Partizan Access Control Management Safe School

User Manual
Abstract

This document is the Software User Manual (SUM) for the Partizan Access Control Management Safe School project and was made according to the software engineering standard described in ISO/IEC JTC 1/SC 7. The Software User Manual instructs how to install and use the Partizan ACM SS software.
Partizan Access Control Management Safe School

User Manual
Contents

Chapter 1. Introduction ........................................................................................................... 7
  1.1  Intended readership ........................................................................................................ 7
  1.2  Applicability .................................................................................................................. 7
  1.3  Purpose .......................................................................................................................... 7
  1.4  How to use this document ............................................................................................. 7
  1.5  Problem reporting .......................................................................................................... 8

Chapter 2. Overview ................................................................................................................. 9

Chapter 3. Installation ............................................................................................................. 10
  3.1  Installing the software .................................................................................................... 10
    3.1.1  System requirements ............................................................................................... 10
    3.1.2  Installing Java SE Runtime Environment 1.8 or above ........................................ 10
    3.1.3  Partizan ACM Safe School installation .................................................................. 10
    3.1.4  Installing Microsoft SQL Server Express 2012 or above ...................................... 17
  3.2  Installing Database ......................................................................................................... 17
  3.3  Data transfer between Databases ................................................................................... 30
  3.4  Partizan ACM Server configuration. Partizan ACM Web server activation ................. 34
  3.5  Uninstalling software .................................................................................................... 37

Chapter 4. Partizan ACM Safe School Web server ................................................................... 38
  4.1  Software settings ............................................................................................................ 38
  4.2  Controllers ..................................................................................................................... 39
4.2.1 Add controller ................................................................................................................. 40
4.2.2 Edit controller .................................................................................................................. 41
4.3 Notifications settings ......................................................................................................... 42
  4.3.1 E-mail settings .............................................................................................................. 43
  4.3.2 SMS settings ............................................................................................................... 44
  4.3.3 Events ......................................................................................................................... 46
  4.3.4 Doors ......................................................................................................................... 49
4.4 Students ............................................................................................................................ 49
4.5 Users .................................................................................................................................. 51

Chapter 5. Partizan ACM Safe School Desktop Software ....................................................... 54
  5.1 Running software .............................................................................................................. 54
  5.2 Device Tab ....................................................................................................................... 55
    5.2.1 Controllers adding ...................................................................................................... 58
    5.2.2 Doors settings ........................................................................................................... 62
    5.2.3 Time zone settings .................................................................................................... 64
  5.3 Authority Tab .................................................................................................................... 66
  5.4 Card Holder tab ............................................................................................................... 68
    5.4.1 Creating new card holder ......................................................................................... 70
    5.4.2 Issue card ................................................................................................................ 71
    5.4.3 Setting authority to the card holders ....................................................................... 72
  5.5 Reports ............................................................................................................................. 75
    5.5.1 Card events report .................................................................................................... 76
    5.5.2 Alarm events report ................................................................................................ 78
    5.5.3 Card event count report .......................................................................................... 80
5.5.4 Work time report ................................................................. 81

5.6 Camera tab ............................................................................ 83

5.7 Time Attendance (TA) ............................................................. 84
  5.7.1 Timetables ......................................................................... 84
  5.7.2 Shifts .................................................................................. 87
  5.7.3 Time attendance calculation options and data ......................... 89

5.8 Patrol ....................................................................................... 90
  5.8.1 Patrol address and line .......................................................... 90
  5.8.2 Users .................................................................................... 92
  5.8.3 Real-time Patrol .................................................................... 93

5.9 Assigning of users privileges .................................................... 94
  5.9.1 New user adding ................................................................. 95
  5.9.2 Authority ............................................................................. 95
Chapter 1. Introduction

1.1 Intended readership

This document covers the use for the following users of the Partizan ACM system:

- the system administrator
- the project administrators
- the application providers
- the resource providers
- the programmers

1.2 Applicability

This Software User Manual applies to the Partizan Access Control Management version 2.1.

1.3 Purpose

The purpose of the SUM is to assist the user in installing and using the Partizan ACM software.

