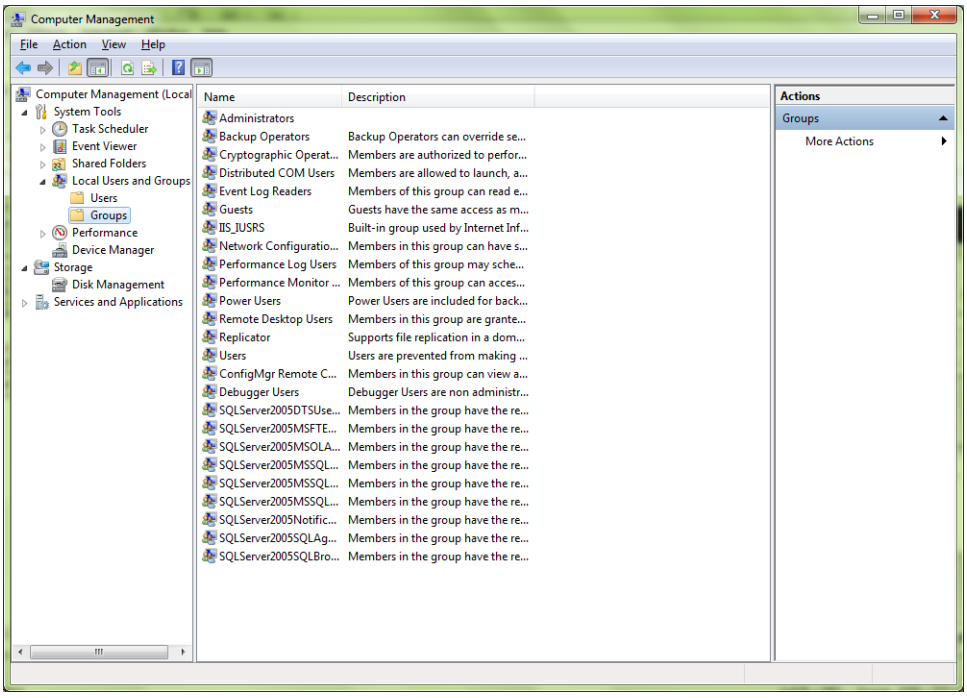
Adding Domain Users

To add the domain users:

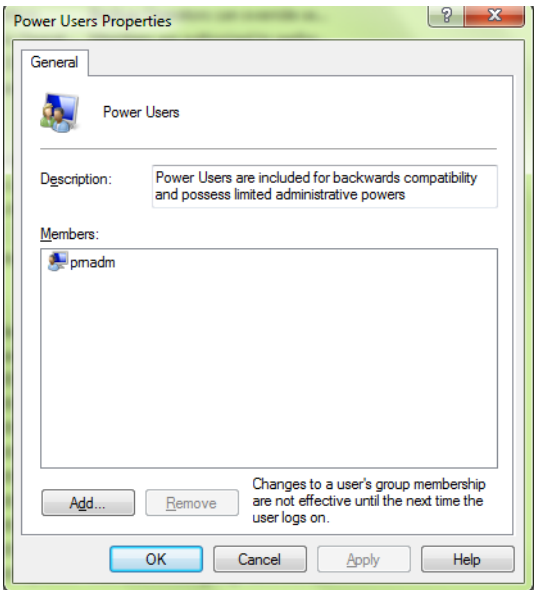
1. Log on to the system as Administrator where WIN-PAK CS/SE/PE Servers are installed.
2. Click **Start** > **Settings** > **Control Panel** and open **Administrative Tools** > **Computer Management**. The **Computer Management** window appears.

Note: If Windows XP is installed on your computer, switch to Windows Classic view.

3. Choose **System Tools > Local Users and Groups** > **Groups**.

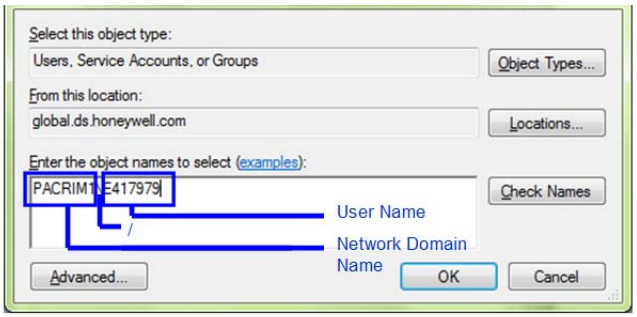


4. On the navigation pane, select and double-click **Power Users**. The **Power Users Properties** dialog box appears.

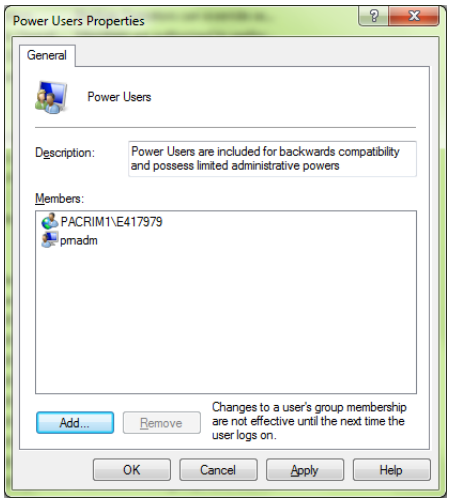


5. Click **Add** to add domain users to the group.

6. Type the network domain name and the 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.

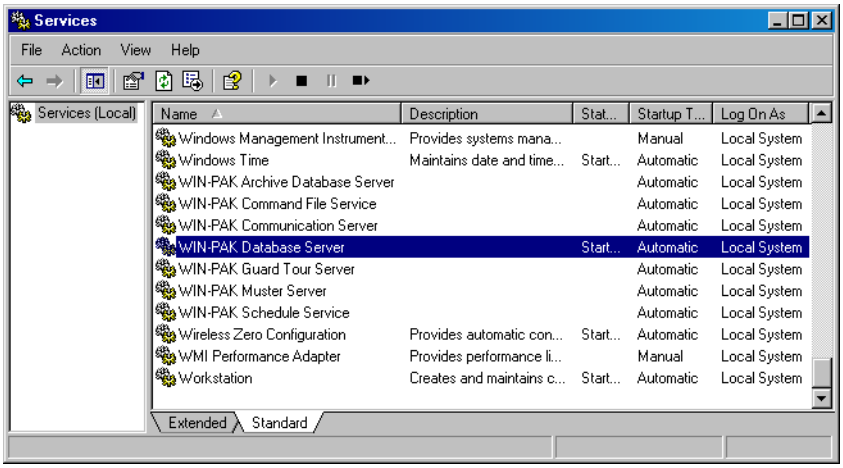
Configuring the Log On Property of WIN-PAK CS/SE/PE Servers

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

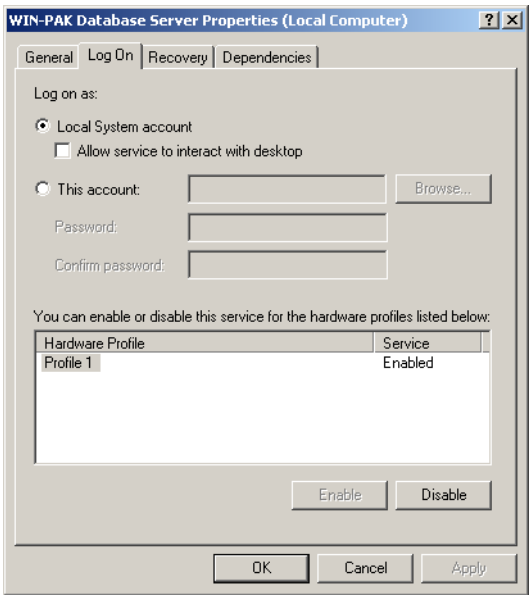
To configure the log on property of WIN-PAK CS/SE/PE Servers:

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 CS/SE/PE servers.

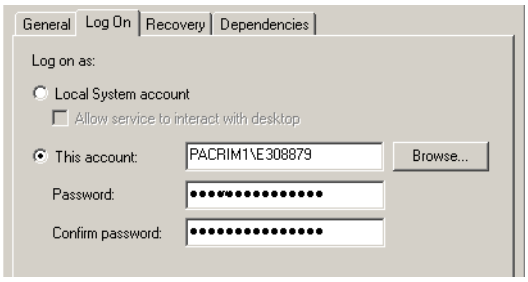


2. Select and double-click the required WIN-PAK CS/SE/PE Server from the right pane of the **Services** window. The **WIN-PAK CS/SE/PE Server Properties** window appears.



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 CS/SE/PE Servers.

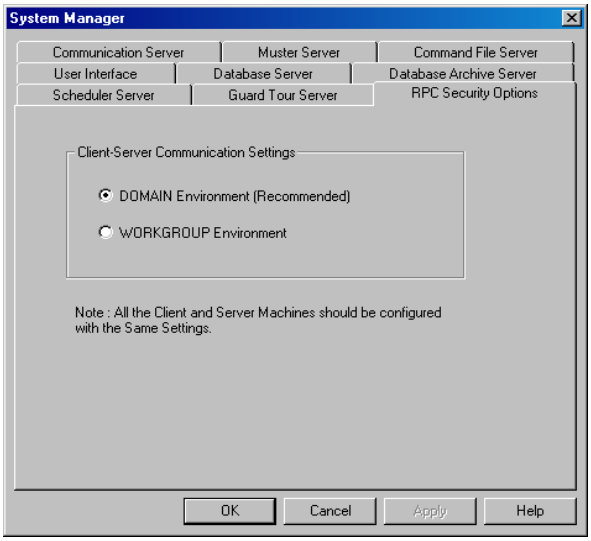
Notes:

- Restart the system to see the changes.
- Log on to the WIN-PAK CS/SE/PE Server System using any account; local or domain. However, the client system must be logged on with the domain user account.
- The username and password of the administrator is required to access the WIN-PAK application which has a Windows user/account without administrator privileges and is enabled with User Account Control (UAC).

Setting Domain Environment

To set the domain environment:

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



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

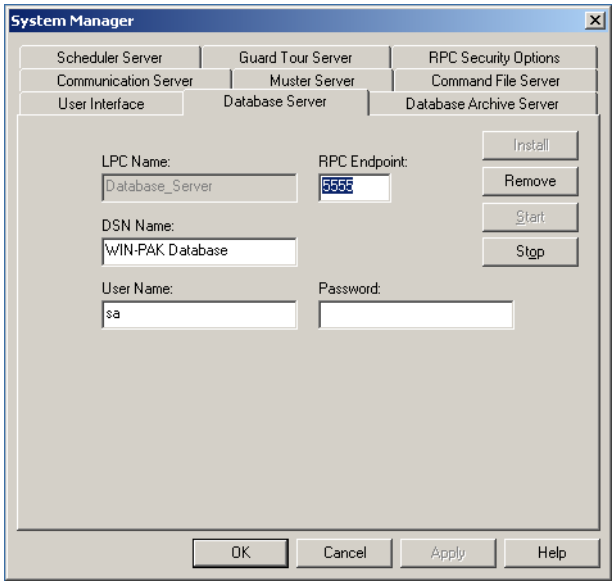
System Manager

The System Manager is a utility in WIN-PAK CS/SE/PE to locate its various software components. The machine name and the 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 > 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.

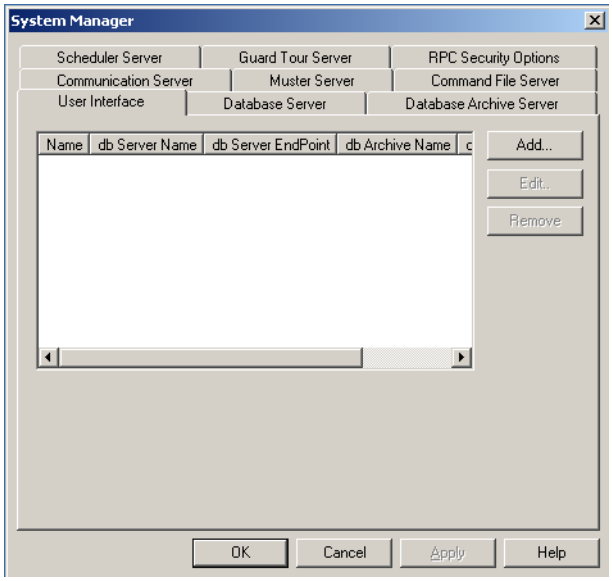
6. Click **OK** to save the changes.

Setting User Interface Workstation

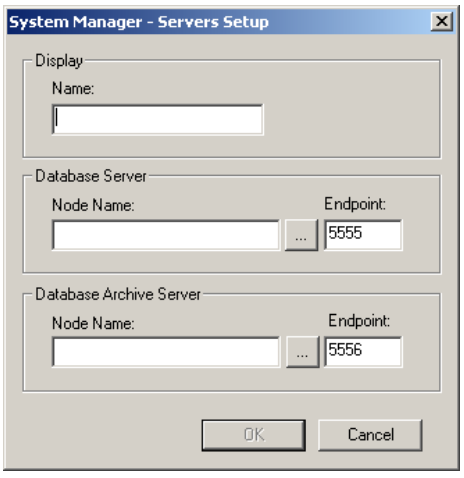
Ensure that you quit the WIN-PAK CS/SE/PE User Interface, prior to setting the User Interface workstation.

To set the user interface workstation,

1. Click **Start > Programs > Honeywell Access Systems > 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. Type a descriptive **Name** to identify the database server from the list.
5. Type 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 the System Manager window, which is detailed in the section "Setting RPC Endpoints".

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 the System Manager window, which is detailed in the section "Setting RPC Endpoints".

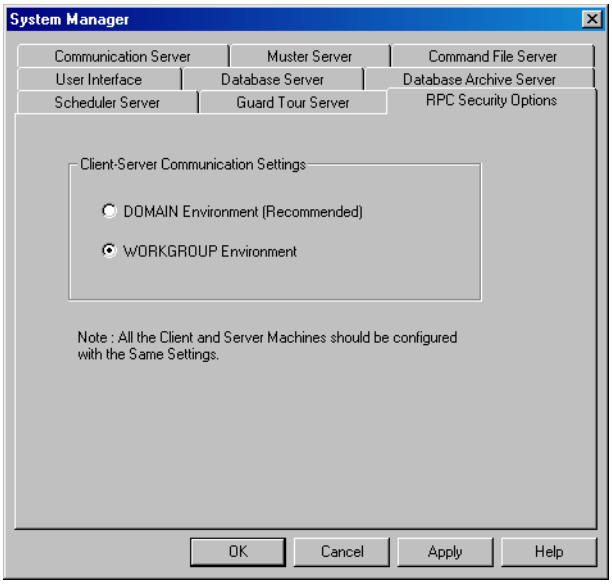
7. Click **OK**. This enables you to start up the User Interface with the new database server.

Setting WorkGroup Environment

To work in a Workgroup Environment, you must set the workgroup environment and then clear the WIN-PAK CS/SE/PE 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 CS/SE/PE services must be allowed before proceeding further.

Comparison between Domain and Workgroup Environment of WIN-PAK CS/SE/PE

The following table compares the configuration between Domain Environment and Workgroup Environment of WIN-PAK CS/SE/PE:

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.
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 allowing all the WIN-PAK CS services and client from Windows Firewall protection. **Note:** In Windows Server 2003, disable the Firewall protection to allow DOMAIN connectivity.	Requires allowing all the WIN-PAK CS services and client from Windows Firewall protection. **Note:** In Windows Server 2003, disable the Firewall protection to allow WORKGROUP connectivity.

Setting Server Location in WIN-PAK CS

You can use the following steps to set the location for all the servers in WIN-PAK CS.

Note: If the communication between a server and WIN-PAK CS fails, a message is displayed, with the name of the corresponding server.

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK System Manager**. The **System Manager** window appears.
2. Click the appropriate server tab.
3. Type the **DB Server Node Name**. This is the location for the Database Server.
4. Type the **DB Server Endpoint** value.
5. Click **OK** to save the changes.

Note: For the **Schedule Server**, set the value for the Report Connection Timeout.

Firewall Exception Settings for WIN-PAK SE/PE

A Windows Firewall Security Alert notifies you that the Windows Firewall is blocking a particular program. When this scenario occurs, you can unblock the program by selecting Unblock this program in the Security Alert dialog box.

External Reference

- For information on firewall settings for **Windows 7**, visit the website: http://www.techtalkz.com/windows-7/515977-how-configure-windows-firewall-windows-7-a.html
- For information on firewall settings for **Windows Server 2008**, visit the website: https://www.google.co.in/#q=firewall+settings+for+windows+server+2008
- For information on firewall settings for **Windows Server 2008 R2**, visit the website: http://windowsitpro.com/windows/windows-server-2008-r2-firewall-security
- For information on firewall settings for **Windows Server 2012**, visit the website: http://www.rackspace.com/knowledge_center/article/managing-the-windows-server-2012-firewall

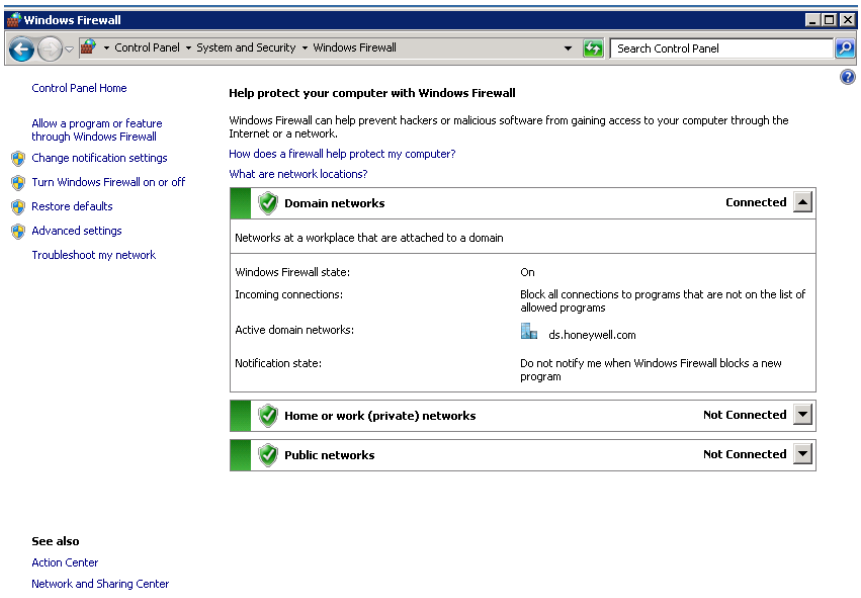
Note: The firewall exception settings are applicable for Windows 8/8.1 and Windows Server 2012 R2.

Unblocking WIN-PAK SE/PE Services on Windows 2008 Server

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

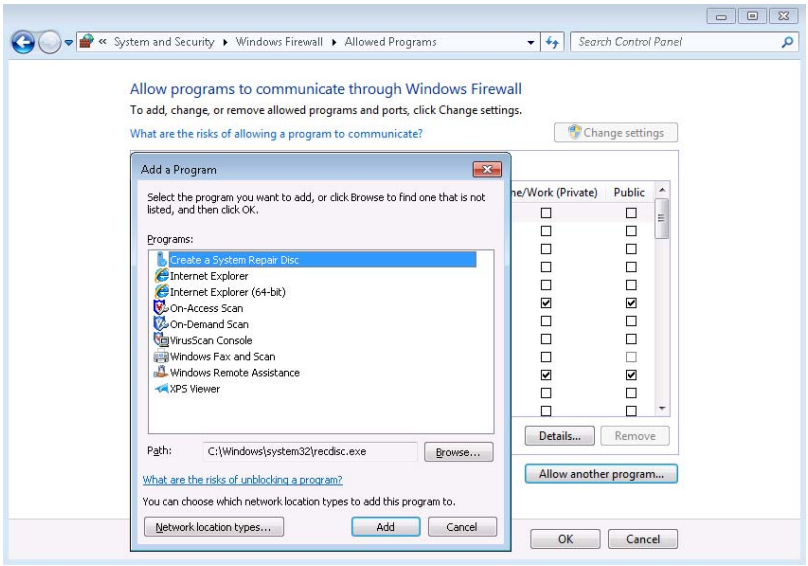
To check Firewall Status and unblock WIN-PAK SE/PE Services:

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



3. In the left pane of the **Windows Firewall** window, click the **Allow a program or feature through Windows Firewall**. The **Allow programs to communicate through Windows Firewall** window appears.

4. Click **Allow another program** to add the WIN-PAK SE/PE services as exceptions from Windows Firewall protection. The **Add Program** dialog box appears.



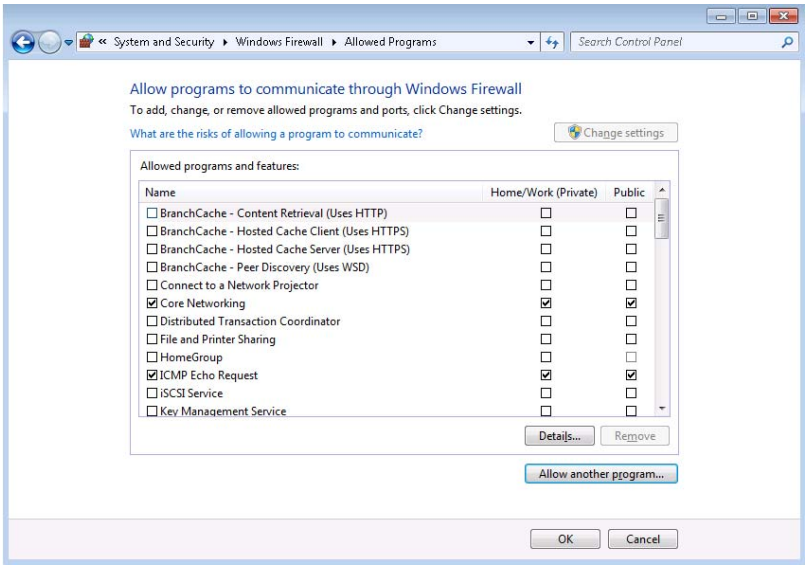
5. Select the following WIN-PAK SE/PE services and click **Add**.

   - WIN-PAK SE/PE User Interface
   - NCIArchive

- NCICore
- WP CmdFile Service
- WP Communications Server
- WP GuardTour Service
- WP Muster Service
- WP Schedule Service
- WP Video Management Service
- Trinity.SystemServices.exe
- Trinity.Controller.exe

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

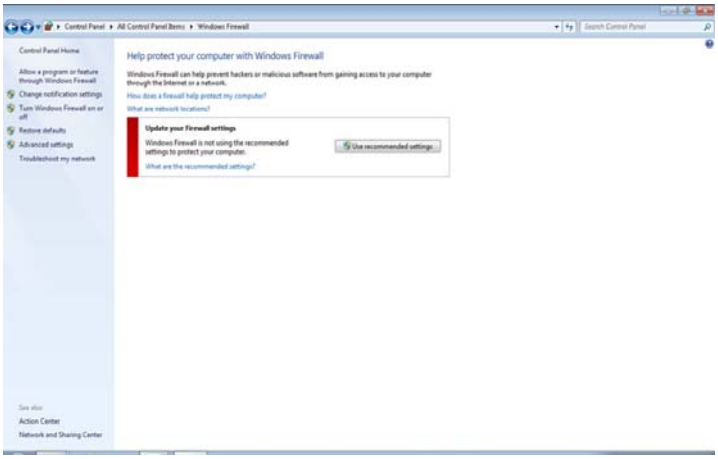
6. In the **Allow programs to communicate through Windows Firewall** window, select **Core Networking** check box to unblock the WIN-PAK SE/PE Database Server.



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

The procedure for Unblocking the WIN-PAK SE/PE Services in Window 7 is similar to that

Tip: See the following figure and unblock the WIN-PAK SE/PE Services in Windows 7.

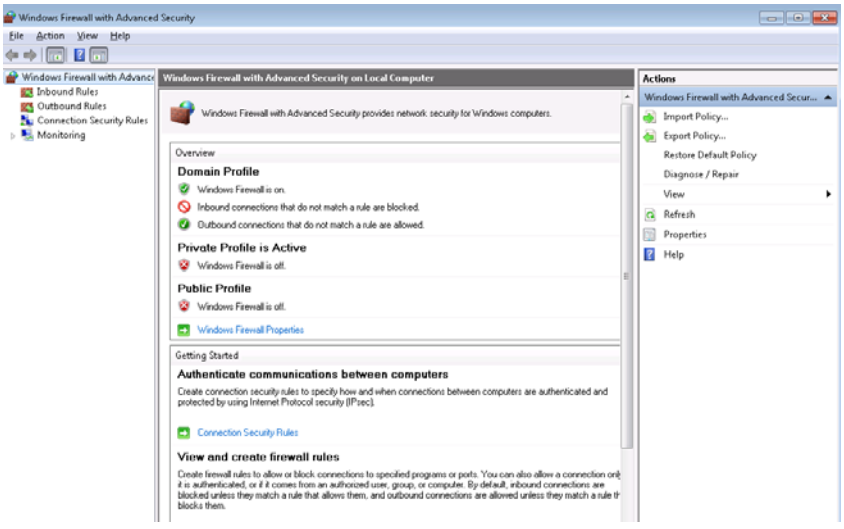


Enabling Ports in Windows 7

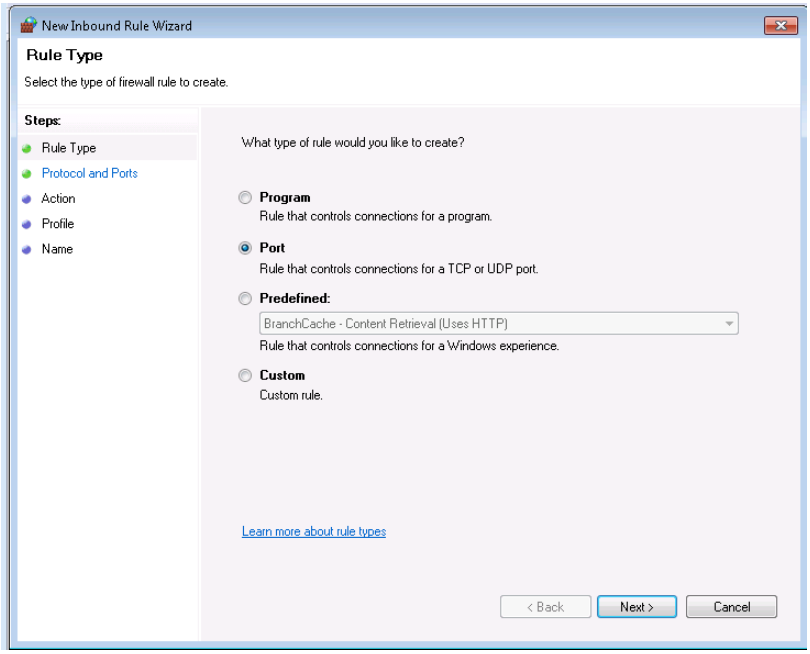
Communication ports in a Windows 7 operating system are disabled for security reasons by Windows Firewall. These ports must be enabled for remote communication to the Galaxy panel.

To enable ports in the Windows Firewall:

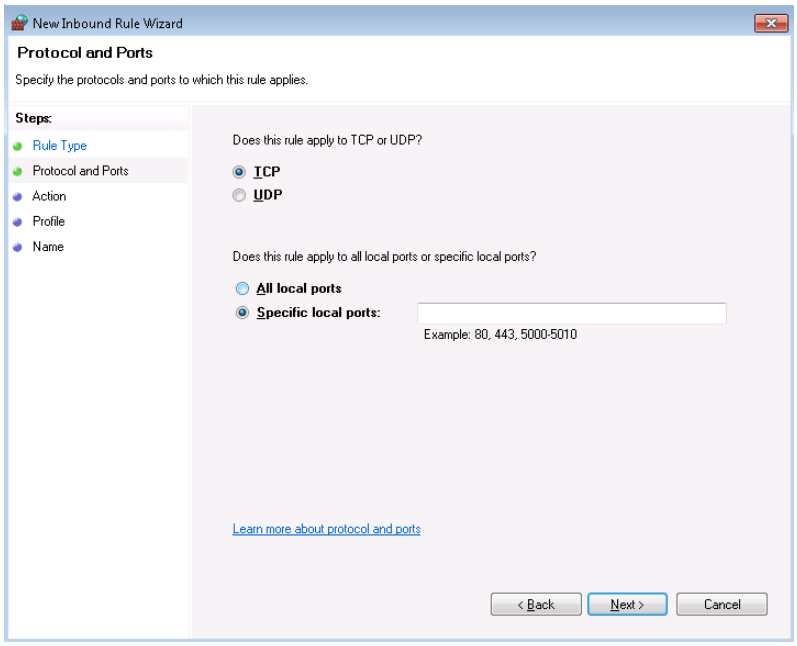
1. Click **Start > Settings > Control Panel** > **System and Security** and open **Windows Firewall**. The **Windows Firewall** window appears.
2. In the left pane of the **Windows Firewall** window, click **Advanced Settings**. The **Windows Firewall with Advanced Security** window appears.



3. Click **Inbound Rules**, and then, in the right pane, click **New Rule**. The **New Inbound Rule Wizard** page appears.

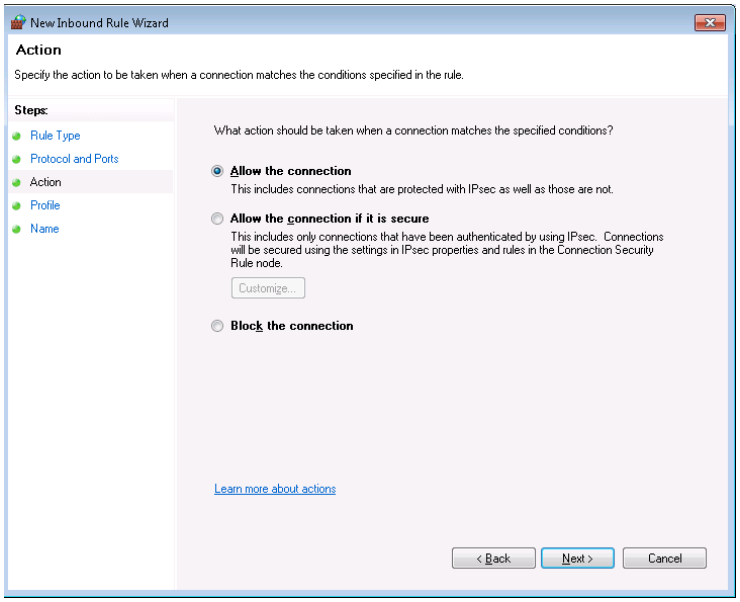


4. Click **Next**. The **Protocol and Ports** page appears.

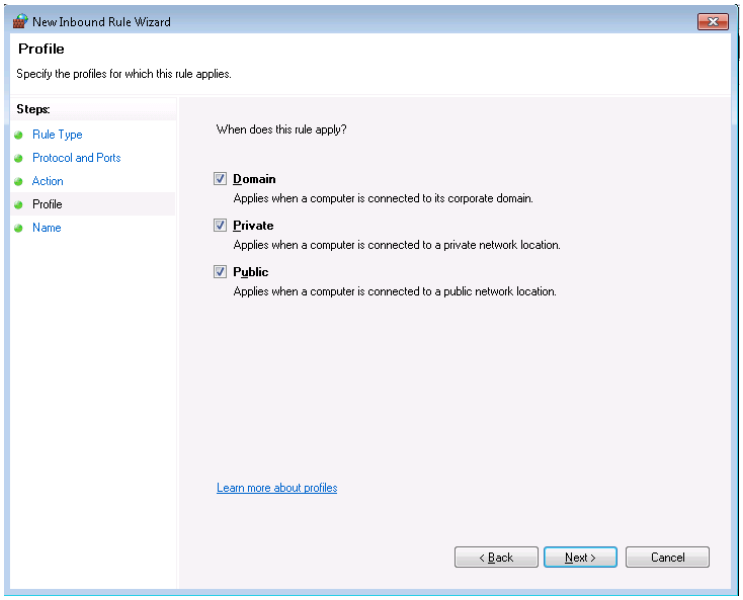


5. Under **Protocol and Ports**, click **TCP** or **UDP** to select the type of port.

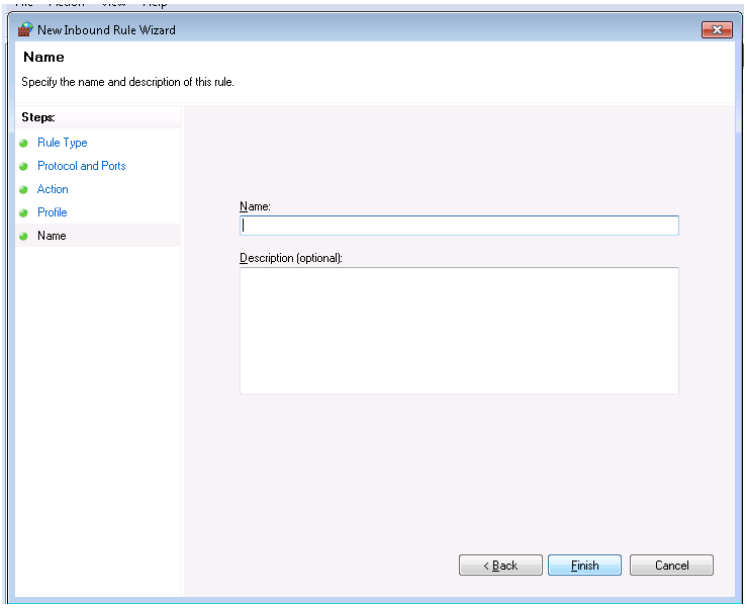
6. Type the **Specific local ports** and then click **Next**. The **Action** page appears.



7. Under **Action**, select **Allow the connection** and then click **Next**. The **Profile** page appears.



8. Under **Profile**, select the scenarios when the rule must be applicable and then click **Next**. The **Name** page appears.



9. Under **Name**, type a **Name** and **Description** for the new port.
10. Click **Finish** to create a new rule and enable the new 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.

Video Management Server Services and Ports

The following services must be excluded in Firewall settings for Video Management Server.

- Trinity.SystemServices.exe
- Trinity.Controller.exe

The following ports must be enabled and opened in Firewall settings for Video Management Server.

Name	Port Number
Trinity Server	20007
Trinity Controller	26026
Trinity Scheduler	20010

Name	Port Number
RapidEye DVR	10000
Fusion DVR	4000
HRDP	4000, 7001
MAXPRO NVR	20007, 26026

Service Manager

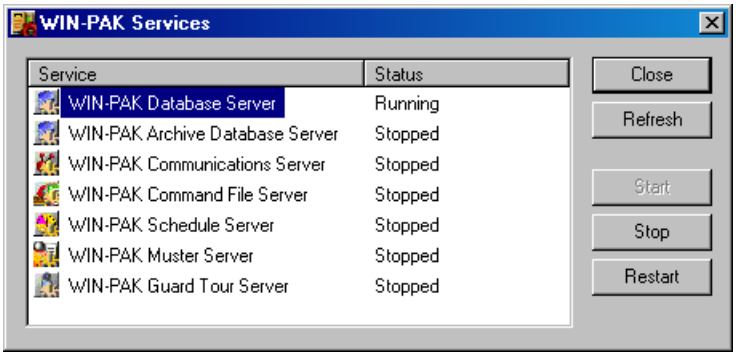
The WIN-PAK CS/SE/PE Service Manager enables you to start and stop the WIN-PAK CS/SE/PE services.

Note: WIN-PAK SE/PE Services running on Microsoft Windows® 7 and Microsoft Windows® Server 2008 Operating system are configured to Automatic (Delayed Start).This delayed start is configured to ensure that SQL starts before WIN-PAK connects. In this scenario, if you try to log on to WIN-PAK SE/PE after a Windows restart (before WIN-PAK SE/PE Services start up), then the error message " Database Connection Failed" appears. The only workaround is to log on to WIN-PAK SE/PE after some time (after the services are up and running).

To start or stop the WIN-PAK CS/SE/PE services:

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK CS/SE/PE Service Manager**. The **WIN-PAK CS/SE/PE 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 start the service again.
5. Click **Refresh** to refresh the services.

User Interface

This chapter describes how to log on and log off from WIN-PAK User Interface, also it enables you to add, monitor and controls devices, card holders, operators, and so on.

Logging on to WIN-PAK CS/SE/PE

Notes:

- Before logging on to WIN-PAK CS/SE/PE, 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 CS/SE/PE:

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

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

Notes:

- By default, the user name "Admin" and a blank password are created by WIN-PAK CS for initial log on. However to ensure security, you must add a password.
- 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. See Setting User Interface Workstation sections for more information.

3. Click **Connect**. The system connects to the servers and the WIN-PAK CS/SE/PE User Interface main window appears.

Notes:

- The CD Key becomes invalid, when you remove the WIN-PAK CS system and install it again.
- Administrator has privileges to access all Accounts whereas Operator has privileges to access only certain accounts. The title bar of the WIN-PAK SE/PE Main windows displays the name of the active account.

Logging on to WIN-PAK T&A

Note: Honeywell recommends you to install the WIN-PAK T&A application on Google Chrome or Firefox.

To log on to WIN-PAK T&A:

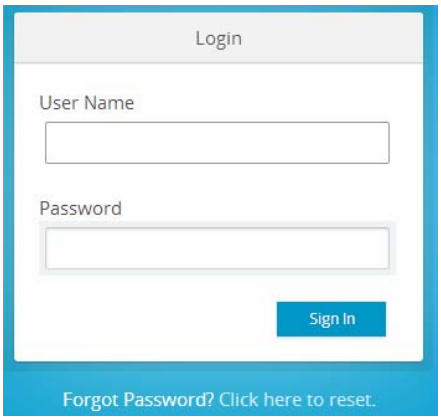
1. Type the following URL in your Web Browser.
   HTTPS://<ipaddress or machine name>/TimeAndAttendance/

   Where, the IP address or machine name refers to the IP address or the name of the computer, where the Web interface is installed.

   OR

   Double click the **Time and Attendance** icon on the desktop.

   The WIN-PAK T&A Web login screen appears.



2. Type your **User Name**.

Note: For the first login, the default **User Name** is **admin** and **Password** is **Admin123**.

3. Type your **Password**.

Note: If the log on is unsuccessful after three consecutive attempts, you need to retry after five minutes.

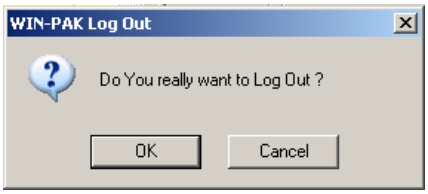
4. Click **Sign In**. The **WIN-PAK T&A Settings** page appears after you have logged on.

Note: Administrator has privileges to access all options whereas an Operator has privilege to access only certain options.

Logging off from WIN-PAK CS/SE/PE

To log off from WIN-PAK CS/SE/PE:

1. In the WIN-PAK CS/SE/PE User Interface main window, from the **File** menu, choose **Log Out** or click from the tool bar. The confirmation dialog box appears.



2. Click **OK** to confirm.

Note: Logging Off from WIN-PAK CS/SE/PE does not automatically stop the WIN-PAK CS/SE/PE services.

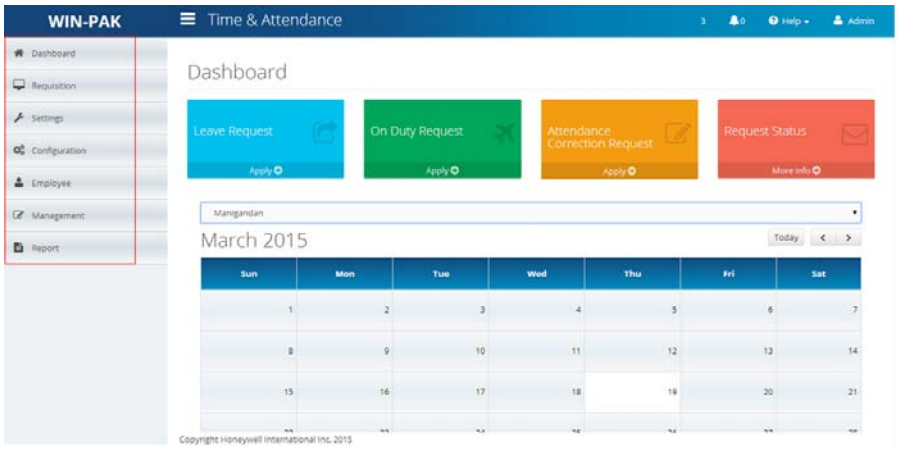
Logging off from WIN-PAK T&A

To log off from WIN-PAK T&A:

- In the WIN-PAK T&A User Interface main page, click **Admin** > **Log Out**.

WIN-PAK T&A Wed interface

The basic Web operation related to configuration, settings, management, and reports can be performed by clicking the respective links, which are highlighted in the following figure.



Quitting WIN-PAK CS/SE/PE

To quit the WIN-PAK CS/SE/PE application:

1. On the **File** menu, click **Exit**. A confirmation message appears.

2. Click **Yes** to quit the application.

System Settings

5

In this chapter...

This chapter describes about the Overview, Accounts, Administrator, Operators, Customers, Default Settings, Database Maintenance, and Database Limits and Capacities of WIN-PAK CS, and SE/PE.

Overview

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

Accounts

This section describes in detail about configuring the accounts. Accounts in WIN-PAK CS are configured with the access related information of the customers. Whereas in WIN-PAK SE/PE the card and card holder information are specific to an account. Therefore, you must select an account to enable card and card holder menu options.

WIN-PAK CS/SE/PE Users

This section describes in detail about configuring users and assigning privileges to them.

Users of WIN-PAK CS/SE/PE are of the following types:

- Administrator
- Operator
- Customer

Note: The user type Customer is available only in WIN-PAK CS.

An administrator has full privileges (view, change, and delete) to work in WIN-PAK CS/SE/PE. Operators and customers have restricted privileges, which are defined by operator levels and customer levels.

When you install WIN-PAK CS/SE/PE on your computer, a default user is created for logging on to WIN-PAK CS/SE/PE 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 and the system settings for a workstation. Default can be changed for alarm printer, sound files, e-mails for reporting alarms, auto log on, and so on.

In the WIN-PAK CS/SE/PE system, these settings are configured by default and WIN-PAK CS/SE/PE functions as per these settings. All the client systems of WIN-PAK CS/SE/PE are 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

An account in WIN-PAK CS is a record of user and device details specific to a customer. The corresponding menus in the WIN-PAK CS UI are available only when an account is selected. The information pertaining to an account is not visible to any other account. Therefore, an account can be configured specific to a customer. The System account in WIN-PAK CS enables you to view information of all the accounts.

Similarly, using WIN-PAK SE/PE accounts, 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.

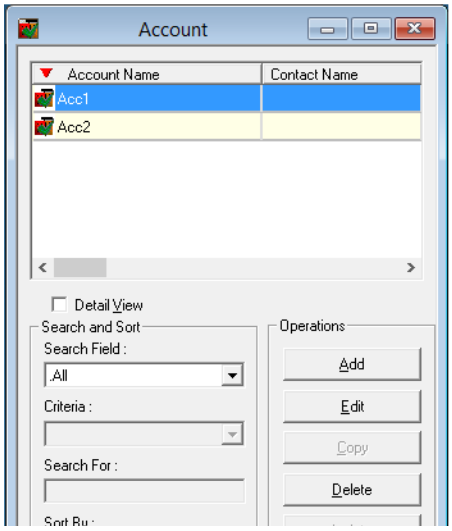
Newly added cards and card holders must be added to a specific account. Therefore, card holder tab menus in the WIN-PAK SE/PE UI are available only when an account is selected.

Note: WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

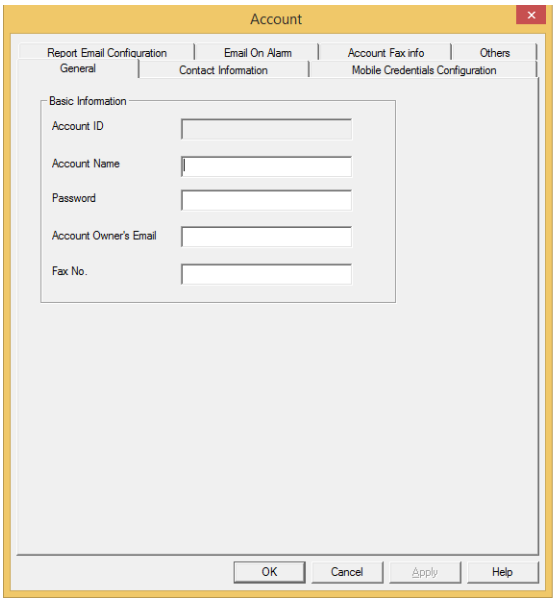
Adding an Account

To add an account in WIN-PAK CS

1. From the **Account** menu, choose **Edit**. The **Account** dialog box appears.



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

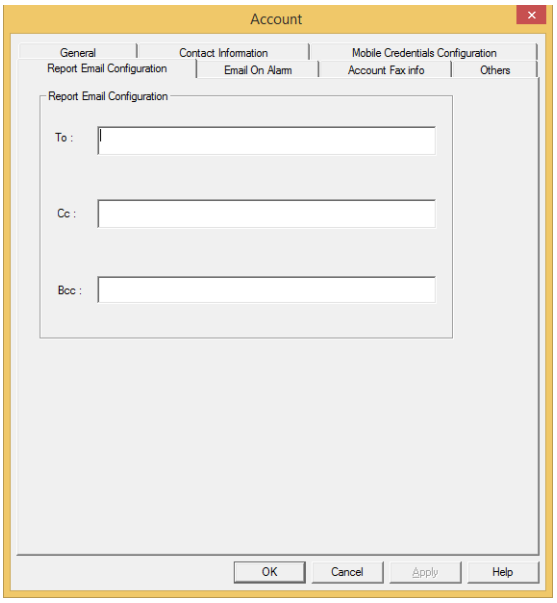


3. In the **General** tab, type the following details of the account:

Table 5-1 General account information

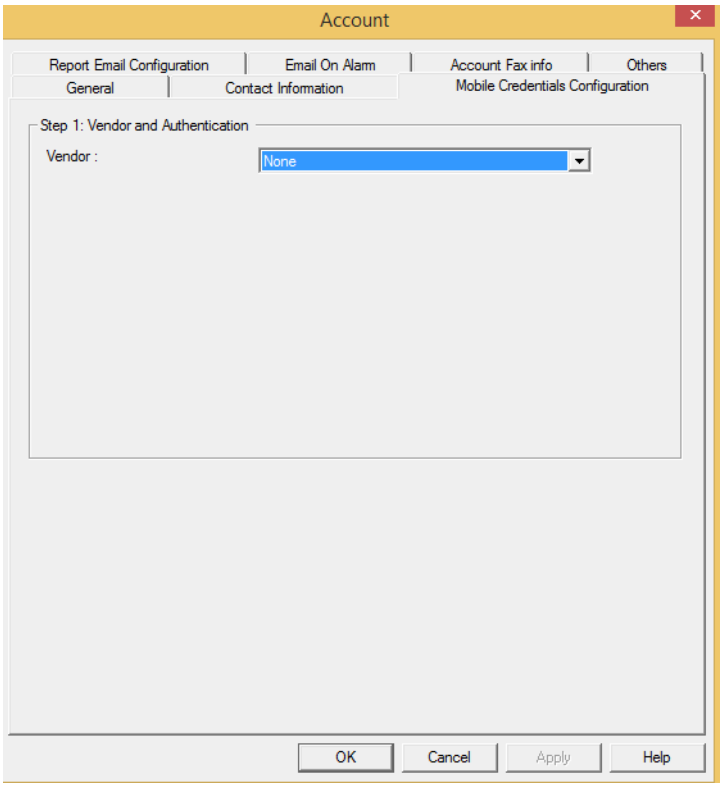
Field	Description
Account Name	The name of the account. You can enter a maximum of 30 alphanumeric characters.
Password	The password for logging on to the account in WIN-PAK CS.
Account Owner’s E-mail	The e-mail ID of the account owner.
Fax No.	The fax number of the account owner.

4. Click the **Contact Information** tab to type the name, telephone number and address of the contact.
5. Click the **Report Email Configuration** tab to type the e-mail Ids of the users to whom the reports specific to this account must to be sent. You can enter multiple e-mail IDs separated by semi-colons. **Cc** and **Bcc** fields can be used for copying mails to additional users when required.

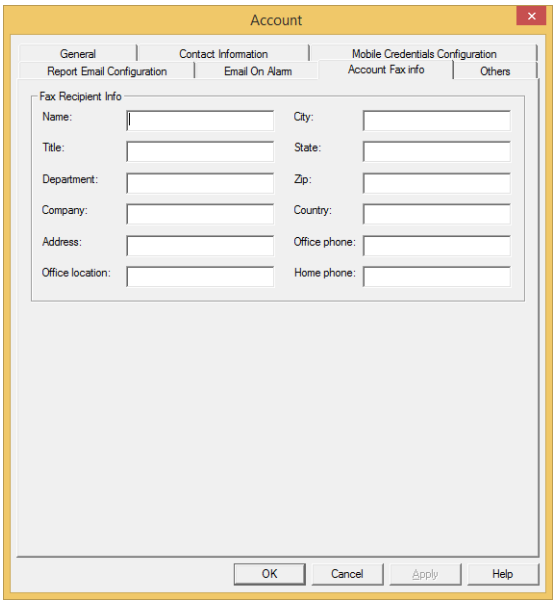


6. Click the **Email on Alarm** tab to type the e-mail Ids of the users to whom the alarm details must be sent. You can enter multiple e-mail IDs separated by semi-colons. **Cc** and **Bcc** fields can be used for copying mails to additional users when required.

7. Click the **Mobile Credentials Configuration** tab to configure the access control cards by HID.



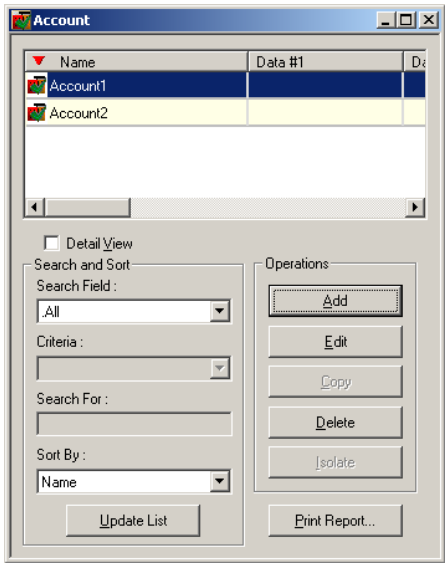
8. From the **Vendor** drop-down list under **Vendor and Authentication**, select **HID**.
9. Click the **Account Fax info** tab to type the fax recipient's information.



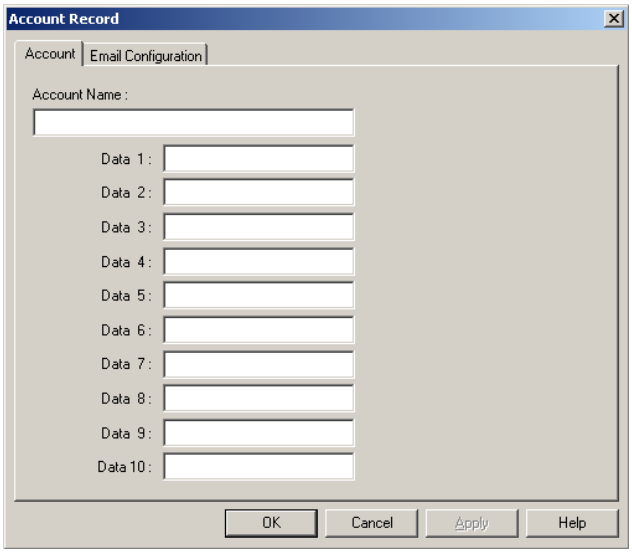
10. Click the **Others** tab to type any additional information pertaining to the account.
11. Click **OK** to save the account information.

To add an account in WIN-PAK SE/PE

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

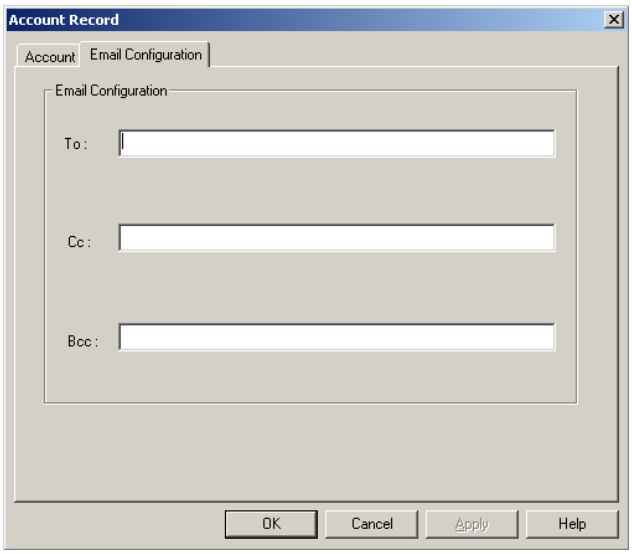


2. Click **Add** to add a new account. The **Account** dialog box appears.



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.

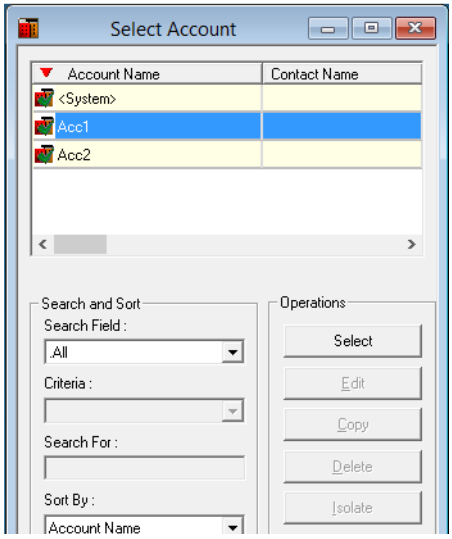


6. In the **To** box, type the e-mail ID of the user to whom the account-specific alarms must be reported.
7. Click **OK** to save the account information.

Selecting an Account

To select an account in WIN-PAK CS/SE/PE:

1. From the **Account** menu, choose **Select**, press **F2** or click the  icon in the toolbar**.** The **Select Account** dialog box appears.



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

Note: If the operator logged on to the application is the administrator, all the accounts in the WIN-PAK CS system are available for selection, including the **System** account.

Editing an Account

To edit an account in WIN-PAK CS/SE/PE:

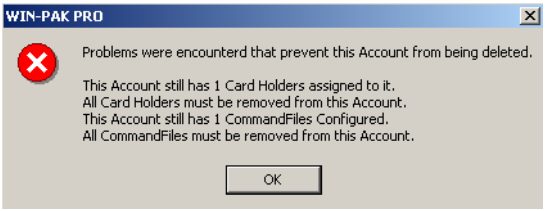
1. From the **Account** menu, choose **Edit**. The **Account** dialog box appears.
2. Click the desired account to be edited and then click **Edit**. The **Account** dialog box appears.
3. Make the necessary changes to the account.
4. Click **OK** to save the changes to the account.

Deleting an Account

To delete an account in WIN-PAK CS/SE/PE:

1. From the **Account** menu, choose **Edit**. The **Account** dialog box appears.
2. Click the account you want to delete, and then click the **Delete** button.

Note: If the account you want to delete is used by one or more entities in the system, a prompt with all the entities dependent on the account, is displayed. To successfully delete this account, isolate the dependent entities.



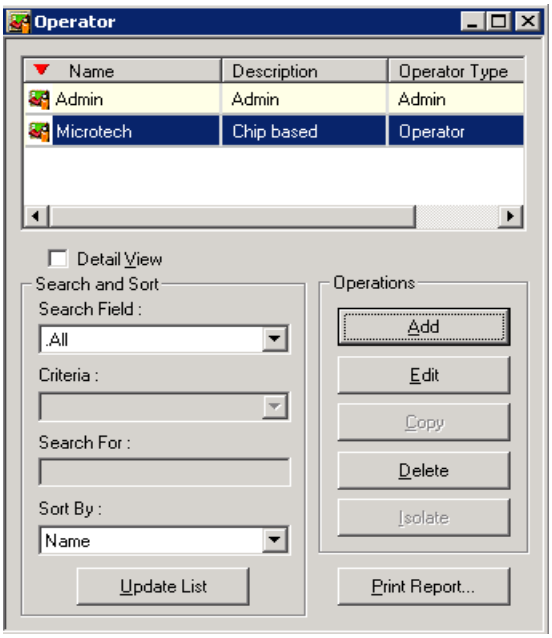
Administrator

By default, the administrator is created when the WIN-PAK CS/SE/PE User Interface is installed. The user name is admin with a blank password. You can change the user name and password to ensure security.

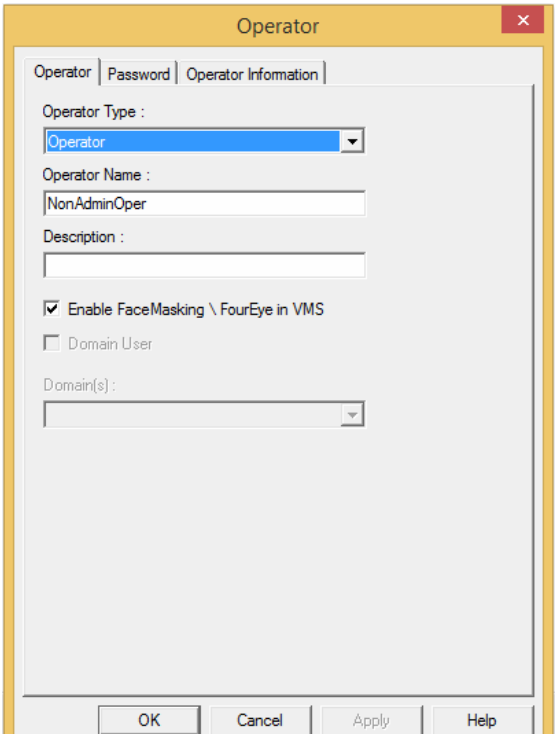
Caution: Do not forget the Admin login password. If you forget the password, contact the Customer Service to reset your password. The password reset is associated with a cost.

To change the default settings for the Administrator:

1. From the **System** menu, choose **Operator**. The **Operator** window appears.



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



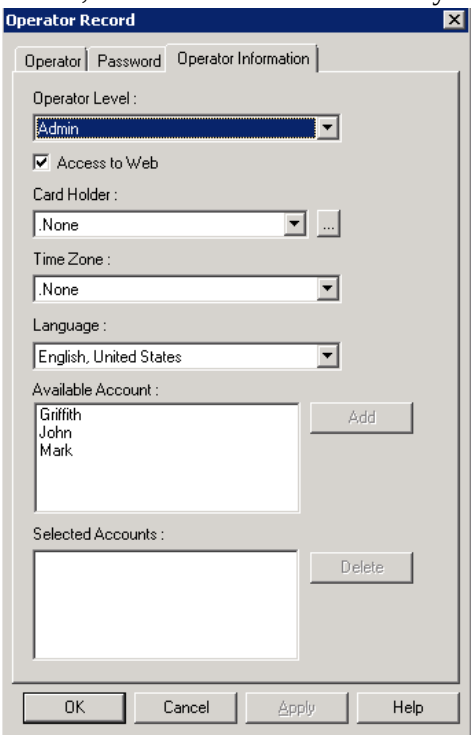
3. In the **Operator** tab, change the **Operator Type**, **Operator Name**, and **Description**, if required.
4. Click the **Password** tab to set the new password for the Administrator.

a. Type the **New Password** for the Administrator to log on. This field is mandatory. Password is case-sensitive and you can enter a 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, language used by the operator, and so on.

Note: When you select Operator as the Operator Type, all options are enabled in the Operator Information tab. When the selected Operator Type is Customer or Administrator, the web access is available by default.



The time zone is the duration, the operator can work on WIN-PAK CS/SE/PE.

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. Select the accounts the Administrator must access under **Available Account** and click **Add**.

   The **Selected Accounts** displays the list of accounts which are selected. You can click **Delete** to delete any selected account.

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

Notes:

- If you are in WIN-PAK CS to add a Customer, perform the following additional steps:
    a. Select the **Operator Level** from the list.
    b. Select the **Time Zone** during which the operator is provided card access.
- To add an Operator, in addition to the above steps, select the **Access to Web** check box to provide access to the Web Interface application.

Operators

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

Note: WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

Operator Levels

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

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

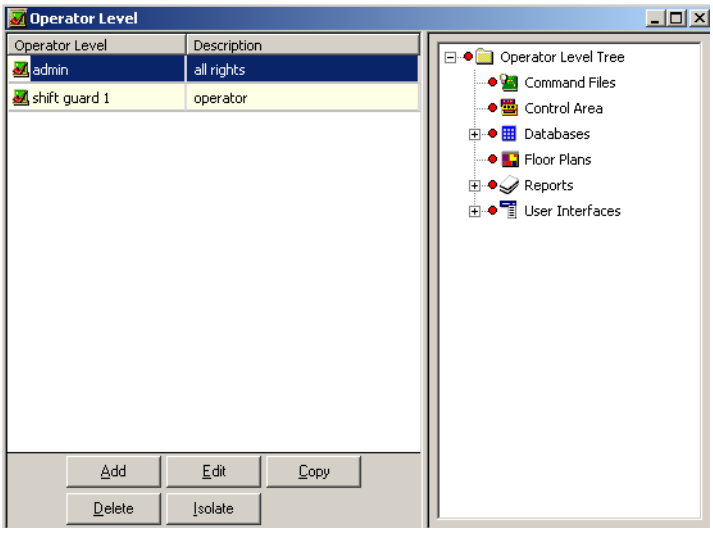
- **Command Files** - To run the command files.
- **Control Area** - To control devices in the control area through Control Map.
- **Databases** - To configure Card Holder, Cards, Floor Plan, and so on.
- **Floor Plans** - To open the floor plans.
- **Reports** - To run the reports.
- **User Interfaces**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

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

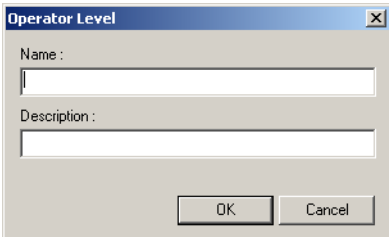
Adding an Operator Level

To add an Operator level:

1. From the **System** menu, choose **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.

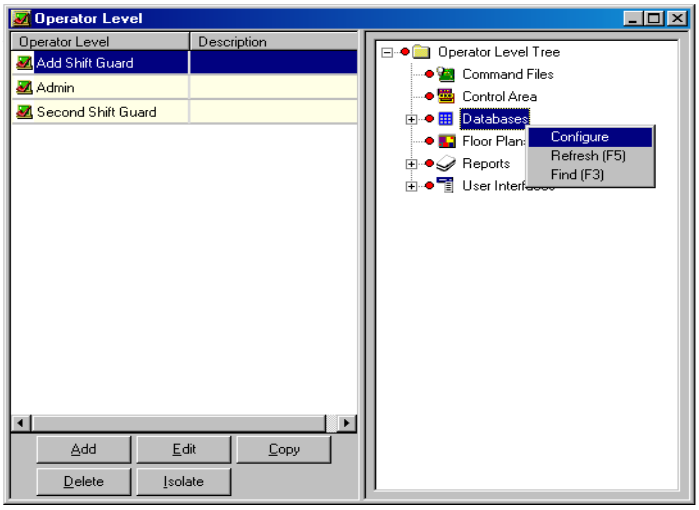
Configuring Operator Levels

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

To configure access rights for an operator level:

1. From the **System** menu, choose **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.

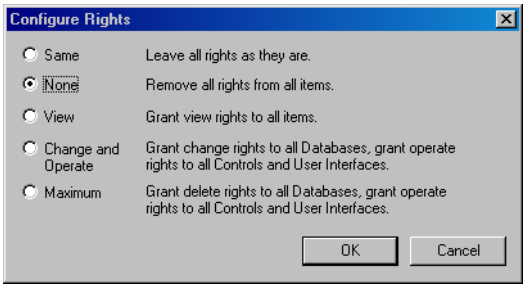


2. In the left-pane, select an operator level in the **Operator Level** list.
3. Right-click the control area device, database, or user interface to configure.
4. Configure rights for an entire branch, an individual device, database, report or user interface element.

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**. The **Configure Rights** dialog box is displayed.



2. Select the appropriate Rights configuration for the Operator Level, and then click **OK**.

Configuring rights for an individual device

To configure access rights at a device level:

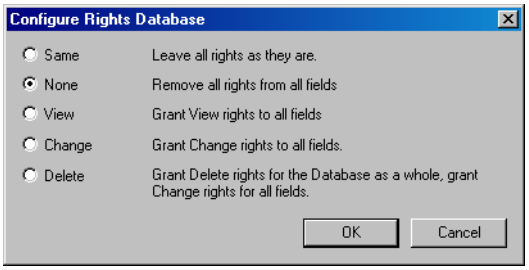
1. In the **Operator Level** window, expand the branch and select a device.

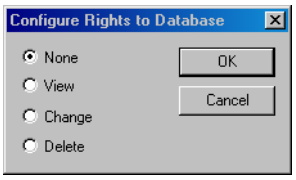
2. Right-click the device and select **Configure**. The **Configure Rights** dialog box appears.

3. Select the appropriate Rights configuration, and then click **OK**.

Configuring 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.

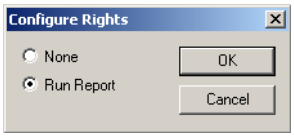




3. Select the appropriate option to set the rights for the database.

Configuring rights for reports

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** window appears.

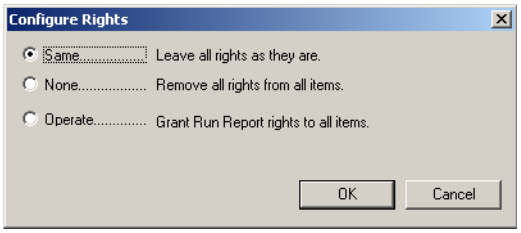


3. Click **None** to provide no access or click **Run Report** to provide rights for running the selected report.
4. Click **OK**.

To assign the same rights to all the reports:

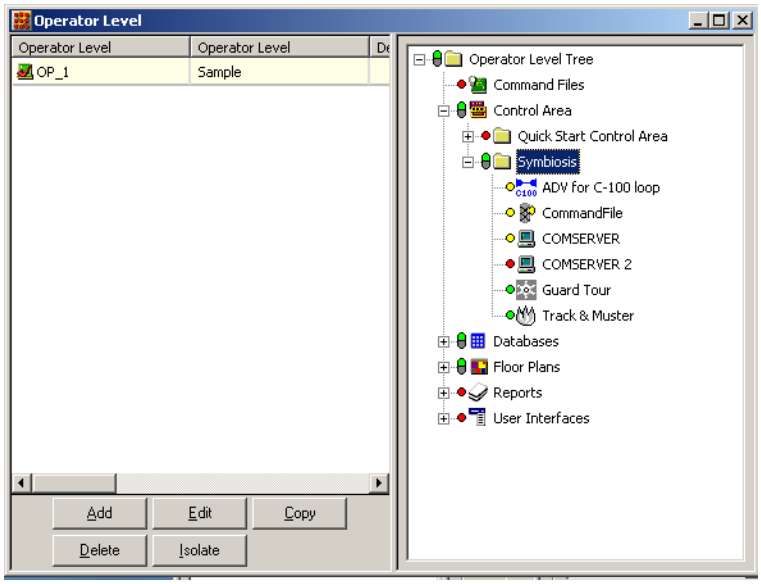
1. In the **Operator Level** window, select the **Reports** branch.

2. Right-click **Reports**, and then click **Configure**. The **Configure Rights** window appears.



3. Select the appropriate option, and then click **OK**. The selected right 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**

See the "Configuring rights summary chart" for details on the rights that can be configured.

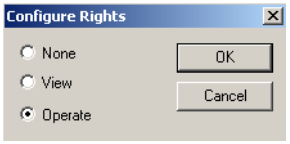
Configuring rights for User Interface Elements

Note: This sections is applicable only for WIN-PAK CS.

To configure rights for User Interface Elements:

1. In the **Operator Level** window, expand the **User Interfaces** branch and select a UI element.

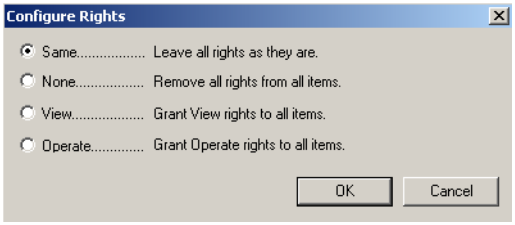
2. Right-click the element and select **Configure**. The **Configure Rights** window appears.



3. Click **None** to provide no access, **View** to provide rights for viewing only and **Operate** to provide access to configure the selected UI element.
4. Click **OK**.

To assign the same rights to all the UI elements in a branch:

1. In the **Operator Level** window, select a **User Interfaces** branch.
2. Right-click the branch, and then click **Configure**. The **Configure Rights** window appears.



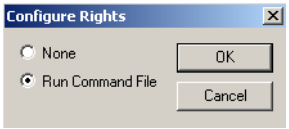
3. Select the appropriate option, and then click **OK**. The selected right is assigned to all the UI elements.

Configuring rights for Command Files

Note: This section is applicable only for WIN-PAK CS.

To configure right for Command Files:

1. In the **Operator Level** window, expand the **Command Files** branch and select a command file.
2. Right-click the command file and select **Configure**. The **Configure Rights** window appears.

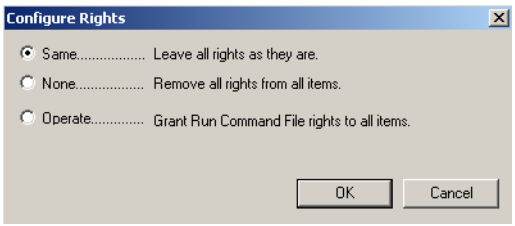


3. Click **None** to provide no access and **Run Command File** to provide access to running the file.
4. Click **OK**.

To assign the same rights to all the command files:

1. In the **Operator Level** window, select the **Command Files** branch.

2. Right-click **Command Files**, and then click **Configure**. The **Configure Rights** window appears.



3. Select the appropriate option, and then click **OK**. The selected right is assigned to all the command files.

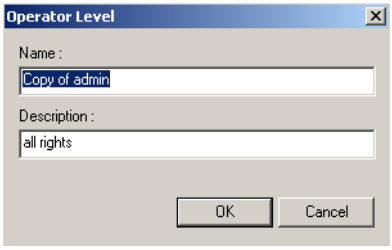
Note: Follow the same steps to configure the Operator access to Floor Plans.

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.

To copy an operator level:

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

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.

Editing an Operator Level

To edit the name or description of an operator level:

1. From the **System** menu, choose **Operator** Level. The **Operator Level** window appears.
2. Select the operator level, and then click **Edit**. The **Operator Level** window appears.
3. Enter the new **Name** and/or **Description**, and then click **OK**.

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

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

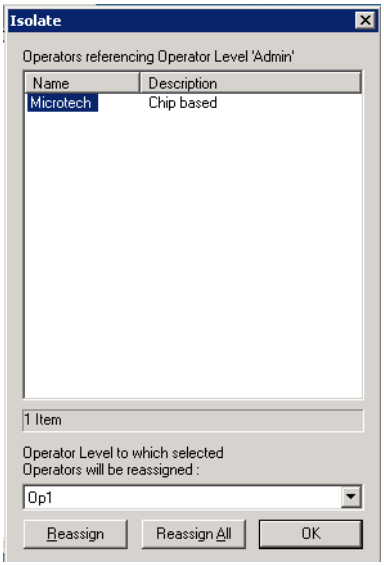
Isolating and Deleting an Operator Level

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. From the **System** menu, choose **Operator** Level. The **Operator Level** window appears.
2. Select the operator level to be isolated, and then 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 confirmatory message appears.

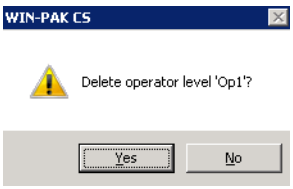
   OR

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

Deleting an operator level

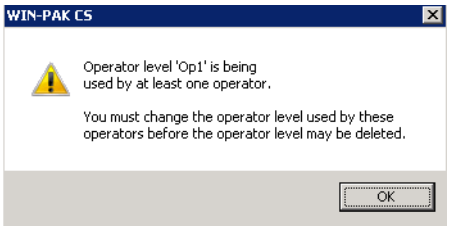
To delete an operator level:

1. Select an operator level from the database list, and then click **Delete**. A confirmatory message 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

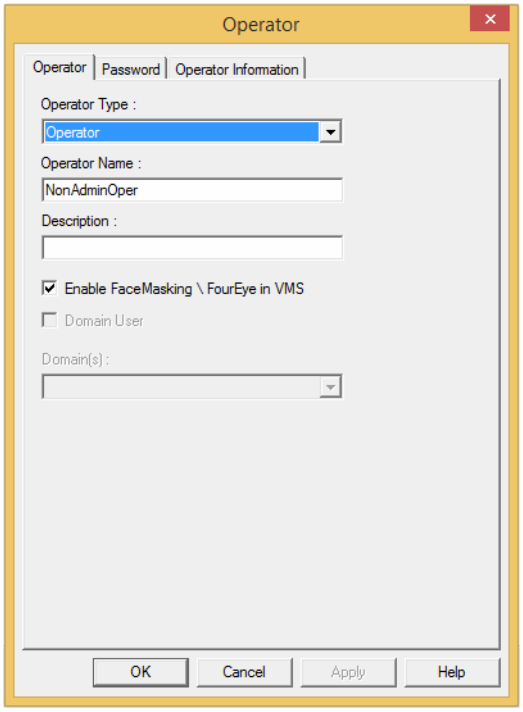
The operators can gain access to various functions of WIN-PAK CS/SE/PE based on the associated operator level and the rights assigned to that level.

Note: WIN-PAK CS installation screens are shown in this section as an example. The screens would change based on the variant selected.

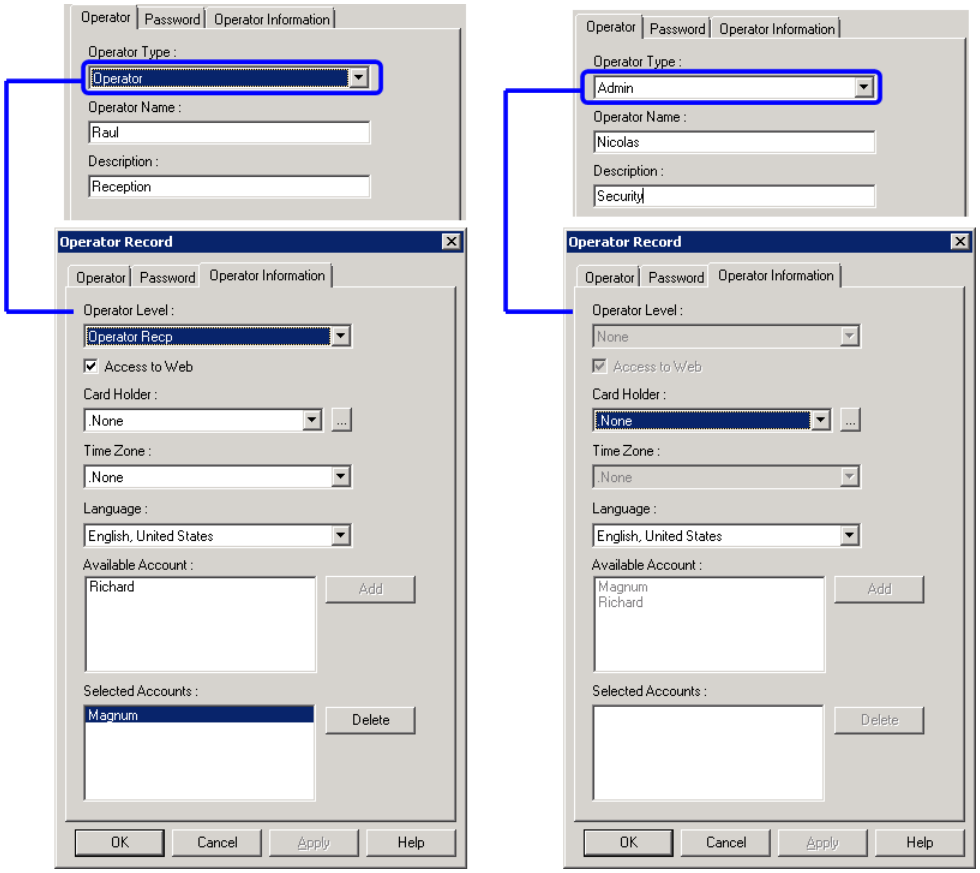
Adding an Operator

To add an operator:

1. From the **System** menu, choose **Operator**. The **Operator** window appears.
2. Click **Add** to display the **Operator** dialog box.



3. In the **Operator** tab, select the **Operator Type** as **Admin** or **Operator**.
4. Type the **Operator Name** and **Description**.
5. Select the **Enable FaceMasking \ FourEye in VMS** check box to mask the face in live/recorded video when the operator logs in. If the check box is not selected, the face will not be masked in the live/recorded video.
6. 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 a maximum of 20 characters.
    b. Retype the password in **Confirm New Password**.
7. Click the **Operator Information** tab. The field inside this tab varies according to the operator type.



Operator **Administrator**

8. 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 CS/SE/PE and so the Operator Level, Time Zone, and Accounts options are not applicable for the Administrator.The Administrator also has default Access to Web.

9. Select the **Access to Web** check box to grant access to the WIN-PAK CS Web Interface application.

Note: The **Access to Web** check box is available only in WIN-PAK CS.

10. 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.

11. 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 CS any time.

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

13. Select the accounts the operator must access under **Available Account** and click **Add**.

    The **Selected Accounts** displays the list of accounts which are selected. You can click **Delete** to delete any selected account.

14. 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:

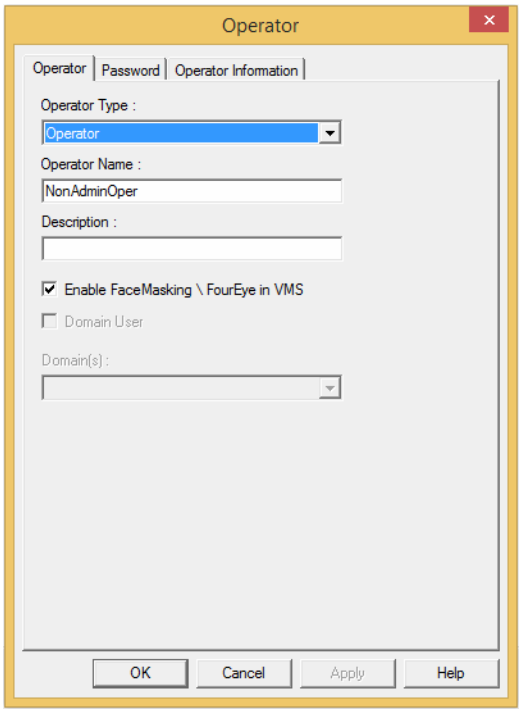
- Pick a simple phrase preceded or followed by one or more numbers.
- Use a password without spaces and capitalize each character. Such passwords cannot be easily decoded either by a random number generator or by a dictionary decoder.
- For tight security, use a combination of both letters and numbers. 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. From the **System** menu, choose **Operator**. The **Operator** window appears.
2. Select the operator to be edited, and then click **Edit**. The **Operator** dialog box appears.



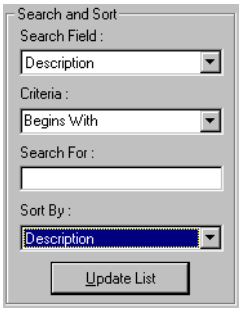
3. Edit the required details of an operator, and then click **OK**.

   See 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. From the **System** menu, choose **Operator**. The **Operator** window appears.
2. Select an item in the **Search Field** list.



- **All** - Lists all the operators and customers.
- **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 Type in the Search Field, select the **Criteria**.
   - **Begins With** - Searches for an item that begins with the text in the **Search For** box.
   - **Equals** - Searches for an item that exactly matches with the text in the **Search For** box.
   - **Greater Than** - Searches for an item that is alphabetically or numerically greater than the text in the **Search For** box.
   - **Less Than** - Searches for an item that is alphabetically or numerically less than the text in the **Search For** box.
4. Type the text to be searched in the **Search For** 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. From the **System** menu, choose **Operator**. The **Operator** window appears.
2. Select the operator to be deleted, and then click **Delete**. The selected operator is deleted.

Customers

Customers are individuals with a set of defined rights and privileges to work with the WIN-PAK CS Web Interface. You can configure the customers' rights to view and modify various Web Interface components such as databases and reports in the customer level.

A customer can log on to the WIN-PAK CS Web Interface using the user name and password that you have set.

See the "Defining Customers" section in this chapter, to set the password and user name for a customer.

Note: The user type Customer is available only in WIN-PAK CS.

Customer Levels

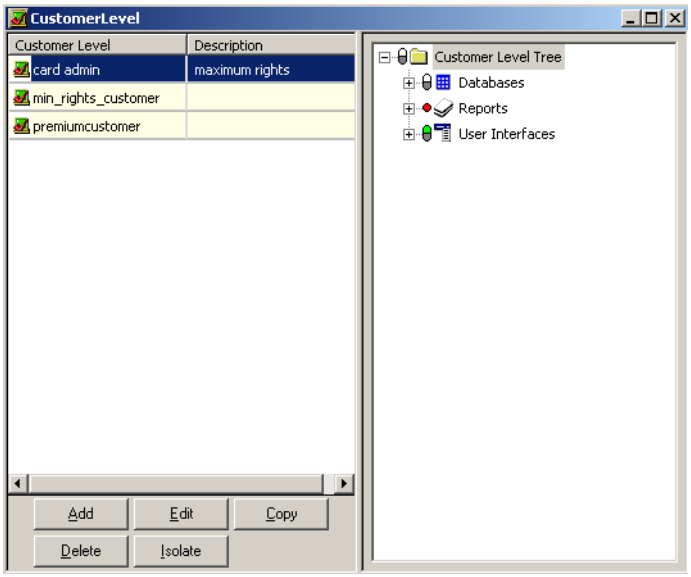
The customer level defines the privileges of the customer to work with the WIN-PAK CS Web Interface. Customers can view and configure the system components defined in the customer level assigned to them.

In a customer level, the rights are configured for the following system components:

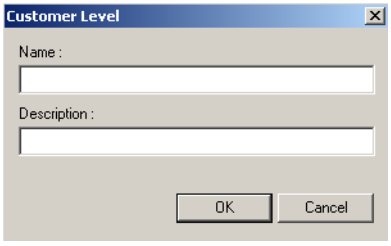
- **Databases** - To configure Card Holder, Cards, Floor Plan, and so on.
- **Reports** - To run reports.
- **User Interfaces** - To control the elements displayed in the WIN-PAK CS Web Interface application.

Adding a Customer Level

1. From the **System** menu, choose **Customer Level**. The **Customer Level** window appears.



2. Click **Add** to add a new customer level. The **Customer Level** dialog box appears.



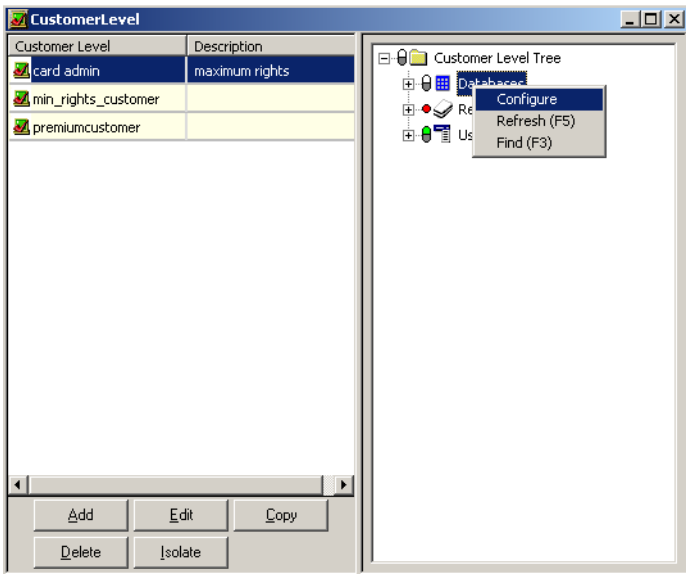
3. Type the **Name** for the customer level. This field is mandatory.
4. Type the **Description** for the customer level.
5. Click **OK** to save and return to the **Customer Level** window.

Configuring a Customer Level

To create and configure a customer level:

1. From the **System** menu, choose **Customer Level**. The **Customer Level** window appears.

Note: The Customer Level window is divided into two panes, the left-pane and the right-pane. The left-pane displays the list of customer levels and the right-pane displays the customer level tree which consists of a few databases, reports, and user interface elements.You can set the access rights for the selected customer level by assigning rights to branches or individual items on the tree.



2. In the left-pane, select a customer level in the **Customer Level** list.
3. Right-click the database, or report, or user interface element.
4. Configure rights for an entire branch, an individual database, an individual report or user interface element.

Configuring rights for an entire branch

To configure access rights for an entire branch:

1. In the **Customer 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 appears.

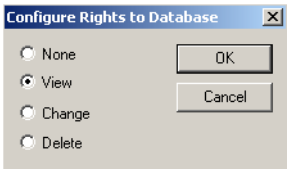
2. Select the appropriate rights configuration for the Customer Level, and then click **OK**.

Configuring rights for databases

To configure rights for databases:

1. In the **Customer 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.

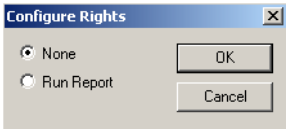


3. Select the appropriate option to set the rights for the database.

Configuring rights for reports

To configure rights to an individual report:

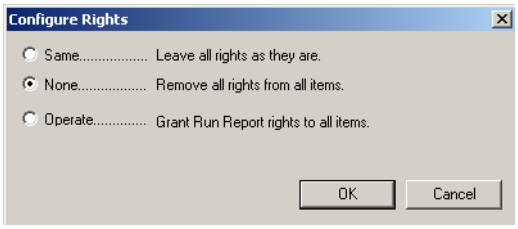
1. In the **Customer Level** window, expand the **Reports** branch and select a report.
2. Right-click the report and select **Configure**. The **Configure Rights** dialog box appears.



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:

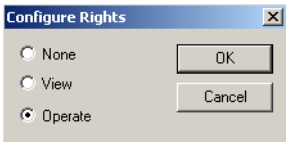
1. In the **Customer Level** window, select the **Reports** branch.
2. Right-click **Reports**, and then click **Configure**. The **Configure Rights** dialog box appears.



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

Configuring rights for User Interface Elements

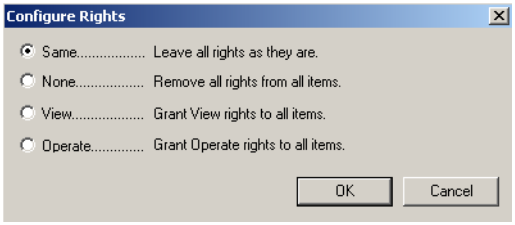
1. In the **Customer Level** window, expand the **User Interfaces** branch and select a UI element.
2. Right-click the element and select **Configure**. The **Configure Rights** dialog box appears.



3. Click **None** to provide no access, **View** to provide rights for viewing only and **Operate** to provide access to configure the selected UI element.
4. Click **OK**.

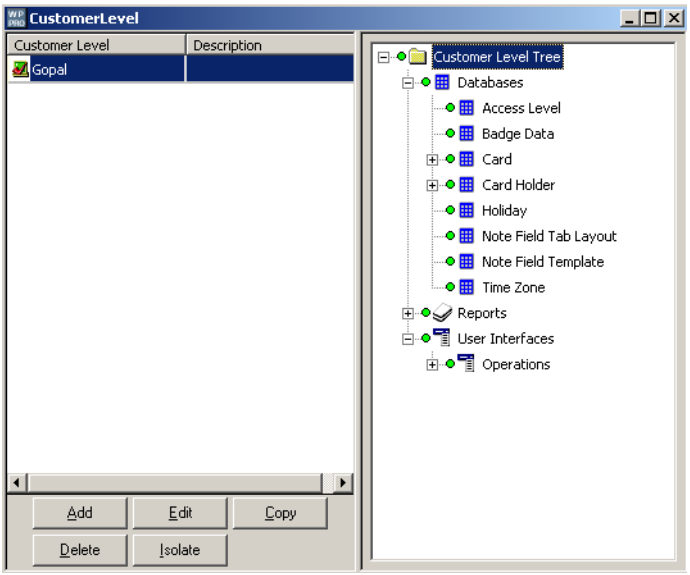
To assign the same rights to all the UI elements in a branch:

1. In the **Customer Level** window, select a branch in **User Interfaces**.
2. Right-click the branch, and then click **Configure**. The **Configure Rights** dialog box appears.



3. Select the appropriate option, and then click **OK**. The selected right is assigned to all the UI elements.

Note: Each 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.

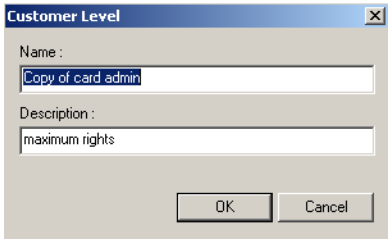
Configuring rights summary chart

Branch, Database	Change Operate	Delete	Max	None	Operator Specific	Same	View
Customer Level Tree	X		X	X		X	X
Database	X	X		X		X	X
Individual Database	X	X		X			X
Reports				X	X	X	
Individual Report				X	X		
User Interface				X	X	X	X
Individual User Interface				X	X		X
Options	**Description**						
Change and Operate	Grant change rights to all databases. Grant operate rights to all reports and user interfaces.						
Delete	Grant delete rights to all databases as a whole. Grant change rights to all fields.						
Maximum	Grant delete rights to all databases. Grant operate rights to all fields.						
None	Remove all rights from all items.						
Operate Specific	Grant operate rights to all items in a branch or specific items.						
Same	Leave all rights as they are.						
View	Grant view rights to all items.						

Copying a Customer Level

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

1. From the **System** menu, choose **Customer Level**. The **Customer Level** window appears.
2. Select the customer level to be duplicated.
3. Click **Copy**. The **Customer Level** dialog box appears.



4. Type a new **Name** for the customer 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 customer level, if required.
6. Click **OK** to save a copy and return to the **Customer 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 a Customer Level

To edit the name or description of a customer level:

1. From the **System** menu, choose **Customer Level**. The **Customer Level** window appears.
2. Select the customer level, and then click **Edit**. The **Customer Level** dialog box appears.
3. Enter the new **Name** and/or **Description**, and then click **OK**.

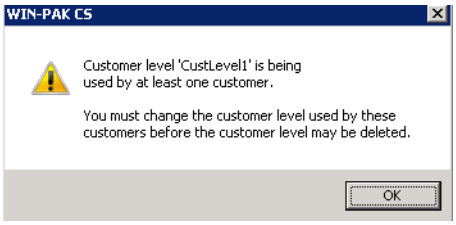
Note: To edit the access rights of a customer level, you can select the customer level and configure new access rights.

See the "Configuring a Customer Level" section in this chapter for details on configuring access rights to an operator level.

Isolating and Deleting a Customer Level

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

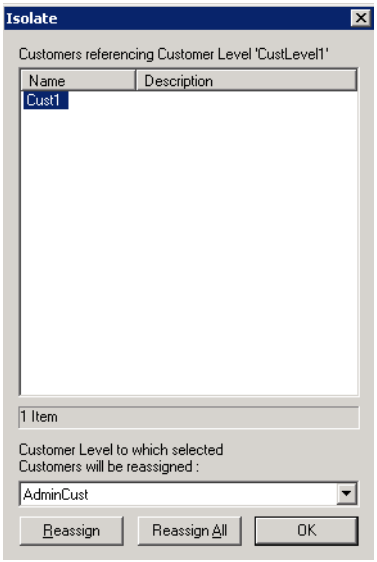
Note: When you attempt to delete a customer level assigned to a customer, the following prompt appears:



Isolating a customer level

To reassign customers to a different customer level and to isolate the customer level:

1. From the **System** menu, choose **Customer Level**. The **Customer Level** window appears.
2. Select the customer level to be isolated, and then click **Isolate**. The **Isolate** dialog box appears.



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

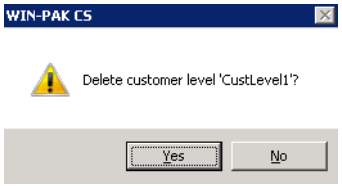
   OR

   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 customer levels are reassigned to another customer level.
7. Click **OK** to return to the **Customer Level** window.

Deleting a customer level

To delete a customer level:

1. Select a customer level from the database list, and then click **Delete**. A message asking for confirmation appears.



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

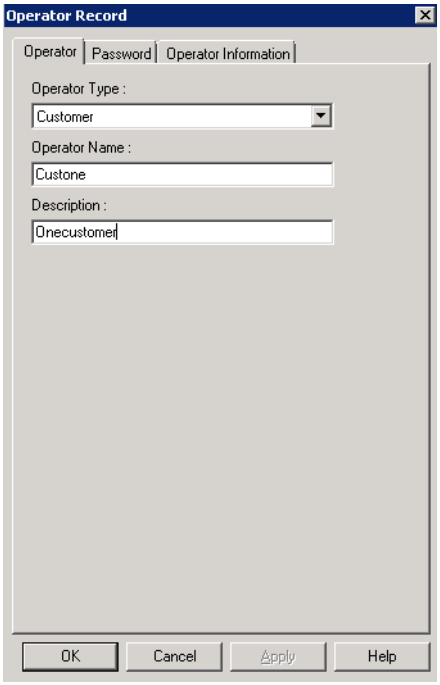
Defining Customers

Customers can gain access to various components of WIN-PAK CS Web Interface, based on the associated customer level and the rights assigned to that level.

Adding a Customer

To add a customer:

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



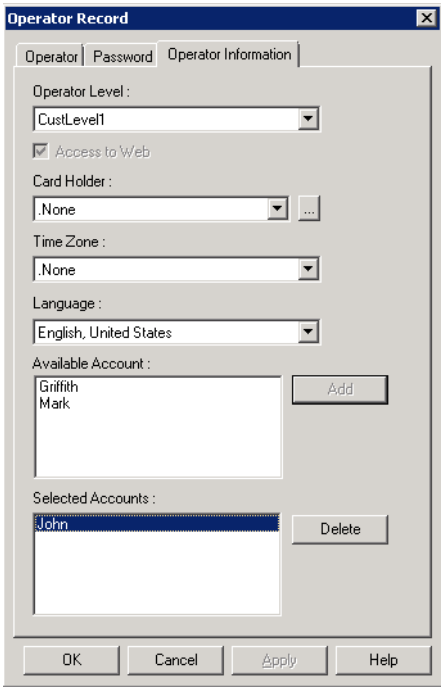
3. In the **Operator** tab, select the **Operator Type** as Customer.
4. Type the **Operator Name** and **Description**.
5. Click the **Password** tab to set the password.

a. Type the **New Password** for the customer 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**.

See the "Tips on Password" section for more information on setting passwords to ensure security in WIN-PAK CS.

6. Click the **Operator Information** tab. The field inside this tab varies according to the operator type.



7. When the operator is of type Customer, **Operator Level** lists the customer levels for WIN-PAK CS. Select the customer level in the **Operator Level** list to assign access rights to the customer.

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

9. Select the **Time Zone** during which the customer has to log on to the WIN-PAK CS Web Interface.

Note: If no time zone is assigned, the customer can log on to the WIN-PAK CS Web Interface any time.

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

11. Select the accounts the customer must access under **Available Account** and click **Add**.

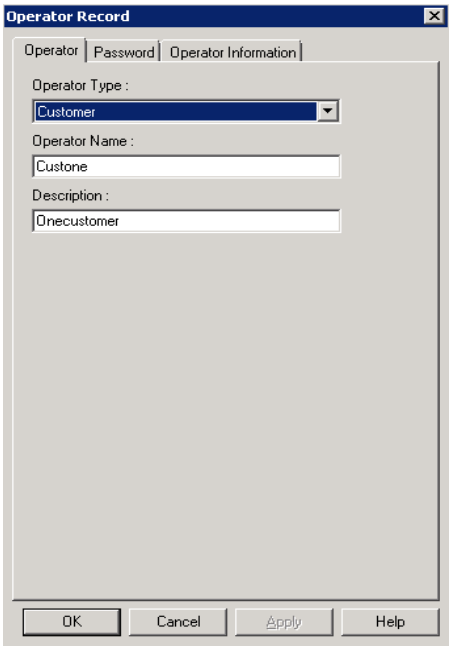
The **Selected Accounts** displays the list of accounts which are selected. You can click **Delete** to delete any selected account.

12. Click **OK** to save the changes and add the customer.

Editing a Customer

To edit the customer details:

1. From the **System** menu, choose **Customer**. The **Customer** window appears.
2. Select the customer to be edited, and then click **Edit**. The **Operator Record** dialog box appears.



3. Edit the required details of the customer, and then click **OK**.

   See the "Adding a Customer" section in this chapter, for details on adding a customer.

Searching and Sorting Customers

The search and sort operation for customers is similar to the search and sort for operators.

See "Searching and Sorting Operators" for details on how to search and sort customer information.

Deleting a Customer

To delete a customer:

1. From the **System** menu, choose **Operator**. The **Operator** window appears.
2. Select the customer to be deleted, and then click **Delete**. The selected customer is deleted.

Default Settings

Default settings can be set for certain system functions in WIN-PAK CS/SE/PE. 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 CS/SE/PE menus for configuring workstation and system settings are:

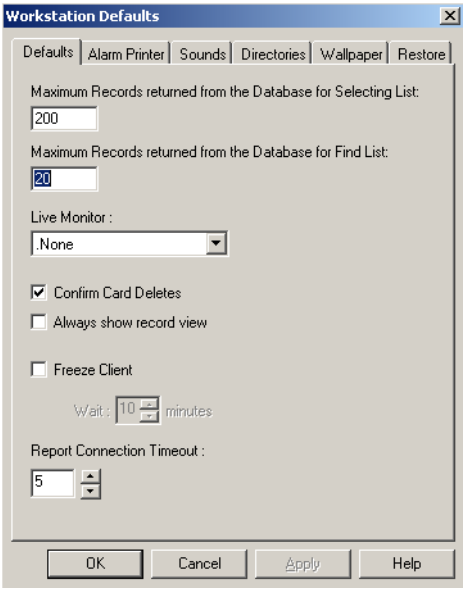
- Workstation Defaults
- System Defaults

Setting Workstation Default

Default settings can be set for alarm printer, sound files, paths, wallpapers and restore options for a workstation with WIN-PAK CS/SE/PE installed.

To set the workstation defaults:

1. From the **System** menu, choose **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:

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 the 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 the 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.
Confirm Card Deletes	A message asking for confirmation appears, when you attempt to delete a card. By default, this check box is 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 is cleared.
Freeze Client and Wait	If the operator leaves the WIN-PAK CS 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 is cleared. The period for inactivity is set in the **Wait** box. The period range from 1 to 60 minutes. Default value is 10 minutes.

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

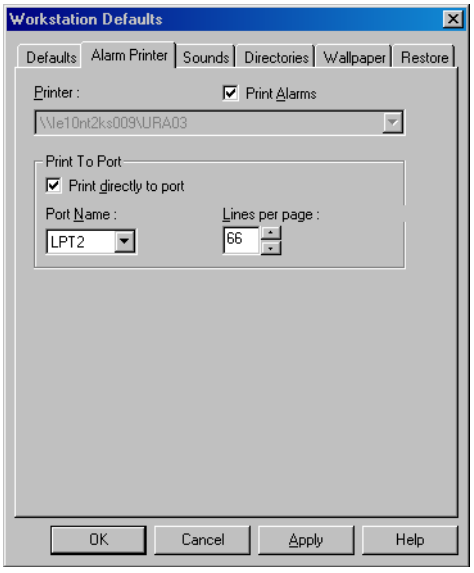
Setting defaults for alarm printers

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 the alarms as soon as they are displayed in the alarm view window using Dot-Matrix printer.

Note: If printer is not configured with Dot-Matrix printer, then the printing will wait till the page buffer is full before printing.

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 on Windows.

    OR

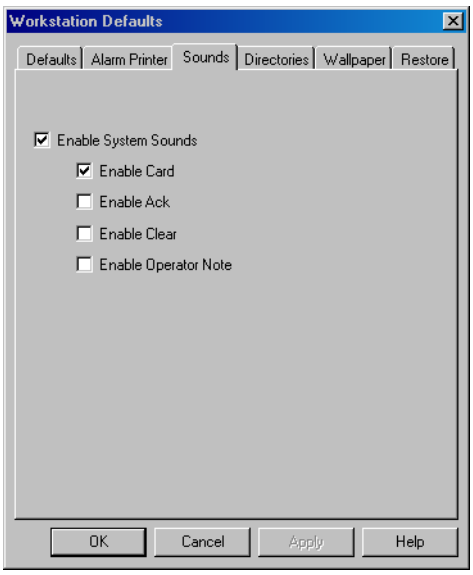
    To select a printer in the network:

    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 default 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:

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

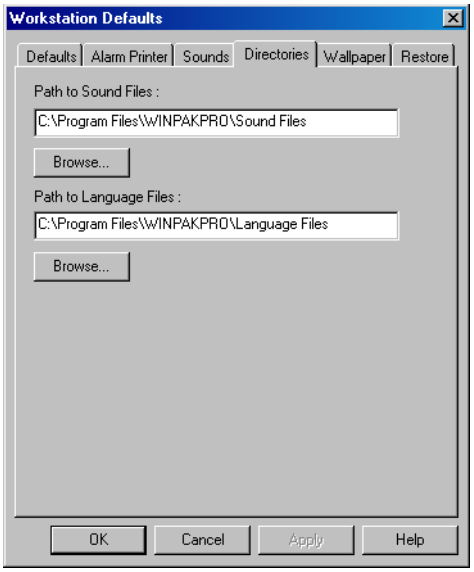
4. Click **Apply** to save the sound file settings.

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.

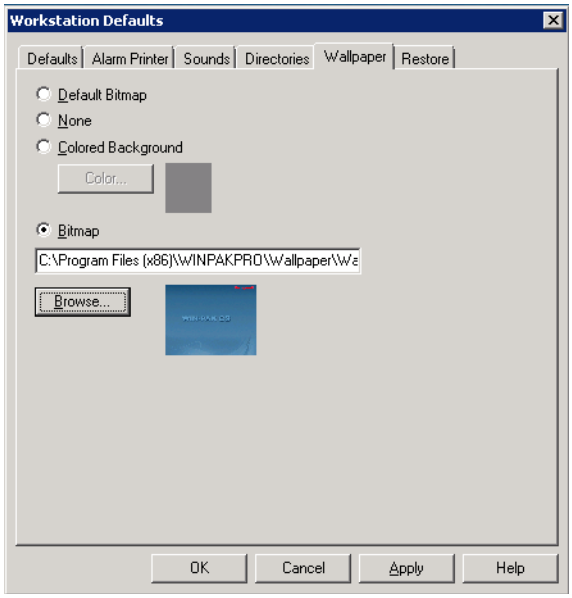


2. In **Path to Sound Files** text box, type the path for the sound files or click **Browse** to locate the sound files folder. By default the path is set to C:\Program Files\WINPAKPRO\Sound Files.
3. In **Path to Language Files** text box, type the path for the language files or click **Browse** to 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 CS/SE/PE User Interface

To set the default wallpaper for WIN-PAK CS/SE/PE:

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



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

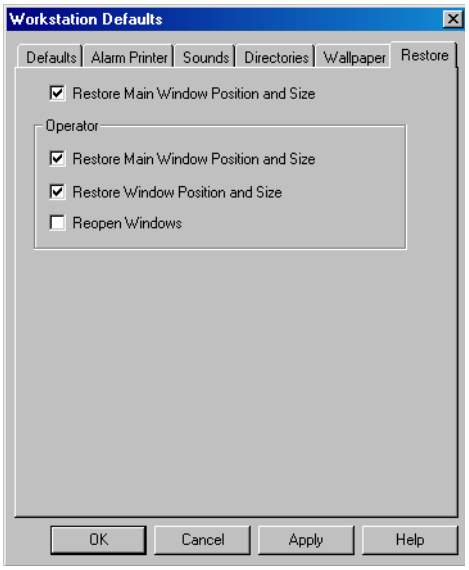
Wallpaper Option	Description
Default Bitmap	Retains the default bitmap set for the User Interface.
None	No wallpaper is set for the User Interface.
Colored Background	Sets a wallpaper color for the User Interface. Click **Color** and choose the background color.
Bitmap	Set a bitmap as a background for 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 CS/SE/PE 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 CS/SE/PE system:
   - Select the **Restore Main Window Position and Size** check box to retain the earlier size and position of the main window.
3. To set the restore options after logging on to the WIN-PAK CS/SE/PE system:

a. Under **Operator**, select the following restore options:

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.

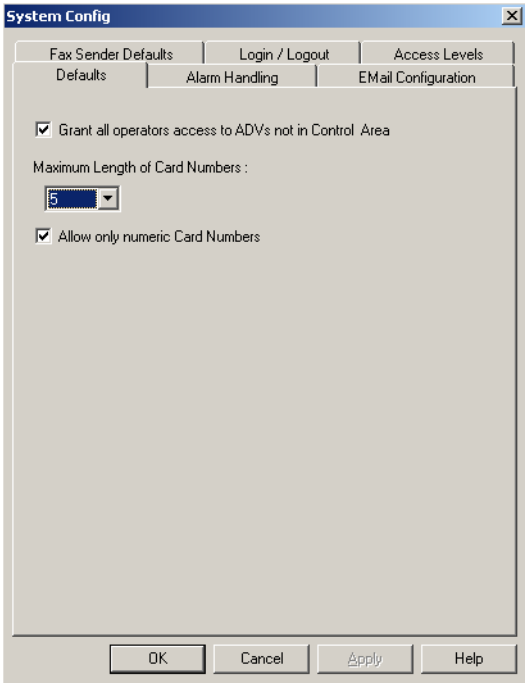
4. Click **Apply** to save the restore settings.
5. Click **OK** to save the workstation settings and close the dialog box.

Default System Setting

Default settings can be set for certain functions in WIN-PAK CS/SE/PE. 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 default system setting:

1. From the **System** menu, choose **System Defaults**. The **System Config** dialog box appears.



2. Click each tab and configure the settings.

3. Click **OK** to save the settings.

Configuring default settings

To configure the default settings:

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

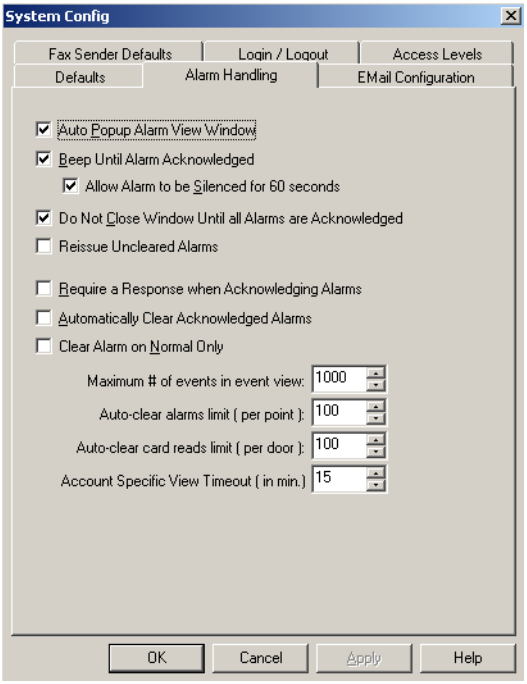
Defaults Option	Description
Defaults option applicable for WIN-PAK CS/SE/PE	
Grant all operators access to ADV not in Control Area	Select the check box to grant permission to all the operators for accessing ADVs that are not in the Control Area
Maximum Length of Card Numbers	The maximum length for card numbers.
Allow only numeric Card Numbers	Card numbers can only be numbers.
Defaults option applicable only for WIN-PAK SE/PE	
Edit Card numbers after addition	By default the check box to edit the card number is selected. Clear the check box to disable the option to edit the card number. **Note:** When you select this option, the **Card Number** under **Card** > **Card** is disabled.
Port Settings for WIN-PAK SE/PE	
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 panel in the TCP/IP encrypted connection.

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

Default setting for alarm handling

To set the default for alarm handling:

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



2. Set the following alarm settings:

Alarm Options	Description
Auto Popup Alarm View Window (Applicable for Administrators only)	When a new alarm is received, the Alarm View window is opened, restored or continues its display. By default this check box appears selected. **Note:** In WIN-PAK SE/PE this feature works on Alarm popups configured in the Operator Level tree. See Alarm Popups for more information.
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.

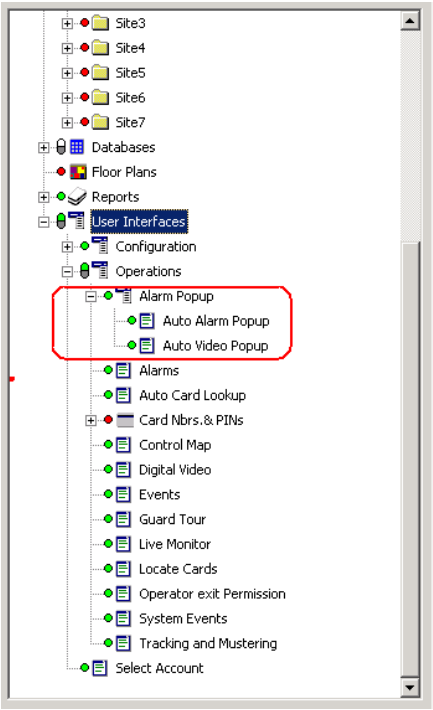
Alarm Options	Description
Require a Response when Acknowledging Alarms	A note must be provided when alarms are acknowledged.
Automatically Clear Acknowledged Alarms	Acknowledged alarms are automatically cleared.
Clear Alarm on Normal Only	The operator can clear an alarm, only if the device or point on which the alarm is generated returns 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 setting limit.
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.
Account Specific View Timeout (applicable only in WIN-PAK CS)	The threshold after which the **Account Specific Alarm View** closes.

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

Alarm Popups

Note: This section is applicable only for WIN-PAK SE/PE.

This option restricts the display of alarm popups and video popups based on the rights configured for an operator in the Operator Level tree. You can define the alarm popup and video popup permissions for the operator.(Operator Level Tree > User Interfaces >Operations).



The Alarm Popup option in the operator level tree includes the following sub items: Auto Alarm Popup, Auto Video Popup. The Configure option for the Auto Alarm/Auto Video Popup has the None/View/Operate options. The Operate option is selected by default for an admin operator. You can choose to configure the permissions for a non-admin operator.

For an admin operator, the selection of Auto Popup Alarm View Window(Applicable for Administrators only) check box in the Alarms Handling tab is considered for enabling/disabling the display of the alarm popup and video popup.

Note: For an non-admin operator:

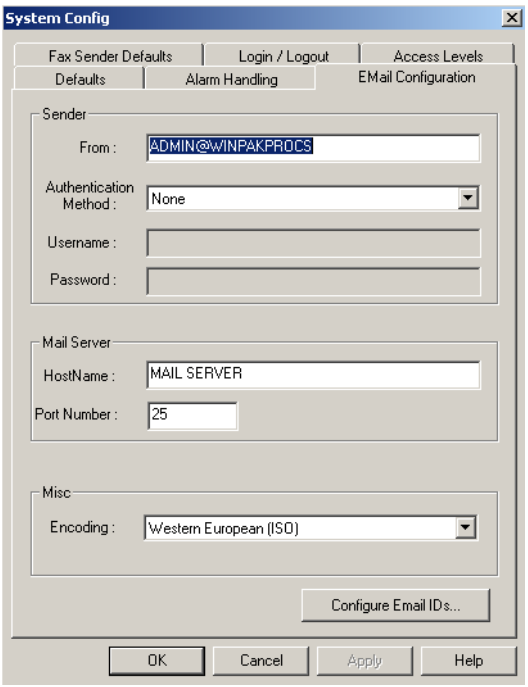
- If you have configured **None** permission for **Alarms** and **View/Operate** permission for **Auto Alarm Popup**, then the operator level does not have any effect and alarm popups do not appear.
- If you have configured **None** permission for **Alarms** and **View/Operate** permission for **Auto Video Popup**, then there is a change in operator level and video popups appear.

Specifying default e-mail IDs for reporting alarms

You can configure the e-mail IDs to which the e-mails for alarms are to be sent.

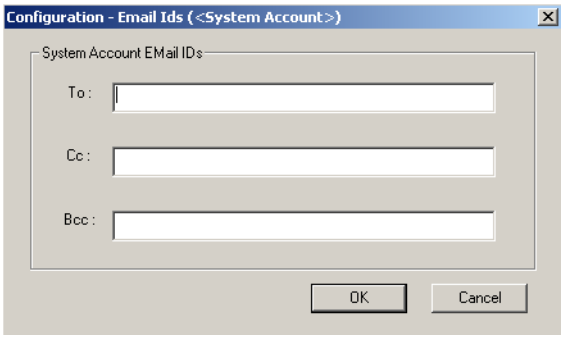
To specify default e-mail IDs for reporting alarms:

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 **To**, **Cc**, and **Bcc** text boxes.

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

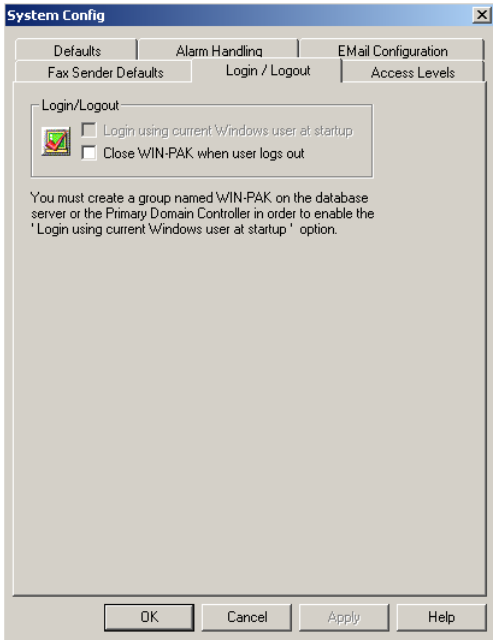
9. Click **OK** to save the e-mail details and return to the **System Config** dialog box.
10. Click **Apply** to save the e-mail configuration details.

Configuring automatic log on and log off settings

You can set the WIN-PAK CS/SE/PE system to log on automatically, when you launch WIN-PAK CS/SE/PE. In addition, you can set to close the WIN-PAK CS/SE/PE 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 CS/SE/PE system to log on automatically using Windows logon user name.

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

- Alternatively, in WIN-PAK SE/PE, you can also log on using **Domin Credentials** check box.

Note: When you log on using domain credentials, operator types are not created by default. You must manually create an Operator Type with Admin rights, associated to the new domain. See Adding an Operator and Deleting an Operator for more information.

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

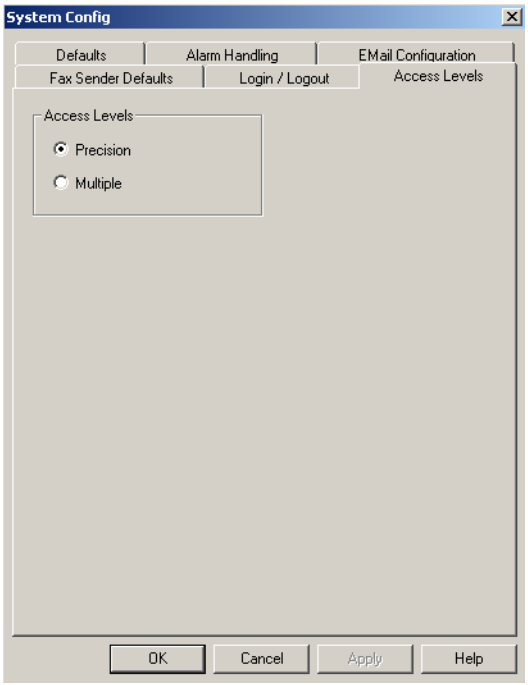
Configuring access levels for cards

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

Note: This configuration is a system level configuration.

To configure the access levels for cards:

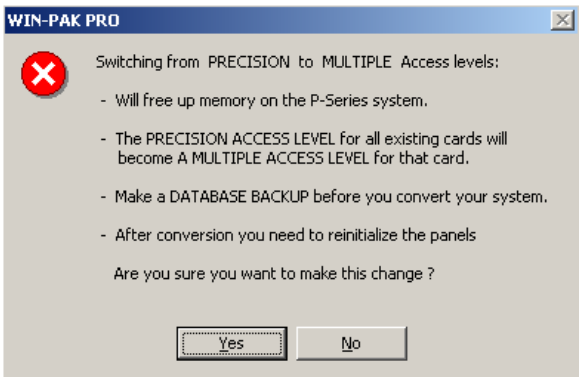
1. In the **System Config** dialog box, click the **Access Levels** tab.



2. Under **Access Levels**, click any of the following options:

- **Precision**: Only one access level is assigned to a card. When this access level is selected, more memory is consumed for a P-Series panel.
- **Multiple**: A maximum of 32 access levels can be assigned to a card.

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



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.

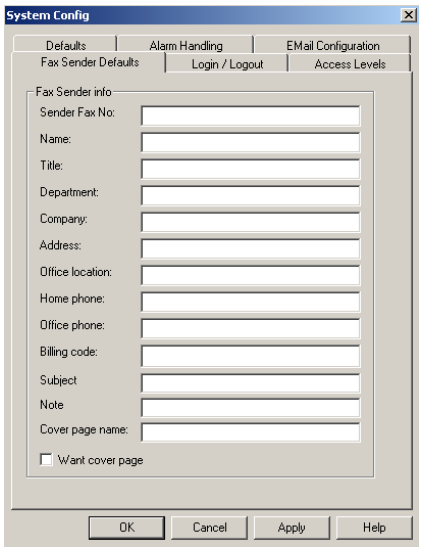
Specifying default fax sender information for reporting alarms

You can configure the sender information for faxing reports.

Note: This section is applicable only for WIN-PAK CS.

To specify the default fax sender information for reporting alarms:

1. In the **System Config** dialog box, click the **Fax Sender Defaults** tab.



2. Specify the following information for sending a fax:

Field	Description
Sender Fax No.	Type the fax number of the sender.
Name	Type the sender's name.
Title	Type the designation of the sender.
Department	Type the sender's department name.
Company	Type the name of the company.
Address	Type the sender's address.
Office Location	Type the official location.
Home Phone	Type the residential contact number.
Office Phone	Type the official contact number.
Billing Code	Enter the Billing Code for the fax report.
Subject	Type the subject of the fax.
Note	Type important information that must be noted by the recipient.
Cover page name	Type the cover page name of the fax report.

3. Select the **Want Cover Page** check box to include a cover page in the fax report.

Note: See the "Faxing the report" section in the Reports chapter for details on configuring the sender details for faxing reports.

4. Click **OK** to save the changes and close the **System Config** dialog box.

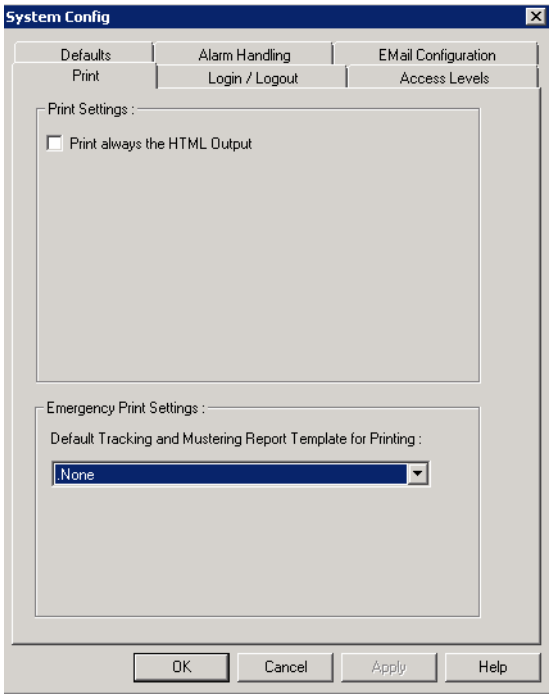
Configuring print settings

Note: This section is applicable only for WIN-PAK SE/PE.

WIN-PAK SE/PE is compatible with many printers. You can configure and set the print settings for all the reports. You can also set the emergency print settings for the selected report templates.

To configure the print settings:

1. In the **System Config** dialog box, click the **Print** tab and select any one of the following options as necessary.



   a. Under **Print Settings**, select **Print always the HTML Output** to print all the reports in HTML format.

   b. Under **Emergency Print Settings**, the **Default Tracking and Mustering Report Template for Printing** is set to **None**. From the drop-down list, select the predefined tracking and mustering template for emergency print. To set the tracking and mustering report template, See Defining Tracking and Mustering Templates, page 838.

   c. Click **Apply**.

2. Click **OK**.

Database Maintenance

Database maintenance provides tools for removing the unused data from the databases. When records are deleted from a database, they are not removed from the hard disk. They are unavailable but still occupy the space in the hard disk.

It is necessary to remove old history from the database file, from time to time. The time interval for removing the files and the amount of history to be retained is based on the requirements of your system.

To remove deleted database records and/or history:

1. From the **File** menu, choose **Database Maintenance**. The **Database Maintenance** dialog box appears.

2. Select **Remove Deleted Records** under **Settings** to delete records from the hard drive.
3. Select **Delete History** under **Settings** to delete history files.
4. Click **Change** to open the **Select Until Date** dialog box.

Note: The deleted records and/or the history till the selected date is removed.

5. Click **Start**. A confirmatory message appears to remind you to backup the database before deleting the files.

Note: After the history has been deleted, it cannot be restored except by restoring the entire database from a backup copy. Therefore, it is recommended that a backup copy of the database be made before deleting the history.

6. Click **Yes** to proceed with the deletion. A progress bar displays the status of the deletion process, including the name of each database as it is being processed.
7. Click **No** to go back and make a backup of the database.

Performance optimization monthly basis

Please follow the below steps for the database maintenance.

1. Take complete database backup of WIN-PAK.
2. Shut down Neverfail Heartbeat on the Primary Active server / Secondary Passive server and do the following steps in Primary Active server.
3. Remove the LAN connectivity of Primary active and Stop the WIN-PAK services from service manager.
4. Follow the steps in sequence as described in the below table.

Note: SQL Server knowledge is a must to perform these steps / procedures.

Sequence #	Database Optimization methodology	Steps to do the Optimization	Intended System to do the step	Responsibility for the maintenance step	Frequency of this step
1	Remove the Deleted Card Records in WINPAK database	Copy the script in the Remove deleted cards.sql file to SQL Query Analyzer and execute the scripts.	WIN-PAK Database server machine	WIN-PAK Administrator	1st day of every month
2	Delete History records older than Six months	1. Go to WIN-PAK File Menu->Data base Maintenance 2. Check the "**Delete history**" option. 3. Mention the date which is six month before the date of operation. 4. Then press Start button. This will remove all the History records from the WIN-PAK database.	WIN-PAK Database server machine	WIN-PAK Administrator	1st day of every month
3	Re index the WINPAK tables	Ensure the WIN-PAK services are stopped. 1. Copy the content of “Stored procedure ind_rebuild.txt” to the store procedures in WINPAK Database.(This required to be done only once and is already present in Primary and secondary WIN-PAK server need to be reconfigured only if servers are rebuild.) 2. Run the Re indexing script by copying the script in “Rebuild indices.sql” to SQL query analyzer. 3. Check the data integrity after this operation.	WIN-PAK Database server machine	WIN-PAK Administrator	1st day of every month

Sequence #	Database Optimization methodology	Steps to do the Optimization	Intended System to do the step	Responsibility for the maintenance step	Frequency of this step
4	Update all statistics	1. Copy the script in the "2-Update_All_Statistics.sql" to the SQL query analyzer and execute.	WIN-PAK Database server machine	WIN-PAK Administrator	1st day of every month
5	Recompile all objects	1. Copy the script in the "3-Recompile_All_objects.sql " to the SQL query analyzer and execute.	WIN-PAK Database server machine	WIN-PAK Administrator	1st day of every month
6	Refresh All Views	1. Copy the script in the "4-Refresh_Views.sql" to the SQL query analyzer and execute.	WIN-PAK Database server machine	WIN-PAK Administrator	1st day of every month

5. Check the data integrity in the database.
6. Optimize the database. Please follow the below procedure through SQL server 2005 Management studio.
   From Start->All Programs->Microsoft SQL Server 2005->Management studio Then Login to the database engine then go to Management->Maintenance plan-> Right click and select Maintenance plan wizard. In this wizard check the "Rebuild Index Task" and select the radio button "Change the free space per page percent to" and give 10% as value. Mention a schedule for this on every Sunday morning 1.00.**This step needs to be scheduled weekly and configured once only, and need not to be repeated every month. This has already been configured in the Primary WIN-PAK server so may not be needed to configure until any rebuild of the server.**
7. Shrink the WIN-PAK PRO DB and leave 25% spare space.
   Please follow the below procedure through SQL server 2005 Management studio.
   From Start->All Programs->Microsoft SQL Server 2005->Management studio. The Login to the database engine and open "databases" then right click on "WIN- PAK PRO"->Tasks->Shrink->Database then in the wizard select the option "Reorganize files before releasing unused space" and mention maximum free space after shrinking as 25%. **This step needs to be scheduled weekly and configured once only, and need not to be repeated every month. This is already configured in the Primary WIN-PAK server. This has already been configured in the Primary WIN-PAK server so may not be needed to configure until any rebuild of the server.**
8. Start Neverfail Heartbeat on Primary and Secondary servers.
9. Allow server pair to re-synchronise (will take considerable time).

10. Synchronize the Active server and Passive server time.
11. Perform Controlled Switchover to verify neverfail functionality with Secondary Server in Active role.
12. Normalize neverfail operations to Primary Active / Secondary Passive state.

Scripts Used - Contents

1. Remove deleted cards.sql

```
Delete From Card where Deleted =1
```

2. Stored procedure ind_rebuild.txt

```
CREATE PROC ind_rebuild
AS
DECLARE @TableName sysname
DECLARE cur_reindex CURSOR FOR
SELECT table_name
    FROM information_schema.tables
    WHERE table_type = 'base table'
OPEN cur_reindex
FETCH NEXT FROM cur_reindex INTO @TableName
WHILE @@FETCH_STATUS = 0
BEGIN
    PRINT 'Reindexing ' + @TableName + ' table'
    DBCC DBREINDEX (@TableName, ' ', 80)
    FETCH NEXT FROM cur_reindex INTO @TableName
END
CLOSE cur_reindex
DEALLOCATE cur_reindex
GO
```

3. Rebuild indices.sql

```
-- Run each step separately!
-- 1 -- dbcc showcontig (cardholder) dbcc showcontig (Card)
-- 2 -- exec ind_rebuild
-- 3 -- dbcc showcontig
```

4. 2-Update_All_Statistics.sql

```
/*********************************************************************
RUN ON THE WIN-PAK Pro DATABASE
This script will update statistics for ALL indexes in
...Statistical information is used by the
query processor to determine the optimal strategy
```

```
for evaluating a query. When statistical information
is out of date performance may be degraded...
**********************************************************************/
USE [WIN-PAK PRO]
DECLARE @tablename varchar(128)
DECLARE @tablename_header varchar(128)
DECLARE tnames_cursor CURSOR FOR SELECT name FROM sysobjects
WHERE type = 'U'
OPEN tnames_cursor
FETCH NEXT FROM tnames_cursor INTO @tablename
WHILE (@@fetch_status <> -1)
BEGIN
    IF (@@fetch_status <> -2)
    BEGIN
        SELECT @tablename_header = 'Updating '
                +RTRIM(UPPER(@tablename))
        PRINT @tablename_header
        EXEC ('UPDATE STATISTICS ' + @tablename )
    END
      FETCH NEXT FROM tnames_cursor INTO @tablename
END
PRINT ' '
PRINT ' '
SELECT @tablename_header = '********** NO MORE TABLES **********'
PRINT @tablename_header
PRINT ' '
PRINT 'Statistics for All WIN-PAK PRO tables have been updated.'
DEALLOCATE tnames_cursor
```

5. 3-Recompile_All_objects.sql

```
/**********************************************************************
RUN ON THE WIN-PAK PRO DATABASE
This may take a while to run there is a built in delay to spread the
task out and ease the processor load.
The queries used by stored procedures and triggers
are optimized when they are compiled.
As indexes or other changes that affect statistics
are made to the database, compiled stored procedures and
triggers may lose efficiency. By recompiling stored procedures
and triggers that act on a table, you can reoptimize the queries.
```

```
**********************************************************************/
Use [WIN-PAK PRO]
DECLARE @tablename varchar(128)
DECLARE @tablename_header varchar(128)
DECLARE tnames_cursor CURSOR FOR SELECT name FROM sysobjects
WHERE type = 'U'
OPEN tnames_cursor
FETCH NEXT FROM tnames_cursor INTO @tablename
WHILE (@@fetch_status <> -1)
BEGIN
    IF (@@fetch_status <> -2)
    BEGIN
        SELECT @tablename_header = 'Updating '+
RTRIM(UPPER(@tablename))
        PRINT @tablename_header
        EXEC ('SP_RECOMPILE ' + @tablename )
    END
--waitfor delay '00:00:02'
    FETCH NEXT FROM tnames_cursor INTO @tablename
END
PRINT ' '
PRINT ' '
SELECT @tablename_header = '********** NO MORE STUFF TO MARK FOR
RECOMPILATION **********'
PRINT @tablename_header
PRINT ' '
PRINT 'ALL Objects in WinPak Pro have been marked for recompilation.'
DEALLOCATE tnames_cursor
```

6. 4-Refresh_Views.sql

```
/**********************************************************************
RUN ON THE WIN-PAK Pro DATABASE
This script will Refresh ALL Views in WIN-PAK Pro
**********************************************************************/
USE [WIN-PAK PRO]
DECLARE @viewname varchar(255)
DECLARE @viewname_header varchar(255)
DECLARE vnames_cursor CURSOR FOR SELECT name FROM sysobjects
WHERE type = 'v'
OPEN vnames_cursor
```

```
FETCH NEXT FROM vnames_cursor INTO @viewname
WHILE (@@fetch_status <> -1)
BEGIN
    IF (@@fetch_status <> -2)
    BEGIN
        SELECT @viewname_header = 'Refreshing '
+RTRIM(UPPER(@viewname))
        PRINT @viewname_header
        EXEC ('sp_refreshview ' + @viewname )
    END
    FETCH NEXT FROM vnames_cursor INTO @viewname
END
PRINT ' '
PRINT ' '
SELECT @viewname_header = '************** NO MORE VIEWS TO REFRESH
**************'
PRINT @viewname_header
PRINT ' '
PRINT 'All WIN-PAK PRo Views Have Been Refreshed.'
DEALLOCATE vnames_cursor
```

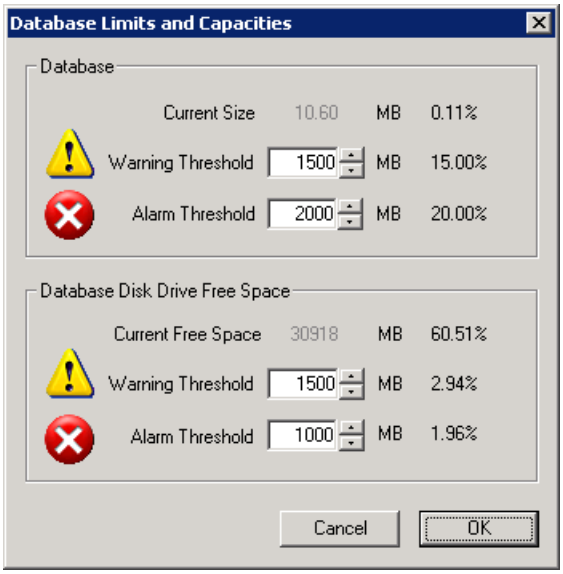
Database Limits and Capacities

This feature monitors the available space for the database (system programming and history, excluding floor plans, photo and badging images) and available hard drive space. Each monitoring feature has two programmable alarm thresholds. The first one is a warning to indicate that action should be scheduled and the second is an alarm to indicate that immediate action should be taken.

Only the WIN-PAK CS administrator has permissions to change the threshold values of these alarms.

To set the database limits and capacities:

1. From the **File** menu, choose **Database Limits and Capacities**. The **Database Limits and Capacities** dialog box appears.



2. To set the **Database** limits:
   - **Current Size**: provides database size information.
   - **Warning Threshold and Alarm Threshold**: Use and to increase or decrease the threshold limit. The corresponding percentages are also displayed.
3. To set the **Database Disk Drive Free Space** limits:
   - **Current Free Space**: provides the free space information of the hard drive in which the database is located.
   - **Warning Threshold and Alarm Threshold**: Use and to increase or decrease the threshold limit. The corresponding percentages are also displayed.

Tip: It is recommended that:

- If the database is located on a separate drive, at least 2.5 times the maximum size of the database should be left as free space.
- If the database is installed on the same drive as the OS, then not more than 1/3 free space of the hard drive be used. This allows enough room for taking backup and archive actions to occur.

Badge Layout

6

In this chapter...

This chapter describes about the badge layout templates of WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
Introduction: Configuring a Badge Layout, page 206	✓	✓
Introduction: Creating Badge Designs, page 211	✓	✓
Introduction: Configuring Badge DLLs, page 237	✓	✓
Introduction: Setting up Badge Printers, page 238	✓	✓

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.

When you define a badge layout for an account, the cards for employees belonging to the account are created based on the badge template.

Badge layouts are not visible across different accounts.

Note: Only an administrator can create a common badge layout at the <System> account.

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:

1. **Selecting an account** - Select the account for which you want to create a badge layout.
2. **Adding a new badge layout** - Create a badge layout with a name and description.
3. **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

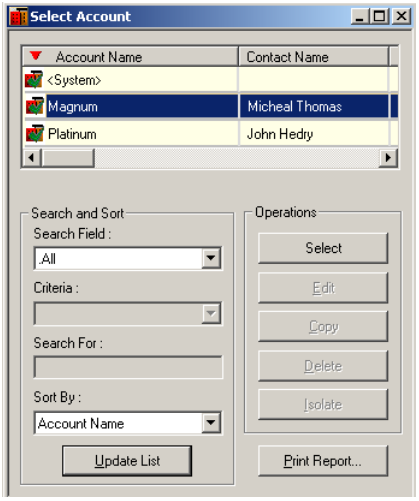
You can create badge layouts for a particular account or for all accounts.

Notes:

- Follow steps from 1 to 3 for selecting the account in WIN-PAK CS.
- Follow steps from 4 to 6 for selecting the account in WIN-PAK SE/PE.

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 <System>.

3. Click **Select**.

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

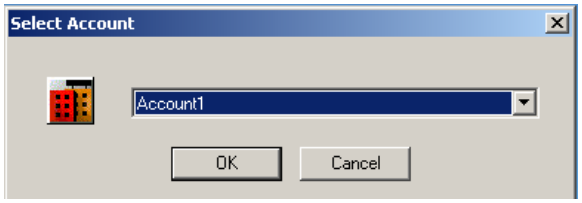


Figure 6-1 Select Account

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

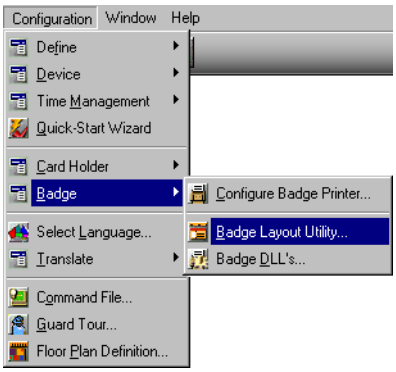
   OR

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

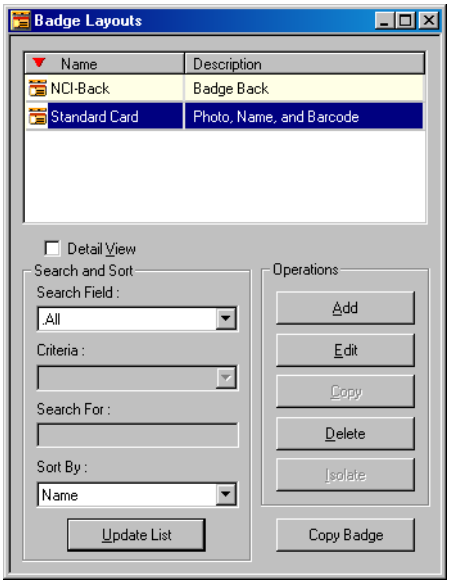
6. Click **OK** to save the account information for creating badge layouts and to exit from the **Select Account** dialog box.

Adding a New Badge Layout

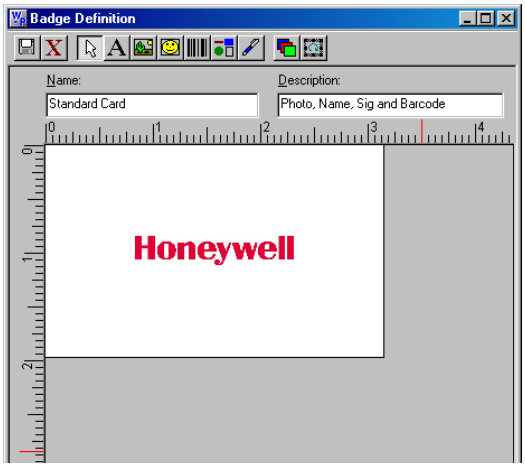
1. Choose **Configuration** > **Badge** > **Badge Layout Utility**.



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.

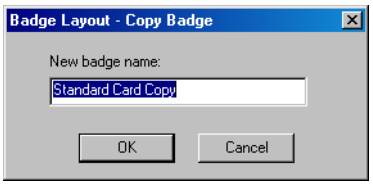
Copying a Badge Layout

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

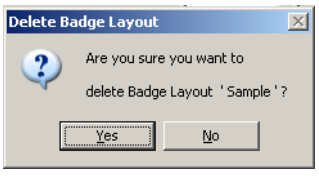
1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select the badge layout you want to edit and click **Edit**. The **Badge Definition** window appears.
3. Edit the **Name** and **Description** of the badge layout.
4. Click the icon.

Viewing a Badge Layout

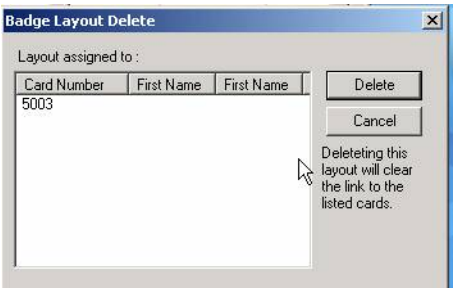
1. Choose **Configuration** > **Badge** > **Badge Layout Utility**. The **Badge Layouts** window appears.
2. Select the badge layout you want to view and select the **Detail View** check box. The **Badge Definition** window appears, with the details of the selected badge layout.

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 involve:

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

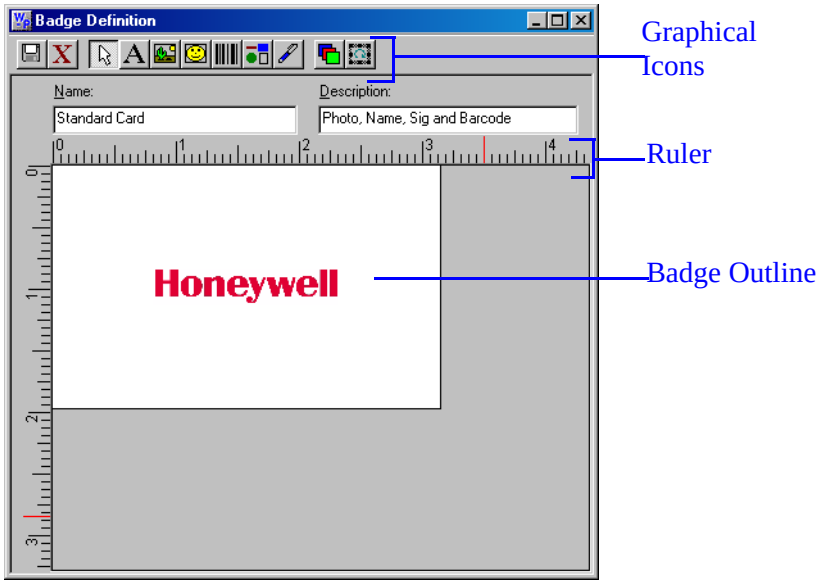
Note: You can design a badge while adding a new badge layout or while editing an existing layout.

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.

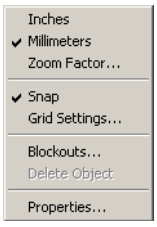


Changing the Ruler Measurement

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.

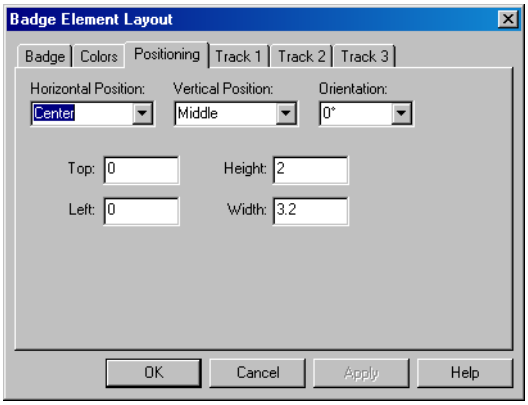


Setting the printable size of the badge

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.

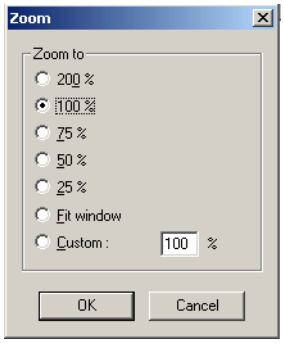
Note: To change the badge orientation from landscape (horizontal) to portrait (vertical) enter a dimension in the **Height** box that is greater than the dimension in the **Width** box.

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.



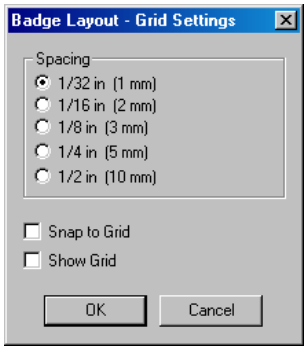
2. Select the required zoom factor, or click **Custom** and type the zoom percentage.
3. Click **OK**.

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

Specifying Grid Settings

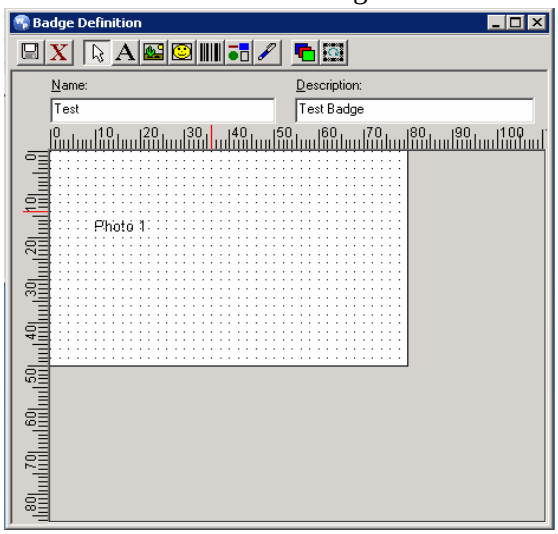
Grids are evenly spaced points on the badge layout area that assist in sizing and aligning items. You can use the as a visual aid for placing items on the badge layout. You can also enable the **Snap** setting for the, which pulls any item moving close to the mark.

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



2. Select one of the five spacing options in the **Spacing** list.
3. Select the **Snap to** check box, if you want items to snap to the when they are moved or added.
4. Select the **Show** check box, if you want the marks to be visible on the screen.

5. Click **OK** to save the settings and return to the **Badge Definition** window.



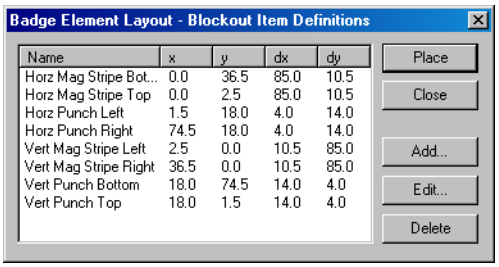
Setting Blockouts

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.

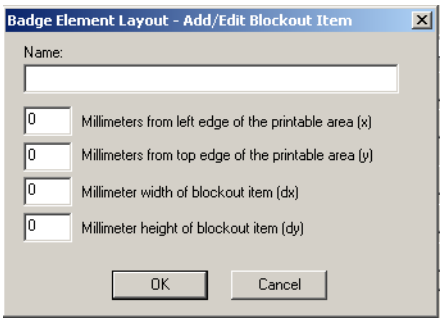
Though the blockout is generally effective in preventing overprinting of the Mag Stripe area, some card printers do print resin black over the blockout. To avoid this, ensure that no blockout is placed over the Mag Stripe area.

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**.

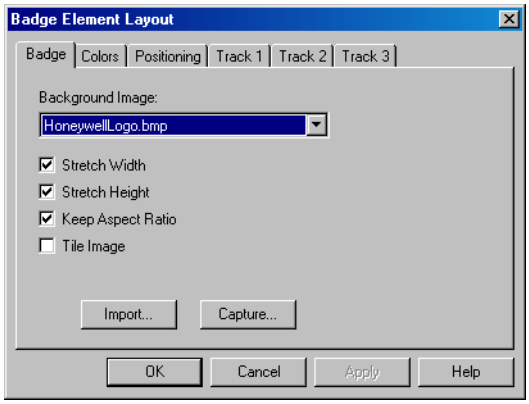
   OR

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.

Notes:

- 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.

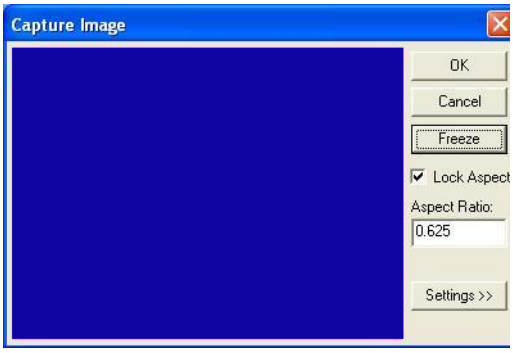
3. Click **Open**. The selected image file is listed in **Background Image**.
4. Click **Apply** to apply the image to the badge background or click **OK** to apply the image to the badge background and to close the **Badge Element Layout** dialog box.

To capture an image using a camera:

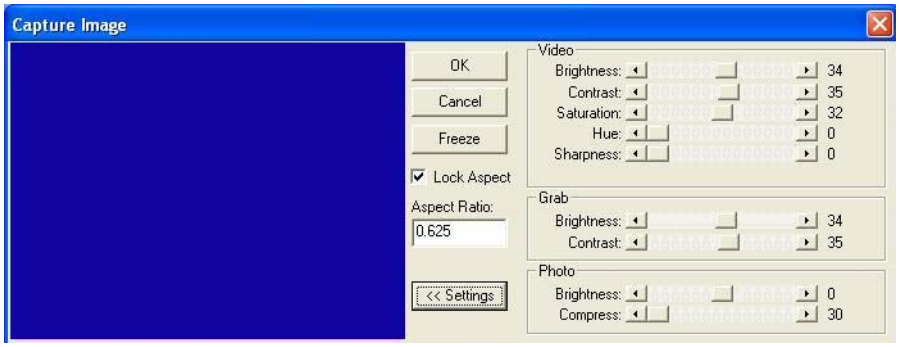
1. On the **Badge** tab of the **Badge Element Layout** dialog box, click **Capture**. The **Capture Image** dialog box opens displaying the live view from your video camera.

Notes:

- 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.

   Live Screen Video Image Settings:

Setting	Description
Brightness	Lightens or darkens the entire tonal range of the image.

Setting	Description
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.

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.

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.

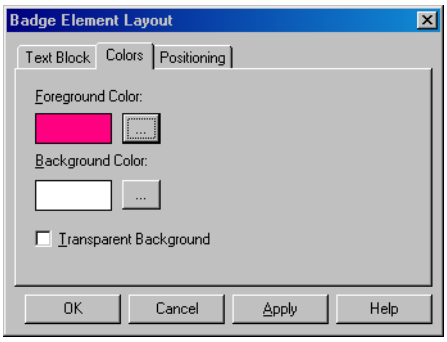
7. Click **OK** to save the image.

Setting a background color

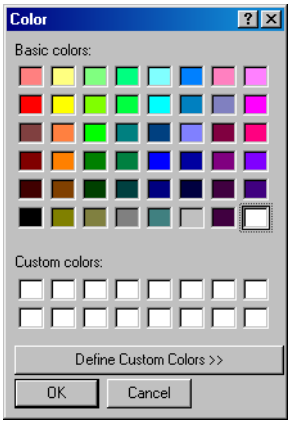
You can set a background color for a badge or for an item on the badge (for example, a bitmap, shape or signature.) The foreground color is not available unless an item is selected.

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.



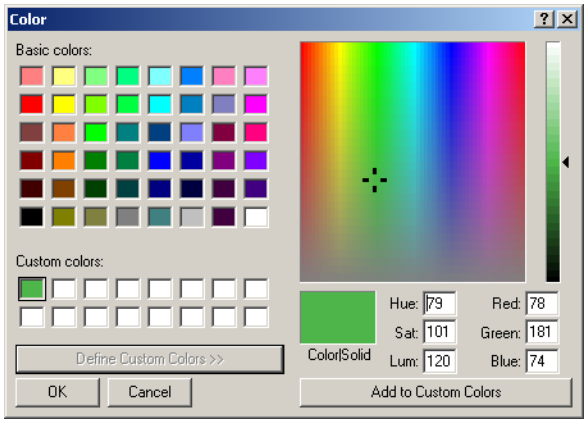
3. Click the ellipsis [...] provided near the **Background Color** box. The **Color** dialog box is displayed.



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.

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.
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).

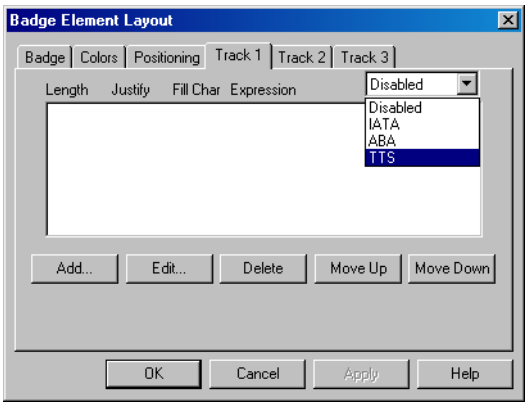
TTS supports only numeric characters 0-9 and various punctuation characters (ASCII 48-63).

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

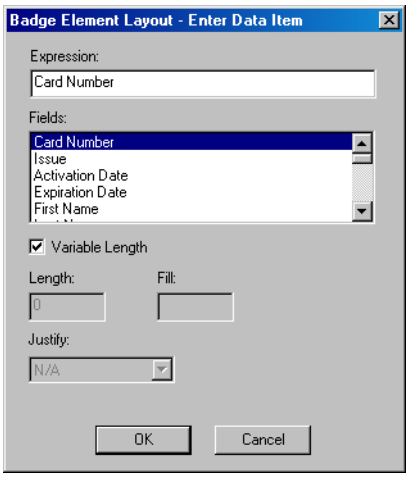
Track	Type of character	Maximum Characters	Bits per inch
1	Alphanumeric	76	210
2	Numeric	37	75
3	Numeric	104	210

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 1**, **Track 2**, or the **Track 3** 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.

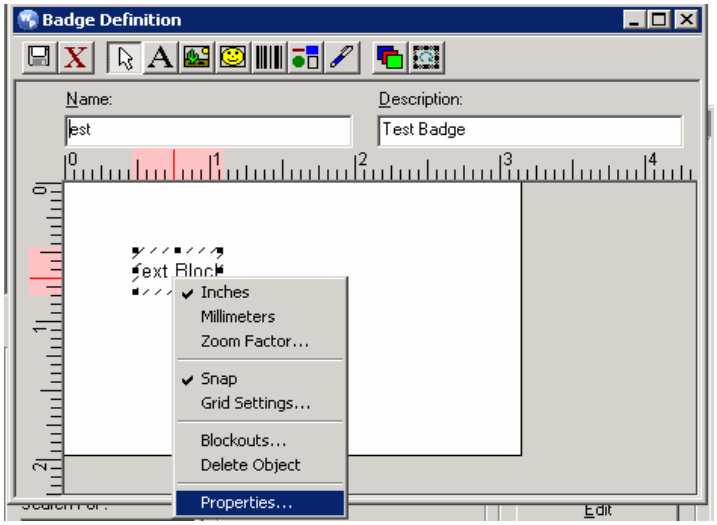
The following are the types of items that can be placed on a badge outline and their corresponding toolbar icons:

Button	Button Name	See..
	Text	"Placing a Text element"
	Photo	"Placing a Photo"
	Shape	"Place a Shape on the Badge outline"
	Signature	"Place a Signature on the Badge outline"
	Bitmap	"Place a Bitmap on a badge"
	Bar code	"Place a Bar Code on the Badge"

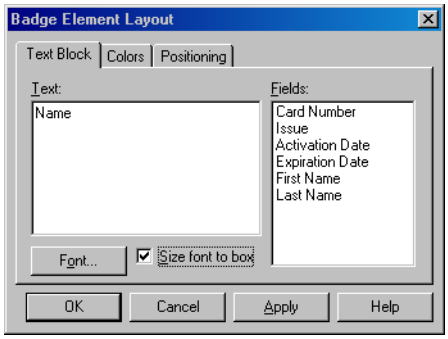
Placing a Text element

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 filled 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 from the **Fields** list. Or, you can type the text in the Text area. The field is now placed under **Text**.

Note: The Fields list displays the list of Note Fields.

  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:

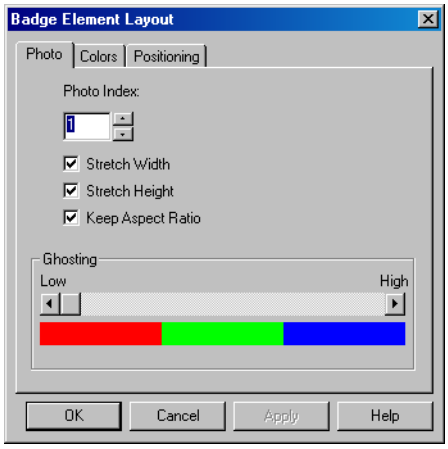
  a. Click  on the toolbar.

  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.

Place a Shape on the Badge outline

- To add a shape on the badge outline:

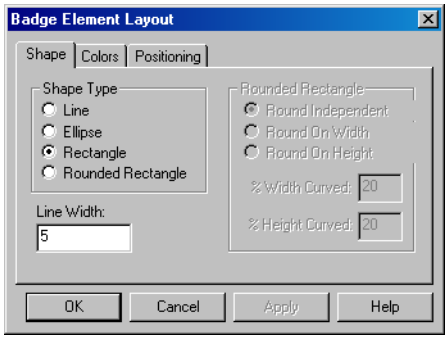
  a. Click  on the toolbar.

  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**.

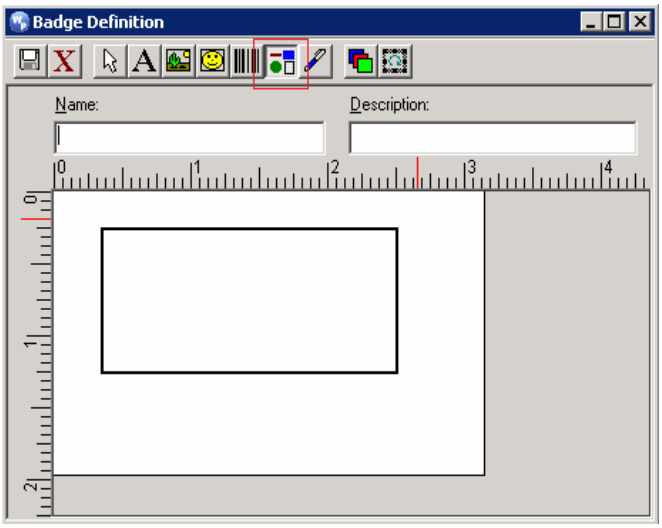
  b. Click the **Shape** tab.



  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.

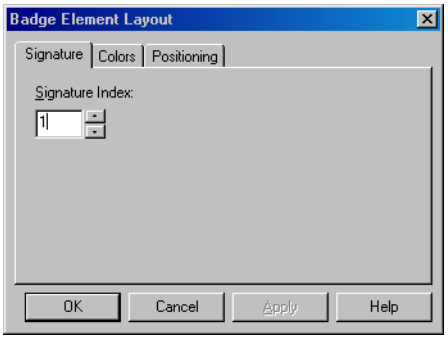


Place a Signature on the Badge outline

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.

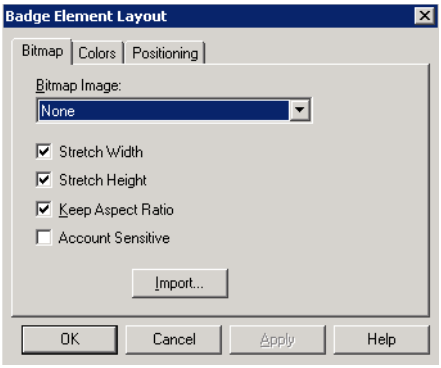
Place a Bitmap on a badge

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 the Account Sensitive Logo on a badge

Note: This section is applicable only for WIN-PAK CS.

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. You must first add a bitmap on the badge and then include the account sensitive logo. 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 include the account sensitive logo:

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

  b. Click the **Bitmap** tab.

  c. Select **Account Sensitive** check box to enable any changes in the system account to affect all the accounts.

  d. Click **Apply** to place the account sensitive logo in the badge outline.

Placing a Photo

Note: This section is applicable only for WIN-PAK CS.

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.

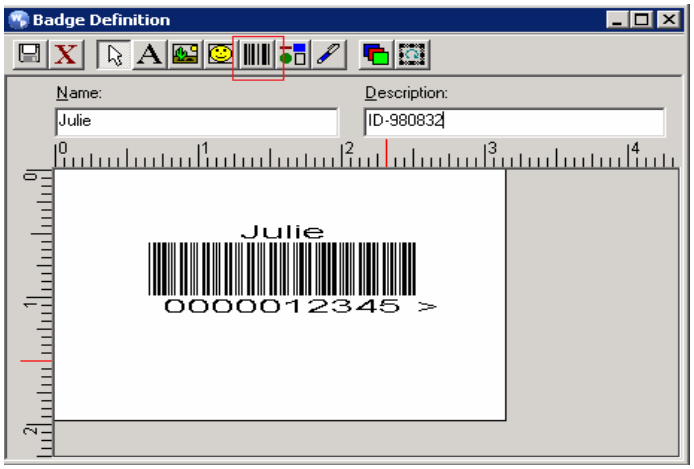
Note: A ghosted photo is harder to photocopy and provides added security against unauthorized reproduction of ID badges.

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

Place a Bar Code on the Badge

- To add a bar code on the badge outline:
    a. Click  on the toolbar.

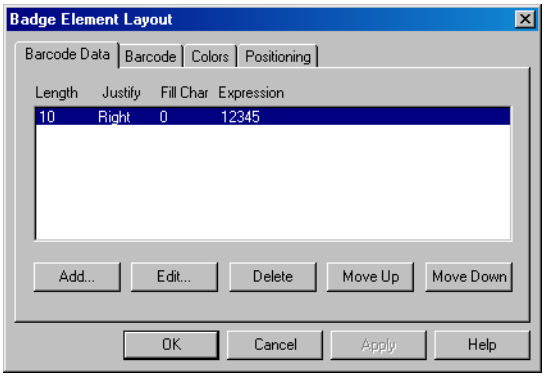
b. Click and drag the mouse pointer on the badge outline to place the bar code. The bar code is now placed on the badge outline.



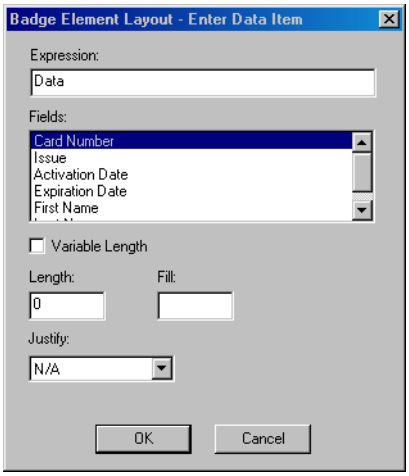
- To add bar code data items:

  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**.

