



bright blue.

bright blue.

User Manual

Ingersoll Rand Copyright Notice

© 2010 Ingersoll-Rand Company

This documentation and the software/hardware described herein, is furnished under license and may be used only in accordance with the terms of such license. Information contained in this manual is subject to change without notice and does not represent any commitment on the part of Ingersoll Rand. Ingersoll Rand assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

CONTACT INFORMATION

Schlage
Electronic Security
575 Birch Street
Forestville, CT 06010
Phone: 860-584-9158
Fax: 860-584-2136
www.schlage.com

To contact a local Ingersoll Rand Security Technologies Consultant in your area go to:
<http://securitytechnologies.ingersollrand.com/ssc.asp>

Contents

Ingersoll Rand Copyright Notice	1
---------------------------------	---

Introduction	7
--------------	---

Minimum System Requirements	7
Login	8
Automatic Timeout	10
Certificate Error	10
Main Page	11

Quick Start	13
-------------	----

Introduction	13
Checking Date and Time	14
Defining Users	16
Defining Time Zones	17
Door Setup	21
Schlage Adaptable AD-300 Series	21
Schlage VIP	26
SBB-RI	31
SBB-NRI	38
Schlage Adaptable AD-400 Series	43
Schlage Wireless Access	50
Personnel Setup	57
User Defined Fields	58
Adding Personnel	59
Adding Access Assignments to Existing Personnel	62
Access by Person	62
Copying Access Assignments	66
Access by Group	69

Activity 73

Introduction	73
Personnel Transactions	74
System and Device Transactions.....	74
Activity Monitor Settings	74
Personnel Transactions	75
System and Device Transactions.....	77

Reports 78

Introduction	78
Activity.....	78
All Access Attempts Valid/Invalid	80
All Access Attempts Valid	82
All Access Attempts Invalid	84
System User Activity	86
System Events (Communications, Power, Relays, and Contacts)	87
Contacts.....	88
Relays	89
Sample Activity Report.....	90
Personnel.....	91
Sample Personnel Report.....	92
Access	93
Access Permission by Person	93
Access Permission by Door	94
Sample Access Report	94
Devices	95
Sample Devices Report	96
Configuration.....	97
Time Zones	97
Calendar Events	97
Sample Configuration Report.....	98
Exporting Reports	98
Saving a report to the PC.....	98
Opening a report from the web browser.....	99
Enabling downloads with Internet Explorer	100
Determining how a report will open.....	103

Personnel 105

Introduction	105
Add new person	106
Personal Info.....	108
Credentials.....	108
Access Assignments.....	111
Access History	111
View, modify or delete personnel record.....	112
Import personnel data	113
Format requirements for imported .csv files	114
How to import a .csv file.....	115
Searching for a Specific Record.....	117
To Search for a Specific Person	118
Details on Search Terms	118
Advanced Search.....	120

Access Assignments 122

Introduction	122
View or change a person's access assignments.....	123
Permit All	125
Edit Details.....	126
Copy from	127
Time Zone.....	128
Toggle.....	129
Pass-Through	130
Block/Unblock	131
Remove All	131
Lockdown.....	132

Block / Unblock a person's access to the facility	133
Reset a person's antipassback state to neutral.....	136
Create common access assignments for a group of people	138
Block / Unblock a group of people's access to the facility	140
Reset everyone's antipassback state to neutral	141
Copy access assignments from one door to other door(s).....	142

Time Zones 144

Introduction	144
Add time zones	145
Clock Application	147
View, modify or delete time zone	148
To edit a Time Zone:	149

Calendar Events 150

Introduction	150
Add calendar event	151
View, modify or delete calendar event	152
To edit or delete an existing calendar entry:	152

Door Status & Control 153

Introduction	153
Status Table	154
Detailed Status.....	155
AD-300 Status.....	155
VIP Status.....	156
SBB-RI Status.....	157
SBB-NRI Status	158
PIM400-SBB Status	159
AD-400 Status.....	160
PIM-SBB Status	161
WAPM Status	162

Control Buttons	163
Door Setup	166

Introduction	166
Installation and Configuration	166
Add doors and hardware	167
View or modify door configuration	175
View or modify global settings	176
Test/Monitor:	184
Viewing installed hardware status	184
Status Table	185
bright blue Controller Status	185
AD-300 Status	186
VIP Status	187
SBB-RI Status	188
SBB-NRI Status	189
PIM400-SBB Status	190
AD-400 Status	191
PIM-SBB Status	192
WAPM Status	193
Account Administration	194

Introduction	194
Administrator	195
Manager	195
Operator	195
Utilities	196

Introduction	196
Set system date, time and time zone	197
To set the time manually:	197
To synchronize time to the PC's clock:	198
To synchronize to an internet time server:	198
To synchronize with video surveillance system:	199

Create or modify User Defined Fields	200
View System Information	201
View or modify network settings.....	202
Update system software.....	203
Miscellaneous Utilities.....	204
Database Utilities	205
Backup Database.....	206
Download and Restore database.....	207
Save archived transactions.....	210
 Glossary of Terms	 213

Index	217
-------------	-----

Introduction

CHAPTER 1

bright blue™ from Schlage is an easy-to-use web-based access control system. Its plug and play design means it does not require software installation or a dedicated PC. Any computer running a standard web browser (Internet Explorer 6.0, 7.0, 8.0 or Firefox 2.0, 3.0) can be used to access, monitor and manage the system. The software is user-friendly and easy to navigate and supports up to 32 doors and 5000 cardholders. The system supports standard card readers as well as the Schlage Adaptable AD-300 Series, Schlage VIP, Schlage Adaptable AD-400 Series and Schlage Wireless Access Series locks.

This document is designed as a detailed user manual for the **bright blue** system. It provides step-by-step instructions for:

- Setting up personnel, time zones, doors and holidays
- Assigning access permissions to personnel
- Monitoring system activity
- Running standard reports
- Setting up login permissions
- Troubleshooting

Minimum System Requirements

bright blue is currently supported on the following browsers: Microsoft Internet Explorer 7.0/8.0 and Firefox 2.0/3.0.

- The **bright blue** controller uses network port 80 to communicate to the user's computer. In order for the system to work properly, port 80 cannot be blocked by any firewall software.
- Javascript must be enabled in the browser.
- Minimum screen resolution is 1024 x 768. At this resolution the browser will need to be in full screen mode.
- Maximum screen resolution is 1600 x 1200.

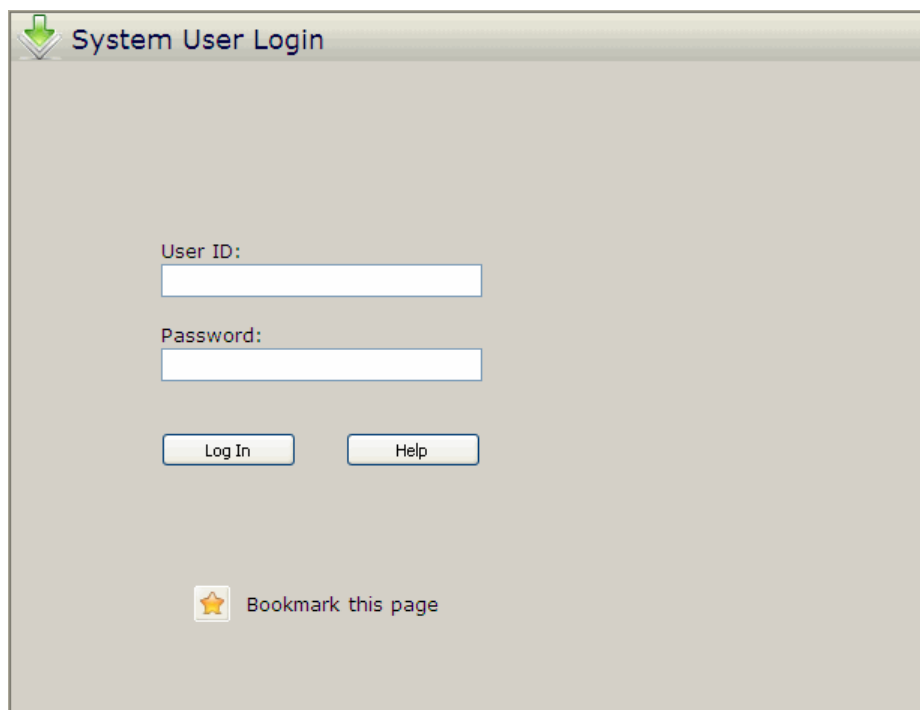
Note: It is recommended that the user change their password. Please see the Defining Users section in the Quick Start chapter for instructions on how to do this.

Login

Open a web browser and enter the IP address of the **bright blue** controller in the address field. Next, the login will appear. Type in the appropriate User ID and Password to log into the system (the default User ID is **usr**. The default Password is **password**). For more information on how to set up system user accounts and login levels see **Account Administration**.

Note: The Password field is case sensitive.

Log out at anytime by clicking on the Log Out button located in the bottom left corner of the screen.



The screenshot shows a web browser window titled "System User Login". The page has a light gray background. At the top left, there is a green downward-pointing arrow icon. Below the title, there are two text input fields. The first is labeled "User ID:" and the second is labeled "Password:". Below the "Password:" field, there are two buttons: "Log In" and "Help". At the bottom of the page, there is a yellow star icon followed by the text "Bookmark this page".

- **User ID** - Enter the User ID into this field.
- **Password** - Enter the password into this field.
- **Log In** - Click on this button to log in.
- **Help** - Click on this button to open the help files.
- **Bookmark this page** - Click on this button to add a bookmark for this page.

Note: It is recommended that the default password be changed upon logging in. Please see the Defining Users section in the Quick Start chapter for instructions on how to do this.

Note: Only one user is permitted to log into the system at any given time.

If an invalid User ID or Password is entered, the following message will occur.



If a user is currently logged in, the following message will occur



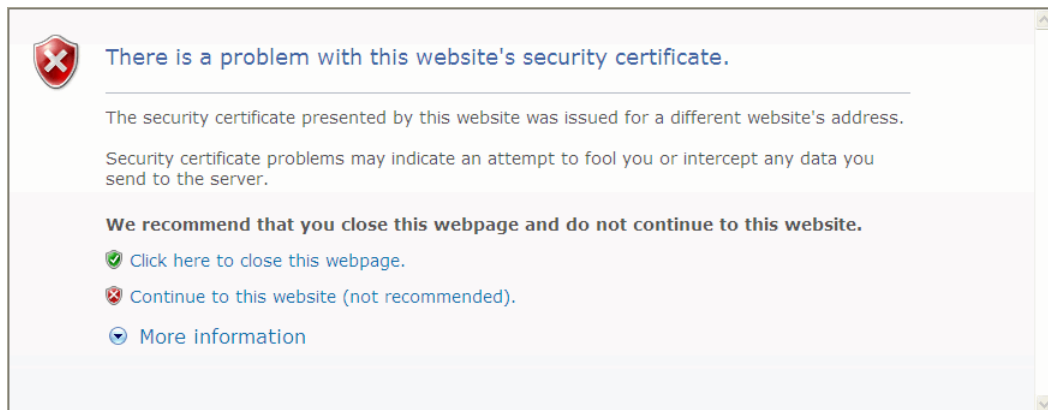
Automatic Timeout

For security purposes, the system will time out after 15 minutes of inactivity.

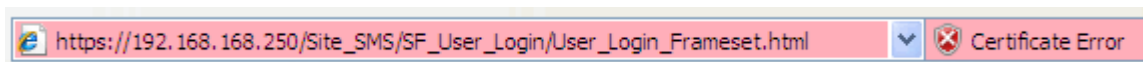


Certificate Error

If, during installation, SSL was enabled then this window will open the first time **bright blue** is accessed:



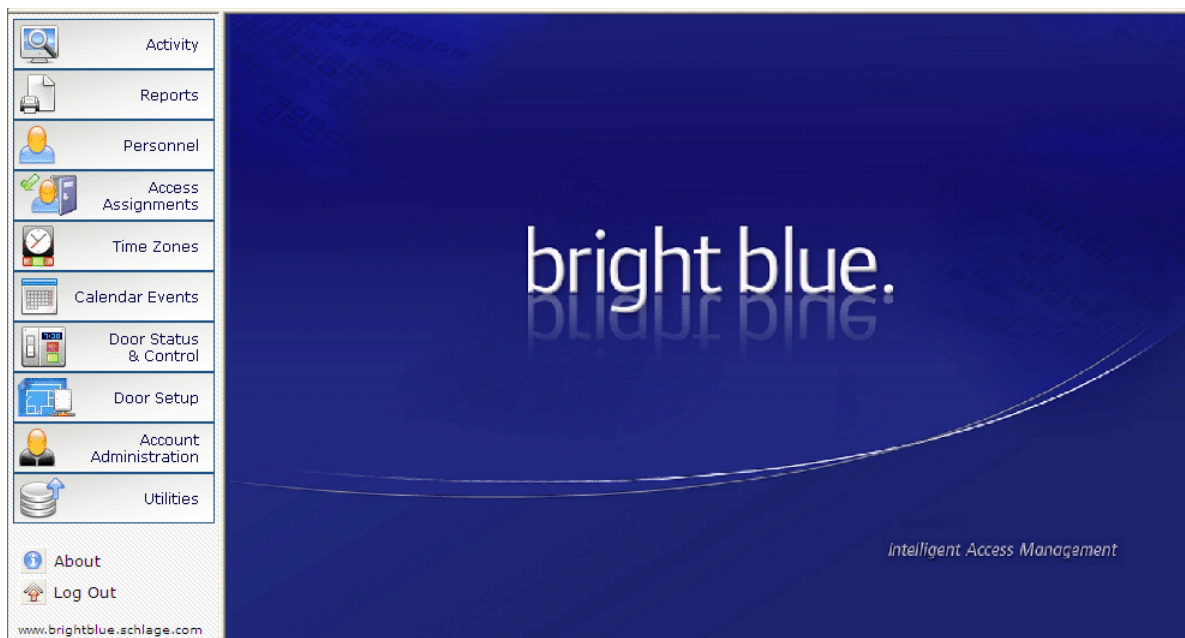
This is not an error and does not affect the use of **bright blue**. Click on the **Continue to this website** button to continue to the log in window. This may also effect the appearance of the address bar of the web browser, altering it to this:



Again, this is not an error and does not affect the use of **bright blue**.

Main Page

Upon login the user will be brought to the Main Page. All the functions of the system can be accessed using the navigation buttons on the left. These buttons are displayed according to the most commonly used components. Each of these tabs is explained at length in its own chapter later in the manual.



Activity - View the latest system transactions by person or by device.

Reports - Generate reports by person, activity, access and other criteria within a specified timeframe.

Personnel - Add, modify, delete and search for personnel information.

Access Assignments - Define access rights by personnel or device.

Time Zones - Define Time Zones to be used in the system.

Calendar Events - Specify events or days, such as holidays, that operate according to different schedules.

Door Status & Control - Manually override standard door functions and check the status of each door connected to the system.

Door Setup - Define door and lock types.

Account Administration - Set up administrator settings for users to access **bright blue**.

Utilities - Edit the database, set-up user defined fields, define date and time and edit facility codes.

About - See version and serial number information for **bright blue**

Log Out - Log out of the system.

Quick Start

CHAPTER 2

Introduction

The Quick Start chapter is here to get you up and running with **bright blue**. You'll find details on how to quickly set up users, define doors and add access assignments that will allow you to hit the ground running. Once you've followed the steps in this chapter you'll have a fully functional access control system keeping your building secure. After that you'll find a further wealth of information in the later chapters which describe the full depth of what **bright blue** can do. At any point during the Quick Start chapter if you want more information on a given subject just simply go to that section of the manual and then return to the Quick Start when you've finished.

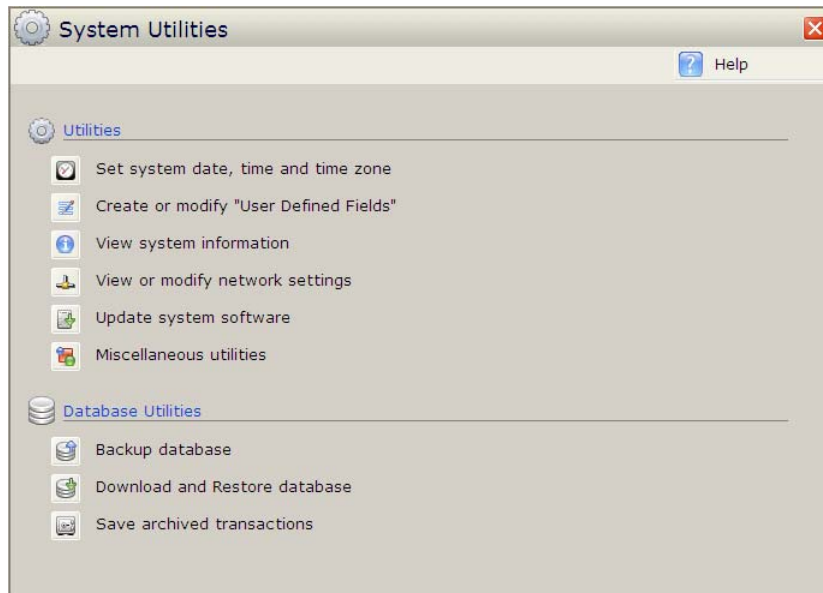
The following criteria must be defined as part of the initial system set up:

- System users and access levels
- Personnel and access assignments
- Lock definitions
- Time zones
- User-defined fields

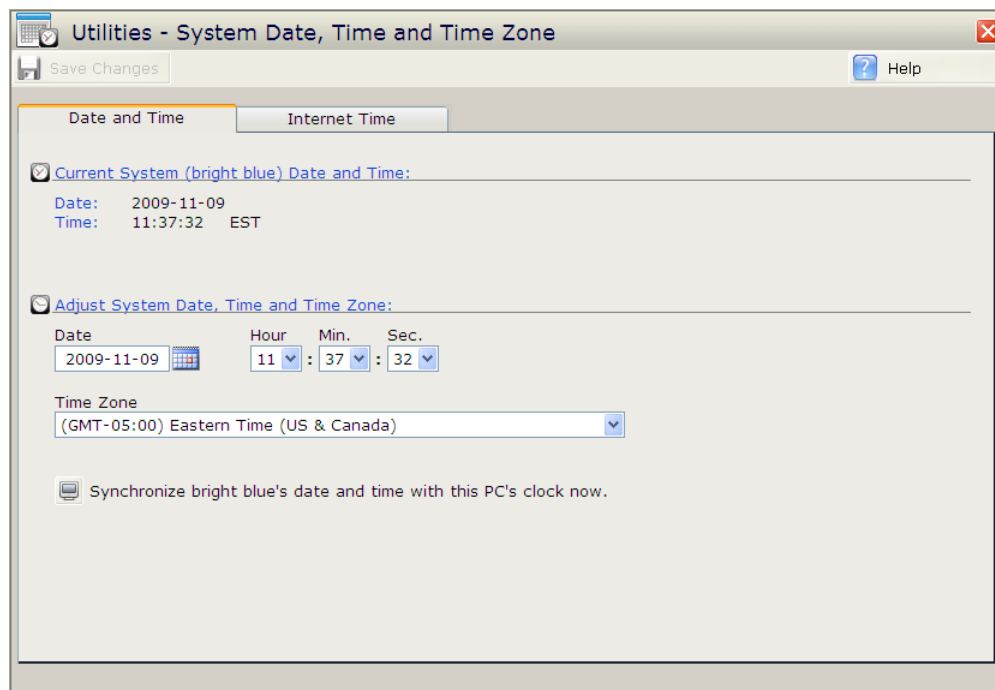
Checking Date and Time

The first step is to check that the date and time have been set.

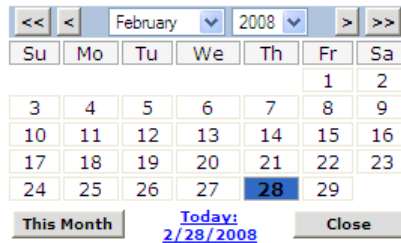
- 1 Click on the **Utilities** button on the left of the main screen. The System Utilities window will open.



- 2 Click on the **Set system date, time and time zone** button. The Utilities - System Date, Time, and Time Zone window will open.



- 3 Check that Current Time is correct. If correct, stop here and move on to the next section of the Quick Start chapter.
- 4 If not correct, set the date, time, and time zone.
 - a) Using the **Time** drop down boxes, specify the time.
 - b) Click on the calendar button to the right of the **Date** field. The calendar pop-up will open.



- c) Select the date. The calendar pop-up will close.
- d) Select the time zone from the **Regional Time Zone** list.
- e) Click on the **Apply** button. The system time, date, and time zone will be updated.

Defining Users

The next step is to define Account Administrators and associated Security Levels.

- 1 Click on the **Account Administration** button on the left side of the main screen.

The screenshot shows the 'Account Administration' window. At the top, there are buttons for 'New User', 'Save User', 'Delete User', and 'Help'. The main form contains fields for 'Last Name *' (Doe), 'First Name' (John), 'Middle Name/Initial', 'User ID *' (John D), 'Password *' (masked), and 'Password * (confirm)' (masked). To the right, the 'Security Level' section has three radio buttons: 'Administrator', 'Manager' (selected), and 'Operator'. Below the form, there is a section titled 'System User Accounts' containing a table with the following data:

User ID	System User	Security Level
John D	Doe, John	Manager
Jane S	Smith, Jane	Operator
test	test, test	Administrator
User	Clark, Aaron B	Administrator

- 2 Click on the **New User** button.
- 3 Type in the user's name in the appropriate fields.
- 4 Select the user's security level by clicking on the appropriate button. There are three security levels with various access rights to the system:
 - **Administrator** - Full access rights to the system.
 - **Manager** - Partial rights to the system. This level of user will not have access to the Utilities, Account Administration and Door Setup sections.
 - **Operator** - Limited rights to the system. Can access Activity, Reports, and Personnel sections.
- 5 Select a User ID and Password for the new user.
- 6 Click on the **Save User** button.

A user has now been defined. Repeat this process for every person that should have access to the system.

Note: After a new user has been defined with Administrator level access, it is recommended that the default user account (User ID: **usr** / Password: **password**) be deleted.

Defining Time Zones

Time Zones are user defined schedules (example: 8:00am - 5:00pm) that the system uses for various functions. A Time Zone schedule can be applied to a specific person to define when that person has access to a particular door. Any cardholder who attempts to access a door during a restricted Time Zone will be denied access. A Time Zone can also be used as a schedule for the automatic unlocking and re-locking of doors and for PIN-Pad operation. For additional information on door set-up and access assignments see the **Door Setup** and **Adding Access Assignment** sections of this chapter.

The Time Zones use a 24 hour clock.


- Midnight to Noon is represented as 0:00 to 12:00
- Noon to 11:59pm is represented as 12:00 to 23:59

TIP : To find the 24hr time:

1. If the desired time is in the AM then leave it as is.
2. If the desired time is in the PM then add 12 to the number.
3. Noon and Midnight are the exceptions.

Example:

- 11:30am is 11:30
- 1:00pm is 13:00
- Noon is 12:00
- Midnight is 0:00

Note: If you are unsure of the 24 hour time to use, click on the  button. A 12 hour standard clock will open allowing you to set the time in AM/PM. Once the time is set and the clock pop up closes, the time will be converted to 24 hour time.

- 1 Click on the **Time Zone** navigation button on the left side of the main screen. The **Time Zones - Tasks** window will open.



- Click on the **Add one or more time zones to the system** button. The **Time Zones - Edit** page will open.

Time Zones - Edit

Time Zone Name *

Notes

☒ **Time Zone Interval #1 (Required)**

Starts: Hour: 0 Min.: 00 Repeats: Every week of each month

Ends: Hour: 0 Min.: 00
 Effective Days of the Week:
 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Includes scheduled "Calendar Events"

☒ **Time Zone Interval #2 (Optional)**

Starts: Hour: 0 Min.: 00 Repeats: Every week of each month

Ends: Hour: 0 Min.: 00
 Effective Days of the Week:
 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Includes scheduled "Calendar Events"

☒ **Time Zone Interval #3 (Optional)**

Starts: Hour: 0 Min.: 00 Repeats: Every week of each month

Ends: Hour: 0 Min.: 00
 Effective Days of the Week:
 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Includes scheduled "Calendar Events"

☒ **Time Zone Interval #4 (Optional)**

Starts: Hour: 0 Min.: 00 Repeats: Every week of each month

Ends: Hour: 0 Min.: 00
 Effective Days of the Week:
 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Includes scheduled "Calendar Events"

- Complete the **Time Zone Name** field. This name should be descriptive of the time zone and easily recognizable. Example: Shift 1: 8 am - 6 pm, Mon-Fri. The **Notes** field is optional and may be used to provide more detailed information about the time zone.
- Enter criteria for the **Time Zone Interval #1** section.

- a) Enter **Starts** and **Ends** time for the Time Zone.
- b) Select Time Zone repeat frequency using the drop down box. See the Time Zone chapter for more details.
- c) Check the appropriate boxes under **Effective Days of the Week** to define days in which the Time Zone will be in effect.
- d) Check the **Includes scheduled "Calendar Events"** box if the Time Zone is to be active during Calendar Events. Examples of Calendar Events might be recurring meetings, Holidays, etc. For more information on Calendar Events, please see the Calendar Events chapter.

Example: Shift 1 is to run from 8:00am to 6:00pm, Monday through Friday, every week of the month except on Calendar Events.

In **Time Zone Interval #1** set the **Starts** time at: 8:00 and set the **Ends** time at: 18:00. Set the **Repeats** drop down to Every week of the month. Under **Effective Days of the Week**, check the boxes for **Mon, Tue, Wed, Thu, and Fri**. Leave the **Includes scheduled "Calendar Events"** box unchecked.

- 5 If this Time Zone is going to span two separate periods of time in the same day or if the Time Zone is to start before midnight and end after midnight, then enter criteria for the **Time Zone Interval #2** section.

Note: If the Time Zone spans midnight, Interval #1 must end at 23:59 and Interval #2 must begin at 0:00.

- a) Click on the Enable button to the right of the Time Zone Interval section to enable the interval.
- b) Enter **Starts** and **Ends** time for Time Zone Interval #2.
- c) Select Time Zone repeat frequency using the drop down box. Please see the Time Zone chapter for more details.
- d) Check the appropriate boxes under **Effective Days of the Week** to define days in which this Time Zone will be in effect.
- e) Check the **Includes scheduled "Calendar Events"** box if this Time Zone is to be active during Calendar Events.

Example: Shift 3 is to run from 8:00pm to 4:00am, Monday through Friday, every week of the month including Calendar Events. This Time Zone will need a second interval because it spans midnight. The first Time Zone Interval will be programmed for 8:00pm to Midnight, Monday through Friday. The second Time Zone Interval will be programmed for Midnight to 4:00am, Tuesday through Saturday.

In **Time Zone Interval #1** set the **Starts** time at 20:00. Set the **Ends** time at: 23:59. Set the **Repeats:** drop down to Every week of the month. Under Effective Days of the Week, check the boxes for **Mon, Tue, Wed, Thu, and Fri**. Check the **Includes scheduled "Calendar Events"**.

In **Time Zone Interval #2** set the **Starts** time at 0:00. Set the **Ends** time at 4:00. Set the **Repeats:** drop down to Every week of the month. Under Effective Days of the Week, check the boxes for **Tue, Wed, Thu, Fri, and Sat**. Check the **Includes scheduled "Calendar Events"**.

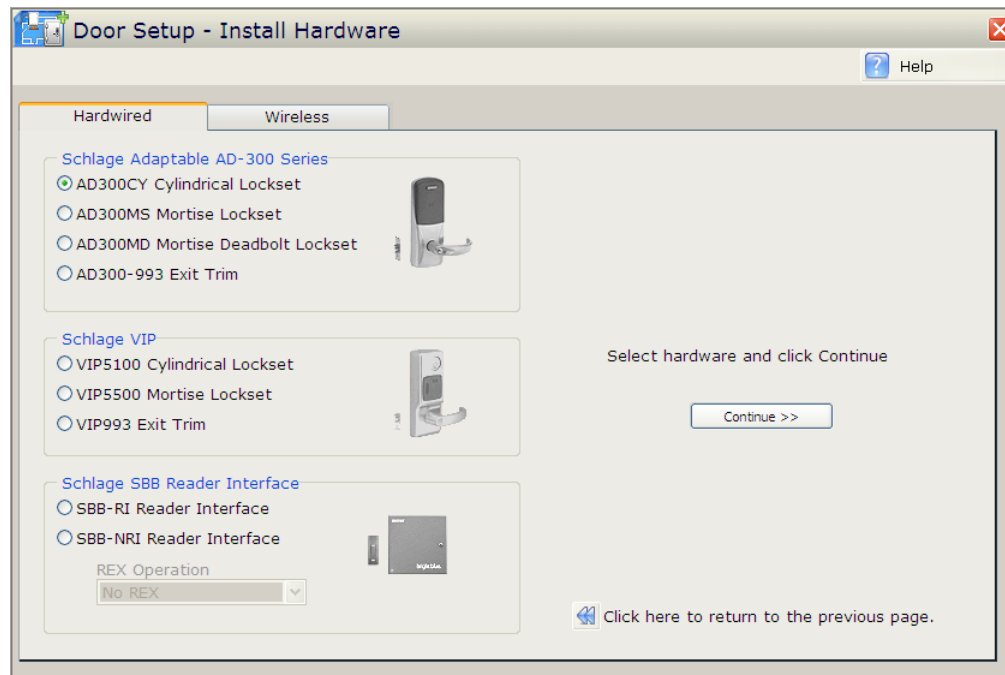
- 6 If this Time Zone requires more intervals, repeat step 5 above for Interval 3 and Interval 4.
- 7 Click the **Save Time Zone** button at the top of the screen.
- 8 Repeat steps 3 through 7 for each Time Zone.

Door Setup

This section details the door set-up process. Each category of lock (AD-300, AD-400, SBB-NRI, VIP, Wireless, and SBB-RI) requires a different set-up procedure. Determine the type of locks to be used and follow the appropriate directions below.

Schlage Adaptable AD-300 Series

- 1 Open **Door Setup** by clicking on the Door Setup navigation button on the left side of the main screen.
- 2 Click the **Add doors and hardware** button in the Installation and Configuration section. The **Door Setup - Install Hardware** window will open.

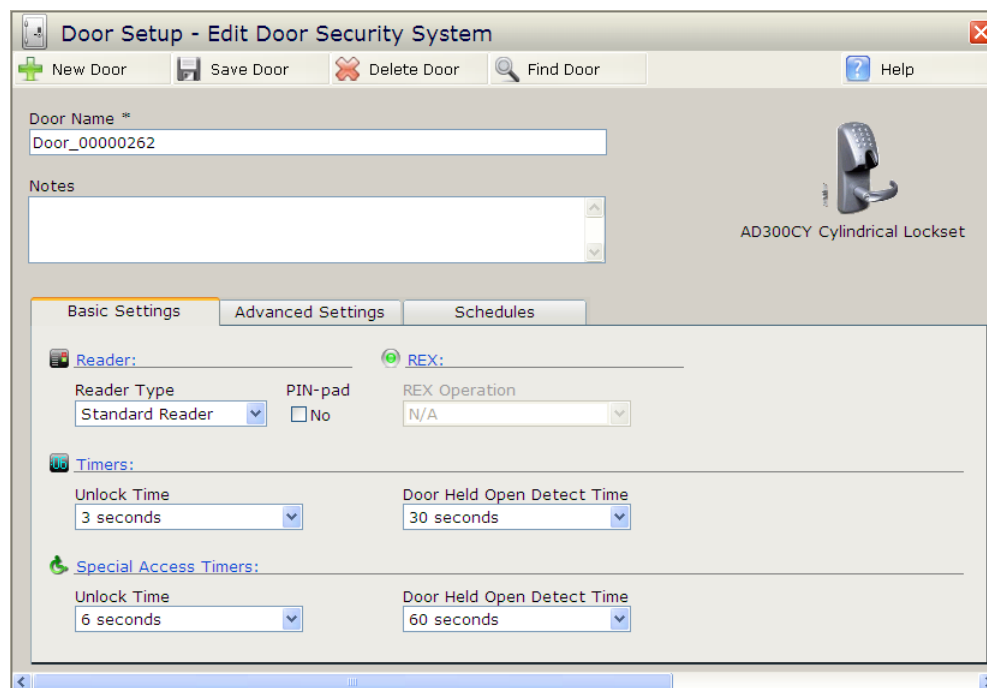


- 3 Click on the appropriate AD-300 lock type that you want to set up.

- Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.



- Click on **OK** if correct. The **Door Setup - Edit Door Security System** window will open.



- Complete the **Door Name** and **Notes** fields.

- 7 Select the **Basic Settings** tab in the bottom half of the screen. This section is broken up into three areas: Reader Type, Timers and Special Access Timers. The REX function is disabled as it is not used with this lock type.

The screenshot shows the 'Basic Settings' tab selected. The interface is divided into three main sections: **Reader:**, **Timers:**, and **Special Access Timers:**.
 - In the **Reader:** section, 'Reader Type' is set to 'Standard Reader', 'PIN-pad' is unchecked (labeled 'No'), and 'REX Operation' is set to 'N/A'.
 - In the **Timers:** section, 'Unlock Time' is set to '3 seconds' and 'Door Held Open Detect Time' is set to '30 seconds'.
 - In the **Special Access Timers:** section, 'Unlock Time' is set to '6 seconds' and 'Door Held Open Detect Time' is set to '60 seconds'.

- 8 Define the following **Reader** options:
- Using the **Reader Type** drop down box, select the Reader Type:
Standard - Readers for any location not using anti-passback.
Entry - Readers that are defined as entry readers for anti-passback purposes..
Exit - Readers that are defined as exit readers for anti-passback purposes.
 - Click the **PIN-pad** option to enable the PIN-pad for this Reader. The Schedules tab will be used to determine when a PIN is required in addition to a credential.
- 9 Define the following **Timer** options:
- Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.
 - Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.
- 10 Define the following **Special Access Timer** options:
- Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.
 - Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

- 11 Select the **Advanced Settings** tab in the bottom half of the screen.

The screenshot shows the 'Advanced Settings' tab selected. The 'Connection' section includes 'Channel Number' (dropdown, 'Channel 1'), 'AD300 Lock Address' (dropdown, '1'), and an 'Installed' checkbox. The 'Event Reporting' section includes 'Enable "Clutch Position" state change reporting' and 'Enable "REX" state change reporting' checkboxes. The 'Enhanced Security' section includes a 'Disable door access during system start-up' checkbox. The 'Video Surveillance System Event Logging' section includes a 'Camera' dropdown menu set to '<not enabled>' and a small icon.

- 12 Define the following options in the **Connection** section:

- Select the **Channel Number**. This specifies the channel number on the controller that the device is wired to.
- Select the **AD300 Lock Address**. This field must match the address that is specified by the Schlage Utility Software (PDA). Please see the installation guide for details.
- Installed**. Click this box if this lock is currently installed on the system.

- 13 Define the following options in the **Event Reporting** section:

- Check the **Enable "Clutch Position" state change reporting** box for the ability to generate reports and see activity based on when the lock's clutch is engaged/disengaged.
- Check the **Enable "REX" state change reporting** box for the ability to generate reports and see activity based on when the REX is activated.


- 14 Check the **Disable door access during system start-up** option if you wish to disable access to this door any time the system restarts.

- 15 If the **bright blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.

- 16 Select the **Schedule** tab in the bottom half of the screen.

- 17 Define the following options in the **Unlock Schedule** section:

- a) Select the time zone for the door using the **Unlock Time Zone** drop down box.


Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- b) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. This feature is used to enable an override when the first valid access card is presented during a time zone. The override will re-lock according to original schedule.

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked if no one is in the building. In the Unlock Timezone drop down select the 7:00am to 5:00pm Time Zone. Then check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after someone has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

- 18 If the PIN-pad option was checked in the Basic Settings tab, then use the **PIN Required Schedule** section to define when a credential AND a PIN are required.

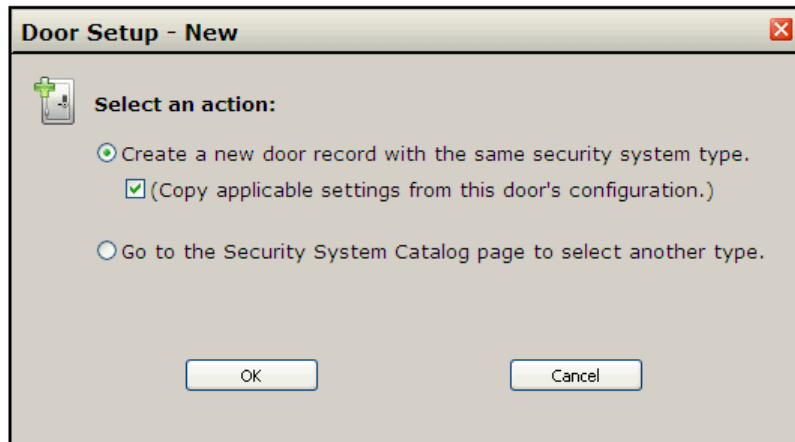
- a) Use the **PIN Required Time Zone** drop down box to define when a PIN will be required.

Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- 19 Define the following options in the **Toggle Cancel Time** section:

- a) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked** box to enable this feature. This will lock this door automatically at the specified time.
- b) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.
- c) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.

- 20 Click the **Save Door** button at the top of the screen. The screen will refresh and the door profile will be saved.
- 21 To add additional doors, click the **New Door** button at the top of the screen. The **Door Setup - New** pop-up window will open.

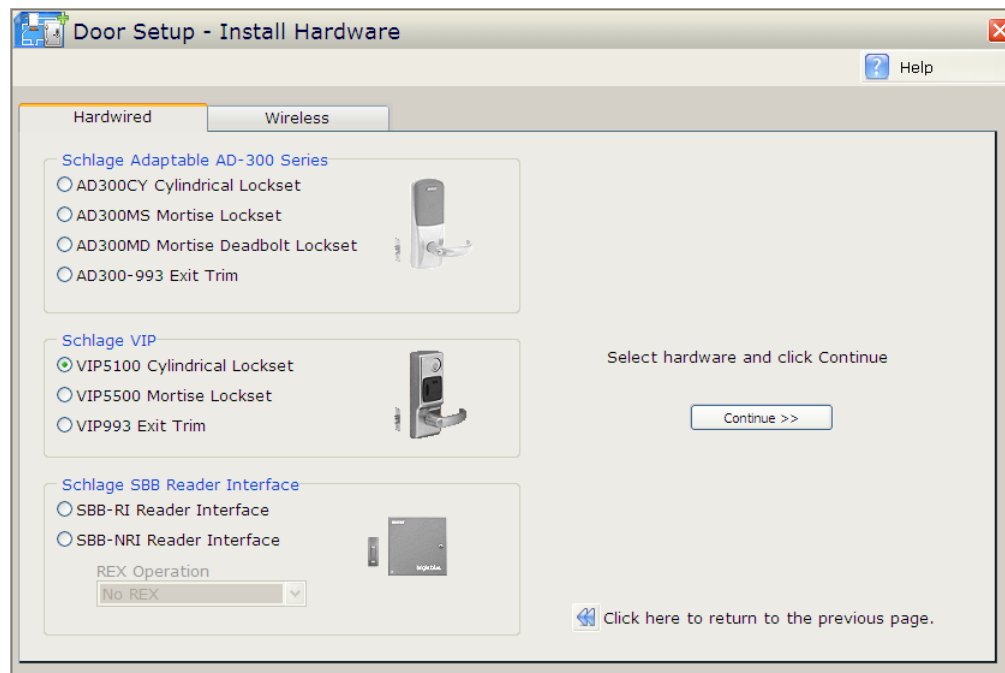


- 22 Select from the following options:
 - **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat steps 6 through 21 above.
 - **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat steps 20 and 21 above.
 - **Go to the Security System Catalog page to select another type.** Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Electronic Security System Hardware** window will open. Follow the steps for the lock type selected.

Schlage VIP

- 1 Open **Door Setup** by clicking on the Door Setup navigation button on the left side of the main screen.

- 2 Click the **Add doors and hardware** button in the Installation and Configuration section. The **Door Setup - Install Hardware** window will open.



- 3 Click on the appropriate VIP lock type that you want to set up.
- 4 Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.



- 5 Click on **OK** if correct. The **Door Setup - Edit Door Security System** window will open.

- 6 Complete the **Door Name** and **Notes** fields.
- 7 Select the **Basic Settings** tab in the bottom half of the screen. This section is broken up into three areas: Reader Type, Timers and Special Access Timers. The REX function is disabled as it is not used with this lock type.

- 8 Define the following **Reader** options:
- Using the **Reader Type** drop down box, select the Reader Type:
Standard - Readers for any location not using anti-passback.
Entry - Readers that are defined as entry readers for anti-passback purposes..
Exit - Readers that are defined as exit readers for anti-passback purposes.
 - The **PIN-pad** option will be disabled. VIP locks do not support a PIN reader.

9 Define the following **Timer** options:

- a) Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.
- b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.

10 Define the following **Special Access Timer** options:

- a) Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.
- b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

11 Select the **Advanced Settings** tab in the bottom half of the screen.

The screenshot shows the 'Advanced Settings' tab of a configuration window. It contains the following elements:

- Connection:**
 - Channel Number *: <undefined>
 - VIP Lock Address *: <undefined>
 - ☐ Installed
- Event Reporting:**
 - ☐ Enable "Lock/Unlock" relay state change reporting
 - ☐ Enable "REX" state change reporting
- Video Surveillance System Event Logging:**
 - Camera: <not enabled>
- Enhanced Security:**
 - ☐ Disable door access during system start-up

12 Define the following options in the **Connection** section:

- a) Select the **Channel Number**. This specifies the channel number on the controller that the device is wired to.
- b) Select the **VIP Lock Address**. This field must match the address that is specified by the dip switches in the VIP lock. Please see the VIP lock installation guide for details.
- c) **Installed**. Click this box if this lock is currently installed on the system.

13 Define the following options in the **Event Reporting** section:

- a) Check the **Enable "Lock/Unlock" relay state change reporting** box for the ability to generate reports and see activity based on when the lock is locked and unlocked.
- b) Check the **Enable REX state change reporting** box for the ability to generate reports and see activity based on when the REX is activated.


14 Check the **Disable door access during system start-up** option if you wish to disable access to this door any time the system restarts.

15 If the **bright blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.

- 16 Select the **Schedule** tab in the bottom half of the screen.

- 17 Define the following options in the **Unlock Schedule** section:

- a) Select the time zone for the door using the **Unlock Timezone** drop down box.

Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- b) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. This feature is used to enable an override when the first valid access card is presented during a time zone. The override will re-lock according to original schedule.

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked if no one is in the building. In the Unlock Timezone drop down select the 7:00am to 5:00pm Time Zone. Then check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after someone has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

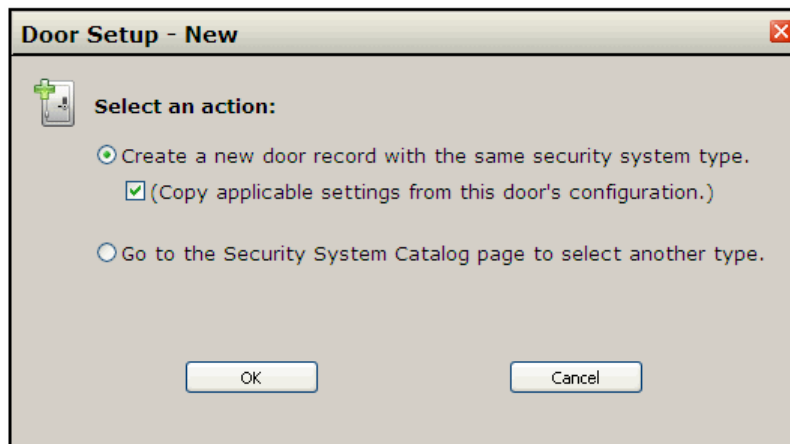
- 18 The **PIN Required Schedule** section will be disabled. This is not an option with VIP locks.

- 19 Define the following options in the **Toggle Cancel Time** section:

- a) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked** box to enable this feature. This will lock this door automatically at the specified time.
- b) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.
- c) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.

- 20 Click the **Save Door** button at the top of the screen. The screen will refresh and the door profile will be saved.

- 21 To add additional doors, click the **New Door** button at the top of the screen. The **Door Setup - New** pop-up window will open.

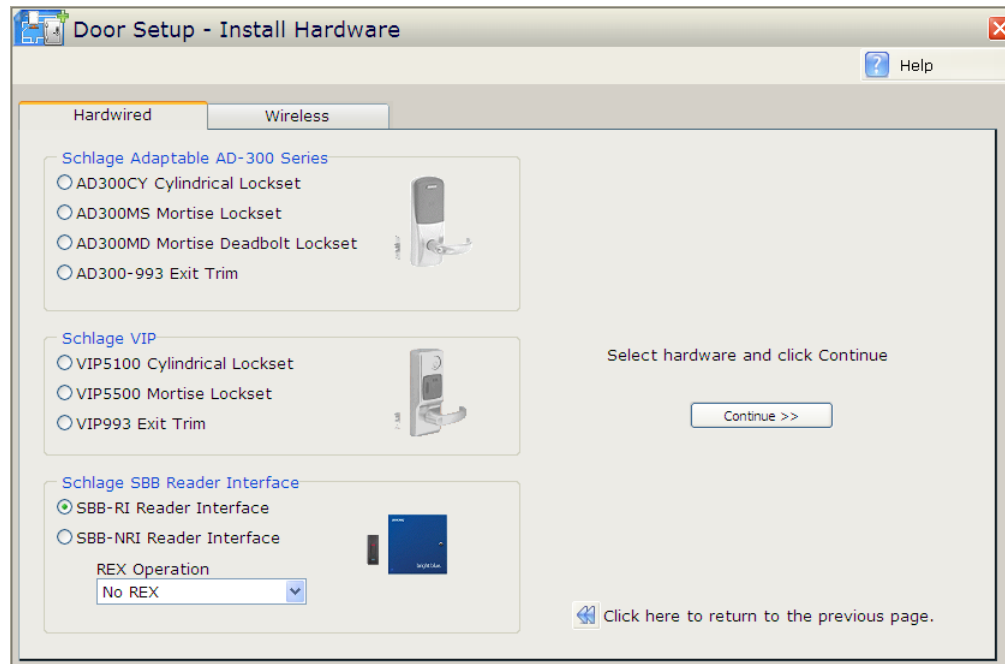


- 22 Select from the following options:
- **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat steps 6 through 209 above.
 - **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat steps 20 and 21 above.
 - **Go to the Security System Catalog page to select another type.** Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Electronic Security System Hardware** window will open. Follow the steps for the lock type selected.

SBB-RI

- 1 Open the **Door Setup** section by clicking on the Door Setup navigation button on the left side of the main screen.

- Click the **Add doors hardware** button in the Installation and Configuration Tasks section. The **Door Setup - Install Hardware** window will open.



- Click on the radio button to the left of SBB-RI Reader Interface.
- Select what type of REX this SBB-RI will use from the REX Operation drop down box.

REX stands for request-to-exit and refers to either a mechanical button or PIR (motion sensor) that is used to gain egress from a secured door.

- **No REX** - No REX for this door. Request-to-exit is not in use. Door Forced Open is not reported.
- **REX - No Unlock** - Request-to-exit is in use to report a valid exit and bypass door contact reporting for a period of time. The REX device will not unlock the electrified locking device. This is typically used when either a door knob or exit bar are used as these devices manually unlatch from the inside of the opening.
- **REX - Unlock** - Request-to-exit is in use to report a valid exit, bypassing door contact reporting for a period of time AND unlocking the electrified locking device. This is typically used when a magnetic lock is used and must be unlocked from the inside of the door to allow exiting.

- 5 Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.



- 6 Click on **OK** if the selected lock is correct. The **Door Setup - Edit Door Security System** window will open.
- 7 Complete the **Door Name** and **Notes** fields.
- 8 Select the **Basic Settings** tab on the bottom half of the screen.

- 9 Define the following **Reader** options:
 - a) Using the **Reader Type** drop down box, select the Reader type:
 - Standard** - Readers for any location not using anti-passback.
 - Entry** - Readers that are defined as entry readers for anti-passback purposes..
 - Exit** - Readers that are defined as exit readers for anti-passback purposes.
 - b) Click the **PIN-pad** option to enable the PIN-pad for this Reader. The Schedules tab will be used to determine when a PIN is required in addition to a credential.

Note: Only revision 11 and above SBB-RIs will accept a PIN. Earlier models do not have this functionality. To determine revision number, see the **Determining Version Number** section below.

- 10 Select the REX setting. REX stands for Request-to- Exit and refers to either a mechanical button or motion sensor that is used to gain exit from a secured door. Using the **REX Operation** drop down box, define the REX operation for the door.

- **No REX** - No REX for this door. Request-to-exit is not in use. Door Forced Open is not reported.
- **REX - No Unlock** - Request-to-exit is in use to report a valid exit and bypass door contact reporting for a period of time. The REX device will not unlock the electrified locking device. This is typically used when either a door knob or exit bar are used as these devices manually unlatch from the inside of the opening.
- **REX - Unlock** - Request-to-exit is in use to report a valid exit, bypassing door contact reporting for a period of time AND unlocking the electrified locking device. This is typically used when a magnetic lock is used and must be unlocked from the inside of the door to allow exiting.

11 Define the following **Timer** options:

- a) Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.
- b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.

12 Define the following **Special Access Timer** options:

- a) Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.
- b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

13 Select the **Advanced Settings** tab in the bottom half of the screen.

The screenshot shows the 'Advanced Settings' tab selected. The interface includes the following elements:

- Basic Settings** | **Advanced Settings** | **Schedules**
- Connection:**
 - Channel Number *:
 - SBB-RI Address *:
 - ☐ Installed
- Event Reporting:**
 - ☐ Enable "Lock/Unlock" relay state change reporting
 - ☐ Enable "REX" state change reporting
- Video Surveillance System Event Logging:**
 - Camera:
- Enhanced Security:**
 - ☐ Disable door access during system start-up

14 Define the following options in the **Connection** section:

- a) Set the **Channel Number**. This specifies the channel on the controller the device is wired to.
- b) Set the **SBB-RI Address**. This field must match the address that is set on the address jumpers. Please see the installation guide for more details.
- c) **Installed**. Click this box if this lock is currently installed on the system.


15 Define the following options in the **Event Reporting** section:

- a) Check the **Enable "Lock/Unlock" relay state change reporting** box if you wish to generate reports and see activity based on when this lock is locked and unlocked.
- b) Check the **Enable REX state change reporting** box if you wish to generate reports and see activity based on when the REX is activated.

- 16 Check the **Disable door access during system start-up** option if you wish to disable access to this door any time the system restarts.
- 17 If the **bright blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.
- 18 Select the **Schedule** tab in the bottom half of the screen.

- 19 Define the following options in the **Unlock Schedule** section:

- a) Select the time zone for the door using the **Unlock Timezone** drop down box.


Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- b) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. This feature is used to enable an override when the first valid access card is presented during a time zone. The override will re-lock according to original schedule.

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked if no one is in the building. In the Unlock Timezone drop down select the 7:00am to 5:00pm Time Zone. Then check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after someone has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

- 20 If enabled, define the **PIN Required Schedule** section.

