Portal Card Access System®
User Guide

Rev. 090831

Portal Card Access System® User Guide

by Bob Hoang, Training Manager, Mykone Saunders, Creative Producer, and Olga Alexeenko, Technical Writer/Editor

Disclaimer

The Portal User Guide is provided *as is*, without warranty of any kind, expressed or implied, including but not limited to performance, merchantability, or fitness for any particular purpose. Neither i³DVR International Inc. nor its dealers or distributors shall be liable to any person or entity with respect to any liability, loss, or damage, caused or alleged to have been caused directly or indirectly by this information. Furthermore i³DVR International Inc. reserves the right to revise this publication, and to make changes to the content at any time, without notice.

This manual offers the easiest, most efficient way of wiring and configuring Portal Card Access system. In most cases, customization can be made at the installer''s discretion. i³DVR will not be held responsible for system malfunctioning as a result of improper wiring and/or configurations. The Quick Setup function in Portal software application may only be used if the suggested wiring standards are followed.

This manual is consistent with Portal Card Access System software v. 2.0.

FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: **(1)** This device may not cause harmful interference, and **(2)** this device must accept any interference received, including interference that may cause undesired operation.

Address:

i3DVR International Inc. • 780 Birchmount Road, Unit 16 • Scarborough • Ontario • Canada M1K 5H4

Tech Support: 1.877.877.7241

Web Site: www.i3dvr.com

Table of Contents

1

Initial Software Installation and Setup

Topics Covered

- Installing Portal Software on Host PC
- Basic Portal Software Configuration

This chapter describes the steps required for initial software installation on the host PC.

Host PC minimum hardware requirements:

- Window XP
- 512 RAM
- Pentium III, 500 MHz
- Super VGA Video Card
- 40 GB Hard drive
- CD/DVD drive
- COM (Serial) port
- Network interface card if RS-232 is unavailable
- .NET Framework 3.0 installed (available on Portal software CD included with the system)

1.1. Installing Portal Software on Host PC

In order to program installed hardware and to operate the Card Access System, install Portal software onto the host PC.

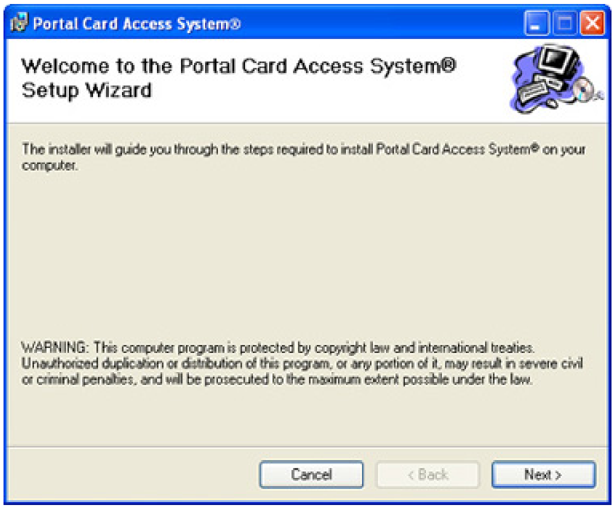
Host PC must be connected to the *first* Controller in the daisy chain network via RS-232 or TCP/IP (optional upgrade) connection.

1. Connect the P-PORTALDB9 cable to the serial COM port on the host PC. If the optional TCP/IP interface is used, connect the network cable from Portal TCP/IP converter to the RJ45 port on the motherboard or the network card of the host PC. Remember that the maximum RS-232 cable length may not exceed 150 feet (50 meters).

2. Locate and open the Portal software CD that was shipped with the Portal Card Access system.

3. Run the Portal software installation file: **setup.exe**.

4. In the first Setup Wizard window, click **Next.**



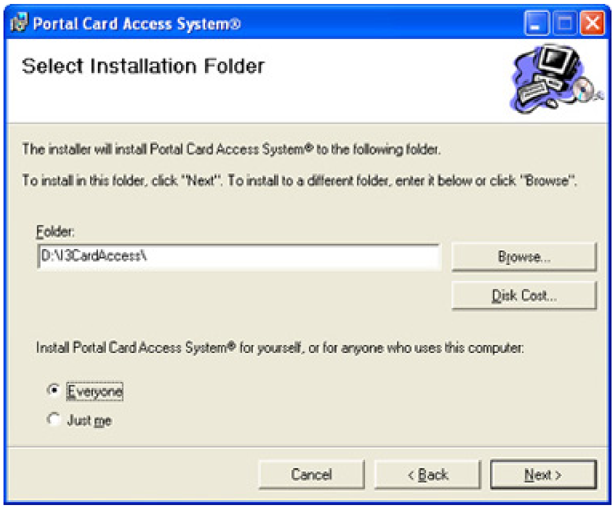
Portal Card Access System®

Welcome to the Portal Card Access System® Setup Wizard

The installer will guide you through the steps required to install Portal Card Access System® on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

5. In the second Setup Wizard window, select the software installation folder by clicking **Browse** or leave the default installation folder. Select **Everyone** or **Just me** radio button to specify who will have access to Portal software application (if you have multiple users on your PC).



Portal Card Access System®

Select Installation Folder

The installer will install Portal Card Access System® to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

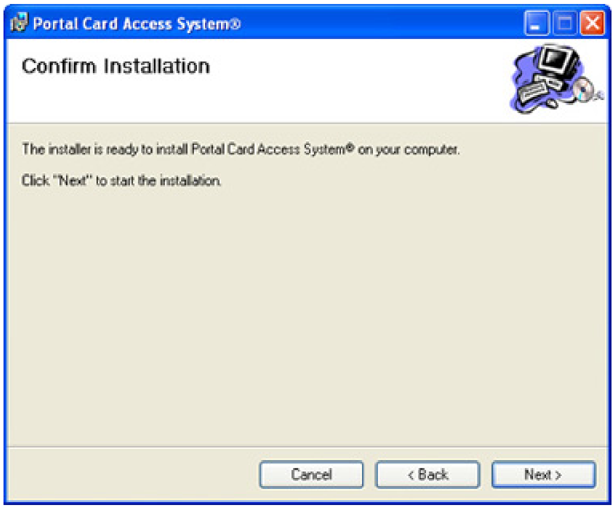
Folder: D:\I3CardAccess\

Install Portal Card Access System® for yourself, or for anyone who uses this computer:

● Everyone

○ Just me

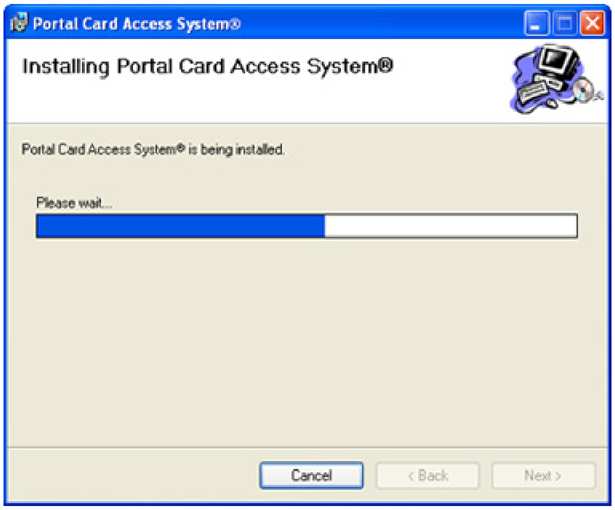
6. Click **Next** in the Confirm Installation window to proceed with the software installation.



The installer is ready to install Portal Card Access System® on your computer.

Click "Next" to start the installation.

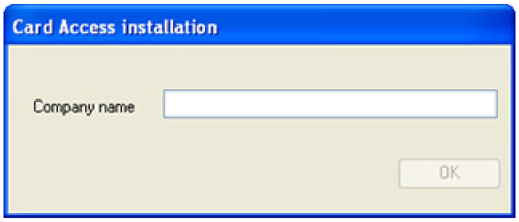
7. Wait while the software is installing on the PC.


Portal Card Access System®
Installing Portal Card Access System®
Cancel
< Back
Next >

Portal Card Access System® is being installed.

Please wait...

8. Enter the **Company name** in the next window and click **OK**.



Tip

Company name may later be edited in the Portal software setup.

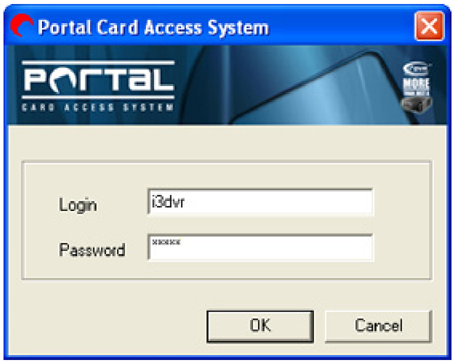
9. Wait for the Installation Complete window to be displayed. Click **Close** to complete the installation.

1.2. Basic Portal Software Configuration

To interface the installed hardware with Portal Card Access System software, follow these instructions.

1. After the portal software was successfully installed onto your Host PC, locate the Portal Card Access System software icon on the Desktop and launch the software application. Portal Card Access System®

2. In the login window, enter the default user name and password: **i3dvr** / **i3dvr**

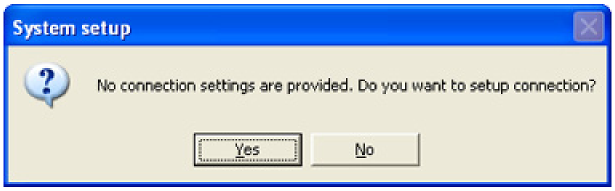


Portal Card Access System

Login: i3dvr

Password: *****

3. Click **Yes** in the System setup window to configure hardware connection settings.

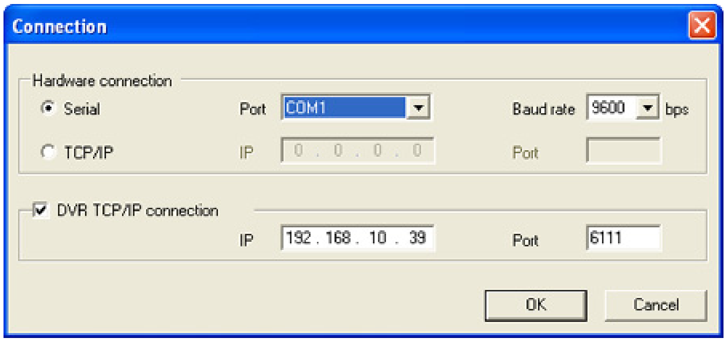


System setup

No connection settings are provided. Do you want to setup connection?

4. The Connection window will be displayed. Configure the connection type to either Serial, if RS-232 connection is used between host PC and the Controller, or to TCP/IP if the converter board (I3-S2E) is used.

   a. For Serial connection, select the serial **COM** port used for RS-232 connection. Make sure that **9600** baud rate is selected, to match Controller setting.



Connection

Hardware connection

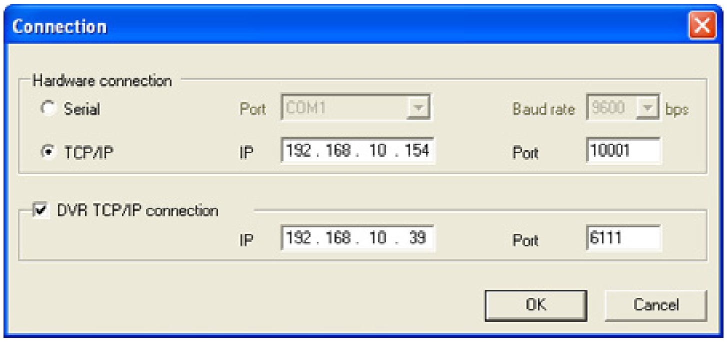
● Serial Port COM1 Baud rate 9600 bps

○ TCP/IP IP 0 . 0 . 0 . 0 Port

☑ DVR TCP/IP connection

IP 192 . 168 . 10 . 39 Port 6111

b. For TCP/IP connection, enter the **IP address** and the **Port** number of the converter. The default port number is **10001**. See section Configuring IP Address for TCP/IP Converter of the manual for information on how to configure IP Address for TCP/IP Converter.


Connection

Hardware connection

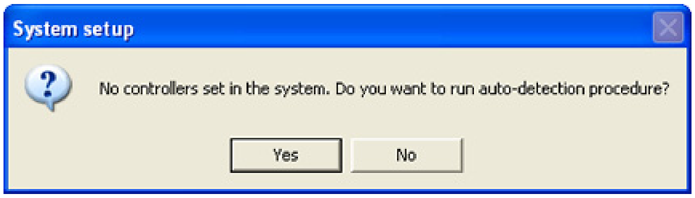
○ Serial Port COM1 Baud rate 9600 bps

● TCP/IP IP 192 . 168 . 10 . 154 Port 10001

☑ DVR TCP/IP connection

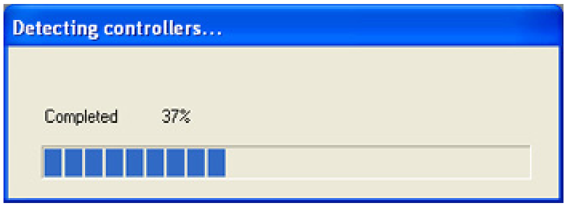
IP 192 . 168 . 10 . 39 Port 6111

5. Click **Yes** in the next System setup window to auto-detect all Controllers connected to the host PC.


System setup

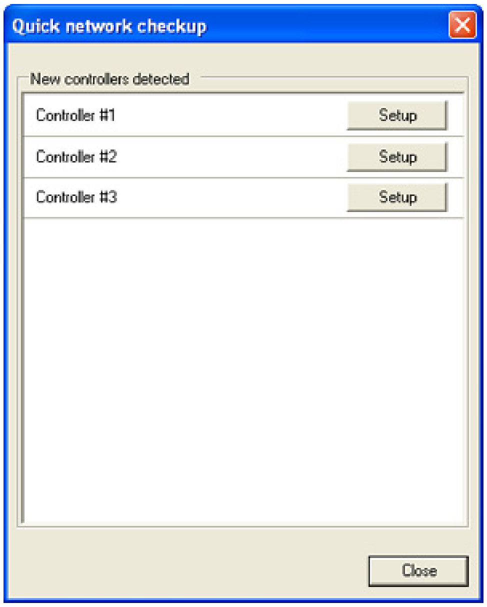
No controllers set in the system. Do you want to run auto-detection procedure?

6. Wait while Portal software checks for connected Controllers.


Detecting controllers...

Completed 37%

7. Click **Setup** button next to the first detected Controller to configure it.



Quick network checkup

New controllers detected

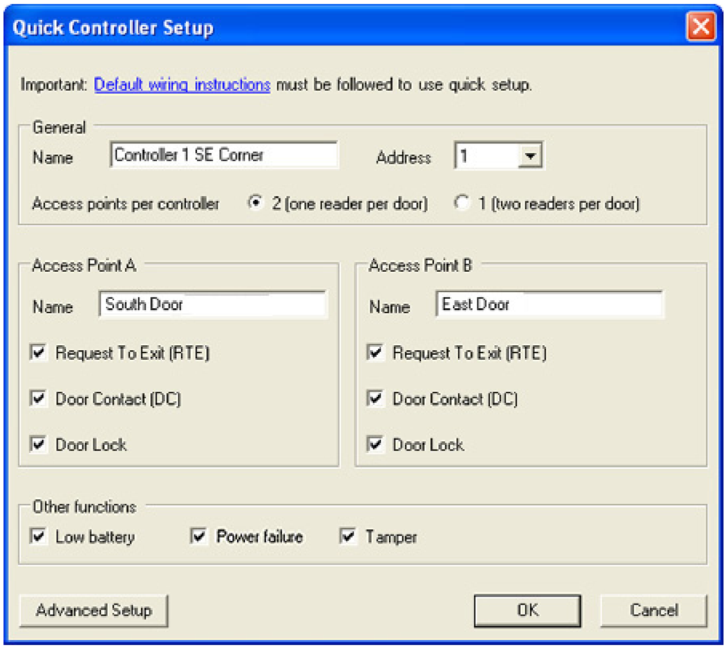
Controller #1 Setup

Controller #2 Setup

Controller #3 Setup

Close

8. Quick Controller Setup window will be displayed.



Quick Controller Setup

Important: Default wiring instructions must be followed to use quick setup.

General

Name: Controller 1 SE Corner Address: 1

Access points per controller ● 2 (one reader per door) ○ 1 (two readers per door)

Access Point A

Name: South Door

☑ Request To Exit (RTE)

☑ Door Contact (DC)

☑ Door Lock

Access Point B

Name: East Door

☑ Request To Exit (RTE)

☑ Door Contact (DC)

☑ Door Lock

Other functions

☑ Low battery ☑ Power failure ☑ Tamper

Advanced Setup OK Cancel

Important

To use this setup window, you must abide by default wiring recommendations. See Card Access Controller Wiring Diagram and Connecting Inputs to Controller, Connecting Outputs to Controller sections for more information. If the devices were wired differently, use Advanced Setup.

a. Name the Controller. It is good practice to name the Controller according to its physical location in the facility. This will simplify the servicing procedure later on.

b. Depending on whether both readers are used on the same access point (door) or on different doors, select the appropriate radio button in **Access points per Controller**. If **1 (two readers per door)** option is selected, Access Point B will be disabled below as well as RTE device for Access Point A (since Reader B will be essentially used as RTE device).

c. Check off all the devices connected to Access Point A and/or B: Request to Exit, Door Contact, and Door Lock.

If both readers are being used on the same door, make sure to wire Door Contact input and/or Door Lock output to Reader A.

Note that to be able to check these devices in the Quick Setup, you must abide by default wiring recommendations. See Card Access Controller Wiring Diagram and Connecting Inputs to Controller, Connecting Outputs to Controller sections for more information.

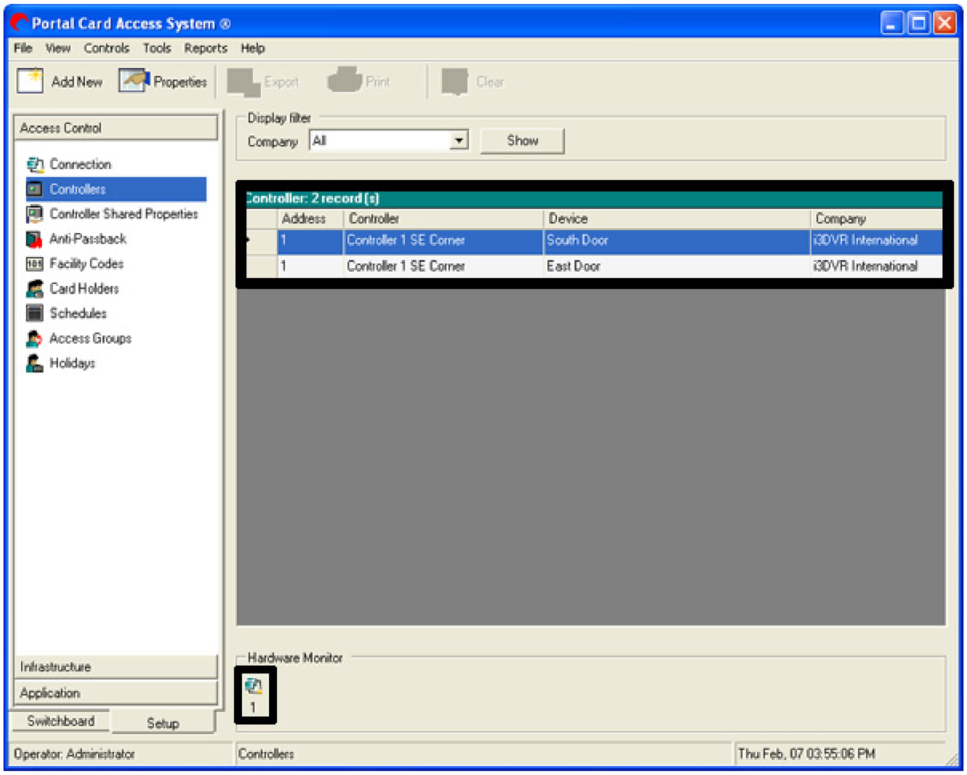
d. Check off all used devices under **Other functions category**: Low battery, Power failure, Tamper.

Please note that an additional battery must be purchased to use **Low battery** and **Power failure** functions. Portal Card Access chassis (P-PORTALCHASSIS) comes with a N/C tamper switch for **Tamper** detection. All these inputs must be properly connected to the Controller board in accordance with wiring recommendations. See Card Access Controller Wiring Diagram and Connecting Inputs to Controller, Connecting Outputs to Controller sections for more information.

e. Click **OK** once the Controller setup is complete.

f. Repeat above steps for all detected Controllers.

9. The configured access points will be added as separate entries in the **Controller** setup. The Controller panel will be displayed in the **Hardware Monitor** below.



Display filter

Company All

Controller: 2 record(s)

Address	Controller	Device	Company
1	Controller 1 SE Corner	South Door	i3DVR International
1	Controller 1 SE Corner	East Door	i3DVR International

Operator: Administrator | Controllers | Thu Feb, 07 03:55:06 PM

This completes the initial Controller installation.

2 Portal Most Commonly Used Functions

Topics Covered

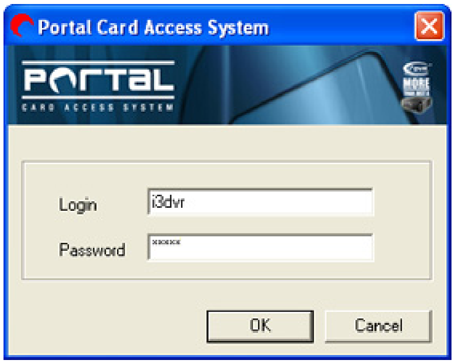
- Navigating Portal Software
- Managing Card Holders
- Managing Access Groups
- Managing Schedules
- Managing Holidays
- Direct Control
- Generating Reports
- Settings Upload

This chapter will demonstrate the usage of Portal most commonly used features. The sections are offered in a logical order that will reduce software setup time. This chapter covers card holder and access group management, access schedules, generation of working hours and event reports, direct control of the access point, input/output configurations as well as anti-passback features.

