GE
Security

Picture Perfect 4.5
User Manual

P/N 460202008C • ISS 25MAR10

Document number/revision: 460202008C (March 2010).

Contents

Preface

References to Picture Perfect 4.5 for AIX are subject to availability -- currently planned for late 2010.

This document provides instructions for initial setup and configuration of the Picture Perfect system and for configuration changes to an existing system. It also contains information for operating the system once it is installed.

This document is intended for system administrators who are responsible for the planning and implementation of the system design, and who perform system configuration and setup using Picture Perfect™ forms that are accessible only to the master-level operator.

Operators using the system should read the chapters which relate to their duties.

The material in this document has been prepared for persons responsible for, and familiar with the security needs of the customer facility.

Read these instructions and all ancillary documentation entirely before installing or operating this product. Refer to *Related documentation* on page xvi.

A qualified service person, complying with all applicable codes, should perform all required hardware installation.

Conventions used in this document

The following conventions are used in this document:

Bold	Menu items and buttons.
Italic	Emphasis of an instruction or point; special terms.
	File names, path names, windows, panes, tabs, fields, variables, and other GUI elements.
	Titles of books and various documents.
Blue italic	(Electronic version) Hyperlinks to cross-references, related topics, and URL addresses.
`Monospace`	Text that displays on the computer screen.
	Programming or coding sequences.

Safety terms and symbols

These terms may appear in this manual:

CAUTION:	*Cautions* identify conditions or practices that may result in damage to the equipment or other property.

WARNING:	*Warnings* identify conditions or practices that could result in equipment damage or serious personal injury.

Related documentation

- Picture Perfect 4.5 Release Notes (460621001F)
- Picture Perfect 4.5 Installation Manual (460620002C)
- Picture Perfect 4.5 External Interface User Manual (460588003B)
- Picture Perfect 4.5 Interface User Manual (460581004B)
- Picture Perfect 4.5 Tables and Fields 460566003B)
- Picture Perfect 4.5 Enterprise Edition User Manual (460234008B)
- Picture Perfect 4.5 Import/Export User Manual (460219007C)
- Picture Perfect 4.5 Guard Tours User Manual (460203007B)
- Picture Perfect 4.5 Redundant Edition User Manual (460134009C)
- Picture Perfect 4.5 Imaging Installation Manual (460119107B)
- UBF Universal Badge Format for Picture Perfect (460625001A)
- Graphics Monitoring and Control User Manual (460624001B)
- Credential Designer User Manual (460557006B)
- CARMA: Card Access Report Management Application for Picture Perfect (460516002C)

Chapter 1 Introduction

This chapter describes Picture Perfect and its features. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

The Picture Perfect system is a powerful, flexible, integrated, computer-based physical access management system. It is a complete end-to-end solution for today's most commonly deployed physical security applications, providing real-time monitoring, command and control, automation, database administration and report management in a single, unified system. Picture Perfect integrates access control, photo identification and credentialing, video surveillance, alarm monitoring, intrusion detection and visitor management. Picture Perfect uses industry leading products such as the Linux and AIX operating systems, Informix Dynamic Server, and a Java RunTime Environment (JRE).

The Picture Perfect platform functions, in large measure, as a database server. The majority of access, alarm, and time-of-day decisions are made locally by intelligent micro controllers. Data necessary to make these intelligent decisions is downloaded from the host to the micro controller, or micro as they will be referred to in this document, as required. Since the majority of the decisions are performed at the micro, the host is free to concentrate on operator functions such as data entry, database queries (requests for data), and report generation.

The system controls access readers using various technologies including, magnetic-stripe, barium ferrite, Wiegand, bar code, and proximity technologies. Smart Card readers and readers with keypads for user-defined PIN entry are also accommodated.

The smallest system will monitor thousands of badge records, transaction history records, digital inputs (alarm contacts), and digital outputs. Capacity limits depend on system resources. The system supports multiple operator work stations and printers, and the Picture Perfect configuration that is deployed.

Scheduling features allow time allocations for use of readers and alarms. Micros, such as the M5, have the capability to perform the majority of scheduling tasks. This provides the user with full scheduling capabilities, even when a communication problem has caused the micro and host to temporarily stop talking to each other.

The user interface is menu driven and user-friendly. The menus provide the operator with various options which lead to input screens, providing the ability to add, change, or delete information. By assigning operator levels to individuals, operators can be restricted in their control of the system. They can be denied the authority to change previously set parameters, and may be able to view information on a screen, but may not be permitted to modify or print out the information.

All conditions sensed by the system can be assigned unique messages, which can be displayed on the computer screen and made available to the operator. A sensor on a door can be coded within the system, not only to activate an alarm if the door is opened, but to notify the operator of where the breach occurred and what action to take. Alarms can be given priorities for action in the event that multiple alarms occur. All alarms are provided with an audio display tone and a flashing alert to warn security personnel of severe conditions.

The system maintains a history of all occurrences reported by its micros, such as access attempts or alarms. Management reports are available to provide the system administrator with the activities within the system any time, on demand.

The program is personalized by the customer to their specific requirements and configuration by simple windows and menus. An operator can change the size and position of a screen, the forms can be customized to include specific fields, and custom lists can be added.

The system uses a relational database management system (RDBMS) which allows the operator to query the database using menu driven forms. These forms allow the operator to specify data fields requested, logical relationships between the fields, and the order in which the fields are to be selected. Once the request for data is made, the matching records are displayed in a grid; the operator selects a record from the grid to display the form. If desired, the operator can print the requested data by selecting the appropriate option.

The system architecture uses a distributed approach, comprised of micros and the host processor.

- On an AIX system, all terminals are graphics terminals except the host console which could be a character-based terminal.
- On a Linux system, all terminals (including the host console) are graphics terminals.

New in Picture Perfect 4.5

Picture Perfect 4.5 introduces the following key capabilities, features, and/or product enhancements:

OS and database technology refresh

- Red Hat Linux 5.3
- AIX 6.1
- Informix 11.5

Picture Perfect 4.5 new features

- Removed the need for “root” access
- Nested Zone Anti-passback – Global and Timed
- Mifare Smart Card Encoding capability
- New fields for Dept and Category on Badge Monitor
- Enhanced LDAP for unique schemas
- Permission Form Preferences button
- New History Rollover Alarm
- Configurable alarm for disk and database full
- Enable case-insensitive data queries from GUI
- Alarm Blinking – user configurable options
- Informix Replication for Picture Perfect Redundant systems (new method of synchronization)
- Picture Perfect and Facility Commander 2.2 single server/database install
- Client support on Microsoft Vista
- Support for Firefox web browser
- Improved robustness and reduced vulnerabilities
- New Lockdown mode
- New database user accounts (important for import/export integrations)
- Additionally supported fields for Badge Activity Monitor

Operating features

- **UNIX-like Operating System** (AIX or Linux) provides multitasking, multi-user capabilities. Multiple tasks can be performed by multiple users simultaneously. An operator can view several windows at once.
- **Host System** architecture is powerful enough to support the operating system and relational database management systems.
- **Graphical Menu-Driven Operator Interface** almost completely frees you from the keyboard. Primary and secondary menus lead to input forms (screens) where you can add, change, or delete information. These forms can be customized to include only those fields necessary for your specific site.
- **Pop-Up Window Alarm Messages** appear on whatever form (screen) is currently displayed. You can continue with the current form or exit to an alarm response form.
- **Online Help** can be accessed by clicking the Help button to display a pop-up help window for any form or field. Help constitutes an online reference manual that explains every form and field in each form.
- **Powerful Query Function.** Picture Perfect uses Informix Dynamic Server, a relational database management system (RDBMS) with a query function that reduces the need for printed reports. The RDBMS frees you from canned search criteria. Use the Find function to query and display data. As an alternative to printing a report, you can display the report on screen and scroll back and forth through data. The RDBMS allows you to define direct relationships between separate database tables so that a single report joins multiple tables. The report function also lets you customize reports with Structured Query Language (SQL) so you can pinpoint just the data you need.
- **Real-Time Monitoring.** Badge activity displays in real time on a scrolling window with image thumbnails, where you can scroll backward and forward through the transaction data or perform a transaction search.
- **Database Protection.** The system database is protected from unauthorized use by the Operator Permissions feature which controls (using a login ID and password) each operator's authorization to display or update forms and to print reports.
- **User-Defined Schedules.** The system provides an interface for user-defined schedules. For example, an area can be scheduled for general employee access during business hours, but restricted to selected employees after hours. All schedules can be manually overridden from the operator's console. If the host and micros stop communicating, the micros continue processing all resident schedule changes.
- **Operator Input Validation.** All system forms (screens) and menus provide extensive data-entry error checking. The system will reject a form if fields do not contain acceptable data; therefore, bad data cannot corrupt the database. Field labels of required entries display in red.
- **Operator Activity Monitoring.** The activity of all system operators can be viewed and is saved to operator history.
- **User-Defined Alarms.** Alarms may be assigned priorities to control processing in the event of simultaneous alarms. Multiple-action messages may be configured to notify the operator when and where the alarm is occurring and what actions to take.
- **Digital Outputs to Operate Output Devices.** Inputs (digital or logical) trigger digital outputs which can operate output devices (door locks, lights, bells, sirens).
- **Transaction History Processing.** The standard system stores history records online, including badge, alarm, operator, and system performance activity transactions which can be archived to disk file, or

tape. Depending on the size of your hard drive, the system can be configured to store more history records online.

- **User-Defined Reports.** The reports feature provides an SQL (Structured Query Language) interface to the online Picture Perfect database so that you can use ANSI standard SQL select statements to query the database and generate reports. (Pre-loaded SQL reports satisfy standard administration requirements.) The query function allows unlimited selection criteria and up to eight sort criteria, including the use of user-defined variables as input to the query. The relational database allows an SQL statement to join multiple database tables in one report, sorting the result by any selected field.
- **DirecDoor, PXNPlus, M5, M3000, and M2000 series microcontroller support for Readers, Alarms, Scheduler.** During normal operation these micros use their resident databases to make local access-control decisions. In the event of communication failure with the host, these micros control and store reader and alarm activity and also implement scheduler events.
- **Global Anti-passback Supported.** Any reader on any M5, M2000, DirecDoor, or M3000 series microcontroller (except a dial-up micro) can be configured as an anti-passback reader.
- **Keypad Reader Support for PIN Entry.** Keypad reader support is provided to enhance security.
- **Time Zone Support**. The Time Zone feature associates a time zone with items in your database that have a physical location, such as micros, operators, or hosts. Monitors display dates and times in the three time zones: Host, Micro, and Operator and can be configured to display only the one you specify. Date and time entry fields on event forms and on the Category scheduler specify a context of either Host, Micro, or Operator which allows you to schedule events or categories in any of those contexts.
- **Templates**. You can create master templates for generating new records with the necessary links predefined. When a template is run, a Wizard guides you through the necessary steps to create a new record for the form.

Optional features

- **Graphics Monitoring and Control.** The Graphics Monitoring and Control option allows you to use site maps of your premises and associate symbols (graphic images or icons) to object types such as doors, readers, micro controllers, or digital inputs. When the condition of a device property changes, on or more of the symbols changes it's appearance based on the condition, if configured to do so.
- **Import/Export.** The Import/Export option enables the transfer of Picture Perfect database information to and from external databases (such as a personnel database). It allows other applications to interface with the Picture Perfect database. You can also use odbc and jdbc database connectivity to connect to the Picture Perfect database and make changes.
- **Redundant.** The Redundant system option allows two host systems (primary and backup) to operate in a fault-tolerant configuration.
- **Imaging.** The Imaging option allows a picture of the badge holder to be captured, imported, exported, displayed on screen, and printed. Swipe and Show can be configured, where a valid badge swipe results in the display of an associated photo on a monitor with authorization to unlock the door. Thumbnail images are displayed on the Badge Activity Monitor.
- **Enterprise.** The Enterprise option allows several hosts to operate together in a network environment.
- **Guard Tours.** The Guard Tours option allows you to monitor the progress of a security officer as he or she tours the facility premises at specified intervals, and to obtain hardcopy reports that show a tour history.

Support services

GE Security and its business partners offer a full range of customer support services, including site surveys, installation supervision, systems acceptance, and training, with total turnkey installation capabilities. These services are options at the discretion of the customer.

Enterprise consulting

Enterprise Consulting is an engineering services team within GE Security that offers custom solutions to GE integrators and end users in areas where the standard products do not meet specific requirements. Examples include custom software development including interfacing to third party systems, backup and recovery solution consultation and implementation, database merge, and migration from one technology platform to another. Enterprise Consulting takes the worry out of custom software development by handling the full project management delivery cycle from requirements gathering to project completion including delivery of documentation.

Training

Training is extensive and all-inclusive. It provides for the needs of customer personnel at all levels—management, technical, and system operations. Classes are conducted by expert training personnel and provide extensive hands-on experience.

National language support

Language translations of Picture Perfect and the online help are installed as part of the standard product installation. New languages will be provided as they become available through standard product maintenance releases.

If you require support in languages other than those provided by GE, please contact your System Integrator.

Chapter 2 Getting started

This chapter describes how to log on to and out of the Picture Perfect system and how to navigate the interface and common elements. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

Once your installation is complete, perform the steps below to begin using your system. Each of these steps is discussed in detail in the following sections.

1. Start Picture Perfect.
2. Log on.
3. Select one or more facilities.
4. Familiarize yourself with the user interface and the navigation tools.

Starting and stopping Picture Perfect

Power on your system to start Picture Perfect. On the desktop open a browser that has a Java plug-in, for example, Internet Explorer or Netscape.

During normal operations the application automatically starts, when the Picture Perfect server is powered on. There may be occasions when the system administrator shuts down Picture Perfect, and other occasions that the entire system and Picture Perfect (TPS and Informix) is shut down. For more information, see *Related procedures*.

Related procedures

The following procedures are performed from the command line in a terminal window on the server console:

- Stopping Picture Perfect
- Shutting down the entire system
- Restarting Picture Perfect

To stop Picture Perfect:

Use the following command sequence to shut down the Picture Perfect application.

1. Log on as `ppadmin` at the console terminal.
2. Make sure no one is logged on as an operator.
   To verify if anyone is logged on, from a new window, type:

   ```
   smutl -o -1
   ```

   A detailed list of all operator sessions currently logged on displays.
3. Type: `rc.pperf -k`

   —or —

   On a redundant system, type: `pprscmd stop`

To restart Picture Perfect:

Use the following command sequence to restart the Picture Perfect application. The third step is a command to stop Picture Perfect and is used to verify that Picture Perfect is not already running.

1. Log on as `ppadmin` at the console terminal.

2. Make sure that no one is logged on as an operator.
3. Stop Picture Perfect:
   - For standalone or host/subhost systems, type: `rc.pperf -k`
   - For redundant systems, type: `pprscmd stop`
4. Wait a minimum of 30 seconds for all processes to stop.
5. Start Picture Perfect:
   - For standalone or host/subhost systems, type: `rc.pperf`
   - For redundant systems, type:
     - `pprscmd start primary`

     —or—

     - `pprscmd start backup`

To shut down the entire system:

Software or hardware maintenance on the Picture Perfect system may require a complete system shutdown. If this is necessary, perform the following command sequence.

1. Log on as `root` at the console terminal.
2. Make sure no one is logged on as an operator.
   To verify if anyone is logged on, from a new window, type:

   ```
   smutl -o -1
   ```
3. Perform the shutdown:
   - For AIX systems, type: `shutdown -Fh now`
   - For Linux systems, type: `shutdown -h now`

   Note: Type `shutdown -h` to halt the system; type `shutdown -r` to reboot the system. The shutdown command also stops Picture Perfect before shutting down the system.
4. Wait until the `**halt completed**` (AIX) or `Power Down` (Linux) message appears, and then turn the power off on the computer.

Logging on to the system

In order to use Picture Perfect, you must log on as an authorized Picture Perfect operator, using a valid Login ID and Password. The first time you log on to the system, you will use the Login ID and password that were configured during installation.

To log on to Picture Perfect:

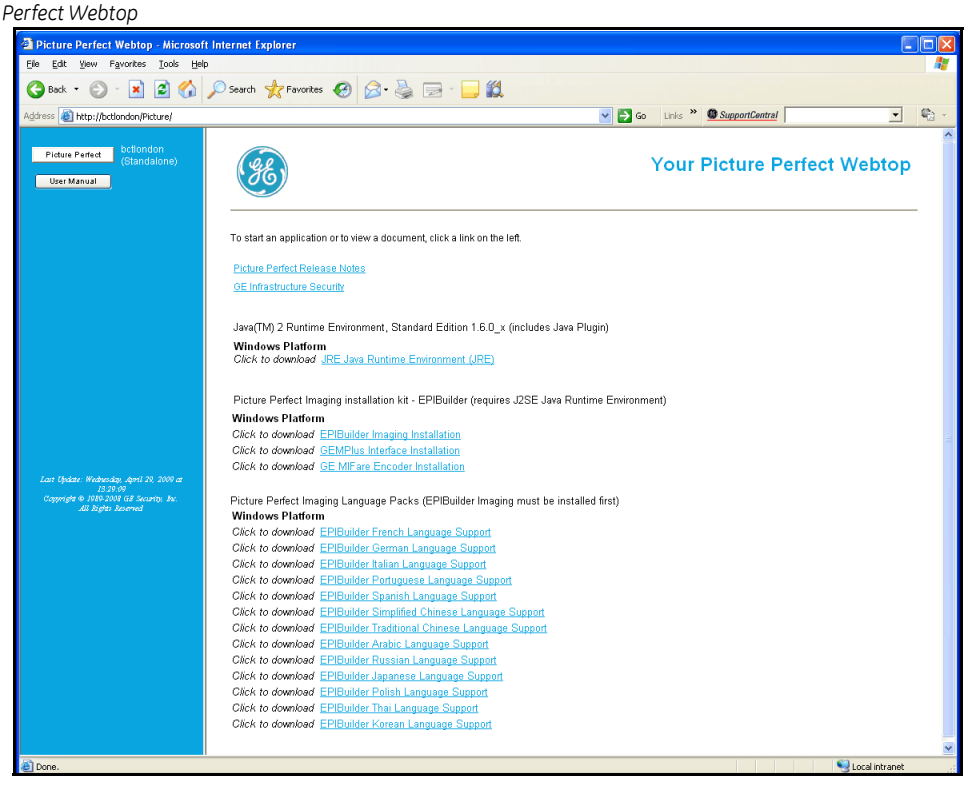
1. In a browser window, type a URL in the address field to connect to the server, for example:

   `http://<hostname>/Picture`

   Note: If you are logging on to an Imaging workstation, you must close all existing browser windows and open a new window.

   The Picture Perfect Webtop displays from which you may launch Picture Perfect.

Figure 1. Picture Perfect Webtop



2. Click the Picture Perfect button in the upper left hand corner. The button color will display white if the server is active, red if it is inactive, and yellow if it is the backup server.

   The system prompts you to acknowledge the signed Java certificate after which the Picture Perfect Operator Login window appears.

Figure 2. Login window

3. Type your Login ID and Password. They tell the system who you are and which functions you are authorized to perform. Both of these fields are case sensitive, so enter the information carefully. For more information about the Login window fields, refer to *Table 1*.
4. Click **Log on**.

   The Picture Perfect desktop appears.

   Note: When logging on to Picture Perfect, with SSL enabled, the following message displays.

Figure 3. SSL Security warning:

Note: Click Yes. This window appears because Picture Perfect self-signs the SSL certificates and does not obtain them from a third party. If you wait too long to click Yes, the application will time out and you will be denied access. If the timeout occurs, close Picture Perfect and try again.

Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 1. Login window fields

Field Name	Description
Login ID	This identifies you as an authorized Picture Perfect operator. It typically incorporates your name and consists of an alphanumeric string of up to eight characters.
Password	Your password keeps unauthorized personnel from logging on to the system and should remain confidential. It typically consists of six to eight characters and, for security reasons, does not display on the screen as you type it.

Related procedures

The following procedures are sometimes required in day-to-day operations and administration:

- Logging off.
- Logging on as the “root” user.
- Logging on as the “install” user.

To log off of Picture Perfect:

It is important to log off of the system when you leave your workstation. This protects the system from unauthorized use, and also allows the next operator to log on.

1. Save any new or changed data.
2. Close open forms by clicking **Close** on the application window title bar.
3. From the **File** menu, select **Log off.**

To log on as the “root” user:

For some of the procedures, you will be instructed to log on as `root`. Logging on is the process of “signing on” to the system as a user. The `root` user (also known as the superuser) is a special user that has access to every program and file on the system. You will be doing the installation and configuration of the operating system as the `root` user. You will install Picture Perfect as the `root` user, as well.

1. At the prompt for user name in the console terminal, type: `root`
2. At the prompt for password, type the `root` password, as configured during installation.

   Note: If you received your system preconfigured by GE, the default root password is pperf1, however it is strongly recommended that you change it, once the initial installation is complete, using the passwd command.

3. Open a terminal window.
4. If Picture Perfect is installed, at the command prompt, type:
   `. /cas/sbin/profile` Enter

To log on as the “ppadmin” user:

For some of the procedures, you will be instructed to log on as `ppadmin`. The `ppadmin` user is a special user that has access to every program and file on the Picture Perfect system. The `ppadmin` user performs such

tasks as starting and stopping the Picture Perfect application, monitoring the system from the command line, and running all tools available in Picture Perfect.

1. At the prompt for user name in the console terminal, type: `ppadmin`
2. At the prompt for password, type the `ppadmin` password, as configured during installation.

   Note: If you received your system preconfigured by GE, the default ppadmin password is ppadmin, however it is strongly recommended that you change it, once the initial installation is complete, using the passwd command.

3. Open a terminal window.
4. If Picture Perfect is installed, at the command prompt, type:

   `. /cas/bin/profile` Enter

To log on as install:

Another user called `install` will automatically be set up when you install Picture Perfect. The `install` user account (that is, log on as `install`) is used to configure Picture Perfect for your site. This user performs such tasks as creating operators, configuring micros, and administrating personnel data.

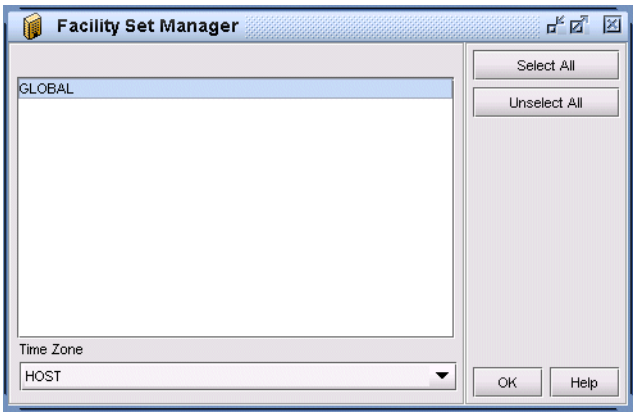
1. At the prompt for user name in the client workstation login window, type: `install` Enter
2. At the prompt for password, type the `install` operator's password.

   After the system loads, the Primary Navigation menu displays the Picture Perfect menu items you are authorized to use.

Selecting one or more facilities

Picture Perfect allows you to create and delete facility records. These records, combined with Facility Profiles and Permissions, allow you to restrict operator access to records assigned to those facilities. Selecting a facility allows the user to view records within that facility that they have permission to view. Following a successful login, the Facility Set Manager window displays a list of those facilities included in your facility profile. If you have access to only one facility, it is automatically enabled.

Figure 4. Facility Set Manager



Fields and controls

Table 2. Facility Set Manager form

Fields	Description
Select All	Click to select all of the available facility sets.
Unselect All	Click to de-select all of the available facility sets.
Time Zone	By default, when you log on to Picture Perfect, the Time Zone selected is that assigned to your Operator record. *Example: If you are traveling and log on to a Picture Perfect session in a different time zone, you can select the appropriate time zone from this list.* See *Verifying time zones* on page 168.

Related procedures

To select a facility:

1. Click on a facility to select or de-select it or click **Select All** or **Unselect All** to select or de-select all of the available facility sets.
2. Click **OK**.
3. By default, when you log on to Picture Perfect, the Time Zone selected is that assigned to your Operator record. If, for example, you are traveling and log on to a Picture Perfect session in a different time zone, you can select the appropriate time zone from this pick-list.
4. To change the active facility set during a session, display the Facility Set window by one of the following methods. The change will not affect forms that are already open.
   - From the **File** menu, select **Facility Set**.

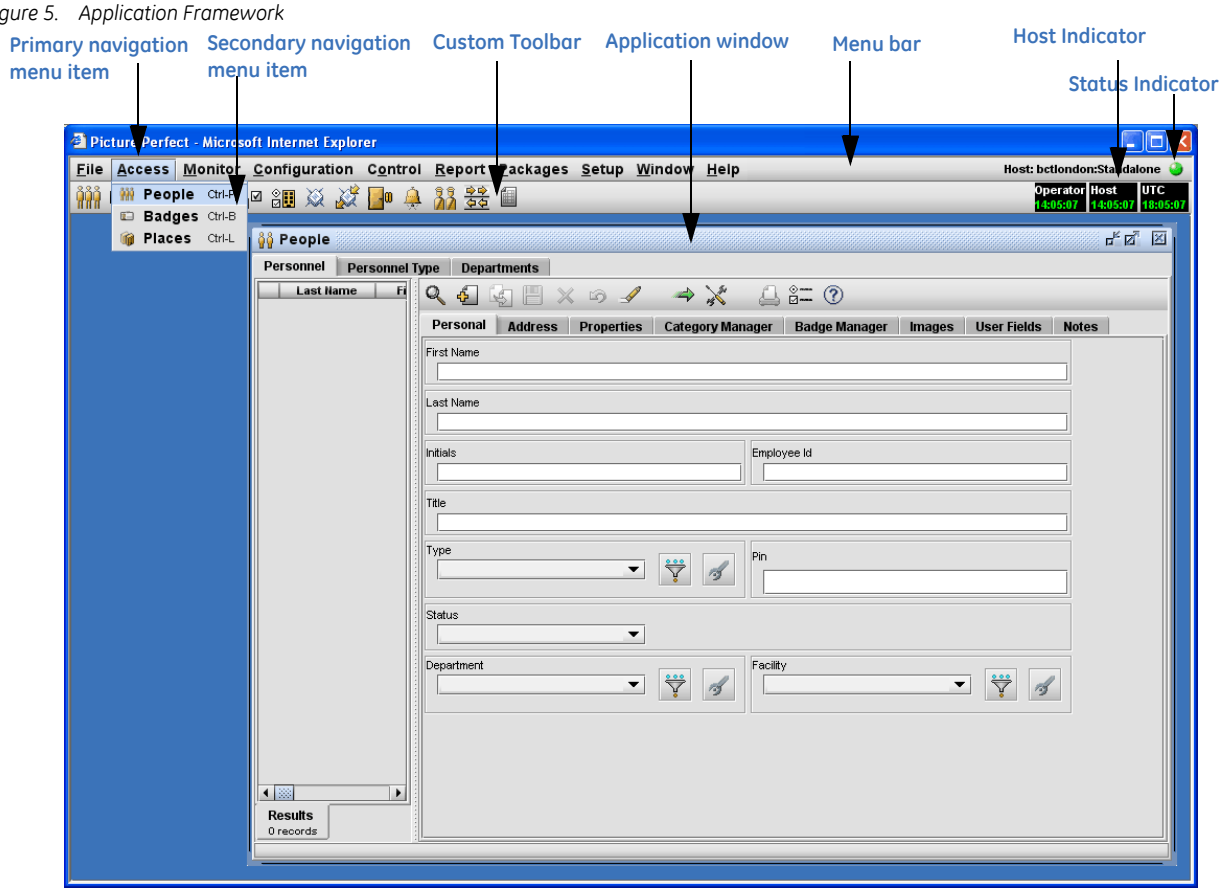
- Right click on the desktop and select **Facility Set** from the resulting window.
- Press **CTRL + F** to display the Facility Set window

Navigating Picture Perfect

The majority of Picture Perfect applications, specifically those that manipulate data contained in the Picture Perfect database tables, are based on a common framework. A typical Picture Perfect application window is shown in *Figure 5*.

The elements that make up the framework are described in more detail in the sections that follow.

Figure 5. Application Framework



The menu bar

When Picture Perfect is initially launched in your browser window, the desktop is comprised of a primary navigation menu bar, and a toolbar. Each primary navigation menu item consists of secondary navigation items, each of which is an application or a function. Only those applications to which an operator has permission, and only those actions that an operator has permission to perform are available. Depending on those permissions, the following primary navigation items are available: File, Access, Monitor, Configuration, Control, Setup, Reports, Window, and Help, and optional packages such as Tours.

See *Table 3* through *Table 12* to view the secondary navigation items and a description of their functions.

Table 3. File Menu

Sub-Menu	Function
Facility Set...	Provides a list of facilities available for selection, based on the operator's facility profiles.
Customize Toolbar...	Displays a list of applications from which you can select/deselect those that you want to display on your toolbar.
Debug Levels...	Displays a list of packages. Debug levels can be set for each package to be used for troubleshooting. The log file, avatar.log, is written to c:\avatar\logs.
Log off	Closes all windows and displays the Login screen.

Table 4. Access Menu

Sub-Menu	Form	Function
People	Personnel	Application used to create and edit Personnel records that identify each badge holder.
	Personnel Type	Application used to create and edit Personnel Type records: to define different types of personnel that are assigned to each badge holder.
	Department	Application used to create and edit Department records: to assign to each badge holder.
Badges	Badges	Application used to create and edit: Badge records: to control the functions and capabilities of the badge
	Badge Format	Application used to create and edit Badge Format records: to add custom formats in addition to the predefined 10-digit badge format.
Places	Area	Application used to create and edit Area records: to describe areas of your site requiring the same level of access control.
	Category	Application used to create and edit Category records to identify groups of badge holders by type, title, function, or shift.
	Area Events	Application used to create and edit Area Events records: to define and schedule the desired characteristics for all the readers, doors, and routings in an area during an event.

Table 5. Monitors Menu

Sub-Menu	Function
Alarm	A monitor used to view, respond to, and remove alarms.
Badge	A monitor used to control and view real-time badge activity.

Table 5. Monitors Menu (continued)

Sub-Menu	Function
Input	A monitor used to control and view the states of input devices, such as door sensors or exit requests.
Operator	A monitor used to view operator history transaction activity.
Status	A monitor used to view the current operating characteristics (status) for a micro controller's areas, categories, readers, doors, inputs, input groups, outputs, output groups, alarms, modes, elevators, category floors, and/or version. You can also view the status of an area's readers and/or doors.
User	A monitor used to view who is logged on and using the system.
Performance	A monitor used to view server system performance.
Log	A real time monitor that lists the contents of the Picture Perfect log file, `/cas/log/log.xxxx` where `xxxx` is the current month and day. *Example: `/cas/log/log.1105` for the log file for November 5th*
Tour	If you have the optional Guard Tours package, this monitor will display tour activity.

Table 6. Configuration Menu

Sub-Menu		Function
Facilities	An application used to create and edit Facility records that group your database records into meaningful units.	
Micros	Micros	An application used to create and edit Micro records to identify each micro controller and define how it operates and communicates.
	Ports	An application used to create and edit Port records to define serial ports for micro controller communications.
	Modems	An application used to create and edit Modem records: to define the types of modems that you intend to use for dial-up communication.
	Network Ports	An application used to create and edit Network Port records to define ports for network micro controller communication.
	Keys	An application used to secure transmission between the host and the network micro by means of a key to create an encryption pattern.
Inputs Outputs	Input Groups	An application used to create and edit Input Group records to trigger output groups when any individual inputs in the input group are detected.
	Inputs	An application used to create and edit Input records: to define the characteristics and the purpose of each input point.
	Output Groups	An application used to create and edit Output Group records to which individual outputs can be assigned. When an input group triggers an output group, all outputs assigned to the group activate.
	Outputs	An application used to create and edit Output records to define the characteristics and the purpose of each output point.
	Input Group Events	An application used to create and edit Input Group Event records to enable or disable a specific input group and/or to change its state to off according to a schedule.
	Output Group Events	An application used to create and edit Output Group Event records to enable or disable a specific output group and/or to change its state to off according to a schedule.

Table 6. Configuration Menu (continued)

Sub-Menu	Function	
Doors and Readers	Doors	An application used to create and edit records: that define how each door operates.
	Readers	An application used to create and edit records that define the readers to which the doors are connected.
	Reader Events	An application used to create and edit records that define and schedule the desired characteristics of a single reader during an event.
	Door Events	An application used to create and edit records that define and schedule the desired characteristics of a single door during an event.
Elevators	Elevator	An application used to create and edit records to control access to floors serviced by an elevator.
	Category Floors	An application used to create and edit records: to assign a category to certain floors of each elevator, which is then used to establish a match between a badge and a floor when granting access.
Alarms	Alarm	An application used to create and edit records: to define both physical and logical alarms.
	Alarm Colors	An application used to create and edit records to define the colors used in the Alarm Monitor so that the color scheme reflects the alarm state.
	Alarm Events	An application used to create and edit records to define and schedule the desired characteristics of a single alarm during an event.
	Alarm Messages	An application used to create and edit records to define alarm instructions displayed on the Alarm or Activity Monitor.
	Alarm Responses	An application used to create and edit records to define alarm responses the operator can select when responding to an alarm.
Time Zone	An application used to assign a unique time zone to each host, device, and operator in the system. See *Verifying time zones* on page 168.	
Data Generator	An application used to add new readers, doors, and areas with all the necessary associated records automatically created and properly linked. See *Running templates* on page 320.	

Table 7. Control Menu

Sub-Menu	Function	
Operators	Operator	An application used to create and edit Operator records to define those individuals who will log on to the Picture Perfect system.
	Permission Group	An application used to create and edit Permission Group records: to limit operator permission to specific categories, areas, and/or reports.
	Permission	An application used to create and edit Permission records that combine system, form, and facility permission profiles. This permission is then assigned to an operator.
	System Permission Profile	An application used to create and edit System Permission records that define the functions each operator level is permitted to perform. The functions included on this form are system related and are not filtered by facility.
	Facility Permission Profile	An application used to create and edit Facility Permission Profile records that describe an operator's level of access to the various forms and fields. The functions included on this form are filtered by facility.
	Form Profiles	An application used to associate custom forms with an operator's permission.
Modes	Change Mode	A function that allows you to change your system operating mode when a different operating strategy, such as an emergency, requires an immediate change.
	Modes	An application used to create and edit Mode records: to define operating modes (in addition to the system defined Normal Mode), that are activated either by schedule or by command.
	Modes Email	An application used to create an email notification for a mode event.
	Mode Events	An application used to create and edit mode events.
	Emergency	An application used to create and edit emergency mode records: to assign the mode, input group, and facility that will define the emergency mode.
Routings	Routings	An application used to create and edit Routing records to define where certain types of messages are sent, in addition to the predefined routings.
	Route definition	An application used to create and edit Route definition records: to define where alarm and activity messages are routed.
	Route points	An application used to create and edit Route point records to specify when and to which operators, alarm and activity messages are routed.
	Email Recipients	An application used to create and edit E-mail records: to allow alarms to be routed to e-mail addresses.

Table 7. Control Menu (continued)

Sub-Menu	Function	
Backup/Restore	Backup Events	An application used to create and edit backup event records that schedule a system backup to run automatically at a specified day and time.
	Backup	An application used to generate a backup of your system to one of the following media: tape, or diskfile.
	Archive	An application used to archive your history data to one of the following media: tape, or diskfile.
	Restore	An application used to restore data from one of the following media: tape, or diskfile.
Access Secure	Doors/Inputs/Input Groups	An application used, in lieu of scheduling an event, to accommodate situations that require operator control. It allows state changes for multiple devices rather than applying the change to each device individually through the applicable form.
Hosts	Hosts	An application used to configure hosts in an Enterprise Picture Perfect system.
Control Outputs	Control Outputs	An application used to allow an authorized operator to turn outputs on or off for the duration of time entered on the Output form.

Table 8. Setup Menu

Sub-Menu	Function	
System Parameters	An application used to assign system parameters used by the system during the setup procedures.	
Printers	An application used to create and edit Printer records to define the printers configured during installation.	
Workstations	An application used to create and edit workstation records to define client terminals that will be used as imaging stations.	
Badge Designs	Badge Designs	An application used to create and edit Badge design records to be used for printing.
	Design Mappings	An application used to create and edit design map records used for linking a person to one or more badge designs.
Custom Lists	An application used to create and edit custom lists to appear on your forms to satisfy specific requirements. *Example: You can create a drop-down list of hair or eye color.*	
Custom Form	An application used to create and edit Picture Perfect forms that include the fields and tabs of your choice, in addition to required fields. *Example: If your facility does not use expiration dates/times on badges, you could exclude those fields. A custom form may be set as the default.*	

Table 9. Reports Menu

Sub-Menu	Function
Reports	An application used to control which activities are stored in history and how to view, format, print, and save reports.
Report Events	An application used to create and edit report event records that schedule history or SQL reports to run at specific times.

Table 10. Window Menu

Sub-Menu	Function
Minimize All	Reduces all windows to an icon.
Restore All	Opens all minimized windows.
Cascade	Arranges windows in an overlapped fashion.
Tile Horizontally	Arranges windows in non-overlapped tiles, one on top of the other.
Tile Vertically	Arranges windows in non-overlapped tiles, side by side.
Open windows	Displays a list of open windows. The window that is currently active displays a check mark next to it. By clicking on a window in this list, it becomes the active window.

Table 11. Help Menu

Sub-Menu	Function
Help Topics	Displays an index of topics on which you can get help.
About Picture Perfect	Displays the Picture Perfect version and patch levels of any packages installed. It also displays license information, memory usage, and allows you to run the "Garbage Collector" utility, which attempts to free up unused memory.

Table 12. Optional Package Menu

Sub-Menu	Function
Tours	When the optional Guard Tours package is installed, this application is used to define the characteristics of a tour, the exception codes, points definition, and tour functions.

Table 13. Status Indicator

Status	Function
Red	A red LED indicates that communication with the server has been lost.
Green	A green LED indicates that the client is communicating with the host.

The toolbar

When Picture Perfect is initially launched in your browser window, the desktop is comprised of a menu bar, and a toolbar. The toolbar is user configurable and can be used to display your most frequently used applications.

Note: Prior to configuration, the toolbar will appear empty.

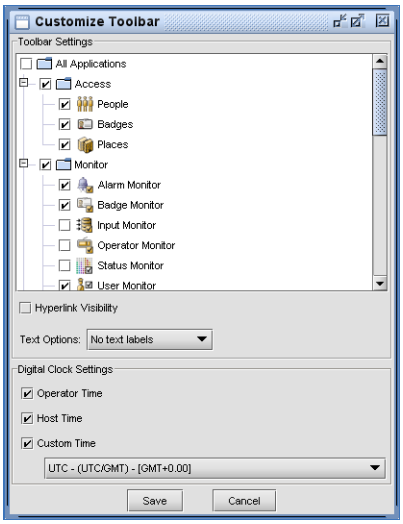
Figure 6. Custom Toolbar

To add an application icon to the toolbar:

1. From the **File** menu, click **Customize Toolbar**.

   The Customize Toolbar window displays a list of applications and a list of text options.

Figure 7. Customize Toolbar



2. From the list of applications, expand the directories and select/deselect those applications that you want to display on your toolbar. Selecting the main branch selects all of the sub-branches.
3. From the Toolbar Settings pane, check the Hyperlink Visibility check box to view the selected application as a hyperlink on the toolbar.
4. From the list of text options, select from the following:
   - Show text labels
     The text label displays below the icon.
   - Selective text on right
     The text label displays to the right of the icon.
   - No text labels
     Only the icon displays. The icons include tooltips.
5. From the Digital Clock Settings pane, select the time (Operator, Host, or Custom) that you want the toolbar clock to display. Custom time allows you to select from a drop-down list of time zones.

6. Click **Save** to save your toolbar preferences to the database. The current settings are retained for your next login session. Click **Cancel** to retain the settings for the current session only.

   Note: If a large number of applications are selected, they could exceed the viewable area of the monitor.

The application window

The majority of Picture Perfect applications, specifically those that manipulate data contained in the Picture Perfect database tables, are based on a common framework. A typical Picture Perfect application window is made up of a title bar, a toolbar, a grid on the left, and the form on the right, similar to *Figure 8*.

See *Table 14* through *Table 20* to view detailed information on these components.

The size of the data grid and the form window can be adjusted by dragging the splitter pane left or right, or resizing the Application window. When you close the Application window, the window size and splitter location settings last used will be retained.

Figure 8. Application Window

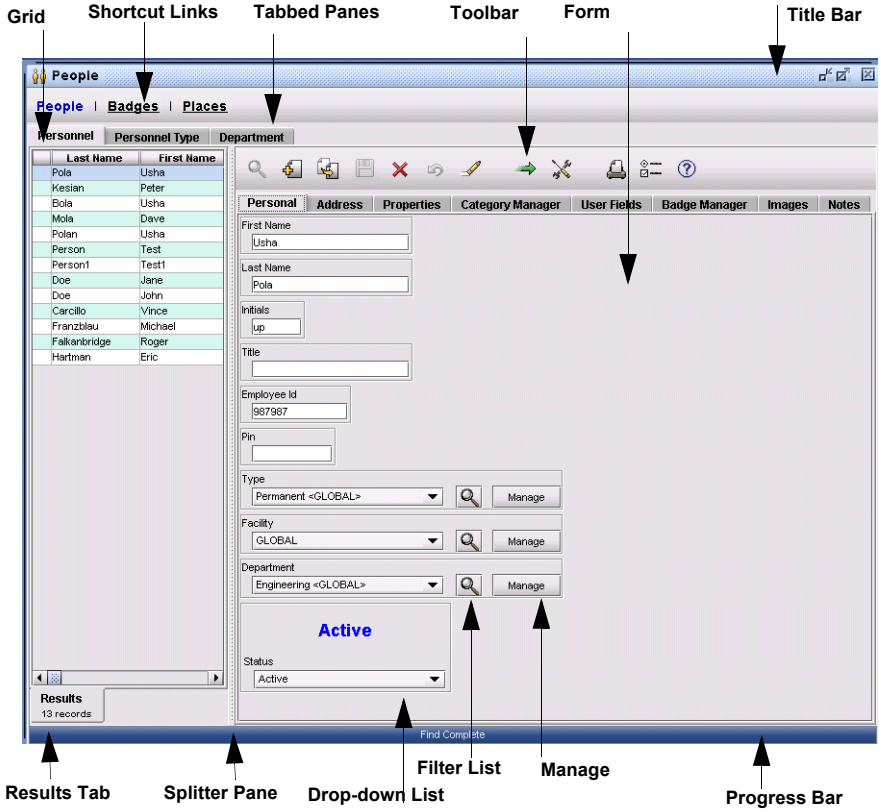


Table 14. Title bar

Item	Description
Title Bar	The Title Bar runs across the top of the window. It displays the label of the primary navigation menu item and contains three buttons: • Minimize: Click to resize your window to a smaller size. • Maximize: Click to resize your window to a larger size. • Close: Click to exit the window.

Table 15. Toolbar

Item	Description
Find 	Click to locate specific data records based on selection criteria entered into any of the fields. This is useful if you want to change data of an existing record. If you click Find without entering any search criteria, the system will find all of the data records in that table. The records found for the search will be displayed in the grid to the left of the form. You must have View record permission to perform a search. The number of results returned is limited to the settings on the Systems Parameters form.
New 	Click to add a new record as the last row in the record list. Any default values are filled in or cleared if there is no default. You must have Insert record permission to create a new record and Update permission for all required fields.
Copy 	Click to create a new record and copy the values of the currently selected record to it. This is a quick way to create a new record that is similar to an existing record. A record must be currently selected in order to copy it. If multiple records are selected, a new record will be created for each one selected. The copied records will be placed at the bottom of the record list and marked with the new record icon  . You must have Insert record permission to copy a record. Only fields that you have permission for will be copied to the new record.
Save 	Click to save the data record currently displayed to the database. If you have created a new record, it will be added to the database. If you displayed an existing record and made changes to it, this new version will replace the old record in the database. You must have Update record permission to save any changes.
Delete 	Click to mark the record currently displayed for deletion. The record will be deleted from the database upon saving. You must have Delete record permission to mark a record for deletion and the record table must support deletion. If the record has record dependencies, a list displays indicating those records that are dependent on it.
Undo 	Click to cancel the previous action and restore the values of the previously edited data.
Clear 	Click to clear the fields and selections on the form. All option settings are set to an unselected state.
Run Template 	Click to display a list of master records that contain information that can be used as a starting point or rough draft for creating a new record. The necessary links have already been defined. You must have Run Template action permission to perform this function.

Table 15. Toolbar (continued)

Item	Description
Manage Template 	Click to display the Template Manager from which you can create, edit, or delete master records. You can lock certain fields so that they cannot be changed when running the template. Records created from a template display in the custom format in which the template was created. You must have Manage Template action permission to perform this function.
Preferences 	Click to display the Preferences form that allows you to reposition and filter the grid columns, as well as reposition the entire grid. The Preferences button on the form applications is controlled by the Form Preferences action permission on the Operator's system permission profile.
Print 	Click to print records in a tabular or form format to your default printer of your client workstation.
Help	Click to display online help about the current form and its fields. To navigate the entire Picture Perfect help system, click Show.

Table 16. Data grid

Item	Description
Grid	The record list window, or data grid, shows the results of search operations and allows you to quickly navigate through the records found by a search. The data displayed in the grid columns consists of one or more fields of the Picture Perfect database table that is being manipulated. The number and order of the fields displayed, as well as the placement of the grid on the screen (left, right, top, or bottom), is configurable by clicking Preferences on the form toolbar. When an application is started, the record list window is initially empty. You use the data grid mainly for record navigation. A single record or multiple records may be selected for manipulation. Each row in the data grid represents a record. The records are obtained by performing a search, by creating a new record, or by copying a record. When a search is performed, the grid is filled with all of the records matching the search criteria. All previous records that were in the grid are removed. When adding new records, the records are placed at the bottom of the grid, and are marked with the new record icon  . Clicking on a single row in the grid will highlight and select that record for editing. The keyboard up and down arrows can also be used to move from one record to the next. The record's field values appear in the various pages of the form. If any field value is changed, the Edit icon  appears next to the row. More than one row can be selected in order to change a value for multiple records at one time, for example, updating a time value for all records. Multiple rows can be selected by left-clicking the first desired record, then dragging the mouse, and releasing it on the last desired record. Non-connected rows may be added to the selection by holding down the CTRL key on the keyboard while selecting the row with the mouse. All selected rows will be highlighted. When multiple rows are selected, the pages of the form window will be cleared and the values replaced by asterisks. Changing a field value changes it for all selected records. If any field value is changed, the Edit icon  appears next to the selected rows. To quickly access an item in a long list in a grid, click in any cell and begin to type the first letters of the item for which you are searching. See *Type ahead search* on page 28.

Table 17. Form

Item	Description
Form	The Form window provides the primary interaction between an operator and an application. It allows direct access to all fields within a single record or a selection of records from a host database table. A standard form is provided, however, it may be customized to display only those fields an operator needs to see or the fields can be arranged differently.

Table 18. Progress bar

Item	Description
Progress Bar	The current status of operations performed.

Table 19. Status bar

Item	Description
Status	The number of records retrieved as well as any errors encountered during creation are displayed here.

Table 20. Drop-down lists

Item	Description
Drop-down List	A drop-down list has an arrow at the right of the box, and when clicked, displays a list of options. The contents of a list consist of items you added using other forms. *Example: If you have not defined any micros in the system (using the Micros form), the Micros drop-down pick-list will be empty.* Selecting an item from a drop-down list will limit the search to records with matching selections. Drop-down lists will auto-complete, allowing you to type in leading characters of a desired item to jump to that point. A blank or an empty drop-down list does not limit the search. **Note:** You must have, at minimum, View permission to the form to which the drop-down list corresponds, to view that drop-down list. **Note:** Only drop-down items that are part of the active facility set are available.
Manage	Picture Perfect forms contain various drop-down lists, such as Facility, Input Group, and so on, that are populated with records created from other Picture Perfect forms. The Manage button next to these lists allows you to access the appropriate form and create or delete records. You must have Manage permission to perform this function.
Filter	Picture Perfect forms contain various drop-down lists, such as Facility, Input Group, and so on, that are populated with records created from other Picture Perfect forms. The Filter button next to these lists allows you to filter the list by description and/or facility using wildcards and operators as described in *Search criteria* on page 27. From the results of the search, select and click Ok.

Search criteria

When performing a search for data, you may want to view all records or only certain records. Prior to clicking Find , search criteria may be entered as follows:

Text boxes

- A blank text box returns all records.
- A text box containing text only returns records that contain the text specified.
- Wildcards and operators can be used to help delimit the search. For instance, the asterisk can expand the search in either direction around a string of characters.
- Text searches are not case sensitive.

Table 21. Wildcards and operators

Item	Function
Son*	The system will find records such as **Son**esta, **son**ya, **SON**NY.
*son	The system will find records such as Robin**son**, jack**son**, NEL**SON**.
son	The system will find records such as Ma**son**ry, sea**son**al.

Other symbols and their functions include the following:

Table 22. Other symbols

Symbol	Function
	Equal to (no symbol required)
!	Not equal to
>	Greater than
<	Less than
*	Match string
?	Match a single character
&	Logical and
|	Logical or
>=	Greater than or equal to
<=	Less than or equal to

Radio buttons

- Selecting radio buttons limits the search to records with matching selections.
- Radio buttons cannot be cleared. Therefore, when a radio button selection is not required, an additional button “Do Not Care” is included in case a radio button is selected in error.

Check boxes

- Checking a check box limits the search to those records that have those options enabled.
- Clearing a check box limits the search to those records that do not have those options available.
- Leaving the check box as is, with the ?, indicates the value in this field does not participate in the search.

Schedule control

- When searching for scheduled events when an Event Time is selected, a specific time of the day must be entered. The search will return only those records that contain a start time that matches the time entered.
- To search for scheduled events based on any time of the day, do not select the At time/mode buttons. Select the days of the week for which scheduled events are desired, and then click Find.

Drop-down lists

- Selecting an item from a drop-down list will limit the search to records with matching selections. Drop-down lists will auto-complete, allowing you to type in leading characters of a desired item to jump to that point.
- A blank or an empty drop-down list does not limit the search.

List window

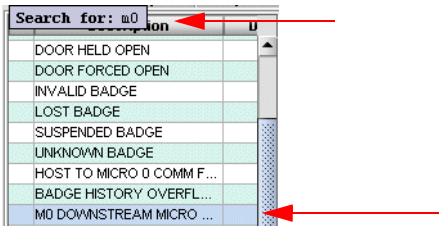
- Adding an item from the Available window to the Selected window limits the search to those records with matching selections.
- If more than one item is selected, the search is limited to those records containing all of the selected items in the exact order shown.

Note: A blank Selected window does not limit the search.

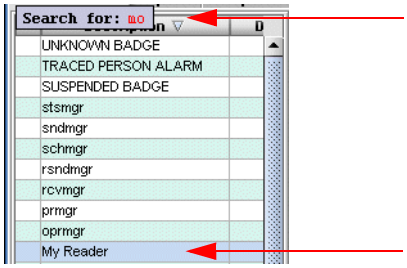
Type ahead search

To quickly access an item in a grid, click in any cell and begin to type the first letters of the item for which you are searching.

For example, if you type m0 (where 0 is zero), the first item beginning with m0 is highlighted



However, if you type mo (where o is oh), the first letter typed, m, takes you to an entry beginning with m, but when you type the o, the text displays in red, indicating that there is no entry beginning with mo.



Chapter 3 Configuration checklist

This chapter describes the preferred order of tasks required for setting up your Picture Perfect system. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

Because the Picture Perfect applications build off one another, it is important that the setup procedures follow a logical flow. The steps below are listed in the preferred order to make the configuration of your system a smooth one.

Configuration steps

Table 23. The steps for configuring a Picture Perfect system

Step	Task	Menu	Reference
1	Assign system parameters to be used by the system during operations.	Setup System Parameters	See *Assigning system parameters* on page 40.
2	Create facility records in order to partition your database records.	Configuration Facilities Facility Tab	See *Creating facilities* on page 53.
3	Create printer records for the printers configured during installation.	Setup Printers Printers Tab	See *Setting up printers* on page 54.
4	Optional: Set up imaging workstations.	Setup Workstations Workstations Tab	See *Setting up workstations (optional)* on page 56.
5	Create modem records to define the types of modems that you intend to use for dial-up micro controller communication.	Configuration Micros Modems Tab	See *Configuring modems* on page 64.
6	Create a port record to define a serial port for micro controller communications.	Configuration Micros PortsTab	See *Configuring ports* on page 66.
7	Create a network port record to define a port for network micro controller communication.	Configuration Micros Network Ports Tab	See *Configuring ports* on page 66.
8	Create e-mail records to allow alarms to be routed to e-mail addresses.	Control Routings Email Recipients Tab	See *Configuring email* on page 70.
9	Create routing records, in addition to the predefined routings, to define where certain types of messages are sent.	Control Routings Routings Tab	See *Defining routings* on page 72.
10	Create badge format records to define formats required in addition to the predefined 10-digit and 12-digit badge formats.	Access Badge Badge Format Tab	See *Defining badge formats* on page 74.

Table 23. The steps for configuring a Picture Perfect system (continued)

Step	Task	Menu	Reference
11	Create department records to assign departments to badge holders.	Access People Department Tab	See *Defining departments* on page 76.
12	Create personnel type records, in addition to those provided by the system, so you can assign a personnel type to badge holders.	Access People Personnel Type Tab	See *Defining personnel types* on page 77.
13	Create facility permission profile records, in addition to Global provided by the system, that describe an operator's level of access to the various forms and fields. The functions included on this form are filtered by facility.	Control Operators Facility Permission Profile Tab	See *Creating facility permission profiles* on page 81.
14	Create system permission profile records, in addition to Global provided by the system, to describe the functions each operator level is permitted to perform. The functions included on this form are system related and are not filtered by facility.	Control Operators System Permission Profile Tab	See *Creating system permission profiles* on page 85.
15	Create form profile records, to associate custom forms with an operator's permission.	Control Operators Form Profile Tab	See *Creating form profiles* on page 89.
16	Create permission group records, in addition to the default record All Groups Allowed, to be used to limit operator permission to specific categories, areas, and/or reports.	Control Operators Permission Groups Tab	See *Setting up permission groups* on page 91.
17	Create permission records that combine system, form, and facility permission profiles. This permission is then assigned to an operator.	Control Operators Permission Tab	See *Setting up permissions* on page 93.
18	Create operator records for those individuals who will log on to the Picture Perfect system.	Control Operators Operators Tab	See *Defining operators* on page 95.
19	Create route definition records to define where alarm and activity messages are routed. This is typically a physical location, such as a building.	Control Routings Route Definition Tab	See *Creating route definitions* on page 109.
20	Create route point records to be used to specify when and to which operators, alarm and activity messages are routed.	Control Routings Route Points Tab	See *Defining route points* on page 110.
21	Create message records to define alarm instructions that will display on the Alarm or Activity Monitor.	Configuration Alarms Alarm Messages Tab	See *Creating alarm instructions* on page 114.

Table 23. The steps for configuring a Picture Perfect system (continued)

Step	Task	Menu	Reference
22	Create response records to define alarm responses that the operator can select when responding to an alarm.	Configuration Alarms Alarm Responses Tab	See *Creating alarm responses* on page 115.
23	Create alarm records to define each alarm, both physical and logical.	Configuration Alarms Alarms Tab	See *Defining alarms* on page 117.
24	Define the colors that will be used in the Alarm Monitor so that the color scheme reflects the alarm state.	Configuration Alarms Alarm Colors Tab	See *Defining alarm colors* on page 120.
25	Create output group records to be used to activate all outputs assigned to the same group.	Configuration Inputs Outputs Output Groups Tab	See *Creating output groups* on page 126.
26	Create input group records to be used to trigger output groups when any individual inputs in the input group are detected.	Configuration Inputs Outputs Input Groups Tab	See *Creating input groups* on page 127.
27	Create micro records to identify each micro controller and define how it operates and communicates.	Configuration Micros Micros Tab	See *Defining micros* on page 132.
28	Create encryption keys to encrypt data between the host and the micro.	Configuration Micros Keys Tab	See *Creating encryption keys* on page 149.
29	Flash the Picture Perfect application code into the micro controllers.	eFlash MicTool Micro Flash Utility	See *Flashing micros* on page 151.
30	Create an output record to define the characteristics and the purpose of each output point and the output group to which it belongs.	Configuration Inputs Outputs Outputs Tab	See *Defining outputs* on page 158.
31	Create an input record to define the characteristics and the purpose of each input point and the input group to which it belongs.	Configuration Inputs Outputs Inputs Tab	See *Defining inputs* on page 161.
32	Define category records to identify groups of badge holders by type, title, function or shift.	Access Places Categories Tab	See *Creating categories* on page 172.
33	Define area records to describe areas of your site that require the same level of access control.	Access Places Areas Tab	See *Creating areas* on page 174.

Table 23. The steps for configuring a Picture Perfect system (continued)

Step	Task	Menu	Reference
34	Create reader records to define how each reader operates and to associate it with any links required to process reader activity.	Configuration Doors and Readers Readers Tab	See *Defining readers* on page 182.
35	Create door records to define how each door operates and to associate any links required to process door status or alarm activity.	Configuration Doors and Readers Doors Tab	See *Defining doors* on page 187.
36	Create records to define operating modes, in addition to the system defined Normal mode, that are activated either by schedule or by command.	Control Modes Modes Tab	See *Creating modes* on page 194.
37	Create mode event records to assign the starting date and time that a mode goes into effect when scheduling a mode change, such as a holiday.	Control Modes Mode Events Tab	See *Changing modes by scheduling a mode event* on page 198.
38	Create area events records to define and schedule the desired characteristics for all the readers, doors, and routings in an area for the duration of the event.	Access Places Area Events	See *Scheduling area events* on page 201.
39	Create reader events records to define and schedule the desired characteristics of a single reader for the duration of the event.	Configuration Doors and Readers Reader Event Tab	See *Scheduling reader events* on page 206.
40	Create door events records to define and schedule the desired characteristics of a single door for the duration of the event.	Configuration Doors and Readers Door Events Tab	See *Scheduling door events* on page 209.
41	Create alarm events records to define and schedule the desired characteristics of a single alarm for the duration of the event.	Configuration Alarms Alarm Events Tab	See *Scheduling alarm events* on page 211.
42	Create input group event records to schedule placing an input group online or offline and to control the output groups or alarms that are triggered for the duration of the event.	Configuration Inputs Outputs Input Group Events Tab	See *Scheduling input group events* on page 213.
43	Create output group event records to schedule enabling or disabling a specific output group and/or to change its state to off or on for the duration of the event.	Configuration Inputs Outputs Output Group Events Tab	See *Scheduling output group events* on page 217.
44	Create backup event records to schedule a system backup to run automatically at the specified day and time.	Control Backup Backup Events Tab	See *Scheduling backup events* on page 219.
45	Create report event records to schedule SQL reports to run at specific times.	Reports Reports Events Report Events Tab	See *Scheduling reports* on page 306.

Table 23. The steps for configuring a Picture Perfect system (continued)

Step	Task	Menu	Reference
46	Create badge records to control the functions and capabilities of the badge.	Access Badges Badges Tab	See *Defining badges* on page 224.
47	Create personnel records to identify each badge holder.	Access People Personnel Tab	See *Defining personnel* on page 231.
48	Optional: Set up badge designs.	Setup Badge Designs Badge Designs Tab	See *Setting up badge designs* on page 256.
49	Optional: Create custom forms.	Setup Custom Forms Custom Forms Tab	See *Creating and editing custom forms* on page 330.
50	Optional: Create custom lists.	Setup Custom Lists Custom Lists Tab	See *Creating and editing custom lists* on page 333.
51	Optional: Create master templates for generating new records with the necessary links predefined.	Any Form Toolbar Manage Templates	See *Managing templates* on page 324.

Chapter 4 Setup

This chapter describes information related to using the Picture Perfect forms. It also includes information on optional setup procedures.

In this chapter:

Overview

When using Picture Perfect, some of the forms contain default information that you can change as required. All forms may be customized to display the fields you choose to display. You may also create custom lists as needed, such as a list box of company or division names.

This chapter includes information on setting your system parameters, working with Picture Perfect forms, and setting up optional items such as printers and imaging stations.

Creating, editing, deleting, and printing records

All Picture Perfect forms use a standard method to add, edit, or delete records.

Note: You must allow appoximately 90 seconds for the cache to update when saving changes to a record.

Creating records

To create a record:

1. From the Primary menu, such as *Access, Configuration, Control*, or *Setup*, select a Secondary menu item, and then click the appropriate tab. For example: *Access, People, Personnel*.

2. Click **New** .

   The record list window, or data grid, displays a row marked with the error record icon . If a search has been performed, the grid is filled with all of the records matching the search criteria. When adding new records, the records are placed at the bottom of the grid, and are marked with the error record icon .

3. Complete the form.

   A detailed explanation of each field on the form can be found on the Fields and Controls section for each form in this manual. Because all Picture Perfect forms are user-customizable, not all fields may appear on your form or they may appear in a different order. All required fields are indicated by red text. When all required information is complete, the error icon is replaced by the new record icon and the Save icon is enabled.

4. Click **Save** . This icon is unavailable if all required information is not entered or if you do not have the required permissions for the form.

Editing records

To edit a record:

1. From the Primary menu, such as *Access, Configuration, Control*, or *Setup*, select a Secondary menu item, and then click the appropriate tab. For example: *Access, People, Personnel*.

2. From the toolbar, click **Find** .

The record list window, or data grid, shows the results of search operations and allows you to quickly navigate through the records found by a search. When an application is started, the record list window is initially empty.

3. Select a record from the list in the data grid.
   - The number and order of the fields displayed, as well as the placement of the grid on the screen (left, right, top, or bottom), is configurable by clicking **Preferences** on the form toolbar.
   - Clicking on a single row in the grid will highlight and select that record for editing. The keyboard up and down arrows can also be used to move from one record to the next. The record's field values appear in the various pages of the form.
   - More than one row can be selected in order to change a value for multiple records at one time, for example, updating a time value for all records. Multiple rows can be selected by left-clicking the first desired record, then dragging the mouse, and releasing it on the last desired record. Non-connected rows may be added to the selection by holding down the CTRL key on the keyboard while selecting the row with the mouse. All selected rows will be highlighted. When multiple rows are selected, if the field data is the same for all records, the field value displays. However, if the field data is not the same in all records the field value is replaced by an asterisk. Changing a field value changes it for all selected records.
   - If any field value is changed, the **Edit** icon appears next to the selected rows.
4. Make the necessary changes to the form.
   - A detailed explanation of each field on the form can be found on the Fields and Controls section for each form in this guide. Because all Picture Perfect forms are user-customizable, not all fields may appear on your form or they may appear in a different order.
   - When editing a form, if you fail to supply required information, the **Error** icon appears in the Function tab label as well as next to the record in the data grid. The field that requires correction is labeled in red.
5. Click **Save** . This icon is unavailable if all required information is not entered or if you do not have the required permissions for the form.

Deleting records

To delete a record:

1. From the Primary menu, such as *Access, Configuration, Control*, or *Setup*, select a Secondary menu item, and then click the appropriate tab. For example: *Access, People, Personnel*.
2. From the toolbar, click **Find** .

   The record list window, or data grid, shows the results of search operations and allows you to quickly navigate through the records found by a search. When an application is started, the record list window is initially empty.
3. Select a record from the list in the data grid.
   - The number and order of the fields displayed, as well as the placement of the grid on the screen (left, right, top, or bottom), is configurable by clicking **Preferences** on the form toolbar.

- Clicking on a single row in the grid will highlight and select that record for editing. The keyboard up and down arrows can also be used to move from one record to the next. The record's field values appear in the various pages of the form.
- More than one row can be selected in order to delete multiple records at one time. Multiple rows can be selected by left-clicking the first desired record, then dragging the mouse, and releasing it on the last desired record. Non-connected rows may be added to the selection by holding down the CTRL key on the keyboard while selecting the row with the mouse. All selected rows will be highlighted. When multiple rows are selected, if the field data is the same for all records, the field value displays. However, if the field data is not the same in all records the field value is replaced by an asterisk.

4. Click **Delete** .

   The selected records appear in the data grid with the deleted icon next to them.

5. Click **Save** . This icon is not available if all required information is not entered or if you do not have the required permissions for the form. If any record dependencies exist for the record you are deleting, a list of those records displays. The list must be cleared before the record can be deleted from the database.

Printing records

To print a record:

1. From the Primary menu, such as Access, Configuration, Control, or Setup, select a Secondary menu item, and then click the appropriate tab. For example: Access, People, Personnel.

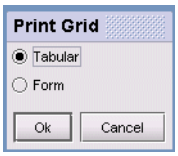
2. From the toolbar, click **Find** .

   The record list window, or data grid, shows the results of search operations and allows you to quickly navigate through the records found by a search. When an application is started, the record list window is initially empty.

3. Select a record from the list in the data grid.

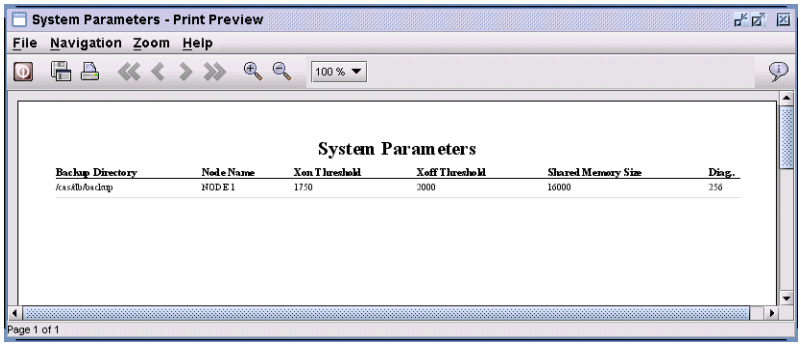
4. From the form toolbar, click **Print** . The Print Grid displays.

Figure 9. Print Grid



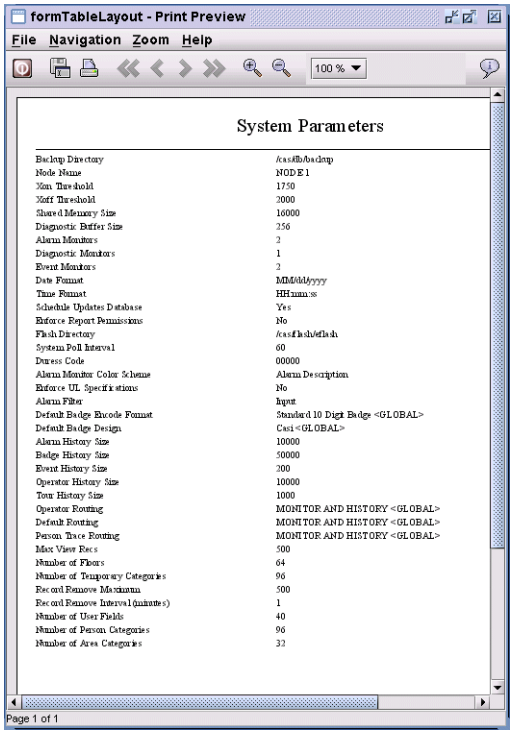
- Select **Tabular** to preview a page layout similar to the following:

Figure 10. Print Preview: Tabular



- Select **Form** to preview a page layout similar to the following:

Figure 11. Print Preview form

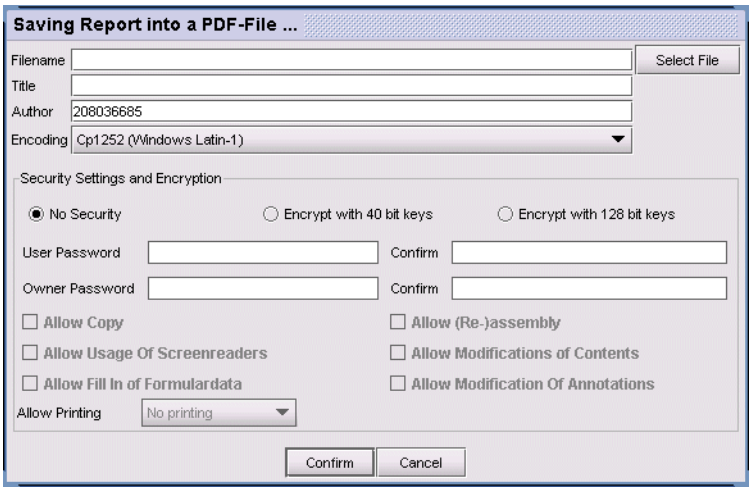


5. When you are satisfied with the preview, click one of the following:

 To close and exit the print window.

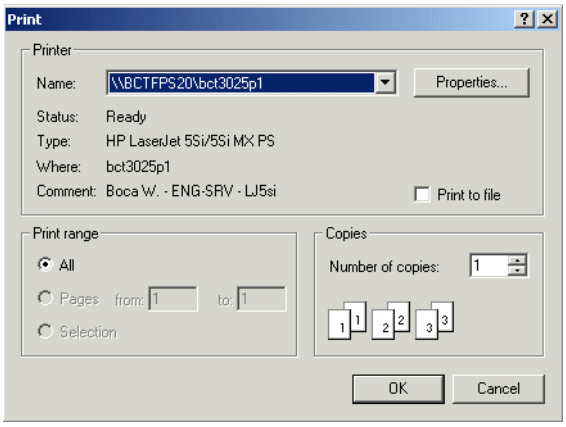
 To print an electronic file in .pdf format. A window similar to the following will display.

Figure 12. Print to a PDF



 To print to your default printer. A window similar to the following displays:

Figure 13. Print to a default printer

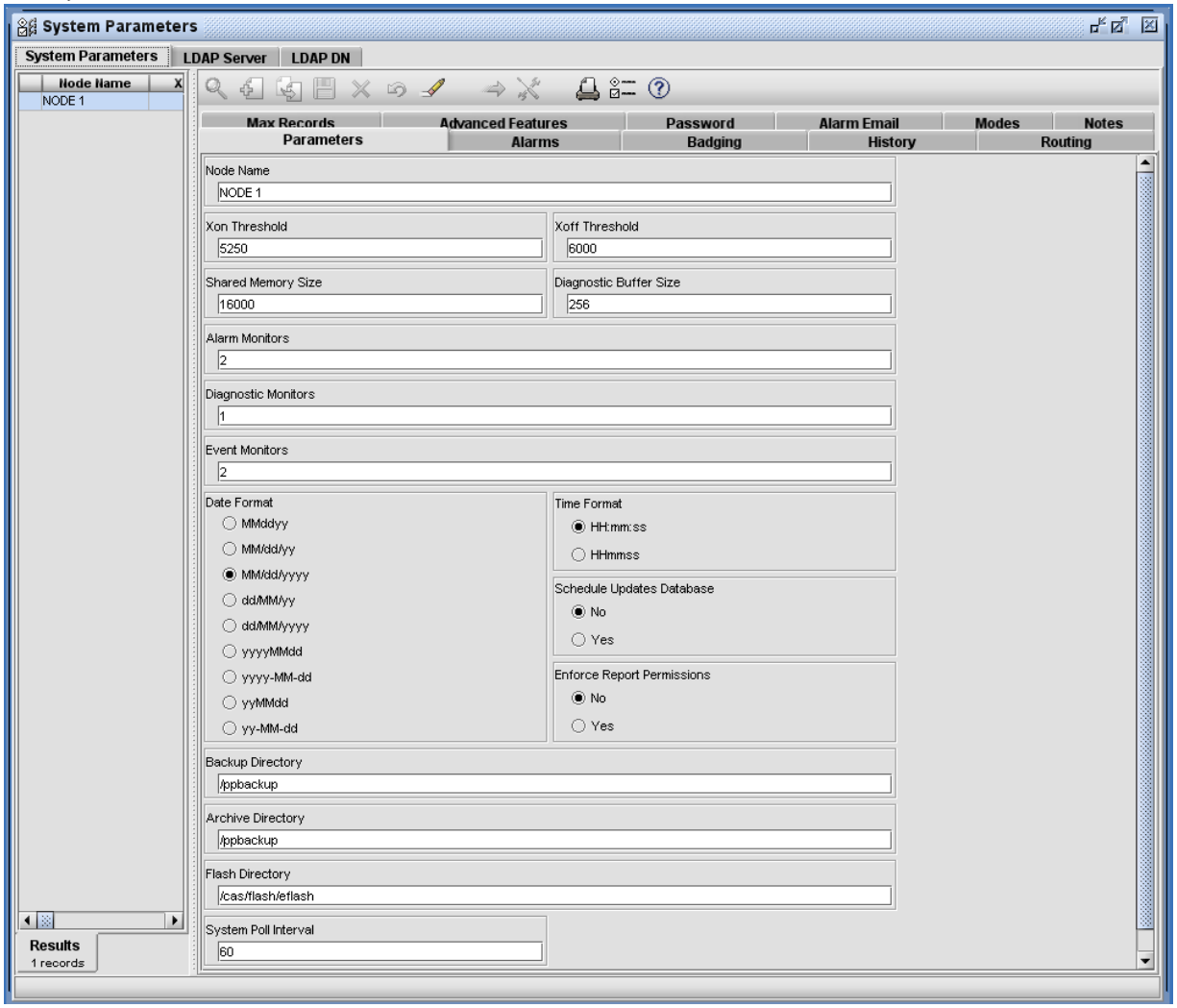


Assigning system parameters

System Parameters Form

The System Parameters form is used to assign system parameters that will be used by the system during the setup procedures. Some fields, as indicated in *Table 24, Parameter Form Fields* on page 42 are pre-set, based on the system installation settings. These should not be changed unless you are directed to do so by Customer Support.

Figure 14. System Parameters form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown inthe following table. There is no required sequence to follow.

Table 24. Parameter Form Fields

Tab	Field name	Description
Parameters	Node Name	Node name of the host (normally set to NODE 1). This field is pre-set and should only be changed as directed by your customer support representative.
	Xon Threshold	The number of queued messages that control TPS message buffering. Xon must be smaller than Xoff. This field is pre-set and should only be changed as directed by your customer support representative.
	Xoff Threshold	The number of queued messages that control TPS message buffering. Xoff must be larger than Xon. This field is pre-set and should only be changed as directed by your customer support representative.
	Shared Memory Size	The size (KBytes) of shared memory used. This field is pre-set and should only be changed as directed by your customer support representative.
	Diagnostic Buffer Size	The size (KBytes) of the diagnostic buffer. This field is pre-set and should only be changed as directed by your customer support representative.
	Alarm Monitors	This field is reserved for future use. Default is 2 for the current version.
	Diagnostic Monitors	This field is reserved for future use. Default is 1 for the current version.
	Event Monitors	This field is reserved for future use. Default is 2 for the current version.
	Date Format	Specify the date format of Month (MM), Day (DD), and Year (YY or YYYY) that the system will use. Click a radio button to select one system date format.
	Schedule Updates Database	When a micro runs a schedule, a SUP (Schedule Update) message is sent to the host. This SUP message gets logged in the /cas/log/sup.mmdd log file where mm is the current month and dd the day. If this value is set to Yes, the database is updated to reflect the value changed by the schedule. **Note:** If this feature is enabled, Area Events will update the database if all micros associated with all readers in the specified Area are within the same timezone.

Tab	Field name	Description
	Enforce Report Permissions	These radio buttons are used if you want to restrict report access to certain permission groups. By default, report permissions will be not be available. Select Yes to enable this option.
	Backup Directory	The default file system in which to store backups when backing up to Disk File.
	Archive Directory	The default file system in which to store archives when archiving to Disk File.
	Flash Directory	Specifies the source directory to search for flash files. This replaces the default directory of: /cas/flash/eflash
	System Poll Interval	Specifies the frequency with which the Performance Monitor data is refreshed.
	Time Format	cooSpecify the way the hour, minutes, and seconds appear in the time of day (HH:MM:SS or HHMMSS). Time displays in military (24-hour) format. Click a radio button to select the system time format. Even though the system will display time in one format or the other, it should be noted that a time value can be entered in either format. It should also be noted that time values can be entered in abbreviated format. The only abbreviated formats supported for data entry are the following: SS MMSS HH:MM
Alarms	Enforce UL Specification	This field will alter the operation of the Remove button in the Alarm Response window. If the No button is selected, the Remove button will operate normally, that is, it will always be available. If Yes is selected (recommended), the Remove button will be grayed out unless the alarm is in reset state. This means that the operator will be unable to remove the alarm until it has been reset. The exception is alarms with the Immediate Reset Input control option set. Because these alarms move instantly into reset state, the Remove button will always be available.

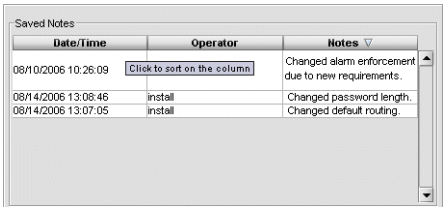
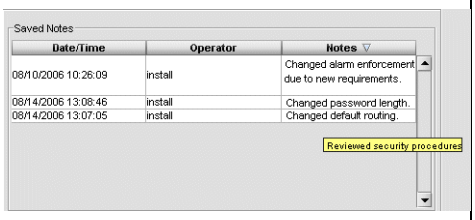
Tab	Field name	Description
	Alarm Filter	**Micro**: If this radio button is selected, the alarm will be assigned the same facility as the micro record from which it originated. **Input**: If this radio button is selected, the alarm will be assigned the same facility as the input record with which it is associated. **Input Group**: If this radio button is selected, the alarm will be assigned the same facility as the input group record with which it is associated. **Alarm**: If this radio button is selected, the alarm will be assigned the same facility as the alarm record with which it is associated. **Location**: The Location column in the Alarm Monitor displays the name of the door, reader, input, or micro that the alarm originated from. If this radio button is selected, the alarm will be assigned the facility of the door, reader, input, or micro displayed in the Location column.
	Alarm Monitor Color Scheme	Select one of the two radio buttons, depending on how you want to implement alarm color. **Processing State** Select this button if you want all alarms of one state to be of the same color. The Processing States are Active, Bumped, Notified, Remote, Pending, and Completed. *Example, if you want all Active alarms to be white text on a red background and all Completed alarms to be white text on a green background, select this button.* See *Alarm monitor color scheme: Processing state* on page 121. **Alarm Description** Select this button if you want to select text and background colors on an individual alarm basis. If you choose this option, the Alarm Color window will be displayed on the Alarms form. See *Defining alarm colors* on page 120.
	Duress Code	Enter the PIN number used to signal duress situations.

Tab	Field name	Description
	Alarm Delay (sec) (RAN)	This field will only appear if the optional RAN (Remote Alarm Notification) package is installed. The Alarm Delay field defines the length of time the operator is given to acknowledge the alarm. Once the notify time is reached and the operator has not responded to the alarm, a message will be sent to the Alarm Monitor. The Alarm Monitor process state for that alarm will be changed to Remote in the case of RAN.
	Alarm Priority (RAN)	This field will only appear if the optional RAN (Remote Alarm Notification) package is installed. The Alarm Priority field sets the upper limit for the priorities of alarms that will be sent to RAN. Any alarms with an alarm priority between 1 and the setting specified here will be examined.
Badging	Default Badge Encode Format	This is a required field that represents the default badge encode setting for the system. Click Default Badge Encode Format and choose a badge encode format from the list box. If the operator does not set a badge encode format on the Badges form, this default setting is used.
	Default Badge Design	The system default for a badge design is set in a manner similar to setting a printer default. When selected, the system default will be used when no other design is specified. For more information on this field, see *Setting a default badge design* on page 260.
	Image Types	This field is only enabled if the optional Image package is installed. Click to change properties of images such as the aspect ratio. These changes apply to all badge images captured or printed on the Imaging workstation where the changes are made. If there are multiple Imaging workstations, the changes must be made on each workstation. Warning: These parameters are critical to the operation of the Image component! Consult Customer Support before making any changes.

Tab	Field name	Description
History	Alarm/Badge/Operator/Event/Tour History Size	The number of transaction records (alarm, badge, or operator) that can be stored in the history table or backup table. This value is set according to the amount of alarm, badge, or operator activity expected, considering the desired archive frequency. These three fields are grayed out which means that they are read-only fields. These fields are set during installation. These fields are pre-set and should only be changed as directed by your customer support representative.
Routing	Default Routing	Define a default routing to ensure that all messages (alarm and activity) are routed somewhere. Whenever the routing of a function is unassigned, the system will use this setting as the default. Click Default Routing to display a list box of routings. Select the desired routing, and then click Close.
	Operator Routing	Define an operator routing for operator activity. Click Operator Routing to display a list box of routings. Select the desired routing, and then click Close.
	Person Trace Routing	Define a routing for traced badges. Click Person Trace Routing to display a list box of routings. Select the desired routing, and then click Close. (See *Tracing badge holder activity* on page 388 for details on this feature.)
Max Records	Max View Recs	Enter the maximum number of records the system will have the ability to find and view. This is usually set to 500. If this value is not defined, the system will assume a value of 500. If this value is greater than 2500, the system will assume a value of 2500. This field controls the number of records shown in a list box. **Note:** This figure is dependent on system memory and number of users. Do not change this field to a higher number unless authorized to do so by your customer support representative. If set too high, the system will use excessive memory and may slow down and become non-responsive.

Tab	Field name	Description
	Record Remove Interval	Specifies a period of time (in minutes) during which a group of badge records may be removed. The system removes badge records for this period of time, or until the number of badge records set under Record Remove Maximum has been reached, whichever comes first. If more badges are to be removed, the system waits until the beginning of the next interval, then automatically initiates the badge removal process again. This process is repeated until all listed badges have been removed. The minimum setting is one minute. It is not required to restart Picture Perfect or the Badges form when changing this setting. **Note:** The badge removal process is initiated by clicking the Remove function button on the Badges form. See *To permanently remove a badge from the database:* on page 230.
	Record Remove Maximum	Specifies the maximum number of badge records that can be removed during the Record Remove Interval. It is not required to restart Picture Perfect or the Badges form when changing this setting.
	Number of Person Categories	This field is read-only and is set to 96 during installation. It is the maximum number of categories that can be assigned to a person.
	Number of User Fields	This field displays the number of User Fields that appear on the Badges form. User Fields are used for detailed badge holder identification. This field is read-only and is set to 40 during installation.
	Number of Area Categories	This field is read-only and is set to 32 during installation. It is the maximum number of categories that can be assigned to an area.
	Number of Floors	Enter the number of floors (0 to 64) serviced by an elevator associated with the Elevator Control feature. See *Elevator control* on page 369.
Advanced Features	Configured Devices	Click Refresh to display the total number of devices currently connected to the host.
	Alarm State	Click Refresh to display information about the most recent alarm as well as the current total number of active and pending alarms.

Tab	Field name	Description
	History Flags	Click Refresh to view an archive indicator for each history type. Yes indicates it is time to archive.
	History Counts	The total number of history records in the database for each history type.
	System Diagnostics	A list of all Picture Perfect sub-systems from which you may select to generate diagnostic information to a log file.
Password	Minimum Length	The minimum number of alpha/numeric characters that a password must contain, within the range of 6 to 60.
	Cannot Begin with Numeric Character	Check to require that passwords begin with an alpha character.; they can not start with a numeric character.
	Cannot End with Numeric Character	Check to require that passwords end with an alpha character; they can not end with a numeric character.
	Must be Mixed Case	Check to require that passwords contain both upper and lower case characters.
	Must Contain Alpha Numeric Characters	Check to require that passwords contain both alpha and numeric characters. If selected, enter the minimum number of numeric character required, within the range of 6 to 59.
	Cannot be Same as Login ID	Check to require that passwords be different than the Login ID.
Alarm Email	Include All Occurrences	Check to include each occurrence of an alarm process state change (for example active or pending) in the email message generated. By default, this requirement is not available.
	Include Priority	Check to include the priority of an alarm in the email message generated. By default, this requirement is not available.
	Include Condition	Check to include the condition of an alarm (for example, alarm/reset) in the email message generated. By default, this requirement is not available.
	Include Input State	Check to include the input state of an alarm (for example, open/closed) in the email message generated. By default, this requirement is not available.

Tab	Field name	Description
	Include Process State	Check to include the process state of an alarm (for example, active/pending) in the email message generated. By default, this requirement is not available.
	Include Count	Check to include the number of times an alarm has set and reset in the email message generated. By default, this requirement is not available.
Modes	Number of Auths for Mode Change	The number of distinct operator authenticators required to allow a mode change.
Notes	Saved Notes	All saved notes applicable to this record are listed including the Date/Time the note was created and the operator that created it. Click on a column heading to sort by Date/Time, Operator, or alphabetically by note.  By hovering the mouse over the note, the entire note displays. 
	Notes	This is a free form text field where you can add information pertinent to System Parameter records. *Example: Changed password length 12/12/09.* **Note:** Notes cannot exceed 210 characters - they will be truncated if exceeded.

Related procedures

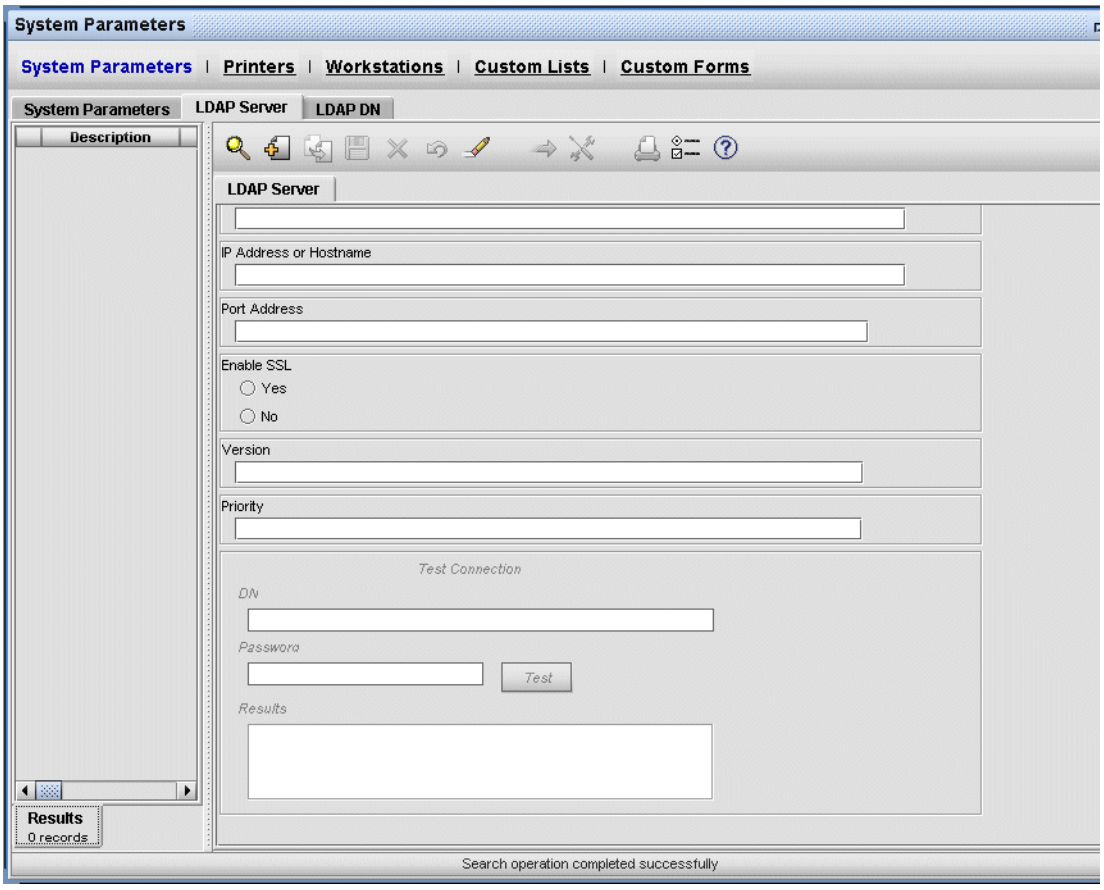
To edit system parameters:

1. From the **Setup** menu, select **System Parameters**, and then click the **System Parameters** tab.
2. Edit the System Parameters form as necessary. Note only certain fields can be edited. See *Table 24, Parameter Form Fields* on page 42 for a description of each field.
3. Click **Save** . This icon is not available unless all required information is entered, or if you do not have the required permissions to use the form.
4. To implement the system parameters you have changed, perform shutdown and restart procedures using the command line. See *Starting and stopping Picture Perfect* on page 8.

Configuring LDAP support

Picture Perfect supports the use of the Lightweight Directory Access Protocol (LDAP) interface to provide single sign on (SSO) where one password for a user is shared between many services. LDAP is configured on the LDAP Server and LDAP DN forms.

Figure 15. LDAP form



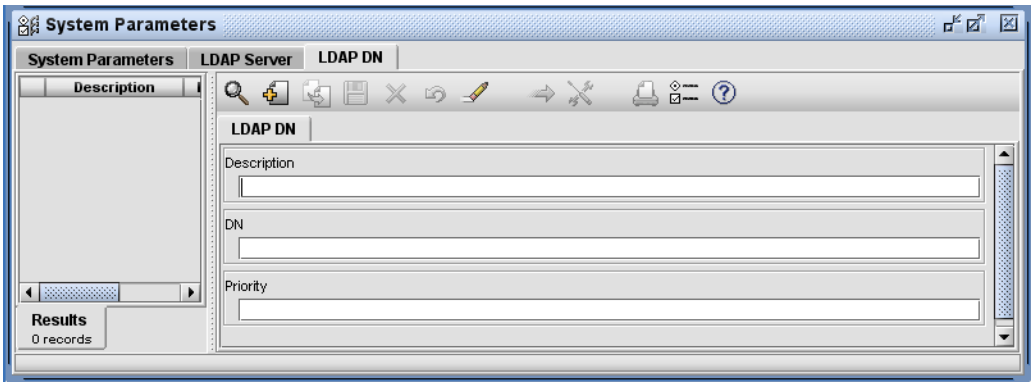
Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 25. LDAP Server form fields

Tab	Field name	Description
LDAP Server	Description	A description of the LDAP server.
	IP Address or host name	The physical address of the LDAP server, for example 204.171.64.2 or the hostname.
	Port Address	The address that identifies the port to be used for communication between the Picture Perfect server and the LDAP server.
	Enable SSL	Click Yes to enable DES encrypted transmission between the LDAP server and the Picture Perfect server. **Note:** In order for the Picture Perfect server to verify the identity of your LDAP server, Picture Perfect must know the LDAP Certificate filename. Prior to enabling SSL: • Log in to Picture Perfect as `root`. • At the command prompt, type: `EnableLdapSSL <certificate filename>`
	Version	The version of the LDAP interface, for example: 3
	Priority	When there are multiple LDAP servers, this is the priority by which to attempt access.
	Test Connection	To test the connection between the LDAP server and the Picture Perfect server, type the LDAP distinguished name (DN) and password and then click **Test**.

Figure 16. LDAP DN form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 26. LDAP DN form fields

Tab	Field name	Description
LDAP DN	Description	A description of the DN entry. For example, Headquarters Security Personnel.

	DN	An LDAP distinguished name (DN) is an LDAP entry that identifies and describes the full path on the LDAP server used to authenticate an authorized user.
		Distinguished names consist of the name of the entry itself as well as the names, in order from bottom to top, of the objects above it in the LDAP directory.
		Supported DNs:
		`ou=people,dc=mycompany,dc=com`
		`cn=[operator.user_name],ou=people,dc=mycompany,dc=com`
		`cn=[operator.login_id],ou=people,dc=mycompany,dc=com`
		`cn=[operator.employee_id],ou=people,dc=mycompany,dc=com`
		When an authorized user types in their username, this path is used by Picture Perfect to authenticate the user's password.

	Priority	When there are multiple LDAP servers, this is the priority by which to attempt access.

Related procedures

To configure LDAP:

1. Add the IP address and host name of the LDAP server to the local host file.
2. From the Picture Perfect **Setup** menu, select **System Parameters**, and then click the **LDAP Server** tab.
3. Fill in the fields with the appropriate data as described in Table 25.
4. Click **Save** . This icon is unavailable if all required information is not entered or if you do not have the required permissions for the form.
5. From the Picture Perfect **Setup** menu, select **System Parameters**, and then click the **LDAP DN** tab.
6. Fill in the fields with the appropriate data as described in Table 26.
7. Click **Save** . This icon is unavailable if all required information is not entered or if you do not have the required permissions for the form.
8. Under **Test Connection**, fill in the **DN** and **Password** fields and click **Test**.
9. From the Picture Perfect **Control** menu, select **Operators**.
10. For each operator record required, enable the **LDAP Authentication** check box.

Creating facilities

The Picture Perfect system allows you to group your system database records according to facilities. A facility is comprised of records associated with a group of buildings in a city, a building, a floor in a building, a tenant, or a room on a particular floor in a building.

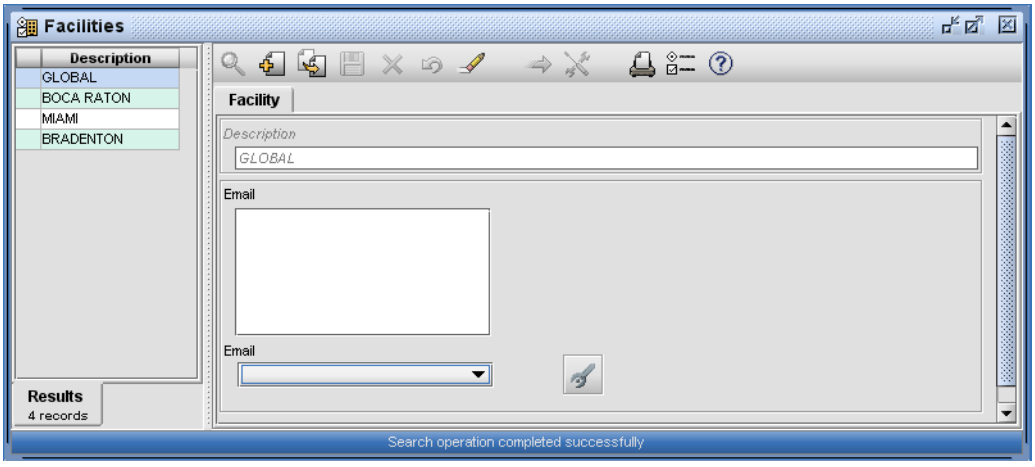
Facility records are text descriptions of these places. Database records can be grouped together by assigning them to a common facility. All Picture Perfect forms support facilities. A facility field is displayed on each form with the following exceptions:

- Although the Monitor forms do not have a Facility field, incoming messages are filtered by facility.
- Although the following forms do not have a Facility field, access to them is governed by system permissions profiles: Backup and Restore, Custom, Edit SQL Statements, Force Logoff, Form Preferences, Log Monitor, Monitor Preferences, Performance Monitor, Purge All Alarms, Send Message, Status Monitor, Tour Functions, User Monitor, Access Secure, Alarm Colors, Control Outputs, Data Generator, Emergency DI, Facilities, LDAP DN, LDAP Server, and Parameters.

At installation, a facility, Global, is created and, by default, all database records are assigned to it. If an existing Picture Perfect system is being upgraded, all existing database records will be assigned to this facility, unless they are already associated with a facility.

Use the Facilities form to create and delete facility records. These records, combined with Facility Profiles and Permissions, allow you to restrict operator access to records assigned to those facilities.

Figure 17. Facilities form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 27. Facility form fields

Field name	Description
Description	Enter a text description, up to 60 alphanumeric characters long, that defines a logical grouping, such as a group of buildings, a building, a floor in a building, or a room on a particular floor in a building. *Example: Headquarters*
E-mail	Select the target e-mail recipients to receive mode change notifications. **Note:** If it is necessary to send a notification to a large group of recipients (for example, all employees) then an e-mail alias should be used.

Related procedures

To create, edit, or delete a Facility record:

1. From the **Configuration** menu, select **Facilities**, to display the **Facility** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

   Note: Before deleting a facility, you should ask yourself two questions:

   a. What do you want to do with the records that have the facility assigned to them?

      You will be given the opportunity to re-assign the facility for those related records to Global or to change them to an existing facility. If you choose to re-assign them to an existing facility, you should keep in mind who has access to that facility because that operator will now have access to those records using their existing facility profile.

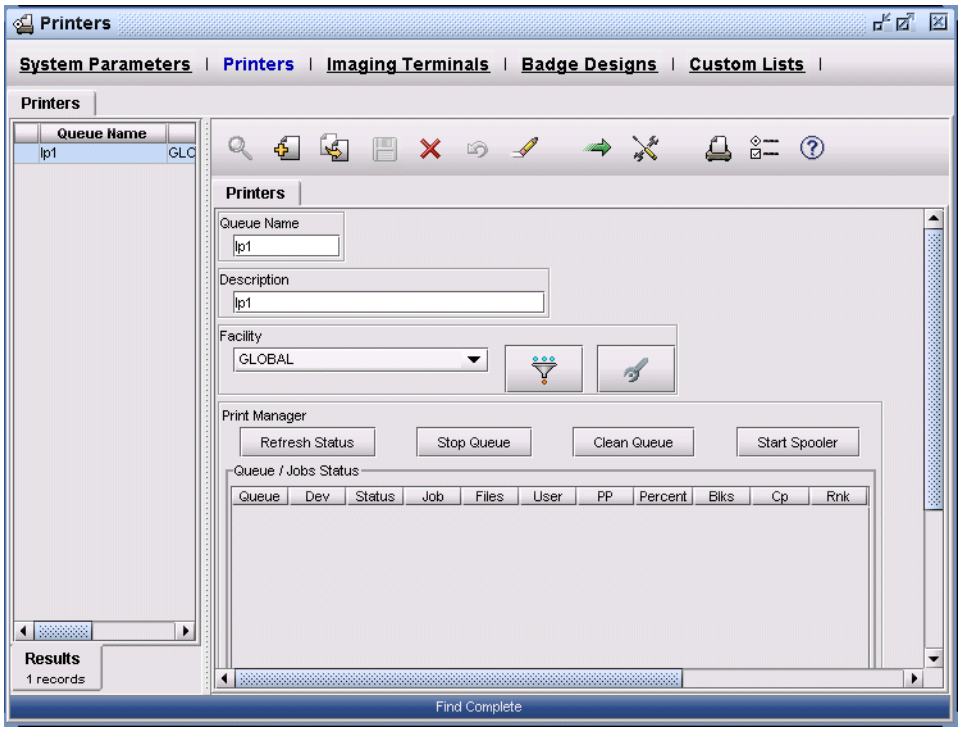
   b. What operators are already using that facility?

      When a facility is deleted, it will remove the facility-to-facility profile relationships for any operator using that facility. The facility record is deleted but the facility profile record is left intact. This means you may need to re-assign the facility profile to a new facility for each operator that may have been using the deleted facility. Deleting an existing facility will effectively remove an operator's access to that facility.

Setting up printers

Use the Printers form to add each printer configured during installation for server-side printing. This only applies to Activity Routing and Report Events.