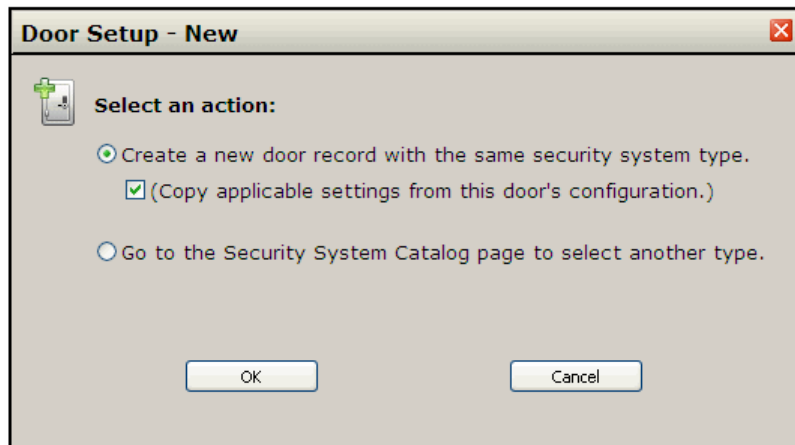
- a) Select the time zone during which a pin will be required by using the **PIN Required Time Zone** drop down box.

Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- 21 Define the different options in the **Toggle Cancel Time** section:

- a) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked** box to enable this feature. This will lock this door automatically at the specified time if the door was left in a toggle-open state.

- b) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.
 - c) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.
- 22 Click the **Save Door** button at the top of the screen. The screen will refresh and the door will be saved.
- 23 To add additional doors, click the **New Door** button at the top of the screen. The **Door Setup - New** pop-up window will open.



- 24 Select from the following options:
- **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat steps 6 through 22 above.
 - **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat steps 22 and 23 above.
 - **Go to the Security System Catalog page to select another type.** Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Electronic Security System Hardware** window will open. Follow the steps for the lock type selected.

Determining Version Number of SBB-RI

If you are unsure of the version number of any SBB-RI's connected to the system you can determine it using the diagnostic function of **bright blue**. The SBB-RI should already be installed in the system and should already have a channel and address number. The channel and address numbers will be used to differentiate between SBB-RI's connected to the system. Follow the directions below to find the version number.

- 1 Log into **bright blue**.
- 2 In the address bar of the web browser enter in the **IP address** of **bright blue** followed by **:30125** and press **Enter**.

Example: if **bright blue**'s IP address is 10.45.49.126 then enter 10.45.49.126:30125 into the address bar and press Enter to access the diagnostic screen.

- 3 A window will open asking if you want to navigate away from the **bright blue** window. Click **Ok**. The Diagnostic window will open.

Enter your name: and password:

Please indicate which command you would like to execute:

☐ System ☐ Reader ☐ Tz ☐ Slave
☐ Clock ☐ Relay ☐ Area ☐ Rname
☐ Holiday ☐ Contact ☐ Alarm ☐ More
☐ SiteCode ☐ Badge ☐ Schedule

and a possible parameter:

- 4 Click on the **Reader** button to select it.
- 5 Click **Submit**. The Reader Definition window will open.

Reader Definition

DevID	IArID	EArID	Chn	Addr	lo/hi	DoorType	RdrType	RIType	Kpd	ARL	APt	OEM	Rev	ADS	Condition
111	3	1	1	1		00000001	Normal	GRI	No	No	0	G1	00.02	No	Comm
265	25	1	1	2		00000001	Normal	GRI	No	No	0	G1	00.11	No	Comm
312	34	0	1	6	**(6, 10)**	00000000	Unknown	Wpim	No	No	0	WA	00.00	No	Comm
314	35	1	1	6		00000001	Normal	Wapm	No	No	0	w6	00.00	No	Comm

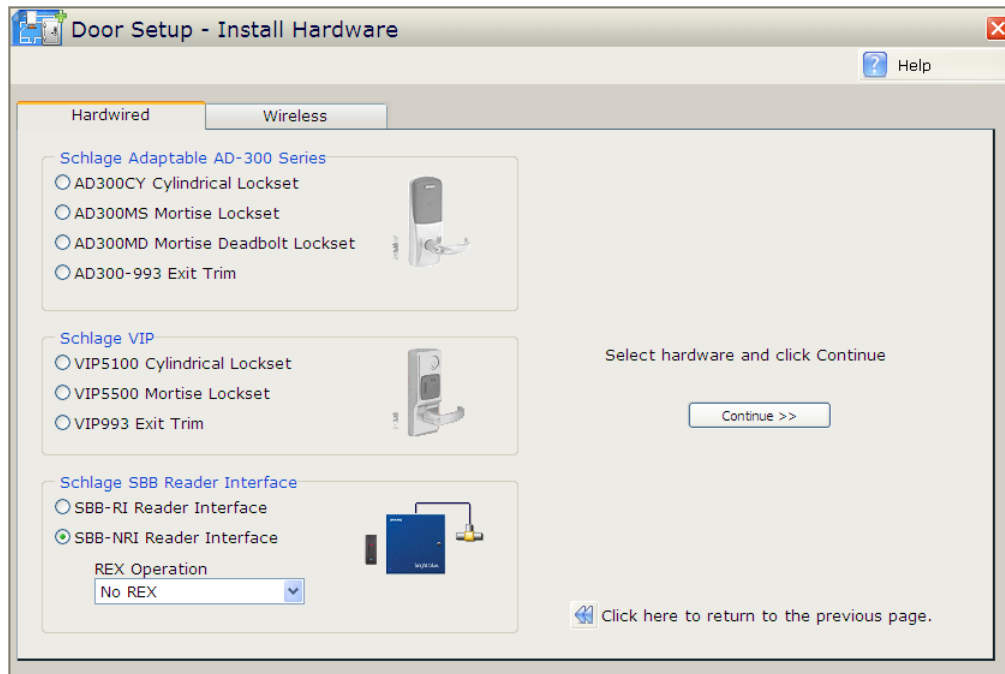
- 6 SBB-RIs will have a **RIType** of GRI. You can tell multiple readers apart by looking at the **Chn** (channel) and **Addr** (address) columns. The version number of the SBB-RI is shown in the **Rev** column.

Example: In the above image there are two SBB-RIs listed. The first is at channel 1 address 1 and the second is at channel 1 and address 2. The first has a Rev value of .02, meaning it is a version 2 SBB-RI. This will NOT accept a PIN-pad reader. The second has a Rev value of .11, meaning it is a version 11 SBB-RI. This WILL accept a PIN-pad reader.

- 7 Once you've determined the version number of your readers, you can close the browser or return to **bright blue**.

SBB-NRI

- 1 Open the **Door Setup** section by clicking on the Door Setup navigation button on the left side of the main screen.
- 2 Click the **Add doors hardware** button in the Installation and Configuration Tasks section. The **Door Setup - Install Hardware** window will open.



- 3 Click on the radio button to the left of SBB-NRI Reader Interface.
- 4 Select what type of REX this SBB-NRI will use from the REX Operation drop down box.

REX stands for request-to-exit and refers to either a mechanical button or PIR (motion sensor) that is used to gain egress from a secured door.

- **No REX** - No REX for this door. Request-to-exit is not in use. Door Forced Open is not reported.
- **REX - No Unlock** - Request-to-exit is in use to report a valid exit and bypass door contact reporting for a period of time. The REX device will not unlock the electrified locking device. This is typically used when either a door knob or exit bar are used as these devices manually unlatch from the inside of the opening.
- **REX - Unlock** - Request-to-exit is in use to report a valid exit, bypassing door contact reporting for a period of time AND unlocking the electrified locking device. This is typically used when a magnetic lock is used and must be unlocked from the inside of the door to allow exiting.

- 5 Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.



- 6 Click on **OK** if the selected lock is correct. The **Door Setup - Edit Door Security System** window will open.
- 7 Complete the **Door Name** and **Notes** fields.
- 8 Select the **Basic Settings** tab on the bottom half of the screen.

- 9 Define the following **Reader** options:
- Using the **Reader Type** drop down box, select the Reader Type:
Standard - Readers for any location not using anti-passback. =
Entry - Readers that are defined as entry readers for anti-passback purposes..
Exit - Readers that are defined as exit readers for anti-passback purposes.
 - Click the **PIN-pad** option to enable the PIN-pad for this Reader. The Schedules tab will be used to determine when a PIN is required in addition to a credential.

Note: Only revision 11 and above SBB-NRIs will accept a PIN. Earlier models do not have this functionality. To determine revision number, see the section above: Determining Version Number of SBB-NRI: the process is the same as listed there.

- 1 Select the REX setting. REX stands for Request-to- Exit and refers to either a mechanical button or motion sensor that is used to gain exit from a secured door. Using the **REX Operation** drop down box, define the REX operation for the door.
 - **No REX** - No REX for this door. Request-to-exit is not in use. Door Forced Open is not reported.
 - **REX - No Unlock** - Request-to-exit is in use to report a valid exit and bypass door contact reporting for a period of time. The REX device will not unlock the electrified locking device. This is typically used when either a door knob or exit bar are used as these devices manually unlatch from the inside of the opening.
 - **REX - Unlock** - Request-to-exit is in use to report a valid exit, bypassing door contact reporting for a period of time AND unlocking the electrified locking device. This is typically used when a magnetic lock is used and must be unlocked from the inside of the door to allow exiting.
- 2 Define the following **Timer** options:
 - a) Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.
 - b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.
- 3 Define the following **Special Access Timer** options:
 - a) Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.
 - b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.
- 4 Select the **Advanced Settings** tab in the bottom half of the screen.

The screenshot displays the 'Advanced Settings' tab of a configuration window. At the top, there are three tabs: 'Basic Settings', 'Advanced Settings' (which is selected), and 'Schedules'. Below the tabs, the 'Connection' section includes an icon of a plug, the label 'Connection:', and two input fields: 'IP Address or Hostname **' containing '192.168.169.249' and 'Port Number **' containing '30127'. To the right of these fields is an 'Installed' checkbox. Below this, the 'Event Reporting' section features an icon of a computer monitor, the label 'Event Reporting:', and two unchecked checkboxes: 'Enable "Lock/Unlock" relay state change reporting' and 'Enable "REX" state change reporting'. To the right, the 'Video Surveillance System Event Logging' section has an icon of a video camera, the label 'Video Surveillance System Event Logging:', a 'Camera' dropdown menu currently showing '<not enabled>', and a small circular icon with a camera symbol. At the bottom, the 'Enhanced Security' section includes an icon of a padlock, the label 'Enhanced Security:', and one unchecked checkbox: 'Disable door access during system start-up'.

- 5 Define the following options in the **Connection** section:
 - a) Set the IP Address: Go to the **IP Address or Hostname** field and specify the IP address of the SBB-NRI (see installation manual for details).

Note: If your SBB-NRI is set up with DNS in conjunction with DHCP the DNS name can be used here instead of the IP address.


- b) Confirm the Port Number. This should be 30127
- c) **Installed.** Click this box if this lock is currently installed on the system.
- 6 Define the following options in the **Event Reporting** section:
 - a) Check the **Enable "Lock/Unlock" relay state change reporting** box if you wish to generate reports and see activity based on when this lock is locked and unlocked.
 - b) Check the **Enable REX state change reporting** box if you wish to generate reports and see activity based on when the REX is activated.
- 7 Check the **Disable door access during system start-up** option if you wish to disable access to this door any time the system restarts.
- 8 If the **bright blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.
- 9 Select the **Schedule** tab in the bottom half of the screen.

The screenshot shows the 'Schedules' tab with three main sections:

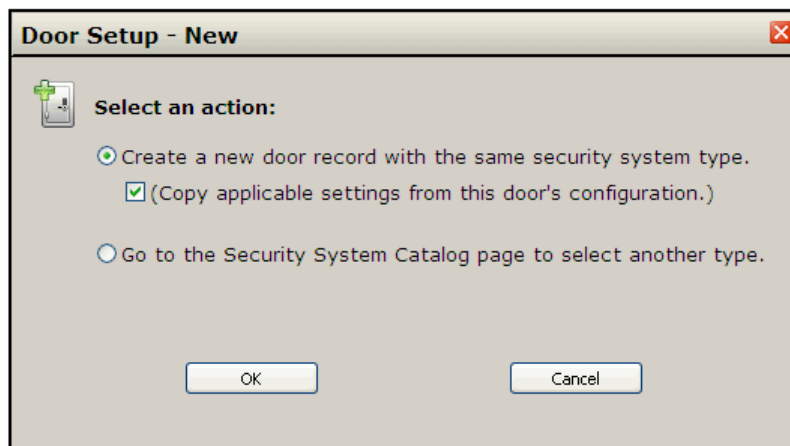
- Unlock Schedule:**
 - Unlock Time Zone: Never (dropdown menu)
 - ☐ Apply "1st Person In" rule
- PIN Required Schedule:**
 - PIN Required Time Zone: Never (dropdown menu)
- Toggle Cancel Time:**
 - ☐ Ensure this door is re-locked automatically at the following time/days, if toggled unlocked:
 - Time: 0 Hour, 00 Min.
 - Effective Days of the Week: ☐ Sun, ☐ Mon, ☐ Tue, ☐ Wed, ☐ Thu, ☐ Fri, ☐ Sat

- 10 Define the following options in the **Unlock Schedule** section:
 - a) Select the time zone for the door using the **Unlock Timezone** drop down box.
 - b) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. This feature is used to enable an override when the first valid access card is presented during a time zone. The override will re-lock according to original schedule.

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked if no one is in the building. In the Unlock Timezone drop down select the 7:00am to 5:00pm Time Zone. Then check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after someone has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.
- 11 If enabled, define the **PIN Required Schedule** section.
 - a) Select the time zone during which a pin will be required by using the **PIN Required Time Zone** drop down box.

Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- 12 Define the different options in the **Toggle Cancel Time** section:
 - a) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked** box to enable this feature. This will lock this door automatically at the specified time if the door was left in a toggle-open state.
 - b) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.
 - c) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.
- 13 Click the **Save Door** button at the top of the screen. The screen will refresh and the door will be saved.
- 14 To add additional doors, click the **New Door** button at the top of the screen. **The Door Setup - New** pop-up window will open.



- 15 Select from the following options:
 - **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat steps 6 through 22 above.
 - **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat steps 22 and 23 above.
 - **Go to the Security System Catalog page to select another type.** Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Electronic Security System Hardware** window will open. Follow the steps for the lock type selected.

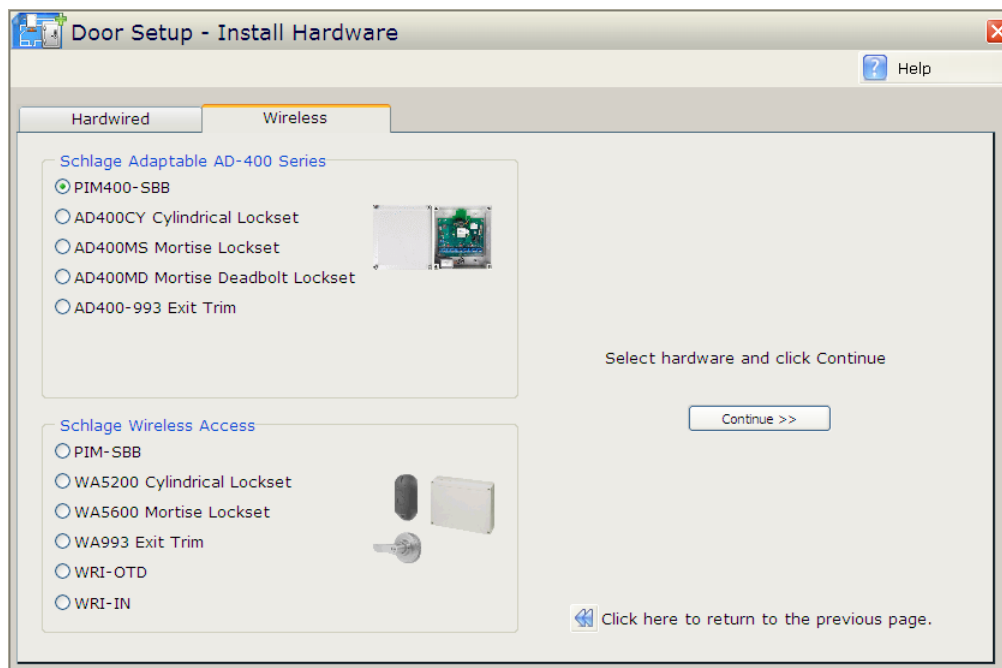
Schlage Adaptable AD-400 Series

There are two hardware components to a Schlage Adaptable AD-400 Series lock; the PIM400-SBB (Panel Interface Module) and the lock. The PIM is connected to the **bright blue** controller and the lock (or locks) communicate with the PIM. A PIM must be connected before any wireless locks can be defined. Below are instructions on setting up a PIM and then a wireless lock.

Note: Before setting up a PIM400-SBB it is necessary to configure the PIM using the SUS (Schlage Utility Software). The SUS is a separate program that can be accessed via the PDA. Please see the installation manual for details.

PIM400-SBB

- 1 Open the **Door Setup** section by clicking on the Door Setup navigation button on the left side of the main screen.
- 2 Click the **Add doors and hardware** button in the Installation and Configuration Tasks section. The Door Setup - Install Hardware window will open.
- 3 Click on the **Wireless** tab.

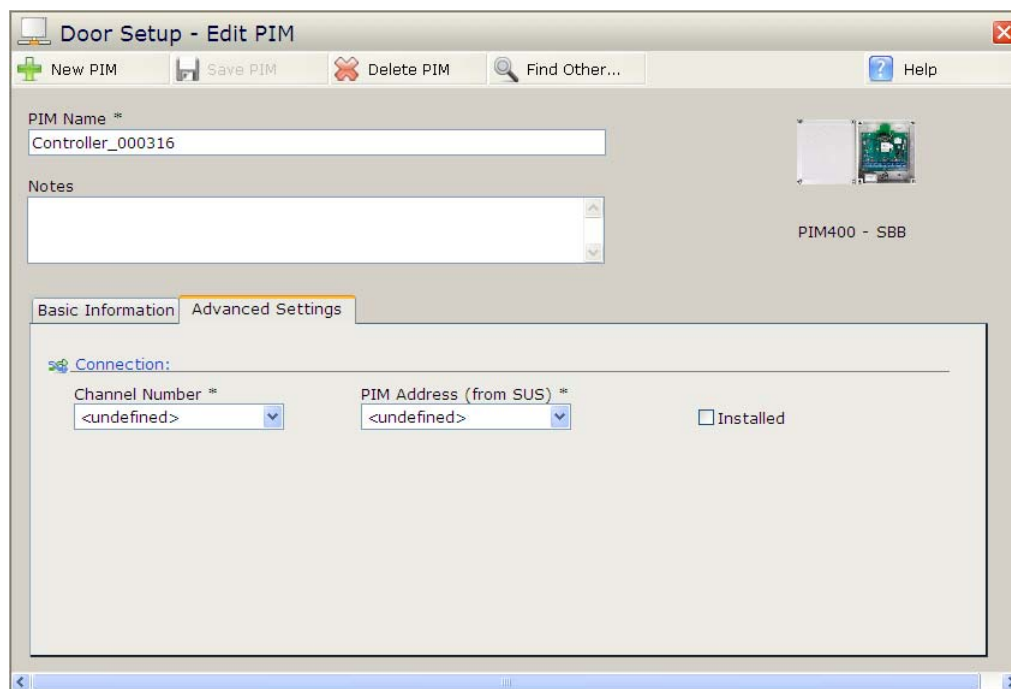


- 4 Click on the radio button to the left of PIM400-SBB.

- 5 Click on the **Continue** button. The **Installation** pop-up window will open asking you to Confirm PIM Record Creation.



- 6 Click **OK** to set up a PIM. The **Door Setup - Edit Door PIM** window will open.



- 7 Complete the **PIM Name** and **Notes** fields.

- 8 Select the **Advanced Settings** tab in the bottom half of the screen.

- 9 Define the following options in the **Advanced Settings** tab:
- Select the **Channel Number**. This specifies the channel on the controller that the device is wired to.
 - Set the **PIM Address (from SUS)**. This field must match the address that is specified by the SUS. Please see the PIM400-SBB section of the installation guide for more details.
 - Installed**. Click this box if this PIM is currently installed on the system.
- 10 Click the **Save PIM** button at the top of the screen. The screen will refresh and the PIM will be saved.

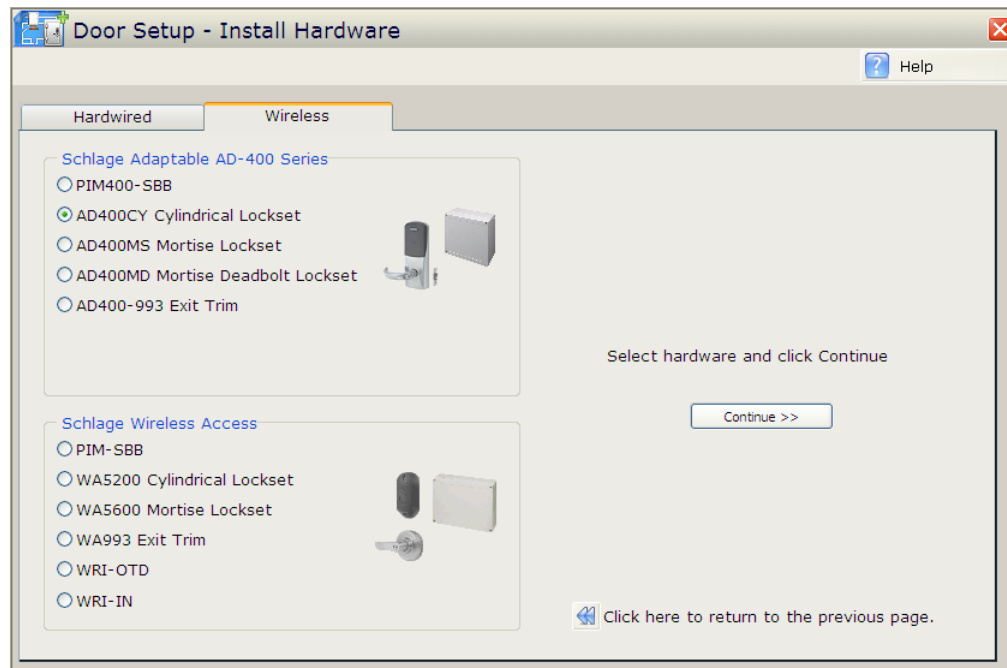
To add additional PIM400s click the **New PIM** button at the top of the screen and repeat steps 3 through 10.

AD-400 Series

Note: If using a Schlage Adaptable AD-400 Series lock(s), a PIM400-SBB must be programmed before continuing. Please see the PIM400-SBB section above for more details.

- Open the **Door Setup** section by clicking on the Door Setup navigation button on the left.
- Click the **Add doors hardware** button in the Installation Tasks section. The **Door Setup - Install Hardware** window will open.

- 3 Click on the **Wireless** tab.



- 4 Click on the radio button to the left of the type of AD-400 lock to be set up.
- 5 Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.



- 6 Click **Ok** to confirm the correct lock. The **Door Setup - Edit Door Security System** window will open.

- 7 Complete the **Door Name** and **Notes** fields.
- 8 Select the **Basic Settings** tab in the bottom half of the screen. This section is broken up into three areas: Reader Type, Timers and Special Access Timers. The REX function is disabled as it is not used with this lock type.

- 9 Define the following **Reader** options:
- Using the **Reader Type** drop down box, select the Reader Type:
Standard - Readers for any location not using anti-passback.

Entry - Readers that are defined as entry readers for anti-passback purposes.

Exit - Readers that are defined as exit readers for anti-passback purposes.

- b) Click the **PIN-pad** option to enable the PIN-pad for this Reader. The Schedules tab will be used to determine when a PIN is required in addition to a credential.

10 Define the following **Timer** options:

- a) Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.
- b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.

11 Define following **Special Access Timer** options:

- a) Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.
- b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

12 Select the **Advanced** tab in the bottom half of the screen. This section is broken up into two areas: Connection and Event Reporting

13 Define the following options in the **Connection** section:

- a) Select the PIM that the lock is connected to from the **PIM** drop down box.
- b) Set the **WAPM Door # (from SUS)**. This field must match the number that is specified by the SUS. Please see the PIM400-SBB section of the installation guide for more details.
- c) **Installed**. Click this box if this lock is currently installed on the system.


14 Define the following options in the **Event Reporting** section:

- a) Check the **Enable "Clutch Position" relay state change reporting** box for the ability to generate reports and see activity based on when this lock is locked and unlocked.
- b) Check the **Enable "REX" state change reporting** box for the ability to generate reports and see activity based on when this REX is activated.
- c) Check the **Enable "Request-To-Enter" state change reporting** box for the ability to generate reports and see activity based on when this Request-To-Enter is activated.

- 15 Check the **Disable door access during system start-up** option if you wish to disable access to this door any time the system restarts.
- 16 If the **bright blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.
- 17 Select the **Schedule** tab in the bottom half of the screen.

- 18 Define the following options in the **Unlock Schedule** section:

- a) Select the time zone for the door using the **Unlock Timezone** drop down box.


Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- b) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. This feature is used to enable an override when the first valid access card is presented during a time zone. The override will re-lock according to original schedule.

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked if no one is in the building. In the Unlock Timezone drop down select the 7:00am to 5:00pm Time Zone. Then check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after someone has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

- 19 If enabled, define the **PIN Required Schedule** section.

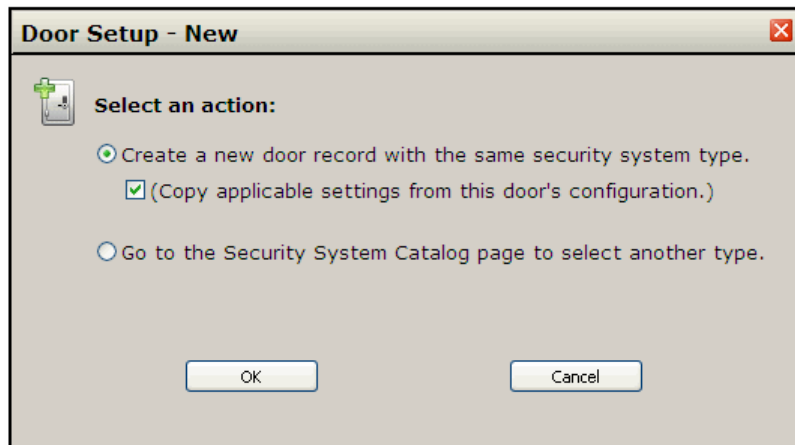
- a) Select the time zone during which a pin will be required by using the **PIN Required Time Zone** drop down box.

Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- 20 Define the following options in the **Toggle Cancel Time** section:

- a) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked:** box to enable this feature. This will lock this door automatically at the specified time.

- b) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.
 - c) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.
- 21 Click the **Save Door** button at the top of the screen. The screen will refresh and the door will be saved.
- 22 To add additional locks, click the **New Door** button at the top of the screen. The Door Setup - New pop-up window will open.



- 23 Select from the following options:
- **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat steps 6 through 22 above.
 - **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat steps 21 and 22 above.

Go to the Security System Catalog page to select another type. Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Hardware** window will open. Follow the steps for the lock type selected.

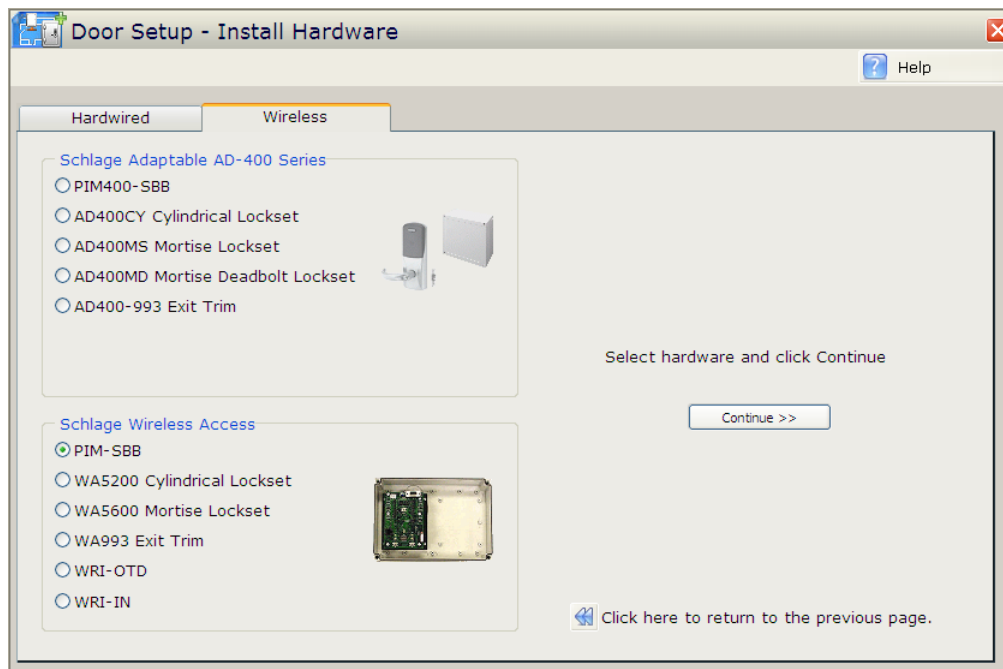
Schlage Wireless Access

There are two hardware components to a Schlage Wireless Access lock; the PIM-SBB (Panel Interface Module) and the lock. The PIM is connected to the **bright blue** controller and the lock (or locks) communicate with the PIM. A PIM must be connected before any wireless locks can be defined. Below are instructions on setting up a PIM and then a wireless lock.

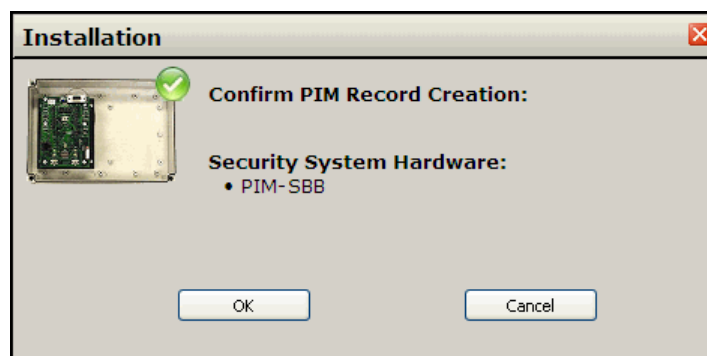
Note: Before setting up a PIM it is necessary to configure the PIM using the CDT (Configuration and Demonstration Tool). The CDT is a separate program that can be downloaded from www.ir-swa.com. Please see the installation manual for details.

PIM-SBB

- 1 Open the **Door Setup** section by clicking on the Door Setup navigation button on the left side of the main screen.
- 2 Click the **Add doors and hardware** button in the Installation and Configuration Tasks section. The Door Setup - Install Hardware window will open.
- 3 Click on the **Wireless** tab.



- 4 Click on the radio button to the left of PIM-SBB.
- 5 Click on the **Continue** button. The **Installation** pop-up window will open asking you to Confirm PIM Record Creation.



- 6 Click **OK** to set up a PIM. The **Door Setup - Edit Door PIM** window will open.

- 7 Complete the **PIM Name** and **Notes** fields.
- 8 Select the **Advanced Settings** tab in the bottom half of the screen.

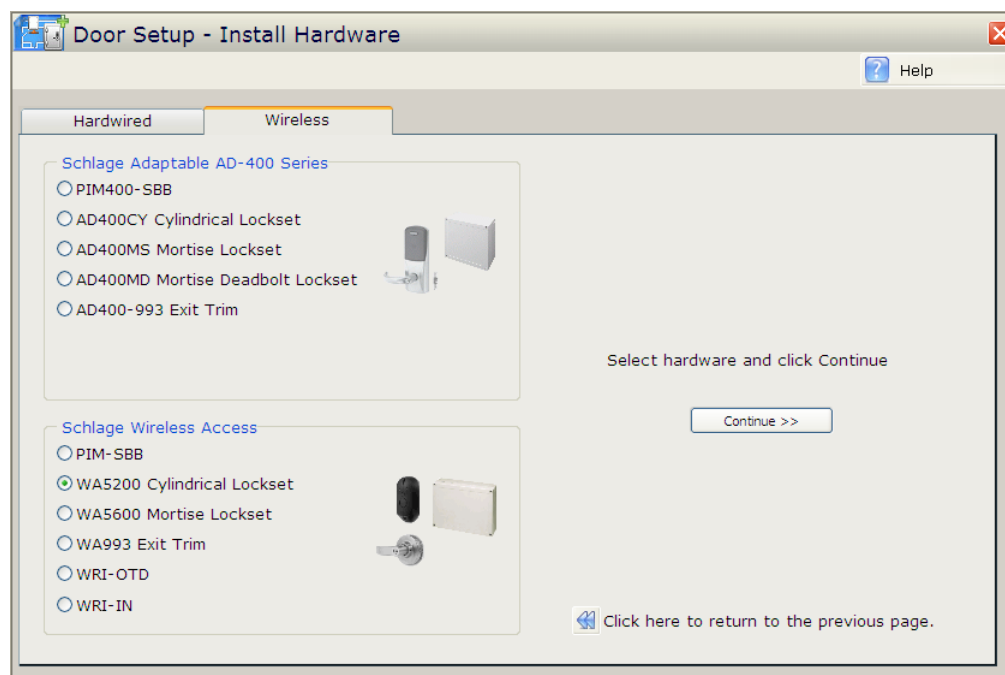
- 9 Define the following options in the **Advanced Settings** tab:
- Select the **Channel Number**. This specifies the channel on the controller that the device is wired to.
 - Set the **PIM Address (from CDT)**. This field must match the address that is specified by the CDT. Please see the PIM section of the installation guide for more details.
 - Installed**. Click this box if this PIM is currently installed on the system.
- 10 Click the **Save PIM** button at the top of the screen. The screen will refresh and the PIM will be saved.

To add additional PIMs click the **New PIM** button at the top of the screen and repeat steps 3 through 10.

WA Series

Note: If using a Schlage Wireless Access lock(s), a PIM-SBB must be programmed before continuing. Please see the PIM-SBB section above for more details.

- 1 Open the **Door Setup** section by clicking on the Door Setup navigation button on the left.
- 2 Click the **Add doors hardware** button in the Installation Tasks section. The **Door Setup - Install Hardware** window will open.
- 3 Click on the **Wireless** tab.



- 4 Click on the button to select the type of Wireless lock to set up.
- 5 Click on the **Continue** button. The **Installation** pop-up window will open asking to Confirm Door Record Creation.



- 6 Click **Ok** to confirm the correct lock. The **Door Setup - Edit Door Security System** window will open.
- 7 Complete the **Door Name** and **Notes** fields.
- 8 Select the **Basic Settings** tab in the bottom half of the screen. This section is broken up into three areas: Reader Type, Timers and Special Access Timers. The REX function is disabled as it is not used with this lock type.

The screenshot shows the 'Basic Settings' tab of the 'Door Setup - Edit Door Security System' window. The window has three tabs: 'Basic Settings', 'Advanced Settings', and 'Schedules'. The 'Basic Settings' tab is active. It contains three sections: 'Reader:', 'Timers:', and 'Special Access Timers:'. The 'Reader:' section has a 'Reader Type' dropdown set to 'Standard Reader', a 'PIN-pad' checkbox labeled 'No', and a 'REX Operation' dropdown set to 'N/A'. The 'Timers:' section has an 'Unlock Time' dropdown set to '3 seconds' and a 'Door Held Open Detect Time' dropdown set to '30 seconds'. The 'Special Access Timers:' section has an 'Unlock Time' dropdown set to '6 seconds' and a 'Door Held Open Detect Time' dropdown set to '60 seconds'.

- 9 Define the following **Reader** options:
 - a) Using the **Reader Type** drop down box, select the Reader Type:
 - Standard** - Readers for any location not using anti-passback.
 - Entry** - Readers that are defined as entry readers for anti-passback purposes.
 - Exit** - Readers that are defined as exit readers for anti-passback purposes.
 - b) The **PIN-pad** option will be disabled. WA Series locks do not support a PIN reader.
- 10 Define the following **Timer** options:
 - a) Using the **Unlock Time** drop down box, define the number of seconds the door will be unlocked before the lock re-engages.
 - b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open before the system is alerted.
- 11 Define following **Special Access Timer** options:
 - a) Using the **Unlock Time** drop down box, define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.
 - b) Using the **Door Held Open Detect Time** drop down box, define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

- 12 Select the **Advanced** tab in the bottom half of the screen. This section is broken up into two areas: Connection and Event Reporting


The screenshot shows the 'Advanced Settings' window with three tabs: 'Basic Settings', 'Advanced Settings' (selected), and 'Schedules'. The 'Connection' section contains a 'PIM *' dropdown menu with '< Select PIM >', a 'WAPM Door # (from CDT) *' dropdown menu with '<undefined>', and an 'Installed' checkbox. The 'Event Reporting' section has three checkboxes: 'Enable "Lock/Unlock" relay state change reporting' (unchecked), 'Enable "REX" state change reporting' (unchecked), and 'Enable "Request-To-Enter" state change reporting' (checked). The 'Enhanced Security' section has a checkbox 'Disable door access during system start-up' (unchecked). The 'Video Surveillance System Event Logging' section has a 'Camera' dropdown menu with '<not enabled>' and a refresh icon.

- 13 Define the following options in the **Connection** section:
- Select the PIM that the lock is connected to from the **PIM** drop down box.
 - Set the **WAPM Door # (from CDT)**. This field must match the number that is specified by the CDT. Please see the PIM section of the installation guide for more details.
 - Installed**. Click this box if this lock is currently installed on the system.
- 14 Define the following options in the **Event Reporting** section:
- Check the **Enable "Lock/Unlock" relay state change reporting** box for the ability to generate reports and see activity based on when this lock is locked and unlocked.
 - Check the **Enable "REX" state change reporting** box for the ability to generate reports and see activity based on when this REX is activated.
 - Check the **Enable "Request-To-Enter" state change reporting** box for the ability to generate reports and see activity based on when this Request-To-Enter is activated.
- 15 Check the **Disable door access during system start-up** option if you wish to disable access to this door any time the system restarts.
- 16 If the **bright blue** system has been integrated with a video server then use the **Video Surveillance System Event Logging** section to select which camera will be linked to this door's events. This section will be disabled if there is no connection to a video server.

- 17 Select the **Schedule** tab in the bottom half of the screen.

- 18 Define the following options in the **Unlock Schedule** section:

- a) Select the time zone for the door using the **Unlock Timezone** drop down box.

Note: If you are unsure of a timezone's range, roll over the information button  with the mouse. An information window will open showing the schedule of the selected time zone.

- b) Check the **Apply 1st Person In Rule** box to enable the 1st Person In Rule. This feature is used to enable an override when the first valid access card is presented during a time zone. The override will re-lock according to original schedule.

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked if no one is in the building. In the Unlock Timezone drop down select the 7:00am to 5:00pm Time Zone. Then check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after someone has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

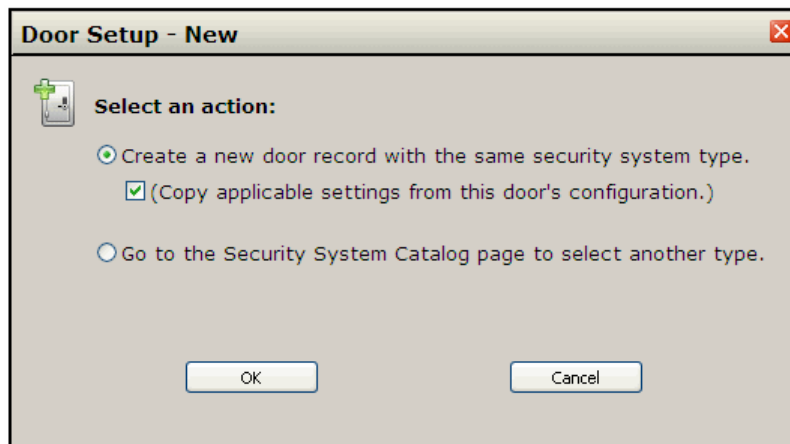
- 19 The **PIN Required Schedule** section will be disabled. This is not an option with WA Series locks.

- 20 Define the following options in the **Toggle Cancel Time** section:

- a) Check the **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked:** box to enable this feature. This will lock this door automatically at the specified time.
- b) Use the **Time: Hour** and **Min.** drop down boxes to specify when the door will automatically lock.
- c) Check the boxes under **Effective Days of the Week:** to specify which days of the week the door will automatically lock.

- 21 Click the **Save Door** button at the top of the screen. The screen will refresh and the door will be saved.

- 22 To add additional locks, click the **New Door** button at the top of the screen. The Door Setup - New pop-up window will open.



- 23 Select from the following options:
- **Create a new door record with the same security system type.** Select this to set up the same type of lock and click **OK**. The pop-up will close and the **Door Setup - Edit Door Security System** window will reopen. Repeat steps 6 through 21 above.
 - **Copy applicable settings from this door's configuration.** Select this along with **Create a new door record with the same security system type**, to set up a new lock with the same settings specified for the previous lock and click **OK**. The pop-up will close and a new **Door Setup - Edit Door Security System** window will open. This lock will have all the same settings as the previous lock. Re-name the lock and complete any **Notes** (if desired). Repeat steps 21 and 22 above.
 - **Go to the Security System Catalog page to select another type.** Select this if you wish to set up a door type different from the previous door type. The pop-up window will close and the **Door Setup - Install Hardware** window will open. Follow the steps for the lock type selected.

Personnel Setup

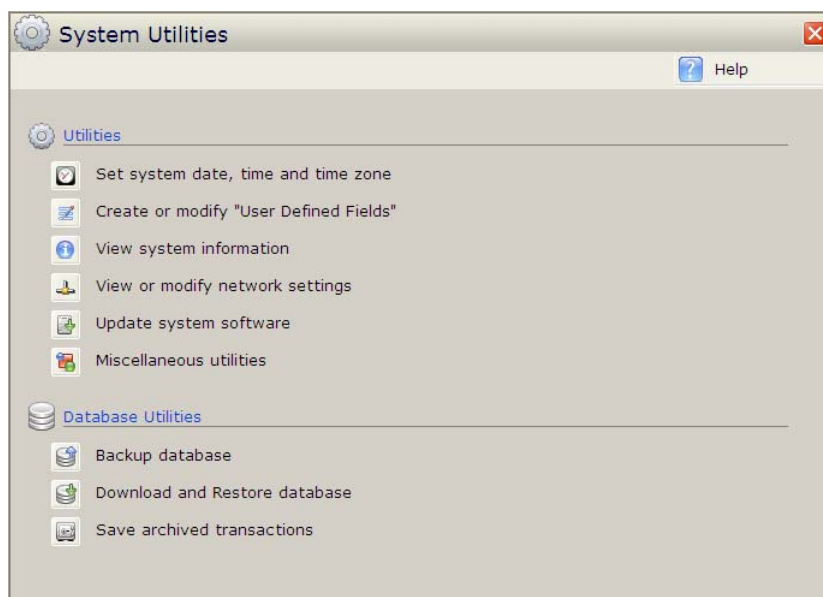
Once the doors have been defined and installed, the next step is to add personnel. The Personnel Management screen allows you to enter new personnel, assign credential information, assign access and view access history. This section will cover setting up User Defined Fields and adding Personnel to your system. For access assignments, see the Adding Access Assignment section.

User Defined Fields

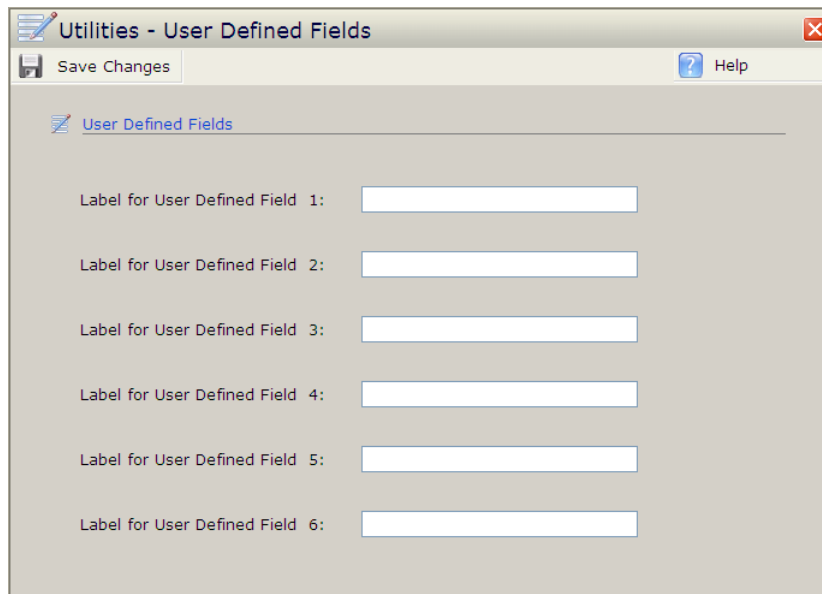
Prior to adding personnel, determine the type of personal information, besides name, that will be included for each person. This system allows up to six User Defined Fields. (i.e. birth date, e-mail address phone number, etc.) Follow the instructions below to create User Defined Fields.

Note: These fields are not required, they are used for additional information that will be visible in the system on both the Personnel page and the Personnel Report. All, any, or none of the fields may be filled out. You may skip this step if you do not wish to include additional cardholder data in User Defined Fields.

- 1 Click on the **Utilities** navigation button on the left side of the main screen. The **System Utilities** window will open.



- 2 Click on the **Create or modify User Defined Fields** button. The **Utilities - User Defined Fields** window will open.



- 3 Fill in **Label for User Defined Field 1:** with the desired information. Maximum length is 64 characters. Example: Date of Birth
- 4 Continue to complete the information for each User Defined Field (up to 6).
- 5 Click the **Save** button. The system will take a moment to update the field(s). When complete, a pop-up window will open describing the fields that have been updated.
- 6 Click **OK** in the pop-up window. It will close. You can now continue to the next step in setting up Personnel.

Adding Personnel

- 1 Select the **Personnel** navigation button to the left side of the main screen. The **Personnel Management - Tasks** window will open.

- 2 Click the **Add new person**, the **Personnel Management** window will open. If personnel have previously been entered, this window will display the first person in the system alphabetically. If there are no personnel set-up in the system, the fields will be blank.

- 3 Click on the **New Person** button at the top of the screen. The Personnel Management window will open.
- 4 Fill in person's last name in the **Last Name** field. This is required.
- 5 Fill in the person's first name and middle name/initial if desired in the **First Name** and **Middle Name/Initial** fields.
- 6 Select the person's activation date by filling in the **Activation Date** field. This is the date at which a person's access assignments will be activated. The default is the current date.
 - a) Click the **Calendar** button located to the right of the date field. This opens a calendar pop-up window.

- b) Select the desired date from this window using the arrow buttons or the drop down menus.
- 7 Select the person's expiration date by filling in the **Expiration Date** field. This is the date at which a person's access assignments will be deactivated. The default is 2199-12-31.
 - a) Click the **Calendar** button located to the right of the date field. This opens a calendar pop-up window.
 - b) Select the desired date from this window using the arrow buttons or the drop down menus.
- 8 Check the **Special Access Privileges** check box if this person is to have special access. This means the doors will remain unlocked for longer than if they had normal access. This is an optional field.

- 9 Leave the **Controlled Antipassback** box checked if this person is to have the antipassback feature activated. If you want this person to be able to override the antipassback feature (Security Personnel for example) un-check this box.

Anti-passback prevents a card from being passed back to another person for the purpose of gaining unauthorized access. To attain this level of security, a separate reader is required at each entrance and exit.

- 10 Select the **Personal Info** tab on the bottom half of the screen. This tab is open by default.

The screenshot shows the 'Personal Info' tab selected. It contains six text input fields arranged in a 2x3 grid, labeled 'User Defined Field Number 1' through 'User Defined Field Number 6'. Below these fields is a larger text area labeled 'Notes' with a scroll bar.

- 11 Complete the fields in the Personal Info tab. These are User Defined Fields. Please see the User Defined Fields section of the manual for more details.

- 12 Select the **Credentials** tab on the bottom half of the screen.

Note: Credential information can be completed at a later time if desired.

The screenshot shows the 'Credentials' tab selected. It features a 'Card' section with three input fields: 'Stamped ID', 'Encoded ID' (which has a red border and the text 'Encoded ID NOT entered'), and 'Issue Code' (a dropdown menu showing '0'). There is also a 'Remove...' button to the right of the 'Issue Code' dropdown.

- 13 Fill in the **Stamped ID** field with the stamped ID of the credential to be used by this person. This field is not required. See the Credentials section of the Personnel chapter for more information.
- 14 Fill in the **Encoded ID** field with the encoded ID of the credential to be used by this person. This field is required. See the Credentials section of the Personnel chapter for more information.
- 15 Select the issue code by using the **Issue Code** drop down box.

Issue codes are an optional function that allow for increased security in the case of lost credentials. If using Issue Codes, the original credential assigned to a person will have an issue code of 1. If that credential is lost, a new credential can be assigned to the person with the same encoding as the original, but the issue code will be increased. If anyone tries to use the older card it will no longer function as its issue code will be different. This is normally only used for Magstripe Credentials

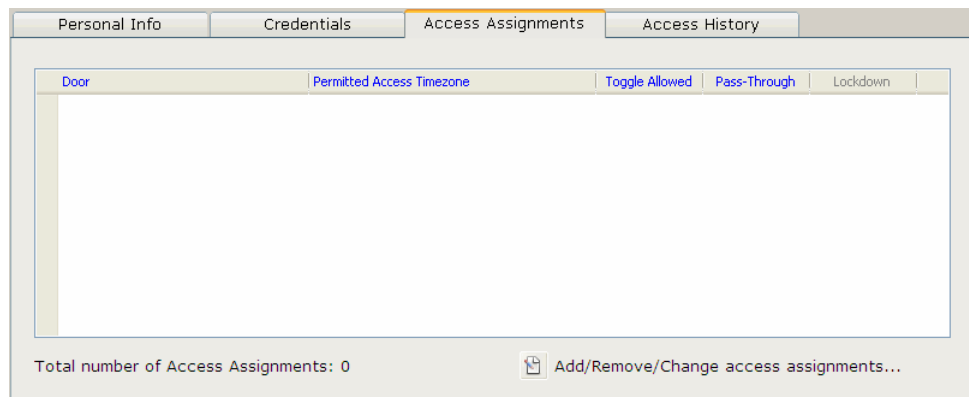
The default is 0.

16 Click the **Save Person** button at the top of the screen.

17 **OPTIONAL:** At this point access assignments can be defined for this person. If there are a small number of personnel in the system you may want to do this now. However, you may find it easier to enter all personnel and then add access assignments by group, or by copying one person's access assignments to others. See the **Adding Access Assignment** section below for details.

To add access assignments now:

a) Select the **Access Assignments** tab in the bottom half of the screen.



b) Click on the **Add/Remove/Change access assignments** button. The **Access Assignment Edit** window will open.

c) Follow steps 5 through 13 in the Access by Person section below.

18 Click on the **Personnel** navigation button on the left to get back to the Personnel Management window.

19 Repeat steps 3 through 16 above for each person who will have access to the doors.

Adding Access Assignments to Existing Personnel

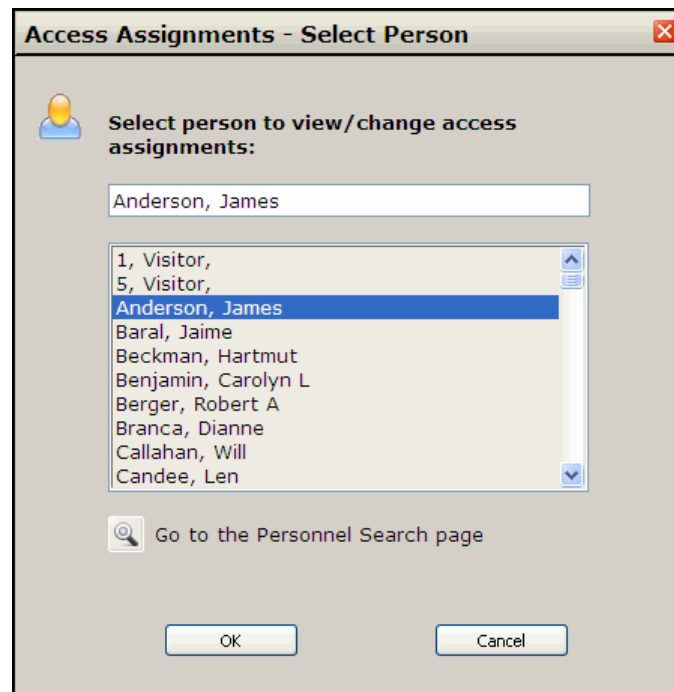
There are three different methods of assigning access: including (1) By Person, (2) By Group or (3) By copying access assignments from one person to others. All methods are covered below.