2.1. Navigating Portal Software

If the Portal Card Access System is not currently open, locate the Portal Card Access System software icon on the Desktop and launch the software application. Portal Card Access System®

In the login window, enter the default user name and password: **i3dvr** / **i3dvr**



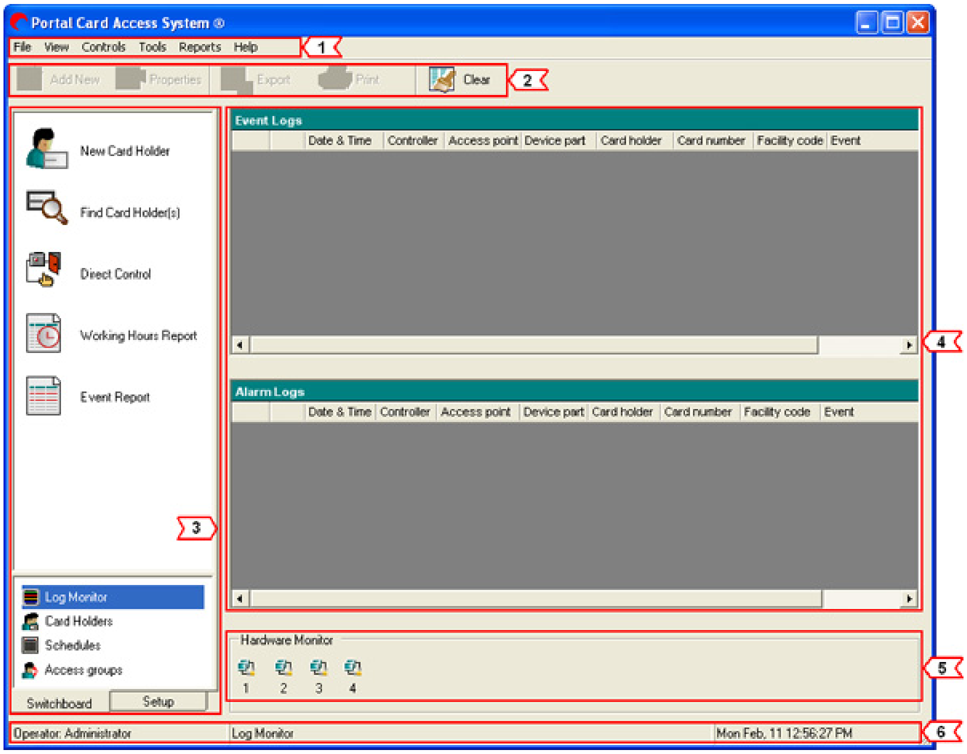
Login i3dvr

Password ******

Tip

i3dvr is a default Administrator user. Additional users (operators) may be created in Setup -> Application -> Operators software section.

Portal Card Access Main Screen will be displayed. Portal Card Access System software GUI (Graphic User Interface) strives towards the ease-of-use through intuitiveness of the software layout.


Portal Card Access System ®
File View Controls Tools Reports Help
1
Add New Properties Export Print Clear
2
New Card Holder
Find Card Holder(s)
Direct Control
Working Hours Report
Event Report
3
Log Monitor
Card Holders
Schedules
Access groups
Switchboard Setup
Event Logs
Date & Time Controller Access point Device part Card holder Card number Facility code Event
4
Alarm Logs
Date & Time Controller Access point Device part Card holder Card number Facility code Event
Hardware Monitor
1 2 3 4
5
Operator: Administrator Log Monitor Mon Feb, 11 12:56:27 PM
6

1. **Main Menu:** Easy access to specific software sections.

   a. **File:** Export to Excel (reports only), Print (reports only), Logout, Work Offline, Exit

b. **View:** Hardware monitor, Log Monitor (Alarm log, Log details)

  i.

  ii.

c. **Control**

  i. Stop downloading logs

  ii. Upload settings

  iii. Synchronize date and time

  iv. Direct control

d. **Tools**

  i. System utilities (Backup settings, Restore settings, Disk space checkup, Archive event logs, Restore arcived logs, Database integrity checkup, Check hardware configuration, Detect new Controllers, Administrative Tools (Deleted card holders, Duplicated card holders, Regional options, Data storage, Firmware)

  ii. Card holders (List all, Add new, Batch load)

  iii. Schedules (List all, Add new)

  iv. Access groups (List all, Add new)

  v. Setup

e. **Reports:** Working hours report, Event report, Custom reports (New, Save, Save As, Rename, Delete)

f. **Help:** Help index, About

2. **Control Panel:** Add New, Properties, Export (reports only), Print (reports only), Clear (reports and log monitor only)

3. **Navigation Panel:** Switch between most commonly used software features and full software Setup

a. **Switchboard:** Easy access to most commonly used software features

  i. **Quick access buttons:** New Card Holder, Find Card Holder(s), Direct Control, Working Hours Report, Event Report

  ii. Log Monitor - see the real-time list of event logs

  iii. Card Holders - see the full list of all added card holders

  iv. Schedules - see the list of all added access schedules

  v. Access groups - see the list of all added access groups

b. **Setup:** Full software setup

  i. **Access Control:** Connection, Controllers, Controller Shared Properties, Anti-Passback, Facility Codes, Card Holders, Schedules, Access Groups, Holidays

  ii. **Infrastructure:** Company Info, Departments, Titles, Employment Categories, Countries, Provinces

   iii. **Application:** General Preferences, Log Monitor Preferences, Operator Groups, Operators

4. **Log Monitor/Navigation window.** Log monitor entries and software detailed settings will be displayed in this window.

5. **Hardware Monitor panel.** Monitor your Controller connections as well as tamper, power failure and low battery events.

   ⚠ Warning signal will be flashing on the Hardware monitor panel until the detected problem is resolved. Doble-click on the flashing symbol to see the Trouble Report.

6. **Status panel**. Status panel displays the current date and time, the name of a current software operator (e.g. Administrator), and the name of a currently displayed software section (e.g. Log Monitor, Event Report, etc.)

2.2. Managing Card Holders

Adding new card holders with Portal software is fast and easy. Up to 2000 card holders can be entered into Portal Card Access system. All used cards must be of the same format: 26 bit or i³DVR proprietary 46 bit format. All cards shipped with Portal Card Access System and/or ordered from i³DVR are 46 bit format.

Due to the relationship of software settings, the following should be configured prior to adding a new card holder:

1. **Facility Codes**
2. **Access group(s) (if used)**
3. **Company Information (optional):** department names, employee titles
4. **Schedules (if custom schedules will be used)**

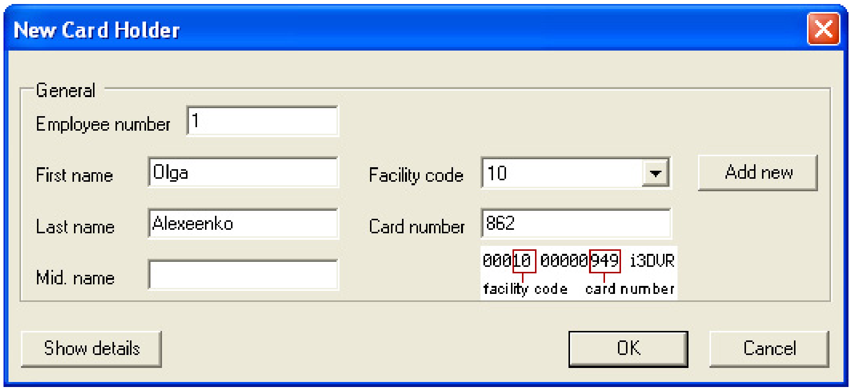
To add a new card holder, do one the following:

In the Switchboard, click **New Card Holder** quick access button .

OR

Go (Tools) -> Setup -> Access Control -> Card Holders. Click **Add New** on the Control Panel or right-click inside the Card Holders Navigation window and select **Add new...** from the context menu.

1. The simple New Card Holder form will be displayed.



New Card Holder

General

Employee number: 1

First name: Olga

Last name: Alexeenko

Mid. name:

Facility code: 10

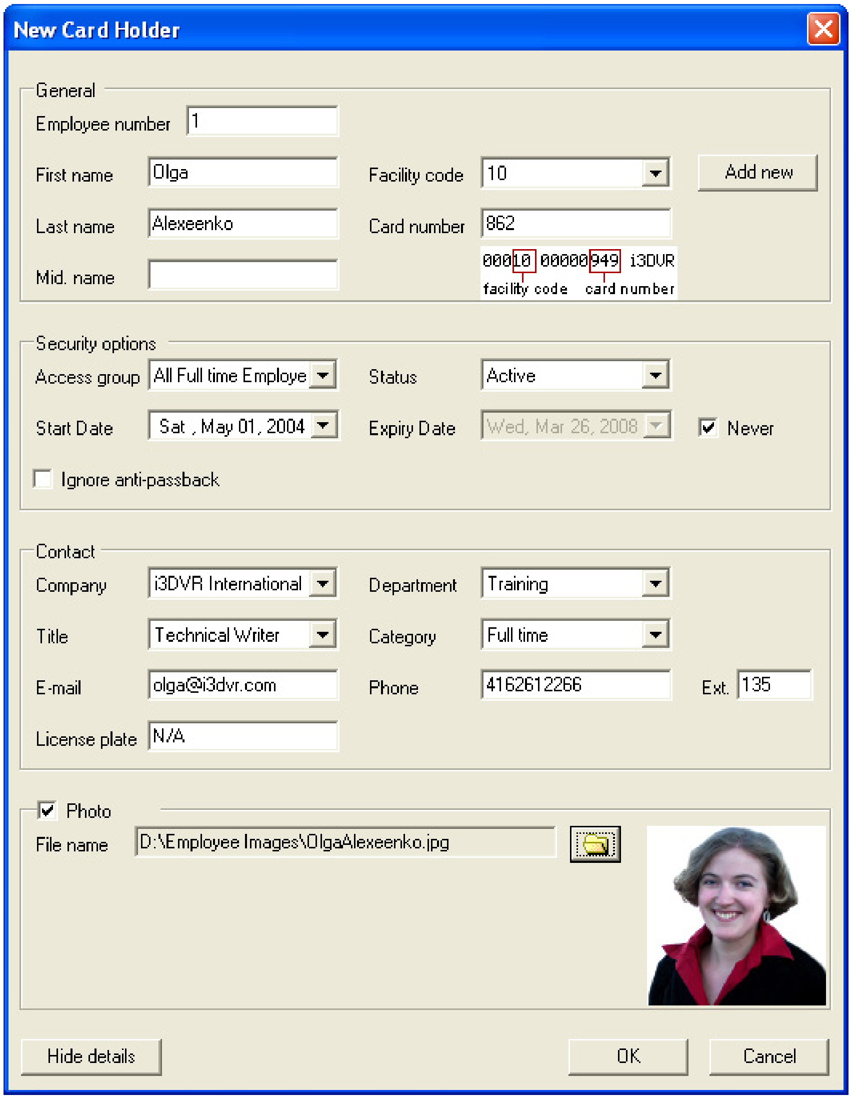
Card number: 862

2. Enter **Employee number** (if applicable). If the employee does not have a unique employee number, the program will automatically assign the next available number in a sequence.
3. Enter employee **First**, **Last** and **Middle** (if applicable) names.
4. Select employee card **Facility code** from the drop-down menu. The facility code is first number printed on the card (see image). If facility codes were not previously configured, click **Add new** button and add all used facility codes.
5. Enter employee **Card number**. The card number is the second number printed on the card (see image.)
6. Click **OK** to add new card holder or click **Show details** to add additional employee information.

   If Show details button was clicked, complete form will be displayed. (see example below)

Tip

Ignore all zeros (0) printed in front of access card number and facility code.



New Card Holder

General

Employee number: 1

First name: Olga

Last name: Alexeenko

Mid. name:

Facility code: 10

Card number: 862

00010 00000949 i3DVR

facility code card number

Security options

Access group: All Full time Employe

Start Date: Sat , May 01, 2004

Status: Active

Expiry Date: Wed, Mar 26, 2008

☑ Never

□ Ignore anti-passback

Contact

Company: i3DVR International

Title: Technical Writer

E-mail: olga@i3dvr.com

License plate: N/A

Department: Training

Category: Full time

Phone: 4162612266

Ext. 135

☑ Photo

File name: D:\Employee Images\OlgaAlexeenko.jpg

7. In Security options area,

   a. Select **Access group** that the new card holder will belong to from the drop-down list. You may leave the default Master access group if so desired.

      If access groups were not previously configured, you will need to save new card holder, close the form and go to Switchboard -> Access groups or Tools -> Access groups to create access groups.

   b. Select the **Status** of new card from the drop-down list. Available options are: Active, Destroyed, Expired, Inactive, Lost, Stolen, Suspended.

   c. Configure the new card''s **Start Date** and **Expiry Date**. The card will not be accepted when presented to the reader(s) before the Start Date or after Expiry Date. This feature is very useful for temporary employees, visitors and new hires that have not resumed their employment yet.

      Check off **Never** checkbox to disabled the Expiry Date.

      Check off **Ignore anti-passback** checkbox for the new card holder if so desired. All configured anti-passback will not apply to this card if this option is selected.

8. In Contact area,

   a. Select **Company** from the drop-down menu if several companies use the same card access database.

      If an additional company name needs to be added or company name needs to be edited, you will need to save new card holder, close the form and go to (Tools) Setup -> Infrastructure -> Company Info.

      To edit exiting company information, click **Edit Company properties**, click **Properties** on the Control Panel or right-click on the company entry and select **Properties** from the context menu.

      To add additional company, click **Add New** on the Control Panel .

   b. Select **Department** that the new card holder will belong to from the drop-down list if so desired.

      If departments were not previously configured, you will need to save new card holder, close the form and go to (Tools) Setup -> Infrastructure -> Departments. To add additional department, click **Add New** on the Control Panel or right-click inside the Departments Navigation window and select **Add new...** from the context menu.

   c. Select **Title** that the new card holder will have from the drop-down list if so desired.

      If titles were not previously configured, you will need to save new card holder, close the form and go to (Tools) Setup -> Infrastructure -> Titles. To add additional titles, click **Add New** on the Control Panel or right-click inside the Titles Navigation window and select **Add new...** from the context menu.

   d. Select **Category** that the new card holder will belong to from the drop-down list if so desired. The default category is **Full time**. Available options: Contract, Full time, Internship, Part time, Visitor.

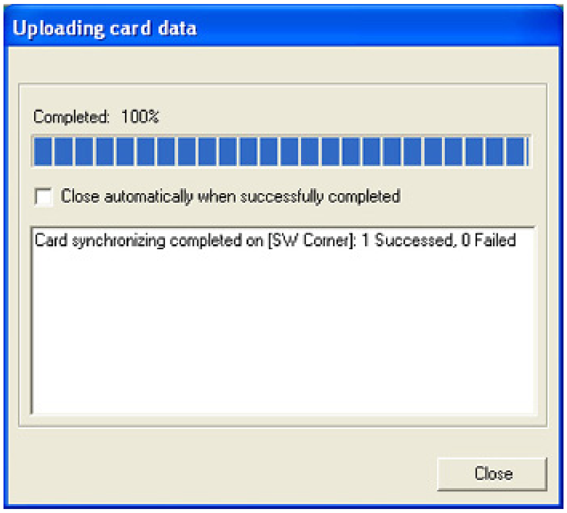
Note

These employment categories have no effect on the card holder''s access level. Access level is defined by the assigned Access group.

   e. Enter other optional contact information: **E-mail** address, **Phone/extension** number, vehicle **License plate**.

   f. An optional avatar photo can be assigned to the card holder. To do so, enable **Photo** checkbox and click on the folder icon to select an image. JPEG, BMP, TIFF, GIF and PNG files are recognized. The selected image will be resized to 112x112 avatar-size picture. The card holder''s photo will be displayed in the bottom right corner.

   g. Click **OK** to save new card holder. The settings will be automatically uploaded to all Controllers. Click Close when card data uploading has completed (see image below).



Uploading card data

Completed: 100%

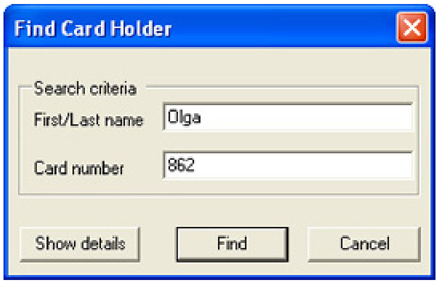
□ Close automatically when successfully completed

Card synchronizing completed on [SW Corner]: 1 Successed, 0 Failed

2.2.1. Find Card Holder(s)

To search for a specific card holder, do the following:

In the Switchboard, click the **Find Card Holder(s)** quick access button . Find Card Holder form will be displayed.



Find Card Holder

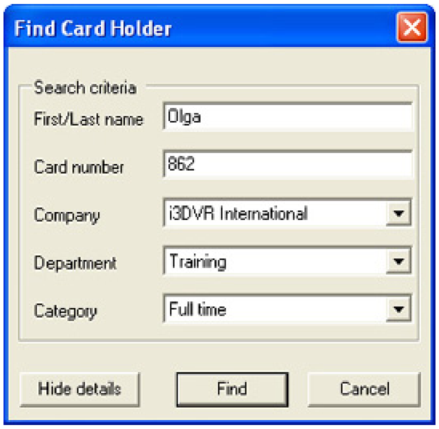
Search criteria

First/Last name: Olga

Card number: 862

Fill out First/Last name of a card holder and/or card number and click **Find**. Card holders Navigation window will be displayed with all card holder records that match the entered information.

Additional criteria may be used for searching card holders: Company, Department, Category. To display additional criteria, click **Show details** in the Find Card Holder window.



Find Card Holder

Search criteria

First/Last name: Olga

Card number: 862

Company: i3DVR International

Department: Training

Category: Full time

To open specific card holder''s record, double-click on the desired entry in the Card holders Navigation window.

To browse through the entire list of all card holders, do one of the following:

In the Switchboard, select Card Holders option

OR

In the Navigation Panel, click the Setup -> Access Control -> Card Holders

OR

Go Tools -> Card Holders

In the Card holders Navigation window, the records can be filtered based on **Company** name, **Department**, and/or employment **Category**.

2.3. Managing Access Groups

Access Groups allow limiting access of a group of people based on access points (doors) and/or schedules. Access groups may be assigned to individual card holders and multiple card holders may be assigned to the same access group. Each card holder may only belong to one access group.

By default, all new card holders are assigned to the default **Master** access group that gives card holders access to all access points (doors) at all times.

Due to the relationship of software settings, the following should be configured prior to adding a new access group:

1. **Access points**

2. **Schedules (if custom schedules will be used)**

To browse through a list of available access groups, do one of the following:

In the Switchboard, select Access groups option

OR

In the Navigation Panel, click the Setup -> Access Control -> Access Groups

OR

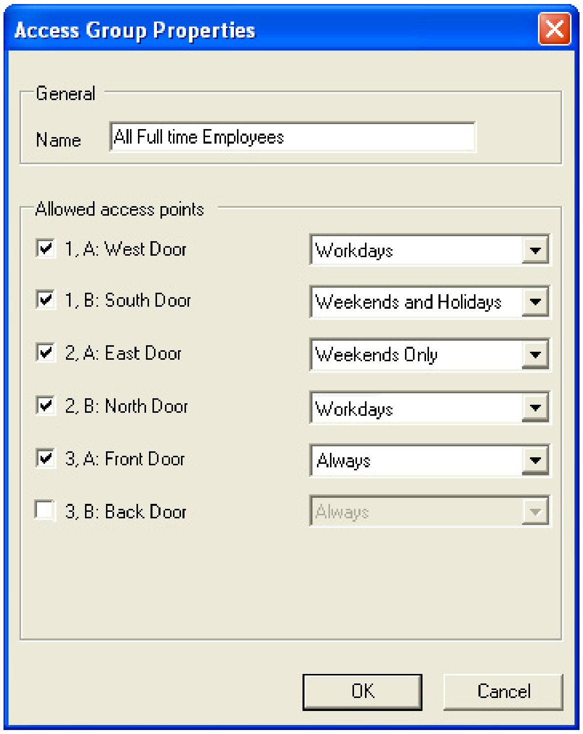
Go Tools -> Access Groups

The Access Groups Navigation window will be displayed.

To add a new access group, do the following:

Click **Add New** on the Control Panel or right-click inside the Access Groups Navigation window and select **Add new...** from the context menu.

Access Group Properties window will be displayed.



Name: All Full time Employees

☑ 1, A: West Door	Workdays
☑ 1, B: South Door	Weekends and Holidays
☑ 2, A: East Door	Weekends Only
☑ 2, B: North Door	Workdays
☑ 3, A: Front Door	Always
☐ 3, B: Back Door	Always

To configure access group, do the following:

1. Enter access group Name. For simplicity, it is recommended to give the access groups unambiguous names, e.g. All Full Time Employees, Contract Employees, Cleaning Staff, Senior Management, etc.

2. Check off all allowed access points (doors/readers). Uncheck access points that will be unaccessible to the selected access group. In the example above, all card holders that belong to "All Full time Employees" access group will have access to all available access points except for Access point B on Controller 3 (Back Door).

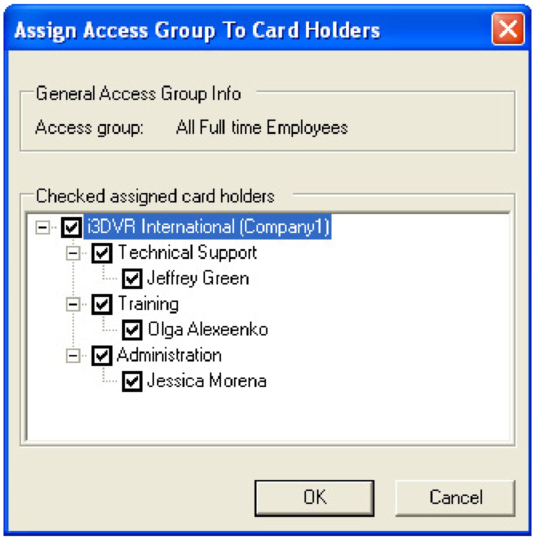
3. Select access schedule for each allowed access point from corresponding drop-down menus. In the example above, all card holders that belong to "All Full time Employees" access group will be able to enter Front door at all times, West and North doors on Workdays, South door on Weekends and Holidays, and East door on Weekends only.

   If schedules were not previously configured, you will need to save new access group, close the form and go to Switchboard -> Schedules or Tools -> Schedules groups to create schedules.

4. Click **OK** to save new access group and to close the form.

To assign an access group to multiple card holders, do the following:

Select the desired access group inside the navigation window, right-click and select **Assign to card holders...** option from the context menu. A new window will be displayed.