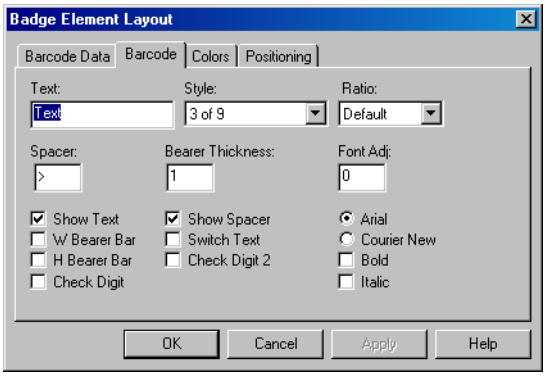
i. To remove a data item from the list, select it and click the **Delete** button.

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.

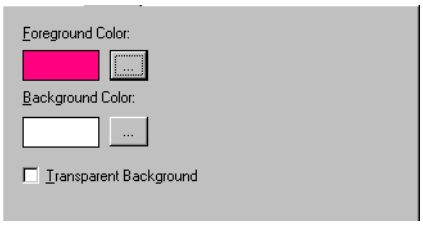
Style	Bar Code
2 of 5	MSI
2 of 5 interleaved	ITF
3 of 9	Code 11
Codabar	Code B
Code 39	Telepen
Code 93	UPC A
Code 128	UPC E
EAN 128	Code 128 A
EAN 13	Code 128 B
EAN 8	Code 128 C

- **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.

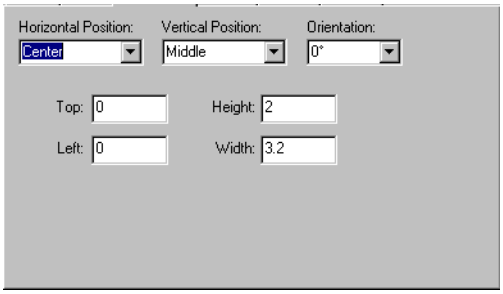
- **Show Text**: Displays the bar code data as text underneath the encoded information.
- **W Bearer Bar**: Displays the width bearer bars (top and bottom borders).
- **H Bearer**: Displays the height bearer bars (left and right borders).
- **Check Digit**: For error detection.
- **Show Spacer**: Displays 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.

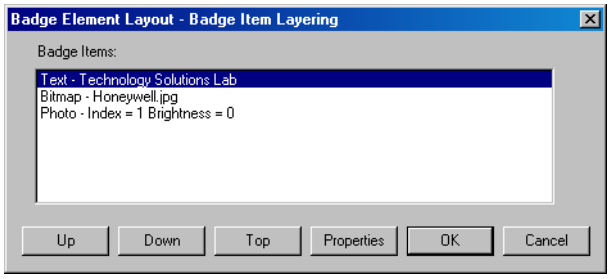
g. Click **Apply** to apply the badge outline.

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.

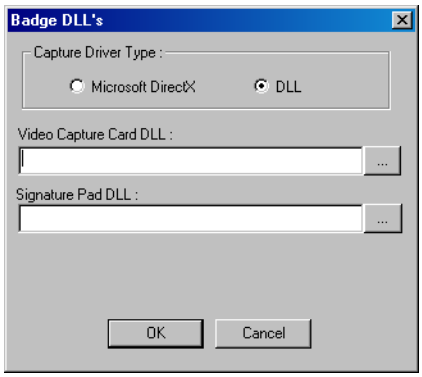
  f. Click **OK** to save the changes.

- 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 CS/SE/PE System. The DLLs for currently supported hardware are included in the WIN-PAK CS/SE/PE directory and are installed from within WIN-PAK CS/SE/PE.

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 CS/SE/PE 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 CS/SE/PE directory,

a. Open the **Windows Explorer**.

b. Choose **Tools > Folder Options**.The **Folder Options** dialog box appears.

c. Click the **View** tab.

d. Under Advanced settings, expand **Files and Folders** and then **Hidden files and folders.**

e. Click **Show hidden files and folders**.

f. Click **Apply** to apply the changes you have made and click **OK** to exit from the dialog box.

5. Click the ellipsis [...] button next to **Signature Pad DLL**. An **Open** dialog box appears with WIN-PAK CS opened as the default directory.
6. 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**.

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

Setting up Badge Printers

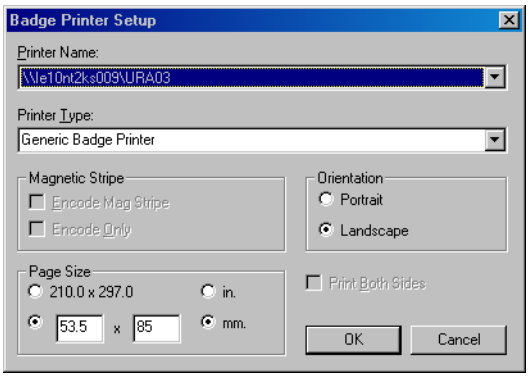
Overview

WIN-PAK CS/SE/PE 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

7

In this chapter...

This chapter describes about the Overview, Configuring Card Holders, Configuring Autocard Lookup, Configuring Card and Card Holder Information, Importing Card and Card Holder Information, and Visitor Management in WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
Configuring Card Holders: Selecting an Account, page 244	✓	✓
Configuring Card Holders: Configuring Note Field Template, page 244	✓	✓
Configuring Card Holders: Configuring Card Holder Tab Layout, page 248	✓	✓
Configuring Autocard Lookup: Configuring Access Levels, page 255	✓	✓
Configuring Card and Card Holder Information: Adding a Card and Card Holder Information, page 258	✓	✓
Configuring Card and Card Holder Information: Adding a Card Holder, page 266	✓	✓
Configuring Card and Card Holder Information: Assigning a Card to a Card Holder, page 284	✓	✓
Configuring Card and Card Holder Information: Configuring Autocard Lookup, page 285	✓	
Configuring Card and Card Holder Information: Adding Bulk Cards, page 285	✓	✓

Section	WIN-PAK CS	WIN-PAK SE/PE
Importing Card and Card Holder Information: Logging on to Import Utility, page 288		✓
Importing Card and Card Holder Information: Defining Order of Fields, page 288		✓
Importing Card and Card Information: Entering Card and Card Holder Information in an Excel Sheet, page 289		✓
Importing Card and Card Information: Assigning Default Values, page 289		✓
Importing Card and Card Information: Importing from Excel Sheet, page 290		✓
Visitor Management: Integrating LobbyWorks, page 293		✓

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 CS/SE/PE 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 in addition, cards can be assigned with a PIN number for enabling high security. WIN-PAK CS/SE/PE enables you to add a single card or a bulk of cards. Later, the cards are associated to the employees, visitors, and so on.

Additionally, in WIN-PAK SE/PE, you can define a card as a privilege 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 SE/PE.

Card Holders

A Card Holder is a person who holds a card. Card Holders in WIN-PAK CS/SE/PE 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.

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

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

- Time Zones
- Devices
- Access Areas
- Badge Design

Notes:

- When the **FIN4000 Biometric** is installed, the appearance of the User Interface (UI) element **Card Holder** in the **WIN-PAK SE/PE** application changes to **Credential Holder**. This is because, the Card Holder functionality additionally supports finger print for two fingers.

- In the **Credential Holder** dialog box, you can modify the support for two fingers under **Finger Print**. And also, each finger must be registered twice (for fingerprints).
- For WIN-PAK CS, See the "Time Management", "WIN-PAK CS/SE/PE Servers and Devices", "Defining Areas", and "Badge Layout" chapters for more details on the above-mentioned sections.
- For WIN-PAK SE/PE, See "Card Holders" chapters for more details on the above-mentioned sections.

Configuring Card Holders

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 define the following to 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 CS/SE/PE system.

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

See 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 to include card holder information.

Notes: In WIN-PAK CS this menu option is disabled in the <System> account.

- **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 **Select**. The selected account name is displayed in the title bar.

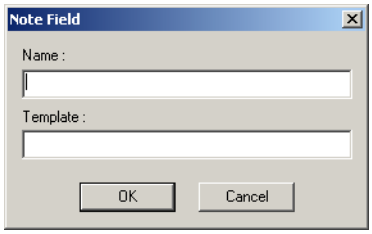
Configuring Note Field Template

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 CS/SE/PE enables you to define a maximum of 40 note fields.

Adding a Note Field Template

To add a note field template:

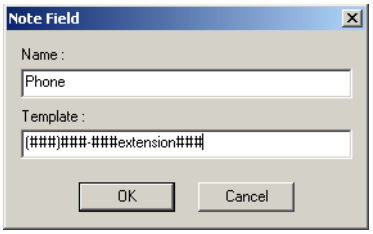
1. Choose **Configuration > Card Holder > Note Field Template**. The **Note Field Template** window appears.
2. Click **Add** to add a new note field template. The **Note Field** dialog box appears.



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:

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.	
~	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.

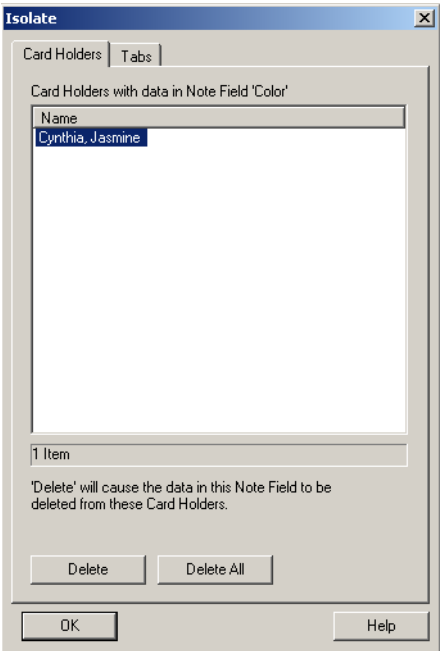
b. Select **None** in the **Sort By** list and then click **Update List**.

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.

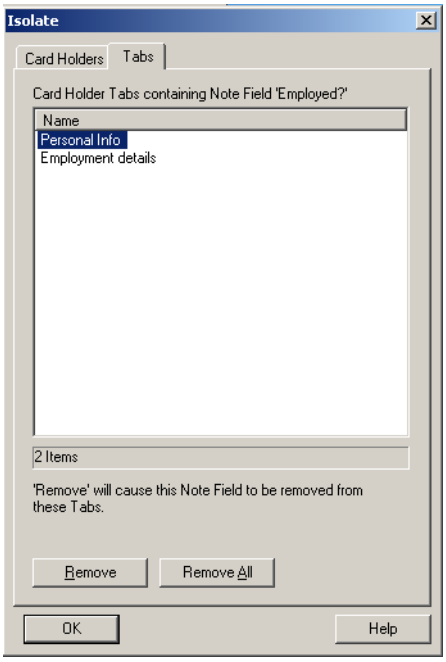
To isolate a Note Field:

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.



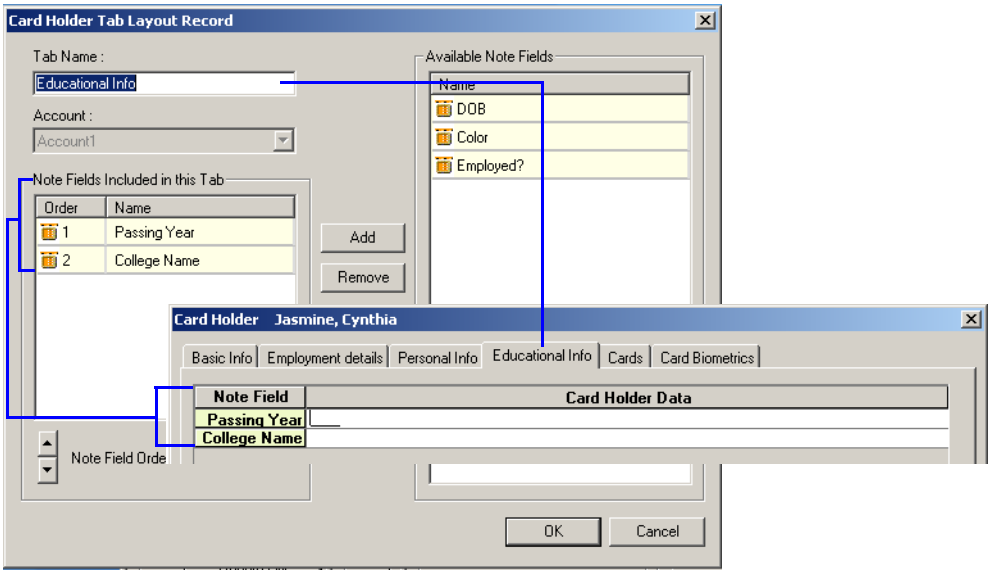
9. Select the tab in the **Name** list. You can also select multiple tabs by holding the SHIFT key or CTRL key while selecting.
10. Click **Remove** to isolate the selected tabs from the tab note fields or click **Remove All** to isolate all the note fields. A confirmation for isolation appears.
11.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

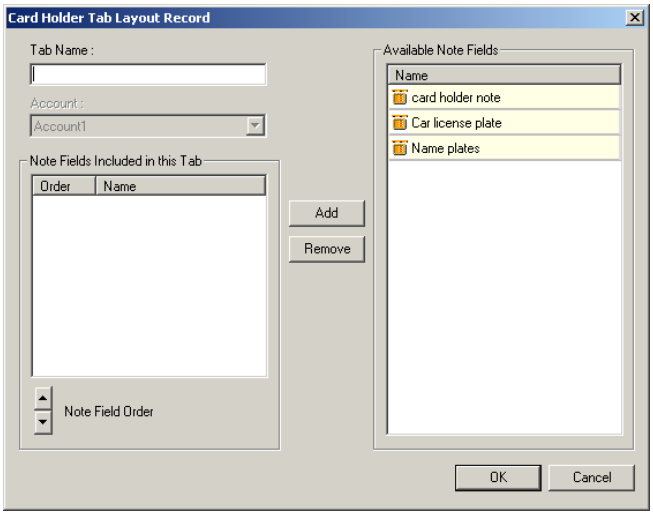


Adding a Card Holder Tab Layout

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.

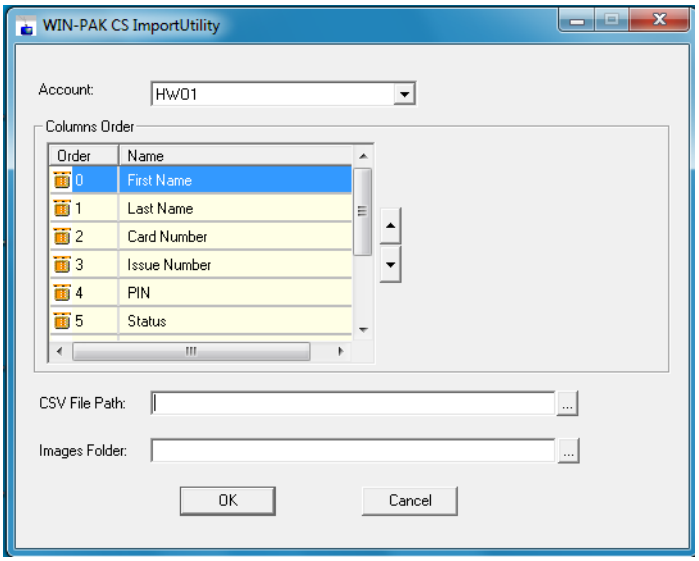
Defining Card and Card Holder Entries in Microsoft Excel

Note: This section is applicable only for WIN-PAK CS.

You can define and import the Card and Card Holder fields in Microsoft Excel. You must ensure to define the note fields and Card Holder tabs before you define the order of the Card and Card Holder fields.

To define the order of the fields:

1. Log on to the **WIN-PAK CS Import Utility**. The **WIN-PAK CS ImportUtility** dialog box appears.



2. Select the **Account** to which the order must be defined. The card holder fields for the selected account are listed under **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 Entries in Microsoft Excel

Note: This section is applicable only for WIN-PAK CS.

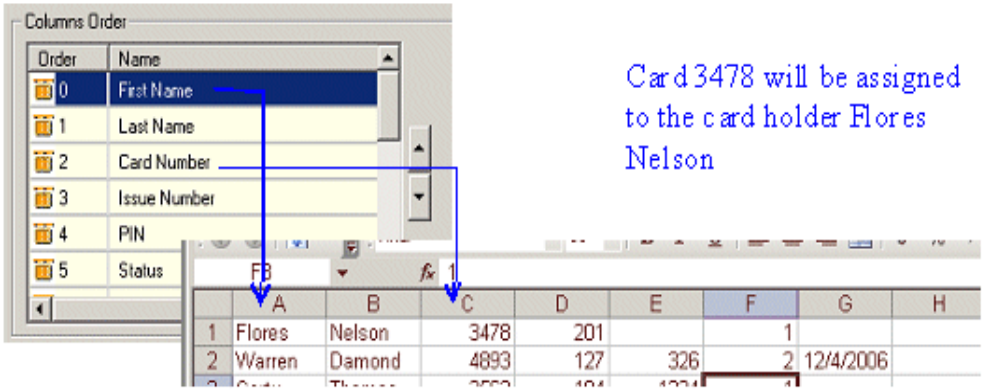
After you define the Card and Card Holder fields in Microsoft Excel, you can enter relevant data in the excel sheet. Before you create the excel sheet, make a note of the column order in which the fields must be entered.

To enter the card and card holder information in the excel sheet:

1. Open a new sheet in **Microsoft Excel**.
2. Enter the card and card holder information in the excel sheet. The entered information should be in sequential order and must match the order that is defined in the **WIN-PAK CS Import Utility.**
3. Save the excel sheet in the .xls or .csv format.

Note: When you import an excel sheet to WIN-PAK CS, 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.



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 CS.
- 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.

Tips:

- Ensure that access levels are configured in WIN-PAK CS 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.

Import from Excel Sheet

Note: This section is applicable only for WIN-PAK CS.

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 CS database, before importing the data to WIN-PAK CS.

To import the card and card holder information from an excel sheet:

1. Log on to WIN-PAK Import Utility. The WIN-PAK CS ImportUtility dialog box appears.

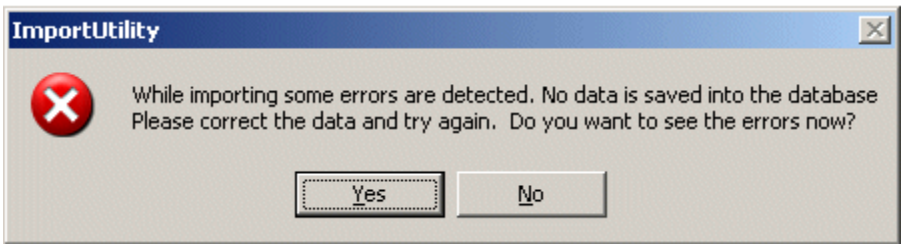
2. Select the Account to which the card and card holder information must be imported. The corresponding fields are displayed in Columns Order.
3. In CSV File Path, specify the path of the excel sheet or click the ellipsis button and select the path.
4. In Images Folder, select the folder in which the 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 CS 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.
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:

Input character	Mask Description
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.

Input character	Mask Description
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.
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.

Configuring Autocard Lookup

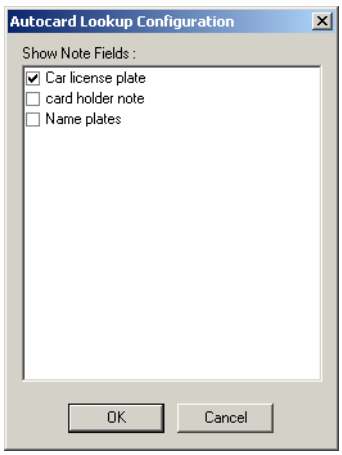
When a card is accessed, WIN-PAK identifies the card holder and displays the basic information in AutoCard Lookup by default.

See the Autocard Lookup, page 755 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 CS/SE/PE users for various areas in the access control system, pertaining to the specific account selected. The **Access Level** window contains information of the existing access levels and the corresponding access areas.

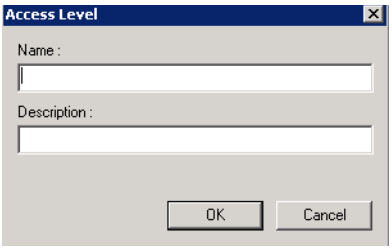
Notes:

- Before you configure the access levels, ensure that you have defined the access areas. See the "Defining Access Areas" section in the chapter Defining Areas.
- WIN-PAK CS configuring screens are shown in this section as an example. The screens would change based on the variant selected.

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. Access levels are specific to accounts.



3. Type the **Name** of the access level and the **Description**.

Notes: Follow the below steps, if you are Configuring Access Levels in WIN-PAK SE/PE:

- 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.
- If you want to assign the access level to another accounts, select the account in the **Available Account** list and click **Add**. The account is moved to the **Selected Account** list.

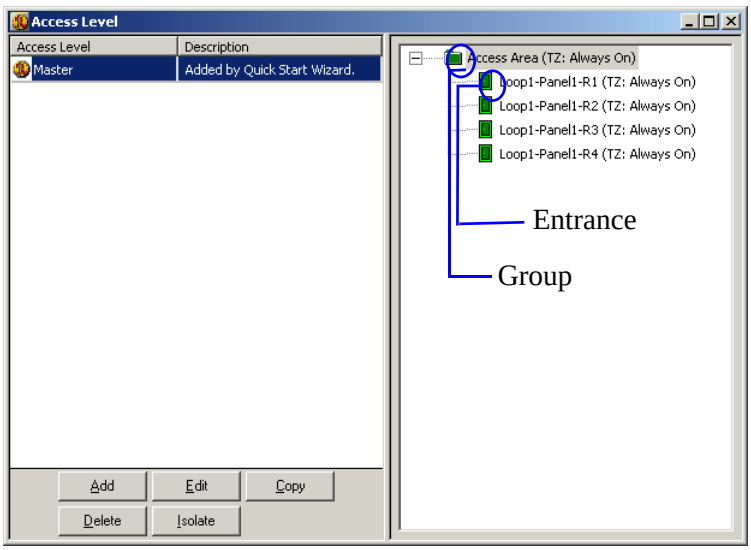
4. Click **OK** to save the details.

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.



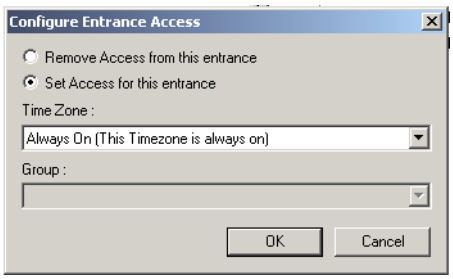
   The left-side of the window lists the access levels and the right-side of the window displays the access area tree.

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.

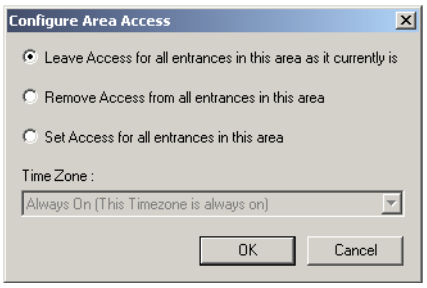
3. In the **Access Level** window, right-click the access area to which you want to set the access levels and select **Configure**. The **Configure Area Access** dialog box appears.

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.
- 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.
- To refresh the list, right-click and select **Refresh**.

Copying the Access Level

WIN-PAK CS/SE/PE 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 CS/SE/PE you can configure card and card holder information by:

1. Adding a card and card holder in WIN-PAK CS/SE/PE manually.

   See the"Adding a Card and Card Holder Information"section in this chapter for adding a card and card holder information in WIN-PAK CS/SE/PE manually.
2. Importing the card and card holder information from the Excel sheet to WIN-PAK SE/PE.

   See the Import from Excel Sheet, page 252 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

A card holder is uniquely identified by the card. The access areas 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.

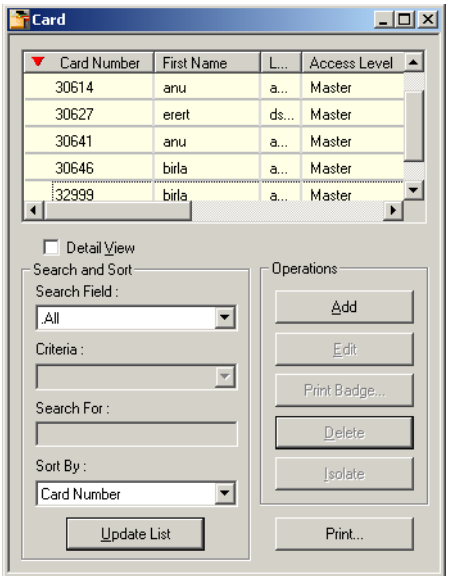
Notes:

- To add a card in WIN-PAK CS, follow steps from 1 to 22.
- To add a card in WIN-PAK SE/PE, follow steps from 1 to 15.

- WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

To add a card:

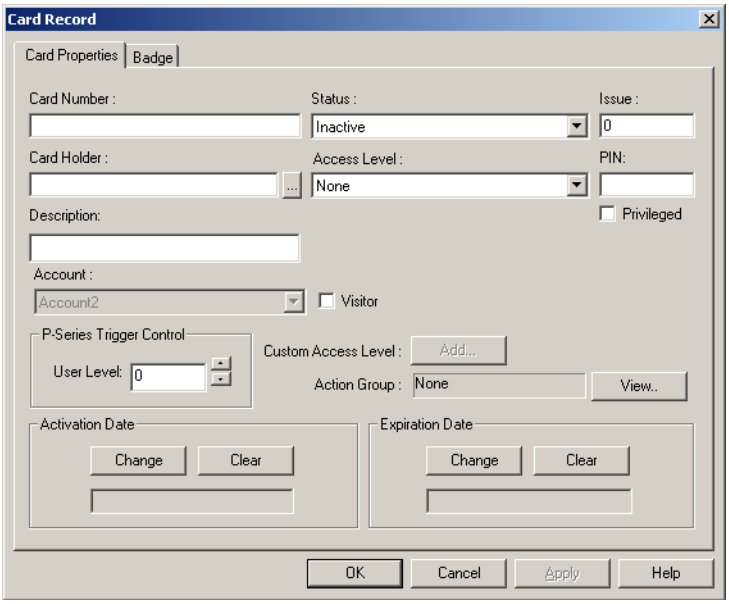
1. Choose **Card > Card** or click  in the toolbar. The **Card** window is displayed.



2. Click **Add** to add a new card.

   OR

   Select the card and click **Edit**. The **Card Record** dialog box appears.



3. Click the **Card Properties** tab. It is selected by default.

4. From the **Mobile Credentials vendor** drop-down list, select **HID** to assign the HID card to the selected card holder.
5. Type a unique **Card Number**.
6. Click the ellipsis button to select the **Card Holder**. The **Select** dialog box appears.
7. Select the **First Name** or **Last Name** in the **Find Key** list.
8. 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.

9. Select the card holder and click **OK**. The **Select** dialog box is closed and returned to the **Card Record** dialog box.
10. 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.
    - **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.

Note: Select the status as Lost or stolen, if the card is lost or stolen. The access will be restricted.

11. 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**.
12. Type the **Issue** number to trace the number of times the card is issued.
13. Type the unique **PIN** number. The PIN number adds more security to the card.

Notes:

- 6 digit PINs are compatible with only the Net AXS and P Series panels. If N1000 panels are present in the system, then you must configure the PIN 1 between 65535. Also, PRO3000 supports up to 10 digits.
- In WIN-PAK SE/PE, select the **Privileged** check box if the card must be assigned as a privilege card. The card holder can set or clear the galaxy groups associated to the reader on which the card is presented. If the Vista feature is enabled, the card holder can arm or disarm vista partitions.

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 CS/SE/PE with LobbyWorks. Also when Lobby Works version 3.2 is used on Windows XP operating system.

16. Under **P-Series Trigger Control**, type the **User Level** number or click ▲ or ▼ buttons to increase or decrease the current index number.

17. 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.

Defining a custom access level

A card is configured with an access level. You can customize the access level for a card without making any change to the main access level.

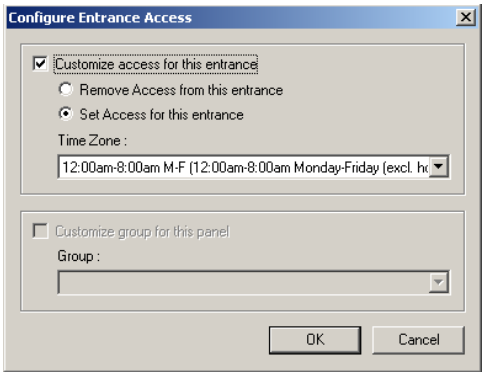
Note: In WIN-PAK CS at present the NetAXS panel is limited to only 128 access levels.

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.

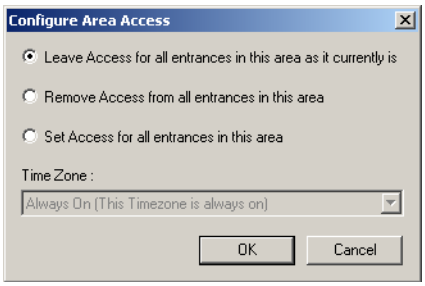
2. Right-click and select configure area access or double-click the area where you want to provide access. The **Configure Entrance Access** or **Configure Area Access** dialog box appears based on the selected area; Entrance or Area.

3. For one entrance, select one of the following:



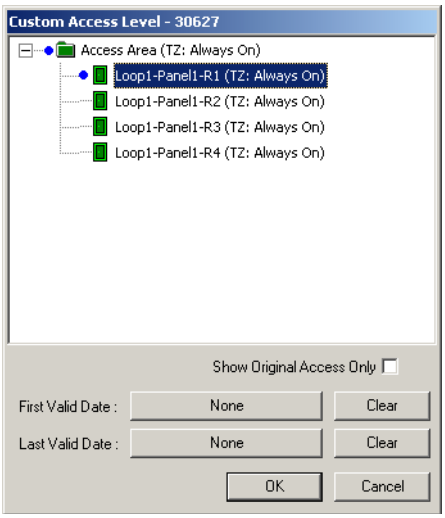
- **Remove Access from all entrances in this area** to deny access through this entrance for this access level.
- **Set Access for all entrances in this area** to allow access through this entrance for a particular time zone. Select the time zone in the Time Zone list to determine periods of access.

For group entrance, select one of the following:



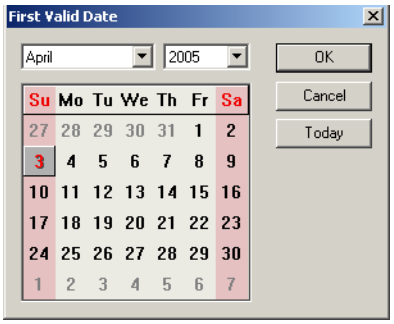
- **Leave Access for all entrances in this area as it currently is** to continue the same for each entrance in this group.
- **Remove Access from all entrances in this area** to deny access through these entrances for this access level.
- **Set Access for all entrances in this area** to allow access 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.

Setting the NetAXS Card type

Cards used with a NetAXS panel can be set with a Card Type. The card types available are: Standard, Supervisor, and VIP. Different card types are introduced to have more flexibility in providing appropriate privileges to card holders.

1. Under **NetAXS Advanced**, select one of the following Card types.
   - **Standard** - Select this card type if the card holder is an employee. This is the default selection.
   - **Supervisor** - Select this card type if the card holder is a supervisor. See Glossary for definition of Supervisor.

- **VIP** - Select this card type if the card holder is a VIP. VIP card has the maximum privileges. They override all Access mode restrictions like Disable, lockdown, card and PIN, card or PIN, pin only and card only. VIP cards do not need a supervisor card to gain access.
- **Limited Number of Uses** - Select this check box and type the number of times a card can be used at the NetAXS panel before it expires in the text box provided. Maximum number of uses is 255. The **Limited Number** of Uses check box is ONLY applicable to the NetAXS panels.

Notes:

- If you select "**VIP**", then the fields, **PIN** and **Limited Number of Uses** and its corresponding text box are disabled.
- In WIN-PAK SE/PE under PRO3000 Card Type, select one of the following card types:
  - **Standard** - Select this card type if the card holder is an employee. This is the default selection.
  - **VIP** - Select this card if the card holder is a VIP. VIP card has the maximum privileges. They override all Access mode restrictions like APB, N-Man rule, dual door interlock, dual door lock, door mode.

2. Select the **Temporary** check box to set a temporary flag for selected card holder. Temporary cards are generally issued to visitors and employees (if they forget their access card).

Note: If the card is to be used with a NetAXS panel, then the **Temporary** check box must be selected for the **Expiration Date** field to be active.

A temporary (Temp) flag can be set for each type of card holder. When the Temp flag is enabled, the Expiration Date becomes an active field.

3. The **Activation Date** of a card is by default the current system date.
4. Click **Change** to set a new activation date or click Clear to reset to the current system date.
5. The **Expiration Date** of a card is set by the NetAXS panel.

Click **OK** to save the changes.

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.

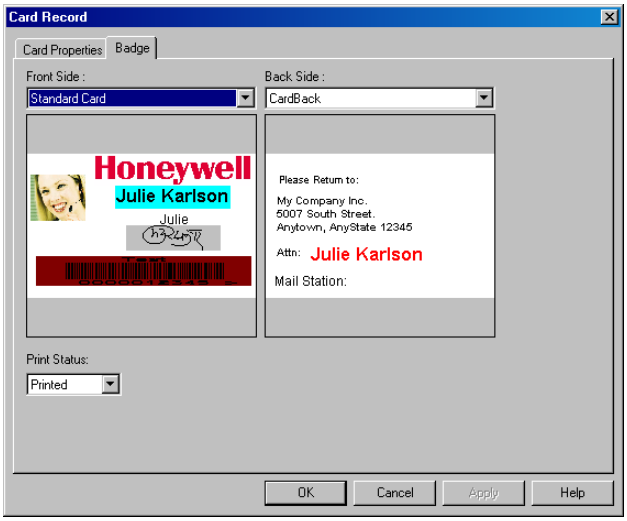
Note: The Activation Date is enabled only if you select the **Status** as Inactive.

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:

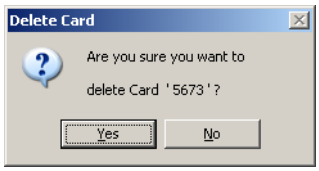
1. Choose **Card > Card** or click  in the toolbar. The **Card** window appears.
2. Select the card to be edited from the list and click **Edit**. The **Card Record** dialog box appears.

   See 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.

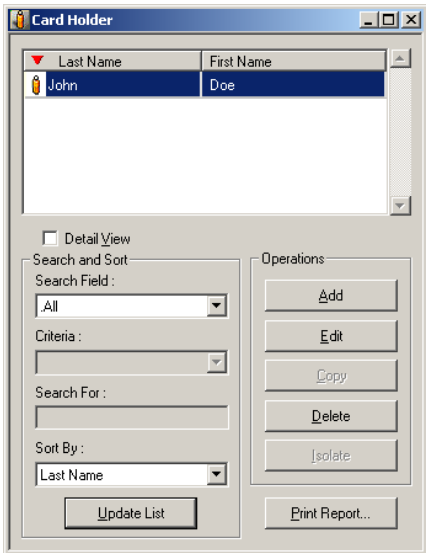
Adding a Card Holder

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.

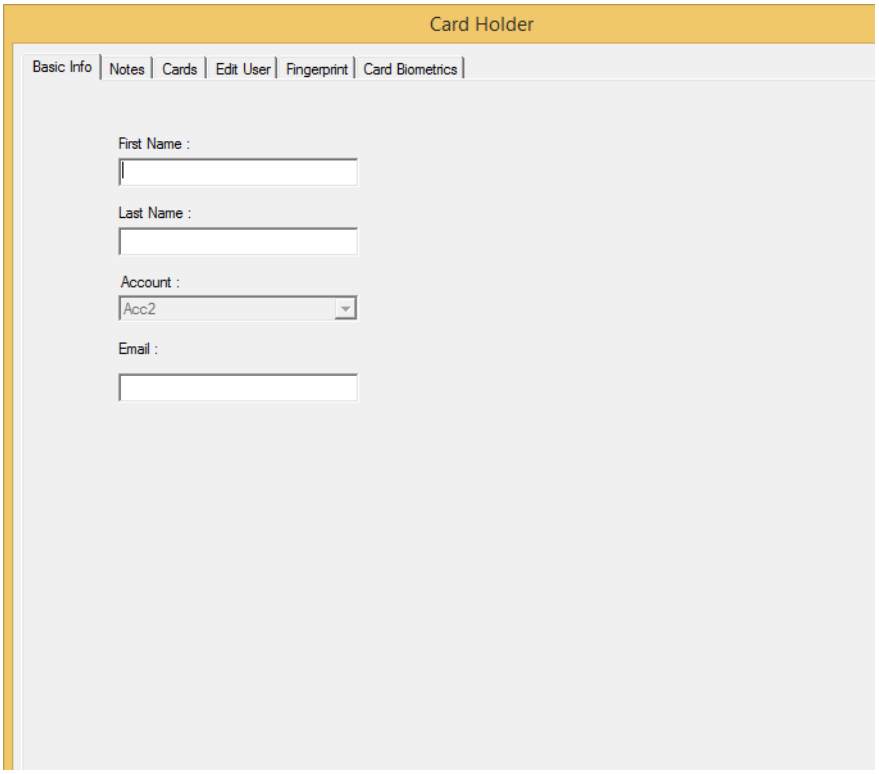
Providing card holder basic information

1. Choose **Card** > **Card Holder** or click in the toolbar. The **Card Holder** window appears.



2. Click **Add**. 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.



4. Type the **Email ID** of the card holder to whom the HID card has to be assigned.

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.

5. Click **OK**. The basic information is saved.

Sending an email as an SMS

To send a short email as a text:

1. Using the email client of your choice, compose your email as you would normally. You can use either your smartphone or your computer to do so.
2. Instead of entering an email address in the recipient box, insert the 10-digit phone number of the person you're trying to reach.
3. Once entered, tack on the appropriate "@gateway" address behind the phone number. Below, we've put together a list of some of the most common service providers in the United States and their corresponding gateway addresses.

Carrier	SMS gateway domain	MMS gateway domain
Alltel	[insert 10-digit number]@message.alltel.com	[insert 10-digit number]@mms.alltelwireless.com
AT&T	[insert 10-digit number]@txt.att.net	[insert 10-digit number]@mms.att.net
Boost Mobile	[insert 10-digit number]@myboostmobile.com	[insert 10-digit number]@myboostmobile.com
Cricket Wireless		[insert 10-digit number]@mms.cricketwireless.net
Project Fi		[insert 10-digit number]@msg.fi.google.com
Sprint	[insert 10-digit number]@messaging.sprintpcs.com	[insert 10-digit number]@pm.sprint.com
T-Mobile	[insert 10-digit number]@tmomail.net	[insert 10-digit number]@tmomail.net
U.S. Cellular	[insert 10-digit number]@email.uscc.net	[insert 10-digit number]@mms.uscc.net
Verizon	[insert 10-digit number]@vtext.com	[insert 10-digit number]@vzwpix.com
Virgin Mobile	[insert 10-digit number]@vmobl.com	[insert 10-digit number]@vmpix.com
Republic Wireless	[insert 10-digital number]@text.republicwireless.com	

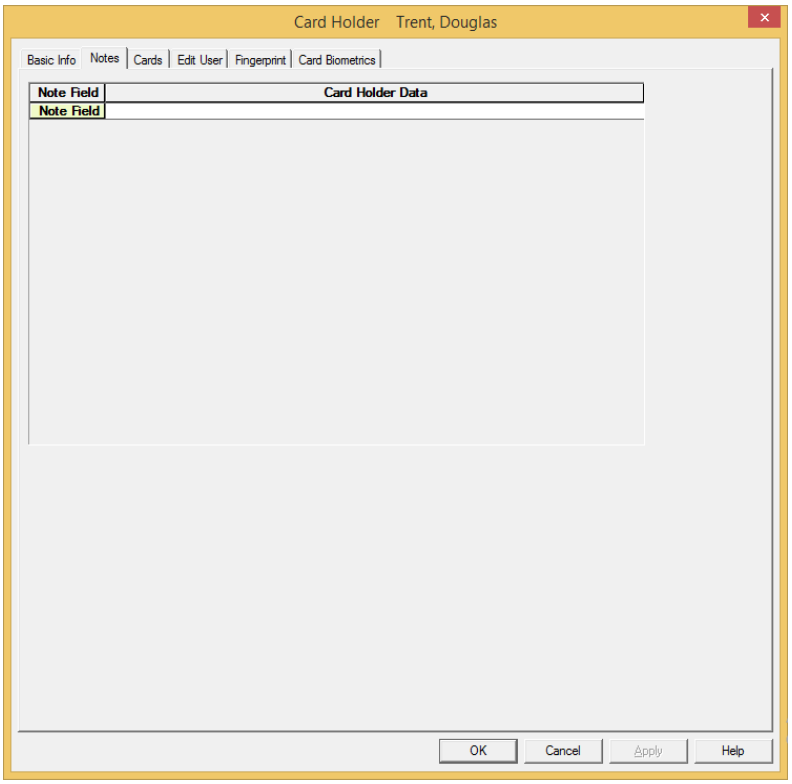
Note: If you are trying to send an email that's more than 160 characters long, it will often be sent through the Multimedia Message Service (MMS). If the person you are messaging does not have a messaging plan that includes Multimedia Messaging, then they will not receive the message.

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**.

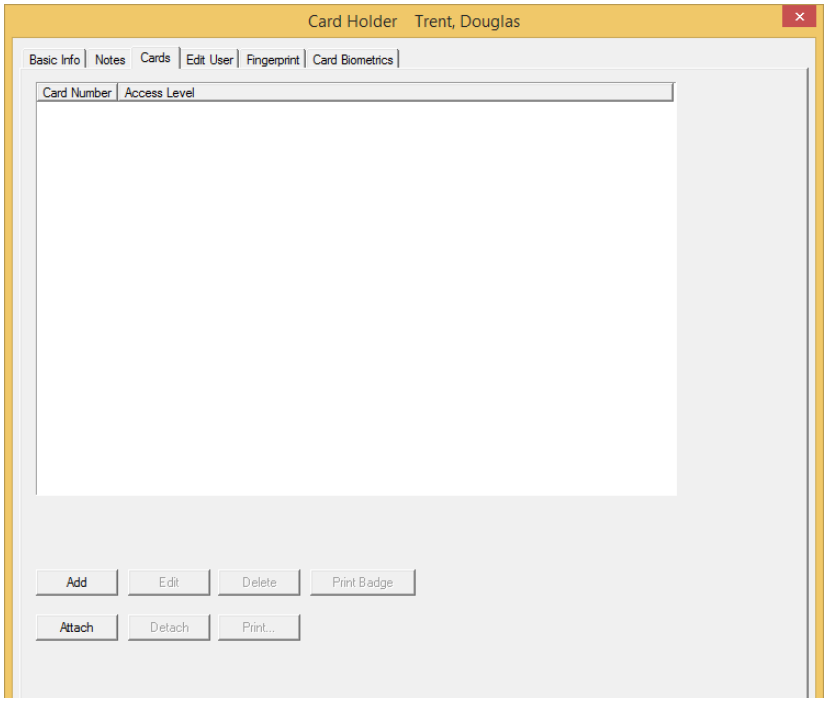
4. Enter the additional information of the card holder in the fields under the **Card Holder Data** column.
5. Repeat steps 3 and 4 for the remaining tabs.
6. Click **Apply**. The additional information is saved.

Adding and attaching a Card to a Card holder

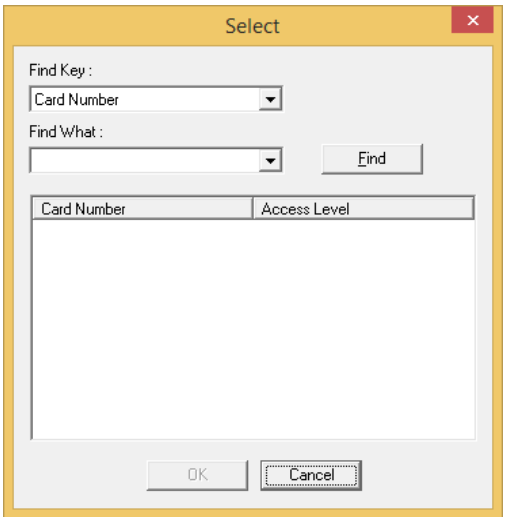
Using the **Cards** tab, you can attach a new card or an existing card to a card holder. In addition, you can print a badge associated to it or you can print the card reports.

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.

See 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:

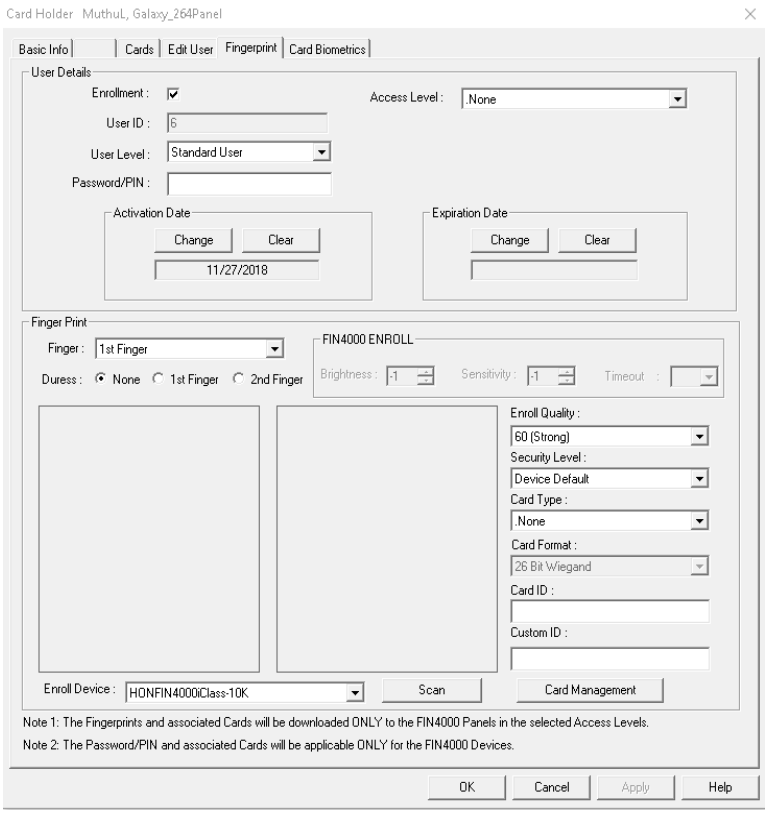
a. Select the card from the list and click **Detach**. The card is detached from the card holder.

Note: If you detach a card, it is dissociated from the card holder and not deleted from the card list.

Attaching a new or an existing Card to a Card Holder in WIN-PAK SE/PE

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 **Fingerprint** tab.



2. Under **User Details**, enter the following details:

Field	Description
Enrollment	Select to enable the process of creating a user and capturing images of fingerprints or issuing access cards.
User ID	The User ID is automatically populated after adding the cardholder. The user ID identifies the user.
User Level	From the drop-down list, select the administration level of the user. The available options are: Standard User Administrator If the configuration has HON FIN4000K-10K panels, Honeywell recommends you to add at least one user with administrator credentials. The user with administrator user level can access the following: Doors that are enabled with timed anti-passback. Doors that are configured with lock time zone option.
Password/PIN	Type the unique Password/PIN number. The PIN number servers as an additional level of security for the User credentials.
Access Level	From the drop-down list, select the required access level. The access level determines the option to provide restricted access to the WIN-PAK users, for various areas in the access control. A maximum of 4 access levels can be assigned in case of multiple access level.

Field	Description
Activation Date	By default, the activation date of a user credential is the current system date. Click Change to set a new activation date or click Clear to reset to the current system date.
Expiration Date	The expiration date is set for the expiry of the user credentials. Click Change to set a new expiration date or click Clear to clear the expiration date.

3. Under **Finger Print**, enter the following details:

Field	Description
Finger	From the drop-down list, select the finger that will be used to enroll the fingerprint. A maximum of two fingers can be registered for any card holder.
Duress	You must select the duress finger that will activate silent alerts when the user is under duress.
HON FIN4000-Enroll Parameters	Set the following parameters when the fingerprints are being enrolled through USB based HON FIN4000-Enroll devices. **Brightness:** Set the modify the brightness of the fingerprint image. **Sensitivity:** Set the sensitivity of the fingerprint scanner (0 [Min] to 7 [Max]). A higher sensitivity setting results in easily captured fingerprint scans, but also increases the sensitivity to external noise. **Timeout:** Set the length of time before the fingerprint scanner will timeout (1 sec to 20 sec).

Field	Description
Enroll Quality	From the drop-down list, select to set the quality threshold of the scanned fingerprint images. If the quality of the scanned fingerprint image is lower than the Enroll Quality value, the scanned fingerprint can be reject to enroll.
Security Level	From the drop-down list, select to set the security level to use the fingerprint. Normal Secure Most Secure Based on the security level that is selected, the likelihood of a false rejection increases.
Card Type	From the drop-down list, select to the card type for reading the card.
Card Format	From the drop-down list, select the card format for reading the Wiegand card.
Card ID	Enter a card ID either manually or by reading from the card.
Custom ID	Enter the custom ID either manually or by reading from the card.
Enroll Device	Select a device to use for scanning fingerprints. Before you begin the enrollment of fingerprints/cards through HON FIN4000K-20K, HON FIN4000K-10K, and HON FIN4000 10K, Honeywell recommends you to use the **Disconnect Panel** option in the **Control Map/Floor Plan**. You can re-connect to the panel through the **Reconnect Panel** option in the **Control Map/Floor Plan**.

Field	Description
Scan	Click to begin scanning the fingerprint.
Card Management	Click to manage the issued cards. The HID cards require only a card ID to complete card registration, while the MIFARE and iCLASS cards support two operation modes: Card Serial Number (CSN): Enables you to read the serial number. Template-on-Card: Enables you to record the user information, including fingerprint templates, directly to the card.

4. Click **OK**.

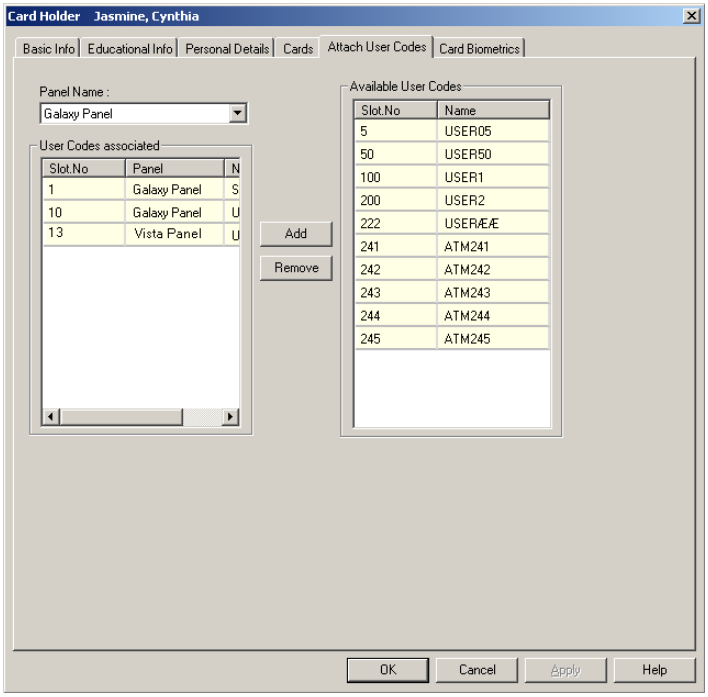
Attaching User Codes to a Card Holder

A card holder can be attached to the user codes for accessing and working on the Galaxy panel or Vista panel.

Note: This section is applicable only for WIN-PAK SE/PE

To attach user codes to the card holder:

1. In the **Card Holder** dialog box, click the **Attach User Codes** tab.



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.

   See the Adding a Galaxy Panel, page 368 or Add a Vista Panel Port, page 424 sections for configuring panels in WIN-PAK SE/PE.

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. In the **Card Holder** dialog box, click the **Cards** tab.

2. Click **Add**. The **Card Record** dialog box appears.

3. 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.

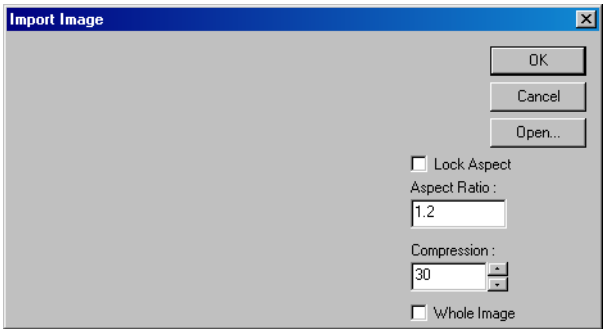
Note: Use the **Previous** and **Next** buttons to move to the rest of the badges associated to the card and click **Print**.

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.

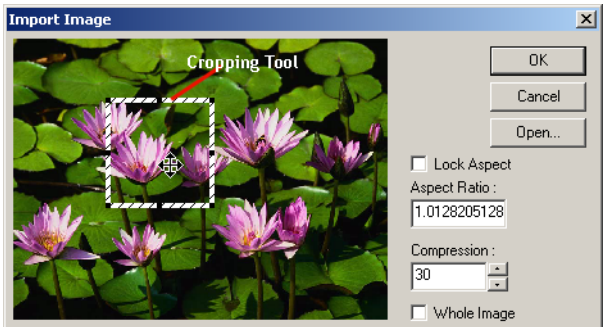


   b. Click **Open** and browse through the required folder.

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.

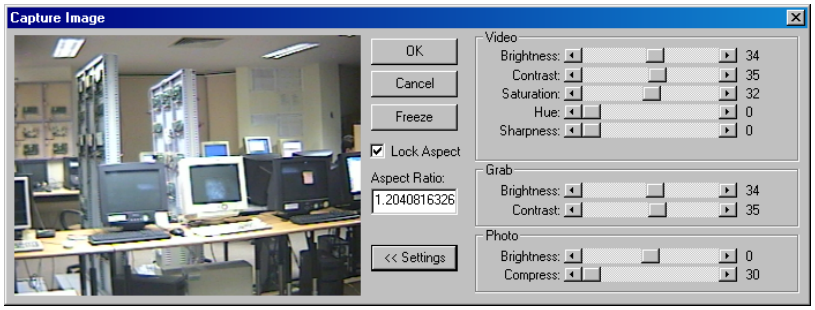
Note: 100 is the least compression and the best quality. 30 is the highest compression and the lowest quality.

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 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.
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 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 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 7-3 Live Screen Photo Settings

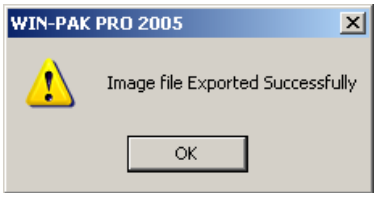
Setting	Description
Photo Brightness	Lightens or darkens the entire tonal range of the captured image.
Compress	The captured image is saved as a .jpg file. If required, use the slider to adjust the compression of the saved image. The lower the number, the greater the compression. **Note:** Images lose 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 CS 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**.

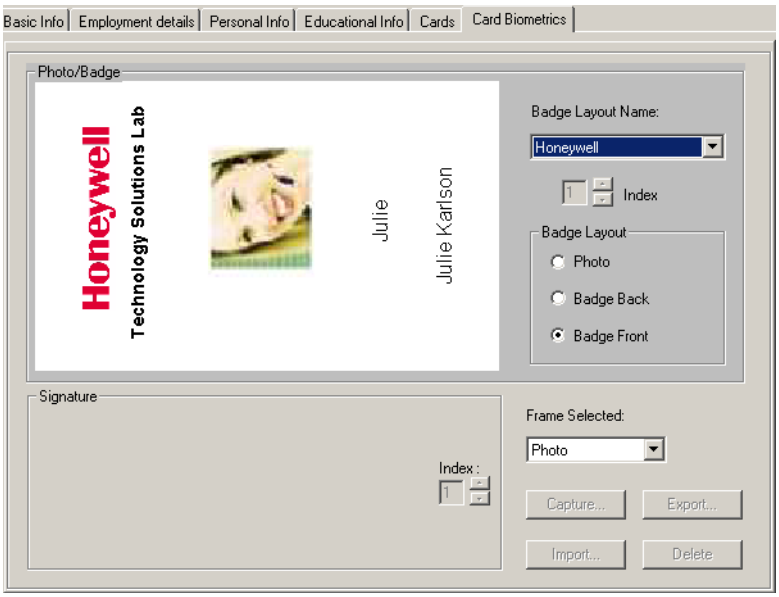
To capture additional card holder photos:

- 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.
3. Under **Badge Layout**, select **Badge Back** or **Badge Front** to attach a badge to a card holder at the back or front.

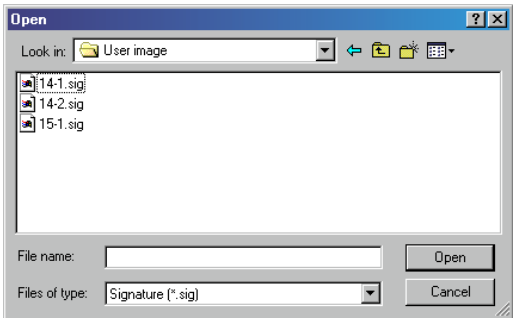


4. Select the badge design in the **Badge Layout Name** list. The selected badge design is displayed in the preview area.

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 the card holder details and close the **Card Holder** dialog box.

Editing Card Holder Information

To edit the card holder details:

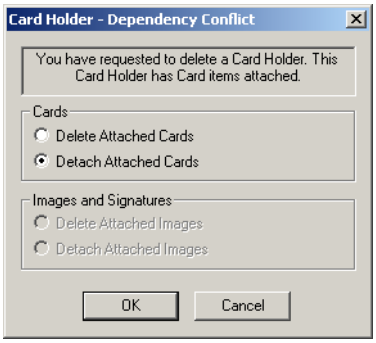
1. Choose **Card** > **Card Holder**. The **Card Holder** window appears.
2. Select the card holder from the list and click **Edit**. The **Card Holder** dialog box appears.

   See the Adding a Card Holder section in this chapter for more 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.

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.

  See 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.

8. See the "Adding a Card Holder" section for more details on adding card holders.

Configuring Autocard Lookup

Note: This section is applicable only for WIN-PAK CS.

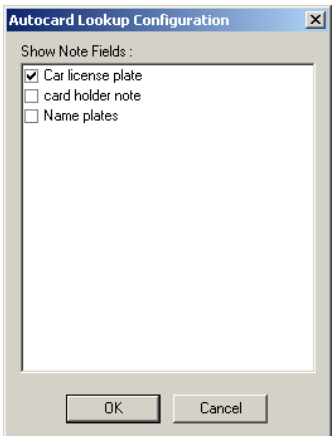
When a card is accessed, WIN-PAK CS identifies the card holder and displays the basic information in **AutoCard Lookup** by default.

See the "System Viewer Real Time" section in Monitoring Actions chapter 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.

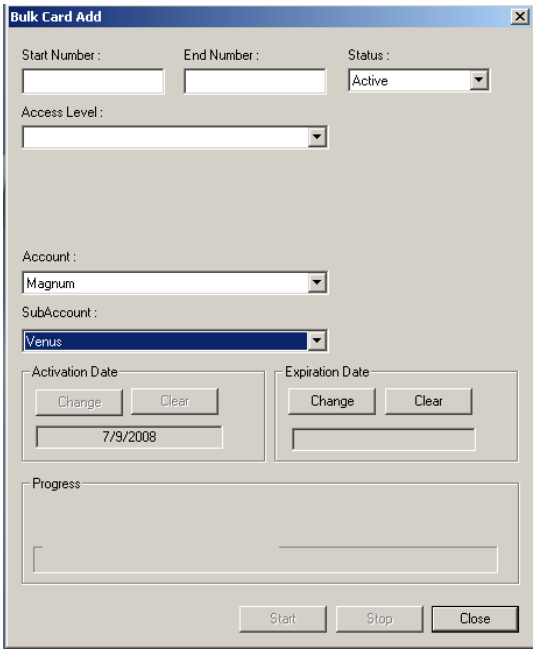
Adding Bulk Cards

This option enables you to collectively add the details of multiple employees simultaneously.

Note: WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

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.

Notes:

- In WIN-PAK CS, the cards added in bulk must be assigned to an access level.
- In WIN-PAK CS, select the account for which you want to add the cards in bulk. If you are in the <System> account, select the account.
- IN WIN-PAK SE/PE, select the **Visitor** check box, if the cards are for visitors.
- In WIN-PAK SE/PE, select the front and back badge designs of the cards in **Badge Front** and **Badge Back**..

5. Select the **Activation Date** and **Expiration Date.**
6. Click **Start** to add the cards. The progress bar displays the progress of adding bulk of cards.

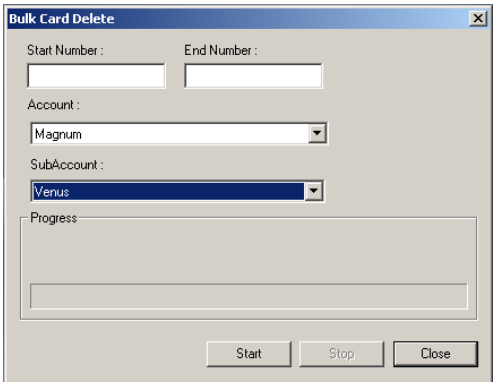
Caution: Do NOT close any WIN-PAK CS/SE/PE services or turn-off the computer while the Bulk Card Add is in progress.

7. Click **Stop**, if you want to cancel generating cards in bulk.
8. 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.

Note: In WIN-PAK CS, select the **Account** and the **SubAccount** for which you want to delete the cards in bulk. If you are in the <System> account, select the account.

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.

Importing Card and Card Holder Information

Note: This section is applicable only for WIN-PAK SE/PE.

The WIN-PAK Import Utility is used for importing the card and card holder details into WIN-PAK SE/PE from an excel sheet. When you import these details into WIN-PAK SE/PE, cards are assigned to the card holders accordingly.

Importing card and card holder details to WIN-PAK SE/PE involves:

1. Defining note fields and card holder tab layouts, and configuring access levels.

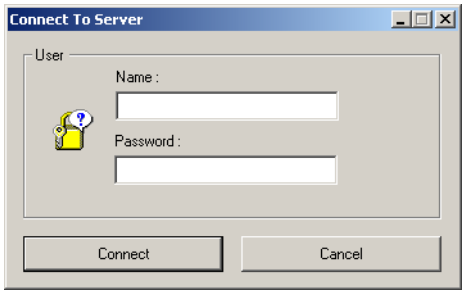
   See the Configuring Card Holders section in this chapter for more details on defining note fields, card holder tab layouts and access levels.

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 SE/PE.

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.



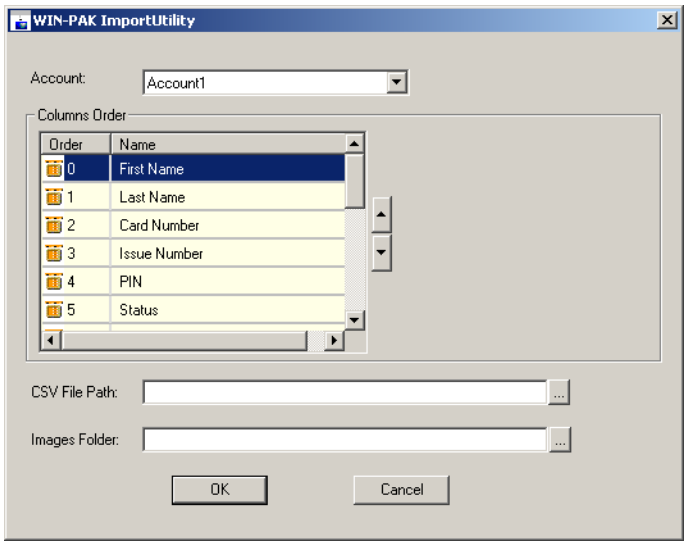
2. Type the **Name** of the user and the **Password**.
3. Click **Connect**. The system retrieves the data from database and displays the **WIN-PAK ImportUtility** dialog box.

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.



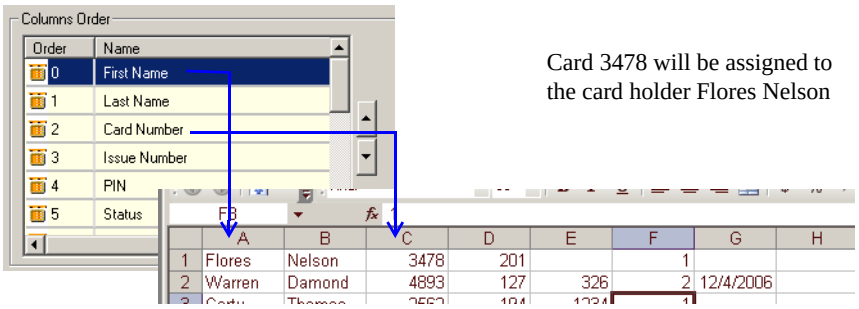
2. Select the **Account** to which the order is to be defined. The card holder fields for the selected account are listed in **Columns Order**.
3. To change the order of a row, select the row in the list and click the up button and/or down button.

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.



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 SE/PE.
- For the Status field, type 1, 2, or 4 to indicate the card status as Active, Inactive, or Trace.
- Ensure that access levels are configured in WIN-PAK SE/PE 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.

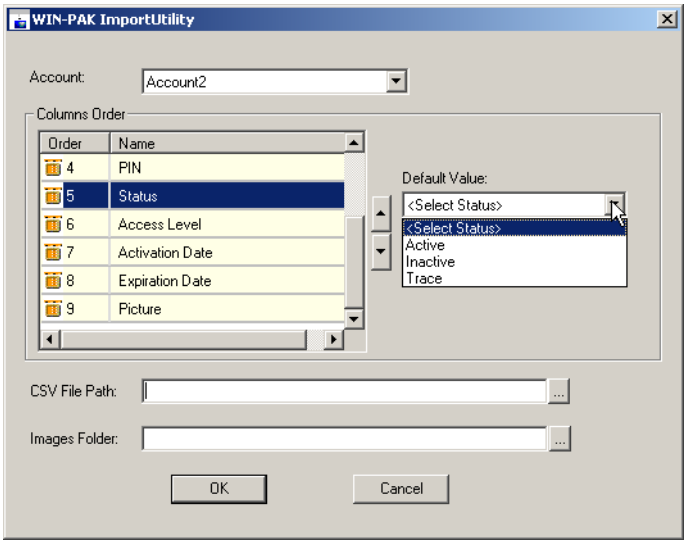
Assigning Default Values

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.

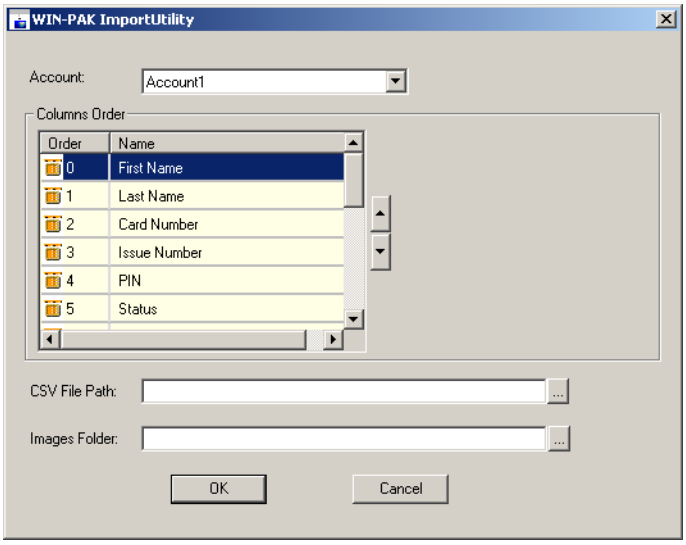
Tip: To set the current dates for Activation Date or Expiration Date, select the check box. To set different dates, click the drop-down list and select the required date in the calendar.

Importing from Excel Sheet

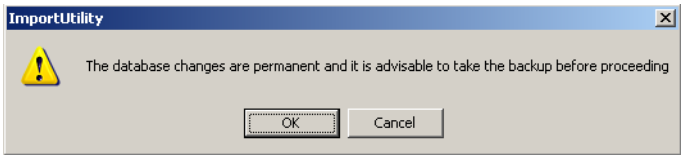
You can import the card and card holder information from the excel sheet in which the card and card holder information is entered.

To import the card and card holder information from an excel sheet:

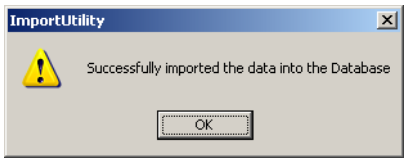
1. Log on to WIN-PAK Import Utility. The **WIN-PAK ImportUtility** dialog box appears.



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.

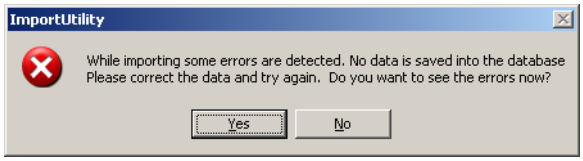


Correcting Errors in Excel Sheet

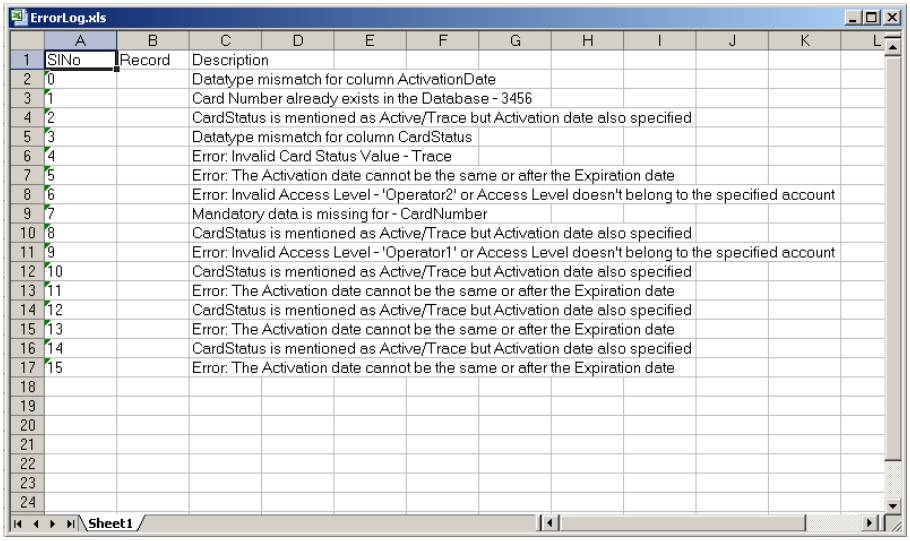
Errors might occur while importing the data from the excel sheet. You cannot import the card and card holder information to WIN-PAK SE/PE until you correct these errors.

To view and correct the errors:

1. In case of errors during an import, the following message appears prompting you to open and view the error list.



2. Click **Yes** to view the errors. The **ErrorLog.xls** file opens.



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:

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.

Error Type	Corrective Action
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.
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

Note: Only Lobby Works version 3.2 when used on a Windows XP operating system is supported.

LobbyWorks, a Visitor Management system that tracks the movement of visitors, assets, and deliveries, can be integrated with WIN-PAK SE/PE. By doing this, the access cards that are created for visitors in LobbyWorks can be used in WIN-PAK SE/PE as access cards. After the access cards are copied from LobbyWorks to WIN-PAK SE/PE, they are provided with the necessary access levels for allowing or restricting visitors to the different areas in the premises.

Integrating LobbyWorks

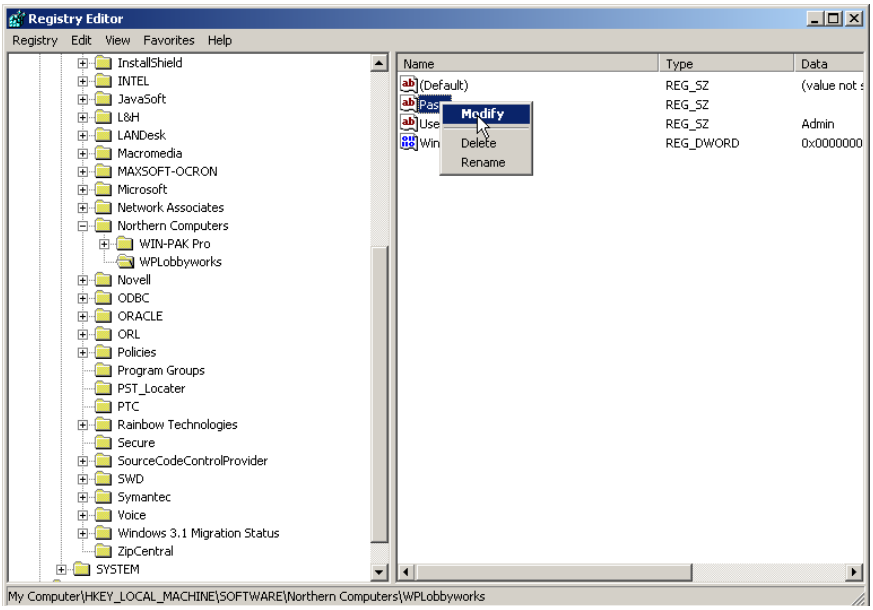
Before you begin:

- Ensure to install WIN-PAK SE/PE and LobbyWorks on the same network.
- Procure the license for integrating LobbyWorks with WIN-PAK SE/PE.

Setting Key Values

To integrate LobbyWorks with WIN-PAK SE/PE:

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 SE/PE in the WIN-PAK SE/PE authentication mode.

    OR

    Set the **Value data** of WinAuth as **1**, if you are logging on to WIN-PAK SE/PE in the Windows authentication mode.

6. Close the **Registry Editor** window.

Time Management

8

In this chapter...

This chapter gives an introduction to the Time Management and describes about the Time Zone, Schedule, Holiday Group, Daylight Saving Group, Holiday Master in WIN-PAK CS, and SE/PE.

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. In WIN-PAK CS the accounts are mutually exclusive. Therefore, a Time Zone configured for an account is unavailable to another.

Notes:

- In WIN-PAK CS the time zones are common across all the accounts and it can be configured in the system account. This is called a System Time Zone.The default system time zones are Always On and Never On.
- In WIN-PAK CS You can create any number of Time Zones. However, a maximum of 63 time slots can be downloaded to a PW-2000, PW-5000, and PW-6000 series panel and 255 time slots can be downloaded to a PRO-2200 and PRO-3200 Intelligent Controller.

See the “Time Zone” section in this chapter for configuring a time zone.

Schedule

A schedule is a planned task that must be performed at the defined time periods. In WIN-PAK CS/SE/PE, a task includes running a command file, guard tour, or generating a report, and so on. Every account in WIN-PAK CS/SE/PE has a unique schedule.

See 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. This is also account specific.

See 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.

See the “Daylight Saving Group” section in this chapter for configuring a daylight saving group.

Holiday Master

Holiday Master is a group of holidays common across accounts. This is a master list from which holidays can be added to a holiday group.

See the "Holiday Master" section in this chapter for configuring a holiday master.

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 time zones that are available in WIN-PAK CS/SE/PE 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.

Notes:

- Time Zones are account specific. A time zone set in an account is not visible in any other accounts.
- You cannot edit the Always On and Never On time zones, as these are generated by WIN-PAK CS/SE/PE.
- WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

Configuring a Time Zone for an Account

To configure a time zone for an account, select an account, and then add a time zone to the specific account.

Selecting an Account

To select an account:

1. Choose **Account** > **Select** or click . The **Select Account** window appears.
2. Under **Account Name**, select the required account.
3. Click **Select**. The account is selected.

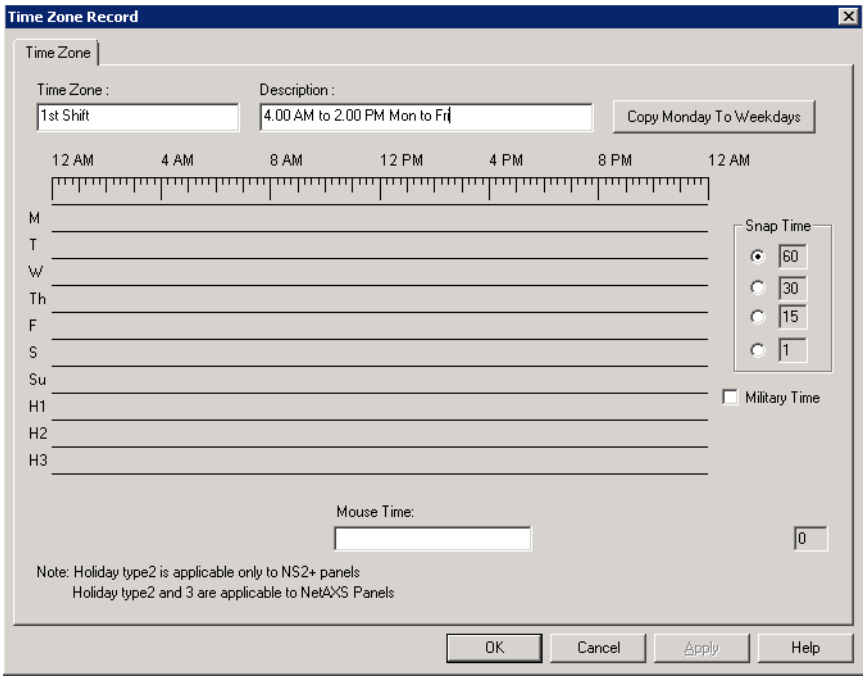
Note: You can also double-click the required account from the **Account Name** list to select it.

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.

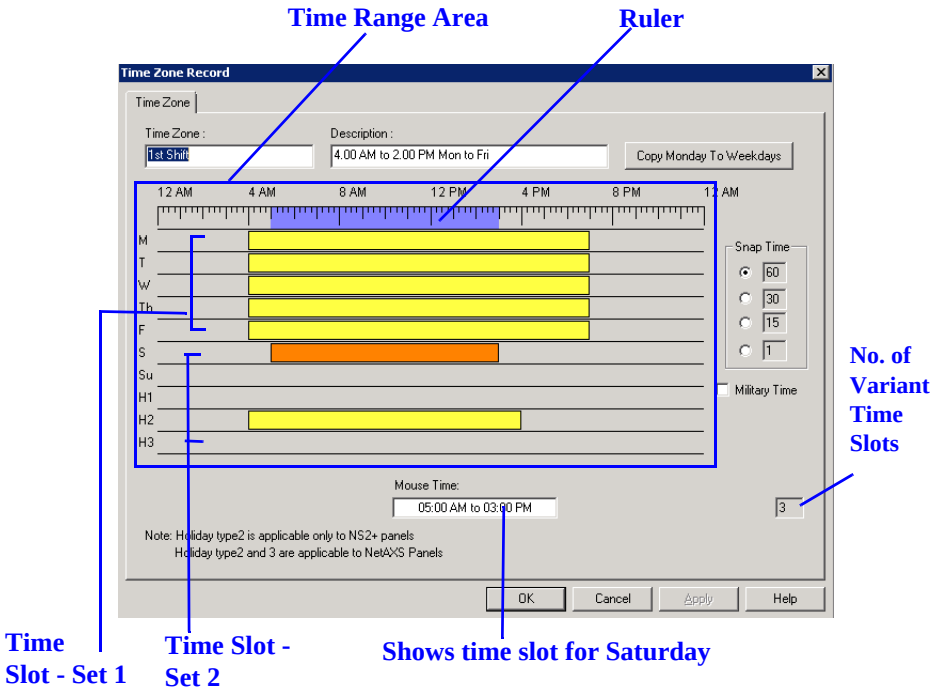


3. Type the name of the **Time Zone** and a brief **Description**.
4. Select the corresponding **Snap Time**. The **Snap Time** option enables you to set the time slot according to the selected snap time.

Example: If you set a **Snap Time** of 60 minutes, you can 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.

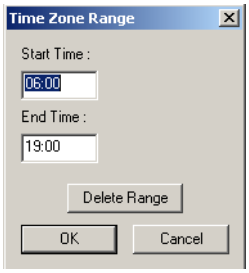


5. To define a time slot:

   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** and **H3**.

Notes:

- When time zones and holiday groups are assigned to an NS2+ panel, the time slots defined for the holidays H1 and H2 are applied to the holiday group.
- Holiday Type H2 is applicable only to NS2+ panels. Both Holiday Type H2 and Holiday Type H3 is applicable to NetAXS panels.
- Follow the below steps, if you are working with WIN-PAK SE/PE:
    a. Click the **Accounts** tab to associate accounts to the time zone. You must assign an account to a time zone, after setting the time slots.
    b. Under **Available Accounts,** select an account and then click **Add**. For multiple selections, use the **Shift** or **Ctrl** key while selecting the accounts.
    c. 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.

10. Click **OK** to save the Time Zone.

Note: These steps can be repeated to configure time zones for all the accounts in WIN-PAK CS/SE/PE.

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 system time zones generated by WIN-PAK CS/SE/PE.

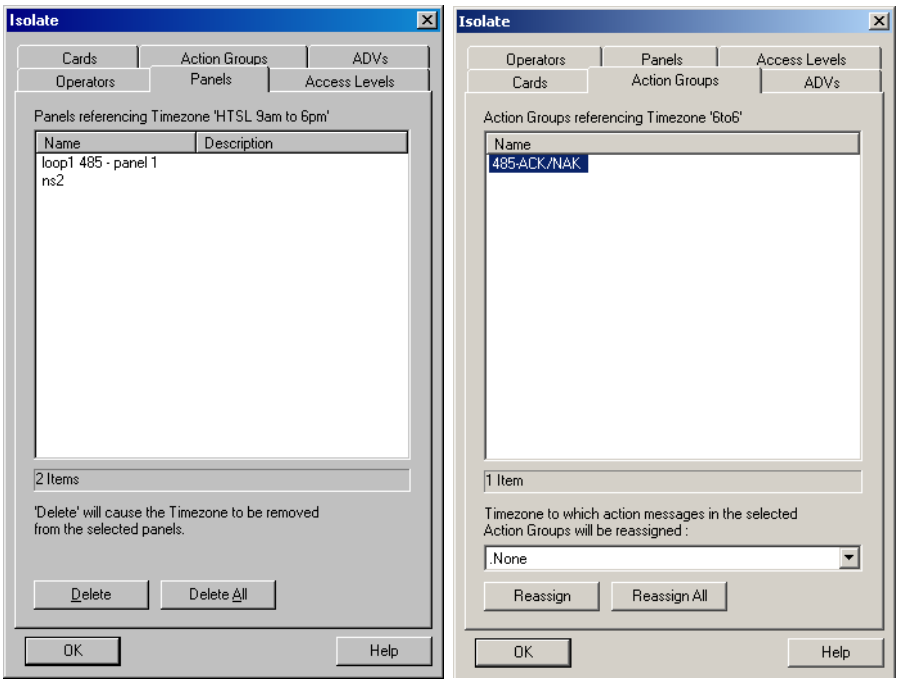
Isolating and Deleting a Time Zone

Time Zones are used in many places throughout the access control system. Therefore, to delete a time zone, you must isolate the time zone from any panel, operator, or access level it is assigned to.

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:

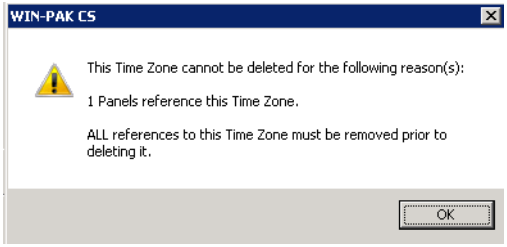
   a. Select the device from the list of devices.

   b. Select the alternate time zone from the drop-down list.

   c. Select **None** from the drop-down list to dissociate the device from time zones.

   d. 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.



6. 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.

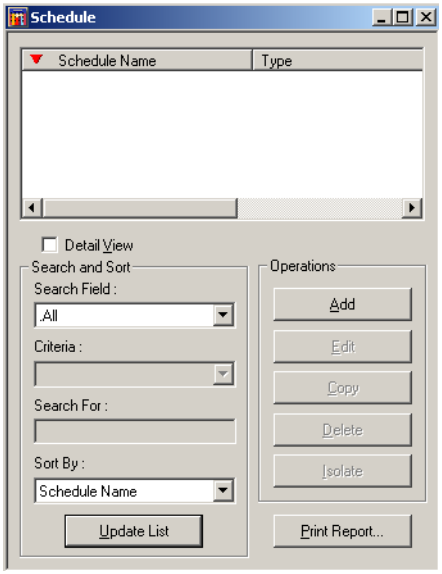
Schedule

You can schedule tasks to run automatically at a defined time. Tasks common to accounts can be scheduled in the System account. To schedule a task for a specific account, select the account before creating the schedule.

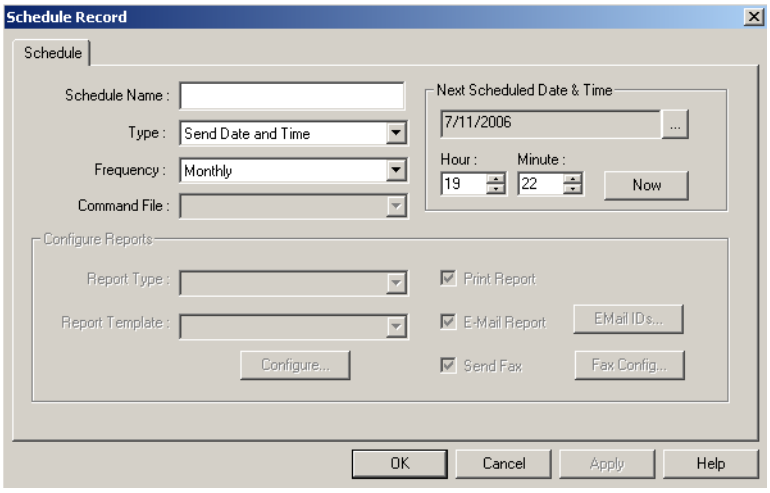
Scheduling a Task in WIN-PAK CS

To schedule a task in WIN-PAK CS:

1. Choose **Configuration > Time Management > Schedule**. The **Schedule** window appears.



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 in the dialog box may be activated.

   The Task types include:

   - **Activate and Deactivate Cards**: Activates or deactivates cards depending on the card activation and deactivation dates. This helps update the card details in the panel.
   - **Dial Remote Area**: Establishes a dial-up connection between the WIN-PAK CS systems and devices and sends commands to the remote communication loop, panel or P-Series panel.
   - **Run Command File**: This schedule runs a command file at a specific time in a defined frequency.
   - **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 CS.
   - **Update Custom Access Level**: Updates custom access level of cards in the panels at a defined frequency.

   See 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:

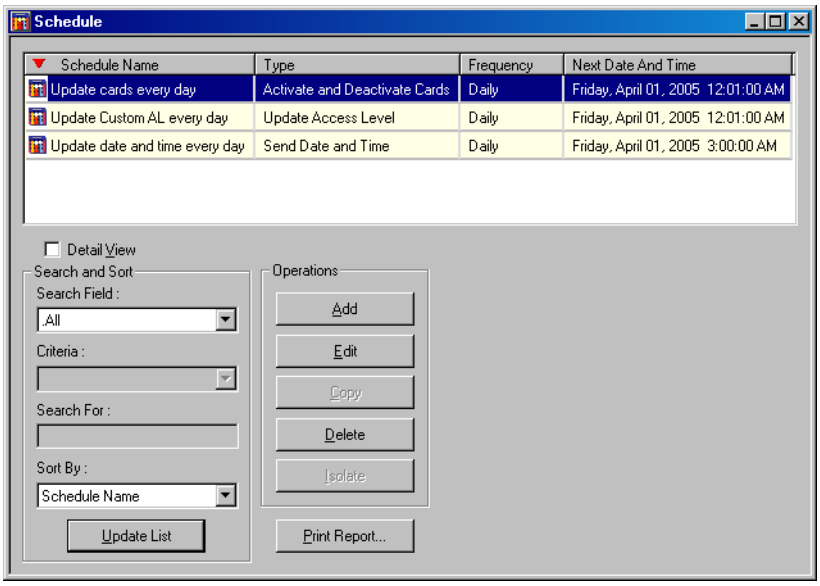
- To select the date, click the ellipsis button and select a date in the calendar.

- 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**.

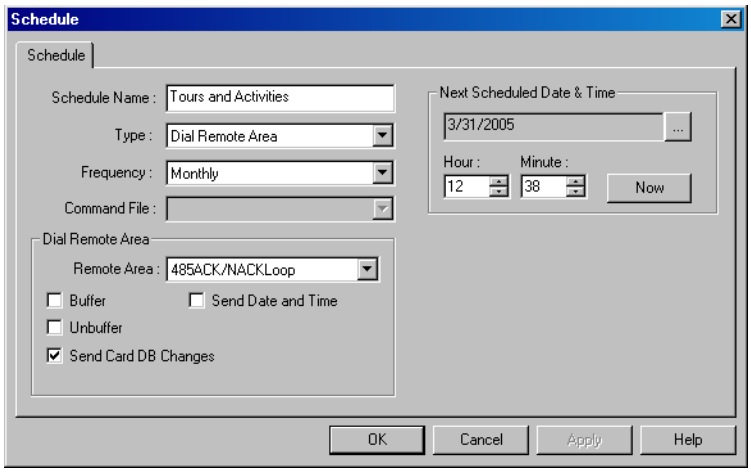
Scheduling a Task in WIN-PAK SE/PE

To schedule a task in WIN-PAK SE/PE:

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 are 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.
- Backup Database: This schedule takes a backup of the database in a defined interval such as daily, monthly, weekly, and so on.
- **Card Frequency Report**: Generates the card frequency report in a defined interval.
- **Dial Remote Area**: Establishes the dial-up connection between WIN-PAK SE/PE systems and sends the command to the panel.
- **Purge History**: Enables you remove the history details. You can also remove the deleted records of the panels.
- **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 SE/PE.
- **Send Holidays**: Sends the holidays list to all the panels attached to WIN-PAK SE/PE.
- **Update Custom Access Level**: Updates custom access level of cards in the panels at a defined frequency.

See the Task Type section in this chapter, for more details on task types and scheduling a task.In the **Frequency** list, select how often the task is to be performed.

5. Under **Next Scheduled Date and Time**, select the date and enter the time (in hours and minutes) for the task to be performed.

- 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 Record** dialog box, a different set of options appear. This section describes the task types and guides you with scheduling a task for each task type.

Note: WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

The Schedule Task Types are as follows:

Task Type	WIN-PAK CS	WIN-PAK SE/PE	Go To
Activate and Deactivate Cards	✓	✓	page 308
Dial Remote Area	✓	✓	page 308
Run Command File	✓	✓	page 311
Run Report	✓	✓	page 312
Send Date and Time	✓	✓	page 313
Update Custom Access Level	✓	✓	page 314
Backup Database		✓	page 315
Card Frequency Report		✓	page 317
Purge History		✓	page 320
Run Guard Tour		✓	page 321
Send Holidays		✓	page 321

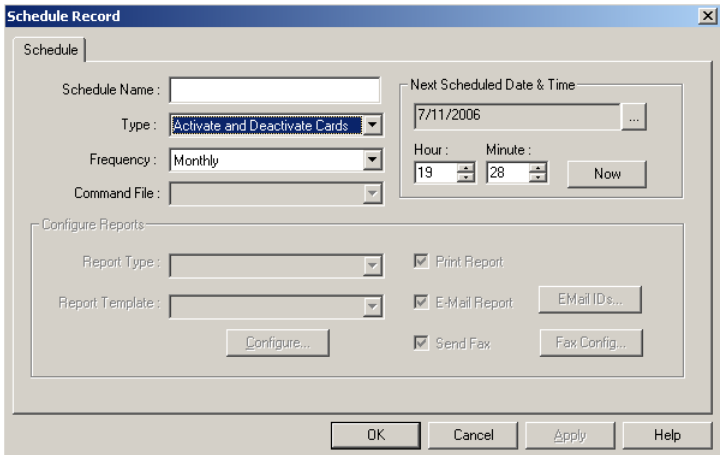
Note: Run Command File and Run Report are the only task types that can be scheduled for the System account.

Activate and Deactivate Cards

Select this task type to schedule a task for activating and deactivating 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. Type the name of the schedule in the **Schedule Name** box.
2. Select how often the task is to be performed from the **Frequency** list.



3. Under **Next Scheduled Date and Time**, select the date and enter the time (in hours and minutes) for the task to be performed.

- To select the date, click the ellipsis  button and select the date in the calendar.
- To enter the time, type the **Hour** and **Minute** button. The hour ranges from 0 to 23 minute ranges from 0 to 59.
- To enter the current date and time, click **Now**.

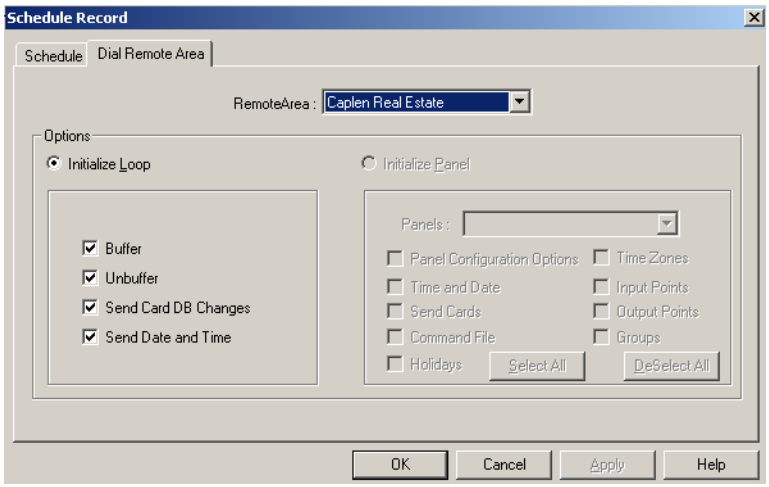
4. Click **OK** to save the schedule.

Dial Remote Area

Select **Dial Remote Area** as the task type, to schedule the task of sending commands to a remote panel or loop, through the modem. You can initialize a loop or a panel through the remote dialing schedule.

Notes:

- In WIN-PAK CS the **Dial Remote Area** tab automatically appears in the **Schedule Record** dialog box.
- In WIN-PAK SE/PE the **Dial Remote Area** box is enabled on the lower-right corner of the Schedule dialog box.



In addition to the basic steps, perform the following steps for scheduling a task:

1. In the **Schedule Record** dialog box, click the **Dial Remote Area** tab.
2. Select the **RemoteArea** from the list. The selected remote area can include a remote loop, panel or a remote P-Series panel. The options displayed for each device are different.
3. Select **Initialize Loop** to send commands to a remote communication loop.
    - Select the following commands to be sent to the loop:

Option	Description
Buffer	If you want the loop to store the task data in the loop's buffer.
Unbuffer	If you want the loop to send the stored data to the WIN-PAK CS/SE/PE system.
Send Card DB Changes	If you want the WIN-PAK CS/SE/PE system to send the updated card details to the panel.
Send Date and Time	If you want the WIN-PAK CS/SE/PE system to send the system date and time to the panel.

Note: Step 4 and 5 is applicable only for WIN-PAK CS.

4. Select **Initialize Panel** to send commands to a remote panel.
    a. Select the panel from the **Panels** list.

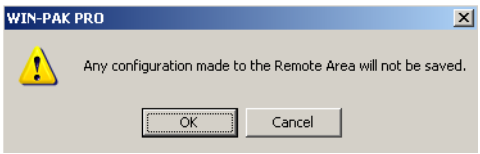
b. Select the following commands to be sent to the panel:

Option	Description
Panel Configuration Options	If you want the panel configuration options to be sent to the panel.
Time and Date	If you want the WIN-PAK CS system to send the system date and time to the panel.
Send Cards	If you want the WIN-PAK CS system to send the system date and time to the panel.
Command File	If you want the WIN-PAK CS system to send the command file information to the panel.
Holidays	If you want the WIN-PAK CS system to send the holiday settings to the panel.
Time Zones	If you want the WIN-PAK CS system to send the time zone settings to the panel.
Input Points	If you want the WIN-PAK CS system to send the input point settings to the panel.
Output Points	If you want the WIN-PAK CS system to send the output point settings to the panel.
Groups	If you want the WIN-PAK CS system to send the group settings to the panel.

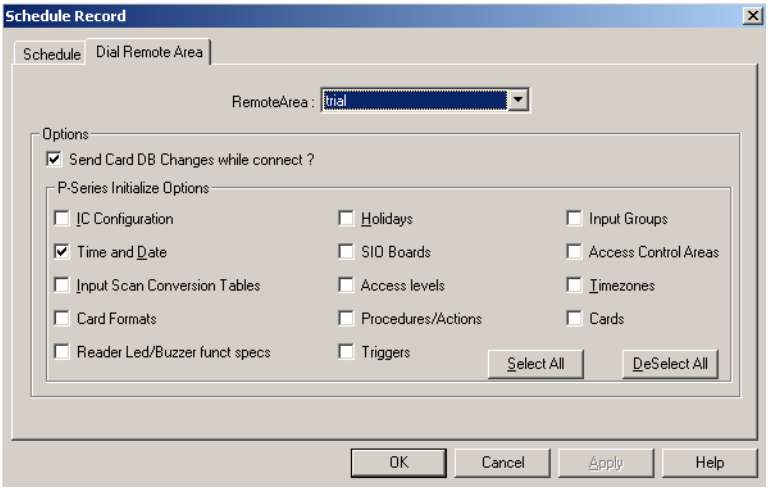
c. Click **Select All** to select all the command check boxes.

d. Click **DeSelect All** to clear all the command check boxes.

5. For a P-Series panel, the following message appears:



Click **OK** to view the P-Series panel initialization options.



a. Select the **Send Card DB Changes while connect** check box to send the updated database information to the panel, during the connection.

b. The following information can be sent to the P-Series panel:

   – IC Configuration
   – Time and Date
   – Input Scan Conversion Tables
   – Card Formats
   – Reader Led/Buzzer funct specs
   – Holidays
   – SIO Boards
   – Access Levels
   – Procedures/Actions
   – Triggers
   – Input Groups
   – Access Control Areas
   – Timezones
   – Cards

c. Click **Select All** to select all the command check boxes.

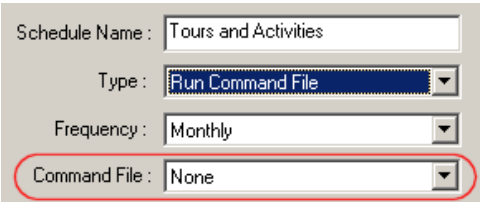
d. Click **DeSelect All** to clear all the command check boxes.

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

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.



In addition to the basic steps, perform the following steps for scheduling a task:

1. In the **Schedule Record** dialog box, select a command file in the **Command File** list. The command files available in WIN-PAK CS/SE/PE are listed.
2. Click **OK** to save the schedule.

Run Report

Select **Run Report** as a task type, to generate a report at a defined interval. You can select from a list of reports available in WIN-PAK CS. In addition, the reports configured in Report Templates can be executed.

When you select this task type, the **Configure Reports** frame appears in the lower end of the **Schedule Record** dialog box.

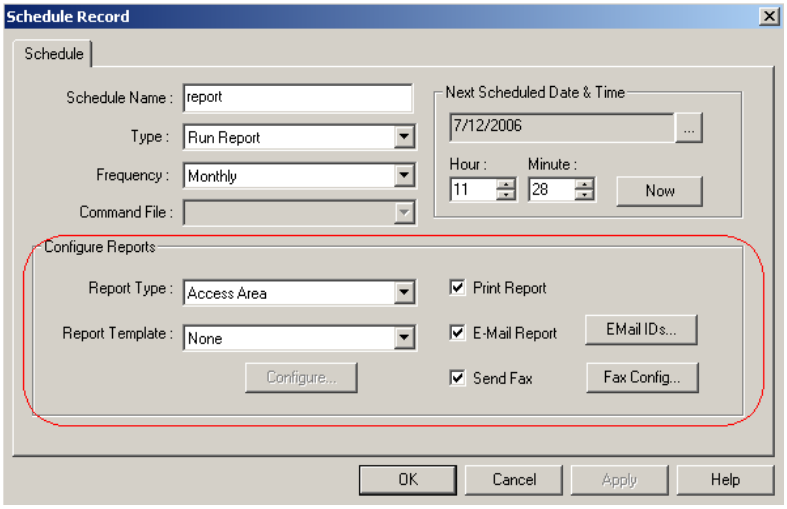
In addition to the basic steps, perform the following steps for scheduling a task:

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 **Configure** to edit the report template configuration. The **Report - Card Holder** or **Report - History** dialog box appears.

   See 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 addresses after configuration.
6. Click **EMail IDs** to compose the e-mail for sending the report. The **Send Email** dialog box appears.

Notes:

- For WIN-PAK CS, see the "Sending the report as an e-mail" section for more details on sending reports as e-mails.
- For WIN-PAK SE/PE, follow the below steps:

    a. 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.

    a. 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.

- Step 7 and 8 is applicable only for WIN-PAK CS.

7. Select the **Send Fax** check box to fax the report to the selected fax recipient.
8. Click **Fax Config** to specify the fax information. The **Send Fax** dialog box appears.

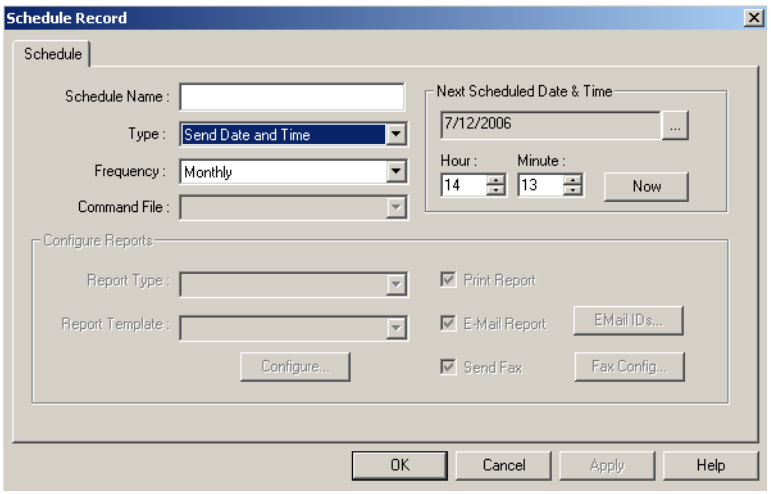
   See the "Faxing the report" section for more details on faxing reports.
9. Click **OK** to save the schedule.

Send Date and Time

Select the **Send Date and Time** task type to update the panel date and time with the system timing. This task is scheduled by default.

If you select this type, perform the following steps:

1. In the **Schedule Record** 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**.

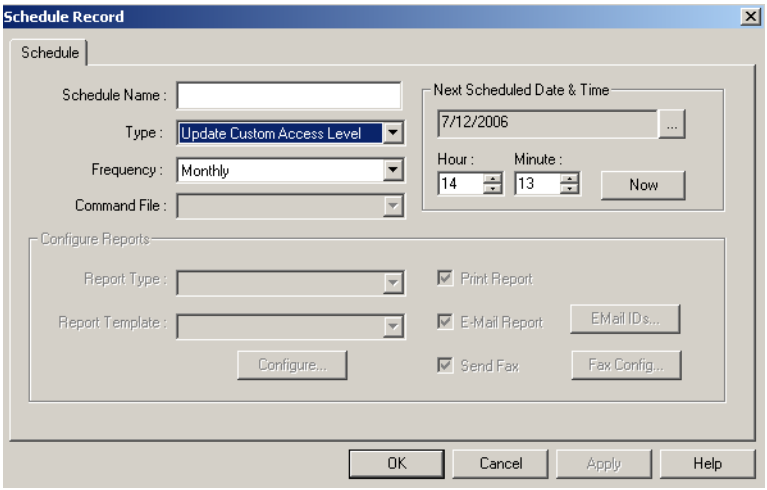
3. Click **OK** to save the schedule.

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 Record** 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**.

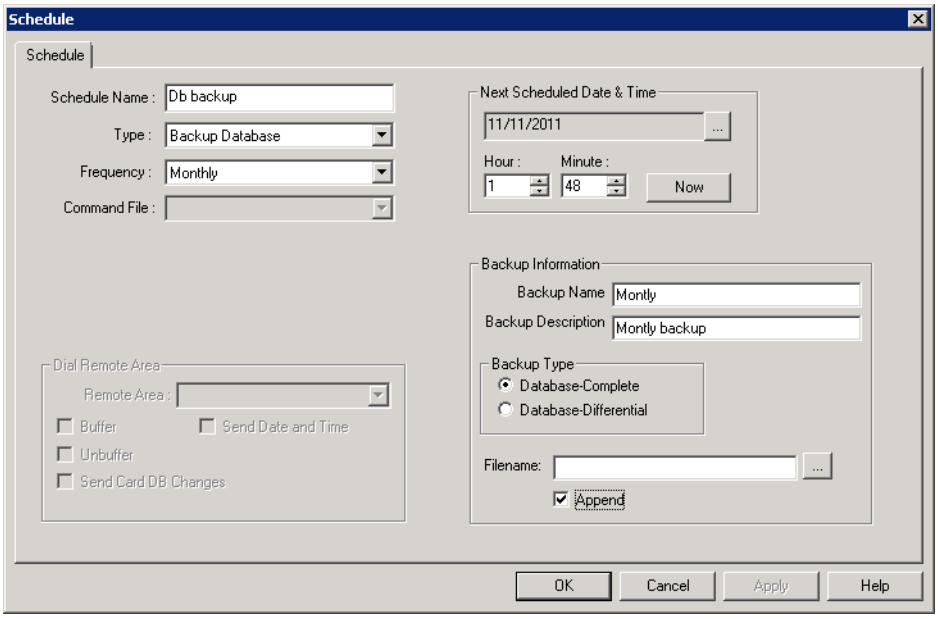
3. Click **OK** to save the schedule.

Backup Database

Select this task type to backup the database on a daily, weekly, bi-weekly, hourly, and monthly basis.

If you select this type, perform the following steps:

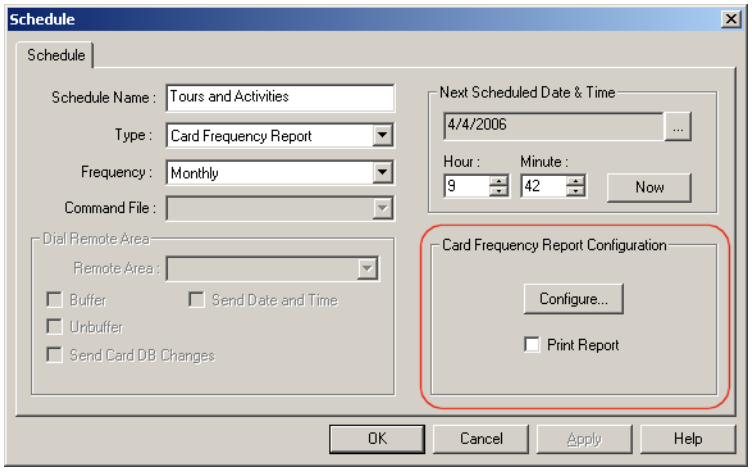
1. In the **Schedule** dialog box, select how often the task is to be performed (Monthly, Once per two weeks, Weekly, Daily, Hourly) in the **Frequency** list.



2. Under **Next Scheduled Date and Time**, select the date and enter the time (in hours and minutes) for the task to be performed.
    - 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. Under **Backup Information**
    - Type the **Backup Name**.
    - Type the **Backup Description**.
    - Select **Database - Complete** or **Database - Differential** as the **Backup Type**.
    - Click . The **Save As** dialog box appears.
        - Select an existing .bak file to overwrite the contents with the new data or type a new **File Name** to save the data to a new file.
        - Click **Append** to append the data that is backed up to contents of selected .bak file.
4. Click **OK** to save the schedule.

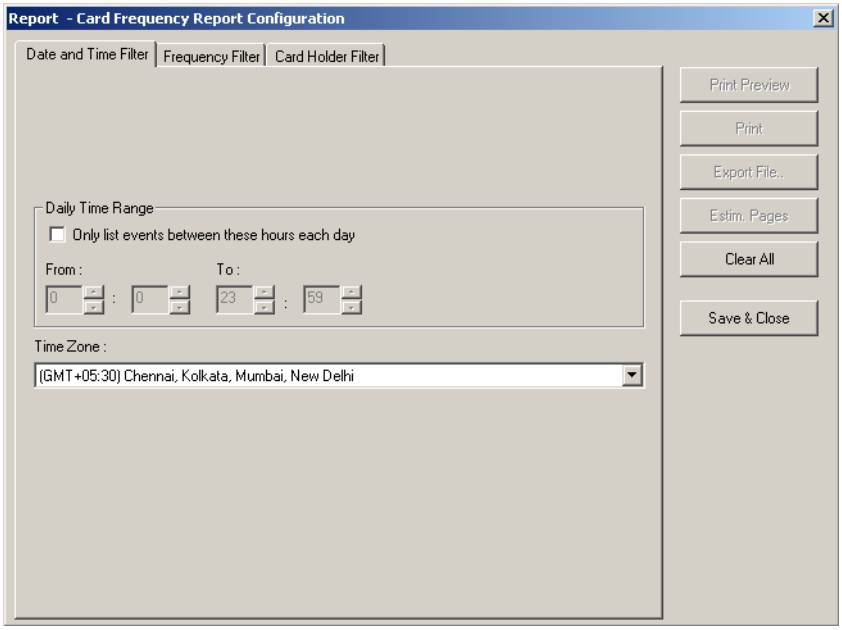
Card Frequency Report

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.



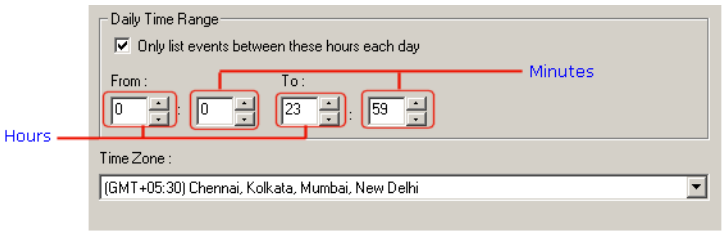
In addition to the basic steps, perform the following steps for scheduling a task:

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.

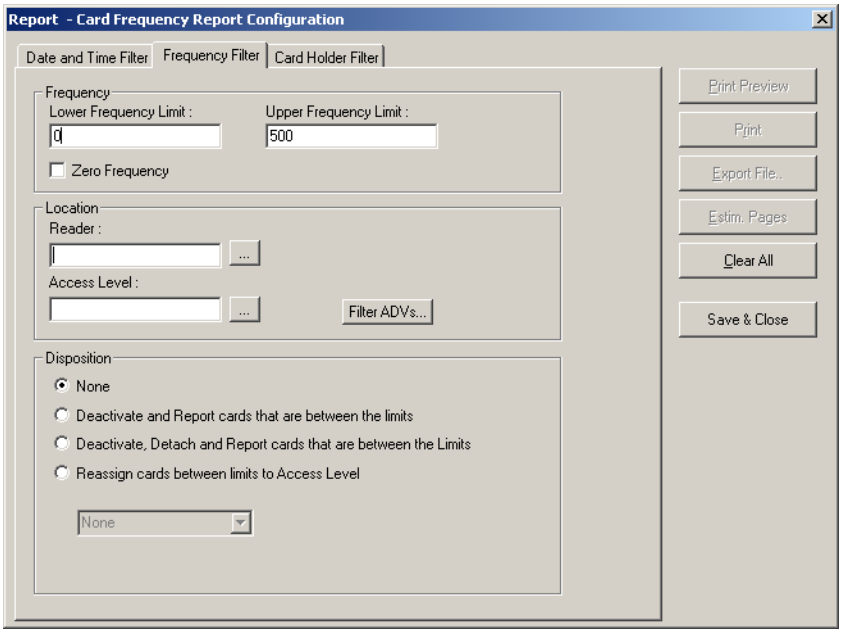
    a. To generate reports for events occurring during the specified period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The **From** and **To** text boxes are enabled.



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.



4. Under **Frequency**, type the **Lower Frequency Limit** and **Higher Frequency Limit** to filter the cards between these limits.

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:

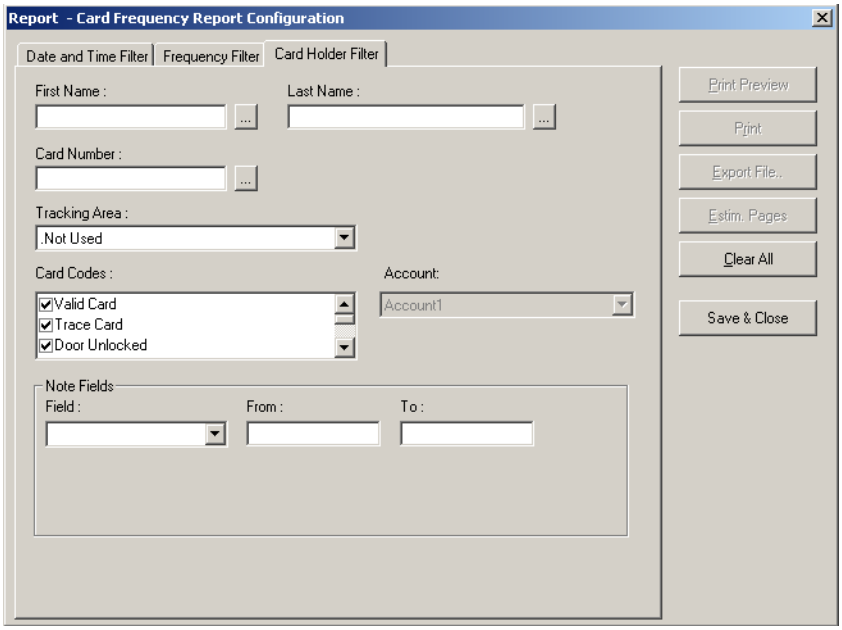
a. **None**: Perform no action on the cards.

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.

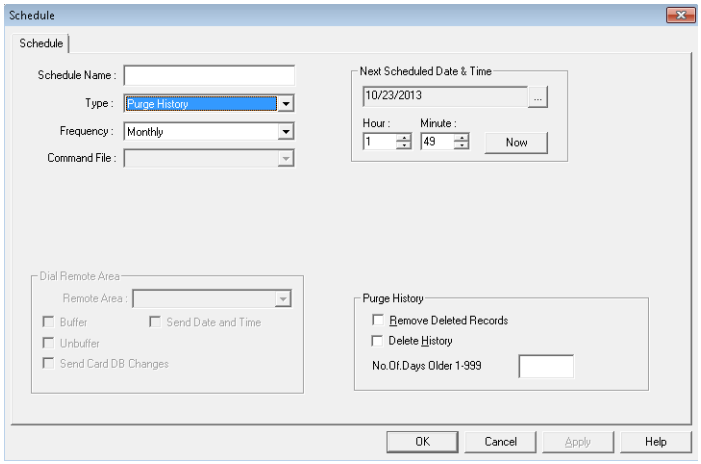
Purge History

Select Purge History as the task type and specify the days for which the history must be removed. You can also remove the deleted records of the panels.

If you select this type, the **Purge History** box is enabled on the lower-right corner of the **Schedule** dialog box.

In addition to the basic steps, perform the following steps for scheduling a task:

1. In the **Schedule** dialog box, select the **Type** as **Purge History**.



2. Select the following commands to be sent to the panel:

Option	Description
Remove Deleted Records	Select this option to remove the deleted records of the panels. **ATTENTION**: The records are permanently removed from the database and cannot be recovered.
Delete History	Select this option and specify the days for which you want the history to be removed.

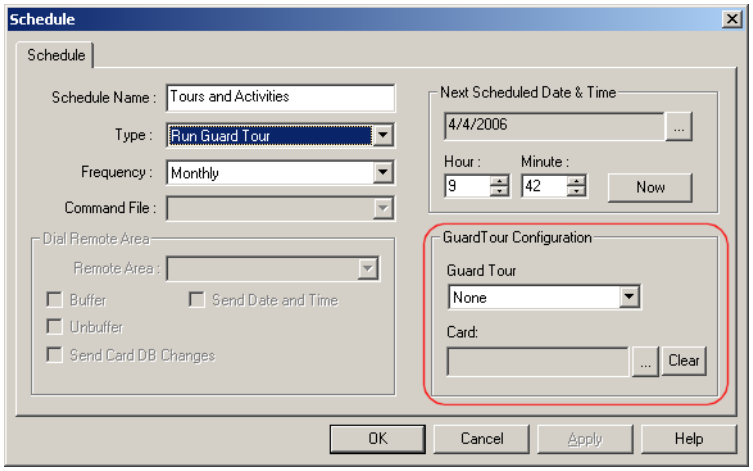
3. Type the days for which the history must be removed in the **No. Of Days Older 1-999** box.
4. Click **OK** to save the changes.

Run Guard Tour

Select **Run Guard Tour** as a task type, if you want to run a guard tour at a defined interval.

See the *Guard Tour Server*, page 352 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.



In addition to the basic steps, perform the following steps for scheduling a task:

1. In the **Schedule** dialog box, under **GuardTour Configuration**, select the guard tour in the **Guard Tour** list.
2. To select the card attached to the card holder (guard), click the ellipsis button and select the card.

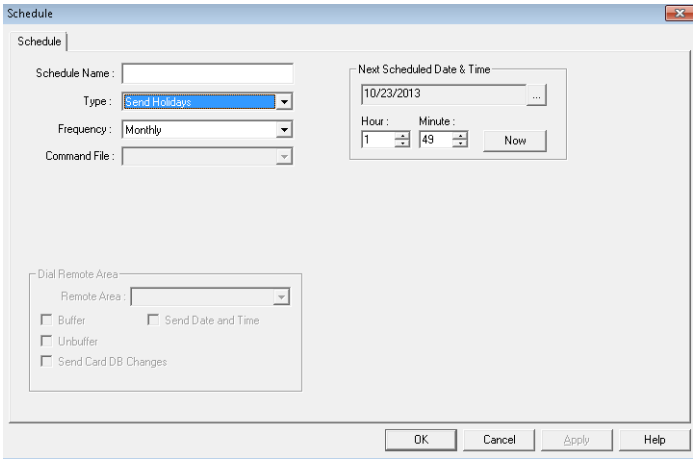
   If you want to remove the card, click **Clear**.
3. Click **OK** to save the schedule.

Send Holiday

Select **Send Holidays** type to send the holidays list to all the panels attached to WIN-PAK CS/SE/PE.

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.
    - 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.

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 CS/SE/PE.
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 CS/SE/PE.
3. Click **Delete**. The selected schedule is deleted.

Holiday Group

Holiday group is a set of holiday definitions. For example, you can group holidays like Christmas, Thanksgiving, and Independence Day which occur on the same date every year into a Holiday group. Holiday Groups are useful for grouping departments which would close and others which would remain open, on holidays.

Each account has its own set of holidays. However, holidays common to accounts can be configured in the Holiday Master list from where it can be added to holiday groups for multiple accounts. The Holiday Group option is not available to the System account.

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.

Note: For WIN-PAK CS, see the "Panel Configuration" section for details on assigning holiday groups to panels.

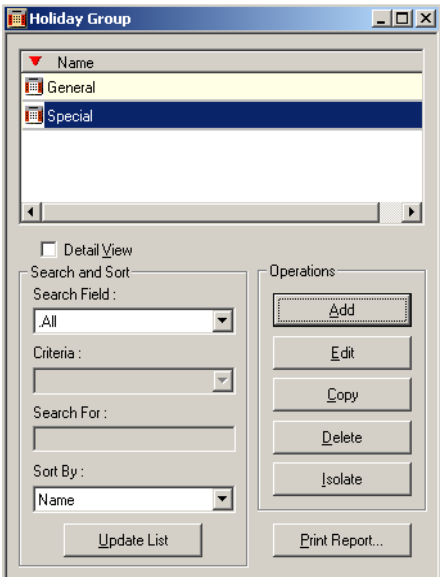
Associating Holiday Groups and Time Zones

When Time Zones and a Holiday Group are assigned to a panel, the start and end times for the H1, H2 and H3 time slots are applicable to the Holiday Group.

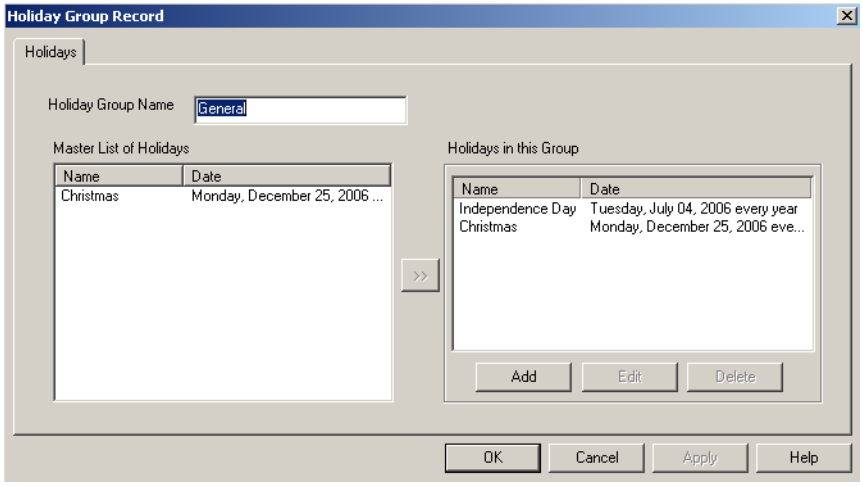
Adding a Holiday Group

To add a holiday group:

1. Select the account to which the holiday group is to be added. See "Selecting an Account" for more information on selecting an account.
2. Choose **Configuration > Time Management > Holiday Group**. The **Holiday Group** window appears.



3. Click **Add** to add holidays to the holiday group. The **Holiday Group Record** dialog box appears.



4. Type the **Holiday Group Name**. For example, Federal Holidays.

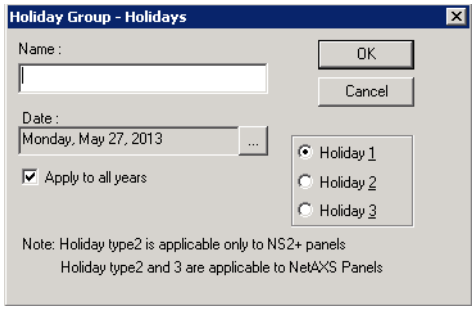
Note: In WIN-PAK CS follow the below steps to add a holiday from the holiday master list to the holiday group:

a. Select the required holiday from the **Master List of Holidays** to add a holiday common across accounts to this holiday group.

b. Click the move one >> button to add the holiday to the **Holidays in this Group** list. The selected holiday appears in the list.

c. Repeat the previous steps to add more holidays from the holiday master list to the holiday group.

5. Click **Add**. The **Holiday Group - Holidays** dialog box appears to add a list of holidays in the holiday group.



6. Type the **Name** of the holiday.
7. Click the ellipsis button to select the date.
8. Select the **Apply to all years** check box, if the holiday must recur every year.
9. Select the holiday category as **Holiday 1** or **Holiday 2** or **Holiday 3**. The holiday groups are grouped into two major categories as Holiday 1, Holiday 2, and Holiday 3. 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 this holiday category. Holiday 2 category and Holiday 3 category is applicable for NetAXS panels.

10. Click **OK** to save the holiday.
11. Repeat steps 5 to 10 for adding more holidays to the holiday group.
12. After adding the required holidays, click **OK** to save the **Holiday Group** settings.

Editing a Holiday Group

To edit a holiday group:

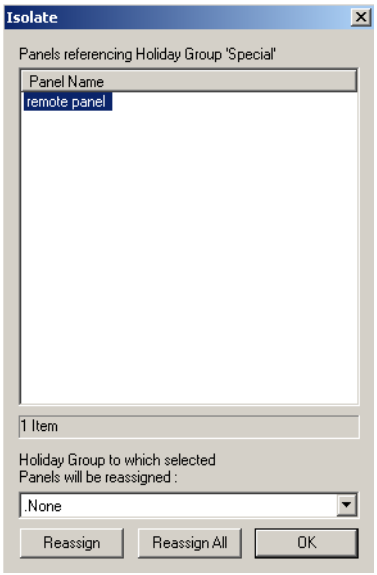
1. Choose **Configuration > Time Management > Holiday Group**. The **Holiday Group** window appears with the list of existing holiday groups.
2. Select a holiday group from the list.
3. Click **Edit**. The **Holiday Group Record** dialog box appears.
4. Change the required details.
5. If you want to 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 locations where the standard daylight saving group is not used. These daylight saving groups are attached to panels so that they use custom timings.

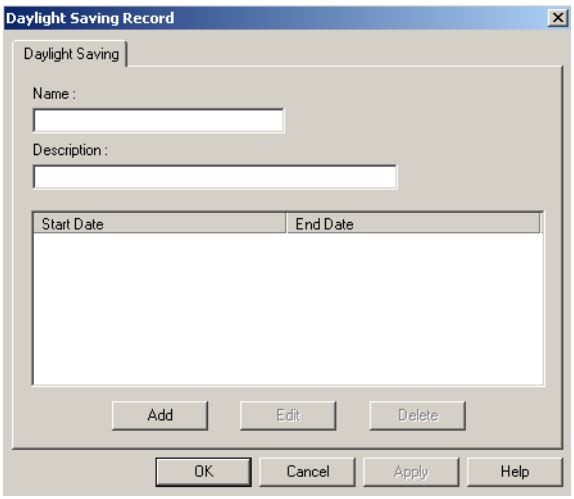
Note: The Daylight Saving Group is applicable only to P-Series Panels (PRO-2000 Intelligent Controller). See the "Adding a P-Series Panel" section for assigning a daylight saving group to a P-Series panel.

For the P-Series panels, you must ensure to setup the Daylight Saving Group before the start of Daylight Saving Time (DST). After setting up the DST, you need to apply the settings to the panels and initialize the panels.

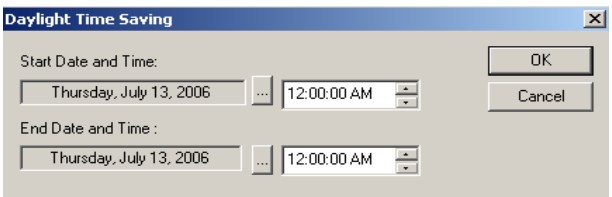
Adding a Daylight Saving Group

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.

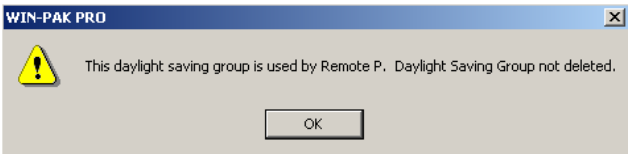
Deleting a Daylight Saving Group

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:



4. Click **OK** to close the message box.

Holiday Master

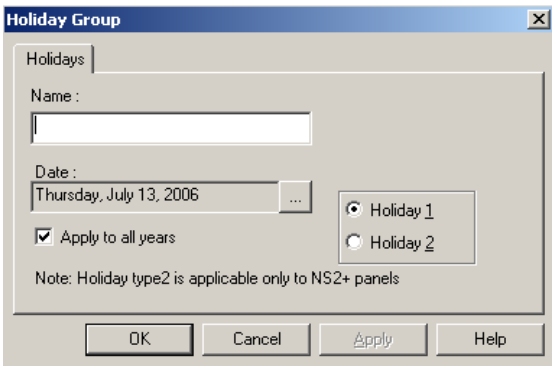
Holidays common across accounts can be added to the Holiday Master list. You can select holidays from this list and add them to a Holiday Group. This avoids re-entering holiday information for each account.

Note: This section is applicable only for WIN-PAK CS.

Adding a Holiday to the Holiday Master

To add a holiday to the holiday master:

1. Choose **Configuration > Time Management > Holiday Master**. The **Holiday Master** window appears.
2. Click **Add**. The **Holiday Group** dialog box appears.



3. Type a **Name** for the holiday master.
4. To set the date:
   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.
5. Select the **Apply to all years** check box, if the holiday must recur every year.
6. Select the holiday category as **Holiday 1** or **Holiday 2 or Holiday 3**. The holiday groups are grouped into three major categories as Holiday 1, Holiday 2

and Holiday 3. You can use these categories to group the mandatory holidays and optional holidays.

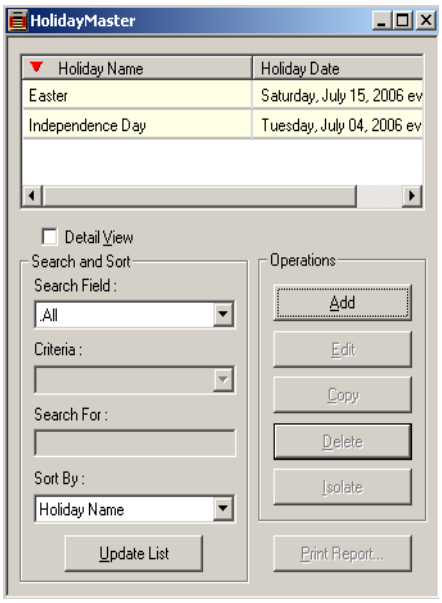
Note: Holiday 2 category is applicable only for NS2+ panel types, as other panels do not support this holiday category.

7. Click **OK** to save the holiday or the changes made to a holiday.
8. Repeat steps 1 to 7 to add more holidays to the holiday master.

Editing a Holiday in the Holiday Master

To edit a holiday:

1. Choose **Configuration > Time Management > Holiday Master**. The **Holiday Master** window appears with the list of existing holidays.



2. Select a holiday from the list.
3. Click **Edit**. The **Holiday Group** dialog box appears.
4. Change the required details.
5. If you want to add a holiday to the holiday master, click **Add** and follow the same procedure as in "Adding a Holiday to the Holiday Master" .
6. Click **OK** to save the changes.

Deleting a Holiday from the Holiday Master

To delete a holiday:

1. Choose **Configuration > Time Management > Holiday Master**. The **Holiday Master** window appears with the list of existing holidays.
2. Select a holiday from the list.

3. Click **Delete**. The selected holiday is deleted from the holiday master.

WIN-PAK CS/SE/PE Servers and Devices

9

In this chapter...

This chapter gives an introduction to the WIN-PAK CS/SE/PE Servers and Devices, Server Configuration, Ethernet Module (Galaxy Panel), Device Configuration, Communication Loops, Vista Panel Port (Home Automation Mode), Video Management System, Recorder Configuration, Panel Configuration, Abstract Devices, and Action Group in WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
485/PCI Panel Loop, page 387	✓	✓
RS-232 Panel Loop, page 392	✓	✓
P-Series Panel Loop, page 397	✓	✓
C-100 or 485 (non-ACK/NAK) Remote Communication Loop, page 401	✓	✓
485 ACK-NAK Remote Communication Loop, page 405	✓	✓
CCTV Switcher, page 410		✓
RS-232 Connection, page 415		✓
Modem Pools, page 418	✓	✓
Add a Vista Panel Port, page 424	✓	✓
Add or Edit a Vista Panel, page 426	✓	
Configuring the vista panel partitions, page 427	✓	
Configuring vista panel zones, page 427	✓	
Configuring the vista panel outputs, page 429	✓	
Defining user codes, page 429	✓	
Editing a Vista Panel, page 430		✓
Isolating and deleting a Vista Panel, page 431		✓
Adding a Video Management Server, page 433	✓	✓
Editing a Video Management Server, page 435	✓	✓
Connect, page 435	✓	✓
Synchronize Event Types, page 436	✓	✓
Deleting Video Management Server, page 436	✓	✓

Section	WIN-PAK CS	WIN-PAK SE/PE
Adding a Recorder, page 437	✓	✓
Associating Events and Event Attributes to a Recorder, page 440	✓	✓
Editing a Recorder, page 444	✓	✓
Recorder Input Configuration, page 444	✓	✓
Connect an Alarm Input to a Recorder, page 445		✓
Edit Input Settings, page 446	✓	✓
Delete Inputs, page 446	✓	✓
To Add/Delete bulk ADV, page 447	✓	✓
Recorder Output Configuration, page 447	✓	✓
Connecting a relay to the recorder, page 448	✓	✓
Edit Output Settings, page 448	✓	
Delete Outputs, page 448	✓	
To Add/Delete bulk ADV, page 449	✓	
Connect an alarm input to a recorder, page 449	✓	
Connect relay to a recorder, page 449	✓	
Deleting a Recorder, page 450	✓	
Associating events and event attributes to a recorder, page 450	✓	
Discover Devices, page 451	✓	
General Settings, page 452	✓	✓
PTZ Settings, page 456	✓	✓
Recording Settings, page 457	✓	✓

Section	WIN-PAK CS	WIN-PAK SE/PE
Adding an N-1000/PW-2000 Panel, page 458	✓	✓
Adding a NetAXS Panel, page 475	✓	✓
Adding an NS2+ Panel, page 481	✓	✓
Adding or Editing a NETAXS Panel, page 495	✓	✓
Setting the card format for NetAXS panels, page 499	✓	✓
Assigning time zones and holiday groups to a NetAXS panel, page 501	✓	✓
Setting the NetAXS panel options, page 502	✓	✓
Configuring input points to the NetAXS panel, page 505	✓	✓
Configuring output points to the NetAXS panel, page 508	✓	✓
Configuring groups to the NetAXS panel, page 511	✓	✓
Configuring a reader to the NetAXS panel in WIN-PAK CS, page 513	✓	
Configuring Readers to the NetAXS panel in WIN-PAK SE/PE, page 522		✓
Adding downstream devices, page 527	✓	✓
Adding downstream NetAXS4 panels to a NetAXS-4 Gateway panel, page 528	✓	✓
Adding downstream NetAXS-123 panels or NetAXS-4 panels to a NetAXS-3 Gateway panel, page 529	✓	✓
Interlocking, page 531	✓	✓
Adding a P-Series Panel, page 532	✓	✓
Adding a FIN4000 Panel for WIN-PAK SE/PE, page 560		✓

Section	WIN-PAK CS	WIN-PAK SE/PE
Adding P-Series Panel in Modem Pool for WIN-PAK SE/PE, page 581		✓
Adding a PRO3000 Panel, page 584		✓
Adding a Remote P-Series Panel, page 594	✓	✓
Configuring an Abstract Device, page 598	✓	✓
ADV Action Groups, page 607	✓	✓
Initializing Panels, page 642	✓	✓

Introduction

The chapter **WIN-PAK CS/SE/PE Servers and Devices** describes how to configure servers and then add devices such as loops, panels, and so on, which includes adding abstract devices and action groups.

In WIN-PAK CS the entire process can be categorized into the following groups:

1. **Server Configuration**: Servers and modem pools, common across accounts, are configured in **Server Configuration**.
2. **Device Configuration**: Direct and remote communication loops, panels and digital video devices are configured in the **Device Map**. The devices configured here are specific to an account and each account can have a unique Device Map structure.

Note: The configured devices are common to all accounts.

Server Configuration

In the **Server** tree structure, all the Servers form the high level nodes of the tree.

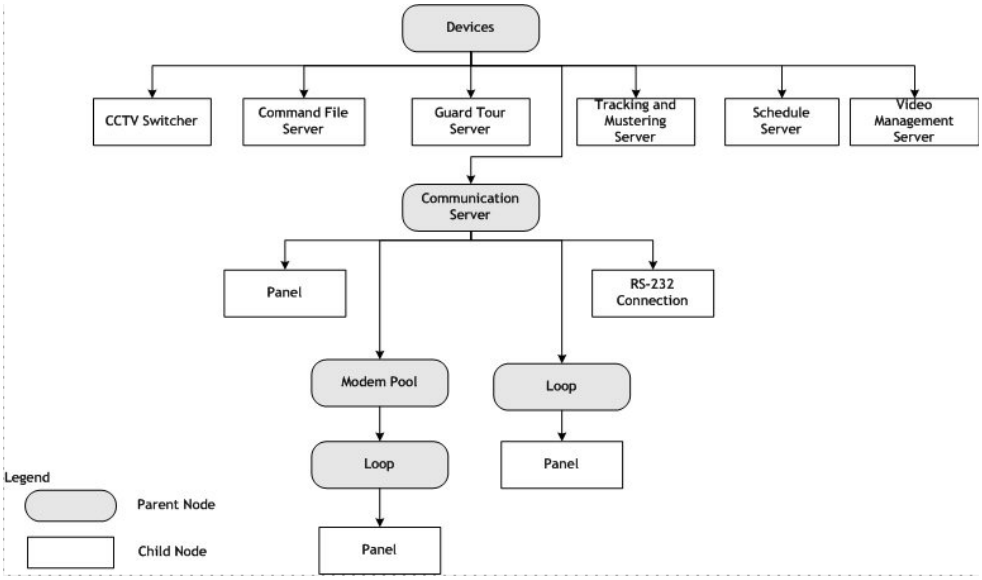
The following is the list of device types in WIN-PAK CS that can be added to the Device Map.

- Communication Server
- Command File Server
- Schedule Server
- Guard Tour Server
- Tracking and Muster Server
- API Server
- Video Management Server

The following is the list of device types in WIN-PAK SE/PE that can be added to the Device Map.

- Servers
- Communication Servers
- Communication Loops
- Panels
- Digital Video Recorder (DVR)
- Abstract Devices

Modem pools can be added to the Communication Server to enable remote communication between panels and WIN-PAK CS. The following figure depicts the structure for server configuration.



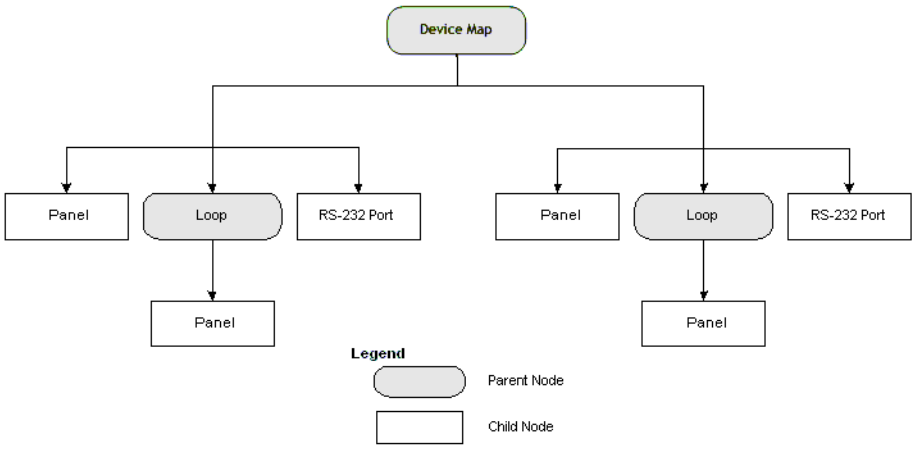
Device Configuration

The Device Map in WIN-PAK CS is a graphical tree structure that represents the physical connections of the devices. The Devices include communication hardware, panels, readers, and digital video equipment. The following is the list of device types that can be added to the Device Map:

- Communication Loops
- Panels
- Digital Video equipment
- Abstract Devices

In the Device Map tree structure, within the Devices folder, Communication Loops form the high level nodes of the tree. A Communication Server must be added in the Server tree to add loops, modem pools and also direct connections to the P-Series panels in the Devices folder.

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:



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 CS/SE/PE.

Servers and Devices

WIN-PAK CS has different servers to perform different tasks. The following is the list of servers in WIN-PAK CS/SE/PE for handling different functions:

Database Server

The WIN-PAK CS/SE/PE 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 CS/SE/PE UI, it is sent to the Database server to update the data in the SQL database.

Archive Database Server

The WIN-PAK CS/SE/PE 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 CS/SE/PE or other servers. Therefore, the servers must request the communication server to interact with panels.

Command File Server

The WIN-PAK CS/SE/PE 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 CS/SE/PE 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 CS/SE/PE 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.

API Server

Note: API Server is applicable only in WIN-PAK CS.

This component is installed by default only when the Web option is selected during installation, and is suitable for web installations.

The API servers are of two types:

- **Communication Server API**: The Communication Server API enables you to create a customized Windows client application to monitor and act on the events/alarms using the WIN-PAK CS UI.
- **Database API**: The Database Server API enables you to create a Windows client application which allows you to set and retrieve data from the WIN-PAK CS database.

Video Management Server

The Video Management Server (VMS) is an enterprise-class video management and storage solution. It is a truly hybrid solution which, enables you to operate the traditional analog and the network and IP based video equipment in the same surveillance network.

You can deploy thousands of cameras in number of locations, and add many video devices such as recorders and monitors.

To set the Video Management Server, you must:

1. Add or Edit Video Management Server. See ‘Adding a Video Management Server’ and ‘Editing a Video Management Server’.

2. Connect the Video Management Server. See ‘Connect’.
3. Synchronize Video Management Server. See ‘Synchronize Event Types’.
4. Add Recorder. See ‘Recorder Configuration’, ‘Camera Configuration’, ‘Recorder Input Configuration’, and ‘Recorder Output Configuration’.
5. Delete Video Management Server. See ‘Deleting Video Management Server’.

Interacting with Cameras

In WIN-PAK CS/SE/PE, the monitoring and viewing of live and recorded videos for a selected area is possible using Video Management Server. This version of WIN-PAK CS/SE/PE supports an enhanced level of integration with the Fusion, HRDP Performance DVRs, RapidEye DVRs, and MaxproNVRs.

The integration enables you to configure various advanced settings for the cameras using WIN-PAK CS/SE/PE after some basic configuration in the DVR software. In addition, you can select the DVRs to be monitored and track actions captured by them (both live and recorded) along with the alarms and notifications.

Interacting with Intrusion Panels

Note: This section is applicable only in WIN-PAK PE.

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.

Note: Intrusion integration is available only with the licensed version of WIN-PAK PE.

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.
2. Add these readers and input points to the access area.
3. Assign access levels for these readers and input points.
4. Add 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.

Server Configuration

Servers and Modem Pools are configured in using **Server Configuration** in WIN-PAK CS/SE/PE.

Servers establish the communication between various WIN-PAK CS/SE/PE devices and databases. This section explains how to set up the servers and modem pools.

Note: The servers you configure are common to all the accounts.

Communication Server

The Communication Server establishes the connection between WIN-PAK CS/SE/PE and the panels that are physically located in the access control system. The communication server must be configured in the WIN-PAK CS/SE/PE Server Configuration tree for the WIN-PAK CS/SE/PE system to communicate with the system devices including the P-Series Intelligent Controller.

Multiple communication servers can be configured for WIN-PAK CS/SE/PE in a networked environment. This speeds up the communication when many devices are involved. However, it depends on the type of WIN-PAK CS/SE/PE license availed.

Note: WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

Adding a Communication Server

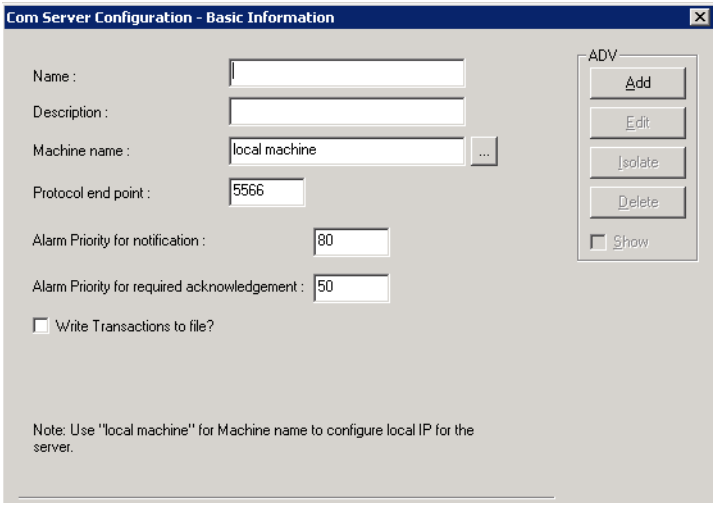
To communicate with system devices such as panels, readers, inputs, or outputs, you must configure the Communication Server for your access control system. The Communication Server can be installed on the same machine as the Database Server or on another computer in a networked system.

To add a communication server:

1. **In WIN-PAK CS:** Choose **System** > **Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Right-click the **Servers** (in WIN-PAK SE/PE Right-click the **Device** folder) 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.
   - 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. By default, the local **Machine Name** appears for the communication server. Click the ... button to select a different machine.

Tip: To find the machine name:

   a. Right-click **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 acknowledgment**"** 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.

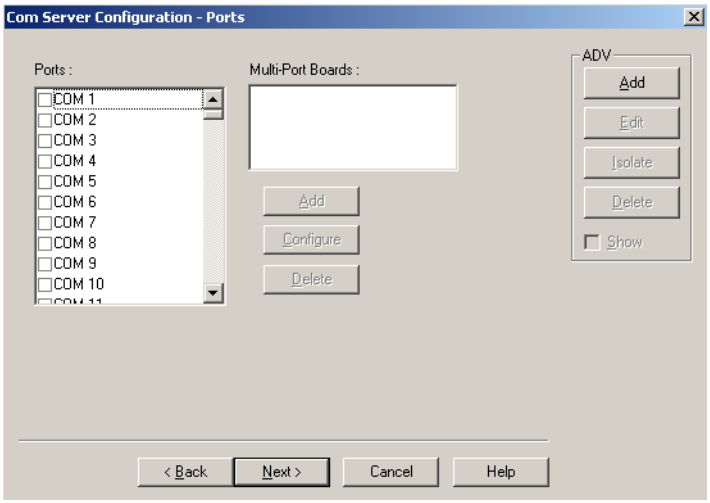
Note: Ensure that this value is higher than the priority number set in the Action Group while adding an ADV for the communication server. If you enter lower value than the priority number, the action is not displayed in Alarm View or in Event View. Rather, it is stored in the history of events.

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.

Note:

- For N-1000/PW-2000, NS/NS2+ 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 CS/SE/PE 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.
- In the **Operating System** area, the OS of the WIN-PAK CS/SE/PE system is displayed.

12. Click **Next**. The **Com Server Configuration - Ports** dialog box appears.

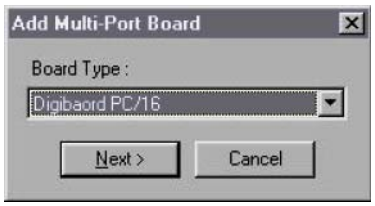


13. In the **Ports** list, select the required check boxes for the COM port that are used on this server for the access control equipment.

Note: Step 14 is applicable only for WIN-PAK CS.

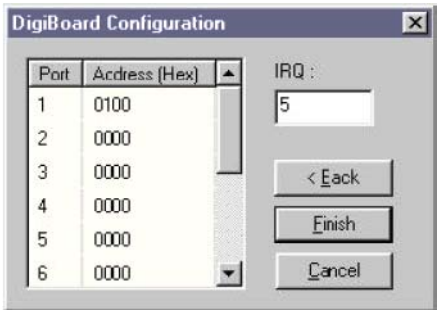
14. If the server has a Multi-Port board,

    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.

15. Click **Next** and then click **Finish** to add the communication server to WIN-PAK CS.

Note: You must ensure to manually open the remote communication server port.

Editing a Communication Server

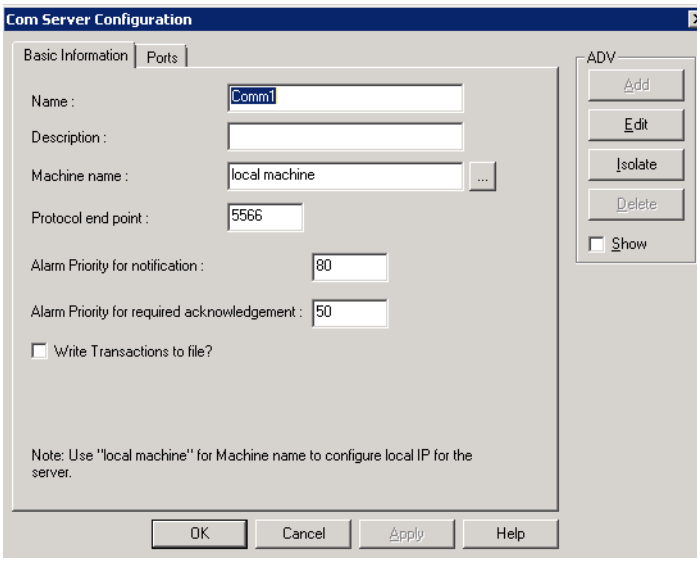
To edit the communication server:

1. **In WIN-PAK CS:** Choose **System** > **Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Server** (**Device** folder in-case of WIN-PAK SE/PE) folder to display the servers and devices added to the device map.

3. Right-click the communication server you want to edit, 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 descriptions.

Isolating a Communication Server

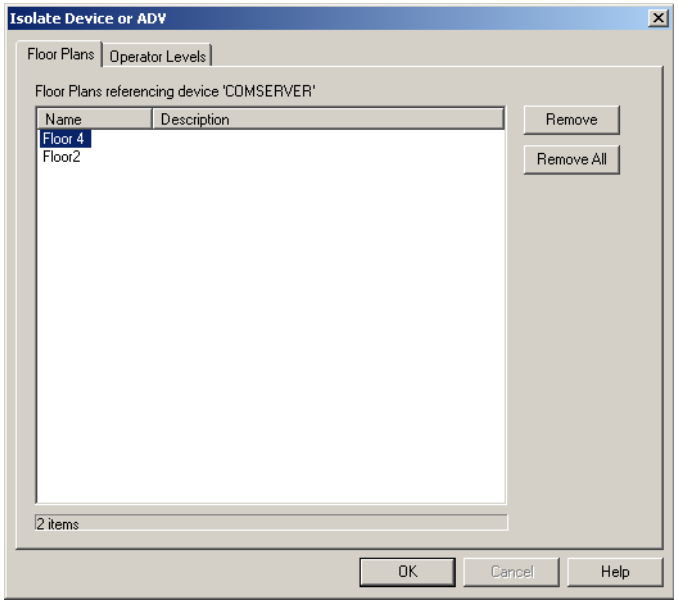
Note: This section is applicable only for WIN-PAK SE/PE.

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**.

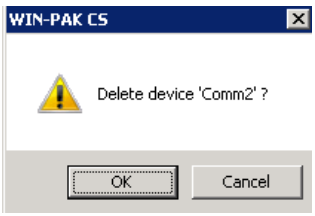
Deleting a Communication Server

You can delete a communication server only if you delete the devices attached to the communication server. To delete a communication server:

1. **In WIN-PAK CS:** Choose **System** > **Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Server** (**Device** folder in-case of WIN-PAK SE/PE) folder to display the servers and devices added to the device map.
3. Right-click the communication server and click **Delete**. A confirmation message appears.



4. Click **OK** to confirm the deletion. The communication server is deleted.

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.

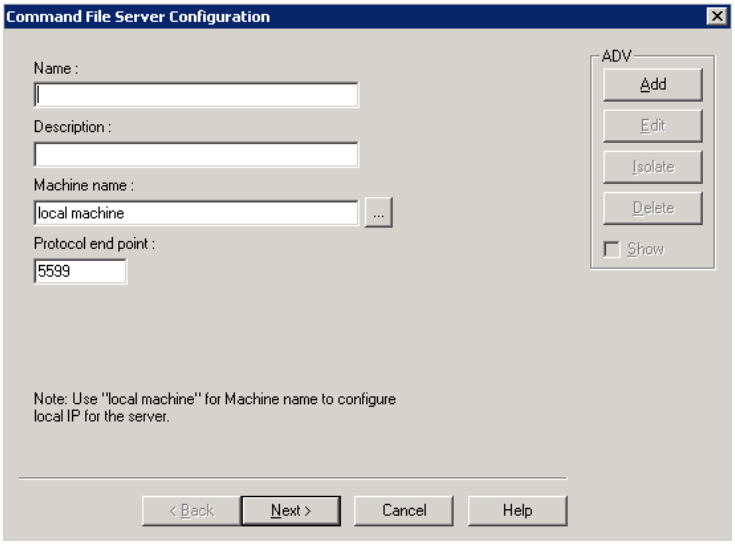
Adding a Command File Server

To add a command file server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Right-click the **Servers** (**Device** folder in-case of WIN-PAK SE/PE) 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 **Command File Server Configuration** dialog box.
   - 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. By default, the local **Machine Name** appears for the **Command File Server**.

Note: You can click the button to browse and locate the local machine.

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.

Editing a Command File Server

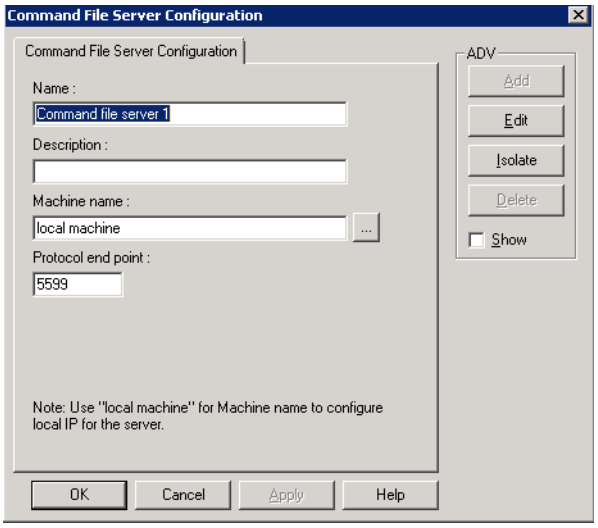
To edit a command file server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Servers (Device** folder in-case of WIN-PAK SE/PE) folder to display the servers added to the tree.

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 a Command File Server

Note: This section is applicable only for WIN-PAK SE/PE.

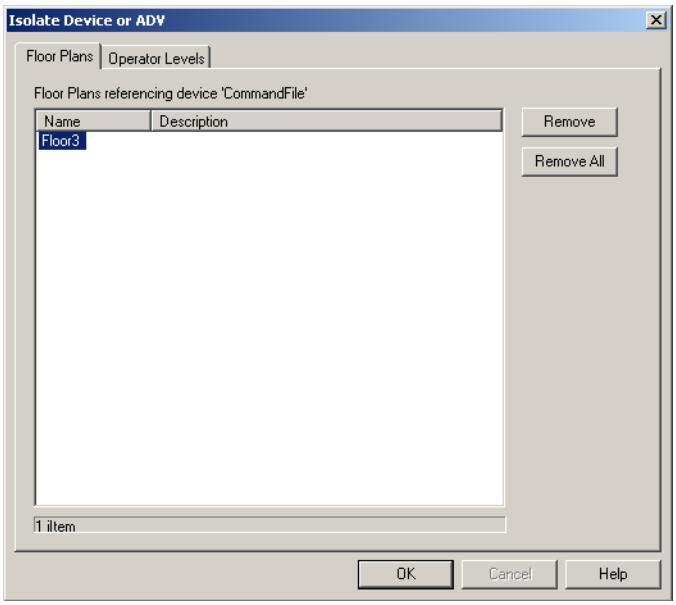
You can delete a command file server in WIN-PAK SE/PE, only if you isolate an ADV of the command file server from floor plans and operator levels.

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

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Servers** (**Device** folder in-case of WIN-PAK SE/PE) folder to display the servers configured.
3. Right-click the command file server and click **Delete**. A confirmation message appears.
4. Click **OK** to confirm the deletion. The command file server is deleted.

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.

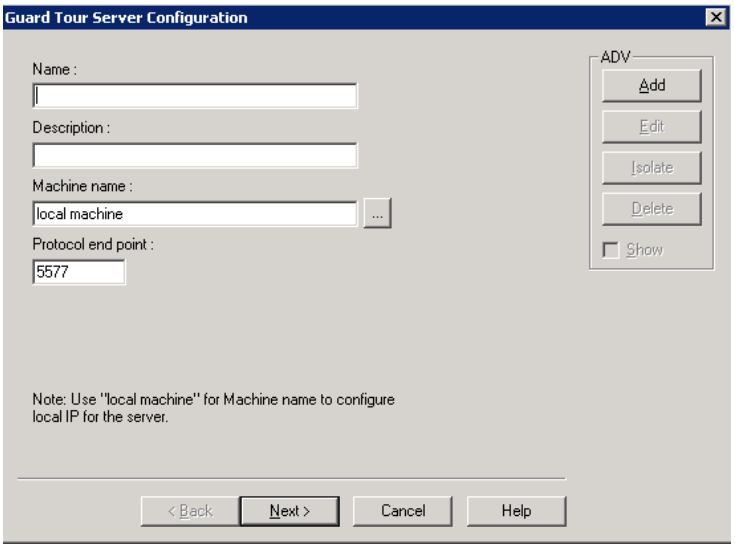
Adding a Guard Tour Server

To add a guard tour server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Right-click the **Servers** (**Device** folder in-case of WIN-PAK SE/PE) 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.
    - 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. By default, the local **Machine Name** appears for the **Guard Tour Server**.

Note: You can click the button to browse and locate the local machine.

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.

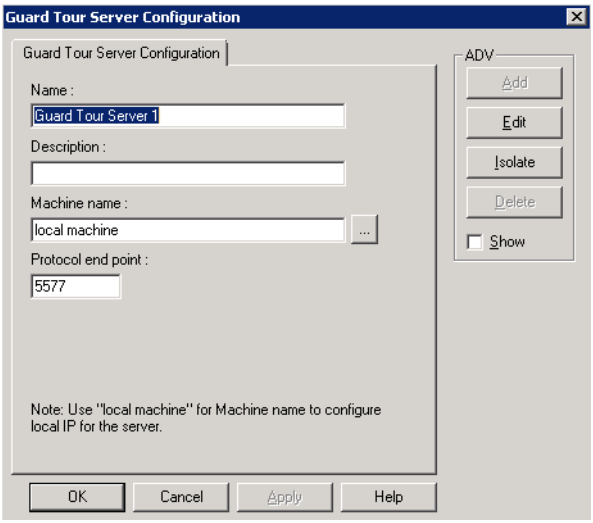
8. Click **Next** to proceed to the final dialog box for the Guard Tour Server Configuration.
9. Click **Finish** to add the server.

Editing a Guard Tour Server

To edit a guard tour server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.
2. Expand the **Servers** (**Device** folder in-case of WIN-PAK SE/PE) folder to display the servers added to the tree.
3. Right-click the guard tour server and click **Configure**. The **Guard Tour Server Configuration** dialog box appears.



4. Make the required changes to 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.

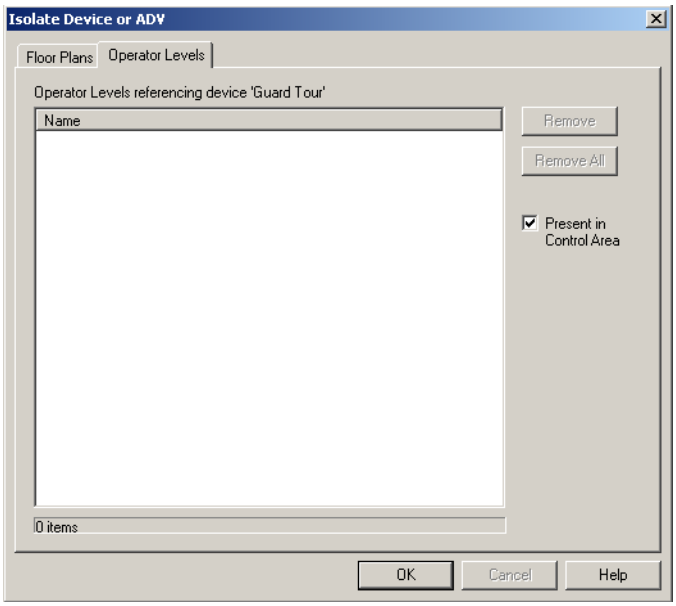
Isolating a Guard Tour Server

Note: This section is applicable only for WIN-PAK SE/PE.

You can delete a guard tour server, only if you isolate an ADV of the guard tour server from floor plans and operator levels.

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. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Servers (Device** folder in-case of WIN-PAK SE/PE) folder to display the servers added to the tree.

3. Right-click the guard tour server and click **Delete**. A confirmation message appears.

4. Click **OK** to confirm the deletion. The guard tour server is deleted.

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.

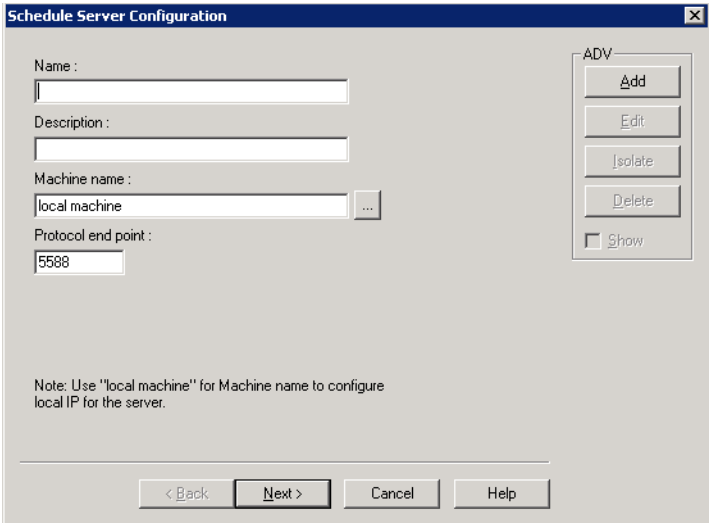
Adding a Schedule Server

To add a schedule server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Right-click the **Servers** folder (**Device** folder in-case of WIN-PAK SE/PE) 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.