Access by Person

To add access assignments on a person-by-person basis:

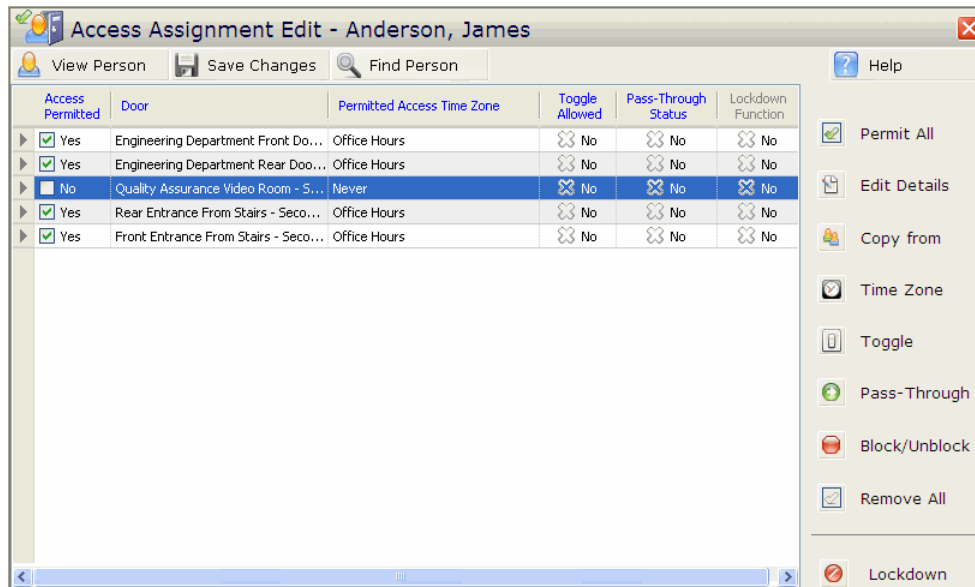
1 Click on the **Access Assignments** navigation button on the left side of the main screen. The **Access Assignments - Tasks** window will open.

- 2 Click on the **View or change a person's access assignments** button. The **Access Assignments - Select Person** - **Select Person** pop-up window will open.

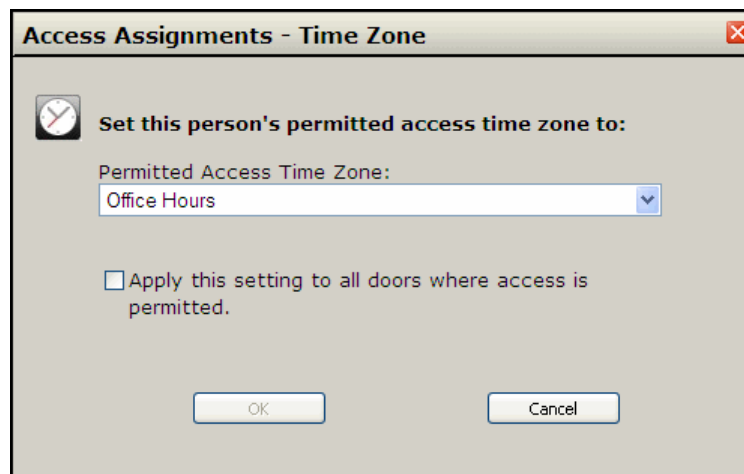


- 3 Click on the person you wish to grant access to from the list. This will highlight the person's name.
 - **OPTIONAL:** Click on the **Go to the Personnel Search page** button to open the **Personnel Search** window. From here you can search for a specific person in the system. Please see the **Searching for a Specific Record** section of the **Personnel** chapter for details.

- 4 Click the **OK** button. The pop-up will close and the **Access Assignment Edit** window will open with the selected person's name at the top.

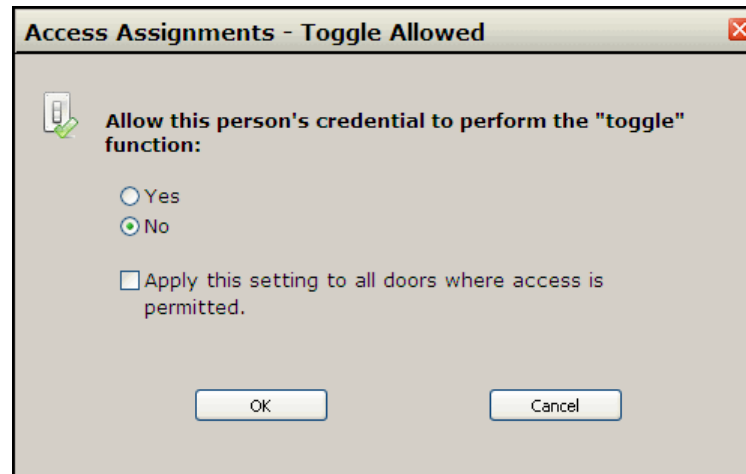


- 5 Click on the **Access Permitted** check box for each of the doors that this person will have access to. This will place a check in the box and change **No** to **Yes**.
- 6 Click on the **Time Zone** button on the right of the screen. This will open the **Access Assignments - Timezone** pop-up window.

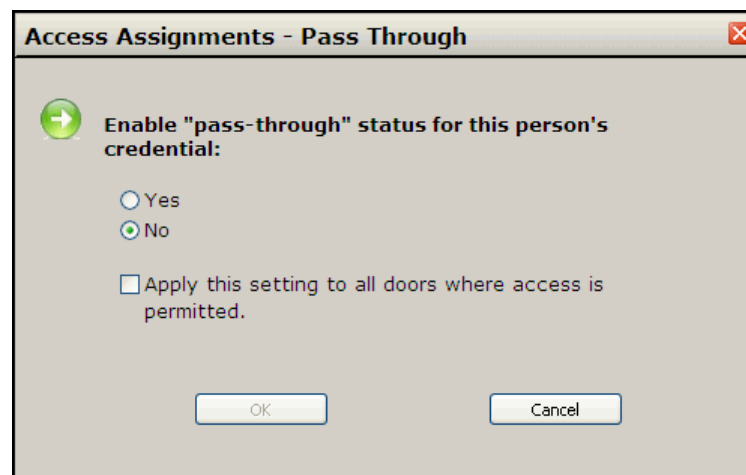


- 7 Using the **Permitted Access Time Zone** drop down menu, select the Time Zone during which this person will have access to these doors.
- 8 Click **OK**. This will close the pop-up window. All the selected doors will now have time zones assigned to them.
- 9 **OPTIONAL** - If this person is to be assigned Toggle rights, then click on the **Toggle** button on the right of the screen. This will open the **Access Assignments - Toggle Allowed** pop-up window.

The Toggle feature allows users to put a door into a continuous unlock state by presenting a valid toggle credential at a reader twice within 3 seconds. The door will remain unlocked until 1) it is toggled again 2) a Resume Normal Operation command is sent from the Door Status & Control screen or 3) a Toggle Cancel time is reached.

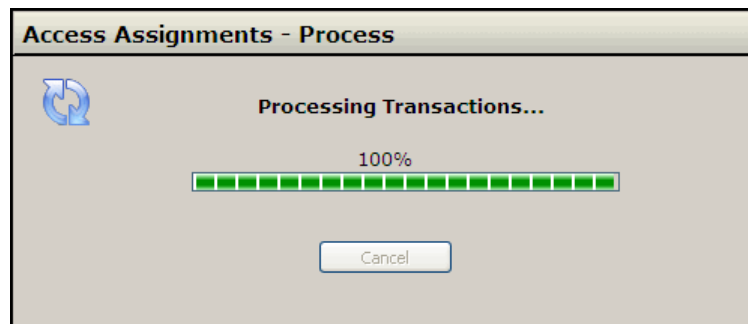


- a) Click on the **Toggled Allowed** check box to enable this feature. The label **(No)** will change to **(Yes)**.
 - b) Click **OK**. This will close the Toggle Allowed pop-up window and enable the Toggle ability for all doors assigned to this person.
- 10 **OPTIONAL** - If this person is to be assigned Pass-Through rights, then click on the Pass-Through button on the right of the screen. This will open the **Access Assignments - Pass Through** pop-up window.
- Pass-Through is a feature that allows a user to gain access at a door even if it is in a Lockdown state.



- a) Click on the **Pass-Through** check box to enable this feature. The label **(No)** will change to **(Yes)**.
 - b) Click **OK**. This will close the Pass-Through pop-up window and enable the Pass-Through ability for all doors assigned to this person.
- 11 Click the **Save Changes** button at the top of the screen. The **Save Changes** pop-up window will open.

- 12 Click **OK**. The **Access Assignments - Process** pop-up window will open. This window shows the progress of the saved changes. It will close when saving is complete.



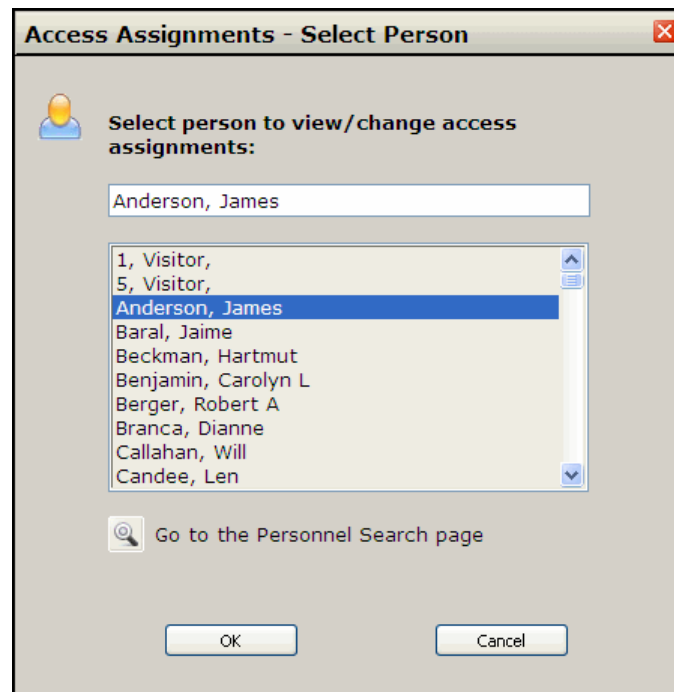
- 13 Repeat steps 1 through 12 for each person who will have access to the system.

Copying Access Assignments

To simplify the process of adding Personnel to the system it is possible to copy one person's access assignments to one or more people.

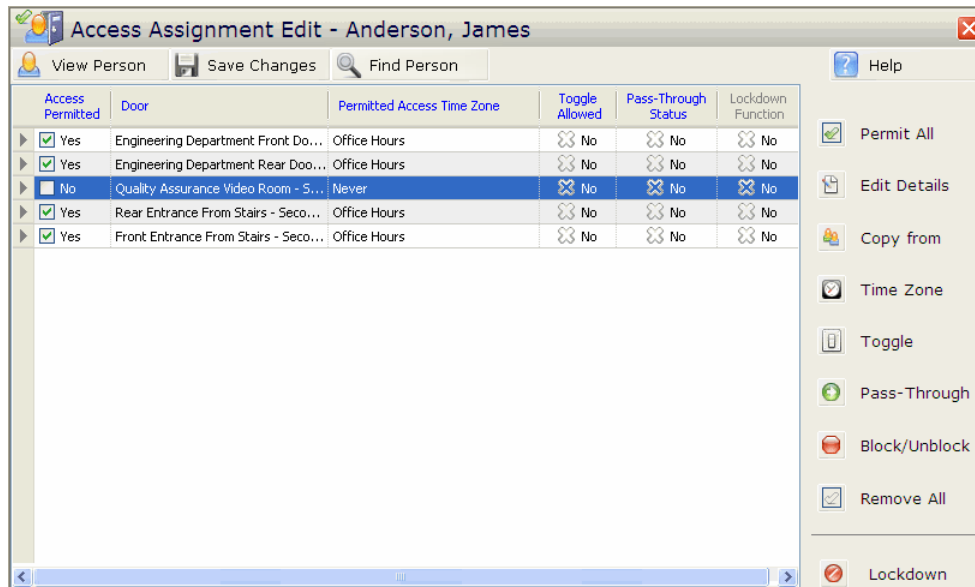
- 1 Decide which personnel record will be used as the access assignment template. The access assignment for this person should be already set up. Make note of that person's name.
- 2 All Personnel that will copy this access assignment template should already be entered into the system. If you need to enter additional Personnel, please see the Personnel Setup section.
- 3 Click on the **Access Assignments** navigation button on the left side of the main screen. This will open the **Access Assignments - Tasks** window.

- 4 Click on the **View or change a person's access assignments** button. The **Access Assignments - Select Person** - **Select Person** pop-up window will open.

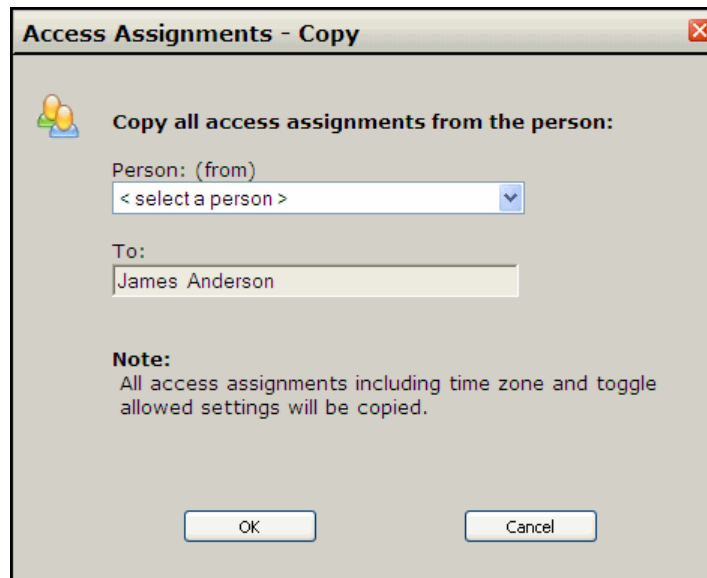


- 5 Select the person from the list of Personnel.
 - **OPTIONAL:** Click on the **Go to the Personnel Search page** button to open the **Personnel Search** window. From here you can search for a specific person in the system. Please see the **Searching for a Specific Record** section of the **Personnel** chapter for details.

- 6 Click **OK**. The pop-up window will close and the **Access Assignment Edit** window will open with the selected person's name at the top.



- 7 Click the **Copy from** button on the right side of the screen. The Access Assignments - Copy pop-up window will open.



- 8 Using the **Person: (from)** drop down box, select the person who's access assignment template will be copied. The **To:** field will already be populated with the name of the person receiving access.
- **OPTIONAL:** Click on the **Go to the Personnel Search page** button to open the **Personnel Search** window. From here you can search for a specific person in the system. Please see the **Searching for a Specific Record** section of the **Personnel** chapter for more details.
- 9 Click **OK**. The pop-up window will close and the access assignment will be copied.
- 10 Repeat steps 3 through 9 above for each person that will receive this access assignment template.

Access by Group

To add identical access rights to a group of people:

- 1 Click on the **Access Assignments** navigation button on the left of the main page. The **Access Assignments - Tasks** window will open.
- 2 Click on the **Create common access assignments for a group of people** button. The **Personnel Search - Group Access Assignments** window will open.

Personnel Search - Group Access Assignments

Execute Search Continue... Help

Find all person records by... Last Name

With the following search term...

With the following rule... Starts with

Range

More Search Terms...

Search Results

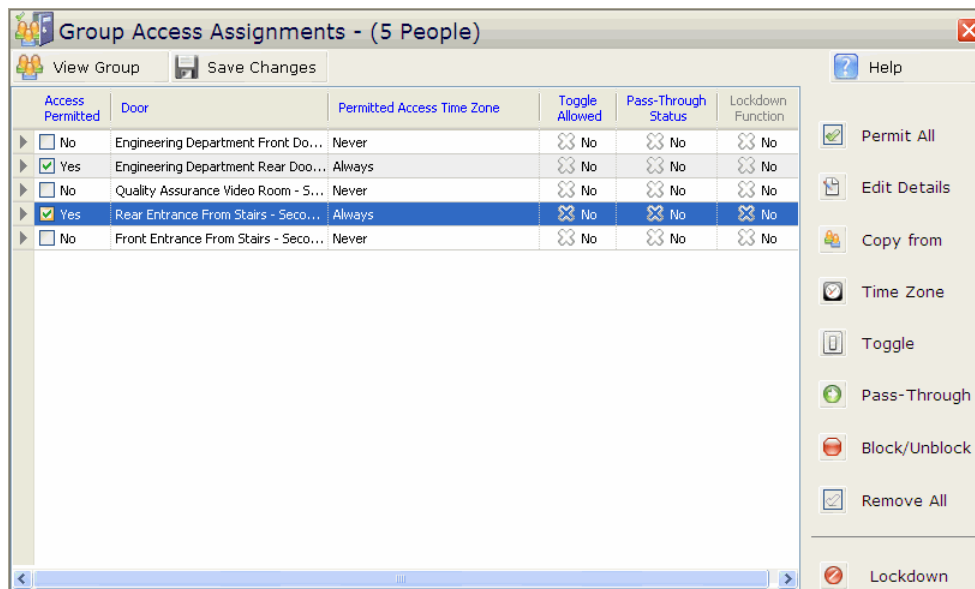
Select	Last Name	First Name	Middle Name	Activation Date	Expiration Date	Access Blocked	Controlled Antipassback	Special Access Privileges
--------	-----------	------------	-------------	-----------------	-----------------	----------------	-------------------------	---------------------------

- 3 Click the **Execute Search** button at the top of the screen. A list of all Personnel in the system will be generated.

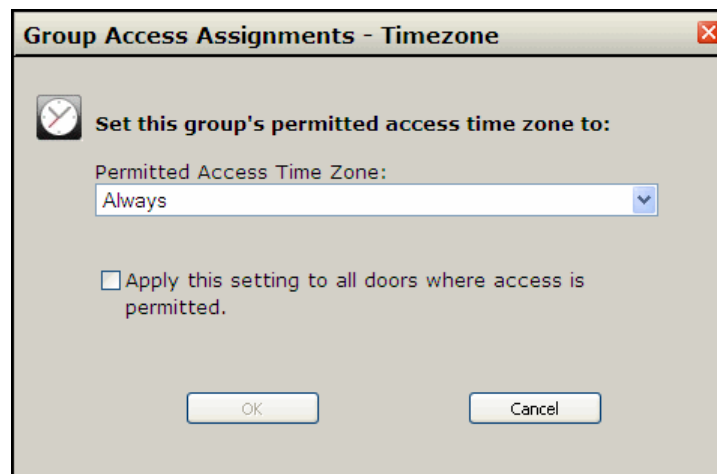
Note: Instead of generating a list of all personnel, a specific list can be created by using the search functions in the Personnel Search window. Please see the Searching for a Specific Record section of the Personnel chapter below for details on how to run a search.

- 4 Click on the **Select** check box for each of the people to be added to this group. This will place a check in the box and change **No** to **Yes**.

- 5 Click the **Continue** button at the top of the screen. The **Group Access Assignments Window** will open.

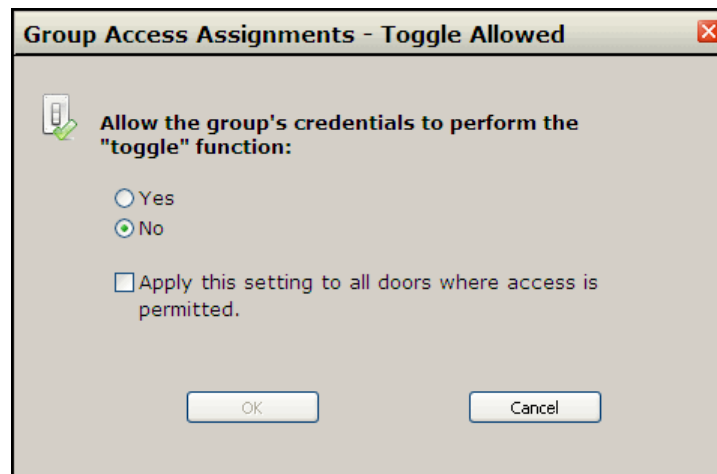


- 6 Click on the **Access Permitted** check box for each of the doors that this group will have access to. This will place a check in the box and change **No** to **Yes**.
- 7 Click on the **Time Zone** button on the right of the screen. This will open the **Group Access Assignments - Timezone** pop-up window.

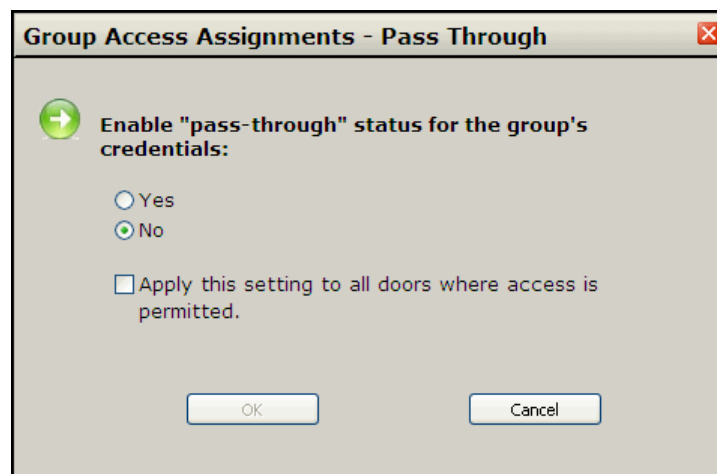


- 8 Using the **Permitted Access Time Zone:** drop down menu, select the Time Zone during which this group will have access to these doors.
- 9 Click **OK**. This will close the pop-up window. All the selected doors will now have time zones assigned to them.

- 10 **OPTIONAL** - If this group is to be assigned Toggle rights, then click the **Toggle** button on the right of the screen. This will open the **Group Access Assignments - Toggle Allowed** pop-up window.



- a) Click on the **Yes** check box to enable this feature.
- b) Click **OK**. This will close the Toggle Allowed pop-up window and enable Toggle for all doors assigned to this group.
- 11 **OPTIONAL** - If this group is to be assigned Pass-Through rights, then click on the Pass-Through button on the right of the screen. This will open the **Group Access Assignments - Pass Through** pop-up window.



- a) Click on the **Yes** check box to enable this feature.
- b) Click **OK**. This will close the Pass-Through pop-up window and enable the Pass-Through ability for all doors assigned to this group.
- 12 Click the **Save Changes** button at the top of the screen. The Save Changes? pop up will open.
- 13 Click **OK**. The **Group Access Assignments - Process** pop-up window will open. This window shows the progress of the saved changes. It will close when complete.

- 14 Repeat steps 1 through 12 for each new group of people to be assigned access.

Activity

CHAPTER 3

Introduction

The Activity Monitor window is used to view all current system activity including personnel and device transactions. This screen is split into two separate sections; the Personnel Transactions section is used to view the activities of personnel while the System and Devices Transactions section is used to view the system, device and System User activity. The Activity Monitor window can be accessed by clicking on the Activity button on the left side of the main screen. This section is accessible by all users.

Activity Monitor - Maximum 100 transactions in the last 72 hours				
Refresh		Personnel Transactions	Settings	Help
Date-Time	Transaction	Personnel	Encoded ID	Door
2009-12-09 12:24:44	Access denied - credential not assigned to anyone		196851	AD400CY Cylindrical Lockset -0
2009-12-09 12:24:36	Valid access	Visitor, Card	109	AD400CY Cylindrical Lockset -0
2009-12-09 12:23:27	Valid access	Visitor, Card	109	AD300MD Mortise Deadbolt Lockset -1
2009-12-09 12:23:21	Valid access	Visitor, Card	109	AD400CY Cylindrical Lockset -0
2009-12-09 12:22:52	Access denied - credential not assigned to anyone		196851	AD400CY Cylindrical Lockset -0
2009-12-09 12:22:39	Valid access	Montalva, Alberto Brian	7171	WA5200 Cylindrical Lockset - 5
2009-12-09 12:22:26	Access denied - credential not assigned to anyone		196851	AD300MD Mortise Deadbolt Lockset -1
2009-12-09 12:21:56	Valid access	Montalva, Alberto Brian	7171	AD400CY Cylindrical Lockset -0
2009-12-09 12:20:52	Toggle - Resume normal operation	Montalva, Alberto Brian	7171	AD400CY Cylindrical Lockset -0
2009-12-09 12:20:36	Toggle - door unlocked	Montalva, Alberto Brian	7171	AD400CY Cylindrical Lockset -0
2009-12-09 12:20:35	Valid access	Montalva, Alberto Brian	7171	AD400CY Cylindrical Lockset -0
2009-12-09 12:20:22	Toggle - Resume normal operation	Montalva, Alberto Brian	7171	AD400CY Cylindrical Lockset -0
2009-12-09 12:19:41	Toggle - door unlocked	Montalva, Alberto Brian	7171	AD400CY Cylindrical Lockset -0
2009-12-09 12:19:40	Valid access	Montalva, Alberto Brian	7171	AD400CY Cylindrical Lockset -0

System and Device Transactions				
Refresh				
Date-Time	Transaction	System Component	Device	System User
2009-12-09 12:23:20	Contact secure	Reader: WA5200 Cylindrical Lockset - 5	Contact: Tamper Switch	
2009-12-09 12:23:20	Tamper switch violation	Reader: WA5200 Cylindrical Lockset - 5	Contact: Tamper Switch	
2009-12-09 12:23:19	Contact secure	Reader: WA5200 Cylindrical Lockset - 5	Contact: Tamper Switch	
2009-12-09 12:22:43	Relay released	Reader: WA5200 Cylindrical Lockset - 5	Relay: Door Unlock Relay	
2009-12-09 12:22:41	Tamper switch violation	Reader: WA5200 Cylindrical Lockset - 5	Contact: Tamper Switch	
2009-12-09 12:22:40	Relay energized	Reader: WA5200 Cylindrical Lockset - 5	Relay: Door Unlock Relay	
2009-12-09 12:22:39	Contact secure	Reader: WA5200 Cylindrical Lockset - 5	Contact: Tamper Switch	
2009-12-09 12:22:16	Contact secure	Reader: AD400CY Cylindrical Lockset -0	Contact: Request To Exit	
2009-12-09 12:22:16	Request to exit activated	Reader: AD400CY Cylindrical Lockset -0	Contact: Request To Exit	
2009-12-09 12:22:14	Contact secure	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	
2009-12-09 12:22:14	Request to enter activated	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	
2009-12-09 12:22:12	Contact secure	Reader: AD400CY Cylindrical Lockset -0	Contact: Request To Exit	
2009-12-09 12:22:11	Request to exit activated	Reader: AD400CY Cylindrical Lockset -0	Contact: Request To Exit	
2009-12-09 12:22:01	Contact secure	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	
2009-12-09 12:22:01	Request to enter activated	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	
2009-12-09 12:22:01	Contact secure	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	
2009-12-09 12:22:00	Request to enter activated	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	
2009-12-09 12:22:00	Contact secure	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	
2009-12-09 12:22:00	Request to enter activated	Reader: AD400CY Cylindrical Lockset -0	Contact: Request to Enter	

Personnel Transactions

This section has five buttons along the top of the window.

- **Refresh** - Refreshes the screen to show the most current transaction activity.
- **Pause** - Stops the screen from auto-refreshing. This button is not active if the refresh rate is set to Never. See the Settings section below for more details.
- **Play** - Re-starts the auto-refreshing after it has been paused. This button is not active if the refresh rate is set to Never. See the Settings section below for more details.
- **Settings** - Opens the Settings window. This is where the Activity Monitor Settings are changed. See the Settings section below for more details.
- **Help** - Access the help file.

System and Device Transactions

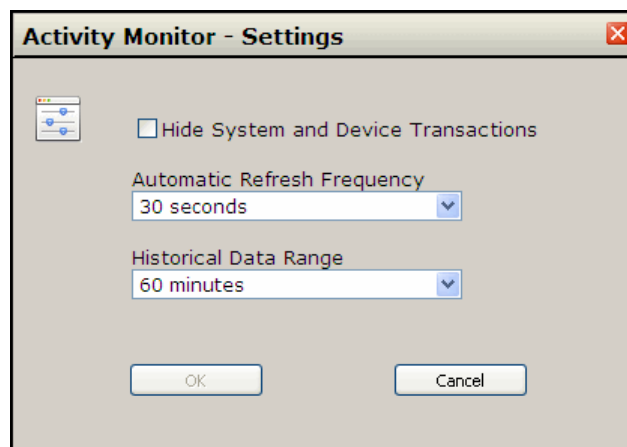
This section has one button.

- **Refresh** - Refreshes the screen to show the most current System and Device Transactions.

Note: The lists of system and device transactions will return to the top whenever the window refreshes. To scroll to the bottom of the list without interruption, click on the **Pause** button before scrolling. Click on the **Play** button to resume the auto-refresh.

Activity Monitor Settings

The Settings window is opened by clicking on the **Settings** button from the Activity Monitor window.



- **Hide System and Device Transactions** - Check this box to hide the System and Device Transactions section of the Activity Monitor window.
- **Automatic Refresh Frequency** - Determines how often the Activity Monitor window refreshes. If Never is selected then the screen will only refresh when the Refresh button is clicked.
- **Historical Data Range** - Shows the last 100 transactions for the selected period of time. Example: If Historical Data Range is set to 60 minutes then the Activity Monitor window will display the most recent 100 transactions that occurred in the last 60 minutes.
-

Personnel Transactions

The Personnel Transactions frame displays the transactions of the personnel that are located in the database. There are a variety of activities that can appear in the Personnel Transactions frame.

- **Access Denied** - There are several reasons why a credential might be denied access.
 - Invalid site code - Indicates that the site code encoded on the card does not match one of the site codes specified in the Door Setup - Global Settings - Facility/Site Code tab.
 - Badge not in controller memory - Appears if a badge has not been uploaded to the controller's memory.
 - Anti-passback violation on entry attempt - Appears when the same credential is swiped twice in a row at an entry reader before the anti-passback time has elapsed (if timed anti-passback is in use) or before the credential has been used at an exit reader.
 - Anti-passback violation on exit attempt - Appears when the same credential is swiped twice in a row at an exit reader before the anti-passback time has elapsed (if timed anti-passback is in use) or before the credential has been used at an entry reader.
 - Badge not yet activated or Door access privileges not yet active - Indicates that a credential is in the database but the activation date has not yet occurred.
 - Badge has expired - Indicates that a credential is in the database but has passed the expiration date that is specified in the personnel record.
 - Badge has been blocked from all access - Appears if the option Access Blocked is selected in the personnel record for this person.
 - Access to door not permitted - Appears if this person does not have access permissions to this door.
 - Access to door not permitted during timezone - Indicates that a person attempted to access a door outside of their scheduled timezone.
 - Access permissions to this door have expired - Indicates that the person had access to this door but their expiration date has passed.
 - Invalid Issue Code - This transaction will occur when issue codes are being used in the system and a person has tried to access a door with a card that has an issue code that precedes the current one. Please see the paragraph on Issue Codes in the Adding Personnel section for details.

- **Valid Access** - Indicates that a person presented their credential and gained access.
- **Valid Access, Special Access Privilege** - Indicates that a person with Special Access Privileges presented their credential and gained access.
- **Valid Entry** - Indicates that a person gained access to a door that is set up as an entry reader.
- **Valid Entry, Special Access Privilege** - Indicates that a person with Special Access Privileges gained access to a door that is set up as an entry reader.
- **Valid Exit** - Indicates that a person gained access to a door that is set up as an exit reader.
- **Valid Exit, Special Access Privilege** - Indicates that a person with Special Access Privileges gained access to a door that is set up as an exit reader.

System and Device Transactions

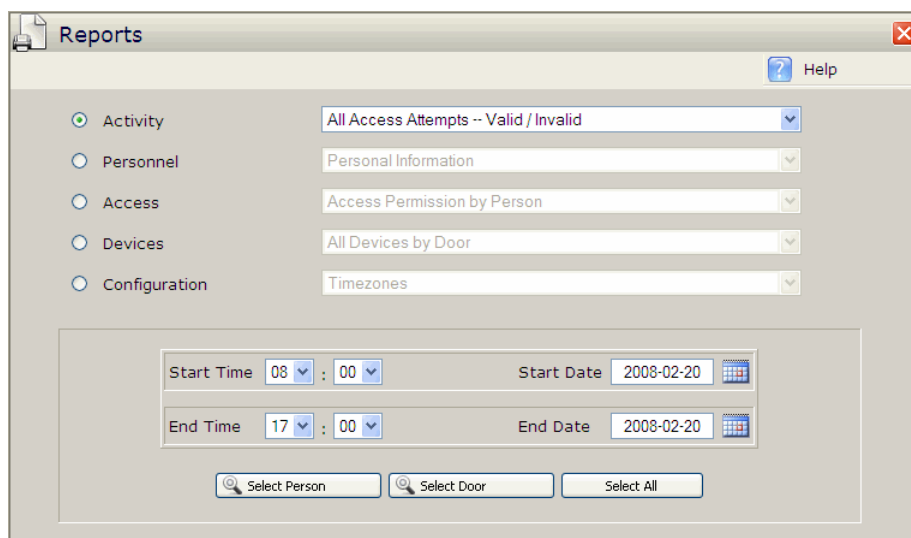
The System and Device Transactions frame is displayed in the bottom of the Activity Monitor screen. This frame displays the transactions that relate to system, device and System User activity.

Reports

CHAPTER 4

Introduction

The Reports window is used to generate and view reports on various activities. There are five different types of reports available: Activity, Personnel, Access, Devices and Configuration. The user selects a report and enters start and end time/date criteria. The Reports window can be accessed by clicking on the Reports button on the left side of the main screen. This section is accessible by all users, however Operators will have Read-only access rights.



The screenshot shows the 'Reports' window with a title bar containing a file icon, the text 'Reports', and a red close button. A 'Help' button with a question mark icon is in the top right. The main area has five radio buttons on the left: 'Activity' (selected), 'Personnel', 'Access', 'Devices', and 'Configuration'. To the right of each radio button is a dropdown menu. For 'Activity', the dropdown shows 'All Access Attempts -- Valid / Invalid'. For 'Personnel', it shows 'Personal Information'. For 'Access', it shows 'Access Permission by Person'. For 'Devices', it shows 'All Devices by Door'. For 'Configuration', it shows 'Timezones'. Below these is a section with two rows of time and date pickers. The first row has 'Start Time' (08 : 00) and 'Start Date' (2008-02-20). The second row has 'End Time' (17 : 00) and 'End Date' (2008-02-20). At the bottom are three buttons: 'Select Person', 'Select Door', and 'Select All'.

Activity

Activity reports display information on transaction activity. Select the Activity button to enable a drop down menu that lists all activity-related reports.

To run a report:

- 1 Click on the desired report from the drop down menu.
- 2 Select the time and date criteria.
- 3 Run report by person, door or both (Select Person, Select Door or Select All).

Each activity report is explained below in detail.

The screenshot shows a 'Reports' window with the following elements:

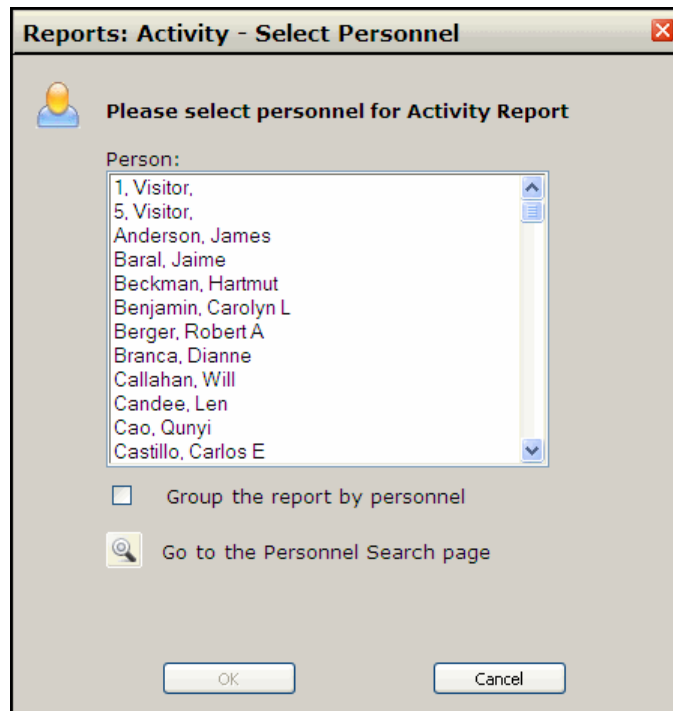
- Activity Selection:** Radio buttons for Activity (selected), Personnel, Access, Devices, and Configuration.
- Report Type List:** A list box showing a dropdown menu with the following options:
 - All Access Attempts -- Valid / Invalid (selected)
 - All Access Attempts -- Valid
 - All Access Attempts -- Invalid
 - Operator Activity
 - System Events (Communications, Power, Relays, and Contacts)
 - Contacts
 - Relays
 - Timezones
- Time and Date Fields:**
 - Start Time: 08 : 00
 - Start Date: 2008-01-10
 - End Time: 17 : 00
 - End Date: 2008-01-10
- Action Buttons:** Select Person, Select Door, and Select All.

- **Start Time** - Used to specify the beginning time of the report. Default is 8:00.
- **End Time** - Used to specify the ending time of the report. Default is 17:00.
- **Start Date** - Used to specify the beginning date of the report. Default is the current date.
- **End Date** - Used to specify the end date of the report. Default is the current date.

All Access Attempts Valid/Invalid

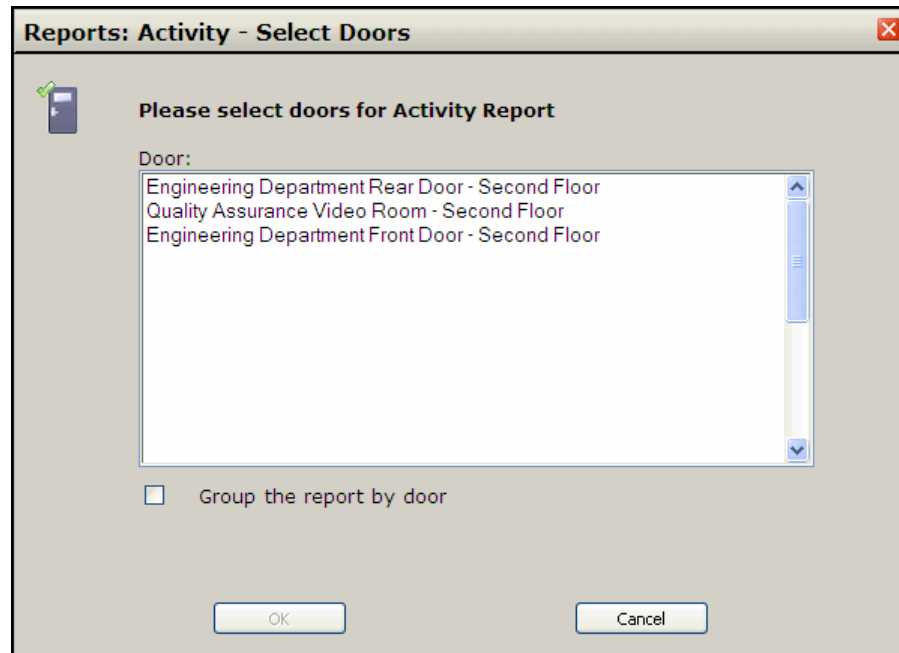
This report displays all valid and invalid access attempts and can be run by person, door or both (Select Person, Select Door, Select All).

- **Select Person** - Clicking on this button will open the Select Personnel pop-up window.



- **Person** - Select the person(s) to run the report on from this list.
- **Group the report by personnel** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by personnel.
- **Go to the Personnel Search page** - Click on this button to open the Personnel Search window. From here specific personnel can be found.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.

- **Select Door** - Clicking on this button will open the Select Door pop-up window.

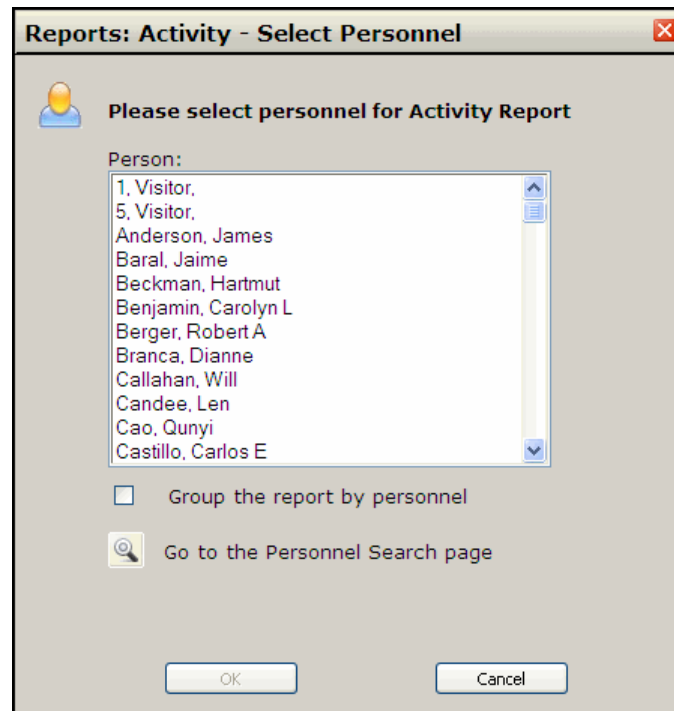


- **Door** - Select the door(s) to run the report on from this list.
- **Group the report by door** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by door.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.
- **Select All** - Clicking on this button will run a report that is inclusive of all attempts, by all personnel at all doors, within the specified time span.

All Access Attempts Valid

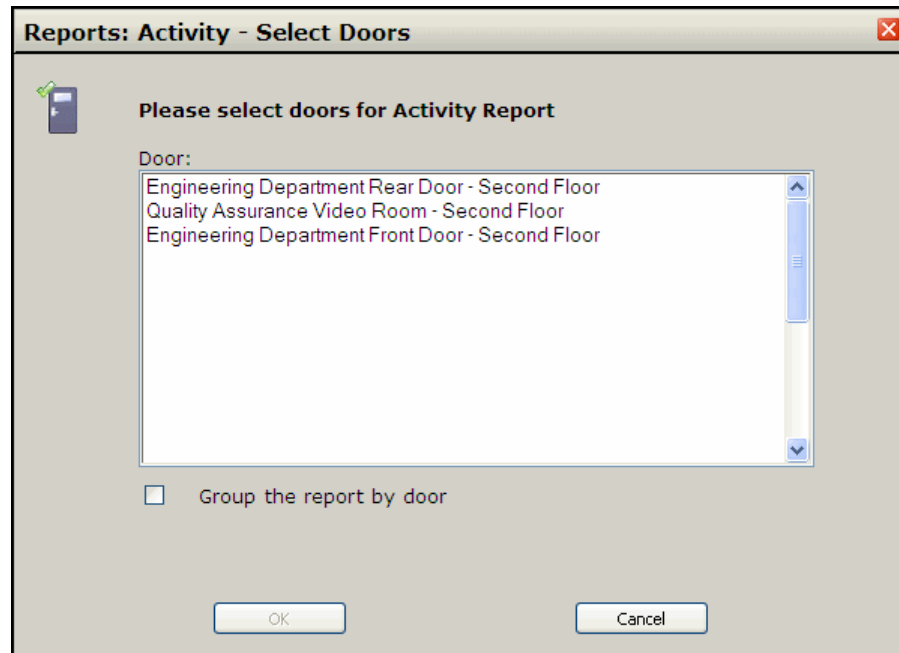
This report displays valid access attempts and can be run by person, door or both (Select Person, Select Door, Select All).

- **Select Person** - Clicking on this button will open the Select Personnel pop-up window.



- **Person** - Select the person(s) to run the report on from this list.
- **Group the report by personnel** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by personnel.
- **Go to the Personnel Search page** - Click on this button to open the Personnel Search window. From here specific personnel can be found.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.

- **Select Door** - Clicking on this button will open the Select Door pop-up window.

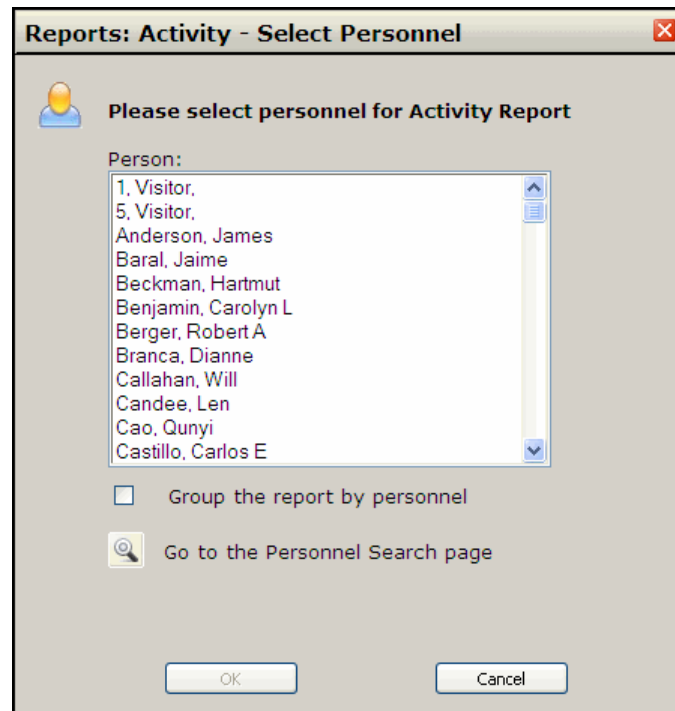


- **Door** - Select the door(s) to run the report on from this list.
- **Group the report by door** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by door.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.
- **Select All** - Clicking on this button will run a report that is inclusive of all valid attempts, by all personnel at all doors, within the specified time span.

All Access Attempts Invalid

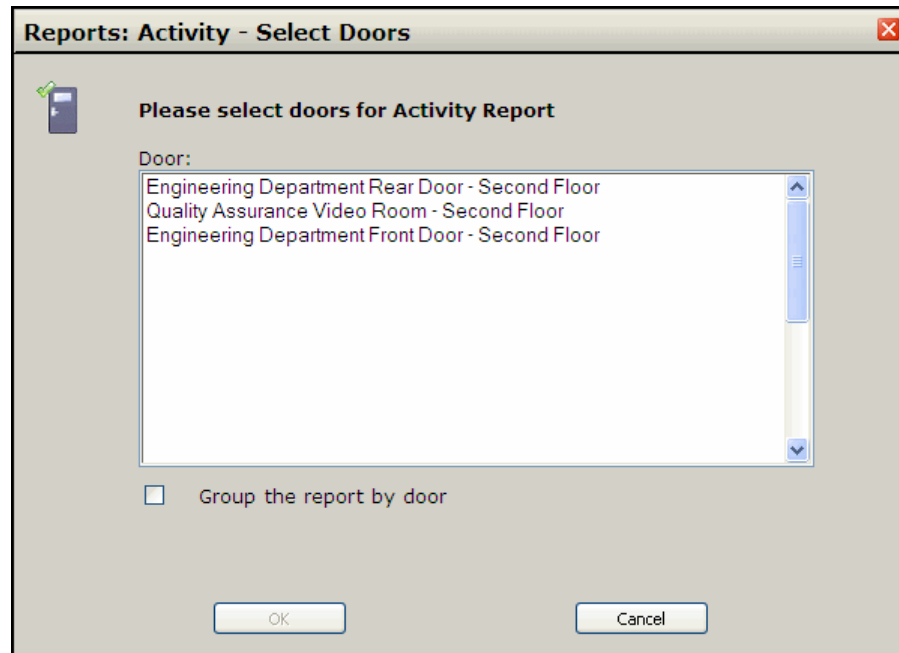
This report displays invalid access attempts and can be run by person, door or both (Select Person, Select Door, Select All).

- **Select Person** - Clicking on this button will open the Select Personnel pop-up window.



- **Person** - Select the person(s) to run the report on from this list.
- **Group the report by personnel** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by personnel.
- **Go to the Personnel Search page** - Click on this button to open the Personnel Search window. From here specific personnel can be found.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.

- **Select Door** - Clicking on this button will open the Select Door pop-up window.

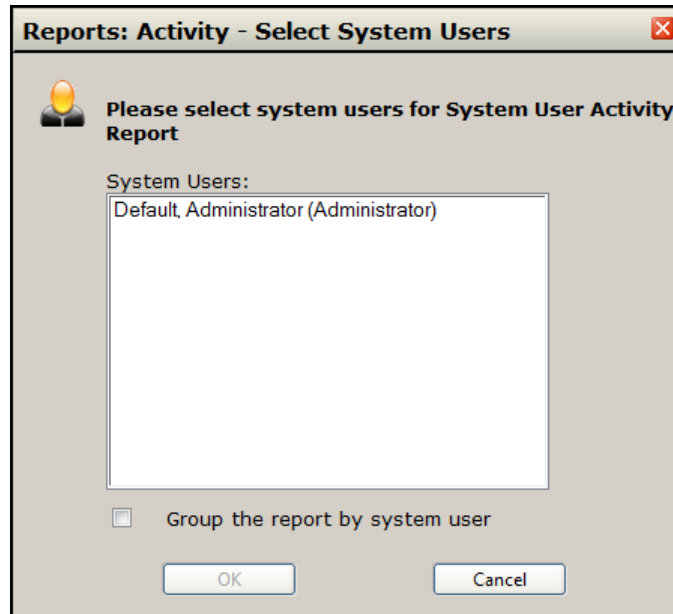


- **Door** - Select the door(s) to run the report on from this list.
- **Group the report by door** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by door.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.
- **Select All** - Clicking on this button will run a report that is inclusive of all invalid attempts, by all personnel at all doors, within the specified time span.

System User Activity

This report displays all System User activity and can be run for a specific user or all users (Select System User, Select All).

- **Select System User** - Clicking on this button will open the Select System Users pop-up window.

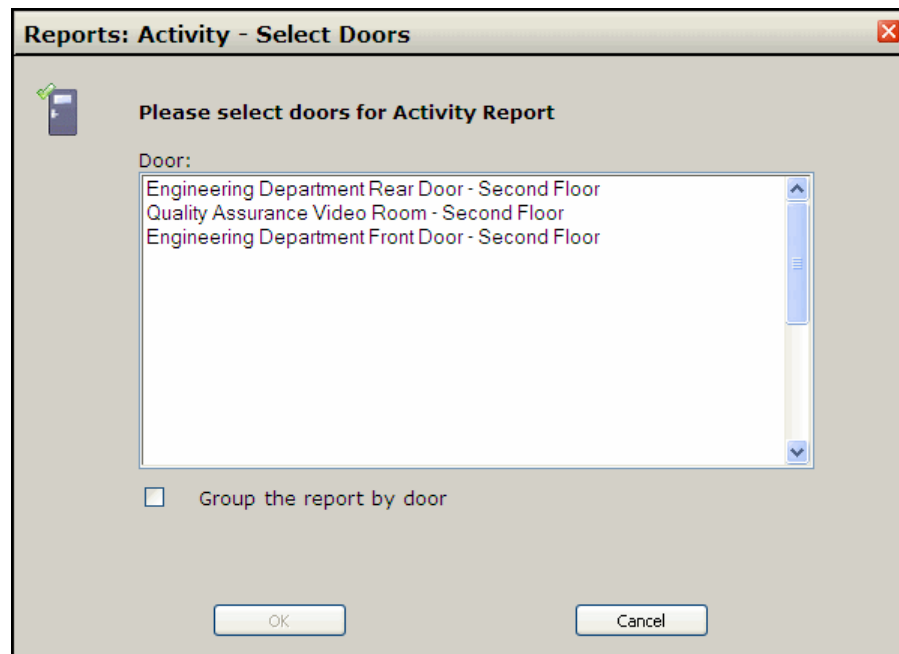


- **System User** - Select the system user(s) to run the report on from this list.
- **Group the report by system user** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by system user.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.
- **Select All** - Clicking on this button will run a report with all the system user activities that have occurred within the specified time span.

