

User manual

Version: 1.6.0

CONTENTS

1 **Introduction** . . . 9
- Sofware Editions . . . 9
- Predor Lite Edition . . . 9
- Predor Enterprise Edition . . . 9
- Registration and extension modules . . . 10
- Demo license . . . 11
- Downloading the software . . . 11
- Installing the Lite Edition . . . 12
  - Creating a database . . . 13
  - Loading the license . . . 14
- Installing the Enterprise edition . . . 15
  - Predor Enterprise edition components . . . 15
  - Server installation . . . 16
  - Configuring the server . . . 17
  - Loading the License . . . 26
  - Starting the server . . . 27
  - Test information page . . . 27
  - Personal web interface . . . 28
  - Logging . . . 29
  - Client installation . . . 30
  - Software upgrade . . . 32

2 **Controller LED feedbacks** . . . 34

3 **First steps** . . . 35
- Login . . . 35
- Software interface . . . 35

4 **Predor mobile application** . . . 36

5 **Monitor menu** . . . 41
- Dashboard . . . 41
- Monitoring . . . 43
- Doors . . . 44
- Display and management of alerts . . . 44
- Evacuation list . . . 46
- Doors and maps . . . 47
  - Doors . . . 47
  - Maps . . . 48
- Event list . . . 49
  - Export daily activities . . . 50
- Person location . . . 51
  - Auto drop out . . . 53

Tracking . . . 53
Surveillance . . . 54
Publish cards . . . 56
Temporary cards . . . 56
Visitors . . . 57
Vehicle activity . . . 60
6 Settings menu . . . 63
System settings . . . 63
System defaults . . . 63
Controller settings . . . 63
E-mail settings . . . 67
Folder settings . . . 67
Controllers . . . 67
Edit controller wizard . . . 69
Security settings . . . 74
NIS2 . . . 74
Authentication . . . 75
Security settings . . . 77
Audit log . . . 80
Disaster recovery . . . 81
Evacuation settings . . . 81
Disaster plans . . . 85
History . . . 86
Cameras . . . 86
Video devices . . . 86
Recording rules . . . 87
Parking management . . . 89
Vehicles . . . 89
License plate recognition . . . 92
Operators . . . 95
Database . . . 99
Data handling . . . 100
Subsystems . . . 101
7 Users menu . . . 105
Users and departments . . . 105
Certificates . . . 109
Visitor settings . . . 115
Card list . . . 118
Venue admission . . . 118
8 Access control settings . . . 123
Access groups . . . 123
Access zones . . . 124

Time profiles . . . 125
Access privileges . . . 126
Access map . . . 127
Door profiles . . . 128
Operating modes . . . 128
Interlock . . . 131
Settings . . . 132
9 Advanced control menu . . . 133
Anti-passback . . . 133
Controller-level settings . . . 133
Global settings . . . 134
Masterlock . . . 136
Settings . . . 136
Headcount limit . . . 139
Controller-level settings . . . 139
Global settings . . . 140
Multicard access . . . 141
Settings . . . 141
Random checking . . . 142
Settings . . . 142
Patrol . . . 144
Patrol routes . . . 144
Patrol log . . . 145
10 Attendance menu . . . 147
Calendar . . . 147
Company calendar . . . 151
User calendar . . . 152
Work shifts . . . 152
Activity codes . . . 155
Activity code defaults . . . 157
Worktime profiles . . . 157
Worktime profile configuration . . . 160
Built-in worktime profiles . . . 181
Worktime reports menu . . . 186
Users' monthly activities . . . 189
Daily activities . . . 192
Users' daily activities . . . 196
Calendar report . . . 197
Attendance report . . . 199
Monthly details . . . 202
Users' daily details . . . 203
Monthly activities . . . 204

Users' summary . . . 205
Days off report . . . 206
Balance report . . . 207
Start screen . . . 208
Worktime terminals . . . 217
Discover terminals . . . 218
Terminal configuration . . . 218
Web settings . . . 221
General settings . . . 222
Responsible user settings . . . 223
E-mail log . . . 224
11 Web interface . . . 225
My calendar (employee web interface) . . . 230
Manager calendar . . . 232
Weekly calendar (manager calendar) . . . 236
My colleagues (employee calendar) . . . 236
Webterminal . . . 236
Group actions . . . 237
12 Operation of the Predor work time processor . . . 242
13 Additional menu . . . 246
Software upgrade . . . 246
License manager . . . 246
Online license activation . . . 247
Offline license activation . . . 248
14 Upload menu . . . 252
Upload . . . 252
15 Subsystem management . . . 253
Operator management . . . 254
Device management . . . 254
User management . . . 255
Event management . . . 255
Manager settings . . . 255
Subsystem-related interfaces . . . 257
Managing several company calendars . . . 259
16 Version tracking . . . 260
1.3.2. . . . 260
1.3.3. . . . 260
1.3.3.1. . . . 261
1.3.3.2. . . . 261
1.3.3.3. . . . 261
1.3.3.4. . . . 261
1.3.3.6. . . . 262

1.3.3.7. 262
1.3.3.8. 262
1.3.3.9. 262
1.3.3.12. 263
1.3.3.13. 263
1.3.3.14. 263
1.3.4. 263
1.3.4.1 263
1.3.4.2 263
1.3.4.3 264
1.3.4.4 265
1.3.4.5 265
1.3.4.6 265
1.3.4.7 265
1.3.4.8 266
1.3.4.9 266
1.3.4.10 267
1.3.4.11 267
1.3.4.12 267
1.3.4.13 267
1.3.4.14 268
1.3.4.15 268
1.3.4.16 268
1.3.5 269
1.3.5.1 270
1.3.5.2 270
1.4.0 270
1.4.1 271
1.4.2 272
1.4.3 273
1.4.4 273
1.4.5 273
1.4.6 273
1.4.7 273
1.4.8 274
1.4.9 274
1.4.10 274
1.4.11 274
1.4.12 274
1.4.13 275
1.4.14 275
1.4.16 275

1.4.17 . . . 275
1.5.0 . . . 275
1.5.3 . . . 275
1.5.5 . . . 276
1.5.7 . . . 276
1.5.8 . . . 277
1.5.9 . . . 277
1.5.10 . . . 277
1.5.11 . . . 278
1.5.11.1 . . . 278
1.5.12.2 . . . 278
1.5.12.3 . . . 278
17 Appendix A: Predor system update guide . . . 279
Predor Lite system update . . . 279
Backing up the database . . . 279
Running maintenancetool on Windows operating system . . . 280
Running maintenancetool on Linux operating system . . . 284
Predor Enterprise . . . 288
Backing up the database . . . 288
PostgreSQL database backup . . . 289
SQLite database backup . . . 291
Predor Server . . . 292
Running maintenancetool on Windows operating system . . . 292
Running maintenancetool on Linux operating system . . . 296
Predor Client . . . 300
Firmware update of devices . . . 300
Firmware update of controllers . . . 300
Firmware update of terminals . . . 302
18 Appendix B: System administrator's guide . . . 304
System overview . . . 304
Software editions . . . 304
Predor Enterprise edition . . . 304
Predor Lite edition . . . 305
System requirements . . . 305
Enterprise server application . . . 305
Enterprise client application . . . 307
Lite client application . . . 308
Network configuration . . . 309
Basic requirements . . . 309
Multi-site access control systems . . . 309
Network diagnostics . . . 310
Default ports . . . 312

First steps . . . 313
Network access of controllers . . . 313
Network access of work time terminals . . . 313
Troubleshooting . . . 315
Special cases . . . 317
Adding a controller from another subnet . . . 317
Temporarily connect the controller to the server, then install it to the desired place. . . . 317
Use a second Predor software on-site to pre-configure the controller and add it manually. . . . 317
Accessing the web from an external IP address . . . 318
Resetting the devices . . . 318
Resetting and factory resetting of the controllers . . . 318
Factory resetting the work time terminals . . . 319
19 Appendix C: Installing Predor Enterprise Server with Docker . . . 320
Preparations . . . 320
Installing dependencies on Ubuntu . . . 320
Configuration . . . 320
Installation and running . . . 323
Useful commands . . . 324
Backing up the database . . . 324
SQLite databases . . . 324
PostgreSQL databases . . . 325
Updating . . . 325
Restoring the database . . . 326
SQLite databases . . . 326
PostgreSQL databases . . . 326
20 Appendix D: Predor terminal installation guide . . . 328
Environmental conditions for installation . . . 328
Cabling . . . 328
Proper construction of the power cable . . . 328
Power cable compliance check . . . 329
Replacing batteries . . . 329
Configuration, network management . . . 330
Troubleshooting . . . 331
21 Appendix E: Predor terminal replacement guide . . . 333
Predor terminal dismounting . . . 333
Replacement Predor terminal installation . . . 334
Replacing a Predor terminal in the software . . . 334
Troubleshooting . . . 337
22 Appendix F: Predor biometric terminal description . . . 339
Introduction . . . 339

Important Notes . . . 341
Deep-discharge mode . . . 341
First steps . . . 342
Predor terminal menu map . . . 343
Adding the terminal to the Predor Enterprise software . . . 346
General usage . . . 349
Adding a new user . . . 349
Registering an activity . . . 349
Registering an activity for groups . . . 350
Fingerprint management . . . 352
Security . . . 354
Troubleshooting . . . 356
23 Appendix G: Hikvision license plate recogniser configuration for Predor Enterprise system . . . 357
24 Appendix H: Dahua license plate recogniser configuration for Predor Enterprise system . . . 360
25 Appendix I: Predor office terminal description . . . 363
Introduction . . . 363
Important Notes . . . 366
First steps . . . 367
Predor terminal menu map . . . 368
Adding the terminal to the Predor Enterprise software . . . 371
General usage . . . 374
Adding a new user . . . 374
Registering an activity . . . 374
Registering an activity for groups . . . 375
Troubleshooting . . . 377
26 Függelék J: Predor Phantom new generation firmware upgrade guide . . . 378
Predor Phantom new generation firmware upgrade . . . 378

1 INTRODUCTION

The Predor Access Control and Time & Attendance Software is published in two different editions which slightly differ in functionality and the services provided. First let's take a look on the major features of each edition.

Sofware Editions

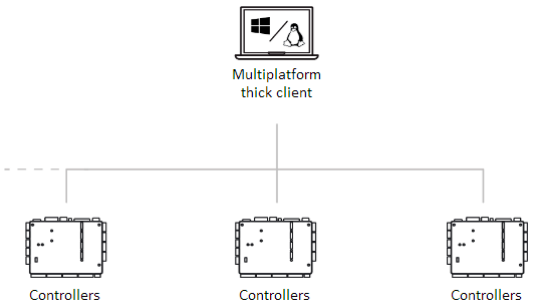
The Predor system is currently available in the following editions:

- Predor Lite Edition
- Predor Enterprise Edition

Predor Lite Edition

The Lite Edition consists of a single multi-platform thick client application which was designed to be run only when monitoring of the system or managing users is necessary. The software automatically synchronizes with the access controller devices and downloads the events each time it runs, but the system usually works autonomously without the aid of the software.

In this version the access control system can be managed from a single computer, on which the Predor Lite application is installed, thus only one operator (a user who is authorized to log into the software) can use the system at a time. As the whole access control system is prepared to run without the aid of the software, real-time **e-mail notifications**, the **Predor mobile application**, some extension modules and the **Predor Time & Attendance Terminals are not available in this edition**. Furthermore some advanced access control features (headcount-limit, anti-passback) are limited to be only controller-level (e.g. anti-passback function between controllers are unavailable).



Main features:

- Only one client at a time
- Linux and Windows platform
- No mobile application available
- Only controller-level functions

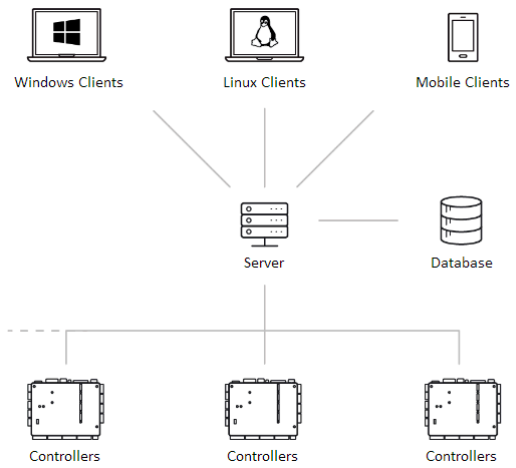
Predor Enterprise Edition

The Predor Enterprise Edition consists of two software pieces: the **Enterprise Server** application and the **Enterprise Client** application. This edition needs a **central server** on

which the Enterprise Server software constantly runs.

The server application does not have a graphical user interface (GUI), it runs as a system service in the background after installation. It serves as the central hub for the access controllers, listens for incoming connections from the number of clients and also provides the Predor Work Time Web page. The Enterprise Clients, i.e. the operators with their own computers and smart phones connect to this server. These clients have their own GUIs. Multiple operators (clients) can manage the system – change settings, manage users, create work time reports – simultaneously. The server must run all the time so it can collect data from the access controllers real-time and send notifications or pre-programmed automated work time reports via e-mail to operators and other staff. The server also provides the Predor Work Time Web page (if the associated module is purchased).

For the Enterprise Edition, PostgreSQL or MSSQL can be used, which supports on-the-fly backup creation among others. Although, using SQLite is still an option, just like in the Lite Edition.



Main features:

- Multiple clients simultaneously
- Linux and Windows platform
- Mobile application
- Global functions
- Automatic e-mail functions
- Automatic reports
- Work time terminals

Registration and extension modules

The process of creating and registering new Predor systems and also the availability of certain modules can vary in each country/region. Please inquire about registration and available modules at your nearest Predor distributor.

Each Predor system has an automatically generated unique **System ID** which consists of 12 alphanumeric characters. It server as the identification point for each system, and also for each purchased licenses and modules, which unlock certain menus in the software. Upon installing the software the SystemID must be provided. Also, after installation Predor systems need activation (after adding at least one access control hardware to the system). After activation the SystemID will not be usable on other computers!

Demo license

Since version 1.3.1.4 a DEMO license is available for evaluating the software or any of its features for free. A Predor device (access control unit and/or terminal) and other hardware accessories are needed for full functionality, but all modules are available with the following limitations:

- This Demo version is only usable for demonstration, test or evaluation purposes. If you want to use the product for normal usage (ie. not for testing), you have to buy a license.
- Up to 5 permanent users and 5 visitor users can be added.
- Up to 2 devices (controller and/or terminal) can be used.
- Up to 2 cameras and 5 vehicles can be registered.

The Demo license can be used by inputting "**DEMO-DEMO-DEMO**" as the System ID (license key) when the installer asks. The Demo license should also be activated, and this requires Internet access.

Downloading the software

The software components of Predor can be downloaded from www.predoraccess.com. Contact your local distributor about login details. The installers are published for the following platforms:

- Microsoft Windows 10, 11 (64 bit)
- Microsoft Windows Server 2012, 2016, 2019, 2022 (64 bit)
- Ubuntu 20.04 LTS 64 bit

When downloading the installers please select the platform appropriate for your system. The downloadable files are offline installers and contain everything necessary to run the software, no additional significant network data usage is required during the installation process.

The Predor mobile applications can be downloaded from the Play Store on Android and from the App Store on iOS. These applications are free to download.

The Predor Enterprise Server is available in a Docker container format as an alternative to the installers obtained from www.predoraccess.com. You can find more information about installing and running Predor Enterprise Server in a Docker container in the appendix, at the end of this manual.



ATTENTION! It's important to keep your Enterprise software version up to date. The mobile applications can be updated from the store, and usually updates automatically. Other components of Predor (server and clients) are not updated automatically on purpose.
Your local system administrator must update the Enterprise server and clients manually. It's important to update these components to the same version together, as different server-client versions are not compatible!

Installing the Lite Edition

Installation prerequisites:

- Administrator privileges on the computer – the installer software must be executed with administrator privileges.
- Internet connection – during installation account credentials provided on website www.predoraccess.com are verified.



TIP: 1.5.9 or newer version of the Predor Lite software can be installed without active internet connection, because no installer authentication required.

Furthermore the minimum system requirements in the table below must be met. Recommended system parameters are for references only, as with increasing system complexity and user count even recommended parameters may become insufficient.



WARNING: We've seen that running the software in Hyper-V was drastically slower because virtualization slowed down IO operations, which caused database read/write to be slow.

Component	Minimum	Recommended
Processor (CPU)	2 GHz, 2 cores (eg. 10th Gen Intel Core i3 or equivalent)	2,4 GHz, 4 cores (eg. 10th Gen Intel Core i5 or equivalent)
Memory	4 GB RAM	8 GB RAM
Disk/storage	10 GB	100 GB
Display resolution	1920x1080 pixels	1920x1080 pixels
Network	100 Mbit Ethernet	1000 Mbit Ethernet

Table 1: System requirements

Creating a database

The system displays a database selection screen before login, where one can create a new database or select an existing one. Choose a directory where the program can write without administrator rights, for example, your own Documents (or Linux home) directory.



WARNING: The database can be neither in the same directory as the executable program nor in a subfolder of it.

First the database connection has to be named. Any name can be given. It will only be displayed in the database connection selector and helps when using multiple databases.

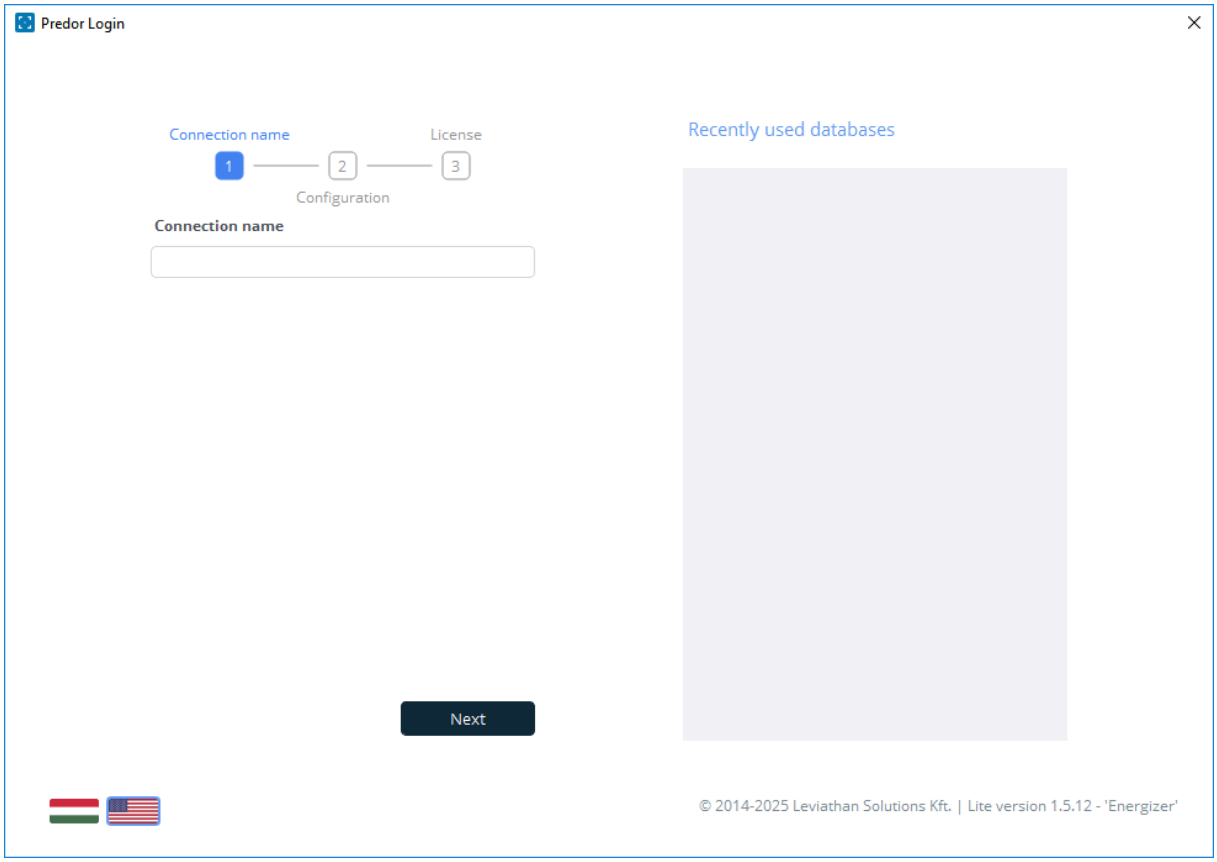


Figure 1: Type in a name for the database connection

Then create a new database with the “Create new” button. You can use an already existing database as well by selecting it using the “Browse” button.

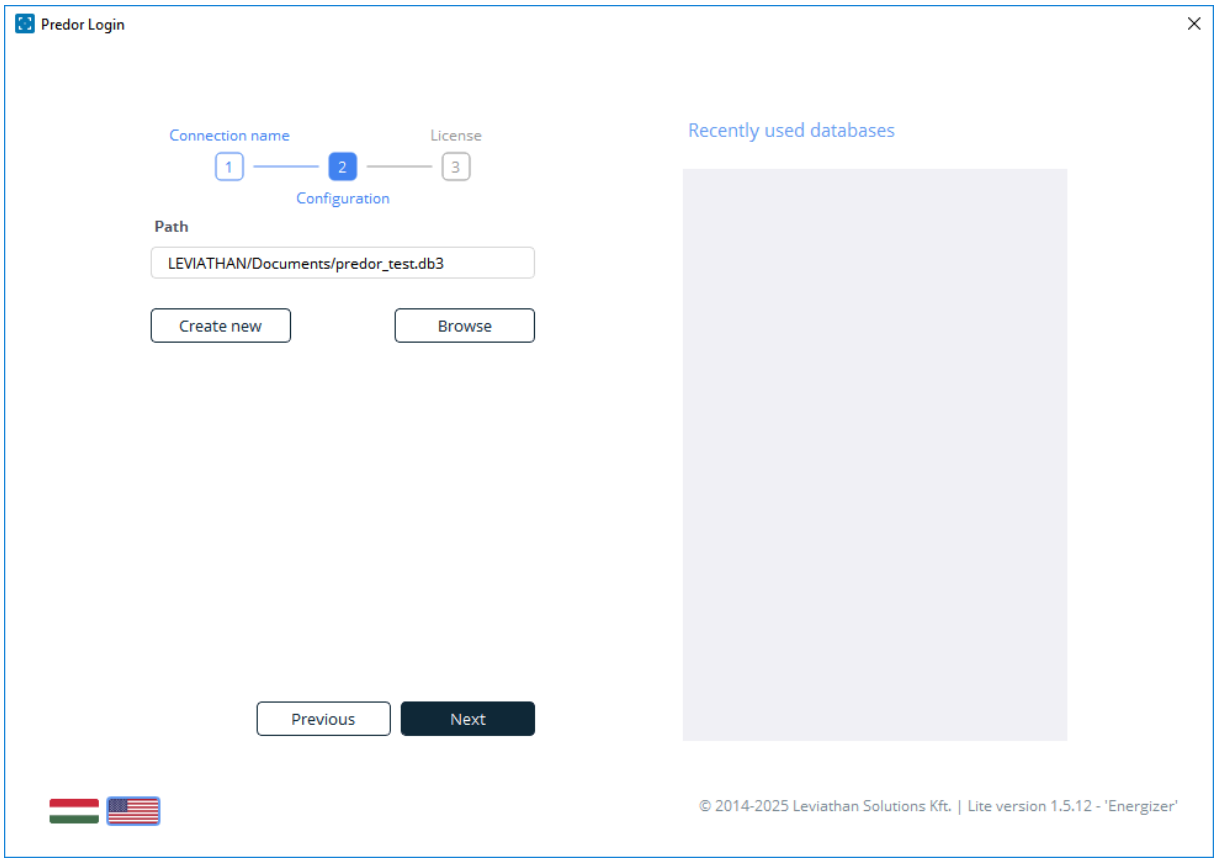


Figure 2: Create a new database

Loading the license

When a new database is created, the system requests the system ID, which you can check at www.predoraccess.com after logging in (installer login). This ID is a sort of license key that connects purchased modules and licenses to a particular system and makes the various functions available accordingly.

Checking the validity of the system ID requires internet connection, but it can also be done offline with a pre-downloaded license file, which can be obtained from the website. After adding modules to the license this procedure is used to refresh the license in the software too.

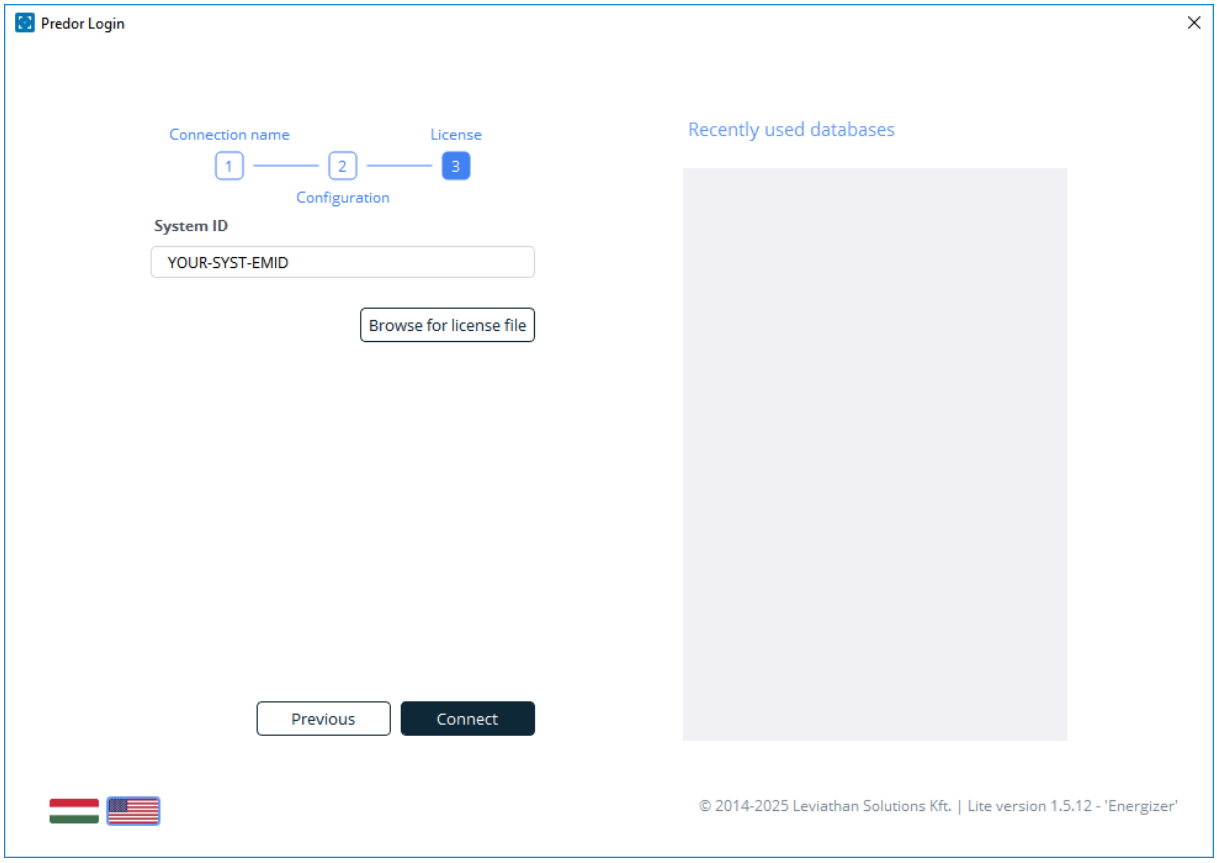


Figure 3: Inputting the system ID

If the database creation and license verifying were successful, the login page appears. You also have to activate the license. See also: Activate your license

Installing the Enterprise edition

ATTENTION! Installing the Enterprise edition requires system administrator skills.

Predor Enterprise edition components

The Predor Enterprise software stack consists of the following elements, with the supported platforms listed:

- Predor Enterprise Server [1]
  - Microsoft Windows 10, 11 (64 bit)

[1] graphical user interface-less application which runs as a system service and handles the connection to the database, access control units and clients, and provides the work time web page

    - Microsoft Windows Server 2016, 2019, 2022 (64 bit)
    - Ubuntu 20.04 LTS (64 bit)
- Predor Enterprise Client [2]
    - Microsoft Windows 10, 11 (64 bit)
    - Microsoft Windows Server 2016, 2019, 2022 (64 bit)
    - Ubuntu 20.04 LTS (64 bit)
- Predor mobile application [3]
    - Android 4.0 (or newer)
    - iOS 10.0 (or newer)
- Predor personal web [4]
    - Available in versions starting from 1.2.1, personal web license module required



ATTENTION! In order to be able to use the Predor Enterprise software stack a valid license is required. For more information please visit www.predoraccess.com.

Server installation

Prerequisites:

- You must have administrator privileges on the operating system. **The installers must be executed as administrator.**
- Active internet connection – the installer will require login credentials (username/password) before allowing to continue. Ask your distributor about details. (The verification of these credentials use minimal network data, so a mobile internet connection is sufficient.)



TIP: 1.5.9 or newer version of the Predor Server can be installed without active internet connection, because no installer authentication required.

The system must also meet the minimal hardware requirements listed in the table below. It's important to note that the exact requirements depend on the complexity of the system. For example in a system with several hundred users even the recommended requirements may be inadequate.

[2] graphical user interface enabled software for the operators to monitor and manage users, make work time reports, etc.

[3] intended to be used by operators to remotely monitor the system, open doors, help in case of evacuation

[4] intended to be used by employees and responsible people with desktop or mobile web browsers where (depending on configuration) they can check work time details, correct arrival/leave times, request day off or shift assignments

Component	Minimal	Recommended
Processor (CPU)	2 GHz, 4 cores (eg. 10th Gen Intel Core i5 or equivalent)	2,4 GHz, 4 cores (eg. 10th Gen Intel Core i7 or equivalent)
Memory	4 GB RAM	8 GB RAM
Disk (SSD recommended)	10 GB	100 GB
Network	100 Mbit Ethernet	1000 Mbit Ethernet

Table 2: Predor server system requirements



WARNING: We've seen that running the software in Hyper-V was drastically slower because virtualization slowed down IO operations, which caused database read/write to be slow. In our experience, this was especially true when using PostgreSQL database.

After completing the installation steps the server will run as a **system service**. The first time though, it will not start automatically, because a few additional configuration steps must be done before. The Predor Configuration Manager application which starts automatically after the server installation helps making these configuration steps.

The Predor Enterprise Server is available in a Docker container format as an alternative to the installers obtained from www.predoraccess.com. You can find more information about installing and running Predor Enterprise Server in a Docker container in the appendix, at the end of this manual.

Configuring the server

There are two ways to configure the server: by using the configuration tool installed during the installation process, or by editing the ini file manually. Using the second method is only recommended if you have basic system administration knowledge.

Configuration editor

The program that you can use to edit the configuration of the server on a graphical interface is automatically started after the installation process is finished. After that you can start it any time from the **bin** directory in the predor server installation directory by running "predor_iniman.exe" on Windows or "predor_iniman" on Linux. The configuration steps are:

1. **System ID**: In this step you must enter your system ID. Using the license check button will try to download the license from the Predor license server to check the system id's validity. This is an optional step to help you prevent typos in the id.

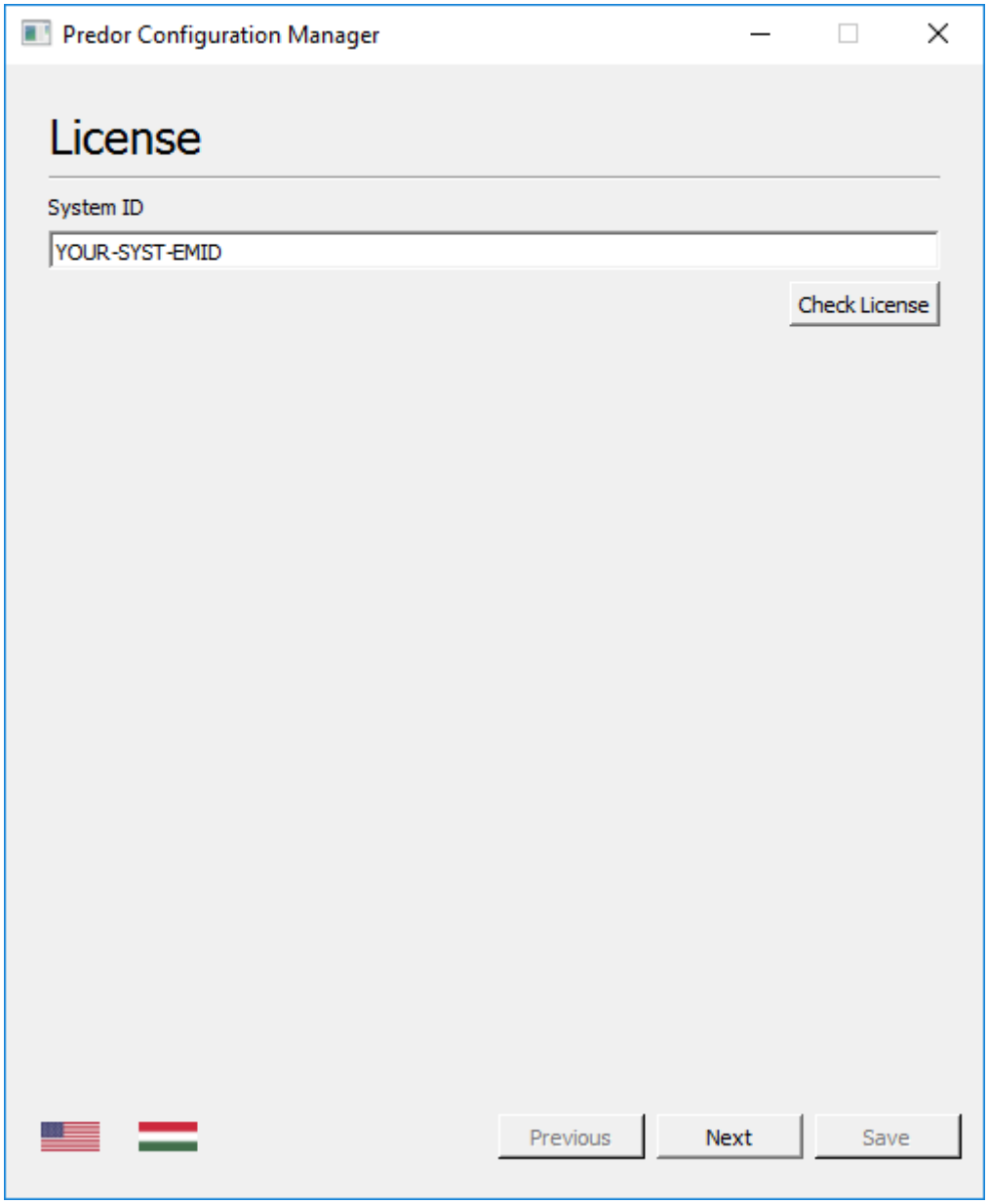


Figure 4: Predor Configuration Manager System ID page

2. **Database**: in the case of an SQLite database you only need to create a new database by using the create button, or select an existing database by using the browse button. Be aware that by using "create" you can overwrite an existing database. In the case of PostgreSQL or MSSQL database you must enter all the required connection information in this form, and use the check button to validate them. An encrypted configuration file can also be created by activating the Encrypt configuration file option.



WARNING: In case of SQLite, the database file must not be saved into the Predor Enterprise Server's folder or any subfolder of it! It is advised that the database is saved into a folder specifically created for this (e.g.: on Windows *C:\PredorData* and on Linux */var/predordata*)



WARNING: If PostgreSQL is chosen as the database engine, the time zone of the database must be matched to the server's time zone! The server cannot operate with incorrect time zone settings!



WARNING: When using an encrypted configuration file, a *predor_server.bin* file is created instead of a *predor_server.ini* file.

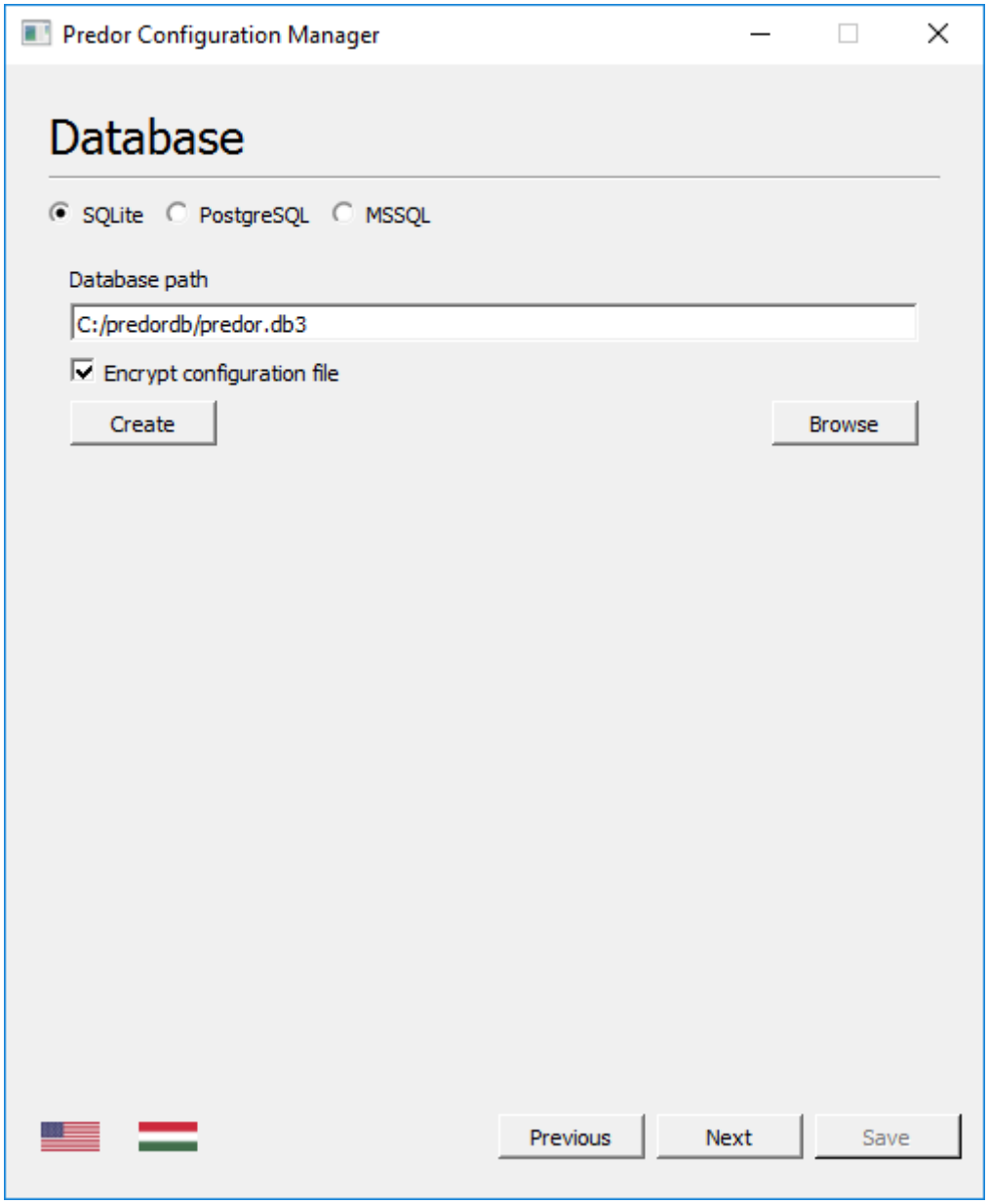


Figure 5: Predor Configuration Manager Database page

3. **API server settings**: the port configured here will be used to communicate between Predor server and clients, desktop and mobile. The IP address here is the server's listening IP address. 0.0.0.0 means that the server will be listening on all it's available addresses, so if you don't want to restrict the server to a specific IP you can leave the default value. You can also leave the default values for ports if no other application is using them on the server. If you want to use encryption you must browse the required files here.

ATTENTION! Using plain communication methods (without SSL) is insecure! Data streams between the server and clients can be easily monitored, replayed or modified and the system is vulnerable to attacks without HTTPS connection!

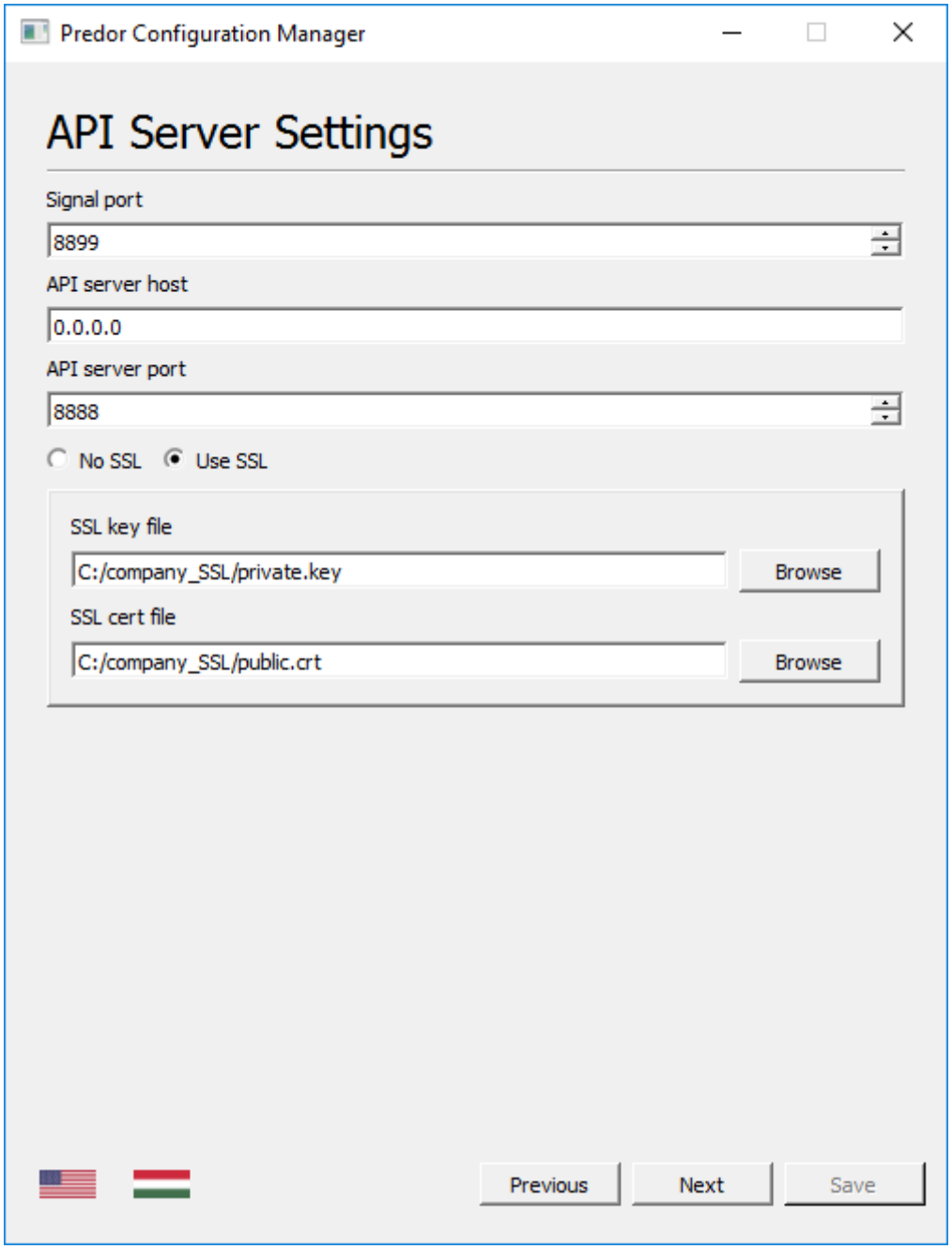


Figure 6: Predor Configuration Manager Communication settings

4. **Worktime web settings**: If you have purchased license for the personal web, you can configure the IP address and port where the web server will be listening here. Like in the API settings before, the default values are suitable for most use cases. The Base URL is optional, but recommended. You must write the URL that will be used to

access the site by the users, including the http[s]:// prefix.

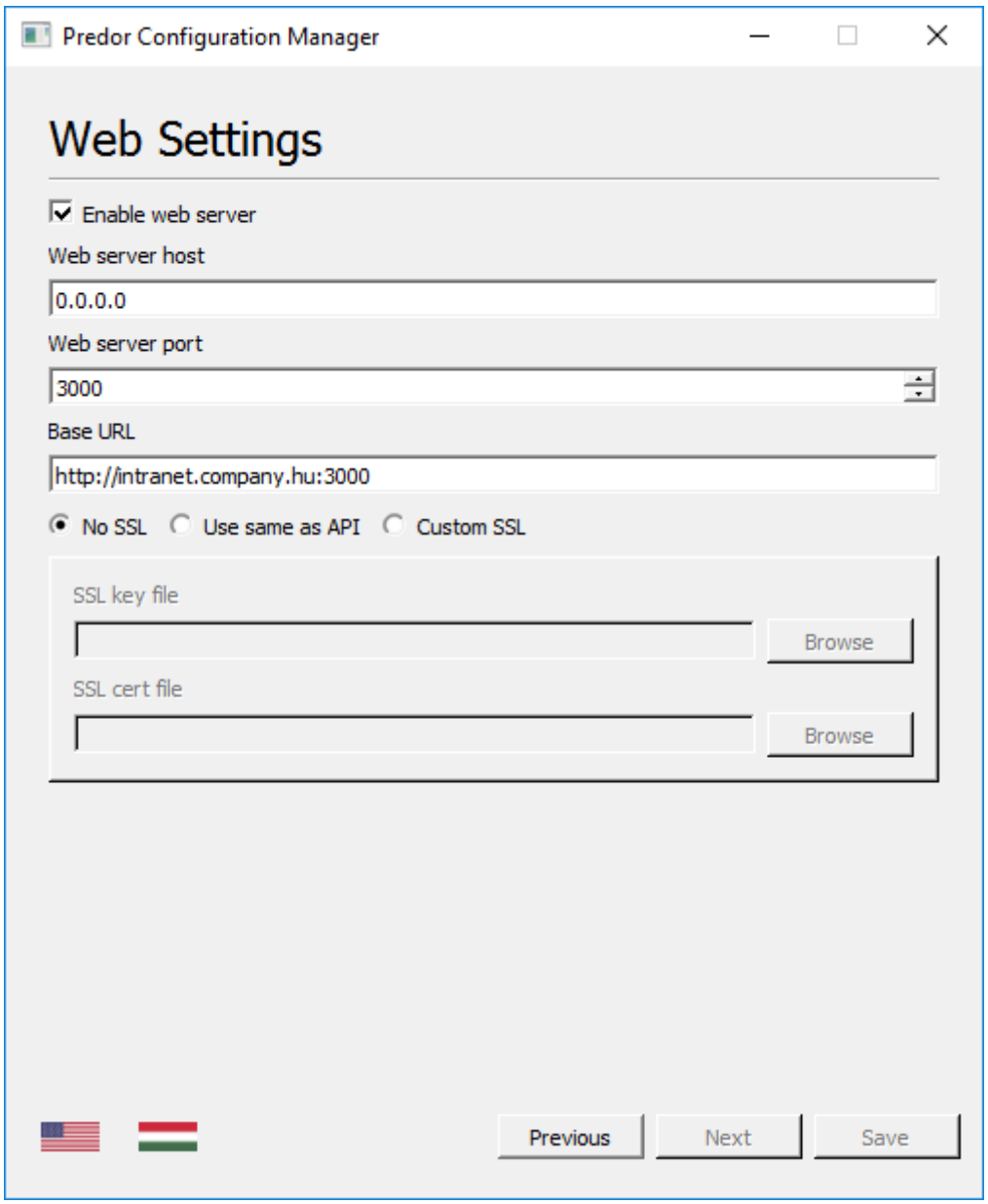


Figure 7: Predor Configuration Manager Worktime Web settings

Editing the configuration file manually



ATTENTION! Encrypted configuration file cannot be modified manually, only with predor_iniman application.

The server configuration file can be edited with administrator privileges. Path to the file:

- on Windows: **[installation directory]\bin\predor_server.ini**

- on Linux: **/etc/predor/predor_server.ini**

The configuration file contains the following settings:

- Database connection parameters (SQLite, PostgreSQL or MSSQL)
- The system ID associated with a license that has the Enterprise license purchased.
- The network settings for client-server communication. **You must open these ports on your firewall and network devices if necessary.**
- If possible use SSL encryption (HTTPS)

After saving the configuration file the service can be started.



WARNING: Without using SSL encryption (HTTPS) the communication between client and server can be recorded, played back, and manipulated, opening possibilities to attack the system.

Configuration file examples

During installation an example configuration file will be created. The following is an example of a complete ini file:



TIP: Lines that start with a semicolon (;) are skipped. You can write comments to each settings or temporarily disable lines with it.

```
[General]
path=D:/Databases/predor.db3
systemId=ABCD-1234-QWER
type=sqlite3

[Signals]
port=8899
sslCertFile=certs/leviathan_cer.cer|certs/leviathan_int.cer
sslKeyFile=certs/leviathan_key.key

[listeners]
1\cleanupInterval=10000
1\maxMultiPartSize=10000000
1\maxRequestSize=16000000
1\maxThreads=100
1\minThreads=4
1\port=8888
1\readTimeout=60000
1\sslCertFile=certs/leviathan_cer.cer|certs/leviathan_int.cer
1\sslKeyFile=certs/leviathan_key.key
size=1
```

This contains the following settings:

- The database is **SQLite**, using the path **D:\Databases\predor.db3**. In the ini file you must use the '**/**' character as path separator even on Windows.
- The system will use **TCP port 8899** for signals sent from the server to the client and the port **8888** for the API communication. These will be encrypted with the certificate provided.



ATTENTION! Always use non-self-signed SSL certificates if possible. The system works with self signed certificates, but this doesn't prevent a man in the middle type attack.



ATTENTION! Always use the same certificates in the API and signal communication. The client will only be able to successfully connect to the server if both are encrypted in the same way.

Another example that uses PostgeSQL database and unencrypted endpoints:

```
[General]
url=localhost
username=predor
password=predor
database=predordb
systemId=ABCD-1234-QWER
type=postgresql

[Signals]
port=8899

[listeners]
1\cleanupInterval=10000
1\maxMultiPartSize=10000000
1\maxRequestSize=16000000
1\maxThreads=100
1\minThreads=4
1\port=8888
1\readTimeout=60000

2\cleanupInterval=10000
2\maxMultiPartSize=10000000
2\maxRequestSize=16000000
2\maxThreads=100
2\minThreads=4
2\port=9999
2\readTimeout=60000

size=2
```

This contains the following settings:

- The PostgreSQL server runs on the same computer as the Predor server (*url=localhost*).
- The PostgreSQL login name and password is "*predor*"
- The PostgreSQL database name is "*predordb*"
- The system will use **TCP port 8899** for signals sent from the server to the client by using a non-encrypted channel (not recommended).
- The server listens on ports 8888 and 9999 for client connections without using SSL. Connection parameters can be customized with prefixes "1\" and "2\" respectively.

If the Work Time Web module is available the INI file must be extended with its configuration settings. Naturally you can use SSL encryption here as well. The next example will show you these settings. Only the text highlighted in yellow belong to the web interface. If you would not like to use SSL encryption, then delete the pair of rows that start with "ssl".

```
[General]
path=D:/Databases/predor.db3
systemId=ABCD-1234-QWER
type=sqlite3

[Signals]
port=8899
sslCertFile=certs/leviathan_cer.cer|certs/leviathan_int.cer
sslKeyFile=certs/leviathan_key.key

[listeners]
1\cleanupInterval=1000
1\maxMultiPartSize=10000000
1\maxRequestSize=16000000
1\maxThreads=100
1\minThreads=4
1\port=8888
1\readTimeout=60000
1\sslCertFile=certs/leviathan_cer.cer|certs/leviathan_int.cer
1\sslKeyFile=certs/leviathan_key.key
size=1

[webapps]
1\webAppKey=worktimeweb
1\cleanupInterval=1000
1\host=0.0.0.0
1\maxMultiPartSize=10000000
1\maxRequestSize=16000000
1\maxThreads=100
1\minThreads=4
1\port=3000
1\readTimeout=60000
1\sslCertFile=certs/leviathan_cer.cer|certs/leviathan_int.cer
1\sslKeyFile=certs/leviathan_key.key
size=1
```

Loading the License

Upon first start, if the server is able to reach the Internet, the license is downloaded automatically. You will also have to activate the license. See also: Activate your license Checking the validity of the system ID requires internet connection, but it can also be done offline with a pre-downloaded license file, which can be obtained from the website www.predor.hu. You have to place the downloaded file to the same folder, where the configuration file (predor_server.ini) is located:

- On Windows it is the “bin” folder in the installation directory, where the executable

program is also located (eg. **C:\Program Files\PredorEnterpriseServer\bin**)

- On Linux it is the **/etc/predor** directory



CAUTION: The file should not be renamed, its correct name is the same as your system ID, and its extension is ".lic", for example: **ASDF1234QWER.lic**.