   See the "Configuring an Abstract Device" section for more details on ADV configuration.

6. After adding an ADV, click **OK** to return to the **Schedule Server Configuration** dialog box.
   - 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. By default, the local **Machine Name** appears for the **Schedule Server**.

Note: You can click the button to browse and locate the local machine.

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.

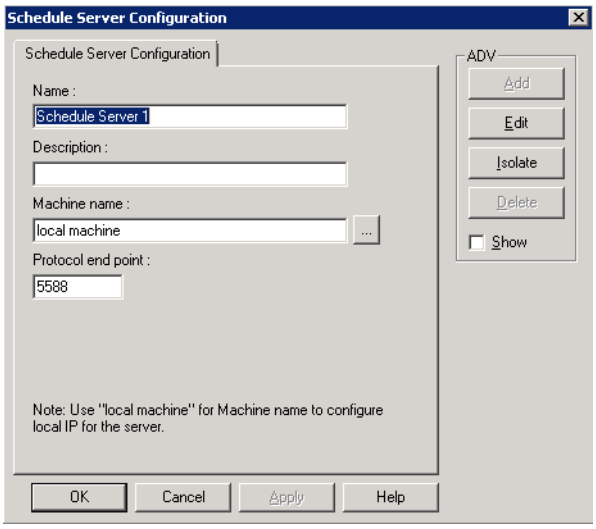
Editing a Schedule Server

To edit a schedule server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Servers (Device** folder in-case of WIN-PAK SE/PE) folder to display the servers added to the tree.
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.

   See the "Adding a Schedule Server" section for configuring guard tour server.

5. Click **OK** to configure the schedule server.

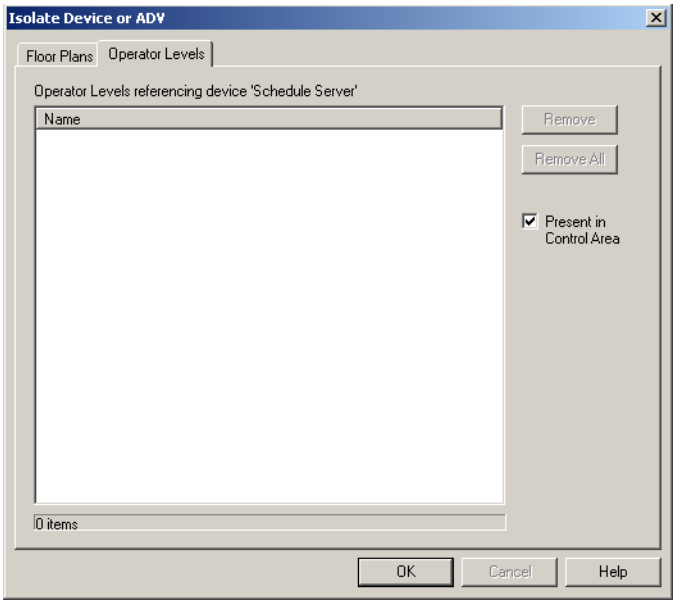
Isolating a Schedule Server

Note: This section is applicable only for WIN-PAK SE/PE.

You can delete a schedule server, only if you isolate the device or an ADV of schedule server from floor plans and operator levels.

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.



1. 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.
2. 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.
3. Click **OK**.

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.

To delete a schedule server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Servers** (**Device** folder in-case of WIN-PAK SE/PE) folder to display the servers configured.
3. Right-click the schedule server and click **Delete**. A confirmation message appears.
4. Click **OK** to confirm the deletion. The schedule server is deleted.

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.

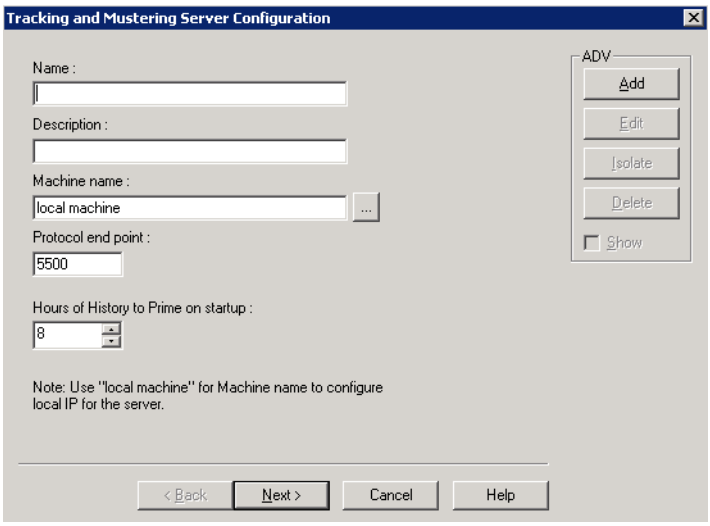
Adding a Tracking and Muster Server

To add a tracking and muster server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Right-click the **Servers** (**Device** folder in-case of WIN-PAK SE/PE) 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.
   - 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. By default, the local **Machine Name** appears for the **Tracking and Mustering Server**.

Note: You can click the button to browse and locate the local machine.

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.

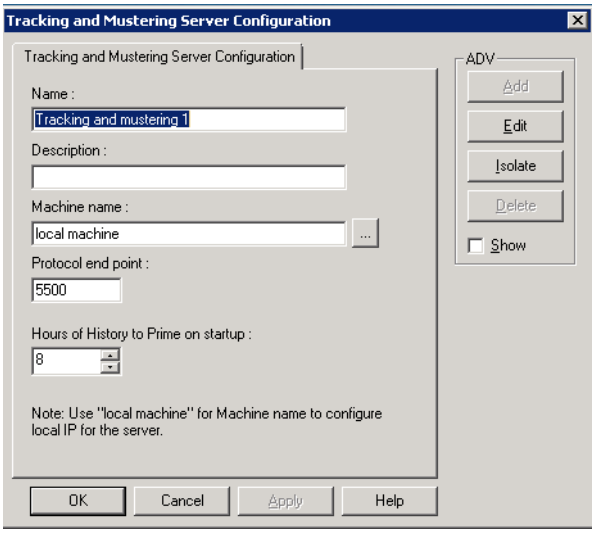
Editing a Tracking and Muster Server

To edit a tracking and muster server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the **Servers (Device** folder in-case of WIN-PAK SE/PE) folder to display the servers added to the tree.
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.

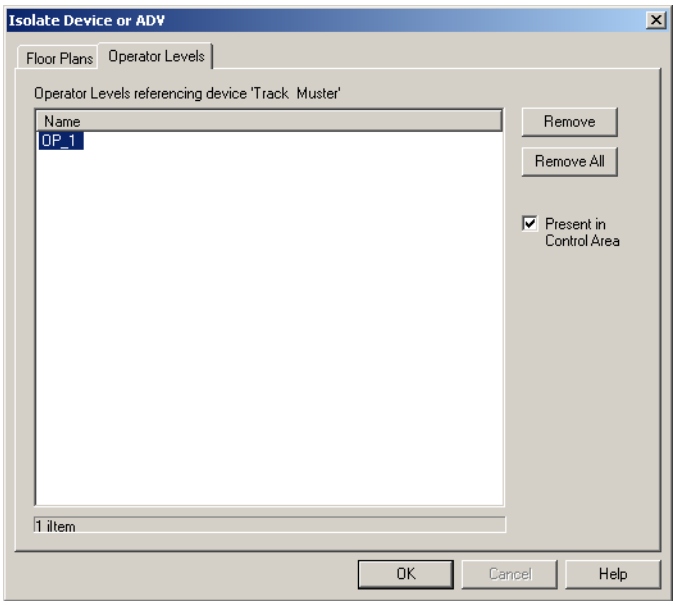
Isolating a Tracking and Muster Server

Note: This section is applicable only for WIN-PAK SE/PE.

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.

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

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.

To delete a tracking and muster server:

1. **In WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.
2. Expand the **Servers** (**Device** folder in-case of WIN-PAK SE/PE) folder to display the servers configured.
3. Right-click the tracking and muster server and click **Delete**. A confirmation message appears.
4. Click **OK** to confirm the deletion. The tracking and muster server is deleted.

Ethernet Module (Galaxy Panel)

The Galaxy panel helps you to monitor and track intrusion happening at different zones in the access control system. Zones are areas covered by a device that is monitored by the galaxy panel. Galaxy panel is configured in the Galaxy Gold User Interface application and then downloaded to WIN-PAK CS/SE/PE. However, the virtual keypad provided on WIN-PAK CS/SE/PE enables you to configure certain features in the Galaxy panel.

Notes:

- Ensure that you have a unique user name and password to operate on the virtual keypad.
- WIN-PAK CS/SE/PE 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 CS/SE/PE. When you add the galaxy panel, its connection with WIN-PAK CS/SE/PE is established and the panel configuration details are downloaded to WIN-PAK CS/SE/PE.
- WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

Adding a Galaxy Ethernet Module

Galaxy panel helps you to monitor and track intrusion happening at different zones in the access control system. Zones are areas covered by a device that is monitored by the Galaxy panel. Galaxy panel is configured using Galaxy Gold/GIRS application suite. However, the virtual keypad provided on WIN-PAK CS enables you to configure certain features in the Galaxy panel.

Note: WIN-PAK supports the Galaxy Dimension Panel series:

- GALAXY_GD_48
- GALAXY_GD_96
- GALAXY_GD_264
- GALAXY_GD_520

- Firmware 6.02 and above
- Ethernet module firmware 2.08 and above

WIN-PAK supports the Galaxy Grade 3 Panel series:

- GALAXY_144
- GALAXY_520
- Firmware 5.04/5.50 and above
- Ethernet module firmware 2.01 and above

WIN-PAK supports the Galaxy Classic Panel series:

- GALAXY_60
- GALAXY_128
- GALAXY_500
- GALAXY_504
- GALAXY_512
- Firmware 4.50 and above
- Ethernet module firmware 2.01 and above

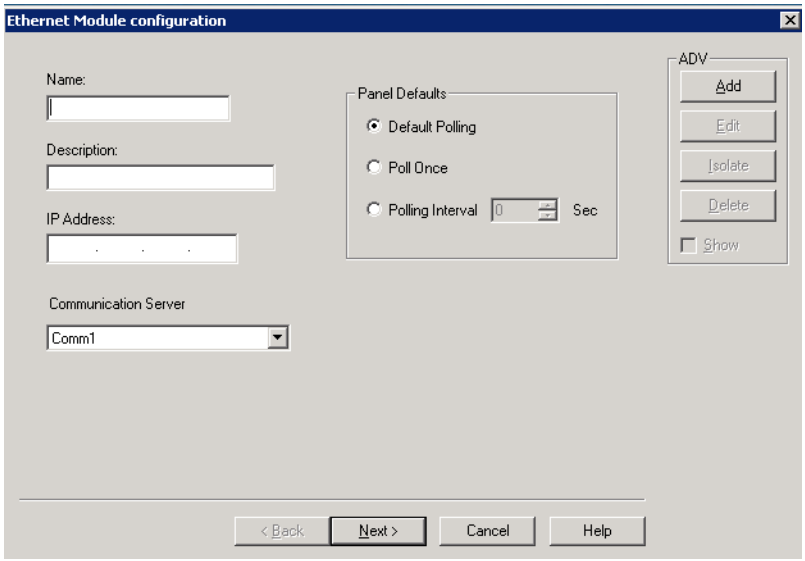
WIN-PAK supports the Galaxy Flex Panel series:

- FX20 (V3.18)
- FX50 (V3.18)
- FX100 (V3.18)
- FX20+ (V3.35)
- FX100+ (V3.35)

To add a Galaxy Ethernet module in WIN-PAK CS/SE/PE:

1. Click **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 polling frequency at which the Galaxy panel will be polled to update the status of the panel and its peripheral devices. The available polling options are:
   - **Default Polling**: Select this option to poll continuously at the interval of 2 seconds.
   - **Poll Once:** Select this option to poll only once after the Communication server is started.
   - **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.

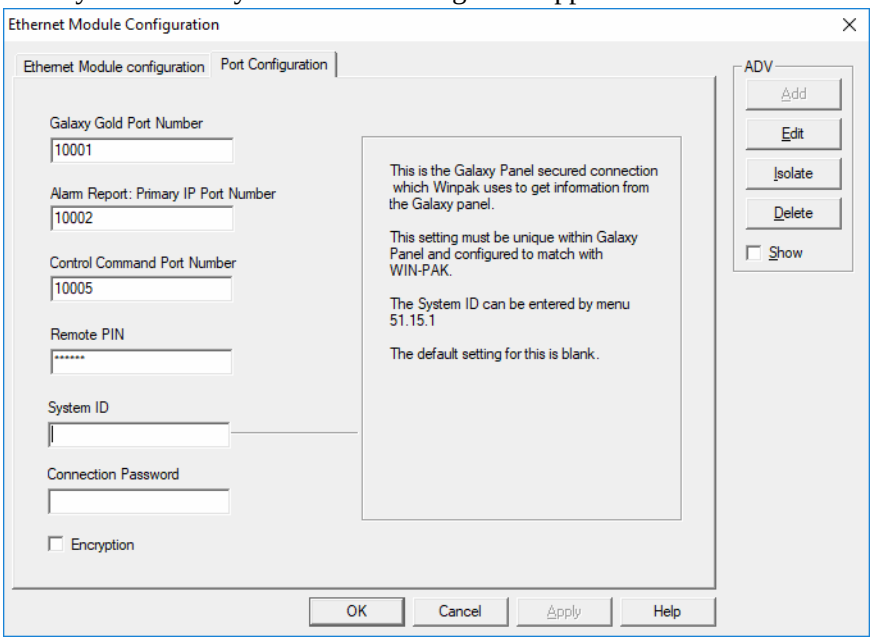
7. **In WIN-PAK CS:** In the **Galaxy Gold Port Number** box, type the TCP IP port number used by the **Galaxy Gold** and is fixed.

   In WIN-PAK SE/PE: In the **Galaxy Gold Port Number** box, type the TCP IP port number used by the **Galaxy Gold** User Interface in WIN-PAK SE/PE. By default, it is set to 10001. If you change the port number, the configuration of the Galaxy Gold UI must be change accordingly.

8. In the **Alarm Report: Primary IP Port Number** box, type the TCP IP port number used by the Galaxy panel for reporting alarms in WIN-PAK CS/SE/PE. By default, it is set to 10002.

Note: When adding multiple galaxy panels, ensure that the primary IP port number field must be unique.

9. In the **Control Command Port Number** box, type the TCP/IP port used for Control Commands. By default, it is set to 10005 and is fixed.
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 CS/SE/PE to Galaxy panel. The connection password is configured in the Galaxy Gold/Galaxy Remote Servicing Suite application.



12. In the Galaxy/Flex panel, you can type the **System ID**.

Note: You can update the same **System ID** in WIN-PAK to check the uniqueness of the Galaxy/Flex panel.

13. Select or clear the **Encryption** check box to enable encryption of password when an alarm is sent to WIN-PAK CS/SE/PE from the Galaxy panel.
14. Under **ADV**, click **Add** to create an ADV for the Ethernet module (E080) of Galaxy. See 'Configuring an Abstract Device'.
15. Click **Next** to advance to the Finish dialog box.
16. Click **Next** to configure the Ethernet module for Galaxy. The Ethernet module (E080) for Galaxy panel is configured. See 'Adding a Galaxy Panel'.

Adding a Galaxy Panel

WIN-PAK CS/SE/PE 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 CS/SE/PE, the Galaxy panel configuration details are downloaded to WIN-PAK CS/SE/PE.

Note: WIN-PAK supports the Galaxy Dimension Panel series:

- GALAXY_GD_48
- GALAXY_GD_96
- GALAXY_GD_264
- GALAXY_GD_520
- Firmware 6.02 and above
- Ethernet module firmware 2.08 and above

WIN-PAK supports the Galaxy Grade 3 Panel series:

- GALAXY_144
- GALAXY_520
- Firmware 5.04/5.50 and above
- Ethernet module firmware 2.01 and above

WIN-PAK supports the Galaxy Classic Panel series:

- GALAXY_60
- GALAXY_128
- GALAXY_500
- GALAXY_504
- GALAXY_512
- Firmware 4.50 and above
- Ethernet module firmware 2.01 and above

WIN-PAK supports the Galaxy Flex Panel series:

- FX20 (V3.18)
- FX50 (V3.18)
- FX100 (V3.18)
- FX20+ (V3.35)
- FX100+ (V3.35)

Note: Before you download the Galaxy panel configuration details to WIN-PAK CS:

- Restart the communication server and ensure it is running.
- Ensure that the Galaxy panel is not in an Engineering Mode.

Note: Galaxy integration feature is available only when you buy the license.

To add a Galaxy panel:

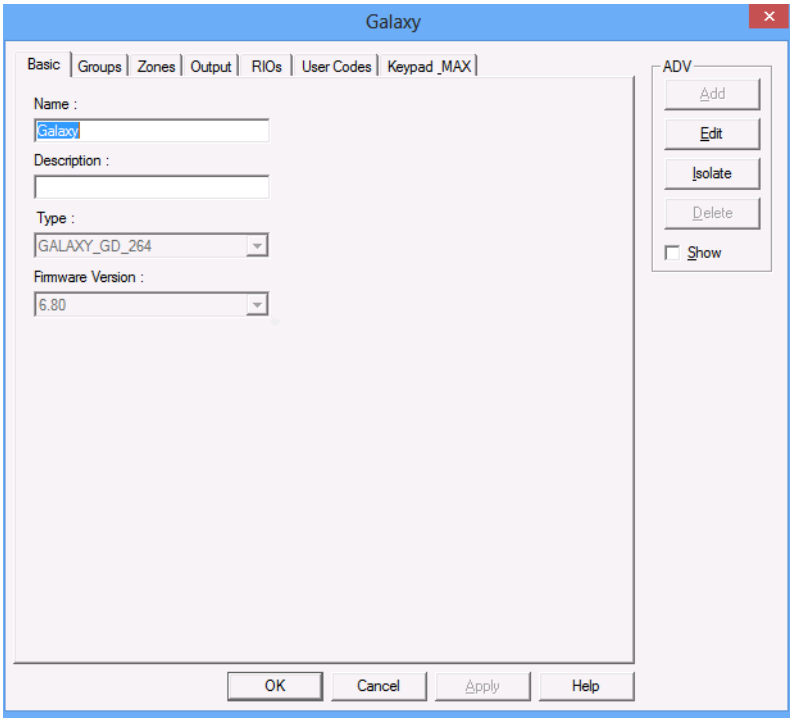
1. Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.

2. Expand the communication server.
3. Right-click the **Ethernet Module Galaxy (Single Panel)** and select **Add New Galaxy Panel**.

   WIN-PAK CS/SE/PE establishes a connection with the Galaxy panel and starts downloading configuration details to the WIN-PAK CS/SE/PE database.

Note: When you download Galaxy panel configuration details to WIN-PAK CS, the abstract devices for group, zones, outputs, RIO boards are automatically created. However, you can change the ADV configuration details in the WIN-PAK CS system.

4. After the panel configuration details are downloaded, the **Panel Configuration - Basic** dialog box appears.



5. Enter the basic details of the panel such as **Name** and **Description**.
6. Details for **Type** and **Firmware Version** are automatically downloaded from the panel to WIN-PAK CS/SE/PE.
7. Click **Next** to perform the following tasks:

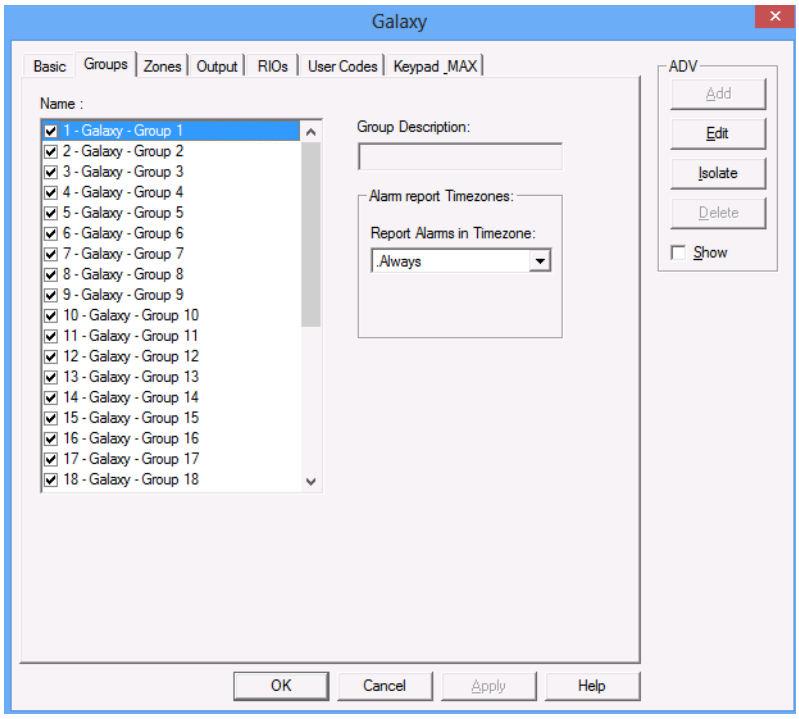
Task	Go To
Setting panel groups	page 370
Setting panel zones	page 371
Setting panel outputs	page 372

Task	Go To
Setting the RIO board	page 373
Defining user codes	page 374
Defining a keypad and MAX	page 375

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.

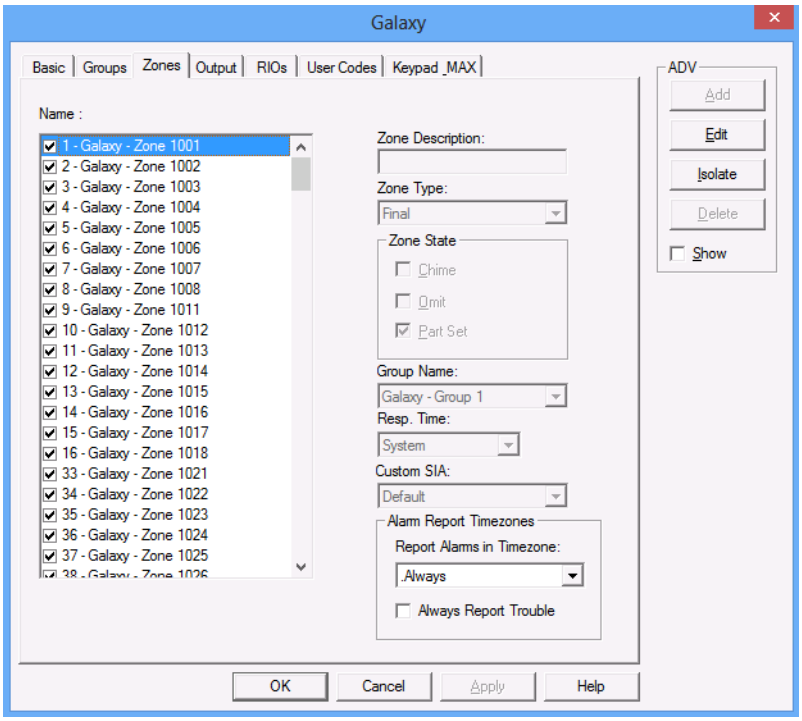
Note: If you want to assign zones to different groups, you must do it in the Galaxy panel and then download it to WIN-PAK.

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: A maximum of 128 time zones can be added to the Panel Configuration.

The **Zone Type**, **Zone State**, **Group of the zone** and other details are displayed on the right. These fields are non-editable.

2. Under **Alarm report Timezones**, select a time zone during which the alarms generated from a group must be reported.
3. Select the **Always Report Trouble** check box to report troubles irrespective of the selected time zone.
4. To edit the group ADV configuration, click **Edit** under ADV and edit ADV and action groups.

Table 9-1 Describing zone properties

Property	Description
Zone Type	The type of the device used in the zone such as Fire, Intruder.

Table 9-1 Describing zone properties

Property	Description
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.

5. Under **Alarm Report Timezones**, select a time zone during which the alarms generated from this zone must be reported.
6. Select the **Always Report Trouble** check box to report troubles irrespective of the selected time zone.
7. To edit the zone ADV configuration, click **Edit** under ADV. See 'Configuring an Abstract Device'.
8. 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 a zone in the **Name** list to rename it.

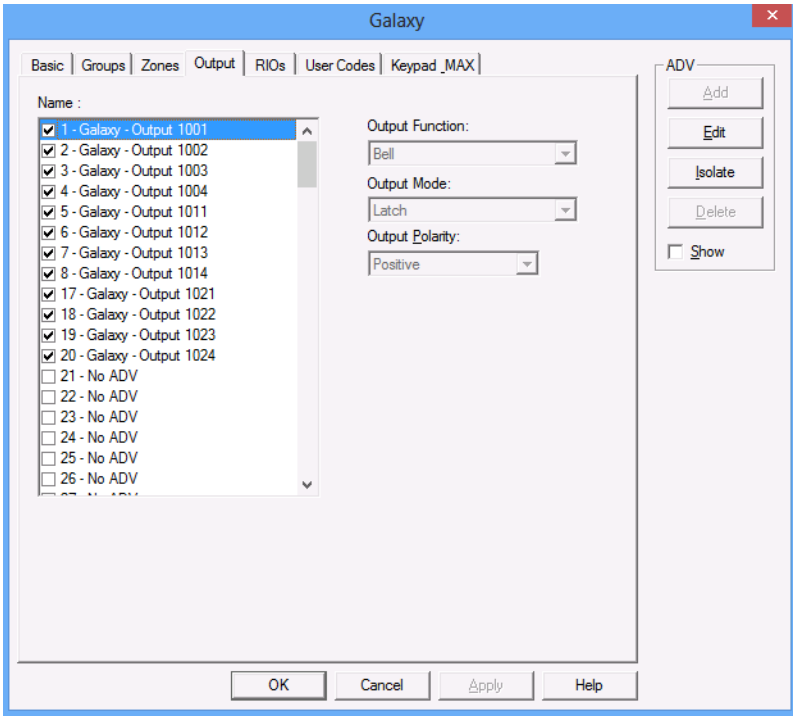


Table 9-2 Describing properties

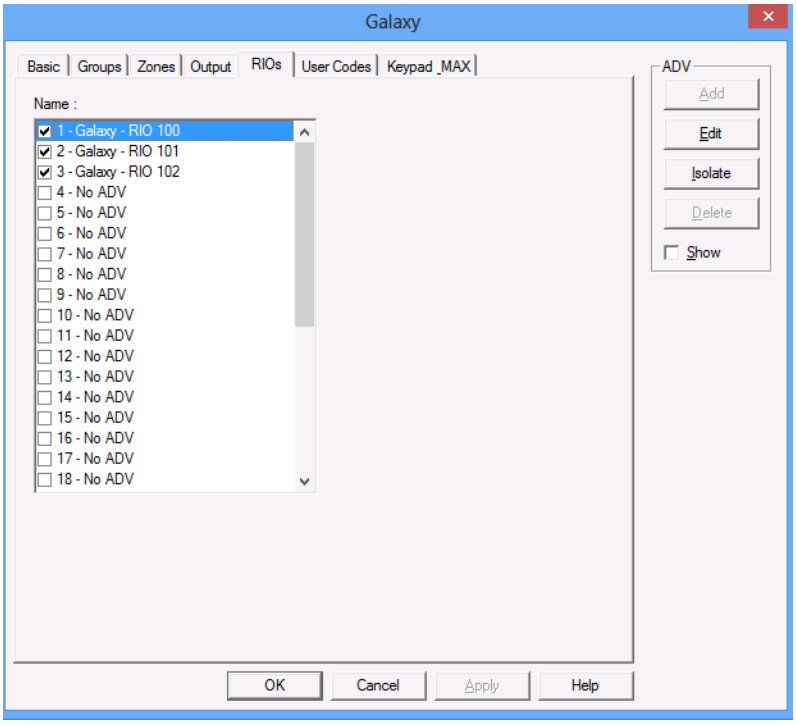
Property	Description
Output Function	The function to be performed by the output device like beep an alarm.
Output Mode	The mode in which the output operates such as Latch, Reflex, and Pulse.

2. To edit the output ADV configuration, click **Edit** under **ADV** and edit ADV and action groups. See 'Configuring an Abstract Device'.
3. Click **Next** to view the RIO board configuration details.

Setting the RIO board

The Relay Input Output (RIO) board is the extendibles 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.



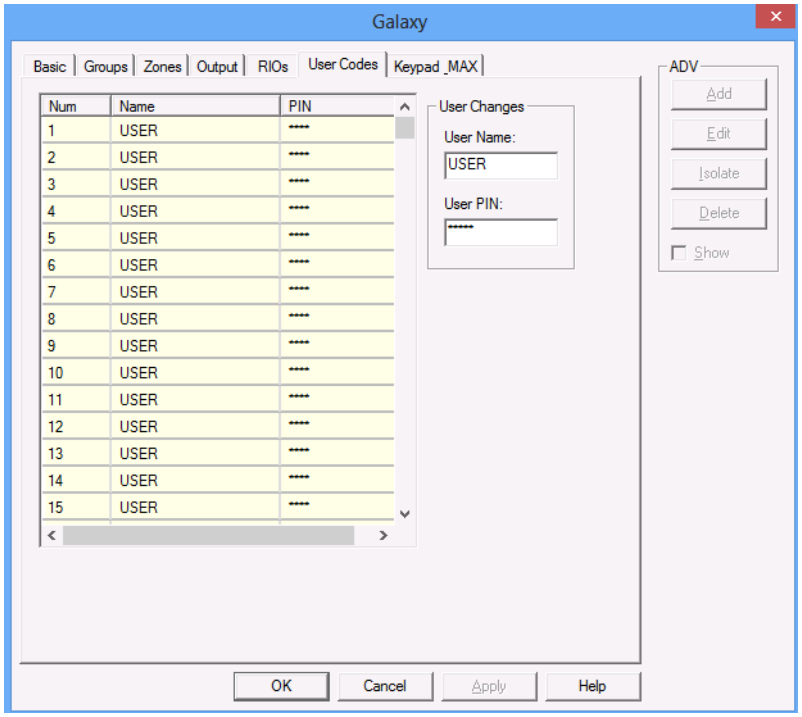
2. Click **Next** to define the user codes. The **Galaxy - User Codes** dialog box appears.

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**.

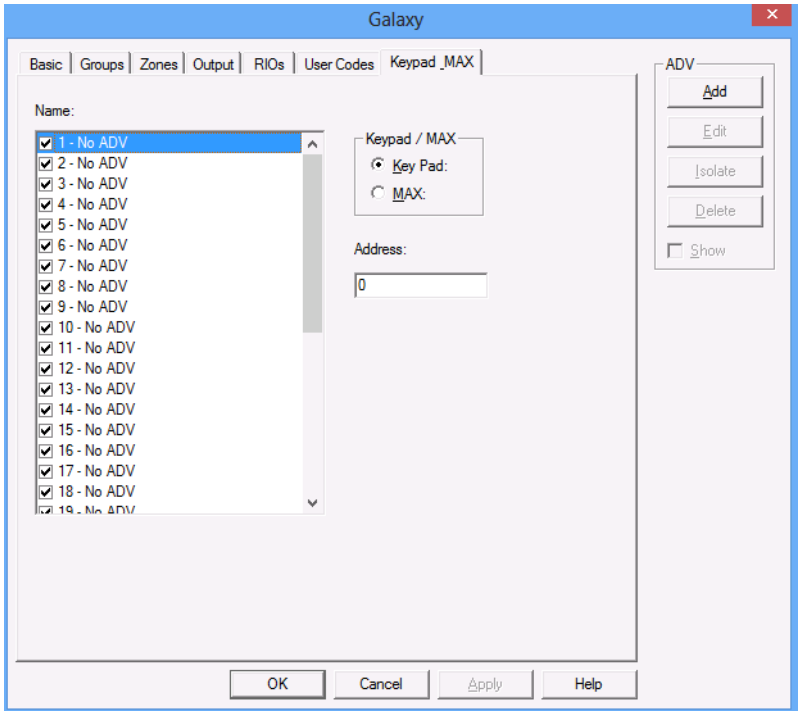


2. Click **Next** for setting the keypad or **Max** for configuring Galaxy panel. The **Keypad & MAX** dialog box appears.

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:

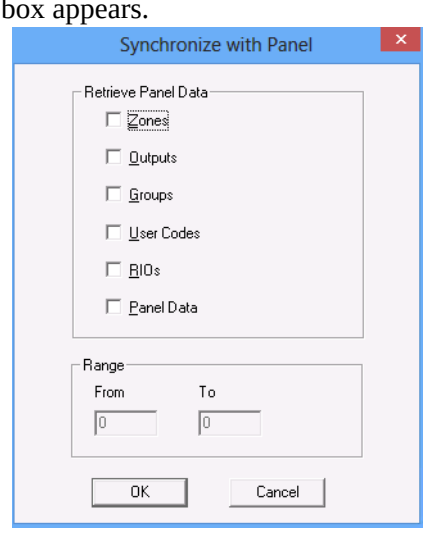
- Synchronize
- Viewing Panel Configuration Details
- Downloading Log Data
- Uploading User Code
- Uploading Date and Time
- Working on Virtual Keypad

Synchronizing with Galaxy Panel

Synchronizing the data in the Galaxy panel with WIN-PAK CS/SE/PE ensures that the data in WIN-PAK CS/SE/PE is updated with the latest data in Galaxy. In addition, any changes made in the Galaxy panel after it was downloaded to WIN-PAK CS/SE/PE are also updated in WIN-PAK.

To synchronize WIN-PAK CS/SE/PE 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 CS/SE/PE.

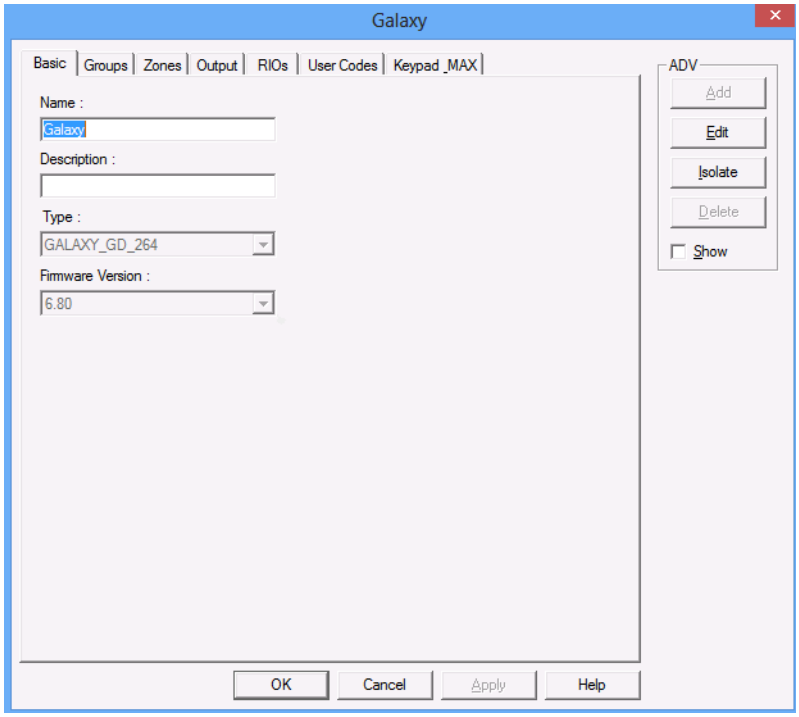
Note: When you upload the data to the panel, the panel data is overwritten with the uploaded data.

Viewing Panel Configuration Details

You can view the latest configuration details of the Galaxy panel that were downloaded to WIN-PAK CS/SE/PE.

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. See 'Adding a Galaxy Panel'.

Note: When you upload the data to the panel, the panel data is overwritten with the uploaded data.

Downloading Log Data

You can download the log information of the Galaxy panel into WIN-PAK CS/SE/PE.

To download the log data to WIN-PAK CS/SE/PE:

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 CS/SE/PE. If you click No, you cannot download log data to WIN-PAK CS/SE/PE.

Uploading User Code

You can upload a range of user code details that are configured in WIN-PAK CS/SE/PE 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 CS/SE/PE system to the Galaxy panel.

To upload the current date and time:

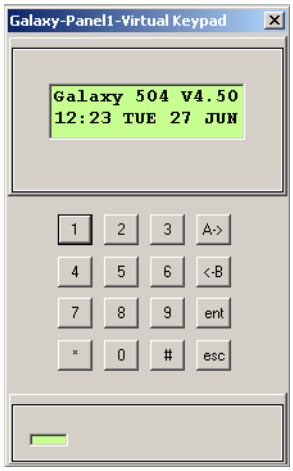
1. Right-click the Galaxy panel and select **Upload date and time** for uploading the current date and time. A confirmation message to stop the polling appears.
2. Click **Yes** to stop polling at communication server and upload the current date and time to the panel.

Work on Virtual Keypad

The virtual keypad is displayed in WIN-PAK CS/SE/PE 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

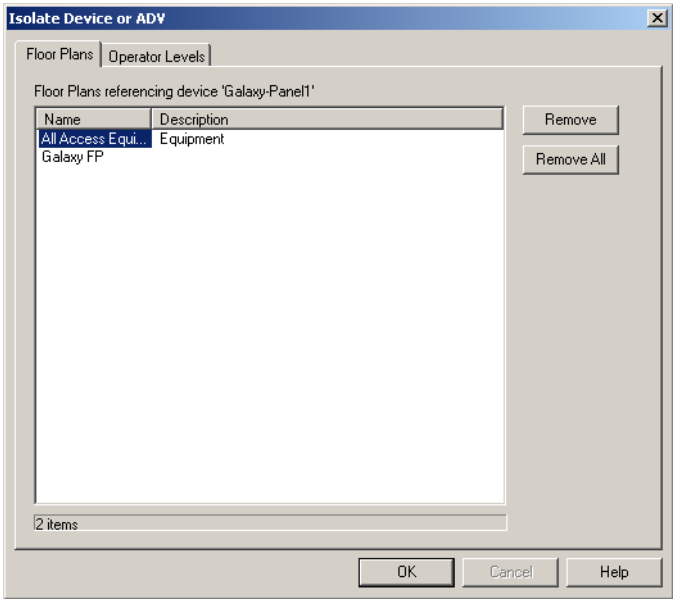
Note: This section is applicable only in WIN-PAK SE/PE.

You can delete the configuration details of the Galaxy panel from WIN-PAK SE/PE. 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.

Device Configuration

After adding the communication server and modem pools in the **Server Configuration** menu, you can add direct and remote loops, panels in the **Device Map**. Digital video devices can also be added in the Device Map.

Note: Devices configured in the Device Map are specific to the account, and the section **Device Configuration** is applicable only in WIN-CS.

Communication Loops

A communication loop is an interface between the panels and the communication server. It must be added to an existing communication server. You must have an available communication port, for each panel or a communication loop to be added.

The communication between the host server and the panels happen through a process known as **Reverse Initiation**. In this mode of communication, the host server is assigned a static IP, the panels are assigned dynamic IPs, and the communication happens through a unique port number in the host server. Communication through Reverse Initiation is possible only for devices which use the TCP/IP protocol. The devices include C100, 485 PCI, and RS 232 Panel Loops.

Note: You must create an ADV for each loop, panel, and other communication interfaces while configuring them.

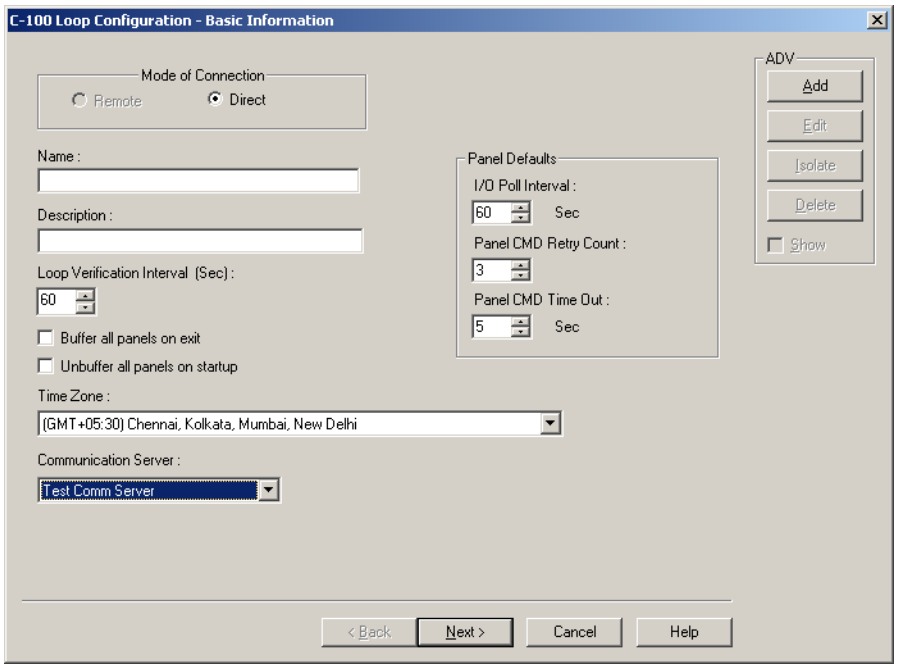
C-100 Panel Loop

Panels using 20-milliamp communications can be connected to the WIN-PAK CS/SE/PE 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 direct C-100 panel loop to the communication server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder, click **Add** and click **Panel Loop (C-100)**. The **C-100 Loop Configuration - Basic Information** dialog box appears.



3. Select the **Mode of Connection** as Direct.
4. Type a unique **Name** for the panel loop. This field is mandatory.
5. Type a **Description** for the panel loop.
6. 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.
7. After adding an ADV, click **OK** to return to the **C-100 Loop Configuration - Basic Information** dialog box.

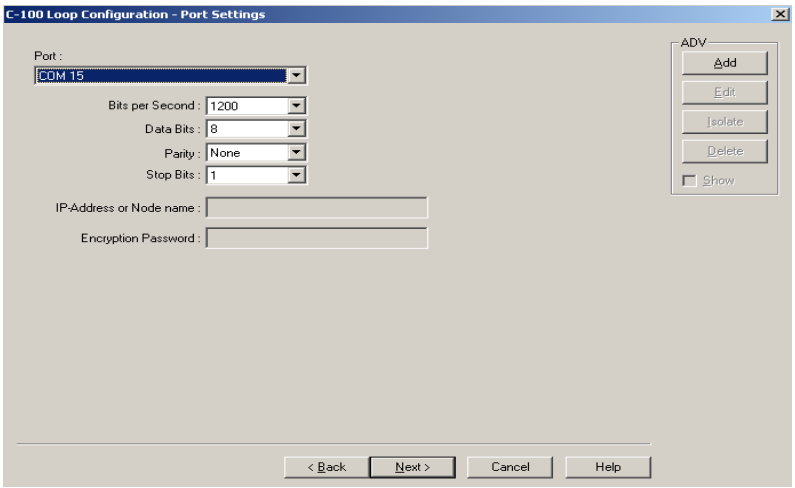
Notes:

- 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 CS SE/PE 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 on all the panels when the communication server is stopped.
10. Select **Unbuffer all panels on startup** to unbuffer all the panel events when the communication server is started.
11. Select the standard **Time Zone** based on the loop location.
12. Select the **Communication Server** from the list.
13. 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.
14. Click **Next** to set the port for the loop.

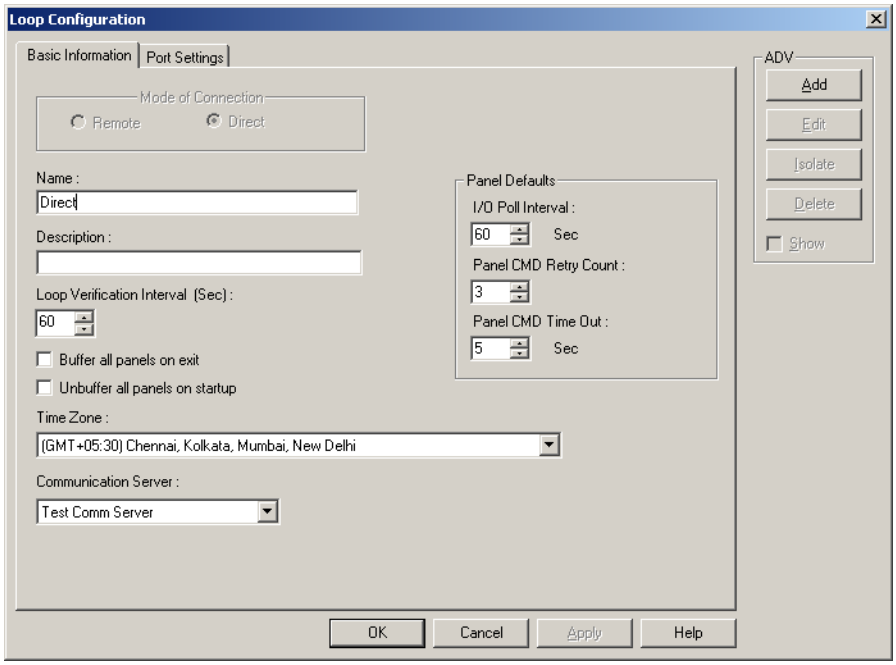


15. In the **Port** list, select a port of the communication server to which the loop is to be connected. The ports that are selected for the communication server and not used for other loops are listed.
16. If you select a port,
    a. Select the communication baud rate for the loop in **Bits per second**.
    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.
17. If you select a **TCP/IP Connection** port, type the **TCP/IP IP-Address or Node name** of the computer where the loop is connected.
18. If you select a **TCP/IP Encrypted Connection** port,
    a. Type the **TCP/IP IP-Address or Node name** of the computer where the loop is connected.
    b. Type the **Encryption Password**.
19. If you select a **TCP/IP Reverse Initiate** port, type the **Port Number**.
20. If you select a **TCP/IP Reverse Initiate With Encryption** port, type the **Encryption Password** and the **Port Number**.
21. Click **Next** to display the **C-100 Loop Configuration - Finish** dialog box.
22. 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

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.

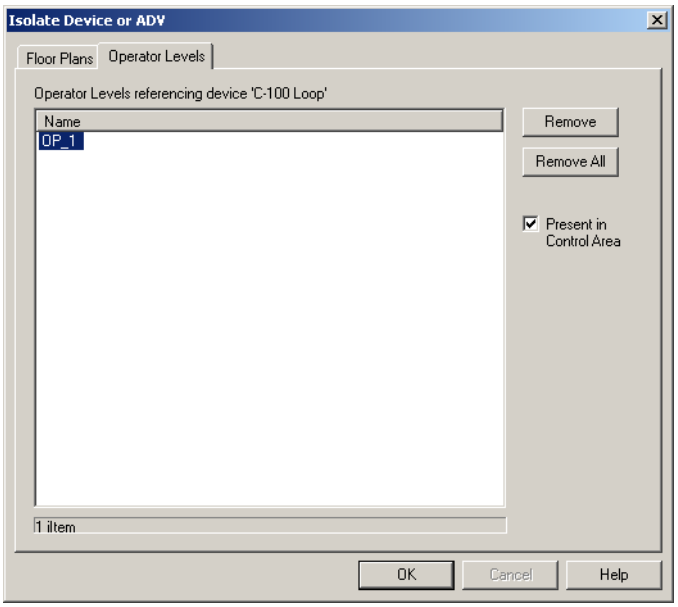
Isolating and Deleting a C-100 Panel Loop

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.

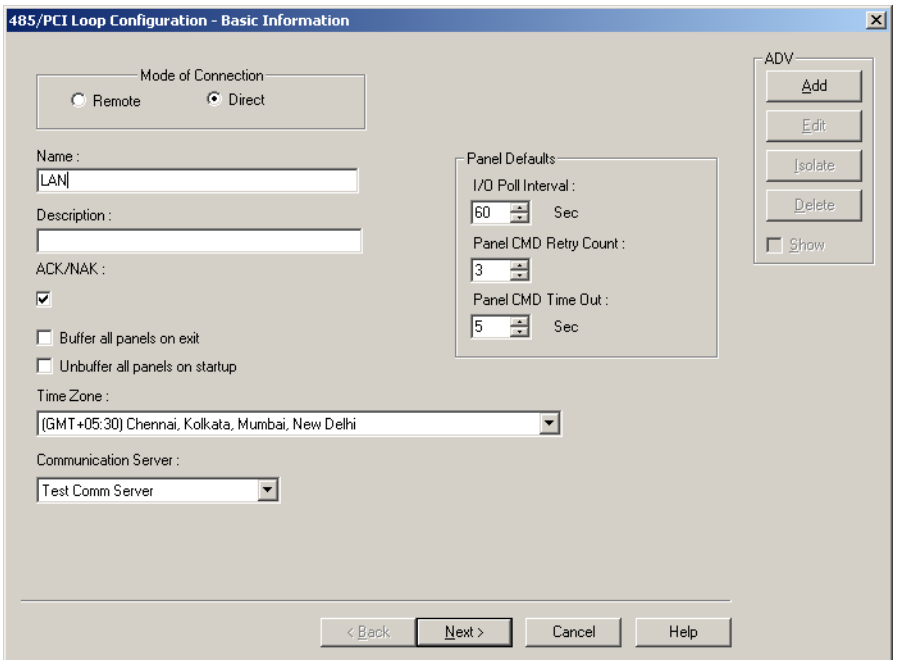
485/PCI Panel Loop

Panels using the RS-485 communication protocol can be connected to the WIN-PAK CS/SE/PE 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 direct 485/PCI panel loop:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder, click **Add** and click **Panel Loop (485/PCI)**. The **485/PCI Loop Configuration - Basic Information** dialog box appears.



Note: In **WIN-PAK CS**, select the **Mode of Connection** as Direct.

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 **485/PCI Loop Configuration Basic Information** 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 the ACK/NAK protocol. The ACK/NAK protocol requires acknowledgment, 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. Select the **Communication Server** from the list.
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 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.
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 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 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.

17. If you select the **TCP/IP Encrypted Connection** port,

    a. Type the **TCP/IP IP-Address or Node name** of the computer where the 485/PCI loop is configured.

    b. Type the **Encryption Password**.

18. If you select a **TCP/IP Reverse Initiate** port, type the **Port Number**.

19. If you select a **TCP/IP Reverse Initiate With Encryption** port, type the **Encryption Password** and the **Port Number**.

20. Click **Next** to display the **485/PCI Loop Configuration - Finish** dialog box.

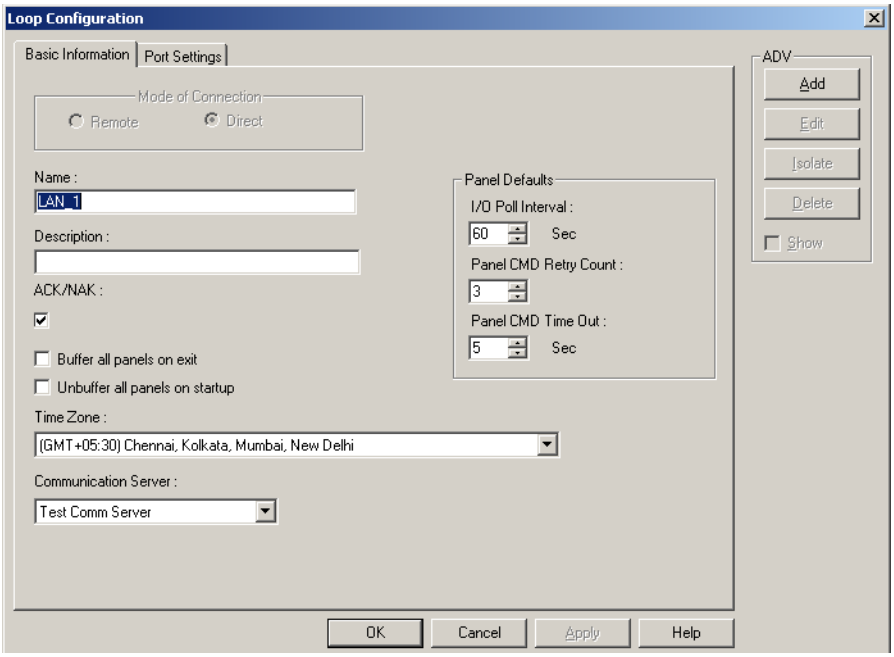
21. Click **Finish** to add the 485/PCI panel loop and return to the **Device** window.

    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.

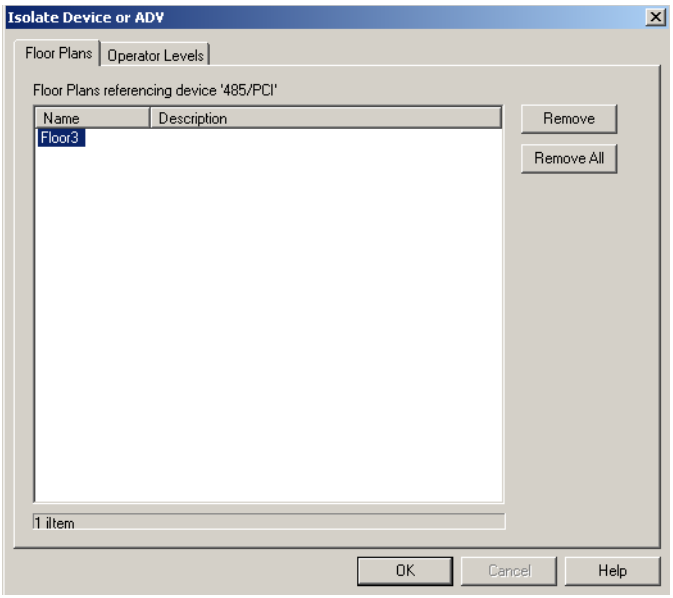
Isolating and Deleting a 485/PCI Panel Loop

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 associated 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.

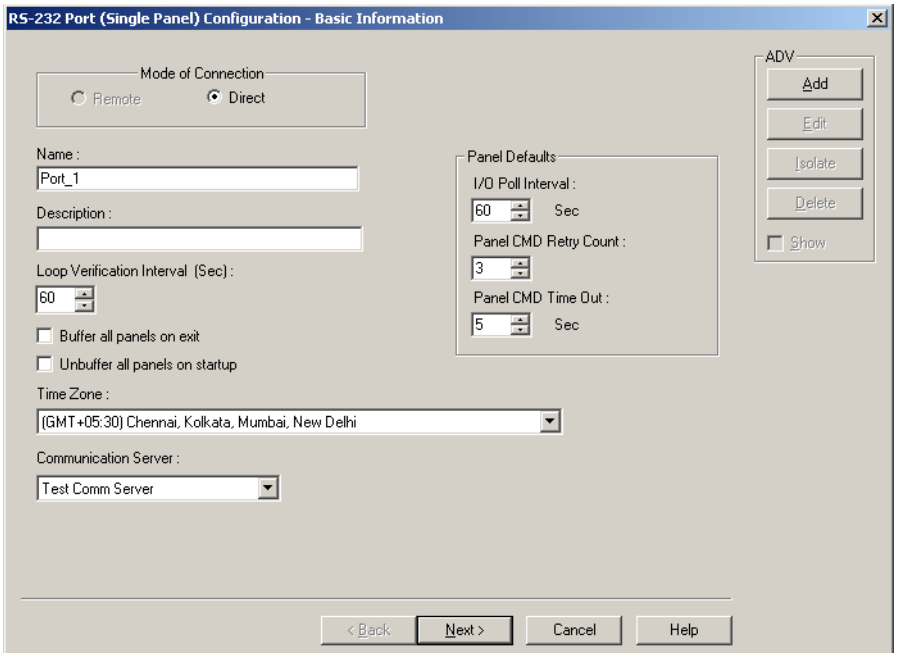
RS-232 Panel Loop

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. Right-click the **Devices** folder, click **Add** and click **RS-232 Port (Single Panel)**. The **RS-232 Port (Single Panel) Configuration - Basic Information** dialog box appears.



3. Select the **Mode of Connection** as Direct.
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-232 loop. Click **Add** under **ADV** to display the **Abstract Device Record - Server** dialog box.

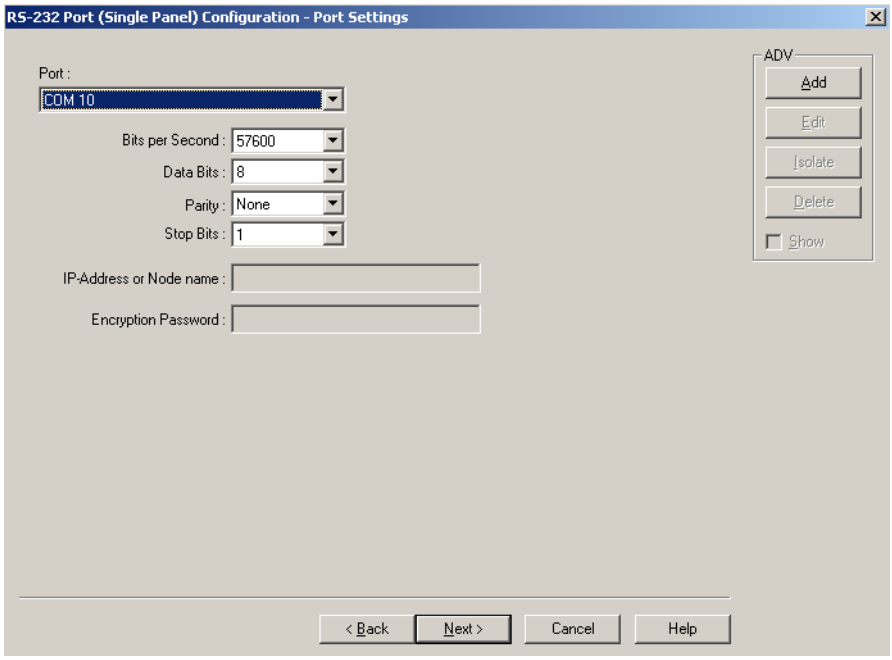
   Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.
7. After adding an ADV, click **OK** to return to the **RS-232 Port (Single Panel) Configuration** dialog box.

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 sent from WIN-PAK CS/SE/PE 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 CS when the communication server restarts.
11. Select the standard **Time Zone** based on the loop location.
12. Select the **Communication Server** from the list.
13. 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.
14. Click **Next** to set the port for the loop.



15. 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.
16. 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.
17. 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.
18. If you select **TCP/IP Encrypted Connection** port,
    a. Type the **TCP/IP IP-Address or Node name** of the computer where the panel is connected.
    b. Type the **Encryption Password** of the computer where the panel is connected.
    a. **Password** of the computer where the 485/PCI loop is configured.
19. If you select a **TCP/IP Reverse Initiate** port, type the **Port Number**.

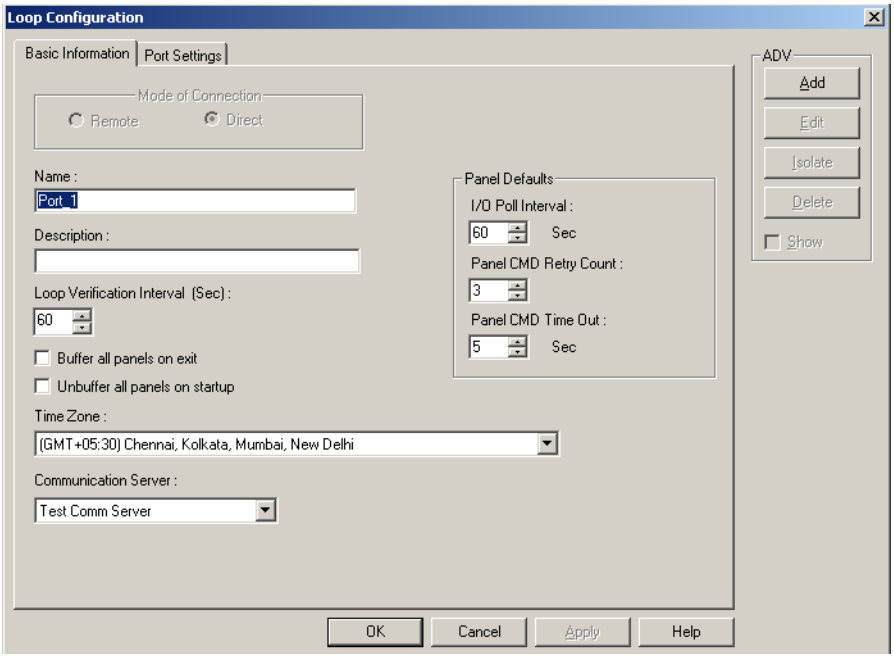
20. If you select a **TCP/IP Reverse Initiate With Encryption** port, type the **Encryption Password** and the **Port Number**.
21. Click **Next** to display the **Finish** dialog box.
22. Click **Finish** to add the RS-232 panel loop and return to the **Device** window.

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.

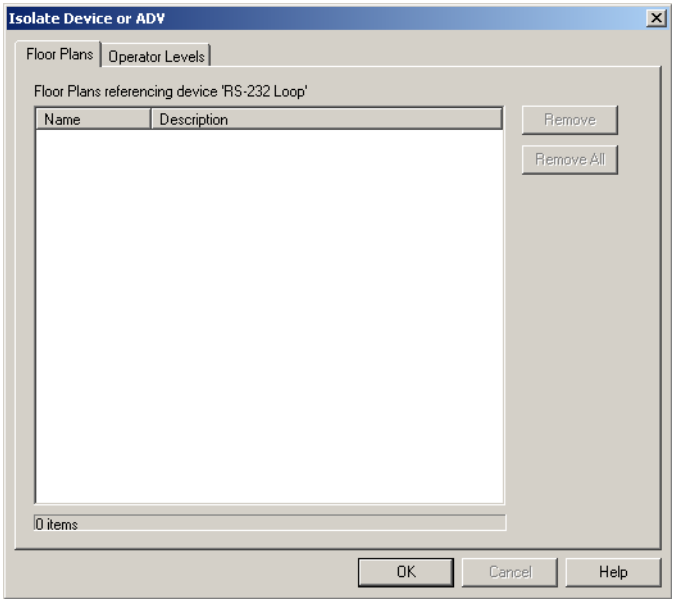
Isolating and Deleting an RS-232 Panel Loop

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 associated 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

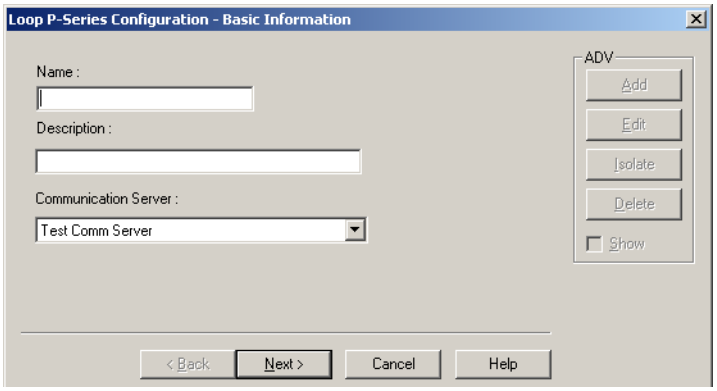
A P-Series panel loop represents a configuration of more than one P-Series Intelligent Controller panel boards. A loop requires only one com port on a communication server, and there can be up to eight Intelligent Controllers per loop, and up to 32 SIO Boards per Intelligent Controller.

Note: Beware, 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:

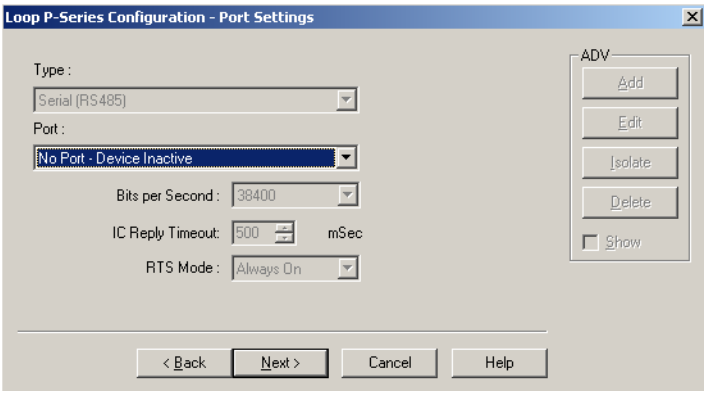
1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder, click **Add** and click **Panel Loop(P- Series)**. The **Loop P-Series Configuration - Basic Information** dialog box appears.



3. Type a unique **Name** for the P-Series panel loop. This field is mandatory.
4. Type a **Description** of the panel loop.
5. Select the **Communication Server** from the list.

Note: An ADV cannot be created for the P-Series panel loops, as the panel is directly connected to the WIN-PAK CS/SE/PE system.

6. Click **Next** to include port details.



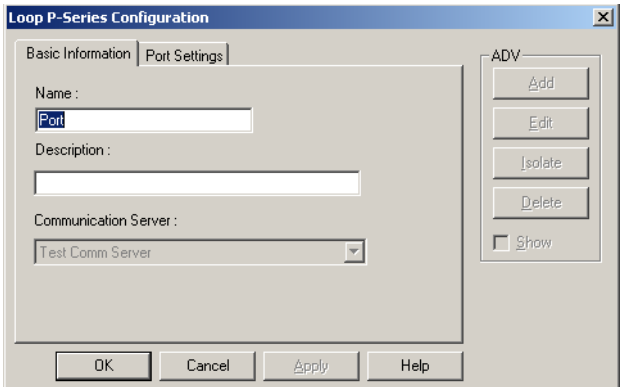
In the **Type** list, **Serial (RS485)** is displayed by default. When you establish a PRO-2200 panel loop, the only applicable type is RS485.

7. 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.
8. 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.
9. Click **Next** to display the **Loop P-Series Configuration - Finish** dialog box.
10. Click **Finish** to add the P-Series panel loop.

Editing 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.

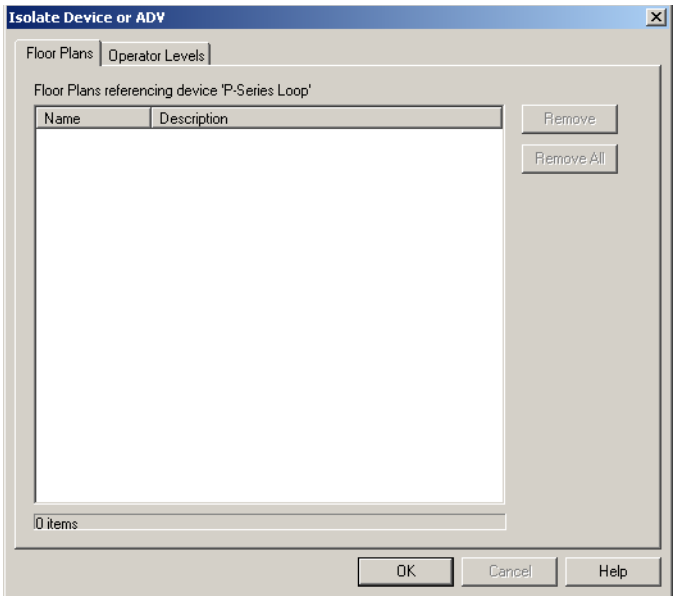
Isolating and Deleting a P-Series Panel Loop

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 associated 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.

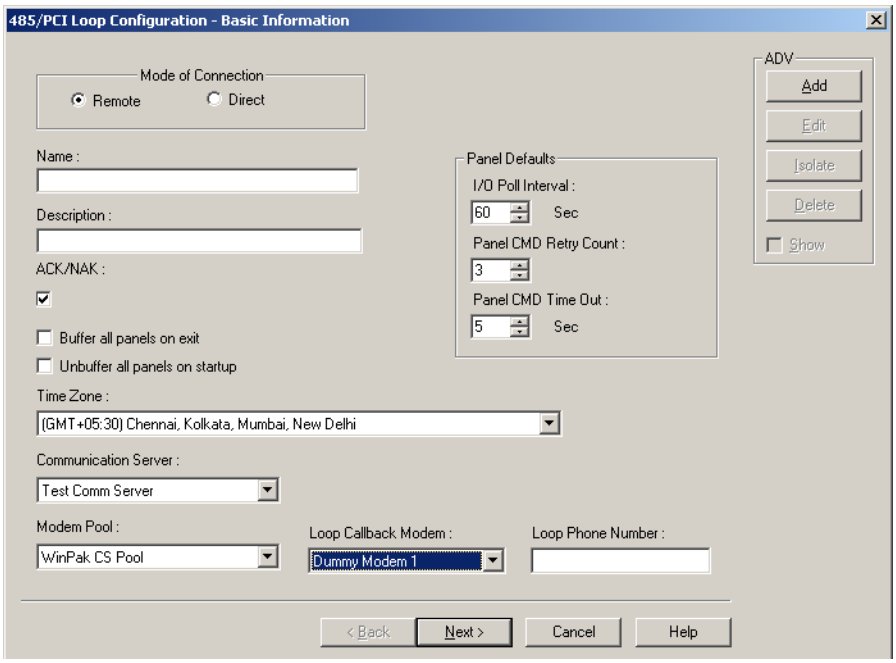
C-100 or 485 (non-ACK/NAK) Remote Communication Loop

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 remote C-100 loop or 485 (non-ACK/NAK) to a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder, click **Add** and click **Panel Loop (C-100)** or **Panel Loop (485/PCI)**. The **Loop Configuration - Basic Information** dialog box appears for the selected loop type (C-100 or 485/PCI).



Note: In WIN-PAK CS, select the **Mode of Connection** as Remote.

3. Type a unique **Name** for the remote communication loop. This field is mandatory.

4. Type a **Description** for the C-100 or 485 (non-ACK/NAK) loop.

Note: In WIN-PAK CS, clear the **ACK/NAK** check box to add a non-ACK/NAK loop.

5. 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: In WIN-PAK SE/PE, 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.

6. Select **Buffer all panels on exit** to buffer the events on all the panels when the communication server stops.
7. Select **Unbuffer all panels on startup** to unbuffer all panel events when the communication server restarts.
8. Select the standard **Time Zone** based on the loop location.

Note: Step 9 to 12 is applicable only in WIN-PAK CS.

9. Select the **Communication Server** from the list.
10. Select the **Modem Pool** of the remote site.
11. Select the **Loop Callback Modem** from the list.
12. In **Loop 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. 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.

Notes:

- In WIN-PAK SE/PE, 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.
- Select the **Modem** of the remote site.

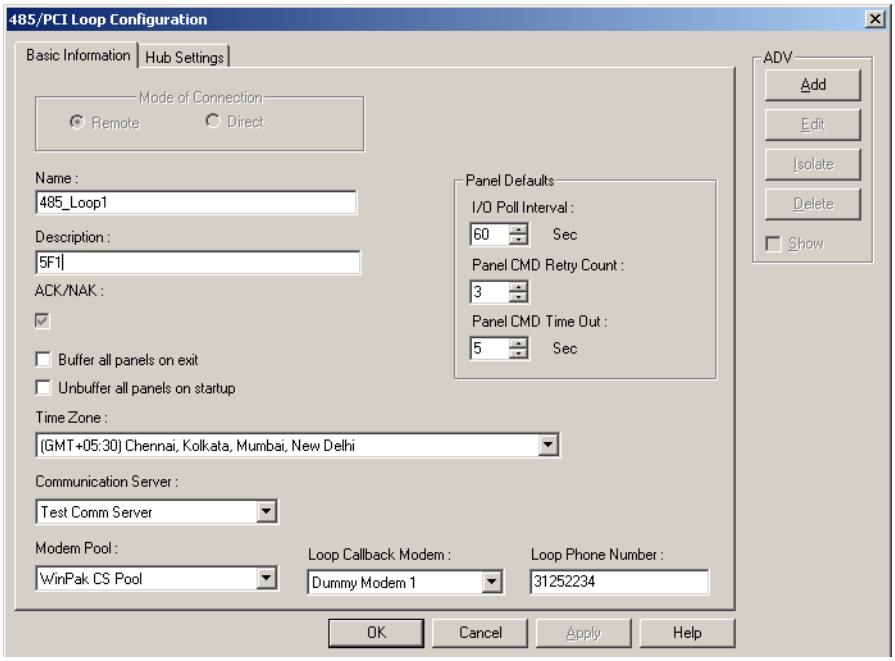
14. Click **Next** to display the **Finish** dialog box.

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.

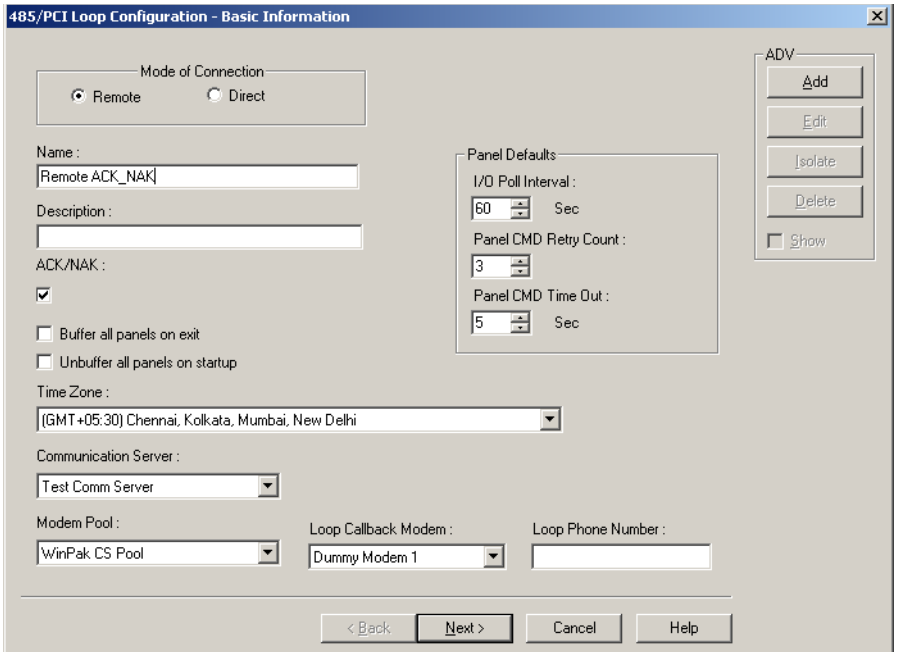
Adding a 485 ACK-NAK Remote Communication Loop

To add 485 remote connection (with ACK/NAK) to a modem pool:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.

Note: In WIN-PAK SE/PE, expand the **Device** folder and the communication server.

2. Right-click the **Devices** folder, click **Add** and click **Panel Loop (485/PCI)**. The **485/PCI Loop Configuration - Basic Information** dialog box appears.



3. Select the **Mode of Connection** as Remote.
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. Select the **ACK/NAK** check box to add an ACK/NAK loop.
7. 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: In WIN-PAK SE/PE, 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.

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.

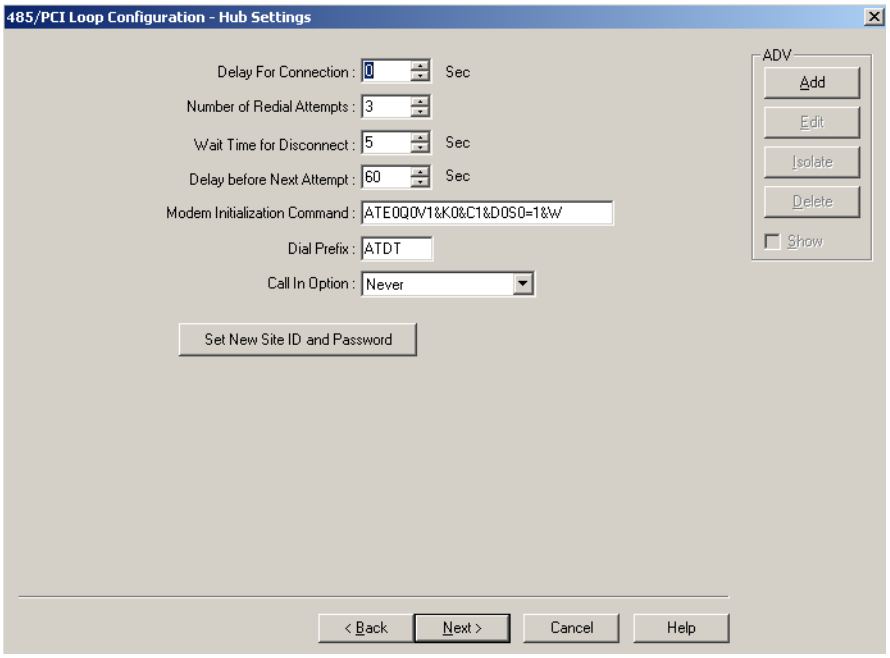
Note: Step 11 to 14 is applicable only in WIN-PAK CS.

11. Select the **Communication Server** from the list.
12. Select the **Modem Pool** of the remote site.
13. Select the **Loop Callback Modem** from the list.
14. In **Loop 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.
15. 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.

Notes: Follow the below steps in WIN-PAK SE/PE

- 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.
- Select the Modem of the remote site.

16. Click **Next** to configure the hub settings. The **485/PCI Loop Configuration - Hub Settings** dialog box appears.



17. 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 retaining the default settings.

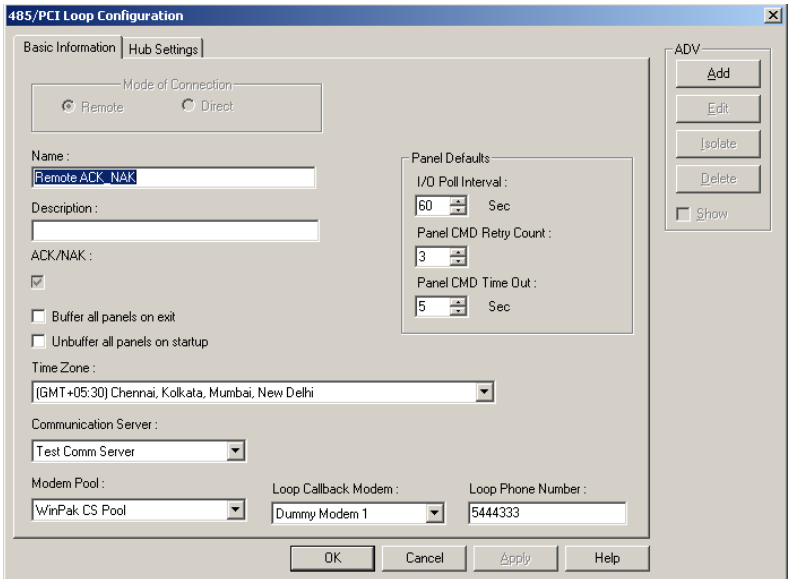
18. To set a new site ID and password, click **Set New Site ID and Password**. The **Site - Password** dialog box appears. The Site ID and password must be given while dialing-up the modem.

19. Type a **New Password**. This field is mandatory and it can be up to 20 characters.
20. Retype the password in **Confirm Password**.
21. 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.
22. Click **OK** to return to the **Hub Settings** dialog box.
23. 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.
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 **Hub 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

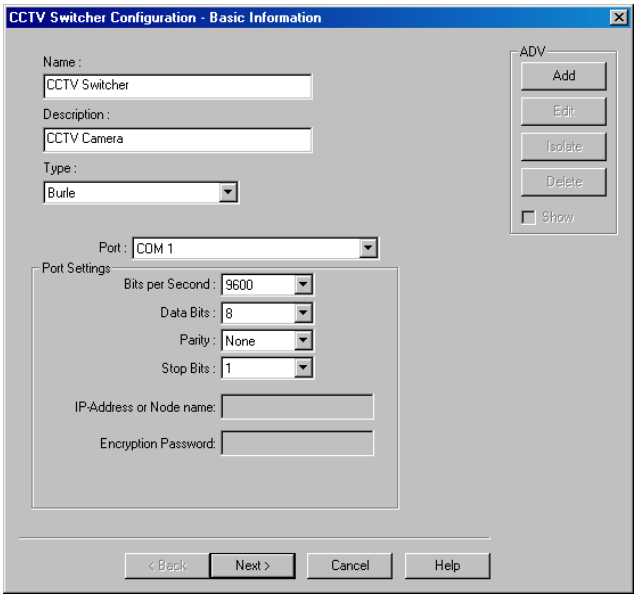
Note: This section is applicable only in WIN-PAK SE/PE.

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

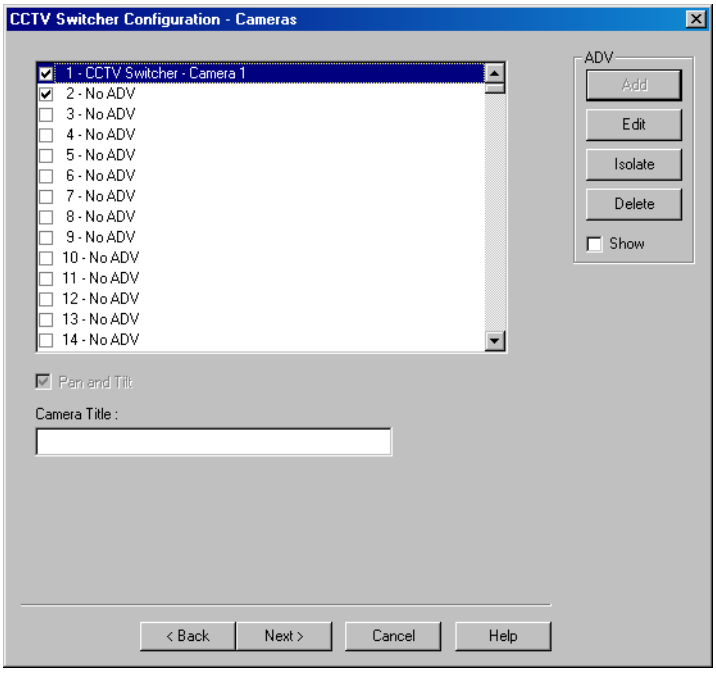
To add a CCTV Switcher:

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.



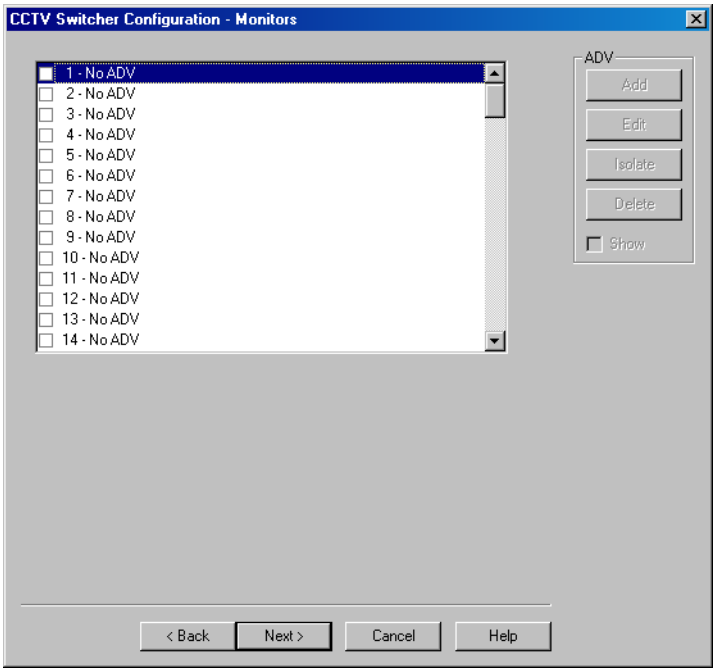
3. Type a **Name** for the CCTV switcher. This field is mandatory.
4. Type a **Description** for the CCTV switcher.
5. Select the manufacturer of the CCTV switcher in the **Type** list.

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.

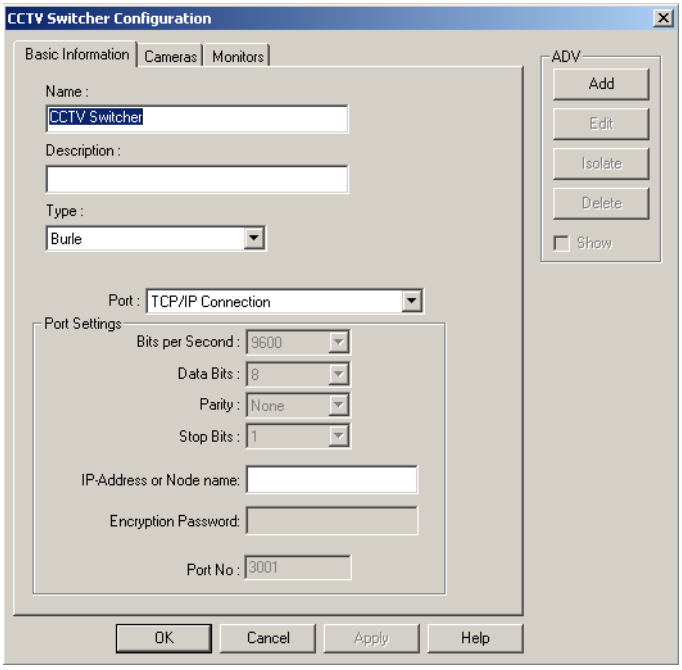


14. Select the check box to select the monitor to be controlled by this switcher.
15. Create an **ADV** for the monitor.
16. Click **Next** and in the next dialog box click **Finish**. The CCTV switcher is configured.

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.

   See the 'Adding a CCTV Switcher' section 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

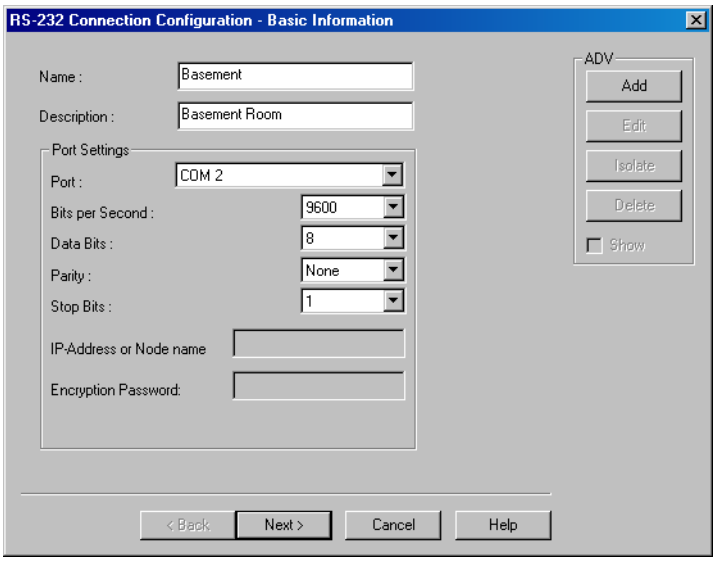
Note: This section is applicable only in WIN-PAK SE/PE.

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**.

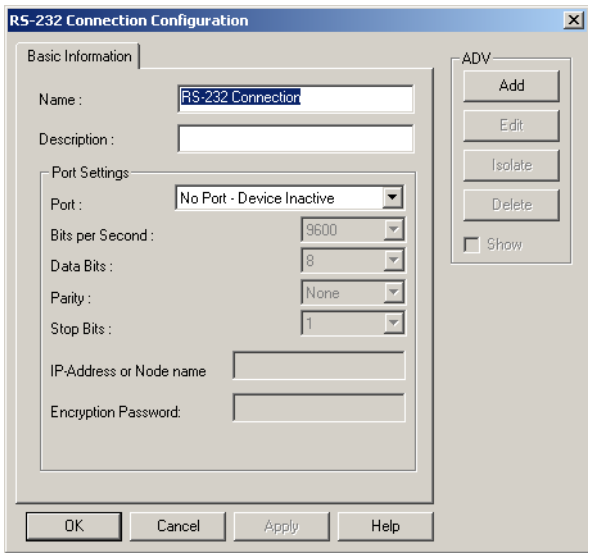
    See the 'Configuring an Abstract Device' section for more details on ADV configuration.

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.

    See the 'Adding an RS-232 Connection' section 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.

Modem Pools

Panels located at remote sites can communicate with each other and with the WIN-PAK CS/SE/PE UI, through modems. You can define modems in the modem pool and then use them to configure remote communication loops. You must have a communication server with an available com port to add a modem pool.

Modem pools are defined by adding them in the Server Configuration menu/Device Map. C-100, 485 with a HUB (non ACK/NAK), 485 with a HUB (ACK/NAK), and P-Series are the different modem pools supported by WIN-PAK CS/SE/PE. The procedure for configuring these panel loop is similar to the procedure for configuring local panel loops.

Once the modem pool is defined, you can configure a remote panel loop for the pool in the Device Map, as is the case with local or direct loops.

Note: Any modem that is supported by the Windows operating system can be used for panel communication.

Adding a Modem Pool in WIN-PAK CS

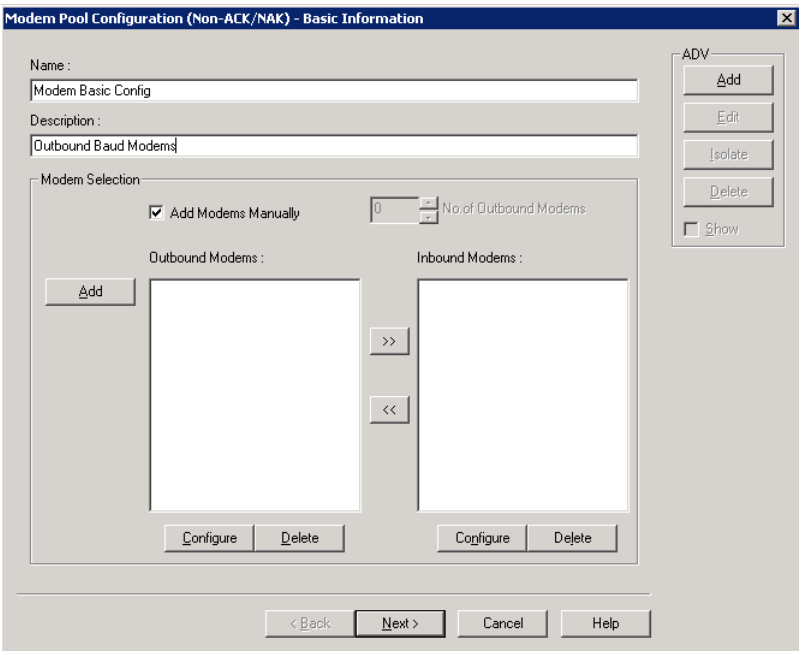
Adding a modem pool involves configuring Inbound and Outbound modems.

When configured, an Inbound modem can be used by a remote panel, to communicate to the CS. When configured as inbound, the modem enables the panel to communicate the occurrence of alarms and events to the WIN-PAK CS UI.

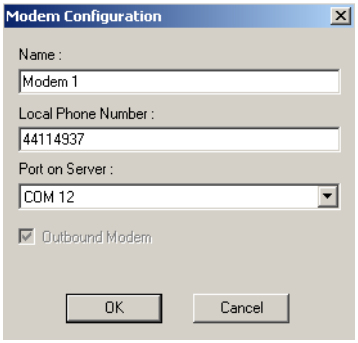
Similarly, the Outbound modem can be used by the CS to communicate with a remote panel. When configured as outbound, the modem enables you to initialize a panel from the WIN-PAK CS UI.

To add a modem pool:

1. Choose **System > Server Configuration**. The **Server** window appears.
2. Expand the **Servers** folder.
3. Right-click the communication server, choose **Add** and then select the type of modem pool connection. The **Modem Pool Configuration** 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. To enable WIN-PAK CS to add modems automatically:
    a. Clear the **Add Modems Manually** check box.
    b. Enter the number of outbound modems in the spin box.
    c. To configure the outbound modems, click **Add**. The **Modem Configuration** dialog box appears.



    d. Type a unique modem **Name** and the **Local Phone Number** for the modem. These fields are mandatory.

Note: The **Local Phone Number** for the modem is the Modem number available at the Central Station.

    e. 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, not used in any modem pool or loop is displayed.

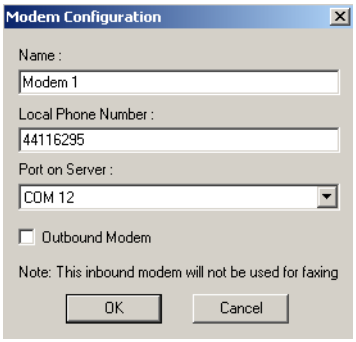
f. Click **OK** to close the **Modem Configuration** dialog box and return to **Modem Pool Configuration** dialog box.

Note: Inbound modems must be configured manually.

7. To add modems manually:

   a. Select the **Add Modems Manually** check box.

   b. Click **Add** on the left of the dialog box to add the modems to the pool. The **Modem Configuration** dialog box appears.



   c. Type a unique Modem **Name** and the **Local Phone Number** for the modem. These fields are mandatory.

   d. 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.

   e. Select the **Outbound Modem** check box to add the modem as an outbound modem or clear it to add the modem as an inbound modem.

   f. Click **OK** to close the **Modem Configuration** dialog box and return to **Modem Pool Configuration** dialog box.

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.

8. Click **Configure** to make changes to the modem information.

9. Click **Delete** to delete the modem from the list.

10. Create an ADV for the modem pool. Click **Add** under **ADV**, enter the ADV properties and click **OK**.

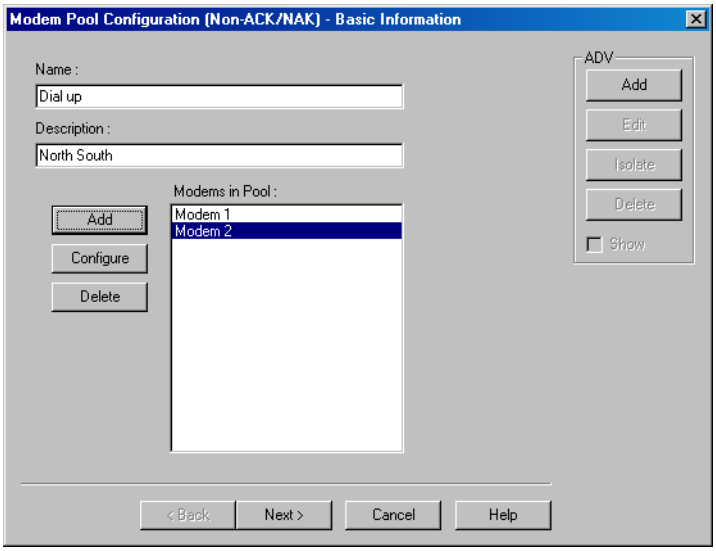
    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

11. Click **Next** and in the next dialog box click **Finish**. The modem pool is added to the Communication Server.

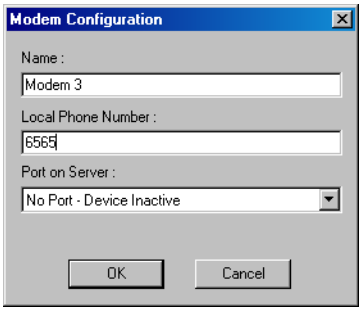
Adding a Modem Pool

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.

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**.

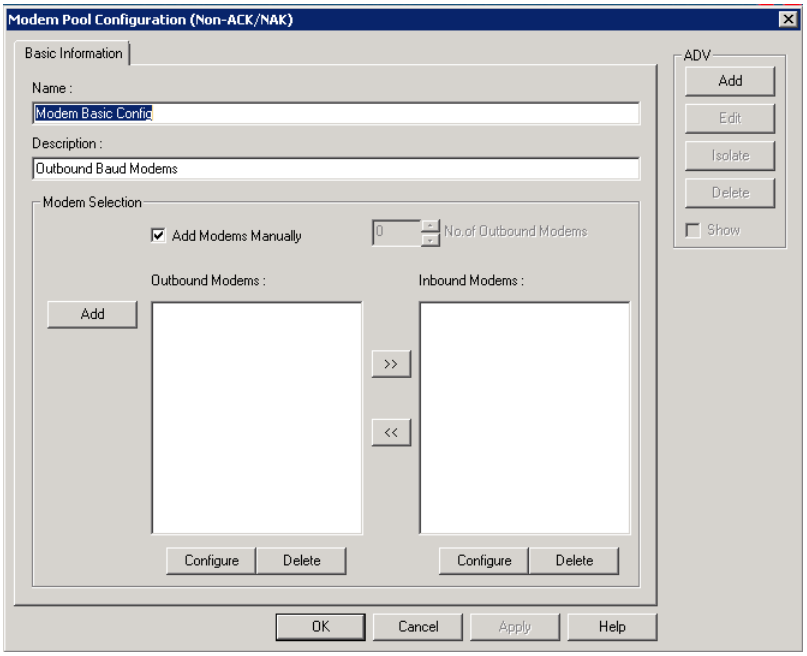
    See the 'Configuring an Abstract Device'section for more information on ADV configuration.
11. Click **Next** and in the next dialog box click **Finish**. The modem pool is added to the Communication Server.

Editing a Modem Pool

To edit a modem pool:

1. In **WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In **WIN-PAK SE/PE:** 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.
2. Expand the **Servers** folder at the top of the tree and right-click the modem pool 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.

   See the "Adding a Modem Pool in WIN-PAK CS" section in this chapter for configuring modem pool.

4. Click **OK** to configure a modem.

Isolating a Modem Pool

Note: This section is applicable only in WIN-PAK SE/PE.

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

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.

To delete a modem pool:

1. In **WIN-PAK CS**: Choose **System > Server Configuration**. The **Server** window appears.

    In WIN-PAK SE/PE: Choose **Configuration** > **Device** > **Device Map**. The Device window appears.

2. Expand the **Servers**/**Device** folder.

3. Right-click the modem pool and click **Delete**. A confirmation message appears.
4. Click **OK** to confirm the deletion. The modem pool is deleted from the device map.

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 CS/SE/PE with its configuration settings.

WIN-PAK CS/SE/PE 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 CS/SE/PE.

Notes:

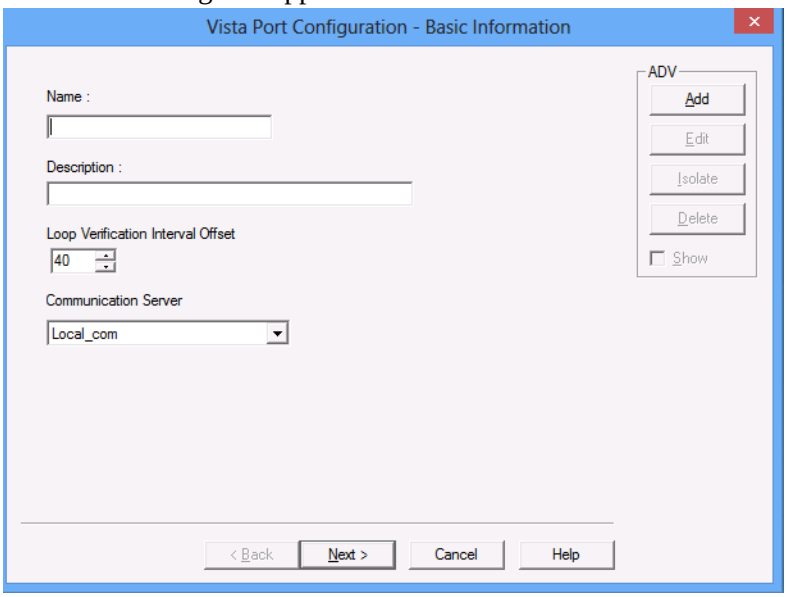
- The virtual keypad is provided in WIN-PAK CS/SE/PE that enables you to work in the Vista panel. You need to have a master code to operate on the virtual keypad.
- The Vista Turbo intrusion controllers 4100SM module is available onboard.
- WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.
- is the only applicable feature for WIN-PAK SE/PE variant.

Add a Vista Panel Port

To add a vista panel port:

1. Click **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.

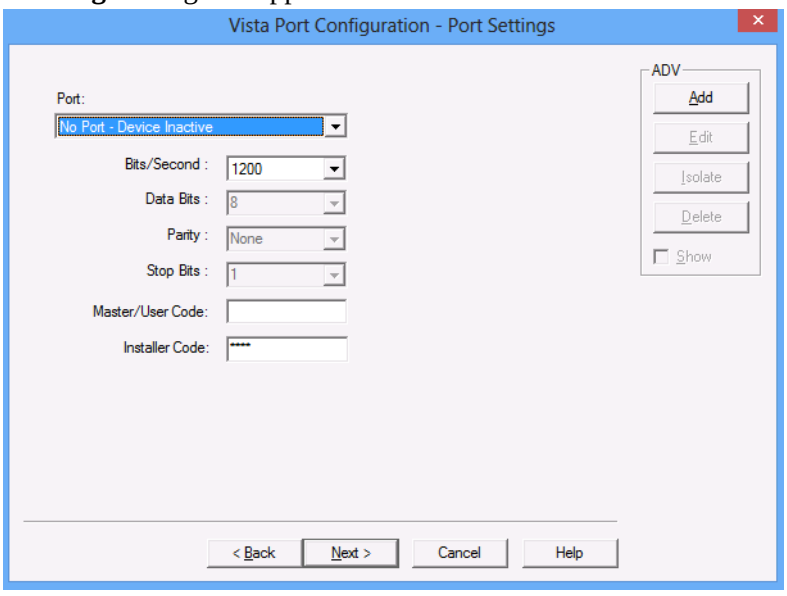


3. Type a **Name** and **Description** for the Vista panel port.

4. Set the **Loop Verification Interval (Sec)** in seconds to verify the connection between WIN-PAK CS/SE/PE and the Vista panel.

5. Create an ADV for the **Vista Port**. Click **Add** under ADV, set the ADV properties and click **OK**. See "Configuring an Abstract Device".

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 CS/SE/PE.
9. Type the **Installer Code** of the Vista panel. This enables you to change the Vista panel settings in WIN-PAK CS/SE/PE.
10. If you select the **TCP/IP Connection**, type the IP-Address or Node Name of the Micro Cobox converter. See Configuring an Abstract Device.
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. See "Add or Edit a Vista Panel".

Add or Edit a Vista Panel

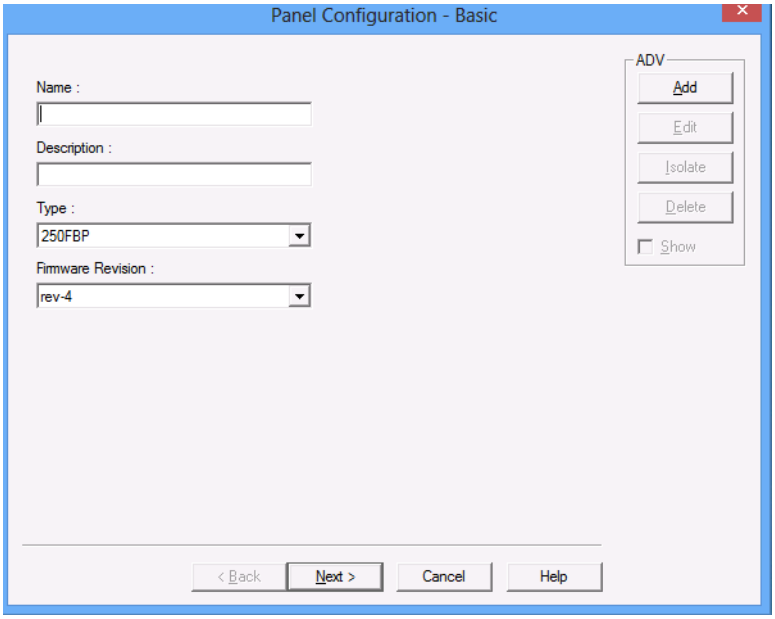
You can monitor and control intrusions using the Vista panel in WIN-PAK CS. In the Vista Panel Port, you can add only one Vista panel. To add multiple vista panels to the communication server, you must add multiple Vista Panel Ports.

To add or edit a Vista panel:

1. Click **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**.

   OR

   Right-click the **Vista** panel and click **Configure** to edit the required details. 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 CS supports two types of Fire Burglary Panels: PANEL VISTA 250FBP and PANEL VISTA 128FBP, and two types of turbo panels PANEL VISTA 128 BPT and VISTA PANEL 250 BPT.

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.

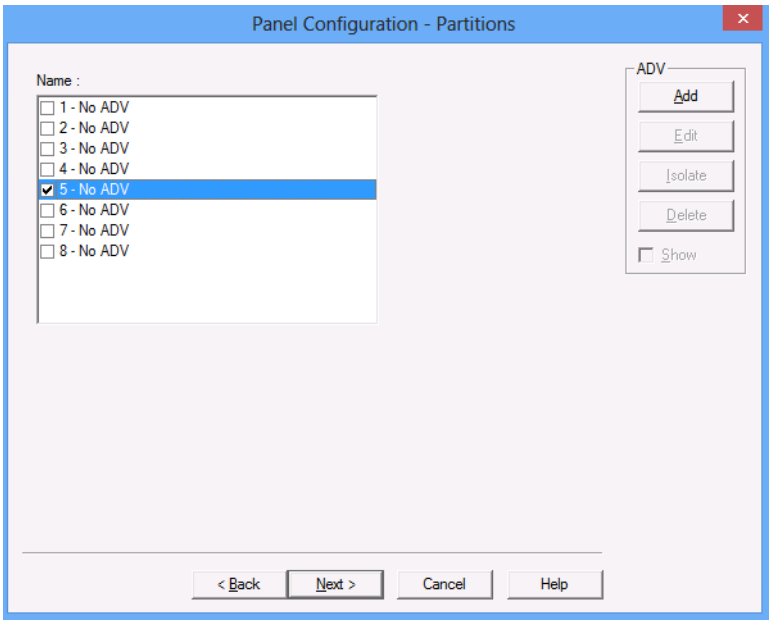
6. Click **Next** to configure the vista partitions. The **Panel Configuration - Partitions** dialog box appears.

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.

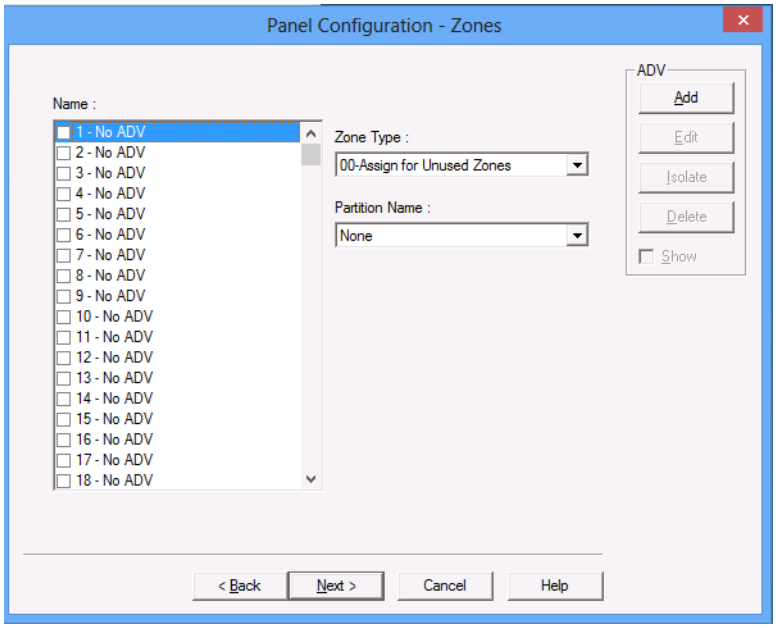


2. Click **Next** to configure the vista panel zones. The **Panel Configuration - Zones** dialog box appears.

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.

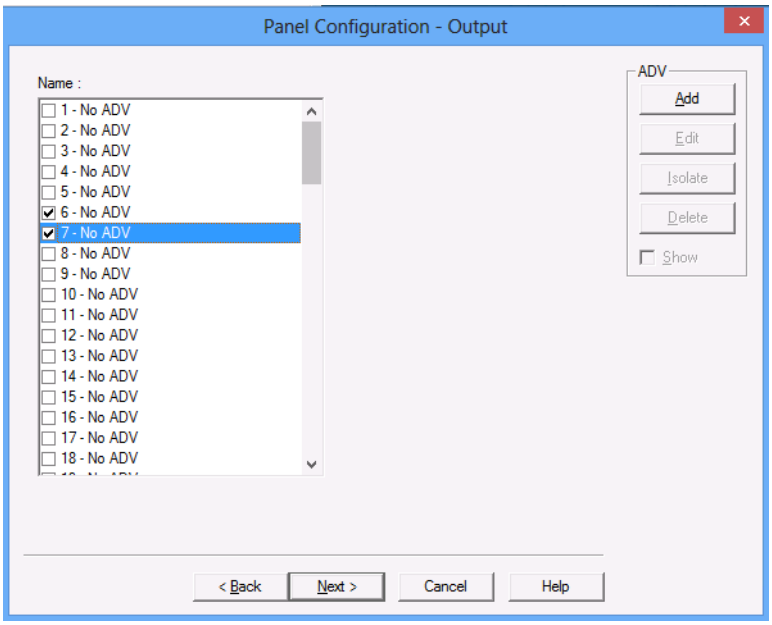


Note: The number of zones in the Name list depends on the selected panel type. In addition, the list contains three more zones for you to define the custom zone types.

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.



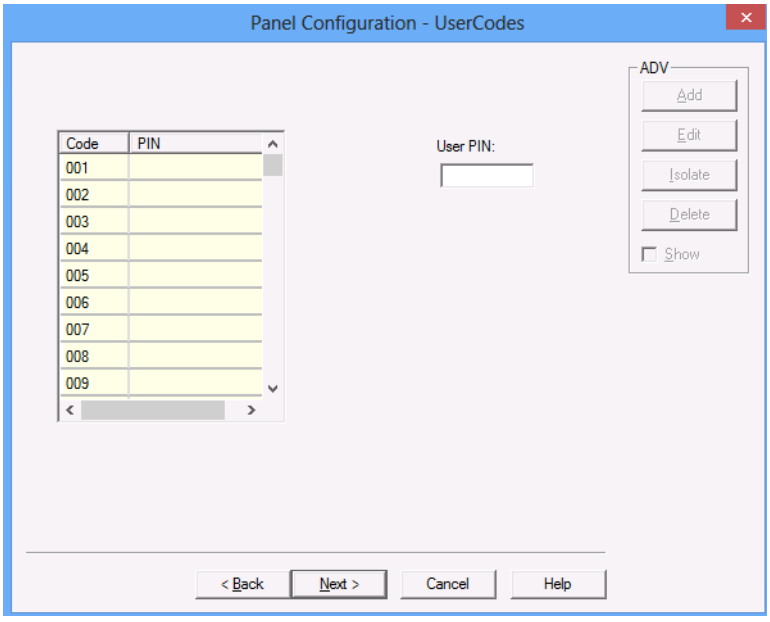
2. Click **Next** to define the user codes. The **Panel Configuration - User Codes** dialog box appears.

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 CS 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.



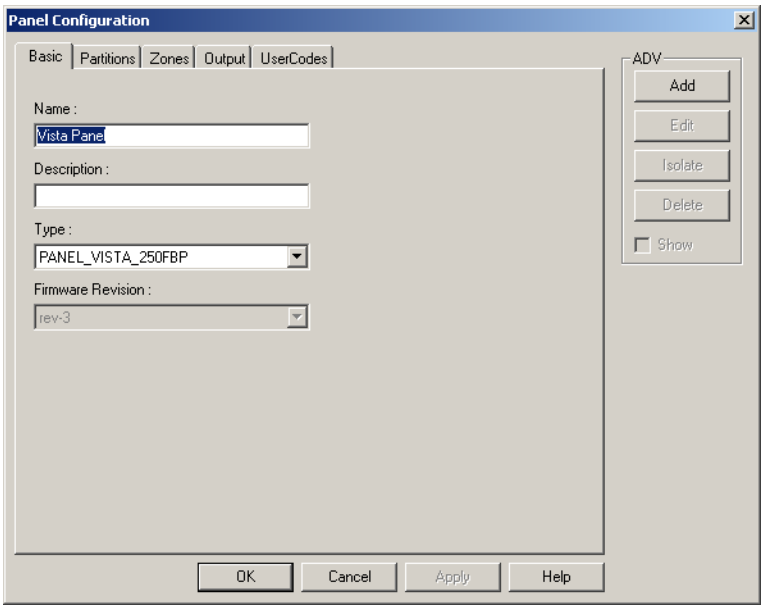
2. In the **UserPIN** box, type the password for the selected user code.
3. Click **Next** to finish the vista panel configuration. The **Panel Configuration - Finish** dialog box appears.
4. Click **Next** to configure the Vista panel.

Editing a Vista Panel

Note: This section is applicable only in WIN-PAK SE/PE.

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.

   See the 'Device Configuration' section for editing vista panel configuration details.

Isolating and deleting a Vista Panel

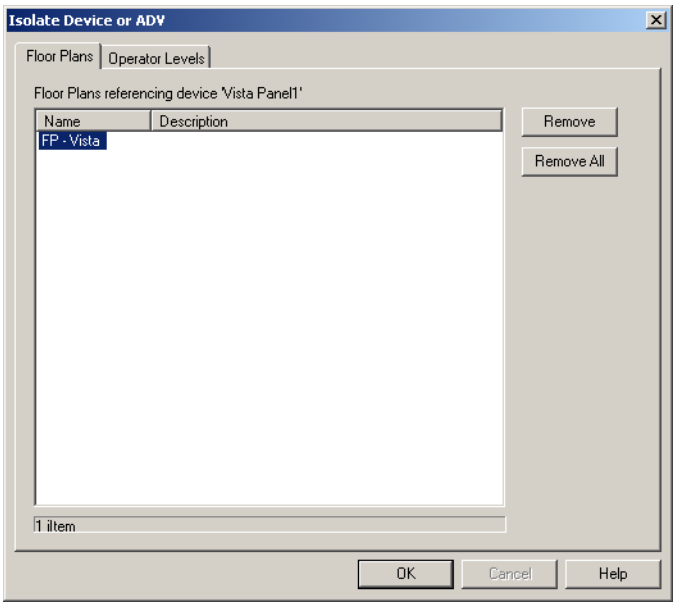
Note: This section is applicable only in WIN-PAK SE/PE.

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.

Video Management System

The Video Management System (VMS) is an enterprise-class video management and storage solution. It is a truly hybrid solution which, enables you to operate the traditional analog and IP based video equipment in the same surveillance network. Using the user interface, you can easily add cameras, recorders, and other devices. Monitoring locations is more effective through features like color correction, digital zoom, and others. Events such as failure of camera or loss of video can be logged. You can retrieve and view video pertaining to specific events. In addition, you can configure alarms to notify the operators when events are triggered.

The Video Management Server channel server information must be added to the device map folder to perform the basic video surveillance operations.

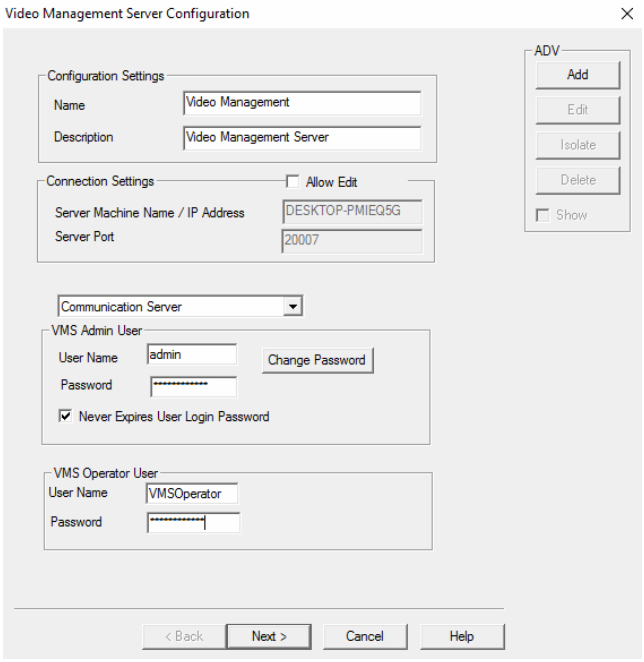
Adding a Video Management Server

To add a Video Management Server:

1. In **WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In **WIN-PAK SE/PE:** Choose **Configuration** > **Device** > **Device Map**. The Device window appears.

2. Right-click the **Servers/Device** folder and choose **Add > Video Management Server**. The **Video Management System Configuration** dialog box appears.



3. Type the **Name** of the server.
4. Type the **Description** for the server.
5. The information in the following fields appears by default.
   - **Server Machine Name/IP1 Address (Local Computer Host Name)**
   - **Server Port (Default Video Management Server Port: 20007)**

Note: The **Video Management Server** must be installed on the WIN-PAK database server.

6. Select the **Allow Edit** check box, edit the **Server Machine Name/IP Address**, and the **Server Port**, as applicable.
7. Select the **Communication Server (to receive alarms)** from the drop-down list.
8. Click Add under ADV to create an ADV for the Video Management Server. **The Abstract Device Record** dialog box appears.

   See "Configuring an Abstract Device" for information on ADV configuration.
9. After adding an ADV, click **OK** to return to the **Video Management System Configuration** dialog box.
10. Enter the **VMS Admin User** credential.
11. Select the **Never Expires User Login Password** check box to ensure that password never expires.
12. Enter the **VMS Operator User** credential.

13. Click **Next.**

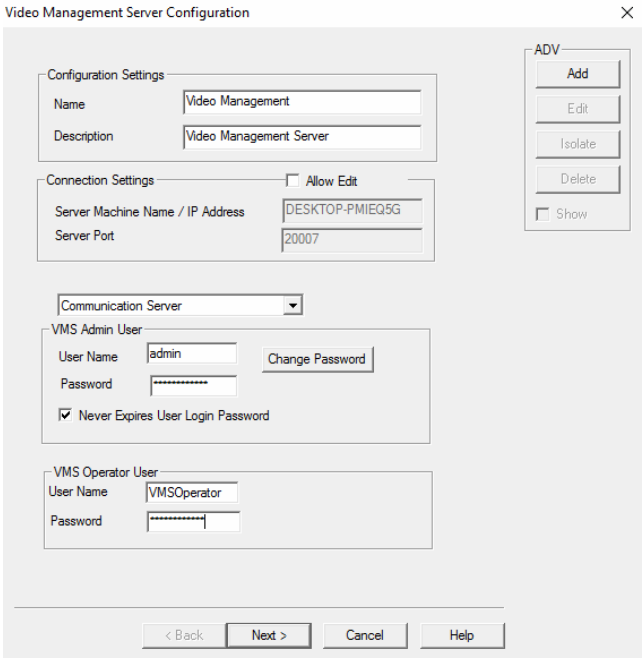
Editing a Video Management Server

To edit the Video Management Server:

1. In **WIN-PAK CS:** Choose **System > Server Configuration**. The **Server** window appears.

   In **WIN-PAK SE/PE:** Choose **Configuration** > **Device** > **Device Map**. The Device window appears.Choose **System > Server Configuration**. The **Server** window appears.

2. Right-click the **Servers/Device** folder and choose **Add > Video Management Server**. The **Video Management System Configuration** dialog box appears.



3. Click the corresponding tab and make the required changes.

   Refer to the "Adding a Video Management Server" section in this chapter for adding a Video Management Server.

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

Note:

- Under ADV, use the **Edit**, **Isolate**, and **Delete** buttons to edit, isolate and delete the ADV.
- Select **Show** to view the ADV details.

Connect

You can connect WIN-PAK server to Video Management Server using the Connect option.

To connect to a Video Management Server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Video Management Server** and choose **Connect**.

Note: The **Connect** option is enabled only when WIN-PAK is not connected to the Video Management Server.

Synchronize Event Types

This option helps you to synchronize all the Video Management Server event types to WIN-PAK.

To synchronize Video Management Server event types:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click **Video Management Server** and choose **Synchronize Event Types**.
   All the event types supported for recorder, cameras, input/output in Video Management Server are imported to the WIN-PAK database.

Note: If new device drivers are installed, you must manually synchronize event types using this option.

Deleting Video Management Server

You can delete a Video Management Server when you do not want to record video from the Video Management Server. All the associations made to the Video Management Server is removed, when you delete it.

Before you begin

From ADV, you must isolate and delete all the associations with the cameras, input, output, and recorders.

You must delete all the recorders before deleting the Video Management Server. To delete the recorder, ensure that you have deleted all the associated devices.

To delete a Video Management Server:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Video Management Server** and choose **Delete**. A dialog box appears.
3. Click **OK** to delete the Video Management Server.

Recorder Configuration

Recorders are devices used for streaming video and recording video from surveillance cameras (analog cameras and IP based digital cameras).

Recorders and Events

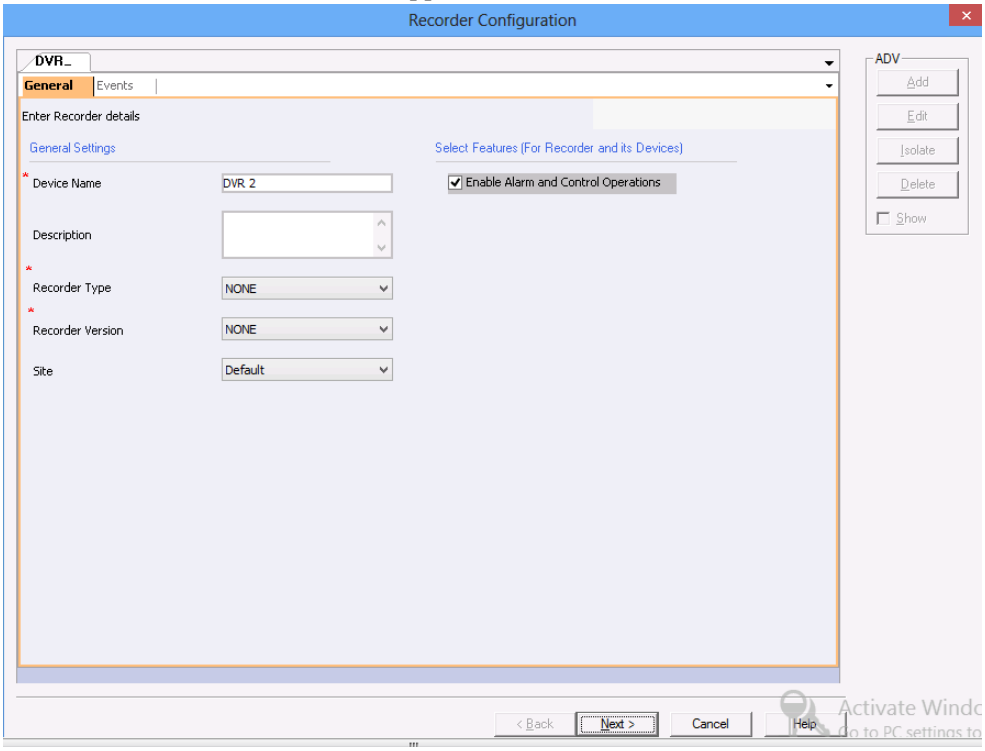
Events are predefined actions. Recorders have predefined events by default. An alarm is triggered whenever an event is generated. For example, when a recorder is disconnected from network, an event 'RecorderDisconnected' is generated.

Adding a Recorder

Recorders are devices used for streaming video and recording video from surveillance cameras (analog cameras and IP based digital cameras) Events are predefined actions. Recorders have predefined events by default and an alarm is triggered whenever an event is generated.

To add a recorder:

1. Choose C**onfiguration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Video Management Server** folder and choose **Add > Recorder**. The **Video Management Server Recorder Configuration** dialog box for the selected server appears.



3. Enter the **Recorder** details under **General Settings**.
4. In the **Device Name** box, type a name for the recorder.
5. In the **Description** box, type a description for the recorder.
6. In the **Recorder Type** drop-down list, select the recorder. Device settings for the selected recorder appears.

For example, if you select "Fusion" as the recorder type, configure the device settings for the selected recorder.

Table 9-3 Recorder Type

Recorder Type	To configure the device settings
Fusion	• In the **Site Address** box, type the numeric IP address or the host name of the Fusion recorder. Click Ping to verify the connection. The field appears in green if the IP address or the host name is valid. • Select the **Check duplicate hostname** to check the availability of the host name. • In the **Site Port** box, the port number appears by default. • In the **User ID** box, type the user name to access the recorder. • In the **Password** box, type the assigned password for the user. • Click the **Time Zone** check box to enable the global time zone box and select the required time zone.
HRDP	• In the **Site Address** box, type the numeric IP address or the host name of the HRDP recorder. Click **Ping** to verify the connection. The field appears in green if the IP address or the host name is valid. • Select the **Check duplicate hostname** to check the availability of the host name. • In the **Site Port** box, the port number appears by default. • In the **User ID** box, type the user name to access the recorder. • In the **Password** box, type the assigned password for the user. • In the **Device Type** drop-down list, select the device type as applicable. • Click the **Time Zone** check box to enable the global time zone box and select the required time zone.

Table 9-3 Recorder Type

Recorder Type	To configure the device settings
MAXPRO NVR	• In the **Unit Address** box, type the numeric IP address or the host name of the MAXPRO NVR recorder. Click **Ping** to verify the connection. The field appears in green if the IP address or the host name is valid. • Select the **Check for duplicate IP address/ device name** to check the availability of the host name. • In the **Site Port** box, the port number appears by default. • In the **User Name** box, type the user name to access the recorder. • In the **Password** box, type the assigned password for the user.
RapidEye	• In the **Unit Address** box, type the numeric IP address or the host name of the RapidEye recorder. Click **Ping** to verify the connection. The field appears in green if the IP address or the host name is valid • Select the **Check for duplicate IP address/ device name** to check the availability of the host name. • In the **Site Port** box, the port number appears by default. • In the **System Password** box, type the password to access the recorder. • In the **Video Format** drop-down list, select "NTSC" or "PAL" as applicable.

7. In the **Recorder Version** drop-down list, select the recorder version.
8. In the **Site** drop-down list, select the site to which the recorder is to be associated. See "Associating events and event attributes to a recorder" for more details.
9. Click **Next**. A message appears displaying that the recorder details are saved.
10. Click **Yes** to begin with the discovery of all the associated devices. See "Discover Devices".

    Or

    Click **No** to manually add the devices. For more information, see 'Camera Configuration', 'Recorder Input Configuration', and 'Recorder Output Configuration'.
11. Click **Add** under ADV to create an ADV for the Recorder. The **Abstract Device Record** dialog box appears.

See "Configuring an Abstract Device" for information on ADV configuration.

12. After adding an ADV, click **OK** to return to the **Video Management Server Recorder Configure** 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.

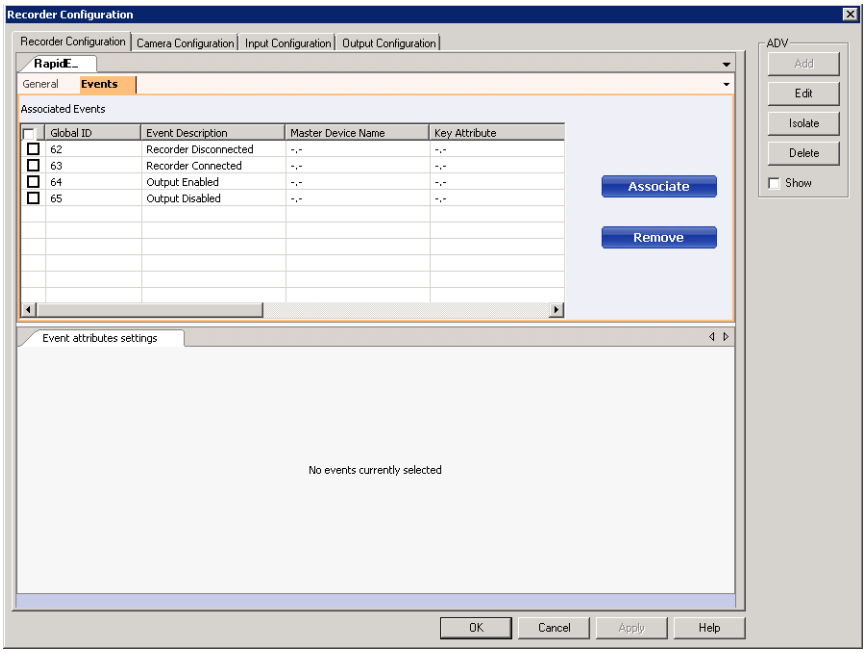
Associating Events and Event Attributes to a Recorder

You can associate one or more events to a recorder. An alarm is triggered whenever any of the associated event occurs for the recorder. For certain events, you can also associate event attributes. For example, for an Encoder Disabled event, you can associate attributes such as Encoder Name, Encoder ID and so on. For every attribute that you associate, you can set a value based on which the event is triggered. In the above example, you can associate the attribute Encoder Name to the event and set its value as Encoder A. When this event is associated to the recorder, an alarm is raised when the event "Encoder Disabled" occurs for the Encoder Name "Encoder A".

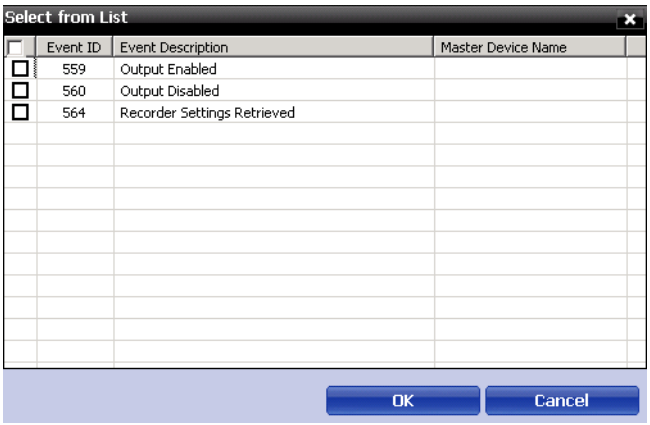
Attributes are available only for certain events. These events can be associated to a recorder multiple times. The event attributes are listed in the details of the alarm in Alarm window. To view the event attributes of an alarm, right-click the alarm, and then click **Show Details**.

To associate events to a recorder:

1. Click the **Events** tab. The screen displays the associated events if any.



2. Click **Associate**. The **Select from List** dialog box appears.



3. Select the check box corresponding to the event you want to associate.
4. Click **OK**.

To disassociate events from a recorder:

- Select the check box corresponding to the event, and then click **Remove**.

To assign severity level:

1. Select the check box corresponding to the event you want assign severity level.
2. Double-click on the **Severity Level (priority**) box and edit the severity level. 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**.

To enter remarks:

1. Select the check box corresponding to the event you want to enter remarks.
2. Click the **Remarks** box and type the remarks.

Notes:

- The remarks for the corresponding event is reflected in the WIN-PAK UI.
- Ensure that you retain the information in the remaining fields to their default settings.

Associating Event Attributes

To associate event attributes:

1. Select the check box corresponding to the event for which you want to associate event attributes. The **Event attributes Settings** appear in the lower pane.
2. Click **Associate**. The **Select Available Event Attributes** dialog box appears.
3. Select the check box corresponding to the event attributes that you want to associate.
4. Click **OK**.

To disassociate event attributes from a recorder:

- Select the check box corresponding to the event attribute, and then click **Remove**.

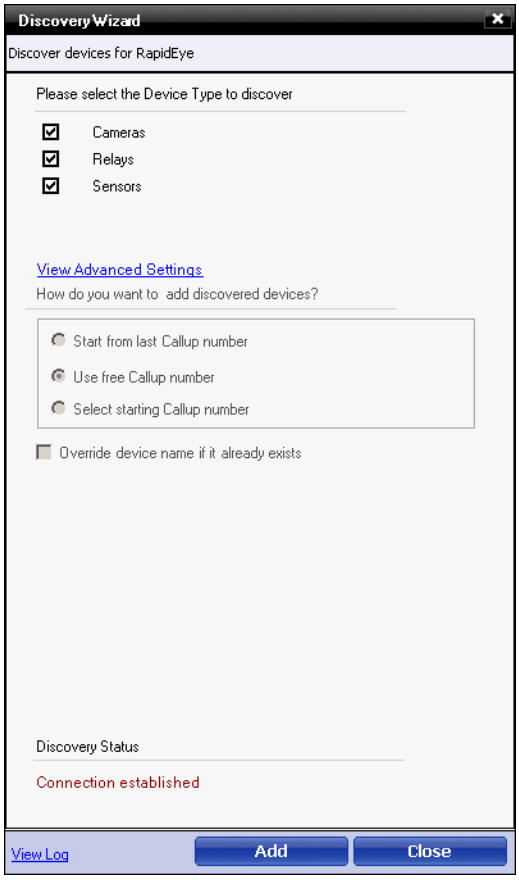
Discover Devices

Discover devices helps you to connect the video server to the recorder, and retrieve all the cameras, inputs, and relays that are configured in the recorder.

All the discovered devices are automatically included in WIN-PAK. You must associate ADV's for the devices that are to be used.

To discover input and output devices:

1. Click **Discover Devices** under **Device Settings** in the **Video Management Server Recorder Configure** dialog box. The **Discovery Wizard** dialog box appears.



2. Under **Please select the Device Type to discover,** select the check boxes for the device types that you want to discover.
3. Click **View Advanced Settings** to configure the advanced settings and the order of the discovered devices.

Settings	Instructions
Start from last Callup number	Select this option if you want to add the device from the last callup number of the device type that has been selected.
Use free Callup number	Select this option to use the available callup number in the device type that has been selected.
Select starting Callup number	Type the starting callup number, and then choose an option from If Callup number already exists, what do you want to do? section. See step 7.

Settings	Instructions
Override device name if it already exists	Select this check box to override the existing device name. The override device gets the name configured in the recorder and uses the same name while adding devices such as cameras, inputs, and outputs.

4. Click **Add** to add the devices.
5. Click **Close** after the "Discovery completed" message appears in the **Discovery Status** section.
6. Click **View Discover Log** to view logs if any.

Editing a Recorder

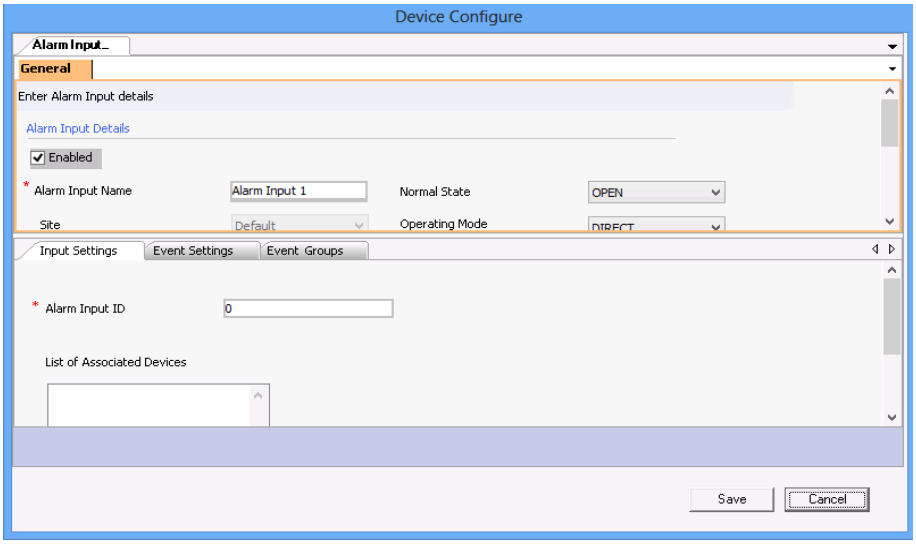
To edit a recorder:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Video Management Server**, right-click a recorder and select **Configure**. The **Digital Video Configuration** window appears with two/four tabs.
3. Click the appropriate tab to make the necessary changes to the configuration settings.
4. Click **Apply** to save the settings.

Recorder Input Configuration

You can add an alarm input and associate it to the devices. These alarm inputs trigger alarms whenever an event occurs.

1. In the **Input Configuration** tab, under **General Settings**, click **Add**. The **Device Configure** dialog box appears.



2. Select the **Enabled** check box to enable the alarm.
3. In the **Alarm Input Name** box, type the alarm input name.
4. From the **Site** drop-down list, select the required site.
5. In the **Normal State** drop-down list, select **Open** or **Closed** as the normal state for the alarm input.
6. From the **Operating Mode** drop-down list, select the required mode. The available modes are listed in the following table.

Table 9-4 Operating mode

Modes	Description
Direct	The alarm condition activates or de-activates when it physically changes state, or is set or cleared with macros.
Latched	Once the alarm is triggered, it remains active until it is reset manually using the alarm clear option.
Toggle	Once the alarm is triggered, it remains active until it is reset manually using the alarm clear option.

7. In the **Connected To** section, click one of the devices for which you want to add the alarm input. The following table lists the available devices to which an Alarm Input can be connected.

Table 9-5 Available device

Device	Description
Recorder	For details on connecting a recorder, see 'Connect an alarm input to a recorder'.

8. Select **Link** if you want to broadcast the status changes and actions performed on the current alarm input on the network.
9. See 'Connect an alarm input to a recorder' to change the **Input Settings** and **Event Settings**.
10. Click **Save**.

Note: **Note**: You can switch on or switch off an alarm input using the **On** and **Off** buttons under **Trigger Alarm Input**.

Connect an Alarm Input to a Recorder

Note: This section is applicable only in WIN-PAK SE/PE.

To connect alarm input to a recorder:

1. The **Recorder** drop-down list by default displays the recorder name.
2. Configure the recorder settings under the following three tabs: **Input Settings**, **Event Settings**, and **Event Groups**.
3. In the **Input Settings** tab, type the **Alarm Input ID**.
4. In the **Event Settings** tab, specify the details listed in the following table.

Settings	Instructions
Event Description	Type a event description for the event.
Global ID	Type the unique global ID. If the Global Event ID is not assigned, WIN-PAK assigns a unique global ID automatically when you save the event settings.
Severity	Type the severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set to 50 on the preferences tab, an alarm is triggered when threshold becomes 51.
Start Macro and End Macro	These fields are reserved for future releases of WIN-PAK.

5. The Information in the **Event Groups** tab is reserved for future releases of WIN-PAK.
6. Click **Save**.

Edit Input Settings

To edit the input settings:

1. Under **General Settings**, select the input to be edited and click **Edit**.
2. Edit the required details. The settings for the selected input is changed.
3. Click **Save** to save the settings.

Delete Inputs

To delete inputs:

1. Under **General Settings**, select the input to be deleted and click **Delete**.
2. Click **OK**. The selected input is deleted.

Note: **Note**: Click **Refresh** to refresh the list of available inputs.

To Add/Delete bulk ADV

Note: This section is applicable only in WIN-PAK CS.

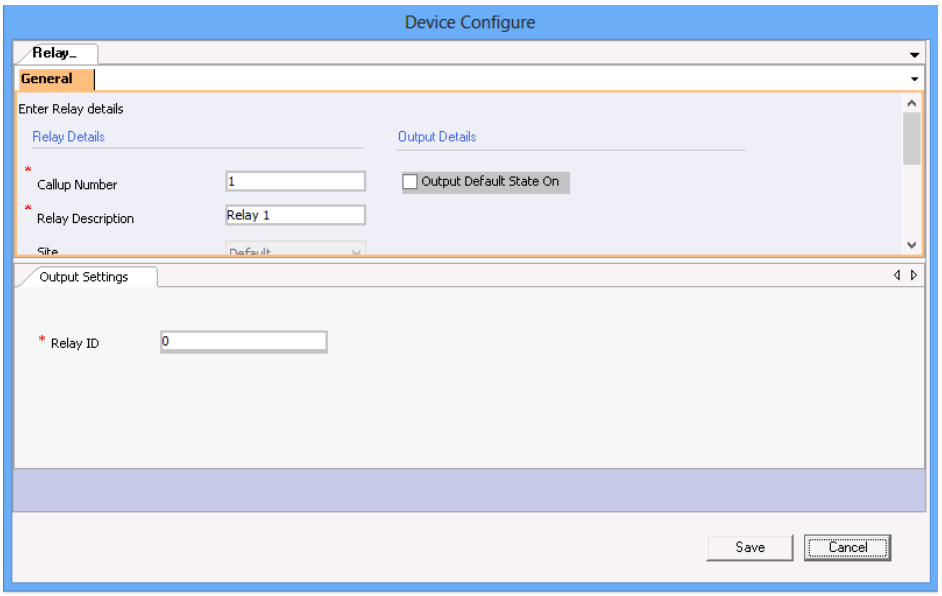
To add/delete bulk ADV:

- Under **ADV Operations**, click
  - **Add ADV**, to add ADV's for all the cameras if it is not added. During Bulk Add Operations, any cameras where ADV has already been added manually, remains unchanged.
  - **Delete ADV**, to delete ADV's for all the cameras.

Recorder Output Configuration

You can add an alarm output and associate it to the devices.

1. In the **Output Configuration** tab, under **General Settings**, click **Add**. The **Device Configure** dialog box appears.



2. In the **Callup Number** box, an automatic number is allocated by default. The operator uses this number to select the output device from the keyboard.
3. In the **Relay Description** box, type a description for the relay.
4. In the **Site** box, select the location in which the output device is used.

5. In the **Connected To** section, click one of the devices from which you want to add a relay. The following table lists the available devices to which a relay can be connected.

Table 9-6 Available device

Device	Description
Recorder	For details on connecting a recorder, see 'Connect relay to a recorder'.

6. Select **Output Default State On** if you want the relay to be set to **On**, when the Video Management Server is started.
7. Click **Save**. The **Trigger Relay** options appear.
8. See 'Connect relay to a recorder' to change the **Output Settings**.
9. Click **On** to trigger relay.
10. Click **Off** to trigger relay.

Connecting a relay to the recorder

To connect relay to a recorder:

1. The **Recorder** drop-down list displays the name of the recorder that is configured. The **Output Settings** appear in the Output Settings tab.
2. In the **Relay ID** box, type the relay ID number for the recorder.

Edit Output Settings

Note: This section is applicable only in WIN-PAK CS.

To edit the output settings:

1. Under **General Settings**, select the output to be edited and click **Edit**.
2. Edit the required details. The settings for the selected output is changed.
3. Click **Save** to save the settings.

Delete Outputs

Note: This section is applicable only in WIN-PAK CS.

To delete outputs:

1. Under **General Settings**, select the output to be deleted and click **Delete**.
2. Click **OK**. The selected output is deleted.

Note: Click **Refresh** to refresh the list of available outputs.

To Add/Delete bulk ADV

Note: This section is applicable only in WIN-PAK CS.

To add/delete bulk ADV:

- Under **ADV Operations**, click
  - **Add ADV**, to add ADV's for all the cameras if it is not added. During Bulk Add Operations, any cameras where ADV has already been added manually, remains unchanged.
  - **Delete ADV**, to delete ADV's for all the cameras.

Connect an alarm input to a recorder

Note: This section is applicable only in WIN-PAK CS.

To connect alarm input to a recorder:

1. From the **Recorder** drop-down list, select the required recorder. The recorder settings appear.
2. In the **Alarm Input ID** box under **Input Settings** tab, type the **Alarm Input ID**.
3. On the **Event Settings** tab, specify the following details:

Table 9-7 Event Settings

Device	Description
Event Description	Type an event description for the event.
Global ID	Type the unique global ID. If the Global Event ID is not assigned, MAXPRO™ VMS assigns a unique global ID automatically when you save the event settings.
Severity	Type the severity level. **Note:** Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set to 50 on the preferences tab, an alarm is triggered when threshold is 51.

4. Click **Save**.

Connect relay to a recorder

Note: This section is applicable only in WIN-PAK CS.

To connect relay to a recorder:

1. From the **Recorder** drop-down list, select the required recorder. The **Output Settings** appear.

2. In the **Relay ID** box, type the relay ID number for the recorder.

Deleting a Recorder

You can delete a recorder only after you delete the devices attached to the recorder. In addition, you must isolate the ADV of the recorder from floor plans and operator levels.

Note: If you delete a recorder, all the associated cameras, inputs/outputs, and recorders are deleted. A warning message appears if an ADV is associated in the Control Map/Floor Map.

Associating events and event attributes to a recorder

Note: This section is applicable only in WIN-PAK CS.

You can associate one or more events to a recorder. An alarm is triggered whenever any of the associated event occurs for the recorder. For certain events, you can also associate event attributes. For example, for an Encoder Disabled event, you can associate attributes such as Encoder Name, Encoder ID and so on. For every attribute that you associate, you can set a value based on which the event is triggered. In the above example, you can associate the attribute Encoder Name to the event and set its value as Encoder A. When this event is associated to the recorder, an alarm is raised when the event “Encoder Disabled” occurs for the Encoder Name “Encoder A”.

Attributes are available only for certain events. These events can be associated to a recorder multiple times. The event attributes are listed in the details of the alarm in **Alarm** window. To view the event attributes of an alarm, right-click the alarm, and then click **Show Details**.

To associate events to a recorder:

1. Click the **Events** tab. The screen displays the associated events if any.
2. Click **Associate**. The **Select From List** dialog box appears.
3. Select the check box corresponding to the event you want to associate.
4. Click **OK**.

To disassociate events to a recorder:

- Select the check box corresponding to the event, and then click Remove.

To assign severity level:

1. Select the check box corresponding to the event you want assign severity level.
2. Double-click on the **Severity Level** (priority) box and edit the severity level. 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 acknowledgment** 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 acknowledgment** field.
- The action is considered as an event, if the action priority is greater than the value in the **Alarm Priority for required acknowledgment**.

To enter remarks:

1. Select the check box corresponding to the event you want to enter remarks.
2. Click the **Remarks** box and type the remarks.

Notes:

- The remarks for the corresponding event is reflected in the WIN-PAK UI.
- Ensure that you retain the remaining fields to default settings.

Associating Event Attributes

Before you begin follow the steps from "Associating events and event attributes to a recorder" section.

To associate event attributes

1. Select the check box corresponding to the event for which you want to associate event attributes. The **Event attributes Settings** appear in the lower pane.
2. Click **Associate**. The **Select Available Event Attributes** dialog box appears.
3. Select the check box corresponding to the event attributes that you want to associate.
4. Click **OK**.

To disassociate event attributes from a recorder:

- Select the check box corresponding to the event attribute, and then click **Remove**.

Discover Devices

Note: This section is applicable only in WIN-PAK CS.

Discover devices enables the video server to connect to the DVR and retrieve all the cameras, inputs, and relays that are configured in the recorder. Later, all the discovered devices are automatically included in WIN-PAK CS. You must associate ADV's for the devices that are to be used.

To discover input and output devices:

1. Click **Discover Devices** under **Device Settings** in the **Video Management Server Recorder Configure** dialog box. The **Discovery Wizard** dialog box appears.
2. Select the device type or devices that you want to discover.
3. Click **View Advanced Settings** to configure advanced settings and to specify the order of discovered devices:

Table 9-8 Discover Devices

Settings	Instruction
Start from last Callup number	Select this option if you want to add the device from the last callup number of the device type that has been selected.
Use free Callup number	Select this option to use the available callup number in the device type that has been selected.
Select starting Callup number	Type the starting callup number, and then choose an option from If Callup number already exists, what do you want to do? section. See step 7.
Override device name if it already exists	Select the option to override the device name that already exits. The override device gets the name configured in the recorder and uses the same name while adding devices such as cameras, inputs, and outputs.

4. Click **View Discover Log** to view any log.
5. Click **Close** after the "Discovery Completed" status appears in the **Discovery Status** section.

Camera Configuration

Adding a camera involves defining the camera's set up and operation across switchers and recorders. You can update or configure the general settings of a camera to configure PTZ settings and connect a camera to a recorder. After configuring the basic DVR details, you must configure settings for the cameras in the Camera Configuration dialog box.

Camera configuration involves three sections:

- "General Settings"
- "PTZ Settings"
- "Recording Settings"

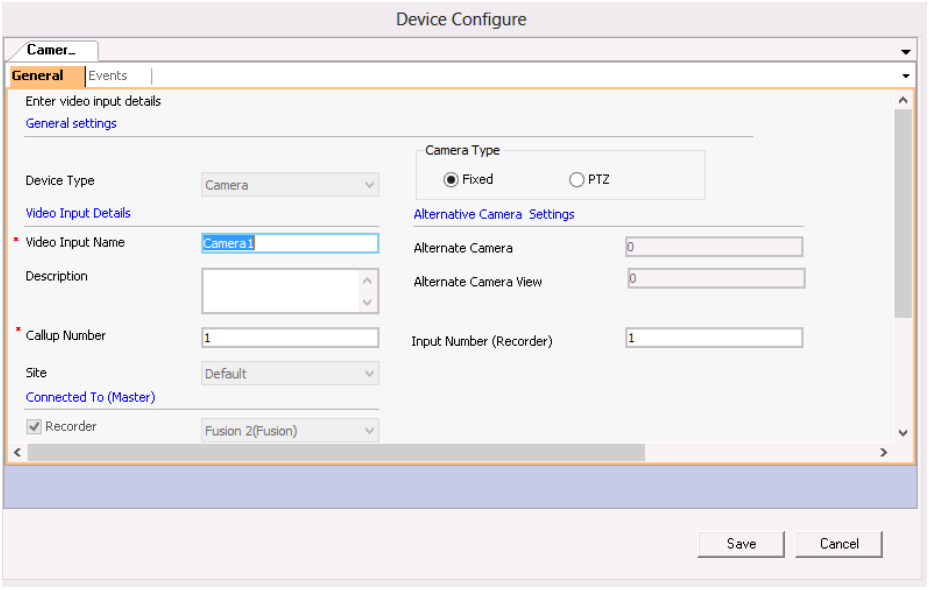
General Settings

You can add, edit, and delete cameras.

Adding a Camera

To add a camera:

1. Click **Add** under **General Settings**. The **Device Configure** dialog box appears.



2. In the **Camera Type** area, click **PTZ** if the configured camera is **PTZ** or click **Fixed** if the configured camera is fixed.
3. In the **Video Input Details** area, specify the camera details listed in the following table:

Table 9-9 Video Input Details

Field	Description
Video Input Name	Type a camera name. The camera name appears in the devices window making it easy to select.
Description	Type a description for the camera.
Callup Number	A unique number that identifies the camera. By default, the next available number is allocated.
Site	Location of the camera. **Note:** You cannot edit the Site field.

4. In the **Alternative Settings** area, specify the following details.:

Table 9-10 Video Input Details

Settings	Description
Alternate Camera	Type the number of the camera that has to be selected. You can select the Alternate Camera option from the context menu while playing or viewing live video. The range of valid camera numbers is 1 – 999999999. Zero (0) is the default value, and indicates no alternate camera is defined.

5. In the **Connected To (Master)** area, select **Recorder**, if you want to connect the camera to a recorder.
6. You can change the **Input Number (recorder)**, if required. The input number is the physical input number on the DVR. See "Associating events and event attributes to a recorder" section for more details.
7. Click **Save**.

Previewing a video

- Under **Preview**, click **Live Video** to view live video from the camera.

Note: You can also define presets and set the PTZ.

Adding/Deleting bulk ADV

To add/delete bulk ADV:

- Under **ADV Bulk Add/Delete**, click
  - **Add ADV**, to add ADV's for all the cameras if it is not added. During Bulk Add Operations, any cameras where ADV has already been manually added remains unchanged.
  - **Delete ADV**, to delete ADV's for all the cameras.

Editing a Camera

To edit a camera:

1. Under **Camera Settings**, select the camera to be edited and click **Edit**.
2. Edit the required details. The settings for the selected camera is changed.
3. Click **Save** to save the settings.

Note: You must disassociate the ADV and then change the PTZ type. After the changes to the PTZ type is saved, you must again associate ADV for this device.

Deleting a Camera

You can delete a camera only after you delete the devices attached to the camera. In addition, you must delete any associated ADV's of the camera.

To delete a camera:

1. Under **Camera Setting**s, select the camera to be deleted and click **Delete**.
2. Click **OK**. The selected camera is deleted.

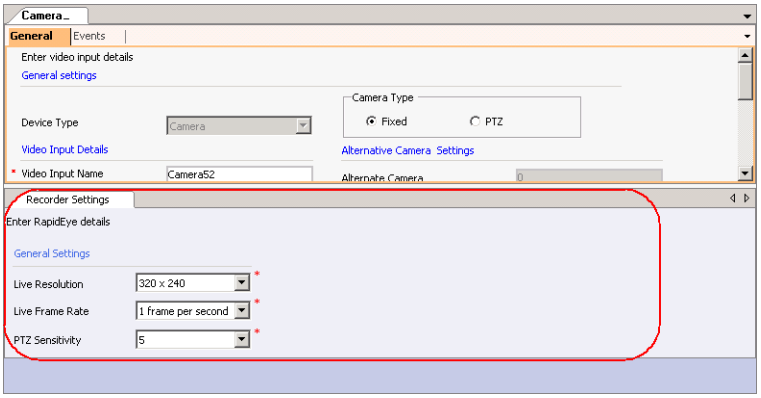
Associate a recorder to a video input device

Note: This section is applicable only in WIN-PAK SE/PE.

Video input devices like cameras can be associated with different recorders. Video clips are recorded and stored in recorders.

To associate a camera to a recorder:

1. In the **Connected To** section, click **Recorder**. The **Recorder** drop-down list is enabled.
2. Select the recorder. The device settings for the recorder appear.



3. Specify the recorder settings listed in the following table.

Recorder Type	Instructions
Rapid Eye	Record Settings In the **Live Resolution** drop-down list, select the required resolution. In the **Live Frame Rate** drop-down list, select the required frame rate. In the **PTZ Sensitivity** drop-down list, select a number for PTZ sensitivity. The **PTZ Sensitivity** drop-down list is enabled only when you select the PTZ option in the General Settings of the camera. The numbers represent speed of the PTZ. The higher the number, the more is the PTZ speed.
Fusion	Record Settings In the **Live Resolution** drop-down list, select the required resolution. In the **Live Frame Rate** drop-down list, select the required frame rate In the **PTZ Sensitivity** drop-down list, select a number for PTZ sensitivity. **PTZ Sensitivity** drop-down list is enabled only when you select the PTZ option in the General Settings of the camera. The numbers represent speed of the PTZ. The higher the number, the more the PTZ speed.
HRDP	Record Settings In the **Live Resolution** drop-down list, select the required resolution. In the **Live Frame Rate** drop-down list, select the required frame rate. In the **PTZ Sensitivity** drop-down list, select a number for PTZ sensitivity. **PTZ Sensitivity** drop-down list is enabled only when you select the PTZ option in the General Settings of the camera. The numbers represent speed of the PTZ. The higher the number, the more the PTZ speed.

PTZ Settings

To configure the PTZ settings

1. Select the **Edit Camera** settings to change the PTZ type. The check box indicates whether it is a PTZ camera.
2. **Select Home** enables you to set the selected preset as the home preset. The default home preset is Preset 1.

3. Specify a maximum **Home Delay Sec** limit of 255 seconds and a minimum limit of 1 second. The default value for the home delay for a PTZ camera is the value that is set during camera configuration.

   Home Delay is the time delay (seconds) in returning the PTZ camera to the configured Home position.

Recording Settings

To configure the settings for the Instant and Intensive recording modes:

1. Click **Instant** or **Intensive** to set the mode for which you want to configure the settings.
2. Select the **Record rate [IPS]** from the drop-down list (images or frames/second).
3. Set the **Duration in sec** value for recording.
4. Select the **Resolution** and **Quality** parameters.

Note: You cannot configure the **Quality** and **Resolution** settings in Intensive mode.

5. Click **Apply**.
6. After the settings are applied to the camera, the message Setup values set successfully in camera is displayed. Click **OK**.

   If the configured settings are not applied to the DVR, the message **Error** in setup values is displayed.

Notes:

- The **Pre-event sec** value can only be configured in the server.
- The IPS value for Intensive recording must be higher than that for the Instant recording.
- The Recording settings are applicable only for Fusion cameras.

Panel Configuration

Panel configuration is required to set 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 CS/SE/PE by adding them to the Device Map.

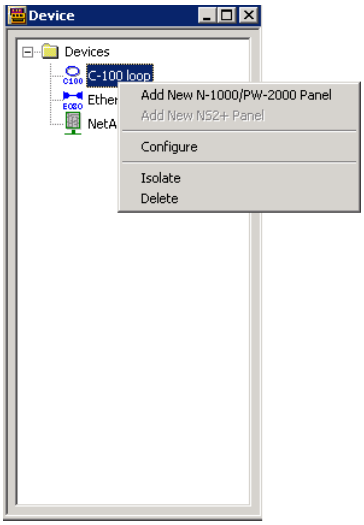
Note: WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

Adding an N-1000/PW-2000 Panel

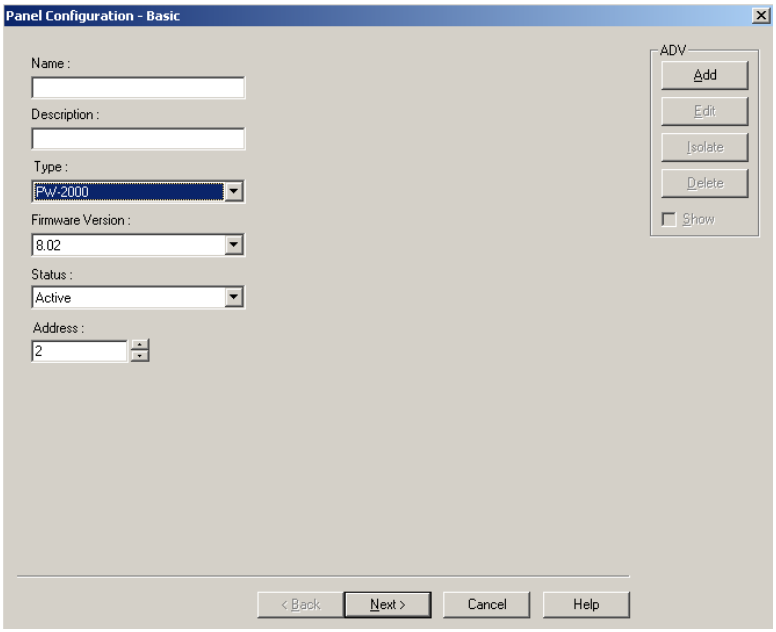
A N-1000 or PW-2000 panel can be added to C-100 and 485/PCI panel loops.

To add an N-1000/PW-2000 panel:

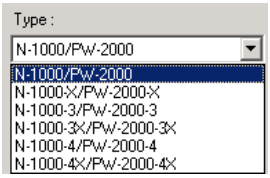
1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder.



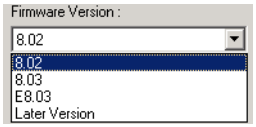
3. Right click the 485/PCI Loop or C-100 Loop and select **Add New N-1000/PW-2000 Panel**. The **Panel Configuration - Basic** dialog box appears.



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 8.02. 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 CS/SE/PE 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.

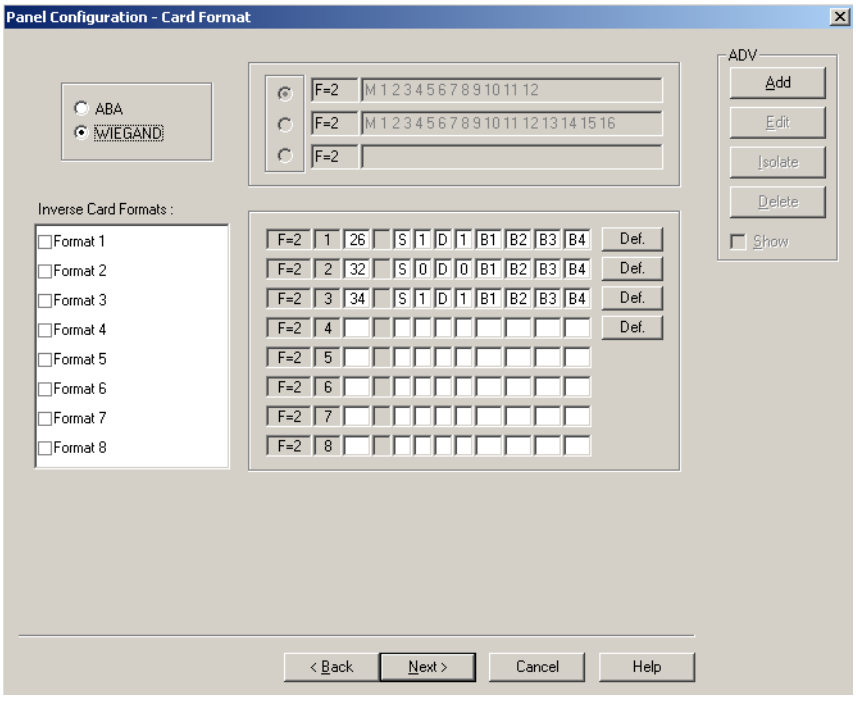
    Refer to the "Configuring an Abstract Device" section in this chapter for more details on ADV configuration.