Figure 18. Printers form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 28. Printer form fields

Field name	Description
Description	A description of the printer, including type, quality, location, etc. as required (up to 30 alphanumeric characters).
Facility	Click Facility to display the facilities list box. This field reflects the facility that this record is assigned to. For more information, see *Creating facilities* on page 53.
Queue Name	The exact name of the print queue specified when printers were configured in the Picture Perfect installation procedure on the server. The print queue name matches the printer name. *Example: If the printer name is lp0, then the printer queue should be lp0.*

Related procedures

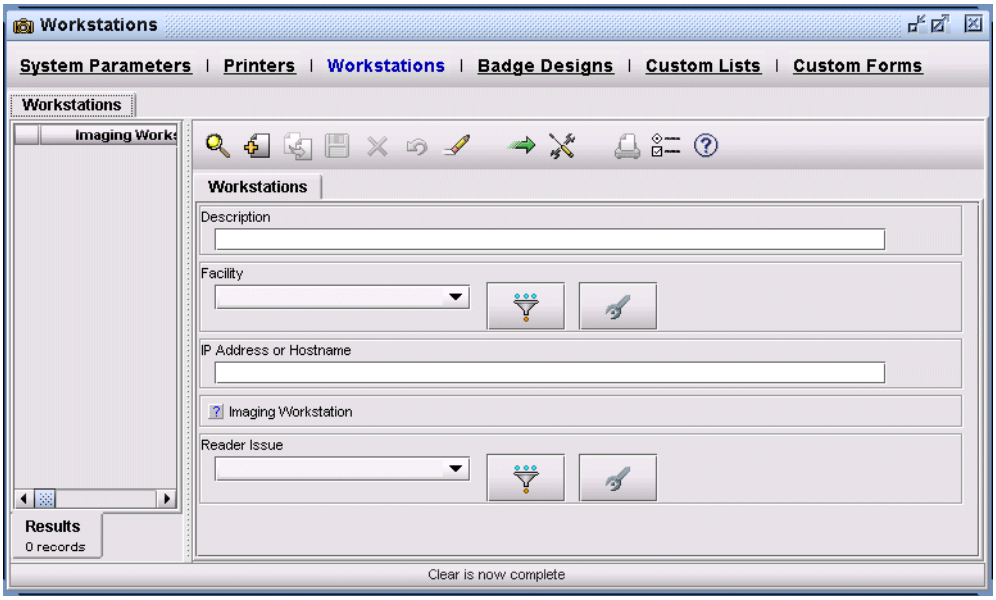
To create, edit, or delete a Printer record:

1. From the **Setup** menu, select **Printers**, and then click the **Printers** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Setting up workstations (optional)

Use the Workstations form to configure terminals that may be used by Picture Perfect as badge issue workstations, or if you have the optional Imaging package installed, as Imaging workstations.

Figure 19. Workstations form



Note: Do not define the host console terminal as a Workstation. The host terminal functions only as an administrative terminal; not as a workstation.

Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 29. Workstation form fields

Field name	Description
Description	Type any alphanumeric combination (1 to 60 characters). *Example: Command Center Workstation*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
IP Address or Host Name	Type the IP address or hostname of the client workstation. This must be specified in the operating system file **`/etc/hosts`** on the host system.
Imaging Workstation	Select this check box if this terminal will be used as an Imaging workstation
Reader Issue	The reader used as the Badge Issue reader. See *Reader Issue* on page 225.

Related procedures

To create, edit, or delete a workstation record:

1. From the **Setup** menu, select **Workstations**, and then click the **Workstations** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

To set up your Imaging workstations:

1. Install the capture card (optional).

   To capture your images, you can use any device that has a TWAIN, WINTAB, or Video for Windows (VFW) driver installed. Follow the instructions provided by the device manufacturer for installing the device.

2. Install the print driver.

   The Imaging package requires the installation of print drivers. Refer to the instructions shipped with your printer.

3. Install signature pad drivers (optional).

   Depending on the signature pad you are using, you may need to install additional TWAIN or WINTAB drivers to make them compatible with the Imaging package. After installing the pad, install a TWAIN or WINTAB driver for the pad.

4. Install the Imaging software.

   - The optional image package must be installed on the host to perform imaging activities on a client workstation. See the *Picture Perfect 4.5 Imaging User Manual* for details.
   - A client workstation that will be used as an imaging terminal requires the installation of the client imaging software on the workstation. First, install the Java Runtime Environment on the workstation. Click the J2SE Java Runtime Environment (JRE) link on the host web page. Then, install the imaging software by clicking the EPIBuilder Imaging Installation link on the host web page.
   - Remember to add this workstation as an imaging terminal.

5. Install the software licence key.

   Obtain and install new Picture Perfect server license to activate the optional image package installed on host. See the *Picture Perfect 4.5 Installation Manual* for details.

6. Set up cameras and lighting (optional).

   Refer to the following document on your documentation CD for helpful information on camera and lighting setup:

   Image Quality Enhancements

Setting up SSL Encryption

Client SSL Encryption

The activation and deactivation of SSL encryption for events and requests transmitted between the Picture Perfect host and its clients is controlled by the `EnableSSL` script. This script can be run anytime after Picture Perfect has been installed.

Note: Turning on Client SSL Encryption will have a negative impact on client performance.

To activate client SSL encryption, perform the following steps:

1. Log on to the system as `ppadmin`.
2. At the command prompt, stop Picture Perfect by typing:

   `rc.pperf -k` Enter

   If this is a redundant configuration, stop Picture Perfect by typing:

   `pprscmd stop`
3. Log on to the system as `root` by typing:

   `su - root`
4. Type the following command to enable SSL:

   `EnableSSL 1` Enter
5. Log on to the system as `ppadmin`.
6. Start Picture Perfect again by typing:

   `rc.pperf` Enter

   If this is a redundant configuration, start Picture Perfect by typing:

   `pprscmd start <primary or backup>`
7. From a client PC browser window, type the following secure URL to connect to the server:

   `https://<hostname>/Picture/`

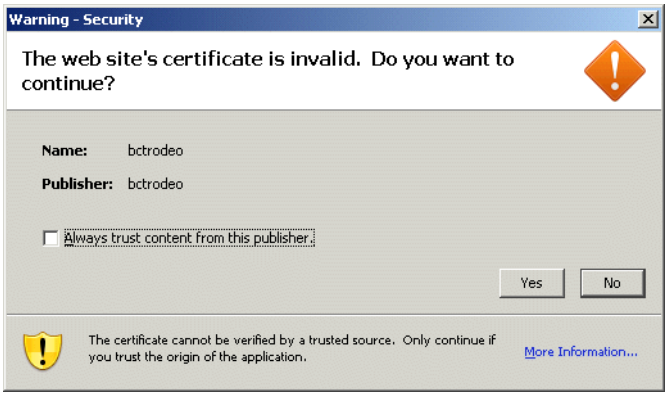
   Note: Once SSL has been enabled, operators should access the client using the secure HTTPS URL (note the "s" after http):
   `https://<hostname>/Picture/`

   If you are using Internet Explorer 7, and you receive a certificate warning screen, follow these steps:

   a. Click on the "Continue to this website (not recommended)" hyperlink.

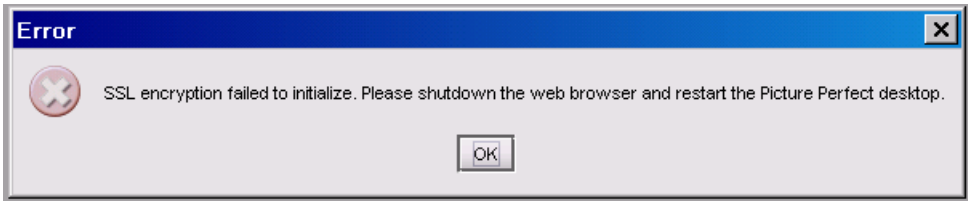
   b. Click on "Certificate Error" at the top of the window, just to the right of the URL drop-down list.
8. In the Certificate Invalid Alert window, select View Certificate.
9. In the Certificate window, select Install Certificate.
10. In the Certificate Import Wizard - Welcome window, select Next.
11. In the Certificate Import Wizard - Certificate Store window, select the Automatically select the certificate store based on the type of certificate radio button. Click Next to continue, and then click Finish.
12. In the Security Warning window, click Yes to install the certificate. The install is complete when the Certificate Import Wizard displays the message "The import was successful." Click OK to close the window.
13. In the Security Alert window, click Yes to proceed.
14. In the Picture Perfect webtop, click the Picture Perfect button in the upper left corner to display the Login screen.
15. Log on to the system.

16. When logging on to Picture Perfect, with SSL enabled, the following window displays:



17. In the Warning - Security window, check the Always trust content from this publisher check box, and then click Yes. This window appears because Picture Perfect self-signs the SSL certificates and does not obtain them from a third party. If you wait too long to click Yes, the application will time out and you will be denied access. If the timeout occurs, close Picture Perfect and try again.

Note: When toggling between SSL disabled to SSL enabled, a client may encounter the following error message when logging in:



In order for the client to successfully login, it will be necessary to first close down the client applet window and close down all open web-tops and perform the login again. This only needs to be done once.

To deactivate client SSL encryption, perform the following steps:

1. Log on to the system as `ppadmin`.
2. At the command prompt, stop Picture Perfect by typing:

   `rc.pperf -k` Enter

   If this is a redundant configuration, stop Picture Perfect by typing:

   `pprscmd stop`
3. Log on to the system as `root` by typing:

   `su - root`
4. Type the following command to disable SSL:

   `EnableSSL 0` Enter

   where 0 = zero.
5. Log on to the system as `ppadmin`.
6. Start Picture Perfect again by typing:

   `rc.pperf` Enter

If this is a redundant configuration, start Picture Perfect by typing:

```
pprscmd start <primary or backup>
```

7. From a client PC browser window, type in the following URL to connect to the server:

   ```
   http://<hostname>/Picture/
   ```

8. When the Picture Perfect webtop displays, click the Picture Perfect button in the upper left corner to display the Login screen.
9. Log on to the system.

Note: Note: Once SSL has been disabled, operators should access the client using the standard HTTP URL: http://<hostname>/Picture/

Database encryption

The activation and deactivation of encryption for client-server database connections is controlled by the `DbSecComm` script. This script can be run anytime after Picture Perfect has been installed.

The Informix CSM module for database encryption requires the `libstdc++.so.5` library, which is installed by the `compat-libstdc++-33-3.2.3-61.i386.rpm` package.

Note: Turning on database encryption will have a negative impact on client performance. You do not need to have database encryption enabled in order to have client ssl enabled, or vice versa.

To determine if the `libstdc++.so.5` library is installed:

1. Log on to the system as `ppadmin`.
2. At the command prompt type the following:

   ```
   rpm -qa | grep "libstdc++"
   ```
   Enter

3. If `compat-libstdc++-33-3.2.3-61.i386.rpm` appears in the list of packages, then `libstdc++.so.5` is already installed on the Picture Perfect host.

   If the `libstdc++.so.5` library is already installed on the host, continue to *To activate database encryption:* on page 61.

   If the `libstdc++.so.5` library is not installed on the host, continue to Step To download and install the `compat-libstdc++-33-3.2.3-61.i386.rpm` package:.

To download and install the `compat-libstdc++-33-3.2.3-61.i386.rpm` package:

1. Log on to the system as `ppadmin`.
2. At the command prompt, stop Picture Perfect by typing:

   ```
   rc.pperf -k
   ```
   Enter

   If this is a redundant configuration, stop Picture Perfect by typing:

   ```
   pprscmd stop
   ```

3. Change to the /tmp directory by typing the following command:

   ```
   cd /tmp
   ```
   Enter

4. Navigate to the following web address to obtain the `compat-libstdc++-33-3.2.3-61.i386.rpm`.

   ```
   http://rpm.pbone.net/index.php3/stat/4/idpl/12267595/com
   /compat-libstdc++-33-3.2.3-61.i386.rpm.html
   ```

   Right-click on one of the mirrors, and then select Properties. Copy the Address: (URL), and then type the following command. Paste the URL in place of the <mirror>.

   ```
   wget <mirror>
   ```
   Enter

5. Install the `compat-libstdc++-33-3.2.3-61.i386.rpm` package by typing the following command:

   ```
   rpm -i /tmp/compat-libstdc++-33-3.2.3-61.i386.rpm
   ```
   Enter

To activate database encryption:

1. Log on to the system as `ppadmin`.
2. At the command prompt, stop Picture Perfect by typing:

   ```
   rc.pperf -k
   ```
   Enter

   If this is a redundant configuration, stop Picture Perfect by typing:

   ```
   pprscmd stop
   ```
3. Log on to the system as `root` by typing:

   ```
   su - root
   ```
4. Type the following command to enable database encryption:

   ```
   DbSecComm 1
   ```
   Enter
5. Log on to the system as `ppadmin`.
6. Start Picture Perfect again by typing:

   ```
   rc.pperf
   ```
   Enter

   If this is a redundant configuration, start Picture Perfect by typing:

   ```
   pprscmd start <primary or backup>
   ```
7. Log on to the Picture Perfect application.
8. Check the Picture Perfect log file for database errors by typing the following command:

   ```
   logtail
   ```
   Enter
9. Press CTRL C to exit and return to the command prompt.
10. Query the database by typing:

    ```
    query operator
    ```
    Enter

    Observe the output. If an error occurs due to the CSM module or Picture Perfect configuration, it may appear here. The correct output will resemble the following:

    ```
    1 Systems Adminstrator 0000 install 1 1 -1 89fb511ffe93ee7826661ca1e3bb468dc1ad0ff2
    0 0 1 1      -1 20041006 170806 -1 System System system 1 1 -1      0 0        -1
    20041018 194738
    ```

To deactivate database encryption, perform the following steps:

1. Log on to the system as `ppadmin`.
2. At the command prompt, stop Picture Perfect by typing:

   `rc.pperf -k` Enter

   If this is a redundant configuration, stop Picture Perfect by typing:

   `pprscmd stop`
3. Log on to the system as `root` by typing:

   `su - root`
4. Type the following command to disable database encryption:

   `DbSecComm 0` Enter

   where 0 = zero.
5. Log on to the system as `ppadmin`.
6. Start Picture Perfect again by typing:

   `rc.pperf` Enter

   If this is a redundant configuration, start Picture Perfect by typing:

   `pprscmd start <primary or backup>`
7. Log on to the Picture Perfect application.

Chapter 5 System configuration

This chapter describes the system hardware and site configuration required to start using your system. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

After your installer completes the initial hardware and software installation, there are Picture Perfect forms that allow you to configure your system according to your specific requirements. Some of the forms contain default information that you can change as required.

The various forms are presented in the order recommended in *Configuration steps* on page 30.

Configuring modems

Use the Modems form to describe each modem type that you intend to use for dial-up communications. Modem types that you define using the Modems form appear in a list box for assignment to a micro (on the Micros form) and a port (on the Ports form). A micro can dial up the host on any available port that is compatible, meaning the modem type matches. Only compatible modem types can establish a connection.

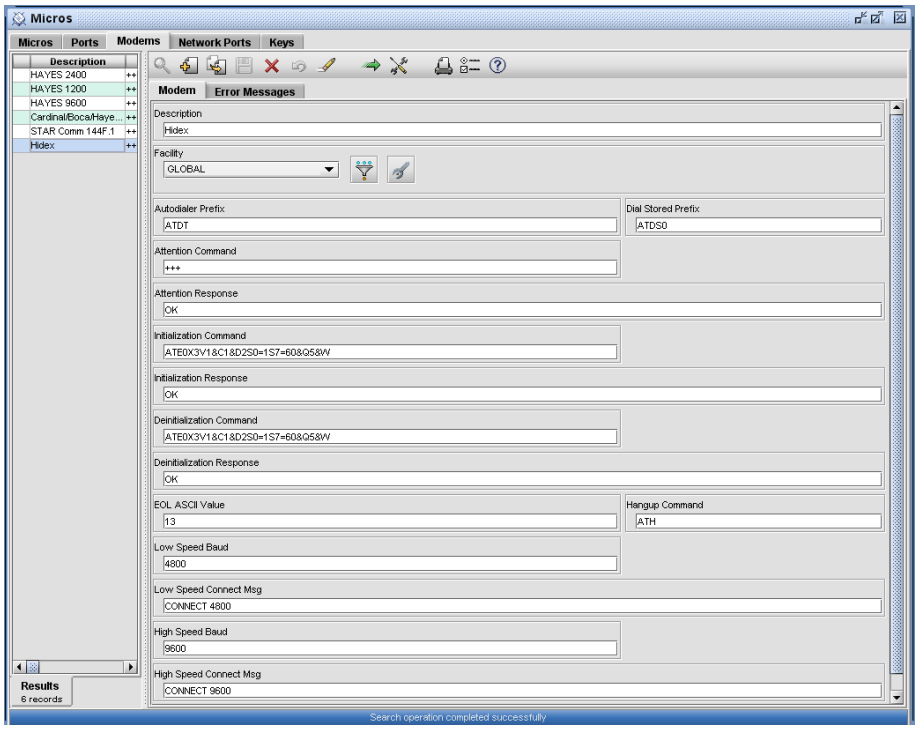
The DirecDoor, PXNPlus, and Micro/5-PX support 9600 baud only.

A dial-up micro uses standard modem communication and standard telephone lines to dial up and respond to the host. Each dial-up micro has a dedicated phone line and a modem for communication with the host. The modem connects via RS-232 cable at the micro's host port (RS-232 serial port).

The host has a list of user-definable phone numbers available for calling any dial-up micro in the system; likewise, all dial-up micros have a list of user-definable phone numbers available for dialing the host.

You can configure modems without having to restart the Picture Perfect system. You will need to refer to your modem manual when filling out the fields on the Modems form. If a default value appears in a field, you can accept that value if the modem type is Hayes-compatible.

Figure 20. Modems form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

If a default value appears in a field, you can accept that value if the modem type is Hayes-compatible.

Note: There are system-supplied forms for the Hidex modem, Hayes 1200, 2400, and 9600 modems, the Cardinal 28.8 V.34 modem, and the STAR Comm 144F.1 modem.

Table 30. Modem form fields

Field name	Description
Description	Type a modem description up to 60 alphanumeric characters long that specifies the modem type. This modem description will appear in a list box on the Micros form and the Ports form so that you can assign a modem type to micros and ports. *Example: Hayes 2400*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Autodialer Prefix	Enter the command string (0 to 30 alphanumeric characters) used to tell the modem to dial the number that follows.
Dial Stored Prefix	Enter the command string (0 to 30 alphanumeric characters) that tells the modem to dial the phone number stored in the modem's non-volatile memory. **Note:** Some modems can store phone numbers at multiple memory locations. On your modem, location 0 is not available for stored phone numbers because it is reserved for the host phone number.
Attention Command	Enter the wake-up string (0 to 30 alphanumeric characters) required to put the modem into command mode, so that it can receive other configuration commands (and eventually the hang-up command).
Attention Response	Enter the string (0 to 30 alphanumeric characters) that the modem returns to indicate that it received the attention command.
Initialization Command	Enter the command string (0 to 30 alphanumeric characters) used when preparing to dial out or answer.
Initialization Response	Enter the string (0 to 30 alphanumeric characters) that the modem returns to indicate that it received the initialization command.
Deinitialization Command	Enter the command string (0 to 30 alphanumeric characters) used to de-initialize the modem when hanging up.
Deinitialization Response	Enter the string (0 to 30 alphanumeric characters) that the modem returns to indicate that it received the de-initialization command.
EOL ASCII Value	Enter the character (expressed in ASCII value) that terminates every command string.
Hangup Command	Enter the command string (0 to 30 alphanumeric characters) used to disconnect or hang up the modem.
Low Speed Baud	For multi-speed modems, enter the lowest baud rate that this modem can use for a connection. The line speed can downgrade to this lower baud rate to accommodate older modems or poor line quality.
Lo-speed Connect Msg	Enter the message (0 to 30 alphanumeric characters) that the modem returns when it connects using its low-speed baud rate.

Table 30. Modem form fields (continued)

Field name	Description
High Speed Baud	For multi-speed modems, enter the highest baud rate that this modem can use for a connection. The modem uses its highest baud rate when it first tries to connect. If it does not receive a carrier using the high-speed baud rate, it steps down to lower baud rates until the connection occurs.
Hi-speed Connect Msg	Enter the message (0 to 30 alphanumeric characters) that this modem returns when it connects using its high-speed baud rate.
Error Message	Enter the message (0 to 30 alphanumeric characters) that this modem gives when it rejects an invalid command.
No Carrier Msg	Enter the message (0 to 30 alphanumeric characters) that this modem gives when it fails to connect; this message differentiates between No Carrier, No Answer, and Busy.
No Answer Message	Enter the message (0 to 30 alphanumeric characters) that this modem gives when it fails to connect; this message differentiates between No Carrier and No Answer.
Busy Msg	Enter the message (0 to 30 alphanumeric characters) that this modem gives when it fails to connect; this message differentiates between No Carrier and Busy.

Related procedures

To create, edit, or delete a modem record:

1. From the **Configuration** menu, select **Micros**, and then click the **Modems** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Configuring ports

Many of the port characteristics for micro communication lines are already configured at the time of installation, so all you need to provide is a port description, tty number, and line settings. If the port supports dial-up micros, you specify a phone number and modem type.

Use the Ports form to define a serial port and the Network Micro Ports form to define a network port. The system then allows you to assign the device port (line) to a micro.

- Unidirectional direct-connection micros require only a primary port.
- Bidirectional direct-connection micros require both a primary and a secondary port.
- Dial-up micros do not require a port assignment, but do require a Ports form.
- Network micros require only a network primary port.

The Ports form supports dynamic configuration for all fields except tty. Dynamic configuration means that you can configure ports without having to restart the Picture Perfect system. If you change the tty name, you must restart Picture Perfect.

Note: The fields on the Ports form will differ when on a redundant system. Refer to the *Picture Perfect Redundant Edition User Manual* for more information.

Figure 21. Ports form

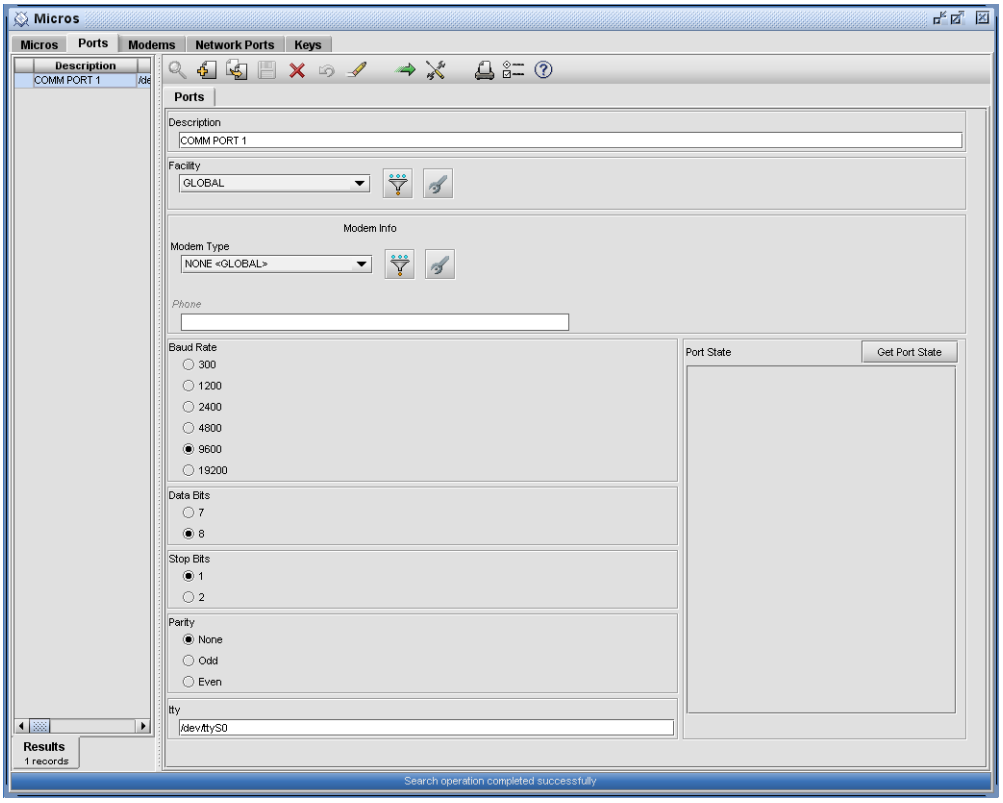
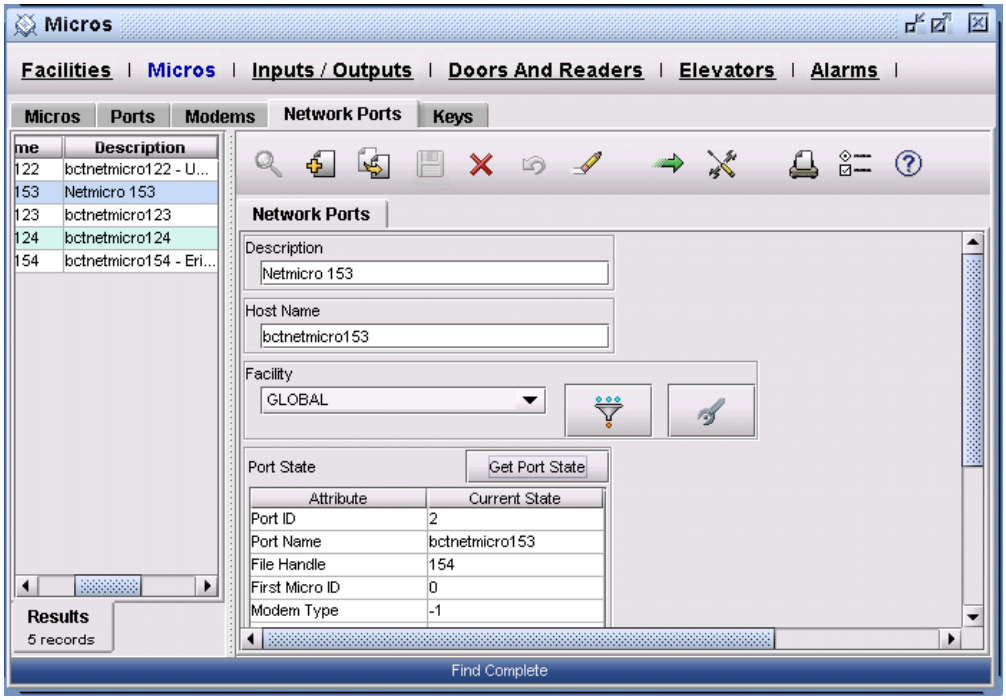


Figure 22. Network ports form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 31. Port form fields

Field name	Description
Description	Type a port description up to 60 alphanumeric characters long. The ports that you define appear in a list box on the Micros form so that you can assign a serial port to direct-communication micros (unidirectional or bidirectional). None appears in the list box so that you can indicate no secondary port for a unidirectional micro and no primary or secondary port for a dial-up micro. A typical description of a host port includes the line number and the port number. *Example: Line 1 Port 1 tty2* There are two serial ports on the host, and additional serial ports are available if a multi-port adapter is attached. **Note:** Serial port (S1) on the RISC/6000 is used by the system console, in the case of an ASCII console.
Modem Type	A port used for direct-communication micros does not require a modem type (select None). None is the default selection. If modems are connected, click Modem Type to display a list box of modems. Select the modem type that matches your modem, and then click Close.
Facility	Click Facility to display the facilities list box. Selecting a facility will allow the administrator to restrict operator access to those records in a specific facility. For more information, see *Creating facilities* on page 53.
Phone	The dial-up (micro-to-host) telephone number. Include the area code but not the PBX prefix or country code. A dial-up micro can use this number to dial the host. A dial-up micro uses a dynamic list of phone numbers to call the host on any compatible port that is available. When the port is assigned the same modem type as the micro, that port becomes compatible. **Note:** A port used for direct-communication micros does not require a phone number. (Leave this field blank for direct-connection micros.) The port used for dial-up communications requires a phone number.
Baud Rate	For direct-communication micros, select the desired baud rate. For dial-up micros, 9600 is the required line setting for the Micro/5-PX.
Data Bits	The required line setting is 8.
Stop Bits	The required line setting is 1.
Parity	The required line setting is None.

Table 31. Port form fields (continued)

Field name	Description
tty	**AIX**: Type the full path name of the port as defined in AIX, such as /dev/ttyN, where N=line number. This must be typed in lower-case characters, and must not be the port assigned to the operator's console. (Typically, tty0 is assigned to the console.) **Linux**: Refer to the following for Port Device Naming conventions for Linux systems: Com Ports com1 /dev/ttyS0 com2 /dev/ttyS1 PCI 8/16 Serial Port Adapter 1 /dev/ttya01 2 /dev/ttya02 3 /dev/ttya03

Table 32. Network port form fields

Field name	Description
Description	Type a port description up to 60 alphanumeric characters long. The ports that you define here will appear in a list box on the Micros form so that you can assign a network port to network micros. (None will automatically appear in the list box so that you can indicate no secondary port.) A typical description of a network micro port should allow an operator to identify it on the ports list box on the Micros form. It should also allow the operator to distinguish it from a serial port. *Example: Network Micro 0 Port*.
Host Name	Type the host name of the network micro. The host name of the network micro must be listed in the `/etc/hosts` file or a Domain Name Server (DNS). This can be either the IP address or the name.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Note: Firewall users: If your installation requires ANY micro and its corresponding host to communicate through a firewall, the firewall must be configured to allow for connections through the following ports: 6767, 6768, 7777.	

Related procedures

To create, edit, or delete a Port or a Network port record:

1. From the **Configuration** menu, select **Micros**, and then click the **Ports** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Configuring email

Use the Email Recipients form to add email addresses for the routing of alarms and mode changes.

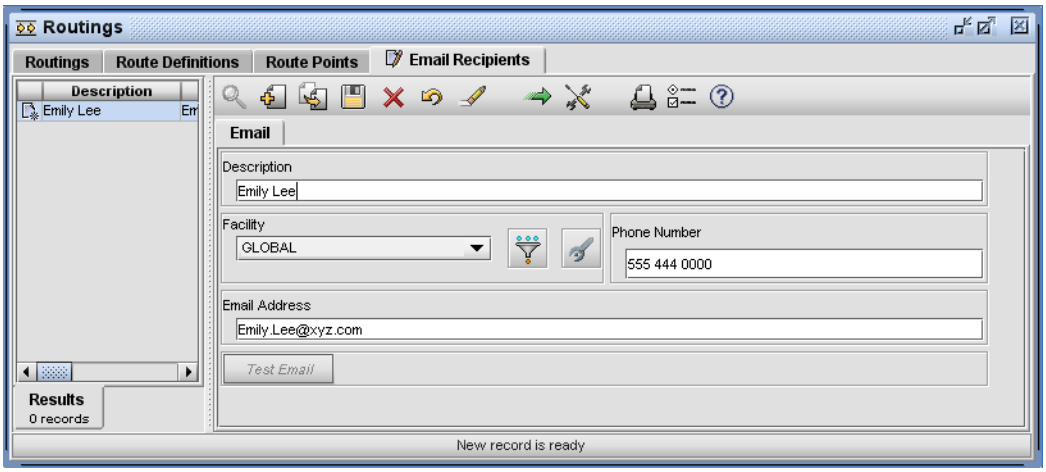
When an alarm is generated, a message will be emailed to the address listed in the Email Address field. Each time an alarm is set or reset, another message will be sent. Configuration parameters of the output included in the email message can be set using the Parameters form. See *System Parameters Form* on page 40.

Note: In order for the Email feature to work properly, the Sendmail subsystem must be properly configured. See your System Administrator or your IS department for assistance.

Example

Alarms that are assigned a routing of Email are sent to Emily.Lee@xyz.com.

Figure 23. Email Recipients form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 33. Email form fields

Field name	Description
Description	The name of the person to whom the e-mail is to be sent, or a description of the group, if using an alias (up to 60 alphanumeric characters).
Email Address	The e-mail address to which the alarm is to be sent. If you want the message to go to multiple addressees, enter a valid e-mail alias. An alias is used if you want to have an message sent to more than one email address. Any messages sent to this address will be handled by the Sendmail subsystem and routed to the appropriate e-mail addresses in the e-mail alias.
Phone Number	The phone number of the person specified by the e-mail address.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Test Email	Click the Test Email button to send a test email to the email address entered.

Related procedures

To create, edit, or delete an email record:

1. Select **Control**, **Routings**, and then **Email Recipients** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

To set up an alias:

1. Open a new terminal window.
2. Change to the `root` user by typing: `su`
3. Using an editor, such as `vi`, add the new alias to the `/etc/aliases` file. Each alias must be unique and must start on a new line. Aliases are in the form:

   ```
   alias: name@somedomain.com, name2@someotherdomain.net
   ```

For more information, at the command prompt, type: `man aliases`

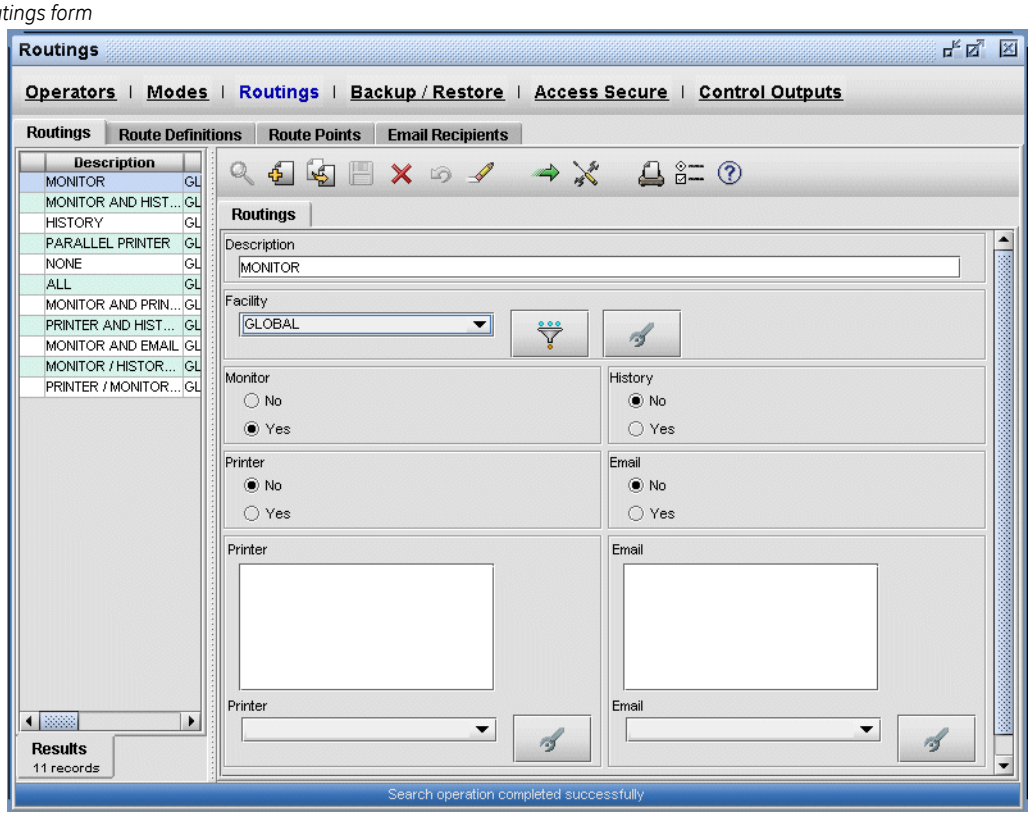
Defining routings

Use the Routings form to define where messages are to be sent. There are eleven predefined routings already entered. The system lets you use these routings to send messages to a printer, history log, e-mail, and/or to the monitor. The routings you create populate list boxes that are used in various aspects of the system.

Example

Incoming alarm messages are assigned a routing of *Monitor*.

Figure 24. Routings form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 34. Routing form fields

Field name	Description
Description	Type a description (0 to 60 characters) to identify the type of messages to be routed. *Example: Badge Activity, Operator Messages, Overnight Messages, or ALL* A single routing description can include multiple routing destinations. *Example: You may want messages received overnight to be routed to the printer, the monitor, and the history log.*
Printer	Select Yes to select a printer as a destination where you want messages to be routed. From the Printer drop-down list, select the specific printer queue.
Monitor	Select Yes to display the message on the alarm and activity monitor; this choice does not create a history record. **Note:** Monitor must be selected as a routing destination in order for an operator to respond to an alarm.
History	Select Yes to record the transaction message in the database history table; this allows the message to be referenced for history reporting.
Email	Select Yes to route messages to an email address or alias. The Email drop-down list contains all of the email addresses currently defined in the system. Select the desired addresses from the list box. **Note:** Yes must be selected for Monitor in order for this feature to be enabled.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete a routing record:

1. Select **Control**, **Routings**, and then **Routings** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

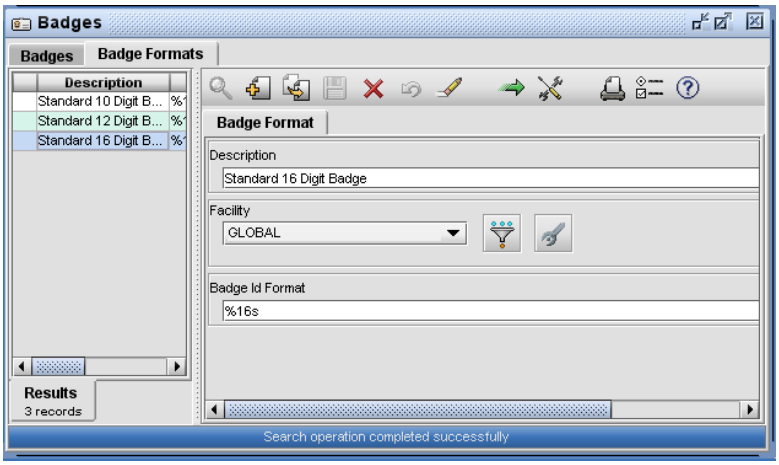
Defining badge formats

The format of the encoded badge is identified by a special character sequence that optionally starts with constant data (such as a facility code common to all badges) and always ends with variable data that indicates the length of the character string required in the Badge Encode Number field on the Badges form. A % sign indicates the beginning of the variable data and a lower-case s marks the end. The entire badge ID must be between 1 and 16 characters long.

Example

For example, the badge ID format 002%10s can be described as a facility code of 002 and a badge encode number of 10 characters. The system comes with one pre-loaded format, %10s, which is the format for 10-digit Wiegand readers. If additional formats are needed, they can be added on the Badge Formats form.

Figure 25. Badge Format form



Constant data (such as a facility code) is data common to all badges, and will be entered in front of the % in this field. (Constant data does not appear in the Badge Encode Number field of the Badges form.)

Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 35. Badge Format form fields

Field name	Description
Description	Type a description (0 to 60 characters) to identify the badge format. *Example: 10 Digit Badge* The badge formats that you define appear in a list box on the Parameters and the Badges forms.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Badge Id Format	Type a badge ID format (1 to 16 characters) using the sequence: Constant data (optional) % Variable data s Recommended: To ensure the Auto Generate function produces a unique badge ID number, the variable portion of the badge ID format must be at least 10 digits.

Related procedures

To create, edit, or delete a badge format record:

1. Select **Access**, **Badges**, and then **Badge Formats** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

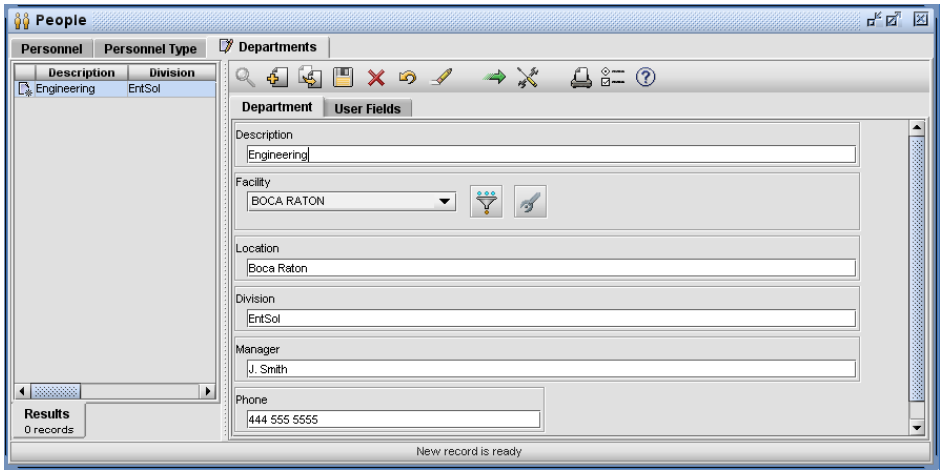
Defining departments

Use the Departments form to define a department. The department names entered here populate a list box that will be used on the Personnel form to assign a department to each badge holder.

Example

Employees working in research and development are assigned to the *Engineering* department.

Figure 26. Department form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 36. Department form fields

Field name	Description
Description	Type a description (1 to 60 characters) to identify the department. *Example: Marketing*
Division	Type a site-specific abbreviation (0 to 3 characters). *Example: ABC*
Location	Type where the department is located (0 to 20 characters) in a building or city. *Example: Lower Level*
Manager	Type the name of the manager of the department (0 to 23 characters).
User Fields	Type comments (0 to 40 characters).
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete a department record:

1. From the **Access** menu, select **People**, and then click the **Departments** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Defining personnel types

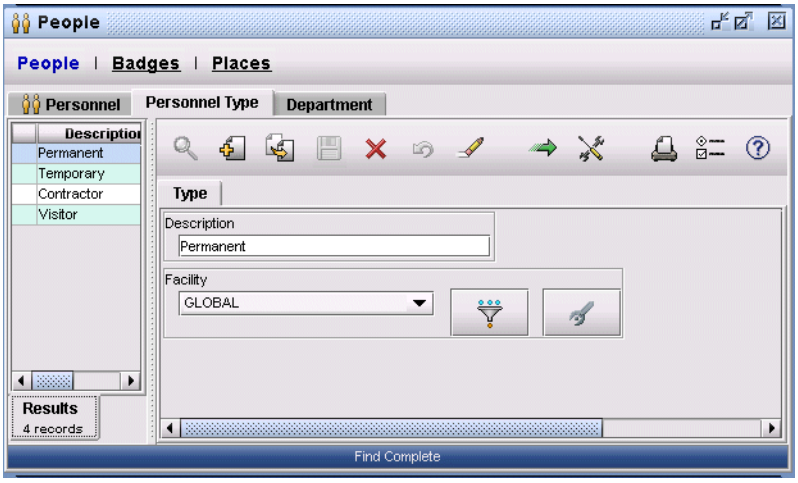
Use the Personnel Type form to define different types of personnel. These entries populate a list box used on the Badges form to assign a personnel type to each badge. Four personnel types are already entered into the system: Permanent, Temporary, Contractor, and Visitor. Additional types can be entered as described in *To create, edit, or delete a personnel type record:* on page 78.

Note: Available Categories and Temporary Categories: When a category is assigned to a person as a temporary category, that category will continue to remain in the "Available" list. This is to allow for the operator to set up multiple schedules for that category on the same person. An example - A cleaning crew needs access from 5pm - 10pm Tuesday - Friday, on Saturday they need access from Noon - 5pm.

Example

Full time employees are assigned a Personnel Type of *Permanent*.

Figure 27. Personnel Type form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 37. Personnel Type form fields

Field name	Description
Description	Enter the identification name of the personnel type to be added (up to 60 alphanumeric characters).
Facility	Click Facility to display the facilities list box. Selecting a facility will allow the administrator to restrict operator access to those records in a specific facility. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete a personnel type record:

1. From the **Access** menu, select **People**, and then click the **Personnel Type** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Chapter 6 Operator administration

This chapter describes how to control the operations that an operator can perform and the applications in which they can be performed. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

The Picture Perfect system allows you to group your system database records according to facilities. A facility can be records associated with a group of buildings in a city, a building, a floor in a building, a tenant, or a room on a particular floor in a building.

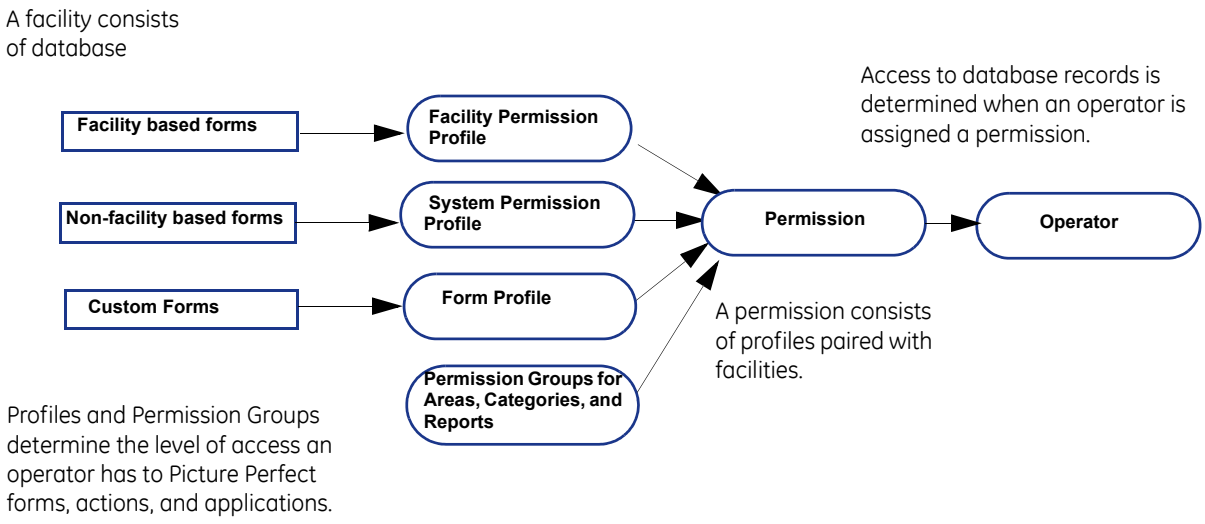
Facility records are text descriptions of these places. Database records can be grouped together by assigning them to a common facility. At installation, a facility, Global, is created and, by default, all database records are assigned to it. Operators using your Picture Perfect system require access to different forms and facilities depending on their function and location. They also require different levels of authority depending on their position.

A Permissions Profile is a way of defining the record and field level access permissions as well as action permissions that control what applications an operator can run. There are two types of profiles: Facility Permission Profiles which define permissions for Picture Perfect forms that are partitioned by facility, and System Permission Profiles that define permissions for the Picture Perfect forms that are not partitioned by facility. Default profiles are created at installation for System and Facility permissions: All, Insert, Update, View, and No. These profiles are locked (cannot be changed), but they may be copied and then edited to create additional profiles.

Once a permission profile is defined, it can be associated with a facility and assigned to a permission. This permission is then assigned to an operator and determines what records the operator is allowed to access and what they are allowed to do with them, based on the facility of the particular record. For example, when the Global facility is paired with the All Facility Permission profile and assigned to an operator, that operator has full access to the database records associated with the Global facility.

The following diagram depicts the relationship of the Picture Perfect tables when setting up facilities in your system. All of the records stored in the Picture Perfect database are either facility based or system based. By default, a Global facility is defined on the system if no other facility is defined. Records that are not associated with a facility are assigned to the Global facility. To determine the records that an operator can access, facilities are paired with a profile defining the level of access, and are then assigned to the operator's permission. Category and Reports availability are not governed by facility or system, but by permission groups.

Figure 28. Operator administration overview



After completing the initial system configuration, records need to be created in order to assign the proper permission sets to each operator. The following forms are required to create these records and are presented in the order recommended in *Chapter 3 Configuration checklist*.

- Facility Permission Profile
- System Permission Profile
- Form Profile
- Permission Groups
- Permissions
- Operators

Examples of the relationship of these records and how to link them is discussed in the section, See *Linking facilities, facility profiles, permissions, and operators* on page 98.

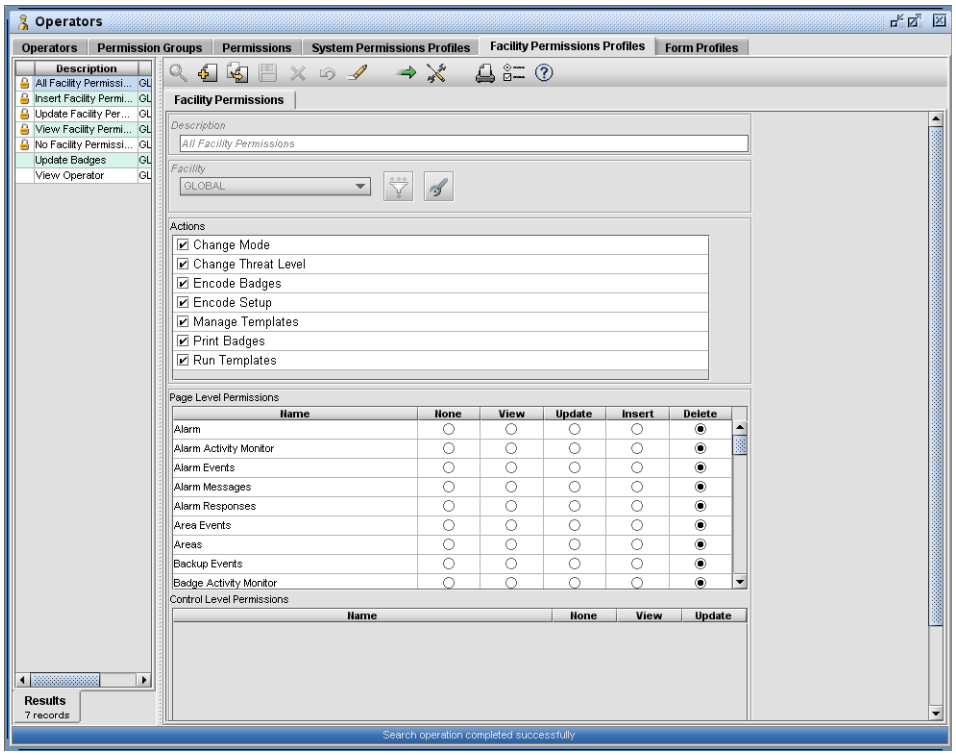
Creating facility permission profiles

A facility permission profile is a way of defining an operator's record and field level access permissions for the Picture Perfect forms that are partitioned by facility. It defines, for each facility, what the operator can do with records assigned to that facility.

Example

When the All Facility Permissions facility profile is assigned to the Global facility and assigned to an operator, the operator has access to all database records in the Global facility only. The term "Global" defines a default facility; it does not encompass other facilities.

Figure 29. Facility Permissions Profile form



Default facility permission profiles are created during installation and, when paired with a facility, give an operator varying levels of access to the associated database records, as referenced in *Table 38*.

This feature allows an administrator to grant an operator a different level of permission for each set of records (Facility) to which he has access. For example, an operator may be assigned the facility permission profile, *All Facility Permissions*, at the one facility which allows full access or the ability to view, update, insert, and delete at the record level on all Picture Perfect forms. Full access also grants view and update permission at the field level. At another facility, that same operator may be assigned the *No Facility Permissions*, which does not allow the operator any access to the records at all.

Table 38. Default Facility Permissions profiles

Profile:	No	View	Update	Insert	All
Page (Form) Permission					
Delete					✓
Insert				✓	✓
Update			✓	✓	✓
View		✓	✓	✓	✓
None					
Action Permission					
Manage Template					✓

Table 38. Default Facility Permissions profiles

Profile:	No	View	Update	Insert	All
Run Template					✓
Change Mode					✓

Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 39. Facility Permission Profile form fields

Field name	Description	
Description	Enter a description (up to 60 characters). This description will appear in the Facility list box of the Permission form.	
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.	
Actions	This section can be used to restrict or enable actions that affect Picture Perfect forms globally, such as:	
	Change Mode	Clicking this box enables the Change Mode feature for this operator. See *Changing modes by command* on page 196 for more information.
	Encode Badges	Clicking this box enables the operator to encode smart cards.
	Encode Setup	Clicking this box enables the operator to access the Encoder Setup button.
	Manage Templates	Clicking this box allows the operator to manage templates. See *Chapter 17 User interface customization* for more information.
	Print Badges	Clicking this box enables the operator to print badges if the optional Imaging package is installed. See *Printing badges* on page 242 for more information.
	Run Templates	Clicking this box allows the operator to run templates. See *Chapter 17 User interface customization* for more information.

Table 39. Facility Permission Profile form fields (continued)

Field name	Description	
Page Level Permission	This section is used to set up the record level permissions for the selected form. The toggle buttons allow you to determine the level of permission of the operator assigned to this facility permission profile. Some of these buttons affect the control (field) level permissions. *Example: If the Page Level Permission for Update is toggled off, the Control Level Permission: Update column will be cleared and unavailable for selection.*	
	Name	The labels displayed correspond to the Picture Perfect forms. Select the one you currently want to work with. *Example: Badges* Select the appropriate None, View, Update, Insert, or Delete radio button for each form. If None is selected, the form will not be available to the operator.
	None	Used to determine if the operator will be allowed access to the selected form. If selected, the Control Level Permission: None column will be activated.
	View	Used to determine if the operator will be allowed to view a record associated with the selected form. If selected, the Control Level Permission: View column is selected by default.
	Update	Used to determine if the operator will be allowed to update a record associated with the selected form. If selected, the Control Level Permission: Update column is selected by default.
	Insert	Used to determine if the operator will be allowed to insert or add a record using the selected form. If selected, the Control Level Permission: Insert columns will be selected by default.
	Delete	Used to determine if the operator will be allowed to delete a record using the selected form. If selected, the Control Level Permission: Delete columns will be selected by default.
Control Level Permission	This section is used to set up the field level permissions. This window becomes active with data when a form has been selected from the Page Level Permission section. The data in the Control Level Permission window is shown in three columns: None, View, and Update. This window should be used to set the field level permissions for the selected form by selecting one of the columns.	
	Name	This column contains the field description of each of the fields that can be selected.
	None	This column determines if the field displays on the selected form.
	VIew	This column determines if the data in this field is viewable on the selected form. The Page Level Permission: View, Update, Insert, or Delete must be selected for this column to be active.
	Update	This column determines if the field can be edited or not from the selected form. The Page Level Permission: Update, Insert, or Delete button must be selected for this column to be active.

Related procedures

To create, edit, or delete a Facility Permission Profile record:

1. Select **Control**, **Operators**, and then **Facility Permission Profile** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Creating system permission profiles

A system permission profile is a way of defining an operator's record and field level access permissions for Picture Perfect forms that are not partitioned by facility, such as the System Parameters or the Facility form. It also controls the ability to perform certain actions, such as Purging Alarms. See *Table 40*.

Example

For example, **All System Permissions** allows the operator to view, update, insert, and delete records on all non-facility partitioned Picture Perfect forms. It also grants full action permission. **No System Permissions**, on the other hand, does not allow the operator any access to the records at all.

Figure 30. System Permissions Profile form

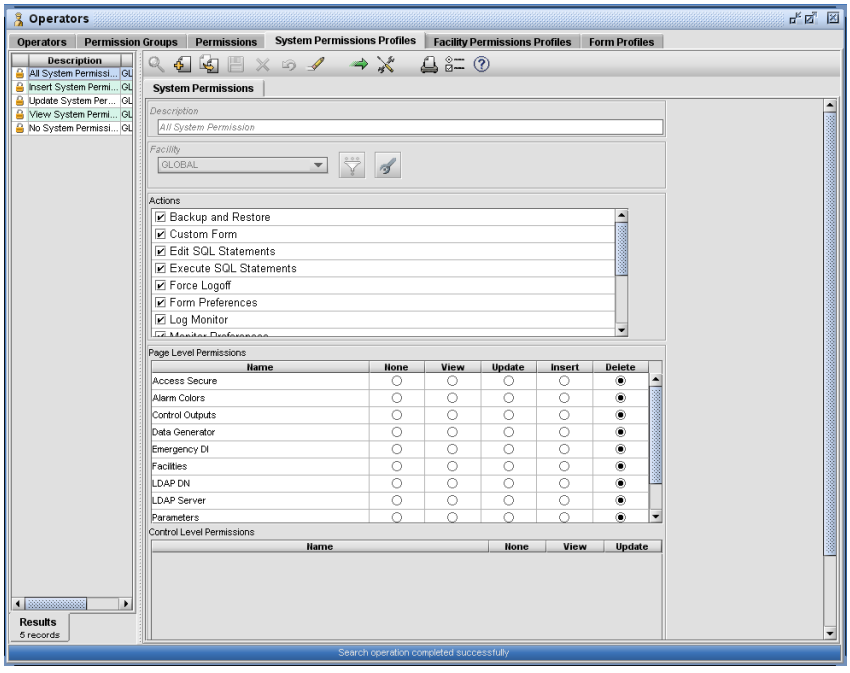


Table 40. Default System Permissions Profiles

Profile:	No	View	Update	Insert	All
Action Permission					
Backup and Restore				✓	✓
Custom Form					✓
Edit SQL Statements			✓	✓	✓
Execute SQL Statements			✓	✓	✓
Force Logoff					✓
Log Monitor			✓	✓	✓
Performance Monitor			✓	✓	✓
Purge All Alarms			✓	✓	✓
Send Message					✓
Status Monitor			✓	✓	✓
Tour Functions			✓	✓	✓
User Monitor			✓	✓	✓
Page (Form) Permission					
Access Secure		✓	✓	✓	✓
Alarm Colors		✓	✓	✓	✓
Control Outputs		✓	✓	✓	✓
Facilities		✓	✓	✓	✓
Parameters		✓	✓	✓	✓

Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 41. System Permission Profile form fields

Field name	Description	
Description	Enter a description (up to 60 characters). This description will appear in the System Permissions Profile list box of the Permission form.	
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.	
Actions	This section can be used to restrict or enable certain actions that are typically performed at a System Administrator level, such as:	
	Backup and Restore	Enables the operator to perform database backup and restore activities. See *Chapter 15 Backup and restore*.
	Custom Forms	Enables the operator to create and edit custom forms. See *Creating and editing custom forms* on page 330.
	Edit or Execute SQL Statements	Enables the operator to create and modify SQL reports. If this is not selected, the operator can only view pre-defined SQL reports. See *Creating and viewing reports* on page 293.
	Force Logoff	Enables the Force Logoff menu item on the User Monitor, which allows the operator to force another operator to log off the system. See *Monitoring users* on page 281.
	Form Preferences	Enables the Preferences button on forms.
	Log Monitor	Enables operator access to the Log Monitor. See *Monitoring log file messages* on page 289.
	Monitor Preferences	Enables the Preferences button on monitors.
	Performance Monitor	Enables operator access to the Performance Monitor. See *Monitoring system performance* on page 286.
	Purge All Alarms	Enables the use of the Purge button on the Alarm monitor. See *Monitoring alarms* on page 264.
	Send Message	Enables the Send Message icon on the User Monitor, which displays the Send Message dialog. This dialog allows the operator to broadcast a message to an individual or to all users. See *Monitoring users* on page 281.
	Status Monitor	Enables operator access to the Status Monitor. See *Monitoring status* on page 280.
	Tour Functions	Enables the operator to perform tour functions such as starting or stopping a tour. See the *Picture Perfect 4.5 Guard Tours User Manual*.
	User Monitor	Enables operator access to the User Monitor. See *Monitoring users* on page 281.

Table 41. System Permission Profile form fields (continued)

Field name	Description	
Page Level Permission	This section is used to set up the record level permissions for the selected form. The toggle buttons allow you to determine the level of permission of the operator assigned to this facility permission profile. Some of these buttons affect the control (field) level permissions. *Example: If the Page Level Permission for Update is toggled off, the Control Level Permission: Update column will be cleared and unavailable for selection.*	
	Name	The labels displayed correspond to the Picture Perfect forms. Select the one you currently want to work with. *Example: Badges* Select the appropriate None, View, Update, Insert, or Delete radio button for each form. If None is selected, the form will not be available to the operator.
	None	Used to determine if the operator will be allowed access to the selected form. If selected, the Control Level Permission: None column will be activated.
	View	Used to determine if the operator will be allowed to view a record associated with the selected form. If selected, the Control Level Permission: View column is selected by default.
	Update	Used to determine if the operator will be allowed to update a record associated with the selected form. If selected, the Control Level Permission: Update column is selected by default.
	Insert	Used to determine if the operator will be allowed to insert or add a record using the selected form. If selected, the Control Level Permission: Insert columns will be selected by default.
	Delete	Used to determine if the operator will be allowed to delete a record using the selected form. If selected, the Control Level Permission: Delete columns will be selected by default.
Control Level Permission	This section is used to set up the field level permissions. This window becomes active with data when a form has been selected from the Page Level Permission section. The data in the Control Level Permission window is shown in three columns: None, View, and Update. This window should be used to set the field level permissions for the selected form by selecting one of the columns.	
	Name	This column contains the field description of each of the fields that can be selected.
	None	This column determines if the field displays on the selected form.
	VIew	This column determines if the data in this field is viewable on the selected form. The Page Level Permission: View, Update, Insert, or Delete must be selected for this column to be active.
	Update	This column determines if the field can be edited or not from the selected form. The Page Level Permission: Update, Insert, or Delete button must be selected for this column to be active.

Related procedures

To create, edit, or delete a System Permission Profile record:

1. Select **Control**, **Operators**, and then **System Permissions Profile** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

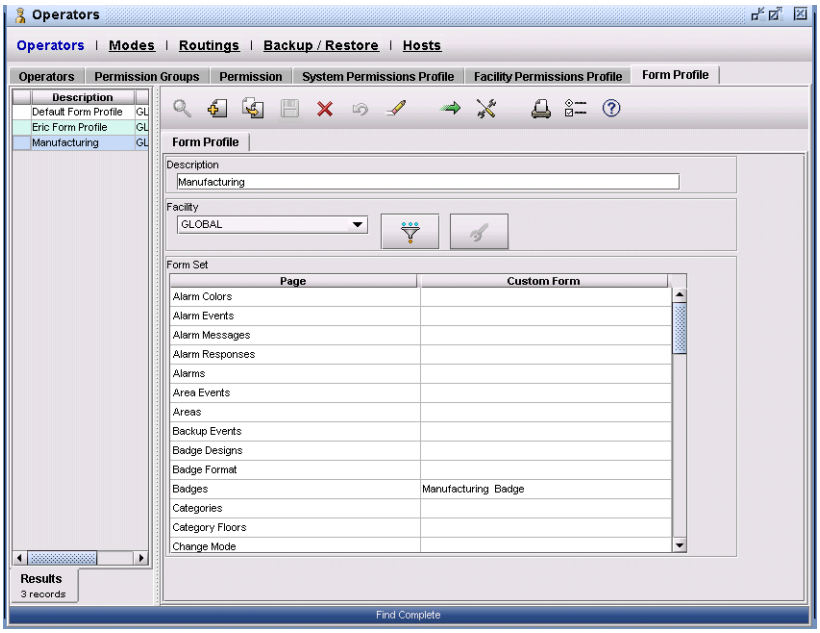
Creating form profiles

A form profile is a way of associating custom forms with an operator's permission. Each Picture Perfect form can have multiple custom forms that display different fields. One operator may need access to different fields than another operator. By assigning a Form Profile to a permission, you can have specific fields display on the various forms when an operator with that permission accesses them.

Example

Jane Doe is responsible for issuing badges to the Manufacturing personnel. She is assigned a Form Profile that displays a custom badge form designed specifically for Manufacturing.

Figure 31. Form Profile Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 42. Form Profile fields

Field name	Description
Description	Enter a description (up to 60 characters). This description will appear in the Form Profile list box of the Permission form.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Form Set	Page: The Picture Perfect form such as, Badges. Custom Form: The custom form that you want to display when the operator accesses the Picture Perfect form.

Related procedures

To create, edit, or delete a Form Profile record:

1. Select **Control**, **Operators**, and then **Form Profile** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Setting up permission groups

Another step in restricting operator access is by defining permission groups, which are assigned to areas, categories, and reports.

Note: Permission Groups are not groups of permissions. They are simply a way of grouping areas, categories, and reports to restrict access by operators.

There are two types of permission groups: Area/Category and Report.

- An Area/Category permission group defines the categories and areas that an operator is permitted to assign. The system requires at least one permission group, in addition to the default permission group: All Groups Allowed. The All Groups Allowed permission group gives an operator full access to all Category groups and all Area groups. Each permission group created with the Area/Category type, will appear on both the Area Permission Group and Category Permission Group list boxes of the Permissions form along with the default All Groups Allowed.
- A Report Permission Group can be assigned to reports if the Enforce Report Permissions option is enabled through the System Parameters form. This offers the capability to assign reports to report permission groups and to restrict operator report access to only those reports that the operator permission record specifies. The All Groups Allowed permission group gives an operator full access to all Report Groups. Each permission group created with the Report type will appear on the Report Permission Group list box of the Permissions form along with the default All Groups Allowed.

Use the Permission Groups form to divide responsibilities among operators by creating a separate permission group for each group of categories and/or areas. For example: Building 1, Building 2, Building 3. Then remove the special permission group, All Groups Allowed, and assign one or more of the newly created permission groups. An operator can have permission to assign up to 20 category and area groups and, if enabled, 5 report groups.

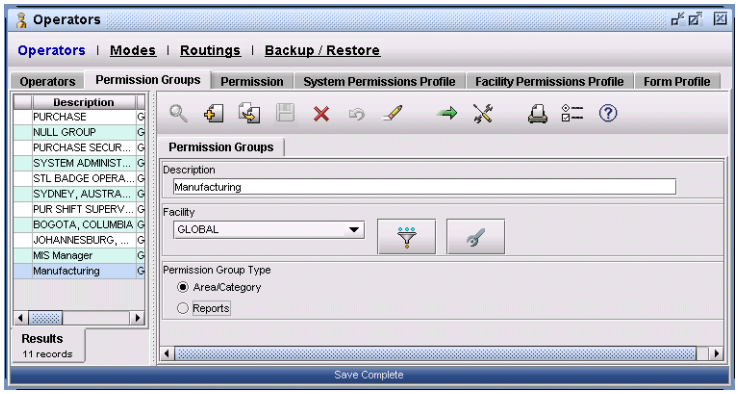
Figure 32. Relationship Between Permissions and Permission Groups

Example

Operator Jane Doe works in a facility made up of two buildings. The personnel working in this facility are divided into different categories, such as Manufacturing, General Access, High Security, Maintenance, Executive staff. Jane is responsible for issuing badges to the Manufacturing personnel in both buildings. She is assigned the permission, Badge Administrator. This permission is assigned to the Area/Cat Manufacturing permission group, which restricts badge-issue functions to those records in that permission group; no permission is granted to issue badges for other permission groups.

If your site does not require this kind of operator restrictions, use the default permission group All Groups Allowed. For example, a Badge Administrator permission can be assigned the permission group All Groups Allowed which gives this operator permission to issue badges to all area and category permission groups without restrictions.

Figure 33. Permission Groups Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 43. Permission Groups form fields

Field name	Description
Description	Type a description to identify the area, category, or report type permission group (0 to 60 characters). *Example: Manufacturing.*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Permission Group Type	• Area/Category Select the Area/Category radio button if the permission group is to be used to control the categories and areas that an operator is permitted to assign. • Reports A Report permission group can be assigned to reports if the Enforce Report permissions option is enabled through the System Parameters form. Select the Reports radio button if the permission group is to be used to restrict operator report access to only those reports that the operator permission record specifies.

Related procedures

To create, edit, or delete a Permission Group record:

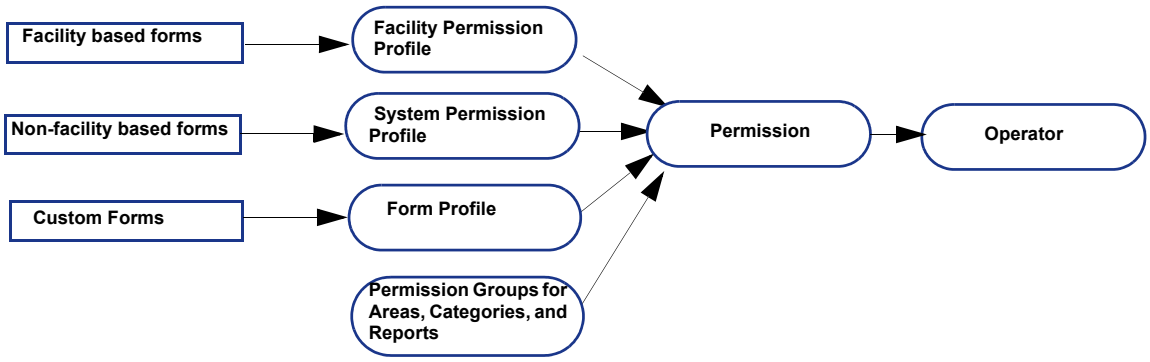
1. Select **Control**, **Operators**, and then **Permission Groups** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Setting up permissions

Use the Permissions form to define the functions that each operator level is permitted to perform, such as System Administrator, Badge Administrator, or Alarm Operator. That permission can then be assigned to individual operators from a list box.

By default, the system provides the permission of System Administrator. This permission should be assigned to one or more operators who have total responsibility for the Picture Perfect system and therefore require all functions.

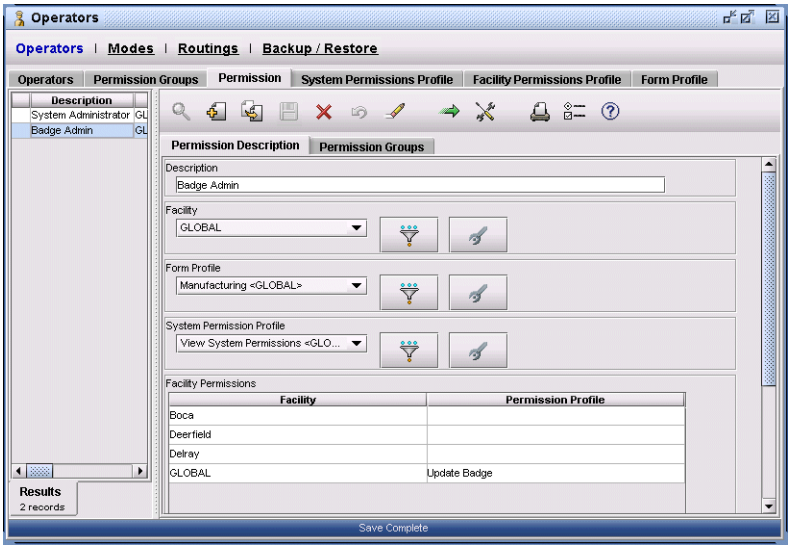
Figure 34. Relationship Between Permissions, Profiles, and Permission Groups



Example

Operator Jane Doe is responsible for issuing badges to the Manufacturing plant in the Global facility. She is assigned the permission Badge Admin. The Badge Admin permission is assigned the Form Profile: *Manufacturing* that has a custom Badge form, the System Permission Profile: View *System Permissions*, and the Facility Permission Profile: *Update Badges* that grants update permission on the Badges form only.

Figure 35. Permission Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 44. Permissions form fields

Field name	Description
Description	The job description of the operators that will be assigned to this permission (1 to 60 characters). *Example: Badge Administrator*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Form Profile	Controls the custom forms that display for an operator with this permission.
System Permissions Profile	Controls the level of access the operator has to the Picture Perfect forms that are not controlled by Facilities, such as the Facility and the System Parameter forms.
Facility Permissions	Controls the level of access the operator has to the Picture Perfect forms that are controlled by Facilities, such as Doors, Readers, and the majority of the Picture Perfect forms. This window displays the facilities currently defined. If the facility has an associated profile, that profile description will appear after it. Select a facility and click on it to display a facility profile list box. If you want to assign a facility profile to this facility, select a profile from the list. **Note:** In addition to any other facility permissions, all users should have access to the Global facility in order to properly use the system.
Category Permission Group	List of permission groups used with categories. Select the permission groups that designate categories this operator permission is allowed to assign to areas and badges. You can select up to 20 Category Permission Groups, or All Groups Allowed which gives operators of this group access to all categories. A category cannot be assigned or removed from an area or badge if that category's permission group is not assigned here.
Area Permission Group	List of permission groups used with areas. Select the permission groups that designate areas this operator permission is allowed to assign to readers and doors. You can select up to 20 Area Permission Groups, or All Groups Allowed which gives operators of this group access to all areas. An area cannot be assigned or removed from a reader or door if that area's permission group is not assigned here.
Report Permission Group	If enforcement of report permissions is enabled, the Report Permission Group button is available and will display a list of permission groups used with PPSQL reports. Only those operators with a permission that has a report permission group selected that matches the report permission group assigned to a certain PPSQL report, may access that report. The selection of All Groups Allowed gives an operator of this permission access to all PPSQL reports. Up to 5 report permission groups may be assigned.

Related procedures

To create, edit, or delete a Permission record:

1. Select **Control**, **Operators**, and then **Permissions** tab.

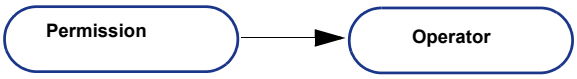
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Defining operators

Use the Operators form to assign operator permissions to individual operators and to give them login capabilities on the system.

Note: Always have more than one operator with System Administrator permissions.

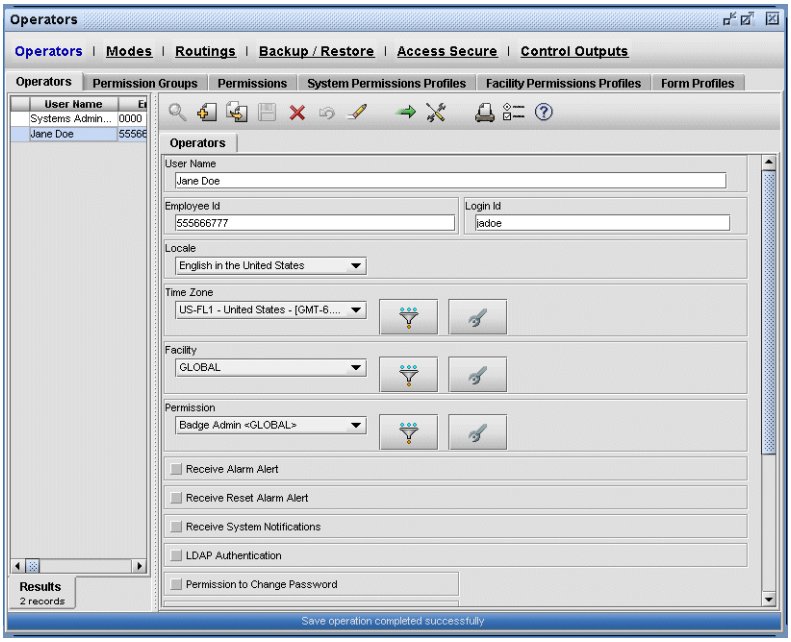
Figure 36. Relationship Between Permissions and Operators



Example

Jane Doe is the badge administrator at the manufacturing plant of Global Corporation. Her employee identification number is *555666777* and her Login Id is *jadoe*. She is assigned the permission *Badge Admin*.

Figure 37. Operator Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 45. Operator form fields

Field name	Description
User Name	Description of the person using the Login ID (1 to 12 characters).
Employee Id	Company identification number assigned to the person using the Login ID.
Login Id	Login name the user types to gain access to the operating system and Picture Perfect. Each operator must have a unique Login ID. The Login ID is case sensitive.
Locale	The locale used by this operator. The list box is created at system installation based on available locales. A locale is a language for a specified region. *Example: English in the United States, Portuguese in Brazil*
Time Zone	Select, from the drop-down list, the time zone in which the operator is located. This allows Picture Perfect to display badge and alarm activity in the operator's local time. See *Verifying time zones* on page 168. **Note:** In order for an operator to use this field, they must have at least *View* page level permission for the Time Zone form. See *Creating facility permission profiles* on page 81.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Permission	The functions the operator can perform. *Example: System Administrator* This list box reflects the permissions created with the Permissions form.
Receive Alarm Alert	Select if this operator is to receive Alarm Alert messages.
Receive Reset Alarm Alert	Select is this operator is to receive Reset Alarm messages.
Receive System Notifications	Select if this operator is to receive System Notification messages.
LDAP Authentication	Select to enable LDAP authentication. See *Configuring LDAP support* on page 50.
Permission to Change Password	Select to allow this operator to change their password. If this option is not selected, the password can only be changed by the System Administrator.
Change Password on Next Login	Select to force this operator to change their password the next time they log on to the system.
Password Expiration	• **Password Never Expires:** If checked, the password has no expiration date. • **Expires in (days):** From the list of values in the drop-down list, select the frequency at which the password should expire. • **Warn prior to Expiration (days):** Enter a numeric value (less than that specified in Expires in) that represents the number of days prior to expiration that the operator should receive a warning message. The warning message includes the number of days before the password expires. If the operator has permission to change their password, they are prompted to change it. If they do not have permission to change their password, they are prompted to contact their System Administrator.

Table 45. Operator form fields (continued)

Field name	Description
Idle Session Time	The amount of time, in minutes, during which there is no operator activity after which the system will attempt to log the operator off. Operator activity can be mouse movements, button clicks, or keystrokes. The default value of 0 indicates no session timeout is enforced. The maximum value is 17800 minutes.
Change Password	Displays the Password dialog used to set the operator's password. The * character displays as you type; the actual password is not visible. When changing an existing password, the old password must be entered before being prompted to enter the new one. A text box lists the password rules that must be followed, according to the parameters specified in the Parameters form. **Notes:** • This dialog is not available if the operator does not have permission to change their password. • When adding a new operator, you must enter a password before saving the record. • Passwords are restricted to contain only 7-bit ASCII characters such as: a-z, A-Z, 0-9. Foreign language characters such as: à, ê, æ, cannot be used within passwords.

Related procedures

To create, edit, or delete an Operator record:

1. Select **Control**, **Operators**, and then **Operators** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Linking facilities, facility profiles, permissions, and operators

Examples:

Table 46. Examples of Operator/Permission/Profile/Facility relationship

Operator	Permission	Profile	Facility	Result
install	System Administrator (responsible for the system administrative functions for the entire system)	All Facility/System (allows full access on all forms)	Global	This combination allows operator, install, to perform all functions on all records assigned to the Global Facility on all forms.
		All Facility/System (allows full access on all forms)	Facility X	This combination allows operator, install, to perform all functions on all records assigned to Facility X on all forms.
		All Facility/System (allows full access on all forms)	Facility Y	This combination allows operator, install, to perform all functions on all records assigned to Facility Y on all forms.
		All Facility/System (allows full access on all forms)	Facility Z	This combination allows operator, install, to perform all functions on all records assigned to Facility Z on all forms.
John Smith	Site Administrator (responsible for the system administrative functions for Facility X)	Update (allows update access on all forms)	Facility X	This combination allows operator, John Smith, to perform update functions on all records assigned to Facility X on all forms.
		View (allows View only access on all forms)	Global	This combination allows operator, John Smith, to view all records assigned to the Global facility on all forms.
Jane Doe	Badge Administrator	Update Badges (allows update access to records on the Badges form)	Global	This combination allows operator, Jane Doe, to update all records assigned to the Global Facility on the Badges form.
		View Operator (allows view access to records on the Operator form)	Global	This combination allows operator, Jane Doe, to view all records assigned to the Global Facility on the Operator form.

To link facilities, profiles, permissions, and operators:

1. Define the facilities in your system, using the Facility form to describe the group of records. *Example: Facility X, Facility Y, and Facility Z.*

   Note: If your system consists of a single facility, you do not need to create additional facility records.

2. Define facility and system profiles, using the Facility Permission Profile form and the System Permission Profile form to describe the level of access the operator will have.
   Example: Full access, View only, Insert only, or Monitor.
3. Define the permission records required, using the Permissions form to describe what function the operator will perform.
   Example: System Administrator, Site Administrator, Badge Administrator, or Guard.

   Then, assign a facility profile to the permission for each facility required. You can assign the same facility profile to multiple facilities and permission records.
   Example: You could assign the Monitor facility profile to a Guard permission in Facility X and Facility Y as well as to a Badge Administrator in Facility Z.
4. Assign the permission to an operator, using the Operator form.
   Example: An operator may be assigned as a Guard at Facility X with a Monitor profile and at Facility Y with a Full access profile.

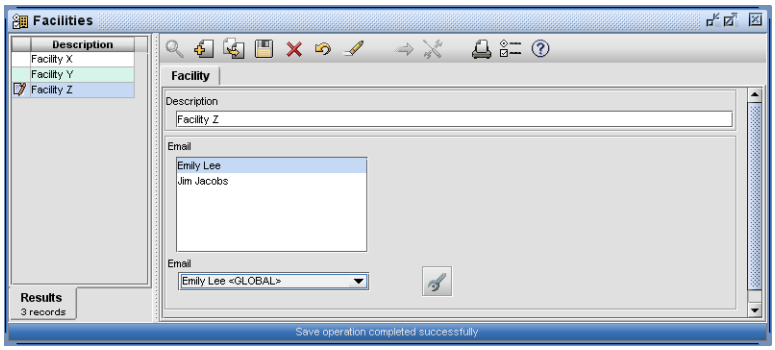
On the following pages we will perform the steps necessary to achieve the following result for operator, Mary Smith,

Mary Smith	Badge Administrator	Update Badges (allows update access to records on the Badges form)	Facility X	This combination allows operator, Mary Smith, to update all records assigned to Facility Y on the Badges form.
		View Operator (allows view access to records on the Operator form)	Global	This combination allows operator, Mary Smith, to view all records assigned to the Global Facility on the Operator form.

Step 1. Define Facilities

1. From the **Configuration** menu, select **Facilities, and then** the **Facilities** tab.
2. From the toolbar, click **Add** .
3. In the **Description** field, enter a unique text description. *Example: Facility X.*
4. From the toolbar, click **Save** .
5. Repeat step 3 and step 4 for *Facility Y* and *Facility Z.*
6. The Facility records will look similar to the following:

Figure 38. Defining Facilities



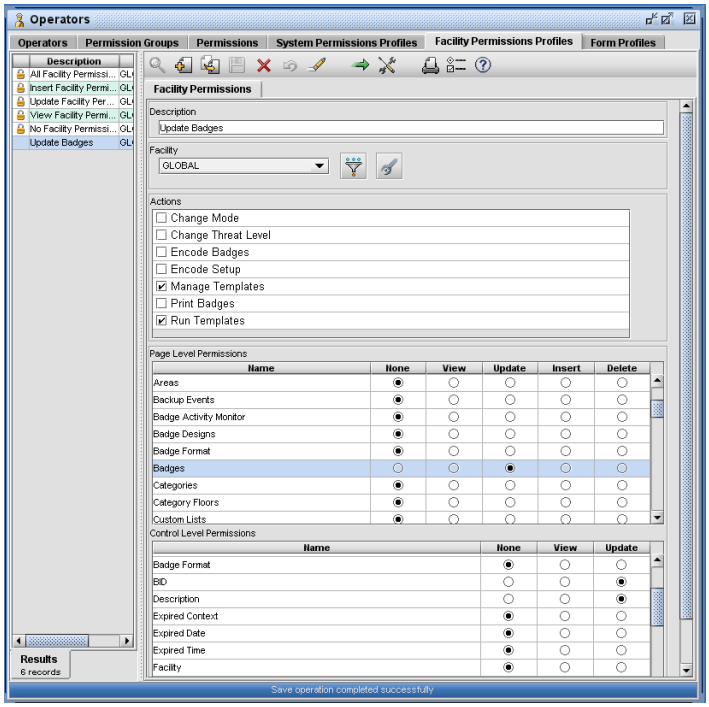
Step 2. Defining Facility Profiles

To create the Update Badges facility profile:

1. From the **Control** menu, select **Operators, and then** the **Facility Permission Profile** tab.
2. From the toolbar, click **Add** .
3. In the **Description** field, type: *Update Badges*
4. From the list of forms in the **Page Level Permissions** pane, select *Badges* and click *Update.*
5. To set the desired **Control Level permissions**, click *Update* for all the fields you want the operator to be able to edit.
6. From the toolbar, click **Save** .

   The *Update Badges* facility permission profile record will look similar to the following.

Figure 39. Defining a facility profile

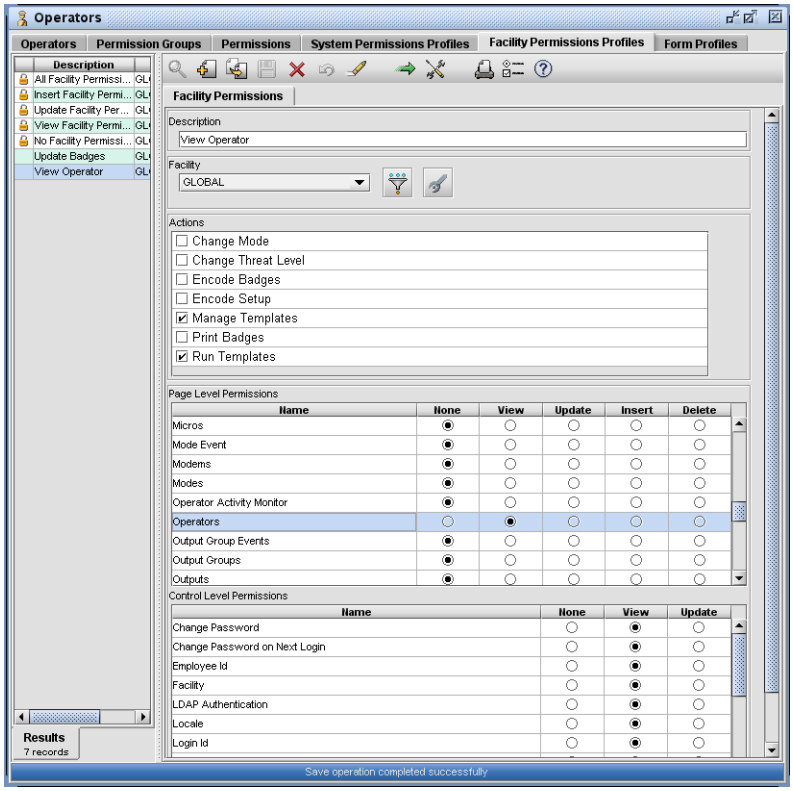


To create the View Operator facility profile:

1. From the **Control** menu, select **Operators, and then** the **Facility Permission Profile** tab.
2. From the toolbar, click **Add** .
3. In the **Description** field, type: *View Operator*
4. From the list of forms in the **Page Level Permissions** pane, select *Operator* and click *View.*
5. To set the desired **Control Level permissions**, click *View* for all the fields you want the operator to be able to see.
6. From the toolbar, click **Save** .

The *View Operator* facility profile record will look similar to the following.

Figure 40. Defining a facility profile



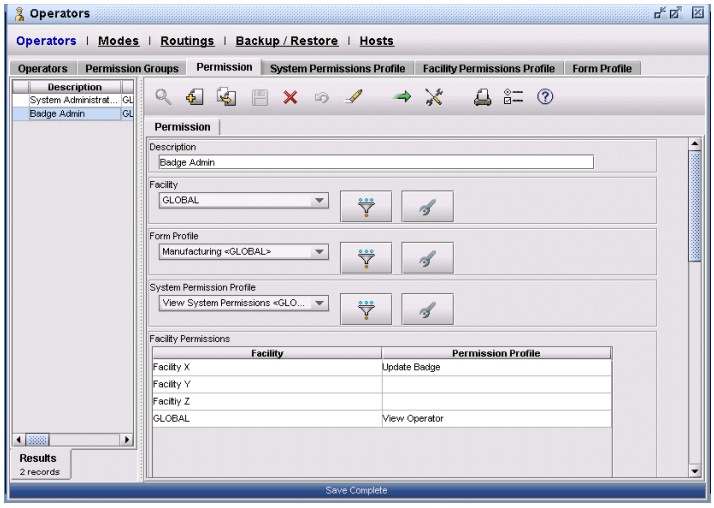
Step 3. Defining Permissions and Assigning a Facility Profile

1. From the **Control** menu, select **Operators, and then** the **Permission** tab.
2. From the toolbar, click **Add** .
3. In the **Description** field, type: *Badge Administrator*
4. Click **Facility** and select: *Global*
5. Under Facility Permissions, from the list of facilities, select *Facility X* and click in the adjacent Permission Profile cell.

   A list of the defined facility profile records displays.
6. From the list, select: *Update Badge.*
7. Repeat step 5 and step 6, substituting *Global* in step 5 and *View: Operator* in step 6.
8. From the toolbar, click **Save** .

   In the Facility Permissions pane, the Permission Profile column will reflect the newly selected profile. In our example, the Badge Admin permission record will now look like this:

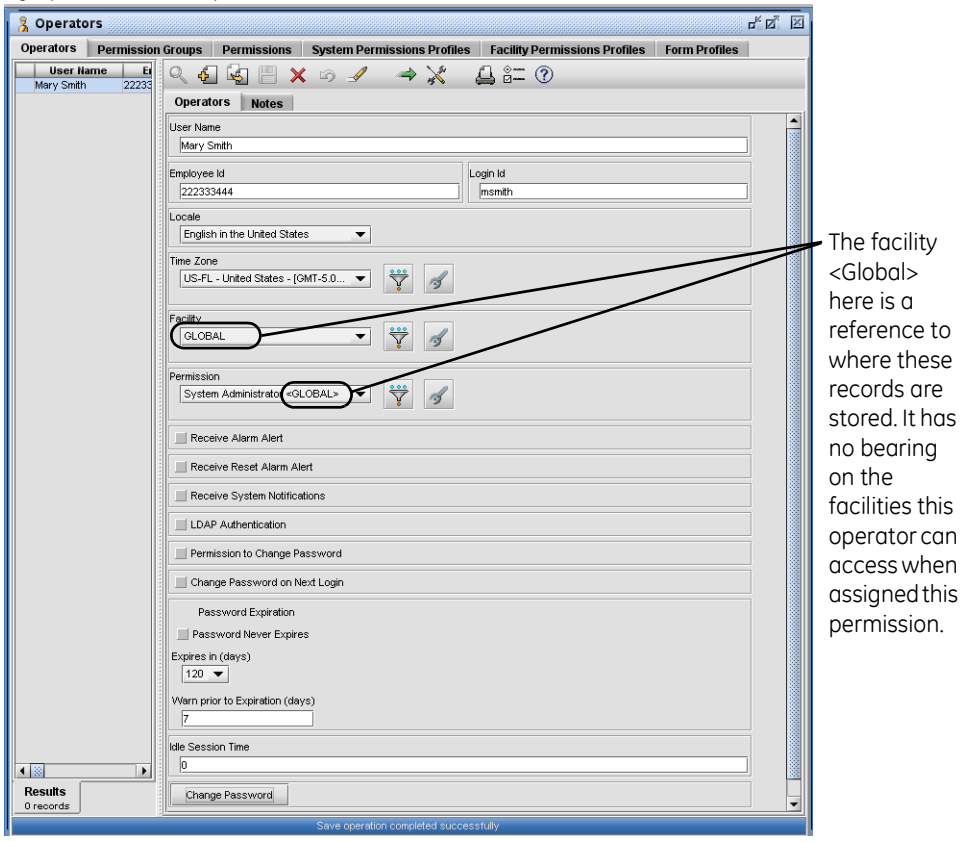
Figure 41. Defining a permission



Step 4. Assign the Permission to an Operator

1. From the **Control** menu, select **Operators, and then** the **Operators** tab.
2. From the toolbar, click **Add** .
3. In the **User Name** field, type: *Mary Smith*
4. In the **Employee ID** field, type: *222333444*
5. In the **Login Id** field, type: *msmith*
6. Click the **Permission** button and select: *Badge Administrator<GLOBAL>*
7. Click the **Locale** button and select: *English in US*
8. Click the **Time Zone** button and select: *US-FL-United States-Florida*
9. Click **Facility** and select: *Global*

Figure 42. Assigning a permission to an operator



10. Click **Change Password** and set a password for this operator.
11. Click **Ok** to return to the **Operators** form.
12. From the toolbar, click **Save** .

The operator, *Mary Smith*, has the permission of *Badge Administrator*, which allows her to update all badge records assigned to Facility X and to view all operator records assigned to the Global facility.

When *Mary Smith* logs on to Picture Perfect:

- If she selects *Facility X* from the Facility Manager, she will have access to the *Badges* records assigned to Facility X:

- If she selects *Global* from the Facility Manager, she will have access to the *Operators* records assigned to the Global facility:

- If she clicks *Select All*, she will have access to the *Badges* records assigned to Facility X and the *Operators* records assigned to the Global facility:

- Depending on the System Permission Profile assigned, there may be other menu options (those not partitioned by facility) available, such as the following:

Chapter 7 Alarm/activity configuration

This chapter describes how to configure alarm and activity messages, how to define alarms, and how to control the way they display on the monitors. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Alarms overview

Alarms are used to notify an operator of an exceptional condition by displaying the information on one or more monitors. The alarm display can be configured to include what caused the alarm, the action required, the alarm priority, the way it looks on the screen, as well as the operators by whom it will be viewed.

The Picture Perfect system monitors digital inputs (DIs), such as sensors or contacts, for alarm conditions and then activates digital outputs (DOs), such as horns or lights, as alarms and output devices. The system notifies the operator of alarms using pop-up windows, and in a scrolling window called the Alarm Monitor.

When an alarm occurs, the system beeps and displays a pop-up window that notifies the operator. The operator then displays alarm instructions by selecting the alarm from a scrolling list on the Alarm Monitor. The operator records a response to an alarm either by selecting a pre-written alarm response from the Alarm Response window or by typing a response.

Alarm/activity routing overview

The Picture Perfect administrator may configure the system so that one set of alarms and activity is routed to a given operator while another set of alarms and activity is routed to another operator. This allows Picture Perfect operators to monitor alarms and activity that affect their own areas.

It should also be noted that activity routing is restricted to badge activity and digital input (DI) activity. Other activity, such as operator activity, cannot be routed to a specific operator.

To route all alarms and activity to all operators:

1. Define alarm routings, that describe where messages are sent. See *Defining routings* on page 107.
2. Assign a routing to each alarm. See *Defining alarms* on page 117.

To restrict the display of alarms and activity to specific operators:

1. Define alarm routings, that describe where messages are sent. See *Defining routings* on page 107.
2. Create route definition records, that generally correspond to an area of your site, such as a building. See *Creating route definitions* on page 109.
3. Create and schedule route point records, that indicate the operators and when the alarms and activity are routed. See *Defining route points* on page 110.
4. Assign a route definition and an alarm routing to each alarm. See *Defining alarms* on page 117.

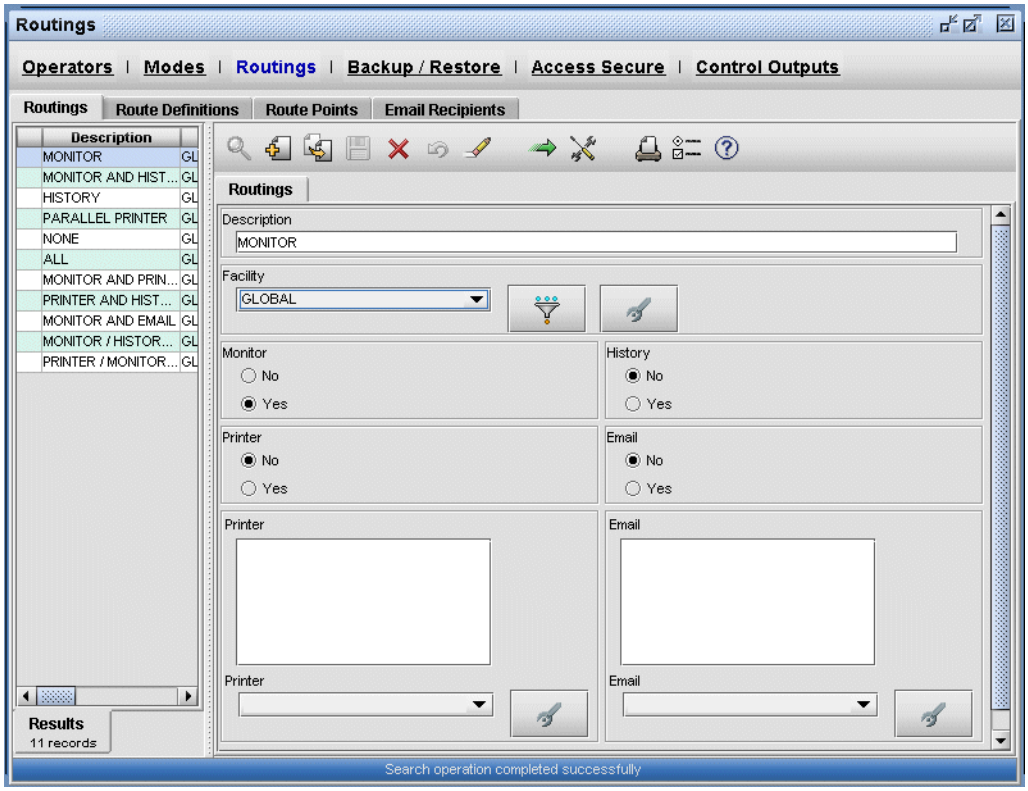
Defining routings

Use the Routings form to define where messages are to be sent. There are eleven predefined routings already entered. The system lets you use these routings to send messages to a printer, history log, e-mail, and/or to the monitor. The routings you create populate list boxes that are used in various aspects of the system.

Example

The ABC Corporation is comprised of a single facility, Global. Therefore they use the default routings supplied with the system.

Figure 43. Routings Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 47. Routing form fields

Field name	Description
Description	Type a description (0 to 60 characters) to identify the type of messages to be routed. *Example: Badge Activity, Operator Messages, Overnight Messages, or ALL* A single routing description can include multiple routing destinations. *Example: You may want messages received overnight to be routed to the printer, the monitor, and the history log.*
Printer	Select Yes to select a printer as a destination where you want messages to be routed. From the Printer drop-down list, select the specific printer queue.
Monitor	Select Yes to display the message on the alarm and activity monitor; this choice does not create a history record. **Note:** Monitor must be selected as a routing destination in order for an operator to respond to an alarm.
History	Select Yes to record the transaction message in the database history table; this allows the message to be referenced for history reporting.
Email	Select Yes to route messages to an email address or alias. The e-mail drop-down list contains all of the email addresses currently defined in the system. Select the desired addresses from the list box. **Note:** Yes must be selected for Monitor in order for this feature to be enabled.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete a Routing record:

1. Select **Control**, **Routings**, and then **Routing** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Creating route definitions

This feature can be used, in conjunction with route points, if you want to restrict the display of alarms and activity. If you want all alarms and activity to be displayed for all operators, you do not need to configure this feature. Note also that activity routing is restricted to badge activity and digital input (DI) activity. Other activity, such as operator activity, cannot be routed to a specific operator.

Your site should be partitioned into sections that represent various sets of alarms and activity (inputs, input groups, output devices, and alarm priorities). A route definition corresponds to one section of your Picture Perfect site.

For example, assume a Picture Perfect site consists of two buildings: Building A and Building B. In each of these buildings, there is an operator at an alarm monitoring station: Operator A and Operator B. During the day, two operators monitor the site; one operator in Building A, and one operator in Building B. At night, only one operator monitors the site from Building A.