Assign Access Group To Card Holders

General Access Group Info

Access group: All Full time Employees

Checked assigned card holders

- ☑ i3DVR International (Company1)
  - ☑ Technical Support
    - ☑ Jeffrey Green
  - ☑ Training
    - ☑ Olga Alexeenko
  - ☑ Administration
    - ☑ Jessica Morena

In Assign Access Group to Card Holders window, a list of all card holders sorted by department and company will be displayed. Check off all users that need to be assigned to the selected access group and click **OK**.

Important

After assigning Access Group to card holder(s), manually upload settings.

2.4. Managing Schedules

Schedules are one of the most commonly used functions in Portal Card Access System software. Schedules are used by Access Groups, Readers, Inputs, and Actions.

Schedules are used by Access Groups to limit card holder access to specific access points (doors) during certain hours and/or days. The auto unlock function for each Access Point, all connected Inputs and their Actions also use the same group of configured schedules. It is therefore recommended to create all custom schedules before configuring access groups and access points. Two default schedules are available: **Always** and **Never**. These default schedules cannot be deleted and can by used by both Access Groups and Access Points. A total of 30 custom schedules can be saved on Portal Card Access System software.

To browse through a list of available schedules, do one of the following:

In the Switchboard, select Schedules

OR

In the Navigation Panel, click the Setup -> Access Control -> Schedules

OR

Go Tools -> Schedules

The Schedules Navigation window will be displayed.

To add a new schedule, do the following:

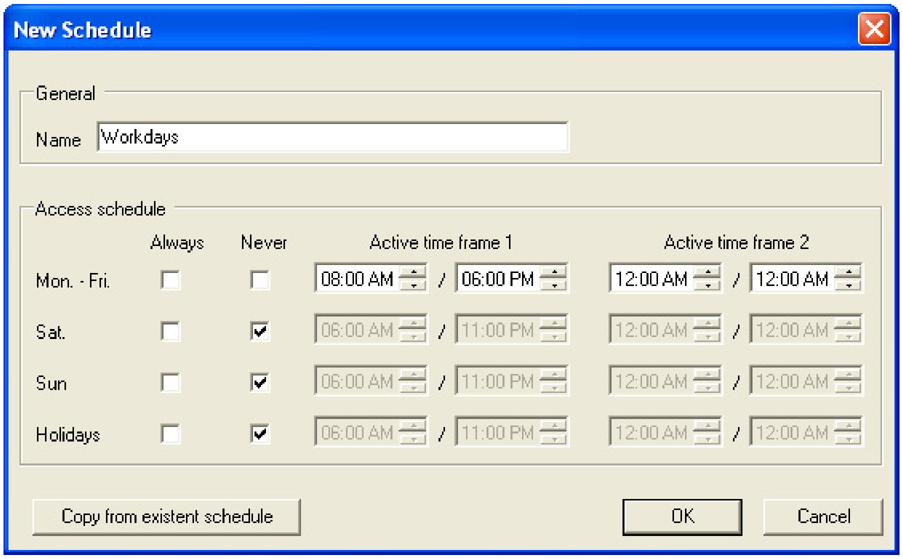
Click **Add New** on the Control Panel or right-click inside the Schedules Navigation window and select **Add new...** from the context menu.

New Schedule window will be displayed. Four time groups are defined: Workdays (Monday to Friday), Saturday, Sunday and Holidays. If holidays were not previously configured, you may configure then at a later time by going to (Tools) Setup -> Holidays.

Each time group has two active time frames (intervals); if only one time frame is required, do not configure the second time frame. By using active time frames, the operator may exclude certain time period from the time group.

Example. To create a working hours schedule that will exclude the lunch hour (12:00 PM - 1:00 PM), configure two active time frames: 8:00AM - 12:00PM and 1:00PM - 5:00PM.

The number of active time frames can be expanded to four (4) if required. To increase number of active time frames, right-click inside the schedule form and select **Add time frame** from the context menu.



New Schedule

General

Name: Workdays

Access schedule

	Always	Never	Active time frame 1	Active time frame 2
Mon. - Fri.	□	□	08:00 AM / 06:00 PM	12:00 AM / 12:00 AM
Sat.	□	☑	06:00 AM / 11:00 PM	12:00 AM / 12:00 AM
Sun	□	☑	06:00 AM / 11:00 PM	12:00 AM / 12:00 AM
Holidays	□	☑	06:00 AM / 11:00 PM	12:00 AM / 12:00 AM

To configure new schedule, do the following:

1. Enter schedule Name. For simplicity, it is recommended to give the schedule unambiguous names, e.g. Workdays, Weekends only, Workdays and Weekends, 9 to 5, etc.

2. Check off **Never** checkbox for all days that will be completely excluded from the access schedule. In the example above, Saturdays, Sundays and Holidays are excluded from "Workdays" schedule.

3. Check off **Always** checkbox for all days that are included in the access schedule and do not require active time frame setup (i.e. 12:00 AM - 12:00 AM).

4. Configure one or two (if required) active time frames for desired days. In the example above, "Workdays" schedule includes days Monday - Friday, 8:00AM - 6:00PM only.

5. Click **OK** to save new schedule and to close the form.

To simplify the schedule setup process, you may first copy information from existing schedule and then make necessary changes to it. To copy information from existing schedule, use **Copy from existent schedule** button or right-click inside the Schedule form, select **Copy from existent schedule** from context menu and select the schedule to copy settings from.

To discard all changes made to the schedule, right-click inside the Schedule form and select **Reset schedule** from context menu.

Important

After creating new schedules, manually upload settings.

2.5. Managing Holidays

Holidays are used by Schedules. New holidays may be added to the list at any time. Portal Card Access System also allows adding yearly holidays that recur on the same day each year.

In the Navigation Panel, click the Setup -> Access Control -> Holidays

OR

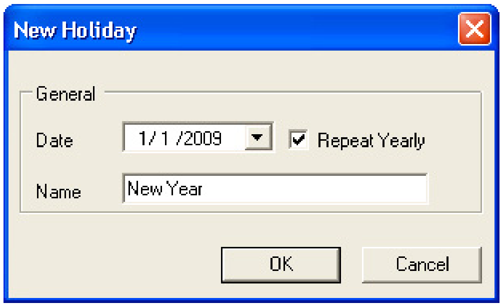
Go Tools -> Setup -> Access Control -> Holidays

The Schedules Navigation window will be displayed.

To add a new schedule, do the following:

Click **Add New** on the Control Panel or right-click inside the Holidays Navigation window and select **Add new...** from the context menu.

New Holiday window will be displayed.



Date 1/ 1 /2009 ☑ Repeat Yearly

Name New Year

To configure new holiday, do the following:

1. Set the holiday date in the calendar drop-down menu.

2. Check off **Repeat Yearly** checkbox if the holiday falls on the same day each year (E.g. Christmas, Boxing Day, New Year, Canada Day / Independence Day)

3. Enter holiday **Name**

4. Click OK to save new holiday and to close the form

Important

After creating new holidays, manually upload settings.

2.6. Direct Control

Direct Control function allows the operator to manually unlock/lock one or more access points (doors). Note that Direct Control overrides all schedules, including auto-unlock schedules configured for the access points until midnight of the same day.

Note

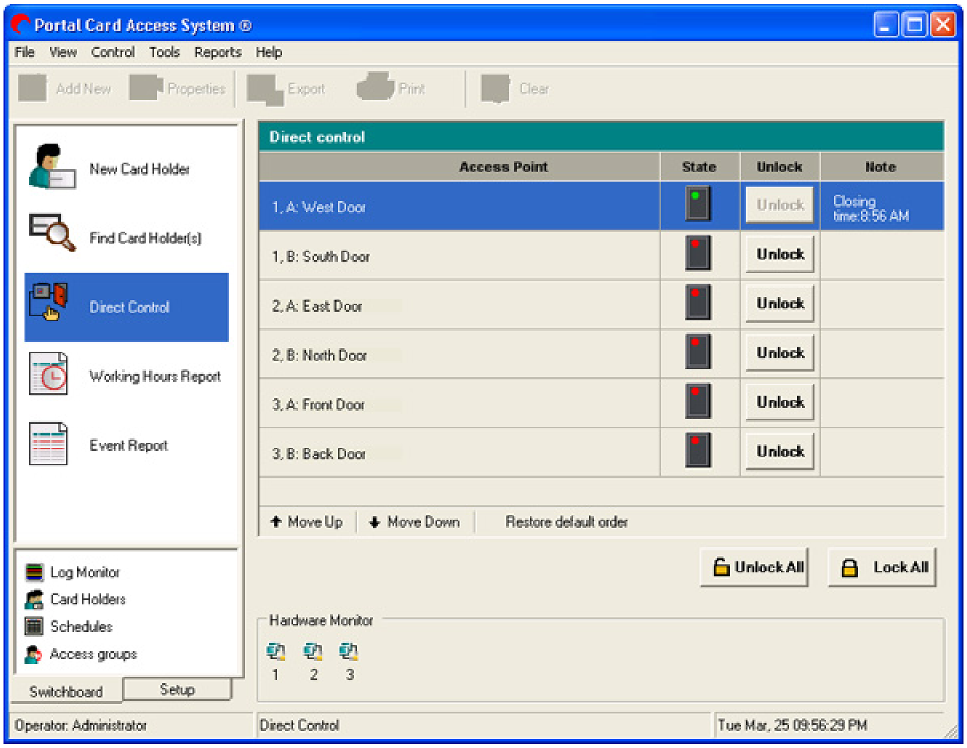
To use Direct Control unlock/lock function on an access point, the Door Lock output must be properly wired to the Controller and configured in Portal Card Access System software.

In the Switchboard, click the **Direct Control** quick access button. Direct control form will be displayed in the Navigation window.

The Direct control navigation window displays the list of all available access points sorted by the Controller ID number.

This window also displays the state of the Door Lock device for each access point: Locked 🔴 and Unlocked 🟢.

By using **Move Up** and **Move Down** buttons the operators can rearrange the access points order in a way most convenient to them. For example, the access points (doors) that are frequently unlocked manually through Direct Control feature can be moved to the top of the list.



Access Point	State	Unlock	Note
1, A: West Door	🟢	Unlock	Closing time:8:56 AM
1, B: South Door	🔴	Unlock	
2, A: East Door	🔴	Unlock	
2, B: North Door	🔴	Unlock	
3, A: Front Door	🔴	Unlock	
3, B: Back Door	🔴	Unlock	

Operator: Administrator Direct Control Tue Mar, 25 09:56:29 PM

To unlock a selected access point (door), do the following:

1. Click **Unlock** button that corresponds with the access point/door that needs to be unlocked
2. The access point State will change to Unlocked for 5 seconds (default unlock time) after which the access point will re-lock automatically

Tip

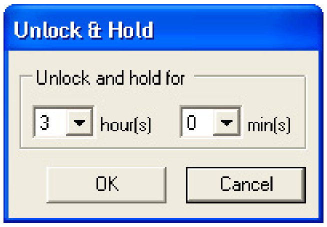
To change the default unlock time, go to (Tools) Setup -> Controller Shared Properties and adjust the Default unlock time (sec) value.

Occasionally the access point may need to be opened for an extended period of time (e.g. for delivery).

To unlock a selected access point (door) for a period of time, do the following:

1. Select an access point from the list

2. Right-click and select **Unlock for...** from the context menu. Unlock & Hold window will be displayed.



3 hour(s) 0 min(s)

3. Set the unlock time by configuring the number of hours/minutes in the corresponding drop-down menus and click **OK** to close the form and unlock the access point.

4. The access point State will change to Unlocked. The note will be displayed for the unlocked access point showing the closing (re-locking) time. In the example above, the Access Point A on Controller 1 (West Door) will re-lock at 8:56 AM.

To re-lock the selected access point (door), do the following:

1. Select the unlocked access point from the list

2. Right-click and select **Lock** from the context menu.

3. The access point State will change to Locked.

Locking/Unlocking all access points (doors)

Caution

Exercise caution in using this feature.

To lock/unlock all access points, click corresponding button: 🔒 Lock All or 🔓 Unlock All, then click **Yes** in a warning window. All access points will be locked/unlocked until midnight of the same day when all regular schedules will come back into effect.

Remember that this feature will override all schedules, including auto-unlock schedules configured for the access points until midnight of the same day.

2.7. Generating Reports

Portal Card Access System software allows generating two types of reports: Working Hours Reports to track employee attendance and Event Reports to monitor system events such as access and alarm logs.

Three additional buttons are available on Control Panel for generated reports:

Export generated report into Excel format

Print generated report (default printer)

Clear report results

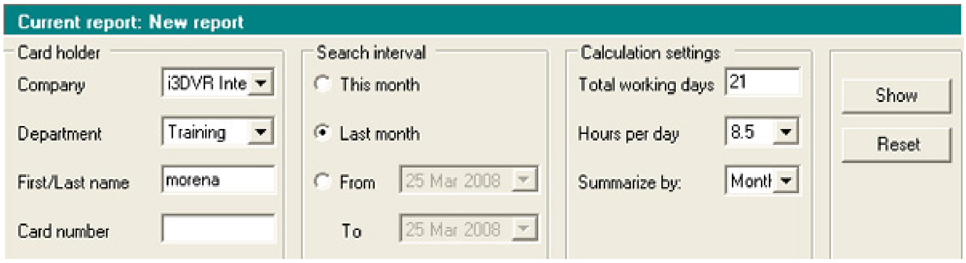
The generated custom reports can be saved for future reference. To save a report, go **Reports** -> **Custom reports** -> **Save**. Unlimited number of custom reports can be saved.

To save a copy of/rename or delete a saved report, go to Reports menu, Custom reports and select a saved report. Once the report is displayed in the Navigation window, go **Reports** -> **Custom reports** -> **Save As.../Rename.../** or **Delete...**

2.7.1. Working Hours Report

Working Hours report allows calculating the number of hours that passed between the first and last time the card holder''s card was presented during the day. Working Hours report can be used for attendance purposes, however it is not designed for accounting / payroll purposes as the results may not be completely accurate (e.g. card holder forgets to present the card to the reader before leaving work).

To generate a Working Hours report, click Working Hours Report quick access button on the Switchboard or go Reports -> Working hours report. New report form will be displayed in the Navigation window.



Current report: New report

Card holder
Company: i3DVR Inte
Department: Training
First/Last name: morena
Card number:

Search interval
○ This month
● Last month
○ From 25 Mar 2008
To 25 Mar 2008

Calculation settings
Total working days: 21
Hours per day: 8.5
Summarize by: Montl

To generate a new report, do the following:

1. Enter as much known information about the card holder as possible: Company, Department, First/Last name and/or Card number

2. Define the search interval: This month, Last month or a defined time period. Note that the number of total working days in the selected search interval will be automatically calculated in Calculation settings. If the company does not operate on a regular Monday - Friday schedule, adjust the number of total working days manually.

3. Select the number of expected **Hours per day** from the drop-down menu. The lunch time should be included in this number. In the example above, the selected Hours per day is 8.5, which includes 30 minutes for lunch time.

4. Select **Summarize by** option from the drop-down menu. Available options are: Day, Month, Selected period

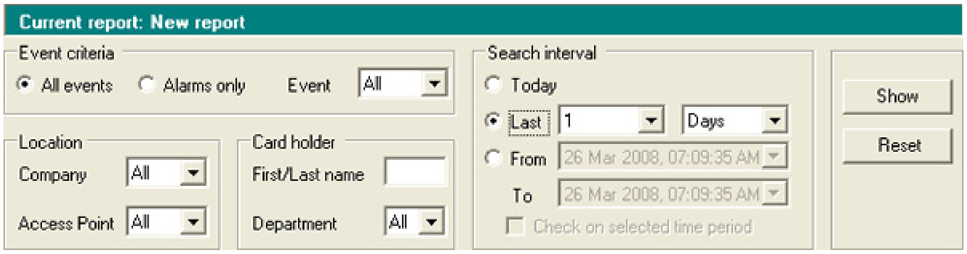
5. Click **Show** to run the report according to the entered criteria

6. All matching logs will be displayed directly underneath. To save this report, go **Reports** -> **Custom reports** -> **Save**.

2.7.2. Event Report

Event report allows generating a custom report of event and alarm logs based on selected time period.

To generate an event report, click Event Report quick access button on the Switchboard or go Reports -> Event report. New report form will be displayed in the Navigation window.



Current report: New report

Event criteria: ● All events ○ Alarms only Event: All

Location: Company: All; Access Point: All

Card holder: First/Last name: ; Department: All

Search interval: ○ Today ● Last 1 Days ○ From 26 Mar 2008, 07:09:35 AM To 26 Mar 2008, 07:09:35 AM □ Check on selected time period

To generate a new report, do the following:

1. Select the Event criteria: **All events**, **Alarms only** or a specific **Event** from the drop-down menu

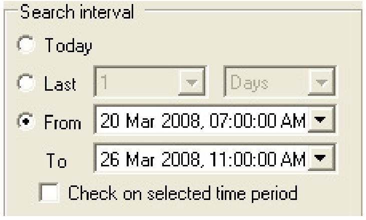
2. Select the specific Access Point (door) to only display events pertaining to the selected Access Point (optional)

3. If the report is needed of the events generated by a specific card holder, enter as much known information about the card holder as possible: **Company**, **Department**, **First/Last name** (optional)

4. Define the search interval: Today, Last X Days/Hours/Months or during a defined time period.

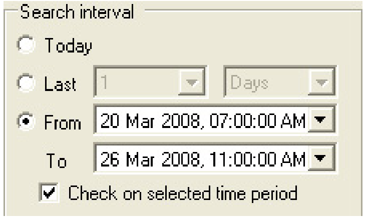
   The defined time period search can be used in two different ways: From the start time of the first day till the End time of the last day OR From the start time till the End time on each day during the selected time period (see examples below).

   In the example below, the search will be generated for selected events that occurred between 7:00AM on March 20th and 11:00AM on March 26th.

   Search interval: ○ Today ○ Last 1 Days ● From 20 Mar 2008, 07:00:00 AM To 26 Mar 2008, 11:00:00 AM □ Check on selected time period

   In the example below, the search will be generated for selected events that occurred between hours 7:00AM and 11:00AM on each of the 7 days (March 20, 21...26th).



Search interval

○ Today

○ Last 1 Days

● From 20 Mar 2008, 07:00:00 AM

To 26 Mar 2008, 11:00:00 AM

☑ Check on selected time period

5. Click **Show** to run the report according to the entered criteria

6. All matching logs will be displayed directly underneath. To save this report, go **Reports** -> **Custom reports** -> **Save**.

2.8. Settings Upload

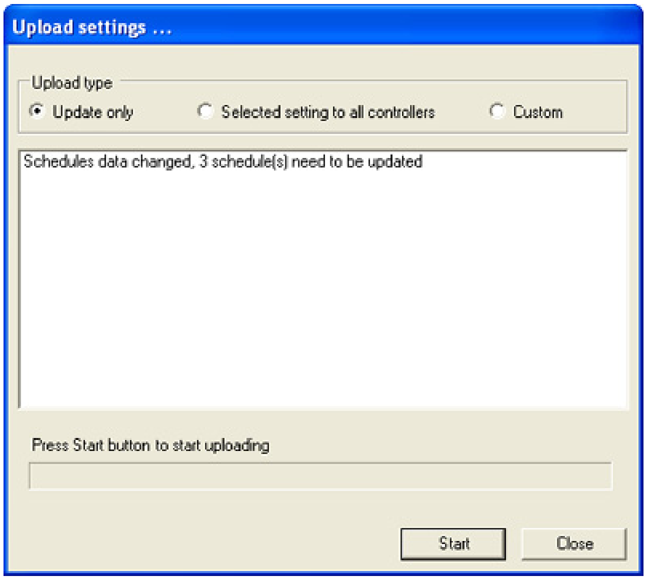
While software and hardware settings are configured on Host PC, the settings are also stored locally on each Controller, which allows them to operate autonomously from the Portal software application.

Most new settings need to be manually uploaded to the Controllers to take effect. The only exception to the rule are the following settings: Card holder settings (card holder added/edited/deleted) and Controller settings (Controller added/deleted, access point enabled/disabled, hardware inputs and/or outputs enabled/edited/disabled). These card holder and Controller-related settings are uploaded automatically by the Portal software.

To manually upload Portal settings Controllers, do the following:

Go to **Control** -> **Upload settings...** in the Main Menu. Upload settings window will be displayed. **Three options are available:**

1. Upload updates only. With this option, all updated settings will be uploaded to all Controllers in the network.



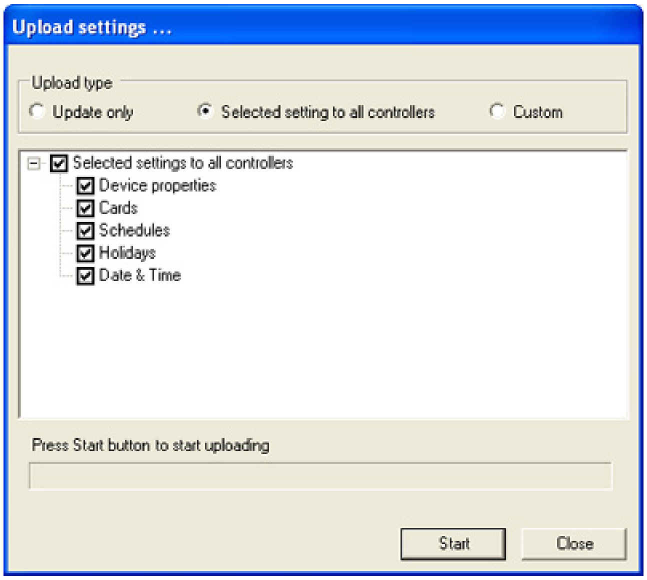
Upload type: ● Update only ○ Selected setting to all controllers ○ Custom

Schedules data changed, 3 schedule(s) need to be updated

Press Start button to start uploading

2. Upload all selected settings to all Controllers. With this option, select desired settings to be uploaded to all Controllers in the network.

   This type of upload is recommended for complete setting upload to all Controllers and as a part of a troubleshooting process. Do not uncheck anything in the tree list for complete setting upload.



Upload settings ...

