



# P2000

Security Management System

---

## Quick Reference Guide

for P2000 Operators

---

PRELIMINARY

Copyright 2011  
**Johnson Controls, Inc.**  
All Rights Reserved  
(805) 522-5555  
[www.johnsoncontrols.com](http://www.johnsoncontrols.com)

No part of this document may be reproduced without the prior permission of Johnson Controls, Inc.

Cardkey P2000, BadgeMaster, and Metasys are trademarks of Johnson Controls, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

These instructions are supplemental. Often they are supplemental to other manufacturer's documentation. Never discard other manufacturer's documentation. Publications from Johnson Controls, Inc. are not intended to duplicate nor replace other manufacturer's documentation.

Due to continuous development of our products, the information in this document is subject to change without notice. Johnson Controls, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with furnishing or use of this material. Contents of this publication may be preliminary and/or may be changed at any time without any obligation to notify anyone of such revision or change, and shall not be regarded as a warranty.

If this document is translated from the original English version by Johnson Controls, Inc., all reasonable endeavors will be used to ensure the accuracy of translation. Johnson Controls, Inc. shall not be liable for any translation errors contained herein or for incidental or consequential damages in connection with the furnishing or use of this translated material.

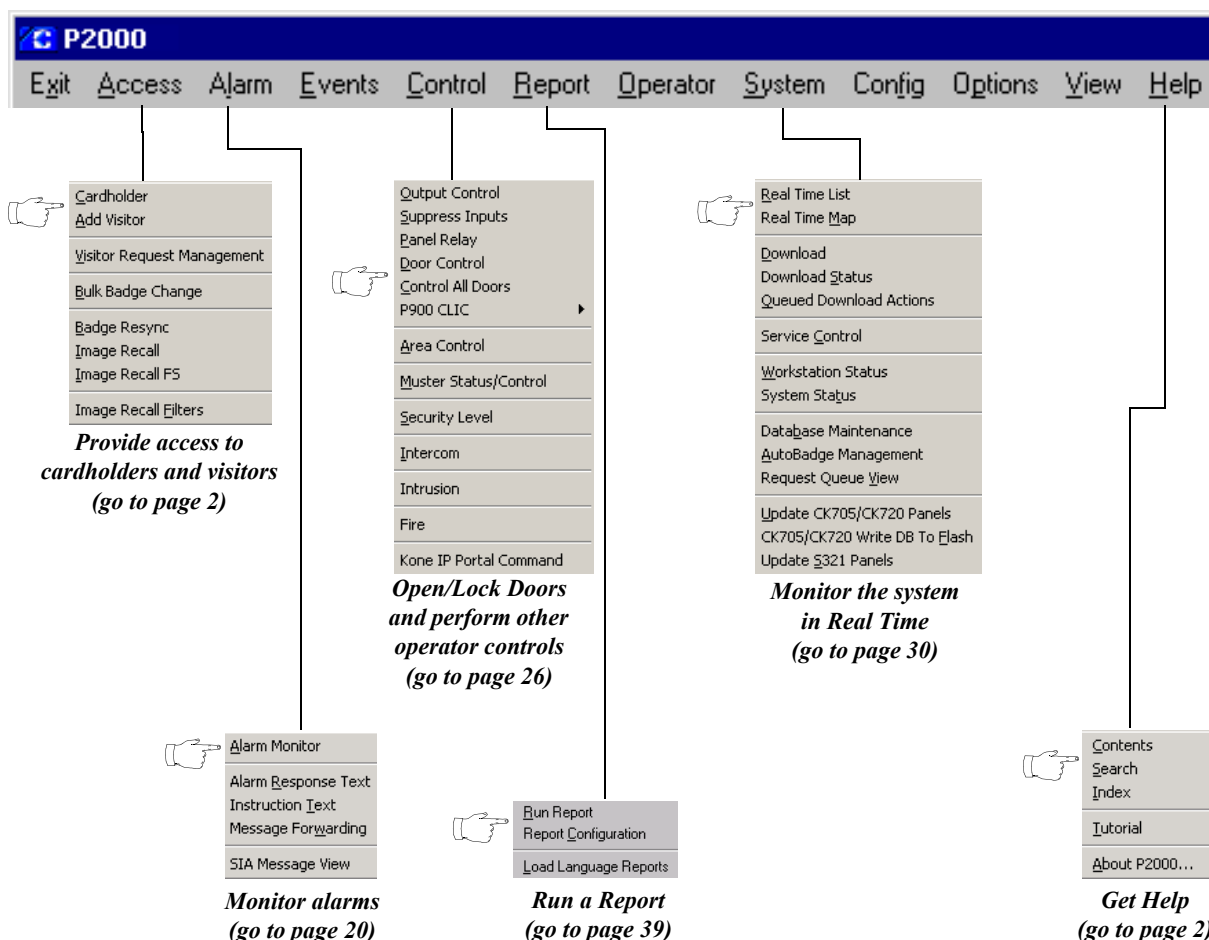
PRELIMINARY

# P2000 Quick Reference Guide

This guide describes procedures typically performed by operators of the P2000 Security Management System. Your system administrator must complete all configuration steps outlined in *Chapter 2: Configuring the System* in the *P2000 Software Users Manual*, before you can program and use the essential functions described in this guide. If configuration is not completed, some of the functions described here will not be ready to operate. Some system features require specific configuration settings before others can be enabled.

Operations typically performed as part of system maintenance; such as downloading data, updating software and panels, starting and stopping service control, and reviewing system and workstation status, must also be performed by a system administrator and are described in *Chapter 5: System Maintenance* in the *P2000 Software Users Manual*.

## Where to go when you want to .....



## Get Help!

Help is available from most P2000 windows or dialog boxes, by pressing <F1>. Once you press <F1>, help text for the selected item displays in a separate window.

The P2000 software contains virtually the entire Software User Manual in online documentation accessed via the **Help** option on the Main menu. You can access information under each of the topics or use the Index to search for specific topics.

## P2000 Tutorial

The tutorial presents an overview of the P2000 security system's major features and options. It also covers a number of system configuration, installation, and troubleshooting tips. Adobe® Flash is required to run the tutorial and can be installed when you launch the tutorial program from the **Help** option in the P2000 menu bar.

The modular design enables navigation to all or specific tutorial topics. The tutorial introduces topics and sub-topics, which are discussed through Flash presentations that provide audio narration (with matching text if desired) to guide users on how to make the most of P2000's main popular features. Software screenshots are used to walk the user through actual configuration and installation steps.

## Provide Access to Cardholders and Visitors

Access privileges define which cardholder or visitor may enter a specific area of the facility, and at what time they may enter. Access privileges are assigned to individual reader terminals and/or group of reader terminals; these devices are assigned to specific access groups, and then when cardholder records are added to the database, the cardholders are assigned to the access groups.

The software provides flexible tools to create cardholder records and assign badges with which to grant

or deny facility access. At a minimum, you must enter a first and last name into the Cardholder database for each person who will have access to your facility. Additional cardholder information can include personal information such as address and phone; company information such as a company name and department; a Photo ID; and any additional information such as car make, parking assigned, or other information defined in User Defined Fields.

## Entering Cardholder Information

Every person who needs access to the facility must have a Cardholder and Badge record entered into the P2000 system. Cardholders can be entered all at once at system startup, and then added, edited, or removed as necessary thereafter. Permanent cardholders and visitor cardholders are viewed and added in the same Cardholder window.

If you use database partitioning, the cardholder can belong to one partition, and could have multiple badges, each in a different partition with different access parameters.

## Viewing Cardholder Information

1. Select **Access>Cardholder** from the P2000 Main menu to open the Cardholder window.

2. To view current cardholder information, select a **Type** from the drop-down list at the right side of the window (All, Regular, or Visitor).

**Note:** The system displays up to 20,000 cardholders at a time, for the partition selected in the **Partition** field. If the number of cardholders in your system exceeds 20,000, use the Search feature, described on page 7, to display specific data.

## Cardholder Types

**Regular** – These are the permanent cardholders in the system. Their access begins with a start date, but unless terminated or temporarily reassigned, no end date will be specified. Select Regular from the Cardholder window Type drop-down list to view only the regular cardholders.

**Visitor** – A visitor is given temporary access to the system on a limited basis. Their access will be limited by start and end dates and times, and they are assigned a company Sponsor to take responsibility for them while visiting the facility. Select Visitor from the Cardholder window Type drop-down list to view only visitor cardholders in the system.

**All** – Select to display all cardholders currently in the system, regardless of cardholder type.

## Additional Cardholder Data

When you select a cardholder from the list, additional cardholder data displays in the tabs in the middle of the Cardholder window, such as:

- Image, Address, Other, Start/End Badges, and UDF information.
- If the cardholder selected is a Visitor, a Sponsor tab is added to the window and displays Sponsor information.
- Regular cardholders display the Sponsored Visitors tab, which displays the visitors sponsored by the selected cardholder.
- If your facility uses P2000 Enterprise, a Site field is added at the top of the window, which allows you to view only cardholders that belong to the selected Site name. In addition, the Enterprise Sites tab is also added to the window to display the site names assigned to the cardholder.

## To Enter Cardholder Information:

1. From the Cardholder window, click **Add**. The Cardholder dialog box opens at the Cardholder Edit tab.

2. Enter the information as described in the following Cardholder Field Definitions section. Required fields are indicated by an asterisk and must be completed before a record is saved.
3. Click **Apply** at any time to save your settings. When you finish click **OK** to return to the Cardholder window, the name of the newly added cardholder will display highlighted in the list box.

## Cardholder Field Definitions

### Cardholder Tab

**Partition** – If this is a partitioned system, select the Partition to which this cardholder is assigned.

**Public** – If this is a partitioned system, select the Public check box if you wish this cardholder record to be visible to all partitions.

**Type** – Select Regular or Visitor. If you select Visitor, the Sponsor box at the bottom of the window is activated. (See “Sponsor” on page 4 for more information.)

**First** – Enter the first name of the cardholder.

**Middle** – Enter the middle name of the cardholder.

**Last** – Enter the last name of the cardholder.

**ID** – This field displays the ID number that was automatically assigned from the Automatic Employee ID pool numbers. Depending on your settings, this field may allow editing.

### Address

Address fields are optional, unless they are defined as required fields in your facility. Enter the suite, street, city, state, Zip, phone number, and extension, if required.

### Other

**Email** – If available in your facility, enter the email address assigned to this cardholder.

**Company and Department** – Select a Company and/or Department from the drop-down lists. Your system administrator must create Companies and Departments before the selections will display in the drop-down lists.

**Guard** – This field is used with the Guard Tour feature and allows you to assign Tour Badges to cardholders who will participate in guard tour operations.

### All Badges

**Start** – This is the date and time that badges become active. Select the check box and click the down arrow to select a start date. This date will apply to all badges assigned to this cardholder. After you select a start date, the time field is enabled. Click the spin box buttons to select the time that badges will be activated.

**End** – This is the date and time that badges will be voided. Select the check box and click the down arrow to select an end date. This date will apply to all badges assigned to this cardholder. This box is typically used for Visitor badges, but can also be edited as needed to void badges for a terminated employee or similar application. The system will automatically void the badge on the date specified. After you select an end date, the time field is enabled. Use the spin box arrows to select the time that badges will be voided.

**Note:** If you create a Visitor badge and do not enter an End date and time, the date and time will default to the Visitor Validity Period value specified in your Site Parameters setting.

### Web Access

**Menu Permission Group** – If your facility uses the Web Access feature, select the permission group that will be assigned to this cardholder. The cardholder will be allowed to perform any Web Access function defined in this permission group.

**Password** – Enter the password that the cardholder will use to log on to the P2000 Web Access site.

### Enterprise

If your facility uses P2000 Enterprise, the Enterprise box will display all the sites defined in the system. Select the check box next to the site that this cardholder may access.

### Sponsor

If you selected **Visitor** as the Cardholder Type, the Sponsor box is activated. A sponsor is the name of the cardholder responsible for the visitor.

## To Enter a Visitor Sponsor:

- Once the Sponsor box is activated at the bottom of the Cardholder Edit dialog box, after you select **Visitor** as the Cardholder Type, click **Select**. The Cardholder – Find Sponsor dialog box opens.

First	Middle	Last	ID	Company
Jeff	R.	Evans	124	
James	A.	Jasper	12346	
Jane	T.	Smith	123	

2. Enter a value in any of the fields. The list box will display the cardholder records that match the entered values.
3. Select a cardholder name and click **OK** to save the setting and return to the Cardholder Edit dialog box. Basic Cardholder information displays in the Sponsor box.

This information will also display in the Sponsor tab of the Cardholder window.

In addition, when you select a sponsor name from the Cardholder window and click the Sponsored Visitors tab, the list displays all visitors sponsored by the selected cardholder. If you double-click a visitor name in the list, the visitor becomes the selected cardholder.

## Adding a Cardholder Image

You can import an image to display in the Cardholder Image tab. The P2000 system supports a large number of image formats; however, if your image format is not supported, you may need to use an image-editing program to convert to a supported format.

If the workstation is configured as a badging workstation, you can use the Badging buttons to capture an image.

## Adding a Cardholder Journal

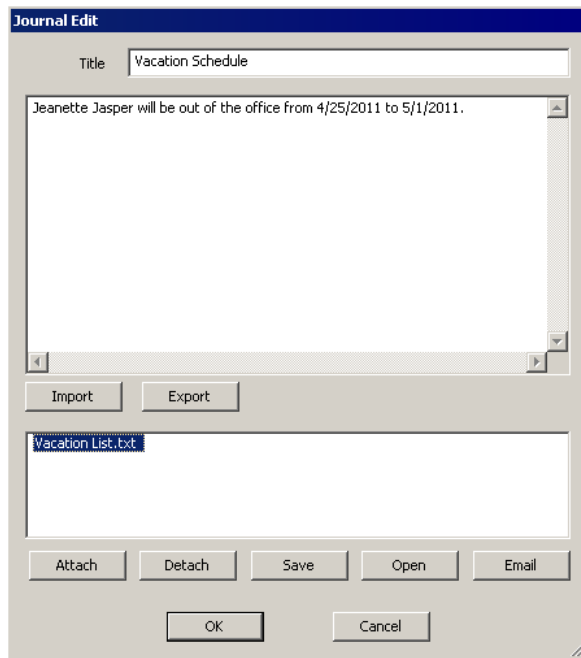
Journal entries supplement cardholder information by storing notes associated with each cardholder. For example, you may want to keep track of cardholders with parking violations, or keep a record of cardholders that attended specific company training, or track cardholders with suspicious behavior.