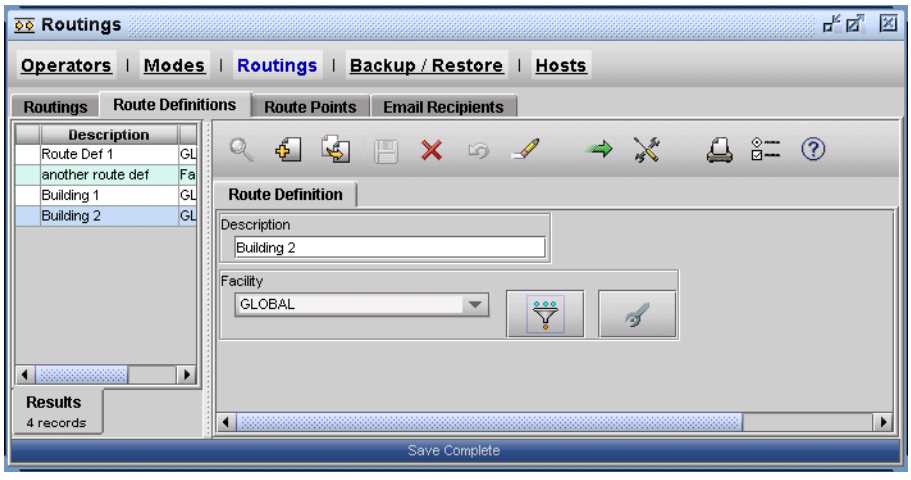
One possible configuration could be that the day shift operators monitor alarms and activity that occur in their respective building, and the night shift operator would monitor alarms and activity that occur in both buildings. This configuration could be extended such that, during the day, if an operator did not respond to an alarm in his building, the alarm would be "bumped" to the operator in the other building.

Note: Changes made to route points will not take effect until Picture Perfect is restarted.

Example

The ABC Corporation is comprised of a single facility, Global. This facility is made up of two buildings: Buildings 1 and 2 and the route definitions are defined as “Building 1” and “Building 2”.

Figure 44. Route Definition Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 48. Route Definition form fields

Field name	Description
Description	Enter a description (up to 60 characters). This description will appear in the Route Definition list box of the Route Points, Alarms, Inputs, and Areas forms.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete a Route Definition record:

1. Select **Control**, **Routings**, and then **Route Definitions** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Defining route points

A route point, assigned to a route definition, indicates to whom and when alarms and activity are routed. A route point can also indicate which alarms are bumped and when they are bumped. A route point belongs to only one route definition, but several route points can belong to the same route definition.

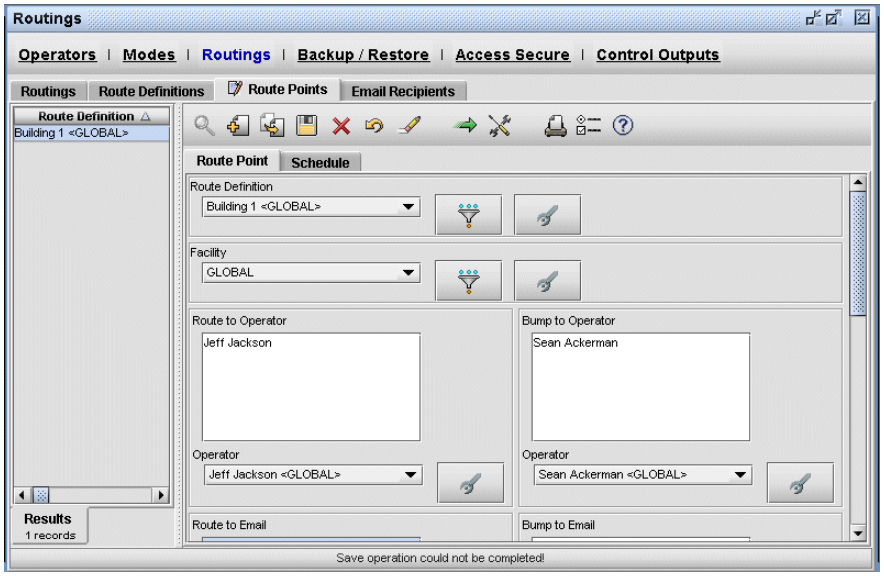
Example

The Global facility is made up of two buildings: Buildings 1 and 2 and the route definitions are defined as “Building 1” and “Building 2”.

Jeff Jackson is the guard at Building 1 and Sean Ackerman is the guard at Building 2. They each view the alarm and activity for their respective buildings during the day. A night shift guard, Barry Evans, views alarm and activity for both buildings at night.

During the day, if Jeff does not respond to an alarm in Building 1, the alarm is “bumped” to Sean in Building 2 and vice-versa.

Figure 45. Route Point Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 49. Route Point form fields

Field name	Description
Route Definition	This field identifies the current route point's route definition. Click the Route Definition button to display a list box. Select the desired Route Definition, and then click OK. *Example: Building A*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Route To Operators	This field identifies the operators to whom the message is to be routed. A list of selected operators is displayed. To add an operator to the list, click the arrow on the Operator drop-down list. One or more operators may be selected for this route point. As operators are selected or unselected from the list box, the Route to Operator window is updated. *This is not a required field; however, if no operators are selected, alarms with this route point's route definition cannot be responded to.* This field should be ignored if you are creating a route point that is used only for Activity Monitor routing.
Bump to Operators	This field identifies an alternate operator to use if the message is not responded to within the time specified in Bump Time. A list of selected operators is displayed. To add an operator to the list, click the arrow on the Operator drop-down list. One or more operators may be selected for this route point. As operators are selected or unselected from the list box, the Bump to Operator window is updated. *This is not a required field; however, if no operators are selected, alarms with this route point's route definition will not be bumped.* This field should be ignored if you are creating a route point that is used only for Activity Monitor routing.

Table 49. Route Point form fields (continued)

Field name	Description
Route to Permission	This field specifies the permissions that an operator must have for a message to be routed to this operator. A list of selected permissions is displayed. To add a permission to the list, click the arrow on the Permission drop-down list. One or more permissions may be selected for this route point. As permissions are selected or unselected from the list box, the Route to Permission window is updated. Only operators with the selected permissions will receive activity and alarms that have this route point's route definition assigned. This field should be ignored if you are creating a route point that is used only for Activity Monitor routing.
Bump to Permission	This field identifies an alternate permission to use if the message is not responded to within the time specified in Bump Time. A list of selected permissions is displayed. To add a permission to the list, click the arrow on the Permission drop-down list. One or more permissions may be selected for this route point. As permissions are selected or unselected from the list box, the Bump to Permission window is updated. This field should be ignored if you are creating a route point that is used only for Activity Monitor routing.
Route to Email	This field identifies which email addresses are associated with the route point. A list of selected email addresses is displayed. To add an address to the list, click the arrow on the Email drop-down list. One or more addresses may be selected for this route point. As addresses are selected or unselected from the list box, the Route to Email window is updated. Only operators with the selected email addresses will receive activity and alarms that have this route point assigned. **Note:** The alarm record (Alarm form) must be associated with a routing record (Routing form) that includes e-mail in order to use this feature.
Bump to Email	This field identifies an alternate email address to use if the message is not responded to within the time specified in Bump Time. A list of selected email addresses is displayed. To add an address to the list, click the arrow on the Email drop-down list. One or more addresses may be selected for this route point. As addresses are selected or unselected from the list box, the Bump to Email window is updated. This field should be ignored if you are creating a route point that is used only for Activity Monitor routing. **Note:** The alarm record (Alarm form) must be associated with a routing record (Routing form) that includes e-mail in order to use this feature.
Start Time	This field identifies when a route point becomes enabled. The format of the value entered should conform to the time format in system configuration. To enable a route point 24 hours, set this time to 00:00:01. If this value is blank, the route definition will not be enforced.
Stop Time	This field identifies when a scheduled route point becomes disabled. The format of the value entered should conform to the time format in system configuration. To enable a route point 24 hours, set this time to 23:59:59. If this value is blank, the route definition will not be enforced.
Time Zone	From the drop-down list, select the time zone of one of the following: the host receiving the alarm, the micro from which the alarm originates, or the operator monitoring the alarm. See *Verifying time zones* on page 168. **Note:** In order for an operator to use this field, they must have at least *View* page level permission for the Time Zone form. See *Creating facility permission profiles* on page 81.
Sun - Sat	These toggle buttons indicate what days of the week this route point should be enabled. Select the desired days of the week by clicking the appropriate toggle button. If no days are selected, the route definition will not be enforced.

Table 49. Route Point form fields (continued)

Field name	Description
Bump Time	The value in this field must be in seconds (minimum=1, maximum=86400). The operator has this number of seconds to respond to the alarm before the alarm is bumped to the operators selected in Bump To Operators. This field should be ignored if you are creating a route point that is used only for Activity Monitor Routing. The default value in this field is blank, meaning that there is no bump time.
Mode	This field identifies the system mode of the Global facility under which this route point is valid. Click the Mode button to display the Mode list box. Select the desired Global facility mode, and then click OK. This is not a required field. If this field is blank, the route point is valid for all system modes.
Note: If you are following the setup sequence recommended in *Chapter 3 Configuration checklist*, the Mode list box will only show the default Normal and Holiday modes. See *Creating modes* on page 194 to create your own custom modes; then return to this procedure to assign routing points for that mode.	

Route point rules and restrictions

There may be times when you question whether an alarm should or should not appear on the Alarm Monitor. Since a system configured for Alarm /Activity Monitor Routing may consist of many route points, it is possible for two route points to have conflicting route operators. For example, assume that Route Point A and Route Point B belong to Route Definition A. Route Point A explicitly routes all alarms to no operators, whereas Route Point B explicitly routes all alarms to all operators. In this case, Route Point B has precedence. Because of the many possible combinations of operators, start times, stop times, bump operators, bump times, and modes, it may be confusing as to where an alarm or activity should be routed. The following lists some rules and restrictions that may be used to configure or troubleshoot Alarm/Activity Monitor Routing.

- If there is an operator route conflict between two route points, the route point that displays the alarm has precedence.
- If an alarm is supposed to be bumped to a given operator and two different bump times are given in two different route points for the alarm's route definition, the shortest length of time determines when the alarm is bumped.
- Once an alarm is displayed on an operator's monitor, only the operator can remove it. The disabling of a scheduled route point will not remove an existing alarm from the Alarm Monitor.
- When a scheduled route point is enabled, affected operators are updated immediately. This event may cause alarms that were already in the system to appear on the Alarm Monitor.
- Alarms and activity with no route definitions are sent to all operators and printers/Email addresses on the alarm routing.
- Alarms and activity with a route definition that has no route points defined, are sent to all operators and printers/Email addresses on the alarm routing.
- If a route definition consists of scheduled route points, every time slot throughout the day and week must be accounted for by a scheduled route point. Times that are not accounted for will default to all operators in the system. This means that if a route definition has a scheduled route point from 8:00:00 to 17:00:00, then alarms and activity with that route point's route definition will be routed to only those operators listed in the route point during that time period. But there are two other time periods for which there are no route points: 23:59:00 to 8:00:00 and 17:00:00 to 23:59:00. During these two time periods, alarms and activity with this route definition will be routed to all operators in the system.
- The Alarm Monitor will reflect any changes made to the Alarm Monitor Routing configuration. Database updates will, however, only add entries to the Alarm Monitor; they cannot remove entries.

The Alarm Monitor Routing feature not only affects the Alarm Monitor; it also affects the Alarm Alerts pop-up. The same rules that apply to the Alarm Monitor also apply to the Alarm Alert. It will display only if alarms can be viewed on the Alarm Monitor.

Related procedures

To create, edit, or delete a Route Point record:

1. Select **Control**, **Routings**, and then **Route Points** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

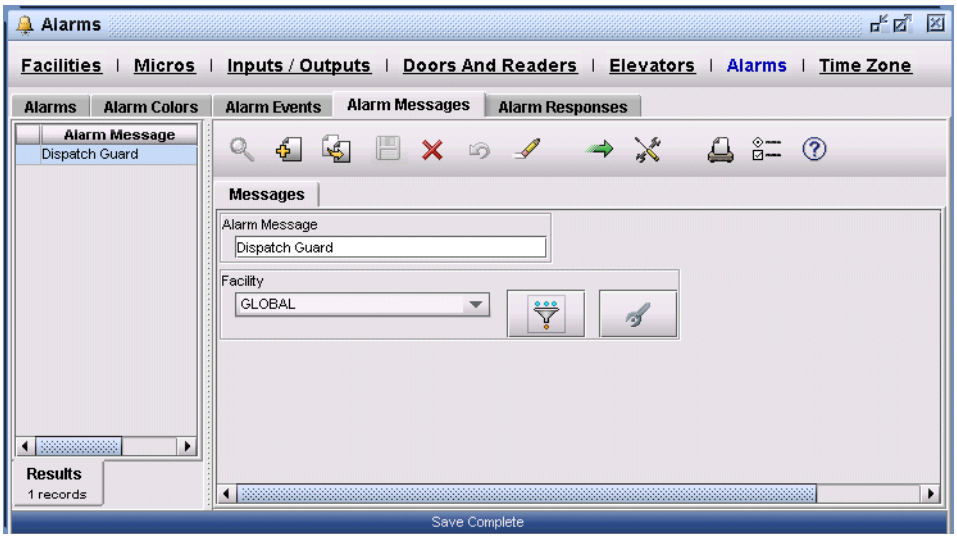
Creating alarm instructions

Use the Alarm Messages form to write instructions that will display when the various alarms occur, and when they reset. Keep in mind that the same alarm may occur at different times of the day or week. Your instructions (who to call, who to dispatch) may change depending on the shift. These alarm messages appear in a list box that is used in the Alarms form.

Example

The policy at Global Corporation is to dispatch a security guard whenever an alarm comes in indicating that a door has been forced open. Therefore, they have created a message that appears on all Door Forced alarms instructing the operator to dispatch a guard.

Figure 46. Alarm Messages Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 50. Alarm Messages form fields

Field name	Description
Alarm Message	Type an alarm instruction for the operator to follow (up to 60 alphanumeric characters). You can assign up to five messages to each alarm. Write generic messages that are common to most of your alarms. *Example: A forced-door alarm on a perimeter door should use a generic alarm instruction such as Forced Door - Send Security Guard, and a response message such as Guard Dispatched.*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete an Alarm Message record:

1. Select **Configuration**, **Alarms**, and then **Alarm Messages** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Creating alarm responses

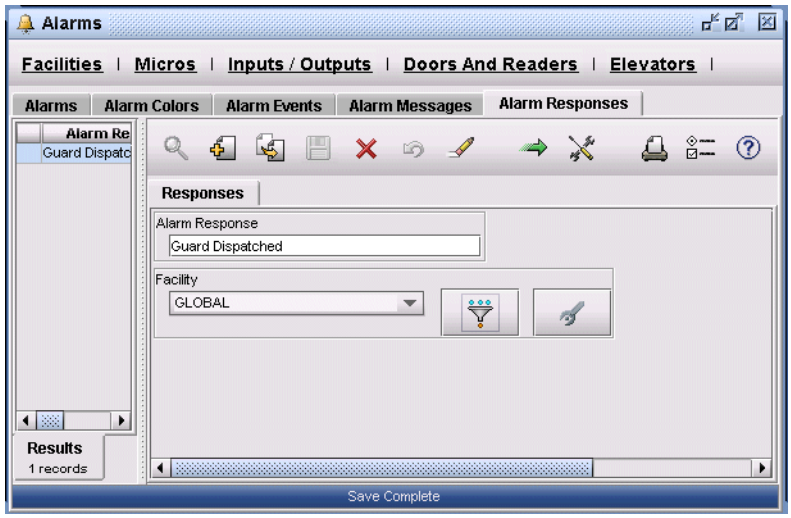
Use the Alarm Responses form to write alarm responses that the operator can select when responding to an alarm. The system allows the operator to enter multiple responses to each alarm.

Create at least one response message that is appropriate for all alarms. *Example: Alarm Acknowledged*.

Example

In keeping with Global Corporation's Door Forced alarm policy, once the operator on duty has dispatched the guard, he selects the response, Guard Dispatched, from the list box on the Alarm Monitor.

Figure 47. Alarm Response Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 51. Alarm Response form fields

Field name	Description
Alarm Response	Type an alarm response for the operator to use (up to 60 alphanumeric characters). These alarm responses appear in a list box that is used when the operator responds to an alarm. When the operator selects a response, the response and the alarm event automatically route to the log. Pre-written responses save time, but if none of the responses on the list box are appropriate, the operator can type a unique alarm response.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete an Alarm Response record:

1. Select **Configuration**, **Alarms**, and then **Alarm Responses** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

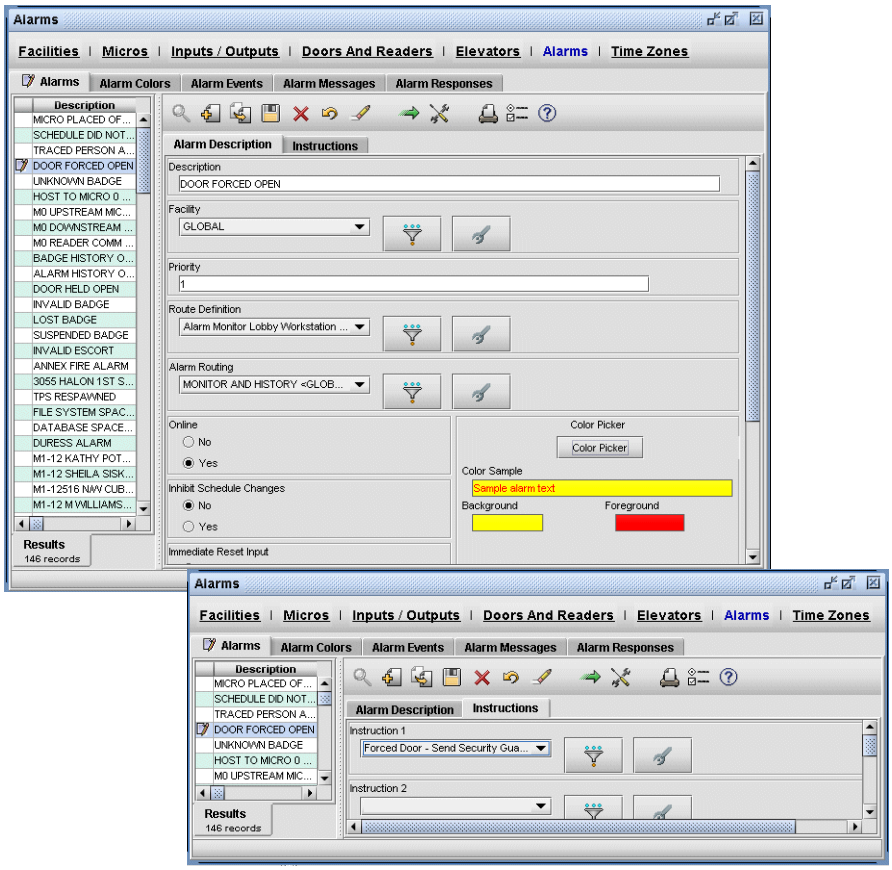
Defining alarms

Use the Alarms form to define each alarm—both physical alarms (such as door forced open) and logical alarms (such as invalid badge). Define the alarm priority, whether or not it can be scheduled, how the alarm inputs and outputs reset, where it is routed, and which alarm instructions display when the alarm occurs. These entries form a list box that is used in the Input Groups form, where alarms are assigned to a specific input group. (See *Input Groups Form* on page 129.)

Example

Ann Davis is the system administrator at Global Corporation and she has defined the Door Forced Open alarm as a priority 1 alarm, to be routed to the Alarm Monitor on the Lobby workstation. The instruction “Forced Door-Send Security Guard” will display in red letters on a yellow background.

Figure 48. Alarms Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 52. Alarms form fields

Tab	Field name	Description
Alarm Description	Description	Type a description for this alarm (up to 30 alphanumeric characters).
	Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
	Priority	Select an alarm priority so that when several alarms occur simultaneously, this alarm displays in order of priority. Highest priority is 1 and lowest is 500. Slide the scroll bar until the number you want to select appears. You may also use the up arrow/down arrow keys to increase or decrease the priority level. One strategy is to leave gaps between the priority numbers so that when you add alarms later, you will not have to re-assign priorities among the existing alarms. The same priority number can be assigned to more than one alarm.
	Route Definition	Click to display the Route Definitions list box. This list box allows the operator to restrict the display of alarms and activity to specific operators. If this field is left blank, this alarm will be routed to all operators.
	Alarm Routing	Click to display the Alarm Routing list box. The monitor should always be included in the routing choice of an alarm. If an alarm is not routed to the monitor, the operator cannot respond to the alarm.
	Online	Toggle this button On if you want this alarm to occur when an associated Input Group is activated. Do not click this button until the alarm is ready to be brought online.
	Inhibit Schedule Changes	Toggle this button On if you want to inhibit schedule changes for this alarm. Otherwise, the system implements alarm schedules created using the Alarm Events form. You may want to inhibit schedule changes for an alarm if no schedules yet exist for alarms, or if you are not ready to implement the schedules you have created.
	Immediate Reset Input	Click Yes if you want the system to reset this alarm as soon as an associated input group triggers this alarm. Logical alarms, such as invalid, suspended, unknown, or lost badges, must have this feature set as there is no reset condition for this type of alarm. Immediate reset allows the operator to remove (clear) an alarm without waiting for the reset condition.
	Immediate Dial Required	This feature is used for dial-up micros only. Click Yes if you want the associated micro to dial the host immediately when this alarm condition occurs.

Table 52. Alarms form fields (continued)

Tab	Field name	Description
	Reset Outputs	• Auto Reset Outputs Select to allow the system to automatically reset any output groups associated with this alarm (when the input resets). The system resets any devices (lights, sirens, etc.) operated by outputs in an output group. *Example: You may decide to use an auto reset for an output device (such as a camera) that requires toggling on or off.* • Manual Reset Outputs Click this button to require an operator to manually reset any outputs associated with this alarm. The system resets any devices associated with the alarm. Any devices (lights, sirens, etc.) operated by outputs stay on until manually reset. *Example: You may decide to use a manual reset for a motion sensor that activates floodlights in a parking lot. The manual reset requires the operator to turn the output off using the Output button on the Alarm Response window.* • Duration Reset Outputs Click this button to allow the system to reset any outputs associated with this alarm when the output duration time elapses. Any devices (lights, sirens, etc.) operated by outputs stay on for the duration time (set on the Outputs form). *Example: You may use a duration reset for an alarm that triggers flood lights to go on. The time duration can be set for the maximum amount of time required to implement the alarm instructions.* **Note:** Both the Alarms form and the Outputs form define reset methods for outputs. Output resets can be overridden as follows: • A Manual Reset of an output overrides any other reset method that is defined for that output. Example: If the Outputs form specifies Reset On Duration for an output, but the Alarms form assigns it Manual Reset, the Manual Reset overrides. • A Duration Reset overrides an Auto Reset defined for an output. Example: If the Alarms form specifies Auto Reset for an output, but the Outputs form assigns it Reset On Duration, the Duration Reset overrides. • A Duration Reset overrides a Reset On Input for an output. If the Outputs form defines a Reset On Input for an output, but the Alarms form assigns it Duration Reset, the Duration Reset overrides.
	Color Picker	Click Change Colors to display a palette of colors. Toggle the button at the top of the palette to set the foreground color (for the text) and the background color (for the background of the alarm message) that you want displayed on the Alarm Monitor.
	Color Sample	Foreground A sample is displayed representing the selected color for the text of the alarm message that will be displayed on the Alarm Monitor. Background A sample is displayed representing the selected color for the background of the alarm message that will be displayed on the Alarm Monitor.
	Alarm Blink	**Yes** - The alarm will blink for specified number of seconds (10 seconds is the default). **No** - The alarm will not blink. **Blink Until Acknowledged** - The alarm will blink until acknowledged. **Note:** When an alarm that is configured with blink options is bumped, it will blink until acknowledged on the operator client workstation that it was bumped to.
Instructions	Alarm Instructions	Click to display a list box. Select up to five alarm instructions. The selected messages will appear as instructions to the operator on the Alarm Monitor when this alarm is activated.

Related procedures

To create, edit, or delete an Alarm record:

1. Select **Configuration**, **Alarms**, and then **Alarms** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Defining alarm colors

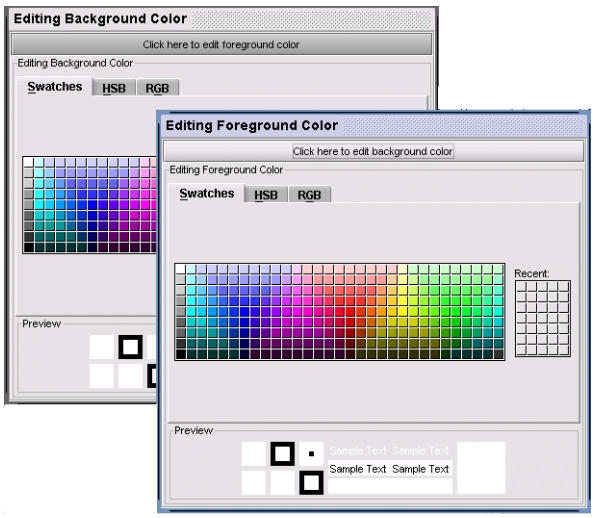
Alarm monitor color scheme: Alarm description

If you have selected Alarm Description in the Alarm Monitor Color Scheme box of the Parameters form, the Alarm Color box will appear on the Alarms form. This box contains the Foreground Color, Background Color, and the Change Color button.

Example

Ann Davis is the system administrator at Global Corporation and she has defined the Door Forced Open to display in red letters on a yellow background. She is considering changing the background color to blue.

Figure 49. Alarm Color Form



Related procedures

To define alarm colors:

1. From the **Configuration** menu, select **Alarms**, and then click the **Alarms** tab.
2. From the toolbar, click **Find** .
3. Select an alarm record from the list in the data grid.
4. Click **Change Colors** to open the color palette.
5. Toggle the button at the top of the palette to set the foreground color (for the text) and the background color (for the background of the alarm message) that you want displayed on the Alarm Monitor.

6. Click **Save** . Once these changes are made, the next alarm that comes in will be displayed with the new colors.

Alarm monitor color scheme: Processing state

It is possible to define the colors that will be used in the Alarm Monitor so that the color scheme reflects the alarm state. This option will be used if Processing State is selected in the Alarm Monitor Color Scheme box of the Parameters form.

Each alarm in the Alarm Monitor will have a foreground and background color based on its processing state and logical state. The Alarm Color form is used to set foreground and background colors for each possible combination of alarm logical and processing states.

The logical states are:

- Set
  Alarms that are in the active alarm state.
- Reset
  Alarms that have been reset (turned off) and are no longer active.
- Tamper
  The wiring of the alarm input has been cut or tampered with.

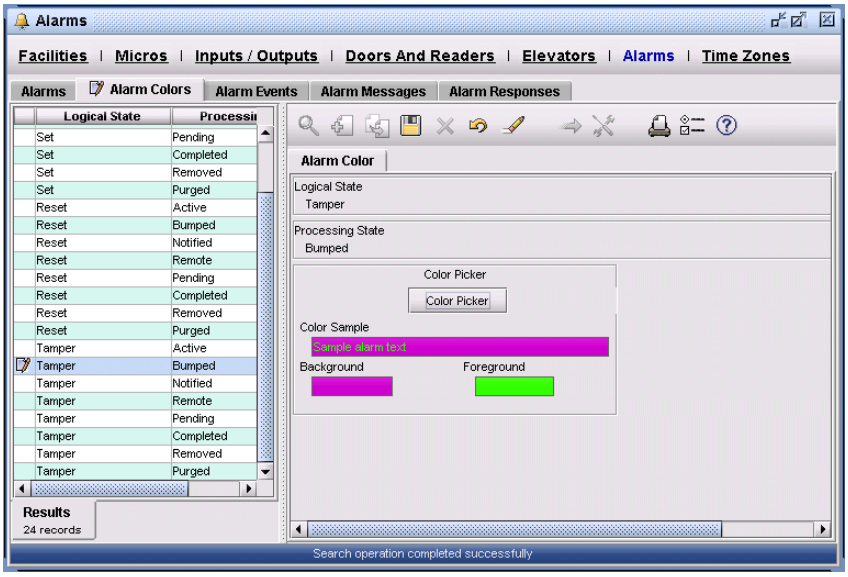
The processing states are:

- Active
  Alarms that are not yet acknowledged.
- Bumped
  Alarms received by the alarm monitor (a specific terminal) that are not acknowledged in a defined amount of time, and are sent to another terminal defined by the user.
- Remote
  Used by RAN (Remote Alarm Notification) alarms that are received by the alarm monitor, but are not acknowledged in a defined amount of time, and are forwarded to a configured remote non-Picture Perfect system.
- Pending
  Alarms that are acknowledged but not removed.
- Completed
  Alarms that are removed (still displayed on the monitor), waiting for a physical reset.

Example

Joe Smith is the system administrator at Global Corporation and he wants all alarms with a Logical State of *Tamper* and a Processing State of *Bumped* to reflect the background color *Purple* and the foreground text color *Green*.

Figure 50. Alarm Colors: Processing State



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 53. Processing alarm states

State	Description
Logical State	This field reflects the logical state (Set, Reset, or Tamper) of the selected alarm.
Processing State	This field reflects the processing state (Active, Bumped, Remote, Pending, or Completed) of the selected alarm.
Color Picker	Click Change Colors to display a palette of colors. Toggle the button at the top of the palette to set the foreground color (for the text) and the background color (for the background of the alarm message) that you want displayed on the Alarm Monitor.

Related procedures

To set Processing State colors:

1. From the **Configuration** menu, select **Alarms**, and then click the **Alarm Colors** tab.
2. From the toolbar, click **Find** .
3. Select an alarm state from the list in the data grid.
4. Click **Change Colors** to open the color palette.
5. Toggle the button at the top of the palette to set the foreground color (for the text) and the background color (for the background of the alarm message) that you want displayed on the Alarm Monitor.
6. Click **Save** . Once these changes are made, the next alarm that comes in will be displayed with the new colors.

Chapter 8 Device management

This chapter describes how to manage and control the various devices that comprise your Picture Perfect system, such as digital inputs (door contacts, push buttons, or sensors), digital outputs (bells, horns, lights), and the micro controllers that control them. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

The Picture Perfect software monitors input devices connected to one or more micro controllers and when an alarm condition is detected, outputs, such as horns, lights, or door strikes, are activated.

Each of the inputs and outputs as well as the micro controllers must be defined in the system. In order to accomplish these tasks, the following forms need to be completed:

- Output Groups
- Input Groups
- Micros
- Keys
- Outputs
- Inputs
- Time Zones

Creating output groups

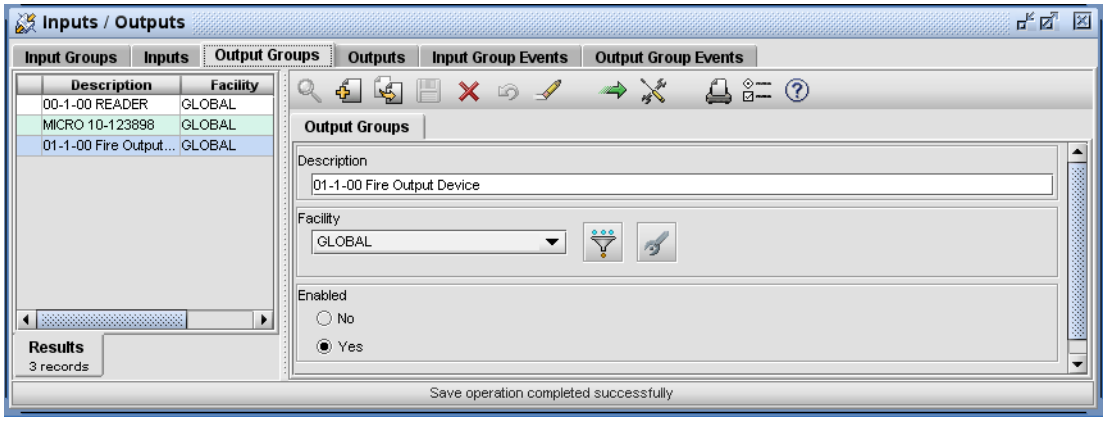
Before you define individual outputs, you must create output groups to which individual outputs can be assigned. When an output group triggers, all outputs assigned to the group activate. (An input group triggers one or more output groups.) Link selected outputs together by assigning the same output group to each output using the Outputs form.

Example

The sprinkler system in Building 1 is assigned to the output group, *01-1-00 Fire Output Device*. The first part of the description indicates the wiring address to which the system is connected.
01 (Micro1) - *1* (Reader board 1) -*00* (the address on the board)

The second part of the description tells the function of the output group, *Fire Output Device*.

Figure 51. Output Groups Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 54. Output Groups form fields

Field name	Description
Description	Enter a description (up to 60 characters). You can write descriptions for output group names to reflect how the outputs in the group function. The description becomes part of the transaction message, telling the monitoring operator what happened and where. One part of this description may include non-technical language for operator information, and the other part may include a wiring address or location. *Example*: *001-0-01 FIRE OUTPUT DEVICE* *001-0-02 PERIMETER SURVEILLANCE DEVICE*
Facility	Click Facility to display the facilities list box. By default, the output group record will be assigned the same facility as the micro to which the door is assigned however, you do have the ability to manually re-assign an output group's facility. This might be desirable in a case where one micro controls more than one facility, for instance two companies occupying the same building that use separate doors for entry/exit. For more information, see *Creating facilities* on page 53.
Enabled	• Select Yes to allow this output group to activate when triggered by an input group. • Select No to prevent the outputs in this output group from activating when triggered by an input group.
Note: An output cannot belong to more than one output group; but more than one output can be assigned to one output group.	

Related procedures

To create, edit, or delete an Output Group record:

1. Select **Configuration**, **Inputs/Outputs**, and then **Output Groups** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Creating input groups

Before defining individual inputs, you must create input groups to which individual inputs can be assigned. Input groups trigger output groups when all or any of the inputs assigned to the group are detected. Input groups are needed for physical inputs such as readers and sensors and for logical events determined by the system or micro.

Logical Input Events for a micro are:

- Badge History Overflow
- Alarm History Overflow
- Upstream Communication Failure
- Downstream Communication Failure
- Reader Communication Failure

Logical Input Events for an area are:

- Invalid Badge
- Unknown Badge
- Lost Badge
- Suspended Badge
- Antipassback Violation
- Duress

Logical Input Events for a door are:

- Door Held Open
- Door Forced Open
- Door Pre-alarm

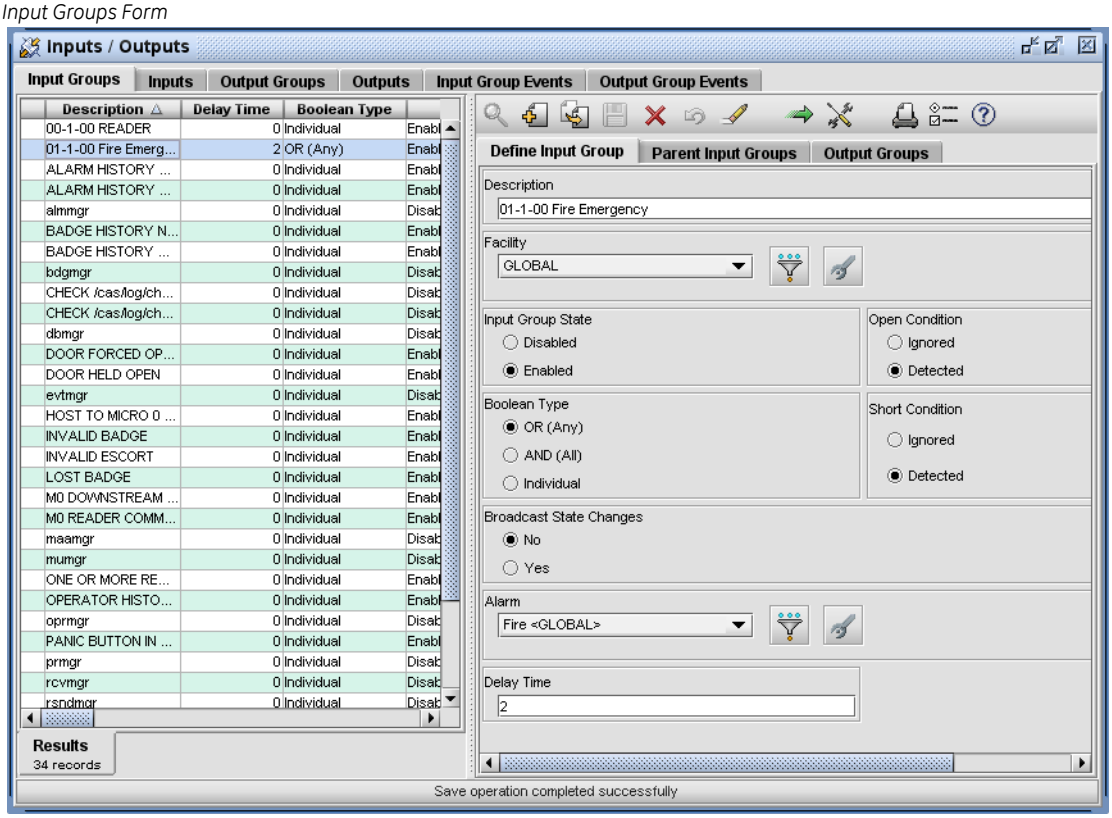
Example

Building 1 contains three smoke detectors (one on each floor), and all three of these inputs go to one Fire Emergency input group. A fire breaks out on the ground floor. If this input group is set up with the *Any* condition, the input group will change state and activate the alarm as soon as the first floor's smoke detector is activated. If this input group is set up with the *All* condition, the input group will change state and activate the alarm only after all three smoke detectors have been activated. This input group will activate an alarm, and will trigger an output group, which will activate the sprinkler system.

The smoke detectors are wired to the following address:

01 (Micro1) - *1* (Reader board 1) -*00* (the address on the board)

Figure 52. Input Groups Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 55. Input Groups form fields

Field name	Description
Description	Type a description of the Input Group, usually including a micro wiring address. **Note:** In both single input groups and in a hierarchy of input groups, all inputs in any given group or hierarchy must be associated with the same micro.
Delay Time	Type the number of seconds an input must be true (On State or Change State) before the input group is true. This delay helps avoid false input detections. **Notes:** • The Off To On Delay Time and On To Off Delay Time set on the Inputs form overrides the Delay Time set on the Input Groups form. • Set Delay Time to zero for any input group assigned to an exit push button.

Table 55. Input Groups form fields (continued)

Field name	Description	
Boolean Type	Boolean refers to an Any or an All condition. If the specified Any or All condition occurs, an input group will change its state. Select one of the following radio buttons:	
	OR (Any)	Click this radio button if you want the Input Group to change state when any of its inputs are activated (Boolean).
	AND (All)	Click this radio button if you want the Input Group to change state only when all of its inputs are activated (Boolean).
	Individual	Click this radio button if you want the Input Group to pass along information that one of its inputs has changed state. This is an individual input group that activates each time one of its inputs changes state. To the system, this input group is transparent, because the message sent by this input group actually reflects the description of the input itself, not the input group. **Notes:** • Logical alarms must always use Individual (Non-Boolean). • Only Individual (Non-Boolean) input groups appear on the Input Group list boxes of the Readers, Areas, Doors, and Micros forms.
Input Group State	Select Enabled to allow this input group to activate. Select Disabled if this input group should not activate.	
Open Condition	Select Detected to allow this input group to trigger associated outputs when the input group detects an open-condition state change. This field is for supervised input. Select Ignored if this is not a supervised input.	
Short Condition	Select Detected to allow this input group to activate associated outputs when the input group detects a short-condition state change. This field is for supervised input. Select Ignored if this is not a supervised input.	
Broadcast State Changes	Select Yes to broadcast any input state changes in this input group to all micros on the system. Select Yes if you want the inputs in this input group to trigger outputs on other micros, or if you want an input from this input group to trigger an Emergency mode. Normally this is set to No.	
Alarm	Displays a description of the selected alarm (if any) associated with this input group. Click the Alarm button to display the Alarm list box. Select the desired alarm. When this input group activates, the selected alarm triggers.	
Facility	Click Facility to display the facilities list box. By default, the output group record will be assigned the same facility as the micro to which the door is assigned; however, you do have the ability to manually re-assign an output group's facility. This might be desirable in a case where one micro controls more than one facility, for instance two companies occupying the same building that use separate doors for entry/exit. For more information, see *Creating facilities* on page 53.	
Parent Input Group	Displays a description of the selected parent input groups (if any) associated with this (child) input group. Click a Parent Input Group button to display the Parent Input Group list box, which is a list of input groups, and select an input group to be the parent for this child. You can select up to three parent input groups for a (child) input group. For more information, see *Parent input groups* on page 131.	
Output Group	Displays a description of the selected output group associated with this input group. Click an Output Group button to display the Output Groups list box. Select up to five output groups (one for each button). When this input group activates, all of the selected output groups trigger.	

Parent input groups

Keep the following in mind, when working with Parent Input Groups:

- An input group that is connected to a parent input group becomes, in essence, an input of that parent input group, and is subject to the parent's boolean or non-boolean settings.
- Each input group can have up to three input groups as its parents, and each input group can be the parent of any number of input groups. An input group cannot be its own parent.
- A tree-like hierarchy of input groups can be built, with each input group propagating its state changes on to its parent input group. Do not create a circular hierarchy, such as A is a parent of B, and B is a parent of A.
- An input group's alarm and output groups are not affected by its association with a parent. They will all work independently.

Note: Changes to parent input groups through schedules will only take effect on the child input groups after the controller has been reset.

Example of a parent input group

A high-security vault is equipped with three motion detectors and a security guard patrols the vault periodically. Any one of the motion detectors must be able to activate the alarm, but the alarm must be disabled during the patrol.

This scenario can be resolved as follows: (See *Figure 53, Example of a Parent Input Group* on page 132)

1. Assign the three motion detectors (inputs 1, 2, and 3) to a *Motion* input group. This input group would have a boolean type of *Any*, so any single motion detector could activate this group.
2. Assign *Motion* the parent input group of *Vault*. No alarms or outputs will be associated directly with *Motion*.
3. Assign *Vault* the appropriate alarm and output groups desired for motion being detected in the vault area, and assign it a boolean type of *All*.
4. Associate a toggle reader (see *Toggle* on page 186) with an input group called *Control*. The toggle reader will be the only input in this group. *Control* will be a Trigger on Input (*Individual*) input group which is non-boolean, so a badge swipe through this reader will toggle the input group's state on or off.
5. Assign *Control* the parent input group of *Vault*. No alarms or outputs will be associated directly with *Control*.

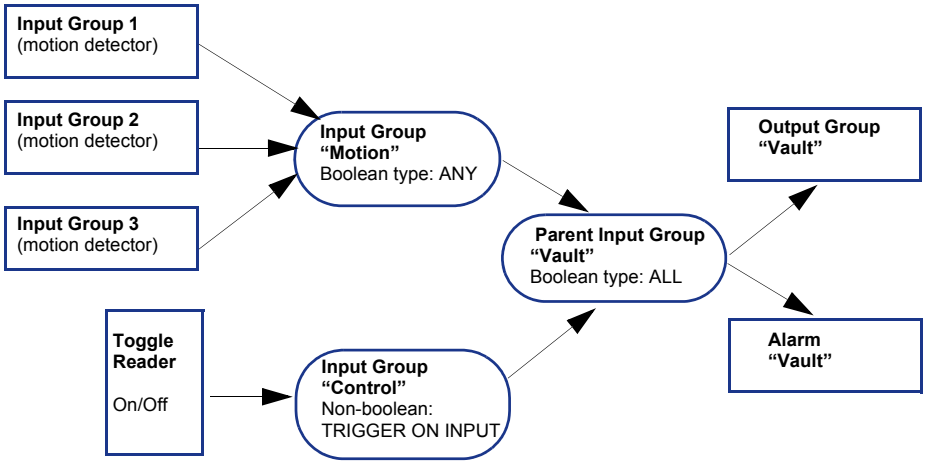
Vault's only inputs are its child input groups, *Motion* and *Control*. Both of these must be activated in order to trigger the alarm, since *Vault's* boolean type is *All*.

When the vault is unpatrolled, the toggle reader is used to toggle-on *Control*, meaning that this input group is activated. If any of the three motion detectors should activate, the *Motion* input group will be triggered (since its boolean type is *Any*). The *Vault* input group will then receive the activated state change of *Motion*. When that happens, the All condition of *Vault* has been met, and the associated alarm and output groups will be triggered.

To deactivate the motion-detector alarm during a routine patrol, the security guard simply swipes their authorized badge through the toggle reader. *Control's* input is deactivated; therefore, the *Vault* input group cannot trigger an alarm, even though the motion detectors will activate the *Motion* input group while the guard

is in the area. When the patrol of the vault is finished, the guard swipes their badge through the toggle reader again, this time to activate it.

Figure 53. Example of a Parent Input Group



Related procedures

To create, edit, or delete an Input Group record:

1. Select **Configuration**, **Inputs/Outputs**, and then **Input Groups** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Defining micros

Each micro controller (micro) controls specific input and output devices, such as readers, doors, and alarms. For the micro to work correctly, you must define communication-port characteristics such as communication retries, polling interval, port assignment, and micro address. (The micro address set in the software must match the micro address in the hardware.) Micro error conditions need to be associated with alarms, input groups, and output groups. The required associations should be defined using the various Picture Perfect forms, such as Ports, Modems, InGroups, and Alarms, before attempting to complete the Micros form.

Picture Perfect supports three kinds of micro communications: direct, dial-up and network. All three types of communications can be combined on a single host.

Note: Depending on the amount of traffic on a system, to avoid performance degradation, a line of micros should contain no more than eight M5 controllers or 64 readers.

For more information refer to:

- *Direct connect micros* on page 140
- *Dial-up micros* on page 140
- *Network micros* on page 143

Do not add or change a micro until you have configured the input groups that you need for the micro and the alarm and output groups that you want to have associated with the selected input groups.

A micro can be configured in the following ways:

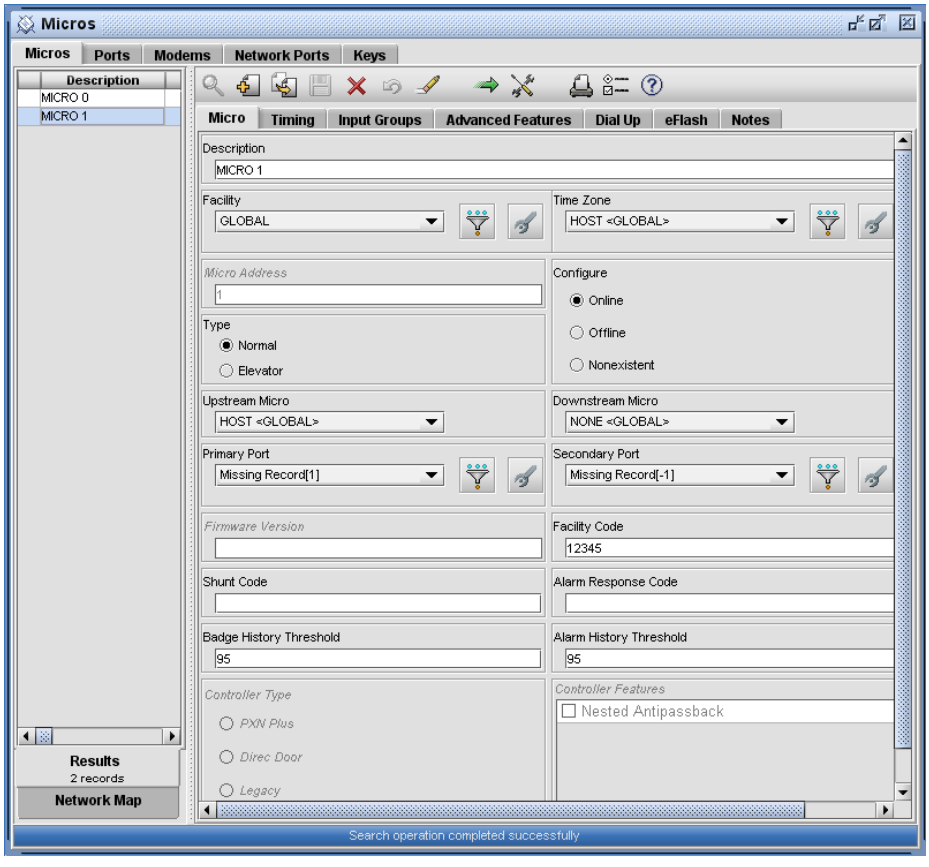
- Non-existent
- Direct connect
- Dial-up
- Downstream dial-up
- Network
- Network dial-up

All of these options are explained in the sections that follow. However, if you prefer, you can configure all of your micros as non-existent and then you can go back later and reconfigure them.

Example

Micro 1 controls all of the inputs, outputs, doors, and readers in Building 1.

Figure 54. Micros Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 56. Micros form fields

Tab	Field	Description
Micro	Description	Type a micro description up to 60 alphanumeric characters long; *Example: Building 1 Micro 0*. This micro description appears in a Micros list box for selection on the Inputs, Outputs, and Readers forms.
	Facility	You must assign a facility to a micro. Other devices, such as readers and inputs, that are connected to the micro will default to this facility, unless they are specifically assigned to another facility.
	Micro Address	Type a number from 0 to 4095 to identify the address of this micro as set in the micro's hardware address switches. Once a micro's address is set, it cannot be changed.
	Upstream Micro	Displays the selected upstream micro. Click the Upstream Micro button to display the Micros list box. Select the micro or host that is upstream from this micro.
	Downstream Micro	Displays the selected downstream micro. Click the Downstream Micro button to display the Micros list box. Select the micro or host (or None) that is downstream from this micro.
	Type Normal/ Elevator	Select whether this is a Normal micro or an Elevator micro type. Only an M5 can be used with Elevator Control. See *Elevator control* on page 369 for more details on this feature. **Note:** An Elevator micro configured with multiple readers, uses Reader 1 to control the elevator.
	Configure Online/ Offline/Non-existent	Select whether the micro is being configured Online, Offline or Non-existent. If neither are selected, the micro is configured as non-existent, that is, not on the system. • Select Online to bring a micro online that was either configured offline or non-existent. The micro will be automatically reset when configured online. • Select Offline to allow this installed and connected micro to be configured before it goes online. This allows normal operations to continue without interruption by a flood of unexpected error messages related to this micro. • Select Non-existent to configure a micro that is not yet installed (physically connected). Once the micro is installed, bring up this form and select Online to put the micro online.
	Time Zone	Select the time zone in which the micro is located from the drop-down list. This allows Picture Perfect to display badge and alarm activity in the micro's local time. It also allows schedules that span multiple time zones to execute in the respective local times. See *Verifying time zones* on page 168. In order for an operator to use this field, they must have at least View page level permission for the Time Zone form. See *Creating facility permission profiles* on page 81.
	Primary Port	Displays the selected primary port for micro communications. Click the Primary Port button to display the Ports list box. Select the primary port to which this micro is wired. • Uni-directional micros require a primary port assignment (and None specified for the secondary port). • Bi-directional micros require both a primary and a secondary port assignment. • Dial-up micros do not require a port assignment (assign None to both the primary and secondary port).

Table 56. Micros form fields (continued)

Tab	Field	Description
	Secondary Port	Displays the selected secondary port for micro communications. Click the Secondary Port button to display the Ports list box. Select the secondary port that will be activated if communication is lost on the primary line. • Uni-directional micros require a primary port assignment (and None specified for the secondary port). • Bi-directional micros require both a primary and a secondary port assignment. • Dial-up micros do not require a port assignment (assign None to both the primary and secondary port).
	Firmware Version	The revision of application code that is contained in the micro. This field is read-only.
	Facility Code	Optional: Type a facility number (1 to 5 digits long). If the 8RP board loses communication with the micro's CPU board, access can still be granted to all badges with a facility code that matches this field. If this field is left empty, the 8RP will grant access to all badges while in this degraded mode. This applies only for 8RP boards in a Micro/2 or Micro/4.
	Shunt Code	Optional: Type a shunt code (1 to 10 digits long). With Shunting Enabled on the Area and Reader forms, this code entered on a keypad allows a badge holder to prop a door open (for the time specified on the Doors form) without triggering a door-held-open alarm.
	Alarm Response Code	Optional: Type an Alarm Response Code (1 to 10 digits long). With Keypad Alarm Response Enabled on the Doors form, this code entered on a keypad allows an authorized badge holder to respond to and reset an active alarm. This Alarm Response Code must be different from the Shunt Code on the Micros form. See *Controlling alarms using a keypad code* on page 384.
	Badge History Threshold	Type the percentage at which the micro triggers the Badge History Overflow input group to notify the host that its Badge Transaction table has reached this percentage of capacity.
	Alarm History Threshold	Type the percentage at which the micro triggers the Alarm History Overflow input group to notify the host that its Alarm Transaction table has reached this percentage of capacity.
	Controller Type	Read only indicator of controller type that is set when the controller establishes communication with the host.
	Controller Features	Read only indicator of new firmware feature capabilities supported by this controller.
Timing	Upstream Retries	Enter the number of times the micro will try to contact its upstream micro before triggering the Upstream Communications Failure input group (normally set to 3). This input group must be defined prior to completing the Micro form. See *Creating input groups* on page 127.
	Upstream Retry Interval	Enter the number of seconds between each upstream retry (normally set to 2 seconds).
	Downstream Retries	Enter the number of times the micro will try to contact its downstream micro before triggering the Downstream Communications Failure input group (normally set to 3). This input group must be defined prior to completing the Micro form. See *Creating input groups* on page 127.
	Downstream Retry Interval	Enter the number of seconds between each downstream retry (normally set to 2).
	Host-Micro Polling Retries	Enter the number of times the host will try to contact this micro before triggering the Upstream Communications Failure input group (normally set to 3). This input group must be defined prior to completing the Micro form. See *Creating input groups* on page 127.
	Host-Micro Polling Retry Interval	Enter the number of seconds between each host-to-micro retry (normally set to 2 seconds for direct connect micros and 8 seconds for dial-up micros).

Table 56. Micros form fields (continued)

Tab	Field	Description
	Polling Interval	Enter the number of days, hours, minutes and/or seconds that must elapse without communication to the host before the host polls this micro to verify that it is still capable of communicating (normally set to 60 seconds). If the polling interval is set to 0, no polling occurs. **Note:** To be UL compliant, the polling interval must be less than 200 seconds. **CAUTION:** **If the micro is configured as Network Dialup**, the polling interval is interpreted differently based on the current communications channel open to the micro. If using the primary channel (network), the polling interval is interpreted as-is. If, however, the secondary channel (dialup) is being used, the polling interval is shifted, seconds are interpreted as minutes, minutes as hours, and hours as days. One side effect of this is that secondary channel communication failures are reported at the "shifted" interval. For example: A network dialup micro is configured with a polling interval of 30 seconds. The polling interval is actually 30 minutes when running on the secondary channel and communication failures are only detectable every 30 minutes.
Input Groups	Select the appropriate input group for each error condition field: Badge History Overflow, Alarm History Overflow, Upstream Comm Failure, Downstream Comm Failure, Reader Comm Failure **Note:** Only Individual input groups which are non-boolean are displayed in the list box.	
Advanced Features	Lock on Duress	This feature allows you to configure a micro to lock a door when a special PIN number, used to signal emergency situations, is entered on a keypad reader.
	Passive Time & Attendance	Used to log a badge holder In and Out using the same reader by swiping the card the normal way for In and reversing the card or turning the card backwards for Out.
	Taped Badge Suspend	This feature can be configured to ignore multiple consecutive badge reads or to suspend the badge when multiple consecutive badge reads occur. If this option is enabled, the Taped Badge Count field is activated.
	Taped Badge Count	The number of consecutive badge reads before the system will suspend the badge. (Minimum count = 2; Maximum count = 255)
	Micro Reset	Click **Reset Now** to manually reset the micro.
	Micro State	Click **Get Micro State** to display the current state of the selected micro's attributes.

Table 56. Micros form fields (continued)

Tab	Field	Description
Dial Up	Modem Type	Displays the selected modem type. Click the Modem Type button to display the Modems list box. Select the type of modem to connect to at the host. • For direct communication micros, select None. • For network micros, without Dial-Up, select None. • For network micros, with Dial-Up, select the host modem type. The modem type selected for the micro must match the modem type (and baud rate) indicated by the micro's DIP switch settings on Switch Bank 2. See the appropriate installation manual for information on DIP switch settings. The modems in this list are created using the Modems form. See *Configuring modems* on page 64 for information on setting up modems.
	Micro Dialout Prefix	Enter the PBX prefix, area code or country code (or other prefix) to be pre-pended to the host phone number in order for the micro to call the host.
	Micro Backup Dialout Prefix	For redundant configurations in which the primary and backup servers are located in two different area codes, enter the PBX prefix, area code or country code (or other prefix) to be pre-pended to the backup host phone number in order for the micro to call the backup host.
	Micro Phone Number	Enter the phone number to be used to call this dial-up micro from the host, including area code, PBX prefix, or country code as necessary.
	Micro Backup Phone Number	For redundant configurations in which the primary and backup servers are located in two different area codes, enter the phone number to be used to call this dial up micro from the backup host, including area code, PBX prefix, or country code as necessary.
	Idle Time	Enter the number of days, hours, minutes and/or seconds that the line must be idle before the line is dropped. This field must be greater than [(Host-micro retries) x (Host-micro retry interval)+1].
	Maximum Connect Time	Enter the maximum number of days, hours, minutes and/or seconds (0 to 65536) that the micro and host may be connected. After a reset to allow for badge download, the default maximum connect time is one hour.

Table 56. Micros form fields (continued)

Tab	Field	Description
	Callback	Specify whether a callback is required from the host, the micro, or neither. In a callback situation, the host or micro receiving the call flags the sender for a callback, then disconnects without a data transaction taking place. This strategy prevents a foreign system from communicating with the host or micro. This strategy may also be cost effective if host-to-micro calls are less expensive than micro-to host calls, or vice versa. • Host The host will call back the micro. • Micro The micro will call back the host. **Note:** A controller configured as Micro Callback cannot be flashed with upgraded application code. If you need to update the application code, set Callback to None prior to running the flash program. Upon completion, set it back to Micro. • None No callbacks are required.
	Dial on Updates	Specifies when the host should dial the micro with record changes: • Always The host always dials the micro for any record changes that affect it. • Never The host will not dial the micro for any record changes. Updates are made during the next communications session. • Ask Operator The host will prompt the operator to see if it should dial the micro for each record change.
	Dial on Startup	Specify whether the host should dial the micros whenever the system is started: • Always The host always dials the micro whenever the system is started. • Never The host will not dial the micro immediately whenever the system is started. Rather, it will wait a random amount of time, no greater than the polling period, before it dials the micro.
	Dial Host on Schedule Update	Specify whether the micro should dial the host whenever changes occur due to a micro schedule. • Always The micro always dials the host for any schedule updates that affect it. • Never The micro will not dial the host for any schedule updates. Updates are made during the next communications session.

Table 56. Micros form fields (continued)

Tab	Field	Description
eFlash		eFlash is a method of flashing your DirecDoor, PXNPlus, Micro/5-PX, Micro/5-PXN, M/PX-2000, and M/PXN-2000 micros. It does not require the micro to be in maintenance mode while the flash code is being downloaded. All communication is handled by the host. The eFlash download program is installed as part of the base Picture Perfect product and can be run on standalone systems, network subhosts, and on the primary host of a redundant system. On a networked system, eFlash should not be run on the network host. It can run on all subhosts simultaneously and is capable of flashing the micros connected to each subhost. eFlash can be run either from the Micros form or from the UNIX command line. Using an optional file, .eflashrc, you can define flashing requirements for the entire system once, and then use part or all of the definition to flash or re-flash micros as needed. This file can be used for scheduling unattended flashing. **Note:** Only one instance of eFlash can be run on a system. When eFlash begins, it creates a lock file: `/cas/log/.eflashrc` If the lock file exists, indicating that the program is running, when you attempt to launch eFlash, an error message will display and the program will exit.

Dynamic configuration

Micros (firmware 4.03 or later required) can be configured dynamically, meaning the Picture Perfect system does not have to be restarted for the changes to take effect. However, there are some rules that must be met. If these rules are not met, an error message displays and none of the changes are made until that rule is satisfied. The error message window remains open until you click OK.

Note: All of the fields on the Micros form support dynamic configuration, except for **Micro ID**. Once a micro's ID is set, it cannot be changed.

Dynamic configuration rules:

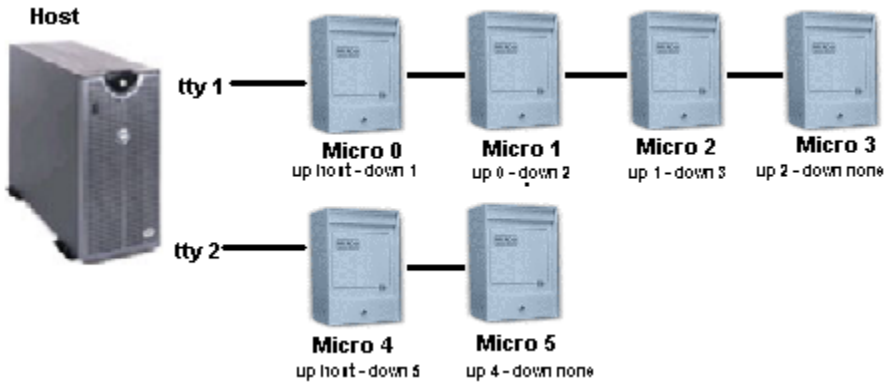
- Every micro must have a head (or upstream) micro.
- Every micro must have a tail (or downstream) micro.
- A micro can be upstream from at most one micro.
- A micro can be downstream from at most one micro.
- The primary port must be the same for a micro and its downstream micro.
- The secondary port must be the same for a micro and its downstream micro.
- An upstream micro must have a matching downstream micro.
- A downstream micro must have a matching upstream micro.
- The last micro in a bi-directional line must have a host downstream.
- Two head micros cannot have the same primary port.
- Two tail micros cannot have the same secondary port.
- A network dial-up micro must have a matching downstream micro.
- A network micro must have a matching downstream micro.

Direct connect micros

A direct communications micro requires direct connection to the host. Communication can be uni-directional as in *Figure 55* or bi-directional as in *Figure 56*.

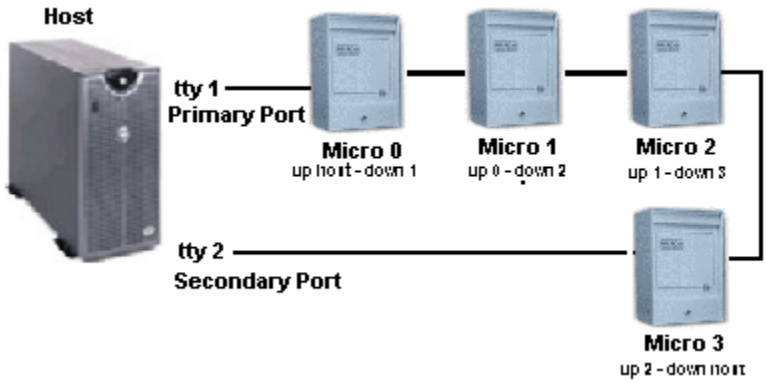
In uni-directional communication, each line of micros is connected to the host from a unique port (In the example below, Micro 0 through 3 are connected to tty1; Micro 4 through 5 are connected to tty2). If communication is lost between downstream micros, the host continues to communicate only with those micros upstream from the break. An alarm is generated, indicating the loss of communication. For example, if a break occurs between Micro 1 and 2, the host will only have communication with Micro 0 and 1 from tty1, and it will maintain communication with Micro 4 and 5 from tty2. Communication with Micro 2 and 3 is lost.

Figure 55. Example of direct communication - Uni-directional micros



In bi-directional communication, the micros are connected to the host using a primary port at one end (tty1) and an alternate port at the other end (tty2). If communication is lost between any micros, the host will communicate from the primary port to all micros upstream from the break and from the alternate port in the opposite direction, to all micros upstream from the break. Using this method, communication with all micros is maintained. For example, if a break occurs between Micro 1 and 2, the host will communicate with Micro 0 and 1 from tty1, and it will communicate with Micro 3 and 2 from tty2. No communication is lost.

Figure 56. Example of direct communication - Bi-directional micros

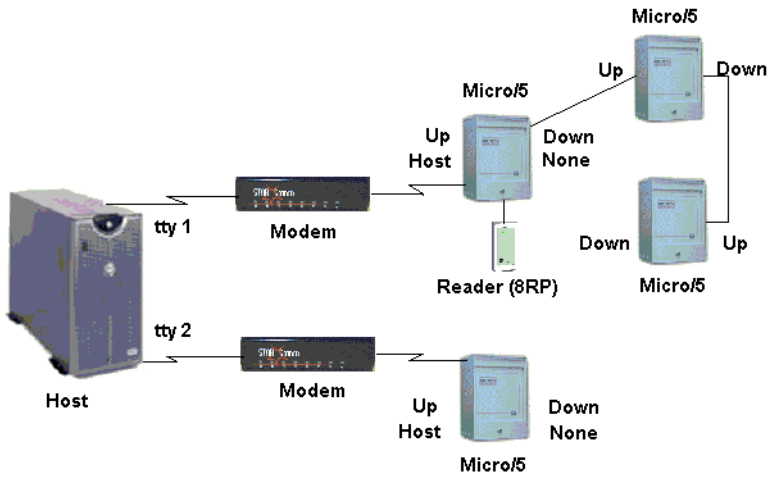


Dial-up micros

A dial-up micro requires an attached modem, a dedicated phone line, and one or more compatible modems attached to the host ports.

There is only one possible configuration for dial-up communication: uni-directional which is detailed in *Figure 57, Example of Dial-up communication*.

Figure 57. Example of Dial-up communication



The table below shows the micros that are supported downstream from dial-up micros

Table 57. Dial-Up micro downstream support

Dial-Up micro	Downstream support			
	Micro/5-PX M/PX-2000	Micro/5-PXN M/PXN-2000	DirecDoor	PXNPlus
DirecDoor	No	No	No	No
PXNPlus	Yes	No	No	Yes
Micro/5-PX M/PX-2000	Yes	No	Yes	No
Micro/5-PXN with dial-up M/PXN-2000 with dial-up[1]	Yes	No	Yes	Yes

1. If the network connection fails and the micro has the dial-up option, it will behave as a dial-up Micro/5-PX after it connects to the host for the first time.

There are events that cause the micro to automatically dial up the host and there are events (usually operator activities such as updates or commands) that cause the host to automatically dial up the micro.

Table 58. Events requiring micro-to-host calls

Event	Micro to host response
Power-on Reset	After a power-on reset, the micro reads its DIP switch settings to determine its attached modem type and the required baud rate for communication to the modem, assumes that the modem is connected to the host port, and then tries to dial the host (using the modem's hard-coded phone number).
Alarm	The micro immediately dials the host when a priority micro alarm activates. Immediate Dial-Up is user-defined. See *Immediate Dial Required* on page 118.

Table 58. Events requiring micro-to-host calls

Event	Micro to host response
Alarm and Badge Threshold	The micro dials the host when the micro's alarm or badge history buffer reaches its threshold (user-defined) and requires uploading to the host.
Badge Table Request	The micro dials the host when there is no micro database record for a badge just presented to a reader. The micro's resident database reduces the requirement for micro-to-host calls for badge records.

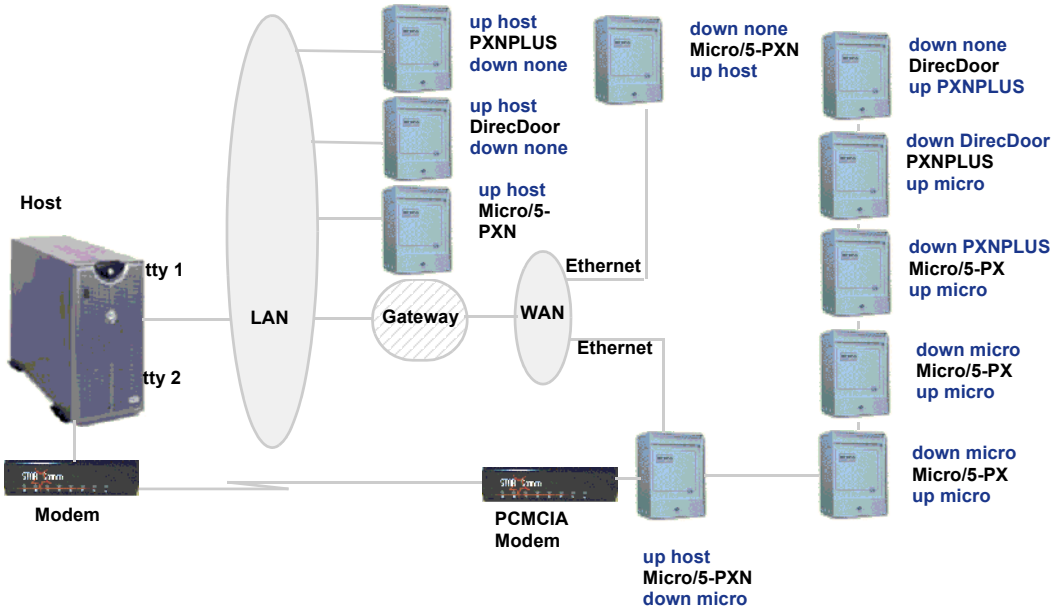
Table 59. Events requiring host-to-micro calls

Event	Host to micro response
Database Updates	The host dials out to send database updates to micros. Whether the host does this automatically, never, or on request is user-defined for each individual micro. For micros that do not require immediate updates, the host stores the updates until the next host-to-micro or micro-to-host call occurs and then downloads the new records.
Outputs and Output Group Commands	The host dials the micro immediately whenever the operator changes the state of an output or output group on that micro. **Note:** For details that show how an operator can command state changes and control outputs using input groups, output groups, or selected outputs, see *Figure 109, Control Output Groups* on page 268.
Operator-generated Commands	The host allows the operator to dial any micro in the system to check the status. See *Monitoring status* on page 280.
Micro Reset Request Command	The host dials the micro to send a reset command when an update to the system database requires major updates to one or more micro configurations. The host dials the micro to send a reset request when an operator uses CMENU to reset a micro. **Note:** Before the reset sequence starts, the micro terminates the call and disconnects to free the communications line; after reset, the micro dials the host to request its database and configuration
Micro Poll	The host can poll micros that have not communicated with the host for a user-defined time period. A zero Polling Interval setting tells the host that no polling is required. See *Polling Interval* on page 136.

Network micros

A network micro requires an ethernet connection to the host. A network micro with the optional dial-up backup feature also requires a PCMCIA modem card in the other available slot, a dedicated phone line, and one or more compatible modems attached to the host port in addition to the network lines.

Figure 58. Sample Ethernet configuration

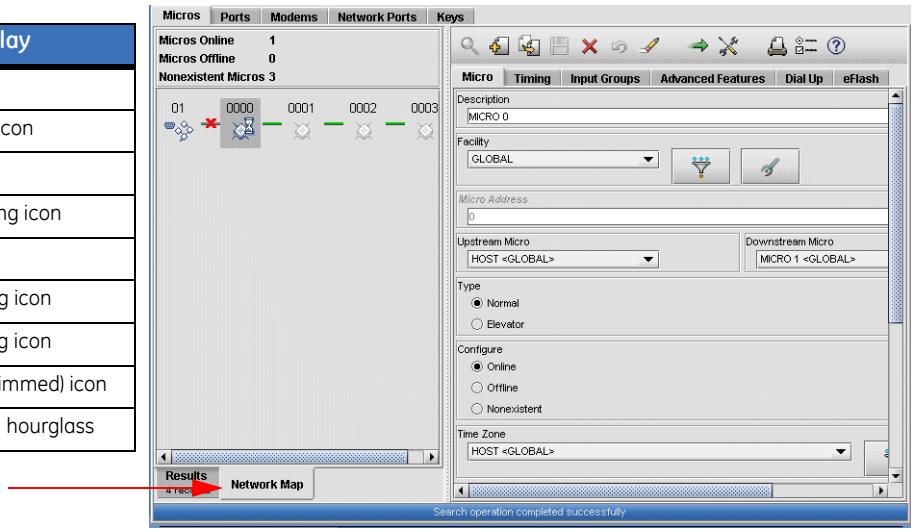


Micro Network Map

The network map on the Micro form provides a visual display of all the micros on the system and their relative position on their respective port lines. To access the network map, click the Network Map tab on the bottom of the navigation pane.

Figure 59. Network Map

Micro State	Virtual Display
Online	Blue icon
Pending online	Blue flashing icon
Offline	Orange icon
Pending offline	Orange flashing icon
Flash failure	Red icon
Resetting	Purple flashing icon
Flashing in progress	Yellow flashing icon
Configured nonexistent	Grayed out (dimmed) icon
Micro with resent list	Blue icon with hourglass



Place your cursor over the micro to display a tooltip containing detailed communication status, as shown in *Figure 60*.

Figure 60. Detailed micro status

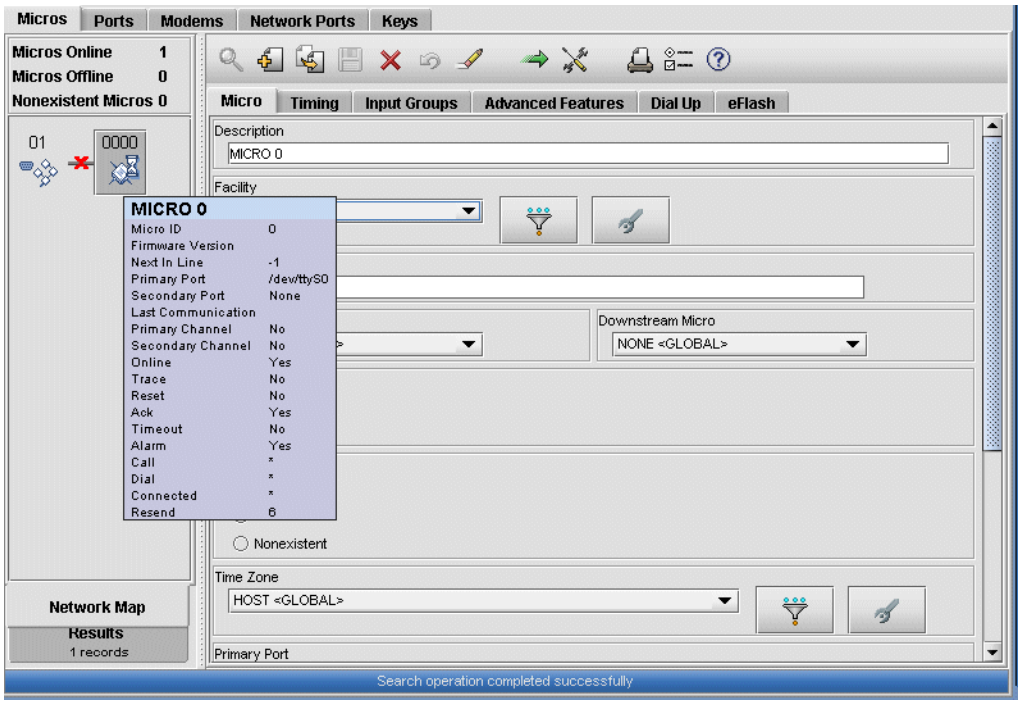


Table 60. Detailed communication status

Event	Micro to host response
Micro ID	Displays the micro's identification number.
Firmware Version	The revision of application code currently flashed in the micro.
Next in Line	Displays the ID number of the downstream micro.
Primary Port	Displays the primary port of the micro.
Secondary Port	Displays the secondary port of the micro.
Last Communication	In the case of a downstream micro, this field shows the last time a non-ACK packet was received from the micro. In the case of a head of line micro, this field shows the last time any packet was received, including ACK packets (an acknowledgement that the last message was received).
Primary Channel	A yes/no (Y/N) flag field indicating whether the micro is communicating via the primary port.
Secondary Channel	A yes/no (Y/N) flag field indicating whether the micro is communicating via the secondary (backup) port.
Online	A yes/no (Y/N) flag field indicating whether the micro is online.
Trace	A yes/no (Y/N) flag field indicating whether the micro is traced.
Reset	A yes/no (Y/N) flag field indicating whether the micro is resetting. If the micro requests a mandatory reset (during power-up) or if the host initiates a mandatory reset command (by operator request), this flag is set to Y until the micro is reset and a final synchronization message is sent to indicate that it is online.
Ack	A yes/no (Y/N) flag field indicating whether the micro has any pending Ack messages. Under normal circumstances for a Head-of-line micro, this flag is set to N. If it is set to Y it indicates an unresponsive micro and a problem that requires troubleshooting.
Timeout	A yes/no (Y/N) flag field indicating if a packet is not acknowledged within the number of attempts specified in the Micro record. When this occurs the micro is considered to be in "error" condition. After an alarm is generated the condition changes to "alarm" and this flag is cleared.
Alarm	A yes/no (Y/N) flag field indicating that a micro is in a communication "alarm" condition. Once a valid ACK or data packet is received from the micro this flag is cleared as well as the "offline" flag if it is set.
Call	Indicates the host is calling the micro using a dial-up connection.
Dial	Indicates the host is dialing the micro using a dial-up connection.
Connected	Indicates the host is connected to the micro using a dial-up connection.
Resend	Indicates the number of messages in queue for the micro.

Related procedures

To create a Direct-connect Micro record:

1. Select **Configuration**, **Micros**, and then **Micro** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.
3. Complete the Micros form with special attention to the items below. The following fields must be set to the given value.
   - Primary port: You must select a direct port.
   - Secondary port: For bi-directional micros, you must also select a secondary port which must be a direct port.
   - Modem type: None.
4. Leave the remaining fields on the Dial Up screen blank.

To create a Dial-up Micro record:

1. Select **Configuration**, **Micros**, and then **Micro** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.
3. Complete the Micros form with special attention to the items below. The following fields must be set to the given value.
   - Specify None for port assignment (primary and secondary), since dial-up micros call the host on any available port that is compatible (same modem type).
   - Select the modem type of the host's modem.
4. Complete the remainder of the Dial Up portion of the screen.

To create a Network Micro record:

1. Select **Configuration**, **Micros**, and then **Micro** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.
3. Complete the Micros form with special attention to the items below. The following fields must be set to the given value.
   - For the primary port, you must select a network micro port.
   - For the secondary port, you must select None.
   - Select a modem type of None.
4. Leave the remaining fields on the Dial Up screen blank.

To create a Network Dial-up Micro record:

1. Select **Configuration**, **Micros**, and then **Micro** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.
3. Complete the Micros form with special attention to the items below. The following fields must be set to the given value.
   - For the primary port, you must select a network micro port.
   - For the secondary port, you must select None.

CAUTION: **If the micro is configured as Network Dialup**, the polling interval is interpreted differently based on the current communications channel open to the micro. If using the primary channel (network), the polling interval is interpreted as-is. If, however, the secondary channel (dialup) is being used, the polling interval is shifted, seconds are interpreted as minutes, minutes as hours, and hours as days. One side effect of this is that secondary channel communication failures are reported at the "shifted" interval. For example: A network dialup micro is configured with a polling interval of 30 seconds. The polling interval is actually 30 minutes when running on the secondary channel and communication failures are only detectable every 30 minutes.

- Select the modem type of the host's modem.

4. Complete the remainder of the Dial Up screen.

To add a configuration for a micro that is downstream from a dial-up micro:

For micros downstream from dial-up communication micros, ports must be configured before adding or changing a micro and the head-end dial-up micro must be configured. Refer to *Table 61* on page 148 for a list of the type of micros that can be downstream.

1. Select **Configuration**, **Micros**, and then **Micro** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.
3. Complete the Micros form with special attention to the items below. The following fields must be set to the given value.
   - Review the items that directly relate to direct connect micros.
   - Callback: None
   - Modem type: Downstream Dial up

To configure a micro before it is on the system:

Picture Perfect allows you to configure a micro without the micro being on the system by configuring it as Non-existent.

1. Select **Configuration**, **Micros**, and then **Micro** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.
3. Complete the Micros form. The Configure field must be set to Non-existent.

To change a micro configuration:

Changing a micro is simply locating the record and changing the necessary fields. Keep in mind that if you change the port or modem setting, you may be changing the type of communications that this micro is using.

Before you modify a micro's configuration, you may want to check the initial settings. There are basically five fields on the Micro form that determine the type of micro communications being used: Primary Port, Secondary Port, Upstream, Downstream, and Modem Type. Refer to *Table 61* on page 148 to determine what type of micro communications is being used.

Table 61. Micro communication

Type of micro communication	Micro form fields				
	Primary Port	Secondary Port	Upstream	Downstream	Modem Type
Direct Uni-directional	Direct Port	None	If a head-of-line micro: Host[1]	If an end-of-line micro: None[2]	None
Direct Bi-directional	Direct Port	Direct Port	If a head-of-line micro: Host[1]	If an end-of-line micro: Host[2]	None
Dial-up	None	None	If a head-of-line micro: Host[2]	If an end-of-line micro: None[2]	Anything except: None or Downstream Dial up
Downstream from Dial-up		None	Anything except: Host or None	If an end-of-line micro: None[2]	Downstream Dial up and the Callback field is set to None
Network	Network Port	None	If a head-of-line micro: Host[2]	If an end-of-line micro: None[2]	None
Network Dial-up	Network Port	None	If a head of line micro: Host[1]	If an end of line micro: None[2]	If a head of line micro, anything except: None or Downstream Dial up Otherwise: Downstream Dial up

1. Otherwise, anything except Host
2. Otherwise, anything except Host or None

1. Select **Configuration**, **Micros**, and then **Micro** tab.
2. From the toolbar, click Find to retrieve all the micro records or enter specific search criteria to limit the search and then click Find.
3. Refer to *Creating, editing, deleting, and printing records* on page 36.

   The updated micro will be reset automatically if the Configure field has been changed to Online. After the micro resets, it requests its new configuration from the host so that it can operate according to its new parameters. The host downloads the new micro configuration. System operations and communications continue normally during a micro reset.

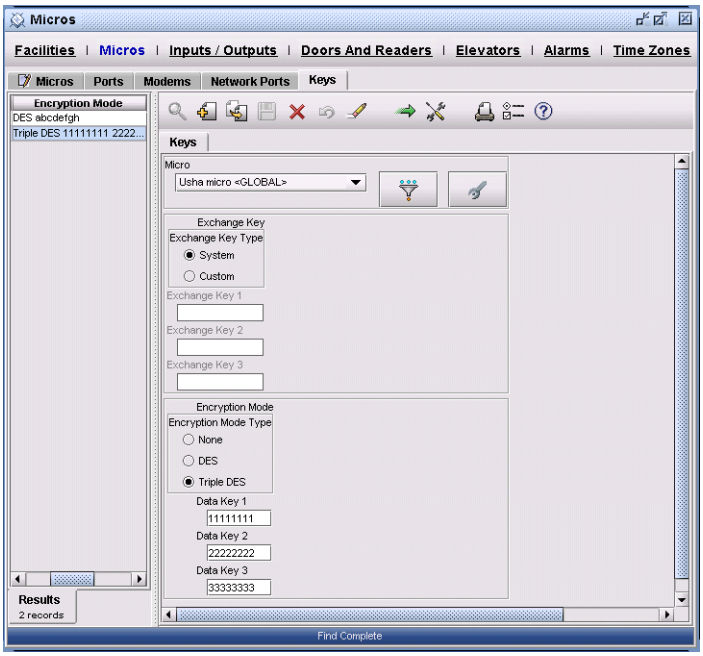
Creating encryption keys

In order to secure transmission between the host and the network micro, the data is encrypted using DES (Data Encryption Standard). This is accomplished by means of a key to create the encryption pattern for transmission.

Example

Triple DES encryption is used between the micro and the host.

Figure 61. Keys form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 62. Keys form fields

Field name	Description	
Micro	The micro that will be transmitting data to/from the host.	
Encryption Mode	This is a required field which defines the encryption mode to be used. It can be set to one of three values:	
	None	No encryption is used; the original or plain text is transmitted. **Note:** None is the default. In order to activate this feature, one of the following must be selected.
	DES	Both sender and receiver use a single key (Key 1) to encrypt and decrypt data.
	Triple DES	Both sender and receiver use three keys (Key 1, Key 2, and Key 3) to encrypt and decrypt data.
Encryption Key Type	System	Encryption is performed using the default system keys.
	Custom	Encryption is performed using user customized keys. This method is more secure.
Encryption Key 1	This key is used for a single DES algorithm as well as the first key used to encrypt the Data Keys in the Triple DES algorithm, before transmitting those keys to the micro.	
Encryption Key 2	The second key used to encrypt the Data Keys in the Triple DES algorithm, before transmitting those keys to the micro.	
Encryption Key 3	The third key used to encrypt the Data Keys in the Triple DES algorithm, before transmitting those keys to the micro.	
Data Key 1	The length of this field must be eight alphanumeric characters. This key is used for a single DES algorithm as well as the first key used in the Triple DES algorithm.	
Data Key 2	The length of this field must be eight alphanumeric characters. This is the second key used in the Triple DES algorithm.	
Data Key 3	The length of this field must be eight alphanumeric characters. This is the third key used in the Triple DES algorithm.	

Related procedures

To manage the DES keys used:

1. Select **Configuration**, **Micros**, and then **Keys** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Note: Due to the sensitive information presented on the screen, you will be prompted for root's password if you attempt to perform any operations with the keys.

Flashing micros

When the micro is powered up, you may need to flash download the Picture Perfect application code into the micro. You can use the eFlash utility which is included in Picture Perfect 4.5.

Before you begin flashing your micros, review the following:

- If the micro is configured for **Micro Callback**, the **Callback** feature must be disabled (the **Callback** field on the Micro form must be set to **None**) in order to perform a flash download. Upon completion of the download, the feature can be enabled (the **Callback** field can be set back to **Micro**).
- If this is a dial-up micro, it must be disconnected from the host before attempting to flash.
- A PXN or PX micro must already be flashed with firmware 4.03 or later to use the eFlash feature.

Micro firmware files

In the **`/cas/flash/eflash`** directory, there is a separate directory for each type of micro's firmware (hex file).

Flashing a micro using eFlash

This download procedure can be used with Picture Perfect version 2.0 host systems or later. The eFlash download program is installed as part of the base Picture Perfect 4.5 product and can be run on standalone systems, network subhosts, and on the primary host of a redundant system.

On a networked system, eFlash should not be run on the network host. It can run on all subhosts simultaneously and is capable of flashing the micros connected to each subhost.

eFlash includes the following features:

- eFlash is a new flash method which does not require the micro to be in maintenance mode while the flash code is being downloaded.
- Flashes DirecDoor, PXNPlus, Micro/5-PX, Micro/5-PXN, Micro/PX-2000, and Micro/PXN-2000 micros.
- All communication is handled by the host.

Note: Micros must first be flashed with Picture Perfect micro firmware version 4.03 or later.

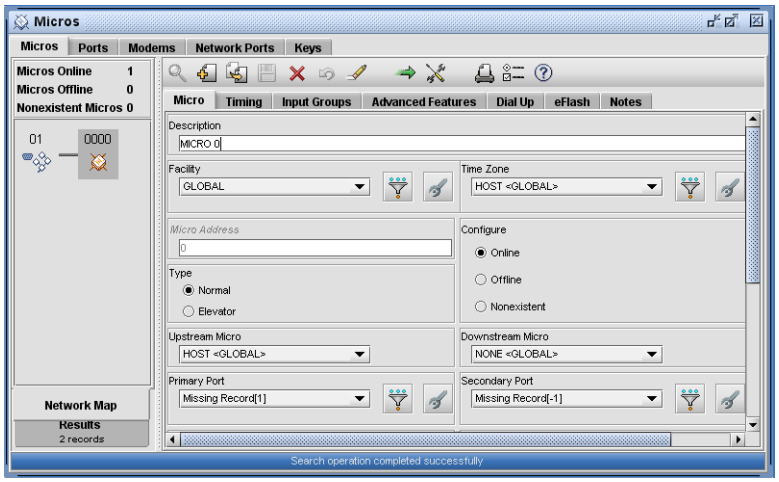
eFlash can be run either from a Graphical User Interface (the default) or from the UNIX command line.

Operating eFlash in a graphical mode

To flash a micro using the eFlash GUI:

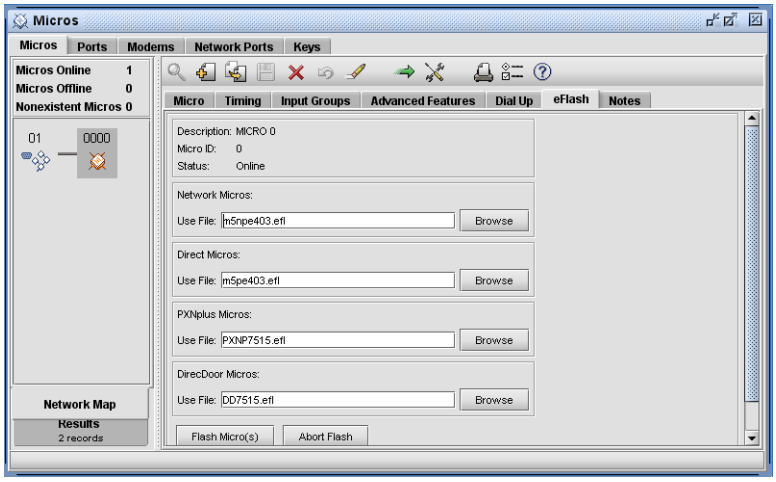
1. Log on to a Picture Perfect client PC.
2. From the **Configuration** menu, select **Micros** to display the **Micro** form.
3. Click **Find**  to search for the micro you want to update.
4. Click the **Network Map** tab located at the bottom of the grid, to display a graphical layout of your micros.

Figure 62. Network Map Tab



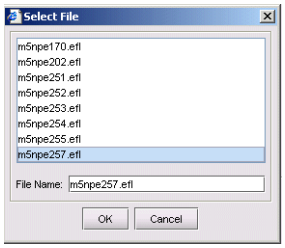
5. Click the eFlash tab to display the eFlash form.

Figure 63. eFlash Form



6. On the **Network Map**, click the micro that you want to flash.
7. Click **Browse** next to the selected micro, to display a list of firmware files and select the file to be used for flashing.

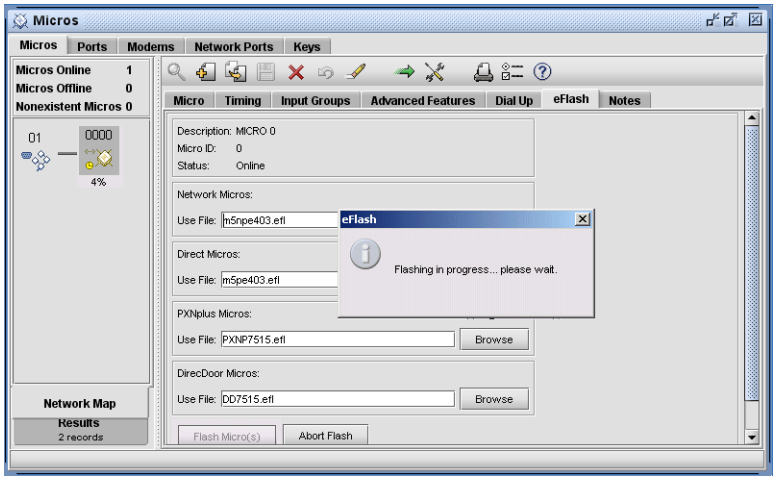
Figure 64. Select File



8. Click **Flash Micro** to begin the flash procedure.

   The flash procedure begins and the micros being flashed are highlighted in yellow.

Figure 65. eFlash in Progress



9. Wait until the flash is complete. You cannot flash another micro until the current selections are complete.

   Note: Only one instance of eFlash can be run on a system. When eFlash begins, it creates a lock file:
   `/cas/log/.eflash.<pid>`
   If the lock file exists, indicating that the program is running, when you attempt to launch eFlash, an error message will display and the program will exit.
   This file is normally removed automatically when the program closes however, under some circumstances, it may still exist and will need to be removed manually.

Operating eFlash from the command line

One or more of the arguments listed in *Table 63* can be included in a command line.

Note: If an option is repeated, only the last value is used with the exception of -m and -l, which may be repeated multiple times. For example, to flash micro id 0 and micro id 2, the entry would be: eflash -m 0 -m 2 Enter

Table 63. eFlash command line arguments

-c	Command line selection option
-p<directory>	Specifies the source directory to search for flash files. This replaces the default directory of /cas/flash/eflash.
-f<filename>	Specifies a flash file to use for the 5PX micro, instead of the default flash.
-n<filename>	Specifies a flash file to use for the 5PXN micro, instead of the default flash.
-r<filename>	Specifies a flash file to use for the DirecDoor controller.
-s<filename>	Specifies a flash file to use for the PXNPlus controller.
-x<number>	Specifies the maximum number of micros that can be flashed at one time.
-h	Starts the HTML based online help.
-u or -?	Prints out the usage message.
-m<micro selection>	Specifies the micro to be flashed. This option can be repeated multiple times. • To flash all active micros in the Picture Perfect database, use: `eflash -m a` Enter • To flash a specific micro, use: `eflash -m <microid>` Enter where `<microid>` is the ID of the micro you wish to flash.
-l<microid>	Specifies a line of micros to be flashed. • To flash a line of micros, use: `eflash -l <microid>` Enter where `<microid>` is the ID of any micro on the line. eFlash adds all other micros on the line to the flash list in the correct order.

To flash a micro using eFlash from the command line:

1. Log on as `root` and open a terminal window.
2. At the command prompt, enter a command using the following parameters:

   `eflash -c -m01 -p /cas/flash/eflash -f mspe170.dfl` Enter

   where `m01` is the micro id and `mspe170.dfl` is the flash file.

   After the flashing has completed, one of the following messages will be displayed:

   `Flashing is successful`

   or

   `Flashing is unsuccessful. See the log file<filename> for details.`

The eFlash configuration file

This is an optional file, `.eflashrc`, that resides on the host in the root user's home directory. The purpose of the file is to allow a Picture Perfect operator to define flashing requirements for the entire system once, and then use part or all of the definition to flash or reflash micros as needed. This file can be used for scheduling unattended flashing.

This file can contain a combination of command line arguments, processing rules, and comments.

Table 64. eFlash configuration file

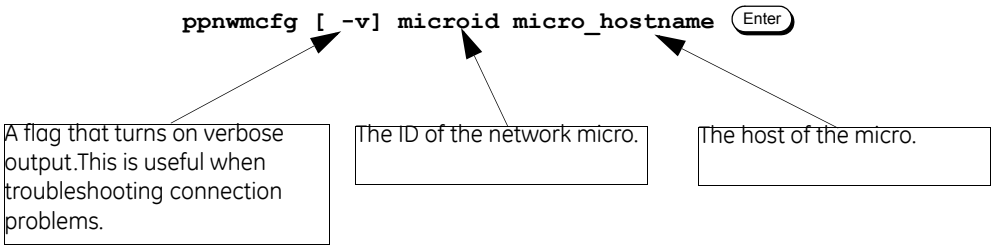
Arguments	All of the following command line options can be included, either one per line or you may concatenate many options per line.	
	-p<directory>	Specifies the source directory to search for flash files. This replaces the default directory of: `/cas/flash/eflash`
	-f<filename>	Specifies a flash file to use instead of the default flash used for direct connect type micros (PX).
	-n<filename>	Specifies a flash file to use instead of the default flash used for network type micros (PXN).
	-r<filename>	Specifies a flash file to use for the DirecDoor controller.
	-s<filename>	Specifies a flash file to use for the PXNPlus controller.
	-m<micro id>	Specifies the micro or micros to be flashed.
	-m a	Specifies that all active micros in the Picture Perfect database be flashed.
	-l<micro id>	Specifies a micro in a line of micros, where the entire line is to be flashed.
	Note: If options are repeated, only the last value read from the file is used. The exceptions are the `-m` and `-l` options, which use all specified micros.	
Processing Rules	Parameters that control the flashing of the micros during the current execution of eFlash may be included. The following parameters may be included:	
	flashwait=value(in seconds)	Sets the time that eFlash waits for the micro to actually flash the EPROM. The flash of a micro is considered a failure if the flash times out. The default is 90 seconds.
	maxflash=value(in seconds)	Sets the maximum number of micros that can be flashed simultaneously. The actual number of micros that is being currently flashed will always be less than this value due to restrictions on flashing multiple micros in the same line. The default is 5. **Note:** Setting this number to a higher value can impact the response time of the system. You should keep this number low for best performance.
Comments	The eFlash configuration file may contain comments. A comment is a line that begins with the pound sign (#). The pound sign and all characters up through the next carriage return are ignored.	

Network micro parameter block configuration (PXN only)

The `ppnwmcfg` command allows the ppadmin user to configure a network micro's parameter block from the host by connecting to the network micro. Once connected, the `ppnwmcfg` utility will put the network micro in maintenance mode and display the current settings.

To display the ppnwmcfg utility:

1. Log on to Picture Perfect as `ppadmin` and type:



The `ppnwncfg` utility will display.

Table 65. ppnwmcfg menus

Menu	Description
S Show parameter block	Displays the contents of the network micro's parameter block.
C Clear parameter	Clears a specific value.
U Update parameter block	Writes the current values to the parameter block.
l - n Modify parameter	Selecting a number will prompt you for a new value.
E Edit all	Prompts you for each parameter block value.
Q Quit	Exits out of `ppnwmcfg`. Once you have quit the `ppnwmcfg` utility, the network micro will require about 30 seconds of idle communication before it resets.

Table 66. ppnwmcfg parameters

Parameters	Description
The fields shown below may vary depending on your firmware version.	
address	The micro ID which is not necessary unless you are configuring a network dialup micro.
phone1	Primary host number for a network dial-up micro to call.
phone2	Secondary host number for a network dial-up micro to call.
mmdmm_init	Modem initialization string.
mdmm_dinit	Modem de-initialization string.
rx_idle_time	The minimum number of characters (20 - 254) to process a buffer.
hop_count	The number of hops (network boards that must be crossed) between the network micro and host.
ring_speed	Specifies ring speed for token ring networks only. (Not supported)
source_ip	The network micro's IP address.
destination_ip	The Picture Perfect host's IP address.
alternate_ip	The backup machine's IP address in a Picture Perfect redundant system.
gateway_ip	The network micro's gateway IP address to reach the destination_ip.
subnet_ip_mask	The network micro's subnet mask.
alt_gateway_ip	The network micro's gateway IP address to reach the alternate_ip.
Note: The network micro will accept connections only from the host defined in this field. If this field is updated incorrectly, the network micro can only be configured from a laptop computer.	

Defining outputs

The Picture Perfect system monitors digital inputs (DIs) for contacts and digital outputs (DOs) for controlling output devices. Outputs are triggered when associated inputs activate. Outputs can operate devices such as door strikes, bells, and lights. Inputs may be physical connections to a micro controller or logical events such as a transaction buffer overflow or an invalid access attempt.

Outputs that operate devices such as door strikes, lights, or sirens must be described to the system. Use the Outputs form to define where this output point is connected, how it is wired to activate, how long it remains on when activated, how it resets, and what output group is associated with it.