Starting the server

After the configuration is finished, the server can be started either by rebooting the computer or – depending on the operating system – by the following methods:

- On Windows the service can be started in the Task Manager's services tab. If everything is correct, the service runs constantly, it's PID is not changing.
- On Linux the following command can be used to start the service:

```
sudo systemctl start predor
```

and the following command can be used to check its status:

```
systemctl status predor
```



TIP: If we want to stop or restart the service, on Windows the Task Manager can be used. On Linux it can be done by issuing the following commands: "sudo systemctl stop predor" and "sudo systemctl restart predor"

Test information page

If the server functions correctly we should see an information page if we connect to one of its endpoints using a browser. By default, the API is using the port **8888**:

- When using HTTPS: https://127.0.0.1:8888 – you can ignore the browser's certificate error warnings
- Without HTTPS: http://127.0.0.1:8888

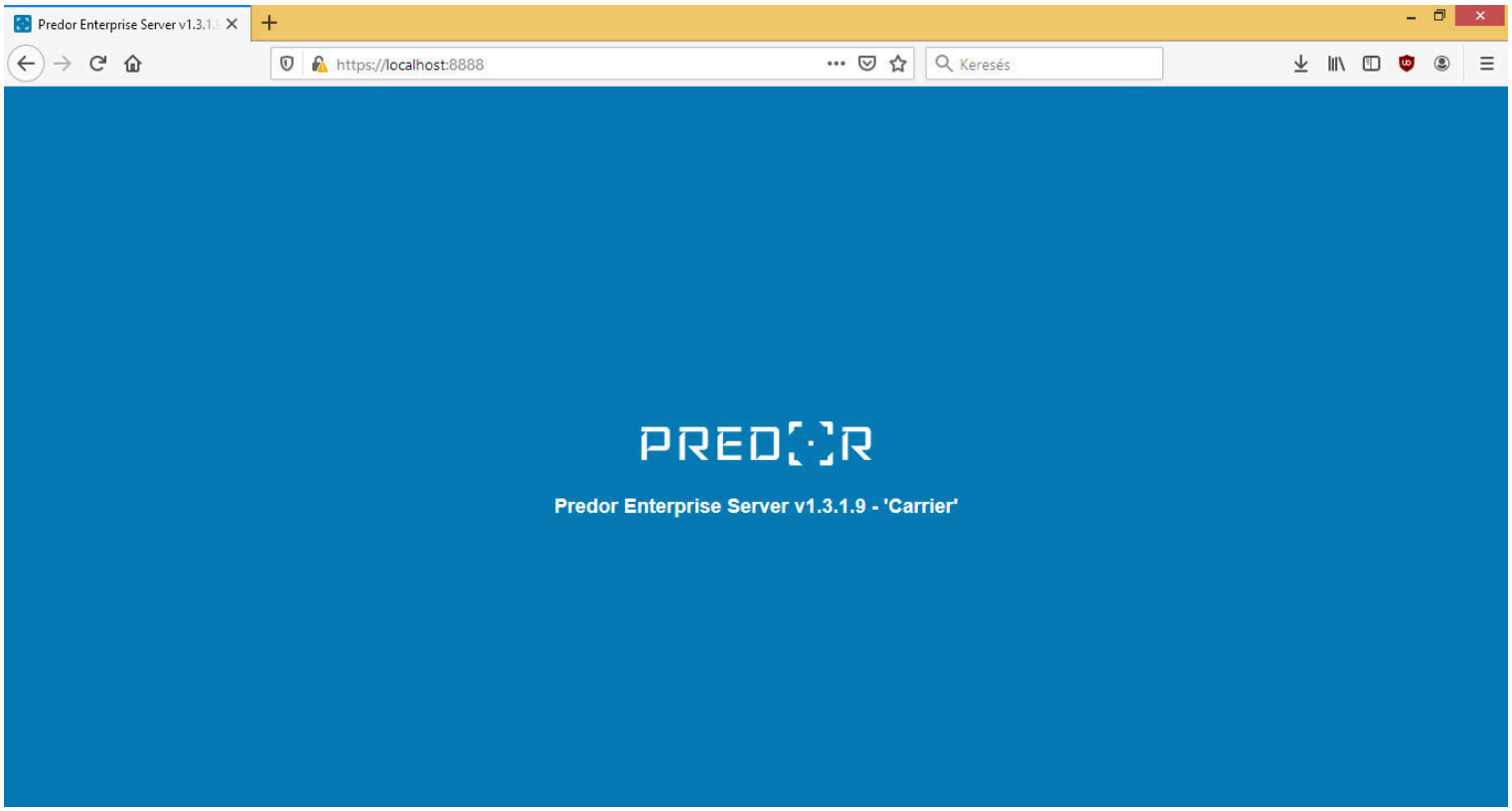


Figure 8: Predor server test information page

ATTENTION! Using plain communication methods (without HTTPS) is insecure! Data streams between the server and clients can be easily monitored, replayed or modified and the system is vulnerable to attacks without HTTPS connection!

ATTENTION! If the server is already running, then the changes to the INI file will only take effect after restarting the service. You should restart it after every modification.

Personal web interface

By purchasing the license the personal web interface will become available, which can be used by the employees to register off-site work, view their worktime data, ask for its correction or for a day-off. Their supervisors can approve day-offs and correction requests, assign them to shifts and check their worktime data.

If we did everything correctly, then on the port we selected (3000 by default) we can look

at the personal web interface's home screen.

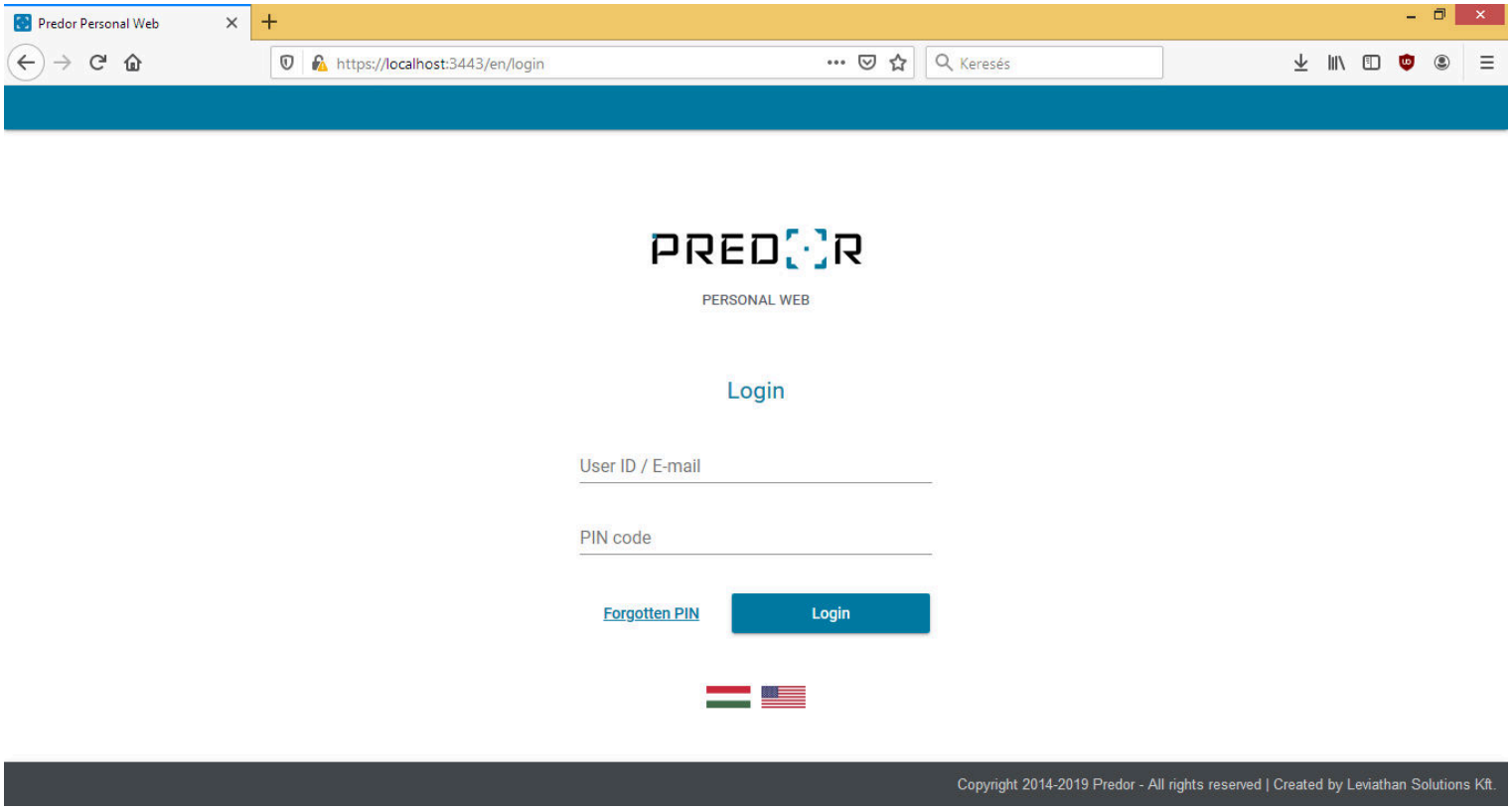


Figure 9: Predor Personal Web login page

Logging

The server logs the important events into a file. The log files can be found in the following locations – assuming that the program was installed with default settings and the services are ran by the default user:

- Windows (64 bit):

C:\Windows\System32\config\systemprofile\AppData\Local\Leviathan Solutions\Predor Server\Predor\logs

- Ubuntu (64 bit):

/var/log/predor.log

New files are created daily, to make it easier to search in the logs. If the server service does not run continuously or the test information page can not be displayed, the logs can help determine the problem.

Client installation

Prerequisites:

- You must have administrator privileges on the operating system. **The installers must be run as administrator.**

The system must also meet the minimal system requirements listed in the table below. It's important to note that the exact requirements depend on the complexity of the system. For example in a system with more than 1000 users even the recommended requirements may be inadequate.

Component	Minimum	Recommended
Processor (CPU)	2 GHz, 2 cores (eg. 10th Gen Intel Core i3 or equivalent)	2,4 GHz, 4 cores (eg. 10th Gen Intel Core i5 or equivalent)
Memory	4 GB RAM	8 GB RAM
Disk/storage	10 GB	10 GB
Display	1920x1080 resolution	1920x1080 resolution
Network	100 Mbit Ethernet	1000 Mbit Ethernet

Table 3: Predor client system requirements



WARNING: We've seen that running the software in Hyper-V was drastically slower because virtualization slowed down IO operations, which caused database read/write to be slow. In our experience, this was especially true when using PostgreSQL database.

When installing on Ubuntu, if the installer didn't run as administrator (by using sudo command), the following commands must be executed to install the required packages:

```
sudo apt update
sudo apt install libgstreamer-plugins-bad1.0-0 libgstreamer-plugins-base1.0-0
libgstreamer-plugins-good1.0-0 libgstreamer1.0-0 gstreamer1.0-libav
gstreamer1.0-plugins-ugly libqt5quick5 libqt5qml5 libqt5x11extras5
libqt5serialport5 libqt5multimedia5 libqt5multimediawidgets5 libqt5svg5
libqt5webengine5 libqt5webenginewidgets5 qml-module-qt-labs-settings
qml-module-qt-labs-folderlistmodel qml-module-qtquick-controls
qml-module-qtquick-dialogs libqt5printsupport5 libqt5sql5 libqt5concurrent5
libqt5sql5-sqlite libqt5sql5-psql libqt5sql5-odbc libpq5 libqt5networkauth5
```

The client can be installed just like the Lite version, then started by the shortcut. Instead of choosing a database a host must be selected, which has to be reachable by the client through the given ports.



TIP: If the client is started with the --lastuser switch, the last used operator name will be filled automatically.

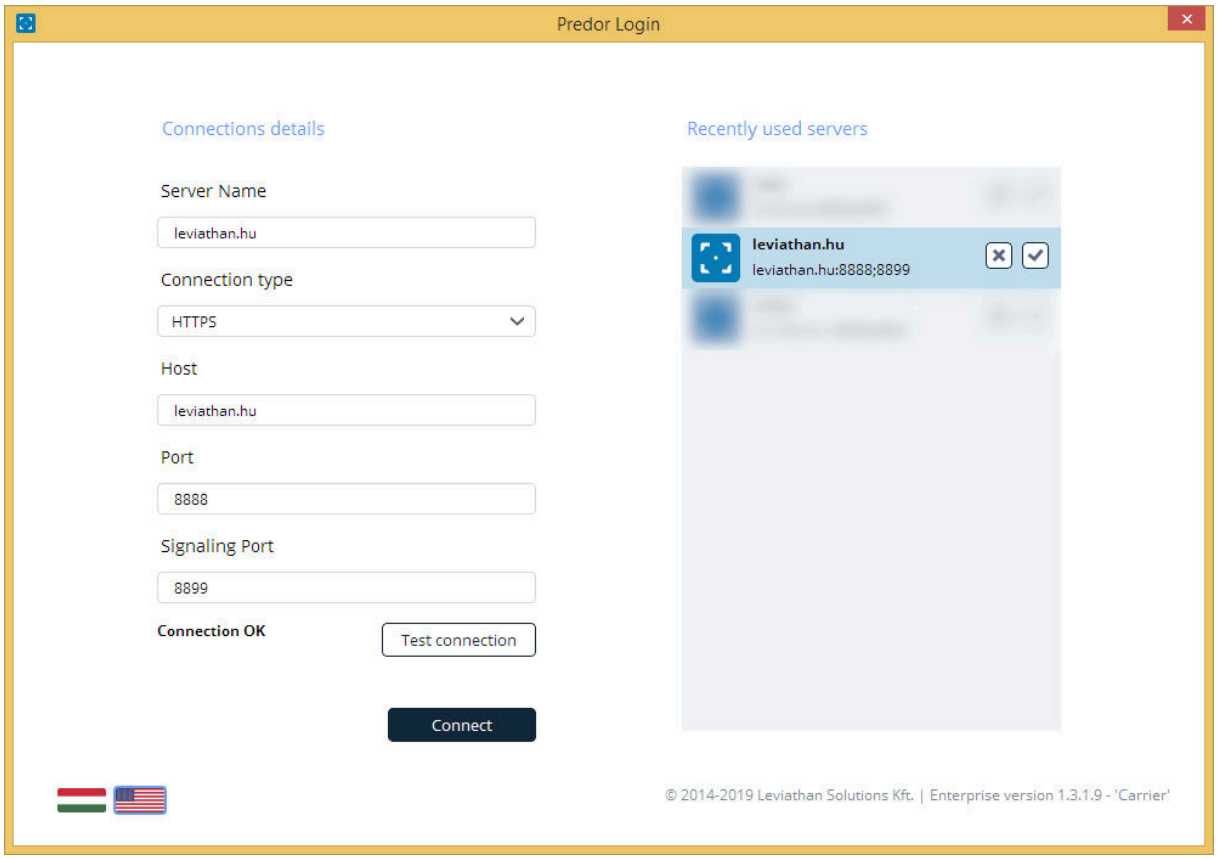


Figure 10: Predor client host selector window

Configuration

- **Server name**: custom name, referring to the connection
- **Connection type**: according to the server settings (**from the safest to the least safe**):
  - HTTPS: SSL connection with certificate authentication
  - HTTPS (self-signed): SSL connection with self-signed certificate
  - HTTPS (internal): SSL connection with a certificate for internal address – it is needed when the server is reachable through an internal name (eg. test.local) or through an IP address (eg. 192.168.5.50)

    - HTTP: communication without encryption
- Host: The host's name or IP address
- Port: communication port (default: 8888)
- Signaling port: the server sends its signals on this port (default: 8899)

Software upgrade



ATTENTION! The server and all the clients must be upgraded together.



ATTENTION! Keeping the software up to date is particularly important in the Enterprise version. The mobile application is automatically updated due to it being distributed over the marketplace, on the other hand other components of the Predor software (server and clients) are deliberately not.
The local administrators can manually upgrade the server and the clients separately. It's important that these should happen at the same time.



CAUTION: If your system uses custom plugins, those are not updated automatically, and have to be downloaded from www.predoraccess.com manually after signing in with installer credentials. If you don't have login information, ask your installer for a system update. If you are not sure if your Predor system uses plugins, you can check it under the Help/About menu in the software.

Upgrading the server

If a new software update becomes available the system will display a notification on the dashboard. The software upgrade has to be started manually.

The server must be upgraded first. In order to get ready for the update the clients must be closed, and the server service has to be stopped.

- On Windows the Task Manager's Services tab can be used to stop the PredorEnterPriseService
- On Linux the following command can be used to stop the service:

```
sudo systemctl stop predor
```

and the following command can be used to check its status:

```
systemctl status predor
```

If the service has successfully stopped, first **make backups of the database**! It is also good practice to make backups of the software installation directories.

If everything is set, start the “Maintenance tool” application which is located in the installation directory. The Maintenance tool connects to the software repository server, downloads and updates all necessary files to the latest version. After the Maintenance tool finished, the software can be restarted.



WARNING: Always make backups from the database and the configuration INI file before updating the software. After the update be sure to check if the INI file is in its location and its content is correct.

After the server is up to date, the clients also have to be updated.

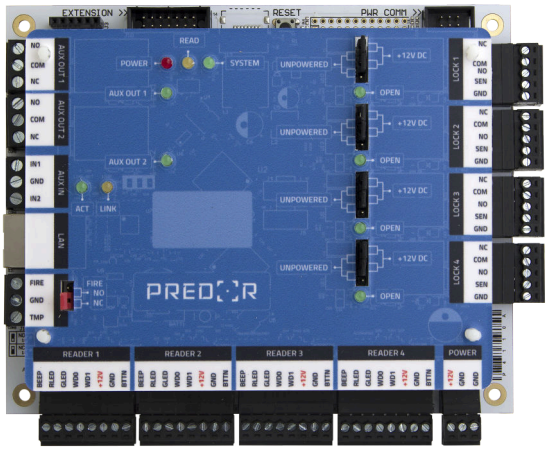
Upgrading the clients

This software update is also done with the “Maintenance tool” found in the installation directory. First of all close the running client, if there is one, then start the “Maintenance tool” program.

Before the update a backup should be created of the installation directory. The Maintenance tool connects to the central server and downloads and installs the latest available version. After it’s finished the updated software can be launched.

If everything went well the client can connect back to the server.

2 CONTROLLER LED FEEDBACKS



Power LED: lit if ACU is powered

Read LED: flashes for 1 second if a readable card number arrives, flashes 4 times rapidly if a parity error is detected (WD0 and WD1 may be swapped)

System LED: flashes once per second if ACU is functional, flashes rapidly if internal date and time is incorrect or not set.

Relay LEDs: lit while relay is operating

ACT LED: flashes when Ethernet communication is in progress

LINK LED: lit while Ethernet link is operational

3 FIRST STEPS

Login

The language of the login popup window can be set by clicking on the flags below. The software's language can be changed after login.

If you are to change the database, click on the "change database" button.

The database type of the LITE version is **SQLite**.

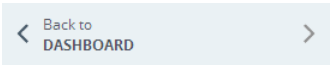
The last used database will be opened if you don't choose.

For newly created databases the default username: admin, password: admin

In case of the ENTERPRISE version, if the connection between the server and the client is lost, the client initiates a short reconnection attempt. If it fails, you will be returned to the login screen.

Software interface

The main menu items are in the header. By clicking on these, the submenus are listed on the left. Clicking on the Predor logo will return you to the dashboard.

Use the arrow keys 

to move forward and backward through the previously opened windows, just like internet browsers.

On the right side of the header you can use the quick search to find the desired functions or menus.

In case of an alert, the color of the header changes to red. The alert messages are displayed at the quick search location and further operations can be performed by opening the drop down menu and clicking on the additional operations ••• button.

The Upload button turns yellow when there are pending changes waiting to be uploaded to the controllers.

By clicking on the column title in the gray header of the tables, they can be sorted according to the content of the column (except the monitoring window). The width of the columns can be changed.

Filters: You can save your filtering criteria with the save icon and load it later with just one click. You can also pin your saved filters on the dashboard.

Edit button: to avoid accidental changes, you need to enable the editing with the edit button. In some menus, the drag and drop function is also activated by this button.

4 PREDOR MOBILE APPLICATION

The Predor mobile application can be downloaded from the appropriate app store (App Store (iOS) or Google Play Store) for free of charge. After installation the server connection parameters need to be typed in – just like in the Predor client. The mobile app does not use the signaling port.

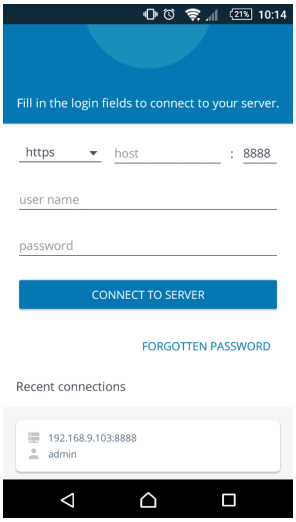


Figure 11: Predor mobile app login screen

After successfully signing in the dashboard is displayed where the latest unseen alerts, number of people inside and outside are shown. This behaviour can be changed by tapping the cogwheel icon on the upper right. If there are any alerts that have not been acknowledged the app header turns to red.

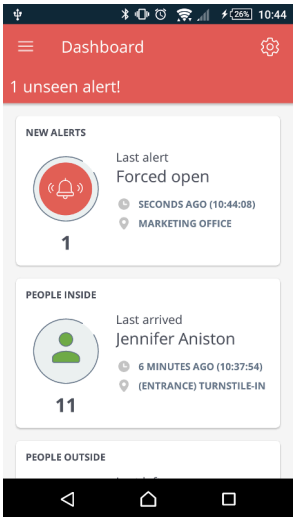


Figure 12: Predor app dashboard screen

A menu can be accessed by swiping from the left edge of the screen (or by using the upper left icon in the dashboard) where further operations can be performed:

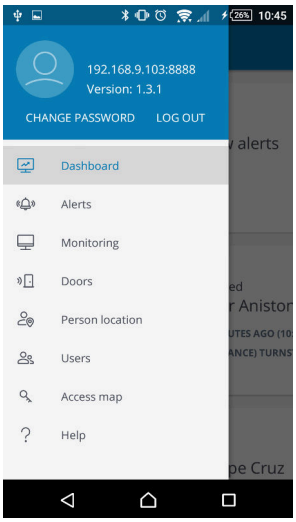


Figure 13: App menu

- List the alerts registered in the system. By tapping the eye icon on the upper right alerts can be acknowledged and the app's header returns to blue until the next alert event.

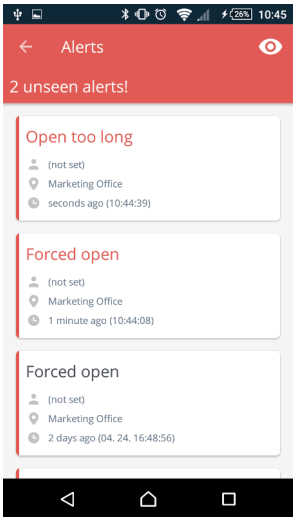


Figure 14: Alerts view

- View events in chronological order. This is similar to the Predor client's Monitoring view. Monitor profiles created in the client software are used here too.

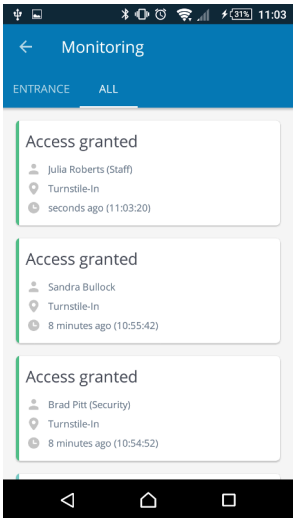


Figure 15: Monitoring view

- List the doors in the system. Doors can be opened remotely if needed. Tapping on a door shows its details where the latest events can be viewed or the applied door profile can be changed.

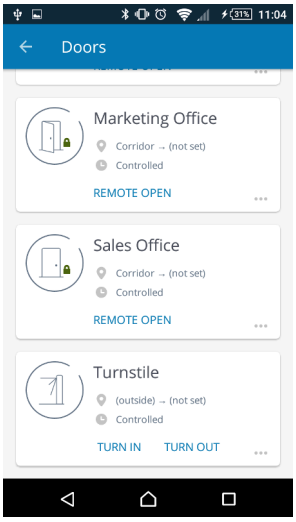


Figure 16: Doors view

- View the location of people by:
  - relative position to the system (inside, outside, unknown)
  - subject (lists everyone with their last known location)
  - location (lists every location and who is inside them)

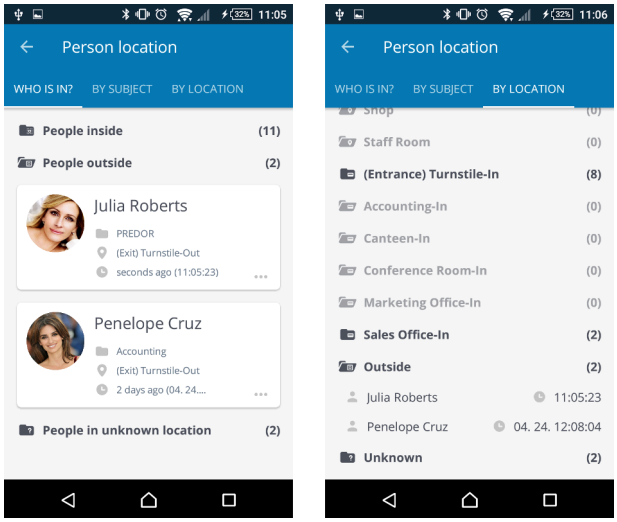


Figure 17: Person location views

- Display all users and visitors currently in the system. Users are organized into the department tree and visitors into visitor types. Tapping on users shows the details of the chosen person where the last events can be viewed or the user can be disabled.

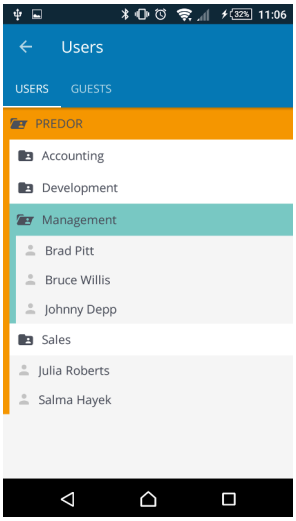


Figure 18: Users view with the department tree

- View access privileges grouped by locations or subjects (users and access groups). Access privileges in the form of time profiles determine if the subject gains access to a door.

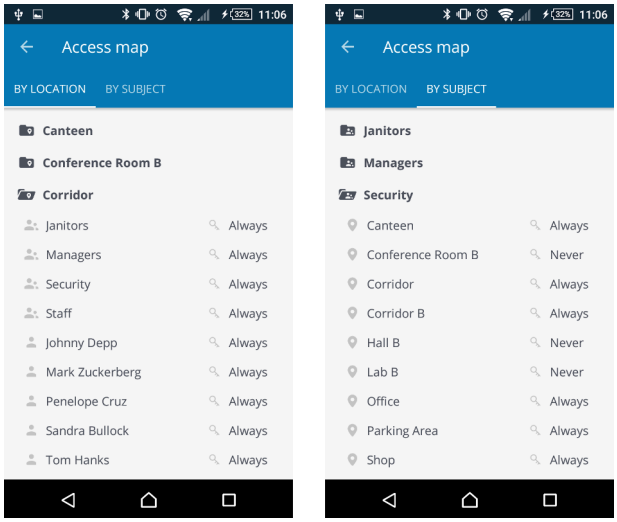


Figure 19: Access map views

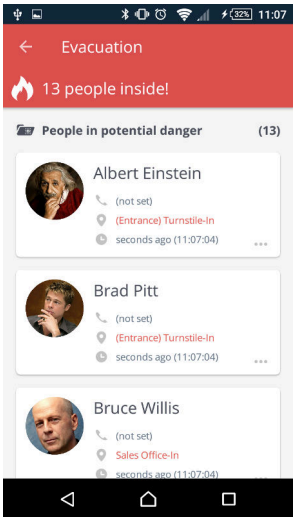


Figure 20: Evacuation screen

In case of a fire alert (evacuation) the Predor mobile application immediately shows the evacuation screen where people inside are listed. Users who register their cards on any reader marked as exit or on readers that belong to an other evacuation area are removed from this list automatically. Operators can remove users manually by swiping them off the list if they are confirmed to be in safety. The evacuation list is constantly refreshed and distributed to all operators.

5 MONITOR MENU

Dashboard

The start screen of the software is the Dashboard menu, which provides a quick overview of important system events. Each tile can be expanded for details or these can navigate you to the certain menu.

By clicking on the “pin” icon in different menus, the saved filters and profiles are pinned as a shortcut. These links are used to load the saved filters or profiles just by one click.

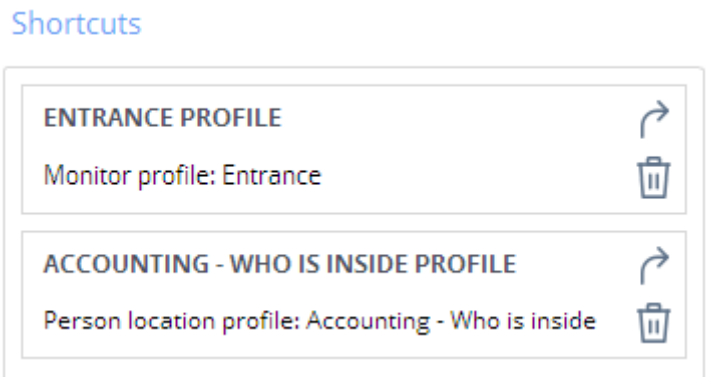


Figure 21: Shortcuts in the Dashboard page

The first steps tile guides you through the system configuration steps, each icon function as a link. A green check mark will appear on the icon if the configuration is done, and a red X sign if a configuration step is missed.

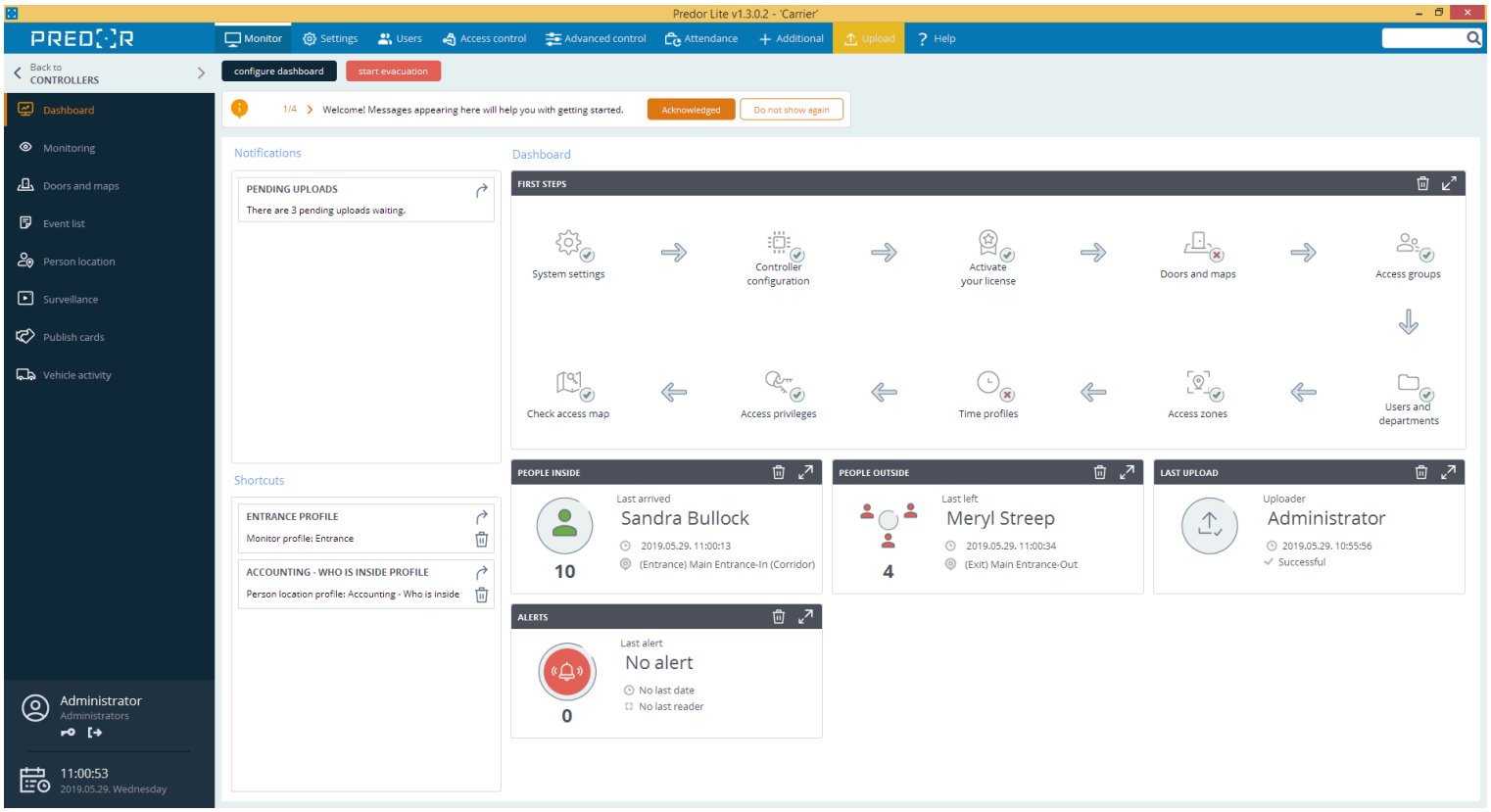


Figure 22: Dashboard page



TIP: After each setup step you can simply return to this window with the “back” arrow.

Click the following links to jump to the appropriate point in the document:

1. step: System defaults
2. step: Controllers
3. step: Activate your license
4. step: Doors and maps
5. step: Access groups
6. step: Users and departments
7. step: Access zones
8. step: Time profiles
9. step: Access privileges
10. step: Access map

Monitoring

The Monitoring window is used for real-time monitoring of the system, the events are listed in chronological order. This is a universal window where you can view the photos of the users and the current status of the doors.

The menu can be easily personalized, so the guards, operators or managers also get the information they need.

By **creating new monitor profiles**, the users can tailor real-time view to their needs. The events can be filtered by doors, types. Additionally the alert display mode can be changed.

Alerts can be displayed as multi-functional tiles, which can directly navigate you to the map view, to data sheets, etc.

The events can be paused and resumed at any time.

In the event line the user's photo, the department, the access group can be displayed by pointing to this icon:

You can change the screen layout. Three different layout can be chosen with this selector:



Mixed View: the photos of the last two authorized users are displayed next to the event list.

Guard View: Large images is displayed of the last two authorized users, so the guards can easily compare the cardholder's photo with the person just entering.

Event list view: if there are no photos uploaded from the users, this view should be chosen.

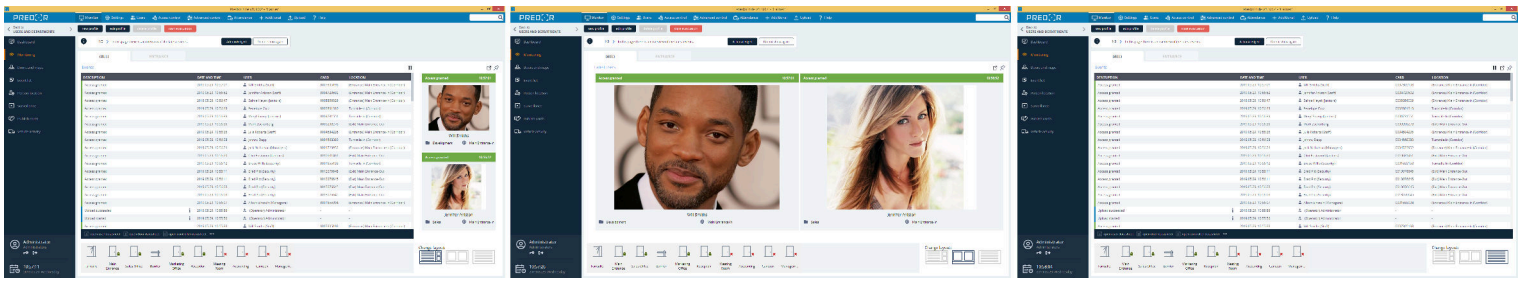


Figure 23: Monitor layouts

TIP: Select a door and with a right click you can choose options from a drop-down list. You can change the door's profile, open the door, view the datasheet etc.

TIP: Create a new profile and select the event types and the doors you are interested in.

TIP: Open the monitoring in a new window to keep an eye on the events while you are checking another menu.

Doors

Graphic feedback on the current status of the doors is also provided. Right-click to perform quick operations on each door. For instance, you can initiate a remote open.

The current status of doors is indicated by the following icons:

 alert, opening sensor is closed

 alert, opening sensor is open

 door is kept locked, but opening sensor is open

 door is kept locked, opening sensor is closed

 door is unlocked, opening sensor is closed

 door is locked, opening sensor is closed

 door is unlocked, opening sensor is open

 door is locked, opening sensor is open

 no connection with the door

Display and management of alerts

Alerts are highlighted in red in the event list and the current alerts can be viewed in the drop-down menu on the right side of the header.

If you choose the **pinned alerts** option in the edit monitoring profile window, the alerts will be displayed in multifunctional tiles, which can directly navigate you to the map, data sheets, etc.

SUGGESTION: The cameras on the network can be assigned to doors, thus the live stream of the certain cameras can be automatically displayed in case of an alarm if needed.

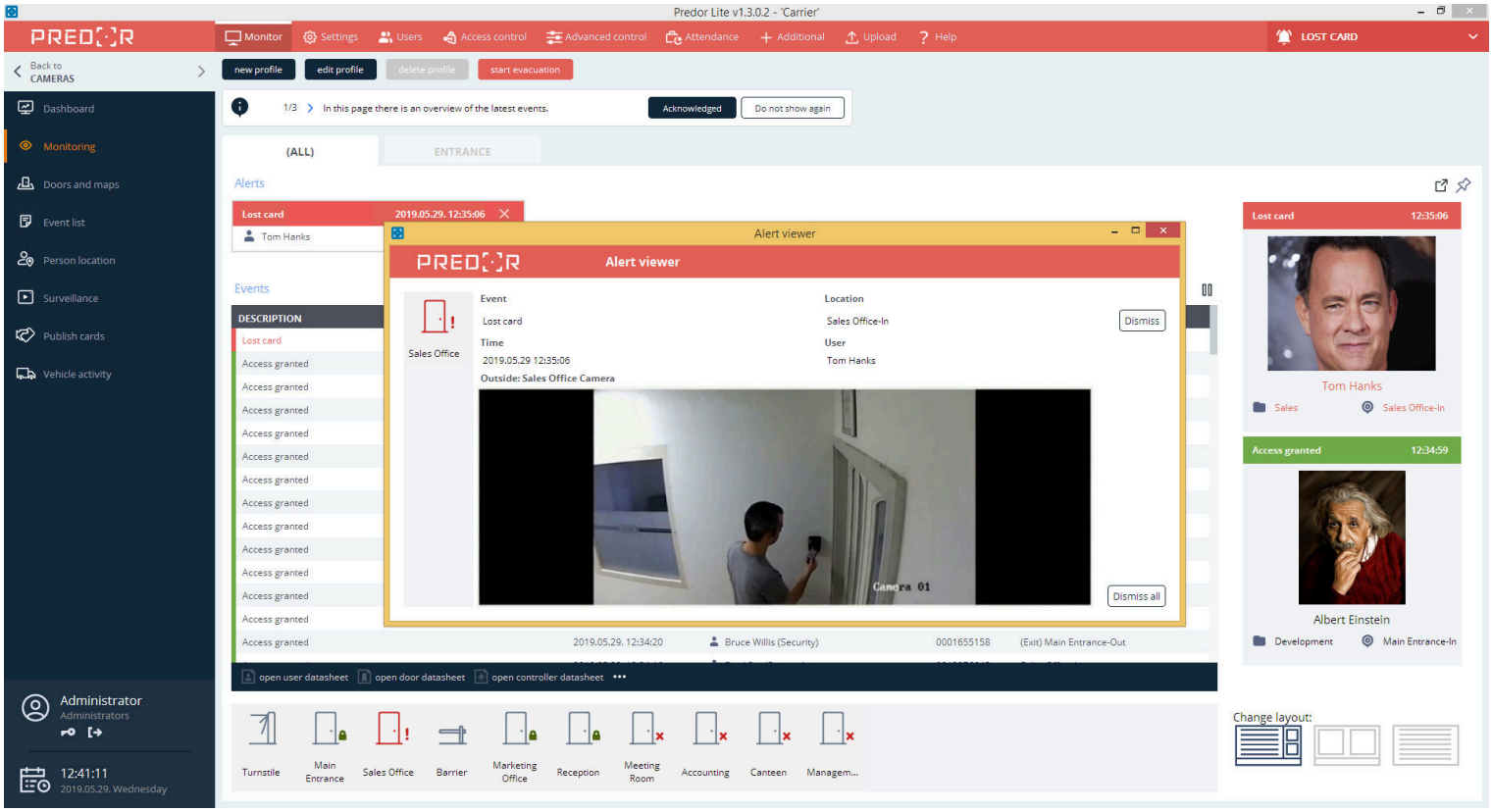


Figure 24: Alert viewer window

SUGGESTION: The location of the alarm event is instantly displayed on the map view.

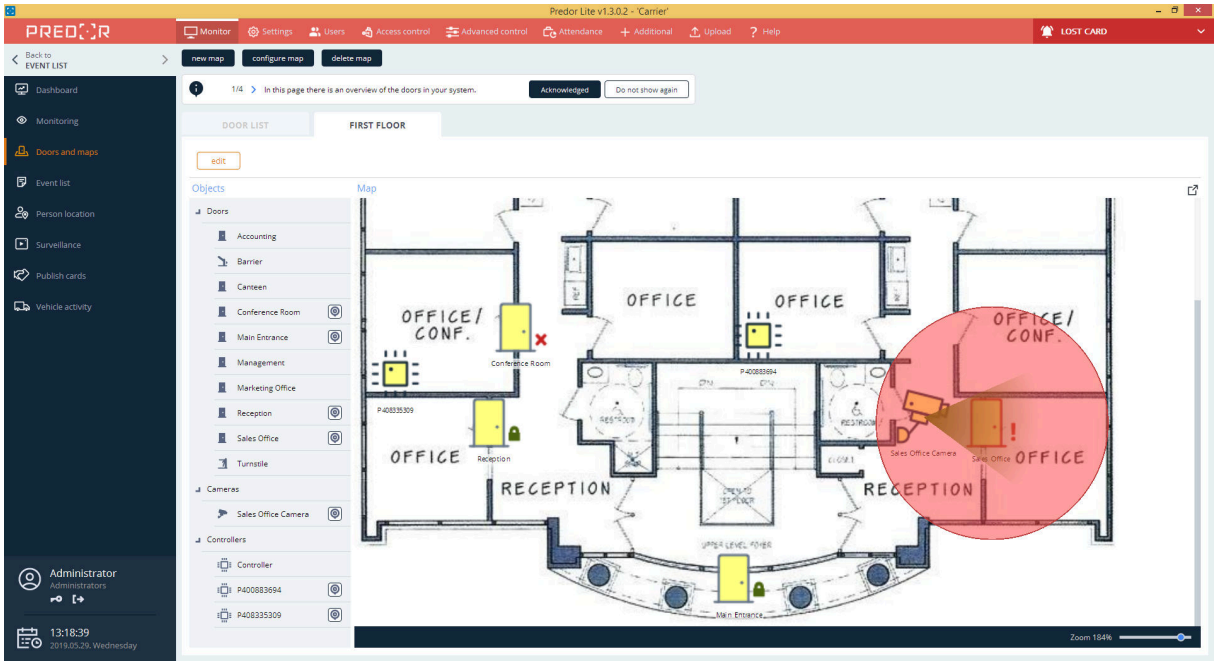


Figure 25: Map view with an alert on a door

Evacuation list

In the event of fire the system automatically generates a list of the people inside. This helps to find out immediately who is potentially in danger.

If Enterprise version is installed, the list is sent automatically by e-mail to the appropriate people, and the evacuation can be handled with the Predor mobile app. In addition the location of people can be seen real time.

Evacuation can be done per building and even multiple can run in parallel.

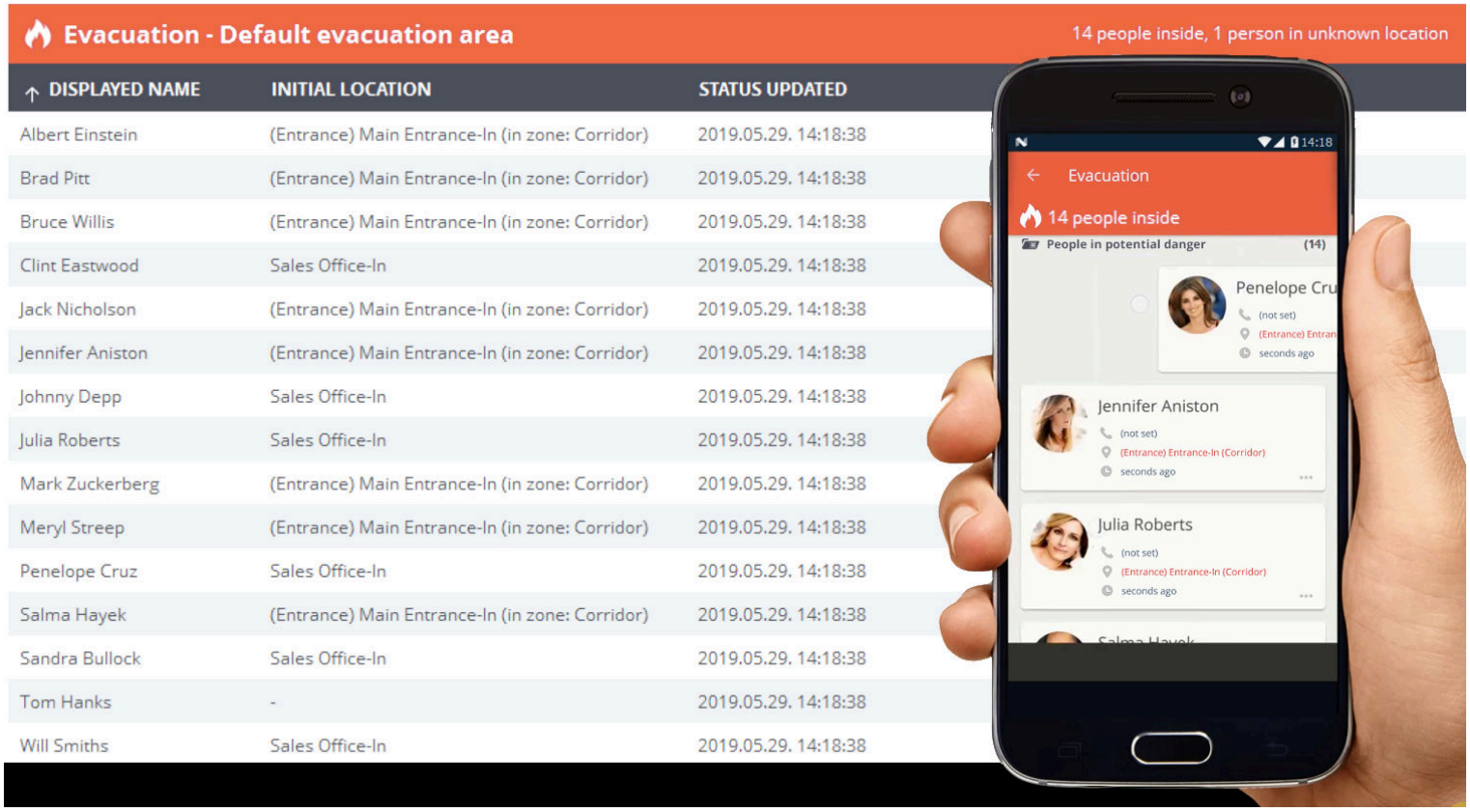


Figure 26: Evacuation list and mobile application view

TIP: Install a reader at the fire assembly point and the people who swipe their cards will be removed from the list immediately. This way it quickly turns out who is potentially in danger.

Doors and maps

In the Doors and Maps menu maps and floor plans can be uploaded of the object. The icons of gateways, cameras, and controllers can be placed on the map. The size and color of the icons can be customized. The current status of each door can be seen on the icons. Just click on a camera icon and view the live stream of the camera.

Doors

The first tab shows the system doors with graphical real-time status feedback. Clicking on the icons of each gateway will display a preview of the most important parameters of the door. The operating mode and the time profile of the door can be seen on the preview right side.

In the “Assign Profile” dialog window (accessible via the ••• button on the lower left actions bar) previously created door profiles can be assigned to one or more doors with specified time intervals if needed.

EXAMPLE: If you select a door and assign the “Keep closed” door profile to it from 13.12.2016 6:00PM and do not specify and ending time, then the door will switch to closed mode at that time and no one can enter from there.

Right-clicking on the icons allows you to perform additional operations.

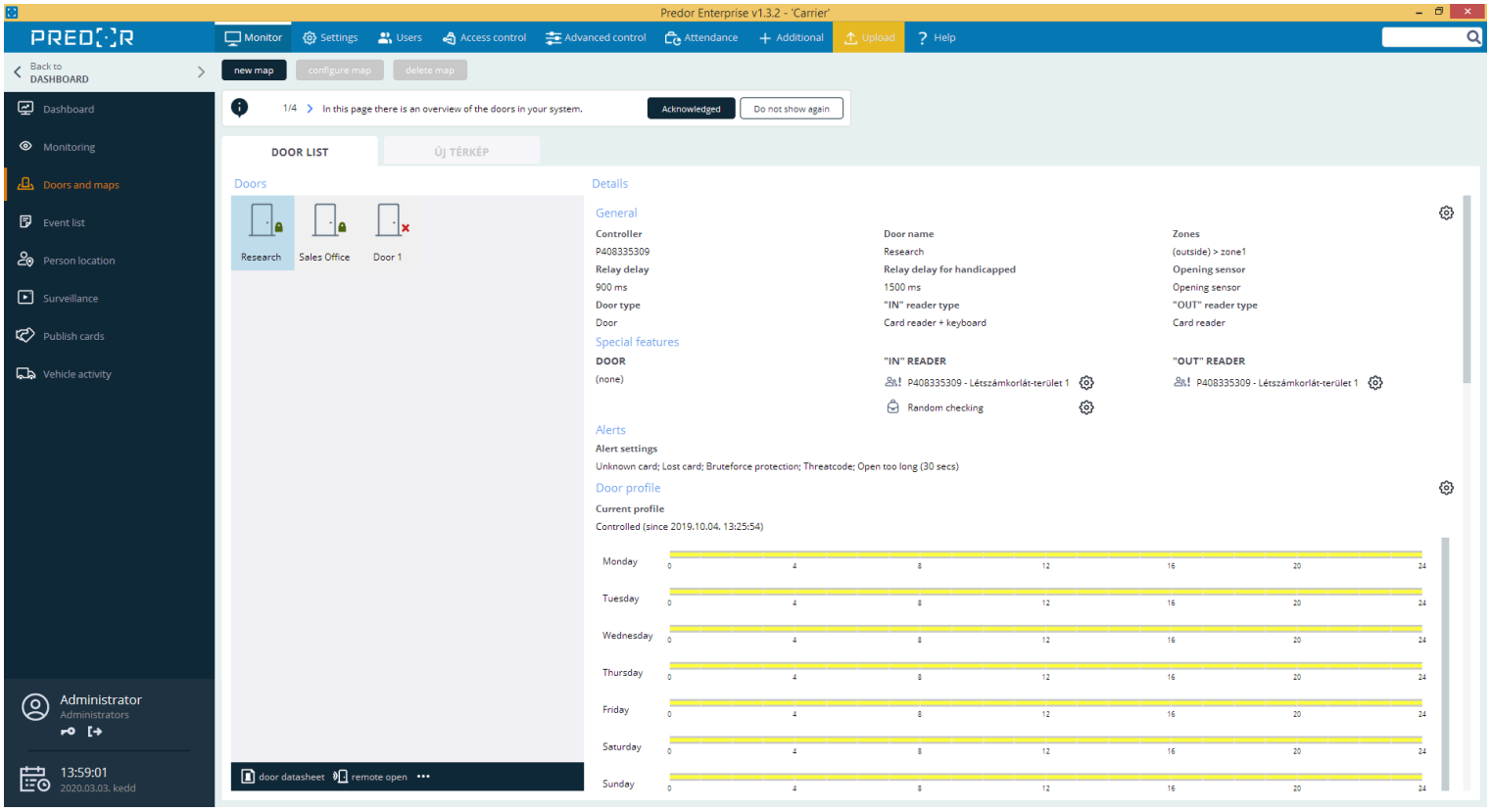


Figure 27: Door List view

Maps

Unlimited number of maps can be uploaded, the size of the uploaded maps can be changed as desired with the slider.