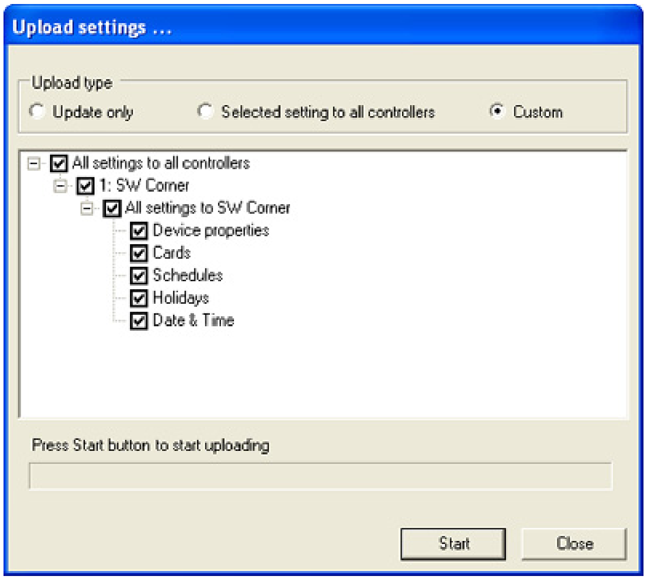
Upload type

○ Update only ● Selected setting to all controllers ○ Custom

- ☑ Selected settings to all controllers
  - ☑ Device properties
  - ☑ Cards
  - ☑ Schedules
  - ☑ Holidays
  - ☑ Date & Time

Press Start button to start uploading

3. Upload selected settings to selected Controllers. With this option, select specific settings to be uploaded to selected Controllers only.



Upload settings ...

Upload type

○ Update only ○ Selected setting to all controllers ● Custom

- ☑ All settings to all controllers
  - ☑ 1: SW Corner
    - ☑ All settings to SW Corner
      - ☑ Device properties
      - ☑ Cards
      - ☑ Schedules
      - ☑ Holidays
      - ☑ Date & Time

Press Start button to start uploading

After selecting upload type (Update only/Selected settings to all Controllers/Custom), click **Start** and wait for "**Uploading completed**" message to be displayed, then **Close** the window.

3

Advanced Setup

Topics Covered

- Adding/Deleting Controllers
- Configuring Readers and External Devices (inputs/outputs)
- Configuring Anti-Passback
- Configuring Text Overlay for DVMS

3.1. Adding/Deleting Controllers

During Portal initial setup, all Controllers are detected automatically, however, if a new Controller is added to the installation it needs to be initialized and configured first.

To add a new Controller, do one of the following:

Go to **Tools** -> **System Utilities** -> **Detect new Controllers...** Then repeat Steps 6-9 of the Basic Portal Software Configuration.

OR

Go to (Tools) **Setup** -> **Access Control** -> **Controllers**. In the Controller Navigation window, right-click and select **Add new...** from the context menu. Quick Controller Setup will be displayed. Provided that the standard wiring recommendations were followed for the new Controller, use Quick Controller Setup to configure new Controller and all attached devices.

To delete a Controller, do the following:

Go to (Tools) -> **Setup** -> **Access Control** -> **Controllers**. In the Controller Navigation window, right-click on the Controller entry to be deleted from the network and select **Delete** from the context menu.

Note that all enabled access points from all Controllers are automatically added to the Master access group, however the new access points have to be manually assigned to all custom access groups.

3.2. Configuring Readers and External Devices (inputs/outputs)

The most common external devices such as Door Lock, Door Contact, Request-to-Exit devices, Tamper, Low Battery and Power Failure are configured during the initial Controller detection. However, all additional general purpose devices (if any), such as alarms and/or sensors (e.g. motion sensor), must be configured in the Controller Advanced setup. Please see Configuring Input Settings and Configuring Output Settings sections for more information.

Before configuring external devices in the Portal Card Access System software, first make sure that the device is properly connected to the Portal Controller. Please consult Card Access Controller Wiring Diagram and Connecting Inputs to Controller, Connecting Outputs to Controller sections for wiring standards.

Warning

Remember never to use Portal power board (P-PWR-U023) to power electric door strike, magnetic lock, and/or any other external devices. External power supply must be used for all door lock outputs and general purpose devices.

Note

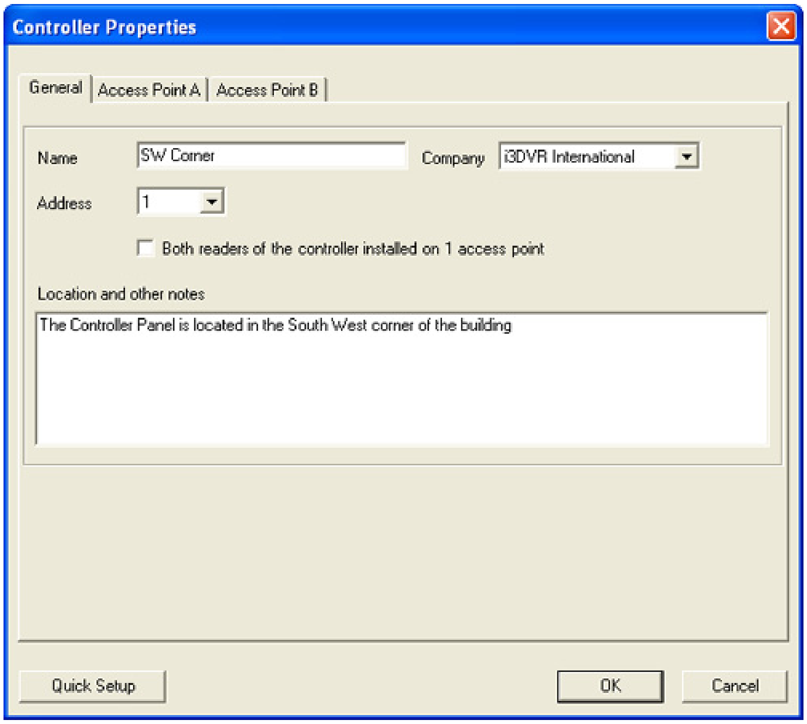
If the Controller settings have been previously customized, Controller Properties window will be displayed.

To configure external devices, do the following:

1. Go to (Tools) Setup -> Access Control -> Controllers

2. In the Controller Navigation window the list of all Access Points will be displayed sorted by Controller number. Double-click on the desired Access Point on the list to open Quick Controller Setup window.

3. Click **Advanced Setup** button to display Controller Properties window.



Name: SW Corner

Company: i3DVR International

Address: 1

□ Both readers of the controller installed on 1 access point

Location and other notes:
The Controller Panel is located in the South West corner of the building

In Controller Properties window, General tab, the operator may rename the Controller, change the Company that the Controller belongs to, change the Controller Address (Dip switch ID must be changed accordingly on the Controller) and enter any notes pertaining to the Controller (optional).

If both readers are used on the same access point (for IN access and OUT confirmation), check the appropriate checkbox in the General tab.

4. To configure an external device connected to the Controller, select either Access Point A or Access Point B tab, depending on which side of the Controller the device is physically connected to. Please consult Card Access Controller Wiring Diagram for more information.

3.2.1. Assigning Access Points to Access Groups

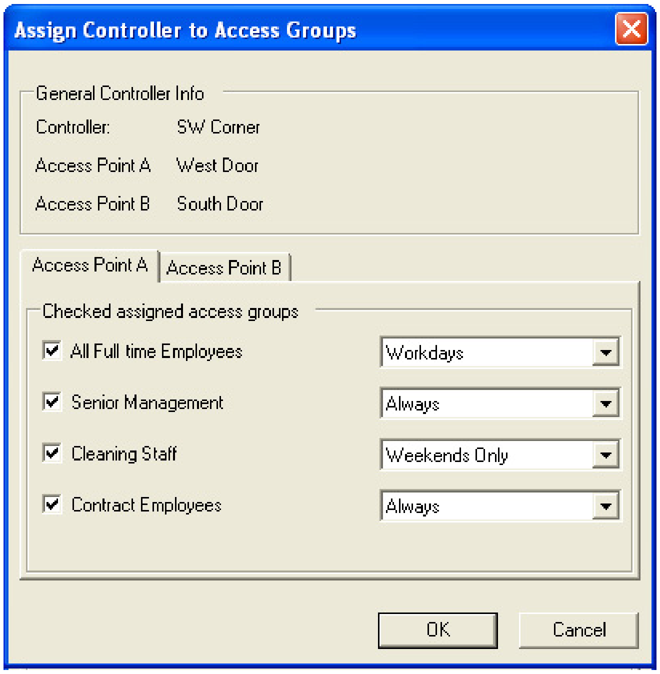
Due to the relationship of software settings, the following should be configured prior to assigning access points to access groups:

1. **Access groups (if used)**

2. **Schedules (if custom schedules will be used)**

Selected Controller can be assigned to a previously configured access groups, which may make the setup process much faster. To assign Controller to access groups, right-click on the desired Access Point on the list and select **Assign to access groups...** from the context menu. Assign Controller to Access Groups window will be displayed.

Note that all enabled access points from all Controllers are automatically added to the Master access group, however the new access points have to be manually assigned to all custom access groups.


Assign Controller to Access Groups
General Controller Info
Access Point A
Access Point B
Checked assigned access groups
OK
Cancel

Controller: SW Corner
Access Point A West Door
Access Point B South Door

☑ All Full time Employees Workdays
☑ Senior Management Always
☑ Cleaning Staff Weekends Only
☑ Contract Employees Always

1. Select desired Access Point tab in the window.

2. Check off all access groups that will have access to the selected Access Point. Uncheck those groups that will not have access to the selected Access Point.

   If access groups were not previously configured, you will need to close the form and go to Switchboard -> Access groups or Tools -> Access groups to create access groups.

3. Select access schedule for each access group from corresponding drop-down menus. In the example above, all card holders that belong to "Senior Management" and "Contract Employees" groups will be able to enter West door at all times; all card holders that belong to "All Full time Employees" access group will have access to West door based

on "Workdays" schedule, while all card holders in the "Cleaning Staff" access group will have access to West door based on "Weekends Only" schedule.

If schedules were not previously configured, you will need to close the form and go to Switchboard -> Schedules or Tools -> Schedules groups to create schedules.

4. Click **OK** to save changes and to close the form.

Important

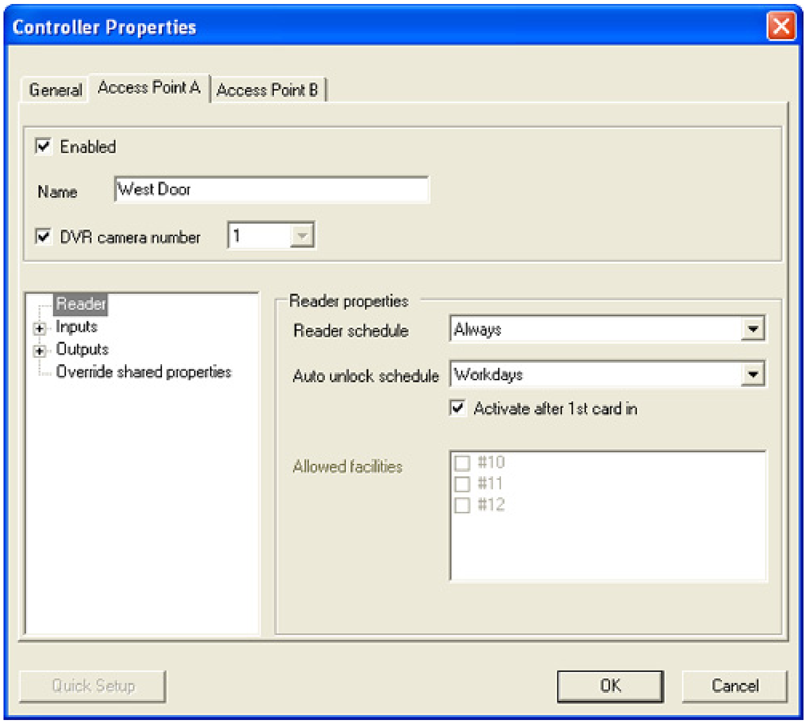
After making changes to this form, manually upload settings.

3.2.2. Configuring Reader Settings

To configure additional Reader settings, do the following:

1. In the Controller Properties window, the operator may Enable/Disable the reader, rename the reader and associate the access point with a specific DVR camera (provided that the connection with the DVR is properly configured in the Connection setup. See Configuring Text Overlay for DVMS section for more information.

2. Select **Reader** entry in the tree list on the left hand side. Reader properties will be displayed on the right side of the window.



☑ Enabled

Name: West Door

☑ DVR camera number: 1

Reader schedule: Always

Auto unlock schedule: Workdays

☑ Activate after 1st card in

Allowed facilities: □ #10 □ #11 □ #12

3. In Reader properties, the operator may configure the **Reader schedule** by selecting one of the previously configured schedules from the drop-down menu. This schedule will determine when the reader will grant access based on a valid credentials (card number/facility code). In the example above, reader A will Always grant access based on valid credentials.

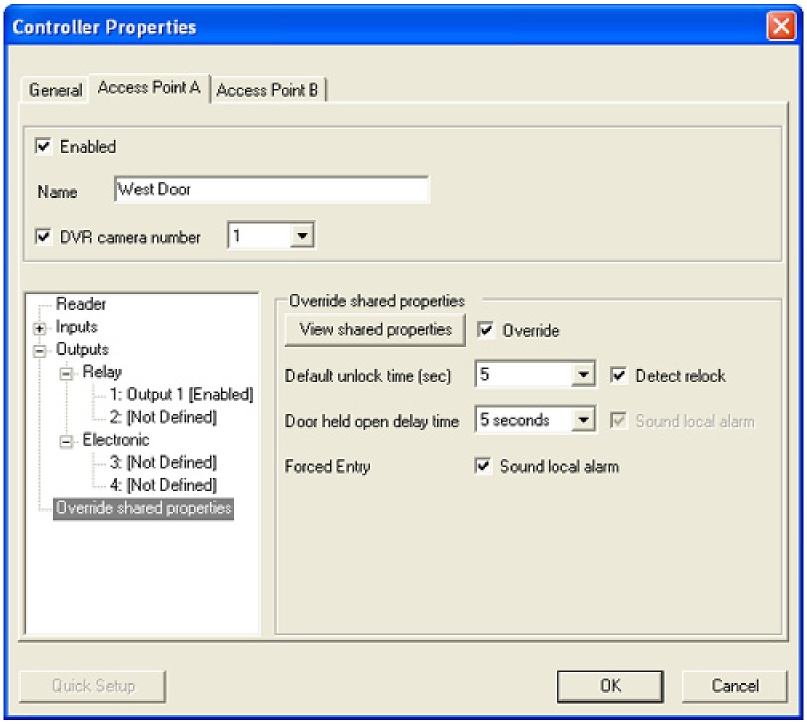
4. The operator also may configure **Auto unlock schedule**. To enable auto unlock schedule, select one of the previously configured schedules from the corresponding drop-down menu.

The Auto unlock schedule can be activated after the first card holder with a valid card enters the facility. To do so, the operator must check off **Activate after 1st card in** checkbox. In the example above, the Reader A will automatically unlock the Access Point called "West Door" based on "Workdays" schedule after the first valid card has been presented.

Tip
Remember that Direct Control will override all auto unlock schedules until midnight of the same day.

5. If the system is configured to grant access based on the Facility code rather than the Card number (configured in Controller Shared Properties), check off up to five allowed facility codes in **Allowed facilities**. Remember that this setting applies only to the selected reader.

6. To override shared Controller properties for this specific Reader, select **Override shared properties entry** in the tree list on the left hand side. Override shared properties will be displayed on the right side of the window.



☑ Enabled

Name: West Door

☑ DVR camera number: 1

☑ Override

Default unlock time (sec): 5 ☑ Detect relock

Door held open delay time: 5 seconds ☑ Sound local alarm

Forced Entry ☑ Sound local alarm

a. To view Controller Shared Properties, click **View shared properties** button

b. To override the shared properties, check off **Override** checkbox

c. Change the **Default unlock time (sec)** in the corresponding drop-down menu for the selected reader (optional). This unlock time will affect the Direct Control function.

d. Check off the **Detect relock** checkbox if so desired. Note that if the Detect relock checkbox is unchecked, the door lock device will not relock when the door closes until the default unlock time (sec) elapses. This means that if the **Default unlock time** is configured to a relatively long period of time, several people may enter the facility before the door re-locks itself without presenting any credentials.

e. Change the **Door held open delay time** in the corresponding drop-down menu for the selected reader (optional). If the door is held open for a longer period of time, the local alarm on the reader will be activated until door is re-locked. To disable this feature, select **Disable** from the drop-down menu.

f. Check off the **Sound local alarm checkbox** on Forced Entry event to sound the local alarm on the reader if the door lock is unlocked without valid credentials being presented to the reader. Uncheck this check box not to sound alarm. The log will still be generated and displayed in the Log Monitor on the Switchboard.

7. To save the settings and close Controller Properties window, click **OK**

3.2.3. Configuring Output Settings

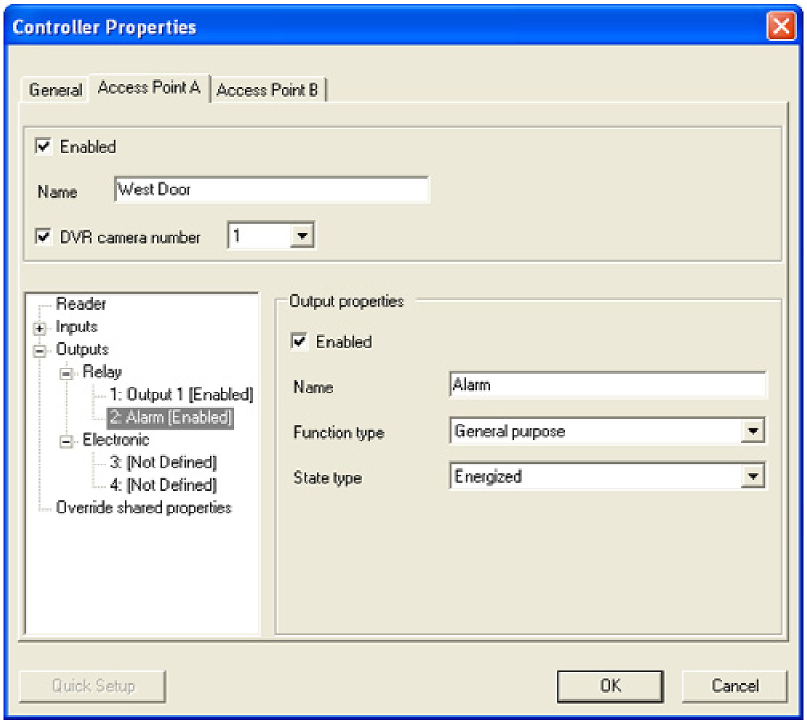
Tip

Use this form if the Door Lock output was not wired according to Card Access Controller Wiring Diagram.

To configure output settings, do the following:

1. Select **Outputs** entry in the tree list on the left hand side, then select one of the outputs: Relay or Electronic. Usually, Relay 1 is reserved for the Door Lock device. In the example below, Relay 2 output is selected. The properties for this output are displayed on the right side.

   The output number (1, 2, 3 or 4) is determined by the port on the Controller which the output is physically connected to. Please consult Card Access Controller Wiring Diagram for more information.



☑ Enabled

Name West Door

☑ DVR camera number 1

- Reader
- Inputs
- Outputs
  - Relay
    - 1: Output 1 [Enabled]
    - 2: Alarm [Enabled]
  - Electronic
    - 3: [Not Defined]
    - 4: [Not Defined]
- Override shared properties

Output properties

☑ Enabled

Name Alarm

Function type General purpose

State type Energized

2. Check off **Enable** checkbox to enable the selected output.

3. Enter the Name for the selected output. For simplicity, it is recommended to give the outputs unambiguous names, e.g. Alarm, Siren, etc.

4. Select **Function type** for the output from the corresponding drop-down menu. Only two function types are available for outputs on Portal Card Access System: Lock Door or General purpose. To connect all external output devices other than door lock device, select **General Purpose**.

5. Select **State type** of the output from the corresponding drop-down menu. The output may either be **Energized** (NC) or **De-energized** (NO). Please follow the device specifications.

6. Repeat steps 1-5 for all outputs connected to the Reader A side of the Controller. Please consult Card Access Controller Wiring Diagram for more information.

7. To save the settings and close Controller Properties window, click **OK**

3.2.4. Configuring Input Settings

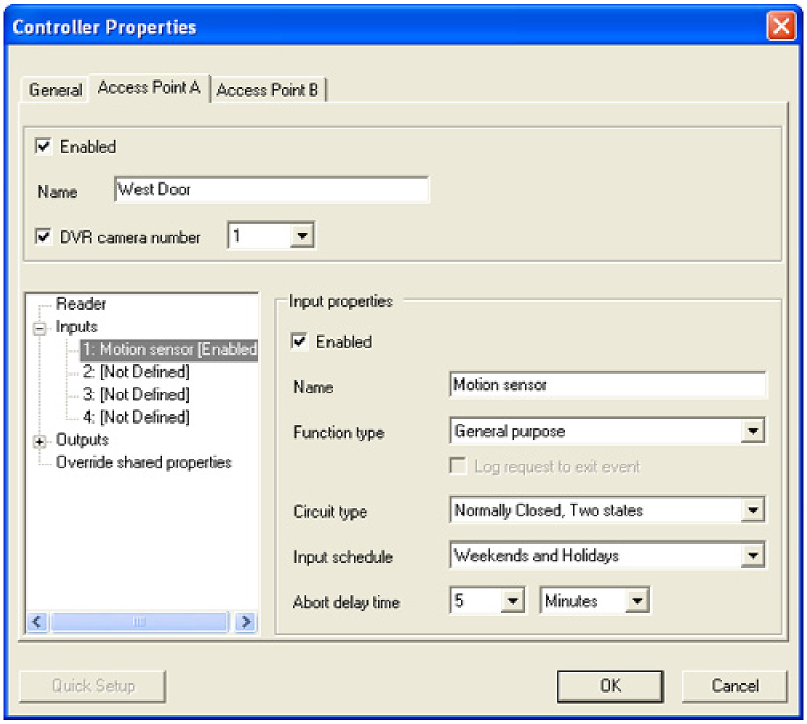
Tip

Use this form if the common inputs (such as RTE, Door Contact, Power Failure, Low Battery and/or Tamper) were not wired according to Card Access Controller Wiring Diagram

To configure input settings, do the following:

1. Select **Inputs** entry in the tree list on the left hand side, then select one of the four available inputs. Some inputs may already be reserved by Request-to-Exit device, Door Contact, Power Failure, Low Battery and/or Tamper devices. In the example below, Input 1 is selected. The properties for this input are displayed on the right side.