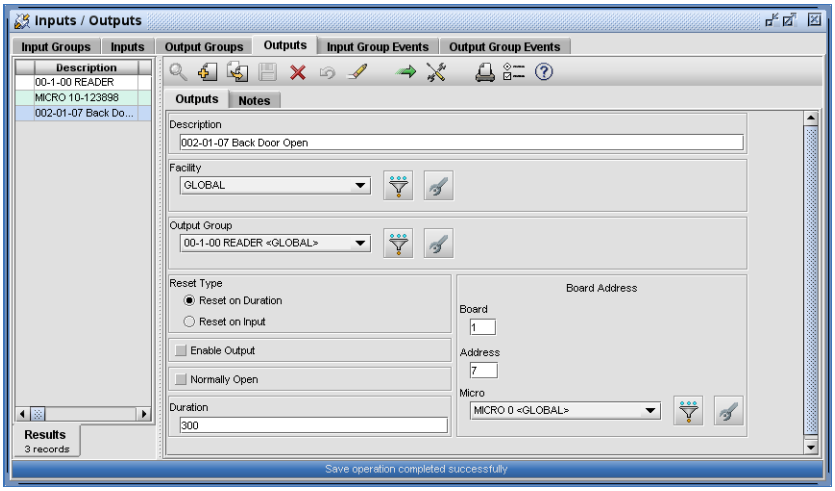
Example

An output may control a light indicating the back door is open. A typical description is: **`002-01-07 Back Door Open`**

The first part of the description indicates that the output is connected to DO point 07 on CPU board 01 of Micro ID 002. The last part of the description indicates the purpose of the output.

Note: How you format output descriptions is entirely an administrative decision, but this format makes the system messages easier to use. To make reports easier to read, the number description should be first so that the text description is aligned with the other records.

Figure 66. Outputs Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 67. Output form fields

Field name	Description
Description	Enter a description (up to 60 characters). This description usually includes a micro board address and a text description.
Facility	Click Facility to display the facilities list box. By default, the output record will be assigned the same facility as the micro to which the output is assigned however, you do have the ability to manually re-assign an output's facility. This might be desirable in a case where one micro controls more than one facility, for instance two companies occupying the same building that use separate doors for entry/exit. For more information, see *Creating facilities* on page 53.
Output Group	Displays a description of the selected output group to link this output point with a group of outputs. Click the Select Output Group button to display the Output Groups list box. Select the desired output group.
Reset on Duration	Select this button if the output should reset after the number of seconds specified in the Duration field. (There is a possible alarm override for a duration reset. See *Reset Outputs* on page 119) *Example: You may want an output to reset on duration if the output device is a door strike and you want it to stay on for a limited duration of time.*
Reset on Input	Select this button if the output should reset as soon as the input resets.
Note: If neither Reset On Duration nor Reset On Input is selected, the output stays on. If Reset On Input is selected, the door does not unlock with a valid badge read.	
Enable Output	Toggle the button On if this output is to be activated when its output group triggers.
Normally Open	The inactive state of an output is either normally open or normally closed. Toggle this button On if it is normally open. **Note:** Ask your installer how the output point is wired. Door DOs are usually wired "normally open."
Board	Type a board number from 0 to 8. The micro controller's power/comm board is always board 0. Use *Table 69* on page 160 to find the board number and address where an output point is located. Verify the board number with your installer.
Address	Type 0, 1, 8, 9, or 16 to 31 for the digital output address where the output is wired to the connector on the board.
Duration	Type the number of seconds this output remains on when activated, if this output is allowed to reset when the duration time expires. The maximum value is 32,767. If 0 is selected, the output will not reset but will remain activated continuously. See *Reset on Input* on page 159.
Micro	Displays a description of the selected micro where this output is connected. Click Select Micro to display the Micros list box. Select the desired micro.

Table 68. M/PX-2000 wiring chart - Outputs

Element	Board number	DO address	Reader address
CPU	--	--	--
Door DO 1 - 2	Picture Perfect Board 1	0 - 1	0 - 1
Door DO 3 - 4	Picture Perfect Board 2	0 - 1	0 - 1

Table 68. M/PX-2000 wiring chart - Outputs

Element	Board number	DO address	Reader address
Aux DO 1 - 2	Picture Perfect Board 1	0 - 1	0 - 1
Aux DO 3 - 4	Picture Perfect Board 2	0 - 1	0 - 1

Table 69. M5 wiring chart - Outputs

Element	Board number	DO address	Reader address
CPU	--	--	--
2RP/2SRP Board	1 - 4	0 - 1	0 - 1
8RP	1 (Picture Perfect Board 1-4)	0 - 1	0 - 1
	2 (Picture Perfect Board 5-8)	0 - 1	0 - 1
16DO/DOR Board	1 - 4	16 - 31	--
• Optional boards include four 20DI boards (20 supervised input points), four 16DO boards (16 output points), four 2RP/2SRP boards (2-reader board), and two 8RP boards (8-reader board). • The M5 cabinet has a seven-slot capacity. Two slots are used by the mandatory Power/Communications and CPU boards. The remaining five slots may be configured to meet your site requirements with any combination of boards, within the limitations listed above.			

Related procedures

To create, edit, or delete an Output record:

1. Select **Configuration**, **Inputs/Outputs**, and then **Outputs** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Defining inputs

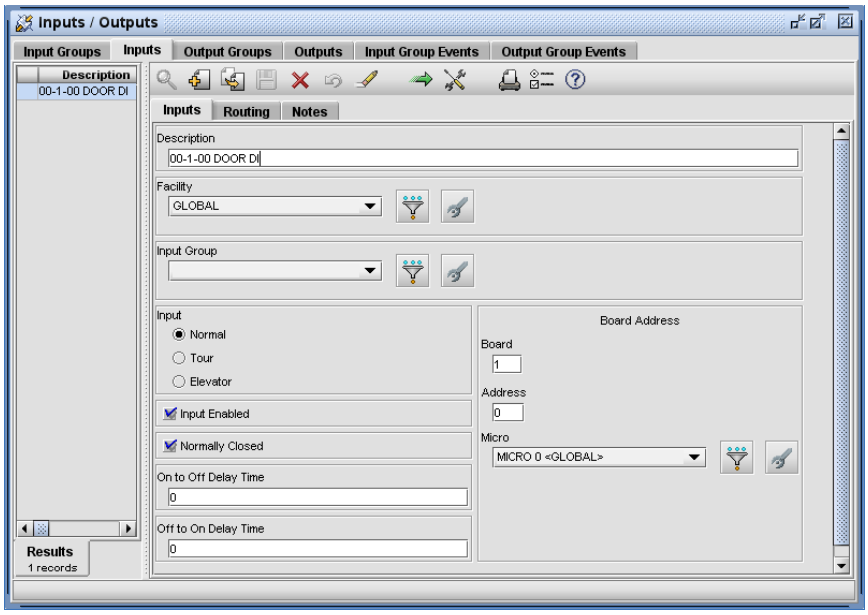
Physical inputs such as sensors or detectors must be described to the system. Use the Inputs form to define where each input point is connected, how it is wired to activate, what kind of state changes activate it, how long it remains detected before it activates, which input group is associated with it, and where messages about this input are routed.

Example

An input controls a door sensor. The sensor detects when the doors is open or closed. A description for this input could be: `01-1-00 Door DI`

The first part of the description indicates that the input is connected to DI point 00 on DI board 1 of Micro ID 01. The last part of the description indicates the purpose of the output

Figure 67. Inputs Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 70. Inputs form fields

Field name	Description
Description	Type a description of the input, usually including a wiring address and a written description.
Board	Type a board number from 0 to 8. The micro controller's power/comm board is always board 0. Use *Table 71* on page 163 to find the board number and address where this input point is located. Verify the board number with your installer.
Address	The Address field indicates what digital input point on the board this input is using. Type a number 0, 1, 8 to 9, or 16 to 35 (for the M5). The address depends on how the input is wired to the connector on the board. Ask your installer.
Micro ID	Displays the selected micro where this input point is located. Click to display the Micros list box from which you can select the desired micro.
Off to On Delay Time	The Off To On Delay Time delays the effect of the input described on this form when it changes state from Off to On. This delay helps avoid false input detections. Type the number of seconds (0 to 65535) required for the delay. Leaving this field blank or typing a 0 (zero) causes no delay. Set this delay to 0 for an Exit DI. This field overrides the Delay Time set on the Input Groups form. See *Delay Time* on page 129.
On to Off Delay Time	The On To Off Delay Time delays the effect of the input described on this form when it changes state from On to Off. This delay helps avoid false input detections. Type the number of seconds (0 to 65535) required for the delay. Leaving this field blank or typing a 0 (zero) causes no delay. Set this delay to 0 for an Exit DI. This field overrides the Delay Time set on the Input Groups form.
Routing	Displays the selected routing where messages about this input are displayed. Click Routing to display the Routings list box. Select the desired routing. The typical routing is None which means that it is not routed.
Input Group	Displays the selected input group for this input. Click Input Group to display the Input Groups list box. Select the desired input group. **Note:** • In both single input groups and in a hierarchy of input groups, all inputs in any given group or hierarchy must be associated with the same micro. • Use the Doors form to assign a door DI. • Assign a door exit button to the same input group as the reader for that door. • Do not assign a door DI to an input group. • If an input group is unselected from an input and a new input group is assigned to the input, the micro has to be reset.
Route Definition	Displays the selected route definition for this input. This route definition is used for Activity Monitor routing. Click Route Definition to display the Route Definition list box. Select the desired route definition. If this field is left blank, this input's activity will be routed to all operators.

Table 70. Inputs form fields (continued)

Field name	Description
Facility	Click Facility to display the Facilities list box. By default, the input record will be assigned the same facility as the micro to which the input is assigned; however, you do have the ability to manually re-assign an input's facility. This might be desirable in a case where one micro controls more than one facility, for instance, two companies occupying the same building that use separate doors for entry/exit. For more information, see *Creating facilities* on page 53
Normally Closed	The inactive state of an input is either normally open or normally closed. If it is Normally Open, toggle this button Off by deselecting it. If it is Normally Closed, toggle it to On by selecting it. **Note:** Ask your installer how the input point is wired. Door DIs are usually wired "normally closed" and exit request DIs are usually wired "normally open."
Input Enabled	Toggle this button On by selecting it, to allow this input to activate. **Note:** If an input is to be used as an Exit Button input in an area designated as M2MR with Door Control, the Normally Closed and Input Enabled buttons must be deselected (the default).
Input	• Normal: Toggle this button On to configure this input as a standard input point. • Tour: Toggle this button On to configure this input as a Tour point. This button will only be enabled if the optional Guard Tours package is installed. • Elevator: Toggle this button On to configure this input as an elevator input.

Table 71. M5 wiring chart - Inputs

Element	Board number	DI address	Reader address	Exit DI address
CPU	--	--	--	--
2RP Board	1 - 4	0 - 1	0 - 1	8 - 9
20DI Board	1 - 4	16 - 35	--	--

- Optional boards include four 20DI boards (20 supervised input points), four 16DO boards (16 output points), four 2RP boards (2-reader board), and one 8RP board (8-reader board).
- The M5 cabinet has a seven-slot capacity. Two slots are used by the mandatory Power/Communications and CPU boards. The remaining five slots may be configured to meet your site requirements with any combination of boards, within the limitations listed above.
- On a M5, the Tamper and AC Power Fail inputs must be wired to connector 6 on the Power/Communications board. The AC Power Fail input will always be defined as Board 0, Address 0; the Tamper input will always be defined as Board 0, Address 1.

Related procedures

To create, edit, or delete an Input record:

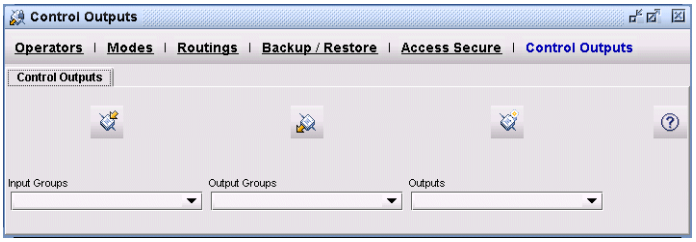
1. Select **Configuration**, **Inputs/Outputs**, and then **Inputs** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Controlling outputs

Outputs are devices that can turn on or off due to an input condition or operator intervention. An authorized operator can turn outputs on or off using the Control Outputs function for the duration of time entered on the Output form.

You can select a single input group, output group, or an individual output from this window. Click the corresponding icon to display the Control Outputs window or the Control Output Groups window.

Figure 68. Control Outputs Form

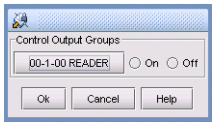


Example

The Control Output Groups window allows you to manually control all associated output devices such as lights or sirens. For example, you may decide to use a manual reset for a motion sensor that activates floodlights in a parking lot.

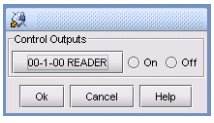
To control all outputs associated with the selected output group, click the On or Off radio button.

Figure 69. Control Output Group Window



To control an individual output associated with the selected output group, double click the output group to display the Control Outputs window.

Figure 70. Control Outputs Window



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than shown in the following table. There is no required sequence to follow.

Table 72. Control Outputs form fields

Field name	Description
Input Group	Select an input group from the list and click Input Group to display a list of all associated output groups. Select an output group and click the On or the Off radio button to fire all the associated outputs.
Output Group	Select an output group from the list and click Output Group to display a list of all associated outputs. Select an output and click the On or the Off radio button.
Output	Select the output you wish to control, and click Output. Select an output and click the On or the Off radio button.
Note: Each transaction is recorded in operator history.	

Related procedures

To control an output from an output group:

When you select an output group from the list on the Control Outputs window, you can trigger any or all of the outputs associated with this output group.

1. From the **Control** menu, select **Control Outputs**.
2. Select an output group from the **Output Group** list.
3. Click **Output Group**. A list of all associated outputs displays.
4. Click the appropriate radio button to turn the desired output on or off.

To control an individual output:

When you select an output from the list on the Control Outputs window, you can trigger the individual output.

1. From the **Control** menu, select **Control Outputs**.
2. Select an output from the **Outputs** list.
3. Click **Outputs**. A list of all outputs displays.
4. Click the appropriate radio button to turn the desired output on or off.

Controlling Access Secure operations

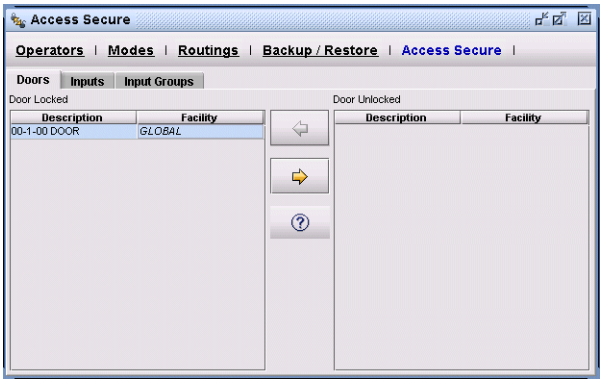
Devices, such as Inputs, Input Groups, or Doors, normally exist in an Access state in which they are disabled or unlocked, or in a Secure state in which they are enabled or locked. These states are reflected on the appropriate device form.

It may be desirable to change this state back and forth to allow for unscheduled conditions, such as heightened security levels or unscheduled peak access times. This feature can be used, in lieu of scheduling an event, to accommodate situations that require operator control. It allows state changes for multiple devices rather than applying the change to each device individually through the applicable form.

Example

For example, you may want all doors to be opened when the security guard arrives at his post, rather than at a scheduled time.

Figure 71. Access Secure Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 73. Access Secure form fields

Device	Fields and controls	Description
Doors	Current State: Access	The door state is Unlocked.
	Current State: Secure	The door state is Locked.
Inputs	Current State: Access	The input state is Enabled
	Current State: Secure	The input state is Disabled
Input Groups	Current State: Access	The input group state is Enabled
	Current State: Secure	The input group state is Disabled

Related procedures

To display the Access/Secure Operations window:

This option does not appear on the Control menu, unless it has been enabled. See How to enable Access/Secure Operations.

1. From the **Control** menu, select **Access Secure**. Then click the appropriate tab: Doors, Inputs, or Input Groups.
2. From the list displayed, select the item whose state you wish to change. Multiple selections may be made.
3. Click the appropriate **Change State** arrow button.

To enable Access Secure Operations:

1. From the **Control** menu, select **Operators**, and then click the **System Permissions Profiles** tab.
2. Click **Find**  to locate the System Permission Profile record to alter.
3. Under **Page Level Permissions**, make sure the profile for Access Secure is set to **Update**, **Insert**, or **Delete**.
4. Click **Save**  .

Verifying time zones

The Time Zone feature associates a time zone with items in your database that have a physical location, such as micros, operators, or hosts.

Monitors display dates and times in all three time zones: Host, Micro, and Operator. Using the Preferences icon  on the Monitor toolbar, you can choose which columns to display.

Date and time entry fields on event forms and on the Category scheduler specify a context of either Host, Micro, or Operator which allows you to schedule events or categories in any of those contexts.

Note: Some Picture Perfect systems may experience a temporary discrepancy in transaction date and time during the DST change. This will only affect systems with servers or micro controllers that span multiple time zones. For example, if a server is located in Central DT and microcontrollers are in Eastern DT they may experience a one-hour divergence. The time will correct itself at the conclusion of DST.

Example

Example 1:

You have three offices, one in New York, one in San Francisco, and one in Houston. You are the system administrator and you are in New York; the host is in Houston. You want to schedule all of the doors in the system to open at 08:00.

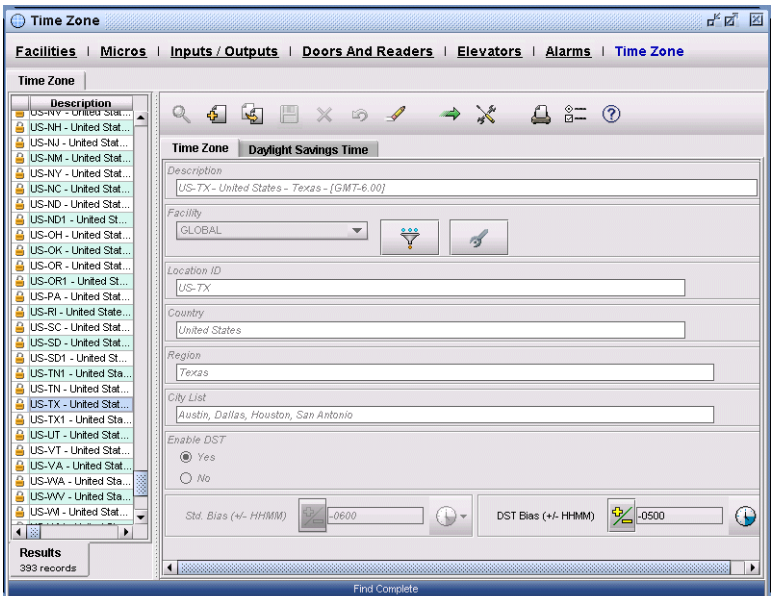
- **Host Context**: If you select Host as the context for this door event, all doors in the system will open simultaneously, at 08:00 Houston time. However, it will be 09:00 in New York and 06:00 in San Francisco.
- **Operator Context**: If you select Operator as the context for this door event, all doors in the system will open simultaneously, at 08:00 New York time. However, it will be 07:00 in Houston, and 05:00 in San Francisco.
- **Device Context**: If, however, you select Device as the context for this door event, all doors in the system will open at 08:00 local time -- the time local to the micro to which the doors are connected. The doors in New York will open first at 08:00 local time, and then, one hour later, the doors in Houston will open at 08:00 local time, and finally, two hours after that, the doors in San Francisco will open at 08:00 local time.

Example 2:

You have three offices, one in New York, one in San Francisco, and one in Houston. You are the system administrator and you are in New York; the host is in Houston. You want to expire a badge at 16:00 today.

- **Host Context**: If you select Host as the context to expire this badge at 16:00, the badge expiration will take effect at 17:00 in New York, 16:00 in Houston, and at 14:00 in San Francisco.
- **Operator Context**: If you select Operator as the context to expire this badge at 16:00, the badge expiration will take effect at 16:00 in New York, 15:00 in Houston, and at 13:00 in San Francisco. This would effectively deny access immediately.
- **Device Context**: If you select Device as the context to expire this badge at 16:00, the badge expiration will take effect at 16:00 in New York, one hour later at 16:00 in Houston, and 3 hours later at 16:00 in San Francisco.

Figure 72. Time Zone form.



Fields and controls

The following is a list of fields that may require additional information for you to complete. The list is in the order that the fields appear on the form. There is no required sequence to follow.

Table 74. Time Zone form fields

Field name	Description
Description	Enter a description (up to 60 characters). This description should include the name of the country and region as well as the GMT time offset. *Example: US-TX-United States-Texas-{GMT-6.00}*
Location ID	The location code based on the ISO 3166-1 standard (up to 10 characters).*Example:US-TX*
Locale	The name of the country (up to 60 characters). *Example: United States*
Region	The name of the region if there is more than one time zone (up to 60 characters). *Example: Texas*
City List	A list of some major cities in this specific region or country (up to 255 characters).*Example: Austin, Dallas, Houston, San Antonio*
Std. Bias (+/- HHMM)	The normal difference in hours and minutes of time in this location from UTC. UTC (Coordinated Universal Time) is more commonly referred to as GMT (Greenwich Mean Time) and is the basis for the worldwide system of civil time.
Enable DST	Click Yes to enable Daylight Savings Time. Click No to disable Daylight Savings Time.
DST Bias (+/- HHMM)	The normal difference in hours and minutes of time in this location from UTC. UTC (Coordinated Universal Time) is more commonly referred to as GMT (Greenwich Mean Time) and is the basis for the worldwide system of civil time.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Table 74. Time Zone form fields (continued)

Field name	Description
Time Zone DST	• Year (YYYY) The year that this DST is in effect • DST Start Date (YYYYMMDD) The date when Daylight Savings Time begins, in local time. • DST Start Time (HHMMSS) The time when Daylight Savings Time begins, in local time. • DST End Date (YYYYMMDD) The date when Daylight Savings Time ends, in local time. • DST End Time (HHMMSS) The time when Daylight Savings Time ends, in local time. • UTC Start Date (YYYYMMDD) The date when Daylight Savings Time begins, in UTC or GMT time. • UTC Start Time (HHMMSS) The time when Daylight Savings Time begins, in UTC or GMT time. • UTC End Date (YYYYMMDD) The date when Daylight Savings Time ends, in UTC or GMT time. • UTC End Time (HHMMSS) The time when Daylight Savings Time ends, in UTC or GMT time.
Edit Daylight Savings Time	• Year (YYYY) The year that this DST is in effect • DST Start Date (YYYYMMDD) The date when Daylight Savings Time begins, in local time. • DST Start Time (HHMMSS) The time when Daylight Savings Time begins, in local time. • DST End Date (YYYYMMDD) The date when Daylight Savings Time ends, in local time. • DST End Time (HHMMSS) The time when Daylight Savings Time ends, in local time. • UTC Start Date (YYYYMMDD) The date when Daylight Savings Time begins, in UTC or GMT time. • UTC Start Time (HHMMSS) The time when Daylight Savings Time begins, in UTC or GMT time. • UTC End Date (YYYYMMDD) The date when Daylight Savings Time ends, in UTC or GMT time. • UTC End Time (HHMMSS) The time when Daylight Savings Time ends, in UTC or GMT time.

Related procedures

To create, edit, or delete a Time Zone record:

1. Select **Configuration**, **Time Zone**, to display the **Time Zone** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Chapter 9 Area management

This chapter describes how to manage the different areas of access control in your system. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

Your Picture Perfect system uses readers to control access to doors. An area contains a group of one or more readers and doors. You can assign categories to these areas to restrict access to certain authorized badge holders.

The readers and doors must be defined in the system and logically grouped according to their location and the categories of access required. In order to accomplish these tasks, the following forms need to be completed:

- Categories
- Areas
- Readers
- Doors

Creating categories

Categories are both the locks and the keys of the Picture Perfect system. A category assigned to an area can act as a lock on the doors in that area. When you assign that same category to a badge, the category functions as the badge holder's key to those doors. There are 96 categories available for assignment to a badge, and 32 categories for assignment to an area or an area event.

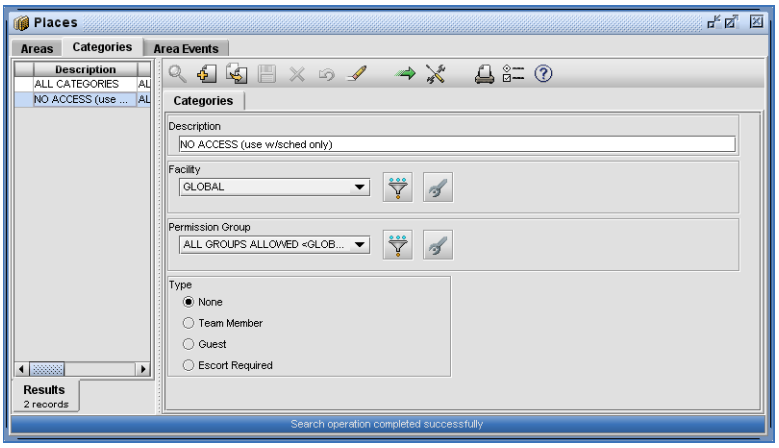
Use the Categories form to create descriptions of each group of people who use the facility. Categories describe users by type, title, group, or shift. Then associate each category with a permission group. The categories form a list box that is used on the Areas, Badges, Generator, and Area Events forms.

Note: A facility map helps identify categories of people who require access. The permission assigned to an operator determines what categories that operator can assign. See *Chapter 6 Operator administration.*

Example

The cleaning crew is required to clean the building from 5 PM to 8 PM. Create a category: Cleaning Crew 17:00-20:00

Figure 73. Categories form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 75. Category form fields

Field name	Description	
Description	Enter a category description up to 30 alphanumeric characters long.	
Permission Group	From the list box, select the permission group to be associated with the category.	
Type	None	Access to an M2MR controlled area is not permitted while M2MR control is enabled. This button is only available to operators with Occupancy Control permission granted. See *Occupancy control* on page 338.
	Guest	A Guest is not allowed entry to an M2MR controlled area unless two (2) team members are already present in the area. This button is only available to operators with Occupancy Control permission granted. See *Occupancy control* on page 338.
	Team Member	If an M2MR controlled area is empty, a Team member is allowed entry only with a second Team member. Additional team members can enter individually after the initial two (2) team members are present in the M2MR controlled area. Additionally, the final two (2) team members will not be permitted to exit until no Guests remain. This button is only available to operators with Occupancy Control permission granted. See *Occupancy control* on page 338.
	Escort Required	A badge with this category must be accompanied into an area by an escort with valid a non-Escort category match. See *Escort required* on page 390 for more information.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.	

Related procedures

To create, edit, or delete a Category record:

1. Select **Access**, **Places**, and then **Categories** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Creating areas

An area is a group of one or more readers. Identify functions within the facility that require the same kind of access control and give descriptive names to these areas. For example: Accounting, MIS, R&D, Lobby, Stairwells, Cafeteria.

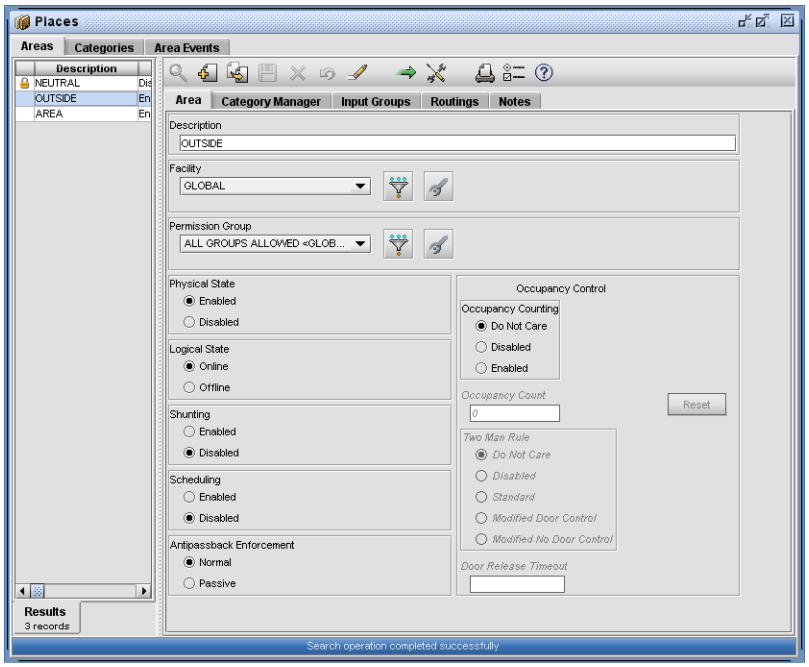
A single area may be assigned to multiple readers and doors. For example, the Accounting Management Area may be assigned to a reader using the Area button on the Readers form. The same area may be assigned to a door using the Area button on the Doors form. Additional readers and doors may be assigned to the same area, but an individual reader or door can only belong to one area.

The permission assigned to an operator determines which areas that operator can assign to readers and doors. See *Chapter 6 Operator administration*.

Example

The following areas require restricted access: Computer Room, the Archive Tape Room, and the MIS Equipment Room. Create an area called: High Security.

Figure 74. Areas form



Nested anti-passback

Nested anti-passback requires that readers be used only in a designated *sequence* to enter or leave a highly-secured area. For each reader that is defined as a nested anti-passback reader, you can specify which area of the building the badge is coming from and which area it is going to. For example, the reader may allow a badge to go from area 1 (e.g., main lobby) to area 2 (e.g., computer room).

The system remembers which area each badge (and each person) is in and updates this information whenever the badge is used and access granted at a reader (all valid transactions update the area of the person and badge). An anti-passback alarm or event is generated if the reader's From area does not match the badge's currently-recorded area. For example, an alarm or event is generated if the From area of the reader is area 3, but the badge is currently recorded as being in area 1. When an area is successfully entered, the new current area will be retained on both the badge that entered the area and on the person record. It is the last area on the person record (not the badge, as a person can have multiple badges) that is recorded by a controller on a reset or learn of a badge.

There are two default areas included in the Picture Perfect application:

- **Neutral** cannot be edited or deleted
- **Outside** can be edited but not deleted

The area on a new person record is set to NEUTRAL (a default area with id=-1). The controller grants access to a badge whose current area is NEUTRAL. The OUTSIDE area is a default area that represents the outside of the facility.

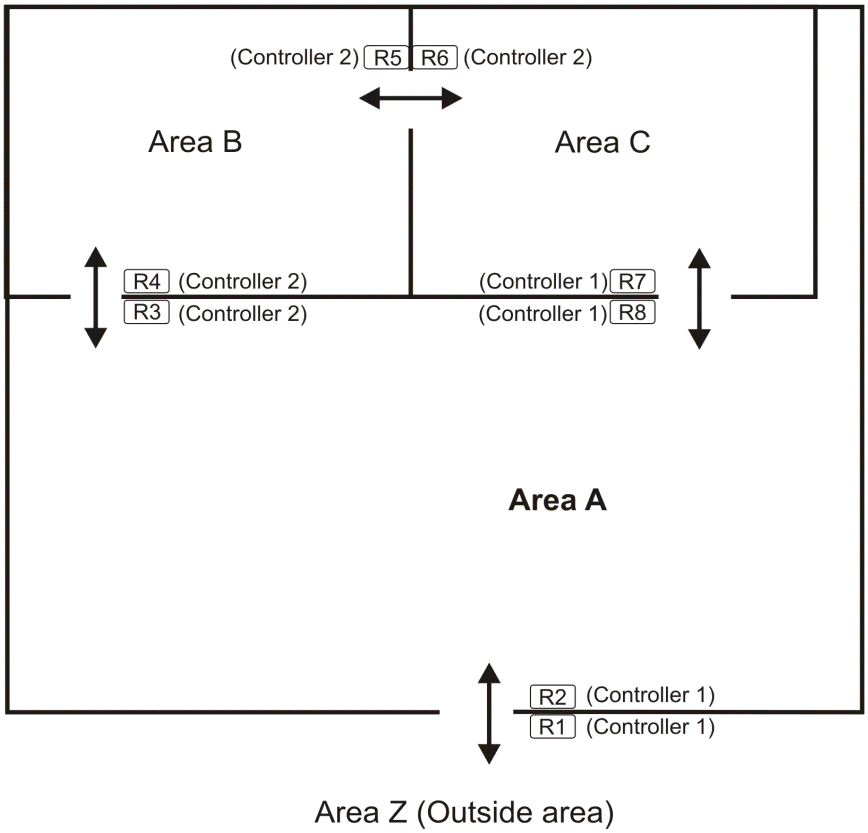
Note: If a badge's currently-recorded area and the From area (of the reader that the badge is being used at) get out of sync, either because of some violation of the system (e.g. a person has previously climbed over a turnstile) or for a legitimate reason (e.g. a person has passed through a fire exit during a fire drill), some means is required to bring the two back into sync. This can be accomplished from the Person form by resetting the last access area to NEUTRAL, so that the next transaction at a nested anti-passback reader is always accepted without violation, and the reader's To area becomes the badge's new area.

To accommodate different performance requirements, the system supports two methods of obtaining the Nested APB status of a badge prior to allowing access. These methods are only to support the Nested APB feature (available on the Reader form when the reader is the Global Nested APB type).

- **Host Broadcasts to Controllers.** This method broadcasts the badge’s last access area status to all associated controllers for each incoming valid APB legacy and nested transaction at the host; this is primarily used for individual, high-traffic readers that need to avoid longer wait times.
- **Controller Requests from Host.** This method relies on the controllers requesting the badge’s last access area status on a per-transaction basis before evaluating access; this involves less overhead (network traffic) at the host, but imposes a longer wait time at the reader for the badgeholder if the host is processing many learn requests at that time.

  “Fail Safe” and “Fail Secure”
  To accommodate different offline behaviors when using the Controller Requests from Host method, there are two modes of operation (Fail Safe and Fail Secure) that can be configured on a per reader basis for readers that have been configured for Global Nested APB operations. If the controller has lost communication with the host and the reader is configured for "Fail Secure," no access is granted at nested APB readers. If the controller has lost communication with the host and the reader is configured for "Fail Safe," access is granted based on categories but not based on the "From" area.

Figure 75. Anti-passback example transactions



Here are the transactions in order with resulting current area after each:

Table 76. Anti-passback example transactions

Person/Badge Last Access Area	Transaction	Person/ Badge Current Area	Controller 1 Person Area (Host Broadcast to Controllers)	Controller 2 Person Area (Host Broadcast to Controllers)	Controller 1 Person Area (Controller Requests from Host)	Controller 2 Person Area (Controller Requests from Host)
Neutral	Initial State	Neutral	Neutral	Neutral	Neutral	Neutral
Neutral	Badge at Reader 1, enters Area A	Area A	Area A	Area A	Area A	Neutral
Area A	Badge at Reader 3, enters Area B	Area B	Area B	Area B	Area A	Area B
Area B	Badge at Reader 5, enters Area C	Area C	Area C	Area C	Area A	Area C
Area C	Badge at Reader 7, enters Area A	Area A	Area A	Area A	Area A	Area C

Nested APB Configurations

Two APB configurations are supported:

- Global Nested APB
- Timed (Local) Nested APB

Global Nested APB - Host Broadcasts to Controllers

The current area status of a badge is synchronized across all relevant controllers on a server (for example, in an Enterprise system at a subhost, but not to the nethost or other subhost controllers).

On all valid APB legacy and nested transactions (VALID_APB_IN, VALID_APB_OUT, PASSIVE_APB_IN, PASSIVE_APB_OUT, VALID_NESTED_APB, PASSIVE_NESTED_APB, FAIL_SAFE) that occur, all controllers (except dial-up) that know the badge and have at least one Host Broadcasts to Controllers type, Global Nested APB reader are notified of the Current Area of the badge.

Global Nested APB - Controller Requests from Host

When Global Nested APB is configured to Controller Requests from Host, every controller will request the "Current Area" for the person the badge belongs to (since the person's current area may have been set from a different badge on that person) from the host for each nested APB transaction that is about to occur prior to evaluating access, when the badge is presented to a reader.

This approach has the least overhead at the host, but will incur longer wait times on badge learn transactions at a Nested APB reader.

Timed (Local) Nested APB

The current area status of a badge is not synchronized across controllers on a server. The status is known local to each controller. The controller will reset the current area status back to NUETRAL once the timeout period has expired.

Note: Local/Timed Nested APB is only useful if all readers are on a single controller.

Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 77. Areas form fields

Field name	Description	
Description	Type an area description up to 30 alphanumeric characters long. *Example: Lobby* The lobby area may include more than one location if the facility has multiple entrances or buildings. An area may be one contiguous physical space (such as the Computer Room) or it may be a number of separate but related spaces that require the same level of access control. *Example: Computer Room, MIS Lab, Computer Vault, MIS Equipment Room*	
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.	
Permission Group	Click display the Permission Group list box. Select the desired permission group for this area to identify operators who can assign this area to readers and doors.	
Physical State	Enabled indicates that the system allows readers in this area to read badges. Disabled indicates that the system does not allow the area's readers to operate.	
Logical State	Online indicates that the readers in this area operate in normal mode. Offline indicates that the readers are not allowed to unlock doors, but are allowed to read badges, pass badge data, route and archive access messages, and activate associated alarms.	
Shunting	Enabled indicates that the system allows use of keypad override of shunt time on doors and readers in this area. Disabled indicates that shunting is not allowed. This has no effect on Door Held Open or Door Forced Open. See Held Open Sensing on the Doors form and Shunting on the Reader form.	
Scheduling	Enabled indicates that the system recognizes scheduled changes associated with this area. Disabled indicates that the system ignores scheduled changes.	
Antipassback Enforcement	If anti-passback is set to Normal for this area, it works in conjunction with the anti-passback status setting on each badge used to access this area. If set to Passive, anti-passback will not be enforced in this area which means that access will be granted regardless of the anti-passback status. However, violations will still be reported. See APB Control on the Personnel form.	
Occupancy Control	Occupancy Counting	The ability to control occupancy counting is available only if the operator has occupancy control permission granted. See *Occupancy control* on page 338. When enabled, it allows the number of persons in a controlled space to be monitored. The occupancy count is reset to zero and the two man rule radio buttons are enabled. When disabled, the two man rule mode is forced to disabled and the two man rule radio buttons are grayed out and not selectable. Picture Perfect will update the occupancy count when a valid entry or exit to/from the area occurs. The default is for this to be disabled.
	Occupancy Count	The value in this field shows the current occupancy count for the area.
	Reset	This button is enabled only if the operator has occupancy control permission granted and occupancy counting has been enabled. It allows the occupancy count for an area to be reset to zero.

Table 77. Areas form fields (continued)

Field name	Description	
Two Man Rule Control	These radio buttons are enabled only if the operator has occupancy control permission granted and occupancy counting has been set to Enabled. Two man rule (2MR) or modified two man rule (M2MR) can only be enabled if the occupancy count is zero. If the operator violates this rule, an error message will appear in the status window. The record cannot be saved unless the count is reset to zero or two man rule mode is set to Disabled.	
	Disabled	Select this radio button to deactivate two man rule mode if it is currently enabled.
	Standard	Select this radio button to activate the standard two man rule mode which ensures that at least two badge holders occupy a given controlled space.
	Modified Door Control	Select this radio button to activate the modified two man rule mode which restricts access to a controlled area based on their M2MR category type. The first two badge holders to enter a controlled space must be of the Team member category type and at least two Team members must be present in the controlled space until all Guests have exited. Additionally, a Team member within the controlled space must press a door release button in order to allow entry to any subsequent badge holders. The door release button must be pressed within the time specified in the Door Release Timeout field or the door will not be unlocked.
	Modified No Door Control	Select this radio button to activate the modified two man rule mode which restricts access to a controlled area based on their M2MR category type. The first two badge holders to enter a controlled space must be of the Team member category type and at least two Team members must be present in the controlled space until all Guests have exited.
	Door Release Timeout	This field is enabled only if the operator has occupancy control permission granted. Valid values range from 0 (no timeout) to 32767 seconds.
Category Manager	This tab contains the active categories, ordered by slot number, that can be assigned to an area or an area event. To access an area, a badge must match at least one category that is assigned to that area. You may add, remove, or replace a category in a slot. Click Filter to enter search criteria to limit the category list or use the type ahead search feature by clicking in any cell and typing the first letters of the item for which you are searching. For more information, see *Category manager* on page 244. **Note:** This field is position sensitive when used in conjunction with area category schedules.	

Table 77. Areas form fields (continued)

Field name	Description	
Input Groups	Invalid	The input group to trigger when an invalid badge error condition occurs: • Deleted - The badge presented has been deleted from the Picture Perfect database. • Invalid PIN number - The PIN number entered in the keypad reader does not match the PIN number in the badge record. • Category mismatch - The category identified in the badge record does not match the area category where the badge read occurred. Click the Invalid Grp button to display the Ingroups list box. Select the desired Input Group, and then click Close.
	Suspended	The input group to trigger when a suspended badge read occurs. A suspended badge is one that has been identified in its badge record as suspended. Click the Suspended Grp button to display the Ingroups list box. Select the desired Input Group for a suspended badge read, and then click Close.
	Lost	The input group to trigger when a lost badge read occurs. A lost badge is one that has been reported and identified in its badge record as lost. Click the Lost Grp button to display the Ingroups list box. Select the desired Input Group for a lost badge violation, and then click Close.
	Unknown	The input group to trigger when an unknown badge read occurs. An unknown badge is one whose BID (The hidden number that uniquely identifies each badge) is not recorded in the Badges table of the Picture Perfect database and therefore is not recognized by the system. Click the Unknown Grp button to display the Ingroups list box. Select the desired Input Group for an unknown badge violation, and then click Close.
	Antipassback	The input group to trigger when an anti-passback violation occurs. When used in conjunction with anti-passback readers, the anti-passback status (In, Out, or Privileged) of a badge plus a category match, regulate its ability to open a door. *Example: If a badge holder starts to enter an anti-passback area by swiping their badge, then allows the door to close without entering, he will not be able to re-enter that area because the system has already registered him as In.* Click the Antipassback Grp button to display the Ingroups list box. Select the desired Input Group for an anti-passback violation, and then click Close.
	Duress	The input group to trigger when a valid duress-code badge read occurs. Duress codes can be used with Badge and Keypad or Keypad readers to alert the system that a valid badge read was made under forced conditions or duress. Click the Duress Grp button to display the Ingroups list box. Select the desired Input Group for a duress-code entry, and then click Close. **Note:** Do not assign a reader's valid input group to one of the above groups. This will result in an unlocked door.

Table 77. Areas form fields (continued)

Field name	Description	
Routings	Select routings for the following types of conditions:	
	Route Definition	Select the desired route definition for this area. This route definition is used for Activity Monitor routing. If this field is left blank, this area's activity will be routed to all operators.
	Invalid Routing	Click the Invalid Routing button to display the Routings list box. Select the desired routing for an invalid badge read, and then click Close.
	Suspended Routing	Click the Suspended Routing button to display the Routings list box. Select the desired routing for a suspended badge read, and then click Close.
	Lost Routing	Click the Lost Routing button to display the Routings list box. Select the desired routing for a lost-badge read, and then click Close.
	Unknown Routing	Click the Unknown Routing button to display the Routings list box. Select the desired routing for an unknown badge read, and then click Close.
	Antipassback Routing	Click the Antipassback Routing button to display the Routings list box. Select the desired routing for a valid anti-passback transaction, and then click Close.
	Escort Routing	Select the desired routing for a valid escort transaction. See *Escort required* on page 390 for more information.
	Valid Routing	Click the Valid Routing button to display the Routings list box. Select the desired routing for a valid badge read, and then click Close.

When you assign an area to a door or a reader, the categories (and controls) defined for the area become valid for all doors and readers that belong to that area.

Some of the controls on the Areas form are also available on the Doors form and the Readers form. In some cases, this may allow an individual door or reader to have controls that differ from the assigned area. Table 78 lists the controls that Areas, Readers, and Doors have in common.

Table 78. Common controls

Areas	Readers	Doors
Scheduling	Scheduling	Scheduling
Shunting	Shunting	
Physical State	Physical State	
Logical State	Logical State	
Note: A setting of Disabled in any of these fields on any of these forms overrides a setting of Enabled in the same field on another form. For example, if Shunting is Enabled for an area, but a reader in that area has Shunting Disabled, the Shunting feature will not work for that reader. Shunting must be set to Enabled on both the Areas and Readers forms.		

Related procedures

To create, edit, or delete an Area record:

1. Select **Access**, **Places**, and then **Areas** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

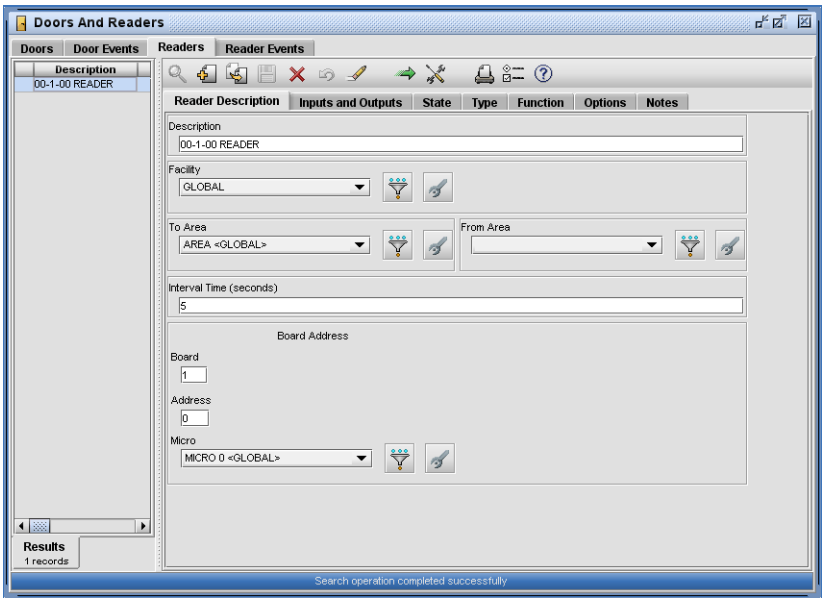
Defining readers

Use the Readers form to define how each reader operates and to associate the reader with an area, a micro, and input group so that the system can process reader activity.

Example

A bank vault employs the added security offered by the Two Man Rule option, requiring a minimum of two occupants in the area. The door to the vault room is controlled by a reader. The vault reader is wired to the following address: *01* (Micro 1) - *1* (Reader board 1) -*00* (the address on the board).

Figure 76. Readers form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 79. Readers form fields

Field name	Description
Description	Type a reader description up to 60 characters long. *Example: 00-1-00 LOBBY DOOR*
Board	Type the board number of the reader board where this reader is connected. See *Table 69, M5 wiring chart - Outputs* on page 160 of *Chapter 8 Device management*.
Address	Type the physical address of this reader on its reader board. See *Table 69, M5 wiring chart - Outputs* on page 160 of *Chapter 8 Device management*.
Micro	Click the Select Micro button to display the Micros list box. Select the micro where this reader is wired.
Facility	Click the Facility list box to display a list of available facilities. The facility set determines which facility will be able to view the associated badge and trace activity on the Activity Monitor if the Badge and Trace options are selected. By default, the reader record will be assigned the same facility as the micro to which the reader is assigned however, you do have the ability to manually re-assign a reader's facility. This might be desirable in a case where one micro controls more than one facility, for instance two companies occupying the same building that use separate doors for entry/exit. For more information, see *Creating facilities* on page 53.
To Area	Click the To Area list box to display a list of available areas. Select the area that this reader protects, and then click Close. The area that you select should have categories and controls appropriate for this reader.
From Area	Click the From Area list box to display a list of available areas. If configuring a nested APB reader, select an area. Refer to Nested APB in this table for more information.
Interval Time	Type the maximum number of seconds allowed to elapse between stages of a transaction, such as entering a PIN number in a keypad reader after a badge swipe, and/or between separate badge transactions on a double-badge reader. (See *Double-badge function* on page 366 for details on this feature.) The time starts after the first transaction.
Valid In Group	Click to display the Input Groups list box. Select the input group to be triggered when a valid badge is swiped through this reader. **Note:** Only Trigger on Input (Individual) which are non-boolean input groups, are displayed in the list box. See *Boolean Type* on page 130.
Invalid In Group	Click to display the Input Groups list box. Select the input group to be triggered when an invalid badge is swiped through this reader. **Note:** Only Trigger on Input (Individual) which are non-boolean input groups, are displayed in the list box. See *Boolean Type* on page 130.

Table 79. Readers form fields (continued)

Field name	Description	
Two man rule output	A drop down list from which you may optionally select an output to associate with an indicator device, such as a blinking light. The indicator device will be activated when the first of two required valid badge reads for entry or exit from a two man rule enabled area has occurred at the reader. When the indicator device is activated, the second person should present their badge at the reader before the timeout period expires, in order to unlock the door to permit entry or exit from the area. The indicator will be deactivated when a timeout or a second valid badge read or an invalid badge read occurs at the reader. The Two man rule output is a digital output (DO) point configured to control the indicator device. The value in the drop down list may only be changed by an operator with Occupancy control permission granted.	
Physical State	Enabled means this reader is allowed to read badges. Disabled means the reader cannot read badges. **Note:** If a reader is not operational, set Physical State to Disabled.	
Logical State	Online permits the normal operating mode for this reader. Offline means the reader is allowed to read badges, pass badge data, route and archive access messages, and activate associated alarms -- but is not allowed to unlock associated doors.	
Number of Badges	Single means the reader requires only one valid badge read to open the door. Double means the reader requires two separate valid badge reads to open the door.	
Physical Reader Function	Select the desired physical reader type for this reader:	
	Badge Only	A reader used only to read badges using a badge swipe.
	Keypad Only	A reader used only as a keypad, where, in lieu of a badge swipe, the badge encode number must be entered using the keypad. Press * or +, enter the badge encode number, and then press #.
	Badge and Keypad	A badge reader used in conjunction with a keypad, where a PIN, a duress code, a shunt override code, or an alarm response code can be entered in addition to the badge swipe. See the procedures for each type of code below: PIN or Duress Code • Swipe the Badge. • Press ***** or **+** , enter the PIN or Duress Code, and then press **#**. • Shunt Override Code • Press ***** or **+**, enter the Shunt Code, and then press **#**. • Swipe the Badge. • Press ***** or **+**, enter the PIN or Duress Code, and then press **#**. Alarm Response Code • Press ***** or **+**, enter the Alarm-Response Code, and then press **#**. • Swipe the Badge. • Press ***** or **+**, enter the PIN or Duress Code, and then press **#**.
	Badge or Keypad	The reader can be used either as a badge reader or a keypad. If Badge is selected, then the reader is used only to read badges using a badge swipe. If Keypad is selected, the badge encode number is entered using the keypad in lieu of a badge swipe. Press * or +, enter the badge encode number, and then press **#**.

Table 79. Readers form fields (continued)

Field name	Description	
Swipe and Show Control	This feature is only visible when the optional Image package is installed. See *Monitoring Swipe and Show activity* on page 274 for more details on Swipe and Show.	
	Swipe and Show	Select Enabled to enable Swipe and Show on this reader. Select Disabled to disable Swipe and Show on this reader. **Note:** A reader cannot be defined as Toggle when Swipe and Show is Enabled. See *Toggle* on page 186.
	Authorization Required	Select Yes to designate a reader that will display a photo in a popup window beside the Activity Monitor and require an operator to unlock a door. Select No to designate a reader that will display a photo in a popup window beside the Activity Monitor and will unlock a door without operator intervention. **Note:** The Yes and No buttons are not available unless Swipe and Show is Enabled. Access cannot be granted through readers defined as Authorization Required while communications to the micro are down.
Logical Reader Function	Select the desired Logical Reader Function for this reader:	
	Normal	Used to grant access into an area.
	Anti-Passback In	Used to log a badge holder “in” when entering.
	Anti-Passback Out	Used to log a badge holder “out” when exiting.
	Time and Attendance In/Out	Used to log a badge holder “in” and “out” using the same reader (such as the Model 100 Wiegand reader) by swiping the badge the normal way for “in” and reversing the badge or turning the badge backwards for “out”.
	Time and Attendance In	Used to log a badge holder “in” at the start of a work shift.
	Time and Attendance Out	Used to log a badge holder “out” at the end of a work shift
	Nested APB	Used to configure APB on nested areas.
APB	If the Logical Reader Function is set to APB In, APB Out, or Nested APB, select the desired APB Type for this reader:	
	Global APB	Used as the default, this allows the host to share APB status/nested APB area status with participating controllers.
	Timed APB	Used to designate the reader as a Timed APB reader in which a badge holder’s APB status/nested APB area will return to Neutral after a defined period of time. A Timed APB reader is useful in a site where a badge holder may enter a site by going through an APB reader but is not required to exit the site by going through an APB reader. If this option is selected, a Timed APB Duration must also be defined. A Timed APB status/nested APB area is local to the micro.
	Reset Timed APB Immediately	Used to reset the Timed APB status/nested APB area back to Neutral immediately following a badge swipe.

Table 79. Readers form fields (continued)

Field name	Description	
	Timed APB Duration	Enter a value to represent how long a badge holder's Timed APB status/nested APB area will be set when their badge is used on the reader. The Timed APB Duration cannot exceed one day. A duration of 0 allows the micro to reset the status to Neutral immediately, producing the same effect as Reset Timed APB Immediately.
	Global Nested APB Status Method	This control is enabled only if Nested APB under Logical Reader Function has been chosen. Host Broadcasts to Controllers - The host actively sends nested APB area information to participating controllers. Controller Requests from Host - The controller requests nested APB area information from the host as needed.
	Global Nested APB Micro Offline Operation Mode	This control is enabled only if Controller Requests from Host has been chosen. Fail Safe - While the controller is offline, the controller will not consider nested APB area information when granting access. Fail Secure - While the controller is offline, the controller will deny access to nested APB readers. **Note:** There is a period of time when the controller loses communication with host, where it is not offline yet and during this time, when a badge is swiped on a Controller Requests From Host type (Fail Safe) reader, a learn timeout is generated. Once the controller is offline, the fail safe/fail secure rules are followed to provide or deny access.
Scheduling	Enabled means established schedule changes will control this reader. Disabled means established schedule changes will not affect this reader.	
Shunting	Enabled means this reader allows the use of keypad override of shunt time. Disabled means the reader will not allow shunting. When enabled, the Alarm Shunting feature allows a valid badge holder to keep a door open (for the time specified, in minutes, in the Keypad Shunt Time field of the Doors form) without getting a Door Held Open alarm. The badge holder enters the shunt code (defined on the Micros form) using the reader keypad, presents their badge, and then enters their PIN number.	
Toggle	A reader used in special applications only, in which a badge swipe toggles the reader's valid input group (non-boolean) On (yes) or Off (no), such as to arm/disarm a burglar alarm system. Toggle readers are not intended for door control, but can be used that way with some limitations. To do this, the door must be configured without a sensor, and the doorstrike output must be configured to reset with an input rather than on duration. With this configuration, the reader can toggle the door between locked and unlocked, but since there is no sensor, there can be no detection of the door being forced open or held open too long. For an example of toggle-reader use, see *Creating input groups* on page 127 of *Chapter 8 Device management*. **Note:** If Toggle is set to Yes and Authorization Required is set to Yes, photos are displayed for invalid transactions, but not valid transactions. See *Monitoring Swipe and Show activity* on page 274.	
Limited Usage	Selecting Enabled defines the reader as a limited usage reader, which will only grant access to a badge holder for the number of times specified in the Usage Count field of the Badges form. There is no limit to the number of readers that can be defined as limited usage readers. See *Chapter 11 Badge management* for related information. The count must be manually reset.	

Table 79. Readers form fields (continued)

Field name	Description
Elevator Reader	Selecting Yes defines the reader as an elevator reader. A maximum of 16 readers on a micro can be configured as elevator readers. **Note:** Swipe and Show cannot be enabled when the reader is defined as elevator. See *Elevator control* on page 369 for related information.

Related procedures

To create, edit, or delete a Reader record:

1. Select **Configuration**, **Doors and Readers**, and then **Readers** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Defining doors

Use the Doors form to define how each door operates. Depending on the features that it should have, you may want to associate the door with an area and with inputs, input groups, and outputs--so that the system can process door status information and operate optional door hardware or alarm devices.

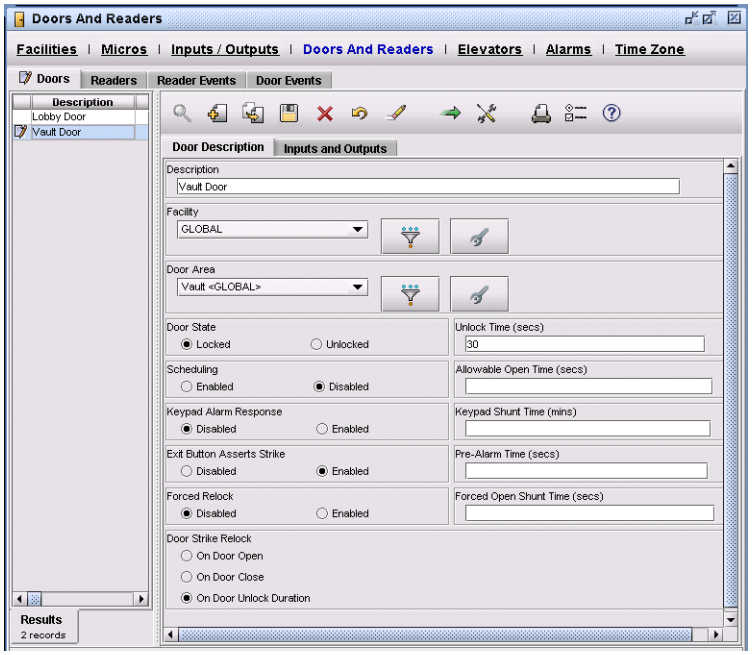
The Doors form links all access and control features of the physical door. These include mechanical and electronic locking devices that keep the door opened or closed, such as: door strikes, magnetic locks, exit buttons, and push bars. They also include sensing and monitoring devices such as door sensors, exit requests, and alarm points. The Doors form fields required for activation of particular features are listed with those features below. Depending on the features required for each door, all fields may or may not be applicable.

Note: To ensure proper operation when the micro runs offline, the door sensor, reader, door strike, and exit button must be wired to the same micro.

Example

The vault area of ABC Bank is accessed through a door equipped with an exit button.

Figure 77. Doors Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 80. Doors form fields

Field name	Description
Door Values	Define the door and the times allowed before alarms are enabled.
Description	Type a door description up to 60 alphanumeric characters long.
Unlock Time (secs)	Enter the number of seconds that this door may remain unlocked due to a valid badge read or an exit button being pushed. This field controls how long the door strike is unlocked for the badge holder to open the door. After that, the Allowable Open Time controls how long the badge holder may keep the door open while the badge holder is passing through.
Forced Open Shunt Time (secs)	Enter the number of seconds that the Door Forced Open alarm will be shunted before an alarm is generated. When the shunt time expires, the Door Forced Open alarm is enabled. The number of seconds set here must be greater than the Unlock Time. This field controls how long a door strike will remain unlocked after the Unlock Time expires so a badge holder can open the door and not get a Door Forced Open alarm.
Allowable Open Time (secs)	Enter the number of seconds that this door may be open (due to a valid badge read) before an alarm condition exists. Be sure to set the Held Open Sensing button to Detected (in the Door Control box) to activate this feature.

Table 80. Doors form fields (continued)

Field name	Description
Keypad Shunt Time (mins)	Enter the number of minutes that this door may remain open due to a badge holder entering an override code into a keypad reader. *Example: Shipping and Receiving may use the override time to keep a shipping door open beyond the Allowable Open Time.*
Door Area	Click Door Area to display the Areas list box. Select the desired area for this door. If a reader is associated with this door, select the same area that is assigned to the reader.
Strike Output	Click the Strike Output button to display the Outputs list box. Select the desired door strike output associated with this door, and then click Close. The door output is a digital output (DO) point associated with the door strike. **Note:** Select a door strike output that is wired to the same micro as the associated door sensor input. The system displays a popup message to the operator if an output point is selected on the wrong micro.
Facility	Click Facility to display the facilities list box. By default, the door record will be assigned the same facility as the micro to which the door is assigned however, you do have the ability to manually re-assign a door's facility. This might be desirable in a case where one micro controls more than one facility, for instance two companies occupying the same building that use separate doors for entry/exit. For more information, see *Creating facilities* on page 53.
M2MR Output	Click M2MR Output to display a list box from which you may optionally select an output to associate with a warning device, such as a horn or a strobe light. The device is used by the Modified two man rule with door control to notify the team members in an area that a person desiring access has presented a valid badge at the reader. The M2MR output is a digital output (DO) point configured to control the warning device. The value in the list box may only be changed by an operator with Occupancy control permission granted. When the warning device is triggered, team members in the area should press the button connected to the exit button input before the door time-out has elapsed (at which point the warning will terminate) to cause the door to unlock and allow entry to the area. The M2MR output must be physically located on the same micro as the strike output.
Door Sensor	Click Door Sensor to display the Input list box. Select the desired input for this door sensor. A door sensor is associated with a digital input (DI) point connected to a door sensor. **Note:** Select a door sensor input that is wired to the same micro as the associated door strike output. The system displays an operator message if you select an input point on the wrong micro. Do not attach an input group to the input unless the input is a supervised input.
Exit Button	Click Exit to display the Inputs list box. Select the desired input for this exit button. Be sure the Exit Button Asserts Strike field (in the Door Control box) is set to Enabled. **Note:** Select an exit button input that is wired to the same micro as the associated door strike output. The system displays an operator message if you select an input point on the wrong micro. Make sure the exit input is tied to the reader's valid input group.
Forced Open In Group	Click to display the Input Groups list box. Select an input group to activate. The associated alarm will be triggered when a Forced Open condition occurs. (Be sure the Forced Open Monitoring field is set to Detected.) **Note:** Only Trigger on Input (non-boolean) input groups are displayed in the list boxes.
Held Open In Group	Click to display the Input Groups list box. Select an input group to activate. The associated alarm will be triggered when a Held Open condition occurs. (Be sure the Held Open Sensing field is set to Detected.) **Note:** Only Trigger on Input (non-boolean) input groups are displayed in the list boxes.

Table 80. Doors form fields (continued)

Field name	Description	
Pre-Alarm In Group	Click to display the Input Groups list box. Select an input group to activate. The associated alarm will be triggered when a Pre-Alarm condition occurs. (Be sure the Pre-Alarm field is set to Enabled.) **Note:** Only Trigger on Input (non-boolean) input groups are displayed in the list boxes.	
Door State	Indicate whether the door is normally Locked (pending a valid badge read or other event) or Unlocked.	
Scheduling	Select Enabled to allow scheduled changes set for this door to take place. Select Disabled to prevent scheduled changes set for this door from taking place.	
Held Open Sensing	Select Detected to allow an alarm condition to occur on this door when the door remains open (with a valid badge reader or exit button) for too long, based on the Allowable Open Time (set in the Door Values box). Select Ignored if the sensing function on this door is not used.	
Forced Open Monitoring	Select Detected to allow an alarm condition on this door to occur immediately when the door is forced open without a valid badge read or exit device. Select Ignored if the Monitoring function on this door is not used.	
Exit Button Asserts Strike	Select Enabled to allow an exit button to unlock this door for the number of seconds in the Unlock Time field and remain open for the number of seconds in the Allowable Open Time field (both set in the Door Values box). Be sure to make a selection in the Exit Button field in the Inputs box. Select Disabled if an exit button is not allowed to unlock this door but will shunt the door DI.	
Pre-Alarm	Select Enabled to allow the Pre-alarm Notification feature to activate. See *Pre-alarm notification* on page 381 for details on this feature. Select Disabled if the Pre-alarm Notification feature is not used. **Note:** Input groups for the above can be generic, that is, one input group and alarm can be used by all doors for forced, held, and pre-alarm.	
Keypad Alarm Response	Select Enabled to allow the Keypad Alarm Response feature to activate. See *Controlling alarms using a keypad code* on page 384 for details on this feature. Select Disabled if the Keypad Alarm Response feature is not used.	
Forced Relock	If enabled, this feature provides further security by locking a door if a second person presents a badge to the reader before the first person opens the door. *Example: If a person badges into a reader but does not open the door, and a second person badges into the same reader before the first person's Unlock Time expires, the door will immediately lock. This will show on the Activity Monitor as two Double Door Locked transactions (one for each person).*	
Door Strike Relock	Door Strike Relock provides additional security by incorporating the ability to relock the door upon a door opening or closing, or after a specified period of time.	
	On Door Open	When the door is opened, the door strike will relock. Do not use this option if you are using magnetic locks with built-in door open sensors.
	On Door Closed	When the door is closed (after being open), the door strike will immediately relock.
	On Door Unlock Duration	The door strike will relock after the Unlock Time (set in the Door Values box) has expired.

Related procedures

To create, edit, or delete a Door record:

1. Select **Configuration**, **Doors and Readers**, and then **Doors** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

To define a door sensor:

A door contact functions as a sensor for two door-open conditions: Door Open Too Long and/or Door Forced Open.

If you are using the alarm shunting function on a door, when a valid badge unlocks the door strike and the badge holder opens the door, the system begins to count the number of seconds of Allowable Open Time. If the door is still open when this time elapses, an associated alarm can occur.

If you are using the monitoring function on a door, when a door is forced open, an associated alarm can occur immediately.

Note: You must define this sensor input (on the Inputs form) before you can select the appropriate Door Sensor Input (on the Doors form).

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. Click **New** .
3. Complete the following fields of the Doors form.
   - Description
   - Forced Open Shunt Time
   - Allowable Open Time
   - Keypad Shunt Time (optional - so the badge holder can use a code to override the Allowable Open Time).
   - Held-Open Sensing
   - Forced-Open Monitoring
   - Input Groups (Forced Open/Held Open/Pre-Alarm)
   - Inputs, Door sensor (associated with a DI point wired to the door sensor)
4. Click **Save** .

To define a door strike setting:

A door strike associated with a reader (and/or an exit device) releases to unlock a door when a valid badge read occurs (or when an exit device is pushed).

When the door strike releases, the system starts counting the Unlock Time set for the door strike and then closes the door strike when the time elapses. The badge holder opens the door during the Unlock Time.

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. Click **New** .
3. Complete the following fields of the Doors form.

- Description
- Unlock Time
- Strike Output DO (digital output point wired to the door strike)

4. Click **Save** .

To define an exit device:

An exit device releases the door strike on a door. Exit devices are often used on lobby doors. The exit button is associated with a door strike so that the latch unlocks (and the sensor is shunted) when the exit button is pushed. You can enable the exit button and define how long the latch remains unlocked using the Doors form.

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. Click **New** .
3. Complete the following fields of the Doors form.
   - Description
   - Unlock Time
   - Exit Button Asserts Strike - Enabled
   - Strike Output DO (digital output point wired to the door strike)
   - Inputs, Exit Button
4. Click **Save** .

Chapter 10 Schedules and modes

This chapter describes how to create modes, how to change your system to a different operating mode (by schedule or command), and how to schedule events within a mode. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

Schedules allow you to change a variety of operational characteristics based on mode, day of week, and time of day. Using the Schedule feature, you can specify when you want a particular type of change to occur. That change will remain in effect until overridden by another schedule or mode event, or manually changed by an operator.

Picture Perfect supports multiple modes of operation, such as emergency and non-emergency modes. Examples of non-emergency modes are Normal or Holiday mode; examples of emergency modes are Fire or Lockdown. When you initially set up the system, make sure that all the values and schedules that you define (for readers, doors, areas, etc.) are associated with your normal operating mode. Weekdays and weekends occur within your normal operating mode, so the system does not need a unique "weekend mode." An "evening mode" is not required either, as the normal mode can contain schedules for multiple shifts and weekends.

To operate the system in a different mode during holidays (or other special events based on the calendar), you must create a mode, re-define the schedules to occur during that mode, and then schedule the mode to become active on a selected date and time.

When a mode becomes active, it remains active until changed by an operator (Change Mode), another scheduled Mode Event, or by a DI-triggered emergency mode. A Mode Event is a scheduled change to one or more of the operating characteristics. Events can occur when a mode starts, when a mode ends, or at a given time of day and day of week within the mode. Typical events are locking and unlocking lobby doors for general access, turning on motion detectors after hours, and changing categories on areas to control access for shift workers.

Administrative procedures can also be scheduled, such as performing backups and running reports. For details on these procedures, see *Scheduling backup events* on page 219 and *Scheduling reports* on page 306.

Creating modes

Use the Modes form to define each system operating mode. Operating modes are an administrative decision, as each facility has unique requirements.

Examples of *scheduled* operating modes are Normal mode and Holiday mode. Examples of *command* operating modes are emergency modes such as Fire or Lockdown mode, which can be initiated by the operator at any time. (See *Changing modes by command* on page 196.) A mode that you can design to provide tighter security in case working conditions change from the routine is Restricted-access mode, which can be scheduled or commanded.

After a mode is created using the Modes form, you will define its characteristics by using the various Events forms.

Normal mode

Normal mode usually does not require any start/end events to be scheduled. A start/end event is something you schedule to happen once; it is not subject to weekly or 24-hour cycles.

Use runtime events to schedule the necessary cycles. You do not need "weekend" or "evening" modes, since the runtime events in a single mode allow you to set different operating characteristics for all days of the week and all times of the day.

Emergency modes

Create Emergency modes to handle situations such as fires, accidents, or other emergency situations. Define these modes on the Modes Tab > Mode Creation form by checking the Emergency Mode check box. Enter a description such as Emergency or Fire.

Emergency modes are usually activated by the operator using Mode Command, and typically use start/end events. Remember that most mode-start events require parallel mode-end events. Unless there are events that need to cycle during the emergency mode, you do not need to set up runtime events.

Holiday modes

Create Holiday modes to handle access-requirement changes during scheduled holidays. Define the mode on the Modes Tab > Mode Creation form using a description such as Holiday or Vacation.

Holiday modes are usually activated automatically by scheduling them using Mode Events, and typically use start/end events. Remember that most mode-start events require parallel mode-end events.

Be sure to schedule the start of a Holiday mode so that its events are timed properly in regard to events of the normal operating mode. For example, a setting of Holiday mode may be to leave the lobby doors locked. Normal mode, however, always unlocks the lobby doors at 7 AM. If Holiday mode starts on Monday morning at 8 AM, and no schedule has been created to lock the doors when the Holiday mode starts, the lobby doors will already have been unlocked by Normal mode an hour before; therefore, the lobby doors will remain in an unlocked state throughout the Holiday mode.

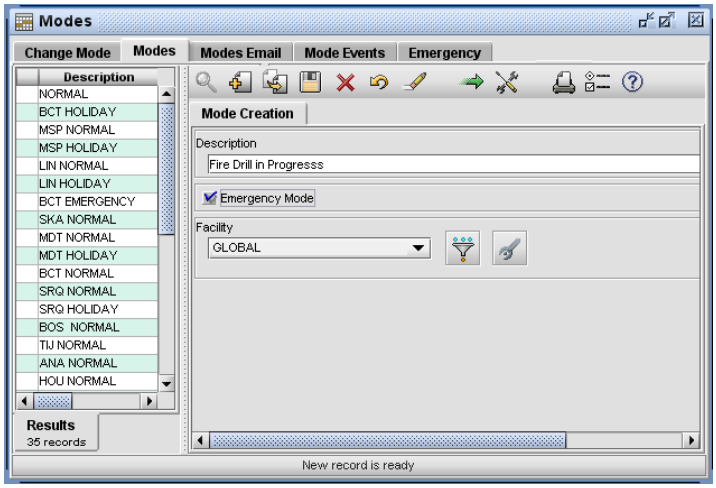
One way to keep the doors locked is to schedule Holiday mode to start when the doors are still in a locked state (prior to 7 AM). Another option is to make a mode-start event that locks the doors when Holiday mode goes into effect.

When you set up a Holiday mode, you do not need to set up runtime events unless you want weekly and daily cycles to occur. If you want any of the runtime events in your normal operating mode to occur during your holiday mode, you must duplicate those runtime events within Holiday mode.

Example

An Emergency mode allows you to conduct fire drills as needed to comply with safety requirements.

Figure 78. Modes form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 81. Modes form fields

Field name	Description
Description	Type any alphanumeric combination (1 to 60 alphanumeric characters) for Description. *Example: Emergency*
Emergency Mode	Click the Emergency Mode button if you want to designate this mode as an Emergency mode.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create, edit, or delete a Mode record:

1. Select **Control**, **Modes**, and then **Modes** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

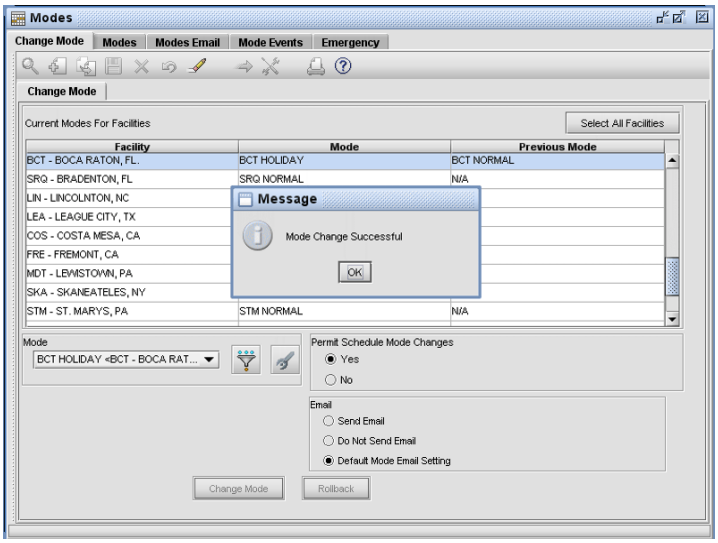
Changing modes by command

Modes can be changed by command, using the Change Mode form, or by schedule, using the Mode Events form. Use the Change Mode form to change your system operating mode immediately. For example, emergency events (such as fire, accident, or work disruption) require an immediate change to a different operating strategy. Mode Command lets you do this.

Example

While in Normal mode, change to Holiday mode.

Figure 79. Change Mode form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 82. Change Mode form fields

Field name	Description	
Current Modes for Facilities	This pane reflects the mode that is currently in effect, and the previous mode for each facility. Select a facility from this pane to rollback or change a mode. For more information, see *Creating facilities* on page 53.	
Select All Facilities	Click this button to select all active facilities.	
Mode	Click to display the Modes list box. Select the operating mode to which you want to change.	
Permit schedule mode changes:	Select Yes or No, to indicate whether you want the system to allow future mode changes to occur as scheduled. You can change this option even if you don't change the mode itself.	
	Yes	Select Yes to allow scheduled mode changes to occur.
	No	Select No to override scheduled mode changes in an emergency. *Example: If you change to an emergency mode on the day before a scheduled holiday and you permit scheduled mode changes to occur, the system will switch to holiday mode as scheduled. If you do not permit scheduled changes to occur, the system will stay in the emergency mode until you use the Mode Command form to change the mode again.*
Email	Send Email	Select Send Email to send a notification to all email addresses associated with the selected facilities.
	Do Not Send Email	Select if sending an email notification is not necessary.
	Default Mode Email Setting	Select to send an email as defined on the Modes form.
Change Mode	Click the Change Mode button to tell the system to change to the selected mode and/or to allow or disallow scheduled mode changes.	
Rollback	Select the Rollback button to revert back to the previous mode. **Note:** Rollback from Emergency mode is not allowed.	

Related procedures

To change mode by command:

1. From the Control menu, select Modes, then click the Change Mode tab.
2. Select one or more facilities that you want to change to the new operating mode.
3. Select the operating mode to which you want to change.
4. Select **Yes** or **No** on the field titled Permit Scheduled Mode Changes, to indicate whether you want the system to allow future mode changes to occur as scheduled. You can change this option even if you don't change the mode itself.
   - **Yes** allows scheduled mode changes to occur.

- **No** allows you to override scheduled mode changes in an emergency.

For example, if you change to an alternate mode on the day before a scheduled holiday and you permit scheduled mode changes to occur, the system, will switch to holiday mode as scheduled. If you do not permit scheduled changes to occur, the system will stay in the alternate mode until you use the Mode Command form to change the mode again.

5. Select an e-mail method under Email.
6. Click Change Mode to tell the system to change to the selected mode and/or to allow or disallow scheduled mode changes. A message window displays the message: Mode Change Successful.

Changing modes by scheduling a mode event

Use the Mode Event form to schedule a mode change such as from Normal to Holiday. To have the system return to normal operations when the mode event is over, schedule another mode event that activates Normal mode.

When the system enters a new mode, it does not execute events for the new mode that are scheduled to occur before the new mode starts. For example, if an event scheduled for 7 AM in normal operating mode unlocks the lobby doors, but the system does not return to normal mode until 8 AM, then the lobby doors will remain locked until the next day at 7 AM.

Exception: If communication with the micro is lost, when the micro resets it will go back to midnight and execute all events scheduled to begin from midnight until the current time. If the event that was in progress, when the micro reset, was scheduled to start before midnight, the micro will not recognize it and will default to the normal mode. To ensure that a schedule is restored when a micro resets, schedule events to begin after midnight, for example 00:01.

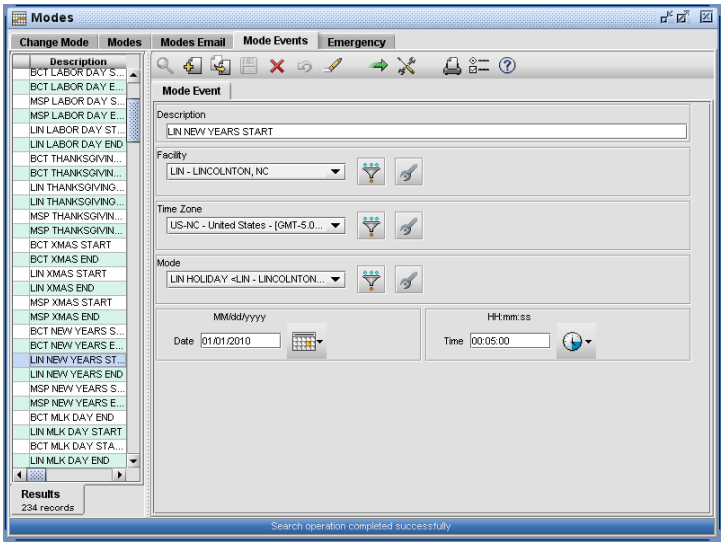
If you schedule or command the system to return to normal operating mode after the time when scheduled runtime events for normal mode are supposed to occur, it is a good idea to schedule start/end events such as unlocking (or locking) the lobby doors. See *Start/end events* on page 200.

It is important to note that if there are three or more modes in the system, activating an event at mode end does not determine the mode to which the system is switching. For example, assume the following three modes are in the system, Normal, Holiday, and Emergency. If the system is currently in Holiday mode, at the end of Holiday mode, the system could switch to either Normal or Emergency mode. Therefore, it is recommended that you activate an event at mode start, if there are three or more modes in the system.

Example

The New Year Holiday mode could be triggered by a New Year Start mode event scheduled at 5 AM on New Year's Day, then returned to Normal mode by an New Year End mode event scheduled at 7 AM on the day after New Year's Day.

Figure 80. Mode Events form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 83. Mode Events form fields

Field name	Description
Description	Type any alphanumeric combination (1 to 60 alphanumeric characters) for Description. *Example: Normal to Thanksgiving*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Time Zone	Select the time zone in which the micro is located from the drop-down list. This allows Picture Perfect to display badge and alarm activity in the micro's local time. See *Verifying time zones* on page 168. **Note:** In order for an operator to use this field, they must have at least *View* page level permission for the Time Zone form. See *Creating facility permission profiles* on page 81.
New Mode	Click New Mode to display the Modes list box. Select the mode that is to go into effect during this mode event, and then click Close to close the list box.
Date	Type the date this mode event begins or click the calendar button.
Time	Type the time this mode event begins or click the clock button.

Related procedures

To create, edit, or delete a Mode Event:

1. From the **Control** menu, select **Modes**, and then click the **Mode Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Events overview

Use the Events forms to define and schedule the desired characteristics for Area Events, Reader Events, Door Events, Alarm Events, Input Group Events, Output Group Events, Backup Events, or Report Events, and assign the appropriate mode to each of them.

Two types of event scheduling options are available: Runtime and Start/End.

- Runtime lets you schedule an event to cycle within a mode, and can occur at a particular time on any days of the week.
- Start/End schedules the event to take place only once, either at mode start or at mode end.

Note: Schedules that run on the micros can update the database. This is configurable on the Parameters form using the field Schedules Update Database. With this feature enabled, as long as there is communication with the micro, the host will reflect the scheduled state of the device. (For example, if a door is scheduled to unlock at 8 AM, the host record will be updated to reflect the change.) If this feature is disabled, the host record will only reflect the host database information

Runtime events

Runtime Events are events scheduled to occur in weekly cycles for selected areas, readers, doors, alarms, input groups, and output groups. A runtime event can occur on one or more days per week at the start time that you select. Runtime events are frequently used for the normal operating mode.

Runtime events must be created in "pairs," so that the entire cycle of events can be completed. Therefore, you need to create two events for each cycle and make sure both events are assigned to the same mode.

For example, an "unlock door at 8 AM" event is paired with a "lock door at 5 PM" event to define a 24-hour cycle for that door. Both events are scheduled for weekdays only. The door does not require a runtime schedule for weekends, because the door locks at 5 PM on Friday and remains locked until Monday at 8 AM when the "unlock door" event occurs (unless someone manually unlocks the door).

Runtime events can be used to allow certain people access to an area at certain times, such as with multiple shifts of workers. You can assign an area certain categories from 8 AM to 5 PM, and other categories for later shifts or for weekends. (Each shift must have its own category, which must be on the appropriate badges.) To do this, set up a series of Area Events that change categories. After you set the days and the time for each event (category change) to occur, the events continue to occur on a weekly cycle.

Start/end events

Start/end events occur only once during the mode, either at mode start or at mode end. Start/end events are frequently used for Emergency and Holiday modes.

A mode-start event may require a parallel mode-end event to "undo" the change. This may not be necessary, however, since the next normal mode change may accomplish the desired change.

For example, a Fire Mode could be set up using mode-start and mode-end events. When the operator uses the Mode Command form to select Fire Mode, all the events associated with this mode will immediately activate, such as triggering a continuous siren and unlocking all doors so people can exit or enter the building without badges.

Scheduling area events

To schedule changes for all the readers, doors, and routings in an area, use an area event. An event can also put the entire area online or offline.

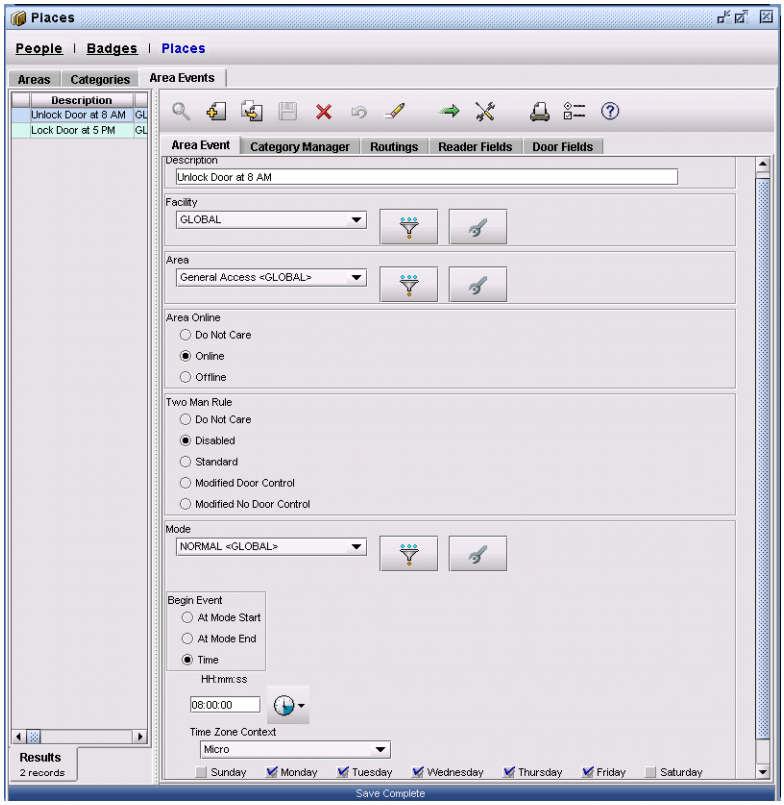
Use the Area Events form to define area events for each mode. You can create events that affect all doors and readers in an area. Defining an event requires you to select a mode, set the time of the event, select an area, and specify one or more changes to the area, readers, or doors.

Note: Do not set up the Area Events form to match the fields on the Area form. Fields that do not need to be scheduled should not be selected, for example, if the area is already online, do not select Online on the Area Event schedule.

Example

An area defined as General Access is made up of several readers and doors. It can be accessed Monday through Friday from 8 AM to 5 PM. To accomplish this, an Unlock Door at 8 AM runtime event is paired with a Lock Door at 5 PM runtime event on weekdays only.

Figure 81. Area Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 84. Area Event form fields

Field name	Description	
Description	Type any alphanumeric combination (1 to 60 alphanumeric characters) for Description. This event may include more than one location if the facility has multiple entrances or buildings. *Example: Unlock Door at 08:00*	
Facility	Click Facility to display the facilities list box. Selecting a facility will allow the administrator to restrict operator access to those records in a specific facility. For more information, see *Creating facilities* on page 53.	
Area	Select the area in which the event will occur.	
Area Online/ Offline	• Online: All readers in the area operate online during the event. • Offline: All readers in the area operate offline during this event: not able to unlock doors, but able to read badges, pass badge data, route and archive access messages, and activate associated alarms. • Do Not Care: See *Radio buttons* on page 27.	
Two Man Rule	These radio buttons are enabled only if the operator has Occupancy Control permission granted. To leave Two Man Rule unaffected, when the event is triggered, none of the radio buttons should be selected. See *Radio buttons* on page 27. **Note:** If the micro is unable to activate a scheduled Two Man Rule event, an alarm, "Schedule did not run," will be sent to the Alarm Monitor. This could occur if the area configuration changed since the schedule was set up. For example, if the Logical Reader Function of a reader in the area was inadvertently changed to Normal, the micro would be unable to activate the schedule.	
	Disabled	Select this radio button to deactivate Two Man Rule mode.
	Standard	Select this radio button to activate the standard Two Man Rule mode which ensures that at least two badge holders occupy a given controlled space.
	Modified with Door Control	Select this radio button to activate the Modified Two Man Rule mode which restricts badge holder access to a controlled area based on their M2MR category type. The first two badge holders to enter a controlled area must be team members. At least two team members must be present in the controlled space until all Guests have exited. Additionally, a team member within the controlled space must press a door release button to allow entry to any subsequent badge holders. The door release button must be pressed within the time specified in the Door Release Timeout field or the door will not be unlocked.
	Modified without Door Control	Select this radio button to activate the Modified Two Man Rule mode which restricts badge holder access to a controlled area based on their M2MR category type. The first two badge holders to enter a controlled space must be team members. At least two team members must be present in the controlled space until all Guests have exited.
Mode	Select the mode in which the area event will occur. An event will not take place, if it is not assigned to a mode and it will only occur in those modes to which it is assigned.	

Table 84. Area Event form fields (continued)

Field name	Description	
Begin Event	At Mode Start	If this is a Start/End event, click if you want the event to activate at the start of the mode.
	At Mode End	If this is a Start/End event, click if you want the event to activate at the end of the mode.
	Time	If the event is a Run Time event, click if you want the event to activate at a specified time.
HHmmss	If the event is a Run Time event, select the time of day that the event will start. Remember to schedule another event as the pair of this one. *Example: If something is turned on every day at 8 AM, it must be turned off at some time later that day.*	
Time Zone Context	Select the time zone context in which the schedule should execute: Host, Micro, or Operator. See *Verifying time zones* on page 168.	
Days of the Week	If the event is a Run Time event, select the days of the week that the event will occur.	
Category Manager	This tab contains the active categories, ordered by slot number, that can be assigned to an area or an area event. To access an area, a badge must match at least one category that is assigned to that area. You may add, remove, or replace a category in a slot. Click Filter to enter search criteria to limit the category list or use the type ahead search feature by clicking in any cell and typing the first letters of the item for which you are searching. For more information, see *Category manager* on page 244. **Note:** This field is position sensitive when used in conjunction with area category schedules.	
Routings	Routings for selected badge activities (valid, invalid, suspended, lost, unknown, anti-passback) in an area can be routed to one or all destinations: log, monitor, printers. *Example*: • *For after hours in a high security area, you can set up an area event that routes all badge activity to the Activity Monitor; or* • *You can set up an area event to route selected activities to a printer or to online history files to be examined later.*	
Reader Online/ Offline	• Online: All readers in the area operate online during the event. • Offline: All readers in the area to operate offline: not able to unlock doors, but able to read badges, pass badge data, route and archive access messages, and activate associated alarms. • Do Not Care: See *Radio buttons* on page 27.	
Physical Reader Type	There are four ways to define the physical reader type of a reader: Badge Only, Badge And Keypad, Keypad Only, and Badge Or Keypad. A reader's physical type may be changed with a reader event. Do Not Care: See *Radio buttons* on page 27. *Example: To provide higher security at certain hours, you can define a badge-and-keypad reader as a badge-only reader from 8 AM to 5 PM and a badge-and-keypad reader from 5 PM to 8 AM. To gain access after 5 PM, a badge holder must swipe their badge and also use the keypad to enter a unique PIN code.*	
Number of Badges	There are two badge controls available: Single and Double. • Single: Only one valid badge is required. • Double: Two complete, valid, and distinct transactions are required. • Do Not Care: See *Radio buttons* on page 27.	

Table 84. Area Event form fields (continued)

Field name	Description	
Swipe and Show Control	This feature is only visible if you have the Image package installed. You can schedule a specific time period for any of the following functions to be active:	
	Select Enabled to enable Swipe And Show on this reader. Select Disabled to disable Swipe And Show on this reader. **Note:** A reader cannot be defined as Toggle when Swipe And Show is Enabled. See *Toggle* on page 186. If Toggle is set to Yes and either Authorization Required or Authorization Not Required is turned on, photos will be displayed for invalid transactions, but not valid transactions.	
	Authorization Required	• Yes: Designate a reader that will display a photo on the Activity Monitor and require an operator to unlock a door. • No: Designate a reader that will display a photo on the Activity Monitor and will unlock a door without operator intervention. • Do Not Care: See *Radio buttons* on page 27. **Notes:** • The Yes and No buttons are not available unless Swipe And Show Enabled is selected. • Access cannot be granted through readers defined as Authorization Required while communications to the micro are down.
Logical Reader Type	To change the way the reader functions, schedule a reader event that changes the logical reader function: Normal, Anti-passback In, Anti-passback Out, Time & Attendance In, Time & Attendance Out, or Time & Attendance In/out. Do Not Care: See *Radio buttons* on page 27. *Example: To provide higher security after hours, you can set up certain readers as anti-passback-in readers and others as anti-passback-out readers;* *or* *To provide data about shifts that badge in and out of an area, you can set up a reader event that changes a normal reader to a Time & Attendance In (or Out) reader.*	
APB Type	To change the way the anti-passback feature functions, schedule an area event that changes the APB Type of all readers in the area: Global APB or Timed APB.	
	Global APB	Used as the default, this allows the host to share APB status/nested APB area status with participating controllers.
	Timed APB	Used to designate the reader as a Timed APB reader in which a badge holder's APB status/nested APB area will return to Neutral after a defined period of time. A Timed APB reader is useful in a site where a badge holder may enter a site by going through an APB reader but is not required to exit the site by going through an APB reader. If this option is selected, a Timed APB Duration must also be defined. A Timed APB status/nested APB area is local to the micro.
	Reset Timed APB Immediately	Used to reset the Timed APB status/nested APB area back to Neutral immediately following a badge swipe.
	APB Duration	A value that represents how long a badge holder's Timed APB status (In or Out) is set when the badge is used on a reader, before being returned to Neutral.

Table 84. Area Event form fields (continued)

Field name	Description
Door State: Unlocked/Locked	You can set up area events to open all doors in an area during normal business hours *Example: Lobby doors or common interior doors such as hallways.* Do Not Care: See *Radio buttons* on page 27.
Held Open Sensing: Detected/Ignored	You can set up area events to ignore doors that are held open. *Example: Lobby doors or common interior doors such as hallways that are held open in an area during peak business hours.* Do Not Care: See *Radio buttons* on page 27.
Forced Open Monitoring: Detected/Ignored	You can set up area events to ignore doors that are forced open in an area. *Example: To keep a loading dock door open indefinitely during business hours without an alarm occurring.* Do Not Care: See *Radio buttons* on page 27.

Related procedures

To create, edit, or delete an Area Event:

1. From the **Access** menu, select **Places**, and then click the **Area Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Scheduling reader events

If you want to change the characteristics of a single reader (rather than a group of readers in an area), use a reader event instead of an area event.

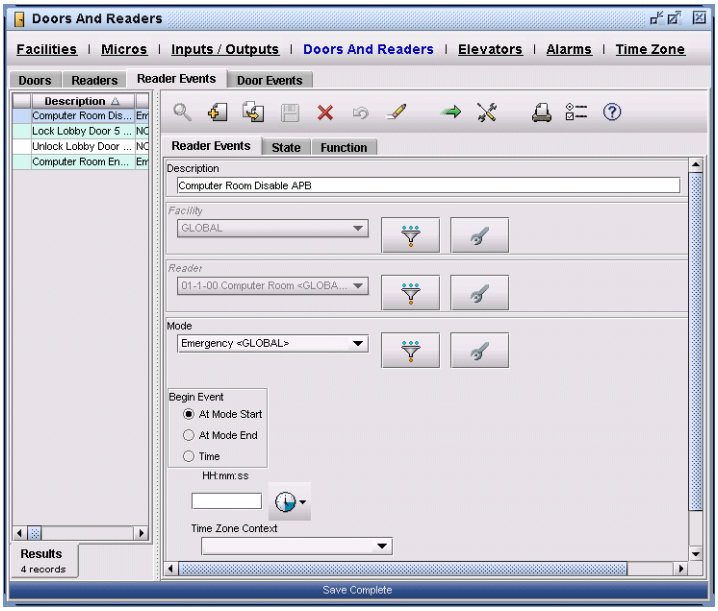
Use the Reader Events form to define reader events for each mode. Defining an event requires you to select a mode, set the time of the event, select a reader, and specify one or more changes to the reader.

Note: Do not set up the Reader Events form to match the fields on the Reader form. Fields that do not need to be scheduled should not be selected, for example, if the reader is already online, do not select Online on the Reader Event schedule.

Example

For increased security, the reader controlling access to the computer room is set for anti-passback control. During Emergency mode this feature is disabled.

Figure 82. Reader Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

.

Table 85. Reader Event form fields

Field name	Description
Description	Type any alphanumeric combination (1 to 60 alphanumeric characters) for Description. *Example: Unlock Lobby Door at 08:00.*

Table 85. Reader Event form fields (continued)

Field name	Description	
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.	
Reader	Select the reader where the event will occur.	
Mode	Select the mode in which the reader event will occur. An event will not take place, if it is not assigned to a mode and it will only occur in those modes to which it is assigned.	
Begin Event	At Mode Start	If this is a Start/End event, click if you want the event to activate at the start of the mode.
	At Mode End	If this is a Start/End event, click if you want the event to activate at the end of the mode.
	Time	If the event is a Run Time event, click if you want the event to activate at a specified time.
HHmmss	If the event is a Run Time event, select the time of day that the event will start. Remember to schedule another event as the pair of this one. *Example: If something is turned on every day at 8 AM, it must be turned off at some time later that day.*	
Time Zone Context	Select the time zone context in which the schedule should execute: Host, Micro, or Operator. See *Verifying time zones* on page 168.	
Days of the Week	If the event is a Run Time event, select the days of the week that the event will occur.	
Physical Reader Type	There are four ways to define the physical reader type of a reader: Badge Only, Badge And Keypad, Keypad Only, and Badge Or Keypad. A reader's physical type may be changed with a reader event. Do Not Care: See *Radio buttons* on page 27. *Example: To provide higher security at certain hours, you can define a badge-and-keypad reader as a badge-only reader from 8 AM to 5 PM and a badge-and-keypad reader from 5 PM to 8 AM. To gain access after 5 PM, a badge holder must swipe their badge and also use the keypad to enter a unique PIN code.*	
Reader Online/Offline	Online: All readers in the area operate online during the event. Offline: All readers in the area to operate offline: not able to unlock doors, but able to read badges, pass badge data, route and archive access messages, and activate associated alarms. Do Not Care: See *Radio buttons* on page 27.	
Number of Badges	There are two badge controls available: Single and Double. Single: Only one valid badge is required. Double: Two complete, valid, and distinct transactions are required. Do Not Care: See *Radio buttons* on page 27.	

Table 85. Reader Event form fields (continued)

Field name	Description	
Swipe and Show Control	This feature is only visible if you have the Image package installed. You can schedule a specific time period for any of the following functions to be active:	
	Select Enabled to enable Swipe And Show on this reader. Select Disabled to disable Swipe And Show on this reader. **Note:** A reader cannot be defined as Toggle when Swipe And Show is Enabled. See *Toggle* on page 186. If Toggle is set to Yes and either Authorization Required or Authorization Not Required is turned on, photos will be displayed for invalid transactions, but not valid transactions.	
	Authorization Required	• Yes: Designate a reader that will display a photo on the Activity Monitor and require an operator to unlock a door. • No: Designate a reader that will display a photo on the Activity Monitor and will unlock a door without operator intervention. • Do Not Care: See *Radio buttons* on page 27. **Notes**: • The Yes and No buttons are not available unless Swipe And Show Enabled is selected. • Access cannot be granted through readers defined as Authorization Required while communications to the micro are down.
Logical Reader Function	To change the way the reader functions, schedule a reader event that changes the logical reader function: Normal, Anti-passback In, Anti-passback Out, Time & Attendance In, Time & Attendance Out, or Time & Attendance In/out. Do Not Care: See *Radio buttons* on page 27. *Example: To provide higher security after hours, you can set up certain readers as anti-passback-in readers and others as anti-passback-out readers; or* *To provide data about shifts that badge in and out of an area, you can set up a reader event that changes a normal reader to a Time & Attendance In (or Out) reader.*	
APB Type	To change the way the anti-passback feature functions, schedule an area event that changes the APB Type of all readers in the area: Global APB or Timed APB.	
	Global APB	Used as the default, Global APB allows the reader to function as a normal APB reader.
	Timed APB	Used to designate the reader as a Timed APB reader, a badge holder's APB status will be set to In or Out and will return to Neutral after a defined period of time. A Timed APB reader is useful in a site where a badge holder may enter a site by going through an APB In reader but is not required to exit the site by going through an APB Out reader. If this option is selected, a Timed APB Duration must also be defined. A Timed APB status is local to the micro.
	Reset Timed APB Immediately	When selected, this option sends a message to the micro to reset the Timed APB status back to Neutral immediately following a badge read.
	APB Duration	A value that represents how long a badge holder's Timed APB status (In or Out) is set when the badge is used on a reader, before being returned to Neutral.

Related procedures

To create, edit, or delete a Reader Event:

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Reader Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Scheduling door events

When you want to change the characteristics of a single door (rather than a group of doors in an area) use a door event instead of an area event.