The icons of gateways, cameras, and controllers can be placed on the map. The size and color of the icons can be customized.

The icon is displayed next to the items that are already placed on the map. Each item can only be placed on one map.

When an alarm event occurs, by choosing the “show door on map” function the software will switch to the map view and display the affected door on the map highlighted with a red circle.

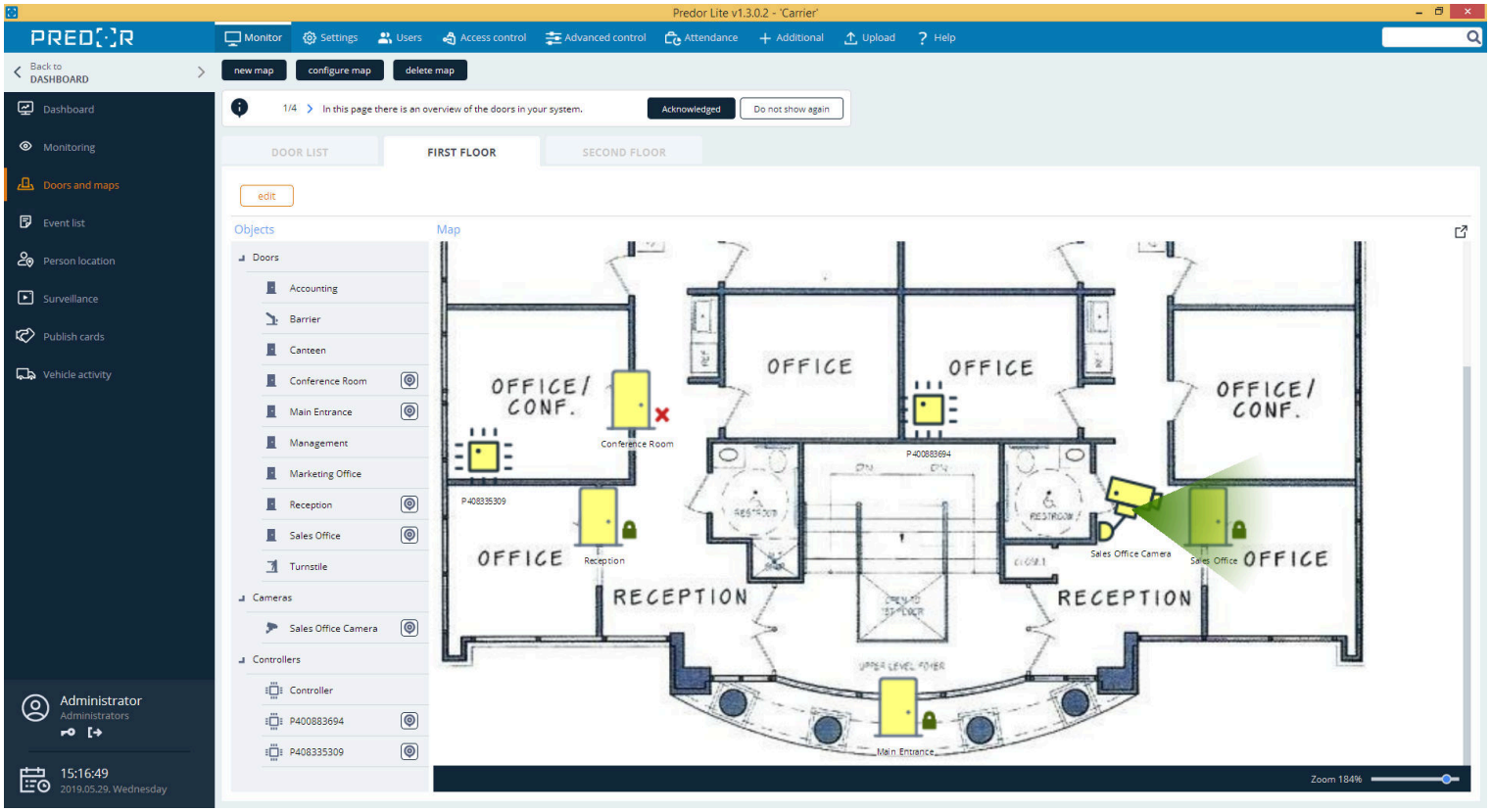


Figure 28: Map view

Event list

The event list window can be filtered by time ranges, locations, users, areas, departments, access groups etc. The configured filtering conditions can be saved.

Saved filters can be loaded or pinned on the dashboard, so it will be available immediately after starting the software.

After setting the filtering criteria, you can **hide the filters** to display more events concurrently on the screen.

ATTENTION! **With the “Delete old movement data” function you can permanently delete events which are older than 6 months.**

The “**Quick Filters**” provides quick overview of important events. (For example, by clicking on the “Alerts”, “Today” or “Last Hour” filtering criteria.)

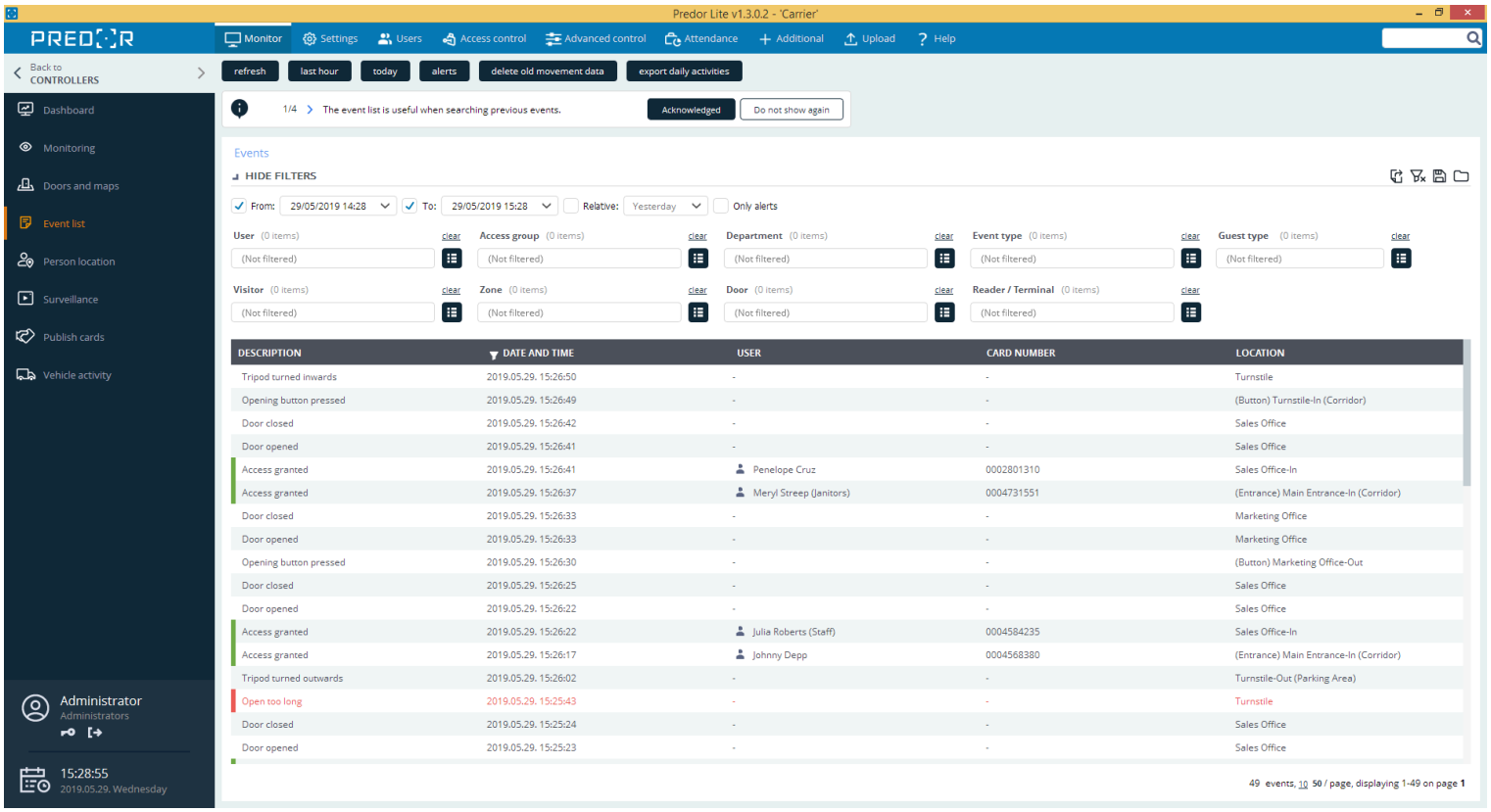


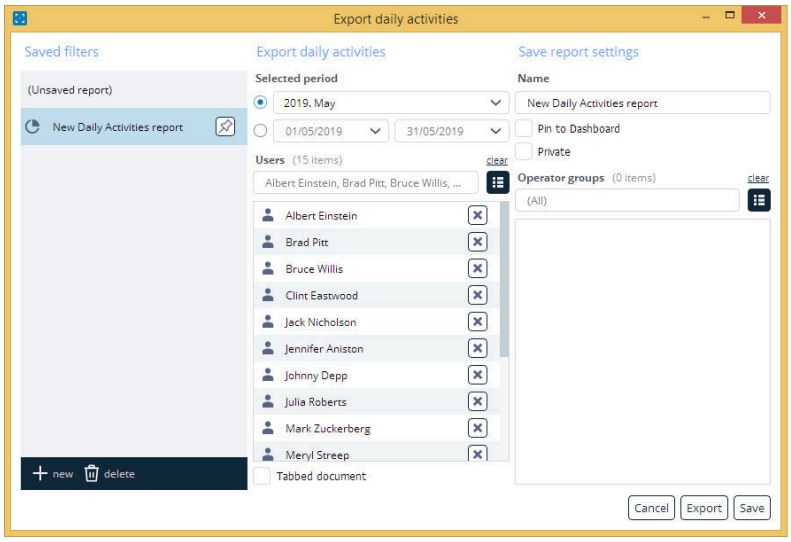
Figure 29: Event list view

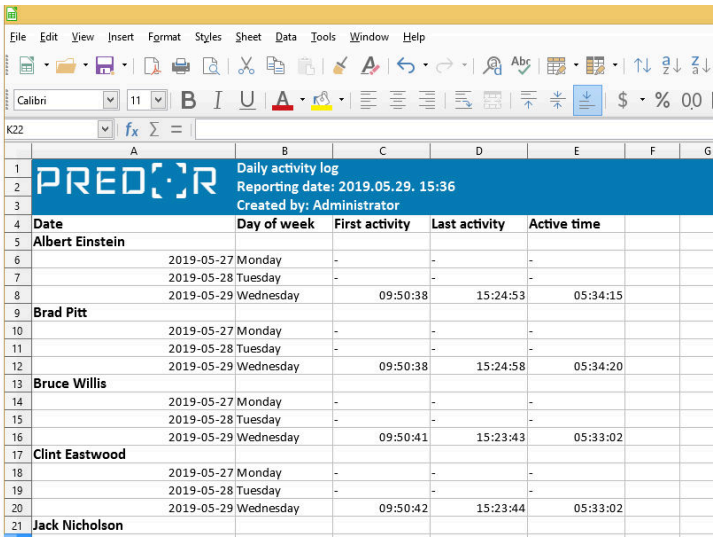
Export daily activities

This module allows you to export your employees' daily first and last access events and the system automatically calculates the work time between the two time flags. It is also possible to export only the summary of the active time, which can be done by ticking the checkbox next to *Sum of active time only*.

The function is available in the Event List menu after purchasing the **Daily activity export** license.

For advanced time & attendance data use the Predor attendance module by purchasing the **Worktime management** license.





	A	B	C	D	E
1	PREDATOR	Daily activity log			
2		Reporting date: 2019.05.29. 15:36			
3		Created by: Administrator			
4	Date	Day of week	First activity	Last activity	Active time
5	Albert Einstein				
6	2019-05-27	Monday	-	-	-
7	2019-05-28	Tuesday	-	-	-
8	2019-05-29	Wednesday	09:50:38	15:24:53	05:34:15
9	Brad Pitt				
10	2019-05-27	Monday	-	-	-
11	2019-05-28	Tuesday	-	-	-
12	2019-05-29	Wednesday	09:50:38	15:24:58	05:34:20
13	Bruce Willis				
14	2019-05-27	Monday	-	-	-
15	2019-05-28	Tuesday	-	-	-
16	2019-05-29	Wednesday	09:50:41	15:23:43	05:33:02
17	Clint Eastwood				
18	2019-05-27	Monday	-	-	-
19	2019-05-28	Tuesday	-	-	-
20	2019-05-29	Wednesday	09:50:42	15:23:44	05:33:02
21	Jack Nicholson				

Figure 30: Daily activity export

Person location

You can get information about the location of people or groups, and you can monitor the location of people by zones as well. In the table, if you move the cursor over the icon, an information window appears showing the name of the employee, the department and the access group which they belong to.

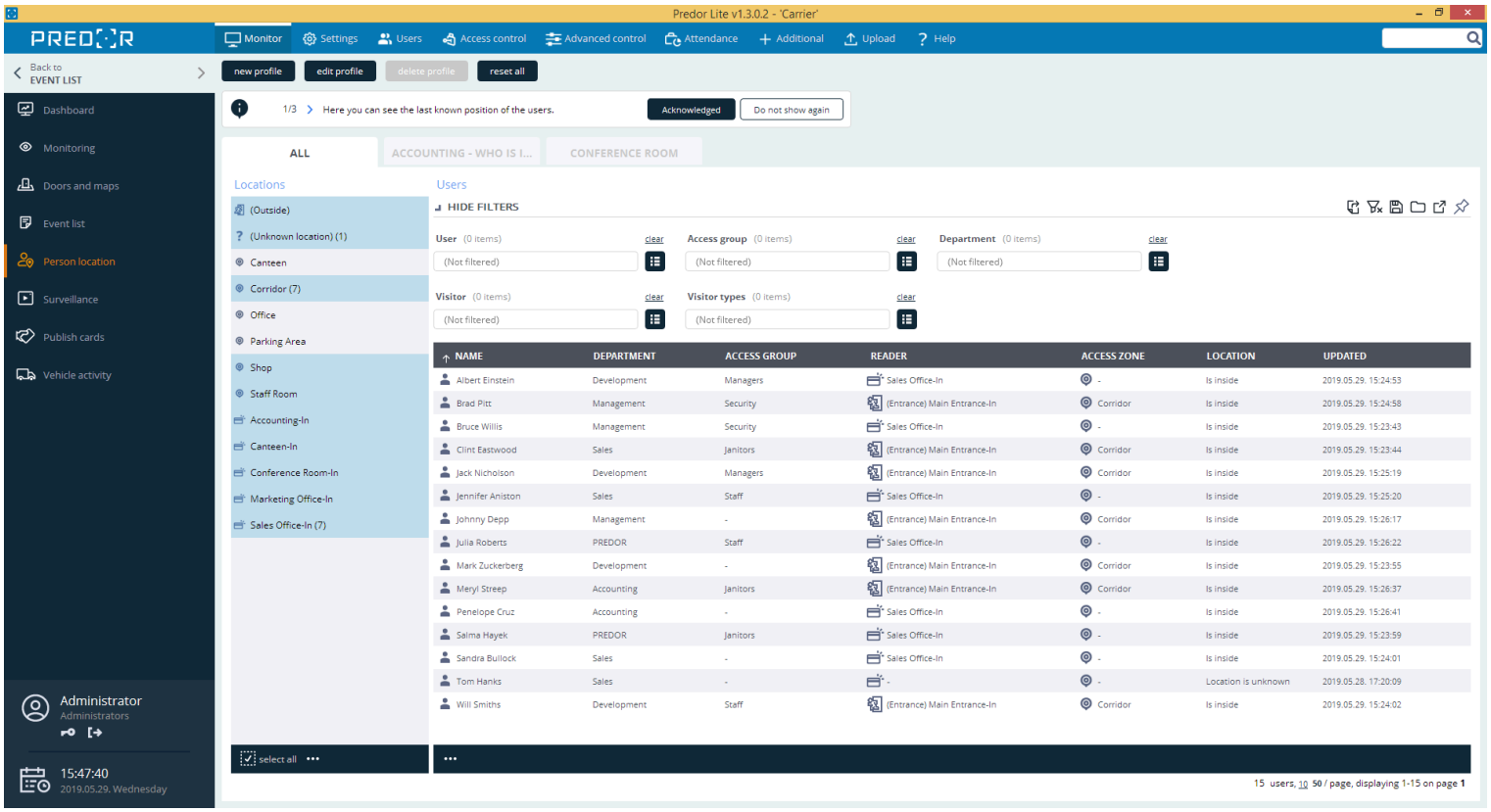


Figure 31: Person location view

The list can be filtered by zones, users, access groups or departments. The filtering conditions can be saved . The saved filters can be pinned on the dashboard, so any customized report can be loaded with just one click. More results are visible on the screen if we choose to hide the filters.

Using the additional operations drop-down list on the footer, we can track people, reset or modify their location, and so on.

TIP: Create your own observation profile according to your preferences and pin it on the dashboard. This way you can quickly review people and zones of interest.

TIP: If the location data has been corrupted (for example by a forgotten card swipe), it can be corrected by using the “Change location” function on affected users.

Auto drop out

If a person does not identify himself/herself when he or she leaves, according to the location data the person will be still inside. This is a problem in case of an evacuation in particular. The “auto drop out” function helps to avoid incorrect location reports.

If somebody doesn’t have movement event for a long time (for instance 24 hours), the system will automatically modify the person’s location to “outside”.

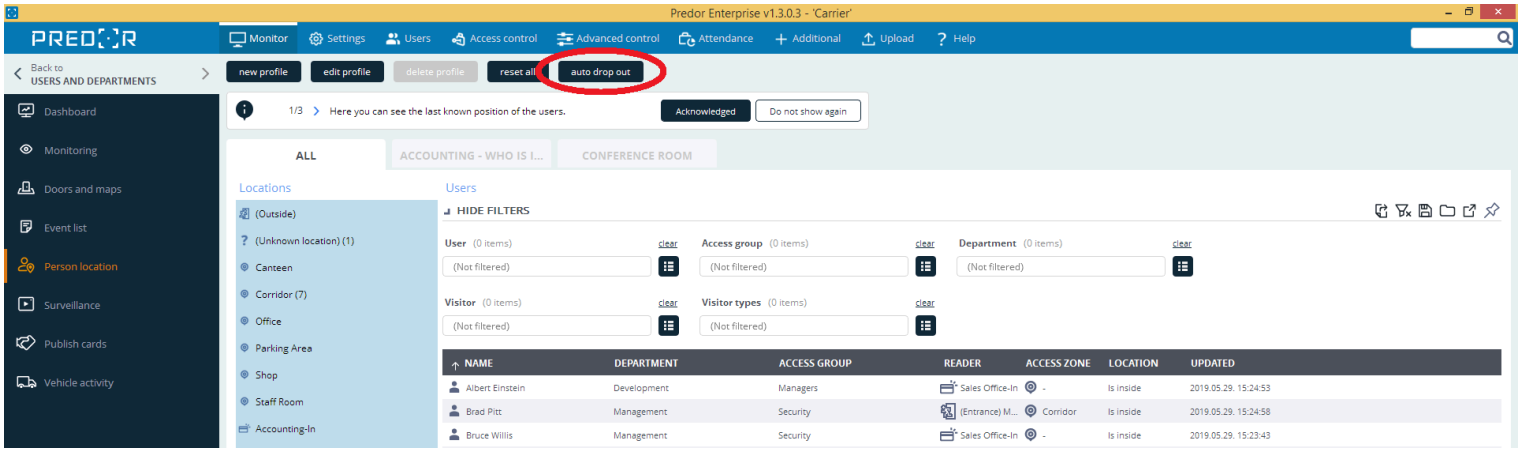


Figure 32: Auto drop-out settings button in the Person location view

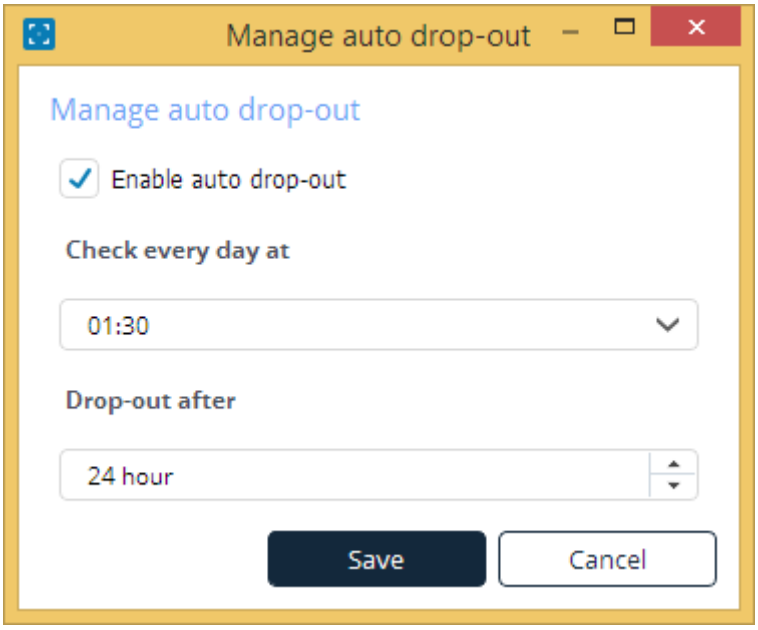


Figure 33: Auto drop-out settings dialog

Tracking

We can keep an eye on any person using the cameras of the object.

The tracking window always display the room where the tracked person is currently located. The live stream is automatically changed to another camera view when the person enters into an other area. At the bottom of the screen, the user's last motion data is displayed.

The video tracking will start automatically when the certain user arrives at the site.

The function can be activated in the person location menu by right-clicking on the user.

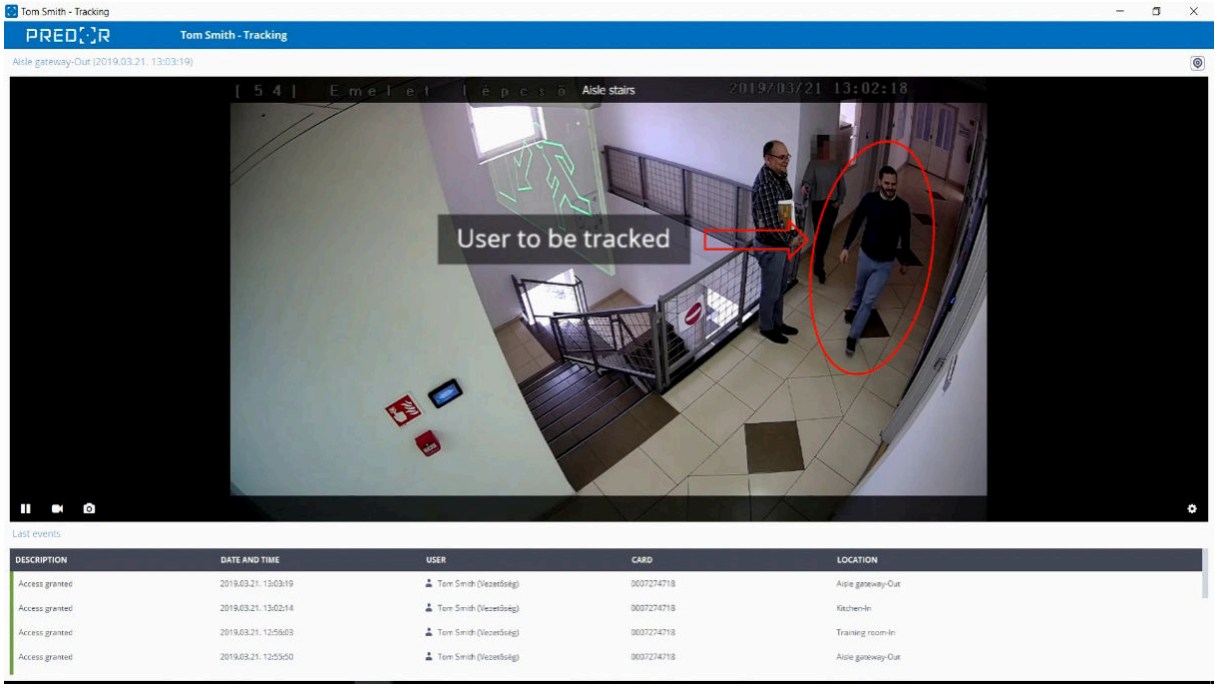


Figure 34: User tracking dialog

Surveillance

The live stream of the cameras can be viewed here. We can start a start record, take a snapshot or pause the stream.

In Settings / Cameras menu the video recorders and cameras need to be set first and then the cameras should be assigned to the doors which they observe. So the live stream of the certain camera is automatically displayed in case of alarm.

We can create new profiles on separate tabs. Up to 16 cameras' live stream can be displayed in a single tab, and any layout can be choosen.

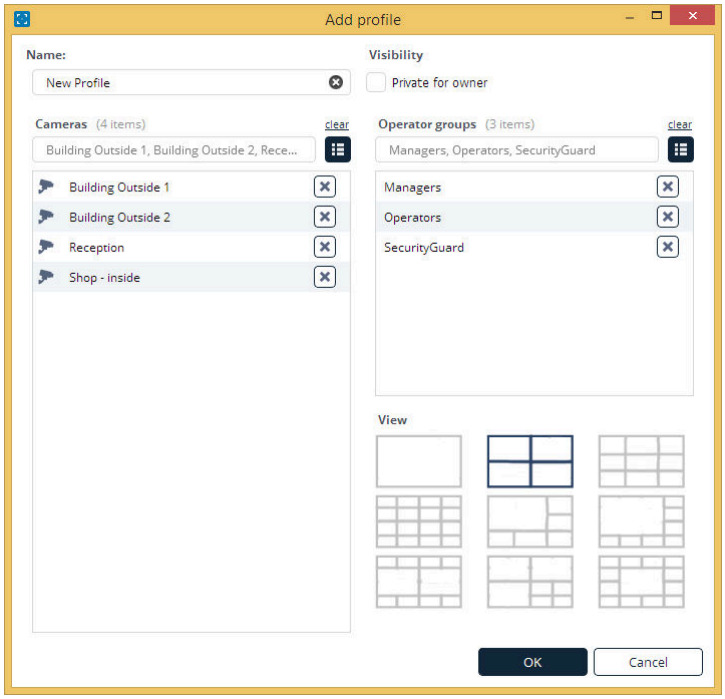


Figure 35: Creating a surveillance profile

The live streams of the cameras can be moved to any cells with drag-and-drop.

Moving the mouse to the camera image will display additional action icons so you can start recording with one click, take a snapshot, or stop the real-time video.

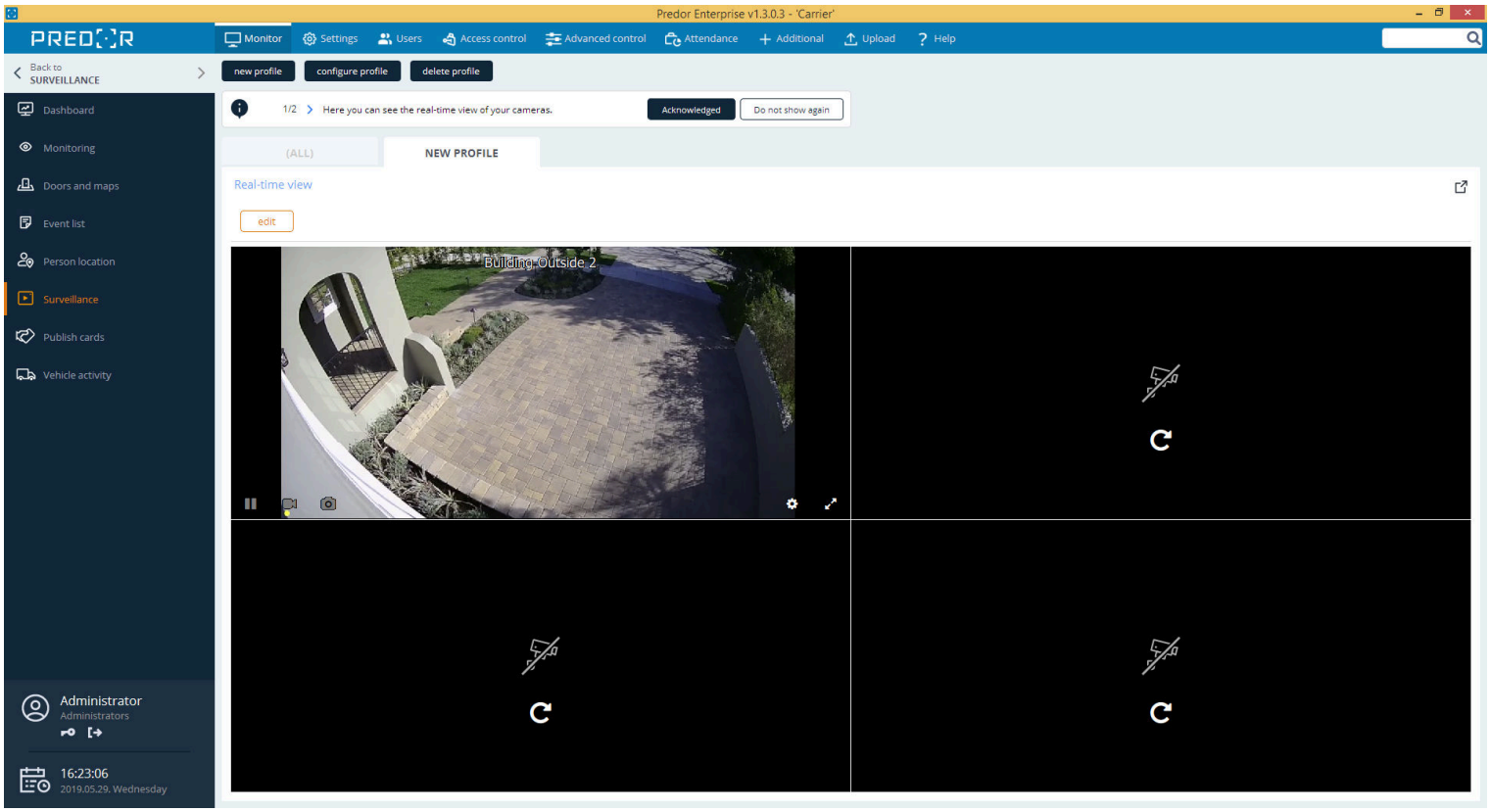


Figure 36: Surveillance view

Any profile can be opened in a new window.

Publish cards

Temporary cards

Temporary cards can be published in a few seconds for those users who have forgotten their ID at home.

After selecting the person in the dialog box, the user's data is automatically filled in. Select the card, which must be replaced. Input the temporary card's number using a USB or system reader or by manually typing it in.

If the "Upload immediately" checkbox is selected, the upload will be done automatically.

While a temporary card is active, the replaced card will be deactivated to prevent any misuse.

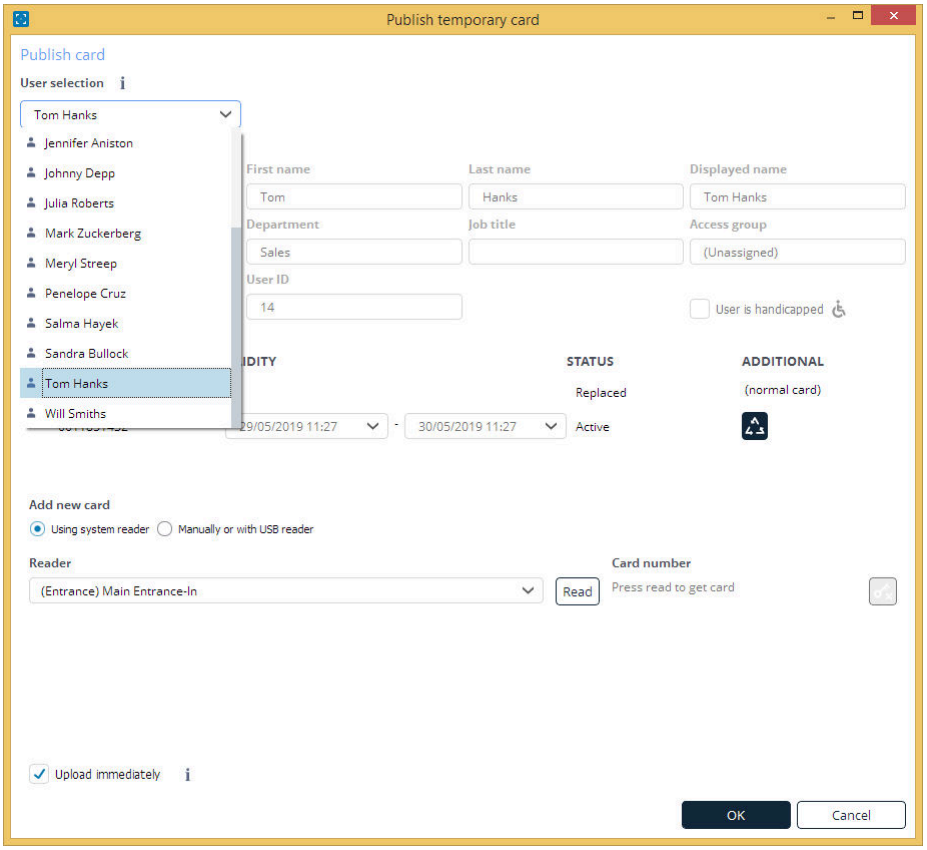


Figure 37: Issuing a temporary card

Visitors

To manage visitors, the **Visitor management** license is required. Visitors are handled differently than normal users in the system. Visitors cannot have unique access rights. Instead in the visitor settings menu visitor types need to be created to determine access rights and time ranges for visitors. The visitor type can be considered as an access group for visitors. Visitors are excluded from work time and attendance management.

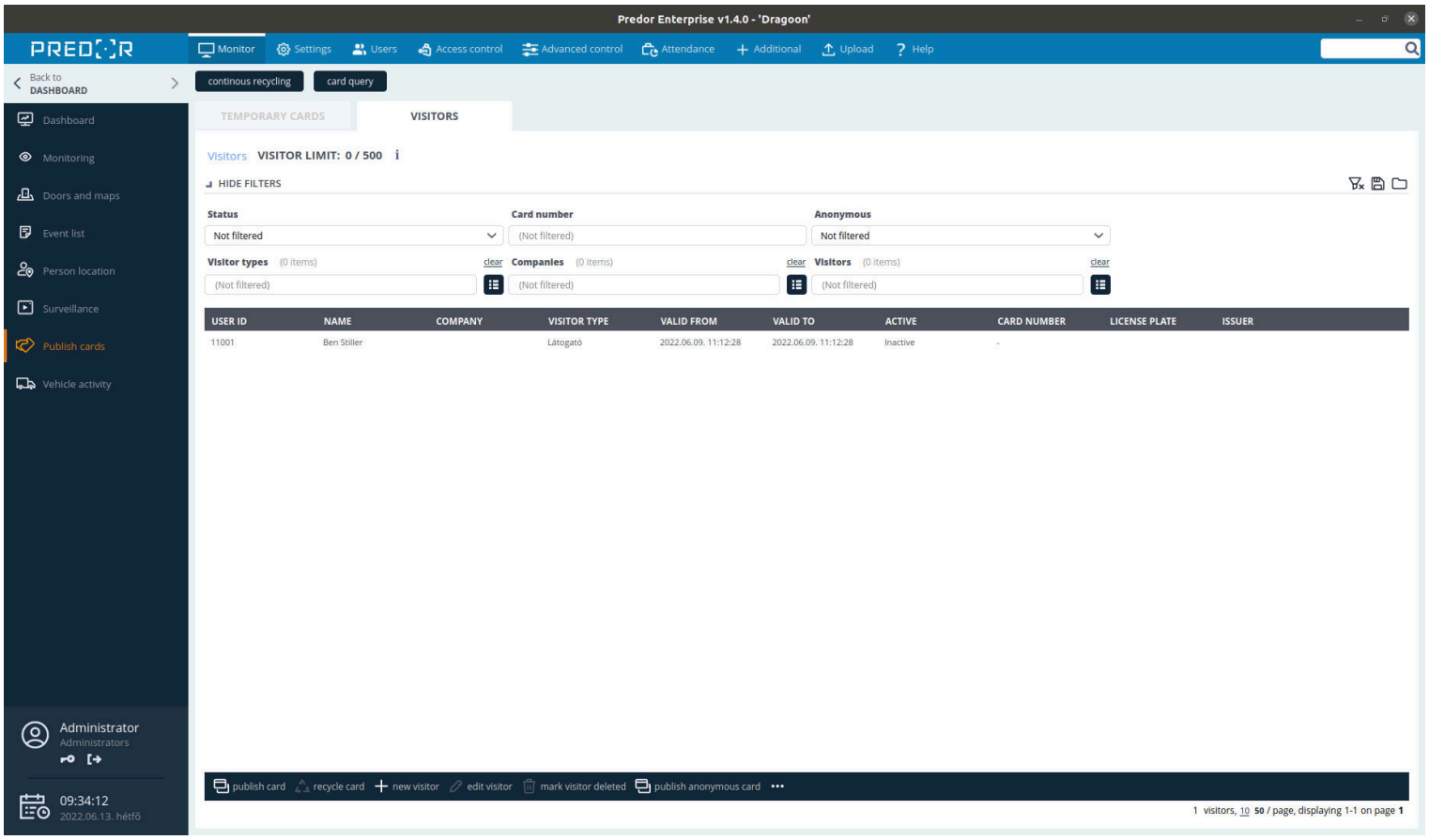


Figure 38: Visitor cards view

You can also publish visitor cards anonymously by using the “Publish anonymous card” function on the toolbar. You only need to enter the visitor type and assign the card for the anonymous visitor by reading or by typing in the card number manually.

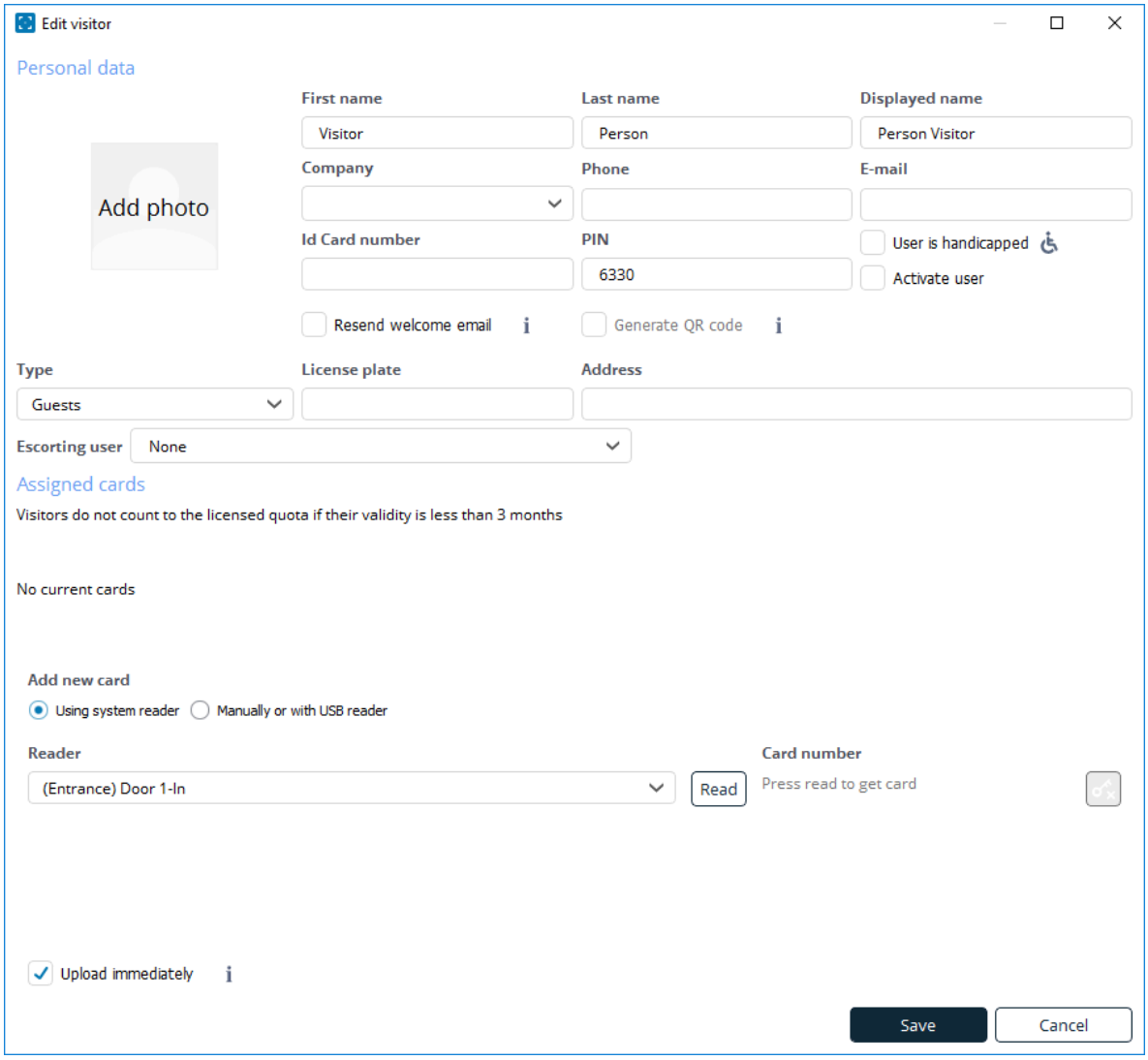


Figure 39: Assigning an anonymous visitor card

If you need to store information about visitors, open a new visitor window and fill in the form. Even photos can be uploaded. It is possible to send a welcome e-mail with the guest's name, expiration date, PIN code for door access. (Sending an e-mail is only possible, if the smtp settings are configured correctly and the guest's e-mail address has been set.) *When using the Venue admission module, after activating the Generate QR code option, the welcome email will contain a QR code that the guest can use on the system readers.* The card can be published by reading on a system reader or the card number can be typed in manually.

The visitor will be active for the period specified in the visitor type.

Guests can optionally be assigned a responsible person who can be selected from among the users in our system.

Card recycle: if a card is recycled, it will be deleted from the system and can be published to other visitors. It becomes a so called blank card.

If many cards must be recycled, choose the "**Continuous recycle**" option. The cards can be read on a system reader continuously. In the end just press OK, and all of the cards will be recycled simultaneously.

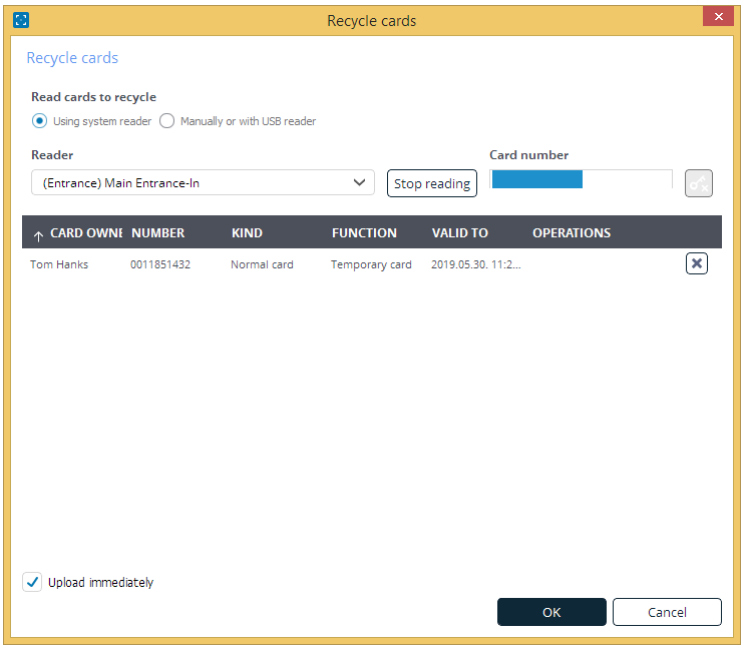


Figure 40: Recycle cards dialog

Card History: the cards are listed which were issued to the selected guest so far.

Vehicle activity

Under the Vehicle activity menu events are listed for gates that are marked as "Vehicle Entry Points". Similar to the Event list you can apply filters that you can save, and also export the filtered data.

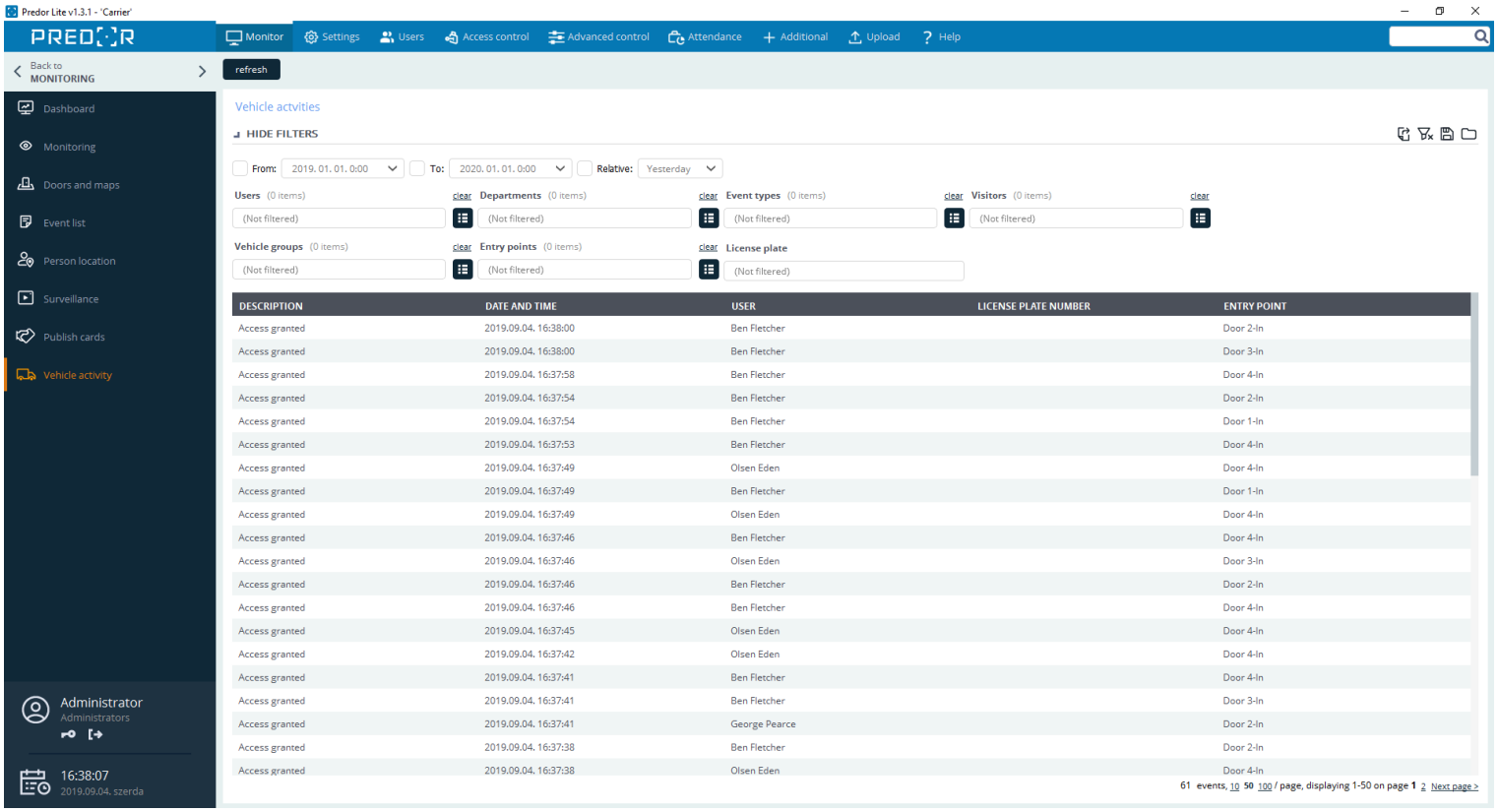


Figure 41: Vehicle activity view – similar to the Event list

You can mark gates as “Vehicle Entry Points” by using the configuration wizard in the Settings/Controllers menu.

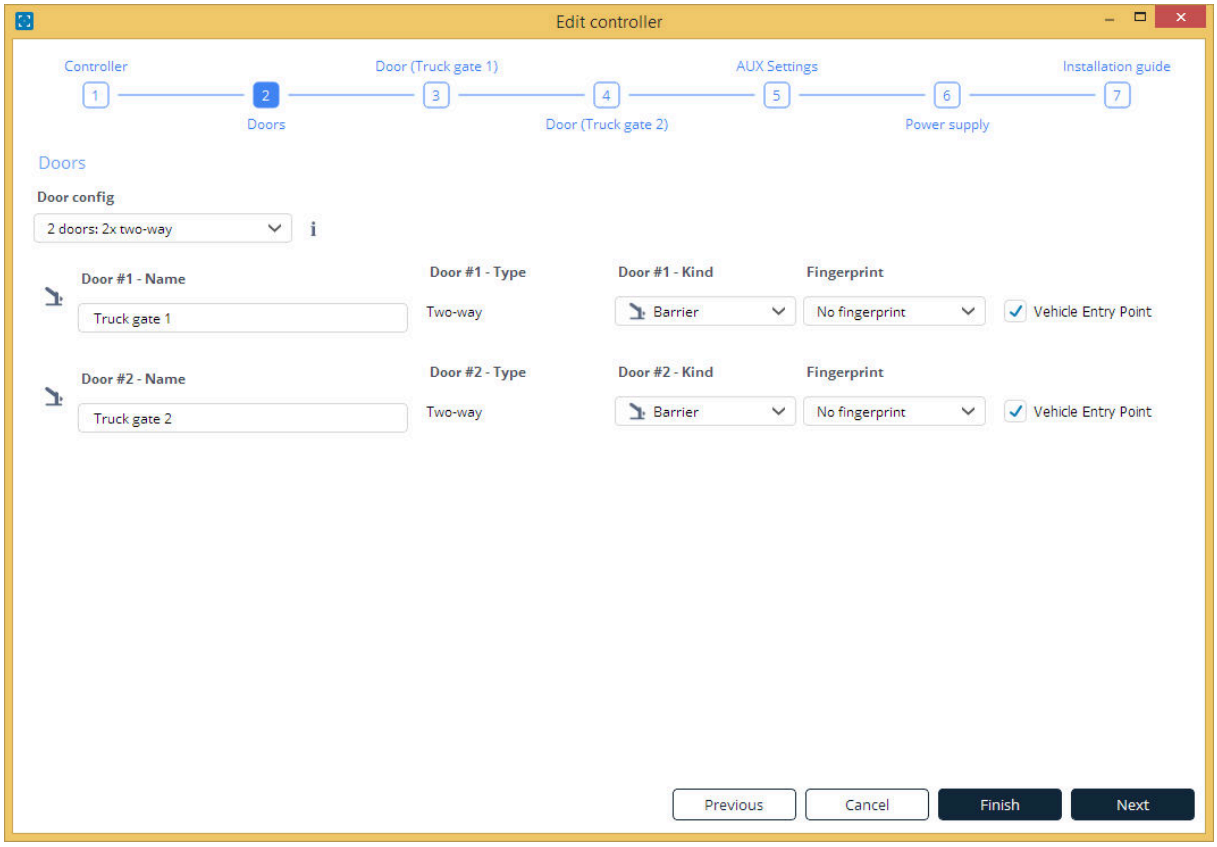


Figure 42: Marking doors as vehicle entry points in the Edit controller dialog

Vehicles can be added in the Settings/Parking management menu. License plate recognizers can be configured and associated with certain gates in the License plate recognition submenu. (see Parking management section)

6 SETTINGS MENU

System settings

System defaults

The basic communication and security settings of the system can be set in this menu. Editing the data on each tab must be enabled with the “edit” button.



ATTENTION! It is important to set up the communication parameters and the defaults of the controllers before adding them to the system.

Enter an IP address range. The system will automatically assign an IP address to the controllers from this address range. It is advised that this IP address range is defined outside of the DHCP IP address range on the network if there is any.

The default IP address of the controllers is 192.168.0.200



TIP: Multiple new controllers can be connected to the network at once, it does not matter if the controllers’ IP addresses collide until they are added to the system.

By enabling the password cracking protection both the software login page and the worktime web login screen blocks the user after 5 failed login attempts. Banned users cannot login in the following 1 hour. **Deactivating the function automatically results in the unblocking of banned persons.**

Bans can be lifted in the following menus:

- Operator bans in the Operators menu
- User (web) bans in the Users and departments menu

Controller settings

On this tab you can set the alert parameters, read mode, etc. These default settings can be individually overwritten in the controller configuration wizard window.