### To Enter Journal Entries:

1. Select a cardholder from the Cardholder list.
2. Click the **Journal** button located in the Image tab in the center of the window. The Journal dialog box opens displaying the journal entries associated with the cardholder together with the date and time when the journal was entered, the name of the operator who last edited the journal, the date and time the journal was last edited, and whether there is an attachment file associated with the journal entry.

Date	Title	Edited By	Edit Time
3/29/2011 3:20:16 PM	Vacation Schedule	SJones	3/29/2011 3:27:40 PM

3. Click the **Add** button. The Journal Edit dialog box opens.



4. Enter a descriptive **Title** to identify the subject of this note.
5. Click in the text area and enter the details of the note.
6. If you wish to add additional information to the note, click the **Import** button and navigate to the directory that contains the text file you want to include. Select the file and click **Open**. The text file will display in the text area.
7. If you wish to save the note as a text file, click the **Export** button and navigate to the directory where the exported notes will be stored. Enter a file name and click **Save**.
8. If you wish to attach a file to the journal entry, click the **Attach** button and navigate to the directory that contains the file you wish to attach. Select the file and click **Open**.
9. If you do not wish to use the attachment file, select the file and click the **Detach** button. The attachment file will be removed from the list.
10. If you wish to save the attachment file, click the **Save** button and navigate to the directory where the attachment file will be stored.
11. If you wish to view the contents of the attachment file, click the **Open** button.
12. To e-mail the attachment file, click the **Email** button. The program will launch your default email

client with the file attached. Check with your Internet Service Provider (ISP) or IT department to verify the required email client settings.

13. When you finish with the note details, click **OK** to save the entry and return to the Journal dialog box.
14. To view the contents of a note, select the note from the list and click **View**. When you finish viewing the note, click **Cancel**.
15. If you wish to modify an existing note, select the note from the list and click **Edit**; make your changes, then click **OK**.
16. To delete a note, select the note from the list and click **Delete**. You will be prompted for verification.
17. When you finish with the Journal entries, click **Exit**. The Journal button will display the number of notes associated with the cardholder.

## User Defined Fields

After your system administrator creates User Defined Fields, use the UDF tab in the Cardholder dialog box to enter additional cardholder information. The number of UDF tabs displayed depends on the number of UDF fields created. Select additional UDF tabs and enter the data as needed.

**Note:** The UDF tab only displays the user defined fields that your system administrator assigns to the operator using the Concealed UDFs feature.

## To Enter User Defined Field Information:

1. Select a cardholder from the Cardholder list.
2. Click the **Edit** button on the right side of the window. The Cardholder dialog box opens.
3. Click the **UDF 1** tab to display the user defined fields. Required fields are indicated by an asterisk and must be completed before a record is saved.



**Cardholder Edit: UDF 1**

Hire Date: 2/12/2009

Car Color: Red

Car Model: Toyota

Car Year: 2004

Parking Access: ☒

Parking Area: West Entrance

\*License Plate: 2T896133

Parking Usage: Monthly

- After you enter the information, click **OK** to return to the Cardholder window.
- Click the **UDF** tab located in the middle of the Cardholder window. The User Defined Fields and entries display for the cardholder selected.

Field	Value
Hire Date	2/12/2009
Car Color	Red
Car Model	Toyota
Car Year	2004
Parking Access	Yes

## To Search for Specific Cardholders:

- In the Cardholder window, click the **Search** button on the right side of the cardholder list. The Database Search dialog box opens.

**Database Search**

First Name:

Middle Name:

Last Name: Jasper

ID:

Company: <all>

Department: <all>

Car Model: Toyota

<none>

Badge Number:

Badge Reason: <all>

Badge Purpose: <all>

Clear

Partial Match Exact Match Cancel

Click to select a UDF

Enter UDF search criteria

- Enter or select from the associated drop-down lists, the information for any or all of the fields to search for specific cardholders.
- If you wish to search by **Company** and/or **Department**, select a previously defined name from the drop-down list.
- You can also search by UDF (up to two UDF fields). Select any of the previously defined UDFs from the drop-down lists (Date type UDFs cannot be included in the search). Then enter the UDF search criteria in the associated fields. (Fields associated with Selection type UDFs are selected from drop-down lists.)

**Note:** The UDF list only displays the UDF fields associated with the operator record.

- If you wish to clear the existing search criteria, click the **Clear** button.
- After you define the search criteria, click one of the following buttons:

**Exact Match** – to display an exact match to your search criteria.

**Partial Match** – to display all possible selections that match the initial characters of the search criteria, for example if you enter *Carl* in the First Name field, the list box will display names such as Carla, Carlos, Carlton, etc.

- The Cardholder window opens showing the number of cardholders and the match specified in the search criteria.

**Cardholder**

Site: Simi Valley

Partition: Super User

Iname = 'Jasper' udf = 'Toyota'

First	Middle	Last	Type	Guard	Partition	Public
Carol	R.	Jasper	Regular	No	Super User	No
James	A.	Jasper	Regular	No	Super User	No

Image Address Other Start/End Badges UDF Enterprise Sites Sponsored Visitors

Field Value

Hire Date 2/12/2009

Car Color Red

Car Model Toyota

Car Year 2004

Parking Access Yes

2 Cardholders

Search Criteria

Number of Cardholders

- Click the **All** button on the right side of the Cardholder window to restore it to display all cardholders.

## Entering Badge Information

The Badge Information box in the Cardholder window displays all badge information for the cardholder selected from the Cardholder list. A badge can be created strictly for identification, or it can be assigned access privileges.

### To Enter Badge Information:

- In the Cardholder window, select a cardholder from the Cardholder list.
- In the **Badge Information** box at the bottom of the Cardholder window, click **Add**. The Badge dialog box opens.

**TIP:** You can also access the Badge dialog box from the Cardholder Edit tab by selecting **Create Badge** at the bottom of the window.

- Enter the information as described in the Badge Field Definitions.

- When all information is entered, click **OK** to return to the Cardholder window. The new badge will be listed in the Badge Information box at the bottom of the window.

---

**Note:** Use the **Duplicate** button at the bottom of the Badge dialog box to create any number of badges for a cardholder. All current badge information will be copied; however, each badge must have a unique number.

---

## Badge Field Definitions

### Badge

**Partition** – If this is a partitioned system, select the Partition in which this badge will be active.

**Public** – Select Public if you wish this badge record to be visible to all partitions.

**Number** – Enter a badge number (the number of allowed characters depends on the parameters selected in Site Parameters). This number is usually pre-assigned to badges provided by Johnson Controls. Access and Identification badges can have the same number, however each access badge must have a unique number. If your system is configured to use FASC-N badges, see “FASC-N Badges” on page 9 for instructions on generating this number.

**Auto** – If your facility is set up to use the AutoBadge Management feature, click the Auto button to insert the next available badge number in the Number field. Not available for FASC-N badges.

**Facility Code** – Select from the drop-down list the facility code to be assigned to this badge. Facility codes are defined in Site Parameters and identify the badges that belong to your particular site. Not available for FASC-N badges.

**Alpha** – Some custom badges may provide space for additional characters. If so, enter them here. (Limited to 4 characters.) Not available for FASC-N badges.

**Issue** – If a cardholder loses a badge, you would give him/her the next available issue level and retain the same badge number. The number of badge issue levels supported depends on your panel type.

**Description** – If desired, enter a description of this badge. (Up to 32 characters.)

**Pin** – Enter the cardholder or visitor personal identification number (PIN) to be used with PIN readers. If an algorithmic PIN is used, leave this field blank.

**Start** – Select the date and time this badge becomes active. Click the down arrow to select a date; then click the spin box buttons to select a time.

**End** – Select the date and time this badge will be automatically voided. Click the down arrow to select a date; then click the spin box buttons to select a time. If this is a Visitor badge and no End date and time is entered, the badge will be automatically voided as configured in Site Parameters.

**Type** – Select a badge Type from the drop-down list. Choices are: Access or Identification.

**Format** – Select from the drop-down list, the badge format to be assigned to this badge. Your system administrator must create Badge Formats before the selections will display in the drop-down list.

**Purpose** – If you wish to include this Badge information, select a Purpose from the drop-down list to indicate the badge's intention. Your system administrator must create Purpose fields before the selections will display in the drop-down list.

**Reason** – Select a Reason from the drop-down list to indicate why the badge is being issued. Your system administrator can add or edit badge reasons using the Edit Badge Reason application.

**Design** – If your system administrator has created badge designs using the Video Imaging software, you can select a design from the drop-down list.

### FASC-N Badges

The P2000 software supports the programming of smart cards that are compliant with the Government Smart Card Interoperability Specification (NIST IR 6887 - 2003 Edition, GSC-IS Version 2.1). These smart cards are programmed using a smart card encoder, physically located in the badge printer.

**Note:** *Smart card encoding is only available if the Video Imaging software option used at your facility is EPI Builder.*

To support the Federal Government smart card encoding protocol, an encoded badge must include FASC-N (Federal Agency Smart Credential Number) data fields. A FASC-N badge number is a unique number assigned to one individual. This type of badge is typically issued to government employees; however, it could also be used by any industry. Data elements in this number determine whether a cardholder should be granted access to specific buildings and controlled places.

To create FASC-N badges, your system administrator must define the Badge Edit Style as **FASC-N Only** or **Normal and FASC-N**.

- If **FASC-N Only** was selected, click the **Add** button in the Badge Information box at the bottom of the Cardholder window, or click the **Create Badge** button in the Cardholder Edit tab.
- If **Normal and FASC-N** was selected, click the **Add** down arrow in the Badge Information box at the bottom of the Cardholder window and select **Add FASCN**. The **Create Badge** button in the Cardholder Edit tab will only allow you to create FASC-N badges.
- To create Normal badges if **Normal and FASC-N** is selected, click the **Add** down arrow in the Badge Information box at the bottom of the Cardholder window and select **Add Normal**.

When the badge dialog box opens, the fields will display the default values defined in Site Parameters to generate a 15-digit badge number as described below.

**Number** – This is a six-digit unique badge number assigned to the cardholder.

**System** – This is a four-digit number identifying the specific government site or facility issuing the badge, that way each site within a government agency will have a system number which is unique to that agency.

**Agency** – This is a four-digit unique number identifying the government agency issuing the badge.

**Series** – This is a one-digit number that can be left to the discretion of the site administrator as to how this number can be used.

**Generated** – This box displays the generated number containing the 15 digits as follows:

AAAASSSRNNNNNN

where *A* is the Agency code, *S* is System code, *R* is Series, and *N* is the Credential Number.

The Agency, System, and Series default values will be used for all badges created in the system; however, an authorized operator can enter specific values for a specific badge. The [...] button on the right side of the Series field opens the FASC-N Fields dialog box.

You can change any of the default values, which will be used instead of the configured default values for the badge currently being edited. If you want to go back to the default values, click the **Defaults** button.

Once the badge record is saved, and if the Badge Edit Style used at your facility is **Normal and FASC-N**, you can edit the badge and use the **Change Style** button at the top right corner of the window to change the badge style, if necessary.

## Security Options Tab

These options allow you to define access privileges for a cardholder. Access decisions are made based on the privileges assigned to the badge.

**Note:** Some security options are panel specific. See Appendix C: Panel Comparison Matrix in the P2000 Software User Manual for a detailed list of features and capabilities supported by your panel type.

In Enterprise systems, the Badge dialog box displays the site name tabs of the sites assigned to the cardholder. The first tab is always the local site tab and is used to assign local access privileges. The second tab is the Enterprise tab and is used to assign global access privileges. Additional tabs show other site names assigned to the cardholder.

Assigning access privileges is determined by the following conditions:

- When you define access to the local site, and select the **Apply Security Options 'Enterprise'** check box, the security options defined in the Enterprise tab will be applied.
- When you define access at a different site, and select the **Apply Security Options 'Enterprise'** check box, the security options defined in the Enterprise tab will be applied to that site.

**Disabled** – When a badge is created, it is automatically enabled. Select this check box to disable this badge. This function is useful when you wish to disable a badge, but do not wish to re-issue or redefine a badge for this cardholder.

**Executive** – If enabled, the cardholder will have unlimited access to all operational doors controlled by the access control system, regardless of any other privileges programmed for this badge. (If a specific terminal requires the use of a PIN code with a badge, the PIN code is still required.)

**Trace** – Enable to trace cardholder movement throughout the facility. Badge transactions will be printed, as they occur, on any printer configured to print trace transactions, as long as the Badge Trace and Printing options are selected in the Real Time List window.

**Override** – If enabled, the cardholder can unlock any door controlled by a keypad reader that has the Override option enabled.

**Download to STI-E** – This option applies only to legacy panels using STI-E terminal interfaces. If selected, the badge is downloaded to the STI-E terminal. The STI-E terminal can save up to 1,000 badges in a resident database for use if the panel becomes inactive.

**Special Access** – Enable any of the three special access flags defined by your system administrator, if the cardholder requires special access at a reader. Special access allows a door's access time to be different.

## Security Level

Select a security level number from 0 (lowest) to 99 or the maximum security level set up at the Site Parameters dialog box. To obtain access at a door, this number must be equal to or greater than the security level set up at the terminal. If the security level at the terminal is raised, cardholders will be denied access, unless the badge has the Executive privilege enabled.

## Event Privilege

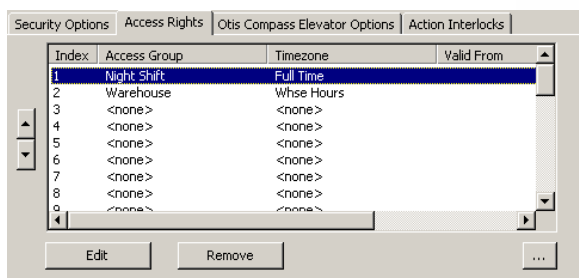
Every badge has an event privilege level, ranging from 0 to 7, with zero as the lowest level. If a cardholder's badge is to initiate a card event, his/her event privilege level must be equal to or greater than the privilege level defined in the Panel Card Event dialog box.

## Guard Tour

The Priority field is used with the Guard Tour feature. Select a priority number from 1 (lowest) to 99. This number determines which tours the selected cardholder can perform. Only tour badges with equal to or greater than this priority can perform a tour.

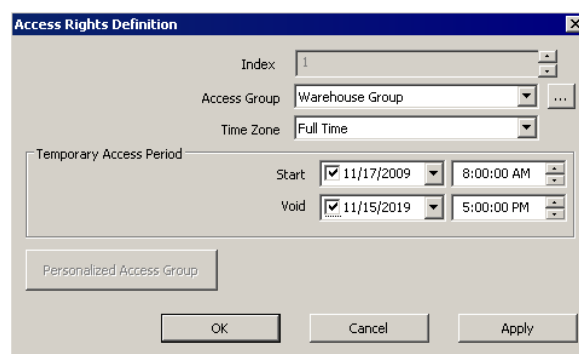
## Access Rights Tab

Use this tab to define the Access Groups and corresponding Time Zones that will be assigned to this badge. The number of groups displayed depends on the values selected in Site Parameters.