1.4 How to use this document

- Chapter 2 gives an overview of the Partizan ACM software
- Chapter 3 contains tutorials for common tasks that enable users to get started quickly
- Chapter 4 gives a reference of the complete Partizan ACM SS software
1.5 Problem reporting

For all problems please contact our support:

E-mail: support@partizan.global

Skype: partizan-support

Tel: +44 207 048-32-05.
Chapter 2. Overview

This module was created to complement the Partizan ACM software and allows to:

- Send e-mail notifications for entry/exit events
- Send SMS notifications for entry/exit events
- Send e-mail/SMS notifications for alarm and fire alarm to system administrators
- Manage notification settings for students
Chapter 3. Installation

3.1 Installing the software

3.1.1 System requirements

- CPU 1GHz
- DDR 1Gb
- Operating systems:
  - Windows Vista
  - Windows 7
  - Windows 8
  - Windows 10
- Java SE Runtime Environment 1.8 or above
- Microsoft SQL Express 2012 or above

3.1.2 Installing Java SE Runtime Environment 1.8 or above

Please visit [http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html](http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html) and download software according to operating system installed at PC. When download is complete, install the software using the instructions provided by the installer.

3.1.3 Partizan ACM Safe School installation

Please, run Partizan ACM SS.exe, choose installation language “English” and click “Next” (Pic. 3.1).
Pic 3.1. Choosing installation language.

- Click “Next” to continue software installation process (Pic. 3.2).
Pic. 3.2. Continuing installation.

- Have a look at the conditions of the License Agreement and click “Next” (Pic. 3.3).
Pic. 3.3. License Agreement.
Pic. 3.4. Install location.

- Select additional tasks and click “Next” (Pic. 3.5).
Pic. 3.5. Selection of additional tasks.

- Click “Install” to start installation process (Pic. 3.6).
Pic. 3.6. Beginning of the installation process.

- Click “Finish” to complete installation process (Pic. 3.7).
3.1.4 Installing Microsoft SQL Server Express 2012 or above

Please visit


and download SQL Server Management studio and SQLEXPR according to operating system installed at PC. After the download is completed, install the software using the instructions provided by the installer.

3.2 Installing Database

After Microsoft SQL Server Express installation, following steps must be done:

- In SQL Server Management Studio (run as administrator):
  - Select by clicking of right key mouse button Databases → Attach (Pic. 3.8)
Then Click “Add...” and choose installation path. Default path is C:\Program Files\Partizan\Partizan ACM 2.1\Database. Select file AXData.MDF and click “OK” (Pic. 3.9)
Pic. 3.9 Choosing AXData.MDF file

- Click “OK” to finish Attaching Databases (Pic. 3.10)
Pic. 3.10 Attach Databases window

- Right click on server instance (in the example server name is DESKTOP-FQTE7K) → Properties → Connections → Allow remote connections to this server (Pic.3.11)
Remote connection settings

- Right click on server instance → Properties → Security → Server authentication → SQL Server and Windows Authentication mode (Pic. 3.12)
Pic. 3.12 Enabling the SQL server authentication

- Create new user. User settings:
  - Server instance → Right click on Security → New → Login
  - General → SQL Server authentication
  - Fill in the fields: Login name, Password, Confirm password (Pic.3.13)
Pic. 3.13 Creating new user

- Server Roles → Server roles = public (Pic. 3.14)
Pic. 3.14 Server roles

- User Mapping → User mapped to this login → AXData
- User Mapping → Database role membership → db_owner, public (Pic. 3.15)
Pic.3.15 User mapping

- Status → Permission to connect to database engine = Grant
- Status → Login = Enabled (Pic. 3.16)
Note: If “User must change password at next login” is checked (Server instance → Right click on Security → New → Login → General → SQL Server authentication). After restart you need to connect with this account through SQL Server Management Studio to change password. (Pic.3.17)
- Create a firewall rule to allow connections on port 1433
- In SQL Server Configuration Manager:
  - SQL Server Network Configuration → Protocols for %INSTANCENAME% → Right click on TCP/IP → Properties → Protocol → Enabled = YES → “OK” (Pic.3.18)
Enable connection by using TCP/IP

- SQL Server Network Configuration → Protocols for %INSTANCENAME% → Right click on TCP/IP → Properties → IP Addresses → IP All → TCP Port = 1433 → “OK” (Pic.3.19)
Pic.3.19 Port setting for TCP/IP

