Gate IP WEB

ACCESS CONTROL SYSTEM SOFTWARE WITH WEB INTERFACE

Installation and programming manual

Contents

About the manual

This manual covers installation, adjustment and utilization of “Gate IP WEB” access control system software.

The document contains information for both installers and system users. Refer to the appropriate manual sections to resolve your goal.

It is recommended to study all sections describing system construction and functioning principle.

Important notes for system installers

Read this manual carefully prior to installing the system. “Gate IP WEB” security system has lot of features different to those in other systems; knowing of the specificities helps in accurate system design, installation and use.

If the manual does not solve the problems you face during system installation refer to the local distributor or vendor for further explanations.

This document is subject of changes and additions due to the continuous system evolution. The latest version is available at the WEB-site http://www.skd-gate.ru.

TECHNICAL SUPPORT

To get warranty and technical support you can apply to authorized service centers, situated on the territory of countries, enlisted in the warranty card.

Warranty and technical support are performed on the territory of the country, where the customer applied for warranty or free service.

TRADEMARKS

System characteristic

Preface

"Gate IP WEB" is an access control system that provides access control for premises of various scale - small offices as well as large enterprises with lot of users and access points.

System composition

The system is an integration of hardware and software components. "Gate IP WEB" software is to be installed on IBM-compatible PC. Ethernet (LAN, WLAN) interfaces are used for communication between hardware and software components of a system.

Access control panels Gate IP Base, Gate-IC Antipassback (global antipassback control panel), Gate-IC-Elevator (elevator control panel) provide a basis for system hardware.

All necessary optional equipment is connected to the control panels.

The list of control panels supported by the software may change. Software version you possess may not support new versions of control panels. Refer to technical assistance service for system updating.

Features

"Gate IP WEB" software is installed on one PC.

The system manages a large number of doors, controlled by access control panels working with one or two access points.

Sensors with normally open or normally closed contact may be connected to the loop terminals of control panels.

More detailed characteristics and functions of control panels are described in the panels' user manuals.

"Gate IP WEB" software runs under Windows 7 or higher operating system.

Terms and concepts

Proximity Identificator (RF ID)

Every user of access control system has a RF ID with unique code. RF ID may be in shape of plastic card, key fob, etc.

Access Card

RF ID in the shape of plastic card.

Reader

Readers are devices assigned for reading information from IDs and transmitting it to a control panel.

There are several types of IDs and readers for them. It is essential that reader and control panel should use the same interface.

PIN (Personal Identification Number)

Some readers have built-in keypad. Keypads may be used for PIN entering. It can be both self-dependent or used as an additional code to user ID. When PIN is programmed as additional code, reader waits for PIN entering after ID is read-out.

RTE (request to exit)

To exit from the premises with a single-sided door, a button wired to control panel is used. This button is called RTE (request to exit) button. If someone opens a door otherwise than pressing RTE button – by re-energizing locking device, opening lock with a key etc., "Door Forced Open" event arises. RTE button may be used for remote door opening as well.

Access point

Access point is a logical concept of the access control system implying control of passing through a door in one direction. It consists of reader, access control panel (or its part), door supervision devices (like magnetic sensor, RTE etc.) and door locking device. For instance, the turnstile with two-way passes has two Access points – one for entrance and the other one for exit, door of this type is called double-sided door. A door with a reader on one side has only one Access point – Entry point, and it is called single-sided door.

Door contact

In access control systems various sensors are used to supervise door status (opened or closed), such as magnetic door sensor, sensor of the turnstile rotor position, inductive sensor of car passing through the road barrier, etc. This ensured that the system prevents situations when several users access the door with one ID or door left open after user's access and so on.

Door Contact terminals of control panels are intended for connection of magnetic door sensor, sensor of the turnstile rotor position, inductive sensor etc.

Antipassback

Antipassback function is implemented in access control panels to prevent the situation when user gives his RF ID to another person after passing into the premises. If this function is on, control panel tracks an ID position – inside or outside the premises. On any attempt to pass in the same direction twice the panel denies access and stores “Access Denied, Antipassback” event into the Log.

Antipassback function can be set only in case of the double-sided door control.

Global antipassback

Prevents user door pass from the areas where he must not appear. The facility spitted into the closed areas connected with double-sided access points, in which system supervises the personnel appearance for this purpose. System detects the global antipassback violation when somebody tries to re-enter such area without exit or tries to enter somewhere from the area he have not enter. System generates message “GLOBAL ANTIPASSBACK: Access Denied” in case of global antipassback violation.

Door time

If door sensor is open, corresponding access point goes into alarm. Alarm is not invoked, if contact is opened during Door Time interval. This interval starts when access is granted and lasts for the programmed time or terminates on opening and subsequent closing of door contact.

Code matching attempt

Control panels can activate alarm on attempt of a code (or ID) matching. Code matching is considered when invalid code (or ID) is entered several times successively. Valid code entering clears the counter. Enabling of this function as well as number of code entries are programmable.

Schedules

Date and time of valid access are indicated when setting user access rights. Control panel stores up to 250 time zones. 250 week schedules can be combined from these time zones.

Moreover, control panel can store up to 250 holidays, which happen once a year.

Synchronization

Control panel is to be synchronized after all parameters are set – modes of loops, outputs, access rights and others. During synchronization parameters are rewritten into access control panel.

Card Collector

Collection device for proximity cards. Special device that works in conjunction with the access control panel. Designed to collect not valid proximity cards of employees, proximity cards of visitors when they leave, and to provide access to employees with valid IDs (the ID is returned to employee).

Installing “Gate IP WEB”

This part is mostly intended for installers and system administrators. System operators may get to know system operation characteristics as well.

Environment characteristics

“Gate IP WEB” is intended for operation under “Windows” operating systems not less than Windows 7. Any other operating system is unsuitable for the software.

Hardware and software minimal configuration

For “Gate IP WEB” proper operation is needed one PC, Ethernet (lan, wlan – wi-fi) local network with TCP/IP protocol.

Hardware and software requirements (same or better) are shown in the table below:

Processor	RAM	Hard drive (free space)	Monitor	Network	Operating system
Intel Celeron Core Duo 2 GHz or similar **AMD**	**4096** MB	**4 GB and up**	**1280x1024**, high 16bit	**100Mbit** Fast Ethernet, TCP/IP	Windows 7, Windows 2008, Windows 8/8.1, Windows 10, Windows 2016 Server

Installing “Gate IP” on PC

“Gate IP Free” is supplied with:

Software and PDF manual on one CD

Setup and first launching of «Gate IP» must be made by operator with administrative rights.

- Insert “Gate IP WEB” CD into CD ROM

- If automatic installation doesn’t start, run Setup.exe

- Description of installation sequence described in the "Installation instructions"

System planning

General notes

This part is intended for system administrators, who determine operation strategy and tactics.

Determine functions of the whole system and every control panel before programming, determine also panels operation modes, number and types of access groups and appropriate time schedules.

Now you can proceed to system programming. Recommended sequence of programming operations is described below.

It is recommended to observe the following rules, which facilitate system operation:

1. Before system programming, or going to change system configuration, draw accurate plan of actions, assign sequence of necessary operations. Hasty actions may lead to system full or partial restoration necessity. “Gate IP” system is sufficiently easy in operation, but due to the wide variety of capabilities, even experienced user may lose himself in the variety of system functions and settings.
2. In case of failure restore system status out of archive file or contact installers for assistance.
3. Devices disconnected one from another without need may cause information, stored in system components, inconsistency. In this case you will have to reboot the system that may lead to unplanned effects. The operation is simple, but before clarification of inconsistency, some unexpected effects may arise. Besides, access control panels contain only strictly limited number of events that central control panel and PC constantly read out and save in database. In case of long deactivating of control panels the oldest events may be lost irreversibly.
4. Create backup copies of system database at least once a week. That will help you in system restoration in case of system fail or PC troubles. Manual database restore can take several weeks.
5. Assign minimal access rights to operators, otherwise an operator ignorant of some system peculiarities can break down the system

Working with the Software

This part covers information concerning work with the software. Description follows items' sequence offered in the section above.

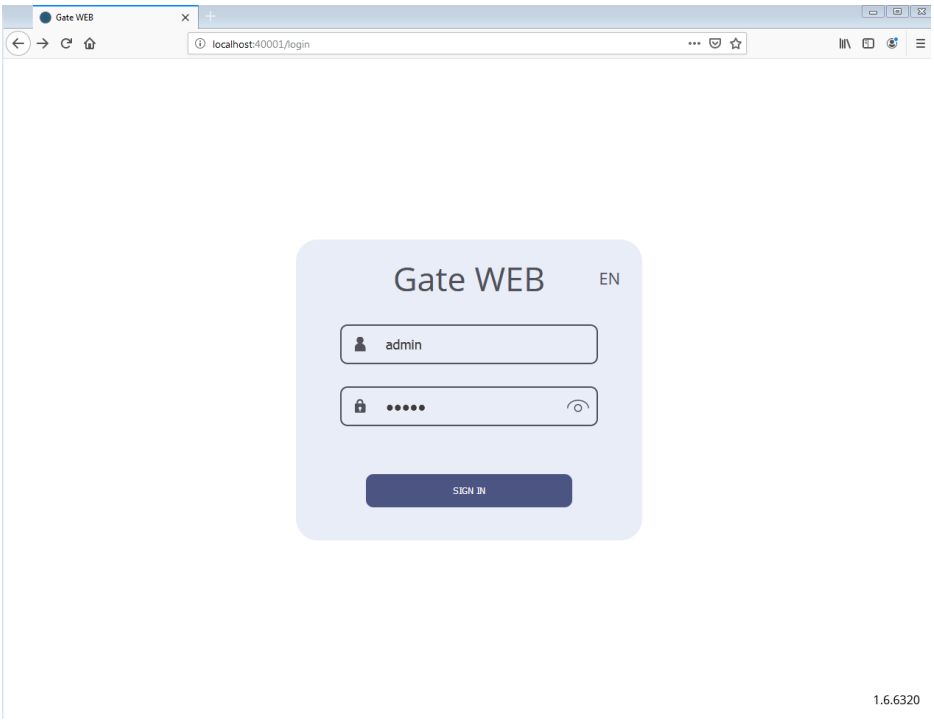
System logon

Start the web browser and enter in the address bar the IP address or domain name of the computer on which the Gate IP Web is deployed.

Recommended browsers: Google Chrome, Mozilla Firefox, Opera, IE10 and above, Edge, Safari.

To increase the security of the Web server, it is recommended to use the https protocol by installing an SSL certificate for this. For detailed instructions, contact Technical Support.

Logon window appears on display:



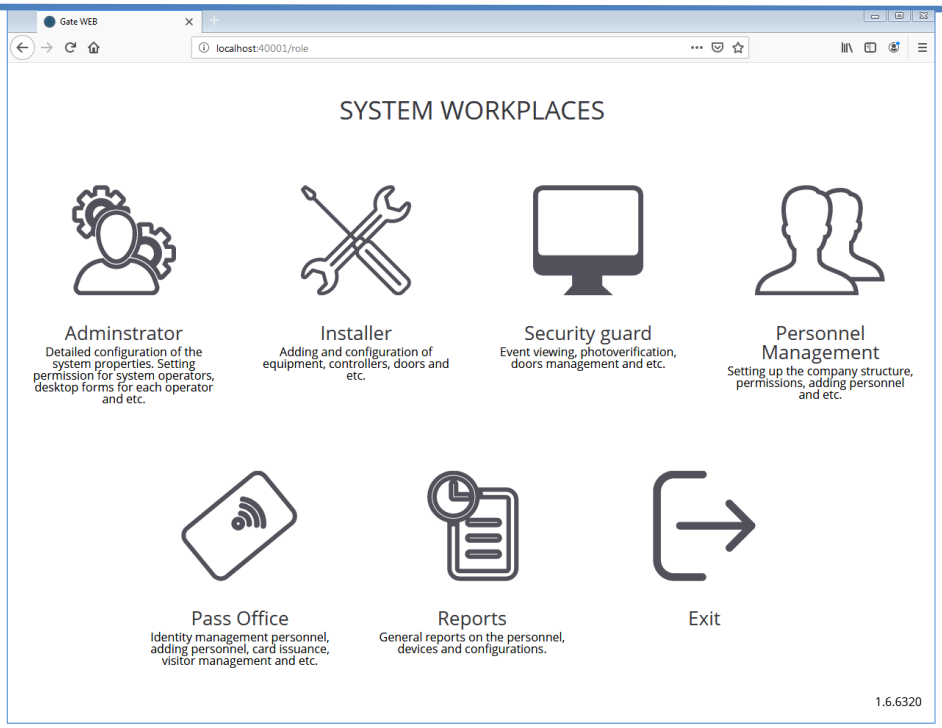
By default:

Login **admin**

Password **admin**

Be sure to change the password!!!

After loading, the main page will be displayed:



System functions collected into the groups named ‘Roles’.

’Administrator’ role

This role collects functions of system operator creation and adjustment of operators’ rights and objects available – doors, panels, events, personnel, IDs etc. (visibility).

‘Installer’ role

This role collects functions of equipment addition and adjustment – panels and doors. It includes firware upgrade and system test.

‘Guard’ role

This role collects functions of event monitoring, photoverification, door control.

‘Personnel control’ role

This role collects functions of enterprise (‘personnel and department tree’), access rights, schedules adjustment and personnel enrolment.

‘Pass’ office’ role

This role collects functions of common ‘Pass office’ routines like ID’s enrollment and remove, ID grant, visitors’ control.

‘Reports’ role

This role collects functions of report generation. Reports on personnel, time and attendance, equipment, event log and system settings available.

System operators' functions adjustment. 'Administrator' role

Operator enrollment required for access to the system functions to avoid unauthorized access. Operator may get access to the different system functions, depending on his rights, set by system administrator.

Only Administrator user exists in the system after software installation. It has logon **admin** and password **admin** by default.

We recommend to change password!!!

How to add system operators

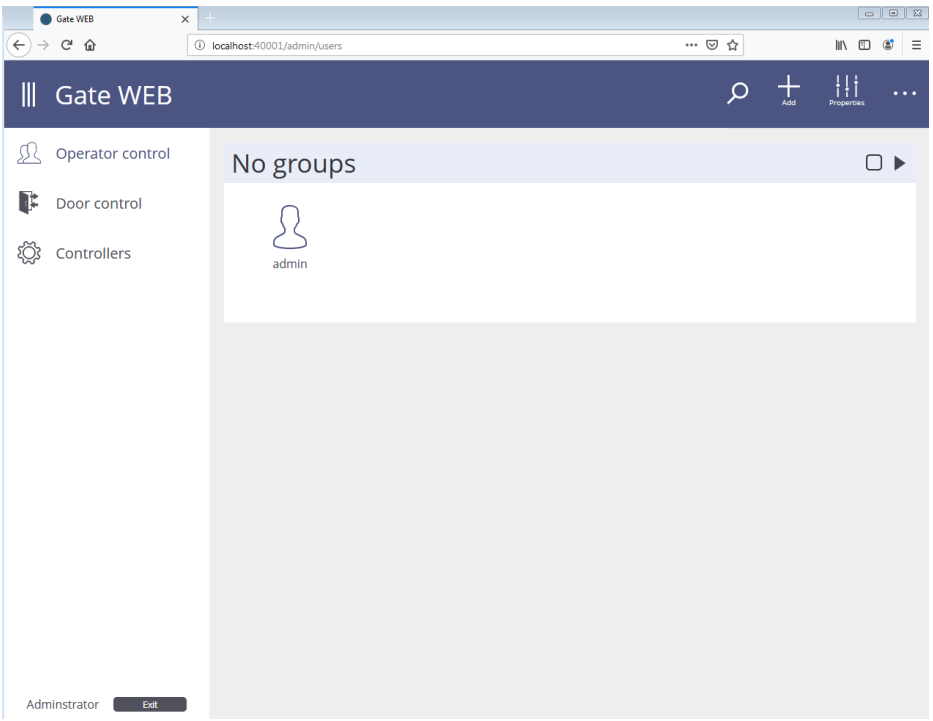
Select 

menu item to add system operator.

Enter user name, his login, password and repeat password.

Set operator role(s) and roles functions available to the operator.

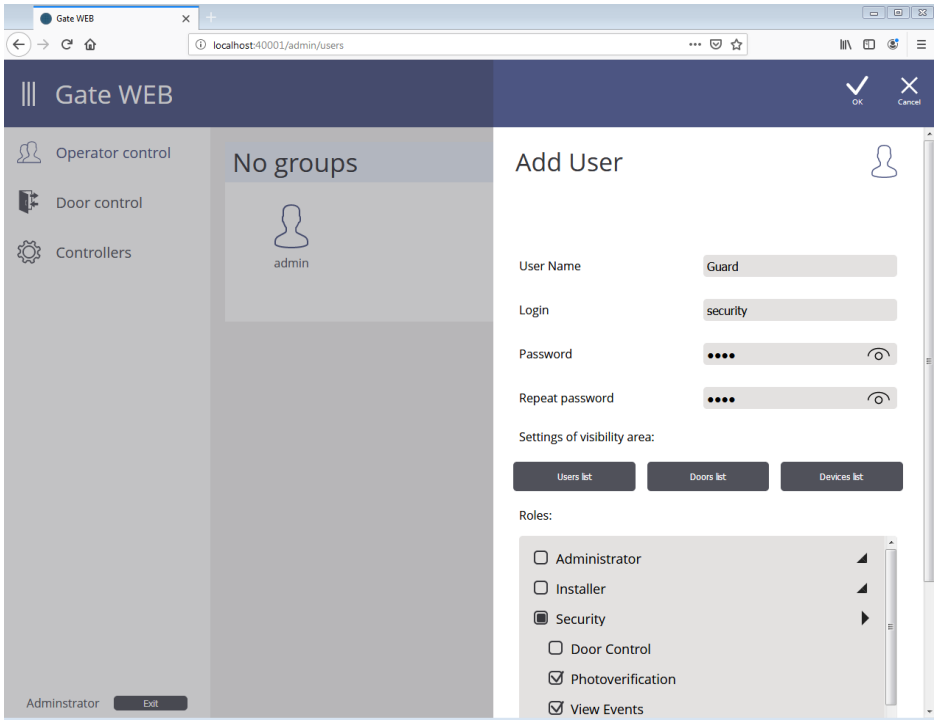
For instance, if you switch off 'Door control' function for the operator with 'Guard' role, he will be able to view event log and photoverification windows only but not available possibility to control doors as door control window will be absent in his view:



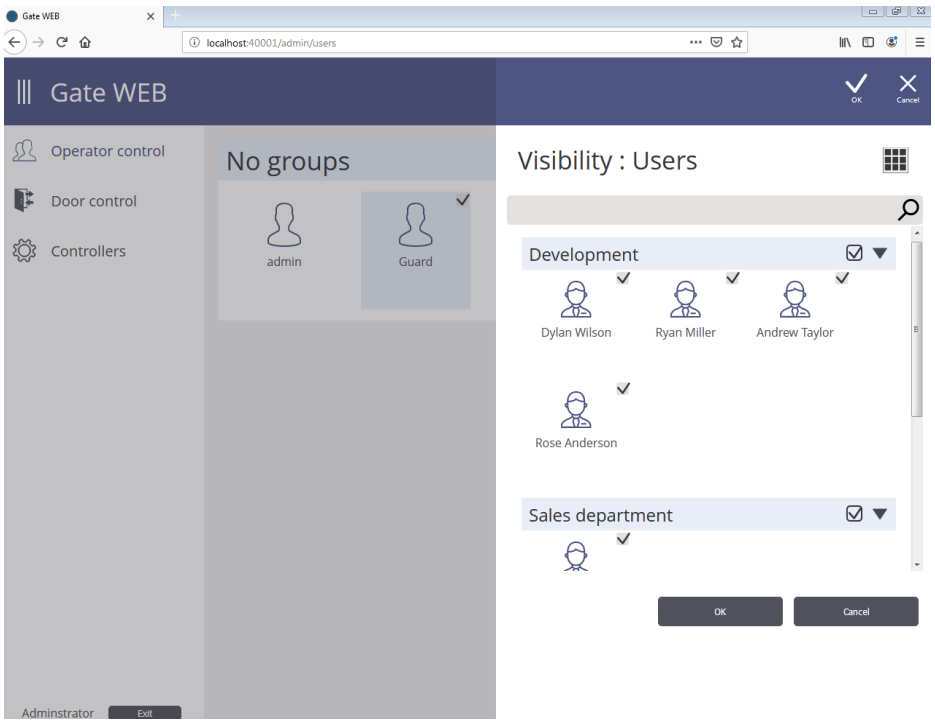
Defining of system elements available to the operator

It is possible to assign individual system elements to each operator with visibility differentiation. For instance, if enterprise has remote office it is possible to adjust visibility in the way, when operator in main office will see access events from the main office and operator in remote office will see access events from remote office only.

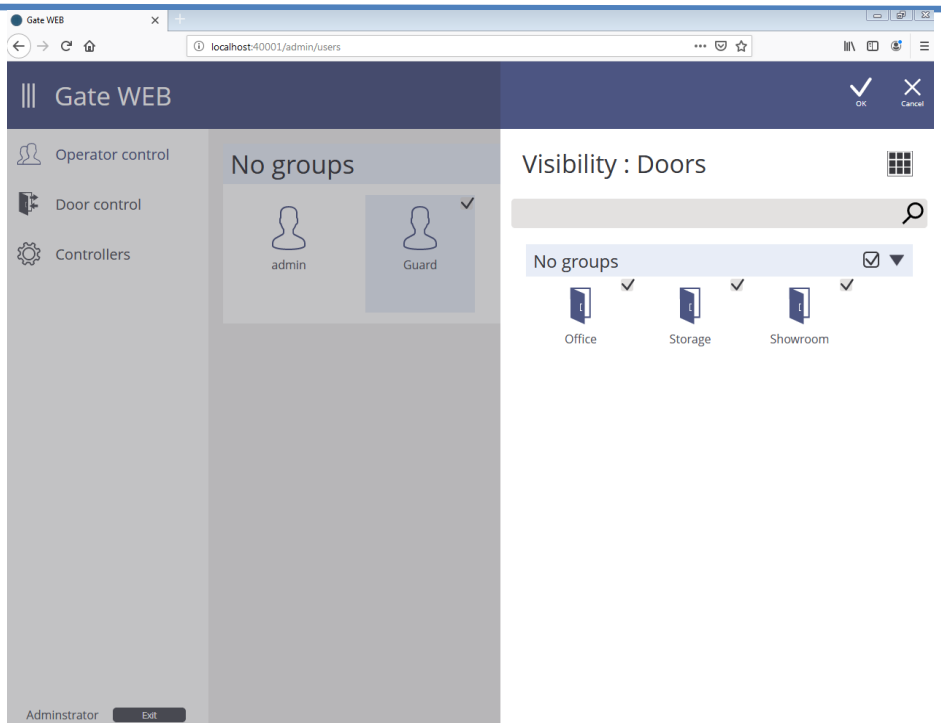
There are three functions for visibility adjustment: ‘Users’, ‘Doors’ and ‘Devices’.



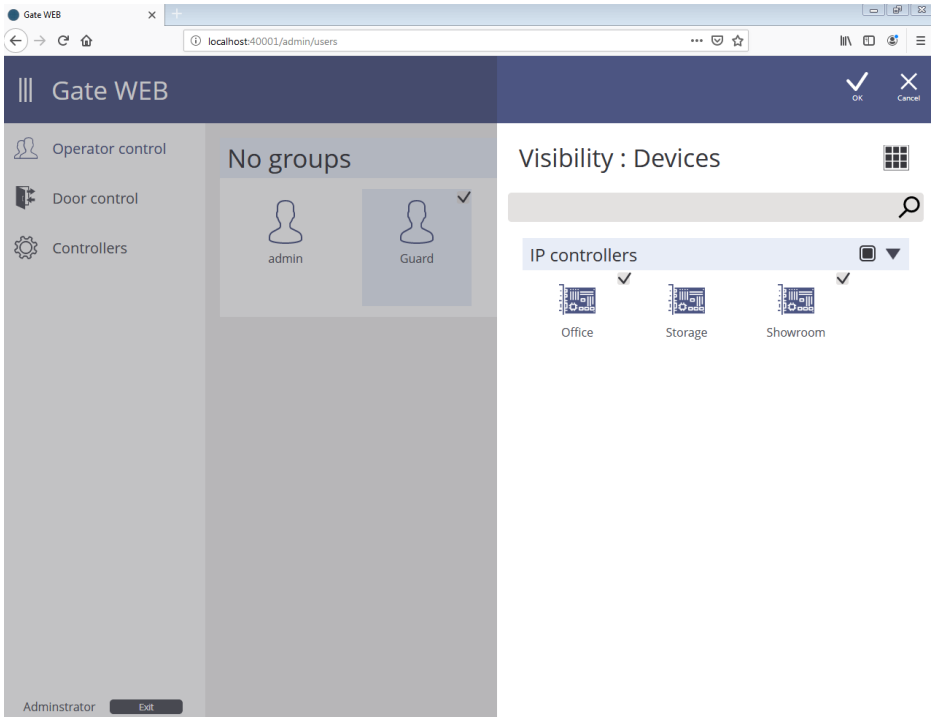
Press ‘Users’ button and select users available for operator actions in window appeared.



Press ‘Doors’ button and select doors available for operator actions in window appeared.



Press ‘Devices’ button and select Devices available for operator actions in window appeared.



Events and actions become available to operator if all conditions are carried out. For instance, the access event will be displayed to the operator if user and panel and door were added into the list of allowed elements.

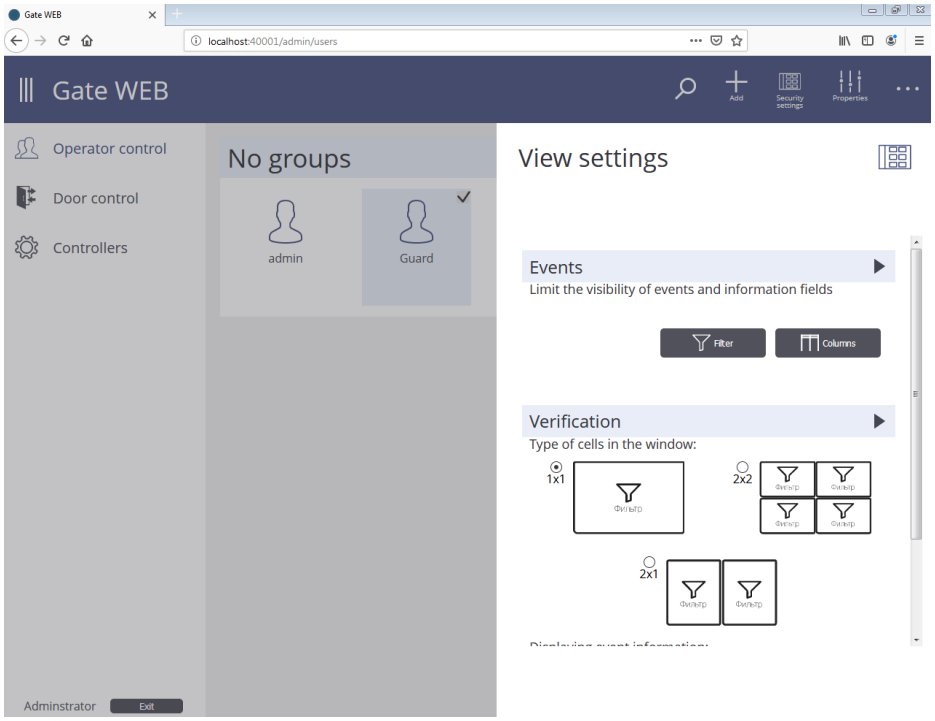
’Guards’ window view adjustment

It is possible to adjust additional event display options in ‘Event log’ and ‘Photoverification’ windows for system operator with ‘Guard’ role.

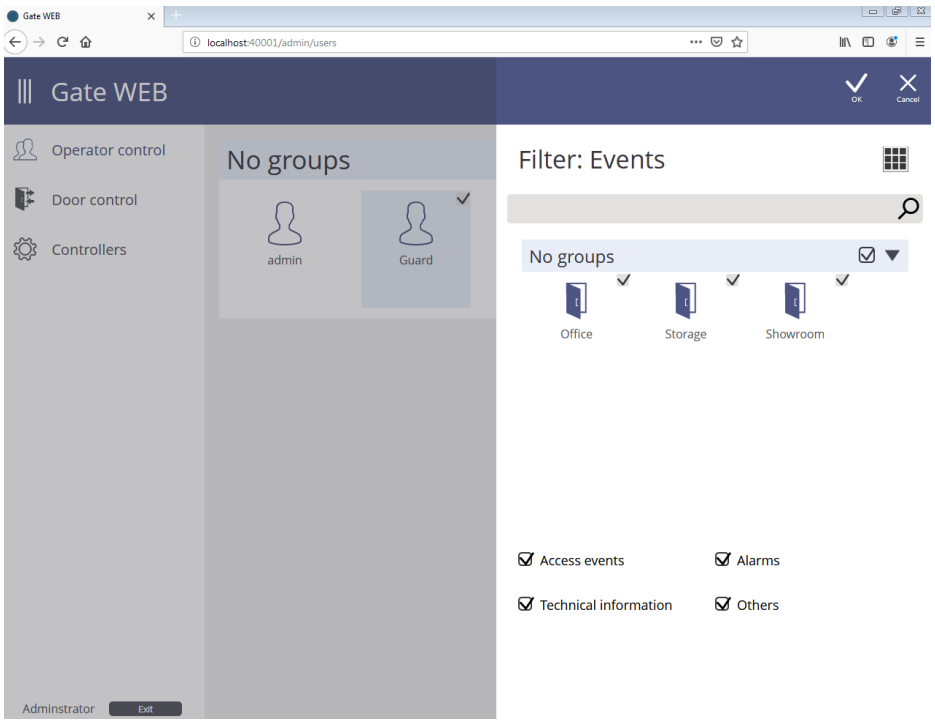
Event log view adjustment

It is possible to adjust sufficient access events display to the system operator with event filter, which separates undesirable access events.

Select operator and press ‘Operator control’ button to adjust event log settings. Then press ‘Filter’ button in ‘Events’ tab.

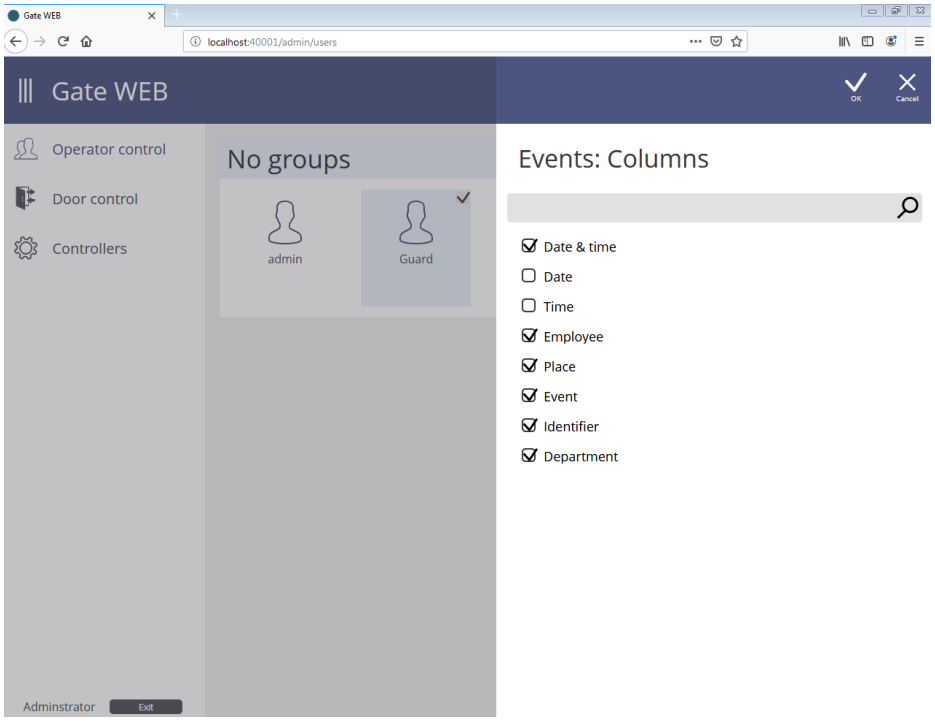


Select desired doors and event categories to be displayed in the log in the window appeared.



Press ‘Columns’ button in ‘Events’ tab to adjust information columns displayed in event log.

Select columns to be displayed in event log in window displayed.

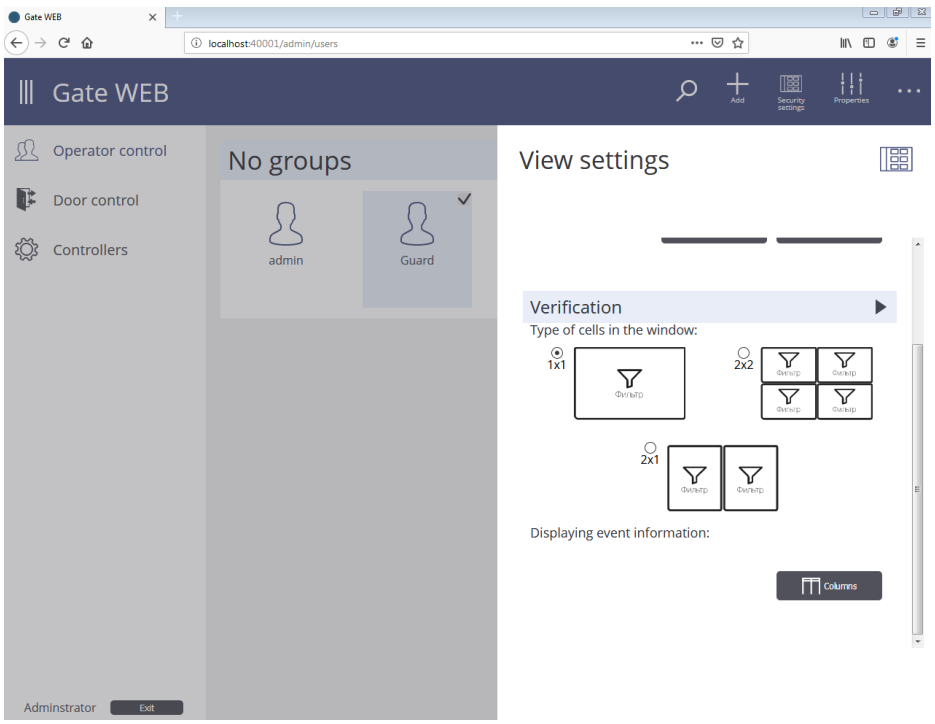


Photoverification view adjustment

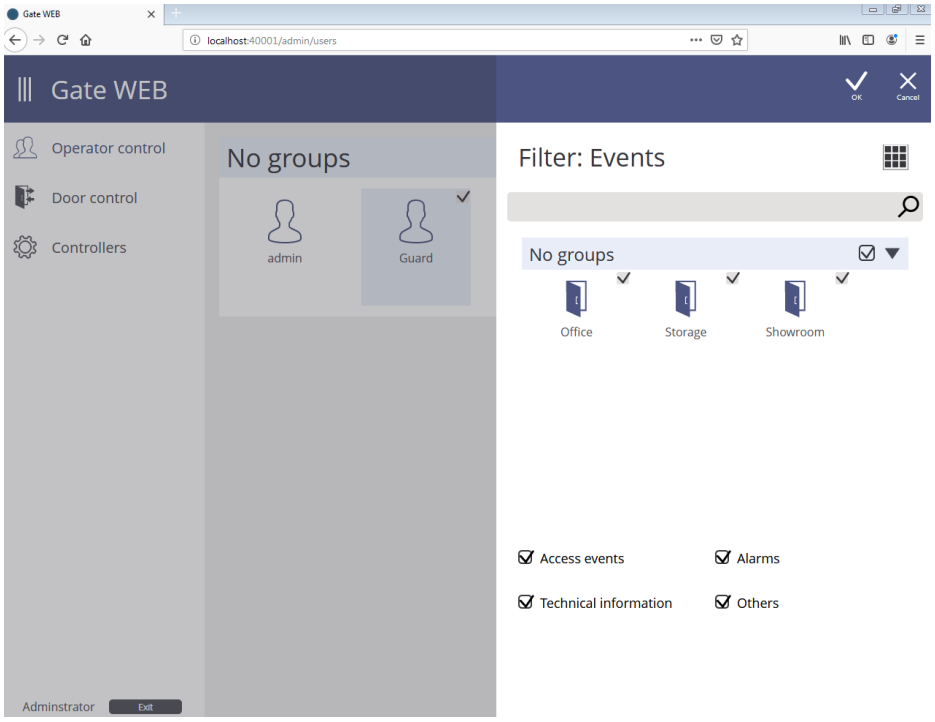
It is possible to associate each photoverification view with doors using event filter.

For instance, enterprise has two entries. You may adjust splitted 1x2 photoverification window in the way when events from first entry will display in first photoverification view and from second entry – in second view.

Select operator □, press ‘Operator control’ button and set number of views (1x1, 2x1, 2x2) in ‘Photoverification’ tab to ajust photoverification settings.

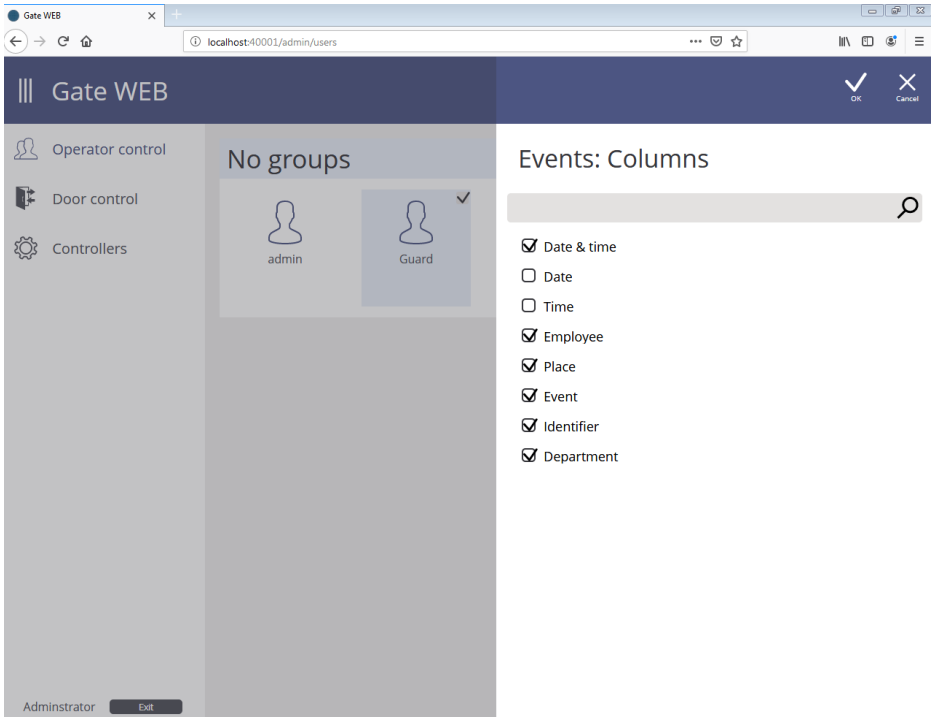


Then press ‘Filter’ button in each view and set events to be displayed. Select desired doors and events’ categories for display.



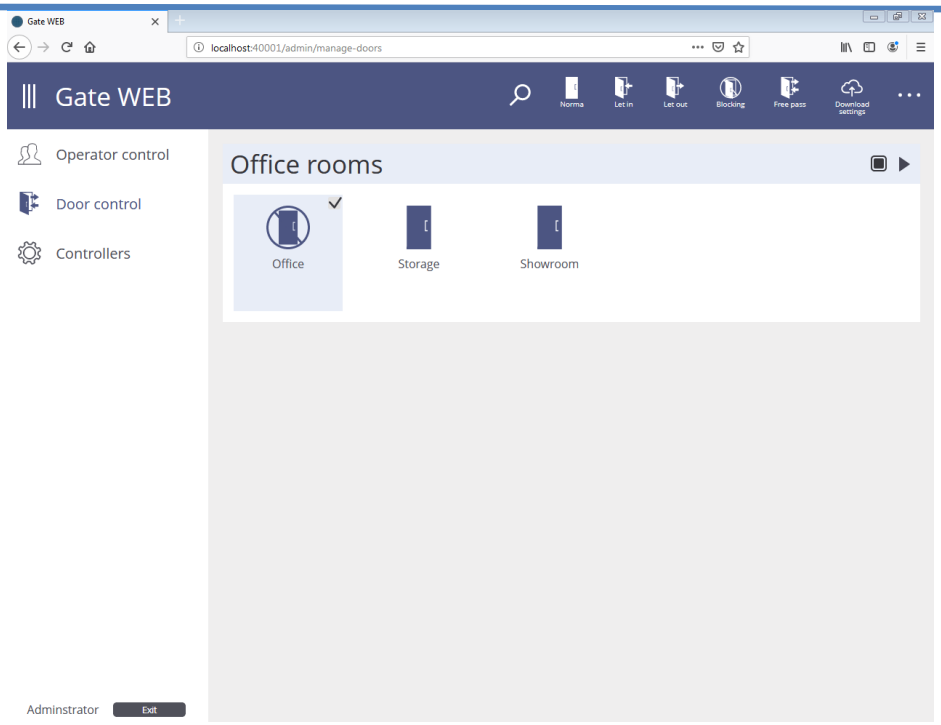
Press ‘Columns’ button in ‘Photoverification’ tab to adjust information columns displayed in event log.

Select columns to be displayed in event log in window displayed.



Door control and state display

Select ‘Door control’ tab. Door current state will be displayed.



Check doors with □ and select necessary command in main menu to change doors' state.

There are available commands as follows:

Norma – Door returns to normal state. Command issued to change doors' state to normal from states of free pass or blocking, which were set by operator. Command doesn't work if above mensioned states appeared as a result of panel inputs state change.

Let in or Let out - commands which open door (for entry or exit). When panel receives this command it sends 'Access point opened by operator request' and switches to access grant mode.

Free pass command switches access point into 'Free pass' mode. Issue 'Normal' command to switch door into the normal mode.

Block- command switches access point into 'Blocked' mode. Issue 'Normal' command to switch door into the normal mode. Issue 'Normal' command to switch door into the normal mode.

Unblock on Fire - group command switches all doors into 'Free pass' mode.

All doors blocking - group command switches all doors into 'Blocked' mode.

Normalise all doors - group command switches all doors into 'Normal' mode.

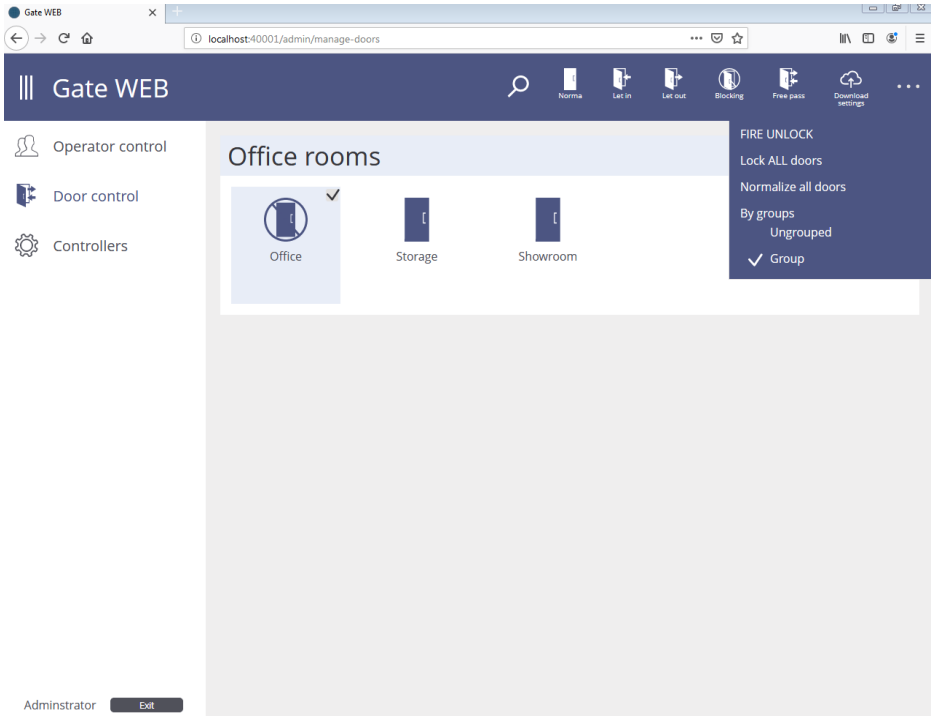
All possible doors' states listed in the table below:

Door states and how they are depicted

State Name

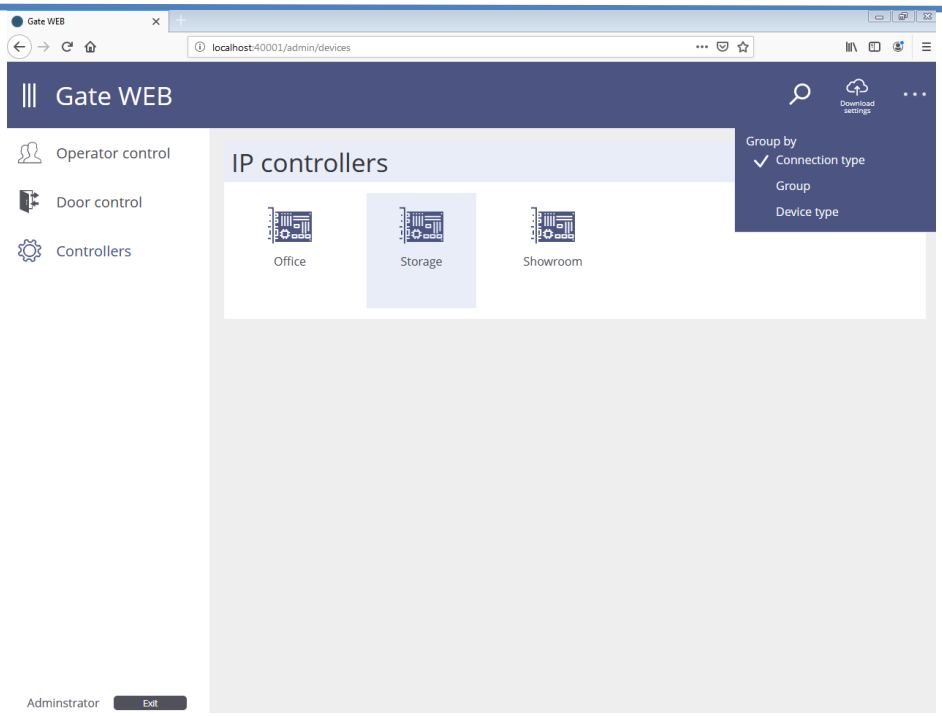
Normal		Door contact normal		Door contact violated
Alarm		Door contact normal. Access is possible after the Alarm state cancellation by operator or with ‘Alarm cancellation’ identifier		Door contact violated. The Alarm state cancellation possible by operator or with ‘Alarm cancellation’ identifier
Block		Door contact normal. Access is possible with ‘Guard’ marked identifier		Door contact violated.
Block and Alarm		Door contact normal. Access is possible with ‘Guard’ marked identifier		Door contact violated. The Alarm state cancellation possible by operator or with ‘Alarm cancellation’ identifier.
Free pass		Door contact normal.		Door contact violated
Trouble		Panel has troubles or there is no connection with it.		

Door search by name and door group order control available in main menu.



Panels’ control and their state display

You have to download panels after adding devices, their configuration changes or personnel access rules changes. Check panels □ and press ‘Download settings’ to do this.



The table below describes all possible panels' states.

Panel's states and icons, depicting them

State		Description
Normal		Panel operates normally
Battery trouble		Battery trouble. Battery fail, battery discharge or panel input for battery supervision violated.
Mains power trouble		Mains power fail or panel input for mains power supervision violated.
Tamper		Panel housing tampered.
General panel trouble		Panel communication lost or panel initializes.
Alarm		Door forced open, code match attempt etc.

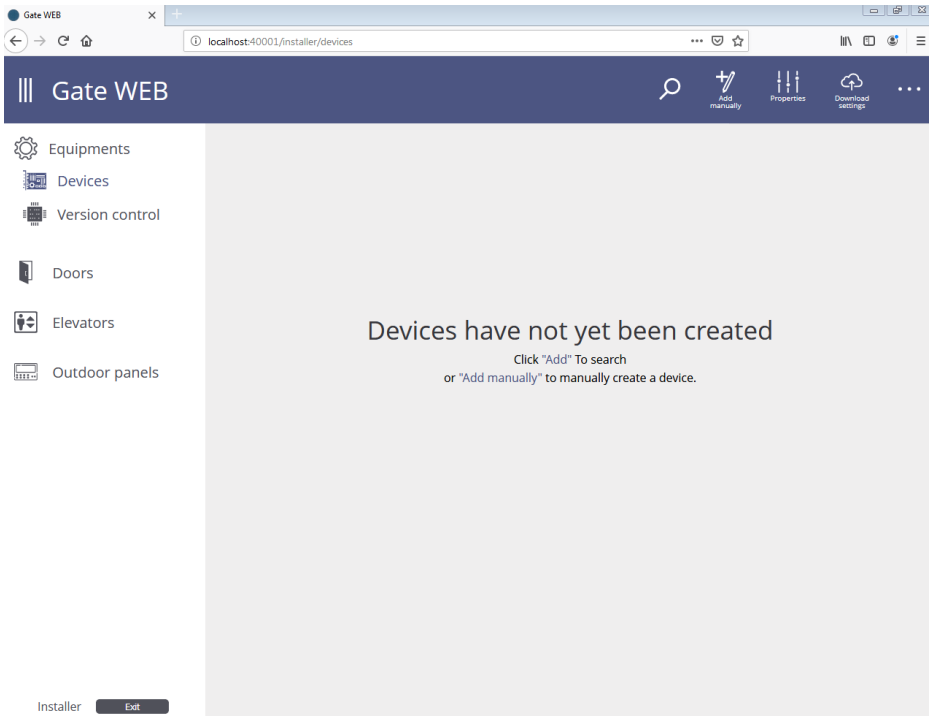
Adding and adjusting devices and doors. ‘Installer’ role

Panels adding

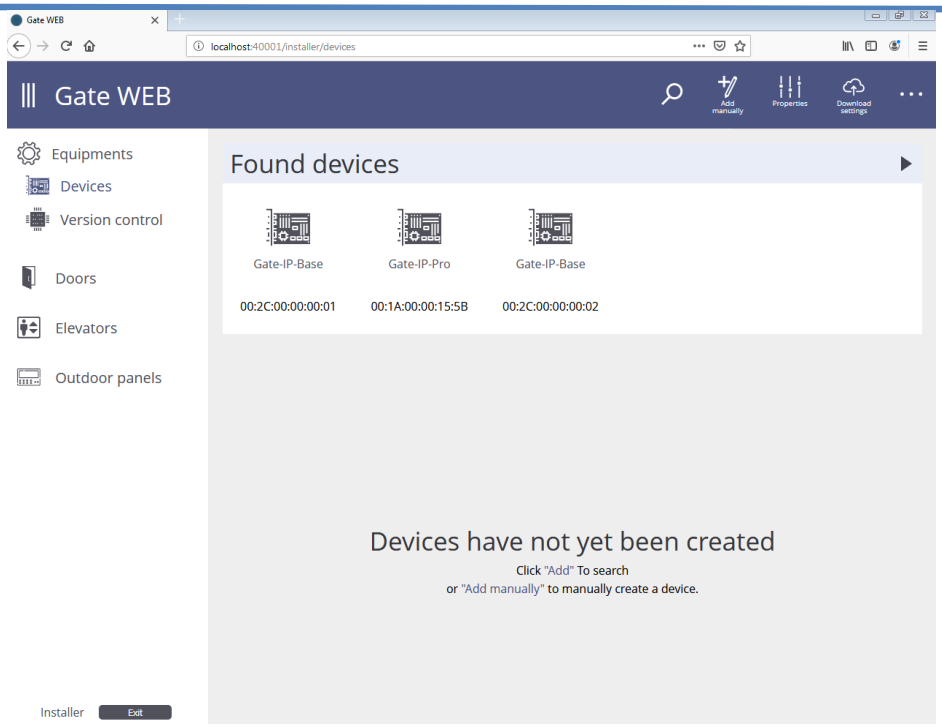
It is necessary to add panels and doors, associate doors with panels and set the doors types (one- or double sided) and adjust panels’ and doors settings.

Connection schema of auxiliary equipment defines types of entry and exit locks of the door, lock open duration and inputs and outputs operation modes.

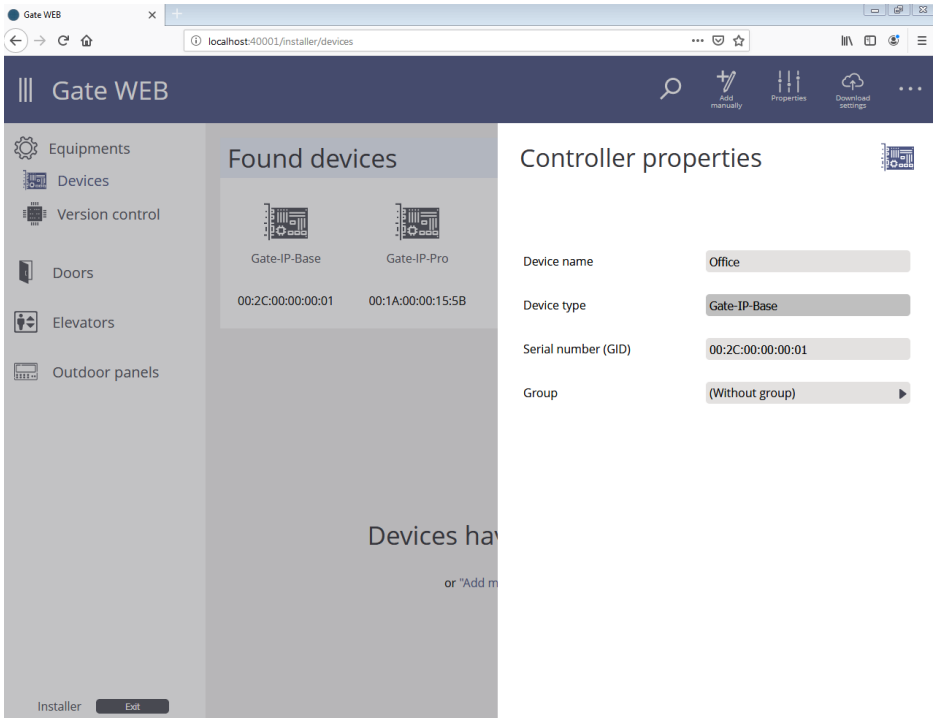
Select ‘Equipment’ tabs (on the right). There are two ways to add equipment – automatic, after search in the local network or manual (device type and serial number required).



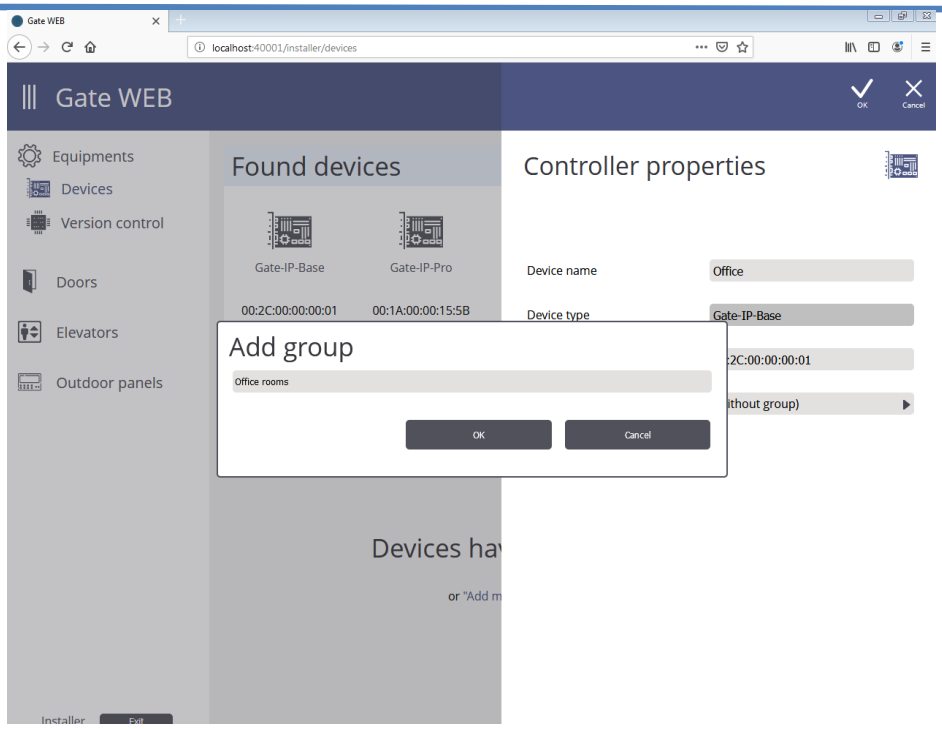
Equipment search panel will display after menu item  selection.



Click with thw left mouse button on device found. Its properties will open.



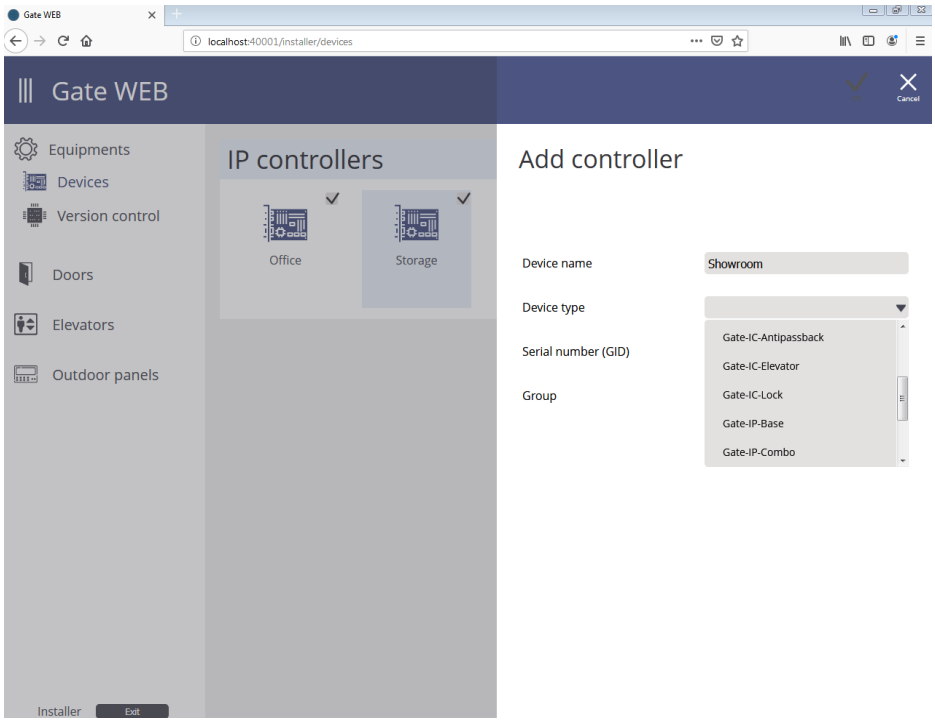
Enter device name and add its group category.



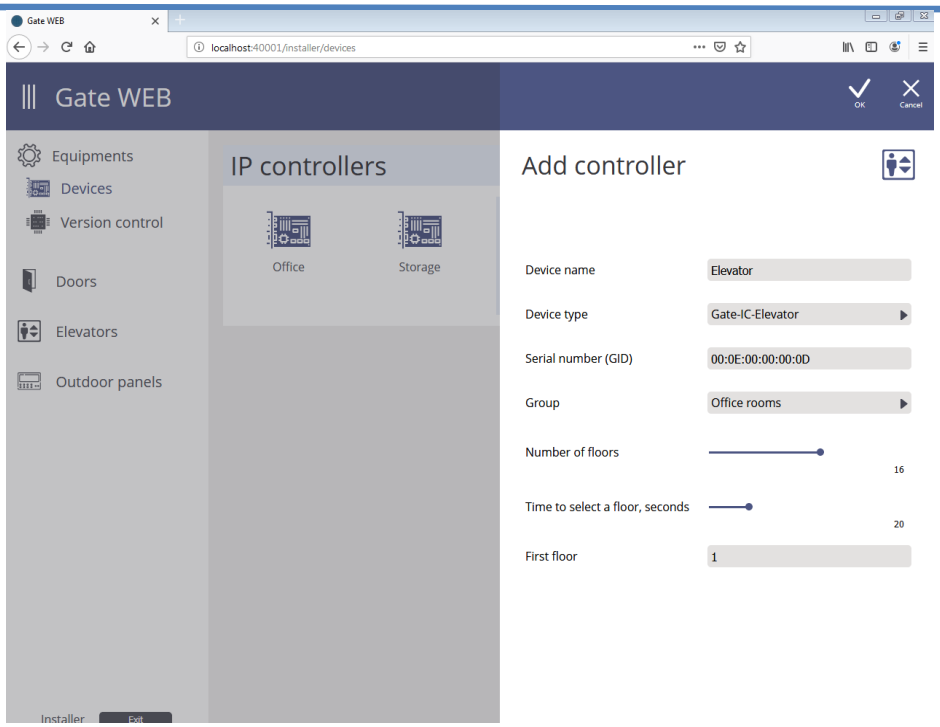
Press ‘OK’ to save changes.

Press  button on equipment search panel to close it.

Select  menu item to add device manually. New panel settings window will open. Enter device name, select panel type, enter serial number and add device group category. Press ‘OK’ to save changes.



It is necessary to adjust additional settings for various panel types. For instance it is number of floors, floor selection duration and starting floor for elevator control panel.

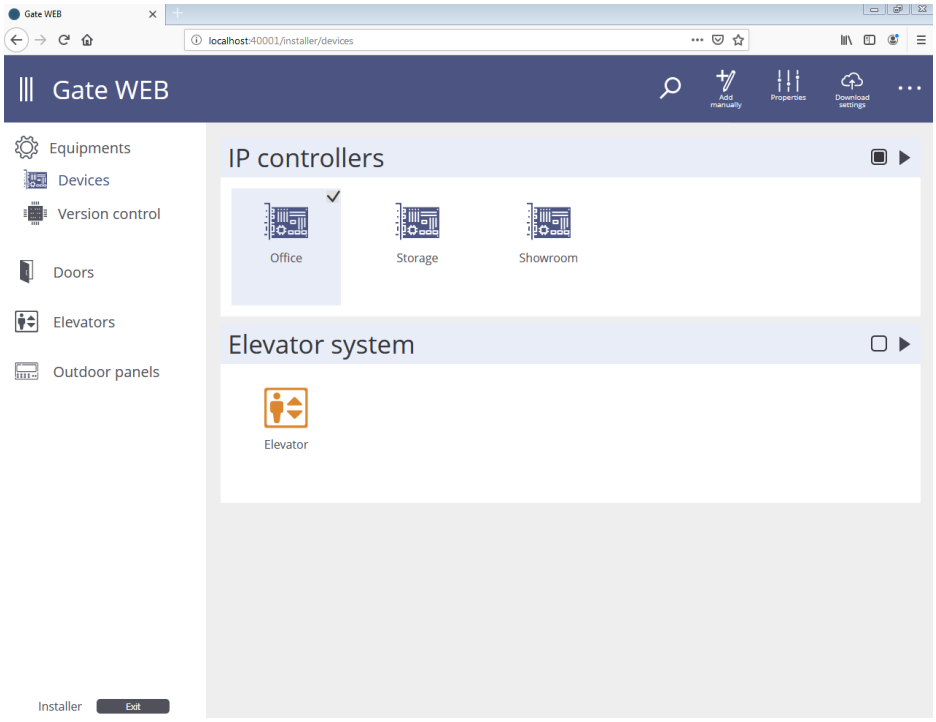


The doors to the floors added automatically after the elevator control panel added.

There are functions of search device by name, selected device settings viewing, device deletion and grouping order device display available in main menu.

Panels' control and state display

It is necessary to download panels after panels' settings change or personnel access rights change. Select panels □ and press 'Download settings' button.



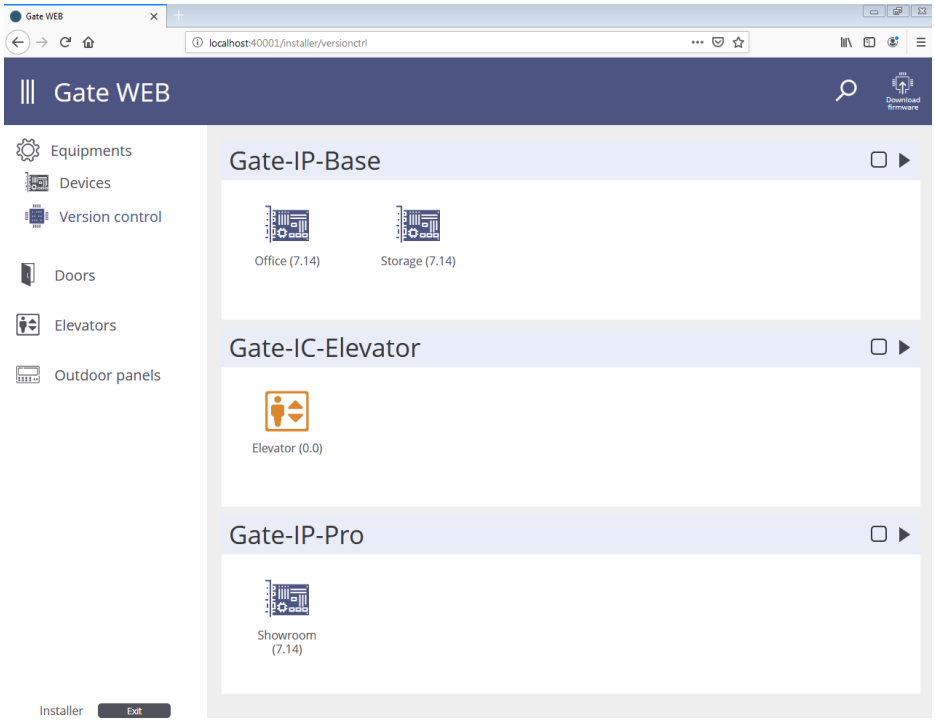
The table below describes all possible panels' states.