## To Define Access Rights:

1. In the Access Rights tab, double-click the line item you wish to define. The Access Rights Definition dialog box opens.



2. The **Index** number automatically displays. Select from the drop-down list, the **Access Group** you wish to assign to this badge.
3. If you wish to modify the settings in the selected Access Group, click the [...] button to open the Access Group Edit dialog box. Make your changes and click **OK** to return to the Access Rights Definition dialog box.
4. In the **Time Zone** field, select a time zone that will be assigned to the selected Access Group. If the Access Group selected includes P900 terminals, the system will use the default time zone defined for each P900 terminal, regardless of the time zone selected here.
5. If you wish to define a **Temporary Access Period** for the selected Access Group, select the check box and use the drop-down lists to select the **Start** date and time when permission for access will be granted. If the check box is not selected, access will be allowed immediately.

**Note:** For example, if the reader doors included in the Access Group normally grant access from 8:00 A.M. to 5:00 P.M., you can set up temporary access on a selected date and time period that will grant the cardholder permission for limited access within the normal time zone. This feature is performed by the Smart Download service and only works on terminals running in Local mode.

6. Select the **Void** check box and use the drop-down lists to select the stopping date and time when permission for access will expire.
7. Click **Apply** to save your settings. To assign another access group to this badge or see other definitions, click the spin box next to the Index field.
8. To define personalized settings, click the **Personalized Access Group** button and enter your set-



tings. See “Personalized Access Groups” at the end of this section.

9. Click **OK** to return to the Access Rights tab.
10. To remove a definition, select the line item and click the **Remove** button.
11. The list displays the access groups assigned to the badge. To edit an access group, select the line item and click the [...] button.

## Personalized Access Groups

When assigning access groups to a badge, you can use personalized access group for each cardholder. The Personalized Access Group button provides a shortcut to set up access groups without the need of scanning through all existing access groups.

By default, the Name of the access group will always be the name of the cardholder. However, be aware that the name of the access group is NOT automatically modified if you change the name of the cardholder.

Once you have all the access group elements defined, such as terminals, terminal groups, elevators or cabinets, click **OK**. The new personalized access group will display automatically in the Access Group field. Assign a time zone to the new access group as you would for any other access group.

**Note:** Although initially created for a particular cardholder, a personalized access group becomes a standard access group within the P2000 system and CAN also be assigned to other cardholders.

## Access Template

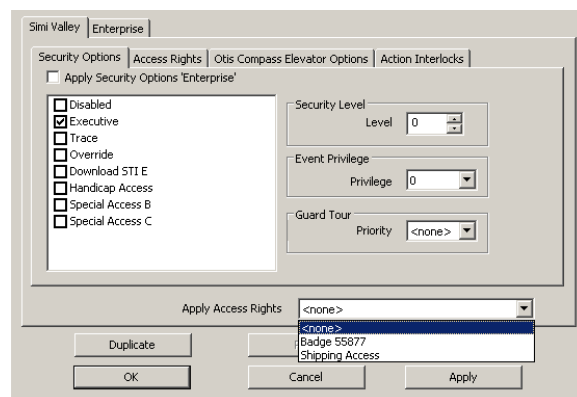
If a large number of cardholders will use badges having the same options, your system administrator can set all badge options at once by applying an Access Template. The Access Template contains preset badge options, access groups, and time zones, and will override any settings already defined in the Badge dialog box, before the template was applied. You can edit badge options individually after the template is applied; if you re-select the template, the settings will again mirror the template settings. In addition, if changes are made to an Access Template, you will have to re-select the template to apply the new settings.

**Note:** Access Templates must first be created before they are available in the Badge dialog box.

**Note:** In addition to selecting Access Templates from the **Apply Access Rights** drop-down list, you can also select another badge owned by the same cardholder and apply the same access rights from the selected badge.

## To Apply Access Rights to a Badge:

1. From the **Apply Access Rights** drop-down list, at the bottom of the Badge dialog box, select the Access Template or badge number you wish to apply to the badge. All access options defined for the Access Template or selected badge number, will be applied to the badge.



2. If you wish, you can change specific options, access groups, or time zones for this badge. All other settings will remain in effect.

## Viewing Badge Data

Badge information such as Number, Status, Options, Type, Partition, and Access Group displays in the list box at the bottom of the Cardholder window. When you select a cardholder from the list, all badges assigned to that cardholder display in the Badge Information box. You can also display the badge's transaction history.

## To Display Badge Transaction History:

1. In the Cardholder window, select a cardholder from the list.
2. In the **Badge Information** box, right-click the badge number you wish to view.
3. From the shortcut menu select **Transaction History**. The Badge Transaction History dialog box opens displaying the selected Cardholder name and Badge number.

Date	Type	Location
7/20/2005 8:57:05 AM	Access Granted Local	North Entrance, Security
7/20/2005 8:55:26 AM	Invalid Card Timezone	North Entrance, Security
7/20/2005 8:54:43 AM	Invalid Card Timezone	North Entrance, Security
7/20/2005 8:53:26 AM	Invalid Reader	North Entrance, Security
7/20/2005 8:53:13 AM	Invalid Reader	North Entrance, Security

The list box displays the date, transaction type and location where the badge was presented.

4. To change the number of transactions displayed, enter the desired number in the **Num Records** field.
5. To update the list box with new data, click the **Refresh** button.
6. Click **Done** to close the dialog box.

## Bulk Badge Change

The Bulk Badge Change tool is used to change badge parameters across multiple records, in a single operation. This feature not only allows you to save time by modifying multiple records at once, but also improves the accuracy from single record editing, and avoids the hassle of updating badge records one entry at a time. In addition, you can also delete multiple badges and/or associated cardholder records at the same time.

## To Bulk Change Badge Records:

1. From the P2000 Main menu, select **Access>Bulk Badge Change**. The Bulk Badge Change dialog box opens.

Badge	First Name	Middle Name	Last Name	Type	Company	Department	Reason	Purpose
3031	Charles	J.	Anderson	Regular		Accounting	New	
3033	James	D.	Carler	Regular	XYZ Security	Accounting	New	ABC Airlines
3055	Robert	L.	Smith	Regular		Accounting	New	
3066	Ann	F.	Evans	Regular		Accounting	New	
3075	James	D.	Carler	Regular	XYZ Security	Accounting	New	ABC Airlines
312	Brenda	T.	Covington	Regular	ABC Industries	Accounting	New	

2. Enter or select from the associated drop-down lists, the information for any or all of the fields to search for specific cardholder records.
3. If you wish to search by **Company** and/or **Department**, select a previously defined name from the drop-down list.
4. You can also search by UDF (up to two UDF fields). Select any of the previously defined UDFs from the drop-down lists (Date type UDFs cannot be included in the search). Then enter or select the UDF search criteria in the associated fields.
5. If you wish to search for badges that have not been used for a while, enter in the **Badge Unused For** field the number of days that the badges have not been used.
6. After you define the search criteria, click one of the following buttons:

**Exact Match** – to display an exact match to your search criteria.

**Partial Match** – to display all possible selections that match the initial characters of the search criteria, for example if you enter *Carl* in the First Name field, the list box will display names such as Carla, Carlos, Carlton, etc.

7. Once the list box displays the cardholders specified in the search criteria, select from the **Action** drop-down list one of the following options:

**Add Access Group** – to assign all badges in the list box with access to all terminals defined in the access group. Select the **Access Group** and **Time-**

**zone** that will be assigned to the selected badges. The access group will be added to the first available slot on the badges.

**Apply Access Template** – to apply all preset access privileges, badge options, access groups, and time zones that were defined in the access template. Select from the **Access Template** drop-down list, the Access Template that will be applied to the selected badges.

**Note:** You cannot apply Facility Code settings using the Bulk Badge Change function.

**Delete Access Group** – to remove from the selected badges access to all terminals defined in the access group. Select the **Access Group** to remove.

**Delete Badge** – to delete all badges in the list box.

**Delete Badge and Cardholder** – to delete all badges and associated cardholders in the list box.

**Note:** If a cardholder owns more than one badge, and that badge is not included in the list box, the cardholder record will not be deleted.

**Disable Badge** – to disable all badges in the list box.

**Replace Access Group** – to replace the existing access group. Select from the **New Access Group** drop-down list the access group you wish to assign. Select from the **Old Access Group**, the access group you wish to replace. The original timezone for the access group will not be changed.

8. If you wish to print the data in the list box, click the **Print** button.
9. Click **Apply** to change the selected badge records.
10. Click **Done** to close Bulk Badge Change.

## Entering Visitor Information

The Add Visitor function introduces an easier and faster way to enter visitor and badge information, by allowing authorized operators to enter visitor and badge data using a single user interface. Prior to a visitor's arrival, the operator enters the appropriate visitor data into the system, assigns a visitor sponsor, enters

the date and time period of the scheduled visit, and assigns access privileges using Access Templates, subsequently and from the same screen, the visitor badge is printed.

## To Enter Visitor Information:

1. From the P2000 Main menu, select **Access>Add Visitor**. The Add Visitor dialog box opens.

2. See the following “Add Visitor Field Definitions” for detailed information.
3. After you enter all the information, click the **Save** button to save the visitor and badge information. The new visitor data will also be reflected in the Cardholder window.
4. If you wish to save and print the badge, click the **Save and Print** button (requires the Video Imaging application).
5. If you wish to enter additional visitors, click the **Clear** button, then enter the information according to the “Add Visitor Field Definitions”.
6. Click **Exit** to close the Add Visitor dialog box.

## Add Visitor Field Definitions

### Visitor Box

**First** – Enter the first name of the visitor.

**Middle** – Enter the middle name of the visitor.

**Last** – Enter the last name of the visitor.

**ID** – Enter a unique ID for this visitor (up to 25 characters).



**Company** – Select from the drop-down list, the visitor's Company name. If the company name does not already exist in the database for the visitor's assigned partition, click the browse button [...] to open the Company window. Refer to the *P2000 Software User Manual* for information on adding a company name to the P2000 database.

**Partition** – Select from the drop-down list, the partition to be assigned to the visitor.

**Found in DB** – Indicates whether or not P2000 has identified a matching Visitor record in the cardholder database after you click the **Search** button. If **Found in DB** shows **Yes**, then the existing visitor record in the P2000 database will be updated. If it shows **No**, the new visitor will be added when you click **Save**.

**Approved Visits** – Displays the number of approved visits. This field is only valid if the **Found in DB** field displays **Yes**.

---

**Note:** *The Add Visitor application creates four UDFs: **Approved Visits**, **Most Recent Visit**, **Second Most Recent Visit**, and **Third Most Recent Visit**. These UDFs are automatically updated and allow you to monitor the visits associated with the selected visitor.*

---

**Search** – If the visitor information already exists in the database, you may search the database by entering a value in any of the Visitor fields and then clicking the **Search** button. The Find Visitor dialog box opens displaying the visitor record(s) that match the entered value(s). You may also click the **Search** button without entering any values to display all visitors in the database.

The Find Visitor dialog box displays search criteria and results. The criteria are: First: John, Middle: (empty), Last: Paulson, ID: (empty), and Company: ABC Marketing. The results table shows one record:

First	Middle	Last	ID	Company
John		Paulson	1221	ABC Marketing

Select the visitor's name and click **OK**.

**Take** – If your facility uses the Video Imaging application, click the **Take** button to capture the visitor's portrait.

## Sponsor Box

**First** – Displays the first name of the person who will sponsor this visitor.

**Middle** – Displays the middle name of the person who will sponsor this visitor.

**Last** – Displays the last name of the person who will sponsor this visitor.

**ID** – Displays the unique ID assigned to the sponsor (up to 25 characters).

**Company** – Displays the sponsor's Company name.

**Partition** – Displays the partition assigned to the sponsor.

**Search** – Click this button to find a Sponsor in the database. The Find Sponsor dialog box opens. When you enter a value in any of the fields, the list box displays the sponsor record(s) that match the entered value(s). If no value was entered, all cardholders in the database will be displayed.

The Find Sponsor dialog box displays search criteria and results. The criteria are: First: (empty), Middle: (empty), Last: (empty), ID: (empty), and Company: <any>. The results table shows multiple records, with Steven Johnson highlighted:

First	Middle	Last	ID	Company
Jane		Doe		
Aron		Humphrey		
Rick		Jaschob		
Steven		Johnson	12265	Johnson Controls
Steve		Jones		
David	Herbert	Lawrence		
Roy	S	May		Johnson Controls
Keith		Paulson		
Mary		Robertson		
James		Smith		
Robert	J.	Smith	5676	Johnson Controls
Susan		Thompson		
Yaron		Tomlinson		

Select the sponsor's name and click **OK**.

## Badge Box

**Number** – Enter a badge number (the number of allowed characters depends on the parameters selected in the Site Parameters dialog box).

**Note:** The Add Visitor application does not support FASC-N badge numbers.

**Auto** – If your facility is set up to use the AutoBadge Management feature, click the **Auto** button to insert the next available badge number in the Number field.

**Issue** – Enter an issue level per badge number. If a visitor loses a badge, you would give the next available issue level and retain the same badge number. The number of badge issue levels supported depends on your panel type.

**Template** – Select from the drop-down list the access template to be applied to this badge. See “Access Template” on page 12.

**Design** – Select the badge design that was created using the Video Imaging application.

**Start Date** – Click the down arrow to select a date from the system calendar that this badge becomes active.

**Start Time** – Click the spin box buttons to select a time that this badge becomes active.

**Void Date** – Click the down arrow to select a date that this badge will be automatically voided.

**Void Time** – Click the spin box buttons to select a time that this badge will be automatically voided.

## Badge Resync

Entry and Exit terminals require cardholders to enter and exit an area in sequence. That is, when cardholders badge *in* at an entry terminal, they must badge *out* at the next badging. If, for example, they follow another cardholder *out* without swiping their badge, their badge will remain in the *In* state (out-of-sync). When they attempt to badge back into the area, they will be denied access. You can manually adjust the state of a badge to return it to the correct state. You can also reconfigure this badge as Undefined to clear the Entry/Exit status until the next badging.

**Note:** For Entry/Exit to work, all Entry and all Exit terminals must either run in Central mode, or they must all be defined on the same panel and run in Local mode.