11. Click **Next** to specify the Card Format. The **Panel Configuration - Card Format** dialog box appears.

Setting the card format for the panel

To set the card formats:

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.

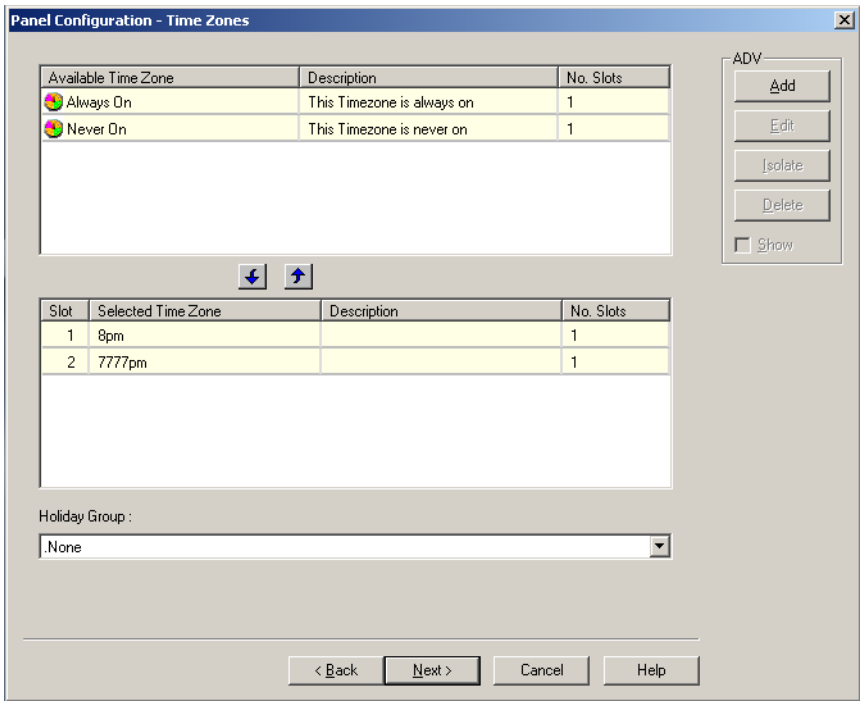
3. If you select **WIEGAND**, Honeywell recommends you to retain the default card format values.

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.

Note: In WIN-PAK SE/PE, the PRO3000 panel has 127 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. 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. **In-Out-In**: 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. **Out-In-Out**: 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.

- 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.
- If there are multiple global panels (in 485 loop with N1000), then any IN reader enables you to enter and any OUT reader enables you to exit from a facility.
- **Groups**:

  Output groups enable a card read to activate more than one output point for 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 CS/SE/PE 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.

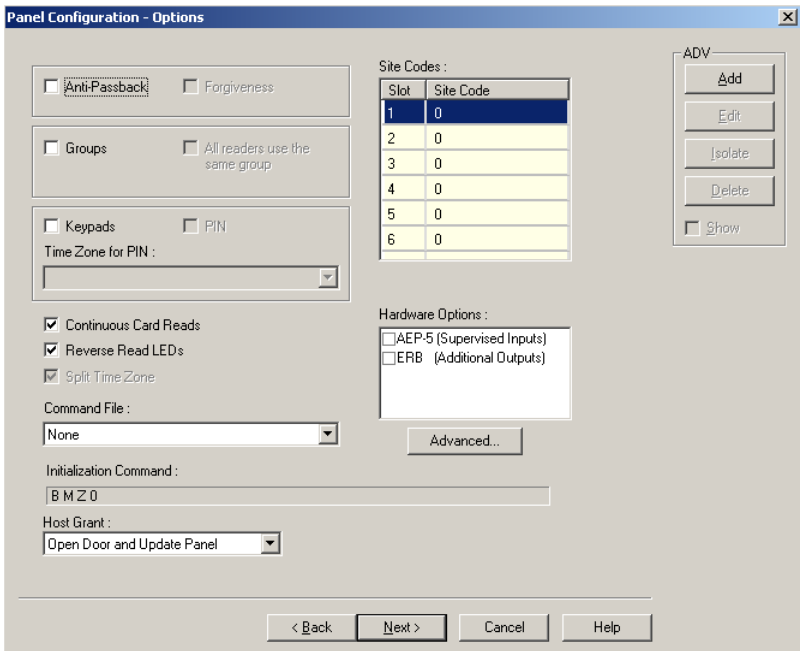
- **Hardware Options**

  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, group tab is enabled and 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.



Notes: Follow the below steps in WIN-PAK SE/PE

- **Local** - Select this option to enforce anti-passback only at doors configured locally to the panel controlling the original card read.
- **Global** - Select this option to enforce anti-passback at panels throughout the PRO3000 loop after a successful card read at any one of the system's readers. After you enable the Global Anti-passback in the PRO3000 Master panel, Cross-Loop Anti-Passback is enabled for the selected loop.
- Cross-Loop Anti-Passback is available only for PRO3000 panels.
- **Forgiveness** - Select this option to allow the door to open but to report the anti-passback violation. This check box is enabled only if Anti-passback is selected.

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.

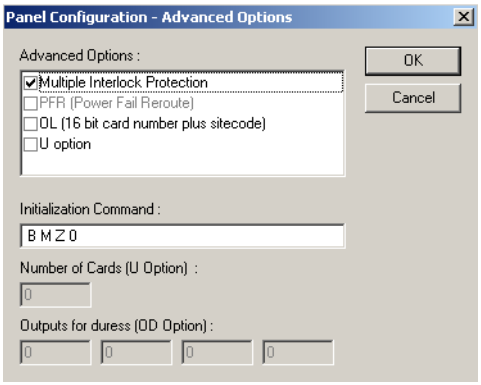
Tip: To enter a site code, double-click any cell in the table, type the site code and press ENTER. If no site code is defined, the reader does not check for site codes to enable card access.

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.

Note: Do not make any changes to Panel Configuration after selecting the MIP option.

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.

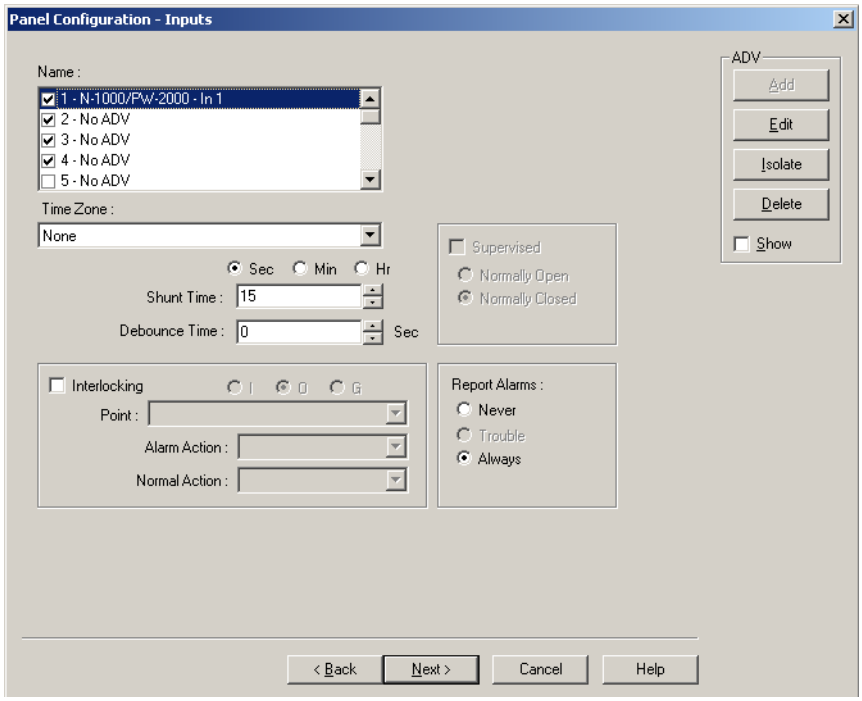
Note: The Advanced Options are available depending on the PW-2000 series panel and the version of firmware that is used.

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 CS/SE/PE 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.

Note: When a **Time Zone** is selected, the door will remain unlocked for the particular time zone.

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 9-11 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 PW-2000 alarm input points and PW-2000 with an AEP-5 default to **Normally Closed**. PW-2000-III/IV inputs can be configured for **Normally Open** circuits and 3-state supervised circuits.

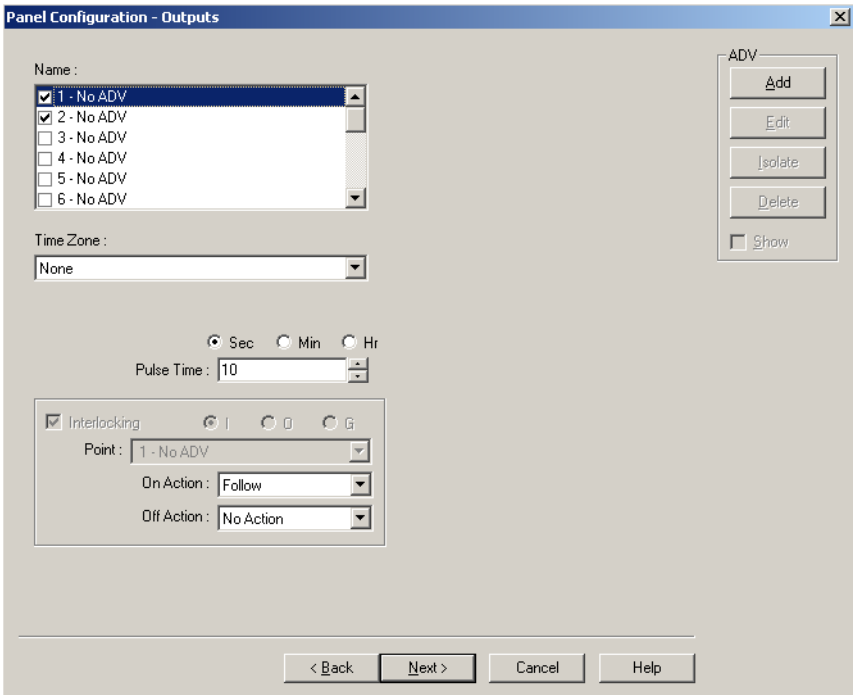
9. Under **Report Alarms**, select the following:
   - **Never**: To prevent from reporting the alarms.
   - **Always**: To report alarms.
   - **Trouble**: To report the trouble conditions. This is typically used for egress devices to detect tampering. This option is enabled only for supervised input 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.



Note:

- WIN-PAK CS/SE/PE 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. See 'Configuring an Abstract Device'.

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 CS/SE/PE 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.

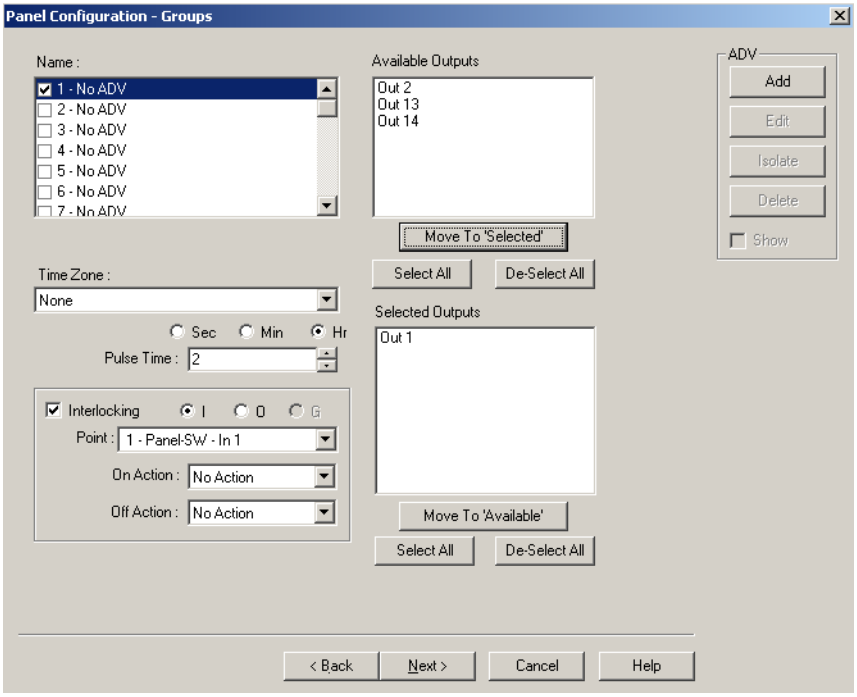
Note: This dialog box appears only if you have opted for Group option in the **Panel Configuration - Options** dialog box.

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

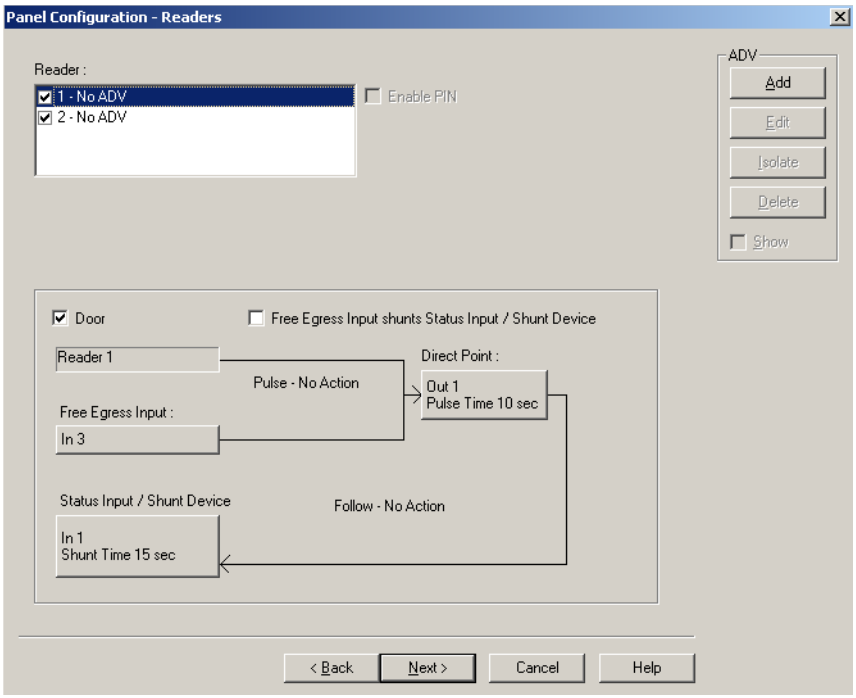
The number of readers available for the panel depends on the type of panel being configured. The WIN-PAK CS/SE/PE system automatically adds readers to the panel. By default, all available readers are active and are defined as doors.

If the anti-passback option is not set, the readers are set for a free egress configuration.

Note: In WIN-PAK SE/PE, 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.

Notes: Follow the below steps in WIN-PAK SE/PE

- Select the **Anti-Passback** check box to set the anti-passback and immediately it locally.
- Select one of the following options to set the reader as IN or OUT and set anti-passback properties.

Table 9-12 Describing the anti-passback properties

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.

- 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.
- 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.

The Card+PIN Time Zone and PIN Only Time Zone are enabled, only if you opt for the Keypad option.

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.

5. If a reader is not attached to a door, it remains as a reader without any door properties.
6. If a reader is attached to a door, the graphical form depicts the way the door is configured.

Notes: Follow the below steps in WIN-PAK SE/PE.

- To associate galaxy groups or vista partitions to this reader, click Group/Partitions and select the groups from the list.
- 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.

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.

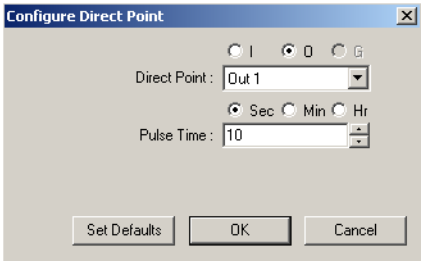
c. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the maximum time allowed for the door to close after it has been unlocked. If the time taken to close the door exceeds the shunt time, an alarm is raised.

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.

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.

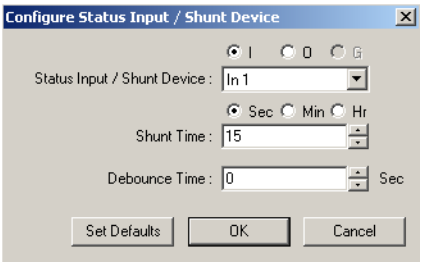
c. Select the **Direct Point** from the list.

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.
    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 NetAXS Panel

Following are the two types of NetAXS panels that are available.

- NetAXS-123
- NetAXS-4

The NetAXS-4 panel and NetAXS-123 panel is called as a “Gateway” when added directly to the communication server.

Following are the two different “NetAXS Gateway panel” scenarios.

- NetAXS-4 panel as a Gateway supports 30 downstream NetAXS-4 panels.

Tip: The downstream devices help in extending the input/output capabilities of the NetAXS panels.

Note: The NetAXS-4 Gateway panel does not support adding of NetAXS-123 downstream panels.

- NetAXS-123 panel as a Gateway supports 30 downstream NetAXS-4 or NetAXS-123 panels.

Note: Mixing of NetAXS panels is supported by the NetAXS-123 Gateway panel.

Notes:

- The N1000, PW2000, NS2 or NS2+, and P-Series panels **CANNOT** be configured as downstream panels.
- A Gateway panel has an in built PCI on board and works as a drop line. Hence a maximum of 30 panels can be connected to the Gateway panel.

Tip: The PCI3 Communications Adapter functions as the interface between a host computer's RS 232 port and one or more Honeywell access control panels connected on an RS485 multi-drop line.

- You must perform the NetAXS-4 panel or NetAXS-123 panel initialization for the first time manually. And then, later on, any configuration changes to the panel is automatically downloaded from the device map.

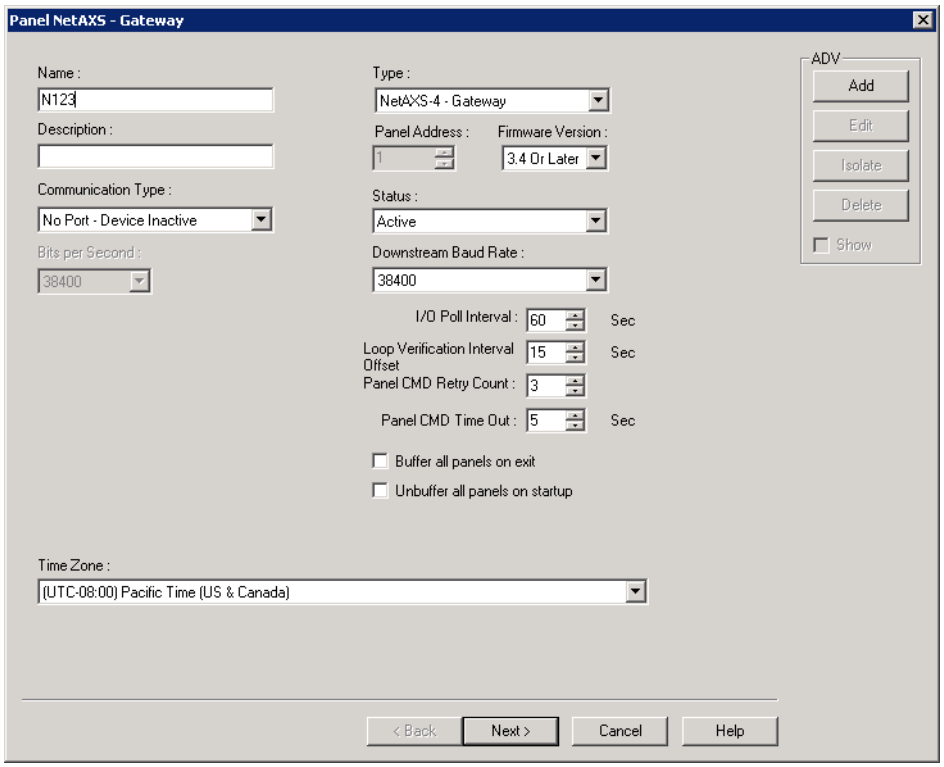
The following table lists the features of NetAXS-123 and NetAXS-4 Gateway panels.

	NetAXS-123 Gateway panel	**NetAXS-4 Gateway panel**
Downstream panel support	NetAXS-4 panel as a Gateway supports 30 downstream NetAXS-4 panels.	NetAXS-123 panel as a Gateway supports 30 downstream NetAXS-4 or NetAXS-123 panels
Communication types supported	TCP/IP, TCP/IP Encrypted Connection, TCP/IP Reverse Initiate and TCP/IP Reverse Initiate with Encryption (No direct RS232/Com port)	RS232, TCP/IP, TCP/IP Encrypted Connection, TCP/IP Reverse Initiate and TCP/IP Reverse Initiate with Encryption.
	The communication types help the NetAXS panels in communicating with WIN-PAK.	
PCI3 support	The NetAXS-4 gateway panel can be added to a 485 loop when the PCI3 is used.	The NetAXS-123 gateway panel can be added to a 485 loop when the PCI3 is used.
	The NetAXS panels (NetAXS-4 and NetAXS-123) can be added to a 485 loop when the PCI3 is used. Support of this is consistent with "legacy" versions of WIN-PAK where the NetAXS panel is programmed per the NetAXS documentation section 3 as an N-1000-IV-X. There is no GUI support for this configuration in the scope of this release	

	NetAXS-123 Gateway panel	NetAXS-4 Gateway panel
Panel Address	Always 1	Always 1
Firmware Version	3.4 or later	3.4 or later

To add a NetAXS gateway panel:

1. Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the communication server, and then click **Direct NetAXS Gateway Panel**. The **Panel NetAXS Gateway** dialog box appears.



3. Type a unique **Name** for the panel. This field is mandatory, and is limited to a maximum of 30 alphanumeric characters.
4. Select either "**NetAXS-4 Gateway**" or "**NetAXS-123 Gateway**" from the Panel **Type** list. The default selection is "**NetAXS-4 Gateway**".
5. Type a **Description** for the selected panel. You can type a description limited to a maximum of 30 alphanumeric characters.
6. For a Gateway panel, the **Panel Address** always defaults to "1", and cannot be changed.
7. In the **Firmware Version** list, select the firmware version of the panel as applicable.

The following are the NetAXS panel firmware versions compatible with WIN-PAK.

- NetAXS – 4 firmware version is 3.4. or later
- NetAXS – 123 firmware version is 3.4 or later

8. In the **Communication Type** list, select any one of the following communication types (for WIN-PAK - NetAXS panel communication) as applicable.
    - If you select "**COM1**", then select a value from the **Bits Per Second** list. The available values are **19200**, **38400**, **57600**, and **115200**. The default value is **38400**.
    - If you select "**TCP/IP Connection**", then type the **IP-Address** or **Node name** of the NetAXS panel.
    - If you select "**TCP/IP Encrypted Connection**", then type the **IP-Address** of the NetAXS panel followed by the **Encryption Password** and **Confirm Encryption Password**.

Note: The **Encryption Password** field is limited to a maximum of 32 hexadecimal characters (0-9, a-f, A-F) only. The "**AES Encryption**" standard is used for encryption.

- If you select "**TCP/IP Reverse Initiate Connection**", then type the **Port Number** (in range 5001 to 65535).
- If you select "**TCP/IP Reverse Initiate with Encryption**", then type the **Port Number** (in range 5001 to 65535) followed by the **Encryption Password** and **Confirm Encryption Password**.

Note: As NetAXS-123 Gateway supports only TCP/IP communication, the "**COM1**" option is not listed in the **Communication Type** list.

9. In the **Status** list, select one of the following states for 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.
    - **Not Present** - The panel is not available and no transactions are saved.
10. In the **Downstream Baud Rate** list, select the baud rate for the downstream panels. The default value is **38400**.
11. Select the following panel defaults as applicable.
    - **IO Poll Interval** - Select an interval between **10** and **600** 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.

- **Loop Verification Interval Offset (sec)** - Select an interval between **15** to **255**. By default, the Loop Verification Interval is set to **15** seconds.
- **Panel CMD Retry Count** - Select the number of times(between **0** and **5**) at which 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.
- **Panel CMD Time Out** - Select the waiting time (between **1** and **30**) for receiving a response from the panel and time out of the command. By default, the loop waits for **20** seconds.

12. Select the **Buffer all panels on exit** check box to buffer the events on all the panels when the communication server is stopped.
13. Select the **Unbuffer all panels on startup** check box to unbuffer all the panel events when the communication server is started.
14. In the **Time Zone** list, select the geographic time zone in which the NetAXS panel operates.
15. Click **Add** under **ADV** and set the ADV properties to create an ADV for the panel. See the 'Configuring an Abstract Device' section for more information on ADV configuration.
16. Click **Next** to specify the card format details.

Setting the Card Formats

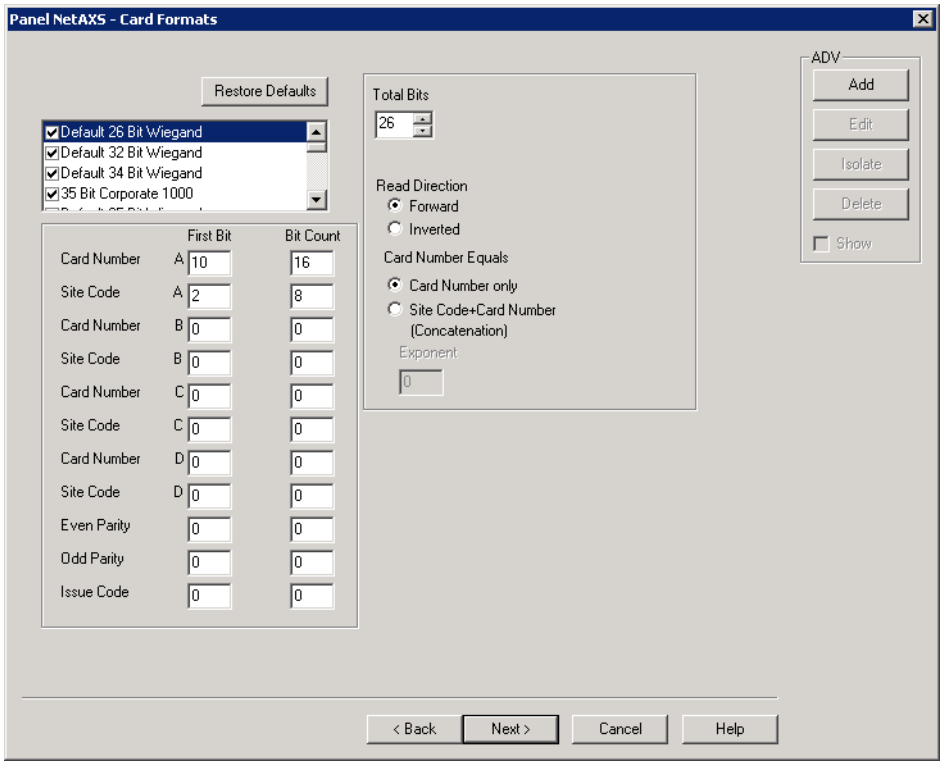
NetAXS panels support only the WIEGAND card format, which supports 128 different card formats limited to a maximum length of 128 bits. Among this 128 card formats, the following eight card formats are standard to all the NetAXS panels (NetAXS-4 and NetAXS-123).

- Default 26 Bit Wiegand
- Default 32 Bit Wiegand
- Default 34 Bit Wiegand
- 35 Bit Corporate 1000
- Default 25 bit Wiegand
- Default 29 bit Wiegand
- Default 37 bit Wiegand
- Default 75 bit Wiegand

Note: The 75-bit Wiegand is the default FIPS card format and while this FIPS format is commonly used, you may need to adjust for your application – consult your WIN-PAK support representative for further assistance if any.

To configure the card formats:

1. In the **Panel NetAXS - Card Formats** dialog box, the list displays the card formats types supported by NetAXS. The check boxes corresponding to the standard card formats supported by NetAXS are selected by default.



2. Default values appear under the **First Bit** and **Bit Count** columns for each the 128 card format types corresponding to the following fields.
    - Card Numbers A through D
    - Site Codes A through D
    - Even Parity
    - Odd Parity
    - Issue Code

Select a card format and change the default **First Bit** and **Bit Count** values for the above listed fields.

Note: You can change the default values for any of the fields listed above. However, click **Restore Defaults** to reset the default values for these fields.

3. The **Total Bits** list by default displays the total number of bits supported by a card format. For card formats **Format 9** through **Format 128**, the total number of bits is defaulted to 0. You must select a bit value greater than 3 for all these formats.
4. Under **Read Direction**, select the **Forward** or **Inverted** option button as applicable for reading the card. By default, the **Forward** option button is selected.
5. Under **Card Number Equals**, select any one of the following option buttons:

- **Card Number only** - represents the standard mode of operation where the card number associated to the card holder is exactly the card number.
- **Site Code + Card Number (Concatenation)** - represents the mode where the site code is added to the card number to create a unique card number. Concatenation of the Site Code and Card Number - commonly used on an N-1000 for “Corporate 1000” card format.

6. The **Exponent** field is grayed out unless the **Site Code + Card Number** is selected. To generate a card's new ID, use this field to insert the desired number of zeroes to be appended to the **Site Code** value. Then add the card ID to calculate the card's new ID.

   For example, a 26-bit card has a site code of 123 and the card ID is 637. When the Concatenate Site Code is enabled with an exponent of 4, 4 zeroes are appended to the site code. The result is a final value of 1230000. This newly modified site code value is then added to the number that the panel has read as the card's Id, 1230000 + 637 = 1230637. The newly combined number becomes the card's new ID value.

7. Click **Next** to assign time zones and holiday group to the NetAXS panel. The **Panel NetAXS - Time Zones** dialog box appears.

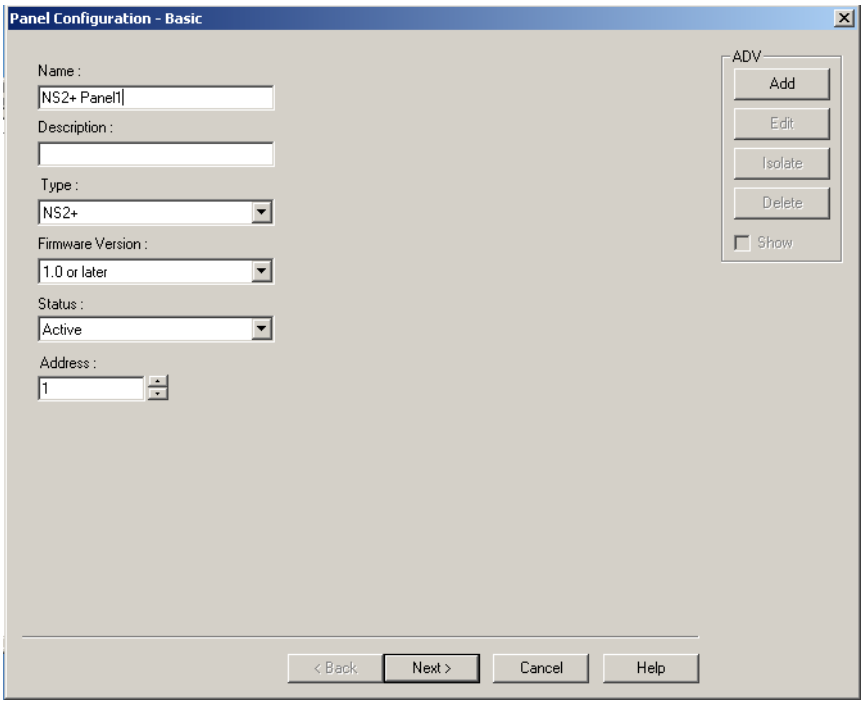
Adding an NS2+ Panel

An NS2+ panel can be added to an RS-232 (single panel) and 485/PCI panel loops.

Note: A personality chip is required for NS2 to work with WIN-PAK. This chip converts the NS2 panel to NS2+ panel and is used in NStar.

To add an NS2+ panel:

1. Choose **Configuration** > **Device** > **Device Map**. The **Device** window appears.
2. Expand the **Devices** 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 CS/SE/PE 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 CS/SE/PE 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.

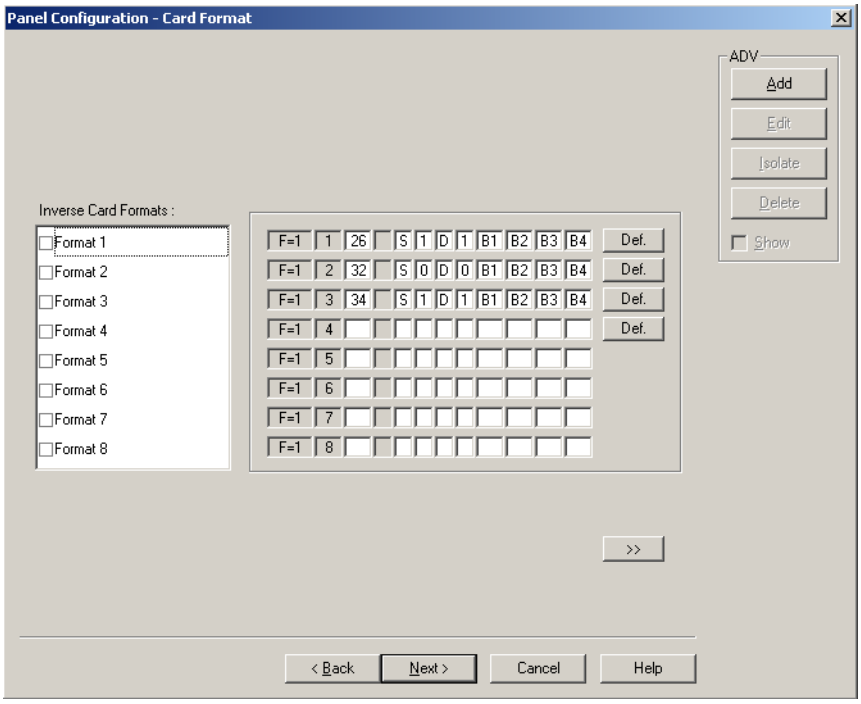
11. Click **Next** to set the Card Format. The **Panel-Configuration - Card Format** dialog box appears.

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

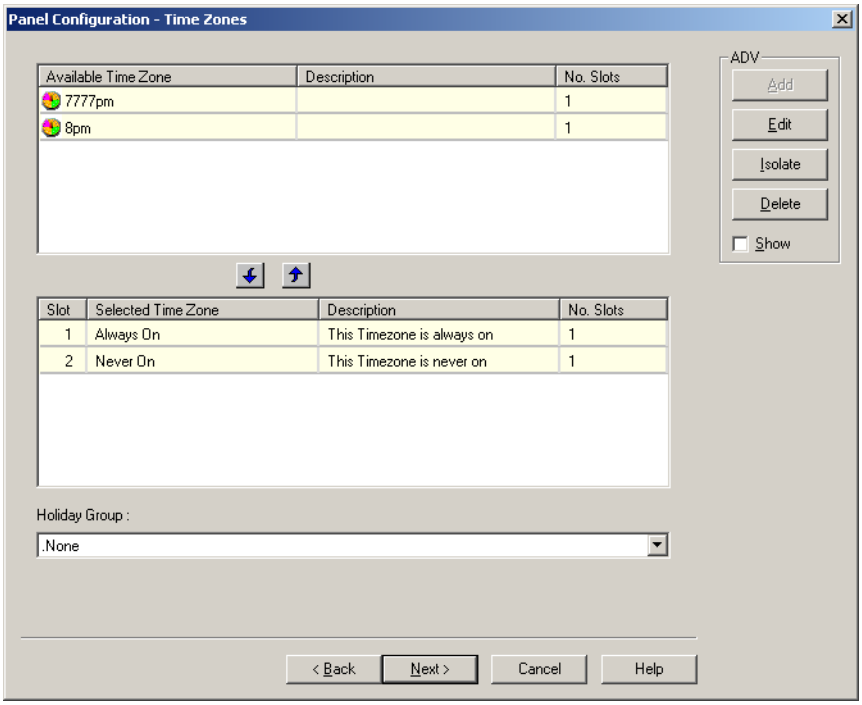
Where *pn* = panel address number and *fsn* = format slot number.

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.
- 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.

Notes: If the anti-passback option is not selected, WIN-PAK CS/SE/PE 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**

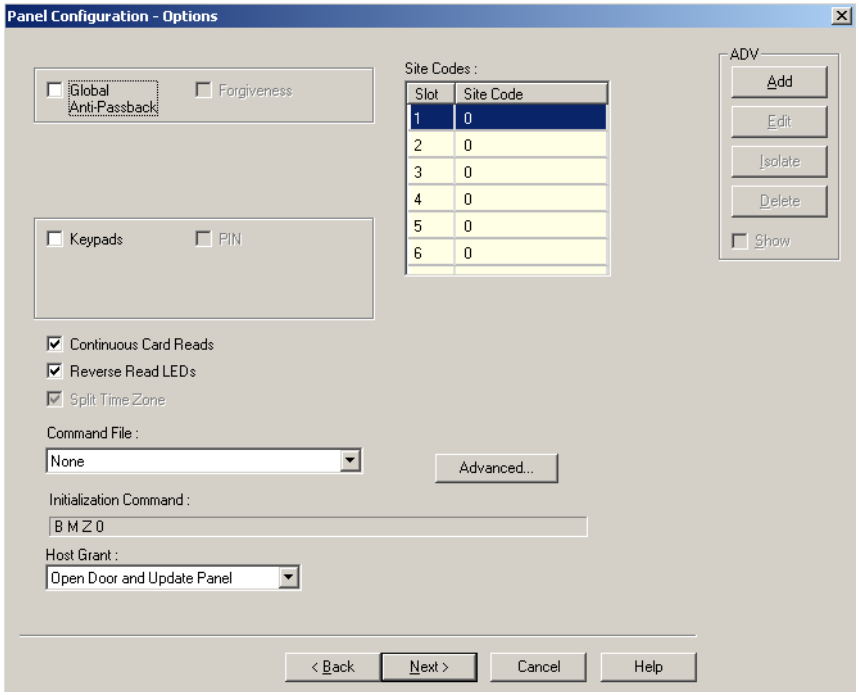
The Host Grant option provides the fault tolerance even if the card is not found in the panel. Host Grant options are used when, for example, a number of cards have been entered in the database, but have not yet been downloaded to the panel.

- **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:



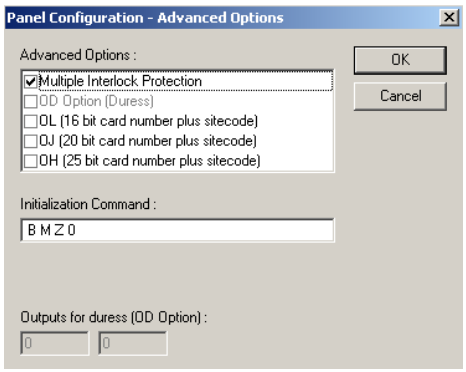
1. Select the **Global Anti-passback** check box to ensure that the card holders present the cards while entering and exiting a building. When you select this option, the anti-passback is globally implemented.
2. Select the **Forgiveness** check box to allow the door to open but to report the anti-passback 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.

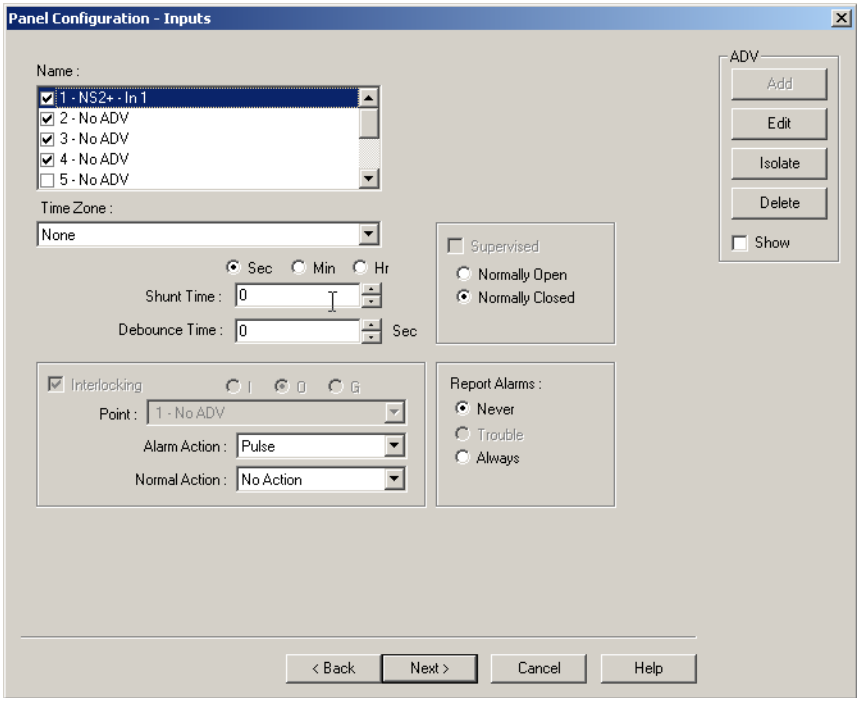
i. In the **Outputs for duress (OD Option)** box, enter the value for Outputs for duress. This option is enabled only if the OD option is selected.

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.



Notes:

- WIN-PAK CS/SE/PE 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.

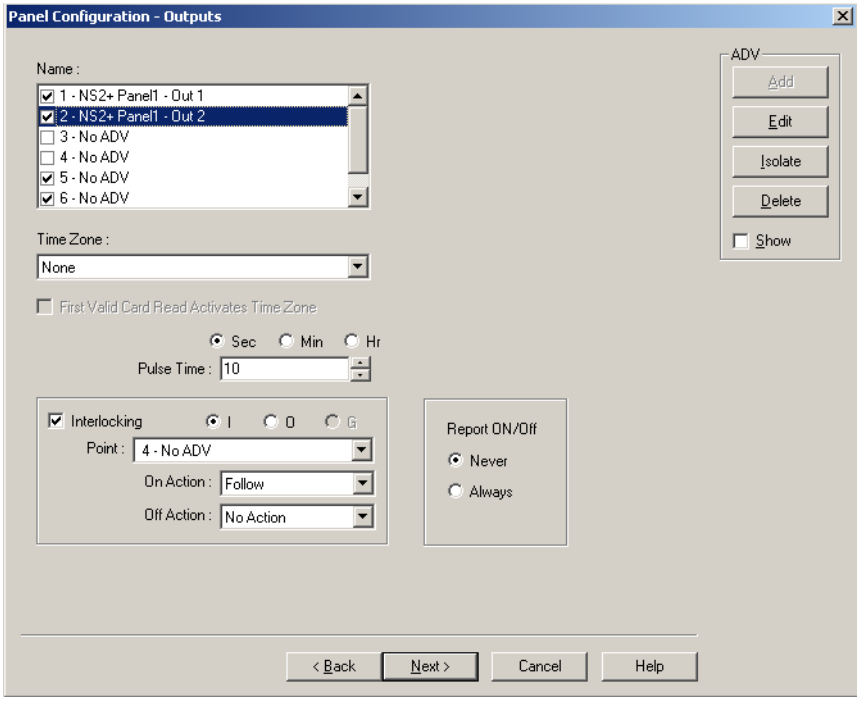
6. Select the **Supervised** check box to report the troubles when there is a change in state of input points.
7. Select **Normally Closed** or **Normally Opened** to specify the normal state of the door.
8. Under Report Alarms, select one of the following options:
   - **Never**: Never report an alarm 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.

   See the "Interlocking" section 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 CS/SE/PE 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 CS/SE/PE 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.

   See the "Interlocking" section 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

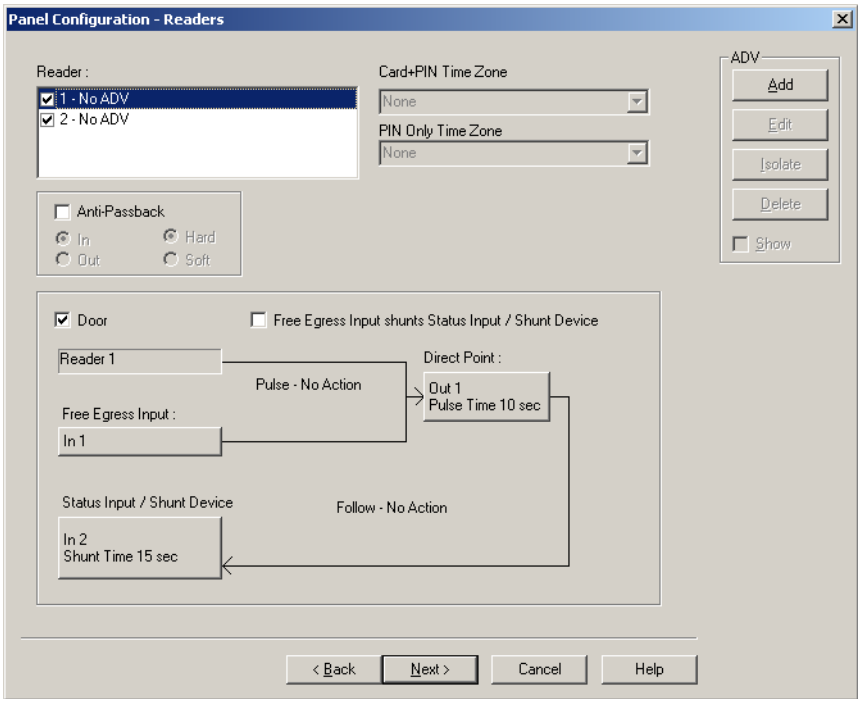
The number of readers available for the panel depends on the type of panel being configured. The WIN-PAK CS/SE/PE system automatically adds readers to the panel. By default, all available readers are active and are defined as doors.

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.

Note: In WIN-PAK SE/PE 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 9-13 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.

Notes:

- The **Card+PIN Time Zone** and **PIN Only Time Zone** are enabled, only if you opt for the Keypad option.
- Step 7 to 9 is applicable only for WIN-PAK SE/PE.

7. Click to enable **N-Man Rule**. During the N-Man Rule, you must swipe multiple cards to gain access. By default, the swipe interval is set to 10 seconds.
    - Click to set the **Count**. The count specifies the total count of valid cards that must be presented at the selected reader to open a door. You can set the card count to a minimum of 2 and a maximum of 9.
    - Click to set the **Time Zone**. The **N-Man Rule** is enabled only during the specified time zone.
8. Select the **Enable PIN** check box if a keycode must be entered before presenting a card to gain access.
9. From the **Mode** drop-down list, select to indicate the state of the door.

Note: The **Mode** option is applicable only for HBAC-WIN2P panels.

Table 9-14 Describing the available option for Mode

Mode	Description
Disable the door	The doors ignore all the card reads and egress actions
Unlock (Unlimited Access)	The doors unlock and enable access to all regardless to card reads
Locked (no Access, Egress Active)	The doors lock irrespective of a valid card read but, unlocks when egress button is pressed
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

10. 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.
11. 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.

12. If a reader is not attached to a door, it remains as just a reader without any door properties.
13. If a reader is attached to a door, the graphical form depicts the way the door is configured.

Notes: Follow the below steps in WIN-PAK SE/PE.

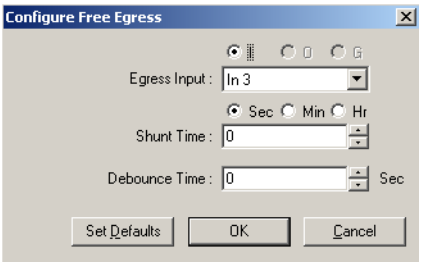
- To associate galaxy groups or vista partitions to this reader, click Group/Partitions and select the groups from the list.
- To associate galaxy groups or vista partitions to the input point, select the input point from the **Input to Set/Arm Galaxy Grps/Partitions** list.

Notes: Follow the below steps in WIN-PAK SE/PE.

- To associate galaxy groups or vista partitions to this reader, click Group/Partitions and select the groups from the list.
- 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.

14. 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.

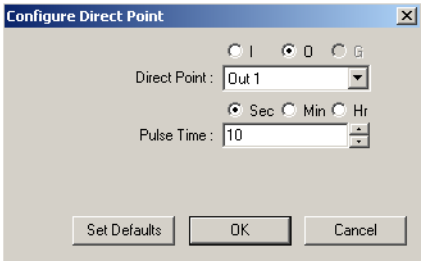
c. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the duration allowed for the door kept unlocked. If the door remains in the unlocked state even after the shunt time, the alarm is raised.

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.

15. 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**.

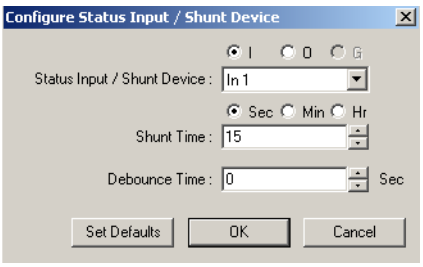
e. Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

The changes to the pulse time are automatically reflected in the appropriate input, output or group.

16. 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.

17. 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.

18. Click **OK** to configure the NS2+ panel.

Adding or Editing a NETAXS Panel

NetAXS panels come in two flavors.

- NetAXS-123
- NetAXS-4

NetAXS-4 panel or NetAXS-123 panel is considered as a "Gateway panel" when added directly to the communication server.

There are two different "NetAXS Gateway panel" scenarios:

- NetAXS-4 as a Gateway can support up to 30 downstream NetAXS-4 panels.
- NetAXS-123 as a Gateway can support 30 downstream NetAXS-4 or NetAXS-123 panels (mixing NetAXS panels is supported by the NetAXS-123 Gateway).

Notes:

- Downstream devices help in extending the input/output capabilities of the NetAXS panels.
- NetAXS-4 Gateway does not support NetAXS-123 downstream panels.

- N1000/PW2000, NS2/ NS2+, and P-Series panels cannot be configured as downstream panels
- A Gateway panel has an in built PCI on board and works as a drop line. Hence a maximum of 30 panels can be connected to the Gateway panel.

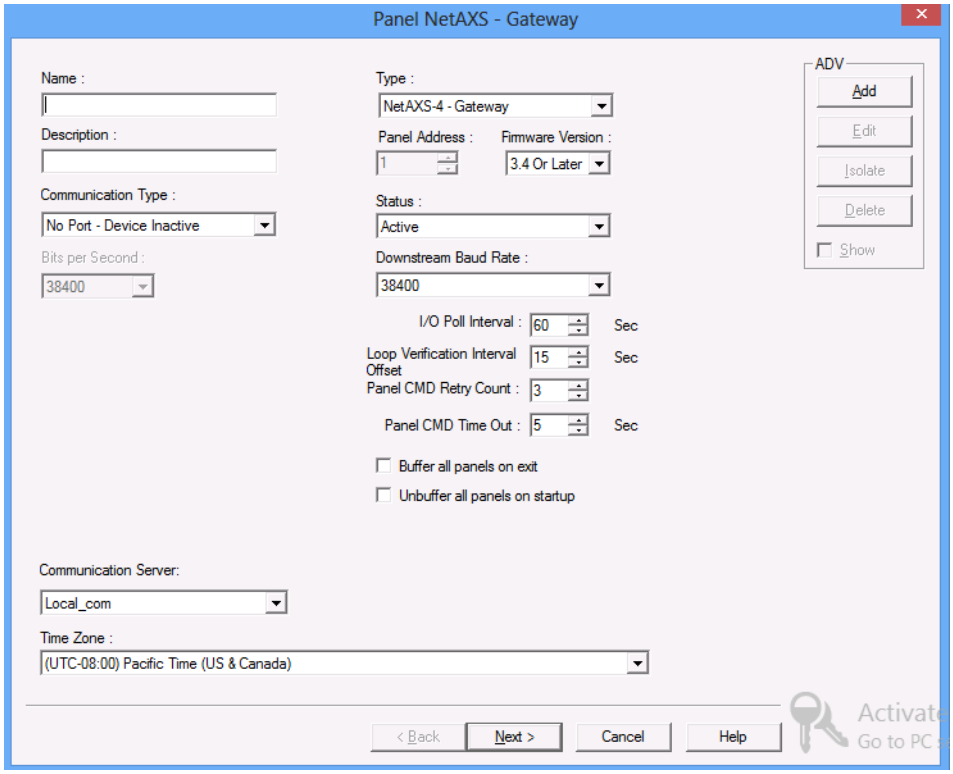
NetAXS-4 panel supports the following communication types for communicating with WIN-PAK: RS232, TCP/IP, TCP/IP Encrypted Connection, TCP/IP Reverse Initiate, and TCP/IP Reverse Initiate with Encryption.

NetAXS-123 supports the following communication types for communicating with WIN-PAK: TCP/IP, TCP/IP Encrypted Connection, TCP/IP Reverse Initiate, and TCP/IP Reverse Initiate with Encryption (No direct RS232/Com port).

Note: NetAXS panels (NetAXS-4 and NetAXS-123) can be added to a 485 loop when the PCI3 is used. Support of this is consistent with "legacy" versions of WIN-PAK where the NetAXS panel is programmed per the NetAXS documentation section 3 as an N-1000-IV-X. There is no GUI support for this configuration in the scope of this project.

To add a NetAXS gateway panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and then right-click the communication server and click **Direct NetAXS Gateway Panel**. The **Panel NetAXS - Gateway** dialog box appears.



3. Type a unique **Name** for the panel. This field is mandatory, and is limited to a maximum of 30 alphanumeric characters.

4. Select either "**NetAXS-4 Gateway**" or "**NetAXS-123 Gateway**" from the Panel **Type** list. The default selection is **NetAXS-4 Gateway**.
5. Type a **Description** for the selected panel. You can type a description limited to a maximum of 30 alphanumeric characters.
6. For a Gateway panel, the **Panel Address** is always defaulted to "1", and cannot be changed.
7. In the **Firmware Version** list, select the Firmware version of the panel.

Notes: The following are the minimum NetAXS panel firmware versions compatible with WIN-PAK.

- Minimum NetAXS – 4 firmware version is 3.4.
- Minimum NetAXS – 123 is firmware version is 3.5.

8. In the **Communication Type** list, select any one of the following communication types for WIN-PAK - NetAXS panel communication.
    - **COM1**- If you select this option, select a value from the **Bits Per Second** list. The available values are **19200**, **38400**, **57600**, and **115200**. The default value is **38400**.
    - **TCP/IP Connection** - If you select this option, type the **IP-Address or Node name** of the NetAXS panel.
    - **TCP/IP Encrypted Connection** - If you select this option, type the **IP-Address** of the NetAXS panel followed by the **Encryption Password** and **Confirm Encryption Password**.

Notes: The **Encryption Password** field must consist of 32 hexadecimal characters (0-9, a-f, A-F) only. The “AES Encryption” standard is used for encryption.

- **TCP/IP Reverse Initiate Connection** - If you select this option, type the **Port Number** (in range 5001 to 65535).
- **TCP/IP Reverse Initiate with Encryption** - If you select this option, type the **Port Number** (in range 5001 to 65535) followed by the **Encryption Password** and **Confirm Encryption Password**.

Notes: As NetAXS-123 Gateway supports only TCP/IP communication, the “**COM1**” option is not listed in the **Communication Type** list.

9. In the **Status** list, select one of the following states for 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.
    - **Not Present** - To define the panel before completing the panel installation. If the panel is marked as Not Present, no card transactions are saved.

10. In the Downstream Baud Rate list, select the baud rate (**38400** or **115200**) for the downstream panels. The default value is **38400**.

11. Select the panel defaults.

    - **IO Poll Interval** - Select the interval between **10** and **600** 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.
    - **Loop Verification Interval Offset (sec)** - Select the interval between **15** to **255**. By default, the **Loop Verification Interval** is set to **15** seconds.
    - **Panel CMD Retry Count** - Specify the number of times between **0** and **5** at which 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.
    - **Panel CMD Time Out** - Specify the waiting time between **1** and **30** for receiving a response from the panel and for time out of the command. By default, the loop waits for 5 seconds.

12. Select the **Buffer all panels on exit** check box to buffer the events on all the panels when the communication server is stopped.

13. Select the **Unbuffer all panels on startup** check box to unbuffer all the panel events when the communication server is started.

14. In the **Time Zone** list, select the geographic time zone in which the NetAXS panel operates.

15. Click **Add** under **ADV** and set the ADV properties to create an ADV for the panel. See "Configuring an Abstract Device".

16. Click **Next** to specify the following details:

Task	Go To
Setting the card format for NetAXS panels	page 499
Assigning time zones and holiday groups to a NetAXS panel	page 501
Setting the NetAXS panel options	page 502
Configuring input points to the NetAXS panel	page 505
Configuring output points to the NetAXS panel	page 508
Configuring groups to the NetAXS panel	page 511
Configuring a reader to the NetAXS panel	page 513
Adding downstream devices	page 527

Task	Go To
Adding downstream NetAXS panels to a NetAXS-4 Gateway panel	page 528
Adding downstream NetAXS-123 panels or NetAXS-4 panels to a NetAXS-3 Gateway panel.	page 529

Setting the card format for NetAXS panels

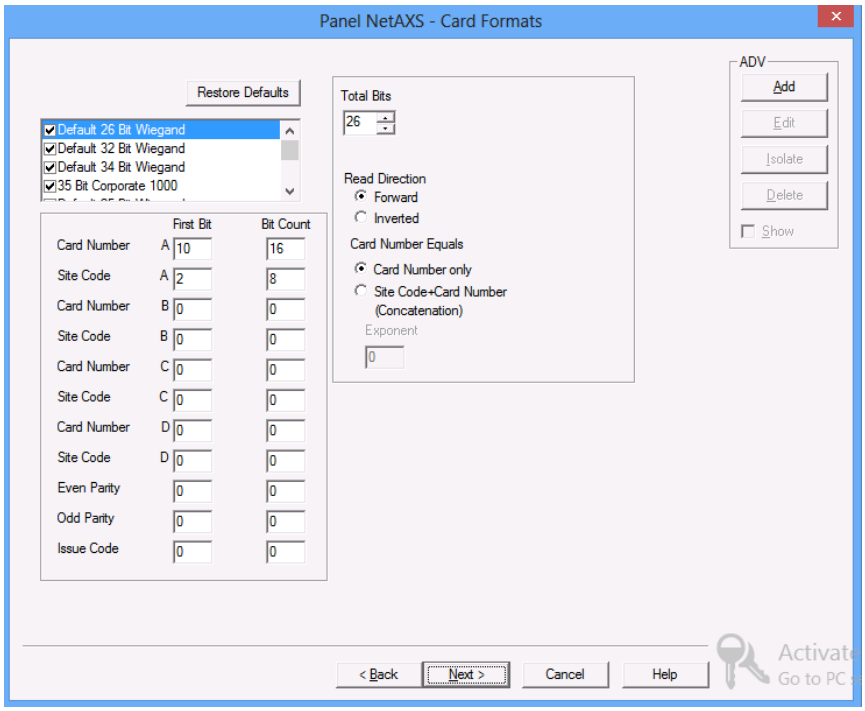
NetAXS panels support only the "WIEGAND" card format. WIEGAND has 128 different card formats limited to a maximum length of 128 bits. Among this 128 card formats, the following eight card formats are standard to all the NetAXS panels (NetAXS-4 and NetAXS-123).

- Default 26 Bit Wiegand
- Default 32 Bit Wiegand
- Default 34 Bit Wiegand
- 35 Bit Corporate 1000
- Default 25 bit Wiegand
- Default 29 bit Wiegand
- Default 37 bit Wiegand
- Default 75 bit Wiegand

Note: The 75-bit Wiegand format is the default FIPS card format and while this FIPS format is commonly used, you may need to adjust for your application, consult your WIN-PAK support representative for further assistance.

To configure the card format:

In the **Panel NetAXS - Card Formats** dialog box, perform the following:



1. The list displays the card formats types supported by NetAXS. The check boxes corresponding to the standard card formats supported by NetAXS are selected by default.
2. Default values appear under the **First Bit** and **Bit Count** columns for each the 128 card format types corresponding to the following fields:
   - Card Numbers A through D
   - Site Codes A through D
   - Even Parity
   - Odd Parity
   - Issue Code
3. Select a card format and change the default **First Bit** and **Bit Count** values for the above listed fields.

Note: You can change the default values for any of the fields listed above. However, click Restore Defaults to reset the default values for these fields.

4. The **Total Bits** list by default displays the total number of bits supported by a card format. For card formats Format 9 through Format 128, the total number of bits is defaulted to 0. You must select a bit value greater than 3 for all these formats.

5. Under **Read Direction**, select the **Forward** or **Inverted** option button as applicable for reading the card. By default, the **Forward** option button is selected.
6. Under **Card Number Equals**, select any one of the following option buttons:
   - Card Number only - represents the standard mode of operation where the card number associated to the card holder is exactly the card number.
   - **Site Code + Card Number (Concatenation)** - represents the mode where the site code is added to the card number to create a unique card number. Concatenation of the Site Code and Card Number - commonly used on an N-1000 for "Corporate 1000" card format.
7. The **Exponent** field is grayed out unless the S**ite Code + Card Number** is selected. To generate a card's new ID, use this field to insert the desired number of zeroes to be added to the right-hand side of the Site Code value. Then add the card ID to calculate the card's new ID.

   Example: A 26-bit card has a site code of 123 and the card ID is 637. When the Concatenate Site Code is enabled with an exponent of 4, 4 zeroes are appended to the site code. The result is a final value of 1230000. This newly modified site code value is then added to the number that the panel has read as the card's ID—that is, 1230000 + 637 = 1230637. The newly combined number becomes the card's new ID value.
8. Click **Next** to assign time zones and holiday group to this panel. The **Panel NetAXS - Time Zones** dialog box appears.

Assigning time zones and holiday groups to a NetAXS panel

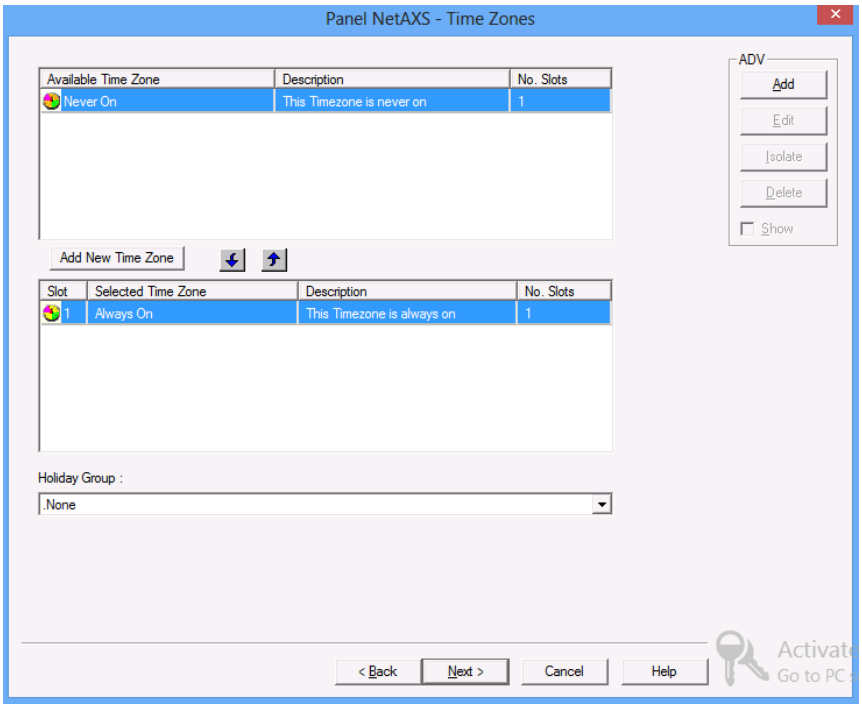
A maximum of 128 time slots and 256 holidays (per holiday group) can be associated to NetAXS panels (NetAXS-123 and NetAXS-4).

A new provision that allows an operator to create and add a new Time Zone while inside the panel database is added to the Panel Configuration - Time Zones tab. When the Add New Time Zone is selected it opens up the Time Zone Record window to allow the operator to create and name the new time zone. After the time zone is created, the new time zone is added to the Time Zones database and applied to the panel's database. When the Time Zone Record window is closed, the user interface returns to the Panel Configuration – Time Zones tab. The newly created time zone is automatically added to the Selected Time Zone list and use the default account.

Note: The "Always on" time zone is selected by default for all NetAXS panels.

To configure time zones and holiday groups:

1. In the **Panel NetAXS- 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.

Tip: Click **Add New Time Zone** to create a new time zone. The **Time Zone Record** dialog box appears. See "Time Zone" for more information.

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 NetAXS- Options** dialog box appears.

Setting the NetAXS panel options

You can set certain panel options such as anti-passback, groups for providing access for the readers, input points, and output points attached to the NetAXS panel.

- Anti-passback/Global Anti-passback

  Anti-Passback discourages card holders to enter without using their cards. Anti-passback violation occurs in the following scenarios.

  - **In-Out-In**: If you have entered the building without using the card and exited from the building using your card. Again, if you try to enter the building the access is denied.
  - **Out-In-Out**: 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. 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.

- 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.

- 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 are not supported by NetAXS-123 panels.

- Continuous Card Reads

  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.

  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

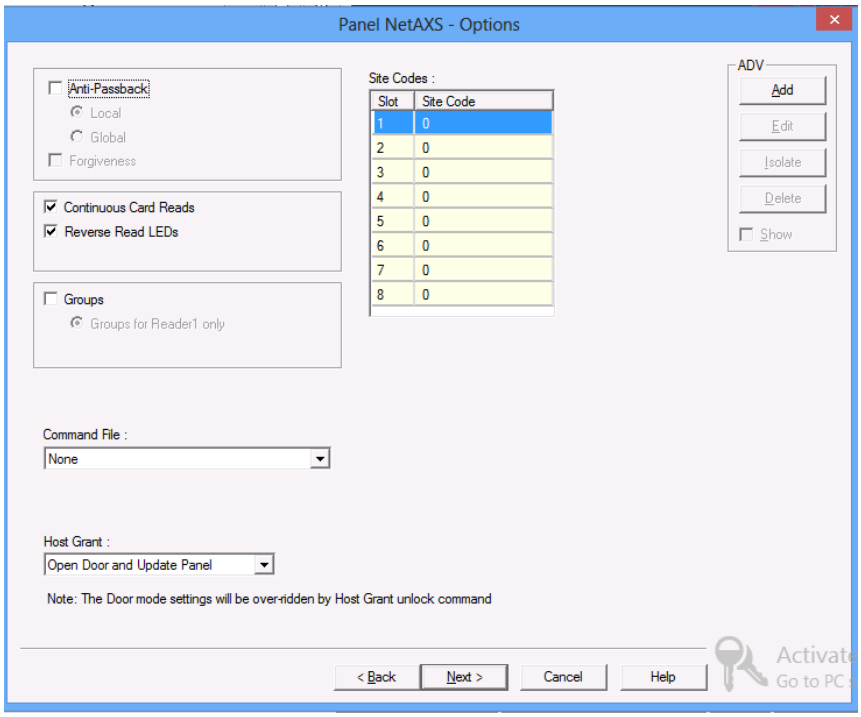
  Site codes ensure that the card belongs to the facility where the card is used for gaining access. The site code is encoded with a card number on cards.

- Command File

  Command files contain a list of commands that can be executed manually or automatically.

To configure the panel options:

1. In the **Panel NetAXS- Options** dialog box, select the **Anti-Passback** check box to ensure that the card holders present the cards while entering and exiting a building.



   - **Local** - Select this option to enforce anti-passback only at doors configured locally to the panel controlling the original card read.
   - **Global** - Select this option to enforce anti-passback at panels throughout the system after a successful card read at any one of the system's readers.
   - **Forgiveness** - Select this check box to forgive anti-passback violation.
2. Select the **Continuous Card Reads** check box to enable card readers to read cards continuously, independent of output pulse time.
3. 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.
4. Select the **Groups** check box to create output relay groups.
   - **Groups for Reader1 only** - Select this check box to enable group operation for reader 1. Other readers use their default or defined relays based on valid card reads
   - **All readers use groups** - Select this check box to pulse the group when a valid card is presented on any reader.
5. In the **Command File** list, select a command file that is applicable to a panel.

6. 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.
7. 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.

8. Click **Next** to configure the Input points to the panel. The **Panel NetAXS-Inputs** dialog box appears.

Configuring input points to the NetAXS panel

A maximum of 14 Inputs are displayed for NetAXS-4 Gateway panel in the Inputs tab with the following default options.

- 1= Door 1 Egress. (Disable Alarm and Normal Messages Time Zone to Always (24X7); Interlocked to O1, Pulse, No Action)
- 2= Door 1 Status. (Shunt time 15.0 Seconds, Auto-Relock enabled to O1)
- 3= Door 2 Egress. (Disable Alarm and Normal Messages Time Zone to Always (24X7); Interlocked to O2, Pulse, No Action)
- 4= Door 2 Status. (Shunt time 15.0 Seconds, Auto-Relock enabled to O2)
- 5= Door 3 Egress. (Disable Alarm and Normal Messages Time Zone to Always (24X7); Interlocked to O3, Pulse, No Action)
- 6= Door 3 Status (Shunt time 15.0 Seconds, Auto-Relock enabled to O3)
- 7= Door 4 Egress. (Disable Alarm and Normal Messages Time Zone to Always (24X7); Interlocked to O4, Pulse, No Action)
- 8= Door 4 Status. (Shunt time 15.0 Seconds, Auto-Relock enabled to O4)
- 9= Reader 1 Tamper / aux
- 10= Reader 2 Tamper / aux
- 11= Reader 3 Tamper / aux
- 12= Reader 4 Tamper / aux
- 13= Primary Power Status
- 14= Tamper

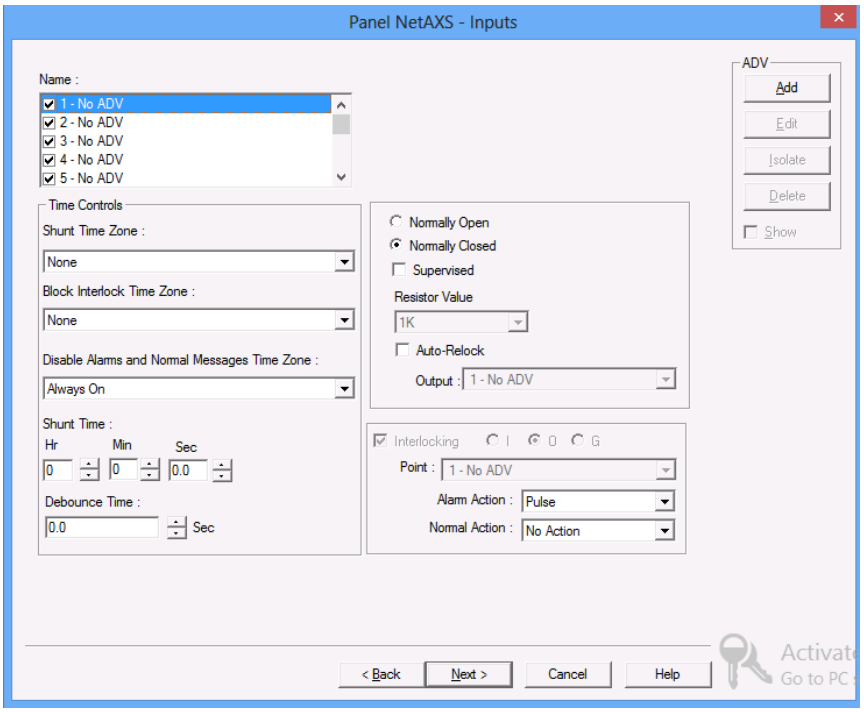
A maximum of 17 Inputs are displayed for NetAXS-123 Gateway panel in the Inputs tab with the following default options.

- 1= Door 1 Egress. (Disable Alarm and Normal Messages Time Zone to Always (24X7); Interlocked to O1, Pulse, No Action)

- 2= Door 1 Status. (Shunt time 15.0 Seconds, Auto-Relock enabled to O1)
- 3= Reader 1A Tamper.
- 4= Reader 1B Tamper.
- 5= General.
- 6= Primary Power
- 7= Reserved (not wired – allow no ADV).
- 8= Reserved (not wired – allow no ADV).
- 9= Door 2 Egress (Disable Alarm and Normal Messages Time Zone to Always (24X7); Interlocked to O7, Pulse, No Action)
- 10= Door 2 Status (Shunt time 15.0 Seconds, Auto-Relock enabled to O7)
- 11= Reader 2A Tamper
- 12= Reader 2B Tamper
- 13=Door 3 Egress (Disable Alarm and Normal Messages Time Zone to Always (24X7); Interlocked to O11, Pulse, No Action)
- 14= Door3 Status (Shunt time 15.0 Seconds, Auto-Relock enabled to O11)
- 15= Reader 3A Tamper
- 16= Reader 3B Tamper
- 20= Panel Tamper

To configure inputs to the panel:

1. In the **Panel NetAXS- 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.

Note: In the ADV definition, three actions are listed for an input point: Energized, De-Energized, and Trouble.

3. In the **Shunt Time Zone** list, select a time zone during which the input is ignored.
4. In the **Block Interlock Time Zone** list, select a time zone during which the programmed action on this input from another point is disabled.
5. In the **Disable Alarms and Normal Messages Time Zone** list, select a time zone during which Alarm and Normal is not be reported, but Short and Cut are reported.
6. 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.

   The maximum number of hours is 1.When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45 and the maximum number of seconds is 59. The sum of all three units comprises the shunt time. Note that you can express seconds in tenths of a second.
7. Enter the **Debounce Time** in seconds. The maximum number of seconds is 6553.5 seconds as 10th of a second are allowed. 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.

For example, consider the following scenarios:

Table 9-15 Examples

Scenario	Shunt Time	Debounce Time	Alarm raised at...
1	15 sec	0 sec	16th sec

Table 9-15 Examples

Scenario	Shunt Time	Debounce Time	Alarm raised at...
2	15 sec	10 sec	25th sec

8. Select **Normally Closed** or **Normally Open** to specify the normal state of the door. The Normally Open state indicates that the door's normal state is open and the Normally Closed state indicates that the door's normal state is closed.
9. Select the **Supervised** check box to specify that the door's electrical circuit is wired with alternative paths supervised by resistors.
10. In the **Resistor Value** list, select the resistor values used in the supervised mode. The available values are:1K (default), 2.2K, 4.7K, 10K.

Note: The **Resistor Value** field is enabled only if you select the **Supervised** check box.

11. Select the **Auto-Relock** check box, and then select the associated output from the **Output** list to re-lock the door immediately when the door status switch closes after entry. The output relay that controls the door strike de-energizes when the associated input returns to normal state instead of remaining energized for the duration of the pulse time.

Note: If you clear the **Auto-Relock** check box, the door closes after entry and stays unlocked.

12. Set the **Interlocking** option for the input point.

Note: Group Interlock is not displayed for NetAXS-123 panels.

13. Click **Next** to configure the output points to the panel. The **Panel NetAXS - Outputs** dialog box appears.

Configuring output points to the NetAXS panel

A maximum of 16 outputs are displayed for NetAXS-4 Gateway panel in the Outputs tab with the following default options:

- O1 = Door 1 lock (Pulse Time 10.0 seconds; Interlock to I2 follow / follow)
- O2 = Door 2 lock (Pulse Time 10.0 seconds; Interlock to I4 follow / follow)
- O3 = Door 3 lock (Pulse Time 10.0 seconds; Interlock to I6 follow / follow)
- O4 = Door 4 lock (Pulse Time 10.0 seconds; Interlock to I8 follow / follow)
- O5 = Aux Output 1 (Pulse Time to 10.0 seconds)
- O6 = Aux Output 2 (Pulse Time to 10.0 seconds)
- O7 = Aux Output 3 (Pulse Time to 10.0 seconds)
- O8 = Aux Output 4 (Pulse Time to 10.0 seconds)
- O9 = Reader 1 Beeper
- O10 = Reader 2 Beeper

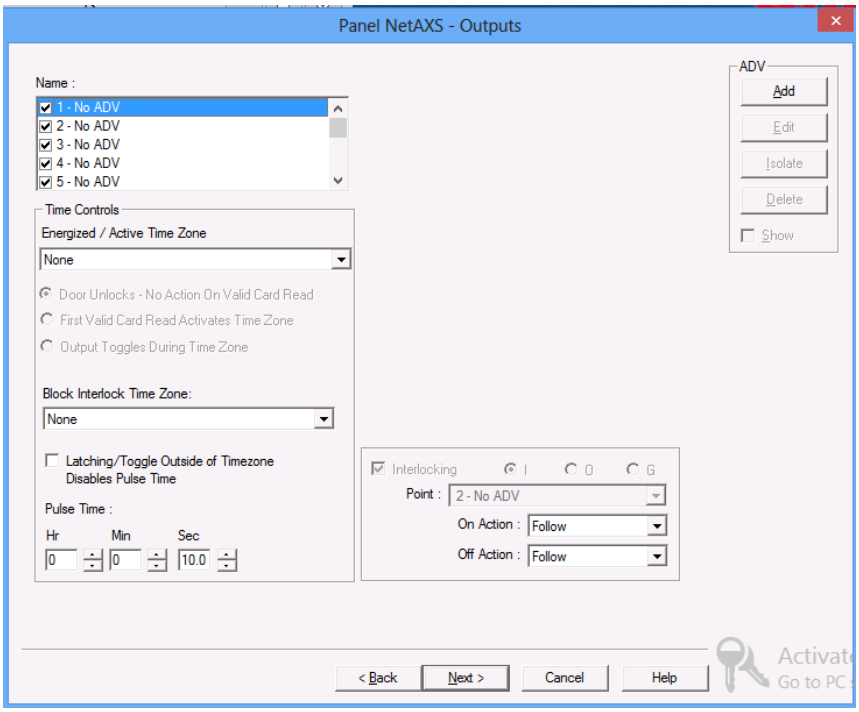
- O11 = Reader 1 LED (Pulse Time to 2.0 seconds)
- O12 = Reader 2 LED (Pulse Time to 2.0 seconds)
- O13 = Reader 3 LED (Pulse Time to 2.0 seconds)
- O14 = Reader 4 LED (Pulse Time to 2.0 seconds)
- O15 = Reader 3 Beeper
- O16 = Reader 4 Beeper

A maximum of 14 outputs are displayed for NetAXS-123 Gateway panel in the Outputs tab with the following default options:

- O1 = Door 1 lock (Pulse Time 10.0 seconds; Interlock to I2 follow / follow)
- O2 = Reader 1A/1B LED (Pulse Time to 2.0 seconds)
- O3 = Aux (Pulse Time to 10.0 seconds)
- O4 = Reader 1A/1B Buzzer
- O5 = n/a – allow no ADV
- O6 = n/a – allow no ADV
- O7 = Door 2 lock (Pulse Time 10.0 seconds; Interlock to I10 follow/follow)
- O8 = Reader 2A/2B LED (Pulse Time to 2.0 seconds)
- O9 = Aux (Pulse Time to 10.0 seconds)
- O10 = Reader 2A/2B Buzzer
- O11 = Door 3 lock (Pulse Time 10.0 seconds;Interlock to I14 follow/follow)
- O12 = Reader 3A/3B LED (Pulse Time to 2.0 seconds)
- O13 = Aux (Pulse Time to 10.0 seconds)
- O14 = Reader 3A/3B Buzzer

To configure output points to the panel:

1. In the **Panel NetAXS - 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** to 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.

3. In the **Energized/Active Time Zone** list, select a time zone.
4. Select any one of the following option buttons:
   - **Door Unlocks** - No Action On Card Read. Door works based on the time zone. This is selected by default.

- **First Valid Card Activates Time Zone** - Requires a valid card read within the time zone to enable the time zone (period in which doors are unlocked) to take effect.
- **Output Toggles During Time Zone** - Requires a valid card read within the time zone to enable the time zone period in which doors are unlocked) to take effect. Unlike the First Valid Card Activates Time Zone rule, you can swipe the card a second time to return the doors to a locked state.

Notes:

- All the three options listed are enabled only if you select a valid time zone from the **Energized/Active Time Zone** list.
- You can select either **First Valid Card** or **Output Toggles**.

5. In the **Block Interlock Time Zone** list, select a period during which the interlock, a programmed interaction between selected inputs and outputs, is disabled. During the selected Time Zone this point ignores all interlock actions to it, effectively disabling it from being a Reacting Component during the Time Zone. Outside of the Time Zone the point reacts to interlocks as expected

Note: Any interlock having the output as the Reacting Component is disabled, if the **Block Interlock Time Zone** is Active at that time.

6. Select the **Latching / Toggle Outside of Time Zone Disables Pulse Time** check box to toggle the state of the outputs between energized and de-energized status upon every activation (code use, interlock, or manual pulse).
7. Select **Sec**, **Min**, or **Hrs** and enter the Pulse Time to set the period during which the output point must be energized when triggered.

   The Pulse time specifies the duration for which a device assumes abnormal status. For example, it specifies how long a horn blows or a door strike remains released. The maximum number of hours is 1; the maximum number of Minutes is 59 when there is no hours set – if hours is set to 1, then the maximum number of Minutes is 45; the maximum number of seconds is 59.9 seconds as 10th of a second are allowed.
8. Set the **Interlocking** for the output point.

Note: Group Interlock is not displayed for NetAXS-123 panels.

9. Click **Next** to set the group or reader properties. The P**anel NetAXS - Group/Reader** dialog box appears.

Configuring groups to the NetAXS panel

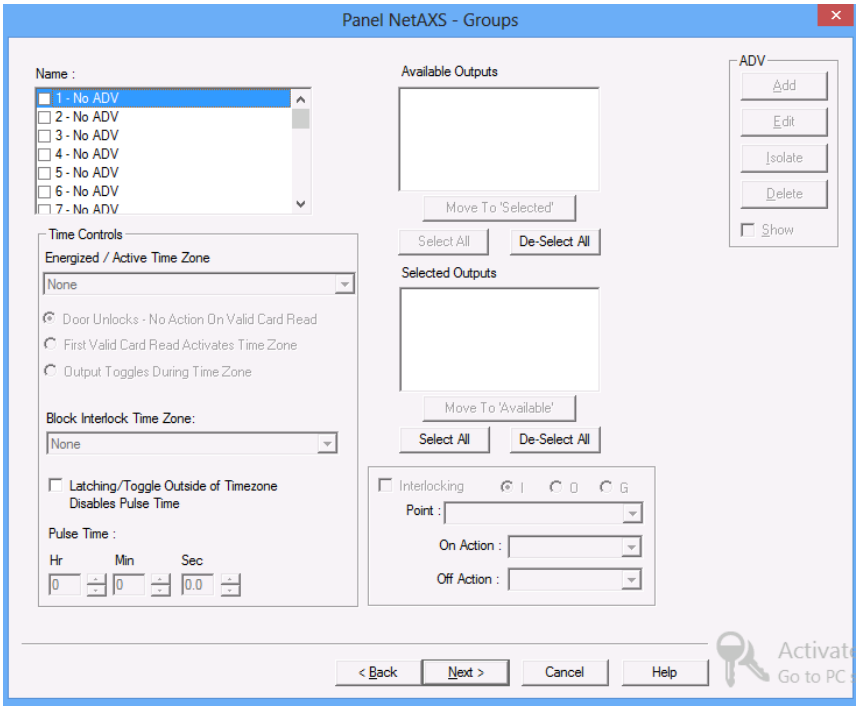
A Group is one or more active output points that are grouped together. Output relay groups enable a card read to activate more than one output relay for applications such as elevator control. As many as 32 groups can be defined per panel. A maximum of 128 groups are supported for NetAXS panels (NetAXS-4). A maximum of 76 outputs

can be selected for one group. The "Groups" feature is not supported by NetAXS-123 panels.

Note: The **Panel NetAXS - Groups** dialog box appears only if you have selected the **Group** check box in the **Panel NetAXS - Options** dialog box.

To define an output group:

1. In the **Panel NetAXS - 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. In the **Energized/Active Time Zone** list, select a time zone.
4. Select any one of the following option buttons:
   - **Door Unlocks** - No Action On Card Read - This is the default selection.
   - **First Valid Card Activates Time Zone** - Requires a valid card read within the time zone to enable the time zone (period in which doors are unlocked) to take effect.

- **Output Toggles During Time Zone** - Requires, like the First Card Rule, a valid card read within the time zone to enable the time zone period in which doors are unlocked) to take effect. Unlike the First Card Rule, however, the user can swipe the card a second time to return the doors to a locked state.

Note: All the three options listed are enabled only if you select a valid time zone from the Energized/Active Time Zone list.

5. In the **Block Interlock Time Zone** list, select a period during which the interlock, a programmed interaction between selected inputs and outputs, is disabled.

Note: Any interlock having that group as the Reacting Component is disabled, if the Block Interlock Time zone is active at that time.

6. Select the **Latching / Toggle Outside of Time Zone Disables Pulse Time** check box to toggle the state of the outputs between energized and de-energized status upon every activation (code use, interlock, or manual pulse).
7. Select **Sec**, **Min**, or **Hrs** and enter the Pulse Time to set the period during which the output point must be energized when triggered.
8. The maximum number of Hours is 1; the maximum number of Minutes is 59 when there is no hours set – if hours is set to 1, then the maximum number of Minutes is 45; the maximum number of seconds is 59.9 seconds as 10th of a second are allowed
9. Set the **Interlocking** for the output point.

Note: Group Interlocking is not applicable for NetAXS-123 panels.

10. Define ADV for each group. Click **Add** under **ADV**, set the ADV properties and click **OK**.
11. Click **Next** to configure readers to the panel. The **Panel NetAXS- Readers** dialog box appears.

Configuring a reader to the NetAXS panel in WIN-PAK CS

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.

NetAXS-4 panel supports 4 readers. NetAXS-123 panel supports 6 readers controlling 3 doors where the “A” reader is the primary reader for the door and the “B” reader is the Out reader for the door when so used. The B Reader can be programmed separately regarding name, Advanced Options, Anti-Passback configuration and Intrusion support. The B Reader cannot work alone as a Reader only. When used, the

B reader is tied to the A reader in terms of the interlock relationships pertaining to Door operation.

The NetAXS panel supports three types of modes:

- **Standard**: A mode where any valid card is granted access.
- **Supervisor**: A mode that enables a supervisor to enter without allowing general access. When this mode is enabled, the reader LED changes color four times per second (usually red then green). When the supervisor presents his card during the time zone just once, he gains access but does not enable general access. If the supervisor presents his card again within 10 seconds, he enables general access and the LED displays a steady red. After the supervisor presents his card twice to allow general access, he can disable the general access for the time zone by presenting his card again twice consecutively. The LED resumes rapid flashing between red and green. VIP cards do not need a supervisor card to gain access
- **Escort**: A mode that requires a supervisor escort to allow entry by an employee card holder. When this mode is enabled, the reader LED changes color four times per second (usually red then green) and employees must be accompanied by a supervisor to gain entry. When the supervisor presents his card, the LED goes solid red for 10 seconds, pending an employee credential. When the employee credential is swiped within 10 seconds of the supervisor card swipe, the door opens to admit the employee and the LED returns to rapid flashing. If the time expires and there is no employee credential swipe, the LED returns to rapid flashing and the reader returns to escort mode. A supervisor can gain entry by simply swiping the card twice. Unlike Supervisor mode, the Escort mode when active cannot be disabled during its time zone; a supervisor is required for all employee access during Escort mode time zone. VIP cards do not need a supervisor card to gain access.

Interoperability Features

Group SET sequence

*consecutive swipes within 10 Seconds

Works only for * card Found, Trace Card, Supervisor Card Found, VIP Card Found events.

* NS4 panel & Galaxy panel should be in the same communication Server.

Table 9-16 Group SET sequence

	Valid - Privileged - Std card + Active/Trace	**Valid - Privileged - Supervisor Card+Active/Trace**	**Valid - Privileged - VIP card + Active/Trace**	
Card And PIN Mode + Standard Mode	3 Swipe and PIN SETS	3 Swipe and PIN SETS	3 Swipe SETS	

Table 9-16 Group SET sequence

	Valid - Privileged - Std card + Active/Trace	**Valid - Privileged - Supervisor Card+Active/Trace**	**Valid - Privileged - VIP card + Active/Trace**	
Card And PIN Mode + Supervisor Mode	3 Swipe and PIN SETS after Supervisor authentication	6 Swipe and PIN SETS	3 Swipe SETS	
Card And PIN Mode + Escort Mode	Alternate 3 Supervisor & Standard card Swipe and PIN (total 6)	6 Swipe and PIN SETS	3 Swipe SETS	
Card or PIN Mode + Standard Mode	3 Swipe/PIN SETS	3 Swipe/PIN SETS	3 Swipe SETS	
Card or PIN Mode + Supervisor Mode	3 Swipe/PIN SETS after Supervisor authentication	6 Swipe/PIN SETS	3 Swipe SETS	
Card or PIN Mode + Escort Mode	Alternate 3 Supervisor & Standard card Swipes/PIN (total 6)	6 Swipe/PIN SETS	6 Swipe/PIN SETS	
Pin Only Mode + Standard Mode	3 PIN Entry SETS	3 PIN Entry SETS	3 Swipe SETS	**Note**: If the PIN is not unique for card numbers, then the first card in the Card Database is taken.
Pin Only Mode + Supervisor Mode	3 PIN SETS after Supervisor authentication	6 PINs SETS	3 Swipe SETS	
Pin Only Mode + Escort Mode	Alternate 3 Supervisor & Standard card PINs (total 6)	6 PINs SETS	3 Swipe SETS	
Card Only Mode + Standard Mode	3 Swipe SETS	3 Swipe SETS	3 Swipe SETS	

Table 9-16 Group SET sequence

	Valid - Privileged - Std card + Active/Trace	**Valid - Privileged - Supervisor Card+Active/Trace**	**Valid - Privileged - VIP card + Active/Trace**	
Card Only Mode + Supervisor Mode	3 Swipe SETS after Supervisor authentication	6 Swipe SETS	3 Swipe SETS	
Card Only Mode + Escort Mode	Alternate 3 Supervisor & Standard card Swipes (total 6)	6 Swipe SETS	3 Swipe SETS	

Group UNSET sequence

Table 9-17 Group UNSET sequence

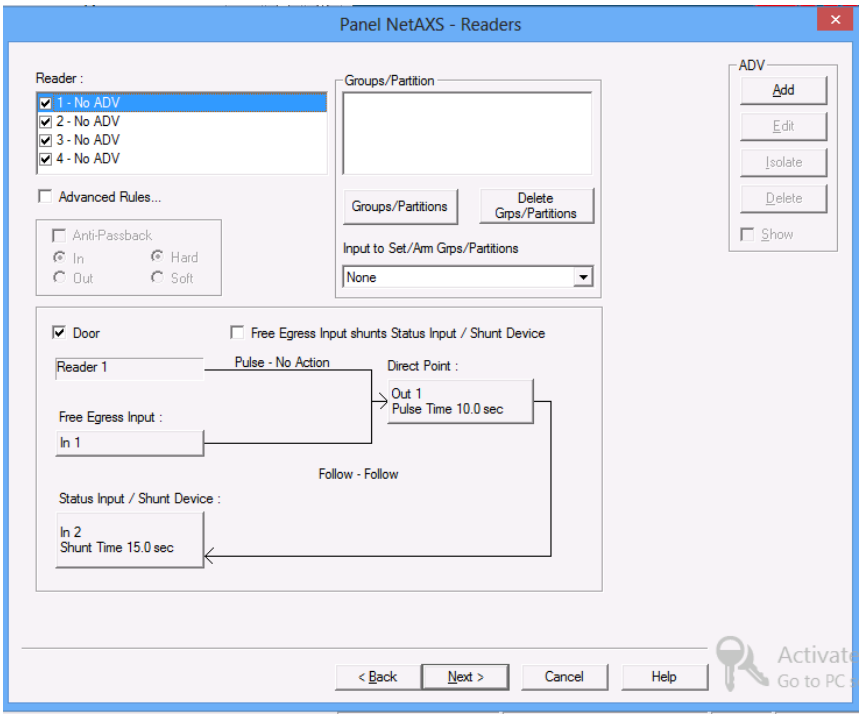
	Valid Std card + Active/Trace	**Valid Supervisor Card+Active/Trace**	**Valid VIP card + Active/Trace**	
Card And PIN Mode + Standard Mode	1 Swipe AND PIN UNSET	1 Swipe AND PIN UNSET	1 Swipe UNSET	
Card And PIN Mode + Supervisor Mode	1 Swipe and PIN UNSETS after Supervisor authentication	1 Swipe AND PIN UNSET	1 Swipe UNSET	
Card And PIN Mode + Escort Mode	1 Swipe and PIN UNSETS after Supervisor authentication	2 Swipe AND PIN UNSET	1 Swipe UNSET	
Card or PIN Mode + Standard Mode	1 Swipe/PIN UNSET	1 Swipe/PIN UNSET	1 Swipe UNSET	
Card or PIN Mode + Supervisor Mode	1 Swipe/PIN UNSETS after Supervisor authentication	1 Swipe/PIN UNSET	1 Swipe UNSET	
Card or PIN Mode + Escort Mode	1 Swipe/PIN UNSETS after Supervisor authentication	2 Swipe/PIN UNSET	1 Swipe UNSET	

Table 9-17 Group UNSET sequence

	Valid Std card + Active/Trace	**Valid Supervisor Card+Active/Trace**	**Valid VIP card + Active/Trace**	
Pin Only Mode + Standard Mode	1 PIN UNSET	1 PIN UNSET	1 Swipe UNSET	**Note**: If the PIN is not unique for card numbers, then the first card in the Card Database is taken.
Pin Only Mode + Supervisor Mode	1 PIN UNSETS after Supervisor authentication	1 PIN UNSET	1 Swipe UNSET	
Pin Only Mode + Escort Mode	1 PIN UNSETS after Supervisor authentication	2 PIN UNSET	1 Swipe UNSET	
Card Only Mode + Standard Mode	1 Swipe UNSET	1 Swipe UNSET	1 Swipe UNSET	
Card Only Mode + Supervisor Mode	1 Swipe UNSETS after Supervisor authentication	1 Swipe UNSET	1 Swipe UNSET	
Card Only Mode + Escort Mode	1 Swipe UNSET after Supervisor card Swipe (total 2)	2 Swipe UNSET	1 Swipe UNSET	

To define a reader:

1. In the **Panel NetAXS-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. Select the **Advanced Rules** check box to define advanced card rules for the selected reader. The **Advanced Reader-Options** dialog box appears.
4. Select one or more check boxes corresponding to a card format from the **Card Formats** list.
5. Click **Add New Format** to add a new card format. See 'Setting the card format for NetAXS panels' for more information.
6. Under **Card Rules**, perform the following:
   - In the **Disable Reader/Door - No Entry, No Exit allowed during this time** list, select a time zone for a reader during which all the card reads are ignored, with the exception of a VIP card, which is allowed access. Contact and Egress will report, but Egress does not open the door.
   - In the **Lock down Reader/Door - No Entry, Exit allowed during this time** list, select a time zone for a reader during which all card reads are ignored (except a VIP card), denies door entry but allows egress.

- In the **Card and PIN - Required during this time** list, select a time zone that grants card access with both a successful card read and a valid PIN entry at the door's keypad. You can perform the card read and PIN entry in either sequence. You must make the second entry within 10 seconds of the first entry, in either sequence. After selecting the time zone, select the **Standard** or **Supervisor** or **Escort** option buttons as applicable.
- In the **Card or PIN - Required during this time** list, select a time zone that grants access either with a successful card read or a valid PIN entry at the door's keypad. After selecting the time zone, select the **Standard** or **Supervisor** or **Escort** option buttons as applicable.
- In the **PIN only - Required during this time** list, select a time zone that grants access with only a valid PIN entered at the door's keypad. After selecting the time zone, select the **Standard** or **Supervisor** or **Escort** option buttons as applicable.
- In the **Card only - Card only allowed during this time** list, select a time zone that grants access to card having valid access level and time zone. After selecting the time zone, select the **Standard** or **Supervisor** or **Escort** option buttons as applicable.

7. Select the **Duress** check box and then select the output to be pulsed when a duress event is received from the **Output for Duress** list.
8. Select the **Anti-Passback** check box to enable this feature on the reader,which requires a valid card for entry and exit. Select one of the following options:
   - **In** - Applies to readers located outside the Anti-passback controlled area. Card holders use these readers when attempting to enter the Anti-passback controlled area. 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.
   - **Out** - Applies to readers located inside the Anti-passback controlled area. Card holders use these readers when attempting to exit the Anti-passback controlled area.
   - **Hard** - Validates IN/OUT status before allowing entry. A second swipe of the card at the same type of reader (IN/OUT) causes a Hard anti-passback violation and the user is denied entry.
   - **Soft** - Validates IN/OUT status before allowing entry. A second swipe of a card at the same type of reader (IN/OUT) causes a Soft anti-passback violation but the user is allowed entry.

Note: The **Anti-Passback** check box is enabled only if you select the **Anti-Passback** check box in the **Panel NetAXS-Options** dialog box.

9. Click **Add** under **ADV** and set the ADV properties to create an ADV for the reader. See 'Configuring an Abstract Device'.

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.

10. To associate groups to this reader, click **Groups/Partitions** and select the groups of Galaxy/Vista from the list.

Notes:

- Any valid card's partition can be disarmed after assigning the partition to a reader. However, the card can be armed after three card swipes.
- If you want to dissociate the group/partition from the reader, select the group and click **Delete Grps/Partitions**.

11. To associate Galaxy/Vista groups to the input point, select the input point from the **Input to set Arm Groups** list. For Interoperability features, see 'Interoperability Features'.

Note: Only the input points that are configured in this panel and not interlocked are listed in the **Input to Set/Arm Grps/Partitions** list.

12. To change the input point used as a free egress input:
    - Click **Free Egress Input** in the graphical form. The **Configure Free Egress** dialog box appears.
    - Select the **Egress Input** from the list.
    - 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. The maximum number of hours is 1; the maximum number of minutes is 59 when there is no hours set – if hours is set to 1, then the maximum number of minutes is 45; the maximum number of seconds is 59.9 seconds as 10th of a second are allowed.
    - 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. The maximum number of seconds is 6553.5 seconds as 10th of a second are allowed.
    - In the **Shunt Time Zone** list, select a time zone during which the input is ignored.
    - Click **OK** to save the settings or click **Set Defaults** to retain the default settings

13. To change the output pulsed on a valid card read:
    - Click **Direct Point** in the graphical form. The **Configure Direct Point** dialog box appears.
    - Select **I** or **O** to indicate Input Point, Output Point. The corresponding points are enabled in Direct Point. The Groups option **G** is disabled for NetAXS-4 panels. The Input Point **I** and Groups option, **G** is disabled for NetAXS-123 panels.
    - Select the **Direct Point** from the list.
    - Select **Sec**, **Min** or **Hr** and change the Pulse Time. The maximum number of hours is 1. When the hour field is blank, the maximum number of minutes is 59. When 1 is entered in the hour field, the maximum number of minutes is 45. The sum of all three units is the pulse time. Note that you can express seconds in tenths of a second.
    - In the **Energized /Active Time Zone** list, select a time zone.
    - 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.
    - Select the **Free Egress Input shunts Status Input / Shunt Device** check box to follow pulse no action on the direct point when a Free Egress Input is activated.
14. To trigger an action in another input, output or group as a series action of direct point:
    - Click **Status Input / Shunt Device** in the graphical form. The **Configure Status Input / Shunt Device** dialog box appears.
    - Select **I** or **O** to indicate Input Point, Output Point, or Group. The corresponding points are enabled in **Status Input / Shunt Device**. The Output Point, **O** is disabled for NetAXS-123 panels.
    - Select the **Status Input / Shunt Device** from the list.
    - 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.
    - 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.
    - Click **OK** to save the settings or click **Set Defaults** to retain the default settings.
15. Click **Next**.

The **NetAXS Panel Configuration Finish** dialog box appears for NetAXS- 123 Gateway panel. Click **Finish** to complete the configuration.

OR

The **Panel-NetAXS Downstream Devices** dialog box appears for NetAXS- 4 Gateway panel.

See Adding Downstream Devices for downstream devices configuration.

Configuring Readers to the NetAXS panel in WIN-PAK SE/PE

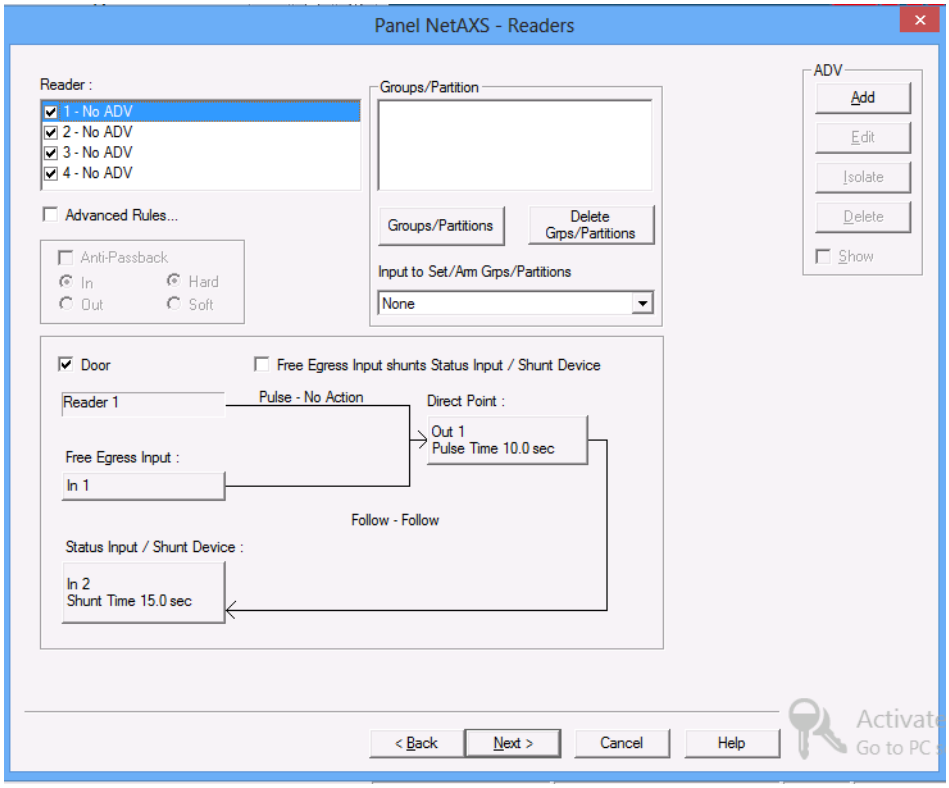
The number of readers available for the panel depends on the type of panel being configured. The WIN-PAK system automatically adds readers to the panel. By default, all the available readers are active and are defined as doors.

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.

NetAXS-4 panel supports 4 readers. NetAXS-123 panel supports 6 readers controlling 3 doors, where the “A” reader is the primary reader for the door and the “B” reader is the Out reader for the door if it is used. The B Reader can be programmed separately using the Name, Advanced Options, Anti-Passback configuration and Intrusion support. The B Reader cannot work alone as a Reader only. When used, the B reader is tied to the A reader in terms of the interlock relationships pertaining to the Door operation.

To define a reader:

1. In the **Panel NetAXS-Readers** dialog box, select a reader from the list to view its settings. The panel configuration displays 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. Select the **Advanced Rules** check box to define advanced card rules for the selected reader. The **Advanced Reader-Options** dialog box appears.
4. Select one or more check boxes corresponding to a card format from the **Card Formats** list.
5. Click **Add New Format** to add a new card format.
6. Under **Card Rules**, perform the following:
   - In the **Disable Reader/Door - No Entry, No Exit allowed during this time** list, select a time zone for a reader during which all the card reads are ignored, with the exception of a VIP card, which is allowed access. Contact and Egress will report, but Egress does not open the door.
   - In the **Lock down Reader/Door - No Entry, Exit allowed during this time** list, select a time zone for a reader during which all card reads are ignored (except a VIP card), denies door entry but allows egress.

- In the **Card and PIN - Required during this time** list, select a time zone that grants card access with both a successful card read and a valid PIN entry at the door's keypad. You can perform the card read and PIN entry in either sequence. You must make the second entry within 10 seconds of the first entry, in either sequence. After selecting the time zone, select the Standard or Supervisor or Escort option buttons as applicable.
- In the **Card or PIN - Required during this time** list, select a time zone that grants access either with a successful card read or a valid PIN entry at the door's keypad. After selecting the time zone, select the Standard or Supervisor or Escort option buttons as applicable.
- In the **PIN only - Required during this time** list, select a time zone that grants access with only a valid PIN entered at the door's keypad. After selecting the time zone, select the Standard or Supervisor or Escort option buttons as applicable.
- In the **Card only - Card only allowed during this time** list, select a time zone that grants access to card having valid access level and time zone. After selecting the time zone, select the Standard or Supervisor or Escort option buttons as applicable.

7. Select the **Duress** check box and then select the output to be pulsed when a duress event is received from the Output for Duress list.

Note: You must select a valid time zone from the **Card and PIN - Required during this time** list for the Duress feature to function.

Tip: Duress Output: Configures the output that trips when a cardholder enters a "duress PIN" at a keypad/card reader. A duress PIN is the PIN a user enters at a keypad when being forced (perhaps in a robbery) to open a door. The user enters his normal PIN, except one of the digits is one number higher or lower than the normal digit. This PIN opens the door, but it also triggers the designated duress output and produces an alarm. The Duress Output requires the

8. Select the **Anti-Passback** check box to enable this feature on the reader, which requires a valid card for entry and exit. Select one of the following options:
   - **In** - Applies to readers located outside the Anti-passback controlled area. Card holders use these readers when attempting to enter the Anti-passback controlled area. 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.
   - **Out** - Applies to readers located inside the Anti-passback controlled area. Card holders use these readers when attempting to exit the Anti-passback controlled area.
   - **Hard** - Validates IN/OUT status before allowing entry. A second swipe of the card at the same type of reader (IN/OUT) causes a Hard anti-passback violation and the user is denied entry.

- **Soft** - Validates IN/OUT status before allowing entry. A second swipe of a card at the same type of reader (IN/OUT) causes a Soft anti-passback violation but the user is allowed entry.

Note: The **Anti-Passback** feature is enabled only if you select the **Anti-Passback** check box **in** the **Panel NetAXS-Options** dialog box.

9. 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.

10. To associate groups to this reader, click **Groups/Partitions** and select the groups of Galaxy/Vista from the list.

Note: If you want to dissociate the group/partition from the reader, select the group and click **Delete Grps/Partitions**.

11. To associate Galaxy/Vista groups to the input point, select the input point from the I**nput to set Arm Groups** list.

Note: Only the input points that are configured in this panel and which are not interlocked are listed in the **Input to Set/Arm Grps/Partitions** list.

12. To change the input point used as a free egress input:
    - Click **Free Egress Input** in the graphical form. The **Configure Free Egress** dialog box appears.
    - Select the **Egress Input** from the list.
    - Select **Sec**, **Min** or **Hr** and change the **Shunt Time**.

Tip: The Shunt Time specifies the time for which the inputs are shunted, or de-activated. For example, it specifies how long a door strike remains released. Enter the desired number of hours (1024 maximum), minutes (60 maximum), and seconds (60 maximum). The sum of all three units is the shunt time.

    - Enter the **Debounce Time** in seconds.

Tip: The Debounce Time specifies the time during which the input remains in a new state before generating an alarm. For example, if a Normal state is changed to Alarm, the state must remain in Alarm for five seconds before an alarm is generated. The maximum number of seconds is 6553.5 seconds as 10th of a second is allowed.

    - In the **Shunt Time Zone** list, select a time zone during which the input is ignored.
    - Click **OK** to save the settings or click **Set Defaults** to retain the default settings.

13. To change the output pulsed on a valid card read:

- Click **Direct Point** in the graphical form. The **Configure Direct Point** dialog box appears.
- Select **I** or **O** to indicate Input Point, Output Point. The corresponding points are enabled in Direct Point. The Groups option "**G**" is disabled for NetAXS-4 panels.

Note: The Input Point, **i** and Groups, **G** are disabled for NetAXS-123 panels.

- Select the **Direct Point** from the list.
- Select **Sec**, **Min** or **Hr** and change the **Pulse Time**.

Tip: The Pulse Time specifies the duration for which the device assumes abnormal status. For example, it specifies how long a horn blows or a door strike remains released. Enter the desired number of hours (1024 maximum), minutes (60 maximum), and seconds (60 maximum). The sum of all three units is the pulse time.

- In the **Energized /Active Time Zone** list, select a time zone.
- 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.

14. Select the **Free Egress Input shunts Status Input / Shunt Device Pulse - No Action Direct Point** check box to follow no action on the direct point when a Free Egress Input is activated.

    To trigger an action in another input, output or group as a series action of direct point:

    - Click **Status Input / Shunt Device** in the graphical form. The **Configure Status Input / Shunt Device** dialog box appears.
    - Select **I** or **O** to indicate Input Point, Output Point. The corresponding points are enabled in Status Input / Shunt Device.

Note: The Output point, **O** is disabled for NetAXS-123 panel.

    - Select the **Status Input / Shunt Device** from the list.
    - 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.
    - 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.
    - Click **OK** to save the settings or click **Set Defaults** to retain the default settings

15. Click **Next**.

- The **NetAXS Panel Configuration Finish** dialog box appears if you are adding a NetAXS 123 Gateway panel. Click **Finish** to complete the configuration.

Or

- The **Panel-NetAXS Downstream Devices** dialog box appears if you are adding a NetAXS -4 Gateway panel. Go to step **16**.

See the 'Adding downstream devices' section for downstream devices configuration

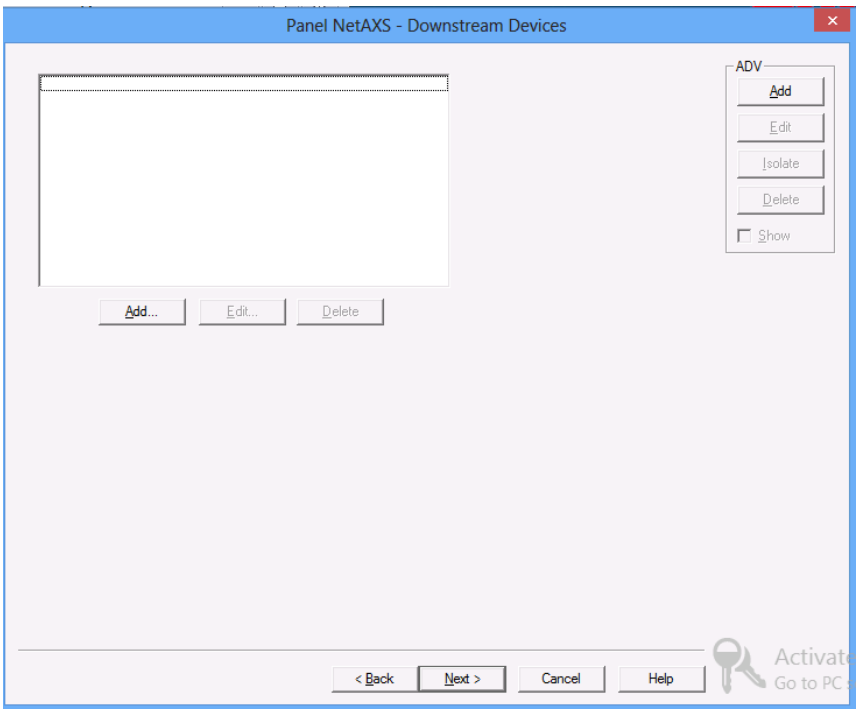
Adding downstream devices

By default, the NetAXS-4 panels come with a fixed number of inputs and outputs. Use the "Downstream Devices" feature to support extended inputs and outputs for these panels. This feature is not available for NetAXS-123 panels.

The extended inputs and outputs can be added using the "NX4IN" and "NX4OUT" options. A maximum of two NX4IN and four NX4OUT can be added, resulting in a maximum of six downstream devices.

To add downstream devices:

1. In the **Panel NetAXS - Downstream Devices** dialog box, click **Add**.



The **Select Device** dialog box appears.

2. Select "**NX4IN**" or "**NX4OUT**" as applicable.
   - NX4IN is a 32 input and 0 output downstream add on device.

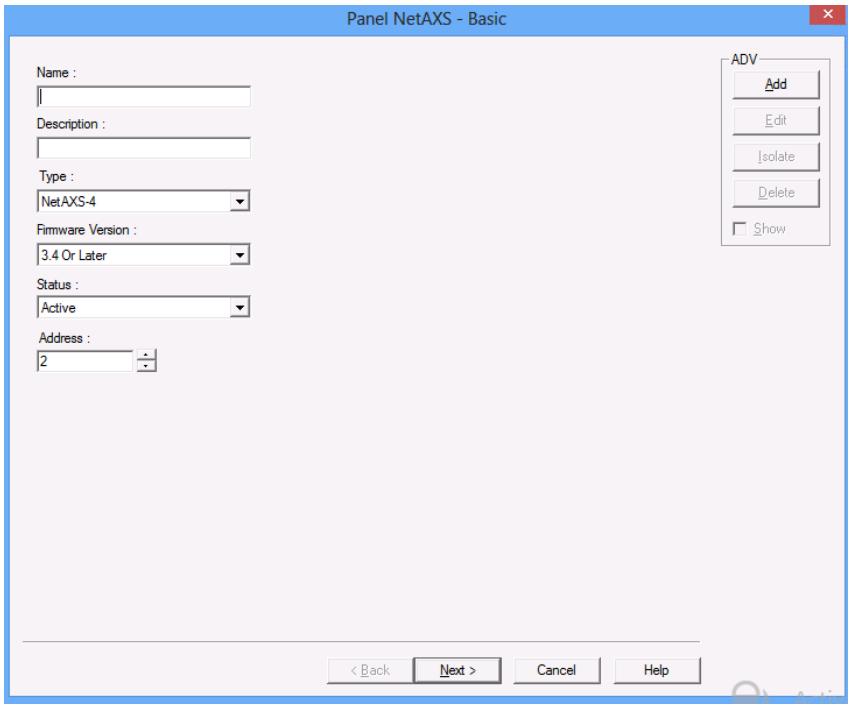
- NX4OUT is a 2 input and 16 output downstream add on device.

3. If you select "**NX4IN**", then the **Panel NX4IN** dialog box appears.
   - In the **Address** list, select "1" or "2" as applicable. See 'Configuring input points to the NetAXS panel' for information on configuring extended inputs.
   - Click the **Inputs** tab to configure the inputs.
   - If you select **Address** as "1" in the **NX4IN Basic** tab, then the input number starts at 25 and ends at 56. If you select **Address** as "2" in the **NX4IN Basic** tab, then the input number starts at 57 and ends at 88.
   - Go to step **5**.
4. If you select "**NX4OUT**", then the **Panel NX4OUT** dialog box appears.
   - In the **Address** list, select any value from 3 through 6.
   - Click the **Inputs** tab to configure the inputs. See 'Configuring input points to the NetAXS panel' for more information on configuring extended inputs.
   - If you select **Address** as "3" in the **NX4OUT Basic** tab, then the input number starts at 89 and ends at 90. If you select **Address** as "4" in the **NX4OUT Basic** tab, then the input number starts at 91 and ends at 92. If you select **Address** as "5" in the **NX4OUT Basic** tab, then the input number starts at 93 and ends at 94. If you select **Address** as "6" in the **NX4OUT Basic** tab, then the output number starts at 95 and ends at 96.
   - Click the **Outputs** tab to configure the outputs. See 'Configuring output points to the NetAXS panel' for more information on configuring extended outputs.
   - If you select **Address** as "3" in the **NX4OUT Basic** tab, then the output number starts at 17 and ends at 32. If you select **Address** as "4" in the **NX4OUT Basic** tab, then the output number starts at 33 and ends at 48. If you select **Address** as "5" in the **NX4OUT Basic** tab, then the input number starts at 49 and ends at 64. If you select **Address** as "6" in the **NX4OUT Basic** tab, then the input number starts at 65 and ends at 80.
5. To define an ADV for each NX4IN or NX4OUT, Click **Add** under ADV. Set the ADV properties and click **OK**. See 'Configuring an Abstract Device'for more information.
6. Click **Next**. The **NetAXS Panel Configuration Finish** dialog box appears.
7. Click **Finish** to complete the Panel configuration.

Adding downstream NetAXS4 panels to a NetAXS-4 Gateway panel

To add downstream NetAXS-4 panels to NetAXS-4 Gateway panel:

1. Right-click on a NetAXS-4 gateway panel, and click **Add NetAXS Panel**. The **Panel-NetAXS Basic** dialog box appears.



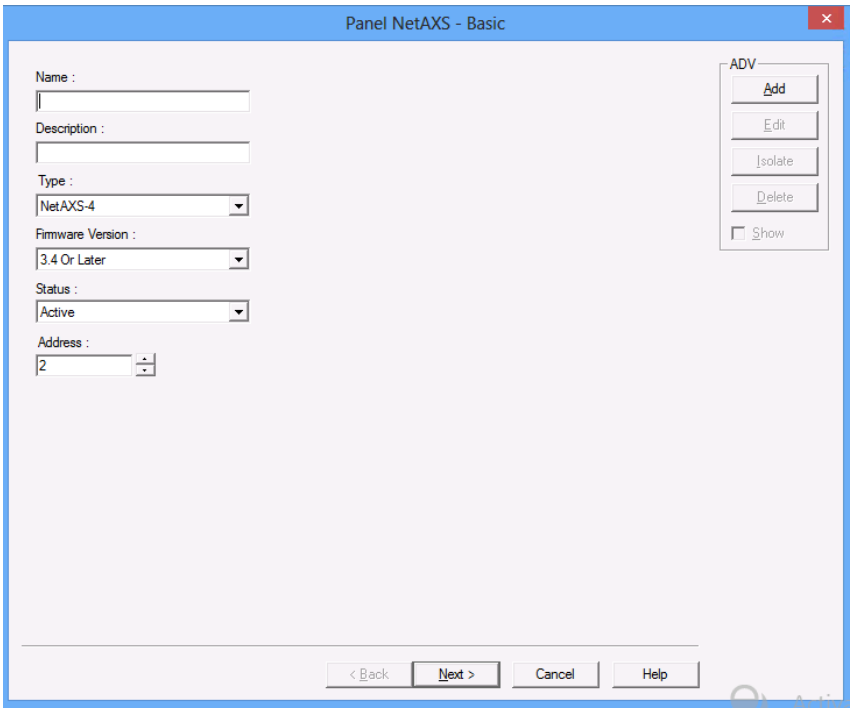
2. Type a unique **Name** for the panel. This field is mandatory, and is limited to a maximum of 30 alphanumeric characters. This field does not allow typing empty spaces.
3. By default, "NetAXS-4" is selected in the **Type** list.

   The **Firmware Version** of the panel is displayed by default.
4. In the **Status**, select one of the following states for 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.
   - **Not Present** - The panel is not present in the system.
5. Enter the panel Address between 2 and 31.
6. To continue the NetAXS-4 downstream panel configuration, repeat the procedure from step 14 onwards as detailed in 'Adding or Editing a NETAXS Panel'.

Adding downstream NetAXS-123 panels or NetAXS-4 panels to a NetAXS-3 Gateway panel

To add downstream NetAXS-123 or NetAXS-4 panels:

1. Right-click on a NetAXS-123 gateway panel, and click **Add NetAXS Panel**. The **Panel-NetAXS Basic** dialog box appears.



2. Type a unique **Name** for the panel. This field is mandatory, and is limited to a maximum of 30 alphanumeric characters. This field does not allow typing empty spaces.
3. In the **Type** list, select "NetAXS-123" or "NetAXS-4" as applicable.

   The **Firmware Version** of the panel is displayed by default.
4. In the **Status**, select one of the following states for 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.
   - **Not Present** - The panel is not present in the system.
5. Enter the panel **Address** between 2 and 31.
6. To continue the NetAXS-4 downstream panel configuration, repeat the procedure from step 14 onwards as detailed in 'Adding or Editing a NETAXS 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 9-18 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

Table 9-18 Describing the available actions for points

Action	Description
Energize	Turns the point on
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 in the device map. A direct connection to the Intelligent Controller enables the Host PC to communicate directly with the P-Series panel through an RS-232 connection or through TCP/IP on the P-Series panel.

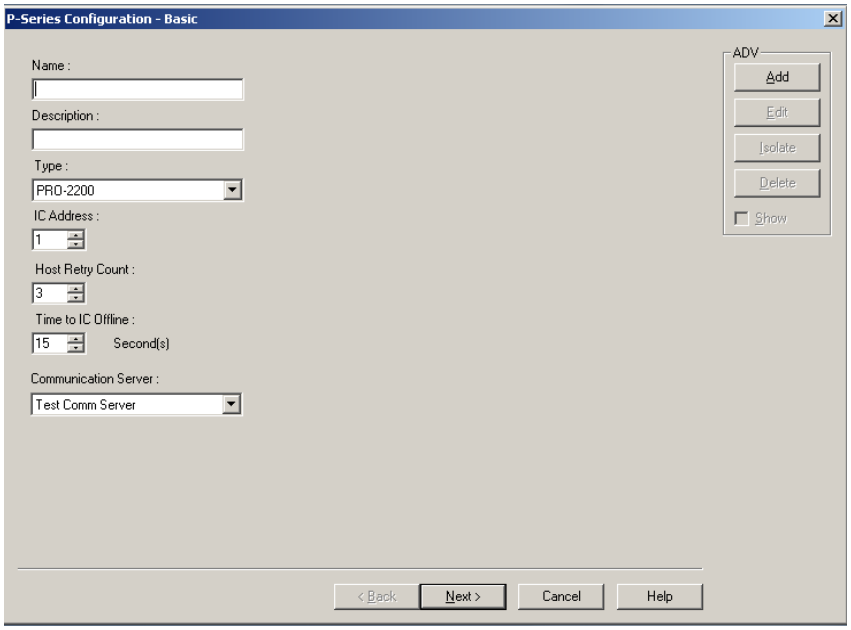
P-Series panel types available in WIN-PAK CS/SE/PE are PRO-2000, PW-5000, and PW-6000. Eight SIO Boards can be included in the PRO-2000 panel and 32 SIO Boards can be included in both the PW-5000 and PW-6000 panel.

Note: You must perform th P-Series panel installation for the first time manually. After you finish adding a new panel, a **Panel Initialization** message box appears. And then, later on, any configuration changes to the panel is automatically downloaded from the service map.

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. Right-click the **Devices** folder, click **Add** and click **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 panel **Type** from the available options of PRO-2200, PRO-3200, PW-5000 or PW-6000.
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.

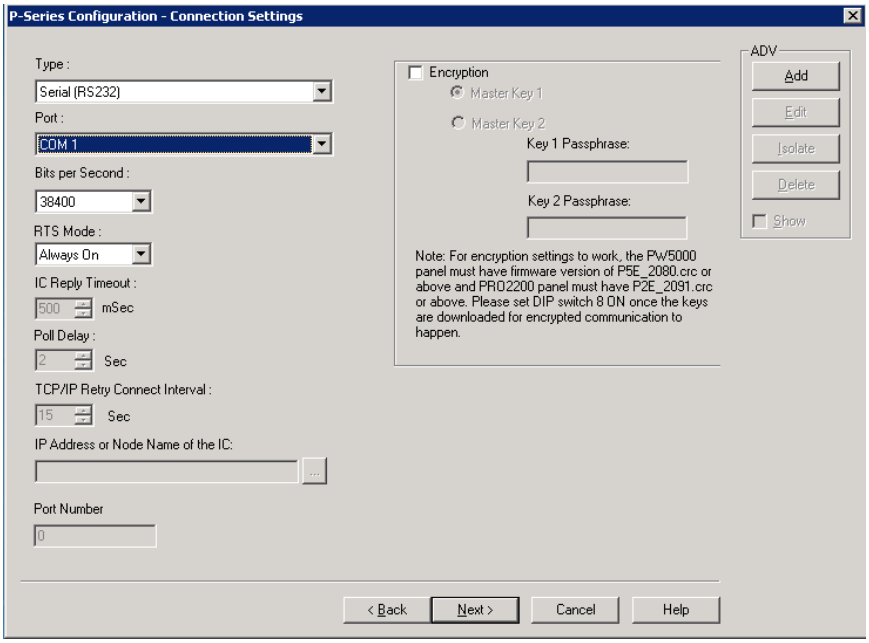
Note: The **Time to IC Offline** can be set from 10 to 65 seconds (with 15 seconds as the default). A range of 10 to 30 seconds is recommended for most applications.

9. Select the **Communication Server** from the list.
10. Click **Add** under **ADV** and set the ADV properties to create an ADV for the P-Series panel.
11. 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.

    e. **Port Number**: This is the Port number to which a socket connection must be established.

Note: This Port Number is available only in WIN-PAK CS and the Port Number can be set from 5001 to 65535.

4. Click **Next** to set the system configuration.

Configuring the Encryption Settings

An encrypted communication provides additional data security between customers access control panels and the WIN-PAK CS server.

Notes:

- This section is applicable only for WIN-PAK CS.

- For encryption settings to work, the PW5K panel must have firmware version of P5E_2080.crc or above and PRO2200 panel must have P2E_2091.crc or above.

To configure the encryption settings for Direct P series Panels.

1. Select the **Encryption** check box to enable the encryption settings.

   When you select the **Encryption** check box, by default, **Master Key 1** is selected and the corresponding **Key 1 Passphrase** is enabled.

   A key passphrase is a sequence of words or ordinary text that can be used for automatically generating an encryption key.

2. Select **Master Key 1** to be used for encryption/decryption and define the corresponding **Key 1 Passphrase** to generate the encryption key or password.
3. Alternatively, you can also set the **Master Key 2** for encryption/decryption and define the **Key 2 Passphrase** for generating the encryption key or password.

Note: The length of a key passphrase must be between 8 and 18 characters.

Configuring the Encryption settings for P Series Panels (using WIN-PAK CS)

Notes:

- This section is applicable only for WIN-PAK CS.
- For encryption settings to work, the firmware versions present in the PRO2200 must be P2E_2091.crc or above and for PW5K it must be P5E_2080.crc or above.

To configure the encryption settings for P series Panels using WIN-PAK CS:

1. Bring the panel online under normal communication without encryption and DIP Switch 8 in OFF State.
2. Now from WIN-PAK CS UI Enable encryption for the panel and configure a set of master keys 1 and 2.
3. Right-click **Initialize** menu from control map and download the encryption settings for the panel.
4. Observe that the panel communication is established.
5. Now, make the DIP Switch 8 on the panel to ON state and switch OFF and switch ON the panel.
6. Observe that the panel communication is established.

   DIP Switch 8 ON means that the data going to the panel must be encrypted. So, the panel will still be online when encryption is enabled in WIN-PAK CS UI and DIP Switch 8 in OFF State. However, if DIP Switch 8 is ON and encryption is disabled in WIN-PAK CS UI then, incorrect password alarms will come and panel communication will be lost.

Note: The encryption password are not the master keys. They are derived from the master keys. Hence the master keys can be shown in WIN-PAK CS UI.

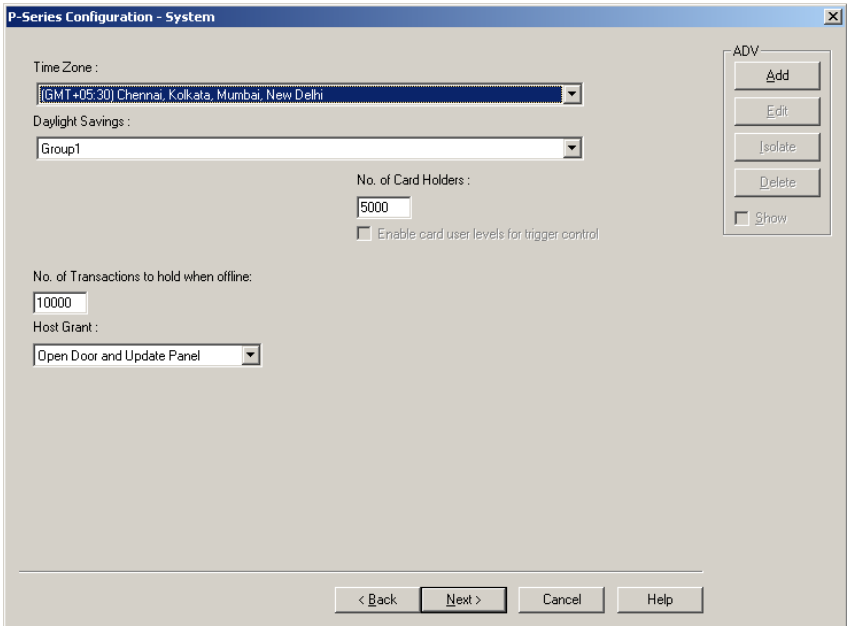
Notes:

- In the P-series configuration page, after connecting through the encryption key, if the Master key is changed or shifted between master key 1 to master key 2, the panel goes offline. Later, when the panel is online, the panel connects through the modified master key.
- For the PRO-3200/PW-6000 panels, after the panel is connected through the encryption key, if you clear the **Encryption** check box in the WIN-PAK CS configuration page, the panel goes offline. Only after you select the **Data Security** as **None** in the panel web interface window, the panel is online.
- For the PRO-2200/PW-5000 panels, after the panel is connected through the encryption key, if you clear the **Encryption** check box in the WIN-PAK CS configuration page, the panel goes offline. The panel is online only after you switch OFF the DIP Switch 8 and reboot the panel.

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.

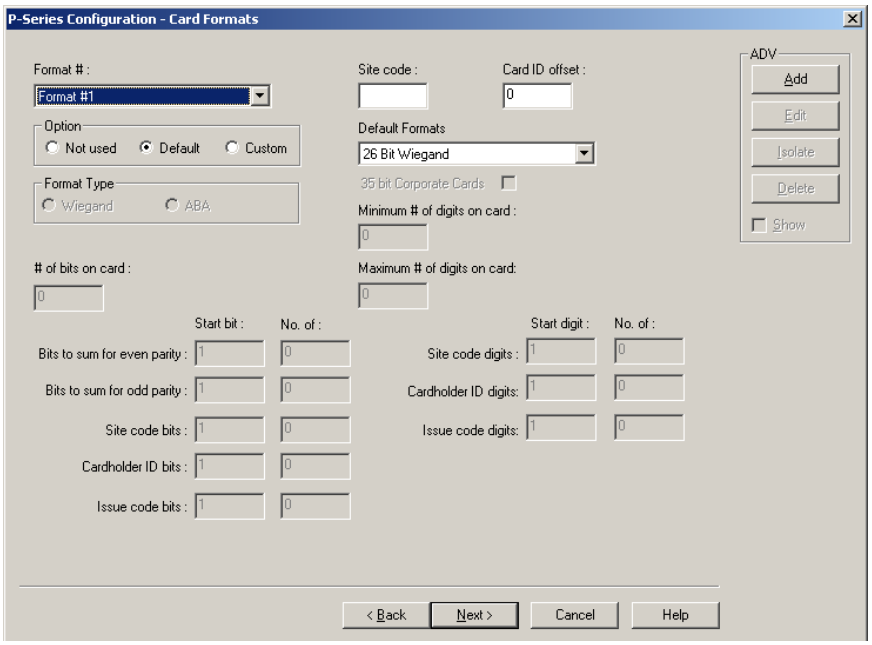
   Tip: Adding an extended memory board to the Intelligent Controller provides more memory to work with.
6. Select the **Host Grant** option to provide fault tolerance, even if the card is not found in the panel device.
   - Host Grant options are used when, for example, a number of cards are entered in 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 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

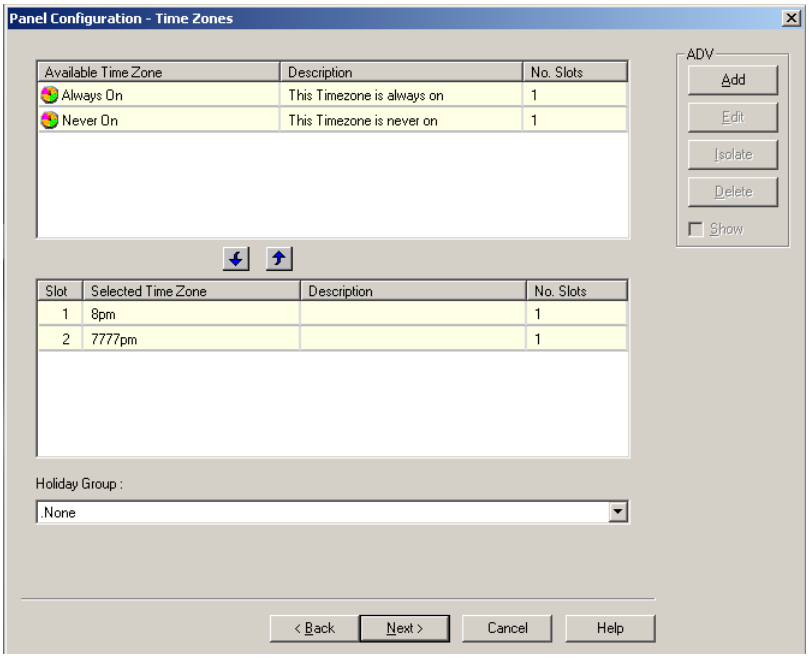
35 bit Corporate Cards	Cleared
Minimum # of digits on card	1
Maximum # of digits on card	12
Site code digits	**Start digit**: 1 **No of**: 0
Cardholder ID digits	**Start digit**: 1 **No of**: 12
Issue code digits	**Start digit**: 1 **No of**: 0

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

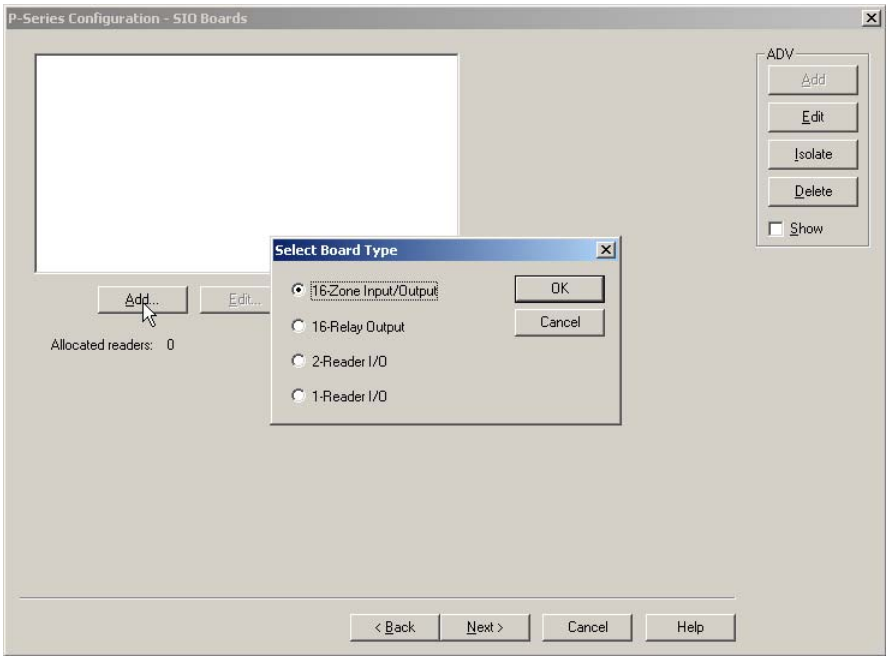
The number of readers, inputs, and outputs that can be connected to the controller is based on the type of SIO Board that is added to the Intelligent Controller. The available SIO Board types are:

SIO Board Type	Maximum Inputs	Maximum Outputs	Maximum Readers
16-Zone Input/Output	16	2	0
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.

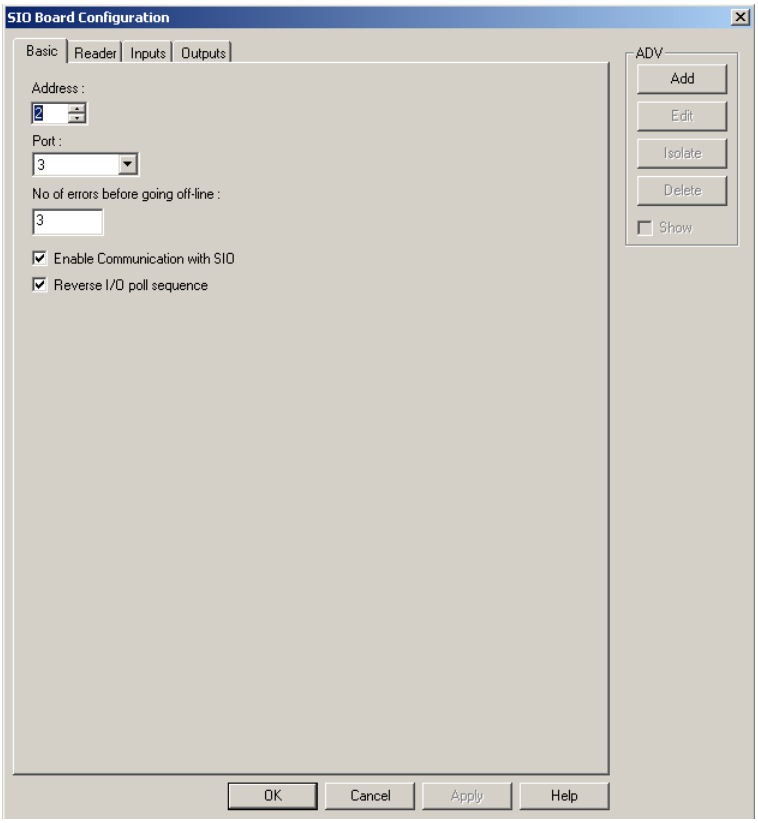
To add an SIO board of 2-Reader IO board type:

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.



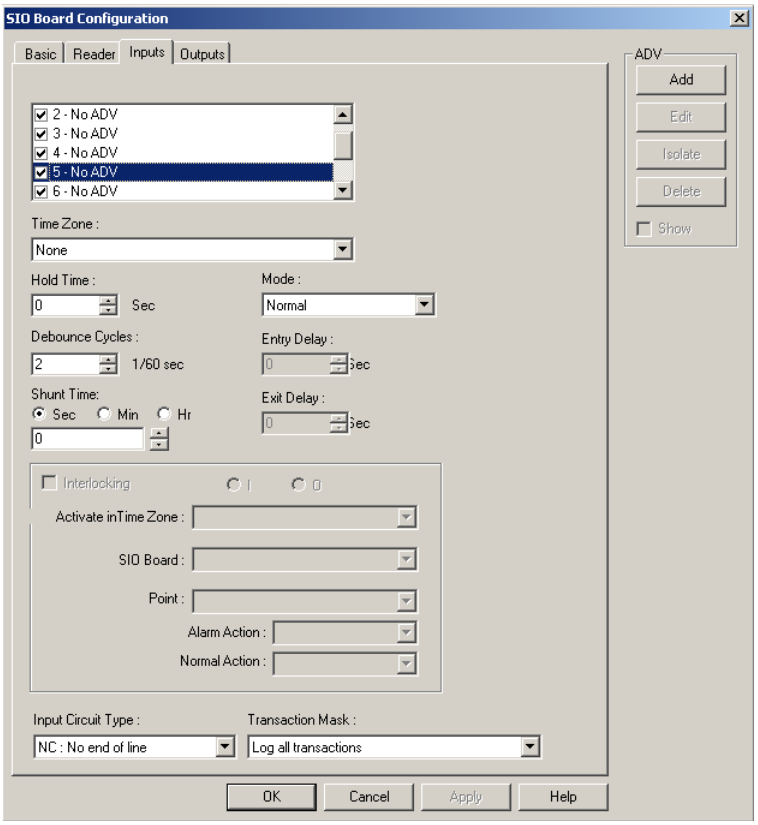
2. In the **Select Board Type** dialog box, select the **2-Reader I/O** board type.

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. Skip the **Reader** tab, and click the **Inputs** 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 a 2 Reader SIO board, In 1 and In 3 are status inputs and In 2 and In 4 are free egress inputs. Whereas for a 1 reader SIO board, In 1 is the status input and In 2 is the free egress 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 9-19 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.

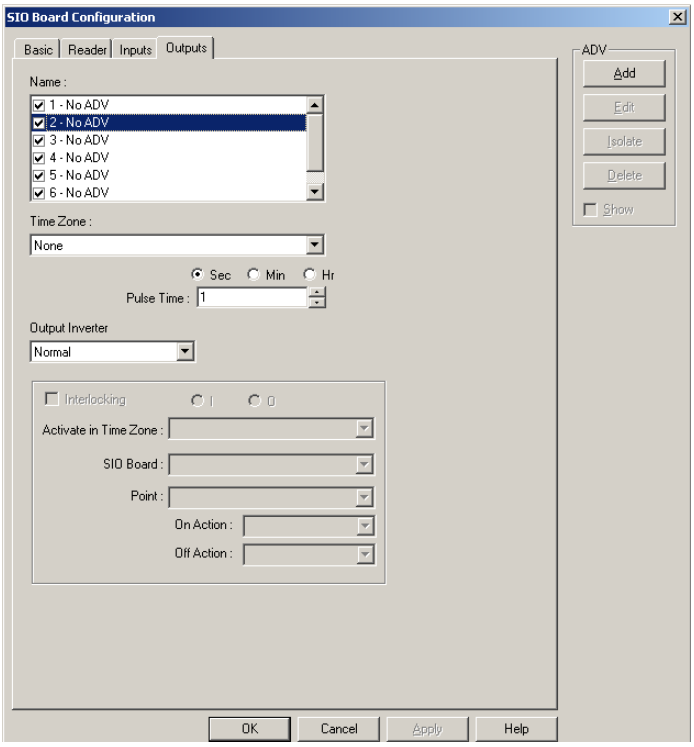
21. Select the **Input Circuit Type** for specifying whether a point is supervised or unsupervised. The available types are:

Table 9-20 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 supervised three-state circuit using 1K resistors (Alarm, Normal, or Trouble) in a normally closed contact points.
NO: Std end of line Normally Opened	Refers to a supervised three-state circuit using 1K resistors (Alarm, 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 CS/SE/PE.

23. Click the **Outputs** 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:

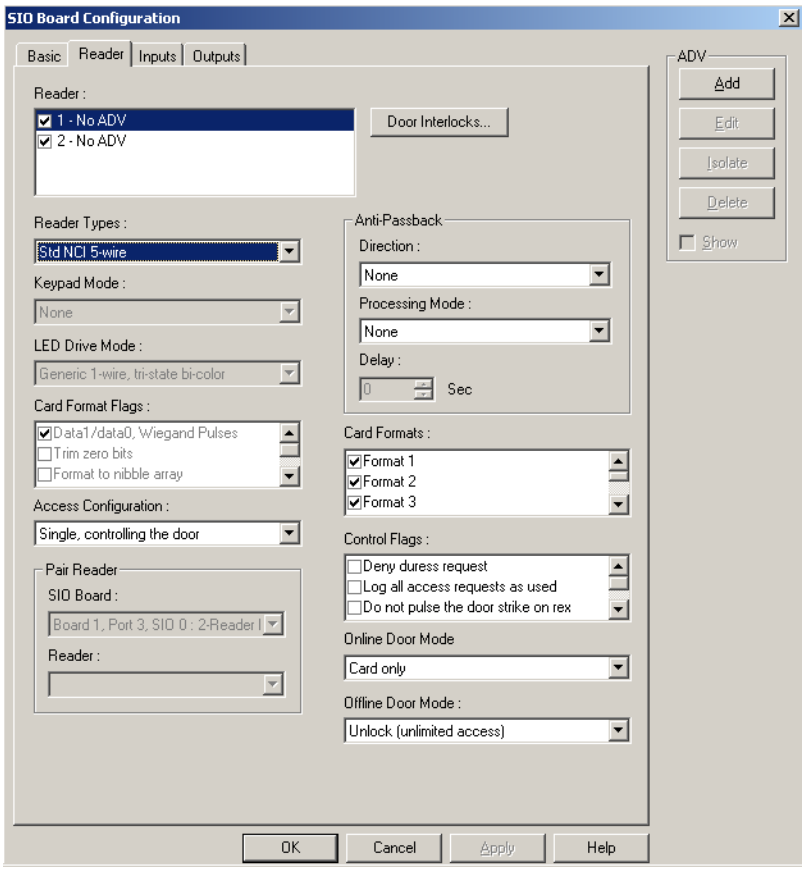
Table 9-21 Describing the Output Inverter settings

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.



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 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 9-22 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 9-23 Describing Outline 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**, **Locked**, and **Facility code only**.

Notes: Follow the below steps in WIN-PAK SE/PE.

- To associate galaxy groups or vista partitions to this reader, click **Group/Partitions** and select the groups from the list.

- 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.

42. Click **OK** to configure the SIO Board.
43. 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

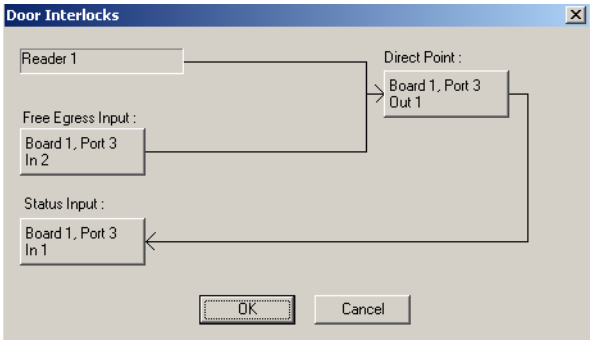
Door Interlocks show input and output relationships available for the reader. Two types of locking devices can be configured with WIN-PAK CS:

- 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.



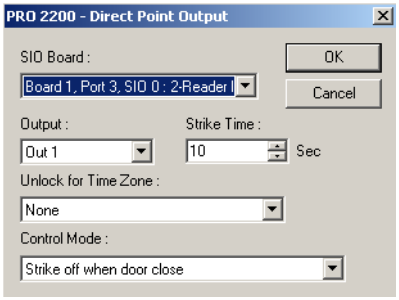
3. Use this dialog box to edit the default settings of the Direct Point, Free Egress Input, and Status Input as desired.

Note: When you click **Door Interlocks**, WIN-PAK CS 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.

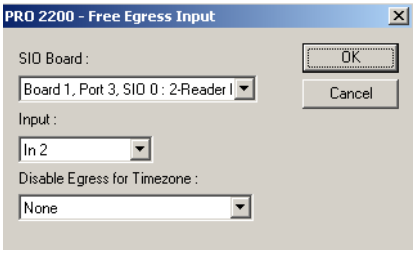
4. Specify the **Strike Time**. This is the amount of time the direct point relay is pulsed or interlocked. The default for this field is ten seconds, but can be set up to 60 seconds.
5. In **Unlock for Time Zone** list, select a Time Zone during which the door must be kept unlocked.

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.

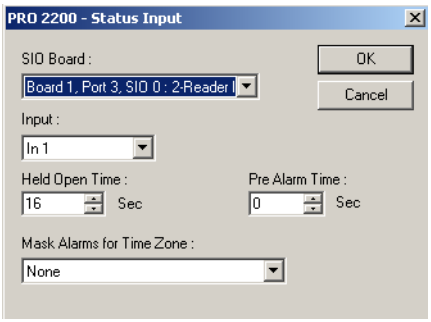
4. In the **Disable Egress for Time Zone** list, select a time zone during which the Egress is disabled.
5. Click **OK** to return to **Door Interlocks** dialog box.

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 CS/SE/PE for use in controlling doors.

1. In the **Door Interlocks** dialog box, click **Status Input** to display the **Status Input** dialog box.



2. Select the **SIO Board** for 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 in 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.

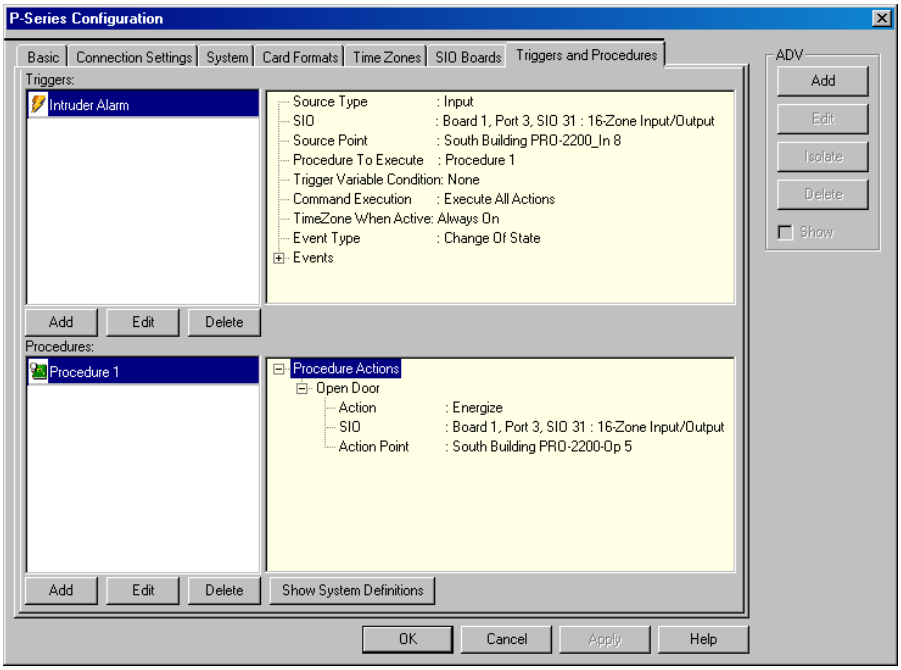
Note: To view the system-defined triggers and procedures, click the **Show System Definitions** button. After you click this button, it changes to **Hide System Definitions**, which hides the system-defined triggers and procedures when you click it.

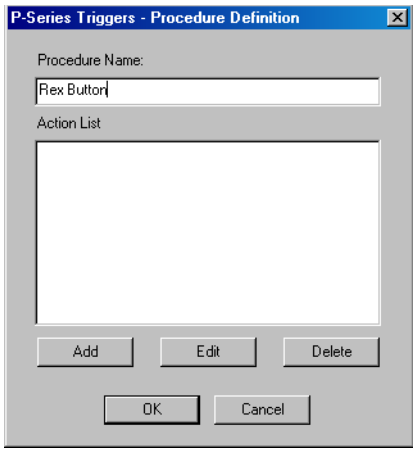
Adding a new procedure

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.

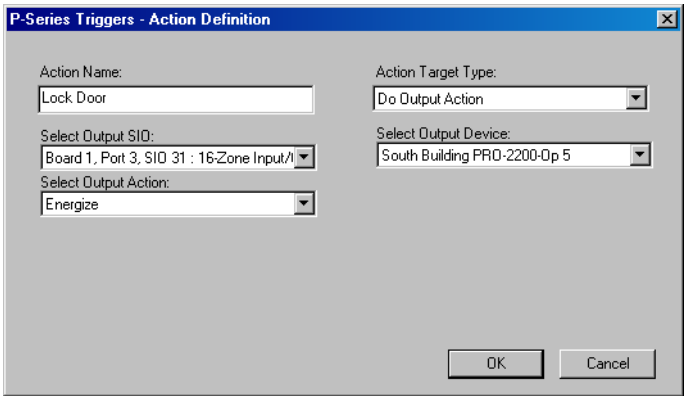
To add a new procedure:

1. In the **Triggers and Procedures** dialog box, click **Add** at the bottom of the Procedures section. The **Procedure Definition** dialog box appears.





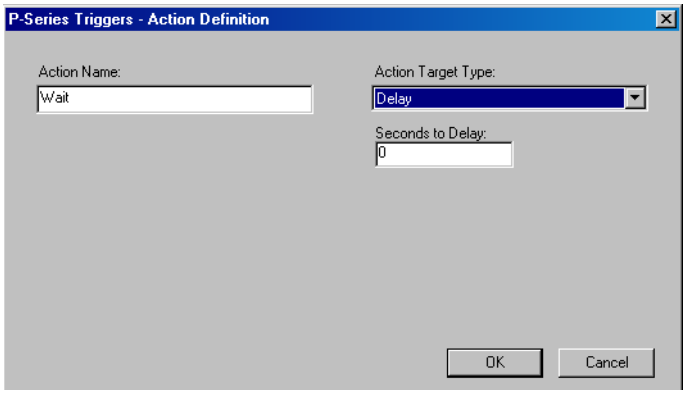
2. Enter a **Procedure Name**. This name is unique and descriptive for easy reference.
3. To define a new action for the procedure, click **Add** at the bottom of the **Action List** box. The **Action Definition** dialog box appears.



4. Type an **Action Name**.
5. In the **Action Target Type** list, select the target of the action: **Reader, Output, Input, Delay**.

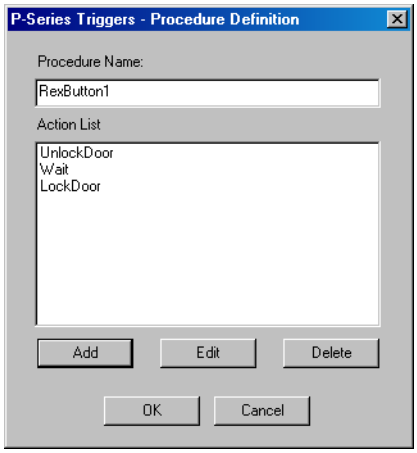
   The remaining fields in the dialog box are activated, based on the selected action target type.
6. If you select **Do Output Action** as the **Action Target Type**, perform the following steps:
   a. In the **Select Output SIO** list, select the SIO board on which the output action must occur.
   b. 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 the **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.

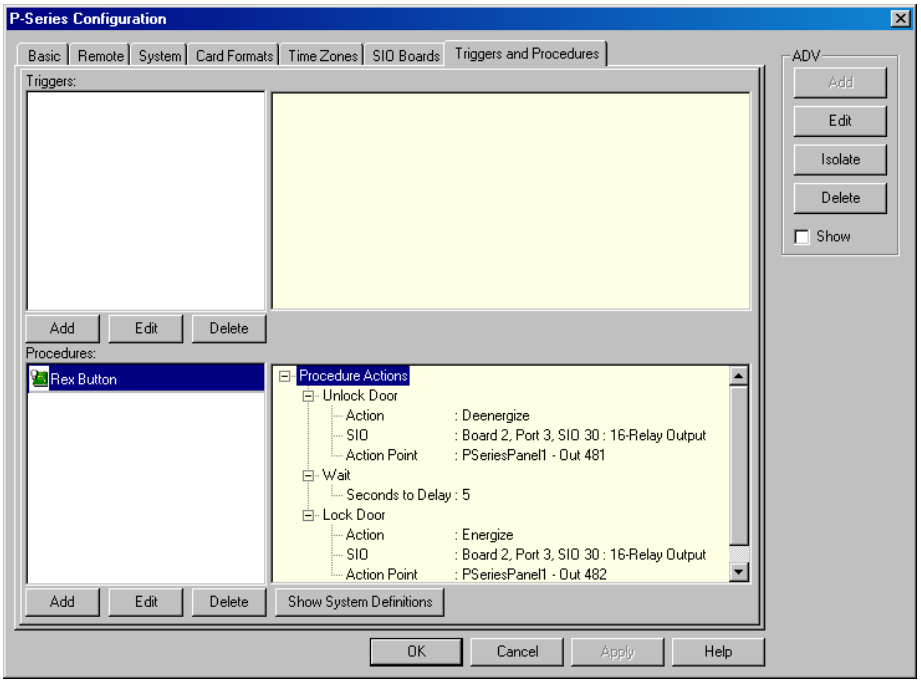


b. Click **OK** to return to **Procedure Definition** dialog box.

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.



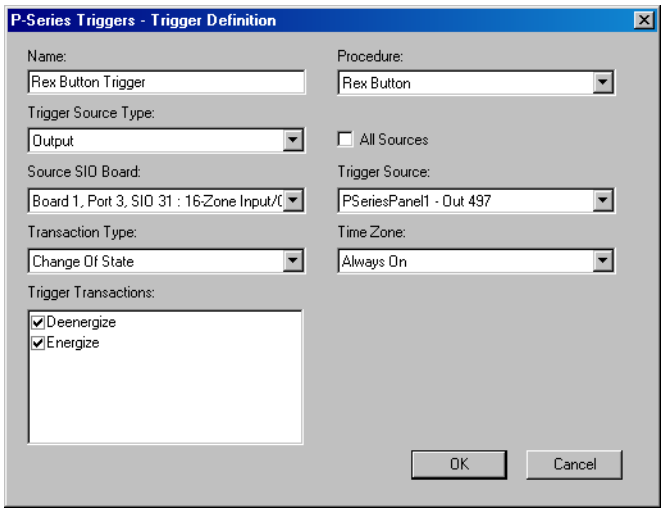
Tip: The newly-defined procedure is shown in the **Procedures** list. To look at the detailed view of each action defined for this procedure, expand the **Procedure Actions** tree.

Adding a New Trigger

After defining a procedure, it must be associated to a trigger for triggering an action.

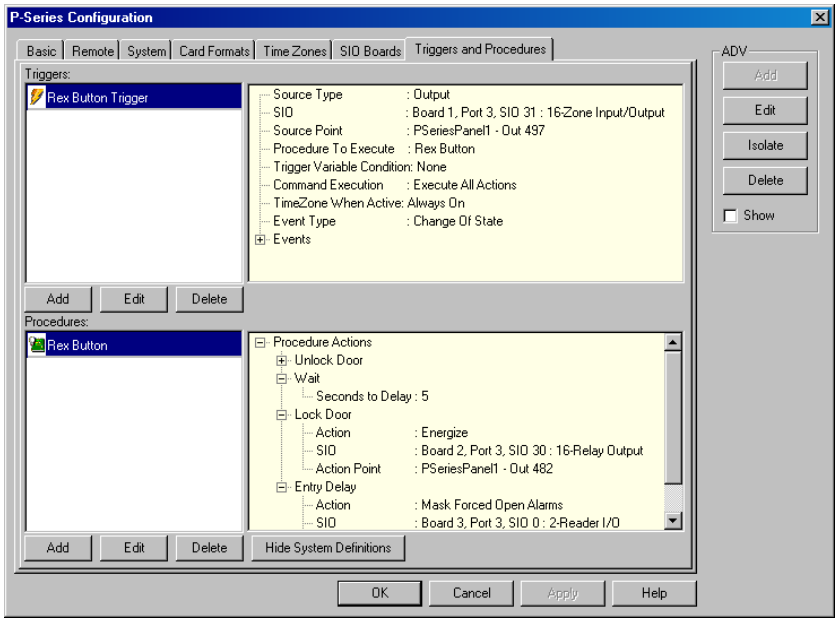
To add a new trigger:

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 a FIN4000 Panel for WIN-PAK SE/PE

The FIN4000 is an access control panel, based on the IP connectivity and biometric security. The FIN4000 biometric devices, installed at each door, work not only as card or fingerprint scanners and card readers, but also as intelligent access controllers. It combines unique biometric identification with configurable access card capabilities.

The FIN4000 also provides administrators with the ability to read HID proximity cards and read, issue, and format MIFARE and iCLASS access cards.

The FIN4000 V1.00 supports the following devices:

- FIN4000xxK-20K
- FIN4000xx-10K
- FIN4000xxK-10K
- FIN4000-Enroll
- FIN4000AC-10K
- FIN4000AC-100K
- FIN4000MIK-20K
- FIN4000ACK-100K

The FIN4000xxK-20K or FIN4000xx-10K devices act simultaneously as both a controller and a reader.

Action Group

Table 9-24 Action Group

Action	Description
Door Open	These are door status messages.
Door Closed	
Door Forced Open	
Door Forced Open Clear	
Door Held Open	
Door Held Open Clear	
Identification, Not Granted	This message appears in the HON FIN4000K-20K panel if the Credential Holder's access to the entrance is restricted in the following scenarios: Access is restricted due to a different time zone, as it is not assigned in the **Access Level**. Access is restricted due to invalid time zone. This occurs during the 1:N operation mode.
Verification, Not Granted	This message appears in the HON FIN4000K-20K panel if the Credential Holder's access to the entrance is restricted in the following scenarios: Access is restricted due to a different time zone, as it is not assigned in the **Access Level**. Access is restricted due to invalid time zone. This occurs during the 1:1 operation mode.
Not Granted	This message appears in the HON FIN4000K-10K and HON FIN4000-10K panels if the Credential Holder's access to the entrance is restricted in the following scenarios: Access is restricted due to a different time zone, as it is not assigned in the **Access Level**. Access is restricted due to invalid time zone.
Timed Anti-Passback Violation	This message appears during the following scenarios: If the entrance/door is set with the timed anti-passback. If the Credential Holder is trying to access the same door more than once in the same period.
Invalid Authentication Mode	This message appears when the mode of operation, that is, the combination of credentials is not accepted at the current instance. This adheres to the time zone for each operation modes set in the **Panel Configuration** > **Operation Mode**.