System Events (Communications, Power, Relays, and Contacts)

This report displays all system events and can be run by a specific door or all doors (Select Door, Select All).

- **Select Door** - Clicking on this button will open the Select Door pop-up window.

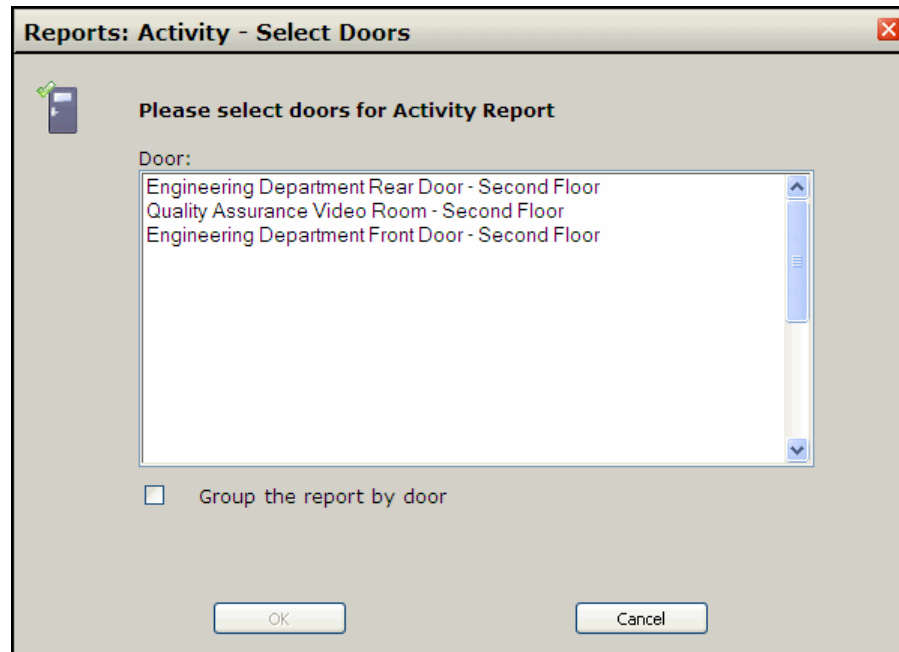


- **Door** - Select the door(s) to run the report on from this list.
- **Group the report by door** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by door.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.
- **Select All** - Clicking on this button will run a report with all the system activities that have occurred within the specified time span.

Contacts

This report displays all door contact activity and can be run by a specific door or all doors (Select Door, Select All).

- **Select Door** - Clicking on this button will open the Select Door pop-up window.



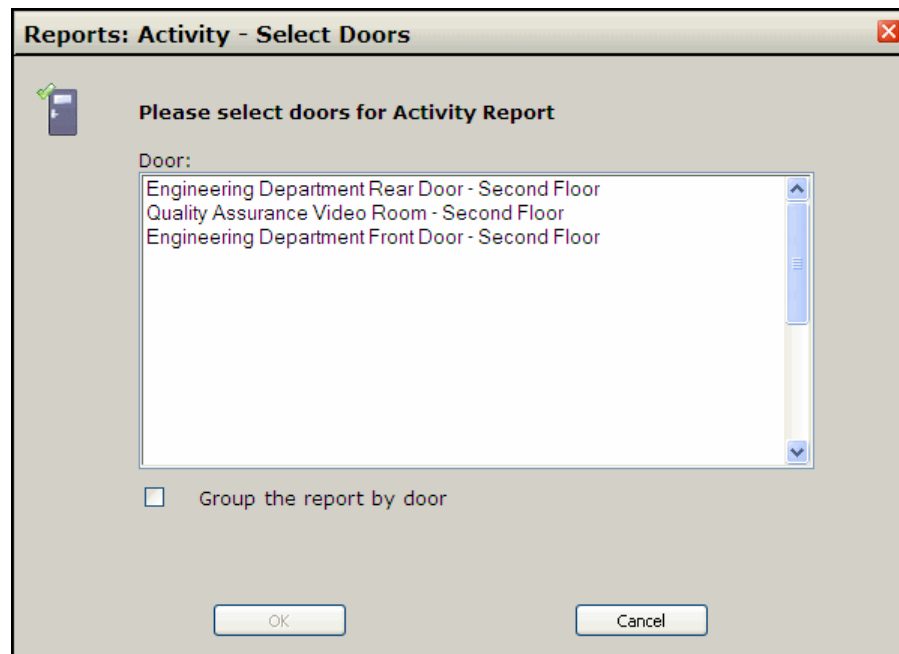
- **Door** - Select the door(s) to run the report on from this list.
- **Group the report by door** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by door.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.
- **Select All** - Clicking on this button will run a report with all the contact activities that have occurred within the specified time span.

Note: With the AD Series locks, when a door has a valid access you will receive a Lock Clutch Energized transaction. This transaction is a contact, not a relay. To run a report on when an AD Series lock was unlocked, you'll want to run a Contact report, not a Relay report.

Relays

This report displays all door relay activity and can be run by a specific door or all doors (Select Door, Select All).

- **Select Door** - Clicking on this button will open the Select Door pop-up window.



- **Door** - Select the door(s) to run the report on from this list.
- **Group the report by door** - This check box changes how the report is displayed. Leaving this box unchecked will display a report in a time specific order. Checking this box will display the information by door.
- **OK** - Click on this button to display the report.
- **Cancel** - Click on this button to close the pop-up without displaying a report.
- **Select All** - Clicking on this button will run a report with all the relay activities that have occurred within the specified time span.

Note: With the AD Series locks, when a door has a valid access you will receive a Lock Clutch Energized transaction. This transaction is a contact, not a relay. To run a report on when an AD Series lock was unlocked, you'll want to run a Contact report, not a Relay report.

Sample Activity Report

The reports generated by the Activity section of the Reports window all have a similar appearance. From here you can Print or Export your report.

Reports - Device Activity			
Print	Export	Reverse Sort	page 21 of 44 Help
<p align="center">ALL SYSTEM EVENTS HISTORY REPORT between 2009-12-09 08:00:00 and 2009-12-09 17:00:59</p>			
Date	Time	Transaction	Door
2009-12-09	12:18:22	Contact secure - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:22	Tamper switch violation - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:23	Contact secure - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:24	Tamper switch violation - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:24	Relay released - Door Unlock Relay	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:26	Contact secure - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:26	Tamper switch violation - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:42	Contact secure - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:42	Tamper switch violation - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:56	Contact secure - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:18:56	Tamper switch violation - Tamper Switch	WA5200 Cylindrical Lockset - 5
2009-12-09	12:19:32	Lock clutch engaged - Lock Clutch Position	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:32	Contact secure - Key Switch Monitor	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:35	Lock clutch released - Lock Clutch Position	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:35	Key override activated - Key Switch Monitor	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:40	Lock clutch engaged - Lock Clutch Position	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:40	Contact secure - Key Switch Monitor	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:45	Request to enter activated - Request to Enter	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:48	Contact secure - Request to Enter	AD400CY Cylindrical Lockset - 0
2009-12-09	12:19:55	Request to enter activated - Request to Enter	AD400CY Cylindrical Lockset - 0

Print - Clicking this button will open the **Print** pop-up window. From there you can select which printer to use and then print the report.

Export - Clicking this button will open the **Export** pop-up window. From there you select where to save the report. Reports are exported as .csv files which can be opened by MS Excel and other spreadsheet programs.

Reverse Sort - Clicking this button will reverse the order of transactions on the screen.

Navigation Arrows - Click these buttons to switch between pages.



Click this to go to the first page of the report.



Click this to go forward a page.



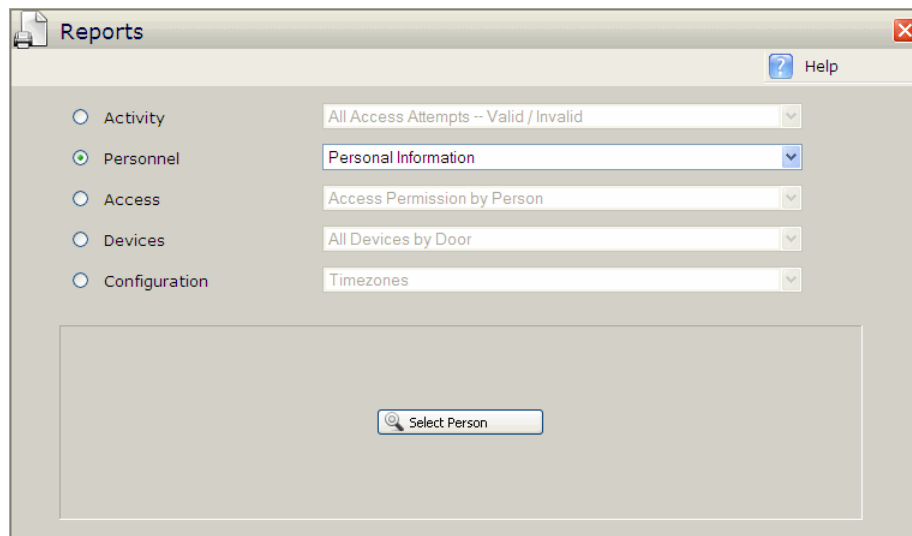
Click this to go backward a page.



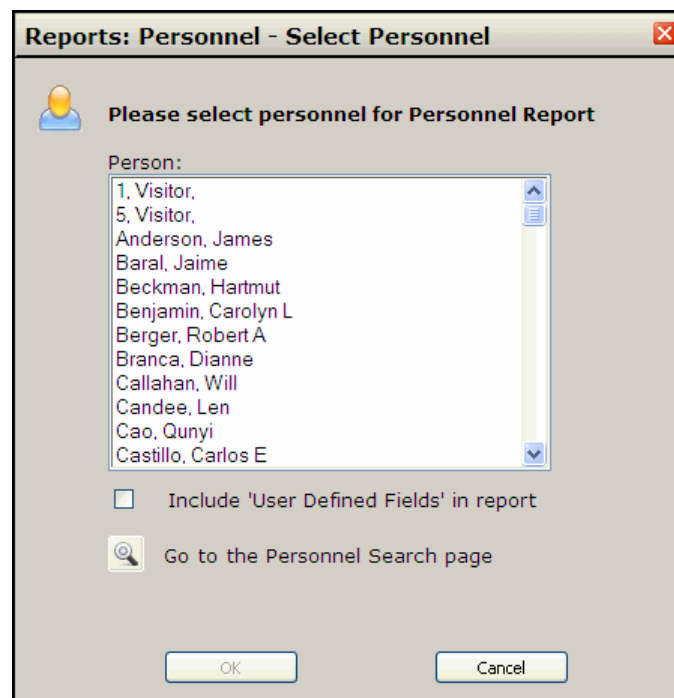
Click this to go to the last page of the report.

Personnel

Personnel reports display the personnel information of persons, such as activation date, expiration date, special access, etc. The personal information contained in the User Defined Fields, such as birth date and contact information, can also be reported.



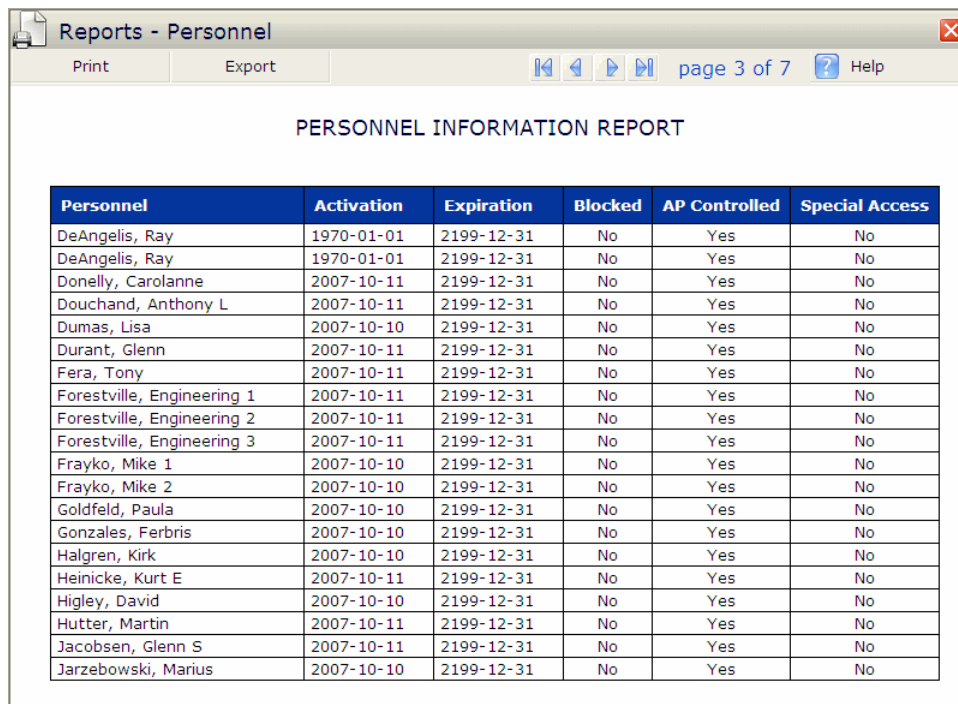
- **Select Person** - Clicking on this button opens the Select Personnel pop-up window.



- **Person:** - Use this field to select the desired person to report on.
- **Include 'User Defined Fields' in report** - Check this box to view the information in the User Defined Fields.
- **Go to the Personnel Search page** - Click this button to open the **Personnel Search** window. From there you can search for a specific person in the system. Please see the **Searching for a Specific Record** section of the **Personnel** chapter for more details.
- **Ok** - Click this button to run the report.
- **Cancel** - Click this button to close the pop-up without running the report.

Sample Personnel Report

The reports generated by the Personnel section of the Reports window all have a similar appearance. From here you can Print or Export your report.



Personnel	Activation	Expiration	Blocked	AP Controlled	Special Access
DeAngelis, Ray	1970-01-01	2199-12-31	No	Yes	No
DeAngelis, Ray	1970-01-01	2199-12-31	No	Yes	No
Donelly, Carolanne	2007-10-11	2199-12-31	No	Yes	No
Douchand, Anthony L	2007-10-11	2199-12-31	No	Yes	No
Dumas, Lisa	2007-10-10	2199-12-31	No	Yes	No
Durant, Glenn	2007-10-11	2199-12-31	No	Yes	No
Fera, Tony	2007-10-11	2199-12-31	No	Yes	No
Forestville, Engineering 1	2007-10-11	2199-12-31	No	Yes	No
Forestville, Engineering 2	2007-10-11	2199-12-31	No	Yes	No
Forestville, Engineering 3	2007-10-11	2199-12-31	No	Yes	No
Frayko, Mike 1	2007-10-10	2199-12-31	No	Yes	No
Frayko, Mike 2	2007-10-10	2199-12-31	No	Yes	No
Goldfeld, Paula	2007-10-10	2199-12-31	No	Yes	No
Gonzales, Ferbris	2007-10-10	2199-12-31	No	Yes	No
Halgren, Kirk	2007-10-10	2199-12-31	No	Yes	No
Heinicke, Kurt E	2007-10-11	2199-12-31	No	Yes	No
Higley, David	2007-10-10	2199-12-31	No	Yes	No
Hutter, Martin	2007-10-11	2199-12-31	No	Yes	No
Jacobsen, Glenn S	2007-10-11	2199-12-31	No	Yes	No
Jarzebowski, Marius	2007-10-10	2199-12-31	No	Yes	No

Print - Clicking this button will open the **Print** pop-up window. From there you can select which printer to use and then print the report.

Export - Clicking this button will open the **Export** pop-up window. From there you select where to save the report. Reports are exported as .csv files which can be opened by MS Excel and other spreadsheet programs.

Navigation Arrows - Click these buttons to switch between pages.



Click this to go to the first page of the report.



Click this to go forward a page.



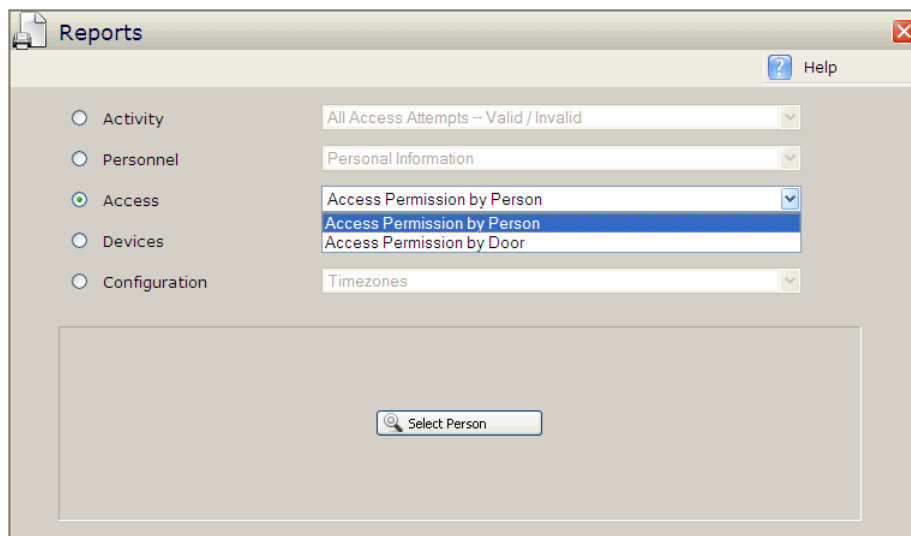
Click this to go backward a page.



Click this to go to the last page of the report.

Access

Access reports display information on who has access to which door. To generate an Access Report click on the button to the left of Access. Two types of access reports can be selected from the drop down menu: "Access Permission by Person" and "Access Permission by Door".



Access Permission by Person

This report displays the doors that a specific person has access to, the times zones assigned to the person for that door and whether toggle rights are available. To run the report:

- 1 Select **Access Permission by Person** from the drop down menu.
- 2 Click on the **Select Person** button. This will open a pop-up window that displays all personnel.
- 3 Select the desired person to report on and click **OK**.
 - a) **OPTIONAL:** Click on the **Go to the Personnel Search** page button. The **Personnel Search** page will open. From here a search can be run for specific Personnel. See the **Searching for Specific Record** section of the **Personnel** chapter for details.

Access Permission by Door

This report displays the personnel assigned to a specific door, what time zones they are using for that door and whether toggle, pass-through and lockdown rights are available. To run the report:

1. Select **Access Permission by Door** from the drop down menu.
2. Click on the **Select Door** button. This will open a pop-up window that displays all doors.
3. Select the desired door to report on and click **OK**.

Sample Access Report

The reports generated by the Access section of the Reports window all have a similar appearance. From here you can Print or Export your report.

ACCESS PERMISSIONS by PERSON							
CLEANING, CARPEL 1							
Door	Timezone	Access Activation	Access Expiration	Blocked	Toggle	Pass Through	Lockdown
Engineering Department Rear Door - Second Floor	Always	2007-12-02 00:00:00	2199-12-31 23:59:59	No	No	No	No
Quality Assurance Video Room - Second Floor	Always	2007-12-02 00:00:00	2199-12-31 23:59:59	No	No	No	No
CLEANING, CARPEL 2							
Door	Timezone	Access Activation	Access Expiration	Blocked	Toggle	Pass Through	Lockdown
Engineering Department Rear Door - Second Floor	Always	2007-12-02 00:00:00	2199-12-31 23:59:59	No	No	No	No
Quality Assurance Video Room - Second Floor	Always	2007-12-02 00:00:00	2199-12-31 23:59:59	No	No	No	No
CLEANING, CARPEL 3							
Door	Timezone	Access Activation	Access Expiration	Blocked	Toggle	Pass Through	Lockdown
Engineering Department Rear Door - Second Floor	Always	2007-12-02 00:00:00	2199-12-31 23:59:59	No	No	No	No
Quality Assurance Video Room - Second Floor	Always	2007-12-02 00:00:00	2199-12-31 23:59:59	No	No	No	No

Print - Clicking this button will open the **Print** pop-up window. From there you can select which printer to use and then print the report.

Export - Clicking this button will open the **Export** pop-up window. From there you select where to save the report. Reports are exported as .csv files which can be opened by MS Excel and other spreadsheet programs.

Navigation Arrows - Click these buttons to switch between pages.



Click this to go to the first page of the report.



Click this to go forward a page.



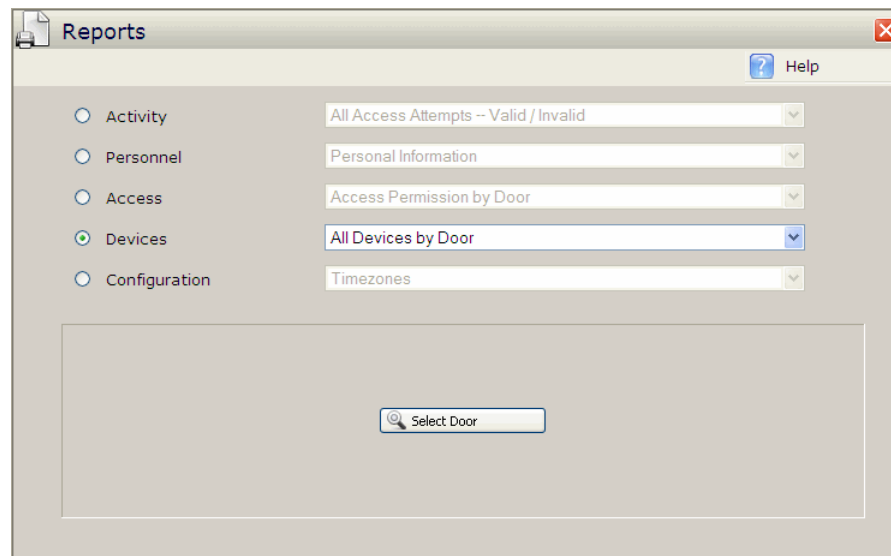
Click this to go backward a page.



Click this to go to the last page of the report.

Devices

Device reports display information about the locking device that is, or will be, installed at a specific door.



To run the report:

- 1 Click on the **Devices** button on the Reports screen.
- 2 Click on the **Select Door** button. This will open a pop-up window that displays all doors.
- 3 Select the desired door to report on and click **OK**.

Sample Devices Report

The reports generated by the Devices section of the Reports window all have a similar appearance. From here you can Print your report.

Reports - Devices [Print] [Navigation Icons] page 2 of 26 [Help]

DOOR INFORMATION REPORT

Quality Assurance Video Room - Second Floor

Device Type	SBB-RI - No REX with DOD Trigger		
Reader Type	Standard Reader		
Channel	2	Unlock Time	3 sec
Address	1	DOD Time	30 sec
Installed	Yes	Special Access Unlock Time	6 sec
AntiPassback Time	0 min	Special Access DOD Time	60 sec

Unlock/Toggle Schedules

Cancel Toggle Time	Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Calendar Days
20:00:00			X	X	X	X	X		

Print - Clicking this button will open the **Print** pop-up window. From there you can select which printer to use and then print the report.

Navigation Arrows - Click these buttons to switch between pages.



Click this to go to the first page of the report.



Click this to go forward a page.



Click this to go backward a page.

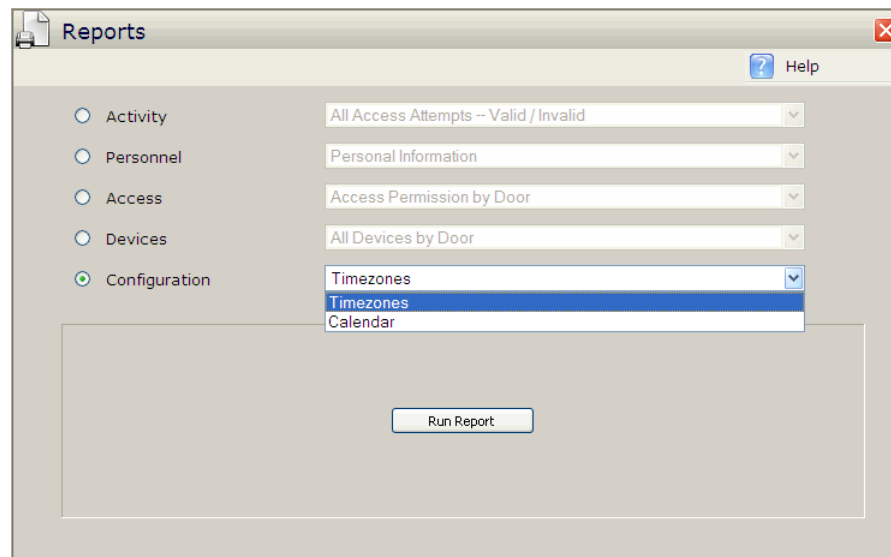


Click this to go to the last page of the report.

Note: There is no Export feature for the Devices Reports.

Configuration

Clicking on the Configuration button will allow you to select one of the configuration reports.



There are two types of configuration reports available: **Time Zones** and the **Calendar** reports.

Time Zones

This report displays information on all of the Time Zones that are set up in the system.

To run the report:

- 1 Click on the Configuration button on the Reports screen.
- 2 Select the **Time Zones** option from the dropdown menu.
- 3 Click on the **Run Report** button. A report will be generated.

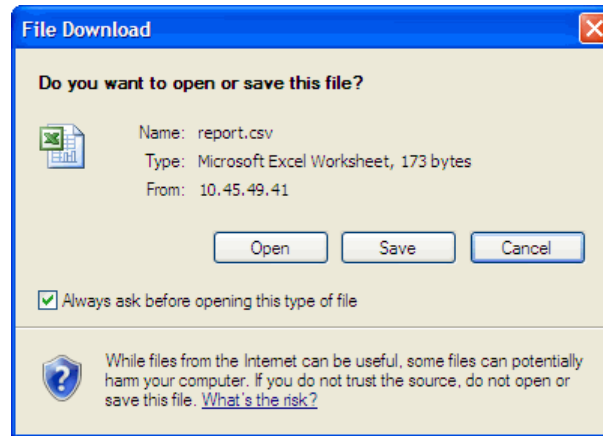
Calendar Events

This report displays information on all of the Calendar Events that are set up in the system.

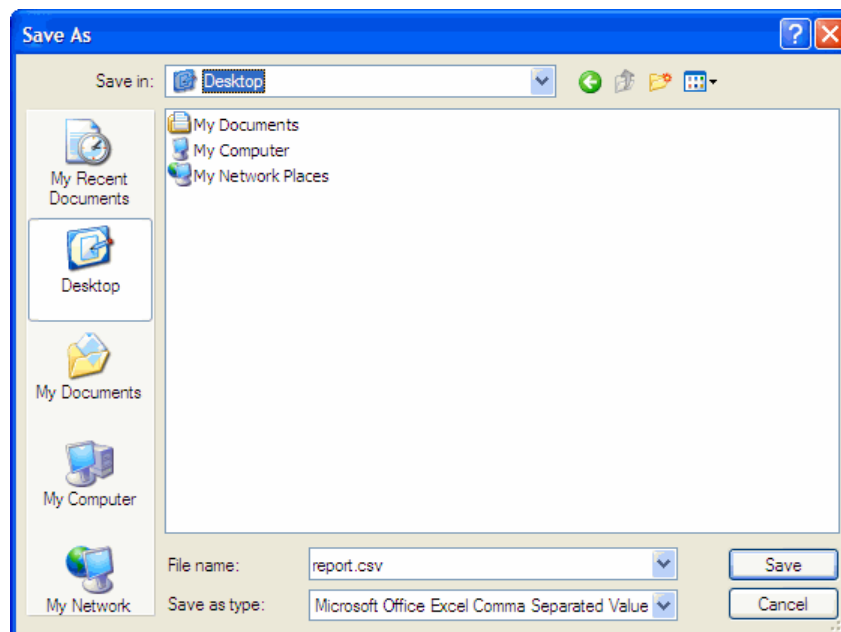
To run the report:

- 1 Click on the **Configuration** button on the Reports screen.
- 2 Select the **Calendar Events** option from the dropdown menu.

- 2 Click on the **Export** button at the top of the window. The File Download pop-up window will open.



- 3 Click on the **Save** button. The Save As pop-up window will open.

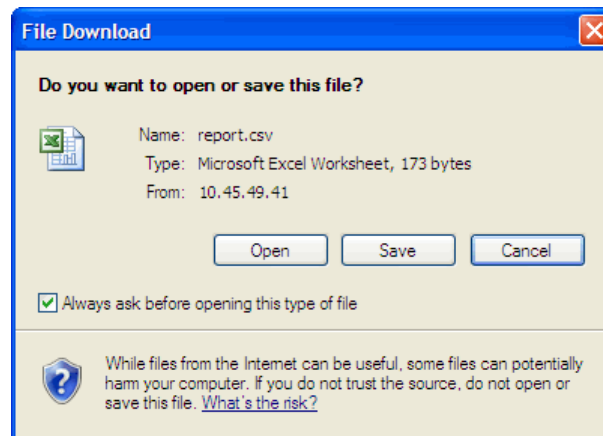


- 4 Select the file destination.
- 5 Click on the **Save** button. The pop-up will close and the file will be saved to the chosen destination.

Opening a report from the web browser

- 1 Generate the report.

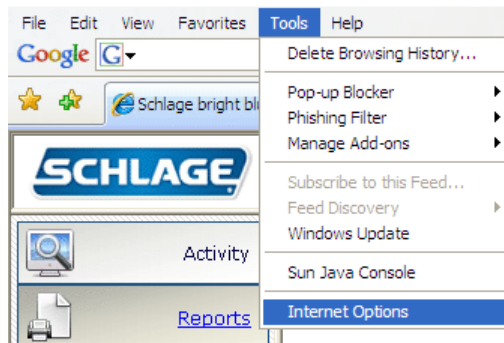
- 2 Click on the **Export** button at the top of the window. The File Download pop-up window will open.



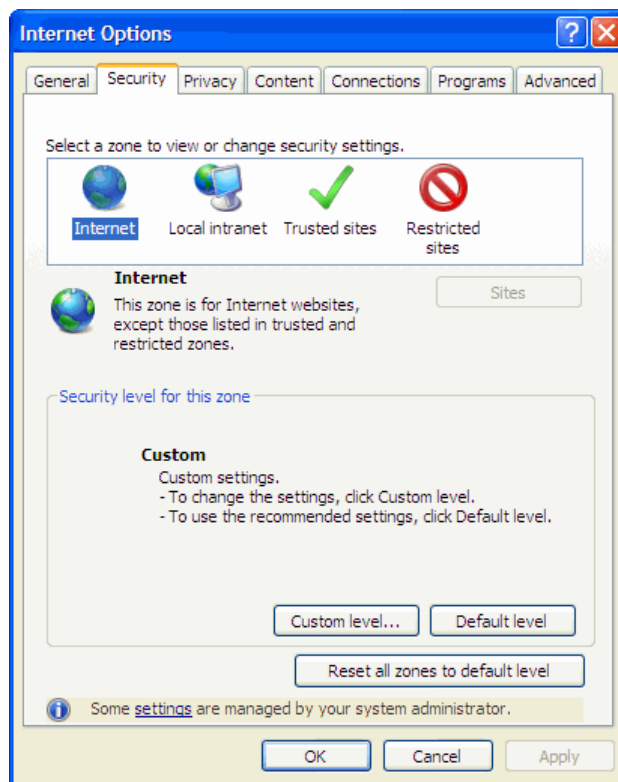
- 3 Click on the **Open** button. The report will open. Depending on the file type settings the report will either open inside the browser or as a separate window.

Enabling downloads with Internet Explorer

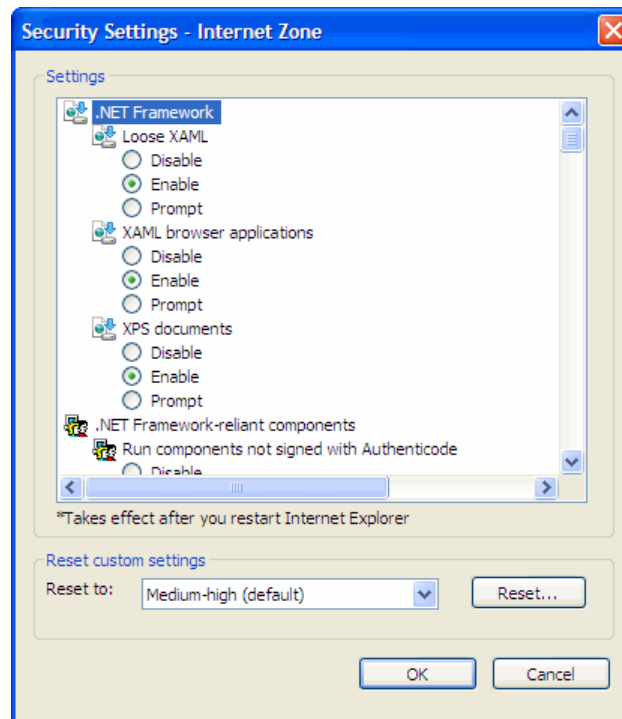
- 1 Open Internet Explorer.
- 2 Go to **Tools>Internet options**.



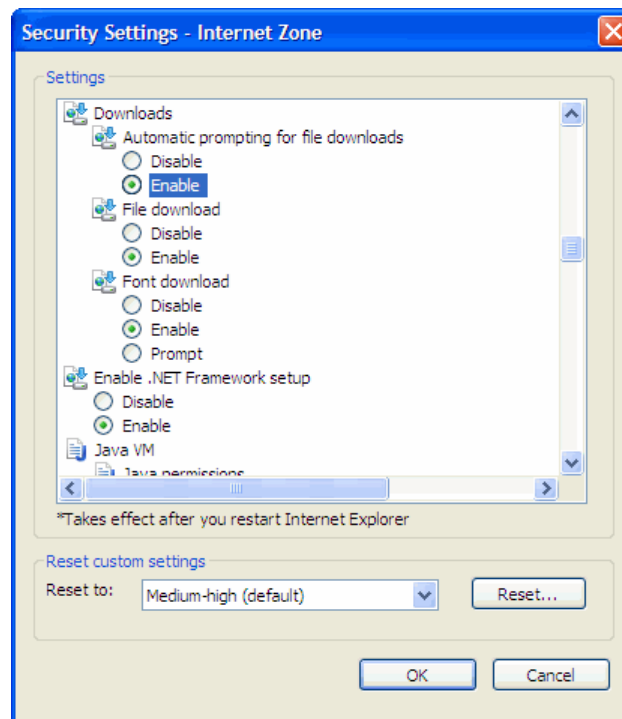
3 Select the **Security Tab**.



- 4 Click on the **Custom level** button. The Security Settings window will open.



- 5 Scroll down to the **Downloads** section.

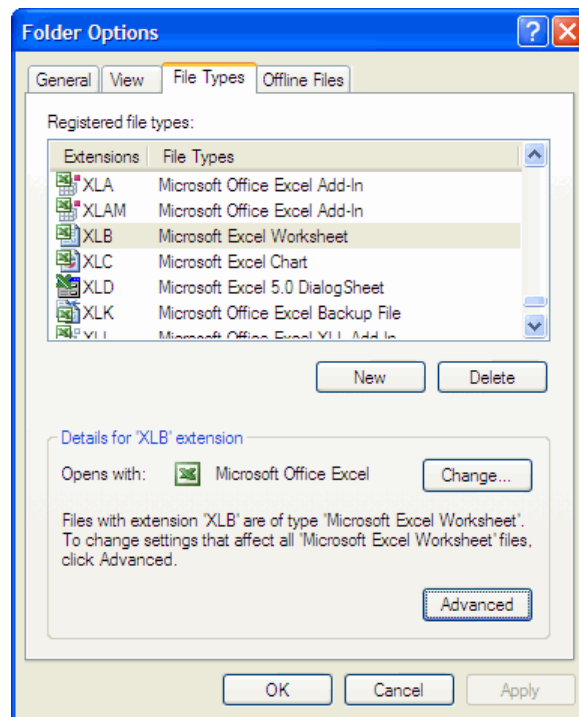


- 6 Under **Automatic prompting for file downloads** click on the **Enable** option.

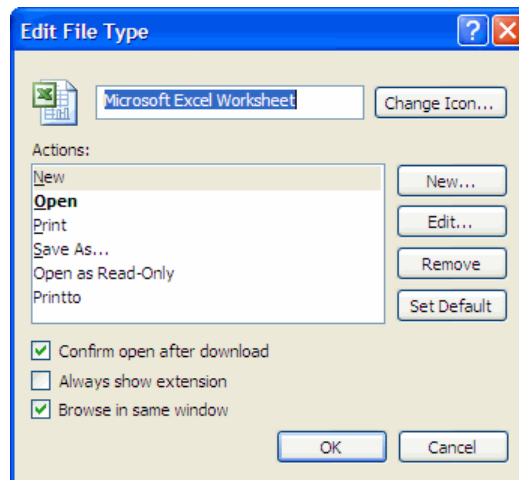
- 7 Click on **Ok**. The Security Settings window will close.
- 8 Click on **Ok** in the Internet Options window. That window will close.
- 9 Reports can now be exported from **bright blue**.

Determining how a report will open

- 1 Double click on **My Computer** from the desktop.
- 2 Go to **Tools>Folder Options**. The Folder Options pop-up window will open.
- 3 Go to the **File Types** tab.
- 4 Scroll down and select the **XLB Microsoft Excel Worksheet**.



- 5 Click on the **Advanced** button. The Edit File Type pop-up window will open.



- 6 Click on the **Browse in same window** check box to determine how an exported report will open.
- **Checked** - Report will open in browser window
 - **Unchecked** - Report will open in separate window
- 7 Click on the **OK** button after making selection. The Edit File Type pop-up will close.
- 8 Click on the **Close** button on the Folder Options pop-up. That window will close.

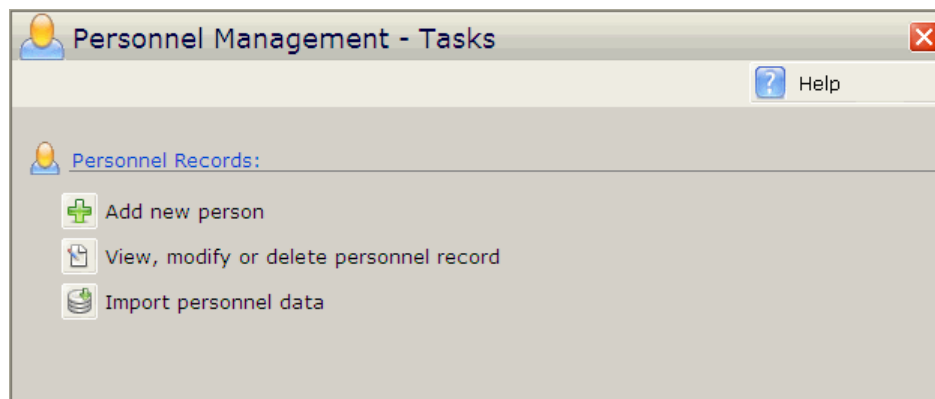
Note - These instructions assume that Microsoft Excel is being used to open .csv files. If a different spreadsheet program is in use, check with an IT person for the correct file type to edit.

Personnel

CHAPTER 5

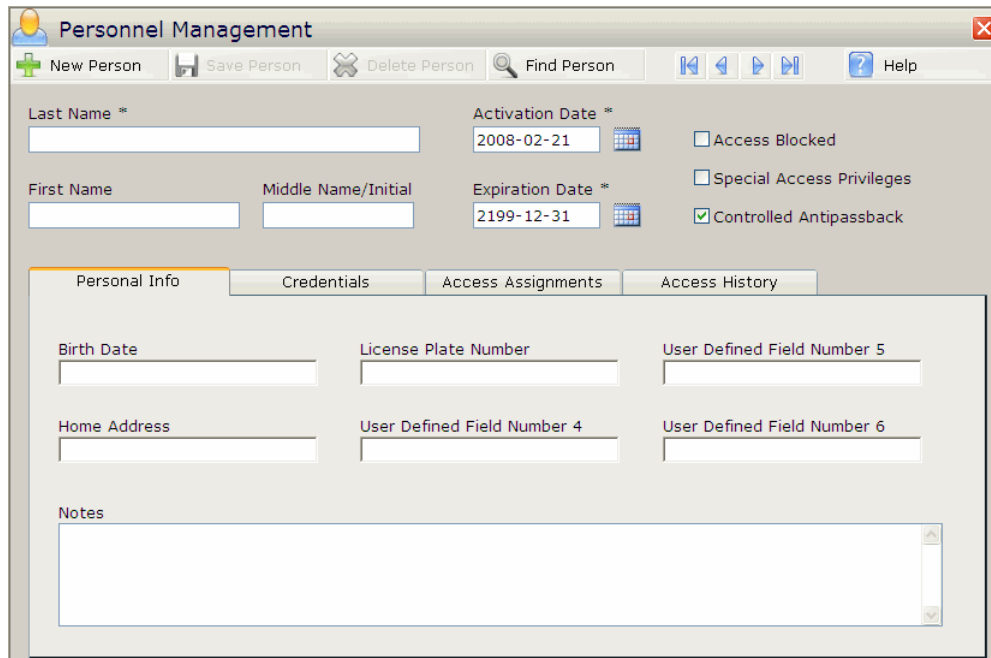
Introduction

The Personnel Management - Tasks window is used to add, modify, delete, and search for personnel in the system. Activation and expiration dates can be set allowing the user to enter a person's information into the system without activating the person's credential. The Personnel Management - Tasks window can be accessed by clicking on the Personnel button on the left side of the main screen. This section is accessible by all users, however, Operators will have Read-only access rights.



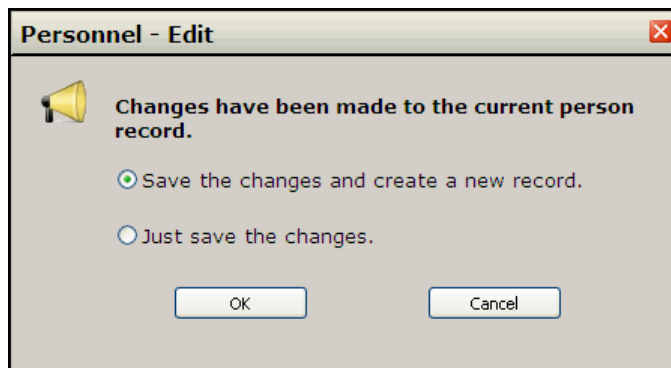
Add new person

Clicking the **Add new person** button opens the Personnel Management window.



The Personnel Management window is a software interface for managing personnel records. It features a title bar with a person icon and the text "Personnel Management". Below the title bar is a toolbar with buttons for "New Person" (green plus icon), "Save Person" (floppy disk icon), "Delete Person" (trash icon), "Find Person" (magnifying glass icon), and a "Help" button (question mark icon). The main area contains several input fields: "Last Name *" (text box), "First Name" (text box), "Middle Name/Initial" (text box), "Activation Date *" (calendar icon, showing 2008-02-21), and "Expiration Date *" (calendar icon, showing 2199-12-31). To the right of these fields are three checkboxes: "Access Blocked", "Special Access Privileges", and "Controlled Antipassback" (checked). Below these fields are four tabs: "Personal Info" (selected), "Credentials", "Access Assignments", and "Access History". The "Personal Info" tab contains fields for "Birth Date", "License Plate Number", "User Defined Field Number 5", "Home Address", "User Defined Field Number 4", and "User Defined Field Number 6". At the bottom of the "Personal Info" tab is a large "Notes" text area.

New Person - Click to add a new personnel record to the database. Please see the Adding Personnel section of the Quick Start chapter for details. If this button is clicked after personnel data has been altered this pop-up window will open:



The Personnel - Edit dialog box is a pop-up window with a title bar that says "Personnel - Edit". It contains a yellow megaphone icon and the text "Changes have been made to the current person record." Below this text are two radio buttons: "Save the changes and create a new record." (selected) and "Just save the changes." At the bottom of the dialog box are two buttons: "OK" and "Cancel".

- **Save the changes and create a new record** - Select this to keep any changes that were made and open a new record.
- **Just save the changes** - Select this to save current personnel changes without opening a new record.
- **OK** - Click on this to execute the selection.
- **Cancel** - Click on this to close the pop-up without changing anything.

Save Person - Click to save any changes that have been made to the current personnel record.

Delete Person - Click to remove the current personnel record from the database.

Find Person - Click to search for a specific personnel record. See the Searching for a Specific Personnel Record section for details.

Navigation Arrows - Click these buttons to switch between personnel records.



Click to go to the first person in the Personnel database.



Click to go to the previous person in the Personnel database.



Click to go to the next person in the Personnel database.



Click to go to the last person in the Personnel database.

Activation Date - Used to set the date that a personnel record becomes active. Prior to the activation date, the credential associated to the personnel record will not work. The default is set to the date that the person is added to the system.

Expiration Date - Used to set the date that a personnel record will expire. After this date, the associated credential will not work. The default date is 2199-12-31.

Access Blocked - Check this box to immediately block a person's access from all doors. The associated credential will not work when access is blocked. Any attempt to use a blocked credential will be displayed in the activity monitor.

Special Access Privileges - Check this box to give this person Special Access Privileges.

Controlled Anti-Passback - Check this box to enable anti-passback. This box is checked by default.

Personal Info

Personal information can be viewed and modified by clicking on the Personal Info tab in the Personnel Management screen. This information is for record keeping purposes only and has no relevance to how the software will view the person's access to doors within the system.

The screenshot shows the 'Personal Info' tab selected. It contains six text input fields arranged in a 2x3 grid, labeled 'User Defined Field Number 1' through 'User Defined Field Number 6'. Below these fields is a large text area labeled 'Notes' with a scroll bar on the right.

- **User Defined Field Number 1 - 6:** The titles of these fields will be renamed to correspond with the User Defined Field section of Utilities.
- **Notes:** Put any additional information about the Personnel record here.

Credentials

A credential is a physical or logical object used at a reader to prove one's identity. The system can store either a magnetic stripe card or a proximity credential. Each person in the system can only be assigned one credential at a time. It is not necessary to assign a credential to a personnel record, but if no credential is assigned then the person will not have access to any doors in the system. A credential can be added to the system by either editing an existing personnel record or creating a new personnel record. The credential information for a person can be displayed by clicking on the Credentials tab.

The screenshot shows the 'Credentials' tab selected. It features a 'Card' icon and three input fields: 'Stamped ID' (a text box), 'Encoded ID' (a text box containing 'Encoded ID NOT entered'), and 'Issue Code' (a dropdown menu showing '0'). A 'Remove...' button is located to the right of the 'Issue Code' dropdown.

- **Stamped ID** - Refers to the number that is printed or stamped onto a credential by the manufacturer. This field is used as a reference to designate cardholders. This is not a required field.
- **Encoded ID** - Refers to the actual raw data stored on a credential. This data is used to verify a person's access privileges. Encoded ID must be entered to save credential data.
- **Issue Code** - This optional field is used to add increased security to the system. When a person loses their credential the replacement credential they receive will be identical to their original with the exception of the Issue Code. The Issue Code for the new card will be one number higher than on the previous card. When the new card is entered into the system it will automatically invalidate any card with a lower Issue Code, making the lost card inoperable.
- **Remove** - Clicking this button will erase all credential data for this person.

Acceptable Card Formats

The system can accept a variety of different magnetic stripe and proximity card formats.

Supported Magnetic Stripe Cards:

- Geoffrey encoded magcard 14-D
- Geo-Image magcard 11-D
- Locknetic 18-D magcard
- One additional custom format. See the Credential Technology section of the Door Setup chapter for details.

Supported Proximity Cards:

- Standard 26-bit
- Schlage 34-bit
- HID 35-bit
- HID/ProxIF 37-bit
- XceedID 40-bit
- Schlage 35-bit (including EV1)
- MiFare 32-Bit Serial Number

Note: The MiFare format is only supported when using a HID read-head with an SBB-RI

How to find a card's encoded ID number

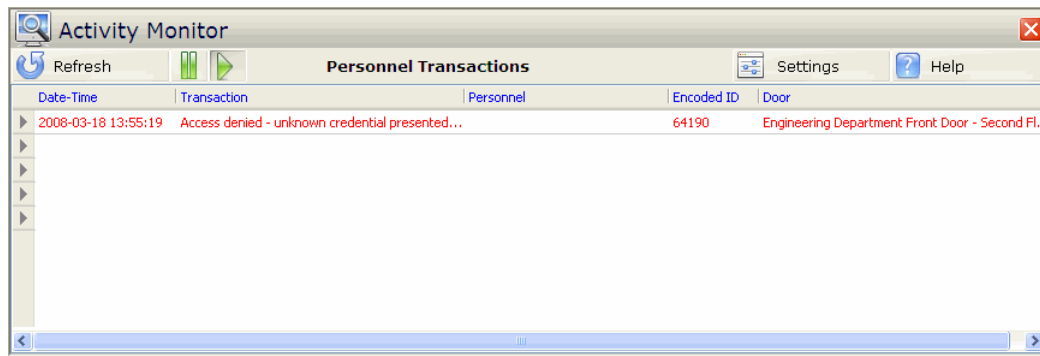
Proximity Card

Proximity cards are shipped with a list of their Stamped and Encoded ID numbers. Sometimes these numbers are identical and sometimes there is an offset value. An offset value is a number that is added to the Stamped ID number to get the Encoded ID number. Example: A card has an offset value of 1000 and the Stamped ID is 2546. The Encoded ID number is 3546.

If there is no stamped id, or if the offset value isn't known, then the Activity Monitor can be used to find the Encoded ID.

- 1 Click on the **Activity** button on the left of the main screen. The Activity Monitor window will open.

- 2 Present the proximity card to a proximity reader that is connected to **bright blue**.
- 3 Wait for the activity monitor to refresh, or click on the **Refresh** button.
- 4 An Access Denied transaction will be displayed on the Personnel Transactions section of the Activity Monitor.



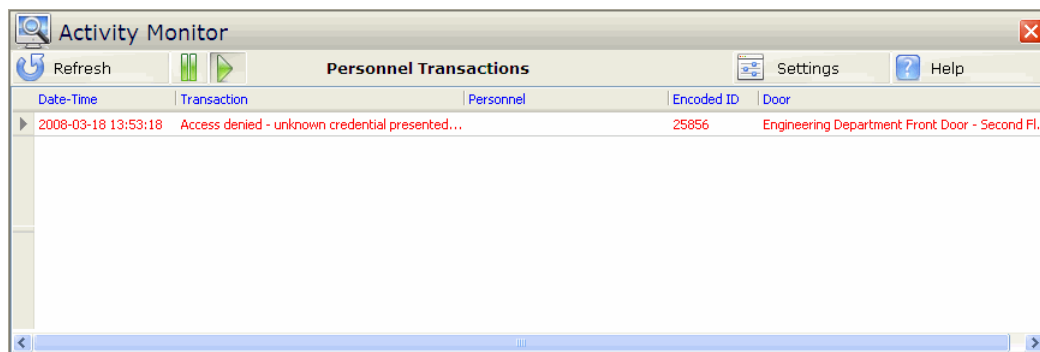
- 5 Look at the Encoded ID column of the Personnel Transactions section. This is the card's Encoded ID.