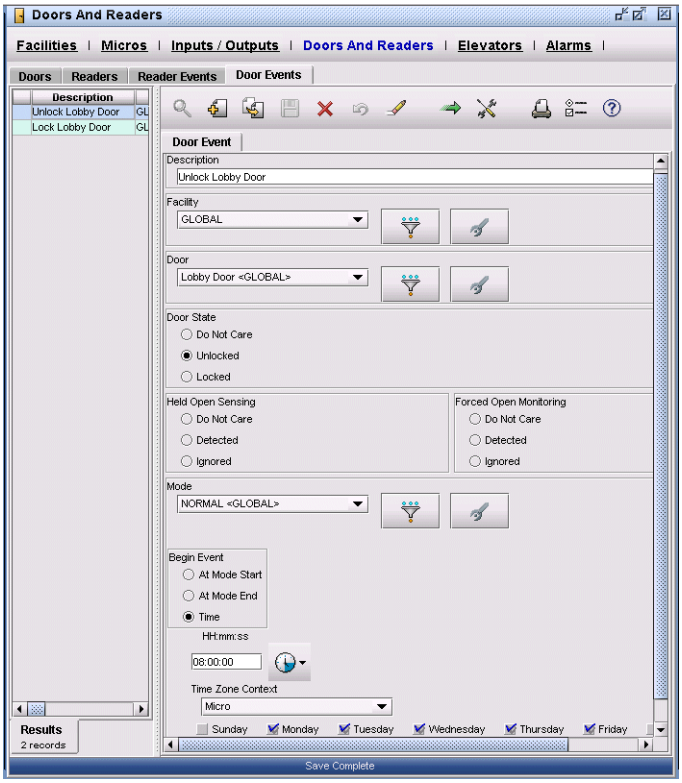
Use the Door Event form to define door events for each mode. Defining an event requires you to select a mode, set the time of the event, specify a door, and change one or more of the operating characteristics of the door

Note: Do not set up the Door Event form to match the fields on the Door form. Fields that do not need to be scheduled should not be selected, for example, if the door is already unlocked, do not select Unlocked on the door schedule.

Example

The lobby door can be accessed Monday through Friday from 8 AM to 5 PM. To accomplish this, an Unlock Door at 8 AM runtime event is paired with a Lock Door at 5 PM runtime event on weekdays only.

Figure 83. Door Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 86. Door Event form fields

Field name	Description	
Description	Type any alphanumeric combination (1 to 60 alphanumeric characters) for Description. This event may include more than one location if the facility has multiple entrances or buildings. *Example: Unlock Door at 08:00*	
Facility	Click Facility to display the facilities list box. Selecting a facility will allow the administrator to restrict operator access to those records in a specific facility. For more information, see *Creating facilities* on page 53.	
Door	Select the door where the event will occur.	
Door State Locked/Unlocked	• Unlocked: To schedule an individual door in an area to unlock at the same time each day, use a door event that sets the Door State field to Unlocked. **Note:** An area event that locks all area doors and occurs after this door event will also lock this individual door. • Locked: To schedule an individual door in an area to lock at the same time each day, use a door event that sets the Door State field to Locked. **Note:** An area event that unlocks all area doors and occurs after this door event will also unlock this individual door. • Do Not Care: See *Radio buttons* on page 27.	
Held Open Sensing: Detected/Ignored	• Detected: To allow an alarm condition on this door to occur during this event when the door is held open beyond the Unlock Time specified in the Doors form. • Ignored: To allow a door to remain open during this event, beyond the Unlock Time specified in the Doors form, without generating an alarm. • Do Not Care: See *Radio buttons* on page 27.	
Forced Open Monitoring: Detected/Ignored	• Detected: To allow an alarm condition on this door to occur immediately when the door is forced open without a valid badge read or exit device. • Ignored: Select Ignored if the Monitoring function on this door is not used. • Do Not Care: See *Radio buttons* on page 27.	
Mode	Select the mode in which the area event will occur. An event will not take place, if it is not assigned to a mode and it will only occur in those modes to which it is assigned.	
Begin Event	At Mode Start	If this is a Start/End event, click if you want the event to activate at the start of the mode.
	At Mode End	If this is a Start/End event, click if you want the event to activate at the end of the mode.
	Time	If the event is a Run Time event, click if you want the event to activate at a specified time.

Table 86. Door Event form fields (continued)

Field name	Description
HHmmss	If the event is a Run Time event, select the time of day that the event will start. Remember to schedule another event as the pair of this one. *Example: If something is turned on every day at 8 AM, it must be turned off at some time later that day.*
Time Zone Context	Select the time zone context in which the schedule should execute: Host, Micro, or Operator. See *Verifying time zones* on page 168.
Days of the Week	If the event is a Run Time event, select the days of the week that the event will occur.

Related procedures

To create, edit, or delete a Door Event:

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Door Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

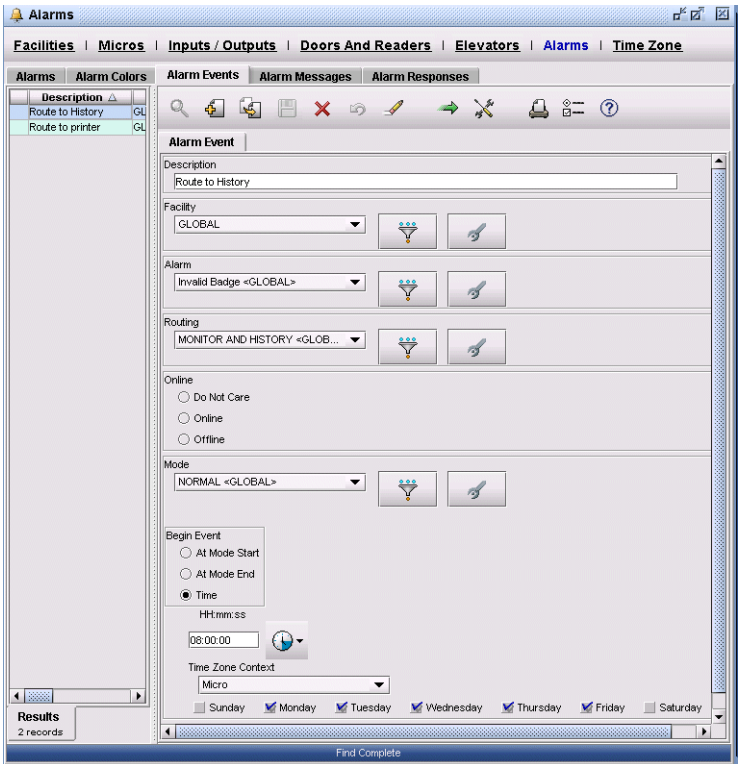
Scheduling alarm events

When you want to change the characteristics of a single alarm (without changing the input group or output group assigned to the alarm) use an alarm event. Use the Alarm Event form to define alarm events for each mode. Defining an event requires you to select a mode, set the time of the event, select an alarm, and specify one or more of the changes to the alarm.

Example

During the business day you want invalid-badge alarms to route to the log and monitor but after hours and weekends, you want them to route to the monitor and a printer. Set an alarm event for MTWTF at 17:00 to start routing invalid-badge alarms to the alarm monitor and to a selected printer. Set a parallel alarm event to occur on MTWTF at 08:00 to start routing the alarm to the history log and monitor.

Figure 84. Alarm Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 87. Alarm Event form fields

Field name	Description
Description	Type an alarm event description up to 30 alphanumeric characters long. *Example: Door Held Offline 08:00 M-F.*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Alarm	Select the alarm for which the event will occur.
Routing	To send an alarm to a different routing at certain times, schedule an alarm event that specifies the new routing and time. You can send the alarm message to the alarm monitor, a printer, the history log, or to a combination of the three. *Example: If you want invalid-badge alarms to route to the log and monitor during the business day but to the monitor and a printer after hours, set an alarm event for MTWT at 17:00 to start routing invalid-badge alarms to the alarm monitor and to a selected printer. Set a parallel alarm event to occur on MTWTF at 08:00 to start routing the alarm to the history log and monitor. If no one watches the alarm monitor on weekends, another alarm event (F at 17:00) can start routing this alarm to the log and to the printer. On Monday, scheduled alarm events begin to repeat the cycle.*

Table 87. Alarm Event form fields (continued)

Field name	Description	
Online	• Online: To set an alarm online when the facility is closed for a holiday, use an alarm event that does not cycle daily. Use a mode-start alarm event associated with your holiday mode. When the system starts to operate in holiday mode, events that cycle during normal operating stop cycling. Set this alarm to remain online until the system switches back to normal operating mode. **Note:** You may need to schedule a parallel mode-end alarm event (in case the system does not return to normal operating mode) for other scheduled events to occur. However, the preferred way is to schedule the input group offline/online. This way no input activity (ISC) is sent to the host. See Input Group Events. • Offline: To ensure that normal daytime activity does not trigger an alarm, use a runtime alarm event to put this alarm offline during the day. *Example: Use an alarm event to set this alarm offline before the business day starts (MTWTF at 07:30). Use a parallel alarm event to set this alarm online after hours (MTWTF at 17:00). During the weekend (between Friday at 5 PM and Monday at 7:30 AM), this alarm is online and does not cycle daily.* • Do Not Care: See *Radio buttons* on page 27.	
Mode	Select the mode in which the alarm event will occur. An event will not take place, if it is not assigned to a mode and it will only occur in those modes to which it is assigned.	
Begin Event	At Mode Start	If this is a Start/End event, click if you want the event to activate at the start of the mode.
	At Mode End	If this is a Start/End event, click if you want the event to activate at the end of the mode.
	Time	If the event is a Run Time event, click if you want the event to activate at a specified time.
HHmmss	If the event is a Run Time event, select the time of day that the event will start. Remember to schedule another event as the pair of this one. *Example: If something is turned on every day at 8 AM, it must be turned off at some time later that day.*	
Time Zone Context	Select the time zone context in which the schedule should execute: Host, Micro, or Operator. See *Verifying time zones* on page 168.	
Days of the Week	If the event is a Run Time event, select the days of the week that the event will occur.	

Related procedures

To create, edit, or delete an Alarm Event:

1. From the **Configuration** menu, select **Alarms**, and then click the **Alarm Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Scheduling input group events

You can use an input group event to place an input group online or offline and to control what output groups or alarms trigger when this input group activates. An event can place an input group online/offline at a scheduled time on a daily/weekly cycle within the normal operating mode; or this event can be set to occur At Mode Start and to continue (with no daily or weekly cycles) until a parallel At Mode End event occurs to reverse the change.

For example:

For use with Fire mode, you could create an event that sets the fire-detector input group to offline, so that Open condition and/or Short condition state changes do not continue to be detected. This input group event prevents the system from receiving a flood of alarms when a fire occurs. Remember that a mode-start event requires a parallel mode-end event.

You could also schedule an event to place a motion detector input group offline during the day and online at night, if after-hours activity in this area indicates a security violation. Or, to conserve electricity after hours, schedule the input group for hallway motion detectors to trigger lights to turn on for a duration, to provide lighting only when required.

An input-group event can change the output groups associated with an input group.

For example:

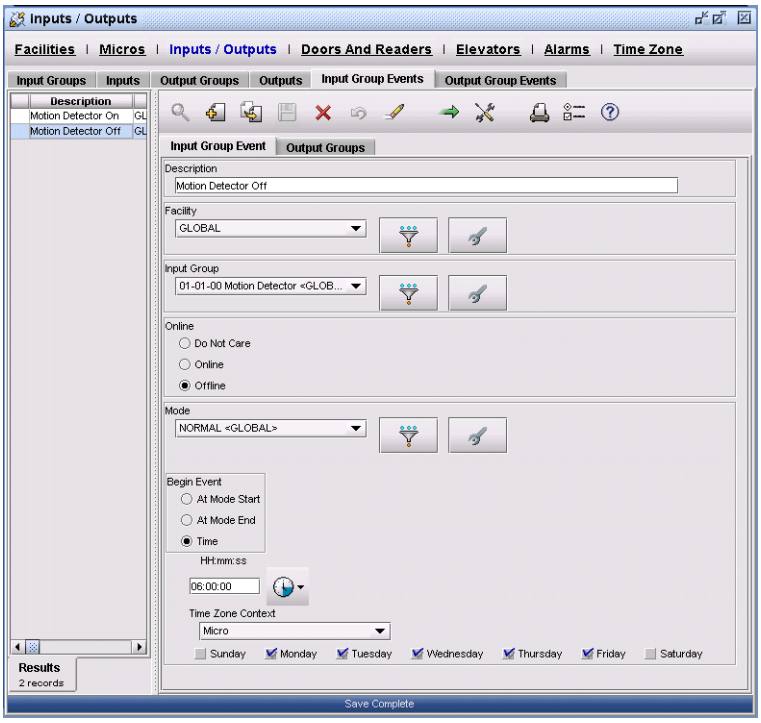
To have security lights turn on when someone opens an exterior door at night (using a badge or using force), schedule an input group event to occur at sundown. Select the output group that operates the security lights. When an exterior door opens, this output group triggers the outdoor security lights.

To have an alarm sound when someone uses an invalid badge between the hours of 5 PM and 8 AM, schedule an input group event. Select the output group that operates a siren. When the reader detects an invalid badge, the reader's invalid input group activates, the associated output group triggers, and associated output devices operate, in this case, a siren.

Example

Schedule two parallel events to place a motion detector input group offline during the day and online at night; after-hours activity in this area indicates a security violation.

Figure 85. Input Group Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 88. Input Group Event form fields

Field name	Description
Description	Type any alphanumeric combination (1 to 60 alphanumeric characters). *Example: Lobby AC Fail Off 17:00 M-F*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Input Group	Select the input group that will be triggered by the event.
Online	Online: To allow an associated alarm and/or output group to trigger if the input is triggered, use an input group event to place an input group online. Offline: To prevent an associated alarm and/or output group from triggering if the input is triggered, use an input group event to place an input group offline. Do Not Care: See *Radio buttons* on page 27.
Mode	Select the mode in which the alarm event will occur. An event will not take place, if it is not assigned to a mode and it will only occur in those modes to which it is assigned.

Table 88. Input Group Event form fields (continued)

Field name	Description	
Begin Event	At Mode Start	If this is a Start/End event, click if you want the event to activate at the start of the mode.
	At Mode End	If this is a Start/End event, click if you want the event to activate at the end of the mode.
	Time	If the event is a Run Time event, click if you want the event to activate at a specified time.
HHmmss	If the event is a Run Time event, select the time of day that the event will start. Remember to schedule another event as the pair of this one. *Example: If something is turned on every day at 8 AM, it must be turned off at some time later that day.*	
Time Zone Context	Select the time zone context in which the schedule should execute: Host, Micro, or Operator. See *Verifying time zones* on page 168.	
Days of the Week	If the event is a Run Time event, select the days of the week that the event will occur.	
Output Group	Click to change the output group associated with an input group during the input group event. Output groups are position sensitive and follow the same scheduling rules as categories on the Area Events form. It is possible to overwrite an existing output group, depending on which output group slot is changed, so familiarize yourself with the existing output groups associated with the input group being changed. **Notes:** • When you add a new output group, make sure you don't overwrite something, such as the existing "door unlock" output group. • If scheduling outputs, they must reside on the same micro. • Remember to define the duration of the output using the Outputs form. A duration of zero turns on the output indefinitely.	

Related procedures

To create, edit, or delete an Input Group Event:

1. From the **Configuration** menu, select **Inputs/Outputs**, and then click the **Input Group Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Scheduling output group events

Use the Outgroups Events form to define output group events for each mode. Defining an event requires you to select a mode, set the time of the event, select an output group, and specify one or more changes to the output group.

An output group event can enable or disable a specific output group, and/or change the state of its outputs to Off or On for the period of time entered in the Time field of the Output form associated with this output group.

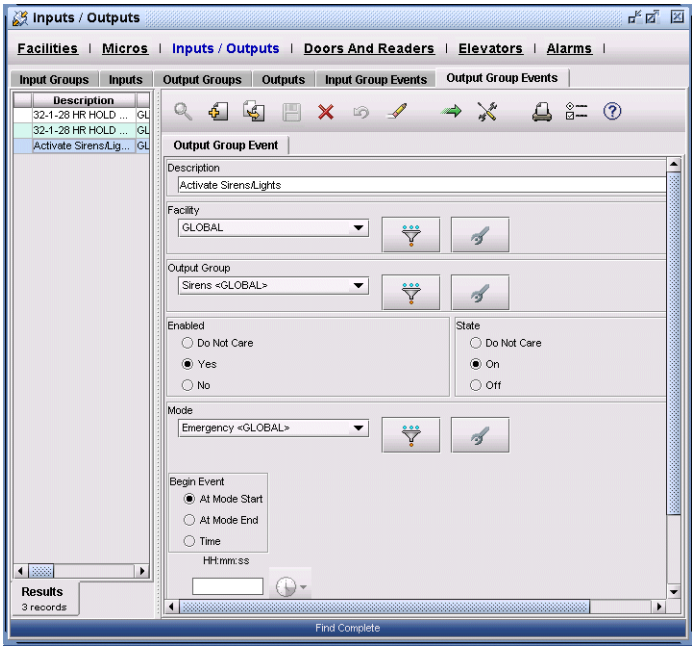
For example:

- You can define an output group event to enable an output group made up of lights or perimeter cameras and have them turned on only during the night.
- You can define an output group event for Emergency mode that turns on sirens and emergency lights for the duration of Time.
- You can define output group events for Normal mode to turn on lights late at night and turn them off in the morning.

Example

Define an output group event for Emergency mode that turns on sirens and emergency lights for the duration of Time.

Figure 86. Output Group Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow

.

Table 89. Output Group Event form fields

Field name	Description	
Description	Type an output group event description up to 60 alphanumeric characters long. *Example: Parking Lot Lights On 18:00 M-F.*	
Facility	Click Facility to display the facilities list box. Selecting a facility will allow the administrator to restrict operator access to those records in a specific facility. For more information, see *Creating facilities* on page 53.	
Enabled	Output groups such as lights or perimeter cameras can be enabled to operate as required at scheduled times Yes: To allow an output group to operate as required at scheduled times. No: To disable an output group during scheduled times. Do Not Care: See *Seed counter* on page 366.	
State	The outputs in the output group, such as emergency lights or sirens, can be turned on or off. **Note:** Remember to define the duration of the output using the Outputs form. A duration of zero turns on the output indefinitely. On: To turn the outputs in an output group On at scheduled times. Off: To turn the outputs in an output group Off during scheduled times. Do Not Care: See *Radio buttons* on page 27.	
Mode	Select the mode in which the output group event will occur. An event will not take place, if it is not assigned to a mode and it will only occur in those modes to which it is assigned.	
Begin Event	At Mode Start	If this is a Start/End event, click if you want the event to activate at the start of the mode.
	At Mode End	If this is a Start/End event, click if you want the event to activate at the end of the mode.
	Time	If the event is a Run Time event, click if you want the event to activate at a specified time.
HHmmss	If the event is a Run Time event, select the time of day that the event will start. Remember to schedule another event as the pair of this one. *Example: If something is turned on every day at 8 AM, it must be turned off at some time later that day.*	
Time Zone Context	Select the time zone context in which the schedule should execute: Host, Micro, or Operator. See *Verifying time zones* on page 168.	
Days of the Week	If the event is a Run Time event, select the days of the week that the event will occur.	

Related procedures

To create, edit, or delete an Output Group Event:

1. From the **Configuration** menu, select **Inputs/Outputs**, and then click the **Output Group Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Scheduling backup events

The Backup Events feature allows you to schedule a system backup to pre-selected media. The backup will then run automatically at the day and time settings specified on the Backup Events form. The backup can go to either tape or disk file, and can include one or more of the following backup types: Badge table, base system, history tables, and any optional packages, such as Alarm Graphics tables.

The scheduled backup will not span multiple tapes, and there will be no prompt for inserting the backup media. Before the backup is to take place, an operator must make sure that the correct media is properly inserted.

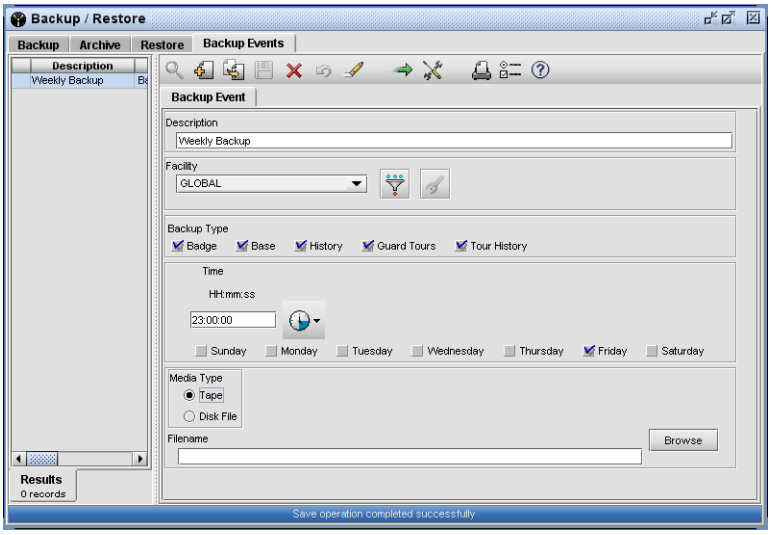
All error messages and completion messages generated as a result of the scheduled backup process will be written to a log file in the `/cas/log` directory called bak.mmdd where `mmdd` = system date (For example: `0302` = March 2nd). You must check the `bak` log file for messages after the scheduled backup process has executed, since there are no pop-up window messages associated with this feature.

Archives of Badge, Alarm, or Operator History cannot be scheduled.

Example

Define a backup event that schedules an automatic tape backup of the Badge, Base, History, Guard Tours and Tour History database tables to occur at 11 PM every Friday.

Figure 87. Backup Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 90. Backup Event form fields

Field name	Description	
Description	Type an output group event description up to 60 alphanumeric characters long. *Example: Parking Lot Lights On 18:00 M-F*	
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.	
Backup Type	Select the databases to be backed up on this schedule.	
Begin Event	At Mode Start	If this is a Start/End event, click if you want the event to activate at the start of the mode.
	At Mode End	If this is a Start/End event, click if you want the event to activate at the end of the mode.
	Time	If the event is a Run Time event, click if you want the event to activate at a specified time.
HHmmss	If the event is a Run Time event, select the time of day that the event will start. Remember to schedule another event as the pair of this one. *Example: If something is turned on every day at 8 AM, it must be turned off at some time later that day.*	
Time Zone Context	Select the time zone context in which the schedule should execute: Host, Micro, or Operator. See *Verifying time zones* on page 168.	
Days of the Week	If the event is a Run Time event, select the days of the week that the event will occur.	
Media Type	Select the media to use for the backup: Tape or Disk File. **Note:** If Disk File is selected, the file `/cas/db/text/diskfile.cfg` must exist.	
Filename	If you chose to save to a Disk File, enter the name of the filesystem to store the backup. Click Browse to select from a list. If your backup file is expected to exceed 2 GB, ensure that the location where the file is to be stored is defined as a Large File System. Otherwise, the backup file will be incomplete.	

Related procedures

To create, edit, or delete a Backup Event:

1. From the **Control** menu, select **Backup/Restore**, and then click the **Backup Events** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Triggering Emergency modes using input groups

Use the Emergency form to define emergency mode triggers for selected facilities. This requires you to select an Emergency mode, Input Group, and one or more facilities. This will allow an input group to trigger a mode change to the assigned facilities.

Figure 88. Emergency Form

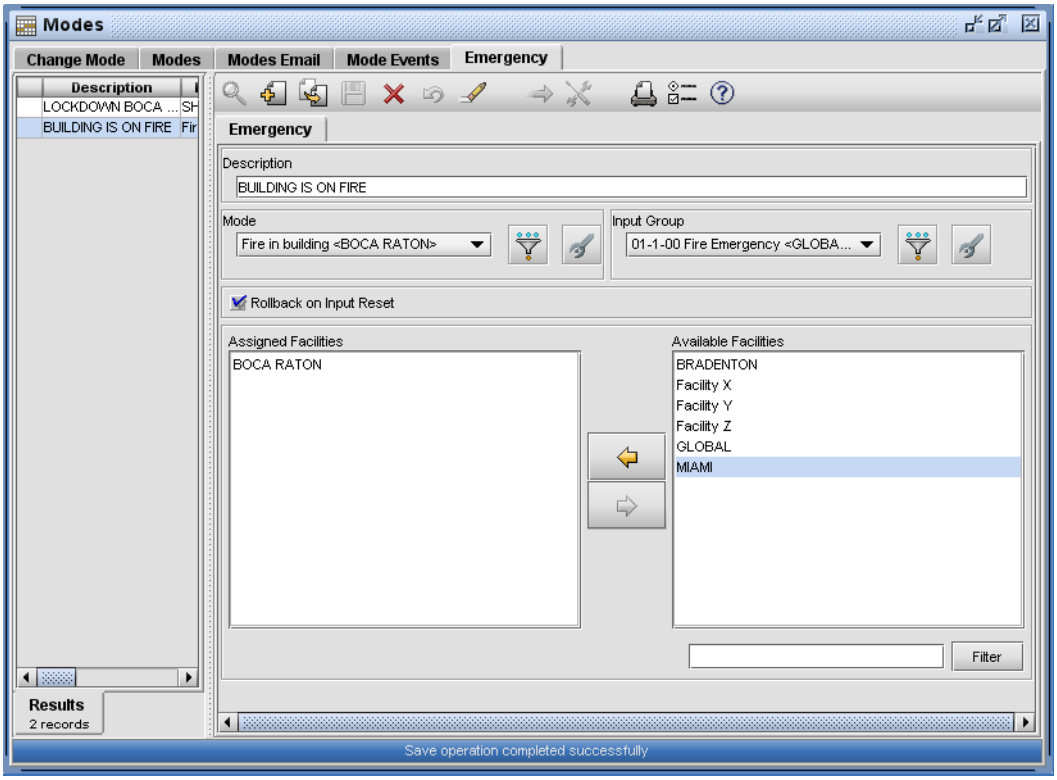


Table 91. Emergency Form

Field name	Description	
Description	Type an emergency trigger description up to 60 alphanumeric characters long. *Example: CAMPUS LOCKDOWN*	
Mode	Select the Emergency mode that will take effect when the emergency trigger occurs.	
Input Group	Select the input group that will trigger the emergency mode. Only input groups with Broadcast State Change selected on the Input Groups form will be available in this list box.	
Rollback on Input Reset	Check to rollback to the previous mode when the input is reset.	
Facilities	Available Facilities	Displays the active facilities available to the operator.
	Assigned Facilities	Displays the assigned facilities that the trigger will effect.

To trigger an Emergency Mode using an Input Group:

1. First, create an Input Group record. See *Creating input groups* on page 127.
2. Next, create an Emergency Mode record by selecting **Control**, **Modes**, and then **Emergency.**
3. Enter a description for this Emergency mode.
4. Select a Mode from the Mode list box.

5. Select an Input Group from the Input Group list box.
6. Select the Facilities this Emergency Mode will be assigned to.
7. Save the record.
8. For detailed information on creating records, refer to *Creating, editing, deleting, and printing records* on page 36.

Chapter 11 Badge management

This chapter describes how to manage badge and personnel records. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

When a person attempts to access an area and at least one category on the badge matches at least one category of that area, the system grants access; if the person attempts to access an area and no categories on the badge match any categories of that area, the system denies access.

This chapter explores various methods of managing the badges, badge holders, and the categories in your system. You will need to become familiar with the following forms:

- Badges
- Personnel
- Category Manager
- Badge Manager

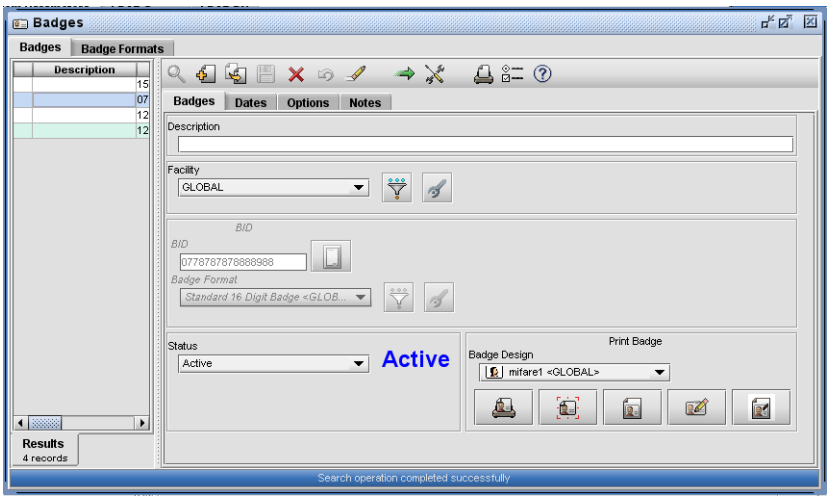
Defining badges

Information on the Badges form identifies the badge ID and format, and also controls the function and capabilities of the badge.

Example

In addition to his normal access control badge, a security guard is issued a tour badge to be used when conducting a facility tour at specified intervals. The guard stops at pre-determined tour points along the way, where he swipes the tour badge in a reader so the system can track his progress.

Figure 89. Badges form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable, some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 92. Badges form fields

Field name		Description
Description	A person or badge holder can have multiple badges. Type a description that defines the purpose of this particular badge.	
Facility	Click Facility to display the facilities list box. Selecting a facility will allow the administrator to restrict operator access to those records in a specific facility. For more information, see *Creating facilities* on page 53.	
BID	BID	This field contains the unique encoded number of a badge. **Note:** The Badge Encode Format field will have no effect on the Badge Encode Number (BID) displayed. The BID displayed will always be the actual full BID read from the badge. If Save is clicked, then the BID entered will be checked against the badge. Format to ensure it satisfies its specifications. If the BID is OK, then the field will be updated and the record saved. **Note:** If the Seed Counter and the Copy to BID options are enabled, the Badge Format, BID and Reader Issue fields are disabled, even on new records. The Badge Format is set to the default chosen during Seed Counter installation and the BID is generated automatically. See *Seed counter* on page 366.
	Badge Format	This field displays the selected format for this badge (10, 12 or 16 digit). **Note:** If you are using a Mifare Wiegand Badge ID 5502 fomat, select Standard 16 Digit Badge. If you are using a Mifare Wiegand Badge ID 26-bit select Standard 10 Digit Badge. Refer to *To create a Mifare badge design:* on page 257.
Reader Issue	Click to allow the Badge Encode Number to be entered by swiping a badge in a local console reader assigned to the workstation used to issue the badge. A prompt advises you when to swipe the badge. The badge encode number appears in the Badge Encode Number field. For information on setting up a badge issue workstation, see *To set up your Imaging workstations:* on page 57. **Note:** If the Seed Counter and the Copy to BID options are enabled, the Badge Format, BID and Reader Issue fields are disabled, even on new records. The Badge Format is set to the default chosen during Seed Counter installation and the BID is generated automatically. See *Seed counter* on page 366.	
Badge Format	Click to display the Badge Format list box. Select the desired format. This is not necessary unless the system has more than one badge format. **Note:** If the Seed Counter and the Copy to BID options are enabled, the Badge Format, BID and Reader Issue fields are disabled, even on new records. The Badge Format is set to the default chosen during Seed Counter installation and the BID is generated automatically. See *Seed counter* on page 366.	
Status	Select one of the four badge status descriptions. There is one type of Valid badge status (Active) and three types of Invalid badge statuses (Suspended, Lost, Deleted). You should update the badge status as needed. *Example: If a valid badge is lost, this status change should be indicated in the Badge Status box. Then, if the lost badge is later tried in a reader, the system will deny access.* **Note:** The Status field on the Personnel form overrides this field on the Badges form. For example, if a personnel record has multiple badges assigned to it, and that person is suspended, you can change the status to Suspended on the Personnel form and all related badges will be suspended.	

Table 92. Badges form fields (continued)

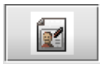
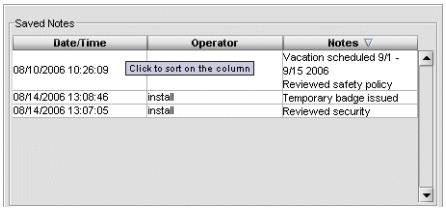
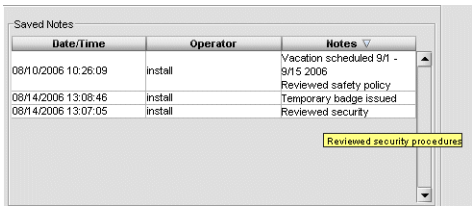
Field name		Description	
Print Badge	Badge Design	Select a badge design to print from the list box. This option will be available if you have the optional Imaging package installed. For more information on printing badges, see *Printing badges* on page 242.	
	Print	Select this button to print a badge. **Note:** To print a badge that contains personnel data , refer to *Table 98., Badge Manager form fields* on page 251.	
	Preview	Select this button to preview a badge before printing. **Note:** To preview a badge that contains personnel data , refer to *Table 98., Badge Manager form fields* on page 251.	
	Page Setup & Options	Select this button to view page setup options for a badge. **Note:** To view the page setup options for a badge that contains personnel data , refer to *Table 98., Badge Manager form fields* on page 251.	
	Encode		Click this button to encode a badge. Refer to **Note:** If this button appears dimmed, refer to *Imaging troubleshooting* on page 401 for assistance.
	External Encoder Setup		Click to launch the External Encoders Setup dialog.
Issued	Date	Type the date the badge was issued. If this field is left blank, the system will automatically enter the current date. **Note:** Type the slashes (/) if the system date format requires them.	
	Time	Type the time the badge was issued. If this field is left blank, the system will automatically enter the current time. **Note:** Type the colons (:) if the system time format requires them.	
	Time Zone Context	Select the time zone context in which the badge was issued. For examples, see *Verifying time zones* on page 168.	
Expires	Date	Type the date the badge expires. **Note:** Type the slashes (/) if the system date format requires them.	
	Time	Type the time the badge expires. **Note:** Type the colons (:) if the system time format requires them.	
	Time Zone Context	Select the time zone context in which the badge expired. For examples, see *Verifying time zones* on page 168.	

Table 92. Badges form fields (continued)

Field name		Description
Return	Date	Type the date the badge was turned in. **Note:** Type the slashes (/) if the system date format requires them.
	Time	Type the time the badge was turned in. **Note:** Type the colons (:) if the system time format requires them.
	Time Zone Context	Select the time zone context in which the badge was turned in. For examples, see *Verifying time zones* on page 168.
Last Access	The system tracks the badge and displays information about when it was last used. This reflects information captured as of the moment the badge record was displayed. **Note:** Type the slashes (/) if the system date format requires them. Type the colons (:) if the system time format requires them.	
	Date	The date the badge was last granted access.
	Time	The time the badge was last granted access.
	Time Zone	The time zone in which the badge was last granted access. For examples, see *Verifying time zones* on page 168.
	Reader	Indicates the reader last granted access to this badge.
	Area	Indicates the area this badge was last granted access to.
Person	Indicates the Personnel record to which this badge is assigned. This field is view only - you can perform a search, but it cannot be edited.	
Temporary	Set to On, if this badge record is to be used as a temporary badge. A pool of badges can be created and used repeatedly for this purpose. A temporary badge must be expired in order to be reissued.	
Usage Count	Limited Usage	To limit the number of times a badge may be used, set the Limited Usage check box to On.
	Count	Type a specific number in the Count field. Each time the badge is used in a Limited Usage reader, the usage count is decremented by 1. When the count is 0, the badge will no longer grant access into a Limited Usage reader.
Tour Badge	If you have the optional Guard Tours package installed, select this option to designate a badge as a tour badge used to conduct guard tours of a facility at specified intervals. This badge will not operate for normal access control.	
Reissue Count	If the Seed Counter option is enabled, every time a badge is issued to a person this incremental number is stored to the badge. This field shows the issue number of this badge and the total number of badge issues for the badgeholder to whom this badge is assigned, for example *3 of 5*. If a badge has not been assigned to a person, the Reissue Count is 00. The maximum number of badge issues allowed is 99. This field is view only - you can perform a search, but it cannot be edited. For more information, see *Seed counter* on page 366.	
Reprint Count	If the Seed Counter option is enabled, for non-MIFARE badge designs, this field indicates the number of times the badge has been printed. For MIFARE badge designs, this field indicates if the badge has been encoded. A new badge will set the reprint count to 00. For non-MIFARE badge designs, any time the badge is printed or previewed, the badge will increment the number, store this number on the badge, and allow a maximum reprint of 99 times. For MIFARE badge designs, when the badge is encoded, the reprint count is set to 01 and is stored on the badge. MIFARE badge designs can only be encoded once. For more information, see *Seed counter* on page 366.	

Table 92. Badges form fields (continued)

Field name	Description
Unique Id	If the Seed Counter option is enabled, the seed counter assigns a unique number to each badge. It is a global counter that is incremented each time a new badge is created. The range is determined by the number of digits allocated to the counter. This field is view only - you can perform a search, but it cannot be edited. For more information, see *Seed counter* on page 366.
Saved Notes	All saved notes applicable to this record are listed including the Date/Time the note was created and the operator that created it. Click on a column heading to sort by Date/Time, Operator, or alphabetically by note.  By hovering the mouse over the note, the entire contents of the note displays. 
Notes	This is a free form text field where you can add information pertinent to Badge or Person records. *Example: Employee work visa will expire on 12/12/05.*

Related procedures

To create a Badge record using the Console-Reader method:

1. Select **Access**, **Badges**, and then **Badges** tab.
2. Click **New** .
3. Click **Reader Issue** .
4. Swipe the badge in the console reader assigned to the terminal. The badge ID number will appear in the BID field.
5. Complete the Badges form. For details on completing each field, see *Badges form fields* on page 225.
6. Click **Save** .

To create a Badge record using the manual method:

1. Select **Access**, **Badges**, and then **Badges** tab.
2. Click **New** .
3. Type the badge encode number into the BID field.
4. Complete the Badges form. For details on completing each field, see *Badges form fields* on page 225.
5. Click **Save** .

To change a badge record:

1. Select **Access**, **Badges**, and then **Badges** tab.
2. Find the desired badge record in one of two ways:
   - When the Badges form appears, click **Reader Issue** . Swipe the badge in a console reader, and then click **Find** to display the existing badge holder data; or:
   - When the Badges form appears, enter search criteria in one or more fields and click **Find** .

   Note: A search using "indexed" fields improves the time required to find the records. Some examples of indexed fields on the Badges form include: Person, Description, and BID.
3. Complete the Badges form for the fields that require updating. For details on completing each field, see *Badges form fields* on page 225.
4. Click **Save** .

To change a badge status to deleted:

1. Select **Access**, **Badges**, and then **Badges** tab.
2. When the Badges form appears, enter search criteria in one or more fields and click **Find** .
3. Click the Status field and select **Deleted**. Although the badge no longer grants access, the badge record remains in the database.
4. Click **Save** .

To permanently remove a badge from the database:

CAUTION: This procedure removes badge records from the database. Since it is possible to remove badge records that should be retained, you should back up your database before running this procedure.

The **Delete** button will be on the Badges form toolbar if the correct permissions have been set on the Permissions form for the current operator. The **Delete** button is used to permanently remove badge records from the Picture Perfect database. This process also removes the badge records from all micros that have learned the badges and have the badge records in their database.

Before any badge can be removed, it must have a badge status of Deleted. To assign the Deleted status, see *To change a badge status to deleted:* on page 229.

Note: Badge delete on person delete is controlled by a setting on the Badge Manager control of the form; by default it is set not to delete associated badges when a person is deleted.

All badge removal activity is recorded in the operator history table.

1. Select **Access**, **Badges**, and then **Badges** tab.
2. When the Badges form appears, enter search criteria in one or more fields and click **Find**. Select **Deleted** in the Status field as part of the criteria when using the **Find** button to select a range of records.
3. Click the **Delete** button. The Badge Removal popup asks if you want to remove the records. If record dependencies exist (for example if the badge is assigned to a Personnel record), a list of these records displays. You must remove the dependencies before the badge record can be deleted.
4. If no dependencies exist, click **OK** to confirm your intention to remove the badge records. If you do not want to proceed with the removal process, click **Cancel**.

   Note: If you are removing a large number of records, the system removes records in increments according to the Record Remove Maximum and Record Remove Interval set on the Parameters form. See *Assigning system parameters* on page 40.

Defining personnel

Information on the Personnel form identifies the badge holder by name, employee number, address, and badge ID, and also controls the function and capabilities of the badge.

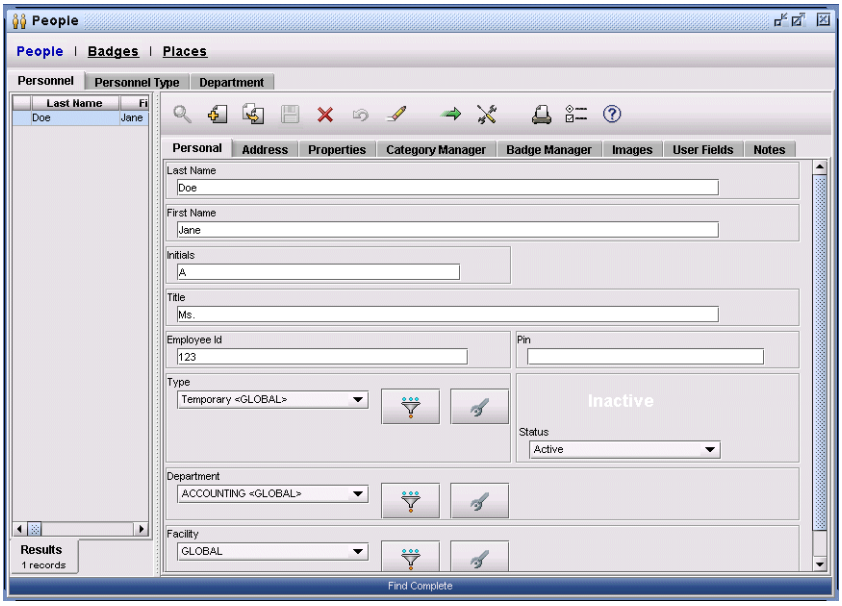
We recommend that Picture Perfect operators ensure that every modified Person record is saved after every individual action of assignment of a badge or un-assignment of a badge. Separating these workflow steps into two save operations is a recommended best practice that ensures integrity of data between host and micro controller.

Note: A search (FIND) using "indexed" fields improves the time required to find the records. Some examples of indexed fields on the Personnel form include: Last Name, First Name, Employee ID, Phone1, Last Access Reader, and Last Access Area.

Example

Jane Doe is a temporary employee assigned to the Accounting Department.

Figure 90. Personnel Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 93. Personnel form fields

Field name	Description
Last Name	Enter the badge holder's last name (up to 60 characters).
First Name	Enter the badge holder's first name (up to 60 characters).
Initials	Enter the badge holder's initials (up to 60 characters).
Title	Enter the badge holder's title (up to 60 characters). *Example: Mr., Mrs., Ms., Dr.*

Table 93. Personnel form fields (continued)

Field name	Description
Employee Id	Enter an alphanumeric employee identification (up to 36 characters). *Example: social security number.*
PIN	Enter a personal identification number (1 to 10 digits) for the badge holder to use with a badge-and-keypad reader.
Type	Click to display the Personnel Types list box. Select the desired type.
Status	Select one of the three personnel status descriptions. There is one type of Valid status (Active) and two types of Invalid badge statuses (Suspended and Deleted). You should update the status as needed. **Note:** The Status field on the Personnel form overrides this field on the Badges form. *Example: If a valid personnel record is suspended, this status change should be indicated in the Status box. Then, if the suspended person's badge is later tried in a reader, the system will deny access.*
Department	Click Department to display the Departments list box. Select the desired department for this badge holder.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Address 1 through Address 5	Enter the badge holder's address (up to 60 alphanumeric characters per field). The Address 1 through Address 5 field names can be changed using the Custom Form option.
Phone1	Enter the badge holder's phone number (up to 30 characters). You may type dashes or spaces between digits in the Phone field.
Phone2	Enter the badge holder's alternate phone number (up to 30 characters). You may type dashes or spaces between digits in the Phone field.
Download Upon Save	**WARNING: Use of this feature can *severely* impact system performance, and is recommended for GE Security Support personnel only.** If you select this button, any time a badge record is saved, it is downloaded to all micros, subject to the following conditions: • New Records: New records that are created by copying an existing record that has this field set to On will be automatically changed so that this field is set to Neutral. This prevents accidental downloads to all micros when using the Copy feature of the New button. You must manually set this field to On. • Updated Records: Updated records are only downloaded to all micros if the previous setting was set to Off. The next time a badge record field is changed for a badge record that previously had this field set to On, the record will only be sent to those micros that have learned this badge. **To resend an updated badge record to all micros:** 1. Set the Download Upon Save field to Off. 2. Save the record. 3. Make any other field changes, if needed. 4. Set the Download Upon Save field to On. 5. Save the record. If you select Off, any time a badge record is saved, it is only sent to those micros that have learned this badge record, which is the normal method of operation. This is the default for any new record, including those that were copied from an existing record. **Note:** Dial-up micros are handled according to the Dial Up settings on the Micros form.

Table 93. Personnel form fields (continued)

Field name	Description	
Person Trace	Use this field only when you want to trace the activity of a particular badge. Set to On to allow the Person Trace feature to track this badge. The letter "T" is inserted in front of the transaction when it appears on the Badge Monitor. Set to Off when you no longer need to trace the badge. See *Tracing badge holder activity* on page 388 for details on this feature. Person trace routing is defined on the System Parameters form.	
Person Trace Alarm	If Person Trace is enabled, this check box is available for selection. When checked, an alarm is generated every time the badge is read.	
Keypad Response	Set to On to give this badge holder the ability to respond to special alarms requiring keypad input. Set to Off if this feature is not required. See *Controlling alarms using a keypad code* on page 384 for details on this feature.	
Activation	Active Date	Enter the date the personnel record became active. If this field is left blank, the system will automatically enter the current date. **Note:** Change of a person's Activation date/time/context so it falls ahead of its badges issue date/time/context will change all its badges issue date/time/context to be the same as person's activation date/time/context. **Note:** Type the slashes (/) if the system date format requires them.
	Active Time	Enter the time the personnel record became active. If this field is left blank, the system will automatically enter the current time. **Note:** Type the colons (:) if the system time format requires them.
	TZ Context	The time zone to which the Activate Date and Time apply. See *Verifying time zones* on page 168.
Deactivation	Deactive Date	The date when the personnel record becomes deactivated by the system. If the date is in the past, none of the badges belonging to this badge holder will be usable. **Note:** Change of a person's Deactivation date/time/context so it falls before its badges expiration date/time/context will change all its badges expiration date/time/context to be the same as person's deactivation date/time/context.
	Deactive Time	The time when the personnel record becomes deactivated by the system. If the date is in the past, none of the badges belonging to this badge holder will be usable.
	TZ Context	The time zone to which the Deactivate Date and Time apply. See *Verifying time zones* on page 168.

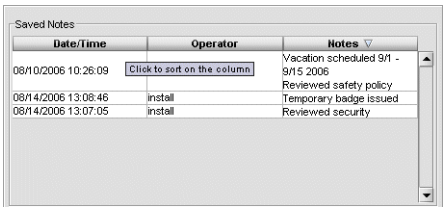
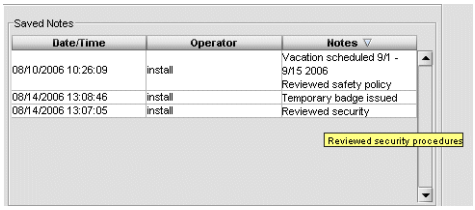
Table 93. Personnel form fields (continued)

Field name	Description	
APB Control	When used in conjunction with anti-passback readers, the Antipassback status of any badge belonging to this badge holder (plus a category match) regulate its ability to open a door. *Example: If a badge holder enters an anti-passback area without using his own badge (such as by following someone else through the open door), that person will not be able to exit that area with his own badge, because the system never registered him as having entered that area. Likewise, if a person exits an anti-passback area without using his badge, he cannot re-enter that area, since the system has not registered his exit.* Antipassback status is global, meaning the system will register whether someone is in or out, but it does not regulate the status on a per-reader basis. *Example: Someone can badge in at an anti-passback reader in one room, follow someone out of that room and into another anti-passback-controlled room without using his own badge, and then be able to badge out of the second room. The system registered him globally as in (without regard to reader location); therefore, he can badge out of any room. If he followed someone out of the first room and then tried to badge in at the second room, however, he would not be given access, because the system has him already registered as in. This example does not apply to Nested APB readers.* If the badge holder is required to use an anti-passback reader, assign the badge an anti-passback status of neutral; otherwise, leave these buttons unselected.	
	Neutral	Indicates an neutral user state, neither In nor Out. The next time any badge belonging to this badge holder is used in an anti-passback reader, the system will set the appropriate In/Out state. Use this setting when creating a new badge, or when a badge holder gets locked in or out of an anti-passback area. This status is not used by nested APB readers.
	In or Out	Indicates whether the last use of any badge belonging to this badge holder logged the badge holder In or Out of the anti-passback reader's area. This reflects information captured as of the moment the badge record was displayed, but the information will not be updated automatically while it is on the screen. It can be changed manually if necessary. This status is not used by nested APB readers.
	Privileged	Indicates that whenever any badge belonging to this badge holder is read by an anti-passback reader, the system ignores the anti-passback status. Access is granted if categories match the area, regardless of whether the badge holder was logged into or out of the area. Assign this status to a badge holder who has to use anti-passback readers, but is not to be governed by them. This status is used by nested APB readers.
	Reset Timed APB	This button sends a message to the micro to reset the Timed APB status back to Neutral.
	Reset Nested APB to Neutral	This button sets the Person Last Access area to neutral and sends a message to micros that have Nested APB readers configured to set APB area back to neutral. **Note:** You must have Schedule Updates Database enabled to use this feature if configuring NAPB with a reader event. See *Assigning system parameters* on page 40.
	Area	Indicates which area the badge was last granted access to.

Table 93. Personnel form fields (continued)

Field name	Description	
Access	The system tracks the badge and displays information about when it was last used. This reflects information captured as of the moment the badge record was displayed. This information can also be changed manually.	
	Date	The date the badge was last granted access. The system supplies this data.
	Time	The time the badge was last granted access. The system supplies this data.
	Time Zone Context	The time zone context in which the badge was last granted access. The system supplies this data. See *Verifying time zones* on page 168.
	Reader	Indicates which reader last granted access to this badge. The system supplies this data.
Category Manager	This tab contains the active categories, ordered by slot number, that can be assigned to an area or an area event. To access an area, a badge must match at least one category that is assigned to that area. You may add, remove, or replace a category in a slot. Click Filter to enter search criteria to limit the category list or use the type ahead search feature by clicking in any cell and typing the first letters of the item for which you are searching. For more information, see *Category manager* on page 244. **Note:** This field is position sensitive when used in conjunction with area category schedules.	
Badge Manager	The Badge Manager allows you to assign a badge to a person or to issue a temporary replacement badge. For more details, see *Badge manager* on page 251.	
Badge Form	You can access the Badge Form directly from the Badge Manager tab on the Personnel Form. For details on the Badge Form, see *Defining badges* on page 224.	
Images	This tab is available if you have the optional Imaging package installed. For information on capturing images and signatures, see *Capturing and displaying images* on page 237.	
User Fields	Enter information (up to 40 characters) in one or more user fields to identify the badge holder. *Example: license tag number* The number of user fields that appear on the Badges form is set to 40 on the Parameters form. The names of the user fields can be changed using Custom Forms. Custom lists can be assigned to user fields when creating custom forms.	

Table 93. Personnel form fields (continued)

Field name	Description
Saved Notes	All saved notes applicable to this record are listed including the Date/Time the note was created and the operator that created it. Click on a column heading to sort by Date/Time, Operator, or alphabetically by note.  By hovering the mouse over the note, the entire contents of the note displays. 
Notes	This is a free form text field where you can add information pertinent to Badge or Person records. *Example: Employee work visa will expire on 12/12/10.*

Related procedures

To create, edit, or delete a Personnel record:

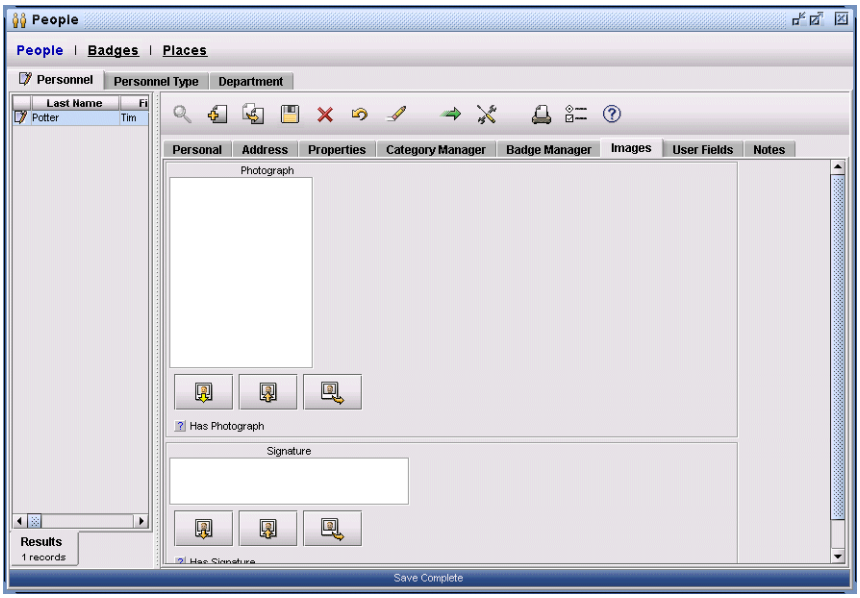
1. Select **Access**, **People**, and then **Personnel** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

Capturing and displaying images

Once Imaging is installed, you can capture, import, and view photographs and signatures from a variety of sources including digital cameras, video cameras, and signature pads.

During normal operations, images are not downloaded from the host. In order to view an existing image for a badge record, the image(s) must be loaded to the PC.

Figure 91. Personnel form: Images



Fields and controls

Table 94. Image tab fields

Field name	Control name	Description	
Photograph	Capture:		Click to capture an image. Depending on the input device used (such as a digital or video camera), the appropriate interface for capturing or loading a new image will display.
	Load:		Click to download the image associated with this personnel record.
	Export:		Click to export the image associated with this personnel record.
	Has Photograph:	Indicates that this personnel record has a photograph associated with it. Use this as a search criteria when searching for personnel with photographs.	

Table 94. Image tab fields (continued)

Field name	Control name	Description	
Signature	Capture:		Click to capture a signature. Depending on the input device used (such as a signature pad), the appropriate interface for capturing or loading the signature will display.
	Load:		Click to download the signature associated with this personnel record.
	Export:		Click to export the signature associated with this personnel record.
	Has Signature:	Indicates that this personnel record has a signature associated with it. Use this as search criteria when searching for personnel with signatures.	

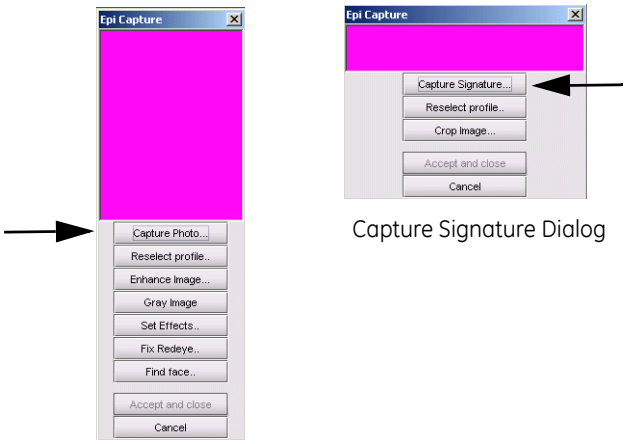
Related procedures

To select a capture input device:

1. From the **Access** menu, select **People**, and then click the **Personnel** tab.
2. Select the **Images** tab, and then click **Find**  to display a current list of records.
3. Select the Personnel record that the image is to be associated with, and then click **Capture**  .

   The Capture screen displays.

Figure 92. Capture dialogs

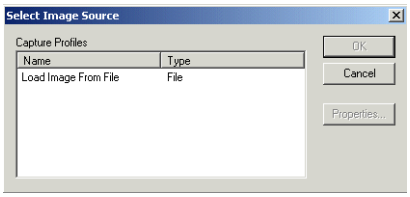


Capture Photo Dialog

Capture Signature Dialog

4. Click **Capture Photo** or **Capture Signature** to display the Select Image Source dialog box listing the available input devices on your computer. By default, the input device loads from a file.

Figure 93. Select Image Source dialog



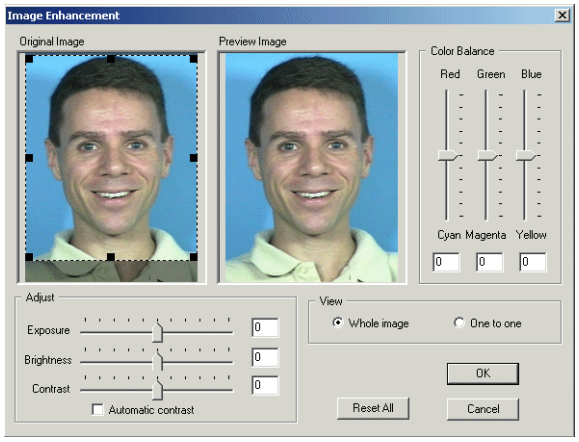
5. Select the device you will be using and click **Ok**. The next time you capture a photo or a signature, the program will use the input device you selected.
6. Repeat these steps to set up an input device for signature pads. The program recognizes a separate input device for photos and signatures.

To capture a new image for a record:

1. Click on the **Capture Photo** or **Capture Signature** button to capture a new image.

   Based on the input device selected, the proper interface will come up for capturing or loading a new image. When the new image is captured (live capture or loaded from a database), the Image Enhancement dialog box displays.

Figure 94. Image Enhancement screen



2. Note the eight sizing handles around the center of the image. Size the image as desired and press **Ok**.
3. At this point, you can either capture the portion of the image "as is," or adjust the highlighting box to capture a different portion of the image.

To move the crop box:

1. Place your mouse pointer within the highlighting box's cropping area.
2. Press and hold down your left mouse button, and drag (move) the cropping area to the desired location on the image. Release the left mouse button when you are satisfied with the new location of the highlighting box.
3. Click **Ok**.

To resize the crop box:

1. Place your mouse pointer directly over one of the highlighting box handles.

   The pointer will change from a four-headed arrow to a two-headed arrow. This allows you to resize the cropping area.

2. Press and hold down your left mouse button, and drag (move) the handle toward the center of the cropping area.
   The size of this highlighting box is fixed to the aspect ratio of the image type: 4 x 5 for photos; 5 x 1 for signatures.

3. When the cropping area is sized to your satisfaction, move the highlighting box so that it covers the portion of the image that you want to capture.

4. Click **Ok**.

5. When you have completed your changes, click **Ok**. Then, from the Epi Capture menu, select **Accept and Close**.

6. From the Images tab toolbar, click **Save** to save the record to your database.

To load the images for a record:

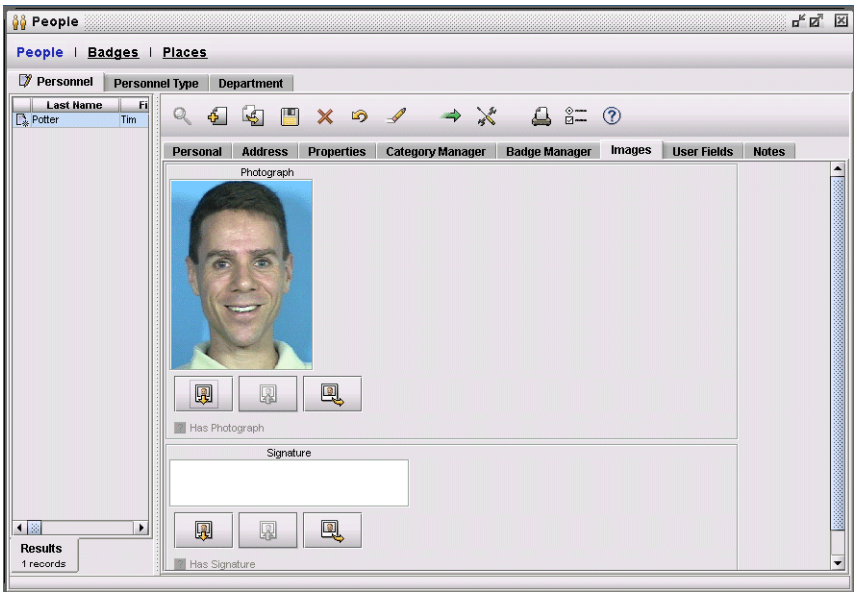
1. From the **Access** menu, select **People**, and then click the **Personnel** tab.

2. Select the **Images** tab, and then click **Find** to display a current list of records.

3. Select the Personnel record that the image is to be associated with, and then click **Load** .

   The image associated with the record displays.

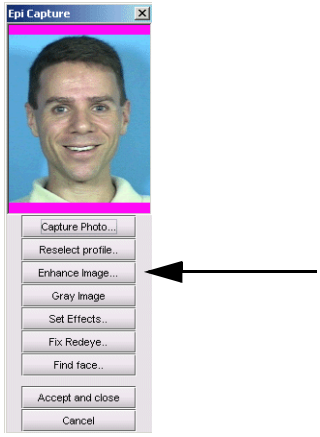
Figure 95. Personnel form: Load Image



To Crop and enhance:

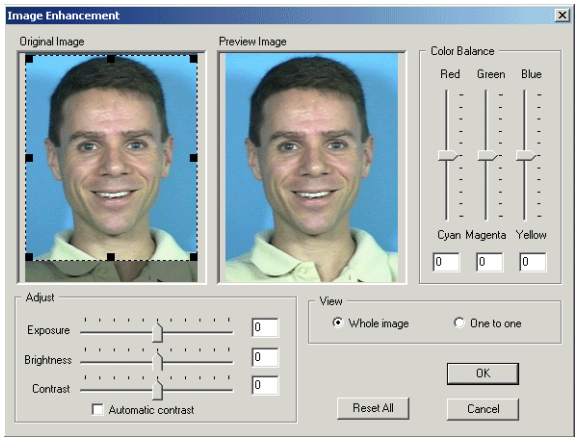
1. Click Capture to display the Epi Capture menu.

Figure 96. EPI Capture menu



2. This offers the option to individually **Enhance** the current image which allows you to adjust the existing image without having to recapture it.

Figure 97. Image Enhancement



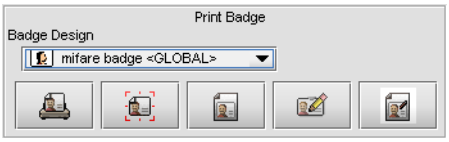
3. When you have completed your changes, click **Ok**. Then, from the Epi Capture menu, select **Accept and Close**.

4. From the Images tab toolbar, click **Save** to save the record to your database.

Printing badges

Once the optional Imaging package is installed, the Print Badge dialog on the Badge form and on the Badge Manager of the Personnel form is enabled.

Figure 98. Print Badge



Fields and controls

Table 95. Print badge controls

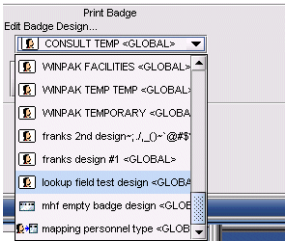
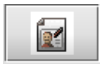
Control name/icon		Description
Badge Design:		Select a badge design or a design mapping from the drop-down list. Beside each design one or two icons appear. • The Person icon indicates the design references a field on the Personnel form and therefore a personnel record must be selected in order to print a badge using this design. • The Badge icon indicates the design references a field on the Badge form and therefore a badge record must be selected to print a badge using this design. • If both icons display, both a personnel and a badge record must be selected in order to print the badge.
Print:		Click to print a badge. **Note:** If this button appears dimmed, refer to *Overview* on page 394 for assistance.
Preview:		Click to view a badge without printing to a printer. **Note:** If this button appears dimmed, refer to *Overview* on page 394 for assistance.
Page Setup and Options		Click to display the Print Options dialog from which you can select the following options:
	Page Setup	Click to select the page orientation, Portrait or Landscape, and the number of badges to be displayed across and down a page. **Note:** The page orientation must match the badge design orientation for the badge to print correctly.
	Encoder Setup	Displays the Card Printer Encoder Setup dialog which allows you to set encoding parameters specific to your Magstripe, Smartchip, or Proximity cards.
	Show print setup dialog	When this option is selected, the Print Dialog displays before printing a badge. This allows you to change the printer selection and properties prior to printing.
	Print Badges to:	Select the printer to be used for printing the badge design.
Encode		Click this button to encode a MIFARE badge. **Note:** If this button appears dimmed, refer to *Overview* on page 394 for assistance.

Table 95. Print badge controls

Control name/icon		Description
External Encoder Setup		Click to launch the External Encoders Setup dialog.

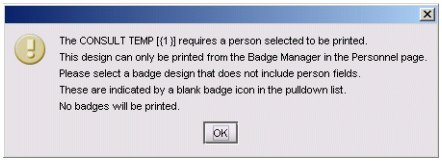
Related procedures

To print a badge from the Badges form:

1. From the **Access** menu, select **Badges**, and then click the **Badges** tab.
2. Click **Find** to display a current list of records.
3. Select the badge record that you want to print. Then, under Print Badges, select a badge design or a design mapping from the drop-down list.

   Note: Make sure there is *not* a Person icon beside the design. If the design is associated with a Personnel record, an error message similar to the following displays:

Figure 99. Error message



4. Click **Print** .

   The badge will print to the printer designated as the default printer for the Imaging terminal.

   Note: If a secondary Printer Setup dialog box displays in the background, access the window either from the Windows taskbar or by typing Alt + Tab. Then, close the window.

   Note: If this button appears dimmed, refer to *Overview* on page 394 for assistance.

To print a badge from the Personnel form:

1. From the **Access** menu, select **People**, and then click the **Personnel** tab.
2. Click **Find** to display a current list of records.
3. Select the personnel record whose badge you want to print.
4. Click the **Badge Manager** tab. The active badges assigned to the selected badge holder are displayed.
5. Select the badge to print and under Print Badges, select a badge design or a design mapping from the drop-down list.
6. Click **Print** .

The badge will print to the printer designated as the default printer for the Imaging terminal.

Note: If a secondary Printer Setup dialog box displays in the background, access the window either from the Windows taskbar or by typing Alt Tab. Then close the window.

Note: If this button appears dimmed, refer to *Overview* on page 394 for assistance.

Category manager

Use the Areas, Badges, and Area Events forms to assign new categories or to change or remove categories already assigned. Each of these forms contain a Category Manager tab, that displays the active categories assigned to the selected personnel (badge holders), area, or area event on one side and the categories that are available for assignment on the other.

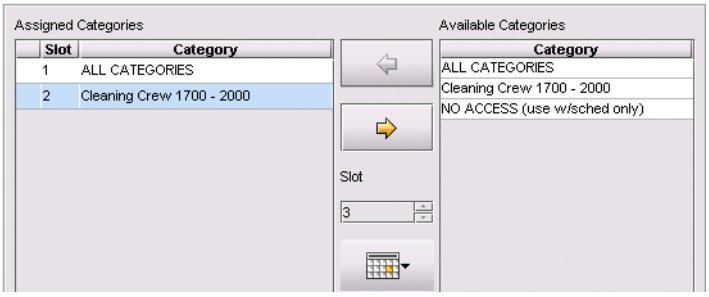
Example

You can assign categories to an area and then schedule area events to change the categories depending on access requirements. Categories are position-sensitive, so be careful not to overwrite categories that should remain intact.

For example:

- An area event can change the categories on an area for a specific time to control which badge holders have access to the area during that time. If you assign a different category to each computer-operator shift, then you can control when certain staff members can access the computer room. Set up area events that add and remove the categories from the area.
- A series of area events that add and remove a single category can control the time frame in which a contractor's job is performed. For example, one area event adds a category to the R&D Lab at 4:00 PM to allow the cleaning crew access; another area event removes the category at 4:30 PM to restrict the time spent in this area. You can use the same strategy to restrict access to a computer vault where daily backups are stored. The categories on an area control who can enter the area, when they can enter, and how long they can remain.
- An area event can change the categories of an area at a specific time. For example, two MIS shifts need to access the computer room during separate times, but the MIS Manager needs access 2 hours a day. The two shifts also require a 30-minute overlap during shift changes. To provide 24-hour access for the MIS manager, create a category (such as MIS 24-Hour) on the Areas form and do not overwrite this category with an area event. The two shifts will require separate categories (such as MIS Shift 1 and MIS Shift 2), which will be used on the Area Events form. Use the None category (pre-defined) to remove an existing category from its slot.

Figure 100.Category Manager form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 96. Category Manager form fields

Field name	Description
Assigned	This is a list of all assigned categories in alphabetical order. Categories which have already been assigned, have their slot number indicated to their left. Active categories, assigned to a temporary category schedule, have an icon before their slot number.
Available	This is a list of all available categories in alphabetical order. To jump quickly to an item in the list, use the type ahead search feature by clicking in any cell and typing the first letters of the item for which you are searching.
Add	Click on this button to add a permanent category to a slot. The category list on the form will be refreshed and will display the new category. This button is enabled when an available category and an empty slot number are selected. By default, the next empty slot number is selected when you select an available category. **Note:** Double clicking will also move the category from the Available to the Assigned column.
Remove	Click on this button to remove a permanent category from a slot. The category list on the Badges form will be refreshed and will no longer display the removed category slot number. This button is enabled if an active category or the corresponding slot number is selected. **Note:** Double clicking will also move the category from the Assigned to the Available column.
Slot	This spin box displays the next available slot. Click the up/down arrow to select a specific slot.
Calendar	When you click the calendar on the Category Manager, the Category Scheduler displays. From here you may define the properties of the schedule.
Filter * . ?	Click Filter to enter search criteria to limit the category list. The following wildcards can be used to help delimit the search: An asterisk can expand the search in either direction around a string of characters. For example, `map*` would return `map`, `maps`, `mapped`, `mapping`, etc. A period replaces a specific character. For example, `map.` would return `maps` A question mark can replace a single character if one exists or ignore it if it does not. For example, `map?` would return `map` and `maps`.

Related procedures

To add a category to the next available slot:

1. Click the **Category Manager** tab. A list of all assigned categories, in alphabetical order, will display on the left pane. If a category has been assigned a slot, the slot number will be displayed beside it. All available categories will display on the right pane.
2. Select the desired category from the Available column on the right.

   The next available slot will be highlighted. 

3. Click  or double click the selected category. The new category and the slot number to which it was assigned displays in the Assigned column on the right.

To add a permanent category to a specific available slot:

1. Click the **Category Manager** tab.

   A list of all assigned categories, in alphabetical order, will display on the left pane. If a category has been assigned a slot, the slot number will be displayed beside it. All available categories will display on the right pane.

2. Select the desired category from the Available column on the right.

   The next available slot will be highlighted. 

3. Select the specific slot to which you want to assign the new category and then click  .

   The new category and the slot number to which it was assigned displays in the Assigned column on the right.

To remove a category from a slot:

1. Click the **Category Manager** tab.

   A list of all assigned categories, in alphabetical order, will display on the left pane. If a category has been assigned a slot, the slot number will be displayed beside it. All available categories will display on the right pane.

2. Select the desired category from the Assigned column on the left.

3. Click  or double click the selected category.

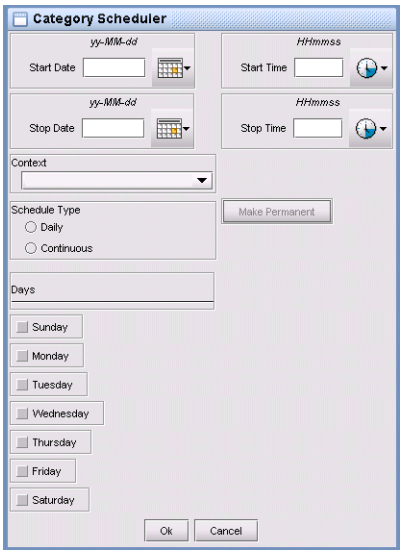
   The category is moved to the Available column and the slot number is removed.

Category scheduler

When you click the calendar on the Category Manager, the Category Scheduler displays. From here you may define the properties of the schedule. Category schedules are set to be enabled during certain times of the day and will expire on a certain date and time. They are selected and set based on an individual personnel record.

Note: Micros must be properly installed before Category schedules become active. In addition, for this feature to work, communications must be present between the host and micro.

Figure 101.Category Scheduler form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 97. Category Scheduler form fields

Field name	Description
Start Date	Enter the date on which the category schedule is to be enabled. Use the format of your system date as set on the Parameters form or use the Calendar icon to set the date.
Start Time	Enter the time at which the category schedule is to be enabled each day (for a Daily schedule type). *Example: Select start times that occur on the hour or half hour. Use the format of your system time as set on the Parameters form or use the Clock icon to set the time.*
Stop Date	Enter the date on which the category schedule is to expire. Use the format of your system date as set on the Parameters form.
Stop Time	Enter the time at which the category schedule is to expire each day (for a Daily schedule type). *Example: Select stop times that occur on the hour or half hour. Use the format of your system time as set on the Parameters form.* The enabling and disabling of temporary categories is logged in operator history.

Table 97. Category Scheduler form fields (continued)

Field name	Description
Context	Specify a context of either Host, Micro, or Operator. This allows you to schedule categories in any of those contexts.
Schedule Type	Choose a schedule type of Daily or Continuous. • A Daily schedule type means that the category will be enabled each day at the Start Time and will be disabled each day at the Stop Time. The default schedule type is Daily. • A Continuous schedule type means that the category will be enabled at the Start Time of the Start Date and will be disabled at the Stop Time of the Stop Date.
Days	You can restrict the days of the week that a category schedule will be enabled. A week day that is selected means that the schedule can run on that day. A week day that is not selected prevents the schedule from running on that day. This has no effect on the Continuous schedule type.

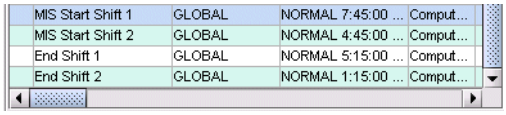
Related procedures

Examples of how to use category assignment

The categories on an area control who can enter the area, when they can enter, and how long they have access to the area.

Example 1: Control who can enter

An area event can change the categories on an area for a specific time to control which badge holders have access to the area during that time. If you assign a different category to each computer-operator shift, then you can control when certain staff members can access the computer room.



Four area events are defined:
one to start Shift 1 at 07:45 AM,
one to end it at 5:15 PM,
one to start Shift 2 at 4:45 PM,
and one to end it at 1:15 AM.

Example 2: Control how long they have access to the area

A series of area events that add and change a single category can control the time frame in which a contractor's job is performed. For example, one area event adds a category to the R&D Lab at 4:00 PM to allow the cleaning crew access; another area event replaces the category at 4:30 PM to restrict the time spent in this area. You can use the same strategy to restrict access to a computer vault where daily backups are stored.

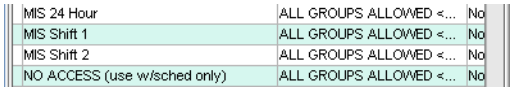
Two area events are defined:
one to allow access to the Clean-
ing crew at 4:00 PM,
one to end it at 4:30 PM.

Example 3: Control when they can enter

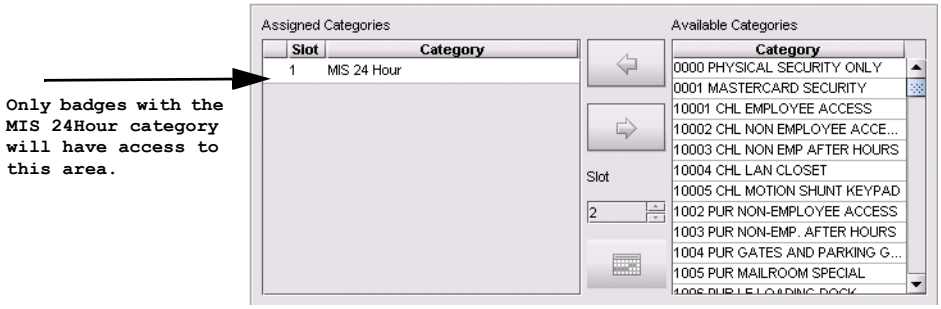
An area event can change the categories of an area at a specific time. For example, two MIS shifts need to access the computer room during separate times, but the MIS Manager needs access 24 hours a day. The two shifts also require a 30-minute overlap during shift changes.

To control when they can enter:

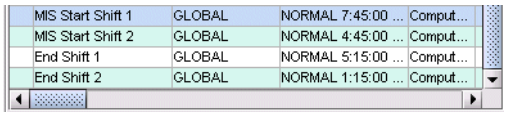
1. First, create three categories, using the Categories form: MIS 24 Hour, MIS Shift 1, and MIS Shift 2.



2. To provide 24-hour access for the MIS manager, assign the MIS 24 Hour category on the Areas form. (Do not overwrite this category with an area event.)



3. To provide access to the two shifts, create separate categories, MIS Shift 1 and MIS Shift 2 to an area event using the Area Events form. Use the category, NO ACCESS (use w/sched only) to end the event. When you assign the area events to a slot, remember that the MIS 24 Hour category was placed in the first position (slot) on the Areas form; since categories are position sensitive, when you add a category, do not overwrite an existing category. Notice that categories entered on previous forms do not display on the current Events form, so you must be familiar with what is already in place.



Four area events are defined:
one to start Shift 1 at 07:45 AM,
one to end it at 5:15 PM,
one to start Shift 2 at 4:45 PM,
and one to end it at 1:15 AM.

4. When the area events occur, the Category Manager on the Areas form will reflect the new categories.

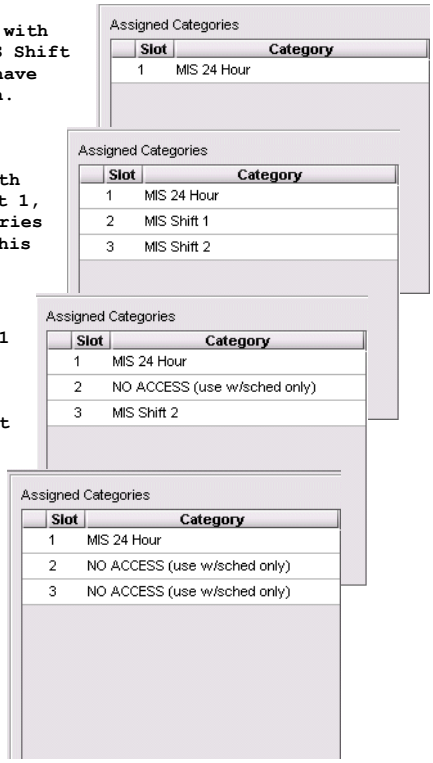
Note: The Schedule Updates Database field on the System Parameters field must be set to Yes. See *Table 24, Parameter Form Fields* on page 42.

At 7:45 AM, badges with MIS 24 Hour and MIS Shift 1 categories will have access to this area.

At 4:45 PM, badges with MIS 24 Hour, MIS Shift 1, and MIS Shift 2 categories will have access to this area.

At 5:15 PM, when Shift 1 ends, badges with MIS 24Hour and MIS Shift 2 categories will have access to this area, but MIS Shift 1 will have NO ACCESS.

At 1:15 AM, badges with the MIS 24 Hour category will have access to this area, but MIS Shift 1 and MIS Shift 2 will have NO ACCESS.



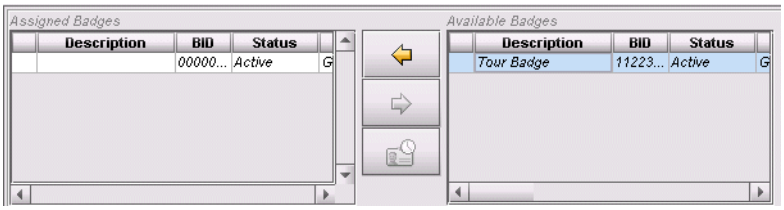
Badge manager

Use the Personnel forms to assign new badges or to change or remove badges already assigned. The Badge Manager tab displays the active badges assigned to the selected badge holder on one side and the badges that are available for assignment on the other.

Example

In addition to his normal access control badge, a security guard is issued a tour badge to be used when conducting a facility tour at specified intervals.

Figure 102.Badge Manager form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

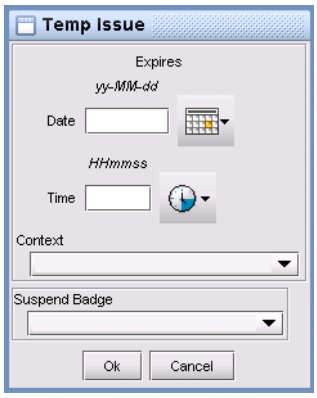
Table 98. Badge Manager form fields

Field name	Description
Assigned Badges	This is a list of all badges assigned to this badge holder (personnel record), regardless of facility. If the badge's facility is not in the operator's selected facilities, the operator will only be able to view, not edit, the badge assignment. If multiple personnel records are selected, only those badges that are common to all records will be displayed.
Available Badges	This is a list of all available badges not assigned to this badge holder (personnel record). Only those records in the operator's selected facilities will be displayed. The operator must have Update permission to the Badge Manager.
Assign Button	Click on this button to add a badge to a personnel record. The badge will appear in the Assigned grid.
Remove Button	Click on this button to remove a Temporary badge or to remove a permanent badge from a personnel record prior to the record being saved. The badge will be removed from the Assigned grid.
Temp Issue	Click to display the Temp Issue dialog. This is used to assign an available badge to a personnel record with an expiration date. Current active badges are suspended.
Badge Form Fields	See *Table 92* on page 225.

Temp Issue

You may replace a permanent badge with a temporary badge, when an employee forgets or misplaces their permanent badge. The permanent badge is suspended, the categories and employee details are copied to the temporary badge and the temporary badge is activated. A pool of badges can be used for temporary reissues.

Figure 103.Temp Issue form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 99. Temp Issue form fields

Field name	Description
Expires Date	The date the temporary badge expires.
Expires Time	The time the temporary badge expires.
Context	The time zone context in which the badge expires: Host, Micro, or Operator. See *Verifying time zones* on page 168.
Suspend Badge	All of the active badges that are currently assigned to this personnel record are listed. If desired, select which badge to suspend. By default, the first badge in the list will be suspended.

Related procedures

To create a pool of temporary badges:

1. Select **Access**, **Badges**, and then **Badges** tab.
2. Complete the Badges form. Under Options, click the **Temporary** button.
3. Press **Save** .

To issue a temporary badge:

1. Select **Access**, **People**, and then **Personnel** tab.

2. Click **Find** to search for the badge holder record for which you are issuing a temporary replacement badge.
3. Click the **Badge Manager** tab.
4. From the **Available Badges** column, select a temporary badge and click the Temp Issue button .

   The Temp Issue window will display.
5. Enter the date and time that the temporary badge will expire.
6. Click **Suspend** to select the permanent badge that should be suspended.
7. Click **Ok**.

Chapter 12 Badge design

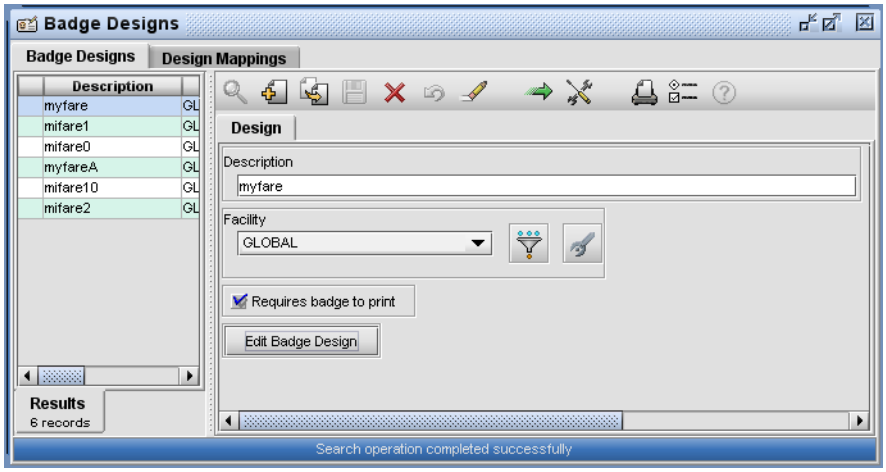
This chapter describes how to set up photo badge designs and link the designs to badge holder (Personnel) records, signatures, and images stored in the Picture Perfect database. These features are available if you have the optional Imaging package installed.

In this chapter:

Setting up badge designs

The first step in producing printed badges is to create a badge design or card layout. The badge design determines the card's background, size, and placement of objects, such as logo, photo, signature, text, or barcode fields that will be displayed on the badge. A specific design can be selected, at print time, using a design mapping based upon field values in the badge or personnel record or a specific design can be assigned to print the badge.

Figure 104.Badge Designs form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 100. Badge Designs form fields

Field name	Description
Description	The name used to describe the badge design. *Example: Temporary*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Requires badge to print	By default, this toggle button is checked, which requires a badge record be associated to the design in order to print. There may be cases where you want to print a badge design for identification purposes only, such as a temporary paper badge, in which case you should toggle this button off.
Edit Badge Design	Click to access the Badge Designer. When you have completed your changes, save the new badge design. For further information, see the *Credential Designer Manual* included on your documentation CD.

Related procedures

To create, edit, or delete a Badge Design record:

1. From the **Setup** menu, select **Badge Designs**, and then click the **Badge Designs** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

To encode a Mifare badge:

1. From the Access menu, select People, Personnel, and then the Badge Manager tab.
2. Under **Print Badge**, select the **External Encoder Setup** button.
3. In the External Encoders Setup dialog, select the **Specialized** tab. Select the Mifare badge, and then click the right arrow to move it from the Unused encoders pane to the Defined encoders pane.
4. Click the **Setup** button to open the Mifare Generic Encoder Setup window.
5. Select the **Key Pairs** tab to create a new key pair ID. You must contact Customer Support to generate a new key pair ID. Refer to *Contacting Technical Support* on page 406.

   Note: By default, a GEKey pair ID is already set in the Mifare badge design. However, for security purposes, it is important to create a unique key pair ID, and then set the Mifare badge design to use that key.

To create a Mifare badge design:

1. From the **Setup** menu, select **Badge Designs**, and then click the **Badge Designs** tab.
2. Click the plus sign to create a new record. This will open the New Badge Design form.
3. Complete the form, and then check the **Mifare Encoding** check box. Click **OK**.

   The Badge Designer application opens to allow you to customize this badge. Refer to the *Credential Designer User Manual* for more information on using Badge Designer.
4. In the Badge Designer, select **File**, and then **Layout Properties**.
5. On the General tab, click on the **Encoding** button. The Card Encoding dialog opens.
6. In the Card Encoding dialog, click on the **Define** button, and then select the **Security** tab.
7. By default, a Mifare badge design has the GEKey Key-Pair ID defined on sector 1. Once you have created your own key pair ID, you must enter it here. Refer to *Mapping badge designs* on page 257. Click OK.
8. In the Card Encoding dialog, click on the **Define** button, and then select the **Data** tab.
9. In the left-hand pane, click **WiegandData**. Under Field or Expression Definition, Badge ID 5502 is the default selected value. If required, click the list box to select Badge ID 26-bit. Click OK.

   Note: Badge ID 5502 requires badge format Standard 16 Digit Badge. Badge ID 26-bit requires badge format Standard 10 Digit Badge.
10. Close all open windows, and then close the Badge Designer. Click **OK** to save all changes.

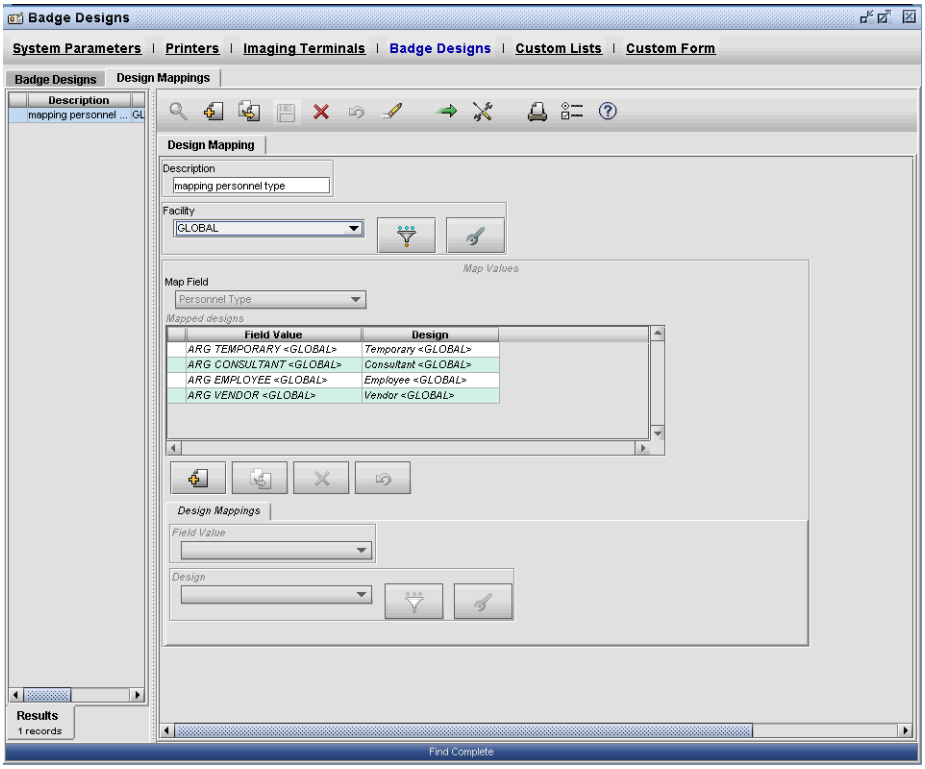
Mapping badge designs

A design mapping allows you to select a badge design based on a field value in the Personnel record. For instance, all members of a certain department may require the same badge design.

Example

A design mapping, “mapping personnel type,” links the following badge designs to the Personnel Type field: Temporary, Consultant, Employee, and Vendor.

Figure 105.Design Mappings form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 101. Design Mappings form fields

Field name	Description
Description	The name that identifies the design mapping. *Example: Facility Mapping, to map all badge records belonging to a specific facility.*
Facility	This is a required field. Assigning a badge design record a facility, allows the administrator to filter the records that can be viewed. See *Creating facilities* on page 53.
Map Values	• Map Fields: The field to be used for mapping: Department, Facility, or Personnel Type. After a design mapping has been saved, the field used for the mapping cannot be changed and will be dimmed or "grayed out." • Mapped Designs: The designs assigned to the corresponding field value are displayed in this column.
Design Mappings	• Field Value: A drop-down list of values associated with the selected field. The Default value allows you to set a default design for any values not directly mapped. • Design: A drop-down list of existing badge designs. A blank value removes the mapping from the Mapped Designs list.

Related procedures

To create a new design mapping:

1. From the **Setup** menu, select **Badge Designs**, and then click the **Design Mapping** tab.
2. Refer to *Creating, editing, deleting, and printing records* on page 36.

To assign a new design to a design mapping:

1. From the **Setup** menu, select **Badge Designs**, and then click the **Design Mapping** tab.
2. Click **Find** and select the design mapping you want to edit.
3. In the **Map Values** pane, click **New**. The Field Values and Design buttons are enabled. Click **Field Values** and select the new value to add to the design mapping.
4. Click **Design** to display a list of badge designs. Select a design to associate with each Field Value.

To remove a design from a design mapping:

1. From the **Setup** menu, select **Badge Designs**, and then click the **Design Mapping** tab.
2. Click **Find** and select the design mapping you want to edit.
3. In the **Map Values** pane, select the mapping entry to be removed.
4. Click **Delete** to remove the entry.

Setting a default badge design

The system default for a badge design is set in a manner similar to setting a printer default. When selected, the system default will be used when no other design is specified.

The Default Badge Design field appears on the System Parameters form and displays a list of defined badge designs. See *Assigning system parameters* on page 40

Beside each design one or two icons appear.

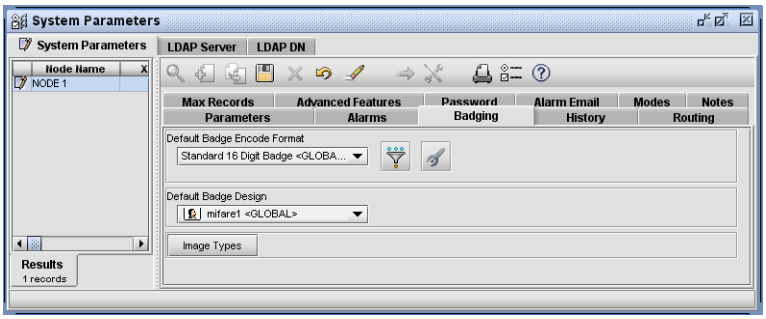
- The Person icon indicates the design references a field on the Personnel form and therefore a personnel record must be selected in order to print a badge using this design.
- The Badge icon indicates the design references a field on the Badge form and therefore a badge record must be selected to print a badge using this design.
- If both icons display, both a personnel and a badge record must be selected in order to print the badge.

Note: A personnel or a badge record must be selected in order to print a badge.

Example

In Figure 106, a default badge design “Employee” is used if no other design is selected when printing a badge.

Figure 106.Parameters form: Default badge design



Related procedures

To set a default badge design:

1. From the **Setup** menu, select **System Parameters**, and then click the **System Parameters** tab.
2. Under Badging, click **Default Badge Design** and select a design from the list.
3. Click **Save** .

Chapter 13 Alarm/activity monitors

This chapter shows you how to view and control incoming alarms and messages that display on the various system monitors. Readers should familiarize themselves with the information in this chapter before continuing to other chapters in this document.

In this chapter:

Overview

Picture Perfect allows you to monitor various aspects of your system using alarm and activity monitors, as well as system monitors that monitor file systems, database usage, and TPS alarms.

Real-time activity displays in a scrolling window. The queue of messages on the monitor scrolls upwards as new messages appear at the bottom. You can control the amount of information the monitor displays by clicking Preferences from the toolbar and selecting the desired columns. You can configure your system to control the inputs and outputs associated with these alarms and messages and the way in which an operator responds to them.

To see all the columns on a monitor, stretch the window frame (use the point-and-drag method).

Monitor toolbars

The following icons appear on the toolbar of the various monitors.

Table 102. Monitor toolbar icons

Icon	Description
Freeze/Unfreeze 	To temporarily stop the Monitor from scrolling, click Freeze. The system continues to queue messages and will resume scrolling the stored information when you click Unfreeze.
Search 	The Search function is available when the number of incoming alarms cannot be displayed in a single screen. If it is possible to display all alarms on a single screen, this function will be disabled. Click to open a search text criteria dialog box where you can enter a string of text. Choose a column from which to search, such as Valid, Invalid, Suspended. The row containing the results of the search is highlighted in green.
Save 	Use the Save function to temporarily save the data in the Monitor to a file on the operator's workstation, which can be used later for troubleshooting. The next time the Save function is used, the current file is overwritten by the new file.
Print 	Click to preview the data displayed in the monitor in a report format. You have the option of printing to a default printer or saving the report in electronic format (.pdf file).
Preferences 	Click to display the Preferences window where you can manipulate the columns that you want displayed. *Example: If you do not want to view alarms in Host time, you can remove those columns, by moving them from the Active to the Inactive column.* You can also access the Active Facility Set window where you can change the facility set and the time zone selection for the current session. See *Verifying time zones* on page 168. **Note:** Active Facility Set settings/selections from the preferences dialog apply only to that page. The Preferences button in the Monitor applications is only available if the "Monitor Preferences" action permission is enabled for this operator's system permission profile.

Table 102. Monitor toolbar icons (continued)

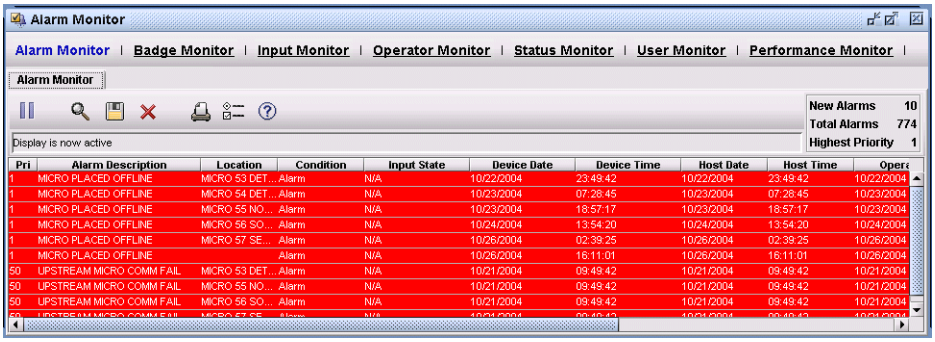
Icon	Description
Clear 	Click to clear the contents of the monitor.
Help 	Click to display online help about the Monitor. To navigate the entire Picture Perfect help system, click Show.
Execute (Status Monitor only) 	Click Execute to generate a status report of the selected characteristics. The report displays in the Results window at the bottom of your screen. Use the scroll bar to view the entire contents of the report.
Purge (Alarm Monitor only) 	If you are having hardware problems and need to clear alarms that will not reset, click Purge in the Alarm Monitor. The system logs the alarms and deletes them all from the monitor, even if they are not reset.
Remove (Alarm Response Window) 	To clear a single alarm that is *not* in a reset condition, highlight the alarm and click Remove in the Alarm Response window. The system logs the alarm (and its responses) and deletes it from the Alarm Monitor. The Alarm Response window can be configured to have the Remove button unavailable unless the alarm is in reset state or has the alarm control Immediate Reset Input set (done on the Alarm form). The configuration is determined by the Enforce UL Specifications parameter in the System Parameters form. The default is No, indicating the Remove button is always available. When set to Yes, the Remove button will be grayed out when an alarm is *not* in a reset condition.
Purge (Alarm Response Window) 	If you are having hardware problems and need to clear individual alarms that will not reset, click Purge in the Alarm Response window.
Outputs (Alarm Response Window) 	An alarm may have associated outputs that require manual reset. You can turn the entire output group on or off, or turn each individual output on or off. See *To control Alarm Outputs:* on page 268.
	If you have Send Message permission, this icon is enabled on the User Monitor which launches the Send Message dialog. Click this icon to send a message to all logged on users. See *Monitoring users* on page 281.

Monitoring alarms

The Alarm Monitor displays incoming alarms and their priority, count, status, and time of occurrence. Alarms display on the Alarm Monitor in order of their priority. The display of alarms within the Alarm Monitor is filtered by the operator's active facility set, so that the operator will only see alarms that are tagged with a facility in their active facility set. By default, incoming alarms are assigned the facility of the micro from which they originate, but this can be changed to assign the facility based on Input, Input Group, Alarm, or Location using the Alarm Filter fields on the System Parameters form.

New alarms will blink for the time specified by the alarm's configuration. When an alarm occurs, the system beeps and displays a pop-up window to notify the operator. Instructions for the alarm are displayed by selecting the alarm from the Alarm Monitor. The operator records a response to an alarm either by selecting pre-written alarm responses from the Alarm Response window or by typing a response.