Table 9-24 Action Group

Action	Description
Inactive/Expired Credentials	This message appears if the credentials has been used for accessing before the **Activation Date** or after the **Expiration Date**.
Verification Failed	This message appears when there is mismatch between the user details and the access credentials (Card, Fingerprint, ID or PIN).
Verification Success, Fingerprint	These access messages appear for any entry through 1:1 operation modes and valid credentials.
Verification Success, PIN	
Verification Success, Card and Fingerprint	
Verification Success, Card and PIN	
Verification Success, Card	
Verification Success, Card, Fingerprint and PIN	
Verification Success, Fingerprint and PIN	
Verification, Duress	
Identification Failed	This message appears when there is mismatch between the user details and the access credentials (Fingerprint or PIN).
Identification Success, Fingerprint	These access messages appear for any entry through 1:N operation modes and access credentials.
Identification Success, Fingerprint and PIN	
Identification, Duress	
User Download Success	This message appears when the credential detail of the **Credential Holder** is successfully transferred to the panel.

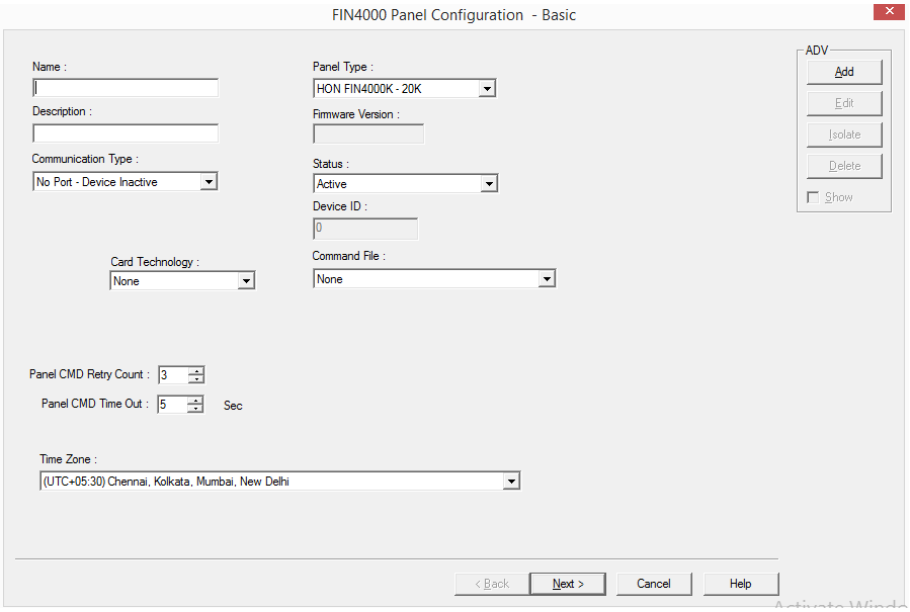
Table 9-24 Action Group

Action	Description
User Download Failed	This message appears when the credential details of the **Credential Holder** is not transferred to the Panel. In case of HON FIN4000K-20K, if the **Check Duplicate Finger** is selected, then, the credentials being downloaded could be a duplicate of some other registered credential in the same panel. Try full panel initialization.
User Download to Card Success	This message appears when the details of the **Credential Holder** is successfully written on the card (Template on Card).
User Download to Card Failed	This message appears when the details of the **Credential Holder** has not been written on the card (Template on Card).
Verify through Card: Duress	These messages appear during the Template on Card operations and Access.
Verify through Card Success	
Verify through Card Failed	
Card Usage Limit Exceeded already	
Card Time Limit Exceeded already	
Invalid Card Authentication Mode	
Inactive/Expired Card	
Access not Granted: Card	

Setting Up a Direct Connection

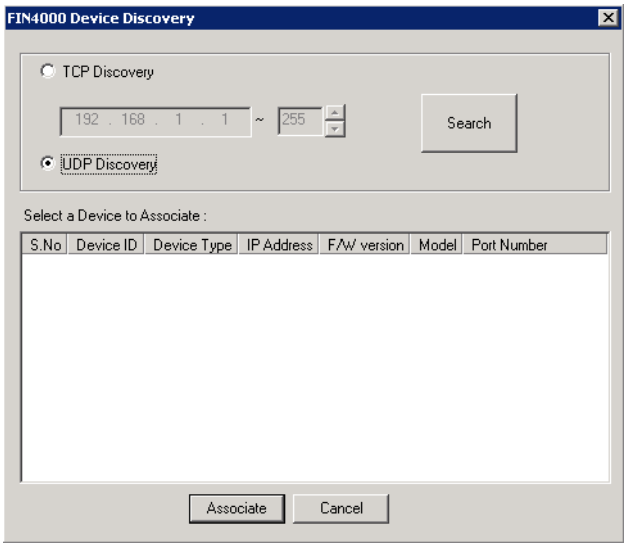
To set up a direct connection of panel:

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 FIN4000 Biometric Device**. 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. In the **Communication Type** list, select any one of the following communication types for FIN4000 panel communication.
    - **No Port - Device Inactive**- If you select this option, no communication is established between the WIN-PAK and the FIN4000 panel and the device remains inactive.
    - **TCP/IP Connection** - If you select this option, type the IP-Address or Node name of the FIN4000 panel.

6. In the **Network Address** field, click **Discover**. The **FIN4000 Device Discovery** dialog box appears.



Note: Honeywell recommends you to **Discover** and then associate the device.

7. In the **FIN4000 Device Discovery** dialog box, select to search for devices using **TCP** or **UDP** protocols. When you select TCP, you can specify an IP address range, the type of device you are searching for (HON-FIN4000xxK-20K: 1470, HON-FIN4000xx-10K, HON-FIN4000xxK-10: 1471, or manually enter the IP address), and the port to search with. If you select UDP, you can search for devices only in the same subnet. UDP Discovery is faster than TCP Discovery.
8. Select the device from the list and then click **Associate**. The selected device is associated with the panel.

Note: After device association, the following fields are automatically populated and grayed out.

- Panel Type
- Firmware Version
- Network Address
- Device ID
- Port Number
- Card Technology

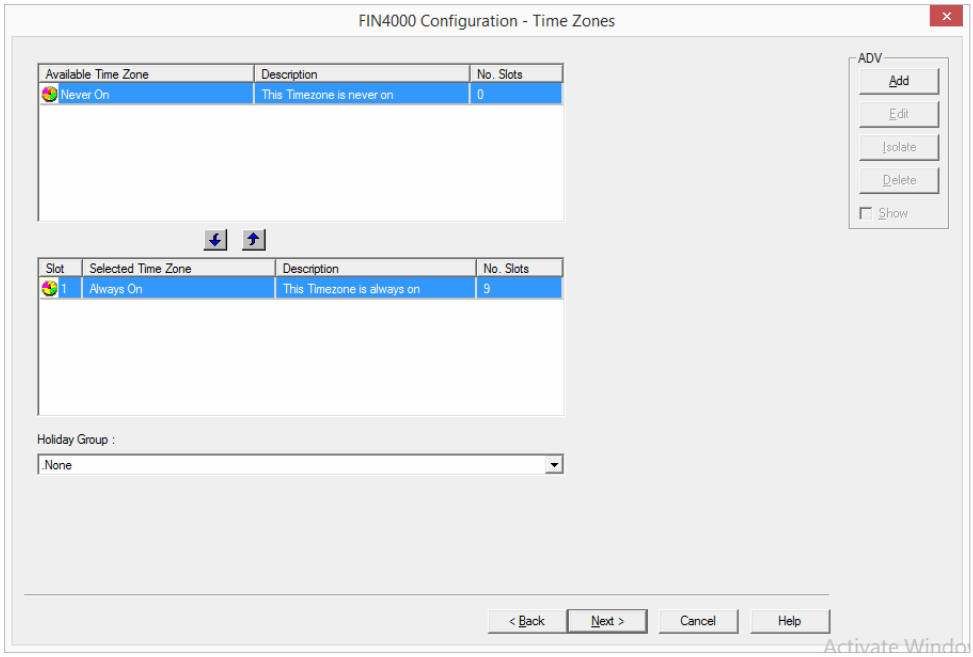
9. Select the type of panel in the **Panel Type** list. The available FIN4000 panel types are HON-FIN4000 10K, HON-FIN4000K 10K, HON-FIN4000K 20K, FIN4000AC-10K, FIN4000AC-100K, FIN4000MIK-20K and FIN4000ACK-100K.
10. Select the firmware version number of your panel in the **Firmware Version** list.

11. 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 SE/PE before completing the panel installation. If the panel is marked Not Present, no transactions are saved.
12. In the **Command File** list, select a command file that is applicable to a panel.
13. Select the following panel defaults as applicable
    - **Panel CMD Retry Count** - Select the number of times (between 0 and 5) at which 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.
    - **Panel CMD Time Out** - Select the waiting time (between 1 and 30) for receiving a response from the panel and time out of the command. By default, the loop waits for 20 seconds.
14. Select the **Time Zone** from the drop-down list.
15. Click **Add** under **ADV** and set the ADV properties to create an ADV for the FIN4000 panel.
16. Click **Next** to configure the connection settings.

To configure the time zone settings of the direct FIN4000 panel

Note: A maximum of 45 slots per time zone can be associated to FIN4000 panels. Each time zone can have a maximum of five time slots per day. The "Always on" time zone is selected by default for all FIN4000 panels.

1. In the **FIN4000 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 operation mode options. The **FIN4000 Configuration - Operation Mode** dialog box appears.

Configuring the Operation Mode

You can configure the Operation Mode for the following type of panels:

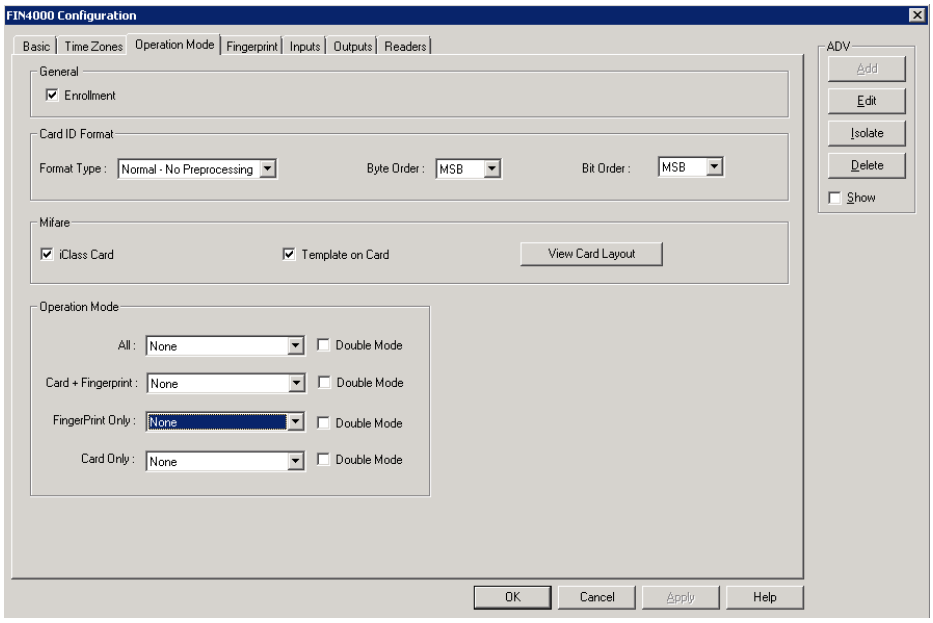
- **FIN4000 K-20K**: For more information on configuring K-20K panels, refer to, ‘Configuring the operation mode to the FIN4000 K-20K panel’.
- **FIN4000 -10K:** For more information on configuring 10-K panels, refer to, ‘Configuring operation mode to the FIN4000 10-K panel’.
- **FIN4000 K-10K:** For more information on configuring K-10-K panels, refer to ‘Configuring operation mode to the FIN4000 K-10K panel’.
- **FIN4000AC-10K:** For more information on configuring AC-10-K panels, refer to ‘Configuring operation mode to the FIN4000 AC - 10K and FIN4000 AC - 100K panels’.
- **FIN4000AC-100K:** For more information on configuring AC-100-K panels, refer to ‘Configuring operation mode to the FIN4000 AC - 10K and FIN4000 AC - 100K panels’.

- **FIN4000MIK-20K:** For more information on configuring MIK-20-K panels, refer to 'Configuring the operation mode to the FIN4000 ACK - 100K and FIN4000 MIK - 20K panels'.
- **FIN4000ACK-100K:** For more information on configuring ACK-100-K panels, refer to 'Configuring the operation mode to the FIN4000 ACK - 100K and FIN4000 MIK - 20K panels'.

Configuring the operation mode to the FIN4000 K-20K panel

To configure the operation mode to the FIN4000 K-20K panel:

1. In the **FIN4000 Configuration - Operation Mode** dialog box, under **General**, you can select:
   - **Enrollment**: The availability of FIN4000 panel for capturing the images of fingerprints or issuing access cards.
   - **Fast ID Matching**: The process to set the device to allow quicker authentication. You must input only the first two digits of the user ID and scan a single fingerprint.



2. Under **Card ID Format**, select the following:
   - **Format Type**: Select if the type of pre-processing to occur on card ID data must be of **Normal** or **Wiegand** type. If you select **Normal**, the card ID data is processed in its original form. If you select **Wiegand**, the device interprets the card ID data according to the Wiegand format settings.
   - **Byte Order**: Select to specify if you must swap the ID card data between cards and devices by Most Significant Byte (MSB) or Least Significant Byte (LSB).

- **Bit Order**: Select to specify if you must swap the ID card data between cards and devices by MSB or LSB.

3. Under **Mifare/iCLASS Cards**, select the following:

   - **Mifare/iCLASS Cards**: Select to enable Mifare/iCLASS card authorization.
   - **Template on Card**: Select to use the template on the Mifare/iCLASS card for authorization.

Note: The **Template on Card** option is not applicable for HID models.

Click **View Card Layout** to view the Mifare/iCLASS card layout used by the device.

Note: The **View Card Layout** displays the card format configuration for HID models.

4. Under **1: 1 Operation Mode**, select the following:

   - **ID/Card + Fingerprint** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus fingerprint authorization.
   - **ID/Card + Password** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus password authorization.
   - **ID/Card + Fingerprint/Password** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus fingerprint or password authorization.
   - **Card Only** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require only card authorization.
   - **ID/Card + Fingerprint + Password** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus fingerprint plus password authorization.

5. Under **1: N Operation Mode**, select the following:

   - **1:N Schedule** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set a schedule for using fingerprint only authentication.
   - **1:N Operation Mode** - From the drop-down list, select **Auto/Freescan**, **Ok/Function Key**, or **None**, based on the requirement. This enables you to set a method for activating the fingerprint sensor.
   - **Double Mode** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require authentication of two users' access cards or fingerprints. The timeout for presenting the second authentication is 15 seconds.

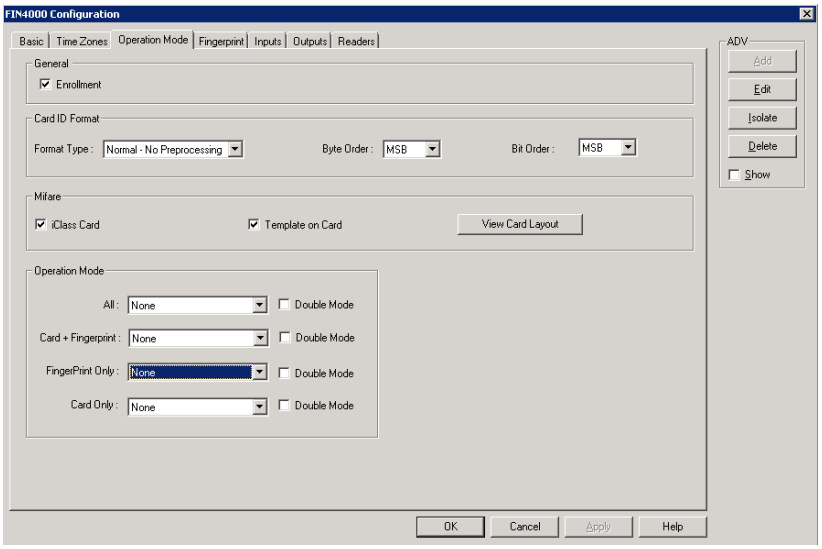
6. Click **Next** to set the fingerprint formats for the FIN4000 panel.

Configuring operation mode to the FIN4000 10-K panel

To configure the operation mode to the FIN4000 10-K panel:

1. In the **FIN4000 Configuration - Operation Mode** dialog box, under **General**, you can select:

   - **Enrollment**: The availability of FIN4000 panel for capturing the images of fingerprints or issuing access cards.



2. Under **Card ID Format**, select the following:

   - **Format Type**: Select if the type of pre-processing to occur on card ID data must be of **Normal** or **Wiegand** type. If you select **Normal**, the card ID data is processed in its original form. If you select **Wiegand**, the device interprets the card ID data according to the Wiegand format settings.
   - **Byte Order**: Select to specify if you must swap the ID card data between cards and devices by Most Significant Byte (MSB) or Least Significant Byte (LSB).
   - **Bit Order**: Select to specify if you must swap the ID card data between cards and devices by MSB or LSB.

3. Under **Mifare/iCLASS Cards**, select the following:

   - **Mifare/iCLASS Cards:** Select to enable Mifare/iCLASS card authorization.
   - **Template on Card:** Select to use the template on the Mifare/iCLASS card for authorization.

Note: The **Template on Card** option is not applicable for HID models.

Click **View Card Layout** to view the Mifare/iCLASS card layout used by the device.

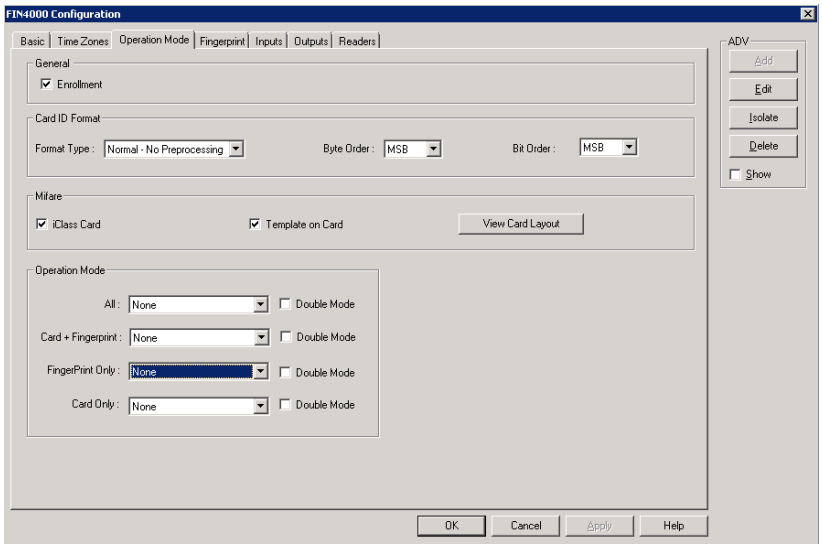
Note: The **View Card Layout** displays the card format configuration for HID models.

4. Under **Operation Mode**, for each of the following options, select to enable **Double Mode**, which requires verification of two users' credentials to gain entry to a door.
    - **All**: Select to set the device to allow all types of authorization.
    - **Card + Fingerprint**: Select to set the device to require card plus fingerprint authorization.
    - **Only Fingerprint**: Select to set the device to require only fingerprint authorization.
    - **Only CARD**: Select to set the device to require only card authorization.
    - **Double Mode**: Select to set the device to require verification from two users during a selected time zone.
5. Click **Next** to set the fingerprint options for the FIN4000 panel.

Configuring operation mode to the FIN4000 K-10K panel

To configure the operation mode to the FIN4000 K-10K panel:

1. In the **FIN4000 Configuration - Operation Mode** dialog box, under **General**, you can select:
    - **Enrollment**: The availability of FIN4000 panel for capturing the images of fingerprints or issuing access cards.



1. Under **Card ID Format**, select the following:
    - **Format Type**: Select if the type of pre-processing to occur on card ID data must be of **Normal** or **Wiegand** type. If you select **Normal**, the card ID data is processed in its original form. If you select **Wiegand**, the device interprets the card ID data according to the Wiegand format settings.

- **Byte Order**: Select to specify if you must swap the ID card data between cards and devices by Most Significant Byte (MSB) or Least Significant Byte (LSB).
- **Bit Order**: Select to specify if you must swap the ID card data between cards and devices by MSB or LSB.

2. Under **Mifare/iCLASS Cards**, select the following:
   - **Mifare/iCLASS Cards**: Select to enable Mifare/iCLASS card authorization.
   - **Template on Card**: Select to use the template on the Mifare/iCLASS card for authorization.

Note: The **Template on Card** option is not applicable for HID models.

Click **View Card Layout** to view the Mifare/iCLASS card layout used by the device.

Note: The **View Card Layout** displays the card format configuration for HID models.

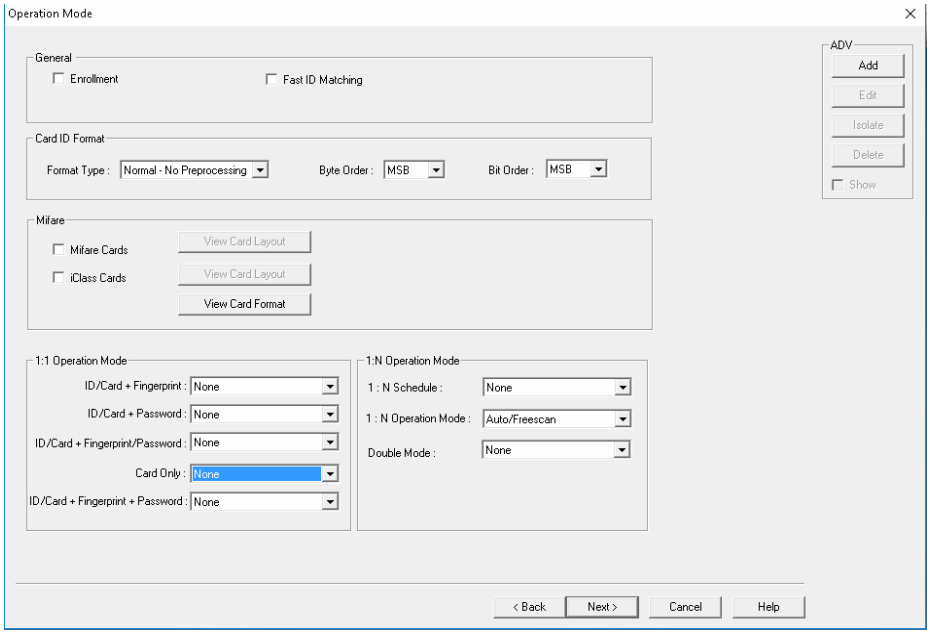
3. Under **Sensor Mode**, you must select:
   - **ID Entered:** Select to set the device sensor to be available on standby only after a valid ID is entered.
4. Under **Operation Mode**, for each of the following options, select to enable **Double Mode**, which requires verification of two users' credentials to gain entry to a door.
   - **Fingerprint Only:** Select to set the device to require fingerprint only authorization.
   - **Password Only:** Select to set the device to require password only authorization.
   - **Fingerprint/Password:** Select to set the device to require fingerprint or password authorization.
   - **Fingerprint + Password:** Select to set the device to require fingerprint plus password authorization.
   - **Card Only:** Select to set the device to require only card authorization.
5. Click **Next** to set the fingerprint options for the FIN4000 panel.

Configuring the operation mode to the FIN4000 ACK - 100K and FIN4000 MIK - 20K panels

To configure the operation mode to the FIN4000 ACK - 100K and FIN4000 MIK - 20K panels:

1. In the **FIN4000 Configuration - Operation Mode** dialog box, under **General**, you can select:
   - **Enrollment**: The availability of FIN4000 panel for capturing the images of fingerprints or issuing access cards.

- **Fast ID Matching**: The process to set the device to allow quicker authentication. You must input only the first two digits of the user ID and scan a single fingerprint.



2. Under **Card ID Format**, select the following:

   - **Format Type**: Select if the type of pre-processing to occur on card ID data must be of **Normal** or **Wiegand** type. If you select **Normal**, the card ID data is processed in its original form. If you select **Wiegand**, the device interprets the card ID data according to the Wiegand format settings.

   - **Byte Order**: Select to specify if you must swap the ID card data between cards and devices by Most Significant Byte (MSB) or Least Significant Byte (LSB).

   - **Bit Order**: Select to specify if you must swap the ID card data between cards and devices by MSB or LSB.

3. Under **Mifare/iCLASS Cards**, select the following:

   - **Mifare/iCLASS Cards**: Select to enable Mifare/iCLASS card authorization.

   - Click **View Card Layout** to view the Mifare/iCLASS card layout used by the device

Note: The **View Card Layout** displays the card format configuration for HID models.

4. Under **1: 1 Operation Mode**, select the following:

   - **ID/Card + Fingerprint** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus fingerprint authorization.

- **ID/Card + Password** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus password authorization.
- **ID/Card + Fingerprint/Password** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus fingerprint or password authorization.
- **Card Only** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require only card authorization.
- **ID/Card + Fingerprint + Password** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require ID or card plus fingerprint plus password authorization.

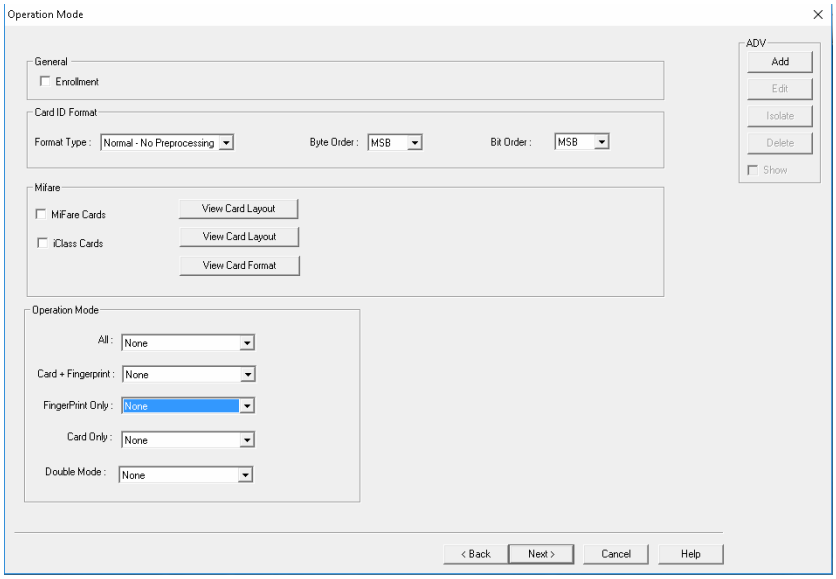
5. Under **1: N Operation Mode**, select the following:
   - **1:N Schedule** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set a schedule for using fingerprint only authentication.
   - **1:N Operation Mode** - From the drop-down list, select **Auto/Freescan**, **Ok/Function Key**, or **None**, based on the requirement. This enables you to set a method for activating the fingerprint sensor.
   - **Double Mode** - From the drop-down list, select **Always**, **Disable**, or **Custom**, based on the requirement. This enables you to set the device to require authentication of two users' access cards or fingerprints. The timeout for presenting the second authentication is 15 seconds.
6. Click **Next** to set the fingerprint formats for the FIN4000 panel.

Configuring operation mode to the FIN4000 AC - 10K and FIN4000 AC - 100K panels

To configure the operation mode to the FIN4000 AC - 10K and FIN4000 AC - 100K panels:

1. In the **FIN4000 Configuration - Operation Mode** dialog box, under **General**, you can select:

- **Enrollment**: The availability of FIN4000 panel for capturing the images of fingerprints or issuing access cards.



2. Under **Card ID Format**, select the following:

   - **Format Type**: Select if the type of pre-processing to occur on card ID data must be of **Normal** or **Wiegand** type. If you select **Normal**, the card ID data is processed in its original form. If you select **Wiegand**, the device interprets the card ID data according to the Wiegand format settings.
   - **Byte Order**: Select to specify if you must swap the ID card data between cards and devices by Most Significant Byte (MSB) or Least Significant Byte (LSB).
   - **Bit Order**: Select to specify if you must swap the ID card data between cards and devices by MSB or LSB.

3. Under **Mifare/iCLASS Cards**, select the following:

   - **Mifare/iCLASS Cards:** Select to enable Mifare/iCLASS card authorization.
   - Click **View Card Layout** to view the Mifare/iCLASS card layout used by the device.

Note: The **View Card Layout** displays the card format configuration for HID models.

4. Under **Operation Mode**:

   - **All**: Select to set the device to allow all types of authorization.
   - **Card + Fingerprint**: Select to set the device to require card plus fingerprint authorization.
   - **Only Fingerprint**: Select to set the device to require only fingerprint authorization.

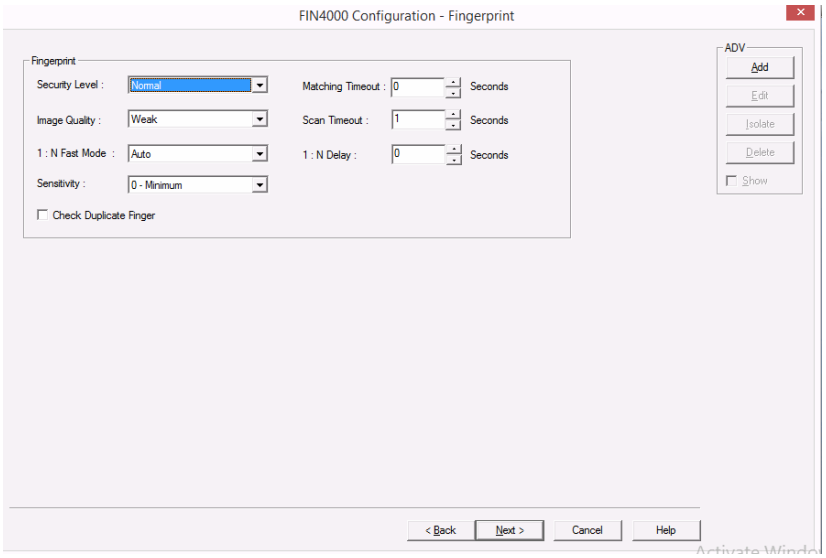
- **Only CARD**: Select to set the device to require only card authorization.
- **Double Mode**: Select to set the device to require verification from two users during a selected time zone.

5. Click **Next** to set the fingerprint options for the FIN4000 panel.

Configuring Fingerprint Formats

To configure the fingerprint format:

1. In the **FIN4000 Configuration - Fingerprint** dialog box, select the option to customize fingerprint authorization.



2. Under **Fingerprint**, select the following options:
   a. **Security Level**: Select **Normal**, **Secure**, or **Most Secure**, based on the requirement. This enables you to set the security level to use for fingerprint authorization.
   b. **Image Quality**: Select **Weak**, **Normal**, or **Strict**, based on the requirement. This enables you to set the strictness of the quality check for fingerprint scans.
   c. **1: N fast Mode**: Select to set the delay between scans when identifying fingerprints (0 seconds to 10 seconds). This delay prevents the scanner from processing the same fingerprint more than once, if you have not yet removed your finger from the scanner.
3. Click **Next** to configure the inputs for the panel.

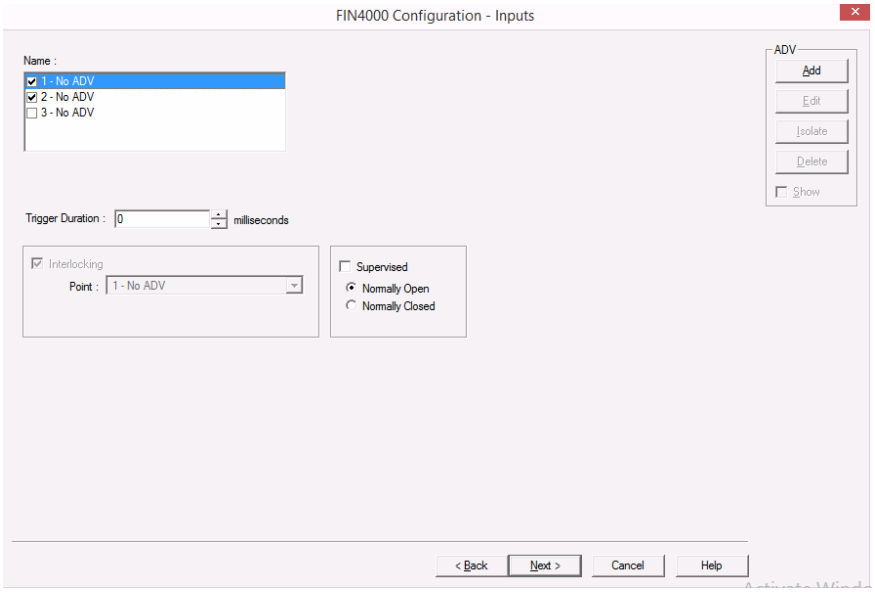
Configuring Input Formats

To configure the input format:

1. In the **FIN4000 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.

Notes:

- WIN-PAK SE/PE 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. In **Trigger Duration**, set the duration (in milliseconds) an input signal must last to trigger the specified action.
3. Set the **Interlocking** for the input point. See the Interlocking section for more information.

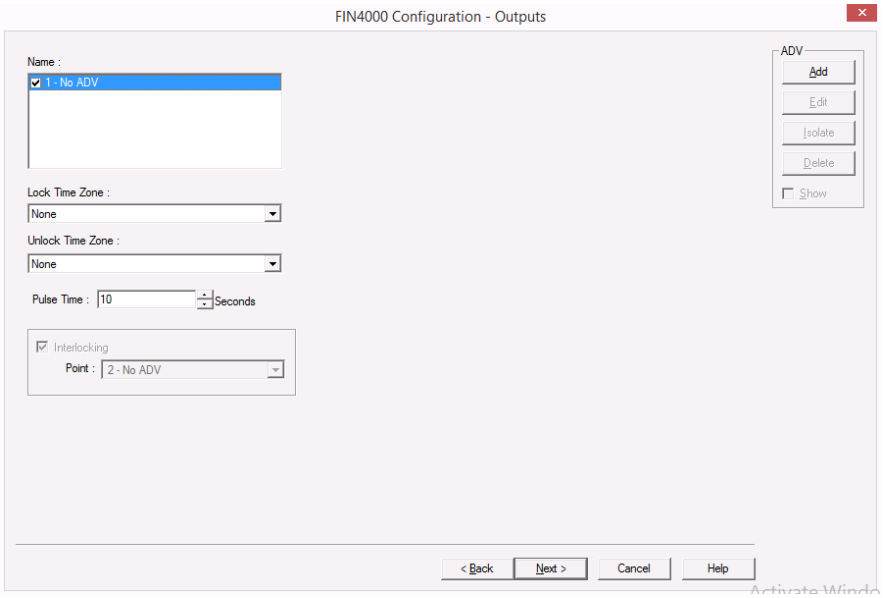
Note: Input three is the tamper detection input and will not be available for **Interlocking**.

4. Select the **Supervised** check box to report troubles when there is a change in state of input points.
5. Select **Normally Closed** or **Normally Opened** to specify the normal state of the door.
6. Click **Next** to configure the outputs for the panel.

Configuring Output Formats

To configure the output format:

1. In the **FIN4000 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.



2. Under **Lock Time Zone**, select a schedule when the door should normally be locked. During this time, door relays are inactive.
3. Under **Unlock Time Zone**, select a schedule when the door should normally be unlocked. During this time, door relays are active.
4. In **Pulse Time**, set the duration (in milliseconds) an output signal must last to trigger the specified action.
5. Set the **Interlocking** for the output point. See the Interlocking section for more information.
6. Click **Next** to configure the readers for the panel.

Note: The status of the FIN4000 output in **Control Map** and **Floor Plan** remains static. This is because of the device limitations.

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.

FIN4000 panel supports two readers:

- In-built reader: Reader 1

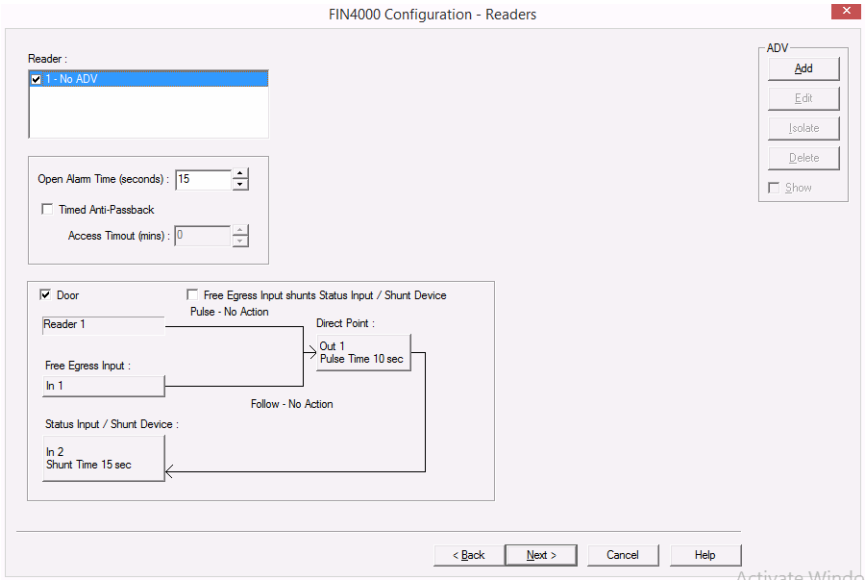
- External reader: Reader 1A

Notes:

- The external reader is a third-party reader, which is connected through a separate wiring to the FIN4000 devices. For more information, refer to FIN4000 Panel Installation Guide.
- The external reader controls the same door and shares the interlocking settings of Reader 1 (internal reader).
- The external reader does not support Operation Mode configuration, Double Mode, Template On-Card, and Timed Anti-Passback.
- The external reader does not work with iCLASS models.

To define a reader:

1. In the **FIN4000 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.

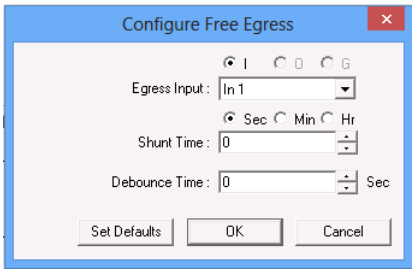


2. In **Open Alarm Time (seconds)**, set the duration.
3. Select **Timed Anti-Passback** to specify a access timeout for re-entry into a zone.
4. Select the **Anti-Passback** check box to set the anti-passback and implement it locally.

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.

5. 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.

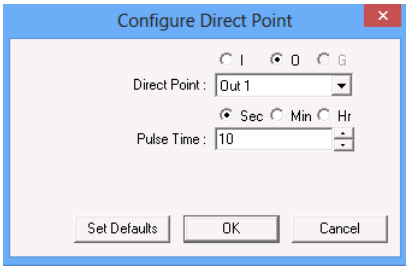
c. Select **Sec**, **Min** or **Hr** and change the **Shunt Time**. Shunt time is the duration allowed for the door kept unlocked. If the door remains in the unlocked state even after the shunt time, the alarm is raised.

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.

6. 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.

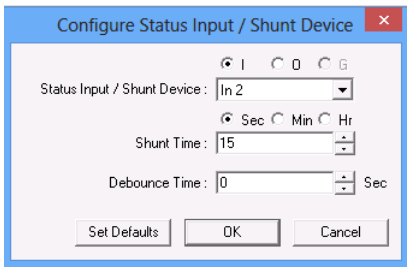
c. Select the **Direct Point** from the list.

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.

7. 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.
8. 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.
9. Click **Next** to configure the FIN4000 panel.

Adding P-Series Panel in Modem Pool for WIN-PAK SE/PE

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.

See the ‘Adding a P-Series Panel’ section for more information on panel configuration.

This section helps you in detailing procedures for providing Remote details and System settings.

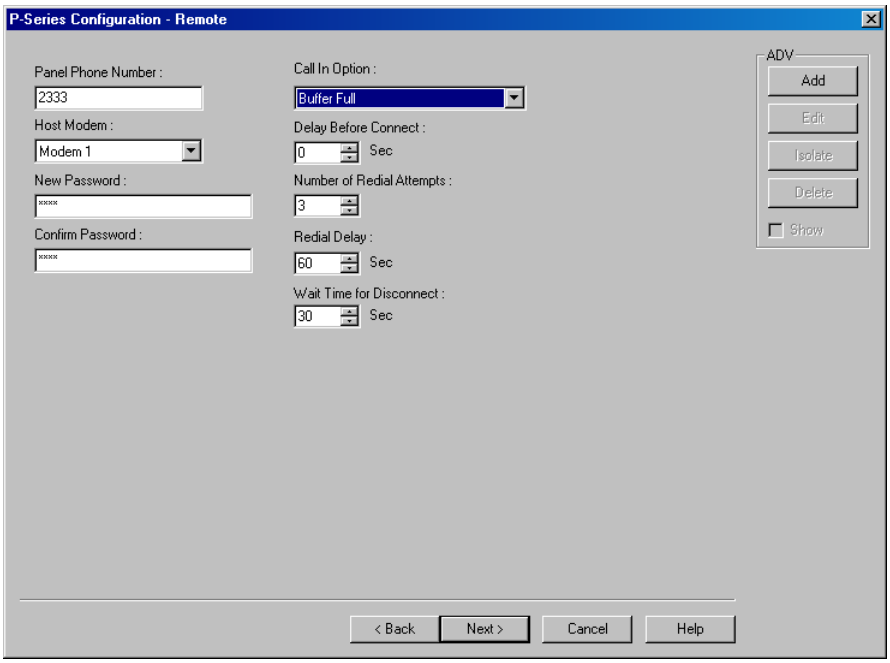
Configuring Remote details

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.

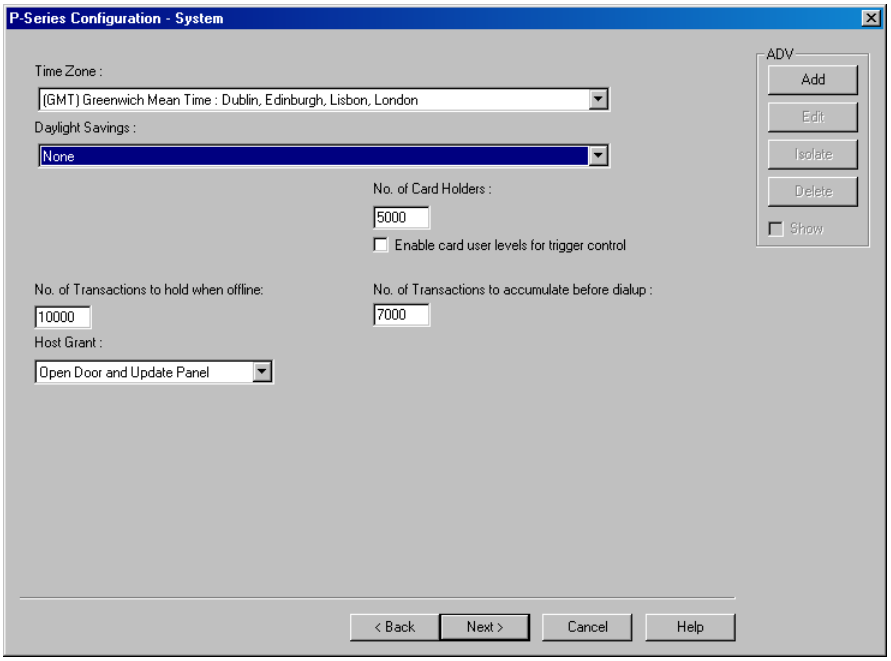
   Refer to the ***PRO-2200 Intelligent Controller Installation Manual*** for details on setting the password switch.
4. In the **Call In Option** list, select an event that determines when the remote panel calls in to the communication server.
5. Enter a value in the **Delay Before Connect** text box, 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.

    See the 'Setting the card format for the panel' section and the following section for more information on configuring the P-Series panel.

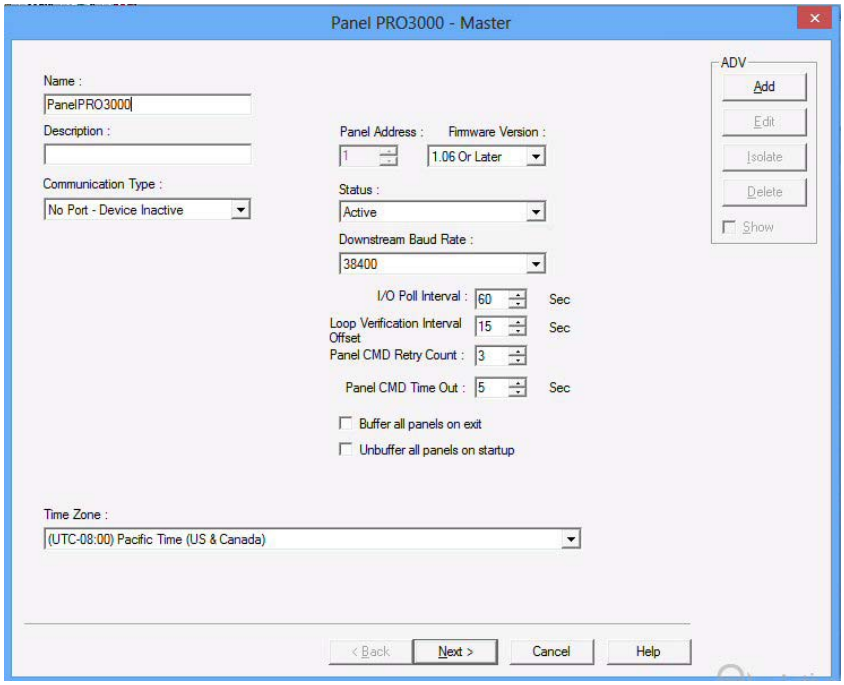
Adding a PRO3000 Panel

Note: The PRO3000 is present if WIN-PAK SE/PE is appropriately licensed. The PRO3000 panel is available in Asian and European markets only.

The PRO3000 is a 2-Door Intelligent Controller. The PRO3000 panel connects for two readers through Wiegand controlling two doors. The controller supports up to 62 doors through a RS485 multi-drop communication where 30 downstream controllers are connected to the gateway controller.

To add a PRO3000 panel:

1. Choose **Configuration > Device > Device Map**. The **Device** window appears.
2. Expand the **Devices** folder and right-click the communication server.
3. Click **Direct PRO-3000 Master Panel**. The **Panel PRO3000 Master** dialog box appears.



4. Type a unique **Name** for the panel. This field is mandatory.
5. Type a **Description** for the panel.
6. From the **Type** drop-down list, you can select:
   - PRO3000

   OR

   - HBAC-WIN2P
7. In the **Communication Type** list, select any one of the following communication types for WIN-PAK - PRO3000 or HBAC-WIN2P panel communication.
   - PRO3000
     - **No Port - Device Inactive**- If you select this option, no communication is established between the WIN-PAK and the PRO3000 panel and the device remains inactive.
     - **TCP/IP Connection** - If you select this option, type the IP-Address or Node name of the PRO3000 panel.
   - HBAC-WIN2P
     - **No Port - Device Inactive**- If you select this option, no communication is established between the WIN-PAK and the PRO3000 panel and the device remains inactive.
     - **TCP/IP Connection**- If you select this option, type the IP-Address or Node name of the HBAC-WIN2P panel.

– **TCP/IP Encrypted Connection**- If you select this option, type the IP-Address of the HBAC-WIN2P panel, followed by the Encryption Password and Confirm Encryption Password.

Note: The **Encryption Password** field must consist of 32 hexadecimal characters (0-9, a-f, A-F) only. The "AES Encryption" standard is used for encryption.

- **TCP/IP Reverse Initiate**- If you select this option, type the Port Number (in range 5001 to 65535).
- **TCP/IP Reverse Initiate With Encryption** - If you select this option, type the Port Number (in range 5001 to 65535) followed by the Encryption Password and Confirm Encryption Password.

8. For a Gateway panel, the **Panel Address** is always defaulted to "1", and cannot be changed.
9. Select the firmware version number of your panel in the **Firmware Version** list.
10. 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.
11. In the **Downstream Baud Rate** list, select the baud rate for the downstream panels. The default value is 38400.
12. Select the following panel defaults as applicable.
    - **IO Poll Interval** - Select an interval between **10** and **600** 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.
    - **Loop Verification Interval Offset (sec)** - Select an interval between **15** to **255**. By default, the Loop Verification Interval is set to **15** seconds.
    - **Panel CMD Retry Count** - Select the number of times(between **0** and **5**) at which 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.
    - **Panel CMD Time Out** - Select the waiting time (between **1** and **30**) for receiving a response from the panel and time out of the command. By default, the loop waits for **5** seconds.

13. Select the **Buffer all panels on exit** check box to buffer the events on all the panels when the communication server is stopped.
14. Select the **Unbuffer all panels on startup** check box to unbuffer all the panel events when the communication server is started.
15. In the **Time Zone** list, select the geographic time zone in which the NetAXS panel operates.
16. Click **Add** under **ADV** and set the ADV properties to create an ADV for the panel. See the 'Configuring an Abstract Device' section for more information on ADV configuration.
17. Click **Next** to specify the card format details.

Cross-Loop Anti-Passback

A PRO3000 loop consists of a single PRO3000 Master panel and multiple Slave panels. Cross-loop anti-passback works across the PRO3000 panel loops. The door does not open when a valid card is repeatedly swiped in any of the IN/OUT reader, across the loops which has the Cross Loop Anti-Passback feature enabled.

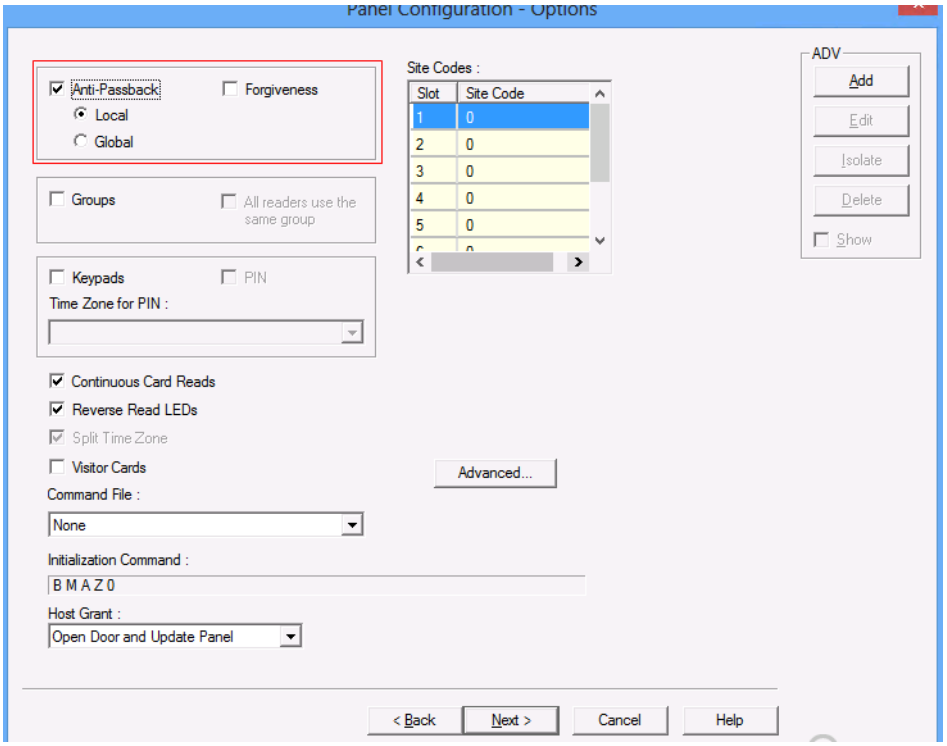
Cross-loop anti-passback is applicable only when there are one or more local or global panels.

The operator obtains a notification during the following scenarios.

- **Hard APB violation**: When an anti-passback violation occurs, the reader strictly restricts the access.
- **Soft APB violation**: When an anti-passback violation occurs, the reader allows the access but sends a report on anti-passback violation.

To enable cross-loop anti-passback for a loop:

1. In the **Panel Configuration - Options** dialog box, select the **Anti-passback** check box.



1. You can select from the following options:

   - **Global**: Enabling the **Global** Anti-Passback option on panel makes the panel a part of the Global and Cross Loop Anti-Passback system. All the valid Card swipes in this panel is synchronized across:

     – All the panels in the same loop (under the Master PRO3000 Panel)

     – All Master and Slave PRO3000 Panels enabled with Global Anti-Passback under a Communication Server.

   The Anti-Passback decision is applied Globally.

   - **Local**: When a **Local** Anti-Passback is enabled on a panel, it is neither a part of:

     – Global Anti-Passback (across its Master and Slave Panels of that Master)

   OR

     – Cross-Loop Anti-Passback System (across all the Master and Slave PRO3000 Panel in the WIN-PAK System)

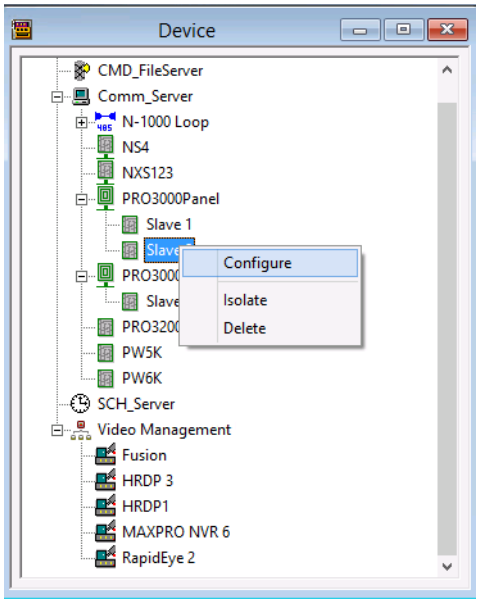
   The Anti-Passback decision is applied Locally.

Notes:

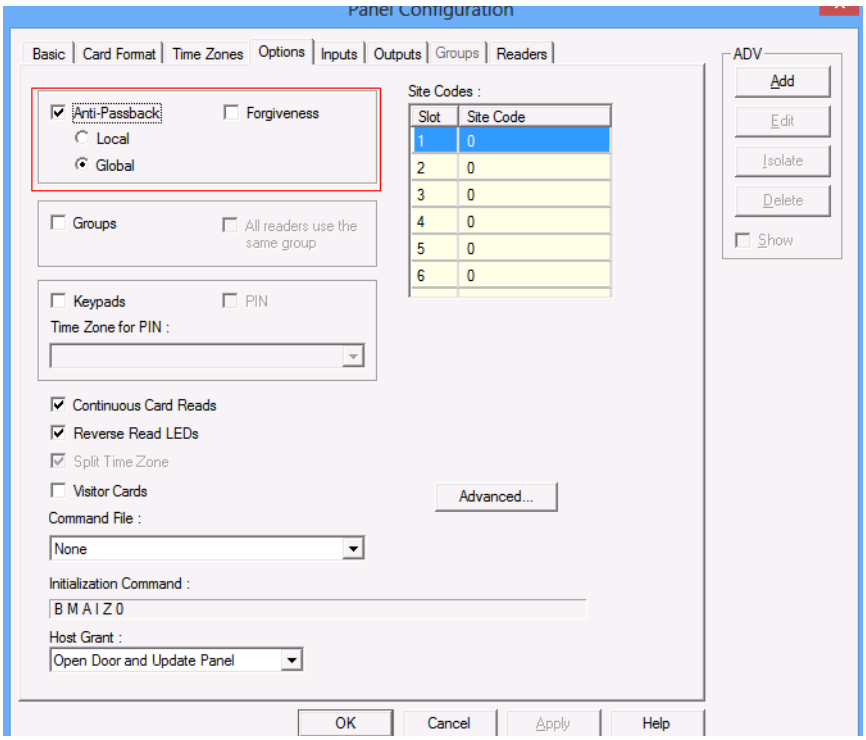
- Enabling the Global Anti-Passback in the PRO3000 Master Panel includes the whole loop (except panels with Local Anti-passback) into the Cross-loop Anti-Passback system.

- Enabling the Local Anti-Passback in the PRO3000 Master excludes the loop from the Cross-loop Anti-passback system.

2. Under **Devices**, right-click the **Slave** panel and the click **Configure**.



3. In the **Panel Configuration** dialog box, click the **Options** tab and select the **Anti-passback** check box.



4. Select the **Global** option. The master and slave panels that are configured with the **Global** anti-passback option must be manually included in the Cross Loop Anti-Passback functionality.

   Else, the master and slave panels are automatically included in the **Global** anti-passback.

5. Select the **Local** option. The master and slave panels that are configured with the **Global** anti-passback option must not be included in the Cross Loop Anti-Passback functionality.

   Else, the master and slave panels are automatically included in the **Local** anti-passback.

6. Click **OK** in the In the **Panel Configuration** dialog box.

Card capacities

Note: This section is applicable only for WIN-PAK CS.

The **PRO 22 IC**, with **1 GB** memory, has a card capacity with 32 access levels.

Access level	Number of digits in cards	Number of card holders	Initialization Status
Precision	5	5000	Initialization OK
	12	5000	Initialization OK
	16	5000	Initialization OK
Multiple	5	5000	Initialization OK
	12	5000	Initialization OK
	16	5000	Initialization OK
Multiple	5	7000	Initialization OK
	12	7000	Initialization OK
	16	7000	Initialization OK

Access level	Number of digits in cards	Number of card holders	Initialization Status
Multiple	5	8000	Initialization OK
	12	8000	Initialization OK
	16	8000	Initialization OK
Multiple	5	9000	Initialization OK
	12	9000	Initialization OK
	16	9000	Initialization OK
Multiple	5	9500	Initialization OK
	12	9500	Initialization OK

The **PRO 22 IC**, with **4 GB** extended memory, has a card capacity with 32 access levels.

Access level	Number of digits in cards	Number of card holders	Initialization Status
Precision	5	5000	Initialization OK
	12	5000	Initialization OK
	16	5000	Initialization OK
Multiple	5	5000	Initialization OK
	12	5000	Initialization OK
	16	5000	Initialization OK

Access level	Number of digits in cards	Number of card holders	Initialization Status
Multiple	5	7000	Initialization OK
	12	7000	Initialization OK
	16	7000	Initialization OK
Multiple	5	8000	Initialization OK
	12	8000	Initialization OK
	16	8000	Initialization OK
Multiple	5	9000	Initialization OK
	12	9000	Initialization OK
	16	9000	Initialization OK
Multiple	5	9500	Initialization OK
	12	9500	Initialization OK
	16	9500	Initialization OK
Multiple	5	10000	Initialization OK
	12	10000	Initialization OK
	16	10000	Initialization OK

Access level	Number of digits in cards	Number of card holders	Initialization Status
Multiple	5	11000	Initialization OK
	12	11000	Initialization OK
	16	11000	Initialization OK
Multiple	5	15000	Initialization OK
	12	15000	Initialization OK
	16	15000	Initialization OK
Multiple	5	20000	Initialization OK
	12	20000	Initialization OK
	16	20000	Initialization OK
Multiple	5	25000	Initialization OK
	12	25000	Initialization OK
	16	25000	Initialization OK
Multiple	5	30000	Initialization OK
	12	30000	Initialization OK
	16	30000	Initialization OK

Access level	Number of digits in cards	Number of card holders	Initialization Status
Multiple	5	35000	Initialization OK
	12	35000	Initialization OK
	16	35000	Initialization OK
Multiple	5	40000	Initialization OK
	12	40000	Initialization OK
	16	40000	Initialization OK
Multiple	5	45000	Initialization OK
	12	45000	Initialization OK
	16	45000	Initialization OK

Note: The card initialization fails if you try to initialize any cards beyond the count of **9500** for **1 MB** and **45000** for **4 MB**.

Adding a Remote P-Series Panel

The procedure for adding a Remote P-Series panel is similar to adding a Direct P-Series panel. When you add a P-Series panel remotely, you must specify the communication server and the P Series Modem Pool to which the panel is being added.

Refer to the "Adding a P-Series Panel"section in this chapter for more details on panel configuration.

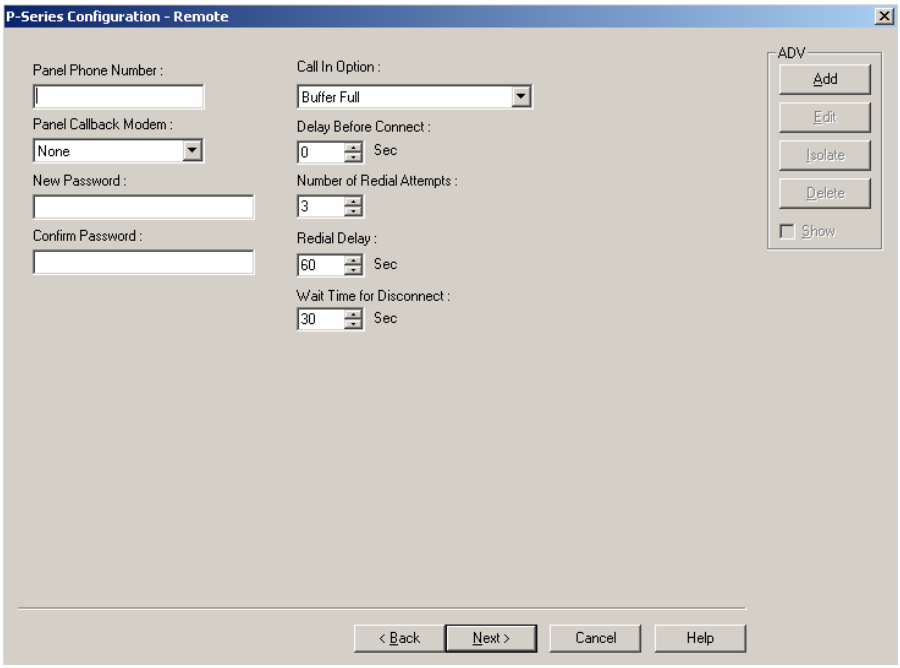
This section helps you with providing the **Remote** and **System** details for a remote P Series panel.

Configuring remote details

When configuring a P-Series panel on a Modem Pool, the **P Series Configuration - Remote** dialog box appears after the **P Series Configuration - Basic** dialog box.

To configure the remote settings:

1. In the **P-Series Configuration - Remote** 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 **Panel Callback 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 CS 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.

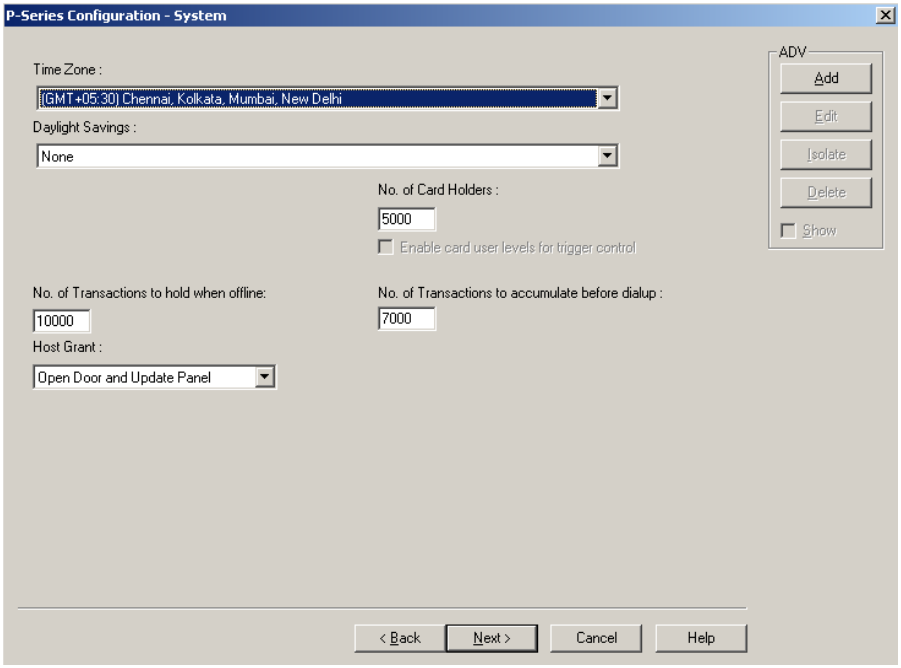
9. Click **Next** to save the panel remote configuration.

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.

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

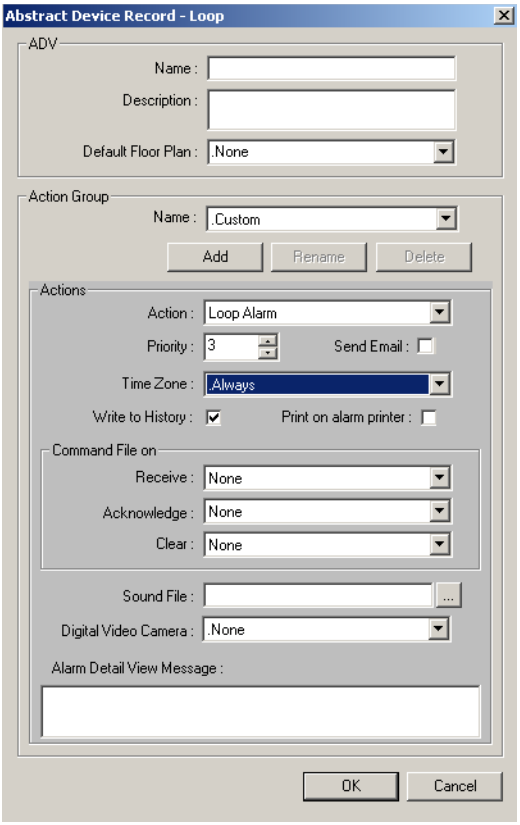
This section describes how to add, edit, and delete an abstract device.

Adding an Abstract Device

You can add an abstract device only while configuring the device map and servers. 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.

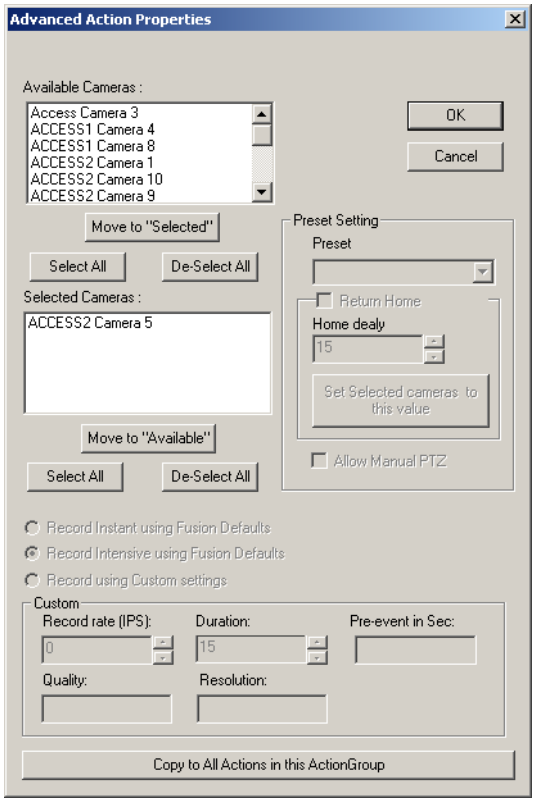
9. Select the **Send Email** check box, if e-mails must be sent to the configured e-mail ids when the action takes place.
10. Select the **Time Zone** for the action. The default setting is **Always**, as the defined actions take effect regardless of the time.
11. Select the **Write to History** check 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.

Note: Follow the below steps in WIN-PAK SE/PE.

- Click **Advanced** to select and configure the cameras for the Action Group. The **Advanced Action Properties** dialog box appears.



See the 'Configuring Advanced ADV Actions' for information on Advanced camera configuration.

Note: You can configure the Advanced action settings only for the Custom Action Groups. The advanced settings are not supported for standard and template action groups.

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.

Configuring Advanced ADV Actions

Note: This section is applicable only in WIN-PAK SE/PE.

To configure advanced ADV actions:

1. In the **Available Cameras** list, select the cameras to be monitored. For multiple selections, use the SHIFT or CTRL key.
2. Click **Move to** "**Selected**", to move the cameras to the **Selected Cameras** list.

   The selected cameras are displayed in the **Selected Cameras** box.
3. Click **Move to** "**Available**", to revert the selection.

Notes:

- The selected ADV, ADV actions, and cameras must belong to the same Communication Server.
- You can select a maximum of four cameras only.

4. Select one of the following options:
   - **Record Instant using Fusion Defaults** - to set the camera properties under instant mode of recording and record an event.
   - **Record Intensive using Fusion Defaults** - to set the camera properties under intensive mode of recording and record an event.

Note: The values displayed under **Custom** are the selected camera's default settings.

- **Record using Custom settings** - to customize the camera properties for recording an event.

Notes:

- The **Record Instant using Fusion Defaults**, **Record Intensive using Fusion Defaults**, and **Record using Custom settings** buttons are enabled only when one Fusion camera is selected from the **Selected camera** list.
- The camera custom settings for **Record Instant**, **Record Intensive**, and **Record using Custom settings** are available only for the fusion cameras 1 to 16.
- The default record data to the fusion camera is downloaded in real-time.

5. Under **Custom** settings, customize the following:
   - **Record rate (IPS)** - to set the images per second (IPS). The value must be lesser than that for Intensive Recording.
   - **Duration** - to set the time duration.

   The camera reverts to the default recording value and home position when the time set in the **Duration** is completed.

Note: The values displayed for **Pre-event in Sec**, **Quality**, and **Resolution** under **Custom** are the default settings for the selected camera. The values for **Duration of recording** and **IPS** can be edited under Custom Actions.

6. Under **Preset Setting**, set the preset value (from a maximum of 8 presets) for the selected PTZ camera.

Notes:

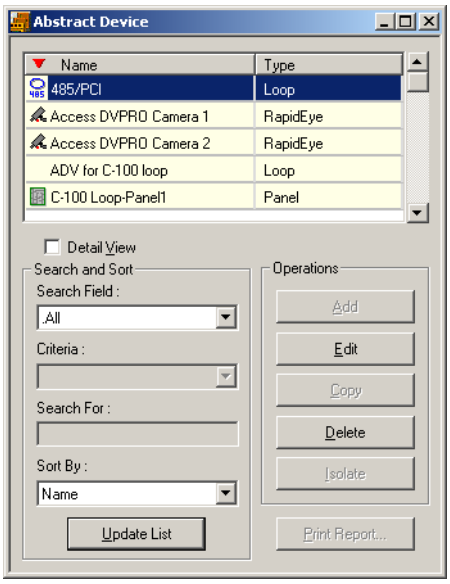
- You must select **Pan and Tilt** in the **Camera Configuration** tab to set a preset value for the camera.
- The configured preset fusion/HRDP Performance camera is downloaded in real-time.

7. Select **Return Home** to bring the camera back to its home position with the default focus, aperture, and zoom settings. You can select and set any of the presets as the default home preset value only in the DVR camera configuration page.
8. Specify a maximum **Home Delay** limit of 255 seconds and a minimum limit of 1 second. The default value for the home delay for a fusion/HRDP Performance camera is the value that is set during camera configuration.
9. Select **Set Selected cameras to this value** to set a common home delay value for the selected PTZ cameras.
10. Select **Allow Manual PTZ to** enable manual PTZ control of the selected camera and override the preset programming. When this check box is cleared, you cannot manually control the camera during the specified recording period.
11. Click **Copy to all Actions in this ActionGroup** to copy the settings in the **Advanced Action Properties** dialog box to all the other actions in the ADV Action Group.
12. Click **OK** to save the changes.

Editing an Abstract Device

To edit an abstract device:

1. Choose **Configuration > Device > Abstract Device (ADV)**. The **Abstract Device** window appears with the list of ADVs added through device map.



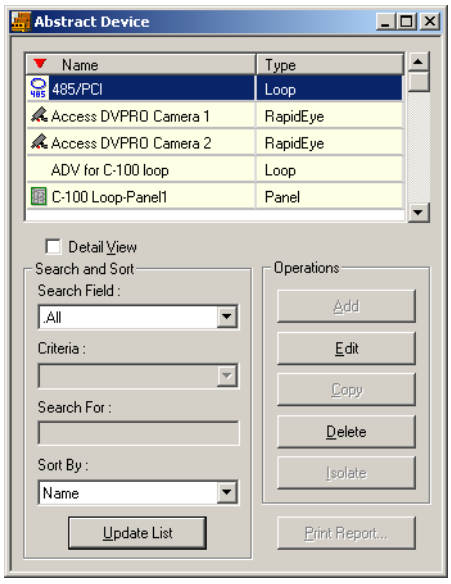
2. Select an abstract device and click **Edit**. The **Abstract Device Record** dialog box for the selected ADV appears.
3. Edit the required details of an ADV.

   Refer to the "Configuring an Abstract Device"section in this chapter for more details on ADV configuration.

Deleting an ADV

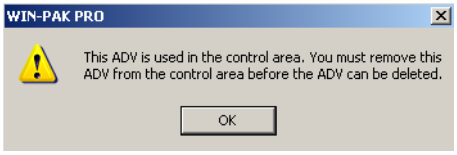
To delete an ADV not in use:

1. Choose **Configuration > Device > 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

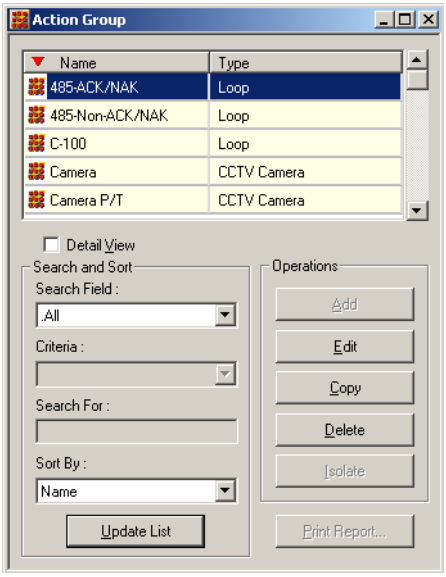
An Action Group is a set of actions assigned to a device when the ADV is defined. All the actions in the action group are set with the list of properties for a response to an action. Responses include executing a command file, activating a sound file, viewing a live video, and so on.

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. These options are specific to the account.

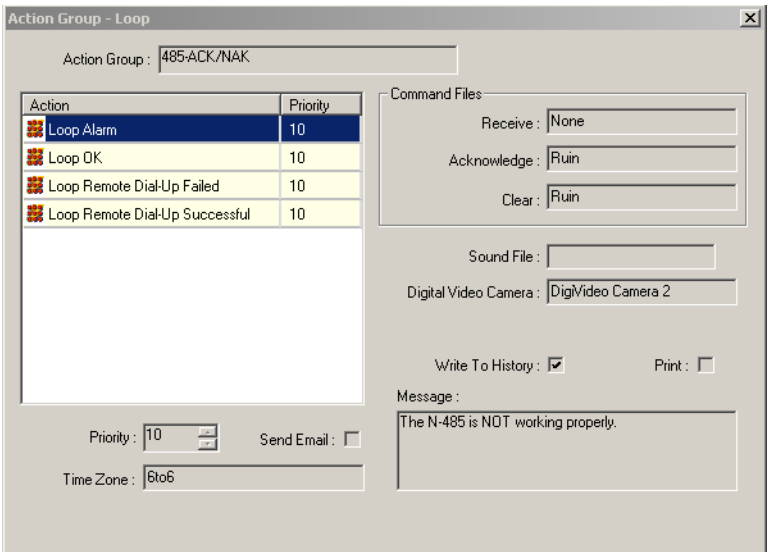
Viewing Action Group Details

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.



Note: Do not make any changes to the default Action group.

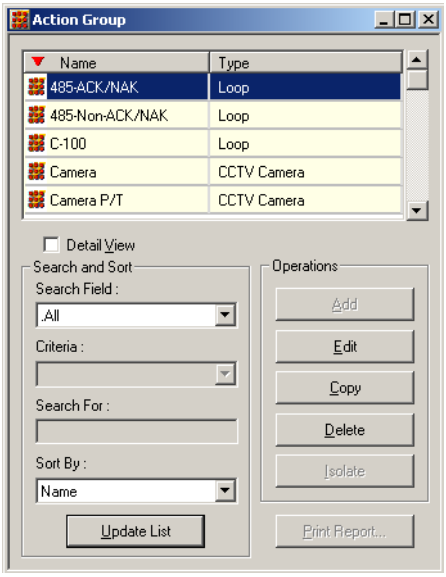
3. View the details of the action group. The priority of the action, time zone, command files and other details are displayed.
4. Select a different action from the list to view the related details.
5. Clear the **Detail View** check box in the **Action Group** window to close the dialog box.

Editing an Action Group

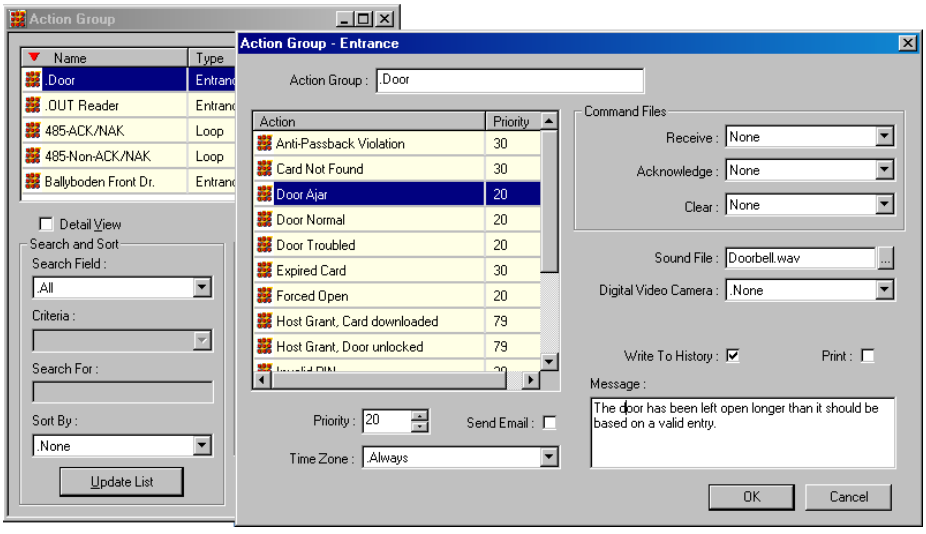
You can edit an Action Group from the Action Group window to make global changes to all ADVs associated with a particular Action Group.

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.

   Ensure that the alarm **Priority** in the ADV's is set between 1 and 50. The following table lists the alarm priority values and the output.

Table 9-25 Alarm Priority Values and Output

Alarm Priority Values	Output
0	The Alarm not set and no record or history appears in the Event or Alarm View.
1 - 50	The Alarm appears in the Event or Alarm View.
51 - 79	The Alarm appears only in Event and not in Alarm View.
80-99	The Alarm is recorded in history and appears in Event or Alarm View.

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 describe the types of actions defined for different ADVs used in WIN-PAK CS/SE/PE.

Table 9-26 Describing 485 ACK/NAK and 485 non-ACK/NAK (loop) Actions

Action	Message/Description
Loop OK	The N-485 is working properly.

Table 9-26 Describing 485 ACK/NAK and 485 non-ACK/NAK (loop) Actions

Action	Message/Description
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 9-27 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.
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 9-28 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.
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.

Table 9-28 Describing Cards (Entrance Reader) Actions

Action	Message/Description
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 9-29 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 CS/SE/PE Command File Server" is running in the WIN-PAK CS/SE/PE Service Manager.

Table 9-30 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 CS/SE/PE Communication Server" is running in the WIN-PAK CS/SE/PE Service Manager.

Table 9-31 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.
Forced Open	The door is in the alarm mode due to invalid entry.

Table 9-31 Describing Door (Entrance) Actions

Action	Message/Description
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 9-32 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 9-33 Describing Group Actions

Action	Message/Description
De-energized	The group of relays is not energized.
Energized	The group of relays is energized.

Table 9-34 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.
Missed	The guard missed the designated check point reader.

Table 9-34 Describing Guard Tour Sequenced Group Actions

Action	Message/Description
Out of Sequence	The guard is out of sequence.

Table 9-35 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 CS/SE/PE Guard Tour Server" is running in the WIN-PAK CS/SE/PE Service Manager.

Table 9-36 Describing Guard Tour Unsequenced Actions

Action	Message/Description
Checked	The guard has checked the required input/reader.

Table 9-37 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 9-38 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 9-39 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 9-40 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.
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.

Table 9-40 Describing NS2+ Panel Actions

Action	Message/Description
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 9-41 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.
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 9-42 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.
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.

Table 9-42 Describing N-1000-III/PW-2000-IV Panel Actions

Action	Message/Description
Tamper Switch Normal	The control panel service door is closed.

Table 9-43 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 CS/SE/PE.
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 CS/SE/PE.

Table 9-44 Describing NetAXS Entrance Actions

Action	Message/Description
Card Expired	Card Expired.
Card Found	A valid card has been used and entry was granted.
Card Not Found	Card Not Found.
Duress Pin Entered	Duress Pin Entered.

Table 9-44 Describing NetAXS Entrance Actions

Action	Message/Description
Escort access granted	Escort access granted.
Hard Anti-Passback Violation	Card was denied entry because it has already been used going in/out without properly going out/in.
Host grant, Card downloaded	Access was granted to the user (if event is within 2 minutes of computer time). The control panel was updated with valid card information.
Host grant, Door unlocked	Access was granted to the user (if event is within 2 minutes of computer time). The control panel was not updated with valid card information.
Temp card expired number of uses	Temporary card expired by number of uses.
Hard Anti-Passback	Anti-Passback.
Input point tamper - Cut	Input point tamper - Cut.
Input point tamper - Shorted	Input point tamper - Shorted.
Invalid Format	Card was denied entry because it was unknown to the reader.
Invalid Pin	A card was denied entry because it was used with an invalid PIN.
N-Man Authenticated	N-Man Authenticated.
N-Man Redundant	N-Man Redundant.
N-Man Waiting	N-Man Waiting.
Occupancy Max Exceeded Soft	Occupancy Max Exceed Attempt.
Occupancy Max Exceeded Hard	Occupancy Max Exceed Attempt.
Occupancy Maximum Reached	Occupancy Max Reached.
Occupancy Min Exceeded Hard	Occupancy Min Exceed Attempt.

Table 9-44 Describing NetAXS Entrance Actions

Action	Message/Description
Occupancy Min Exceeded Soft	Occupancy Min Exceed Attempt.
Occupancy Minimum Reached	Occupancy Min Reached.
Occupancy Minimum Waiting	Occupancy Min Waiting.
Site Code Violation	Card was denied because it did not have a proper site code.
Soft Anti-Passback Violation	Card was denied entry because it has already been used going in/out without properly going out/in.
Soft Anti Passback	Anti Passback.
Supervisor Authenticated	Supervisor Authenticated.
Supervisor Card Found	Supervisor Card Present.
Supervisor mode disabled	Supervisor mode disabled.
Supervisor mode enabled	Supervisor mode enabled.
Supervisor Not Enabled	Supervisor Not Enabled.
Supervisor Required	Supervisor Required.
Temporary card expired by date	Temporary card expired by date.
Temporary card expired number of uses	Temporary expired number of uses.
Time Zone Violation	A card was denied because it was used outside its time period.
Trace Card	A card that is being traced was used and entry was granted.
VIP Card Found	VIP Card Present.

Table 9-45 Describing NetAXS Group Actions

Action	Message/Description
De-energized	The group of relays is not energized
Energized	The group of relays is energized.

Table 9-46 Describing NetAXS Input Actions

Action	Message/Description
Input Alarm	The Input is in the alarm state
Input Normal	The Input is in the normal state.
Input Trouble Cut	The Input is cut.
Input Trouble Short	The Input is shorted.

Table 9-47 Describing NetAXS NX4 device Actions

Action	Message/Description
Poll Response Alarm	The NetAXS NX4 device board is not responding to polling.
Primary Power Failure	The NetAXS NX4 device board is responding normally to polling.
Primary Power Failure	The NetAXS NX4 device board primary power is lost.
Primary Power Normal	The NetAXS NX4 device board primary power has been restored.
Tamper Switch Alarm	The NetAXS NX4 device board service door is open.
Tamper Switch Normal	The NetAXS NX4 device board service door is closed.
Unsupported NX4 Device Version	An Unsupported NetAXS NX4 device board version is connected.

Table 9-48 Describing NetAXS Output Actions

Action	Message/Description
De-energized	The output to the door is not energized.

Table 9-48 Describing NetAXS Output Actions

Action	Message/Description
Energized	The output to the door is energized.
Trouble	The output to the door is in trouble.

Table 9-49 Describing NetAXS Panel Actions

Action	Message/Description
Battery Shorted	The NetAXS backup battery is shorted. Corrective action is required.
Battery Voltage is low	The NetAXS backup battery voltage is low. Corrective action is required.
Battery Voltage is Normal	The NetAXS backup battery voltage has returned to normal.
Common Database Deleted	A common database table has been deleted.
Common Database Updated	A change in the common database table has occurred.
Hybrid Mode	NetAXS Gateway has enabled Hybrid Mode.
Incorrect Firmware Version	Unsupported Panel Version.
Offline	A NetAXS auxiliary board is offline.
Online	A NetAXS auxiliary board is online.
Panel Communication Alarm	Communication to the control panel has been lost.
Panel Communication Normal	Communication to the control panel has been restored.
Panel Database Deleted	A panel database table has been deleted.
Panel Database Updated	A change in panel database table has occurred.
Panel Reset	The control panel has been reset.

Table 9-49 Describing NetAXS Panel Actions

Action	Message/Description
Panel Restarted	The panel has restarted. If this issue continues repeatedly contact your service provider.
Panel Time Changed	Panel time has been changed.
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 Alarm	Control panel primary power has been lost.
Primary Power Normal	Control panel primary power has been restored.
Process Watcher Restarted	A NetAXS process has been restarted. If this issue continues repeatedly contact your service provider.
RTC Clock Error	An error has occurred with the NetAXS clock. Verify that the time and date is set correctly.
Tamper Alarm	The control panel service door is open.
Tamper Normal	The control panel service door is closed.
Unknown System Event	An Unknown System Event has occurred. If this issue continues repeatedly contact your service provider.
Unsupported Panel Version	Unsupported Panel Version.

Table 9-50 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.

Table 9-50 Describing P-Series Dial-Up Actions

Action	Message/Description
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 9-51 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.
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.

Table 9-51 Describing P-Series Reader Actions

Action	Message/Description
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.
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.

Table 9-51 Describing P-Series Reader Actions

Action	Message/Description
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 9-52 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 9-53 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 9-54 Describing Galaxy Panel Action Groups

Action	Message/Description
Alarm Cancel	
Alarm Reset	
Automatic Test	
Battery Restore	The Module Battery which was low is restored.

Table 9-54 Describing Galaxy Panel Action Groups

Action	Message/Description
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.
RF NVM RAM Fail	RF NVM RAM Fail.
Standby Battery Low	Standby Battery is low.
Standby Battery OK	Standby Battery is OK.

Table 9-54 Describing Galaxy Panel Action Groups

Action	Message/Description
Tamper Alarm	Module 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 9-55 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 9-56 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 9-57 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 CS Schedule Server" is running in the WIN-PAK CS Service Manager.

Table 9-58 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 CS Muster Server is running in the WIN-PAK CS Service Manager.

Table 9-59 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.
Galaxy Polling Started	Galaxy is stopped polling.

Table 9-60 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.

Table 9-60 Describing Galaxy Group Actions

Action	Message/Description
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.
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 9-61 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 9-62 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	
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.

Table 9-63 Describing Fusion DVR Action Groups

Action	Message/Description
DVR Online	DVR is OK and online.
DVR Offline	DVR is not online. Connection is lost or is not able to establish the connection with the DVR.
Fusion Stationary Camera	Video signal restored.
Fusion Stationary Camera	Video signal loss.
Fusion Stationary Camera	Camera motion alarm.
Fusion PTZ Camera	Video signal restored.
Fusion PTZ Camera	Video signal loss.
Fusion PTZ Camera	Camera motion alarm.
Fusion DVR Input	DVR Input is normal.
Fusion DVR Input	DVR input is in alarm state.
Fusion DVR Output	DVR output is de-energized.

Table 9-63 Describing Fusion DVR Action Groups

Action	Message/Description
Fusion DVR Output	DVR output is energized.

Table 9-64 Describing HRDP DVR Action Groups

Action	Message/Description
HRDP DVR	DVR is OK and online.
HRDP DVR	DVR is not online. Connection is lost or is not able to establish connection with the DVR.
HRDP Stationary Camera	Video signal restored.
HRDP Stationary Camera	Video signal loss.
HRDP Stationary Camera	Camera motion alarm.
HRDP PTZ Camera	Video signal restored.
HRDP PTZ Camera	Video signal loss.
HRDP PTZ Camera	Camera motion alarm.
HRDP DVR Input	DVR Input is normal.
HRDP DVR Input	DVR input is in alarm state.
HRDP DVR Output	DVR output is deenergized.
HRDP DVR Output	DVR output is energized.

Table 9-65 Describing Fusion Recorder

Action	Message/Description
Recorder Disconnected	Alarm raised when DVR is disconnected.
Recorder Connected	The door is supported with a prop.

Table 9-66 Describing Fusion Camera

Action	Message/Description
Camera User Recording Started	This alarm is raised when an Alarm Event starts Instant Recording.
Camera User Recording Completed	This alarm is raised when an Alarm Event stops Instant Recording after certain duration.
Motion Detected	Motion is detected in this camera View.
Video Lost	Video is lost from this camera.
Video Restored	Video is restored from this camera.

Table 9-67 Describing Fusion Recorder Input

Action	Message/Description
Input Normal	DVR Input is in normal state.
Input Alarm	DVR Input is in alarm state.

Table 9-68 Describing Fusion Recorder Output

Action	Message/Description
Output Enabled	DVR Output is Energized.
Output Disabled	DVR Output is De-energized.

Table 9-69 Describing Rapid Eye Recorder

Action	Message/Description
Recorder Disconnected	Alarm raised when DVR is Disconnected.
Recorder Connected	Alarm raised when DVR is Connected.
Session Rejects	RE Sessions exhausted.
System - Self Restart	RE restarting on internal exception.
System - Reboot	Manual reboot of RE.

Table 9-69 Describing Rapid Eye Recorder

Action	Message/Description
System - No Video Recording	DVR unable to record cameras.
System - Storage Devices Missing	DVR hardisk not getting detected by RE.
System - Time Server Unusable	RE unable to connect to NTP server.
System - No Synchronization in 24 Hours	RE unable to synchronize to NTP server.
System - S.M.A.R.T. Disk Failure	Early indication for hard disk failure.
Rule Engine Action Triggered	Rule Engine configured in RE is triggered.
System - Excessive System Clock Drift	Time difference between NTP Server and RE is large.
Maintenance - Configuration Modification	Configuration is modified in RE.
Maintenance - Security Modification	Security settings in RE is modified.
Maintenance - System Files Modification	System files in RE is modified.
Maintenance - Synchronize Time	Time has been synchronized in RE.
Maintenance - Clear Storage	Recordings has been erased on RE.
Maintenance - Clear Storage	Resetting video stream.
System - Runtime Failure	Resetting video stream.
System - Runtime Failure	Runtime error in RE.
Session Disconnected	Disconnected from RE.
Session Connected	Connected to RE.

Table 9-70 Describing RapidEye Camera

Action	Message/Description
Motion Detected	Motion is detected in this camera view.
Video Signal Lock	Video lost from this camera.
Video Signal Unlock	Video restored from this camera.
Camera Blind Detection Enabled	Camera Blind Detection Enabled for this camera in RE.
Camera Blind Detection Disabled	Camera Blind Detection Disabled for this camera in RE.
Camera Blur Detection Enabled	Camera Blur Detection Enabled for this camera in RE.
Video CSD Moved On	Camera scene of view changed.
Video CSD Moved Off	Camera scene of view restored.
Video Boost Record On	Boosted Recording for this Camera is turned ON.
Video Boost Record Off	Boosted Recording for this Camera is turned OFF.
Started moving in wrong direction	Video Analytics: Object started to move in Wrong Direction.
Stopped moving in wrong direction	Video Analytics: Object stopped to move in Wrong Direction.
On fence line	Video Analytics: Object on Fence line.
Running	Video Analytics: Object/ Person started running.
Stopped running	Video Analytics: Object/ Person stopped running.
People converged	Video Analytics: People Converged in an area.
People passed by	Video Analytics: People passed by.
Entered restricted zone	Video Analytics: Object/ Person/ Car entered Restricted Zone.
Exited restricted zone	Video Analytics: Object/ Person/ Car exited Restricted Zone.
Running in the wrong direction	Video Analytics: Object/ Person started running in wrong direction.
Trespassing line	Video Analytics: Object/ Person crossed Tress passing line.

Table 9-70 Describing RapidEye Camera

Action	Message/Description
Speeding	Video Analytics: Object/ Car Speeding.
Made illegal U-turn	Video Analytics: Car made illegal U Turn.
Car parked in handicapped zone	Video Analytics: Car Parked in Handicapped Zone.
Pulled off the road	Video Analytics: Car Pulled off the Road.
Needs assistance	Video Analytics: Car Needs Assistance.
Counted as exiting	Video Analytics: Car/ Person Counted Entering.
Counted as entering	Video Analytics: Car/ Person Counted Exiting.
Entered lot	Video Analytics: Car entered lot.
Exited lot	Video Analytics: Car exited lot.
Removed	Video Analytics: Object removed.
Left unattended	Video Analytics: Object left unattended.
Possible theft	Video Analytics: Possible theft of the object.
Loitering in restricted zone	Video Analytics: Person loitering in restricted zone.
Counted in lane	Video Analytics: Car counted in lane.
Entered target zone	Video Analytics: Object/Person/Car entered target zone.
Staying in target zone	Video Analytics: Object/Person/Car staying in target zone.

Table 9-71 Describing RapidEye Recorder Input

Action	Message/Description
Input Normal	DVR Input is in normal state.
Input Alarm	DVR Input is in alarm state.

Table 9-72 Describing RapidEye Relay Output

Action	Message/Description
Output Enabled	DVR Output is energized.
Output Disabled	DVR Output is de-energized.

Table 9-73 Describing MAXPRO NVR Recorder

Action	Message/Description
MAXPRONVR Server Connected	Alarm raised when NVR is Disconnected.
MAXPRONVR Server Disconnected	Alarm raised when NVR is Connected.
Low Disk Space	Alarm raised when disk space is low.
Recording Server Connected	Alarm raised when the recorder begins recording.
Recording Server Disconnected	Alarm raised when the recorder stops recording.
MAXPRONVR Controller Connected	Alarm raised when the PTZ and status is regained by the recorder.
MAXPRONVR Controller Disconnected	Alarm raised when the PTZ and status is lost by the recorder.

Table 9-74 Describing MAXPRO NVR Camera

Action	Message/Description
Camera Blind Detection Enabled	Camera Blind Detection Enabled for this Camera in RE.
Camera Blind Detection Disabled	Camera Blind Detection Disabled for this Camera in RE.
Camera Blur Detection Enabled	Camera Blur Detection Enabled for this Camera in RE.
Camera Blur Detection Disabled	Camera Blur Detection Disabled for this Camera in RE.
Video CSD Moved On	Camera Scene of View Changed.
Video CSD Moved Off	Camera Scene of View Restored.
Camera User Recording Started	User started Recording.
Camera User Recording Completed	User stopped Recording.

Table 9-74 Describing MAXPRO NVR Camera

Action	Message/Description
Camera Disconnected	Camera Disconnected from NVR.
Camera Connected	Camera connected to NVR.
Camera Background Recording Disabled	Camera Background Recording Disabled.
Camera Background Recording Enabled	Camera Background Recording Enabled.
Camera Event Recording Started	Camera Event Recording Started.
Camera Event Recording Completed	Camera Event Recording Completed.
Camera Disabled	Camera disabled in NVR.
Camera Enabled	Camera Enabled in NVR.
Camera User recording error	Failed to record.
Camera NoMotion Detected	No Motion is detected in this Camera View.
Camera Motion Detected	Motion is detected in this Camera View.

Table 9-75 Describing HRDP Recorder

Action	Message/Description
Recorder Disconnected	Alarm raised when DVR is Disconnected.
Recorder Connected	Alarm raised when DVR is Connected.

Table 9-76 Describing HRDP Camera

Action	Message/Description
Motion Detected	Motion is detected in this Camera View..
Video lost	Video lost from this camera.
Video restored	Video restored from this camera.

Table 9-77 Describing HRDP Recorder Input

Action	Message/Description
Input Normal	DVR Input is in Normal State.
Input Alarm	DVR Input is in Alarm State.

Table 9-78 Describing HRDP Recorder Output

Action	Message/Description
Output Enabled	DVR Output is Energized.
Output Disabled	DVR Output is De-energized.

Table 9-79 Describing DVR Camera ADV Actions

Action	Message/Description
Motion Alarm	The camera movement raises an alarm when any motion is detected
Video Signal Loss	Indicates any loss in video signal.
Video Signal Restored	Indicates any restoration in the video signal.

Table 9-80 Describing Video Switcher (CCTV Switcher) Action Group

Action	Message/Description
CCTV Switcher OK	The video switcher is working properly.
CCTV Switcher Trouble	The video switcher is NOT working properly.

Table 9-81 Describing PRO3000 Input Actions

Action	Message/Description
Ajar State	The door has been left open longer than it must be based on a valid entry.

Action	Message/Description
Input Alarm	The Input is in the alarm state.
Input Normal	The Input is in the normal state.
Input Trouble Cut	The Input is cut.
Input Trouble Short	The Input is shorted.

Table 9-82 Describing PRO3000 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.
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.

Action	Message/Description
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 9-83 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 9-84 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.

Moving Loops and Panels

Note: This section is applicable only in WIN-PAK SE/PE

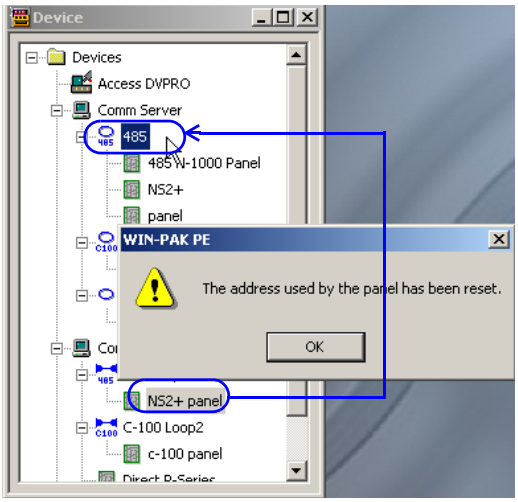
You can move loops and panels across communication servers if the following conditions are met:

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.

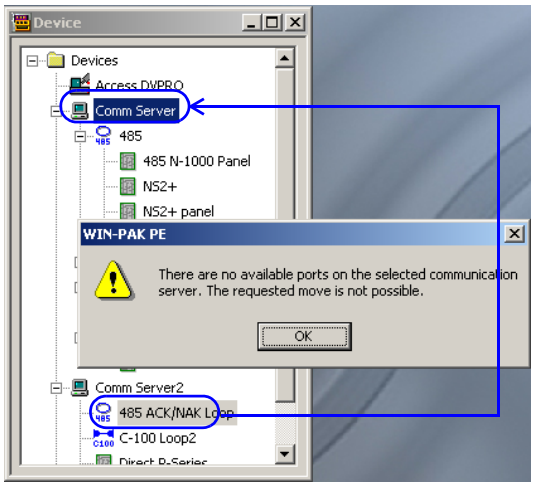
Moving loops across communication servers

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.



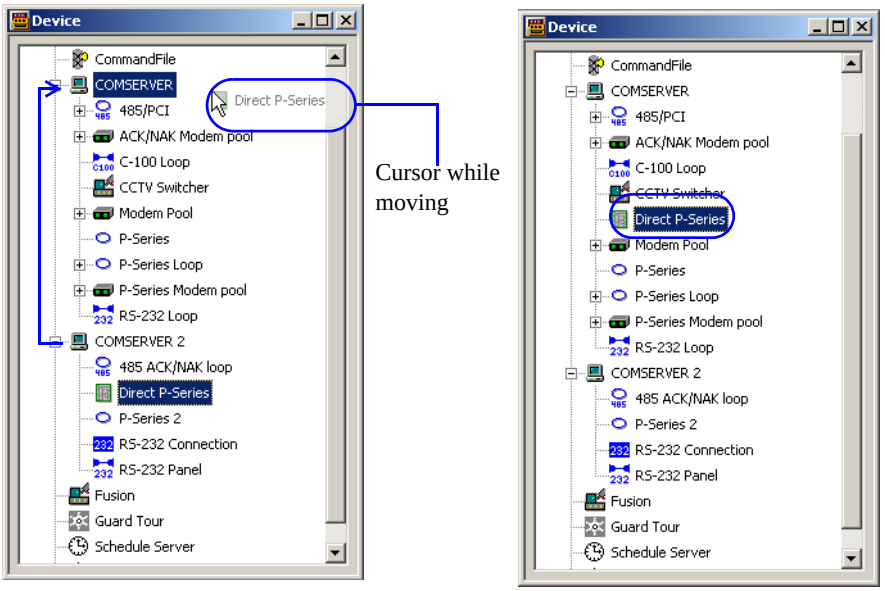
3. Click **OK**. The loop is moved to the destination communication server.



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.

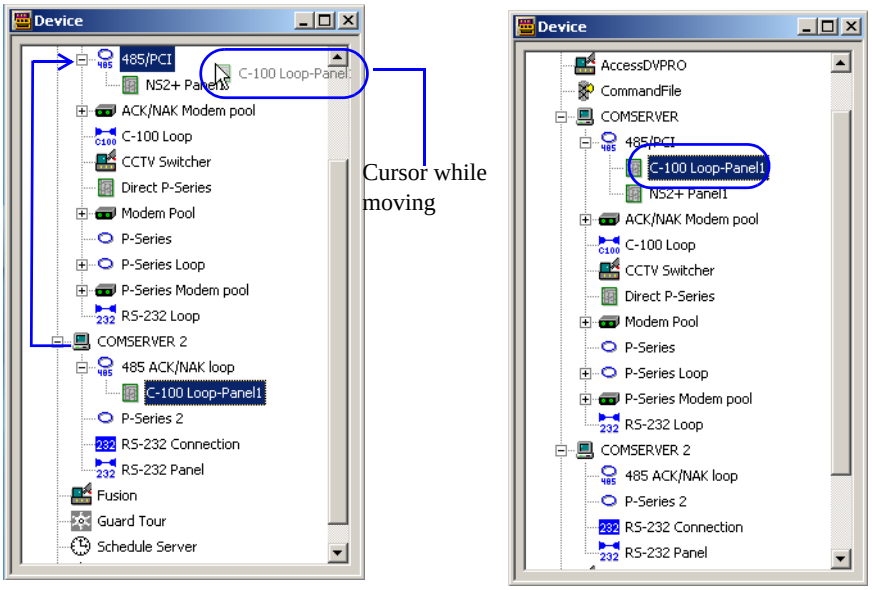


3. Release the mouse button at the destination communication server. The direct panel is moved.

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

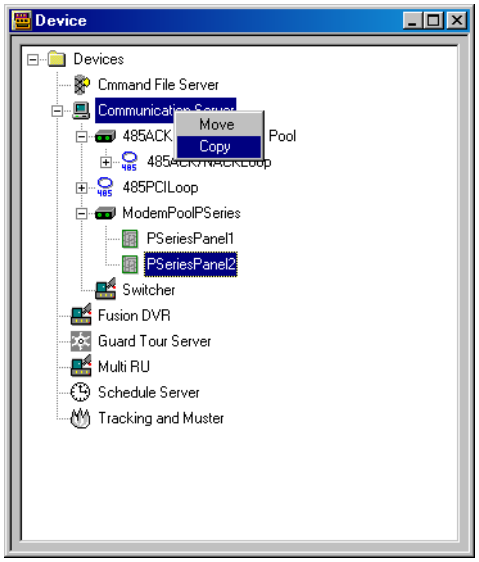
You can create a copy of loops and panels onto another communication servers if the following conditions are met:

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.

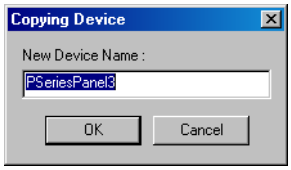
Copying a direct panel

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.

Initializing Panels

Programming information entered into the WIN-PAK CS/SE/PE 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 the 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 Panels from Control Map" section in the chapter Defining the Areas for details on panel initializing on floor plans.

Defining Areas

10

In this chapter...

This chapter describes about the Introduction to Defining Areas, Defining Access Areas, Defining Tracking and Mustering Areas, Defining Control Areas, and Viewing Control Areas in WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
Defining Tracking and Mustering Areas: Removing a Branch or an Entrance, page 657	✓	✓
Defining Tracking and Mustering Areas: Finding an Item in the tree, page 657	✓	✓
Defining Tracking and Mustering Areas: Configuring Mustering Areas, page 658	✓	✓
Defining Tracking and Mustering Areas: Adding a Mustering Area Branch, page 658	✓	✓
Defining Tracking and Mustering Areas: Adding an Entrance to the Mustering Area, page 659	✓	✓
Defining Tracking and Mustering Areas: Moving an Entrance, page 660	✓	✓
Defining Tracking and Mustering Areas: Renaming a Branch, page 660	✓	✓
Defining Tracking and Mustering Areas: Removing a Branch or an Entrance, page 660	✓	✓
Defining Tracking and Mustering Areas: Finding an Item in the tree, page 661	✓	✓
Defining Tracking and Mustering Areas: Tracking and Muster View, page 661	✓	✓
Defining Control Areas: Adding a Site, page 666	✓	✓
Defining Control Areas: Adding a branch to a site, page 667	✓	✓
Defining Control Areas: Renaming a Site or a Branch, page 667	✓	✓
Defining Control Areas: Adding a Device, page 668	✓	✓
Defining Control Areas: Moving a Device, page 669	✓	✓
Defining Control Areas: Removing a Site, Branch or Device, page 669	✓	✓

Section	WIN-PAK CS	WIN-PAK SE/PE
Viewing Control Maps: Controlling Devices from a Control Map, page 669	✓	✓
Viewing Control Maps: Initializing a Panel from Control Map, page 676	✓	✓

Introduction

Areas in WIN-PAK CS/SE/PE are classified as Access Areas, Control Areas, Tracking Areas, and Muster Areas. These areas are configured according to the specific requirements of an account.

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 timezone 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 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.

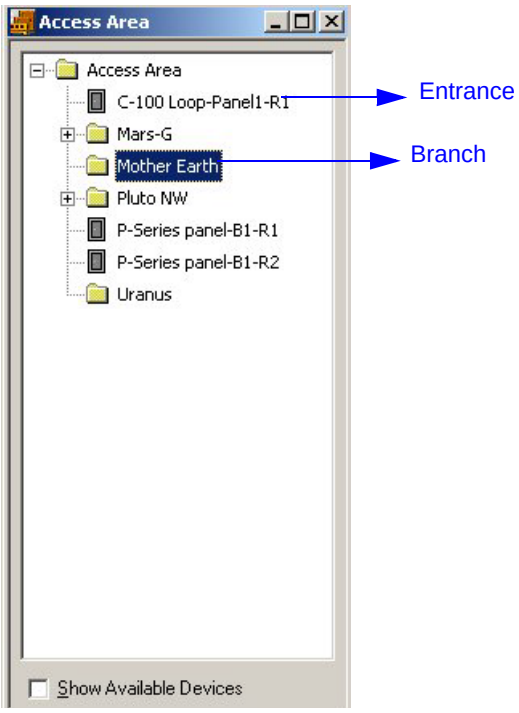
Tracking Areas are used for tracking card holder movements and Mustering areas are used for tracking card holder movements in the event of emergency situations such as a fire.

This chapter describes how to configure access areas, configure control areas and view control maps, and 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 CS/SE/PE 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.

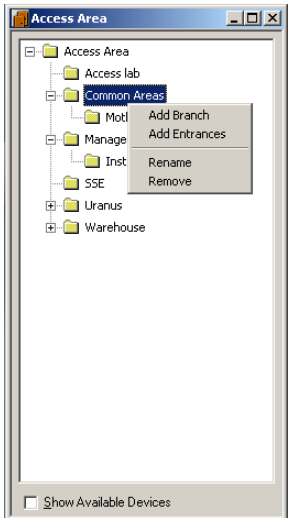
Example: If a reader R1 is located in the first floor of a building, you can define “First Floor” as the branch and R1 as the entrance within “First Floor.”

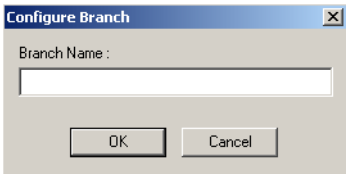


Readers, loops and doors that are already defined in the device map can be added to the access areas. The access areas are later mapped to access levels. The card holders who are associated with the access levels can gain access to the entrances in the access areas. The access areas configured are account specific.

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.





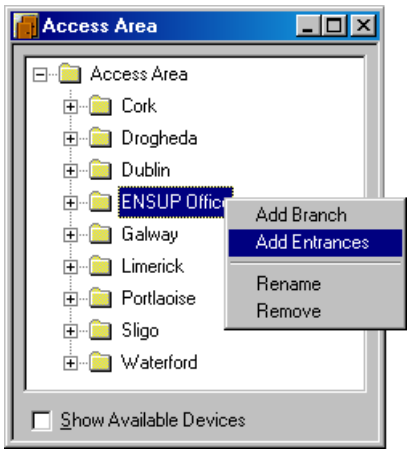
3. Type the **Branch Name**.
4. Click **OK**. The new branch is listed below the **Access Area** folder.

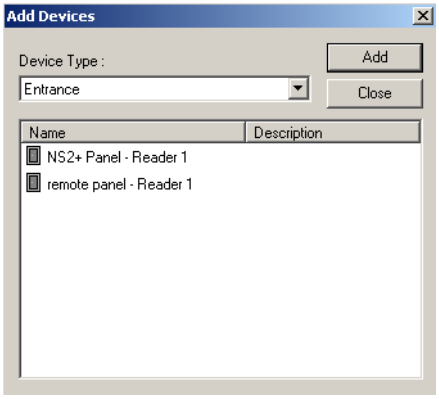
Note: If you are adding a branch inside another branch, the new branch appears below the selected branch.

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.

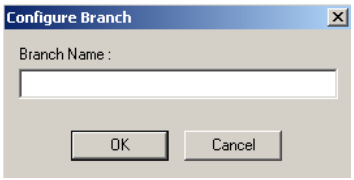
Moving an entrance

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.

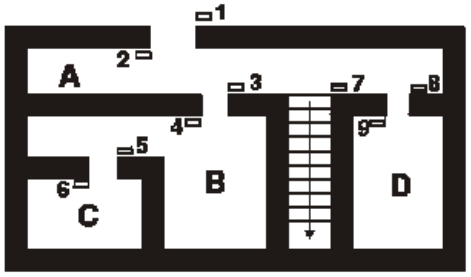
Note: You cannot remove an entrance if it is assigned to an access level.

Defining Tracking and Mustering Areas

Tracking and Mustering areas in WIN-PAK CS/SE/PE are logical areas consisting of entrances, and are used for tracking cardholder movements, for a particular account.

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 CS 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

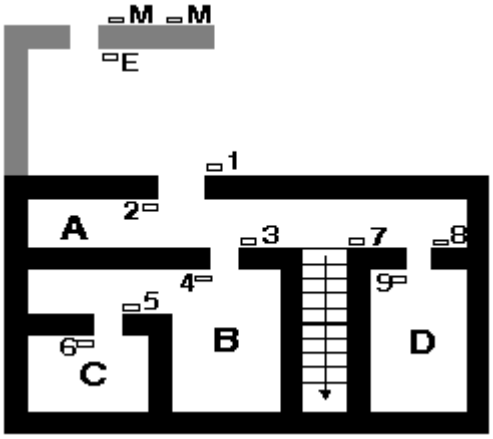
Nested areas are created when a tracking area is defined inside another tracking area and when a mustering area is defined under another mustering area. However, tracking areas cannot be nested inside mustering areas and vice versa.

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 CS/SE/PE 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.

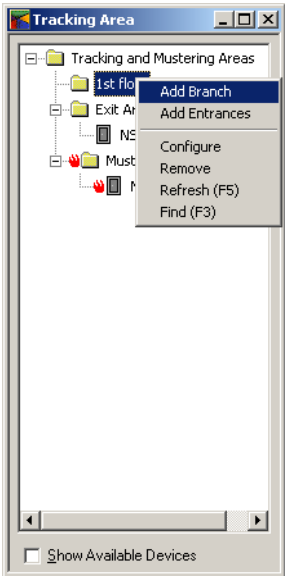
2. Run a special line for the muster units to provide a unique data path, even if the wiring from the main facility is damaged. The tracking units also have a unique data path.
3. Use 485 communications with ACK-NAK enabled. A battery backup power supply is required for the 485-API-2 on any N-1000 or NS2+ or P-Series panel.
4. Provide a UPS or other backup power source for the WIN-PAK CS/SE/PE 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 CS/SE/PE 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.

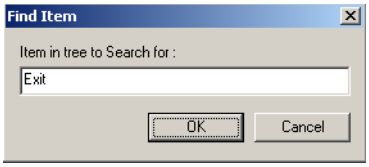
Removing a Branch or an Entrance

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:

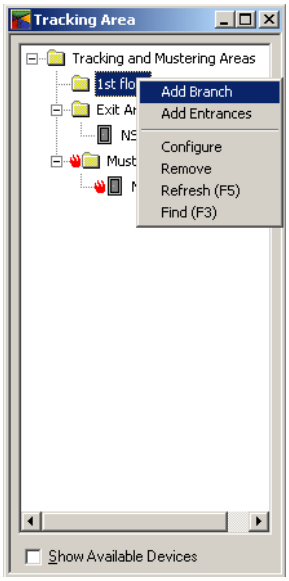
- From a tracking area you cannot search for a branch or an entrance in the mustering area.
- Right-click on a branch, and click **Refresh** to refresh the items in the tree.

Configuring Mustering Areas

Mustering areas are defined as branches of the **Tracking and Mustering** area tree of the WIN-PAK CS/SE/PE 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.

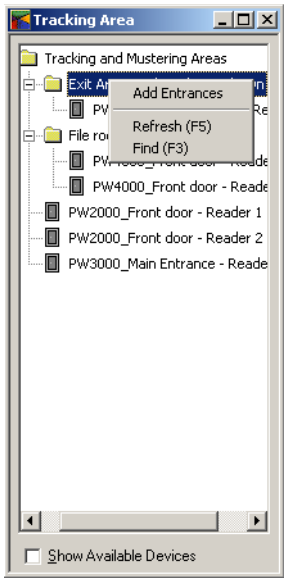
Note: The check box appears disabled if you are defining an area inside another mustering area.

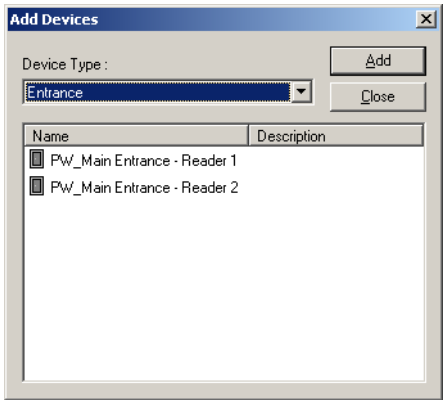
5. Click **OK**. The new branch is displayed in the **Tracking Area** window.

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.

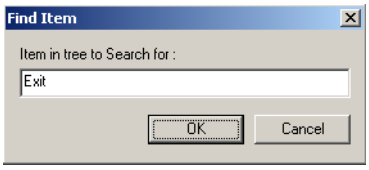
Removing a Branch or an Entrance

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.

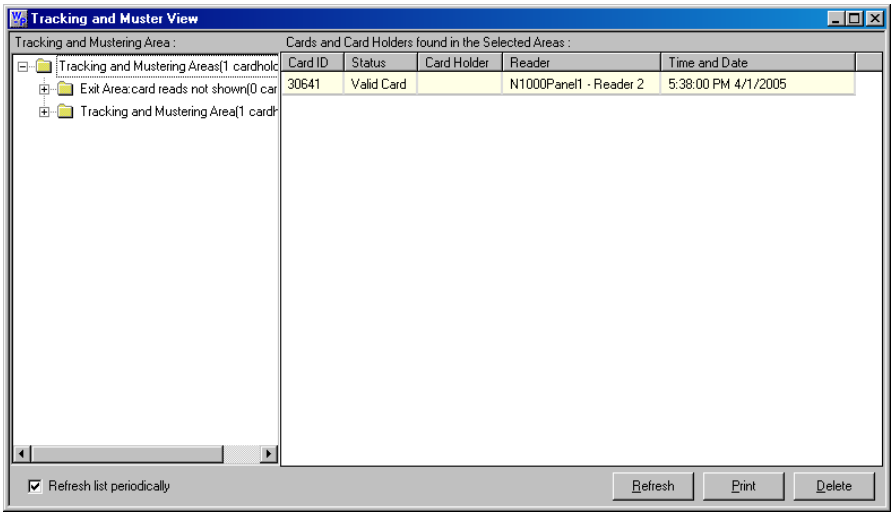
Before viewing the muster information, ensure the following:

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.

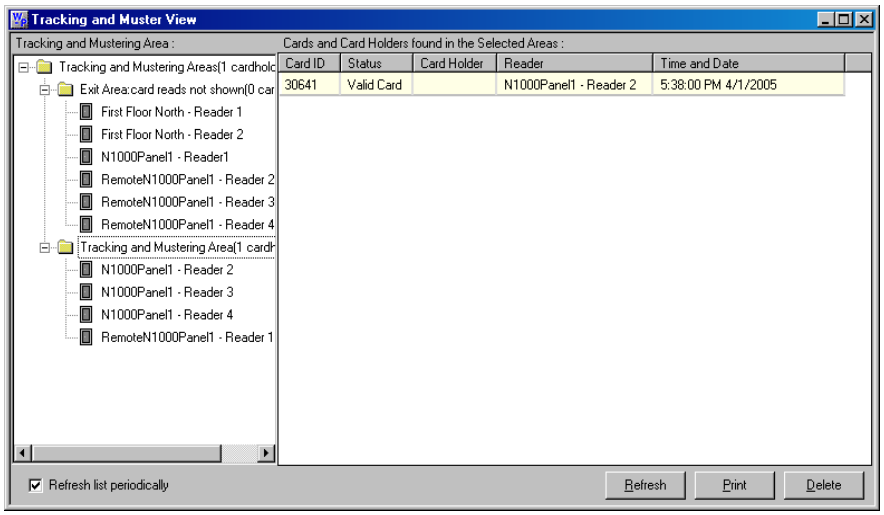


2. Expand the **Tracking and Mustering Areas** folder to list the branches and the entrances belonging to the selected branch.

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

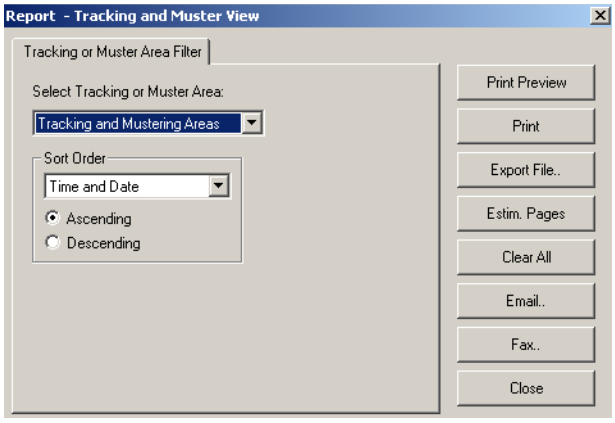
When a card holder has moved out of the tracking area without accessing the reader in the area, you can delete the card holder details from the **Tracking and Muster View** window.

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.
        - If you do not have 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 field that are specific to the selected account. If <**All accounts**> is selected, the note field 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.

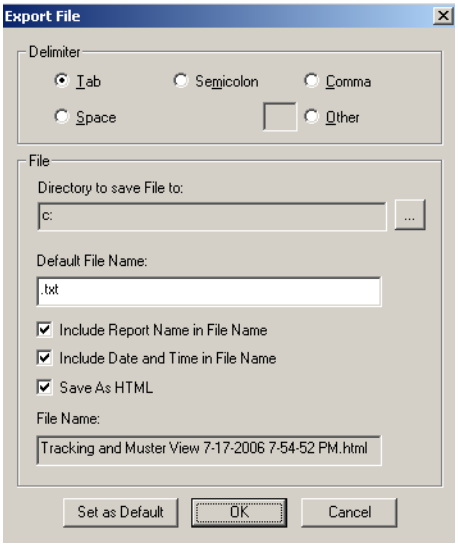
Note: The **Select NoteField** is available only in WIN-PAK SE/PE.

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 save the file in html format, select the **Save as HTML** check box. (applicable only in WIN-PAK CS).

   h. To set the delimiter and filename information as default for all text files, click **Set as Default**.

   i. 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**.

Note: Step 10 and 11 are applicable only for WIN-PAK CS.

10. To send the Tracking and Mustering report as an e-mail, click **Email**.

    Refer to the section "Sending the report as an e-mail" in the Reports chapter, for more details on sending the Tracking and Mustering report by e-mail.

11. To fax this report, click **Fax.**

Refer to the section "Faxing the report" in the Reports chapter, for more details on sending the Tracking and Mustering report by fax.

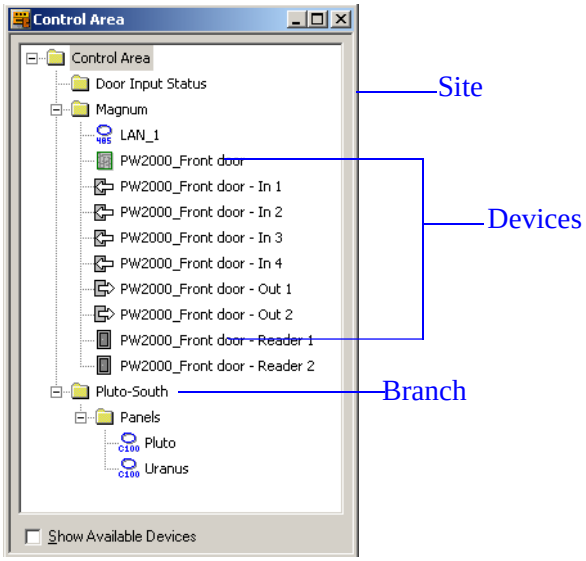
12. To close the **Report-Tracking and Muster View** dialog box, click **Close**.

Defining Control Areas

Control areas are logical areas containing devices such as 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.

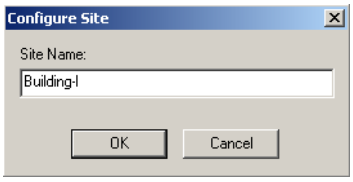
Control Maps are defined by adding a site, adding branches to the site and then adding devices to the branches. The devices can also be added directly to a site.



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.

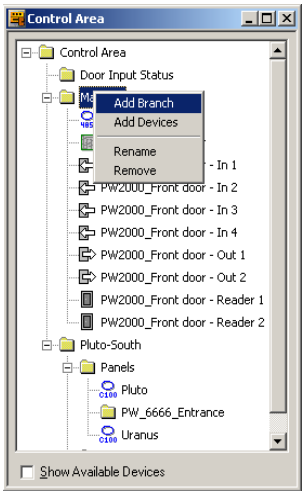


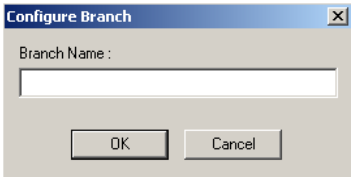
3. Enter the **Site Name**.
4. Click **OK** to add the site as a control area.

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**.

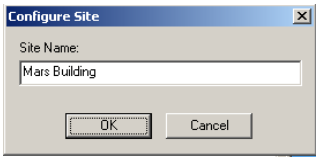




3. Type the **Branch Name**.
4. Click **OK**. The branch is listed under the site or the branch in the **Control Area** window.

Renaming a Site or a Branch

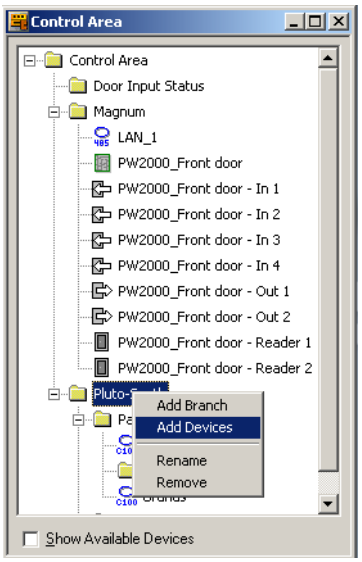
1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Right-click the branch or the site you want to rename.
3. Click **Rename**. The dialog box for renaming the branch or site appears.

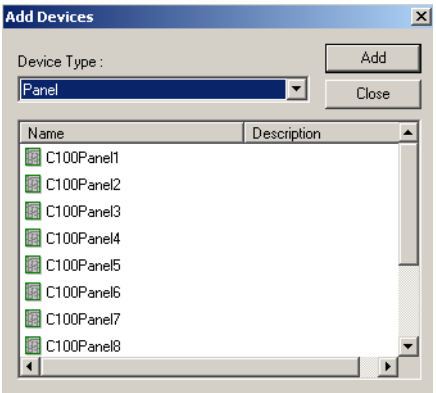


4. Type the site or the branch name.
5. Click **OK** to save the change.

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.

4. Select the device to be added and click **Add**.

Note: To select 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

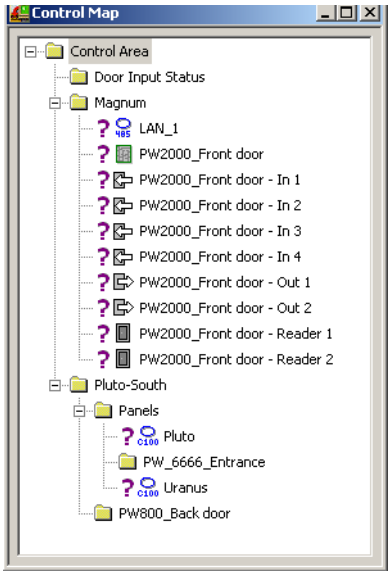
1. Choose **Configuration > Define > Control Areas**. The **Control Area** window appears.
2. Right-click the branch, site or device you want to remove.
3. Click **Remove**. A message asking for confirmation appears.
4. Click **OK** to remove the selected site, branch or device. The site, branch or device 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

   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 10-1 Typical ADVs and Control Functions of WIN-PAK CS/SE/PE

ADV	**Control Functions**
Alarm View	Open Click **Open** to open the **Alarm View** window through the floor plan.
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

Table 10-1 Typical ADVs and Control Functions of WIN-PAK CS/SE/PE

ADV	Control Functions
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 See 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
Static Camera	Acknowledge All Alarms, Clear All Alarms
Galaxy Communication	Acknowledge All Alarms, Clear All Alarms

Table 10-1 Typical ADVs and Control Functions of WIN-PAK CS/SE/PE

ADV	Control Functions
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.
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

Table 10-1 Typical ADVs and Control Functions of WIN-PAK CS/SE/PE

ADV	Control Functions
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. **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. **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.
Vista Output	Acknowledge All Alarms, Clear All Alarms **Activate** - Activates the output. **Deactivate** - Deactivates the output. **Refresh** - Refreshes the latest status of an output.

Table 10-2 Typical ADVs and Control Functions of WIN-PAK SE/PE

ADV	Control Functions
NetAXS Panel	Acknowledge All Alarms, Clear All Alarms, Buffer All Panels, Unbuffer All Panels, Initialize, Cancel Data Transfer, Set Cards to Unused, Disable NetAXS Web Mode, Time Zone.
NetAXS Input	Acknowledge All Alarms, Clear All Alarms, Shunt, Unshunt, Restore to Time Zone, Time Zone (Shunt Time Zone, Block Interlock Time Zone, Disable Alarms and Normal Messages in Time Zone).
NetAXS Output	Energize, De-energize, Pulse, Timed Pulse, Restore to Time Zone, Acknowledge All Alarms, Clear All Alarms, Time Zone (Energize Active Time Zone, Block Interlock Time Zone).
NetAXS Reader	Acknowledge All Alarms, Clear All Alarms, Unlock, Lock, Shunt, Unshunt, Restore to Time Zone, Time Zone (Shunt Time Zone, Block Interlock Time Zone, Disable Alarms, and Normal Messages in Time Zone).

Table 10-3 Control Map icons for PRO3000 entrances/doors in WIN-PAK SE/PE

Icon	Lock State	Description
	Manually Locked (Lockdown)	This is a state when there is a manual lock done through WINPAK SE/PE (that is, through Control Map, Floor plan, Command file, and so on) Whenever a door is in this state, the door does not: accept any valid card swipes. report any card events to WINPAK SE/PE. The door can be unlocked only through egress (usage of REX).
	Manually Unlocked	This is a state when there is a manual unlock done through WINPAK SE/PE (that is, through Control Map, Floor plan, Command file, and so on). No card reads or REX is necessary to unlock the door.
	REX on Lockdown	The door, which is in lockdown state, is now in unlocked state by the usage of egress (usage of REX).
	Auto Lock	When there is no human intervention, the lock remains in the Auto Lock state.

	Auto Unlock	When there is an egress (usage of REX) or a valid card swipe/read, the door unlocks and changes to auto unlock state.

The icons for the Galaxy devices and Vista devices for WIN-PAK SE/PE 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:

Table 10-4 Device Types and their respective icons in WIN-PAK SE/PE

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)

Device Types	Action	Icon	Status	Description
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)
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)

Initializing a Panel from Control Map

When panels are added to the WIN-PAK CS/SE/PE 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 an P-Series panel from the control map:

1. Choose **Operations > Control Map**. The **Control Map** dialog box appears.

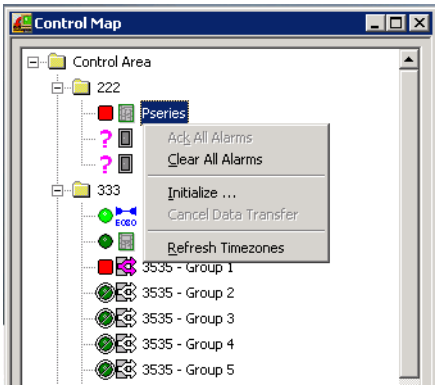


Figure 10-1 Control Map

2. Right-click the **P-Series** panel in the Control Map tree, and select **Initialize**. The **Panel Initialization Options** dialog box appears.

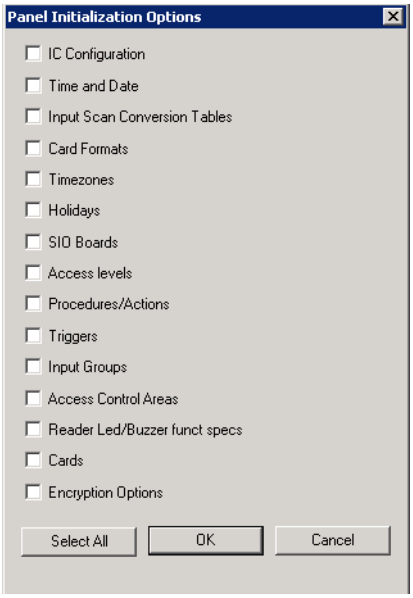


Figure 10-2 Panel Initialization Options

See 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.

See the Initializing Status section in this chapter for details on status of the initialization.

Panel Initialization Options

Table 10-5 Describing panel initialization options

Panel Initialization Options	Description
IC Configuration	Sends all IC configuration information. This resets your panel programming. It is recommended that you use the "Select All" feature (button) when the IC 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.
Input Scan Conversion Tables	

Additionally, new or updated information on the following features, functions, and panel elements are sent to the panel:

- Card Formats
- Time Zones
- Holidays
- SIO Boards
- Access Levels
- Procedures/Actions
- Triggers
- Input Groups
- Access Control Areas
- Reader LED/Buzzer specs
- Cards
- Encryption Options

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.

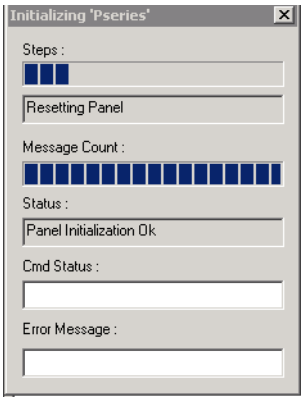


Figure 10-3 Initialization Status

Table 10-6 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.

To initialize a NetAXS panel from the control map:

1. Choose **Operations > Control Map**. The **Control Map** dialog box appears.

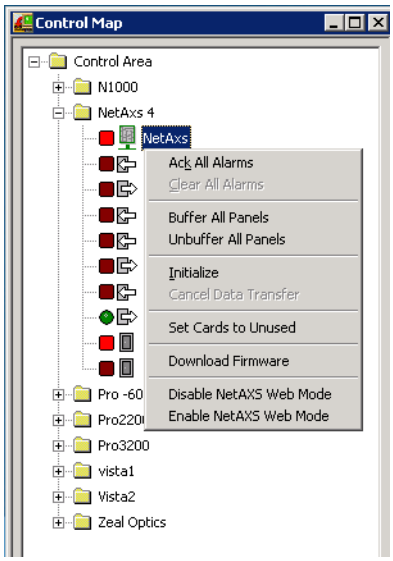


Figure 10-4 Control Map

Note: In WIN-PAK CS/SE/PE the Enable NetAXS Web Mode and Disable NetAXS Web Mode are available only if you log on with admin privileges.

2. Right-click the **NS3** panel in the Control Map tree, and select **Initialize**. The **Panel Initialization Options** dialog box appears.

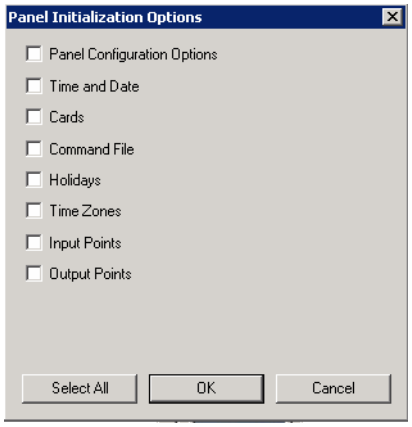


Figure 10-5 Panel Initialization Options

See 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.

See the Initializing Status section in this chapter for details on status of the initialization.

Panel Initialization Options

Table 10-7 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.

Table 10-7 Describing panel initialization options

Cards	Downloads 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 downloaded to the panels. All other card information changes are downloaded using this command.

Additionally, new or updated information on the following features, functions, and panel elements are sent to the panel:

- Command File
- Holidays
- Time Zones
- Input Points
- Output Points

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.

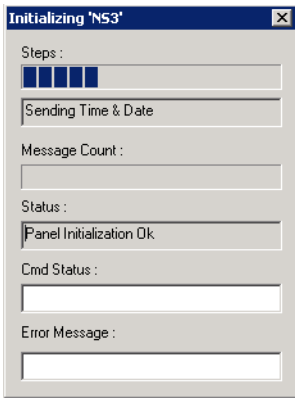


Figure 10-6 Initialization Status

Table 10-8 Describing fields in the Status dialog box

Field name	Description
Steps	Indicates what information is sent.
Message Count	Indicates the progress of messages sent.

Table 10-8 Describing fields in the Status dialog box

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.

Download firmware in NetAXS panels

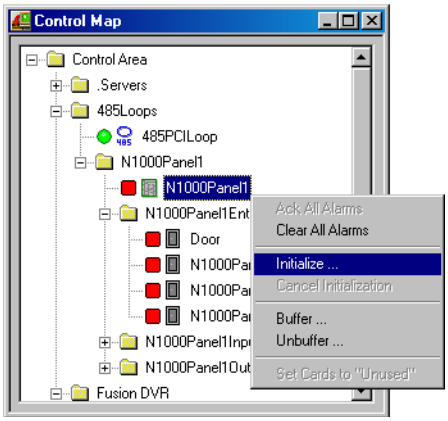
Notes:

- You can download the firmware only if you have logged on with admin privileges.
- You can download the firmware only from the NetAXS gateway panel to the NetAXS panel.

The latest firmware is available at C:\Program Files\WINPAKPRO\Firmware\releases. For all the new firmwares included, ensure to upload the firmware at C:\Program Files\WINPAKPRO\Firmware\releases.

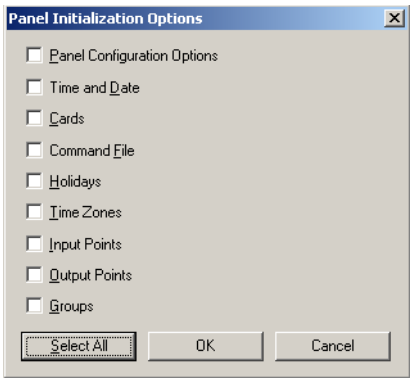
To initialize an N1000 panel from the control map:

1. Choose **Operations > Control Map**. The **Control Map** dialog box appears.



2. Right-click the N1000 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.

Note: Remote panels can also be initialized in the schedule record dialog box. Refer to the Dial Remote Area section in the Time Management chapter for more information about this.

Panel Initialization Options

Table 10-9 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.

Table 10-9 Describing panel initialization options

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.

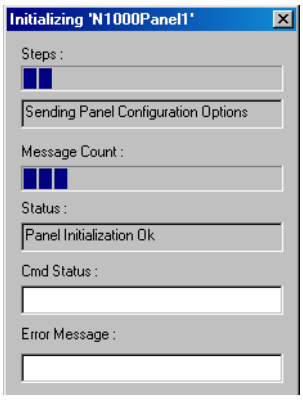


Table 10-10 Describing fields in the Status dialog box

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

11

In this chapter...

This chapter describes about the Introduction to Floor Plan, Floor Plan Definition, and Floor Plan Operation in WIN-PAK CS, and SE/PE.

Introduction

A floor plan is a map or plan of the building, used for viewing, monitoring, and controlling devices for the selected account within the WIN-PAK CS/SE/PE Access Control System.

This chapter describes how to create floor plans and to control system devices using floor plan views for the selected account.

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) with a resolution of 600X800 and are stored in the **WIN-PAK\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. Selecting an Account (applicable only in WIN-PAK CS).
2. Adding a floor plan.
3. 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.
4. Adjusting the size of the floor plan and previewing it.
5. Editing and deleting a floor plan.

Selecting an Account

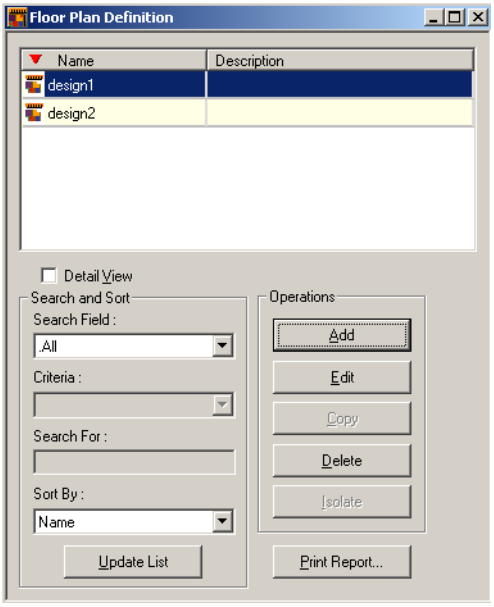
To select an account:

1. Choose **Account** > **Select**. The **Select Account** window appears.

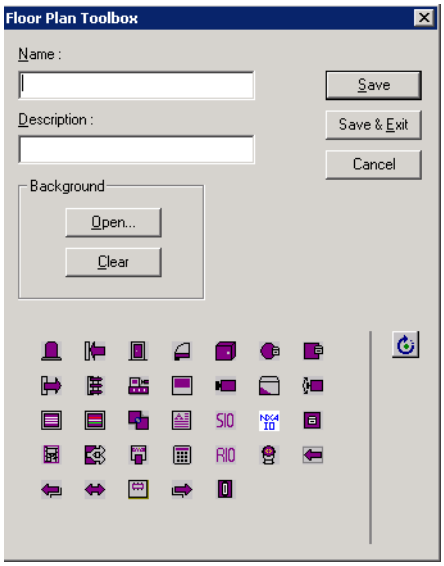
2. Select the required account and click **Select**. The name of the selected account appears in the title bar.

Adding a Floor Plan

1. Choose **Configuration > Floor Plan Definition**. The **Floor Plan Definition** window appears.

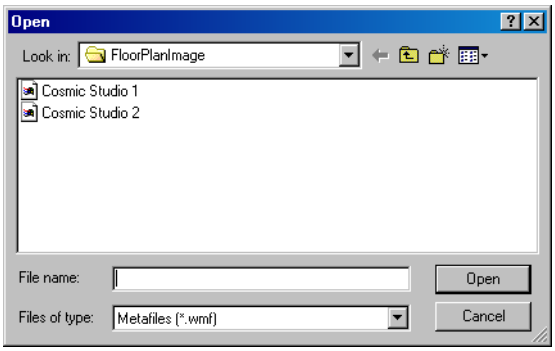


2. Click **Add**. The **Floor Plan Toolbox** dialog box together with a blank window for creating a floor plan design appear.



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 through 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 **WIN-PAK\Database\ FloorPlanImage** folder.

Note: The background image must be less than 5 MB and the image filename must not be more than 30 characters.

7. Add ADVs, links, and text objects to the background.

   See 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.

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.

   See 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.

Note: In WIN-PAK SE/PE, under the **General Configuration** option, you can set the **Type** for the following floor plan icons:

- Input
- Output
- Galaxy group
- Galaxy output
- Galaxy zone

The various **Types** are:

  - Door contract
  - Generic
  - Manual break glass/Egress Device
  - PIR Egress Device

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.

See the following table for information on ADV icons, ADV names, and description.

Table 11-1 ADV Icons and Description

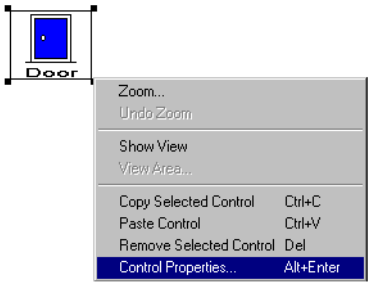
Icon	Name	Description
	Input (WIN-PAK CS)	For any alarmed condition, Input sends an alarm.
	Input (WIN-PAK SE/PE)	Signals an alarm condition for configuring four different types of zones, namely Generic, Manual Break glass / Egress device, Magnetic Contact/Door contact or Passive Infra Red Detector/Egress device.
	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.
	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 (WIN-PAK CS)	Used with relay output ADV.

	Output (WIN-PAK SE/PE)	Used with relay output ADV for configuring four different types of output such as, Generic, Lamp, Siren or Strobe. Each output type displays an animation for activated or inactive state.
	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.
	NetAXS Input and Output	Used to extend the input and output capabilities of the NetAXS panels.
	Galaxy Communication	Used with Galaxy Ethernet module (E080) ADV.
	Galaxy Panel	Used with Galaxy panel ADV.

	Galaxy Group (WIN-PAK CS)	Used with Galaxy group ADV.
	Galaxy Group (WIN-PAK SE/PE)	Used with Galaxy group ADV for configuring three different types of groups such as, Generic, Outline or Room. Each group type displays an animation for normal, alarm, trouble, tampered state and additionally indication of (dis)armed state and indication of group reset required.
	Galaxy MAX	Used with Galaxy MAX ADV.
	Galaxy Keypad	Used with Galaxy keypad ADV.
	RIO Control	Used with Galaxy RIO control ADV.
	Galaxy Output (WIN-PAK CS)	Used with Galaxy output ADV.
	Galaxy Output (WIN-PAK SE/PE)	Used with Galaxy output ADV for configuring four different types of output such as, Generic, Lamp, Siren or Strobe. Each output type displays an animation for activated or inactive state.
	Galaxy Zone (WIN-PAK CS)	Used with Galaxy zone ADV.

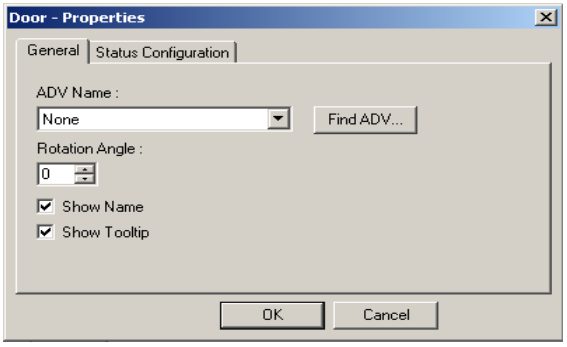
	Galaxy Zone (WIN-PAK SE/PE)	Used with Galaxy zone ADV, for configuring the following types of Zones: • Active Infra Red detector • Fire Detector • Generic • Glass Break Detector • Magnetic Contact • Passive Infra Red Ceiling Detector • Passive Infra Red Detector • Passive Infra Red Long Detector • Personal Attack Button • Seismic Sensor or Shunt Lock Contact Each zone type displays an animation for the different states such as Normal, Alarm, Trouble, and Tampered. In addition, depending on the Galaxy group to which the zone belongs to, the status of Arm/Disarm is displayed.
	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.

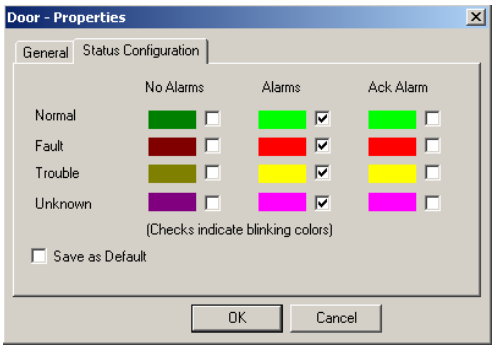
    c. Select an ADV from the list and click **OK** to return to the properties dialog box.

    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.

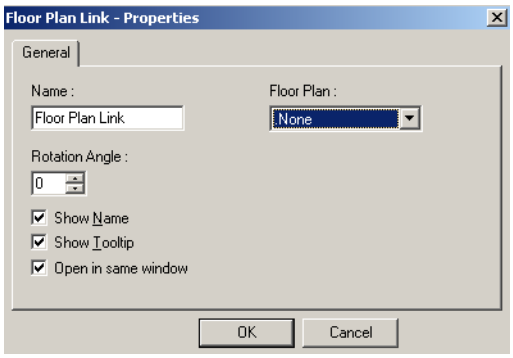
Adding Links to other Floor Plans

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.



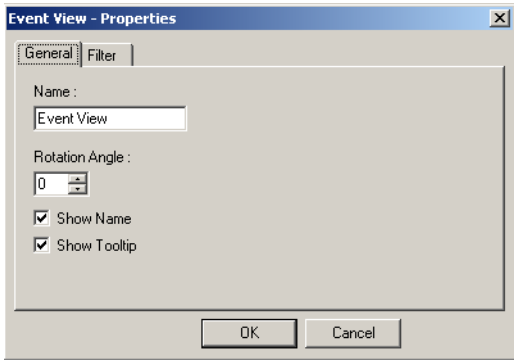
3. Type a name for the floor plan link in **Name**. By default, the link appears with **Floor Plan Link** as its name.
4. Select the name of the floor plan to be linked in the **Floor Plan** list.
5. To rotate the ADV control, enter the **Rotation Angle** or use the scroll bars to select an angle from 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

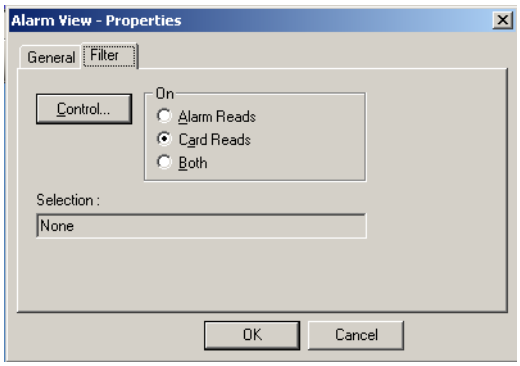
Alarm View and Event View links enable you to view the alarms and events occurring for a device from the floor plan.

To add an Alarm View or an Event View link to the floor plan:

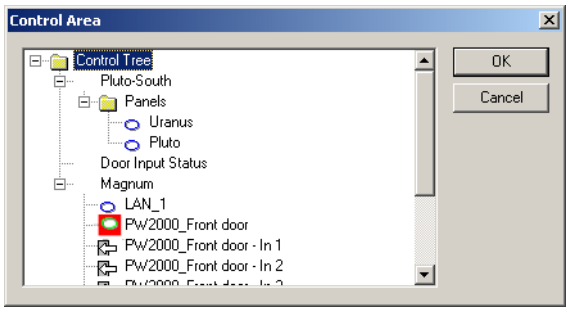
1. In the **Floor Plan Toolbox** dialog box, select the  for Alarm View or  for Event View and drag it to the floor plan design.
2. Right-click the link object and click **Control Properties.** A properties dialog box appears



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**.

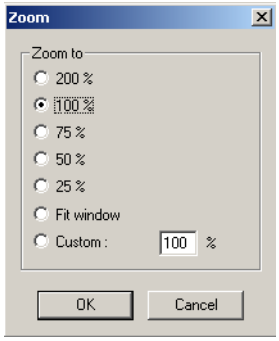
Adding a Text Box to the Floor Plan

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.



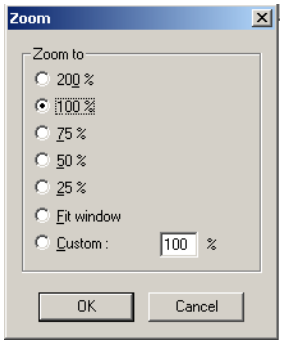
    b. Select the zoom percentage or enter the percentage in **Custom**.
    c. Click **OK** to save the zoom percentage and to close the **Zoom** dialog box.

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.

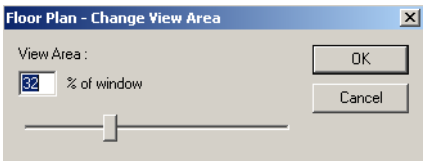
Note: Right-click anywhere inside the floor plan design and select **Undo Zoom** to display the floor plan in its previous size.

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. Highlight 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 status of the ADVs, which is indicated by different colors.

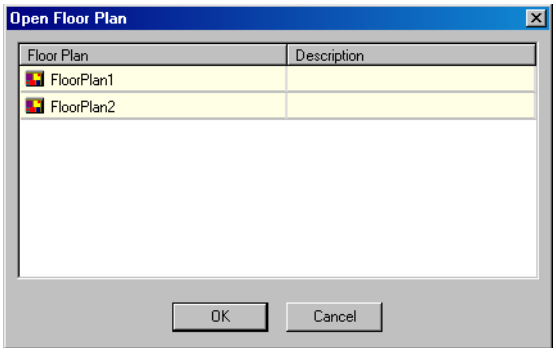
Note: Ensure that you have defined the color-coding for the various ADV statuses while designing the floor plan.

See the "Adding an ADV to the Floor Plan" section of this chapter for information on setting the status colors for ADVs.

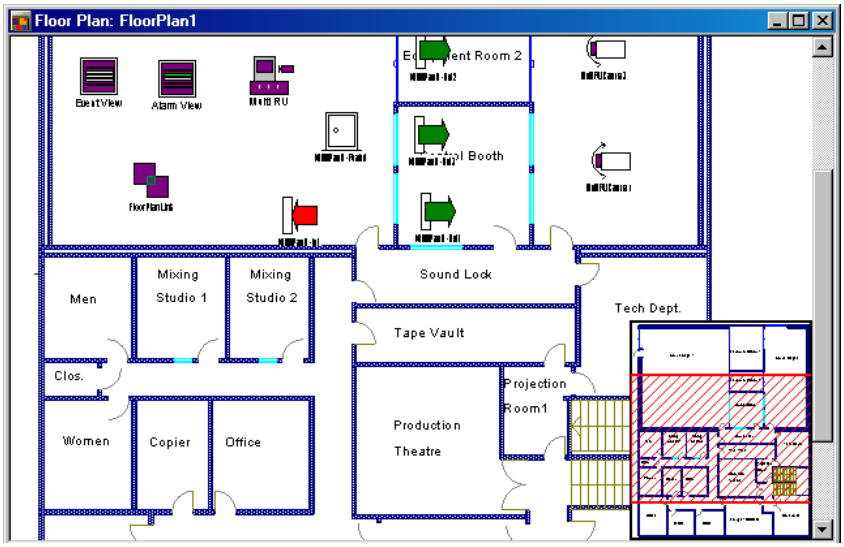
Working with Floor Plan Views

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

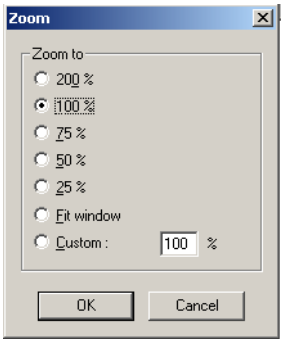
You can resize a floor plan view by adjusting the zoom percentage. In addition, you can preview the floor plan view to view the entire floor plan as a snap shot inside the floor plan view window.

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.

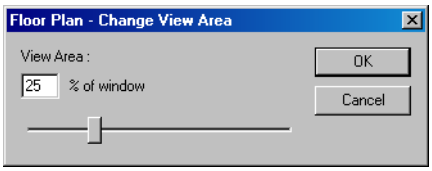
Note: Right-click anywhere in the floor plan view and select **Undo Zoom** to view the floor plan in its original size.

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 11-2, Table 11-3, Table 11-4 and 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 views:

- 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 11-2 ADV Control Functions from floor plan for WIN-PAK CS/SE/PE

ADV	Control Functions
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
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
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

ADV	Control Functions
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.
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

ADV	Control Functions
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. **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.
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. **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.

Table 11-3 ADV Control Functions from Floor plan for WIN-PAK CS

ADV	Control Functions
Digital Video	Send Time & Date, Send Camera Titles, Camera to Monitor Switch, Acknowledge All Alarms, Clear All Alarms
Loop C-100/RS-232 Port	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms
Loop PCI	Buffer All Panels, Unbuffer All Panels, Set Retry Count, Set Command Timeout, Acknowledge All Alarms, Clear All Alarms

Table 11-4 ADV Control Functions from Floor plan for WIN-PAK SE/PE

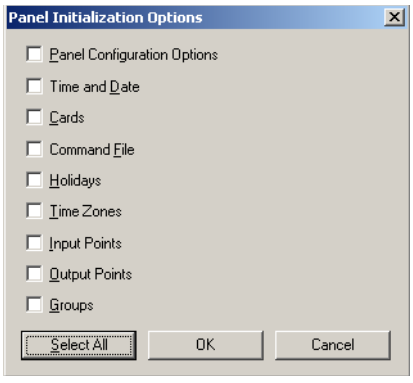
ADV	Control Functions
CCTV Switcher	Send Time & Date, Send Camera Titles, Camera to Monitor Switch, Acknowledge All Alarms, Clear All Alarms.
Comm Server	Acknowledge All Alarms, Clear All Alarms.
Command File Server	Run Command File.
C-100 Local Connection	Buffer All Panels, Unbuffer All Panels, Set 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.
Modem Pool	Hang-Up Modem, Rest Modem, Acknowledge All Alarms, Clear All Alarms.
CCTV Monitor	Acknowledge All Alarms, Clear All Alarms

Initializing Panels from Floor Plan

When panels are added to the WIN-PAK CS 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.



See 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.

See the "Initializing Status" section in this chapter for details on status of the initialization.

Panel Initialization Options

Table 11-5 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.

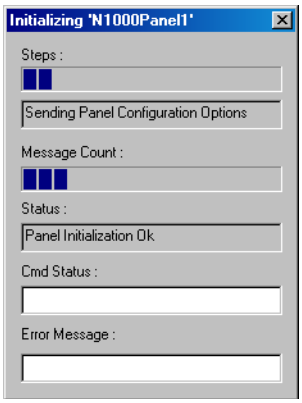


Table 11-6 Describing fields in the Status dialog box

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

12

In this chapter...

This chapter describes about the Command File Configuration in WIN-PAK CS, and SE/PE.

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. The commands are defined specific to the account.

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.

In WIN-PAK CS, the Command File is configured to suit the varied and specific requirements of each account. Therefore, it is necessary to select an account before proceeding with the command file configuration.

Selecting an Account

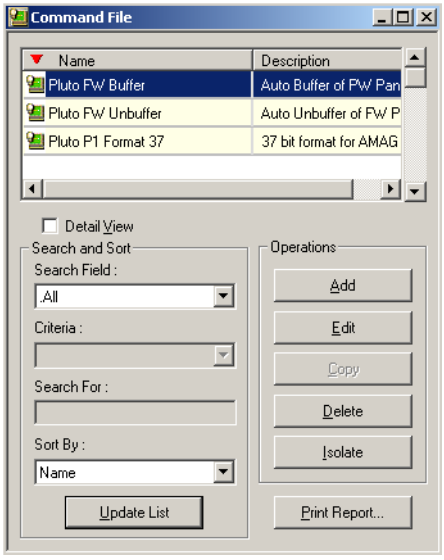
Note: **Selecting an Account** is applicable only in WIN-PAK CS.

To select an account:

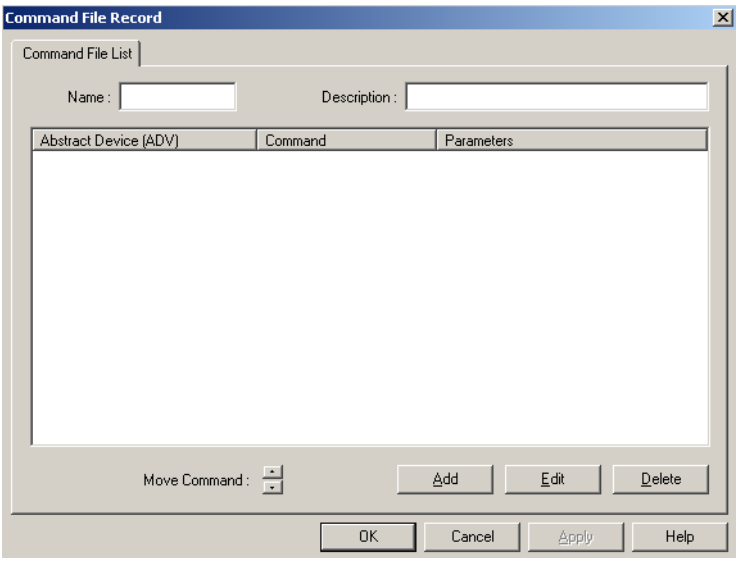
1. Choose **Account** > **Select**. The **Select Account** window appears.
2. Select the required account and click Select. The name of the selected account appears in the title bar.

Adding a command file

1. Choose **Configuration > Command File**. The **Command File** window appears.



2. Click **Add**. The **Command File Record** dialog box appears.

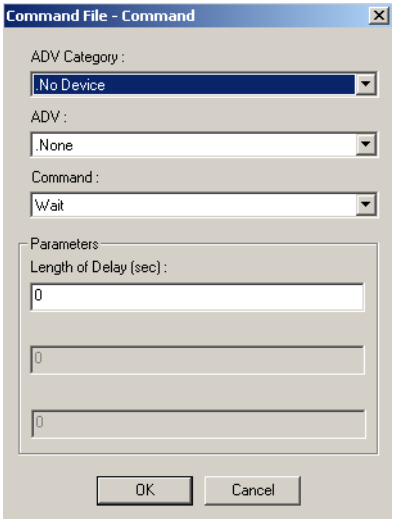


3. Type the name of the command file in the **Name** box.
4. Type a **Description** for the command file.
5. To add commands to the command file, click **Add**.

   See 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 12-1 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.

See the "Running a Command File" section in this chapter for more details on adding a custom command.

See Table 12-1 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 12-1 for the parameters fields displayed for the ADV controls.

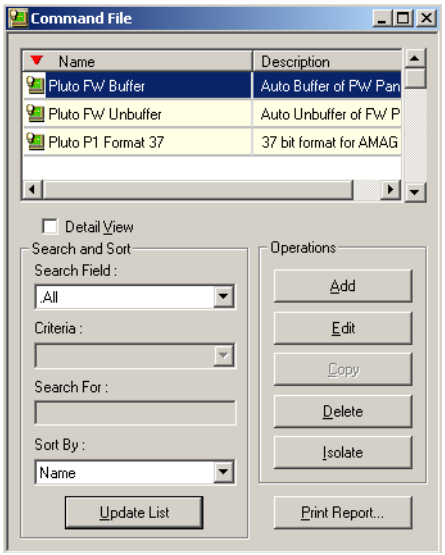
5. Click **OK** to save the changes.