Panel's states and icons, depicting them

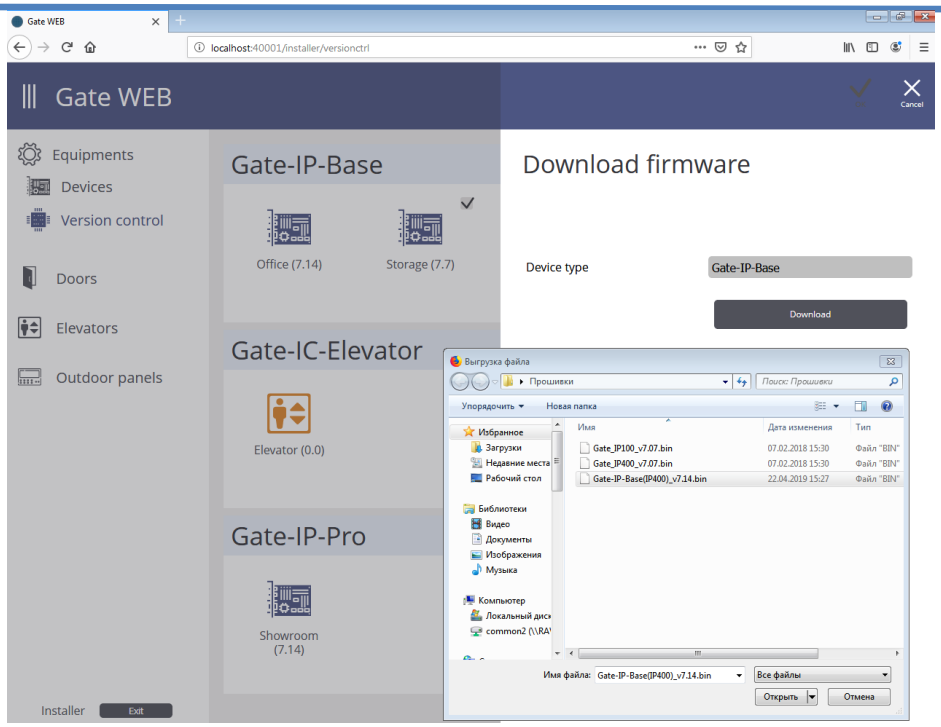
State	Description
Normal 	Panel operates normally
Battery trouble 	Battery trouble. Battery fail, battery discharge or panel input for battery supervision violated.
Mains power trouble 	Mains power fail or panel input for mains power supervision violated.
Tamper 	Panel housing tampered.
General panel trouble 	Panel communication lost or panel initializes.
Alarm 	Door forced open, code match attempt etc.

Device firmware upgrade

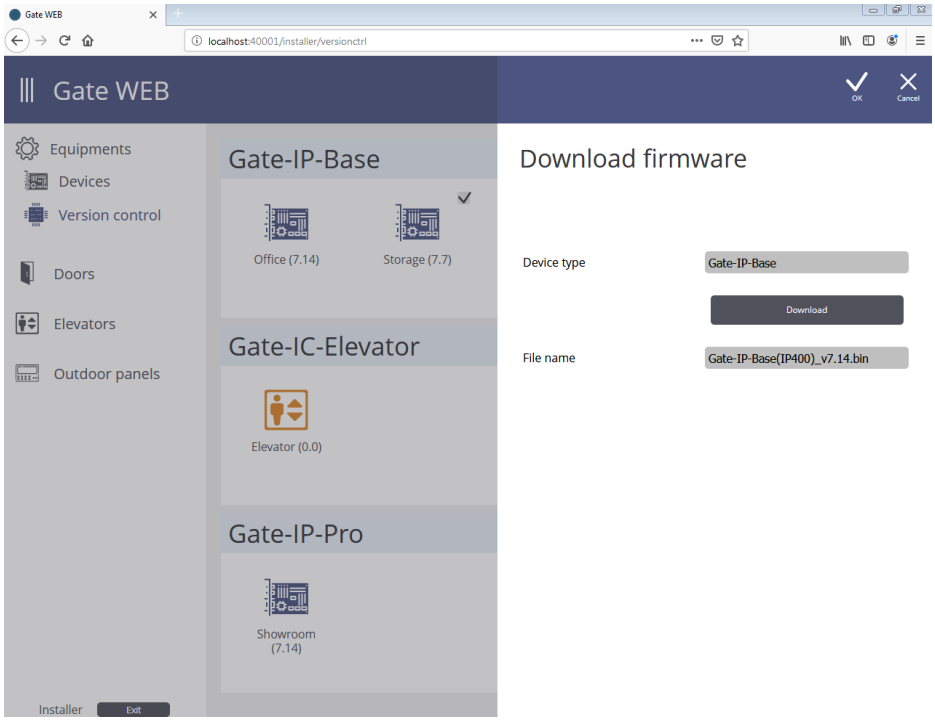
Select 'Version control' tab. Select one or more panels of the same type and press 'Download firmware' button.



Press 'Download' button in window appeared and choose the path to the file containing the firmware in the window displayed.

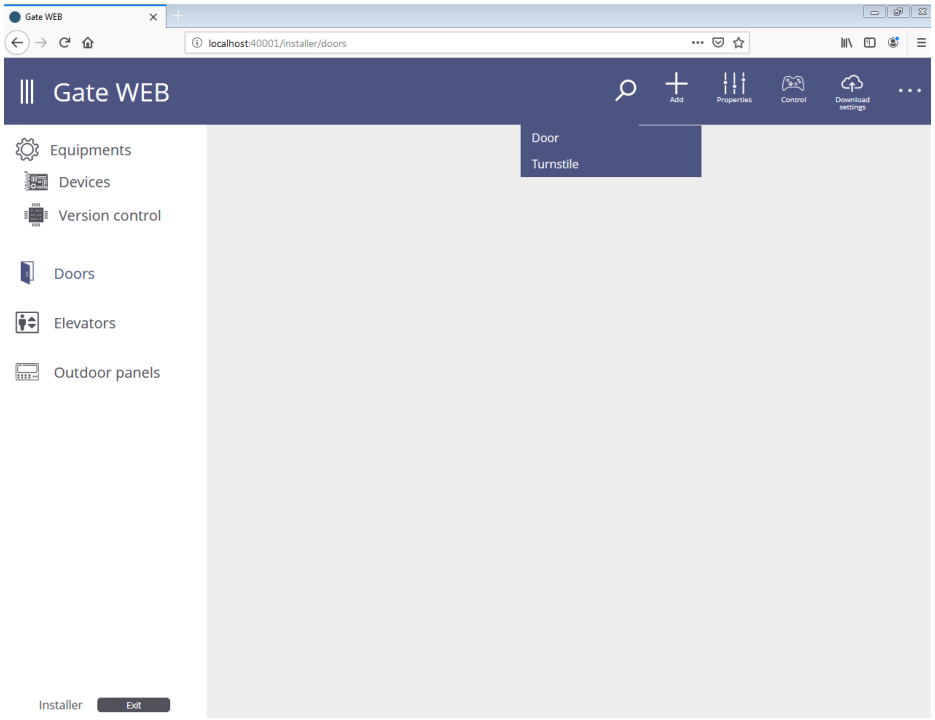


Selected panels will be downloaded with firmware after ‘OK’ button press. The progress bar displaying the download process displayed under each panel icon.

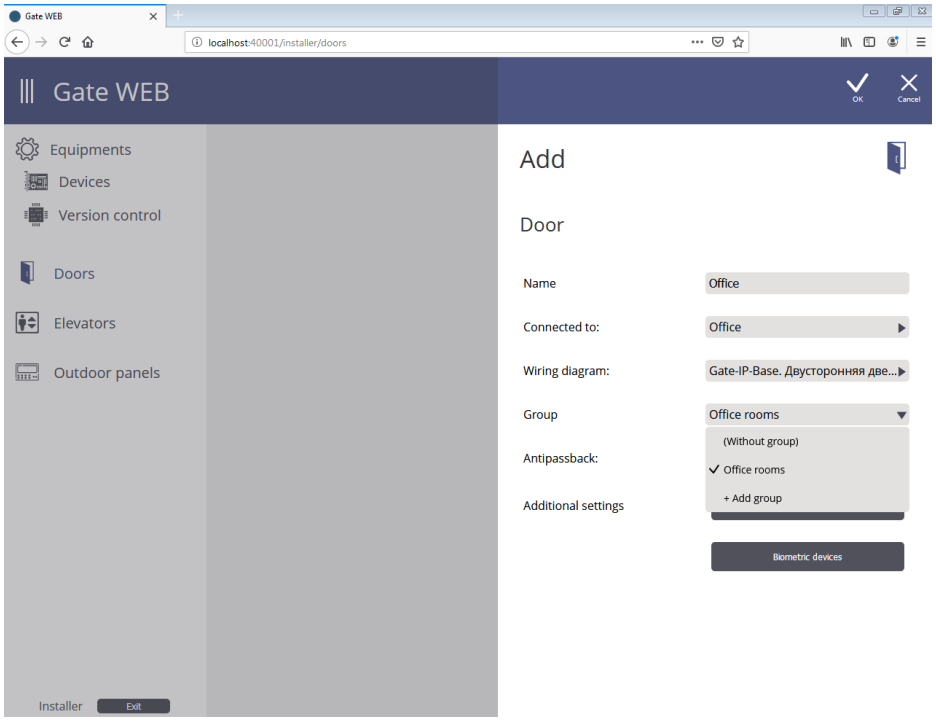


Door adding

Select ‘Doors’ tab. Press ‘Add’ button.



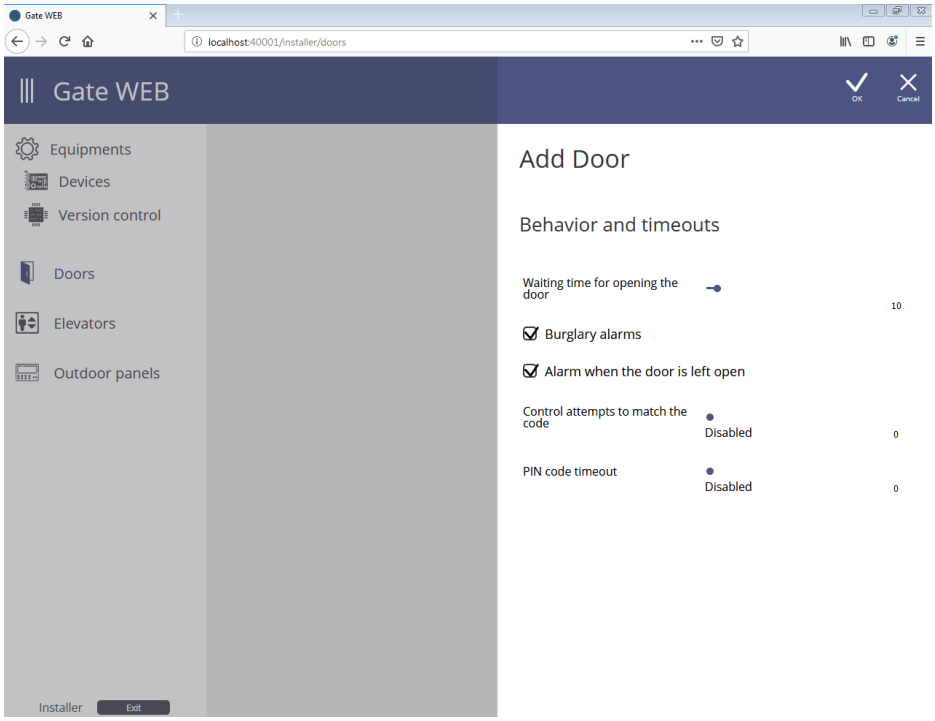
Enter door name and select panel which will control this door. Connection schemas become available after this. This schemas define inputs response types, outputs operation modes and antipassback operation.



Add created doors into groups. Groups describe the facility structure to make the work with doors easier. For instance, ‘Ground floor doors’, ‘First floor doors’ etc.

It is possible to change group name in future.

Press ‘Behavior and timeouts’ button to change the default door settings. Settings as follows adjustable in window displayed.



Door time– Waiting time for opening the door. Duration of door must be opened and closed at access granted. Door opening and closure defined by door contact violation and normalization.

Door forced open alarm – door and panel will not go into ‘Alarm’ state if door sensor violated without access granted if this option is OFF.

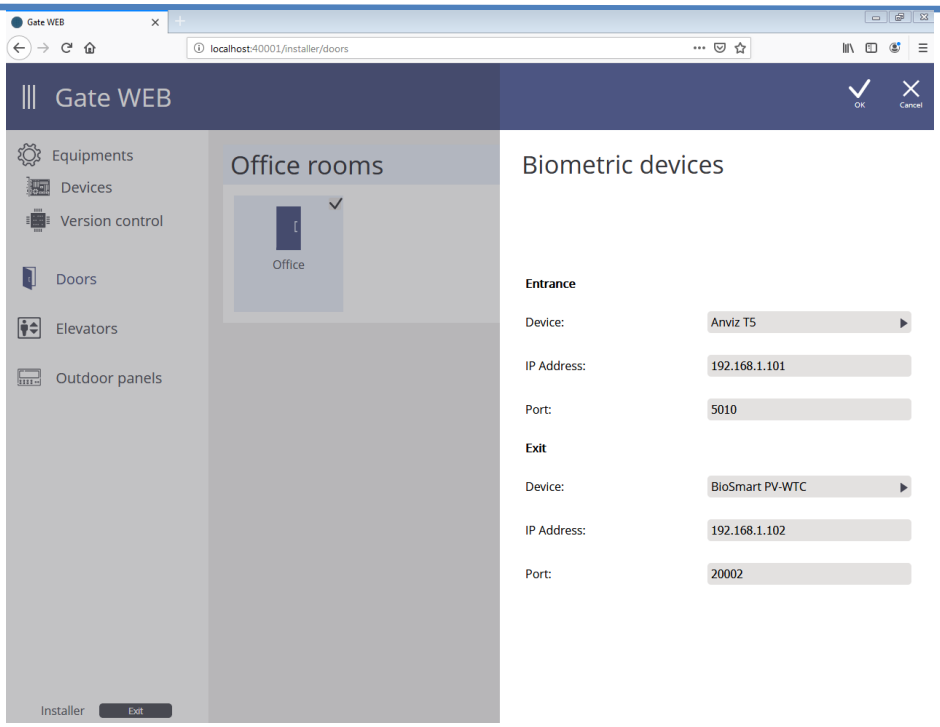
‘Door opened too long’ – door and panel will not go into ‘Alarm’ state if door was opened too long if this option is OFF.

Code match attempts – number of wrong codes or cards, entered in during short time, causing panel to switch into the ‘Alarm’ mode.

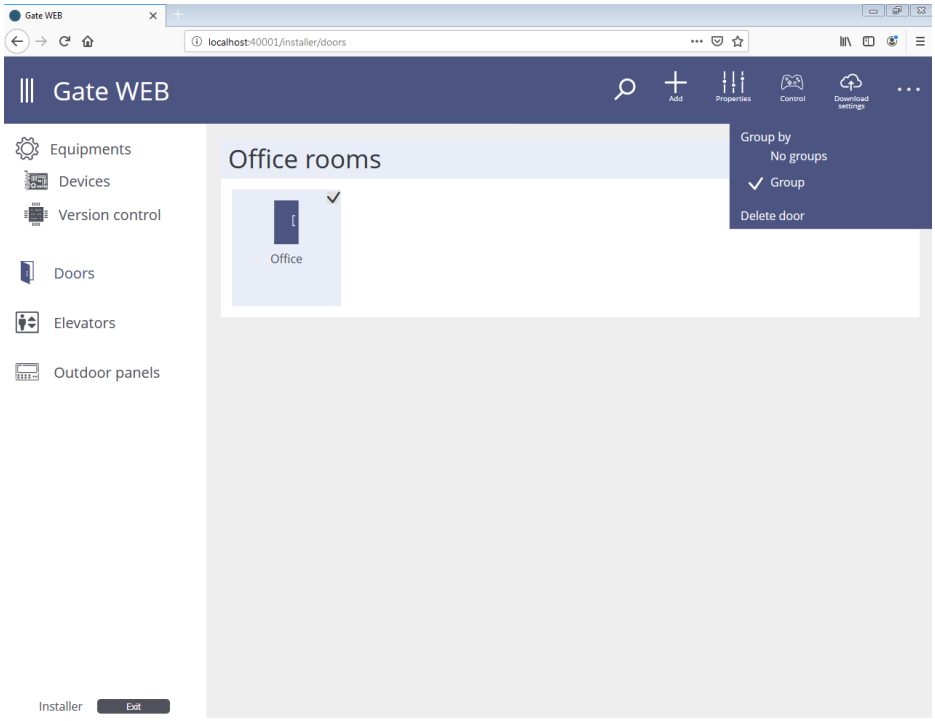
PIN entry wait duration – Each access point may have PIN reader for PIN entry. It is necessary to enter PIN besides card passing to access door with PIN reader.

Set nonzero time during which panel will wait for PIN entry after card pass. Set zero time to disable PIN entry supervision.

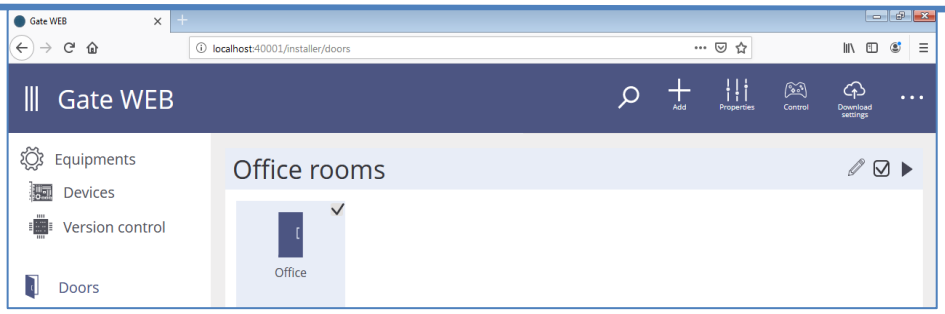
"Biosmart" and "Anviz" biometric devices, operating as readers, integrated into the Gate-IP WEB system. Press ‘Biometric Devices’ in the door properties tho set up diametric devices. Set the biometric device type, it’s IP address and port for both entry and exit point of door for device control ams download:



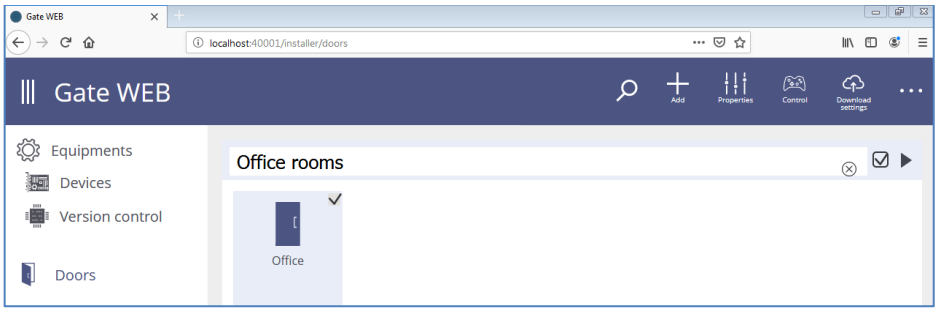
Door search by name, door properties view and door groups' display way available in the window main menu.



Point the door group name with mouse cursor and press □ icon to rename it.

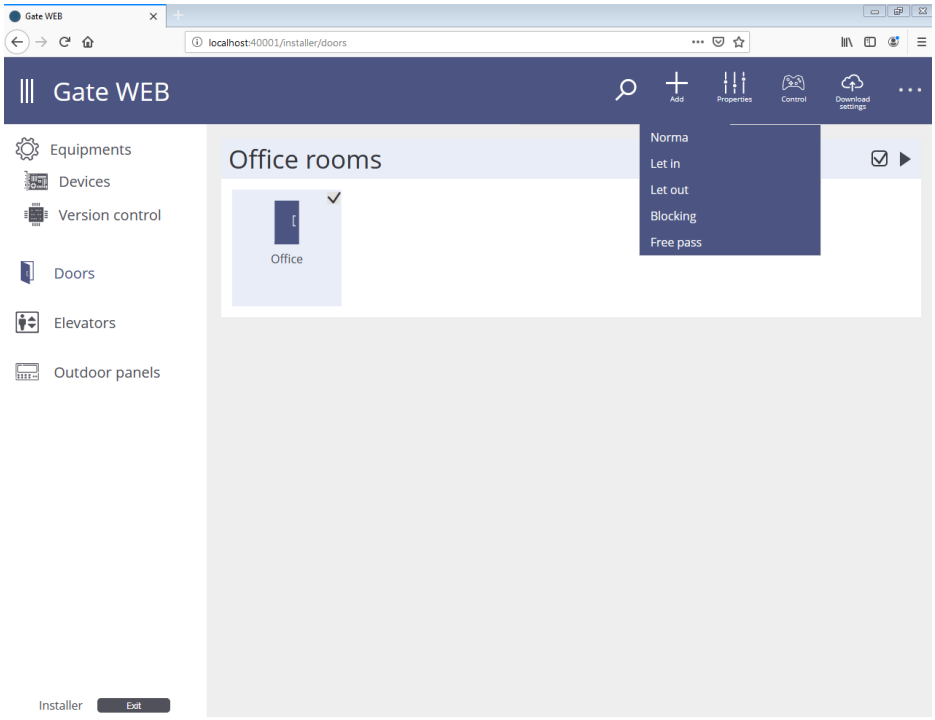


Enter new door group name in the window appeared:



Door state control and display

Mark door(s) □ and select menu item ‘Control’ in the main menu to change door(s) operation mode.



Commands available:

Let in, let out – those commands open the door (for entry or exit). Panel sends ‘Door opened by operator request’ event message, unlocks the door and switches into access grant mode.

Norma – This command returns door into ‘Normal’ operation mode from ‘Free pass’ or ‘Block’ states. Command doesn’t have effect if ‘Free pass’ or ‘Blocked’ states arose due to panel inputs violation.

Free Pass – This command switches door into ‘Free Pass’ state. Send ‘Norma’ command to switch door into normal state back.

Blocking – This command switches door into ‘Blocked’ state. Send ‘Norma’ command to switch door into normal state back.

Download panels after door adding, doors settings or personnel access rights change. Check doors □ and press and press ‘Download settings’ to do this.

All possible door states and their depiction are in the table below.

Door state and their depiction table.

Name				
Normal state		Door sensor closed		Door sensor opened

Alarm		Door sensor closed. Access is possible only after alarm cancellation from system or with ID, marked as ‘Alarm cancellation’.		Door sensor opened. Cancel alarm from system or with ID, marked as ‘Alarm cancellation’.
Blocking		Door sensor closed. Access is possible with ID, marked as ‘Guard’ only.		Door sensor opened
Blocking and alarm		Door sensor closed. Access is possible with ID, marked as ‘Guard’ only.		Door sensor opened. Cancel alarm from system or with ID, marked as ‘Alarm cancellation’.
Free pass		Door sensor closed.		Door sensor opened.
Trouble		Panel trouble or connection with panel lost		

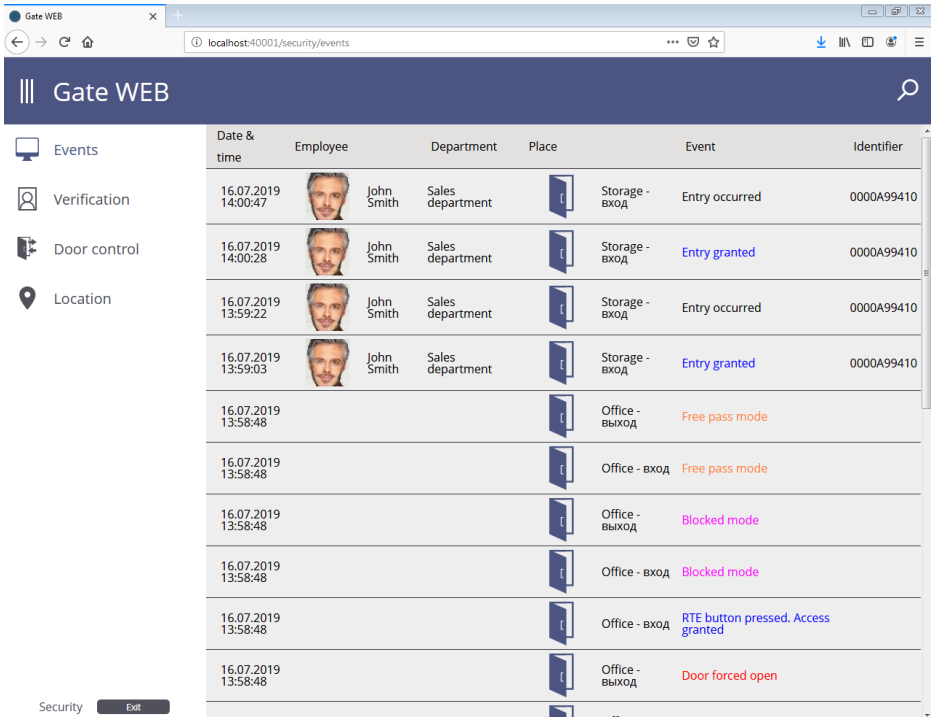
’Guard’ role

This role provides online event monitoring, photoverification and door control.

Event monitoring

Personnel entry and exit, door open and close and other events occur during system operation. Control panels log all this events and send them to the central server. It is possible to display events on the workplaces of the system.

Select ‘Events’ tab to the left to display current event log.



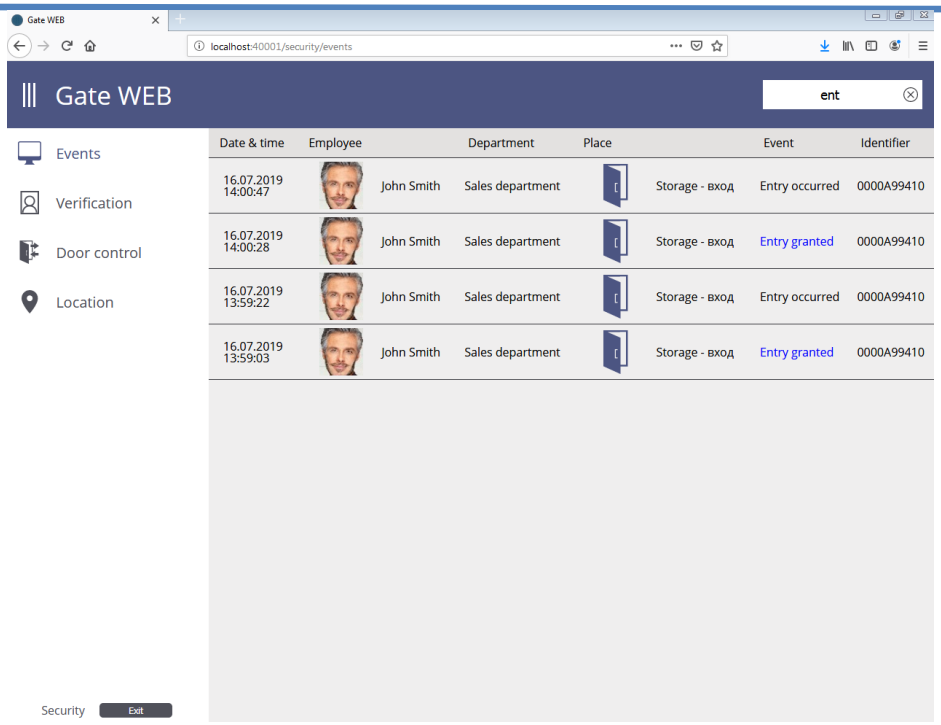
Window contains data:

- event date and time;
- photo and name of the cardholder
- Door where event occurred or panel logged this event
- Event description;
- ID number.

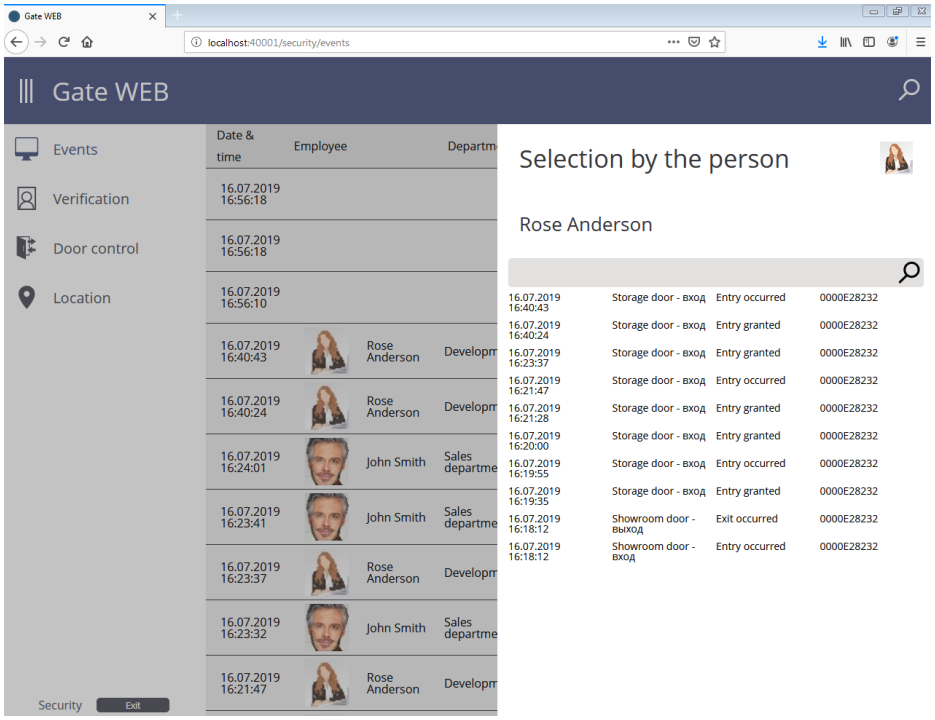
It is possible to adjust the fields displayed in ‘Administrator’ workplace

Select menu item ‘Search’ in main menu and enter the keyword or part of it for fast event filtering.

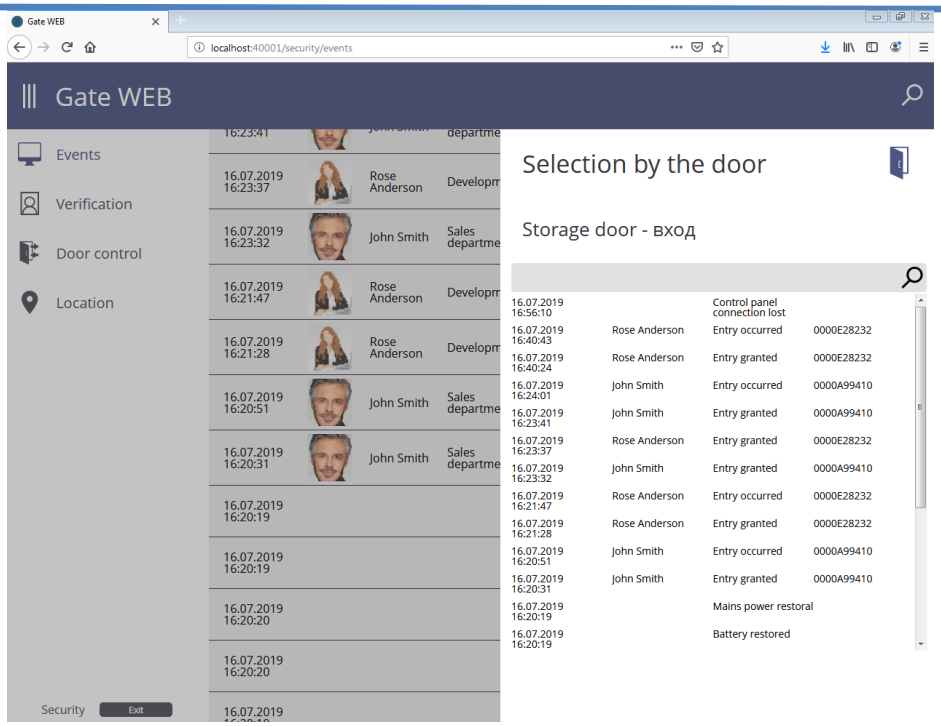
’Entr...’ event filtering, for instance:



It is possible to use person or access point fast selection function for filtration. Click on the person photo or name in the event log to open selection by person



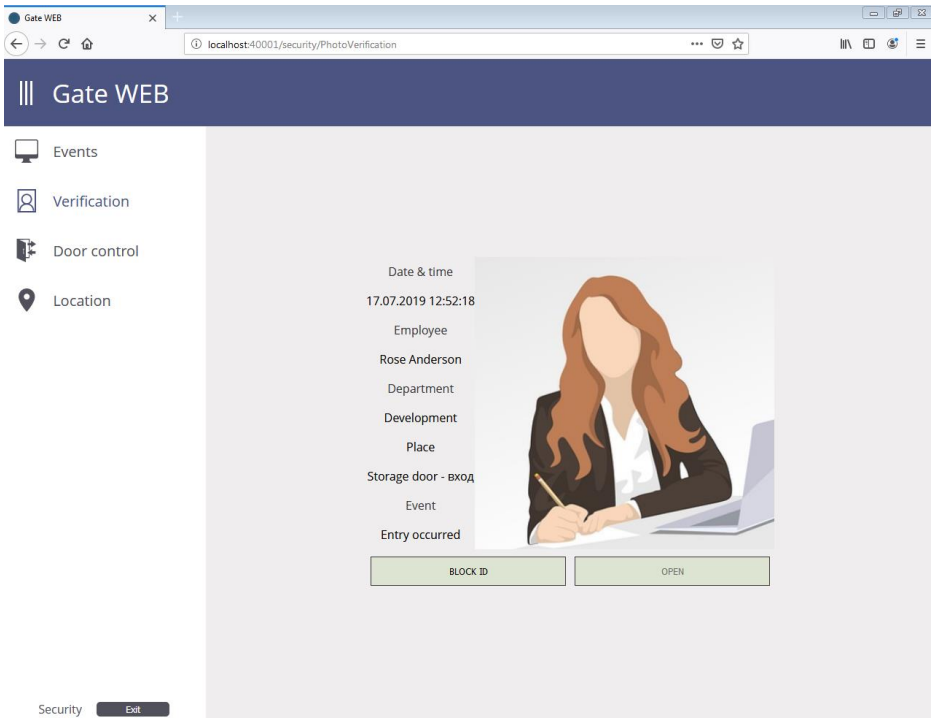
Click on the door icon or name in the event log to open selection by door:



Photoverification

The main goal of photoverification is to enable operator to compare the person face with true photo in the database.

Select ‘Verification’ tab to the left. Information about the new event displayed in the window. The photo from the database of the person, passed the card, displayed as well.



It is possible to split the photoverification window into several cells. The events from the certain door displayed in each cell of the window.

Date and time, cardholder name, event place and it's description displayed to the left side of the cell and photo – to the right.

Photoverification window also contains two buttons – 'Block ID' and 'Open'.

Open – Command, which opens the door send to panel on this button press. Panel logs 'Door opened by operator request', unlocks the door and switches to the access grant mode.

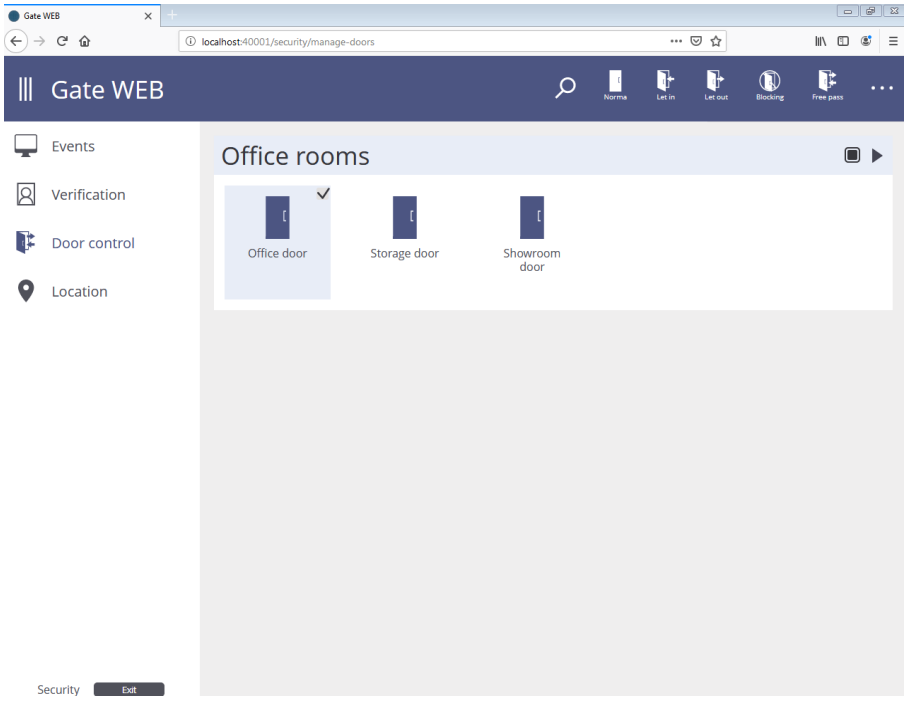
This command usually used to grant access to the employee, needed on the enterprise territory, but information of this access absent in the panel. For instance, when employee called to be at work in his non-working hours.

Block ID – this button send to all panels the command to block ID immediately.

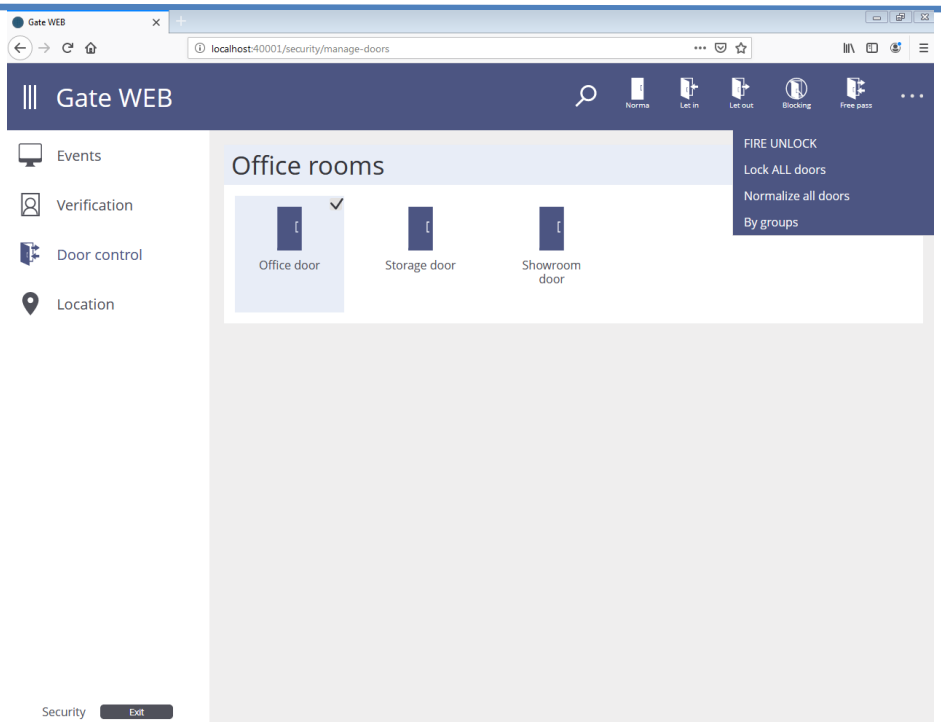
It is possible to adjust the fields displayed, number of cells and sell association with the doors, in 'Administrator' workplace

Door control

Select 'Door control' tab. The current state of doors will display.



Check ☐ door(s) and select desired command to change door(s) state.



Commands available:

Norma – This command returns door into 'Normal' operation mode from 'Free pass' or 'Block' states. Command doesn't have effect if 'Free pass' or 'Blocked' states arose due to panel inputs violation.

Let in, let out– those commands open the door (for entry or exit). Panel sends 'Door opened by operator request' event message, unlocks the door and switches into access grant mode.

Free Pass – This command switches door into 'Free Pass' state. Send 'Norma' command to switch door into normal state back.

Blocking – This command switches door into 'Blocked' state. Send 'Norma' command to switch door into normal state back.

Download panels after door adding, doors settings or personnel access rights change. Check doors □ and press and press 'Download settings' to do this.

Fire UNLOCK – This command switches all doors into 'Free Pass' state.

All doors Blocking – This command switches all doors into 'Blocked' state.

Normalize all doors – This command returns all doors into 'Normal' operation mode

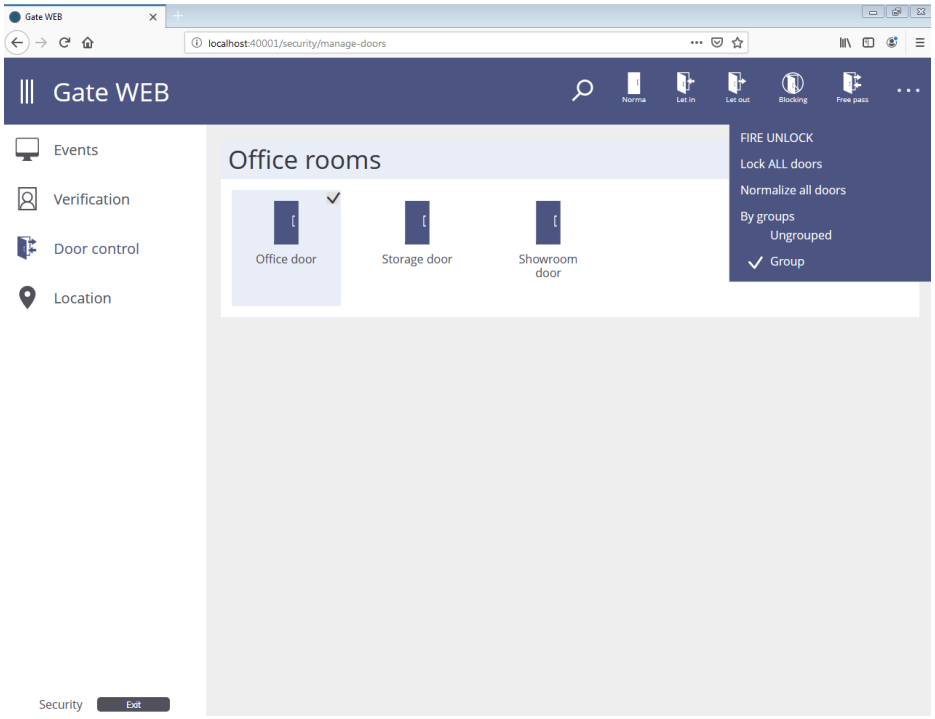
All possible door states and their depiction are in the table below.

Door state and their depiction table.

Name				
Normal state		Door sensor closed		Door sensor opened

Alarm		Door sensor closed. Access is possible only after alarm cancellation from system or with ID, marked as ‘Alarm cancellation’.		Door sensor opened. Cancel alarm from system or with ID, marked as ‘Alarm cancellation’.
Blocking		Door sensor closed. Access is possible with ID, marked as ‘Guard’ only.		Door sensor opened
Blocking and alarm		Door sensor closed. Access is possible with ID, marked as ‘Guard’ only.		Door sensor opened. Cancel alarm from system or with ID, marked as ‘Alarm cancellation’.
Free pass		Door sensor closed.		Door sensor opened.
Trouble		Panel trouble or connection with panel lost		

Door search by name and display order available in main menu.



Personnel and access rights settings. ‘Personnel managing’ role

Access rights, schedules, enterprise structure and employees and IDs adding available for this role.

Each employee belongs to the certain group or department in most of enterprises. Those groups and departments have different acer rights. Security department personnel usually has access to all premises without limits for instance. On contrary, employees of production facility #1, for instance must attend only this facility and do not have rights to attend production facility #2.

Examples above show that enterprise department structure strictly enough describes essential access rights of employees.

There are exceptions certainly. For instance, chief of the production facility #1 may attend other places in enterprise on contrary to his subordinates. He must have wider access rights.

It is more convenient to create access rights for group than to each employee personally because the number of departments less than number of employees. That’s why the access rights schema based on enterprise structure will be simple and understandable.

Give the group access rights to the most of personnel. Give access individually only to several employees, for instance to ciefs of departments.

Create for the first time the group access rights and then find and create exceptions for personal access rights. Gate IP WEB provides possibility to create both group and personal access rights.

First of all add schedules, than rules for access rights and fill the database with enterprise hierarchic structure. Make the list of all departments, production facilities and groups. Add all departments and groups to the database, beginning from the highest level.

Attention!!! Download panels after employees, visitors, ID cards added or access rights changed. Press ‘Download settings’ button to do this.

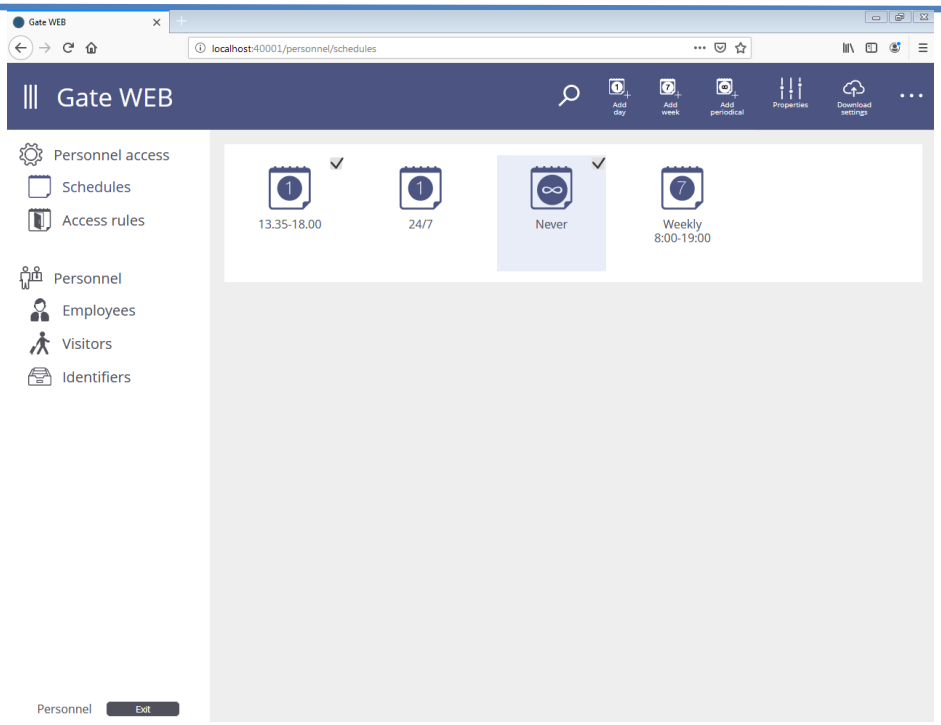
Personnel access: schedules

Schedule is an important part of access rights because panel defines employee access time from the schedule.

System provides periodic schedules with arbitrary period. Schedules may be weekly or any other number of days.

Three schedules available at once after system installation: “24/7”, i.e. always; ‘Never’ and “Week 8:00 – 19:00” (Mon - Sun).

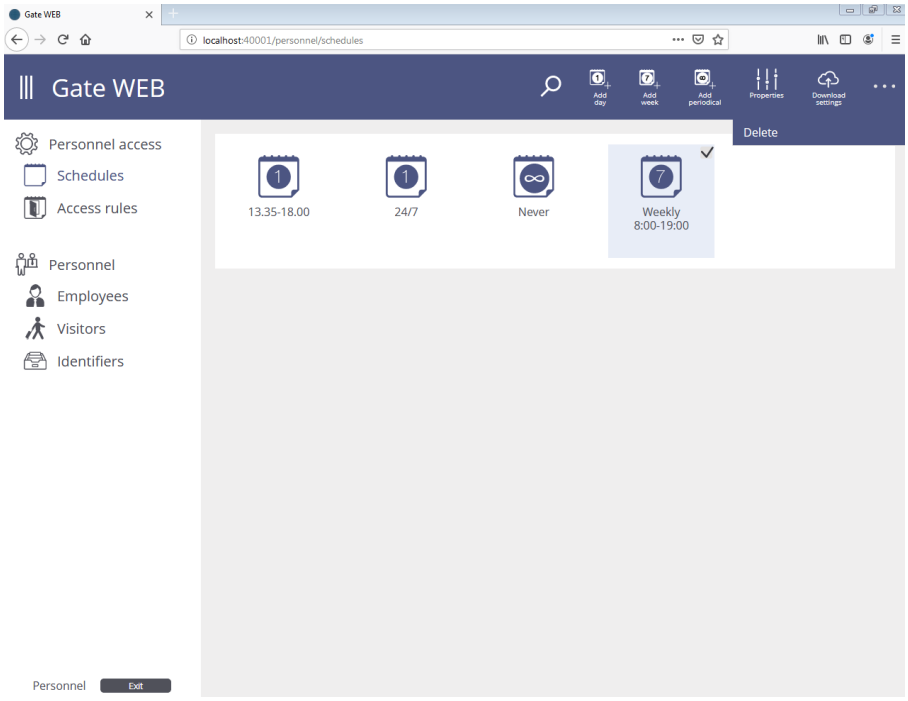
Select ‘Schedules’ and press button corresponding to the desired schedule: ‘Add day’, ‘Add week’ or ‘Add periodic’.



Select □ schedule and press ‘Properties’ button to change it. Edit window will display.

Download panels after schedules’ settings change. Press ‘Download settings’ to do this. Select ‘Search’ item in main menu and enter keyword or its part in edit field to fond schedule by name quickly.

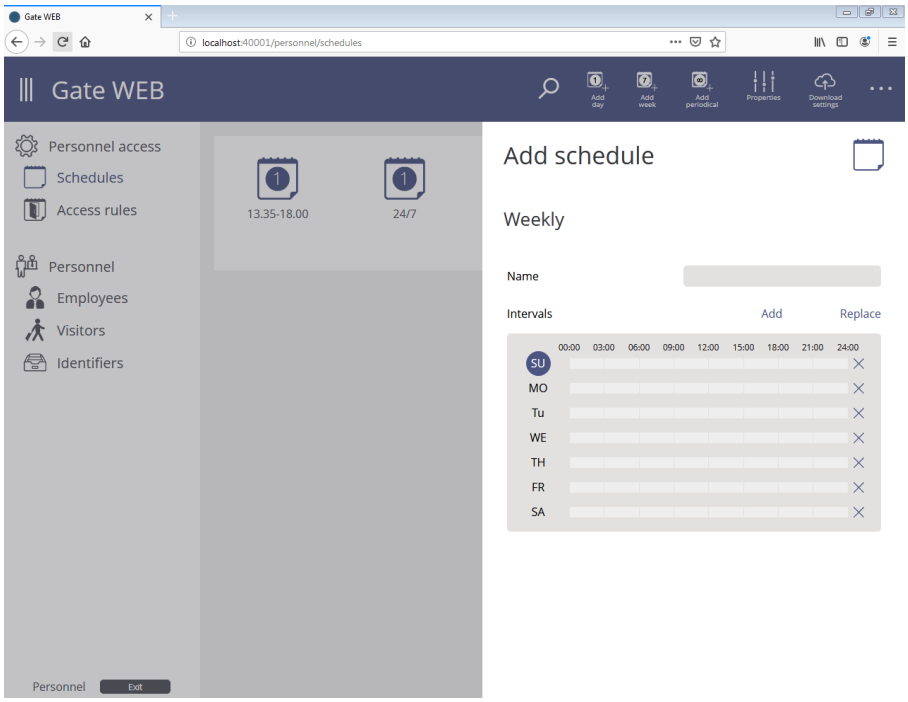
Select □ schedule and press ‘Delete’ button to delete it.

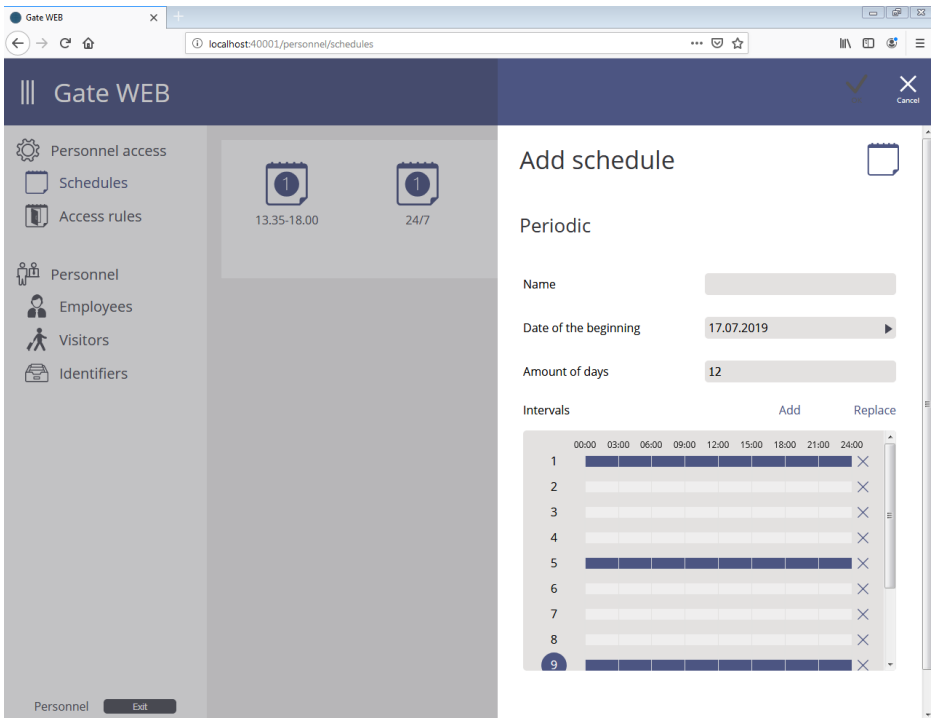


Schedule adding, intervals adjustment

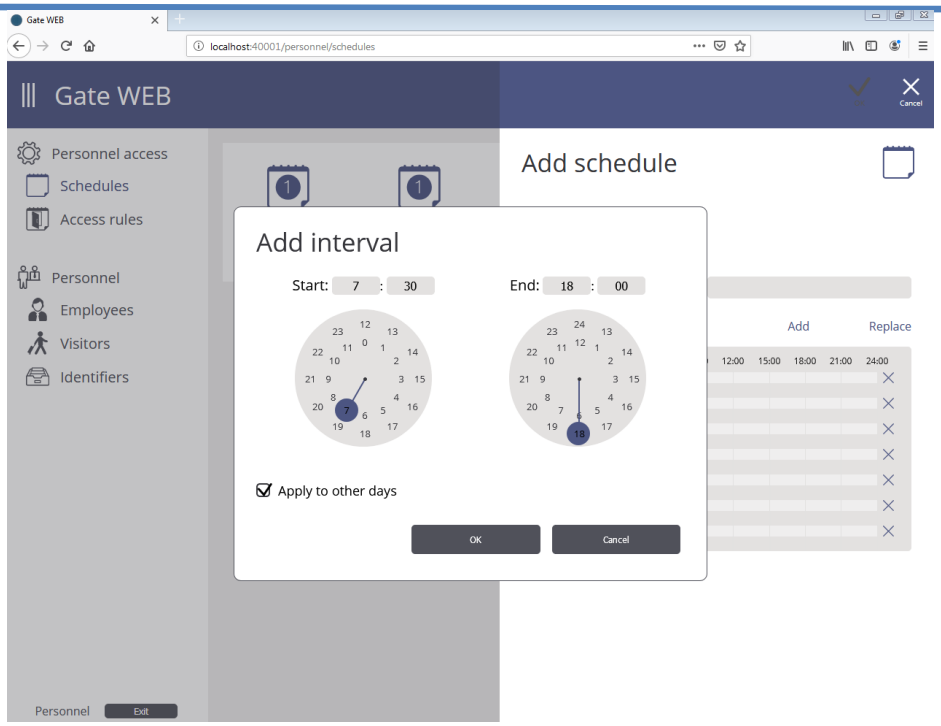
Schedule edit window will open after button ‘Add’ press.

Enter schedule name and adjust time zones, allowed for admission. For periodic type of schedule set the period in days.

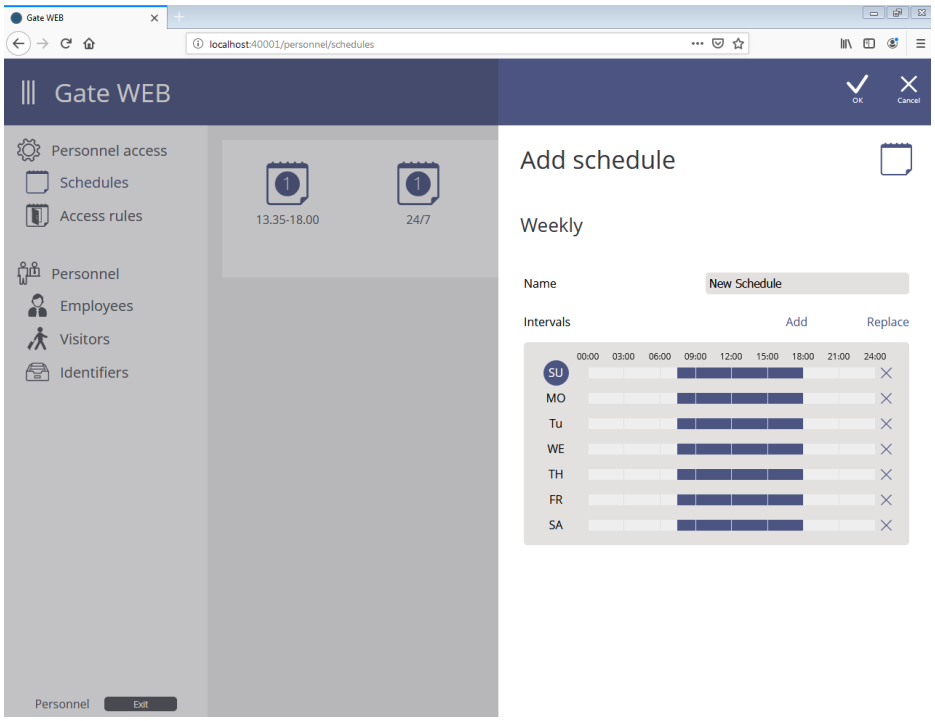




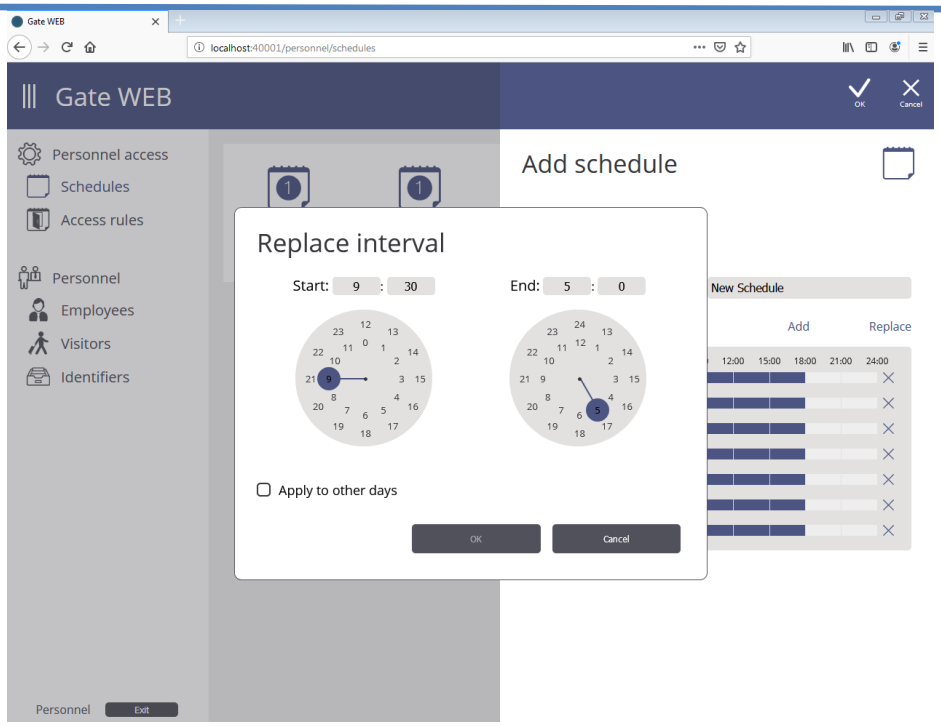
Select day to the left and press ‘Add’ to add time zone for access grant. Mark ‘Start’ and ‘End’ values in the window displayed. Use text edit fields to set time precisely.



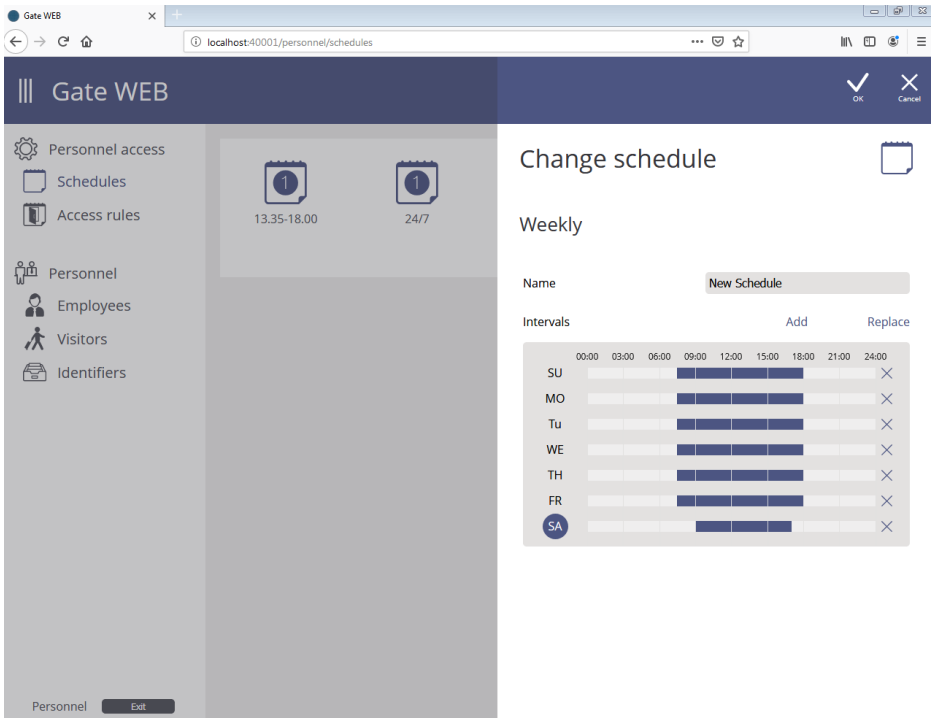
Time zone will expand on all days below if ‘Apply to other days’ option checked.



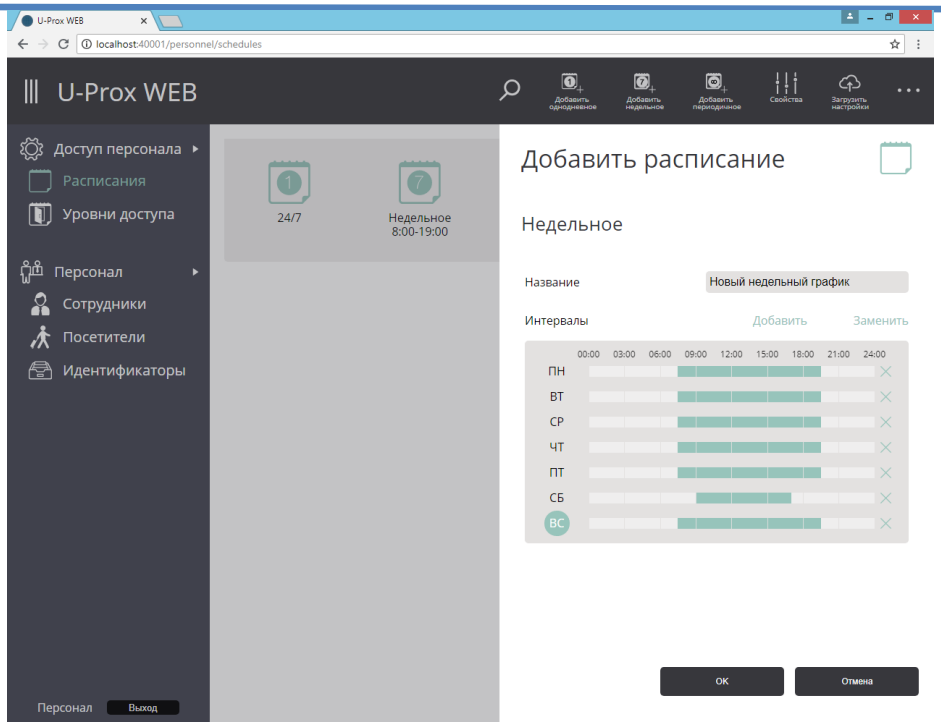
Select day to the left and press ‘Replace’ to replace time zone. Mark ‘Start’ and ‘End’ values in the window displayed. Use text edit fields to set time precisely.