## To Resync Badges:

1. From the P2000 Main menu, select **Access>Badge Resync**. The Badge Resync dialog box opens.

2. If this is a partitioned system, select the **Partition** in which the badges are active.
3. From the **Show** drop-down list, select one of the following options:

**Cardholders** – to resync the status of badges that belong to all or specific cardholders.

**Last Badging Terminal** – to resync the status of all badges last presented at the selected terminal.

**Last Badging Terminal Group** – to resync the status of all badges last presented at all terminals in the selected terminal group.

**Note:** The **Last Badging Terminal** and **Last Badging Terminal Group** options are used for example, to quickly reset the status of all badges after a mustering event or reset the status of badges in situations when cardholders badged *in* at an entry terminal and they were not able to badge *out* at an exit terminal because the exit terminal was down.

4. If you selected **Last Badging Terminal** or **Last Badging Terminal Group**, select a terminal or terminal group from the list and continue with step 16.
5. If you selected **Cardholders**, select from the **Type** list the cardholder type (Regular, Visitor, or <all>) that you wish to display in the list box.
6. If you wish to display specific cardholders (within the type selected), click the **Search** button. The Database Search dialog box opens.

7. Enter the information on any or all of the fields to search for specific cardholders.
8. If you wish to search by **Company** and/or **Department**, select a previously defined name from the drop-down list.
9. You can also search by UDF. Select any of the previously defined UDFs from the drop-down list (Date type UDFs cannot be included in the search). Then enter or select the UDF search criteria in the associated field.
10. If you wish to clear the existing search criteria, click the **Clear** button.
11. After you define the search criteria, click one of the following buttons:
 

**Exact Match** – to display an exact match to your search criteria.

**Partial Match** – to display all possible selections that match the initial characters of the search criteria, for example if you enter *Carl* in the First Name

field, the list box will display names such as Carla, Carlos, Carlton, etc.

12. The list box in the Badge Resync dialog box opens displaying the cardholders specified in the search criteria.
13. If you wish to display all cardholders again (within the type selected), click the **All** button.
14. After you define the cardholders you wish to display in the list select a cardholder from the list.
15. The badge number and status of all badges assigned to this cardholder displays in the Badges list. Select the badge or badges to be resync.

---

**Note:** To resync the status of all badges of all cardholders currently in the list, enable the **Select All** check box.

---

16. Click the appropriate button, **In**, **Out**, or **Undefined** to change the status of the badge(s).
17. Click **Done**. The badge status is now changed.

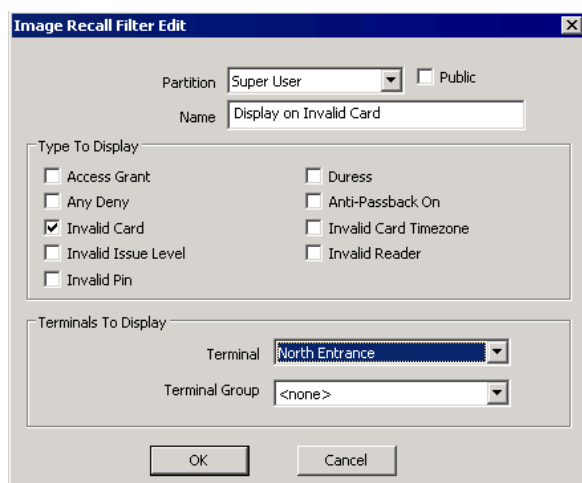
## Image Recall

If the Image Recall window is open on the workstation, any badging (for the partition selected in Image Recall Filters) will display the cardholder's image and information. An operator with proper menu permissions can define access conditions and other filter criteria (transactions set up in the Image Recall Filter Edit dialog box, such as an Access Grant or any invalid transaction), to determine if an image will display in the Image Recall window.

## Image Recall Filters

1. From the P2000 Main menu, select **Access>Image Recall Filters**. The Image Recall Filters dialog box opens.

- Click **Add**. The Image Recall Filter Edit dialog box opens.



The 'Image Recall Filter Edit' dialog box contains the following fields and options:

- Partition:** A dropdown menu set to 'Super User' and a checkbox for 'Public'.
- Name:** A text field containing 'Display on Invalid Card'.
- Type To Display:** A group box containing two columns of checkboxes:
  - Left column: ☐ Access Grant, ☐ Any Deny, ☒ Invalid Card, ☐ Invalid Issue Level, ☐ Invalid Pin.
  - Right column: ☐ Duress, ☐ Anti-Passback On, ☐ Invalid Card Timezone, ☐ Invalid Reader.
- Terminals To Display:** A group box containing:
  - Terminal:** A dropdown menu set to 'North Entrance'.
  - Terminal Group:** A dropdown menu set to '<none>'.
- Buttons:** 'OK' and 'Cancel' at the bottom.

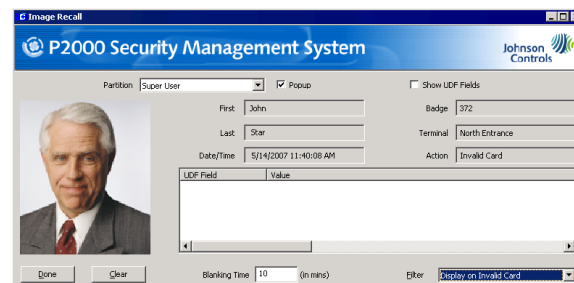
- If this is a partitioned system, select the **Partition** in which this image recall filter will be active.
- Select **Public** if you wish this image recall filter to be visible to all partitions.
- Enter a descriptive **Name** for the image recall filter.
- From the **Type to Display** box, select the transactions that you wish to monitor. You do not need to select all conditions. If you select *Any Deny*, all other filtering conditions will be grayed out, except *Access Grant* and *Duress*.

**Note:** Cardholder image and information will always display in the Image Recall window if the associated badge has the *Trace* option enabled, regardless of the filter conditions selected here.

- Select a **Terminal** name from the drop-down list to specify the terminal to be monitored.
- Select a **Terminal Group** name from the drop-down list if you wish to monitor a Terminal Group.
- Click **OK**. The new image recall filter will display in the Image Recall Filters list.
- Click **Done**.

## To Activate Image Recall:

- From the P2000 Main menu, select **Access>Image Recall**. The Image Recall window opens.



The 'Image Recall' window displays the following information:

- Header:** 'P2000 Security Management System' and 'Johnson Controls' logo.
- Partition:** A dropdown menu set to 'Super User' and a checkbox for 'Popup'.
- Show UDF Fields:** A checkbox.
- Cardholder Information:**
  - First:** John
  - Last:** Star
  - Badge:** 372
  - Terminal:** North Entrance
  - Date/Time:** 5/14/2007 11:40:08 AM
  - Action:** Invalid Card
- UDF Field:** A table with two columns: 'UDF Field' and 'Value'.
- Buttons:** 'Done', 'Clear', and 'Filter'.
- Blanking Time:** A field set to '10 (in mins)'.
- Filter:** A dropdown menu set to 'Display on Invalid Card'.

- If this is a partitioned system, select the **Partition** in which the image recall will be active.
- Select **Popup** if the Image Recall window is to move to the front of all windows on the P2000 screen whenever an access attempt that matches the current filter occurs.

**Note:** Some computers may not allow the Image Recall window to automatically pop up in front of other windows on the screen; instead, the Image Recall button will begin flashing in the Windows taskbar.

- Select the **Show UDF Fields** check box, if you wish to display the user defined fields associated with the cardholder.
- In the **Blanking Time** field, enter the time in minutes after which the image and the data will be cleared. If you enter a value of zero the display will not be blanked.
- Select a **Filter** from the drop-down list.
- When a cardholder presents a badge at a terminal or group of terminals that meets the filtering conditions, the cardholder's image displays, along with the current cardholder information.
- This image and information will remain in the window until another cardholder badges within the partition, or until the **Blanking Time** defined elapses, or until you click the **Clear** button to clear the information in the Image Recall window.
- Leave the Image Recall window open on the workstation to view images displayed as a result of subsequent badgings.

## Image Recall FS (Full Screen)

The Image Recall FS feature offers a simplified display and works in both default and full screen modes.

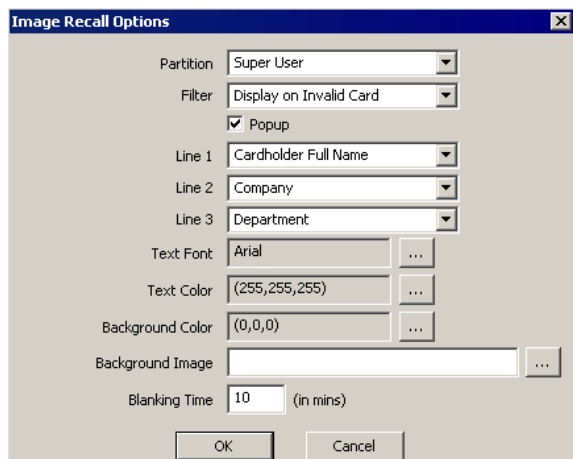
When the Image Recall FS window is open and a cardholder presents a badge at a terminal or group of terminals that meets the filtering conditions, the cardholder's image displays along with the cardholder name. Optionally, one or two of the following can also display: Company, Department, ID, and any text or numeric user defined field (UDF).

### To Activate Image Recall FS:

1. From the P2000 Main menu, select **Access>Image Recall FS**. The Image Recall FS window opens.



2. Select **Edit>Options** to open the Image Recall Options dialog box and define the elements you wish to display.



3. If this is a partitioned system, select the **Partition** in which the image recall will be active.
4. Select a **Filter** that contains the access conditions that determine which images to display. See "Image Recall Filters" on page 17.
5. Select the **Popup** check box if the Image Recall FS window is to move to the front of all windows on the P2000 screen whenever an access attempt that matches the current filter occurs.

**Note:** Some computers may not allow the Image Recall window to automatically pop up in front of other windows on the screen; instead, the Image Recall button will begin flashing in the Windows taskbar.

6. From **Line 1**, **Line 2**, or **Line 3** drop-down lists, select the data to be displayed in the first, second, or third line under the cardholder's image. You can select Badge Expiration Date, Cardholder Expiration Date, Cardholder First Name, Cardholder Full Name, Cardholder Last Name, Company, Department, ID, or any text or numeric user defined field.
7. Click the **Text Font** browse button [...] to open the Font window and select the font type you wish to display. The font style and size are not configurable.
8. Click the **Text Color** browse button [...] to open the standard Color window and select the text color you wish to display.
9. Click the **Background Color** browse button [...] to open the standard Color window and select the background color you wish to display.
10. Click the **Background Image** browse button [...] to select a background image.
11. In the **Blanking Time** field, enter the time in minutes after which the image and the data are erased and the background is displayed. If you enter a value of zero the display will not be blanked.
12. Click **OK** to save your options and return to the Image Recall FS window.
13. Select **View>Full Screen** to change the display mode to "full screen." Click <Esc> to return to previous view.



14. The image and information will remain in the window until another cardholder badges within the partition, or until the **Blanking Time** defined in Image Recall Options elapses, or until you select **View>Clear** to clear the information.
15. Leave the Image Recall FS window open on the workstation to view images displayed as a result of badgings, or select **File>Exit** to close.

## Monitor Alarms

Alarm monitoring is at the heart of the *P2000 Security Management* system. According to system devices configuration, alarms display in the Alarm Monitor queue as they occur.

Operators assigned to monitor alarms respond according to individual company policy, and the alarm instruction and response text configured for the various alarm types. The Alarm Response text can be pre-configured for operator selection and/or set to enter manually for a more appropriate response.

The Alarm Monitor window opens immediately after logging on to the Server, so that ongoing alarms are always visible. The Alarm Monitor window cannot be closed at the Server, to ensure that alarm conditions do not go unnoticed. However, it can be minimized using the minimize button on the title bar.

If the Alarm Monitor window is minimized, an alarm message popup can alert the operator that a new alarm has been reported. When an alarm is reported, the operator acknowledges the alarm, makes the appropriate response, and then completes the response.

---

**Note:** *Some computers may not allow the Alarm Monitor window to automatically pop up in front of other windows on the screen; instead, the Alarm Monitor button will begin flashing in the Windows taskbar.*

---

Pending alarm messages remain in the Alarm Queue until acknowledged and removed by an operator. Alarm History is stored in the system as configured in Site Parameters.

---

**Note:** *Elements that report alarms, such as input points, must NOT have the **Disable Alarm** option selected to have the alarm displayed in the Alarm Monitor window.*

---

## Alarm Handling

As an operator, you may be required to handle alarm conditions, depending on the Message Filter Group and Alarm Processing Group assigned by your system administrator. The Alarm Monitor verifies that alarms pass the Alarm Processing Group filter (if any) for the operator before allowing the operator to acknowledge, respond or complete alarms. Refer to the instructions starting on page 23 for details.

---

**Note:** *Message Filtering and Alarm Processing Groups apply on P2000 Workstations only, not on P2000 Servers.*

---

The alarm response will typically include steps similar to the following:

1. **Acknowledge** that an alarm condition has been reported by the system.
2. **Respond** by entering the appropriate response.
3. **Complete** the alarm.
4. **Remove** the completed alarm condition from the Alarm Monitor window.

**Acknowledging an alarm** – An operator may be required to acknowledge a new alarm as soon as it is received. They may do so and then return later to actually respond to the alarm, depending on company policy and the priorities assigned to that alarm. The time and date of the acknowledgment is recorded in the alarm history. Acknowledging an alarm silences the audible beep (unacknowledged alarms will continue to beep until recognized). Alarm acknowledgment is optional and does not need to occur prior to response; its use is typically dictated by company policy.

**Responding to an alarm** – When an operator responds to an alarm, the operator name is entered in the User Name column of the Alarm Monitor window. The Response time is date and time stamped for the alarm history record. The operator would typically review the Alarm State and Description to note any known conditions. Specific instructions created for the particular alarm will display in the Instruction box during

the response to help the operator perform the appropriate action.

**Completing an alarm** – Several actions may take place during the handling of an alarm. When all actions needed to process the alarm have been completed, the operator “completes” the alarm. This action is date and time stamped for the alarm history record. An alarm can only be completed if the alarm state is “secure.”

---

**Note:** *Responding to an alarm that has not been acknowledged will automatically cause an acknowledgment to occur. Similarly, completing an alarm causes an automatic acknowledge, if needed.*

---

**Removing the Alarm from the queue** – According to company policy, operators may remove completed alarms from the alarm queue. The alarm response sequence will remain in the alarm history record.

**Refreshing the Alarm Monitor window** – The Refresh button is used to read again all current alarms from the database (this should not be needed unless there was a loss of communication with the Server).