   The input number (1, 2, 3 or 4) is determined by the port on the Controller which the input is physically connected to. Please consult Card Access Controller Wiring Diagram for more information.



Controller Properties

General | Access Point A | Access Point B

☑ Enabled

Name: West Door

☑ DVR camera number: 1

Reader
Inputs
1: Motion sensor [Enabled
2: [Not Defined]
3: [Not Defined]
4: [Not Defined]
Outputs
Override shared properties

Input properties

☑ Enabled

Name: Motion sensor

Function type: General purpose

☐ Log request to exit event

Circuit type: Normally Closed, Two states

Input schedule: Weekends and Holidays

Abort delay time: 5 Minutes

2. Check off **Enable** checkbox to enable the selected input

3. Enter the Name for the selected input. For simplicity, it is recommended to give the inputs unambiguous names, e.g. Motion sensor, etc.

4. Select **Function type** for the output from the corresponding drop-down menu. The following function types are available for inputs on Portal Card Access System: Request to Exit, Door Contact, Power failure, Low battery, Tamper or General purpose. To connect all external input devices other than the ones listed in the Function type menu, **General Purpose**.

5. Select appropriate **Circuit type** for the connected input from the corresponding drop-down menu. Six circuit types are supported by Portal Card Access System; a separate event log will be generated for each circuit state. Please follow the device specifications to make this selection.

6. Configure the **Input schedule** by selecting one of the previously configured schedules from the drop-down menu. This schedule will determine when the input is being monitored (armed). In the example above, Input 1 on Access Point A is active based on "Weekends and Holidays" schedule.

7. Configure **Abort delay time** (seconds/minutes) for the selected input.

8. Repeat steps 1-7 for all inputs connected to the Reader A side of the Controller. Please consult Card Access Controller Wiring Diagram for more information.

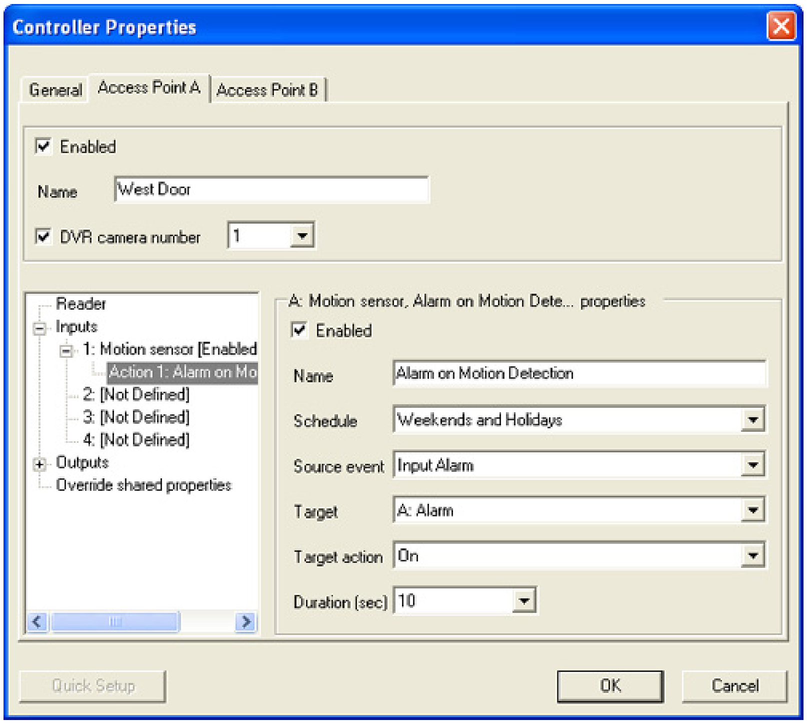
9. To save the settings and close Controller Properties window, click **OK**

3.2.5. Configuring Input Actions

Actions allow establishing a link between the inputs and outputs connected to the Controller. For example, if the motion is detected by the connected input, the output alarm device will be turned on.

To create an action for a configured input, do the following:

1. Select it in the tree list on the left hand side, right-click and select **Add new action...** from the context menu. In the example below, action was created for Input 1 on the Access Point A. The properties for the new action are displayed on the right side.



Controller Properties

☑ Enabled

Name: West Door

☑ DVR camera number: 1

A: Motion sensor, Alarm on Motion Dete... properties

☑ Enabled

Name: Alarm on Motion Detection

Schedule: Weekends and Holidays

Source event: Input Alarm

Target: A: Alarm

Target action: On

Duration (sec): 10

2. Check off **Enable** checkbox to enable the new action

3. Enter the Name for the created action. For simplicity, it is recommended to give the actions unambiguous names, e.g. Alarm on Motion Detection, etc.

4. Configure the action **Schedule** by selecting one of the previously configured schedules from the drop-down menu. This schedule will determine when the action is active. In the example above, Action 1 on Input 1, Access Point A is active based on "Weekends and Holidays" schedule.

5. Select appropriate **Source event** from the corresponding drop-down menu. The source event is a "trigger" event that happens on the configured input and that will in turn activate related action. The list of available source event will depend on the input''s Function type.

   Request to Exit events: Door unlocked on RTE

Low Battery events: Low battery, Low battery restored

Power failure events: No power, No power restored

Door Contact events: Door held open, Door held open restored, Forced entry, Forced entry restored, Input trouble, Input trouble restored

Tamper events: Tamper violation, Tamper violation restored

General purpose events: Input alarm, Input alarm restored, Input trouble, Input trouble restored

6. Configure the **Target** by selecting one of the previously configured outputs from the drop-down menu. The target defines which output will be activated when source event on the input is detected. In other words, which output will be activated as a result of this Action.

   In the example above, Alarm output on Access Point A will be activated on Input Alarm event detected on Input 1 on Access Point A.

7. Configure **Target action** from the corresponding drop-down menu. Depending on the selected output, the target actions may be On/Off (for General Purpose outputs) or Lock/Unlock (for Door Lock outputs).

8. Configure the **Duration (sec)** time for the new action. This time will specify how long the target output will remain active/inactive (depending on Target action). In the example above, Alarm output will remain ON for 10 seconds when Input Alarm is detected on Input 1. It is possible to set unlimited duration time, to do so select **Forever** from the drop-down menu.

9. Repeat steps 1-8 to create additional actions if so desired.

10. To save the settings and close Controller Properties window, click **OK**

3.3. Configuring Anti-Passback

Anti-Passback is a feature that against more than one person using the same card or number by preventing successive use of one card to pass through any access point in the same direction. This feature is optional and may be used in higher security applications.

To configure Anti-Passback feature, do the following:

Go to (Tools) -> Setup -> Access Control -> Anti-Passback -> Edit Anti-Passback properties. The Anti-Passback window will be displayed.

Portal Card Access System offers two types of Anti-Passback: Timed and Standard. These two anti-passback types are mutually exclusive, which means that each Controller on the network may participate only in one type of anti-passback at-a-time.

Timed Anti-passback prevents the use of the same card on the same Reader (door) for a period of time up to 1 hour. After the set time elapses, the card may be presented to the same reader (door) again.

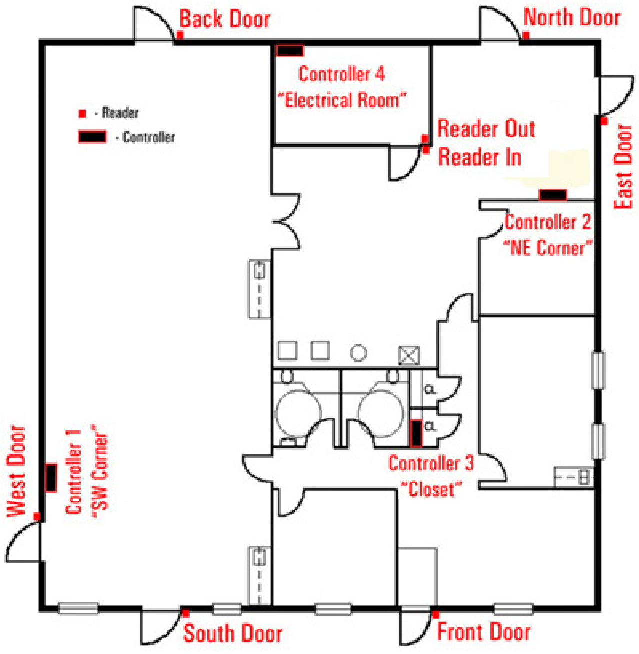
Standard Anti-passback requires assigning the readers with a status of either IN or OUT, where the card must be first presented to the IN reader for entry and then to OUT reader on exit. The same card may not be re-used on the IN reader until it is presented to the OUT reader. Standard anti-passback can only be used on the two readers connected to the same controller. Ideally, these readers should be mounted on the inside and on the outside of a single door of a secured facility.

Both Timed and Standard anti-passback settings can be set to either **Soft** or **Hard** type. In case of the Soft anti-passback setting violation, the access will still be granted, but a violation log will be generated. In case of the Hard anti-passback setting violation, the access will be denied and an alarm log will be generated.

Important

Anti-pass back will be forgiven at midnight of each day.

Sample of a Floor Plan

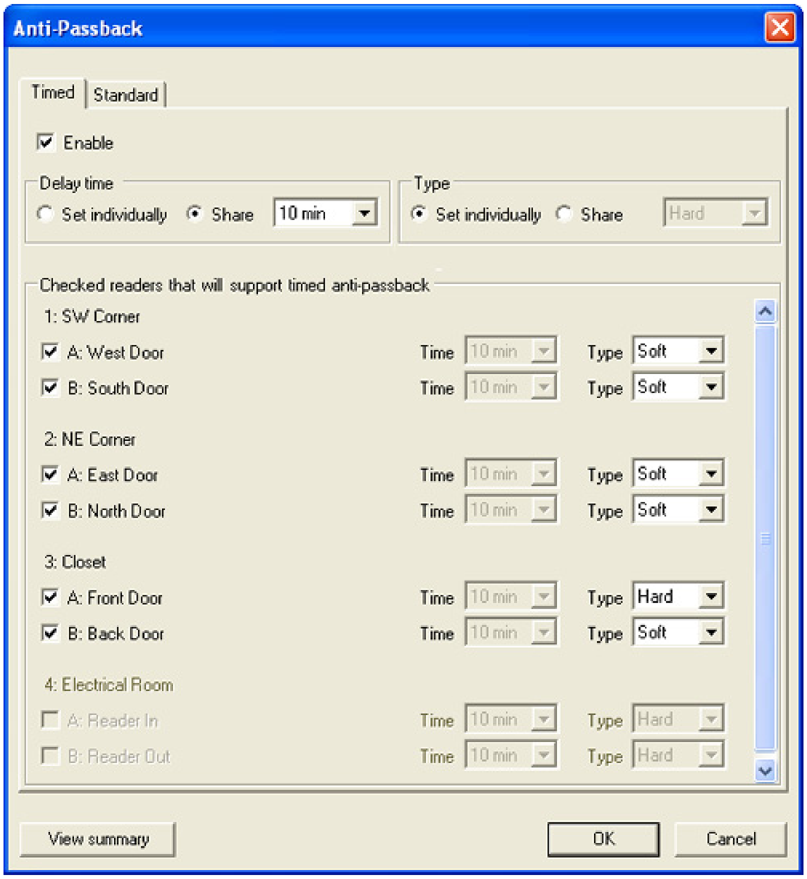


3.3.1. Configuring Timed Anti-Passback

Timed Anti-passback is configured separately for each reader.

To configure Timed Anti-Passback, do the following:

1. Click Timed tab in the Anti-Passback window. A list of all Controllers with their enabled readers will be displayed.



Anti-Passback

Timed | Standard

☑ Enable

Delay time: ○ Set individually ● Share 10 min

Type: ● Set individually ○ Share Hard

Checked readers that will support timed anti-passback

1: SW Corner			
☑ A: West Door	Time	10 min	Type Soft
☑ B: South Door	Time	10 min	Type Soft
2: NE Corner			
☑ A: East Door	Time	10 min	Type Soft
☑ B: North Door	Time	10 min	Type Soft
3: Closet			
☑ A: Front Door	Time	10 min	Type Hard
☑ B: Back Door	Time	10 min	Type Soft
4: Electrical Room			
☐ A: Reader In	Time	10 min	Type Hard
☐ B: Reader Out	Time	10 min	Type Hard

2. In the Delay time area, select **Set individually** radio button to set individual delay time for each participating reader.

   OR select **Share** radio button to set the same delay time for all participating readers. If Share option has been selected, set the shared delay time from the drop-down menu. Available delay time options are: 5 min, 15 min, 30 min, 45 min and 60 min. Delay time determines how many minutes must pass before the card holder can present the same card to the same reader.

   In the example above, the shared delay time has been set to 10 minutes.

Important

Remember that anti-pass back will be forgiven at midnight of each day.

3. In the Type area, select **Set individually** radio button to set individual anti-passback type for each participating reader.

   OR select **Share** radio button to set the same type all participating readers. If Share option has been selected, set the shared type from the drop-down menu. Available type options are: Soft and Hard. Anti-passback type determines whether or not access will be granted in the event violated anti-passback.

In the example above, the anti-passback type is configured individually for participating readers.

4. Check off all readers that will support timed anti-passback. In the example above, both readers from Controllers 1,2 and 3 will support timed anti-passback. Readers from the Controller 4 participate in the Standard anti-passback and therefore may not be selected for Timed anti-passback.

5. If **Set individually** was selected for the delay time setting, configure the delay time for each participating reader from the corresponding drop-down menu.

6. If **Set individually** was selected for the type setting, configure the type for each participating reader from the corresponding drop-down menu.

Important

After making changes to this form, manually upload settings.

According to the settings in the above example, the card holder will not be able to re-enter the Front Door for 10 minutes after their card was first presented to the Front Door reader. While North, South, East, West and Back doors all participate in the timed anti-passback, the card holders will still be granted access if their card is presented twice to either one of the doors within a 10-minute period. An anti-passback violation log will be generated in this case (use the sample floor plan image as a guide to better understand these settings).

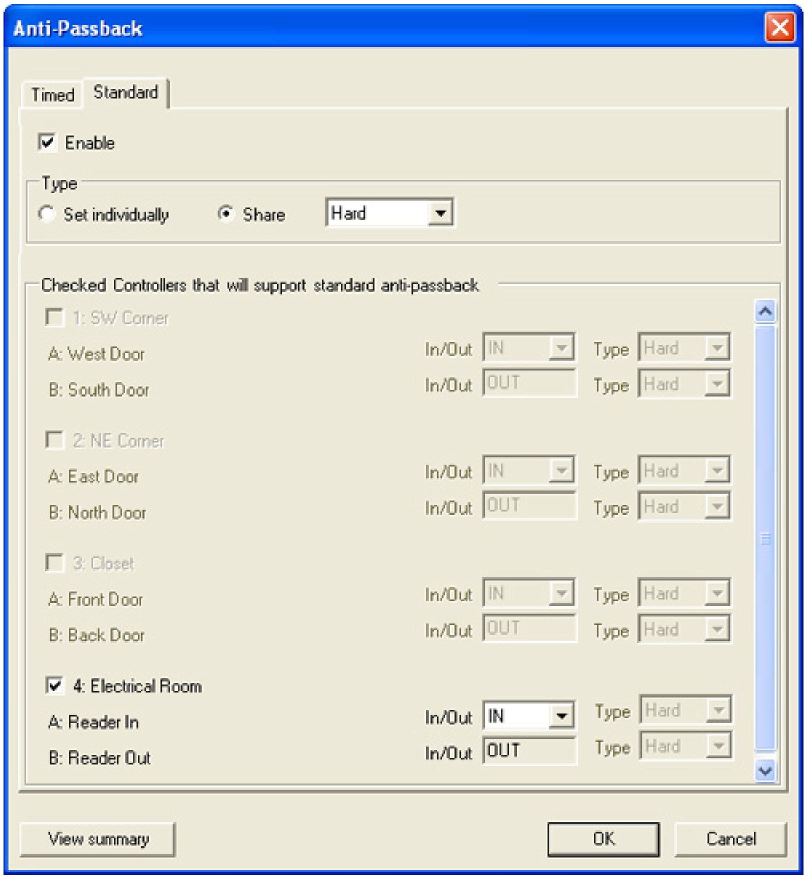
Important

Standard Anti-passback is configured separately for each controller.

3.3.2. Configuring Standard Anti-Passback

To configure Timed Anti-Passback, do the following:

1. Click Standard tab in the Anti-Passback window. A list of all Controllers with their enabled readers will be displayed.



Anti-Passback

Timed | Standard

☑ Enable

Type

○ Set individually ● Share Hard

Checked Controllers that will support standard anti-passback

☐ 1: SW Corner

A: West Door In/Out IN Type Hard

B: South Door In/Out OUT Type Hard

☐ 2: NE Corner

A: East Door In/Out IN Type Hard

B: North Door In/Out OUT Type Hard

☐ 3: Closet

A: Front Door In/Out IN Type Hard

B: Back Door In/Out OUT Type Hard

☑ 4: Electrical Room

A: Reader In In/Out IN Type Hard

B: Reader Out In/Out OUT Type Hard

2. In the Type area, select **Set individually** radio button to set individual anti-passback type for each participating reader.

OR select **Share** radio button to set the same type all participating readers. If Share option has been selected, set the type time from the drop-down menu. Available type options are: Soft and Hard. Anti-passback type determines whether or not access will be granted in the event violated anti-passback.

In the example above, the shared type has been set to Hard.

Remember that anti-pass back will be forgiven at midnight of each day.

3. Check off all controllers that will support standard anti-passback. In the example above, Controller 4 will support standard anti-passback. Controllers 1, 2, and 3 participate in the Timed anti-passback and therefore may not be selected for Standard anti-passback.

4. If **Set individually** was selected for the type setting, configure the type for each participating reader from the corresponding drop-down menu.

According to the settings in the above example, the card holder will not be able to re-enter the Electrical Room without presenting their card to the "Reader Out" first. This setting also means that if the card holder has entered the secured room without presenting their card to the "Reader In" first (e.g. the door was ajar, someone else has used their card to let the card holder in), access will not be granted (use the sample floor plan image as a guide to better understand these settings).

Important

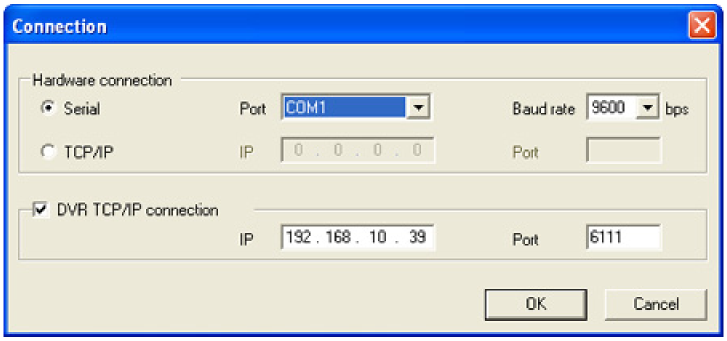
After making changes to this form, manually upload settings.

3.4. Configuring Text Overlay for DVMS

It is possible to configure Portal Card Access System to display logs on one of the i^{3}DVR DVMS video channels in form of text overlay. The DVMS must have a static IP address (no dynamic IP addresses are supported in this version) and a valid SPK key with text overlay support.

To configure Portal Card Access System for text overlay, do the following:

1. Go to (Tools) -> Connection -> Edit Connection properties. Connection window will be displayed.



Connection

Hardware connection

● Serial Port COM1 Baud rate 9600 bps

○ TCP/IP IP 0 . 0 . 0 . 0 Port

☑ DVR TCP/IP connection

IP 192 . 168 . 10 . 39 Port 6111

2. In the Connection window, check **off DVR TCP/IP connection** checkbox.

3. Enter the DVMS **IP** address (can be located in the DVMS Setup -> Server Info setup tab)

4. Enter **6111** as the text overlay *Port*

5. Click **OK** to save changes and close the Connection form.

6. Go to (Tools) Setup -> Access Control -> Controllers

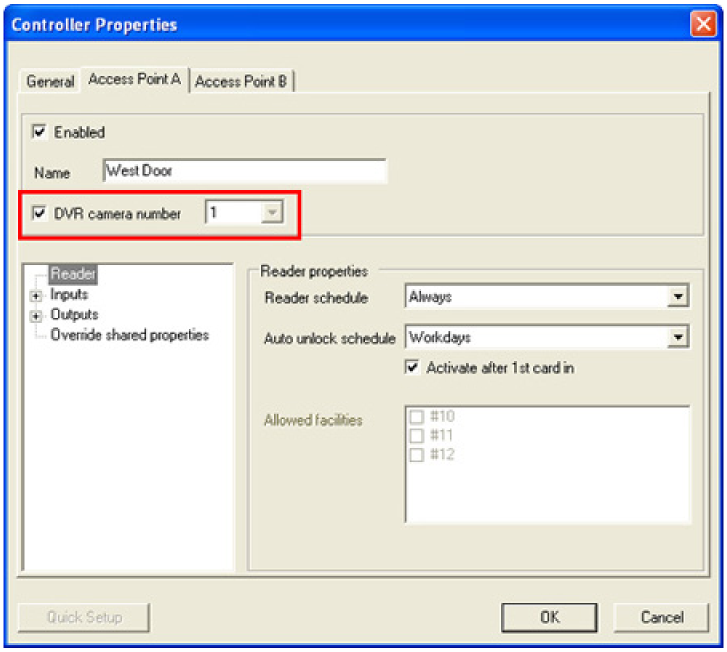
7. In the Controller Navigation window the list of all Access Points will be displayed sorted by Controller number. Double-click on the desired Access Point on the list to open Quick Controller Setup window.

8. Click **Advanced Setup** button to display Controller Properties window.

9. In the Controller Properties window, check off the DVR camera number checkbox and select the desired DVMS video input (refers to the Channel number and not to the physical BNC input number) from the drop-down menu. All event logs generated by this reader will be displayed on the selected DVMS channel.

Note

If the Controller settings have been previously customized, Controller Properties window will be displayed.