Magnetic Stripe Card

Magnetic stripe (also called mag stripe) cards are shipped with a list of their Stamped and Encoded ID numbers. Sometimes these numbers are identical and sometimes there is an offset value. An offset value is a number that needs to be added to the Stamped ID number to get the Encoded ID number. Example: A card has an offset value of 1000 and the Stamped ID is 2546. The Encoded ID number is 3546.

If there is no Stamped ID, or if the offset value isn't known, then the Activity Monitor can be used to find the encoded ID.

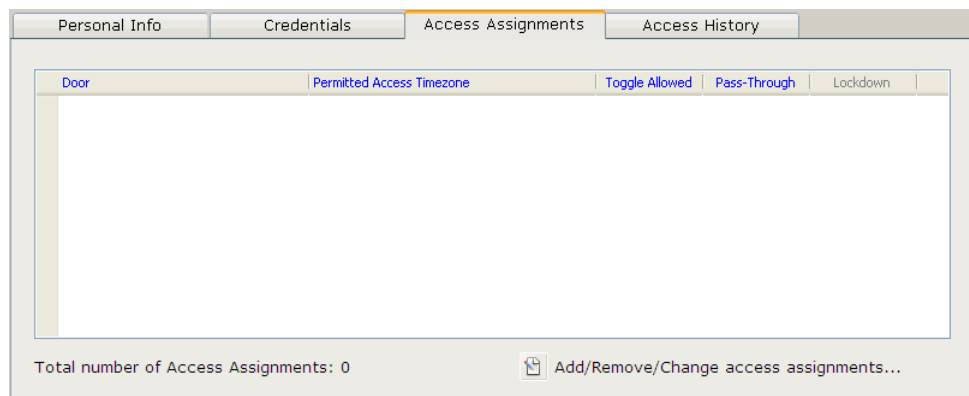
- 1 Click on the **Activity** button on the left of the main screen. The Activity Monitor window will open.
- 2 Swipe the magnetic stripe card to a magnetic stripe reader that is connected to **bright blue**.
- 3 Wait for the activity monitor to refresh, or click on the **Refresh** button.
- 4 An Access Denied transaction will be displayed on Personnel Transactions section of the Activity Monitor.



- 5 Look at the Encoded ID column of the Personnel Transactions section. This is the card's Encoded ID.

Access Assignments

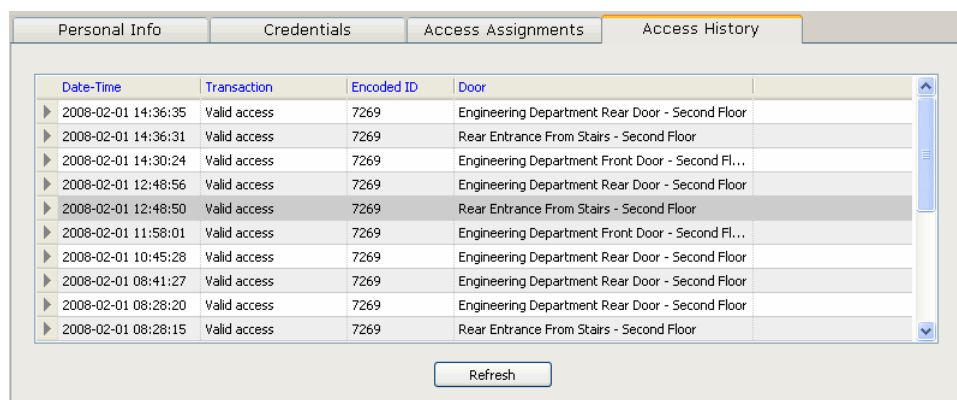
The Access Assignments tab displays a person's access assignments. In addition, this screen provides details on the availability of Toggle, Pass-Through and Lockdown functions.



- **Door** - Provides the name of the door(s) that a person has access to.
- **Permitted Access Timezone** - Details the time zone(s) during which a person is permitted access.
- **Toggle Allowed** - Shows whether a person has the toggle function enabled for the door.
- **Pass-Through** - Shows whether a person has the pass-through function enabled for the door.
- **Lockdown** - Shows whether a person has the lockdown function enabled for a door.
- **Add/Remove/Change access assignments** - Click this button to edit the person's access assignments. The Access Assignment Edit window will open. See the Access Assignment chapter for details.

Access History

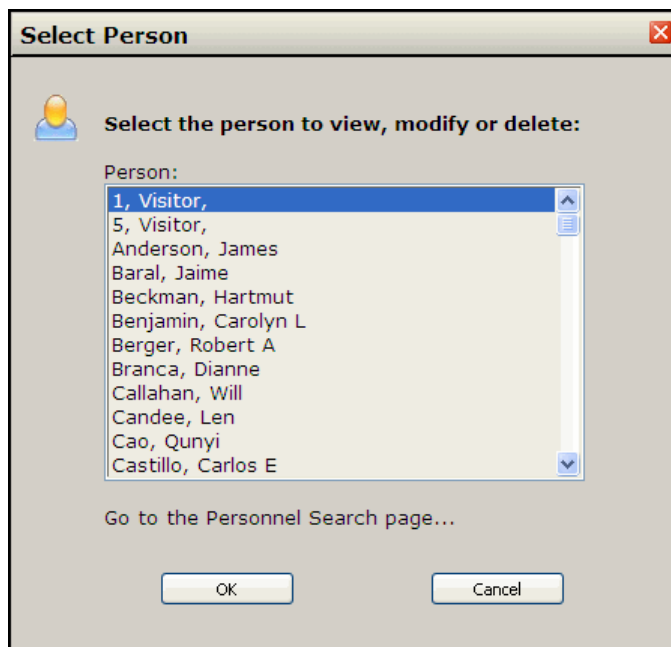
The Access History tab displays the 20 most recent transactions pertaining to the selected person. The Access History tab will only appear after a person has been assigned a credential.



- **Date-Time** - Displays the date and time of the event.
- **Transaction** - Specifies the type of transaction that took place.
- **Encoded ID** - Displays the Encoded ID of the person.
- **Door** - Specifies the door at which the transaction occurred.
- **Refresh** - Displays the most current history of events.

View, modify or delete personnel record.

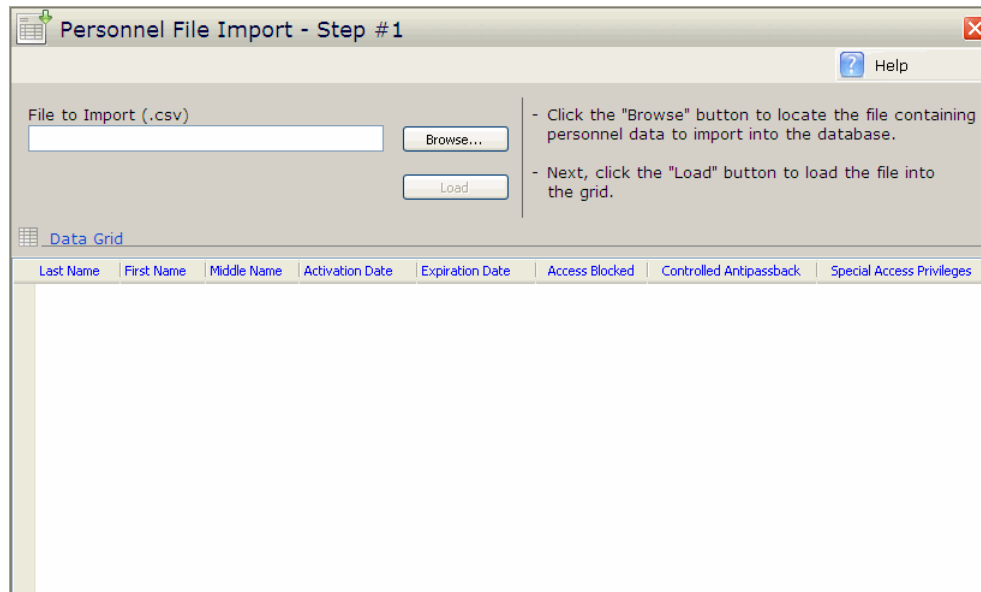
The **View, modify or delete personnel record** button allows you to select a specific personnel record to view, modify or delete. Clicking the **View, modify or delete personnel record button** opens the Select Person pop-up window.



- **Person** - Shows a list of all personnel records in the system. Click on the person to be modified.
- **Go to the Personnel Search page** - Opens the Personnel Search window. See the section on Searching for a Specific Record for details.
- **Ok** - Opens the Personnel Management window with the selected person's record.
- **Cancel** - Closes the Select Person pop-up window.

Import personnel data

Clicking this button opens the **Personnel File Import** window. This window is used to import personnel files that are in .csv format into the system.



- **File to Import (.csv)** - Shows the selected file path.
- **Browse** - Click this button to select a file to import.
- **Load** - Once a file has been selected, click this button to load the file.
- **Data Grid** - Displays the values of the imported file. Columns can be resized and the scroll bar at the bottom can be used to see all columns.

Format requirements for imported .csv files

Imported files need to be in the following format:

LN,FN,MN,ACT,EXP,BLK,SA,AP,U1,U2,U3,U4,U5,U6,SID,EID,IC,PN

- LN - last name. Enter person's last name.
- FN - first name. Enter person's first name.
- MN - middle name. Enter person's middle name.
- ACT - activation date. Date should be in format yyyy-mm-dd HH:MM:SS where yyyy is year, mm is month, dd is day, HH is hour, MM is minute, SS is second.
- EXP - expiration date. Date should be in format yyyy-mm-dd HH:MM:SS where yyyy is year, mm is month, dd is day, HH is hour, MM is minute, SS is second.
- BLK - access blocked. This will be a 0 or a 1. 0 for no blocked access, 1 for access blocked.
- SA - special access. This will be a 0 or a 1. 0 for no special access. 1 for special access.
- AP - controlled antipassback. This will be a 0 or a 1. 0 for disabled controlled antipassback. 1 for enabled controlled antipassback.
- U1 - user defined field 1. Enter information for UDF 1.
- U2 - user defined field 2. Enter information for UDF 2.
- U3 - user defined field 3. Enter information for UDF 3.
- U4 - user defined field 4. Enter information for UDF 4.
- U5 - user defined field 5. Enter information for UDF 5.
- U6 - user defined field 6. Enter information for UDF 6.
- SID - stamped id. Enter the stamped id number. 19 digit maximum, leading zeros will be dropped.
- EID - encoded id. Enter the encoded id number. 9 digit maximum, leading zeros will be dropped.
- IC - issue code. Enter the issue code.
- PN – pin number. Enter the PIN Number. 4 digit maximum, leading zeros will be dropped.

Not all fields need to be entered. The minimum is the last and first names. Any field that does not have information needs to be left blank and separated with a comma.

Data can be surrounded by "", this does not affect the formatting. Example: Doe,John is the same as "Doe","John".

If activation date or expiration date are not in the correct format or are missing from the file, the fields are set to the following defaults:

- activation date: current date, such as "2008-02-04 18:36:45"
- expiration date: "2199-12-31 23:59:59"

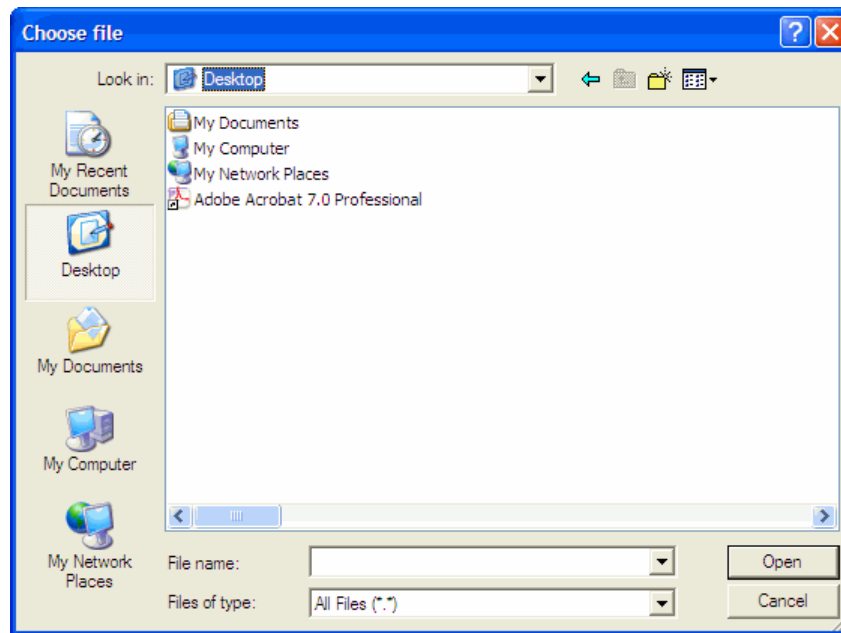
If access blocked, special access, or controlled antipassback are not in the correct format or are missing from the file, the fields are set to the following defaults:

- access blocked: 0 - person is not blocked
- special access: 0 - person does not require special access privileges
- controlled antipassback: 1 - person has controlled anti-passback enabled

Stamped ID, Encoded ID, and PIN number all have maximum allowances and will drop any leading zeros. So an entered value of "000555" would be entered into the system as "555".

- Stamped ID (SID) - 19 digits maximum.
- Encoded ID (EID) - 9 digits maximum.

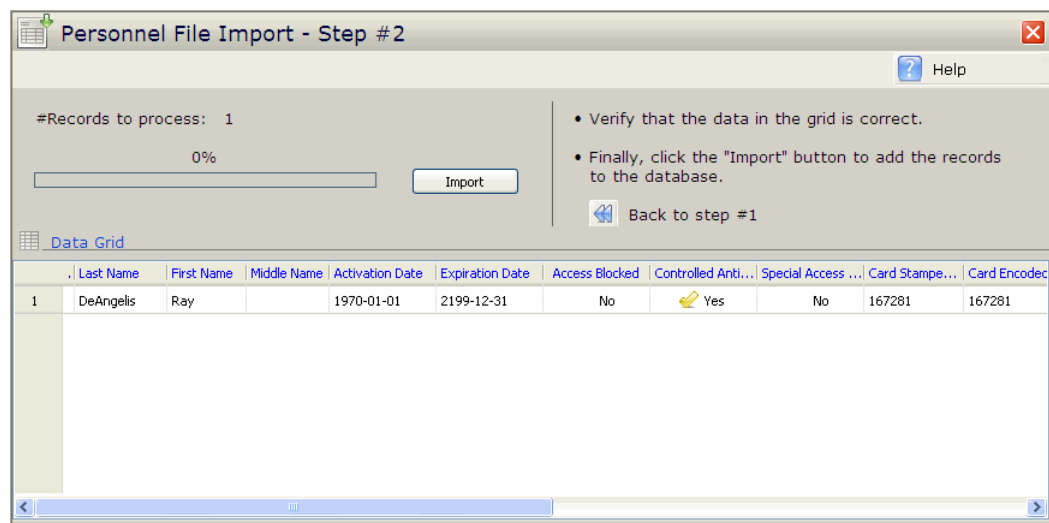
- 3 Click on the **Browse** button. The Choose file pop-up window will open.



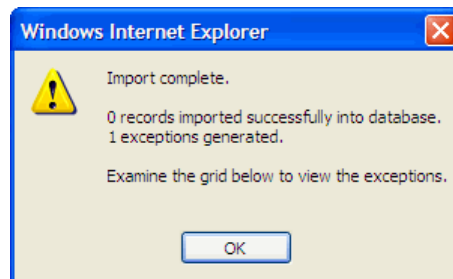
- 4 Find and select the .csv file to be imported.
- 5 Click on the **Open** button. The Choose file pop-up window will close. The File to Import field will now show the selected file path.



- 6 Click on the **Load** button. The Upload File pop-up window will open.
- 7 The Upload File pop-up will close when the file is uploaded. The Personnel File Import - Step #2 window will open displaying the imported fields.



- 8 Verify that the data has uploaded correctly. Click on the **Import** button. The Import complete pop-up window will open.



- 9 Click on **OK**. The Import complete pop-up will close.

To import another file click on the Start over button and repeat steps 3 through 9 above.

Searching for a Specific Record

The Personnel Search window is used to find a specific person(s) in the system. It is accessed from various places from Personnel Management to Access Assignments. This search engine is used by all areas of **bright blue** when a specific person, or specific groups of people, need to be found.

Last Name	First Name	Middle Name	Activation Date	Expiration Date	Access Blocked	Controlled Antipassback	Special Access Privileges
1, Visitor			2007-10-10	2199-12-31	Yes	Yes	No
5, Visitor			2007-10-10	2199-12-31	Yes	Yes	No
Anderson	James		2007-10-10	2199-12-31	Yes	Yes	No
Baral	Jaime		2007-10-10	2199-12-31	Yes	Yes	No
Beckman	Hartmut		2007-10-10	2199-12-31	Yes	Yes	No
Benjamin	Carolyn	L	2007-10-11	2199-12-31	Yes	Yes	No

The buttons along the top of the page:

- **Execute Search** - Click this to run the search. If no parameters have been entered in the search field then this button will generate a list of all personnel in the system.
- **Continue** - Click this button to move on to the next page after personnel have been selected.
- **Help** - Click for help with this section.

The search engine is broken up into three different drop down boxes that are used to define the search parameters:

- **Find all person records by**
- **With the following search term**
- **With the following rule.**

To Search for a Specific Person

- 1 Click the **Find Person** button on the Personnel Management window. The Personnel Search window will open.
- 2 Using the **Find all person records by** drop down, define which field in Personnel will be searched.
- 3 Enter your search criteria into the **With the following search term** field.
- 4 Using the **With the following rule** drop down box, define any additional rules for the search.
- 5 Click **Execute Search**.

Example: You wish to search for someone but you only know the first three letters of their last name. You would select **Last Name** from the **Find all person records by** drop down box. Then you would type in the three letters you know in the **With the following search term** field. After that has been entered you would select **Starts with** from the **With the following rule** drop down box. Then press **Execute Search** to get your results. The bottom pane of the window will now display your search results.

Details on Search Terms

Both **With the following search term** and **With the following rule** drop down boxes have selections based on the **Find all person records by** drop down. Various search options are shown below.

Find all person records by	With the following search term	With the following rule
Access Assignment (Door)	List of Doors in the System Range List of Doors in the System	Exact match In the range Does not match Is not in the range
Access Blocked Controlled Antipassback Special Access Privileges	Disabled Enabled	Exact match Does not match

Activation Date Expiration Date	Date Selection Range Date Selection	Exact match In the range Does not match Is not in the range
Credential Stamped ID Credential Encoded ID First Name Last Name User Defined Field Number 1 - 6	Open Search Field Range Open Search Field	Contains End with Exact match In the range Starts with Does not contain Does not end with Does not match Is not in the range Does not start with

Find all person records by:

- **Access Assignment (Door)** - Search by access assignments.
- **Access Blocked** - Search by blocked status.
- **Activation Date** - Search by activation date.
- **Controlled Antipassback** - Search by antipassback status.
- **Credential Stamped ID** - Search by stamped ID number.
- **Credential Encoded ID** - Search by encoded ID number.
- **Expiration Date** - Search by Expiration date.
- **First Name** - Search by first name.
- **Last Name** - Search by last name.
- **Special Access Privileges** - Search by special access status.
- **User Defined Field Number 1 - 6** - Search by data in any of the six user defined fields.

With the following search term:

- **List of Doors in the System** - Specify which door to search by.
- **Disabled** - Specify if the search criteria is disabled.
- **Enabled** - Specify if the search criteria is enabled.

- **Date Selection** - Specify the beginning and ending dates of the search.
- **Open Search Field** - Specify what you're searching for.
- **Range** - Used when looking for personnel within a range of search terms.

With the following rule:

- **Contains** - Has the search term in its name/title.
- **End with** - Ends with the search term.
- **Exact match** - Exact match with the search term.
- **In the range** - Is in the range of the two different search terms.
- **Starts with** - Starts with the search term.
- **Does not contain** - Desired result will not contain the search term.
- **Does not end with** - Desired result will not end with the search term.
- **Does not match** - Desired result will not match the search term.
- **Is not in the range** - Desired result is not in the search range.
- **Does not start with** - Desired result does not start with the search term.

Advanced Search

Advanced Search option is activated by clicking on the More Search Terms button in the Personnel Search window. Advanced search adds another layer of criteria to the search.

The screenshot shows the 'Personnel Search' window. At the top, there are buttons for 'Execute Search', 'Continue...', and 'Help'. Below these, the search criteria are defined in two rows. The first row has 'Find all person records by...' set to 'Last Name', 'With the following search term...' (empty), and 'With the following rule...' set to 'Starts with'. The second row has 'Additionally...' set to 'First Name', 'With the following search term...' (empty), and 'With the following rule...' set to 'Starts with'. There are 'Range' input fields for each search term and a 'Less Search Terms' button. The logical operator is set to 'AND'. Below the criteria, there is a 'Search Results' section with a table of results.

	Last Name	First Name	Middle Name	Activation Date	Expiration Date	Access Blocked	Controlled Antipassback	Special Access Privileges
▶	1, Visitor			2007-10-10	2199-12-31	Yes	Yes	No
▶	5, Visitor			2007-10-10	2199-12-31	Yes	Yes	No
▶	Anderson	James		2007-10-10	2199-12-31	Yes	Yes	No
▶	Baral	Jaime		2007-10-10	2199-12-31	Yes	Yes	No

To use Advanced Search:

- 1 Click on the **More Search Terms** button.
- 2 Using the **Find all person records by** drop down, select which field in Personnel will be searched.

- 3 Enter the search criteria into the upper **With the following search term** field.
- 4 Define additional rules using the upper **With the following rule** drop down menu..
- 5 Click either the **AND** or **OR** box, putting a check into it.
 - **AND** - If the AND checkbox is selected the results of the search must meet the criteria specified in both fields. A record will only be displayed if it meets both of the criteria specified.
 - **OR** - If the OR checkbox is selected the results of the search will display records that contain terms specified in either of the fields.

Note: One of these options must be selected to use the Advanced Search option.

- 6 Using the lower **Find all person records by** drop down, define which field in Personnel will be searched.
- 7 Enter the search criteria into the lower **With the following search term** field.
- 8 Using the lower **With the following rule** drop down menu, define the additional rule for the search.
- 9 Click on **Execute Search**.

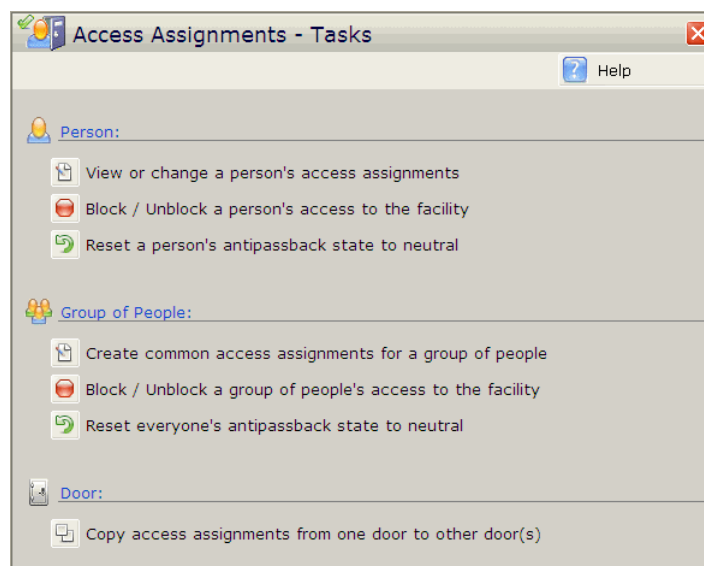
The results will display in the lower pane of the window.

Access Assignments

CHAPTER 6

Introduction

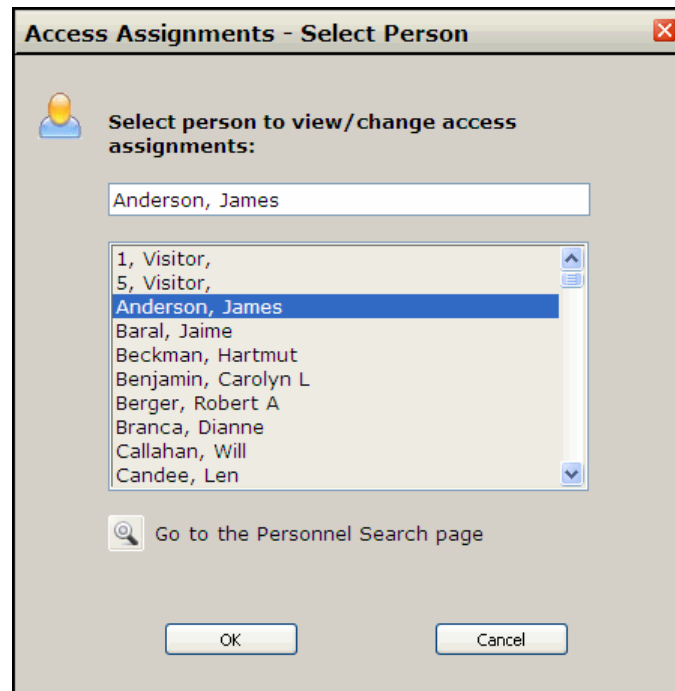
The Access Assignments - Tasks window is used to define which personnel have access to which doors. Access can be assigned per person or per group of people. This screen can also be used to block all access for an individual or for a group. The Access Assignments - Tasks window can be accessed by clicking on the Access Assignments button on the left side of the main screen. This section is accessible by users with Administrator or Manager security levels.



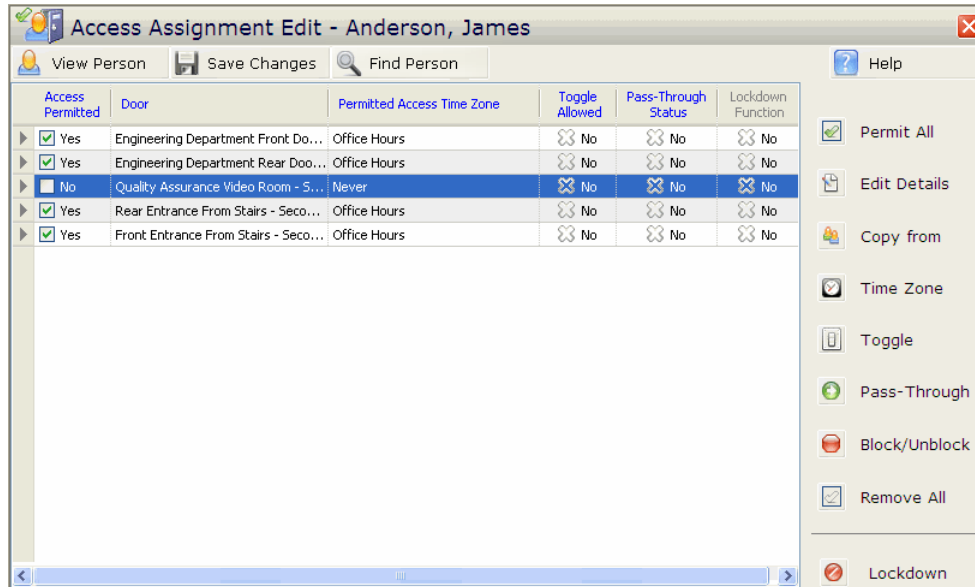
Note: If there are no doors defined in the system the a warning pop-up window will open.

View or change a person's access assignments

This section allows the user to view a specific person's access assignments and make modifications if necessary. Clicking on this link will bring up a pop-up that allows the user to select a specific person's record.



Once a person is selected, the **Access Assignments - Edit** screen will open, allowing the user to change the access assignments for that person.



There are three buttons along the top of the page:

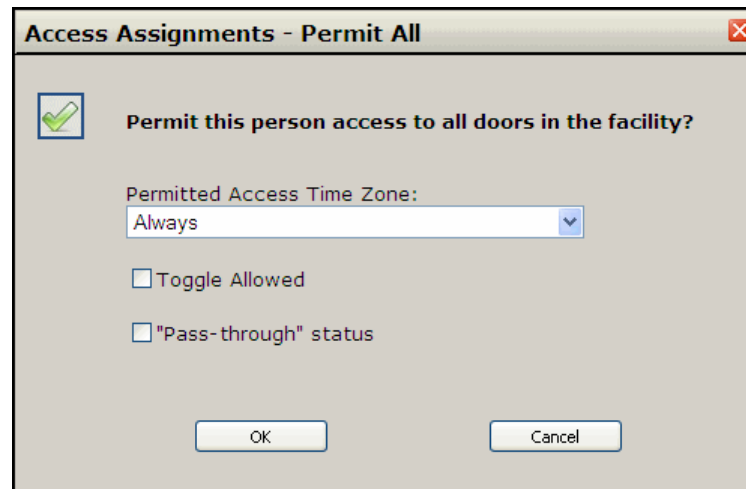
- **View Person** - Brings the user to the Personnel window.
- **Save Changes** - Saves any changes made to the access assignments.
- **Find Person** - Opens the Access Assignment - Find Person pop-up window. From the pop-up a new person can be selected.
- **Help** - Opens the Help file for this page.

The Access Assignments - Edit window has a table showing a person's access assignments. The table has six columns:

- **Access Permitted** - Shows whether the selected person has access or not.
- **Door** - Shows which door is being specified.
- **Permitted Access Time Zone** - Specifies which time zones this person has access to this door.
- **Toggle Allowed** - Specifies whether this user has toggle allowed at this door.
- **Pass-Through Status** - Specifies whether this user has the Pass-Through feature enabled at this door.
- **Lockdown Function** - Specifies if this user can use their credential to enable the Lockdown feature at this door.

Permit All

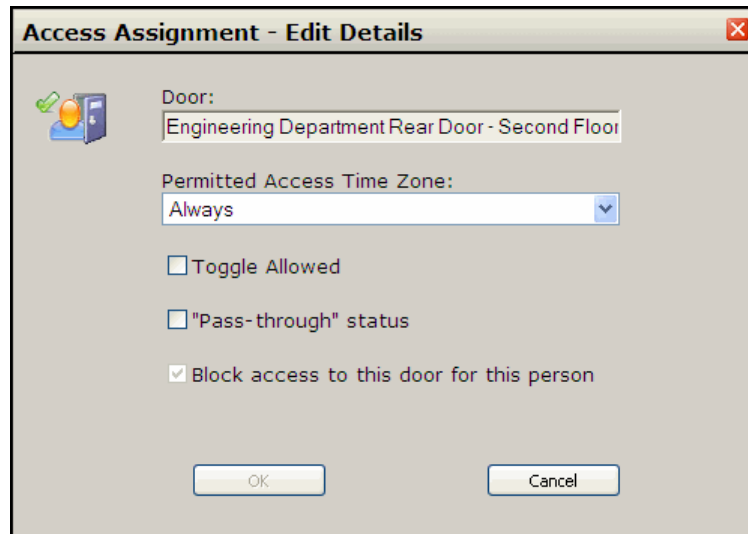
Clicking on this button opens the **Access Assignments - Permit All** pop-up window. This window allows the user to grant access to all the doors in the system.



- **Permitted Access Time Zone** - Select a timezone to apply for access to all doors.
- **Toggle Allowed** - If this box is checked, the person will be able to toggle a door open or closed by swiping their card twice within a certain time span. The door will remain in this state until a person, with the toggle option enabled, presents their credential in the same manner.
- **Pass-through status** - If this box is checked, the person will be granted access to doors even if they are in the Lockdown state.
- **OK** - Grants access to all doors with the criteria specified and closes the pop-up window.
- **Cancel** - Click this to exit out of the window without saving any changes.

Edit Details

Clicking on this button after selecting a door from the table will open the **Access Assignment - Edit** pop-up window. This window allows the user to edit access assignments for the selected door.

The image shows a Windows-style dialog box titled "Access Assignment - Edit Details". On the left is an icon of a door with a green checkmark. To the right of the icon, the "Door:" label is followed by a text box containing "Engineering Department Rear Door - Second Floor". Below this, the "Permitted Access Time Zone:" label is followed by a dropdown menu showing "Always". There are three checkboxes: "Toggle Allowed" (unchecked), "\"Pass-through\" status" (unchecked), and "Block access to this door for this person" (checked). At the bottom are "OK" and "Cancel" buttons.

Access Assignment - Edit Details

Door:
Engineering Department Rear Door - Second Floor

Permitted Access Time Zone:
Always

☐ Toggle Allowed

☐ "Pass-through" status

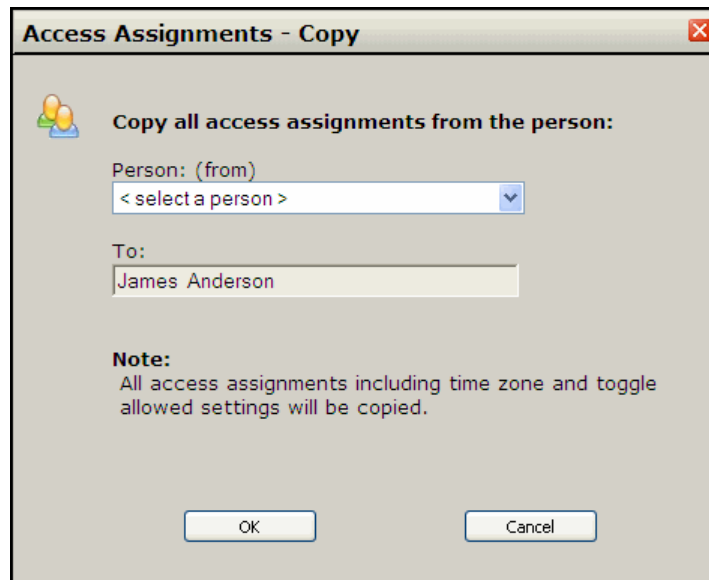
☒ Block access to this door for this person

OK Cancel

- **Door** - Shows which door is currently selected.
- **Permitted Access Time Zone** - Select a timezone to apply for access to this door.
- **Toggle Allowed** - If this box is checked, the person will be able to toggle this door open or closed by swiping their card twice within a certain time span. The door will remain in this state until a person, with the toggle option enabled, presents their credential in the same manner.
- **Pass-through status** - If this box is checked, the person will be granted access to doors even if they are in the Lockdown state.
- **Block access to this door for this person** - checking this box will disable access to this door for this person.

Copy from

Clicking on this button opens the **Access Assignments - Copy** pop-up window. This window allows the user to select another person in the database and add their access assignments to the selected person's record.

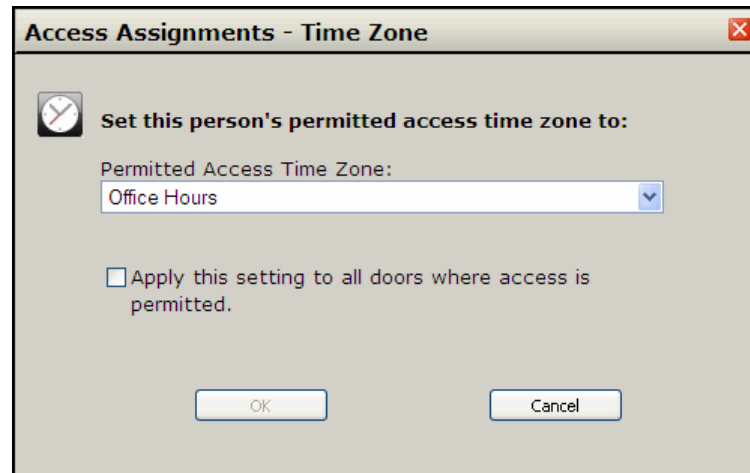


- **Person: (from)** - Select the person whose access assignments will be copied.
- **To:** - Shows which person is currently selected and who will receive the copied access assignment.
- **OK** - Copies the access assignments and closes the pop-up window.
- **Cancel** - Closes the pop-up window without saving any changes.

Note: All access assignments settings, including time zone and toggle allowed, will be copied.

Time Zone

Clicking on this button opens the **Access Assignments - Timezone** pop-up window. This window allows the user to select a time zone and apply it to all of the selected person's access assignments.

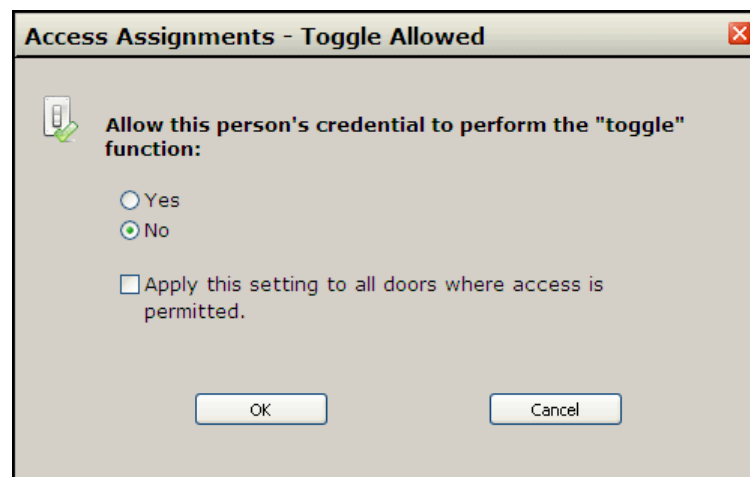
A screenshot of a software dialog box titled "Access Assignments - Time Zone". The dialog has a light gray background and a standard window border with a close button (X) in the top right corner. Inside the dialog, there is a clock icon to the left of the text "Set this person's permitted access time zone to:". Below this text is a dropdown menu labeled "Permitted Access Time Zone:" with "Office Hours" selected. Underneath the dropdown is a checkbox that is currently unchecked, followed by the text "Apply this setting to all doors where access is permitted.". At the bottom of the dialog are two buttons: "OK" and "Cancel".

- **Permitted Access Time Zone** - Select a timezone to apply.
- **Apply this setting to all doors where access is permitted** - If this box is checked then the selected Time Zone will be applied to every door for which the person has access.
- **OK** - Applies the selected time zone and closes the pop-up window.
- **Cancel** - Closes the pop-up window without saving any changes.

Note: The selected time zone will be applied to all access assignments for this person. To modify specific access assignments, select access and click on the details link.

Toggle

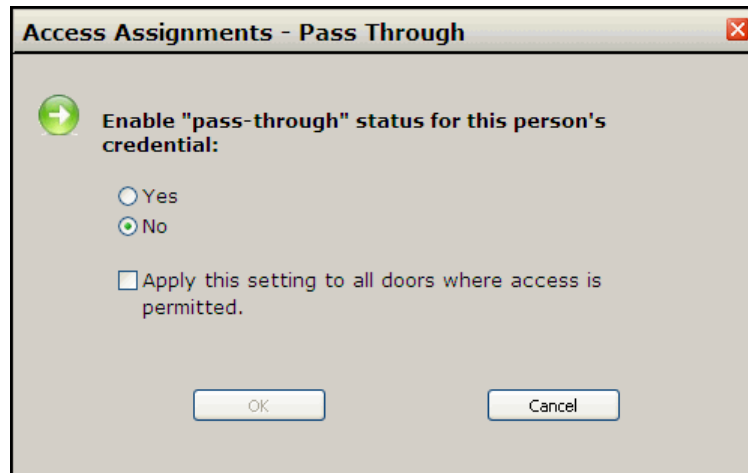
Clicking on this button opens the **Access Assignments - Toggle Allowed** pop-up window. This window allows the user to enable the toggle function for all of a person's access assignments.



- **Allow this person's credential to perform the "toggle" function:**
 - **Yes** - Select this to grant the toggle function for this person.
 - **No** - Select this to remove the toggle function for this person.
- **Apply this setting to all doors where access is permitted** - If checked, the toggle function will be affected for all doors to which this person has access. If unchecked, only the selected door will be affected.
- **OK** - Enables toggle and closes the pop-up window.
- **Cancel** - Closes the pop-up window without saving any changes.

Pass-Through

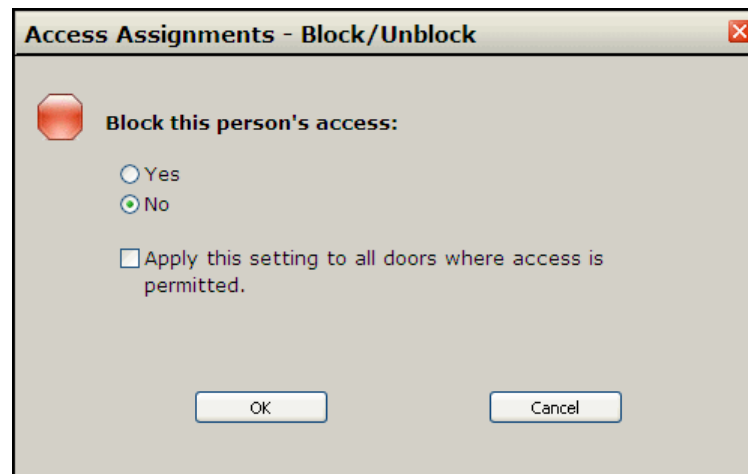
Clicking on this button opens the **Access Assignments - Pass Through** pop-up window. This window allows the user to enable the pass-through function for all of a person's access assignments.



- **Enable "pass-through" status for this person's credential:**
 - **Yes** - Select this to grant the pass-through function for this person.
 - **No** - Select this to remove the pass-through function for this person.
- **Apply this setting to all doors where access is permitted** - If checked, the pass-through function will be affected for all doors to which this person has access. If unchecked, only the selected door will be affected.
- **OK** - Enables pass-through and closes the pop-up window.
- **Cancel** - Closes the pop-up window without saving any changes.

Block/Unblock

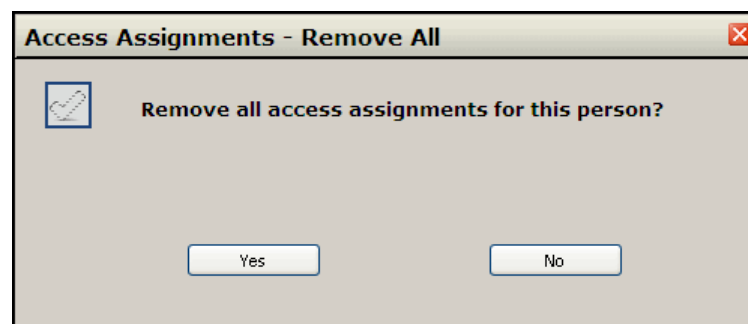
Clicking on this button opens the **Access Assignments - Block/Unblock** pop-up window. This window allows the user to block (if unblocked) or block (if blocked) all access to all doors in the system for the selected person.



- **Block this person's access:**
 - **Yes** - Select this to block access for this person.
 - **No** - Select this to unblock access for this person.
- **Apply this setting to all doors where access is permitted** - If checked, the block status will be affected for all doors to which this person has access. If unchecked, only the selected door will be affected.
- **OK** - Executes the block or unblock for the specified person and closes the pop-up window.
- **Cancel** - Closes the pop-up window without changing the block/unblock status of the specified person.

Remove All

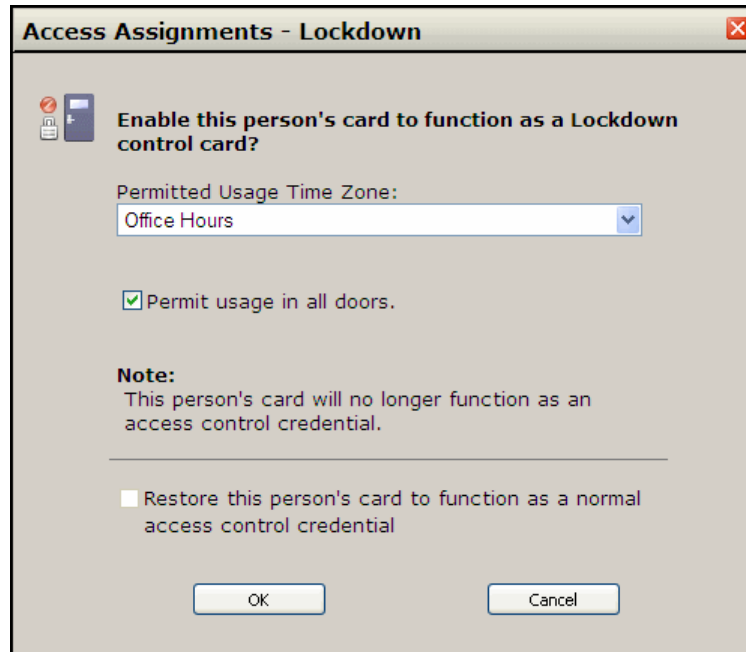
Clicking on this button opens the **Access Assignments - Remove All** pop-up window. This window allows the user to remove all access from the selected person.



- **Yes** - Removes all access from the selected person and closes the pop-up window.
- **No** - Closes the pop-up window without removing access.

Lockdown

Clicking on this button opens the **Access Assignments - Lockdown** pop-up window. This window allows the user to define a credential as a Lockdown control card. A Lockdown control card can put a lock into the Lockdown state by swiping it at a reader.

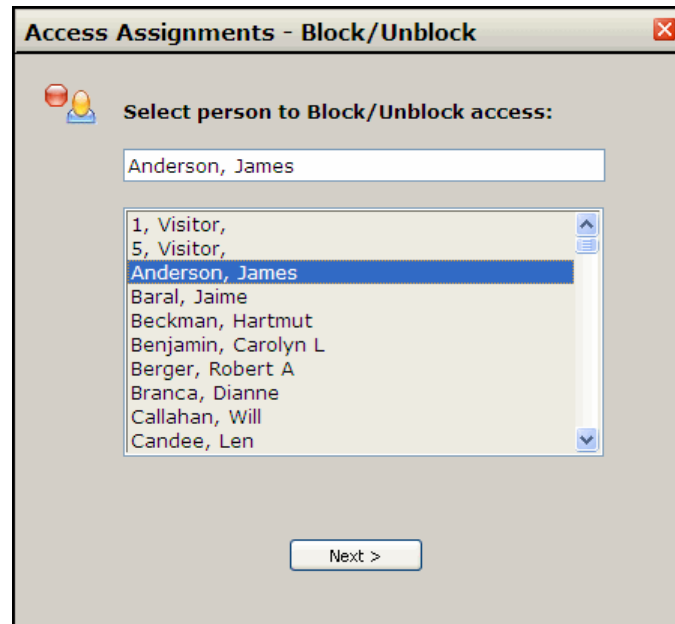
The image shows a software dialog box titled "Access Assignments - Lockdown". It has a standard Windows-style title bar with a close button (X) in the top right corner. The main content area has a light gray background. At the top left of the content area is an icon of a card with a red lock symbol. To its right is the text "Enable this person's card to function as a Lockdown control card?". Below this is a label "Permitted Usage Time Zone:" followed by a dropdown menu currently showing "Office Hours". Underneath the dropdown is a checked checkbox with the text "Permit usage in all doors.". A horizontal line separates this section from a "Note:" section. The note text reads: "This person's card will no longer function as an access control credential.". Below the note is an unchecked checkbox with the text "Restore this person's card to function as a normal access control credential". At the bottom of the dialog are two buttons: "OK" and "Cancel".

- **Permitted Usage Time Zone** - Defines during which timezone the credential can be used as a Lockdown control card.
- **Permit usage in all doors** - Check this box to make this credential a Lockdown control card for every lock in the system.
- **Restore this person's card to function as a normal access control credential** - Check this box to remove the Lockdown feature from this credential. This will remove the feature from all locks for this user. When the lockdown feature is removed all access to every door will also be removed.

Note: This person's card will no longer function as an access control credential at the doors in which the lockdown feature is enabled.

Block / Unblock a person's access to the facility

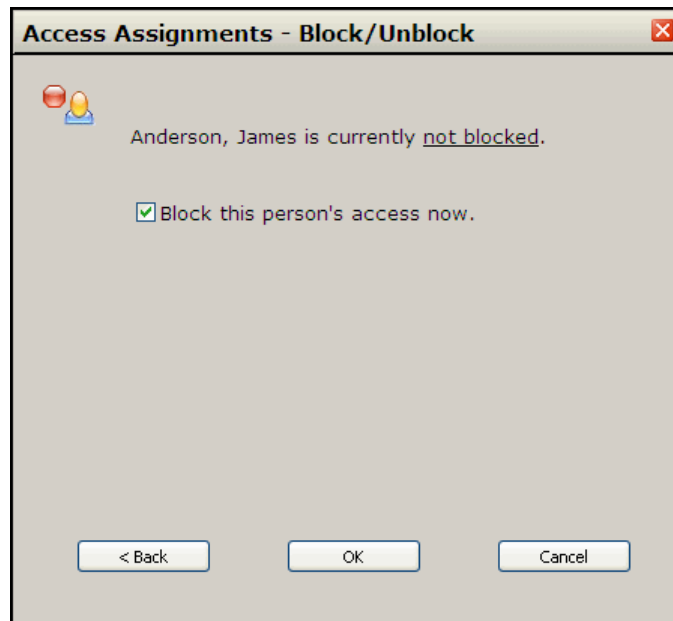
This button allows the user to block or unblock a person's access to the entire facility. Clicking on this button opens the **Access Assignments – Block/Unblock** pop-up window.



- **Person:** - This lists every person that is in the system. Select the person that will be blocked/unblocked from the list.
- **Next>** - After the person that is being blocked/unblocked has been selected, click this button to move to the next step.

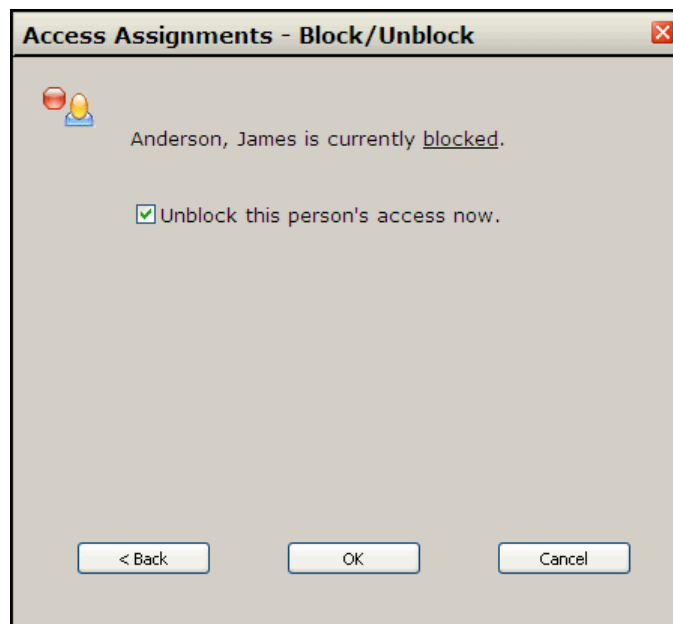
To exit out of this window without making any changes, click the X in the upper right corner of the pop-up window. Once the person has been selected, click the **Next>>** button. This will open the next window, which will display the current blocked/unblocked status of that individual.

If they are currently unblocked, the window will look like this:



- **Block this person's access now.** - This box will be checked by default.
- **<Back** - Click this button to go back to the previous window without making any changes to the block status.
- **Cancel** - Click this button to close the pop-up window without making any changes to the block status. This will open the main Access Assignments window.
- **OK** - Click this button to block this person's access. The Task completed window will open. Click **Done** to return to the Access Assignments main window.