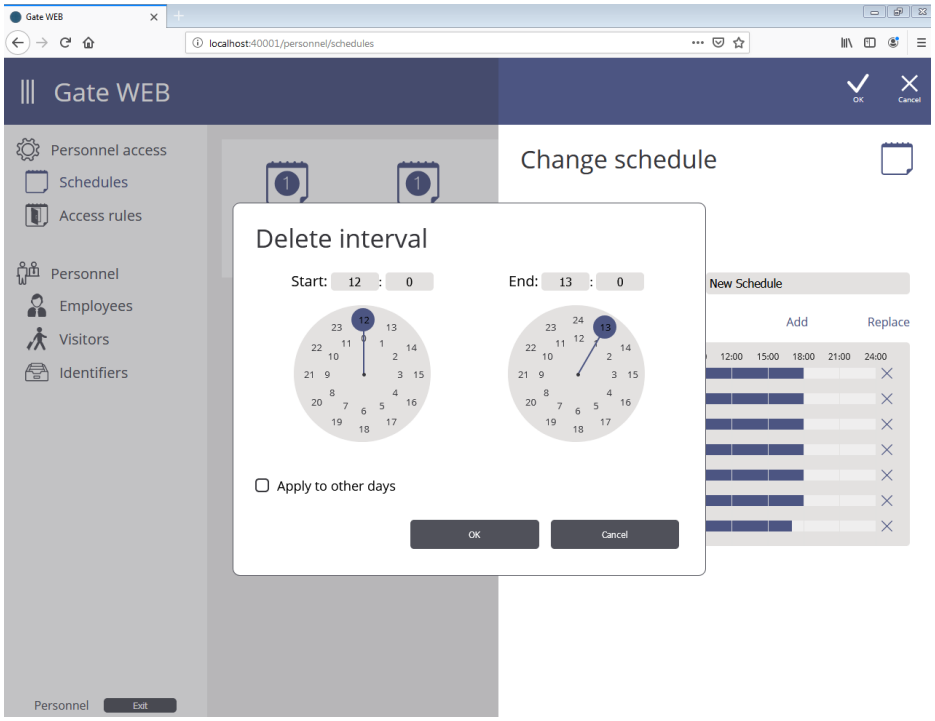


Time zone will expand on all days below if ‘Apply to other days’ option checked.

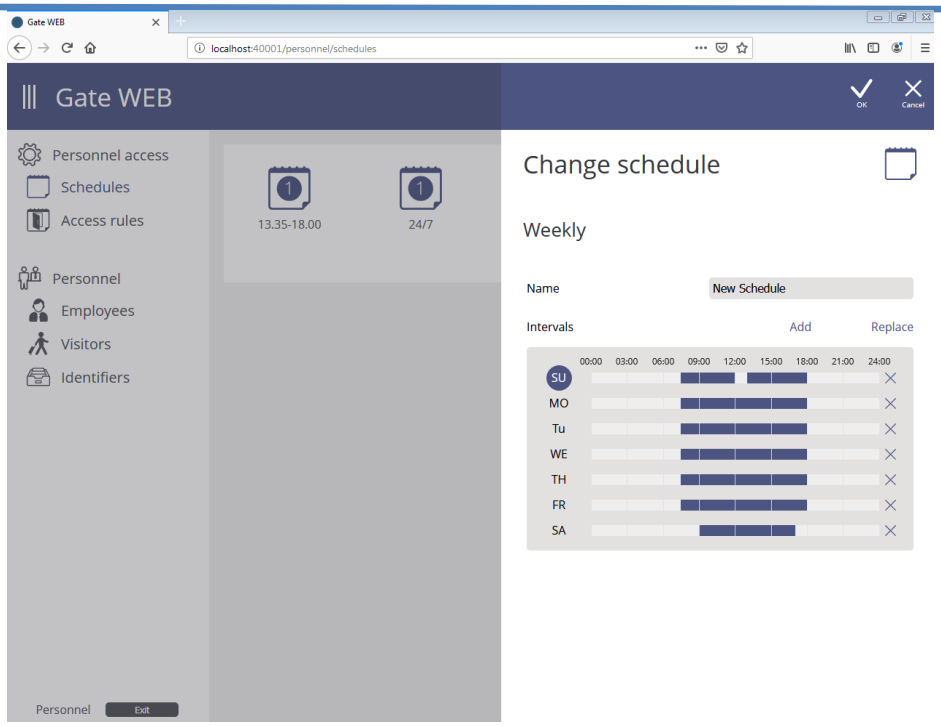


Press ‘X’ symbol in the row to remove correspondent time zone and mark ‘Start’ and ‘End’ values of time zone to be removed.





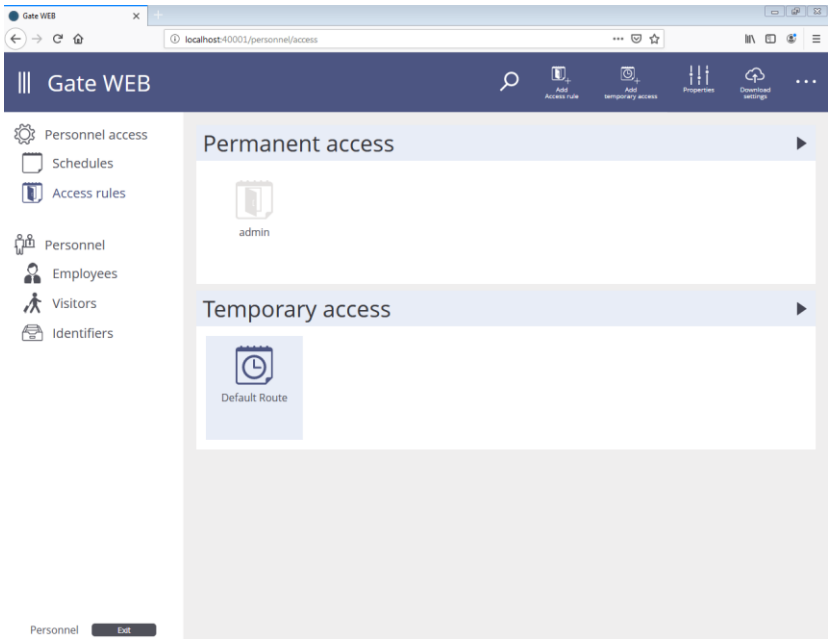
Time zone remove will expand on all days below if ‘Apply to other days’ option checked.


Gate WEB
localhost:40001/personnel/schedules
Gate WEB
OK
Cancel
Personnel access
Schedules
Access rules
Personnel
Employees
Visitors
Identifiers
13.35-18.00
24/7
Change schedule
Weekly
Name
New Schedule
Intervals
Add
Replace
00:00 03:00 06:00 09:00 12:00 15:00 18:00 21:00 24:00
SU
MO
Tu
WE
TH
FR
SA
Personnel
Exit

Personnel access: Access Rules

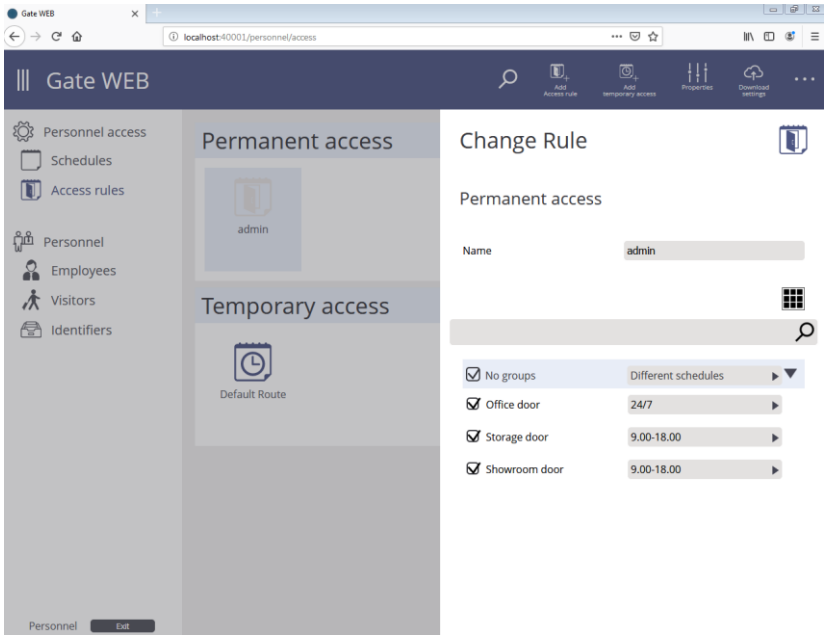
Access Rules is the rules which panel uses to define the doors and time to grant access to the card holder. Access Rules may be assigned to employee or to the department and derived by employee from the department.

There are two types of Access Rules: permanent for personnel and temporary for visitors.



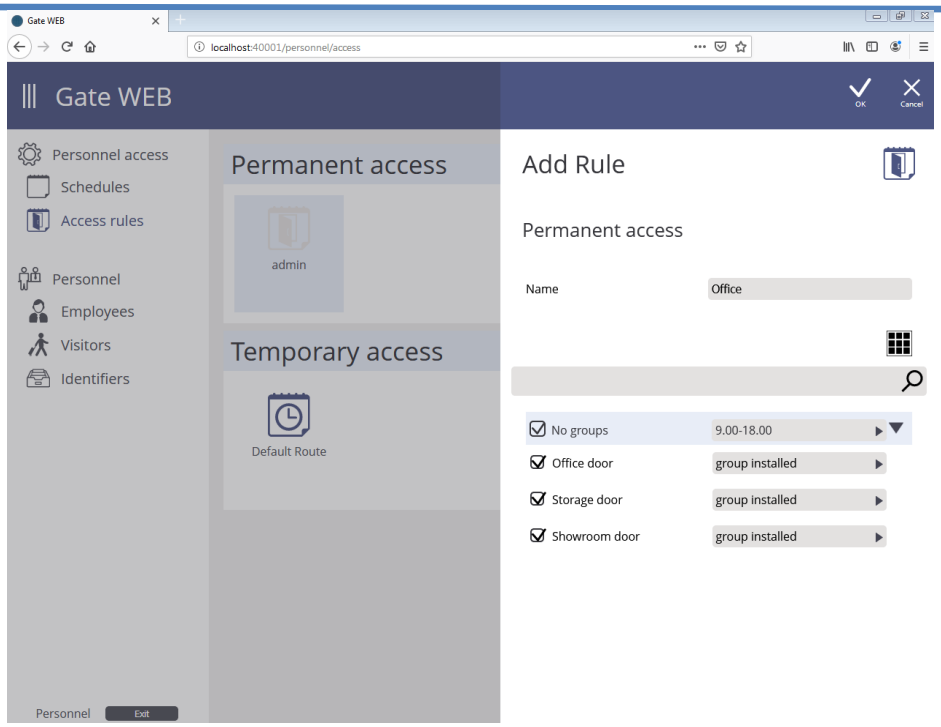
Adding Access Rules for personnel

Select ‘Access Rules’ and press ‘Add Access rule’ to add permanent access rule for employees.

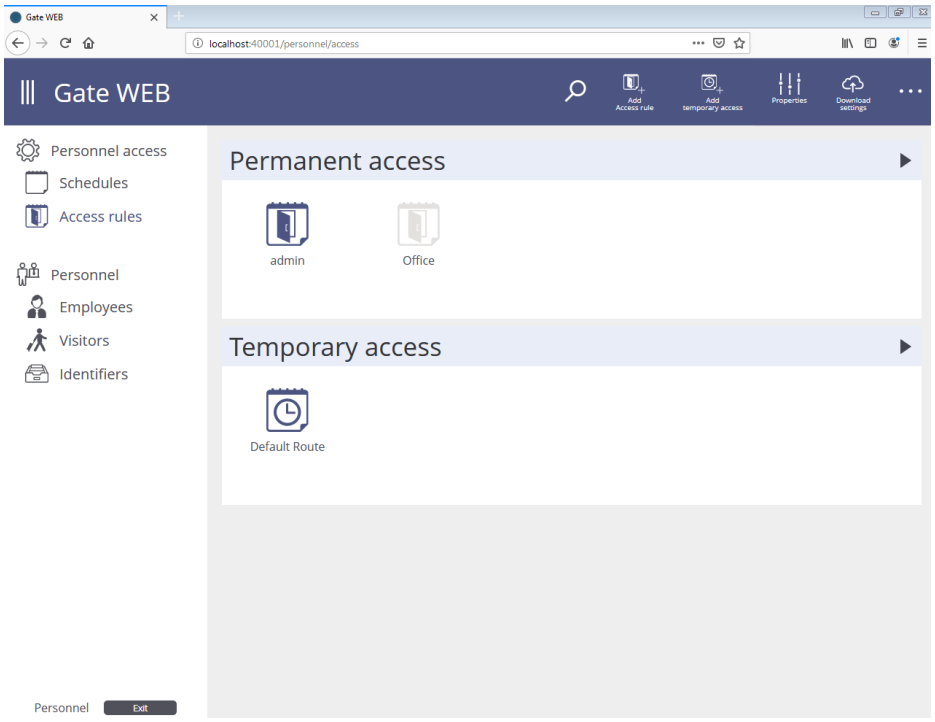


Type rule Name in edit field, select doors and schedule in window appeared.

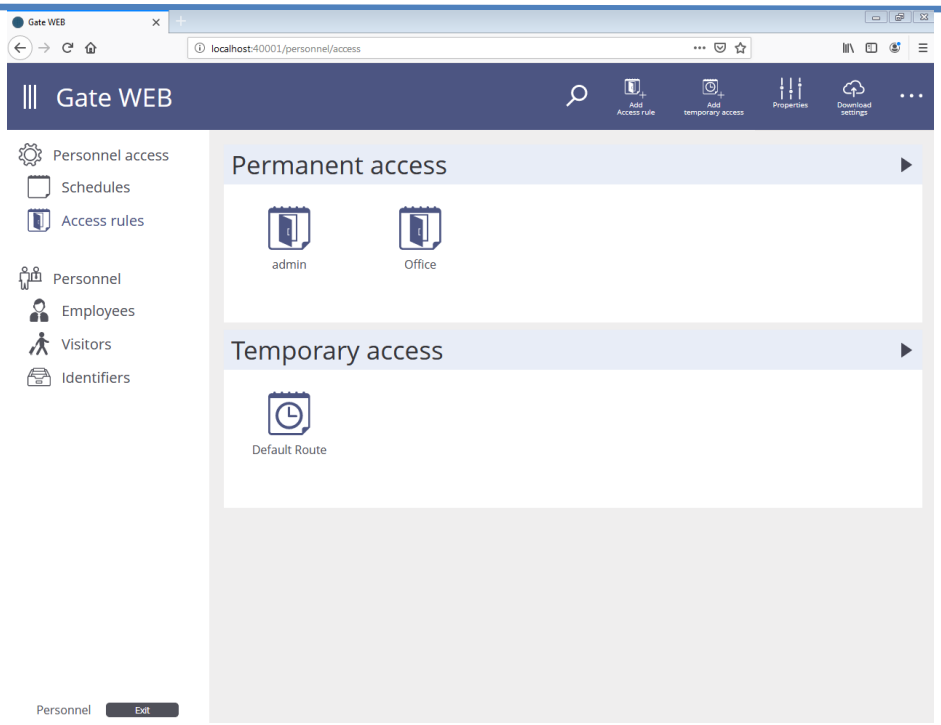
You may select group, if doors combined into groups.



Access rule will be added. Access rule icon colored in gray if it doesn't assigned to any employee and it is possible to remove it.

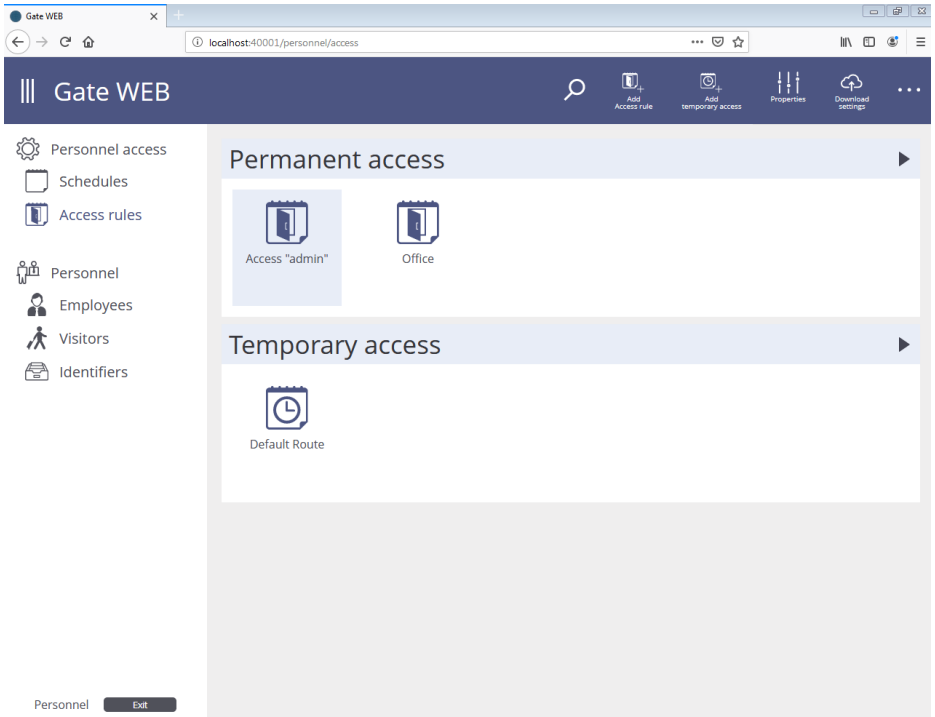


Access rule icon colored in if it is assigned to one employee or department at least and it is impossible remove it.



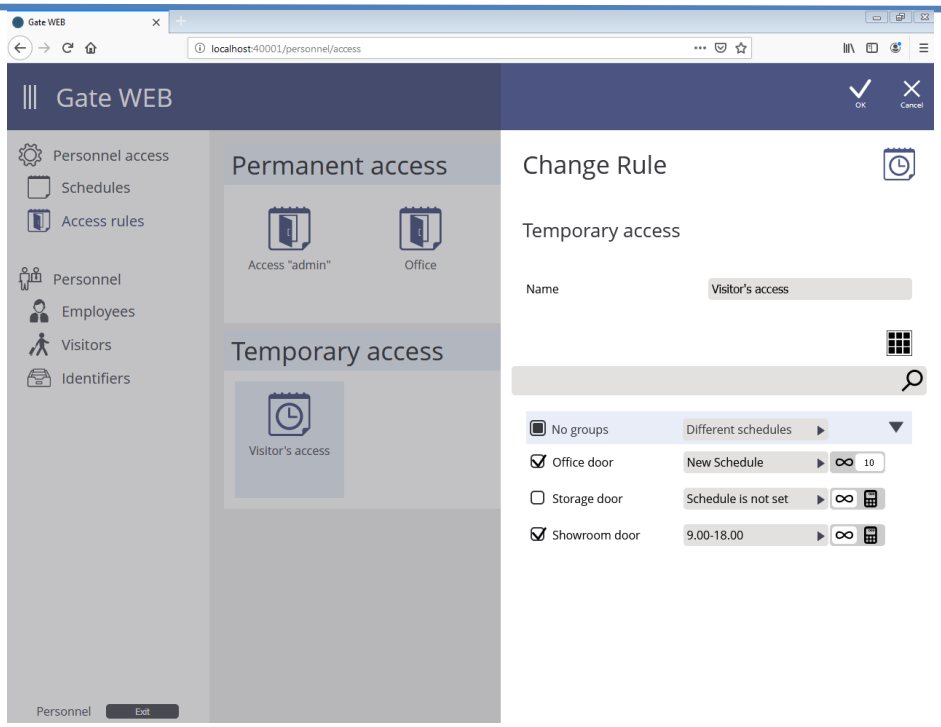
Adding Access Rules for visitors

Press 'Add temporary access' in Access rules tab to add temporary access rule for visitors.

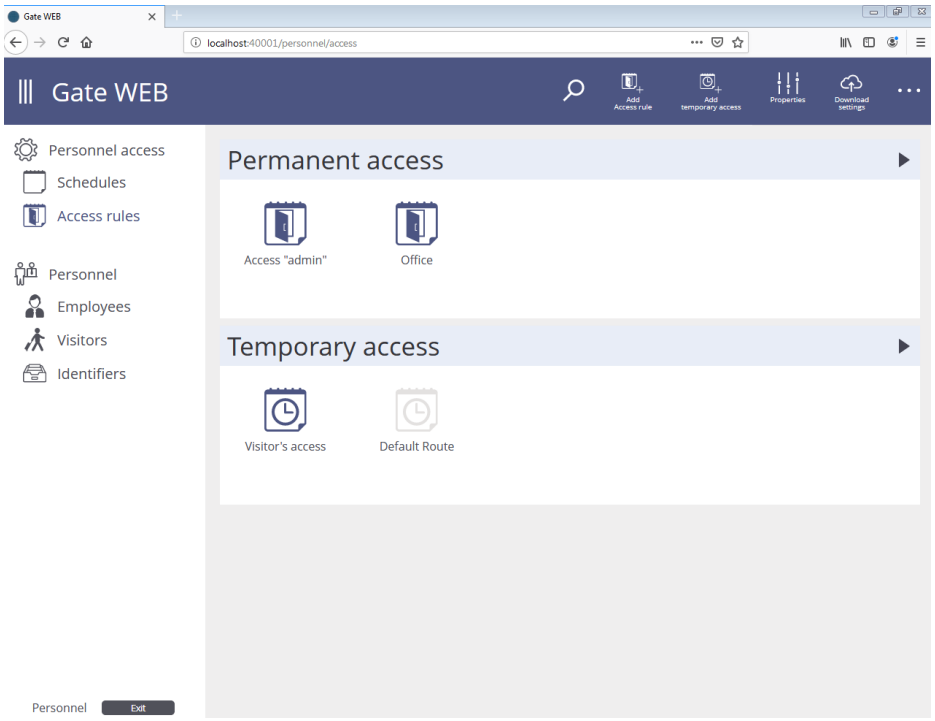


Type rule Name in edit field, select □ allowed doors and schedule in window appeared. Set the limit of visits for each door or select unlimited access ∞.

It is possible to assign rules to the groups of doors.

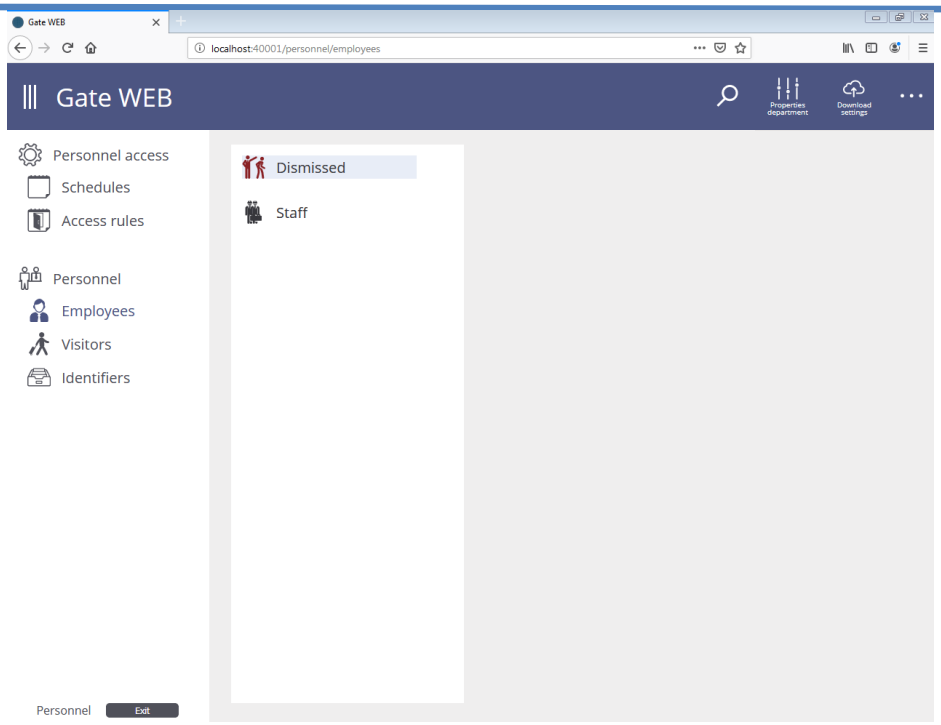


Access rule will be created. Access rule will be added. Access rule icon colored in gray if it doesn't assigned to any employee and it is possible to remove it. Access rule icon colored in cyan if it is assigned to one employee or department at least and it is impossible remove it.

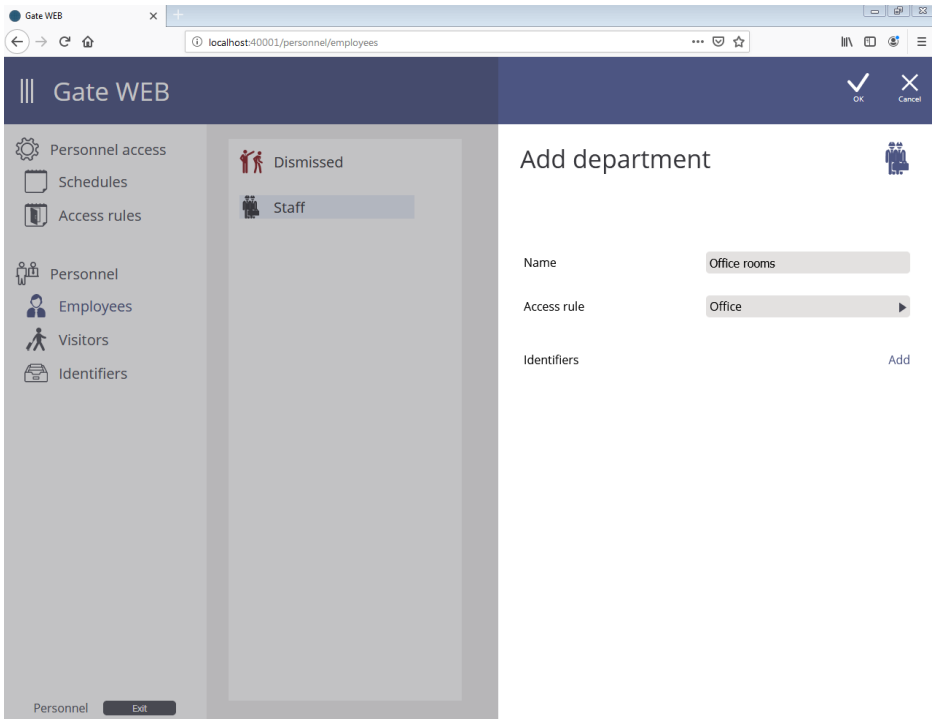


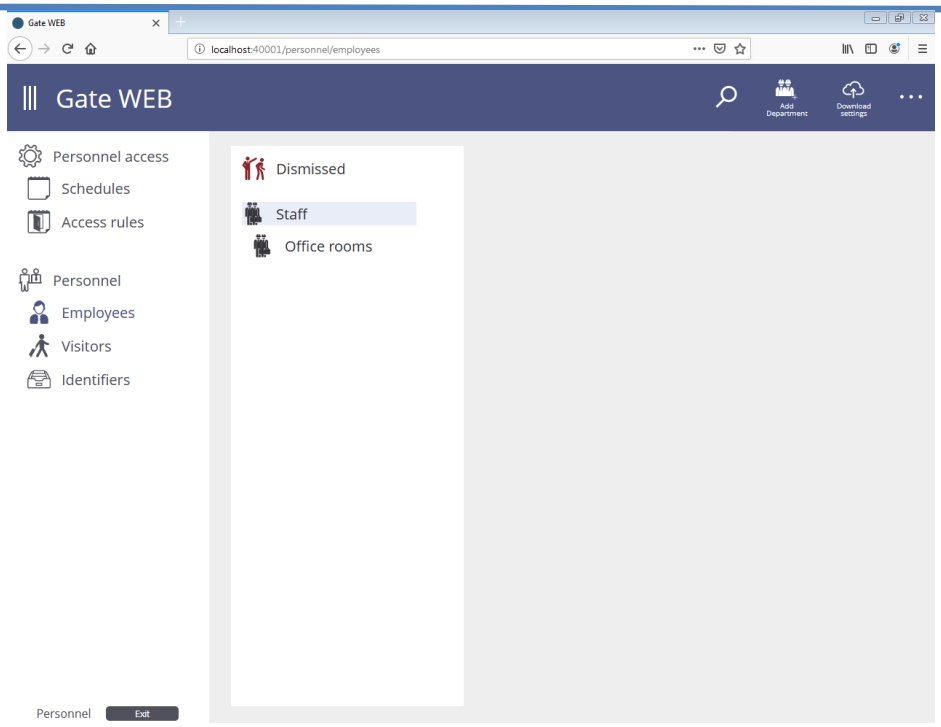
Personnel: departments

Select 'Employees' to add highest level department. Then select 'Staff' and press 'Add department' button.

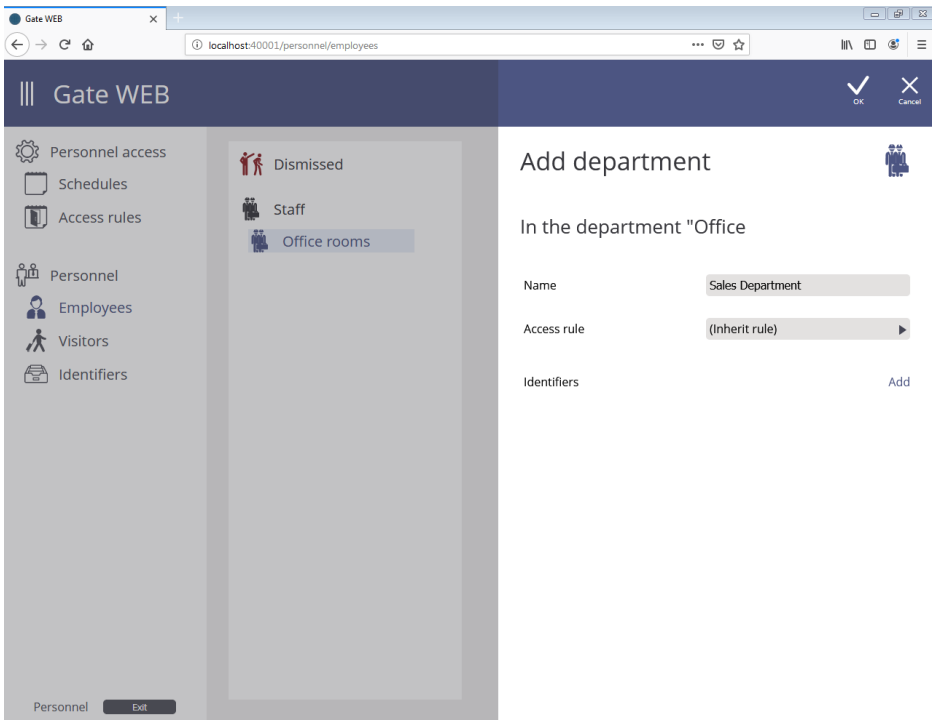


Type department name and select access rule to be used in group access settings in window displayed.

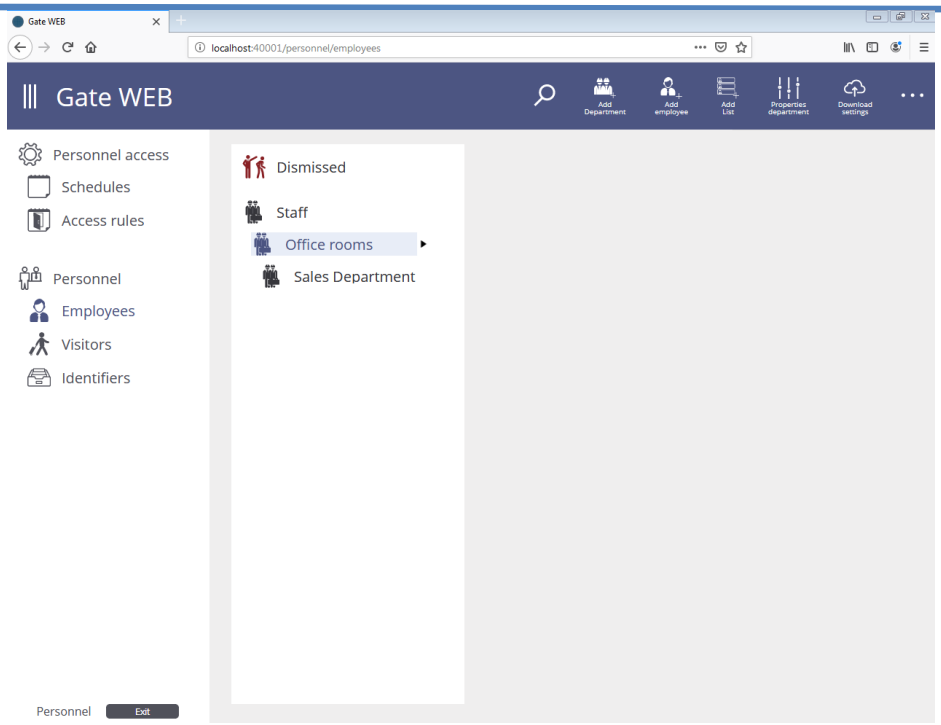




Select existing department in the departments tress and press ‘Add department’ to add sub department.

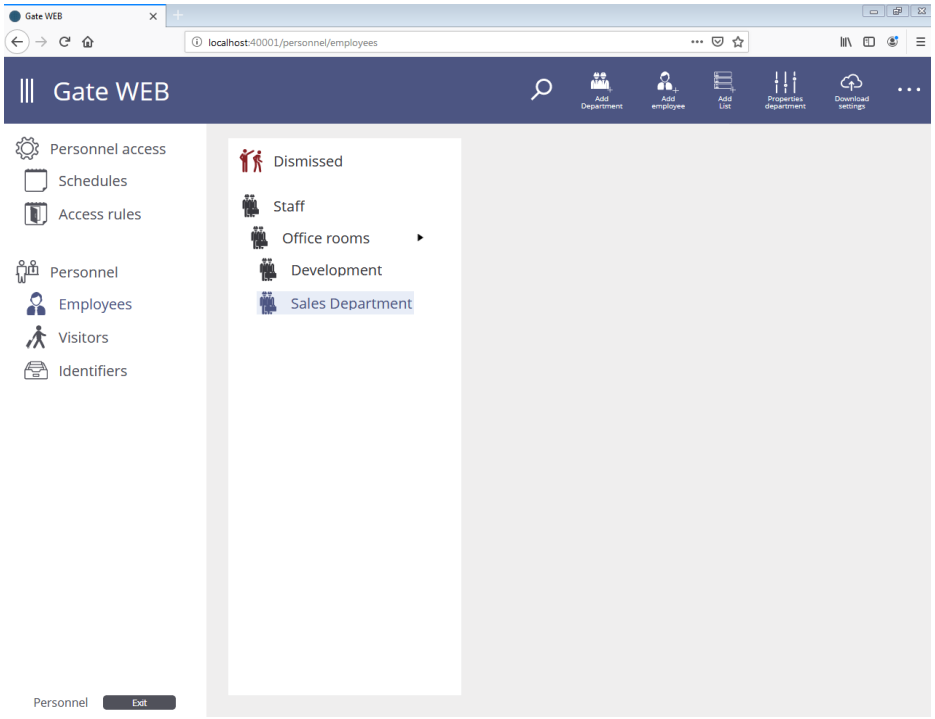


Sub department added.

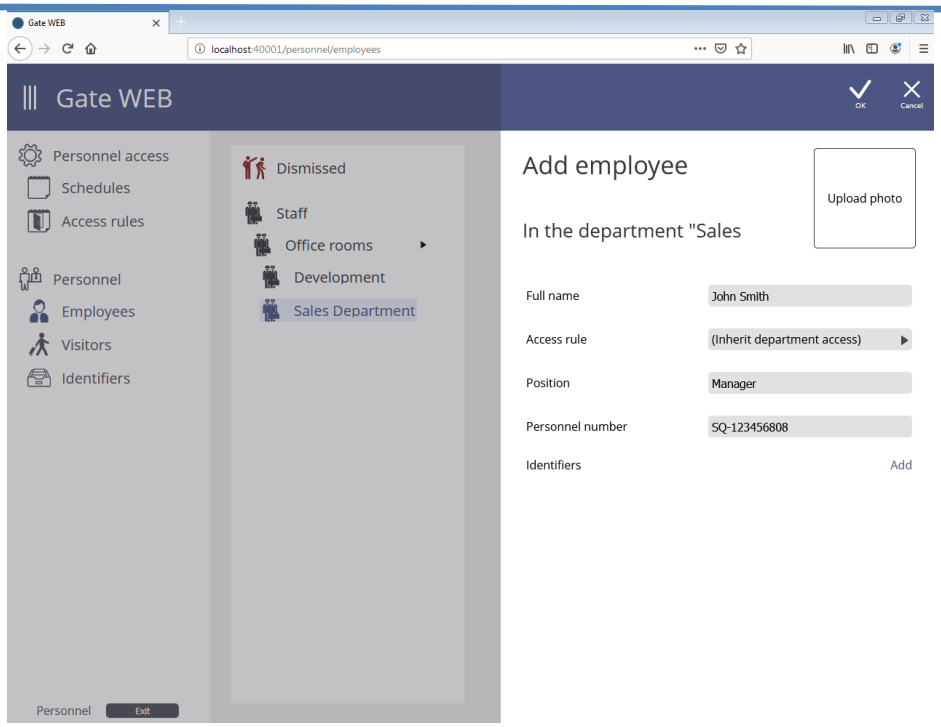


Personnel: employees

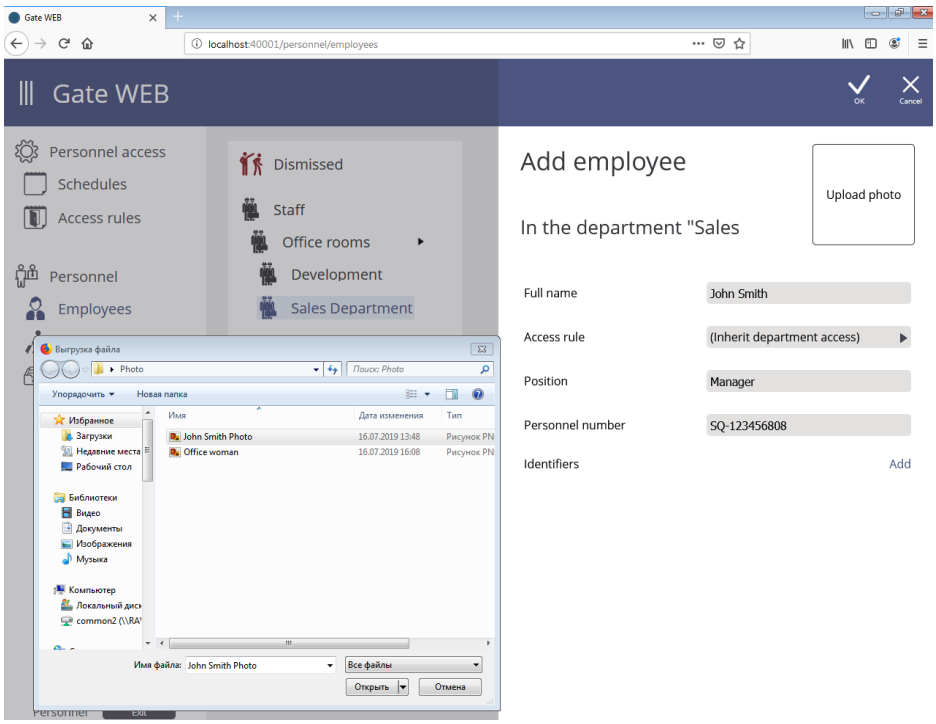
Select existing department in department tree and press ‘Add employee’ to add employee.



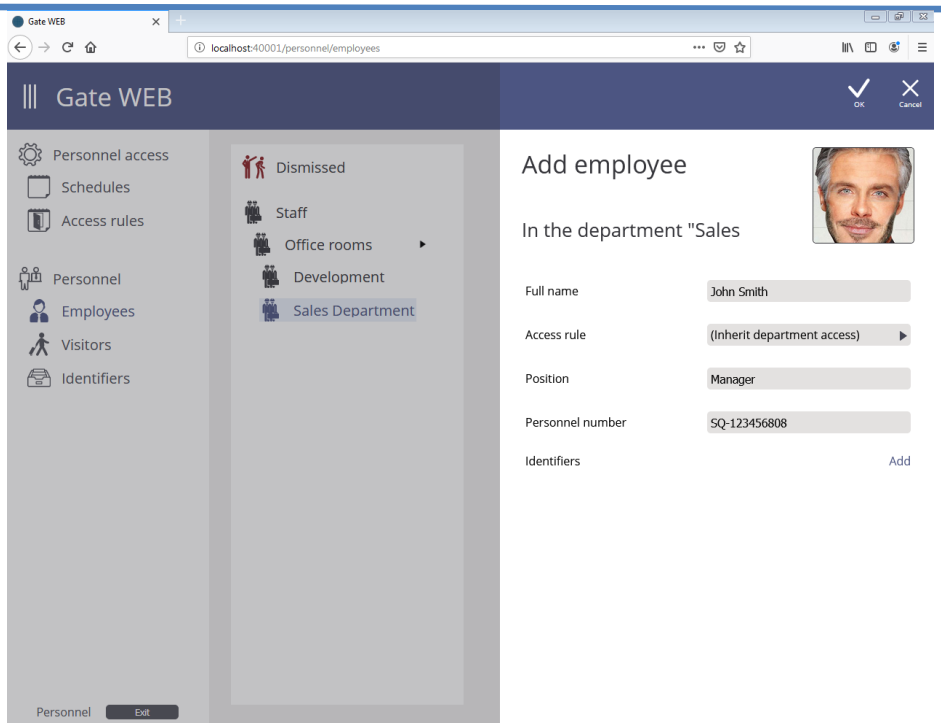
Type employee name and set his personal access rule or mark that he inherits the department access rule in window displayed.



Click photography placeholder and select employee photo file in dialog window displayed to add employee photography.



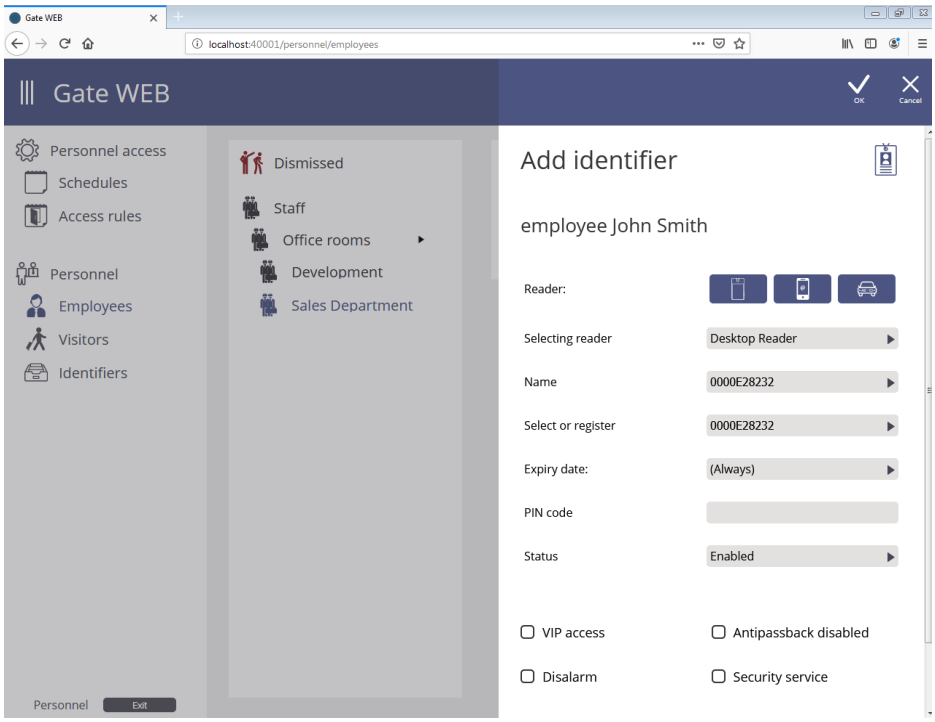
Press ‘Add’ button to give ID to the employee.



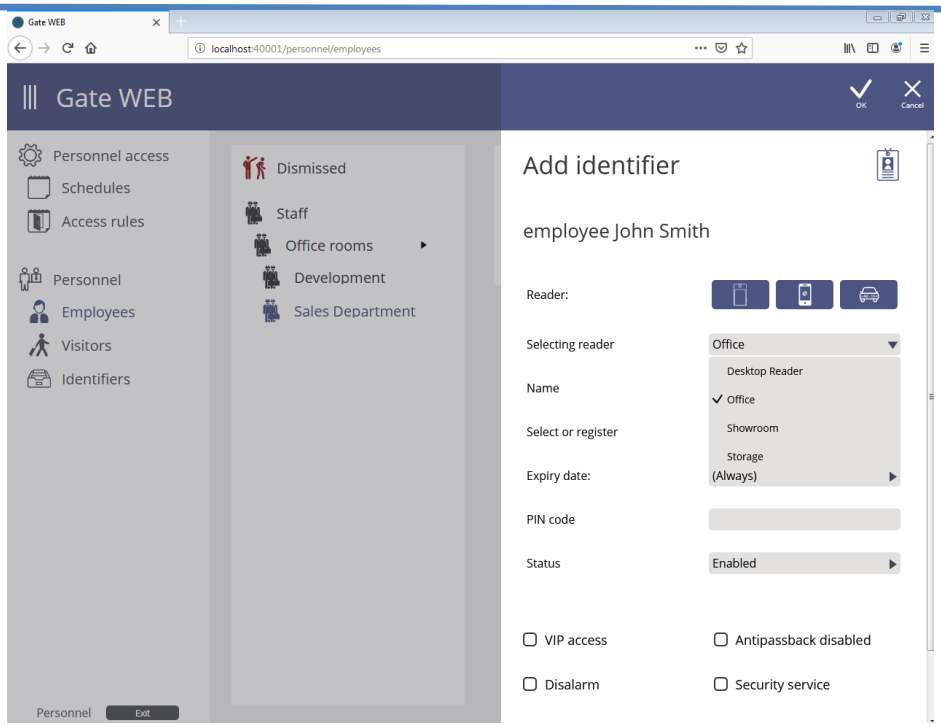
ID enrollment device in window displayed.

Available enrollment ways:

1. With desktop reader for RF ID cards:



2. From the any reader in system



Additional options shall be set after ID enrollment:

PIN – Personal Identification number associated with ID. PIN Must consist of six to ten decimal digits.

Some rider equipped with keypad. System provides possibility to use RF ID and PIN for access. Reader changes LED blinking after card pass if PIN required. User must enter PIN after RF ID pass in this case during the time set in panel options.User must enter # button on the keypad or wait for the PIN entry delay. Panel grants access if valid PIN entered. Otherwise panel will deny access, log 'Invalid PIN entered' event and sound warning signal by reader buzzer.

Expiry date – ID expiry date

ID is valid until the date entered.For example, if the expiry date is January 1, 2020, then the last day when access granted will be December 31, 2019.

Status – ID status. This option may have values: Valid, Invalid, Blocked, Lost or Damaged.

Access granted to Valid IDs only. ID is Valid if. Only Valid IDs shall be issued to employees with right to access premises.

Access not granted to the invalid IDs and those IDs are not loaded into the panel. That's why panel logs 'Unknown card' event on invalid ID pass. Usually this status set for cards enrolled to the system database but not issued to employee.

Reader emits warning beep and panel logs 'Blocked card found' event when ID with 'Blocked' status passed to the reader. Usually this status assigned to IDs belong to employees who have ID and rights for access, but their attendance not expected.

System processed IDs with ‘Damaged’ status in the same way as ‘Invalid’ ID, but has different sense for system operators.

Assign ‘Lost’ status to the lost cards. It helps to find them because when those cards passed to the reader, door is blocked and panel switches on alarm output.

It is impossible to change ID attributes (Alarm Cancel, Guard, VIP, AntiPassBack) if ID is not valid (Invalid, Blocked, Lost or Damaged).

Attributes. Alarm Cancel – ID will have right to cancel door alarm if ‘Alarm cancel’ attribute checked.

Panel logs ‘Alarm state end’ event and switches door into normal state when card with ‘Alarm cancel’ attribute passed. Panel logs ‘Access denied. Door in alarm.’ event when card without ‘Alarm cancel’ attribute passed.

Attributes. Guard card – ID with ‘Guard’ attribute allows to enter the blocked door.

Door is blocked if it is necessary to deny access for all employees and visitors, except the guard. Door is blocked with corresponding panel input violation or by the command from system server.

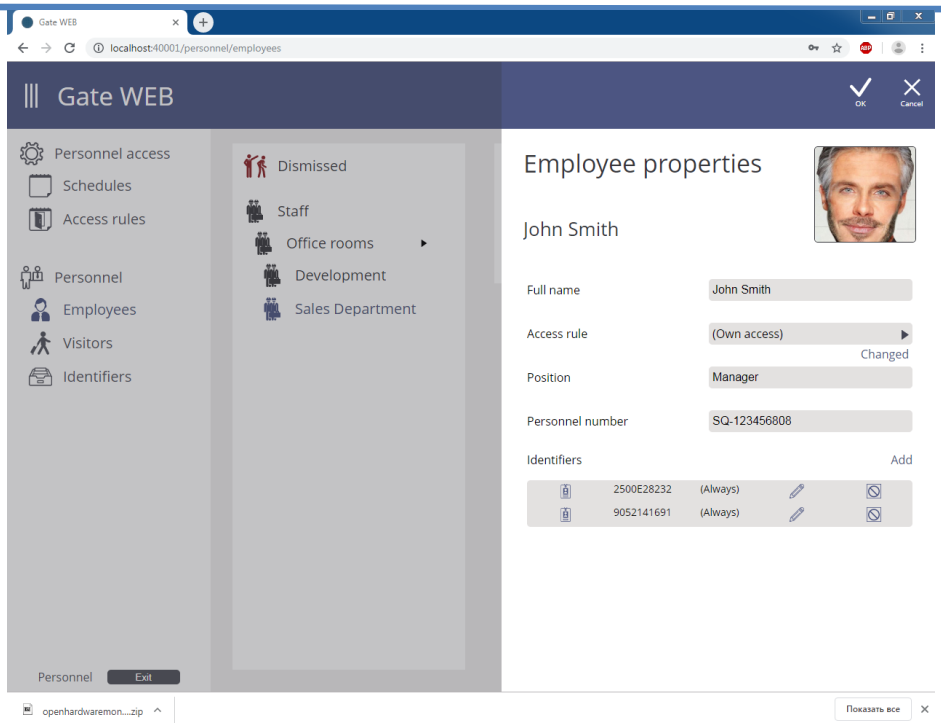
Reader emits warning signal on ID without ‘Guard’ attribute pass if door is blocked. Panel logs ‘Access denied. Door BLOCKED’. Panel grants access and logs ‘Access granted. BLOCKED state’ on valid ‘Guard’ ID pass.

Attributes. VIP – Person having ID with ‘VIP’ attribute may open any door at any time, except the doors in ‘Blocked’ state.

Schedule, antipassback attribute and use time limit does not affect the operation of this ID. ID with this attribute may have PIN.

Panel logs ‘Access denied. Blocked state’ event, denies access and reader emits warning signal when VIP ID passed to the reader of the blocked door.

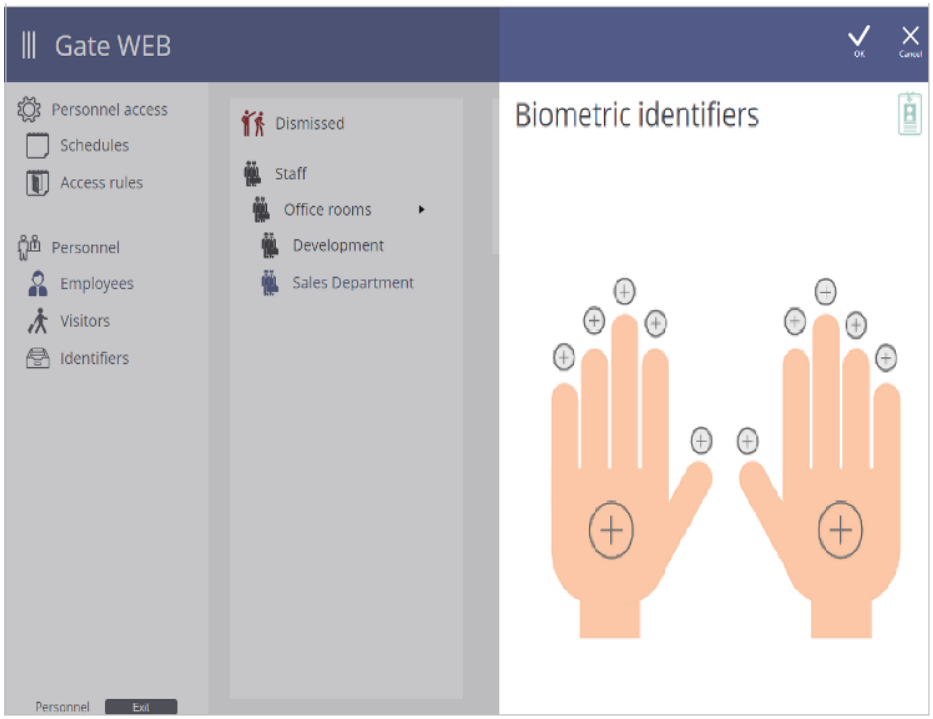
Attributes. AntiPassBack OFF– Employee with ID with this attribute passes doors without antipassback registration. Access is granted independently from the side of door and registered employee position.



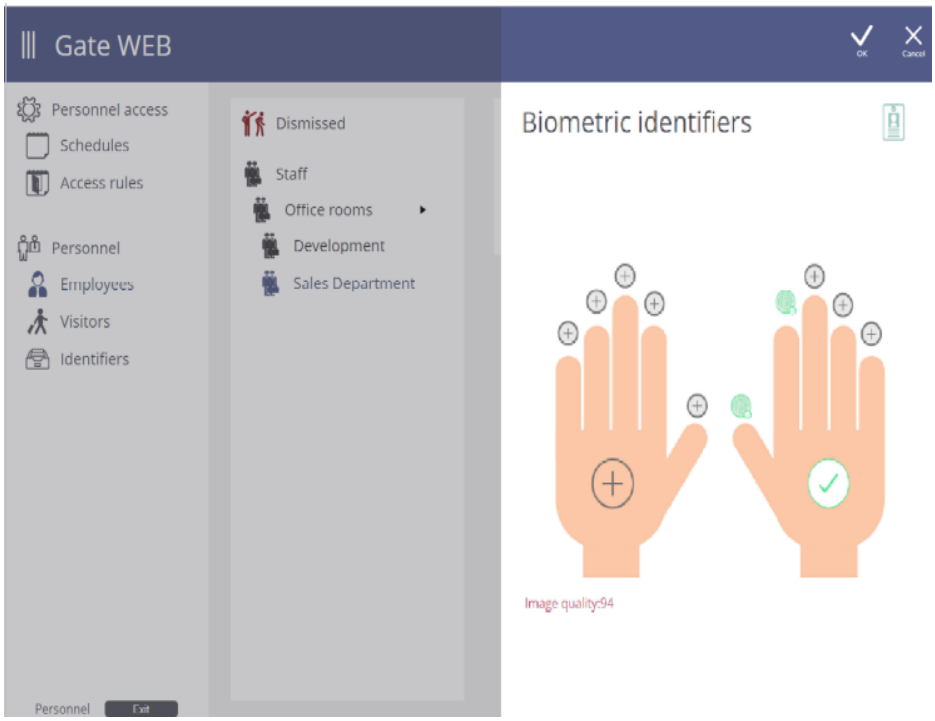
Biometric ID enrollment becomes available if there are biometric readers connected to the system.

Attention!!! Employee must have at least one normal (RF or mobile) ID for biometric ID enrollment.

Press ‘Biometric Identifiers’ and select in the window displayed ID type – fingerprint or palm vein will be enrolled.



Enroll biometric ID following enrollment master instructions.



Press ‘OK ’ to save changes.

Personnel. Adding employees’ group

Use employees’ list adding to add multiple employees quickly.

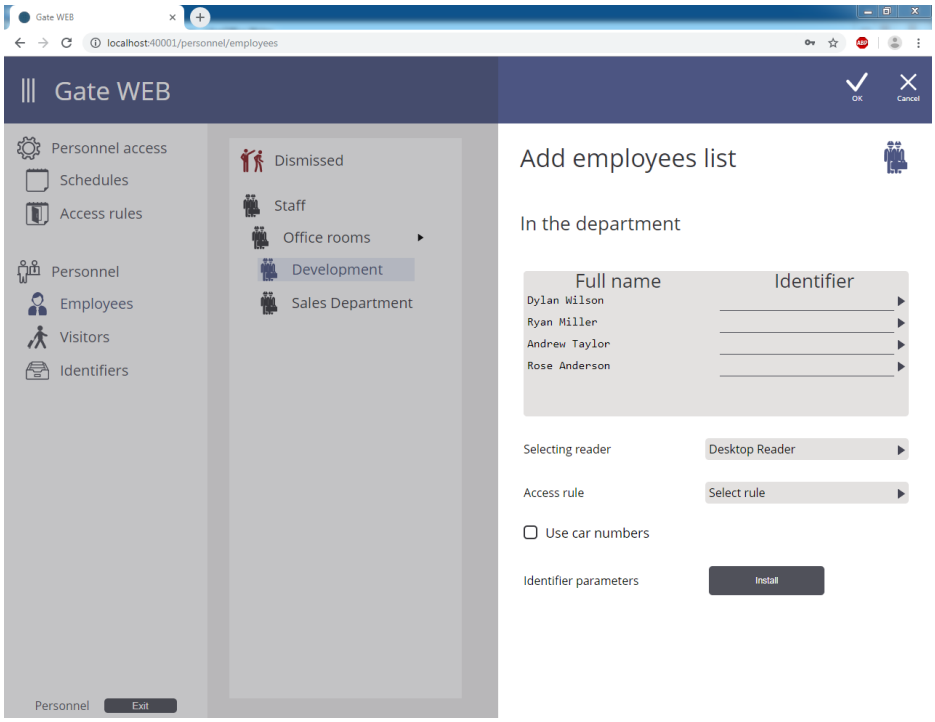
Create file with employees’ names listed in the column as below:

Dylan Wilson

Ryan Miller

Andrew Taylor
Rose Anderson

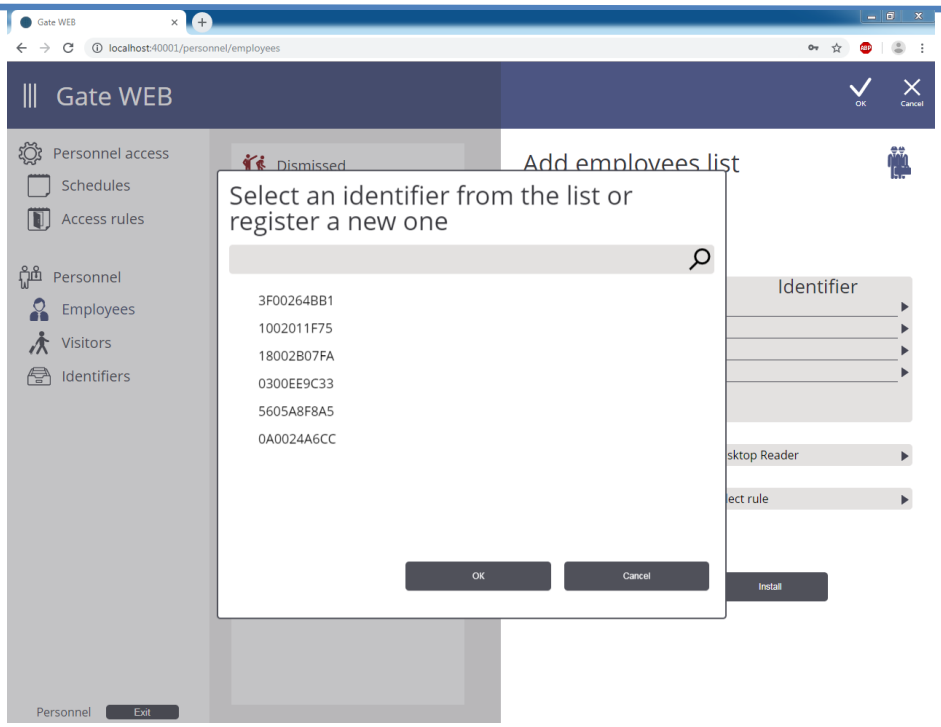
Press ‘Add list’ button in the main menu and copy the list from the file into the window displayed:



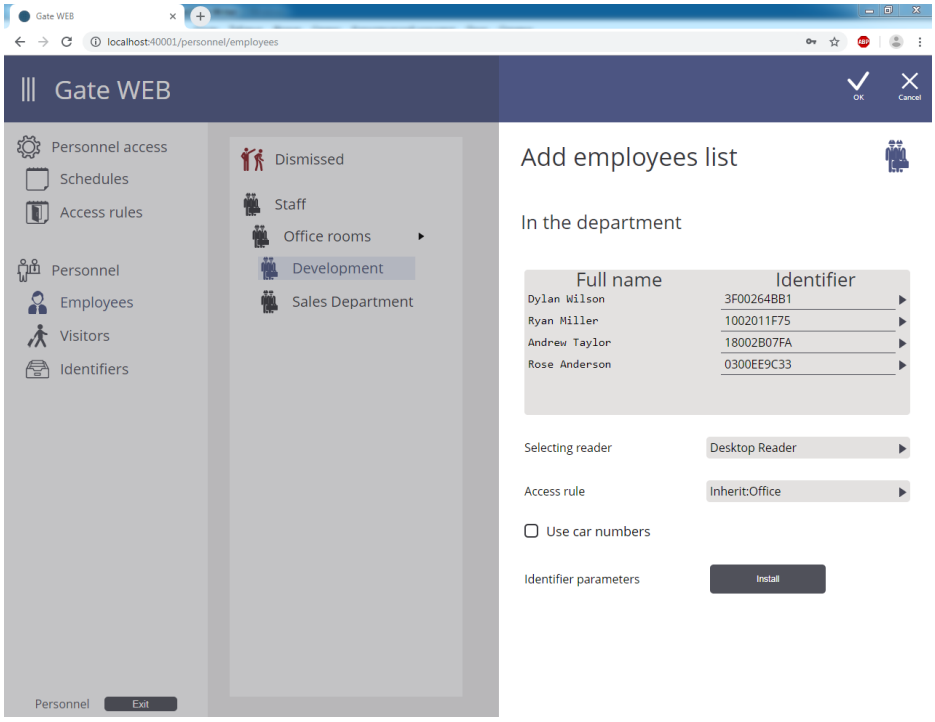
Then enroll IDs for each employee from desktop reader or any other reader of the system.

Enrollment reader selected in ‘Selecting reader ’ list.

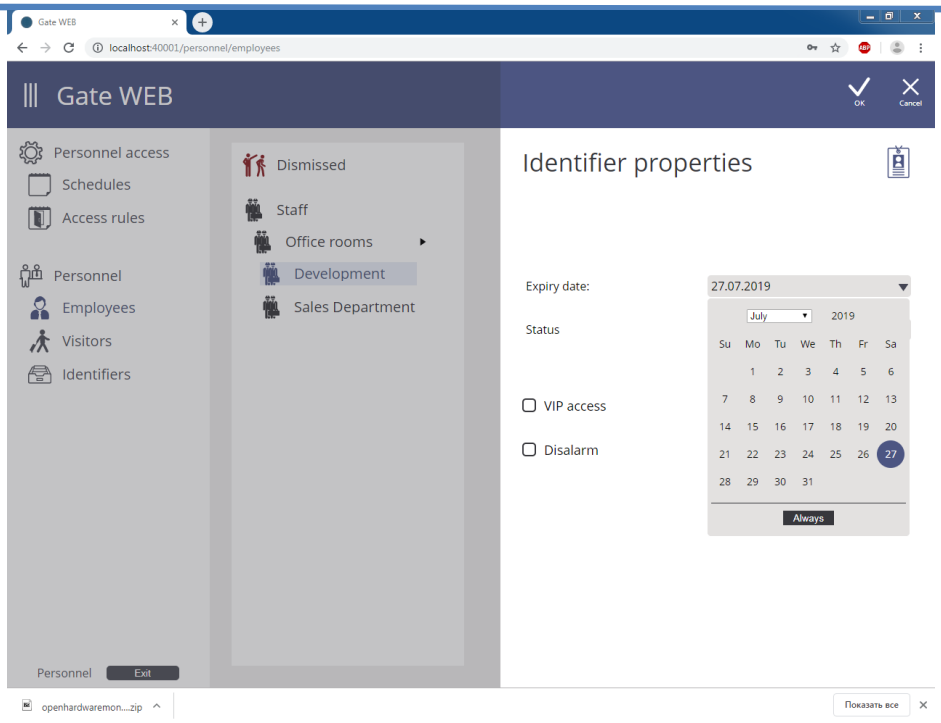
ID selection or enrollment window will display on click on ‘Identifier’ field. Select or enroll Identifier and press ‘OK’ button.



Assign access rules to all employees after IDs enrollment in ‘Access rule’ field.