- SQL Native Client Configuration → Client Protocols → Right click on TCP/IP → Properties → Protocol → Default Port = 1433
- SQL Native Client Configuration → Client Protocols → Right click on TCP/IP → Properties → Protocol → Enabled = YES. Click “OK” (Pic.3.20)
- Restart SQL Server Service
3.3 Data transfer between Databases

In the case, if MDF-file was used as Databases (DB) and when it became necessary to transfer data to Microsoft SQL Server, you can use program DataMoveToolNew (default installation path is C:\Program Files\Partizan\Partizan ACM 2.1\DataMoveToolNew) for data transfer.
• Please choose by using checkbox initial DB, data from which DB will be copied and click “Next” (Pic 3.21).

[Image of Data Import Tool]

Pic. 3.21 Choosing initial DB

• Please choose by using checkbox DB where data will be copied and press “Next” (Pic 3.22)
• Please choose beginning date of records to be imported and click “Next” and after that click “Start Import” (Pic 3.23)
• After import was finished please choose DB by using checkbox that will be used in software. Go to System-DATABASE Config (Pic 3.24)
Pic. 3.22 Choosing destination DB
Pic. 3.23 Choosing beginning date of records
3.4 **Partizan ACM Server configuration. Partizan ACM Web server activation**

- Run server.bat (default installation path is C:\Program Files\Partizan\Partizan ACM 2.1\bin\server.bat) and open link [http://127.0.0.1:8089](http://127.0.0.1:8089) in any browser (Port can be later changed in file config.ini).
- Copy “Your ID” and send it to yours sales manager. After you will receive license key, enter it in the appropriate field and click “Validate” (Pic. 3.25).
Pic. 3.25 License key validation

- Please sign in to the web server. Default user is *admin* and password is also *admin* (Pic. 3.26).
- After that main form will be opened (Pic. 3.27). If this is your first login, the list of controllers will be empty.
Pic. 3.26 Web server log in
3.5 Uninstalling software
All the applications can be easily uninstalled by using uninstall.exe.
Chapter 4. Partizan ACM Safe School Web server

In this chapter will be discussed all possibilities and options of Partizan ACM SS software.

4.1 Software settings

After login please click on Software settings button. General settings tab will appear (Pic. 4.1).

There you can:

- Select your preferred language (default language is English)
- Use group alarm and fire alarm management
- Connect to DB by entering following data:
  - SQL server IP address, if SQL server is installed on the same PC where web server is running, leave “localhost” value
  - SQL server port, default value is “1433”
  - Database name, please enter DB name, which were added in Chapter 3.2. Default value is AXData
  - Authentication type, You can choose between SQL or Windows authentication
  - User name, must be filled If SQL server authentication is chosen
  - Password, User name password

Note: User “sa” can’t be used for DB connection, please create new user and give him rights for DB connection and management
4.2 Controllers

On tab controllers, you can (Pic. 4.2):

- See controllers connection status
- Edit controller
- Delete controller
- Add controller
4.2.1 *Add controller*

Please click on Add button (Pic 4.3):

- **IP address**, controller’s IP address, displayed on the controller’s sticker
- **Port**, default value is “8000”, can be changed through controller’s web
- **Virtual port for ACM**, virtual port for connecting by using Partizan ACM software
After controller was successfully added to the server application, you can use controllers in Partizan ACM software. Now instead of controller IP and Port device controller will be added by **PC IP** and **Virtual port**.

### 4.2.2 Edit controller

Please click on Edit controller button (Pic 4.4).
4.3 **Notifications settings**

Please click on notification settings button to open them.
### 4.3.1 E-mail settings

<table>
<thead>
<tr>
<th>NAME</th>
<th>IP ADDRESS</th>
<th>PORT</th>
<th>VIRTUAL PORT</th>
<th>STATUS</th>
<th>ACM CONNECTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concord</td>
<td>192.168.0.160</td>
<td>9000</td>
<td>20001</td>
<td>✔</td>
<td>0</td>
</tr>
<tr>
<td>Main entrance</td>
<td>192.168.0.148</td>
<td>9000</td>
<td>28000</td>
<td>✔</td>
<td>1</td>
</tr>
</tbody>
</table>

Pic. 4.5 Email settings

- **SMTP server**, your smtp server
- **SMTP server port**, your smtp server port
- **SSL**, enable/disable checkbox
- **E-mail authorization**, enable/disable checkbox
- **Sender e-mail**
- **Sender password**
- **Form for testing email**
4.3.2 SMS settings

Only Smsgateway.to is supported for SMS notifications. Please register account at https://www.smsgateway.to/en. You can try demo for 10 SMS without paying.