☑ Enabled

Name: West Door

☑ DVR camera number: 1

Reader schedule: Always

Auto unlock schedule: Workdays

☑ Activate after 1st card in

Allowed facilities: □ #10 □ #11 □ #12

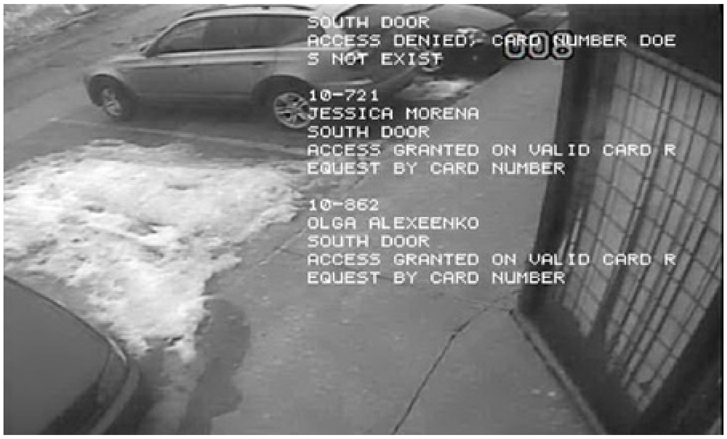
10. Repeat steps 7 - 9 for all desired readers. The operator may choose to associate all readers with the same video channel on DVMS or send event logs from different readers to different video channels. This type of setup may be preferred when DVMS cameras monitor Portal access points. The DVMS must have an SPK key that supports multiple text overlay channels if the text overlay from Portal Card Access System is being sent to multiple DVMS video channels.

    On the DVMS side, the operator must enable Text Overlay for all video channels selected in Portal Card Access System. Configure the Text Overlay Area, Text Color and Text Delay Time according to user preference.

> **Important**
>
> After completing the setup, manually upload settings.

11.

12. After uploading the settings, present a card to any of the configured readers to test text overlay function. The result should be similar to the one presented below.



```
SOUTH DOOR
ACCESS DENIED: CARD NUMBER DOE
S NOT EXIST

10-721
JESSICA MORENA
SOUTH DOOR
ACCESS GRANTED ON VALID CARD R
EQUEST BY CARD NUMBER

10-862
OLGA ALEXEENKO
SOUTH DOOR
ACCESS GRANTED ON VALID CARD R
EQUEST BY CARD NUMBER
```

13. Once the text overlay is properly configured on both sides (SRX-Pro and Portal), the operator may start using the camera icon that accompanies each event in the Portal Log Monitor. On double-click, the DVMS will open the corresponding video channel in the SRX-Pro Search mode. The exact moment of the event occurrence will be displayed in the search mode.

4

Appendix

Topics Covered

- Step-by-Step Hardware Installation Guide
- Card Access Controller Wiring Diagram
- Portal Card Access System Specifications
- Status LED''s and Reset Button
- Glossary

4.1. Step-by-Step Hardware Installation Guide

Tip

Take time to carefully label all connections, this will simplify the servicing procedure later on.

Caution

Any deviations from recommended installation sequence may result in the loss of product warranty.

Warning

Do NOT apply power to the unit until all installation steps, including wiring, mounting and grounding have been correctly completed. Remember to turn the power OFF when servicing the panel.

Thank you for purchasing Portal Card Access System, a product of i³DVR International.

This step-by-step manual describes the current installation considerations for the Portal Card Access system. The following document is designed to help a qualified technician to complete the installation safely and effectively. Before proceeding with the installation, please read the Installation Guide thoroughly and follow the instructions exactly. The following steps must be completed in order to set up the Portal Card Access system.

Step 1. Unpacking the Portal Card Access system and identifying system components

Step 2. Mounting Portal Card Access system on the wall

Step 3. Grounding Portal Card Access system

Step 4. Setting Portal Controller board(s) ID

Step 5. Connecting Power board(s) to Controller board(s)

Step 6. Connecting DB9 cable (RS-232) to *first* Controller board in the daisy chain

Step 7. Connecting Readers to their respective Controller board(s)

Step 8. Connecting multiple Controller boards into a daisy chain RS-485 network (if applicable)

Step 9. Connecting Inputs to the Controller board

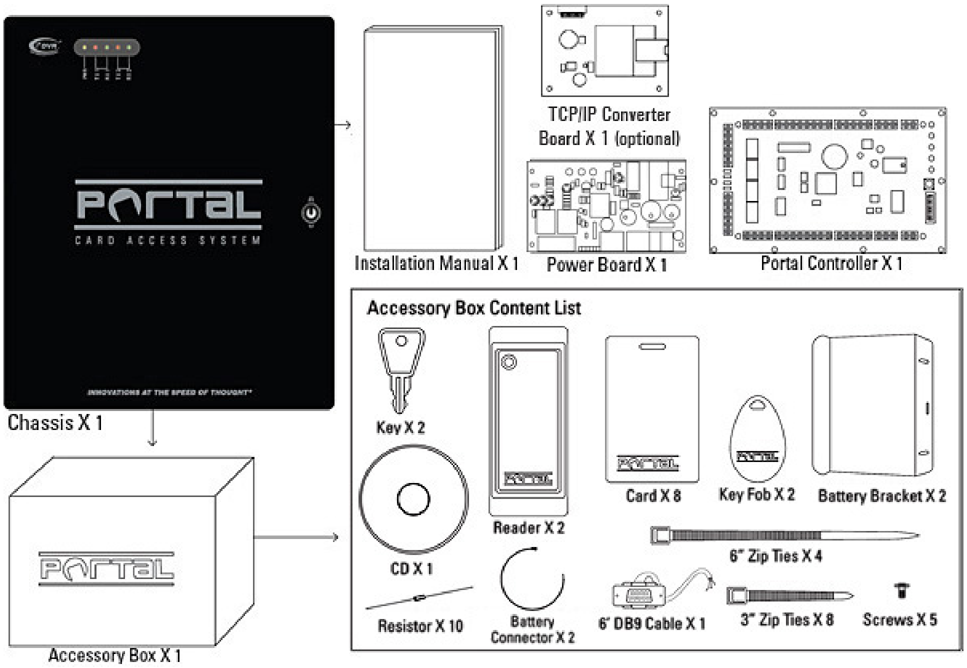
Step 10. Connecting Outputs to the Controller board

With any further questions or concerns, visit our website at http://www.i3dvr.com or contact our technical support team at 1-877-877-7241.

4.1.1. Unpacking

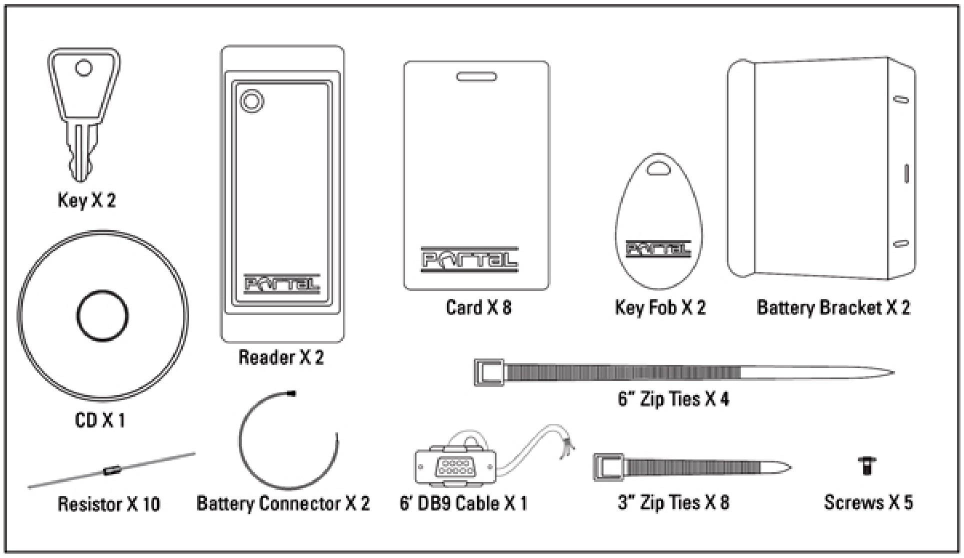
Make sure all the parts listed below have been included.

Power Board (P-PWR-U023) and Portal Controller boards (P-CA288) come pre-mounted inside the Portal chassis (P-PORTALCHASSIS). The accessory box (P-ACCESSORY) along with the installation manual (P-PORTALMANUAL) will be resting on top of the mounted boards inside the chassis.



Part No.	QTY	Description
P-PORTALCHASSIS	1	Portal Chassis. CamLock Included, Equipped with a Tamper Switch. Supports 1 x P-CA288, 1 x P-PWR-U023, 1 x I3-S2E (optional), 1 x Battery (not included)
P-CA288	1	Portal Card Access Controller Board. Supports 2 Readers
P-PWR-U023	1	Power Converter Board. Converts 24-28VAC input to 12VDC; supports Low Battery, Power Failure and Tamper inputs; charges the battery.
P-ALADDIN24	2	Aladdin 24 Proximity Reader. Wiegand Output, 4 to 5.5 inch Read Range, Metal Compensated, Mullion Width Indoor/Outdoor
P-ACCESSORY	1	Portal Accessory Box. Contains 2 x Keys, 5 x Screws, 2 x Battery Brackets, 2 x Battery Connectors, 4 x 6" Zip Ties, 8 x 3" Zip Ties, 10 x Resistors, Software CD w/User Manual
P-PORTALCARD	8	Badge Card. Pre-punched in Portrait Orientation
P-PORTALKEYFOB	2	Proximity Key Tag
P-PORTALDB9	1	6 foot serial 9-pin DB9 Cable to connect P-CA288 to PC/DVMS
P-PORTALMANUAL	1	Printed Installation Manual for Portal Card Access System
I3-S2E	(1) Optional	Serial to TCP/IP converter board for the Portal Card Access System

Accessory Box Content List



Additional parts required for each Controller (not included in the package):

- 24-28 AC, 40 VA, 1-3 Amp Transformer
- 12V Battery, recommended 7.0 Ah

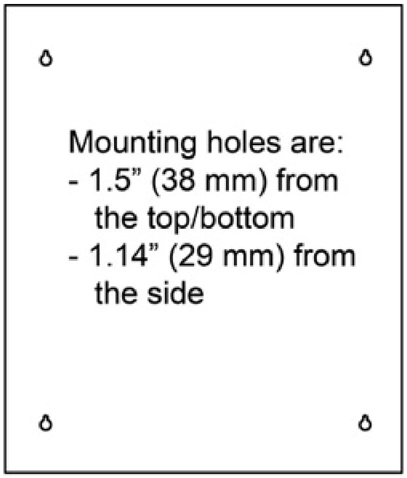
It is the installer''s responsibility to purchase and install additional required parts. A 24-28 AC transformer is required to convert commercial 110 AC to 24 VAC accepted by power board (P-PWR-U023). Power board will then convert 24 VAC to 12 VDC accepted by Portal Controller board (P-CA288).

Compatible battery type: 12V rechargeable battery, recommended rating of 7.0 Ah. The unit will operate normally without a battery, however battery-operated power backup is highly recommended to prevent Portal system downtime due to power failure.

4.1.2. Mounting Portal Card Access System

Mounting

- The operating environment for the Portal is 0° to 70°C (35° ~ 150°F) and 20-80% RH non-condensing
- The dimension for the Portal chassis is: 14" H x 11 ¾ " W x 3 ¼" D (35.56 cm H x 29.85 cm W x 8.26 cm D)
- Screw the Portal chassis onto a secure wall

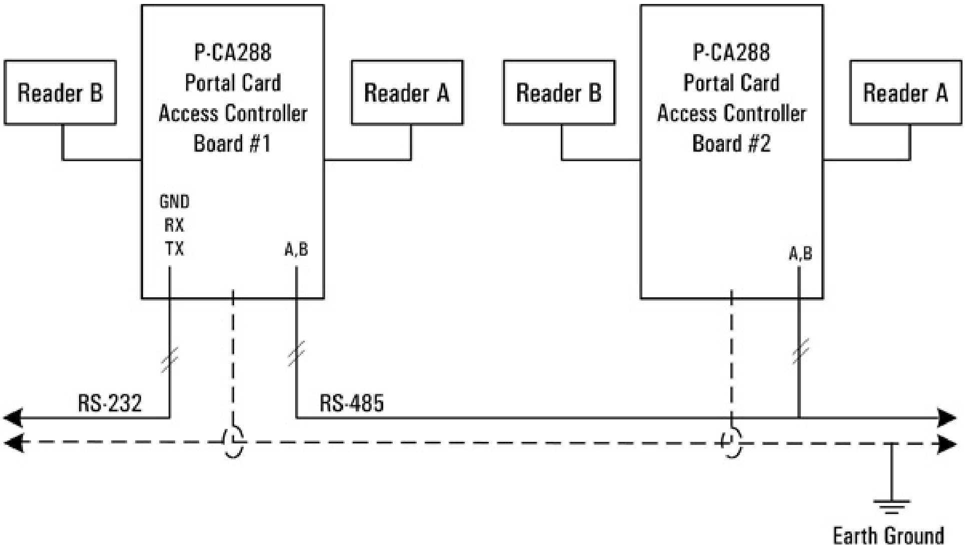

Mounting holes are:
- 1.5” (38 mm) from the top/bottom
- 1.14” (29 mm) from the side

4.1.3. Grounding Portal Card Access System

Grounding the Portal metal chassis box is very important to prevent damage due to lightning or static discharge. Direct grounding of the chassis is essential and can be done by connecting a 16 AWG or heavier cable to earth ground. The length of grounding cable must not exceed 50 feet (15 m). Each Portal chassis should be grounded individually to the earth ground.

When installing Portal, you MUST ground yourself to prevent static discharge. Do not apply power the unit before completing all installation steps and correctly grounding each Portal Controller Chassis (P-PORTALCHASSIS).

Grounding multiple Portal panels.



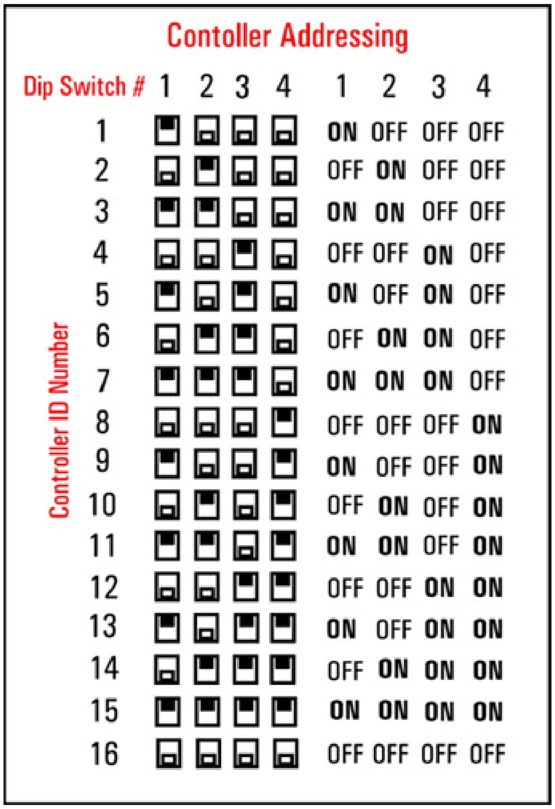
4.1.4. Configuring Controller ID

To locate the dip switch on the board, see the Card Access Controller Wiring Diagram.

Use the dip switch on the Portal Card Access board(s) to configure ID for each Controller board in the network. Portal Card Access System supports up to 16 Controller boards in a single network, each one must be assigned a unique ID from "1" to "16".

Each Controller board has 8 dip switches, first 4 (four) are designated for configuring the Controller ID. Follow the table below to set the Controller ID.

Complete this step for each Portal Controller board.

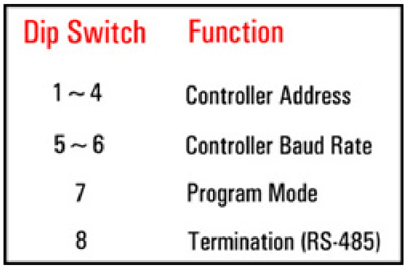


Contoller Addressing

Controller ID Number / Dip Switch #	1	2	3	4	1	2	3	4
1	⬒	⬓	⬓	⬓	ON	OFF	OFF	OFF
2	⬓	⬒	⬓	⬓	OFF	ON	OFF	OFF
3	⬒	⬒	⬓	⬓	ON	ON	OFF	OFF
4	⬓	⬓	⬒	⬓	OFF	OFF	ON	OFF
5	⬒	⬓	⬒	⬓	ON	OFF	ON	OFF
6	⬓	⬒	⬒	⬓	OFF	ON	ON	OFF
7	⬒	⬒	⬒	⬓	ON	ON	ON	OFF
8	⬓	⬓	⬓	⬒	OFF	OFF	OFF	ON
9	⬒	⬓	⬓	⬒	ON	OFF	OFF	ON
10	⬓	⬒	⬓	⬒	OFF	ON	OFF	ON
11	⬒	⬒	⬓	⬒	ON	ON	OFF	ON
12	⬓	⬓	⬒	⬒	OFF	OFF	ON	ON
13	⬒	⬓	⬒	⬒	ON	OFF	ON	ON
14	⬓	⬒	⬒	⬒	OFF	ON	ON	ON
15	⬒	⬒	⬒	⬒	ON	ON	ON	ON
16	⬓	⬓	⬓	⬓	OFF	OFF	OFF	OFF

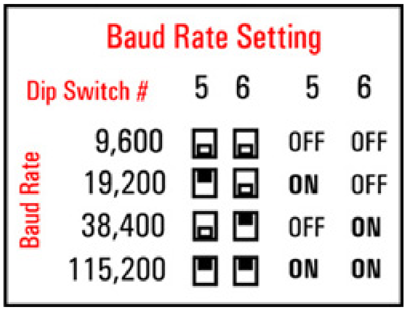
4.1.4.1. Controller Dip Switch

Aside from Controller addressing, the Controller dip switch is also used to configure Controller baud rate, enable system for firmware upgrade and to terminate the data transmission for longer cable runs.



Dip Switch	Function
1 ~ 4	Controller Address
5 ~ 6	Controller Baud Rate
7	Program Mode
8	Termination (RS-485)

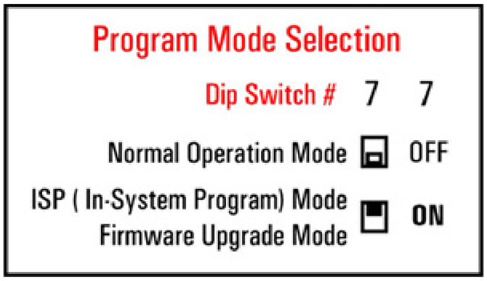
The baud rate used for Portal Card Access system is 9600, therefore dip switches 5 and 6 must be left in the OFF position on ALL Controllers in the network.



Baud Rate Setting

	Dip Switch #	5	6	5	6
Baud Rate	9,600	▄	▄	OFF	OFF
	19,200	▀	▄	ON	OFF
	38,400	▄	▀	OFF	ON
	115,200	▀	▀	ON	ON

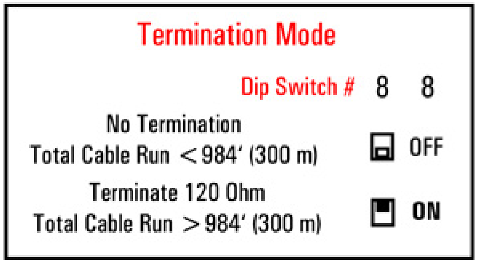
Dip switch 7 must be in the ON position *only* during the firmware update. For normal operation, dip switch 7 must remain in the OFF position.



Program Mode Selection

Dip Switch #	7	7
Normal Operation Mode	▄	OFF
ISP (In-System Program) Mode Firmware Upgrade Mode	▀	ON

Dip switch 8 is used when the total cable run in the daisy chain is longer than 984 ft (300 m). In this case, dip switch 8 must be in the ON position on the last Controller board in the chain, leave the dip switch in the OFF position for shorter cable runs. Dip switch 8 must stay in the OFF position at all times for all Controller boards except for the last one in the chain.



Termination Mode

Dip Switch #	8	8
No Termination Total Cable Run < 984' (300 m)	▄	OFF
Terminate 120 Ohm Total Cable Run > 984' (300 m)	▀	ON

4.1.5. Connecting Controller to Power Board

Power board converts the 24 VAC to 12 VDC. The Portal Controller board requires 10.8 to 13.2 volts DC and draws approximately 250mA.

Each Portal Card Access system comes with a Power board, pre-mounted inside the Portal chassis. Remember that the 24-28 AC, 40 VA, 1-3 Amp transformer is required to convert the 110 AC to 24 VAC accepted by Power board. Transformer is not shipped with the system and must be purchased separately by the installer.

Connect the 24VAC power transformer to the AC terminals on the Power board (P-PWR-U023). Then connect the Controller board (P-CA288) to the DC terminals on the P-PWR-U023. Follow the Card Access Controller Wiring Diagram to properly wire the Portal Controller board to Power board.

Next, install the 12V rechargeable battery (not included with the system) inside Portal Chassis. Connect the battery to the corresponding terminals on the Power board (P-PWR-U023). Note that each Portal Controller board requires a separate battery.

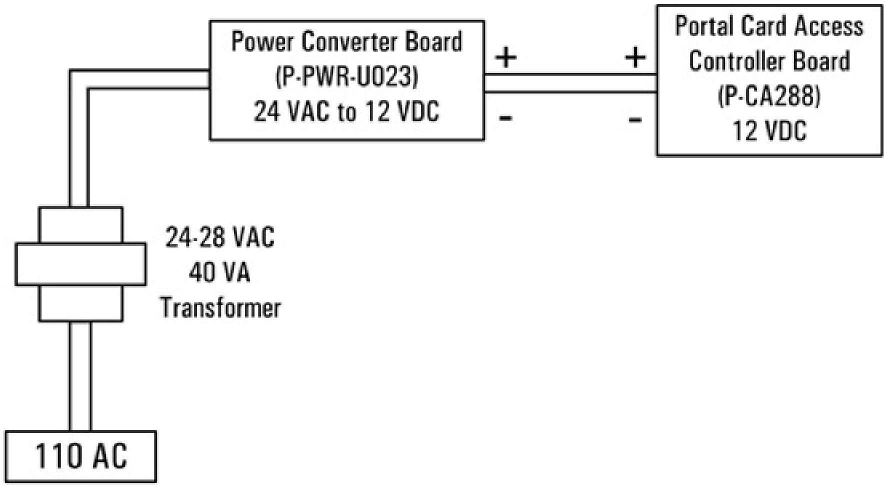
Warning

Electric door strike, magnetic lock, and all other peripheral devices must use external power supply. Although the Portal Card Access System comes with a power board (P-PWR-U023), it is designated for the Portal Controller board use ONLY.