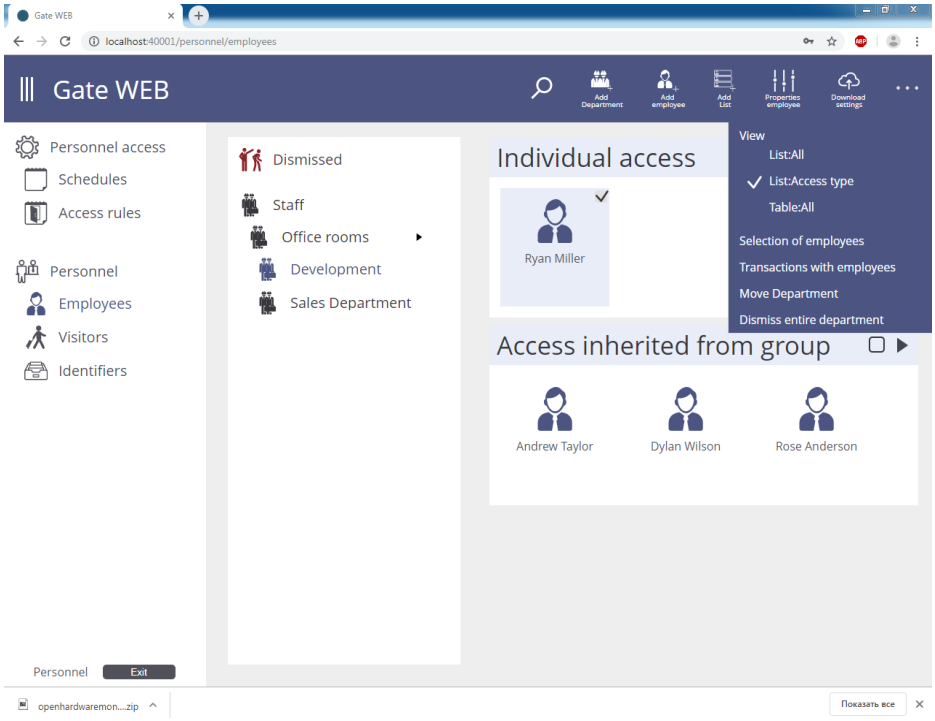


IDs’ options and attributes are set in the same way. Press ‘Set’ in window displayed to do:



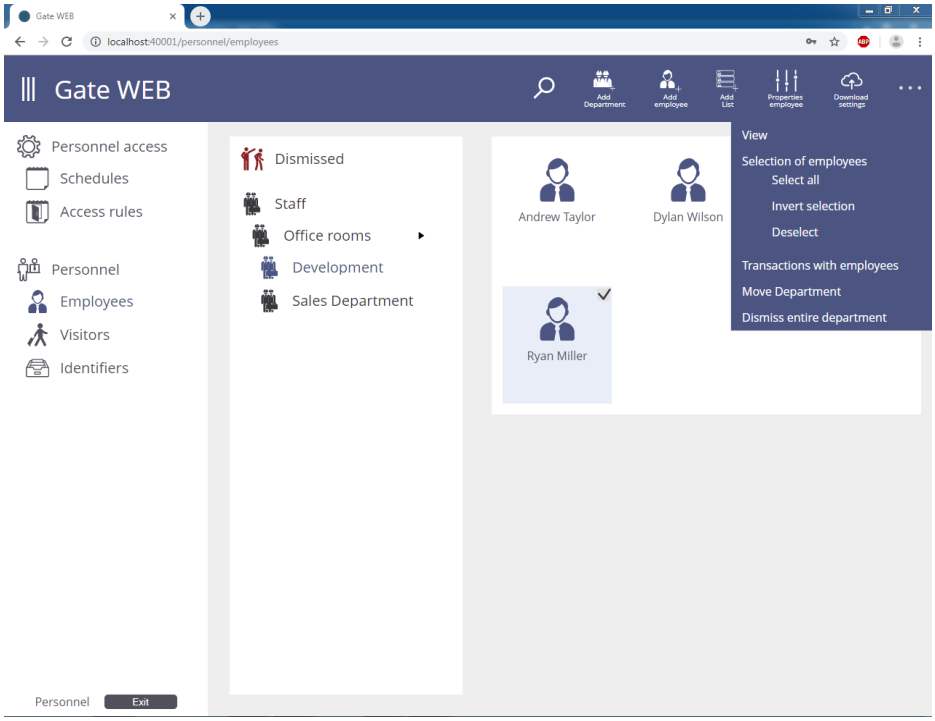
Personnel: Defining employees with individual access

Select ‘View’ then ‘List: Access type’ in main menu to define what employees will have personal access or inherit groups. Following will display:



Personnel: employee selection

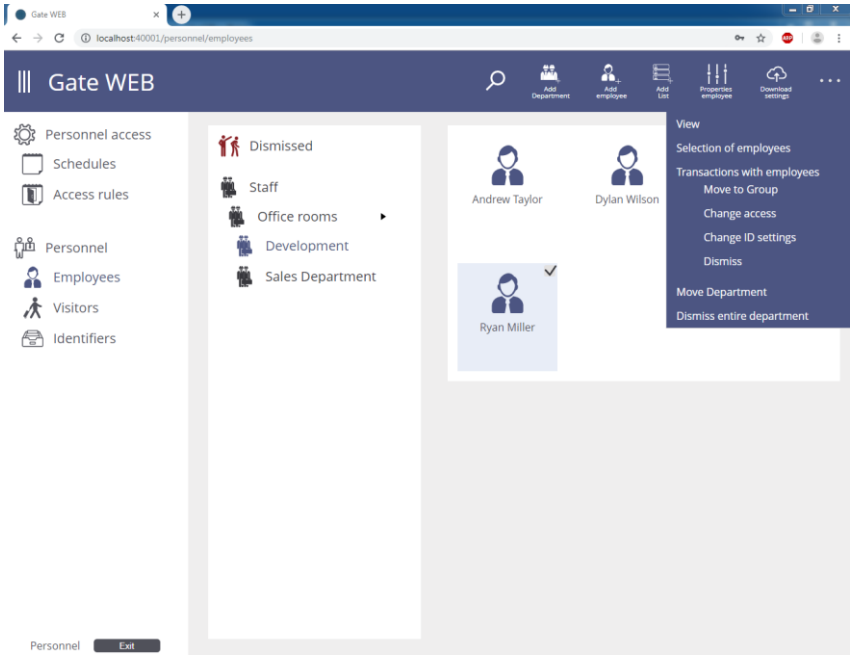
Select ‘Selection of employees’ in main menu and choose desired action ‘Select all’, ‘Invert selection’ or ‘to change employee selection:



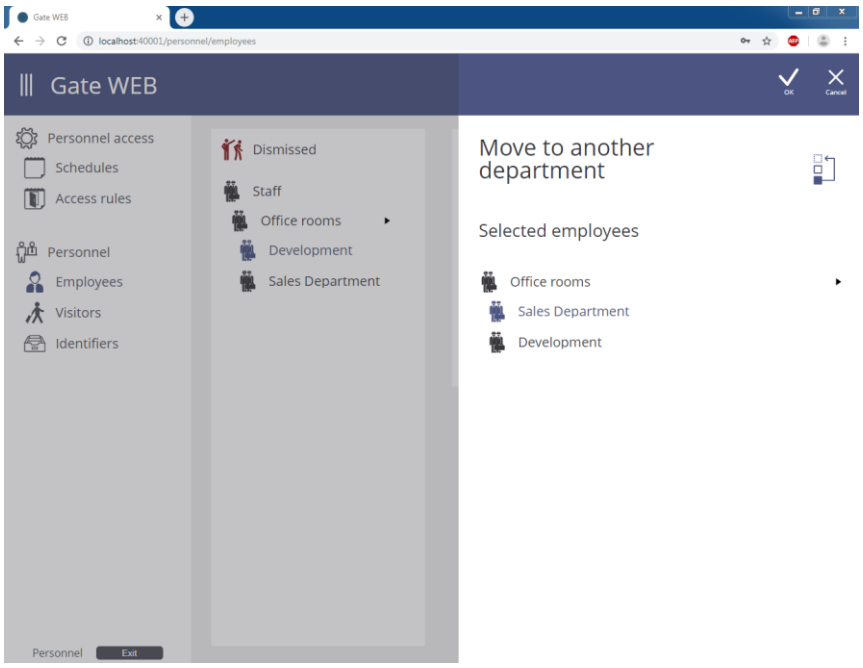
Personnel: Group operations with employees

Actions as follows available with employees:

- Moving into the another group or department
- Access options change
- IDs options change
- Dismission

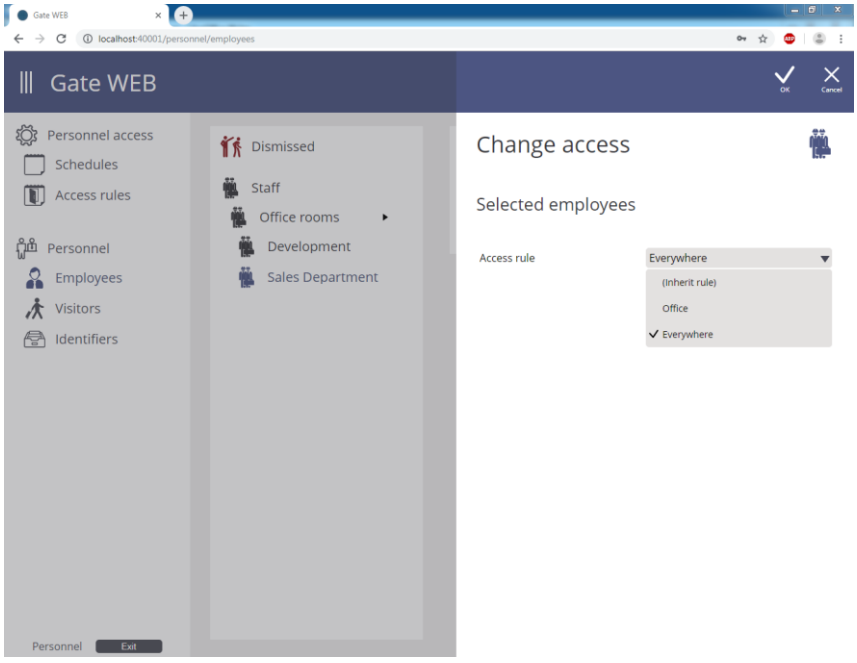


Check employees and select ‘Transactions with employees’ in main menu and choose ‘Move to group’ item to move employees into another department. Select desired department in the window displayed and press ‘OK’.

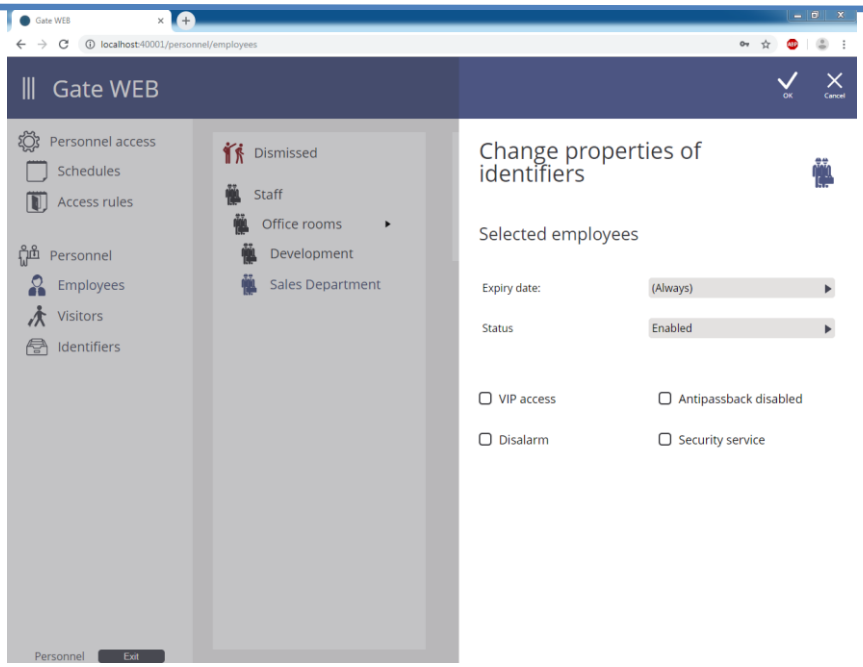


Employees who inherit department access will inherit access rule of the department where they were moved.

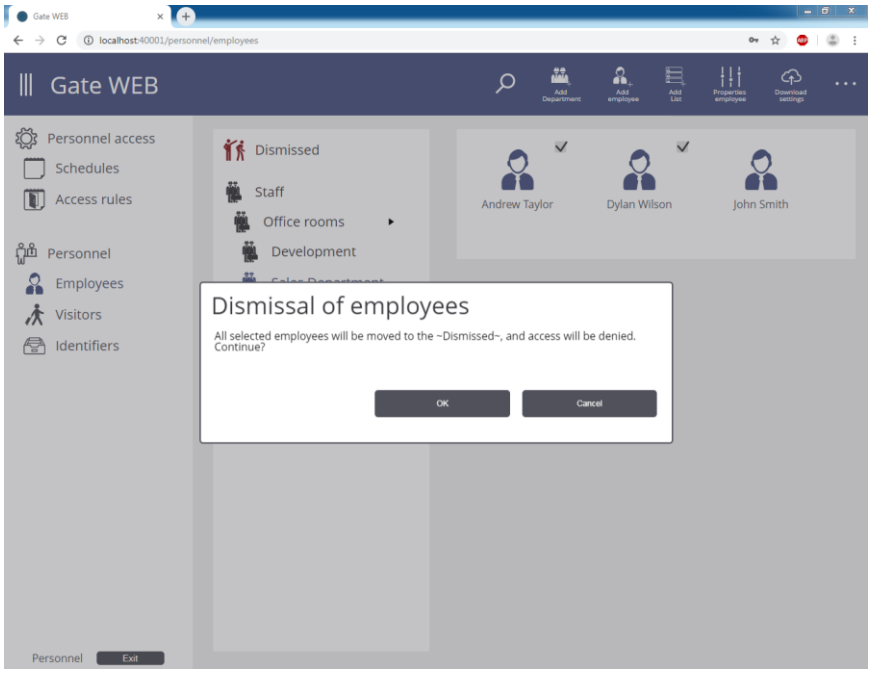
Check employees, select ‘Transactions with employees’ in main menu and choose ‘Change access’ to change employees access rules options. Select new access rule to be assigned to employees and press ‘OK’ in the window appeared.



Check IDs, select ‘Transactions with employees’ in main menu and choose ‘Change IDs options’ to change employees’ IDs options. Select new IDs options to be assigned to employees and press ‘OK’ in the window appeared.



Check ☐ employees, select ‘Transactions with employees’ in main menu and choose ‘Dismiss’ to assign ‘Dismissed’ status to employees. Confirm dismission in the window displayed.

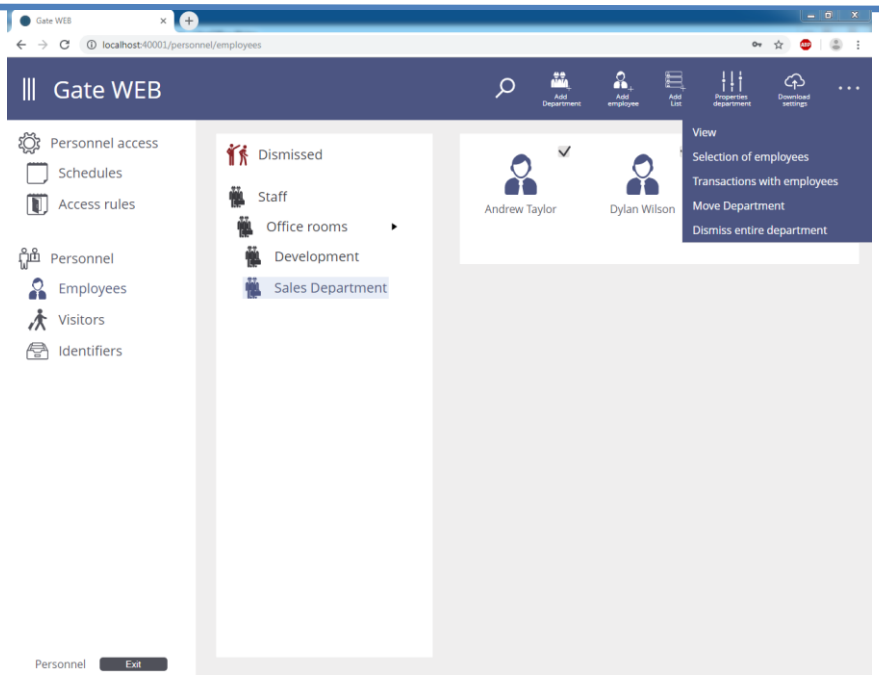


Employees’ records moved into the ‘Dismissed’ folder and their access stopped. All other employees data preserved.

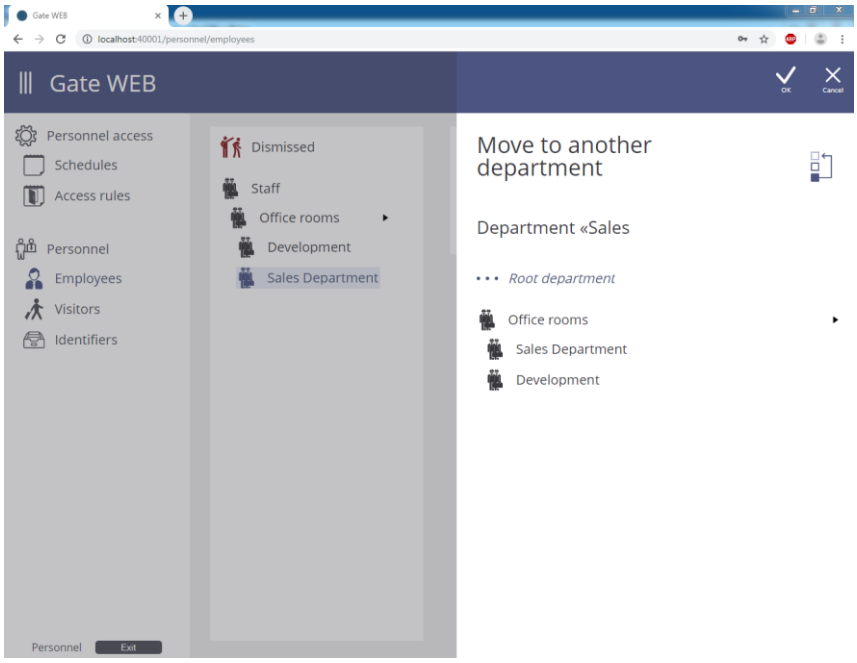
Personnel: Actions with departments

Actions with departments available:

- Moving department into another group/department
- Dismission of the whole department

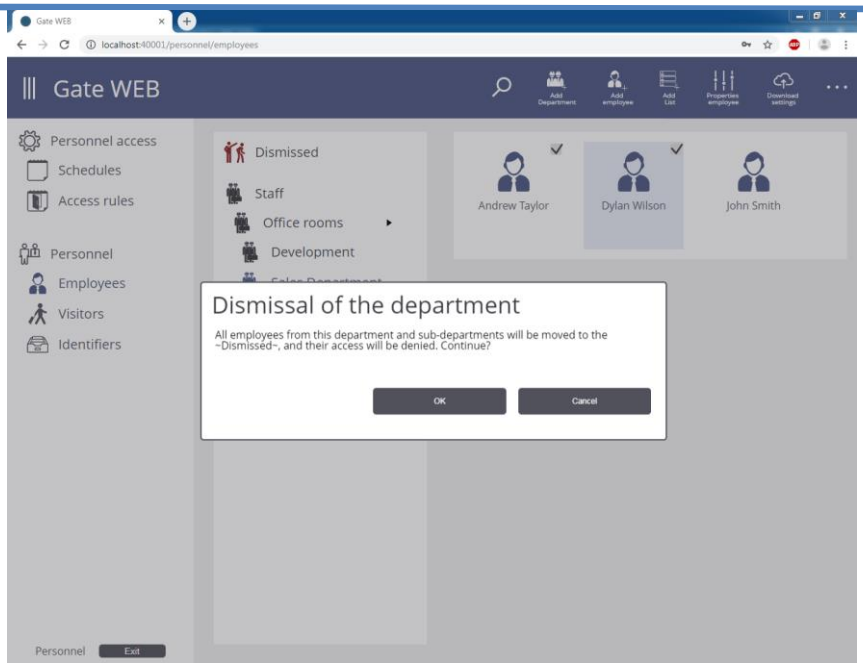


Select ‘Operations with departments’ in main menu and choose ‘Move Department’ item to move department into another department. Select the department into which the current department will move and press ‘OK’.



Employees who inherit department access will inherit access rule of the department where they were moved.

Select ‘Transactions with departments’ in main menu and choose ‘Dismiss entire department’ to assign ‘Dismissed’ status to all employees of department. Confirm dismission in the window displayed.

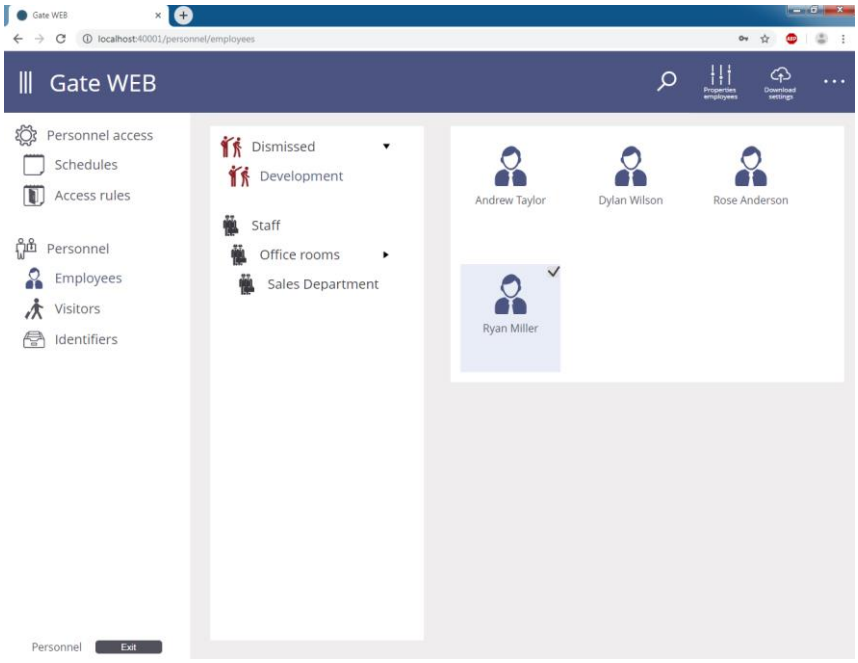


Department employees' records moved into the 'Dismissed' folder and their access stopped. All other employees' data preserved.

Personnel: 'Dismissed' folder

There is 'Dismissed' folder for safe storage of data of the dismissed employees and departments and for future deletion.

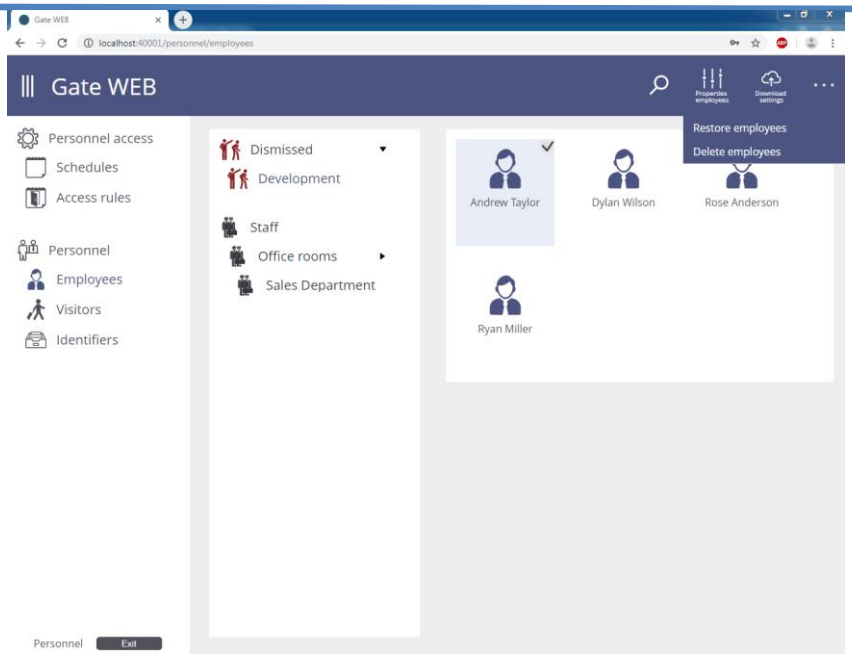
Employees' data (access rules, IDs e.t.c) preserved after move into this folder but not loaded into the panels.



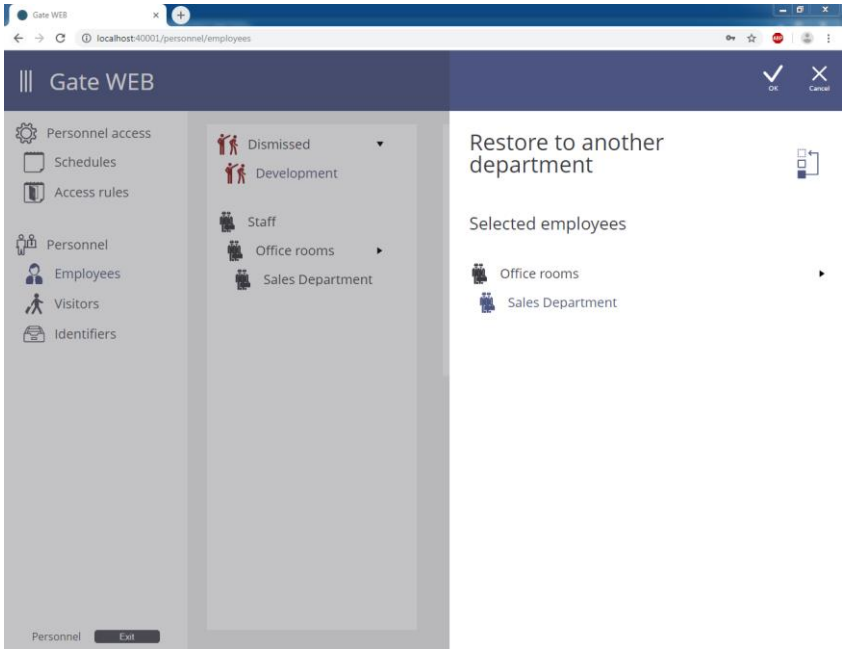
Actions with employees

Actions with employees available:

- Restoring into the group/department
- Deletion

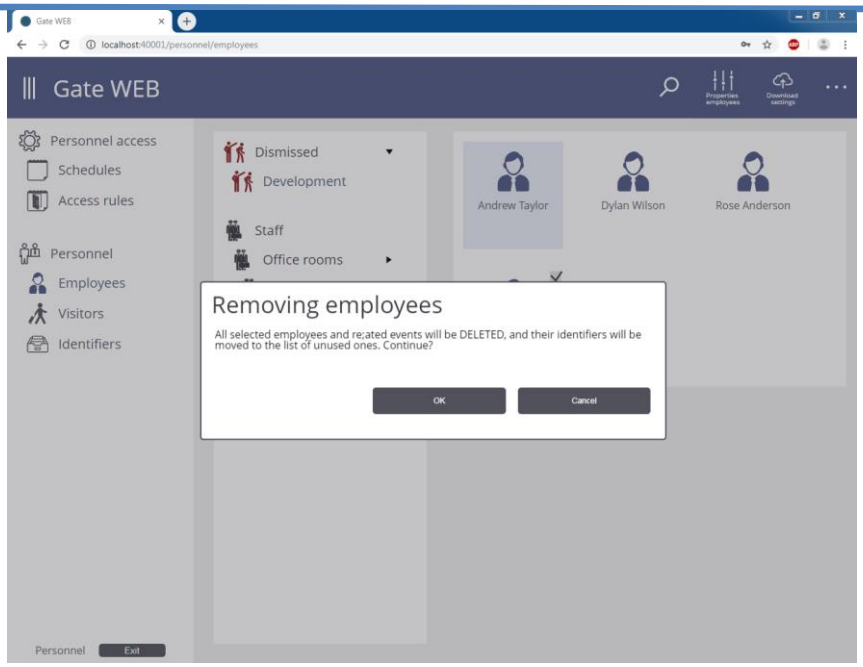


Check □ employees and select ‘Restore employees’ item in main menu. Select department for employees’ restore and press ‘OK’.



Employees who inherit department access will inherit access rule of the department where they were moved.

Check □ employees and select ‘Remove employees’ item in main menu to remove employees and all information about them. Confirm removal in window displayed. All checked employees’ records will be deleted permanently.

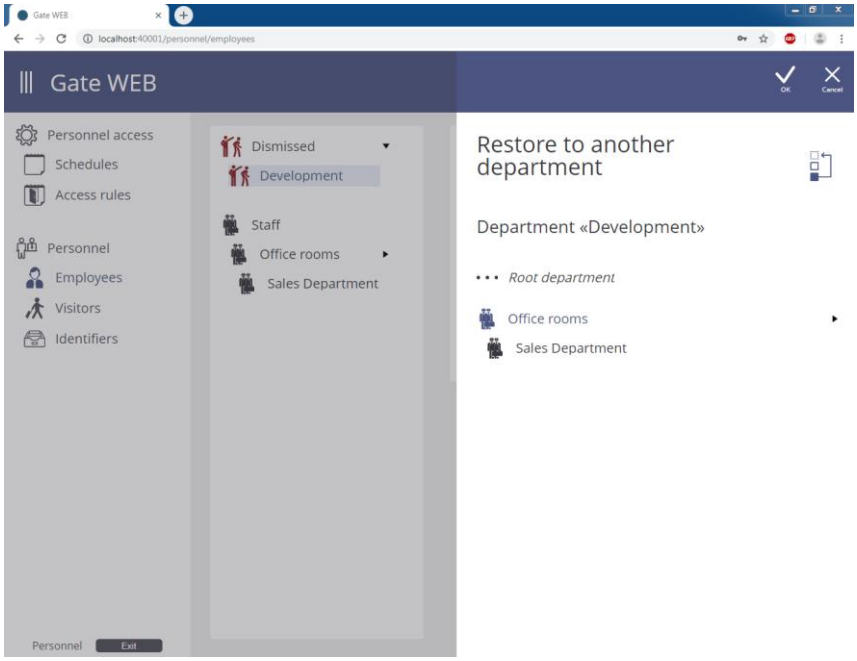


Actions over department

Actions over department available:

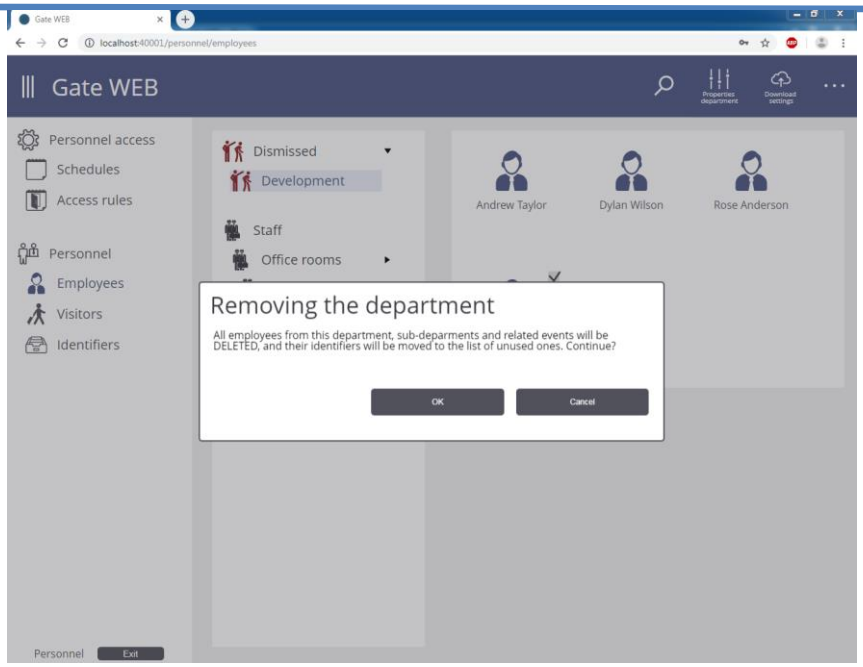
- Restore to another department
- Deletion

Select ‘Restore’ item in main menu to restore department. Select department where restored department will move in the window displayed and press OK.



Employees who inherit department access will inherit access rule of the department where they were moved.

Select ‘Remove Department’ item in main menu to remove department with all employees and all information about them. Confirm removal in window displayed. All department and department employees’ records will be deleted permanently.



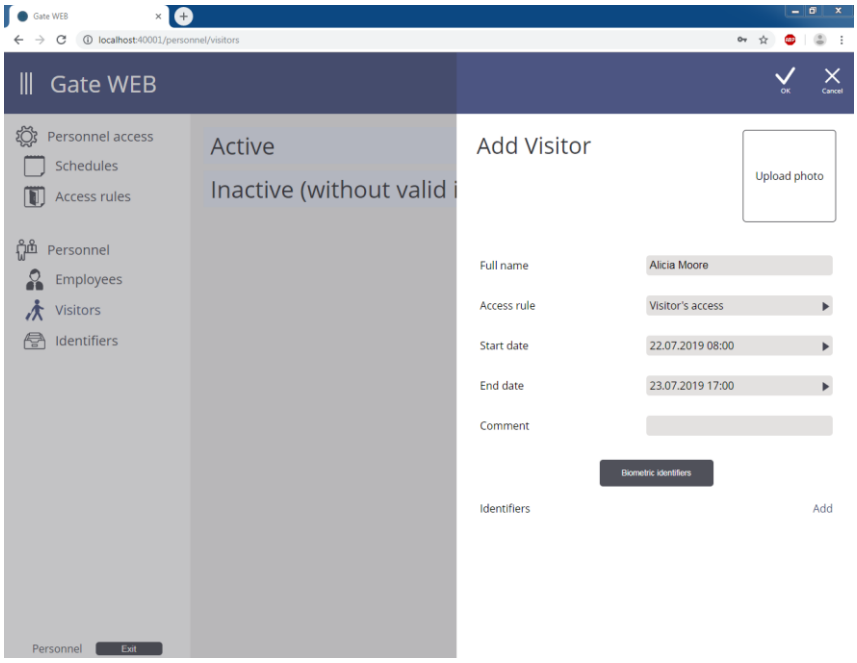
Personnel: Visitors

The visitor attendance is frequent task in many enterprises. ID with access rules to desired department and time limit for temporary access issued to each visitor.

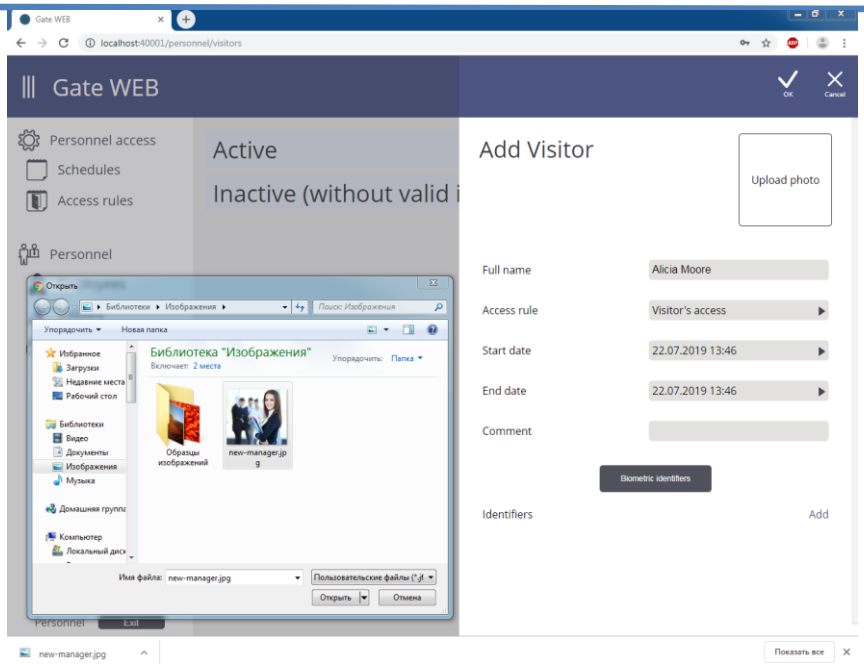
Adding visitors

Select ‘Personnel’ then ‘Visitors’ and press ’Add Visitor’ in menu.

Fill visitor’s name, access level and start and stop dates of his credential validity.



Click ‘Upload photo’ form and select file to add visitor’s picture.

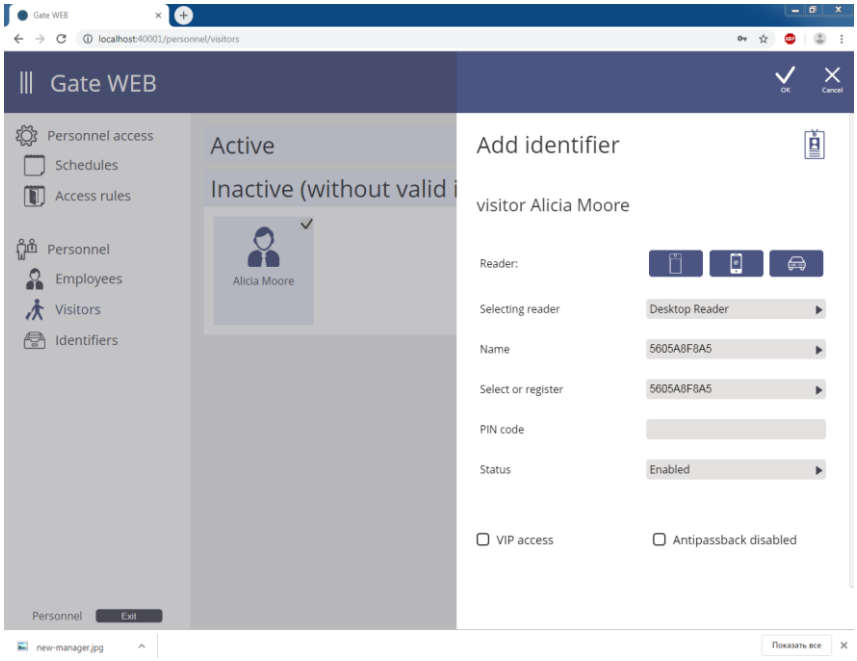


Press ‘Add’ next to ‘Identifiers’ field and select ID enrollment device in window displayed.

Enrollment available from:

1. RF IDs from the USB desktop reader
2. RF IDs from any reader of the system.

Additional options may be adjusted during ID enrollment:



PIN – Personal Identification number associated with ID. PIN Must consist of six to ten decimal digits.

Come rider equipped with keypad. System provides possibility to use RF ID and PIN for access. Reader changes LED blinking after card pass if PIN required. User must

enter PIN after RF ID pass in this case during the time set in panel options.User must enter # button on the keypad or wait for the PIN entry delay. Panel grants access if valid PIN entered. Otherwise panel will deny access, log 'Invalid PIN entered' event and sound warning signal by reader buzzer.

Expiry date – ID expiry date

ID is valid until the date entered. For example, if the expiry date is January 1, 2020, then the last day when access granted will be December 31, 2019.

Status – ID status. This option may have values: Valid, Invalid, Blocked, Lost or Damaged.

Access granted to Valid IDs only. Only Valid IDs shall be issued to employees with right to access premises.

Access not granted to the invalid IDs and those IDs are not loaded into the panel. That's why panel logs 'Unknown card' event on invalid ID pass. Usually this status set for cards enrolled to the system database but not issued to employee.

Reader emits warning beep and panel logs 'Blocked card found' event when ID with 'Blocked' status passed to the reader. Usually this status assigned to IDs belong to employees who have ID and rights for access, but their attendance not expected.

. System processed IDs with 'Damaged' status in the same way as 'Invalid' ID, but has different sense for system operators.

Assign 'Lost' status to the lost cards. It helps to find them because when those cards passed to the reader, door is blocked and panel switches on alarm output.

It is impossible to change ID attributes (Alarm Cancel, Guard, VIP, AntiPassBack) if ID is not valid (Invalid, Blocked, Lost or Damaged).

Attributes. Alarm Cancel – ID will have right to cancel door alarm if 'Alarm cancel' attribute checked.

Panel logs 'Alarm state end' event and switches door into normal state when card with 'Alarm cancel' attribute passed. Panel logs 'Access denied. Door in alarm.' event when card without 'Alarm cancel' attribute passed.

Attributes. Guard card – ID with 'Guard' attribute allows to enter the blocked door.

Door is blocked if it is necessary to deny access for all employees and visitors, except the guard. Door is blocked with corresponding panel input violation or by the command from system server.

Reader emits warning signal on ID without 'Guard' attribute pass if door is blocked. Panel logs 'Access denied. Door BLOCKED'. Panel grants access and logs 'Access granted. BLOCKED state' on valid 'Guard' ID pass.

Attributes. VIP – Person having ID with ‘VIP’ attribute may open any door at any time, except the doors in ‘Blocked’ state.

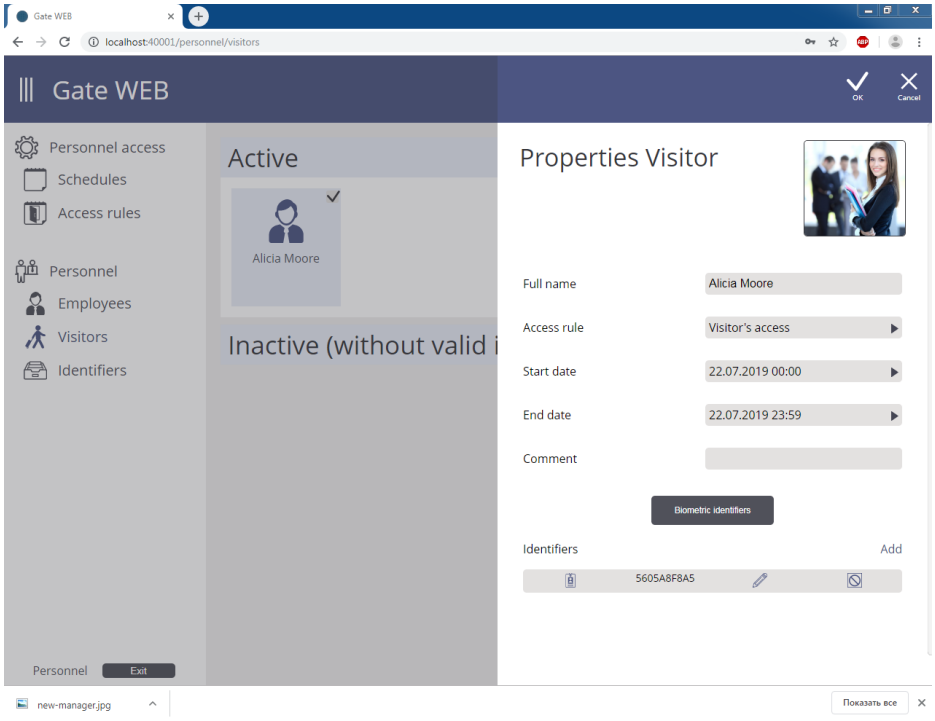
Schedule, antipassback attribute and use time limit does not affect the operation of this ID. ID with this attribute may have PIN.

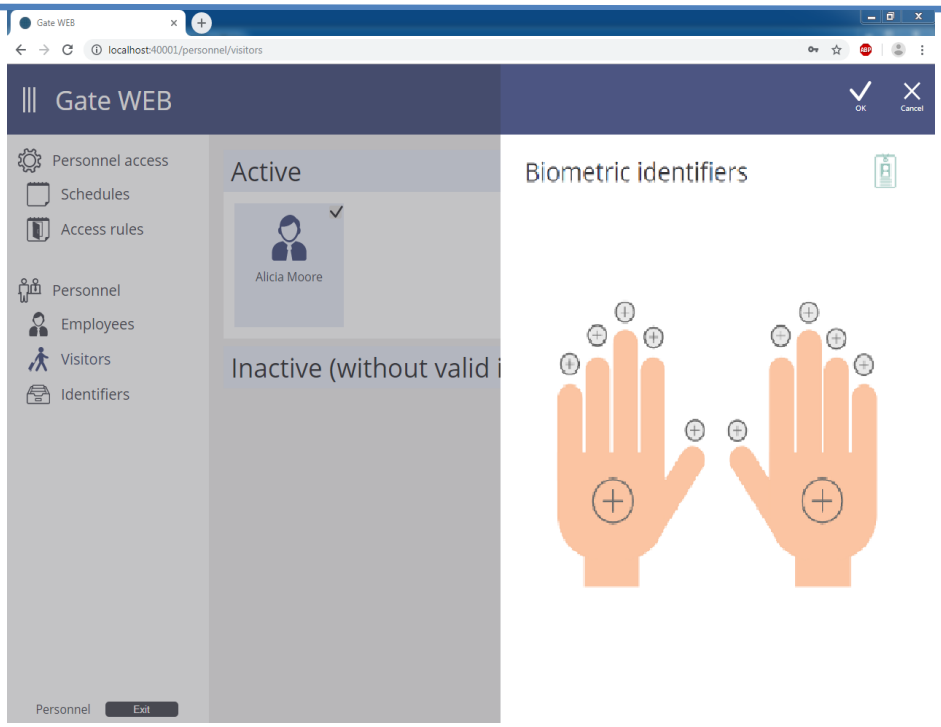
Panel logs ‘Access denied. Blocked state’ event, denies access and reader emits warning signal when VIP ID passed to the reader of the blocked door.

Attributes. AntiPassBack OFF– Employee with ID with this attribute passes doors without antipassback registration. Access is granted independently from the side of door and registered employee position.

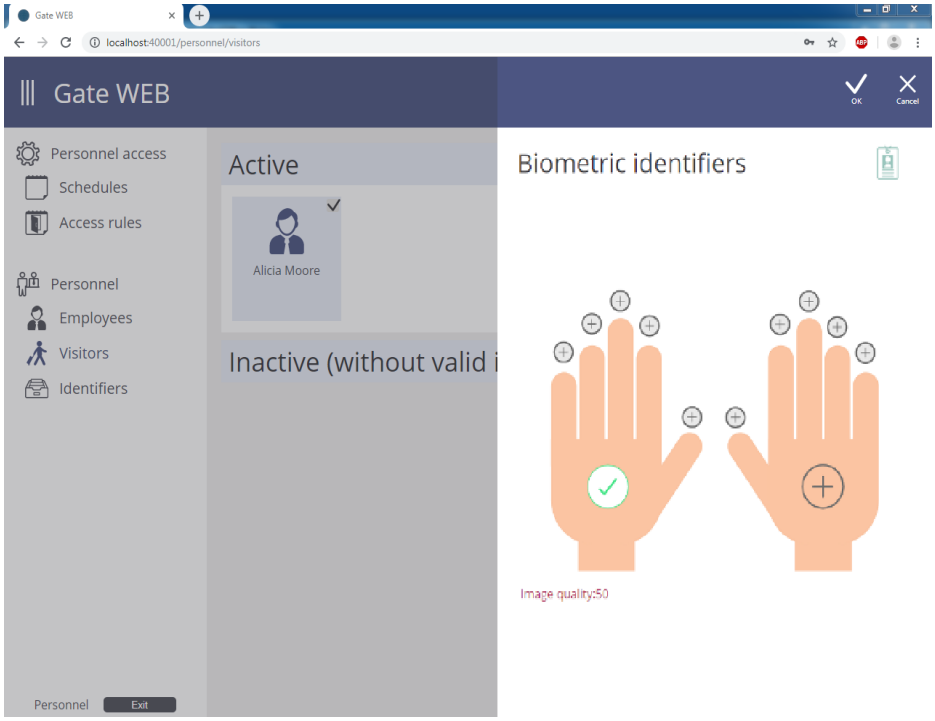
Biometric ID enrollment becomes available if there are biometric readers connected to the system. ***Attention!!!*** *Employee must have at least one normal (RF or mobile) ID for biometric ID enrollment.*

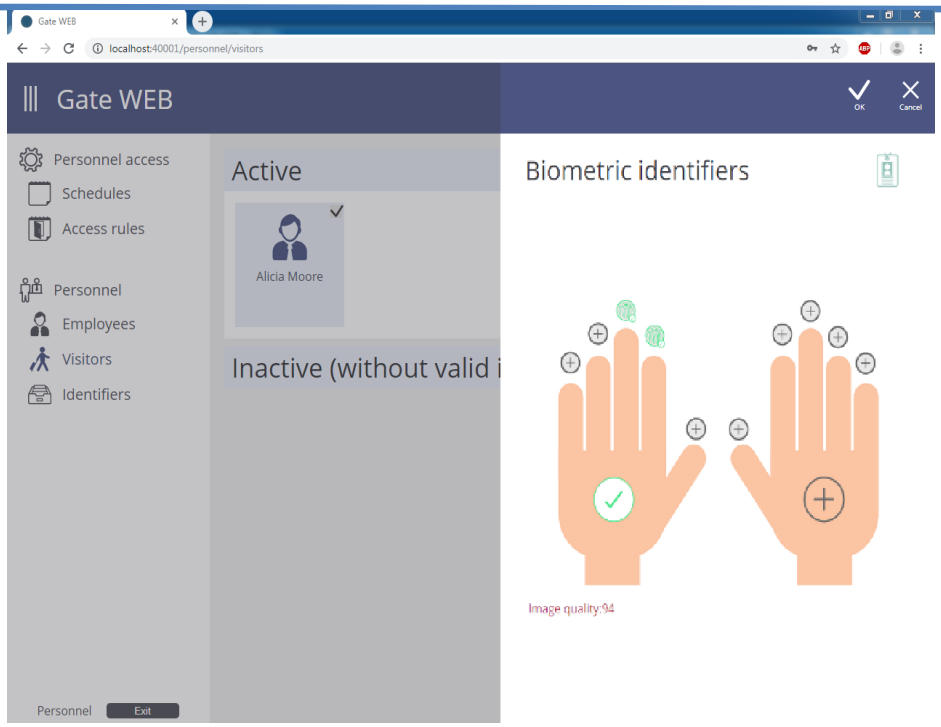
Press ‘Biometric Identifiers’ and select in the window displayed ID type – fingerprint or palm vein will be enrolled.





Add biometric identifier following enrollment wizard.





Press ‘Save’ to save changes

Add group of visitors

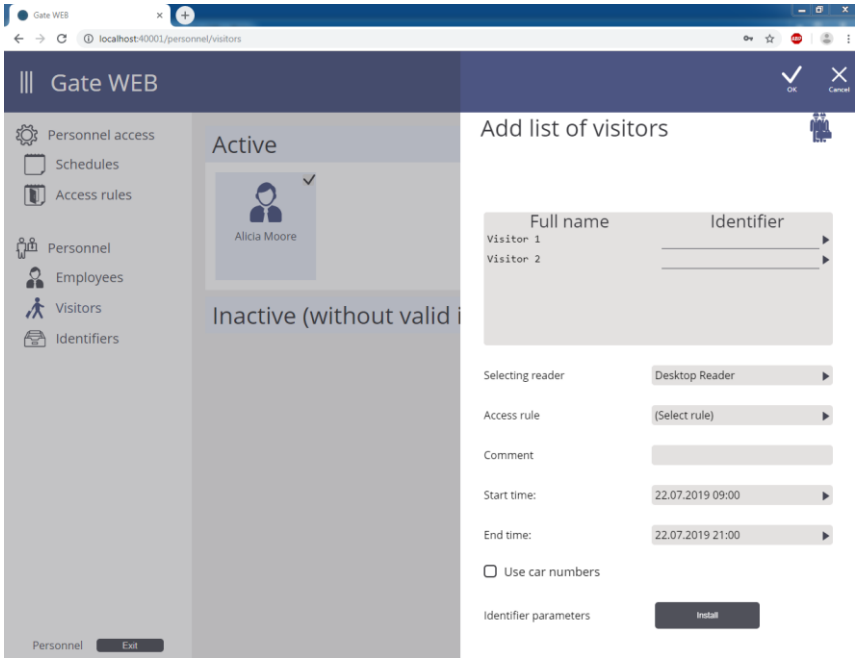
Use visitors’ list adding to add multiple visitors quickly.

Create file with visitors’ names listed in the column as below:

Visitor 1

Visitor 2

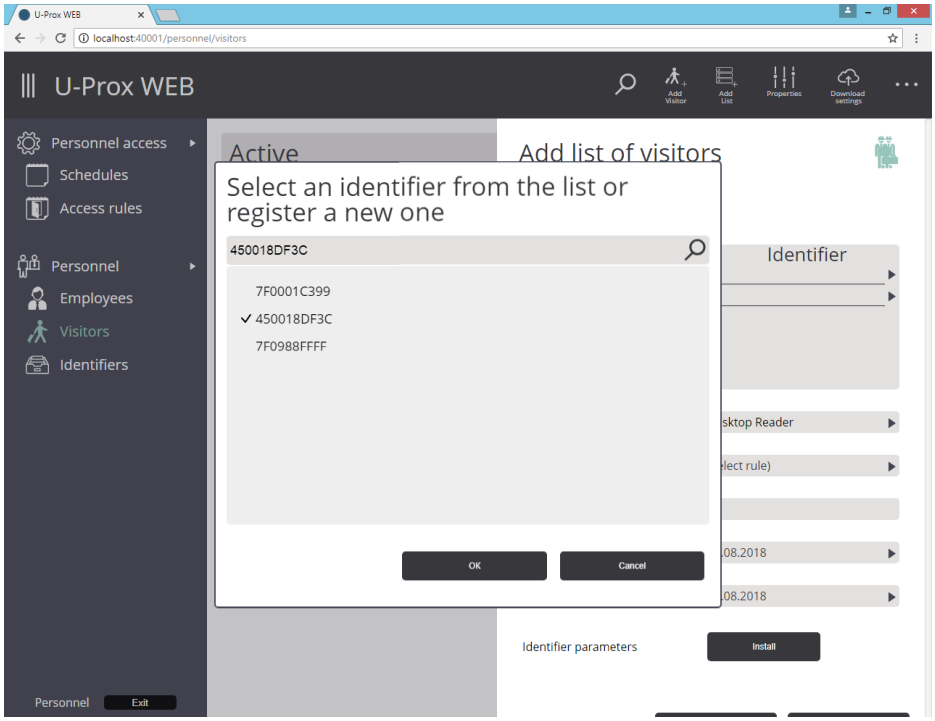
Press ‘Add list’ button in the main menu and copy the list from the file into the window displayed:



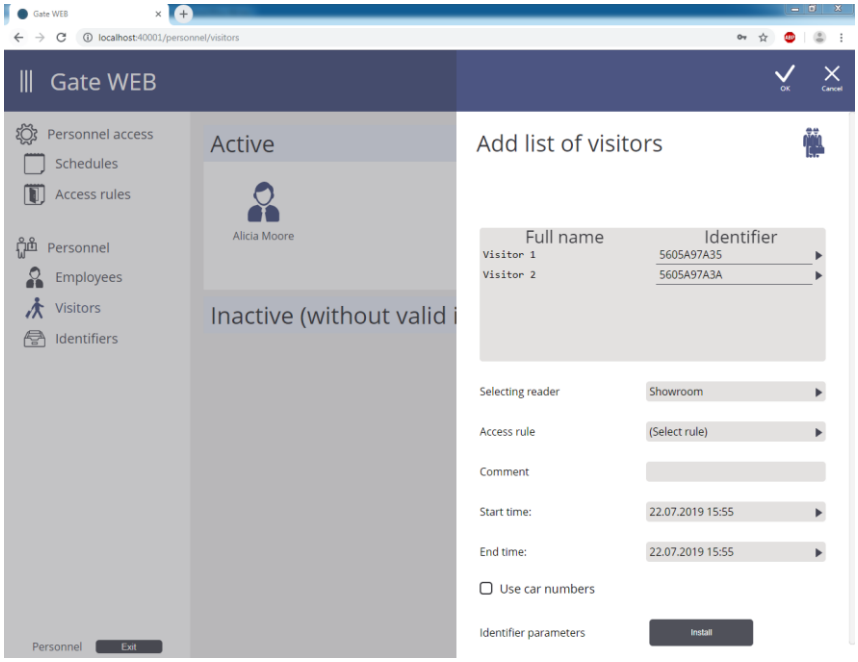
Then enroll IDs for each visitor from desktop reader or any other reader of the system.

Enrollment reader selected in ‘Selecting readers list.

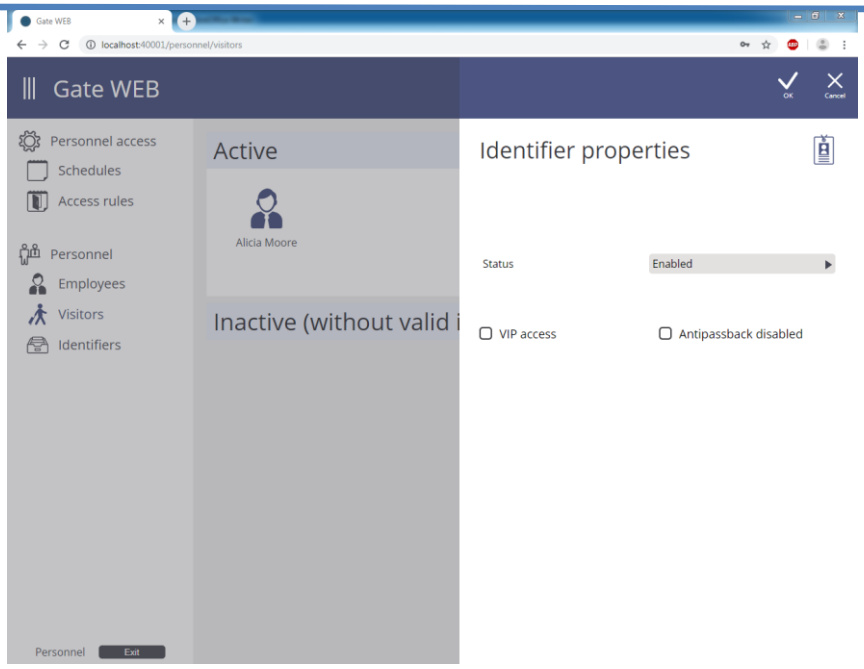
ID selection or enrollment window will display on click on ‘Identifier’ field. Select or enroll Identifier and press ‘OK’ button.



Assign access rules to all employees after IDs enrollment in ‘Access rule’ field.



IDs’ options and attributes are set in the same way. Press ‘Set’ in window displayed to do this:



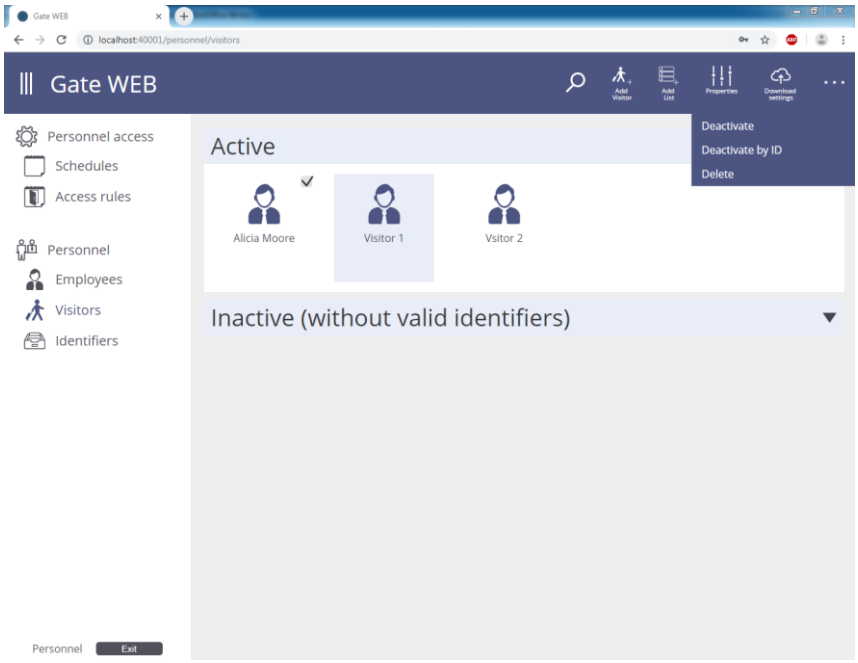
Actions with visitors

Actions with visitors available:

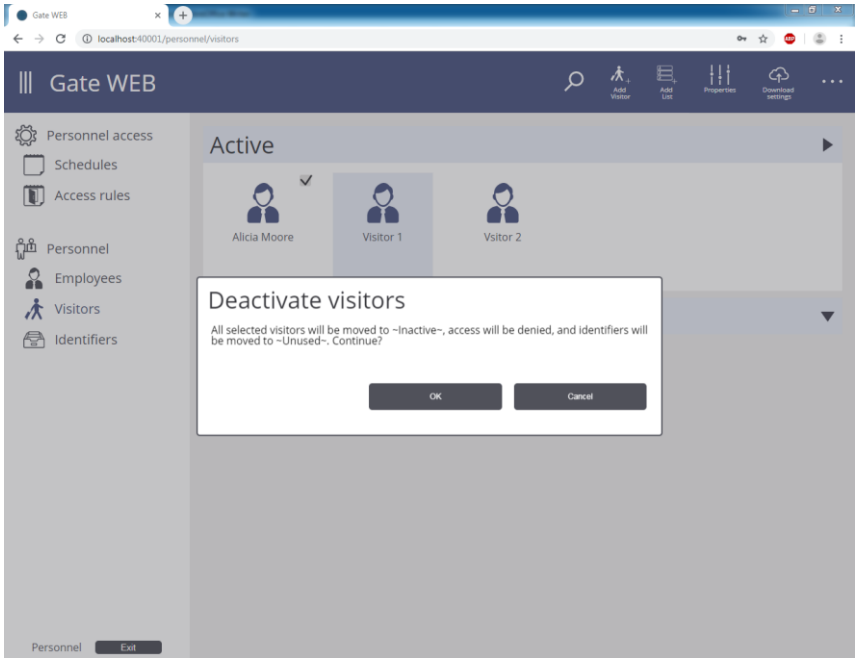
- Deactivation
- Deactivation by ID
- Removal

It is necessary to deactivate visitor's ID to remove visitor and his ID from the control panel. Visitor moved to 'Inactive' group and his ID returns into the list of unused after deactivation. It is possible to deactivate one visitor as well as for several enrolled IDs.

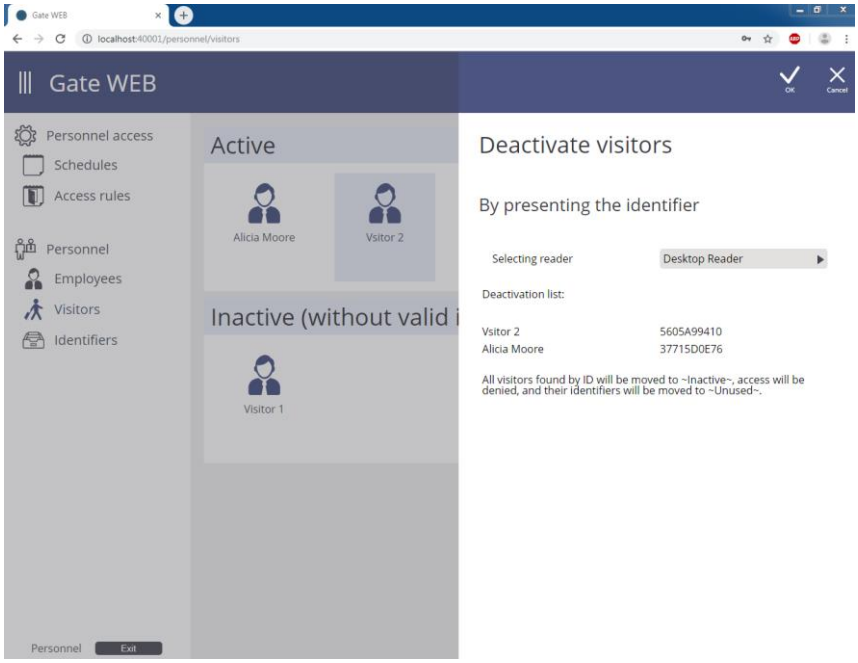
Check □ visitors and select 'Deactivate' in main menu to deactivate visitors.



Confirm visitors' deactivation in window appeared.

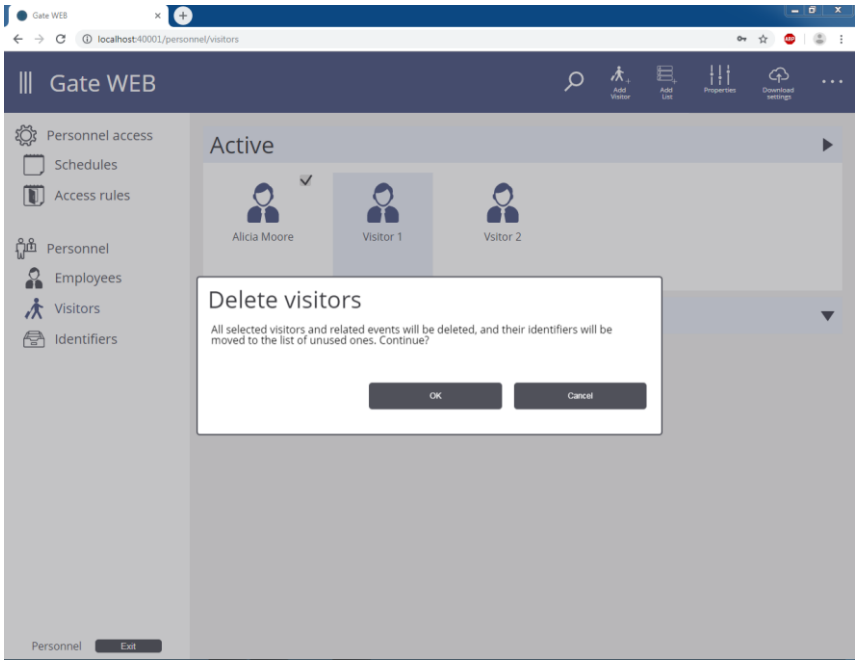


Select 'Deactivate by ID' in main menu to deactivate visitors by IDs.



Select reader for ID to be deactivated reading Visitors deactivated after all ID read with selected reader and 'OK' button pressed.

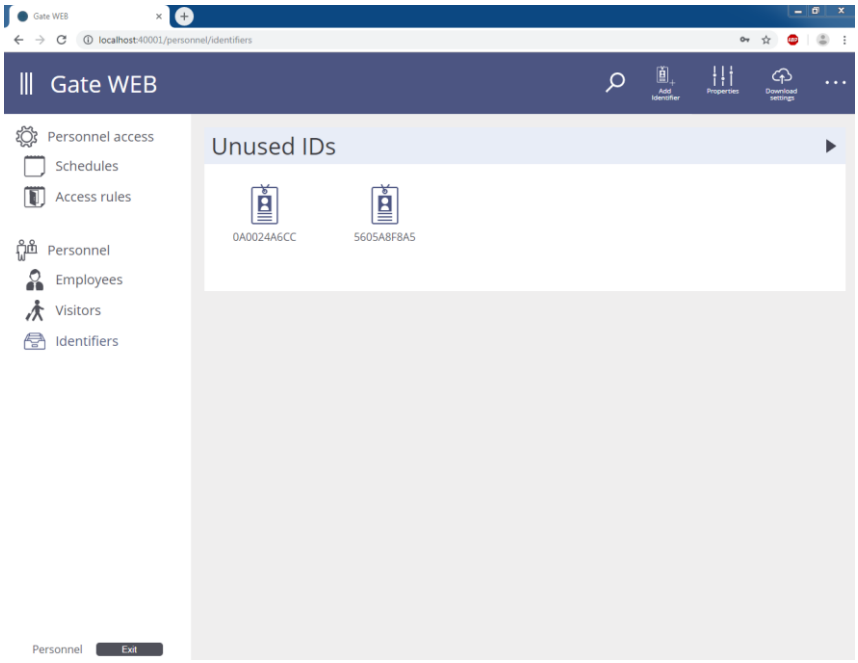
Check □ visitors and select ‘Remove’ item in main menu to remove visitors. Confirm remove in window displayed. All visitors’ data deleted permanently after remove.