Access the Alarm Monitor from the P2000 Main menu. Select **Alarm>Alarm Monitor**, or if minimized just click the Alarm Monitor button to restore it.

The Alarm Monitor queue displays alarms in a scrolling list, as they occur. The alarm response changes as the operator performs the response steps (see the Alarm Status column header in the Alarm Monitor window); and the date and time of each step is recorded in the alarm history record.

When a new alarm displays, an audible beep sounds, and a red color bell icon in the line item entry message begins flashing. The entry will continue in this “Pending” state until an operator acknowledges the alarm, after which the beep stops and the bell icon changes to yellow.

## Monitoring Remote Alarms

Your system administrator can configure the system to receive alarm messages from remote P2000 sites, allowing operators to simultaneously monitor alarms locally and at multiple remote sites. This feature is useful to monitor alarms at unattended sites that are closed for the weekend or a holiday, and ensures that all alarm conditions, even at far away locations, are watched closely at all times.

To monitor remote alarms, your system administrator must properly configure both your local and the remote site. If all conditions are met, your local Alarm Monitor window will display alarm messages that are generated at remote sites when their alarm status or state changes.

The procedures for handling remote alarms are similar as for local alarms; however, the following points should be noted:

**Responding to remote alarms** – Alarm instructions are sent to remote sites; however, the alarm responses remain local. While the Alarm Status column in the Alarm Monitor displays a “Responded” status, the alarm response entered at a remote site will NOT be part of the alarm history in your local site.

**Completing remote alarms** – Remote alarms can be completed, regardless of the current alarm state.

**Removing remote alarms** – Remote alarms can be removed from the queue, regardless of the current alarm state. Removed alarm will be automatically completed.

## Alarm Monitor Definitions

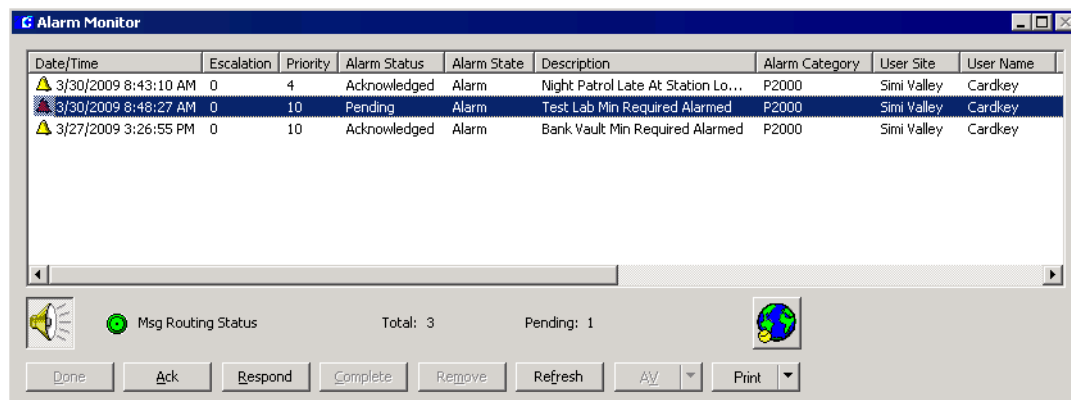
**Date/Time** – Displays the date and time the alarm was reported to the system. Alarms that are originated at remote sites with different geographical time zones will display the actual time at the remote site.

---

**Note:** *Click any of the column headings to sort the alarms by the selected column heading.*

---

**Escalation** – Displays the escalation level of the alarm (the highest is “10”).



**Priority** – Displays the Alarm Priority set for each alarm type (the highest is “0”).

You can assign sounds to Alarm Priorities 0 to 255 in groups of 10. The sound files can be set up from the **Control Panel** in your Windows desktop, clicking the **Sounds** icon. In the **Sounds** tab, select any of the Pegasys Alarm Priorities from the Program events box, then select the corresponding sound file from the Sounds drop-down list.

**Note:** To access the P2000 alarm priority sounds, you must open the Alarm Monitor window at least once at the workstation.

**Alarm Status** – Displays any of the following Alarm Status.

- **Pending** – Not yet acknowledged.
- **Acknowledged** – Acknowledged but no action taken.
- **Responding** – Acknowledged and response action in progress.
- **Complete** – Action taken.

**Alarm State** – Indicates the state of the alarm, such as Secure, Alarm, Open, Short, Suppressed, Tamper, Bypassed, etc.

**Description** – A description of the element that activated the alarm.

**Alarm Category** – Displays the Alarm Category to which the alarm belongs. The default category is “P2000.” When an alarm is assigned to multiple Alarm Categories, and the operator is configured to view alarms from these multiple categories, the alarm will display separately for each category.

**User Site** – Displays the site name from where the operator is handling the alarm.

**User Name** – The name of the operator who handles the alarm.

**Action Date/Time** – Displays the date and time the action (respond, complete, etc.) takes place. This will always be the local time, regardless if a remote site is in a different geographical time zone.

**Query String** – Displays the query string value (if it was defined) of the item associated with the alarm.

**Alarm Site** – Displays the name of the P2000 site where the alarm was originated.

**Partition** – Displays the name of the partition containing the item (input point, terminal, panel, etc.) that originated the alarm.

**Public** – Displays whether the alarm message is visible to other partitions.



**Audible Alarm Button** – Click the Audible Alarm button to temporarily disable the audible alarm beep. All alarms will be affected.

Unless you acknowledge, respond, or complete the alarm, the beep will become audible again in two minutes. If you wish to turn off the audible alarm beep, select from the **Sounds** dialog box in the **Control Panel**, any of the Pegasys Alarm Priorities, then browse for the *None.wav* file located in the “bin” folder of the P2000 software installation.



**Msg Routing Status** – The Message Routing Status indicator will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.



**Total** – Displays the total alarm count in the Alarm Monitor window.

**Pending** – Displays the number of pending alarms in the Alarm Monitor window.



**Map Button** – You can see the location of an alarm on a Real Time Map from the Alarm Monitor window. Select an alarm and click the Map button. The map displays and the icon will blink indicating the location of the alarm. For more information see “Using the Real Time Map” on page 33. This feature is available for local alarms only.

**AV** – This button is enabled if your facility uses the DVR feature. If the alarm message displayed is associated with a camera, you can select the message line from the list and click the AV arrow, then select whether you want to display live or stored video. For more information, refer to the DVR documentation.

**Print** – Click the Print arrow and select whether you want to **Print All** alarms in the queue or select **Print Displayed** to print the alarms that are visible in the Alarm Monitor list box.

## To Acknowledge an Alarm:

1. Click the line item you wish to respond to and click the **Ack** button. The Alarm Status changes to “Acknowledged.” This informs the system and anyone else monitoring the system that the alarm has been recognized.
2. If a number of alarms come in at once, you can acknowledge them in any order you wish; however, company policy may dictate that you respond by priority. If desired, select the highest priority by number, or click the **Priority** column title to sort by priority, moving the highest priority to the top of the list.

## To Respond to an Alarm:

1. With the line item to which you wish to respond selected, click the **Respond** button. The Alarm Response dialog box opens.

Action Date/Time	Alarm Status	User Name	Alarm State	Date/Time
3/30/2009 8:53:10 AM	Acknowledged	Cardkey	Alarm	3/30/2009 8:48:27 AM
3/30/2009 8:48:27 AM	Pending	Cardkey	Alarm	3/30/2009 8:48:27 AM
3/30/2009 8:45:49 AM	Responding	Cardkey	Secure	3/30/2009 8:45:10 AM
3/30/2009 8:45:10 AM	Pending	Cardkey	Secure	3/30/2009 8:45:10 AM

2. The following information displays for each alarm selected:

**Description** – Displays the description of the alarm.

**Condition** – Displays the alarm condition.

**Instruction** – If Instruction text was created, the instruction text will display here.

**History** – Displays all stored history for the line item selected from the Alarm Monitor.

3. Select from the **Predefined Alarm Response Text** drop-down list, the name of the response text. See “Creating Predefined Alarm Response Text” on page 25 for more information.
4. The **Text** box displays the full text entered from the Predefined Alarm Response Text selection. You can also enter a specific response.
5. Click the **Add** button on the Response box to enter the current Date/Time and Response in the scrolling text box at the bottom of the Alarm Response dialog box. This will store a record of the response in the transaction history. The Alarm Status will change to Responding.

**Note:** You can open multiple Alarm Response windows and respond to multiple alarms simultaneously. You can also acknowledge or complete alarms in the Alarm Monitor window while the Alarm Response window is open, but you cannot acknowledge or complete those alarms that are currently open in the Alarm Response windows.

6. Click **Done** to return to the Alarm Monitor window.

## To Complete an Alarm:

1. Click **Complete** to end the alarm processing sequence. The Alarm Status changes to Complete. Alarms can only be completed if the alarm state is “secure.”

## To Remove an Alarm Message from the Queue:

The Complete and Remove buttons do not become active until the alarm is in the secure state.

1. Select a line item from the scrolling list.
2. Click **Remove**.

**TIP:** As an alternative, right-click a line item in the Alarm Monitor window to perform from the shortcut menu any of the above functions (acknowledge, respond, complete, and remove alarms). You can also display the alarm details for the line item selected, display the alarm instruction associated with the alarm, see the location of the alarm on a Real Time Map, display live or stored AV video (if available), or view all items when you click the **Display All** option. In addition, if the element that generates the alarm was configured to manually activate events, the event name will also display in the shortcut menu. Also, the shortcut menu allows you to print **All** alarms in the queue or only the alarms that **Displayed** in the list box.

## To Activate an Event from the Alarm Monitor:

1. In the Alarm Monitor window, select the line item you are responding to and right-click to open the shortcut menu.
2. Click the event name you wish to activate. The event will be triggered.

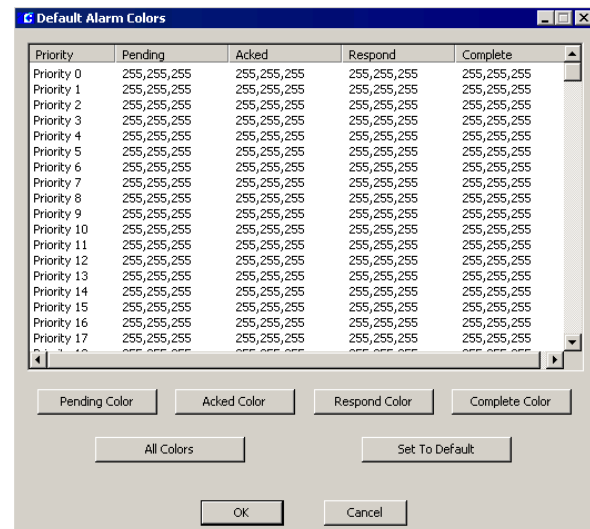
## Configuring Alarm Colors

The P2000 system provides color configuration capability for each alarm priority (0 to 255) and its corresponding alarm status. Each alarm status can have a unique color assigned to help operators recognize spe-

cific alarms. When a new alarm displays in the Alarm Monitor window, the line for the affected alarm will display in the color that was assigned using the Default Alarm Colors dialog box.

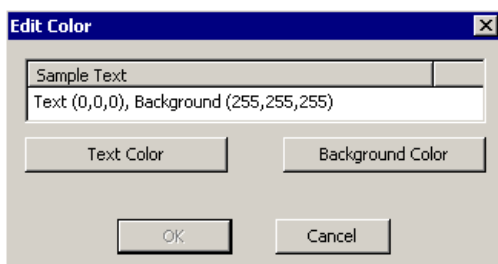
## To Define Color-Coded Alarms:

1. From the P2000 Main menu, select **Config>System**. Enter your password if prompted. The System Configuration window opens.
2. Click the plus (+) sign next to the root **Site Parameters** icon to display default system parameters.
3. Click the **Default Alarm Colors** icon and click **Edit**. The Default Alarm Colors dialog box opens.



4. Click the **Priority** line you wish to define.
5. Click one of the following buttons:
  - **Pending Color** – to assign a specific color to alarms that have not yet been acknowledged.
  - **Acked Color** – to assign a specific color to alarms that have been acknowledged.
  - **Respond Color** – to assign a specific color to alarms that have been responded.
  - **Complete Color** – to assign a specific color to alarms that have been completed.
  - **All Colors** – to assign the same color to all alarm status for the priority selected.

Regardless of the option selected, the Edit Color dialog box opens.

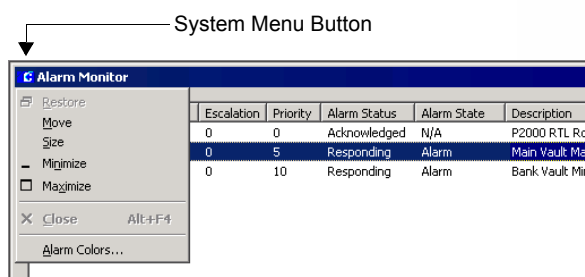


6. Click the **Text Color** button and select the desired text color from the color palette. Click **OK**.
7. Click the **Background Color** button and select the desired background color from the color palette. Click **OK**.
8. The Sample Text box will display the selected colors. Click **OK** to return to the Default Alarm Colors dialog box. You will not see the new color until you select other priority number or click anywhere on the screen.
9. Repeat the same steps if you wish to assign colors to other alarm priorities.
10. To return to the default system colors, select the Priority line and click the **Set To Default** button.
11. When you finish setting all alarm colors, click **OK**.

The assigned colors for each priority and corresponding alarm status will be the default colors for all operators; however, operators who are required to handle certain alarm conditions may want to use different colors for the alarms they need to see. In that case, the default alarm colors can be changed from the Alarm Monitor window.

**Note:** The ability to change alarm colors from the Alarm Monitor window is controlled by menu permissions. See your system administrator if you need menu permissions to override the default alarm colors.

12. Open the Alarm Monitor window, and click the system menu button.



13. From the control menu select **Alarm Colors**. The Alarm Colors dialog box opens displaying the default colors that were defined from the System Configuration window.
14. Assign the desired colors as described before, then click **OK** to save your settings.

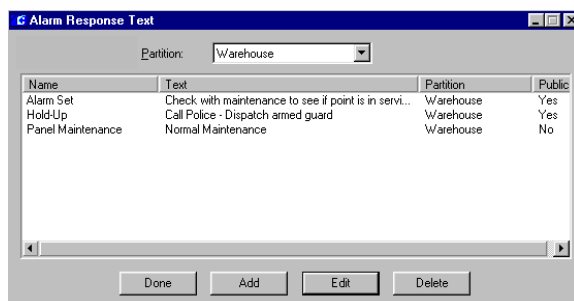
**Note:** Alarm colors that are assigned from the Alarm Monitor window are associated with the operator who made the changes. In addition, the **Set To Default** button will reset to the default colors assigned from the System Configuration window.