If they are currently blocked, the window will look like this:



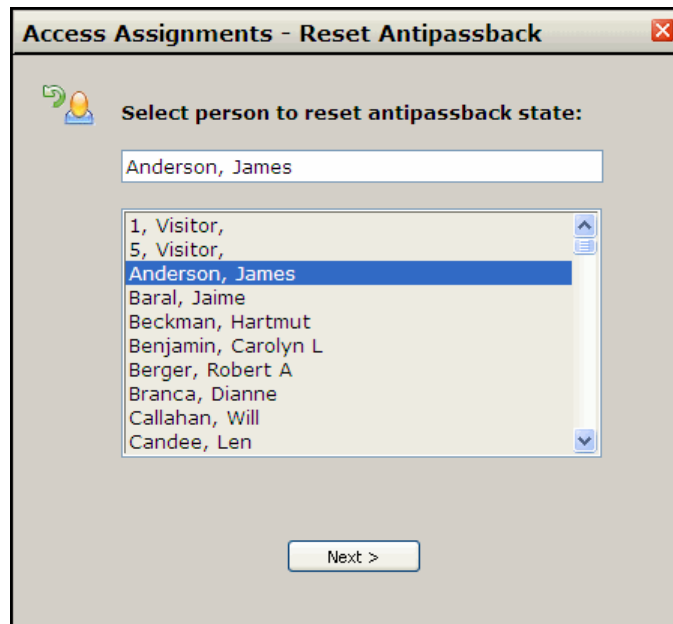
- **Unblock this person's access now.** - This box will be checked by default.
- **<Back** - Click this button to go back to the previous window without making any changes to the block status.
- **Cancel** - Click this button to close the pop-up window without making any changes to the block status. This will open the main Access Assignments window.
- **OK** - Click this button to unblock this person's access. The Task completed window will open. Click **Done** to return to the Access Assignments main window.

Reset a person's antipassback state to neutral

This button resets a person's antipassback state to neutral. By using this feature, a person with the antipassback feature enabled can be granted access to an entry reader even if they have not exited via an exit reader nor has the specified amount of time passed.

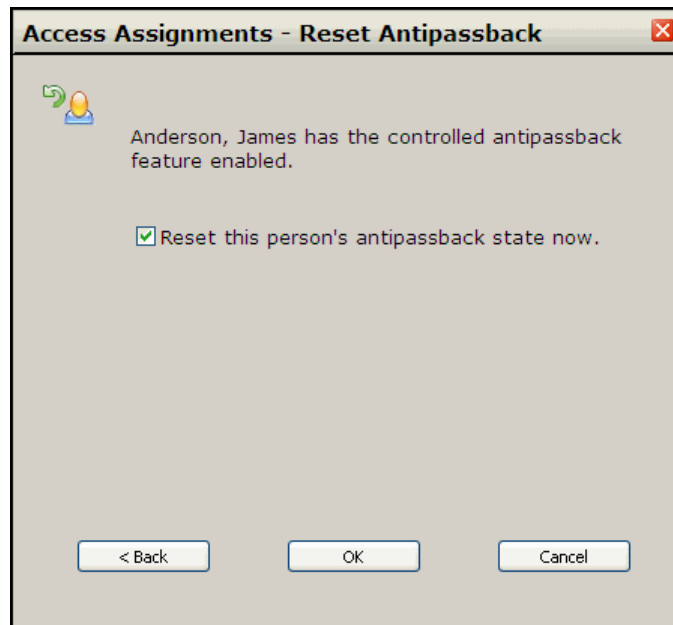
Example: Your company has a parking garage with a secured entrance and exit. There is an entry reader on the exterior side and an exit reader on the interior side of the gate. Due to maintenance the gate is being held in the up position. During the time that the gate is in the up position many employees come to work and park their cars without using their credentials at the entry reader. At the end of the day the gate has been fixed and is secured. When the employees attempt to leave, the gate will not open for them as the exit reader will not allow an exit to a credential that has not been through an entry reader. For these employees to be able to exit the parking garage they will need to have their antipassback state reset to neutral at which point the exit reader will allow them to leave.

Clicking on this button will bring up the **Access Assignments - Reset Antipassback** pop-up window.



- **Person:** - This lists every person in the system. Select the person whose Antipassback state will be reset.
- **Next>** - After the person has been selected, click this button to move to the next step.

To exit out of this window without making any changes, click the X in the upper right corner of the pop-up window.



- **Reset this person's antipassback state now.** - This box will be checked by default.
- **<Back** - Click this button to go back to the previous window without making any changes to the antipassback state.
- **Cancel** - Click this to close the pop-up window without making any changes to the antipassback state. This will open the main Access Assignments window.
- **OK** - Click this button to reset this person's antipassback state.

Personnel Search - Group Access Assignments

Find all person records by...

 With the following search term...


 With the following rule...



Range

[_ Search Results](#)


Select	Last Name	First Name	Middle Name	Activation Date	Expiration Date	Access Blocked	Controlled Antipassback	Special Access Privileges


Once the list is generated, click on the **Select** column for each person to be added to the group. Once all personnel for the group have been selected click **Continue** at the top of the screen. The **Group Access Assignments** page will open.



Group Access Assignments - (5 People)


 View Group
  Save Changes


Access Permitted	Door	Permitted Access Time Zone	Toggle Allowed	Pass-Through Status	Lockdown Function
<input type="checkbox"/> No	Engineering Department Front Door	Never	No	No	No
<input checked="" type="checkbox"/> Yes	Engineering Department Rear Door	Always	No	No	No
<input type="checkbox"/> No	Quality Assurance Video Room - Security	Never	No	No	No
<input checked="" type="checkbox"/> Yes	Rear Entrance From Stairs - Security	Always	No	No	No
<input type="checkbox"/> No	Front Entrance From Stairs - Security	Never	No	No	No


 Help


 Permit All


 Edit Details


 Copy from


 Time Zone

 Toggle

 Pass-Through

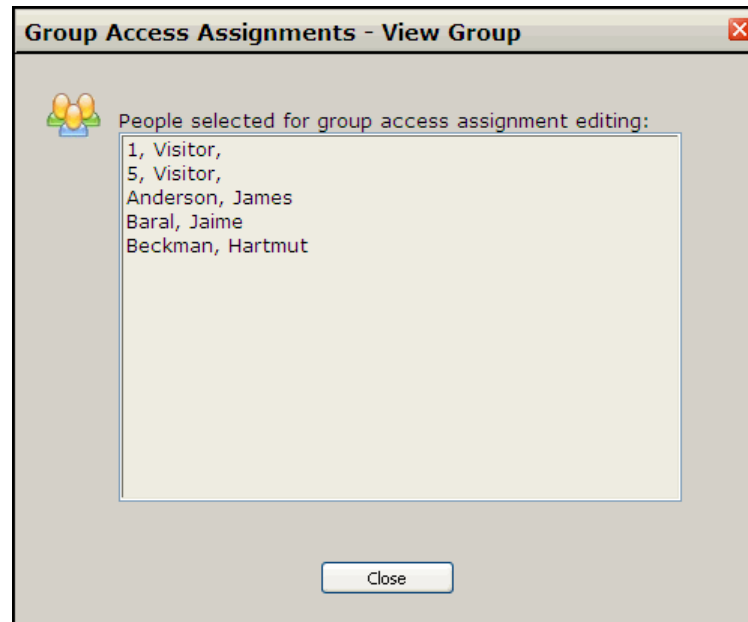
 Block/Unblock

 Remove All

 Lockdown

There are three buttons along the top of the page.

- **View Group** - Opens the Group Access Assignments - View Group pop-up window.



- **Close** - Closes the pop-up window.
- **Save Changes** - Saves any changes made to the access assignments.
- **Help** - Opens the Help file for this page.

The Group Access Assignments window has a table showing a group's access assignments. The table is broken up into six columns.

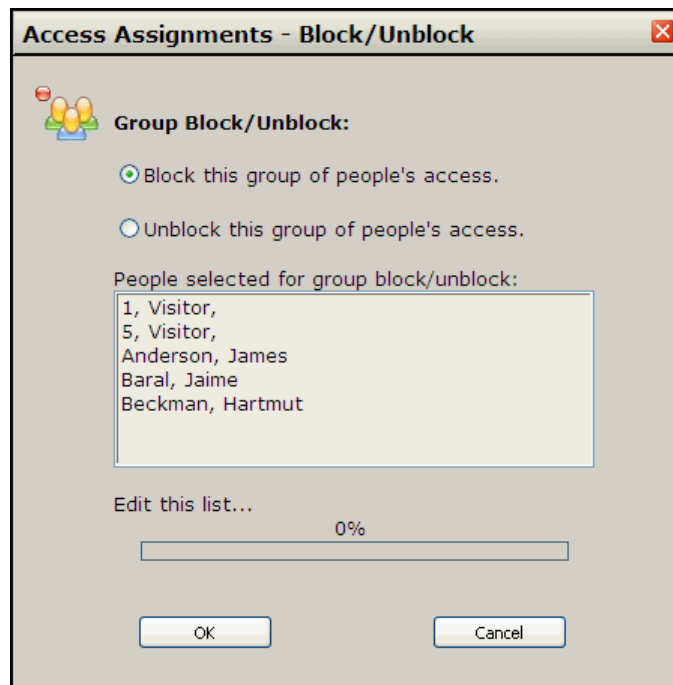
- **Access Permitted** - Shows whether the selected group has access or not.
- **Door** - Shows which door is being specified.
- **Permitted Access Time Zone** - Specifies which time zones this group has access to this door.
- **Toggle Allowed** - Specifies whether this group has toggle allowed at this door.
- **Pass-Through Status** - Specifies whether this group has the Pass-Through feature enabled at this door.
- **Lockdown Function** - Specifies if this group can use their credential to enable the Lockdown feature at this door.

For details on the buttons on the right of the screen (Permit All, Edit Details, Copy from, etc.) see the **View or change a person's access assignments** section of this chapter.

Block / Unblock a group of people's access to the facility

Clicking this button will open the **Personnel Search - Group Access Assignments - Block/Unblock** window. From this window a group of personnel can be selected. Once defined, the group can have access blocked or unblocked in the system.

Select the desired people from the Search Results window (please see the Searching for a Specific Record section of the Personnel Chapter for details). Click on **Continue**, the **Access Assignments - Block/Unblock** pop-up window will open.

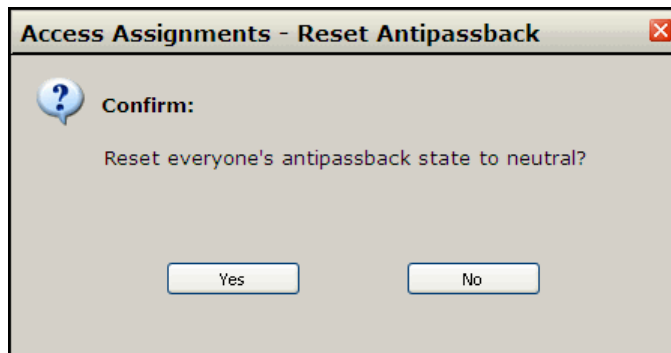


- **Block this group of people's access** - Check this box to block the selected group of people.
- **Unblock this group of people's access** - Check this box to unblock the selected group of people.
- **People selected for group block/unblock** - Will display the list of people to be blocked/unblocked.
- **Edit this list** - Click on this button to edit the block/unblock list.
- **OK** - Click this button to execute the block/unblock for the group of people. The pop-up window will close when finished.
- **Cancel** - Click this button to close the pop-up window without making any changes.

Reset everyone's antipassback state to neutral

This button resets every person's antipassback state to neutral. See the Reset a person's antipassback state to neutral section for details.

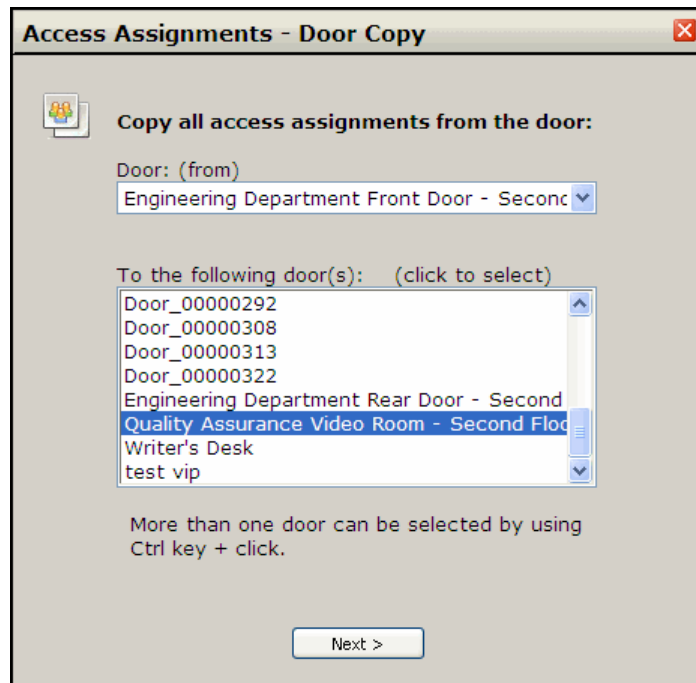
Clicking on this button will open the Reset Antipassback pop-up window.



- **Yes** - Clicking on this button resets everyone's antipassback state to neutral. A confirmation pop-up window will open.
- **No** - Clicking on this button closes the pop-up without changing antipassback state.


Copy access assignments from one door to other door(s)

Clicking this button will open the **Door Copy** pop-up window. From this window a door's access assignments can be copied over to another door or to a group of other doors.



The image shows a software dialog box titled "Access Assignments - Door Copy". It contains a section "Copy all access assignments from the door:" with a "Door: (from)" dropdown menu currently set to "Engineering Department Front Door - Second". Below this is a list box titled "To the following door(s): (click to select)" containing several door names, with "Quality Assurance Video Room - Second Floor" selected. A note at the bottom states "More than one door can be selected by using Ctrl key + click." and a "Next >" button is at the bottom right.

Access Assignments - Door Copy

 **Copy all access assignments from the door:**

Door: (from)
Engineering Department Front Door - Second

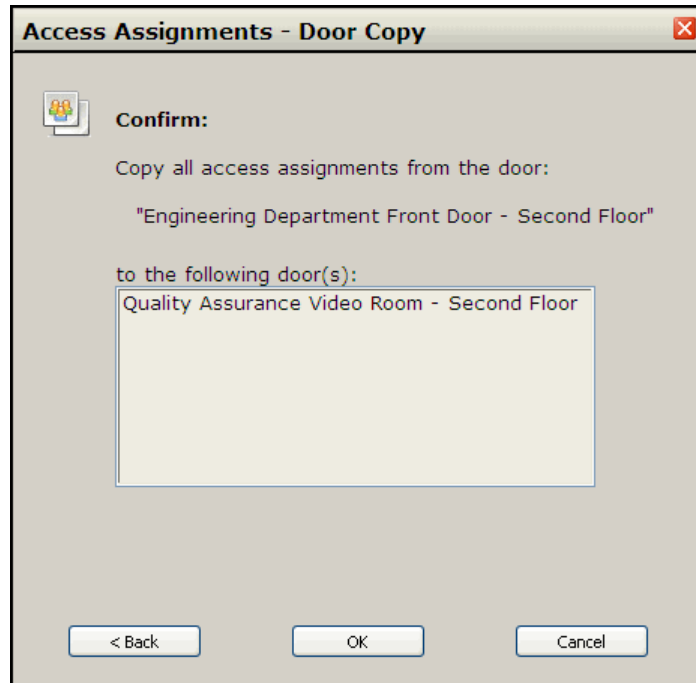
To the following door(s): (click to select)

- Door_00000292
- Door_00000308
- Door_00000313
- Door_00000322
- Engineering Department Rear Door - Second
- Quality Assurance Video Room - Second Floor**
- Writer's Desk
- test vip

More than one door can be selected by using
Ctrl key + click.

Next >

- **Door: (from)** - Select which door's access assignments will be copied using this drop down box.
- **To the following door(s)** - Select which doors to have the access assignment copied to. Multiple doors can be selected by holding down the Ctrl key while selecting doors.
- **Next>** - Click on this after the doors have been selected. A confirmation pop-up window will open.



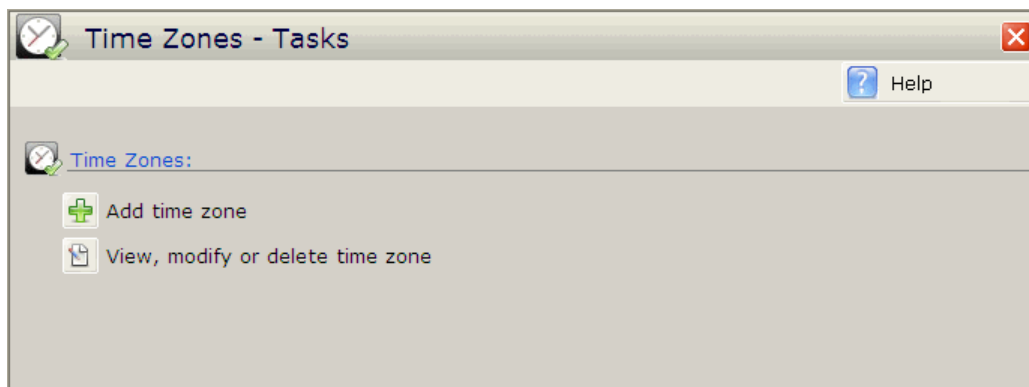
- **<Back** - Click on this button to return to the previous pop-up window.
- **OK** - Click on this button to copy the access assignments of the selected doors.
- **Cancel** - Close the pop-up window without changing access assignments.

Time Zones

CHAPTER 7

Introduction

The Time Zones - Tasks window is used to add, modify, and delete time zones. Time Zones determine when a door will be unlocked and during which times a specific person has access. The Time Zone - Tasks window can be accessed by clicking on the Time Zone button on the left side of main screen. This section is accessible by users with Administrator or Manager security levels.





Add time zones

Clicking this button from the **Time Zone - Task** window will open the **Time Zones - Edit** window. Here the user can define new time zones.


The screenshot shows the 'Time Zones - Edit' window with the following components:


- Toolbar:** New Time Zone, Save Time Zone, Delete Time Zone, Find Time Zone, and Help.
- Time Zone Name:** A text input field.
- Notes:** A text area.
- Time Zone Interval #1 (Required):**
 - Starts:** Hour (0), Min. (00), and a clock icon.
 - Ends:** Hour (0), Min. (00), and a clock icon.
 - Repeats:** Every week of each month.
 - Effective Days of the Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all unchecked).
 - Includes scheduled "Calendar Events":** Unchecked.
- Time Zone Interval #2 (Optional):**
 - Starts:** Hour (0), Min. (00), and a clock icon.
 - Ends:** Hour (0), Min. (00), and a clock icon.
 - Repeats:** Every week of each month.
 - Effective Days of the Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all unchecked).
 - Includes scheduled "Calendar Events":** Unchecked.
 - Enable:** Button.
- Time Zone Interval #3 (Optional):**
 - Starts:** Hour (0), Min. (00), and a clock icon.
 - Ends:** Hour (0), Min. (00), and a clock icon.
 - Repeats:** Every week of each month.
 - Effective Days of the Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all unchecked).
 - Includes scheduled "Calendar Events":** Unchecked.
 - Enable:** Button.
- Time Zone Interval #4 (Optional):**
 - Starts:** Hour (0), Min. (00), and a clock icon.
 - Ends:** Hour (0), Min. (00), and a clock icon.
 - Repeats:** Every week of each month.
 - Effective Days of the Week:** Sun, Mon, Tue, Wed, Thu, Fri, Sat (all unchecked).
 - Includes scheduled "Calendar Events":** Unchecked.
 - Enable:** Button.

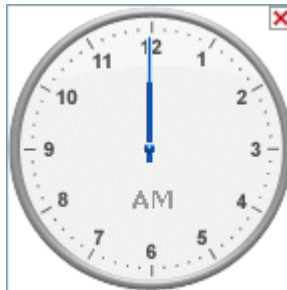
- **New Time Zone** - Click this button to create a new time zone.
- **Save Time Zone** - Click this button to save the time zone once it has been defined.
- **Delete Time Zone** - Click this button to delete the currently selected time zone from the database.
- **Find Time Zone** - Click this button to open the Time Zones - Listing window. Please see the **View, modify or delete time zone** section for details.
- **Time Zone Name** - Enter the name of the time zone.
- **Notes** - Enter any notes about this time zone.
- **Time Zone Interval #1** - This section is used to define the start and end time of the time zone. This section is required.
 - **Starts** - Use the **Hour** and **Min.** drop down menu to specify when the time zone will begin.
 - **Ends** - Use the **Hour** and **Min.** drop down menu to specify when the time zone will end.
 -  - Click on this button to open the Clock application. This application allows you to set the clock in standard time and it will then convert it to 24 hour time. Can be used on both **Start** and **Ends** sections. See below for details on the Clock application.
 - **Repeats:** - Use this drop down to specify how often the time zone will occur during a month. This function allows for access privileges that only occur occasionally throughout a month.

Example: The maintenance staff only needs access to the building on third week of each month. Create a Time Zone named "Maintenance" and select the **3rd occurrence in each month** option from the **Repeats** drop down menu when setting up the time zone. The maintenance staff would then only be granted access on the third week of the month.
 - **Effective Days of the Week** - Check the box for each day of the week that the time zone will be active.
 - **Includes scheduled "Calendar Events"** - Check this box if this time zone will be active during Calendar Events.
- **Time Zone Interval #2, #3, and #4** - These are optional sections used only if a time zone is required to cover two or more different time periods in the same 24 hour period or if a time zone will span midnight. Example: The user wants a time zone that is effective from 6:00 - 12:00 and from 13:00 - 18:00. In Time Zone Interval #1 the user selects a Start time of 6:00 and an end time of 12:00. In the Time Zone Interval #2 the user selects a Start time of 13:00 and an end time of 18:00.
 - **Enable** - Click this button to Enable the additional Interval. Must be clicked for each additional Interval that will be used.
 - **Starts** - Use the **Hour** and **Min.** drop down menu to specify when the time zone will begin.
 - **Ends** - Use the **Hour** and **Min.** drop down menu to specify when the time zone will end.
 -  - Click on this button to open the Clock application. This application allows you to set the clock in standard time and it will then convert it to 24 hour time. Can be used on both **Start** and **Ends** sections. See below for details on the Clock application.
 - **Repeats:** - Use this drop down to specify how often the time zone will occur during a month. This allows for access privileges that only occur occasionally throughout a month.
 - **Effective Days of the Week** - Check the box for each day of the week that the time zone will be active.
 - **Includes scheduled "Calendar Events"** - Check this box if this time zone will be active during Calendar Events.

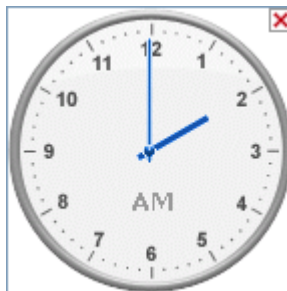
Clock Application

When the  button is clicked the clock application opens. This is a simple application that allows you to set the time in a standard format and then converts that into 24 hour time for you. To use the clock application:

- 1 Click on the  button. The application will open.



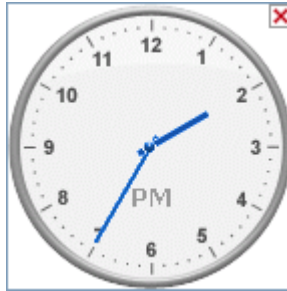
- 2 Click and hold on the shorter arm and position it to set the hour.



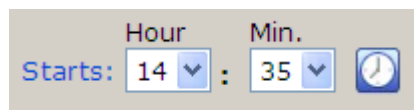
- 3 Click and hold on the longer arm and position it to set the minutes.



- 4 Click on the AM or PM section above the 6 to set AM or PM.



- 5 When the correct time is set, click on the X button in the upper right corner of the clock application. The clock application will close and the time will be set in 24 hour time.



View, modify or delete time zone

Here the user can select a time zone to edit from a table of existing timezones. Clicking on the **View, modify or delete time zone** button from the **Time Zone - Task** window will open the **Time Zones - Listing** window.

Time Zone	Interval #1 Start Time	Interval #1 End Time	Interval #1 Days of the Week	Interval #1 Repeats	Interval #2 Start Time	Interval #2 End Time	Interval #2 Days of the Week
▶ Never							
▶ Always	00:00:00	23:59:59	Sun, Mon - Fri, Sat	Every wee...			
▶ Late Night Employee 8:00pm - 4:00am	20:00:00	23:59:59	Mon - Fri	Every wee...	00:00:00	03:59:59	Tue, Wed, Thu, Fri,
▶ Lobby Unlock 7:00am to 6:00pm	07:00:00	18:00:59	Mon - Fri	Every wee...			
▶ Weekend Shift	06:00:00	22:00:59	Sun, Wed, Sat	Every wee...			

The Time Zone - Listing window has seventeen columns (scroll right to see them all):

Time Zone - Shows the name of the time zone.

Interval #1 Start Time - Shows the start time of the time zone.

Interval #1 End Time - Shows the end time of the time zone.

Interval #1 Days of the Week - Shows which days this time zone affects.

Interval #1 Repeats - Shows how often this time zone occurs.

Interval #2 Start Time - Shows the start time of the time zone.

Interval #2 End Time - Shows the end time of the time zone.

Interval #2 Days of the Week - Shows which days this time zone affects.

Interval #2 Repeats - Shows how often this time zone occurs.

Interval #3 Start Time - Shows the start time of the time zone.

Interval #3 End Time - Shows the end time of the time zone.

Interval #3 Days of the Week - Shows which days this time zone affects.

Interval #3 Repeats - Shows how often this time zone occurs.

Interval #4 Start Time - Shows the start time of the time zone.

Interval #4 End Time - Shows the end time of the time zone.

Interval #4 Days of the Week - Shows which days this time zone affects.

Interval #4 Repeats - Shows how often this time zone occurs.

To edit a Time Zone:

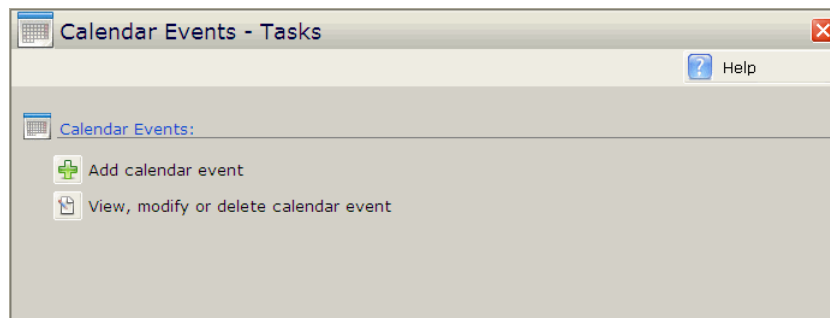
- 1 Click on a time zone to highlight it.
- 2 Click on the **Open** button. The **Time Zones - Edit** window will open.
- 3 Make any changes needed. See the **Add time zones** section for details.
- 4 Click on the **Save Time Zone** button when done.

Calendar Events

CHAPTER 8


Introduction

Calendar Event are defined calendar days or holidays when the "normal" work schedule does not apply. During calendar events, "normal" time zones are overridden by the Calendar Events that are specified. This includes Time Zones that are specified per person such as Permitted Access Time Zones and time zones that are specified per door such as Unlock Time Zones. The only exception to this are time zones that have the checkbox **Includes scheduled Calendar Events** selected. Time Zones with this selected will function normally during Calendar Events. The Calendar Events - Tasks window can be accessed by clicking on the Calendar Events button on the left side of the main screen. This section is accessible by users with Administrator or Manager security levels.



Add calendar event

Clicking on this button opens the Calendar Events - Edit window. Add, modify, delete or search for a specific calendar event from this screen. A blank record will be displayed when the window is first opened. To add a new calendar event, fill in the appropriate information and click on the **Save Calendar Entry** button at the top of the screen.

- **New Event** - Clicking this button will open a blank Calendar Events - Edit page. From this page a new Calendar Event can be defined.
- **Save Event** - After a new Calendar Event has been added, or an existing Event has been modified, click this button to save changes.
- **Delete Event** - Clicking this button deletes the currently selected Calendar Event.
- **Find Event** - Clicking this button opens the Calendar Events - Listing window. This window is used to find existing Calendar Events.
- **Calendar Event Name** - Put the name of the Calendar Event in this field. Example: Winter Break. This is a required field.
- **Notes** - Put any notes about this Calendar event in this field. This is not a required field.
- **Calendar Event** - Use the drop down menus in this section to define the dates and times of the Calendar Event.
- **Starts** - Use the **Hour** and **Min** drop down boxes to define the time at which the Calendar Event will start. Use the **Date** field to specify which day the Calendar Event will begin.
- **Ends** - Use the **Hour** and **Min** drop down boxes to define the time at which the Calendar Event will end. Use the **Date** field to specify which day the Calendar Event will end.
-  - Click on this button to open the clock application. This application allows you to set the clock in standard time and it will then convert it to 24 hour time. Can be used on both **Start** and **Ends** sections. See the Clock Application section of the Time Zone chapter for details.

View, modify or delete calendar event

Clicking this button will open the Calendar Events - Listing window. From this window an existing calendar event can be selected and modified.

Calendar Event	Starts: Date-Time	Ends: Date-Time	Status
▶ Winter Holiday	2007-12-13 00:00:00	2007-12-13 23:59:59	Inactive, occurred at an earlier date.
▶ Spring Holiday	2008-04-01 00:00:00	2008-04-01 23:59:59	
▶ Summer Holiday	2008-08-30 00:00:00	2008-09-07 23:59:59	
▶ Fall Holiday	2008-10-31 00:00:00	2008-10-31 23:59:59	
▶ Team Building Day	2008-12-26 00:00:00	2008-12-26 23:59:59	

The Calendar Events - Listing screen has four columns:

Calendar Event - Shows the name of the calendar event.

Starts: Date-Time - Shows the starting date and time of the calendar event.

Ends: Date-Time - Shows the ending date and time of the calendar event.

Status - Shows if the calendar event has occur.

To edit or delete an existing calendar entry:

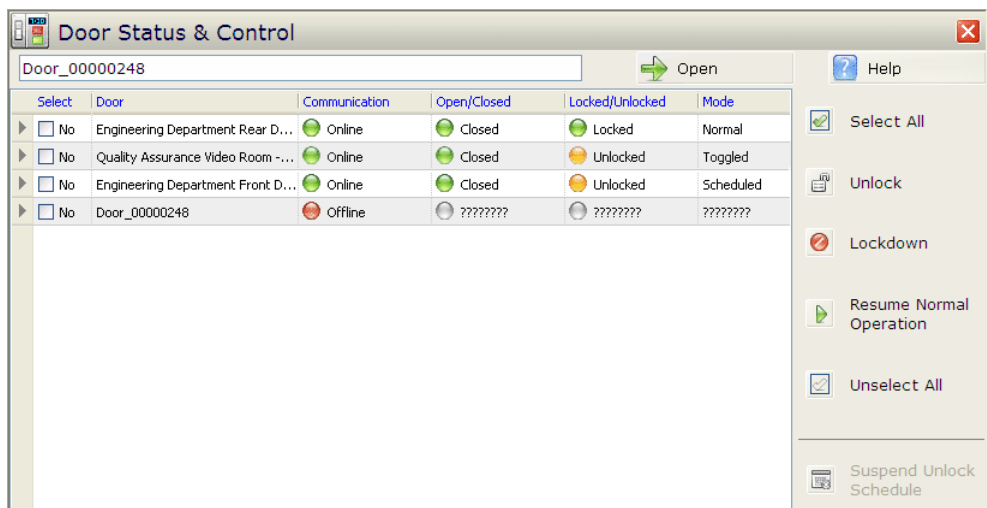
- 1 Click on the **View, modify or delete calendar event** button. The Calendar Event - Listing window will open.
- 2 Highlight the calendar event to be modified by clicking on it.
- 3 Click on the **Open** button. The **Calendar Events - Edit** page will open displaying the record for the calendar event that is selected.
- 4 Edit fields as necessary.
- 5 Click the **Save Calendar Entry** button at the top of the frame, to save the record. If no changes are to be made, exit out of this page by clicking on the "X" button in the upper right corner or click another button in the main menu to exit the Calendar Events - Edit page.
- 6 To delete this record, click on the **Delete Calendar Entry** button.

Door Status & Control

CHAPTER 9

Introduction

The Door Status & Control window allows the user to view the status of, and manually control, the doors in the system. A list of doors in the system is displayed in the status table. This table displays the communication status of the door, whether the door is opened or closed, locked or unlocked and the mode that the door is currently in. The Door Status & Control window can be accessed by clicking on the Door Status & Control button on the left side of the main screen. This section is accessible by users with Administrator or Manager security levels.



Status Table

The status table is located in the center of the Door Status & Control window.

- **Open** - Click on this button when a door is selected to open a detailed status pop-up window for that door.
- **Select** - Shows if a door has been selected. Check the box to change it from "No" to "Yes". This box must be checked for the door to be selected.
- **Door** - Displays the door description.
- **Communication** - Displays door communication status.
- **Open/Closed** - Shows the open/closed status of the door.
- **Locked/Unlocked** - Shows the lock status of the door.
- **Mode** - Displays the door state.
 - **Normal** - The door is in its default state.
 - **Manual** - The door is in a Manual Override state.
 - **Toggled** - The door is in a toggled open state.
 - **Scheduled** - The door is in a scheduled unlock state.
 - **Lockdown** - The door is in a lockdown state.






Detailed Status

To view a more detailed status of the door double click on the door or select it and click on the **Open** button. This will bring up a **Hardware - Status** pop-up window with information specific to the security hardware installed on that door.

AD-300 Status



The **Hardware - Status** window displays the following information:

- Door Name:** AD300MD Mortise Deadbolt Lockset -4
- Online:**  Online
- PIN Required:** No
- Mode:** Normal
- AD300MD:** 
- Inputs and Outputs:**
 - Door Position Switch (DOD)  Open
 - Clutch Position  Locked
 - Exit Request (REX)  Inactive
 - Deadbolt Position  Extended
 - Status of Key Switch  Not Engaged
 - Tamper Switch  Active
 - Battery Status  N/A
 - Interior Push Button  Inactive

Close

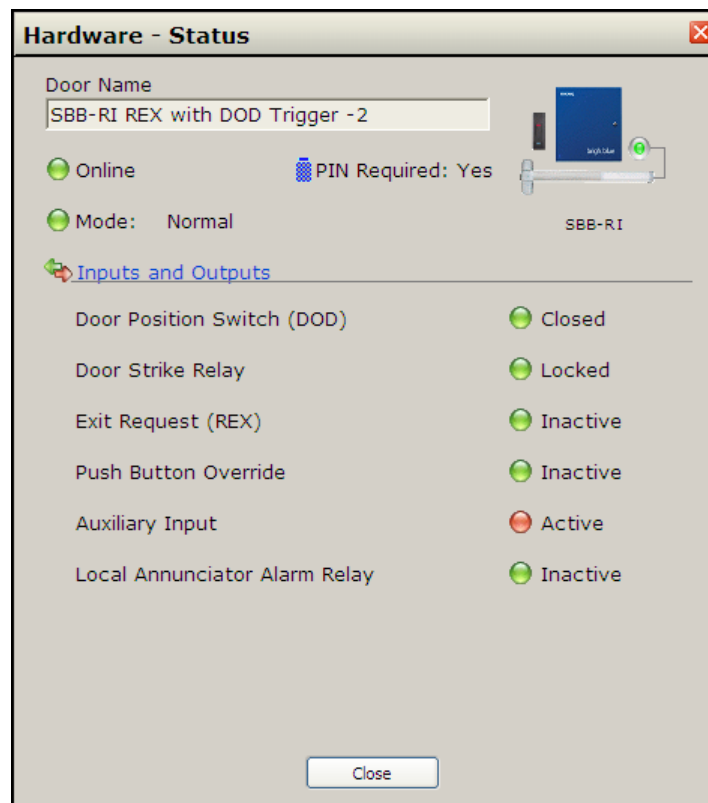
- **PIN Required** - Shows whether a PIN is required at this time or not.
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Clutch Position** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Status of Key Switch** - Shows whether the key switch is engaged or not.
- **Tamper Switch** - Shows whether the tamper switch is active or not.
- **Batter Status** - Not applicable with this lock.
- **Interior Push Button** - Shows whether the interior push button is active or not.

VIP Status



- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Status of Key Switch** - Shows whether the key switch is engaged or not.

SBB-RI Status



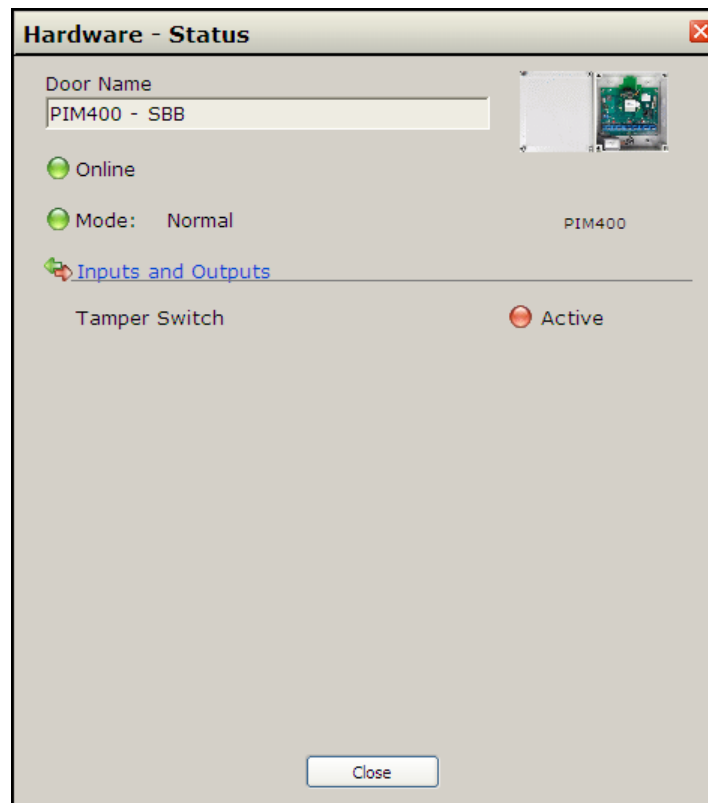
- **PIN Required** - Shows whether a PIN is required at this time or not.
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Auxiliary Input** - Shows whether there is any activity on the auxiliary input.
- **Push Button Override** - Shows whether this is a push button override connected to this lock.
- **Local Annunciator Alarm Relay** - Shows the status of any alarm relay connected to this lock.

SBB-NRI Status



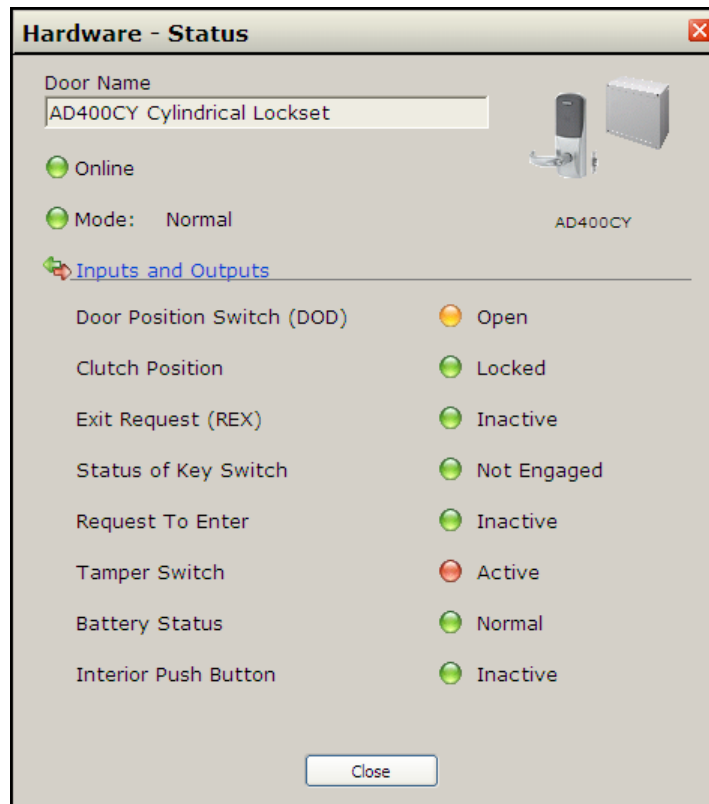
- **PIN Required** - Shows whether a PIN is required at this time or not.
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Push Button Override** - Shows whether this is a push button override connected to this lock.
- **Auxiliary Input** - Shows whether there is any activity on the auxiliary input.
- **Local Annunciator Alarm Relay** - Shows the status of any alarm relay connected to this lock.

PIM400-SBB Status



- **Mode** - Shows what state the PIM is in.
- **Tamper Switch** - Shows whether the tamper switch is active or not.

AD-400 Status



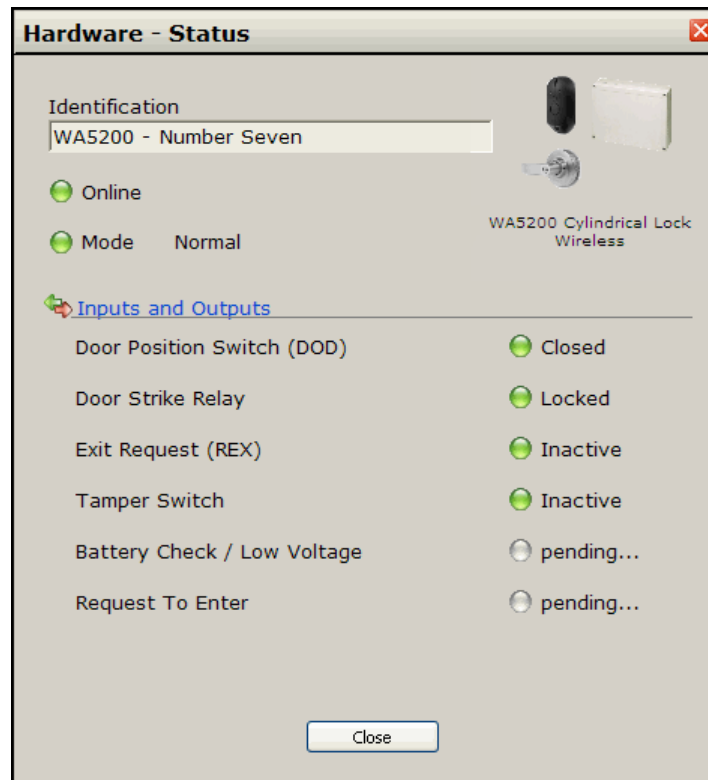
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Clutch Position** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Status of Key Switch** - Shows whether the key switch is engaged or not.
- **Request To Enter** - Shows whether there is a Request to Enter associated with this door.
- **Tamper Switch** - Shows whether the tamper switch is active or not.
- **Batter Status** - Shows the battery status of the lock.
- **Interior Push Button** - Shows whether the interior push button is active or not.

PIM-SBB Status



- **Mode** - Shows what state the PIM is in.
- **Tamper Switch** - Shows whether the tamper switch is active or not.

WAPM Status

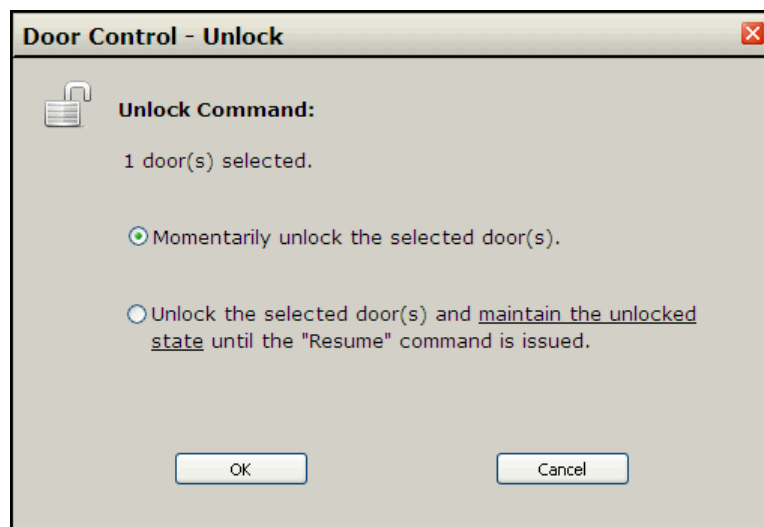


- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Tamper Switch** - Shows whether the tamper switch is active or not.
- **Battery Check/Low Voltage** - Shows whether the low voltage switch is active.
- **Request To Enter** - Shows whether there is a Request to Enter associated with this door.

Control Buttons

To the right of the status table, there are a series of buttons that allow the user to control the doors in the system. These buttons will override any lock or unlock schedules that are in use.

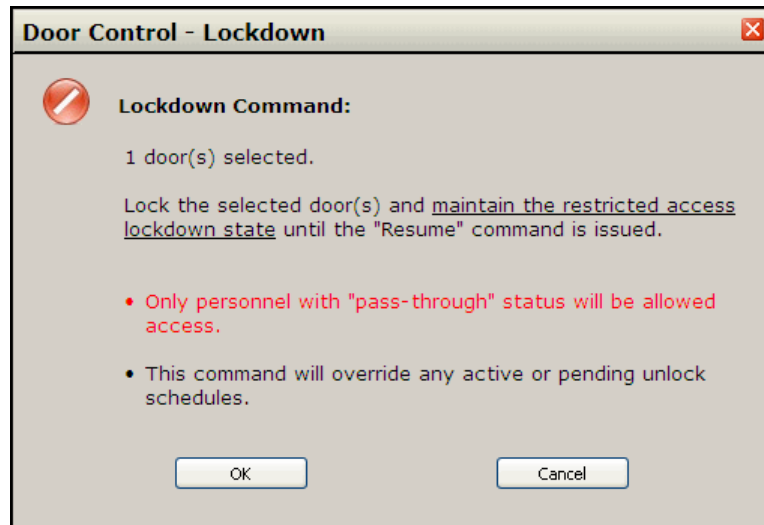
- **Select All** - Clicking this will select all doors.
- **Unlock** - Clicking this will open the **Door Control - Unlock** pop-up window. From this window the user can unlock the door(s) that have been selected in the Status Table.



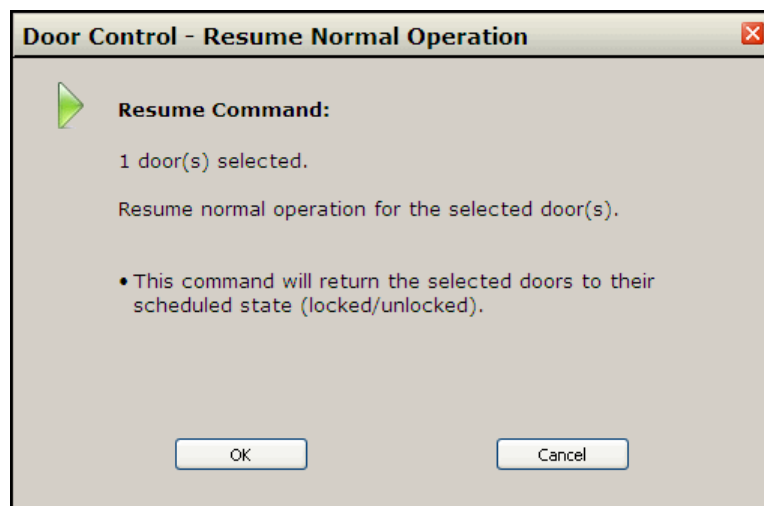
- **Momentarily unlock the selected door(s)** - Check this to unlock the door for 3 seconds.
- **Unlock the selected door(s) and maintain the unlocked state until the "Resume" command is issued.** - Check this if the door is to remain unlocked indefinitely. A Resume command will need to be issued to re-lock this door.
- **OK** - Click this to activate the unlock command. The Command Processor window will open. When this is done the selected door(s) will be unlocked and the pop-up window will close.
- **Cancel** - Closes the pop-up window without unlocking the door(s).

Note: The **Momentarily unlock the selected doors** control does not work with WAPM locks unless a Request to Enter button is in use. It also does not work with WRI locks.

- **Lockdown** - Clicking this will open the **Door Control - Lockdown** pop-up window. From this window the user can lock the door(s) that have been selected in the Status Table.



- **OK** - Click this to Lockdown the selected door. The Command Processor window will open. When complete, the selected door(s) will be locked and the pop-up window will close.
- **Cancel** - Click this to close the Door Control - Lockdown window without locking out the selected door.
- **Resume Normal Operation** - Clicking this button will open the **Door Control - Resume Normal Operation** pop-up window. From this window the user can return the selected door(s) to their scheduled state.



- **OK** - Click this to restore the scheduled state. The Command Processor window will open. When complete, the selected door(s) will be returned to their regular state and the pop-up window will close.
- **Cancel** - Closes the pop-up window without restoring the door(s).

- **Suspend Unlock Scheduled** - Clicking this button will open the **Door Control - Suspend Unlock Schedule** pop-up window. From this window the user can cancel the unlock schedule for the door(s) that have been selected in the Status Table.



- **OK** - Click this to suspend the unlock schedule of the selected door. The Command Processor window will open. When complete, the selected door(s) will be locked and the pop-up window will close.
- **Cancel** - Closes the pop-up window without locking the door(s).
- **Unselect All** - Clicking this will unselect all of the doors that have been selected.

Door Setup

CHAPTER 10

Introduction

The Door Setup - Tasks window is split into two sections. The Installation and Configuration section is used to add new doors and locks to the system, modify existing doors and to set up global door settings. The Test/Monitor section is used to check door status. The Door Setup - Tasks window can be accessed by clicking on the Door Setup button on the left side of the main screen. This section is only accessible by users with Administrator security level.

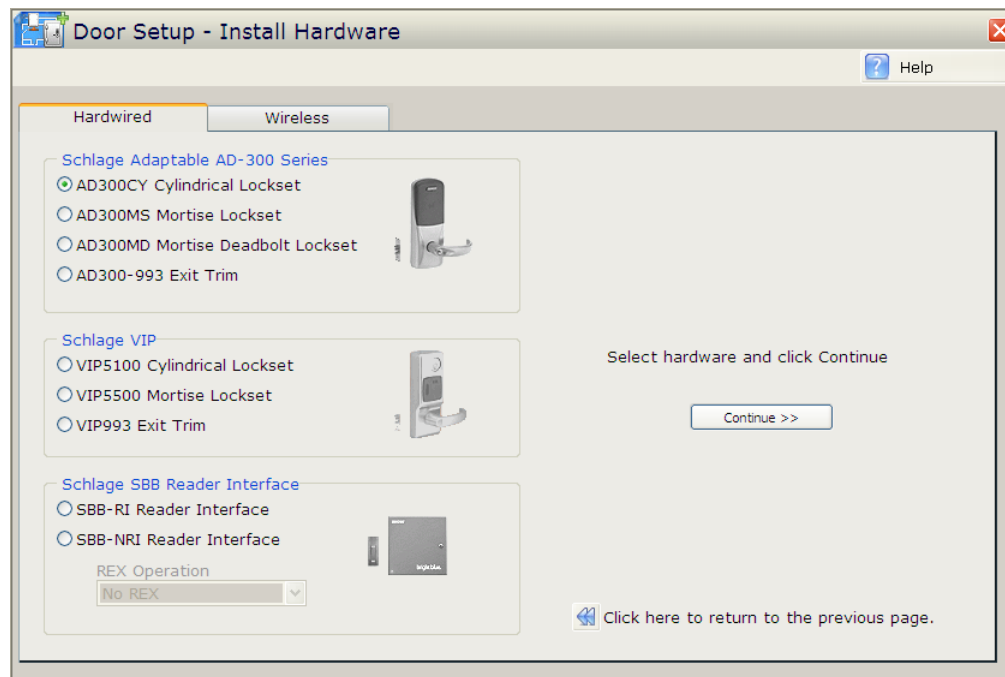


Installation and Configuration

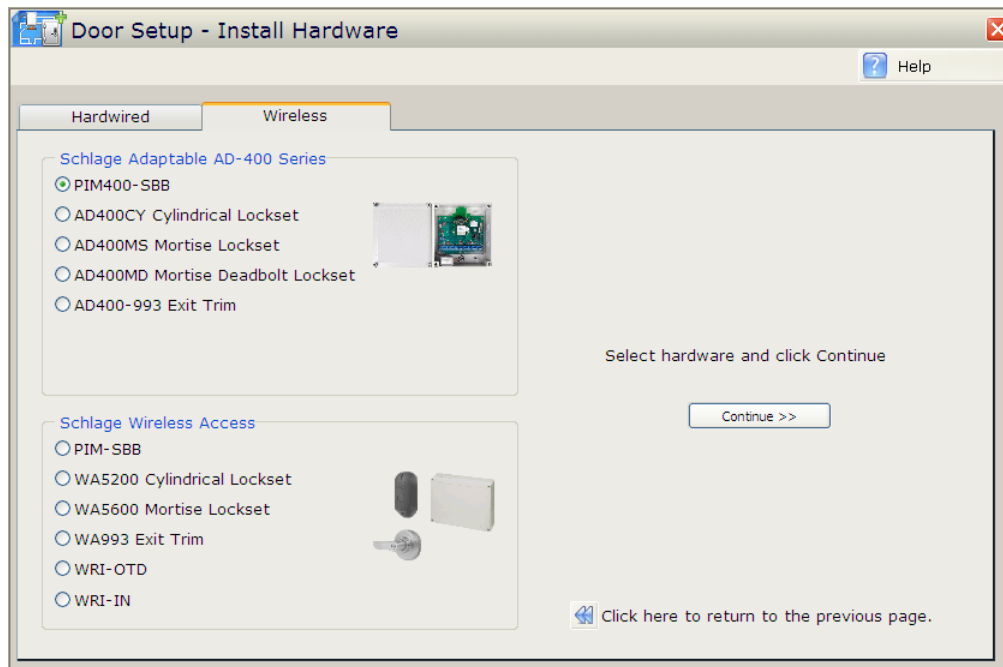
The Installation Tasks section contains buttons for **Add doors and hardware**, **View or modify door configuration** and **View or modify global settings**.