TIP: It is a good practice if we configure the settings here to apply to most doors in the system. This way only doors with unique settings will need to be edited later.

Controller defaults

Threat code: Even the locked doors can be opened by entering the threat code. The function can be enabled or disabled per door.



CAUTION: The threat code overrides the interlock rules either! Use it carefully!

Supercode: By entering the code, the doors in normal operating mode can be opened without a card. Locked doors cannot be opened. The function can be disabled per door.

Relay delay: the default opening time of the door opener relay.

Handicap relay delay: the default opening time for the door opener relay if a disabled user is entering. Users can be flagged as disabled in the edit user window.

Alert defaults

The selected event types will generate software alerts. It is advised to select the alert types that need to be reported from the majority of the doors. These parameters can be overridden on each door. Opening sensor is required for the “Forced open” and “Open too long” alerts.

Reader defaults

The commonly used reader type and the identification method should be specified here. The default parameters can be overwritten in the control settings window per reader.

Pass-through monitoring: people’s location data will be updated only if the opening sensor also indicates that the door is opened. By using this function the location data will be more accurate.

There are several options to choose from:

- **Card:** you only need to read a card to pass
- **Card + PIN:** after card reading PIN code is also needed to pass (press # or Enter after the PIN)
- **(User ID + PIN) or card:** you can pass through by reading your card. If the card is not available, enter the user ID then the PIN code. **After typing a user ID, you have to press # or Enter and then enter the PIN, then press # or Enter again.**
- **(Card or User ID) + PIN:** after reading a card or typing in a user ID, PIN code is mandatory. **Entering User ID + PIN: Type in the user ID then press # or Enter, then enter PIN and press # or Enter again.**

- **Activity code + Card: after typing in an activity code (optionally press # or Enter and then) read the card.** If you do not enter an activity code, the default activity code for that reader will be registered for the passage. If a default activity code is not assigned to this reader, the access is denied. If you enter an incorrect activity code, you must try again.
- **Activity code + Card + PIN: After entering an activity code (optionally press # or Enter, then) read the card and enter the PIN, then press # or Enter.** If you do not enter an activity code, the default activity code will be registered.

Bruteforce protection

If somebody try to gain access to the object by trying out many codes within a short period of time, the given reader will be locked for the specified period of time.



EXAMPLE: Time window = 30 sec; Attempts = 5; Blocked time = 60sec; In this case the reader is blocked for 60 seconds if there are at least 5 consecutive unsuccessful authentication attempts either via PIN codes or cards

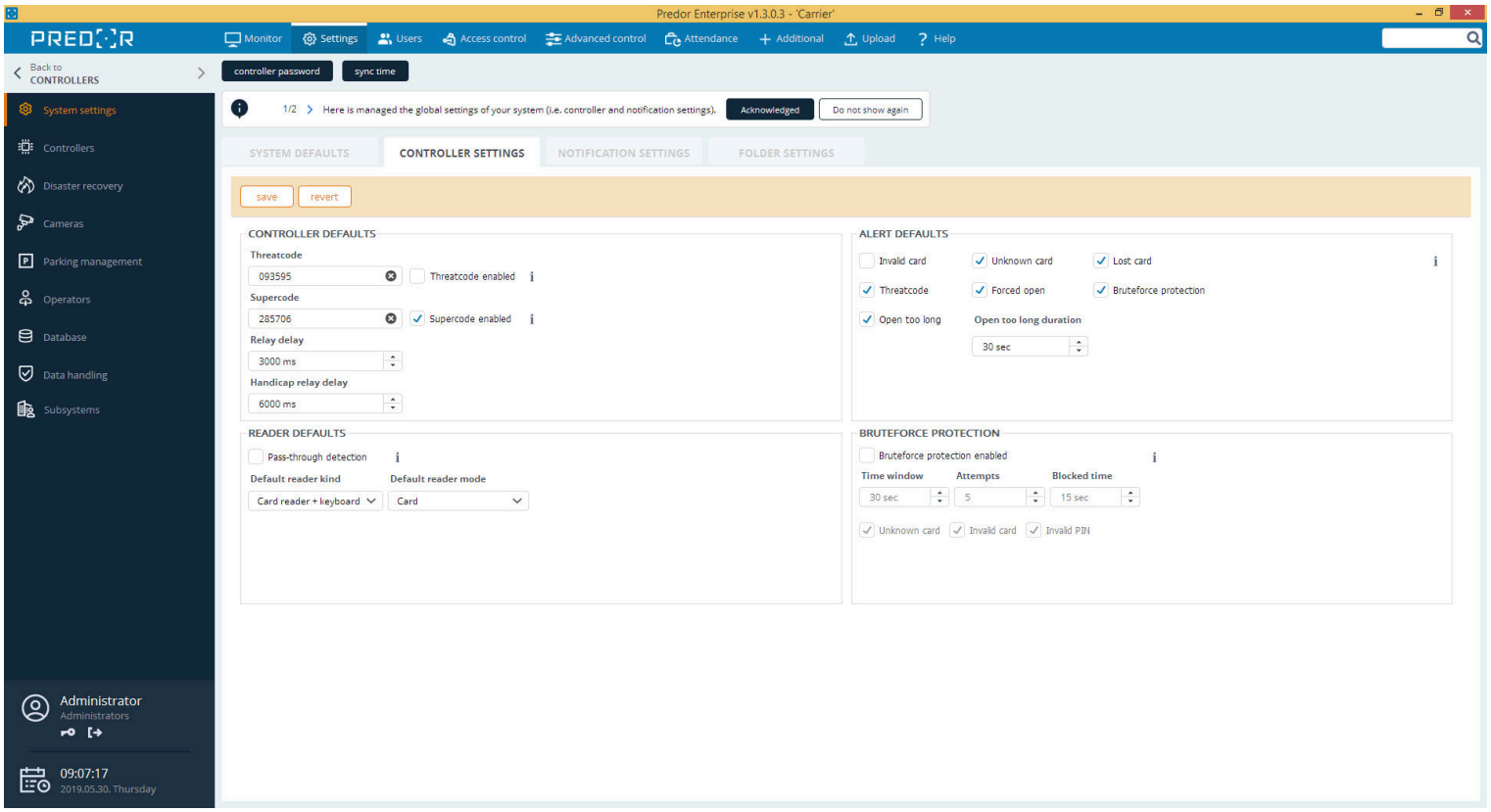


Figure 43: Bruteforce settings in the Controller settings page

Controller password: the communication with the controllers can be encrypted by en-

tering a password so that our system controllers will not be discoverable to others.

Smtp settings: here you can configure the SMTP server settings and test its correctness by sending test e-mails. If a self-signed SSL certificate is in use, SSL error tolerance must be set to allow such certificates.

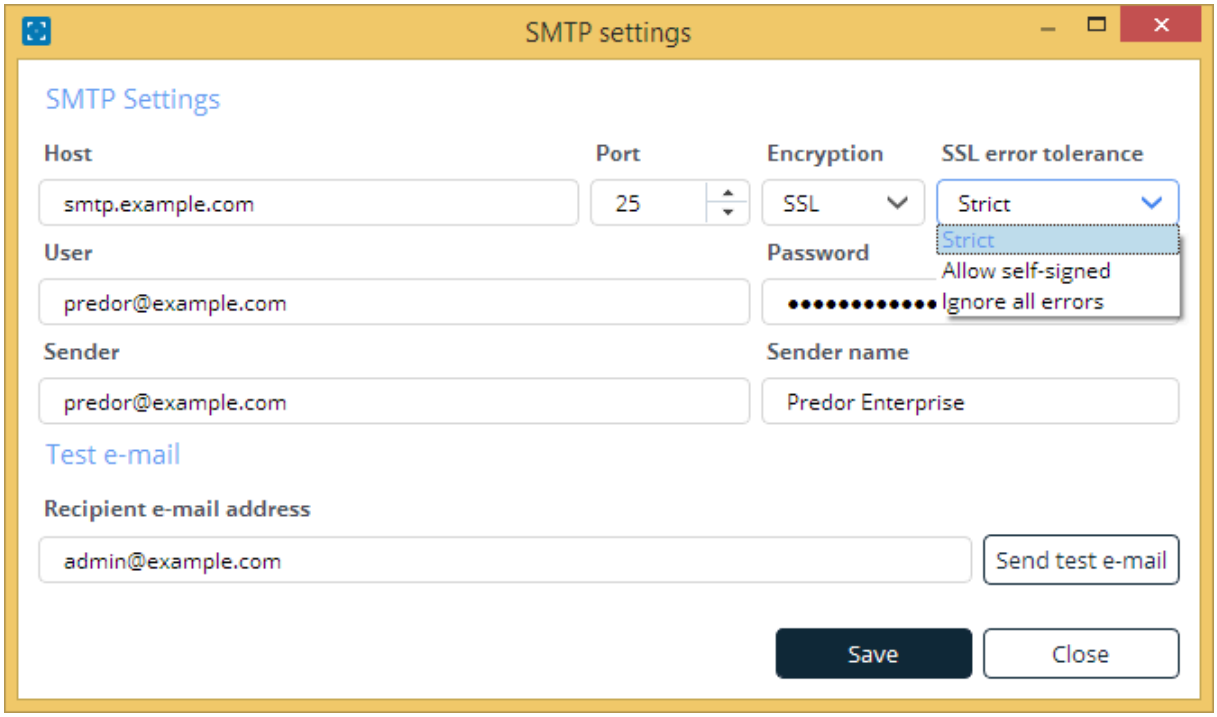


Figure 44: SMTP settings

For example, if you want to use a Gmail account to send e-mails then the following settings need to be configured:

- Host: smtp.gmail.com
- Port: 465
- Encryption: SSL
- User: e-mail address to be used (e.g. example@gmail.com)
- Password: password associated with the Gmail account to be used
- Sender: e-mail address to be used (e.g. example@gmail.com)
- Sender name: custom name, e.g.: Predor

If the test e-mail fails with authentication error please check if access for less secure apps is enabled on the Gmail account on this page: https://myaccount.google.com/lesssecureapps

E-mail settings

Under the e-mail settings tab you can create automated e-mail notification rules. You can configure who you want to notify on what events, about who or from what areas. You can also choose on what days and time you want to send out the emails.

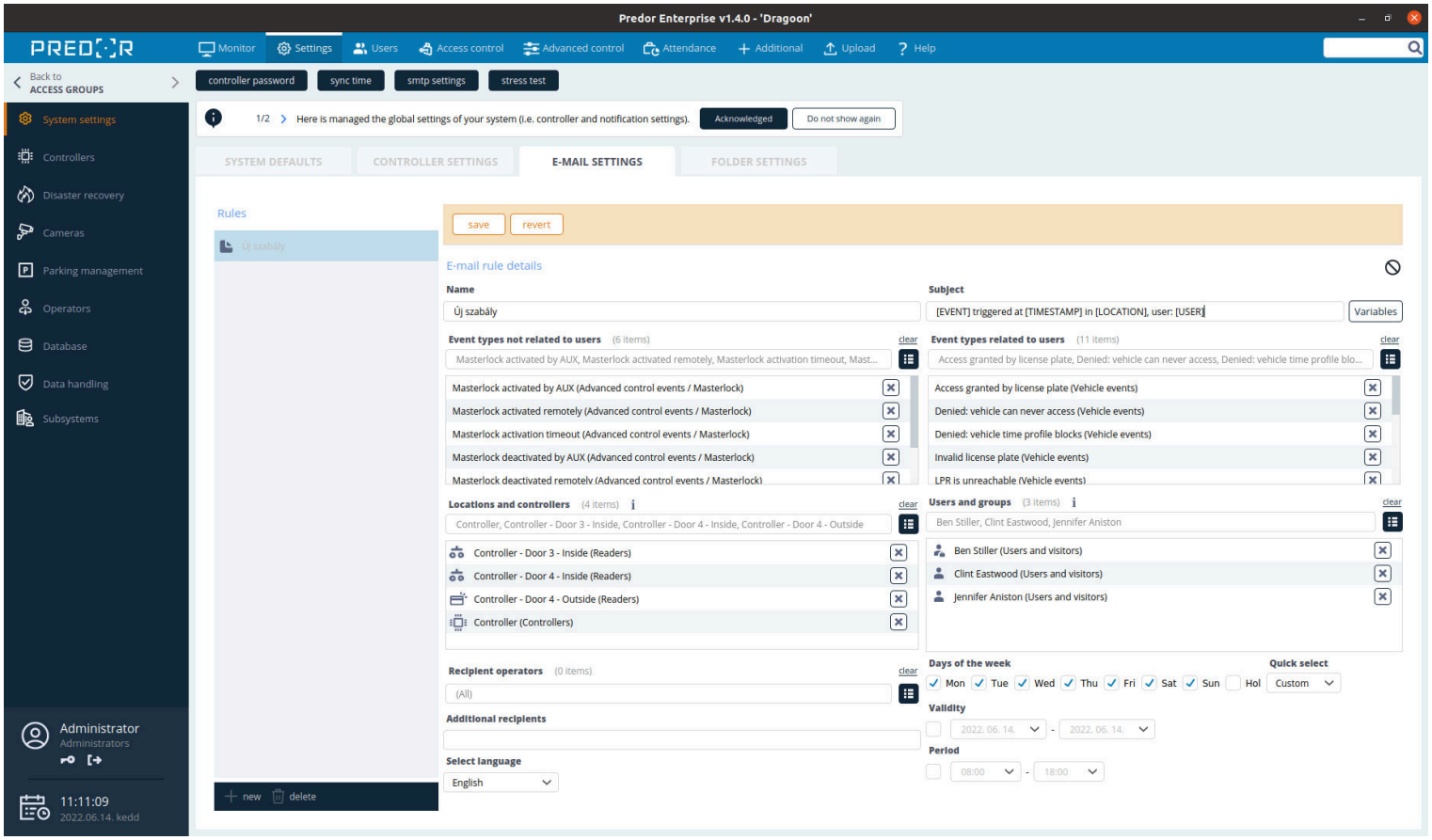


Figure 45: Setting up an automated e-mail notifier rule

Folder settings

Here you can configure the upload, recording and the logs folder locations.

Controllers

In this menu you can add new controllers and configure the ones added previously.

With the help of the **discovery** function you can search the network for available controllers, and select those that you wish to add to the system.

The most important parameters of the controllers can be viewed in the table view. Under the table you can configure these with the following functions:

- **New controller:** You can add a new controller to the system, manually configuring it.
- **Edit:** Opens the edit controller wizard which is used to configure the controller that is currently selected. This wizard shall be explained in detail on the following pages.
- **Delete:** Removes the currently selected controller from the system. Keep in mind, that the device will retain every setting (IP address, password, cards, time profiles, access privileges), only the communication with the software stops. Controllers cannot be deleted while uploading is in progress.



TIP: To reset the controller to factory settings use the RESET (Sentinel controller) or FAC DEFAULT SOFT RESET (Phantom controller) button on it with the following special sequence: Press down and hold the RESET (Sentinel controller) or FAC DEFAULT SOFT RESET (Phantom controller) button until the SYS LED (Sentinel) or STAT LED (Phantom) keeps flashing. If it stops then release it in 1-2 seconds, then it should start flashing again. After this, pressing the RESET (Sentinel controller) or FAC DEFAULT SOFT RESET (Phantom controller) button will return the controller to its factory communication settings (default IP address 192.168.0.200 and no password).

- **Controller datasheet:** Opens the controller's datasheet, where you can view its characteristics and its actual state.
- **Replace controller:** Replaces the currently selected controller with one of the same model, which must be on the same network, and it can't be already added to the system. With this option you can copy the configuration of a virtual or faulty controller to a new one.
- **Reset and upload:** If you encounter any functional or uploading errors then with this option you can reprogram the currently selected controller with its actual configuration.
- **Reboot:** Restarts the controller remotely.
- **Upgrade firmware:** Updates the controller's software if the client finds a new update for it (this will show up as a yellow triangle next to the controller's firmware version). You can't upload anything to it until it has been updated to the newest firmware version.

Double clicking on any of the controllers, or clicking the pencil icon, opens the edit controller wizard.

Edit controller wizard

The first page is for basic configuration.



TIP: Select the "Provide later" option next to the serial number. This allows you to create virtual controllers. All the settings can be set beforehand, without knowing the actual serial number. On-site the pre-configured "virtual" controllers must be replaced (by the "replace" function) with the real controllers. This way all the settings can be loaded onto the real controllers by one click.

Service mode: disables the tamper input during service and maintenance. Attention! The service mode automatically switches off every day at 03:15.

Note: notes can be written about the controller or about the installation. The note will appear by pointing to the "Info" icon next to the controller

Evacuation area: select which evacuation area should the controller belong to, this provides a more accurate location data in case of emergency.

Number of Doors: the controller can be configured to control 1, 2, 3 or even 4 doors. As the device has 4 Wiegand reader inputs, it can manage up to 2 doors in 2-way or 4 doors in 1-way control.

Here you can also set which doors should be used as vehicle entry points if you have the Parking management license.

Doors and readers settings

Setting of doors: if you enable the default settings in each section, the settings set in the Settings → Global settings → Controllers menu are used.

Door type:

- **Normal door, gate and barrier:** the opening relay is pulled during the specified opening time
- **Bistable door:** after authentication the relay is pulled and released only at the next valid identification
- **Turnstile:** in case of special gateways the opening is initiated by contact. 2 relays are required for operation.

Opening sensor: some functions and events require the installation of an opening sensor. Choose this option if a passive opening sensor is installed. Door relays will only unlock until the door is opened (or the relay delay expires).

Built-in opening sensor: this option should be chosen when a door-lock magnet is installed with a built-in opening sensor. The magnet will be released till the end of the predefined opening time, regardless of the door is open or closed.

Pass-through monitoring: if a door has an opening sensor and this function is enabled, it will be monitored whether the person has opened the door after authenticating. Location data will be updated only if the opening sensor also indicates that the door is opened. The location data will be more accurate. In case of turnstiles (because these devices are commonly impulse operated) a dedicated pass-through timeframe can be set independently of the opening time.

Opening time for disabled: longer opening time can be used for the door opener if a disabled user is entering. Users can be flagged as disabled in the edit user window.

The reader type and the identification method can be specified per reader. There are several options to choose from:

- **Card:** you only need to read a card to pass
- **Card + PIN:** after card reading PIN code is also needed to pass (press # or Enter after the PIN)
- **(User ID + PIN) or card:** you can pass through by reading your card. If the card is not available, enter the user ID then the PIN code. **After typing a user ID, you have to press # or Enter and then enter the PIN, then press # or Enter again.**
- **(Card or User ID) + PIN:** after reading a card or typing in a user ID, PIN code is mandatory. **Entering User ID + PIN: Type in the user ID then press # or Enter, then enter PIN and press # or Enter again.**
- **Activity code + Card: after typing in an activity code (optionally press # or Enter and then) read the card.** If you do not enter an activity code, the default activity code for that reader will be registered for the passage. If a default activity code is not assigned to this reader, the access is denied. If you enter an incorrect activity code, you must try again.
- **Activity code + Card + PIN: After entering an activity code (optionally press # or Enter, then) read the card and enter the PIN, then press # or Enter.** If you do not enter an activity code, the default activity code will be registered.

Role of the reader: the main ENTRANCES and main EXITS can be set. (The main entrances and exits can be configured in the access zones menu as well). If somebody identifies oneself on the exit reader, the system logs it as leave.

Do Not Disturb: usually it can be activated with a switch or remote control. While the function is active, the reader will reject all cards. The reader also flashes the “Do Not Disturb” operating mode.

Master code, Threat code, Bruteforce protection are explained in the System settings chapter.

Mandatory activity code entering: A valid activity code is required to enter, regardless if a default activity code is defined on this reader or not.

Beep settings: Each card reader's built-in beeper can be activated if a forced open or too long open condition is detected.

Ignore events: Unkown card events can be suppressed per reader.

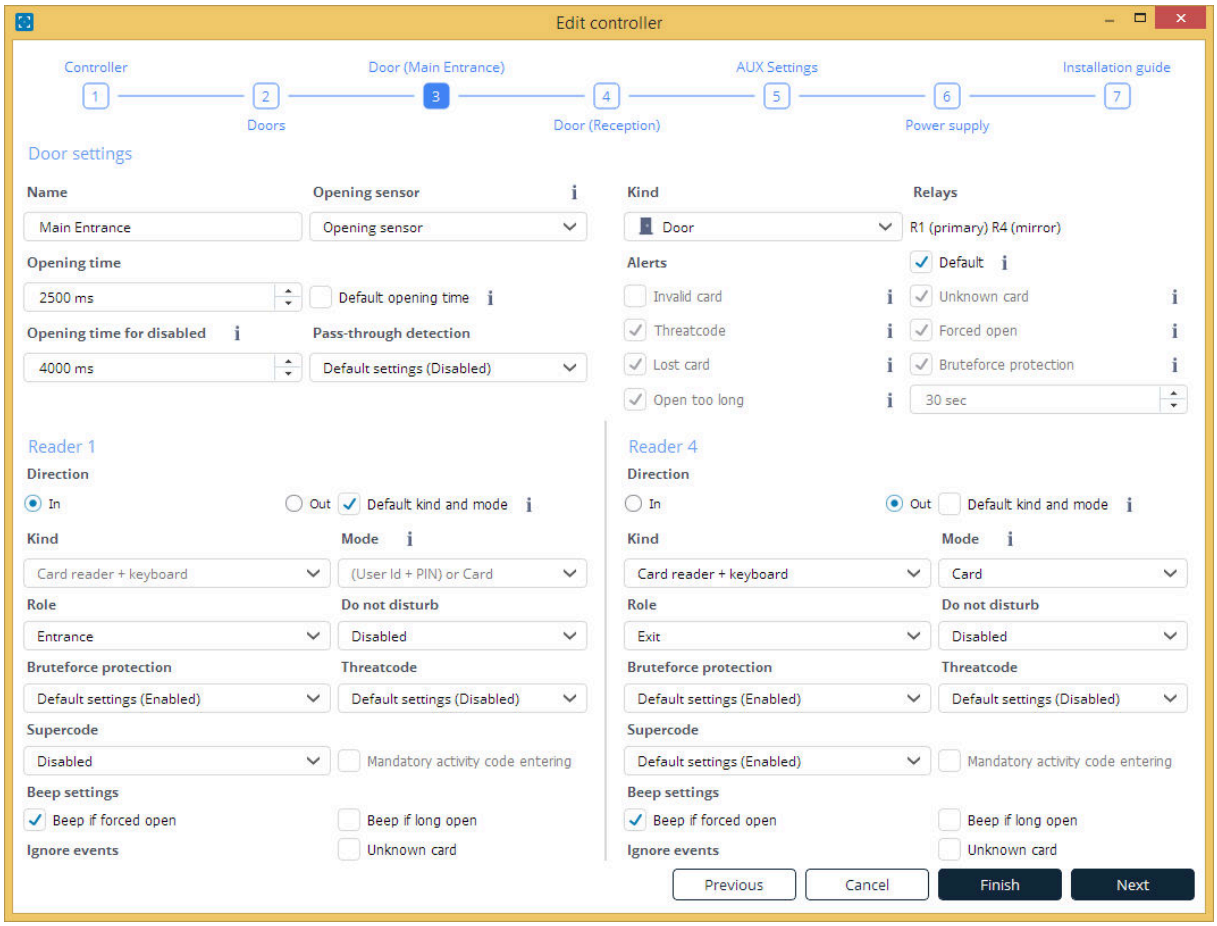


Figure 46: Setting up door and reader parameters

AUX settings

Auxiliary inputs and outputs can be configured here, which can activate or signal numerous events. Outputs can be configured flexibly by selecting trigger functions and setting timings. The default state of the enabled input is *normally open (NO)*. If you want to use the *normally closed(NC)* mode, you can change the operation of the AUX by changing the "AUX inputs" settings.

AUX settings:

- **Follow AUX input:** the relay will follow the status of the selected input

- **AUX IN activated:** the AUX relay will be active for the predefined time period, if the selected input status changes to activated.
- **AUX IN deactivated:** the AUX relay will be active for the predefined time period, if the selected input status changes to deactivated.
- **AUX IN changed:** the AUX relay will be active for the predefined time period, if the selected input status has changed.
- **Random selection:** the AUX relay follows the status of the selected input with the specified probability.
- **Follow opening sensor:** the AUX relay will be activated till the door is open.
- **Door open:** the door opening event will activate the AUX relay for the predefined time period.
- **Door close:** the door closing event will activate the AUX relay for the predefined time period.
- **Door open and close:** the AUX relay will be active for the predefined time period, if the door opening sensor state has changed.
- **Follow door relay:** the AUX relay will follow the state of the door opening relay
- **On door unlock:** the AUX relay will be active for the predefined time period, if the door opening relay's state is changed to unlocked.
- **On door lock:** the AUX relay will be active for the predefined time period, if the door opening relay's state is changed to locked.
- **On door lock and unlock:** the AUX relay will be active for the predefined time period, if the door opening relay's state is changed.
- **Alert on door (except fire):** the AUX relay will be active for the predefined time period in case of any alert event (except fire).
- **Interlock broken on doors:** the AUX relay will be active when the interlock has been broken on the selected doors until it recovers
- **Fire alert:** the AUX relay will be active for the predefined time period, if fire alert is activated.
- **Follow fire alert:** the AUX relay will be activated till the fire alert is active on the controller's fire input
- **... card on reader:** if the selected card type is presented on the reader, the AUX relay will be activated.
- **Threatcode on reader:** the threatcode will activate the AUX relay
- **Supercode on reader:** the supercode will activate the AUX relay

- **Periodic:** the AUX relay can be activated at any time for an arbitrary time period
- **Bruteforce protection on reader:** if the reader is locked due to bruteforce protection, the AUX relay will be activated for the predefined time period.
- **Random checking on reader:** the AUX relay will be activated, if the random checking function blocks a user
- **Random checking in progress on reader:** active during the random check of the selected readers
- **Random checking failed on reader:** it is activated for the duration of the set timing when the random check on the selected reader fails
- **Random checking timed out on reader:** it is activated for the duration of the set timing when the random check on the selected reader timed out
- **Headcount not empty:** the AUX relay will be activated till the area is not empty.
- **Headcount full:** if the headcount limit is reached, the AUX relay will be activated
- **Manager user:** if a manager card is presented, the AUX relay will be activated.

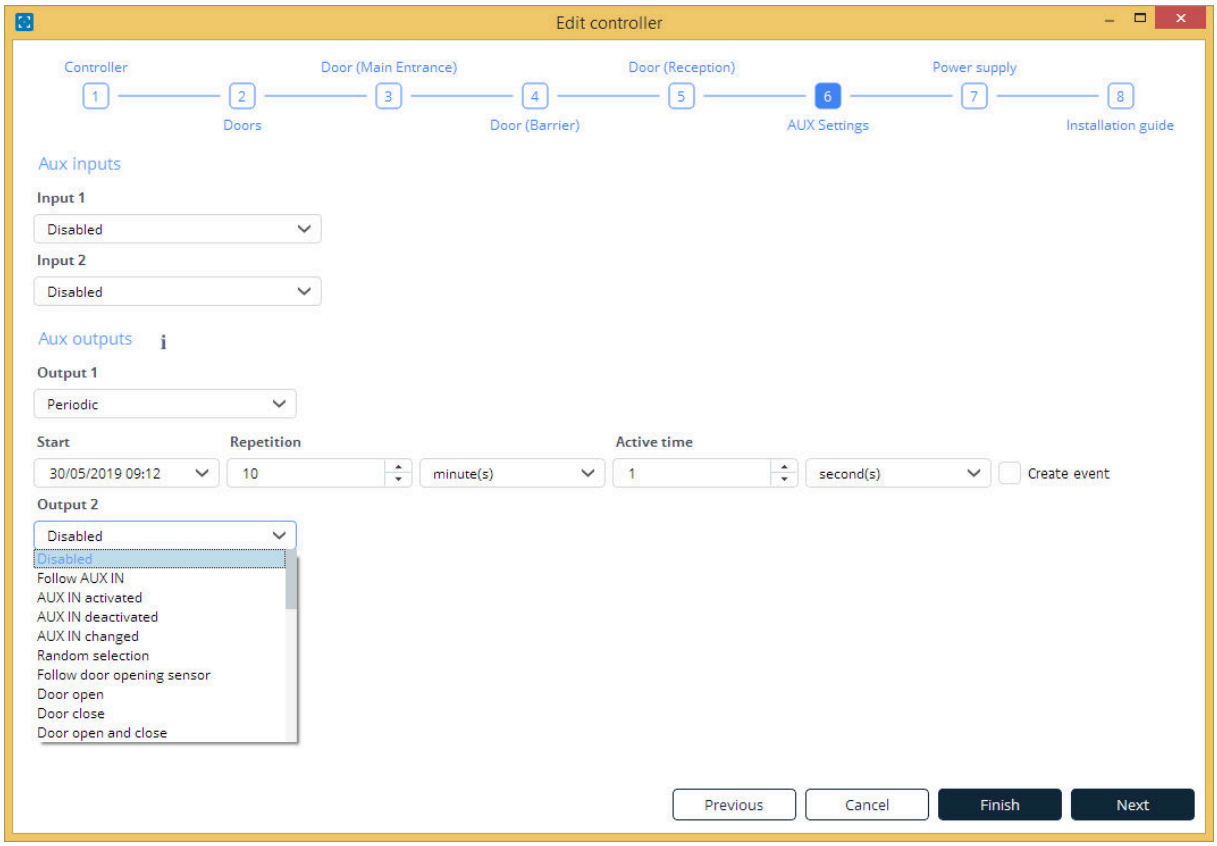


Figure 47: AUX settings

Power supply

If the controller is used with a Predor power supply, it can monitor the battery's performance and input and output power levels. By using e-mail rules the system can send notifications about power losses and battery performance degrading. When the battery is replaced, clicking on the icon will change the "Battery installation date" to today.

Cabling diagram

Don't worry about wiring anymore! The software creates custom wiring diagrams (installation guide) for each controller based on your settings and labels. By this way, this part of the installation can be outsourced or printed for later reference.

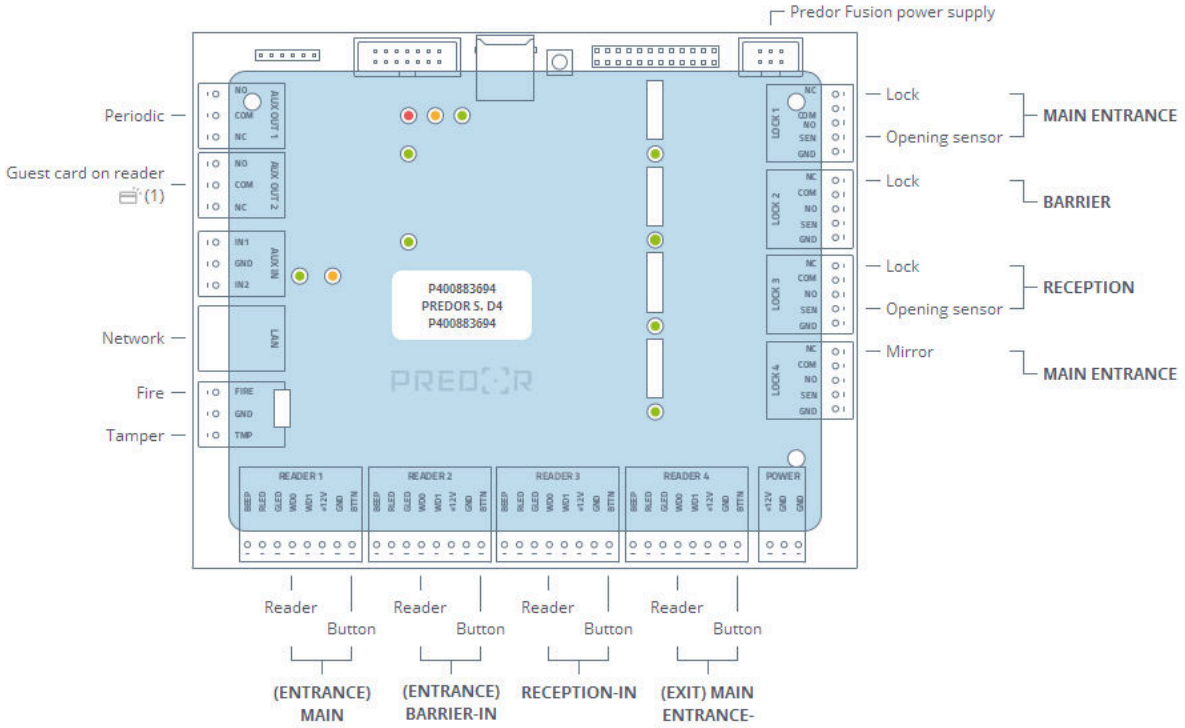


Figure 48: Automatically generated wiring diagram

Security settings

From this interface, the security settings of the system can be managed and the system's compliance with the NIS2 policy can be monitored. Access card encryption is also available from this menu, when using an SSCP reader.

NIS2

The tab shows the various NIS2 rules, and clicking on them will show a short description. An icon in front of the rules indicates whether the system is compliant (green tick) or not (red exclamation mark).

By clicking on the icon in the rules row, a reminder can be set to check the settings, which will appear on the right side under Actions. This allows you to schedule a task for yourself to review or implement the rule later.

Clicking on the icon will take you to the menu where the settings for the rule can be configured.

Clicking on the button will mark the rules as accepted.

By clicking on the button, the rules can be marked as ignored. The rule will be placed at the end of the line and shown in grey.

By clicking on the button, a comment can be added to the rules.

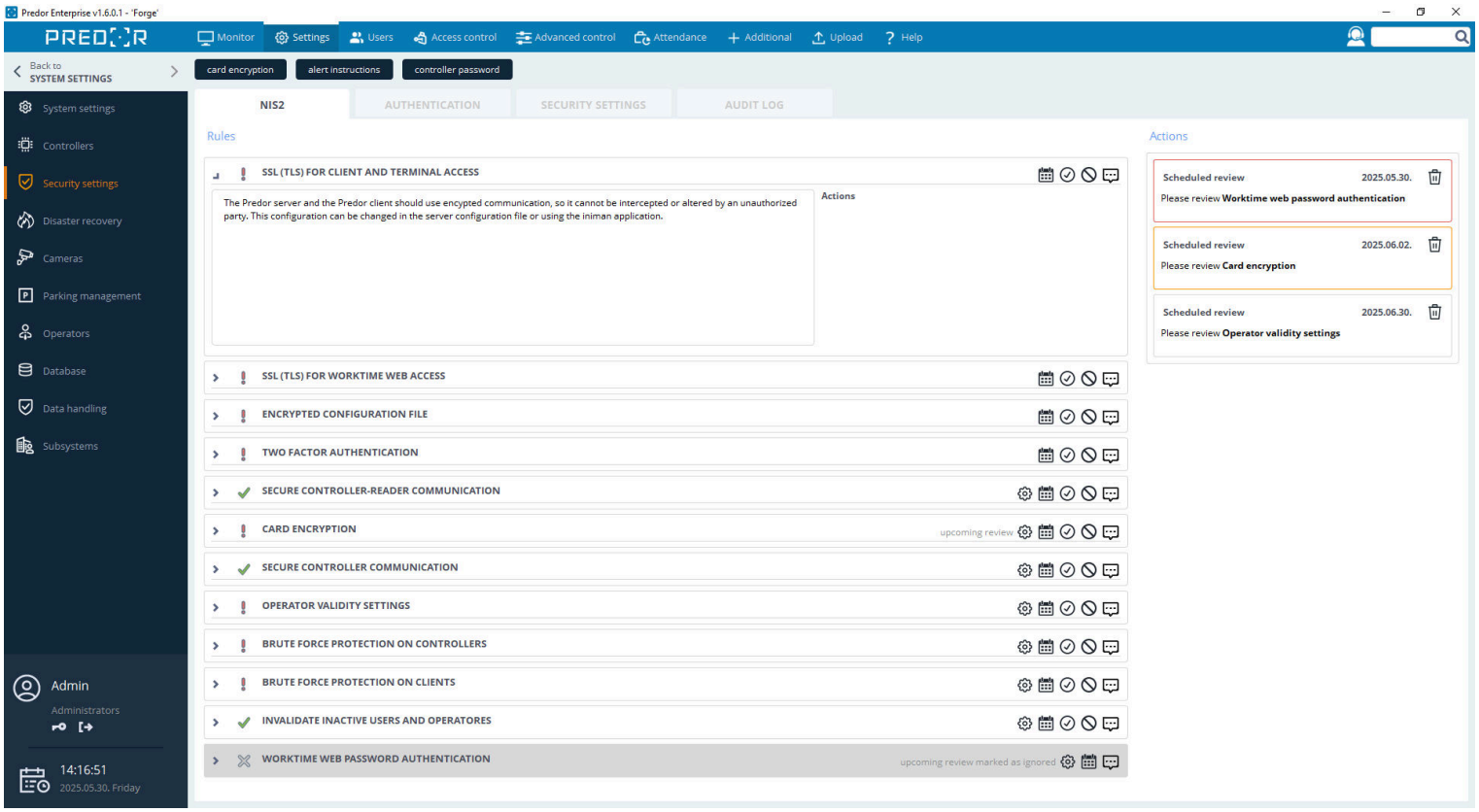


Figure 49: NIS2 rules

Authentication

Predor server settings

Password cracking protection can be activated for logging into the Predor client and the web interface. If enabled, the system will defend against bruteforce attacks. Operators and users who attempt to log in too many times without success in a short time, will receive a one-hour ban.

You can also set a global data handling time limit, in which case the rules will only run if the global data handling time limit has been exceeded.

The user password scheme can also be configured, which uses keywords for generation. This scheme is used when creating a user. When creating an operator the password must be entered manually. The keywords can be viewed by dragging the mouse over the **i** next to the password scheme.

Controller bruteforce protection

If somebody try to gain access to the object by trying out many codes within a short period of time, the given reader will be locked for the specified period of time.

EXAMPLE: Time window = 30 sec; Attempts = 5; Blocked time = 60sec; In this case the reader is blocked for 60 seconds if there are at least 5 consecutive unsuccessful authentication attempts either via PIN codes or cards

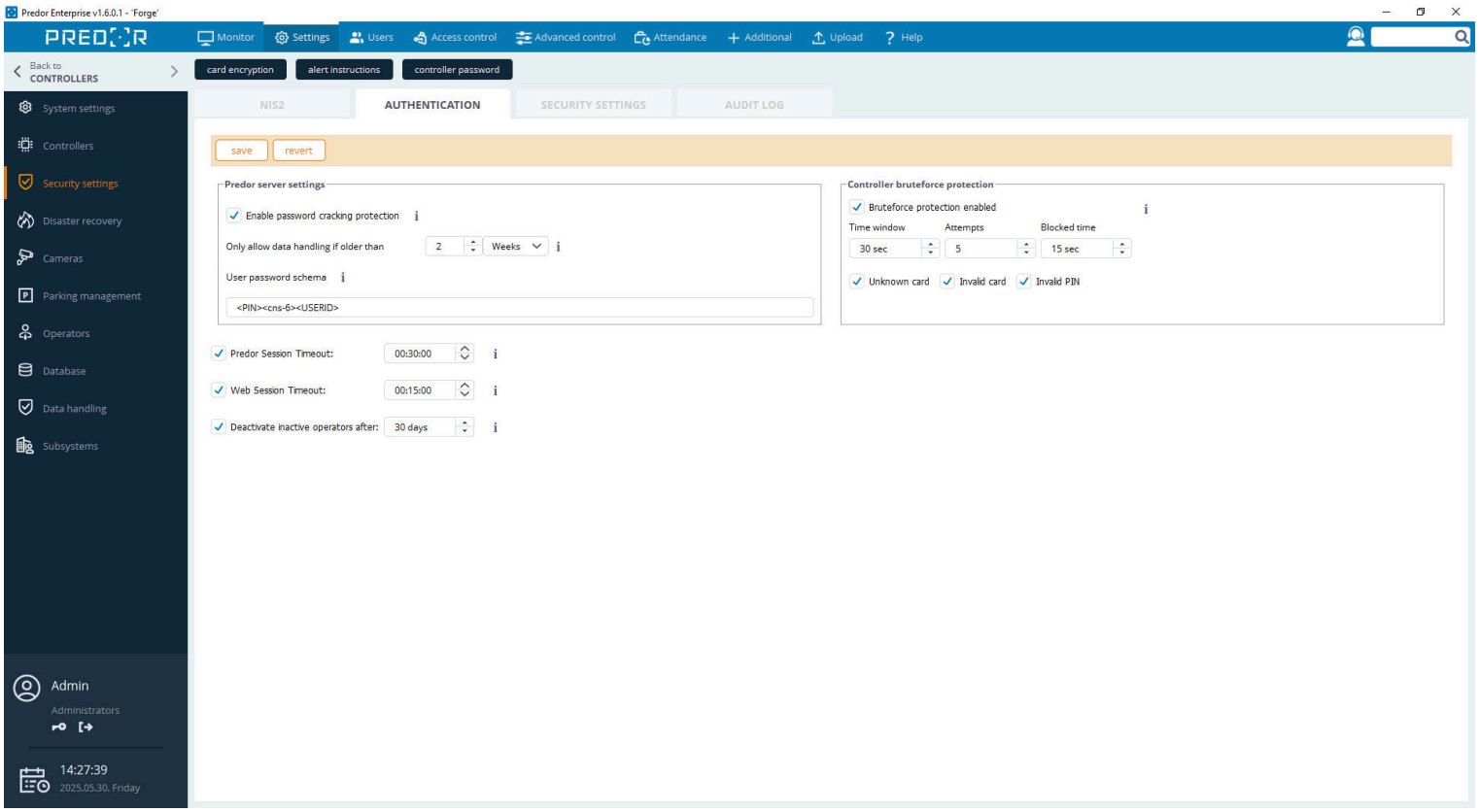


Figure 50: Authentication configuration

Predor client and web session expiry times can be specified in the format of HH:MM:SS. If the operator or user is inactive for the specified time, the system logs them out. For

operators, a counter with the remaining expiry time is displayed next to the operator's name in the software, which counts down to the specified time if less than one hour is left. When navigating, modifying or saving the counter is reset.

It is also possible to deactivate inactive operators. Operators that have been inactive for a specified number of days and have not logged into the software will be deactivated and will not be able to log into the client software until they are reactivated.

Security settings



WARNING: Only SSCP readers produced by **STid** will work. For the current list, please contact the software manufacturer at info@predor.hu or support@predor.hu addresses.



TIP: The system is currently compatible with readers with the following article numbers:
Wall mounted: ARCS-W35-G/BT1-7AD/y, ARC-W35-G/PH5-7AD/y
USB: ARCS-W35-G/BT1-5AD/y, ARC-W35-G/PH5-5AD/y

The volume of the reader's speaker can be adjusted. Drag the slider to the right to adjust the volume.

The sabotage detection threshold can be adjusted by dragging the slider to the right. If the detection threshold is set to a value other than None, when the reader is moved, the system disables the reader and remains in this state until it is approved.

The colours of the reader can be configured as preferred. After changing the settings, the preview shows the result.

The reader communication key is used to encrypt the communication between the reader and the controller. Click on the key icon to generate a new key.



WARNING: If the card reader's encryption key is lost (for example, the database is wiped or the back-up memory is corrupted), there is no way to recover this data. The controllers will continue to communicate with the readers, but in case of any modification or upgrade, the card readers must be sent back to the manufacturer to reset the default encryption key.

Card encryption

The security level can be set for encrypted cards.

For high security, Mifare DESFire cards (Ev1, Ev2 and Ev3 can be used. The Ev0 or older known as D40 DESFire card is not supported) and STid mobile id can be used. If STid mobile id is used, a card can be created in a free application on a smartphone and can be used to authenticate on the readers.



TIP: When generating encryption settings, only modify the data if you are competent to do so. Otherwise, leave the default settings, as the keys generated by default by the software are sufficiently secure.

For custom security, Mifare Classic and Mifare Ultralight cards can also be used.

The settings can be exported by clicking on the  button in the top right corner of the menu. The export output is a file in json format. The keys are exported in a non-decryptable format, they can only be read by the Predor software.



TIP: After configuring the settings, export them. Place the file on a storage device/computer that is not physically located at the server computer. In case of damage to the database or the server computer, the settings can be restored from the file at any time.

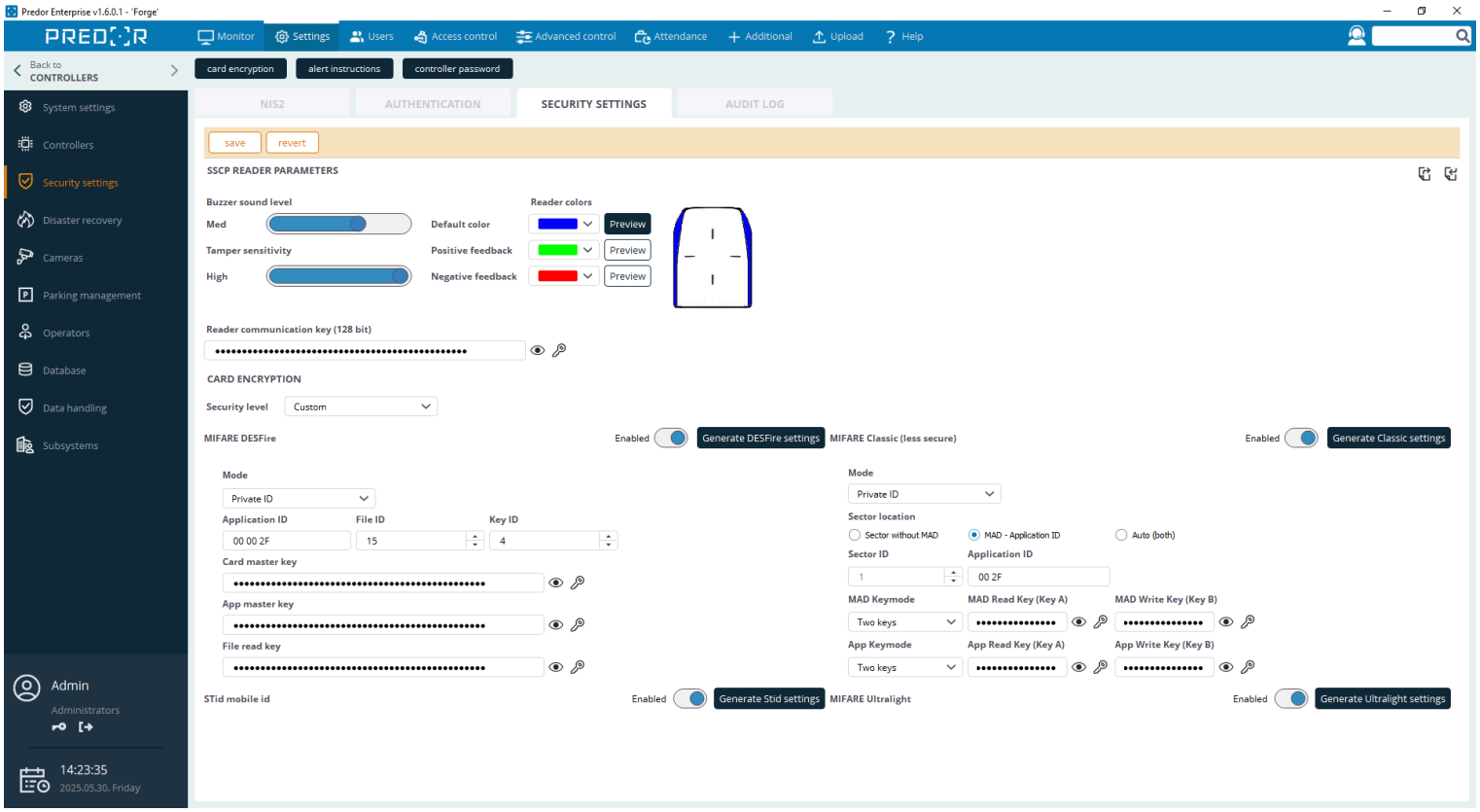


Figure 51: Security settings

Click on the **card encryption** button to encrypt the cards. After selecting the card type, the card operation and mode can be selected.

If the card number selection option is automatic, the system will generate a card number. With manual setting, a hexadecimal number can be entered.

In the reader field, you can select the USB reader you want to use for encryption, which is connected to the computer as a serial port.



WARNING: For Linux, the encryption USB reader can be used on a serial port only if the logged in user is a member of the "dialout" group. Otherwise, it is disabled and can only be used with administrator (sudo) privileges.

If the connection is successful, the reader preview will change to green. If a card is read which has been encrypted based on the keys set, the card number is displayed in the Detected card field. If the field is empty, the card has not yet been encrypted. Click on the Encryption button to encrypt the read card.

The event list displays all the events that occurred during the encryption process. By clicking on the  button on the left, the newly assigned card numbers can be exported

in CSV format. Clicking on the button on the right side will export the event list in TXT format.

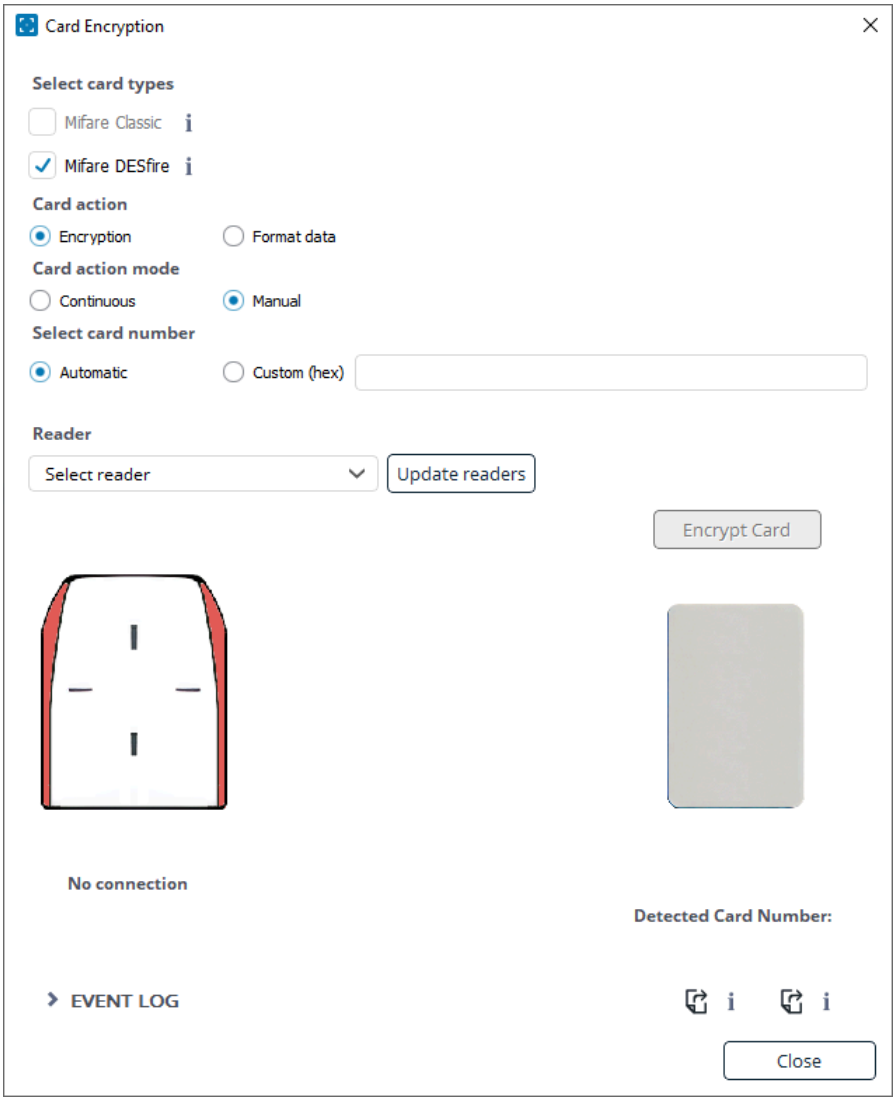


Figure 52: Card encryption window

Audit log

This interface displays the change events in the system. When using filters, the table can be refreshed by clicking on the refresh button in the top right corner.