Tip

A single transformer could be used for all Portal Controller boards in the network. The transformer rating needs to be adjusted according to the number of Portal Controller boards connected to it.

Complete these steps for each Portal Card Access panel.



4.1.6. Connecting RS-232 DB9 Cable to First Controller

Note

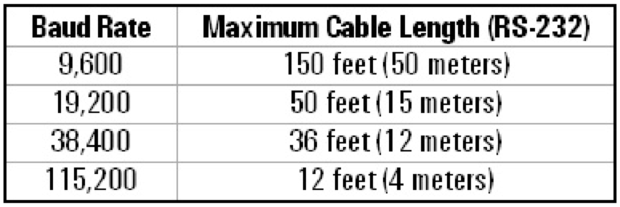
Skip this step if TCP/IP interface is used to connect first Controller to Host PC and refer to Serial to TCP/IP Converter Board section for further instructions.

Connect DB9 RS-232 cable (P-PORTALDB9) shipped with the system to the *first* Portal Controller board in the daisy chain. This cable will be later connected to the COM port on the Host PC in order to communicate with the installed Portal software application. Follow the Card Access Controller Wiring Diagram to properly wire the DB9 cable to the Controller board.

Complete this step only for the *first* Controller board in the network chain.

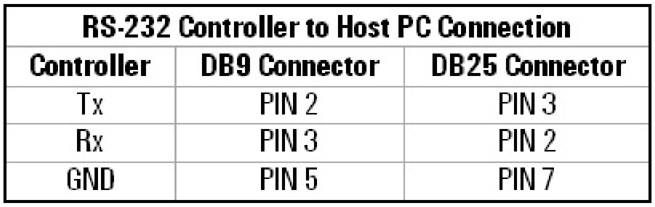
Follow the table below for maximum RS-232 cable runs. Since 9600 baud rate must be used with Portal Card Access system, the maximum RS-232 cable length may not exceed 150 feet (50 meters).

For longer cable runs, TCP/IP interface upgrade can be used. See Serial to TCP/IP Converter Board section for more information.



Baud Rate	Maximum Cable Length (RS-232)
9,600	150 feet (50 meters)
19,200	50 feet (15 meters)
38,400	36 feet (12 meters)
115,200	12 feet (4 meters)

Communication to the host computer via RS-232 serial COM port.



RS-232 Controller to Host PC Connection		
Controller	DB9 Connector	DB25 Connector
Tx	PIN 2	PIN 3
Rx	PIN 3	PIN 2
GND	PIN 5	PIN 7

4.1.6.1. Serial to TCP/IP Converter Board

If Serial to TCP/IP converter board (I3-S2E) was purchased as a part of the optional system upgrade, you will need to connect the converter to the 5-pin ethernet connector on the Controller board. See Card Access Controller Wiring Diagram to locate the ethernet connector on the P-CA288 board. Then connect the Ethernet connector to Local Area Network and connect the Host PC to LAN as well.

Set the converter''s IP address with the dedicated software application found on the software CD that is shipped with the system. During Portal Card Access System software installation enter the converter''s IP address and port number in the Controller Connection setup. The default port number is **10001**.

4.1.6.2. Configuring IP Address for TCP/IP Converter

The IP address of the TCP/IP converter is configured with the Lantronix software that can be found on Portal Card Access System CD that is shipped in the accessory box.

Follow these instructions to configure the IP address for TCP/IP converter:

1. Connect the RJ45 network cable to LAN (switch, hub, etc.) on one side and to TCP/IP converter board on the other side.

2. Connect the TCP/IP converter board to the 5-pin connector on the Controller board.

3. Open the Portal Card Access System CD and locate Lantronix folder.

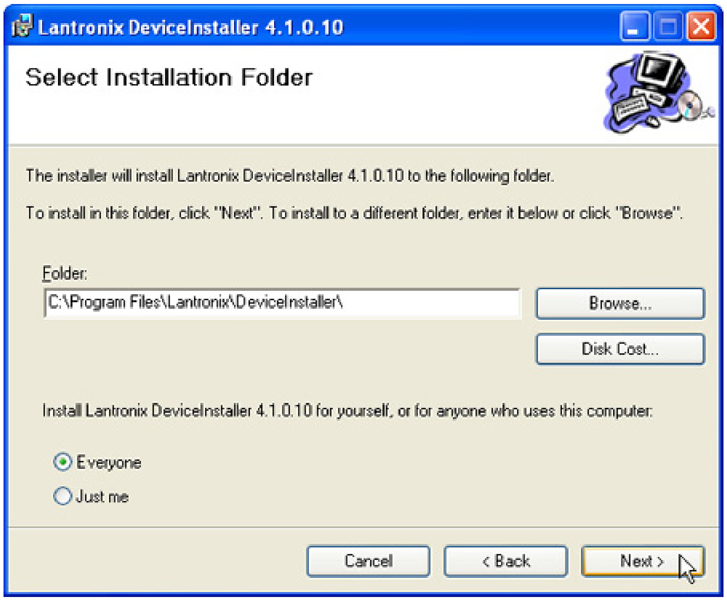
4. Double-click the **Launch.exe** file inside the Lantronix folder.

5. The Xport Direct Device Server wizard window will be displayed. Click on **DeviceInstaller** option.

6. Lantronix Device Installer wizard window will be displayed. Click **Next**.

7. In Select Installation Folder screen, select installation drive and folder by clicking **Browse...** or keep the default installation folder (recommended).

   Select **Everyone** radio button and click **Next**.



Lantronix DeviceInstaller 4.1.0.10

Select Installation Folder

The installer will install Lantronix DeviceInstaller 4.1.0.10 to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Lantronix\DeviceInstaller\

Install Lantronix DeviceInstaller 4.1.0.10 for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

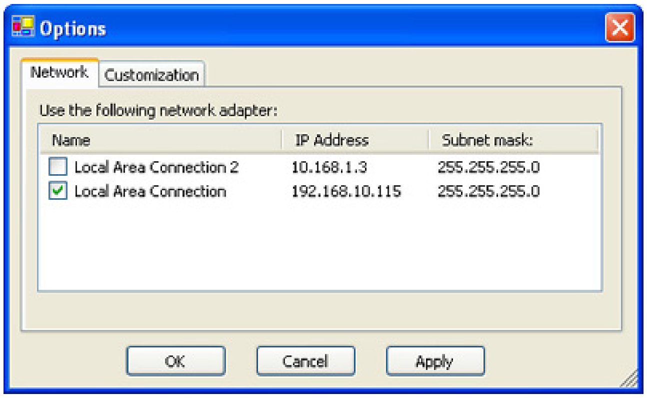
8. In Confirm Installation screen, click **Next** to proceed with the installation.

9. Wait while the Lantronix DeviceInstaller software is installing onto the local system.

10. Wait for the Installation Complete screen to be displayed and click **Close**.

11. **Go Start** -> **All Programs** -> **Lantronix** -> **DeviceInstaller** -> **DeviceInstaller** to launch the Lantronix DeviceInstaller application.

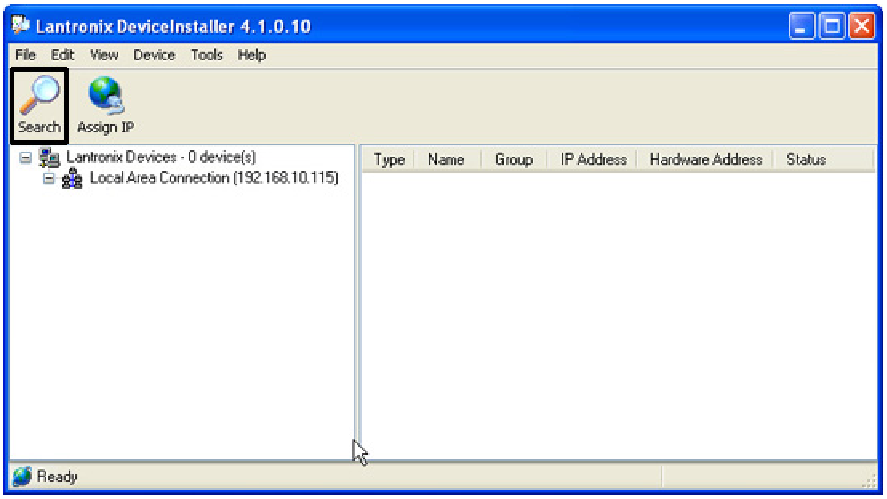
12. If you have multiple network adapters (network cards) on your PC, click **Yes** in the Multiple Network Adapters Present window, then check off the desired Local Area Connection to be used in conjunction with this application and click **OK**. This step does not apply if you have only one network adapter installed on your PC, the default available Local Area Connection will be selected automatically.



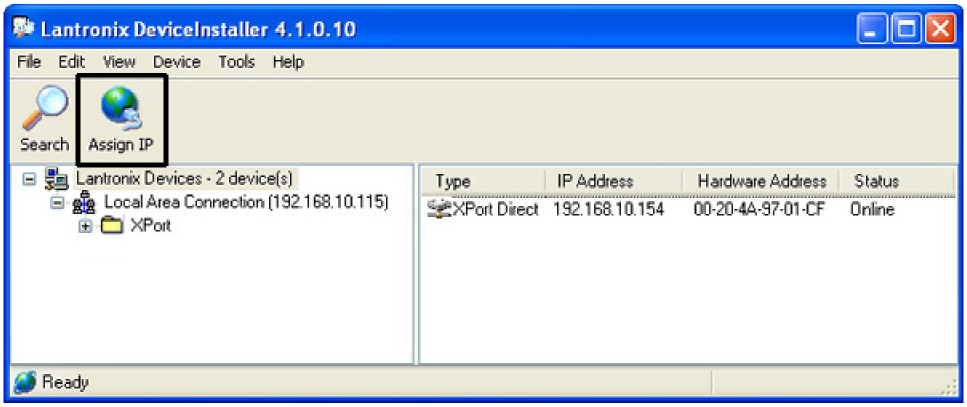
Use the following network adapter:

Name	IP Address	Subnet mask:
□ Local Area Connection 2	10.168.1.3	255.255.255.0
☑ Local Area Connection	192.168.10.115	255.255.255.0

13. In the Lantronix DeviceInstaller application window, click the **Search** button to search for the TCP/IP converter on LAN.


Lantronix DeviceInstaller 4.1.0.10
File
Edit
View
Device
Tools
Help
Search
Assign IP
Lantronix Devices - 0 device(s)
Local Area Connection (192.168.10.115)
Type
Name
Group
IP Address
Hardware Address
Status
Ready

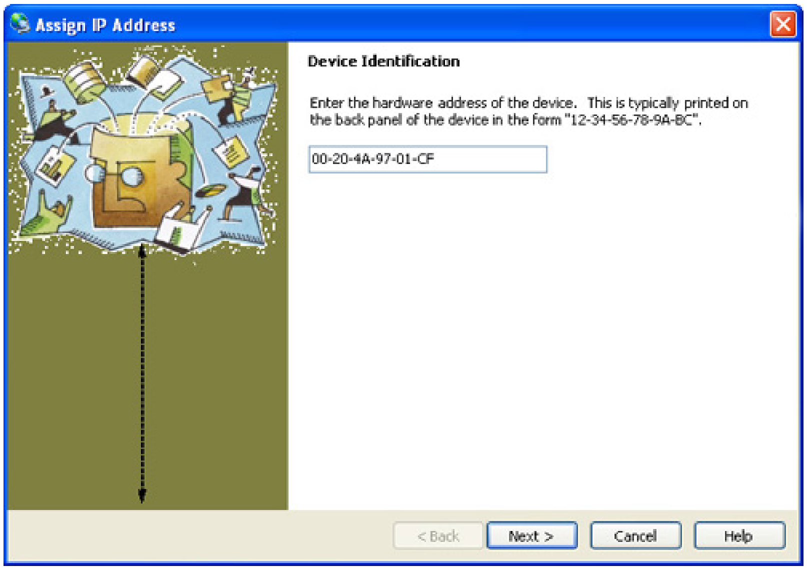
14. The XPort Direct device will be displayed as shown in the image below. Write down the Hardware Address displayed for XPort Direct device in the right window pane, then click the **Assign IP** button.


Lantronix DeviceInstaller 4.1.0.10
File Edit View Device Tools Help
Search
Assign IP
Lantronix Devices - 2 device(s)
Local Area Connection (192.168.10.115)
XPort
Ready

Type	IP Address	Hardware Address	Status
XPort Direct	192.168.10.154	00-20-4A-97-01-CF	Online

> **Tip**
>
> The Hardware Address is the MAC address, which is also printed on the TCP/IP converter device (I3-S2E).

15. In the Device Identification window, enter the Hardware Address noted in the previous step and click **Next**.



Device Identification

Enter the hardware address of the device. This is typically printed on the back panel of the device in the form "12-34-56-78-9A-BC".

00-20-4A-97-01-CF

16. In the next window, select one of the two available options: **Obtain an IP address automatically** or **Assign a specific IP address** and click **Next**.

    Select the first option to assign the IP address automatically, select the second option only if specific IP address is preferred.

    If the first option is selected, simply click **Next** in the IP Discovery Settings window. If the second option is selected, enter **IP address**, **Subnet mask** and **Default gateway**, then click **Next**.

17. Click **Assign** button in the Assignment window and wait while the IP address is being assigned to the device.

18. Wait for the "**Completed successfully**" message to be displayed, then click **Finish**.

19. If the IP address was assigned automatically to the TCP/IP converter, make a note of the device IP address.

20. Close any Lantronix windows that may still be open.

4.1.7. Connecting Reader(s) to Controller

Note

This step may also be completed after system mounting.

Note

All access cards (P-PORTALCARD) purchased from i³DVR are 46 bit i3DVR proprietary format.

Important

The cable run from the reader to Controller board must not exceed 1000 ft (305m). Shielded Straight 22 AWG 6 Stranded cable must be used for this connection.

Each Portal Controller board supports up to 2 (two) proximity readers (P-ALADDIN24), readers A and B. The readers support Wiegand output, 26 bit and/or i3DVR proprietary format, 46 bit.

Follow the Card Access Controller Wiring Diagram as well as a wiring diagram below to properly connect each reader to Portal Controller board.

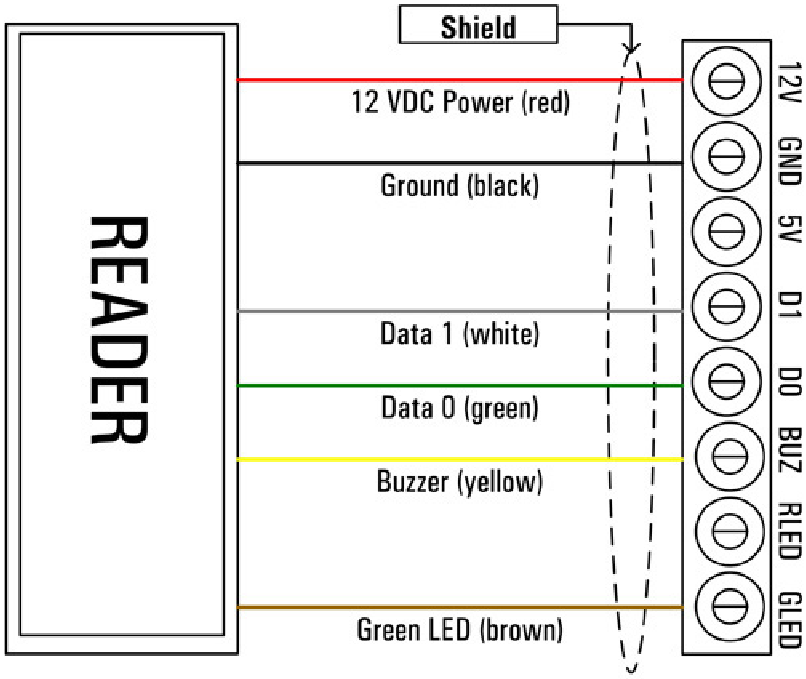
Complete this step for each Portal Controller boards.

Seven wires from each Reader must be connected to the Portal Controller board terminals:

Wire Color	Controller terminal	Purpose
orange	not used	cut and tape
violet	not used	cut and tape
blue	not used	cut and tape
red	**12V**	**12VDC power**
black	**GND**	**ground**
white	**D1**	**Data 1**
green	**D0**	**Data 0**
yellow	**BUZ**	**buzzer (optional)**
brown	**GLED**	**green LED**
silver (shield)	**shield**	**earth ground at panel**

Tip

Buzzer (optional) is used to sound local alarm in case of detected forced entry and door held open. Buzzer is also used to indicate that the card has been successfully read by the reader device.



The two supported readers may be used on two separate access points (doors) for the IN access to the premises or on a single access point (door) for IN access/OUT confirmation.

When installing two readers back-to-back on opposite sides of the wall at a doorway, interference may occur preventing the normal operation of the readers. Avoid installing the readers back-to-back, instead space them out along horizontal axis. In addition, insert metal between the back-to-back readers, for example, aluminum foil spread out in the space between the drywall, or a metal sheet (larger than the reader) between one reader and the wall behind it.

Tip

To prevent interference, avoid mounting the readers back-to-back. Use shielding between back-to-back readers to prevent interference.

A metal shield behind a reader will shorten its read range in front of the reader.

Depending on whether readers are used on two or one access point (door), the designations for input and output devices will change. See Card Access Controller Wiring Diagram and Connecting Inputs to Controller, Connecting Outputs to Controller sections for more information.

Please also refer to Aladdin 24 Proximity Reader installation sheet for more instructions.

4.1.8. Connecting Multiple Controllers into a Network (RS-485)

Note

Skip this step if only one (1) Portal Controller board is used.

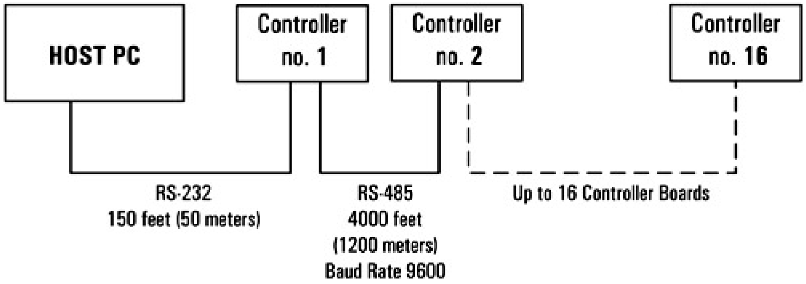
Connect all Portal Card Access system into a single daisy-chain network. Follow the Card Access Controller Wiring Diagram to properly connect Controllers into a network. Use single twisted pair, shielded, 18 to 22AWG cable.

All used Controller boards must be connected into a daisy-chain network via RS-485 interface. The *first* Controller in the chain will be connected to the Host PC via RS-232 interface (See Connecting RS-232 DB9 Cable to First Controller section for more information). If the total RS-485 network cable run length exceeds 984 ft (300 m) but is still within allowed 4000 feet (1200 m), terminate the data transmission on *last* Controller in the chain with the dip switch #8. (See Controller Dip Switch section for more information)

Note

Up to 16 Controller boards can be used in a single network.

Complete this step for the each Controller boards in the daisy chain.



Follow the table below for maximum RS-485 cable runs.

Baud Rate	Maximum Cable Length (RS-485)
9,600	4000 feet (1200 meters)
19,200	3000 feet (1000 meters)
38,400	3000 feet (1000 meters)

Communication between Controller boards via RS-485 connection.

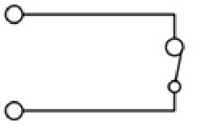
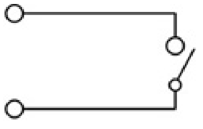
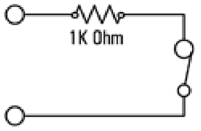
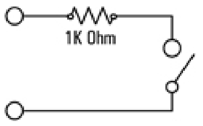
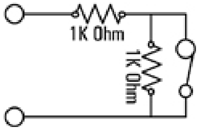
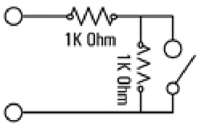
RS-485 Controller to Controller Connection	
Controller n	Controller n+1
G	G
N (-)	N (-)
P (+)	P (+)

4.1.9. Connecting Inputs to Controller

Each P-CA288 Controller supports two sets (banks) of four inputs with one common terminal, one bank of inputs per each reader. Note that even if only one reader is used per Controller, all 8 inputs may still be used.

All inputs can be individually programmed in Portal software application via host PC.

Six circuit types are supported. A log will be generated for each change of state in the Portal software application.

1. Normally closed. Two states: Alarm, Restore		**2.** Normally open. Two states: Alarm, Restore	
3. Normally closed, with 1 resistor. Three states: Alarm, Restore, Trouble.		**4.** Normally open, with 1 resistor. Three states: Alarm, Restore, Trouble.	
5. Normally closed, with 2 resistors. Four states: Alarm, Restore, Trouble - Open Circuit, Trouble - Short Circuit		**6.** Normally open, with 2 resistors. Four states: Alarm, Restore, Trouble - Open Circuit, Trouble - Short Circuit	

The Controller inputs are used for: **RTE (Request to Exit)** devices, **Door Contacts**, **Tamper**, **Low battery** and **Power failure** inputs as well as **General Purpose** inputs. Below is the standard wiring chart for both input banks. Follow this chart *exactly* to use the *Quick Setup* function when configuring the system inside Portal software application.

If each reader is used on a separate access point for IN access:

- Connect each reader''s **RTE device** to **AIN1** and **BIN1** inputs on Controller board respectively. Skip this step if no RTE devices are used.

- Connect each reader''s **Door Contact** to **AIN2** and **BIN2** inputs on Controller board respectively. Skip this step if no Door Contacts are used.

  Door Contact is a magnetic contact that is mounted on the frame of the controlled opening (e.g. door). Door contact is used to monitor the door status and to detect such occurrence as forced entry, door held open alarm/warning. The Portal software recognizes Door Contact states, generates emergency logs and uses the local alarm (if enabled) when forced entry or door held open is detected.

  Only one Door Contact input should be used per access point (door), therefore if both readers are used on the same access point, only **AIN2** terminal should be used for Door Contact device.

- Connect **Tamper** input to **AIN3** input on Controller board. Portal Card Access chassis (P-PORTALCHASSIS) already comes with a N/C tamper switch for tamper detection, no additional hardware is needed. Skip this step if you choose not to use Tamper input.

- Connect **Low battery** sensor to **AIN4** input on Controller board and to the appropriate terminals on Power board (P-PWR-U023). Skip this step if no Low battery input is used.