## Creating Predefined Alarm Response Text

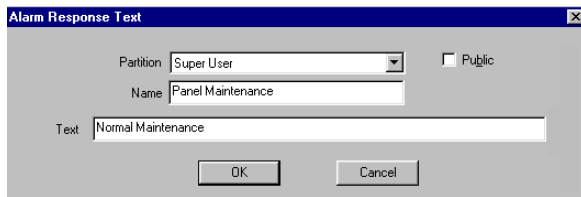
You can create Response text to speed alarm response to specific types of alarms. For example, when panels go down for regular maintenance, a “Panel Down” soft alarm is sent to the Alarm Queue. The operator can quickly respond by selecting a predefined response from the drop-down list.

### To Create Predefined Alarm Response Text:

1. From the P2000 Main menu, select **Alarm>Alarm Response Text**. The Alarm Response Text list opens.



2. If this is a partitioned system, select the **Partition** in which this alarm response text will apply.
3. The Name, Text, Partition, and whether or not the text is Public will display in the list.
4. Click **Add**. The Alarm Response Text dialog box opens.



The **Alarm Response Text** dialog box has a title bar with a close button. It contains a **Partition** dropdown menu set to "Super User", a **Public** checkbox, a **Name** text field containing "Panel Maintenance", and a **Text** text area containing "Normal Maintenance". At the bottom are **OK** and **Cancel** buttons.

5. Select a **Partition**, if applicable, and select **Public** if you wish the text to be seen by all partitions.
6. Enter a descriptive **Name** for the text.
7. Enter the actual **Text** you wish to enter into the Alarm Response record.
8. Click **OK**. The Response text name will be available in the drop-down list of the Alarm Response dialog box.

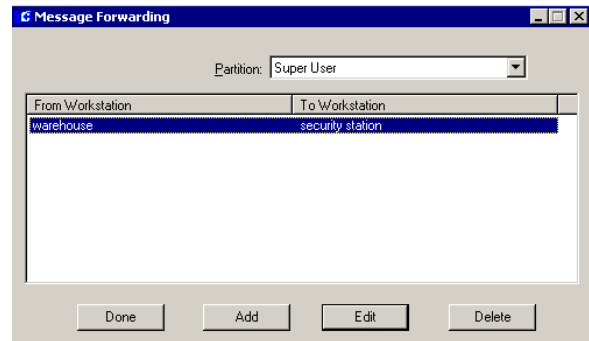
## Message Forwarding

Message Forwarding is useful when using message filters. At times, it may be necessary to temporarily forward messages from one workstation to another; for example, if an operator must leave the workstation for a short period of time, or during a vacation or sick leave. When the operator is ready to receive messages at his/her workstation again, message forwarding for the workstation can be deleted.

**Note:** When forwarding messages from one workstation to another, the system must decide which messages are to be forwarded depending on the operator that is logged on at the receiving workstation. The system will only transmit messages that pass the filter criteria associated with the operator.

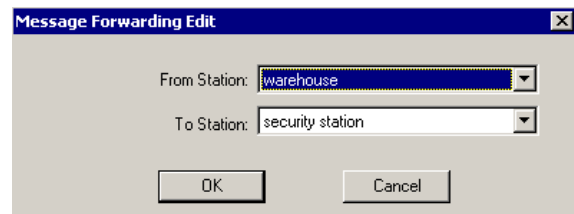
### To Forward Messages from One Workstation to Another:

1. From the P2000 Main menu, select **Alarm>Message Forwarding**. The Message Forwarding dialog box opens listing the workstations from where and to where all current messages are forwarded.



The **Message Forwarding** dialog box has a title bar with standard window controls. It features a **Partition** dropdown menu set to "Super User". Below is a table with two columns: **From Workstation** and **To Workstation**. The first row contains "warehouse" and "security station". At the bottom are **Done**, **Add**, **Edit**, and **Delete** buttons.

2. If this is a partitioned system, select the **Partition** in which the workstations are active.
3. Click **Add**. The Message Forwarding Edit dialog box opens.



The **Message Forwarding Edit** dialog box has a title bar with a close button. It contains two dropdown menus: **From Station** (set to "warehouse") and **To Station** (set to "security station"). At the bottom are **OK** and **Cancel** buttons.

4. From the **From Station** drop-down list, select the workstation that will be forwarding the messages.
5. From the **To Station** drop-down list, select the workstation to which you wish to forward the messages.
6. Click **OK**. The new entry will display in the Message Forwarding list.
7. Click **Done**.

## Operator Controls

Most system functions operate automatically; however, some functions may be operated manually from a workstation. Operators with the appropriate permissions can manually control doors, output devices, or raise the security level of the terminals to restrict access in emergency situations. Operator controls are panel specific. See the *P2000 Software User Manual* for a detailed list of features and capabilities supported by your panel type.

## Controlling Doors

An operator can manually control a door, a group of doors, or all doors (override system controls) for a specific time period. For example, an authorized operator can manually control access to a specific door during off business hours. If this is a partitioned system, the doors or door groups available from the drop-down list will be only those active in the operator's partition.

**Note:** Isonas panels do not report transactions associated with manual door control changes.

### To Manually Control Doors:

1. From the P2000 Main menu select **Control>Door Control**.
2. Enter your password if prompted. The Door Control dialog box opens.

3. If this is a partitioned system, select the **Partition** in which this door is active.
4. In the Control box, select either **Door** or **Group** to populate the Name drop-down list with selections.
5. Select a **Name** from the drop-down list.
6. In the Action box, select one the following:  
**Return to Normal** – to return the door to its normal state.  
**Open for Access Time** – to unlock the door for the amount of time set in the Access Time field defined in the Terminal dialog box.

**Unlock** – to unlock the door for the number of minutes entered (up to 1440 minutes) in the **Duration** field, after which the doors will revert back to their original system-controlled condition.

**Lockout** – to prevent access by all badges at the door. Only supported by OSI and Assa Abloy panels.

7. Click **Perform**. The Action selection goes into effect.
8. Click **Done** to exit the window.

### To Control all Doors at once:

1. From the P2000 Main menu select **Control>Control All Doors**.
2. Enter your password if prompted. The Control All Doors dialog box opens.

3. If this is a partitioned system, select the **Partition** in which the doors are active.
4. Select the **All Panels** radio button if you wish to control all doors in the system, or select **Selected Panel** and select a panel from the drop-down list to control all doors connected to the selected panel.
5. Select the **Unlock All Doors** option if you wish to unlock all doors.
6. Click **Perform**. The system will inform you that the doors will remain unlocked until you lock the doors again, and prompt you to continue.
7. Click **Yes**. This will override the system control until you reverse the command.

8. To return the doors to their previous state, select the **Resume Normal Operation** option.
9. Click **Perform**. The system will prompt for verification.
10. Click **Yes**. The Door Control override is reversed.

## Controlling Outputs

An operator can manually control an output (override system controls) for a specific output point or group. (The operator must first have menu permissions for Output Control to use this feature.) If it is a partitioned system, the outputs available from the drop-down list will be only those active in the operator's partition.

**Note:** Isonas and HID panels do not report transactions associated with output point status changes.

### To Manually Control an Output Point:

1. From the P2000 Main menu, select **Control>Output Control**. The Output Control dialog box opens.

The screenshot shows the 'Output Control' dialog box. At the top, there is a 'Partition' dropdown menu currently showing 'Super User'. Below this, the 'Output' section has two radio buttons: 'Point' (which is selected) and 'Group'. To the right of these is a 'Name' dropdown menu showing 'Activate Audible Alarm'. The 'Action' section has three radio buttons: 'Activate' (selected), 'Deactivate', and 'Disable'. To the right of the 'Activate' radio button is a dropdown menu showing 'Preset' and a 'Duration' field with the value '0' and the unit 'sec'. At the bottom of the dialog are two buttons: 'Perform' and 'Exit'.

2. If this is a partitioned system, select the **Partition** in which this output is active.
3. In the Output box, select either **Point** or **Group** to populate the Name drop-down list with selections.
4. Select an output point or output group **Name** from the drop-down list.

5. Click **Activate** to activate the output point (or group) and select from the drop-down list one of the following choices (the actions available in the list depend on the panel type):

- **Preset** – to turn the output point to a predefined state.
- **Set On** – to turn on the output point.
- **Slow Flash** – to toggle the output point on and off slowly.
- **Fast Flash** – to toggle the output point on and off quickly.
- **Timed/Pulse** – to turn the output point for a specified time in seconds. If you select this option, you must enter the time in seconds in the **Duration** field.

**Note:** If you manually turn a P900 output point for a timed duration, you must click the **Refresh** button in the System Status window to update the P900 output point status information after the timed duration has expired.

6. Click **Perform** to manually activate the output point.
7. If you wish to return the output point to a Normal state, click **Deactivate**, then click **Perform**.
8. If you wish to temporary disable a P900 output point, click **Disable**, then click **Perform**.
9. Click **Exit** to close the dialog box.

## Security Threat Level Control

Security threat level control provides a rapid method of restricting access in case of an emergency. In the event of a security breach, an authorized operator will be able to quickly change access privileges for all cardholders at any reader terminal connected to a panel that supports security threat level control. The default security level for these terminals is 0 (the lowest) and could be raised up to 99 (the maximum security level).

For this feature to work you must assign security levels to badges (see page 11). To obtain access at a door, the badge security level must be equal to or higher than the terminal security level. When an event occurs, the operator will raise the security level of the terminals in question, and access will be immediately restricted, unless the badge has the Executive privilege option enabled.



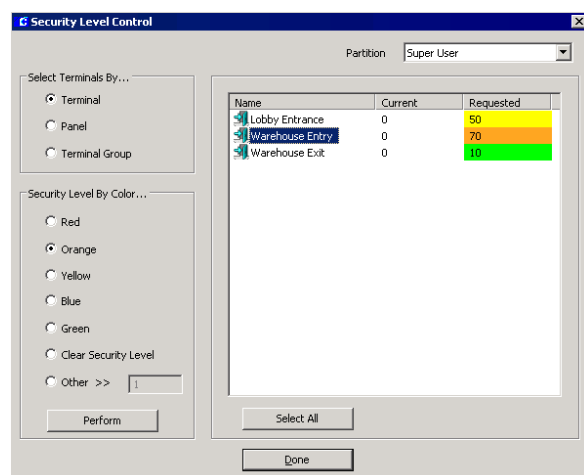
## Defining Security Levels

The Security Level Range Editor application allows a system administrator to modify the default values of the security level. Security levels are represented by five colored alert codes (Red, Orange, Yellow, Blue, and Green). For each color there is a range defined by Minimum, Maximum, and Set numeric values between 1 and 99. Once the system administrator defines the Security Level ranges, the operator can rapidly apply a Security Level value to terminals using the Security Level Control dialog box.

## To Apply Security Levels:

1. From the P2000 Main menu, select **Control>Security Level**. The Security Level Control dialog box opens.

**TIP:** As an alternative, you can click the Security Level Control icon in the P2000 toolbar to rapidly open the Security Level Control dialog box.



2. If this is a partitioned system, select the **Partition** in which the terminals reside.
3. In the **Select Terminals By** box, select one of the following options:

**Terminal** – All terminals (for the partition selected) will be listed on the right side of the dialog box. Use this option to restrict access to the selected terminals.

**Panel** – All panels (for the partition selected) will be listed on the right side of the dialog box. Use this option to restrict at once access to all terminals connected to the selected panels.

**Terminal Group** – All terminal groups (for the partition selected) will be listed on the right side of the dialog box. Use this option to restrict at once access to all terminals that belong to the selected terminal groups.

4. Depending on your selection in the Select Terminals By box, select from the list box the desired terminal, terminal group or panel name. You can select multiple names by holding down the <Ctrl> key, or click the **Select All** button to select all items in the list.
5. In the **Security Level By Color** box, select one of the colored security levels you wish to apply, then click the **Perform** button.

The selected terminals in the list box will display in the **Requested** column the default value for that colored security level. The **Current** column will display the current security level at the terminal.

**Note:** If you raise the security level at terminals that use the "Override Reset Threat Level" option, all time zone based overrides, host initiated overrides, and card-holder overrides will be immediately disabled. Refer to the P2000 Software User Manual for more information.

6. If you wish to assign a particular value, select the **Other** option in the Security Level By Color box, enter the desired security level value, then click **Perform**. The selected terminals in the list box will be set to this value as well as display the color of that value.
7. Once management determines that the emergency is over, you can either put the terminals in their previous level or remove the security level by selecting the item (terminal, terminal group or panel) from the list box then selecting the **Clear Security Level** option from the Security Level By Color box. The color will be removed from the terminal and the Requested and Current columns will display 0.
8. Click **Done** to close the Security Level Control dialog box.

# Monitor the System in Real Time

The Real Time List and Real Time Map are dynamic displays of system transactions and operations. The Real Time List is a time-stamped display of all (or specified) local or remote transactions as they occur. The Real Time Map displays the current status of local terminals, inputs, outputs, and other defined elements on a map layout of your site. The Real Time List and Real Time Maps are typically used not only to view current status, but as troubleshooting tools.

## Using the Real Time List

The Real Time List is a time-stamped display of all system transactions as they occur. If desired, an operator can monitor only specific transaction types. For example, an operator concerned with learning when a cardholder is denied access can select only *Access Deny* to filter the information displayed. The Real Time List will then display only who, what, when, where, and why the access was denied.

You can open multiple windows of the Real Time List. For example, you could have one window open with all the types enabled. You could open a second window with only the Badge Trace option selected that would display only those transactions.

---

**Note:** A description of each transaction type is presented in the *Printing tab* section of the *Software User Manual*. The *Printing* function of *Site Parameters* operates independently from the *Real Time List* function.

---

An operator may want to look at the Real Time List as a “health check”; for example, to ensure all transaction types are being processed, or trace why a specific cardholder is being denied access.

## Monitoring Remote Messages in Real Time

As with remote alarm monitoring (page 21), you can monitor transactions from multiple facilities at multi-

ple geographical locations. Although each remote site administrator has total control over their access control hardware and system information related to their site, operators can control system and event information from different sites. This means that remote operators might for example, monitor their transactions locally during normal working hours, while your local operators might monitor transactions messages generated at their remote sites after hours, as long as both the local and remote P2000 sites are set up and configured to receive and send transaction messages across P2000 sites during such periods.

With the proper configuration, an unlimited number of sites can be monitored simultaneously, allowing operators to administer multiple regions from a single site. To monitor remote messages, your system administrator must properly configure both your local and the remote site.