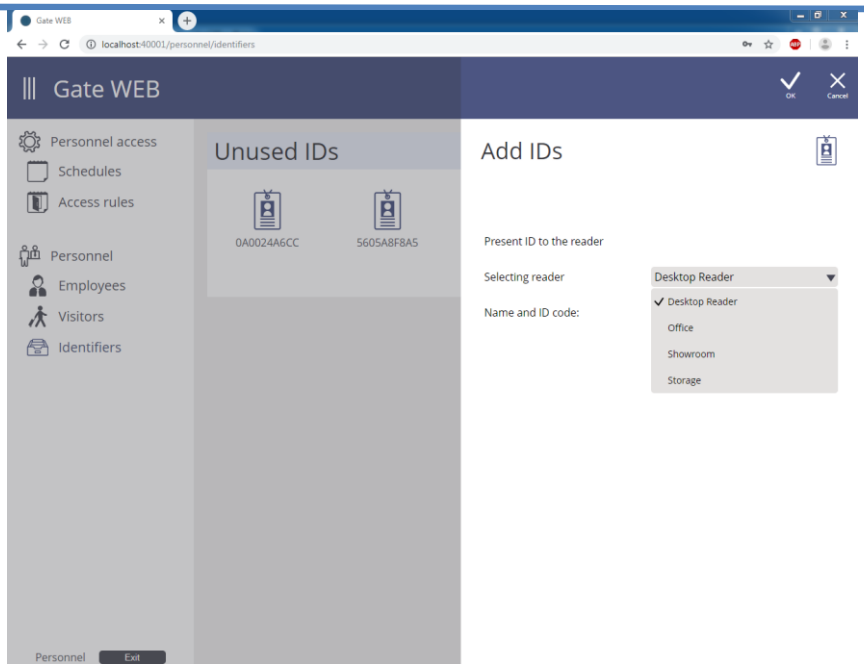
Personnel: IDs

Enroll all IDs before filling database with employees’ data. This operation is not necessary as you may enroll ID during employee options adjustment.

Select ‘Personnel’ tab to the left, then ‘IDs’. Unused IDs list will display.

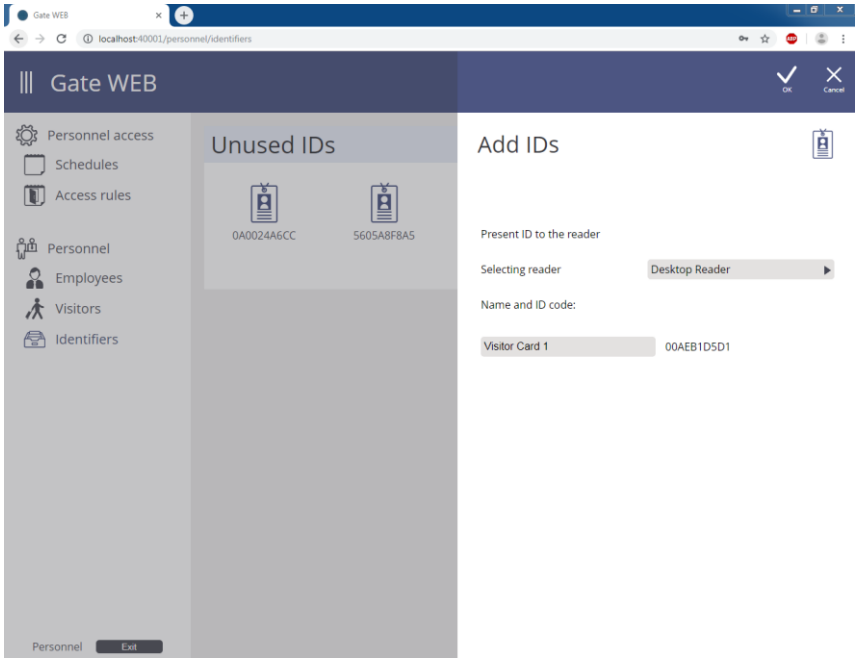


Press ‘Add ID’ to add new ID. Select enrollment reader in ‘Reader selection’ field.

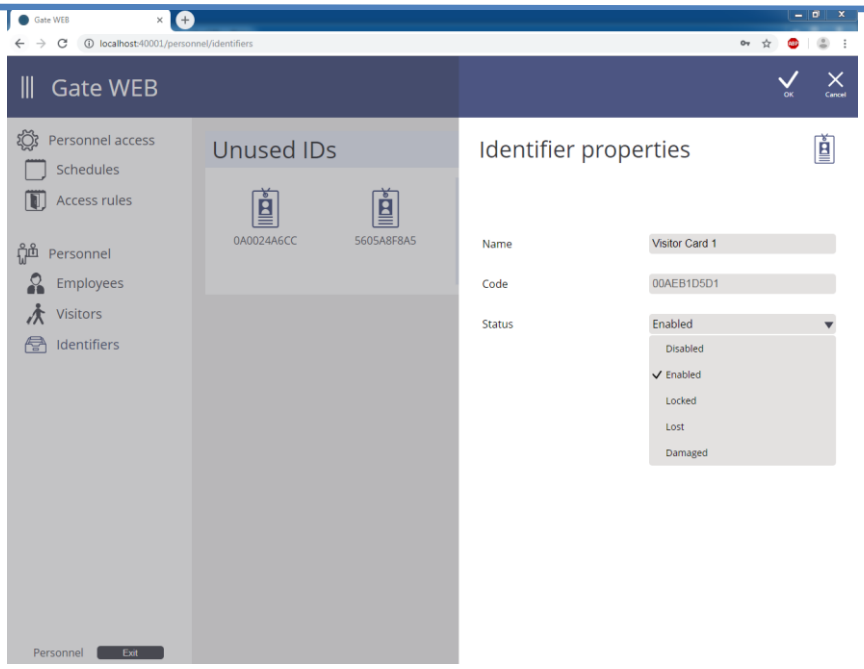


ID code displayed in window on ID pass to the reader. System warns about the IDs already in system.

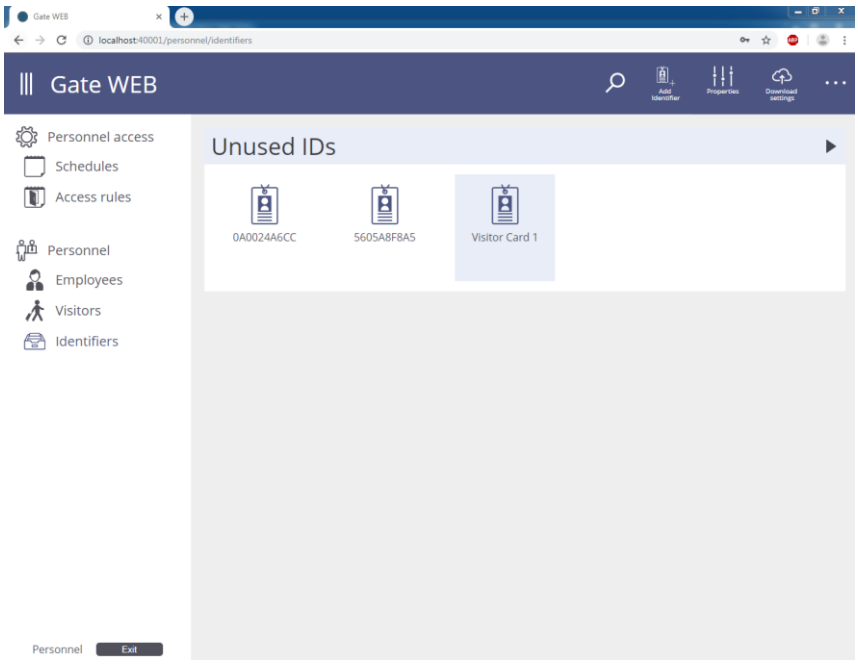
Operator may change ID name.



Operator may adjust options for all IDs to be added. Press ‘Install’ button next to the ‘Identifier parameters’ and adjust options in window displayed to do this.



New IDs will appear in ‘Unused IDs’ folder.

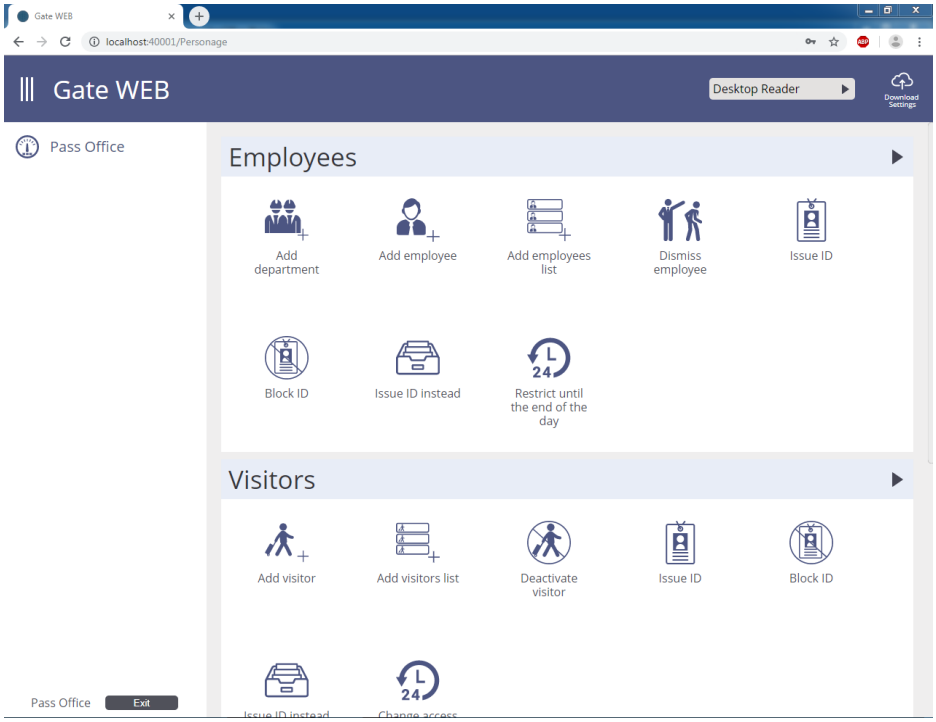


‘Pass’ office’ role

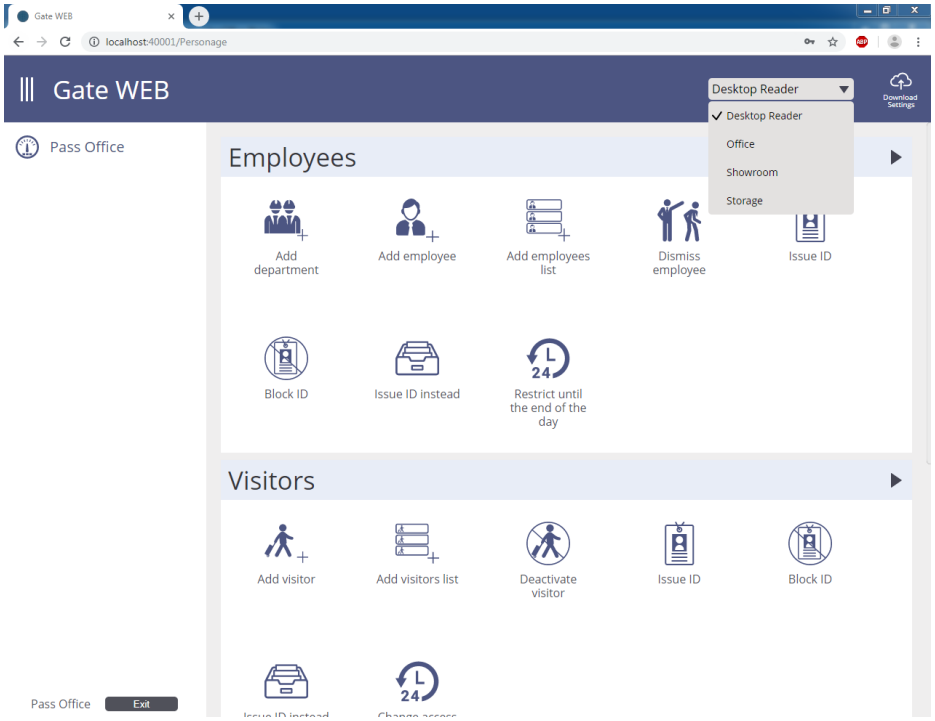
‘Pass’ office adds and deletes credentials, gives IDs to users, manages visitors.

This role allows to add and edit departments and employees; operate with IDs and mobile IDs, deactivate visitors. Allows to find user record by ID and determine users position in the premises (last door entered).

All actions of ‘pass’ office collected into set of wizards for easiest use by rookie.



Enrollment device selection drop down list situates in the main menu on the top of window. This device allows to enroll new ID or find user by ID quickly. Device shall be selected before any wizard start.



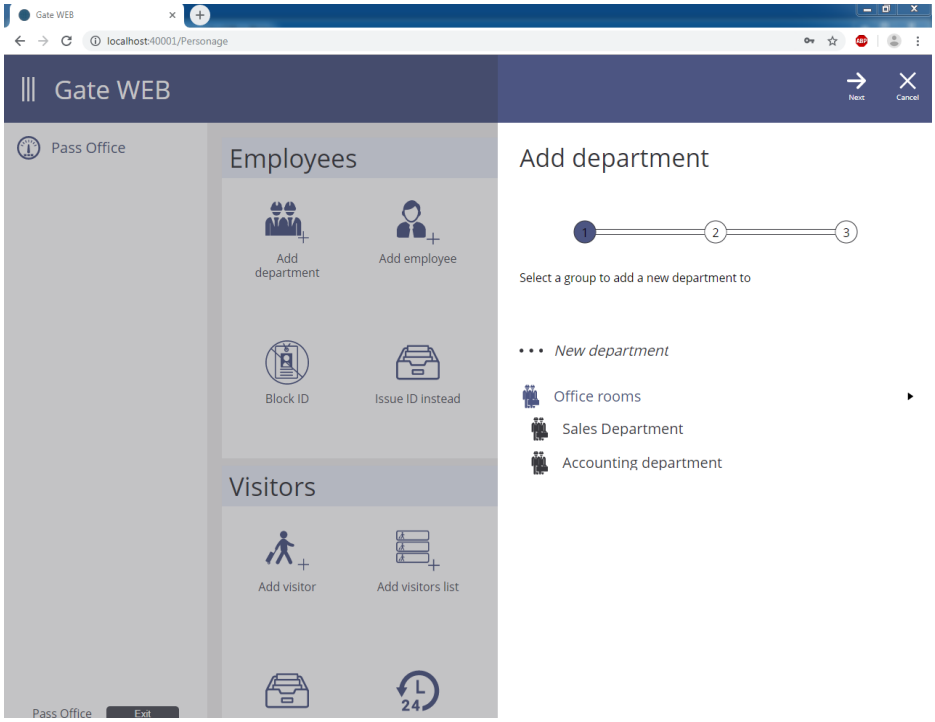
Attention!!! Download panels after employees, visitors, ID cards added or access rights changed. Press ‘Download settings’ button to do this.

‘Employees’ actions

Department adding

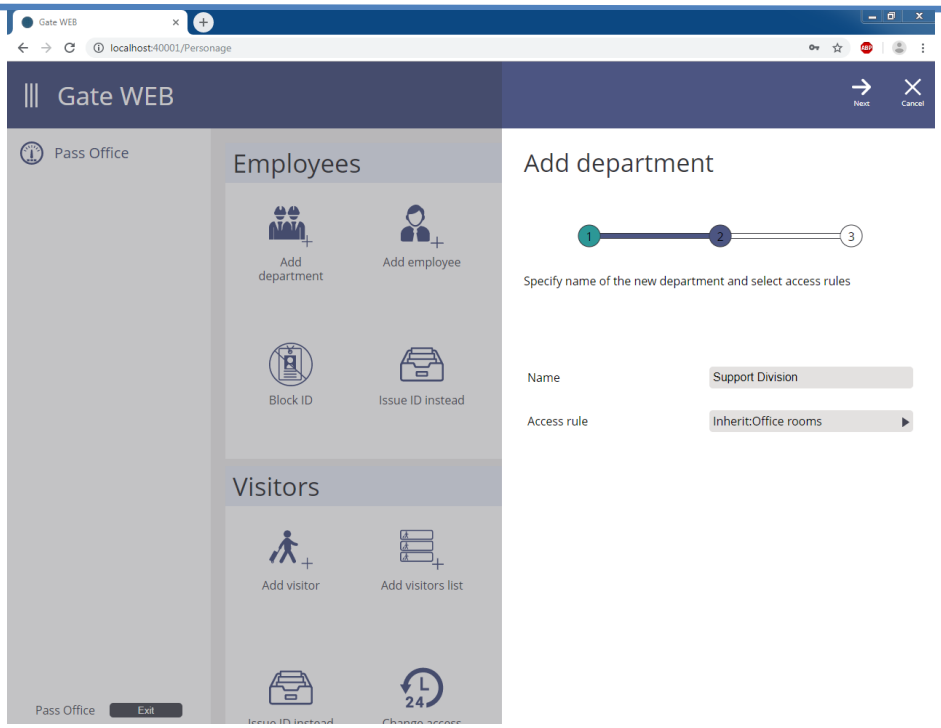
Press ‘Add department’ in ‘Employees’ section to add department.

Select department into which new department will be added and press ‘Next’.

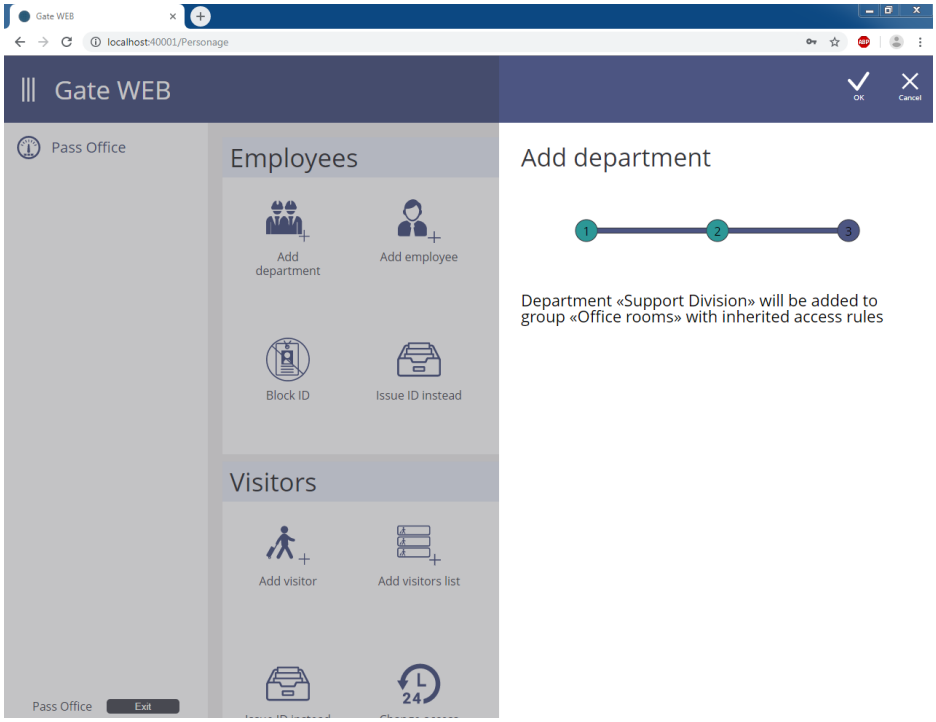


Select ‘New department’ item to add department of the highest level.

Type department name and access rule used for all department employees by default. Press ‘Next’.



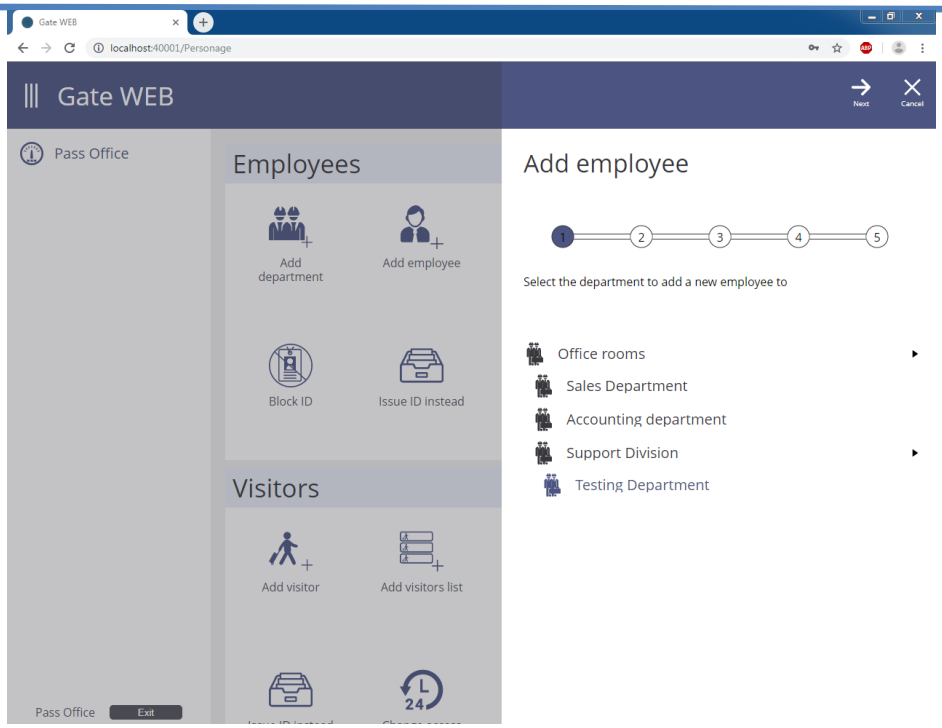
Press ‘OK’ to save changes and add new department.



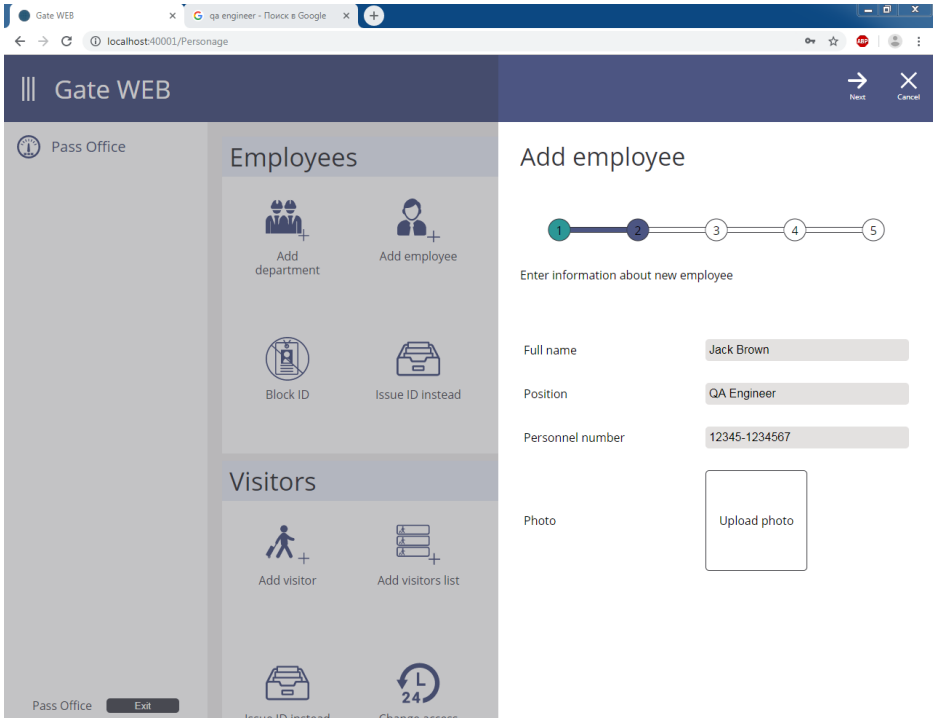
‘Employees’ adding

Press ‘Add employee’ icon in ‘Employees’ section to add employee.

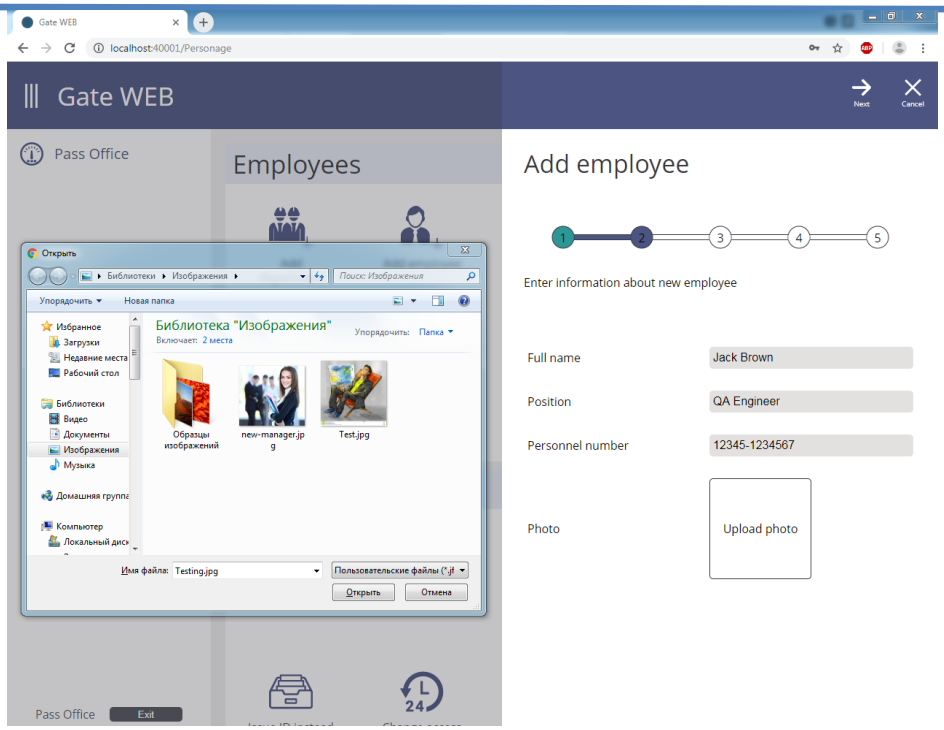
Select the department to add in employee in window displayed and press ‘Next’.



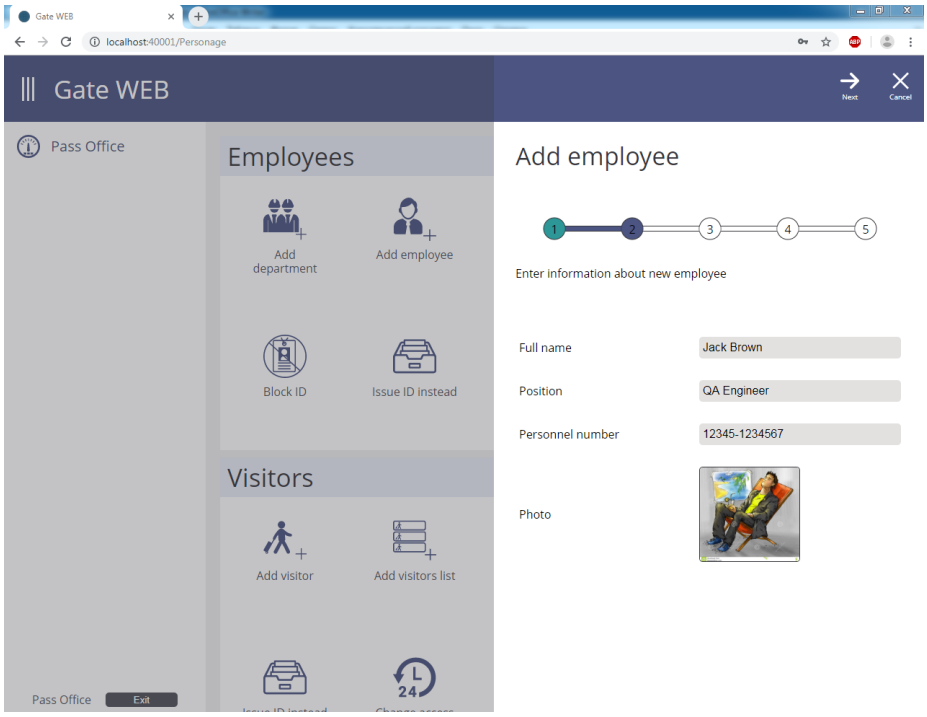
Type employee name and his position.



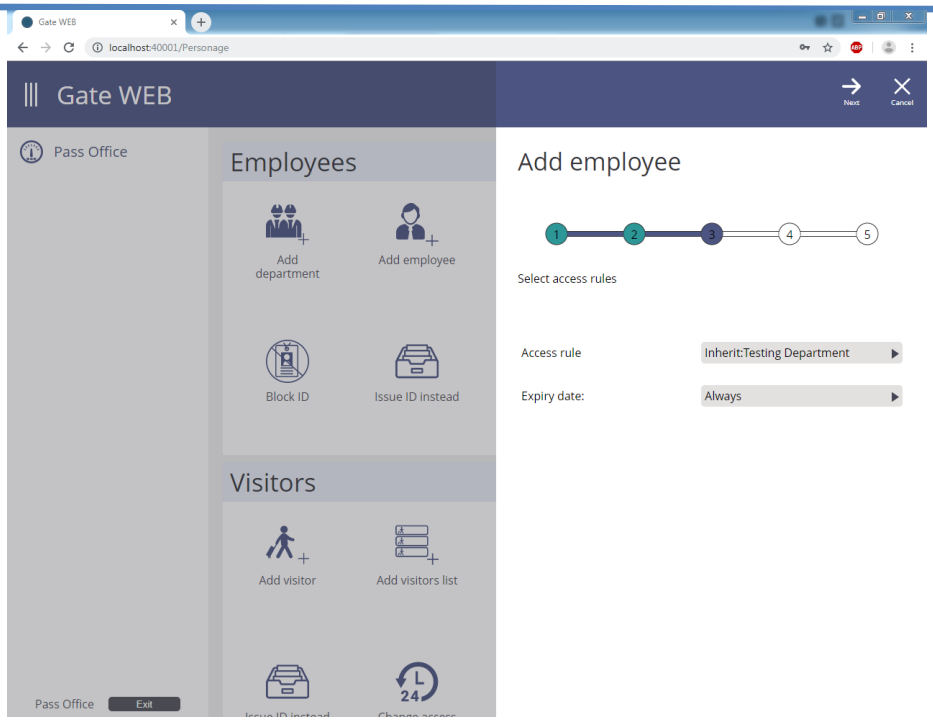
Clock photo form and select file with employee photo in window displayed to add the photo.



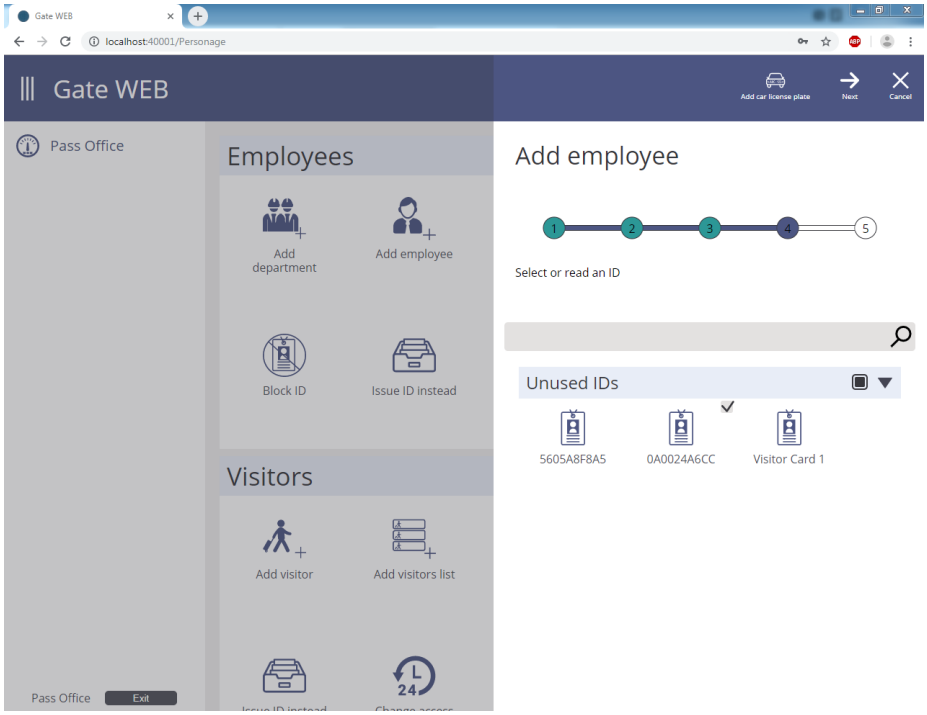
System will add photo. Press ‘Next’.



Select individual employee access rule or mark that employee inherits department access rule.

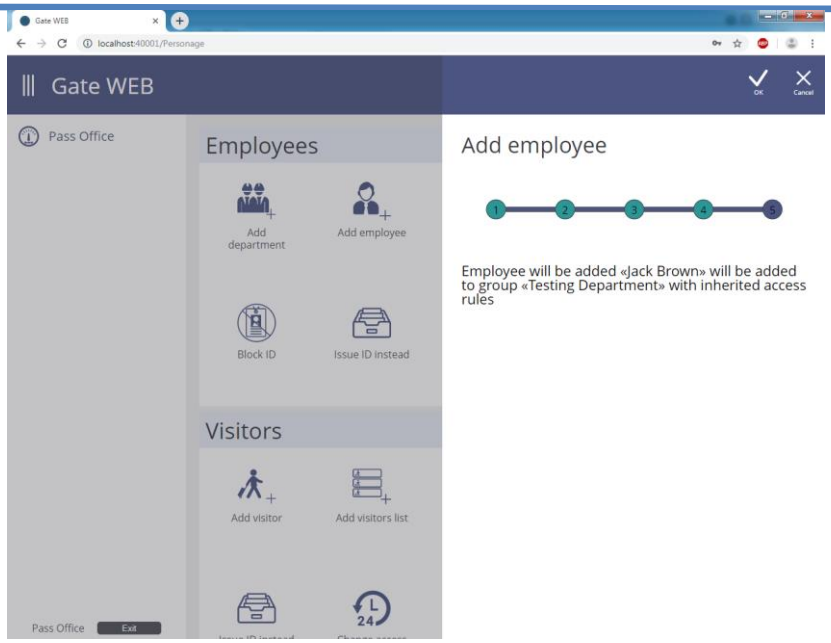


Add IDs to the employee, selecting them from the list of unused identifiers or enrolling new IDs.



Press ‘Next’ after ID adding.

Press ‘OK’ to add employee and save changes.


Gate WEB
localhost:40001/Personage
Gate WEB
OK
Cancel
Pass Office
Employees
Add department
Add employee
Block ID
Issue ID instead
Visitors
Add visitor
Add visitors list
Pass Office
Exit
Add employee
1
2
3
4
5
Employee will be added «Jack Brown» will be added to group «Testing Department» with inherited access rules

Adding employees' list

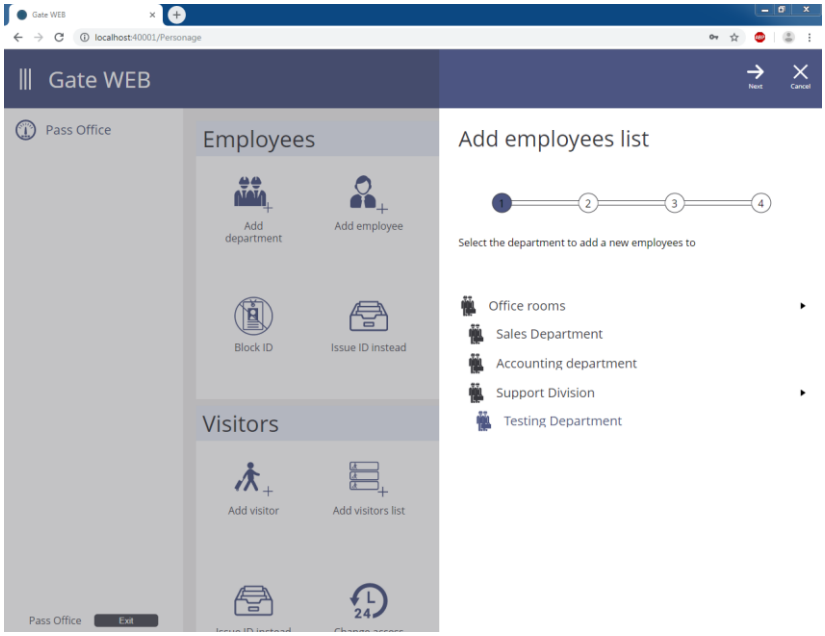
Press 'Add list' icon in 'Employees' section to add numerous employees quickly.

Prepare file with employees' names listed in column beforehand. For instance:

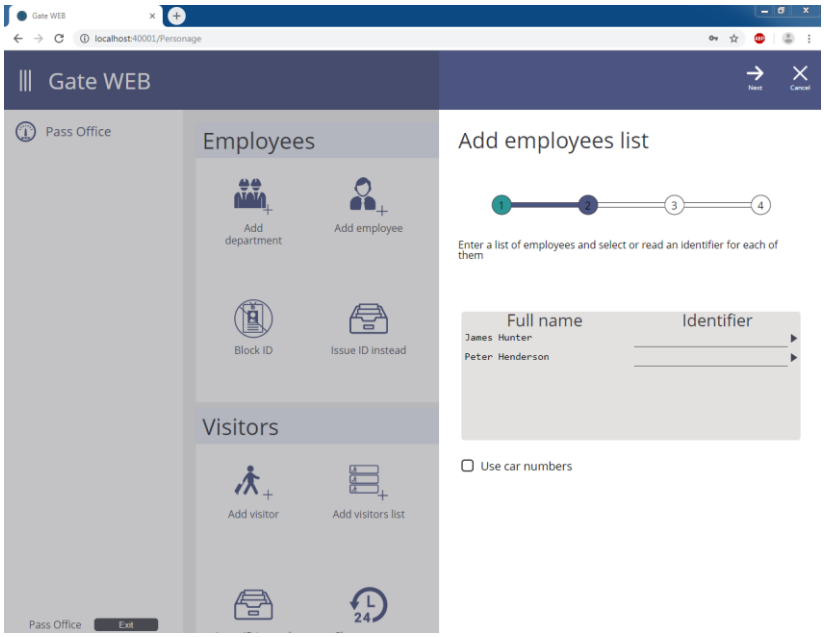
Jonnie Walker

Jack Daniels

Select department to add in employees in the window displayed and press 'Next'.

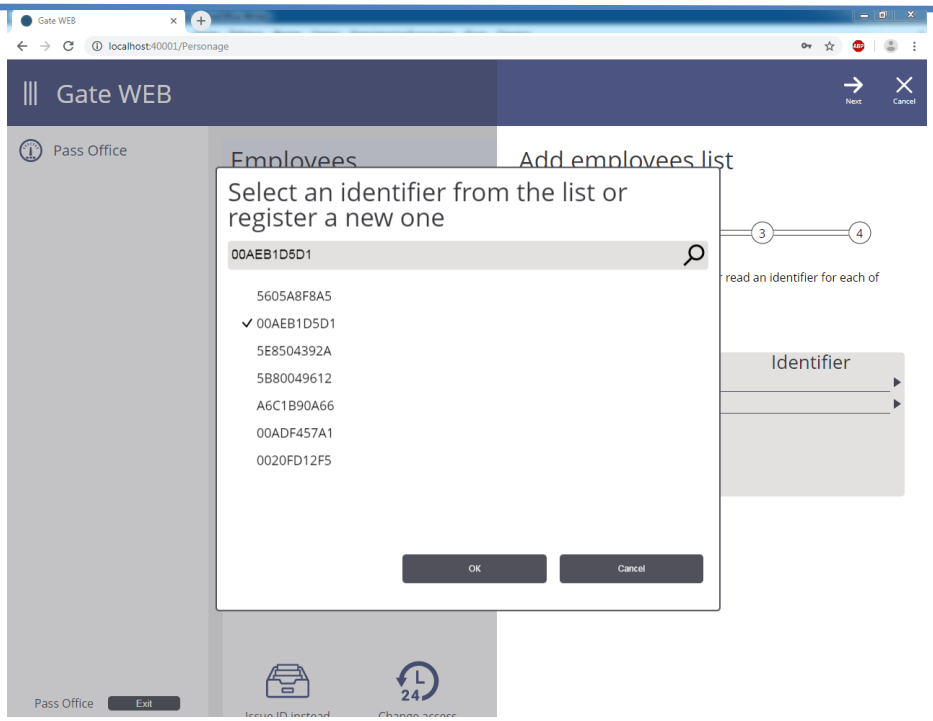


Then copy employees list from the file.

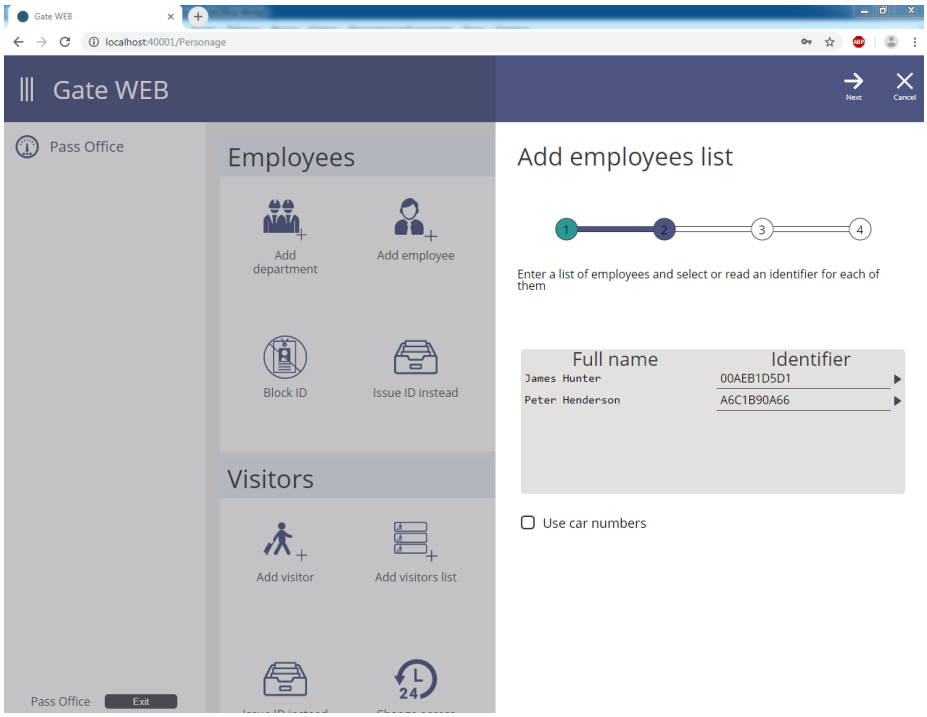


Add identifiers for each employee, enrolling them from device selected before wizard started.

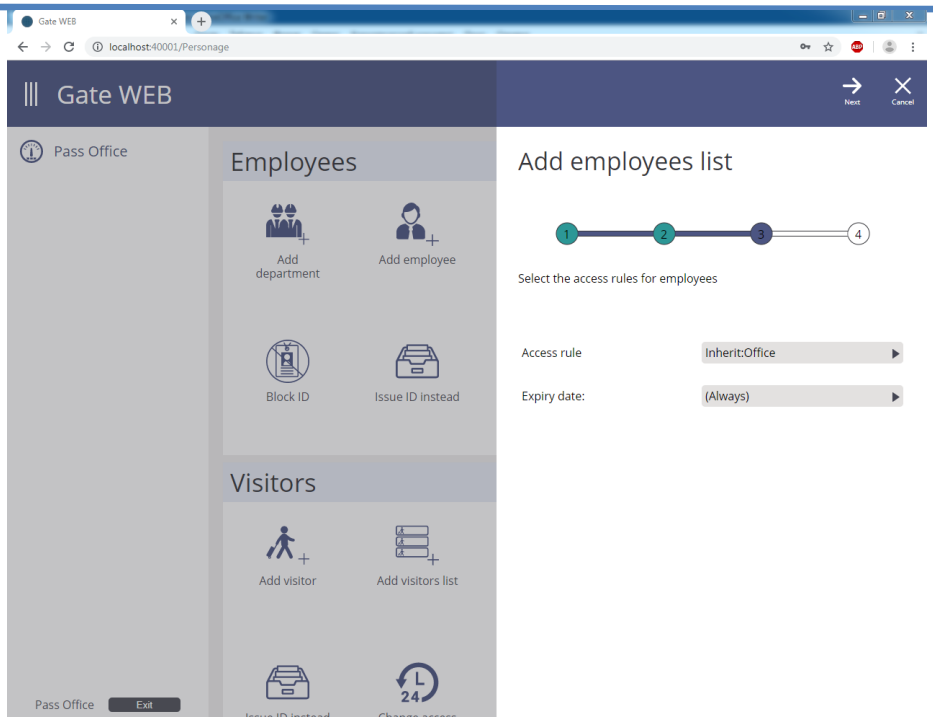
Enrollment window will display on mouse click on the 'ID' field. Select ID from the list or enroll it. Then press 'OK'.



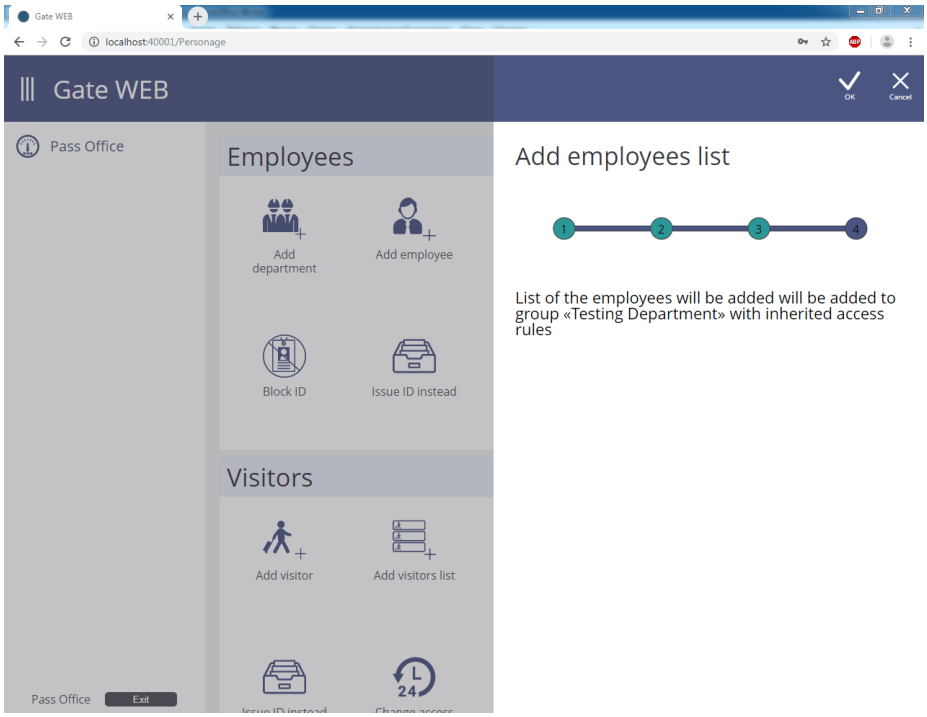
Press ‘Next’ button after all employees’ IDs added.



Set access rules and press ‘Next’



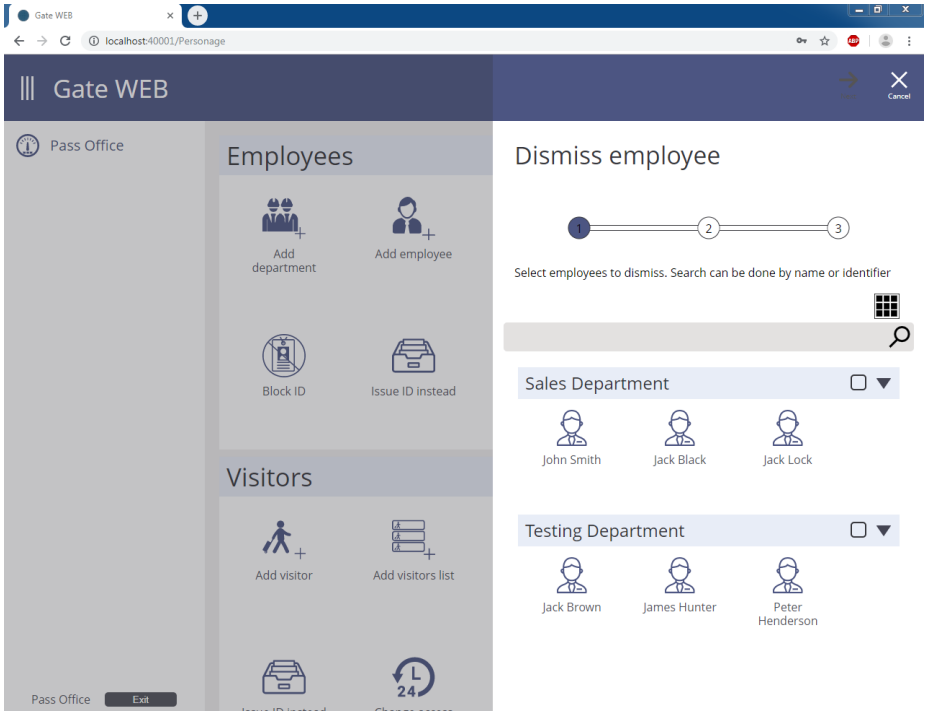
Press ‘OK’ to add all employees and save changes.



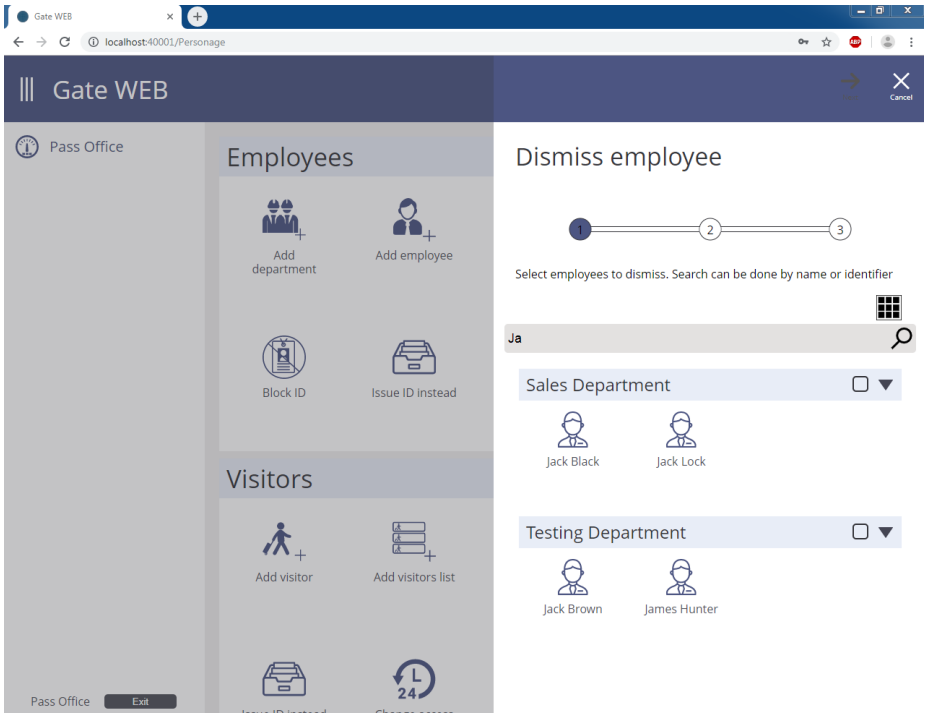
Dismissing employee

Press ‘Dismiss employee’ in ‘Employees’ section to dismiss employee.

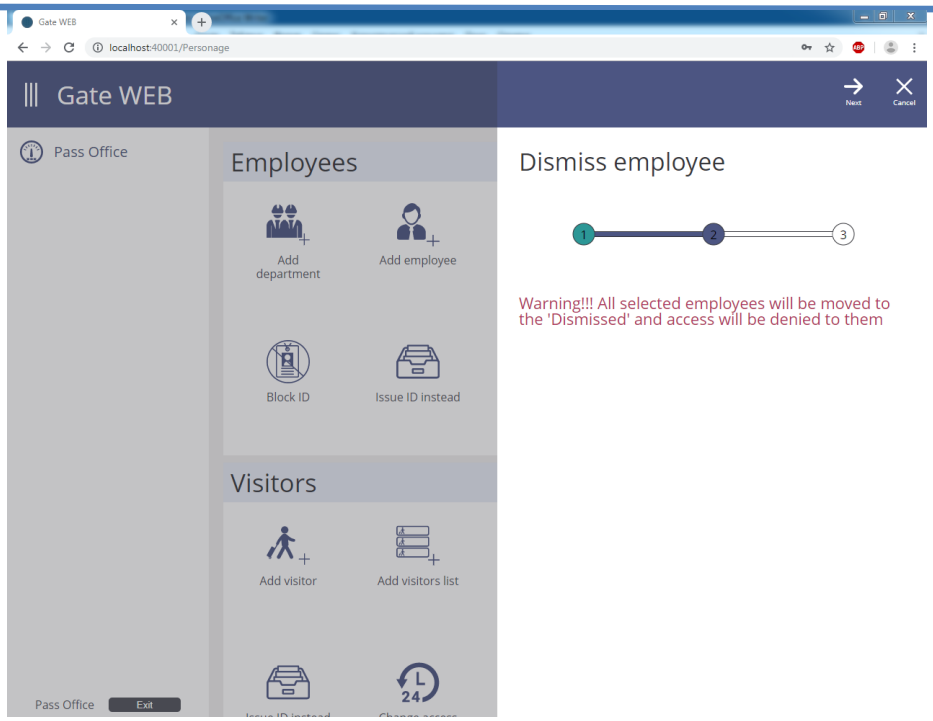
Select employee for dismission.



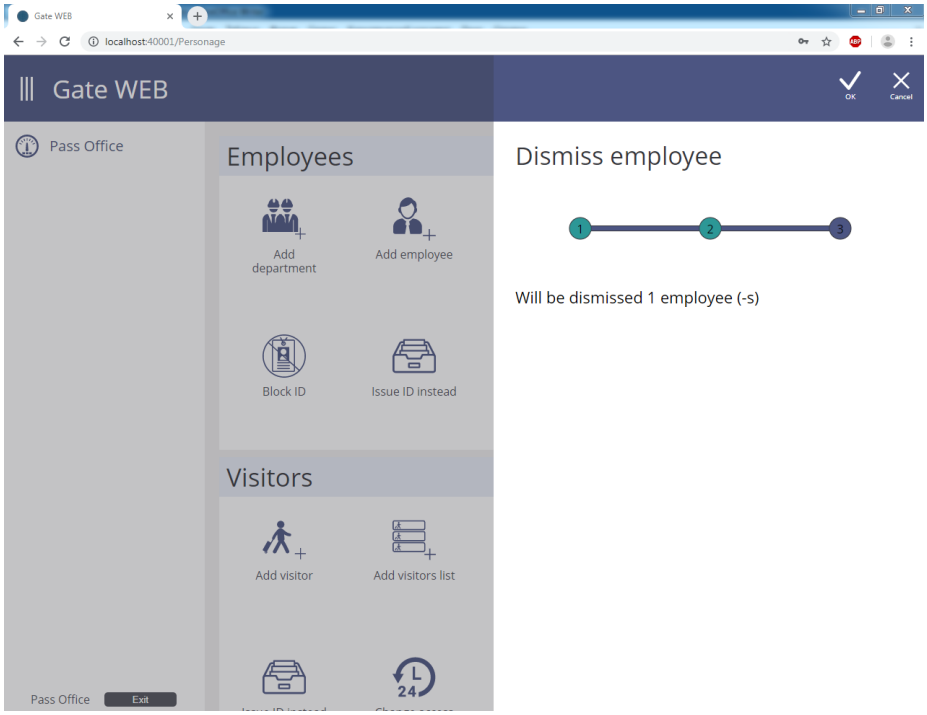
Use search by part of employee name or by ID for fast find.



Press ‘Next’ to confirm dismission.



Press ‘OK’ to dismiss employee and save changes.

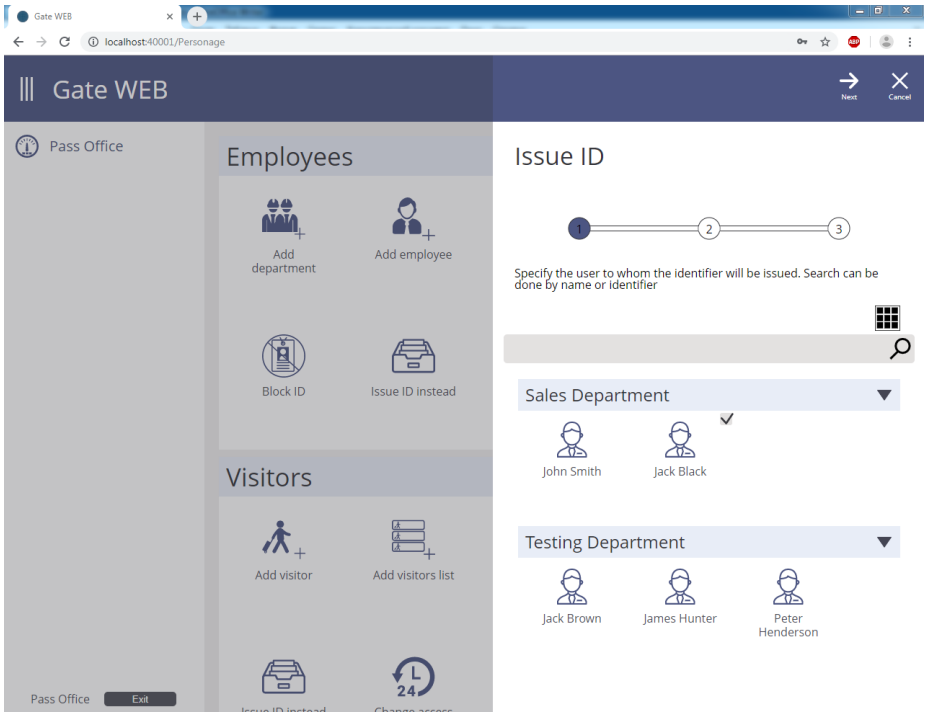


Give ID to employee

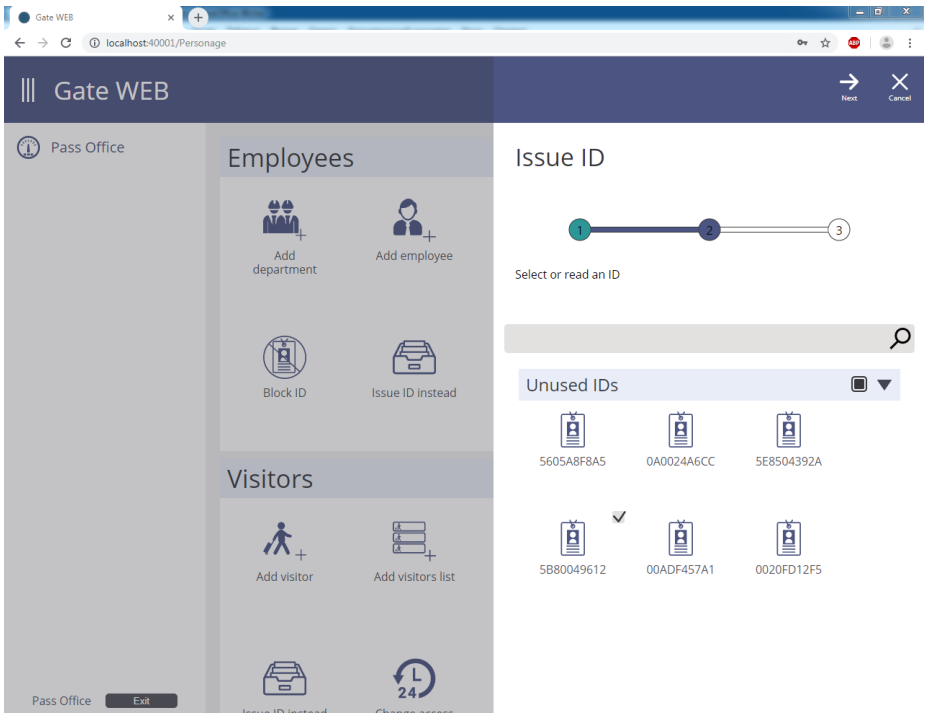
Press ‘Give ID’ icon in ‘Employees’ section to give ID to employee.

Select employee to give him ID.

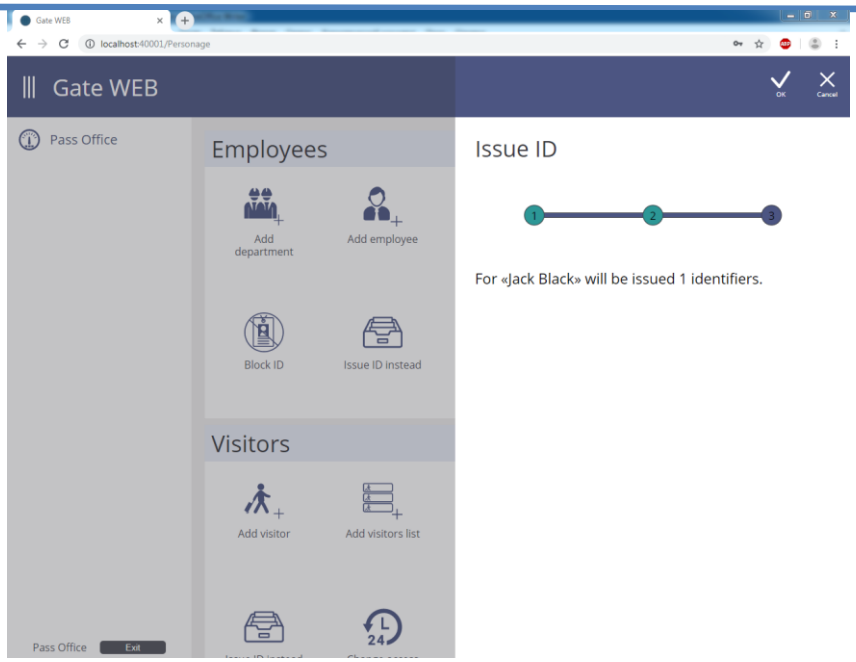
It is possible to use search by part of name or by ID for quick search.



Give to employee IDs from the list of unused IDs or enroll new.



Press ‘OK’ to save changes and give ID to the employee.

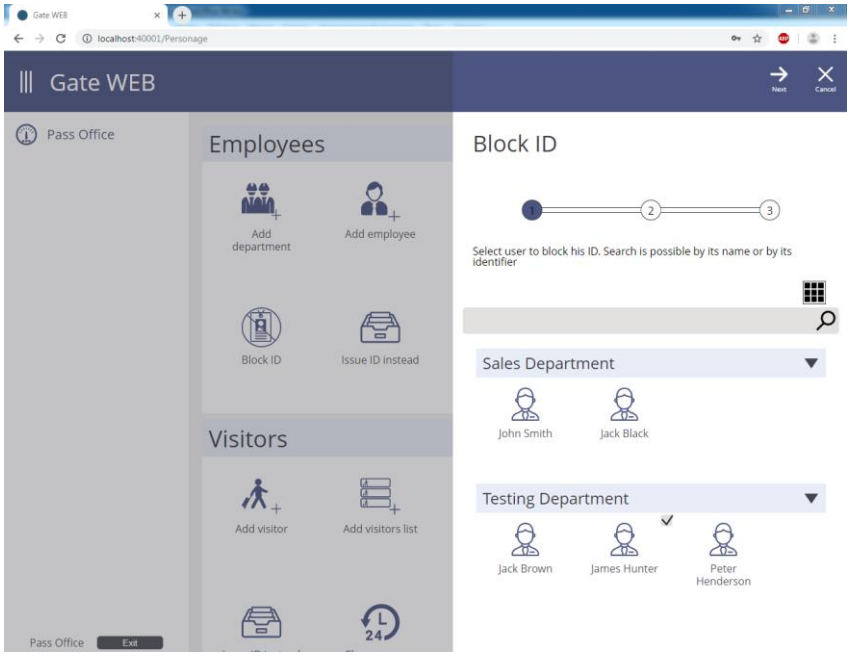


ID blocking

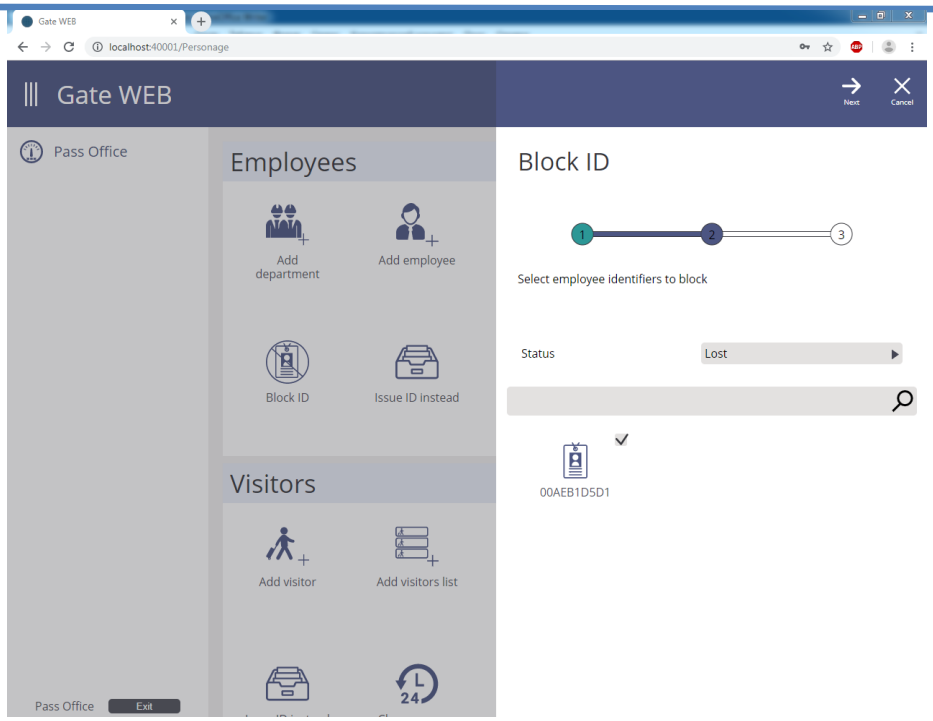
Press ‘Block ID’ icon in ‘Employees section’ to block employee’s ID.