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 12-1 Command and Parameter list for ADVs for WIN-PAK CS/SE/PE

ADV	Commands	Parameters
Door	Lock	
	Pulse	
	Timed Pulse	0 - 65, 335 sec.
	Unlock	
DVR Input	Shunt	
	Unshunt	
DVR Output	De-Energize	
	Energize	
	Timed Pulse	Pulse time in sec
Galaxy Group	Part Set	
	Set	
	Timed Set	Set Time (in Sec) = 0 to 180 sec.
	Unset	
Entrance	Lock	
	Pulse	
	Timed Pulse	Pulse (Sec)
	Unlock	
Galaxy Output	Activate	
	Deactivate	
Galaxy Panel	Reset	
	Set Panel	
	Unset Panel	
Galaxy Zone	Bypass	
	Force Bypass	
	Unbypass	

Table 12-1 Command and Parameter list for ADVs for WIN-PAK CS/SE/PE

ADV	Commands	Parameters
Loop	Buffer All Panels	0 = Soft, 1=Hard
	Unbuffer All Panels	0 = Soft, 1=Hard
Output & Group	De-energize	
	Energize	
	Pulse	
	Switch to TimeZone Control	
	Timed Pulse	0 - 65, 335 sec.
Panel	Buffer Panel	
	Unbuffer Panel	0 = Soft, 1=Hard
	Anti Passback - Set all cards to Unused	
	Anti Passback - Set card number to Unused	
	Lock Web Mode	
	Unlock Web Mode	
	Custom Command	
PTZ Camera	Goto Home Preset	
	Goto Preset	
	Record Duration	
	Record Intensive	
	Record Normal	
	Record Normal Off	
	Record Quality	
	Record Rate	
	Record Resolution	
Server (All)	Refresh	

Table 12-1 Command and Parameter list for ADVs for WIN-PAK CS/SE/PE

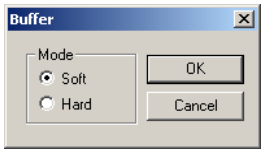
ADV	Commands	Parameters
RS232 Connection	Custom Command	
Stationary Camera	Record Duration	Duration (sec)
	Record Intensive	
	Record Normal	
	Record Normal Off	
	Record Quality	Quality
	Record Rate	Frame/Images Per Seconds
	Record Resolution	Resolution
Vista Output	Activate	
	Deactivate	
Vista Panel	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	

Table 12-2 Command and Parameter list for ADVs in WIN-PAK SE/PE

ADV	Commands	Parameters
CCTV	Camera	Go Home
	Go to Present	Preset #
	Iris Open	0 - 65, 335 sec.
	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	Door Lock
	Switch Camera ID	Camera ADV

Notes: 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 CS User Interface.
- When you select an **Unbuffer** command, the event details that are buffered in the panel are transmitted to the WIN-PAK CS 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 12-3 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 CS/SE/PE. Therefore, the events buffered only between 2 to 3 P.M. are sent to WIN-PAK CS/SE/PE.
Second **Unbuffer** Command at 3 P.M.	Events buffered between the first and the second buffer commands are sent to WIN-PAK CS/SE/PE. Therefore, the events buffered between 1to 2 P.M. are sent to WIN-PAK CS/SE/PE.

Table 12-4 Scenario 2

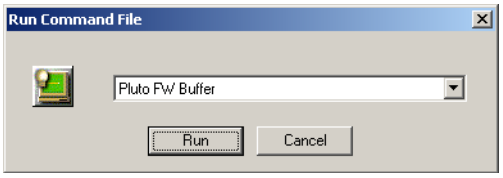
Action	**Result**
Buffer Command at 1 P.M.	Events buffered in the panel from 1 P.M.
Buffer Command at 2 P.M.	Events continue to be buffered in the panel even after 2 P.M.
Mode	Hard
Single **Unbuffer** Command at 3 P.M.	All the buffered events (from 1 P.M. to 3 P.M.) are sent to WIN-PAK CS/SE/PE.

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

13

In this chapter...

This chapter describes about the Introduction to Guard Tour, Configuring Gaurd Tours, and Running Guard Tours in WIN-PAK CS, and SE/PE.

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 defined are unique to an account.

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:

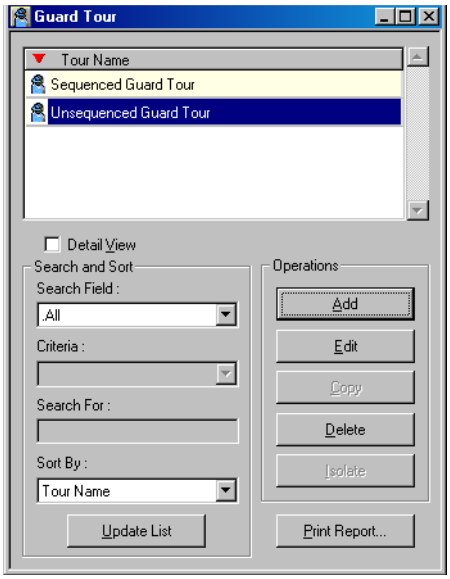
- Adding a guard tour.
- Defining readers and input points as a part of sequenced and unsequenced check points.
- Associating action groups to check points and specifying priority for each state together with the command file to be executed when the action occurs.

Adding a Guard Tour

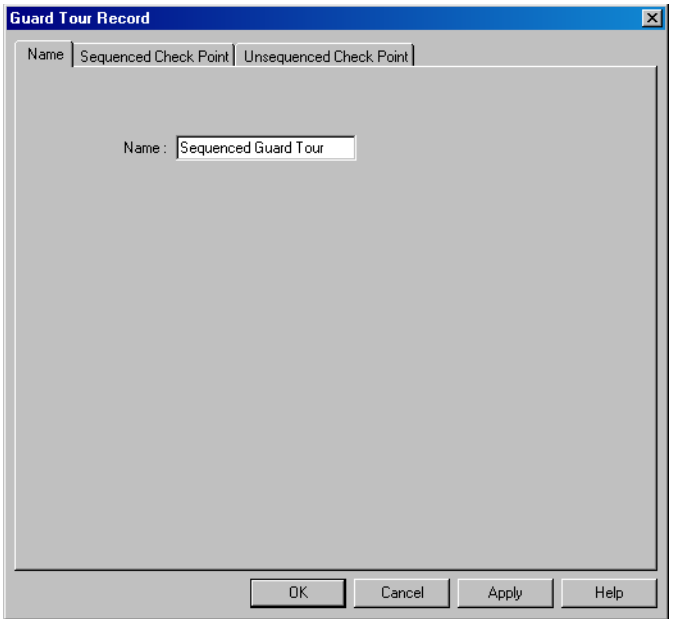
Adding a guard tour involves defining a name for the guard tour and specifying at least one check point for the guard tour.

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 close the **Guard Tour Record** dialog box.

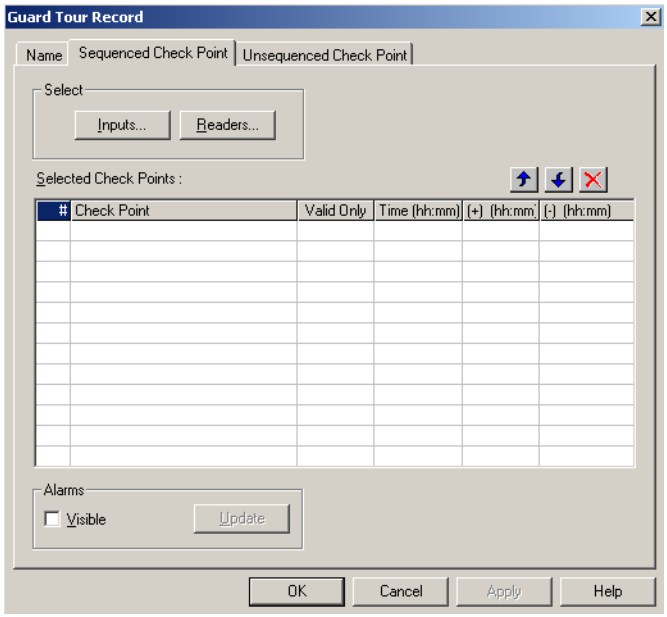
Adding Check Points

Readers and Input points can be added as sequenced and un-sequenced check points to the guard tour.

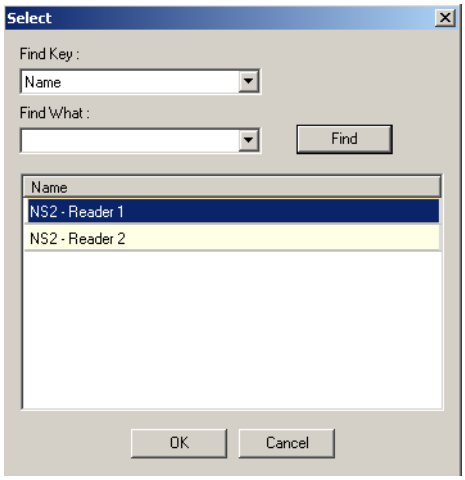
Note: It is mandatory to add at least one check point to the guard tour.

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.

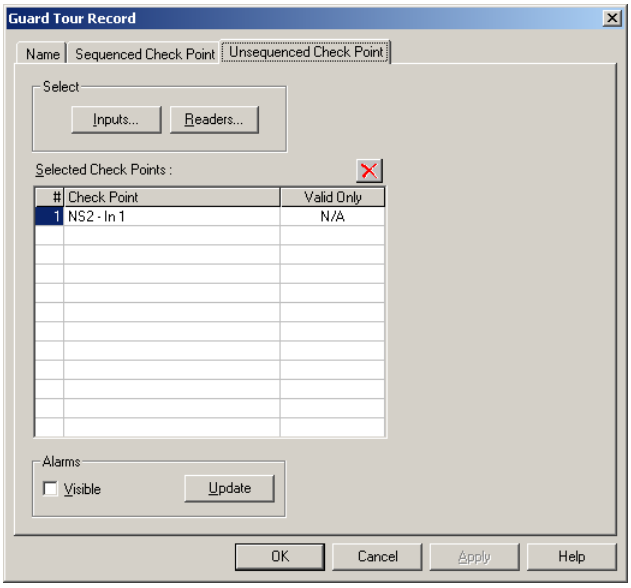
    Note: Clear the **Visible** check box to close the **Abstract Device Record** dialog box.
12. To change the display order of the checkpoints:
    - Select a reader or input point in the **Selected Check Points** list, and click  to shift it to the top of the list.
    - Select a reader or input point 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.

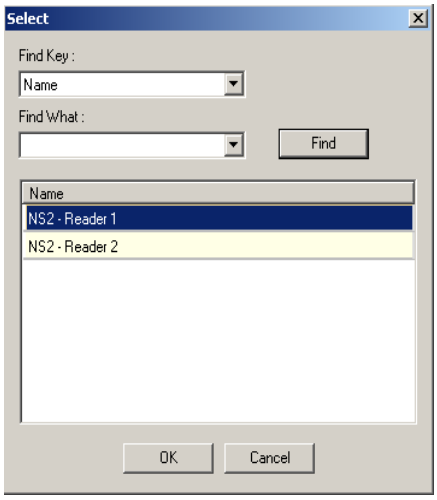
13. To remove a reader or an input point from the list of check points, select the reader or input point in **Selected Check Points** and click .

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:

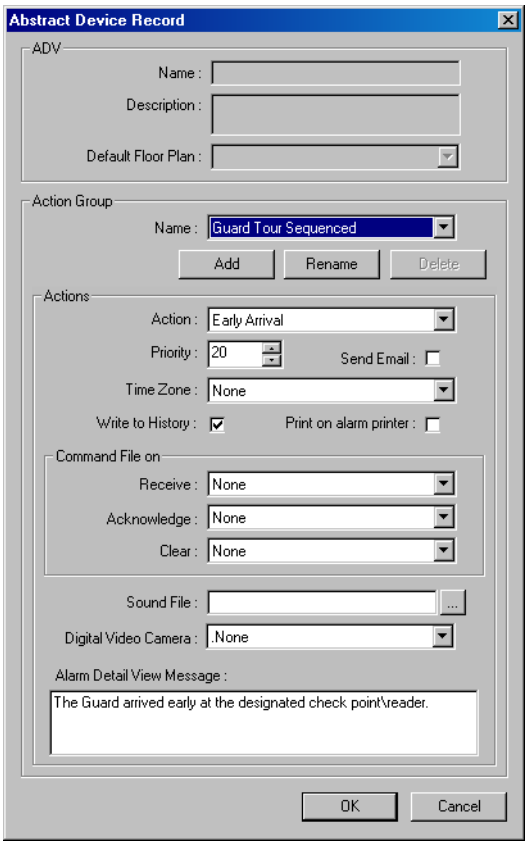
a. An action group is associated to a sequenced or unsequenced check point.

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.



See the "Configuring an Abstract Device" section in the WIN-PAK CS Servers and Devices 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.

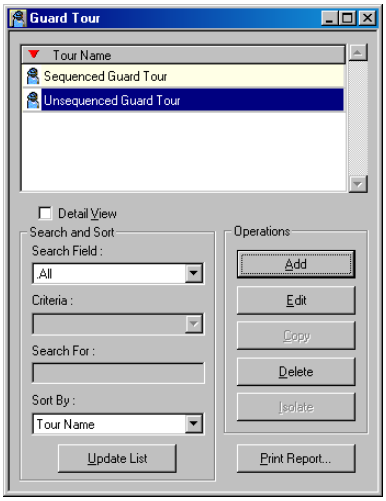
See the "Adding a Guard Tour Server" section of the WIN-PAK CS/SE/PE Servers and Devices chapter for information on configuring a guard tour.

Running a guard tour for a specific account involves:

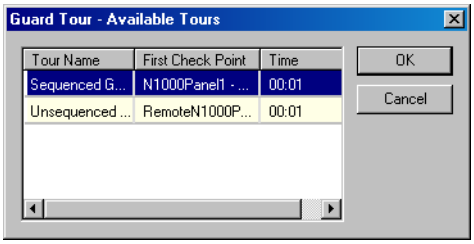
- Selecting the guard tour you want to run.
- Specifying the card that is used by the guard for accessing various check points.
- Starting the guard tour.
- Viewing the status of the sequenced and unsequenced check points that the guard accesses while the guard tour progresses.
- Viewing the alarms and events generated for the actions configured for the various check point states in the guard tour.

Starting a Guard Tour

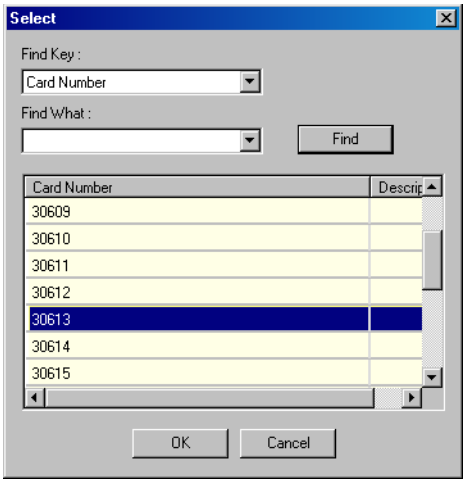
1. Choose **Operations > Guard Tour**. The **Guard Tour** window appears.



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.

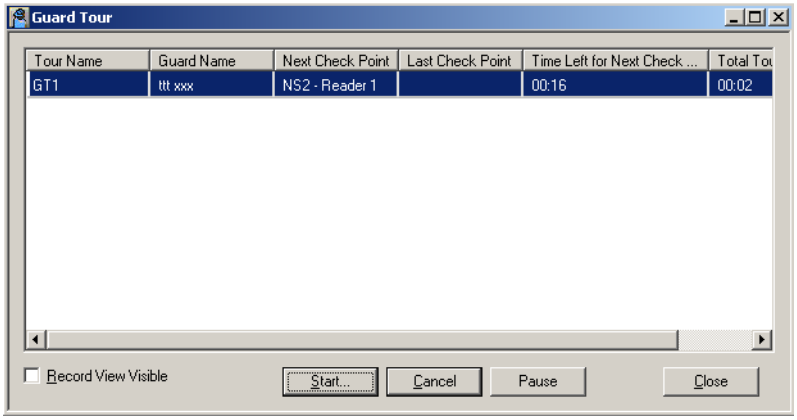
    b. In the **Find What** list, enter all or a part of the card number or description.

    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.

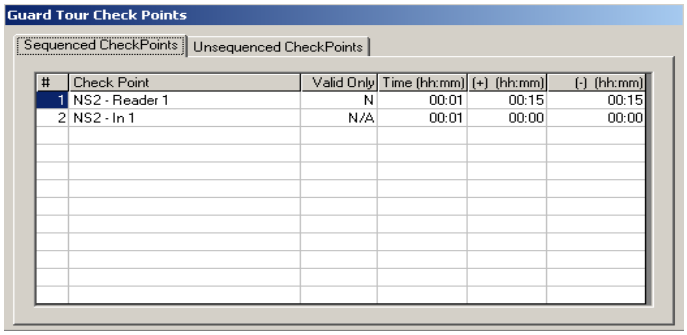
Note: Cards need not be added to a guard tour, having only input points as its checkpoints.

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

14

In this chapter...

Introduction

In the WIN-PAK CS 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 CS.

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 CS 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

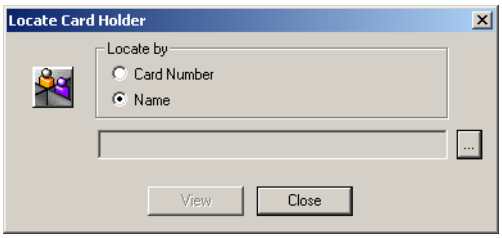
- The Digital Video Display window displays the live video or the recorded video from the DVRs.

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.

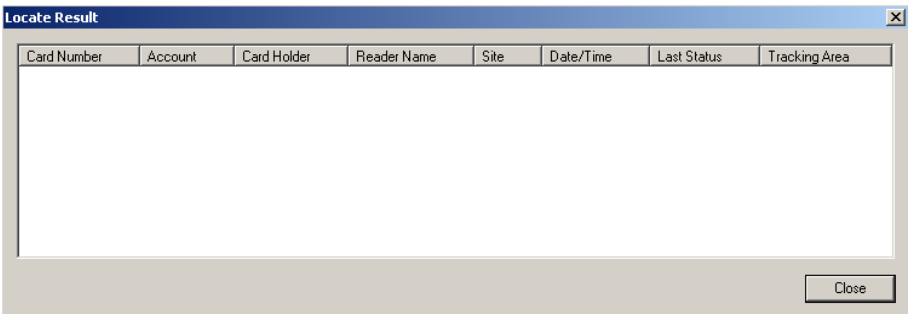


2. Under **Locate by**, click **Card Number** or card holder **Name**.
3. Click the ellipsis button to search for the card holder. The **Select** dialog box appears.

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

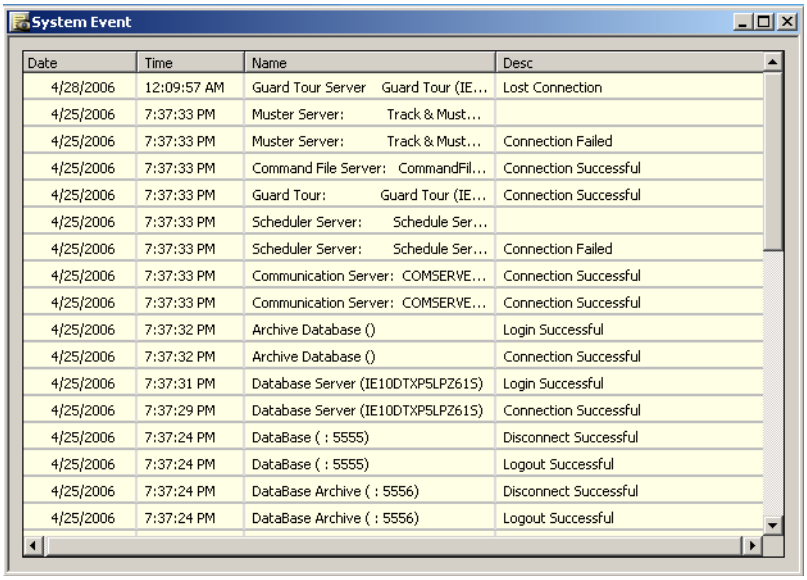
The System Event window displays the details of the WIN-PAK CS system activities, such as successful and unsuccessful server connections, log on details, and server disconnections. Details such as the name, time, and date of the activity are displayed. This enables you to easily identify the sources of problems during server communications.

Viewing System Events

The WIN-PAK CS system provides an option to the user to view the history of the WIN-PAK CS 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

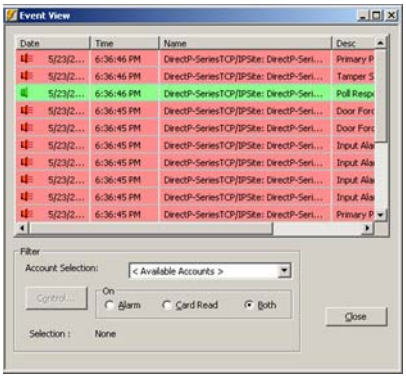
An event is an access control activity such as a card read, change in the state of input, and so on. The **Event View** window displays the details of access control activities as and when they occur. The number of events displayed in the Event View depends on the setting made for the maximum number 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 CS system.

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.

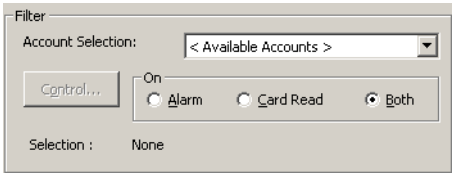
Note: Rows with icon indicate alarms.

Filtering Event Views

The WIN-PAK CS 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:

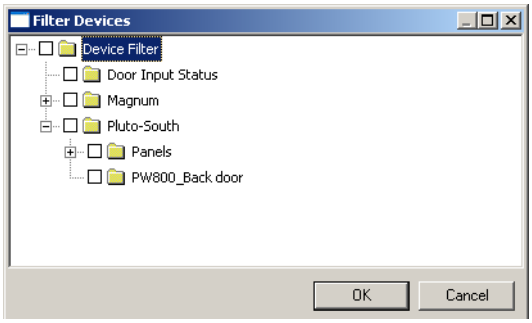
1. Click **Operations > Events** or click the View Events icon on the tool bar. The **Event View** window is displayed.
2. Select the account whose events you want to view, in the **Account Selection** list.
3. Select one of the following options under **On**:



   - **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.

4. To filter the events that occur in the specific areas and devices, click **Control** under **Filter**. The **Filter Devices** window appears.

Note: The **Control** button is enabled only when you select an account.



5. Expand the tree by clicking the plus [+] symbol.
6. Select a branch or an individual device to be filtered for monitoring.
7. 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.

8. 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.
9. To filter a device, right-click the device and select **Invert Selection Status** to select the device or clear the selection.
10. 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**.

11. 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 occurs. 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 14-1 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 in 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**.

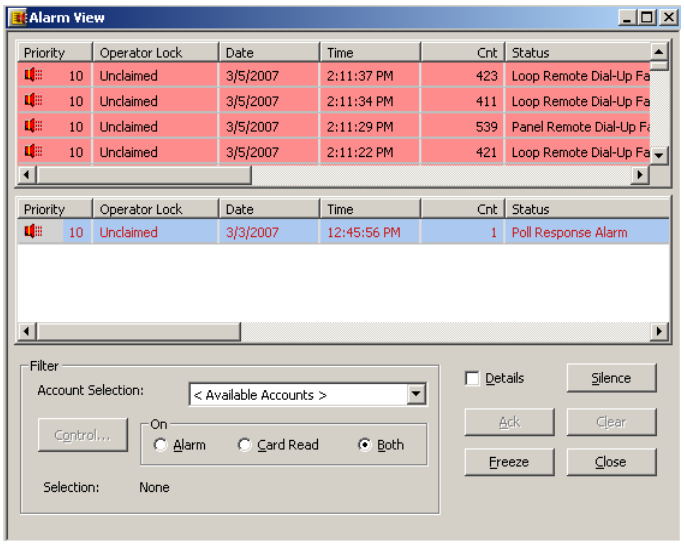
Opening an Alarm View Window

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.

The **Alarm View** window displays the alarms for all the accounts or for a single selected account.

To open the general Alarm View window:

1. Choose **Operations > Alarms**. The **Alarm View** window appears.



The details of an alarm are 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 details of all the alarms, irrespective of the accounts, are displayed.

The **Cnt** (Count) column on the **Alarm View** window shows the number of state changes in a point.

2. Select an account in the **Account Selection** list, to view the alarms raised for a specific account.
3. Click **Close** to close the **Alarm View** window.

Note: When an alarm is displayed in the **Alarm View**, it beeps until you acknowledge the alarm. However, this default setting can be changed in System Defaults.

You can handle the alarms of a single account in the **Account Specific View** window. When you right-click any alarm in the general **Alarm View** window, the **Lock Account** control option is displayed. **Lock Account** allows only one operator to handle the alarms for a specific account, at a given time. Refer to Figure 14-1.

When the account specific alarm view is opened for an account, no other operator can handle the alarms for that account. Therefore, the account is said to be locked.

Note: At a given time, an operator can lock only one account.

To open the Account Specific View window:

1. Choose **Operations > Alarms**. The **Alarm View** window appears.
2. Right-click any alarm in the general **Alarm View** window and select the **Lock Account** option. The **Account Specific View** window appears.

To unlock an account:

- Click the **Close** in the **Account Specific View** window.

  OR

- Right-click an alarm from the same account in the general alarm view window and select **Unlock Account**.

Note: The **Account Specific View** window closes on the expiry of the **Account Specific View Timeout** value, displaying a message indicating the same. The time out value can be set in the System Defaults.

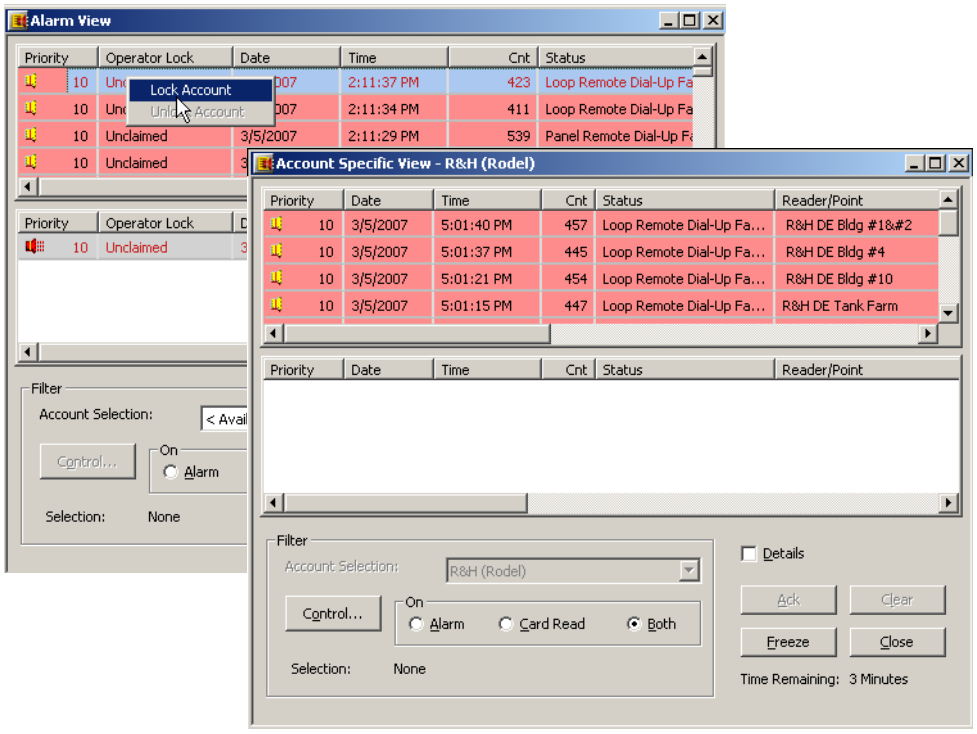


Figure 14-1 Open the Account Specific View

Handling Alarms using the right-click menu options

In the account-specific alarm view, when you right-click an alarm, a list of options to handle the alarms is displayed. Based on the selected alarm type, the list of menu options differ.

Control Functions to Handle an Alarm

The following control functions are available in the right-click menu, based on the alarm type:

- The available control functions for **Input** alarms: Acknowledge, Clear, Open Default Floor Plan, Add Note, Shunt, Unshunt, and Restore to Time Zone.
- The available control functions for **Door** alarms: Acknowledge, Clear, Open Default Floor Plan, Add Note, Unlock, Lock, Pulse, Timed Pulse, and Restore to Time Zone.
- The available control functions for **Reader** alarms: Acknowledge, Clear, Open Default Floor Plan, and Add Note.

- The available control functions for **Reader or Point** alarm attached to a camera: Acknowledge, Clear, Open Default Floor Plan, Add Note, Digital Video Live, and Digital Video Retrieval.
- The available control functions for **Panel System** alarms: Acknowledge, Clear, Open Default Floor Plan, Add Note, Buffer, and Unbuffer.

Table 14-2 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 WIN-PAK CS Servers and Devices, 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 enable you to easily handle basic, routine alarm tasks.

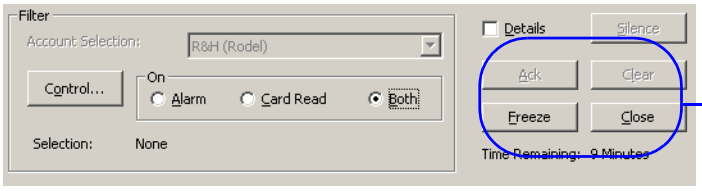


Table 14-3 Describing command buttons in the Alarm View window

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.
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 the **Alarm View**, click **Close**.

Note: While acknowledging or clearing alarms, to select multiple alarms:

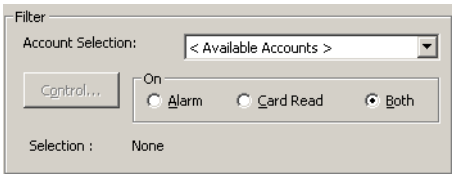
- In sequence: Press and hold the SHIFT key and click the first and last alarms in the range.
- At random: Press and hold the CTRL key and click each alarm.

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.

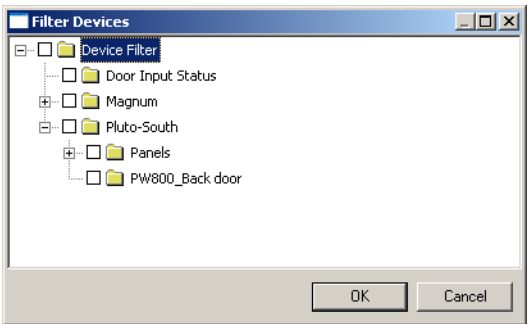
To filter the alarms:

1. Click **Operations > Alarms** or click the Dynamic Alarm View icon on the tool bar. The **Alarm View** window is displayed.
2. Select the account for which you want to view the alarms, from the **Account Selections** list.
3. Under **On**, click **Alarm**, **Card Read** or **Both** to view only the alarms, card reads or both respectively.



4. To filter the branches and devices, click **Control** under **Filter**. The **Filter Devices** window appears.

Note: The **Control** button is enabled only when you select an account.



5. Expand the tree by clicking the plus [+] symbol.
6. Select a branch or an individual device to be filtered for monitoring.
7. 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.

8. 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.
9. To filter a device, right-click the device and select **Invert Selection Status** to select the device or clear the selection.
10. Click **OK** to return to the **Filter Devices** dialog box.

11. 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.

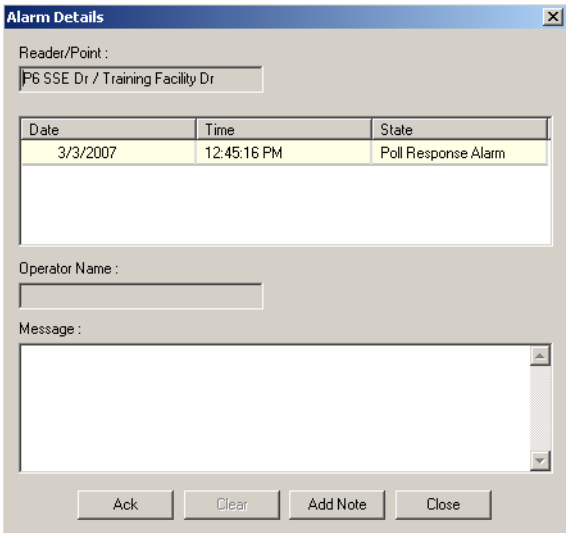
Note: The filter settings are lost once you close the Alarm View window. Therefore, to view the floor plan with filter settings, you can open the Alarm View window from the Floor Plan.

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:

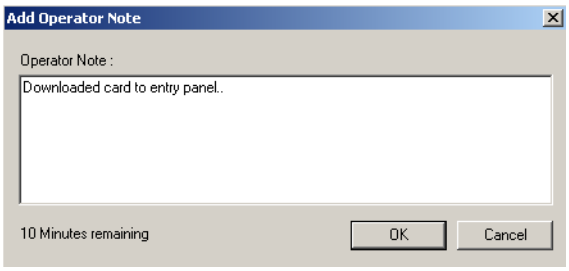
1. Choose **Operations** > **Alarms** or double-click an alarm to open an **Alarm View** dialog box.
2. Select the **Details** check box. The **Alarm Details** window is displayed.



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.

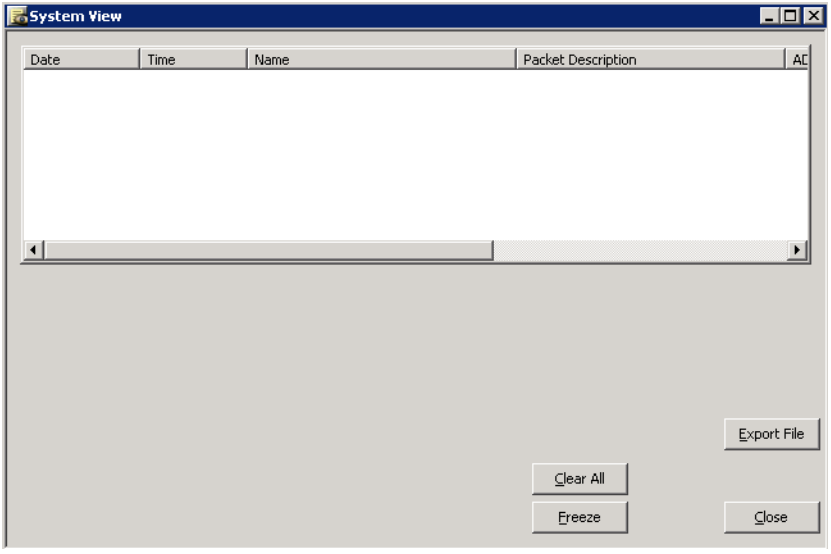
System Viewer Real Time

The System Viewer is available only to the operators with "Administrator" permissions, and displays data coming in and out of the communication port. This data can be generated as a report and exported to a file. A viewer freeze button is provided to freeze the scrolling information and allows you to scroll up and down the available list. The quantity of lines that can be viewed in real-time can be selected between 10 and 32,000 with a default setting of 1000.

Open the System Viewer Real Time window

To open the System Viewer Real Time window:

1. Choose **Operations > System Viewer Real Time**. The **System Viewer Real Time** window appears displaying the communication port data.



2. Click any of the following to customize the port data.
   - **Clear All** - clears the data.

- **Freeze** - Freezes the scrolling information.
- **Export File** - exports the data to Microsoft Excel.

Note: Ensure to install Microsoft Excel to view the .xls/.cvs files.

- **Close** - closes the system viewer real time window.

Autocard Lookup

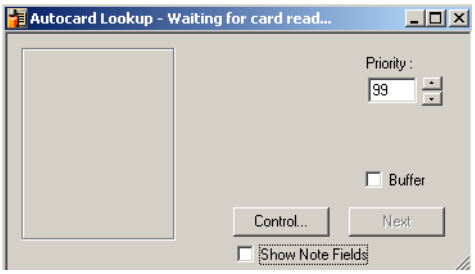
The Autocard Lookup feature enables you to view the card holders' details from the designated readers or card reads that have a status priority higher than a designated threshold. If the **Autocard Lookup** window is minimized and a card read is received, the window will pop-up automatically.

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:

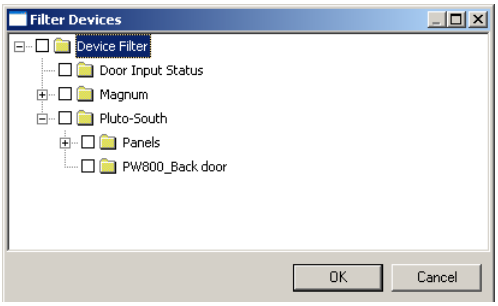
1. Choose **Operations > AutoCard Lookup**. The **AutoCard Lookup - Waiting for card read** window appears.



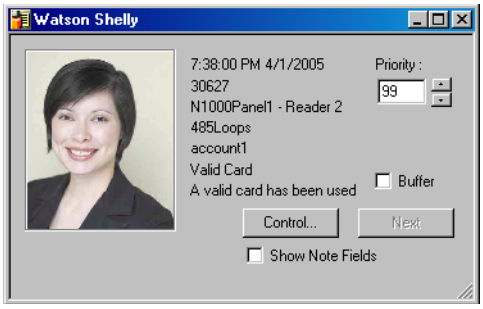
2. Set the **Priority** of card read. The card holder details of all card reads having a higher priority (lower number) than this priority is displayed in Autocard lookup. The priority of a given card read event is set in the reader's Action Group.

   Refer to the "Configuring an Abstract Device" section in the chapter WIN-PAK CS Servers and Devices 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.

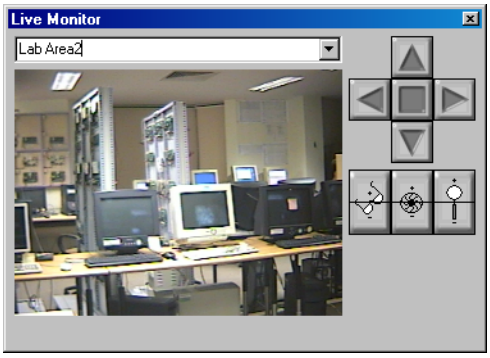


Figure 14-2 Live Monitor

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**.

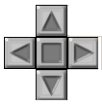
Controlling the Camera

You can control the focus, aperture adjustment, zoom, pan and tilt, and homing presets of switchers and cameras remotely through WIN-PAK.

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 14-4 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.

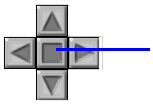
Clearing Limits

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 CS 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.

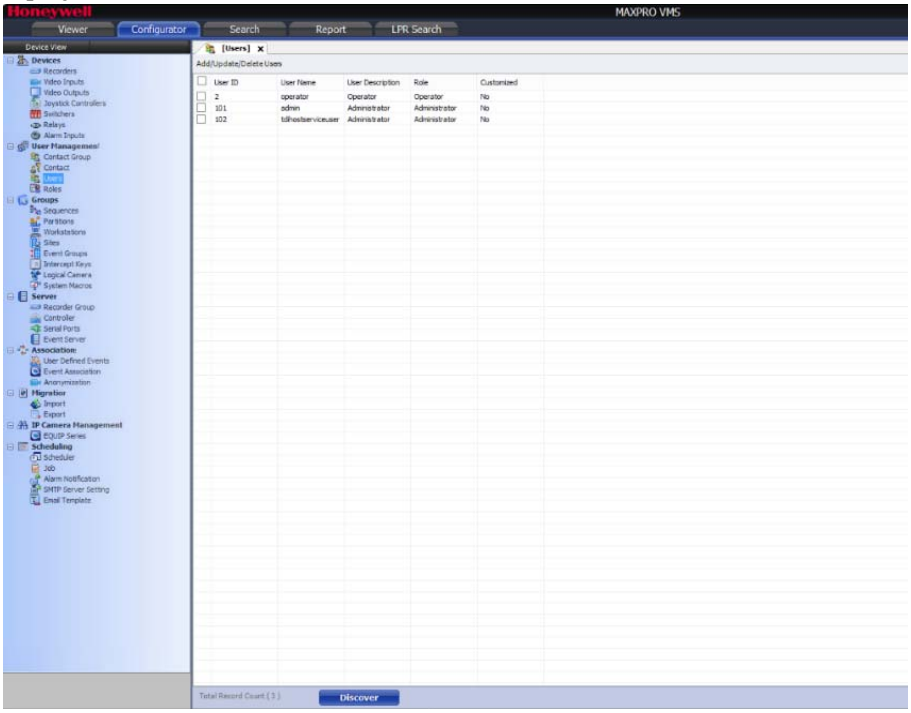
WINPAK-VMS integration GDPR Compliance

To implement GDPR compliance in WINPAK-VMS integration (support of Face masking and FourEye):

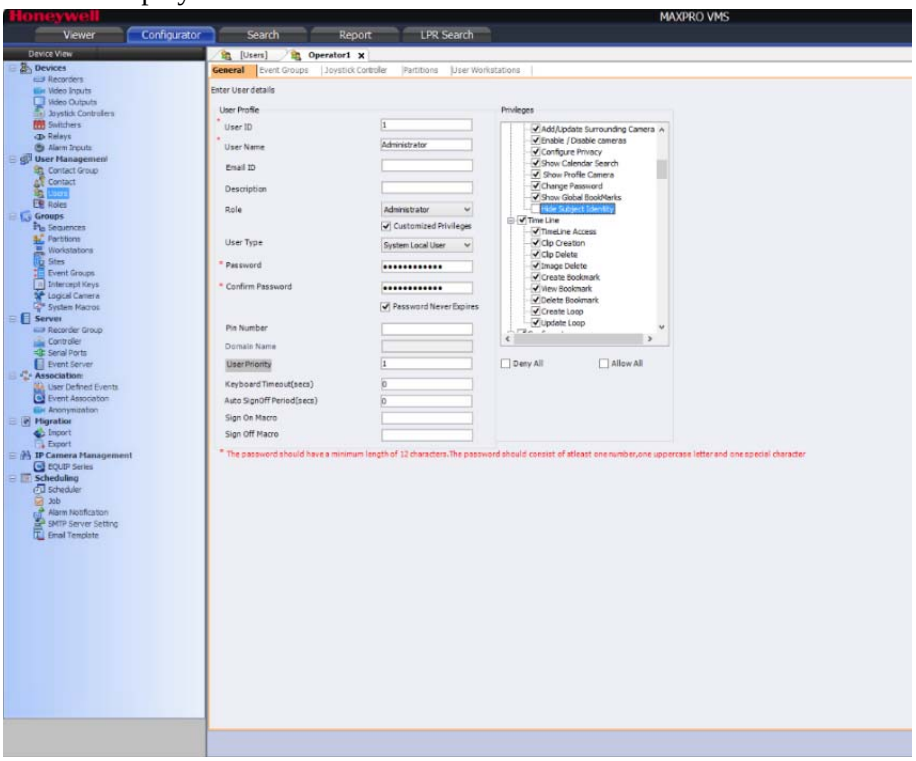
1. Navigate to **C:\Program Files(x86)\WINPAKPRO\Honeywell\TrinityFramework\Bin** folder.

Right-click on **MMSHELL.exe** and select **Run as administrator** from the popup menu. The **Login Information** dialog box appears.

2. Type your **Admin User Name** and **Password**.
3. Click **Configure** and select **Users** in Device View. The following screen is displayed with a list of users available.

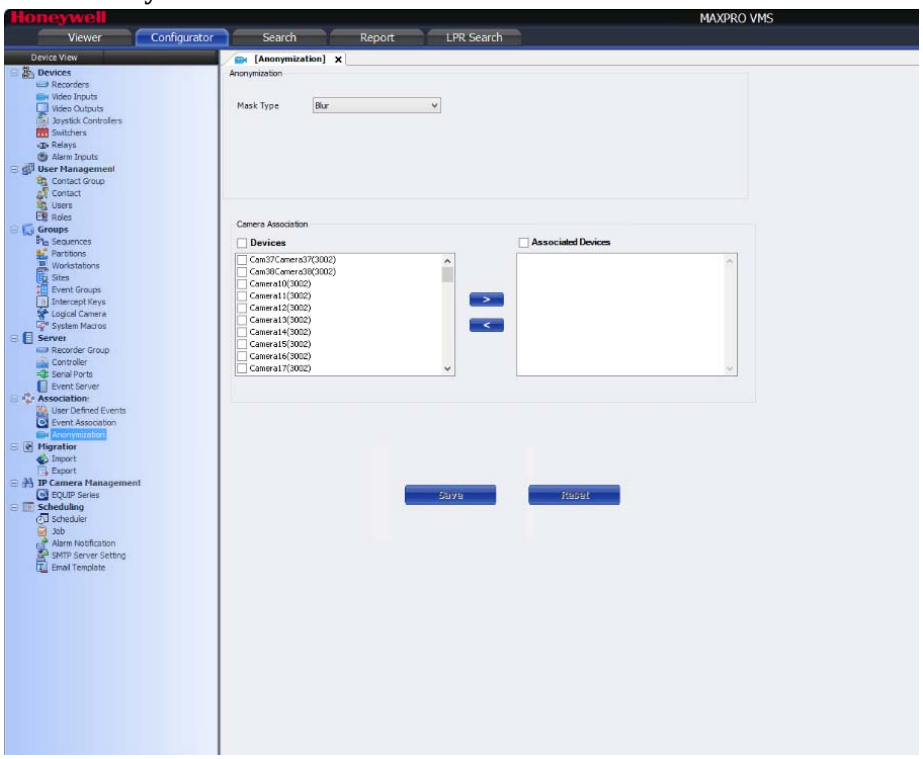


4. Click the **Add** button to create a new VMS administrator user. The following screen is displayed.



5. Type the **User Name**, **Email ID** and **Description**.
6. Select the **Role**.
7. Select the **Customized Privileges** check box and select the **Allow All** check box.
8. Click **Save** to save the VMS Operator user.

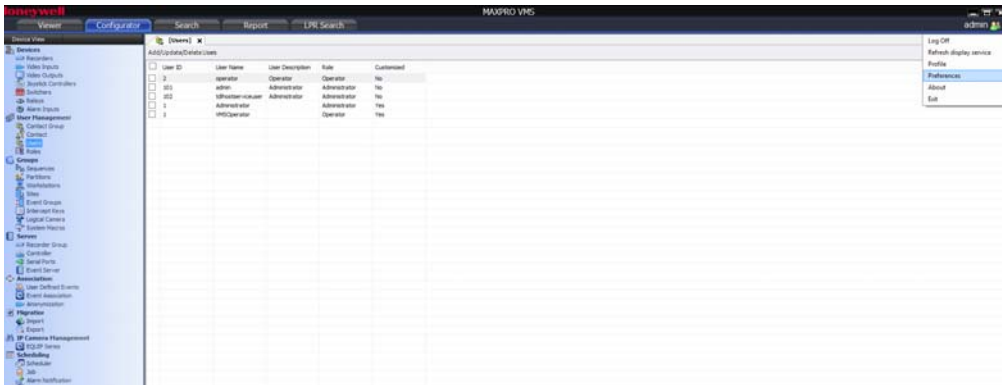
9. Click **Anonymization** in Device List to view all the cameras available.



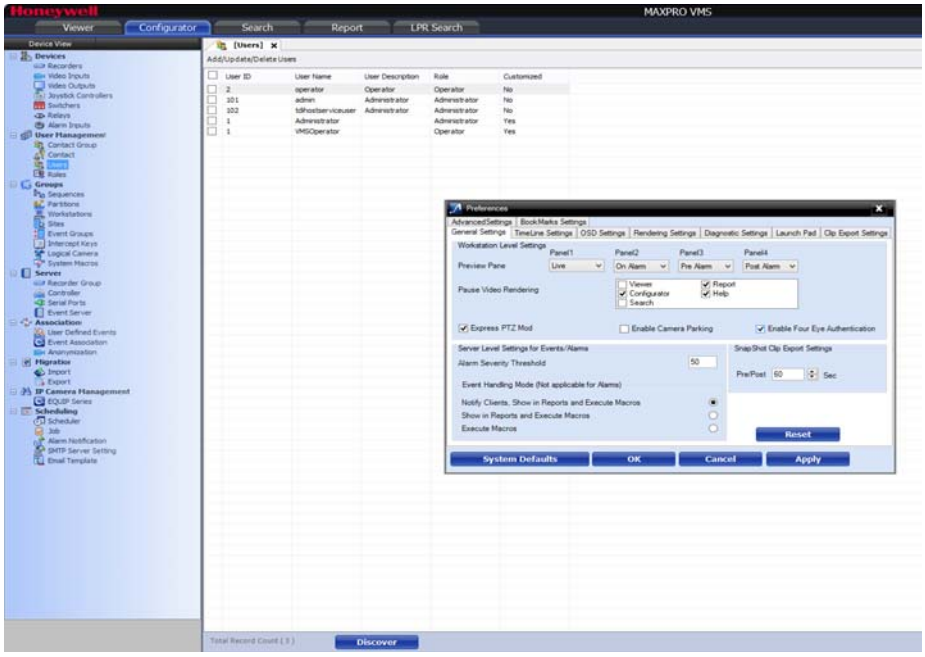
10. Select the **Mask Type** (Blur/Pixelize) and Select all cameras and move to **Associated Devices**.

11. Click **Save** to save the associated list of cameras for face masking.

12. Click the username icon on the top right corner and select **Preferences**.

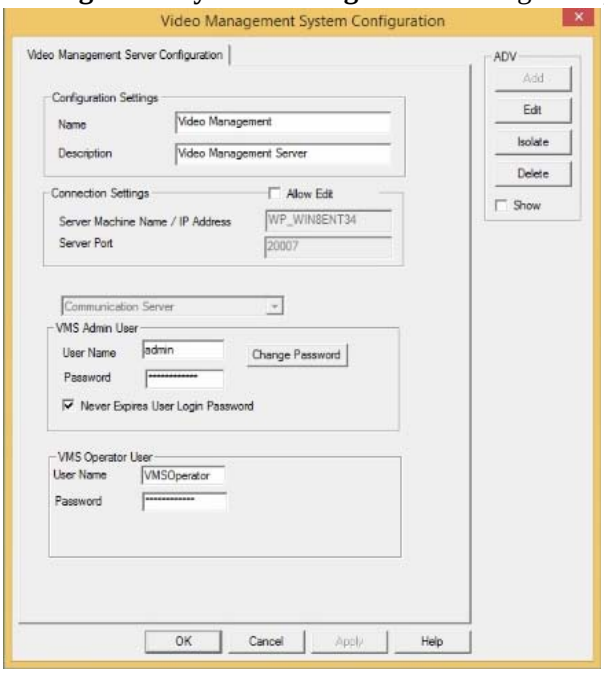


13. In **General Settings** tab, select the **Enable Four-Eye Authentication** check box to enable the Four Eye Authentication.

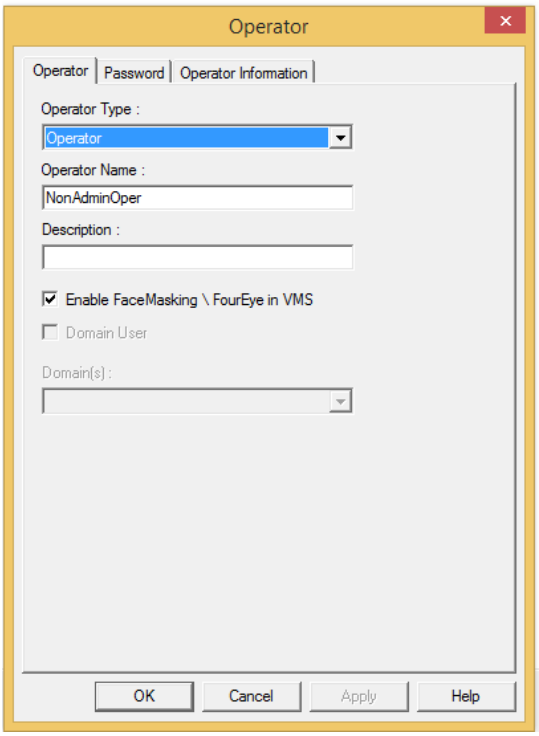


14. Open the WIN-PAK Application and choose **System->ServerConfiguration**.

15. Right-click the **Video Management** and choose **Configure**. The **Video Management System Configuration** dialog box appears.



16. Enter the VMS User credentials for both **VMS Administrator User** and **VMS Operator User**.
17. While creating an Operator in WIN-PAK, select the **Enable FaceMasking \ FourEye in VMS** check box to mask the face in live/recorded video when the operator logs in. If the check box is not selected, the face will not be masked in the live/recorded video.



Four Eye Authentication dialog will be displayed for Non-Administrator operator to view the recored video. Enter the VMS administrator credentials to view the recored video.

Note:

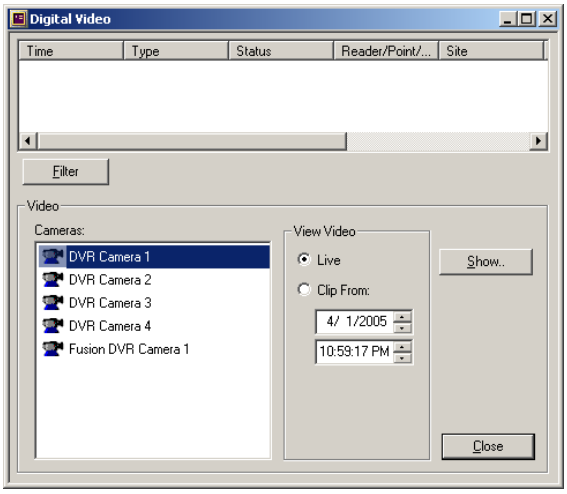
After clicking the **Authenticate** button, close the dialog manually to get the recorded video.

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.



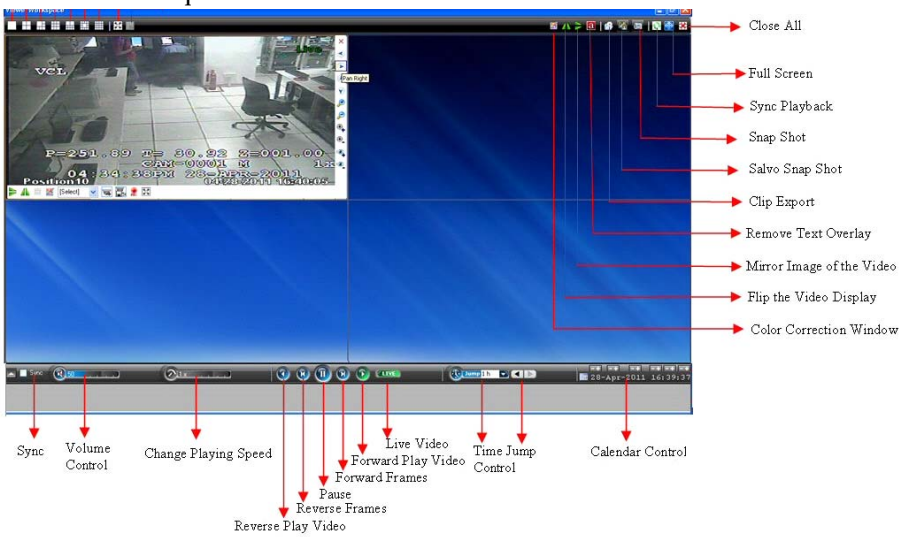
2. Select the cameras in the **Cameras** list. For multiple selections, use the SHIFT or CTRL key.
3. To view live video, click **Live**.

   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.

6. Use the camera controls in the **Viewer Salvo Layout** window to adjust the camera as required.



Icon	Description
	Salvo View.
	Color Correction.
	Flip the video display.
	Mirror image of the video.
	Remove text overlay
	Clip export.

Icon	Description
	Salvo snapshot.
	Snapshot.
	Synch playback.
	Full screen.
	Close All.
	Sync.
	Volume control.
	Change playing speed.
	Reverse play video.
	Reverse frames.
	Pause video.

Icon	Description
	Forward frames.
	Forward play video.
	Live video.
	Time jump.
	Calendar.

Video control options in panel toolbars

The panel toolbars appear when you hover the mouse over the video displayed in a panel. The toolbar that appears on top of a panel enables you to view the name of the video source and close the video display. The toolbar that appears on the bottom and on the right of a panel consists of icons that enable you to perform the following actions.

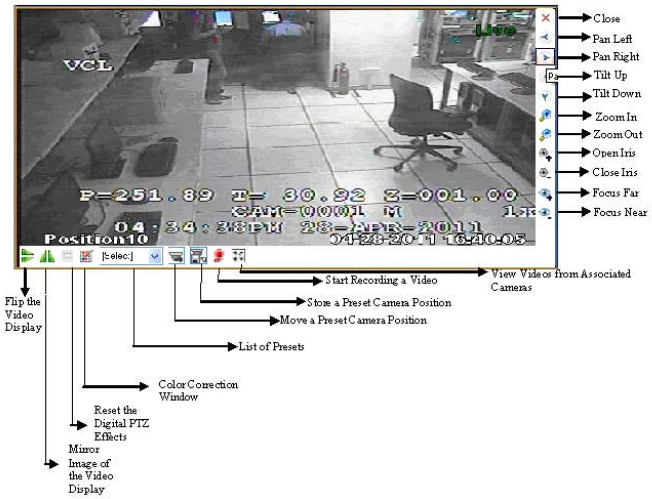


Table 14-5 Video Control Options in Panel Toolbar

Button	Description
	Zoom in to the video.
	Zoom out of the video.
	Flips the video display. Alternatively, you can click this icon in the toolbar on the top of the salvo layout.
	View the mirror image of the video display. Alternatively, you can click this icon in the toolbar on top of the salvo layout.
	Resets the digital PTZ effects on the video display.
	Displays the color correction window. Move the sliders to set the brightness, contrast, hue, and saturation. You can select the Blur check box to blur the video display and the Sharpness check box to increase the image sharpness or clarity. Alternatively, you can click this icon in the toolbar.
	Displays a drop down box of presets. You can select a preset for the camera. Note: The drop down box is disabled when digital PTZ is enabled. You need to disable the digital PTZ feature to select a preset. See "Panning, Tilting, and Zooming" on page 767 for information on enabling and disabling the digital PTZ feature.
	Moves a preset camera position. To move a preset, select a preset number from the drop down list and then click the icon. The camera position (pan, tilt, and zoom) is moved to the selected preset. Note: This icon is disabled when digital PTZ is enabled. You need to disable the digital PTZ feature to move a preset. See "Panning, Tilting, and Zooming" on page 767 for information on enabling and disabling the digital PTZ feature.

Button	Description
	Stores a preset camera position. To store a preset, select a preset number from the drop down list and then click the icon. The camera position (pan, tilt, and zoom) is saved in the selected preset. Note: The icon is disabled when digital PTZ is enabled. You need to disable the digital PTZ feature to move a preset. See "Panning, Tilting, and Zooming" on page 767 for information on enabling and disabling the digital PTZ feature.
	Starts user activated recording. This feature is currently not implemented and is reserved for future releases of WIN-PAK.
	Surrounding cameras. This feature is currently not implemented and is reserved for future releases of WIN-PAK.
	Pan left.
	Pan right.
	Tilt up.
	Tilt down.
	Open iris.
	Close iris.
	Focus far.
	Focus near.

Context menu options

When you right-click on a panel displaying live video, a context menu appears. The following table lists the commands in the context menu.

Command	Click to...
Full Screen	maximize the salvo layout to full screen. Alternatively, you can click  in the toolbar on the top of the salvo layout.
Remove Text Overlay	to remove text overlay displayed on the video. Alternatively, you can click  in the toolbar on the top of the salvo layout.
Digital PTZ	enable digital PTZ. See “Panning, Tilting, and Zooming“ on page 767 for information on digital PTZ.
Save Image	save the frame displayed in the panel as an image in the BMP format. Alternatively, you can click in the toolbar on the top of the salvo layout to save the image in BMP format. See “Saving Images“ on page 768.
Save Image As	save the frame displayed in the panel in different image formats such as JPG, PNG, and GIF. See “Saving Images“ on page 768.

Panning, Tilting, and Zooming

You can pan, tilt, and zoom (PTZ) the video displayed in a panel. You can perform two types of PTZ namely, analog PTZ and Digital PTZ.

Analog PTZ is the panning, tilting, and zooming of PTZ cameras.

Using the digital PTZ feature, you can perform panning and tilting on live and recorded video and clips. The digital PTZ feature when enabled allows you to perform panning and tilting on the video display that is zoomed or enlarged.

Zooming the video display

Use the mouse scroll wheel to enlarge (zoom in) or reduce (zoom out) the video display in the panel. Alternatively, hover the mouse over the video display. A toolbar appears in the lower part of the panel. You can click  to zoom in and  to zoom out the video display.

Panning and Tilting

To perform analog PTZ:

1. Click the **Viewer** tab.
2. Center-click anywhere on the video panel. A point is highlighted.
3. Move the mouse to the preferred location, and then click and hold left mouse button to perform pan and tilt. A arrow appears in the direction where the mouse is being moved.
4. Center-click again to stop panning and tilting.

Note: The digital PTZ must be disabled to use analog PTZ. To disable the digital PTZ feature, click and clear Digital PTZ in the context menu.

5. Click the video display and drag the mouse pointer in the direction to pan or tilt. An arrow appears on the video display indicating the pan or tilt direction.

To perform digital PTZ:

1. Right-click on the video display in a panel. A context menu appears.
2. Select **Digital PTZ**. The digital PTZ feature is enabled for the video display in the panel.
3. Zoom the video display.
4. Center-click anywhere on the video panel. A point along with left, right, up, and down arrows appear.
5. Move the mouse in the required direction to pan and tilt.
6. Center-click again to stop panning and tilting.

Saving Images

While viewing video in the panel, you can save a frame of the video as an image. The image can be saved in Bitmapped Graphics (BMP), Joint Photographic Experts Group (JPG) format, Portable Graphics format (PNG), and Graphics Interchange Format (GIF).

To save a frame displayed in a panel as an image :

1. Click the **Viewer** tab.
2. Right-click the panel to display a context menu.
3. Select Save Image to save the image in .BMP format. Alternatively, you can click  on the toolbar on top of the salvo layout. The images are saved in the **ImagesAndClips** folder at the location in the hard drive in which Video Management Server files are installed. For example, **X:\Program Files\WIN-PAK PRO\Honeywell\TrinityFramework\ImagesAndClips**. Here, **X:** is the hard drive.

   OR

   Select S**ave Image As** to save the image in other formats. The **Save As** dialog box appears when you select the Save Image As command. You can select the format in the **Save As Type** box and type the name for the image in **File Name** box. You can also select a folder to save the image.

To save the salvo layout as an image

- Click  on the toolbar on top of the salvo layout.

The salvo layout is saved as an image (.BMP format) in the **ImagesAndClips** folder.

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 lower portion of the live video display.

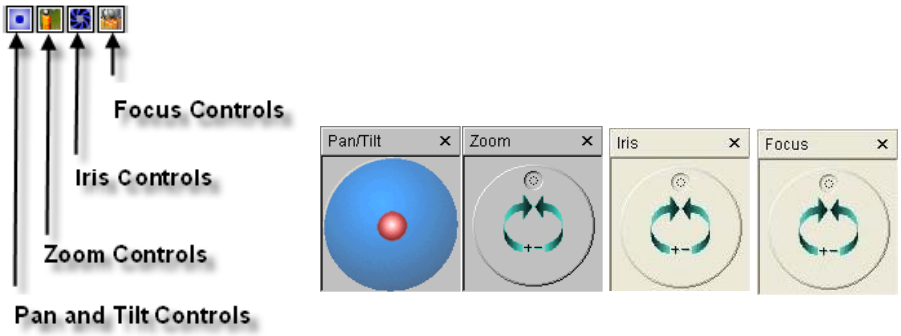
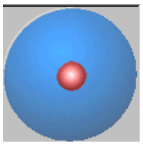


Figure 14-3 Depicting camera controls on the live digital video display

The following table describes the control buttons on the live digital video display:

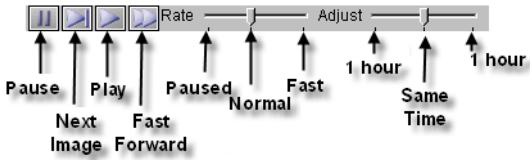
Table 14-6 Describing control buttons on the Live Monitor window

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 14-7 Describing the Live Video Display control options

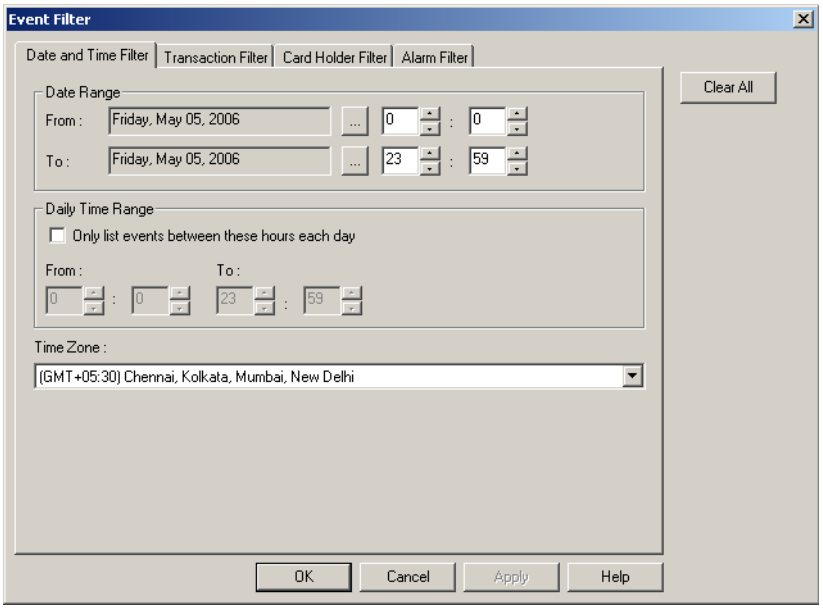
Control Option	Description
Show Title	The title bar displays the ADV name and the status icon. By default it is selected.
Show Controls	The camera controls are available in the live video display. By default it is selected.
Auto Focus	Camera automatically focuses on subject, provided it is an auto-focus 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

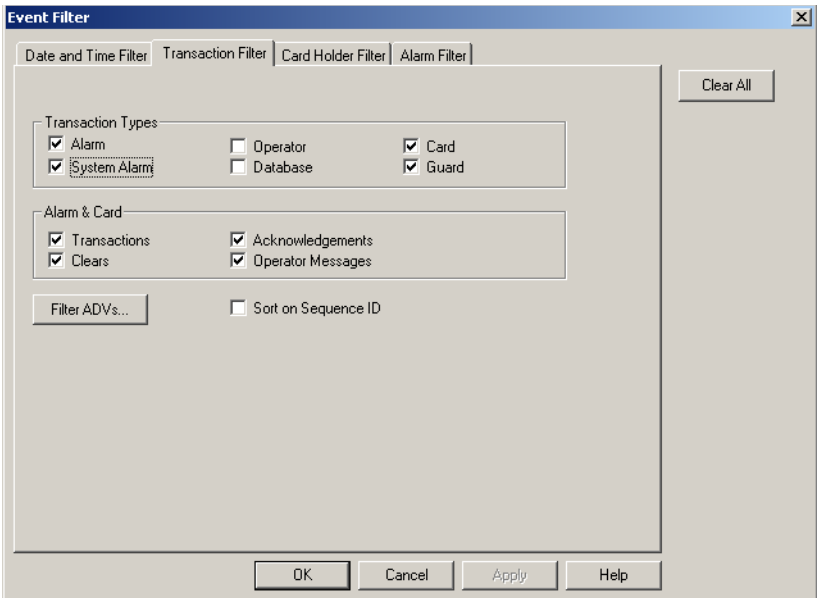
The filter option in the Digital Video window helps you to view the events for a specific period. Therefore, it enables you to retrieve the digital video that is associated to an ADV, which is configured for an auto pop-up display. For example, you may want to view the events from March 15, 2005 to April 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 14-8 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 14-9 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.

Table 14-9 Describing the alarm and card options for filtering video display

Card Option	Description
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

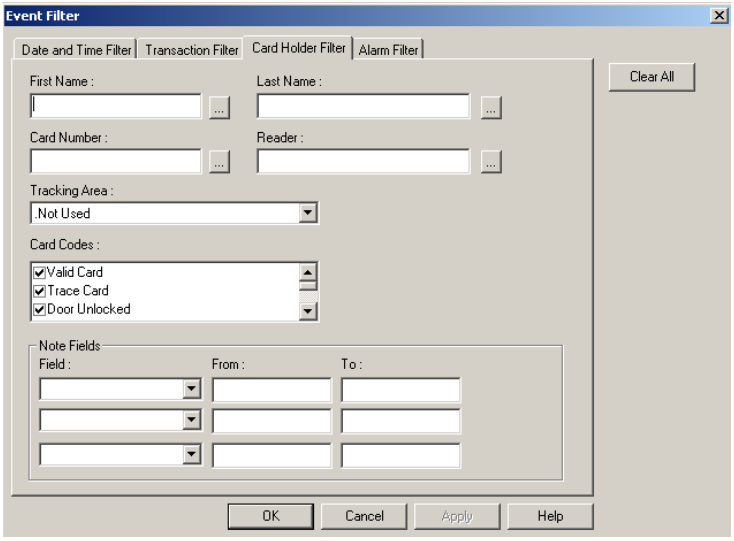
OR

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.

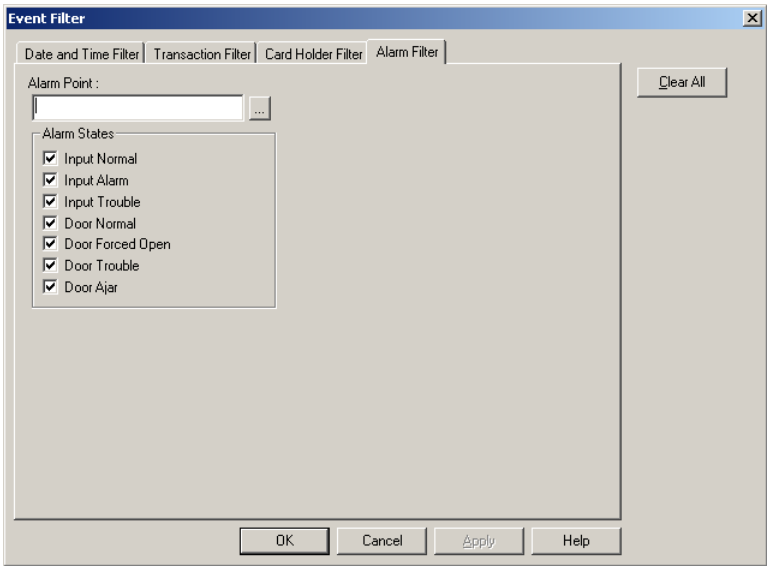
d. To display the video of the card holders accessing a specific area, select an area in the **Tracking Area** list that is configured in Tracking and Mustering Area.

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

15

In this chapter...

This chapter describes about the Introduction to Translation, and Language Configuration in WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
Language Configuration: Adding or Editing Language Information, page 778	✓	✓
Language Configuration: Selecting a language for translation, page 780	✓	✓
Language Configuration: Adding or editing entries for translating Dialogs, Menus, and Other Text, page 781	✓	✓

Introduction

WIN-PAK CS/SE/PE 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 CS/SE/PE user interface. The text files for French, German, Dutch, Italian, English, Simplified Chinese, and Traditional Chinese languages are available by default in the **WIN-PAK\Language Files** folder of WIN-PAK CS/SE/PE.

Translating WIN-PAK CS/SE/PE User Interface involves:

1. Adding a new language with its text and help files into the **WIN-PAK\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 CS/SE/PE is designed to work with U.S. English operating systems. Therefore, a special version of WIN-PAK CS/SE/PE 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 CS/SE/PE and its details cannot be edited.

Adding or Editing Language Information

You can add a new language for translation by providing the following information:

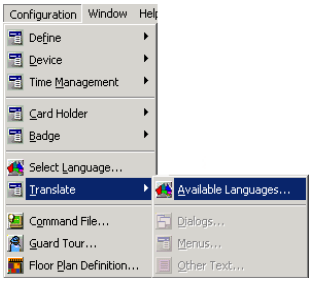
- the language name
- the language text file
- the language help file

Note: Before adding a language, ensure that the language text file and help file (chm) are present in the **WIN-PAK\Language Files** folder.

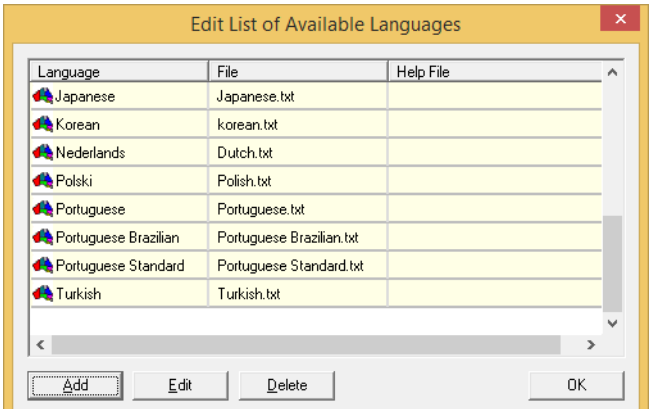
Adding a New Language

Note: Honeywell recommends you to contact its support center for creating language text files.

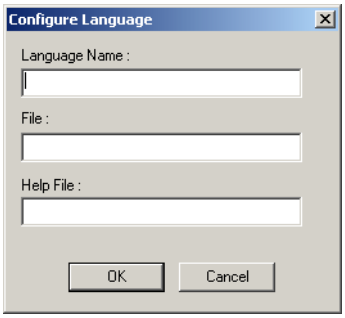
1. Choose **Configuration > Translate > Available Languages**.



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 **WIN-PAK\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 **WIN-PAK\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.

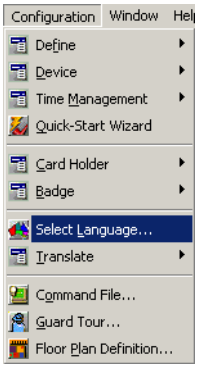
Selecting a language for translation

You can select a language for translating the WIN-PAK CS/SE/PE user interface. When a language is selected, the WIN-PAK CS/SE/PE user interface is translated based on the entries in the language text file.

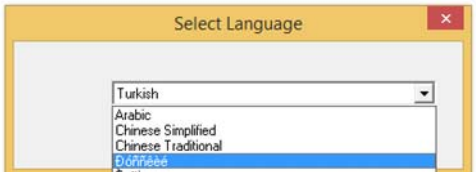
In addition, you can set the language for operators using the **Operator** option in the **System** menu. The WIN-PAK CS/SE/PE user interface is translated to the language of the operator who logs on to WIN-PAK CS/SE/PE.

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 CS/SE/PE 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 section Selecting a language for translation of 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.

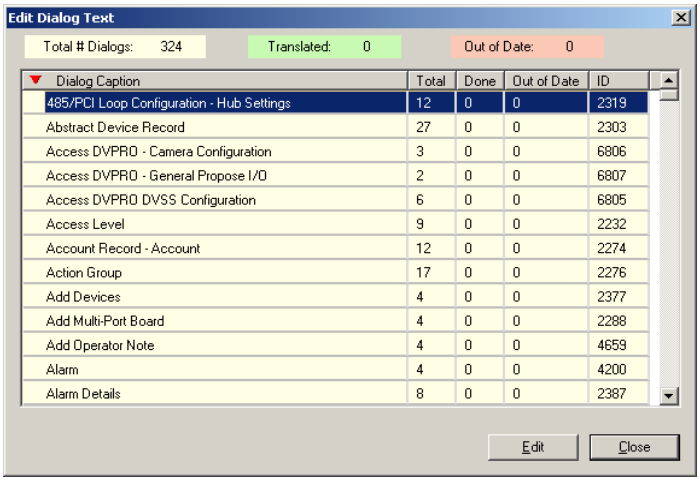
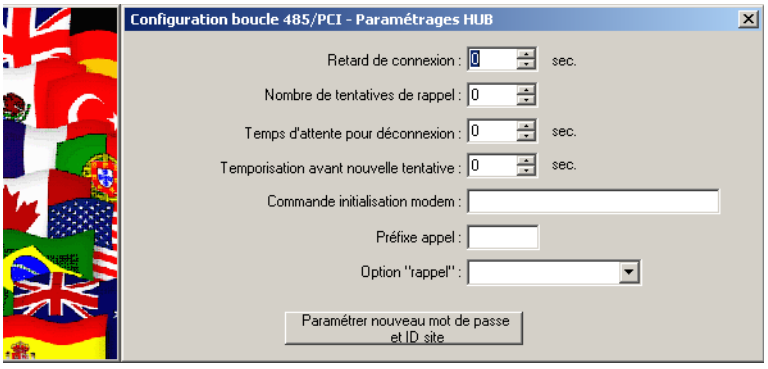


Table 15-1 Edit Dialog Text - Elements and Descriptions

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 CS/SE/PE (applies only to a WIN-PAK CS/SE/PE upgrade.)
Dialog Caption	The caption of the dialog box.

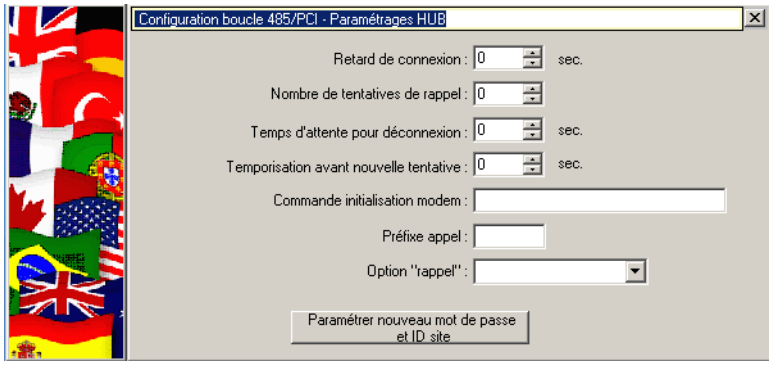
Field/Column	Description
Total	The total number of fields in the dialog box.
Done	The number of fields that has been translated in the dialog box.
Out of Date	The number of fields that were translated in this dialog box in the previous version of WIN-PAK CS/SE/PE (applies only to a WIN-PAK CS/SE/PE upgrade.)
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.

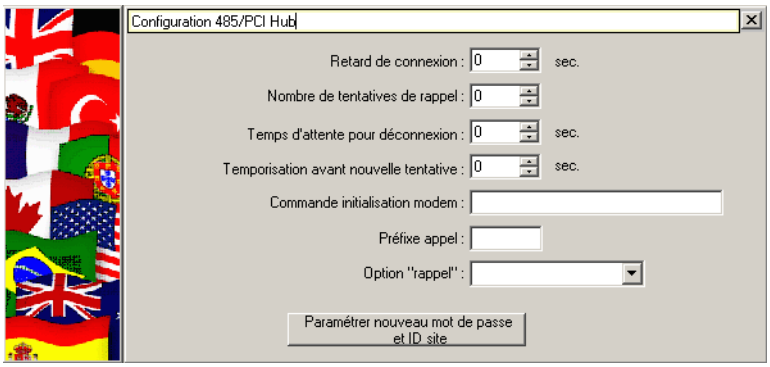


3. Click the field you want to edit. The field name is highlighted.

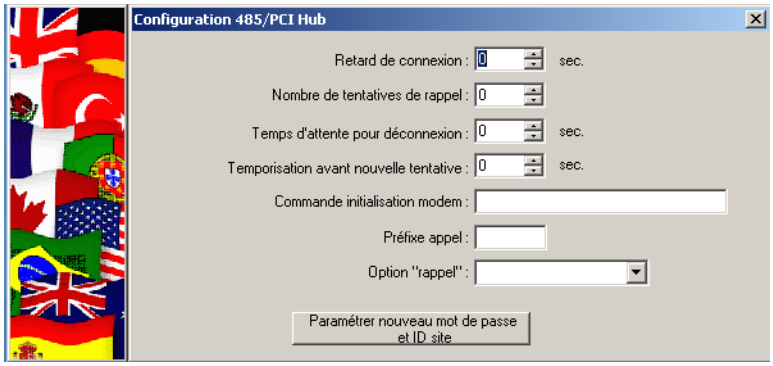
Note: To change the title of the dialog box, click the title and edit the dialog box.



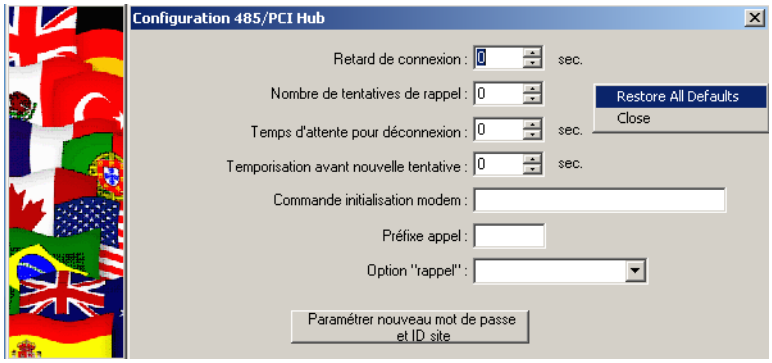
4. Type the text in the highlighted area.



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.

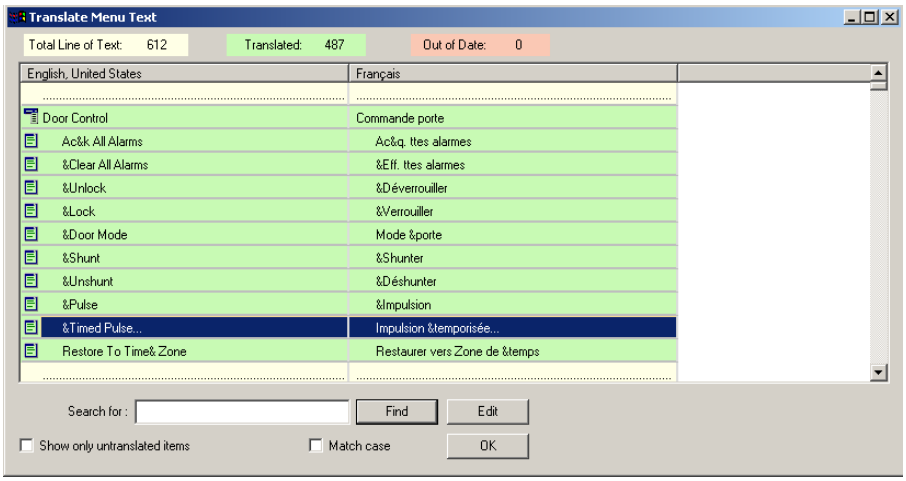


Table 15-2 Translate Menu Text - Elements and Description

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 CS (applies only to a WIN-PAK CS upgrade.)
English, United States	The menu captions in the original language of WIN-PAK CS.
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.

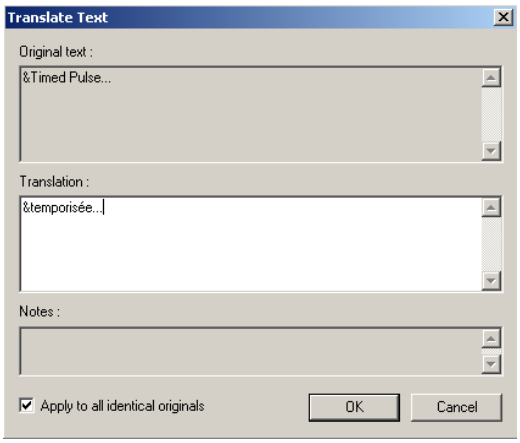
Note: To search for the menu item in a scrolling list:

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.

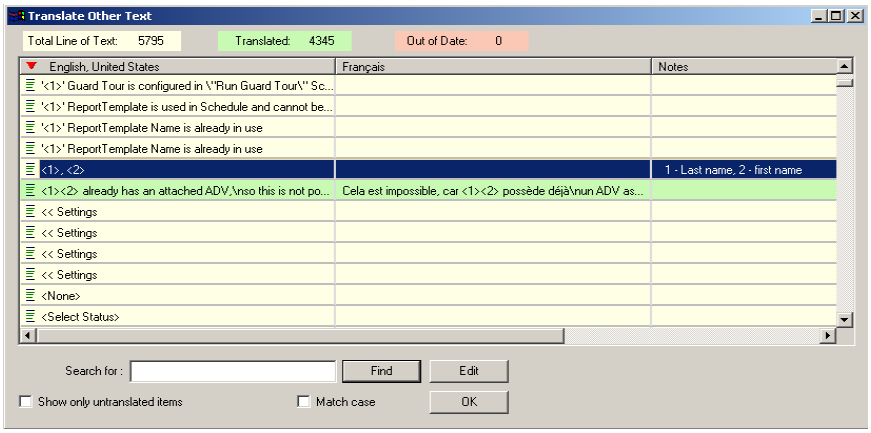


Table 15-3 Translate Other Text Options

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 CS/SE/PE (applies only to a WIN-PAK CS/SE/PE upgrade.)
English, United States	The text in the original language of WIN-PAK CS.
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.

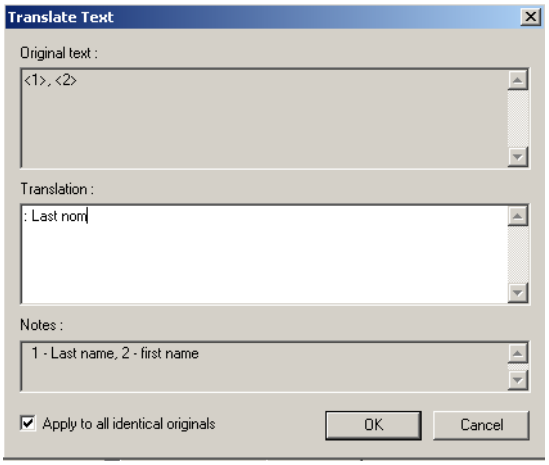
Note: To search for the text item in a scrolling list:

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.

Configuration

16

In this chapter...

This chapter describes about the Configuration in WIN-PAK.

Introduction

Overview

This section describes the basic configuration details of managing the time and assigning duties to several employees.

You can configure the following for an employee.

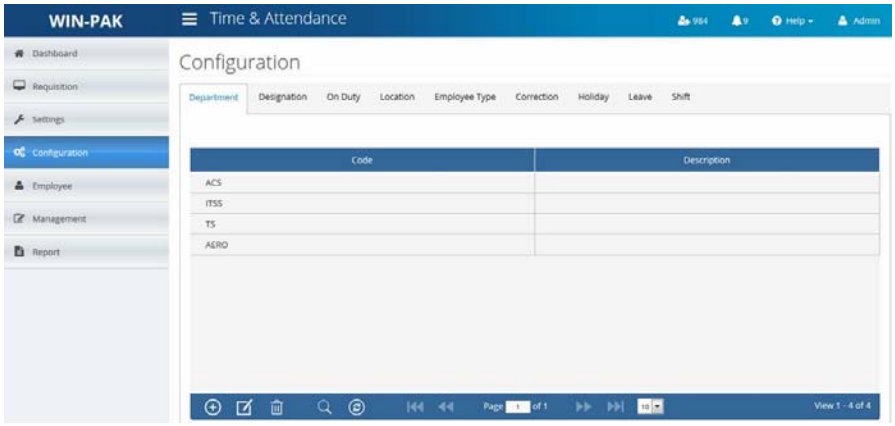
- Department
- Designation
- On Duty
- Location
- Employee Type
- Correction
- Holiday
- Leave
- Shift

Department

The **Department** tab displays the details of all the departments under which the employees are working.

To configure the department:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Department** tab. A list of all the available departments are displayed.

3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-1 List of icons appearing on the lower pane

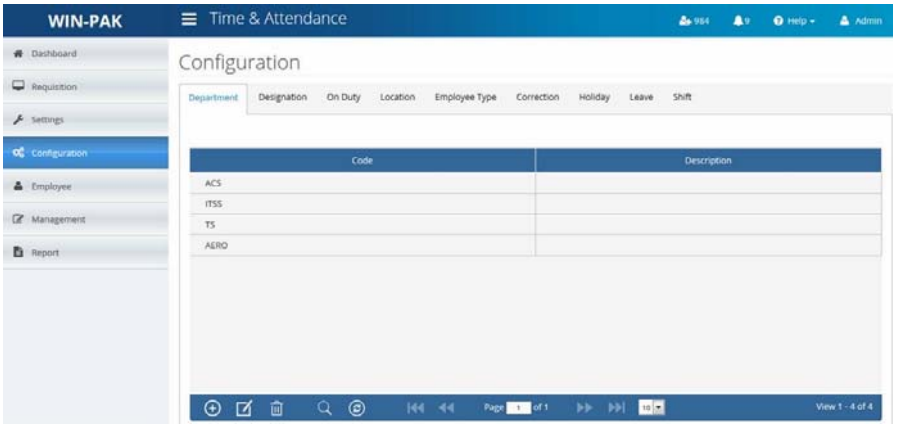
Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.
	Delete the selected record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Designation

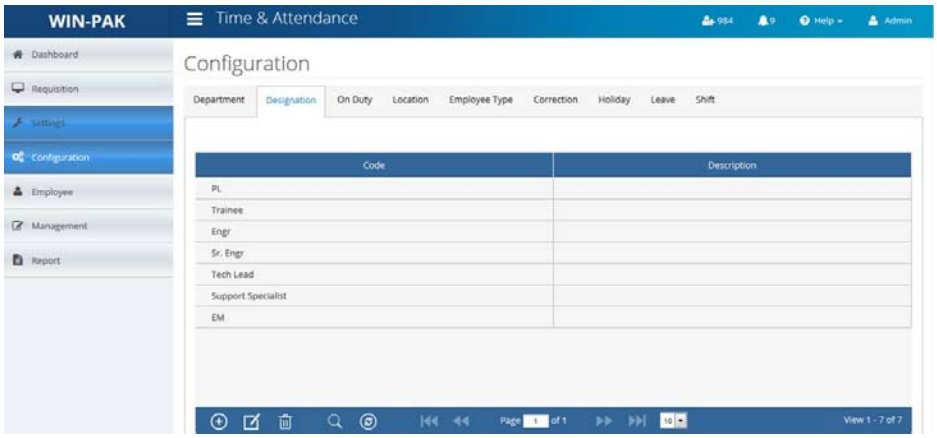
The **Designation** tab displays the details of the designation assigned to employees in the company.

To configure the designation:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Designation** tab. A list of all the available designations are displayed.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-2 List of icons appearing on the lower pane

Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.
	Delete the selected record.

Table 16-2 List of icons appearing on the lower pane

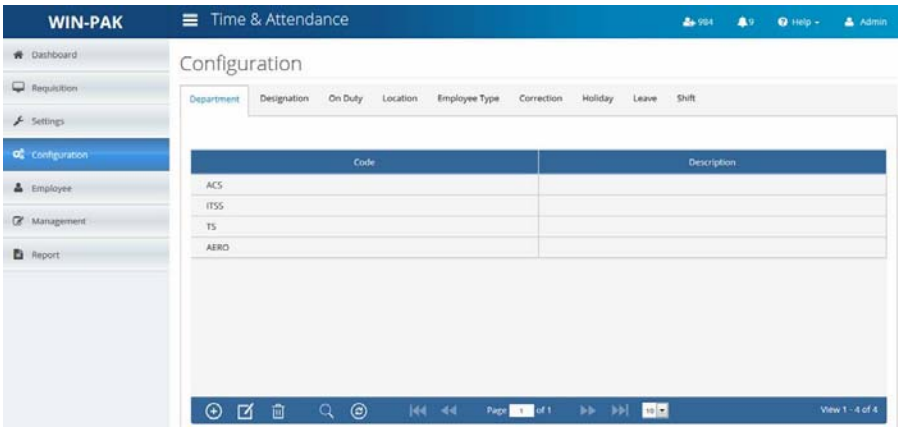
Icons	Click to...
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

On Duty

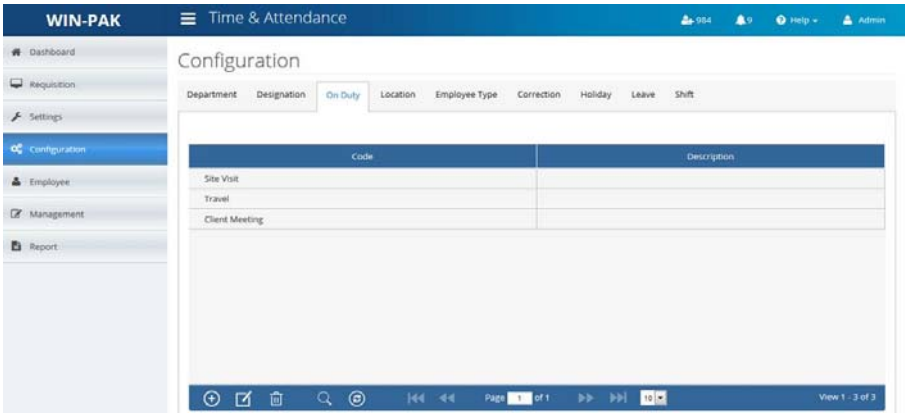
The **On Duty** tab displays the details of the details of on duty application status.

To configure the on duty details:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **On Duty** tab. Details of on duty application is displayed.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-3 List of icons appearing on the lower pane

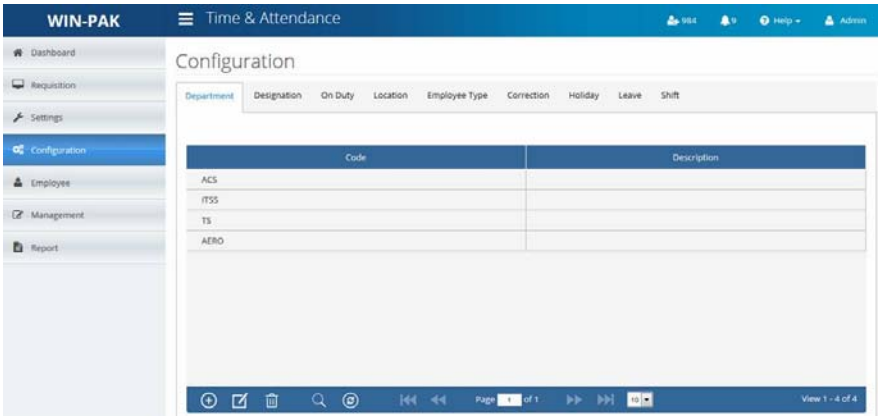
Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.
	Delete the selected record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Location

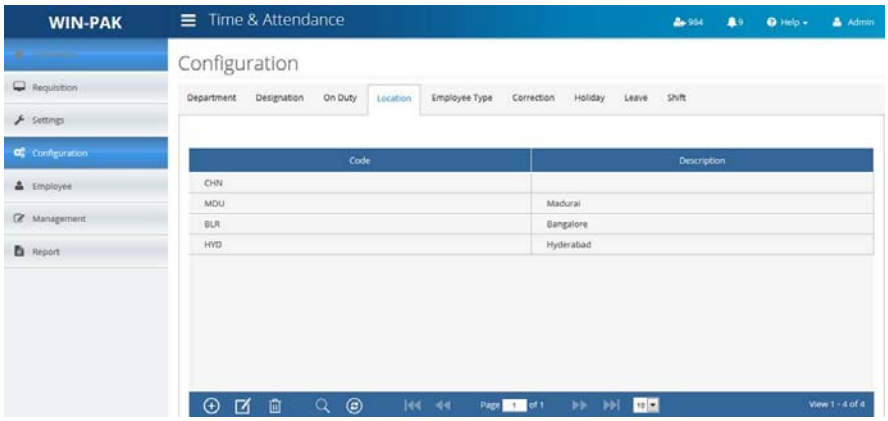
The **Location** tab displays the location details of where the company is situated.

To configure the location details:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Location** tab. Displays the location details of where the company is situated.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-4 List of icons appearing on the lower pane

Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.
	Delete the selected record.

Table 16-4 List of icons appearing on the lower pane

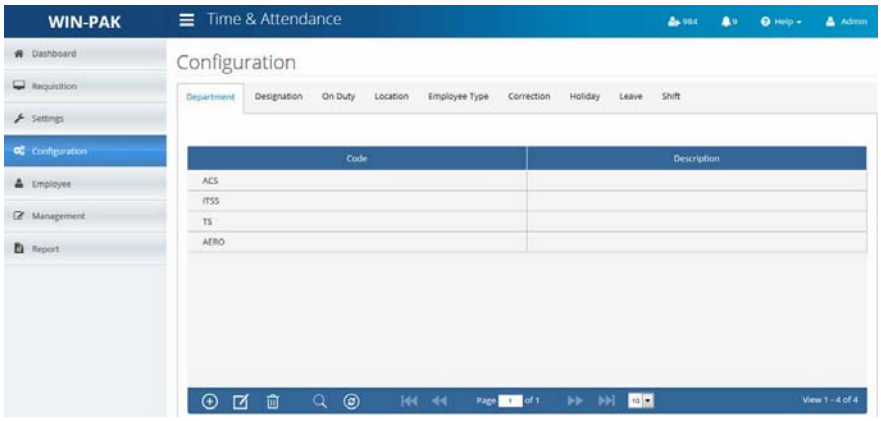
Icons	Click to...
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Employee Type

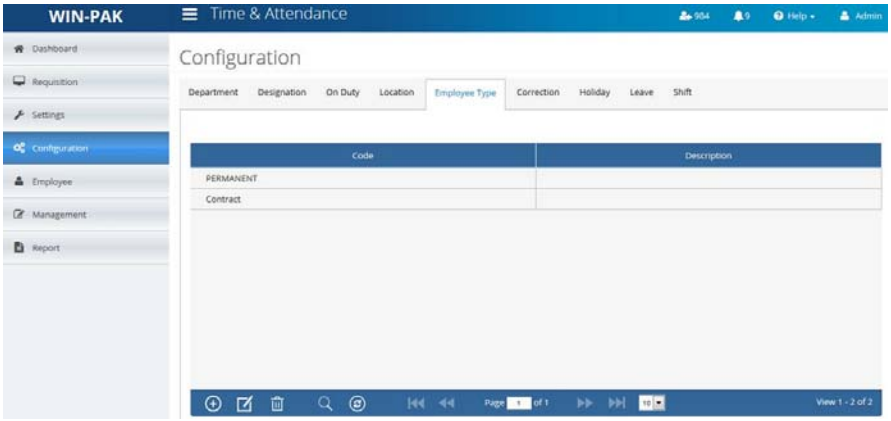
The **Employee Type** tab displays the details of all types of employees in the company.

To configure the employee type details:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Employee Type** tab. Displays the details of all types of employees in the company.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-5 List of icons appearing on the lower pane

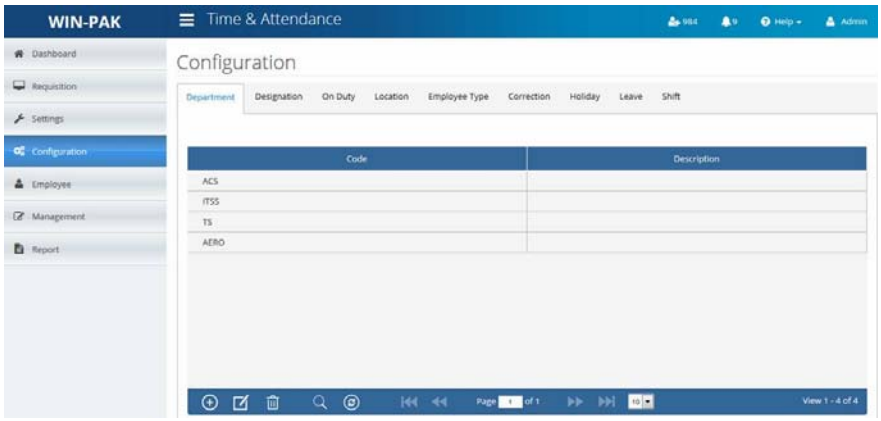
Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.
	Delete the selected record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Correction

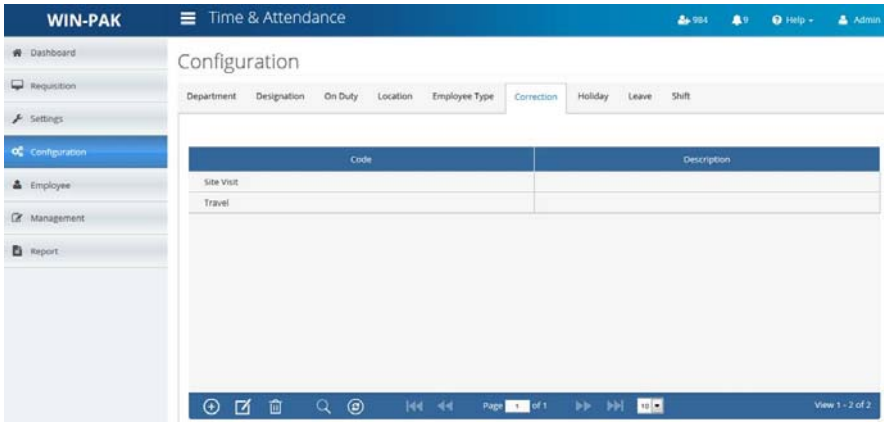
The **Correction** tab displays the list of corrected time and attendance.

To configure the correction details:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Correction** tab. Displays the list of corrected time and attendance.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-6 List of icons appearing on the lower pane

Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.

Table 16-6 List of icons appearing on the lower pane

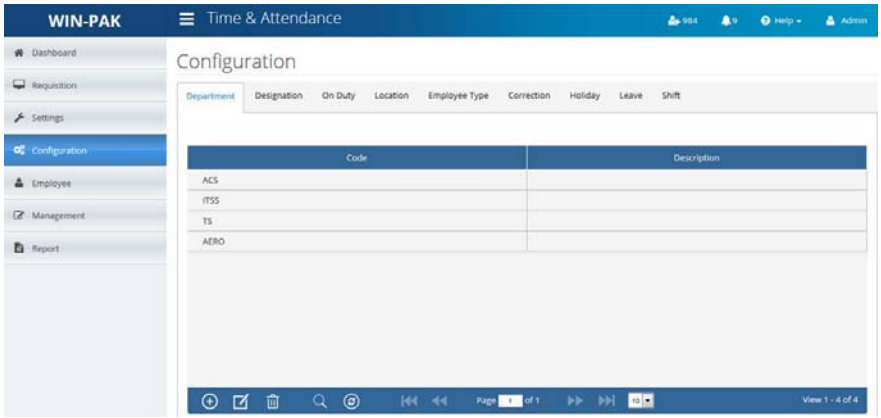
Icons	Click to...
	Delete the selected record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Holiday

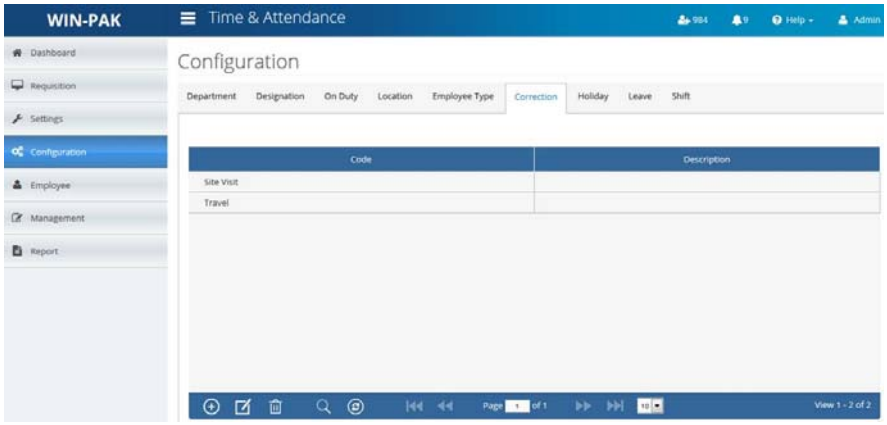
The **Holiday** tab displays the details of holidays declared by the company.

To configure the holiday details:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Holiday** tab. Displays the details of holidays declared by the company.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-7 List of icons appearing on the lower pane

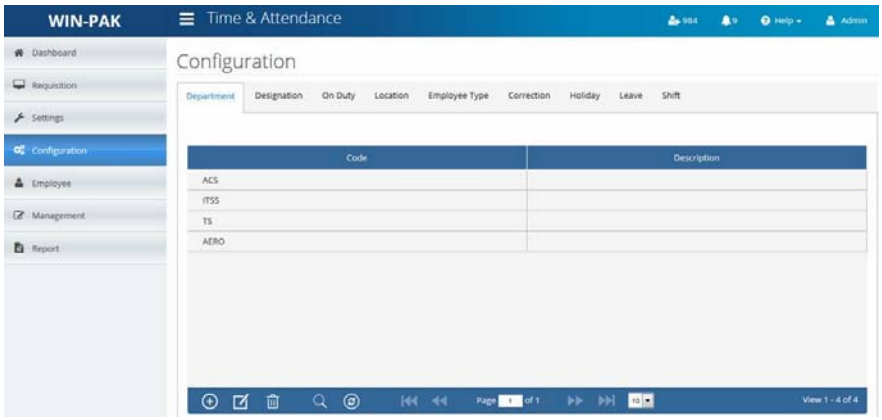
Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.
	Delete the selected record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Leave

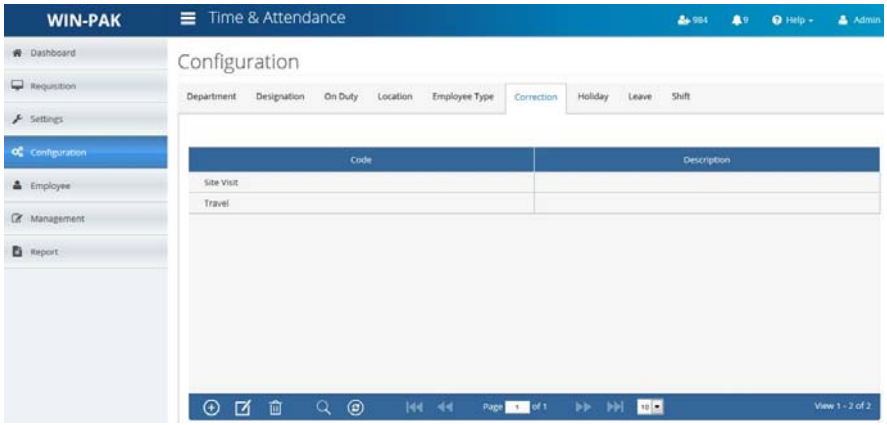
The **Leave** tab displays the location based leave details, allocated to employees.

To configure the leave details:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Leave** tab. Displays the location based leave details, allocated to employees.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-8 List of icons appearing on the lower pane

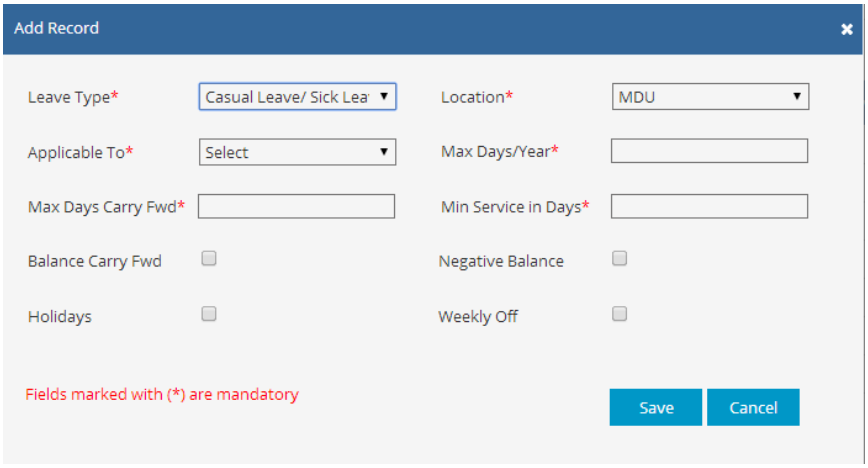
Icons	Click to...
	Add a new record, along with a description.

Table 16-8 List of icons appearing on the lower pane

Icons	Click to...
	Edit an existing record.
	Delete the selected record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

To add a new leave record:

1. In the **Leave** tab, click the  icon at the lower pane of the page. The **Add Record** page appears.



2. View/edit the following details.

Table 16-9 Add a new leave record

Setting	Description
Leave Type	From the drop-down list, select the type of leave from the following list: Casual Leave/Sick Leave Earned Leave Loss Of Pay Maternity Leave Paternity Leave
Location	From the drop-down list, select the employee location.
Applicable To	From the drop-down list, select the gender as applicable. For example, if the selected **Leave Type** is **Earned Leave**, select the **Applicable To** option as **Both**.
Max Days/Year	Type the maximum number of days an employee is eligible to avail leave, in a year.
Max Days Carry Forward	Type the maximum number of days an employee is eligible to carry forward his leaves to the next year.
Min Service in Days	Type the minimum number of days after which the employee is eligible to apply leave.
Balance Carry Forward	Select to enable carry forward of balance leaves to next year.
Negative Balance	Select to enable the employee to apply for leaves, even if the leave balance is nil.
Holidays	Select to enable inclusion of holidays as part of the leave availed by the employee.
Weekly Off	Select to enable inclusion of weekly off as part of the leave availed by the employee.

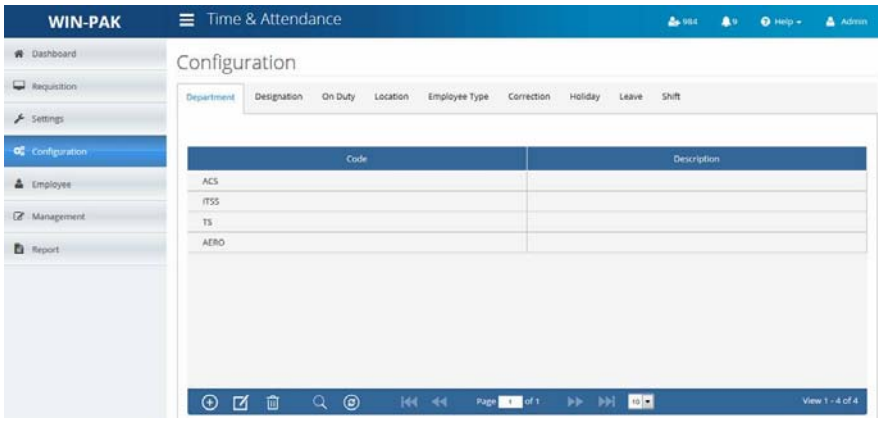
3. Click **Save**.

Shift

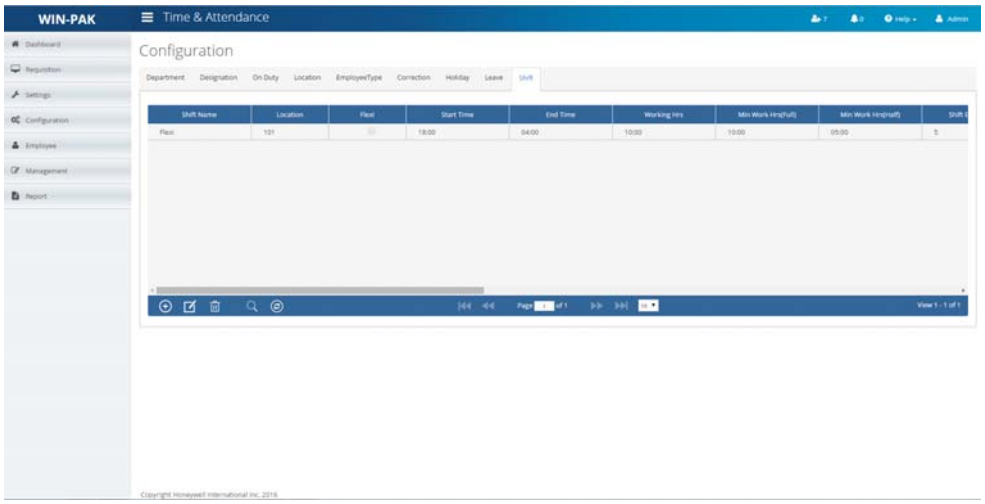
The **Shift** tab displays the location based shift details, allocated to employees.

To configure the shift details:

1. Click **Configuration** on the left pane. The **Configuration** page appears.



2. Click the **Shift** tab. Displays the location based shift details, allocated to employees.



3. To add, edit, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 16-10 List of icons appearing on the lower pane

Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.

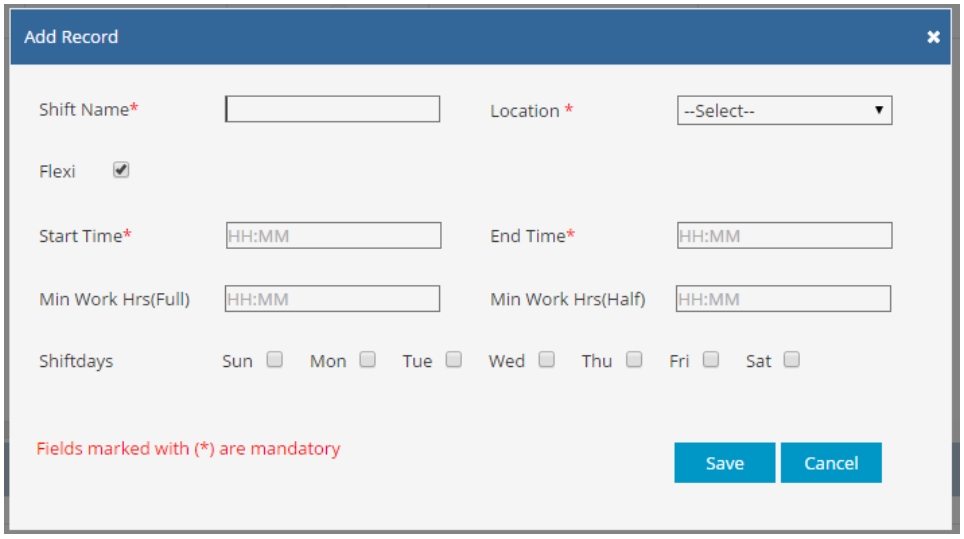
Table 16-10 List of icons appearing on the lower pane

Icons	Click to...
	Delete the selected record. If the shift is already associated with more than one employee, use the **Shift Allocation** option to assign another shift to the selected employee and delete the selected record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

To add a new flexi shift record:

Note: You must ensure to allocate all the employees to a shift.

1. In the **Shift** tab, click the  icon at the lower pane of the page. The **Add Record** page appears.



2. Provide the following details.

Table 16-11 Add a new flexi shift record

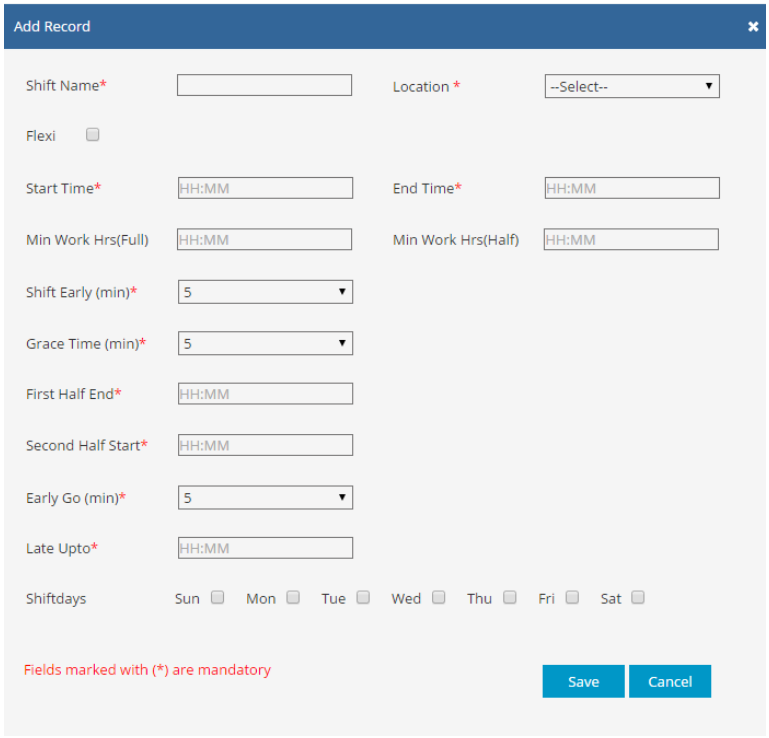
Setting	Description
Shift Name	Type a name for the specified shift.
Location	From the drop-down list, select the employee location.
Start Time HH:MM	Type the shift start time (hh:mm). For example, the time slot begins at 09:00.
End Time HH:MM	Type the shift end time (hh:mm).
Flexible Time	Select if the flexible shift hours are applicable to employee, instead of regular shifts.
Min Work Hrs (Full) HH:MM	Type the minimum work hours an employee must be present in the premises, for full day.
Min Work Hrs (half) HH:MM	Type the minimum work hours an employee must be present in the premises, for half a day.
Weekdays	You can either select all days of the week or a specific day in the week.

3. Click **Save**.

To add a new non-flexi shift record:

Note: You must ensure to allocate all the employees to a shift.

1. In the **Shift** tab, click the icon at the lower pane of the page. The **Add Record** page appears.



2. Provide the following details.

Table 16-12 Add a new non-flexi shift record

Setting	Description
Shift Name	Type a name for the specified shift.
Location	From the drop-down list, select the employee location.
Start Time HH:MM	Type the shift start time (hh:mm). For example, the time slot begins at 09:00.
End Time HH:MM	Type the shift end time (hh:mm).
Flexible Time	Select if the flexible shift hours are applicable to employee, instead of regular shifts.
Min Work Hrs (Full) HH:MM	Type the minimum work hours an employee must be present in the premises, for full day.
Min Work Hrs (half) HH:MM	Type the minimum work hours an employee must be present in the premises, for half a day.

Table 16-12 Add a new non-flexi shift record

Setting	Description
Shift Early (min)	From the drop-down list, select the time (in minutes) by which the employee is allowed to arrive early and start work before the shift starts. For example, from the **Shift Early** drop-down list, if you have selected the value as **60** and the **Shift Starts** at **09:00** then, the system calculates **08:00** as **Min Early Time**.
Grace Time (min)	From the drop-down list, select the time by which the employee is allowed to arrive late once the shift starts. For example, from the **Grace Time** drop-down list, if you have selected the value as **5** and the **Shift Starts** at **09:00** then, the system calculates **09.05** as **Grace Time**.
First Half End HH:MM	Type the time when the first half of the day ends. For example, if you enter the **First Half End** time slot as 04:00 and if the **Start Time** as 09:00 then, the system calculates 09:00 +04:00 =13:00 as the **First Half End**.
Second Half Start HH:MM	Type the time when the second half of the day starts. For example, if you enter the **Second Half Start** time slot as 04:30 and if the **Start Time** as 09:00 then, the system calculates 09:00 +04:30 =13:30 as the **Second Half Start**.
Early Go (min)	From the drop-down list, select the time (in minutes) for which the employee is allowed to leave the company before the shift ends. For example, from the **Early Go** drop-down list, if you have selected the value as **5** and the **Shift Ends** at **18:00** then, the employee can leave the premises 5 minutes before the shift ends.
Late Upto (Hrs)	From the drop-down list, select the maximum hours the employee can work. For example, if the **Late Upto** (hh:mm) is set to **01:00** and the **Shift End** is set to **18:00** then, 1 hour of work will be considered as overtime.
Weekdays	You can either select all days of the week or a specific day in the week.

3. Click **Save**.

For more details, see the below table that shows the examples for flexi and non-flexi shift records.

Flexi Shift	
Shift Start	9:00
Shift End	18:00
Min.Hrs. Full Day	4:00
Min.Hrs. Half Day	8:00
Attendance Status for Flexi Shift:	
Present	Only if his working hr for Min hrs for Full day ie 08:00 hrs
Half Day Absent	Only If his working hr for >= Min hrs for Half day and < Min hrs for Half day
Absent	If his working hr < Min hr for Half Day

Non Flexi Shift (Day Cross)		
	Value to Enter	Calculative Value
Shift Early (min)	0:05	20:55, 01:25
Shift Start	21:00	21:00
Shift End	6:00	6:00
Min.Hrs. Half Day	4:00	1:00
Min.Hrs. Full Day	8:00	5:00
Grace Time (min)	0:05	21:05:00 , 01:35:00
First Half End	4:00	1:00
Second Half Start	4:30	1:30
Early Go (min)	0:05	5:55:00
Late Upto	1:00	7:00:00 AM
Attendance Status for Non Flexi shift:		
Present	Only if his working hr for Min hrs for Full day ie 08:00 hrs	
FHA	Only If his working hr for >= Min hrs for Half day and < Min hrs for Half day	
SHA	Only If his working hr for >= Min hrs for Half day and < Min hrs for Half day	
Absent	If his working hr < Min hr for Half Day	

Employees

17

In this chapter...

This chapter describes about the Employees in WIN-PAK.

Introduction

Overview

This section displays the employee details and enables you to manage time and attendance of several employees.

You can configure the following:

- New employee
- All employee

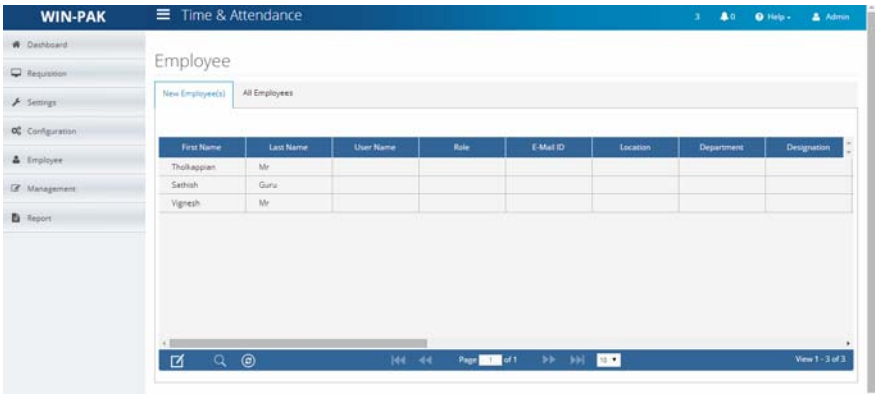
New Employee

The **New Employee** tab displays the employee details such as, user name, first and last name, role, and so on.

Note: You can only edit an existing employee. To add or delete a new employee, you must use the WIN-PAK SE/PE application.

To edit an employee:

1. Click **Employee** on the left pane. The **Employee** page appears.



2. To edit, search, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 17-1 List of icons appearing on the lower pane

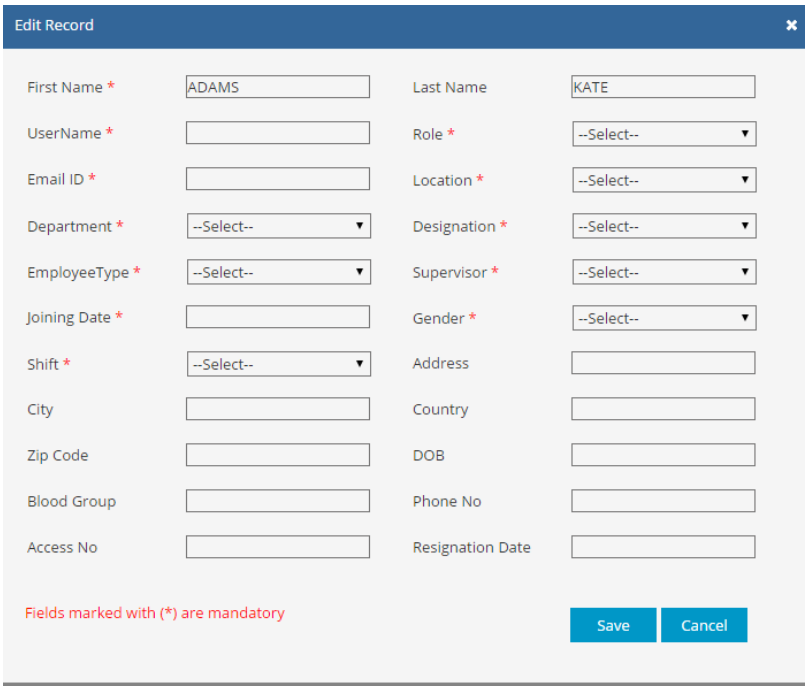
Icons	Click to...
	Edit an existing record.
	Search based on selected criteria.

Table 17-1 List of icons appearing on the lower pane

Icons	Click to...
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

To edit an employee record:

1. In the **New Employee(s)** or **All Employees** tab, click the icon at the lower pane of the page. The **Edit Record** page appears.



2. View/edit the following details.

Note: Ensure to log on with the admin credentials to edit the employee record.

Table 17-2 Edit a employee record

Setting	Description
FirstName	Displays the first name of the employee.

Table 17-2 Edit a employee record

Setting	Description
LastName	Displays the last name of the employee.
UserName	Displays the user name defined by the employee.
Role	From the drop-down list, select the employee role.
Email Id	Type the e-mail address of the employee.
Location	From the drop-down list, select the employee location.
Department	From the drop-down list, select the department in which the employee is working.
Designation	From the drop-down list, select the designation for the employee.
Employee Type	From the drop-down list, select the employee type.
Supervisor	From the drop-down list, select the supervisor for the employee.
Joining Date	Select the employee joining date in the month, date, and year format.
Gender	From the drop-down list, select the gender of the employee.
Shift	From the drop-down list, select the shift of the employee. By default, all the new employees are associated to a shift for a month. After a period of 30 days, the supervisor must again associate the employee to a shift.
Address	Type the address of the employee.
City	Type the city of the employee.
Country	Type the country of the employee.
Zip Code	Type the city zip code of the employee.
DOB	Type the date of birth of the employee.
Blood Group	Type the blood group to which the employee belongs.
Phone No	Type the phone number of the employee.
Access No	Type the access card number.

Table 17-2 Edit a employee record

Setting	Description
Resignation Date	Select the employee resignation date in the month, date, and year format.

3. Click **Save**.

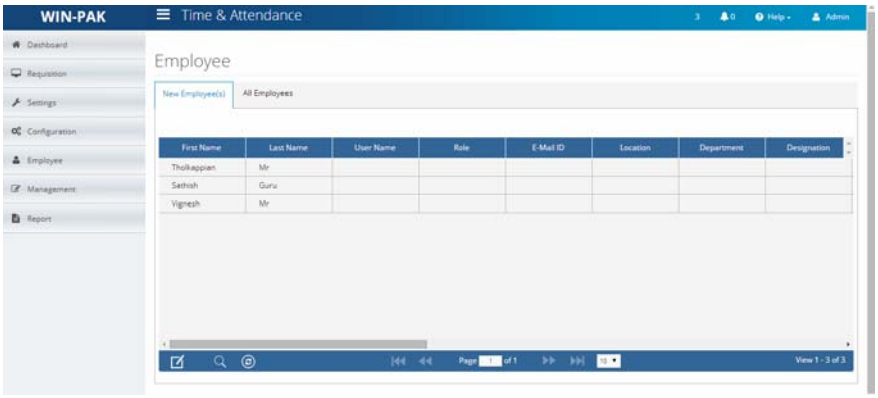
All Employee

The **All Employee** tab displays the employee details such as, User name, first and last name, role, and so on.

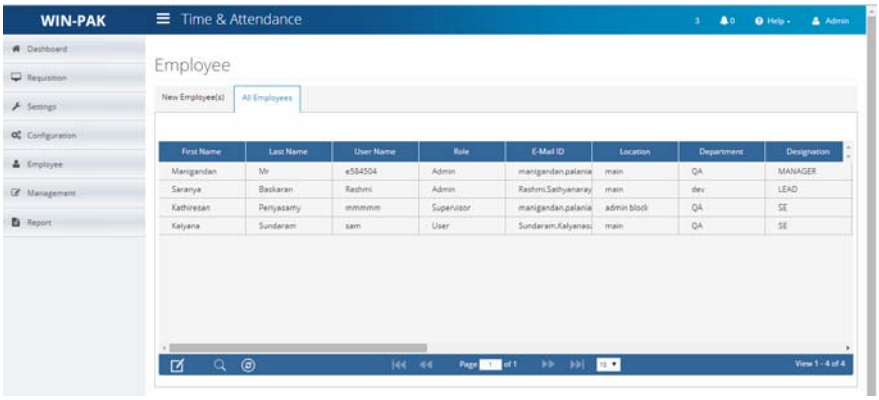
Note: You can only edit an existing employee. To add a new employee, you must use the WIN-PAK SE/PE application.You can only edit an existing employee. To add a new employee, you must use the WIN-PAK SE/PE application.

To edit all employees:

1. Click **Employee** on the left pane. The **Employee** page appears.



2. Click the **All Employee** tab.



Note: After a new employee is added, a welcome mail is generated from the T&A application, which includes information such as the user name, password, and the Website URL. You can use the user login credentials to access the T&A application.

3. To edit, search, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 17-3 List of icons appearing on the lower pane

Icons	Click to...
	Edit an existing record.
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Management

18

In this chapter...

This chapter describes about the Management in WIN-PAK.

Introduction

Overview

This section describes the basic configuration details of managing shift allocation and shift rotation. You can also update the supervisor on the changes.

You can configure the following:

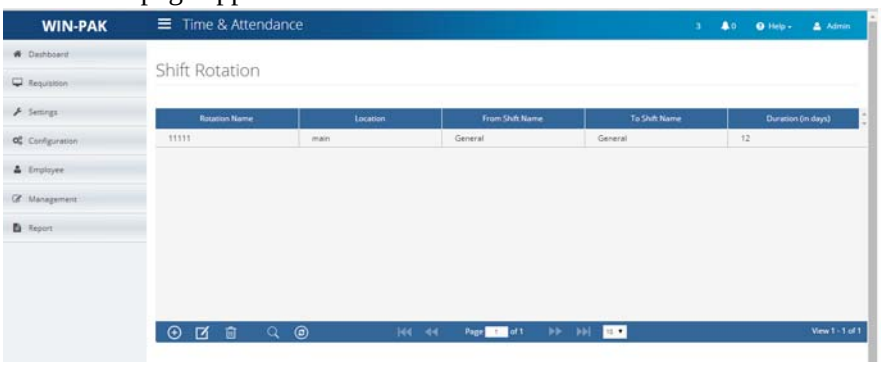
- Shift rotation
- Update supervisor
- Report schedule
- Shift allocation

Shift Rotation

The **Shift Rotation** page displays the rotation name, location, from shift name, and so on.

To assign an employee to shift rotation:

1. Click **Management** on the left pane and then select **Shift Rotation**. The **Shift Rotation** page appears.



2. To add, edit, search, and perform the following functions, you can use the icons available at the lower pane of the page.

Table 18-1 List of icons appearing on the lower pane

Icons	Click to...
	Add a new record, along with a description.
	Edit an existing record.

Table 18-1 List of icons appearing on the lower pane

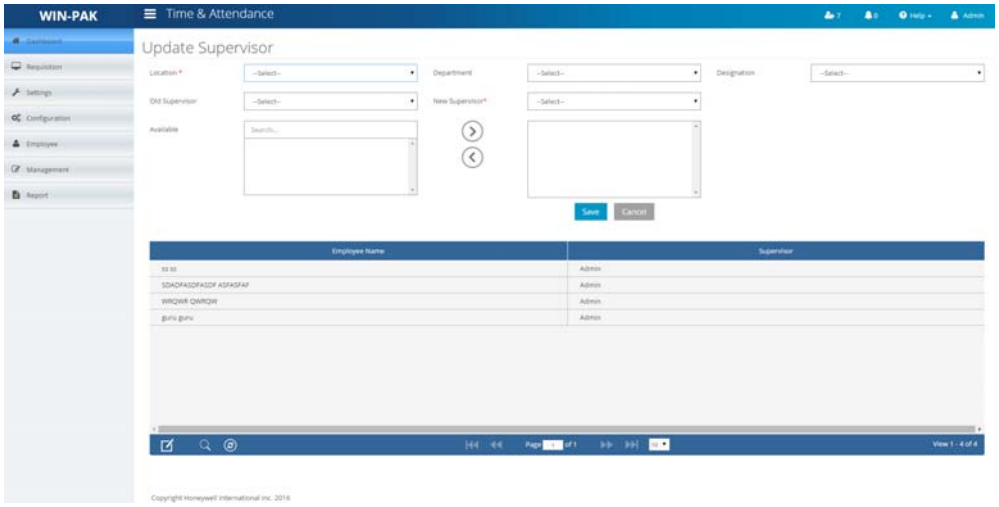
Icons	Click to...
	Search based on selected criteria.
	Refresh and reload the grid.
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Update Supervisor

The **Update Supervisor** page displays the location, old supervisor details, department, designation, and so on.

To update employee supervisor:

1. Click **Management** on the left pane and then select **Update Supervisor**. The **Update Supervisor** page appears.



2. Enter the following details.

Table 18-2 Update Supervisor

Field	Description
Location	From the drop-down list, select the location of the employee.

Table 18-2 Update Supervisor

Field	Description
Department	From the drop-down list, select the department of the employee.
Designation	From the drop-down list, select the designation of the employee.
Old Supervisor	From the drop-down list, select the old supervisor of the employee.
New Supervisor	From the drop-down list, select the new supervisor for the employee.
Available	The **Available** box under **Old Supervisor** lists all the employees assigned to the existing supervisor. The **Available** box under **New Supervisor** lists all the employees assigned to the new supervisor. You can use the and arrow to move the list of employees from old to new supervisor and vice versa.

3. Click **Save**.

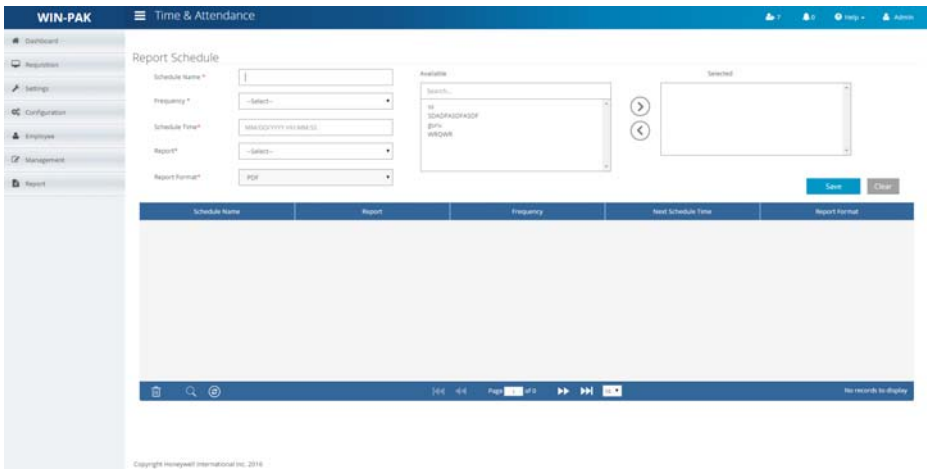
   A list of all the employees, along with their respective supervisors, appears.

Report Schedule

The **Report Schedule** page displays a list of all the scheduled reports along with the report name, frequency, schedule, and the format of the report.

To schedule generating a report:

1. Click **Management** on the left pane and then select **Report Schedule**. The **Report Schedule** page appears.



2. Enter the following details.

Table 18-3 Report Schedule

Field	Description
Schedule Name	Type the name for the schedule for the report.
Frequency	From the drop-down list, select the frequency of the report generation.
Schedule Time	Type the schedule time for the report generation.
Report	From the drop-down list, select the report name.
Report Format	From the drop-down list, select the report format.
Available	The **Available** box lists all the employees. You can use the and arrow to move the list of employees from available to selected list and vice versa.
Selected	The **Selected** box lists the selected employees. You can use the and arrow to move the list of employees from available to selected list and vice versa.

3. Click **Save**.

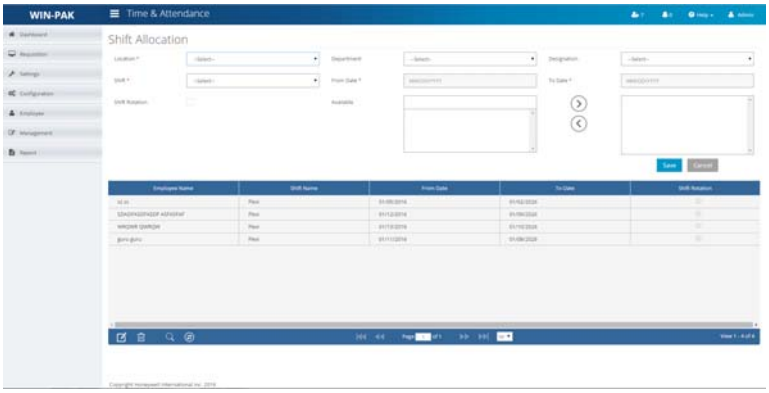
   A list of all the report schedules appears, along with the report name, frequency, schedule time and the format of the report.

Shift Allocation

The **Shift Allocation** page displays the location, department, designation, and so on.

To allocate a shift to an employee:

1. Click **Management** on the left pane and then select **Shift Allocation**. The **Shift Allocation** page appears.



2. Enter the following details.

Table 18-4 Shift Allocation

Field	Description
Location	From the drop-down list, select the location of the employee.
Department	From the drop-down list, select the department of the employee.
Designation	From the drop-down list, select the designation of the employee.
Shift	From the drop-down list, select the old supervisor of the employee.
From Date	Select the date (in month, date, year format) from when the shift must commence.
To Date	Select the date (in month, date, year format) at when the shift must conclude.
Shift Rotate	Select to assign an employee to shift rotation.
Available	The **Available** box under **Old Supervisor** lists all the employees assigned to the existing supervisor. The **Available** box under **New Supervisor** lists all the employees assigned to the new supervisor. You can use the ⟨ and ⟩ arrow to move the list of employees from old to new supervisor and vice versa.

3. Click **Save**.

A list of all the employees, along with the shift name, from date, and to date appears. The shift rotate option, to directly assign the employees to a different shift, appears.

Reports

19

In this chapter...

This chapter describes about the Introduction to Reports, Report Templates, and Generating and Printing a Report in WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
Generating and Printing a Report: Account Report, page 860	✓	✓
Generating and Printing a Report: Account Summary Report, page 862	✓	
Generating and Printing a Report: ADV Actions, page 864		✓
Generating and Printing a Report: Attendance Report, page 866	✓	✓
Generating and Printing a Report: Card Report, page 868	✓	✓
Generating and Printing a Report: Card Audit Report, page 872	✓	✓
Generating and Printing a Report: Card Frequency Report, page 875	✓	✓
Generating and Printing a Report: Card History Report, page 879	✓	✓
Generating and Printing a Report: Card Holder Report, page 882	✓	✓
Generating and Printing a Report: Card Holder Tab Layout Report, page 887	✓	✓
Generating and Printing a Report: Command File Report, page 888	✓	✓
Generating and Printing a Report: Control Area Report, page 891	✓	✓
Generating and Printing a Report: Device Map Report, page 892	✓	✓
Generating and Printing a Report: Door Schedule Report, page 902	✓	
Generating and Printing a Report: Elevator Groups Report, page 903	✓	
Generating and Printing a Report: Galaxy Panel Report, page 904	✓	
Generating and Printing a Report: Floor Plan Report, page 905	✓	✓

Section	WIN-PAK CS	WIN-PAK SE/PE
Generating and Printing a Report: Galaxy Panel Log Report, page 907		✓
Generating and Printing a Report: Guard Tour Report, page 909	✓	✓
Generating and Printing a Report: History Report, page 910	✓	✓
Generating and Printing a Report: Holiday Report, page 916	✓	
Generating and Printing a Report: Holiday Group Report, page 917	✓	✓
Generating and Printing a Report: Note Field Template Report, page 919	✓	✓
Generating and Printing a Report: Operator Report, page 921	✓	✓
Generating and Printing a Report: Operator Audit Report, page 923	✓	
Generating and Printing a Report: Operator Actions Report, page 926		✓
Generating and Printing a Report: Operator Level Report, page 930	✓	✓
Generating and Printing a Report: Operator Summary Report, page 932	✓	
Generating and Printing a Report: Schedule Report, page 934	✓	✓
Generating and Printing a Report: Time Zone Report, page 936	✓	✓
Generating and Printing a Report: Tracking and Mustering Area Report, page 938	✓	✓

Introduction

You can generate a number of reports using WIN-PAK CS/SE/PE. 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 CS/SE/PE:

- Access Area
- Access Level
- Account
- Account Summary (in WIN-PAK CS)
- ADV Action (in WIN-PAK SE/PE)
- Attendance
- Card
- Card Audit (in WIN-PAK SE/PE)
- Card Frequency
- Card History
- Card Holder
- Card Holder Tab Layout
- Command File
- Control Area
- Device Map
- Floor Plan
- Galaxy Panel Log (in WIN-PAK SE/PE)
- Guard Tour
- History
- Holiday Group
- Note Field Template
- Operator
- Operator Audit (in WIN-PAK CS)
- Operator Action (in WIN-PAK SE/PE)
- Operator Level
- Operator Summary (in WIN-PAK CS)
- Schedule
- Time Zone
- Tracking and Mustering Area
- Master Report
- Shift Allocation Report
- OverTime Report

- Attendance Report
- Attendance Correction Report
- On Duty Report
- Leave Report
- Leave Balance Report

In addition, WIN-PAK CS provides an option to define the templates for the following reports.

- Access Level
- Card
- Card History
- Card Holder
- Door Schedule
- History
- Holiday
- Time Schedule

Report Templates

In WIN-PAK CS/SE/PE, you can define the report templates for the frequently-generated reports.

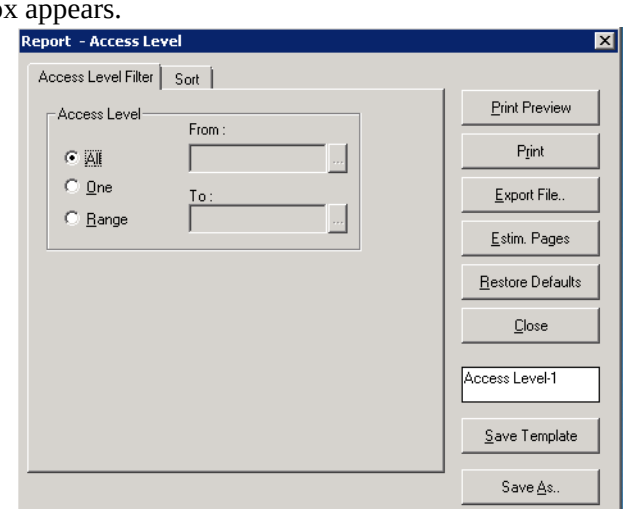
Defining Access Level Report Template

Note: This section is applicable only for WIN-PAK CS.

Adding an Access Level Report Template

To define the Access Level report template:

1. Click **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the various template folders.
3. Right-click the **Access Level** folder and click **Add**. The **Report - Access** Level dialog box appears.



4. See **Report Types** for more information on defining the filter options for the access level report.
5. Type the name of the **Access Level** report template in the text box on the right.
6. Click **Save Template** to save the template.
7. To create a copy of the template, click **Save As**. The **Save As/Copy - Report** Template dialog box appears.
8. Type a new name for the template and click **OK** to create a copy of template and return to **Report - Access Level** dialog box.
9. Click **Close** to close the dialog box.

Editing an Access Level Report Template

To edit the Access Level Report template:

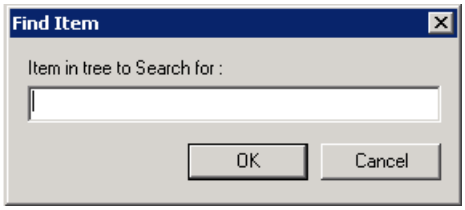
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Access Level** folder.
3. Right-click the report template and click **Edit**. The **Report - Access Level** dialog box appears.

   See the section "Adding an Access Level Report Template" in this chapter for details on editing the template.

Searching an Access Level Report Template

To search an Access Level Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Access Level** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.

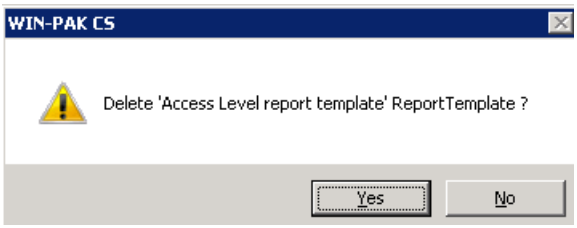


4. Type the name of the template to be searched and click **OK**. The template with the specified name is highlighted.

Deleting an Access Level Report Template

To delete an Access Level Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Access Level** folder.
3. Right-click the report template and click **Delete**. A cofirmatory message appears.



4. Click **Yes** to confirm the deletion. The selected report template is deleted.

To delete all the Access Level report templates:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder.
3. Right-click the **Access Level** folder and click **Delete All**. A confirmatory message appears.
4. Click **Yes** to confirm the deletion.

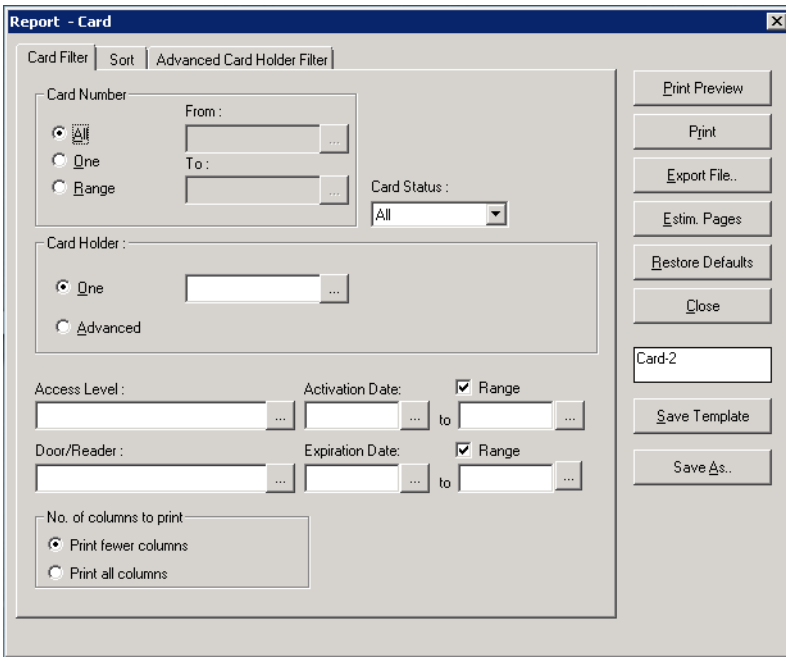
Defining Card Report Templates

Note: This section is applicable only for WIN-PAK CS.

Adding a Card Report Template

To define the Card report template:

1. Click **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the various template folders.
3. Right-click the **Card** folder and click **Add**. The **Report - Card** dialog box appears.



4. Type the name of the **Card 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** dialog box.
8. Click **Close** to close the dialog box.

Editing a Card Report Template

To edit a Card Report template:

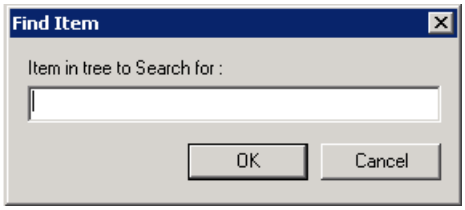
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card Report** folder.
3. Right-click the report template and click **Edit**. The **Report - Card Report** dialog box appears.

   See the section "Adding a Card Report Template" in this chapter for details on editing the template.

Searching a Card Report Template

To search a Card Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card Report** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.



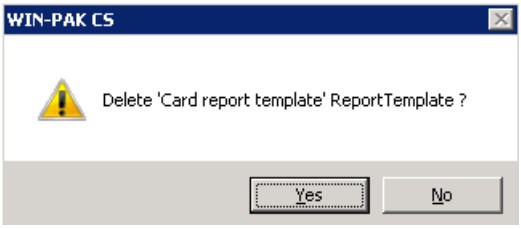
4. Type the name of the template to be searched and click **OK**. The template with the specified name is highlighted.

Deleting a Card Report Template

To delete a Card Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card Report** folder.

3. Right-click the report template and click **Delete**. A cofirmatory message appears.



4. Click **Yes** to confirm the deletion. The selected report template is deleted.

To delete all the Card Report templates:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder.
3. Right-click the **Card Report** folder and click **Delete All**. A confirmatory message appears.
4. Click **Yes** to confirm the deletion.

Defining Card History Report Templates

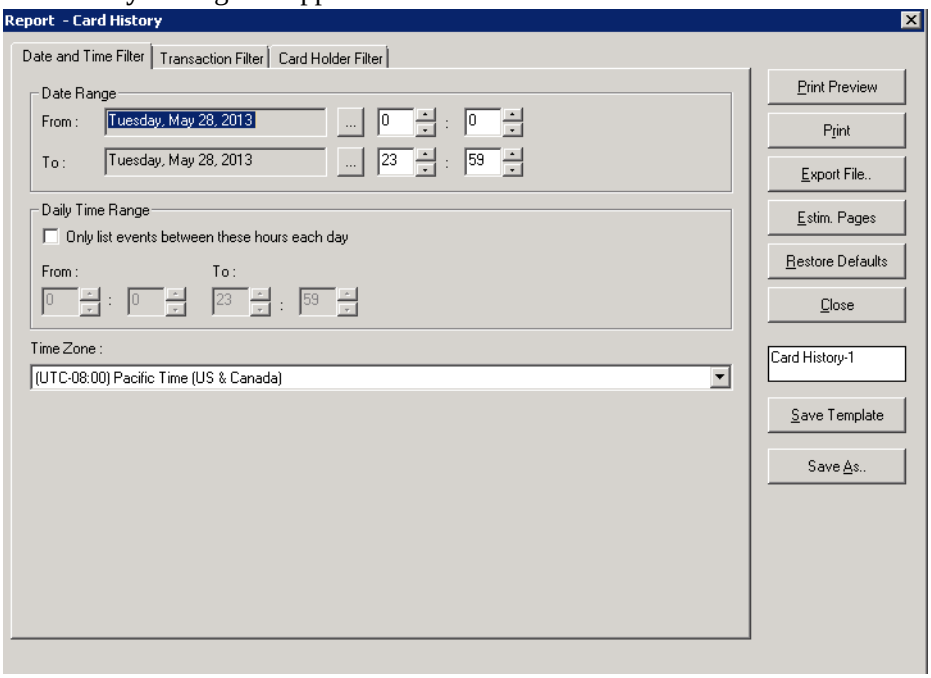
Note: This section is applicable only for WIN-PAK CS.

Adding a Card History Report Template

To define the Card History report template:

1. Click **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the various template folders.

3. Right-click the **Card History** folder and click **Add**. The **Report - Card History** dialog box appears.



4. Type the name of the **Card 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 S**ave 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 History** dialog box.
8. Click **Close** to close the dialog box.

Editing a Card History Report Template

To edit a Card Hisotry Report template:

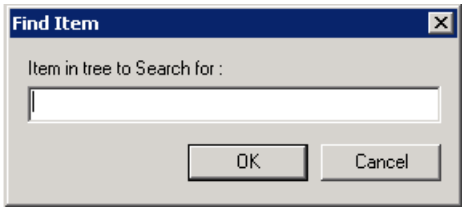
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card History Report** folder.
3. Right-click the report template and click **Edit**. The **Report - Card History Report** dialog box appears.

   See the section "Adding a Card History Report Template" in this chapter for details on editing the template.

Searching a Card History Report Template

To search a Card History Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card History Report** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.

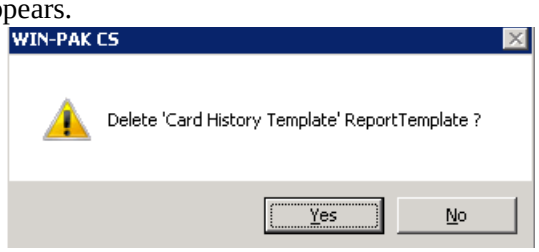


4. Type the name of the template to be searched and click **OK**. The template with the specified name is highlighted.

Deleting a Card History Report Template

To delete a Card History Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Card History Report** folder.
3. Right-click the report template and click **Delete**. A cofirmatory message appears.



4. Click **Yes** to confirm the deletion. The selected report template is deleted.

To delete all the Card History Report templates:

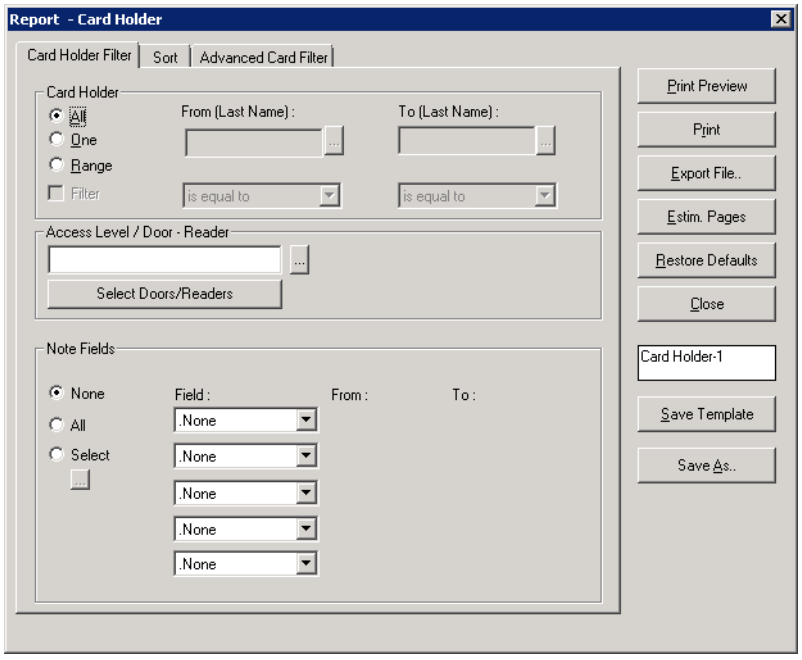
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder.
3. Right-click the **Card History Report** folder and click **Delete All**. A confirmatory message appears.
4. Click **Yes** to confirm the deletion.

Defining Card Holder Report Templates

Adding a Card Holder Report Template

To define the Card Holder report template:

1. Click **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the various template folder.
3. Right-click the **Card Holder** folder and click **Add**. The **Report - Card Holder** dialog box appears.



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.

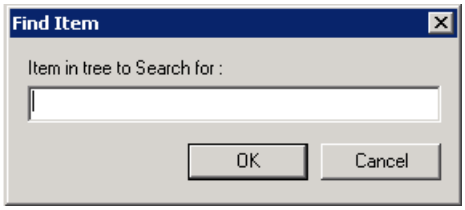
3. Right-click the report template and click **Edit**. The **Report - Card Holder** dialog box appears.

   See 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.

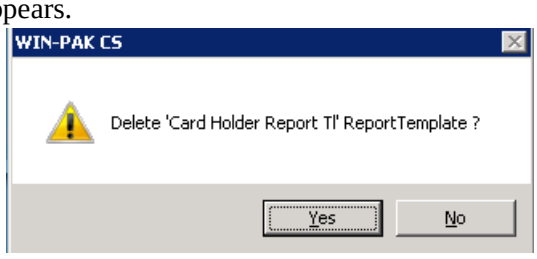


4. Type the name of the template to be searched and click **OK**. The template starts with the specified name is highlighted.

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 confirmatory message 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 confirmatory message 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.

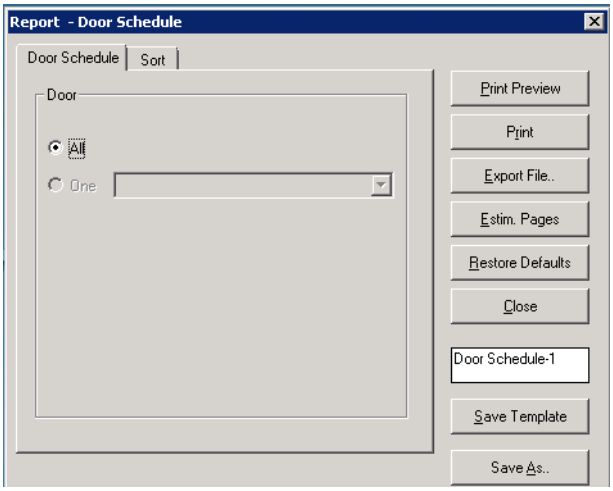
Defining Door Schedule Report Templates

Note: This section is applicable only for WIN-PAK CS.

Adding a Door Schedule Report

To define the History report template:

1. Click **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the various template folder.
3. Right-click the **Door Schedule** folder and click **Add**. The **Report - Door Schedule** dialog box appears.



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 -Door Schedule** dialog box.
8. Click **Close** to close the dialog box.

Editing a Door Schedule Report Template

To edit the Door Schedule Report template:

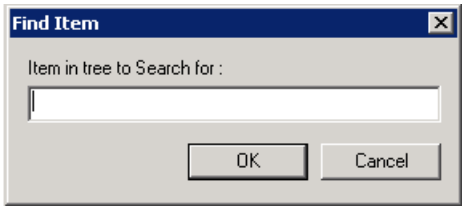
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Door Schedule** folder.
3. Right-click the report template and click **Edit**. The **Report - Door Schedule** dialog box appears.

   See the section "Adding a Door Schedule Report" in this chapter for details on editing the template.

Searching a Door Schedule Report Template

To search a Door Schedule Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Door Schedule** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.

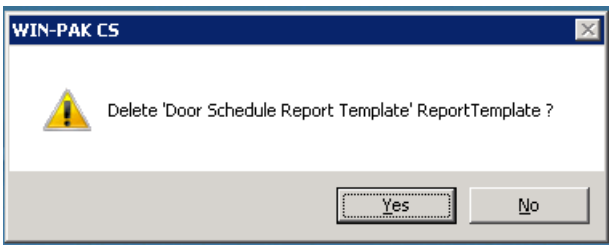


4. Type the name of the template to be searched and click **OK**. The template that starts with the specified name is highlighted.

Deleting a Door Schedule Report Template

To delete a Door Schedule Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Door Schedule** folder.
3. Right-click the report template and click **Delete**. A confirmatory message 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 **Door Schedule** folder and click **Delete All**. A confirmatory message 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.

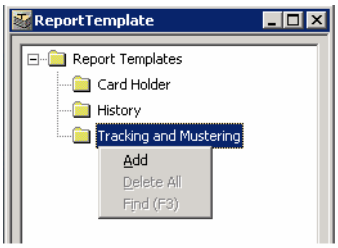
Defining Tracking and Mustering Templates

Note: This section is applicable only for WIN-PAK SE/PE.

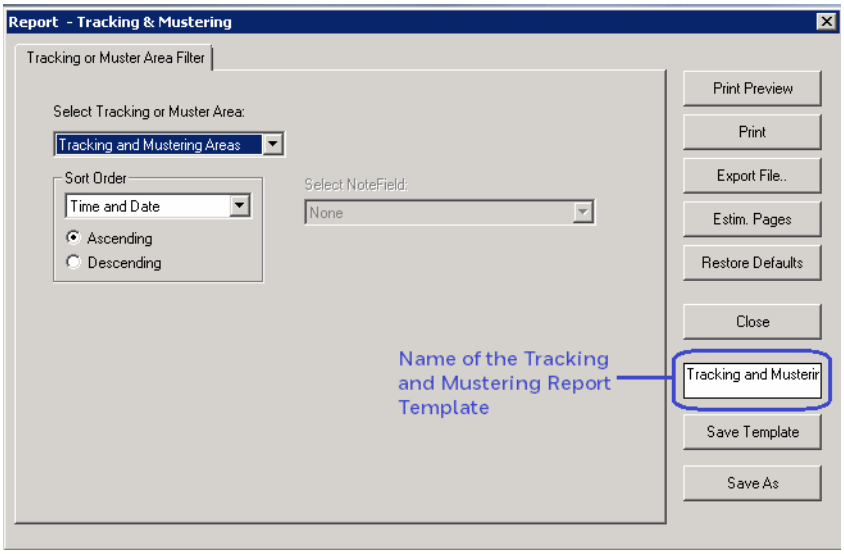
Adding a Tracking and Mustering Report Template

To define the Tracking and Mustering report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the Tracking and Mustering folders.

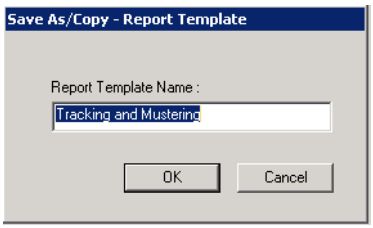


3. Right-click the **Tracking and Mustering** folder and click **Add**. The **Report - Tracking and Mustering** dialog box appears.



See the "Tracking and Mustering Area Report" section in this chapter for more on defining the filter options for the generating tracking and mustering report.

4. Type the name of the Tracking and Mustering 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 - Tracking and Mustering** dialog box.
8. Click **Close** to close the dialog box.

Editing a Tracking and Mustering Report Template

To edit the Tracking and Mustering Report template:

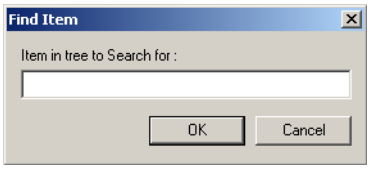
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Tracking and Mustering** folder.
3. Right-click the report template and click **Edit**. The **Report - Tracking and Mustering** dialog box appears.