Figure 107. Alarm Monitor



Fields and controls

Table 103. Alarm Monitor columns

Field name	Description	
Priority	The priority level assigned to the alarm in the Alarms form. This tells the system in which order it should alert the operator, should multiple alarms occur at the same time.	
Alarm Description	The alarm's text description as defined in the Alarms form.	
Location	The alarm location can be an 8RP board number or the description field of any of the following forms: Inputs, Readers, Micros, or Input Groups.	
Condition	Alarm	The alarm is in the active alarm state (either Open or Closed). The active alarm state for an alarm is defined in the Alarms form.
	Reset	The alarm has been reset or turned off. It is no longer in the active alarm state.
	Tamper	The wiring of the alarm input has been cut or tampered with.

Table 103. Alarm Monitor columns (continued)

Field name	Description	
Input State	Open	The wires connecting the input are registering more than normal (infinite) resistance, indicating the connection has been broken.
	Closed	The input contacts are in the closed position.
	N/A	This field is not applicable for this type of alarm.
	Short	The wires connecting the input are registering less than normal or no resistance, indicating the contact has been bypassed.
	Cut	
Device Date	The date the alarm occurred, in the time zone context of the device. See *Verifying time zones* on page 168.	
Device Time	The time the alarm occurred, in the time zone of the device. See *Verifying time zones* on page 168.	
Host Date	The date the alarm occurred, in the time zone of the host. See *Verifying time zones* on page 168.	
Host Time	The time the alarm occurred, in the time zone of the host. See *Verifying time zones* on page 168.	
Operator Date	The date the alarm occurred, in the time zone of the operator. See *Verifying time zones* on page 168.	
Operator Time	The time the alarm occurred, in the time zone of the operator. See *Verifying time zones* on page 168.	
Process State	Active	Alarms that have not been acknowledged.
	Pending	Alarms that have been acknowledged but not removed.
	Completed	Alarms that have been removed but not reset.
	Bumped	Active alarms that have been bumped to another operator.
	Notified	Active alarms sent to the Network alarm Notification manager.
	Remote	Alarms sent to the Remote Alarm Notification manager.
Facility	The facility of the alarm as determined by the Alarm Filter setting on the System Parameters form.	
Count	The number of times the alarm has set and reset.	

Related procedures

To view alarms on the Alarm Monitor:

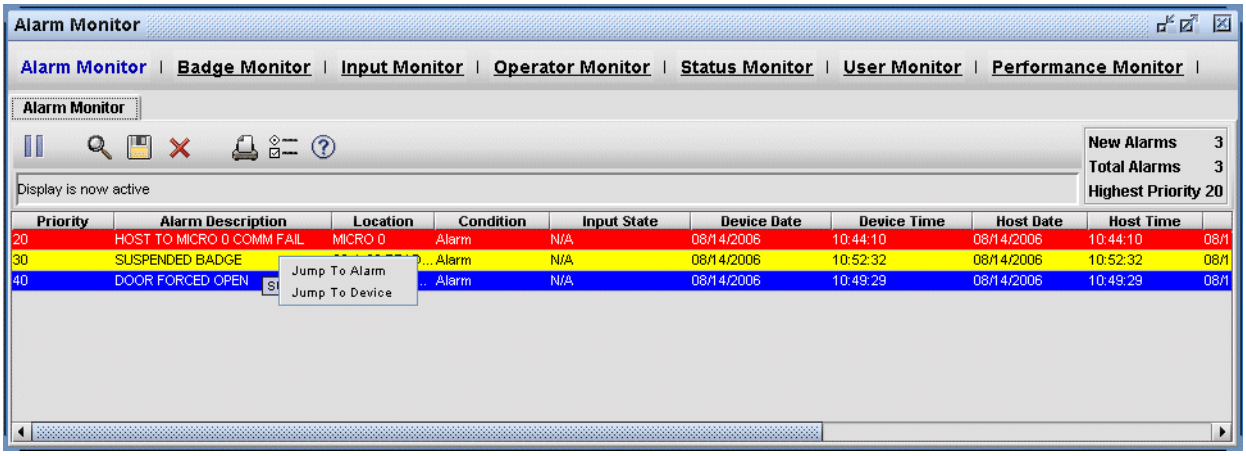
Use the Alarm Monitor window to view and select any alarms that occur: active, pending, or completed. Alarms that are not yet acknowledged are active; alarms that are acknowledged but not removed are pending; and alarms that are removed but not yet reset are completed.

1. From the **Monitor** menu, select **Alarm Monitor**.
2. To view all the columns on the Alarm Monitor, stretch the window frame or use the scroll bar.

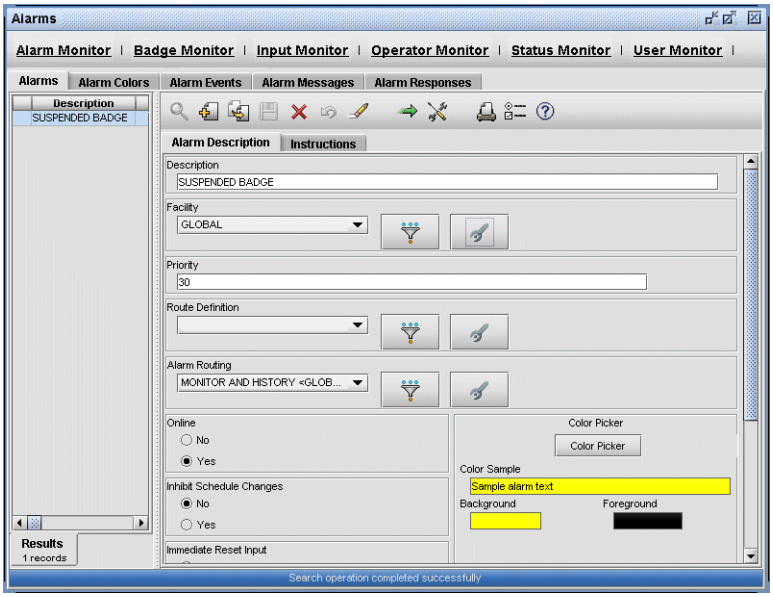
To jump to a record from the Alarm Monitor:

Note: If an operator does not have permission to view the associated record, the option is dimmed.

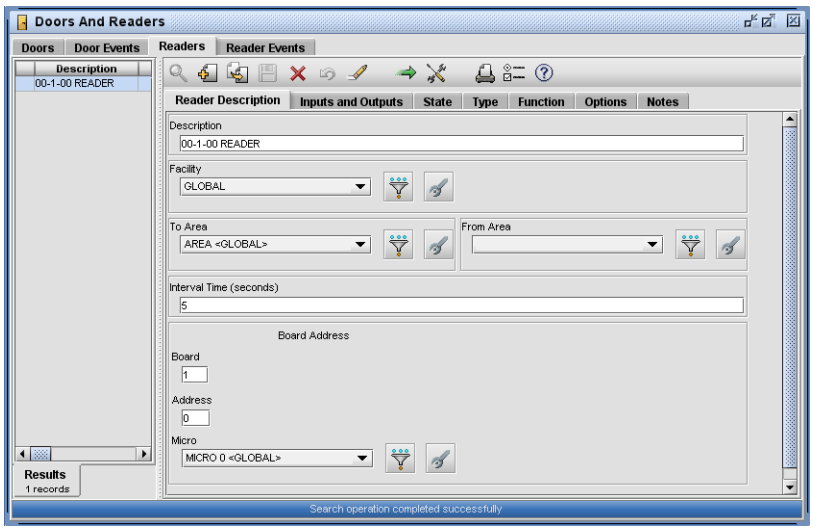
1. From the **Monitor** menu, select **Alarm Monitor**.
2. Right-click an alarm to display the following menu.



3. If you select **Jump to Alarm**, the associated alarm record displays, such as the following:



If you select **Jump to Device**, the associated device record displays, such as the following:



To use the Alarm Alert pop-up:

1. When an alarm occurs, a pop-up Alarm Alert window appears for every operator that is configured to receive alarms. The window beeps and displays the number of new alarms, the number of unanswered alarms, and the highest priority alarm that is pending.
2. Click **Silence**, to stop the beeping. The button will change to **Stand By**. If another alarm occurs, the beeping resumes and the information displayed is updated.

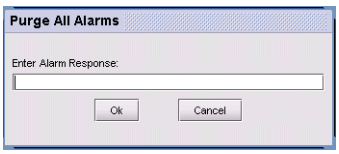
To remove all alarms from the Alarm Monitor:

If you are having hardware problems and need to clear alarms that will not reset, use **Purge** ✕ in the Alarm Monitor. The system logs the alarms and deletes them all from the monitor, even if they are not reset.

Note: An operator must have system permission to have access to the Alarm Monitor **Purge** button.

1. Click **Purge** ✕ located on the Alarm Monitor (not the Alarm Response window). The Purge All Alarms window appears.

Figure 108. Purge All Alarms



2. Type the reason for clearing all alarms (for log records).
3. Click **OK** in the Purge All Alarms window.

To clear a single alarm that is in a reset condition:

Click **Remove** ✕ in the Alarm Response window. The system logs the alarm (and its responses) and deletes it from the Alarm Monitor.

Note: The Alarm Response window may now be configured to have the Remove function button unavailable unless the alarm is in reset state or has the alarm control Immediate Reset Input set (Alarm form). The configuration is determined by the Enforce UL Specifications parameter in the System Parameters form. The default is No, indicating the Remove function button is always available. When set to Yes, the Remove function button will be grayed out when the alarm is not in the reset condition.

To clear a single alarm that is *not* in a reset condition:

Click **Purge** in the Alarm Response window, if available. The system logs the alarm (and is responses) and deletes it from the Alarm Monitor.

To control Alarm Outputs:

1. From the **Monitor** menu, select **Alarm Monitor**.
2. Select the alarm. The Alarm Response window appears and the instructions for this alarm will be listed. The alarm type is displayed in the title bar of the window.
3. Click **Outputs** on the Alarm Response window toolbar to display the Control Outputs window.

Figure 109. Control Output Groups

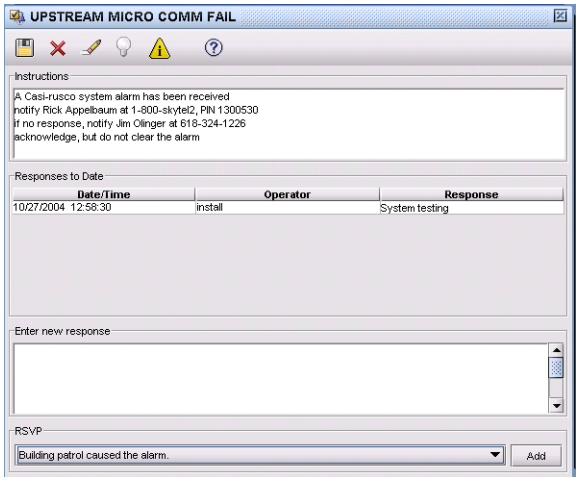
4. Click a radio button to turn the entire output group on or off, and then click **OK**.

Responding to alarms

The system allows the operator to respond to (acknowledge) alarms and to manually reset alarm outputs (if manual reset was selected using the Alarms form).

Open the Alarm Monitor window and select the alarm to display the Alarm Response window. The alarm type is displayed in the title bar of the window. Pre-written alarm responses appear in the Responses list box. When you select a response and clear the alarm, the system will archive the alarm record and the response. The pre-written response saves time. If none of the responses on the selection list are appropriate, the operator can type a unique response.

Figure 110. Alarm Response window



Fields and controls

Table 104. Alarm Response form fields

Field name	Description	
Instructions	Displays alarm instructions, such as who to call or who to dispatch to the area. Messages can be defined in the Alarm Messages form. Up to five messages can be assigned to each alarm in the Alarm form.	
Responses to Date	Displays all the responses to the alarm event up to the current time.	
	Date/Time	The date and time of the response.
	Operator	The operator's user name.
	Response	The response text.
Enter new response	Use to enter a custom text response. Use up to 255 characters.	
RSVP	Click to select from a list of predefined alarm responses. To create a new response based on a predefined alarm response, click Add. The selected response displays in a window where you may edit it and save as a new response.	

Related procedures

To respond to an alarm:

1. Silence the alarm by clicking **Silence** on the Alarm Alert window.

2. Select **Monitor**, and then **Alarm Monitor**.
3. Select the alarm. The Alarm Response window appears.
4. Optional: Click **Outputs**  to toggle associated outputs on or off.
5. Optional: Enter a response--either click the **RSVP** button to select from a list of alarm responses, or type a new response. When you click **Add**, the selected response appears in the Enter New Response box. The maximum length of a response is 255 characters. If the responses selected from the Responses list box exceed this limit, a warning will pop-up indicating this and the response will be truncated down to the maximum length. The response may then be edited in the Enter New Response: box to make the truncated response more presentable.
6. Log the response.
   - To log the response without clearing the alarm, click **OK**. You can continue to select this alarm again to enter new responses. The previous responses appear in the Responses To Date box.
   - To log the response and clear the alarm, click **Remove** on the Alarm Response window. See *Related procedures* on page 266.
7. Optional: Click the close button (X button) to close the window without altering the state of the alarm.

Monitoring badge activity

The Badge Monitor displays the following types of badge activities:

Table 105. Badge activities - Valid

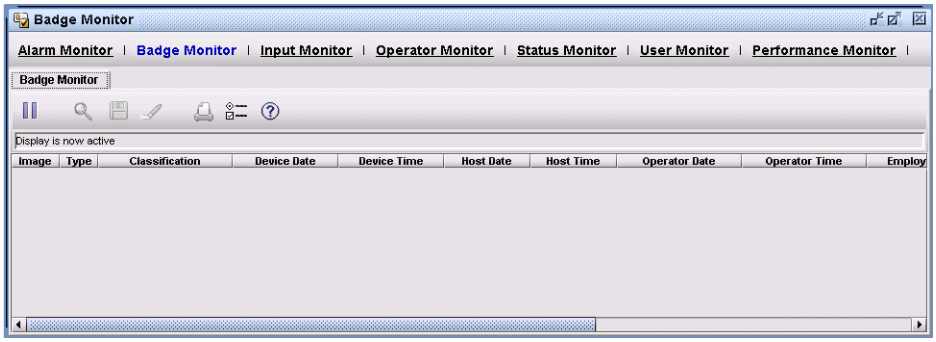
Valid transactions	
APB In	A valid read occurred in an Antipassback In reader.
APB Out	A valid read occurred in an Antipassback Out reader
Degraded Open	A read occurred when an 8RP board was offline from the Micro/4 CPU.
Open	A valid read occurred in a Normal reader or a Keypad reader and the door was opened.
Open Duress	A valid read occurred in a Keypad reader but was followed by a duress code. The door was opened.
Open Shunt	The door was opened as part of an alarm shunting process.
Passive APB In	A badge holder was granted access in two successive APB IN readers.
Passive APB Out	A badge holder was granted access in two successive APB OUT readers.
Swipe And Show	A valid read occurred on a reader configured for Swipe and Show. This will be followed by another valid transaction, indicating how the transaction ended.
T&A In	A valid read occurred in a Time & Attendance In reader.
T&A Out	A valid read occurred in a Time & Attendance Out reader.
Valid Door Locked	In a Double Badge reader, the first badge read was valid but will not open the door until the second is validated.
Valid Floor	A valid floor number was selected with elevator reader/DI/DO configuration.
Valid No Passage	A valid read occurred but the door was not opened.
Valid Toggle	A valid read occurred in a Toggle reader which reversed the current state of the Input Group.
Valid Nested APB	A valid read occurred at a nested APB reader.
Valid Timed Nested APB	A valid read occurred at a timed nested APB reader.
Passive Nested APB	A badgeholder was granted access at a nested APB reader despite a nested APB violation.
Fail Safe	A badgeholder was granted access at a global nested APB reader configured for “Controller Requests from Host” and the micro was offline. Additionally, the offline operation mode was configured for “Fail Safe.”

Table 106. Badge activities - Invalid

Invalid transactions	
Area Offline	The area was selected as offline.
Badge Deleted	A deleted badge was used in a reader.
Badge Expired	An expired badge was used in a reader.
Badge Lost	A lost badge was used at a reader.

Invalid transactions	
Badge Suspended	A suspended badge was used at a reader.
Badge Unknown	An unknown badge was used at a reader.
Invalid APB In	An invalid read occurred in an APB IN reader.
Invalid APB Out	An invalid read occurred in an APB OUT reader.
Invalid Code	The number entered was not a valid code for a Shunt or Keypad reader.
Invalid Floor	An invalid floor number was selected with elevator/DI/DO configuration.
Invalid KR BDG	The badge used at a Keypad reader was not a keypad response badge.
Invalid PIN	The pin entered at the Keypad reader was invalid.
Invalid Shunt	The shunt value was entered at a reader not enabled as a Shunt reader.
Invalid T&A In	An invalid read occurred at a T&A IN reader.
Invalid T&A Out	An invalid read occurred at a T&A OUT reader.
KR INVLD Open DR	A keypad response was given while the door was still open.
KR Not Enabled	A keypad response was given at a reader not enabled as a Keypad reader.
Learn Timeout	A badge was not learned by the micro within the set amount of time of 5 seconds.
No Categ Match	An invalid badge read occurred because the badge holder's categories did not match one of the area's categories.
Not Validated	In a Double-Badge reader, the second badge read was not validated because the first was invalid.
Reader Offline	A read took place in an offline reader.
Usage Exhausted	The badge holder's usage count for limited usage readers has been exhausted.
Double Door Locked	A second valid read occurred before the door was opened for the first valid read.The door then locks.
Invalid Nested APB	An invalid read occurred at a nested APB reader.
Invalid Timed Nested APB	An invalid read occurred at a timed nested APB reader.
Fail Secure	An invalid read occurred at a global nested APB reader configured for "Controller Requests from Host" and the micro was offline. Additionally, the offline operation mode was configured to be "Fail Secure."

Figure 111. Badge Monitor



Fields and controls

Table 107. Badge Monitor fields

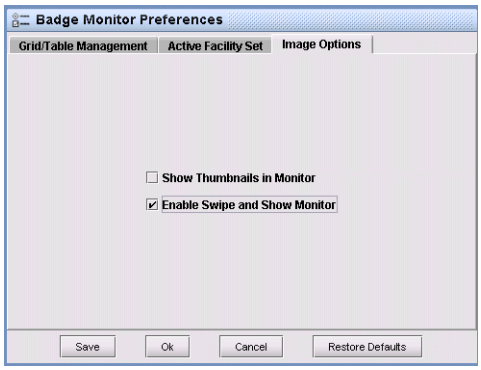
Field name	Description
Image	If Show Thumbnails in Monitor is selected in Preferences, a thumbnail image of the badge holder that generated the transaction displays in this column.
Classification	The type of valid or invalid badge transaction displayed. *Example: Badge Expired*
Type	Displays B to denote badge activity, or T to denote trace activity.
Device Date	The date the badge activity occurred, in the time zone of the device. See *Verifying time zones* on page 168.
Device Time	The time the badge activity occurred, in the time zone of the device. See *Verifying time zones* on page 168.
Host Date	The date the badge activity occurred, in the time zone of the host. See *Verifying time zones* on page 168.
Host Time	The time the badge activity occurred, in the time zone of the host. See *Verifying time zones* on page 168.
Operator Date	The date the badge activity occurred, in the time zone context of the operator. See *Verifying time zones* on page 168.
Operator Time	The time the badge activity occurred, in the time zone context of the operator. See *Verifying time zones* on page 168.
Employee ID	The badge holder's employee number.
Initials	The badge holder's initials.
Last Name	The badge holder's last name.
First Name	The badge holder's first name.
Reader	The description of the reader that read this badge.
Category	The description of the category that resulted in the valid transaction.
Area	The description of the area where the reader is located.
Department	The description of the department that the badge holder belongs to.
BID	The unique identification number associated with this badge.
Facility	The facility of the input as defined in the Facility field of the Badges form.

Monitoring Swipe and Show activity

When properly configured for Swipe and Show, the Activity Monitor displays a photo when a valid badge read is received from a reader. The photo is imported from the photo database. For double badge transactions, the photo is displayed when the first swipe is detected, and the door is allowed to be unlocked when the second swipe is detected.

To enable the Swipe And Show function, the reader must be designated as Authorization Required or Authorization Not Required on the Reader form. Enable Swipe And Show Monitor must be selected on the Image Options tab of the Badge Monitor Preferences window. This option is available only when the Image package is installed in the system.

Figure 112. Swipe and Show Monitor



If Authorization Required is active, a dialog allows the operator to unlock the door or advises the operator why the door cannot be unlocked. If the door is allowed to be unlocked, the dialog includes an OK button and a Cancel button. The OK button unlocks the door and dismisses the dialog. The Cancel button dismisses the dialog, but does not unlock the door. If the door is not allowed to be unlocked, the dialog only shows a Close button, which dismisses the dialog.

If the operator clicks the OK button to unlock the door, the door strike output command event is recorded in operator history. Any invalid transaction denies the operator the option of unlocking the door.

The monitor is frozen while the photo is being displayed to allow the operator to read the text description of the transaction. The text description includes the name of the badge holder and the name of the reader where the transaction originated. If a photo cannot be displayed, a dialog advises the operator of the reason. This dialog includes a Close button to dismiss the dialog and free the Activity Monitor.

Save, Search, and Print affect the contents of the window, but not the photo. New clears the monitor window, but does not dismiss the photo. Freeze freezes the monitor, but will not free the monitor while it is frozen by a photo. The monitor returns to normal when the operator dismisses the photo by clicking the Close box.

If Authorization Not Required is active, the photo will appear and the door will automatically unlock if this was a valid badge read.

Related procedures

To view badge activity:

1. From the **Monitor** menu, select **Badge Monitor**.
2. To view badge activity make sure that routing for each of the badge transaction types, as listed on page 271, is routed to the Badge Monitor.
3. If you want to create a report of this information, click **Save** to save the report as a `.txt` file.

To view swipe and show activity:

To enable Swipe and Show, the reader must be designated as Authorization Required or Authorization Not Required on the Reader form.

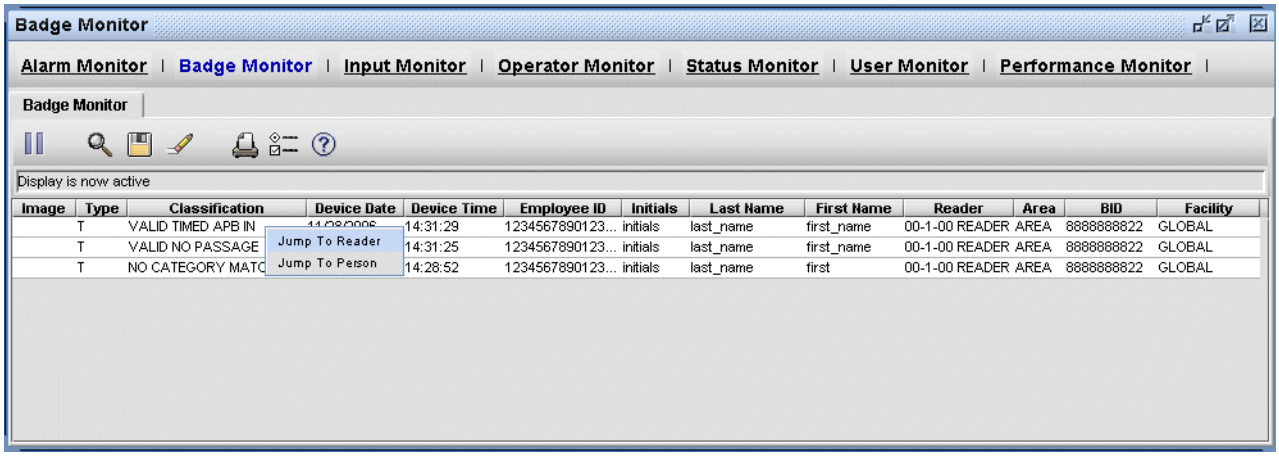
1. Select **Monitors**, and then **Badge Monitor**.
2. From the toolbar, click **Preferences** , to display the Badge Monitor Preferences window.
3. Click the **Image Options** tab.

4. Select **Enable Swipe and Show Monitor** and click **Ok**.

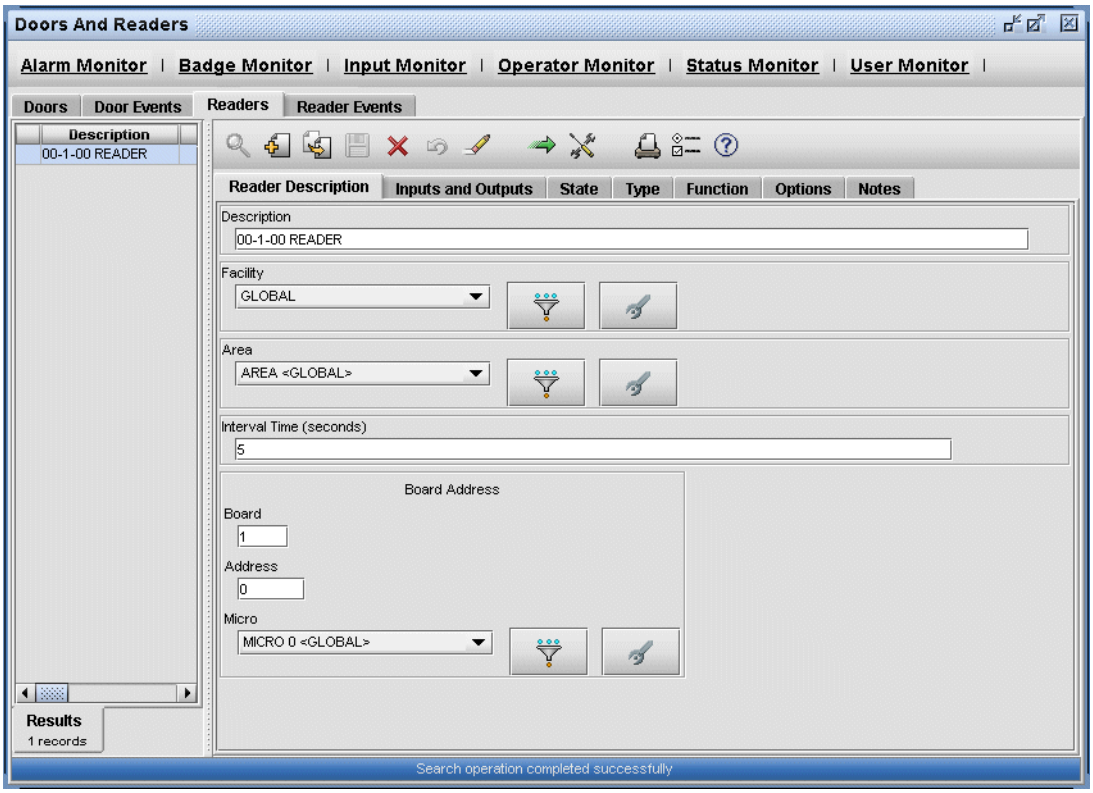
To jump to a record from the Badge Monitor:

Note: If an operator does not have permission to view the associated record, the option is dimmed.

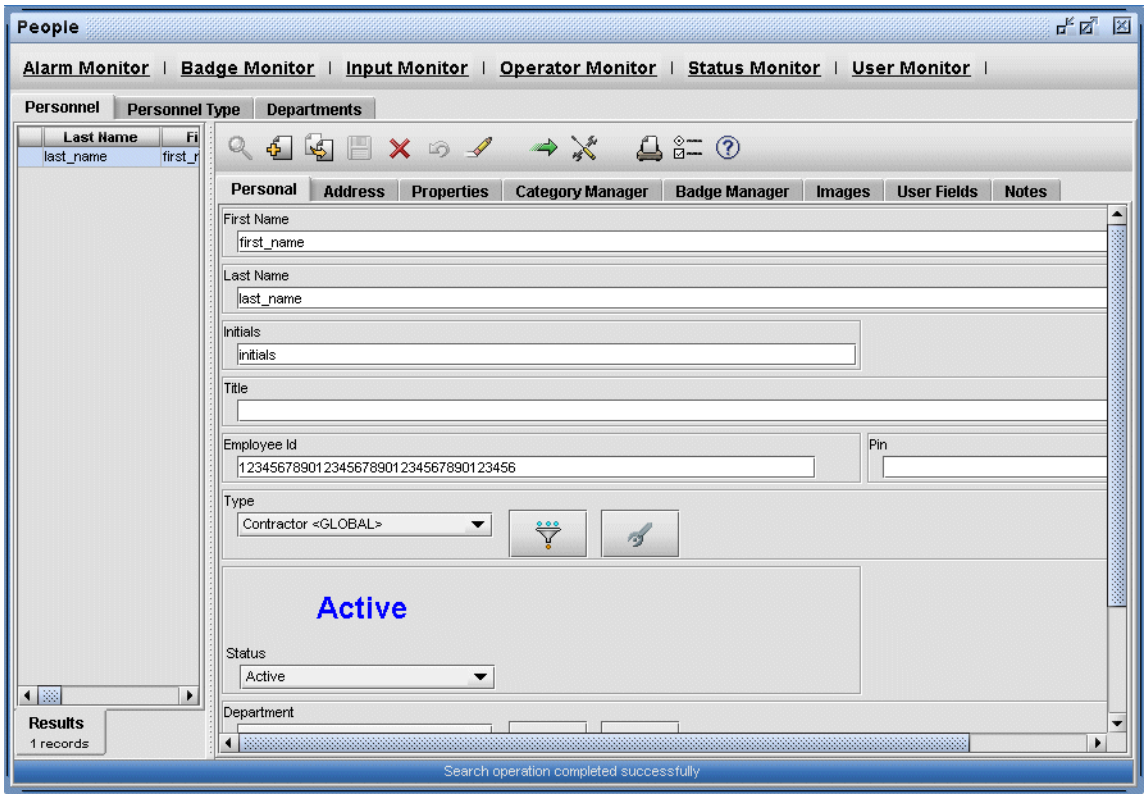
1. From the **Monitor** menu, select **Badge Monitor**.
2. Right-click an entry to display the following menu.



3. If you select **Jump to Reader**, the record for the reader where the badge activity occurred displays, such as the following:



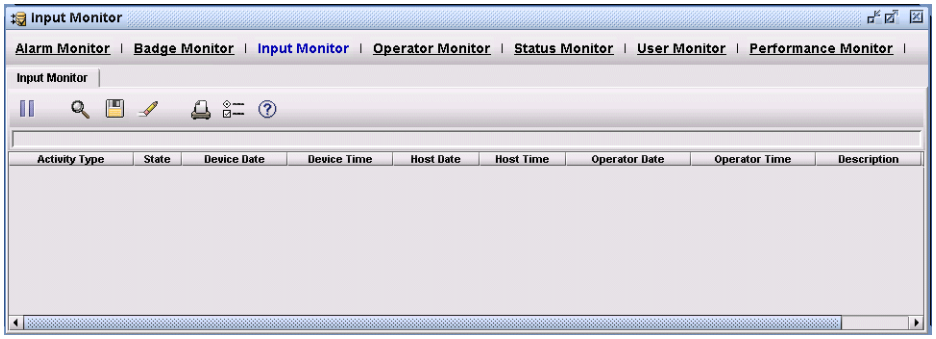
If you select **Jump to Person**, the person record of the badgeholder displays, such as the following, or in the case of an Unknown Badge, a blank person record displays:



Monitoring input activity

The Input Monitor displays input activity transactions.

Figure 113. Input Monitor



Fields and controls

Table 108. Input Monitor fields

Field name	Description
Activity Type	The type of input transaction displayed: INPUT
State	The actual state of the input, either open, closed, short, ground, or error.
Device Date	The date the activity occurred, in the time zone of the device. See *Verifying time zones* on page 168.
Device Time	The time the activity occurred, in the time zone of the device. See *Verifying time zones* on page 168.
Host Date	The date the activity occurred, in the time zone of the host. See *Verifying time zones* on page 168.
Host Time	The time the activity occurred, in the time zone of the host. See *Verifying time zones* on page 168.
Operator Date	The date the activity occurred, in the time zone of the operator. See *Verifying time zones* on page 168.
Operator Time	The time the activity occurred, in the time zone of the operator. See *Verifying time zones* on page 168.
Description	A description of the input, usually including a wiring address and a written description.
Facility	The facility of the input as defined in the Facility field of the Input form.

Related procedures

To view input activity:

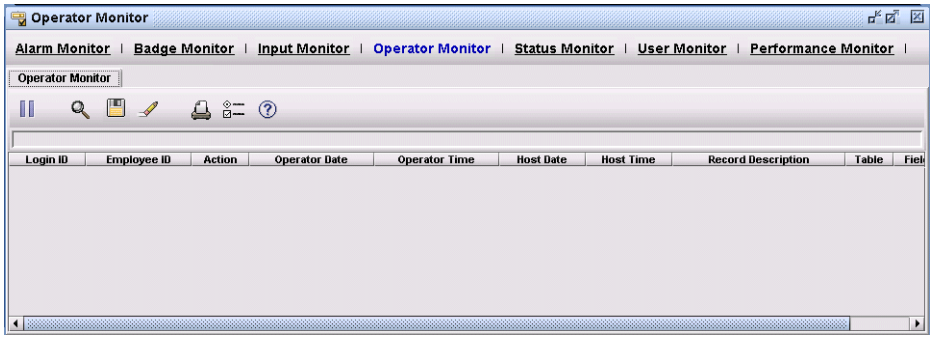
1. From the **Monitor** menu, select **Input Monitor**.
2. To view input activity make sure that routing for each of the input transaction types, as listed on page 278, is routed to the Input Activity Monitor.
3. If you want to create a report of this information, click **Save** to save the report as a `.txt` file.

Monitoring operator activity

Select Operator Monitor to view the incoming operator activity transactions. Operator transactions include Inserts, Updates, and Deletes to records in the database tables. The system can log this activity and the operator's ID.

Make sure that an operator routing is defined on the System Parameters form. Make sure that Global facility is chosen as part of the active facility set.

Figure 114. Operator Monitor



Fields and controls

Table 109. Operator Monitor fields

Field name	Description
Login ID	The Login name the operator types to gain access to Picture Perfect, as defined in the Login ID field of the Operator form.
Employee ID	The company identification number assigned to the operator using the system, as defined in the Employee Id field on the Operator form.
Action	One of the following types of activity performed by the operator: Log on, Log off, Update, Delete, Query, Command Event, Status request, Shutdown request, or Insert.
Operator Date	The date the activity occurred, in the time zone of the operator.See *Verifying time zones* on page 168.
Operator Time	The time the activity occurred, in the time zone of the operator. See *Verifying time zones* on page 168.
Device Date	The date the activity occurred, in the time zone of the device. See *Verifying time zones* on page 168.
Device Time	The time the activity occurred, in the time zone of the device. See *Verifying time zones* on page 168.
Host Date	The date the activity occurred, in the time zone of the host. See *Verifying time zones* on page 168.
Host Time	The time the activity occurred, in the time zone of the host. See *Verifying time zones* on page 168.
Record Description	The description of the record viewed, updated, or deleted. *Example: Smith, David*
Table	The Picture Perfect table to which the record that was changed belongs. *Example: person*
Field	The field name of the record that was changed on the form. *Example: Address 5*
Value	The change that was made in the field. *Example: FL*

Related procedures

To view operator activity:

1. From the **Monitor** menu, select **Operator Monitor**.
2. Operator transactions include Inserts, Updates, and Deletes to records in the database tables. Make sure that routing on the System Parameters screen is set up to the Operator Monitor. If you want to create a report of this information, click **Save** to save the report as a `.txt` file.

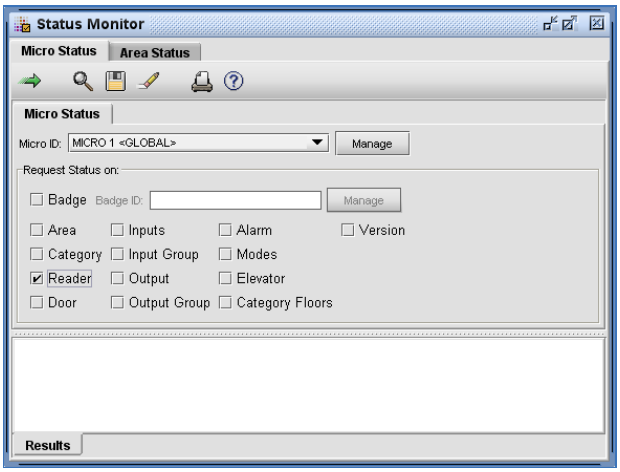
Monitoring status

The Status Monitor lets you see a micro's current operating characteristics (status) for its areas, categories, readers, doors, inputs, input groups, outputs, output groups, alarms, modes, elevators, category floors, and/or version. You can also view the status of an area's readers and/or doors.

Scheduled events change the micro database and can also be used to update the host database. The Status Monitor allows the operator to view the micro database in real time to see any changes the scheduler has made.

You must first select to view by micro or by area.

Figure 115. Status Monitor



Fields and controls

Table 110. Status Monitor fields

Field name	Description
Micro/Area ID	Click to display a drop-down list from which you can select the micro or area whose status you want to view.
Request status on:	Enable the check boxes of the characteristics that you want to include in the status report.

Related procedures

To view status by micro:

1. From the **Monitor** menu, select **Status**, and then click the **Micro** tab.
2. From the **Micro ID** drop-down list, select a micro.
3. From the **Request status on**: selections, check the characteristics that you want to view.
4. Click **Execute** .
5. A report displays in the Results window at the bottom of your screen. Use the scroll bar to view the entire contents of the report.
6. Click **Save** to save the report as a `.txt` file.

To view status by area:

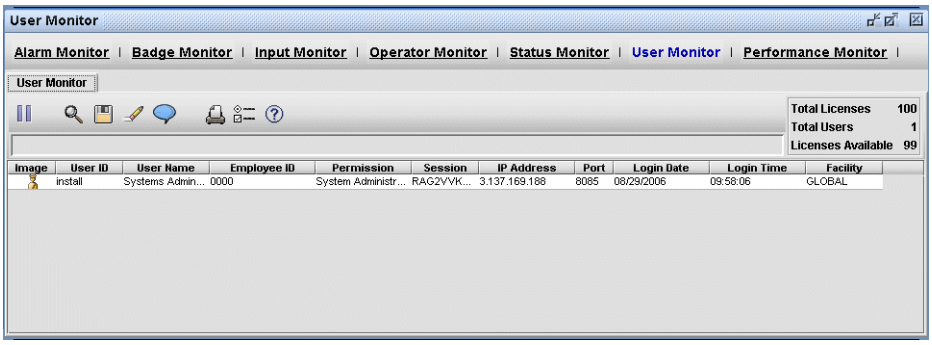
1. From the **Monitor** menu, select **Status**, and then click the **Area** tab.
2. From the **Area ID** drop-down list, select an area.
3. From the **Request status on**: selections, check the characteristics that you want to view.
4. Click **Execute** .
5. A report displays in the Results window at the bottom of your screen. Use the scroll bar to view the entire contents of the report.
6. Click **Save** to save the report as a `.txt` file.

Note: You can also receive status information from the command line by typing statuscmd. The command statuscmd is the only option where badge status information can be viewed.

Monitoring users

The system records the operators that are logged on to the system and displays other details about the session and the operator.

Figure 116. User Monitor



Fields and controls

Table 111. User Monitor fields

Field name	Description
User ID	The Login name the operator types to gain access to Picture Perfect, as defined in the Login ID field of the Operator form.
User Name	The description of the operator using the Login ID, as defined in the User Name field on the Operator form.
Employee ID	The company identification number assigned to the operator using the system, as defined in the Employee Id field on the Operator form.
Permission	The operator's database access control, as defined in the Permission field of the Operator form.
Session	A system generated unique number identifying the session to which the operator is logged on.
IP Address	A multi-digit number (such as 10.41.200.57) that identifies a unique location within a network of the computer to which the operator is logged on.
Port	This is a number that identifies the port through which the host and the client communicate when transmitting real-time events.
Login Date	The date the operator logged on to the session.
Login Time	The time the operator logged on to the session.
Facility	The facility of the operator as defined in the Facility field of the Operator form.

Related procedures

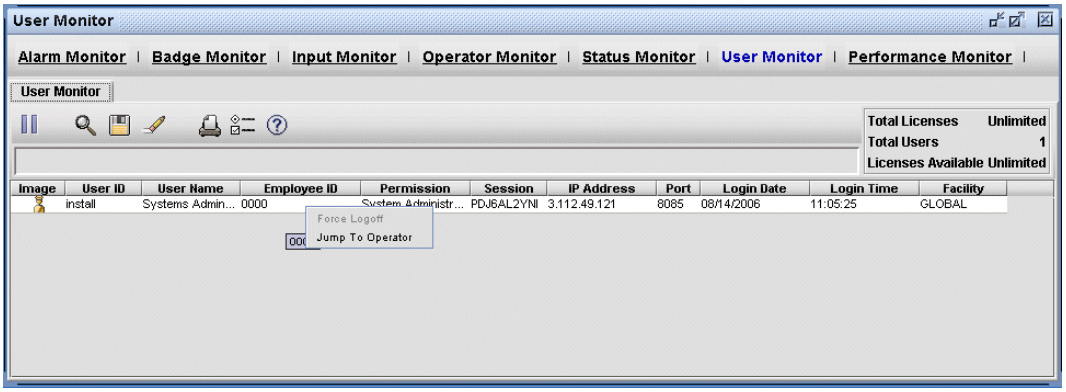
To view user activity:

1. From the **Monitor** menu, select **User Monitor**.
2. If you want to create a report of this information, click **Save** to save the report as a `.txt` file.

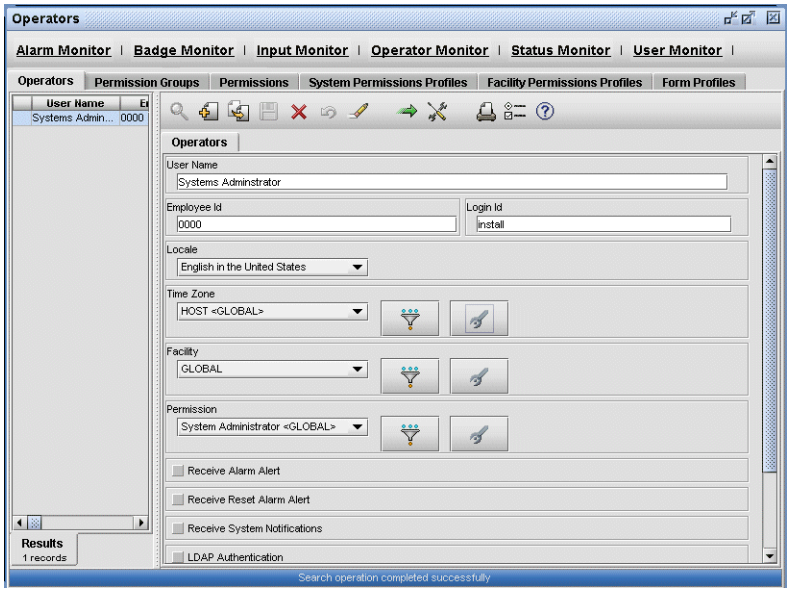
To jump to an operator record from the User Monitor:

Note: If an operator does not have permission to view the associated record, the option is dimmed.

1. From the **Monitor** menu, select **User Monitor**.
2. Right-click an entry to display the following menu.



3. Select **Jump to Operator**. The operator record associated with that user displays, such as the following:

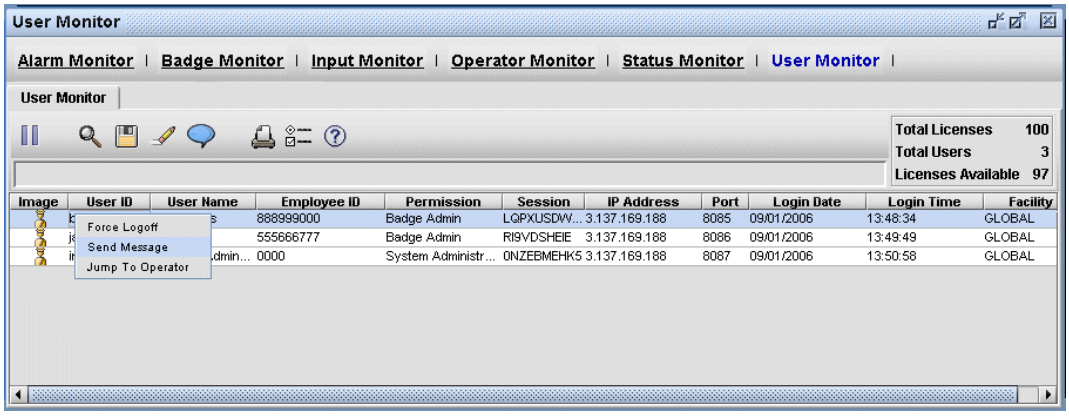


To force a selected user to log off the system:

Note: In order to perform this action, you must have Force Logoff permission. From the Main menu select Control, Operators, System Permissions Profile. Make sure the Force Logoff action is selected on your System Permission profile.

Note: You can not force the user that you are logged in as to log off. The option will appear dimmed.

1. From the **Monitor** menu, select **User Monitor**.
2. Right-click the user entry to display the following menu.



3. Select **Force Logoff**. The user is immediately logged off of the system.

   Note: You can also force logoff from the command prompt. Type: pplogoff <userid>

To force all users to log off the system:

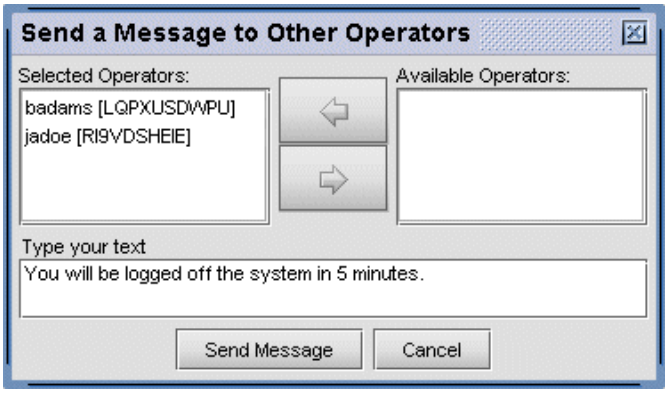
1. Make sure you are logged on to the operating system. Open a terminal window.
2. At the command prompt, type: `pplogoff all`

To broadcast a message to all users that are logged into the system:

Note: In order to perform this action, you must have Send Message permission. From the Main menu select Control, Operators, System Permissions Profile. Make sure the Send Message action is selected on your System Permission profile.

1. From the **Monitor** menu, select **User Monitor**.
2. From the toolbar, click the **Send Message** icon.

Figure 117. Send Message: All Operators



3. All operators that are currently logged in display under **Selected Operators**. If you do not want one or more operators to receive the message, highlight the login IDs and click the right arrow to move the selections to the **Available Operators** column.

Note: You can not send a message to the user that you are logged in as. Your user ID will not display in the list.

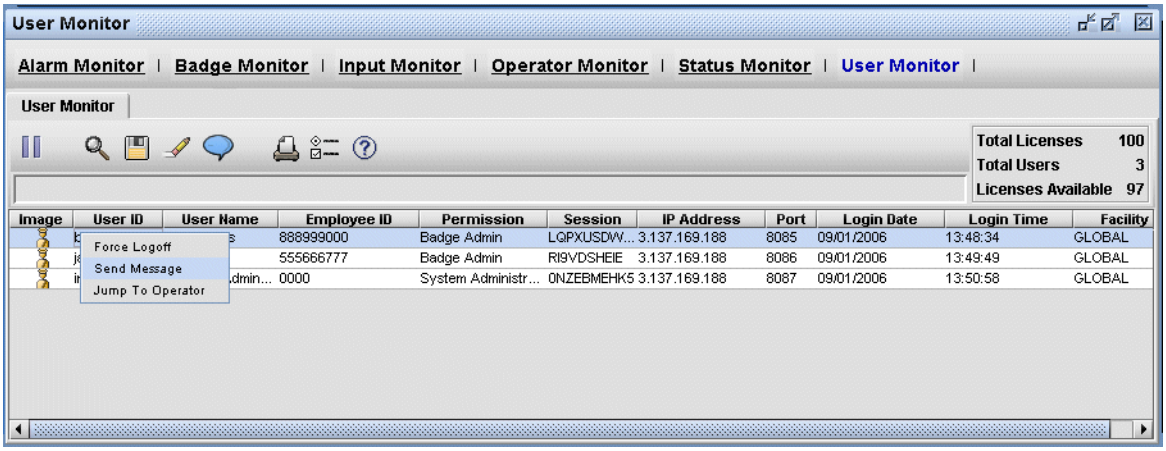
4. Type the message in the **Type your text** area.
5. Click **Send Message** to send or **Cancel** to quit.

To broadcast a message to a selected user that is logged into the system:

Note: In order to perform this action, you must have Send Message permission. From the Main menu select Control, Operators, System Permissions Profile. Make sure the Send Message action is selected on your System Permission profile.

1. From the **Monitor** menu, select **User Monitor**.

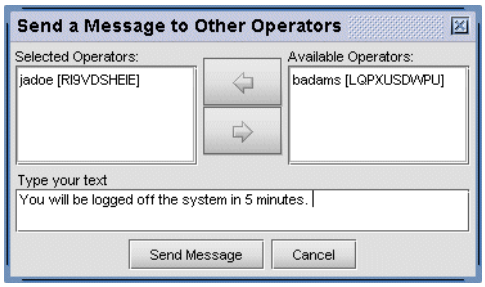
Figure 118. User Monitor: Send Message



2. Select the User ID of the operator to whom you want to send a message and right-click to display a context menu.
3. Select **Send Message**. Under **Selected Operators**, only the UserID of the operator you selected displays.

Note: You can not send a message to the user that you are logged in as. The Send Message option will appear dimmed.

Figure 119. Send Message: Selected Operator



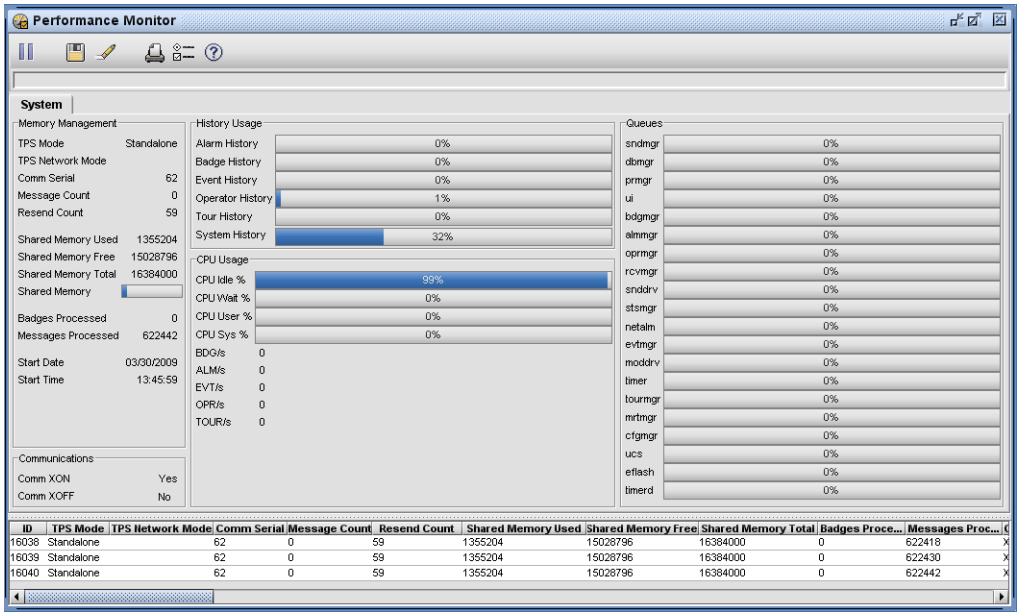
4. Type the message in the **Type your text** area.
5. Click **Send Message** to send or **Cancel** to quit.

Monitoring system performance

The Performance monitor allows an operator to view the overall performance characteristics of the Picture Perfect host. Vital statistics such as memory usage, history usage, CPU usage, and queue sizes are refreshed periodically and are logged temporarily on Picture Perfect's system history table.

This data can be useful when optimizing the system or when diagnosing host-related performance issues.

Figure 120. Performance Monitor



Fields and controls

Table 112. Performance Monitor fields

Field name	Description	
Memory Management	TPS Mode	Standalone, Primary, or Backup Displays the current TPS mode when using a standalone or redundant system.
	TPS Network Mode	Network Host or Subhost Shows the type of host in an Enterprise system.
	Comm Serial	Serial number for I/O messages.
	Message Count	Total number of messages on all queues.
	Shared Memory Used	The size (Bytes) of shared memory currently in use.
	Shared Memory Free	The amount (Bytes) of shared memory currently available.
	Shared Memory Total	The total amount (Bytes) of shared memory (used + free) on the system.
	Shared Memory	Graphical display of used shared memory capacity.
	Badges Processed	The number of badge transactions processed since the time shown in Start Date/ Start Time.
	Messages Processed	The number of messages processed since the time shown in Start Date/Start Time.
	Start Date	The date the system was last started.
	Start Time	The time the system was last started.
Communications	Comm XON	Yes: Communicating with devices No: Not communicating with devices (buffer too full)
	Comm XOFF	Yes: Not communicating with devices (buffer too full) No: Communicating with devices
History Usage	Alarm History	Alarm History capacity used The number of alarm transactions in the history table.
	Badge History	Badge History capacity used The number of badge transactions in the history table.
	Event History	Event History capacity used The number of event transactions in the history table.
	Operator History	Operator History capacity used The number of operator transactions in the history table.
	Tour History	Tour History capacity used The number of tour transactions in the history table.
	System History	System History capacity used The number of system transactions in the history table.

Table 112. Performance Monitor fields (continued)

Field name	Description	
CPU Usage	CPU Idle %	The percent of Server CPU clock cycles unused.
	CPU Wait %	The percent of server CPU clock cycles waiting on resources.
	CPU User %	The percent of server CPU clock cycles used by user processes.
	CPU Sys %	The percent of server CPU clock cycles used by system processes.
	BDG/s	The number of badge transactions currently being processed per second.
	ALM/s	The number of alarm transactions currently being processed per second.
	EVT/s	The number of event transactions currently being processed per second.
	OPR/s	The number of operator transactions currently being processed per second.
	TOUR/s	The number of tour transactions currently being processed per second.
Queues	sndmgr	Send Manager queue size.
	dbmgr	Database Manager queue size.
	prmgr	Print Manager queue size.
	ui	UI Manager queue size.
	bdgmgr	Badge Manager queue size.
	almmgr	Alarm Manager queue size.
	oprmgr	Operator Manager queue size.
	rcvmgr	Receive Manager queue size.
	snddrv	Send Driver queue size.
	stsmgr	Status Manager queue size.
	netalm	Network Alarm Manager queue size.
	evtmgr	Event Manager queue size.
	moddrv	Modem Driver queue size.
	timer	Timer Manager queue size.
	tourmgr	Tour Manager queue size.
	mrtmgr	Routing Manager queue size.
	cfgmgr	Configuration Manager queue size.
	ucs	UCS Manager queue size.
	eflash	eFlash Manager queue size.
	timerd	Timer Daemon queue size.

Related procedures

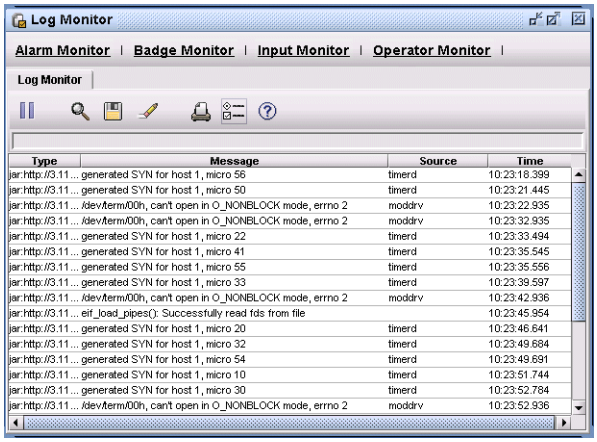
To view performance:

1. From the **Monitor** menu, select **Performance Monitor**.
2. If you want to create a report of this information, click Save to save the report as a `.txt` file.

Monitoring log file messages

The Log monitor allows an operator to view, in real time, the contents of the Picture Perfect log file: `/cas/log/log.xxxx`
where `xxxx` is the current month and day. For example: `/cas/log/log.1105` is the log file for November 5th.

Figure 121. Log Monitor



Fields and controls

Table 113. Log Monitor fields

Field name	Description
Type	The type of message sent to the log file, such as information, warning, or error.
Time	The time the messages was generated.
Source	The sub-system that generated the message.
Message	The text of the message sent to the log file.

Related procedures

To view the log monitor:

1. From the **Monitor** menu, select **Log Monitor**.
2. If you want to create a report of this information, click Save to save the report as a `.txt` file.

Chapter 14 Reports

This chapter shows you how to create and schedule SQL and History reports.

In this chapter:

Overview

The Reports form provides an interface to the online Picture Perfect database, so you can use ANSI standard SQL select statements to query the database and generate reports. The SQL query function allows unlimited selection criteria and up to eight sort criteria. The relational database allows a query to join separate database tables into one report.

To optimize complex queries used for reporting and decision making, Picture Perfect uses Informix-OnLine, a Relational Database Management System (RDBMS) designed to run on a wide range of UNIX-like operating systems in standalone or networked environments. Informix optimizes the processing of large databases that are shared by many concurrent users. Some advantages of Informix file management are:

- The operating system does not limit the number of tables used at one time. For example, the SQL form lets you select data from all Picture Perfect database tables for a single report.
- The size of a database table is not limited, except by disk size.

The Picture Perfect system captures history information for alarms, badges, and operator activity. This information can then be manipulated into various reports that can be viewed on screen or sent to a printer. Alarm history includes acknowledged alarms. Badge history includes access attempts by valid, invalid, lost, and suspended badges, plus Swipe and Show transactions on readers. Operator history includes database changes, login transactions, control outputs, alarm graphics, and Swipe-and-Show record changes to output state.

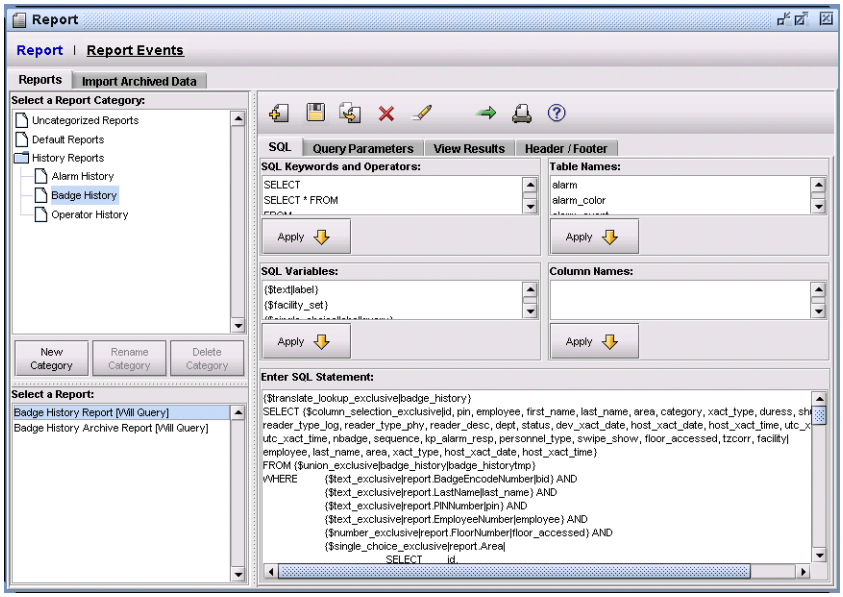
You can control which activities go to history. The History log is online history, and is one of the destinations specified by routing instructions used throughout the system. You can set up routing-control information to direct selected operator activity and badge activity to selected destinations: Printer, Monitor, or History. The routings that you define on the Routings form appear in the Routings list box on the Areas, Inputs, and Alarms forms. If the current routing on a form includes History, the activities defined on that form are captured in history. If there is no current routing assigned, the activity routes to the default routing as defined on the System Parameters form. If the default routing does not include History in its setting, the activity will not be captured in history.

Creating and viewing reports

Example

The following example is a Badge History report.

Figure 122.Reports Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 114. Reports form fields

Field name	Description
Select a Report Category	When you select a category, the existing reports in that category display in the Select a Report list pane. You can create a new category by clicking *New Category*, rename an existing category by clicking *Rename Category*, or delete a category by clicking *Delete Category*.
Select a Report	A list box from which you can open a predefined report. Select the desired report. **Note:** If report permissions are enabled, only the reports that the operator has access to will be displayed
SQL Keywords and Operators	This list box displays SQL reserve words, relational operators, and logical operators which you select and apply to an SQL statement. When you select a name and click Apply, the name appears wherever your cursor is located in the Enter SQL Statement window. See *Working with SQL* on page 300 for more information.
SQL Variables	This list box displays pre-defined variables. See *SQL variables* on page 300 for a description of the syntax of these variables.

Table 114. Reports form fields (continued)

Field name	Description	
Table Names	Select and apply table names to SQL statements after FROM. This list box includes all the table names in the Picture Perfect database, and each contains different types of data that you may want to include in your report. When you select a table name and click Apply, the name appears wherever your cursor is located in the Enter SQL Statement window.	
Column Names	Select and apply column names from the Column Names list box which includes all the column names in the selected database table. When you select a column name and click Apply, the name appears wherever your cursor is located in the SQL window.	
Enter SQL Statement	Enter the following SQL reserved words in the SQL window to form the beginning of each SQL clause. Use all caps to differentiate the reserved words from the rest of the clause. Only the SELECT clause and the FROM clause are required. WHERE and ORDER BY are optional. SELECT FROM WHERE ORDER BY Instead of typing these names, you can select and apply words from the SQL Keywords and Operators list box.	
Query Parameters	The Query window allows you to specify search criteria for your report. If you do not specify any criteria, the report will contain all information from the selected database table. If you have a large database table, the report may run out of space requiring you to limit your query by specifying search criteria.	
	Text fields	You can insert or edit text in these fields by selecting the field and typing the desired text. Text can contain wild card characters. The asterisk (*) is a wild card indicating 0 or more characters. The question mark (?) is a wild card indicating a single character. *Example: You could query alarm history for all records with associated badge encode numbers starting with 123 by typing 123* in the Badge Encode Number field.*
	Combo Boxes	Clicking one of these buttons causes a list box to appear. From this list you can choose an item or you can enter your own text by editing the text field at the bottom of the window. *Example: If you want to query the history database by micro, click the Micro button and the list box will list all defined micros for the system. You can select one of these micros from the items list. Click Ok in the list box to specify which micro the report will cover.*

Table 114. Reports form fields (continued)

Field name	Description	
	Date Time Ranges	History contains a date and time stamp of when the transaction occurred. Use the date and time range boxes to specify date and/or time ranges for the report. You can specify either a Daily or Continuous date/time query. Daily refers to what happened between a start and end time each day from start to end date. Continuous refers to what happened from start date at start time through end date at end time. *Example: Suppose you want to know what happened between 8AM and 5PM during the month of December 2003. Enter 12/1/03 as the start date, 12/31/03 as the end date, 8:00 as the start time and 17:00 as the end time and click Daily. In contrast, leave the dates and times as specified for the Daily example, but click Continuous. Now you would get all information on what happened starting at 8AM on the 1st of December through 5PM on the 31st.*
	List Boxes	Some query windows contain list boxes that allow multiple selections for valid and invalid transactions. By selecting any of the items in the list, you will be querying for only those records that satisfy that condition.
	Toggle Buttons	Toggle buttons allow you to specify values for various conditions. By clicking any of these buttons, you will be querying only those records that satisfy that condition.
	Submit	Accepts your changes and runs the report.
View Results	Click to view a list of the data records included in the report.	
Header	Specify text to be used as a header to be printed at the top right of every page.	
Footer	Specify text to be used as a footer to be printed to the left of the page number at the bottom of every page.	
New	Click to create a new report.	
Save	Saves the current report with the existing title and current changes. Use the Save As command to assign a new title to a new report.	
Save As	Allows you to save the current report under a different name, with the original report still existing under the previous name. The Save As window will appear. Type a new name for the current report, and then click Save As to save it and exit the window.	
Delete	Select the desired report, and then click Delete. Click OK to exit the window. This option appears only if you have operator permission to delete. **Note:** If report permissions are enabled, only the reports that the operator has access to will be displayed.	
Clear	Clears the form so you can create a new report.	
Run	Click this button to generate the report, which will then appear in the View Results tab. There is no limit on the amount of data returned by the select statement, and the View Results window shows how many data records are in the report. When there are more than 1000 rows, it also shows you the current page and the total number of pages. If there are more than 1000 rows found, the first 1000 can be viewed using the scroll bars; click Next Page to see more. To view the previous 1000 rows, click Prev Page. Click Go to Page to access a particular page.	
Print	Displays the Print Preview window. You can adjust the paper size, format the way the map will appear on the page, select the number of copies, and preview the page before printing. The Print Report window allows you to Print to pdf, if you want to create an electronic copy, or to Print to your local printer. There are also several formats to which you can export, such as Excel, HTML, or CSV. **Note:** The Save as text file option does not function with Picture Perfect.	

Table 114. Reports form fields (continued)

Field name	Description
Import Archived Data	Click the Import Archived Data tab to display the Restore form where you can restore an archived database to use for reporting purposes.

Related procedures

To create a new report:

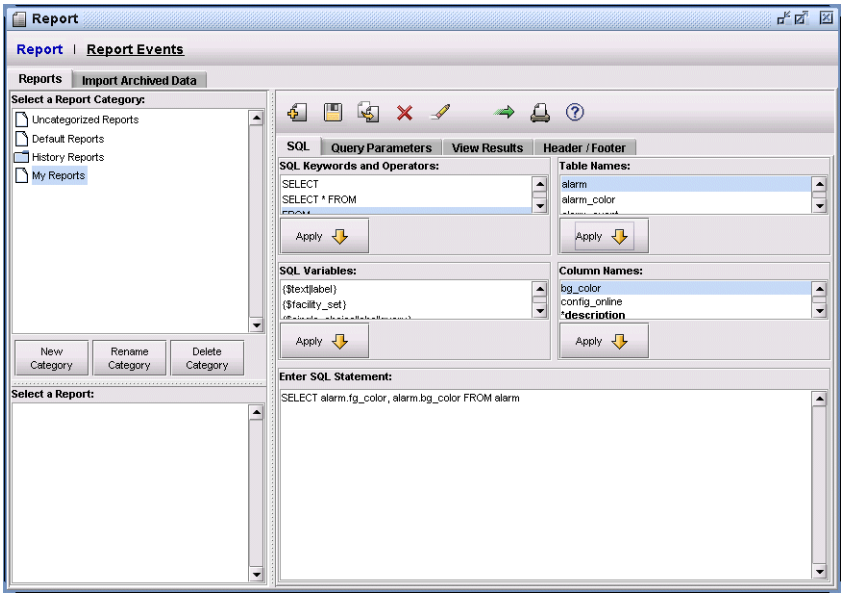
1. From the **Reports** menu, select the **Report** menu item, and then click the **Report** tab.
2. Click **New** . A Modified Report dialog box displays. Click **Yes** to continue.
3. From the **Select a Report Category** list pane, select a category for this report, such as *My Reports*. When you select a category, the existing reports in that category display in the Select a Report list pane. You can create a new category by clicking New Category or rename an existing category by clicking Rename Category.
4. From the **Table Names** list pane, select the database table from which the data should be extracted, such as *alarm_color*. Once you have selected the table, the Column Names list pane displays the columns in the database.
5. Enter your SQL statement. Refer to the topic SQL Syntax for more information on how to write an SQL statement. The only required elements include the type of data to include (SELECT) and what database table the data is to be extracted from (FROM) in the format:

   SELECT <Column Name>, <Column Name> FROM <Table Name>

   For example:

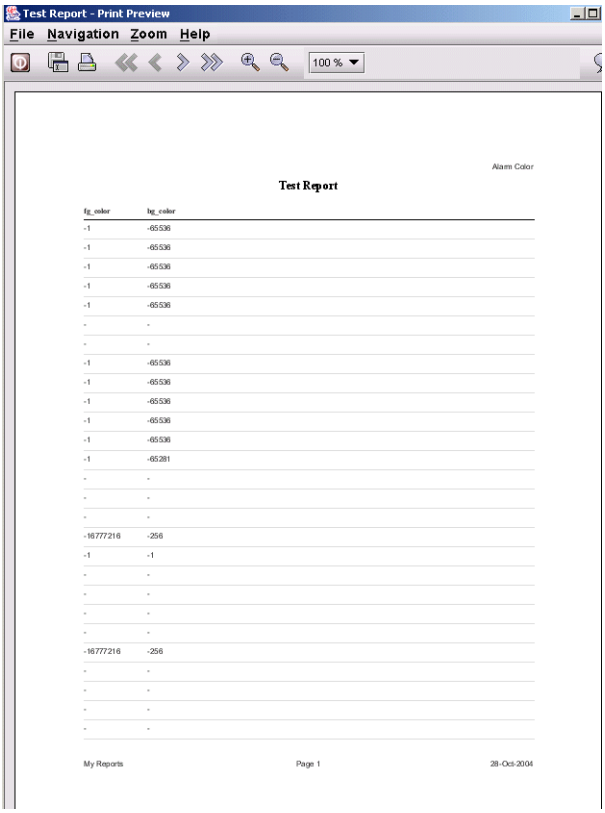
   - From the **Table Names** list pane, select **alarm**.
   - From the **SQL Keywords and Operators** list pane, select **SELECT** and click **Apply**.
   - From the **Column Names** list pane, select the columns that you want to include in the report, such as Foreground Color (**fg_color**) and Background Color (**bg_color**). Separate the columns to be included with commas. Click **Apply**.
   - From the **SQL Keywords and Operators** list pane, select **FROM** and click **Apply**.
   - From the **Table Names** list pane, select **alarm**. Click **Apply**.

Figure 123.Example Report form



- If desired, click the **Header/Footer** tab and enter text that you want to appear at the top and bottom of each page of the report.
- From the toolbar, click **Run** .
- From the toolbar, click **Save As** . Select the report category and enter a Title for the report.
- Click **Print** to display the Print Preview page. From this window you may Save to pdf or Print to your local printer.

Figure 124.Print Preview: Test Report



- Click **Save** . This icon will not be available if all required information is not entered or if you do not have the required permissions for the form.

To view an existing report:

1. From the **Reports** menu, select the **Report** menu item, and then click the **Report** tab.
2. From the **Select a Report Category** list pane, select the category for this report, such as *My Reports*. When you select a category, the existing reports in that category display in the **Select a Report** list pane.
3. To open an existing report, select it from the **Select a Report** list pane. Then, from the toolbar, click **Run** .
4. Click **Print** to display the Print Preview page. From this window you may Save to pdf or Print to your local printer.
5. Click **Save** . This icon will not be available if all required information is not entered or if you do not have the required permissions for the form.

Note:

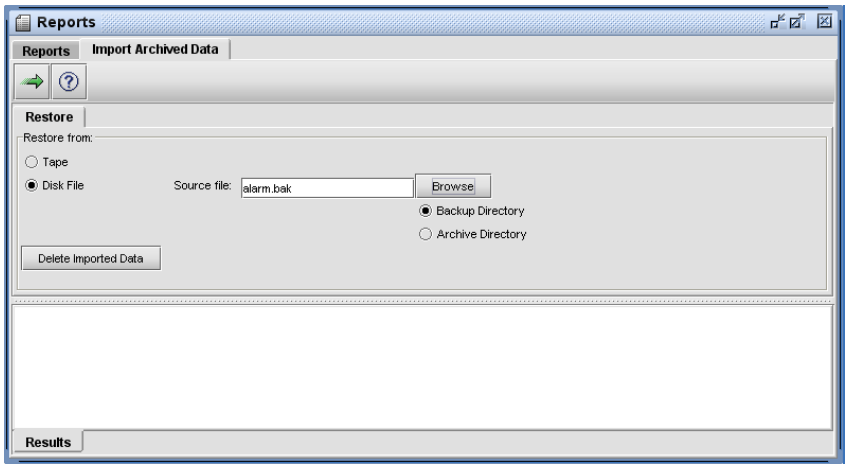
Importing archived data

You can restore archived data from backup tapes. This data can then be used to run archived data reports for Badge, Operator, and Alarm, history.

Example

The following example is a restore of the Badge history archive.

Figure 125.Import Archived Data form



Fields and controls

The following is a list of fields that may require additional information for you to complete. The list is in the order that the fields appear on the form. There is no required sequence to follow.

Table 115. Archive form fields

Field name	Description
Restore from: Tape, Disk File	Select the media that contains the data to be restored.
Source file:	If you chose to restore from a Disk File, enter the name of the filesystem where the data is stored. Click Browse to select from a list.
Delete Imported Data	This button will remove system generated tables containing the restored data.

Related procedures

To perform a restore:

1. From the **Reports** menu, select the **Report** menu item, and then click the **Import Archived Data** tab.

2. Use the appropriate radio button to specify whether you are restoring from **Tape** or **Disk File**.

   Note: When Disk File is selected, clicking Browse displays a list from which you can select the file from which the data will be restored.

3. Click **Execute** to start the restore. When the Media pop-up window appears, insert the tape.
4. Click **OK** to start the restore.

Note: Importing an archive can consume a large amount of available database space. It is recommended that you delete imported data when execution of Archive Reports is completed. This will free up the database space.

Note: Archive data must be imported prior to running an Archive History report.

Working with SQL

SQL variables

Picture Perfect 4.5 supports an expanded version of SQL variable syntax. The SQL Variables list box contains a list of pre-defined "template" versions of the four types of variables as described below.

User defined variables may be embedded directly into the SQL syntax by enclosing the variable inside brackets {}. It is up to the operator to put double quotes outside the variable as needed for character fields. The variable will be detected when the operator clicks Run, and the Variable window displays. When the operator fills in the desired value and clicks OK, the report is executed. The value is then substituted in place of the variable. SQL supports a maximum of ten variables in the SQL select statement. If there are no variables detected, the Report Variables window will not display.

Notes:

- Multiple words with spaces for substitution variables cannot be supported for column descriptions. SQL leaves it up to the operator to make the decision regarding the choice of variables and their textual descriptions.
- The Report Events feature does not support variables. An audit routine that detects variables in the Report Events form prevents reports from being scheduled if they contain variables.
- If you use informix "today" function, time comparisons with Picture Perfect date format must be done using "to_date"function.

  For example: TODAY - TO_DATE (person.access_date::VARCHAR(8), '%Y%m%d')

{$text|label}

UI Control:
Text field with a label

Output:
Replaces tag with user-supplied text.

Example Query:
*SELECT * FROM badge_history WHERE last_name="{$text|Last Name:}"*

{$facility_set}

UI Control:
None

Output:
Replaces tag with comma-delimited list of active facility ids for the current operator.

Example Query:
*SELECT * FROM badge_history WHERE facility IN ({$facility_set})*

{$single_choice|label|query}

UI Control:
Drop-down list with the given label, and entries generated by the given query. The query should select only two columns: the first one is the value for the option, the second is the label for the option to be displayed in the dropdown.

Output:
Replaces tag with value (not label) of choice selected by operator.

Example Query:
*SELECT * FROM badge_history WHERE dept=”{$single_choice|Department:|SELECT id, description FROM department}”*

{$multiple_choice|label|query}

UI Control:
Group of check boxes with the given label, and check boxes generated by the given query. The query should select only two columns: the first one is the value for the check box, the second is the label for the check box to be displayed in the drop-down.

Output:
Replaces tag with comma-delimited values (not label) of check boxes selected by operator.

Example Query:
*SELECT * FROM badge_history WHERE dept=”{$multiple_choice|Department:|SELECT id, description FROM department}”*

{$host_date}

{$host_date|n}

{$host_time|}

{$host_time|n}

{$operator_date|}

{$operator_date|n}

{$operator_time|}

{$operator_time|n}

{$utc_date|}

{$utc_date|n}

UI Control:
None

Output:
Current date minus “n” days
Current time minus “n” hours

Example Query:
*SELECT * FROM badge_history WHERE dept=”{$multiple_choice|Department:|SELECT id, description FROM department}”*

{$translate_lookup_exclusive|<tablename>}

UI Control:
Translates the view results lookup values for the specified table

Output:
None

{$column_selection_exclusive|<all possible columns>|<columns selected by default>}

UI Control:
“Column Manager” provides a control to select the columns to be included in the report results.

Output:
Comma-delimited list of column names

{$union_exclusive|<table1>|<table2>}

UI Control:
Expands the SQL query into two queries; one against table1 and one against table2

Output:
None

{$number_exclusive|<label>|<field>}

UI Control:
Text field with a label

Output:
Replaces tag with user-supplied number

{$time_range_exclusive|report.DateAndTime|report.Device|report.Host|report.UTC|dev_xact|host_xact|utc_xact}

UI Control:
Date and time control

Output:
Replaces tag with SQL clauses that correspond to Date and Time criteria selected in the control

{$label_exclusive|<text>}

UI Control:
Displays a text heading only

Output:
Replaces tag with 1=1

{$yes_no_checkbox_exclusive|<text>|<checked value>|<unchecked value>|field}

UI Control:
Displays a check box with the text label

Output:
Replaces tag with either checked value or unchecked value

SQL keywords

In an SQL select statement, only the SELECT clause and the FROM clause are required. The other clauses are optional.

SQL is case sensitive. For example, if you specify %Door%, the query finds anything with the word Door in initial caps, but does not find the word DOOR in all caps. To include both, type:

WHERE description = "%Door%" OR "%DOOR%"

The SQL database stores information in tables. A table is a collection of information organized into columns and rows. Each table contains one or more columns. A column contains one specific type of information, such as last_name. Each row contains all the data about one of the records the table describes. A row contains one or more columns. In your SQL select statement, the SELECT clause limits the columns and the WHERE clause limits the rows.

You can create direct relationships between tables when you query a database to generate a report. The report displays data from several different tables as if the data belongs to a single table.

See *Logical operators* on page 305 and *Relational operators* on page 305 for information on describing relations between two values.

SELECT

Use the SELECT clause to find data from selected columns in a table. The report retrieves columns of data and lists the data under each column heading in the report. The sequence of column names in the SELECT clause determines the sequence of column headings on the report title bar.

FROM

Use the FROM clause to name the tables where the selected data is located. You can include (join) multiple database tables.

For example, the following (unfinished) SQL select statement retrieves data from the category, badge, and department tables. Notice that each column name in the SELECT clause has a table indicator. If there is more than one table, identify each column name with the table name, since identical column names that belong to different tables cause an ambiguous error.

SELECT badge.last_name, category.description, department.description FROM badge, department, category

The above SQL statement is unfinished because it requires a WHERE clause. The WHERE clause is discussed next.

Note: When selecting columns with the same name from multiple tables, make sure to specify the display table. For example:

SELECT reader.description reader, area.description area FROM reader, area

WHERE

Use the WHERE clause to set conditions on the select statement so that the query finds only selected (not all) rows in a table. The WHERE clause describes acceptable values for one or more columns. Use relational operators after the WHERE keyword, followed by search conditions or descriptions of the rows you want to find. See *Relational operators* on page 305.

When your search conditions include a column name, a relational operator, and a value, enclose character values in quotation marks.

For example, the following SQL select statement retrieves reader descriptions from the reader table that matches only the Cafeteria Reader description:

SELECT description FROM reader WHERE description = "Cafeteria Reader"

ORDER BY

Use the ORDER BY clause to sort the ROWS FOUND (data records returned). The report can sort by any column name; however, it is faster to order by columns that are indexed, such as last_name and description.

If the SQL statement does not specify the sorting order, Informix-SQL creates an index in ascending order: that is: A to Z for character fields, low to high for number and money fields, from earlier to later in time and date fields, and from smallest time span to largest time span for interval fields.

For example, the following SQL select statement retrieves data from the reader table that matches all reader descriptions, which appear in ascending alphabetical order.

SELECT description FROM reader ORDER BY description

LIKE

Use LIKE after a column name to specify a value or pattern that data must match in order to be found.

Characters typically used in a LIKE string are:

% A percent character matches zero or more characters.

_ An underscore character matches any single character.

The following SQL select statement retrieves a list of reader descriptions from the reader table where the reader description starts with the characters Lob and ends with zero or more unspecified characters.

SELECT description FROM reader WHERE description LIKE "Lob%"

The following SQL select statement retrieves a list of reader descriptions from the reader table where the reader description contains the word Door or DOOR anywhere in the description.

SELECT description FROM reader WHERE description LIKE "%Door%" OR "%DOOR%"

Logical operators

Use AND, OR, and NOT to connect one or more search conditions that create a comparison condition.

AND

Use AND to retrieve data that matches both of the values connected by AND.

The following SQL comparison statement retrieves each reader described as Engineering Reader and also has a set interval time of less than 5 seconds.

SELECT description FROM reader WHERE description = "Engineering Reader" AND Interval_Time < 5

OR

Use OR to retrieve data that matches either one of the values connected by OR.

The following SQL comparison statement retrieves reader descriptions that match either Lobby Reader or Cafeteria Reader:

SELECT description FROM reader WHERE description = "Lobby Reader" OR description = "Cafeteria Reader"

NOT IN

Use NOT IN to screen out data that you do not want in the report.

For example, the following SQL comparison statement retrieves all reader descriptions except those described as Engineering or Antipassback.

SELECT description FROM reader WHERE description NOT IN ("Engineering", "Antipassback Reader")

Relational operators

Relational operators describe a relationship between two values. Use the following characters as relational operators in a WHERE clause:

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

For example, the following SQL select statement retrieves data for employees with last names that start with the letter A or above and also start with letters below G; in other words, last names that start with the letters A through F:

SELECT last_name, employee, FROM badge WHERE last_name >= "A" AND last_name < "G"

Table 116. Data type relational operators

Data type	Greater than (>) means	Less than (<) means
DATE	Later in date	Earlier in date
TIME	Later in time	Earlier in time
INTERVAL	Longer span of time	Shorter span of time
CHAR	Later in the alphabet	Earlier in the alphabet

Scheduling reports

If there are certain history reports that you want to run at specific times, you can use this scheduling feature to run these automatically. The scheduled report will follow the day and time settings specified on the Report Events form.

All error messages and completion messages generated as a result of the scheduled report process are written to a log file in the `/cas/log` directory called `log.mmdd` where `mmdd` = system date (For example: `0302` = March 2nd). You must check the log file for messages after the scheduled report process has executed, since there are no pop-up window messages associated with this feature.

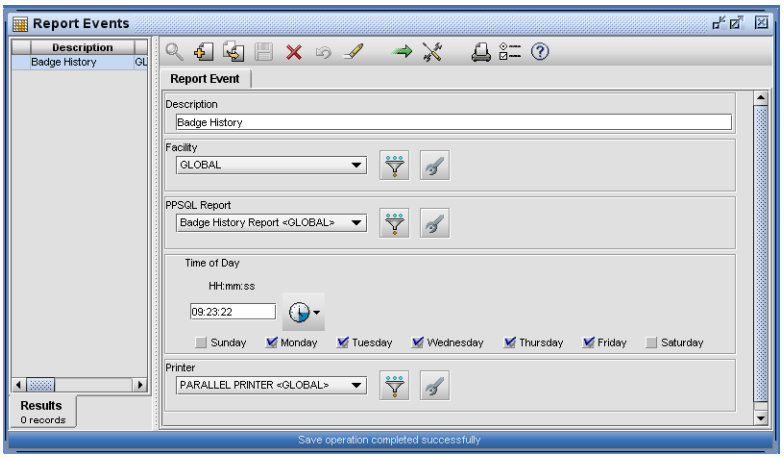
This scheduling feature can be used for both History and SQL reports, and they can be run together or separately. Each report type will have a prefix in the log file to indicate its execution. History reports will have a prefix of hist, and SQL reports will have a prefix of `ppsql`.

Note: This feature will not support variables. An audit routine that detects variables in the Report Events form prevents reports from being scheduled.

Example

Define a report event that schedules a history report of the Badge database tables to occur at 8 PM every Friday.

Figure 126.Report Event form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 117. Report Event form fields

Field name	Description
Description	Type a report event description up to 30 alphanumeric characters long.
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Report Type	Select the report you want to schedule from the PPSQL Report drop-down list. **Note:** If Enforcement of Report Permissions is enabled through the System Parameters form, only those reports that the operator has permission to access will be displayed.
HHmmss	Enter the time of day that this report is to run.
Days of the Week	Select the days of the week that the report is to run.
Printer	From the drop-down list, select a printer. (Remember to consider the width specifications of the report when choosing a printer.)

Related procedures

To schedule an SQL report:

1. From the **Reports** menu, select **Report**, and then click the **Reports** tab.
2. Define your query and report format through the Reports form, and save it under the desired name.
3. From the **Reports** menu, select **Report Events,** and then click **New** .
4. Type the **Description** of this report event.
5. Enter the time this report is to run, and select the days on which it is to run.
6. Click the **PPSQL Report** button to display a list box of SQL reports. Select the desired report.
7. Click the **Printer** button to display a list box of printers. Select the printer where this report should print. (Remember to consider the width specifications of the report when choosing a printer.)
8. Click Save .

Wide carriage printing of report events

Picture Perfect provides support for printing reports from report events to a wide carriage printer on the host. However, in order to do this, a few changes must be manually made on the host.

Keep the following items in mind if you intend to use wide carriage printing:

1. Prior to PP4.5 SP3, if you had a report wider than 80 columns, it would print in landscape mode regardless of what type of paper was being used.
2. Report events use a program called enscript to facilitate printing. This command only supports postscript printers. If your printer does not support postscript, it will not work.

3. Reports printed from Report Events use the full length of each field. For example, last_name and first_name in the person table are each 60 columns wide. It may be necessary to use the truncate statement in your reports in order to setup a predetermined size. If you only want to report the first 20 characters of the last_name, you use the syntax "last_name[1,20]" instead of "last_name" when selecting the last_name column. If this field is to be used in an ORDER BY clause, then you must refer to it by its order number. For example: "`SELECT last_name[1,20], employee[1,15] FROM person ORDER BY 1`". This will order the results by the last_name field.

Follow these steps after you have added a printer to your OS and to Picture Perfect:

1. Configure report width. After a report is created, a SQL command must be run to setup the width of the report manually. This is not a configurable field within the UI. Please follow the table below to configure the `page_width` field for each `report_event` record.

Table 118. Wide Carriage Printing Configuration

Report width	Printer paper size	Orientation	Page width
<80 columns	Letter	landscape	No action
<80 columns	Letter	portrait	81
>80 and <132	Letter	landscape	132
any	Wide paper	portrait	132

2. Type the following using the Page width from the above table:

```
# sqlstmt "update report_setup set page_width=132 where title='<title of your report>'"
```

3. You can verify the change took place by doing the following:

```
# selectrpt "select title, page_width from report_setup where title='<title of your report>'"
```

4. Optional procedure if using wide paper: Configure enscript to use wide paper when printing. Enscript, by default, uses Letter size paper. In order to use a different paper size, a configuration file must first be edited. All dimensions of paper size are measured in points. A printer's point is approximately 1/72 of an inch. The following is an example using a wide carriage printer with wide track paper (14in x 11in):

   On Linux, edit the file called `/etc/enscript.cfg`. Find the Letter line in "Media definitions" section, it will look as follows:

```
#       name       width    height   llx     lly     urx      ury
Media: Letter     612      792      24      24      588      768
```

   Change the width of this type of paper as follows:

```
Media: Letter    1008      792      24      24      984      768
```

   On AIX, edit the file called `/usr/lib/ps/MediaSizes`. Find the Letter line, it will look as follows:

```
# Name    Width   Depth   llx lly urx ury PageRegionName PaperTrayName
Letter    612     792     18  17  597 776 letter
```

Chapter 15 Backup and restore

This chapter shows you how to perform an archive, back up the database, restore the database, and recover the entire system.

In this chapter:

Overview

We recommend that during initial system setup, you perform a daily backup. Every day during initial setup, new inputs, outputs, and alarms are configured and new badge data is entered. Regular backups will protect this setup process.

The system stores badge transactions, alarm events, and operator activity in online history tables. When the online history table for an activity is almost full, the system displays an Archive Alert pop-up window with a message to archive the records of that particular table. If you prefer to archive data on a regular schedule, a Force-Rollover option can be used instead. This lets you archive a table even if it hasn't reached its threshold point.

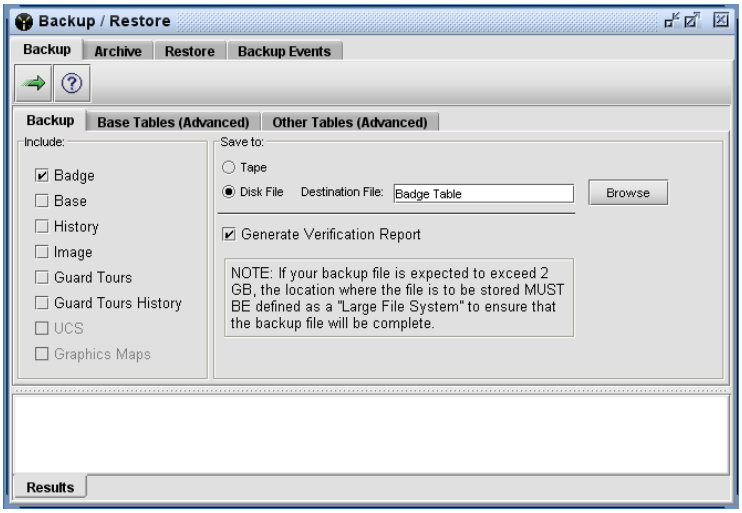
Backing up your database

A backup of your access-control database should be performed periodically. The system allows you to back up the database to tape, or disk file. If your system has optional packages installed, use separate tapes to back up each database, because each backup initializes the tape.

Example

The following example is a backup of the Badge table to a Disk file.

Figure 122.Backup form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow

Table 114. Backup form fields

Field name	Description
Include: Badge, Base, History, Optional Packages	Select the database whose files you want to back up. It is strongly recommended that you only back up one database at a time. If the Badge database is not large, then you can combine Base and Badge. Each package should be backed up to a separate tape or disk file.
Save to: Tape, Disk File	Select the media to use for the backup. **Note:** If Disk File is selected, any file or path selected is appended to the system configured backup directory.
Destination File	If you chose to save to a Disk File, enter the name of the file system to store the backup. Click Browse to select from a list. If your backup file is expected to exceed 2 GB, ensure that the location where the file is to be stored is defined as a Large File System. Otherwise, the backup file will be incomplete.
Generate Verification Report	Click to generate an on-screen verification report.
Base Tables	This is an advanced option that allows you to select only certain tables in the Base database for backup or you can click Check All to select all the tables.
Other Tables	This is an advanced option that allows you to select only certain tables in the various databases on your system for backup. You can click Check All to select all the tables.

Related procedures

To perform a backup:

1. From the **Control** menu, select the **Backup Restore** menu item, and then click the **Backup** tab.
2. From the **Include:** section, select one or more of the options: Badge, Base, History, or an optional package, corresponding to the tables you want to back up.
3. If you want to see exactly which tables are included in your selection, you may click the **Base Tables (Advanced)** or **Other Tables (Advanced)** tabs. These tabs display a listing of all the tables in the database. The tables included in your selection will be toggled on.

   Note: Do not toggle any of the individual table buttons unless instructed to do so by your support representative.
4. If you want to generate an on-screen verification report, click **Generate Verification Report**.
5. Use the appropriate radio button to specify whether you are backing up to **Tape** or **Disk File**.

   Note: When Disk File is selected, clicking Browse displays a list from which you can select the destination file for the backup/archive.
6. Click **Execute** to start the backup.

Perform a backup using the command line option cba

The command line version of backup uses a configuration file, `backup.cfg`, located in `/cas/db/text`. This file contains the flat files to be backed up. You can edit this file if you want to add or delete files to be backed up.

You must precede each file or directory name with a package name followed by a colon and a space (or tab). This will cause the specified files to be backed up only when the associated package is backed up. The syntax of the contents of the `backup.cfg` file is:

package name	directory or file to back up
base:	/etc/`passwd`
base:	/etc/group
base:	/etc/security

The following table describes the cba command line options.

Table 115. CBA Command Line Option

Command	Description
-o (htable)	Rollover, then archive the selected history table
-b	Backup specified table or group of tables
-a (htable)	Archive the specified history table
-r	Force rollover on history (archive only)
-rt (#)	Retry rollover (#) of times (default is 100)
-d (file)	Write to the specified disk file
-t	Tape - write to /dev/pptape
-v	Verify that data was written successfully
-np	Do not prompt for tapes if specified with -c
-nb	Run from netback
-e (table)	Backup specified tables
-l (file)	Backup tables specified in file

The following tables can be backed up (b) or archived (a):

Table 116. Tables that can be backed up or archived

Table	(b) or (a)	Description
-badge	ba	badge table / badge history
-base	b	basic database
-hist	ba	all three history tables
-image	b	badge photos and related files
-graph	b	alarm graphics (if installed)
-tour	b	guard tours (if installed)

Table 116. Tables that can be backed up or archived (continued)

Table	(b) or (a)	Description
-thist	ba	tour history (if installed)
-visitor	b	visitor tables (if installed)
-vhist	ba	visitor history (if installed)
-alarm	a	alarm history
-oper	a	operator history

To launch the cba backup option:

1. Open a terminal window.
2. Type a command, including options. For example: to backup and verify the base Picture Perfect package to a disk file, type:

   `cba -c -b -v -d /tmp/basebackup -base -badge` Enter

   The cba backup option will back up the files contained in the `backup.cfg` file.

Archiving your database

The system prompts you (by way of an alarm) to perform a specific archiving function for Badge History, Alarm History, or Operator History when the primary table for that history reaches 95 percent capacity. At that time, the system takes the records stored in that primary history table and moves them to a temporary history table. When an archive is performed for a particular history, it uses the information in its temporary table; that way, the primary table is free to start collecting new information right away.

If an archive is not performed before the primary table 95 percent capacity again, the data in the temporary table will be overwritten, and the original archive data lost. It is therefore important to perform the indicated archive when the system notifies you through an alarm.

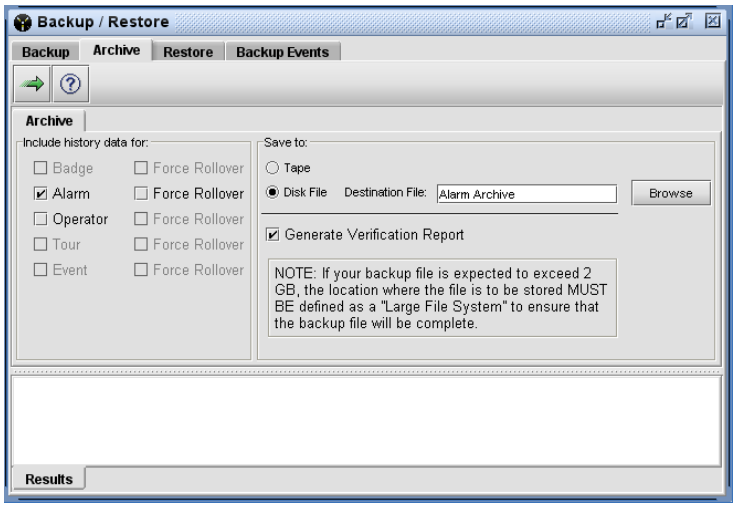
Since the time needed to reach a history threshold varies with activity levels, it's hard to predict when a particular threshold will be reached. A Force-Rollover option exists, therefore, which allows you to archive data on a regular schedule, such as once a week. This task can then be incorporated into your normal backup procedure. The Force-Rollover option takes data in the primary table and transfers it to the temporary table even if the primary table is not full. The Force-Rollover option will only be displayed on the Backup window if the data currently in the temporary table has already been archived. This prevents un-archived data from being erased when new data overwrites it. (This data will, however, be overwritten when the primary table becomes full.)

Note: In Picture Perfect 4.1, in addition to the Archive Notice pop-up, an alarm is triggered to notify that it is time to perform an archive.

Example

The following example is an archive of the Alarm table to a Disk file.

Figure 123.Archive Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 117. Archive form fields

Field name	Description
Include: Badge, Alarm, Operator, Event, Optional Packages	Select the type of history files you want to archive. It is strongly recommended that you only archive one database at a time. Each package should be archived to a separate tape or disk file. Since the time needed to reach a history threshold varies with activity levels, it's hard to predict when a particular threshold will be reached. A Force-Rollover option exists, therefore, which allows you to archive data on a regular schedule, such as once a week. This task can then be incorporated into your normal backup procedure. The Force-Rollover option takes data in the primary table and transfers it to the temporary table even if the primary table is not full.
Force Rollover	Picture Perfect uses two history tables for each type of history: primary and temporary. When the primary fills up, it is renamed: history_tmp and an archive notification window for that table displays. Since the time needed to reach a history threshold varies with activity levels, it's hard to predict when a particular threshold will be reached. A Force-Rollover option exists, therefore, which allows you to archive data on a regular schedule, such as once a week. This task can then be incorporated into your normal backup procedure. The Force-Rollover option takes data in the primary table and transfers it to the temporary table even if the primary table is not full.
Save to: Tape or Disk File	Select the media to use for the archive. **Note:** If Disk File is selected, any file or path selected is appended to the system configured backup directory.

Table 117. Archive form fields (continued)

Field name	Description
Destination File	If you chose to save to a Disk File, enter the name of the file system to store the archive. Click Browse to select from a list. If your archive file is expected to exceed 2 GB, ensure that the location where the file is to be stored is defined as a Large File System. Otherwise, the archive file will be incomplete.
Generate Verification Report	Click to generate an on-screen verification report.

Related procedures

To archive data:

1. From the **Control** menu, select the **Backup Restore** menu item, and then click the **Archive** tab.
2. From the **Include:** section, select one or more of the tables: Badge, Alarm, Operator, Event, or an optional package, corresponding to the tables you want to archive.
3. The **Force Rollover** option is displayed beside each history option. Toggle this button On if you want to force a rollover of information and archive that data.
4. If you want to generate an on-screen verification report, click **Generate Verification Report**.
5. Use the appropriate radio button to specify whether you are backing up to **Tape** or **Disk File**.

   Note: When Disk File is selected, clicking Browse displays a list from which you can select the destination file for the backup/archive.

6. Click **Execute** to begin archiving.

Restoring your database

Use the Restore function to restore a database from disk files or tapes. Keep the following in mind before you restore your database:

CAUTION: Do not restore non-history data on a running system.