## Viewing Real Time List Transactions

To access the Real Time List, select **System>Real Time List**. Transaction types displayed in the list area of the Real Time List can be color coded to help operators recognize a specific type of transaction. You can use the default system colors, or customize a transaction type with a different color. You can also set up a printer to print transactions as they occur, or print all transactions in the list.

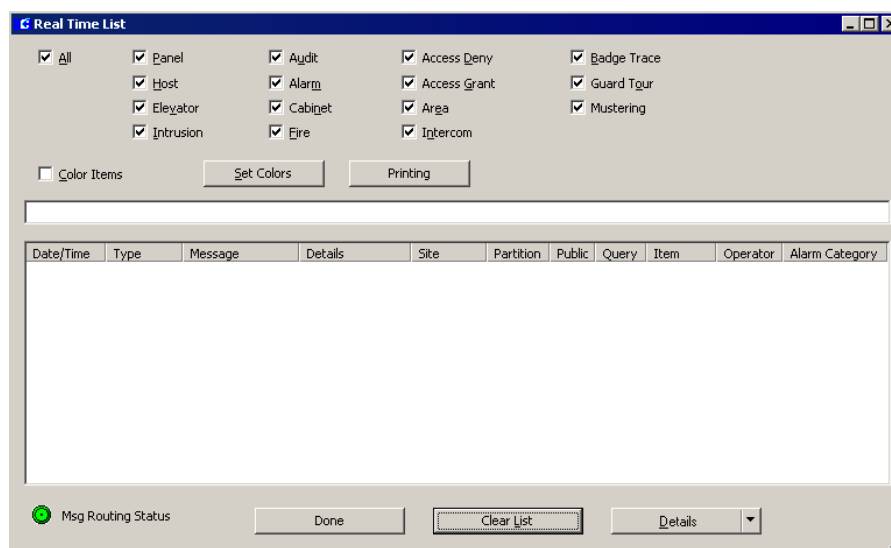
The Real Time List displays transaction messages in the order they are received. When a message is received, it displays in the row above the scrolling list and in the first line of the list. As new transactions occur, they move to the top of the list.

When you open the Real Time List for the first time in the session, the scrolling list will be empty. Depending on the transaction types selected at the top of the window, transactions will begin to display in Date/Time order at the top of the list. As transactions occur, the older ones will scroll down in the list as the newer ones are added at the top.

The following information is shown for each transaction in the list.

**Date/Time** – Displays the date and time of the message. Transaction messages that are originated at remote sites with different geographical time zones will display the actual time at the remote site. However,





remote alarms will display the time at which they were received at your local site.

**Type** – Displays the transaction types that were selected for monitoring (Audit, Access Deny, Badge Trace, and so on).

**Message** – Displays a message related to the transaction type, for example Invalid Card for an Access Deny transaction type.

**Details** – Displays details related to the message, such as Badge number, Terminal and Cardholder name.

**Site** – Displays the name of the local or remote P2000 site where the message was originated.

**Partition** – Normally displays the name of the partition containing the item (input point, terminal, panel, etc.) associated with the message.

**Public** – If the item associated with the message is marked as Public, this column will normally display whether the message is visible to other partitions.

**Query** – Displays the query string value (if it was defined) of the item associated with the message.

**Item** – Displays the name of the item (panel, terminal, input point, etc.) that is associated with the message.

**Operator** – Displays the name of the operator who handled the message (alarms in non pending state or audit messages only).

**Alarm Category** – Displays the Alarm Category to which the associated alarm belongs.

---

**Note:** The Message Routing Status indicator at the bottom of the Real Time List window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.

---



---

**Note:** If your facility uses the DVR feature and the selected transaction message displayed is associated with a camera, click the **Details** button located at the bottom of the window to launch the AV Player in live mode. As an alternative, you can click the **Details** drop-down arrow and select **AV Player (Live)** to launch AV Player in live mode or select **AV Player (Stored)** to launch AV Player in video retrieval mode. For more information, refer to your DVR documentation.

---

## To View all Options in the Real Time List:

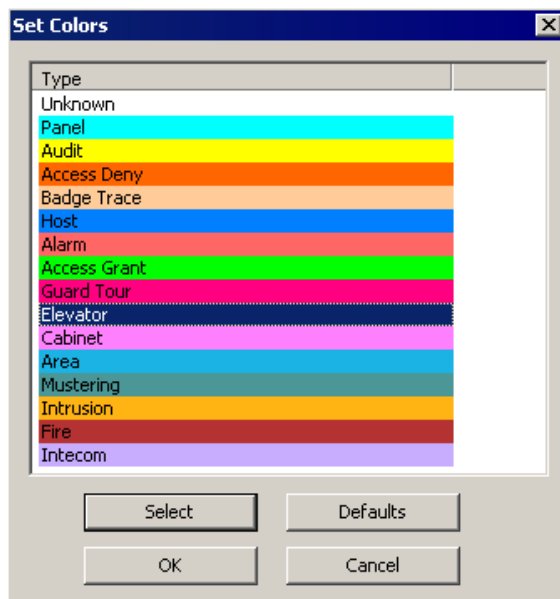
1. From the Real Time List window, select **All** from the options at the top of the window. All transactions will begin to accumulate in the scrolling list.

## To View Specific Options in the Real Time List:

1. Clear the **All** option and select only those options you wish to view. Only those options will begin to accumulate in the scrolling list.

## To Display Color Coded Transactions:

1. Select the **Color Items** check box. All transactions will display in a different color, using the default system colors.
2. To display a transaction type with a different color, click the **Set Colors** button. The Set Colors dialog box opens.

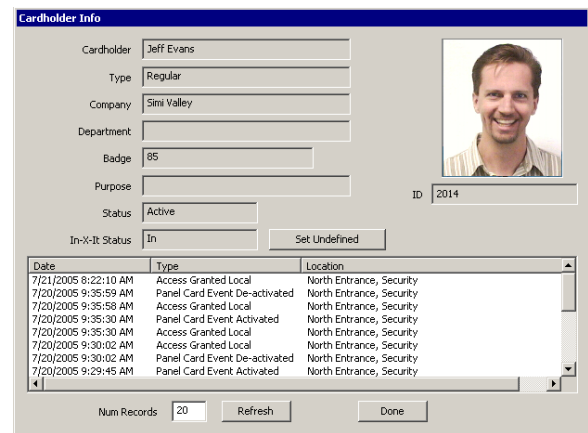


3. Select a transaction type, then click the **Select** button. A Color dialog box opens.
4. Select the desired color and click **OK** to return to the Set Colors dialog box.
5. Click the **Defaults** button if you wish to reset the colors to the default system colors.
6. Click **OK** to return to the Real Time List window.

## To Display Cardholder Details:

1. Select from the scrolling list, the transaction line item associated with a cardholder (Access Deny, Access Grant or Badge Trace transactions).

2. Click the **Details** drop-down arrow located at the bottom of the window, and select **Cardholder Info**. The Cardholder Info dialog box opens.



The top portion of the window shows the cardholder details including image, if available.

The bottom portion includes a chronological list of badge transactions associated with the cardholder.

3. To manually adjust the In or Out state of a badge until next badging, click the **Set Undefined** button.
4. To change the number of transactions displayed, enter the desired number in the **Num Records** field.
5. To update the list box with new data, click the **Refresh** button.
6. Click **Done** to return to the Real Time List.

## Printing the Real Time List

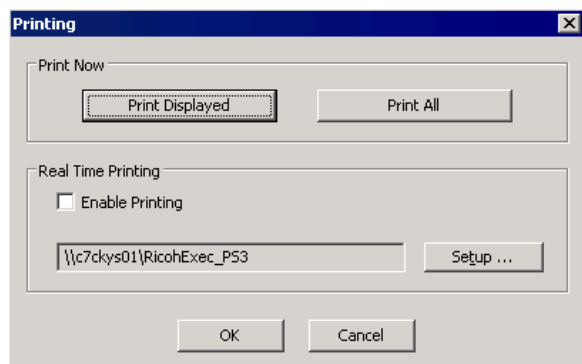
An operator can print from the workstation, all (or all displayed) transactions in the Real Time List, or print individual transactions as they occur.

**IMPORTANT:** Real time printing is not guaranteed on foreign language systems.

Printers must first be set up using the Windows Printer Settings dialog box. See your system administrator if you need more information, or refer to your Microsoft Windows documentation.

## To Print the Real Time List:

1. In the Real Time List window, select the **Printing** button in the top portion of the window. The Printing dialog box opens.



2. Click the **Print Displayed** button to print the transactions that are visible in the Real Time List box, or click the **Print All** button to print all transactions in the list.
3. Select a printer name and any other information for the printer to be used.
4. Click **OK** to start printing.

## To Print Real Time List Line Items:

1. In the Real Time List window, select the **Printing** button in the top portion of the window. The Printing dialog box opens.
2. Click the **Enable Printing** check box. Line items will continuously print as long as the Real Time List window is open or minimized on the workstation. Line items will stop printing when the Real Time List window is closed.
3. Click the **Setup** button to select a printer name and any other information for the printer to be used.

---

**Note:** We recommend a dot matrix printer be used exclusively for printing line items from the Real Time List, and independently from the transactions printed from the Site Parameters window.

---

4. Click **OK**. The printer name displays.
5. Click **OK** to enable printing.

## Using the Real Time Map

The Real Time Map displays the current status of terminals, inputs, outputs, and other defined elements on a map layout of your facility. Your system administrator can create maps using the Map Maker feature to “drag-and- drop” dynamic icons to their actual locations on imported layout images. All that is needed are simple layout maps that can be either scanned or drawn in any draw application, then saved in an importable format.

Once the maps are created, they are accessed from the P2000 System menu. If a terminal goes down or an alarm sets, the Real Time Map shows you the state change and exactly where the device is located.

## Sub Maps and Attachments

Your system administrator can create facility-level maps and attach sub maps (Normal and Popup maps) that detail specific areas in the facility. Sub maps may also contain sub maps to add further detail.

If an alarm sets in an area detailed in a sub map, the sub map icon will blink, indicating the location of the alarm. You can double-click the blinking sub map icon to jump to the associated detail map.

Map Maker provides image sets to display various device states such as “panel up,” “panel down,” “input set,” and so on. However, your system administrator can create icons and include them in image sets in Map Maker.

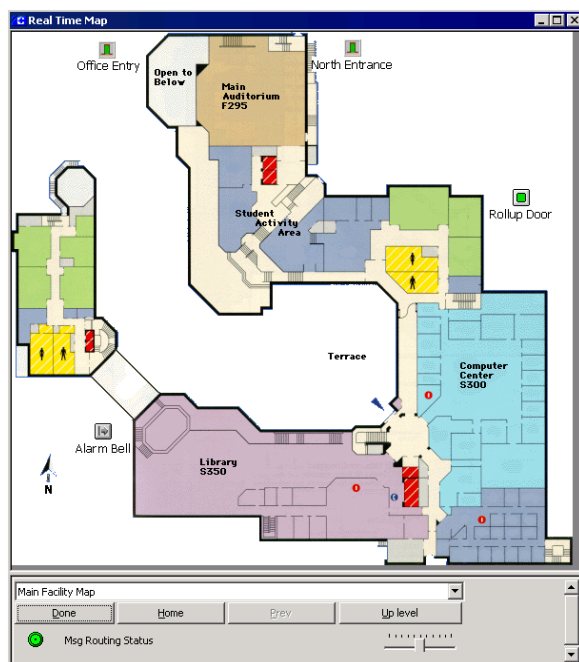
---

**Note:** The Message Routing Status indicator at the bottom of the Real Time Map window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.

---

## To View the Real Time Map:

1. From the P2000 Main menu, select **System>Real Time Map**. The Real Time Map window opens.



2. The current status of Panels, I/O Terminals, Readers, Input and Output points, and other defined elements will display as designed in Map Maker. The Main Map will display as assigned on Map Maker; however, you can select any map created in the system.

**Note:** Icons that are crossed out with a yellow bar indicate that the items' parent devices are not functioning. For example, an input point will be marked as unreliable if its parent terminal or panel is down.

**Note:** If your facility uses the DVR feature, when you right-click a map icon that is associated with a camera, a popup menu will display the "AV Player (Live)" option. If there are stored videos (associated with alarms), the popup menu will display the "Show Alarm Video" and "Start Recording" options. For more information, refer to your DVR documentation.

3. From the drop-down list at the bottom of the window, select the name of the map you wish to view. The list only displays Normal maps.
4. If your facility uses Map Attachments, use the **Prev** button to return to the previous map, or use the **Home** button to return to the main facil-

ity-level map. Clicking the **Up level** button will take you to the previous facility-level map.

**Note:** The **Prev**, **Home**, and **Up level** navigation tools are not used with Popup Map Attachments.

5. Use the slider control to enlarge or reduce the view of the active map. The zooming of the map can also be controlled with the mouse wheel. You can also use keyboard commands to enlarge or reduce the view of the active map. Use the **Up** or **Left** arrow keys to reduce the view and the **Down** or **Right** arrow keys to enlarge the view.
6. Click **Done** to exit the window.

## Opening a Door

You can open a door from a Real Time Map. The door will remain opened for the time configured in the door terminal's access settings, and then close. When a door is opened in this manner, the map icon image for the terminal changes from a closed door to an opened door, as long as the door is opened, then reverts back to a closed door image when the door closes.

1. Locate the door terminal icon for the door you wish to open.
2. Right-click the icon and select **Open Door** from the shortcut menu. The door opens for the configured time period, then closes.

**Note:** If you need to open the door for a period other than that configured, you must do so using the Door Control function.

## Activating Events from the Real Time Map

Events can be manually activated by an operator from the Real Time Map, rather than by the defined trigger conditions. Icons on the Real Time Map, such as Panels, Terminals or Inputs, can be configured to initiate events; or you can just place Event icons on the Map.

1. In the Real Time Map, locate the icon that contains the event you wish to activate.

- Right-click the icon and select the Event name from the shortcut menu. The event will be triggered.

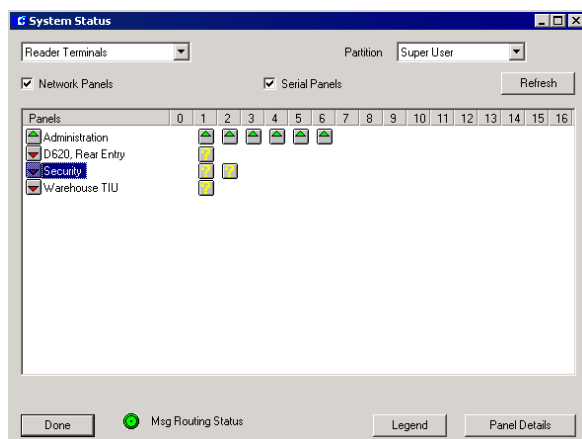
## Using the System Status

The System Status window is a dynamic display of the status of panels, associated devices, and other integration components configured in the system. This is a useful troubleshooting tool that allows you to quickly determine if panels and connected devices are communicating. If communications go down between the Server and the panels, the System Status window reports the last known status of the devices.