After registration go to your account settings (Pic. 4.7).
Scroll down and fill in all the fields in the “Login Details” (Pic. 4.8). Press “Save” button.

Pic. 4.7 Account settings

Pic. 4.8 Login Details
Go to the tab “API Keys”. There is a product token (Pic. 4.9), which you need for Partizan ACM: Safe School.

![Image of API Keys page](https://dashboard.onlinesmsgateway.com/en/settings#api-keys)

**Pic. 4.9 Product token**

In the SMS notification settings of Partizan ACM Safe School (Pic. 4.7) fill in the following fields:

- *Sender name* – should be the same as the First Name in `smsgateway.to`
- *Product token* – copy from the API Keys tab in `smsgateway.to` (Pic. 4.10)
- *Test phone number* - phone number must be entered in international format (i.e., +380XXXXXXXX)

Click “Test” button to receive a test SMS.

4.3.3 **Events**

Here you can manage settings for following events:

- Exit
- Entry
- Alarm
- Fire alarm

Entry and Exit events have the same properties (Pic. 4.10)

Pic. 4.10 Entrance event

- **Event type**, choose event type for management
- **E-mail subject**
- **Message template**, must be between 10 and 160 symbols. You can use following variables:
  - `<name>` - students name
Alarm and Fire alarm events have following properties (Pic. 4.11)

- **Send e-mail notification** checkbox
- **Send sms notification** checkbox
- **E-mails**, multiple addresses can be entered separated by comma
- **Phone numbers**, multiple addresses can be entered separated by comma
- **E-mail subject**
• Message template

4.3.4 Doors

Doors are chosen there for sending notifications (Pic. 4.12)

4.4 Students

There is information about students added by desktop Software (Pic. 4.13).
To manage notification settings of the Student, click on an edit button (Pic. 4.14)
Pic. 4.14 Notification settings: Students

- **E-mail addresses**, multiple addresses can be entered separated by comma
- **Phone numbers**, multiple addresses can be entered separated by comma
- **E-mail, SMS notifications** for different events

### 4.5 Users

There you can manage user's access to the web server (Pic. 4.15)
To add user you need to click on “Add user” button (Pic. 4.16)
- **Login**, users login
- **Password**, users password
- **Role**, Users role, can be:
  - *Admin* – full access to the web server
  - *User* – only student settings are enabled
Chapter 5. Partizan ACM Safe School Desktop Software

5.1 Running software

Please run Partizan ACM.exe file. Following window will appear (Pic. 5.1)

![Software authorization](image)

Pic. 5.1 Software authorization

While software was installed default user **admin** without password was created. If the need arises you can change password or create new user in User rights management.

There are four functional areas in the software (Pic 5.2):

1. Main menu
2. Side menu, options are grouped according to similar tasks
3. Active tab (on default it is the «Device» tab)
4. Logs, events, photo identification window.
5.2 Device Tab

This tab is designed for adding and configuring controller’s parameters settings. It consists of the following functional blocks:

- **Area.** This block is designed to group controllers. Area “All” was created on default. Following operations can be carried out by opening of context menu using right mouse button (Pic. 5.3)
Pic 5.3 Area block

- **Adding/editing controller’s parameters.** This block is designed for adding the controllers and their settings to software (Pic. 5.4)
Pic 5.4 Controllers adding

- *Doors management*. This block is designed for doors settings management and control (Pic 5.5.)
5.2.1 **Controllers adding**

There are 2 options of equipment`s connection:

- **RS-485.** For this option you should use converter RS-485/RS-232. When adding of equipment you should select COM-port to which converter is connected;

- **TCP IP.** For this operation mode it is necessary that PC and controller were in one subnet. Default network settings of controller are displayed at controller`s sticker. Changing of IP-address can be made via Web (Pic. 5.6). You should enter following data for access to the device:
Login: **admin**  
Password: **888888**