See the "Adding a Tracking and Mustering Report Template" section in this chapter for details on editing the template.

Searching a Tracking and Mustering Report Template

To search a Tracking and Mustering Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Tracking and Mustering** 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 Tracking and Mustering Report Template

To delete a Tracking and Mustering Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Tracking and Mustering** 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 Tracking and Mustering Report templates:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Tracking and Mustering** folder.
3. Right-click the **Tracking and Mustering** folder and click **Delete All**. A message asking for confirmation appears.
4. Click **Yes** to confirm the deletion.

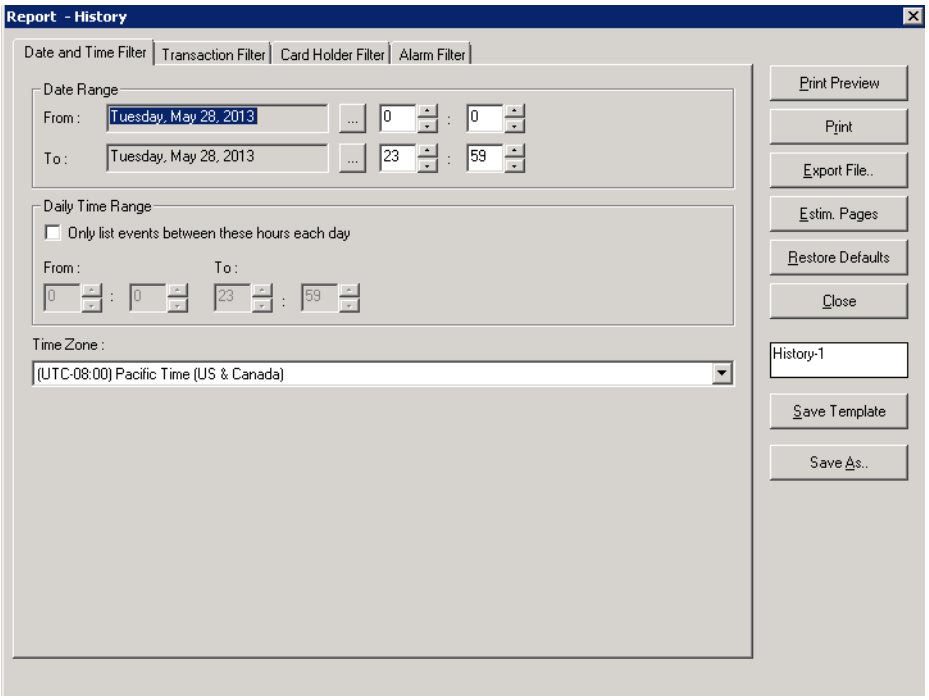
Defining History Report Templates

Note: WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

Adding a History Report Template

To define the History report template:

1. Click **Reports > Report Templates**. The Report Template window appears.
2. Expand the **Report Templates** folder to view the various template folders.
3. Right-click the **History** folder and click **Add**. The **Report - History** dialog box appears.



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.

See "Generating and Printing a Report" on page 848 for more information on defining the filter options for generating a history report.

TEditing a History Report Template

To edit the History Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.

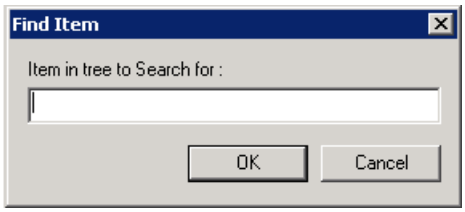
2. Expand the **Report Templates** folder and the **History** folder.
3. Right-click the report template and click **Edit**. The **Report - History** dialog box appears.

   See 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.

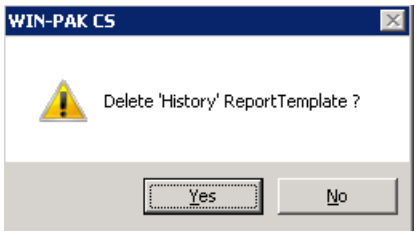


4. Type the name of the template to be searched and click **OK**. The template that starts with the specified name is highlighted.

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 confirmatory message 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.
3. Right-click the **History** folder and click **Delete All**. A confirmatory message 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.

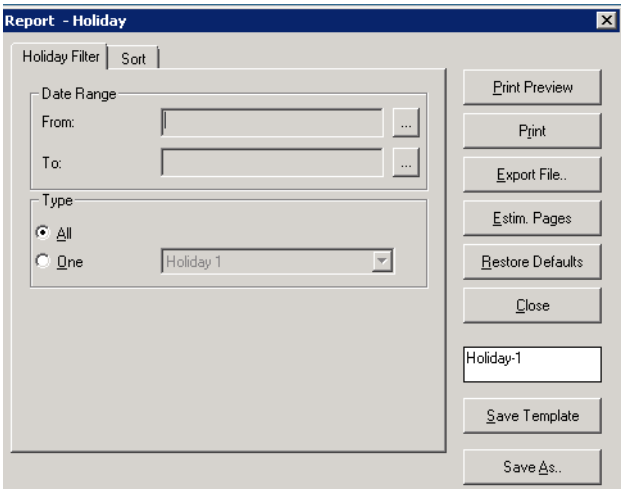
Defining Holiday History Report Templates

Note: This section is applicable only for WIN-PAK CS.

Adding a Holiday Template

To define the Holiday report template:

1. Click **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the various template folders.
3. Right-click the **Card History** folder and click **Add**. The **Report - Holiday** dialog box appears.



4. Type the name of the **Holiday 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 S**ave 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 - Holiday** dialog box.
8. Click **Close** to close the dialog box.

Editing a Holiday Template

To edit the Holiday template:

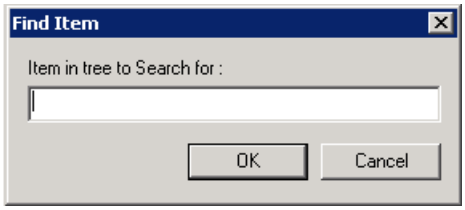
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Holiday** folder.
3. Right-click the report template and click **Edit**. The **Report - Holiday** dialog box appears.

   See the section "Adding a Holiday Template" in this chapter for details on editing the template.

Searching a HolidayTemplate

To search a Holiday template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Holiday** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.

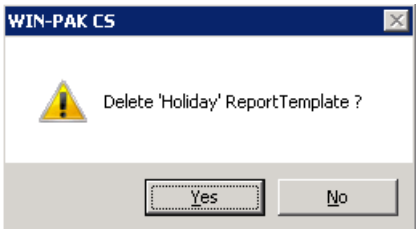


4. Type the name of the template to be searched and click **OK**. The template that starts with the specified name is highlighted.

Deleting a HolidayTemplate

To delete a Holiday template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Holiday** folder.
3. Right-click the report template and click **Delete**. A confirmatory message appears.



4. Click **Yes** to confirm the deletion. The selected report template is deleted.

To delete all the Holiday templates:

1. Choose **Reports** > **Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder.
3. Right-click the **Holiday** folder and click **Delete All**. A confirmatory message appears.
4. Click **Yes** to confirm the deletion.

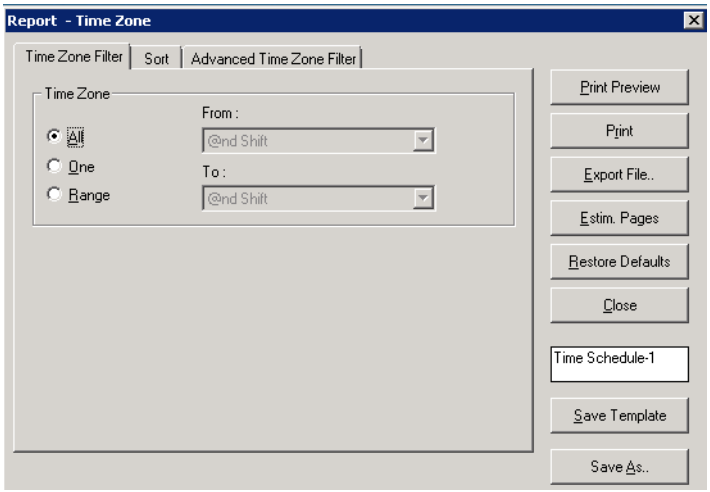
Note: All the report templates are deleted except for the templates that are used in the schedule.

Defining Time Zone History Report Templates

Adding a Time Zone Report Template

To define the Time Zone report template:

1. Click **Reports** > **Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder to view the various template folders.
3. Right-click the **Time Zone Report** folder and click **Add**. The **Report - Time Zone** dialog box appears.



4. Type the name of the **Time Zone** 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 - Time Zone** dialog box.
8. Click **Close** to close the dialog box.

Editing a Time Zone Report Template

To edit the Time Zone Report template:

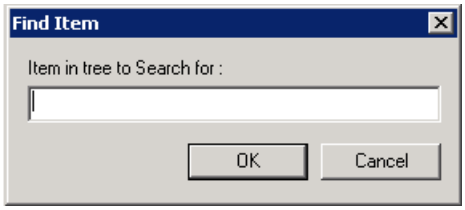
1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Time Zone** folder.
3. Right-click the report template and click **Edit**. The **Report - Time Zone** dialog box appears.

   See the section "Adding a Time Zone Report Template" in this chapter for details on editing the template.

Searching a Time Zone Report Template

To search a Time Zone Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Time Zone** folder.
3. Right-click the report template and click **Find**. The **Find Item** dialog box appears.

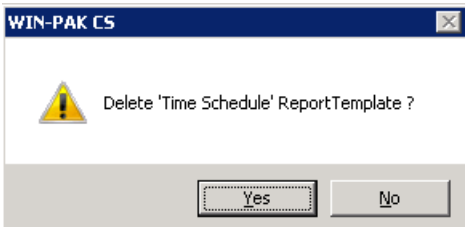


4. Type the name of the template to be searched and click **OK**. The template that starts with the specified name is highlighted.

Deleting a Time Zone Report Template

To delete a Time Zone Report template:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder and the **Time Zone** folder.
3. Right-click the report template and click **Delete**. A confirmatory message appears.



4. Click **Yes** to confirm the deletion. The selected report template is deleted.

To delete all the Time Zone Report templates:

1. Choose **Reports > Report Templates**. The **Report Template** window appears.
2. Expand the **Report Templates** folder.
3. Right-click the **Holiday** folder and click **Delete All**. A confirmatory message 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.

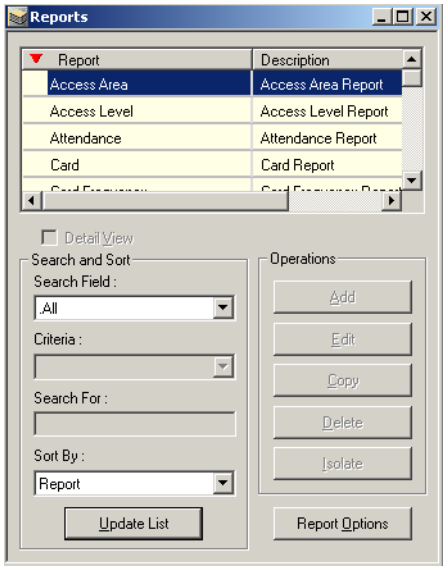
Generating and Printing a Report

Note: The following Report Types have no filtering options:

- Access Area Report
- Control Area Report
- Note Field Template Report
- Card Holder Tab Layout Report
- Tracking and Mustering 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.

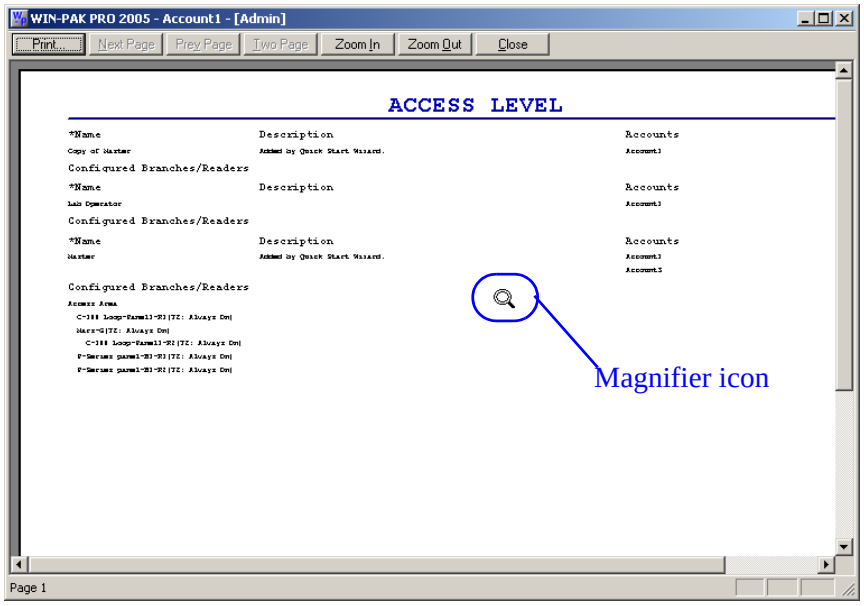
3. Set the filtering parameters for generating the report.
4. Select the **Run from Archive Database** check box in the report window to view the reports from the Archive Database.

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.

Note: Ensure Printer driver is installed in the system.

2. To enlarge the preview size:
    a. Click **Zoom In**.

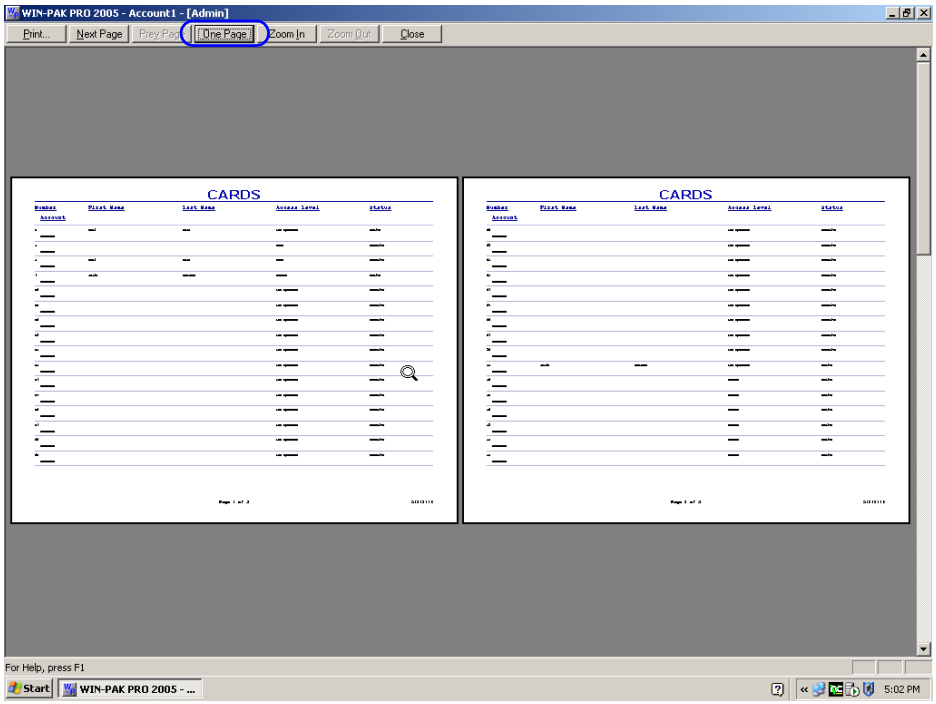
    OR

    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

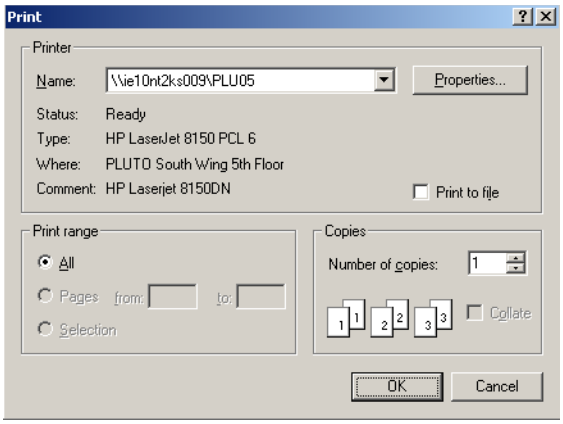
Click anywhere on the preview area using the magnifier icon. Ensure that the **Zoom Out** button is enabled before clicking.

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.

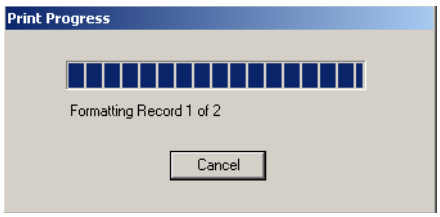
c. Click **OK**. The report is printed to the selected printer.

7. To close the preview window without printing the report, click **Close**.

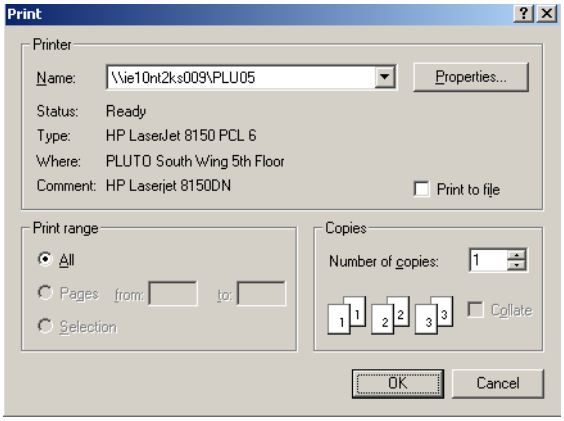
Printing the report

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.

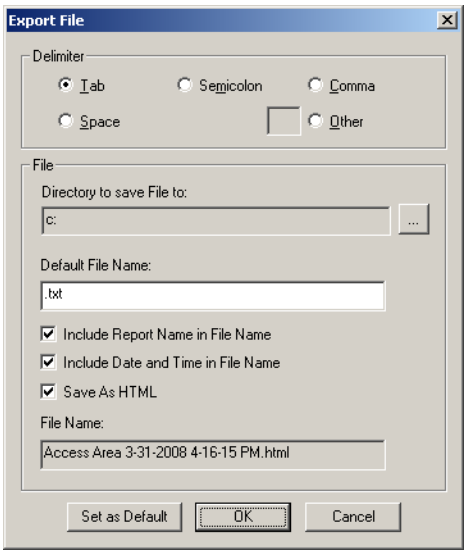
Note: If you have selected the **Print to file** check box, the **Print to File** dialog box appears. Change the path and file name, if required, and click **OK**.

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**.

   d. Select **Save As HTML** to save the file in the HTML format.

   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.

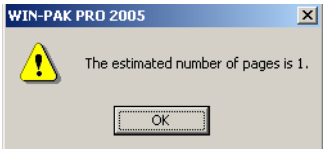
   Tip: To open and view the report file, browse through the specified location and open it.

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.

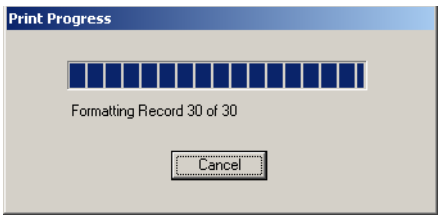
Note: The sorting options for the report are not cleared.

Sending the report as an e-mail

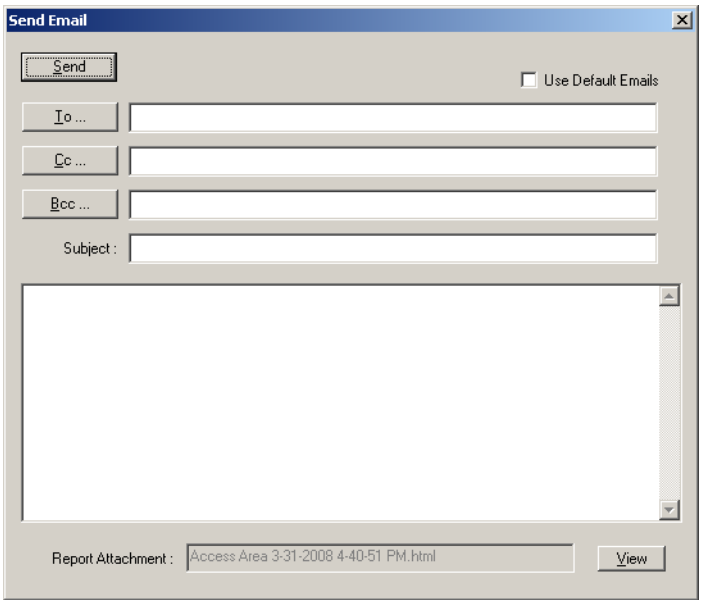
Note: **Sending the report as an e-mail** section is available only in WIN-PAK CS.

To send the report by e-mail:

1. Click **Email..** in the **Report** dialog box. The **Print Progress** dialog box appears showing the formatting status.



   Then the **Send Email** dialog box appears.



2. Type the e-mail addresses in the **To**, **Cc**, and **Bcc** fields.
3. Select the **Use Default Emails** box to use the default e-mail addresses set for the account.

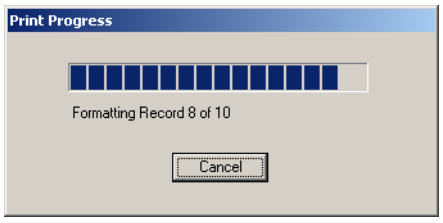
   Refer to the section "Specifying default e-mail IDs for reporting alarms"in the System Settings chapter, for more details on configuring the default e-mail ID to send reports.
4. Click **View** to preview the report.
5. Type the **Subject** for the e-mail.
6. Click **Send** to send the e-mail with the attached file.

Faxing the report

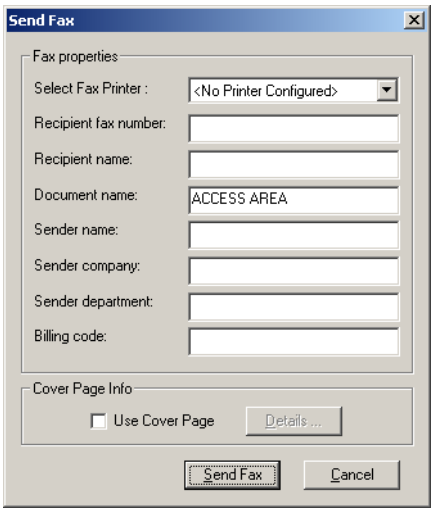
Note: **Faxing the report** section is available only in WIN-PAK CS.

To fax the report:

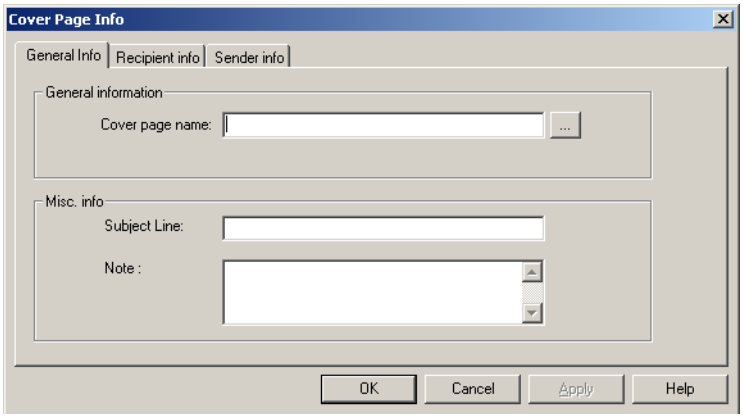
1. Click **Fax** in the **Report** dialog box. The **Print Progress** dialog box appears showing the formatting status.



   Then the **Send Fax** dialog box appears.



2. Select the fax printer from the **Select Fax Printer** list.
3. Enter the **Recipient fax number.**
4. Type the name of the recipient in the **Recipient name** box.
5. Type the name of the document in the **Document name box.** The name of the selected report appears by default.
6. Type your name in the **Sender name** box.
7. Type your company's name in the **Sender company** box.
8. Type your department's name in the **Sender department** box.
9. Enter the **Billing code**.
10. Select the **Use Cover Page** check box to include a cover page.
11. Click **Details**. The **Cover Page Info** dialog box appears, where you can configure the cover page information.



a. Type a name for the cover page in the **Cover page name** box. This is mandatory.

b. Type a **Subject Line** and a **Note** if required.

c. Click the **Recipient info** tab. Enter the **Name**, **Fax number**, **Company**, **Address**, **Title**, **Department**, **Office location**, **Home phone**, and **Office phone** information related to the fax recipient. All this information appears on the cover page of the fax.

d. Click the **Sender info** tab. Enter your **Name**, **Department**, **Fax number**, **Company**, **Address**, **Title, Office location**, **Home phone**, and **Office phone** information.

e. Click **OK** to save the cover page settings.

12. Click **Send Fax** to fax the report.

Reporting from the 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:

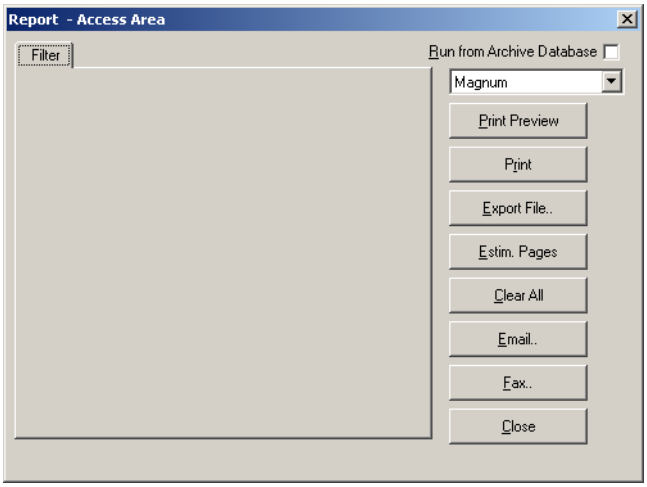
1. Click **Close**. The dialog box is closed.

Access Area Report

The Access Area report displays the branches and entrances or readers that are configured in Access Area.

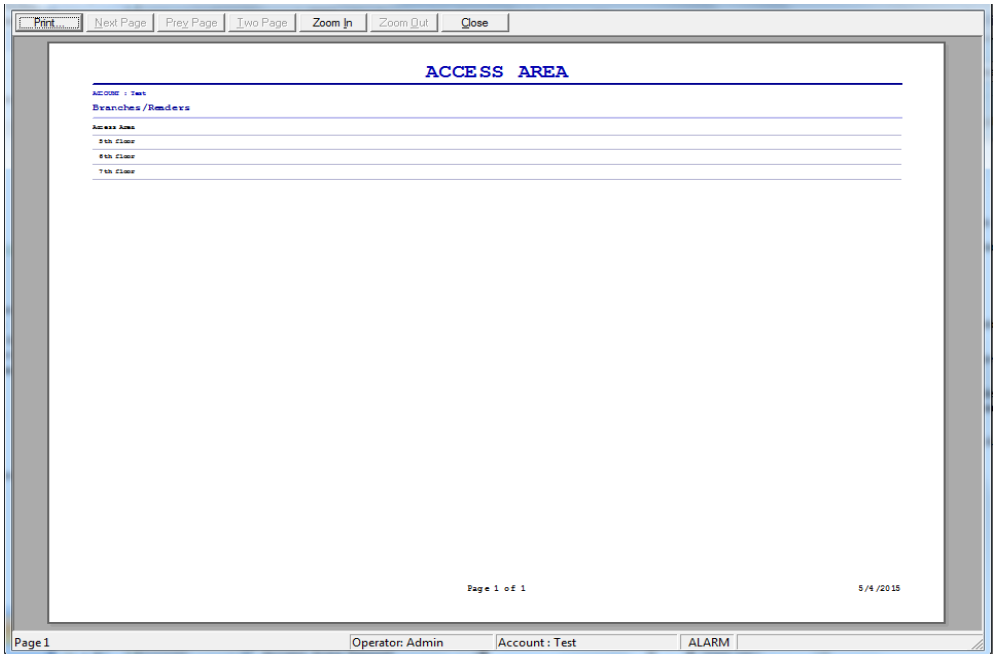
To generate an access area report:

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. Select the account from the drop-down list in the upper-right corner of the dialog box.
3. Click **Print Preview** to view the Access Area Report prior to printing.



4. Click **Print** to send the report to your printer.

Note: Step 5, 6, and 7 are applicable only in WIN-PAK CS.

5. Click **Email..** to send a copy of the report by e-mail, to the customer.
6. Click **Fax..** to fax a copy of the report.
7. 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 an Access Level.

Note: WIN-PAK CS screens are shown in this section as an example. The screens would change based on the variant selected.

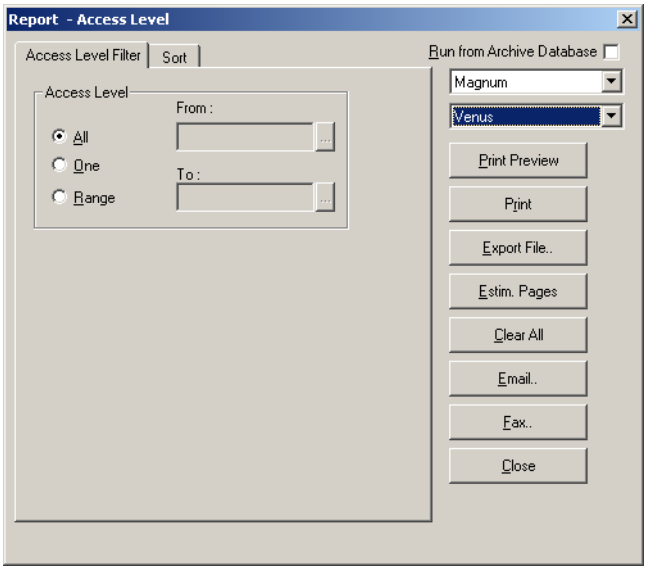
To generate the access level report:

1. In the **Reports** window, select the **Access Level** report and click **Report Options**. The **Report - Access Level** dialog box appears.

Note: Step 2, 7, and 8 are applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.

Note: By default, the current account is selected.

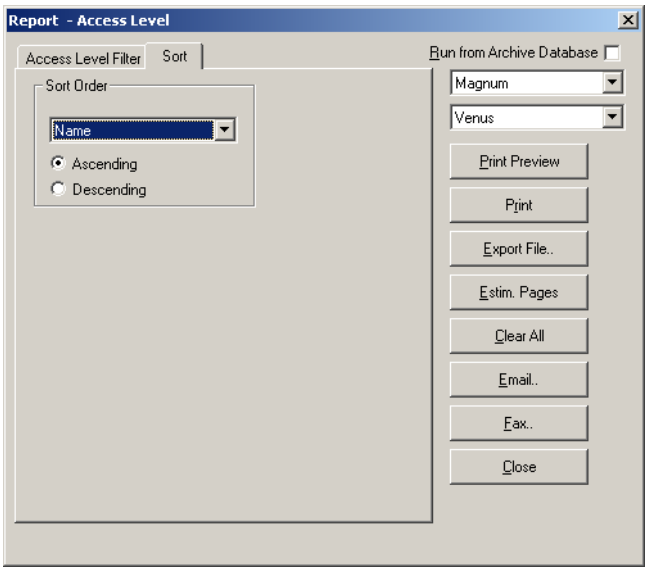


3. To generate reports for the specific access levels:
   a. Click the **Access Level Filter** tab.
   b. Under **Access Level**, select one of the following options:

Table 19-1 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.

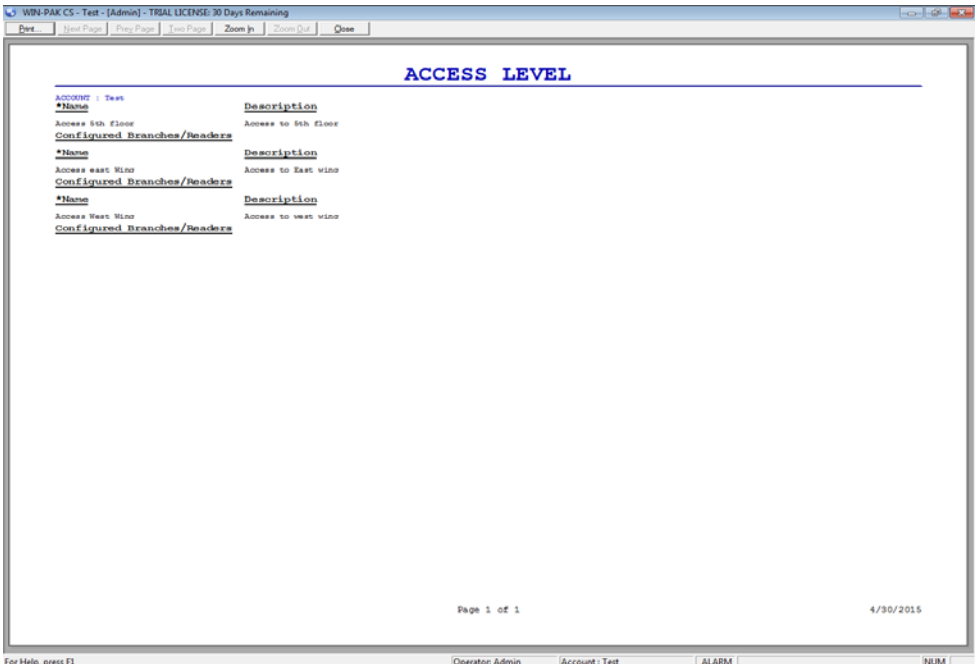
4. To sort the report by access level name:
   a. In the **Report - Access Level** dialog box, click the **Sort** tab.



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.

5. Click **Print Preview** to view the Access Level Report prior to printing.



6. Click **Print** to send the report to your printer.
7. Click **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.

9. Click **Close** to return to the **Report** window.

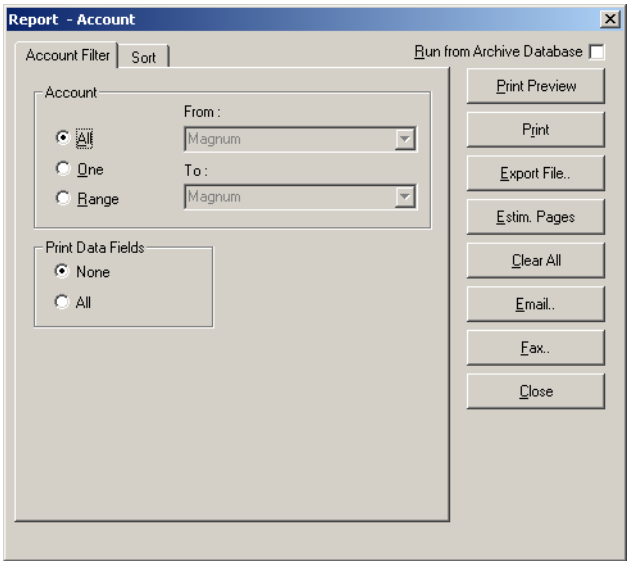
Note: In the report, some access levels are identified by numbers instead of the name. This indicates that these access levels are the custom access levels for the cards.

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 19-2 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.

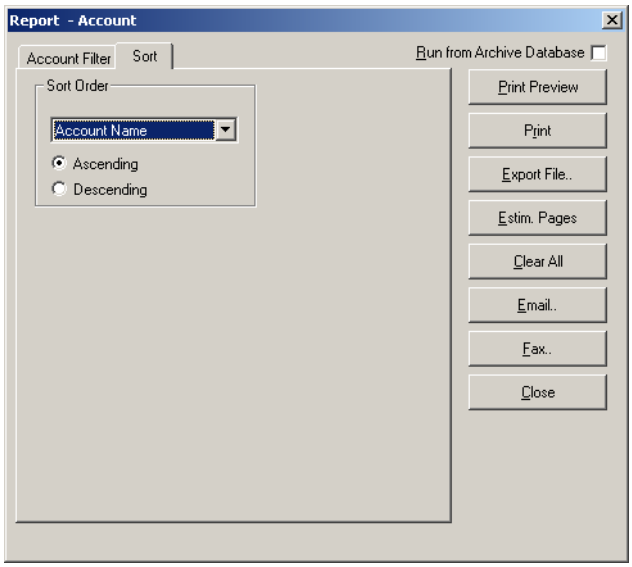
Table 19-2 Describing the filter options for Account report

Filter Option	Description
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.

Note: Step 6, and 7 is applicable only in WIN-PAK CS.

6. Click **Email..** to send a copy of the report by e-mail, to the customer.

7. Click **Fax..** to fax a copy of the report.

8. Click **Close** to return to the **Reports** window.

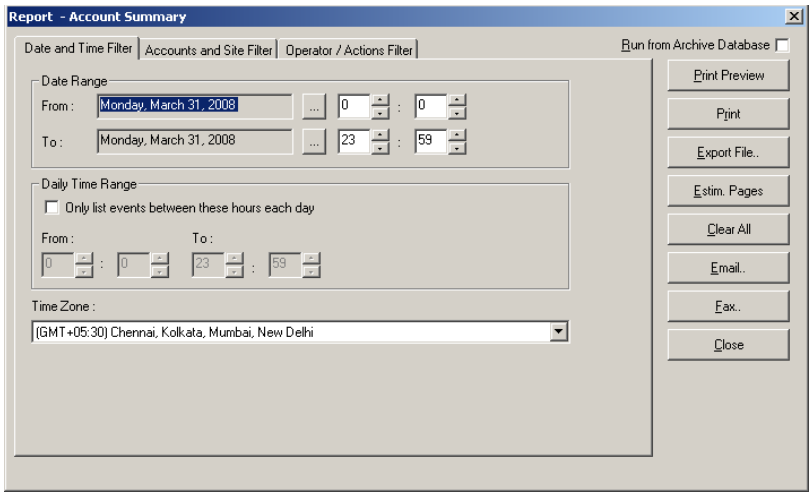
Account Summary Report

The Account Summary Report enables you to generate a report of all the operations carried out on a specific account, during a specific time interval.

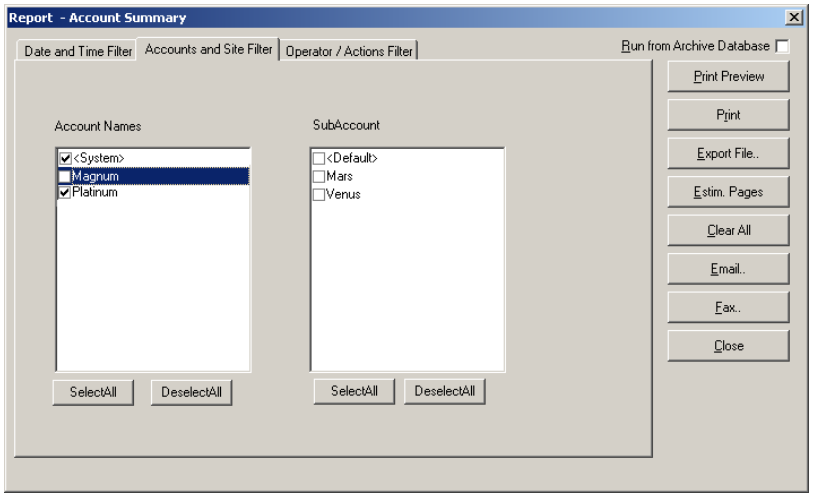
Note: Account Summary report can be generated only by the Administrator. This report feature is available only in WIN-PAK CS.

To generate the account summary report:

1. In the **Reports** window, select the **Account Summary** report and click **Report Options**. The **Report - Account Summary** 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 filter the records based on the accounts:
    a. Click the **Accounts and Site Filter** tab.

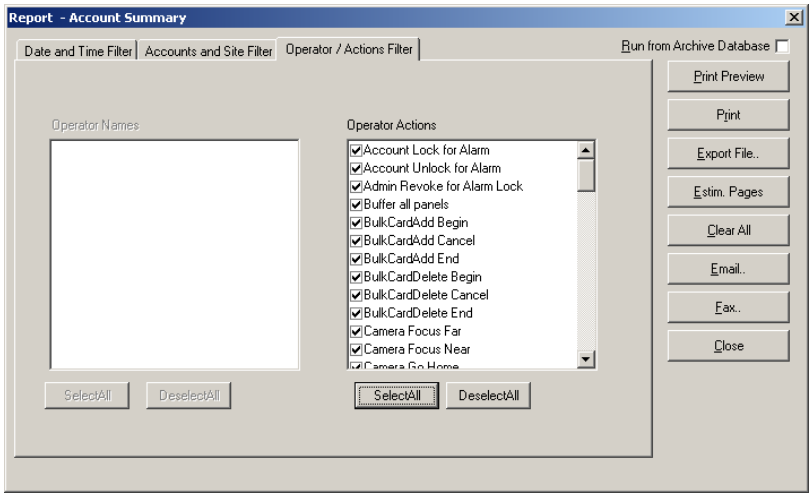


b. The **Account Names** contains a list of the accounts in WIN-PAK CS. Select the check boxes of the accounts for which reports are required.

Note: To generate a report for all the accounts, click **SelectAll** under the respective boxes.

4. To filter the records based on the operator actions performed:

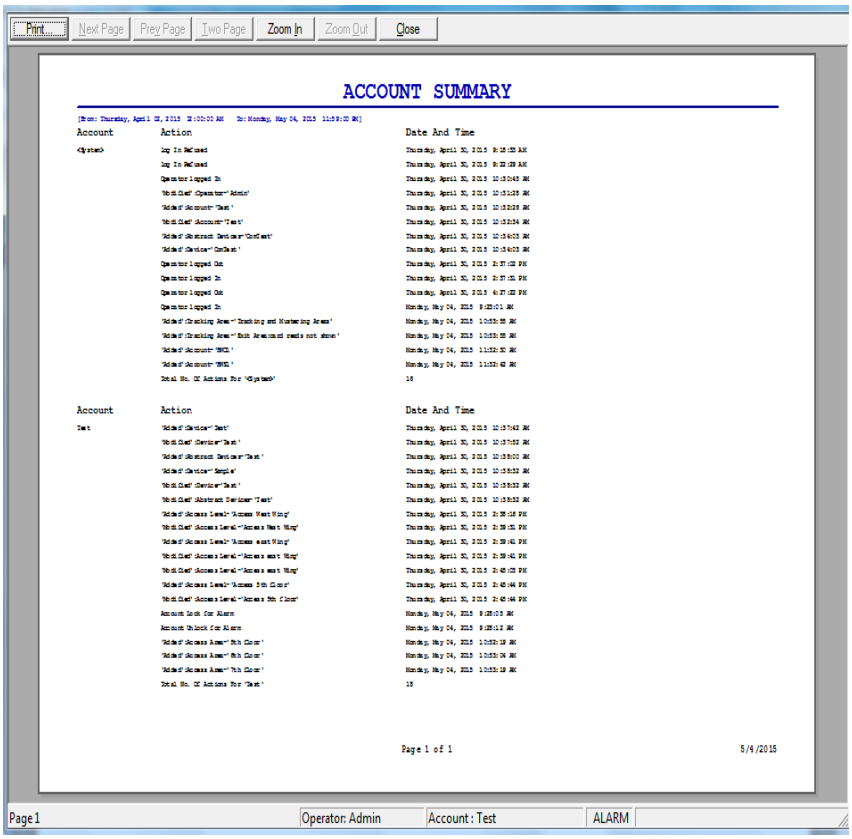
   a. Click the **Operator/Actions** tab.



   b. The **Operator Actions** contains a list of all the operator actions in WIN-PAK. Select the check boxes of actions for which reports are required.

Note: To generate a report for all the tasks performed by the operator, click **SelectAll**.

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 **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.
9. Click **Close** to return to the **Reports** window.

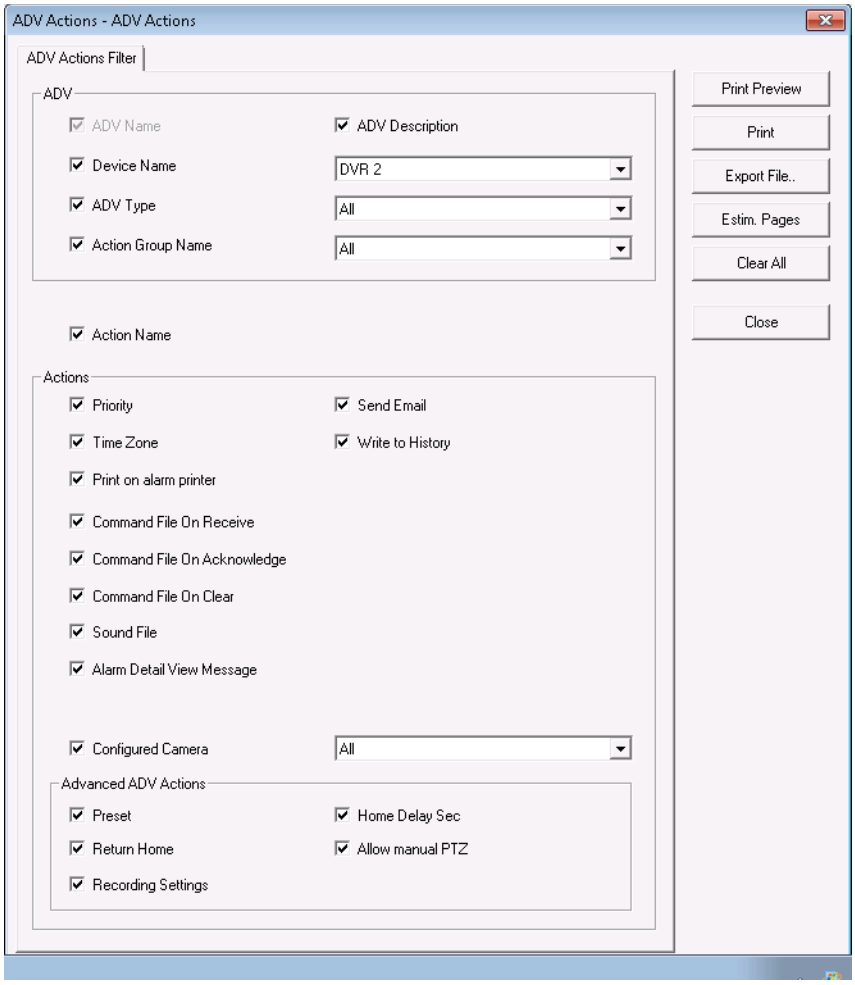
ADV Actions

The ADV Actions report contains the ADV actions for all the available devices.

To generate the ADV Actions report:

Note: The ADV Actions report is available only in WIN-PAK SE/PE.

1. In the **Reports** window, select the **ADV Actions** report and click **Report Options**. The **ADV Actions** dialog box appears.



2. Under **ADV**

   - The **ADV Description** check box is selected by default. Click to clear the **ADV Description** check box if you do not want to include this filter.
   - The **Device Name** check box is selected by default. Select a device name from the drop-down list. Click to clear the **Device Name** check box if you do not want to include this filter.
   - The **ADV Type** check box is selected by default. Select an ADV from the drop-down list. Click to clear the **ADV Type** check box if you do not want to include this filter.
   - The **Action Group Name** check box is selected by default. Select an Action group from the drop-down list. Click to clear the **Action Group Name** check box if you do not want to include this filter.

3. The **Action Name** check box is selected by default. Click to clear the **Action Name** check box if you do want to include this filter.

4. The following filters under **Actions** are enabled only if you select the **Action Name** check box. Click the check boxes corresponding to each of these filters to include them in the report.
    - Priority
    - Time Zone
    - Print on alarm printer
    - Command File on Receive
    - Command File on Acknowledge
    - Command File On Clear
    - Sound File
    - Alarm Detail View Message
5. Select the **Configured Camera** check box and then select a camera from the drop-down list.
6. The following filters under **Advanced ADV Actions** are enabled only if you select the **Configured Camera** check box.
    - Preset
    - Return Home
    - Recording Settings
    - Home Delay
    - Allow manual PTZ
7. Click **Print** to send the report to your printer.

Attendance Report

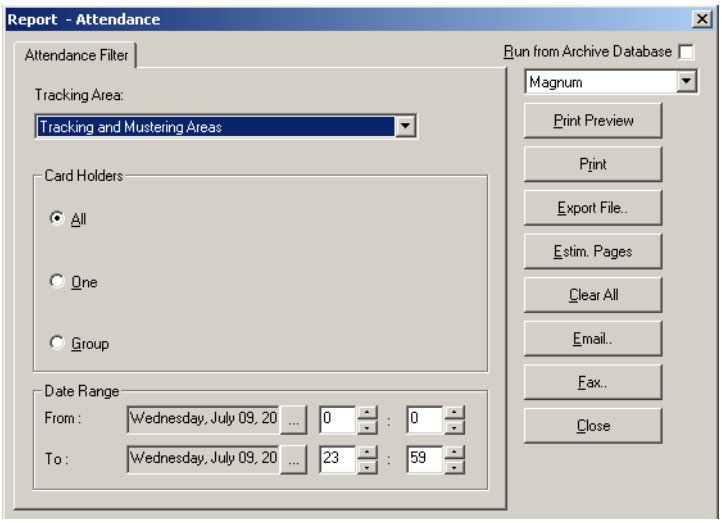
The Attendance Report helps to know the entry and exit details of the card holders who have presented their card in the reader of the tracking area. The Administrator requires this report for audit purposes.

To generate the attendance report:

1. In the **Reports** window, select the **Attendance** report and click **Report Options**. The **Report - Attendance** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. In the **Attendance Filter** tab, 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.

4. Select one of the following options for filtering the card holders under **Card Holders**:

   Table 19-3 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.

5. 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.

6. To specify the time range, enter the time in hours and minutes for the **From** and **To** fields.

Notes: In WIN-PAK SE/PE, follow the below steps 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.

7. Click **Print Preview** to view the report prior to printing it.
8. Click **Print** to send a copy of the report to your printer.

Note: Step 9 and 10 is applicable only in WIN-PAK CS.

9. Click **Email..** to send a copy of the report by e-mail, to the customer.
10. Click **Fax..** to fax a copy of the report.
11. Click **Close** to return to the **Reports** window.

Card Report

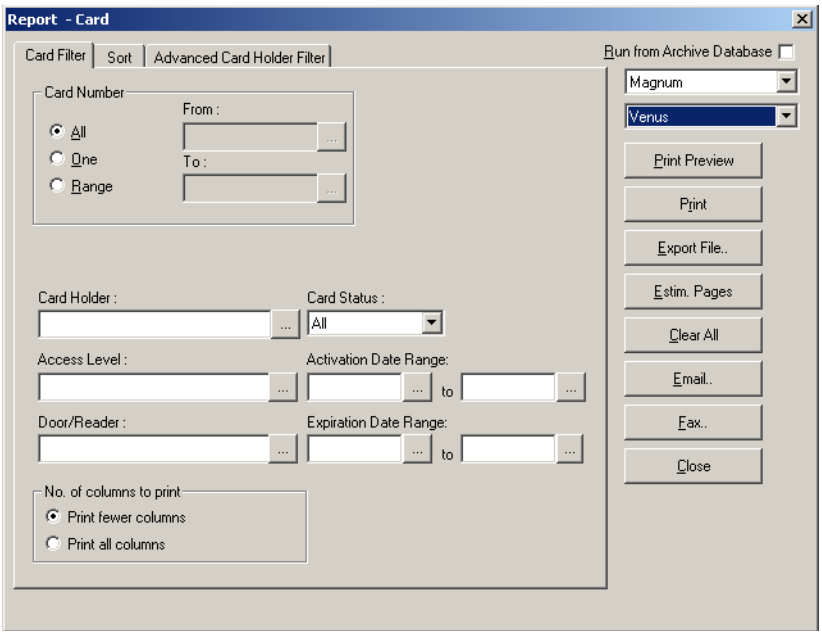
The Card Report is generated based on the selected account or on the all the accounts that are available for the operator. This report enables you to obtain the details of card holders holding a card, the card status and access level.

To generate the attendance report:

1. In the **Reports** window, select the **Card** report and click **Report Options**. The **Report - Card** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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 19-4 Describing the options for filtering the card number

Filter Option	Description
All	Generates a report for all cards.
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:

      - Card Holder
      - Access Level
      - Door/Reader

- Card Status
- Activation Date Range
- Expiration Date Range

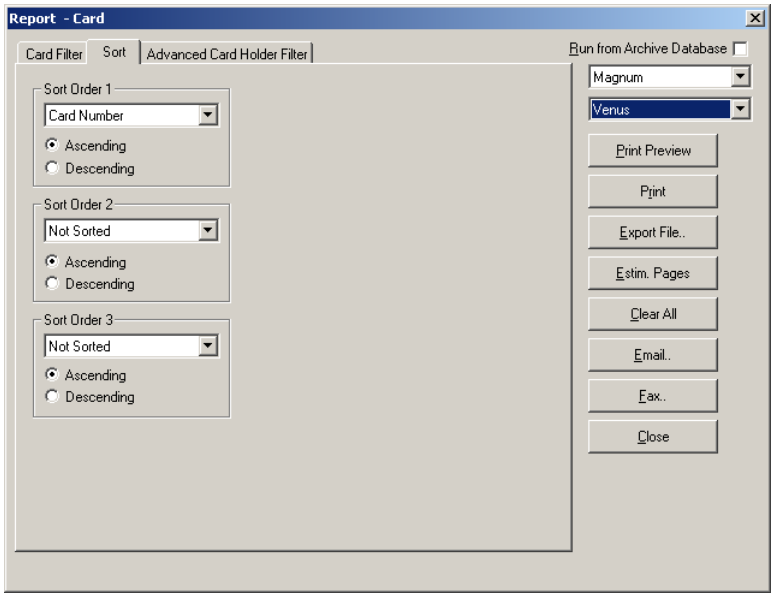
Note: You can use the ellipsis button to search for these options.

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.

4. 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.

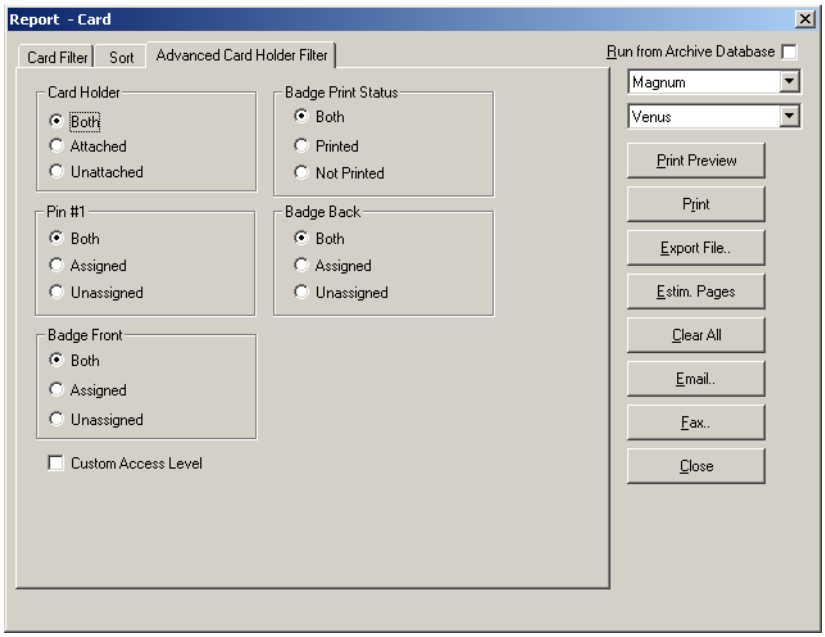
d. Under **Sort Order 2**, select the field by which the report must be sorted in the second level. If you select **Not Sorted** the report is sorted on the basis of the field selected in Sort Order 1.

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.

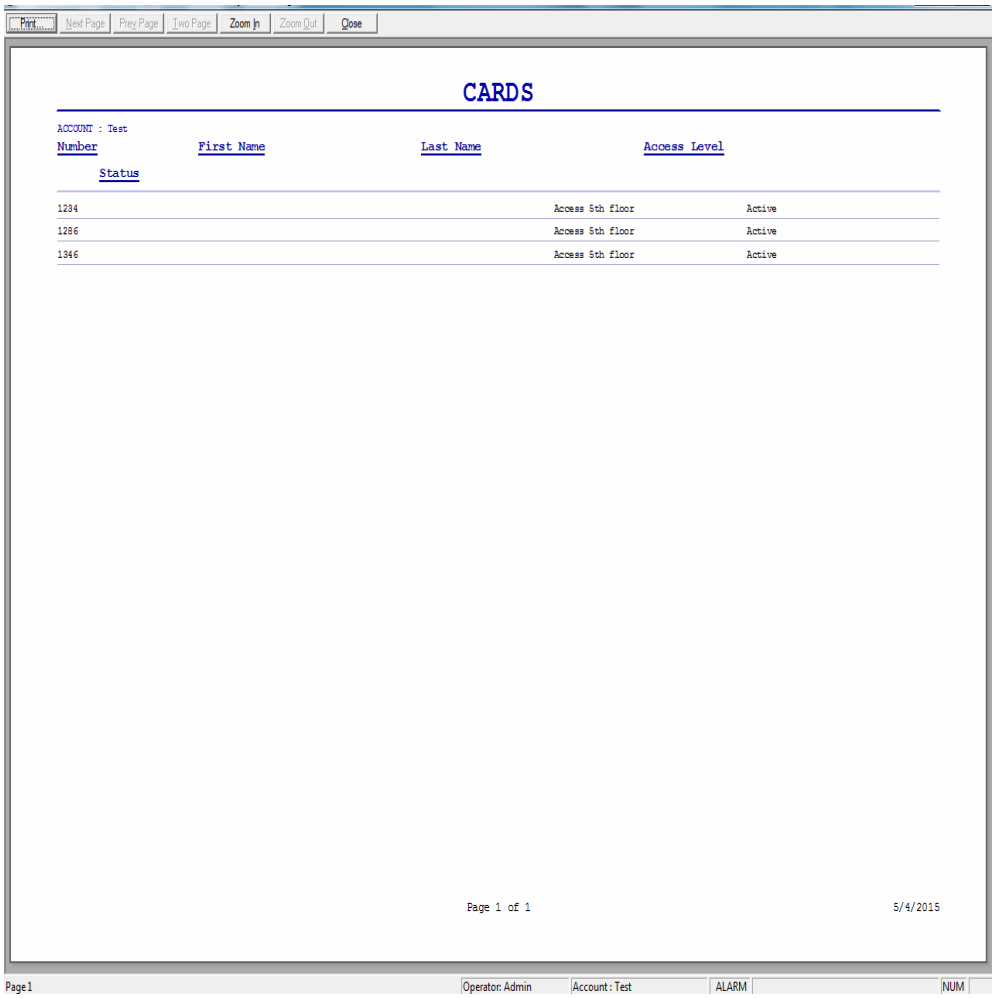
5. To filter cards based on card holder categories, click the **Advanced Card Holder Filter** tab.



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.

6. Select the **Custom Access Level** check box to include all cards that have custom access levels assigned to them.
7. Click **Print Preview** to view the report prior to printing it.



8. Click **Print** to send a copy of the report to your printer.

Note: Step 9 and 10 is applicable only in WIN-PAK CS.

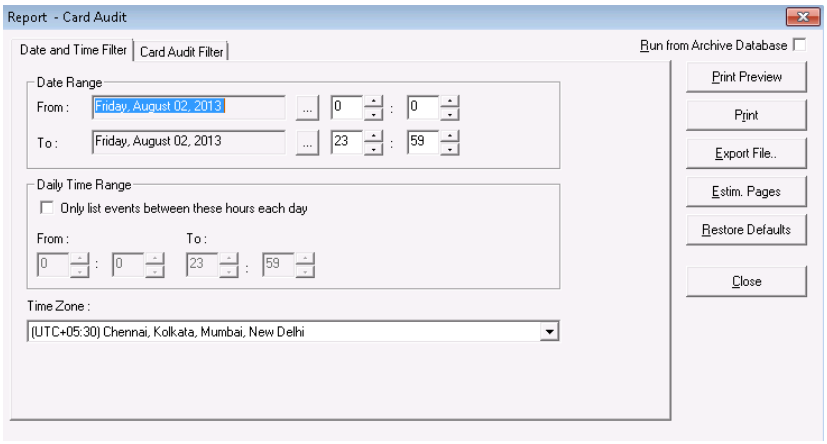
9. Click **Email..** to send a copy of the report by e-mail, to the customer.
10. Click **Fax..** to fax a copy of the report.
11. Click **Close** to return to the **Reports** window.

Card Audit Report

The Card Audit Report is generated based on the total number of cards, changes in the associated cards, and the type of changes. This report enables you to obtain the changes in the data in the format of old data and new data.

To generate the card audit report:

1. In the **Reports** window, select the **Card Audit** report and click **Report Options**. The **Report - Card Audit** dialog box appears.



2. To filter the card audit 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.

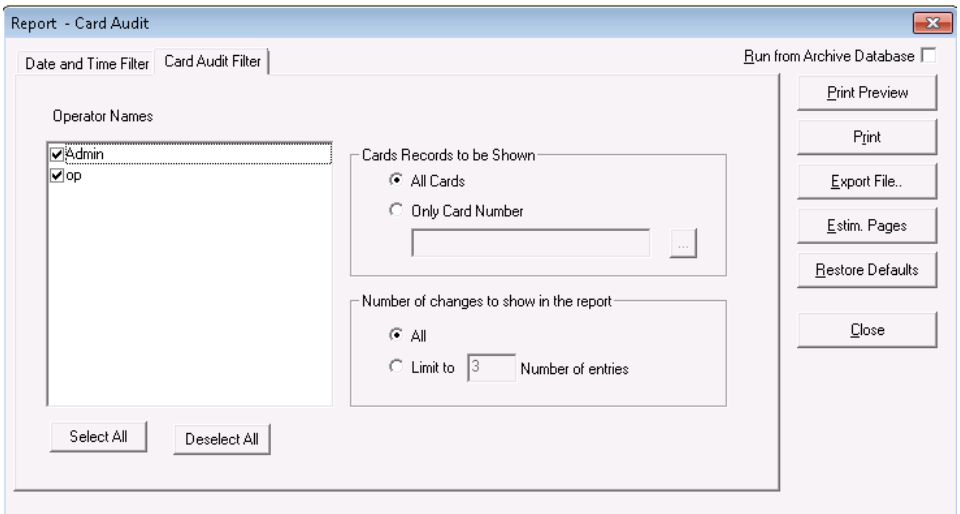
    d. To generate reports for events that occurred during the specified period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The **From** and **To** text boxes are enabled.

    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 filter the card audit details:

    a. Click the **Card Audit Filter** tab.



b. Select or clear the **Operator Names** to be included or excluded. By default, all the operators are selected.

Note: Click **Select All** to select all the operators or click **Deselect All** to clear all the operators.

c. Under **Cards Records to be Shown**, select the following options to filter the cards:

Table 19-5 Describing the options for card audit filtering

Filter Option	Description
All Cards	Generates the report that includes all the cards.
Only Card Number	Generates a report for a single card. You can use the ellipsis button to find the card number.

4. Under **Number of changes to show in the report**

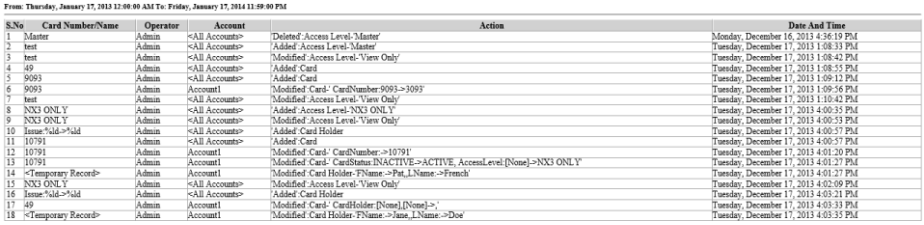
   a. Click **All** to obtain a report with all the entries.

   b. Click **Limit to** and type the **Number of entries** to obtain a report with the required number of entries. A maximum of 999 entries can be obtained.

5. Click **Print** to send a copy of the report to your printer.

   You can view the **Card Audit** report output in two different formats.

   Example: The **Card Audit** report format in html view.



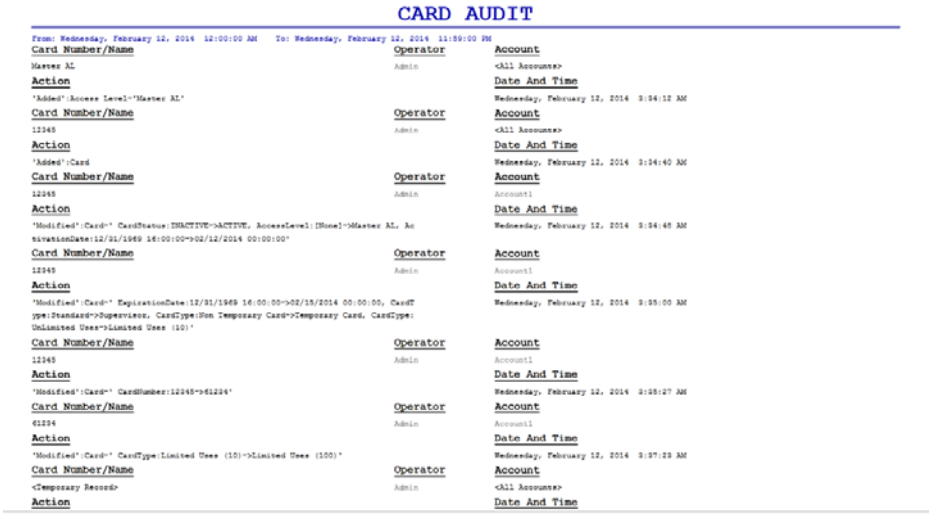
From: Thursday, January 17, 2013 12:00:00 AM To: Friday, January 17, 2014 11:59:00 PM

S.No	Card Number/Name	Operator	Account	Action	Date And Time
1	Master	Admin	<All Accounts>	'Deleted':Access Level-'Master'	Monday, December 16, 2013 4:36:19 PM
2	test	Admin	<All Accounts>	'Added':Access Level-'Master'	Tuesday, December 17, 2013 1:08:33 PM
3	test	Admin	<All Accounts>	'Modified':Access Level-'View Only'	Tuesday, December 17, 2013 1:08:42 PM
4	49	Admin	<All Accounts>	'Added':Card	Tuesday, December 17, 2013 1:08:55 PM
5	9093	Admin	<All Accounts>	'Added':Card	Tuesday, December 17, 2013 1:09:12 PM
6	9093	Admin	Account1	'Modified':Card-' CardNumber:9093->3093'	Tuesday, December 17, 2013 1:09:56 PM
7	test	Admin	<All Accounts>	'Modified':Access Level-'View Only'	Tuesday, December 17, 2013 1:10:42 PM
8	NX3 ONLY	Admin	<All Accounts>	'Added':Access Level-'NX3 ONLY'	Tuesday, December 17, 2013 4:00:35 PM
9	NX3 ONLY	Admin	<All Accounts>	'Modified':Access Level-'View Only'	Tuesday, December 17, 2013 4:00:53 PM
10	Issue:%id->%id	Admin	<All Accounts>	'Added':Card Holder	Tuesday, December 17, 2013 4:00:57 PM
11	10791	Admin	<All Accounts>	'Added':Card	Tuesday, December 17, 2013 4:00:57 PM
12	10791	Admin	Account1	'Modified':Card-' CardNumber:->10791'	Tuesday, December 17, 2013 4:01:20 PM
13	10791	Admin	Account1	'Modified':Card-' CardStatus:INACTIVE->ACTIVE, AccessLevel:[None]->NX3 ONLY'	Tuesday, December 17, 2013 4:01:27 PM
14	<Temporary Record>	Admin	Account1	'Modified':Card Holder-'FName:->Pat,_LName:->French'	Tuesday, December 17, 2013 4:01:27 PM
15	NX3 ONLY	Admin	<All Accounts>	'Modified':Access Level-'View Only'	Tuesday, December 17, 2013 4:02:09 PM
16	Issue:%id->%id	Admin	<All Accounts>	'Added':Card Holder	Tuesday, December 17, 2013 4:03:21 PM
17	49	Admin	Account1	'Modified':Card-' CardHolder:[None],[None]->,'	Tuesday, December 17, 2013 4:03:33 PM
18	<Temporary Record>	Admin	Account1	'Modified':Card Holder-'FName:->Jane,_LName:->Doe'	Tuesday, December 17, 2013 4:03:35 PM

   In this view:

   - The **Card Number /Name** column in the table displays the **Card Number**, **Card Holder Name**, or **Access Level Name** details of the records modified.
   - The **<Temporary Record>** in the **Card Number /Name** column refers to the temporary records that are created when a **Card** or a **Card Holder** is added in the WIN-PAK SE/PE.
   - The **NX3 ONLY** in the **Card Number /Name** column refers to the name of the modified **Access Level**.

Example: The **Card Audit** report in default view.



CARD AUDIT

From: Wednesday, February 12, 2014 12:00:00 AM To: Wednesday, February 12, 2014 11:59:00 PM

Card Number/Name	Operator	Account
Master AL	Admin	<All Accounts>
Action		**Date And Time**
'Added':Access Level='Master AL'		Wednesday, February 12, 2014 9:34:12 AM
Card Number/Name	**Operator**	**Account**
12345	Admin	<All Accounts>
Action		**Date And Time**
'Added':Card		Wednesday, February 12, 2014 9:34:40 AM
Card Number/Name	**Operator**	**Account**
12345	Admin	Account1
Action		**Date And Time**
'Modified':Card=' CardStatus:INACTIVE->ACTIVE, AccessLevel:[None]->Master AL, Activ ationDate:12/31/1969 16:00:00->02/12/2014 00:00:00'		Wednesday, February 12, 2014 9:34:48 AM
Card Number/Name	**Operator**	**Account**
12345	Admin	Account1
Action		**Date And Time**
'Modified':Card=' ExpirationDate:12/31/1969 16:00:00->02/15/2014 00:00:00, CardT ype:Standard->Supervisor, CardType:Non Temporary Card->Temporary Card, CardType: UnLimited Uses->Limited Uses (10)'		Wednesday, February 12, 2014 9:35:00 AM
Card Number/Name	**Operator**	**Account**
12345	Admin	Account1
Action		**Date And Time**
'Modified':Card=' CardNumber:12345->61234'		Wednesday, February 12, 2014 9:35:27 AM
Card Number/Name	**Operator**	**Account**
61234	Admin	Account1
Action		**Date And Time**
'Modified':Card=' CardType:Limited Uses (10)->Limited Uses (100)'		Wednesday, February 12, 2014 9:37:29 AM
Card Number/Name	**Operator**	**Account**
<Temporary Record>	Admin	<All Accounts>
Action		**Date And Time**

Card Frequency Report

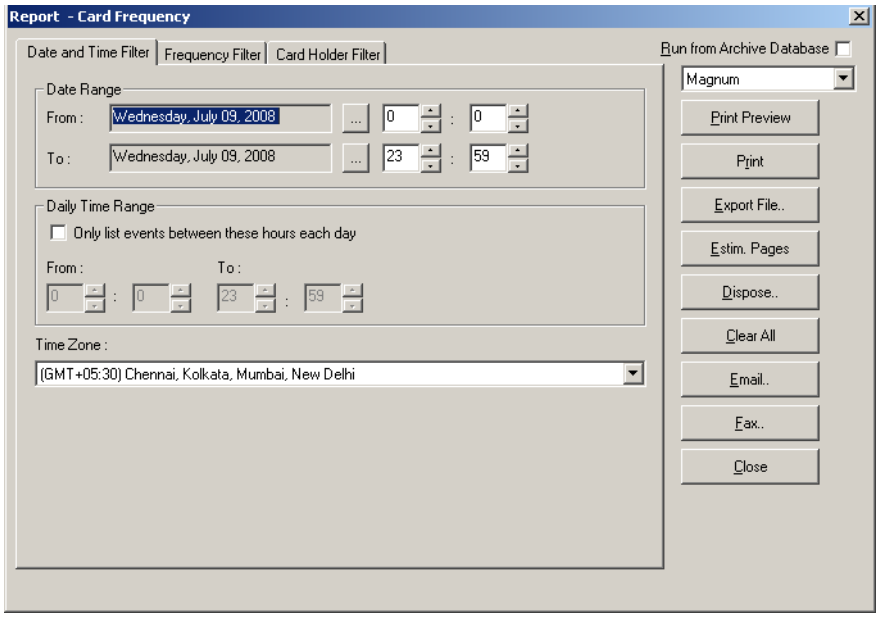
The Card Frequency Report enables you to generate a report to know the number of times a card holder has accessed a particular reader using the card. This report also helps the user to obtain the details of the unused cards and to prevent any misuse of the card.

To generate a card frequency report:

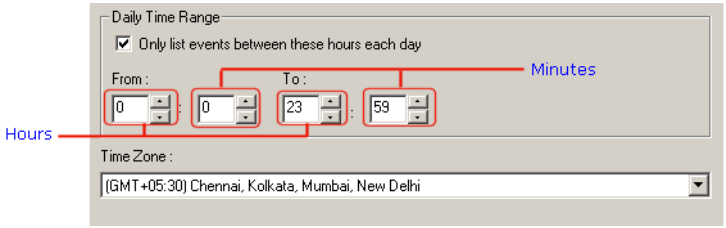
1. In the **Reports** window, select the **Card Frequency** report and click **Report Options**. The **Report - Card** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

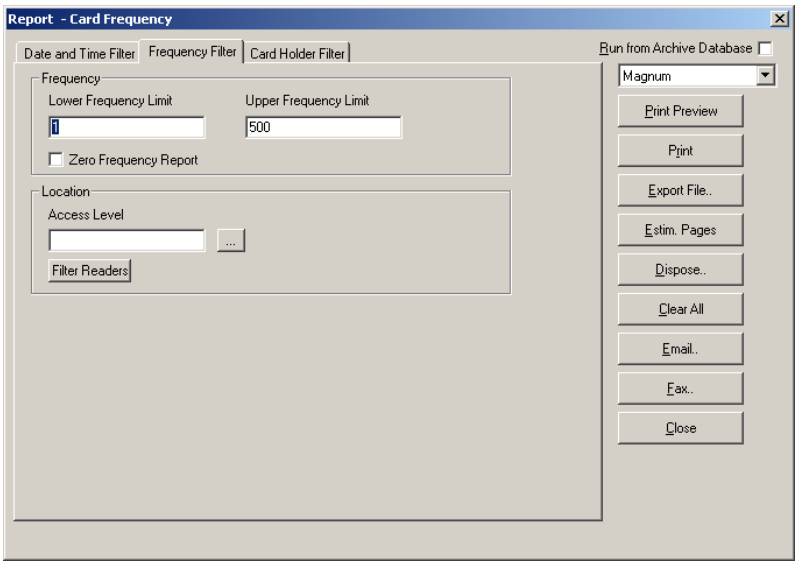
2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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.
4. 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.

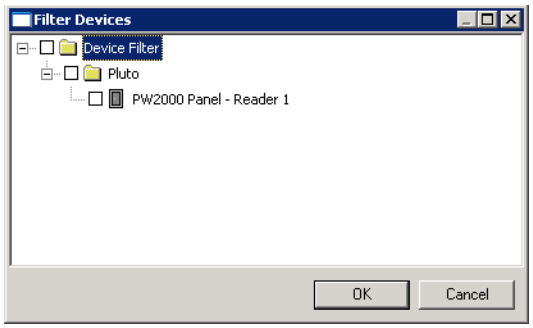
Notes:

- In WIN-PAK CS, if you want to generate a report on cards that are not used, select the **Zero Frequency** check box.
- In WIN-PAK SE/PE, 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.

c. 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.

d. In WIN-PAK, to generate the card frequency reports by filtering the readers:

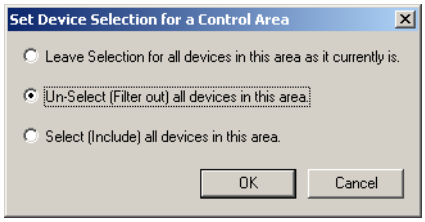
- Click **Filter Readers**. The **Filter Devices** window appears.



- Double-click the branch (folder) to select all the devices in the branch.

OR

- Expand the branch and double-click a device to select the particular device of the branch.The **Set Device Selection for a Control Area** dialog box appears.



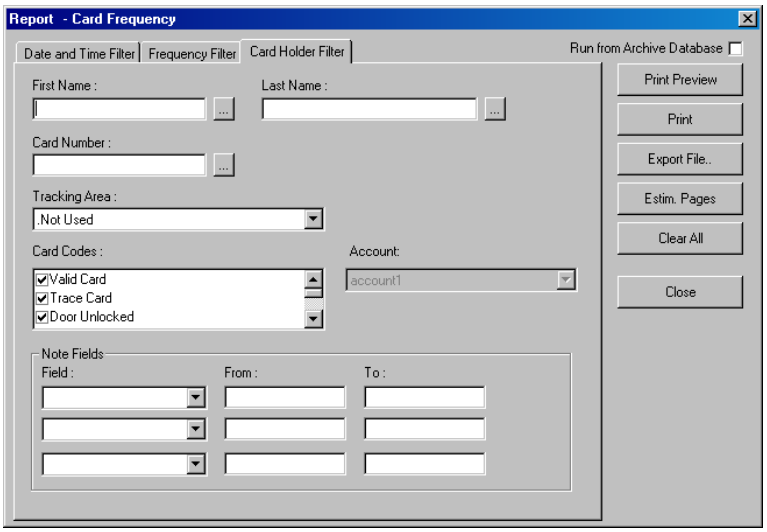
- Click the appropriate option and click **OK**.

e. In WIN-PAK SE/PE, To include only certain devices, Click **Filter ADVs** to select the ADVs. In the **Filter Device** dialog box, select the appropriate ADV or ADV type from the tree and Click **OK**

- Under **Disposition**, select one of the following actions that must be performed on the cards that are filtered for frequency report.

5. 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 the **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.

6. Click **Print Preview** to view the report prior to printing.
7. Click **Print** to print the card frequency report.

Note: Step 8 and 9 is applicable only in WIN-PAK CS.

8. Click **Email..** to send a copy of the report by e-mail, to the customer.
9. Click **Fax..** to fax a copy of the report.
10. Click **Close** to return to the **Reports** window.

Card History Report

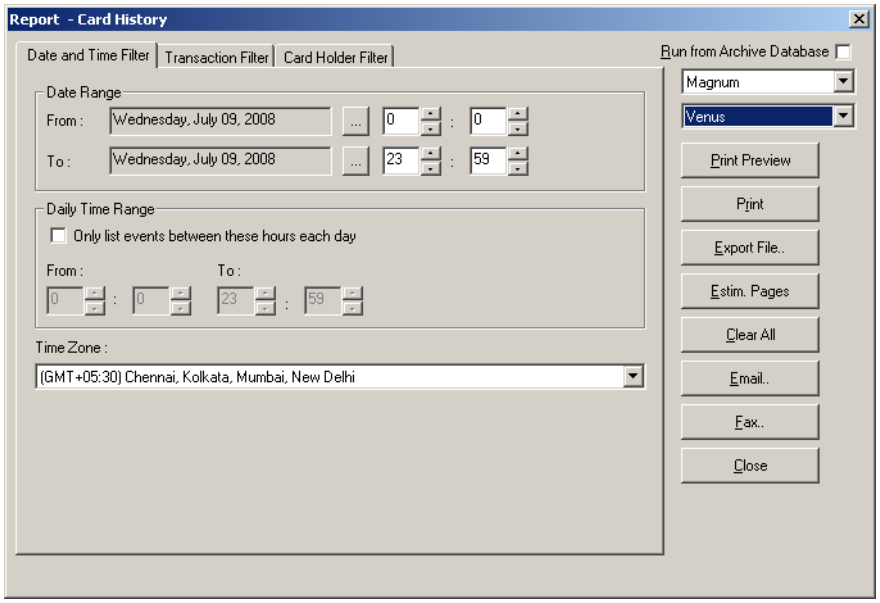
The Card History report contains the history of card transactions and events.

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.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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.

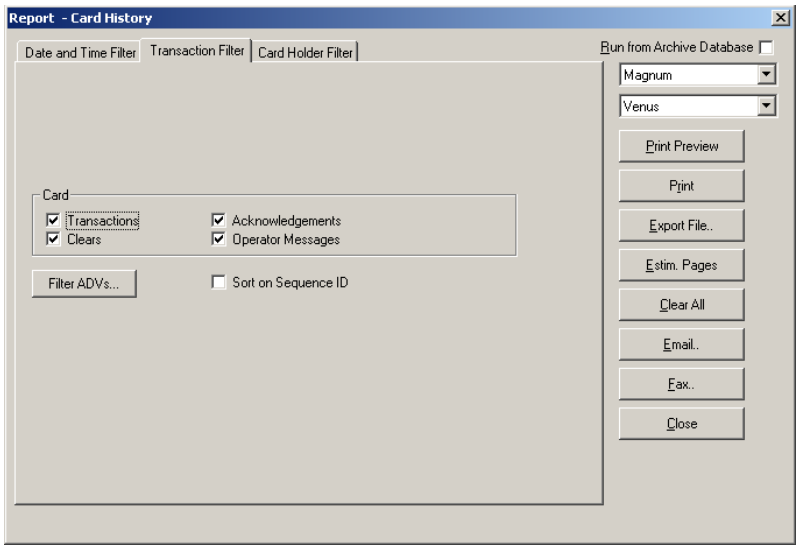
d. To generate reports for events occurring during a particular period, select the **Only list events between these hours each day** check box, under **Daily Time Range**. The **From** and **To** text boxes are enabled.

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.

4. 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 card behaviors, select the following options, under **Card**:

Table 19-6 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.
Acknowledgments	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.

c. To filter the transactions performed on specific ADVs (devices), click **Filter ADVs**. The **Filter Devices** dialog box appears.

d. Double-click the branch (folder) to select all the devices in the branch.

OR

Expand the branch and double-click a device to select the particular device of the branch.

e. Click **OK** to return to the **Report - History** dialog box.

f. Select the **Sort on Sequence ID** check box to sort the report by the sequence number of each action.

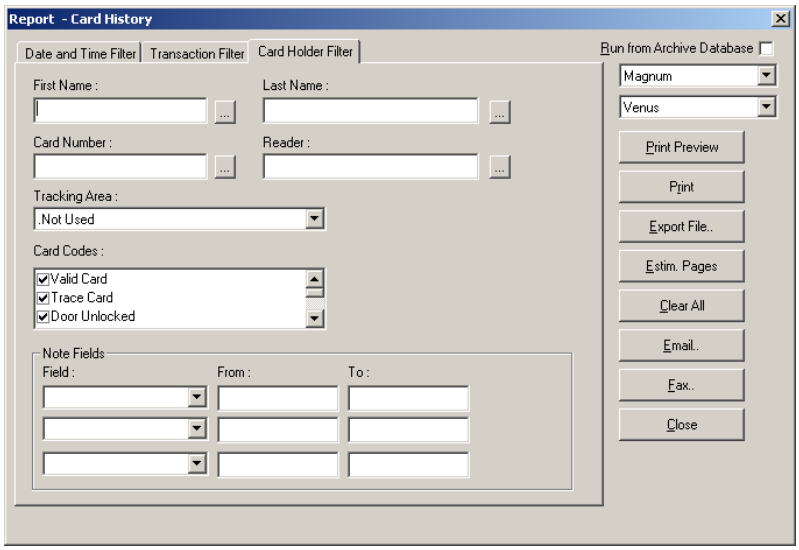
When a new event is identified, it is given a sequence ID and any change in the event carries a new sequence ID.

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.

5. 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.

6. Click **Print Preview** to view the report prior to printing.
7. Click **Print** to print the card history report.

Note: Step 8 and 9 is applicable only in WIN-PAK CS.

8. Click **Email..** to send a copy of the report by e-mail, to the customer.
9. Click **Fax..** to fax a copy of the report.
10. Click **Close** to return to the **Reports** window.

Card Holder Report

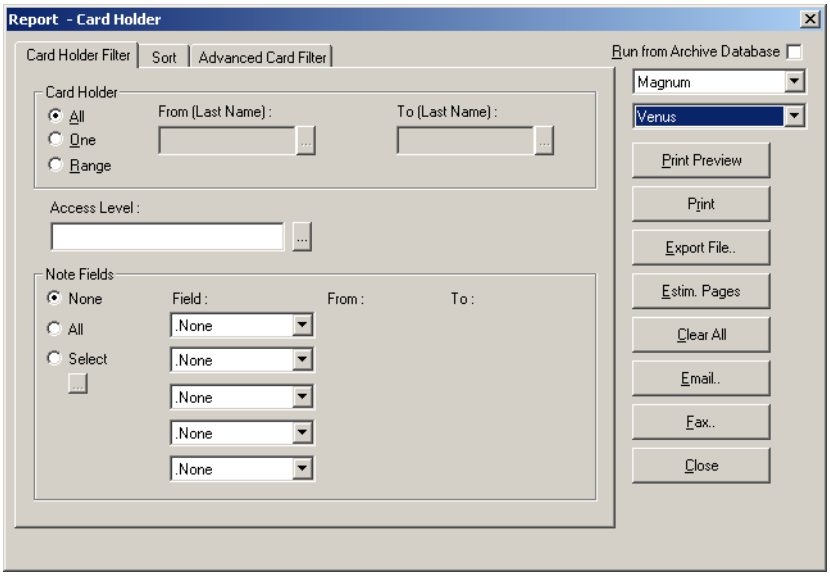
The Card Holder report displays the list of card holder details.

To generate a card holder report:

1. In the **Reports** window, select the **Card Holder** report and click **Report Options**. The **Report - Card Holder** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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 19-7 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/Door-Reader** list.

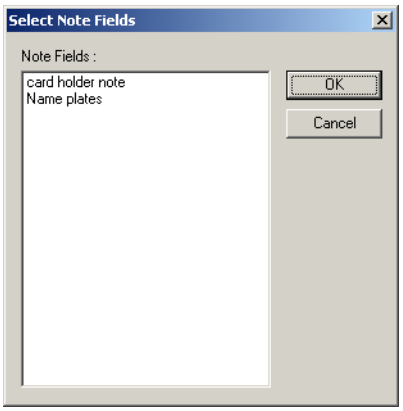
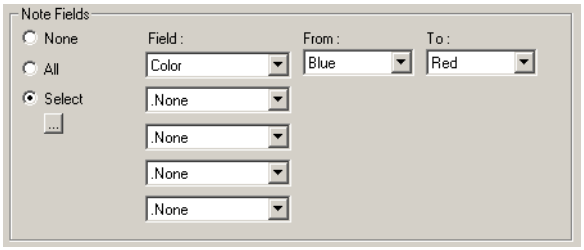
Note: In WIN-PAK, you can also click the **Select Doors/Readers** option to enable the PCI Audit report to display the card holders that have access to the selected doors, including activation/expiration date, and access level details.

d. To include the note fields in the report, select the following options under **Note Fields**.

Table 19-8 Describing the options for filtering note fields

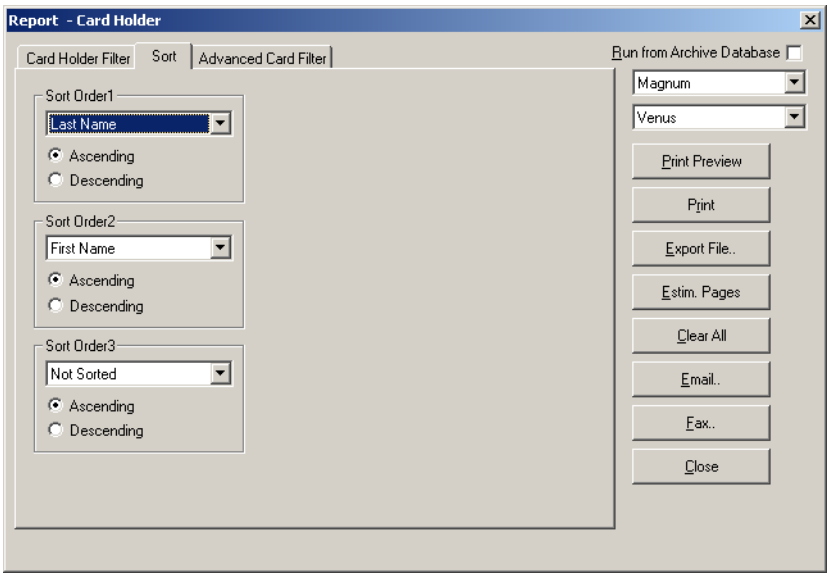
Option	Description
None	To include NO note fields in the report.
All	To include all the note fields in the report.

Table 19-8 Describing the options for filtering note fields

Option	Description
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.
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.

4. 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.

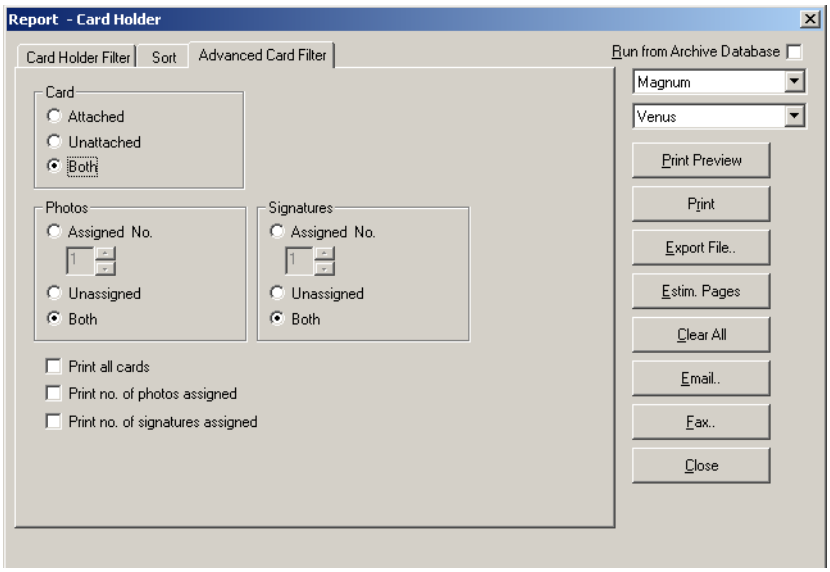
d. Under **Sort Order 2**, select the field by which the report must be sorted in the second level. If you select **Not Sorted** the report is sorted on the basis of the field selected in Sort Order 1.

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.

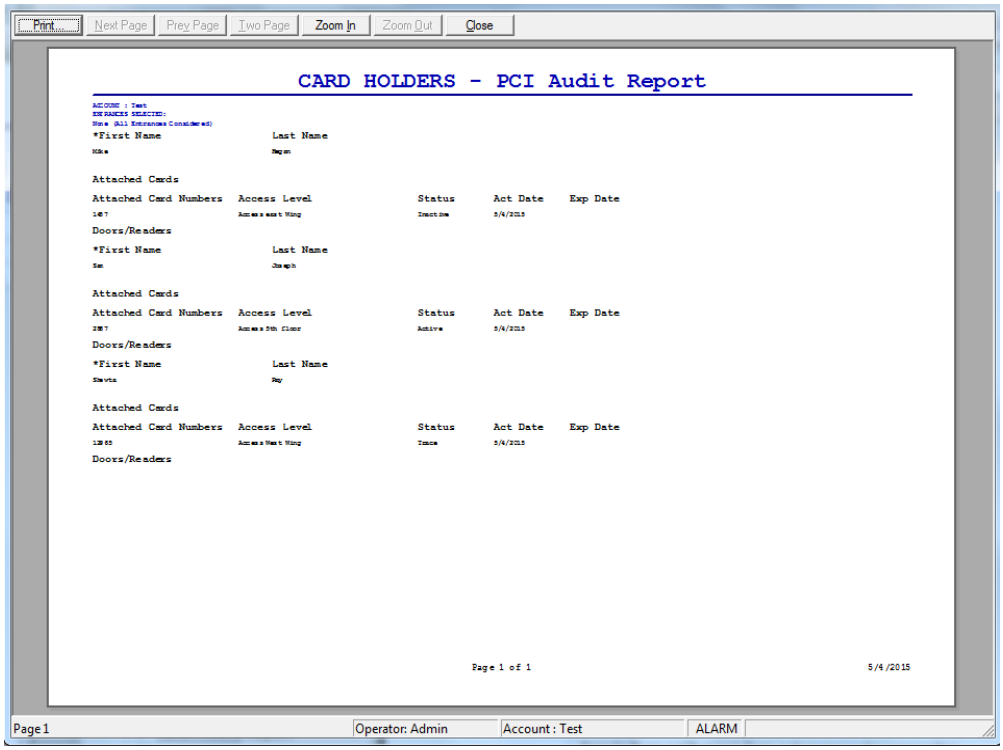
5. To filter the cards based on the card details, click the **Advanced Card Filter** tab.



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.

6. 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**
7. Click **Print Preview** to view the report prior to printing it.



8. Click **Print** to send a copy of the report to your printer.

Note: Step 9 and 10 is applicable only in WIN-PAK CS.

9. Click **Email..** to send a copy of the report by e-mail, to the customer.
10. Click **Fax..** to fax a copy of the report.
11. Click **Close** to return to the **Reports** window.

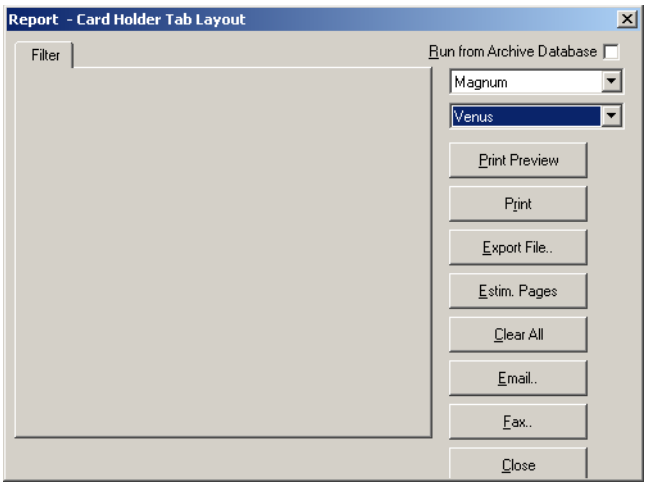
Card Holder Tab Layout Report

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.

Note: Step 2 is applicable only in WIN-PAKCS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



Notes:

- In WIN-PAK CS, the Card Holder Tab Layout report shows the "Note Fields" associated with each Tab on the Card Holder Layout.
- In WIN-PAK SE/PE, 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.

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.

Note: Step 5 and 6 is applicable only in WIN-PAK CS.

5. Click **Email..** to send a copy of the report by e-mail, to the customer.
6. Click **Fax..** to fax a copy of the report.
7. Click **Close** to return to the **Reports** window.

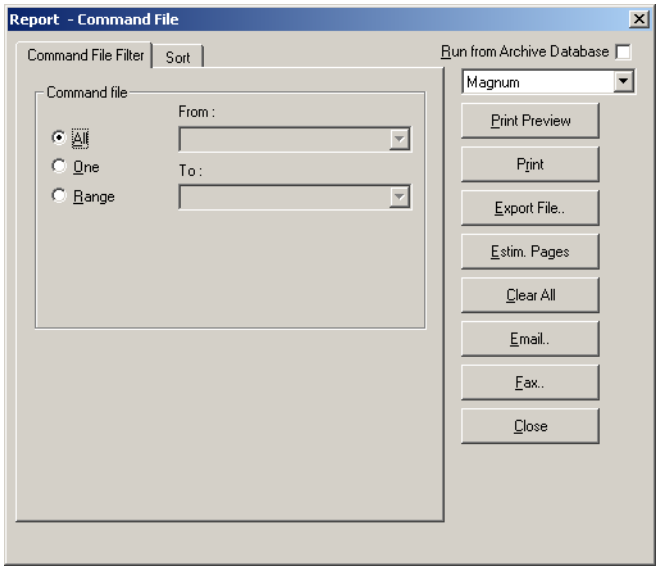
Command File Report

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.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.

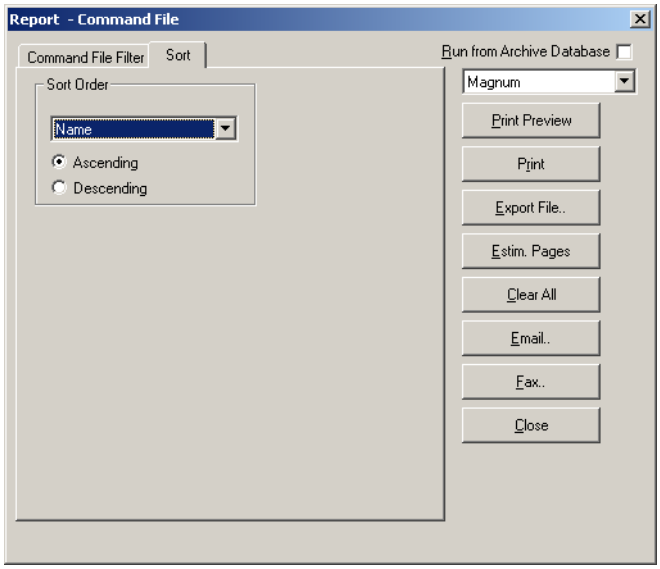


3. To filter command files to be included in the report:
    a. Click the **Command File Filter** tab.
    b. Under **Command File**, select one of the following options:

Table 19-9 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 or type the name of the command file to generate the report.
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**.

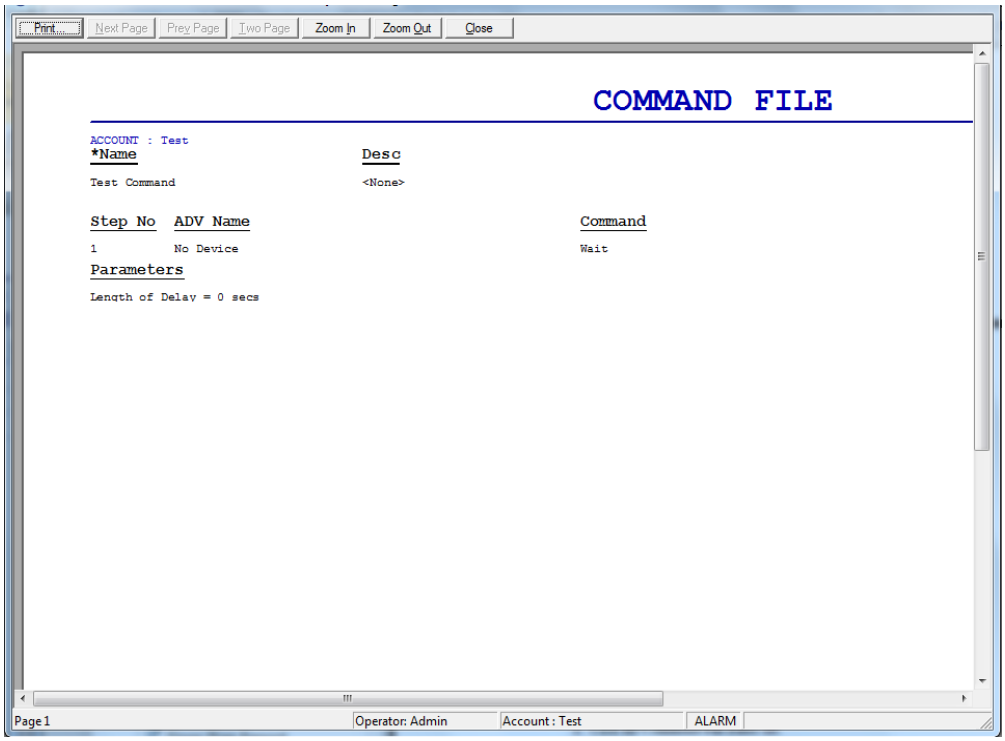
4. To sort the list in the report in the ascending or descending order:
    a. Click the **Sort** tab.



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.



Note: Step 7 and 8 is applicable only in WIN-PAK CS.

7. Click **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.
9. Click **Close** to return to the **Reports** window.

Control Area Report

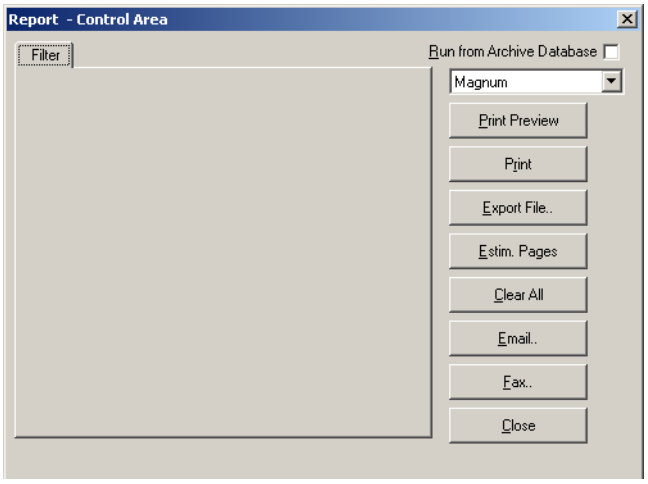
The Control Area report displays the branches or devices that are configured in Control Area.

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.

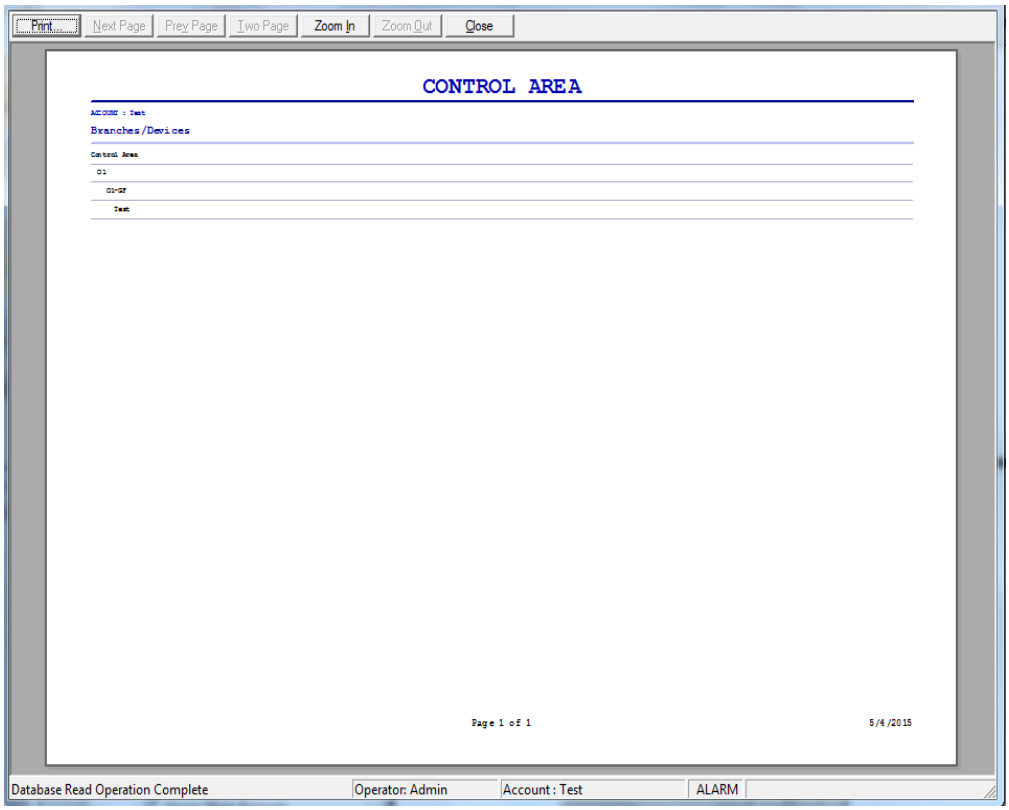
Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



No filter or sort options are provided for the control area report.

3. Click **Print Preview** to view the Access Area Report prior to printing.



4. Click **Print** to send the report to your printer.

Note: Step 5 and 6 is applicable only in WIN-PAK CS.

5. Click **Email..** to send a copy of the report by e-mail, to the customer.
6. Click **Fax..** to fax a copy of the report.
7. Click **Close** to return to the **Reports** window.

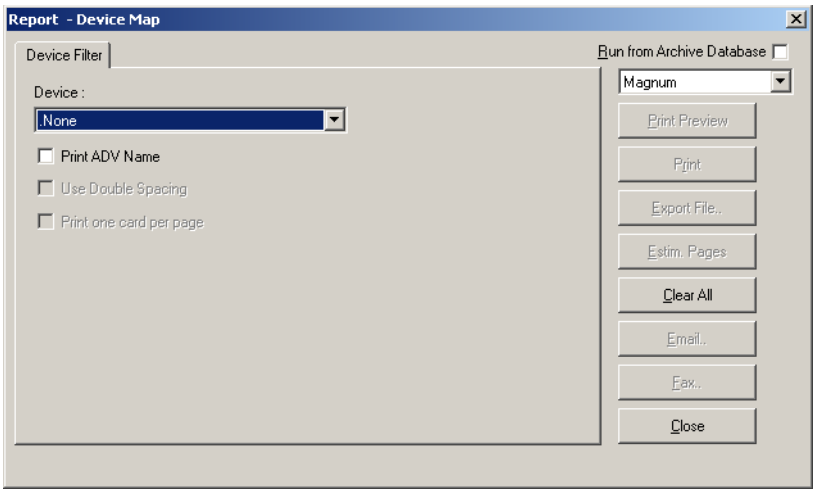
Device Map Report

To generate a device map report:

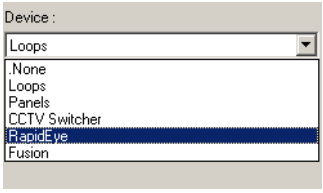
1. In the **Reports** window, select the **Device Map** report and click **Report Options**. The **Report - Device Map** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

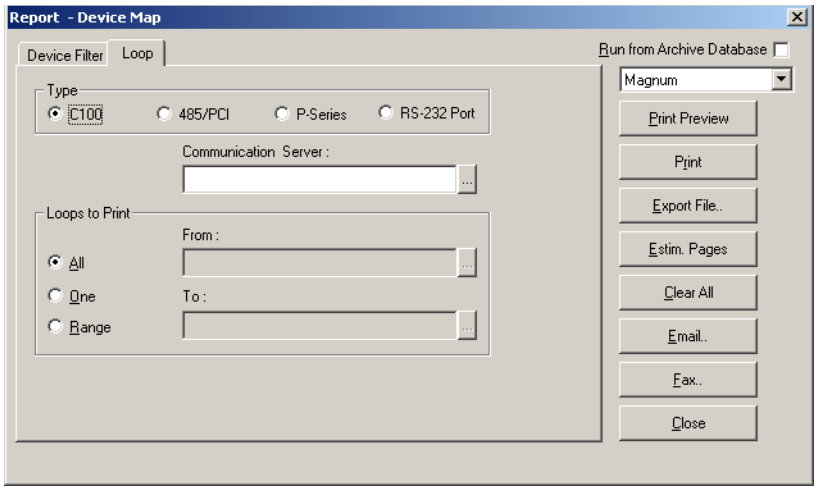
2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. Under **Device Filter**, select the **Print ADV Name** check box to include the abstract device names in the report.
4. 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.
5. Follow the below steps for WIN-PAK CS/SE/PE:
   - **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.

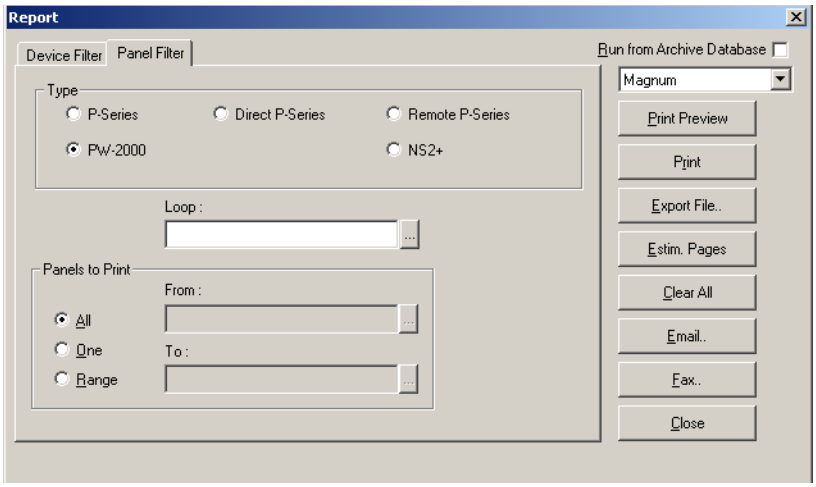
– To select the range of loops:

  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, or NS2+ of the selected loop. Alternatively, the report can display the details of panels of all the loops. There is an additional option to display the details of panels 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, PW-2000** or **NS2+**.

  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 Direct P-Series panel type is selected.
- The Loop option changes to Modem Pool, if the Remote P-Series panel type is selected.

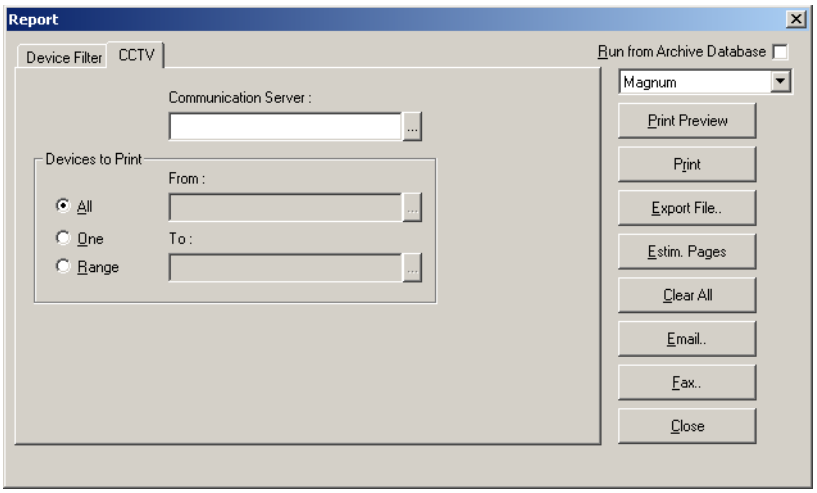
– To select the range of panels:

  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.

CCTV Switcher

– The **Device Map Report** can display the details of a CCTV Switcher of all or the selected communication server. There is an additional option to display the details of all or a range of CCTV switchers.



– To select the server:

  a. Enter the name of the **Communication Server** to include only the CCTV Switchers available in the selected communication server. You can use the ellipsis [...] button to select the communication server.

– To select the range of switchers:

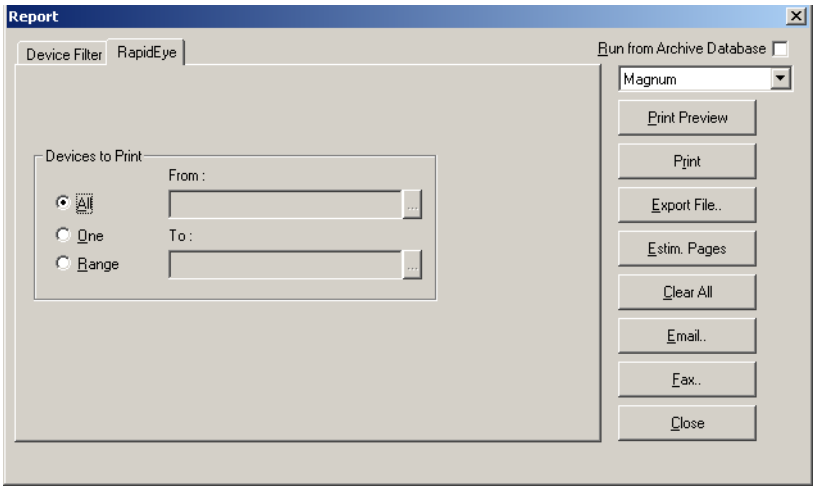
  a. Under **Devices to Print**, select one of the following options:

  - **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 the ellipsis [...] button to select a CCTV switcher.

RapidEye:

Note: **RapidEye** is applicable only in WIN-PAK CS.

– The **Device Map Report** can display the details of all or a range of access DVPROs.



– To select the range of access DVPROs:

a. Click the **Switcher Filter** tab. It is displayed by default when you select the device as **RapidEye**.

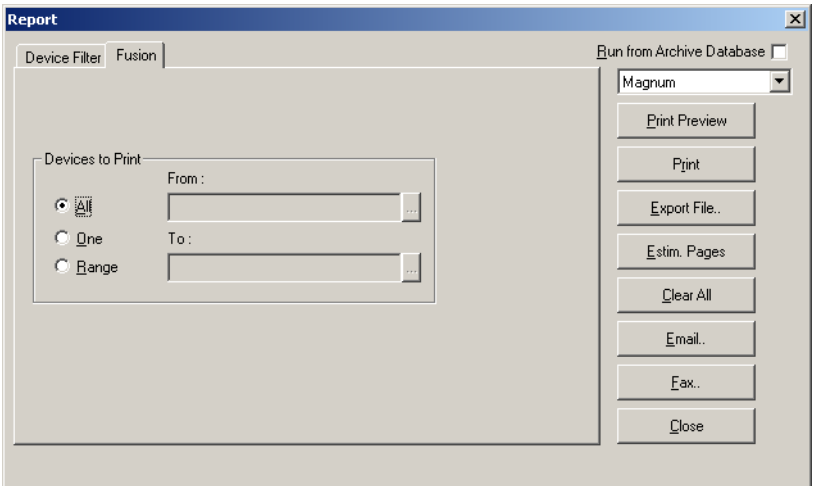
b. Under **Devices to Print**, select one of the following options:

- **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:

Note: **Fusion** is applicable only in WIN-PAK CS.

– The **Device Map Report** can display the details all or a range of Fusion DVR devices.



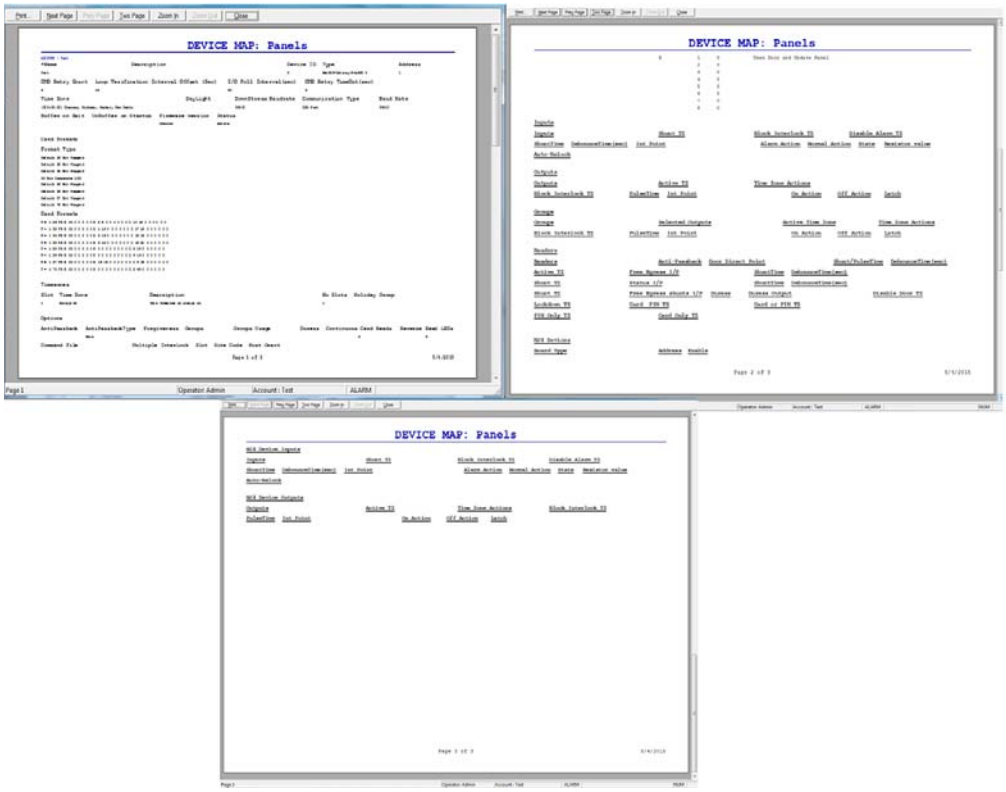
– To select the range of Fusion DVR servers:

  a. Click the **Switcher 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.

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.

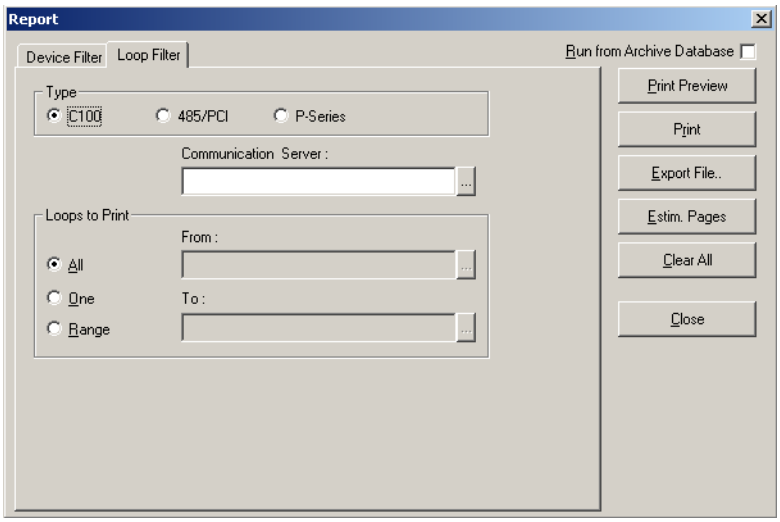
Note: Step 8 and 9 is applicable only in WIN-PAK CS.

8. Click **Email..** to send a copy of the report by e-mail, to the customer.
9. Click **Fax..** to fax a copy of the report.
10. Click **Close** to return to the **Reports** window.

Modem Pools:

Note: **Modem Pools** is applicable only in WIN-PAK SE/PE.

– 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:

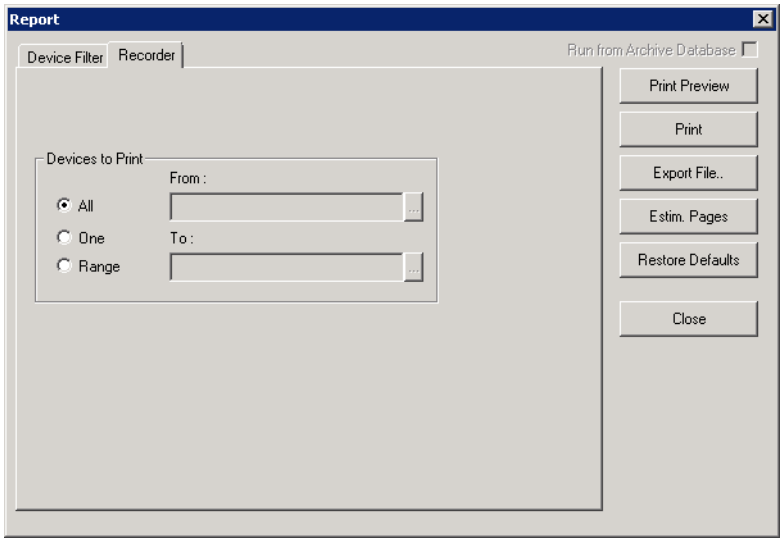
  a. Under **Loops to Print**, select one of the following options:

  * **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.

Recorder:

Note: **Recorder** is applicable only in WIN-PAK SE/PE.

The **Device Map Report** can display the details all or a range of recorders.



– To select the range of recorders:

a. Click the **Recorder** tab. It is displayed by default when you select the device as **Recorder**.

b. Under **Devices to Print**, select one of the following options:

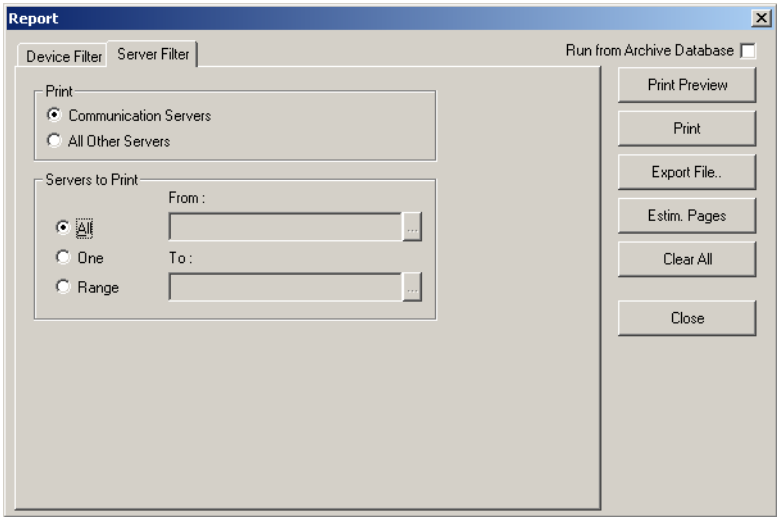
* **All** - to include all the recorders.
* **One** - to include a single recorder that you select in the **From** field.
* **Range** - to include a range of recorders that you select in the **From** and **To** fields.
* You can use the ellipsis button to select an access DVPRO server.

11. Click **Print** to send a copy of the report to your printer.

Servers:

Note: **Servers** is applicable only in WIN-PAK SE/PE.

– 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:

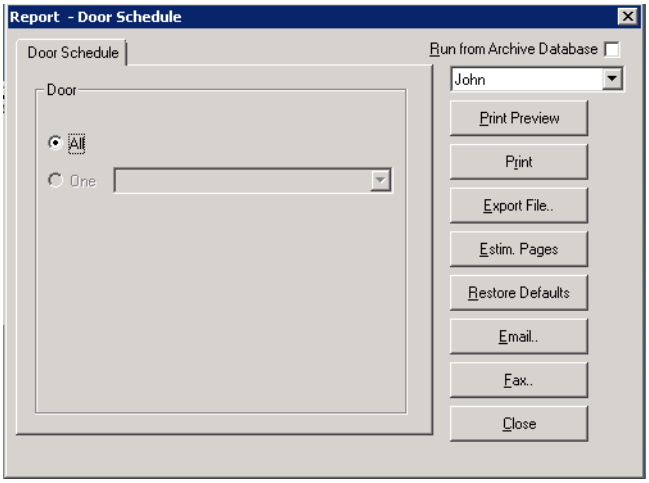
  * **All** - to include all the servers.
  * **One** - to include a single server that you select in the **From** field.
  * **Range** - to include a range of servers that you select in the **From** and **To** fields.
  * You can use the ellipsis button to select a server.

Door Schedule Report

Note: This section is applicable only in WIN-PAK CS.

To generate a door schedule report:

1. In the **Reports** window, select the **Door Schedule** report and click **Report Options**. The **Report - Door Schedule** dialog box appears.
2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. Under **Door Schedule**, a list of all the doors with associated unlocked schedule and associated group names appears.

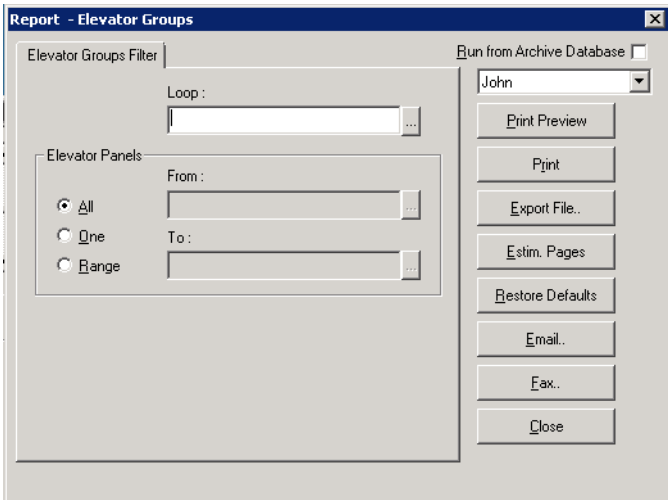
   By default, a report of all the doors is generated. You can filter a single door and view the report, containing the details of associated unlocked schedule and associated group name..

Elevator Groups Report

Note: This section is applicable only in WIN-PAK CS.

To generate a elevator groups report:

1. In the **Reports** window, select the **Elevator Groups** report and click **Report Options**. The **Report - Elevator Groups** dialog box appears.
2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. To filter the elevator groups to be included in the report,
4. Click the **Elevator Groups Filter** tab.

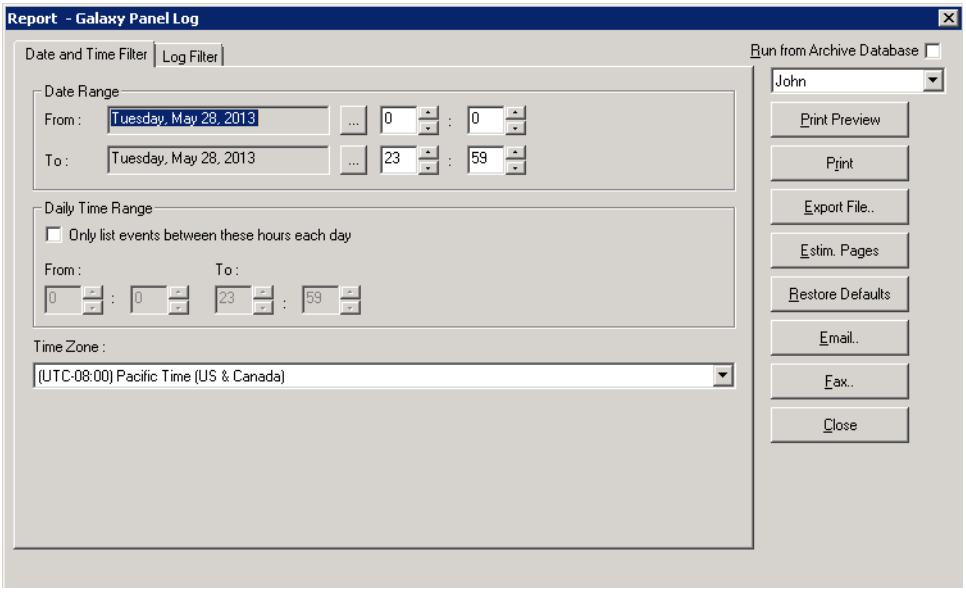
5. Click the ellipsis button to search for the **Loop**. The **Select** dialog box appears.
6. Select an item in **Find Key** and enter the keyword in the **Find What** box.
7. Click **Find**. The loops that match the criteria are listed.

Galaxy Panel Report

Note: This section is applicable only in WIN-PAK CS.

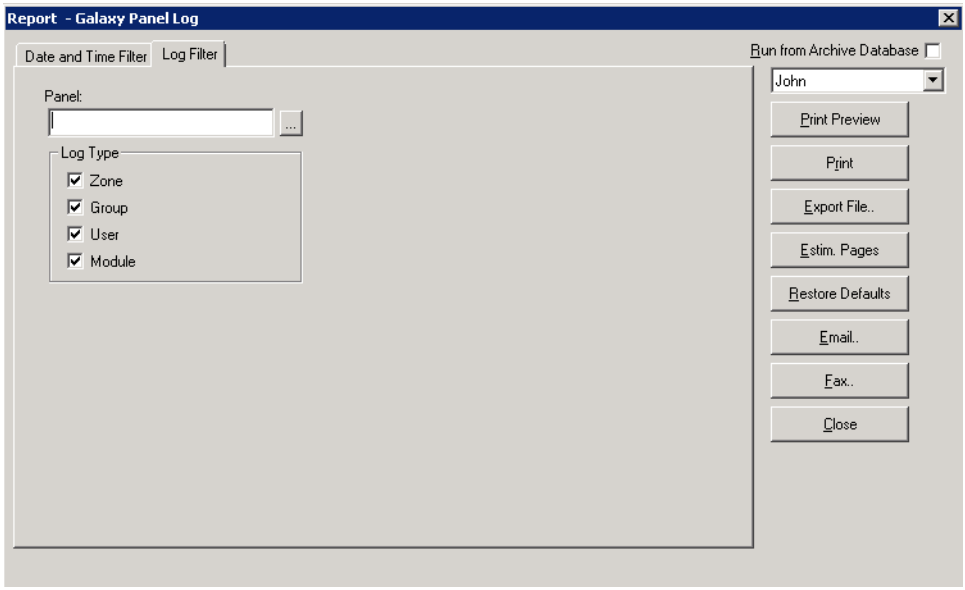
To generate a galaxy panel report:

1. In the **Reports** window, select the **Galaxy Panel** report and click **Report Options**. The **Report - Galaxy Panel** dialog box appears.
2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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.

4. 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.

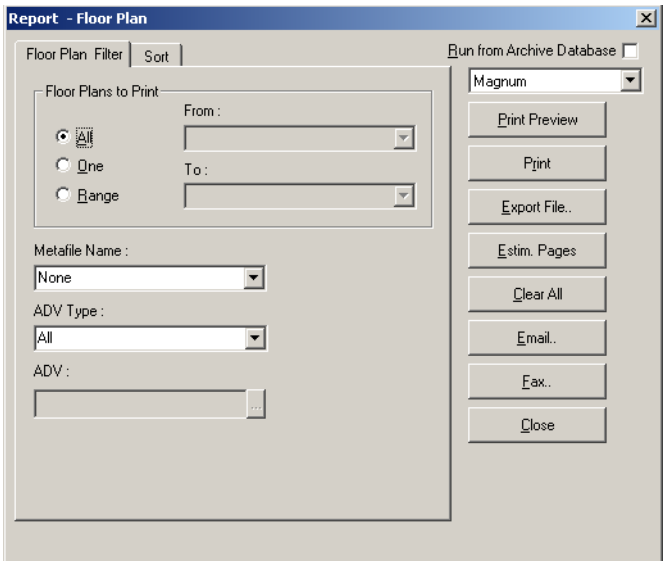
Floor Plan Report

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.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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 19-10 Describing the options for filtering floor plans

Option	Description
All	Generates the report that includes all the floor plans.
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.
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**.

4. To filter floor plans based on metafiles, select the **Metafile Name** in the list.
5. 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.
6. 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.
7. Click **Print Preview** to view the report prior to printing it.

8. Click **Print** to send a copy of the report to your printer.

Note: Step 9 and 10 is applicable only in WIN-PAK CS.

9. Click **Email..** to send a copy of the report by e-mail, to the customer.
10. Click **Fax..** to fax a copy of the report.
11. Click **Close** to return to the **Reports** window.

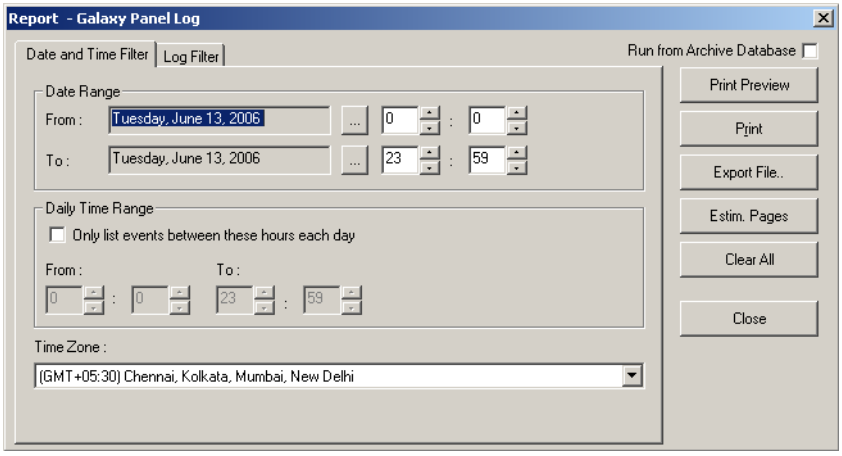
Galaxy Panel Log Report

Galaxy Panel Log report is used for tracking the events happening at the Galaxy panel. This report can be generated if you have procured the license for the Galaxy feature in WIN-PAK SE/PE.

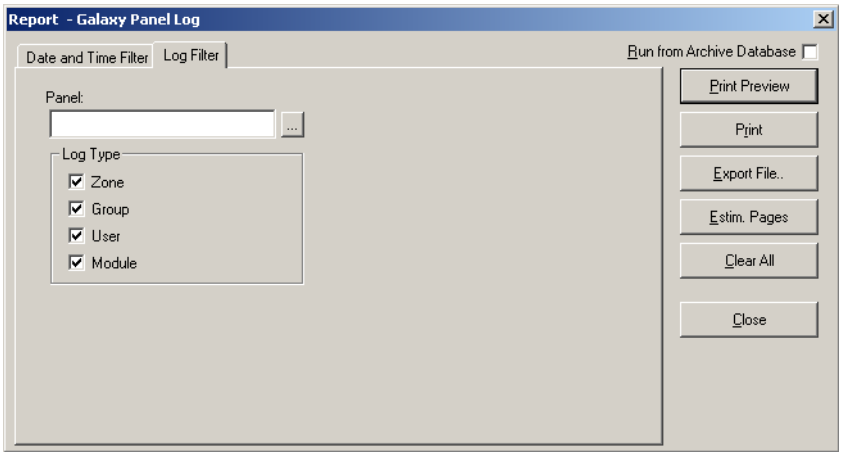
Note: This section is applicable only in WIN-PAK SE/PE.

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** to send a copy of the report to your printer.

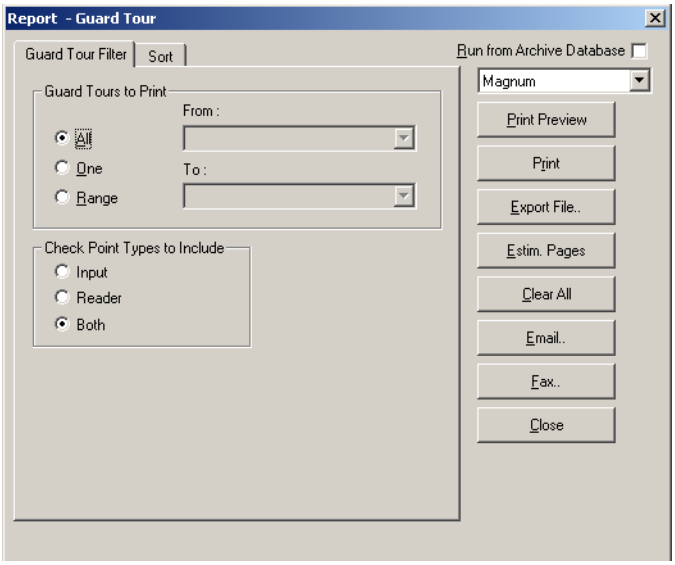
Guard Tour Report

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.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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 19-11 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.

Table 19-11 Describing the options for filtering guard tours

Option	Description
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**.

4. To filter the check point types, select one of the **Check Point Type to Include** options.
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.

Note: Step 8 and 9 is applicable only in WIN-PAK CS.

8. Click **Email..** to send a copy of the report by e-mail, to the customer.
9. Click **Fax..** to fax a copy of the report.
10. Click **Close** to return to the **Reports** window.

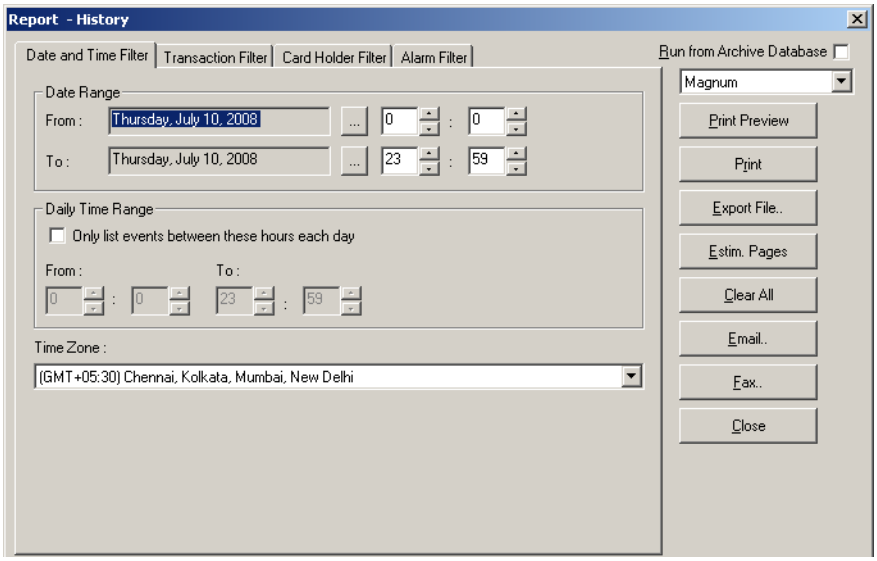
History Report

To generate a history report:

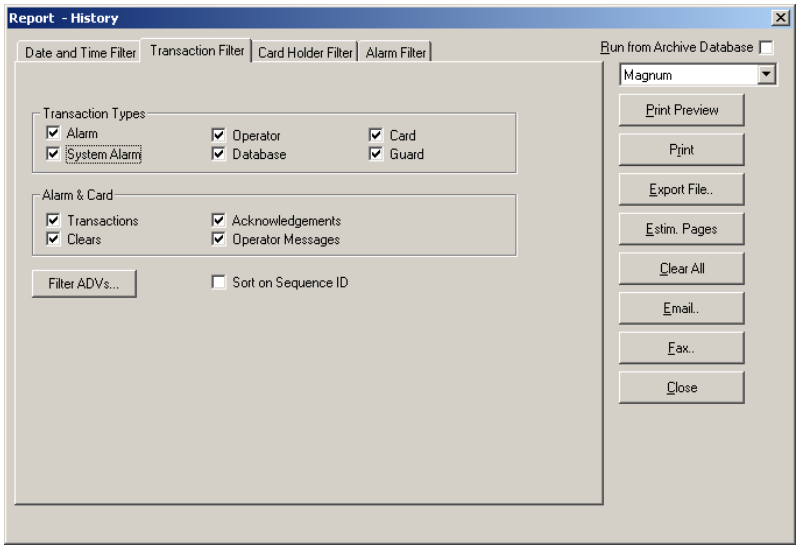
1. In the **Reports** window, select the **History** report and click **Report Options**. The **Report - History** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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.
4. 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 19-12 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 19-13 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.

Table 19-13 Describing the Alarm & Card options for filtering history details

Card Option	Description
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.

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.

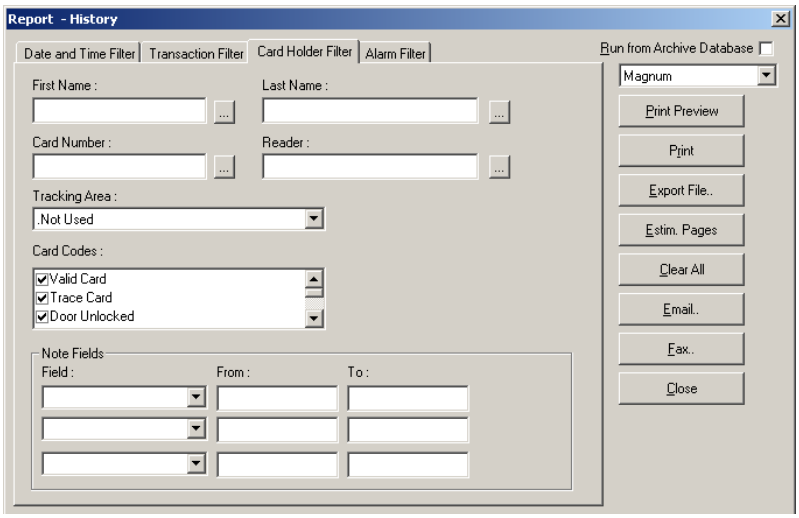
When a new event is identified, it is given a sequence ID and any change carries a new sequence ID.

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.

5. 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.

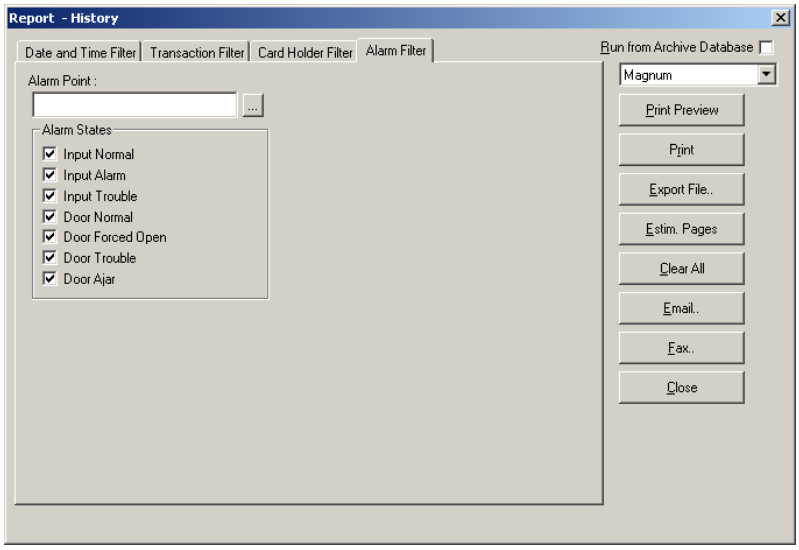
e. Select one or more **Card Codes** which define the card transaction.

f. Select the **Note Fields** to be displayed in the report. You can also specify the range if you select the numerical note field.

Note: The options in **Card Holder Filter** tab are enabled, only if you have selected **Card** transaction type in the **Transaction Filter** tab.

6. To filter further on alarm events:

   a. Click the **Alarm Filter** tab.

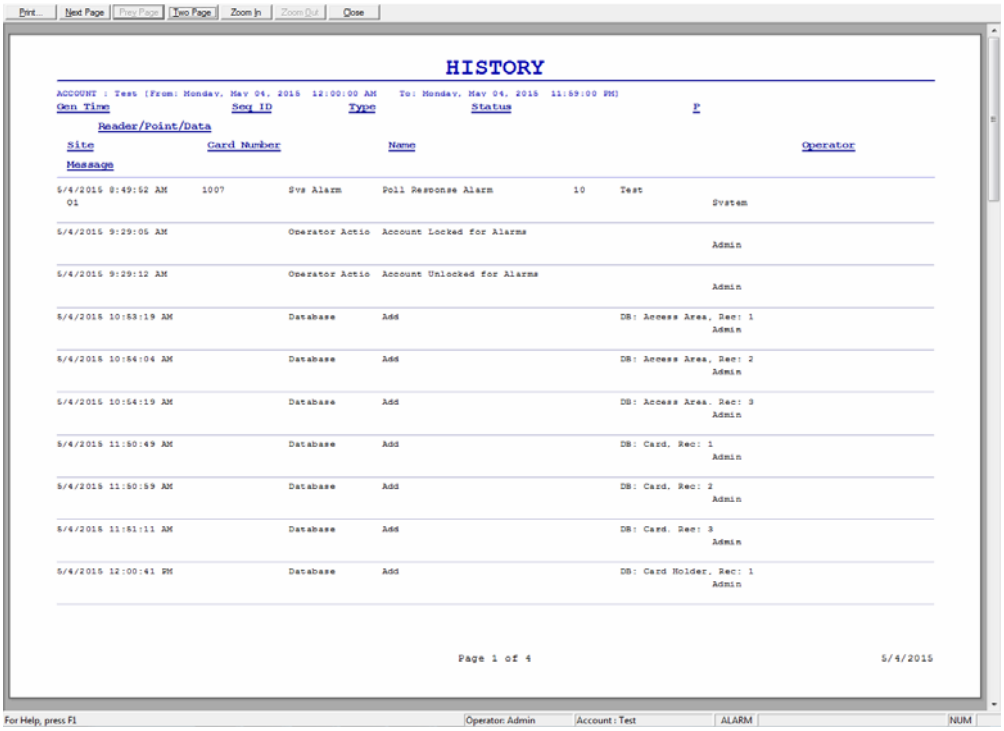


b. In the **Alarm Point** text box, enter the device or point name. You can also use the ellipsis button to find the device or point on which the alarms to be viewed.

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.

7. Click **Print Preview** to view the report prior to printing.



8. Click **Print** to print the card history report.

Note: Step 9 and 10 is applicable only in WIN-PAK CS.

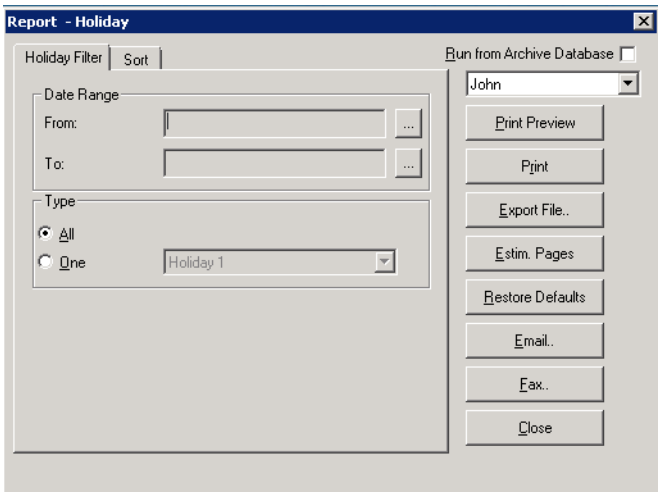
9. Click **Email..** to send a copy of the report by e-mail, to the customer.
10. Click **Fax..** to fax a copy of the report.
11. Click **Close** to return to the **Reports** window.

Holiday Report

Note: This section is applicable only in WIN-PAK CS.

To generate a holiday report:

1. In the **Reports** window, select the **Holiday** report and click **Report Options**. The **Report - Holiday** dialog box appears.
2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. To filter the holiday to be included in the report,
   a. Click the **Holiday Filter** tab.
   b. Under **Date Range Group**, select one of the following options:

Table 19-14 Describing the options for filtering holiday

Option	Description
From	Click the ellipsis button to select the from date.
To	Click the ellipsis button to select the to date.

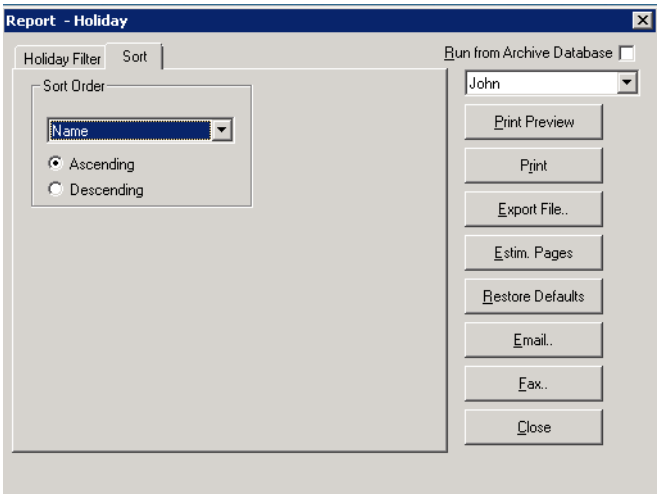
c. Under **Type**, select one of the following options:

Table 19-15 Describing the options for filtering holiday types

Option	Description
All	Click this option to select all the holidays.
One	Click this option to select only a particular holiday.

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.

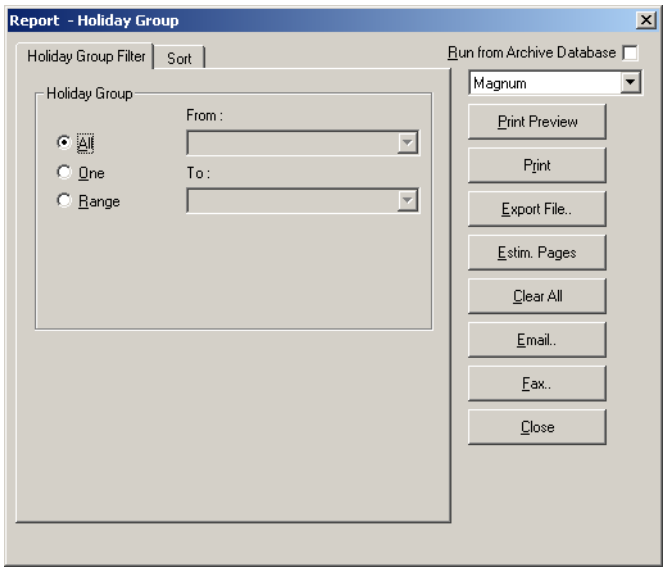
Holiday Group Report

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.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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 19-16 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.

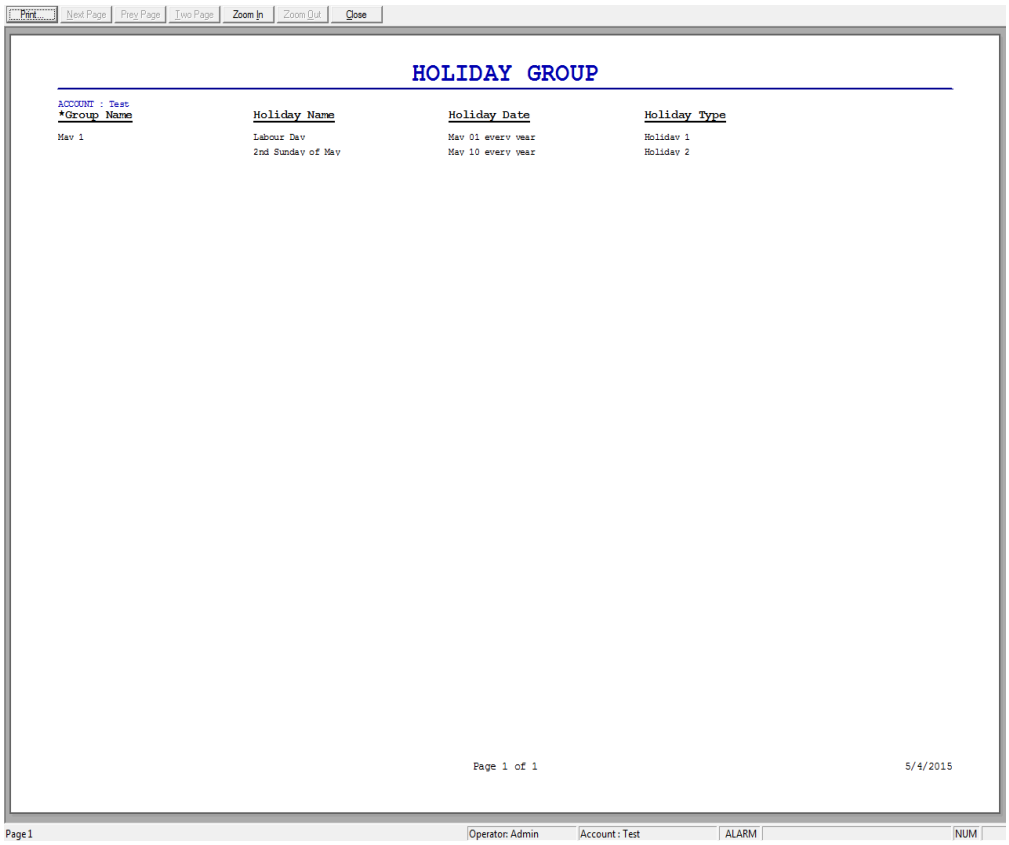
4. To sort the list in the report in the ascending or descending order:

   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.

Note: Step 7 and 8 is applicable only in WIN-PAK CS.

7. Click **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.
9. Click **Close** to return to the **Reports** window.

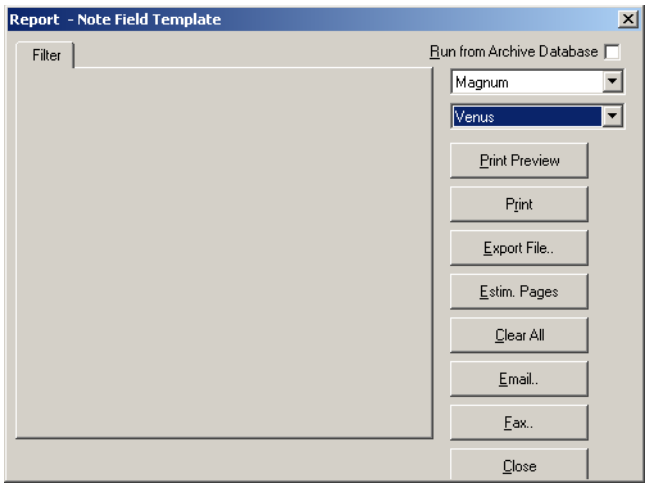
Note Field Template Report

To generate an access area report:

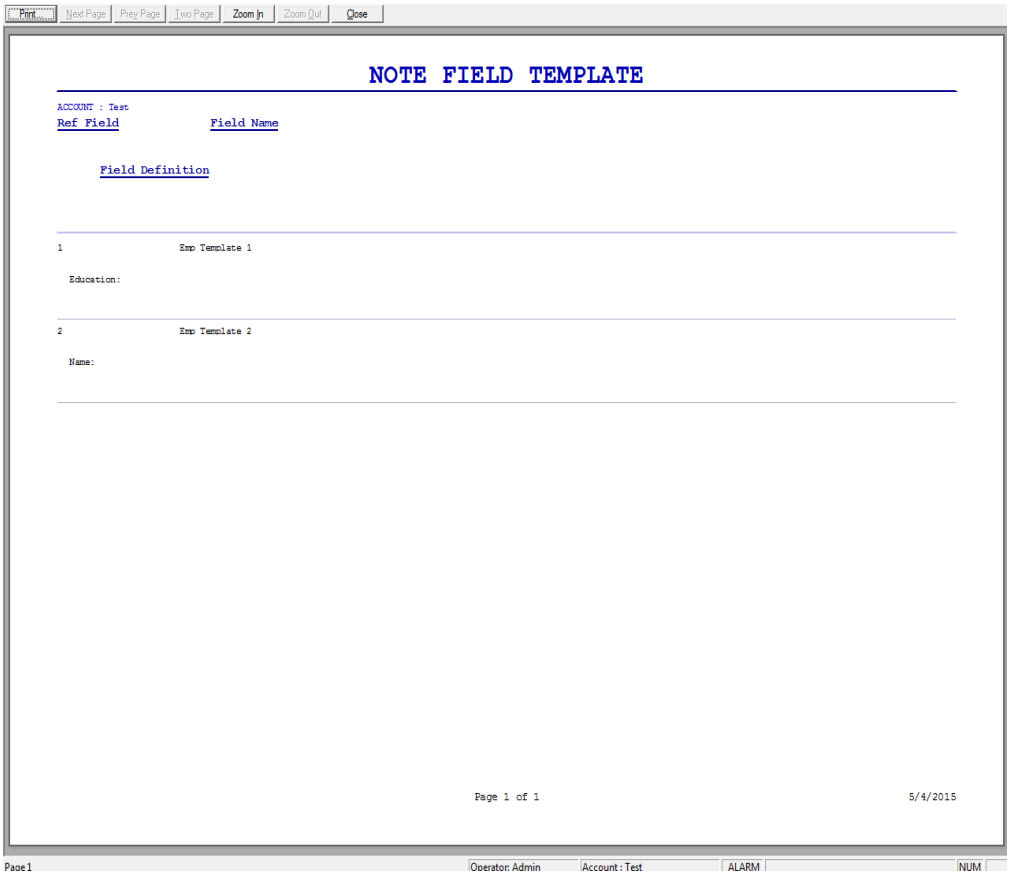
1. In the **Reports** window, select the **Access Area** report and click **Report Options**. The **Report - Access Area** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. Click **Print Preview** to view the report prior to printing.



4. Click **Print** to send the report to your printer.

Note: Step 5 and 6 is applicable only in WIN-PAK CS.

5. Click **Email..** to send a copy of the report by e-mail, to the customer.
6. Click **Fax..** to fax a copy of the report.

7. Click **Close** to return to the **Reports** window.

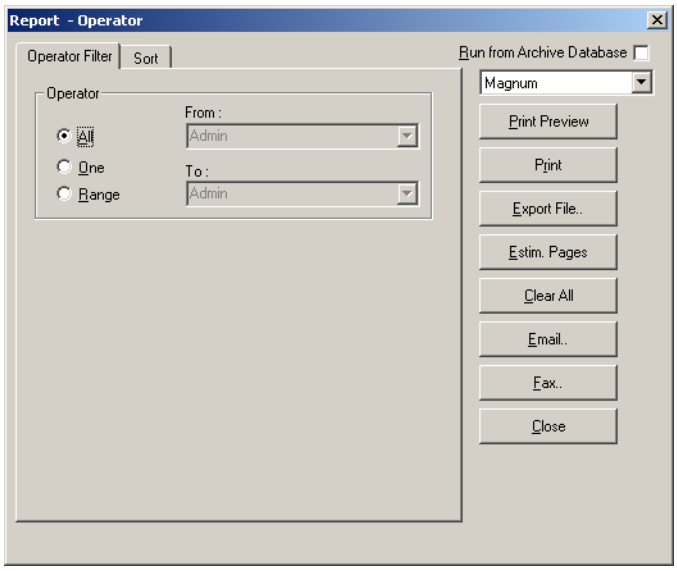
Operator Report

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.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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:

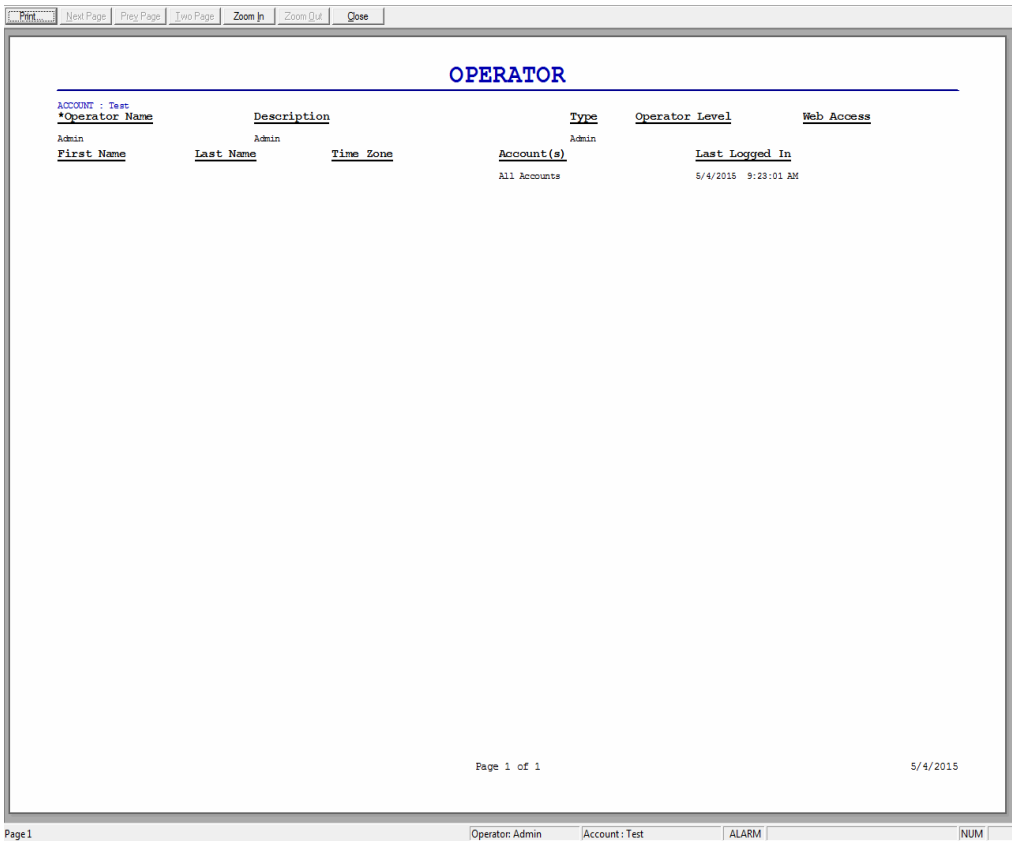
Table 19-17 Describing the options for filtering operators

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.

Table 19-17 Describing the options for filtering operators

Option	Description
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.

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.

Note: Step 7 and 8 is applicable only in WIN-PAK CS.

7. Click **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.
9. Click **Close** to return to the **Reports** window.

Operator Audit Report

Note: This section is applicable only in WIN-PAK CS.

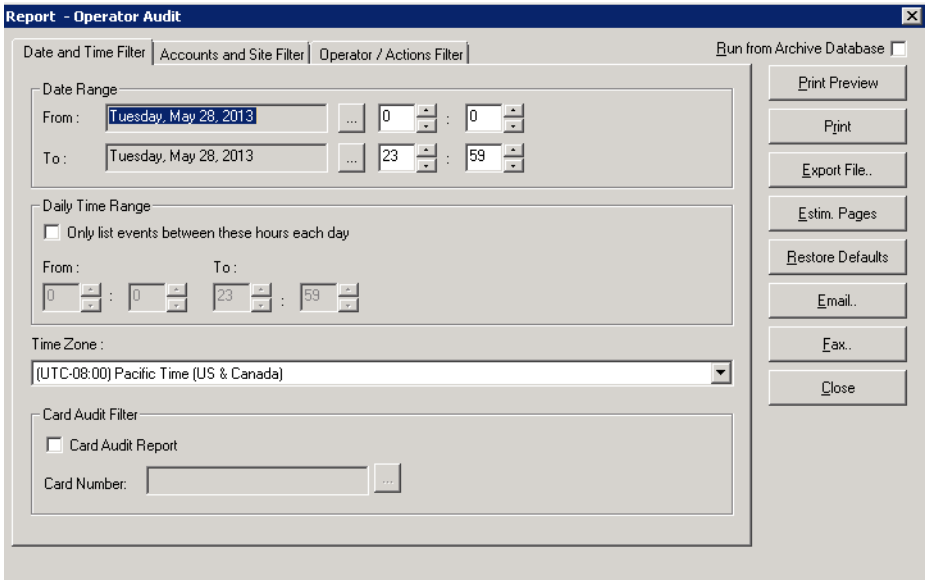
The Operator Audit report consists of a record of all the operations performed on an account by an operator, along with the exact time of their execution.