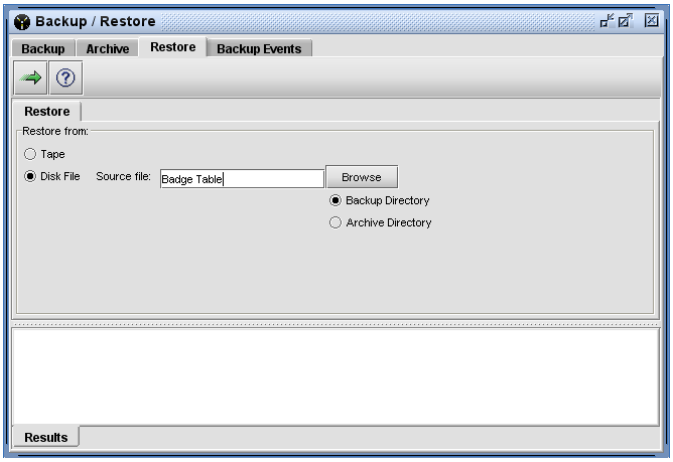
- The Restore function does not overwrite existing data. To clear your tables, contact your support representative.
- Before you restore a database, you should perform a database initialization. For instructions on how to perform this task, contact your support representative.
- The Restore function restores database files only, not regular files. To restore non-database files, use the command line database restore option, cbr, or the database restore utility, restore.sh.
- When a database is restored, please note that data is not downloaded to the controllers until the controllers are reset.

Note: Archives are restored to tmp tables.

Example

The following example is a restore of the Badge table to a disk file.

Figure 124.Restore form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow

Table 118. Restore form fields

Field name	Description
Restore from: Tape or Disk File	Select the media that contains the data to be restored. **Note:** If Disk File is selected, any file or path selected is appended to the system configured backup directory.

Table 118. Restore form fields

Field name	Description
Source file:	If you chose to restore from a Disk File, enter the name of the file system where the data is stored. Select Backup Directory or Archive Directory, and then click Browse to select from a list.

Related procedures

To perform a restore:

1. From the **Control** menu, select the **Backup Restore** menu item, and then click the **Restore** tab.
2. Use the appropriate radio button to specify whether you are restoring from **Tape** or **Disk File**.

   Note: When Disk File is selected, clicking Browse displays a list from which you can select the file from which the data will be restored. See the User Manual for detailed information on configuring this option.

3. Click **Execute** to start the restore. When the Media pop-up window appears, insert the tape.
4. Click **OK** to start the restore.

Perform a restore using the command line option cbr

The command line version of restore uses a configuration file, `restore.cfg`, located in `/cas/db/text`. This file contains the flat files to be restored. You can edit this file if you want to add or delete files to be restored.

The syntax of the contents of the `restore.cfg` file is:

```
/etc/passwd
/etc/group
/etc/security
```

The following table describes the cba command line options.

Table 119. CBA Command Line Option

Command	Description
-o (htable)	Rollover, then archive the selected history table
-b	Backup specified table or group of tables
-a (htable)	Archive the specified history table
-r	Force rollover on history (archive only)
-rt (#)	Retry rollover (#) of times (default is 100)
-d (file)	Write to the specified disk file
-t	Tape - write to /dev/pptape
-v	Verify that data was written successfully
-np	Do not prompt for tapes if specified with -c
-nb	Run from netback
-e (table)	Backup specified tables

Table 119. CBA Command Line Option

Command	Description
-l (file)	Backup tables specified in file

To launch the cbr restore option:

1. Open a terminal window.
2. Type a command, including options. For example: to restore and verify the base Picture Perfect package from a disk file, type:

   ```
   cbr -c -a -v -d /tmp/basebackup
   ```
   Enter

   The cbr restore option will restore the files contained in the `restore.cfg` file. After the database records are restored and if your backup included "flat" files, messages similar to the following display:

   ```
   This program edits the configuration file, /cas/d/text/restore.cfg before running
   the backup or restore programs.
   ```

   For backups, you must also precede each file or directory name with a package name followed by a colon and a space (or tab). This will cause the specified files to be backed up only when the associated package is backed up.

   For restores, *do not* precede each file or directory name with a package name, colon, or space. Simply supply the file or directory you want to be restored from the media.

   ```
   P - Print Current List
   A - Add Item to List
   E - Edit Item on List
   D - Delete Item from List
   Q - Quit and Save File
   Enter Function (P/A/E/D/Q): p
   ```
3. Type the letter p to print the list of files to be restored. A list, similar to the following, of the files contained in the **`restore.cfg f`**iles displays:

   ```
   Current File List
   1. /cas/forms/*
   2. /cas/lists/*
   3. /photo/photo/*
   4. /photo/designs/*
   ```
4. If these are the files you want to restore, press Q to quit and save the file. If you want to edit the list, press A, E, or D, as appropriate. When you have completed your edits, press Q to quit and save the file.

To restore the entire system:

1. To recover the entire system, perform the installation procedures. For the complete installation procedures for Picture Perfect and the operating system, refer to the Picture Perfect Installation Manual.

   When you reach the Database Restore utility during installation, select option 2 (Restore customer's Database from Tape), or option 3 (Restore Customer's Database from Disk File), depending on your media type, and reload your database backup rather than the minimum or sample database.

Chapter 16 Data Generator and templates

This chapter shows you how to use templates and template groups to create records.

In this chapter:

Overview

The ability to run Data Generator is governed by your system permission profile. The ability to run templates is governed by your facility permission profile. The action permission Run Templates must be enabled on the Facility Permissions Profile form. This function allows you to generate new records based on a template.

There are two ways to use templates:

- Generate new records of the same type using the Run Template option on the form toolbar. When a template is run, a Wizard guides you through the necessary steps to create a new record for the form.
- Generate and link all records required to set up a particular device using the Run Template Group option on the toolbar of the Data Generator form. The Data Generator guides you through the necessary templates required for all the associated records.

Running templates

All Picture Perfect forms, with the exception of the system forms such as Facilities and the various monitors, allow you to run a wizard to create new records based on a template. Your system is installed with some default templates that you may use or you can create your own. See *Managing templates* on page 324.

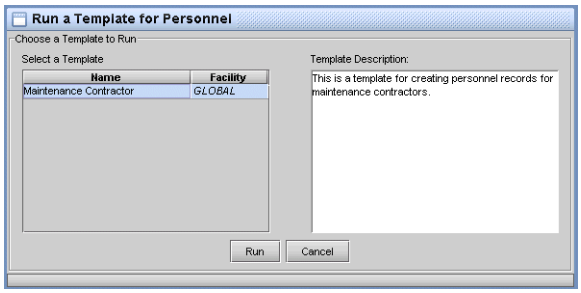
Related procedures

To run a template:

1. From the Primary menu, such as Access, Configuration, Control, or Setup, select a Secondary menu item, and then click the appropriate tab to access the form for which you are creating a new record. For example: **Access**, **People**, **Personnel**.
2. Click  .

   A screen similar to the following will display.

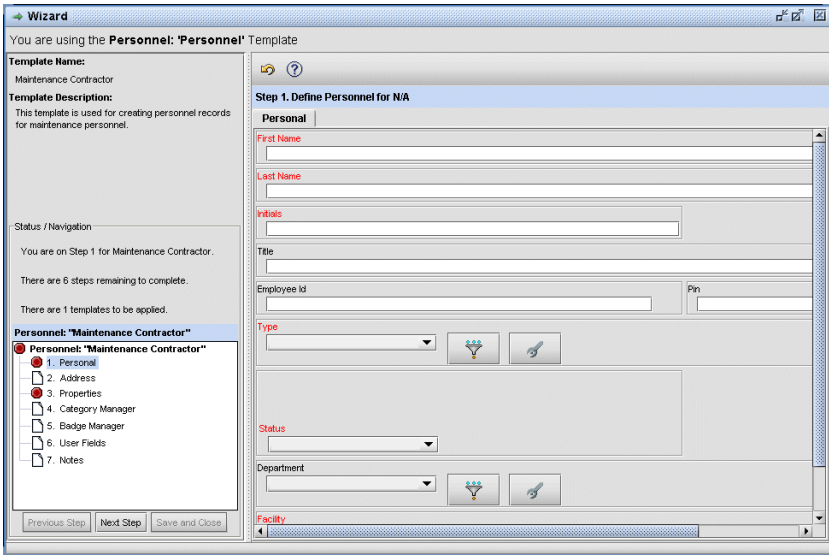
Figure 125.Personnel Template



3. From the **Select a Template** pane, highlight a template. A description of what this templates creates displays in the **Template Description** pane.
4. Click **Run**.

   A Wizard similar to the following displays.

Figure 126.Template Wizard: Step 1



5. In our example, under **Status/Navigation**, notice that you are on Step 1 and the Wizard displays the Personal tab. Fill in the required fields that appear in red and then click **Next Step**.
6. Continue to fill in the remaining tabs until all required fields are compete.When you have finished, click **Save and Close**.

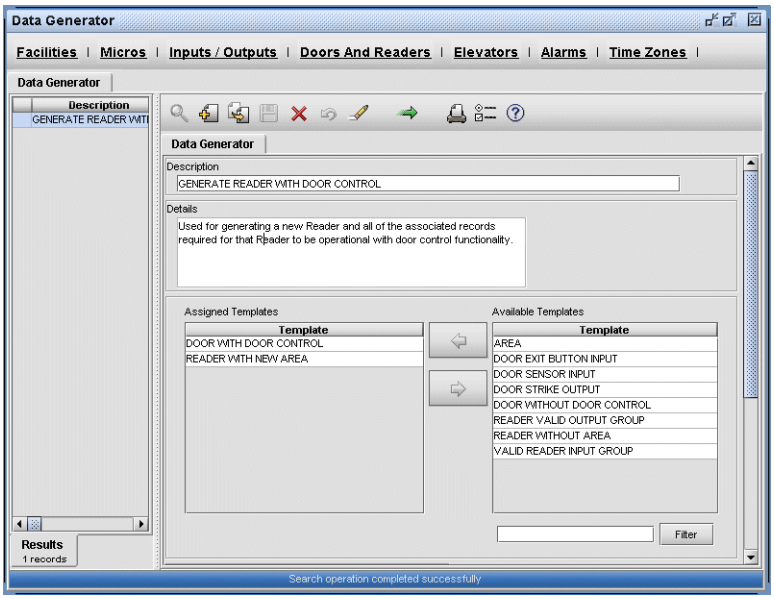
Data Generator

The Data Generator form allows you to run a template group which contains templates for all the associated records required to set up a device. Default template groups are provided for you.

Data Generator form

The following example reflects a template group designed to generate a new reader.

Figure 127.Data Generator form



Fields and controls

The following is a list of fields that may require additional information for you to complete.

Table 120. Data Generator form fields

Field name	Description
Description	A description (up to 60 characters) to identify this template group, for example: *GENERATE READER WITH DOOR CONTROL*.
Details	A synopsis of the kind of records that are created by this template group, for example: *Used for generating a new reader and all the associated records required for that reader to be operational with door control functionality.*
Assigned Templates	The templates that make up this template group.
Available Templates	A list of all defined templates not included in the template group.

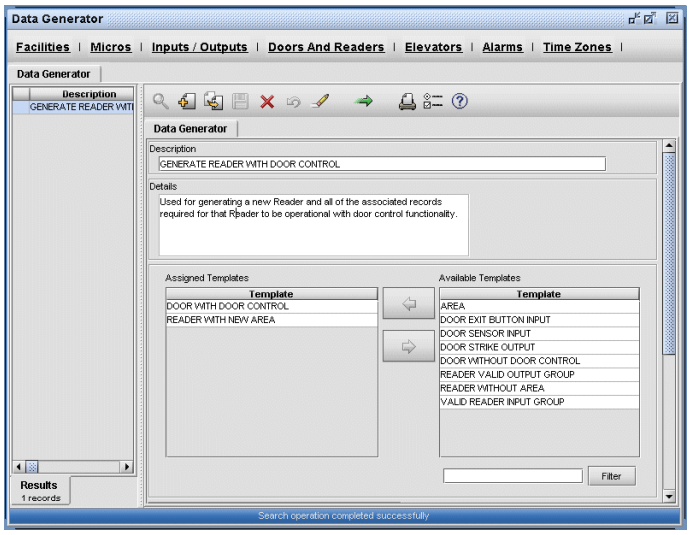
Related procedures

To run a template group:

1. From the **Configuration** menu, select **Data Generator**.
2. From the toolbar, click **Find** .

   The record list window, or data grid, displays a list of template groups defined in the system.
3. Select a template group from the list. For example the default GENERATE READER WITH DOOR CONTROL template group as shown below.

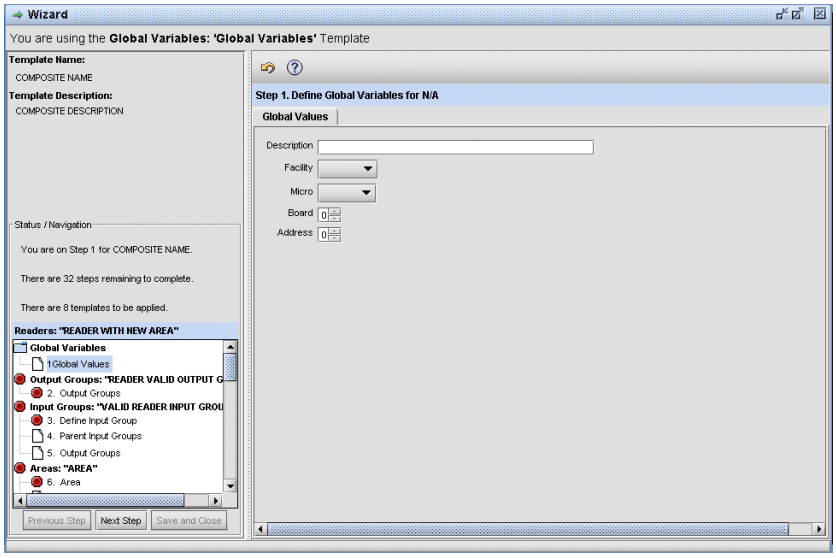
Figure 128.Data Generator: Template group example



4. Click  .

   A screen similar to the following will display.

Figure 129.Template group Wizard



5. In our example, under **Status/Navigation**, notice that you are on Step 1 of 32 and there are 8 templates included in this template group. The first step allows you to assign a global name to be applied to the related records but this is not required. Click **Next Step**.
6. Continue to fill in the remaining tabs until all required fields are compete.When you have finished, click **Save and Close**.

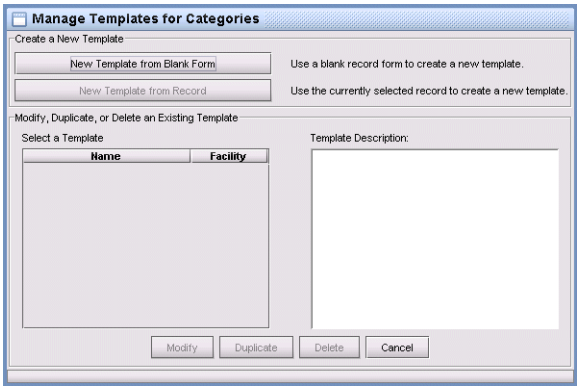
Managing templates

The ability to manage templates for operators and system administrators is governed by their Facility Permission Profile. The action permission Manage Templates must be enabled on the Facility Permissions Profile form. This function allows users to create a new template from a blank form or use an existing record as the basis for a new template. Existing templates may be modified, deleted, or duplicated.

Example

The following example reflects the Manage Templates dialog for the Categories form.

Figure 130.Manage Template



Fields and controls

Table 121. Manage template form fields

Field name	Description
Create a New Template	New Template from Blank Form: Click to create a new template from a blank form with all fields initially empty. New Template from Record: Click to create a new template based on an existing record. The fields in the new template are populated with the information from the existing record.
Modify, Duplicate, or Delete an Existing Template	• Select a Template: From the list of existing templates, select the template you want to modify, duplicate, or delete. • Template Description: This field is view only and reflects the description of the selected template. • Modify, Duplicate, Delete, Cancel: Click the appropriate button based on the action you want to perform.

Related procedures

To add a template:

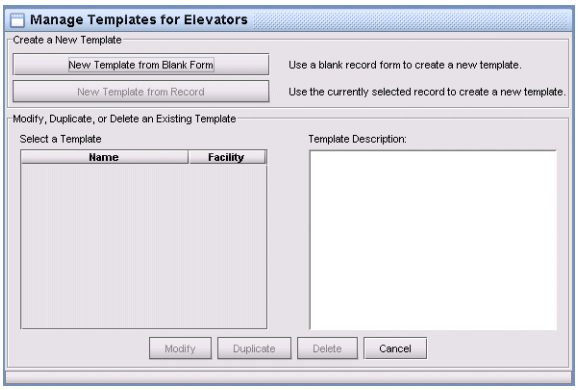
1. From the Primary menu, such as Access, Configuration, Control, or Setup, select a Secondary menu item, and then click the appropriate tab for the form that you are creating a template. For example: *Configuration, Elevators, Elevators*.

2. To create a template from a blank record, click . The example that follows is based on a blank record.

   Note: If you want to create a template from an existing record, first perform a search and select the record that you want to base the template on.

   A screen similar to the following displays.

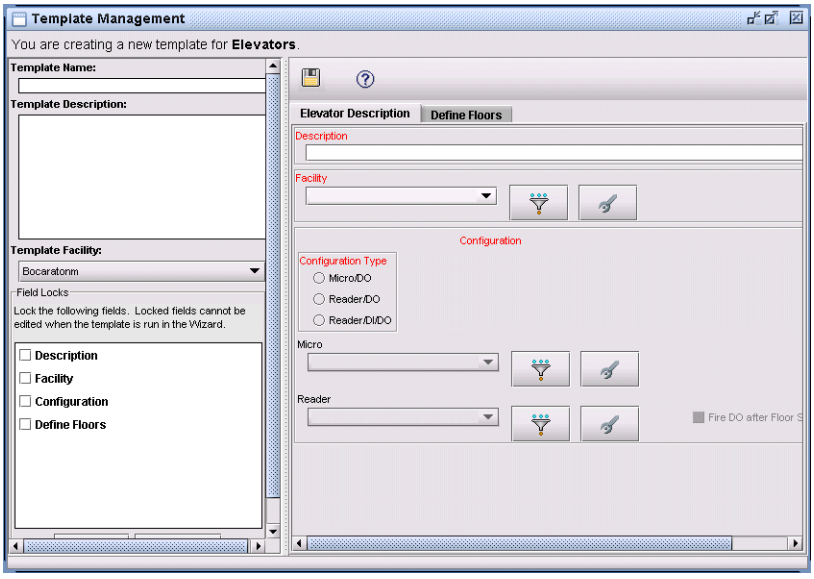
Figure 131.New Template



3. Click **New Template from Blank Form**.

   A screen similar to the following displays.

Figure 132.New Template from blank form



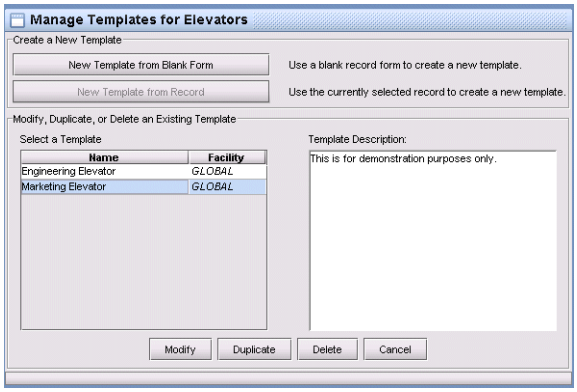
4. Under **Template Name**: enter a name for this template record, for example *Marketing Elevator form*.
5. Under **Template Description**: enter text that describes the purpose for which this template is used.
6. Under **Template Facility**: select the facility to which this record is assigned.
7. Under **Field Locks** select any fields that you do not want the user to edit when the template is run. Be sure to populate those fields with the information that you want locked.

8. When you have completed the template, click Save .

To edit a template:

1. From the Primary menu, such as Access, Configuration, Control, or Setup, select a Secondary menu item, and then click the appropriate tab for the form whose template you are going to edit. For example: *Configuration, Elevators, Elevators.*
2. Click . A screen similar to the following displays.

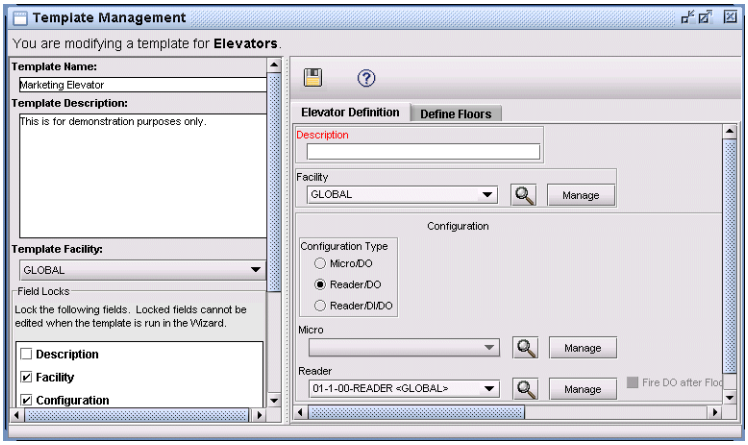
Figure 133.Manage Template



3. Select the template you want to edit and click **Modify**.

   A screen similar to the following displays.

Figure 134.Modify Template



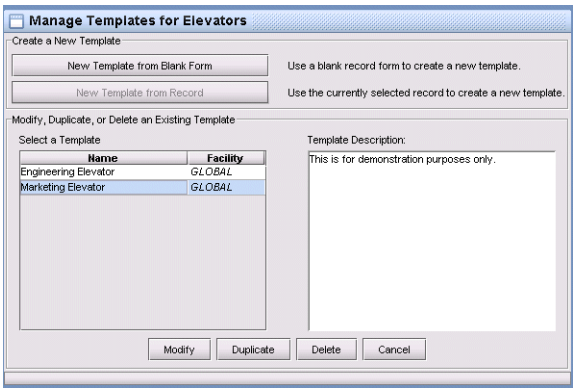
4. Make the desired changes.
5. When you have completed your changes, click Save .

To delete a template:

1. From the Primary menu, such as Access, Configuration, Control, or Setup, select a Secondary menu item, and then click the appropriate tab for the form whose template you are going to edit. For example: *Configuration, Elevators, Elevators*.
2. Click .

A screen similar to the following displays.

Figure 135.Manage Template



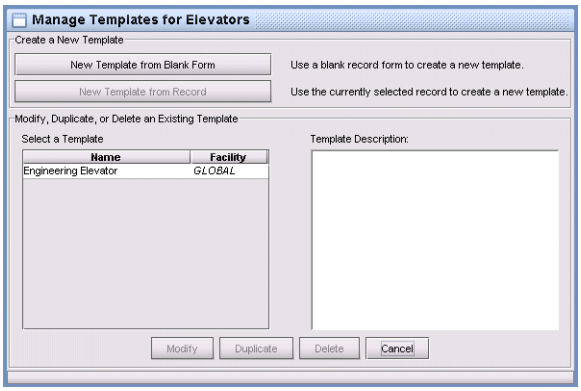
3. Select the template you want to edit and click **Delete**.

To duplicate a template:

1. From the Primary menu, such as Access, Configuration, Control, or Setup, select a Secondary menu item, and then click the appropriate tab for the form whose template you are going to edit. For example: *Configuration, Elevators, Elevators*.
2. Click .

   A screen similar to the following displays.

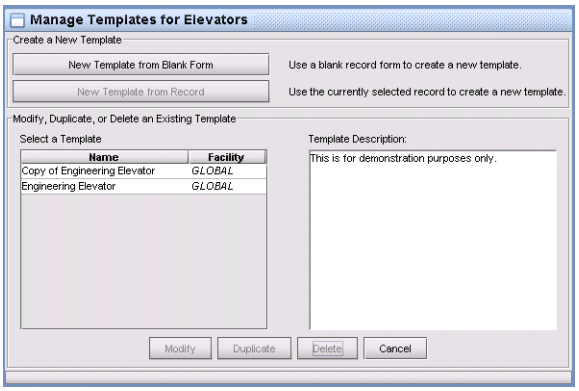
Figure 136.Manage Template



3. Select the template you want to copy and click **Duplicate**.

   A screen similar to the following displays.

Figure 137.Duplicate Template



4. If you want to save it under a different name or edit any fields, select it and click **Modify** to make the necessary changes.

Chapter 17 User interface customization

This chapter shows you how to customize your system to your particular needs using custom forms and custom lists.

In this chapter:

Overview

All Picture Perfect forms support custom forms and templates that can be created based on an existing record or by modifying a blank record. The templates can then be used to generate new records with the necessary links already set up, saving the operator time. Custom lists can be created to appear in the user fields on your Personnel forms to satisfy specific requirements

Creating and editing custom forms

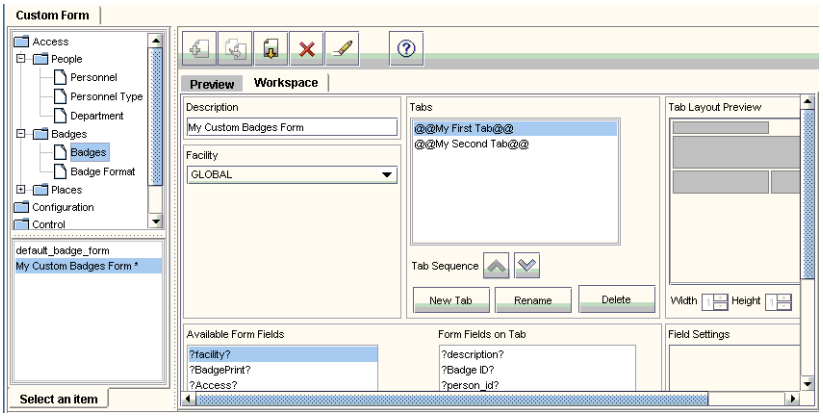
In addition to required fields, Picture Perfect forms can be customized to include the fields and tabs of your choice. For example, if your facility does not use expiration dates/times on badges, you could exclude those fields. You can use names that are more meaningful to your particular business. Once you have designed your form in the Workspace, you can preview the results by clicking the Preview tab. A custom form may be set as the default.

Note: In an Enterprise system, the following restrictions apply:

- The default Custom Form may be set for the network host and each subhost. However, functions, such as editing and creating, must be performed from the network host.
- Custom Forms cannot be deleted from any host in an Enterprise system.

Note: In a Redundant system, the default Custom Form can only be set from the primary host. This will set the default Custom Form to be used by both the primary and backup hosts. All other functions, such as editing and creating, must be performed from the primary host.

Figure 138.Custom Form



Fields and controls

The following is a list of fields that may require additional information for you to complete.

Table 122. Custom form fields

Field name	Description
Description	The name used to describe the custom form.
Facility	This is a required field. Assigning a facility to a custom form record allows the administrator to filter the records that can be viewed.

Table 122. Custom form fields (continued)

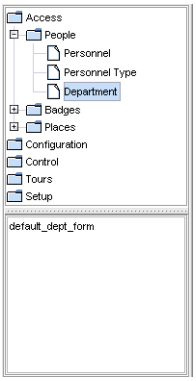
Field name	Description
Tabs	The labels of the tabs that you create are displayed in this box.
Tab Sequence	The order in which the tabs display can be manipulated by using the Tab Sequence arrows.
New Tab	Click to create a new tab. The label New Tab will display in the Tabs window.
Rename	Click to rename a selected tab. *Example: Rename New Tab, to a descriptive label, such as Personal Info.* Select the current text, rename as desired, and then press <Enter>.
Delete	Click to delete a selected tab.
Tab Layout Preview	Once fields have been added to a tab, the layout is displayed in this window.
Width	To adjust the width of a field, select the field label in the Form Fields on Tab window. The selected field layout will be highlighted and you can make adjustments using the Width spin box.
Height	To adjust the height of a field, select the field label in the Form Fields on Tab window. The selected field layout will be highlighted and you can make adjustments using the Height spin box.
Available Form Fields	The fields that you can choose to place on a tab.
Form Fields on Tab	The fields that you have chosen to place on a tab.
Field Sequence	The order in which the fields display can be manipulated by using the Field Sequence arrows.
Field Settings	The field attributes are listed in this window, such as maximum length.

Related procedures

To create a custom form:

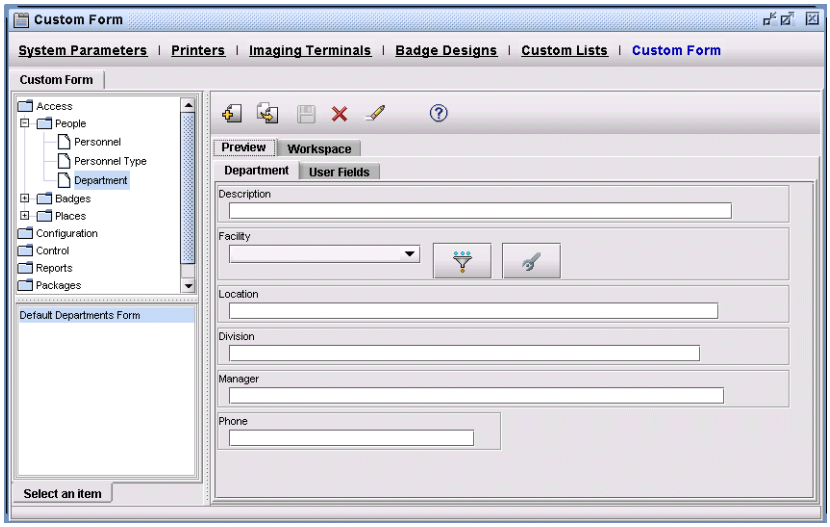
1. From the **Setup** menu, select **Custom Form**.
2. From the data grid, navigate to the type of custom form you want to create, for example, *Department*.

Figure 139.Data Grid



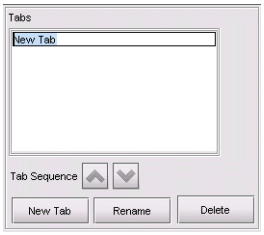
Note: `default_dept_form` is shown in the bottom portion of the grid. If you select it, the preview pane displays the current default Department form.

Figure 140.Blank Preview pane



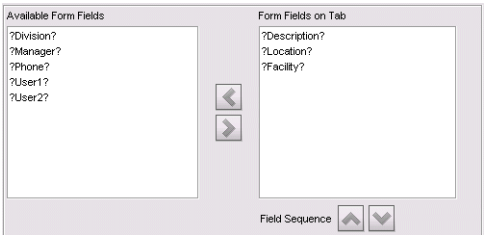
3. From the toolbar, click **New**  to display a blank preview pane.
4. Click the **Workspace** tab to begin creating your custom form.
5. In the **Description** field, highlight **New Custom Form** and type a name for the custom form, such as: *Accounting Department Form*.
6. Click the **Facility** drop-down list to assign the custom form record to a facility.
7. Click **New Tab** and then **Rename** to assign a meaningful name to the tab.

Figure 141.Tabs



8. From the **Available Form Fields** list box, select a field that you want to appear on the tab and click the arrow to display it in the **Form Fields on Tab** list box.

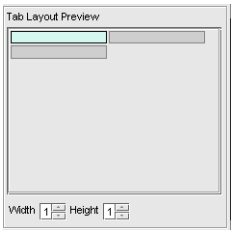
Figure 142.Form fields



9. Continue to add or remove fields from the form. You can rearrange the order of the fields using the arrows.

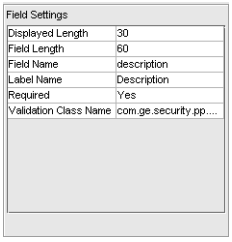
10. As fields are added to the **Form Fields on Tab** list box, corresponding boxes are displayed in the **Tab Layout Preview** window. To adjust the width or height of a field box, highlight the field in the **Form Fields on Tab** list box. The corresponding field box in the **Tab Layout Preview** window will be highlighted and can be manipulated using the **Width** or **Height** spin boxes.

Figure 143.Tab layout



11. Under **Field Settings**:
    - To make a field mandatory, change the required attribute to Yes.
    - To change the name of a field, type the new name in the fieldname box.

Figure 144.Field settings

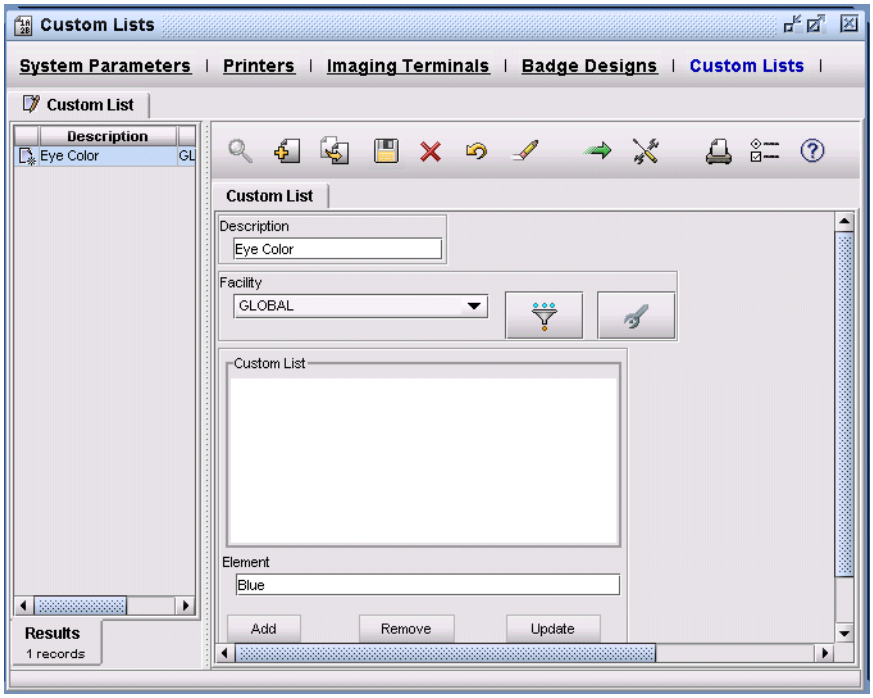


12. Click **Save** to save your custom form.

Creating and editing custom lists

You can create custom lists to appear in the user fields of the Personnel form to satisfy specific requirements. For example, you can create a custom Personnel form that contains a drop-down list of company or division names.

Figure 145.Custom List form



Fields and controls

Table 123. Custom List form fields

Field name	Description
Description	Type any alphanumeric combination (1 to 60 characters). *Example: Eye Color*
Custom List	The items that will appear in the custom list are displayed in this box.
Item	Type the name of the item to be included in the custom list.
Add	Click Add to insert the text entered in the Item: box to the Custom List box.
Remove	Select one or more items in the Custom List box and click Remove to delete them from the list.
Update	Select an item in the Custom List box. It will be displayed and available for editing in the Item box. When you have completed your edits, click Update.
Set Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.

Related procedures

To create a custom list:

1. From the **Setup** menu, select **Custom Lists**, and then click the **Custom List** tab.
2. Click **New** .
3. Enter a meaningful description to represent the list, such as *Eye Color*.

4. Assign the record a facility from the **Facility** drop-down list. Click **Manage** to display the Facilities form, where you may add or delete facilities from this drop-down list. You must have Manage permission to perform this function.
5. In the **Element** field, type an item to be added to the list.
6. Click **Add** to add the item to the Custom List box.
7. Repeat steps 5 and 6 as necessary to complete the list.
8. Click **Save** to save your custom list.

To delete a custom list:

1. From the **Setup** menu, select **Custom Lists**, and then click the **Custom List** tab.
2. From the toolbar, click **Find** .

   The record list window, or data grid, shows the results of search operations and allows you to quickly navigate through the records found by a search. When an application is started, the record list window is initially empty.
3. Select a record from the list in the data grid.
4. Click **Delete** .

   The selected record appears in the data grid with the deleted icon next to it.
5. Click **Save** . This icon will not be available if all required information is not entered or if you do not have the required permissions for the form.

   Note: If you delete a custom list that is being used on a custom form, the custom list will *not* be deleted from the form.

Chapter 18 Advanced access control features

This chapter describes how to control specific areas of access in your system according to your specific requirements.

In this chapter:

Overview

Your access control system is a group of devices working together, including a host, micros, readers, doors, inputs, and outputs. To accommodate high security areas, elevators, and varying stages of security alerts, these devices can be configured to operate in different manners, based on your particular needs.

Occupancy control

Picture Perfect allows the number of persons in a controlled space to be monitored by enabling Occupancy Control through the Area form. This option is used when the number of people in an area must be controlled, such as fire code enforcement regulations or when Two Man Rule is enforced. The occupancy count is set to zero and Picture Perfect updates the occupancy count when a valid entry or exit to/from the area occurs.

Note: Areas with Occupancy Counting enabled cannot span micros. All readers and doors must be physically connected to the same micro.

How to set up occupancy control

You need to complete the following forms to set up occupancy control for an area:

- Reader form: To configure the area readers.
- Door form: To configure the doors in the area.
- Facility Profile form: To enable Occupancy Control.
- Area form: To enable Occupancy Counting for the area.

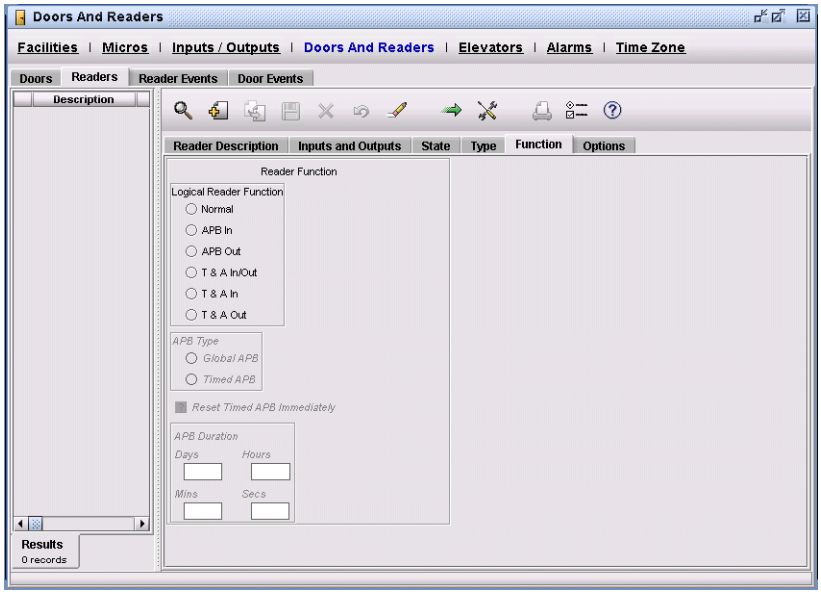
To set up the area readers:

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Readers** tab.
2. From the toolbar, click **Find**  to locate the reader record you want to set up.
3. On the **Function** tab, under **Logical Reader Function**, enable the appropriate radio button: APB In, APB Out, T&A In, or T&A Out.

   Note: In an area with Occupancy Control enabled:

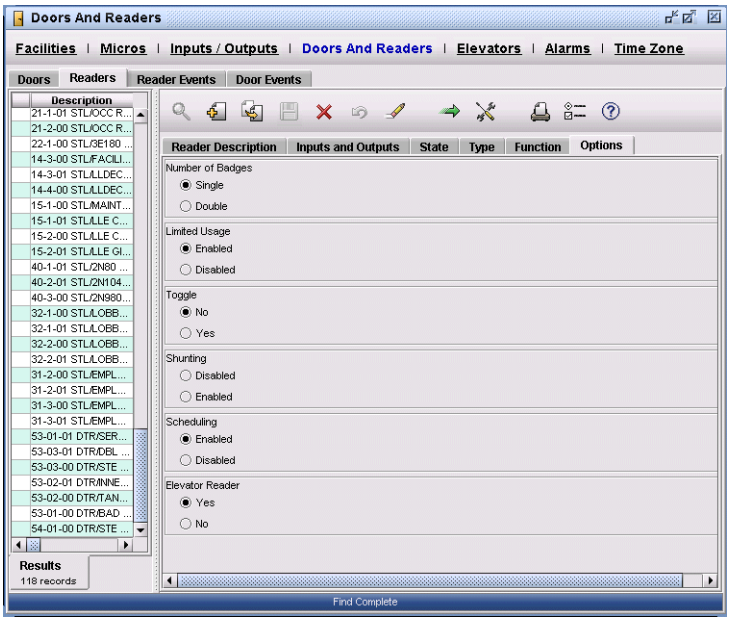
   - All readers in the area must be assigned one of these logical functions: APB In, APB Out, T&A In, or T&A Out.
   - APB readers must be set to Global. Timed APB is not allowed.
   - The logical reader function T&A In/Out is *not* allowed for any reader.

Figure 146.Reader form: Reader Function



4. On the **Reader Description** tab, under **Micro**, verify that all readers in the area are assigned to the same micro.
5. On the **Options** tab, under **Number of Badges**, verify that all readers are set to **Single**.

Figure 147.Reader form: Options



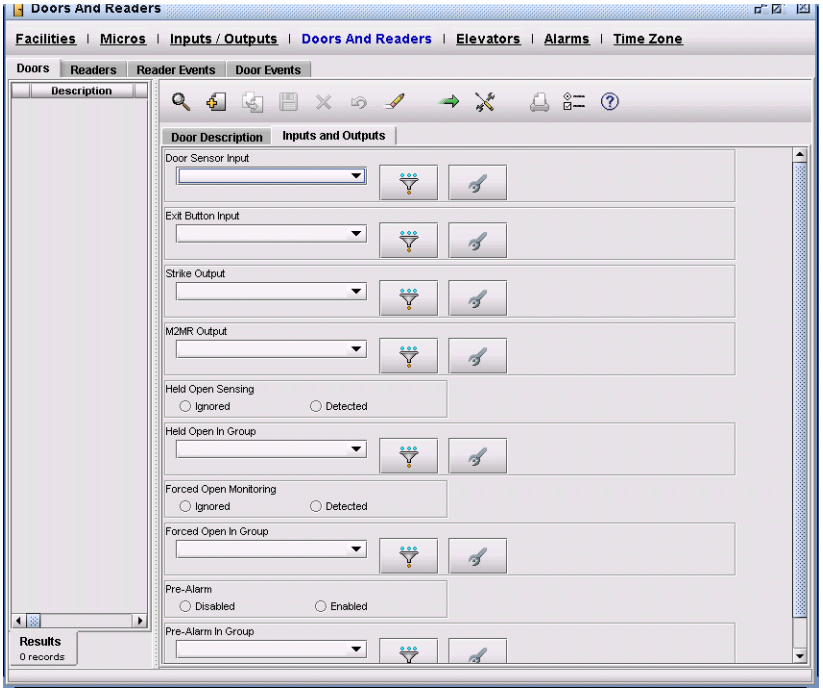
6. **Save** and exit the Readers form.

To set up the area doors:

Note: The door sensor input and the door output must be physically connected to the same micro.

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. From the toolbar, click on **Find** to locate the door record you want to set up.
3. On the **Inputs and Outputs** tab, click **Door Sensor Input**.

Figure 148.Doors form: Inputs and Outputs

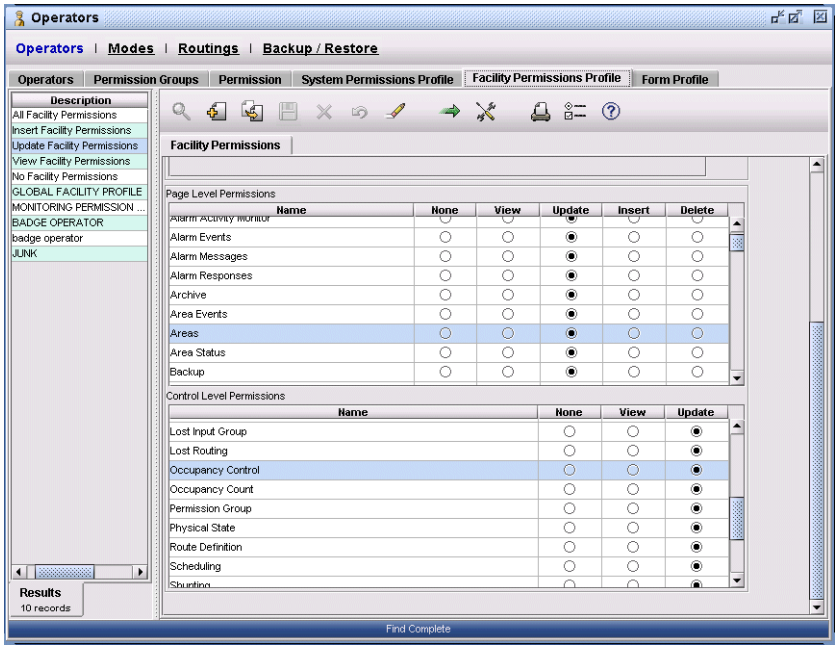


4. Select the appropriate input from the list displayed.
5. **Save** and exit the Doors form.

To enable Occupancy Control:

1. From the **Control** menu, select **Operators**, and then click the **Facility Permissions Profile** tab.
2. From the toolbar, click on **Find** to locate the Facility Permission profile record you want to modify.
3. Under **Page Level Permissions**, click on **Areas** and make sure the level of permission is set to **Update**.
4. Under **Control Level Permissions**, click on **Occupancy Control** and make sure the level of permission is set to **Update**.

Figure 149.Facility Permissions Profile form



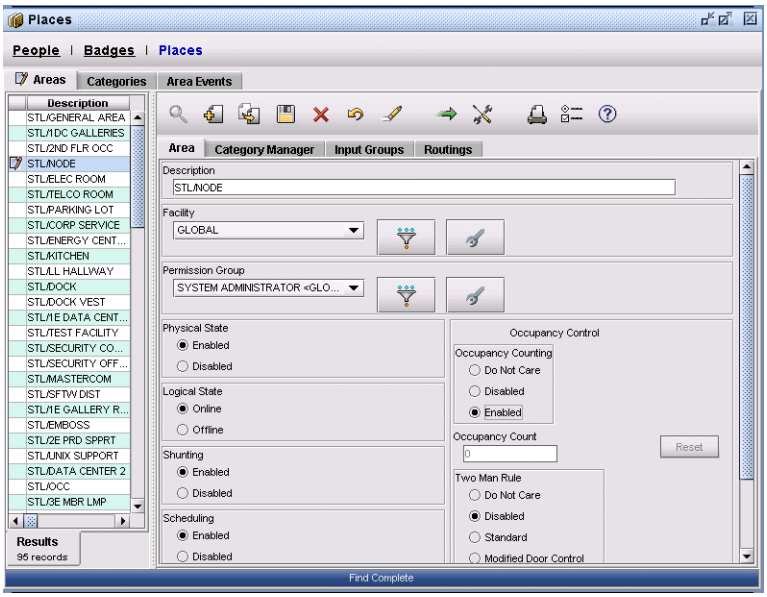
5. **Save** and exit the Facility Permissions Profile form.

To enable Occupancy Counting for the area:

Note: In order to perform this function, you must have Occupancy Control permission. See *To enable Occupancy Control:* on page 340.

1. From the **Access** menu, select **Places**, and then click the **Areas** tab.
2. From the toolbar, click on **Find** to locate the area record you want to set up.
3. On the **Area** tab, under **Occupancy Control**, enable the **Occupancy Counting** radio button.

Figure 150.Areas form: Occupancy Control



4. **Save** and exit the Areas form.

Two man rule (2MR)

Some high security areas, such as banks, may require that a minimum of two people occupy an area. Picture Perfect has the ability to control occupancy in an area by placing the area in Two Man Rule (2MR) or Modified Two Man Rule (M2MR) mode and then monitoring the count of badge holders that enter and exit the area. This type of area control can be set up through the Areas form or an area event can be scheduled for a specific time through the Area Events form.

The standard Two Man Rule (2MR), when enabled, requires that at least two authorized badge holders occupy a controlled space at the same time. The Modified Two Man Rule (M2MR), when enabled, further restricts access to controlled areas based on specific M2MR category types. See *Table 124, Badge transactions for Occupancy Counting and Two Man Rule features* on page 363.

When using Occupancy Control with the Two Man Rule feature, the following restrictions apply:

- Occupancy Count must be enabled and the count must be zero in order to enable Two Man Rule.
- If Two Man Rule is enabled, Occupancy Count cannot be disabled. An error message will display and you will not be allowed to save the record.

If Standard Two Man Rule or Modified Two Man Rule is enabled and the occupancy count is greater than zero, Two Man Rule can be disabled, but you cannot switch to another Two Man Rule state. For example, if the area is set up as 2MR and the occupancy count is 2, you cannot change the area to M2MR with Door Control. Instead you must disable 2MR, reset the occupancy count to zero, and then enable M2MR with Door Control.

If desired, a digital output (DO) such as a blinking light can be activated on the reader following the first badge swipe, to alert the badge holder that a second badge swipe is required before access will be granted. This is an optional feature available by selecting 2MR Output from the Readers form.

Modified two man rule (M2MR)

The modified two man rule further restricts access to a controlled area based on the badge holders M2MR category type. Additionally, a Door Control option can be enforced which, after access has been granted to the first two badge holders, requires a door release button to be pressed before access is granted to any subsequent badge holders.

M2MR category type

There are three M2MR category types assigned through the Categories form:

- **None**
  Access to an M2MR controlled area will not be permitted while M2MR control is enabled. By default, any existing or new categories are assigned this category type.
- **Guest**
  A Guest is not allowed entry to an M2MR controlled area unless two (2) Team Members are already present in the area.
- **Team Member**
  If the M2MR controlled area is empty, a Team Member is allowed entry only with a second Team Member. Additional Team Members can enter individually after the initial two (2) Team Members are present in the M2MR controlled area. Furthermore, at least two (2) Team Members must be present until all Guests have exited.

Note: If the micro controlling an M2MR area resets, it will automatically reset the occupancy count to zero. Therefore, in the unlikely event that this occurs while the area is occupied, the system administrator must disable Two Man Rule, evacuate the area, and then reinstate M2MR.

Modified two man rule without door control

The first two badge holders to enter a controlled space must be Team Members and at least two Team Members must be present in the controlled space until all Guests have exited.

Modified two man rule with door control

The first two badge holders to enter a controlled space must be Team Members and at least two Team Members must be present in the controlled space until all Guests have exited. Additionally, before any subsequent badge holders are allowed entry, a Team Member within the controlled space must press a door release button. The door release button must be pressed within the time specified in the Door Release Timeout field on the Areas form or the door will not be unlocked.

A warning device, such as a horn or a strobe light, can be activated to notify the team members in an area that a person desiring access has presented a valid badge at the reader and is awaiting entry. A digital output (DO) point is configured to control the warning device through the Doors form, by selecting an M2MR output. When the warning device is triggered, team members in the area press the door release button before the door timeout has elapsed to cause the door to unlock and allow entry to the area.

How to set up a two man rule (2MR) controlled space

You need to complete the following forms to set up standard 2MR for an area:

- Reader form: To configure the area readers.
- Door form: To configure the doors in the area.
- Facility Profile form: To enable Occupancy Control.
- Area form: To enable Occupancy Counting and 2MR for the area.

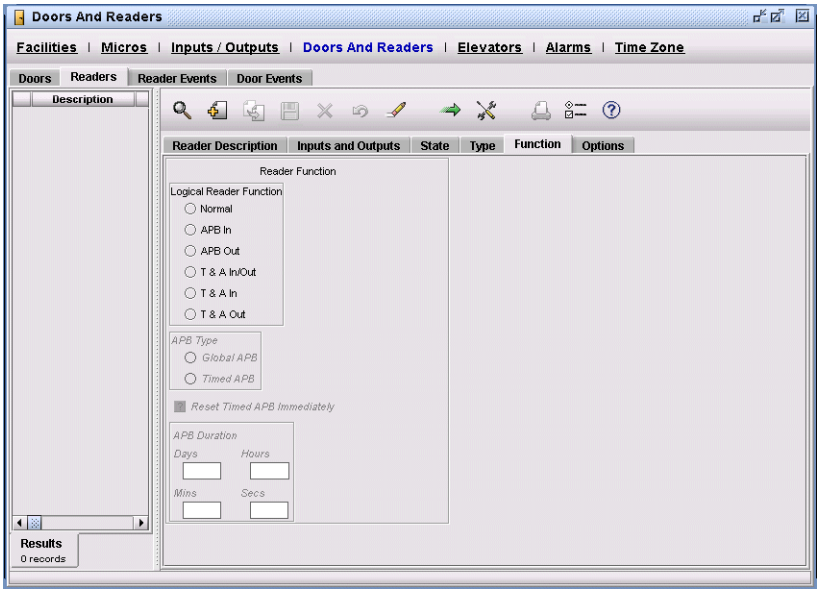
To set up the area readers:

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Readers** tab.
2. From the toolbar, click **Find** to locate the reader record you want to set up.
3. On the **Function** tab, under **Logical Reader Function**, enable the appropriate radio button: APB In, APB Out, T&A In, or T&A Out.

   Note: In an area with Occupancy Control enabled:

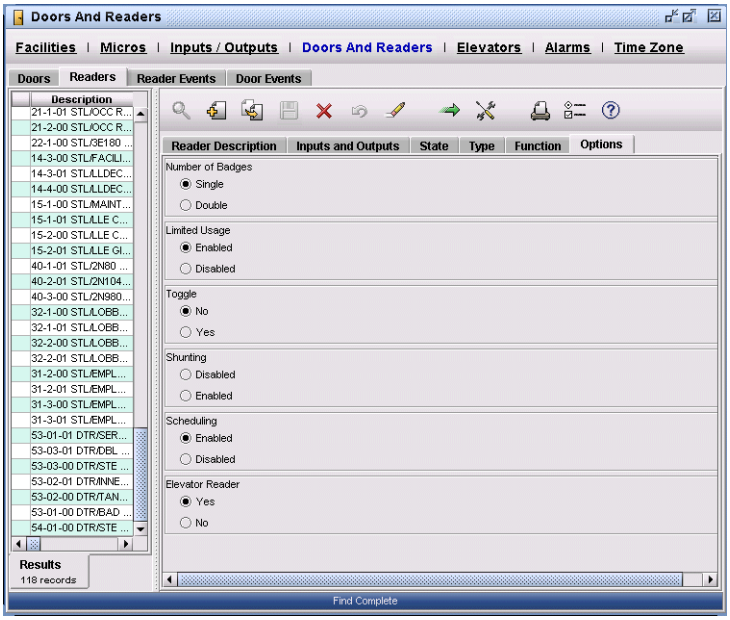
   - All readers in the area must be assigned one of these logical functions: APB In, APB Out, T&A In, or T&A Out.
   - APB readers must be set to Global. Timed APB is not allowed.
   - The logical reader function T&A In/Out is *not* allowed for any reader.

Figure 151.Readers form: Reader Function



4. On the **Reader Description** tab, under **Micro**, verify that all readers in the area are assigned to the same micro.
5. On the **Options** tab, under **Number of Badges**, verify that all readers are set to **Single**.

Figure 152.Readers form: Options



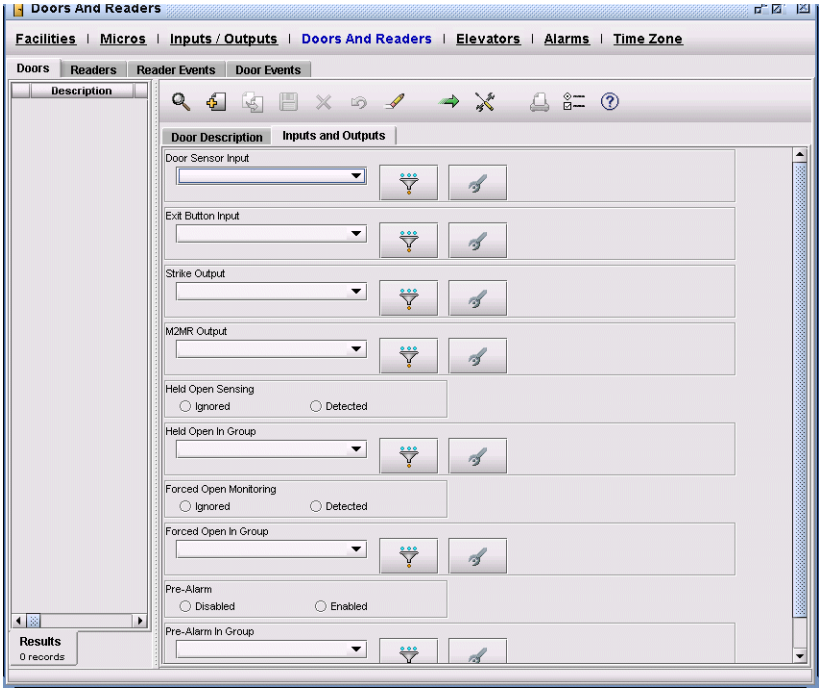
6. Optional: If you want to activate a DO (such as a blinking light) between the first and second required badge swipes, click Two Man Rule Output and select the output to be triggered.
7. **Save** and exit the Readers form.

To set up the area doors:

Note: The door sensor input and the door output must be physically connected to the same micro.

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. From the toolbar, click on **Find** to locate the door record you want to set up.
3. On the **Inputs and Outputs** tab, click **Door Sensor Input**.

Figure 153.Doors form: Inputs and Outputs

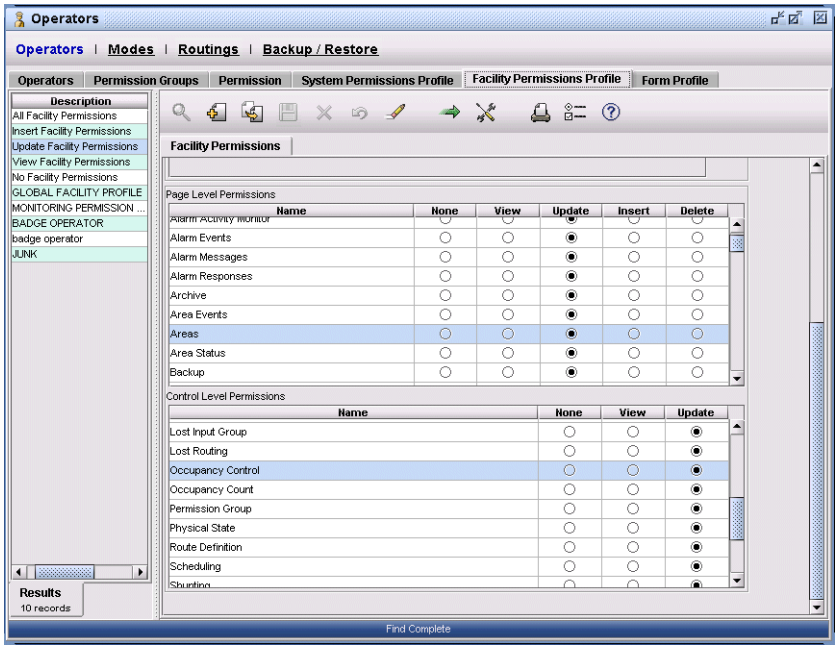


4. Select the appropriate input from the list displayed.
5. **Save** and exit the Door form.

To enable Occupancy Control:

1. From the **Control** menu, select **Operators**, and then click the **Facility Permissions Profile** tab.
2. From the toolbar, click on **Find** to locate the Facility Permission profile record you want to modify.
3. Under **Page Level Permissions**, click on **Areas** and make sure the level of permission is set to **Update**.
4. Under **Control Level Permissions**, click on **Occupancy Control** and make sure the level of permission is set to **Update**.

Figure 154.Facility Permissions Profile form



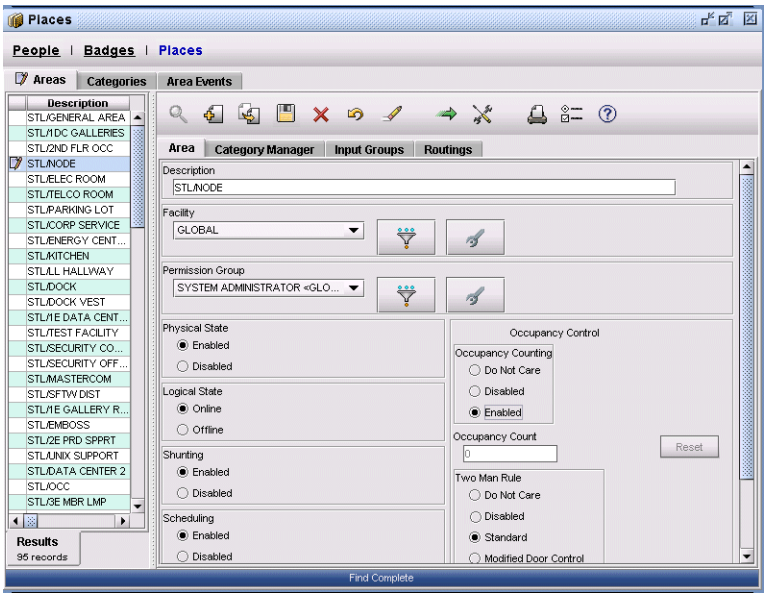
5. **Save** and exit the Facility Permissions Profile form.

To enable Occupancy Counting for the area:

Note: In order to perform this function, you must have Occupancy Control permission.

1. From the **Access** menu, select **Places**, and then click the **Area** tab.
2. From the toolbar, click on **Find** to locate the area record you want to set up.
3. On the **Area** tab, under **Occupancy Control**, enable the **Occupancy Counting** radio button.
4. Under **Two Man Rule**, enable the **Standard** radio button.

Figure 155.Area form: 2MR



5. **Save** and exit the Area form.

How to set up a modified two man rule (M2MR) controlled space with door control

You need to complete the following forms to set up M2MR with Door Control for an area:

- Reader form: To configure the area readers.
- Door form: To configure the doors in the area.
- Facility Profile form: To enable Occupancy Control.
- Area form: To enable Occupancy Counting, M2MR, and to assign M2MR Categories to the area.
- Category form: To define Categories for M2MR Category Types
- Personnel form: To assign M2MR Categories to Badge holders

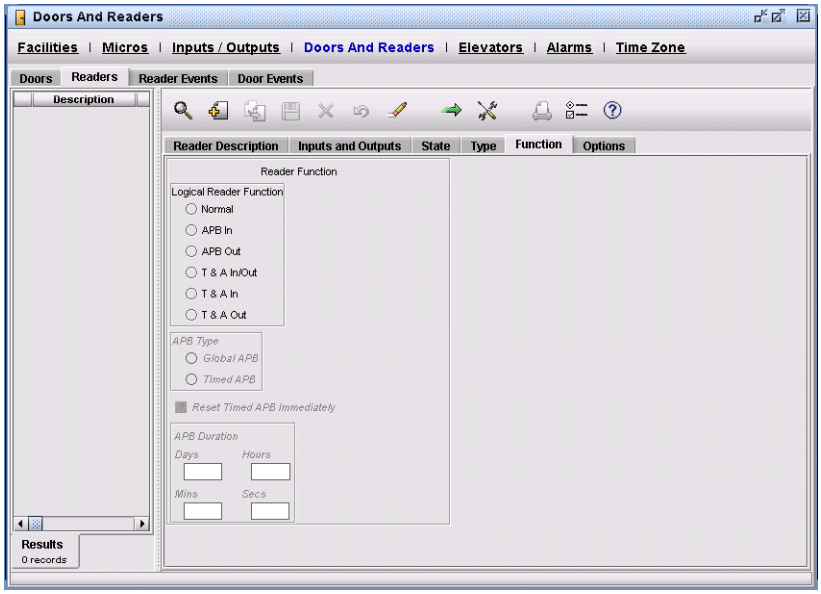
To set up the area readers:

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Readers** tab.
2. From the toolbar, click **Find** to locate the reader record you want to set up.
3. On the **Function** tab, under **Logical Reader Function**, enable the appropriate radio button: APB In, APB Out, T&A In, or T&A Out.

   Note: In an area with Occupancy Control enabled:

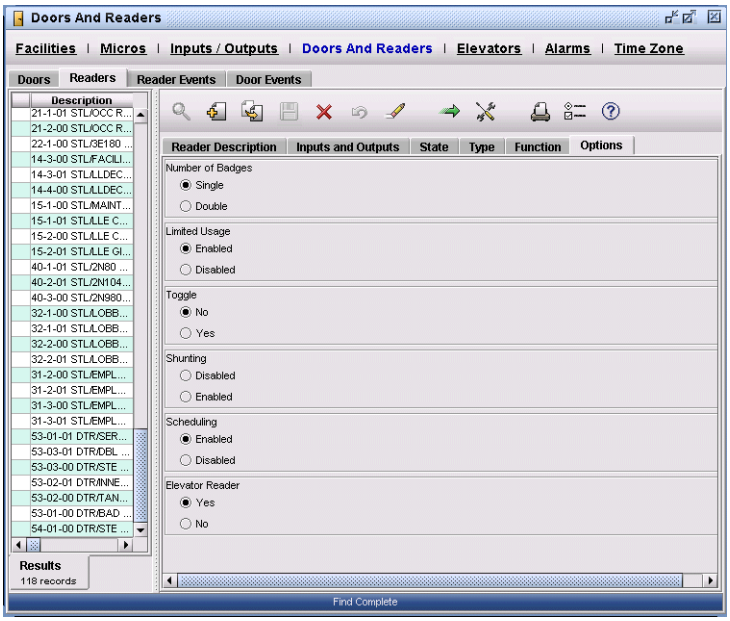
   - All readers in the area must be assigned one of these logical functions: APB In, APB Out, T&A In, or T&A Out.
   - APB readers must be set to Global. Timed APB is not allowed.
   - The logical reader function T&A In/Out is *not* allowed for any reader.

Figure 156.Readers form: Reader Function



4. On the **Reader Description** tab, under **Micro**, verify that all readers in the area are assigned to the same micro.
5. On the **Options** tab, under **Number of Badges**, verify that all readers are set to **Single**.

Figure 157.Readers form: Reader Control



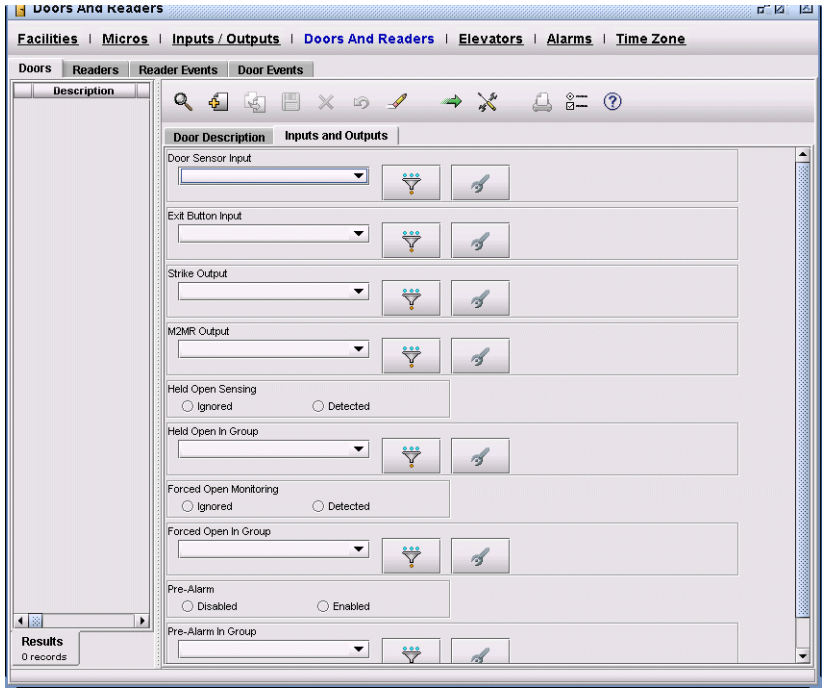
6. Optional: If you want to activate a DO (such as a blinking light) between the first and second required badge swipes, click Two Man Rule Output and select the output to be triggered.
7. **Save** and exit the Readers form.

To set up the area doors:

Note: The door sensor input and the door output must be physically connected to the same micro.

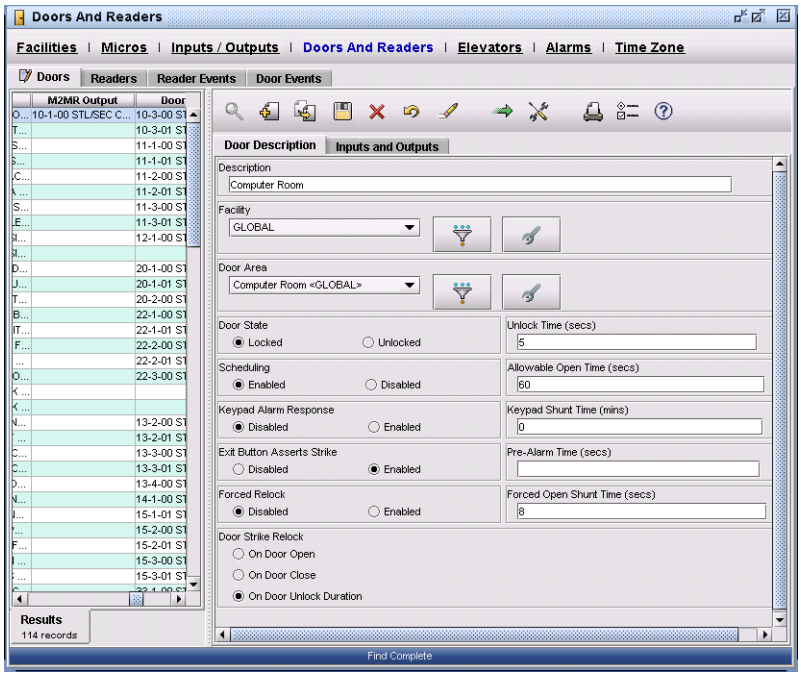
1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. From the toolbar, click **Find** to locate the door record you want to set up.
3. On the **Inputs and Outputs** tab, click **Door Sensor Input**.
4. Select the appropriate input from the list displayed.
5. Define an M2MR output on each door to the area that will be used for entry (APB IN or T&A IN). Click **M2MR Output** and select an output to associate with a warning device, such as a horn or strobe light.
6. Define an input as the exit button. Click **Exit Button Input** and select an input to associate with the exit button.

Figure 158.Doors form: M2MR



7. The input selected as the exit button input must be set to the following: On the Inputs form, under Input Control Setup, the **Input Enabled** button must be de-selected (the default).
8. Set **Exit Button Asserts Strike** to enabled.

Figure 159.Doors form: M2MR

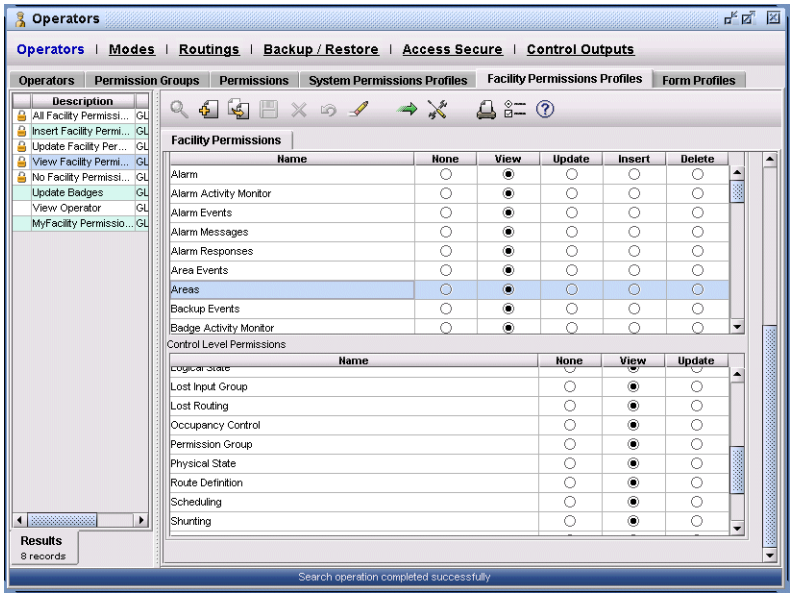


9. **Save** and exit the Door form.

To allow an operator to view Occupancy Control:

1. From the **Control** menu, select **Operators**, and then click the **Facility Permissions Profile** tab.
2. From the toolbar, click on **Find** to locate the Facility Permission profile record you want to modify.
3. Under **Page Level Permissions**, click on **Areas** and make sure the level of permission is set to **View**.
4. Under **Control Level Permissions**, click on **Occupancy Control** and make sure the level of permission is set to **View**.

Figure 160.Facility Permissions Profile form

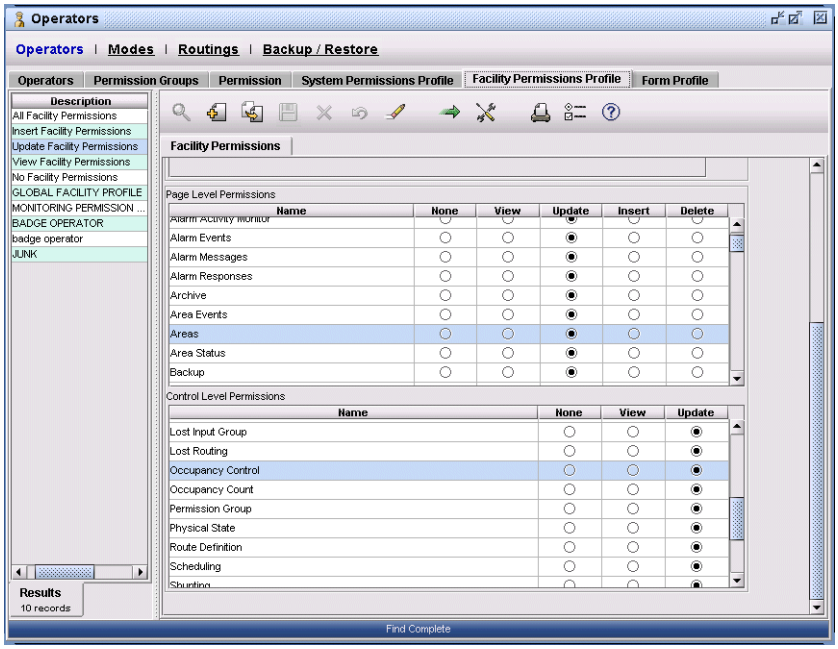


5. **Save** and exit the Facility Permissions Profile form.

To allow an operator to enable Occupancy Control:

1. From the **Control** menu, select **Operators**, and then click the **Facility Permissions Profile** tab.
2. From the toolbar, click on **Find** to locate the Facility Permission profile record you want to modify.
3. Under **Page Level Permissions**, click on **Areas** and make sure the level of permission is set to **Update**.
4. Under **Control Level Permissions**, click on **Occupancy Control** and make sure the level of permission is set to **Update**.

Figure 161.Facility Permissions Profile form



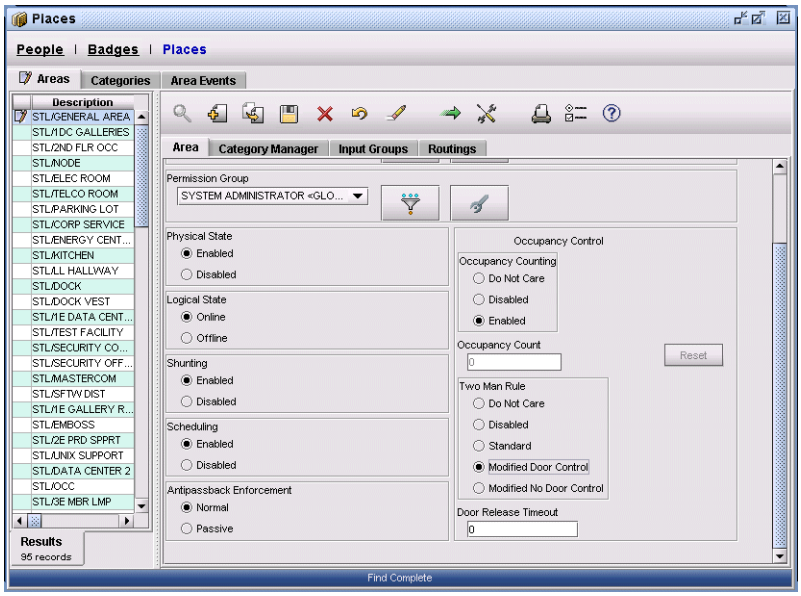
5. **Save** and exit the Facility Permissions Profile form.

To enable Occupancy Counting for the area:

Note: In order to perform this function, you must have Occupancy Control permission.

1. From the **Access** menu, select **Places**, and then click the **Area** tab.
2. From the toolbar, click **Find** to locate the area record you want to set up.
3. On the **Area** tab, under **Occupancy Control**, enable the **Occupancy Counting** radio button.
4. Under **Two Man Rule**, enable the **Modified Door Control** radio button.
5. Enter a value in the **Door Release Timeout** field.

Figure 162.Area form: M2MR

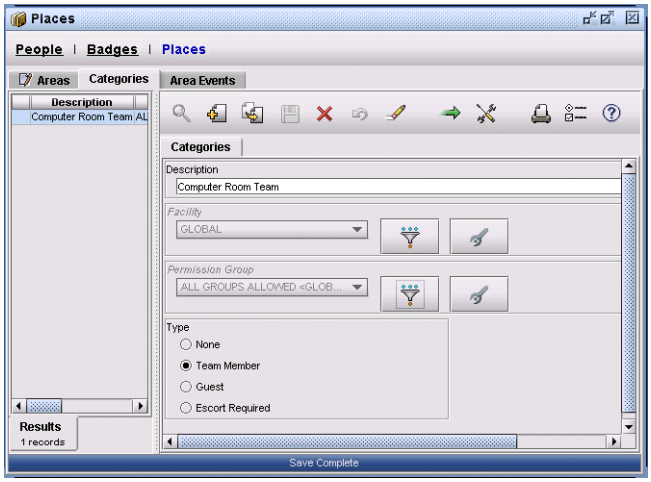


6. **Save** and exit the Area form.

To define categories for M2MR category types:

1. From the **Access** menu, select **Places**, and then click the **Categories** tab.
2. Click **New** .
3. Define one or more categories (groups of people) who will access the controlled area and, under **Type**, enable the appropriate radio button, **None**, **Guest**, or **Team Member**.

Figure 163.Categories form: M2MR

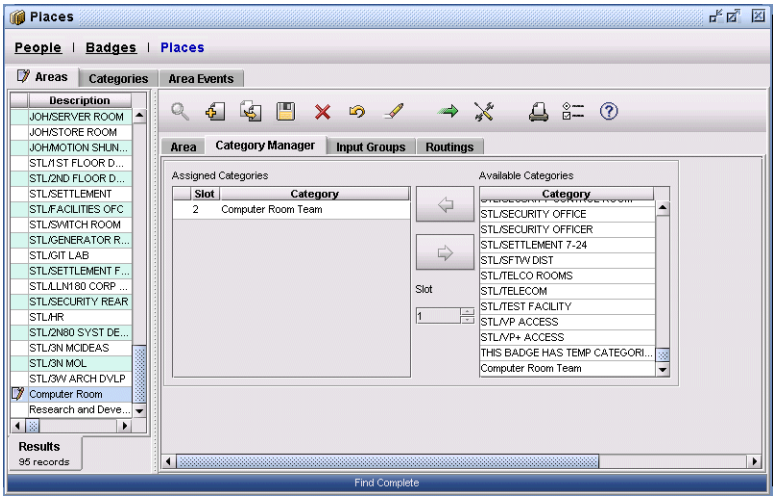


4. **Save** and exit the Category form.

To assign M2MR categories to areas and badge holders:

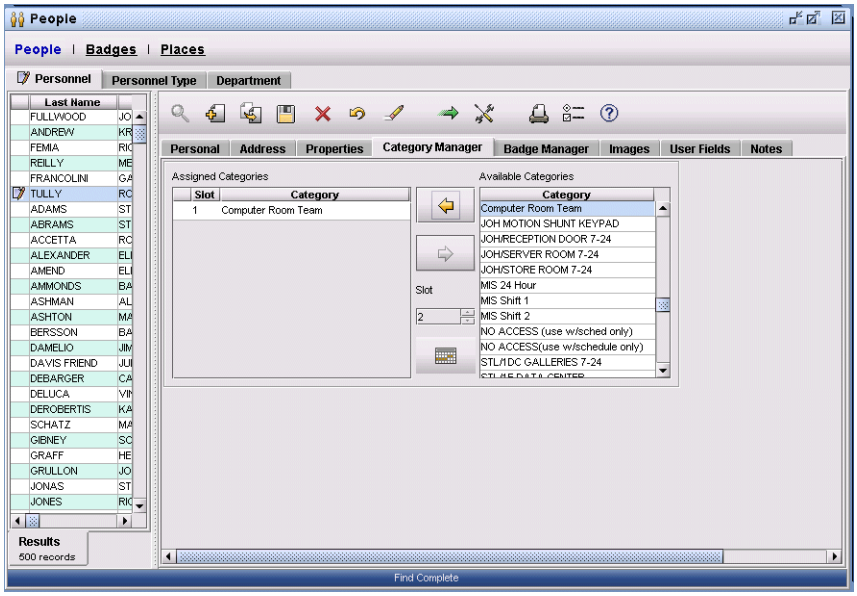
1. From the **Access** menu, select **Places**, and then click the **Areas** tab.
2. From the toolbar, click **Find** to locate the area record to be controlled.
3. Click the **Category Manager** tab and select an M2MR category from **Available Categories** and move it to **Assigned Categories**.

Figure 164.Area Form: M2MR Category



4. **Save** and exit the Area form.
5. From the **Access** menu, select **People**, and then click the **Personnel** tab.
6. From the toolbar, click **Find** to locate the Personnel records of the badge holders requiring access to the controlled area.
7. Click the **Category Manager** tab and select an M2MR category from **Available Categories** and move it to **Assigned Categories**.

Figure 165.Personnel form: M2MR Category



8. **Save** and exit the Personnel form.

How to set up a modified two man rule (M2MR) controlled space without door control

You need to complete the following forms to set up M2MR with Door Control for an area:

- Reader form: To configure the area readers.
- Door form: To configure the doors in the area.
- Facility Profile form: To enable Occupancy Control.
- Area form: To enable Occupancy Counting and to assign M2MR Categories to the area.
- Category form: To define Categories for M2MR Category Types.
- Personnel form: To assign M2MR Categories to badge holders.

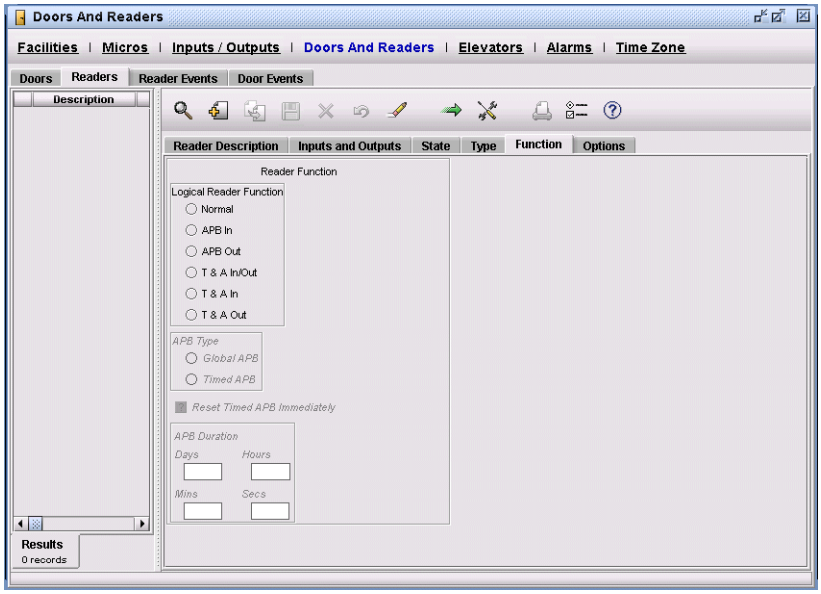
To set up the area readers:

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Readers** tab.
2. From the toolbar, click **Find** to locate the reader record you want to set up.
3. On the **Function** tab, under **Logical Reader Function**, enable the appropriate radio button: APB In, APB Out, T&A In, or T&A Out.

   Note: In an area with Occupancy Control enabled:

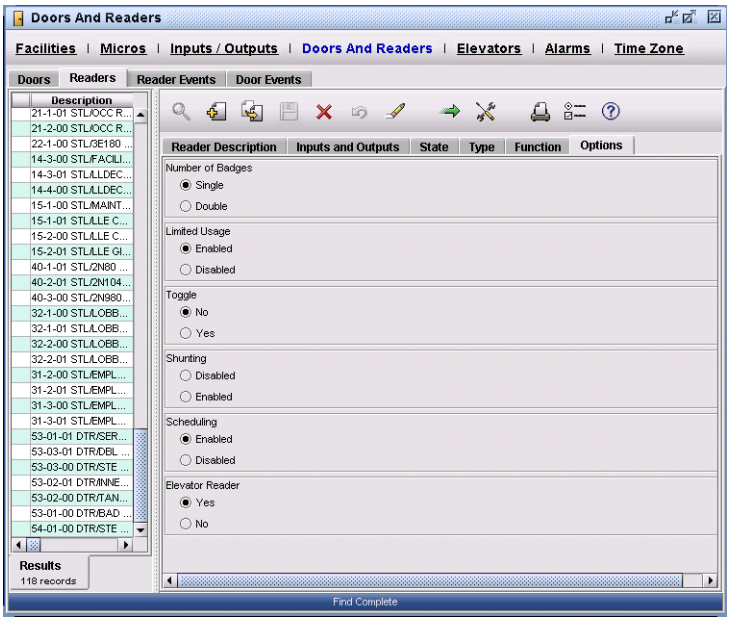
   - All readers in the area must be assigned one of these logical functions: APB In, APB Out, T&A In, or T&A Out.
   - APB readers must be set to Global. Timed APB is not allowed.
   - The logical reader function T&A In/Out is *not* allowed for any reader.

Figure 166.Readers form: Reader Function



4. On the **Reader Description** tab, under **Micro**, verify that all readers in the area are assigned to the same micro.
5. On the **Options** tab, under **Number of Badges**, verify that all readers are set to **Single**.

Figure 167.Readers form: Options



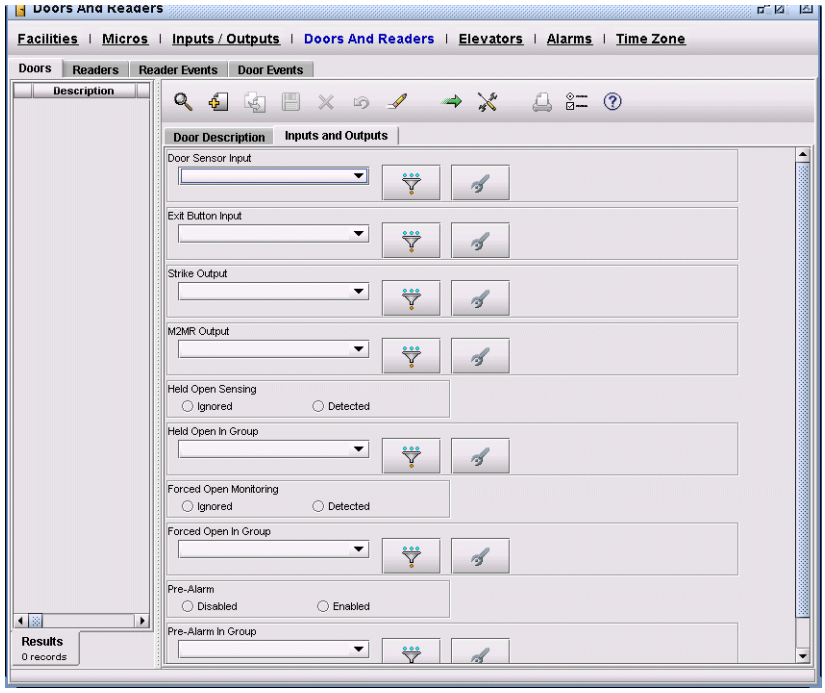
6. Optional: If you want to activate a DO (such as a blinking light) between the first and second required badge swipes, click Two Man Rule Output and select the output to be triggered.
7. **Save** and exit the Readers form.

To set up the area doors:

Note: The door sensor input and the door output must be physically connected to the same micro.

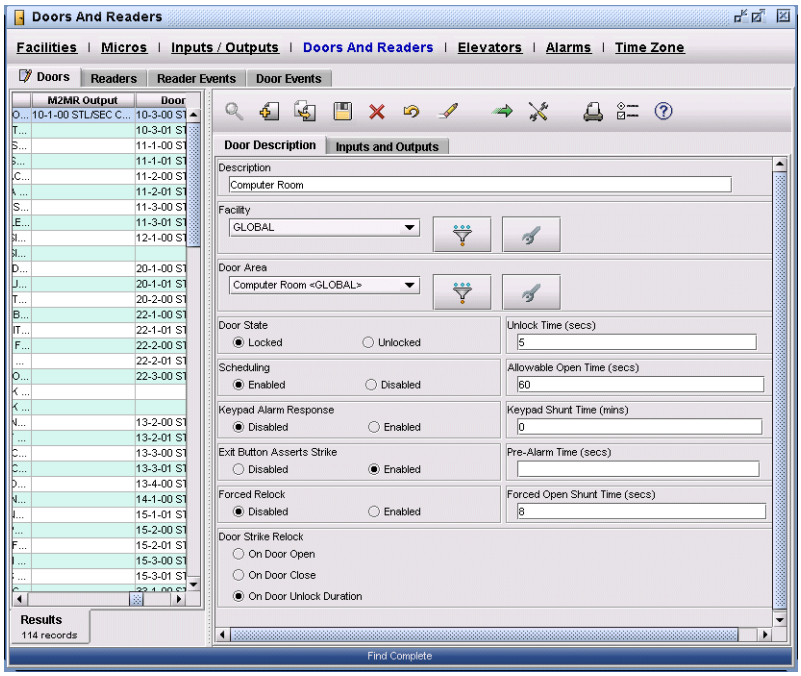
1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. From the toolbar, click **Find** to locate the door record you want to set up.
3. On the **Inputs and Outputs** tab, click **Door Sensor Input**.
4. Select the appropriate input from the list displayed.
5. Define an M2MR output on each door to the area that will be used for entry (APB IN or T&A IN). Click **M2MR Output** and select an output to associate with a warning device, such as a horn or strobe light.
6. Define an input as the exit button. Click **Exit Button Input** and select an input to associate with the exit button.

Figure 168.Doors form: M2MR



7. The input selected as the exit button input must be set to the following: On the Inputs form, under Input Control Setup, the **Input Enabled** button must be de-selected (the default).
8. Set **Exit Button Asserts Strike** to enabled.

Figure 169.Doors form: M2MR

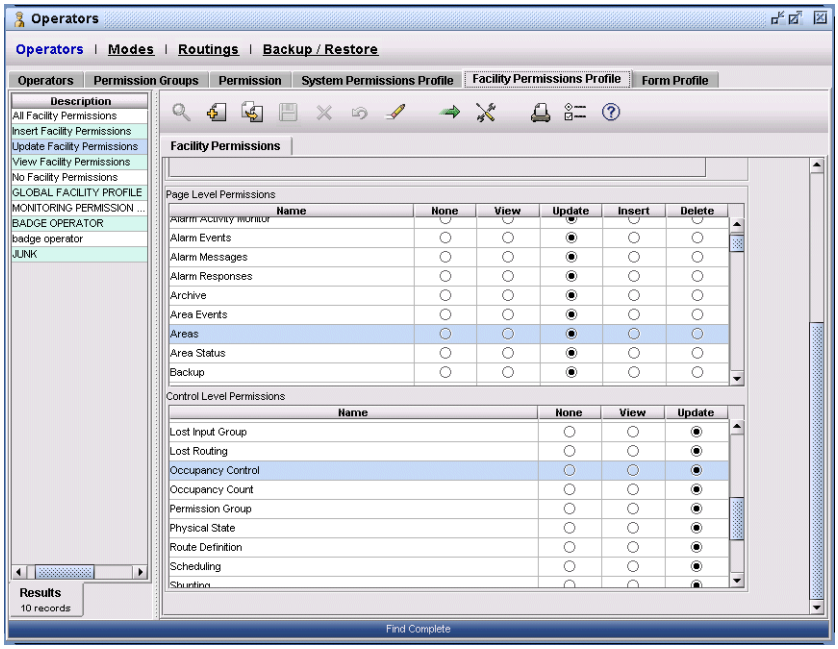


9. **Save** and exit the Door form.

To enable Occupancy Control:

1. From the **Control** menu, select **Operators**, and then click the **Facility Permissions Profile** tab.
2. From the toolbar, click on **Find** to locate the Facility Permission profile record you want to modify.
3. Under **Page Level Permissions**, click on **Areas** and make sure the level of permission is set to **Update**.
4. Under **Control Level Permissions**, click on **Occupancy Control** and make sure the level of permission is set to **Update**.

Figure 170.Facility Permissions Profile form



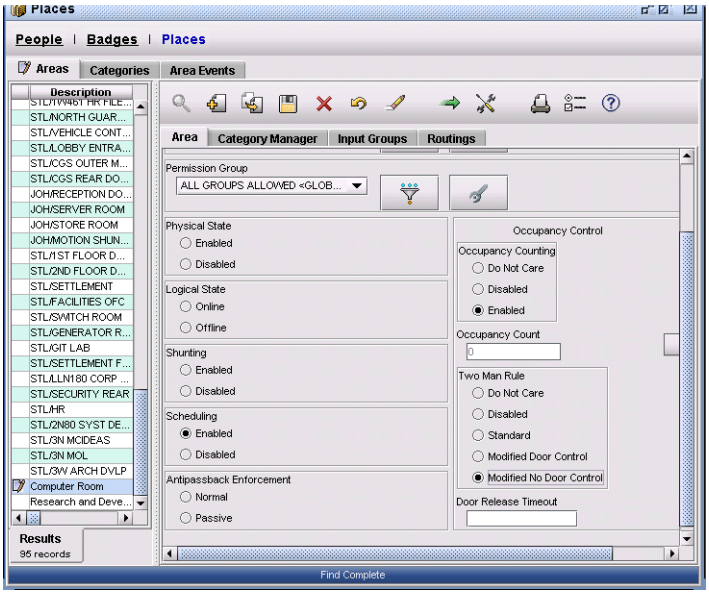
5. **Save** and exit the Facility Permissions Profile form.

To enable Occupancy Counting for the Area:

Note: In order to perform this function, you must have Occupancy Control permission.

1. From the **Access** menu, select **Places**, and then click the **Areas** tab.
2. From the toolbar, click **Find** to locate the area record you want to set up.
3. On the **Area** tab, under **Occupancy Control**, enable the **Occupancy Counting** radio button.
4. Under **Two Man Rule**, enable the **Modified** radio button.

Figure 171.Area form: M2MR without door control

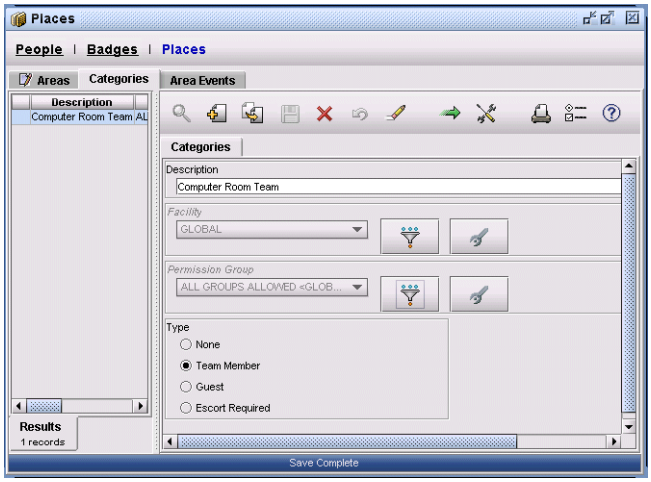


5. **Save** and exit the Area form.

To define categories for M2MR category types:

1. From the **Access** menu, select **Places**, and then click the **Categories** tab.
2. Click **New** .
3. Define one or more categories (groups of people) who will access the controlled area and, under **Type**, enable the appropriate radio button: **Guest**, or **Team Member**.

Figure 172.Categories form: M2MR

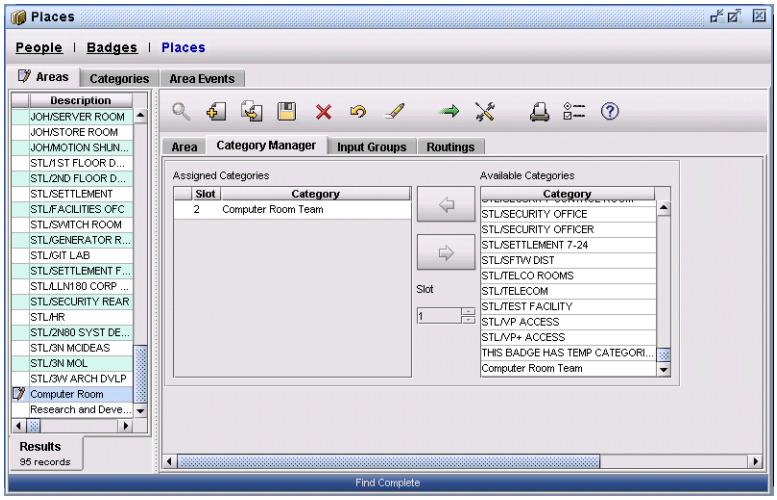


4. **Save** and exit the Category form.

To assign M2MR categories to areas and badge holders:

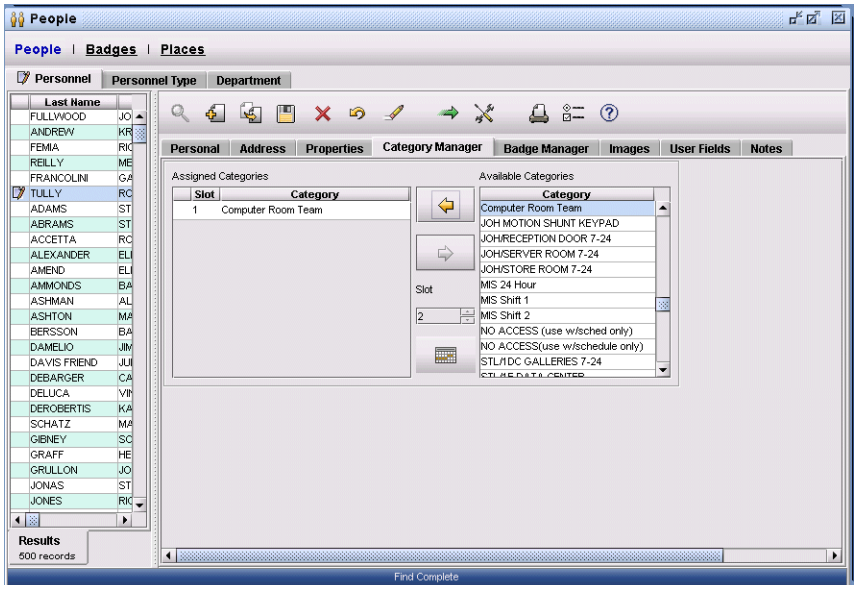
1. From the **Access** menu, select **Places**, and then click the **Areas** tab.
2. From the toolbar, click **Find** to locate the area record to be controlled.
3. Click the **Category Manager** tab and select an M2MR category from **Available Categories** and move it to **Assigned Categories**.

Figure 173.Area form: M2MR Category



4. **Save** and exit the Area form.
5. From the **Access** menu, select **People**, and then click the **Personnel** tab
6. From the toolbar, click **Find** to locate the Personnel records of the badge holders requiring access to the controlled area.
7. Click the **Category Manager** tab and select an M2MR category from **Available Categories** and move it to **Assigned Categories**.

Figure 174.Personnel form: M2MR Category



8. **Save** and exit the Personnel form.