---

**Network Address**

**Time:** May 19, 2014 14:40:44, A2697/TFTP, 64 485 WG, 48564, RS485  
**Note:** Please restart system!

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>00:04:A3:E5:00:44</td>
</tr>
<tr>
<td>Name</td>
<td>2DOORBOXCONTROL</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.0.68</td>
</tr>
<tr>
<td>Port</td>
<td>1254</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

![Setting network parameters via Web-interface](image)  

For controller adding you should open context menu by right mouse button and select item “New controller” or use the hotkeys combination “Ctrl+Alt+A” at functional block Adding/editing of controller`s parameters. You should specify following information (Pic. 5.7):

- **Name** – controllers name in system
- **Serial No** – controllers serial number, displayed on sticker
- **Model No** – controllers model
- Select the option of connection to controller **RS-485** or **TCP/IP** by using checkbox. If TCP/IP is selected, you need to fill the field **IP address** when
static IP address is used or Area field if dynamic IP is used and specify port for controller access (on default 8000). If RS-485 is selected, you should select COM port;

- **Domain** – used for controllers grouping.

![Edit controller](image)

Pic. 5.7 Adding the controller

- If the controller was added successfully button “More…” becomes active, which allows to set controller`s advanced options (Pic. 5.8):
  - **Anti-pass back zone.** It is used for controllers` grouping into anti-pass back mode
  - **Alarm and fire alarm time.** Numerical value in seconds for alarm duration setting (99 means no limits);
  - **Interlock.** Option allows to group read points of two or four-door controllers into interlock. At interlock mode doors are working under following algorithm: in the case, when one of the doors is open, readers and exit buttons are locked. If first door is closed, the second transfer to
regular operation mode. Door sensors must be used for correct operation of this mode

- **Alarm password.** If this code (from 4 to 6 digits) will be entered, controller will generate an event "door alarm". To enter the code reader with keypad is required.

![Pic. 5.8 Controller’s advanced options](image)

If controller was added successfully, door icons will be green, otherwise they will be gray. In events log there will be event *Connect* with additional information about controller (Pic. 5.9).
5.2.2 Doors settings

After adding the controllers you should set door parameters. To do this you should open context menu and select menu item “Edit…” (Pic. 5.10).
### Edit door parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Door open time</strong></td>
<td>The value can be in the range from 1 to 65535 seconds. 99 means no limitation</td>
</tr>
<tr>
<td><strong>Door overtime</strong></td>
<td>Time parameter for person to go through door. It can take values in the range from 1 to 255 seconds. For proper operation the connection of door sensor is required</td>
</tr>
<tr>
<td><strong>Alarm if the door is open overtime</strong></td>
<td>In the case if door will be opened for more time that was set in parameter <em>Door overtime</em>, alarm will be activated</td>
</tr>
<tr>
<td><strong>Double direction test</strong></td>
<td>If the check box is not selected the controller will not generate events <em>entry</em> and <em>exit access</em>, there will be one event <em>Effective card</em></td>
</tr>
<tr>
<td><strong>Attend time attendance</strong></td>
<td>It is necessary to select check box in the case, when door will be used in time attendance (TA)</td>
</tr>
<tr>
<td><strong>Alarm time</strong></td>
<td>Duration time of the alarm. It can take value in the range from 1 to 65535 seconds. 99 means no limitations;</td>
</tr>
<tr>
<td><strong>Door alarm</strong></td>
<td>Alarm output will be activated if door will be opened without authorization, door sensor must be installed for the correct operation;</td>
</tr>
</tbody>
</table>

---

**Alarm output**

- **Alarm kept time**: 10
- **Alarm items**:
  - Door alarm
  - Invalid card
  - Swipe card during invalid time

---

Pic. 5.10 Edit door parameters
• **Door is open overtime.** In the case if door will be opened for more time that was set in parameter *Door overtime*, alarm output will be activated

• **Invalid card.** Alarm output will be activated if not authorized card or pin will be used

• **Swipe card during invalid Time zone.** Alarm output will be activated if card holder will try to go through the door in invalid time zone