Add doors and hardware

Clicking this button will open the **Door Setup - Install Hardware** window with the **Hardwired** tab selected.



Click on the Wireless tab to open the Wireless setup page.

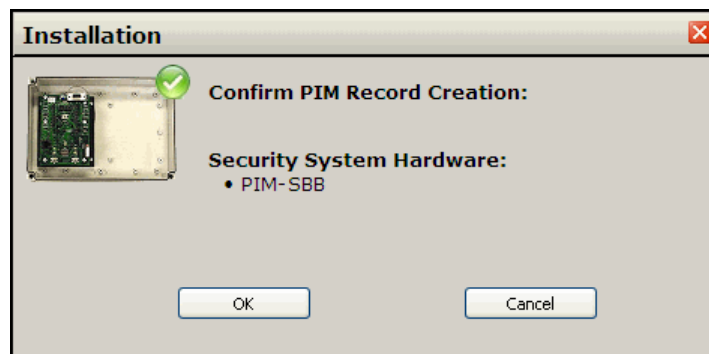


These screens enables the user to set up new door hardware, including locks, readers and interfaces. Click on the button to the left device to begin set up. After selecting the correct device, click the **Continue** button.

Note: If a Schlage Adaptable AD-400 Series device or a Schlage Wireless Access device(s) is in use, a PIM400-SBB or a PIM-SBB must first be set up in the system. This can be done by selecting the button next to the **PIM400-SBB** or the **PIM-SBB** then clicking on the **Continue** button to the right.

Adding a PIM

After selecting the correct PIM option from the Wireless tab and clicking on **Continue**, the Installation pop-up window will open.

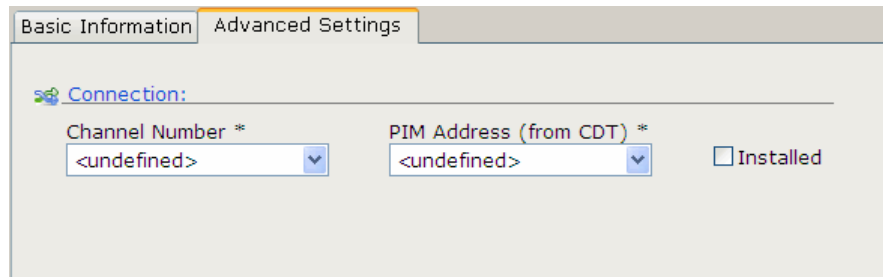


OK - Clicking this will open the **Door Setup - Edit PIM** page.

Cancel - Clicking this will close the pop-up window without making any changes.

- **PIM Name** - This is what is displayed in reports and when assigning access to the door. It is a required field.
- **Notes** - It can be used to store information that is specific to this PIM. This field is optional.
- **Basic Information** - This tab shows all doors linked to the PIM. If this is a new PIM, the pane will be blank and no doors will be displayed.
 - **Channel #** - Shows the channel number of the selected door.
 - **Address** - Displays the address of the selected door.
 - **Hardware** - Displays the type of wireless lock being used.
 - **Identification** - Shows the name of the selected door.
 - **Installed Status** - Shows whether the selected door is installed or not.

- **Advanced Settings** - This tab contains information pertaining to where the PIM is connected to the controller board.



The screenshot shows the 'Advanced Settings' tab of a software window. It features a 'Connection:' section with two dropdown menus: 'Channel Number **' and 'PIM Address (from CDT) **', both currently showing '<undefined>'. To the right of these fields is an unchecked checkbox labeled 'Installed'.

- **Channel Number** - Used to select the appropriate channel number for the PIM.
- **Address** - Select the address of the PIM-SBB that was configured using the CDT program or for the PIM400-SBB that was configured using the Schlage Utility Software (SUS).
- **Installed** - Check this box to indicate that this PIM is currently installed.

Adding a Door

After selecting the correct lock option for the door, click the **Continue** button. The Installation pop-up window will open.



OK - Clicking this will open the **Door Setup - Edit Door Security System** window.

Cancel - Clicking this will open the **Door Setup - Install Hardware** page.

Door Name - This is what is displayed in reports and when assigning access to the door. This is a required field.

Notes - Put any notes that are pertinent to this door. This field is optional.

Basic Settings - This tab is used to define the reader type and time specifications for this door.

- **Reader** - This section of the tab is used to define the reader.
 - **Reader Type** - Use this drop down box to specify what type of reader this is.
 - Standard Reader** - A Standard Reader is the most common type of reader. In this setup there is a reader on the exterior of the door and none on the interior. The interior is usually set up as free egress.
 - Entry Reader** - An Entry Reader is generally used in a situation where **Anti-passback** is being used. This refers to the exterior reader that grants access to the door.
 - Exit Reader** - An Exit Reader is generally used in an **Anti-passback** situation, also. This refers to the reader that is located on the interior side of the door.
 - Example:** Your company has a parking garage with a secured entrance and exit. There is an entry reader on the exterior side and an exit reader on the interior side of the gate. Due to maintenance the gate is being held in the up position. During the time that the gate is in the up position many employees come to work and park their cars without using their credentials at the entry reader. At the end of the day the gate has been fixed and is secured. When the employees attempt to leave, the gate will not open for them as the exit reader will not allow an exit to a credential that has not been through an entry reader. For these employees to be able to exit the parking garage they will need to have their antipassback state reset to neutral at which point the exit reader will allow them to leave.
- **PIN-pad** - Check this box if the lock has a PIN-pad that will be in use. The Schedules tab (see below) will be used to define when the PIN is required. (This option will be disabled for any locks that do not support a PIN-pad.)
- **REX** - This section of the tab is used to define the REX. REX stands for request-to-exit and refers to either a mechanical button or PIR (motion sensor) that is used to gain egress from a secured door. This is only enabled if setting up an SBB-RI.
 - **REX Operation** - This drop down has three options:
 - No REX** - No REX for this door. Request-to-exit is not in use. Door Forced Open is not reported.
 - REX - No Unlock** - Request-to-exit is in use to report a valid exit and bypass door contact reporting for a period of time. The REX device will not unlock the electrified locking device. This is typically used when either a door knob or exit bar are used as these devices manually unlatch from the inside of the opening.
 - REX - Unlock** - Request-to-exit is in use to report a valid exit, bypassing door contact reporting for a period of time AND unlocking the electrified locking device. This is typically used when a magnetic lock is used and must be unlocked from the inside of the door to allow exiting.
- **Timers** - This section of the tab is used to specify time for normal access.
 - **Unlock Time** - Use this drop down field to define the number of seconds the door will be unlocked before the lock re-engages.
 - **Door Held Open Detect Time** - Use this drop down field to define the amount of time a door can be held open before the system is alerted.
- **Special Access Timers** - This section of the tab is used to specify time for special access.
 - **Unlock Time** - Use this drop down field to define the number of seconds a door will be unlocked for a person with Special Access before the lock re-engages.
 - **Door Held Open Detect Time** - Use this drop down field to define the amount of time a door can be held open, after being unlocked by someone with Special Access, before the system is alerted.

Advanced Settings - This tab is used to define the lock's connection to the system, to enable reports for this door, to specify if enhanced security is in use and to define a camera if video surveillance is enabled. This tab changes specifications depending on what type of door is being set up.

The screenshot shows the 'Advanced Settings' tab of a configuration window. It is divided into three main sections:

- Connection:** Contains two dropdown menus labeled 'Channel Number *' and 'SBB-RI Address *', both showing '<undefined>'. There is also an 'Installed' checkbox.
- Event Reporting:** Contains two checkboxes: 'Enable "Lock/Unlock" relay state change reporting' and 'Enable "REX" state change reporting'.
- Enhanced Security:** Contains a checkbox 'Disable door access during system start-up'.


To the right of the Event Reporting section, there is a 'Video Surveillance System Event Logging' section with a 'Camera' dropdown menu showing '<not enabled>' and a camera icon button.

- **Connection** - This section of the tab is used to define the lock's connection to the system.
 - **Channel Number** - Use the drop down box to specify the channel on the controller the device is wired to. This is for AD300 Series, VIP, PIM-SBB, PIM400-SBB and SBB-RI locks only.
 - **Lock Address** - Use the drop down box to specify the Lock Address. The address is found in different ways for each type of lock:
 - PIM400-SBB** - Find the address using the Schlage Utility Software (SUS) located on the PDA. Please see the install manual for more information.
 - PIM-SBB** - Find the address using the CDT. Please see the install manual for more information.
 - Series 300** - Find the address using the Schlage Utility Software (SUS) located on the PDA. Please see the install manual for more information.
 - VIP** - The address is specified by the position of the address switches on the lock. Please see the install manual for more information.
 - SBB-RI** - The address is specified by the Jumpers on the SBB-RI. Please see the install manual for more information.
 - **PIM** - Use this drop down box to specify which PIM this lock is connected to. This is for Wireless locks only.
 - **Door #** - Find the door number using the CDT for WA Series locks and using the SUS for AD-400 Series locks. This is for Wireless locks only.
 - **IP Address or Hostname** - This is where the IP address or Hostname of the SBB-NRI controller is entered. Find the IP Address using either the SBB-NRI Configuration GUI or the Discovery and Configuration Tool. Please see the install manual for more information.
- **Event Reporting** - This section of the tab is used to define which types of reports will be enabled for each door.
 - **Enable "Lock/Unlock" relay state change reporting** - Check this box to generate reports and see activity based on when the door is locked and unlocked.



- **Enable "REX" state change reporting** - Check this box to generate reports and see activity based on when the REX is activated.
- **Enable "Request-To-Enter" state change reporting** - Check this box to generate reports and see activity based on when the Request-To-Enter feature is added. This is for Wireless locks only.
- **Enable "Clutch Position" state change reporting** - Check this box to generate reports and see activity based on when the lock's clutch is engaged/disengaged.
- **Video Surveillance System Event Logging** - This section of the tab is used to select a camera that will be associated with this door. This section will only be enabled if the **Enable video Surveillance System Interface** option has been checked in the **Video** section of **Global Settings**. Please see the section on Global Settings for more details.
 - **Camera** - Use the drop down to select which camera will be associated with this door.
- **Enhanced Security** - This section of the tab is used to enable/disable door access during a system start up. If bright blue has to restart for any reason while it is loading its database the doors in the system will be, by default, put into enhanced security mode. This means that, during a system start-up, any personnel with a credential with the correct Facility/Site code will be given access to a door whether or not that person would normally have access rights to that door. If you wish to disable this feature, and make it so a door remains locked during a system start-up, no matter what credential is presented, then check the box below.
 - **Disable door access during system start-up** - Check this box to disable door access during a system start up. This box is unchecked by default.

Schedules - This tab is used to define the schedules of the door as well as the Toggle Cancel Time.

The screenshot shows the 'Schedules' tab in the software interface. It contains two main sections: 'Unlock Schedule' and 'PIN Required Schedule'. The 'Unlock Schedule' section has a dropdown menu for 'Unlock Time Zone' currently set to 'Never', an unchecked checkbox for 'Apply "1st Person In" rule', and a 'Toggle Cancel Time' section with an unchecked checkbox and a time/day selection area. The 'PIN Required Schedule' section has a dropdown menu for 'PIN Required Time Zone' currently set to 'Never'.

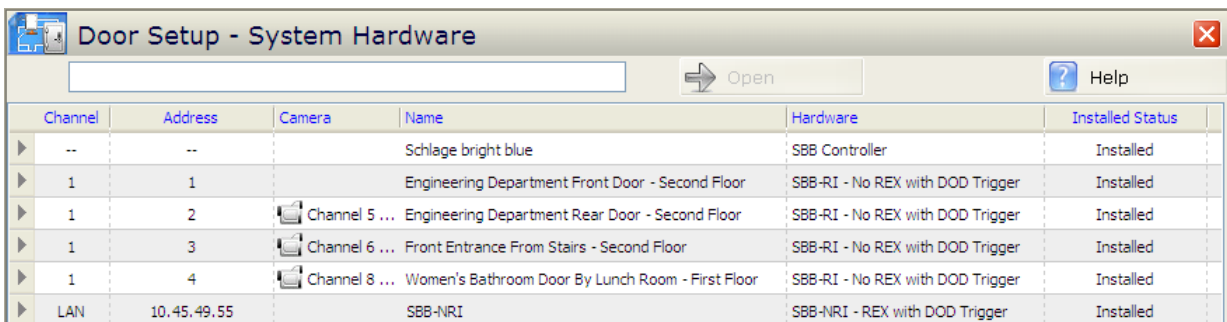
- **Unlock Schedule:** - This section of the tab is used to define which time zone will be associated with the door.
 - **Unlock Time Zone** - Use this drop down field to select the time zone for which the door will be automatically unlocked.
 - **Time Zone Information**  - Rolling over this icon will show the time range of the selected Time Zone.
 - **Apply "1st Person In" rule** - Check this field to apply the "1st Person Rule" to this door. This feature is used to enable an override when the first valid access card is presented during a time zone. The override will re-lock according to original schedule.

Example: The front door of a facility is to be unlocked from 7:00am until 5:00pm every day but the door should not be unlocked if no one is in the building. In the Unlock Timezone drop down select the 7:00am to 5:00pm Time Zone. Then check the Apply 1st Person In Rule box. Now the door will only follow the unlock schedule after someone has presented a valid credential at the door. This function is particularly useful when a facility is closed (or has a delayed opening) due to inclement weather because the doors will remain locked until a valid credential is presented.

- **PIN Required Schedule:** - This section of the tab is used to define which time zone will determine when a PIN number is required as well as a credential to unlock the door. This section will only be enabled if the **PIN-pad** option is checked in the **Basic Settings** tab.
 - **PIN Required Time Zone** - Use this drop down box to select the time zone during which a PIN will be required.
 - **Time Zone Information**  - Rolling over this icon will show the time range of the selected Time Zone.
- **Toggle Cancel Time:** - This section of the tab is used to specify times when the door will lock automatically if the door was left in a toggle-open state.
 - **Ensure this door is re-locked automatically at the following time/days, if toggled unlocked:** - Check this box to enable this feature.
 - **Time:** - Use these drop down boxes to specify when the door will lock.
 - **Clock**  - Click this icon to open the clock application. The clock application allows you to set the time in a regular format and it will translate it into the 24 hour format that is used by the system. See the **Clock Application** section of the **Time Zone** chapter for details.
 - **Effective Days of the Week:** - Use the specific day's check boxes to specify which days of the week the door will automatically lock.

View or modify door configuration

This button opens the Door Setup - System Hardware window.



Channel	Address	Camera	Name	Hardware	Installed Status
▶	--		Schlage bright blue	SBB Controller	Installed
▶	1	1	Engineering Department Front Door - Second Floor	SBB-RI - No REX with DOD Trigger	Installed
▶	1	2	Channel 5 ... Engineering Department Rear Door - Second Floor	SBB-RI - No REX with DOD Trigger	Installed
▶	1	3	Channel 6 ... Front Entrance From Stairs - Second Floor	SBB-RI - No REX with DOD Trigger	Installed
▶	1	4	Channel 8 ... Women's Bathroom Door By Lunch Room - First Floor	SBB-RI - No REX with DOD Trigger	Installed
▶	LAN	10.45.49.55	SBB-NRI	SBB-NRI - REX with DOD Trigger	Installed

Note: The Camera column will be visible only if the Video Surveillance System Interface is enabled. See the **View or modify global settings** section for details.

Double clicking on the door will open the Door Setup - Edit Door Security System showing the door that was selected. From here the selected door or controller can be modified. Click on Save Door when finished.

Door Setup - Edit Door Security System

New Door Save Door Delete Door Find Door Help

Door Name *
Door_00000262

Notes

AD300CY Cylindrical Lockset

Basic Settings Advanced Settings Schedules

Reader:
Reader Type: Standard Reader
PIN-pad: ☐ No
REX Operation: N/A

Timers:
Unlock Time: 3 seconds
Door Held Open Detect Time: 30 seconds

Special Access Timers:
Unlock Time: 6 seconds
Door Held Open Detect Time: 60 seconds

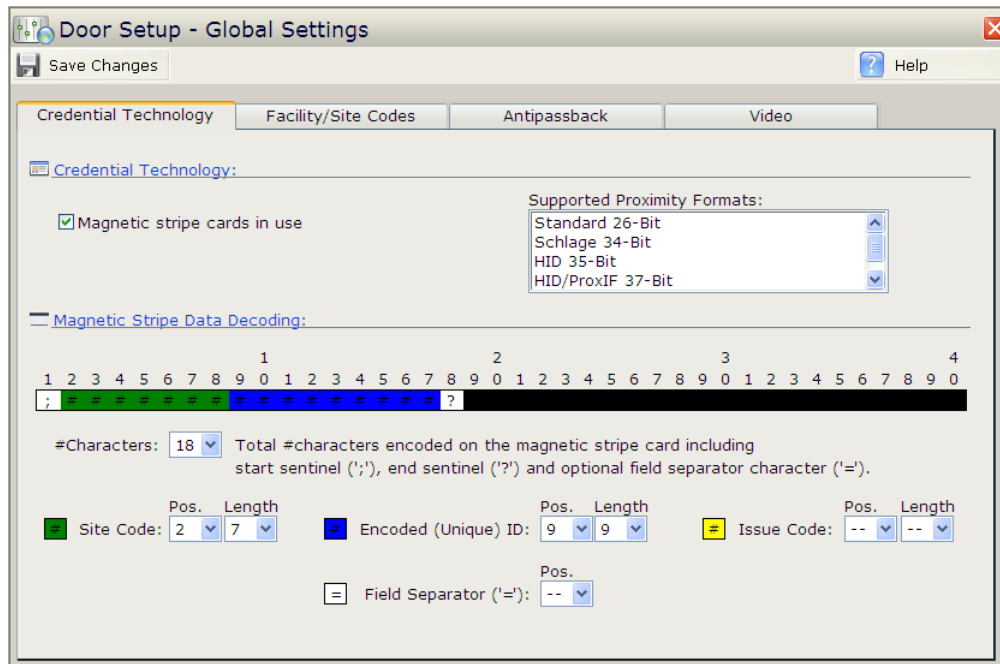
For more information, please see the **add doors and install hardware** section.

View or modify global settings

The **Door Setup - Global Settings** page is used to make changes to card settings. There are four tabs on this screen; Credential Technology, Facility/Site Codes, Anti-passback time and Video

Credential Technology

The Credential Technology Tab is used to define what type of credential is in use with **bright blue** and to configure a custom format for a magnetic stripe card if necessary. Only one additional magnetic stripe format can be entered.



Credential Technology - This section is used to define the type of card technology in use with **bright blue**. Only one type of technology can be used per system. For a list of acceptable proximity and magnetic stripe card formats please see the **Acceptable Card Format** section of the **Personnel** chapter.

- **Magnetic stripe cards in use** - This checkbox determines if proximity or magnetic stripe cards are in use. If the box is unchecked then proximity cards are in use. If the box is checked then magnetic stripe cards are in use.
- **Supported Proximity Formats** - This is a list of the types of proximity cards that **bright blue** supports. Nothing needs to be selected from this list, it is for information only.

Magnetic Stripe Data Decoding - This section only applies if magnetic stripe cards are in use. This section will be grayed out if the **Magnetic stripe cards in use** checkbox is left unchecked. .

Note: These settings should only be altered if non-Schlage magnetic stripe cards are being used.

Magnetic Stripe Template - This image displays how many characters on the magnetic stripe card the system will reference. This graphic will change as the parameters for Characters, Site Code, Encoded ID, and Issues Code are altered.

- **#Characters** - This drop down field specifies how many characters in total will be used by the magnetic stripe card. This is the number of bits used by the card. Example: An 18 bit card would have a #Characters value of 18. The default is 13.

Site Code - Site codes are the first set of characters on a magnetic stripe card, they are represented by green boxes. These characters are unique to each facility or building. Site codes are not required.

- **Pos** - Defines the starting position of the site code. Default is 2.
- **Length** - Defines how many characters the site code will take up. Default is 3.

Note - To disable site codes select the "--" character from the **Pos** and **Length** drop down boxes.

Encoded ID - Encoded ID is the second set of characters on a magnetic stripe card. They are represented by blue boxes. These characters are unique to each person and are required.

- **Pos** - Defines the starting position of the encoded ID. Default is 5.
- **Length** - Defines how many characters the site code will take up. Default is 6.

Issue Code - Issues Code is the last set of characters on a magnetic stripe card. They are represented by yellow boxes. An Issue Code is used to add increased security to the system. When a person loses their credential the replacement credential they receive will be identical to their original with the exception of the Issue Code. The Issue Code for the new card will be one number higher than on the previous card. When the new card is entered into the system it will automatically invalidate any card with a lower Issue Code, making the lost card inoperable.

- **Pos** - Defines the starting position of the encoded ID. Default is 11.
- **Length** - Defines how many characters the site code will take up. Default is 2.

Note - To disable issue codes select the "--" character from the **Pos** and **Length** drop down boxes.

How to set up Magnetic Stripe Data Decoding

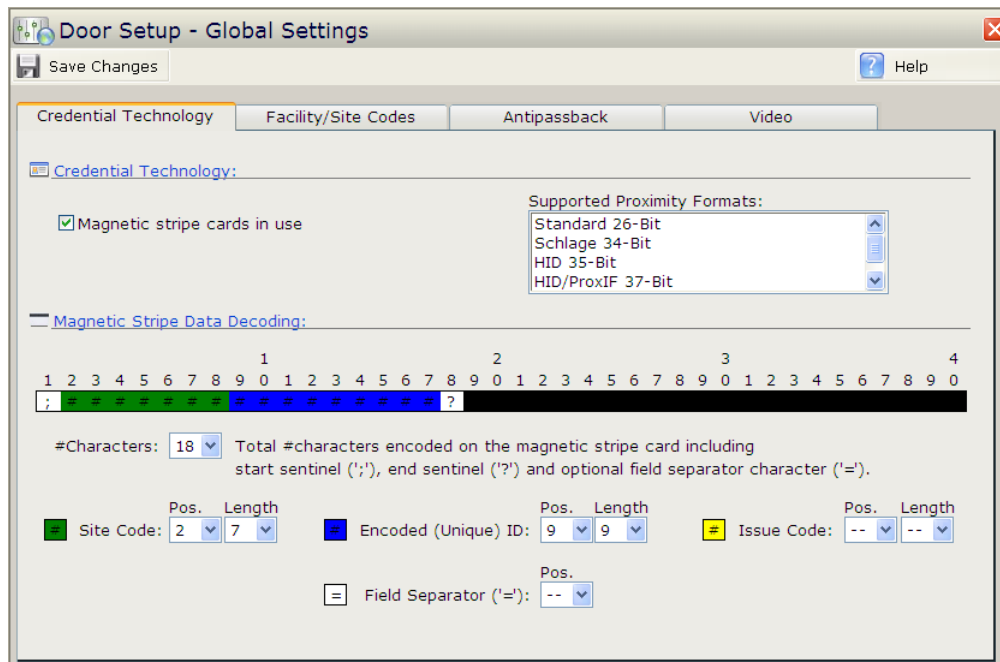
The Magnetic Stripe Data Decoding is used to set up a template for non-Schlage magnetic stripe cards. Each type of magnetic stripe card has a different bit pattern with the credential information in a specific format. The Magnetic Stripe Data Decoding must be configured for that specific format in order for **bright blue** to interact with that card type.

Determine the bit number, the number of bits for the site code, the number of bits for the Encoded ID, the number of bits for the Issue Code, and if there is a separator between any of the fields. This information will be provided by the vendor of the magnetic stripe cards.

Note - A customer defined magnetic stripe template will override a Schlage magnetic stripe template if they are the same bit number. If the card template being added to bright blue is for a bit value of a Schlage template (11, 14, or 18 bits) then that Schlage template will no longer be valid. Example: A 11 bit magnetic stripe template is added to **bright blue**. The Geo-Image magcard 11-D will no longer work.

- 1 Click on the **Door Setup** button on the left side of the main screen. The Door Setup - Tasks window will open.

- Click on the **View or modify global settings** button. The Door Setup - Global Settings window will open with the Credential Technology tab selected.



- Click on the **Magnetic stripe cards in use** check box. The Magnetic Stripe Data Decoding section will be enabled.
- Select the number of bits from the **#Characters** drop down box.
- Select the position and length of the Site Code information using the **Site Code Pos.** and **Length** drop down boxes.
- Select the position and length of the Encoded ID using the **Encoded (Unique) ID Pos** and **Length** drop down boxes.
- Select the position and length of the Issue Code using the **Issue Code Pos.** and **Length** drop down boxes.
- Optional:** Select the position of the Field Separator using the **Field Separator Pos.** drop down box.
- Check the template to make sure there are no grey or red boxes. Grey signifies that there is no data in that field, red signifies that there is an overlap with another field.
- Click on the **Save Changes** button.

Example of setting up magnetic stripe template

For this example the steps above will be followed with a card format of 16 bits with a site code of 4 bits, an Encoded ID of 8 bits and an Issue Code of 2 bits.

- Select 16 from the **#Characters** drop down box. This informs the system that it is a 16 bit card.
- Using the **Site Code Pos.** drop down box, select 2. This is the first available position for data.

- 3 Using the **Site Code Length** drop down, select 4. This is the number of bits the card uses for Site Code data.
- 4 Using the **Encoded ID Pos.** drop down box, select 6. This is the first position available for data after the Site Code.
- 5 Using the **Encoded ID Length** drop down box, select 8. This is the number of bits the card uses for Encoded ID data.
- 6 Using the **Issue Code Pos.** drop down box, select 14. This is the first position available for data after the Encoded ID.
- 7 Using the **Issue Code Length** drop down box, select 2. This is the number of bits the card uses for Issue Code data. After this step the Magnetic Stripe Template should look like this:

The screenshot shows the 'Magnetic Stripe Data Decoding' window. At the top, a horizontal bar represents the 16-bit template, divided into four sections labeled 1, 2, 3, and 4. Section 1 (bits 1-4) is green, Section 2 (bits 5-12) is blue, Section 3 (bits 13-14) is yellow, and Section 4 (bits 15-16) is black. Below the bar, the '#Characters' is set to 16. A text box explains: 'Total #characters encoded on the magnetic stripe card including start sentinel (';'), end sentinel ('?') and optional field separator character ('=')'. Below this, three fields are configured: 'Site Code' with Pos. 2 and Length 4 (green icon), 'Encoded (Unique) ID' with Pos. 6 and Length 8 (blue icon), and 'Issue Code' with Pos. 14 and Length 2 (yellow icon). A 'Field Separator' field is also present with Pos. --.

- 8 Click on the **Save Changes** button. 16 bit cards with this format will now work in the system.

Facility/Site Codes

A site or facility code is a set of information used in a magnetic stripe or proximity card to increase security. When presenting a credential to a reader the site code as well as the encoded id will be read to verify if the credential holder has access. If either the site code or the encoded id is not in the system then the card holder will not be granted access. Site codes are determined in a few different ways:

- For proximity cards, site codes are designated by the access control supplier. The site code information will be included with the cards.
- For Schlage branded magnetic stripe cards, site codes are designated by Schlage. The site code information will be included with the cards.

To add site codes to the system:

- 1 Click on **Door Setup** button on the left side of the main screen. The **Door Setup - Tasks** window will open.
- 2 Click on the **View or modify global settings** button. The **Door Setup - Global Settings** window will open.

- 3 Click on the **Facility/Site Codes** tab.

The screenshot shows the 'Door Setup - Global Settings' window with the 'Facility/Site Codes' tab selected. The window has a title bar with a 'Save Changes' button and a 'Help' button. Below the tabs, there is a section titled 'Facility/Site Codes:' containing a table with two columns: 'Code' and 'Notes (optional)'. The table has five rows. The first two rows are filled with data: the first row has a checked checkbox, the code '22', and the note 'North Building'; the second row has a checked checkbox, the code '58', and the note 'South Building'. The remaining three rows have unchecked checkboxes and empty code and note fields.

	Code	Notes (optional)
<input checked="" type="checkbox"/>	22	North Building
<input checked="" type="checkbox"/>	58	South Building
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

- 4 Click on the check box to the left of the first blank field.
- 5 Enter the site code into the **Code** field.
 - a) **Optional:** Enter any notes about this site code in the **Notes** field.
- 6 Repeat for up to five different site codes.
- 7 Click the **Save Changes** button.

Anti-passback

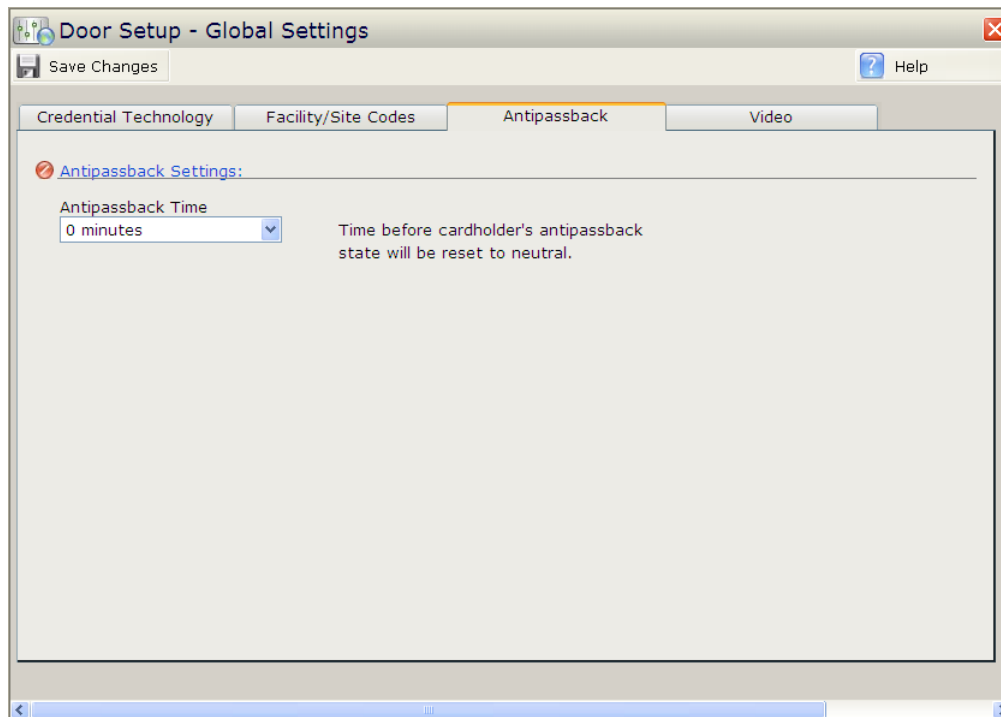
Anti-passback is a function that provides extra security to the system. When anti-passback is in use it is difficult for a credential to be used and then passed to another person for use. This is accomplished through the use of entry and exit readers. When a credential is granted access at an entry reader it will no longer work at another entry reader until it has been granted egress from an exit reader.

The Anti-passback Settings section allows the user to designate an amount of time before a credential will automatically return to a neutral state. When in a neutral state the credential can be used at either an entry or an exit reader.

Example: Anti-passback is enabled and the Anti-passback time has been set to 10 minutes. A cardholder presents their credential at an entry reader and gains access. When 10 minutes have elapsed the cardholder will be able to gain access by presenting their credential at an entry reader even though they have not yet gone through an exit reader.

To set Anti-passback time:

- 1 Click on **Door Setup** button on the left side of the main screen. The **Door Setup - Tasks** window will open.
- 2 Click on the **View or modify global settings** button. The **Door Setup - Global Settings** window will open.
- 3 Click on the **Anti-passback** tab.



- 4 Using the **Anti-passback Time** drop down box select the amount of time before a credential's anti-passback state returns to neutral.
- 5 Click **Save Changes**.

Note: If the credentials should never return to a neutral state set the Anti-passback time to 0.

Video

The Video tab is used to connect to a third party video server. From here you define if a video server is in use, the video server IP address, and the user name and password needed to access that server.

The screenshot shows the 'Door Setup - Global Settings' window with the 'Video' tab selected. The window has a title bar with a close button and a 'Help' button. Below the title bar are four tabs: 'Credential Technology', 'Facility/Site Codes', 'Antipassback', and 'Video'. The 'Video' tab is active. The main content area is titled 'Video Surveillance System Interface:'. It contains a checkbox 'Enable Video Surveillance System Interface' which is checked. Below this is a dropdown menu for 'Video System Model' with 'SEVMS-SBB' selected. To the right of these fields is a large empty box labeled 'Cameras'. Below the dropdown menu are three input fields: 'Server IP Address or Hostname *', 'User Name *', and 'Password *'. Below the 'Password *' field is a 'Password (confirm) *' field. At the bottom left is a 'Test connection' button. At the bottom right of the 'Cameras' box is a 'Refresh the camera list' button. The window has a standard Windows-style scrollbar at the bottom.

Door Setup - Global Settings

Save Changes Help

Credential Technology Facility/Site Codes Antipassback Video

Video Surveillance System Interface:

☒ Enable Video Surveillance System Interface

Video System Model
SEVMS-SBB

Server IP Address or Hostname *

User Name * Password *

Password (confirm) *

Test connection

Cameras

Refresh the camera list

Enable Video Surveillance System Interface - Check this box to enable the interface between **bright blue** and the video server.

Video System Model - Use this drop down box to select either the 3VR or the SEVMS-SBB DVR.

Server IP Address or Hostname - Enter the server IP address or Hostname of the video server here. (See the install manual for details.)

User Name - Enter the user name of the video server account: schlage

Password - Enter the password of the video server account: schlage

Password (confirm) - Re-enter the password of the video server account for confirmation: schlage

Test connection - Click this button to test the connection between **bright blue** and the video server.

Cameras - Shows a list of cameras that are connected to the video server.

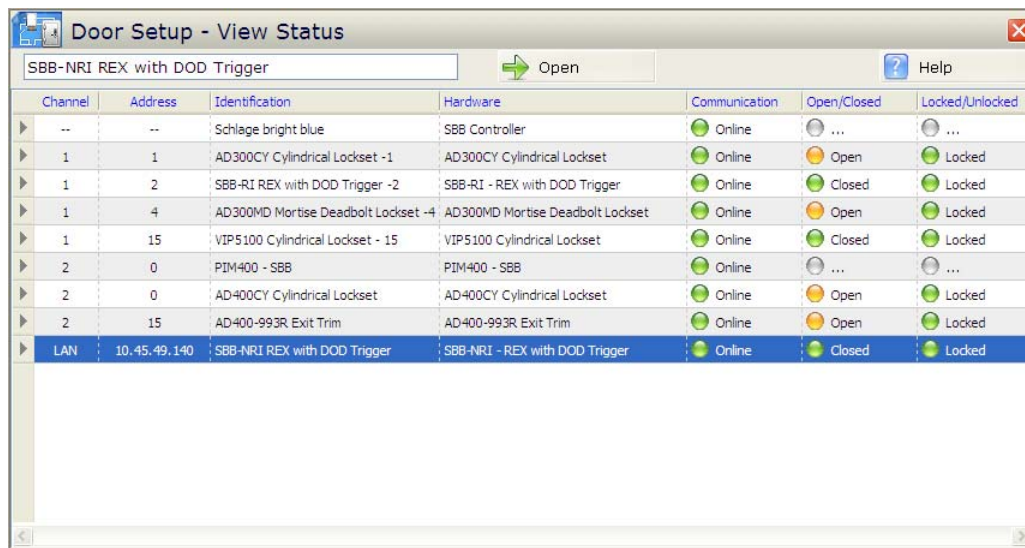
Refresh the camera list - Refreshes the camera list to show any new information on cameras connected to the video server.

Test/Monitor:

Viewing installed hardware status

The Door Setup - View Status window allows the user to view the status of the doors in the system. A list of all of the doors in the system is displayed in the status table. This table displays the following status of the door:

- Online vs. Offline
- Open vs. Closed
- Lock vs. Unlocked.



Channel	Address	Identification	Hardware	Communication	Open/Closed	Locked/Unlocked
--	--	Schlage bright blue	SBB Controller	Online
1	1	AD300CY Cylindrical Lockset -1	AD300CY Cylindrical Lockset	Online	Open	Locked
1	2	SBB-RI REX with DOD Trigger -2	SBB-RI - REX with DOD Trigger	Online	Closed	Locked
1	4	AD300MD Mortise Deadbolt Lockset -4	AD300MD Mortise Deadbolt Lockset	Online	Open	Locked
1	15	VIP5100 Cylindrical Lockset - 15	VIP5100 Cylindrical Lockset	Online	Closed	Locked
2	0	PIM400 - SBB	PIM400 - SBB	Online
2	0	AD400CY Cylindrical Lockset	AD400CY Cylindrical Lockset	Online	Open	Locked
2	15	AD400-993R Exit Trim	AD400-993R Exit Trim	Online	Open	Locked
LAN	10.45.49.140	SBB-NRI REX with DOD Trigger	SBB-NRI - REX with DOD Trigger	Online	Closed	Locked

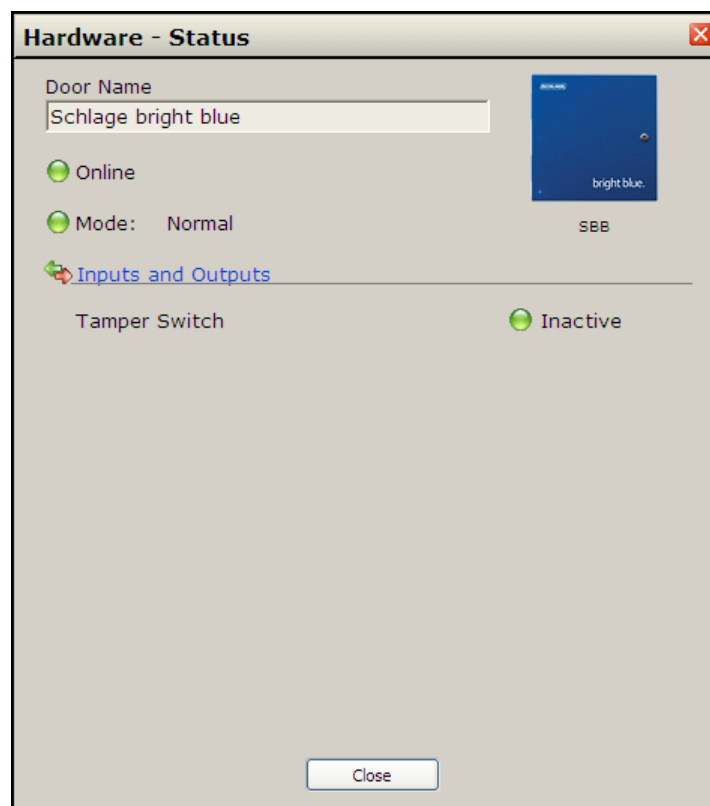
Status Table

The status table is located in the center of the Door Setup - View Status window.

- **Identification** - Shows the name of the door.
- **Hardware** - Shows the type of security hardware that is installed on the door.
- **Communication** - Shows if the door is communicating with the system or not.
- **Open/Closed** - Shows the open/closed status of the door.
- **Locked/Unlocked** - Shows the lock status of the door.

To view a more detailed status of the door, highlight the door then click the **Open** button or double click the door. This will bring up a **Hardware - Status** pop-up window with information specific to the security hardware installed on that door.

bright blue Controller Status



- **Mode** - Shows what state the controller is in.
- **Tamper Switch** - Shows whether the tamper switch is active or not.

AD-300 Status

Hardware - Status

Door Name

AD300MD Mortise Deadbolt Lockset -4

Online

PIN Required: No

Mode: Normal

AD300MD

Inputs and Outputs

Door Position Switch (DOD)	Open
Clutch Position	Locked
Exit Request (REX)	Inactive
Deadbolt Position	Extended
Status of Key Switch	Not Engaged
Tamper Switch	Active
Battery Status	N/A
Interior Push Button	Inactive

Close

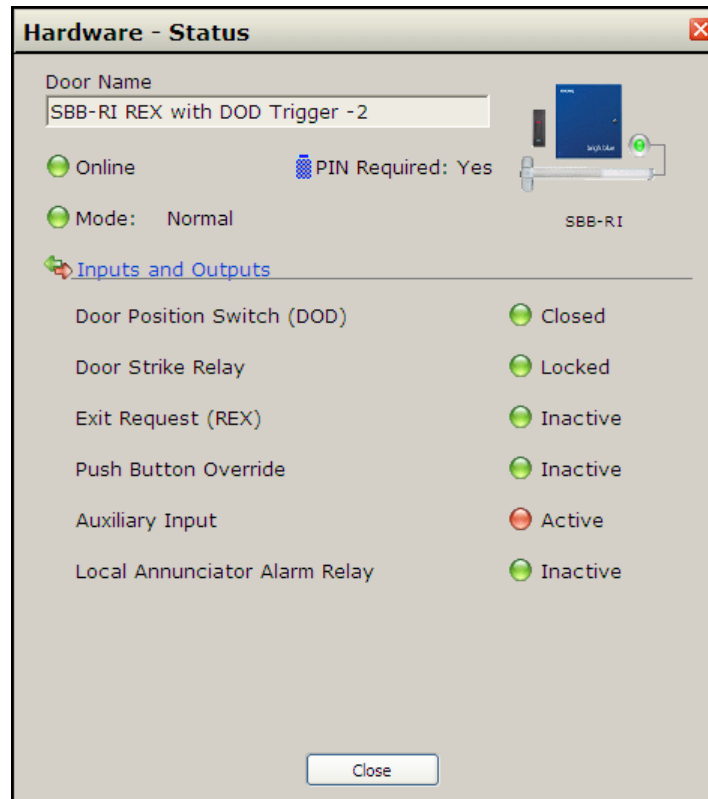
- **PIN Required** - Shows whether a PIN is required at this time or not.
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Clutch Position** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Status of Key Switch** - Shows whether the key switch is engaged or not.
- **Tamper Switch** - Shows whether the tamper switch is active or not.
- **Batter Status** - Not applicable with this lock.
- **Interior Push Button** - Shows whether the interior push button is active or not.

VIP Status



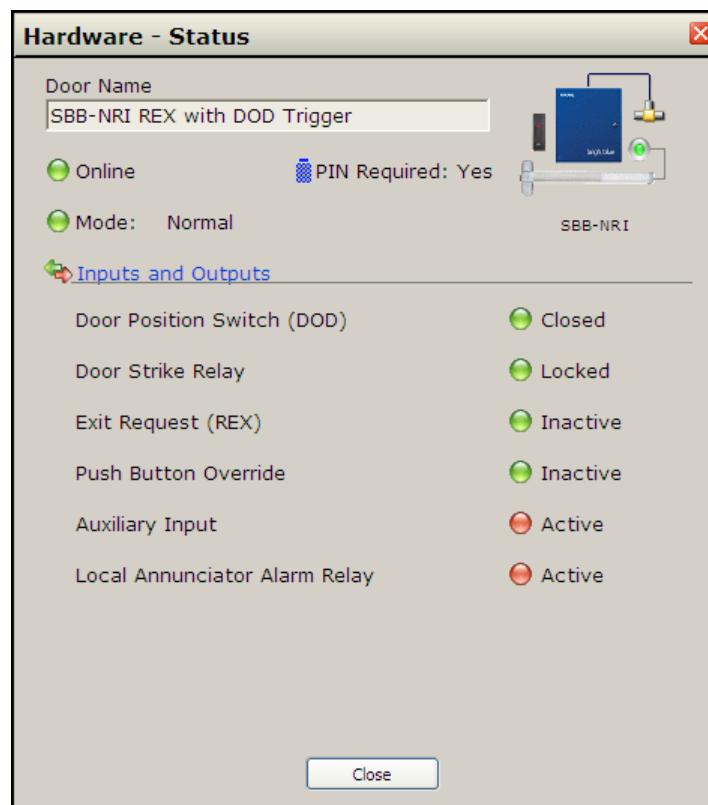
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Status of Key Switch** - Shows whether the key switch is engaged or not.

SBB-RI Status



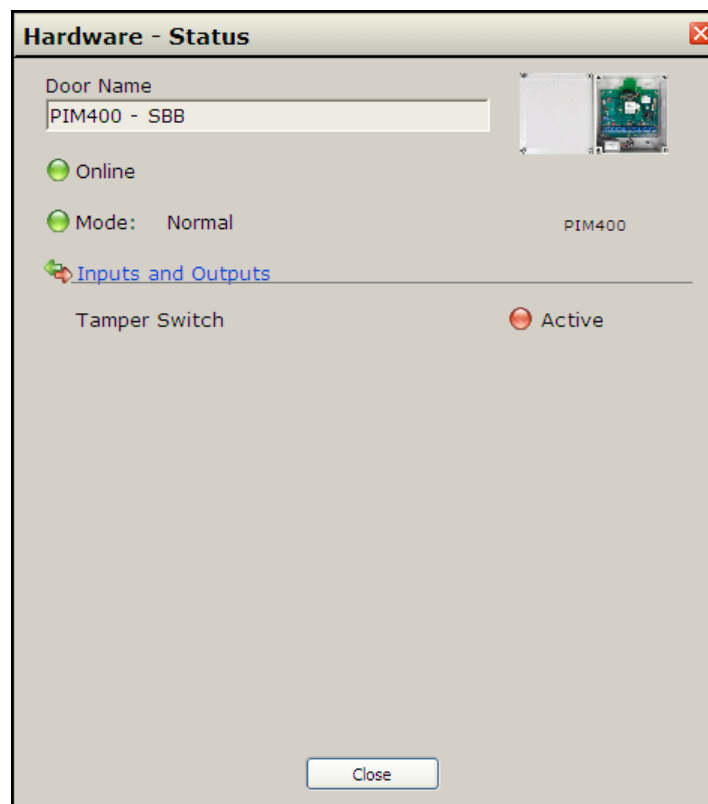
- **PIN Required** - Shows whether a PIN is required at this time or not.
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Auxiliary Input** - Shows whether there is any activity on the auxiliary input.
- **Push Button Override** - Shows whether this is a push button override connected to this lock.
- **Local Annunciator Alarm Relay** - Shows the status of any alarm relay connected to this lock.

SBB-NRI Status



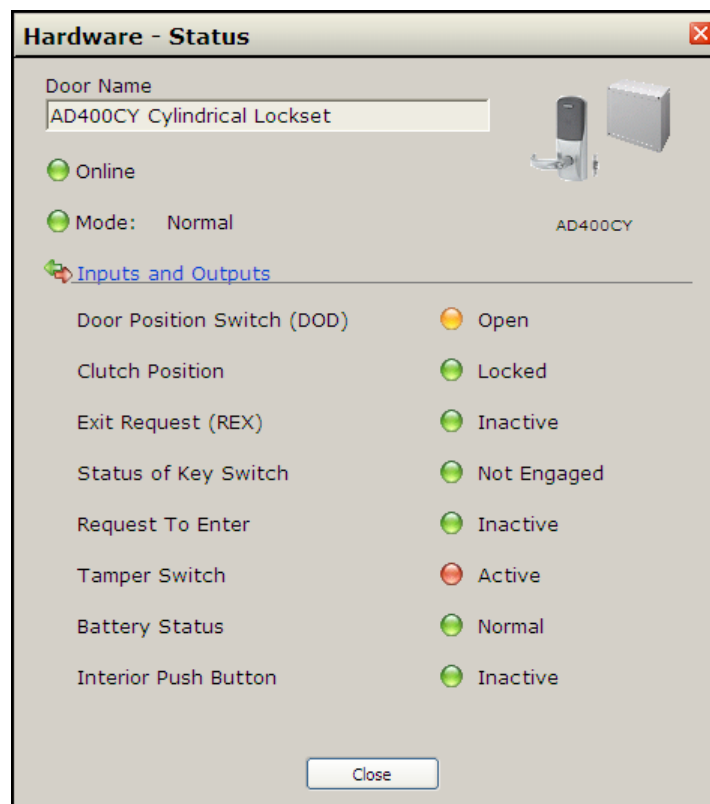
- **PIN Required** - Shows whether a PIN is required at this time or not.
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Push Button Override** - Shows whether this is a push button override connected to this lock.
- **Auxiliary Input** - Shows whether there is any activity on the auxiliary input.
- **Local Annunciator Alarm Relay** - Shows the status of any alarm relay connected to this lock.

PIM400-SBB Status



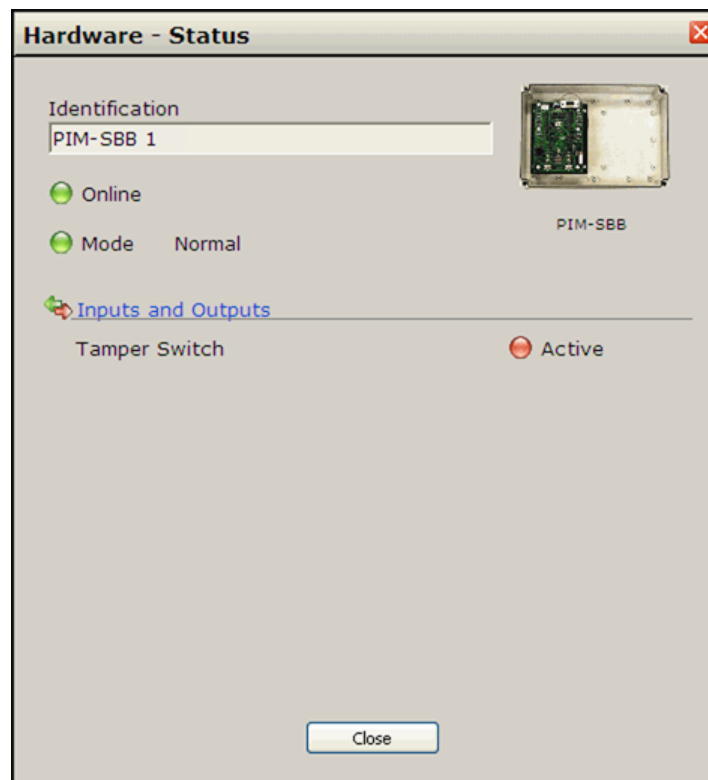
- **Mode** - Shows what state the PIM is in.
- **Tamper Switch** - Shows whether the tamper switch is active or not.