Select employee and press ’Next’.

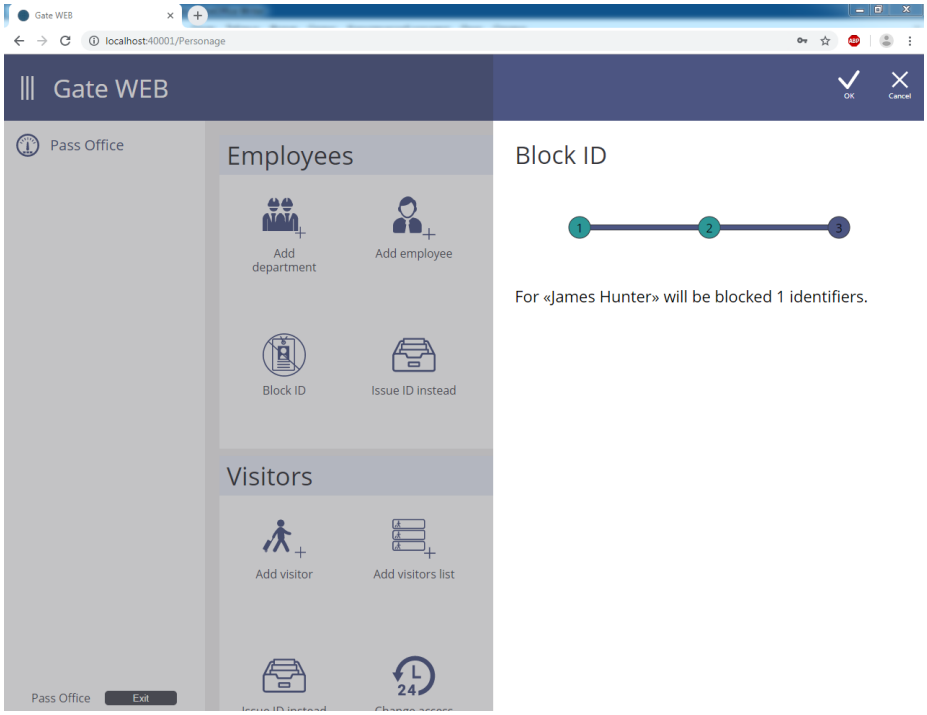
It is possible to use search by part of name or by ID for quick search.



Select ID and its status for blocking.



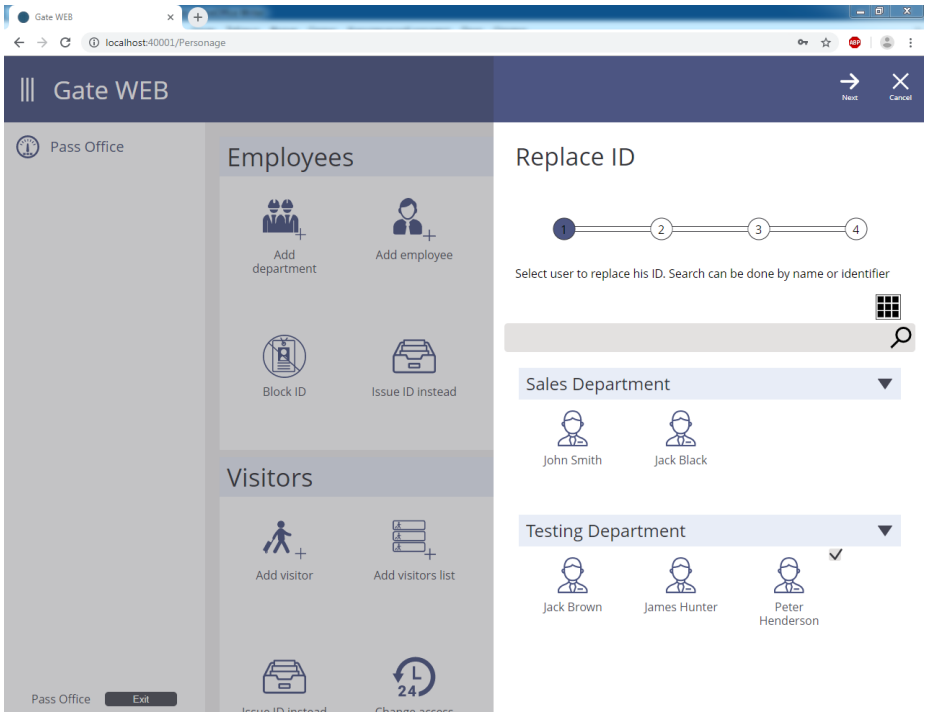
Press ‘OK’ to block employee’s ID and save changes.



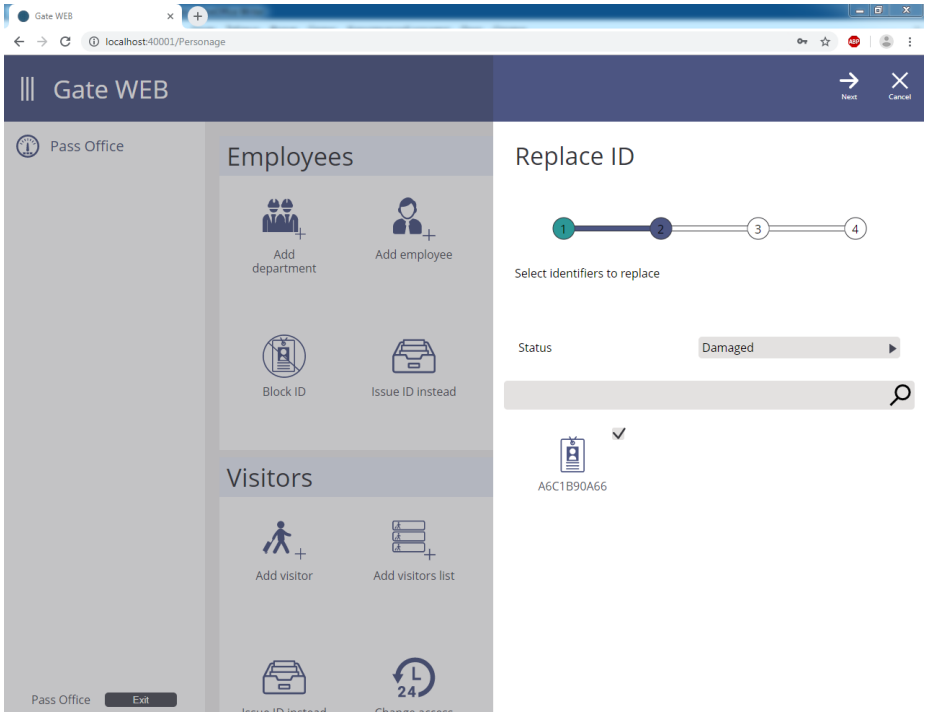
Spoiled or lost ID replacement

Press ‘Replace ID’ icon in ‘Employees section’ to replace spoiled or lost employee’s ID.

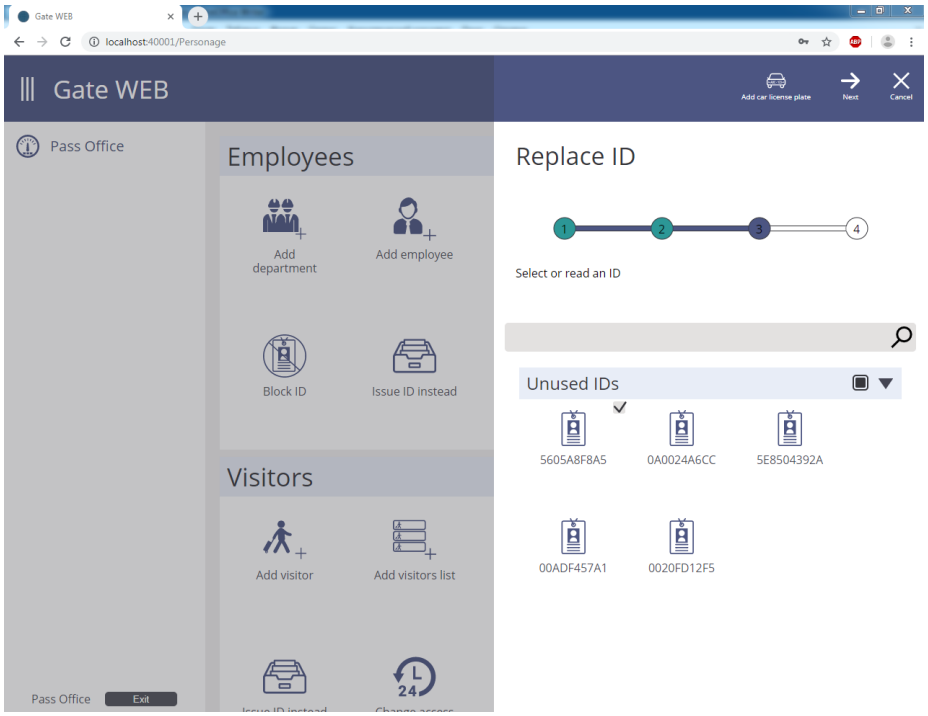
Select employee for ID substitution.



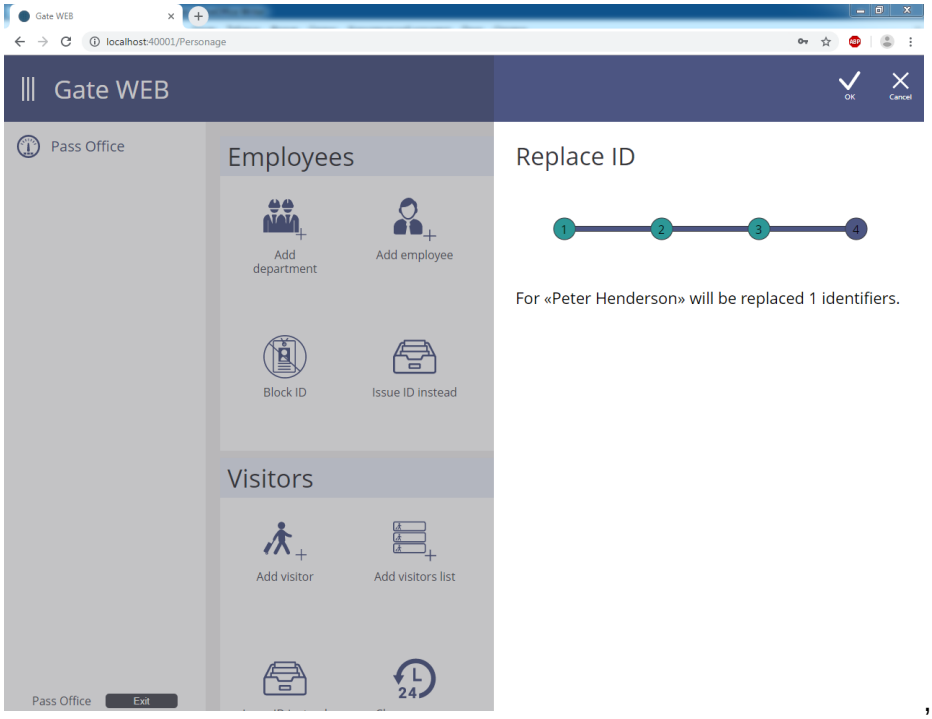
Select ID and its status for substitution.



Give to employee IDs from the list of unused IDs or enroll new.



Press ‘OK’ to replace employee’s ID and save changes.

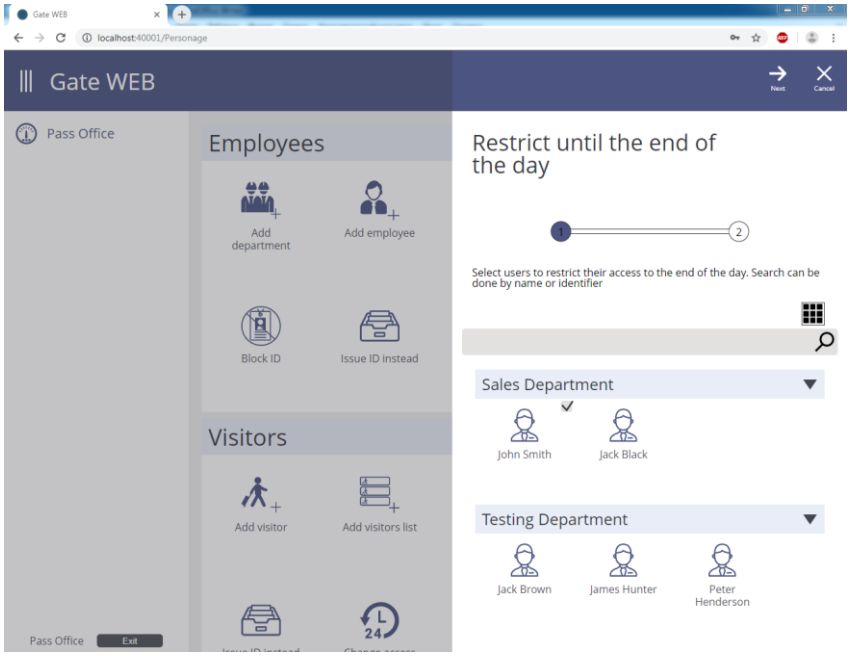


Setting access till the end of day (access time restriction)

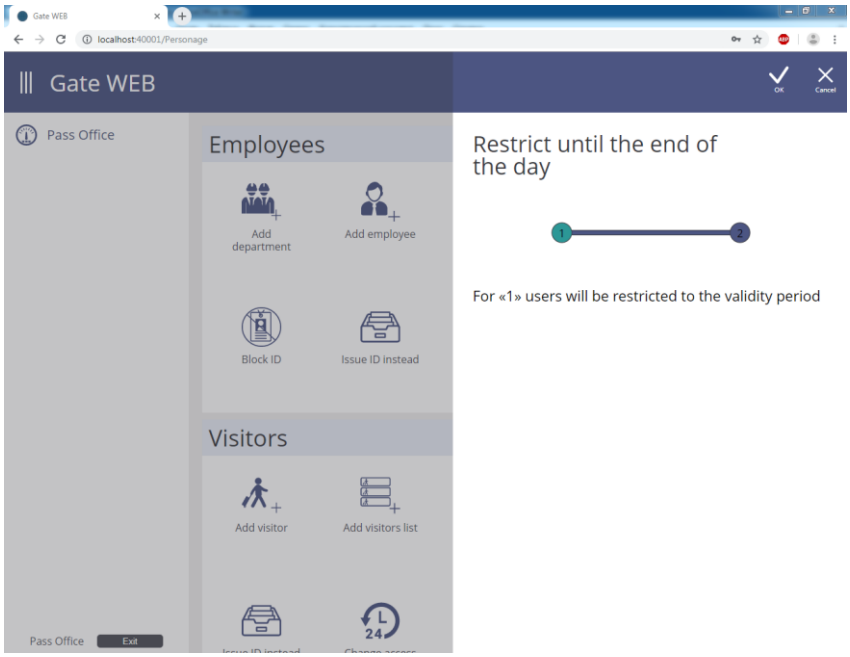
Press ‘Restrict access time’ icon in ‘Employees’ section to set access till the end of day only.

Select employee and press ’Next’.

It is possible to use search by part of name or by ID for quick search.



Press ‘OK’ to restrict access till the end of day.

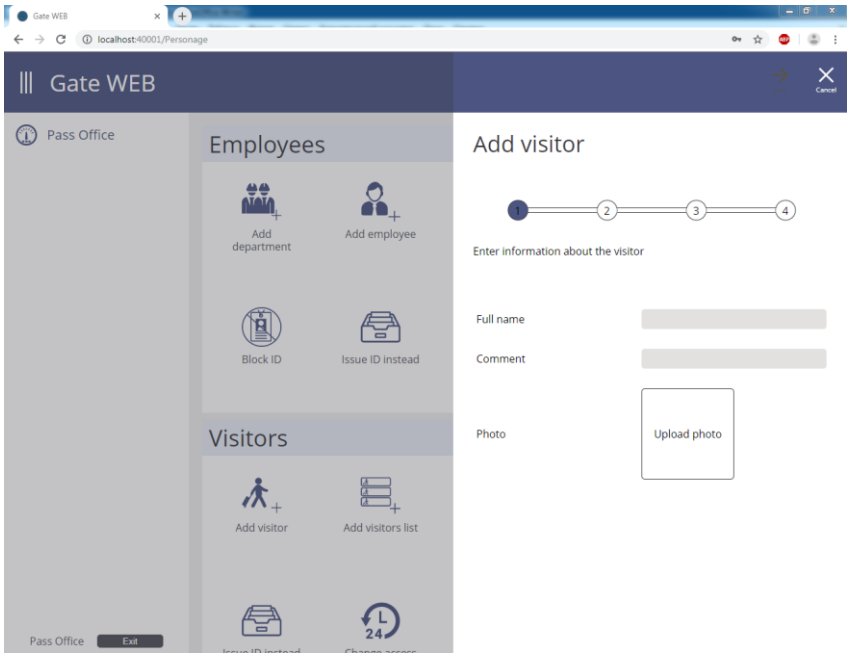


Operations with visitors

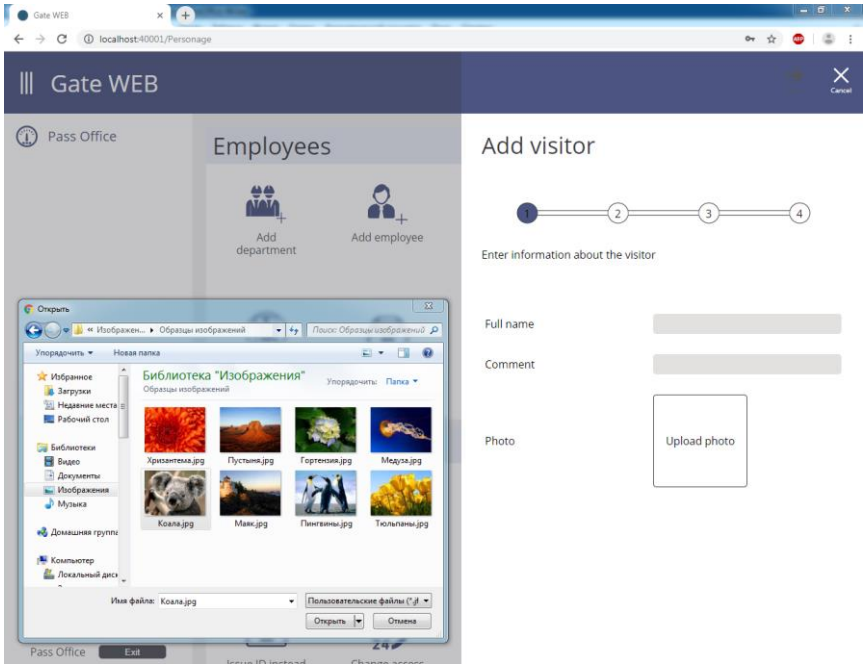
Adding visitors

Press ‘Add visitor’ icon in ‘Visitors’ section to add visitor.

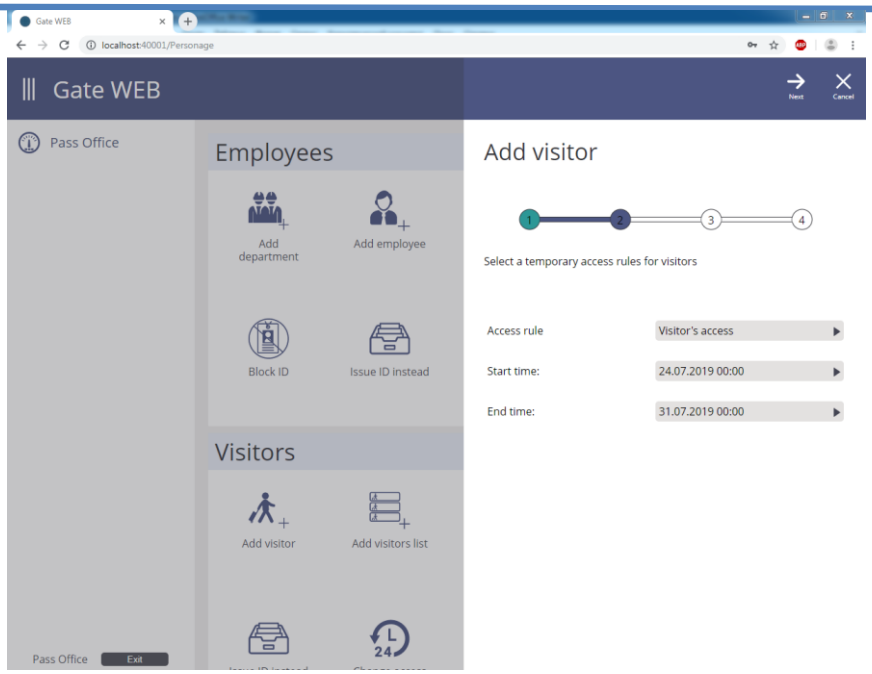
Type visitor name and comment (visit purpose, for instance) in the window displayed.



Click photo form to add visitors photography and select file in the window displayed. Press ‘Next’.

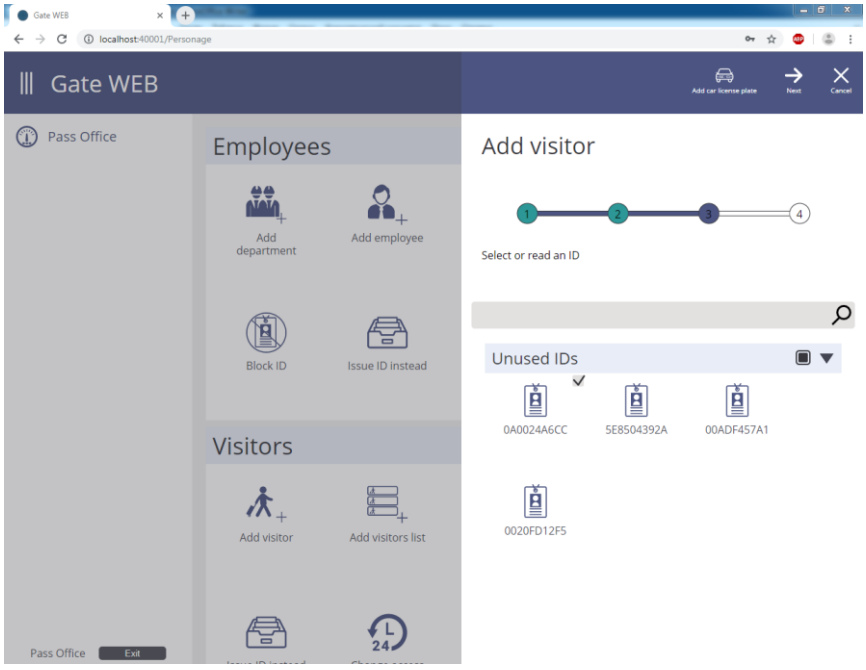


Select access rule and credential validity term in the window displayed.



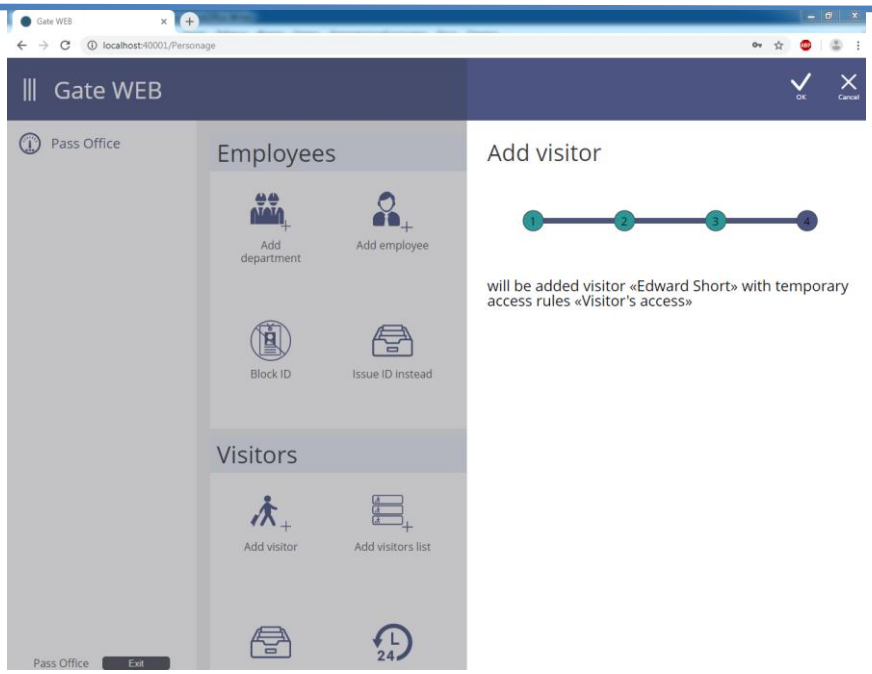
Give to visitor IDs from the list of unused IDs or enroll new.

Select ID enrollment device in ‘Reader selection’ field to enroll new ID.



ID code will display in the window on ID pass to the reader.

Press ‘OK’ to save changes, add ID and activate access for the visitor.

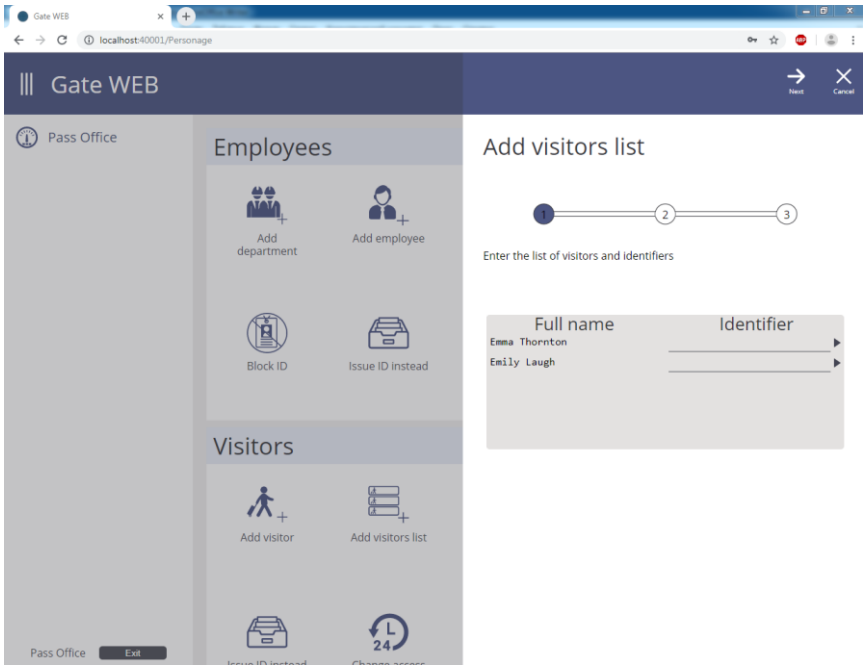


Adding visitors list

Press ‘Add visitors list’ icon in ‘Visitors’ section to add list of visitors quickly.

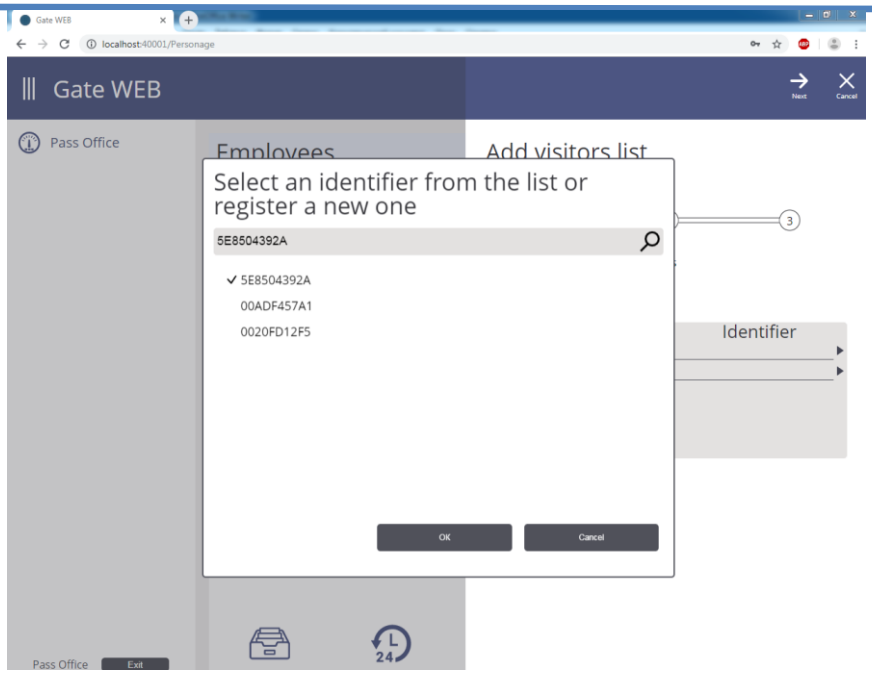
Create file with visitors’ names listed in column beforehand.

Copy visitors list from file to the window displayed:

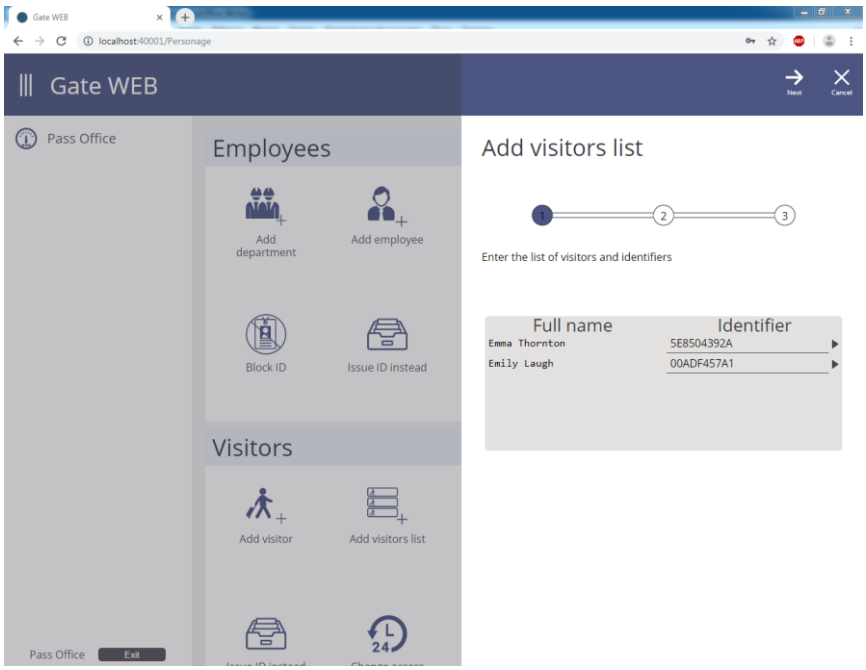


Add IDs for each visitor. To do this, enroll IDs from desktop reader or reader connected to the control panel.

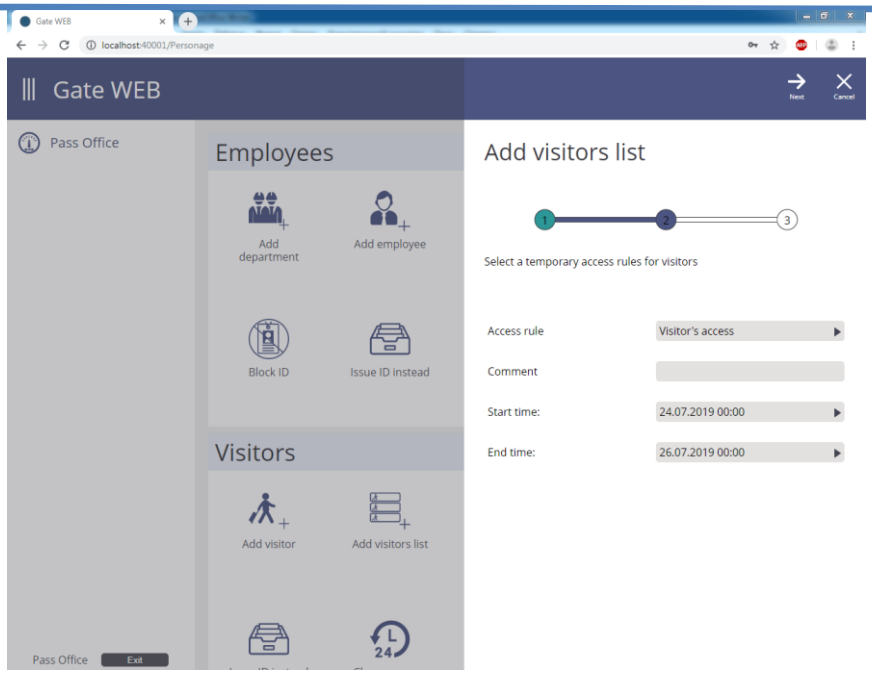
ID enrollment and selection window will open on mouse click on ‘ID’ field. Select ID from the list of unused or enroll new ID and press ‘OK’.



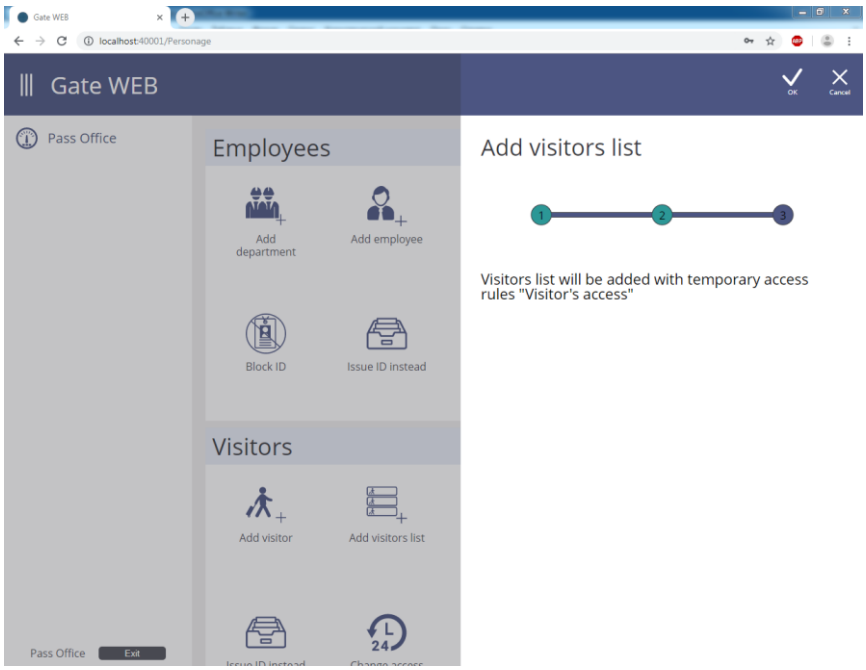
Press ‘Next’ after IDs assigned to all visitors from the list.



Set credential expiry date and access rules in ‘Access rule’ field and press ‘Next’.



Press ‘OK’ to save changes, add and activate access for the list of visitors.

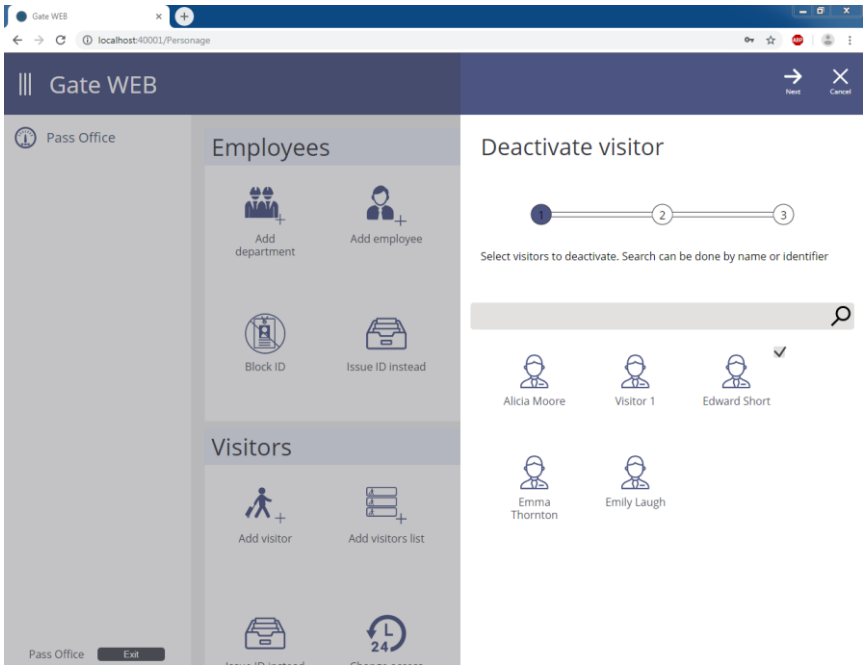


Visitor deactivation

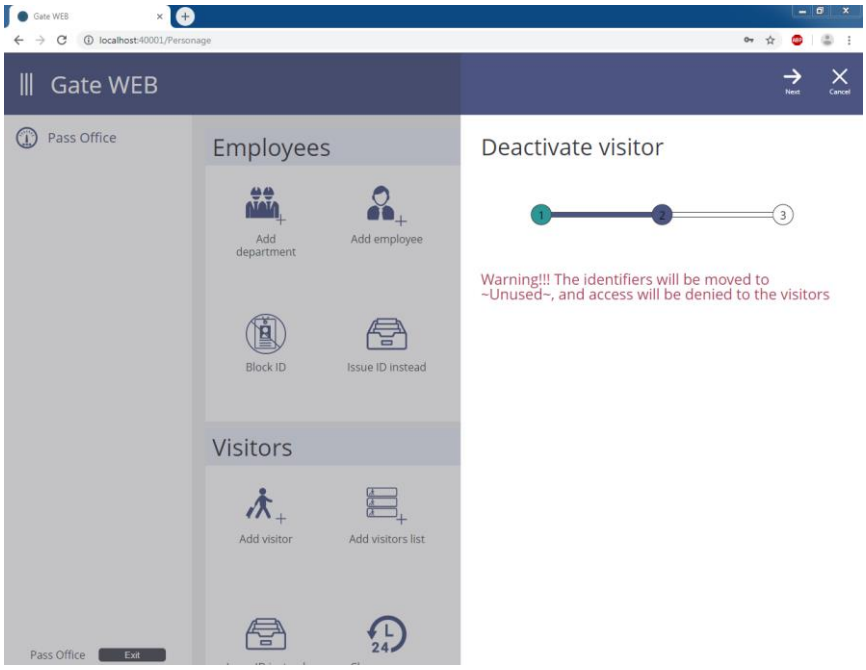
Press ‘Deactivate visitor’ in ‘Visitors’ section to deactivate visitor.

Select visitors for deactivation.

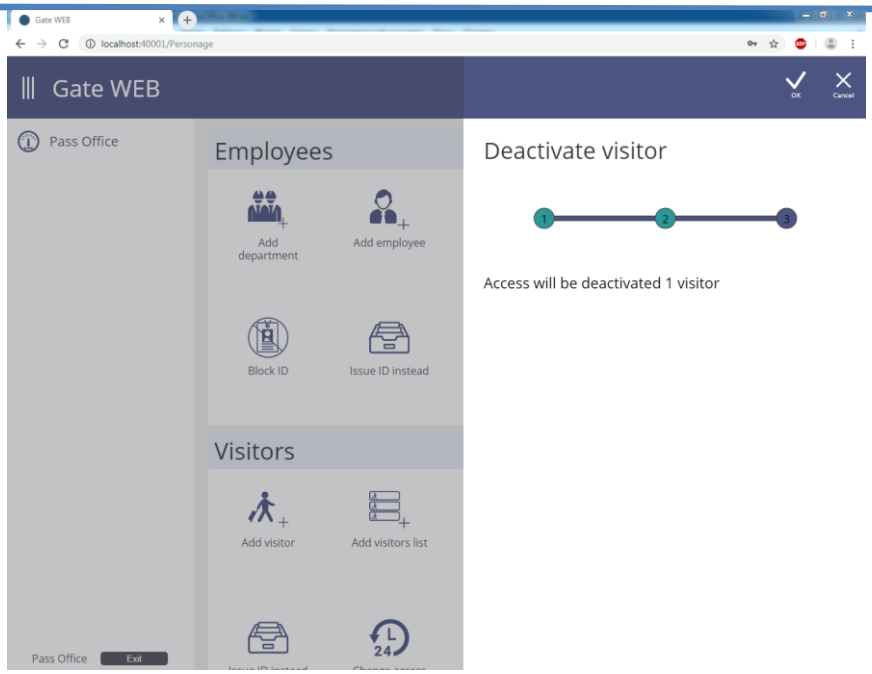
Use search by part of name or by ID for quick visitor search.



Press ‘Next’ to confirm deactivation.



Press ‘OK’ to save changes and deactivate visitor.

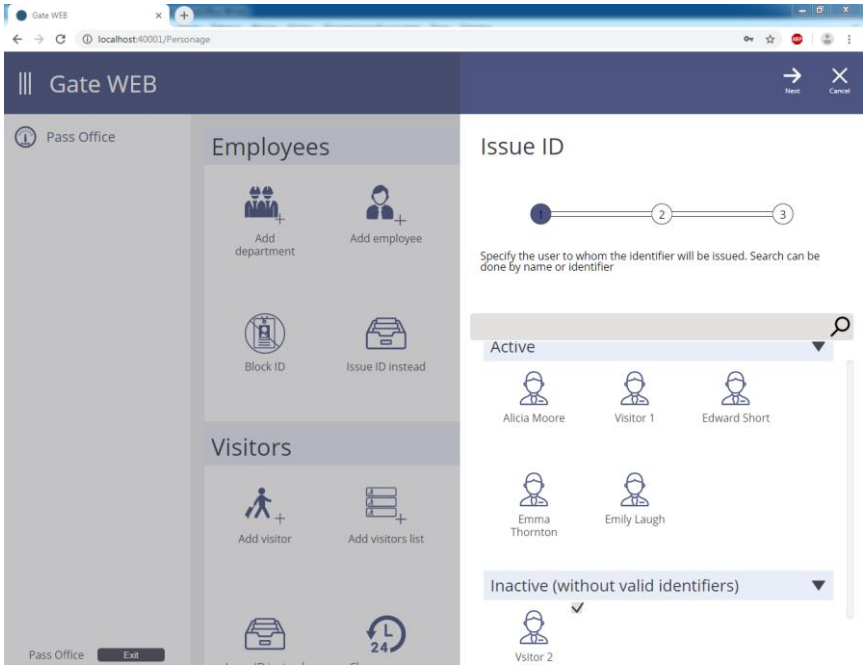


Give ID to visitor

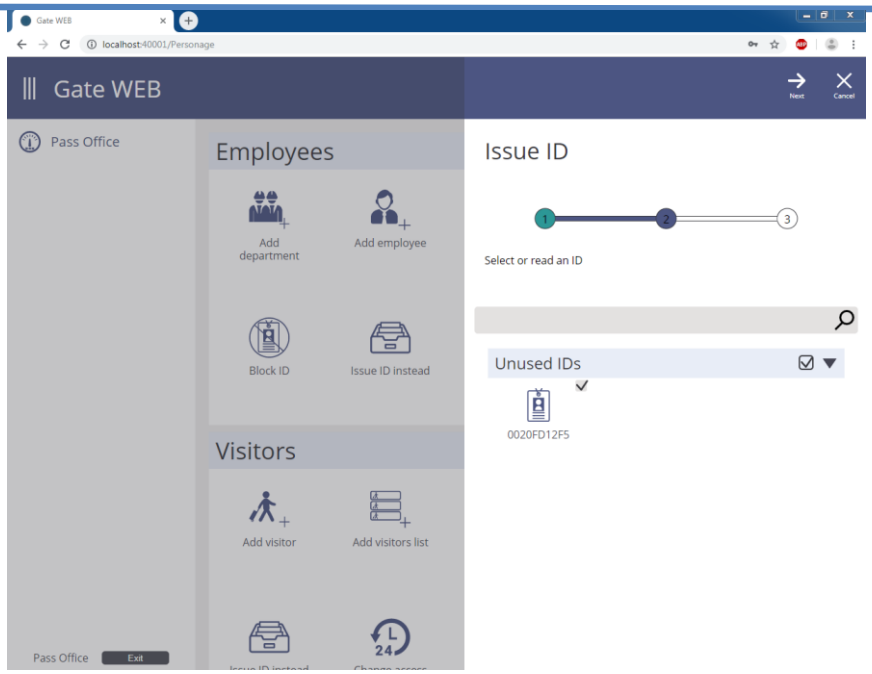
Press ‘Give ID’ icon in ‘Visitors’ section to give ID to visitor.

Select visitor to give him ID.

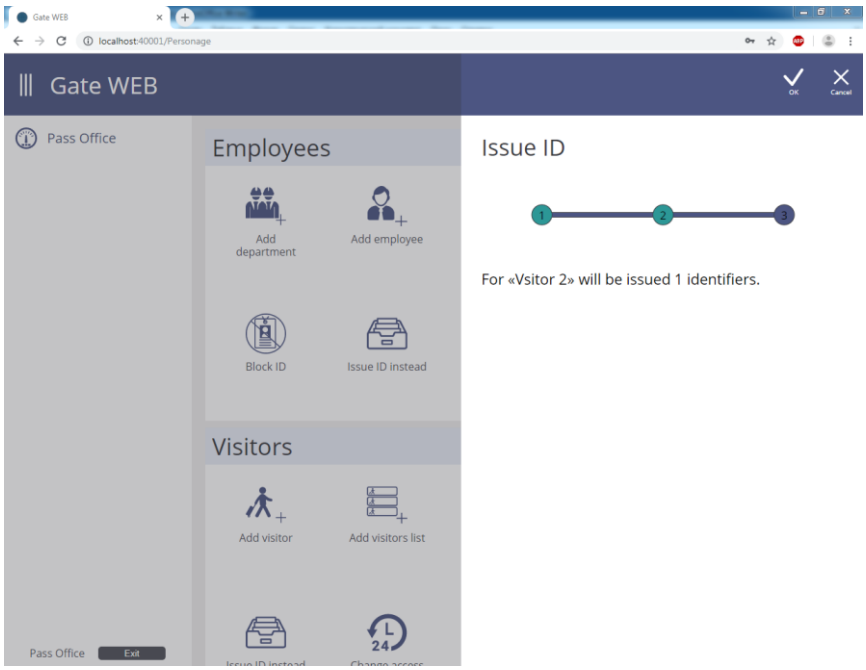
Use search by part of name or by ID for quick visitor search.



Select IDs from list of unused or enroll new to add IDs to visitor.



Press ‘OK’ to save changes and deactivate visitor.

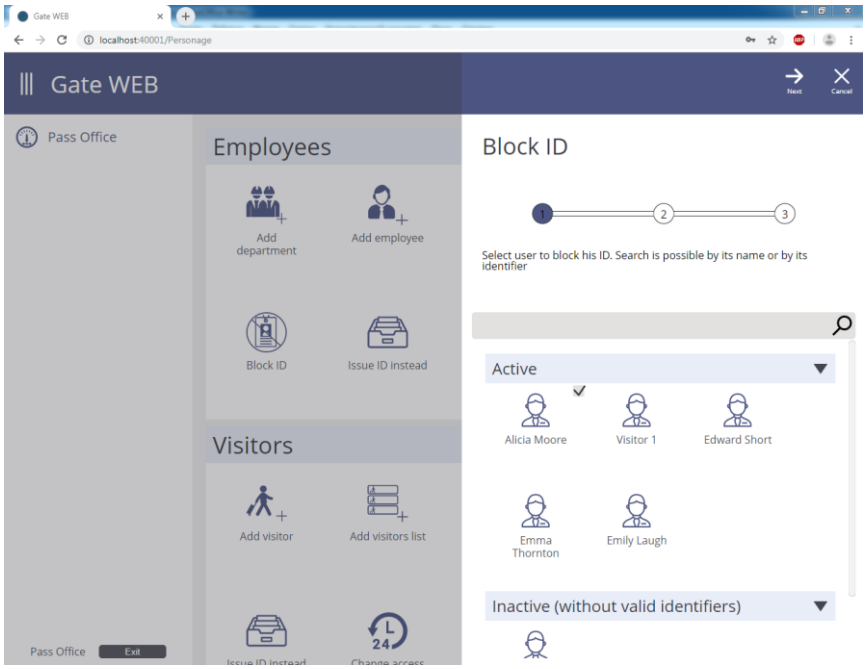


ID blocking

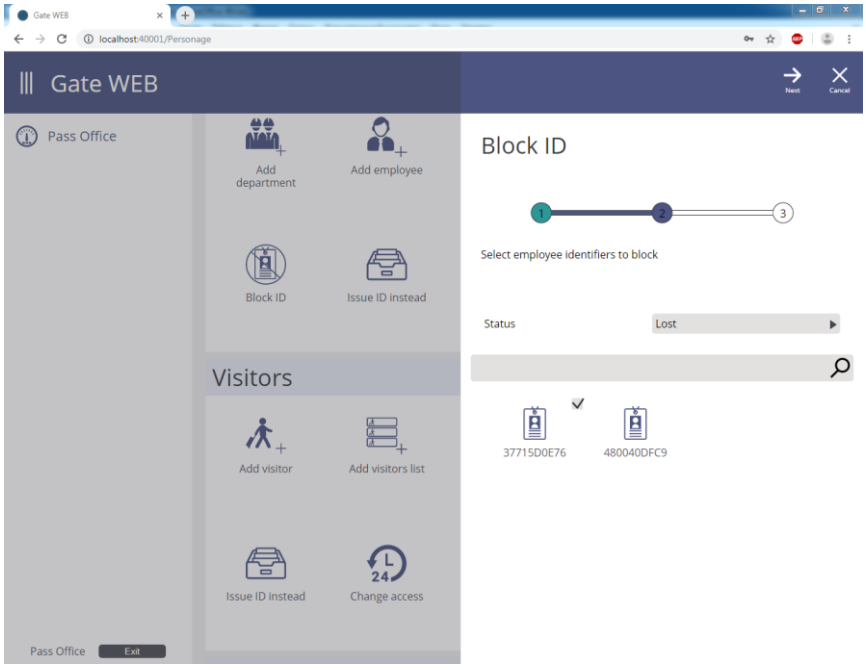
Press ‘Block ID’ icon in ‘Visitors’ section to block visitor’s ID.

Select visitor and press ‘Next’.

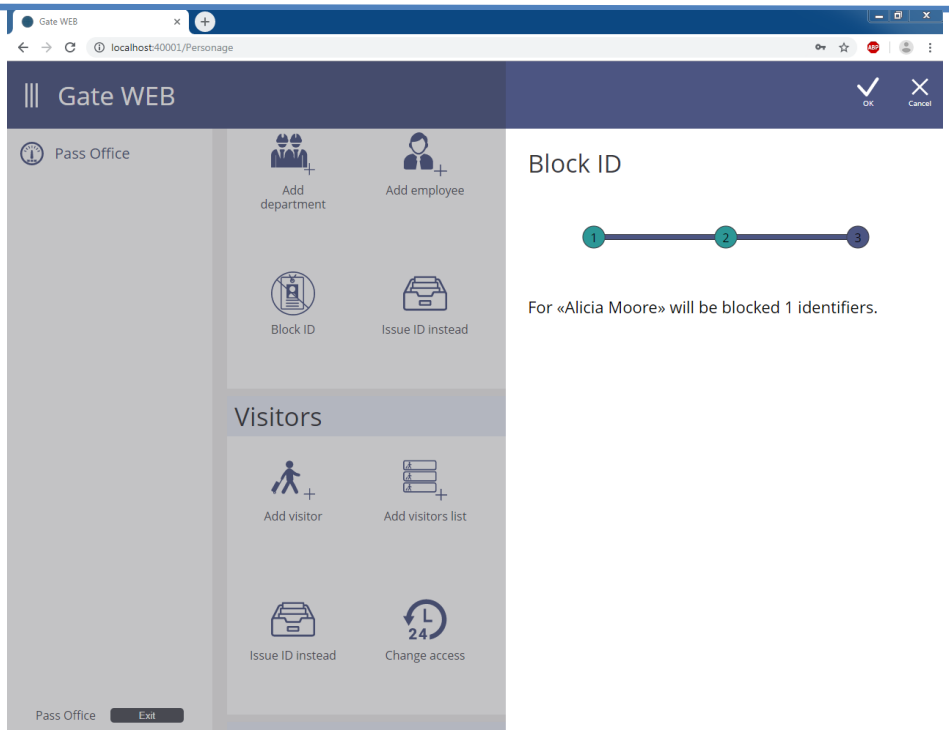
Use search by part of name or by ID for quick visitor search.



Select ID with status for blocking.



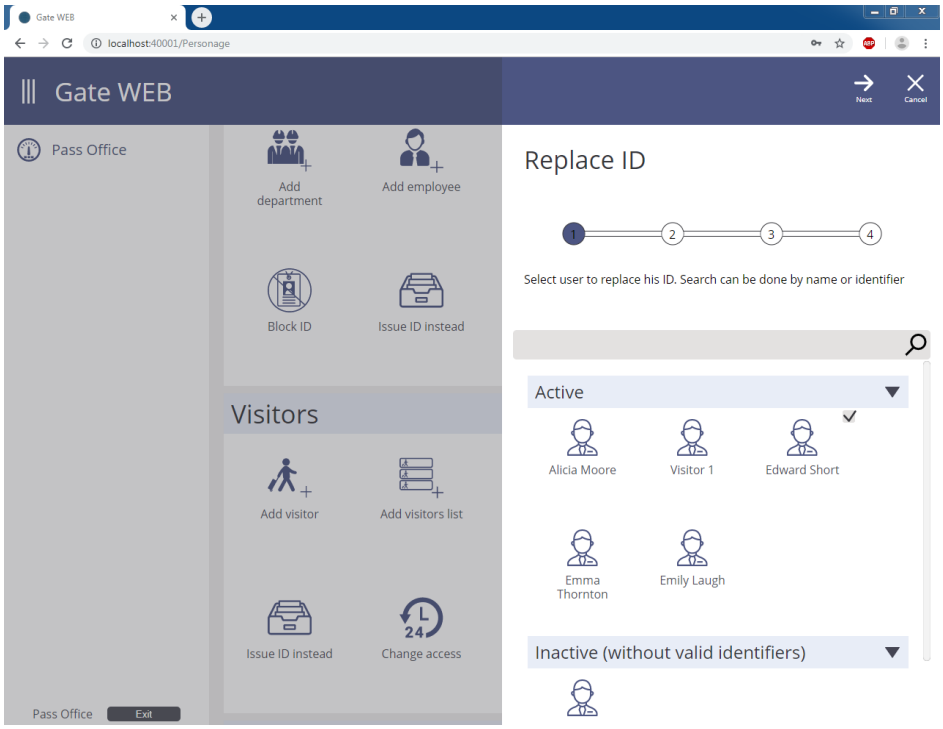
Press ‘OK’ to save changes and block visitor’s ID.



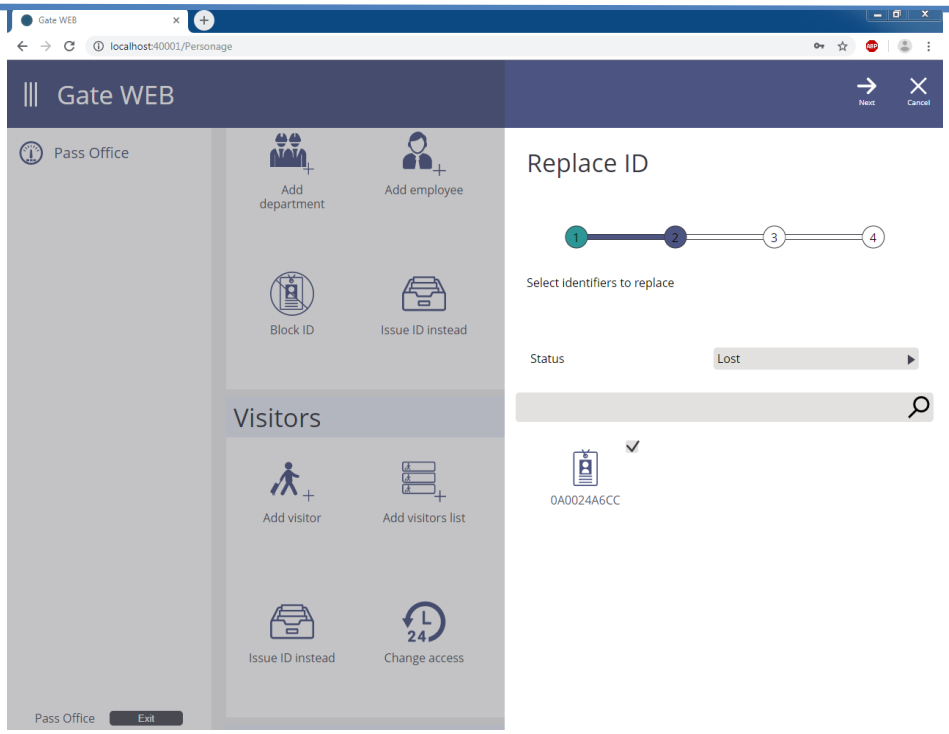
Spoiled or lost ID replacement

Press ‘Replace ID’ icon in ‘Visitors’ section to replace spoiled or lost visitor’s ID.

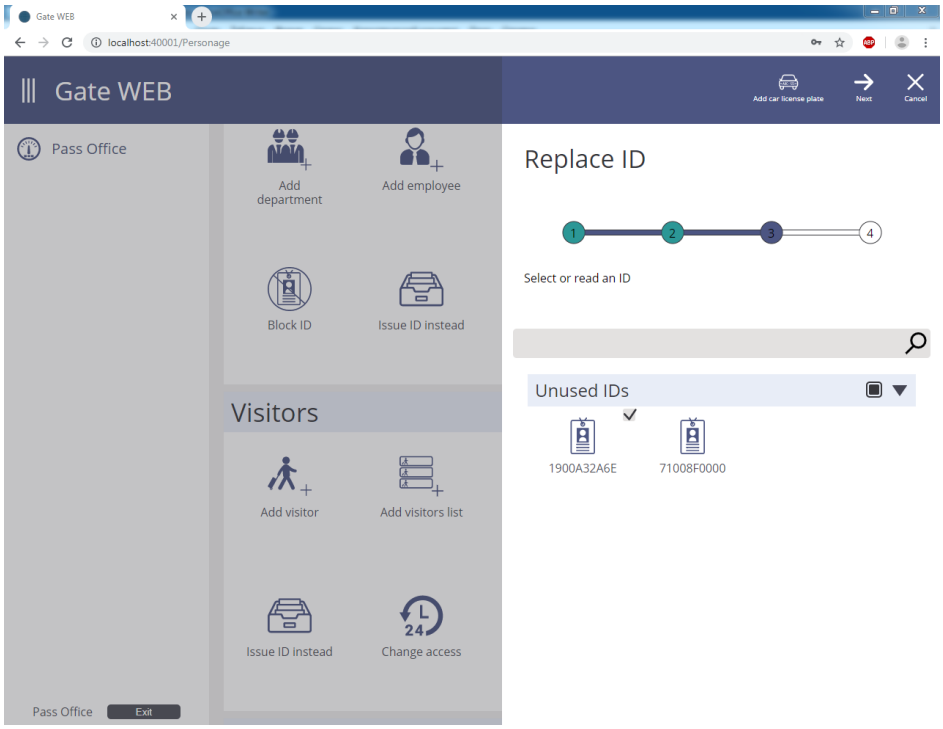
Select visitor for ID substitution.



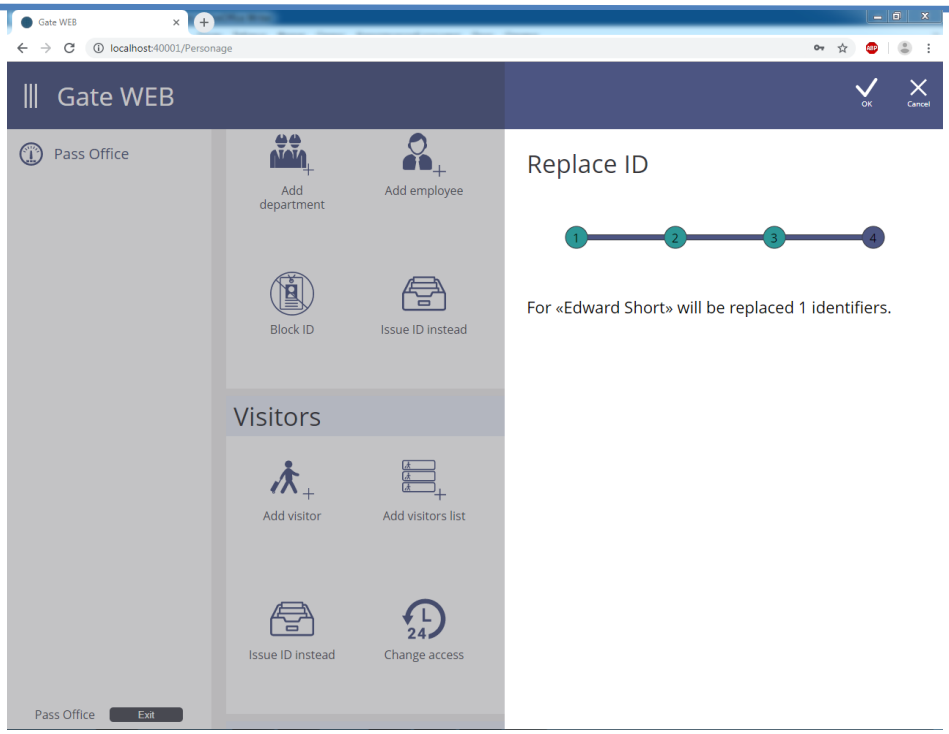
Select ID and its status for substitution.



Give to visitor IDs from the list of unused IDs or enroll new.



Press ‘OK’ to replace visitor’s ID and save changes.

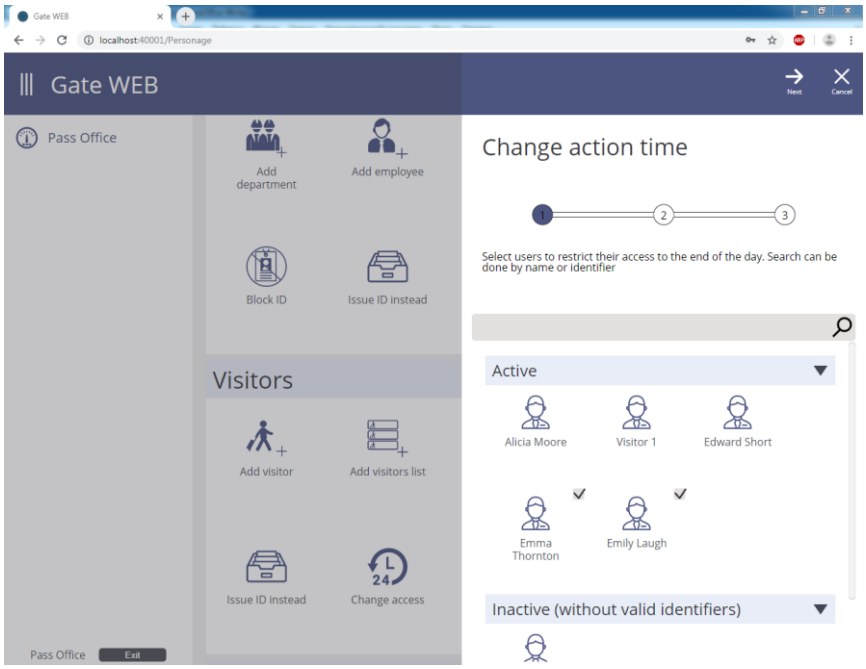

Gate WEB
localhost:40001/Personage
Gate WEB
OK
Cancel
Pass Office
Add department
Add employee
Block ID
Issue ID instead
Visitors
Add visitor
Add visitors list
Issue ID instead
Change access
Pass Office
Exit
Replace ID
1
2
3
4
For «Edward Short» will be replaced 1 identifiers.