### 5.2.3 Time zone settings

After door’s parameters setting, you should set the time zones (Pic. 5.11). 8 time zones for 4 doors controllers and 16 time zones for 1 or 2 doors controllers can be managed. Parameters:

- **Name**
- **Time and day scopes** should be set
- **Verification mode.** Select doors working mode
  - *Card.* RFID card is used in this mode
  - *Password.* Password is used in this mode. It can be up to 6 digits
  - *Card + Password.* In this mode, you first should use a card and then enter your password
  - *Double card.* In this mode you should use two cards to pass through the door
  - *Free pass.* In this mode the door will switch to the status “*Keep door open*”, after any card holder with correct user rights will go through the door. The Door will automatically be closed when the time zone end time will be occurred
  - *Card or password.* In this mode either card or password can be used by card holder for passing through the door
  - *Door timer.* In this mode door will be opened after begin time of time zone and closed at end time of time zone
  - *Alarm output timer.* In this mode you can set the activation of the alarm output during the time scope of a time zone
- **Door button timer.** In this mode can automatically block the exit on the schedule button
  
  - **Expiry date.** Specify the end time of the time zone. 2000-01-01 means no limitations
  
  - **Enable anti-pass back** – switch on the Anti-pass back.

After the door parameters configuration was made, you should download the configuration to the controller. To do that should open the context menu of the controller and select Update parameters (Pic. 5.12).
5.2 Authority Tab

The authority of entry and exit defines a using of access control permissions. Here the access control authority is equivalent to position power, said some position can entry the door, and in what time can exit the door. It can be also explained as a combination of the door opening time. Choose the authority in the Main menu to open define authority interface (Pic 5.13).
To create new authority please use context menu and choose “New…” or use hotkeys combination “Ctrl+Alt+A” (Pic 5.14)
To create a new authority, you need to set following parameters:

- **Authority name.**
- **Choose doors and doors time zone to give access** by using checkboxes

After that you will need to set authority to users or group of users. How to do it will be explained in chapter 5.4.3

### 5.4 Card Holder tab

At this tab you can manage card holder, issue cards and set authority to the users (Pic 5.15)
• Structure of the company is created in the area “Department”
• In the area Position you can separate the card holders by positions;
• Opening the context menu in users area you can:
  o Add new card holder
  o Edit employee’s data
  o Issue a card
  o Replace the card for card holder
  o Assign authority to card holder
  o Upload card data to controller
  o Upload card data to port
Time and attendance point check
- Delete (lock the card)
- Demission
- Delete (employee from the list)
- Set up the list of displayed fields
- Export/Print
- Set the expiry date

5.4.1 Creating new card holder

Pic. 5.16 Creating/editing card holder

To create new card holder, right click on active tab → New. Than to enter the following information:
• User No
• User Name
• User Surname
• Gender Male/Female
• Birth date
• Activation and expiry date
• Department
• Position
• Photos issuance. Following options are possible:
  o File. Select image on computer
  o Clipboard. Insert the image from the clipboard
  o USB video. Capture the image using web-camera
  o Camera 1 or 2. Use connected cameras
• Other personal information

After creating new card holder you need to give him card or password. Use context menu and choose Issue card or use hotkeys combination “Ctrl+Alt+C”.

5.4.2 Issue card

At this moment you can issue the card in three ways (Pic 5.17):

• Enter card number manually or copy from the event log
• Use the door to register the card. To do this, select the desired door from the drop-down list and use card at the reader at a chosen door
• Use USB-reader for card registration

Also there you can specify password to card holder. It can be up to 8 digits.
5.4.3 Setting authority to the card holders

To do that you need to use context menu and select “Authority” or use hotkeys combination “Ctrl+Alt+A” (Pic. 5.18)
You just need to choose by using checkboxes required time zones and click "OK" button. After that you need to upload data to the controllers. Now system is ready to work.

5.5 Map (Module of graphical plans)

This tab allows you to add graphics substrate for controllers and cameras, manage them, and add various counters.

Using the context menu (Pic. 5.19) you can enjoy the following features:
Pic. 5.19 Context menu

- Add object on Map. In the new window, you can select, add and manage controllers, access points and cameras (Pic. 5.20).