AD-400 Status



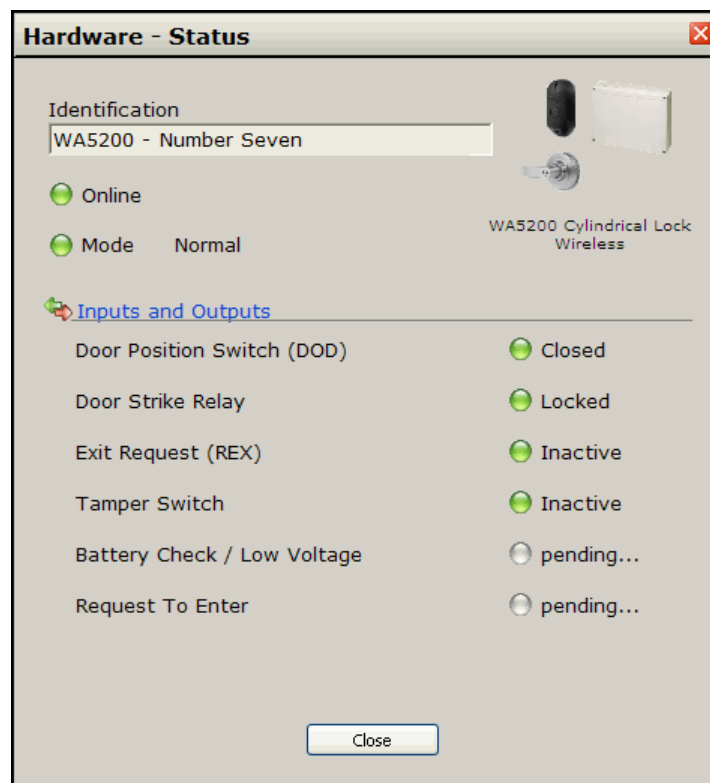
- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Clutch Position** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Status of Key Switch** - Shows whether the key switch is engaged or not.
- **Request To Enter** - Shows whether there is a Request to Enter associated with this door.
- **Tamper Switch** - Shows whether the tamper switch is active or not.
- **Batter Status** - Shows the battery status of the lock.
- **Interior Push Button** - Shows whether the interior push button is active or not.

PIM-SBB Status



- **Mode** - Shows what state the PIM is in.
- **Tamper Switch** - Shows whether the tamper switch is active or not.

WAPM Status



- **Mode** - Shows what state the door is in.
- **Door Position Switch (DOD)** - Shows whether the door is open or closed.
- **Door Strike Relay** - Shows whether the door is locked or unlocked.
- **Exit Request (REX)** - Shows whether there is a REX associated with this door.
- **Tamper Switch** - Shows whether the tamper switch is active or not.
- **Battery Check/Low Voltage** - Shows whether the low voltage switch is active.
- **Request To Enter** - Shows whether there is a Request to Enter associated with this door.

Account Administration

CHAPTER 11

Introduction

The Account Administration screen is used to set up system user accounts. System users are those individuals that administer or manage the **bright blue** system. Here, accounts can be added or edited. The Account Administration window can be accessed by clicking on the Account Administration button on the left side of the main screen. This screen is only visible when logged in as an administrator.

Note: When changing or creating a new password, the password must be a minimum of 5 alphanumeric characters. No special symbols are allowed. The password field is case sensitive.

To edit an existing account, double click on the account in the System User Accounts section of the window. There are three types of system user accounts that can be created: Administrator, Manager and Operator. Each user account is detailed below.

The screenshot shows the 'Account Administration' window with a toolbar containing 'New User', 'Save User', 'Delete User', and 'Help'. The main area has input fields for 'Last Name *' (Doe), 'First Name' (John), and 'Middle Name/Initial'. A 'Security Level' section has radio buttons for 'Administrator', 'Manager' (selected), and 'Operator'. Below is a 'Login Information' section with 'User ID *' (John D), 'Password *' (masked), and 'Password * (confirm)' (masked). At the bottom is a 'System User Accounts' table.

User ID	System User	Security Level
▶ John D	Doe, John	Manager
▶ Jane S	Smith, Jane	Operator
▶ test	test, test	Administrator
▶ User	Clark, Aaron B	Administrator

Administrator

The Administrator account is the highest level account and provides the user with full functionality of the system. The system is set up with a default administrator account of **usr** and a default password of **password**. It is strongly recommended that the Administrator change the default password.

Manager

The Manager account is the next level down from the Administrator account. The Manager security level is intended for users that will be assisting the administrator. They have the ability to manage users and time related functions but will not be able to modify doors or any system level settings. A Manager account has access to the following navigation buttons:

- Activity
- Reports
- Personnel
- Access Assignments
- Time Zones
- Calendar
- Door Status & Control

Operator

The Operator security level user account. An operator has read-only access, meaning that information can be viewed but not modified. An Operator has access to the following navigation buttons:

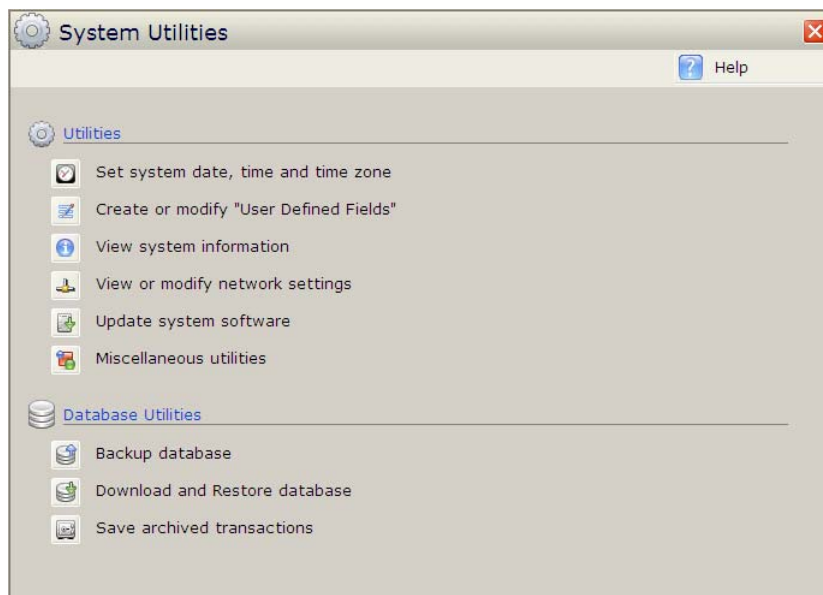
- Activity
- Reports
- Personnel

Utilities

CHAPTER 12

Introduction

The System Utilities page is split into two sections. The Utilities section is used to set system date and time, create and modify User Defined Fields, view system information and update network settings and system software. The Database Utilities sections is used to restore or delete the database and to save archived transactions to the PC. The System Utilities window can be accessed by clicking on the Utilities button on the left side of the main menu. This section is only accessible by users with Administrator security level.

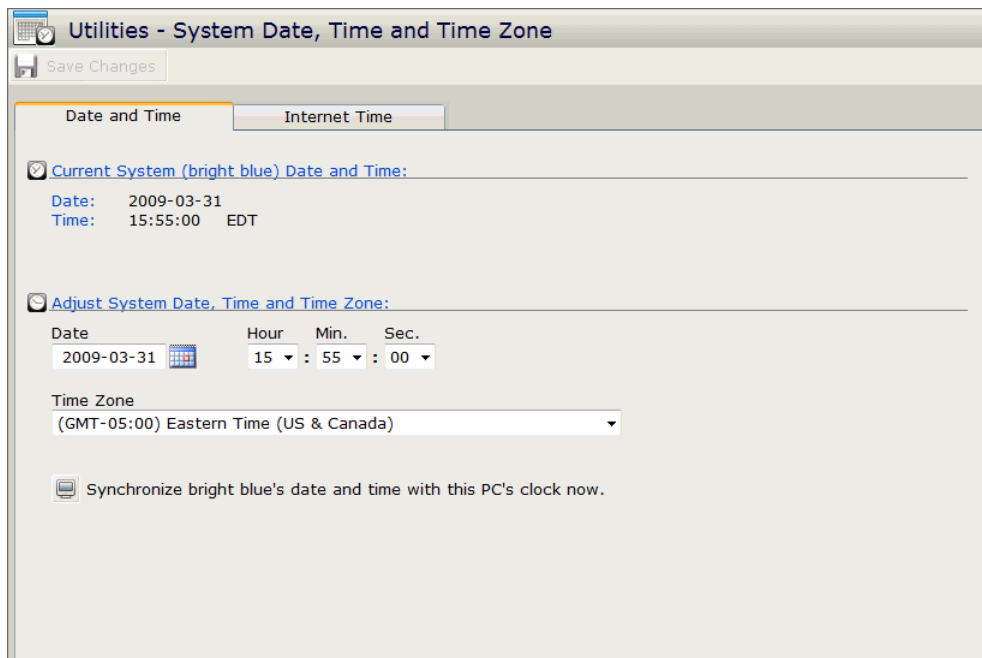


Set system date, time and time zone

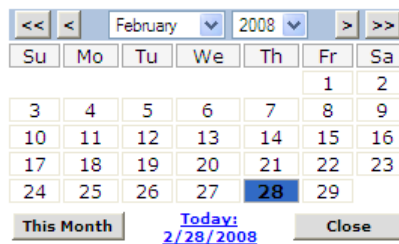
There are four ways of setting the date and time: 1) Manually 2) synchronize with a PC's clock 3) synchronize with video surveillance system 4) synchronize with an internet time server.

To set the time manually:

- 1 Click on the **Utilities** button on the left side of the main screen. The System Utilities window will open.



- 2 Click on the Set system date, time and time zone button. The Utilities - System Date, Time and Regional Time Zone window will open.
- 3 Using the Time drop down boxes, specify the time.
- 4 Click on the calendar button to the right of the Date field. The calendar pop-up will open.



- 5 Select the date. The calendar pop-up will close.
- 6 Select the time zone from the Time Zone list.

- 7 Click on the **Save Changes** button. The system time, date, and time zone will be updated.

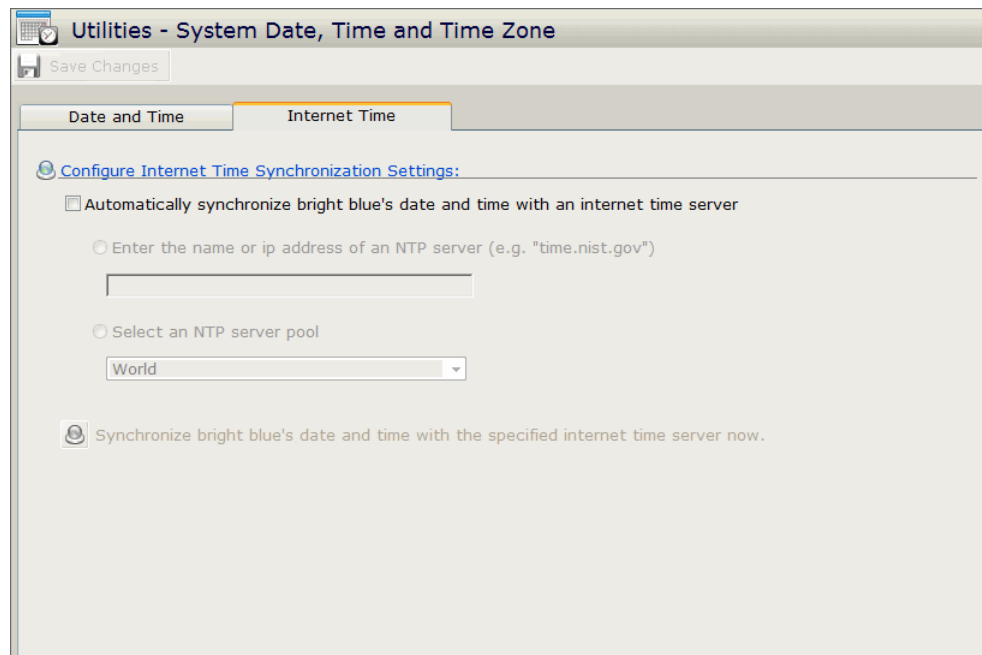
To synchronize time to the PC's clock:

- 1 Using the **Time Zone** drop down box, select which time zone you are in.
- 2 Click **Synchronize bright blue's date and time with this PC's clock now**. A confirmation window will open.
- 3 Click on **OK**. The window will close a progress bar will open. The progress bar will close and the Success pop-up window will open.
- 4 Click on **Close**. **bright blue**'s time has been synchronized to the PC.

To synchronize to an internet time server:

Note: The Internet Time tab will be disabled if the **bright blue** controller is configured to be used with a video surveillance system.

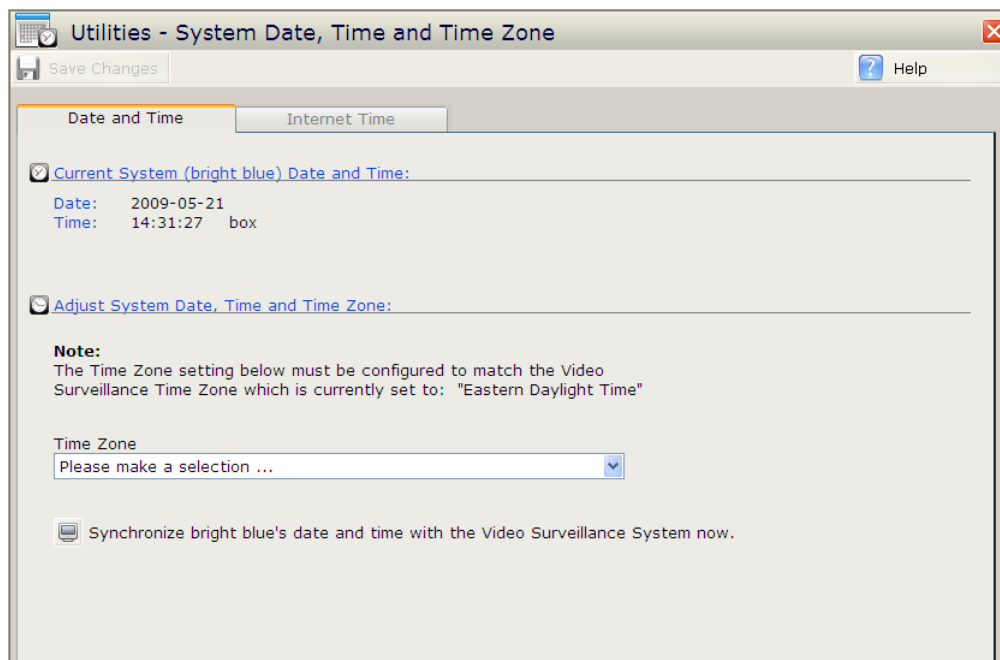
- 1 In the **Date and Time** tab use the **Time Zone** drop down box to select the Time Zone you are in.
- 2 Click on the **Internet Time** tab.



- 3 Click on the **Automatically synchronize bright blue's date and time with an internet time server** button.
- 4 Click on the **Enter the name or IP address of an NTP server** button if you wish to manually enter an NTP server.
 - a) Enter the name of the NTP server in the field provided.or
- 5 Click on Select an NTP server pool button.
 - a) Select an option from the drop down box.

- 6 Click on the **Synchronize bright blue's date and time with the specified internet time server now** button. A confirmation pop-up will open.
- 7 Click on **OK**. A progress bar will open. When it closes the Success pop-up window will open.
- 8 Click on **OK**.
- 9 Click on the **Save Changes** button at the top of the screen. The **bright blue** time will now synchronize with the specified NTP server once a day.

To synchronize with video surveillance system:

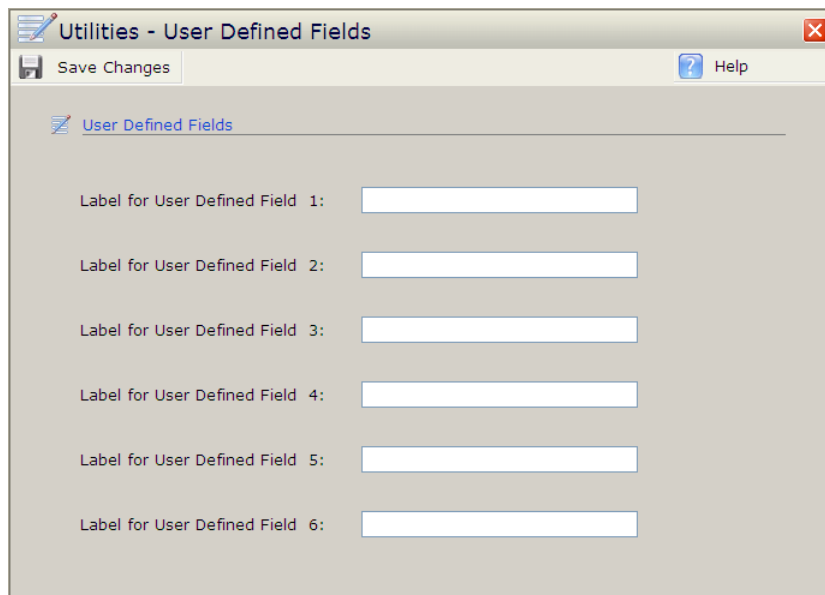


Note: This option will only appear if Video Surveillance System is enabled in **Door Setup - Global Settings**.

- 1 Using the **Time Zone** drop down box, select which time zone you are in.
- 2 Click **Synchronize bright blue's date and time with the Video Surveillance System now**. A confirmation window will open.
- 3 Click on **OK**. The window will close a progress bar will open. The progress bar will close and the Success pop-up window will open.
- 4 Click on **OK**.
- 5 Click on the **Save Changes** button at the top of the screen. **bright blue's** time has been synchronized to the Video Surveillance System.

Create or modify User Defined Fields

Clicking on this button will open the Utilities - User Defined Fields window. Here up to 6 user defined fields can be specified to be displayed in the personnel records. The names for these fields can be up to 32 characters long.



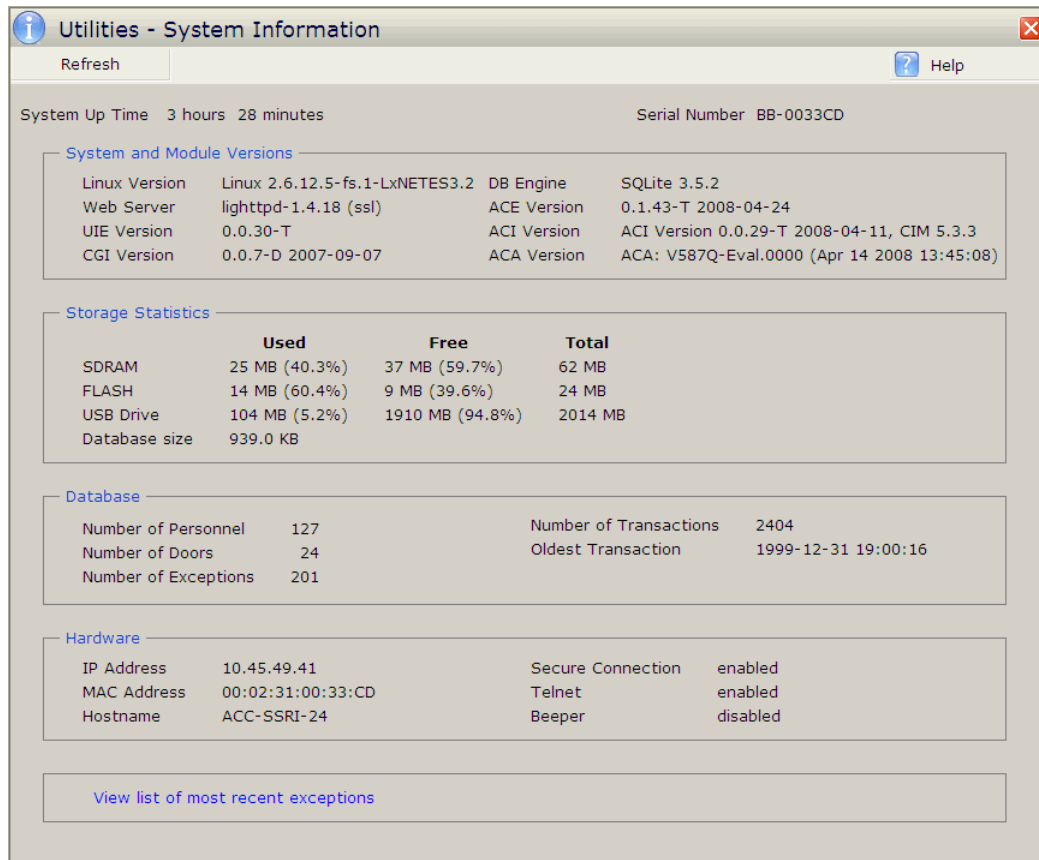
The screenshot shows a window titled "Utilities - User Defined Fields". At the top, there is a toolbar with a "Save Changes" button (floppy disk icon) and a "Help" button (question mark icon). Below the toolbar, the window contains a section titled "User Defined Fields" with a pencil icon. This section lists six user-defined fields, each with a label and a corresponding text input field:

- Label for User Defined Field 1:
- Label for User Defined Field 2:
- Label for User Defined Field 3:
- Label for User Defined Field 4:
- Label for User Defined Field 5:
- Label for User Defined Field 6:

- **Label for User Defined Field 1 - 6** - Enter up to 6 different labels to be used in the personal information section of the Personnel screen.
- **Save** - Click on this to save the user defined field labels.

View System Information

Clicking this button opens the Utilities - System Information window.



- **Refresh** - Clicking this button will refresh the window so that it shows the most current information.
- **System and Module Versions** - This section displays information on the version numbers of the various applications in **bright blue**.
- **Storage Statistics** - This section displays information on the used, free, and total storage space of the various memory types in **bright blue**.
- **Database** - This section displays information on the **bright blue** database.
- **Hardware** - This section displays information on the **bright blue** hardware.
- **View list of most recent exceptions** - Clicking on this button opens the Exceptions page. The Exceptions page displays the most recent system exceptions.

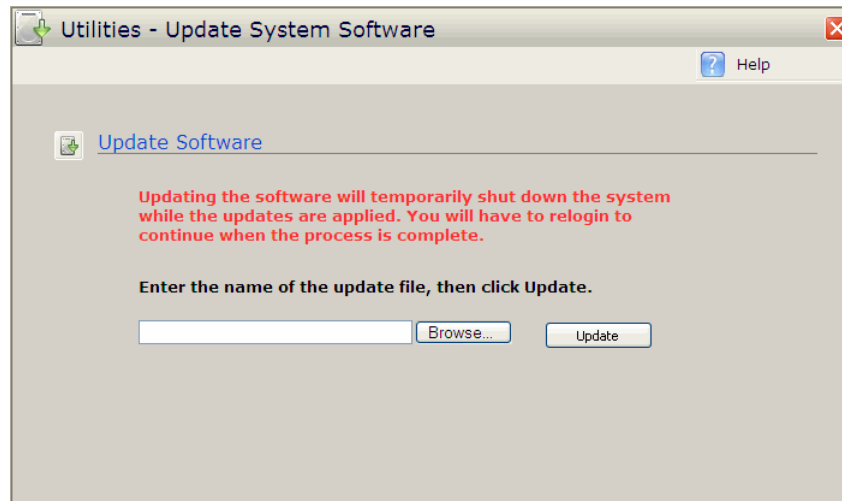
View or modify network settings

Clicking on this button opens the Network Settings window. From here network settings can be viewed and altered.

- **Hostname** - Displays the hostname of the **bright blue** controller.
- **Domain/Workgroup** - Displays the current workgroup name.
- **DHCP** - Click on this button to enable DHCP. This will disable Static IP.
- **Static IP** - Click on this button to enable static IP. This will disable DHCP.
 - **IP Address** - Displays the current IP address.
 - **Subnet mask** - Displays the current subnet mask.
 - **Default gateway** - Displays the current default gateway.
- **Obtain DNS server address automatically** - Click on this button to automatically configure DNS server addresses. This option will be disabled if Static IP is being used.
- **Manually configure DNS server address** - Click on this button to manually configure DNS server addresses.
 - **Primary DNS server** - Displays the primary DNS server.
 - **Secondary DNS server** - Displays the secondary DNS server.
- **Save Changes** - Click on this to save any changes to the network settings.

Update system software

Clicking on this button opens the Utilities - System Software Update window. From here, updates to the **bright blue** software can be uploaded to the system.



- **Browse** - Click on this button to select the software update file. The **Choose file** pop-up window will open. Find the file on the local machine or on the network and select it. Click on **OK**. The file name will display in the field to the right of the browse button.
- **Update** - Click this button to update the software once the update file has been selected.

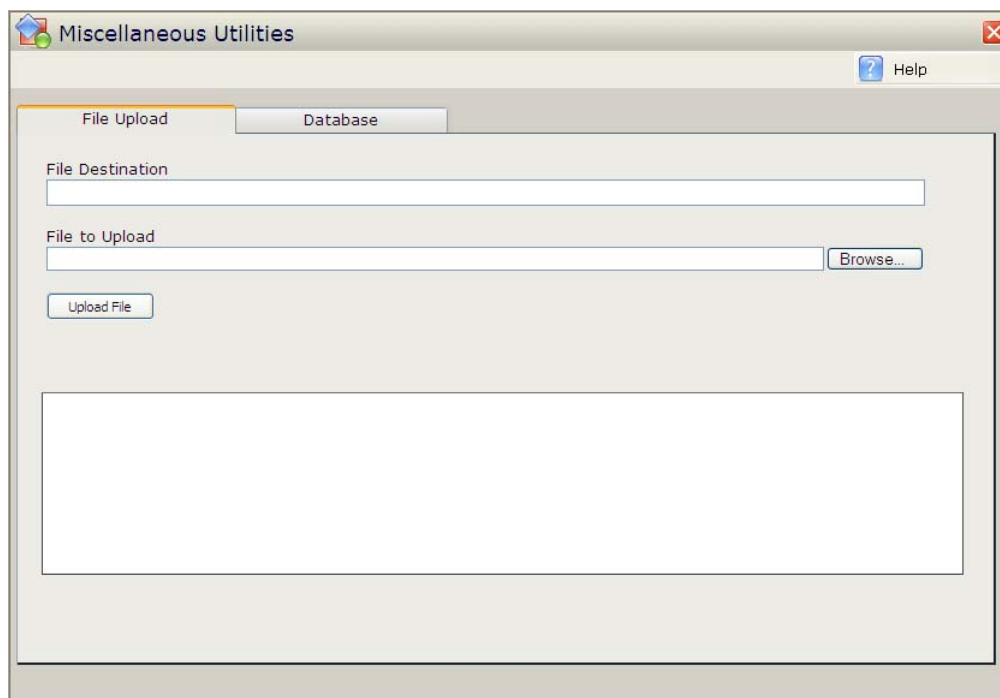
Miscellaneous Utilities

Clicking on this button opens the Miscellaneous Utilities window. From here, individual files of the **bright blue** software can be updated and the database can be cleared. This section is password protected and cannot be accessed without help from Schlage technical support.



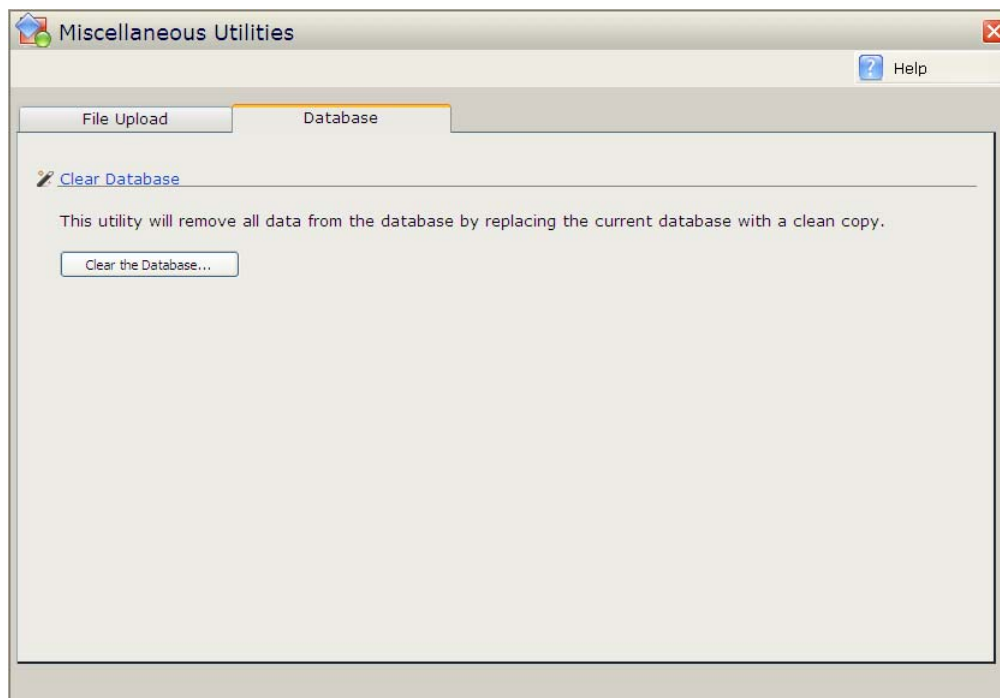
- **Password** - Enter the password into this field.
- **OK** - Click on this button once the password has been entered. The pop-up will close and the Miscellaneous Utilities window will open.
- **Cancel** - Click on this button to close the pop-up and return to the main Utilities window.

File Upload tab - Use this section to upload individual **bright blue** software files.



- **File Destination** - Enter the destination of the uploaded file.
- **File to Upload** - Enter the location of the file to be uploaded.
- **Browse** - Click on this button to browse for the file to be uploaded.
- **Upload File** - Once the file has been located and the destination specified, click on this button to upload the file.

Database tab - Use this section to clear the database of all data by over-writing current data with a clean copy.



- **Clear the Database** - Click on this button to clear the database.

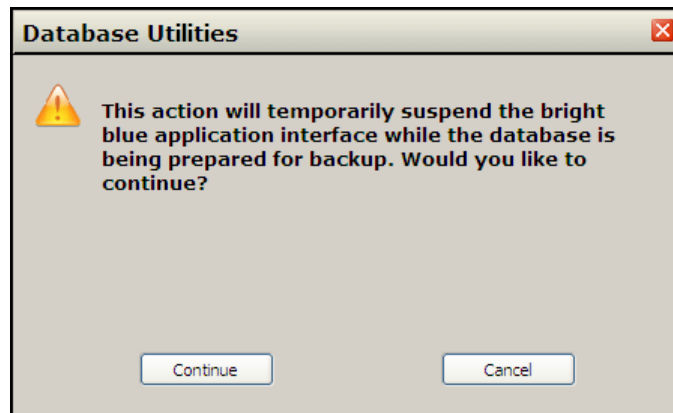
Database Utilities

The Database Utilities section of the Utilities screen has three buttons that affect the status of the **bright blue** database: **Backup Database**, **Download and Restore database**, and **Save archived transactions**.

Backup Database

This button is used to backup the database. To backup the database follow the steps below.

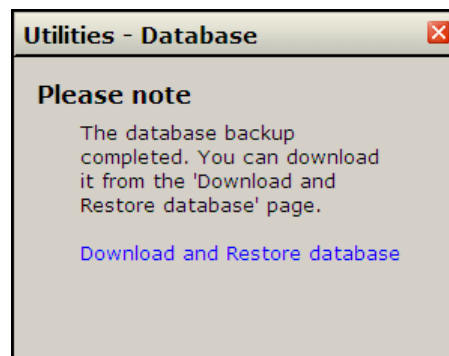
- 1 Click on the **Backup Database** button. The Backup confirmation pop-up window will open.



- 2 Click on **Continue**. The pop-up window will close and the progress window will open.

NOTE: the system will be temporarily disabled while the database is backed up.

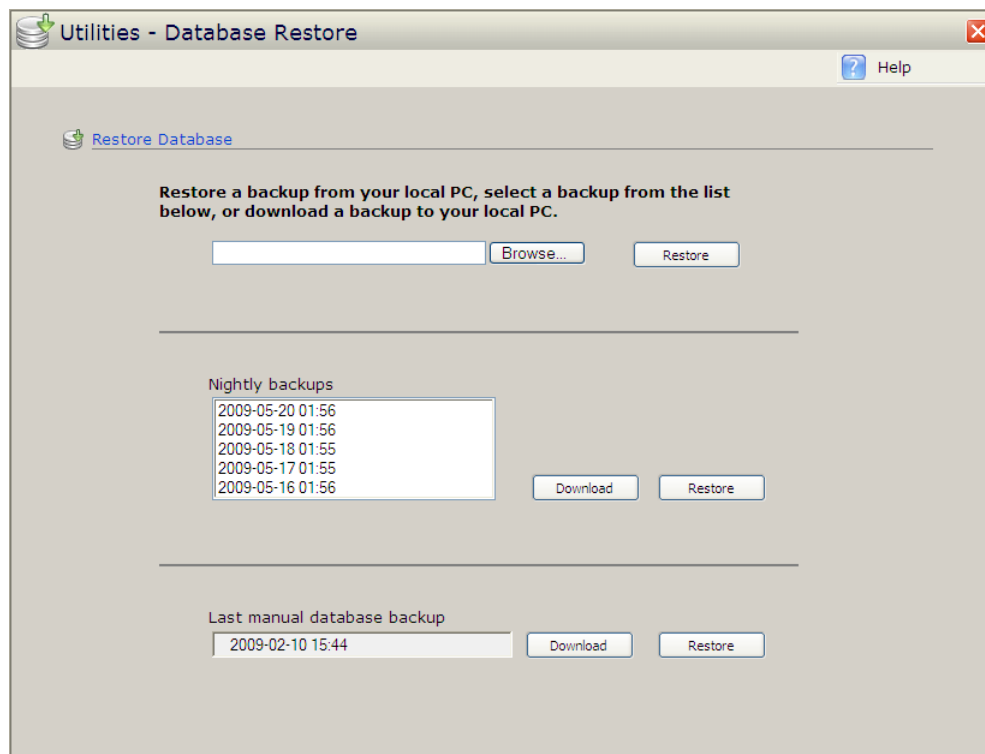
- 3 When the progress window finishes the database will be backed up and the **Please note** pop-up window will open.



- 4 From here either:
 - a) Click on the **X** button in the top right corner of the pop-up to close it and return to the Utilities main page or
 - b) Click on **Download and Restore database** to go to the Download and Restore database page.

Download and Restore database

Clicking this button opens the Utilities - Database Restore window. From here an archived database can be saved to the PC or restored.



Restore a backup from your local PC, select a backup from the list below, or download a backup to your local PC.

- **Browse** - Click on this button to open the Choose File pop-up window. From this pop-up select the database file to be restored.
- **Restore** - Once a database file has been selected click on this button to restore that database.

Nightly backups

- **Download** - Click this button to download the selected database to a PC.
- **Restore** - Click this button to restore the selected database.

Last manual database backup

- **Download** - Click this button to download the selected database to a PC.
- **Restore** - Click this button to restore the selected database.

How to restore a database

There are two ways of restoring a database. 1) From a database stored on **bright blue**. 2) from a database stored on the PC.

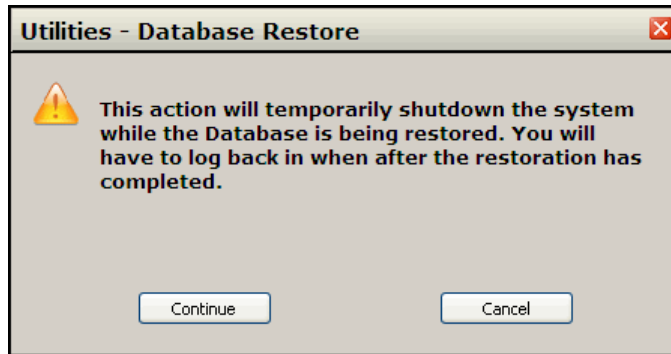
Restoring a database from a PC.

- 1 Click on the **Utilities** button on the left side of the main screen. The System Utilities window will open.
- 2 Click on the **Browse** button. The Choose File pop-up window will open.



- a) Select the database file to be restored.
- b) Click on the **Open** button. The pop-up will close and the name and location of the file will appear in the browse window.

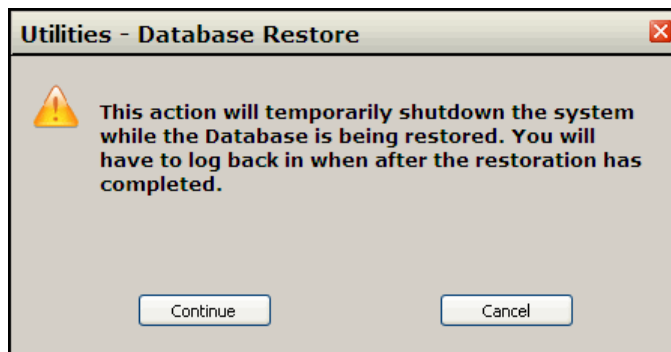
- 3 Click on the **Restore** button. After a moment the Database Restore pop-up will open.



- a) Click on the **Continue** button. **bright blue** will temporarily shut down while the database is restored.

Restoring a database from **bright blue**:

- 1 Click on the **Utilities** button on the left side of the main screen. The System Utilities window will open.
- 2 Select a saved database from:
 - a) the list provided in the **Nightly backups** section.
 - or
 - b) the **Last manual database backup** section.
- 3 Click on the **Restore** button. After a moment the Database Restore pop-up will open.

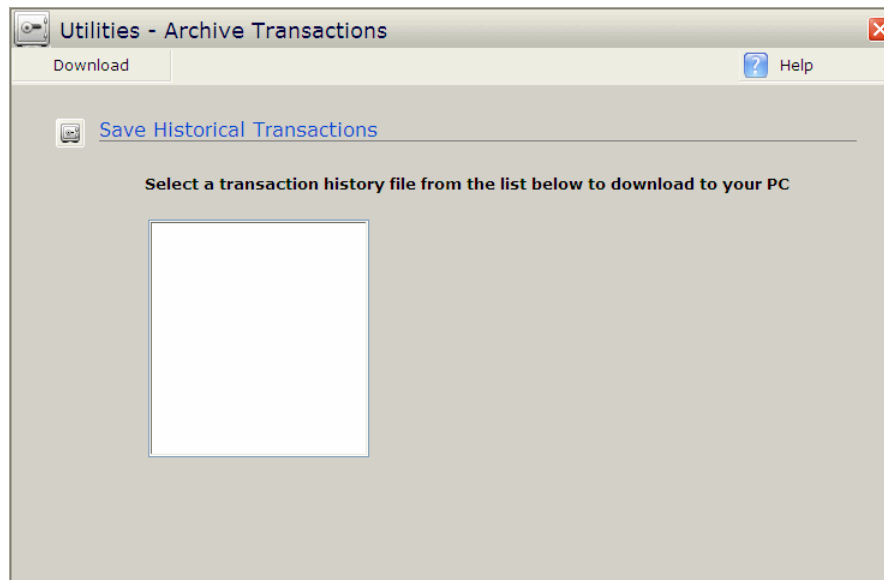


- a) Click on the **Continue** button. **bright blue** will temporarily shut down while the database is restored.

Note: The system will temporarily shut down while restoring the database. Doors will not be in their Enhanced Security state during this time and no system activity will be logged.

Save archived transactions

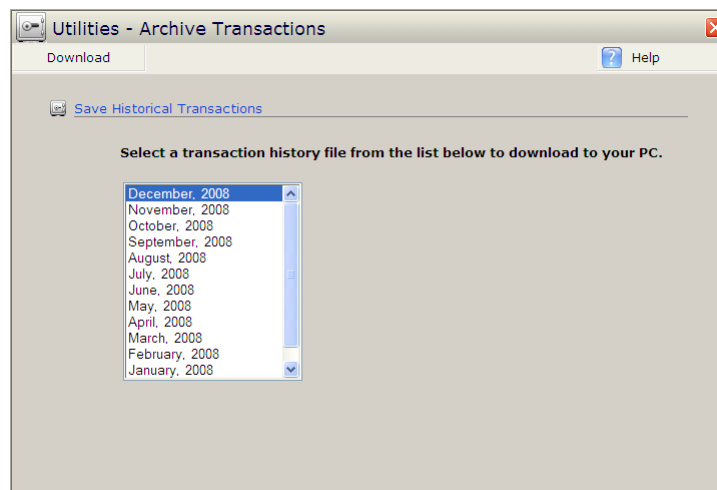
Clicking on this button opens the Archive Transactions window. From here archived transaction history files can be saved to a PC.



- **Download** - Click on this button to download a selected history file to a PC.

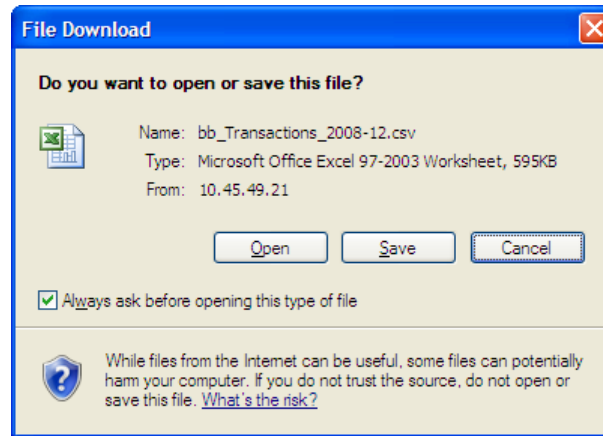
To access the archived history:

- 1 Go to Utilities
- 2 Click on the **Save archived transactions** button. The Archived Transaction window will open.



- 3 Select the month you wish to download.

- 4 Click on the **Download** button. The File Download window will open.



- 5 Click on the **Save** button. The Save As window will open.
- 6 Select where the file will be saved.
- 7 Click on the **Save** button. The transaction history file will be saved to your computer.
- 8 Use Excel (or other csv. spreadsheet program) to open the file and view the information.

Note: MS Excel has a 65,535 line maximum. If your history files are larger than this you will need to use a different spreadsheet program to view all the history.

Glossary of Terms

1

1st Person In

This is a rule that can be applied to a door. If an **Unlock Time Zone** is applied this door and this rule is selected, the door will not automatically unlock unless a valid credential is presented within the specified time zone.

A

Access Blocked

Immediately prohibits entry or exit from a reader. This field overrides all area access privileges and activation or expiration dates.

Anti-passback

A process that prevents a card from being presented at the same entry or exit reader twice in a row. Once a card is presented at an entry reader, it must then be presented at an exit reader. This function is used to restrict cardholders from passing their badge to another person for illegal entry.

B

BASH

BASH or Bourne Again SHell is the POSIX compatible shell (command interpreter or command line) that is used to pass commands to Linux.

C

Calendar Events

Calendar Events are user definable events that override the normally scheduled unlock time zones and users' permitted access time zones. If the option **Includes scheduled "Calendar Events"** is selected in a time zone, the Calendar Event will not override the time zone.

CDT (Configuration and Demonstration Tool)

Utility for configuring Schlage Wireless Access products. The CDT will run in Microsoft Internet Explorer 5.0 or later and requires Microsoft Java Virtual Machine.

Comma Separated Value

.csv stands for Comma Separated Value. A file that ends with the .csv extension is a text file that can contain several records/fields. Fields are separated in a .csv file by commas.

Credential

A physical or logical object used at a reader to prove one's identity; credentials for **bright blue** are either Proximity or Magstripe cards.

D

Driver

A program used by the operating system to run hardware such as printers, video or sound cards.

E

Encoded ID

A unique numeric value that is required to add a badge to a cardholder record. For instance, a proximity card has a chip programmed with the number. A magnetic stripe card will have the number embedded in the stripe.

Encryption

Data is coded using a special algorithm to provide confidentiality and to prevent hackers from reading private information.

Enhanced Security

Enhanced Security is a feature that is used to enable/disable door access during a system start up. If **bright blue** has to restart for any reason while it is loading its database the doors in the system will be, by default, put into enhanced security mode. This means that, during a system start-up, any personnel with a credential with the correct Facility/Site code will be given access to a door whether or not that person would normally have access rights to that door. If you wish to disable this feature, and make it so a door remains locked during a system start-up, no matter what credential is presented, then check the **Disable door access during system start-up** option in Advanced Tab of the Door Setup section.

Expiration Date

The fields used to define when a cardholder record or area access permissions will terminate.

F

File Server

A file server (FS) is a robust, high-speed computer with substantial memory, hard disk space and processing power. It maintains all of the system database files and communicates with workstations and the System Processor. Only system administrators should have permission to a file server. Filter A software operation that allows only selected and limited data to appear on the monitor or report.

H

Hardware

Any physical component of the access control system such as the **bright blue** controller, locks, readers, etc.

I

Issue Code

The number that represents how many badges have been added to a cardholder record. The first badge is Issue Code 1; the second badge is Issue Code 2 and so on. This is not a required field.

L

Linux

A Unix-like operating system created by Linus Torvalds that is available under the GNU General Public License.

Log out

An exit procedure performed by a System User at the conclusion of a software session.

Login

A procedure performed at the beginning of a software session by a System User that usually requires entering both a user name and password to gain access to an application.

O

Operating System

The main computer program that runs all other applications and is responsible for basic tasks and security.

P

PDF

Portable Document Format. Software distributed by Adobe Acrobat that allows files to be viewed and printed over several platforms.

PIM (Panel Interface Module)

Module used to connect the **bright blue** controller to Schlage Wireless locksets.

POSIX

POSIX stands for Portable Operating System Interface. It is the set of IEEE standards that were established to ensure compatibility between different distributions of Unix.

Processor

One of the most important and powerful pieces of computer hardware. It executes numerous commands and instructions.

R**REX (Request to exit)**

A contact type programmed on the Contact Definition window.

RI (Reader Interface)

The RI is a physical hardware device that reads the access card. It connects the Read Head to the system controller board. The RI will support one Read Head, one or two relays and 7 contact inputs

RS485

A serial communication standard that is used by many access control systems to communicate to readers, reader boards and/or locking devices.

S**SBB-RI**

Schlage **bright blue** Reader Interface. Connects the read head to the **bright blue** controller.

Site Codes

Unique numerical values that are pre programmed into access cards. Site codes are stored at the Reader level.

Software

Programs that run on a computer

Special Access Privileges

This option allows for a longer relock time than that of a normal relock period. It is generally used in conjunction with disabled personnel.

SQL (Structured Query Language)

A powerful, relational database capable of handling large-scale applications

SSL

Secure Sockets Layer is a protocol to provide additional security over an internet connection. **bright blue** uses 128 bit encrypted https to communicate between the controller and the browser.

Stamped ID

An internal company defined numbering system that is sometimes displayed on the back of a badge. Stamped ID is not a required field to add a badge

T**TCP/IP**

Transfer Control Protocol / Internet Protocol. A common language (protocol) used by computers to communicate on the internet and with other computers.

Toggle

Toggle opens a door and leaves it open until it is closed again by a toggle credential. It toggles a door between locked and unlocked. A person with the toggle option must present their credential twice within the specified time in order to toggle a door.

Transaction

Transactions are the events that happen in **bright blue**. "Valid Access", Access Denied", Relay Energized" etc. are some examples of transactions that can occur. Every transaction is associated with a time, type and other information associated with it depending on the type of the transaction.

U

UDF (User Defined Fields)

Customized fields that can be added to Cardholder and Guest records

UTC (Universal Time, Coordinated)

This is also known as Greenwich Mean Time (GMT)

W

Workstation

A computer used by operators to access software applications, to input data, retrieve transaction information and alarms. Workstations are generally networked to a server.

Index

1

1st Person In • 213

A

Acceptable Card Formats • 109

Access • 93

Access Assignments • 112, 123

Access Blocked • 213

Access by Group • 69

Access by Person • 62

Access History • 112

Access Permission by Door • 94

Access Permission by Person • 93

Account Administration • 194

Activity • 73, 78

Activity Monitor Settings • 74

AD-400 Series • 45

Add calendar event • 151

Add doors and hardware • 167, 176

Add new person • 106

Add time zones • 145

Adding a Door • 170

Adding a PIM • 168

Adding Access Assignments to Existing Personnel • 62

Adding Personnel • 59

Administrator • 195

Advanced Search • 122

All Access Attempts Invalid • 84

All Access Attempts Valid • 82

All Access Attempts Valid/Invalid • 80

v2.1.1

Anti-passback • 172, 182, 213

B

Backup Database • 206

BASH • 213

Block / Unblock a group of people's access to the facility • 140

Block / Unblock a person's access to the facility • 133

Block/Unblock • 131

C

Calendar Events • 97, 150, 213

CDT (Configuration and Demonstration Tool) • 213

Checking Date and Time • 14

Clock Application • 147

Comma Separated Value • 213

Configuration • 97

Contacts • 88

Copy access assignments from one door to other door(s) • 142

Copy from • 127

Copying Access Assignments • 66

Create common access assignments for a group of people • 138

Create or modify User Defined Fields • 200

Credential • 213

Credential Technology • 177

Credentials • 108

D

Database Utilities • 205

Defining Time Zones • 17
Defining Users • 16
Determining Version Number of SBB-RI • 36
Devices • 95
Door Setup • 21, 166
Door Status & Control • 153
Download and Restore database • 207
Driver • 213

E

Edit Details • 126
Encoded ID • 213
Encryption • 213
Enhanced Security • 214
Expiration Date • 214
Exporting Reports • 98

F

Facility/Site Codes • 180
File Server • 214
Format requirements for imported .csv files • 115

H

Hardware • 214
How to find a card's encoded ID number • 110
How to import a .csv file • 116

I

Import personnel data • 114
Ingersoll Rand Copyright Notice • 1
Installation and Configuration • 166
Introduction • 7
Issue Code • 214

L

Linux • 214

Lockdown • 132
Log out • 214
Login • 8, 214

M

Main Page • 11
Manager • 195
Minimum System Requirements • 7
Miscellaneous Utilities • 204

O

Operating System • 214
Operator • 195

P

Pass-Through • 130
PDF • 214
Permit All • 125
Personal Info • 108
Personnel • 91, 105
Personnel Setup • 57
Personnel Transactions • 75
PIM (Panel Interface Module) • 215
PIM400-SBB • 43
PIM-SBB • 51
POSIX • 215
Processor • 215

Q

Quick Start • 13

R

Relays • 89
Remove All • 131
Reports • 78
Reset a person's antipassback state to neutral • 136

Reset everyone's antipassback state to neutral • 141

REX (Request to exit) • 215

RI (Reader Interface) • 215

RS485 • 215

S

Sample Access Report • 94

Sample Activity Report • 90

Sample Configuration Report • 98

Sample Devices Report • 96

Sample Personnel Report • 92

Save archived transactions • 210

SBB-NRI • 38

SBB-RI • 31, 215

Schlage Adaptable AD-300 Series • 21

Schlage Adaptable AD-400 Series • 43

Schlage VIP • 26

Schlage Wireless Access • 50

Searching for a Specific Record • 63, 119

Set system date, time and time zone • 197

Site Codes • 215

Software • 215

Special Access Privileges • 215

SQL (Structured Query Language) • 215

SSL • 215

Stamped ID • 215

System and Device Transactions • 77

System Events (Communications, Power, Relays, and Contacts) • 87

System User Activity • 86

T

TCP/IP • 216

Test/Monitor: • 184

Time Zone • 128

Time Zones • 97, 144

Toggle • 129, 216

Transaction • 216

U

UDF (User Defined Fields) • 216

Update system software • 203

User Defined Fields • 58

UTC (Universal Time, Coordinated) • 216

Utilities • 196

V

Video • 183

View or change a person's access assignments • 124

View or modify door configuration • 175

View or modify global settings • 176

View or modify network settings • 202

View System Information • 201

View, modify or delete calendar event • 152

View, modify or delete personnel record. • 113

View, modify or delete time zone • 148

Viewing installed hardware status • 184

W

WA Series • 53

Workstation • 216



Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure and productive. The sector's market-leading products include electronic and biometric access-control systems; time-and-attendance and personnel scheduling systems; mechanical locks; portable security; door closers, exit devices, architectural hardware, and steel doors and frames; and other technologies and services for global security markets.

860-584-9158 • 866-322-1237

www.schlage.com www.ingersollrand.com