Changing access rights

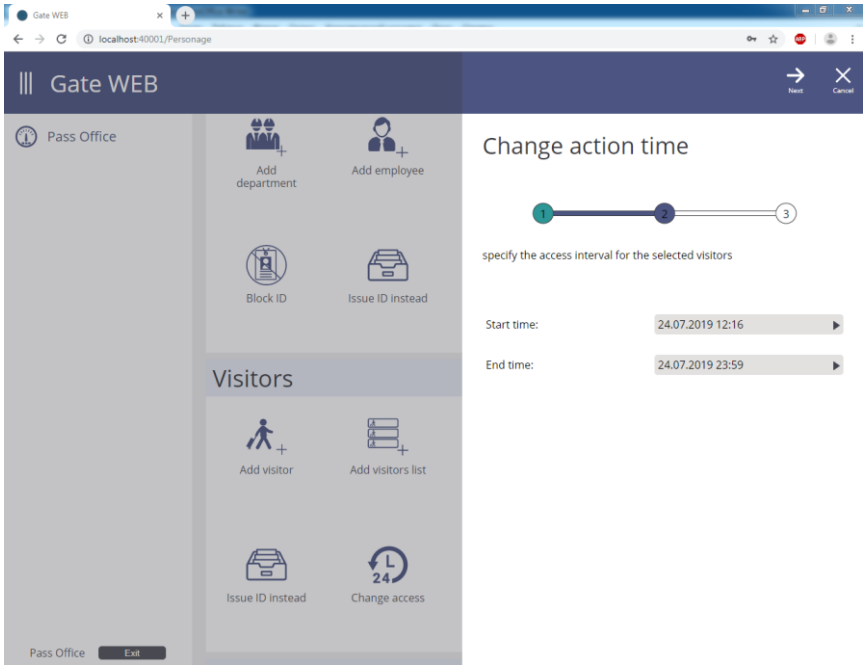
Press ‘Change access’ icon in ‘Visitors’ section to set new credential expiry date.

Select visitor and press ‘Next’.

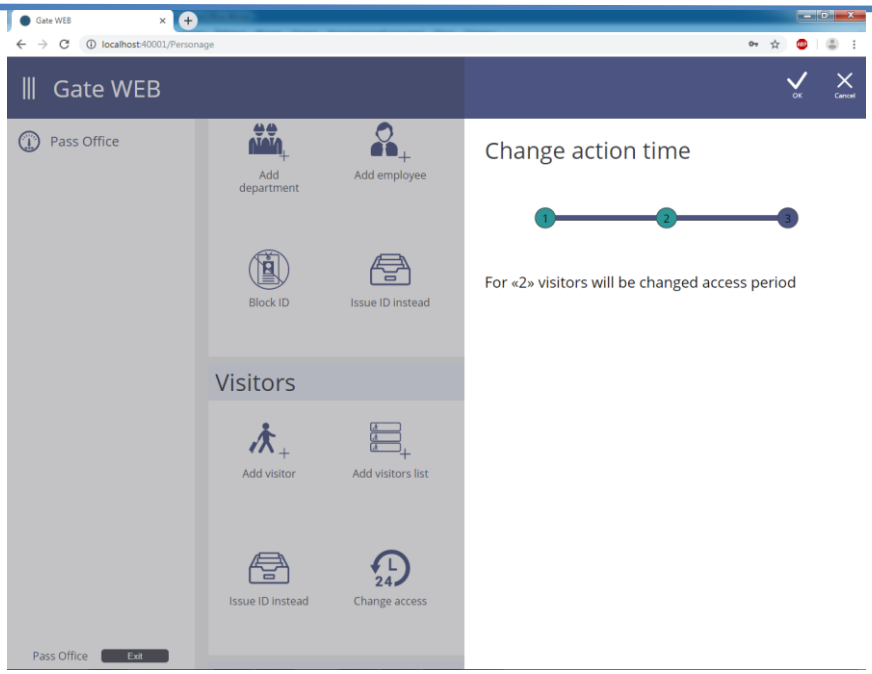
Use search by part of name or by ID for quick visitor search.



Set new credential expiry date.



Press ‘OK’ to replace visitor’s access rights and save changes.

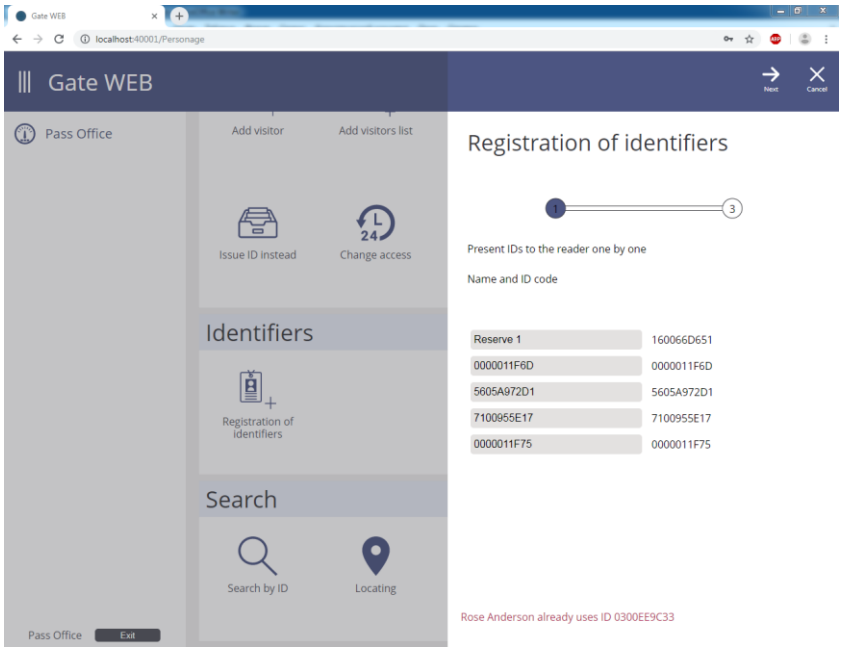


IDs enrollment

Press ‘Enroll IDs’ in ‘Identifiers’ section to enroll IDs into the system. System will place identifiers into unused IDs’ list.

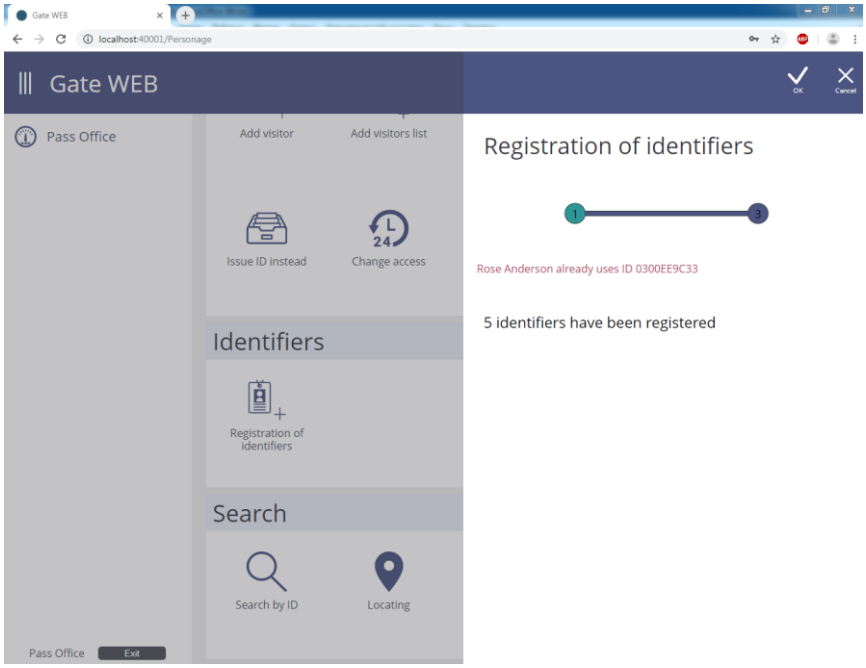
ID’s code displayed in the window on ID pass to the reader. System will warn about duplicate cards.

Operator can change the card name.



Set options for enrolled IDs in window displayed.

Press ‘OK’ to save changes.

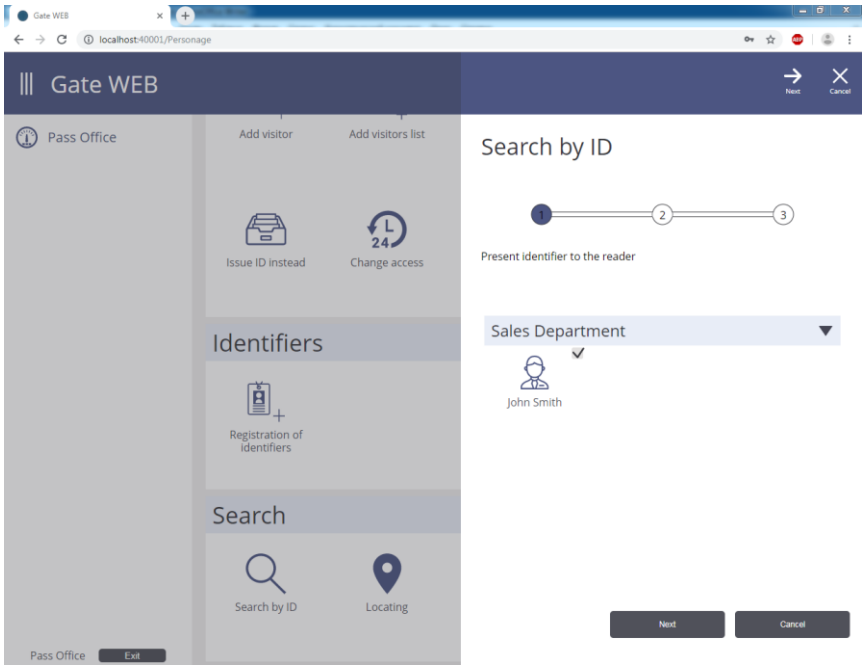


Search operations

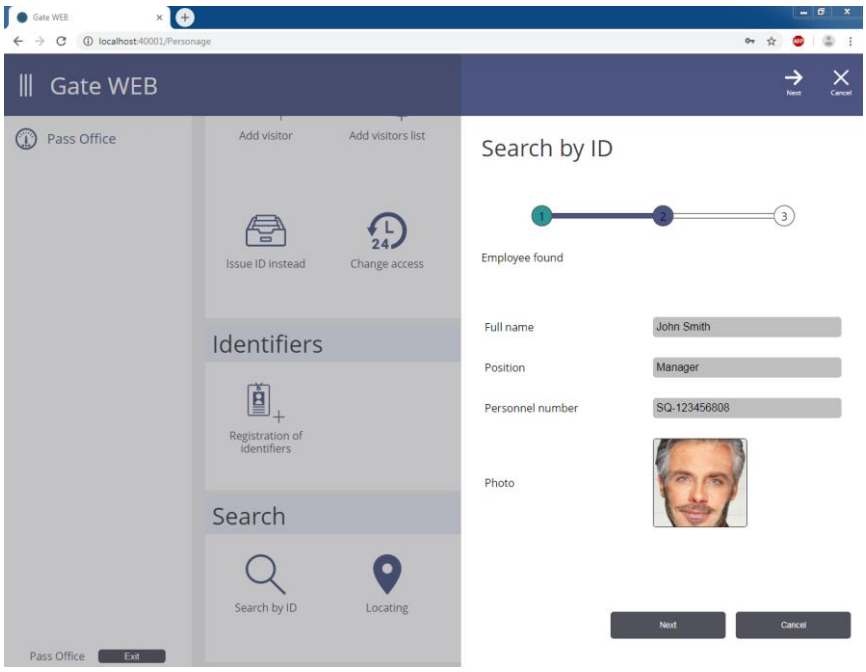
Search by ID

‘Search by ID’ function purpose is to find employee or visitor by his ID.

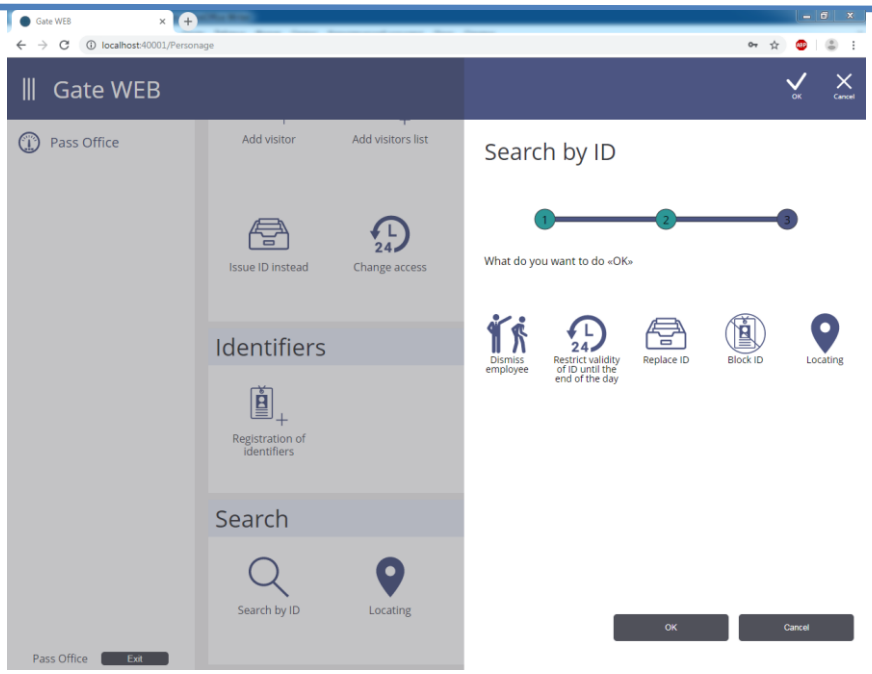
Press ‘Search by ID’ icon in ‘Search’ section. Pass ID to the reader. Employee or visitor data will display. Press ‘Next’.



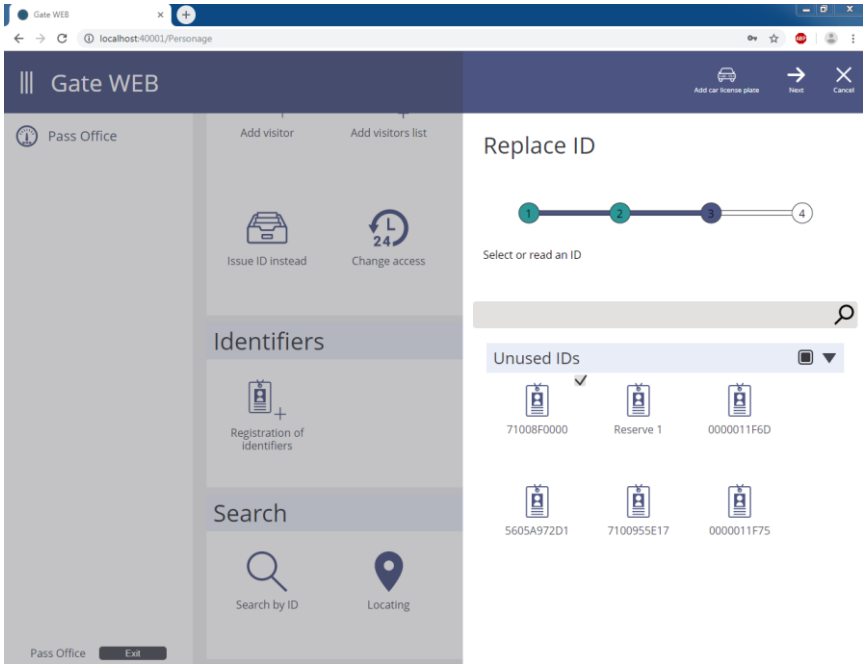
Employee or visitor data will display. Press ‘Next’.



Operator may perform additional operation on found employee’s data. Change ID, for instance:



Corresponding wizard window will open after operation selected and ‘OK’ button pressed.

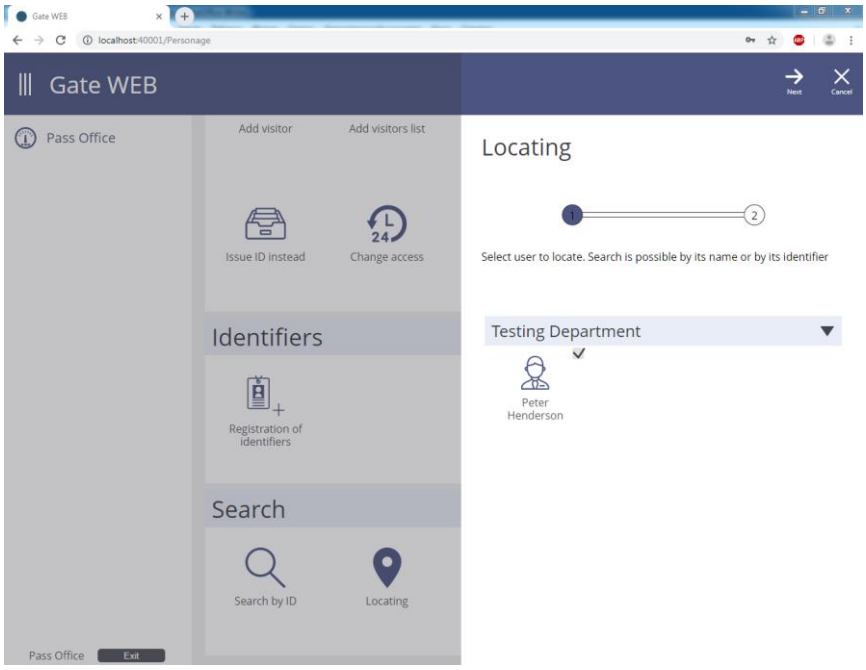


ID position

‘ID position’ function displays the last place where employee’s ID was used.

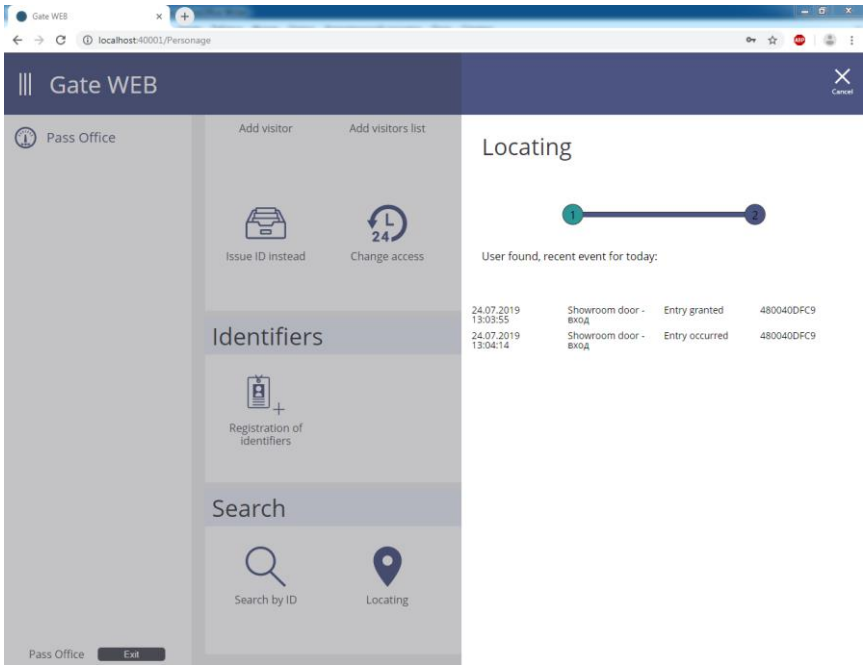
Press ‘ID position’ in ‘Search’ section.

Select employee in window displayed and press ‘Next’.



Search by part of the name or ID available.

Last reported employee ID passes will display.

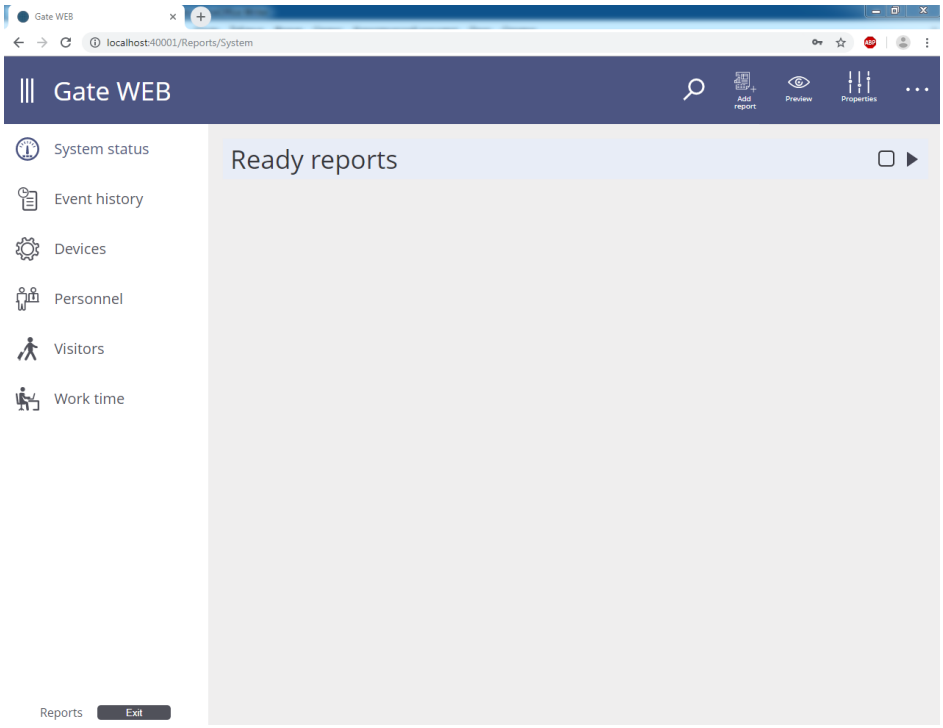


Report generation. ‘Reports’ role.

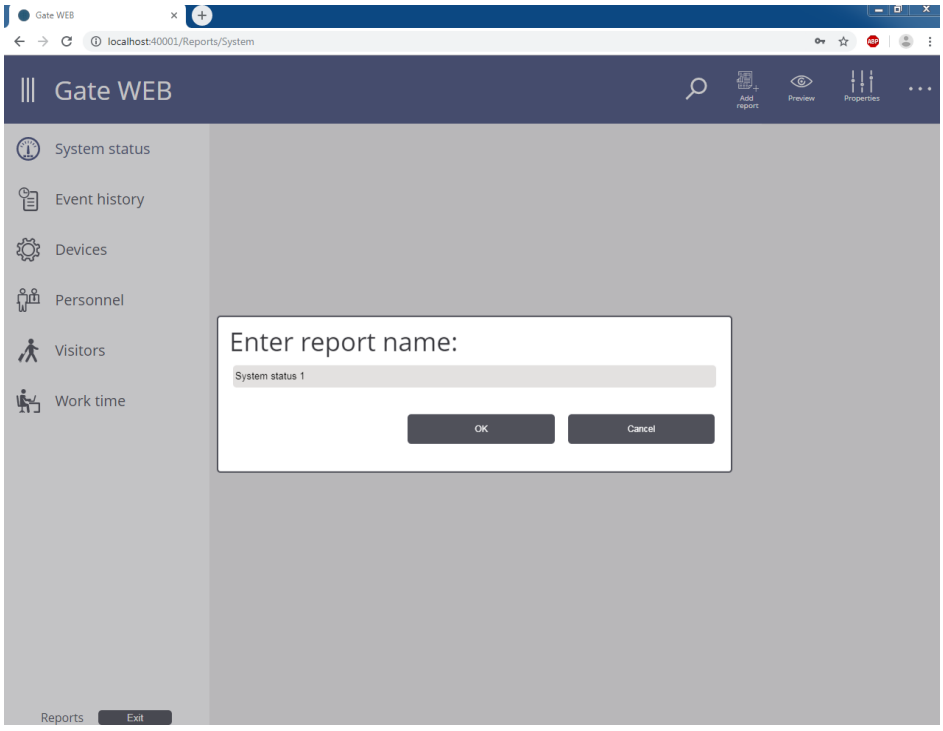
’System state’ report

This report contains convergent information about state of all doors and devices in the system.

Press ‘Add report’ item in ‘System state’

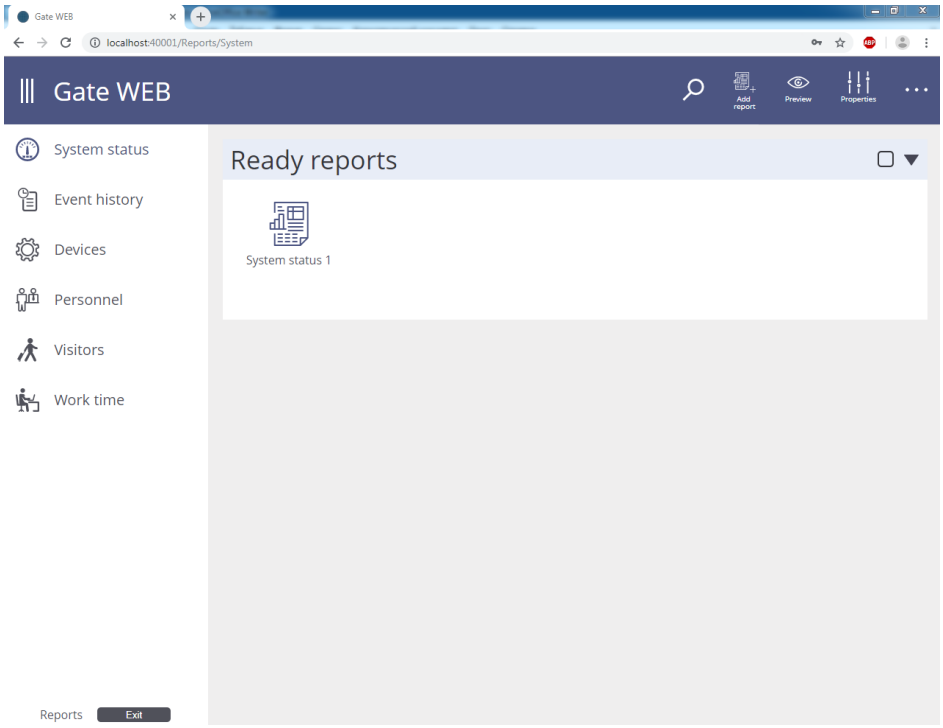


Type report name in window displayed and press ‘OK’.

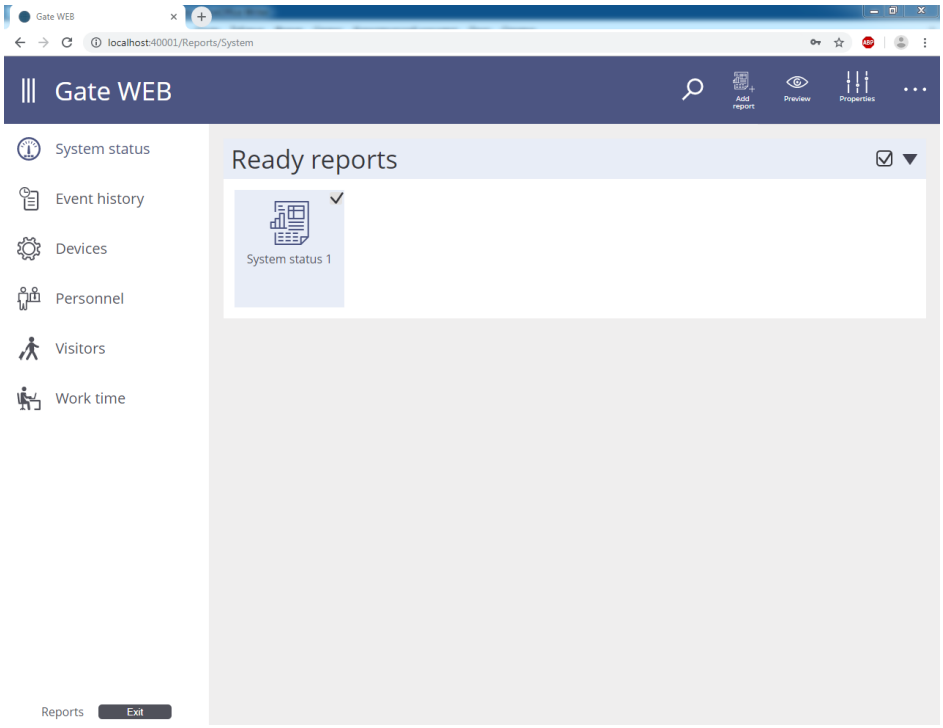


System will start report generation. Unfinished report placed into ‘Reports in progress’ category.

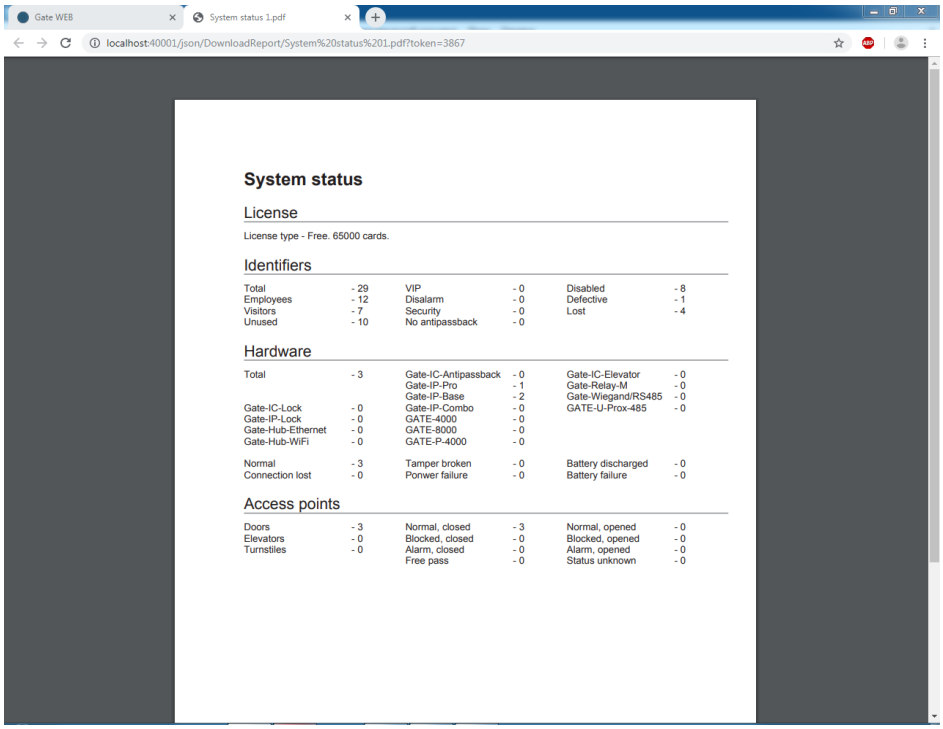
System places finished report into ‘Finished reports’ category:



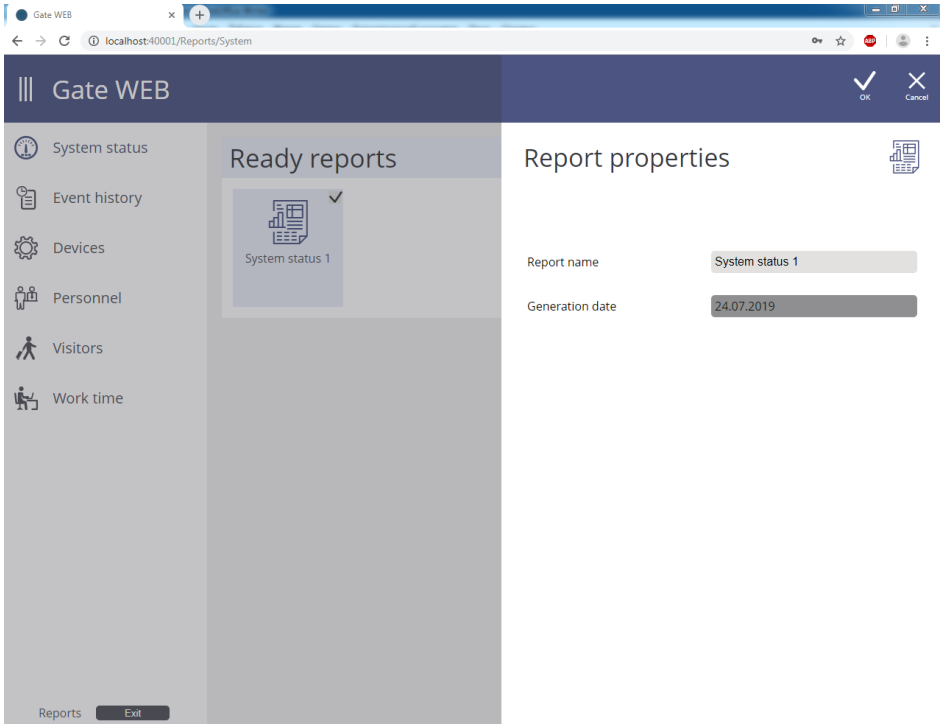
Check □ report and press ‘View’ menu item to view report:



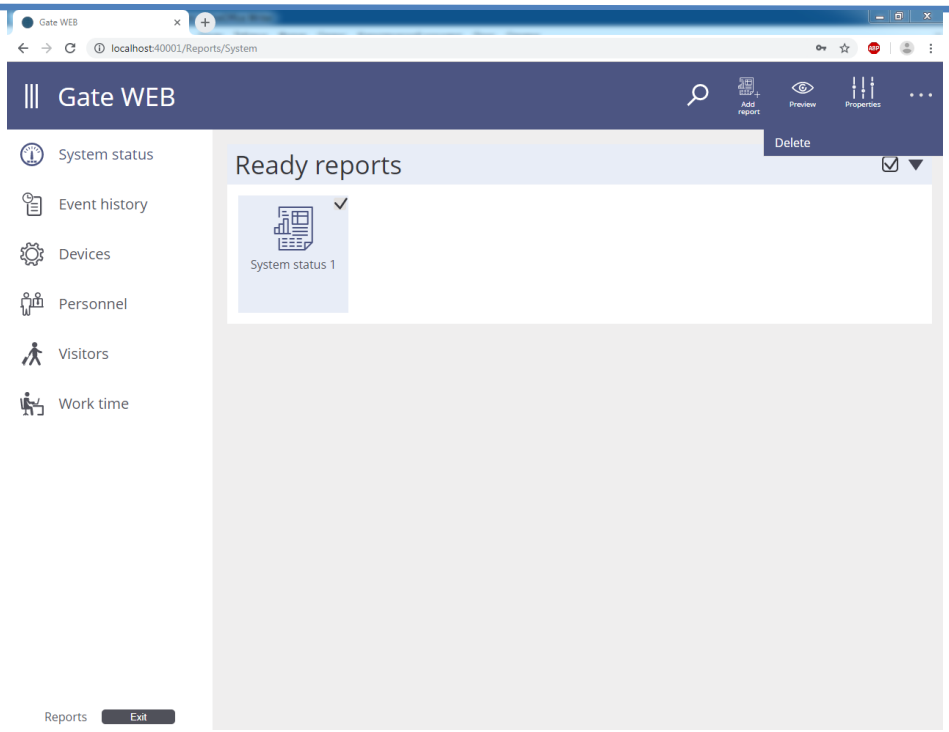
Final report opened in separate window or tab of the browser in .pdf format. It is possible to save or print it with standard browser means.



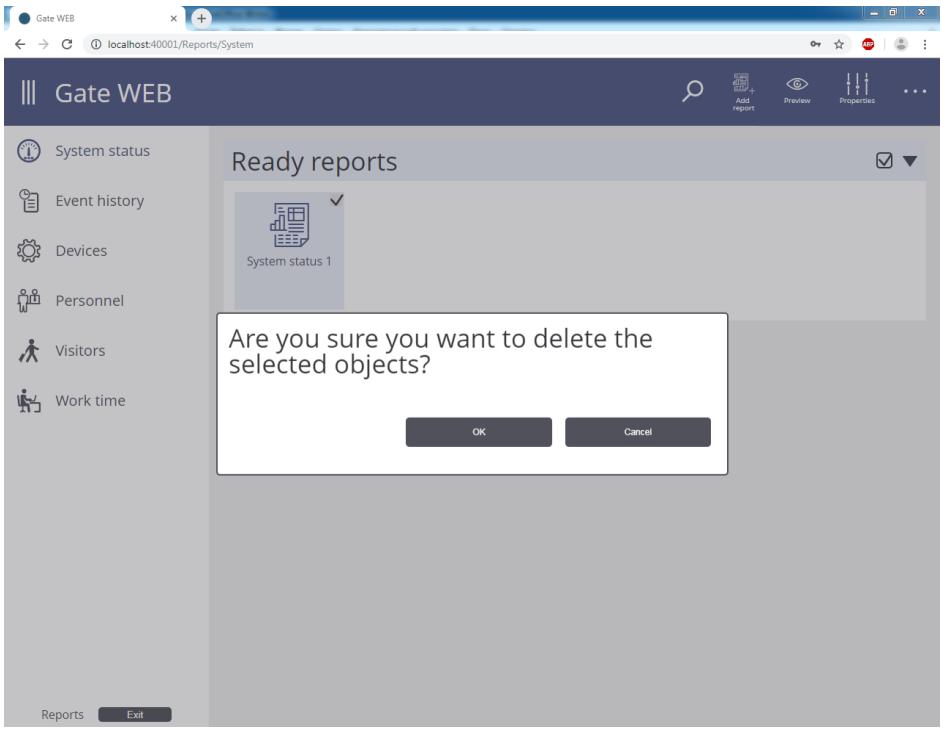
Check □ report and select ‘Properties’ menu item to change report name:



Check □ report and select ‘Delete’ menu item to delete report:



Confirm deletion in window displayed – report deleted permanently.

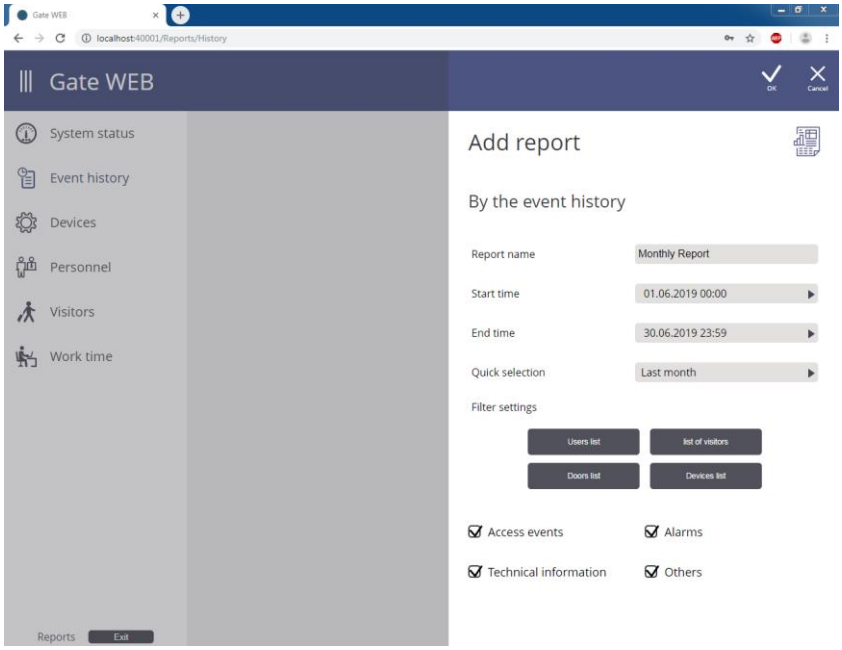


’Event history’ report

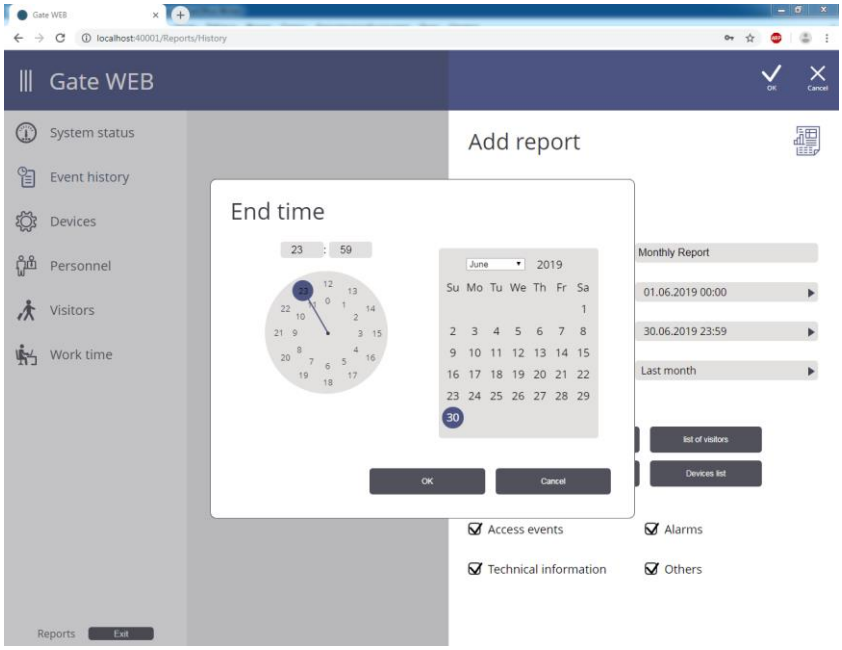
Event history report is extract from the system event log. It is necessary to specify date and time of start end date and time of end of the report period, set of employees, devices and event types to include into report.

Choose ‘Event history’ and select ‘Add report’ menu item.

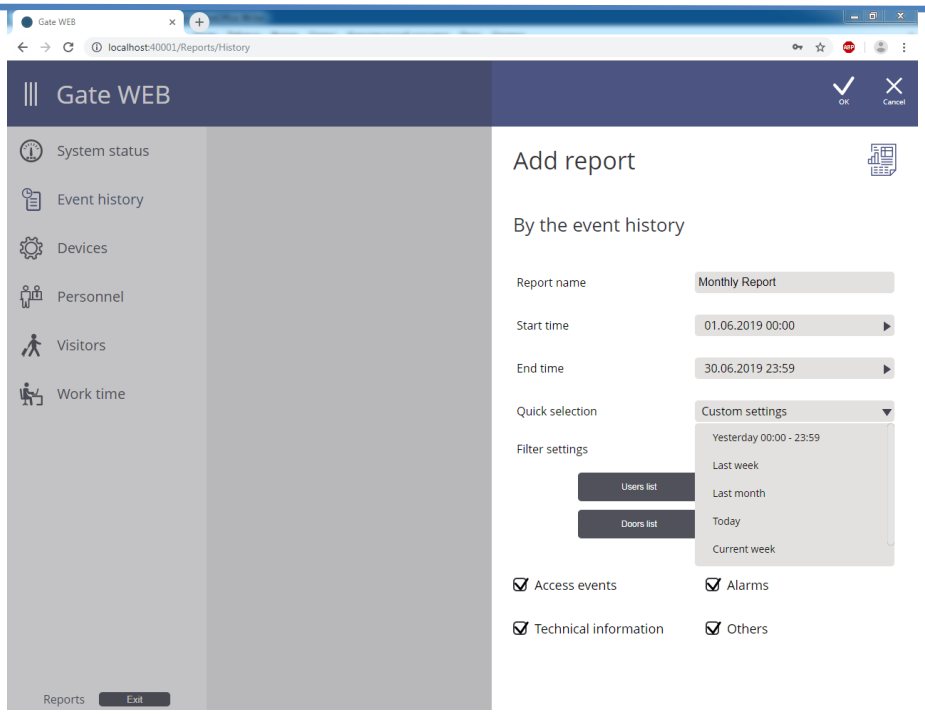
Type report name in window displayed



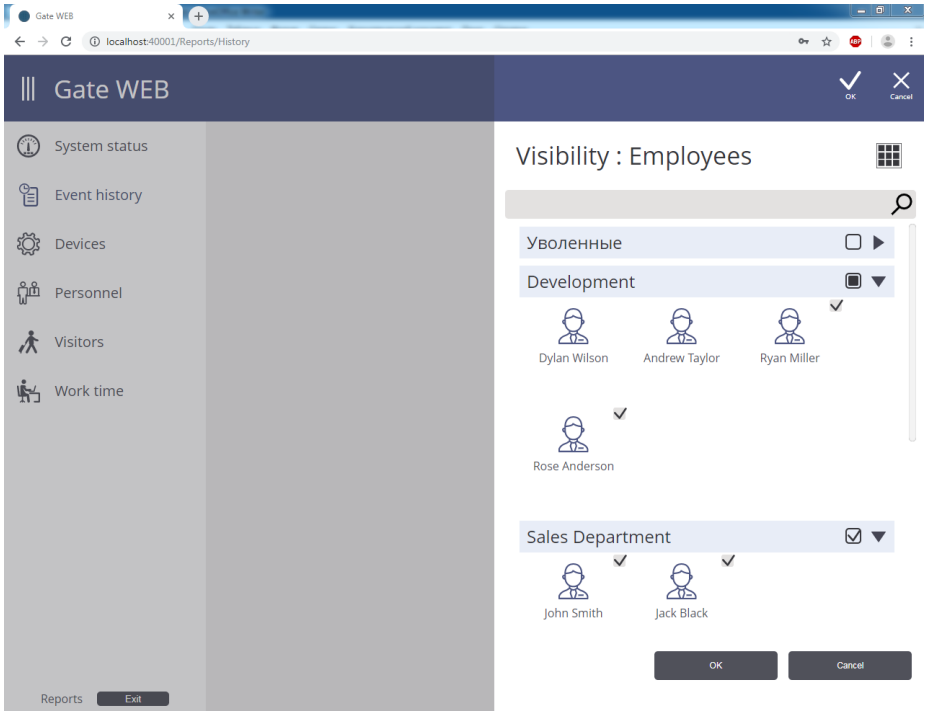
Specify dates of start and end of report period manually



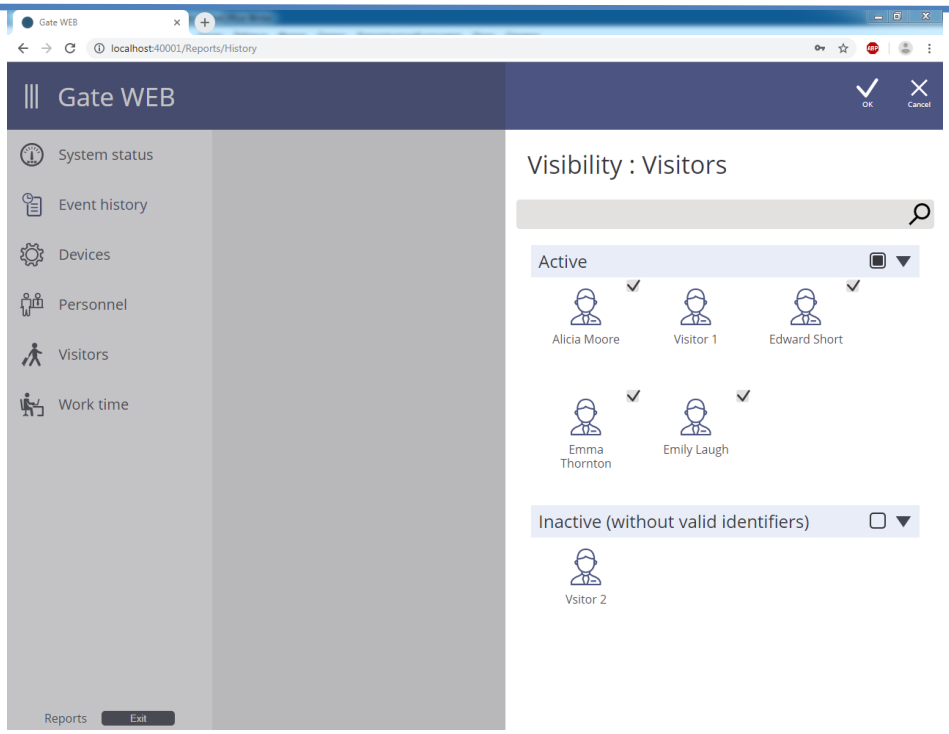
Or use period interval presets from ‘Quick selection’ list:



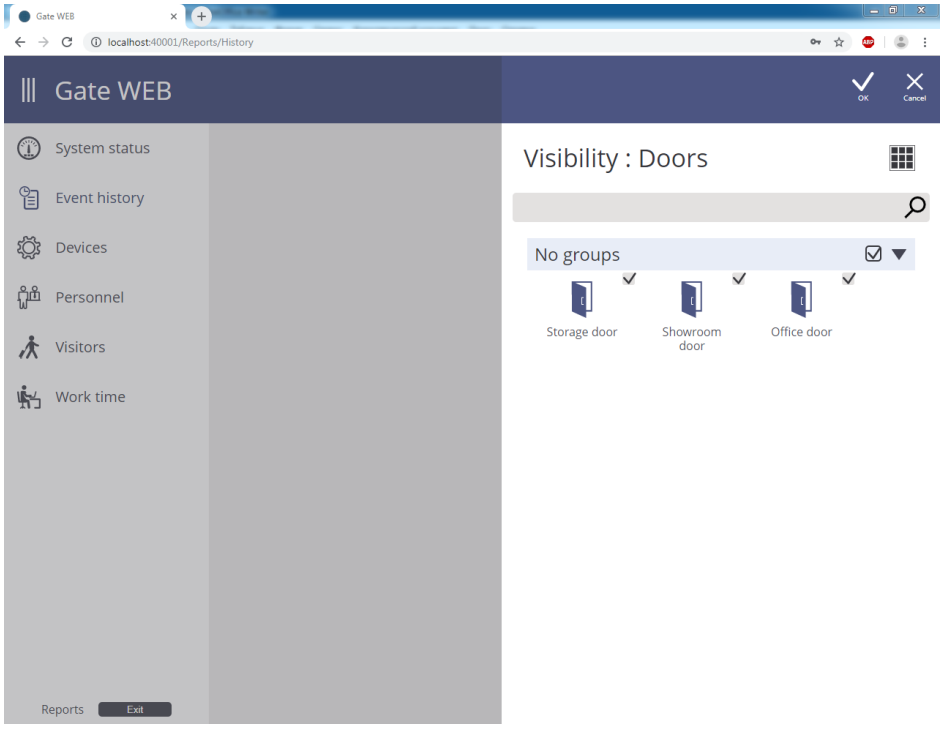
To exclude certain employees from the report, press ‘Employees list’ button, remove check next to the employees name to exclude and press ‘OK’.



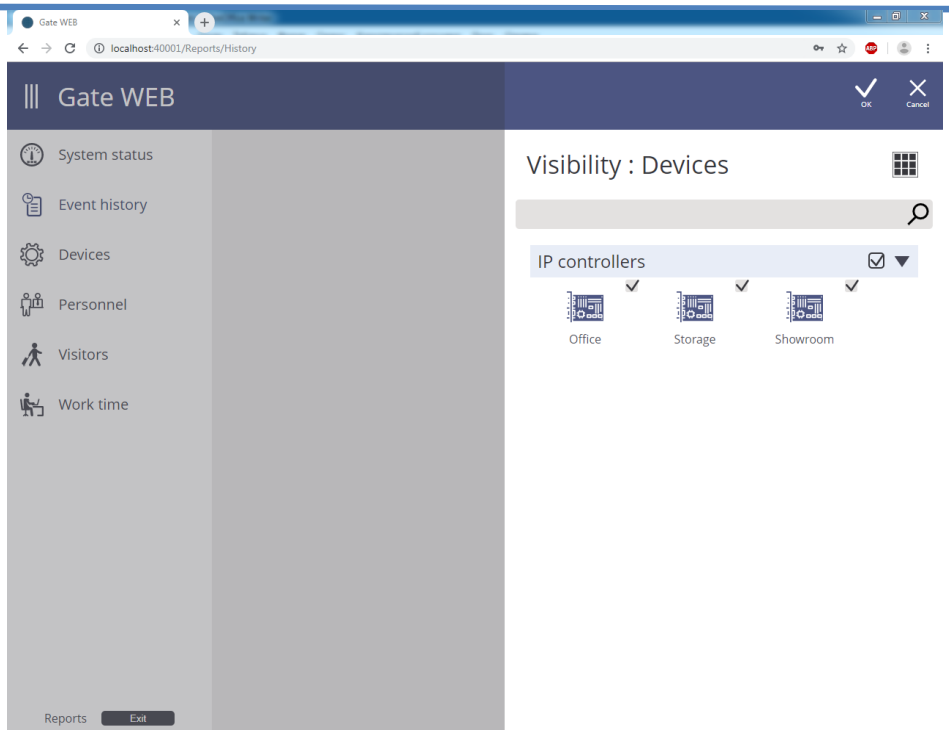
To exclude certain visitors from the report, press ‘Visitors list’ button, remove check next to the visitors name to exclude and press ‘OK’.



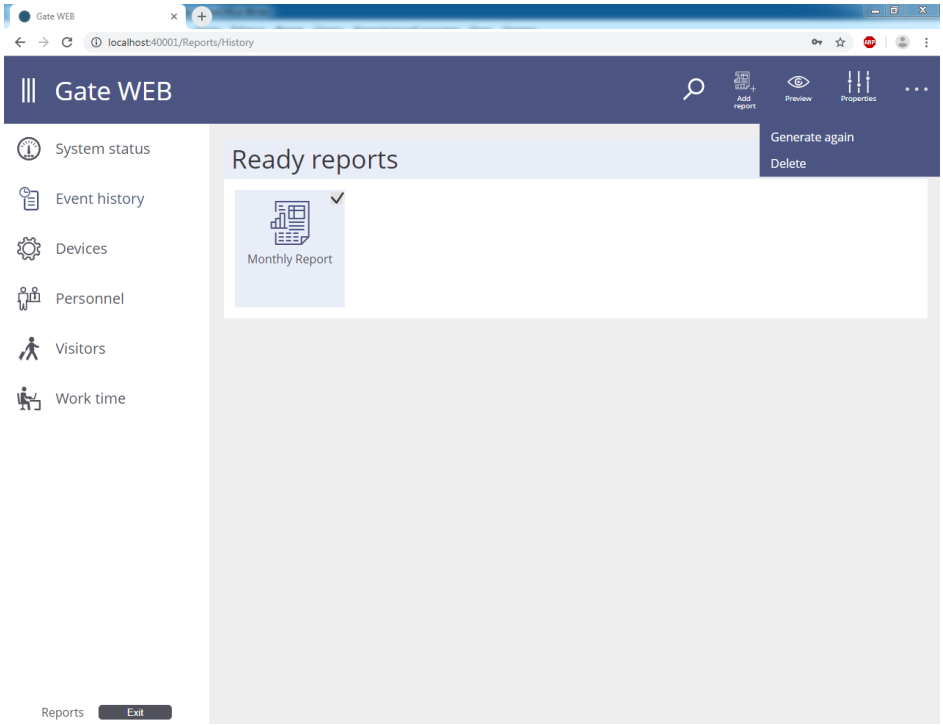
To exclude certain doors from the report, press ‘Doors list’ button, remove check next to the doors to exclude and press ‘OK’.



To exclude certain devices from the report, press ‘Equipment list’ button, remove check next to the device to exclude and press ‘OK’.

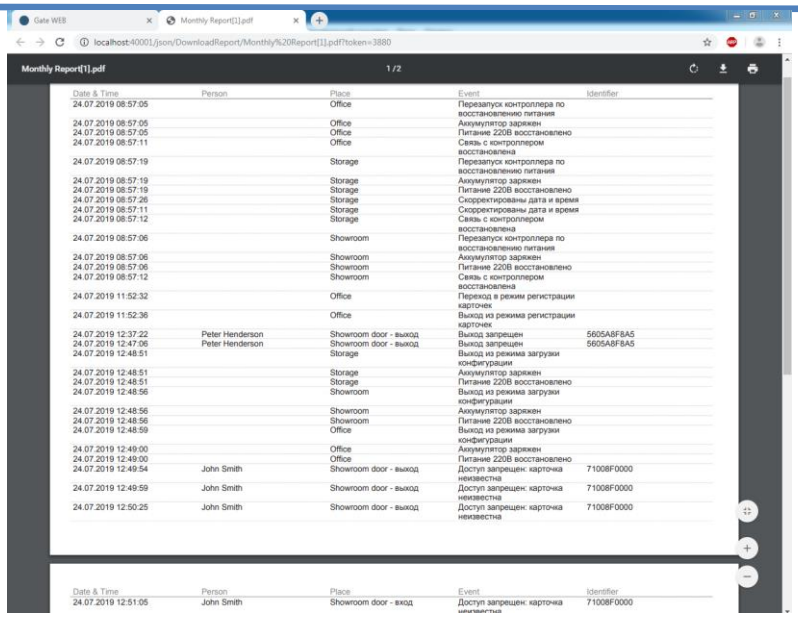


System will start report generation after ‘OK’ press and place it into ‘Generation in process’ category. Report placed into ‘Ready reports’ after generation finished.



Select □ report and press ‘View’ menu item to view .

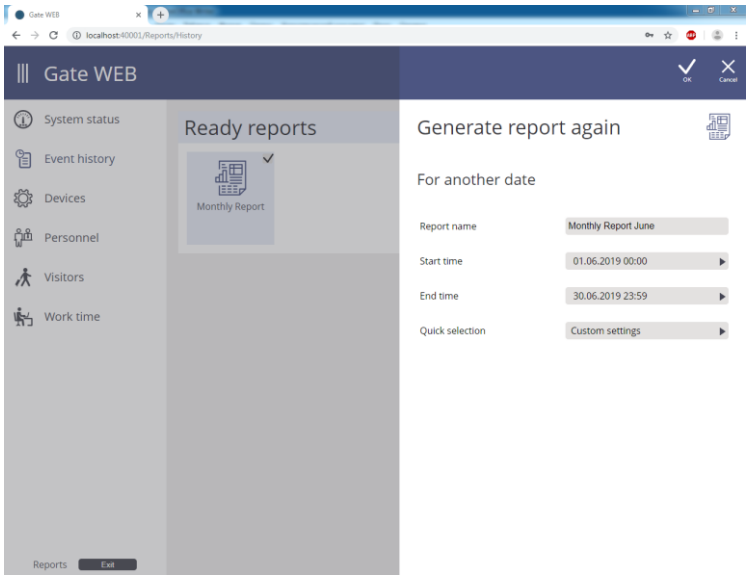
Ready report in .pdf format will be displayed in separate browser window/tab. Save it with standard browser purposes.



Check □ report and press ‘Delete’ menu item to delete report. Confirm action in the window displayed. Report will be deleted permanently.

Check □ report and press ‘Properties’ menu item to rename it. Type new name in the window displayed.

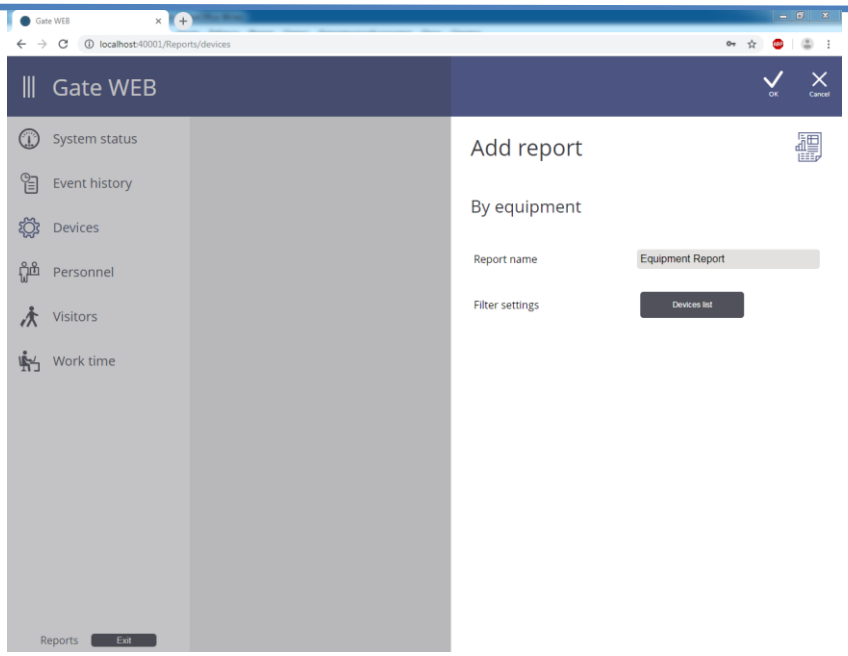
Often it is necessary to generate report with the same properties but with different period. Check □ report and press ‘Re-generate’ menu item. Type new report name and set new period start and end dates in the window displayed. New report generated after ‘OK’ press.



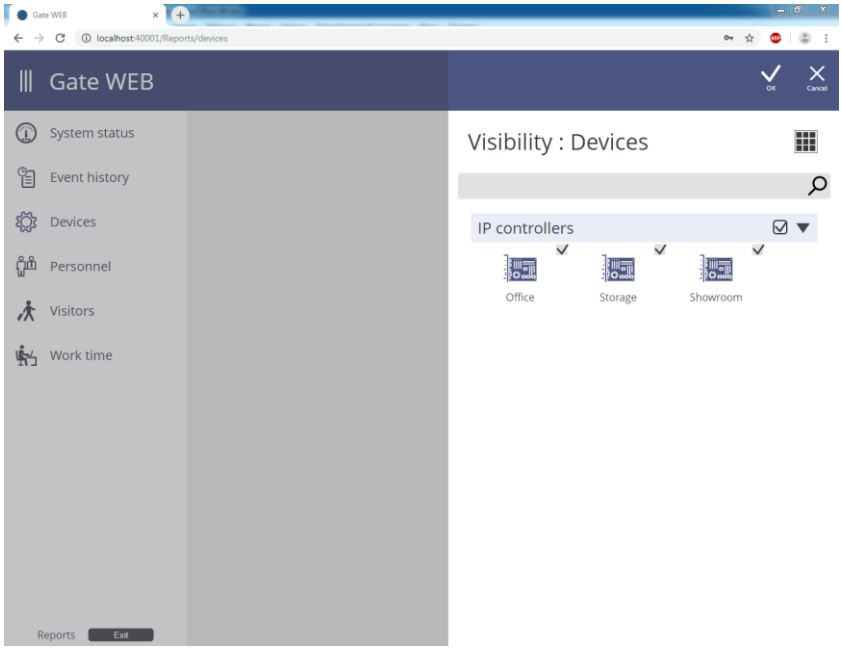
’Devices’ report

‘Devices’ report accumulates general information about all doors and devices in system including inputs and outputs.

Press ‘Add report’ menu item in ‘Devices’ section. Type report name in the window displayed.

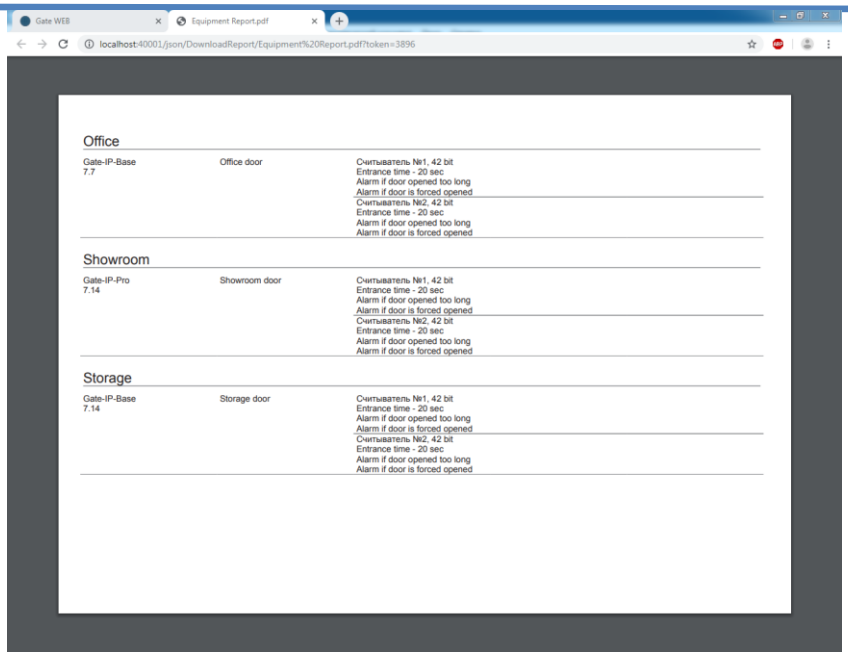


Press ‘Equipment list’ button and remove selection from devices undesirable in report. Press ‘OK’ button.



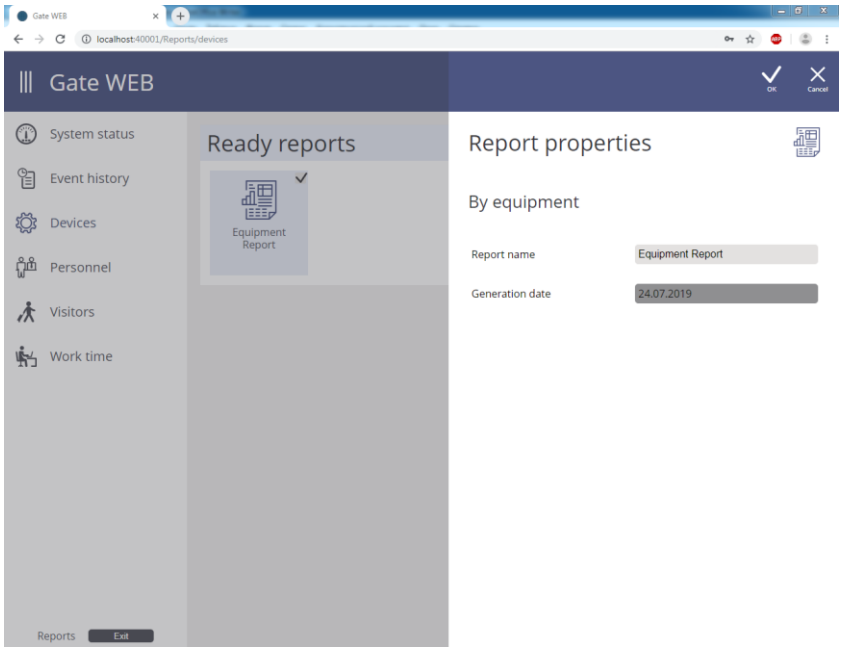
Select report and press ‘View’ menu item to view report:

Ready report in .pdf format will be displayed in separate browser window/tab. Save it with standard browser purposes.



Check □ report and press ‘Delete’ menu item to delete report. Confirm action in the window displayed. Report will be deleted permanently.