The System Status window is view only. You can manually change the status of a component using features accessed from the Control menu.

### To Access the System Status Window:

- From the P2000 Main menu, select **System>System Status**. The System Status window opens.



- Select a component (Reader Terminals, Input Terminals, Output Terminals, Inputs, Outputs, OTIS Elevator Status, Mustering Zones, Security Level Terminals, Intrusion Areas, Intrusion Zones, Intrusion Annunciators, Fire Zone, Fire Detector, Fire IO Module, Wireless Parameters, or Integration Components) from the drop-down list at the top left of the window. Information displayed for each component is presented at the end of this section.

- If this is a partitioned system, select the **Partition** to which the component belongs.
- Select the **Network Panels** and/or **Serial Panels** check box. The list of displayed devices will be limited according to the type of panel selected.
- Click the **Refresh** button to update the system status display.
- To see icon definitions for the different condition indicators, click the **Legend** button at the bottom of the window.



**Note:** Unreliable icons (crossed out with a yellow bar), indicate that the items' parent devices are not functioning. For example, an input point will be marked as unreliable if its parent terminal or panel is down.

- Click **Done** to close the System Status Legend dialog box.
- To display Serial or Network panel information, select the panel and click the **Panel Details** button. A Panel Details dialog box opens displaying current panel information.

Changes to **Polling Direction** for Serial Panels

**Name** – Displays the name given to the panel.

**Configured type** – Displays the panel type.

**Firmware version** – Displays the firmware version of the panel.

**IPL version** – Displays the IPL (Initial Program Load) version of the panel.

**Version description** – Displays the version description of the panel.

**Last poll communication** – Displays the last time the Server received information from the panel.

**Serial Number** – This the serial number assigned to the panel. Available only for S321-DIN panels.

**Primary or Alternate** – Displays whether the Primary or Alternate connection is in use for a network panel.

**Polling Direction** – Displays the polling direction (forward or reverse) in which the Server communicates with a legacy panel in a loop configuration.

**# of failed download connections** – Displays the number of times the Server has failed to connect to this panel.

**# of failed download transfers** – Displays the number of times an in-progress transfer was aborted.

**Delay Downloads Until** – Displays the time the Server will attempt the next download connection to this panel.

**Reset Time** – Click this button to immediately try a new download connection to this panel.

**Counters last cleared** – Displays the last time you clicked the Reset Counters button.

**Panel avg. clock drift (seconds)** – Displays the average time difference between the Server and the panel.

**Panel max clock drift (seconds)** – This is the largest time difference between the Server and the panel.

**Reset Counters** – Click this button to reset the values to 0.

9. Click **Done** to close the Panel Details dialog box and return to the System Status window.

**Note:** The Message Routing Status indicator at the bottom of the System Status window will be displayed in green to indicate that all communications between the workstation and the Server are up. If communications go down, the Message Routing Status indicator will turn red.

10. Click **Done** to close the System Status window.

### System Status – Reader Terminals

When you select **Reader Terminals** from the drop-down list, all panels in the system for the type of panel selected are listed by name in the Panels column. The reader terminals connected to the panels display by number in the same row as their panel. (The numbers correspond directly to the terminal number assigned when configuring the terminals. When you place the cursor over the terminal icon, the terminal name displays in a popup box.

### System Status – Input Terminals

When you select **Input Terminals**, all panels in the system for the type of panel selected are listed by name in the Panels column.

The input terminals display by number in the same panel row. When you place the cursor over the input terminal icon, the input terminal name displays in a popup box.



### System Status – Output Terminals

When you select **Output Terminals**, all panels in the system for the type of panel selected are listed by name in the Panels column.

The output terminals display by number in the same panel row. When you place the cursor over the output terminal icon, the output terminal name displays in a popup box.

### System Status – Inputs

When you select **Inputs**, all terminals and panels in the system for the type of panel selected, are listed by name in the Terminals/Panels column.

A status icon is represented for each possible input state. If no icons are present, no input points are associated with the terminal/panel.

The input points display by number in the terminal or panel row. When you place the cursor over the input point icon, the input point name displays in a popup box.

All input points above 16 are reserved for Soft inputs. You can expand the size of the window to view these inputs (up to 25).

### System Status – Outputs

When you select **Outputs**, all I/O terminals in the system for the type of panel selected are listed by name in the Terminals column.

A status icon is represented for each possible output state. The output points display by number in the terminal row. When you place the cursor over the output point icon, the output point name displays in a popup box.

---

**Note:** Your system administrator must enable the “Log Output Status Message” setting to display outputs in the System Status list.

---

### System Status - OTIS Elevator Status

When you select **OTIS Elevator Status**, all Otis elevator servers in the system are listed by name. The individual status icon indicates if the associated Otis Destination Entry Computers is Up or Down.

### System Status – Mustering Zones

When you select **Mustering Zones** from the drop-down list, the system displays the zone hardware status of each Muster Zone.

### System Status – Security Level Terminals

When you select **Security Level Terminals**, all panels that have security level terminals in the system, for the type of panel selected, are listed by name in the Panels column.

All security level terminals display in their respective panel row, showing the security level setting for each terminal. A number 0 indicates the security level is not used or is not assigned.

### System Status – Intrusion Areas

When you select **Intrusion Areas**, all intrusion areas associated to the intrusion panel display in the same row as their panel indicating their current status. You can issue commands for the areas by right-clicking the associated status icon. The following commands may be available, depending on the current state of the area:

**Arm (Aritech)** – Arms the selected Aritech area if at the time that you issue the command the area’s state permits it.

**Arm (Bosch)** – Arms the selected Bosch area with a pre-configured delay.

**Forced Arm (Aritech)** – Arms the selected Aritech area regardless of the area’s state at the time when you issue the command.

**Forced Arm (Bosch)** – Arms the selected Bosch area immediately.

**Disarm** – Disarms the selected area.

### System Status – Intrusion Zones

When you select **Intrusion Zones**, all intrusion zones associated to the intrusion panel display in the same row as their panel indicating their current status. You can issue commands for the zones by right-clicking the associated status icon. The following commands may be available, depending on the current state of the zone:

**Bypass On** – Commands the selected zone to be bypassed.

**Bypass Off** – Turns off bypassing of the selected zone.

**Reset** – (Not supported by Bosch). Resets the state of the selected zone. If you issue this command while the input point is still in alarm due to still being unsealed, you must seal the input and send this command again to reset it.

**ResetAck** – (Not supported by Bosch). Resets the state of the selected zone. If you issue this command while the input point is still in alarm due to still being unsealed, there is no need to re-send the command after the input is sealed. The command will remain valid and reset the zone as soon as the input seals.

### **System Status – Intrusion Annunciators**

When you select **Intrusion Annunciators**, all intrusion annunciators associated to the intrusion panel display in the same row as their panel indicating their current status. You can issue commands for the annunciators by right-clicking the associated status icon. The following commands may be available, depending on the current state of the annunciator:

**Activate** – Activates the selected annunciator.

**Deactivate** – Deactivates the selected annunciator.

### **System Status – Fire Zone**

When you select **Fire Zone**, all fire zones associated to the fire alarm panel display in the same row as their panel indicating their current status. The fire zones are displayed by number. You can display the status of up to 20 fire zones per row. If more than 20 fire zones are defined, they will display in the following rows. Place the cursor over a fire zone icon to display the fire zone name. You can issue commands for the fire zones by right-clicking the associated status icon. The following commands may be available, depending on the current state of the zone:

**Disable Zone** – Disables the selected fire zone(s).

**Enable Zone** – Enables the selected fire zone(s).

### **System Status – Fire Detector**

When you select **Fire Detector**, all fire detectors associated to the fire alarm panel display in the same row

as their panel indicating their current status. The fire detectors are displayed by number. You can display the status of up to 20 fire detectors per row. If more than 20 fire detectors are defined, they will display in the following rows. Place the cursor over a fire detector icon to display the fire detector name. You can issue commands for the fire detectors by right-clicking the associated status icon. The following commands may be available, depending on the current state of the detector:

**Disable Detector** – Disables the selected fire detector(s).

**Enable Detector** – Enables the selected fire detector(s).

### **System Status – Fire IO Module**

When you select **Fire IO Module**, all fire IO modules associated to the fire alarm panel display in the same row as their panel indicating their current status. The fire IO modules are displayed by number. You can display the status of up to 20 fire IO modules per row. If more than 20 fire IO modules are defined, they will display in the following rows. Place the cursor over a fire IO module icon to display the fire IO module name. You can issue commands for the fire input/output modules by right-clicking the associated status icon. The following commands may be available, depending on the current state of the IO module:

**Disable Module** – Disables the selected fire input/output module(s).

**Enable Module** – Enables the selected fire input/output module(s).

**Activate Module** – Activates the selected output of a fire input/output module(s).

**Deactivate Module** – Deactivates the selected output of a fire input/output module(s).

### **System Status – Wireless Parameters**

In addition to the normal Up, Down, or Override status of OSI devices, you can also verify status values of OSI devices that are related to the wireless signal they receive. When you select **Wireless Parameters** from the drop-down list, the list box displays the signal strength, packet ratio, and battery voltage values that are reported by the OSI devices.



These parameters are only updated by the reader about every 30 minutes (to conserve battery power). The System Status window will automatically refresh itself approximately every 30 seconds.

The Wireless Parameters display can be sorted by any column by clicking on the desired column header.

**Green** bars indicate that the OSI devices are operating within acceptable parameters. **Yellow** bars indicate a weakness in the devices (you will want to investigate further to determine the cause and if corrective action is required). **Red** bars indicate a fatal breakdown in the OSI devices.

Refer to the *P2000 Software User Manual* for detailed information on the status values for each OSI reader.

### System Status - Integration Components

Select **Integration Components** from the drop-down list to display the status of all Assa Abloy Door Service Routers (DSR) configured in the system. The status column indicates one of the following states:

**Unknown** – The status of the DSR has not yet been determined.

**Up** – The P2000 system is able to communicate with the DSR.

**Down** – The P2000 system is not able to communicate with the DSR.

**Disabled** – The P2000 system has been instructed not to communicate with the interface.

## Run Reports

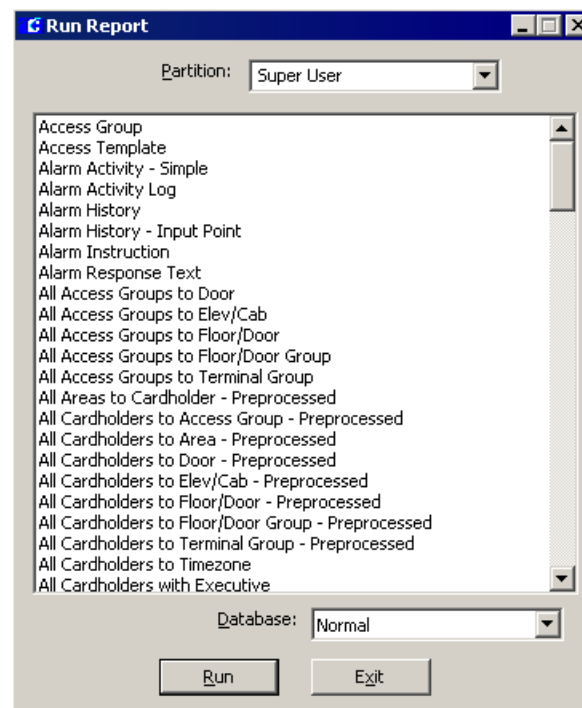
You can get information about cardholders, panels, alarms, and other system activity by running a report. P2000 Standard Reports can be sorted to produce the data you need, and they can be reviewed on screen or printed. A complete list of these reports is presented in the *P2000 Software User Manual*, along with a brief description of each and how they can be used.

P2000 Standard Reports provide the fields you need to generate reports on system databases and activities. If you do not find a report that meets your needs within P2000 Standard Reports, your system administrator

can create custom reports and import them into the P2000 system. Custom reports display in the Run Report list and can be run as any Standard Report.

### To Run a Report:

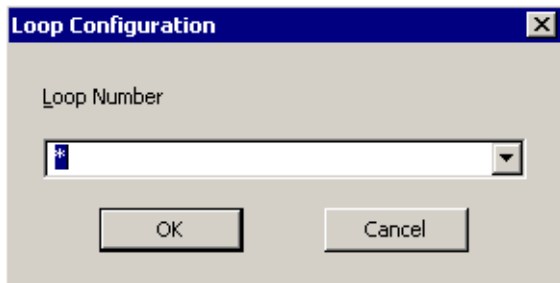
1. From the P2000 Main menu, select **Report>Run Report**. The Run Report dialog box opens.



2. If your system is partitioned, select the **Partition** that contains the data you want to report on. Also, the list box will display only the report names that belong to the partition selected.
3. Select the name of the report you wish to run.
4. Select the **Database** source: select **Normal** if the report will be generated from the current system data; or select **Archive** if you wish to run the report from an archived database.

**Note:** Before you run any "Preprocessed" report against an archived database, you must perform the "Update Preprocessed Report Archive tables" task from the Database Maintenance application, see the *P2000 Software User Manual* for details.

5. Click **Run**. Some reports, such as *Message Forwarding*, have no specific options and display directly in the preview window after you click **Run** and enter the printer options. Most reports, however, have filtering options and present a dialog box in which to select your choices. See the following example:



6. To run the default report, which lists all records, leave the asterisk in the field box.
7. To run a report on a specific option, choose the option from the drop-down list.

8. Click **OK**. Select a printer name and any other printer setup information.

---

**Note:** You must configure a default printer to retain the fonts displayed on a report. It is not required to have a printer physically connected to the workstation; you only need to setup the default printer. Do not use "Generic Text" printers. The **No Printer** option in the Print Setup dialog box displays P2000 reports correctly and is selected by default if you have not installed any printer drivers. Alternatively, you can manually select the **No Printer** option if you have installed one or more drivers, but you want to use a generic printer driver.

---

9. Click **OK**. After a moment, the report displays in the preview window.
10. Use the tool bar at the top of the window to scroll forward and back through the pages; resize the window for the best display, search for specific records, and print all or single pages of the report.