Pic. 5.20 Add object on map window

- Add label (Pic. 5.19):
  - Popup message at a specific event;
  - Add counting label (it allows you calculate the number of visitors in a particular area);
- Scroll label
- Changing label
- Add event form
- Add cards list
- Add picture
- Add Alarm
- Add timer

5.5 Reports

To access the Reports, you should use the side menu Reports and select needed one (Pic 5.22).
5.5.1 Card events report
To generate the report you should open context menu and select “Inquiry” or press key combination Ctrl+Q. In the opened window, select the desired options and click “OK” button (Pic. 5.23)

![Inquiry card events](image)

**Pic. 5.23 Inquery card events**

- You should first select *date* and *time* scopes on which the report is based. You can use special filters that will allow you to choose quickly the most popular time scopes
- **Card number.** Here you can specify desired card numbers separated by commas;
- **Employee personal number, Name, Surname.** Similar to card number;
- **Department, Position, Device parameters and Event parameters.** In given menu using the popup forms, you can specify the report parameters. In Pic. 5.24 popup form choosing doors is displayed
Clicking on “OK” will form the report.

5.5.2 Alarm events report

This report is formed according to the alarm events in the system (Pic. 5.25)
You can refine the report by selecting only the necessary alarm events (Pic. 5.26)
5.5.3 Card event count report

First you should go to Options (right click → context menu) and set the time intervals, which are needed to be analysed. Let’s suppose, there is the task to analyse the arrival time of employees. To do that we need to create 4 time intervals 8:30-9:05, 9:05-9:15, 9:15-9:30, 9:30-11:00 (Pic. 5.27).

![Option]

Pic. 5.27 Report options

Then choose desired report details (Pic. 5.28). Standard search events window on card will be opened, where we select date intervals. After that you can see the report.
5.5.4 Work time report

This report allows you to count time attendance without creating any shifts and time stands. It will count time between Entry and Exit records for all card holders. First you should go to the “Config” menu (right click → Options) and select units of measurement (minutes, hours or days). Pressing “Filter” button and flipping the tabs, you can specify the report parameters (Pic. 5.29). Further you should select grouping option using context menu. Possible grouping options: by days, weeks or months (Pic. 5.30). After that, you can view the report results.
Pic. 5.29 Report parameters

Pic. 5.30 Grouping selection
5.6 Camera tab

First of all ActiveX elements must be installed. To do that please open %InstallationPath%\ActiveX folder and find there web.inf file. By using context menu choose “Install” and follow the instructions.

Then in the main menu choose “Camera” and by using mouse right button click - “New”. In order to connect to the camera or DVR you should enter necessary information:

- Name
- IP address (default IP address for Partizan equipment 192.168.1.10)
- Port (default port 34567)
- Subnet mask (no need to fill it)
- Gateway (no need to fill it)
- MAC address (no need to fill it)
- User name (default admin)
- Password (default admin)
- Installation place (no need to fill it)
After that please click “Test” button. If connection is OK you will see image from camera or DVR.

5.7 Time Attendance (TA)

Please use side menu and enter Time Attendance. First of all you will need to create Timetables.

5.7.1 Timetables

For time attendance you should create Timetables – the time of clock in and clock out from work with indication of periodicity. You should use menu item Time Attendance and select Timetable (Pic 5.32)
On the left there are displayed all created timetables, on the right detailed information concerning selected timetable. To create new timetable you need to open context menu in the left column and select item “Add”.

Pic. 5.32 Timetable
After creating the timetable, you need to add time fields. To do this, select the created timetable and select in the right column Add via context menu or press Ctrl+Alt+A. (Pic. 5.33)

Here you should specify:

- **Name**, unique identifier of time frame (it is preferable to use day of weeks)
- **Time zones**. You can create up to three time zones, for their activation you should select check box next to appropriate field. The most popular mode is using of one time zone, for example from 8:00 to 18:00 and two time zones with meal period, for example from 8:00 to 12:00 and from 13:00 to 18:00
- **Absence**. How many minutes staff can swipe card in advance. If over this time, the records will not be calculated
- **Delay**. How many minutes staff can delay card swiping. If over this time, the records will not be calculated
If it is necessary to take into account overtime work and night shift, you need to select appropriate check boxes.

After timetables are created you need to assign them to users.