The Administrator can generate an operator audit report to monitor an operator's performance.

The filtering for this report can be on the basis of the specified duration, accounts, operators, and operator actions.

To generate an operator actions report:

1. In the **Reports** window, select the **Operator Audit** report and click **Report Options**. The **Report - Operator Audit** dialog box appears.



2. To filter the records based on the specific date and time ranges:
   a. Under **Date Range**, select the **From** and **To** dates using the ellipsis button.
   b. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.
   c. 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.

d. In the **From** and **To** boxes, enter the time range (in hours and minutes).

e. Select the standard time zone in the **Time Zone** list.

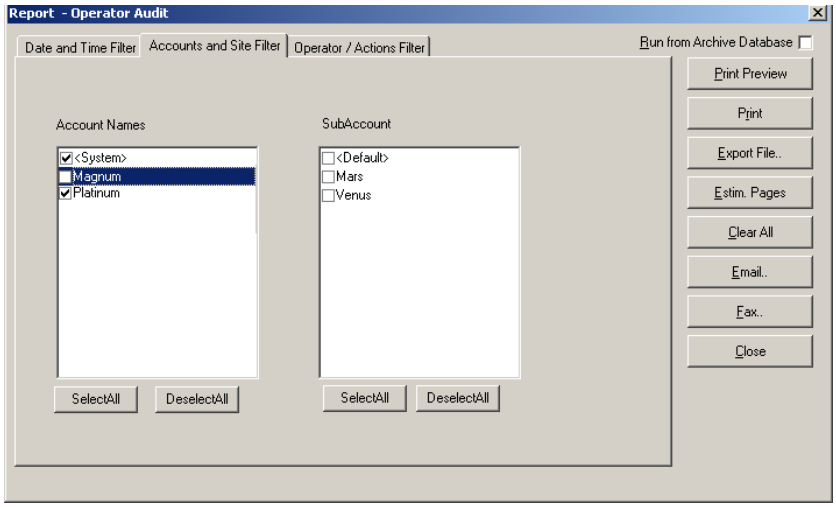
f. Under **Card Audit Filter**, select **Card Audit Report**.

Notes:

- The **Accounts and Site Filter** tab is disabled
- The **Operator Actions** box in the **Operator/Actions Filter** tab is unavailable.

3. To filter the specific accounts:

   a. Click the **Accounts and Site Filter** tab.

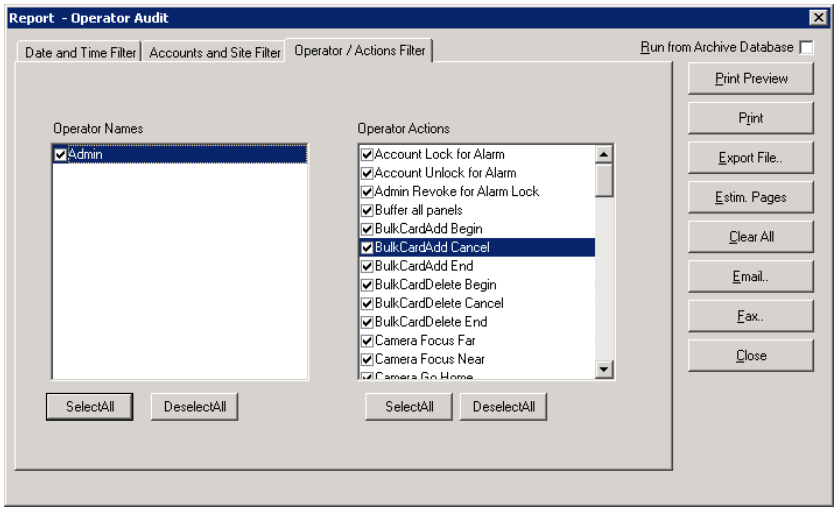


   b. Under **Account Names**, select or clear the accounts to be included or excluded. By default all the accounts are selected.

      Tip: Click **Select All** to select all the accounts or click **Deselect All** to clear the selection of all the accounts.

4. To filter only the specific operator actions:

   a. Click the **Operator/ Actions Filter** tab.

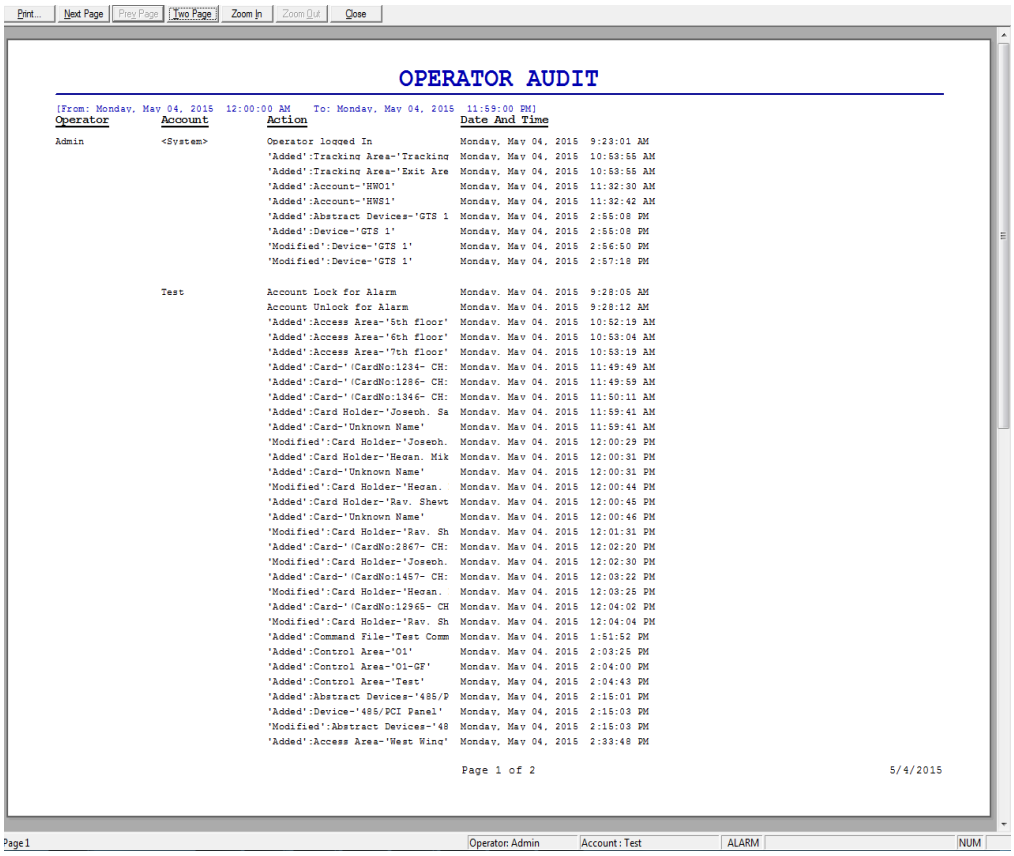


b. Under Operator Names select or clear the operator names to be included or excluded. By default, all the operator names are selected.

c. 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.

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 **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.
9. Click **Close** to close **Operator Actions Report dialog** box.

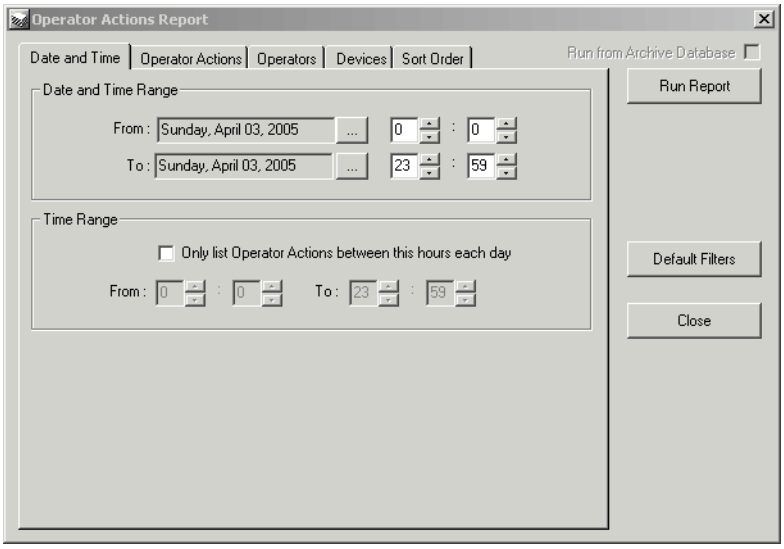
Operator Actions Report

Note: This section is applicable only in WIN-PAK SE/PE.

The Operator Actions report is an Audit Report for the Administrator to monitor the actions performed by the operator using WIN-PAK SE/PE 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.

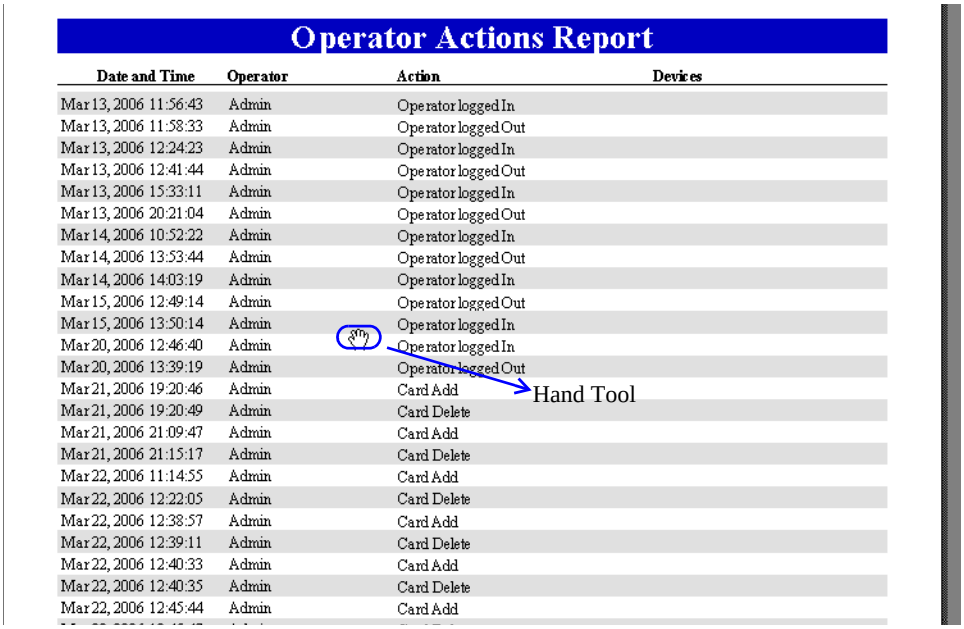
5. To filter the devices on which the actions are performed:

   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**.
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 19-18 Defining toolbar buttons

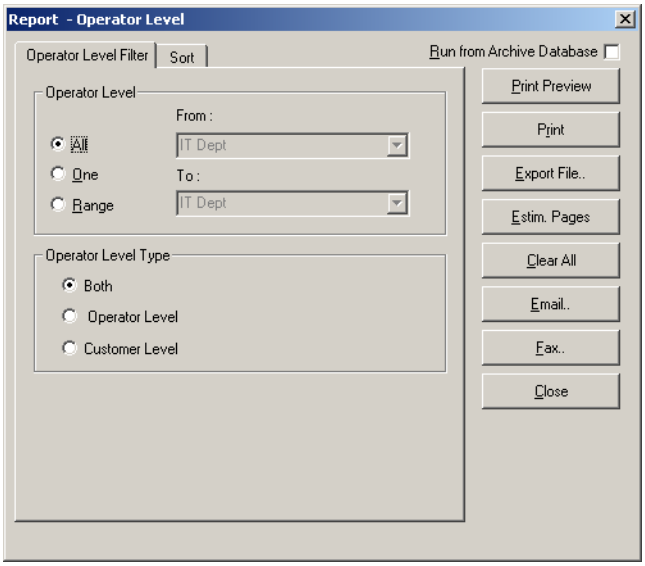
Toolbar button	Description
Print	Sends the report to the printer.
Copy	Copies the content of the report and it can be pasted in any of the text applications like Word, Excel, Notepad.
Find	Searches for a particular text in the report. When you click this button, the **Find** dialog box appears. Enter 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.
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.

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 Level** 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 19-19 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.
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**.

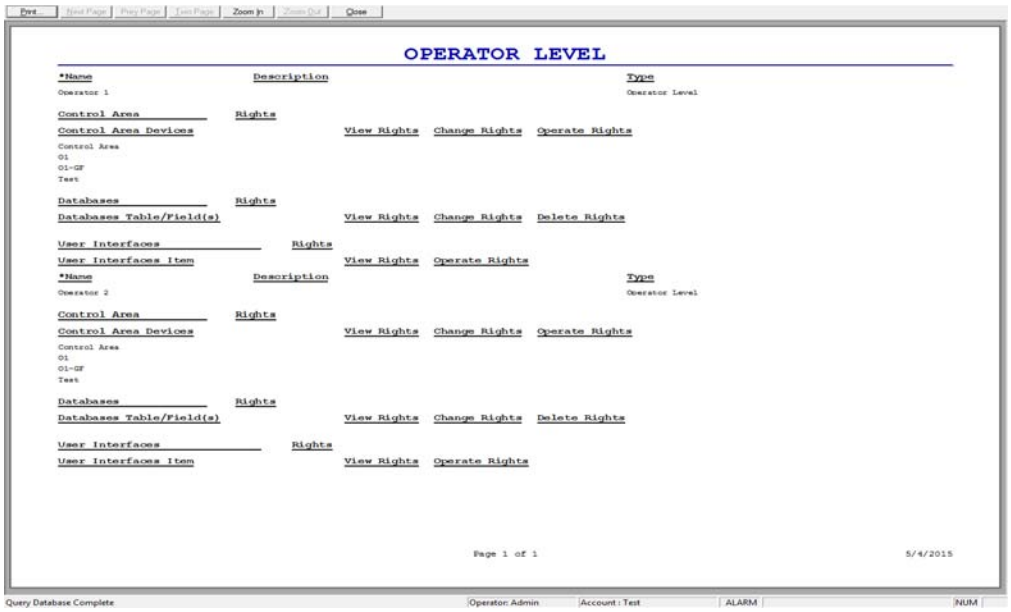
Note: On the basis of the operator type selection, the operator level or customer level report is generated.

c. Under **Operator Level Type** select one of the following options:

Table 19-20 Describing the options for filtering operator level types

Option	Description
Both	Generates the report that includes the operator levels and customer levels.
Operator Level	Generates the report for only the operator levels.
Customer Level	Generates the report for only the customer levels.

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.

Note: Step 6 and 7 is applicable only in WIN-PAK CS.

6. Click **Email..** to send a copy of the report by e-mail, to the customer.
7. Click **Fax..** to fax a copy of the report.
8. Click **Close** to return to the **Reports** window.

Operator Summary Report

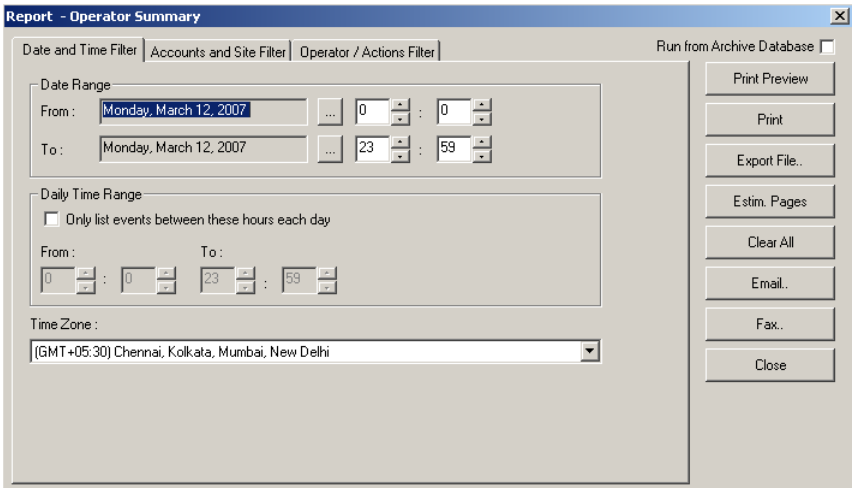
Note: This section is applicable only in WIN-PAK CS.

The Operator Summary report is a report of all the important actions performed by an operator on an account, with an exact count of the number of times each action was executed.

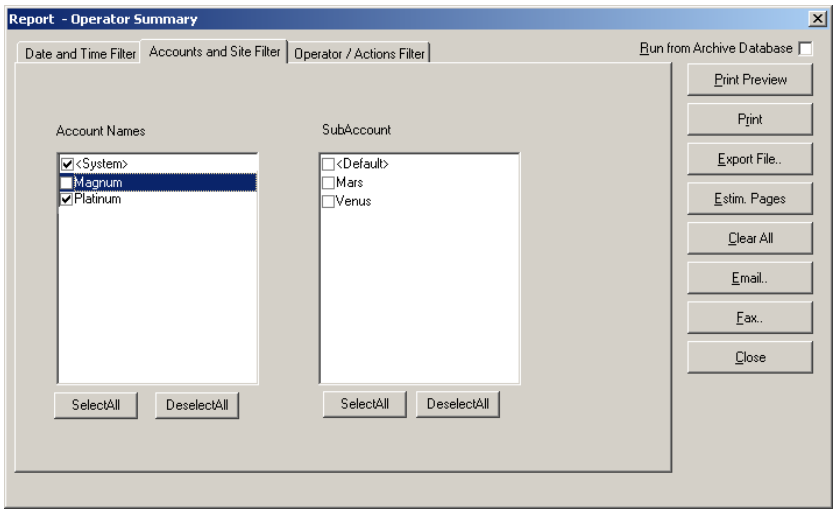
This report can be generated based on the accounts, operators, and operator actions.

To generate an operator actions report:

1. In the **Reports** window, select the **Operator Summary** report and click **Report Options**. The **Report - Operator Summary** dialog box appears.



2. To filter the records based on the specific date and time ranges:
    a. Under **Date Range**, select the **From** and **To** dates using the ellipsis button.
    b. Enter the **From** and **To** time (in hours and minutes) in the corresponding boxes.
    c. 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.
    d. In the **From** and **To** boxes, enter the time range (in hours and minutes).
    e. Select the standard time zone in the **Time Zone** list.
3. To filter the specific accounts:
    a. Click the **Accounts and Site Filter** tab.

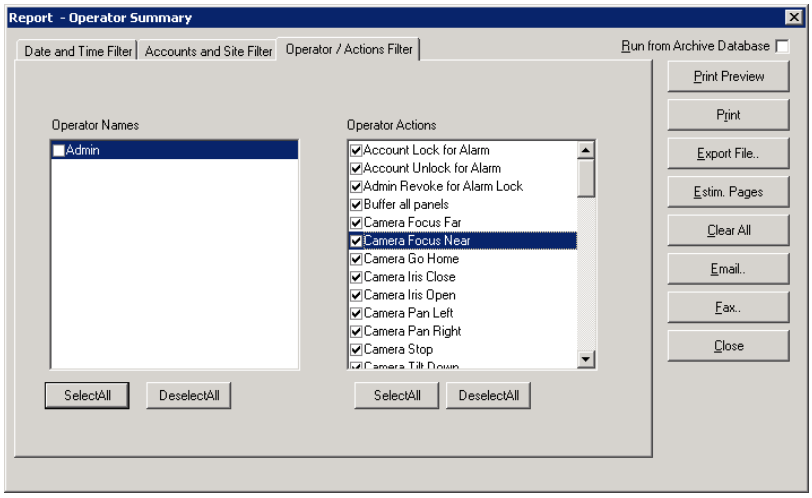


b. Under **Account Names**, select or clear the accounts to be included or excluded. By default all the accounts are selected.

Tip: Click **Select All** to select all the accounts or click **Deselect All** to clear all the accounts.

4. To filter only the specific operator actions:

a. Click the **Operator/ Actions Filter** tab.

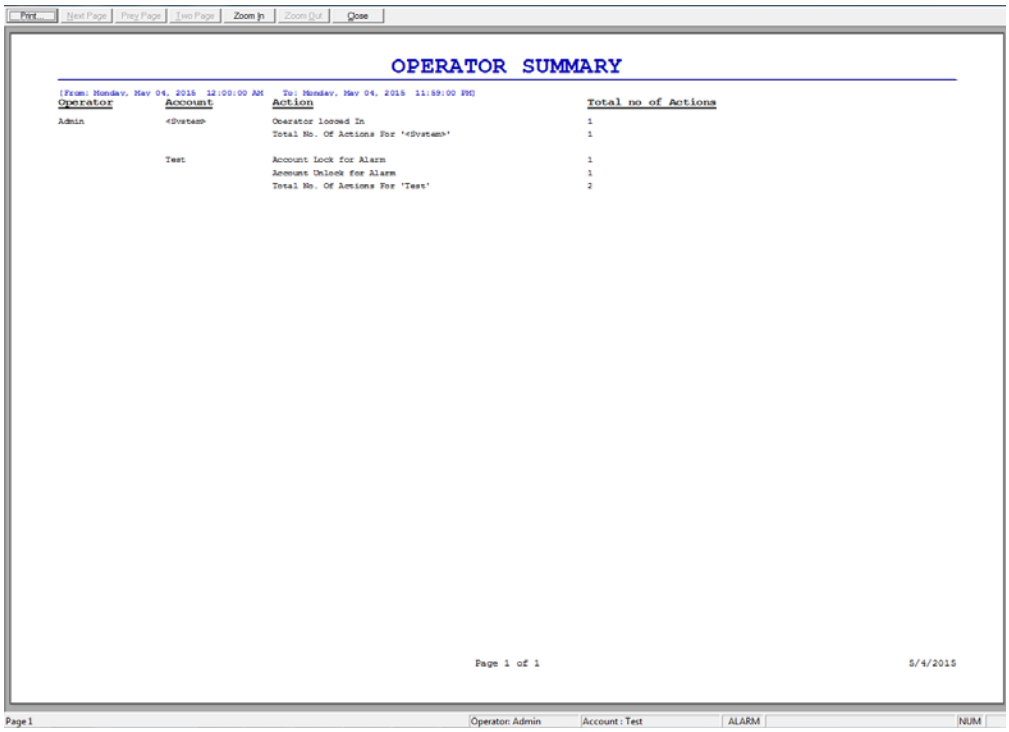


b. Under Operator Names select or clear the operator names to be included or excluded. By default, all the operator names are selected.

c. 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.

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 **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.
9. Click **Close** to close **Operator Actions Report dialog** box.

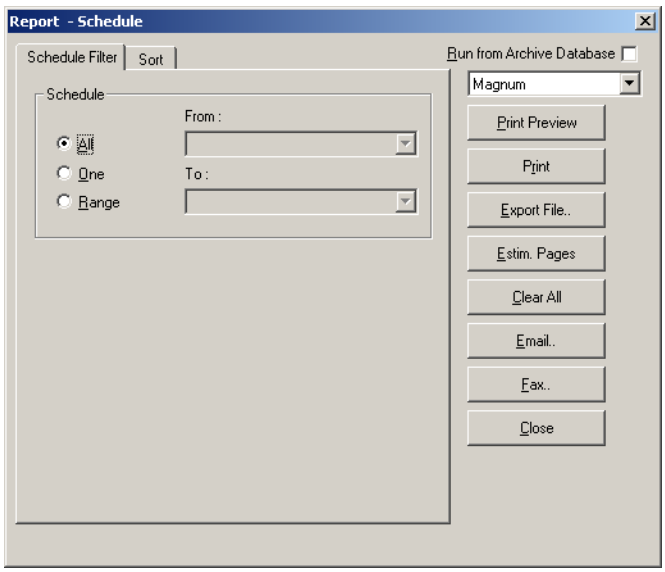
Schedule Report

To generate a schedule report:

1. In the **Reports** window, select the **Schedule** report and click **Report Options**. The **Report - Schedule** dialog box appears.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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 19-21 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.

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.

Note: Step 7 and 8 is applicable only in WIN-PAK CS.

7. Click **Email..** to send a copy of the report by e-mail, to the customer.
8. Click **Fax..** to fax a copy of the report.
9. Click **Close** to return to the **Reports** window.

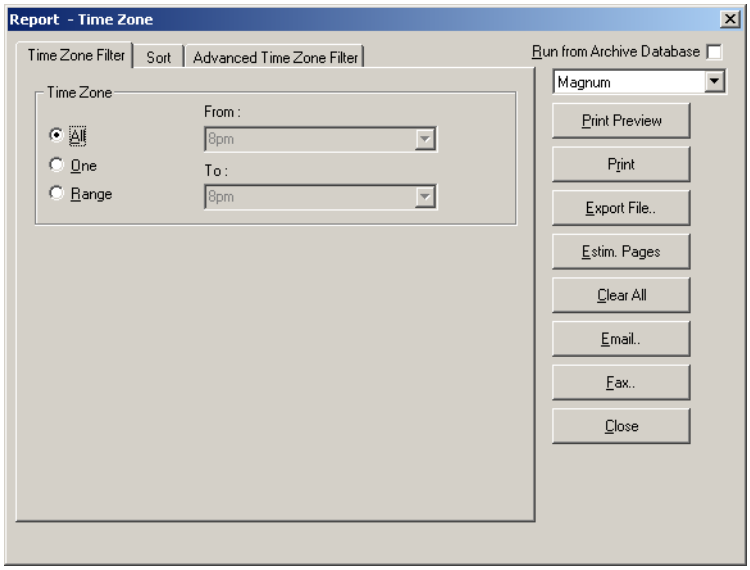
Time Zone Report

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.

Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



3. 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:

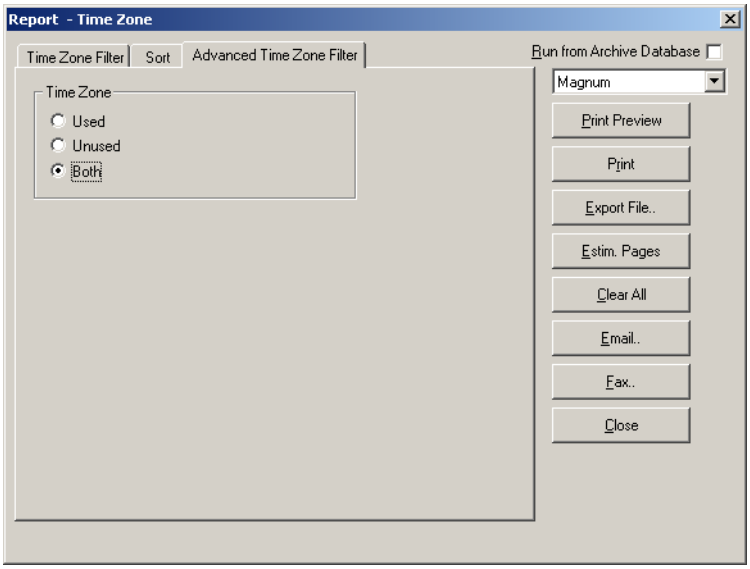
Table 19-22 Describing the options for filtering time zones

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.

Table 19-22 Describing the options for filtering time zones

Option	Description
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**.

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. To perform advanced filter on time zones:
    a. Click the **Advanced Time Zone Filter** tab.

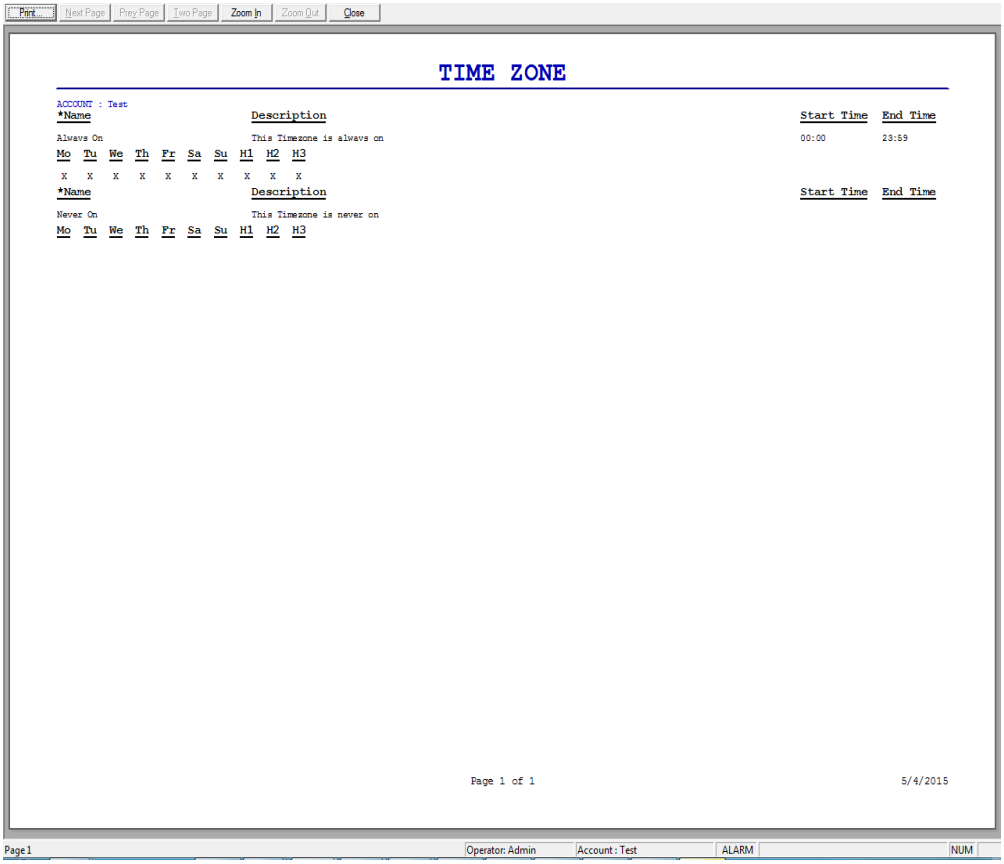


    b. Under **Time Zone**, select one of the following options:

Table 19-23 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.

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.

Note: Step 8 and 9 is applicable only in WIN-PAK CS.

8. Click **Email..** to send a copy of the report by e-mail, to the customer.
9. Click **Fax..** to fax a copy of the report.
10. Click **Close** to return to the **Reports** window.

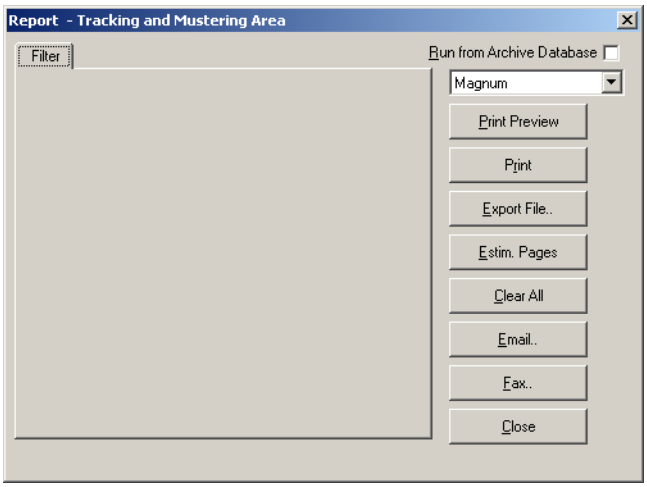
Tracking and Mustering Area Report

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.

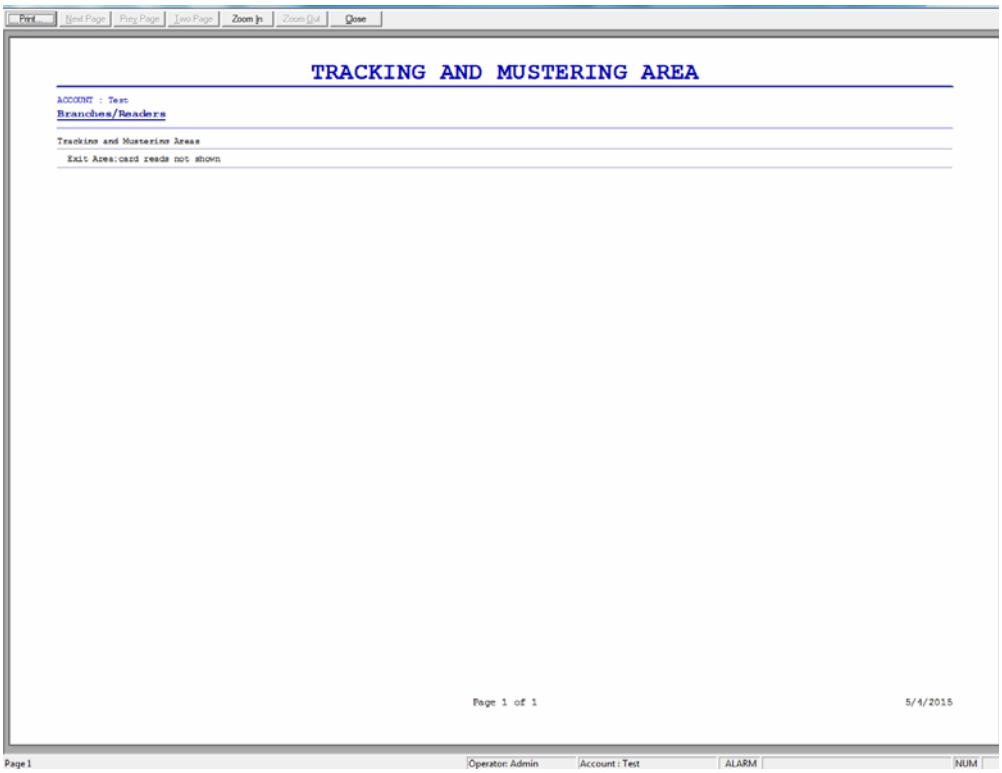
Note: Step 2 is applicable only in WIN-PAK CS.

2. Select the account from the drop-down list in the upper-right corner of the dialog box.



No filter or sorting options are provided for the tracking and mustering area report.

3. Click **Print Preview** to view the Access Area Report prior to printing.



4. Click **Print** to send the report to your printer.

Note: Step 5 and 6 is applicable only in WIN-PAK CS.

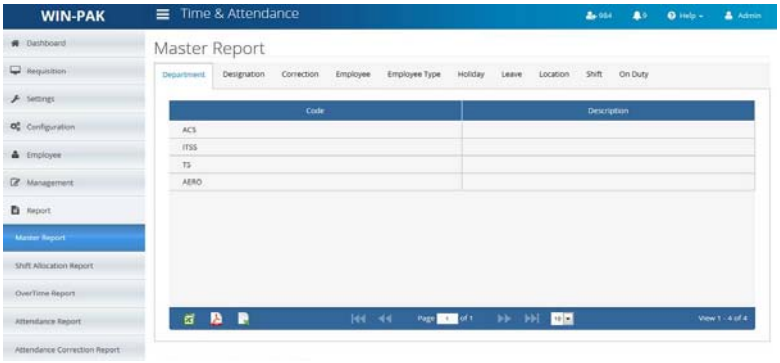
5. Click **Email..** to send a copy of the report by e-mail, to the customer.
6. Click **Fax..** to fax a copy of the report.
7. Click **Close** to return to the **Reports** window.

Master Report

The **Master Report** page displays the department, designation, employee, and so on.

To generate a master report:

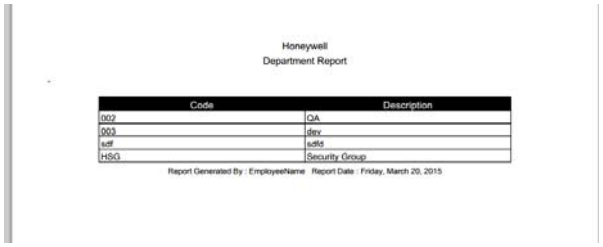
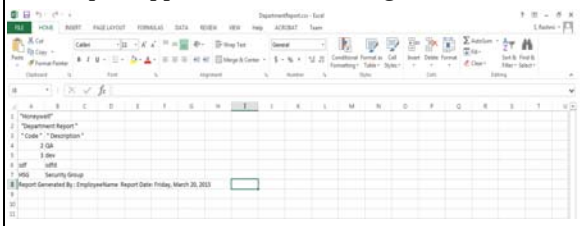
1. Click **Reports** on the left pane and then select **Master Report**. The **Master Report** page appears.



2. You can generate master report based on the following criteria:
   - Department
   - Designation
   - Att. Correction
   - Employee
   - Employee Type
   - Holiday
   - Leave
   - Location
   - Shift
   - On Duty

3. To generate a master report in .xls, .csv, and .pdf formats, you can use the icons available at the lower pane of the page.

Table 19-24 List of icons appearing on the lower pane

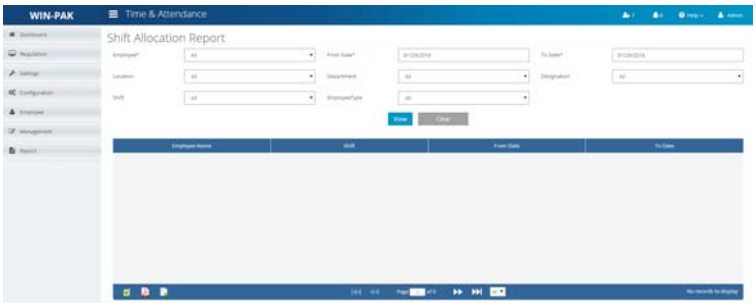
Icons	Click to...
	Click to generate a master report in .xls format. The report appears in the following format. 
	Click to generate a master report in .pdf format. The report appears in the following format. 
	Click to generate a master report in .csv format. The report appears in the following format. 
	Shuffle between multiple pages (grids).
	Display the selected number of records on each grid.

Shift Allocation Report

The **Shift Allocation Report** page displays the department, designation, employee, and so on.

To generate a master report:

1. Click **Reports** on the left pane and then select **Master Report**. The **Master Report** page appears.



2. Enter the following details.

Table 19-25 Shift Allocation Report

Field	Description
Employee	From the drop-down list, select the employee for which you must generate the shift allocation report.
From Date	Set the from date (in month, date, year format) for the report generation.
To Date	Set the to date (in month, date, year format) for the report generation.
Location	From the drop-down list, select the location of the employee.
Department	From the drop-down list, select the department of the employee.
Designation	From the drop-down list, select the designation of the employee.
Shift	From the drop-down list, select the shift allocated to the employee.
Employee Type	From the drop-down list, select the type of employee.

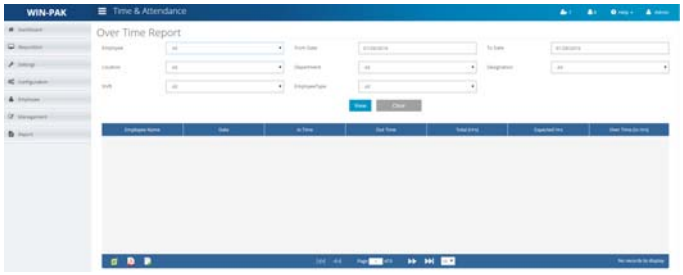
3. Click **View**.

Work/ Over Time Report

The **Work/Overtime Report** page displays the department, designation, employee, and so on.

To generate an work/overtime report:

1. Click **Reports** on the left pane and then select **Over Time Report**. The **Over Time Report** page appears.



2. Enter the following details.

Table 19-26 Shift Allocation Report

Field	Description
Employee	From the drop-down list, select the employee for which you must generate the shift allocation report.
From Date	Set the from date (in month, date, year format) for the report generation.
To Date	Set the to date (in month, date, year format) for the report generation.
Location	From the drop-down list, select the location of the employee.
Department	From the drop-down list, select the department of the employee.
Designation	From the drop-down list, select the designation of the employee.
Shift	From the drop-down list, select the shift allocated to the employee.
Employee Type	From the drop-down list, select the type of employee.

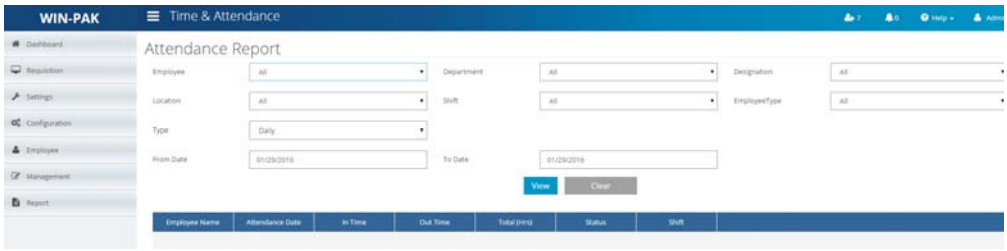
3. Click **View**.

Attendance Report

The **Attendance Report** page displays the department, designation, employee, and so on.

To generate an attendance report:

1. Click **Reports** on the left pane and then select **Attendance Report**. The **Attendance Report** page appears.



2. Enter the following details.

Table 19-27 Attendance Report

Field	Description
Employee	From the drop-down list, select the employee for which you must generate the shift allocation report.
Location	From the drop-down list, select the location of the employee.
Type	From the drop-down list, select the report based on daily, monthly, or weekly report generation.
Department	From the drop-down list, select the department of the employee.
Shift	From the drop-down list, select the shift allocated to the employee.
Designation	From the drop-down list, select the designation of the employee.
Employee Type	From the drop-down list, select the type of employee.
From Date	Set the from date (in month, date, year format) for the report generation.
To Date	Set the to date (in month, date, year format) for the report generation.

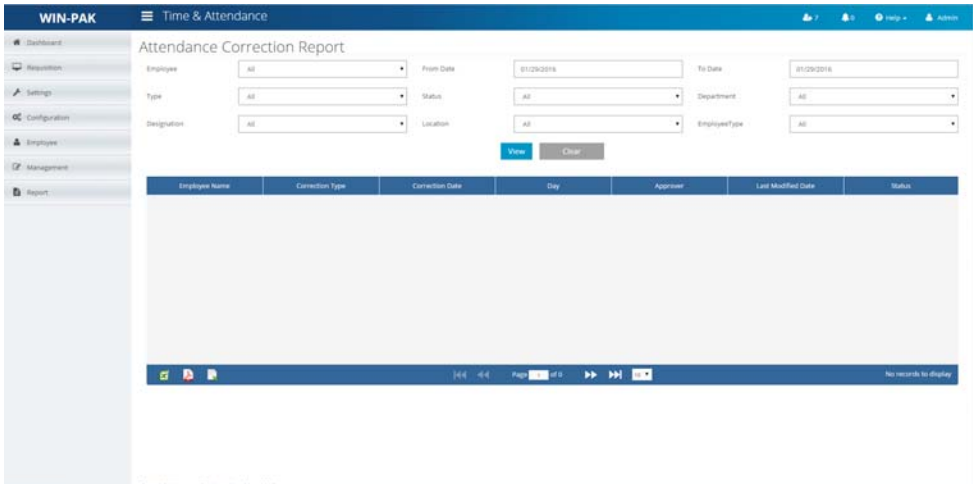
3. Click **View**.

Attendance Correction Report

The **Attendance Report** page displays the department, designation, employee, and so on.

To generate an attendance report:

1. Click **Reports** on the left pane and then select **Attendance Correction Report**. The **Attendance Correction Report** page appears.



2. Enter the following details.

Table 19-28 Attendance Correction Report

Field	Description
Employee	From the drop-down list, select the employee for which you must generate the shift allocation report.
From Date	Set the from date (in month, date, year format) for the report generation.
To Date	Set the to date (in month, date, year format) for the report generation.
Type	From the drop-down list, select the report based on card status.
Status	From the drop-down list, select to set the status for the on correction report.
Department	From the drop-down list, select the department of the employee.
Designation	From the drop-down list, select the designation of the employee.
Location	From the drop-down list, select the location of the employee.
Employee Type	From the drop-down list, select the type of employee.

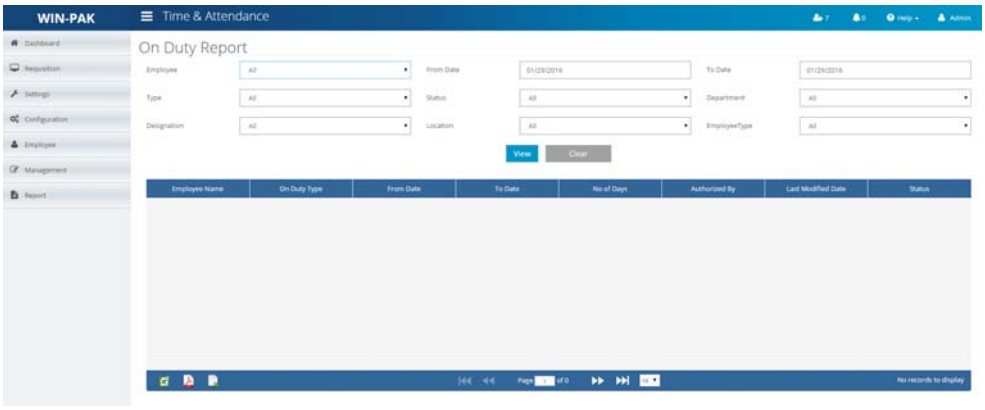
3. Click **View**.

On Duty Report

The **On Duty Report** page displays the department, designation, employee, and so on.

To generate a master report:

1. Click **Reports** on the left pane and then select **On Duty Report**. The **On Duty Report** page appears.



2. Enter the following details.

Table 19-29 On Duty Report

Field	Description
Employee	From the drop-down list, select the employee for which you must generate the shift allocation report.
From Date	Set the from date (in month, date, year format) for the report generation.
To Date	Set the to date (in month, date, year format) for the report generation.
Type	From the drop-down list, select the types of on duty such as, travel and so on.
Status	From the drop-down list, select to set the status for the on duty report.
Department	From the drop-down list, select the department of the employee.
Designation	From the drop-down list, select the designation of the employee.
Location	From the drop-down list, select the location of the employee.
Employee Type	From the drop-down list, select the type of employee.

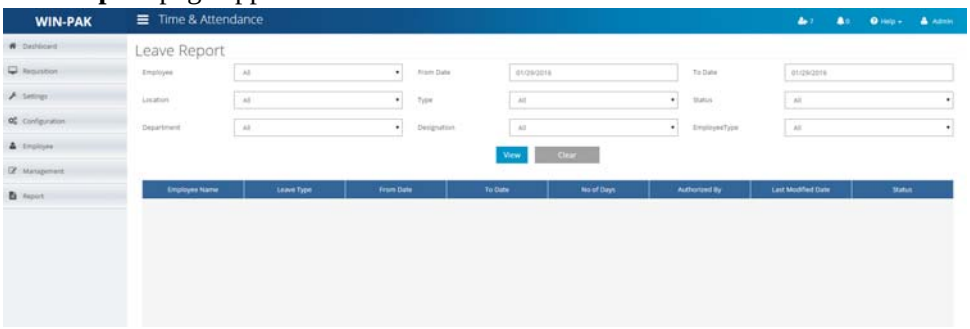
3. Click **View**.

Leave Report

The **Leave Report** page displays the department, designation, employee, and so on.

To generate a leave report:

1. Click **Reports** on the left pane and then select **Leave Report**. The **Leave Report** page appears.



2. Enter the following details.

Table 19-30 Leave Report

Field	Description
Employee	From the drop-down list, select the employee for which you must generate the shift allocation report.
From Date	Type the start date of your leave.
To Date	Type the end date of your leave.
Location	From the drop-down list, select the location of the employee.
Type	From the drop-down list, select the type of the leave.
Status	From the drop-down list, select to set the status for the leave report.
Department	From the drop-down list, select the department of the employee.
Designation	From the drop-down list, select the designation of the employee.
Employee Type	From the drop-down list, select the type of employee.

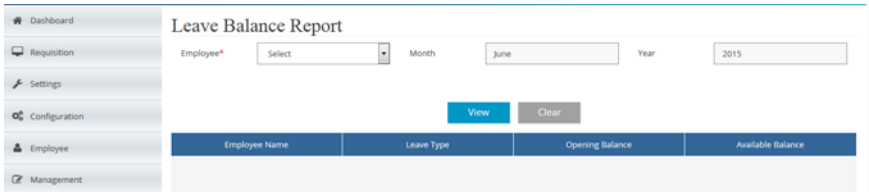
3. Click **View**.

Leave Balance Report

The **Leave Balance Report** page displays the department, designation, employee, and so on.

To generate a leave balance report:

1. Click **Reports** on the left pane and then select **Leave Report**. The **Leave Balance Report** page appears.



2. Enter the following details.

Table 19-31 Leave Balance Report

Field	Description
Employee	From the drop-down list, select the employee for which you must generate the shift allocation report.
Month	Displays the current month.
Year	Displays the current year.

3. Click **View**.

Import Utility

20

In this chapter...

This chapter describes about the Introduction to Import Utility in WIN-PAK SE/PE.

Introduction

The WIN-PAK SE/PE Import Utility is used for importing the card and card holder details into WIN-PAKSE/PE. When you import these details into WIN-PAK, cards are assigned to the card holders as applicable.

Importing card and card holder details to WIN-PAK SE/PE includes the following:

1. Defining note fields and card holder tabs in WIN-PAK SE/PE for including card holders' additional information.
2. Defining the sequence of the fields.
3. Entering card and card holder details in the excel sheet.
4. Assigning default values to certain fields.
5. Importing the excel sheet into WIN-PAK SE/PE.

Defining Note Fields and Card Holder Tabs

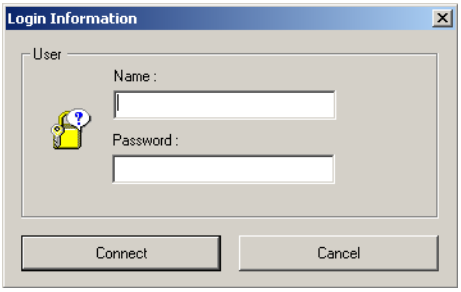
Note Field is the user-defined field for entering the additional information of the card holder in WIN-PAK SE/PE . The user-defined fields are grouped under various categories called card holder tabs.

Defining Sequence of Fields

After you define the note fields and card holder tabs, you must define the sequence of the card holder fields.

To define the sequence of the card holder fields:

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK Import Utility**. The **Login Information** dialog box appears.

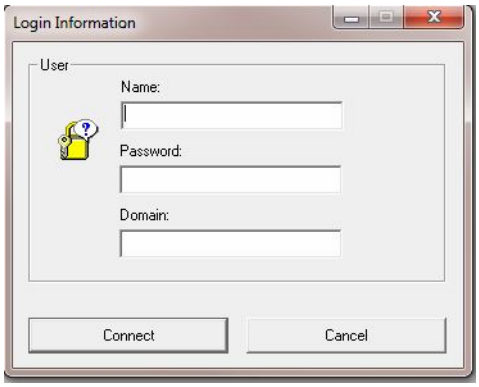


2. Type the **Name** of the user and the **Password**.

Notes:

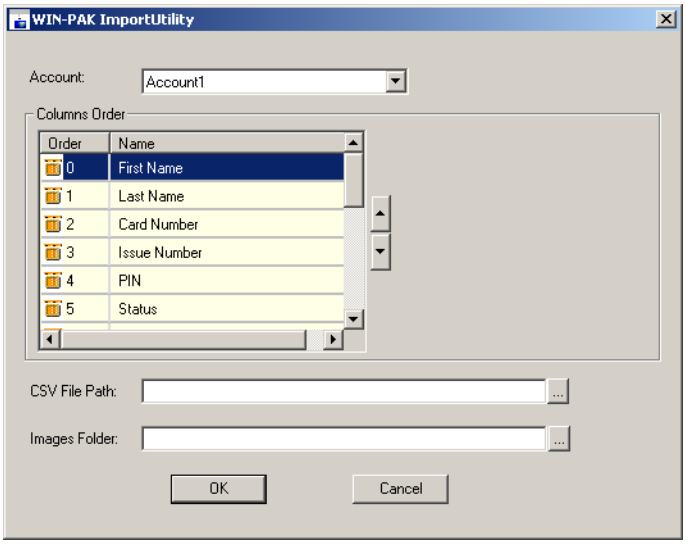
- Only the Administrator can log on to WIN-PAK SE/PE Import Utility.

- You can also log on to WIN-PAK SE/PE Import Utility using the **Domain** credentials.



The **Domain** field box appears when you select **Login using domain credentials** in **System Config** dialog box. For more information, See section Configuring automatic log on and log off settings, page 191.

3. Click **Connect**. The system fetches the data from database and displays the **WIN-PAK ImportUtility** window.



4. Select the **Account** to which the sequence has to be defined. The card holder fields for the selected account are listed in **Columns Order**.
5. To change the order of a row, select the row in the list and click the up button and/or down button.

Note: You must follow the **Order** of the fields, when you enter the card holder information in the excel sheet. 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.

Creating the Excel Sheet

Before you create the excel sheet, make a note of the column order in which the fields must be entered.

To create the excel sheet:

1. Open the Microsoft Excel application.
2. Enter the card and card holder information as in the sequence you defined in the WIN-PAK SE/PE Import Utility.
3. Save the excel sheet in the. xls or. csv format.

Tips on entering card and card holder details in the excel sheet

- Do not enter the field names in the first row. If you enter the field names to identify the field of the column, delete it before you use the excel sheet for importing data into WIN-PAK SE/PE.
- For the Status field, type 1, 2, or 4 to indicate the card status as Active, Inactive, or Trace.

Note: Leave the Activation Date and Expiration Date fields empty, if you specify the card status as Active or Trace.

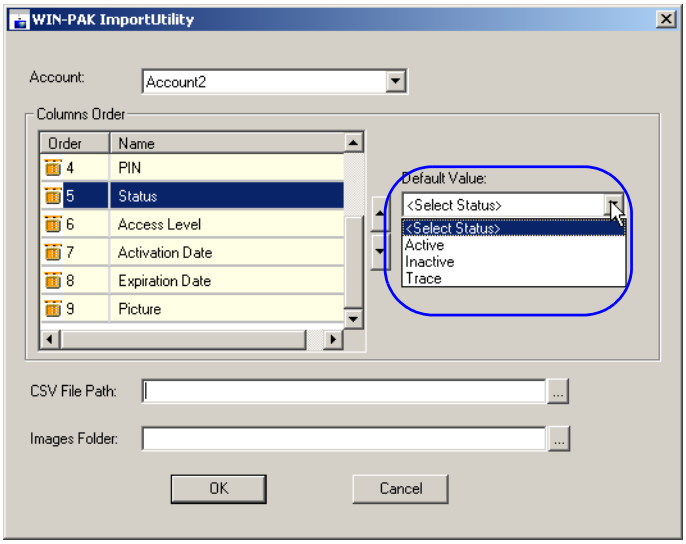
- Ensure that access levels are configured in WIN-PAK SE/PE for the respective account, before you enter the name of the access levels.
- Avoid duplication of card numbers.
- To assign default value for the fields, leave the fields empty. You can assign default value to the Issue Number, Status, Access Level, Activation Date, and Expiry Date fields and the user-defined fields.
- Ensure to use the format of note field templates for the user-defined fields.
- In the Photo column, enter the name of the image file to assign the photo of the card holder.

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 WIN-PAK SE/PE Import Utility. The **WIN-PAK ImportUtility** window appears.
2. Select the **Account** for assigning the default values. The corresponding fields are displayed in **Columns Order**.
3. Under **Columns Order**, select the field to which the default value to be assigned. The **Default Value** box appears on the right.



4. Type or select the default value to be assigned to all the card holders.

Tip: For Activation Date or Expiration Date, select the check box to select the current date. To change the date, click the drop-down list and select the required date in the calendar.

Note: The expiration date must be greater than the activation date.

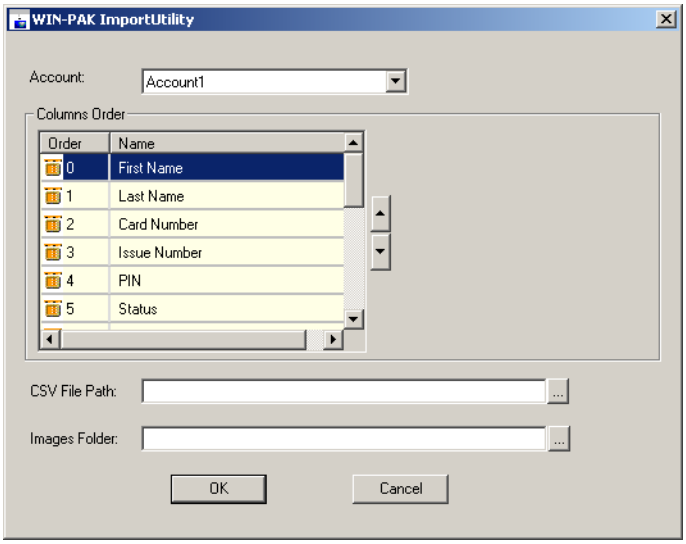
Importing Card and Card Holder Information

You can import the card and card holder information, after you create the excel sheet and assign the default values.

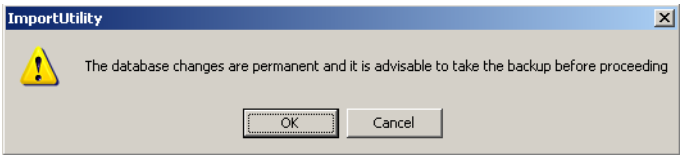
Note: Honeywell recommends you to take a backup of the current WIN-PAK SE/PE database, before importing the data to WIN-PAK SE/PE.

To import the excel sheet:

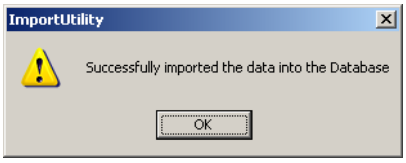
1. Log on to WIN-PAK SE/PE Import Utility. The **WIN-PAK SE/PE ImportUtility** window appears.



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 **CVS File Path**, specify the path of the excel sheet or click the ellipsis button and select the path.
4. In **Images Folder**, specify the path of the folder where the photo images are stored.
5. Click **OK**. A message appears asking for confirmation.



6. Click **OK** to proceed with importing the data. A message appears indicating that import is successful.

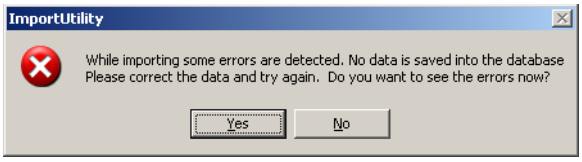


Correcting Errors in Excel Sheet

If any error occurs while importing the data, you cannot successfully import the card and card holder information to WIN-PAK SE/PE until you correct the errors.

To view and correct the errors:

1. In case of unsuccessful import, the following error message appears asking whether to open the list of errors occurred.



2. Click **Yes** to view the errors. The **ErrorLog.xls** file is opened.

	A	B	C
1	SlNo	Record	Description
2	0		Datatype mismatch for column ActivationDate
3	1		Card Number already exists in the Database - 3456
4	2		CardStatus is mentioned as Active/Trace but Activation date also specified
5	3		Datatype mismatch for column CardStatus
6	4		Error: Invalid Card Status Value - Trace
7	5		Error: The Activation date cannot be the same or after the Expiration date
8	6		Error: Invalid Access Level - 'Operator2' or Access Level doesn't belong to the specified account
9	7		Mandatory data is missing for - CardNumber
10	8		CardStatus is mentioned as Active/Trace but Activation date also specified
11	9		Error: Invalid Access Level - 'Operator1' or Access Level doesn't belong to the specified account
12	10		CardStatus is mentioned as Active/Trace but Activation date also specified
13	11		Error: The Activation date cannot be the same or after the Expiration date
14	12		CardStatus is mentioned as Active/Trace but Activation date also specified
15	13		Error: The Activation date cannot be the same or after the Expiration date
16	14		CardStatus is mentioned as Active/Trace but Activation date also specified
17	15		Error: The Activation date cannot be the same or after the Expiration date
18			
19			
20			
21			
22			
23			
24			

3. View the errors in ErrorLog.xls file and correct them in the source file.

Troubleshooting

21

In this chapter...

This chapter describes about the Introduction to Troubleshooting, Definition, and about the section How to in WIN-PAK CS, and SE/PE.

Section	WIN-PAK CS	WIN-PAK SE/PE
Definition: Backup types, page 961	✓	✓
Definition: Restore types, page 962	✓	✓
Definition: Video Management Server, page 966	✓	✓
How to: How to setup the PW-5000 or P-Series panel for Daylight savings?, page 968	✓	✓
How to: How to setup the PW-5000 or P-Series panel for a 12 digit ABA Format?, page 968	✓	✓
How to: How to setup WIN-PAK CS/SE/PE for elevator control with the PW-5000 or P-Series panel?, page 970	✓	✓
How to: How do the various Offline Door Modes work for the PW-5000 and the P-Series panel?, page 973	✓	✓
How to: How to set a Time zone for Card and PIN or Card Only on the PW-5000 or P-Series panel with PROXPRO-K readers?, page 974	✓	✓
How to: How to enable P-Series panels to read the HID Corporate 1000 format?, page 974	✓	✓
How to: How to add Carriage Return in a Command File?, page 975	✓	✓

Section	WIN-PAK CS	WIN-PAK SE/PE
How to: How to include ADV Priority Value Definitions as it relates to Alarm/Event/History?, page 976	✓	✓
How to: How to define PW-5000/P-Series Anti-Passback/Timed Anti-Passback Processing Mode?, page 976	✓	✓
How to: How to enable any valid card read to trip an additional relay on the P-Series reader board?, page 979	✓	✓
How to: How to set alarm in WIN-PAK CS/SE/PE / NStar based on Database Limits and Capacities?, page 980	✓	✓
How to: How to enable Triggers and Procedures in WIN-PAK CS?, page 980	✓	
How to: How to configure the PW-5000 or P-Series IC panel to read the Kronos cards?, page 981	✓	✓
How to: How to configure Windows users for WIN-PAK CS/SE/PE log on using Windows Authentication?, page 983	✓	✓
How to: How to setup magstripe encoding and duplexing with a Fargo DTC4500 printer in WIN-PAK CS/SE/PE?, page 983	✓	✓
How to: How to manually remove WIN-PAK CS/SE/PE Services through a command line prompt?, page 984	✓	✓
How to: How to define a Pre-Alarm trigger to energize an output?, page 985	✓	✓
How to: How to define procedure Timezone for PW-5000 and P-Series?, page 987	✓	✓
How to: How to set the PW-5000 or P-Series relay or relays to latch and time zone controlled?, page 987	✓	✓
How to: How to explain the usage of crash bar in a PW-5000 or P-Series panel, which in turn causes a Forced Open alarm?, page 992	✓	✓

Section	WIN-PAK CS	WIN-PAK SE/PE
How to: How to configure WIN-PAK CS/SE/PE Server for multiple communication servers?, page 993	✓	✓
How to: How do I shunt the door contact using the door egress on a PW-5000/P-Series panel?, page 996	✓	✓

Introduction

WIN-PAK CS/SE/PE 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 CS/SE/PE user interface. The text files for French, German, Dutch, Italian, English, Simplified Chinese, and Traditional Chinese languages are available by default in the **WIN-PAK\Language Files** folder of WIN-PAK CS/SE/PE.

Translating the WIN-PAK CS/SE/PE User Interface involves:

1. Adding a new language with its text and help files into the **WIN-PAK\Language Files** folder. "Language Configuration"
2. Modifying the translated text (if required) for the dialog box captions, menus, and the other text in the User Interface.

By default, WIN-PAK CS/SE/PE is designed to work with U.S. English operating system. Therefore, a special version of WIN-PAK CS/SE/PE 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.

Definition

The definition of various terms and types are explained.

Backup types

There are four backup types:

- Complete Backup (No Append)
- Append
- Incremental
- Differential

When a file is created or modified, the operating system keeps track of its file name, size, and other characteristics, called attributes. One of these attributes is the archive bit, also called the archive flag. Your backup software uses the archive bit to determine whether or not a file needs to be backed up.

The archive bit works like the flag on a mailbox. When the flag is up (on), the program knows that the file needs to be backed up. After the file has been backed up, the program can "lower the flag" to turn the file's archive bit off.

Once a file is created, modified, or opened the archive bit is reset on (flag is up). Then that file will be selected on the next incremental backup.

Complete Backup (No Append) type

A Complete Backup (No Append) backs up the main WIN-PAK CS/SE/PE Database with the new changes into one backup file. The Archive Bit is reset.

Incremental backup type

Backs up all selected files that have changed since the most recent All selected files or incremental backup. All files that have the archive bit on are backed up. When the backup is complete, the archive bit(s) are turned off.

Differential backup type

The differential type backs up all selected files that have changed since the last full backup, and does not turn off their archive flags. Consequently on the very next differential, the backed-up files will be backed up again along with any new files that have changed since the last differential backup.

This cycle will continue until another Full backup is performed on the drive. To run this type of backup you must first perform a Full backup of your system.

Append-Complete backup type

Append-Complete backs up the main database with the incremental information, thus the archive bit(s) are turned off. When the next backup is scheduled the Database is backed up in the same file. What information has changed from the last incremental backup is appended with the main backup of the database.

Note: When using the back up facility in WIN-PAK CS/SE/PE, the following files are not backed up.

- User image (*.JPG's) files
- Badge image (*.BMP/ *.JPG's) files
- Floor Plan Image (*.WMF) files
- Signatures (*.SIG) files

Therefore, you must manually backup the above files after back up.

Restore types

There are four restore types:

- Complete Restore (No Append)
- Append
- Incremental
- Differential

Complete Restore (No Append) type

Complete Restore (No Append) includes the WIN-PAK CS/SE/PE main database information, you don’t have to search through several tapes to find the files you need to restore. If you should need to restore WIN-PAK CS/SE/PE database, all or most current information would be found on the last backup tape.

Incremental Restore type

Multiple tapes needed for restore- Files can be spread over all the tapes in use since the last full backup. You would need to search several tapes to find the file you wish to restore. In addition, the media must be restored in the correct order to effectively bring the system up to date.

Differential Restore type

Restoring a system backed up with a differential requires a maximum of two backups- the latest full backup and the latest differential backup.

Append-Complete Restore type

Restores the main database with what information was changed from the last full and appended database.

Notes: Bits is the smallest unit of data. It consists of a single binary digit that can take the value of 0 or 1. When using the restore option in WIN-PAK CS/SE/PE, the following files are not restored:

- User image (*.JPG's) files
- Badge image (*.BMP/ *.JPG's) files
- Floor Plan Image (*.WMF) files
- Signatures (*.SIG) files

Therefore, you must manually restore the above files.

P-Series/PW-5000 Anti-Passback - Timed Anti-Passback Processing Mode and Results

The following is the Anti-Passback/ Timed Anti-Passback Processing Mode and Results for the PRO-2200/PRO-3200/PW-5000.

Note: PRO-2200/ PRO-3200/PW-5000 keeps track of the door status being used, not used, etc, unless the Reader option "Log all access Requests as used" is checked forces all card transactions as "used" to the WIN-PAK PE software.
If the reader option ”Log all access Requests as used” is not checked the PRO-2200/PRO-3200/PW-5000 will wait for the status of the door.
When a card is presented to the reader the PRO-2200/PRO-3200/PW-5000 will wait for 20 seconds. (for the status of the door), if the door is not used it will report in the WIN-PAK PE Event Viewer.
”Valid card, Door not Used”. As long as the door is not used after the card swipe, the card still has access to the reader door.
If the card is swiped at the reader and the cardholder opens the door the Event Viewer reports back as ”Valid Card, Door used”. When the card is presented again it will report back in the Event Viewer (Soft Anti-Passback: AB violation, door used/ not used)/ (Hard Anti-Passback: Anti-Passback Violation)

1. None

   No Anti-Passback in effect

2. Anti-Passback

   a. Soft

      Upon an Anti-Passback violation on any in/out reader that is set for Soft Anti-Passback, the card is still granted access and reports in alarm view either:

– "APB Violation, Door Used"

– "APB Violation, Door not Used"

Example: SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as "Processing Mode (SOFT)/ Direction (IN)" SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (SOFT)/ Direction (OUT)". Delay "# " would be grayed out.

A card is swiped at SIO Board 1 Reader 1 for the first time, the card is valid and is granted access (Alarm View shows "Valid card, door used").

If the Cardholder then decides to swipe at SIO Board 2 Reader 1, the card is granted access (Alarm View shows "APB Violation, Door Used").

Note: Global Soft Anti-Passback Per Card

b. Hard

Upon an Anti-Passback violation on any in/ out reader that is set for Hard Anti-Passback, the card is not granted access. (Alarm View shows "Anti-Passback Violation: (Card #)(User Name)(Account: ”r;account name"))

Example: SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as "Processing Mode (HARD)/ Direction (IN)" and SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (HARD)/ Direction (OUT)". Delay "#" would be grayed out.

A card is swiped at SIO Board 1 Reader 2 for the first time, the card is valid and is granted access (Alarm View shows "Valid card, door used").

If the cardholder decides to swipe at SIO Board 2 Reader 2, the card is denied access. (Alarm View shows "Anti-Passback Violation: (Card #)(User Name)(Account:"account name"))

Note: Global Hard Anti-Passback Per Card

c. Panel Based Time AB

When this option is enabled, Panel Based Timed ABA (Anti-Passback) combines Hard and Soft Anti-Passback. If a card is swiped a second time within the set Delay time, the system becomes Hard Anti-Passback. After the set Delay Time, the Anti-Passback card is swiped a third time, the system becomes Soft- Anti-Passback resetting the delay time. When the same card is swiped again within the set delay time, the system becomes Hard Anti-Passback.

Example: SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as "Processing Mode (Panel based Timed APB)/ Direction (IN)" and SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (Panel based Timed APB)/ Direction (OUT)". Delay time is set to 30 Sec.

A card is swiped at SIO Board 1 Reader 1 and is granted access. (Alarm View shows" Valid Card, door used: (card #)(User

Name)(Account:"account name")) When the same card is swiped at the same reader within the set delay time the card is denied access.

(Alarm View shows "Anti-Passback Violation: (Card #)(User Name)(Account:"account name"))

If the card is swiped after the set delay time, the card is granted access. (Alarm View shows "APB Violation, door used: (card #)(User Name)(Account:"account name))

When the same card is swiped at the same reader within the set delay time the card is denied access. (Alarm View shows "Anti-Passback Violation: (Card #)(User Name)(Account:"account name"))

Note: Global Panel Based Timed Anti-Passback Per Card

3. Timed Anti-Passback

a. Card Based Time APB

If this option is enabled, a card cannot be swiped twice at the same panel within the amount of time selected for the delay. Any card that is swiped at the same reader will have it's own delay time, if the cards are swiped at another panel reader, the cards will gain access to the Anti-Passback reader.

Example: SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as "Processing Mode (Card Based Timed APB)/ Direction (None)" and SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (Card Based Timed APB)/ Direction (None)" Delay time is set to 30 Sec.

A card is swiped for the first time at SIO Board 1 Reader 1. The card is valid and granted access. If the card is swiped a second time at the same reader before the 30 second delay has expired, the card will not grant access.

(Alarm View shows "Anti-Passback Violation: (Card #)(User Name)

(Account:"account name"))

Note: Per Panel Card Based Anti-Passback Per Card

b. Reader Based Time APB (Anti-Passback)

If this option is enabled, a card cannot be swiped twice at the same panel within the amount of time selected for the delay or a different card to take the set delay.

Example: SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as "Processing Mode (Reader Based Timed APB)/ Direction (None)" and SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (Reader Based Timed APB)/ Direction (None)". Delay time is set to 30 Sec.

A card is swiped for the first time at SIO Board 1 Reader 1. The card is valid and granted access. If the card is swiped a second time at the same reader before the 30 second delay has expired, the card will not grant access.

(Alarm View shows "Anti-Passback Violation: (Card #)(User Name)(Account:"account name"))

If a second card is swiped at SIO Board 1 Reader 1, the second card will take the delay time of the first card. When the first card is swiped at the same reader, the card is granted access.

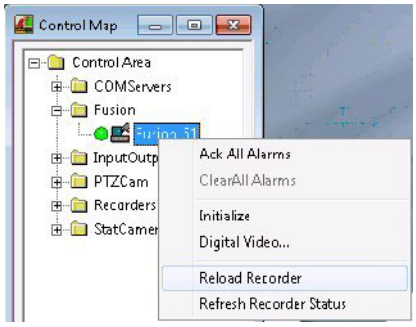
(Alarm View shows" Valid Card, door used: (card #)(User Name)(Account:"account name"))

Note: Per Panel Reader Based Anti-Passback Global card

Video Management Server

1. **Refresh Display Services**: If the video is not showing in the Salvo Viewer from the associated DVR, the video/clip export fails displaying the following error message "Video retrieval error". Click **Refresh Display Service** option in **Salvo Viewer** to refresh the display services.

2. **Reload Recorder**: If PTZ is not working for PTZ camera belonging to that recorder and if the status of recorder/ camera is shown as unknown in control map, then right click the **Recorder** in **Control Map** tree and select **Reload Recorder** option.



3. Refresh Camera Status: If the status of camera is not displayed in **Control Map** tree view, right click the **Camera** in **Control Map** tree and select **Refresh Camera** option.
4. In the WIN-PAK CS/SE/PE UI Client, if a blank page appears when you select the **Configurator** page, select **Logout** and then **Login**.

How To

This section contains the list of questions encountered by the technical support team. Click a question to navigate to the answer.

Table 21-1 List of questions

S.No.	Questions
1	"How to setup the PW-5000 or P- Series panel for Daylight savings?"
2	"How to setup the PW-5000 or P-Series panel for a 12 digit ABA Format?"
3	"How to setup WIN-PAK CS/SE/PE for elevator control with the PW-5000 or P-Series panel?"
4	"How do the various Offline Door Modes work for the PW-5000 and the P-Series panel?"
5	"How to set a Time zone for Card and PIN or Card Only on the PW-5000 or P-Series panel with PROXPRO-K readers?"
6	"How to enable P-Series panels to read the HID Corporate 1000 format?"
7	"How to add Carriage Return in a Command File?"
8	"How to include ADV Priority Value Definitions as it relates to Alarm/Event/History?"
9	"How to define PW-5000/P-Series Anti-Passback/Timed Anti-Passback Processing Mode?"
10	"How to enable any valid card read to trip an additional relay on the P-Series reader board?"
11	"How to set alarm in WIN-PAK CS/SE/PE / NStar based on Database Limits and Capacities?"
12	"How to enable Triggers and Procedures in WIN-PAK CS?"
13	"How to configure the PW-5000 or P-Series IC panel to read the Kronos cards?"
14	"How to configure Windows users for WIN-PAK CS/SE/PE log on using Windows Authentication?"
15	"How to setup magstripe encoding and duplexing with a Fargo DTC4500 printer in WIN-PAK CS/SE/PE?"
16	"How to manually remove WIN-PAK CS/SE/PE Services through a command line prompt?"

S.No.	Questions
17	"How to define a Pre-Alarm trigger to energize an output?"
18	"How to define procedure Timezone for PW-5000 and P-Series?"
19	"How to set the PW-5000 or P-Series relay or relays to latch and time zone controlled?"
20	"How to explain the usage of crash bar in a PW-5000 or P-Series panel, which in turn causes a Forced Open alarm?"
21	"How to configure WIN-PAK CS/SE/PE Server for multiple communication servers?"
22	"How do I shunt the door contact using the door egress on a PW-5000/P-Series panel?"

How to setup the PW-5000 or P- Series panel for Daylight savings?

The Daylight Savings are automatically updated in the Windows 2000 Professional or Windows 2000 Server without asking for confirmation.

Note: Daylight Saving Time (DST) begins at 2:00 A.M. on the first Sunday of April and reverts to Standard Time at 2:00 A.M. on the last Sunday of October.

To set the PW-5000 or P-Series panel for Daylight Saving:

1. Set the Daylight Savings Group.
2. Assign the Daylight Savings to the PW-5000/P-Series panel.
3. Initialize the PW-5000/P-Series panel.

How to setup the PW-5000 or P-Series panel for a 12 digit ABA Format?

Perform the following tasks:

1. Customize the Card Format.
    a. In the **Devices** window, right-click a PW-5000 or P-Series panel and click **Configure**.
    b. Click the **Card Formats** tab.
    c. In the Format # list, select Format #1 and set the options as Not Used. Repeat the same procedure for Format #2 and Format #3 too.

d. Select Format #4 and set the following:

Option	Set to...
Option	Not Used
Format Type	ABA
Site Code	- leave it blank -
Card ID offset	0
35 bit Corporate Cards	Clear
Minimum # of digits on card	1
Maximum # of digits on card	12
Site code digits - Start digit, No. of	1, 0
Cardholder ID digits - Start digit, No. of	1, 12
Issue code digits - Start digit, No. of	1, 0

2. Set the reader configuration for the SIO Board.

Note: You must follow these steps for each reader on the SIO board that must be configured for 12 digits.

a. Click the **SIO Boards** tab.

b. Select the SIO Reader Board in which the reader is assigned and click **Edit**.

c. Click the **Reader** tab and set the following:

Option	Set to...
Reader Type	Custom
Keypad Mode	None
Led Drive Mode	Generic 1 wire, tri-state bi-color

Option	Set to...
Led Drive Mode	Select: a. Data1/data0, wiegand pulses b. Trim zero bits c. Format to nibble array d. Allow bi-dir mag decode e. Allow NCI mag decode
Access Configuration	Single, controlling the door
Anti-Passback	
Direction	None
Processing Mode	None
Delay	0
Card Format	Select Format 4
Control Flags	Clear all
Online door mode	Card only
Offline door mode	Unlock (unlimited access)

How to setup WIN-PAK CS/SE/PE for elevator control with the PW-5000 or P-Series panel?

1. Click **Configuration>Device>Device Map**. The Device window appears.
2. Expand the **Devices** folder.
3. Right-click the **PW-5000/P-Series** panel and click **Configure**. The P-Series Configuration dialog box appears.
4. Click the **System** tab.
5. Select the relevant **Daylight Savings** from the drop-down list.
6. Under **No. of Card Holders**, select **Enable card user levels for trigger control**.
7. Click the **Triggers and Procedures** tab.

Note: If the Triggers and Procedures tab is not enabled, refer to the document "Triggers & Procedures in Win- Pro grayed out".

8. Under **Procedures**, click **Add**.
9. Add the following procedures:

Option	Set to...
P- Series Triggers – Procedure Definition dialog box	
Procedure Name	Type a name for the procedure
Action List	Select from the list

Note: Ensure that you click **Add** and **OK** after including the **Triggers-Procedure** in the **P- Series Triggers – Procedure Definition** dialog box.

Option	Set to...
P- Series Triggers- Action Definition dialog box	
Action Name	Type the name for the procedure
Action Target Type	Select the Do Output Action
Select Output SIO	Select the elevator relay board
Select Output Device	Select a relay
Select Output Action	Select a pulse
Seconds to Pulse	Type a pulse time for the relay

Note: Ensure that you click **Add** and **OK** after including the Triggers-Action in the P-Series Triggers-Action Definition dialog box

10. Under **Triggers**, click **Add**.
11. Add the following triggers:

Option	Set to...
P- Series Triggers- Triggers Definition dialog box	Procedure 1
Name	Type the name for the procedure
Trigger Source Type	Select the trigger source type as Reader

Option	Set to...
Source SIO Board	Select the SIO Reader Board for the elevator control
Transaction Type	Select the transaction type as Formatted Card: Number only
Trigger Transactions	Ensure to select: • Valid Card, Door Not Used • Valid Card, Door Used
Procedure	Select the Procedure for the reader to fire
Trigger Source	Select a Reader to trigger the Procedure
Time Zone	Select Always On **Note**: If a specified Timezone is assigned, the Trigger is enabled only during the specified timezone.
Card User Level to Trigger On	Type the level number with a range from 1- 255

12. After you add and modify the triggers and procedures, click **OK** in the P-Series Configuration dialog box.
13. Click **Card>Card Holders**. The **Card Holder** window appears.
14. Click **Add** or select a card holder from the list and click **Edit**. The **Card Record** dialog box appears.
15. Click the **Card Properties** tab. It is selected by default.
16. Under **P- Series Trigger Contro**l, set the **User Level**. You must assign the number set in "**Card User Level To Trigger On**" option.
17. Click **Configuration > Device > Device Map**. The **Device** window appears.
18. Expand the **Devices** folder.
19. Right-click the **PW-5000/P-Series** panel and click **Configure.** The **P-Series Configuration** dialog box appears.
20. Click the **SIO Boards** tab. The **SIO Board Configuration** dialog box appears.

21. In the **Basic** tab, which is displayed by default, select the 2 Reader SIO Board used for **Elevator** Control. For example, Board 1, Port 3, SIO 0: 2-Reader I/O.
22. Click **Edit**.
23. Click the **Reader** tab.
24. Select the elevator **Reader**.
25. Under **Control Flags**, select **Log all access requests as used**.
26. Click **OK**.

How do the various Offline Door Modes work for the PW-5000 and the P-Series panel?

Offline Door Mode occurs when the 2-Reader SIO Board loses communications to the IC panel. Though it is powered up, the 485 connection to the SIO board stops working and stops communicating with the IC for an anonymous reason. The card reads during this time will not be reported.

At this time, the 2-Reader SIO Board goes into a degraded mode, which is known as Offline mode. Each door on the 2-Reader SIO Board enters into its Offline Door Mode state. The doors then act according to one of the three Offline Door Modes that were selected in the Reader Setup tab in WIN-PAK CS/SE/PE.

When the board is shipped from the factory it is un-programmed and blank. The Offline Mode once selected and downloaded will remain in the Board's memory until it is changed in the programming and these changes are then downloaded to the SIO Board. This mode will remain in the panel's memory, regardless of any firmware updates, replacing of the firmware chip, or by powering down then up the SIO Board.

The four different modes are Disable the Reader, **Unlocked (unlimited access)**, Locked (no access, Egress active) and Site Code Only. By default the Offline Door Mode is set to Unlocked (unlimited access). The SIO Board is initialized with the selected mode information. When the SIO Board loses its communication with the IC board, the door enters into the selected Offline Door Mode.

1. **Disable the Reader:** The doors ignore all card reads and egress actions, when the SIO Board loses its communication with the IC board.
2. **Unlocked (unlimited access):** The doors unlock and enable access to all regardless to card reads, when the SIO Board loses its communication with the IC board.
3. **Locked (no access, Egress active):** The doors lock irrespective of a valid card read but, unlocks when egress button is pressed, when the SIO Board loses its communication with the IC board.
4. **Site Code Only:** The doors unlock for a valid card read or when the egress button is pressed.

The card formats to which the site codes are not assigned allows access to any card of that format, when the SIO Board goes to the Offline mode.

How to set a Time zone for Card and PIN or Card Only on the PW-5000 or P-Series panel with PROXPRO-K readers?

1. Create two time zones for Card Only and Card and PIN. For example, create the 8AM - 5PM (Mon-Fri) time zone for Card Only and the All Times time zone. The All Times time zone should include weekends and holidays except the 8AM - 5PM (Mon-Fri) time frame.
2. Add these time zones to the panel.
3. Add the following triggers and procedures:

Option	**Set to...**	
	Procedure 1	**Procedure 2**
Action Name	Card Only	Card Only
Action Target Type	Set Reader Mode	Set Reader Mode
Select Output SIO	Board 1 Port 3, SIO 0, 2 Reader I/O	Board 1 Port 3, SIO 0, 2 Reader I/O
Select Reader Device	Reader 1 or Reader 2	Reader 1 or Reader 2
Select Reader Action	Card Only	Card and PIN
	Trigger 1	**Trigger 2**
Name	Card Only	Card and PIN
Procedure	Card Only	Card and PIN
Trigger Source Type	The time zone created for Card Only (8AM - 5PM (Mon-Fri)	The time zone created for Card and PIN Time Zone (All Times)
Transaction Type	Activate	Activate
Trigger Transaction	Became active	Became active
Time Zone	Always On (disabled)	Always On (disabled)

After setting the panel, reinitialize the panel. You MUST let the panel roll into the time zone, you cannot “force” the card mode by updating the time to trick the panel.

How to enable P-Series panels to read the HID Corporate 1000 format?

The 35-Corporate Cards check box is available in the Card Formats tab, when you edit the card format of a P-Series panel.

P-Series panels are enabled to read the HID Corporate 1000 format, when this check box is selected with the following settings:

1. Select an unused Format #.
2. Change the Option to Custom.
3. Select Wiegand as the Format Type.
4. Enter the following information in the format area.

	Start bit	**No. of**
Bits to sum for even parity	1	0
Bits to sum for odd parity	1	35
Site Code Bits	3	12
Cardholder ID bits		
Issue Code bits	1	0

5. **Site Code** can be left blank.
6. **Card ID offset:** This is a very important value because the number entered into here is where the SC will be placed in relation to the Card Number. For example, if a card consists of SC = 132 and Card # = 53124. The customer wants the card reads to look like 132053124. Since the SC # starts in the 1 millionth place then the value of 1000000 would be entered in to the Card ID offset box.
7. Select the **35-bit Corporate Cards** check box.
8. Select the new format at each of the readers it will be required to work at, click **OK** to save the changes, and Initialize the P-Series panel.

Note: When you use the 35-bit Corporate Cards option with the above setting, the Site Code and the Card Number is combined to one while reading the 35-bit card. For example, if a card has a Site Code of 141 and a Card number of 238544, using the 35-bit Corporate Card option and correct Card format would allow the user to combine the 2 numbers so that the card when read would be viewed as 141238544.

How to add Carriage Return in a Command File?

The following command syntax is required to add a carriage return to the command file.

<13> or <0x0d>

Note:

In the syntax:

- The special parentheses<> is required.
- The 13 is the ASCII version and 0d is the hex.
- The 0x signifies to the program that it is a hex number.

How to include ADV Priority Value Definitions as it relates to Alarm/Event/History?

The Priority value definitions of ADV (Abstract Device) as it relates to the Event\Alarm Views and recording to History must be set in the following format:

Priority (0):

- Transactions are not displayed in the Alarm or Event View and is not recorded to History.

Priority (1 – 50):

- Transactions appear in the Alarm and Event Views and are also recorded to history.

Priority (51 – 79):

- Transactions appear only in the Event View and not in the Alarm View. But, the transactions are recorded to History.

Priority (80 – 99):

- Transactions are recorded only to history and does not appear in Event or Alarm Views.

How to define PW-5000/P-Series Anti-Passback/Timed Anti-Passback Processing Mode?

The following options lists the Anti-Passback/Timed Anti-Passback Processing Mode and results for the PW-5000/P-Series.

Note:

PW- 5000/P-Series keeps track of the door status being used, not used, etc, unless the Reader option “Log all access Requests as used” is checked forces all card transactions as “used” to the WIN-PAK CS/SE/PE software. If the reader option “Log all access Requests as used” is not checked the PW- 5000/P-Series will wait for the status of the door.

When a card is presented to the reader, the PW-5000/P-Series waits for 20 seconds to obtain the status of the door. If the door is not used, it reports to the WIN-PAK CS/SE/PE Event Viewer with the message “Valid card, Door not Used”. The card continues to have access to the reader door as long as the door is not used after the card is swiped.

If the card is swiped at the reader and the card holder opens the door, the Event Viewer reports back a message “Valid Card, Door used”.

When the card is presented again, it will report back in the Event Viewer with messages such as, Soft Anti-Passback: AB violation, door used/ not used/Hard Anti-Passback: Anti-Passback Violation”.

1. None

   No Anti-Passback in effect

2. Anti-Passback

– Soft

Upon an Anti-Passback violation on any in/ out reader that is set for Soft Anti-Passback, the card is still granted access and reports in alarm view either:

a. "APB Violation, Door Used"

b. "APB Violation, Door not Used"

Example:

SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as “Processing Mode (SOFT)/ Direction (IN)”.

SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as “Processing Mode (SOFT)/ Direction (OUT)”.

Note: Delay “#” is grayed out.

When a card is swiped at the SIO Board 1 Reader 1 for the first time, the card is valid and is granted access, where the Alarm View displays “Valid card, door used”. If the Cardholder decides to swipe at the SIO Board 2 Reader 1, the card is granted access, where the Alarm View displays “APB Violation, Door Used”.

Note: Global Soft Anti-Passback Per Card

– Hard

Upon an Anti-Passback violation on any in/ out reader that is set for Hard Anti-Passback, the card is not granted access and the Alarm View displays” Anti-Passback” Violation: (Card #)(User Name) (Account: “account name”)).

Example:

SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as “Processing Mode (HARD)/ Direction (IN)”.

IO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as “Processing Mode (HARD)/ Direction (OUT)”.

Note: Delay “#” is grayed out.

When a card is swiped at the SIO Board 1 Reader 2 for the first time, the card is valid and is granted access and the Alarm View displays “Valid card, door used”.

If the cardholder decides to swipe at the SIO Board 2 Reader 2, the card is denied access and the Alarm View displays “Anti-Passback Violation: (Card #)(User Name) (Account:” account name”))

Note: Global Soft Anti-Passback Per Card

– Panel Based Time AB

When this option is enabled, Panel Based Timed ABA (Anti-Passback) combines Hard and Soft Anti-Passback. If a card is swiped a second time

within the set Delay time, the system becomes Hard Anti-Passback. After the set Delay Time, the Anti-Passback card is swiped a third time, the system becomes Soft- Anti-Passback resetting the delay time. When the same card is swiped again within the set delay time, the system becomes Hard Anti-Passback.

Example:

SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as Processing Mode (Panel based Timed APB)/ Direction (IN)".

SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (Panel based Timed APB)/ Direction (OUT)".

Note: Delay time is set to 30 seconds.

When a card is swiped at the SIO Board 1 Reader 1, the card is valid and is granted access and the Alarm View displays" Valid Card, door used: (card #)(User Name) (Account: "account name")).

When the same card is swiped at the same reader within the set delay time, the card is denied access and the Alarm View displays "Anti-Passback Violation: (Card #)(User Name) (Account: "account name").

If the card is swiped after the set delay time, the card is granted access and the Alarm View displays "APB Violation, door used: (card #)(User Name) (Account: "account name)).

When the same card is swiped at the same reader within the set delay time, the card is denied access and the Alarm View displays "Anti-Passback Violation: (Card #)(User Name) (Account: "account name").

Note: Global Panel Based Timed Anti-Passback Per Card.

3. Timed Anti-Passback

   – Card Based Time AB

     If this option is enabled, a card cannot be swiped twice at the same panel within the amount of time selected for the delay. Any card that is swiped at the same reader has its own delay time. If the cards are swiped at another panel reader, the cards will gain access to the Anti-Passback reader.

     Example:

     SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as "Processing Mode (Card Based Timed APB)/ Direction (None)".

     SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (Card Based Timed APB)/ Direction (None)".

Note: Delay time is set to 30 seconds.

When a card is swiped for the first time at the SIO Board 1 Reader, the card is valid and granted access.

If the card is swiped at the same reader for a second time, before the 30 second delay has expired, the card is denied access and the Alarm View displays “Anti-Passback Violation: (Card #)(User Name) (Account: “account name”)).

Note: Per Panel Card Based Anti-Passback Per Card.

– Reader Based Time APB (Anti-Passback)

If this option is enabled, a card cannot be swiped twice at the same panel within the amount of time selected for the delay or a different card to take the set delay.

Example:

SIO Board 1 Reader 1 and SIO Board 2 Reader 1 is set as "Processing Mode (Reader Based Timed APB)/ Direction (None)".

SIO Board 1 Reader 2 and SIO Board 2 Reader 2 is set as "Processing Mode (Reader Based Timed APB)/ Direction (None)".

Note: Delay time is set to 30 seconds.

When a card is swiped for the first time at the SIO Board 1 Reader 1, the card is valid and is granted access.

If the card is swiped at the same reader for a second time, before the 30 second delay has expired, the card is denied access and the Alarm View displays “Anti-Passback Violation: (Card #)(User Name) (Account: “account name”).

If a second card is swiped at SIO Board 1 Reader 1, the second card will take the delay time of the first card. When the first card is swiped at the same reader, the card is granted access and the Alarm View displays” Valid Card, door used: (card #)(User Name) (Account: “account name”)).

Note: Per Panel Card Based Anti-Passback Per Card.

How to enable any valid card read to trip an additional relay on the P-Series reader board?

1. Procedures

i) Click **ADD**

a. Procedure Name: You can define the name of the procedure.

b. Action List

i) Click **ADD**

a. Action Name: You can define the name of the action.

b. Action Target Type: Do Output Action.

c. Select Output SIO: Output that is pulsing to shunt Alarm system.

Note: Ensure that the Output has an ADV assigned.

d. Select Output Action: Pulse. You can define the name of the action.

e. Seconds to Pulse: You can define the timing of the pulse.

2. Triggers

i) Click **ADD**

a. Name: You can define the name of the trigger.

b. Procedure: Select the above procedure for multiple triggers.

c. Trigger Source Type: Reader.

d. Source SIO Board: Select SIO reader board to trigger Procedure.

e. Trigger Source: Select Reader to trigger Procedure.

f. Transaction Type: Formatted Card Number Only.

g. Trigger Transaction: Clear everything except Valid Card, Door not used and Valid Card, Door Used.

h. Time Zone: Always On “24/7”.

How to set alarm in WIN-PAK CS/SE/PE / NStar based on Database Limits and Capacities?

You can set an alarm based on the selected WIN-PAK CS/SE/PE database size. You can also monitor the hard drive size set and generate an alarm when the size is reached.

This function is used only with a MSDE\SQLExpress Database Engine.

If a complete version of SQL is installed, the Database Limits and Capacities is unavailable. The complete SQL incorporates a database maintenance which can be configured through the SQL Management Studio.

How to enable Triggers and Procedures in WIN-PAK CS?

In WIN-PAK CS, when you are programming a PW-5000/P-Series panel, the **Trigger and Procedure** tab is unavailable.

To enable the **Trigger and Procedure** tab, you must edit the windows registry:

1. Click **Start > Run**.
2. In the **Run** window, type REGEDIT. The **Registry Editor** dialog box appears.
3. In the left tree window, expand HKEY_LOCAL_MACHINE>SOFTWARE>WOW6432NODE>Northern Computers>WIN-PAK CS.
4. Right click the WIN-PAK CS folder and select **New>String Value**.
5. Right click **New Value #1** and select **Rename**.
6. Type allowusertriggers, without any space and click **Enter**.

7. Right click **allowusertriggers** and select **Modify**.
8. In the **Edit String** dialog box, under **Value data,** type 1.
9. Click **OK** and close the **Registry Editor** dialog box.

How to configure the PW-5000 or P-Series IC panel to read the Kronos cards?

To configure the PW-5000 or P-Series IC panel to read Kronos cards, you must:

1. Click **Configuration>Device>Device Map**. The Device window appears.
2. Expand the **Devices** folder.
3. Right-click the PW-5000/PRO-2200 panel and click **Configure**. The **P-Series Configuration** dialog box appears.
4. Click the **Card Formats** tab.
5. Select a card format to be used for the panel, in the **Format #** list. The format number ranges from 1 through 8.
6. Under **Option**, select the following options:
   - **Not Used:** To prevent the usage of card formats for the P-Series panel. If you select this option, all the fields are disabled. Select this option for Format #1, 2, and 3.
   - **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. Select this option for Format #4.
7. Select the Format Type as ABA and set the following:

Option	Set to...
Site Code	No Value
Card ID Offset	0
Default Formats	Unavailable
35 bit Corporate Cards	No Value
Minimum # of digits on card	1
Maximum # of digits on card	18

Option	Set to...
Site Code digits	Start digit: 1 No of: 0
Cardholder ID digits	Start digit: 5 No of: 7
Issue code digits	Start digit: 1 No of: 0

8. Click the **SIO Boards** tab. The **SIO Board Configuration** dialog box appears.
9. Under **Reader**, select the PW-5000 or P-Series SIO Board reader board and click **Edit** to edit the following fields:

Option	Set to...
Reader Types	Custom
Keypad Mode	None
LED Drive Mode	Generic 1 -wire, tri-state bi-color
Card Format Flags	Select all the card format flag types
Access Configuration	Single, controlling the door
Anti-Passback	• Direction: None • Processing Mode: None • Delay: Unavailable
Card Formats	Format 4
Control Flags	Clear all the selected control flags
Online Door Mode	Card Only
Offline Door Mode	Unlock (unlimited access)

10. Click **OK** to save and close the **SIO Board Configuration** dialog box.
11. Click **Operations** > **Control Map**. The **Control Map** dialog box appears.
12. Right-click the PW-5000 or P-Series panel in the Control Map tree, and select **Initialize**. The **Panel Initialization** Options dialog box appears.
13. To send all types of information, click **Select All**.
14. Click **OK** to update the panel details.

How to configure Windows users for WIN-PAK CS/SE/PE log on using Windows Authentication?

1. Create a group named WIN-PAK CS/SE/PE on the database server or the Primary Domain Controller of the local computer or in the domain.
2. Create a user on the database server or the Primary Domain Controller with a username of Admin (or you can use the username of the WIN-PAK CS/SE/PE admin account) and assign the user to the WIN-PAK CS/SE/PE group.
3. All the Windows users who will access and use the WIN-PAK CS/SE/PE application must be added to the WIN-PAK CS/SE/PE group.
4. In the WIN-PAK CS/SE/PE UI, click **System > System defaults**.
5. Click the **Login/Logout** tab and select the **Login using current Windows user at startup**.
6. Restart the computer and then launch the WIN-PAK CS/SE/PE UI. You can now log on with the Windows credentials.
7. Click **File > Log out**. You must now log on with the admin credentials. When you log on to the WIN-PAK CS/SE/PE UI with admin credentials, the list with all the operators in WIN-PAK CS/SE/PE, with every Windows user added to the WIN-PAK CS/SE/PE group, is populated.
8. Click **System > Operator.** You must now **Edit** the Windows users. You must now enable the users with admin rights. Or, you can also change the user to an operator and assign the appropriate operator level.
9. Log out and then log on to the WIN-PAK CS/SE/PE. You can now log on with Windows credentials and the WIN-PAK CS/SE/PE operator will have appropriate rights.

How to setup magstripe encoding and duplexing with a Fargo DTC4500 printer in WIN-PAK CS/SE/PE?

1. Click **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. Under **Printer Type**, select **Ultra Magicard**.
4. Under **Magnetic Stripe**, ensure to clear the **Encode Mag Stripe** option.
5. Select **Print Both Sides**, which is required for duplexing.
6. Click **OK**.

Setting Up the Badge Layout

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

2. Click **Add** to add a new badge layout or **Edit** to edit an existing layout. The **Badge Definition** window appears.
3. Create a text box in the badge layout. Right click the text box and click **Properties**. The **Badge Element Layout** window appears.
4. In the **Text Block** tab, insert the text based on the following list:

- ~ = tells the printer to print on the back of the following layout
- 1, 2 or 3 = represents the track number
- ; or % = separator used for recognizing the following as the data to encode
- ? = signals the end of the command

For example:

- ~1%{Card Number}? (Note: track 1 requires that "%" is used as the separator, all others are ";"
- ~2;{Card Number}?
- ~3;{Card Number}?

5. Click **OK** in the **Badge Element Layout** window.

Note: The information entered in the text box is not printed on the card if you enter incorrect information.

How to manually remove WIN-PAK CS/SE/PE Services through a command line prompt?

When you try to remove WIN-PAK CS/SE/PE services through the WIN-PAK CS/SE/PE System Manager present in Windows 7 or Server 2008 Operating Systems, the WIN-PAK CS/SE/PE displays the following error message.

The following list displays the WIN-PAK services:

- **WPDatabaseArchiveService:** WIN-PAK Archive Database Server
- **WPCommandFilerService:** WIN-PAK Command Filer Server
- **WPCommunicationService:** WIN-PAK Communications Server
- **WPDatabaseService:** WIN-PAK Database Server
- **GuardTourService:** WIN-PAK Guard Tour Server
- **WPMusterService:** WIN-PAK Muster Server
- **ScheduleService:** WIN-PAK Schedule Server

You must use the following command syntax to stop and remove the WIN-PAK CS Service through the command line:

- sc stop <service name>
- sc delete <service name>

The following example displays the procedure to stop and delete the **Muster Server Service**:

- In the command prompt window, type **sc delete WPMusterService**.

- The **WIN-PAK System Manager** enables you to reinstall any of the **WIN-PAK CS/SE/PE Services.**

§ You can click **Install** to reinstall the required **Muster Server service**.

How to define a Pre-Alarm trigger to energize an output?

A Pre-Alarm is the time specified before the door reports an ajar that can trigger an output or relay for a warning (typically a beeping sound) that indicates that the Pre-Alarm is activated.

(Door Contact Shunt Time) - (Pre-Alarm Time) = (Pre-Alarm)

Application

The specific application outlines how to set up a pre-alarm to energize another output when a door is held open. When the door closes or returns to a normal condition, the output de-energizes and the sounder or specific device wired to the relay trips off.

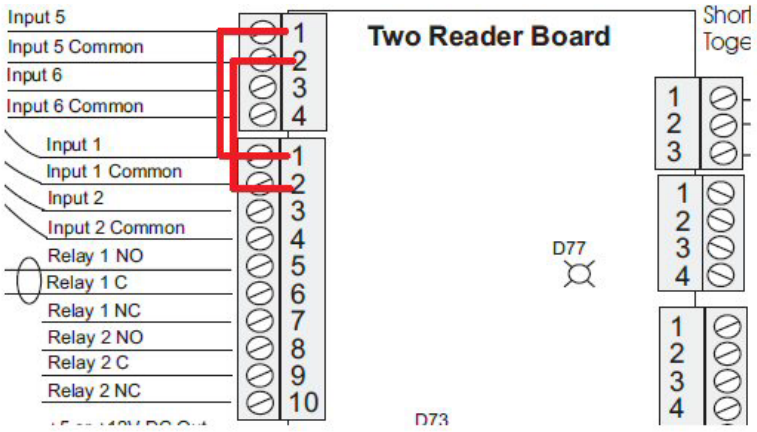
This application requires 2 Input points and 1 Output point.

- Input 1 (Door Contact) to energize the Output on a Pre-alarm
- Input 5 (Hardwired to Input 1) designed to de-energize the output when the door returns to a normal condition

Input # 1 assigned a 20 second Shunt time and a 5 second Pre-alarm time. If a valid card is presented at the reader or a valid egress, the door will unlock and in turn shunt the door contact for 20 seconds. If the door opens and is held open for longer than 15 seconds, the output 2 will energize and if the door closes or returns to normal output 2 will de-energize. If the door is held open past the held open time of 20 seconds then the door contact will trip an additional relay.

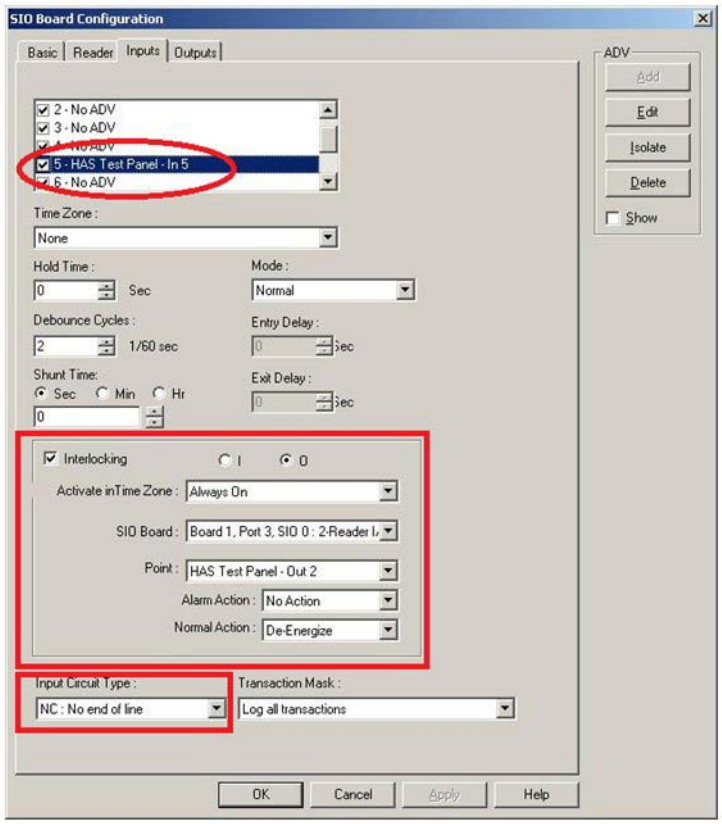
Wiring

The wiring image details that the Input 5/Input 1 and Input 5 Common/Input 1 Common are wired in parallel on the PRO22R2 board.



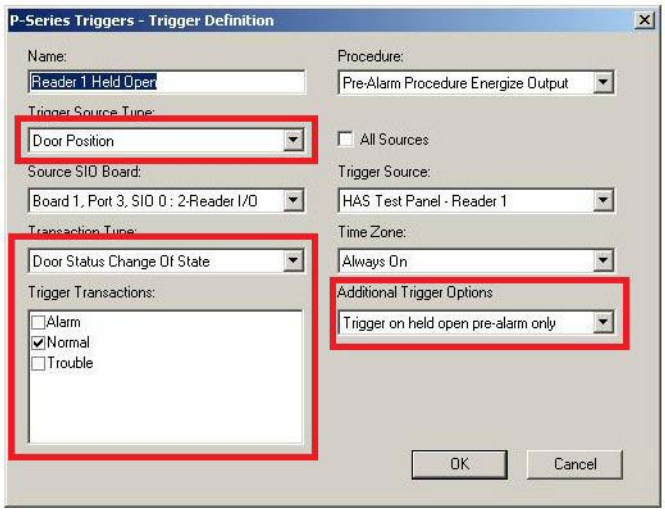
Inputs

The inputs image outlines how to set up the input interlock.



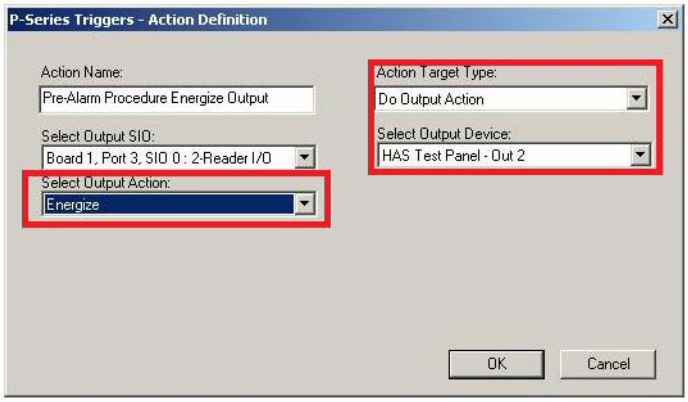
Triggers

The triggers image outlines how the trigger needs to be configured for the Pre-Alarm associated to Input 1.



Procedures

The procedures image outlines how to configure a procedure to fire output 2 upon being triggered.



If configured correctly, the pre-alarm triggered upon door held open will energize secondary outputs useful for sounders/buzzers/alarms of any kind. After the door closes, that is, when it returns to the normal state, it will de-energize the output.

How to define procedure Timezone for PW-5000 and P-Series?

You must define the actions for enabling and disabling timezones within the configuration of a procedure. The following table defines the procedure and action to set timezones.

Procedure	Actions
Clear All Commands Time Based State	Sets the selected timezone back to its original timezone.
Enable Timezone Permanently	Sets the selected timezone to ‘24 Hours’.
Disable Timezone Permanently	Sets the selected timezone to None.
Disable Timzone Until Start Time	Sets the selected timezone to ‘None’ until the start time of the selected timezone.
Disable Timzone Until End Time	Sets the selected timezone to ‘24 hours’ until the end time of the selected timezone.

How to set the PW-5000 or P-Series relay or relays to latch and time

zone controlled?

Scenario 1: The first cardholder to arrive at the main entrance swipes the card at the reader which latches the relay 1 on and activates the relay 1 Time zone assigned to it. When the time zone expires, the door locks.

Scenario 2: When few cardholders swipe at the second reader, relay 3 latches and activates the relay Time zone assigned to it. When the time zone expires, the door locks.

Procedures:

1.In the WIN-PAK CS/SE/PE UI, click **Configuration** > **Time Management** > **Time Zone**.

i) Under Operations, click **ADD**.

a. In the Time Zone tab, enter a name for the Time Zone. For example: **Main Entrance Time**.

b. Set the time at which you want the relay to be switched ON.

c. Click **OK**.

2. In the WIN-PAK CS/SE/PE UI, click **Account > Select**.

ii) Select the **Account** and click **OK**.

Note: You can follow the above procedure to add multiple time zones.

3. Click **Configuration > Device > Device Map**. The Device window appears.

i) Right-click the **PW-5000/P-Series** panel and click **Configure**.

ii) In the **System** tab, select **Enable card** user levels for trigger control.

iii) In the **Time Zones** tab, select the time zone for the relay control.

iv) In the **SIO Boards** tab, select and edit the **Board 4, Port 3, SIO 0: 2- Reader I/O**.

v) In the **SIO Board Configuration** dialog box, click the **Reader** tab.

vi) Select the Reader you want to assign a time zone and click **Door Interlocks**.

a. Select Direct Point.

b. Assign a Time zone.

c. Click **OK**.

4. Click the **Triggers and Procedures** tab.

5. Under **Procedures** in the left pane, select **Main Entrance Latch**.

6. Click **Add**.

7. In the **P-Series Triggers - Procedures Definition** window, add the following.

Option	**Set to...**
Procedures	
1. Procedure Name	Type a name. For example, Main Entrance Latch
2. Action List	Click Add. The . P-Series Triggers- Action Definition window appears.
a. Action Name	Type a name. For example, Trigger 1 Latching Relay 1.
b. Action Target Type	Do output action
c. Select Output SIO	Select the reader SIO Board. For example, Board 1, Port 6, SIO: 2-Reader I/O.
d. Select Output Device	Specify the device. For example, SIO Output 4.
e. Select Output Action	Energize
Click **OK**	
3. Action List	Click **Add**
a. Action Name	Type a name. For example, Delay 2.
b. Action Target type	Delay
c. Seconds to Delay	2 seconds
Click **OK**	
4. Action List	Click **Add**
a. Action Name	Type a name. For example, Executive TZ Control.
b. Action Target Type	Time Zone Control
c. Select Time Zone Action	Enable Time Zone Until End Time
d. Select Time Zone	Select Entrance time zone
Click **OK** in both the windows	

8. Under **Procedures** in the left pane, select **Executive Latching**.
9. Click **Add**.
10. In the **P-Series Triggers - Procedures Definition** window, add the following.

Option	**Set to...**
Procedures	
1. Procedure Name	Type a name. For example, Executive Latching
2. Action List	Click Add. The P- Series Triggers – Action Definition window appears.
a. Action Name	Type a name. For example, Executive latching relay.
b. Action Target Type	Do output action
c. Select Output SIO	Select the reader SIO Board.
d. Select Output Device	Specify the device. For example, SIO Output 3.
e. Select Output Action	Energize
Click **OK**	
3. Action List	Click **Add**
a. Action Name	Type a name. For example, Delay 3.
b. Action Target type	Delay
c. Seconds to Delay	2 seconds
Click **OK**	
4. Action List	Click **Add**
a. Action Name	Type a name. For example, Executive TZ Control.
b. Action Target Type	Time Zone Control
c. Select Time Zone Action	Enable Time Zone Until End Time
d. Select Time Zone	Select Executive time zone
Click **OK** in both the windows	

11. Under **Triggers** in the left pane, select **Executive Trigger Latching**.
12. Click **Add**.
13. In the **P-Series Triggers - Triggers Definition** window, add the following.

Option	**Set to...**
Triggers	
Name	Type a name. For example, Executive Trigger Latching
Procedure	Select Executive Latching
Trigger Source Type	Reader
Source SIO Board	Reader Board
Trigger Source	Reader 2
Time Zone	Always on
Trigger Transactions	Clear all and select only Valid Card, Door Not Used and Valid Card, Door Used.
Card User Level to Trigger on	Type 1
Click **OK**	
Name	**Type a name. For example, Trigger Latching**
Procedure	Select Main Entrance Latch
Trigger Source Type	Reader
Source SIO Board	Reader Board
Trigger Source	Reader 1
Time Zone	**Always on**
Trigger Transactions	Clear all and select only Valid Card, Door Not Used and Valid Card, Door Used.
Card User Level to Trigger on	Not used
Click **OK** in both the windows	

14. Click **Card > Card Holder**. The **Card Holder** window appears.

15. Search for an Executive Card holder and under **Operations**, click **Edit.** The **Card Holder** window, with the details of the selected card holder, appears.
16. Click the **Cards** tab.
17. Select the card and click **Edit**. The **Card Record** window appears.
18. Under **P-Series Trigger Control**, select **1** in the **User Level** field.
19. Click **Operations > Control Map**. The **Control Map** window appears.
20. Select the **P-Series Panel** and initialize.

How to explain the usage of crash bar in a PW-5000 or P-Series panel, which in turn causes a Forced Open alarm?

When you are using a PW-5000 or P-Series panel system and when a crash bar is used to exit through one of the doors, the door opens with a “Forced Open” alarm.

What occurs is, the door is being opened before the egress can shunt the Door status point. For example, when a person pushes or hits a Crash Bar, everything happens very quickly at the panel. The IC Board encounters both the points going into alarm at once. But as the panel cannot process this information at once, it starts to scan at the lowest input, checks this point for changes, and updates the system accordingly. The IC scans the next point and continues until all inputs have been checked.

For example, someone uses the crash bar on Door 2, input 3 (Door 2 status input) and input 4 (Door 2 egress) both go into alarm at once. Following the above description, the IC first checks Input 3 and see it is in alarm, which then causes a Forced Open alarm. The IC then checks input 4, which in turn shunts input 3. If the system had checked input 4 first, the Forced open would not have been reported since input 4 would have shunted input 3.

The following list defines the possible solutions:

1. In the WIN-PAK CS/SE/PE or INTL, each of the 2 door inputs have a default Debounce Cycles option.
    a. Edit the 2-Reader SIO Board and click the **Inputs** tab.
    b. Select one of the **Door Inputs**.
    c. The left pane in the window lists the **Debounce Cycles**. The range is from two to fifteen 60ths of a second. The default value is 2 for all inputs.
    d. For the **Door Status** inputs, modify to a higher value. You are suggested to modify he value to 6. The value of 6 is also the new default value for the Status inputs.
2. You can also modify the programming and wiring so that the status inputs are after the egress points. For example, the standard default setup is as follows:

- Input 1 is the door 1 status input
- Input 2 is the door 1 egress
- Input 3 is the door 2 status input
- Input 4 is the door 2 egress

You must reverse the programming by modifying the inputs.

- Input 1 as door 1's egress
- Input 2 as door 1's status input
- Input 3 as door 2's egress
- Input 4 as door 2's status input

Also, you must ensure to physically reverse the wiring on the board.

3. In the WIN-PAK CS/SE/PE or INTL builds 381 and later, there is a new option that has been added called Reverse I/O poll Sequence.
    a. Edit the 2-Reader SIO Board.
    b. Click the Basic tab to view the option **Reverse I/O poll.**

- When **Reverse I/O poll** is disabled (default in WIN-PAK CS/SE/PE), the IC checks the inputs and outputs starting at the lowest point (Input 1 or Output 1) and work its way up to the last input or output on the board.
- When **Reverse I/O poll** is enabled, the IC checks the inputs and outputs starting at the highest point (Input 16 or Output 16 in most cases) and work its way down to the first input or output on the board.

How to configure WIN-PAK CS/SE/PE Server for multiple communication servers?

Notes:

- Ensure that you are logged into Windows with administrator privileges. Also, you must be logged into the WIN-PAK CS/SE/PE with complete privileges.
- Before you configure the WIN-PAK CS/SE/PE with multiple Communication Servers, ensure that the WIN-PAK CS/SE/PE application is licensed for multiple Communication Servers.

A. Communication Server Configuration - Basic Information

1. Click **Configuration > Device > Device Map**. The **Device** window appears.
2. Right-click the **Devices** folder, click **Add** and click **Communication Server**. The **Comm Server Configuration - Basic Information** dialog box appears.

Note: In the additional Communication Servers that must be added, ensure that the Protocol end point is modified. If you do not modify the Protocol end point, you will receive the Protocol end point 5566 is already in use by Server “Server name” message.

3. Type a **Name** (maximum of 30 characters) for the communication server.
4. Type the **Description** (maximum 60 characters) 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. See **Configure an Abstract Device** 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. By default, the local Machine Name appears for the communication server.

Notes:

You can click the button to browse and locate the local machine. Or, you can type the computer name or IPAddress of the computer in which the Communication Server is installed.

8. Type a **Protocol end point** number that is not used by any other application or service on that computer. You must modify the end point number to 5567 or higher (maximum of 65535).
9. Retain the default value of the **Alarm Priority for notification** value. An action with lower priority than this value is displayed as an event in the Event view.
10. Retain the default value of the **Alarm Priority for required acknowledgment** 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.
11. Clear the **Write Transactions to file?** check box. If selected, this file is used for debugging purposes. In the **Operating System** area, the OS of the WIN-PAK CS/SE/PE system is displayed.
12. Click **Next**. The **Com Server Configuration - Ports** dialog box appears.
13. In the **Ports** list, select the required check boxes for the COM port that are used on this server for the access control equipment.
14. 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.

15. Click **Next** and then click **Finish** to add the communication server to the Device Map.

B. WIN-PAK CS User Interface (UI) and Communication Server Configuration

To set the user interface workstation,

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK CS/SE/PE 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.
6. Retain the default **RPC Endpoint** value.
7. Under **Database Archive**, type the computer name or IP address of the server in the **Node Name** field.
8. Retain the default **RPC Endpoint** value.
9. Click **OK**. This enables you to start up the User Interface with the new database server.

To set the communication server configuration,

1. Click **Start > Programs > Honeywell Access Systems > WIN-PAK CS/SE/PE System Manager**. The **System Manager** window appears.
2. Click the appropriate server tab.
3. Type the **DB Server Node Name**. This is the location for the Database Server.
4. Retain the default **DB Server Endpoint** value.
5. Click **OK** to save the changes and close the **System Manager** window.
6. Click the **WIN-PAK CS/SE/PE Service manager** to STOP and START the WIN-PAK CS Communication Server.
7. Log on to the **WIN-PAK CS/SE/PE UI** and click **Operation > Control Map**.

You must verify if the status icon for both local and remote Communication Server is green.

How do I shunt the door contact using the door egress on a PW-5000/P-Series panel?

1. Click **Configuration > Device > Device Map > Communication Server**. The **Device** window appears.
2. Right-click the **Devices** folder, click **PW-5000** or **PRO-2200 Loop** and click **Configure**. The **Panel Configuration - Basic dialog** box appears.
3. Click the **SIO Boards** tab and select the Reader SIO board type.
4. Click **Edit**.
5. Click the **Reader** tab and select the reader you want the door egress to shunt the door Status point.
6. Click **Door** Interlocks to display the **Door Interlocks** dialog box.
7. Use this dialog box to edit the default settings of the **Free Egress Input**.
8. Select **None** for the SIO Board.
9. Click **OK**.
10. In the **SIO Board Configuration** dialog box, click the **Inputs** tab to configure the input point details of SIO Board.
11. Select the **Input 2 (Reader 1 door egress)** input point and create an ADV for the Input 2. Here you can decide on the alarm or trouble condition of an input point.
12. Click **OK**.
13. Add the following in the **Triggers and Procedures** tab.

Option	**Set to...**
Procedures	
1. Procedure Name	Door Egress shunts door status
2. Action Name	Door Status Shunt
a. Action Target Type	Door Forced Mask
b. Select Reader SIO Board	Select the SIO reader board which will shunt the door status. For example, Board 1, Port 6, SIO: 2-Reader I/O
c. Select Reader Device	Select the reader. For example, PW-5000-R1
d. Select Door Action	Mask Forced open alarm
3. Action Name	Delay 1

Option	Set to...
a. Action Target Type	Delay
b. Seconds to delay	Specify the delay. For example, 15 seconds.
4. Action Name	Energize Relay 4
a. Action Target Type	Do output action
b. Select Output SIO	Select the reader SIO Board. For example, Board 1, Port 6, SIO: 2-Reader I/O.
c.Select Output Device	Specify the device. For example, SIO Output 4.
d. Select Output Action	Energize
5. Action Target type	Delay 2
a. Action Target type	Delay
b. Seconds to Delay	1 second
6. Action Name	Door Status Un-shunt
a. Action Target Type	Door forced mask
b. Select Reader SIO Board	Select the SIO reader board which will shunt the door status. For example, Board 1, Port 6, SIO: 2-Reader I/O.
c. Select Reader Device	Select the reader. For example, PW-5000-R1.
d. Select Door Action	Unmask forced open
7. Action Target type	Delay 3
a. Action Target type	Delay
b. Seconds to Delay	1 second
8. Action Name	De-Energize Relay 4
a. Action Target type	Do output action

Option	Set to...
b. Select Output SIO	Select the reader SIO Board. For example, Board 1, Port 6, SIO: 2-Reader I/O.
c. Select Output Device	Specify the output device. For example, SIO Output 4.
d. Select Output Action	De-Energize
Triggers	
Name	Name: Input 1 Shunt
Procedure	Door Egress shunts Door Status
Trigger Source Type	Input
Source SIO Board	Reader Board
Trigger Source	Input 2
Transaction Type	Change of State
Trigger Transactions	Clear all and select only Alarm
Timezone	Always on

14. You must wire the extra Output (For example, Relay 4) Parallel to Input 1

Notes:

- If the Input 1 is **Normally Open** or **Normally Close**, you must wire to the Output accordingly.
- After the door egress is configured to the WIN-PAK CS/SE/PE application, no free egress is granted through the door.

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 CS/SE/PE 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.

How to resolve the Low Virtual memory error message in Windows operating system which restricts WIN-PAK from normal operation?

Due to the compatibility issue of McAfee HIP service with MSSQL, the low virtual memory error message appears.

To resolve this issue, you must remove the McAfee HIP service. For more information, refer to

http://social.msdn.microsoft.com/Forums/sqlserver/en-US/403e8bf1-0e72-4c5f-96e5-f07e0311dfc5/sqlservrexe-high-commit-usage-causing-a-low-virtual-memory-conditions?forum=sqlsetupandupgrade

Move Loops and Panels

Note: This section is applicable only in WIN-PAK CS.

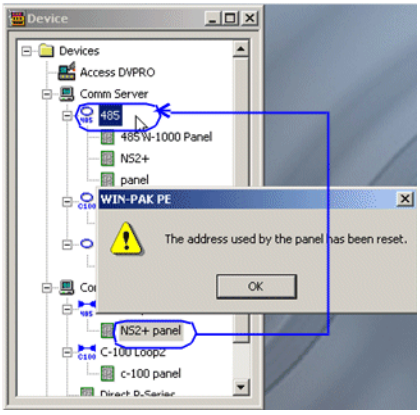
You can move loops and panels across communication servers if the following conditions are met:

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

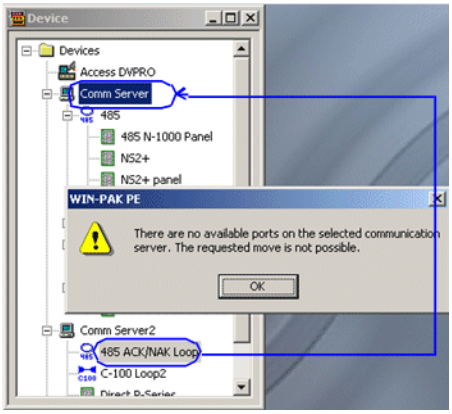
To move a loop across communication servers:

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.

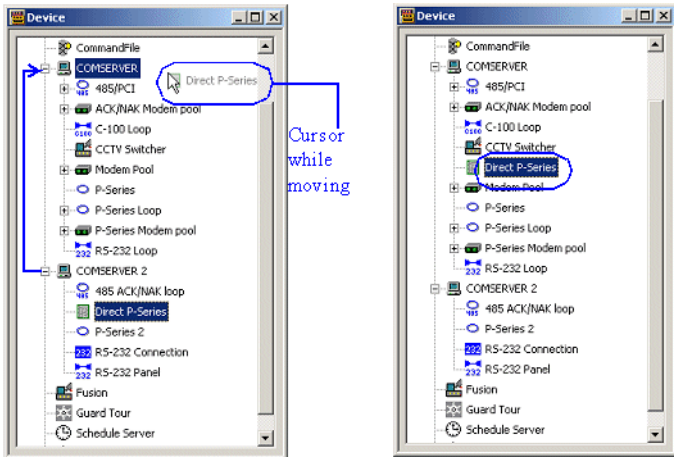
Note: If the destination communication server does not contain a port and if you attempt to move a loop, the following message appears:



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.



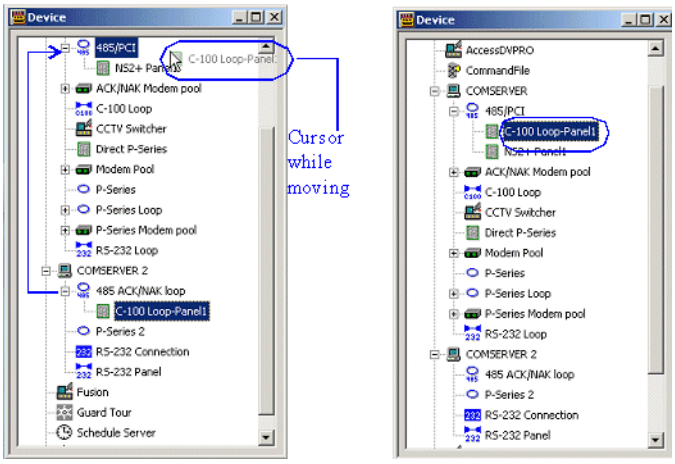
3. Release the mouse button at the destination communication server. The direct panel is moved.

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.

Set up System Account and Enable API

Pre-requisites

Prior to setting up a system account and enabling the API, you must meet the following pre-requisites:

1. The end user organization must already have an account in the HID Mobile Access Production Portal (https://managedservices.hidglobal.com).
2. The PACS solution integrated with the portal must have been validated by Partner Services.

If the end user organization does not have an account in the HID Mobile Access Production Portal, they must contact their Sales Representative or the HID Mobile Orders team.

Enable Production API

In order to enable the Production API:

1. Send an email to tpp@hidglobal.com in the template format given below. It takes up to 2 business days to process the request.

Dear Partner Services Team,

Please enable access to API for our production accounts. Find the required information below:

- Organization Name - [Enter your exact organization name of the account on the production portal]
- Solution Name - [Enter the name of the PACS solution to be used with your account]

2. Once the account has been set up, Partner Services will provide a confirmation over email.

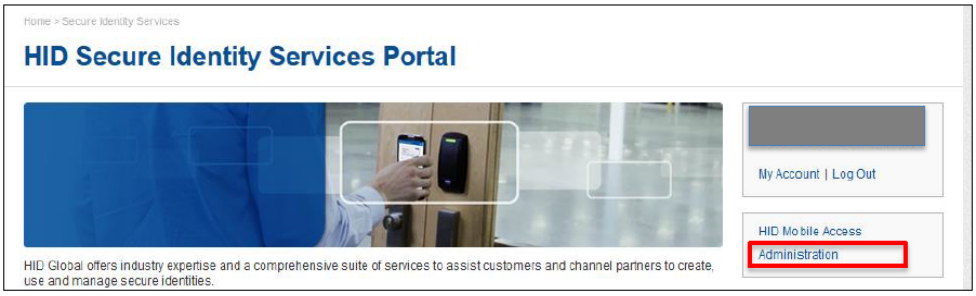
After the account has been set up, the user must set up the system account.

Set up System Account

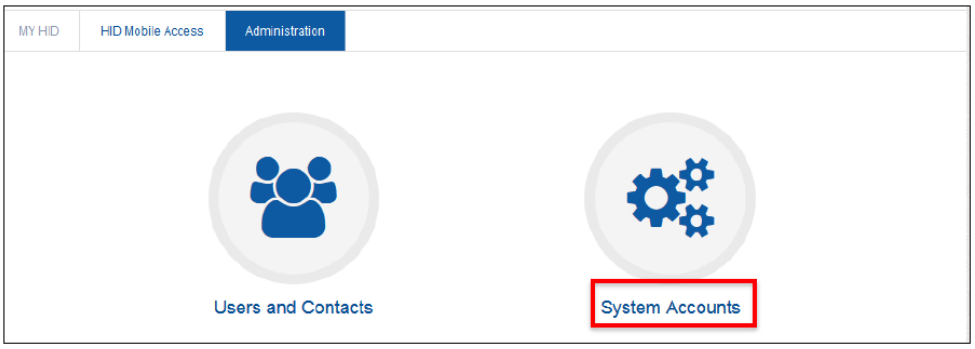
Note: You need to be an Org Admin to view the options below and set the Client Authentication.

In order to setup the Client ID and Client Secret to access the Portal API, you must do the following:

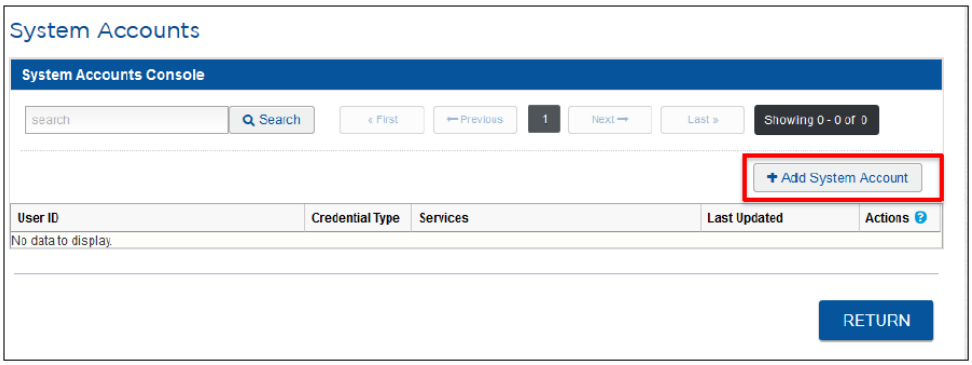
1. Ensure that your Service Provider has registered you on the https://managedservices.hidglobal.com portal as an Org Admin.
2. Ensure that your Service Provider has enabled the Portal SDK for your account.
3. Log in to https://managedservices.hidglobal.com using your administrative credentials (email ID and password).
4. Click on **Administration** on the right panel.



5. Click **System Accounts**.



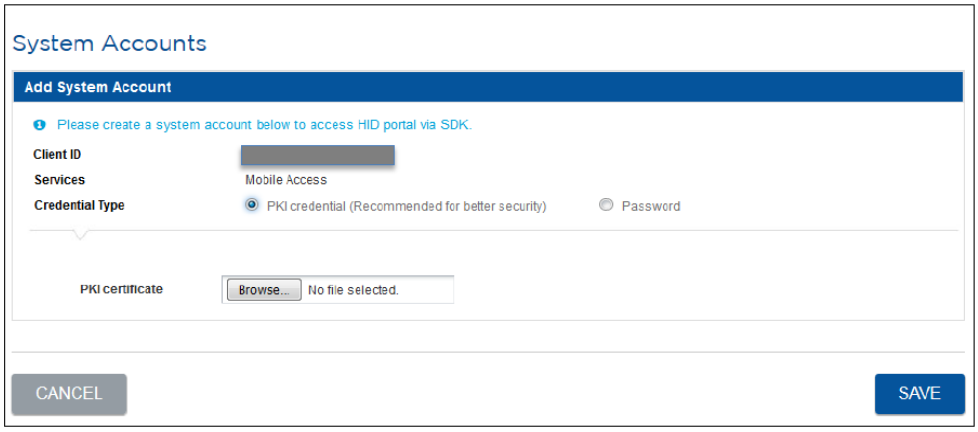
6. In the section **System Accounts**, click **Add System Account.**



7. You can choose the **Credential Type** as per your requirement.
   - To use PKI Credentials, see Using PKI Credential
   - To use password, see Using Password
8. Click **Save**.

Using PKI Credential

If you would like to use your PKI Credential, select PKI Credential and browse for the .cer file that contains the public key.



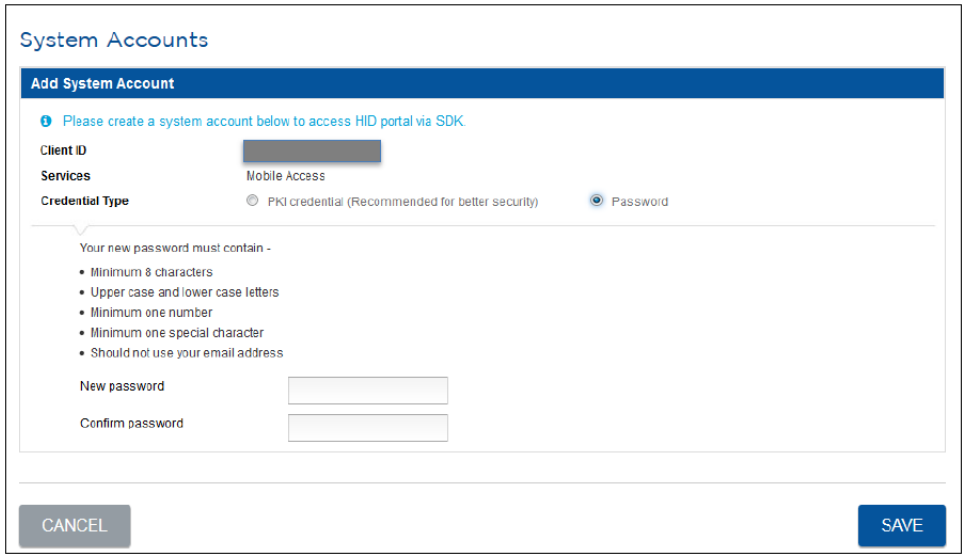
The following CAs are supported:

- Verisign/Symantec: Standard, Premium SSL
- GeoTrust: QuickSSL, True Business ID
- IdenTrust: TrustID Personal, Business

Note: Other vendors can be supported; however you will need to inform tpp@hidglobal.com in advance so these vendors can be verified. Self-signed certificates are not supported.

Using Password

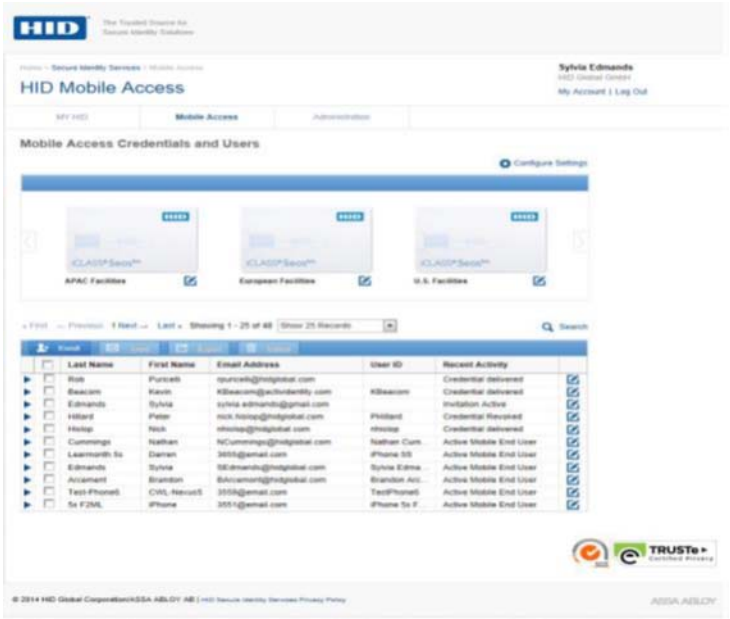
If you would like to set a password, select Password, and then enter a password which satisfies the five given criteria shown below.



Warning: Once the password has been set, it cannot be viewed. It is advised that you remember it carefully. If the API is being used by multiple people, it is advisable that each time when the password is changed by the org admin, it is discreetly given to all the users without compromising the security.

Managing HID users through Secure Portal

The WIN-PAK administrator manages users, issues/revokes mobile IDs through the **Secure Identity Services** portal.



Configuring HID Readers

To configure the HID readers in the mobile device:

1. Open **Play Store** application in the mobile device.

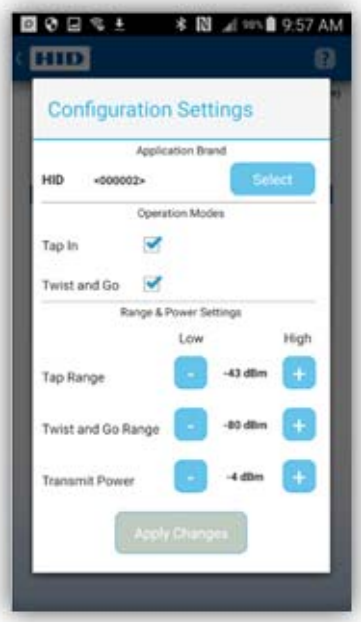
2. Search for HID **BLE Config App** and then tap **Install**.

3. Open the **BLE Config App** and then tap **Scan for Readers**.

4. Scan to select the installed HID reader.

5. Tap **Set Configuration**.

6. Add the **Configuration Settings** for the reader.



7. Tap **Apply Changes**.

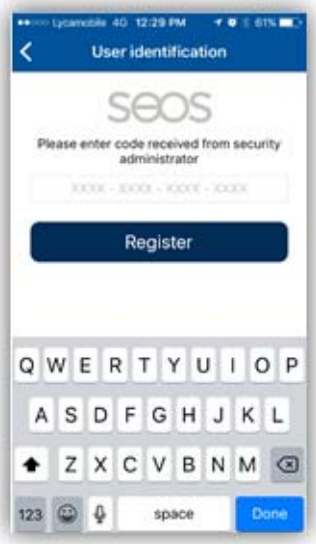
Configuring HID Cards

To configure the HID cards in the mobile device:

1. Open **Play Store** application in the mobile device.
2. Browse to https://play.google.com/store/apps/details?id=com.hidglobal.mobilekeys.andr

oid.v3 (for Android) and https://appstore.com/hidmobileaccess (for iOS) and then tap **Install**.

3. Tap **OPEN**.
4. Enter the registration code.



5. Tap **Register** to register the app with the configuration key.

Glossary

12 Digit Cards: Cards that use a combination of a 9-digit card number with a 3-digit issue number. This term also refers to applications that require a card number greater than 65,535. It is usually implemented for bar code and magnetic stripe applications. WIN-PAK PE supports up to 16 digits but these are still referred to as 12-digit applications.
485 ACK-NAK: A communications verification system of the 485 converter which double-checks that information packets have been sent and received from one device to another.

A

Abstract Device: A logical representation of a physical device (e.g., a communication server, control panel, or door). Similar in appearance to an icon, an ADV is associated with an actual device in your access control system.
Access Control: Controlling entry into a physical area by means of a controller and electronic components including locks, readers, sensors, buttons and more. This term can also refer to controlling access into a computer.
Access Level: A level of authorization defined by a reader (or readers) and the time periods during which those readers can be accessed.
Access Point: A physical point of entry or exit, such as a door or gate, which is controlled by the system.
Account: A division within an access control system that segregates the card and card holder information of one group of users from the card and card holder information of another group of users; for example, in a multiple-tenant building, each tenant can be set up as a separate account.
ACK: Abbreviation for Acknowledge.
ACK-NAK: A communications verification system of the 485 converter which double-checks that information packets have been sent and received from one device to another.
Activate: Enable. Make functional. See Energize.
Activation State: Indicates the behavior of an activated output point.
ADV: An abstract device; a logical representation of a physical device (e.g., a communication server, control panel, or door). Similar in appearance to an icon, an ADV is associated with an actual device in your access control system.

Address: The identification number of a specific control panel.
Alarm: A signal that indicates a problem.
Alarm Input: A physical input terminal on a control panel. The point at which an input device is connected to a control panel.
Alarms View: A display window that shows alarm activation and enables an operator to respond to situations reported on the system.
Alarm Priority: Priority rankings of 1 to 99 are assigned to alarms. Priority 1 is the highest and 99 is the lowest.
Alarm State: On an input, this refers to the state that is the opposite of a normal state. Software can recognize an input when that input goes into alarm, unless some other condition (such as a shunt) applies.
Alarm Type: An alarm determined by its unique priority, global shunt status, forced note, auto clear and RTN separate alarm characteristics, and the message displayed when an alarm is reported.
Alphanumeric: A combination of numeric, alphabetical and, in some cases, symbol characters.
Annunciation: A device that indicates a condition. This condition can be announced by a message on a computer monitor, a flashing sign, a bell or similar device, or by a combination of these events.
Anti-Passback: An access control feature that reduces the likelihood that two or more people can use the same access credential to gain admission to a controlled area. This is done by requiring that the credential be presented upon entrance to an area and again when leaving the area. If the same credential is used for two entrances without an exit in between, an alarm is triggered and access is denied.
Arm Points: Enable specific input points to report alarms when they occur.
Arm: To enable.
Audit: The act of checking something to make sure it is correct; for example, checking wiring connections.
AUX Port Alarm: An alarm triggered when the panel senses a communication failure from the auxiliary port.

B

Badge: A card that provides information about the person who is using it; usually a photo ID.
Badging: The act of creating an ID card. Photo badging includes a picture on the card.
Bar Codes: A series of black lines of various thicknesses that represents a code that is read through an optical reader and interpreted by a computer or EAC system.
Battery Backup: A battery that supplies power to a device when standard primary AC power has been abruptly cut off.
Battery Low Alarm: A soft alarm that announces that the battery on a control panel is low.

Biometrics: The ability to use a person's physical characteristics, such as an eye, to uniquely identify a person.
Buffer: To store transactions in the panel's RAM memory. Once stored, the information can be retrieved at a later time (called unbuffering the panel). See also Hard Buffer/Soft Buffer and Hard Unbuffer/Soft Unbuffer.
Buffer All: The act of buffering all panels.

C

Capture: Acquire a graphic image by scanning or video.
Card: Any type of credential used to carry electronic information in an electronic access control system.
Card Event: A card read. WIN-PAK PE can be programmed to initiate a variety of actions in response to a card event, depending on the status of the card.
Card Holder: A person who has been enrolled into the access control system.
Central Station (CS): A remotely located control and monitoring center that supplies a client with monitoring services.
Chain of Events: A process that starts at one device and triggers numerous other devices and/or actions before it is done.
Cold Restart: Restarting a panel after the power has been completely removed, then restored. This might happen after a storm knocks out power to the area. After a cold restart, a panel's programming is missing and the panel needs to be initialized.
Communications Loop: See Loop.
Configuration: The way in which computers, software and related equipment are interconnected to operate as a system.
Contact: An electrical switch that can be in an open or closed state. That state may be electrically, magnetically or physically controlled.
Continuous Reads: A software setting that enables a panel to continuously monitor a card reader and/or keypad. If this setting is not enabled, all cards and keypunches are ignored until the panel completes the actions dictated by the previous card read or keypunch.
Control Panel: A specialized computer that manages access for specific doors and related devices (e.g., PW-2000).
CPU: Central processing unit. It is the main chip (microprocessor) in a computer and control panel.

D

Data: Information. At the lowest level, data is represented as an electrical signal and interpreted as a code. At the highest level, data represents information that people can read and understand.
DC: Direct Current.

De-energize: To remove energy from an output point. On a system, the normal state of an output point is "de-energized."
Default: A standard condition or setting. Default settings are those provided by software prior to customization by the user.
Default Time Zone: A standard Time Zone that is always in effect unless overridden by another process or feature.
Dial-Up: (Also dial-in, dial-out) A system of control panels connected to a communications line (loop or multi-drop) that is not directly connected to a computer. To communicate with the panels, the computer must use a modem at its end to connect with a modem on the communications line. The act of establishing a connection is called dialing, as in “dialing a telephone number”.
Disable: To render a function or feature unavailable.
Distributed Processing: The ability of control panels connected to a single communications loop or multi-drop line to function independently of one another, yet communicate to and receive information from a central computer.
Distributed System: A computer network wherein each device (a PC or control panel) can work independently of one another, yet at the same time, communicate with one another.
Documentation: Any written record of activities and processes.
Door Contact: A position locator that senses when a door is fully closed or open.
Duplex Printing: Printing on two sides of a single material, such as two sides of an access card.
Duress Alarm: A special alarm from a keypad reader which indicates that the card holder is being forced to provide entry to a secured area.
Duress: An event in which a card holder is being forced to provide entry into a secured area by an unauthorized person or people. A keypad can be configured in a way to produce a duress alarm when the user types in the PIN.

E

EAC: Abbreviation for Electronic Access Control.
Egress Button: A button by a controlled door which, when pushed, sends a signal to the controller indicating that someone wants to leave the area. This device may also mechanically allow the door to unlock, overriding the control.
Egress: To exit. See also free egress.
Electronic Access Control: Controlling entry into a physical area by means of a controller and electronic components including locks, readers, sensors, buttons and more.
Enable: To make a feature or function on the system usable.
Enclosure: An electrical utility box. It can hold control panels, splices, power outlets, etc.
Energize: Activate. Often refers to the state of an output point. Output points are in a normal state when they are “de-energized”. An energized state means that the output is active.

EPROM: Erasable Programmable Read-only Memory.

Exit Button or Switch: When pressed or tripped, this device allows a person to exit from a controlled area. See also free egress.

Exit Reader: A reader that controls egress from a controlled area; used in anti-passback applications.

Escort: A mode that requires a supervisor escort to allow entry by an employee card holder. When this mode is enabled, the reader LED changes color four times per second (usually red then green) and employees must be accompanied by a supervisor to gain entry. When the supervisor presents his card, the LED goes solid red for 10 seconds, pending an employee credential. When the employee credential is swiped within 10 seconds of the supervisor card swipe, the door opens to admit the employee and the LED returns to rapid flashing. If the time expires and there is no employee credential swipe, the LED returns to rapid flashing and the reader returns to escort mode

F

Facility Codes: The first part of the ID number on some cards, providing a higher degree of security against a duplicate card number being used in a system.

Fail Safe Lock: A lock that is in the unlatched or unlocked state when the unit is not energized.

Fail Secure Lock: (Also known as Non-Fail Safe.) A lock that is in the latched or locked state when the unit is not energized.

Firmware: The computer chip (PROM or EPROM) that runs a control panel. Firmware chips are identified by a version number.

Floor Plan: A view made up of ADVs placed on a Floor Plan background, showing the layout of an access control system; used to monitor and control devices in the system.

Floor Plan Background: A Floor Plan, graph or other digital graphic saved as a Windows Metafile (.wmf) that can be used to create a Floor Plan view.

Follow: In an interlock, a second point (component B) takes on the same state as the triggering point (component A). See Invert Follow.

Forgiveness: This feature adjusts the use of antipassback to accommodate people who did not properly exit the antipassback area. When forgiveness is enabled, a person who did not use the proper exit reader will be allowed to use the enter reader the following day without an antipassback violation occurring. For example, a card holder who enters a controlled area, but does not leave until the next day, would cause the system to go into alarm the next day because the card was not used to check in before checking out.

Format J: Enables the J card format on a panel. This accommodates the 35-bit card number where the first 20 bits are read as the card number and the balance as the site code.

Format L: Enables the L card format option on a panel. This allows the card number to be linked with the site code, creating one linked card number.

Free Egress: Allows a person to exit without requiring the presentation of a credential. This is usually accomplished by using an egress button, a motion sensor that trips a momentary shunt of the door alarm input, thus allowing exit without an alarm.

G

Global Shunt: A period of time when all the points assigned to an event type are shunted, regardless of time zones entered on individual points records.

Ground Connection: A point where a cable is bonded to the grounding system.

Ground Fault: A grounding problem that needs to be corrected for proper system operation.

Grounding System: A unified (bonded) system designed to drain excess electrical energy from a circuit in order to protect life and property, and reduce the potential for signal interference.

Group: A group of output points that are activated by an input point or reader. This usually refers to a configuration used to program elevator cab door access control.

H

Hard Buffer/Soft Buffer: A hard buffer command overrides any number of soft buffer/unbuffer commands. If a panel receives multiple unbuffer commands, it will remain buffered until it receives the same number of unbuffer commands. If the panel receives a hard unbuffer command it changes to unbuffered mode, regardless of the number of soft buffer commands it has received.

Hard Unbuffer/Soft Unbuffer: A hard unbuffer command overrides any number of soft buffer/unbuffer commands. The softeware keeps track of the number of buffer commands received by panels. The panel remains in buffered mode until it receives the same number of unbuffer commands. If the panel receives a hard unbuffer command it changes to unbuffered mode, regardless of the number of soft buffer commands it has received.

Hardware: The physical equipment that makes up an access control system.

Hardware Components: The individual physical components in an access control system. These include the communications loop, panels, locks, readers, sensors, and monitors, printers and workstations.

Hardwired: A system of control panels connected to a communication line (loop or multi-drop) that is connected directly to a computer.

Holidays: Exceptions to the normal way of operating an EAC system.

A holiday on a weekday, for example, can cause normally opened doors to remain locked.

Host Computer: The main computer in an EAC network that is directly connected to a controller or controller network. It holds EAC software and databases, and manages the system.

I

Icon: A picture or graphic that represents a concept.

Infrared Bar Code Cards: A bar code card in which the bar code information is opaque to visible light, but transparent to infrared light. The bar-coded information on the card may be read by the reader, but not copied by a photocopy machine.

Input: A point which receives information. An input device, such as an egress button, sends information to a control panel. Software monitors the state of an input. When that input state changes, such as when a related input device sends information to the panel, software regards that input as being in a state of alarm.

Insertion Card or Token: A card or token that is inserted into a reader, rather than swiped through or passed near a reader.

Integration: The art of controlling electronic devices through activities known as “chains of events”. Especially, in EAC, controlling other systems in a unified way.

Interlock: Refers to creating a chain of events between input and output points.

Invert Follow: In an interlock, a second point (component B) takes on the opposite state as the triggering point (component A). See Follow.

J

Job Specifications: All the written documentation that must be followed in order for a job to be correctly completed.

K

Key Control: In an EAC system, key assignment and control is managed by the controller.

Keypads: A keyboard device, often, but not always, limited to numbered keys between 0 to 9.

L

Latching: The manual use of electronic access control credential in which one credential read causes a lock to unlock and a second read locks the lock. The lock changes state only after a credential is read.

LED: Light Emitting Diode (a small lamp).

Linear Power Supply: A power supply using a series regulator to control voltage by dissipating excess voltage as heat. Provides a very high quality output at the expense of power efficiency.
Local Relay: The communication occurring between an input device and an output on a control panel.
Log In: Signing on to the system. When system operators change shift, the new operator logs in.
Loop: A communications network wherein the communications cable begins and ends at the same point, with control panels linked at increments along the loop.
Low Voltage: A battery is too low. PW-2000-III and IV panels can be configured to report a low voltage alarm. This has a default priority of 1 (very high).

M

Memory: In a control panel, this refers to the amount of information that can be stored in RAM (Random Access Memory).
Message: Information displayed on the Alarm Detail screen in response to the activity (state changes) of an input.
MIP: See Multiple Interlock Protection.
Modem: A device that translates digital signals to analog signals and the reverse, allowing a computer to send information over a standard phone line.
Multi-drop Line: A cabling configuration used for 485 communication networks wherein control panels are connected to a length of cable by t-taps.
Multiple Interlock Protection (MIP): An option requiring that all input points tied to a single output be returned to a normal state to de-energize the point. Without this option, only one input needs to return to the normal state to de-energize the output.
Multi-technology Cards: A single card that uses several information technologies, such as magnetic stripe and bar codes.
Muster Area: A designated area where people go to be acknowledged as being safe during an emergency.

N

NEC: The National Electrical Code.
No Action: In an interlock, a second point (component B) does nothing in response to the state change of the triggering point (component A).
Node: A connection point on a network cable. It indicates that a computer is linked to the network.
Non-Distributed System: A computer or EAC network that requires a single host computer that supplies the programming and decision making resources to other computers and EAC controllers in the system.
Normally Closed (NC): Refers to contact points that always touch when a device is in its normal position.

Normally Open (NO): Refers to contact points that do not touch when a device is in its normal position.
Numb Mode: Disables readers for a set period of time following a card read.

O

Off Line: Disconnecting one computer device from another in a way that stops the flow of information between them.
On Line: Connecting one computerized device with another in a way that can send information between them.
Operating Humidity: The relative humidity range in which a device can operate.
Operating Temperature: The temperature range in which a device can operate.
Operator: A person who operates the system directly through the software; i.e., a user. Operator privileges are determined by operator level or individually.
Operator Level: The privilege a user or operator has to control, view, or edit an aspect of the access system.
Output Control Group: A configuration of output points that are grouped in such a way that all can be activated when the status of a single input point changes. This is commonly used in elevator applications.
Output: This can refer to a location on a controller at which an output device (such as a lock) is connected, or a point on the controller that software controls to produce a transaction.
Override: Reverses a condition. When a locked door is overridden, it is unlocked and the reader shows a valid access.

P

Panel: An access control panel, typically a PW-2000-II or PW-2000-III/IV.
Panel Primary Power Alarm: An alarm reported when a control panel loses primary power.
Panel Reset Alarm: An alarm triggered when a control panel is reset.
Parallel Port: A connector on a computer that is generally attached to a printer.
Parameter: Specific information (often a number) that controls the behavior of the system.
PC: Abbreviation for personal computer.
Piggybacking: Another term for Tailgating.
PIR: A passive infrared sensor that is usually installed above a door to sense motion in an EAC installation. A dual technology PIR combines passive infrared and microwave or passive infrared and ultrasound.
Poll Response Alarm: Refers to an alarm that occurs when panels do not respond when polled by the software. Three polling attempts are made. If

there is no panel response during these attempts, the alarm is reported. This has a default priority of 1 (very high).

Poll: To ask for information. In a computerized system, one computer asks another for information.

Port Expander: A device that allows you to have more than two serial ports on a personal computer.

Port: A means of connecting a communications cable or device to a computer.

Power Drop: The change in the available electrical voltage or current supplied to a device. This is a function of the size and length of the supply wires.

Power Fail Reroute: An option that reroutes the Power Fail alarm from Input 8 to Input 19 on PW-2000-II panels only.

Power Supply: The source of power that changes AC to filtered DC.

Priority: See Alarm Priority.

PROM: Programmable Read-Only Memory. This type of memory is programmed once and can only be read thereafter.

Pulse: A command to energize an output point or shunt an input point for a specific amount of time.

Push Bar: A door-unlatching device. When pushed, it releases a lock. If the push bar is connected electronically to the controller, it signals the controller that an egress event has taken place.

R

RAM: Random access memory used in a computer or control panel. Generally, the operating system and application programs are loaded into RAM. This part of a computer's memory can read (find and display) and write (record) information, and the user can update or add to it.

Reader: Any device that reads encoded information from a card or token and transmits the information to a control panel.

Real Time: Processing events as they happen.

Redundant: Having two or more means of doing things to minimize the effects of failures and errors. Redundant hardware indicates that two or more items exist for every single function. The duplicate hardware can replace failing hardware at a moment's notice.

Re-enable: Return the system to normal operation.

Relay: An electronically operated switch that, when activated by a change in conditions on an electronic circuit, activates other devices on the same or another electronic circuit.

REX: Request-to-Exit device. Refers to a button, pushbar or similar device that allows free egress without setting off an alarm.

RFI: Radio frequency interference In the radio frequency (RF) spectrum, noise introduced by electromagnetic radiation, which causes undesirable effects in nearby electronic components that may be susceptible to disturbance.

S

Secure: To arm or enable.
Serial Port: A connector on a computer that is normally used for communications functions. These functions include attaching a computer to a modem, or a computer to communications loops that are connected to control panels.
Server: The host computer. This is the computer which maintains the system or system functions.
Shunt: The automated or manual means of ignoring an input or an input alarm through software.
Shunt Points: Suppressing the ability of input points to report an alarm. Input points can be shunted individually or by group.
Shunt Time: The length of time a door open alarm is suppressed (shunted) after a valid card access or free egress request. This time should be just enough to allow a card user to open a door or gate, pass through and then close it.
Signal Strength: Indicates the size or quality of an electrical signal. The signal strength decreases as the length of its path in the medium increases. The media type (generally cable) and length are selected so that a signal can travel from the transmitter to the receiver and still be interpreted. If the signal is transmitted via a radio signal, the choice of antenna type and location will affect the signal strength.
Specifications: Rules and measures governing what a device does and how it can be used.
Split Time Zones: An option that allows you to apply different time zones to readers on a single panel.
Stand-alone System: A single, independently working computer or EAC controller that is not networked with other computers.
Standard Mode: A mode where any valid card is granted access.
State: A device's current mode. A change of state means that the mode of a device has changed.
Status: The current state or condition of a system parameter, such as the state of an alarm point.
Supervision: Special electronic protection of a communications line that is accomplished by sending a continuous or coded signal through the circuit. When this feature is enabled, any change of the circuit will be detected and a tamper alarm will result.
Surge Protection: A device that prevents power surges in system or power wiring from affecting or damaging the EAC system or its components.
Supervisor Mode: A mode that enables a supervisor to enter without allowing general access. When this mode is enabled, the reader LED changes color four times per second (usually red then green). When the supervisor presents his card during the time zone just once, he gains access but does not enable general access. If the supervisor presents his card again within 10 seconds, he enables general access and the LED displays a steady red. After the supervisor presents his card twice to allow general access, he can disable the general access for the

time zone by presenting his card again twice consecutively. The LED resumes rapid flashing between red and green. VIP cards do not need a supervisor card to gain access

Switching Power Supply: A power supply system that uses high frequency switching to regulate voltage and current. This type of regulation is more efficient, but may allow some high frequency noise to be present in the power supply output.

System Administrator: A system operator who has full privileges to all applications that are part of the access control system. This person is familiar with hardware components and the software that controls them. He or she is also responsible for assigning passwords and privileges to other system operators.

System Operators (Users): The people who operate the system directly through WIN-PAK PE. Operator privilege is determined by Operator Level.

System Thresholds: The maximum number of components the system is designed to handle.

T

Tailgating: In access control, this is the act of two or more people entering a controlled area by using a single card. (Also known as piggybacking.)

Tamper Alarm: An alarm caused by someone tampering with a system, such as opening the control panel cabinet or removing a reader from a wall.

Tamper Switch: A special switch or contact sensor used to create an alarm when an enclosure or device is opened in an unauthorized manner.

Tampering: The unauthorized act of destroying, modifying, or removing a device.

Terminals: Points on a circuit board where cables from various devices are attached.

Throughput Rate: This can be the rate at which people or vehicles pass through a controlled area, or the rate that information (data) moves through the computer and controller network.

Time and Attendance: The means of recording employee time and attendance through a computer-controlled reader.

Time Zone: A range of times and days of the week that are assigned to clearance codes (access levels). These allow usage of the system within their specifications.

Timing: A procedure that times events so the controller can determine whether or not the event is normal and within limits.

Tracking Area: An area defined by readers. When a person is inside the tracking area, the computer reports that person is being tracked until that person uses a muster reader or a different tracking area reader. This feature does not require anti-passback.

Transaction: An event that occurs as a result of a card read, alarm, or other physical or software action or circumstance occurring at a panel or workstation

in the system. All transactions are recorded in the real-time Transaction History log.
Transmit when Buffer Full: Enables a panel to transmit all activity reports when the buffer nears capacity.
Trigger: An input or condition that initiates a set response to an output or action.
Trouble State: A condition when an alarm circuit is out of specified tolerance, which may indicate tampering or other troubles with the alarm point.
Troubleshooting: The act of figuring out a problem through deductive reasoning.
TTL: Abbreviation for Transistor-Transistor Logic.
Turnstile: A type of rotating gate.

U

Unbuffer: A panel mode in which transactions are not stored in the panel's RAM memory. When a panel is unbuffered, it either transmits stored information to a computer, then continues to transmit ongoing access transactions to that computer, or it ignores access transactions. See Buffer, Hard Unbuffer.
Uninterruptable Power Supply (UPS): A device that continues to provide power even after the main power has been accidentally shut down. It also protects equipment against voltage spikes that can cause damage.
Unshunt: See Shunt.
UPS: See Uninterruptable Power Supply.
Users: The people who operate the system directly through the software; operators.
User Defined Fields: User-customizable fields for the Card Holder Database.

V

W

Wiegand Card: A card that has specially treated wires embedded in it which, when it passes through a Wiegand reader, emits a discrete electrical signal.

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