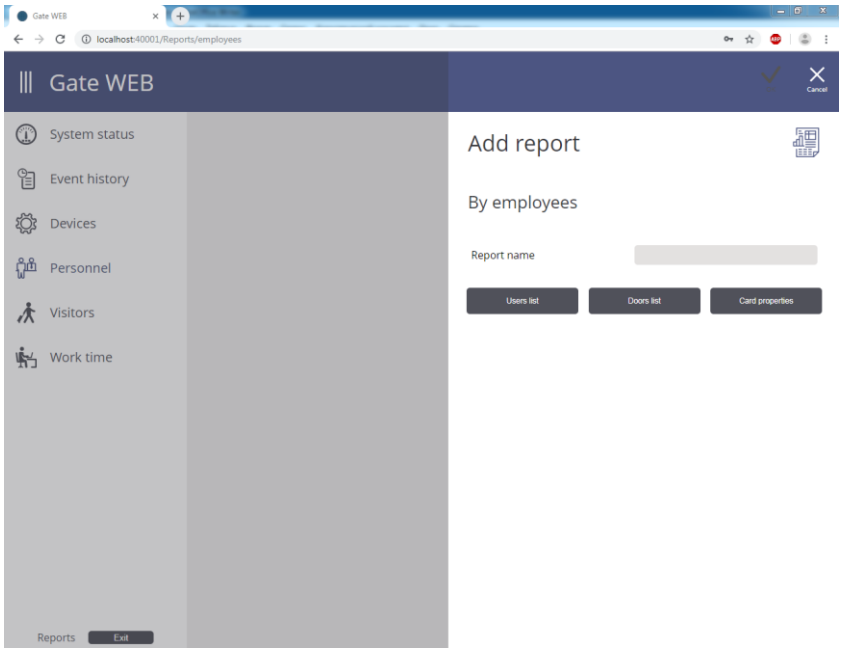
Check □ report and press ‘Properties’ menu item to rename it. Type new name in the window displayed.



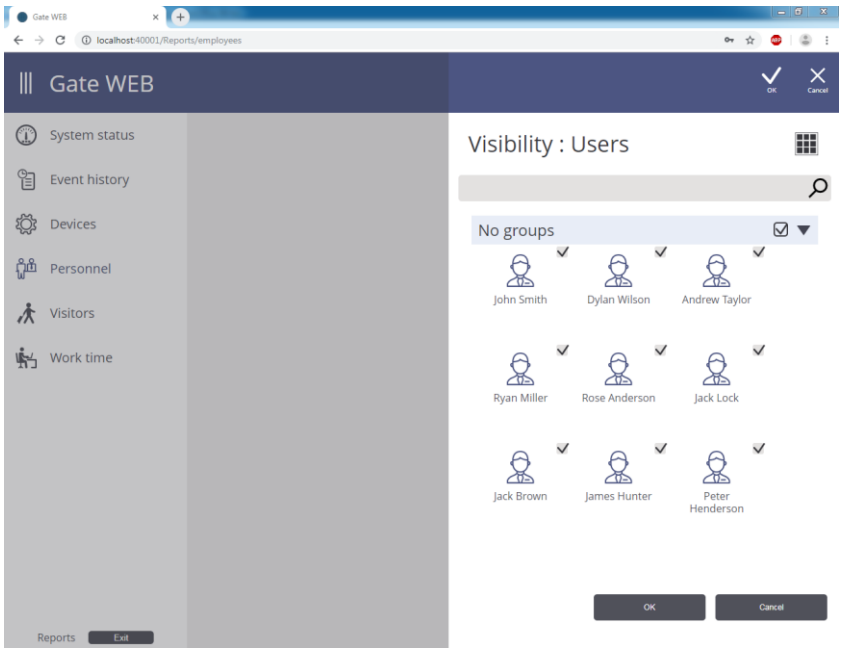
'Personnel' report

This report provides general information on employees with their access rights and IDs.

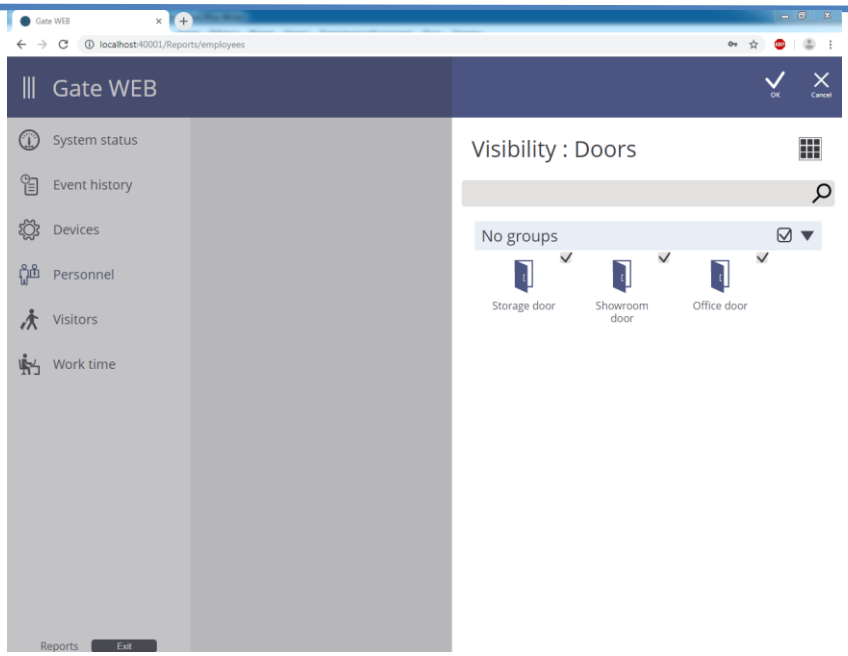
Select "Add report" menu item in "Personnel" section. Type report name in window displayed.



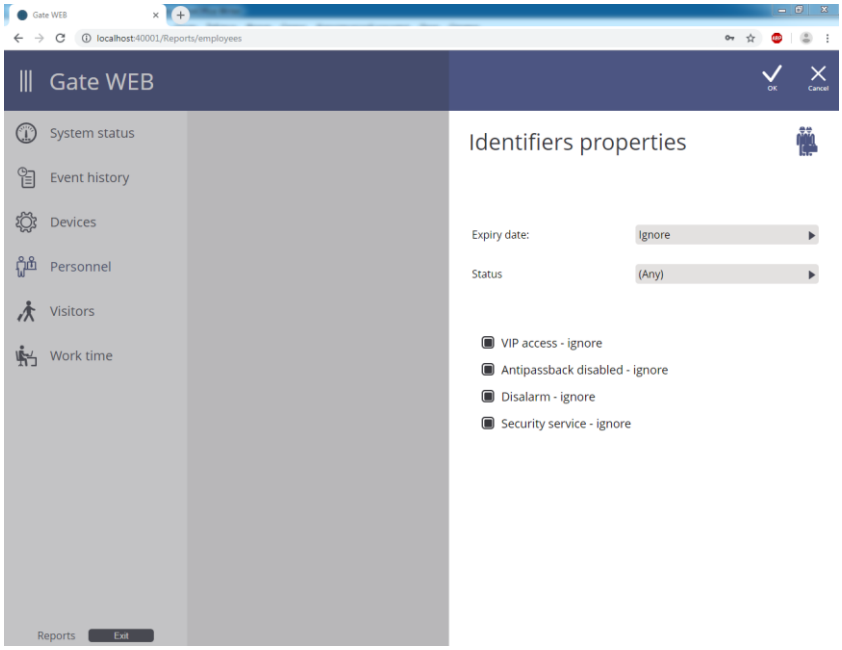
Press "Employees list" button, uncheck employees in the window displayed and press "OK", to remove certain employees from the report.



Press "Doors list button", uncheck doors and press "OK" to remove from the list employees with access to the certain doors.



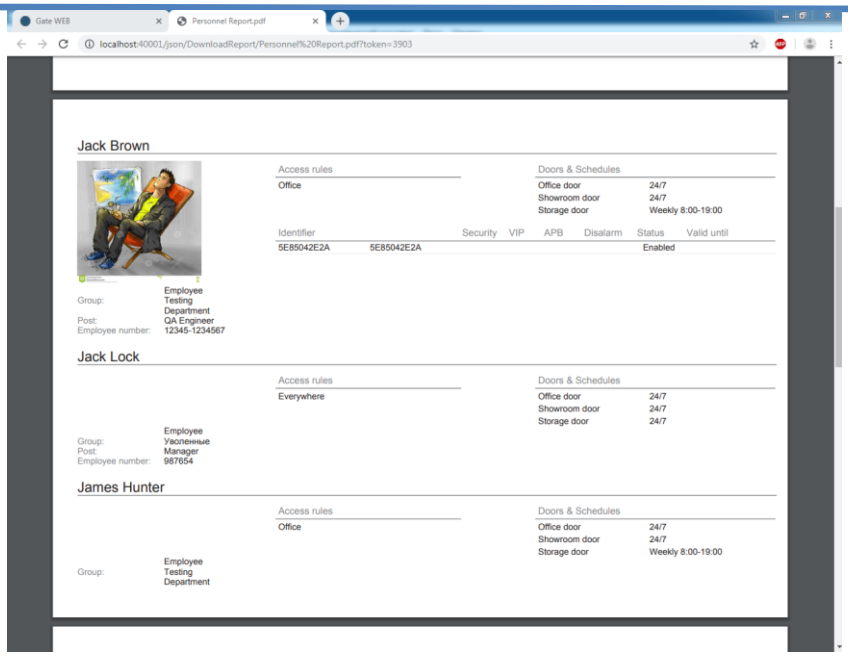
Press “IDs list” button, set desired ID settings in the window displayed and press OK to add to the report employees holding cards with certain settings.



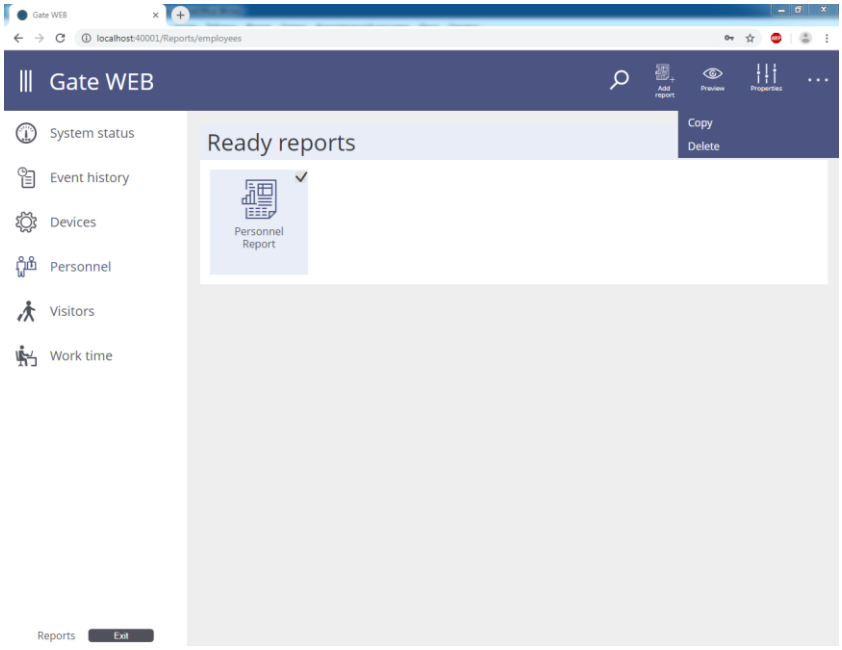
Report generation will start after “OK” button press. Report will be placed into “Generation progress” category. It will be moved into “Ready reports” category after generation finished.

Check □ report and select “View” item in menu.

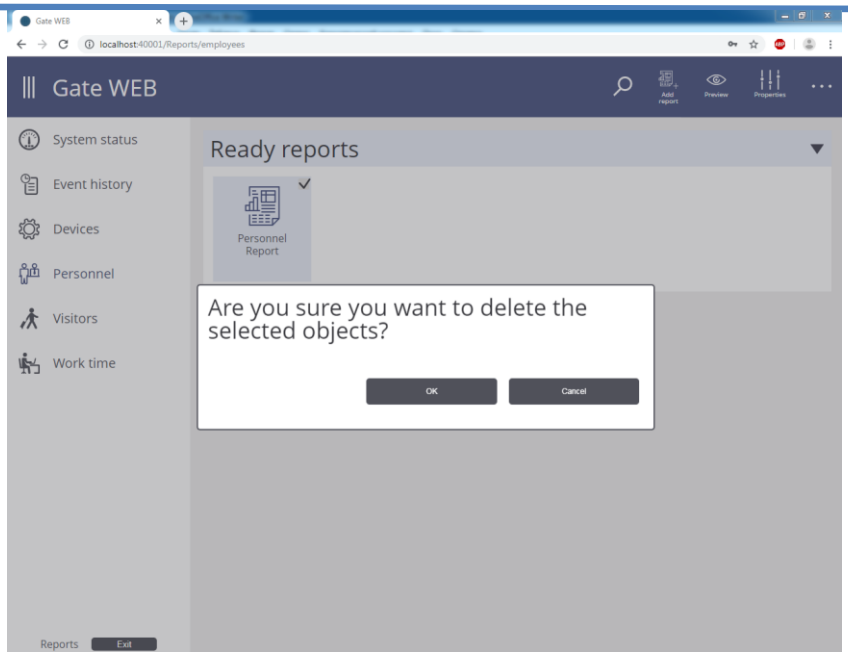
Generated .pdf file will be opened in the separate browser window/tab. It is possible to save and print report with the browser standard means.



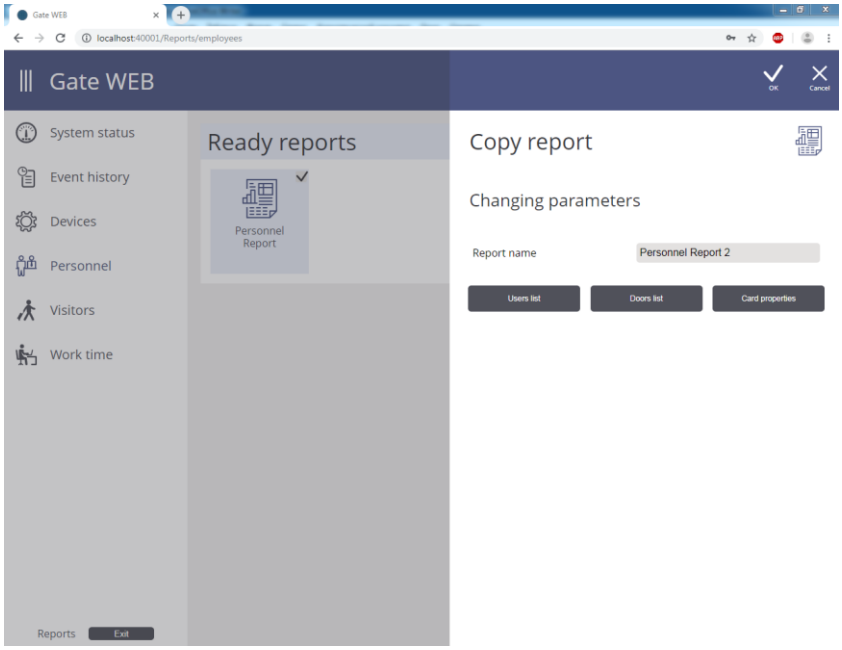
Check report □ and select “Delete” menu item to delete report:



Confirm deletion in the window displayed. Report will be deleted permanently.



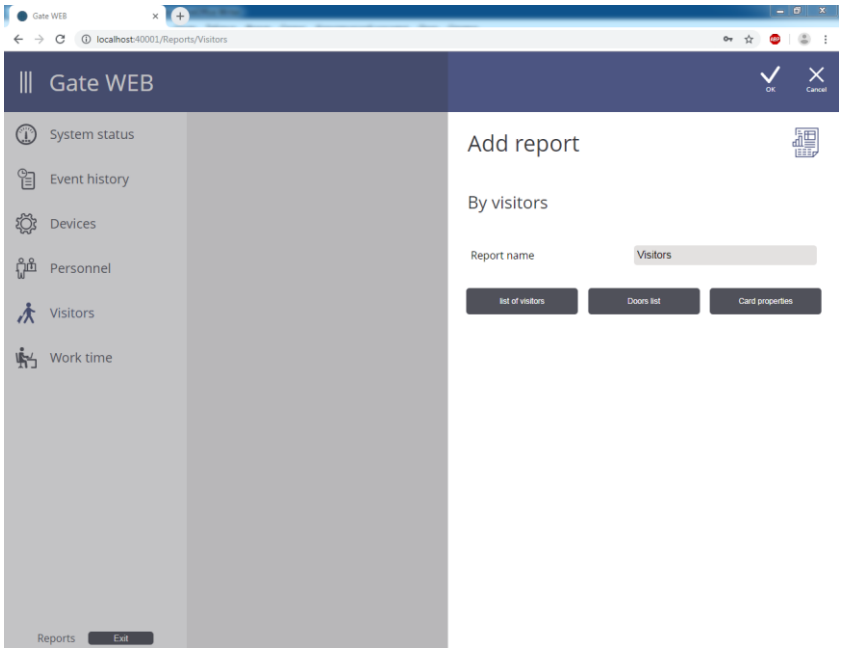
To generate report similar to existing, but with some settings different, check □ report in the list and select “Copy” menu item. Type new report name in the window displayed and change filter settings. New report will be generated after “OK” button press.



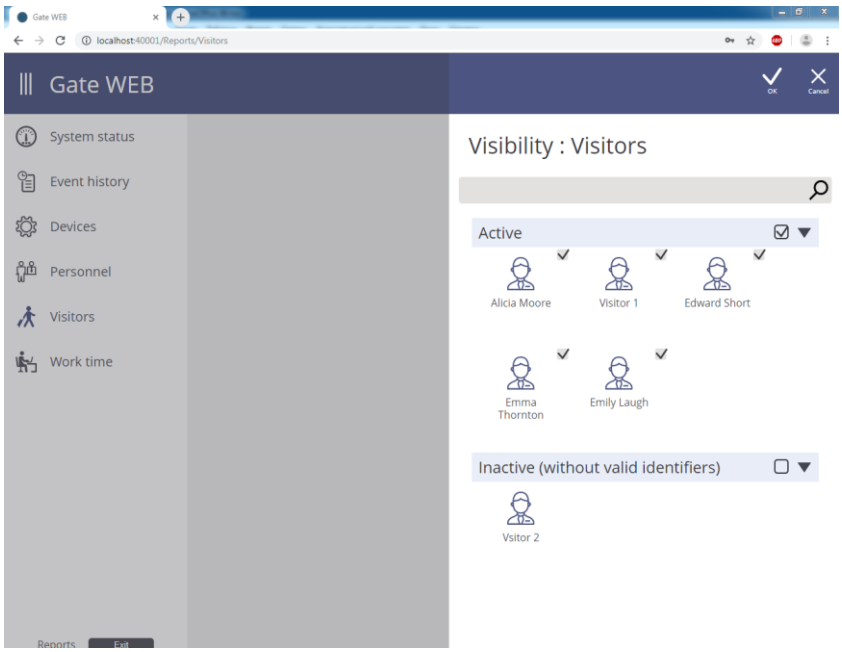
“Visitors” report

This report provides general information about visitors with their access rights and IDs.

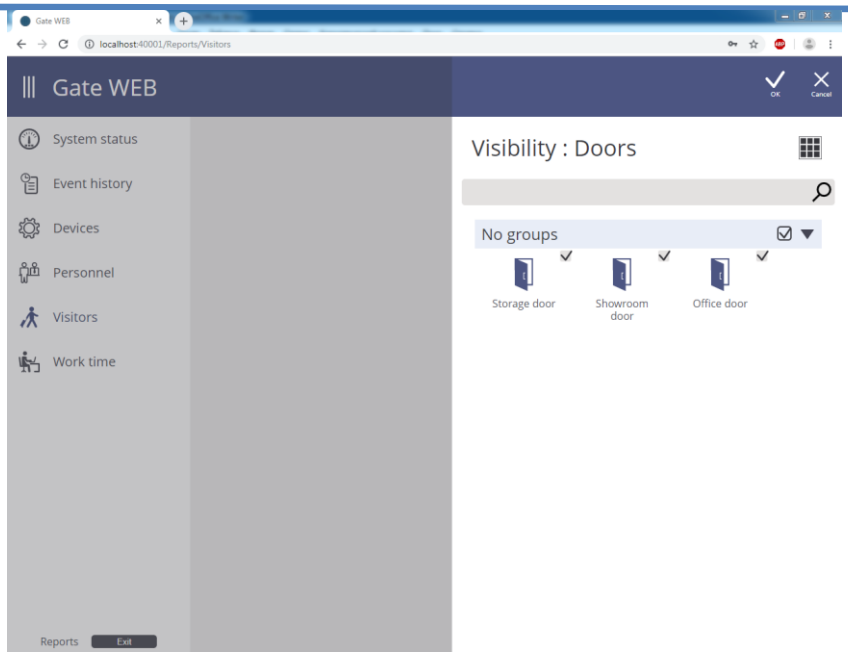
Select “Add report” menu item in “Visitors” section. Type report name in the window displayed.



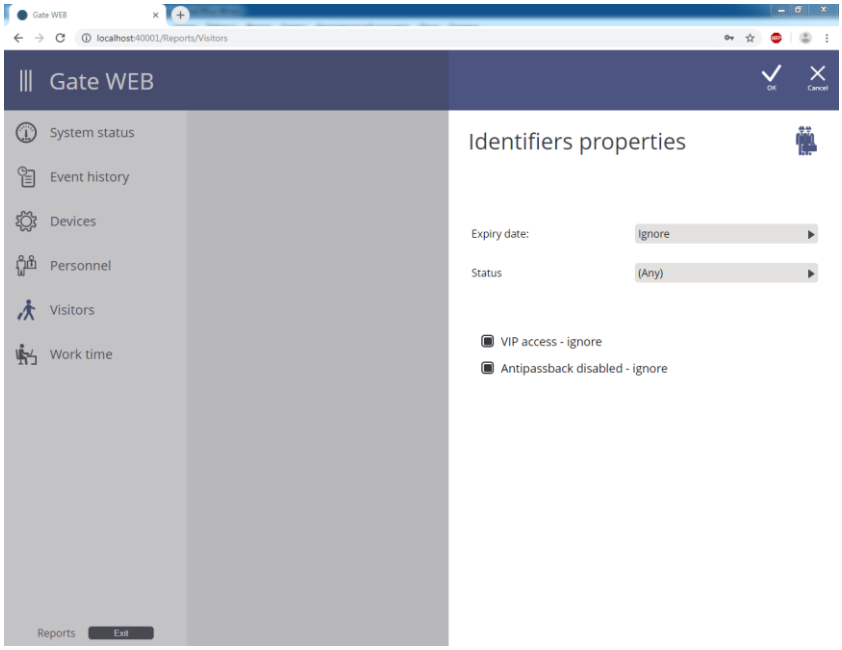
Press “Visitors list” button in the window displayed uncheck □ visitors you want to exclude from the report and press “OK” to exclude certain visitors from the report.



Press “Doors list button”, uncheck doors and press “OK” to remove from the list visitors with access to the certain doors.



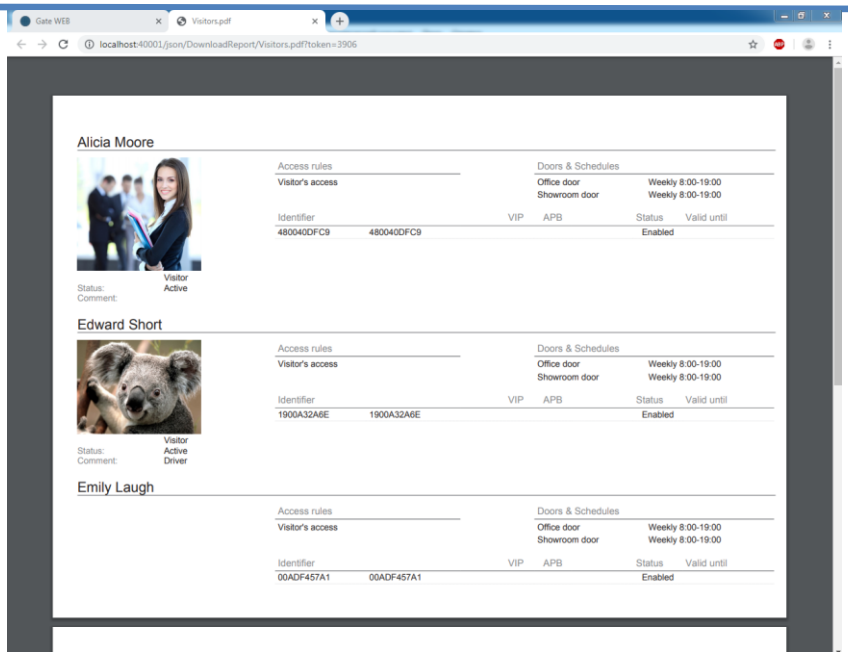
Press “IDs list” button, set desired ID settings in the window displayed and press OK to add to the report visitors holding cards with certain settings.



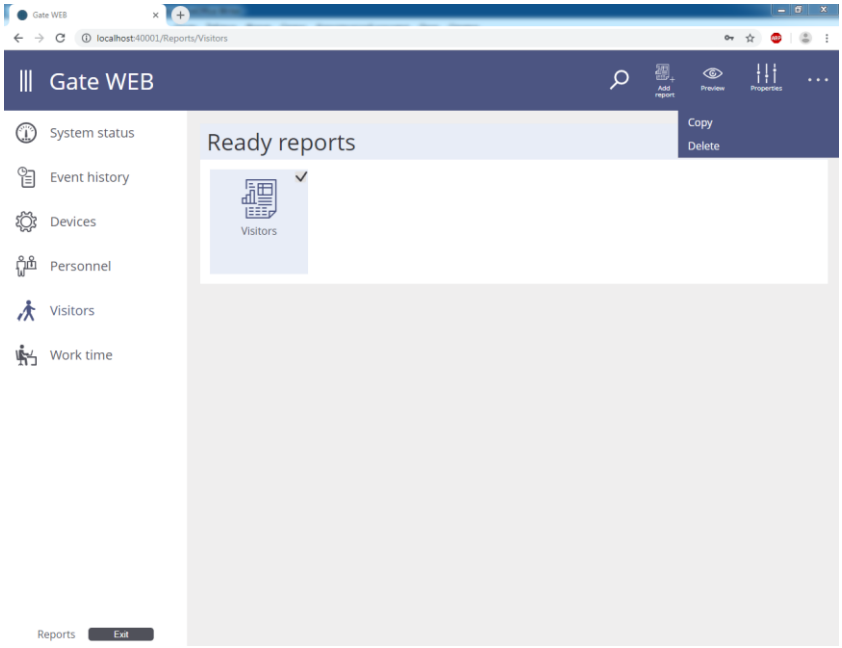
Report generation will start after “OK” button press. Report will be placed into “Generation progress” category. It will be moved into “Ready reports” category after generation finished.

Check □ report and select “View” item in menu.

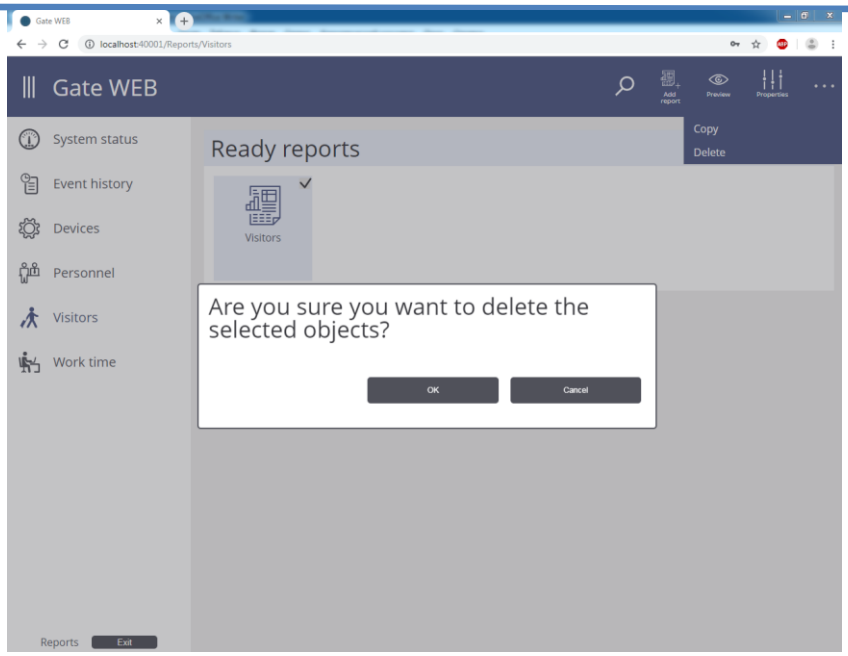
Generated .pdf file will be opened in the separate browser window/tab. It is possible to save and print report with the browser standard means.



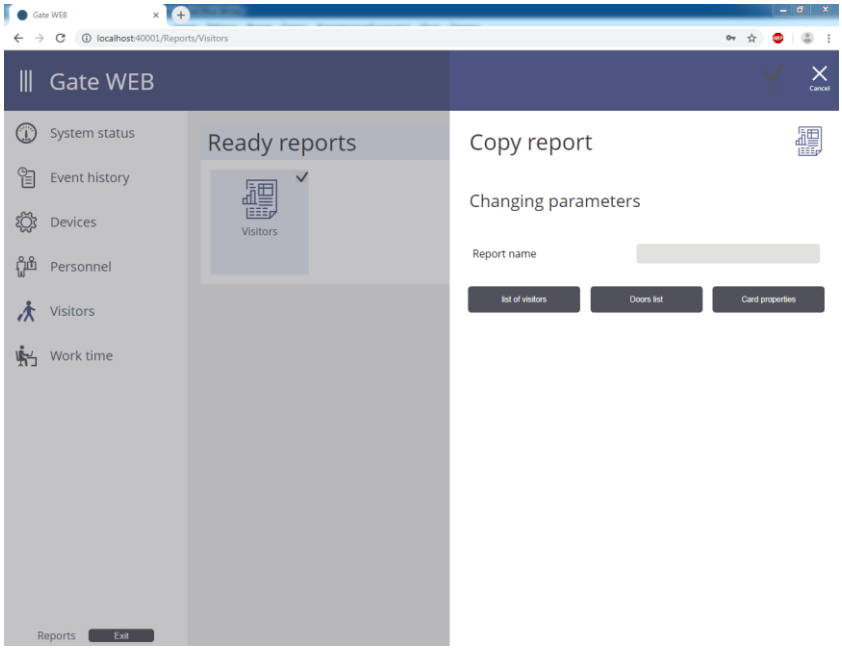
Check □ report and press ‘Delete’ menu item to delete report.



Confirm action in the window displayed. Report will be deleted permanently.



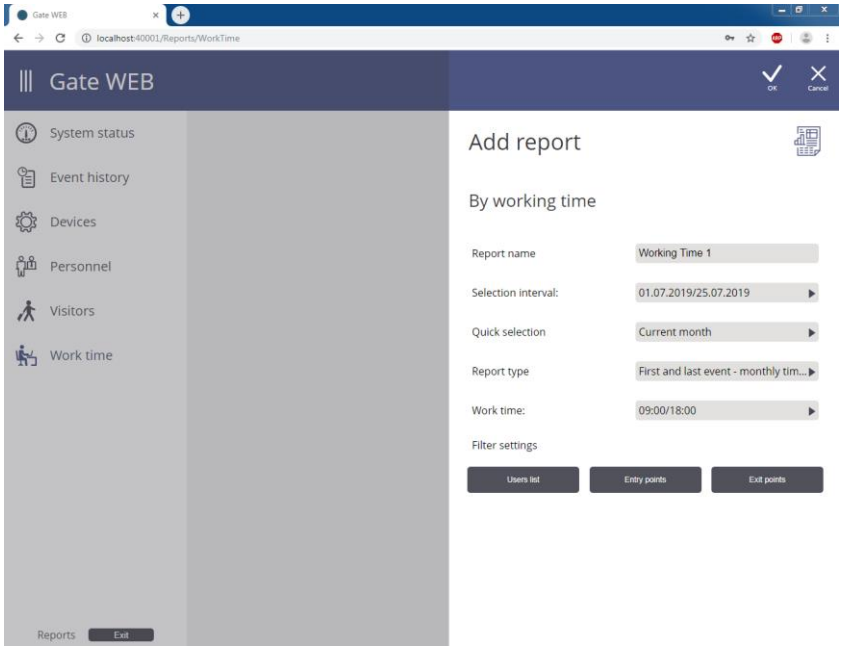
To generate report similar to existing, but with some settings different, check □ report in the list and select “Copy” menu item. Type new report name in the window displayed and change filter settings. New report will be generated after “OK” button press.



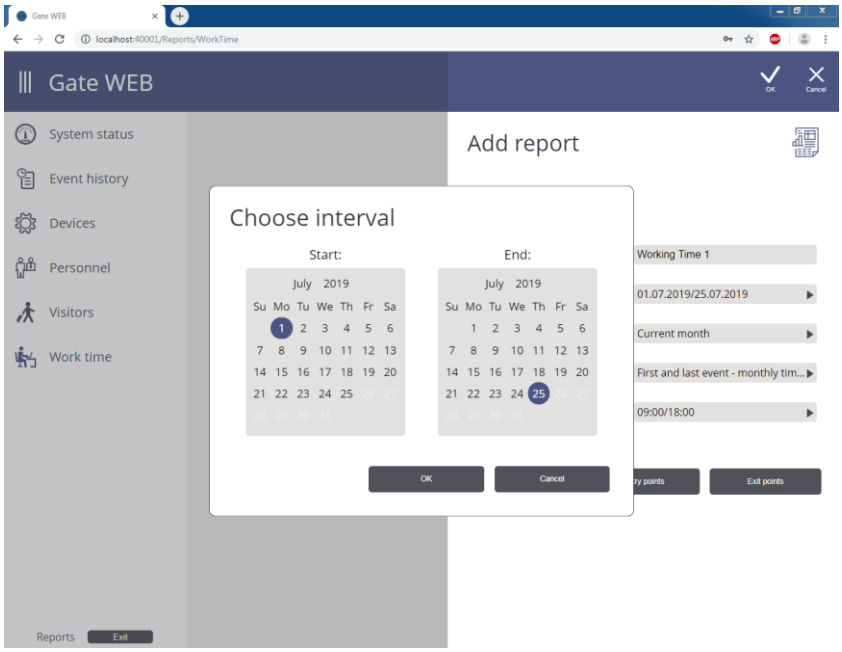
“Worktime report”

Report provides simple work time calculation based on the work start and work end time. Allows to generate the monthly working hours table or simple report on employees for work hour accounting, day missing, late coming and delays, depending on the report settings.

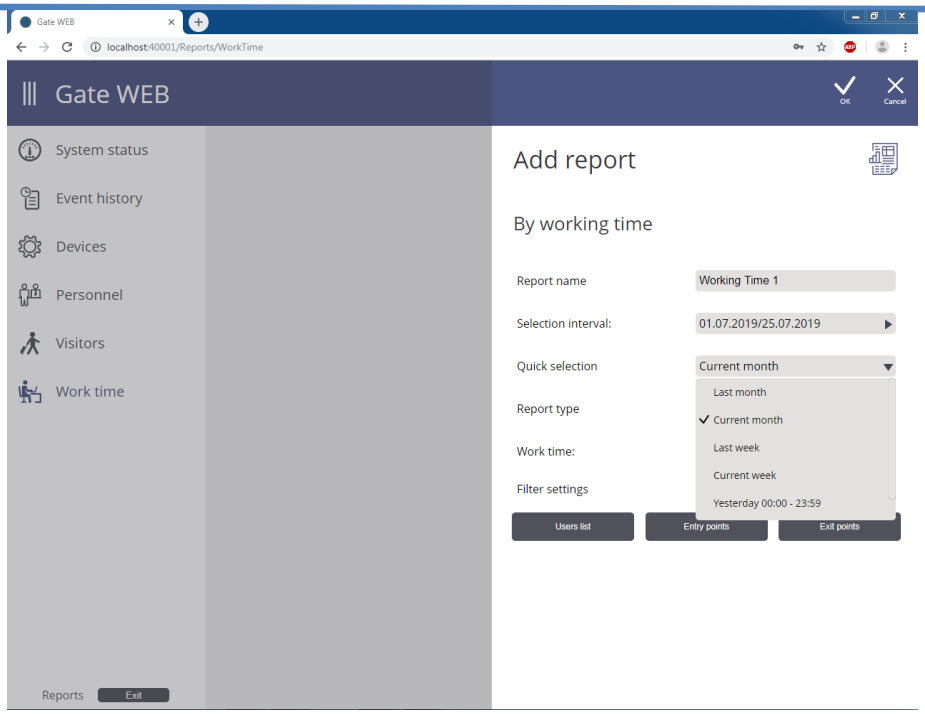
Press “Add report” menu item in the “Work time” section. Type report name in the window displayed.



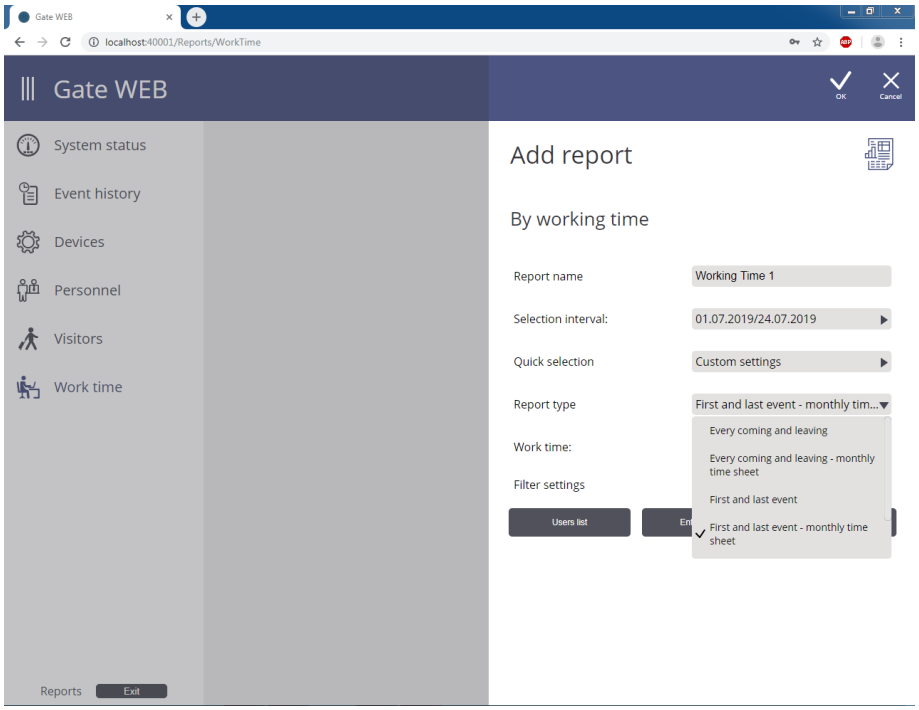
Set start and final time of the sampling manually



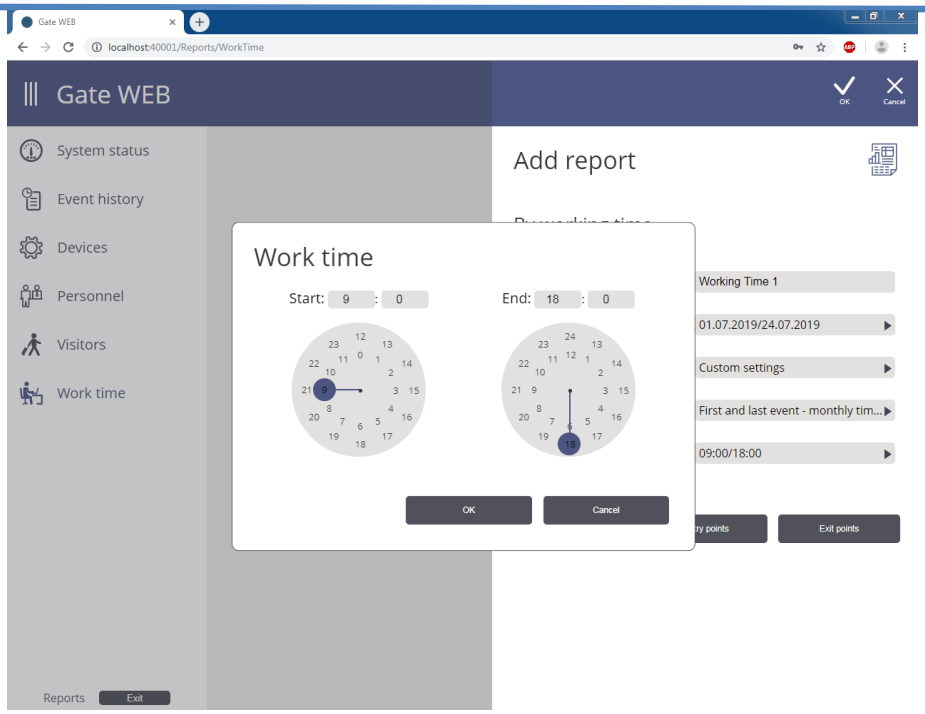
Or use preset time periods patterns from the “Quick selection” list:



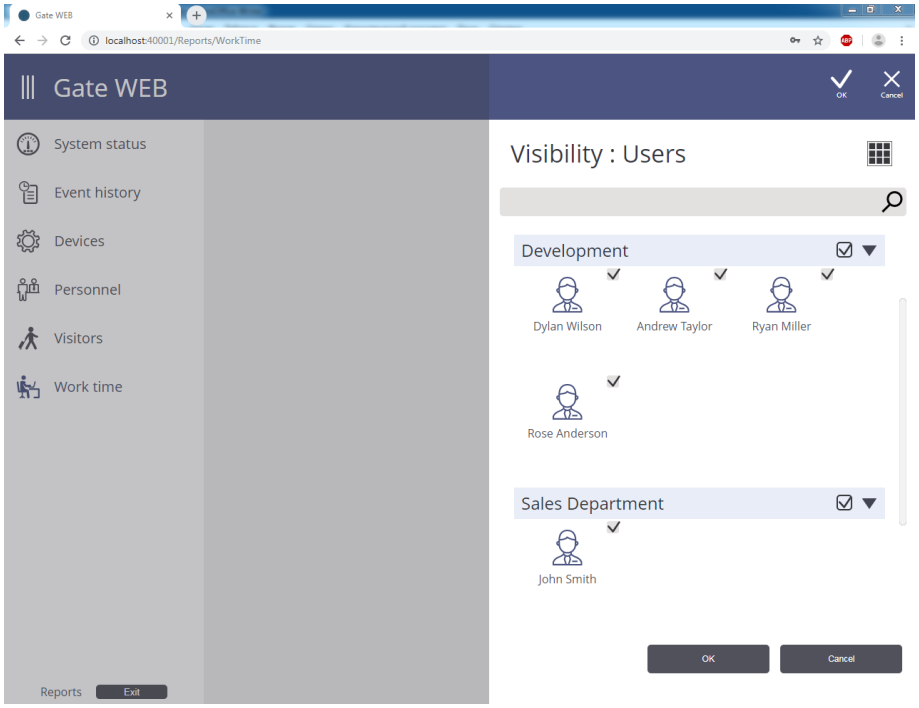
Set report type:



Set work time start and finish for the report generation:

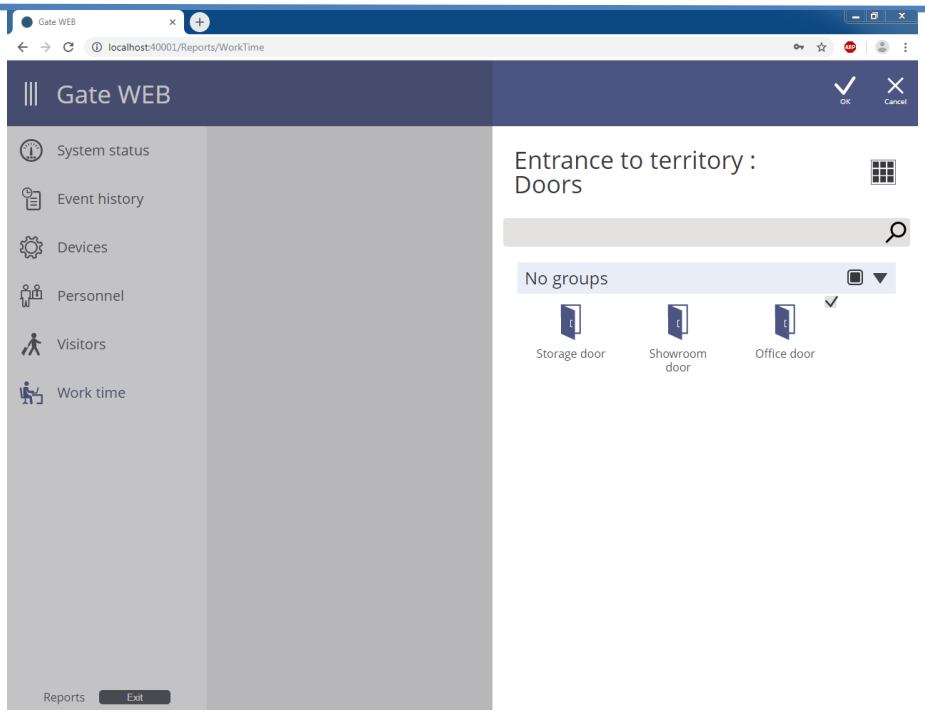


Press “Employees list” button and uncheck employees, undesirable in the report and press “OK”.

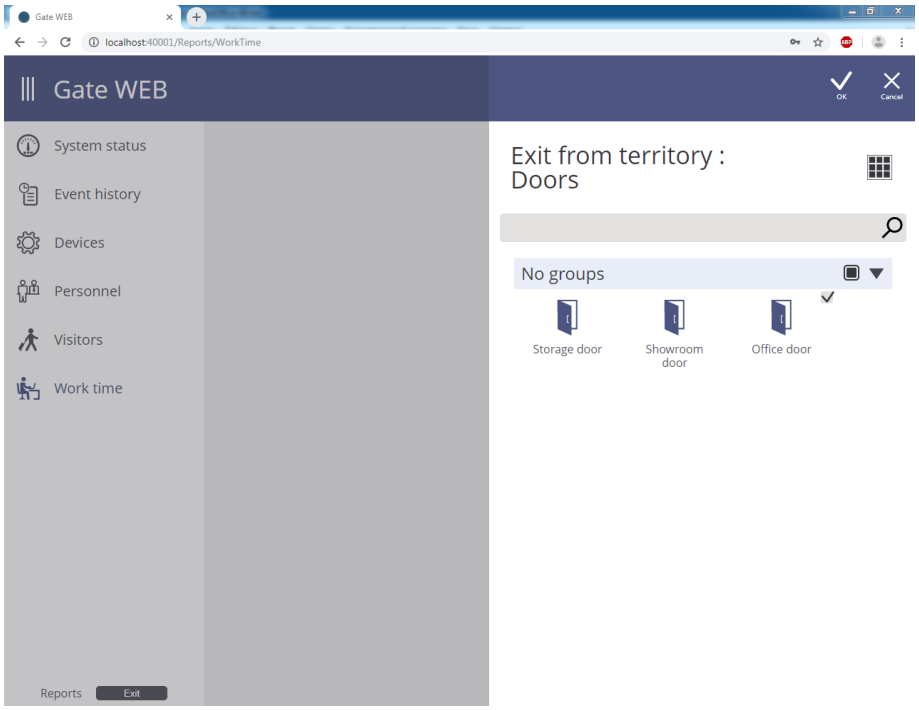


Set entry/exit doors to/from work area to be used for wok time start/end notification.

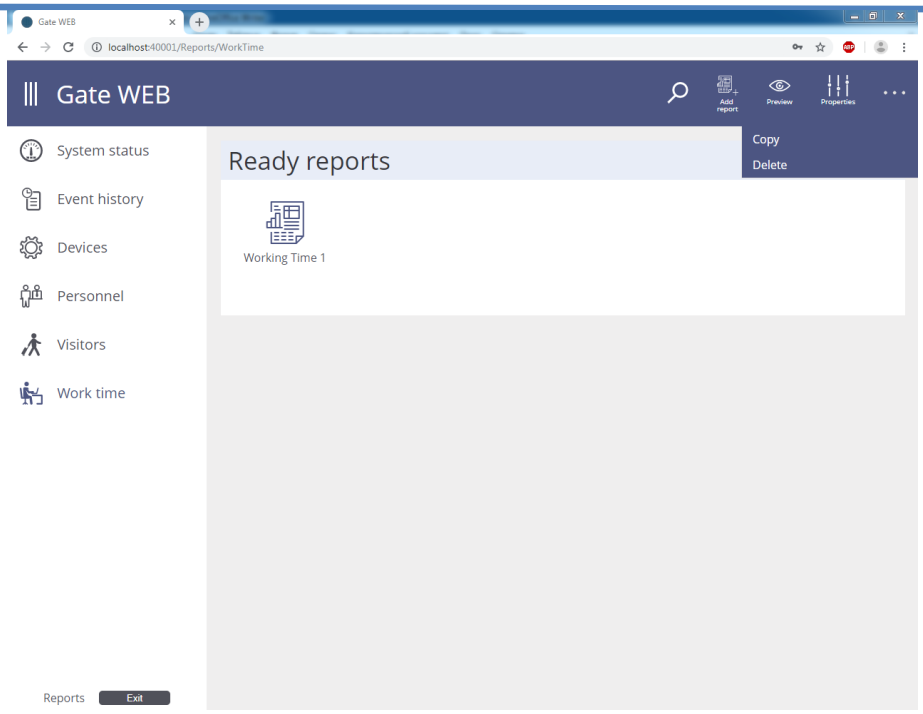
Area entry:



Area exit:

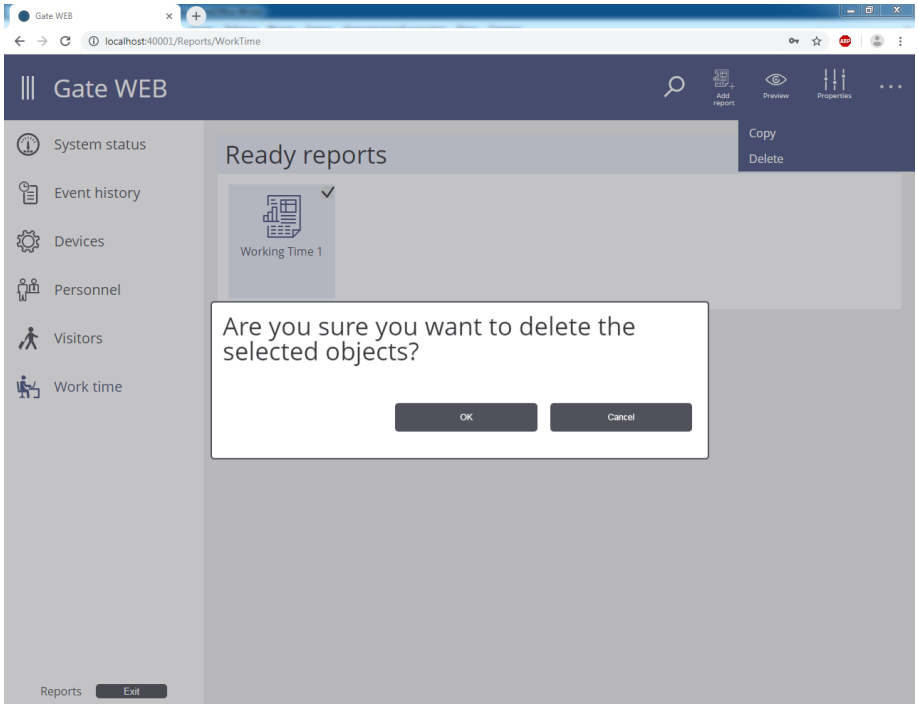


Press “OK” report will start to generate. It will be places into “Generation in process” category. Report is placed into “Ready reports” category after generation finished.

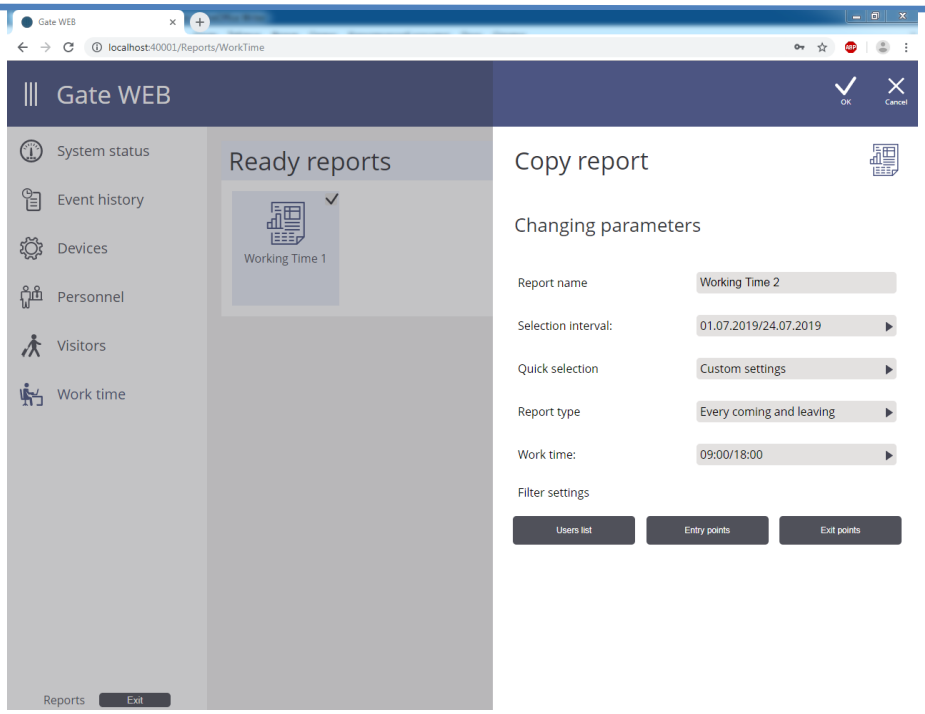


Check □ report and select ”Delete” menu item to delete

Confirm deletion in window displayed/ Report will be deleted permanently.



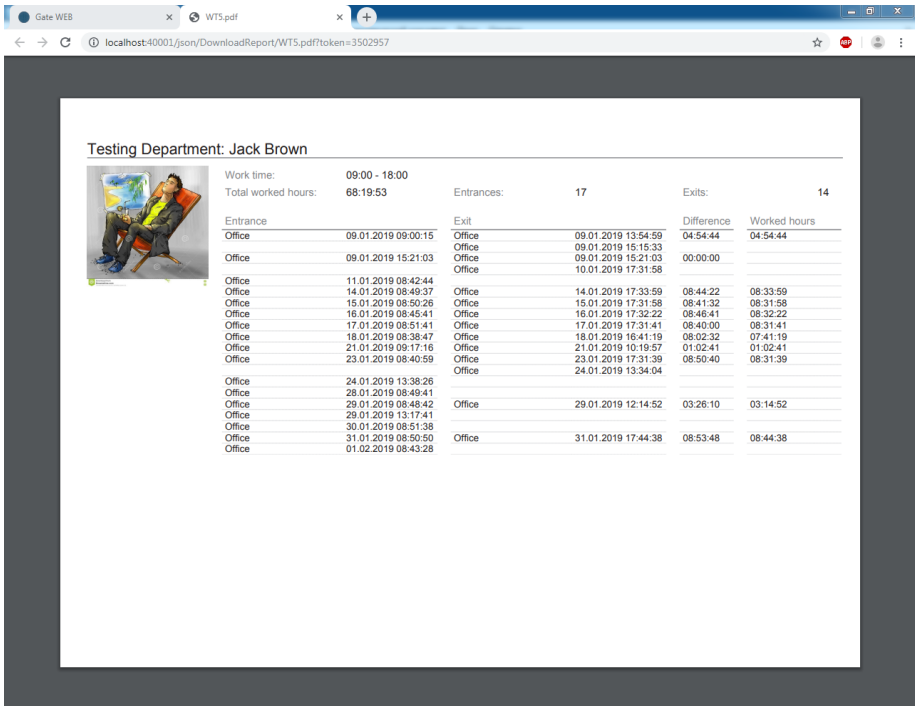
It is necessary to generate report with slightly changed settings oft-times. Check □ report and select “Copy” menu item. Type new report name in window displayed and change sampling settings. New report generated after “OK” button press.



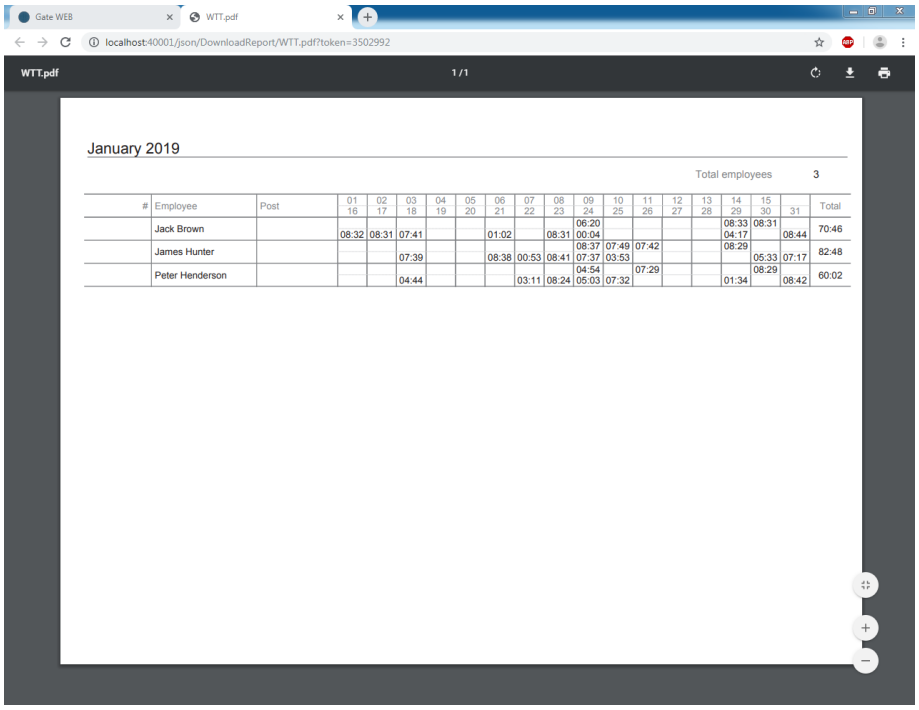
Check □ report and select “View” menu item to view it.

The report generated will be displayed in the separate browser window/tab in .pdf format. It is possible to print or save report by the browser standard means.

Report example: Every coming and leaving



Report example: Every coming and leaving - table

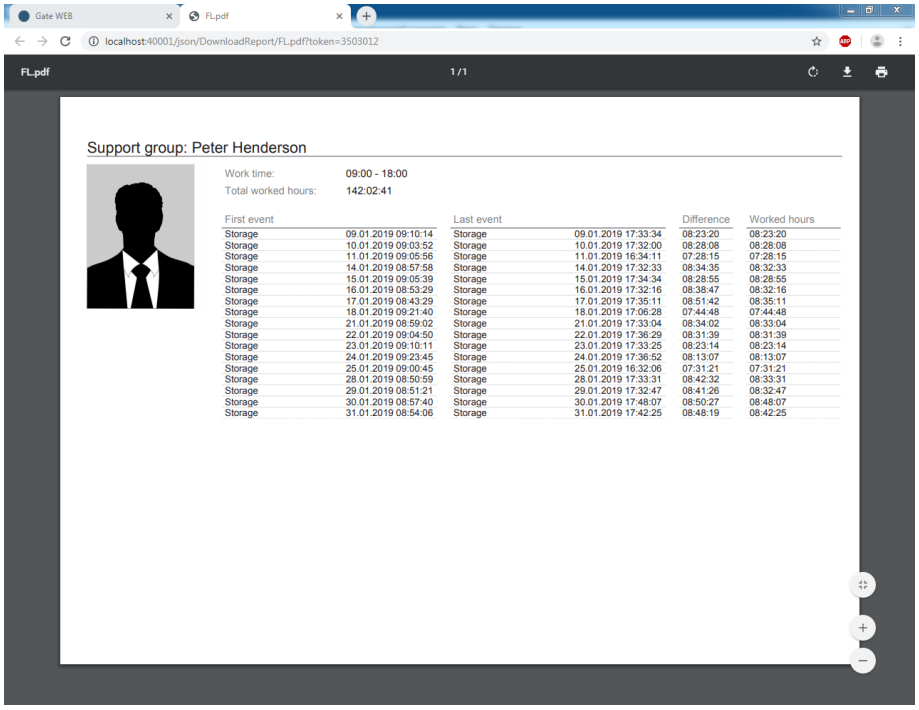


January 2019

Total employees 3

#	Employee	Post	01 16	02 17	03 18	04 19	05 20	06 21	07 22	08 23	09 24	10 25	11 26	12 27	13 28	14 29	15 30	31	Total
	Jack Brown		08:32	08:31	07:41			01:02		08:31	06:20 00:04					08:33 04:17	08:31	08:44	70:46
	James Hunter				07:39			08:38	00:53	08:41	08:37 07:37	07:49 03:53	07:42			08:29	05:33	07:17	82:48
	Peter Henderson				04:44				03:11	08:24	04:54 05:03	07:32	07:29			01:34	08:29	08:42	60:02

Report example: First and last event



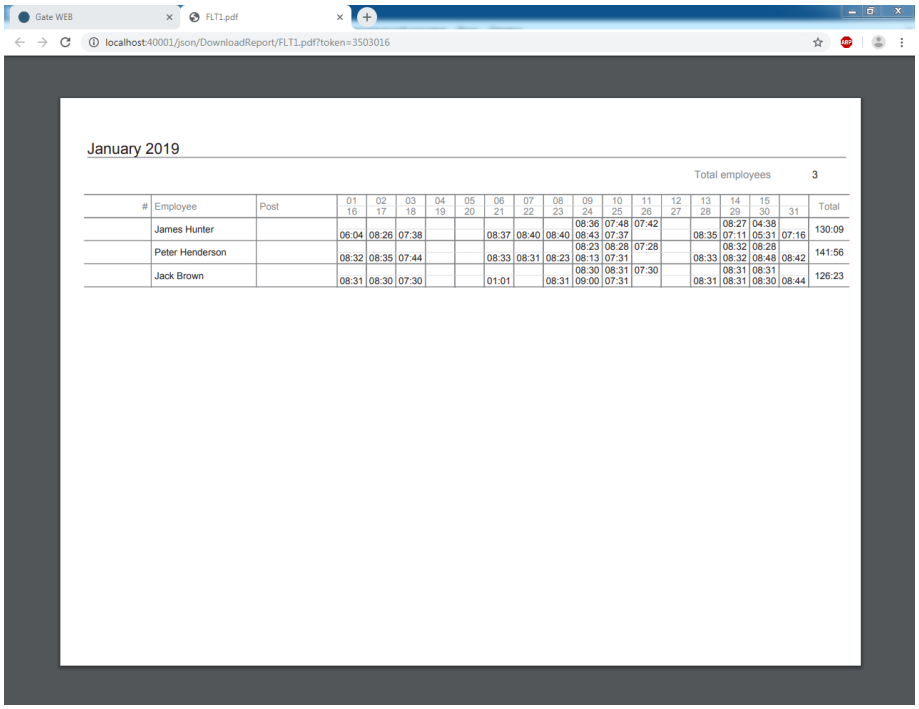
Support group: Peter Henderson

Work time: 09:00 - 18:00

Total worked hours: 142:02:41

First event		Last event		Difference	Worked hours
Storage	09.01.2019 09:10:14	Storage	09.01.2019 17:33:34	08:23:20	08:23:20
Storage	10.01.2019 09:03:52	Storage	10.01.2019 17:32:00	08:28:08	08:28:08
Storage	11.01.2019 09:05:56	Storage	11.01.2019 16:34:11	07:28:15	07:28:15
Storage	14.01.2019 08:57:58	Storage	14.01.2019 17:32:33	08:34:35	08:32:33
Storage	15.01.2019 09:05:39	Storage	15.01.2019 17:34:34	08:28:55	08:28:55
Storage	16.01.2019 08:53:29	Storage	16.01.2019 17:32:16	08:38:47	08:32:16
Storage	17.01.2019 08:43:29	Storage	17.01.2019 17:35:11	08:51:42	08:35:11
Storage	18.01.2019 09:21:40	Storage	18.01.2019 17:06:28	07:44:48	07:44:48
Storage	21.01.2019 08:59:02	Storage	21.01.2019 17:33:04	08:34:02	08:33:04
Storage	22.01.2019 09:04:50	Storage	22.01.2019 17:36:29	08:31:39	08:31:39
Storage	23.01.2019 09:10:11	Storage	23.01.2019 17:33:25	08:23:14	08:23:14
Storage	24.01.2019 09:23:45	Storage	24.01.2019 17:36:52	08:13:07	08:13:07
Storage	25.01.2019 09:00:45	Storage	25.01.2019 16:32:06	07:31:21	07:31:21
Storage	28.01.2019 08:50:59	Storage	28.01.2019 17:33:31	08:42:32	08:33:31
Storage	29.01.2019 08:51:21	Storage	29.01.2019 17:32:47	08:41:26	08:32:47
Storage	30.01.2019 08:57:40	Storage	30.01.2019 17:48:07	08:50:27	08:48:07
Storage	31.01.2019 08:54:06	Storage	31.01.2019 17:42:25	08:48:19	08:42:25

Report example: First and last event - table



January 2019

Total employees 3

#	Employee	Post	01 16	02 17	03 18	04 19	05 20	06 21	07 22	08 23	09 24	10 25	11 26	12 27	13 28	14 29	15 30	31	Total
	James Hunter		06:04	08:26	07:38			08:37	08:40	08:40	08:36 08:43	07:48 07:37	07:42		08:35	08:27 07:11	04:38 05:31	07:16	130:09
	Peter Henderson		08:32	08:35	07:44			08:33	08:31	08:23	08:23 08:13	08:28 07:31	07:28		08:33	08:32 08:32	08:28 08:48	08:42	141:56
	Jack Brown		08:31	08:30	07:30			01:01		08:31	08:30 09:00	08:31 07:31	07:30		08:31	08:31 08:31	08:31 08:30	08:44	126:23