5.7.2 Shifts

For this you should use menu item Time Attendance and select Shift (Pic. 5.34)

On the left there are three tabs with the ability of assigning shifts by departments, positions and individually for each displayed user. On the right assigned shifts for active tab are displayed. When opening the context menu and selecting item *Add* (or pressing combination “Ctrl+Alt+A”), the window adding/editing schedule will be opened (Pic. 5.35):

- *Type*, here the type of shift creation is specified (for example the shift is created on the tab Department)
- **Name**, user is identified (for example the shift is created for Sales)
- **Time period**, shift duration is specified, on default, shift duration is 3 months;
- **Timetable**, choice of created timetable;
- **Current day of timetable**, First time frame for beginning of time period is specified. For example, time table begins from 2015-08-02 (Sunday), timetable (5 working days) from 9 to 18 is selected; accordingly the current timetable day should be selected Sunday.

![Edit Schedule](image)

Pic. 5.35 Assigning the shifts for card holders

After shift assigning, you should add counting strategy (Pic. 5.36). For this you should open the context menu and select Add strategy. It consists of 5 tabs: Late, Leave early, Absence, Overtime and Holiday. For each tab you should specify numeric parameters for data accounting.
5.7.3 Time attendance calculation options and data

In this menu calculation principles of working hours are specified (Pic. 5.37) There are possible 2 options of working hour’s calculation: use standard time (in this case, if at least one record will be per day, the parameter “How many minutes to calculate as work day”, specified on tab Others will be record for employee as working hours or real card events time (for correct calculation of working hours it is necessary at least one event for entry and exit for each card holder).

Also you can set unit measurement for each parameter and select rounding variant.
After that you need to calculate working hours and you can view data in Time attendance data and Group by Employee.

5.8 **Patrol**

This module is designed for security tours controlled by security guards. For its correct operation in system at least one controller should be added.

5.8.1 *Patrol address and line*

Patrol address and line are assigned in this menu. For this you should enter menu “Patrol” → “Patrol address and line”. For route assigning, on the left window “Line” by right mouse button you need to open popup menu and select “New line”. On this form you should specify name of the Line (Pic. 5.38).
Now you can create patrol points by clicking of right mouse button in right program field and selecting the item “New address” (Pic. 5.39).

You should enter following data:

- **Name** of assigned patrol point
- Select the **address** of patrol point
- **Distance** time from previous point
- **Range** (in the case of exceeding this parameter the events late or earlier arrival will be generated).
5.8.2 Users

After address and line creation you should create the users and assign patrol lines to them. For this purpose select menu item “Patrol” and select item “Person and plan”. You should specify the user from data base for plans and routed creation. For this purpose you need to open menu by clicking right mouse button in the left side of the window and select “Add person”. In the appeared window you should specify employee name, performing the patrol, and also add his card number (Pic. 5.40).

![Person window](Pic. 5.40 Person)

Then in the right window part you should activate popup window by right mouse button, in which select “New plan” (Pic. 5.41).
In this menu necessary shift parameters are assigned to employee, and also patrol starting time. Patrol plan consists of one or several routes, which can have different patrol starting time.

5.8.3 Real-time Patrol

Tracking the patrol rout in real time. In this window the name of user, route and time of patrol starting is specified. Identification time will be recorded when timely card submitting. If the employee have registered earlier or have not time for registration, relevant events will be highlighted in red. Also patrol plan can be run or stopped manually. This menu is available in the top tab “Patrol” → “Real-time Patrol”.

Pic. 5.41 Patrol plan creation
5.9 Assigning of users privileges

In menu “Users” you can create new users, change passwords, and to assign access privileges to the capabilities of the software. After installation of the software new user admin is created without password.

Pic. 5.42 Users management

Opening the context menu you can:

- Add new user
- Edit the existing user
- Delete the user
• Set authority

5.9.1 New user adding

Choosing menu item “New” or “Edit” of the user, you should enter following parameters (Pic. 5.43)

![Modify user dialog box](image)

Pic. 5.43 Modify user

5.9.2 Authority

Selecting the menu item authority, you can assign the rights (Pic 5.44).
If you have any questions or suggestions regarding our products, please contact our Technical Support:

- Skype: partizan-support
- E-mail: support@partizan.global
- Web: partizan.global