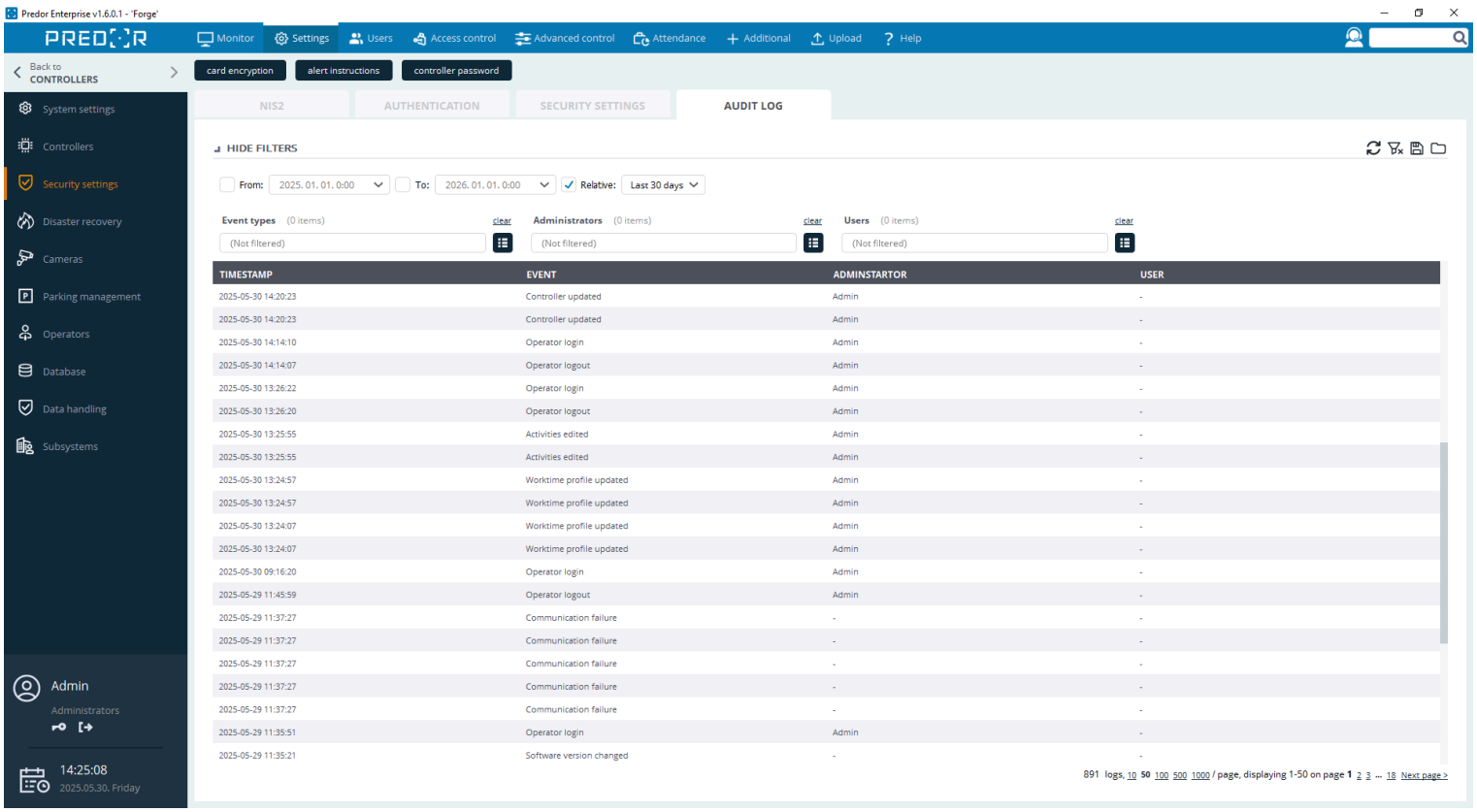


Figure 53: Audit log

Disaster recovery

ATTENTION! The user quota in the evacuation module and the base license has to be the same.

Evacuation settings

Evacuation areas should be created, so that each building can be evacuated individually. Each building can be a separate evacuation area.

Press Edit, then add a new area.

You can define different settings for each area.

Keep open until manual acknowledgement: the doors will not close automatically when the fire signal ceases. Only the acknowledgement from the software at the end of the evacuation process will set the doors back to normal operation.

Controllers send IP broadcast messages in case of fire alert: the controllers in the same evacuation area will send messages to each other about the fire alerts. Every con-

troller will switch to open mode during the alert, even those that do not have cable connection with the fire alarm system. This option is merely a secondary security feature! Always connect all controllers' fire input to the fire alarm system!

Select the controllers that create the area, also you can add the worktime terminals to it.

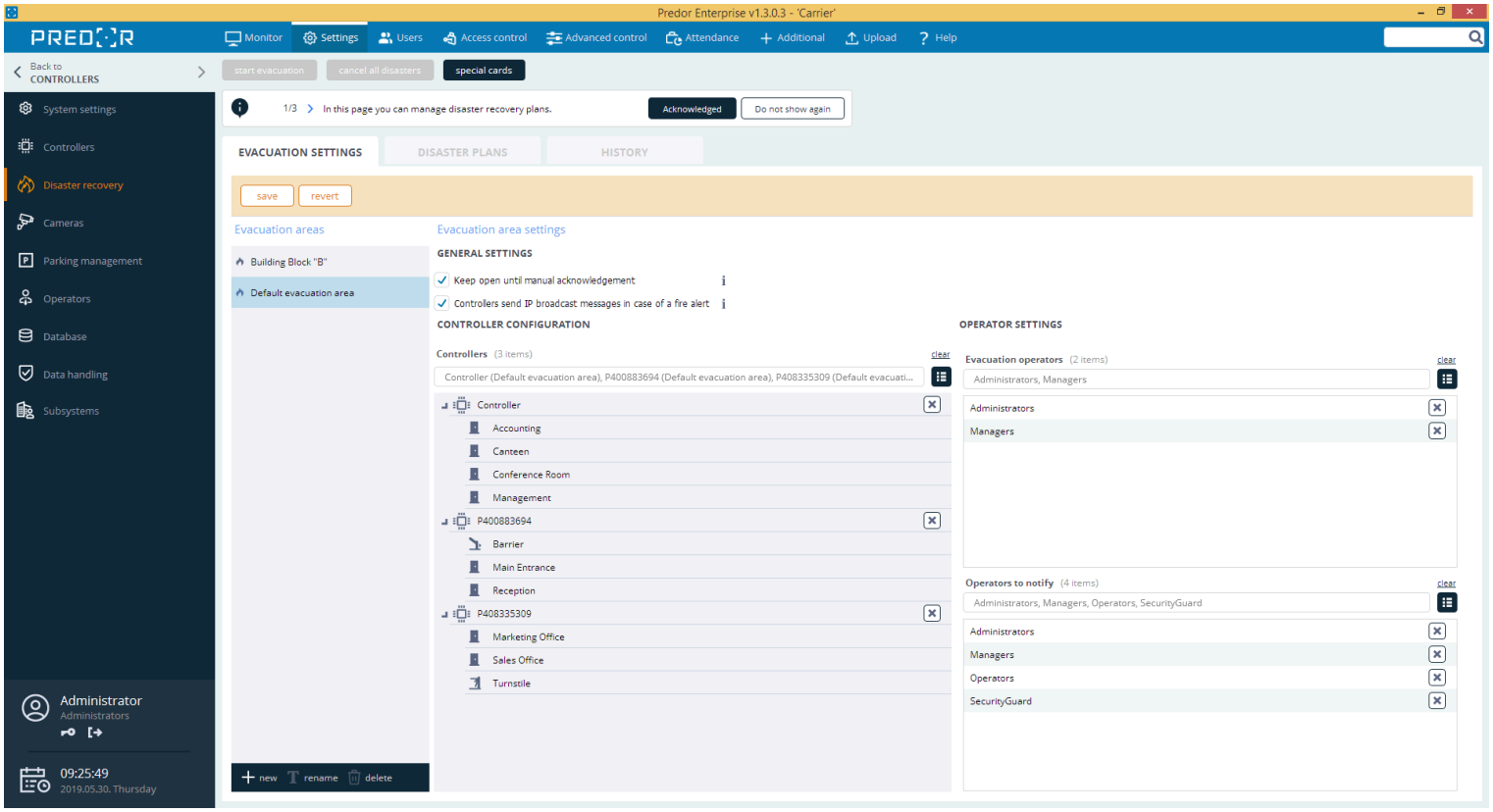


Figure 54: Evacuation settings

The authorized operator groups can acknowledge and stop the ongoing evacuation. They can also start an evacuation manually. In the dialog box the areas can be selected which need to be evacuated.

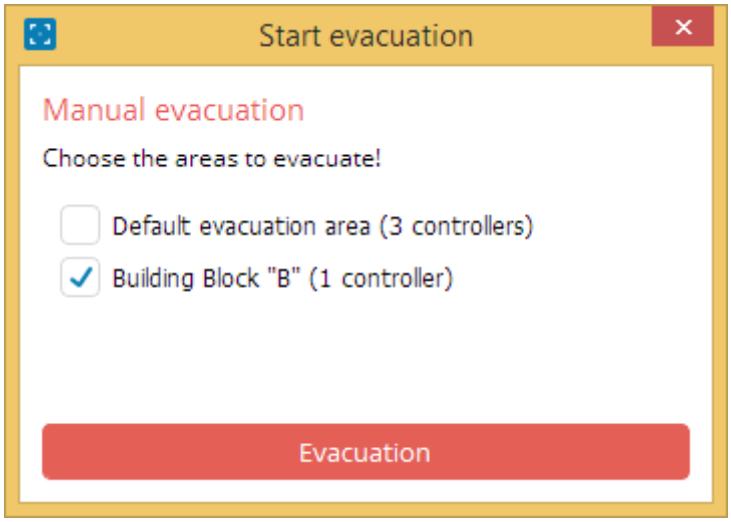


Figure 55: Starting an evacuation plan manually

Operators who are selected in **Operators to notify** will receive an email notification when an evacuation is started, which will include the evacuation list in Excel format as an attachment, and in the client software a red Evacuation button will appear above the name of the operator who is logged in. The evacuation list contains the names of the persons who are inside or in an unknown location, their last known location, their status and the time when their location was updated.

To monitor an evacuation in progress, open the evacuation list by clicking on the red **Evacuation** button above the logged in operator's name. The location data of the people in this list can be changed by clicking on the "**...**" button in the bottom menu bar after selecting the people and then select *Change Location*.

The evacuation can be cancelled by clicking on the **cancel evacuation** button. In the window that appears, the reason for the interruption must be entered in the **Comment** field.

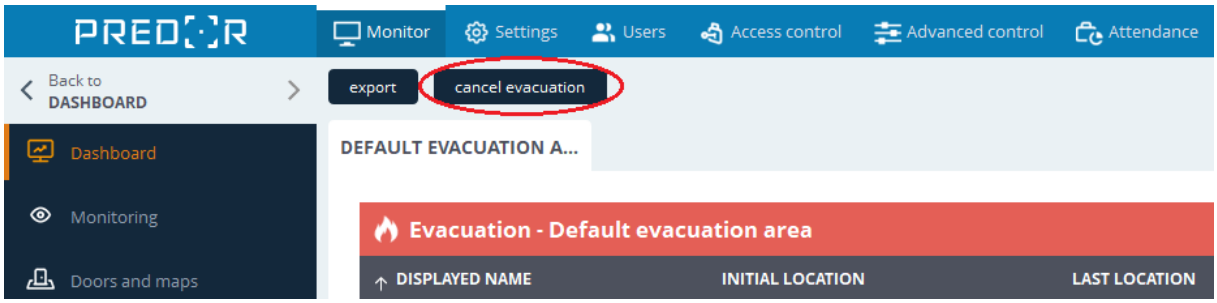


Figure 56: Cancel evacuation button

After we are sure that the people are in a safe place, we can close the evacuation by clicking on the **acknowledge evacuation** button. In the window that appears, a note can be entered in the **Comment** field.

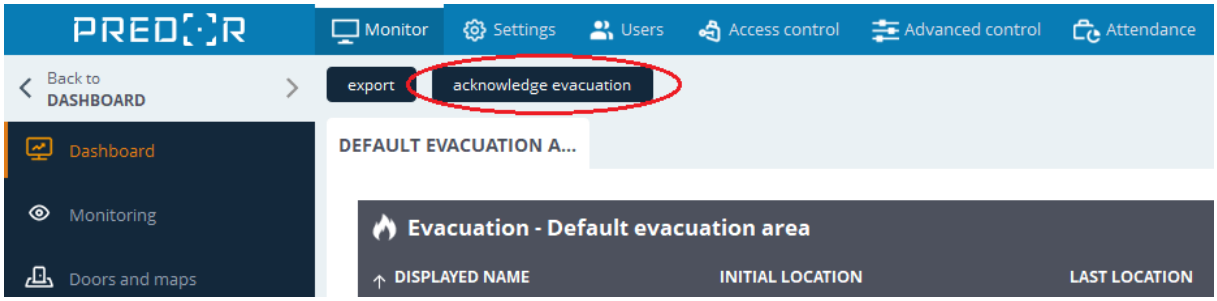


Figure 57: Acknowledge evacuation button

The **cancel all disasters** button can be used to stop disaster plans, all pending evacuations and to reset doors to their normal mode.

Clicking on the **special cards** button will bring up a dialog box where you can add special cards to your system. These special cards are emergency cards or disaster plan cards. Emergency cards can open all doors, so they should be stored in a safe place and used with care. The disaster plan card activates the disaster plan setting that you have created. None of these cards are assigned to a person.

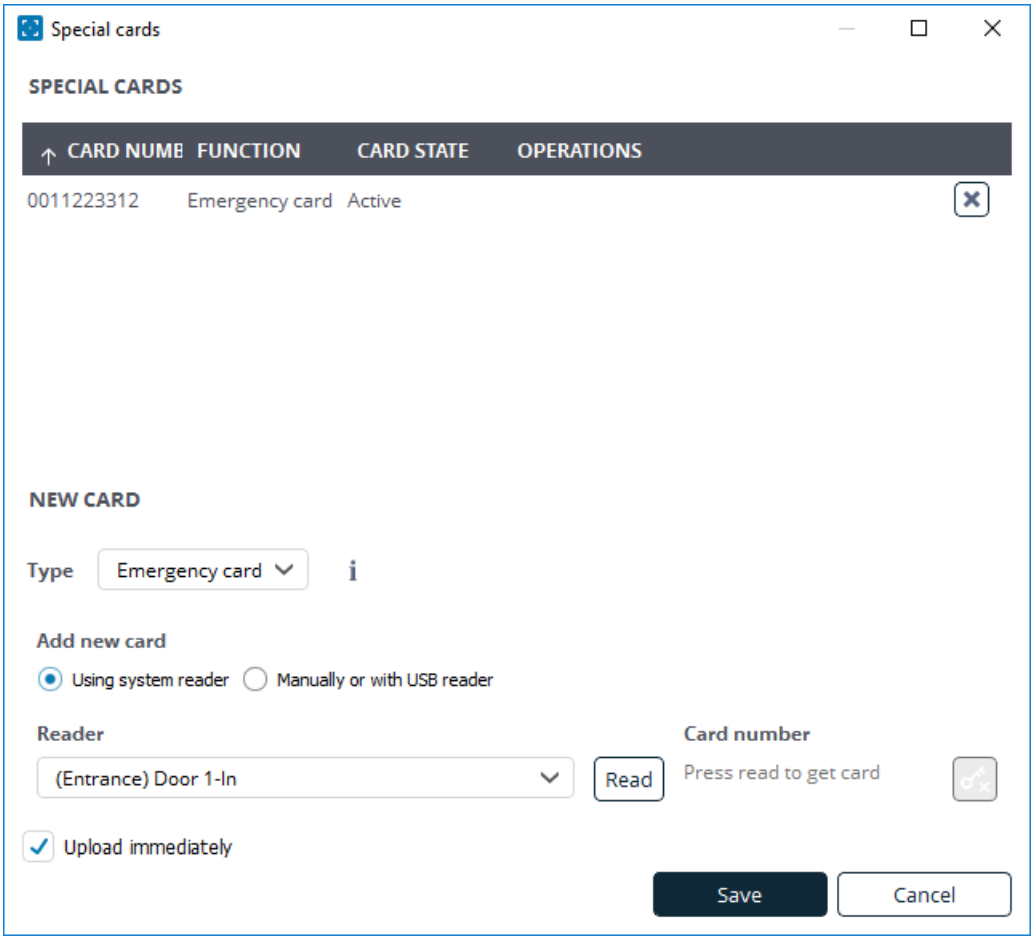
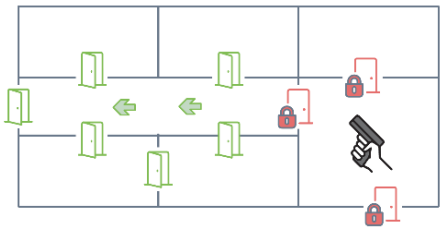


Figure 58: Special cards dialog

Disaster plans



Some objects must be prepared to various emergencies or even an armed attack. If necessary we can activate any pre-configured plans triggered by software, card read, button or emergency code.

For example, we can lock off the attacker's path and open the escape routes for the employees. The whole object can be locked down if needed.

Emergency plans activation options:

- **Manually from the software**
- **With a button connected to the AUX input. At first the input should be set (NO/NC) in the edit controller wizard.**
- **With special card: plan activation card can be created for each emergency plan.**
- **Activated by threatcode: reader with keyboard is needed. The threatcode should be enabled on the reader.**

The plan activation can be delayed as well. Thus, the doors' operating mode will switch after after the predefined time.

The system can send email notification about the activated plans.

The plans can be flexibly configured and any door modes can be set.

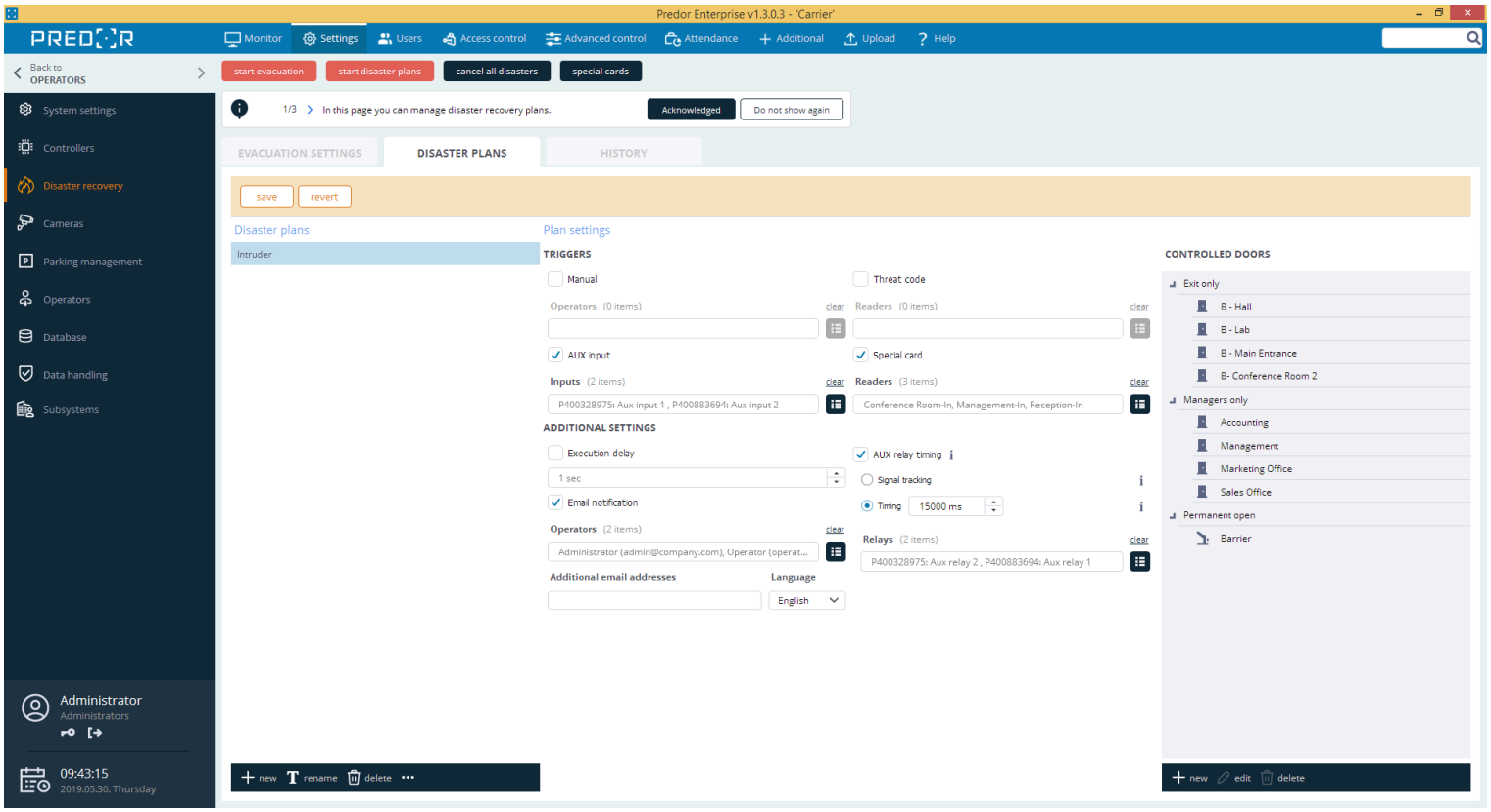


Figure 59: Setting up disaster plans

History

On this tab the list of evacuation and emergency plans can be seen. Detailed evacuation lists can be viewed and exported again.

Cameras

Video devices

On the left you can see the cameras and recorders that are added to the system.

To add a camera, click on the “new” icon. In the dialog box, the parameters are specified, and then the device is added to the system using the OK button.

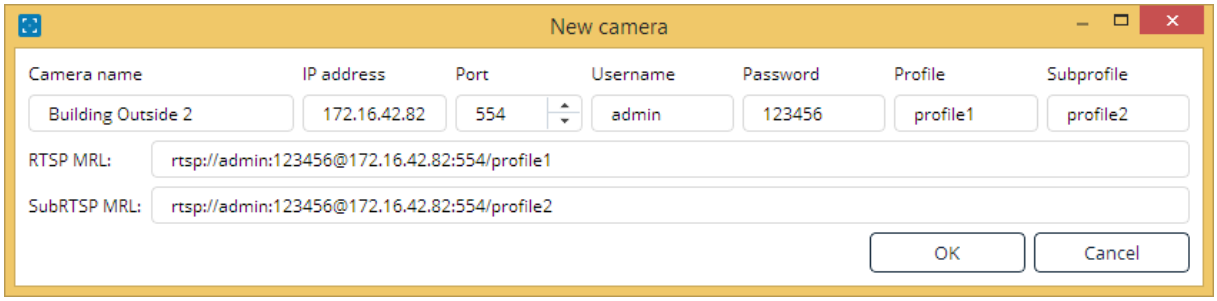


Figure 60: Adding new camera to the system

The cameras can be assigned to doors. The side of the gateway should be choosen for each cameras. In the event of an alert, the live stream of the cameras is automatically displayed in a pop-up window.

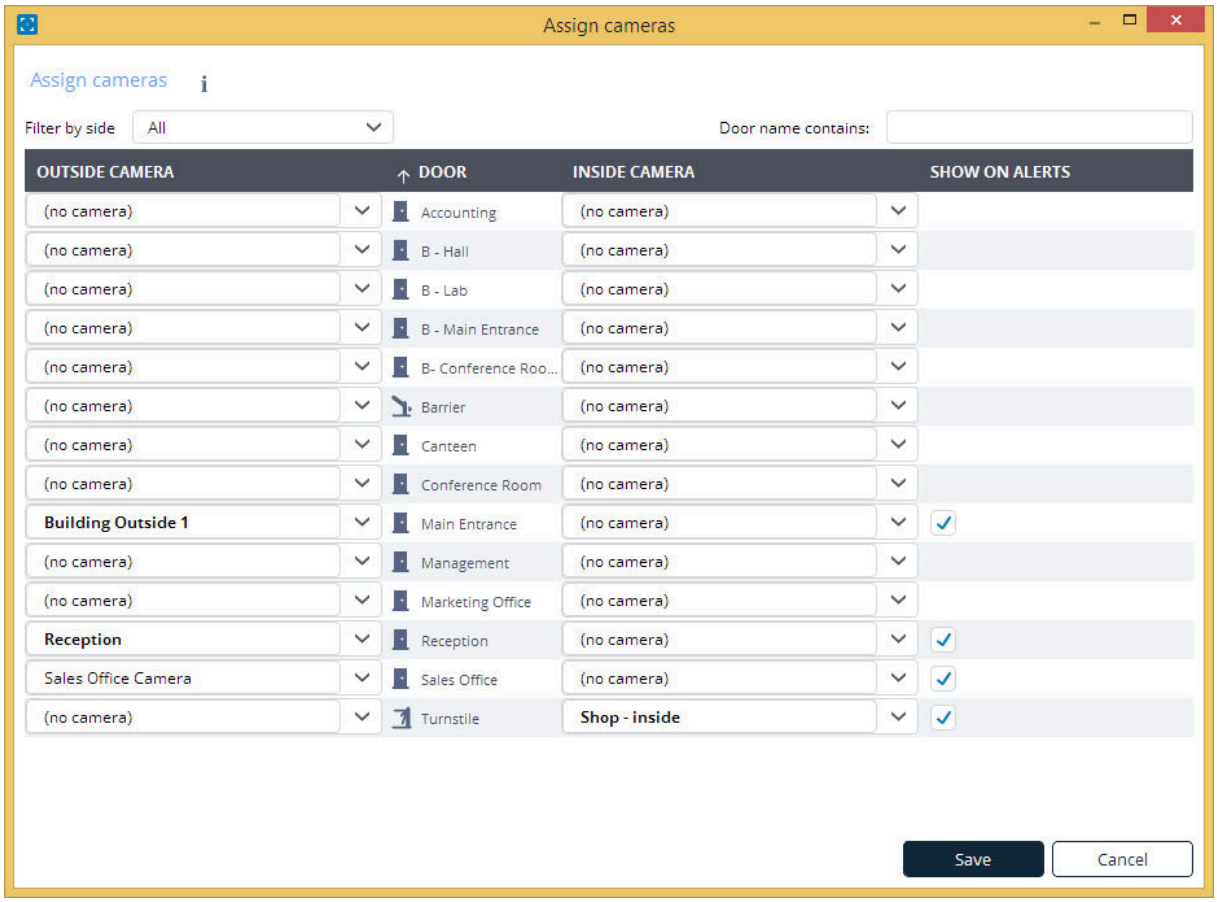


Figure 61: Assigning cameras to doors

Recording rules

You can create custom rules that specify which events will trigger snapshots and/or video recordings. Of course you can set the cameras, the doors, the users and you can specify whether to record the event-side camera stream, the opposite side, or both. Thus, the

system will always record the stream of the proper camera, depending on the event type.

Additional parameters can also be set. For instance, the rule's validity period, the day of the week, which users' events to record. Be careful with these parameters because the recording will only happen if *ALL* conditions are met. For example if a rule is set to record a camera when a door is opened, and a user or user group is provided, then this rule will never be active because in the Predor system the "Door opened" event does not include user or user groups.

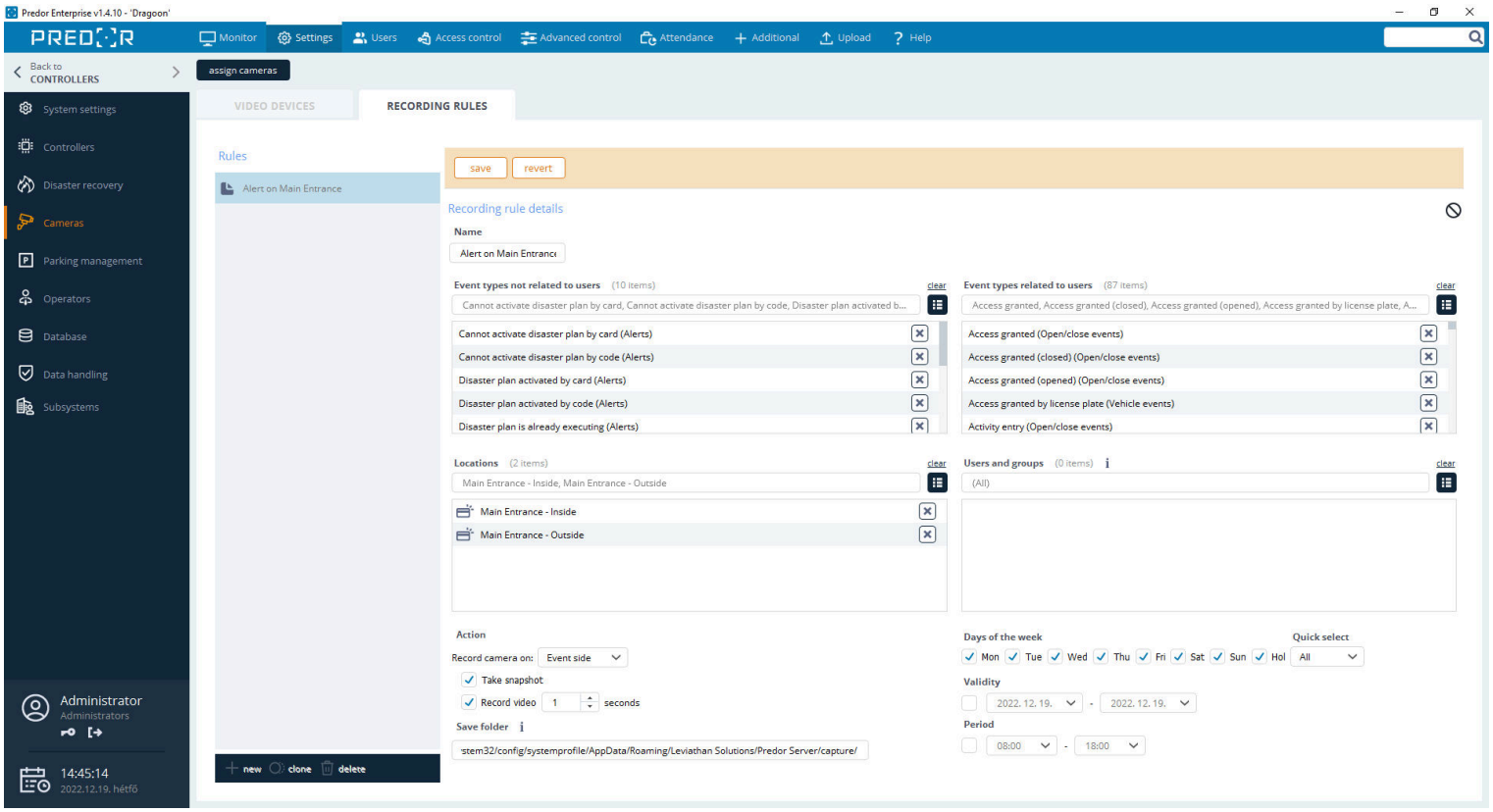


Figure 62: Recording rule editor page

To activate this function, you must assign the cameras to doors (assign cameras button).

Video streams and screenshots will be saved in the folder that is set in the Settings / System Settings submenu. You can watch the recordings in the Event List submenu by clicking on the camera icon.

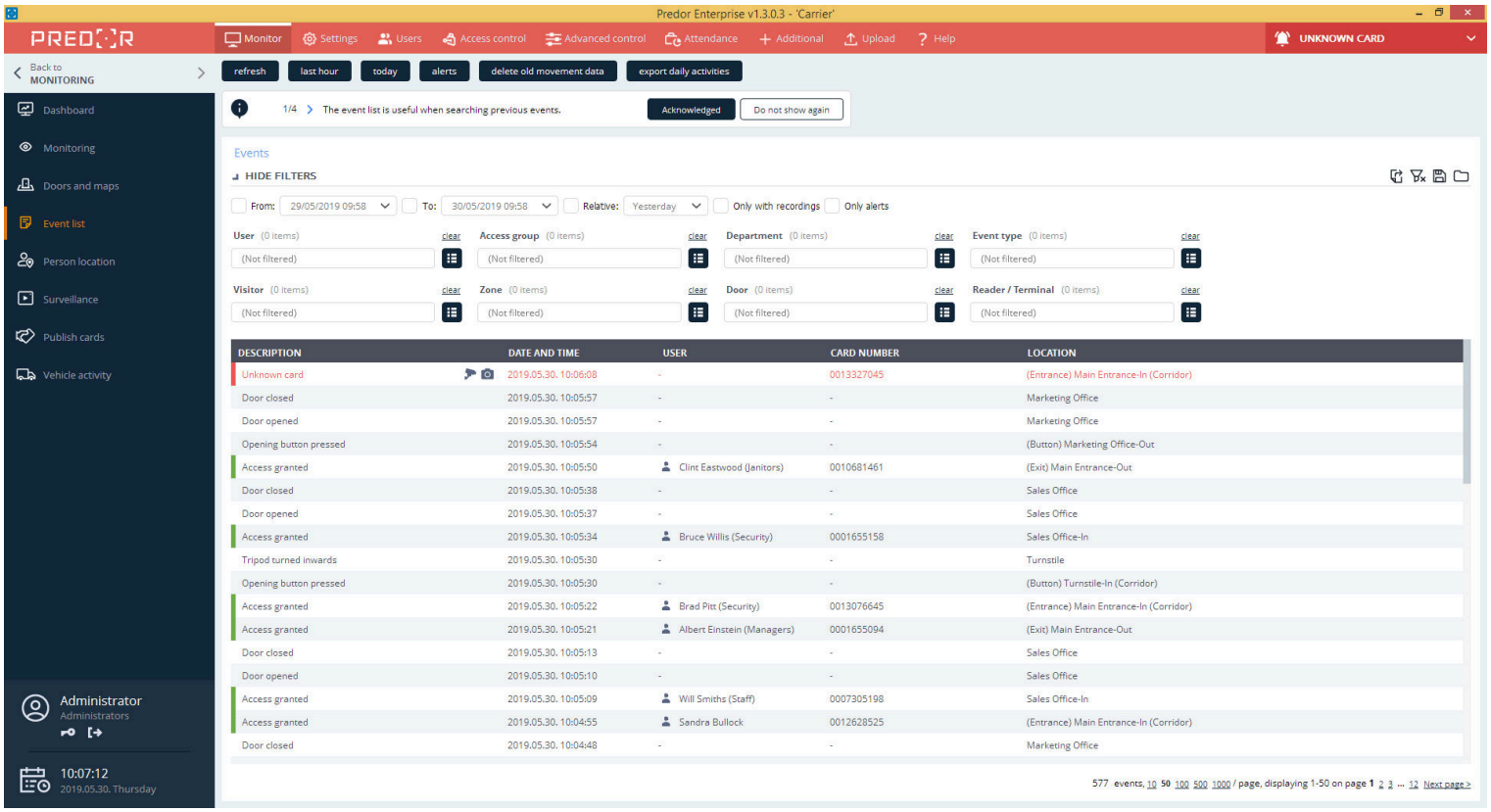


Figure 63: Event with captured photo and video recording

Parking management

In this menu you can manage the vehicles and set the license plate recognition. You can use the **import vehicles** button on the top to import vehicles from an Excel file. The **export vehicles** button next to it will export the vehicles in your system to an Excel file.



TIP: If you find it easier to put the vehicle details into an Excel file, you can create a sample export, add the necessary details and then import the file into the system.

Vehicles

Vehicles can be categorized into vehicle groups, so you can easily limit their access rights and the authorized drivers. If you create a new vehicle group, you can specify the members and the authorized users / access groups who are allowed to drive the cars.

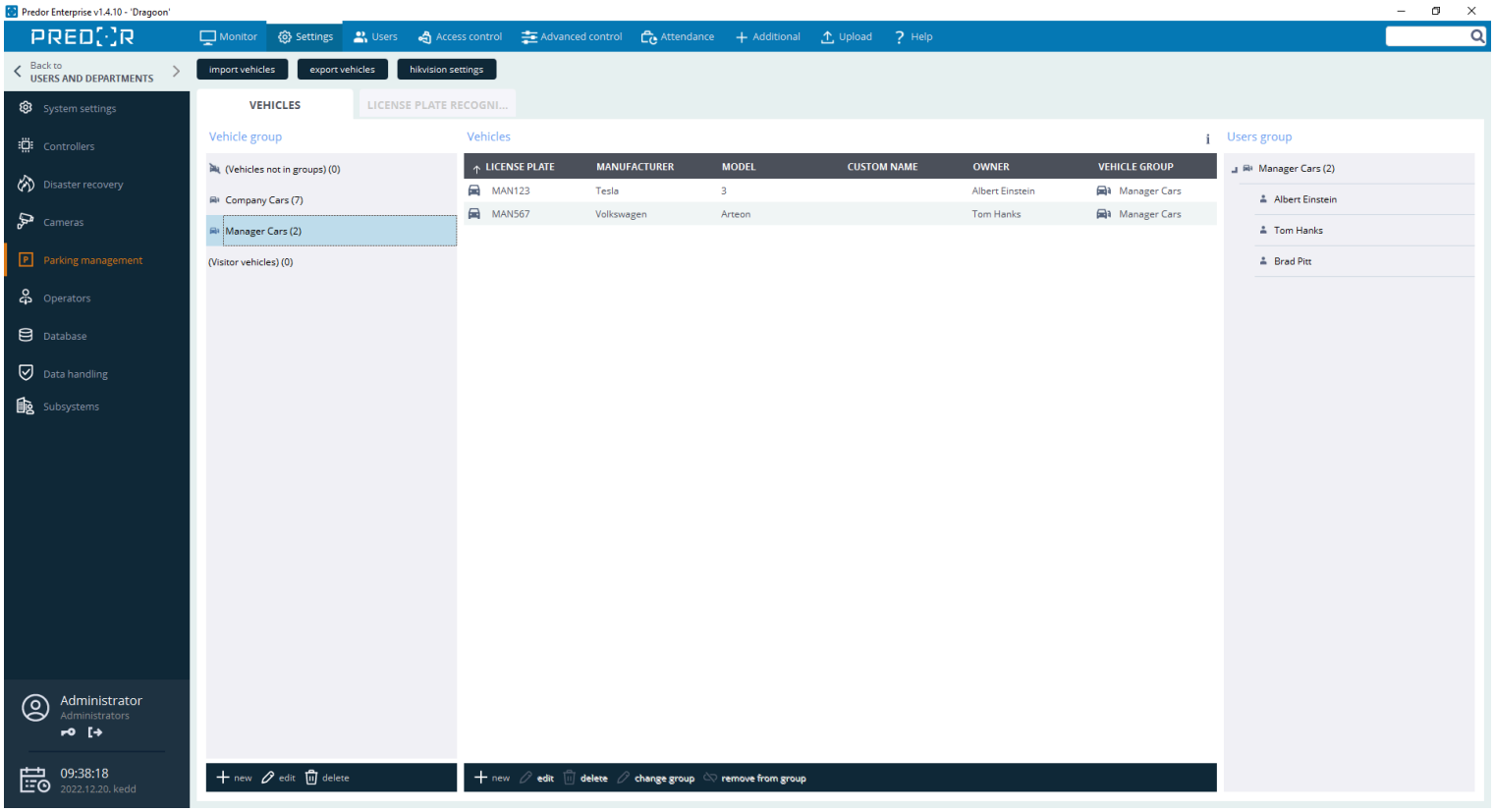


Figure 64: Vehicles and vehicle groups

If you select a particular user as the owner, this user can drive the vehicle independently from the access groups. If an access group is selected as drivers, then the members of the group can use the vehicle.

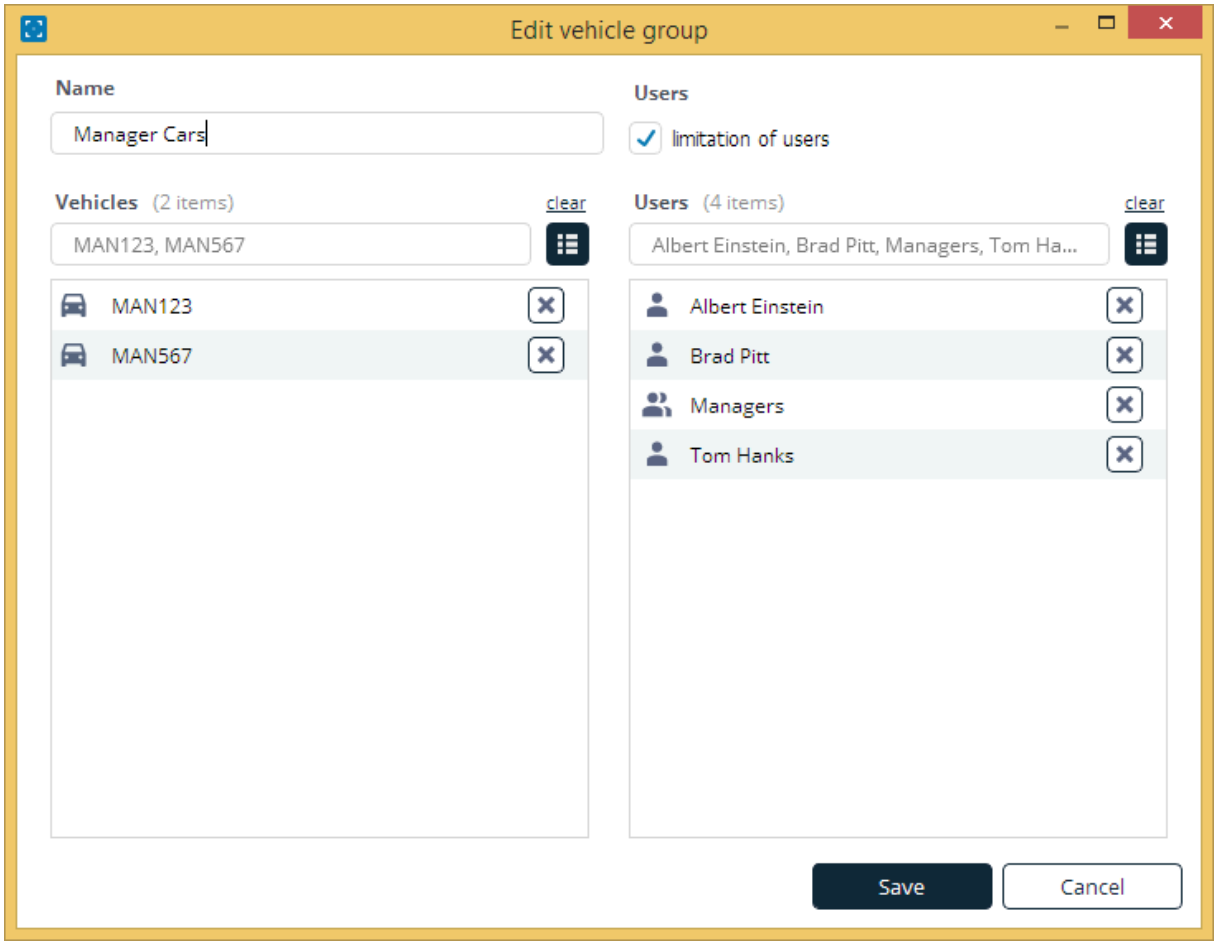


Figure 65: Edit vehicle group dialog

When adding a new vehicle, the registration number is required, which will identify the vehicle. In addition, you can specify the type, model, unique name, owner and vehicle group.

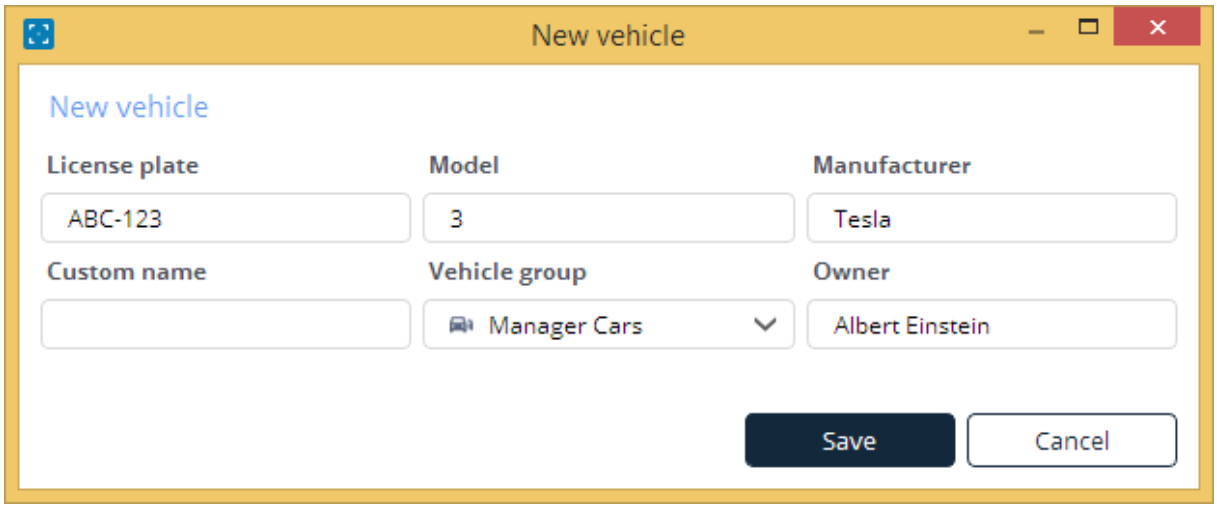


Figure 66: Adding a new vehicle

Vehicle and vehicle groups should also be given access rights. You can do this in Access Control / Access privileges menu.

Guest vehicles can be registered in the New Guest window (Monitor / Publish card or User / Visitor settings) by entering the registration number of the guest vehicle. These vehicles also can be seen in the Parking Management submenu.

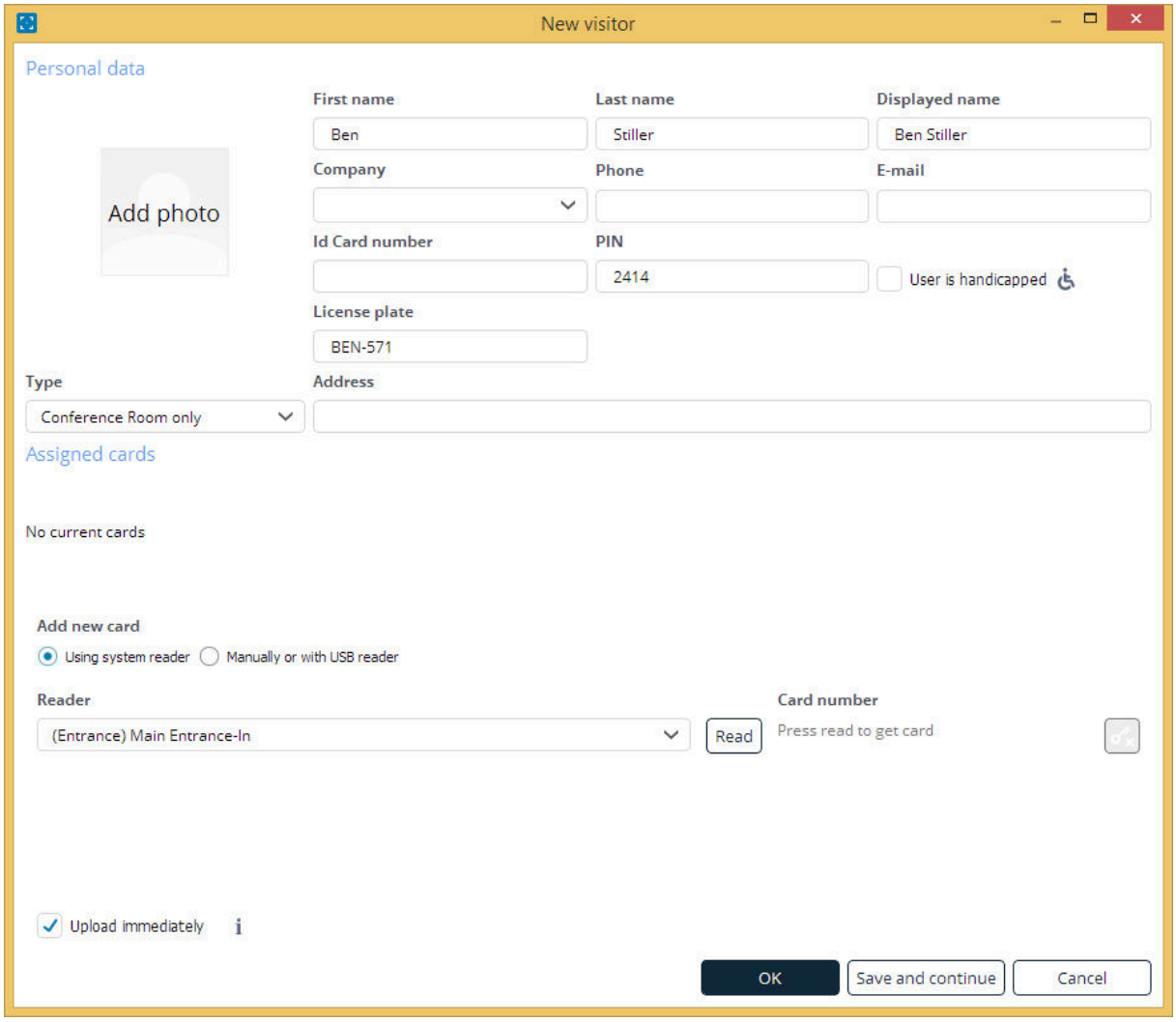


Figure 67: License plate input field in the add new visitor dialog

Use the buttons on the top to export or import the vehicles. In both cases, we only work with non-guest vehicles.

License plate recognition

Lpr port settings button: by pressing this button, a small input field appears. In it we can set the port on which our system listens for data packets from the LPR (Hikvision, Dahua) camera.



WARNING: When using Hikvision or Dahua license plate recogniser, the settings must also be configured in the camera interface, to work properly. For a detailed description, see the Hikvision license plate recogniser configuration for Predor Enterprise system or Dahua license plate recogniser configuration for Predor Enterprise system appendix.

Clicking on a new button will allow you to add a **TechsonLPR**, **Hikvision** or **Dahua** license plate recogniser. Here we can set the IP address, and in the case of TechsonLPR, the data and control port. For Hikvision, it is also possible to save the license plate image. We can then specify the entry method per LPR channel:

- **License plates only:** the license plates are used as access credentials. The vehicle must be included in the list of registered vehicles and must have the right to the selected reader.
- **Card OR License plate number:** the gateway opens if the license plate is correct or a proper user card is presented. The license plate is also read and logged.
- **User card AND license plate:** the gateway opens only if the user presents an authorized card, the LPR reads a proper license plate number and the user has rights to drive the vehicle. For Hikvision cameras, the system reads the license plate first, and the waiting time for card reading must be specified in the *Timeout of card read* field.
- **Mixed:** first, the system scans the license plate number. If the license plate number has a user, guest, or permanent user associated with it, either by association or indirectly through a vehicle group, then the entry is performed in **User AND license plate** mode. If the license plate number is not assigned to a user or guest in any way, then the entry is performed in **Only license plate number** mode. If there is no license plate number, only identification (e.g. card reading) and the user or guest has no license plate number associated with it and the authorization is appropriate, then the system allows entry.



TIP: When using a Hikvison or Dahua camera, ONE license plate recognizer has only ONE channel.

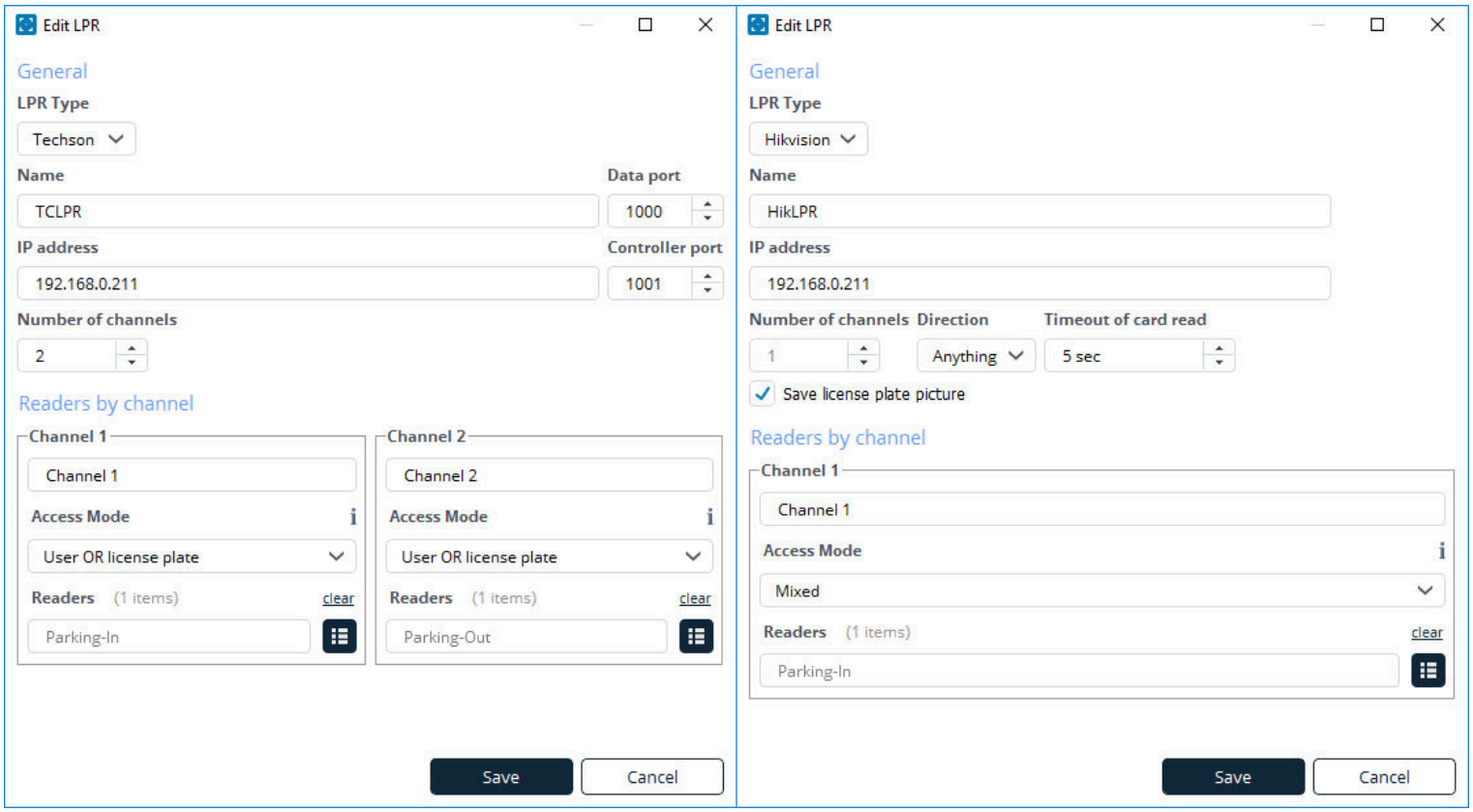


Figure 68: Configuring Techson and Hikvision License Plate Recogniser and access modes

When using a Dahua camera, the valid detection time can also be modified. If the Predor server goes down, the camera will continue to try to send data to the server, which cannot process it. When the Predor server is up again, the camera will resend the license plate numbers it has read, which may cause the barrier to open several times, unnecessarily. By changing the valid detection time, this problem can be avoided and data older than the set time will not be processed.