Badge transactions for occupancy counting and 2MR

Table 124. Badge transactions for Occupancy Counting and Two Man Rule features

2MR mode	Badge event description	Badge transaction generated
DISABLED (Occupancy Counting is enabled)	Invalid badge swipe	Invalid badge
	Unknown badge swipe	Badge Unknown
	Valid badge swipe on IN reader; door is *not* opened	Valid no passage
	Valid badge swipe on IN reader; door *is* opened	APB/T&A IN, occupancy count incremented by one
	Valid badge swipe on OUT reader; door is *not* opened	Valid no passage
	Valid badge swipe on OUT reader; door *is* opened	APB/T&A OUT, occupancy count decremented by one
STANDARD 2MR	Invalid badge swipe	Invalid badge
	Unknown badge swipe	Badge Unknown
	Two valid badge swipes on IN reader when room is empty, within specified reader interval time; door is *not* opened	Valid no passage
	Two valid badge swipes on IN reader when room is empty, within specified reader interval time; door IS opened	Two APB/T&A IN, occupancy count incremented by two (to two)

Table 124. Badge transactions for Occupancy Counting and Two Man Rule features (continued)

2MR mode	Badge event description	Badge transaction generated
	Two badge swipes on IN reader when room is empty, but second swipe is not within specified reader interval time	NO Transaction
	Two badge swipes on IN reader when room is empty, but second badge is invalid	Valid door locked
	Two badge swipes on IN reader when room is empty, but second badge does not have a valid category	Valid Door Locked and No Categ Match
	Two badge swipes on IN reader when room is empty, but first badge does not have a valid category and second badge is valid	No Categ Match and Not Validated
	One valid badge swipe on IN reader when occupancy count is at least two, door is *not* opened	Valid no passage
	One valid badge swipe on IN reader when occupancy count is at least two, door IS opened	One APB/T&A IN, occupancy count incremented by one
	One valid badge swipe on OUT reader when occupancy count is at least three; door is *not* opened	Valid no passage
	One valid badge swipe on OUT reader when occupancy count is at least three; door IS opened	One APB/T&A OUT, occupancy count decremented by one
	Two valid badge swipes on OUT reader when occupancy count is two, within specified reader interval time; door is *not* opened	Valid no passage
	Two valid badge swipes on OUT reader when occupancy count is two, within specified reader interval time; door IS opened	Two APB/T&A OUT, occupancy count decremented by two (to zero)
	Two valid badge swipes on OUT reader when occupancy count is two, but second swipe is not within specified reader interval time	NO Transaction
MODIFIED 2MR NOTE: Door *not* opened case includes door release not pressed within specified time interval.	Invalid badge swipe	Invalid badge
	Unknown badge swipe	Badge Unknown
	Two valid badge swipes on IN reader when room is empty, within specified reader interval time, M2MR category type *not* Team Member and is Valid GUEST	Two Valid door locked
	Two badge swipes on IN reader when room is empty, within specified reader interval time, but second badge category type id *not* valid (not on area)	Valid door locked and No Categ Match

Table 124. Badge transactions for Occupancy Counting and Two Man Rule features (continued)

2MR mode	Badge event description	Badge transaction generated
	Two badge swipes on IN reader when room is empty, within specified reader interval time, but first badge category type id is *not* valid (not on area)	No Categ Match and Not Validated
	Two valid badge swipes on IN reader when room is empty, within specified reader interval time, M2MR category type IS Team Member; door is *not* opened	Valid no passage
	Two valid badge swipes on IN reader when room is empty, within specified reader interval time, M2MR category type IS Team Member; door is opened	Two APB/T&A IN, occupancy count incremented by two (to two)
	Two valid badge swipes on IN reader when room is empty, but second swipe is not within specified interval time, M2MR category type is Team Member	NO Transaction
	One valid badge swipe on IN reader when occupancy count is at least two, M2MR category type NOT None; door is *not* opened	Valid no passage
	One valid badge swipe on IN reader when occupancy count is at least two, M2MR category type NOT None; door *is* opened	One APB/T&A IN, occupancy count incremented by one
	One valid badge swipe on IN reader when occupancy count is at least two, M2MR category type is None but valid (on area)	Valid door locked
	One valid badge swipe on IN reader when occupancy count is at least two, M2MR category type is None and category not on area	No Categ Match
	One valid badge swipe on OUT reader when occupancy count is at least three and there would *not* be two Team Members left in the room	Valid door locked
	One valid badge swipe on OUT reader when occupancy count is at least three and there would be two Team Members left in the room; door is *not* opened	Valid no passage
	One valid badge swipe on OUT reader when occupancy count is at least three and there would be two Team Members left in the room; door is opened	One APB/T&A OUT, occupancy count decremented by one
	Two valid badge swipes on OUT reader when occupancy count is two, within specified reader interval time; door is *not* opened	Valid no passage
	Two valid badge swipes on OUT reader when occupancy count is two, within specified reader interval time; door is opened	Two APB/T&A OUT, occupancy count decremented by two (to zero)
	Two valid badge swipes on OUT reader when occupancy count is two, but second swipe is not within specified reader interval time	NO Transaction

Seed counter

The seed counter option provides a way to:

- Automatically generate a unique Id number for each badge.
- Automatically generate the badge Id (BID) number for each badge (optional).
- Keep count of the number of badges a person has been issued.
- Keep count of the number of times a person's badge has been printed.

In order to use this feature, the seed counter feature must be selected at the time of **base** installation. The base installation will ask you a series of questions to help you set up the seed counter options. The setup can only be done at installation. For more information, refer to the Picture Perfect 4.5 Installation Manual. Changing the option settings later can cause difficulties.

If enabled, three new fields will appear on the Badges form: Reissue Count, Reprint Count, and Unique Id.

Reissue count

Every time a badge is issued to a person this incremental number is stored to the badge. This field shows the issue number of this badge and the total number of badge issues for the badgeholder to whom this badge is assigned, for example *3 of 5*. If a badge has not been assigned to a person, the Reissue Count is 00. The maximum number of badge issues allowed is 99. This field is view only - you can perform a search, but it cannot be edited.

Reprint count

This is the number of times the badge has been printed. A new badge will set the Reprint Count to 00. Anytime the badge is printed or previewed, the badge will increment the number, storing it to the badge. The Reprint Count is tracked a maximum of 99 times. This field is view only - you can perform a search, but it cannot be edited.

Unique Id

The seed counter assigns a unique number to each badge. It is a global counter that is incremented each time a new badge is created. The range is determined by the number of digits allocated to the counter. This field is view only - you can perform a search, but it cannot be edited.

Double-badge function

This feature provides double-badge control for access to high security areas. Operator-defined readers will require two badges or two badges with PINs to be presented before a door strike is activated.

Access through double-transaction readers is granted only when two complete, valid, and distinct transactions are presented to the reader. "Complete" means that both transactions have all necessary information. "Valid"

means that both transactions are recognized by the reader. “Distinct” means that both transactions are individually distinguishable (a single badge cannot be used twice to complete a double-badge transaction).

- Badge-only readers need two distinct badges.
- Keypad-only readers need two distinct badge-encode numbers.
- Badge-and-keypad readers need two complete badge-and-keypad transactions. The first reader activity may be a shunt code or an alarm response code entered on the keypad. This first activity is optional. Next must come the presentation of a badge to the reader. Following that, a PIN or duress code must be entered on the keypad. The two transactions must have different badges, but they may use the same PIN or duress code. The required order for a badge-and-keypad reader transaction is outlined below:

  a. Shunt or Alarm Response code

  b. Badge swipe

  c. PIN or Duress code

  Note: On badge-and-keypad readers, shunt codes, duress codes, and alarm responses may be entered by either or both transactions. For example, the first transaction may shunt the reader’s door while the second transaction responds to an alarm on that door.

The separate transactions comprising a double transaction may use the same or different categories while gaining access through the reader.

Each double-badge reader must have an Interval Time defined on the Devices/Doors/Reader form. This specifies the number of seconds allowed between stages of the transaction. If, during the processing of a transaction, there is no reader activity for the specified interval-time period, the transaction “times out” and is considered at an end. The next reader activity will be considered the start of a new transaction. “Time outs” are not reported to users.

Double-badge reporting

All reader transactions are tracked by two separate reports, one for each component transaction. These reports are presented in the Badge Monitor and/or Badge History.

Each transaction reports whether it is the first or second activity on a single- or double-transaction reader. When both transactions are valid, each transaction reports that access was granted. When both transactions fail, each transaction reports its individual reason for failure. When only one transaction fails, it reports its reason for failure while the other reports that it was valid but did not gain access. It is possible to detect the one component transaction's failure before the other component transaction has been completely validated. In this case, the other component transaction will report that it was not completely validated.

All transaction reports include a time stamp. It shows the time at which the access decision was made, not when the transaction started. Since a double-transaction's access decision is made when both component transactions are complete, both transactions will report the same time stamp.

Double-badge configuration

To configure a reader for double-badge function, set the **Number Of Badges** field on the Readers form to **Double**. All readers can be configured to require one or two transactions for granting access. In addition, the **Interval Time** field on this form must be completed. The interval time specifies the number of seconds allowed between stages of the transaction. (See *Chapter 9 Area management* for details on the Readers form.)

The double-badge configuration can also be changed by scheduling. This is done by setting the **Number Of Badges** field on the Reader Events form. (See *Chapter 10 Schedules and modes* for details on the Reader Events form.)

A change to the definition will be reflected in a micro's local database. The only micro affected by any change to a reader's Number-of-Badges definition is the one which is physically connected to the reader.

A change in the micro's local database does not affect any on-going reader activity. In other words, changing a reader from double-transaction to single-transaction while the micro is processing the reader's activity does not affect that process; two complete valid transactions are still needed before access may be granted. After the two transactions are processed, the micro will grant or deny access based on a single transaction.

A reader's Number-of-Badges definition is not limited by the reader's physical or logical type. For example, it is possible to define a double-transaction, badge-and-keypad, anti-passback-in reader.

Reader status requests will display the reader's current Number-of-Badges definition.

Elevator control

Elevator Control allows you to control access to floors serviced by an elevator. This feature works only with the Micro/5, M/PX-2000, and M/PXN-2000 micro controllers. It allows the micro to control multiple elevator readers, DI's and DO's. This section shows how to implement the Elevator Control feature using any one of the following methods:

- Elevator Micro/DO Configuration
- Elevator Reader/DO Configuration
- Elevator Reader/DI/DO Configuration

System configuration standards

- Elevator Control is a part of the **base** Picture Perfect software package.
- Elevator Control is implemented on Micro/5, M/PX-2000, or M/PXN-2000 configurations only.
- A maximum of 64 floors can be serviced by one elevator.
- 128 separate, user-configurable elevator categories are supported per elevator.
- The elevator buttons are enabled for a length of time (duration) defined on the Outputs form. All the buttons (outputs) should be set to the same duration.
- Badges must be authorized for an elevator reader in order to gain access to an assigned floor.
- Picture Perfect can address up to 4096 micros with each micro having up to a maximum of 16 elevator readers. The recommended limit is based on memory and disk capacity of the Picture Perfect host system.

Elevator access

There are two ways to grant access to an elevator floor. Both require a valid badge swipe to an elevator configured reader and a valid category match between the badge and a floor or floors. Depending on the elevator control configuration, one of the following methods will then activate the elevator floors.

Method 1

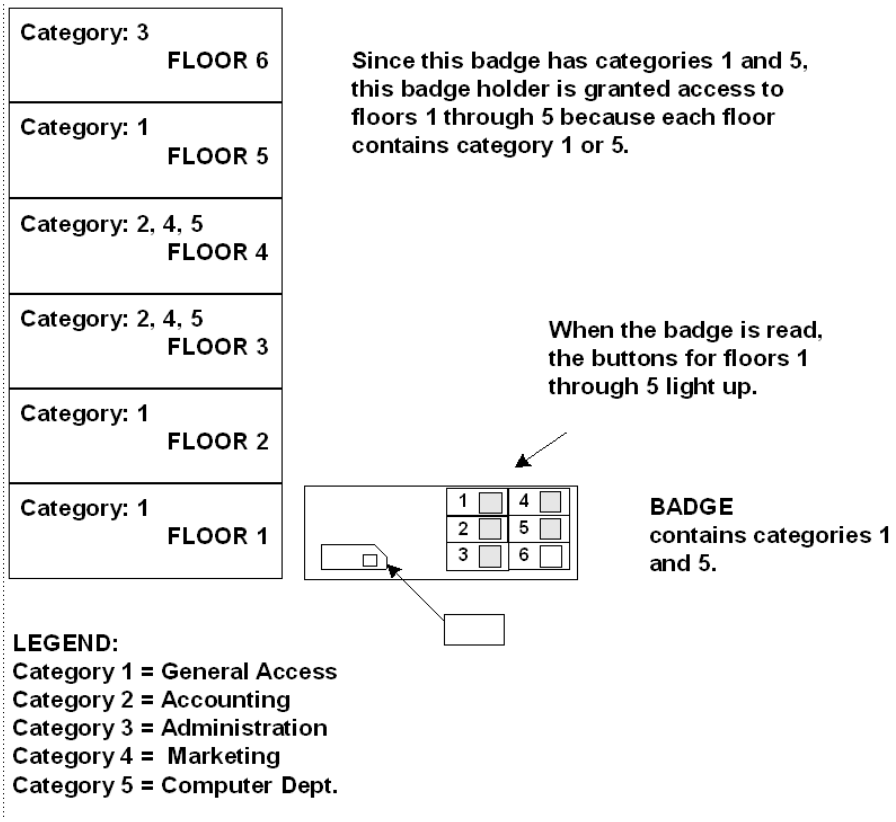
This is the default and is available on all configurations.

Following a valid badge swipe, the badge is checked for category floors for this elevator. For each badge category that matches the elevator's categories, access is granted to the set of floors denoted by the matched category. Therefore, the set of accessible floors will be the combined set of matched category floors.

For example, a badge holder has General Access and Computer Department as categories on their badge. The elevator allows floors 1, 2, and 5 for General Access, and floors 3 and 4 for Computer Department. Therefore, when this badge holder enters the elevator, floors 1 through 5 will be activated. Refer to *Figure 175*.

For a double-badge transaction configuration, each badge must first have access to the reader, then the same access validation as above takes place. The difference is that the final set of accessible floors will be denoted by the union of the two badges' matched categories (which correspond to floors). In other words, if the elevator category matches a category found on either badge, access is granted. See *Double-badge function* on page 366.

Figure 175.Example of Elevator Control - Method 1



Method 2

When enabled, this method is available on the following elevator configurations:

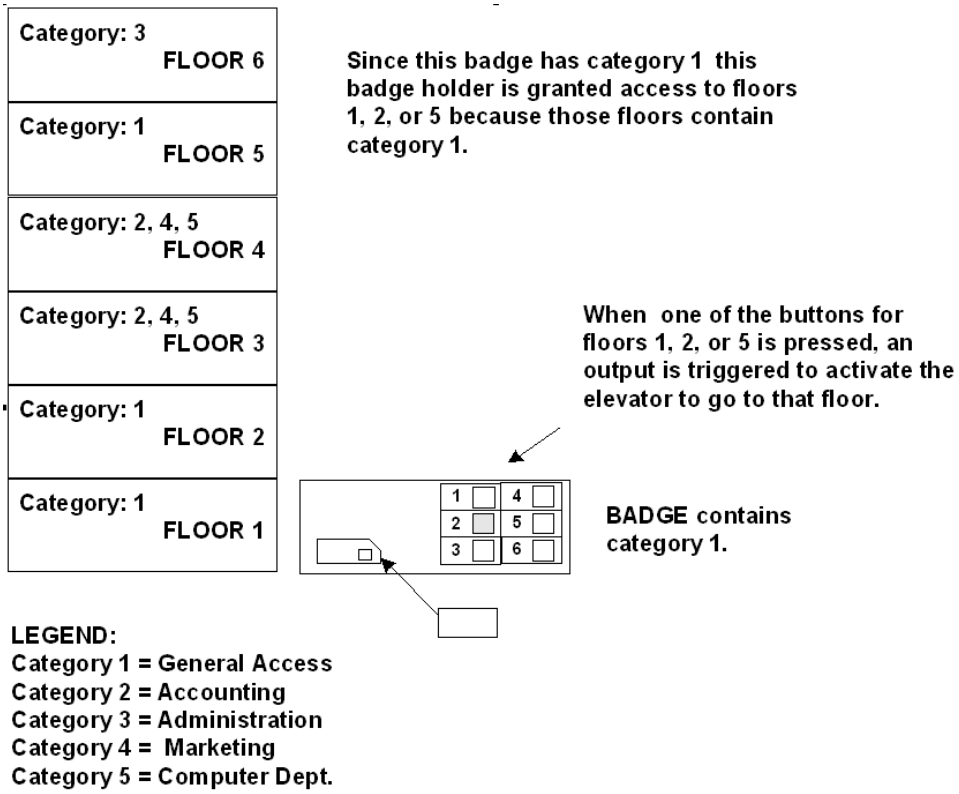
- Reader/DI/DO - See *To set up Example 2 in a Reader/DI/DO configuration:* on page 377.

  Following a valid badge swipe, a floor button (DI) is used to enter a floor number. A category match must exist between the floor selected and the badge before the DO (digital output) is fired to activate the elevator. This method will generate a floor transaction, valid or invalid, which is stored, along with the floor selected, and can be used for history and reporting purposes.

  For example, a badge holder has General Access as the sole category on their badge. The elevator allows floors 1, 2, and 5 for General Access, and floors 3 and 4 for Computer Department. Therefore, when this badge holder enters the elevator and pushes floor buttons 1, 2 or 5, the elevator will be activated and a Valid floor transaction will be generated. Entering numbers 3 or 4 would return an Invalid floor transaction and no access would be granted. Refer to *Figure 176*.

  For a double-badge transaction configuration, each badge must first have access to the reader, then the same access validation as above takes place. The difference is that the final set of accessible floors will be denoted by the union of the two badges' matched categories (which correspond to floors). In other words, if the elevator category matches a category found on either badge, access is granted. See *Double-badge function* on page 366.

Figure 176.Example of Elevator Control - Method 2



Method 1

During the period of time when the elevator's digital outputs are active (buttons are lit), any number of those buttons may be selected. The amount of time that the elevator buttons are active, after a valid badge swipe, is set using the Outputs form. The same duration time should be used for all digital outputs assigned to floors.

Method 2

During a set period of time, a button may be selected. This amount of time in which the entry is accepted, after a valid badge swipe, is set using the Outputs form. The same duration time should be used for all digital outputs.

Elevator access for all categories

A badge that has the All Categories category assigned to it will be allowed access to all floors defined for the elevator, regardless of whether the All Categories category is present on the area.

Free access floors

There are two methods of allowing free access to particular elevator floors. One method requires a badge swipe; the other does not need a badge at all.

Free access for all badges

Free access for all badges allows any badge that has access to the elevator reader to have free access to designated floors. The “wild-card” category is used as an elevator category on the Category Floors form to designate which floors are free access.

To set up a wild-card category, you must select All Categories from the Category list box, and assign the free-access floors to it. This allows a badge holder to gain access to the free-access floors, as long as the badge is authorized for the elevator reader.

Free access without a badge

The free access without a badge method allows anyone to walk onto an elevator and have free access to designated floors (without using a badge in any way). For this method to work, you must configure a Door State of “unlocked” for the door to each floor you want included, then associate a digital output to the door.

When this is in place, the free-access floor buttons will always be lit, regardless of a badge swipe. When a badge is swiped, access is given to all floors for which the badge is valid, along with the free-access floors. Free access without a badge can be scheduled as described in *Scheduling elevator free access* on page 379.

How to set up elevator control

To implement elevator control, follow these steps for each access-controlled elevator in the system:

1. Define the maximum number of floors you want to control using the System Parameters form. Depending on the configuration, this number is based either on a per elevator micro basis or is divided between all elevator readers on a micro.
2. Depending on the configuration, define a Micro/5 as an elevator micro on the Micros form, or define a Micro/5 as a normal micro and a reader on that micro as an elevator reader on the Readers form.
3. Define an output for each floor on the Output form.
4. For a Reader/DI/DO configuration, define an input for each floor on the Input form.
5. Define the type of elevator configuration, the number of floors for the elevator and assign an output (and an input in the case of a Reader/DI/DO configuration) to each floor on the Elevator form.
6. Define sets of floors for categories on the Category Floors form.

Defining the number of floors

Use the System Parameters form to specify the maximum number of elevator floors on a micro. This number could be per elevator (Micro/DO configuration) or it could be distributed between up to 16 elevators (Reader/DO or Reader/DI/DO configurations). The maximum number of floors serviced by a micro (elevator) is 64. See *Assigning system parameters* on page 40.

Defining micros

Required for: Micro/DO Configuration Only

Use the Micros form to define the micro type as an Elevator for each micro used with an elevator in the Picture Perfect system. See *Defining micros* on page 132.

Defining readers

Required for:

- Reader/DO Configuration
- Reader/DI/DO Configuration

Use the Reader form to define the reader type as Elevator for each reader used with an elevator in the Picture Perfect system. See *Defining readers* on page 182.

Defining outputs

Use the Output form to define a digital output for each elevator floor button. This output will light and activate the button for a floor to which access is allowed. For more information, see *Defining outputs* on page 158.

Keep the following in mind when defining elevator floor outputs:

- At least one 16-digital-output (16 DO/DOR) board must be configured with an elevator micro.
- The elevator digital-output addresses must be in the 16 to 31 range for each 16 DO/DOR board used.
- For a maximum configuration (64 floors), four 16 DO/DOR boards must be installed in a Micro/5.
- The duration time should be the same for all elevator digital outputs.

  Note: In a Reader/DI/DO configuration, make sure the Reader Interval Time does not exceed the Output (DO) Duration.

- Elevator digital outputs do not require output groups to be associated with them.

Defining inputs

Required for: Reader/DI/DO Configuration

Use the Input form to define a digital input for each elevator floor button. When this input is received by the micro, it performs a category match and if successful, activates the associated output for a floor to which access is allowed. For more information, see *Defining inputs* on page 161.

Keep the following in mind when defining elevator floor inputs:

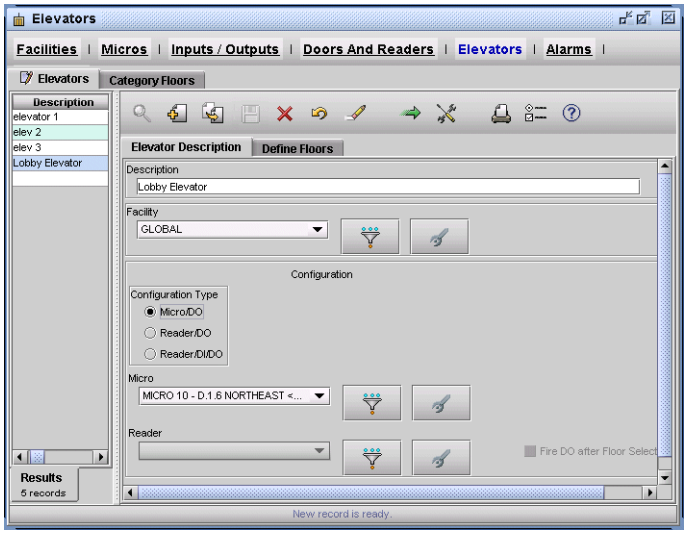
- Toggle the Elevator Point button to On to make this input an elevator input.
- At least one 20DI board must be configured with an elevator configured to have the Reader/DI/DO configuration.
- For a maximum configuration (39 floors), an 8RP reader configured to be an elevator reader, two 20DI boards and two 16DO boards must be installed in a Micro/5.
- Elevator DI’s do not require an input group to be associated with them.

The Elevators form

Use the Elevators form to select the type of elevator configuration, define the number of floors, assign the elevator to a previously defined elevator micro or reader and then tie previously defined outputs (and inputs in

the case of Reader/DI/DO configurations) to the corresponding floors. Perform this setup for each of the access-controlled elevators in your facility.

Figure 177.Elevator Form



Fields and controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

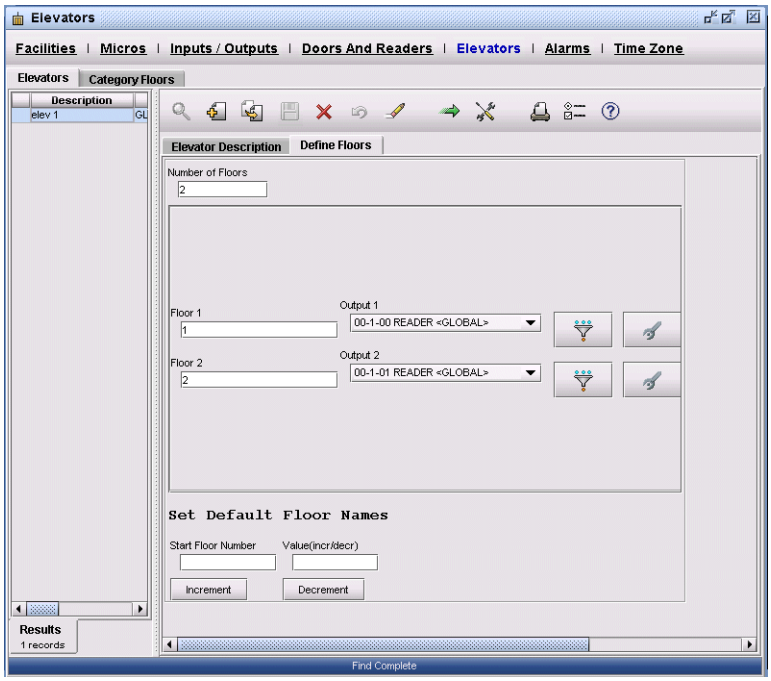
Table 125. Elevators form fields

Field name	Description
Description	Type any alphanumeric combination to describe the elevator (up to 60 alphanumeric characters). *Example: Lobby, East Wing 1, West Wing 3*
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Configuration Type	Select one of the following types: • Micro/DO - See *To set up Example 2 in a Micro/DO configuration:* on page 377. • Reader/DO - See *To set up Example 2 Reader/DO configuration:* on page 377. • Reader/DI/DO - See *To set up Example 2 in a Reader/DI/DO configuration:* on page 377.
Micro	When using the Micro/DO configuration type, click to select a micro from the list box. If multiple readers are configured on an elevator micro, the first reader controls the elevator.
Reader	When using the Reader/DO or the Reader/DI/DO configuration type, click to select a reader from the list box.
Fire DO after Floor Selection	When using the Reader/DI/DO configuration type, select the Fire DO after Floor Selection to enable Elevator Access Method 2 in which, after a valid badge read, a floor has to be selected and if it is an accessible floor, the DO will be activated. Otherwise, the default Method 1 in which, after a valid badge read, the DOs for all accessible floors are activated, will be employed.

Table 125. Elevators form fields (continued)

Field name	Description
Define Floors	Click Define Floors to specify the number of floors, which in turn will determine how many floor buttons will display for that elevator on the screen.
Number of Floors	An entry is required in this field for the Floor label, input and output controls to be displayed. If no entry is made an error message will display when the record is saved. Valid entries are based on the type of elevator configuration chosen and the number of floors on other elevators on the same micro. Micro/DO: Maximum 64 floors, only one elevator per micro. Reader/DO: Maximum 64 floors, distributed among the elevators defined for that micro. Reader/DI/DO: Maximum 39 floors, distributed among the elevators defined for that micro. **Note:** The "real" maximum number of floors allowed is defined on the System Parameters form.
Floor Labels	The default floor labels are Floor 1 through Floor x, where x=the maximum number of floors. There are two ways to edit the floor labels. See *How to edit floor labels* on page 376.

Figure 178.Define Floors Window



How to edit floor labels

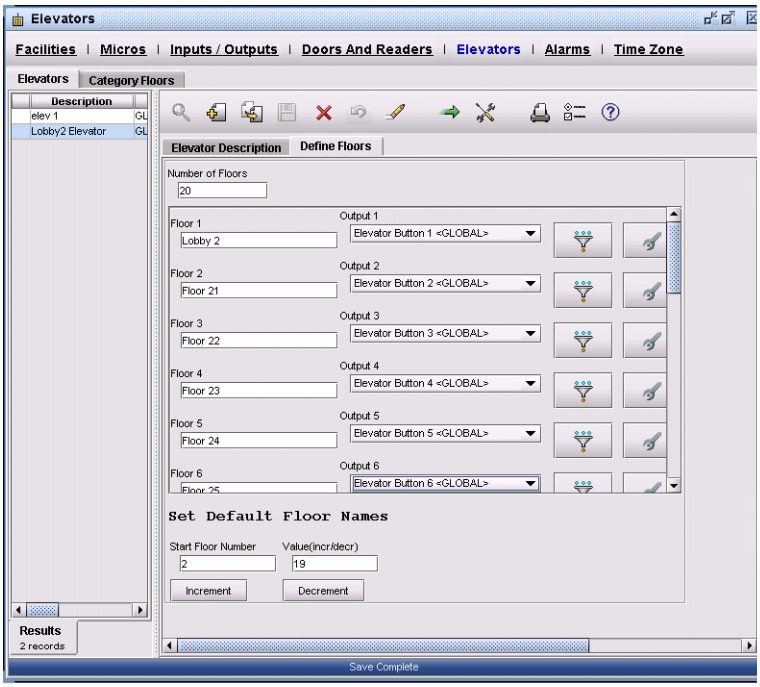
The default floor labels are Floor 1 through Floor x, where x=the maximum number of floors. There are two ways to edit the floor labels:

1. Type directly in the text box.
2. Specify a starting floor number and an Increment/Decrement value. The default is 0. Click the Increment or Decrement buttons to set default floor labels.

Example 1: Set up an elevator that will only access floors 20 through 40, and the name of floor 20 is Lobby 2:

Figure 179.Example of Increment Floors

1. Type in description: Lobby 2 in Floor 1.
2. Enter Start Floor Number: 2
3. Enter Increment Value: 19
4. Click Increment. This will result in Floor 2 displaying a description of Floor 21 (19 + 2), Floor 3 will display as Floor 22, and so on.



To reset the default floor labels (Floor 1....Floor n, corresponding to floors 1...n):

1. Enter "1" as the **Starting Floor Number**.
2. Enter "0" or blank as the **Increment** or **Decrement** value.
3. Click **Increment**.

Example 2: Set up an elevator that will access 64 floors described as Basement, Parking, Lobby and Floor 2 through Floor 62:

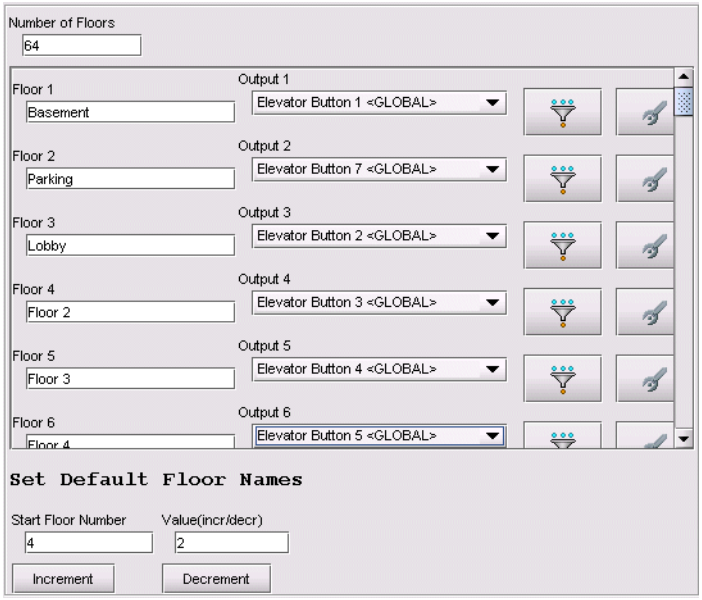
Figure 180.Example of Decrement Floors

1.Type in descriptions: Basement, Parking, Lobby

2. Enter Starting Floor number as "4".

3. Enter Decrement Value as "2".

4. Click Decrement. This will result in Floor 4 displaying a description of Floor 2 (4-2), Floor 5 will display as Floor 3, and so on.



To set up Example 2 in a Micro/DO configuration:

1. In **Configuration Type**, select **Micro/DO**.
2. Click the **Micro** button and select a micro from the list box. If multiple readers are configured on an elevator micro, the first reader controls the elevator.
3. For each floor, click the appropriate button and select an output from the list box. Make sure you select a different output for each floor. This type of configuration supports up to 64 floors per micro.
4. For each floor, define floor names. See *How to edit floor labels* on page 376.

To set up Example 2 Reader/DO configuration:

1. In **Configuration Type**, select **Reader/DO**.
2. Click the **Reader/DO Config** button.
3. Click the **Reader** button and select a reader from the list box. The reader should be defined as an elevator reader.
4. For each floor, click the appropriate button and select an output from the list box. Make sure you select a different output for each floor. This type of configuration supports up to 64 floors per micro.
5. For each floor, define floor names. See *How to edit floor labels* on page 376.

To set up Example 2 in a Reader/DI/DO configuration:

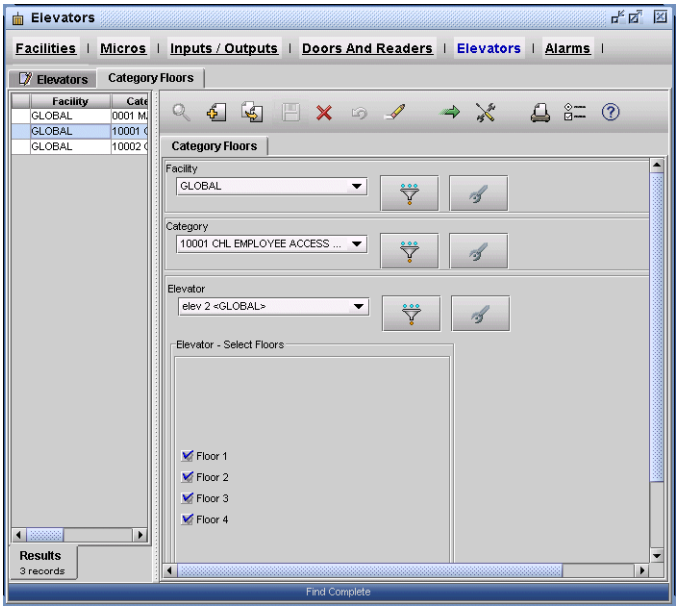
1. In **Configuration Type**, select **Reader/DI/DO**.
2. Click the **Reader/DI/DO Config** button.

3. Select the **Fire DO after Floor Selection** button to enable Elevator Access Method 2 in which, after a valid badge read, a floor has to be selected and if it is an accessible floor, the DO will be activated. See page 370 for more information on this method of elevator access. Otherwise the default Method 1 in which, after a valid badge read, the DOs for all accessible floors are activated, will be employed. See page 369 for more information on this method of elevator access.
4. Click the **Reader** button and select a reader from the list box. The reader should be defined as an elevator reader.
5. For each floor, click the appropriate button and select an input and output from the list boxes. To appear in the list box, the input must be defined as an elevator input. Every input chosen must have a corresponding output chosen. This type of configuration supports up to 39 floors per micro. Click the **Refresh Floor Defs** button to update the floor labels if changes have been made since the **Config** window was displayed.
6. For each floor, define floor names. See *How to edit floor labels* on page 376.

The Category Floors form

Use the Category Floors form to assign a category to certain floors of each elevator. This category is used to establish a match between the badge and the floor when granting access. The number of categories assigned to each elevator must not be greater than 128. The number of floors displayed on this form is determined by the **Number Of Floors** field defined on the Elevator form.

Figure 181.Category Floors form



Fields and Controls

The following is a list of fields that may require additional information for you to complete. Because forms are user customizable some of these fields may not appear, or may appear in a different order than that shown in the following table. There is no required sequence to follow.

Table 126. Category Floors form fields

Field name	Description
Facility	Click Facility to display the facilities list box. This field reflects the facility to which this record is assigned. For more information, see *Creating facilities* on page 53.
Category	Click the Category button to display a list box of categories. Select the category to which you want to assign floors for this elevator.
Elevator	Click the Elevator button to display a list box of elevators. Select the elevator to which you want to assign Category Floors, and then click Close.
Select Floors	These toggle buttons are available only after an elevator is selected. Toggle the buttons on for each floor that is to be assigned this category.

Scheduling elevator free access

In order to schedule elevator free access, a door must be defined on the Doors form and a digital output corresponding to a floor number must be assigned to the **Door Strike Output** field. By using this setup, a door can be scheduled to **Lock** or **Unlock** through the Schedule, Door Events form. When the door is scheduled to unlock, the digital output is triggered and the associated floor's button is activated.

See *Defining doors* on page 187 and *Scheduling door events* on page 209.

If a door is unlocked by a Door Event, a badge is not required to activate the digital output corresponding to that floor. This button may be selected by anyone, not necessarily an authorized badge holder.

The digital output can be deactivated in the same manner by scheduling a door to lock using the Door Events form. The button will not be lit, and a valid badge will be required to access the elevator's floors.

For each floor requiring a scheduled free access, its digital output must be associated with a door, and each door must then be scheduled for a specific action.

Floor tracking

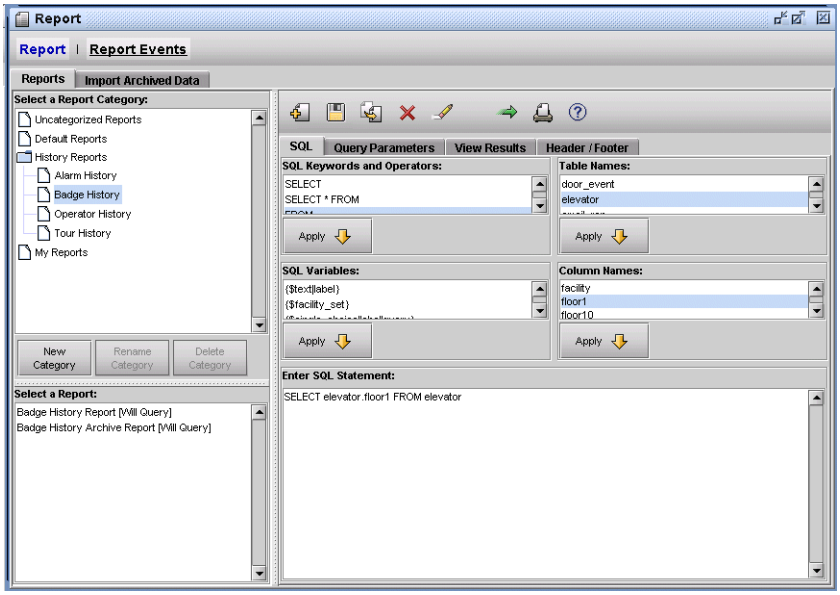
When Method 2 is employed for Elevator Access, floor transactions are generated and stored along with the floor selected. This data can then be used for history and reporting purposes.

To generate a Floor Tracking report:

1. From the **Reports** menu, select the **Report** menu item, and then click the **Report** tab.
2. Click **New** . A Modified Report dialog box displays. Click **Yes** to continue.
3. From the **Select a Report Category** list pane, select **History Reports**, **Badge History.**

4. From the **Table Names** list pane, select *badge_history*. Once you have selected the table, the Column Names list pane displays the columns in the database.
5. From the **SQL Keywords and Operators**, select **SELECT** and click **Apply**.
6. From the **Column Names** list pane, select *floor accessed*. Other fields, such as transaction type (*xact_type*), date (*xact_date*), or time (*xact_time*) can be selected.
7. Click **Apply**.
8. From the **SQL Keywords and Operators**, select **FROM** and click **Apply**.
9. From the **Table Names** list pane, select *badge_history*. Click **Apply**.

Figure 182.Floor Tracking report setup



10. Click **Print** to display the Print Preview page. From this window you may Save to pdf or Print to your local printer.

Pre-alarm notification

Pre-alarm Notification informs users that a sensing violation is about to occur. The warning notification method can vary. It can be set to trigger an output, such as a horn or a light, and/or send a signal to the Alarm Monitor.

Pre-alarm function

Pre-alarm is activated at a specified interval before a sensing violation occurs on an open door, and will not function if the Allowable Open Time for that door is less than the specified interval. The length of the Pre-alarm interval is user configurable.

Pre-alarm can be reset by a valid reader transaction or by closing the door. Otherwise, it resets when the sensing violation occurs.

Activating the Pre-alarm means activating the Pre-alarm input group. Resetting the Pre-alarm means resetting the Pre-alarm input group.

When a valid reader transaction occurs while waiting for the Pre-alarm to activate, its timing is restarted. During the interval between the Pre-alarm and the sensing violation, a valid reader transaction will restart the timing and reset the Pre-alarm. When the Pre-alarm interval expires, the Pre-alarm resets and the sensing violation activates. Typically, the sensing violation is reset by closing the door.

Pre-alarm notification methods

There are three methods of Pre-alarm notification:

- An alarm can be sent to the host which, if routed, will be displayed on the Alarm Monitor.
- An audible warning signal can be activated.
- A combination of the above (an alarm and an audible warning signal).

Disabling pre-alarm

Pre-alarm can be disabled in the following ways:

- Do not configure a Pre-alarm input group for a door.
- Disable Pre-alarm on the Doors form.
- Configure the door with an Allowable Open Time less than or equal to the Pre-alarm interval.
- Disable the Pre-alarm input group. This entirely disables the Pre-alarm by preventing the Pre-alarm input group and its associated alarm and outputs from changing state.
- Disable the Pre-alarm input group's alarm. This only disables Pre-alarm notification. It does not affect the outputs associated with the Pre-alarm input group.
- Disable the Pre-alarm input group's associated output groups and/or outputs. This only disables the Pre-alarm outputs; it does not affect Pre-alarm notification. When a Pre-alarm is associated with more than one output, they can be individually disabled using the separate outputs and output groups.

  Note:

  - Disabling a door's ability to detect a sensing violation will not cancel the door's current timer.

- Enabling or disabling Pre-alarm using the radio button has no effect on an on-going timing process. If Pre-alarm is disabled when the door opens, it stays disabled until the door closes. If Pre-alarm is enabled when the door opens, it stays enabled until the door closes.
- Creating a Pre-alarm input group during a timing process will not affect the Pre-alarm; it continues to behave as if it were enabled. Removing a Pre-alarm input group during the timing process will have different effects based on when it is removed. Removing it before Pre-alarm activates will prevent activation. Removing it after activation will prevent Pre-alarm from resetting. By removing the input group, the door loses its pointer to the input group and its associated alarm and outputs.
- Changing the door's Allowable Open Time also has different effects, based on when it is changed and the value to which it is changed. The rules below are listed in priority order. In other words, the second rule has no effect when the first rule overrides it.
  - Changing the Allowable Open Time after Pre-alarm activates has no effect.
  - When the old Allowable Open Time prevents Pre-alarm from activating and it is changed after the door is opened, the change has no effect.
  - Pre-alarm will not activate when the new Allowable Open Time prevents it from doing so.
  - When Pre-alarm can activate and the Allowable Open Time is changed to a value which means Pre-alarm should already have activated, it immediately does so.
  - When Pre-alarm can activate and the Allowable Open Time is extended, the timing continues uninterrupted. Pre-alarm activates when the door has been opened for the new Allowable Open Time minus the Pre-alarm interval.

Pre-alarm configuration

Use the Doors form to configure Pre-Alarm for an individual door.

Enable this feature using the Pre-alarm radio button. In order for Pre-alarm to generate a warning signal, an input group must be defined. The associated outputs operate any type of physical device that can be connected to a micro, including devices that produce audible warning signals.

The Pre-alarm feature is not designed to associate inputs with the Pre-alarm input group. Pre-alarm uses the Alarm routing defined on the Alarms form, and the Door Status will display the door's Pre-alarm input group and whether the door is disabled or enabled for Pre-alarm.

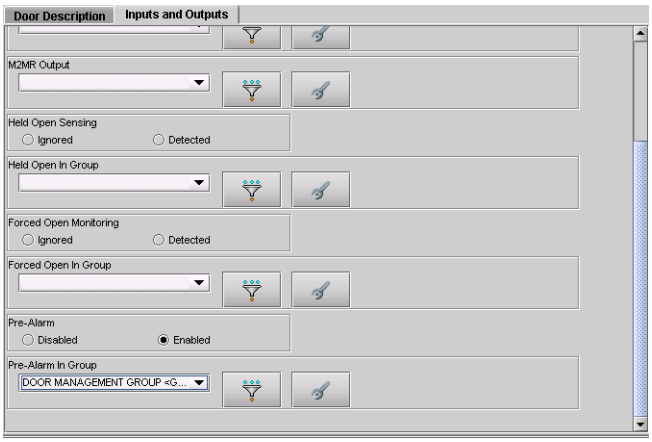
The Allowable Open Time on the Doors form must be greater than the Pre-alarm interval in order to use Pre-alarm, as the Pre-alarm input group will be triggered at the specified interval before a sensing violation is detected and reported. Keypad Shunt Time can be used to extend the allowable open time on a door. In this case, the Pre-alarm warning signal will be triggered at the specified interval before the Held Open Too Long violation is issued.

To set up pre-alarm notification:

1. From the **Configuration** menu, select **Doors and Readers**, and then click the **Doors** tab.
2. From the toolbar, click **Find** to locate the door record you want to set up.
3. On the **Inputs and Outputs** tab, enable **Pre-alarm**.
4. Click the **Pre-alarm** button to display a list box of input groups. Select the desired input group.
   - If a warning signal is required at the host, an alarm must be associated with that input group.
   - If an audible warning signal is required, an output group containing at least one digital output must be associated with that input group.

See *Defining doors* on page 187.

Figure 183.Door form: Pre-Alarm



5. Click **Save** to save your changes.

Controlling alarms using a keypad code

Keypad Alarm Response allows alarms to be cleared only after an input has been physically reset (such as closing a door that has been forced open), and an authorized badge has been swiped, and a keypad code entered. The use of this feature is intended for strict controlled resets by authorized card holders only.

This feature requires a response to access violations at both the host and reader levels. The alarm response consists of two actions: a response at the host or sub-host and a response badge swipe and keypad code at the reader. The badge must be specially authorized for Keypad Alarm Response.

This section shows how to configure a Picture Perfect system to implement the Keypad Alarm Response feature.

Keypad alarm response function

The Keypad Alarm Response function starts with an access violation: the door is forced open or is held open too long. The violation activates one of the door's input groups, which then triggers the alarm and outputs associated with that input group. Forcing the door open activates the door's forced-open input group, and holding the door open for too long activates the door's open-too-long input group. The input group and its associated outputs are not reset until the door is closed and a valid keypad response and badge swipe are made on the reader associated with the door.

Without the Keypad Alarm Response feature, the access violation would end when the door closes. With Keypad Alarm Response, the violation ends when a valid keypad response is entered after the door closes. When the violation ends, the violation's input group along with the associated alarm and outputs are reset.

Note: Ending the violation is not the same as completely responding to the violation's alarm. The alarm response is not complete until the violation is ended by a keypad response and the operator has fully responded to the alarm on the Alarm Monitor.

Violation notification

When a violation starts, the host displays an alarm on the Alarm Monitor. The Condition field on the Alarm Monitor indicates "alarm". When the violation ends, the alarm changes to "reset" state. The access violation alarms must be routed to the Alarm Monitor for Keypad Alarm Response to function properly.

Keypad response

Alarm response at the Badge-and-Keypad reader requires an alarm-response code, a badge swipe, and a PIN or duress code. The alarm-response code is entered on the keypad as the first activity. The required order of activity is outlined below:

1. Press (*) or (+), enter the Alarm-Response Code, and then press (#).
2. Swipe the badge.
3. Press (*) or,(+) enter the PIN or Duress Code, and then press (#).

When the reader is configured for double-transaction, the first and/or second component transaction may enter an alarm-response code. See *Double-badge function* on page 366.

Keypad response only affects an active access violation on a door to which the reader is associated. It cannot affect any other door. The following situations must exist for the keypad response to be valid:

- The door must be closed before the keypad response.
- The badge must be authorized for keypad response.
- The entire reader transaction must be granted access. For example, an invalid PIN or a category mismatch will invalidate the keypad response.

Valid keypad alarm response does not unlock the door. Keypad alarm response is essentially an acknowledgment that the door is secure, so it makes no sense to unlock the door for the keypad response. Since the door does not open, keypad response is independent from anti-passback. This means that keypad response cannot fail due to the badge's anti-passback status. It also means that keypad response cannot change the badge's anti-passback status.

As with all other reader activity, keypad response is reported in the host's badge monitor and/or badge history. The transaction explicitly reports that it is keypad response. When keypad response is valid, a report is made that the transaction was valid but did not gain access. Invalid keypad responses report the reason for failure. In addition to usual failure reports, the keypad response feature also reports the following:

- Invalid alarm-response code.
- Badge is not authorized for keypad response.
- Door is not secured (the door is physically open).

Operator response

Operators respond to alarms requiring keypad alarm response in the same manner as any alarm associated with a physical input. The only difference is that the keypad alarm response resets the alarm rather than a physical change in an input.

The vehicle for operator response is the Alarm Monitor. Its operation is not changed by keypad alarm response. The Alarm Monitor presents information to the operator on each alarm that is routed to it. The information includes the alarm's Condition and Process State.

Condition

- **Alarm** - Alarm is logically on.
- **Reset** - Alarm is logically off.

When the violation first occurs, its Condition is "alarm" and its Process State is "active". When a valid keypad response occurs, the violation's Condition goes to "reset".

Process state

- **Active** - No alarm response has been made.
- **Pending** - Partial alarm response has been made.
- **Complete** - Final alarm response has been made.

Selecting the alarm on the Alarm Monitor pops up a window which displays the alarm's instructions and allows the operator to enter a response. The instructions are the only means of notifying the operator that keypad alarm response is required. The ways in which the operator can exit the pop-up are listed below:

- **Cancel** - Response is ignored and the Process State stays the same.
- **OK** - Response is saved and the Process State goes to "pending". The alarm remains on the Alarm Monitor.
- **Remove** - Response is saved and the Process State goes to "complete". When the alarm's Condition is "reset", the alarm is removed from the Alarm Monitor. When the alarm's Condition is "alarm", the alarm remains on the Alarm Monitor.

Multiple access violations

It is possible for the same access violation to occur more than once during a keypad alarm response. For instance, a door can be forced open, then closed, and then forced open again all before the keypad alarm response is completed for the first violation. In this situation, only one alarm appears in the Alarm Monitor. The alarm first appears with a count of one, and is incremented by each subsequent violation.

A single valid keypad response resets all occurrences of the violation and the operator responds to all occurrences using the single alarm.

It is also possible for a door to be forced open and open too long during a single keypad alarm response. For instance, the door can be held open for too long, then closed, and then forced open all before a valid keypad response is made for the sensing violation. In this situation, the violations appear as separate alarms on the Alarm Monitor.

A single valid keypad response resets both alarms. Each alarm is separately removed from the Alarm Monitor when the response is completed.

Door operation while violation is active

The door will continue to operate normally while the keypad alarm response is active. This makes it possible for someone to gain access through the door even though the response to the violation has not been completed.

Keypad alarm response configuration

To set up a Keypad Alarm Response (details on each step are given below):

1. Define the Alarm-Response Code (maximum of 10 digits) on the Micros form.
2. Define a reader as a Badge-and-Keypad reader on the Readers form.
3. Enable the Keypad Alarm Response on the Door form.
4. Enable a badge to be used as the Keypad Alarm Response badge on the Badge form.

Defining the alarm-response code

Use the Micros form to define an alarm-response code (up to 10 digits) for each micro on which Keypad Alarm Response will be implemented. When an authorized badge holder responds to an access violation on a door using this feature, he will enter this code (for reader keypads on this micro).

The same code can be used on any number of the system's micros, or you can configure different codes for different micros. The alarm-response code must be different from the shunt code assigned to that micro. Failure to define an alarm-response code prevents Keypad Alarm Response from working on any of the micro's doors.

See *Defining micros* on page 132.

Defining a reader

Use the Readers form to define a reader as a Badge-and-Keypad reader. Keypad Alarm Response only works with doors associated with Badge-and-Keypad readers. Once the reader is defined, you then associate it with a door that has Keypad Alarm Response enabled.

See *Defining readers* on page 182.

Enabling keypad alarm response

Use the Doors form to enable Keypad Alarm Response. This feature can be enabled or disabled for individual doors, and status requests on doors will show this. The door must be associated with a Badge-and-Keypad reader. You will be warned if the door is not associated with at least one Badge-and-Keypad reader connected to a micro with an alarm-response code. You may save the door information anyway, or make the necessary associations before saving the door again, but Keypad Alarm Response does not function correctly unless those associations are made.

While it is possible to configure a Picture Perfect system to have more than one reader associated with one door, and for one reader to be connected to more than one doorstrike output, Keypad Alarm Response does not support this configuration.

Keypad Alarm Response can be incorporated into scheduling. For instance, if a reader is scheduled to change between being a Badge-Only reader and a Badge-and-Keypad reader for a door with Keypad Alarm Response enabled, alarms occurring during the badge-only state will not require a keypad alarm response, while those occurring during the badge-and-keypad state will require it. If an alarm occurs during the badge-and-keypad state, but has not yet been responded to when the schedule change goes into effect, the reader will remain in the Keypad Alarm Response mode until proper response is made, then the reader will change to the badge-only mode.

See *Defining doors* on page 187.

To enable Keypad Alarm Response:

Use the Badges form to enable a badge for Keypad Alarm Response. Status requests on badges show whether or not a badge is authorized for keypad response. Keypad response authorization is independent of badge type (such as permanent, contractor, etc.), but it must be an active badge.

See *Defining badges* on page 224.

Disabling keypad alarm response

Keypad Alarm Response can be disabled in the following ways:

- Disable Keypad Alarm Response on the Doors form. This prevents Keypad Alarm Response for both types of access violations on that door.
- The following situations inhibit an access violation completely. The violation is not reported to the host and Keypad Alarm Response does not function.
  - Access Violation input group not configured.
  - Access Violation input group disabled.
  - Access Violation input group not associated with an alarm.
  - Disabled alarm associated with the Access Violation input group.

Disabling or enabling Keypad Alarm Response does not affect an active access violation. Therefore, enabling Keypad Alarm Response while a door is forced open does not change the fact that the violation resets as soon as the door closes. The change has no effect until the current violation ends.

Tracing badge holder activity

This feature allows an operator to trace an individual badge holder and route activity to a specific routing location--regardless of the routing definition for each of the area's input groups. When the traced badge holder swipes a badge through a reader, a record of the transaction is sent to the Person Trace routing destination (usually to the Badge Monitor and the History Log). The routing for Person Trace transactions is set up on the System Parameters form. Specific badge holders that are to be traced are identified on the Personnel form.

If Person Trace is routed to the Badge Monitor, a T is displayed in front of the activity record to indicate that the badge holder is being traced.

If the Person Trace is routed to the History Log, the data is identified as a normal badge transaction.

To configure the Person Trace feature, select a routing for traced badge holders using the Person Trace Routing field of the Parameters form. (See *Assigning system parameters* on page 40 for details on completing this form.)

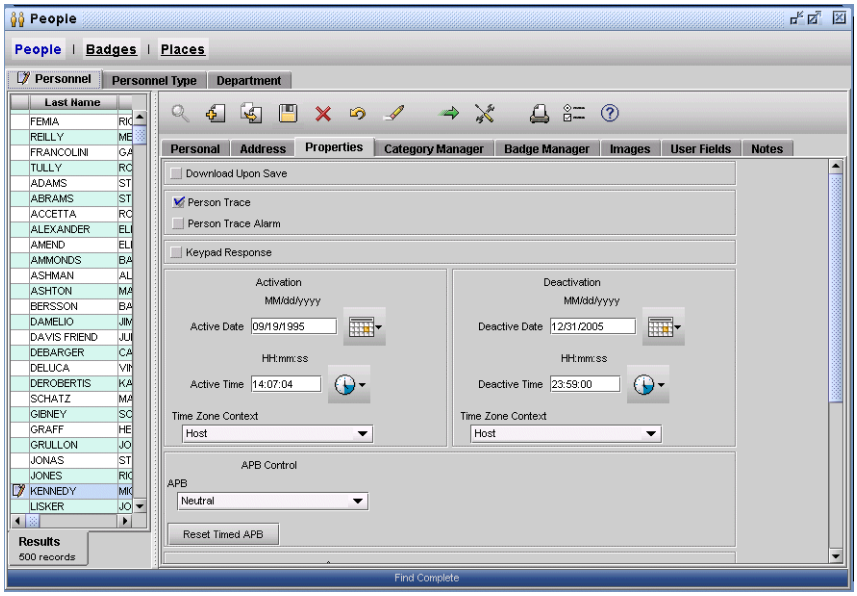
When you want to trace a particular person (badge holder), you must enable Person Trace on the Personnel form. When you no longer want to trace them, you must disable Person Trace.

If you want an alarm to be generated every time the badge is read, enable the Person Trace Alarm option.

To enable or disable Person Trace:

1. From the **Access** menu, select **People, and then** click the **Personnel** tab.
2. Click **Find** to display the desired Personnel (badge holder) record.
3. Click the **Properties** tab.
4. Enable the **Person Trace** button to begin tracing or disable it to discontinue the Person Trace. Additionally, if you want an alarm to be generated every time the badge is read, enable the **Person Trace Alarm** button.

Figure 184.Personnel form: Person Trace



5. Click **Save** .

Escort required

Escort Required is a feature that can be used when a person or group must be escorted into an area by a person with valid access.

Escort categories are assigned, as other categories, to Area records and Badge Records. A maximum of 10 Escort categories per Area record will be permitted. The Escort category does not change access to areas where a badge holder already has access; however, attempted access to an area where the Escort category is the only match will start an Escort Transaction.

Note: For PXN+ controllers, you will see two additional valid normal transactions at the end of the escort sequence.

An Escort Transaction causes an LED on the door reader to blink, indicating that it is waiting for an additional badge read. The door remains locked until a badge read with a non-Escort category match occurs. If a valid non-Escort access badge read does not occur within the Interval Time set on the Reader form, the Escort Transaction will time out. An Escort Transaction is “time extended” by the presentation of another badge with a matching Escort category, even if the Escort category is different between consecutive visitors. Example: If visitor A gets a match on Escort Cat 1 and is followed by Visitor B who gets a match on Escort Cat 2, then the time is extended.

An Escort Transaction can be terminated by one of three circumstances:

- A badge with a non-Escort category match to the area is presented after the transaction begins and before the transaction timeout value is reached (valid termination case)
- The transaction timeout condition is reached
- A badge without a category match is presented before either one of the conditions above are met (intervening badge case).

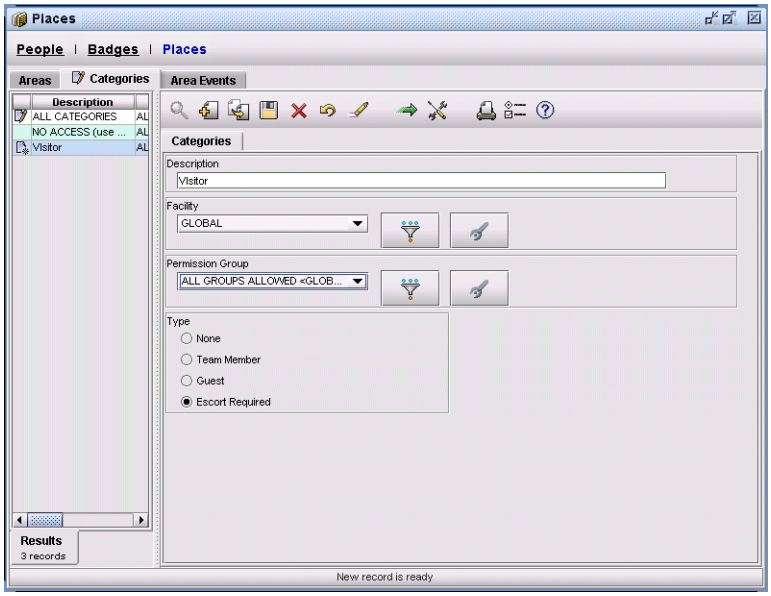
A group of visitors can be accompanied by a single escort. There is no limit to the number of Escorted badge holders (visitors) that can be processed, as long as they all occur within 20 seconds of each other. Badge History will be sent to the host as each badge is processed.

An Escort category match will generate a Badge History message sent to the host with “Escort Requested” status and the matching category ID. The transaction will be displayed on the host’s Badge Monitor.

A terminating badge read (non-Escort category match) will generate a Badge History message with “Escort Provided” status and the matching category. The transaction will be displayed on the host’s Badge Monitor.

Timeout or any other termination condition will cancel the LED indication and post an “Invalid Escort” alarm, which will be recorded in Alarm History on the Host.

Figure 185.Categories form: Escort Required



To enable or disable Escort Required:

1. From the **Access** menu, select **Places, and then** click the **Categories** tab.
2. Click **Find** to display the desired Category record.
3. Enable the **Escort Required** button.
4. Click **Save** .

Chapter 19 Troubleshooting, maintenance, support

This chapter provides information to help you troubleshoot problems as well as technical support contact information in case you need assistance with your GE equipment.

In this chapter:

Overview

This section provides information to help you diagnose and solve various problems that may arise while configuring or using your GE product and offers technical support contacts in case you need assistance. (See *Contacting Technical Support* on page 406.)

Troubleshooting your Picture Perfect 4.5 system

Troubleshooting tools:

Note: If you receive a syntax error popup when logging onto the Picture Perfect webtop from your browser, make sure that you are using the following supported Web Browsers and Java Plug-in.

- Java Plug-in: Java Runtime Environment (JRE) 6.0 update 13
- Web Browsers:
  - Internet Explorer 6.0 with Service Pack 1 or later
  - Internet Explorer 7.0
  - Firefox: 3.0

The client log file and the Java console contain useful information that can be used for troubleshooting client issues. To access these tools:

- The client log file is located in: `c:\avatar\logs\avatar.log`
- There are two ways to open the Java console:
  - From the Internet Explorer window titled "Picture Perfect Webtop", navigate to Tools->Sun Java Console.
  - From the coffee cup icon that appears at the right side within the Windows taskbar, right click it and select "Open Console" from the context menu.

Log on troubleshooting

If you get one of the following error messages during the login process, please follow the steps below to troubleshoot and help resolve the issue:

- `An error occurred during login. Please try again later.`
- `Unable to transmit login message to host.`

1. Verify that the client workstation (WS) OS is Windows XP professional SP3 or Windows Vista SP2 and that the WS has a minimum of 2 GB of RAM.
2. Verify that you are using Internet Explorer (IE) Internet Explorer 6.0 with Service Pack 1 or later, Internet Explorer 7.0, or Firefox: 3.0
3. Verify that the Java plug-in used by your Web Browser is ava Runtime Environment (JRE) 6.0 update 13. Turn off Automatic Updates in the Java Control Panel under the Update tab.
4. Verify that the client “Java Runtime Parameters Specification” for the JVM is using the recommended memory, typically -Xms256m –Xmx512m for a system with 512 MB of RAM and not the default setting of 100 MB.

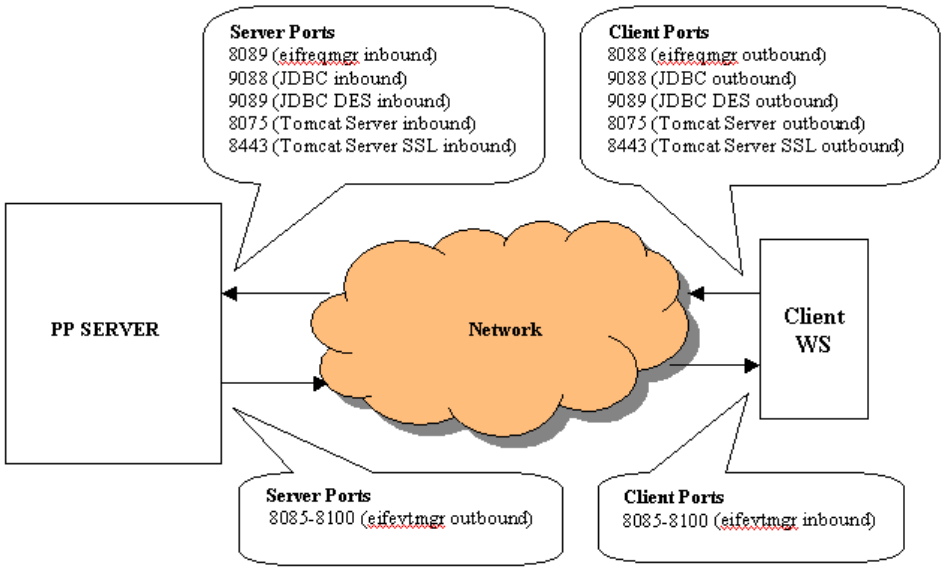
Open and check the Java Console Panel / Advanced tab / Java Runtime Parameters Specification settings:

- Right click the Java icon (coffee mug) on the Windows taskbar, and then select Open Console Panel.
- The JVM memory settings can also be checked from the Picture Perfect client under Help/About Picture Perfect/About tab - Max Memory field.

5. If you receive the error message: `Unable to transmit login message to host:`
   a. Verify that the hostname in the URL on the browser's address field. `http://<hostname>/Picture/` is either the host IP such as, `http://192.9.200.1/Picture/`, or the fully qualified hostname.
   b. Verify that you have a valid Picture Perfect license. Run `skver` on the server.
   c. Try removing the cache folders for both Picture Perfect and Java. If the Picture Perfect cache data is stale, the client requires a new Avatar jar file. This will force the Picture Perfect client and Java to download and build new cache files from the server.
   d. On the Client workstation, remove all folders under `c:/avatar/`
   e. Clear the Java cache from the Java Control Panel under the Cache tab by pressing Clear.
   f. Close all browser windows and retry logging on.
6. Verify that the user logged into the client workstation has read/write privileges to the local drive `c:\Avatar` folder. If it is an Imaging workstation, then also check the read/write privileges on `c:\Documents and Settings\<user>\Local Settings\Temp\GE_SECURITY`
7. Verify that the following inbound/outbound TCPIP ports are not blocked between the client workstation and the Picture Perfect server. See Figure 186.

Note: The default ports used can be over written by user defined port entries.

Figure 186.Troubleshooting ports



8. Verify that personnel firewall and PC protection applications are turned off on the client workstation or have exception lists to allow inbound/outbound TCPIP ports, used by the Picture Perfect client, to pass messages to and from the Picture Perfect server. The following are some of the common personnel firewall and PC protection applications that are known to cause problems:
   - Cisco security agent
   - BlackICE
   - XP Personnel Firewall
   - OfficescanNT firewall.
9. Check the Java Console output on the client workstation for any error messages or any indication of the problem with the login process.
   - Right click on the Java icon (coffee mug) on the Windows taskbar.
   - Select Open Console to open the Java console, and then check the messages for any errors.
10. Verify that the Apache Tomcat server on the Picture Perfect server is running properly:
    - Enter the following URL in the Internet Explorer address field: `http://<hostname>:8075/PPServer/ppservlet`
    - Click Go. If you get the following message in the body of the web page `This is a test response,` then the Tomcat server is running properly.

      In the event that the Tomcat server is not running properly:

      - Stop and restart the Tomcat server.

      To shut down the server, type:

Linux

```
/var/www/apache-tomcat-5.5.12/bin/shutdown.sh
```

AIX

```
/usr/HTTPServer/apache-tomcat-5.5.12/bin/shutdown.sh
```

To start up the server, type:

Linux

```
/var/www/apache-tomcat-5.5.12/bin/startup.sh
```

AIX

```
/usr/HTTPServer/apache-tomcat-5.5.12/bin/startup.sh
```

- Check the **`catalina.out`** log file for any Java exceptions during startup.

Linux

```
/var/www/apache-tomcat-5.5.12/logs/catalina.out
```

AIX

```
/usr/HTTPServer/apache-tomcat-5.5.12/logs/catalina.out
```

Listed below is a sample printout of a proper startup:

```
...
...
...
```

```
2006-05-16 09:50:30,301 INFO - Executing... size=[2277],
query=[DropDownForeignControlPanel.category] [main] db.QueryUtil
(QueryUtil.java:255)
2006-05-16 09:50:30,563 INFO - Executing... size=[2277],
query=[DropDownForeignControlPanel.category2] [main] db.QueryUtil
(QueryUtil.java:255)
2006-05-16 09:50:32,578 INFO - initializeStaticDatacache() semi-static10 number
queries run:2 [main] server.ServerCache (ServerCache.java:158)
May 16, 2006 9:50:35 AM org.apache.coyote.http11.Http11BaseProtocol start
INFO: Starting Coyote HTTP/1.1 on http-8075
May 16, 2006 9:50:35 AM org.apache.coyote.http11.Http11BaseProtocol start
INFO: Starting Coyote HTTP/1.1 on http-8443
May 16, 2006 9:50:36 AM org.apache.jk.common.ChannelSocket init
INFO: JK: ajp13 listening on /0.0.0.0:8009
May 16, 2006 9:50:36 AM org.apache.jk.server.JkMain start
INFO: Jk running ID=0 time=0/345  config=null
May 16, 2006 9:50:36 AM org.apache.catalina.storeconfig.StoreLoader load
INFO: Find registry server-registry.xml at classpath resource
May 16, 2006 9:50:37 AM org.apache.catalina.startup.Catalina start
INFO: Server startup in 122212 ms
```

11. Verify the **`client.html`** file on the Picture Perfect server is configured properly with the proper settings.

    Linux

    ```
     /var/www/html/Picture/client.html
    ```

    AIX

    ```
    /usr/HTTPServer/htdocs/en_US/Picture/client.html
    ```

    See default sample file below for proper port and other settings (in blue):

    ```
    <html>
    <head>
    <script type="text/javascript" language="JavaScript">
    <!-- Hide script from old browsers

    function openHelp(path, page, title)
    {
            var file = path + page;
            var HelpWindow = window.open(file,title,
                    "scrollbars=yes,resizable=yes,width=800,height=650");
    }

    // End hiding Script -->
    </script>

    <title>Picture Perfect</title>
    <head>
    <body leftmargin=0 marginheight=0 marginwidth=0 topmargin=0>
            <!--"CONVERTED_APPLET"-->
    ```

```
    <!-- HTML CONVERTER -->
    <center><object name="PicturePerfectApplet"
        classid="clsid:8AD9C840-044E-11D1-B3E9-00805F499D93"
       codebase="http://java.sun.com/products/plugin/autodl/jinstall-1_4_2-windows-
i586.cab#Version=1,4,2,0"
        width=100%
        height=100% mayscript="mayscript">
 <param name="DriverClass" value="com.informix.jdbc.IfxDriver">
        <param name="Hostname" value="redmoon">
        <param name="Database" value="proteus">
        <param name="Environment"
value="INFORMIXSERVER=redmoon;INFORMIXDIR=/cas/db;JDBCTEMP=c:\avatar;">
        <param name="Username" value="informix">
        <param name="Language" value="English">
        <param name="Protocol" value="jdbc:informix-sqli:">
        <param name="Proto" value="HTTP">
        <param name="HTTP_Port" value="8075">
        <param name="EIFPort" value="8085-8100">
        <param name="EIFIncomingPort" value="8088">
        <param name="NUM_RETRIES" value="3">
        <param name="PING_INTERVAL" value="3">
        <param name="code" value="com.ge.security.avatar.Avatar.class">
       <param name="archive" value="lib/xmlrpc-1.2-b1-applet.jar,lib/jhall.jar,lib/
PPHelp.jar,Avatar.jar,lib/log4j-1.2.8.jar,lib/geSecurityNlsProject.jar,lib/
kunststoff.jar">
        <param name="type" value="application/x-java-applet;version=1.4.2">

        <comment><embed
            type="application/x-java-applet;version=1.4.2" \
            code="com.ge.security.avatar.Avatar.class" \
            archive="lib/xmlrpc-1.2-b1-applet.jar,lib/jhall.jar,lib/
PPHelp.jar,Avatar.jar,AvatarLocales.jar,lib/log4j-1.2.8.jar,lib/
geSecurityNlsProject.jar,lib/kunststoff.jar" \
            width=100% \
            height=100% \
                        mayscript="mayscript" \
            DriverClass="com.informix.jdbc.IfxDriver" \
            Hostname="redmoon" \
            Database="proteus" \
            Environment="INFORMIXSERVER=redmoon;INFORMIXDIR=/cas/
db;JDBCTEMP=c:\avatar;" \
            Username="informix" \
            Language="English" \
            Protocol="jdbc:informix-sqli:" \
            Proto="HTTP" \
                              HTTP_Port="8075" \
            EIFPort="8085-8100" \
            EIFIncomingPort="8088" \
            pluginspage="http://java.sun.com/products/plugin/index.html#download">
        <noembed>
```

```
            alt="Your browser understands the &lt;APPLET&gt; tag but isn't running
the applet, for some reason."
            Your browser is completely ignoring the &lt;APPLET&gt; tag!
        </noembed></embed></comment>
    </object></center>
    <!--
        <applet code="com.ge.security.avatar.Avatar.class" width=1 height=1>
        </applet>
    -->
    <!--"END_CONVERTED_APPLET"-->
</body>
</html>
```

12. Verify that the Apache Tomcat server configuration file server.xml is configured properly.

    Linux

    `/var/www/apache-tomcat-5.5.12/conf/server.xml`

    AIX

    `/usr/HTTPServer/apache-tomcat-5.5.12/conf/server.xml`

    For standard connections the section (in green) port 8075 needs to be uncommented (no XML tags <!-- --> around the block of code) listed below, and the SSL connections section (in blue) commented out (XML tags <!-- --> around the block of code) listed in the next section:

```
   <Connector port="8075" maxHttpHeaderSize="8192"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
      enableLookups="false" redirectPort="8443" acceptCount="100"
      connectionTimeout="20000" disableUploadTimeout="true" />

<!--
   <Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="/cas/db/text/tomcat.key"
keystorePass="install" keystoreType="PKCS12" />
-->
```

    For SSL connections the section (in blue) port 8443 needs to be uncommented (no XML tags <!-- --> around the block of code) listed below, and the standard connections section (in green) commented out (XML tags <!-- --> around the block of code) listed in the next section:

```
   <Connector port="8443" maxHttpHeaderSize="8192" maxThreads="150"
minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="/cas/db/text/tomcat.key"
keystorePass="install" keystoreType="PKCS12" />

<!--
   <Connector port="8075" maxHttpHeaderSize="8192"
      maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
```

```
      enableLookups="false" redirectPort="8443" acceptCount="100"
      connectionTimeout="20000" disableUploadTimeout="true" />
-->
```

13. If there is a problem connecting to the server via SSL connection:

    - Verify that the URL on the browser's address field is:

`https://<hostname>/Picture/` and not
`http://<hostname>/Picture/`

    - Also verify that the SSL certificate used on the server has not expired. Use the following command on the server to check the certificate:

```
/usr/bin/openssl x509 -in /cas/db/text/<hostname>.crt -text
```

Imaging troubleshooting

- *Problem*

  Exception output is shown in the Java Console and Imaging functionality is disabled in the client.

  There is a known limitation whereby a client PC that is an imaging workstation (the ImageWare software has been installed) can only run one client at a time to a host where the image package is installed. Only one imaging client can be run at a time on a PC.

- *Problem*

  The **Print** and/or **Preview** buttons on the Badge or Personnel form are not active (dimmed). See *Printing badges* on page 242 for more information.

  1. Verify the following:

     1a. Verify that the operator has permission to print badges in the facility in which the particular badges they are working with reside. If the operator had been logged on previously to an account that did not grant imaging permissions, the operator should log out, close all browser windows and open a new browser window to log on again.

     Note: The operator must always log on for imaging operations from a newly opened top level browser window.

     Possible causes include:

     - Permission profiles were changed by an administrator.
     - A known problem in the EPIBuilder software allows it to be initialized only one time. As long as the top level browser window is open, subsequent initializations will fail causing imaging functionality to not be available.

     1b. Verify that the operator workstation is correctly identified as an imaging workstation. On the Workstation record (see *Setting up workstations (optional)* on page 56), verify that:

     - The **Imaging Workstation** check box is enabled.
     - The IP address entered in the `/etc/hosts` file matches the **IP Address or Hostname** value in the Workstation record and it is the true IP address of the workstation.

     Possible causes include:

     - The flag was disabled by an administrator.
     - The host name or IP addresses of the workstation was changed.
     - The IP address and host name entry for the imaging workstation is missing from the `/etc/hosts` file.
     - The host name of the workstation was changed after it was configured as an imaging workstation.

     1c. Verify that the EPIBuilder imaging installation kit is installed and working correctly on the operator's workstation. The correct installation sequence is specified in Chapter 4 of the *Picture Perfect 4.5 Imaging User Manual* and is briefly stated below. Ensure that the operating system installed on the workstation meets the requirements specified in the *Picture Perfect 4.5 Imaging User Manual*.

     - Examine the `c:\avatar\logs\avatar.log` log file on the workstation to see if EPIBuilder initialization errors are written to the log.

- Verify that all Java versions were removed prior to installation of the EPIBuilder package on the workstation. If in doubt, reinstall.
- Verify that the operating system is at the correct service pack level: Windows XP professional SP3 or Windows Vista SP2

1d. If the problem still persists, remove and reinstall the EPIBuilder Imaging installation kit.

2. EPIBuilder Imaging Kit Installation and Verification Sequence

2a. Verify workstation meets minimum software standards:

- Windows XP professional SP3
- Windows Vista SP2

Note: Windows 2003 Server or Advanced Server have not been certified for EPIBuilder Imaging software.

2b. Remove all currently installed Access Vision packages:

- From the windows taskbar, select **Start**, **Settings**, **Control Panel**, **Add/Remove Programs**.
- Select any installed **Language** or **Service Packs**; click **Remove**.
- Select **Imaging Option 2.0**; click **Remove**
- Select **Access Vision 2.0**; click **Remove**
- Select **EPIBUILDER 5.3 Redistribution**; click **Remove**.
- Select **EPI Builder Runtime files for Picture Perfect**; click **Remove**.

2c. Remove any existing versions of EPIBuilder 6.3 from the workstation.

2d. Remove all currently installed versions of Java from the workstation.

2e. Open the web browser and navigate to the Picture Perfect web page. *Do not launch the client at this time*. If you do so, repeat step *2d*.

2f. Click the link to install the Java Runtime environment.

2g. Click the link to install the EPIBuilder Imaging installation kit.

2h. Reboot the workstation. Verify that you have the correct host name and IP address for the workstation.

2i. Open the web browser and navigate to the Picture Perfect web page. Click on the client button to launch the client and log on as the administrator. Create a workstation record for the imaging workstation. Be sure to enter the correct host name and to enable the **Imaging Workstation** check box. Save the record. Log out completely and close all browser windows.

2j. On the Picture Perfect server edit the `/etc/hosts` file and add the IP address and host name entry for the imaging workstation.

2k. Create the operator account or update an existing operator account and grant Badge Print and other imaging permissions as appropriate.

2l. On the imaging workstation, open the web browser and then navigate to the Picture Perfect web page. Click on the client button to launch the client and log on. Verify that the permissions granted to the operator are reflected in the client software. The operator should be able to perform badge capture and print functions if they were granted to the operator.

- *Problem*

  When using the **Reselect profile** button to select the image device to use in capturing an image, the first attempt at setting the device fails. After clicking **OK** on the Select Image Source window, the change is not accepted.

  This is a known problem that can occur the first time the Select Image Source window is used after the client application is started. Perform the following workaround:

  1. After selecting the device, click **Reselect profile** a second time to confirm that the desired capture device is highlighted. If not, highlight the desired capture device.
  2. Click **OK**.

- *Problem*

  When clicking the **Print** and/or **Preview** buttons on the Badge or Personnel form, the application appears to hang.

  This problem can occur if there is a hidden window requiring input, that is obscured by another window. If the **Show print setup dialog** button is enabled on the Print Options screen, the printer options window can be hidden behind another window. Perform the following workaround to bring the hidden window to the top of the screen:

  1. Hold down the keyboard **Alt** key.
  2. Click the **Tab** key until the Java coffee mug icon is selected
  3. Release the **Alt** key.

  The hidden window should now appear on top and can be dispatched to allow the print or preview operation to continue.

- *Problem*

  Application appears to hang.

  The first time that an operator logs in on an imaging workstation, the client applet will perform a one-time analysis of the badge designs to determine their use of fields in the person and badge tables. Please be patient as this process may take a few minutes if you have a large number of badge designs.

- *Problem*

  Badge designs do not display as expected.

  Picture Perfect 4.5 imaging provides enhancements to the badge designer, some of which have defaults that may produce undesired results when printing badges. After the upgrade to Picture Perfect 4.5 we recommend you examine all of your badge designs. For each badge design perform the following checks:

  - Examine the dynamic text field objects to verify that there are no undesired duplicates. Remove any duplicates you may find.

- Right click on each dynamic text field object and select Properties from the menu. On the Dynamic Text Properties dialog, click on the Conditional Display tab. The Always show object radio button must be selected. Enable it if necessary and then click **OK** to save the change.

- *Problem*

  Objects on the badge appear to be missing.

  This is usually caused by old conditional expression data that was enabled at some time in the past and then disabled. The object can be restored to proper functionality by editing the badge design as follows:

  - Select the area where the missing object would be. (It is actually there but not rendered) Right click on each dynamic text field object and select Properties from the menu.
  - On the Dynamic Text Properties dialog, click on the Conditional Display tab.
  - If the text boxes under the radio buttons contain data that should not be there, click the **Show object only when field/expression** radio button to enable the text boxes.
  - Clear the contents of the text boxes.
  - The Always show object radio button must be selected. Enable it if necessary and then click **OK** to save the change.

- *Problem*

  Objects on the badge are doubled, that is, two copies, one slightly offset from the other.

  This is caused by a problem with the badge design conversion. If two copies of one or more objects are displayed, edit the badge design by deleting the extra copy of each object as follows:

  - Select the extra copy. The extra copy of the object is usually the one that is slightly to the right and lower than the original.
  - Click **Delete**.
  - Click **OK** to save the change.

- *Problem*

  Unable to log on.

  When logging out of the client applet on an imaging workstation, it is necessary to close all of the browser windows before trying to log on again.

- *Problem*

  Badge printing functionality is disabled on the Badge Manager tab of the Personnel form.

  If this occurs, try closing the Personnel form and then reopening it.

- *Problem*

  After capturing a new image for an existing personnel record, you undo the change but the newly captured image still appears in the image panel.

If this occurs, close the Personnel form and then reopen it to see the original image stored in the database.

- *Problem*

  Badge design does not preview or print correctly.

  When previewing or printing badges with Picture Perfect 4.5 imaging for badge designs created with Picture Perfect 4.0 some badge designs with a very large background static image may not preview or print correctly. The problem is due to an internal library incompatibility in third party vendor software. The badge design can be repaired to work correctly with Picture Perfect 4.5 imaging by following these steps:

  1. Locate the original image file for the background. If it is a true color image, reduce its color depth to 32,768 (16 bit) colors.
  2. Edit the badge design and remove the background static image object. Save the badge design.
  3. Edit the badge design again and replace the background static image object using the new image. Save the badge design.
  4. Preview or print a badge using the updated design. It should now work correctly.

  Please note that you must save the badge design after removing the original image and before adding the new image. If you try to remove and replace within the same editing session the update will not work correctly.

Contacting Technical Support

For assistance installing, operating, maintaining, and troubleshooting this product, refer to this document and any other documentation provided. If you still have questions, you may contact technical support during normal business hours (Monday through Friday, excluding holidays, between 8 a.m. and 7 p.m. Eastern Time).

GE Security

United States: 1-888-GE SECURITY (1-888-437-3287)

Asia: 852-2907-8108

Australia: 61-3-9259-4700

Europe: 48-58-326-22-40

Latin America: 503-885-5700

Glossary

This section explains some terms as they apply to Picture Perfect 4.5.

Table 127. Picture Perfect 4.5 terms explained

Term	Definition
Access	The ability to enter or pass through, such as to enter a building by going through a door. See Access Control.
Access Control	A security system that controls an individual's ability to enter an area (building, parking lot, room). Typically, readers protect doors or gates. Badges used in the readers permit or deny access based on a person's authorization.
ACK	Acknowledgment. See ACK Packet.
ACK Packet	A message sent between computers to acknowledge that the preceding message was received correctly.
Active Window	The window with the input focus, in which what you type appears. Only one window is active at a time.
AIX	Advanced Interactive Executive; the UNIX-based operating system developed by IBM; used for Picture Perfect.
Alarm Notification Message	An alarm alert message that displays on the Alarm Notification Window on Picture Perfect X Terminals when an alarm occurs.
Alarm State	When an alarm sensor detects an alarm condition (such as an open door), its contacts open or close (depending on the type of sensor and how it is wired to the system), and the sensor is said to be in alarm state.
Allowable Open	The length of time a door can remain open before an alarm occurs.
Antipassback	Normal: A badge with an APB status of In will not be granted access through an APB In reader; a badge with an APB status of Out will not be granted access through an APB Out reader; a violation message is generated. Passive: A badge with an APB status of In will be granted access through an APB In reader; a badge with an APB status of Out will be granted access through an APB Out reader; a violation message is generated.
Archive	To copy history transactions from the database to magnetic tape. Some fields are expanded from IDs to descriptions. Archives are used for later examination of transactions; archives cannot be restored.
Area	A logical grouping of readers and doors; used to control access.
Array	A collection of independent disks which allow you to spread your data among two or more hard disks. See RAID.
Asynchronous Transfer Mode (ATM)	A fixed-route network protocol in which transmission packets have direct paths and destinations. ATM is an alternative to TCP/IP, which tags each packet with destination information in the header and can be routed through arbitrary paths on a carrier network such as the Internet.
Available Language	A language that can be used by Picture Perfect operators. A language must be supported by Picture Perfect and translated before it can be made available.

Table 127. Picture Perfect 4.5 terms explained (continued)

Term	Definition
BID	The hidden number that uniquely identifies each badge.
BIOS	Basic Input/Output System. The BIOS is a set of system instructions on a chip built in the computer.
Backup	To copy tables from the database to magnetic tape. A backup can be used to restore the system to a previous state or to recover from a failure.
Badge	A plastic card issued to each person who uses the facility. The system reads the information on the badge to determine whether or not to grant access to a person.
Badge Encode Number	The hidden number that uniquely identifies each badge.
Badge-Issue Reader	A reader assigned to a workstation used to issue a badge.
Badge Learn	Occurs when a micro checks with the host on an unknown badge and stores that badge information in its database. The next time the badge is presented to a reader connected to that micro, it will have the needed badge information.
Badge Reader	A device, usually located near a door, used to read badges. When a badge is presented to a badge reader, the system reads it and determines whether or not to unlock the door.
Badge Status	Indicates either the intended use of a badge (such as permanent or temporary) or its current condition (such as active or lost).
BAUD	A unit that measures the speed of transmission, such as for data through a modem.
Category	A “lock” and “key” that controls access. Each area and badge has one or more assigned categories. If a category on a badge matches any of the categories on an area, the badge works as a “key” in readers assigned to that area. A category assigned to an area functions as a lock; a category assigned to a badge functions as a key.
CMENU	A diagnostic program that runs on the console in order to monitor and control microcontrollers and X Terminals; can also be used to monitor database activity and configuration in the host or micro.
Code Set	A collection of character codes that express one or more languages. Picture Perfect only supports code sets defined by the International Standards Organization (ISO). Western European languages use the ISO8859-1 code set; Hebrew uses the ISO8859-8 code set.
Console	The host computer used for administrative functions (also called host console).
Coordinated Universal Time (UTC)	The mean solar time of the meridian of Greenwich, England, used as the basis for calculating standard time throughout the world.
Daemon	A continually running background process that is not controlled by a terminal. See Process.
Database	Picture Perfect configuration, transaction, and historical data stored on the hard disk of the host computer or the resident memory of a microcontroller. See Distributed Database and Relational Database.
Date Format	The order that the system requires for month, day, and year.
Devices	Physical peripherals such as disks, tapes, printers, networks, and serial port adapters for modems and lines of microcontrollers.

Table 127. Picture Perfect 4.5 terms explained (continued)

Term	Definition
DHCP	Dynamic Host Configuration Protocol (DHCP) is network protocol for automatically assigning TCP/IP information to client machines. Each DHCP client connects to the centrally-located DHCP server that returns the client's network configuration including IP address, gateway, and DNS servers. DHCP is useful for fast delivery of client network configuration.
Digital Input	A physical sensing device used to monitor an electronic contact connected to a microcontroller. Also called a DI.
Digital Output	A physical control device used to turn on/off an electronic contact connected to a microcontroller. Also called a DO.
Disk Array	See Array.
Disk Partition	A division of storage disks into physical or logical segments such that each segment acts as an independent component.
Distributed Database	Resident database downloaded to a microcontroller that allows independent decision-making and faster response time.
DNS	A service database that translates an IP address into a domain name.
Domain Name	The site's name that an organization uses. *Example: GE has a domain name of ge.com.*
Door	A database record that links the logical functions of a door with the door strike output, exit button, and door sensor inputs.
Door Forced Open	A logical alarm caused when the door opens without a valid badge read and the door contact reports the door-open state.
Door Open Too Long	A logical alarm caused when a door (unlocked by a valid badge read) remains open longer than the Allowable Open Time (a shunt time that starts when the door contact reports the door-open state).
Downstream	A relative position on a communication line originating at a host computer. *Example, the second micro on a line is "downstream" from the first micro.* See Microcontroller (micro).
Duress Code	A special PIN number used (on a keypad reader) to signal emergency situations.
Enabled Reader	A condition in which a reader is enabled to read badges. An enabled reader can be online or offline. See Online Reader and Offline Reader.
Encryption	The encoding of data for security purposes by converting standard data code into a proprietary code.
ENQ	An inquiry message to poll a micro to see if it is responding.
Facility	A facility is a partitioning of the records of the database of the security system.
Facility Profile	A facility profile is a permission set that an operator can access. The operator's facility profile can be different based on the facility to which it is assigned.
Firewall	A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.
Form	An electronic data-entry worksheet used to enter, find, view, or update data. A form may have input fields, pop-up lists, and pushbuttons for various functions.
Gateway	A network device or machine that connects a local private network to another network or the Internet.
Graphical Terminal	A terminal using a graphical interface for logging on to a desktop environment, such as Windows, GNOME Desktop Manager (GDM), XDM and KDM.

Table 127. Picture Perfect 4.5 terms explained (continued)

Term	Definition
Host	A host is generally a device or program that provides services to some smaller or less capable device or program.
Host Console	The host computer terminal used for AIX functions.
Informix	The relational database management system (RDBMS) used by the Picture Perfect system. See Relational Database.
Input	A digital input (DI) or a logical condition detected by the microcontroller. An input is assigned to an inputgroup.
Input Field	An area of the screen where an operator can type in information.
Input Group	A group of one or more digital inputs (or logical inputs) that can cause an alarm (and/or trigger output groups) when any (or all) inputs in the group are detected as true.
Insertion Point	A point (marked by a cursor) where the text that you enter will appear.
IP Address	A numeric address used by computer hosts to transmit and receive information over the Internet.
ISA	A type of bus conforming to the Industry Standard Architecture.
Keypad Override Code	See Shunt.
LAN	A Local Area Network. X Terminals are connected to the host computer using an Ethernet LAN.
Linux	Linux (often pronounced LIH-nuhks with a short "i") is a UNIX-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems. Linux has a reputation as a very efficient and fast-performing system. Linux is a remarkably complete operating system, including a graphical user interface, an X Window System, TCP/IP, the Emacs editor, and other components usually found in a comprehensive UNIX system. Linux is publicly open and extendible by contributors. Because it conforms to the Portable Operating System Interface standard user and programming interfaces, developers can write programs that can be ported to other operating systems.
Locale	A language and the location in which it is used. All languages in Picture Perfect are defined in terms of locale. Each language has a unique locale identifier. Picture Perfect uses the locale identifiers defined by AIX. Refer to the Operator's form for a list of locale identifiers.
Log on	The procedure used by operators to identify themselves to the system. To use the system, an operator must "log on" with a Login ID and Password. The Login ID is associated with a Permissions level that defines the functions an operator can perform. A Password provides secondary validation for that operator.
Log off	A security procedure that protects the system from unauthorized use. When an operator logs off, the system displays the Login screen and requires the next operator to log on.
LVM	Logical Volume Management. A kernel-level subsystem for managing multiple storage devices. Physical drive partitions are collected into logical volumes and provide dynamic resizing of logical volumes with the addition (or removal) of physical drives.
Message	Transaction information that the system displays.
Micro	See Microcontroller (micro).

Table 127. Picture Perfect 4.5 terms explained (continued)

Term	Definition
Microcontroller (micro)	The metal box containing the circuitry that controls the opening and closing of doors. Badge readers, alarm points, and digital output points are wired to micros, and micros are connected to the host computer. See Upstream and Downstream.
Mode	A set of schedules that defines how the system operates and specifies the characteristics of readers, areas, doors, and other system components. See Operating Mode.
Modem	Hardware device used to communicate between computer systems over telephone or other communications lines.
Monitoring	See Door Forced Open and Shunt.
Offline	A condition in which the micro is not communicating with the host computer.
Offline Reader	A condition in which a reader is not enabled to release the doorstrike when a valid badge read occurs. Access attempts at an offline reader can be routed to monitors, printers and online history.
Online	A micro is communicating with the host.
Online Reader	A reader is enabled to release the doorstrike when a valid badge read occurs. Access attempts at an online reader can be routed to monitors, printers and online history.
Open Too Long	See Door Open Too Long.
Operating Mode	The mode associated with a set of schedules that defines system operating specifications.
Output	A physical digital output (DO) that actuates devices such as a siren, a doorstrike, or lights, which can be triggered by an output group.
Output Group	A group of one or more outputs that can be triggered when activated by an associated input group.
Packet	See ACK Packet.
Password	A special code, used during login, that determines if an operator is authorized to log on to the system.
PCMCIA	A standard for PC cards. Adding a modem, network card, and removable disk drives (especially on portable computers) sometime requires the use of PCMCIA cards and compatible slots on computer systems.
Permissions	A level of operator permission to perform system functions. Each group of operators functions is a “permission group” that can be assigned to an operator authorized to perform those functions. See Log on and Password.
Physical Volume	A partition or segment of a storage disk that can be integrated into a one logical volume and controlled by logical volume management (LVM).
PIN #	A Personal Identification Number that identifies a person. If a facility uses both a keypad and badge reader, employees present their badge to the reader, then enter their PIN on the reader keypad.
Port Group	A single line of microcontrollers connected to a port.
Port Group Leader	The first microcontroller in the port group. See Port Group.
Primary Language	Language used by Picture Perfect for alarm notification, archive notification, describing alarms in the Alarm Monitor, and describing badge, input, and status activity in the Activity Monitor. These are always described in the primary language, even when viewed by operators working in a different language.
Priority	A number used to indicate the response priority of an alarm. The lower the priority number, the more serious the alarm.

Table 127. Picture Perfect 4.5 terms explained (continued)

Term	Definition
Process	One of many independent programs running at the same time in the computer.
Provided Language	A language whose translations are provided by GE. All provided languages are available at installation.
RAID	The use of two or more disk drives in a single computer system, which can provide better disk performance, error recovery, and fault tolerance.
RAN	Remote Alarm Notification. An optional package which, when installed, routes alarms from the Picture Perfect system to a remote (non Picture Perfect) system. The alarms can then be processed by and responded to, from the remote system.
Readers	Badge readers are devices connected to the system that read the encoded badge numbers. They are usually located near doors or gates, or in elevators that the system controls.
Redundant System	A Picture Perfect redundant system detects faults and automatically transfers the workload to the backup host. The transfer of control from the primary host to the backup host occurs rapidly to ensure that there is almost no loss of data or alarms.
Relational Database	A database that uses a table structure to store data. Relationships among tables are logically specified at the time of user access into the database; they are not built into the data structures themselves.
Response	Text that the operator selects or types when answering an alarm.
RS-232	A standard method of transmitting data across serial cables, used by modems, printers, and other serial devices.
Schedule Event	A time-dependent change to a mode, area, reader, door, alarm, input group, or output group. See Operating Mode.
SCSI	A high-speed interface that can connect to computer devices such as hard drives, CD-ROM drives, and tape drives. SCSI is pronounced as "Scuzzy."
Semaphore	In programming, especially in UNIX-based systems, semaphores are a technique for coordinating or synchronizing activities in which multiple process compete for the same operating system resources. A semaphore is a value in a designated place in operating system (or kernel) storage that each process can check and then change.
Server	Generally, a server is a computer program that provides services to other computer programs in the same or other computers. In the client/server programming model, a server is a program that awaits and fulfills requests from client programs in the same or other computers.
Shunt	Override an alarm on a door contact that detects an open state on the door. A digital input device monitors the door state. If the door opens with a valid read (or exit device), the input device (a door contact) detects a state change but does not report the change until a shunt time elapses. The shunt time allows the badgeholder enough time to get through the door. See Door Forced Open and Door Open Too Long. To override a door sensor for a longer time, enter a keypad override code (a microcontroller-dependent code set on the Micros screen).
Shutdown	To stop running the application and the operating system.
SSL	SSL (Secure Sockets Layer) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

Table 127. Picture Perfect 4.5 terms explained (continued)

Term	Definition
Subnet	Network nodes that are related by the same IP address range. *Example: computers with an address beginning with 192.168.1.x are in the same subnet*.
Subnet mask	A 32-bit address used in conjunction with an IP address to segment network traffic; used to restrict transmissions to certain subnets.
Status	The current condition of something, such as a badge or a micro. The Status monitor is used for viewing a micro's current database to verify configuration and scheduling.
Supported Language	A language that can be used in Picture Perfect. All languages other than English and French must be translated and made available before they can be used.
SYN	A message from the host that synchronizes the micro's clock.
System Administrator	A full-function operator; an operator permission without any function restrictions.
TCP/IP	Communications protocol used to connect to a variety of different types of hosts on both private networks and carrier networks such as the Internet.
TPS	Transaction Processing System; the program that communicates with microcontrollers.
Transaction	Microcontroller activity.
TTY	In UNIX-based operating systems, any terminal at all; sometimes used to refer to the particular terminal controlling a given job. Also the name of a UNIX command which outputs the name of the current controlling terminal.
UDP	A communications protocol for the Internet network layer, transport layer, and session layer, which makes it possible to send a datagram transmissions from one computer to a recipient computer.
UNIX	A multi-user, multitasking network operating system developed at Bell Labs in the early 1970s. Linux is based on, and is highly compatible with, UNIX.
Unlock Time	The length of time a door latch is to remain unlocked after a valid badge read (or after an exit button activates). This time allows the badgeholder to open and pass through the door.
Upstream	A relative position on a communication line originating at a host computer. *Example: the second micro on a line is "upstream" from the third micro, because the second micro is relatively closer to the host*.
Workstation	An X Terminal that displays the forms that the operator uses to interact with the system; connected to the host computer using an Ethernet LAN (Local Area Network). See LAN.
xdm	The login utility used to allow an operator to log on to an X Terminal. The operator uses an xdm window to enter a Login ID and a Password. The X Window Display Manager (xdm) is the program that controls workstation windows.
X Terminal	The computer monitor that displays the screens that the operator uses to interact with the system. Also called a workstation.
X Window System	A portable network-transparent window system that handles graphics and multiple fonts in a hierarchy of windows on a wide variety of bit-mapped display devices.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X