  In case when a low battery level is detected by Power board (P-PWR-U023), **AIN4** Input on Controller board will be triggered and an emergency log will be generated by the Portal software.

- Connect **Power Failure (AC)** sensor to **BIN3** input on Controller board and to the appropriate terminals on Power board (P-PWR-U023). Skip this step if no Power Failure input is used.

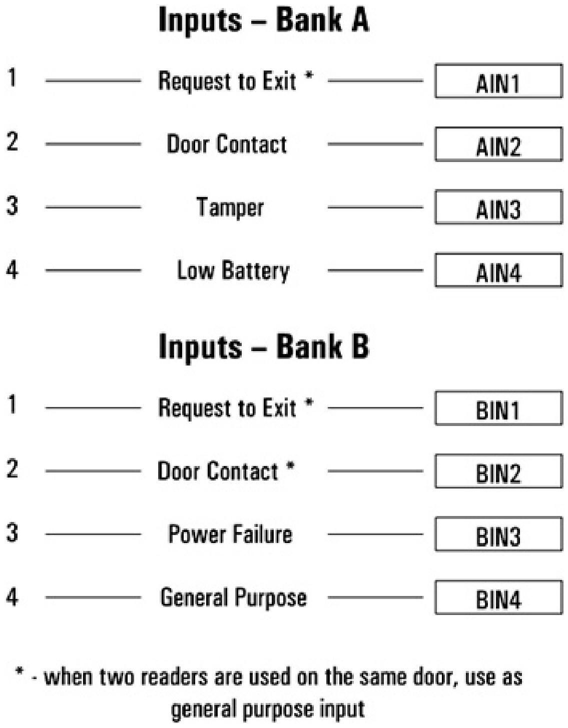
  In case when AC power failure is detected by Power board (P-PWR-U023), **BIN3** Input on Controller board will be triggered and an emergency log will be generated by the Portal software.

  Note that the compatible battery must be purchased and installed in order to keep the system online during the general AC power failure. If no battery is used with Portal Card Access system, AC power failure will be undetectable from the software point of view as no power will be available to trigger the corresponding sensor and to send information back to the host PC.

- Connect general purpose input devices to **BIN4** input on Controller board.

If both readers are used on the same access point for IN access/OUT confirmation:

- No RTE devices will be used
- Only one Door Contact will be used (AIN2 input) as only one door contact per access point is required
- Connect general purpose input devices to **AIN1**, **BIN1** and **BIN2** inputs on Controller board



Inputs – Bank A

1	Request to Exit *	AIN1
2	Door Contact	AIN2
3	Tamper	AIN3
4	Low Battery	AIN4

Inputs – Bank B

1	Request to Exit *	BIN1
2	Door Contact *	BIN2
3	Power Failure	BIN3
4	General Purpose	BIN4

* - when two readers are used on the same door, use as general purpose input

4.1.10. Connecting Outputs to Controller

Each P-CA288 Controller board supports two sets (banks) of relay outputs and two banks of electronic outputs split equally between two readers. Note that even if only one reader is used per Controller, all 8 outputs may still be used.

All outputs can be individually programmed in Portal software application via host PC.

The Controller inputs are used for: **Door Lock** contacts as well as **General Purpose** outputs. Below is the standard wiring chart for both output banks. Follow this chart *exactly* to use the *Quick Setup* function when configuring the system inside Portal software application.

Caution

Please confirm with your local fire bylaw code before installing any door strike or magnetic lock

If each reader is used on a separate access point for IN access,

- Connect Door Lock contacts for each reader to their respective relay Output 1 (**AOUT1** and **BOUT1**) terminals on Controller board. Skip this step if no Door Lock output is used.

  Follow the Card Access Controller Wiring Diagram for instructions on how to connect door strike and/or magnetic lock to the Portal Controller board.

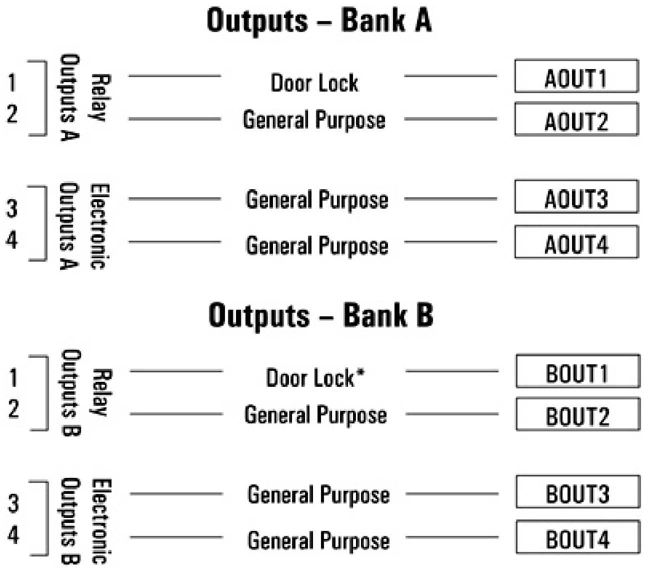
- Use relay Outputs 2 on both readers (**AOUT2** and **BOUT2**) as well as all electronic Outputs (**AOUT3**, **AOUT4**, **BOUT2**, **BOUT3**, and **BOUT4**) terminals on Controller board for general purpose output devices. Follow the device specifications to properly connect them to the Portal Controller board.

Warning

Remember never to use Portal power board (P-PWR-U023) to power electric door strike, magnetic lock, and/or any other peripheral devices. External power supply must be used for all door lock outputs and general purpose output devices.

If both readers are used on the same access point for IN access/OUT confirmation,

- Use **BOUT1** relay output terminal on Controller board for general purpose output since only one Door Lock output per access point is required.



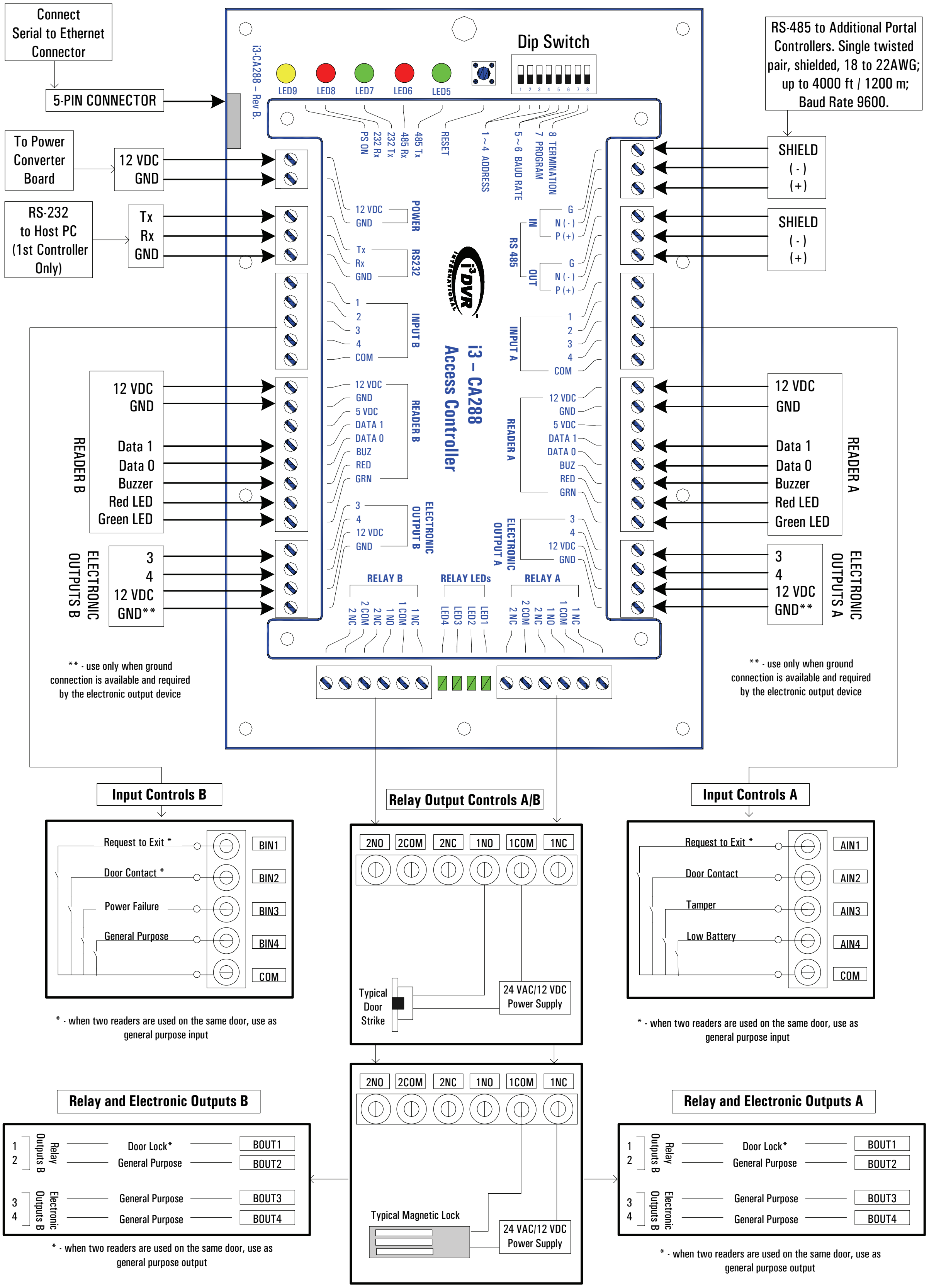
* - when two readers are used on the same door, use as general purpose output

Once all the above steps have been completed and carefully verified, apply power to the system.

4.1.11. Tips and Reminders

- Ground each Portal Chassis (P-PORTALCHASSIS) to Earth Ground.
- Do not exceed recommended cable lengths specified in this manual.
- The RS-485 network must be connected as a daisy chain.
- When Portal Card Access system has more than one Controller and the RS-485 cable run exceeds 300 m turn dip switch 8 to the ON position on the *last* Controller board in the daisy chain.

Portal Access Controller (i3 – CA288). Wiring Diagram



4.3. Portal Card Access System Specifications

- **Power Requirements:** 12 VDC
- **Current Consumption per Controller:** 250mA
- **Flash ROM:** 64 Kbytes
- **Firmware Upgrade from PC:** supports In-System Program (ISP) via RS-232
- **Number of Readers supported per Controller:** two (2): Wiegand 26 bit format or i3DVR proprietary 46 bit format access cards
- **Number of Controllers per Network:** sixteen (16)
- **Card holder Database Capacity:** 2000 cards
- **Event Log Capacity per Controller:** 2000 events
- **Network Connection:** RS-232: Controller to Host PC

  RS-485: Controller to Controller
- **Control Outputs:** four (4) form C dry contact relay outputs and four (4) electronic outputs
- **Sensor Inputs:** eight (8) digital inputs
- **Real Time Clock (RTC) Support:** battery backup on Controller
- **Portal Chassis Dimensions:** 14" H x 11 ¾ " W x 3 ¼" D (35.56 cm H x 29.85 cm W x 8.26 cm D)
- **Operating Temperature:** 0° to 70° C (35° ~ 150° F)
- **Operating Humidity:** 20 to 80% RH (non-condensing)

4.4. Status LED''s and Reset Button

There are five LED light indicators that are visible on the Portal Card Access chassis. (See Card Access Controller Wiring Diagram)

From left to right:

LED 9: Power ON

LED 8: RS-232 Receive (Rx)

LED 7: RS-232 Transmit (Tx)

LED 6: RS-485 Receive (Rx)

LED 5: RS-485 Transmit (Tx)

Reset Button is used to erase RAM

4.4.1. Firmware Update

Portal Card Access system is always shipped with the newest available firmware and does not need a firmware update. However, in the unlikely event that the firmware will need to be upgraded in the future, follow the instructions below.

Important

If TCP/IP Converter board (I3-S2E) is used with the Controller board, it must be disconnected from Controller board (P-CA288) before firmware can be uploaded.

For firmware update, use Philips LPC2000 utility located on the software CD shipped with your Portal system.

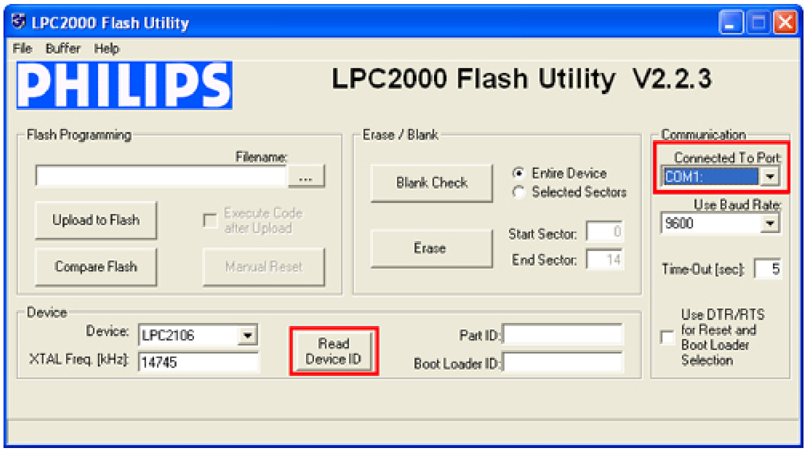
Firmware may only be updated via RS-232 connection, therefore in case of a network with multiple Portal Controllers, you may only upgrade firmware of the *first* Controller on the network through the Host PC. To upgrade the firmware on the remaining Controllers, it is recommended to use a portable laptop with previously installed Philips LPC2000 utility.

1. Connect the serial COM port on the laptop to the RS-232 port on the Controller.

2. Turn the dip switch 7 to the ON position on Controller board.

3. Run the Philips LPC2000 Flash utility on the laptop.

4. In the LPC2000 Flash Utility window, select the correct **COM** port number.



Connected To Port: COM1:

Use Baud Rate: 9600

Time-Out [sec]: 5

● Entire Device ○ Selected Sectors

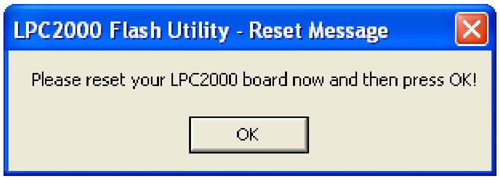
Start Sector: 0

End Sector: 14

Device: LPC2106

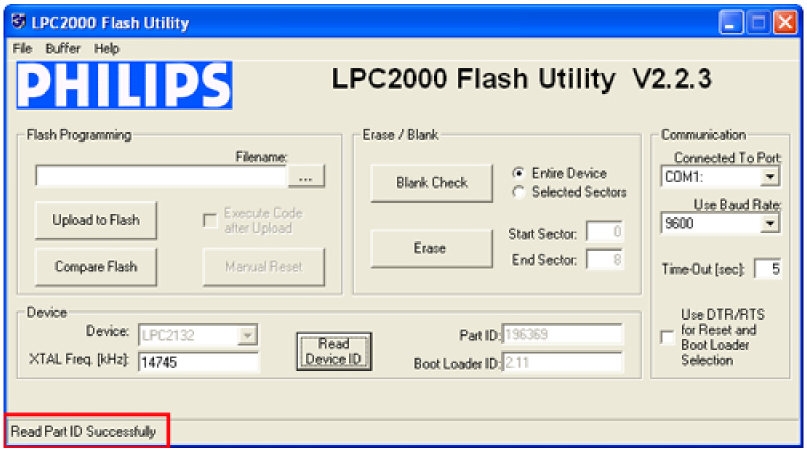
XTAL Freq. [kHz]: 14745

5. Click **Read Device ID** button in the LPC2000 utility. A Reset Message window will be discased: ''Please reset your LPC2000 board now and then press OK!''. (Do not click **OK** at this time)



Please reset your LPC2000 board now and then press OK!

6. Press down the **Reset Button** on the Controller board for 3 seconds, then click **OK** in the Reset Message window. The status in LPC2000 Flash Utility window will change to: "**Read Part ID Successfully.**"



Filename:

● Entire Device
○ Selected Sectors

Start Sector: 0
End Sector: 8

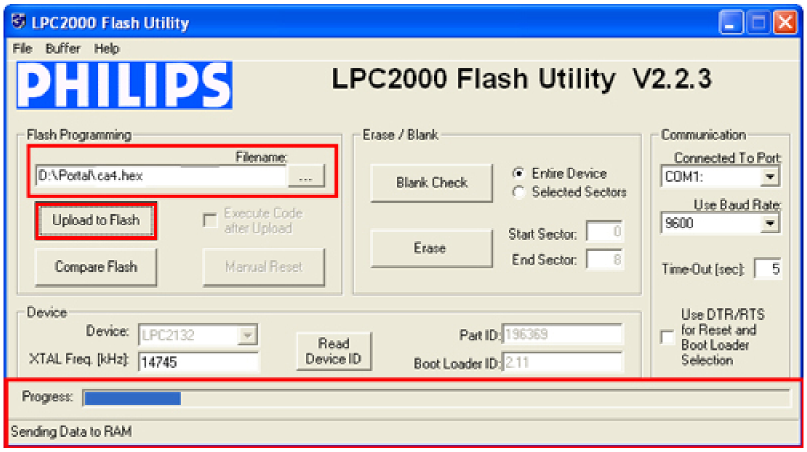
Connected To Port: COM1:
Use Baud Rate: 9600
Time-Out [sec]: 5

Device: LPC2132
XTAL Freq. [kHz]: 14745
Part ID: 196369
Boot Loader ID: 2.11

Read Part ID Successfully

7. Click the Browse button in the **Filename:** field of the Philips Flash Utility window to locate the most recent ***.hex** firmware file. For example: **D:\Portal\ca4.hex**

   Select the firmware file and click **Open**.



Filename: D:\Portal\ca4.hex

● Entire Device
○ Selected Sectors

Start Sector: 0
End Sector: 8

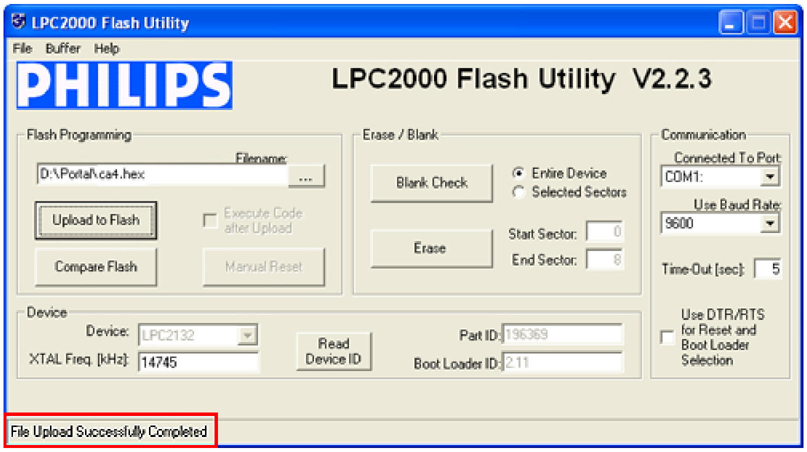
Connected To Port: COM1:
Use Baud Rate: 9600
Time-Out [sec]: 5

Device: LPC2132
XTAL Freq. [kHz]: 14745
Part ID: 196369
Boot Loader ID: 2.11

Sending Data to RAM

8. Click the **Upload to Flash** button. The status in LPC2000 Flash Utility window will change to: "**Sending Data to RAM**" and the Progress bar will indicate the firmware update progress.

9. Wait for the firmware update to finish. The status in LPC2000 Flash Utility window will change to: "**File Upload Successfully Completed**"



Filename: D:\Portal\ca4.hex

□ Execute Code after Upload

● Entire Device
○ Selected Sectors

Start Sector: 0
End Sector: 8

Connected To Port: COM1:
Use Baud Rate: 9600
Time-Out [sec]: 5

Device: LPC2132
XTAL Freq. [kHz]: 14745
Part ID: 196369
Boot Loader ID: 2.11

□ Use DTR/RTS for Reset and Boot Loader Selection

File Upload Successfully Completed

10. Turn the dip switch 7 to the OFF position on Controller board.

11. Press down the **Reset Button** on the Controller board for 3 seconds again. This completes Controller firmware upgrade.

4.5. Glossary

Access Card - a card used in conjunction with a Reader to grant or deny access. Two access card formats are supported by Portal Card Access system: Wiegand 26 bit (less secure) and i³DVR proprietary 46 bit (more secure). The cards for Portal Card Access must be ordered from i³DVR International.

Access Point - a controlled opening (e.g. door). One or two readers may be used per access point.

Controller (Board) - the "brain" of the Portal Card Access System. Each board accepts a maximum of 2 readers and 8 digital inputs. The Controller contains 4 form C dry contact relay outputs and 4 electronic outputs. The board establishes a two-way communication with Portal Card Access software via Serial or TCP/IP communication. The Controller board ID is assigned by the Controller ID dip switch.

Controller ID Dip Switch - located on the Controller and used to assign ID number to the Controller, set the Controller baud rate, set the Controller to firmware upgrade mode and to terminate data transmission in case of a longer cable run.

Door Contact - a magnetic contact mounted on the frame of the controlled opening. Door Contact should be connected to AIN2 and BIN2 input terminals on the Controller board. Only one Door Contact should be used per access point (door), therefore if both readers are used on the same access point, only AIN2 terminal should be used for Door Contact input.

Electronic Locking Device - releases when a valid access card is presented to the reader. One Door Lock output must be enabled for each access point. Only one electronic locking device should be used per access point (door), therefore if both readers are used on the same access point, only AOUT1 terminal should be used for electronic locking device output.

Network - consists of linear-connected Controller boards (daisy-chain network). A single network supports up to 16 Controller boards and up to 32 readers. Controller board network can be connected to the user PC or DVR via serial or TCP/IP connection. The latter requires a converter.

Reader (Card Reader) - a hardware device that is connected directly to the Controller board and is mounted **outside and/or inside** of the secured area (door/cage). Each Controller board accepts a maximum of two readers, Reader A and Reader B.

Request to Exit (RTE) - a device that is connected directly to the Controller board"s input terminal and is mounted **inside** the secured area (e.g. an exit button, motion detector, etc.). RTE device allows releasing the door without having to scan the card.

Index

MORE
THAN JUST A

i^{3}DVR INTERNATIONAL INC.

1.866.840.0004
www.i3dvr.com

U.S.A. 415 Lawrence Bell Drive,
Suite 2, Williamsville.
NY, 14221

Canada 780 Birchmount Road,
Unit 16, Scarborough.
ON, M1K 5H4