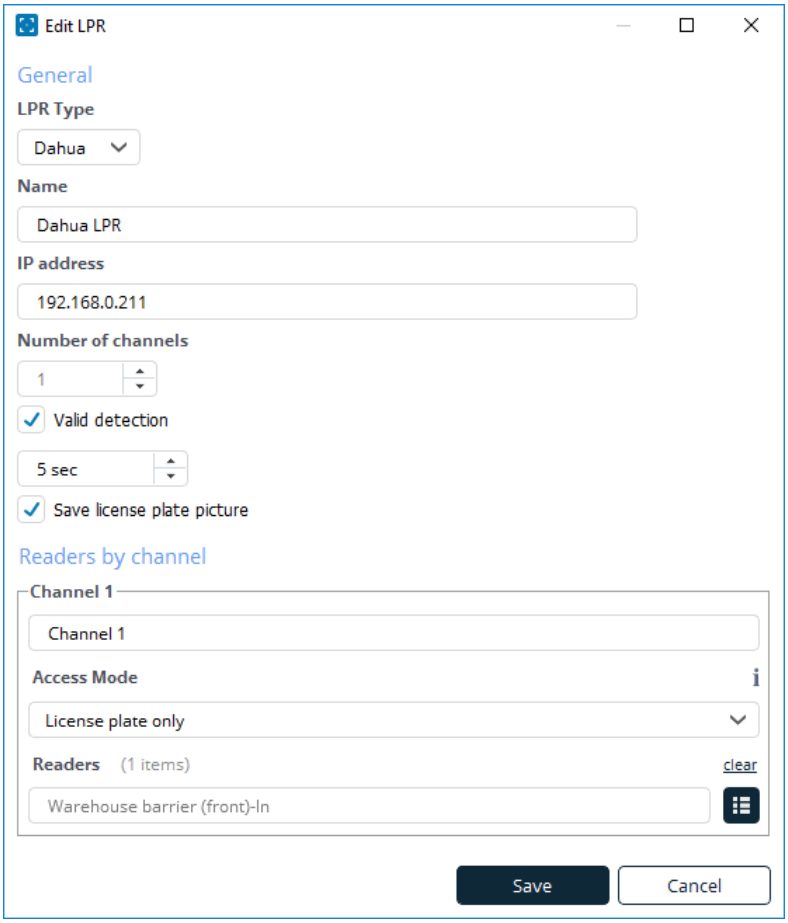


Figure 69: Configuring Dahua License Plate Recogniser and access modes

Operators

Operators are the people who use the software. *Do not confuse them with the card holder users.*

On the **Operator groups** tab authorization levels can be adjusted for each submenu in the software. New operator groups can be created by using the **+new** button, under the operator group list.

There are 3 authorization levels for each menu item:

- **No access:** the operator cannot see this menu
- **Restricted:** the operator can see this menu, but cannot modify anything. In case of the "Calendar", "Worktime profiles" and "Worktime reports" menus, this option allows the operator to have unique access levels for each department.
- **Full:** the operator can modify and delete as well

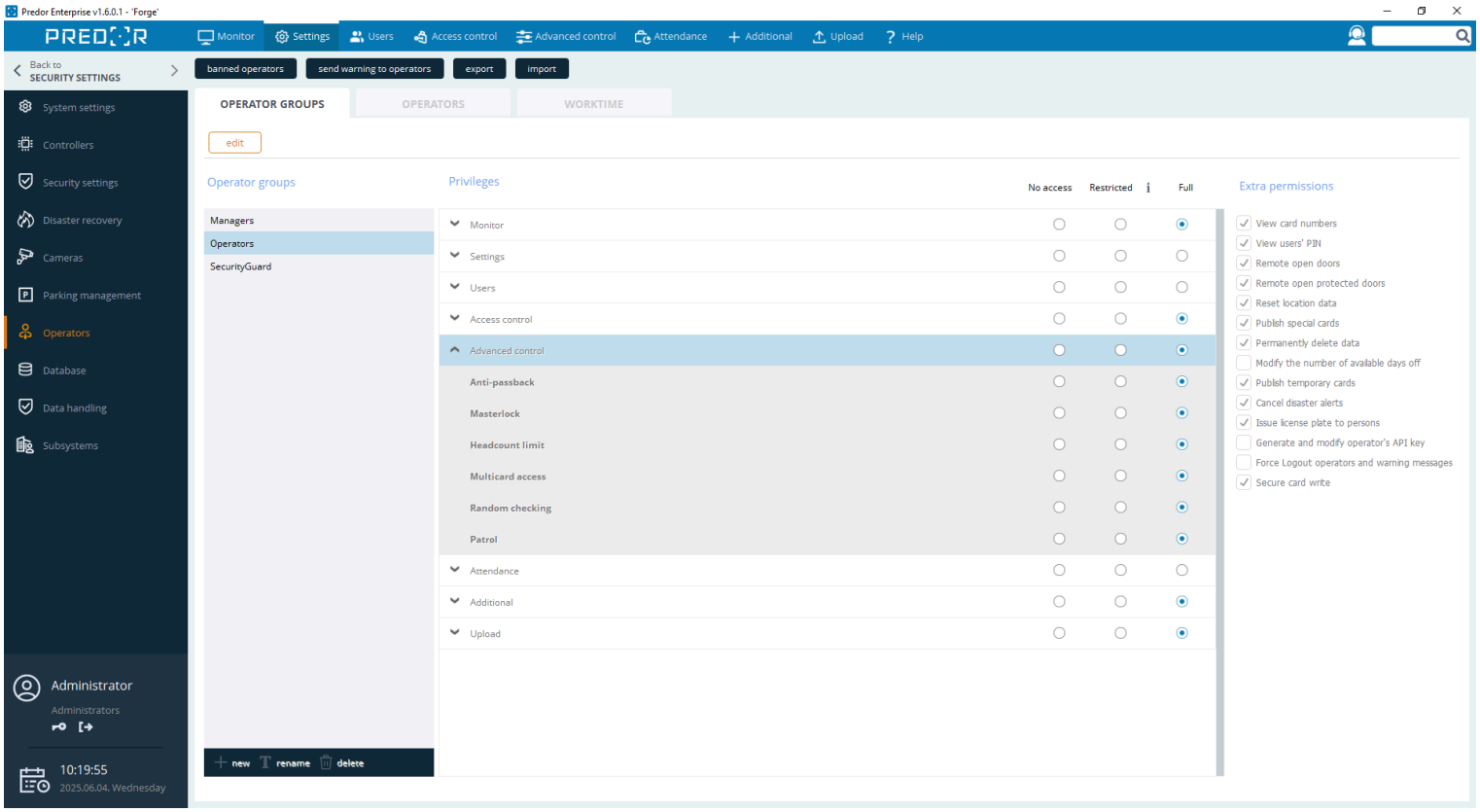


Figure 70: Managing operator groups

Extra permissions can be set to:

- **View card numbers:** if enabled, the operator can view the number of the cards
- **View users' PIN:** if enabled, the operator can view the pin codes
- **Remote open doors:** if enabled, the operator can open doors from the software
- **Remote open protected doors:** if enabled, the operator can open doors from the software, which belong to a zone marked as protected in the access zones menu
- **Reset location data:** if enabled, the operator can reset the location data of the users
- **Publish special cards:** if enabled, the operator is authorized to give out emergency cards and other special card types
- **Permanently delete data:** if enabled, the operator can delete data from the system permanently
- **Modify the number of available days off:** if enabled the operator can modify the number of the users' available days off
- **Publish temporary cards:** if enabled, the operator can publish temporary cards
- **Cancel disaster alerts:** if enabled, the operator can cancel any disaster alert events.

- **Issue license plate to persons:** if enabled, the operator can add license plate number to users and visitors
- **Generate and modify operator's API key:** if enabled, the operator can generate and modify the API key of the operators
- **Force Logout operators and warning messages:** if enabled, the operator can
- **Secure card write:** if enabled, the operator can

On the **Operators** tab the operators in the system are listed. Use the **+new** button to create a new operator. In the new operator dialog all basic information can be filled for the new operator. If we wish, we can set a temporary password and tick the "Must change password" checkbox, which will enforce a password change upon the first login of this operator. Don't forget to appropriately set the operator's group!

When editing an operator, an API key and the expiry date of the key can be specified. By clicking on the Logout from all sessions button, it is possible to log out the operator from the Predor system.

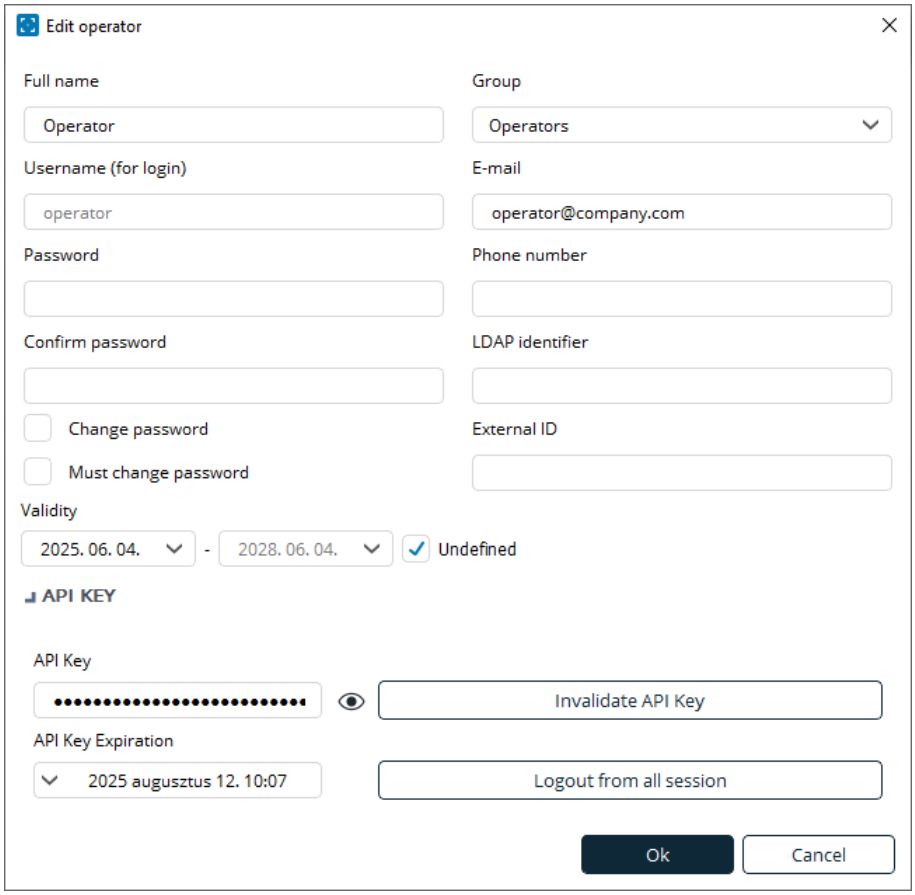


Figure 71: Edit operator dialog

The **activate/deactivate** buttons on the operators tab can be used to temporarily re-

voke the login permission of the selected operators.

On the **Worktime** tab the table consists of the operators and the departments. The value in each cell defines whether the operator can access the work time data of the department or is also allowed to make changes to it. There are 3 access levels, just like in the operator groups tab: no access, read or modify. The table contains only those operators who have restricted access to at least one of the “Calendar”, “Worktime profiles” or “Worktime reports” menus.

The access levels for the above mentioned menus can be interpreted as access for functions:

- **Calendar** - Handling the assignments of users
- **Worktime profiles** - Handling the worktime profile assignments of users
- **Worktime reports** - Handling the worktime data of users

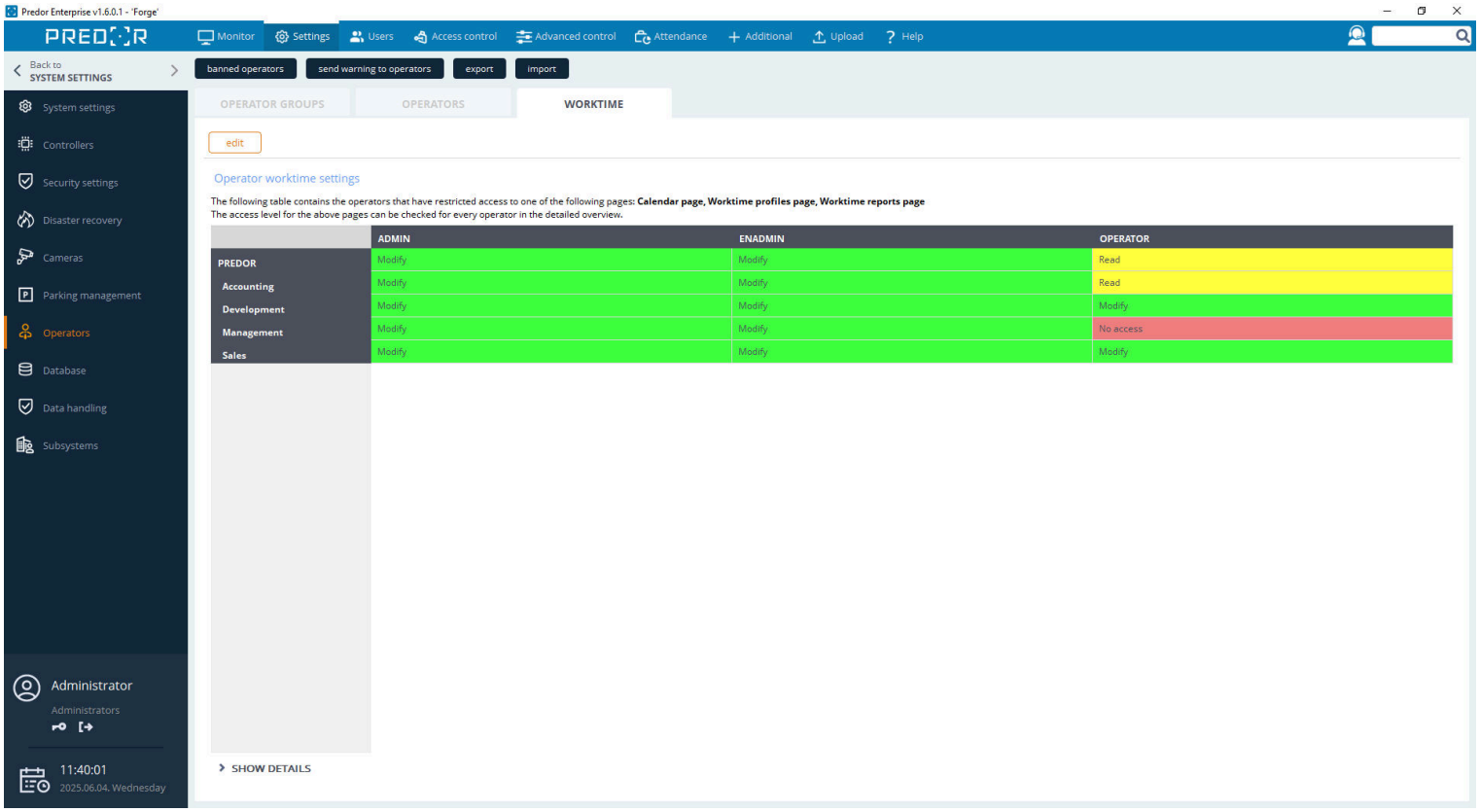


Figure 72: Work time data access for operators can be further resticted for each department.



EXAMPLE: The operator in the “Accountants” operator group has restricted access level to the “Calendar” menu and full access to the “Worktime reports” menu, also only has full access for the “Accountants” department and read access to every other department (the latter can be set on the “Worktime” tab). In this case, the operator can see and edit the worktime data of every employee, but can only edit the worktime shift assignments of those employees who are in the “Accountants” department.



TIP: If we want an operator to be able to create shift assignments, but not to see any worktime data, the solution is for the operator to have full access for the “Calendar” menu and no access for the “Worktime reports” menu. In this case, the reports menu will not appear for the operator and the user calendar tab on the “Calendar” menu will not display worktime data for any employees.

In the **banned operators** menu a list of the operators can be viewed who are currently banned by the password cracking protection function. Bans can be lifted immediately by removing the operators from this list.

By clicking on the **send warning to operators** button, a message can be entered in the dialog, which can be sent to the currently logged in operators by clicking on the OK button. *For example, in the case of a software update, it can be used to indicate that the server will be down soon.*

Database

On this screen, you can view the details of the currently active database connection, as well as the steps to backup and restore the database.

If the database has been backed up, it is possible to restore the database to its previous state in case of corruption. In this case, the settings that were valid at the time of the database backup will be applied. Whenever a database is restored, data loss should be expected, because the changes made since then and their effect will have been lost. Some examples are: *controller password, users, cards, network configuration, door settings, etc.*. Therefore, it is necessary to perform **Reset and Upload** on all controllers and terminals after restoring. Two things are important to note about this:

- If the network settings, the controller password, or a device has been changed, the reset and upload will fail because the devices are not available with the previous set-

tings. So it is necessary to apply changes to the devices in Predor according to their last state. The password, network settings and other changes must be set.

- The Predor software tries to collect events *(For example: door opening events, activity entries, fire alarms, etc.)* from controllers and terminals since the database backup, which can only be done if it can access the devices. So if this data is needed, wait until all the events from the devices are received, only after that should **Reset and Upload** be selected.

All changes made by operators and employees since the database was backed up must be redone. *These can be for example: day-off and other working time entries, new users, calendar and profile changes, etc.*



CAUTION: Database backup is essential to avoid data loss.

Data handling

This menu helps companies to comply with **GDPR** rules. *The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).*



ATTENTION! The user quota in the GDPR module and the base license has to be the same.

The range of data to be deleted and the schedule can be configured in rules that can be run automatically. So the system can handle personal data without any interference.

You can specify the type of data you need to delete and how long the data can be stored in the system.

Caution! The selected data will be permanently and irreversibly deleted!

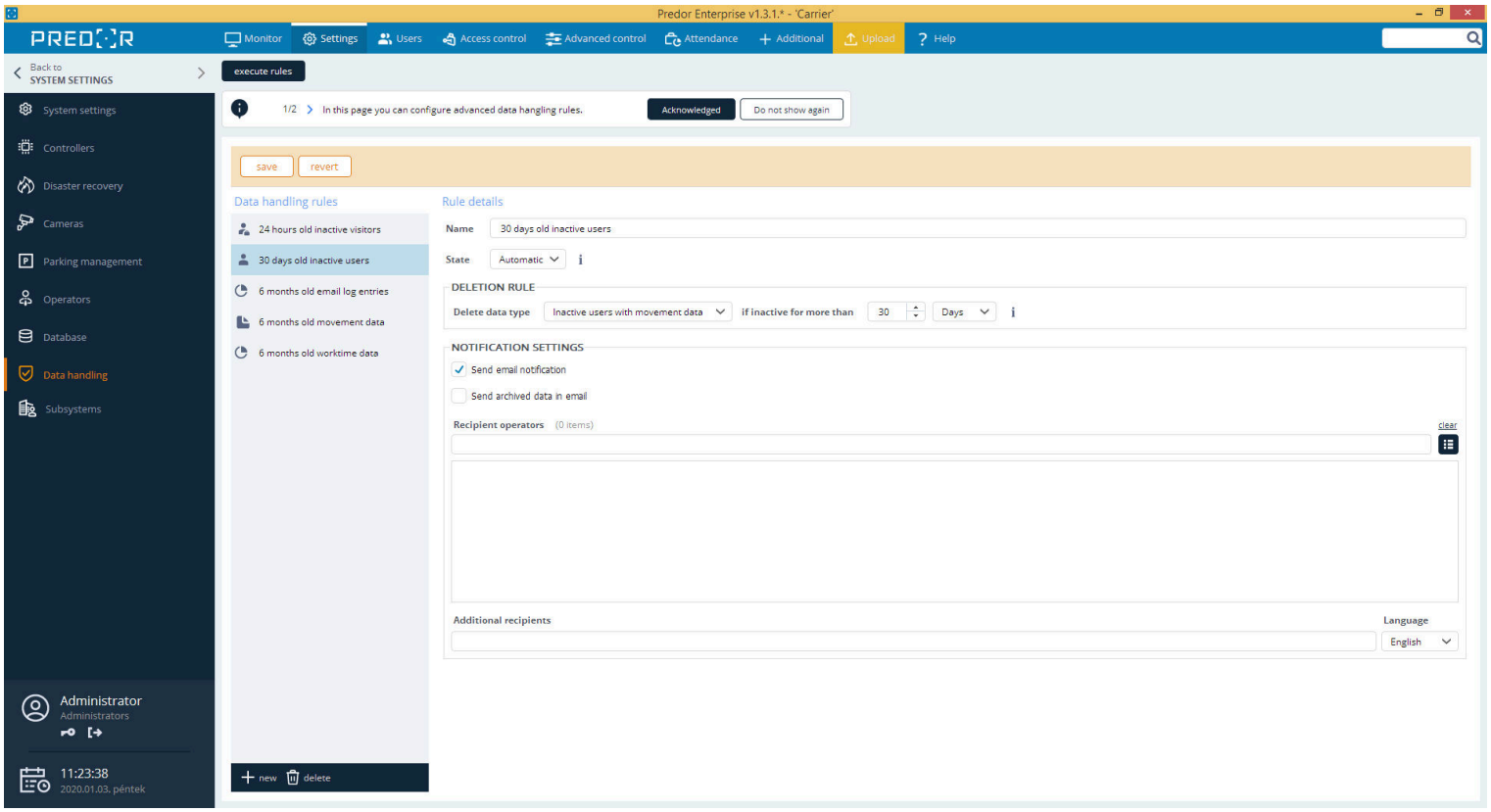


Figure 73: Data handling rules

Subsystems

To use the menu, you must have the Subsystem management module. The Manager Company can manage subsystems under this menu. In the **Subsystems** tab, it is required to enter a name for the subsystems, set the license package for the company, and some other optional data can be entered: *tax number, headquarters, main contact name, phone number, e-mail address*. In addition, this interface allows to configure the subsystem's access rights to the devices (*Working Time Terminals, Cameras, Access Points*)

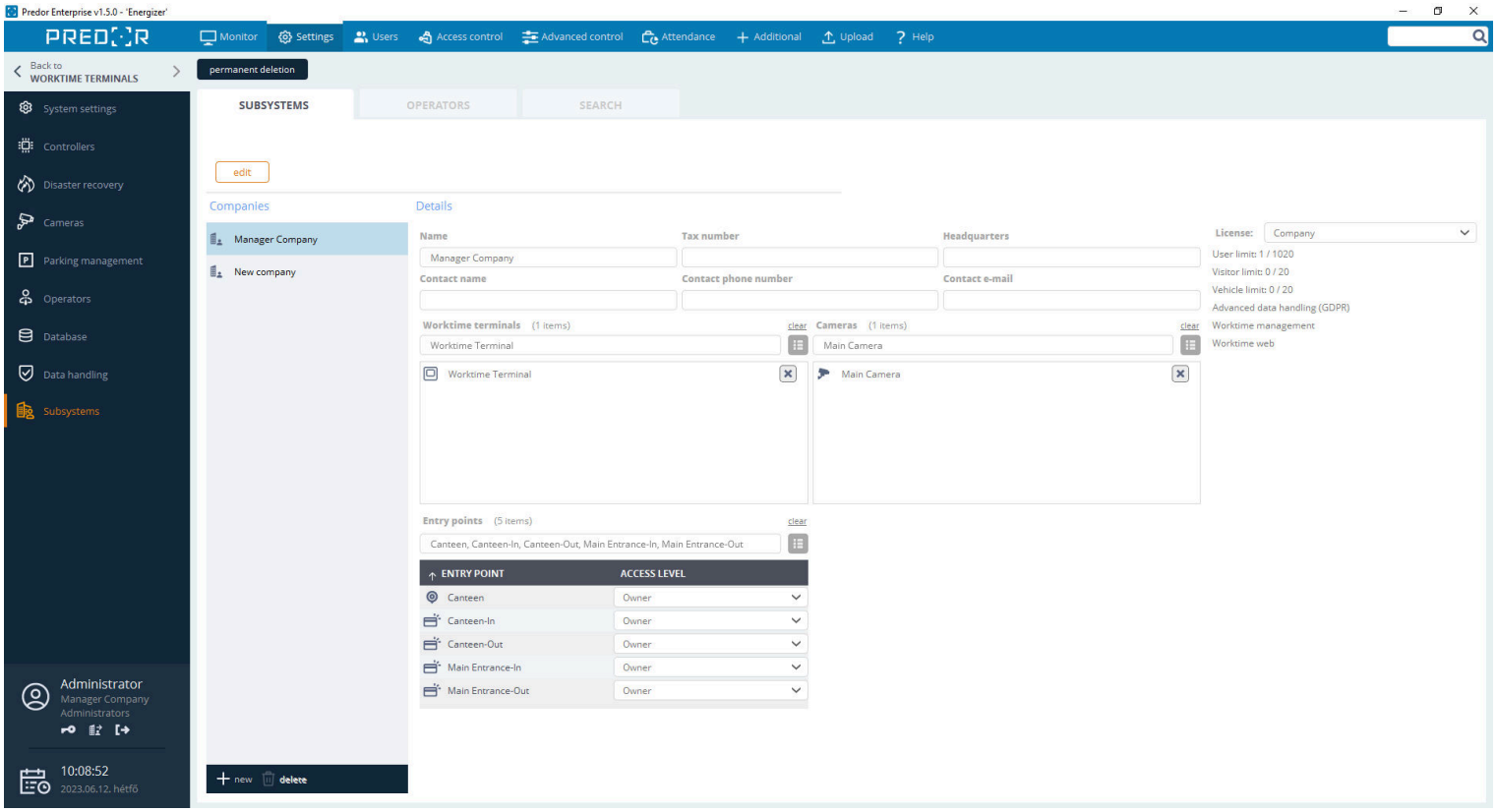


Figure 74: Subsystems tab

Under the **Operators** tab, you can configure operator access by subsystem.

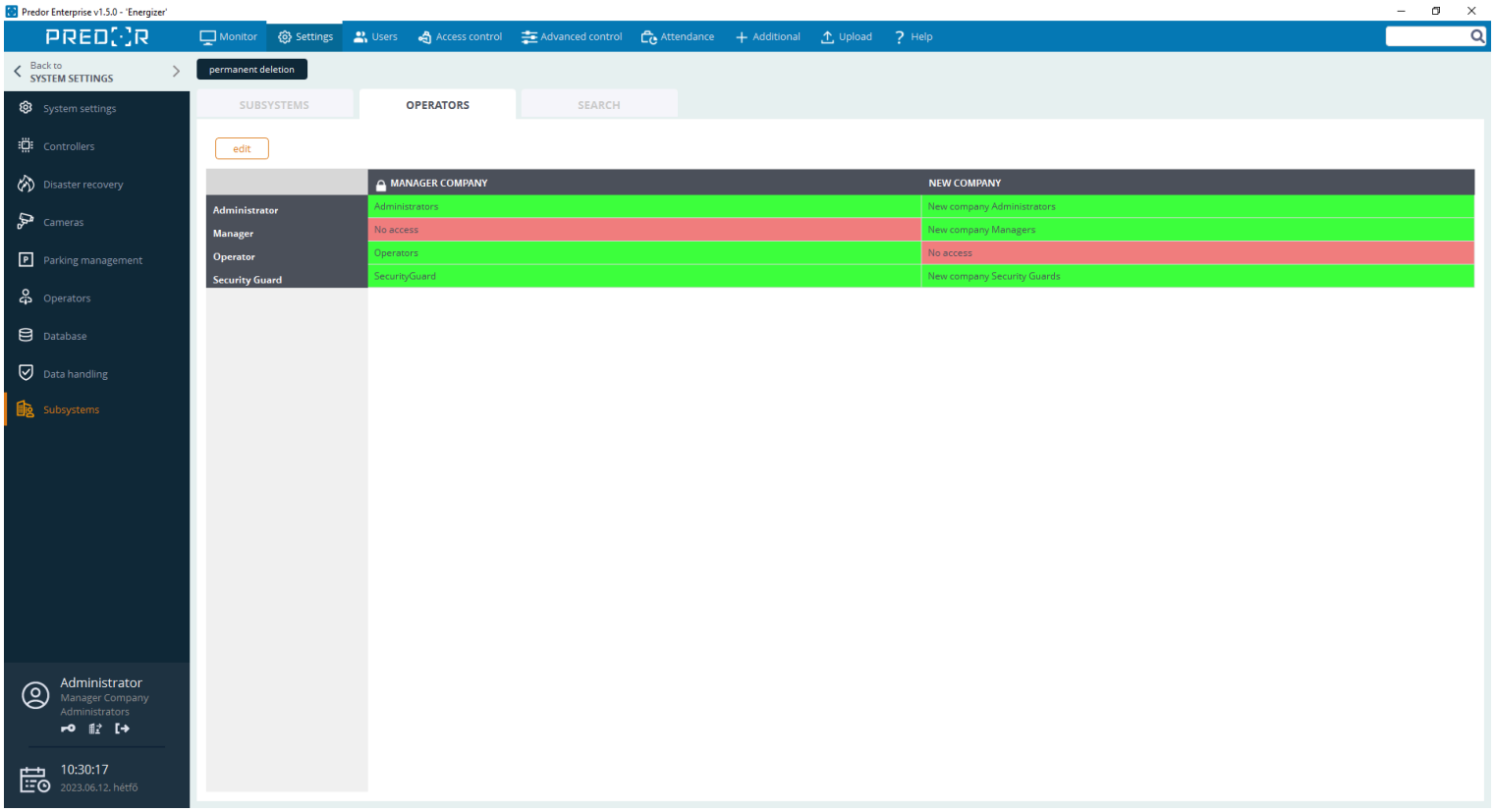


Figure 75: Managing operators by company

The manager operators can search users by name or card number under the **Search** tab.

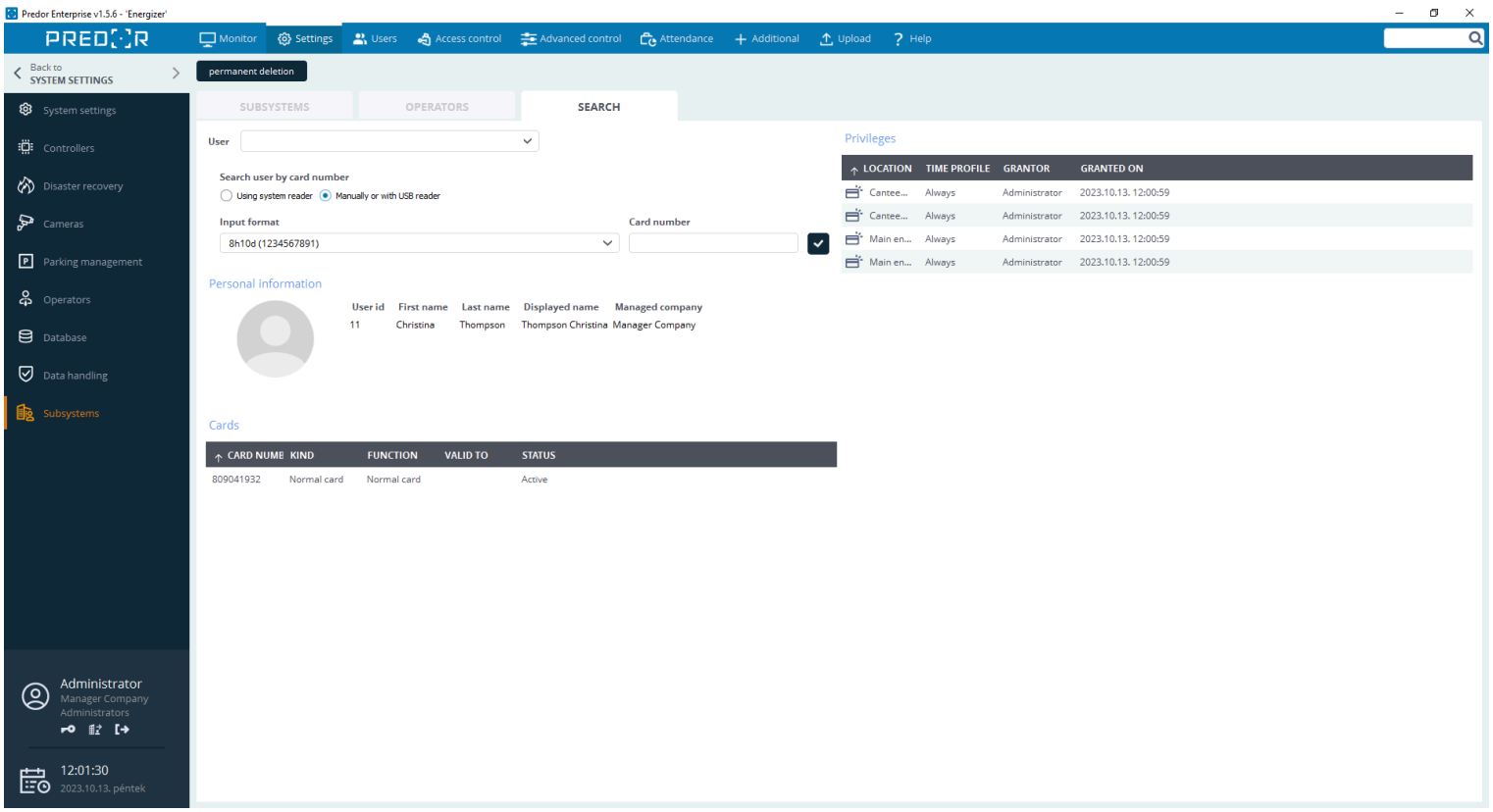


Figure 76: Search for users

7 USERS MENU

Users and departments

In this menu users of the system can be managed and overviewed. Between the filters and the table, the program indicates how many users can be managed with the purchased license. New users can be added by clicking on the **+new user** button. First, last and displayed names are must be filled, other fields are optional. The **Displayed name** is the person's unique name in the software and is used in every menu and work time report with the exception of the attendance report. By using unique displayed names, persons with the same name are distinguishable in the software.

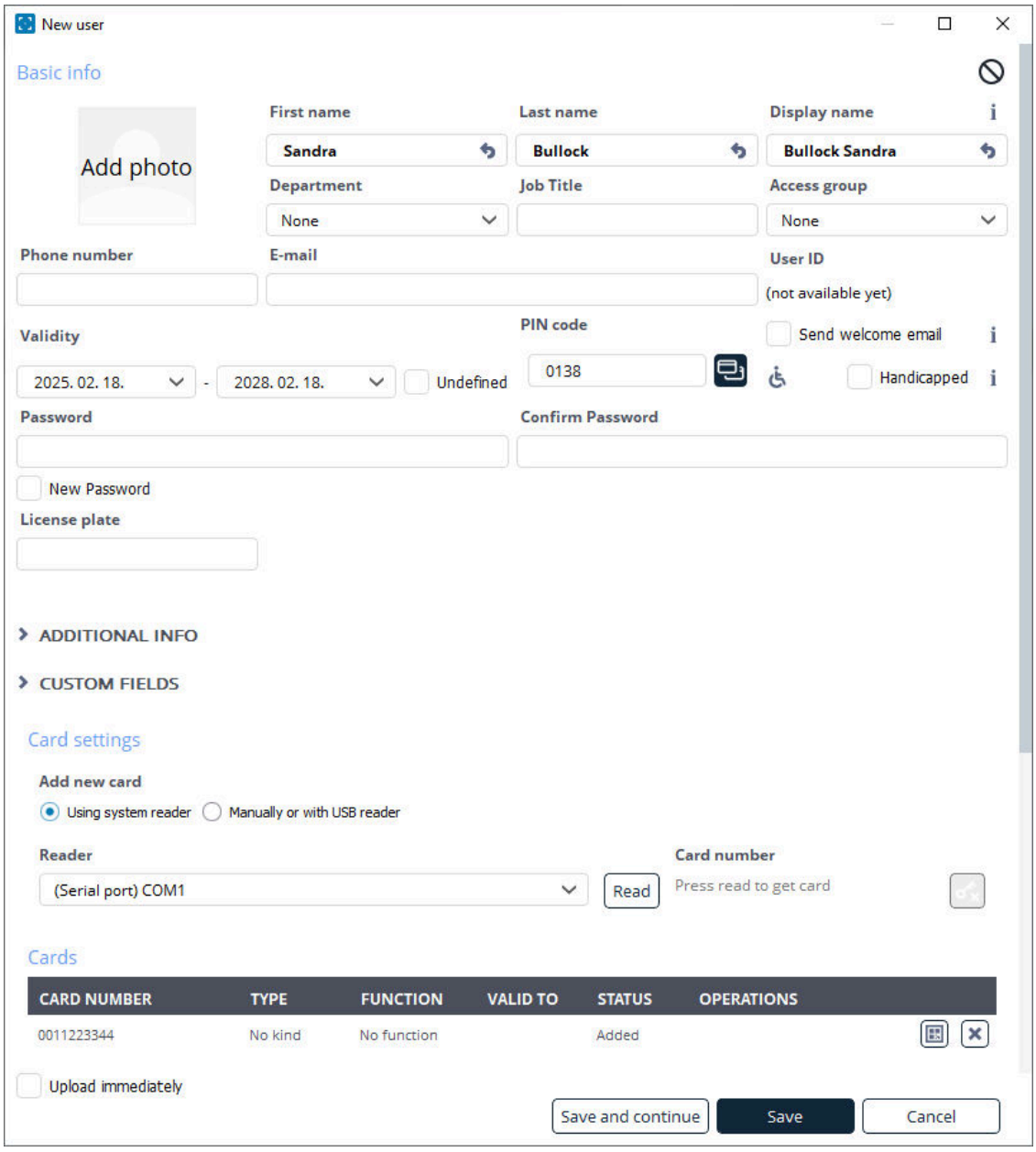


Figure 77: Adding a new user to the software

Use the **Add photo** button to upload or take a picture of the user. Previously uploaded pictures can also be changed or deleted here.

The **Validity** fields set the time period when the user is enabled in the access control system. The starting date is set to the creation date by default, but it can be changed. The ending date is either a fixed date or it can be undefined. The user's all identifiers are considered invalid outside this validity period.

The **PIN code** is used for authentication on the access control card readers if PIN code access is enabled, and for the personal work time web page. A 4 digit random code is automatically generated for every user upon creation. PIN codes can be modified by the user on the personal work time web page. PIN codes must consist of 4-8 digits.

The set **password** can be used when logging in to the personal web interface. When a user is created, the system will generate a password based on the specified scheme, which will be included in the welcome email. The password can be changed after activating the New password option.

After checking the **Send welcome email** option and saving the user, the system sends an email to the user (if the email address is set and the smtp settings are correctly configured) containing the user's name, PIN code, password and expiration date.

The **Handicapped** checkbox can be used to request the access control units to use longer opening times for the door locks for this user.

Click the **Addition info** text to uncover other extra fields which can be filled optionally for the user.

By clicking on **custom fields**, the custom fields added to the system can be attached to the user.

Cards and other identifiers for this user are managed here too. New card can be added by choosing a system reader, a USB card reader attached to the computer or manually typing in the card number, and you can also generate a QR code by clicking on the blue QR code generator button. The identifiers (cards, fingerprints) associated with this user are listed in the table titled **Cards**. Clicking on the email icon in the row of the identifier will send a QR code to the user's email address, and clicking on the QR code button will save the QR code associated with the card number as an image. The delete button can be used to unassign a card from the user, or in case of a fingerprint to delete it from the system (including all attached access control devices).

The certificates assigned to users can be managed in the **Certificates** section at the bottom of the window. To add a new certificate, the ID (optional), validity period and certificate type must be specified, and then it will be assigned to the user by pressing the + button. To delete a certificate, select the row of the certificate in the table and click on the Delete button in the menu bar below.

On the lower left corner, if the **Upload immediately** checkbox is activated, all changes

made in this window are automatically uploaded to the access controllers.

Users can be temporarily deactivated by clicking on the deactivate button on the upper right. Deactivated users can be activated with the button. A deactivated user's all identifiers are immediately invalidated, thus all access requests will be denied in the system.

The Save button saves all changes made to this user and closes the editor window while the **Save and continue** button saves all changes and opens a new editor window.

Deleting the users' is done at two levels in the system. The first level is the **marked for deletion**, which becomes available when you are in edit mode. To do this, you first click on the **edit** button, then select the users you want to delete and select the *mark user deleted* option in the bottom menu bar. Click on the yellow **save** button to save the changes. When using door controllers, this modification needs to be uploaded to them, before permanent deletion. Once the user(s) have been marked for deletion, they will be taken to the permanent deletion dialog window, which can be opened by clicking on the button marked **permanent deletion**. In the dialog box, you can select the users whose data is no longer needed in the system and click on the red **Delete** button to permanently delete them.



WARNING: If users are marked for deletion, they will no longer hold the quota included in the license, but their events and worktime reports can be viewed retrospectively.



WARNING: When using the worktime management module, the necessary corrections must be made before marking for deletion, because after that, the data cannot be modified!



WARNING: If users are permanently deleted, all data and events associated with them will be deleted from the database!

Users can be organized into departments and a complete department tree can be created. **Departments** can be added to the system by clicking on the **edit** button first and then clicking on the *+add department* button in the bottom menu bar of the Departments, in a tree structure. If no department is selected before adding a new department, it will create a new main department. If a department is selected and then the add button is clicked, a sub-department will be added. The users can be categorized by "drag and drop" method. To make changes, the edit button should be enabled first.

TIP: The users, the complete department tree, the access groups, user card numbers etc. can be imported from an Excel sheet with just one click.

Users can also be exported to an Excel sheet using the button.

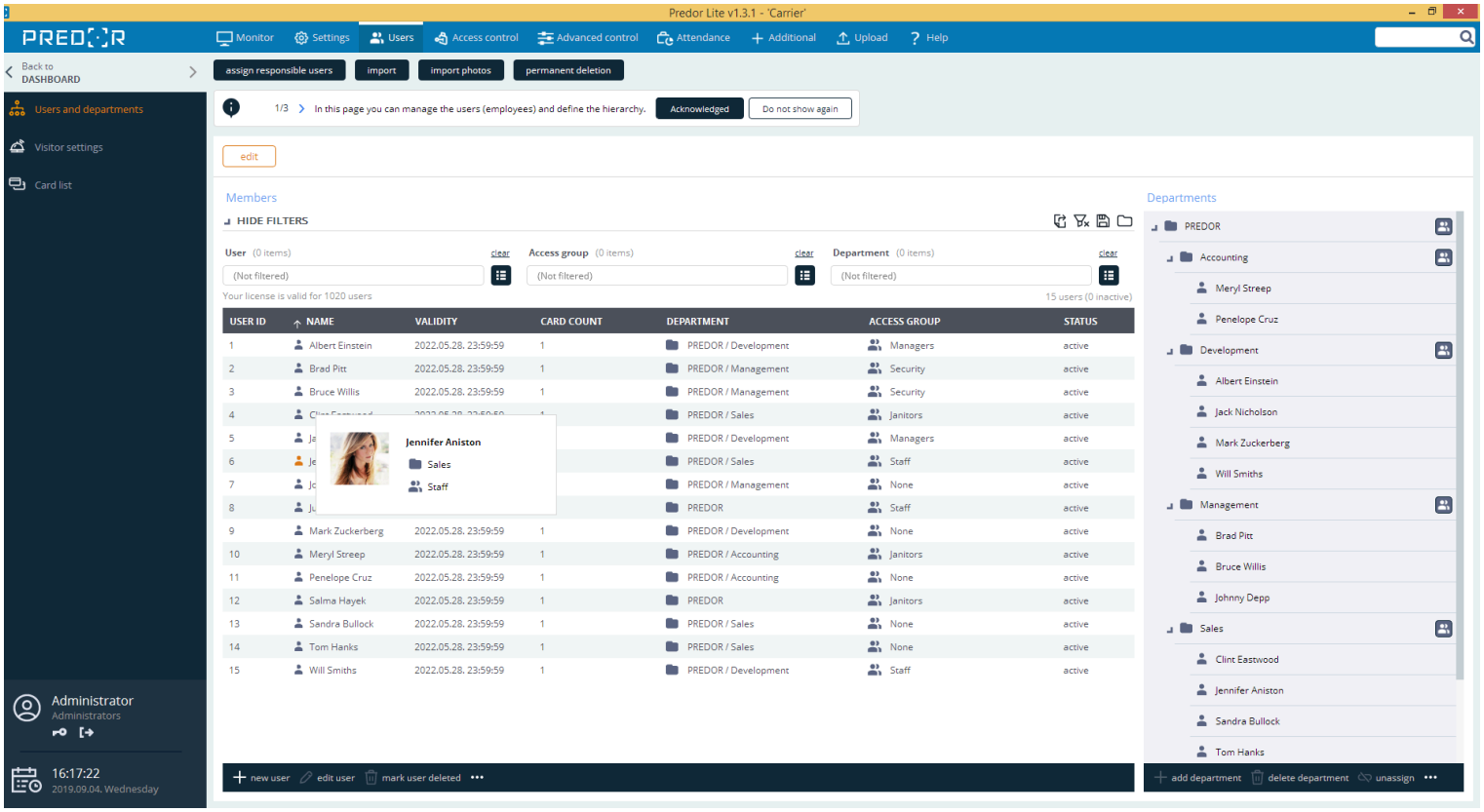


Figure 78: Users and departments view

The data can be filtered by name, department, or even access group.

To create a subdepartment, select the appropriate parent department, then click the new icon.

Responsible people can be specified for each department. The responsible managers can view the details of their subordinates on the **personal web interface**.

ATTENTION! Departments are used for grouping by organizational structure only. For grouping access rights, access groups are used instead.

TIP: Assigning cards for multiple users is faster if you select multiple users and use the "Assign cards" function via the *** button instead of editing users one by one.

Import photos: the name of the user's photo should be the same as the user's displayed name. Compress the photos into a ZIP file and simply browse it. The system will add the photos to users automatically.

Banned users: Users banned by the password cracking protection function are listed here. Bans can be lifted immediately by removing the users from this list.

Permanent (unrevocable) deletion: after marking selected users for permanent deletion the users' events can still be listed. The selected users are only added to a final deletion list which is displayed in this dialog window. If the deletion is confirmed here, **all movement events will be deleted with their personal data!**

CAUTION: **The user's personal data and movement events will be permanently deleted if you choose the final deletion!**

Department history: By editing a user's department transfer timing table ("history"), the transfer date from one department to another can be trimmed accurately even before or after the actual transfer in the Predor software. Worktime reports generated for departments use this timetable and therefore will show the correct results.

Custom fields: Custom fields can be configured in the dialog. The name and type can be defined freely, which can be added to users to record additional data.

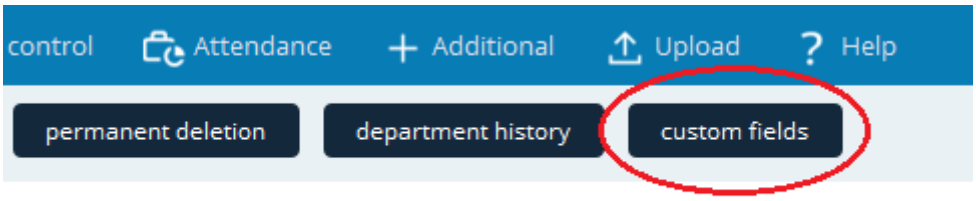


Figure 79: Custom fields button

Certificates

This menu item requires the **Manage Certificates** module. Certificates can be managed from this interface.

Certificate types: A new certificate type can be added to the system by clicking on the **+new** button below. Once added, it is required to enter the name of the certificate and then enter edit mode to configure the settings. The certificate type can be activated/deactivated by enabling/disabling the *Active* option. The default validity period is mandatory (1 year by default) and can be unlimited. The system can send an **expiration notification**, where the notification time can be set in relation to the expiration of the certificate and the persons to be notified *(Employees, Certificate type responsible users, Department responsible users)*. The persons in charge of the certificate type can be selected from the users in the **Responsible users** field. The access of users with expired certificates *(e.g. Medical fitness)* can be restricted for **Phantom controllers**. Readers can be selected from **Blocking readers** on which the restriction is applied. **Exceptions** can also be selected, who will not be affected by the access restriction. There may be different ways of restricting access:

- **Not preventing entry:**The system will allow/deny access according to the employee's privileges and does not take account of certificates.
- **Warning:**The system will warn that the employee's certificate has expired, but will not deny entry if eligible.
- **Preventing entry:** The system will deny entry for the employee if the certificate has expired.

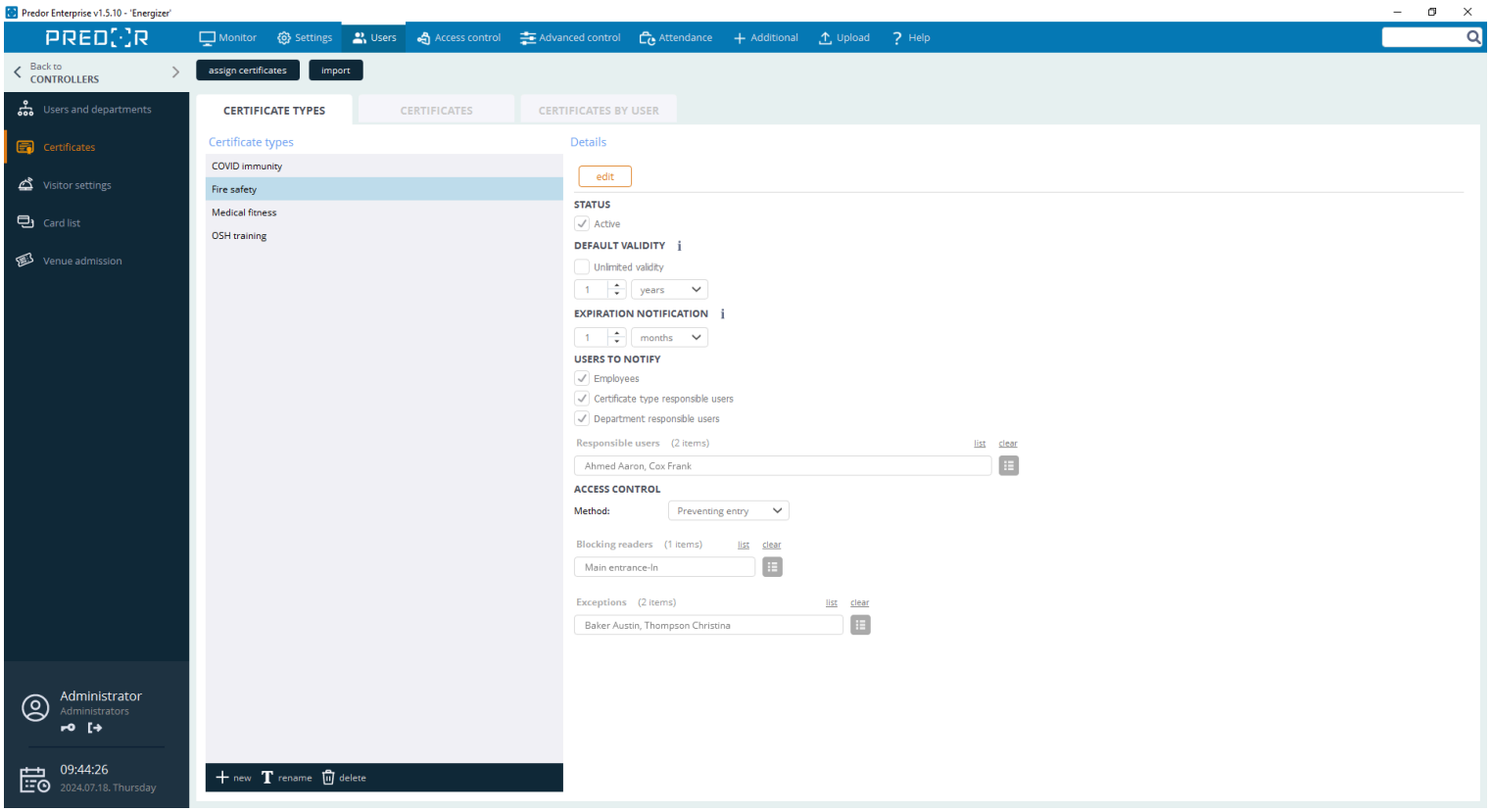


Figure 80: Certificate types

WARNING: The expiry date of the last valid certificate is always uploaded to the controllers. If there is a break between the validity periods *(For example: today is 2023.08.10., if one certificate has a validity period of 2022.08.22-2023.08.22. and the next one 2023.09.23-2024.09.23.)*, the end date of the first validity period is uploaded. The scheduler will upload the new expiration date at the next expiration start date *(2023.09.23. in the example)*, but if Predor is not running at that time (it is highly possible for Lite software) or the controller is not available, the new expiration date will not be uploaded, so in case of **Preventing entry mode** the employee's access will be denied by the system.

After the certificate types have been configured, they can be assigned to users. Clicking on the **assign certificates** button at the top of the page will open a dialog window where you can select the user(s), certificate type, validity period. When selecting one user, it is also possible to enter the certificate ID.

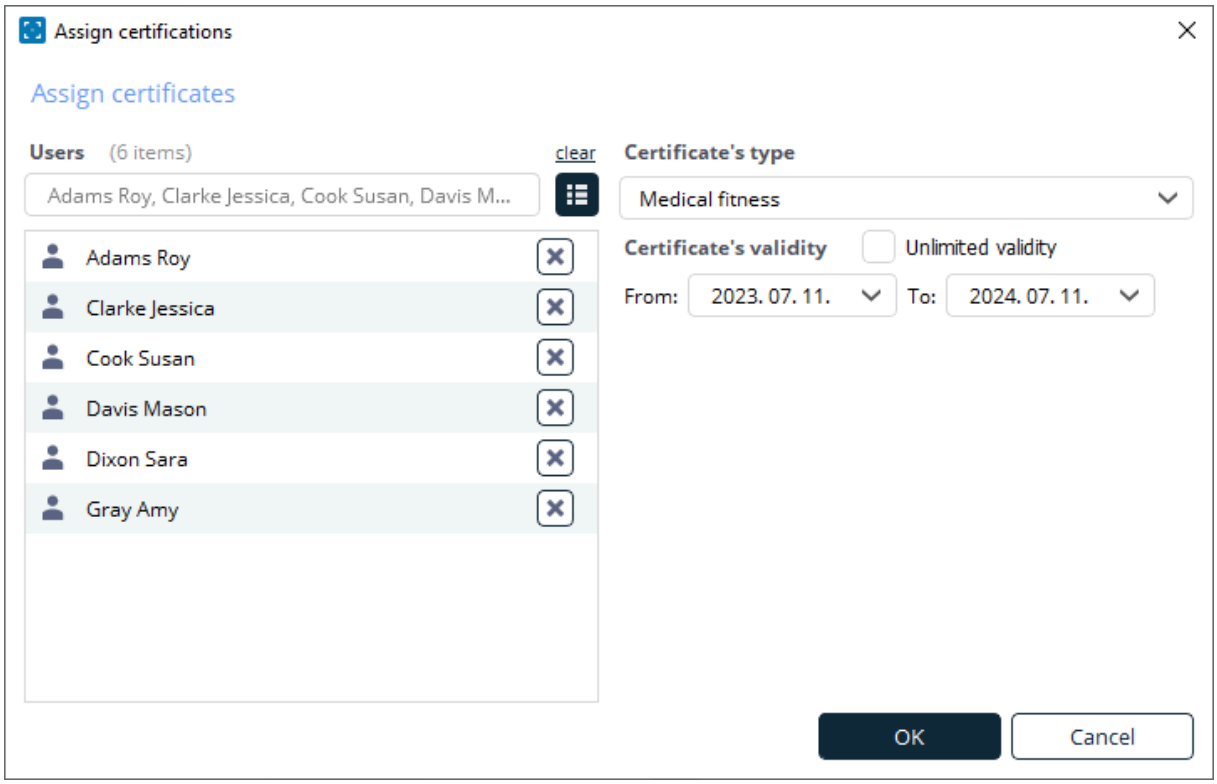


Figure 81: Assign certificates dialog

Within the **Users and Departments** menu, when adding a new user or editing an existing one, certificates can also be assigned to a user in the **Certificates** section at the bottom of the window by clicking on the + button after specifying the certificate ID (optional), expiry

date and type.

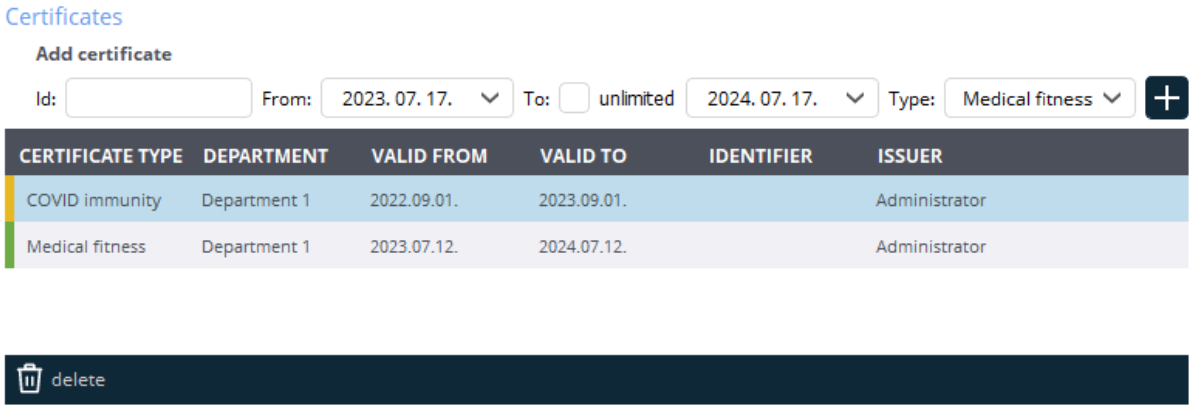


Figure 82: Assigning certificates in edit user dialog

It is also possible to import **certificates** from an Excel file. This import file must contain the name of the users, the certificate type and the validity period.



TIP: Before creating an import file, it is suggested to create a sample export of the certificate list, to which the necessary data can be added and then imported into the software.

Certificates: This tab lists the certificates assigned to all users in different colors:

- **Green:** the expiry date of the certificate will be more than 90 days later
- **Yellow/orange:** the certificate will expire soon (within 90 days)
- **Red:** the certificate has expired

Different filters can be applied to the list. It is also possible to apply quick filters by clicking on the *Valid only, Expired only* or *Expires soon* buttons. Using the Expires soon quick filter, certificates that expire within 90 days can be listed. The list can be exported to an Excel file by clicking on the  button above the filters. Certificates can be deleted by selecting the relevant row and clicking the Delete button in the menu bar below.

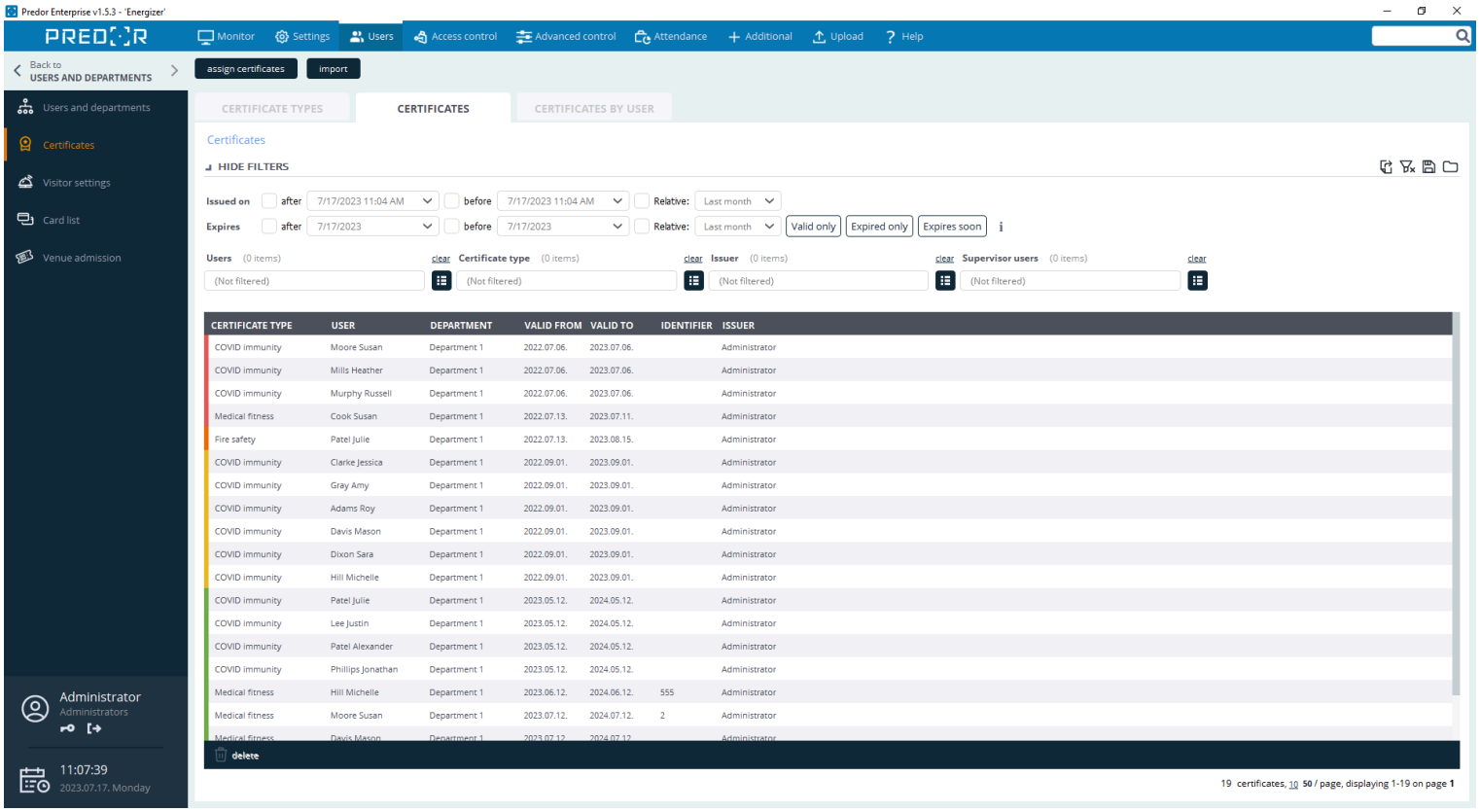


Figure 83: List of certificates

Certificates can also be listed by users. In the table, next to the name of the user, their department is displayed, as well as the name and expiration date of the certificates assigned to them. Filters can also be applied to the table. Filtering by certificate type makes the *Show users who not own selected certificates* option available, which can be used to list users without certificates. Clicking on the pencil icon to the right of the table rows will open the Edit User dialog, where the certificates assigned to the user can be added/deleted.

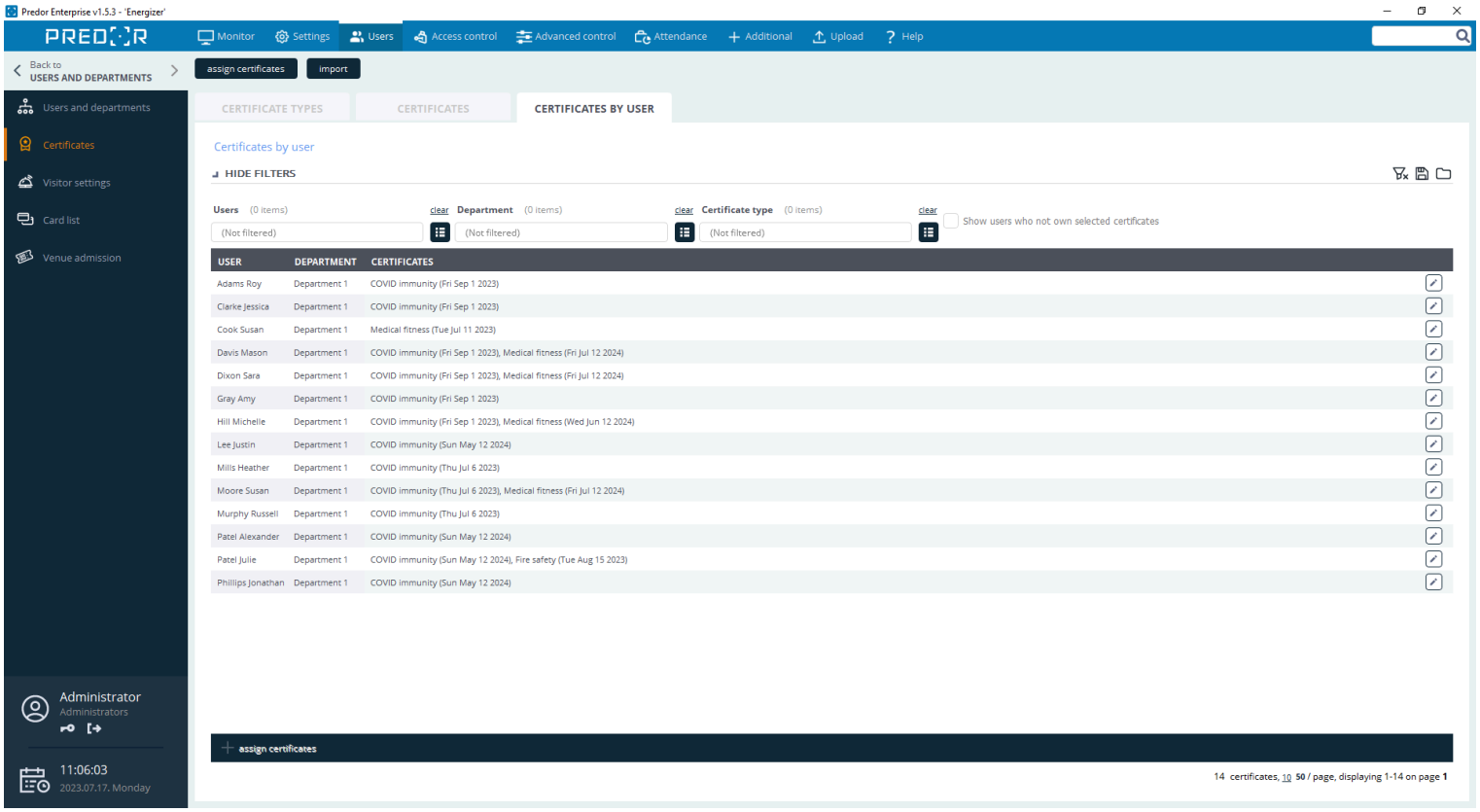


Figure 84: List of certificates by users

Users can see the certificates assigned to them by logging into the **web interface**. When logged in as a department responsible user, the certificates of the employees belonging to the department are listed under Certificates menu. When logged in as a certificate responsible user, the certificates belonging to them are listed here. This feature requires the **Working time web** license.

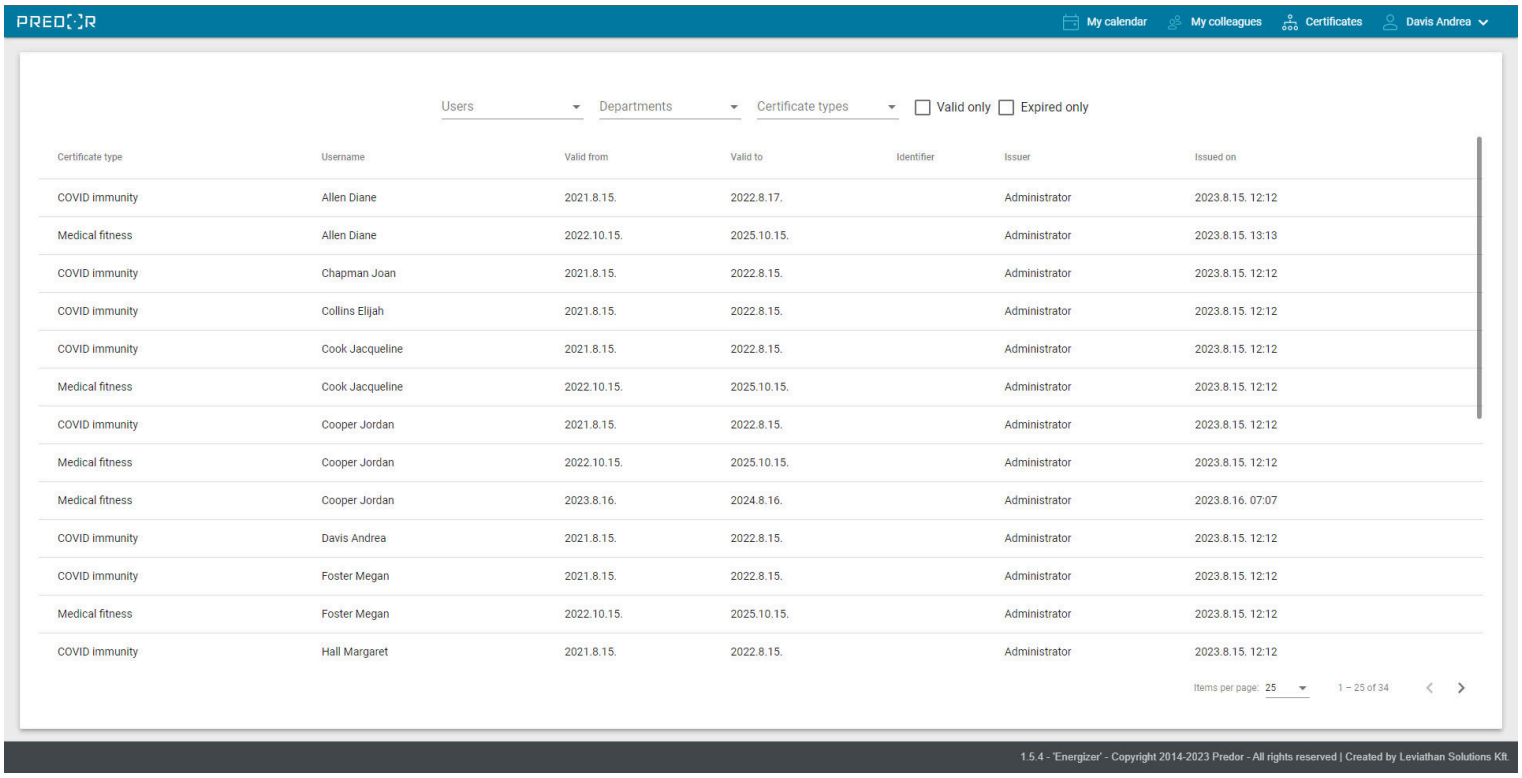


Figure 85: List of certificates on web interface

Visitor settings

Visitors are handled differently than normal users in the system. Visitors cannot have unique access rights, instead visitor types need to be created to determine the access rights and time ranges for them. The visitor type can be considered as an access group for visitors. Click the *manage companies* button to add and edit companies where you expect guests from. To publish cards, go to Monitor menu and use the Publish cards. It's possible to activate a guest without a card, then they can enter with a PIN code or a registration number. Visitors are excluded from work time and attendance management.

After creating visitor types visitors can be added to the system on the Publish card submenu where they can be assigned to a visitor type which define their access rights.

A validity time range should be specified for each type. Each published credential will be valid for this time period.

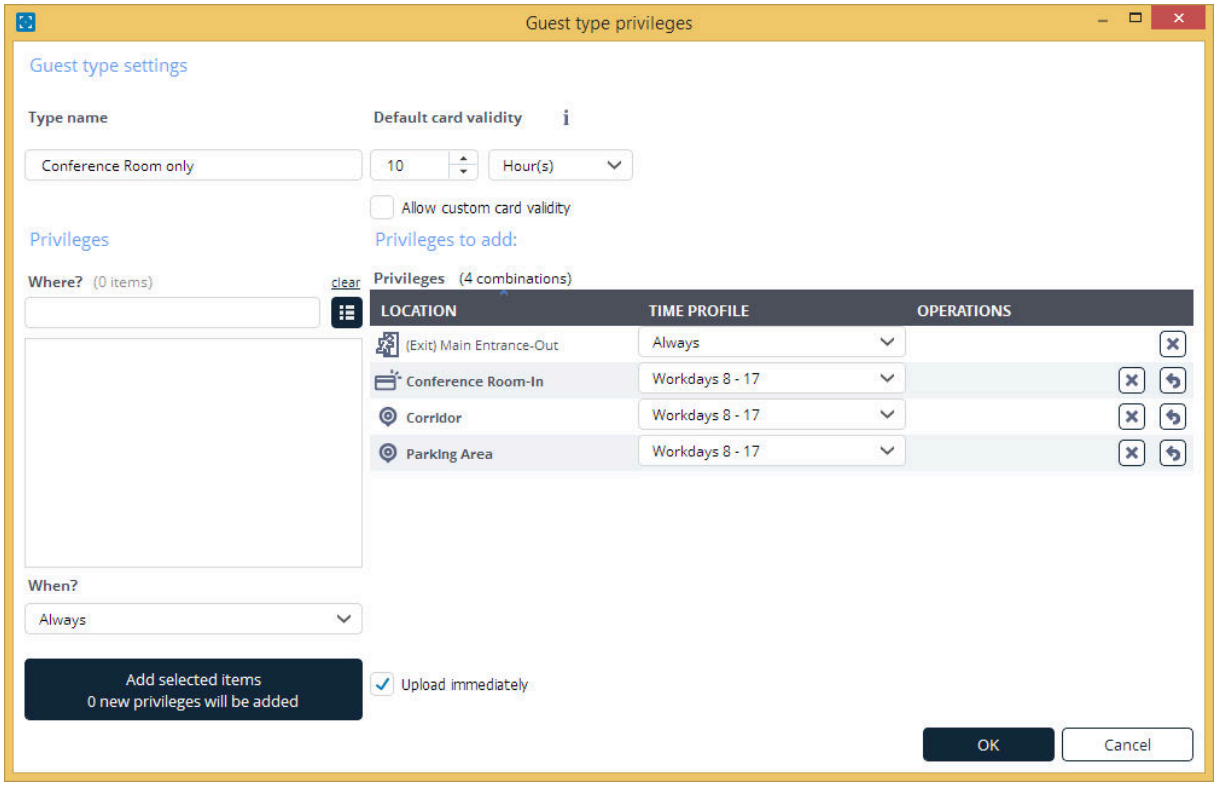


Figure 86: Configuring visitor type privileges

If the *Visitors and season tickets* module is purchased, then visitor types can be defined as season tickets. Season tickets may have a validity limit extended indefinitely, and they feature an entry limit. By defining a visitor type as season ticket, a new tab becomes available in the visitor type settings dialog where the entry limits, and the readers that decrease the remaining entry count can be set.

WARNING: Season tickets are only available in the Predor Enterprise system! The *Visitors and season tickets* for Predor Lite only grants the extended validity and visitor limit.

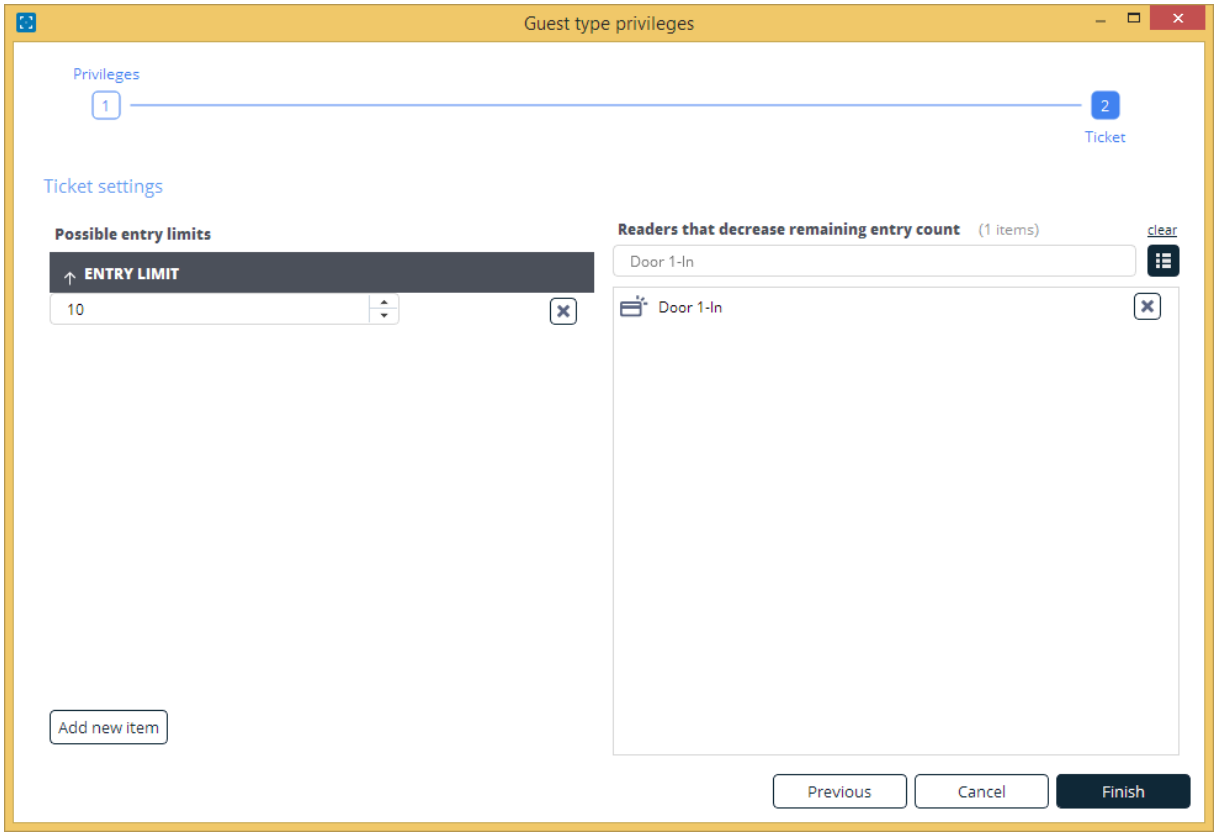


Figure 87: Guest type additional settings when defined as season ticket

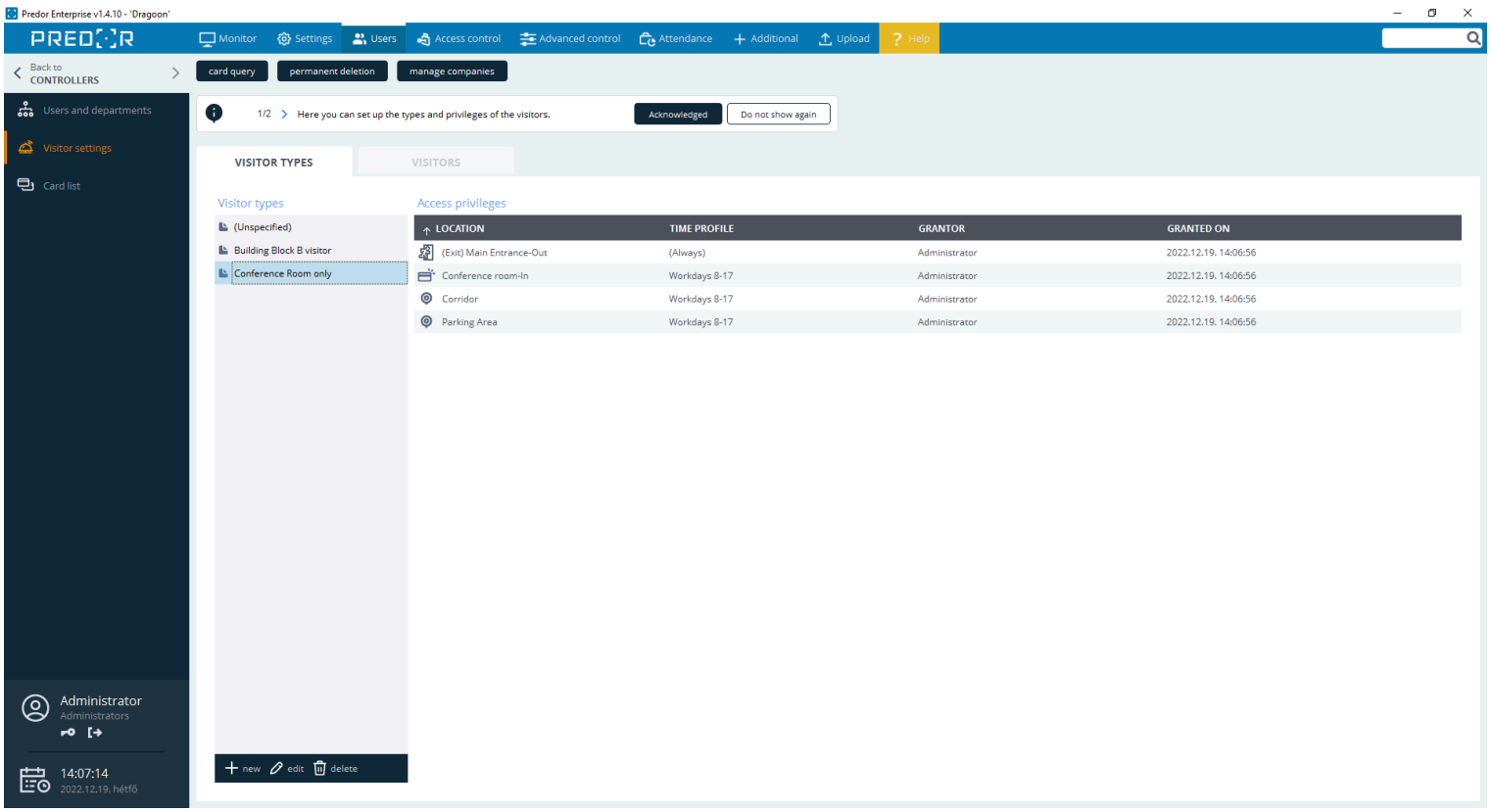


Figure 88: Visitor types summary view

Card list

The registered cards of the system can be viewed in this view, and the list can be short-listed by detailed filters.

Card query button: Shows information about cards presented on a selected USB or system reader. If the "Visitors and season tickets" module is used, then additional information appear here if the card is a season ticket: remaining entry count, and past entry dates.

Card History: this view provides information about the history of the card. You can check the issue date, the former owners or the operator who has issued the card.

Lost cards: if a user has lost his or her card, the badge must be marked as lost. If an unauthorized person tries to enter with a lost card, the system will generate an alert event.

Deactivation: the cards can be quickly and easily deactivated if it's needed. Deactivated cards can be activated any time just by a click.

Venue admission

This submenu is only available with **Venue admission** license. The QR code settings in the system can be configured through this interface. A new ticket configuration can be

added to the system by clicking on the **+new** button below. You can change the settings by entering edit mode (by clicking on the yellow edit button). Printing can also be started by a contact connected to the AUX input after the controller and AUX input have been selected. When configuring the ticket type, it is required to select the appropriate guest type, which can be added and configured under Visitor settings submenu. The language of the ticket (English/Hungarian) can be set, and **custom text** can be added. By selecting the supervisor persons (operators/users), you can specify who is allowed to print the ticket type. Additional data can be displayed on the tickets, which can be: *Custom text, Entry number, Guest type, Serial number, Valid from, Valid to*. Automatic guest deletion can be configured after clicking **guest deletion** button on the top. In the window that appears, it is possible to select which visitors should be deleted *(Visitor status expired, Visitor is inactive, Visitor depleted all tries)*, at the starting point. Furthermore, the frequency can be configured.

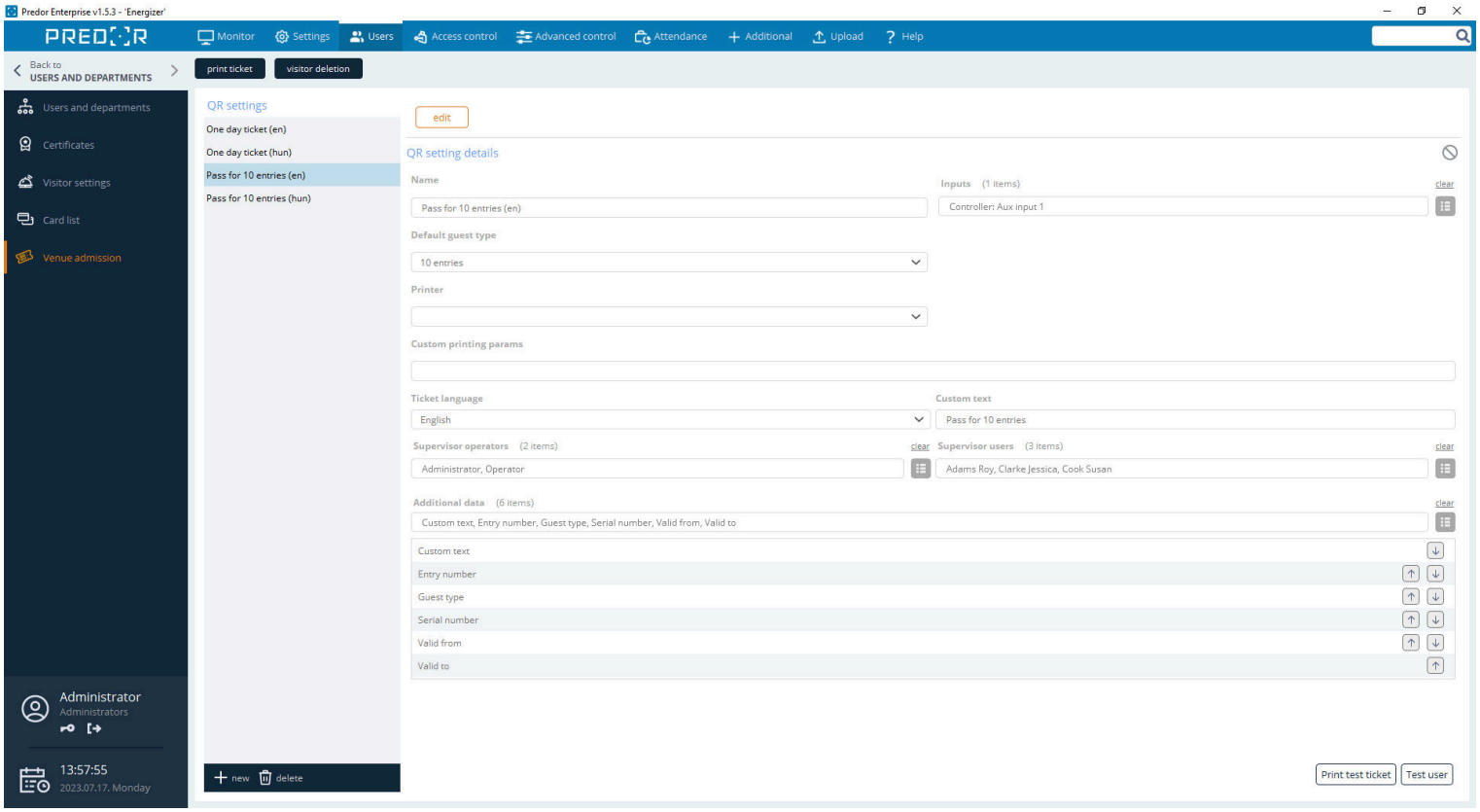


Figure 89: Venue admission

After selecting the printer, you can also enter specific printing parameters if there are problems during printing. When printing over network, a typical problem is that the print message needs to be modified, this field can be used for this purpose. The following keys can be entered (without quotes), separated by ";" if necessary:

- PREPEND - this changes the prefix of the code sent to the printer. By default "PREPEND=P${", which is added by network printing to the parameters sent, it is recommended to replace it with an empty string: "PREPEND="

- APPEND - this changes the suffix of the code sent to the printer. By default, "APPEND=}$", which is added by the network printer to the parameters sent, and should be replaced by an empty string: "APPEND="
- REPLACE_FROM - REPLACE_TO - can be used in pairs if you want to replace certain expressions with others. It can be useful if the client and server are running on different operating systems and you need to swap end-of-line characters, for example. Their default values are: "REPLACE_FROM=\n; REPLACE _TO=\r\n"
- DATATYPE - this tells the printer what format the code is sent in, this can be false and the ZPL code describing the QR code will appear on the printed label, not the QR code. Default value: "DATATYPE=TEXT"

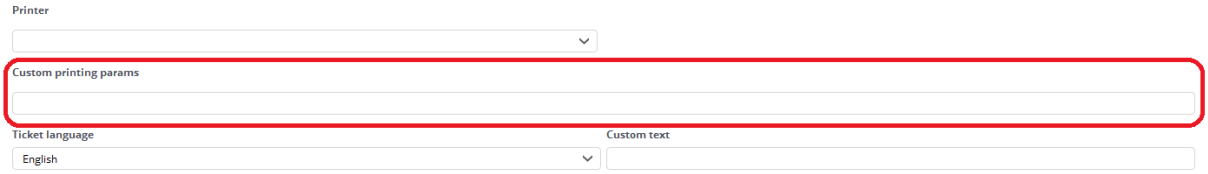


Figure 90: Custom printing parameters field

Within the client software, clicking on the **print ticket** button will open a dialog window where the **supervisor operators** can print their assigned ticket types by clicking on the **print ticket** button located inside the tile of the ticket type. After pressing the button, a pop-up window will appear to confirm the printing of the ticket to avoid misprinting. By selecting the **skip confirmation** option, the system will print the ticket without further confirmation.

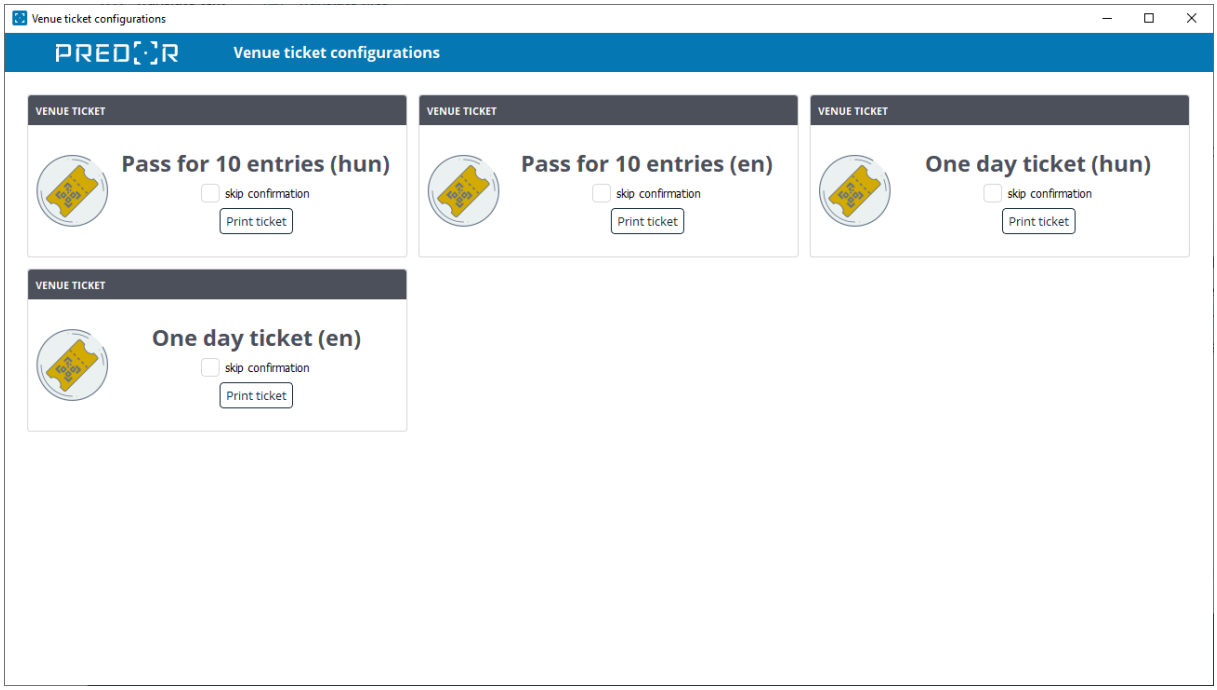


Figure 91: Ticket printing from client software

The **supervisor users** can login to web interface with user ID and PIN. On this interface, the corresponding ticket types can be printed under the **Venue admission** menu. To use this feature, the **Worktime web** license is required.

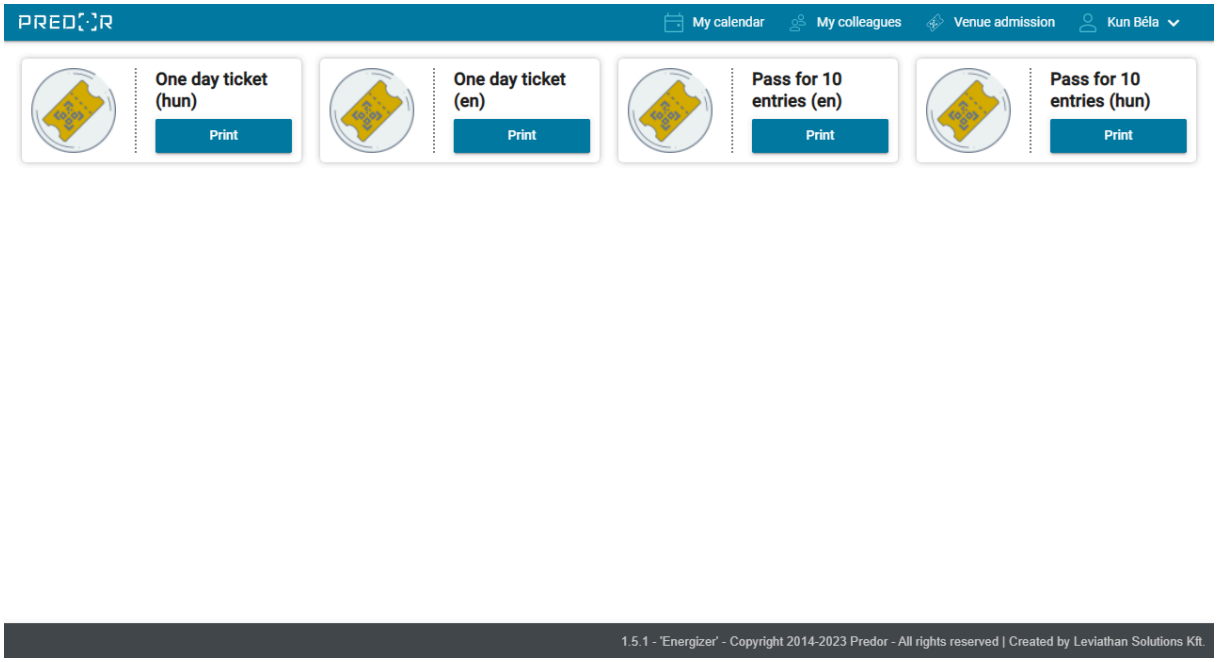


Figure 92: Ticket printing from web

When adding guests, in addition to sending a welcome email, it is possible to generate

a QR code and send it in the welcome email. With this QR code they can have access to doors, which have QR code readers.

Supported printers: Zebra GC420t

8 ACCESS CONTROL SETTINGS

Access groups

Up to 255 access groups can be created. Each group function as an access level. Before setting the access rights, it is advisable to specify the members of the access groups. If you change the access group of a certain user, its access rights also will be changed immediately.

Click on each group to list all members of the group.

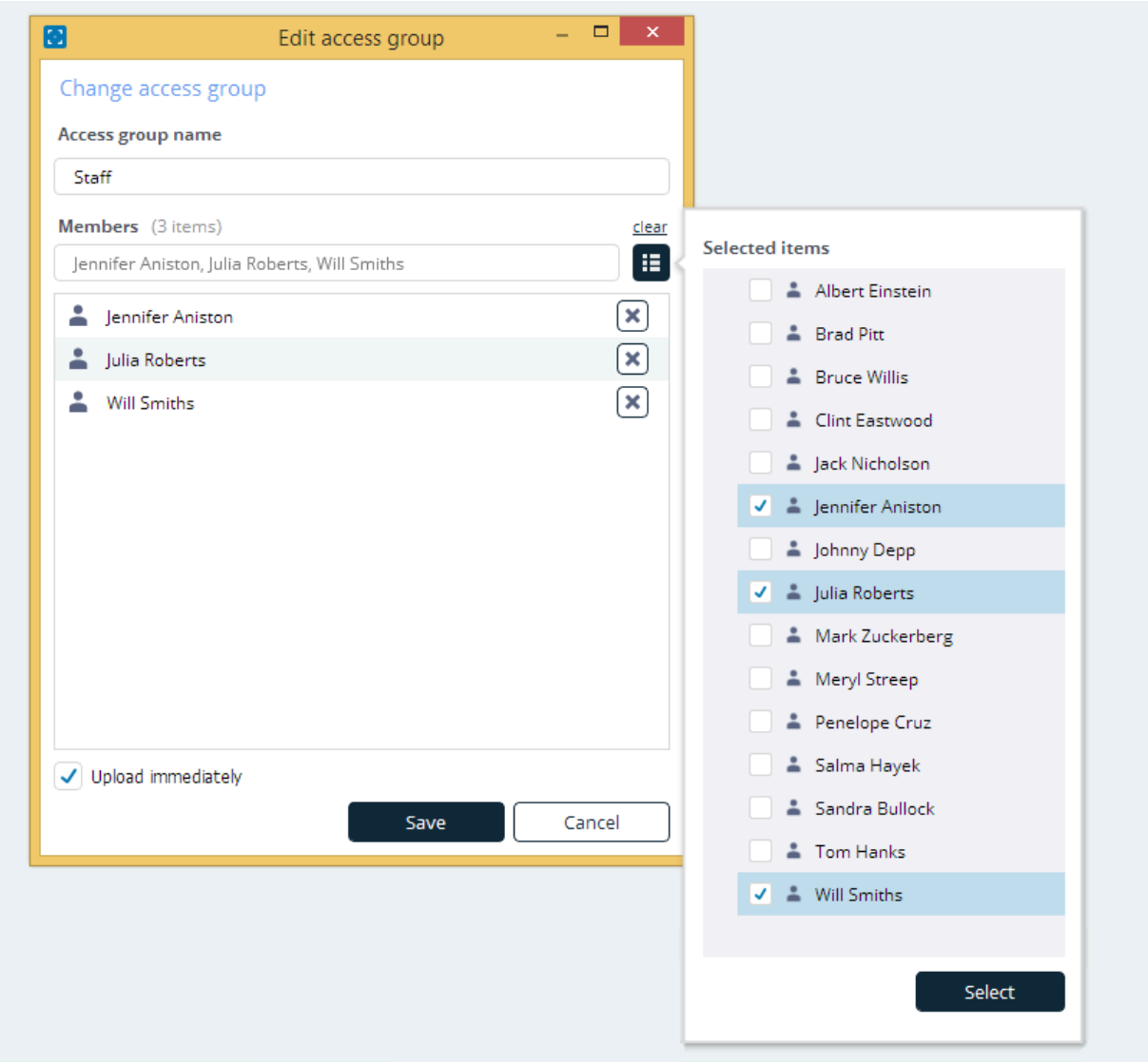


Figure 93: Editing an access group

Access zones

The configuration and management of the system can be simplified by dividing the managed object into zones. Individual rules can be set for each zone. The individual zones consist of readers that form connected areas. A zone cannot contain another zone. Therefore a certain reader cannot be for instance, the entrance of more than one zone at the same time.

Configuring zones: first you need to add and name system zones. In the configuration dialog window you should determine the borders of the zones. A gateway can be between two zones or – as an internal door – inside a certain zone. This way, each zone consist of system readers.

Protected zones: zones can be made protected during the zone configuration. It can be done by selecting the zone and then clicking on the ••• below and selecting “Protected”. One of the advantages of the protected zone is that in the operator privileges settings, it is possible to decide whether the doors leading to the zone can be opened remotely. The other is that if a user tries to leave a protected zone without the right to enter it (this means that he is in the protected zone without authorization), we will receive a “**Protected zone violation**” type alert in our system.

Entrances / Exits: Entrances and exits determine the boundaries of the protected object. Defining entry and exit gateways is essential for the correct location data and for work time tracking as well.

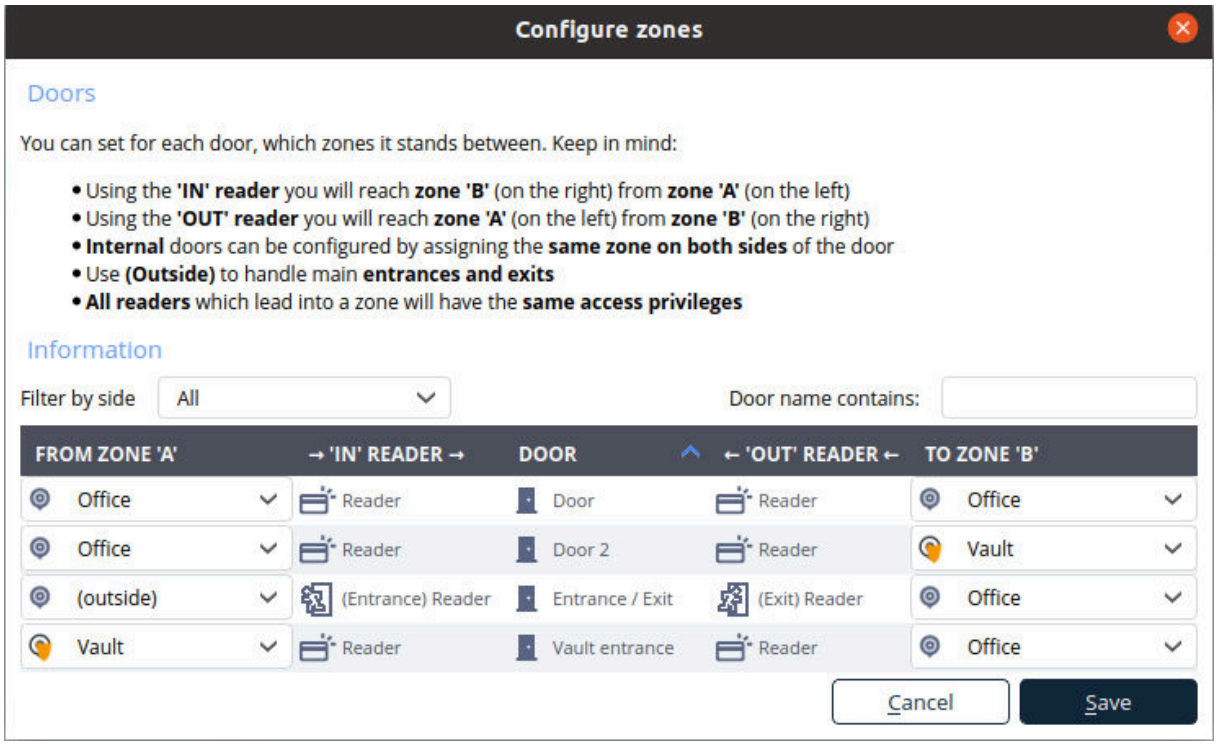


Figure 94: Configuring access zones

Time profiles

By creating time profiles, you can configure the time periods, when the users are allowed to pass through certain gateways. The time profiles created here can be assigned to users or access groups.

Up to 5 time ranges (intervals) can be defined each day, when access is permitted. One or more days posessing the same rules make up a timeline. To add a new time range, click on the + button on the right side at the bottom of the window after specifying the time interval. When different access conditions are needed on some days, an additional timeline is needed. The sum of all timelines is called a time profile.

In the Enterprise version each time range can be tied to an additional condition:

- **Always:** access is always granted in this time interval
- **Assigned to work:** access is granted only if the user required access in their assigned working time. Worktime is considered as the accepted timeframe in the worktime profile.
- **Not assigned to work:** access is granted only if the user presented their identifier outside of their assigned working time.

Access control units need to communicate with the server frequently when using the worktime-assignment based access control function. If the communication fails – for example because of a network error – the default action can be chosen:

- **Fallback: Allow:** In case of a communication error, the ACU allows the access.
- **Fallback: Deny:** In case of a communication error, the ACU denies the access.

New Profile: in the new profile dialog you can create and configure time profiles. Enter the name of the profile, and choose the days of the week the profile will be applied. Then set the time periods on the timeline you in which the entry is allowed. Different timelines can be created for different days.

Clone: If you are to create a new profile which is similar to an existing time profile, select the existing profile and click on the ••• below and select “Clone”. This way you can copy the settings and only the differences must be set.

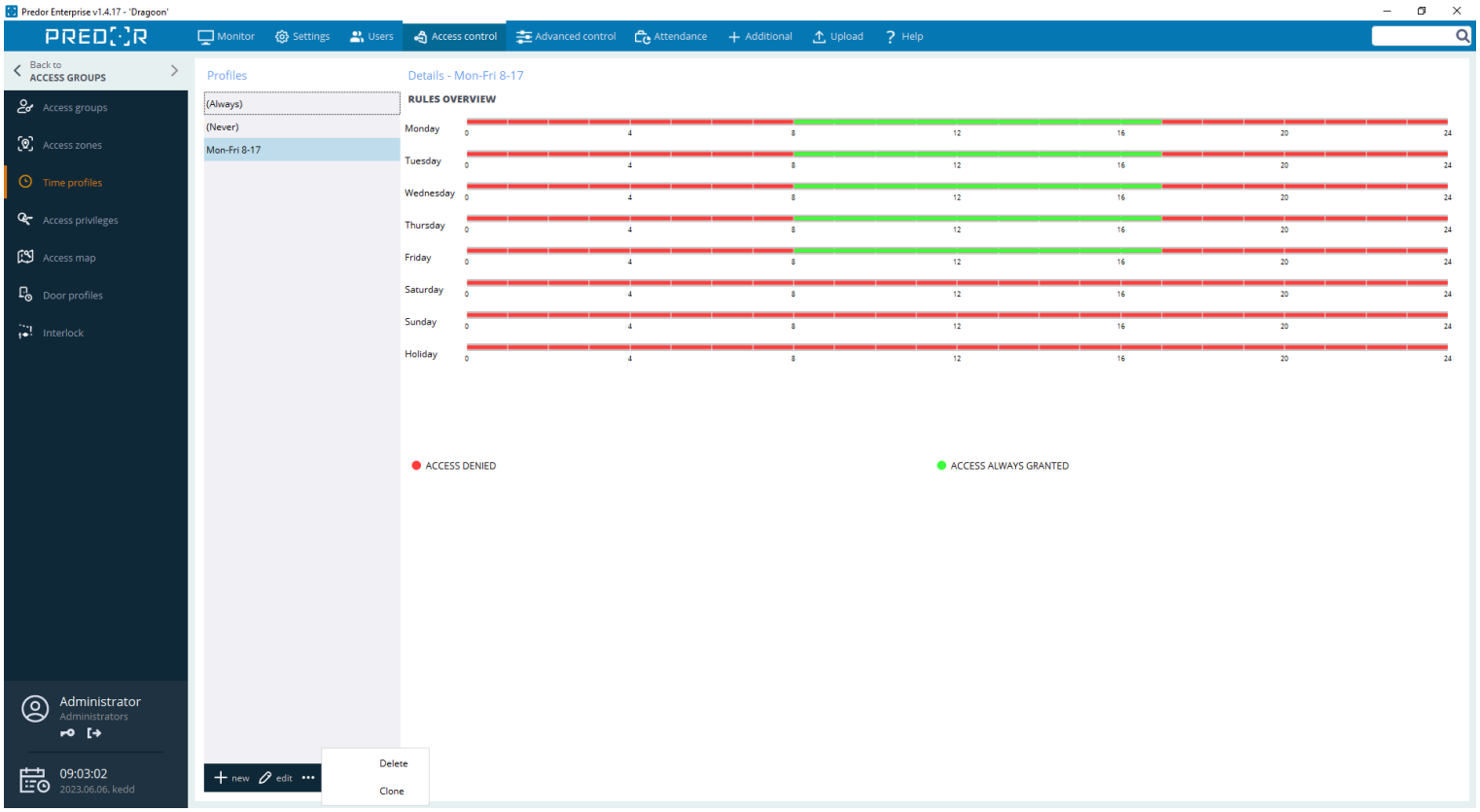


Figure 95: Time profiles summary view

Access privileges

The access rights are assigned to users, not to cards. A user may have several access credentials.

In the “add privileges” dialog window you can set the access rights.

Who?: Select the appropriate users or access groups in the window and click on the Select button.

Where?: Use the same method to select the readers or zones where you wish to grant access.

When?: Select the proper time profile from the drop-down list.

The “Add Selected Items” button turns yellow color to indicate that all required parameters are selected. You can apply the changes by clicking on this button, then click to save.

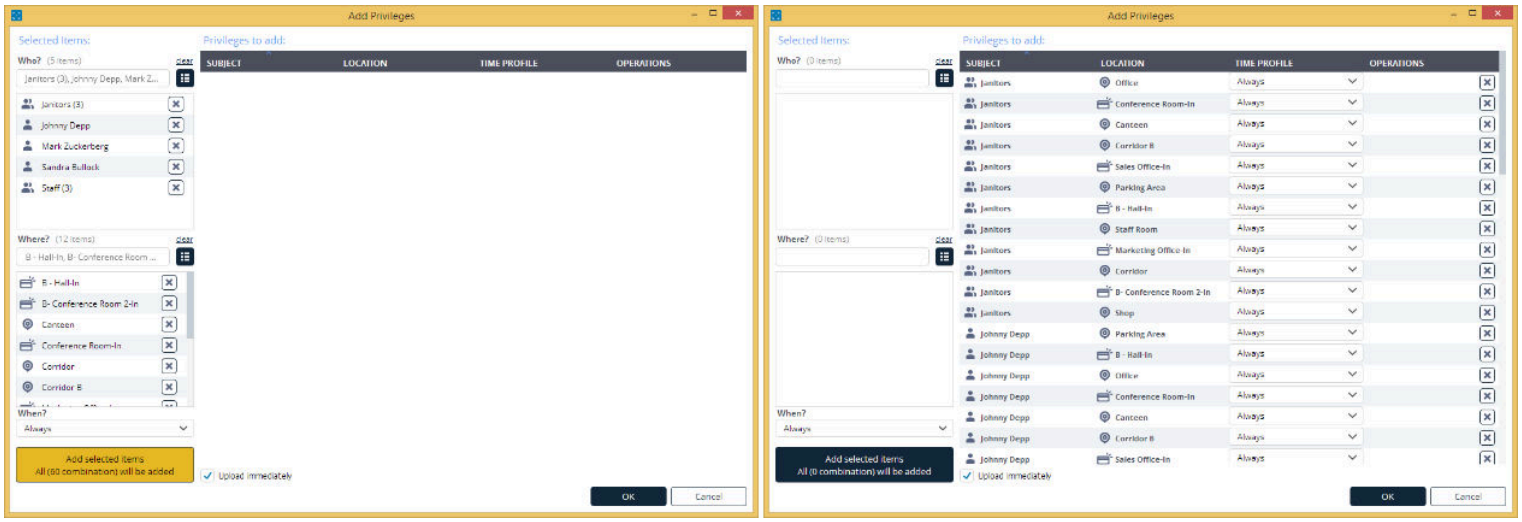


Figure 96: Adding new access privileges

This page also shows what permissions you have in the system, by clicking on the appropriate tab you can see the settings by subject or location. If you want to modify a privilege, clicking on the “change privileges” button will bring up a dialog box where you can edit the settings.

Access map

The access map allows you to quickly overview the access rights.

The columns of the table show the zones of the system and the readers that are not arranged in any zone.

The rows of the table show the access groups, the visitor types and the individual users.

In each cell can be seen the assigned time profile. So you can check that in which time period is allowed to the user to enter the given zone.



TIP: You can modify the time profiles just by a right click, if you change to edit mode first.

The access map can be opened in new window and also can be exported to Excel.

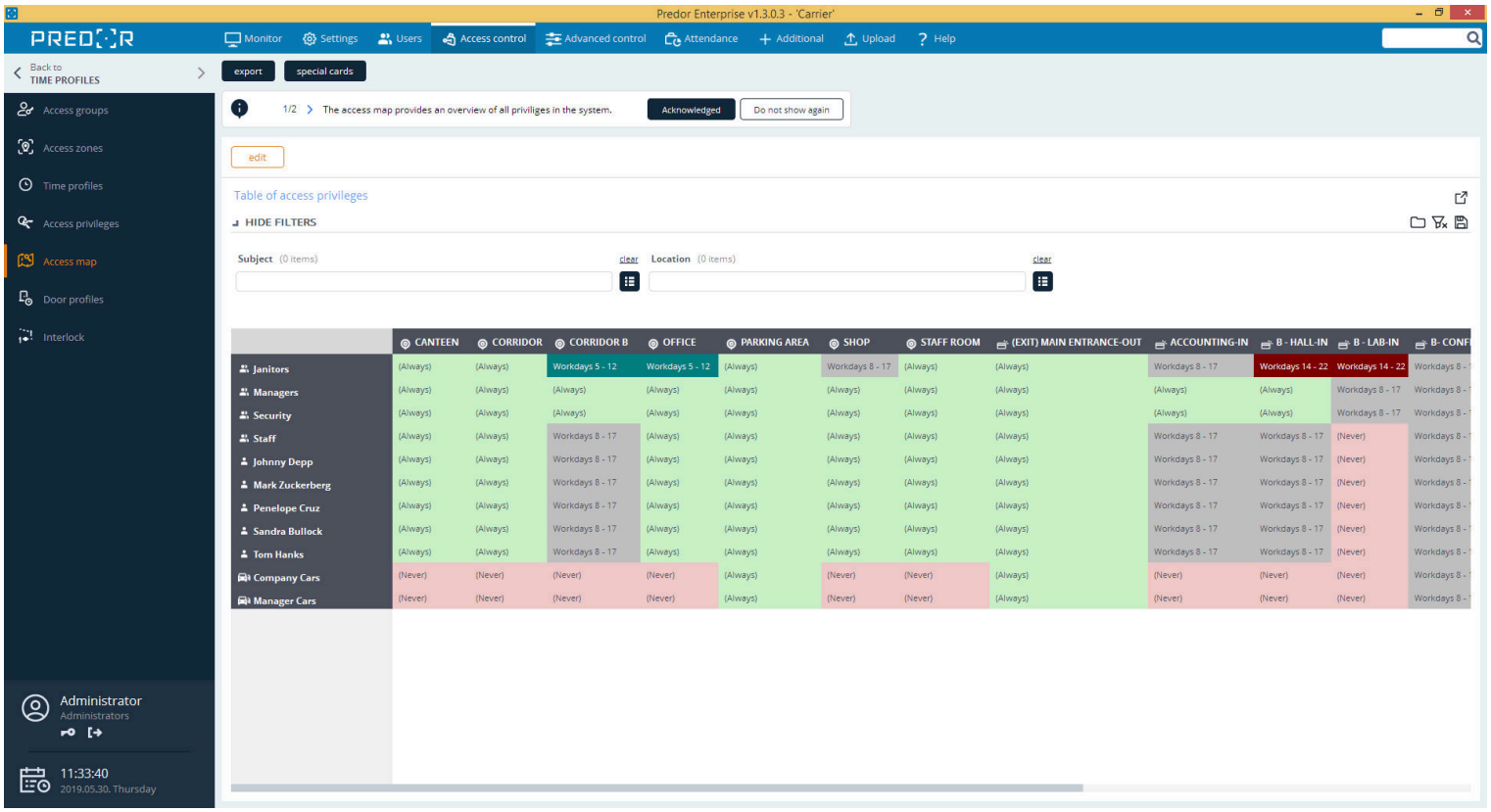


Figure 97: Access map view

Door profiles

Door operating modes can be configured. For instance, closed, open, only managers etc. You can create door profile if you determine time periods for the certain door operating modes. For instance, it can be useful if a door needs to opened or closed independently from access rights.

New profile: in the new profile dialog you can create door profiles. Enter the name of the profile, and choose the days of the week the profile will be applied. Then set the time ranges (intervals) and the operating modes on the timeline. To add a new time range, click on the + button on the right side at the bottom of the window after specifying the time interval. Different timelines can be created for different days. If the operating mode requires, the managers also must be determined.

Operating modes

Doors can be set to operate in the following modes:

- **Controlled:** the users can pass through who has the privileges to open the door
- **Open:** the door is open, anyone can enter to the area

- **Closed:** the door is closed, therefore no one can enter, even if the user has privilege to enter. The closed doors will open in case of emergency, for instance when the fire alarm goes off.
- **Only managers:** only users with managerial privileges can pass through the gateway. The manager users can be choosen in the assign profile window.
- **Only exit:** when the gateway is completely locked, there is a risk of someone being trapped in the room. In “only exit” mode the users cannot enter the area, but they are able to get out.
- **Manager->different modes:** the operation mode changes due to valid card reading of a manager. This way, a person with managerial rights can change the operating mode with his or her own badge without opening the software. The door retains it’s mode until the manager swipe happens.



EXAMPLE: If the door is configured as follows: 00:00-06:00 closed, 06:00-10:00 manager->controlled, 10:00-14:00 open, then between 06:00 and 10:00 the door is kept closed until the manager card swipe.

If the manager swipe their card, then between the time of the swipe and 10:00 the door is in controlled state, which means it only opens after presenting a valid card, but after 10:00 it switches to open mode, everyone is free to pass without a card.

If the manager card swipe does not happen between 06:00-10:00 then the door is kept closed until 10:00, then it immediately changes to open mode at 10:00.

Assign profile: each doorprofile can be assigned to any gateways. In addition, in the dialog window the profile time range and the manager users must be determined.

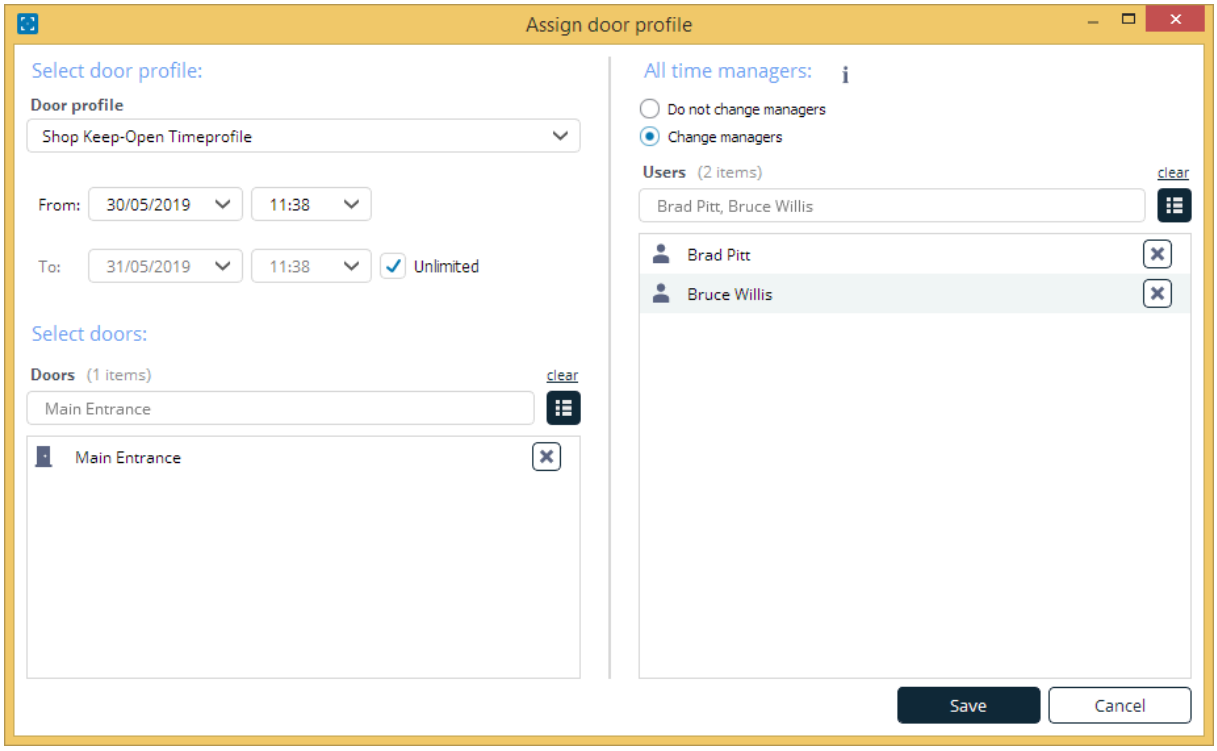


Figure 98: Assigning door profiles to doors

Clone: if you already set a time profile, the existing time profile settings can be copied. This way you just need to modify the different data.

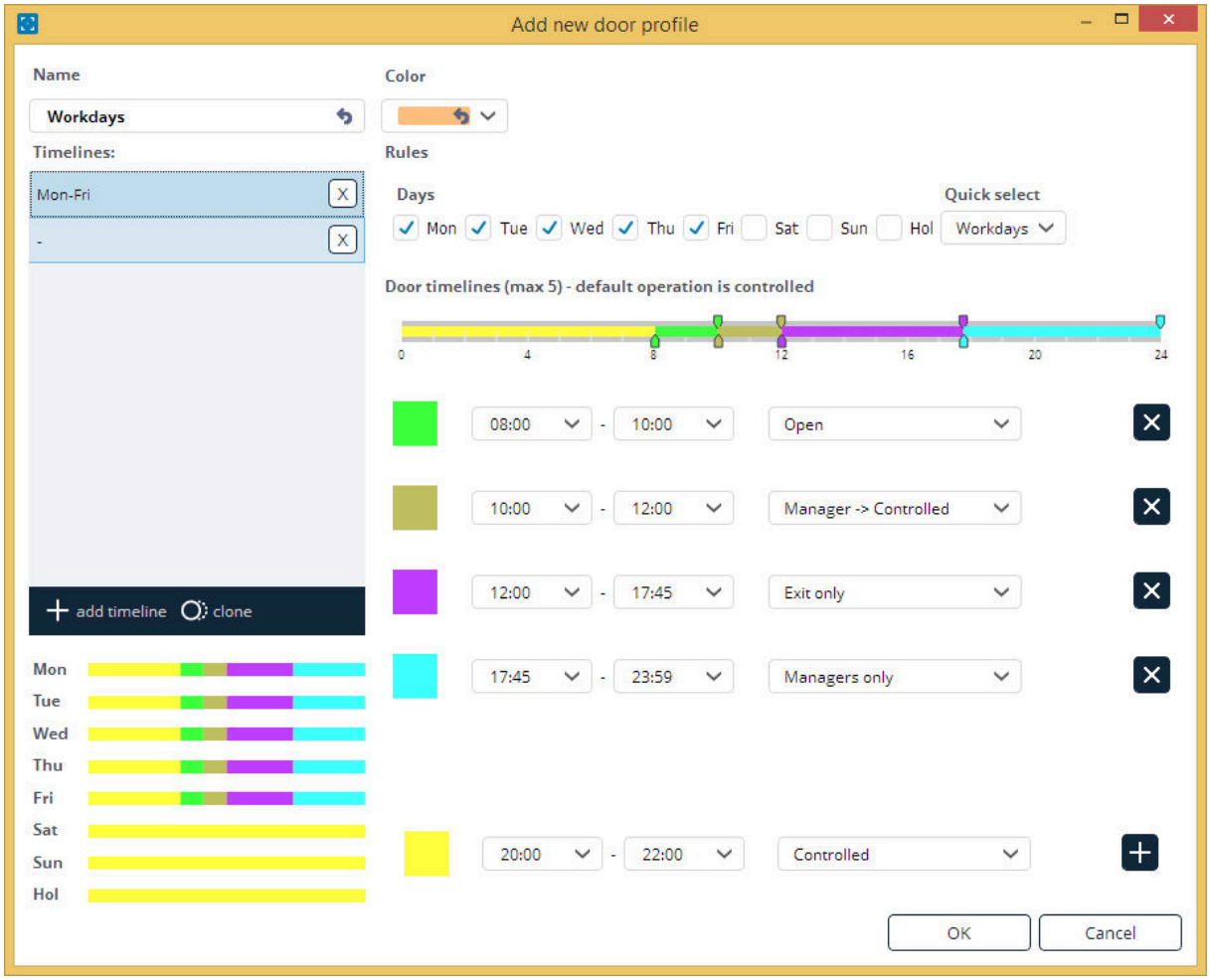


Figure 99: Edit door profile dialog

The Door Profiles tab lists the default and created doorprofiles. Clicking on them the preview can be seen. The color codes indicate which operating modes are active at which time range.

The doors tab shows the list of doors and the assigned profiles.

Profile History: you can see what profiles each door was operating on.



TIP: Operators can only change door profiles on any page which allows it, if they have full access to this submenu.

Interlock

Doors can be incorporated into interlock rules. Only one of these doors can be open concurrently. Doors working in this mode are usually located in the vicinity of each other, thus this function only works on doors connected to the same controller.

TIP: This function is particularly useful if used between partitions of a building where air pressure difference must be kept, for example a laboratory.

Settings

Creating a new interlock rule

1. step: Choose a controller
2. step: Click on the edit button
3. step: Click on the "**+** new" icon to create a new area. Select the doors for the interlock area, and name it.
4. step: Save the settings

This function can be temporarily disabled by clicking on the disable button.

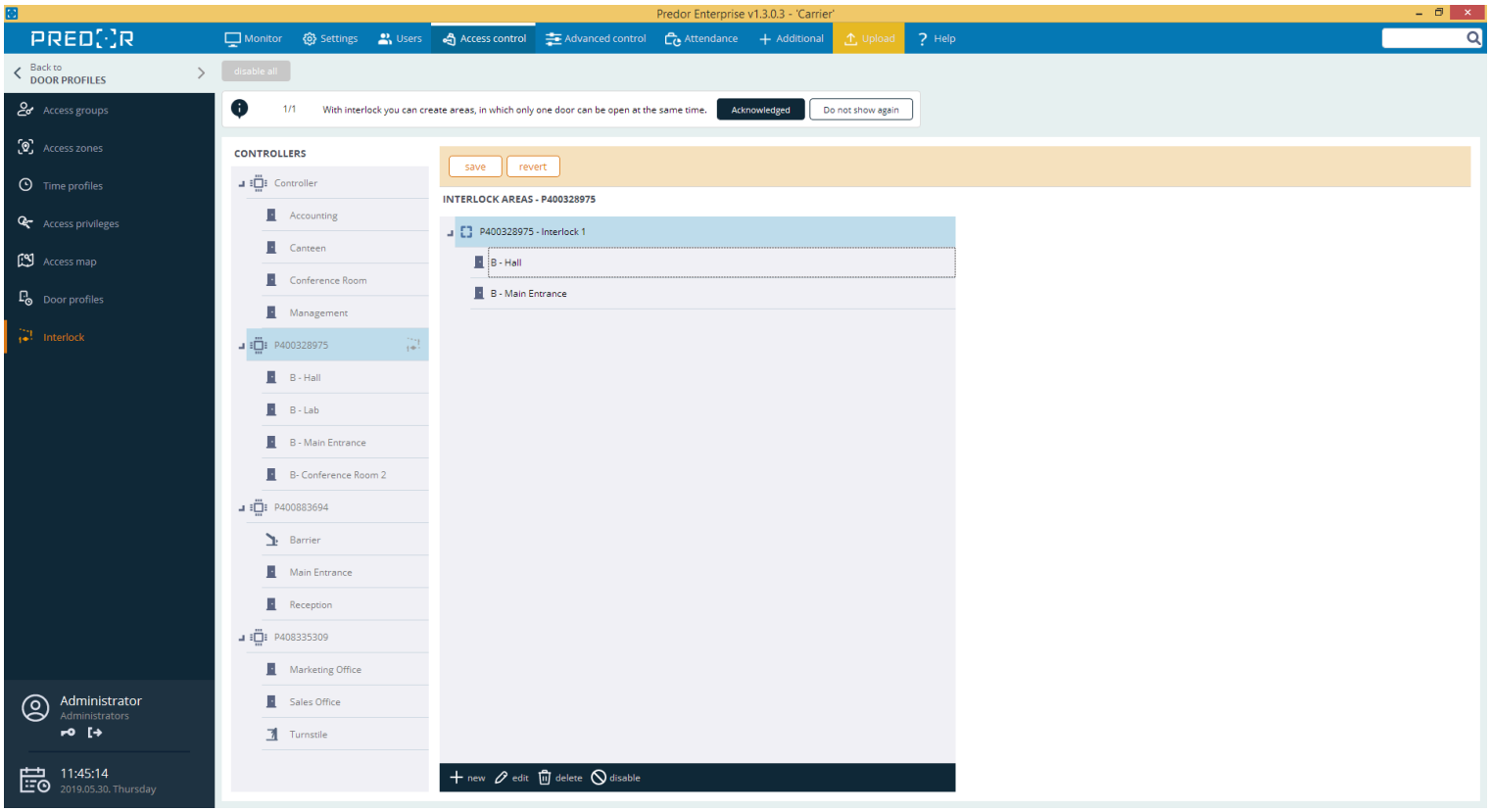


Figure 100: Setting up interlock rules

9 ADVANCED CONTROL MENU

Anti-passback

Anti-passback is used to enhance the security of an area or enforce that the users identify themselves every time before passign a gateway. If they neglect this we can even block their movement.

The **enable all**/**disable all** buttons on the top of the page allow/disable all of the rules with a single click. The **reset all** button can be used to reset the users' location data.

The feature is usable on a controller basis and globally too. With Lite software, only the controller based functions are available, otherwise found on the controllers tab.

Controller-level settings

The controller-level anti-passback function is implemented on the doors of a single controller, and the controller itself can manage it without server connection.

Anti-passback methods:

- **Log only:** the user can pass the gateway if they have the necessary access privilege, even if they did not identify themselves in the required checkpoint readers, but the system generates a warning or alert about breaking the anti-passback rules.
- **Block:** if a user with the necessary privilege neglected to identify themselves on the required checkpoints the system will refuse their entry. They cannot proceed without releasing the block first.
- **Hold up:** to encourage the compliance with the anti-passback rules, the system will hold up the offender for a given time, so for example for the next 2 minutes no gateway will open for them. This way, no furher action or constant monitoring necessary.

Alert on violation: when enabled, every anti-passback rule violation will generate an alert.

Creating new anti-passback area (on controller-level):

1. step: Select the controller
2. step: Press the edit button, then select the anti-passback method
3. step: Click on the new icon to create a new area. Fill in the name of the area and select the readers. IMPORTANT, that every area needs at least one IN and one OUT reader.

4. step: Select users and access groups as exceptions from the rule. They can still move freely.

5. step: **Prevent immediate returning:** this checkbox forbids the rapid in and out reads to **prevent using the same card repeatedly to let more that one person in.**

6. step: Save the changes.

The rule can temporarily disabled with the **“disable”** button.

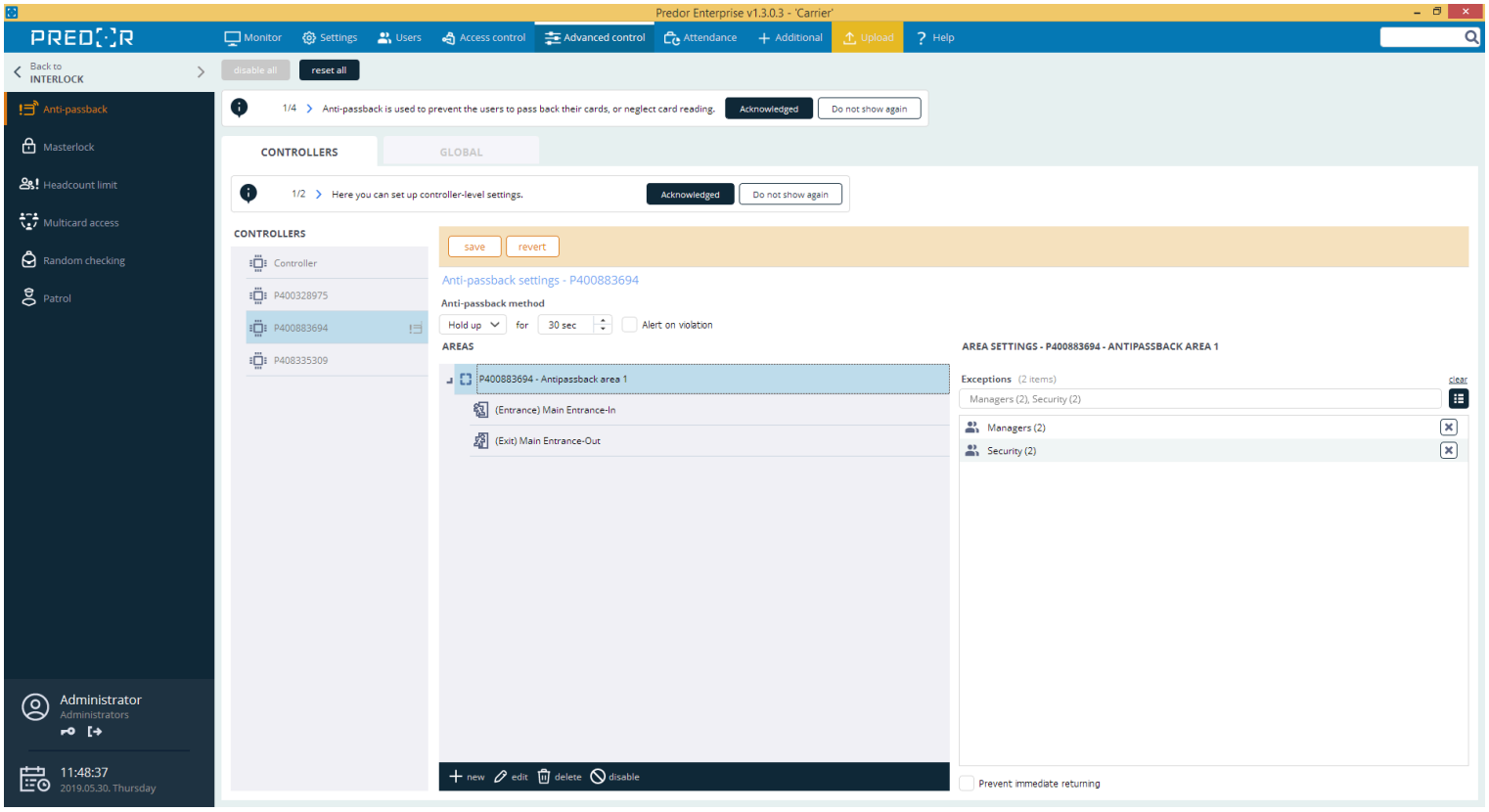


Figure 101: Configuring controller-level anti passback

Global settings

Global anti-passback requires Enterprise version, because the server facilitates communication with other controllers. **The anti-passback areas are built from access zones so these should be defined beforehand.**

Anti-passback method

- **Warning only:** the user can pass the gateway if they have the required access privilege, even if they did not identify themselves in the required checkpoint readers, but the system generates a warning or alert about breaking the anti-passback rules.

- **Block:** if a user with the necessary privilege neglected to identify themselves on the required checkpoints the system will refuse their entry. They cannot proceed without releasing the block first.
- **Hold up:** to encourage the compliance with the anti-passback rules, the system will hold up the offender for a given time, so for example for the next 2 minutes no gateway will open for them. This way, no furher action or constant monitoring necessary.

Alert on violation: when enabled, every anti-passback rule violation will generate an alert.

Anti-passback application:

- **Border only:** the rules are only enforced at the borders (in and out readers of the area) inside the area, everybody moves freely.
- **Full:** every passing inside and between zones requires identification

In the **exceptions** section, we can select access groups and users who are unaffected by APB rules.

Creating new anti-passback area (on global-level):

1. step: Press the edit button, then select the anti-passback method
2. step: Click on the new icon to create a new area. Fill in the name of the area.
3. step: Select the anti-passback application mode based on whether identification is required inside the area or only on the borders.
4. step: Select users and access groups as exceptions from the rule. They can still move freely.
5. step: Prevent immediate returning: this checkbox forbids the rapid in and out reads in order to prevent using the same card repeatedly to let more that one person in.
6. step: Save the changes.

The rule can temporarily disabled with the “disable” button.



EXAMPLE: We are not allowed to open door inside the building, unless we identified ourselves on main the entrance with a card read. After we did this, the border-only anti passback rules will no longer limit our movement while we are inside.

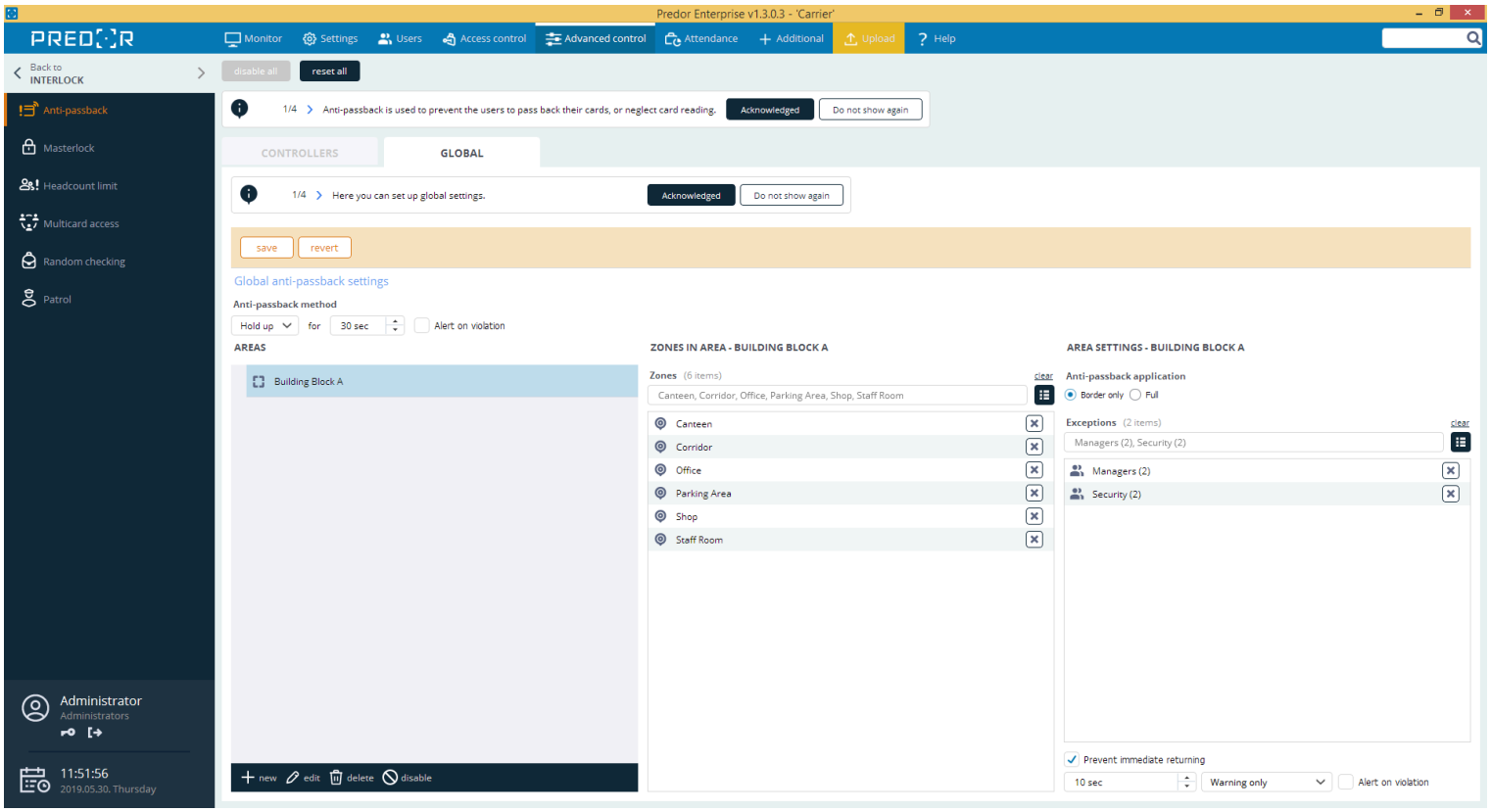


Figure 102: Configuring global anti passback

Masterlock

With the masterlock feature, areas of the system can be easily locked.

The “masters” of and area can unlock it on any reader of the area, or - with the necessary operator privileges - it can be easily deactivated from the client software.

The function can be activated on **card readers with a keypad** or by activating the corresponding **aux input by a contact**.

The activation (or deactivation) sequence is the following:

1. step: Press the number “0” then the “ENTER” (or“#”) button on the reader’s keypad.
2. step: The LED on the reader starts flashing
3. step: Swipe the mastercard on the reader

Settings

In the global settings, any access zone can form an area, while on the controller level, the area has to be built from the readers on a single controller.

Controller-level settings

The controller-level masterlock function is implemented on the readers of a single controller, and the controller itself can manage it without server connection.

Creating new masterlock area (on controller-level):

1. step: Select the controller
2. step: Press the edit button
3. step: Click on the “new” icon to create a new area. Fill in the name of the area and select the readers.
4. step: Select the users or groups as masters, who can lock the area
5. step: Save the changes.

From the drop-down menu above the masters window, it is possible to select which AUX input activates the masterlock.

The rule can be temporarily disabled with the “disable” button.

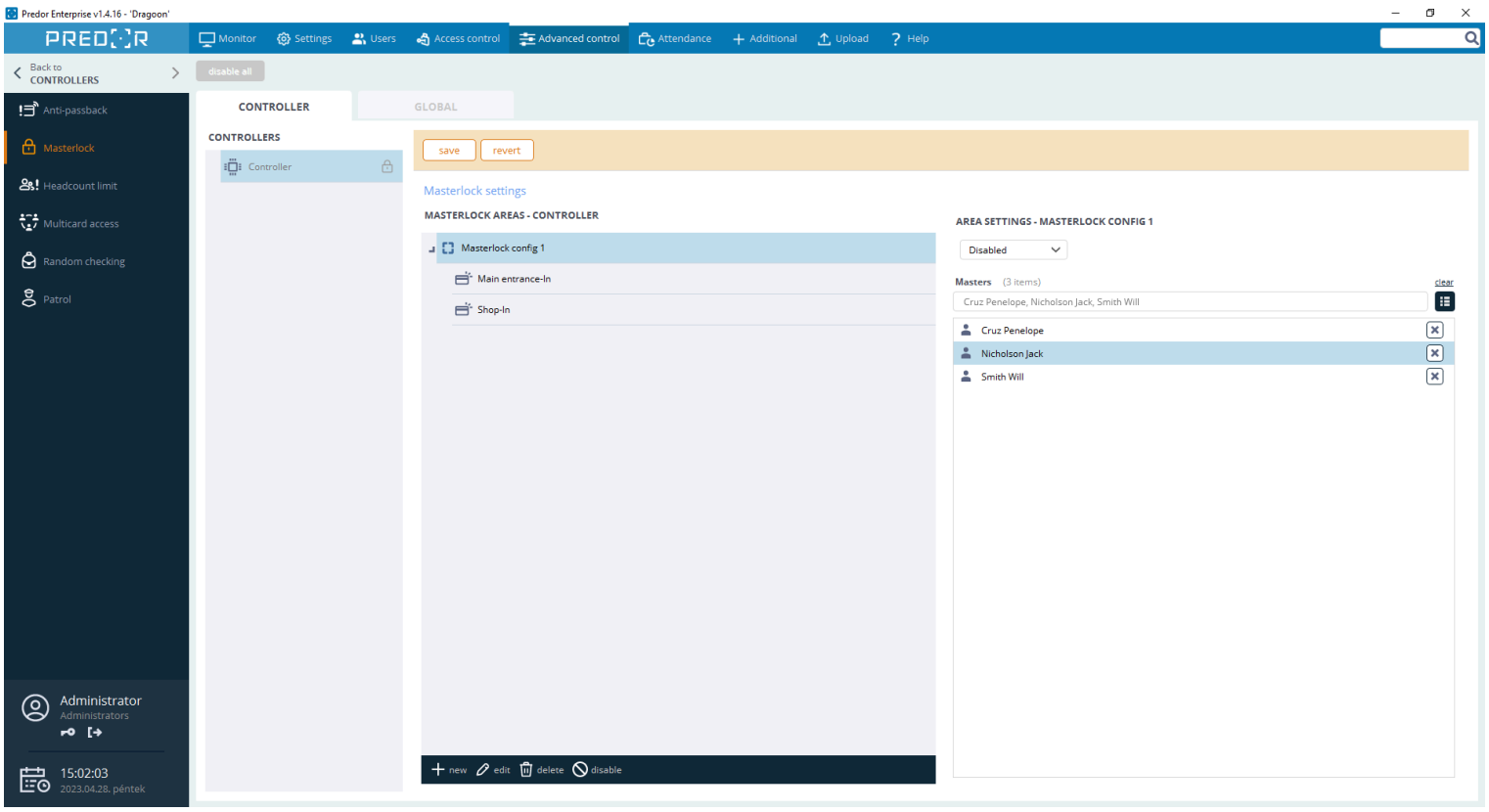


Figure 103: Configuring controller-level masterlock

Global settings

Global masterlock requires Enterprise version, because the server is necessary to facilitate communication with other controllers. **The masterlock areas are built from access zones so these should be defined beforehand.**

Creating new masterlock area (on global-level):

1. step: Press the edit button
2. step: Click on the “new” icon to create a new area. Fill in the name of the area.
3. step: Select the newly created area. This activates the zone selection. The pre-established zones are available for selection to form the new area.
4. step: Select the users or groups as masters, who can lock the area
5. step: Save the changes.

Masterlock application: On top of the masterlock area’s inwards readers the internal and/or the outwards readers can be locked too.

The rule can be temporarily disabled with the “disable” button.

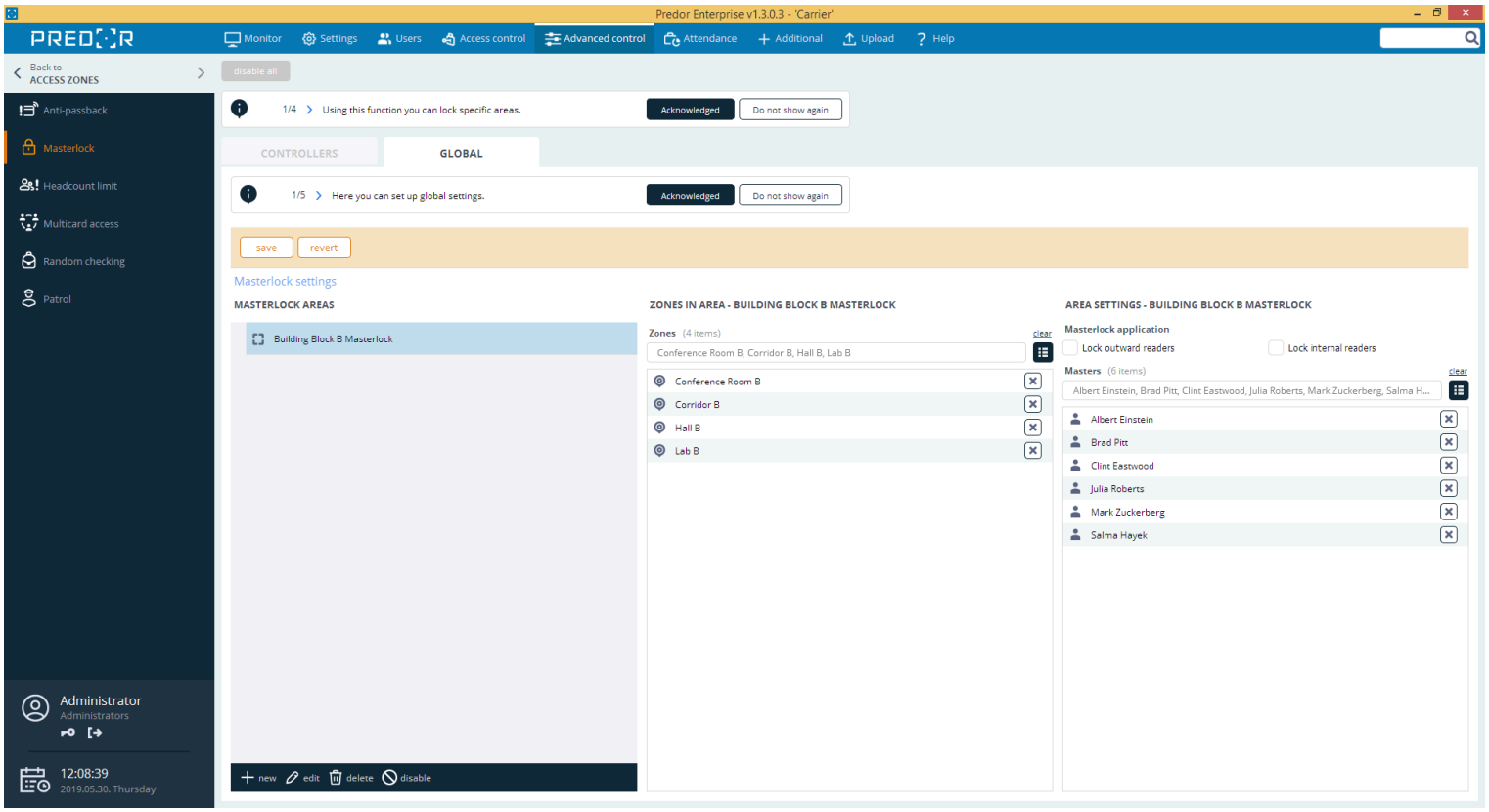


Figure 104: Configuring global-level masterlock

Headcount limit

In some establishments or events, it is beneficial to keep track and limit the number of people inside an area (this can be helpful in case of an emergency).

We can setup limits for individual groups too.

The **enable all**/**disable all** buttons on the top of the page allow/disable all of the rules with a single click. The **reset all** button can be used to reset the users' location data.

Controller-level settings

The controller-level headcount limit keeps track user numbers in areas built from doors on the same controller.

Headcount limit method

We can configure what happens when we reach the headcount limit.

- **Warning only:** The user can pass the gateway with the necessary privileges, even above the limit.
- **Block:** If the headcount inside the area reaches the limit, no more users are allowed in the area, regardless of their access privileges.
- **Tolerant (both):** The combination of the two methods above. In this case, two limits are established. A soft limit, that only generates warning and a hard limit that also prevents movement into the area.

We can select **exceptions** to the headcount limit. They can move into the area regardless of the current headcount (for example security guards).

Headcount for groups: By clicking on the **advanced** button at the bottom of the page, we can set up headcount limits for access groups individually. There is also a simpler method that only distinguishes between total and guest limits.

Creating new headcount limit area (on controller-level):

1. step: Select the controller
2. step: Press the edit button
3. step: Click on the "new" icon to create a new area. Fill in the name of the area and select the readers. IMPORTANT that every area needs at least one IN and one OUT reader.
4. step: Select users and access groups as exceptions from the rule. They can still move freely.

5. step: Use the simple limit definitions with the checkboxes in the area-settings secion, or press the **“Advanced”** button to establish group rules.

6. step: Save the changes.

The rule can be temporarily disabled with the “disable” button.

Global settings

Global headcount requires Enterprise version, because the server is used to facilitate communication with other controllers. **The masterlock areas area built from access zones so these should be defined beforehand.**

Headcount limit method

We can configure what happens when we reach the headcount limit.

- **Warning only:** the user can pass the gateway with the necessary privileges, even above the limit.
- **Block:** if the headcount inside the area reaches the limit, no more users are allowed in the area, regardless of their access privileges.
- **Tolerant (both):** The combination of the two methods above. In this case, two limits are established. A soft limit, that only generates warning and a hard limit that also prevents movement into the area.

We can select **exceptions** to the headcount limit. They can move into the area regardless of the current headcount (for example security guards).

Headcount for groups: By clicking on the **advanced** button at the bottom of the page, we can set up headcount limits for access groups individually. There is also a simpler method that only distinguishes between total and guest limits.

Creating new headcount limit area (on global-level):

1. step: Press the edit button, then select the headcount limit method (Soft, Hard, Soft & Hard)

2. step: Click on the new icon to create a new area. Fill in the name of the area.

3. step: Select the newly created area. This activates the zone selection. The pre-established zones are available for selection to form the new area.

4. step: Select users and access groups as exceptions from the rule. They can still move freely.

5. step: Use the simple limit definitions with the checkboxes in the area-settings secion, or press the **“Advanced”** button to establish group rules.

6. step: Save the changes.

The rules can temporarily disabled by areas with the “disable” button.

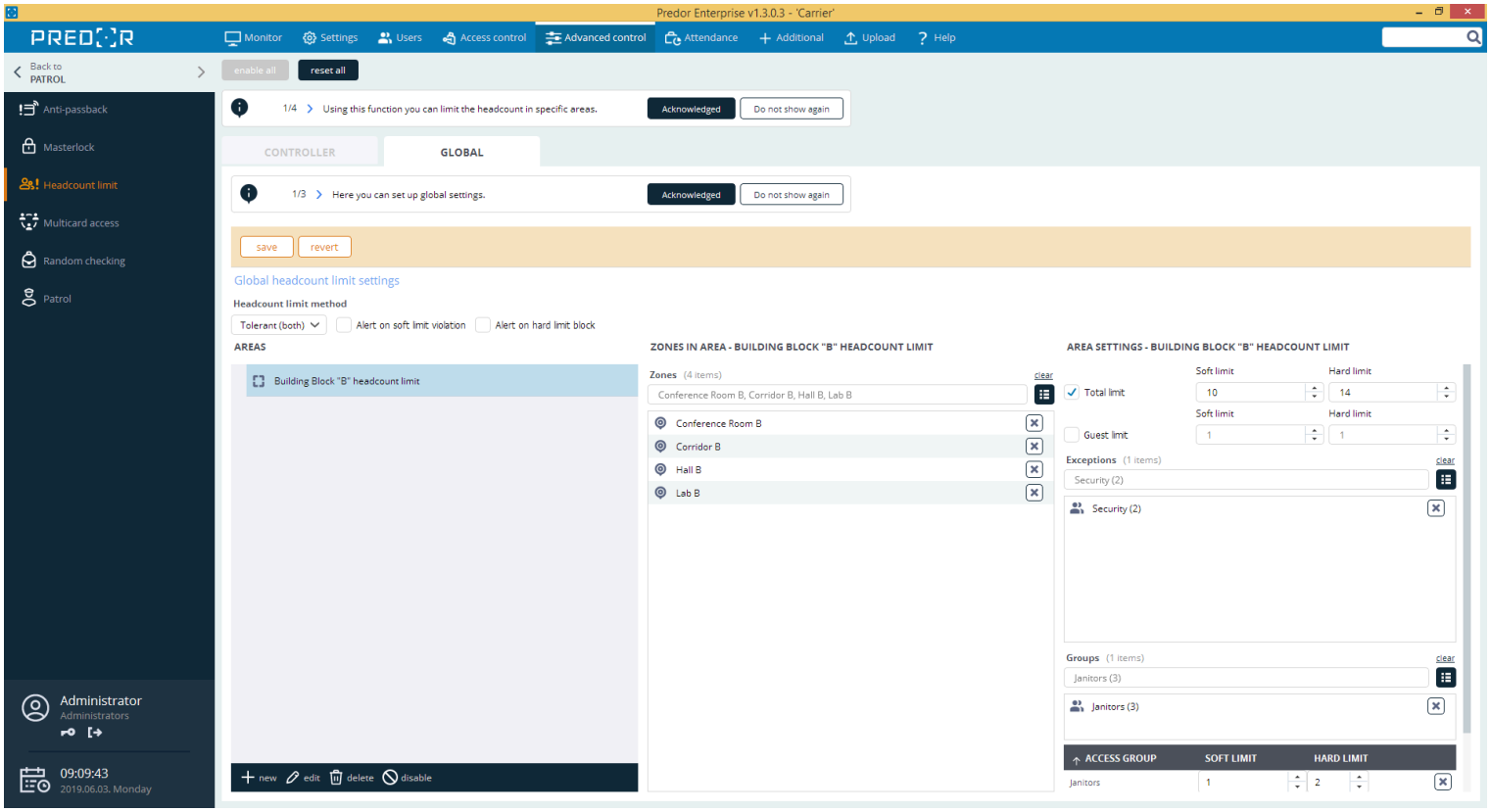


Figure 105: Configuring global-level headcount limit

Multicard access

For increased security, we can enforce that opening the gateway needs more than one authorized person. These rules are enforced on readers.

- **Multicard groups:** the gateway unlocks if a given number of members of a multicard group identifies themselves. Access groups can be selected here.
- **Mandatory attendance:** the door only unlocks when one of the selected mandatory personnel is present.
- **Exceptions:** these users can open the gateways alone.

Settings

Creating a new multicard rule:

1. step: Select a reader

2. step: Press the edit button
3. step: Select the multicard groups
4. step: Select mandatory and exceptions users
5. step: Save the changes

The rule can be temporarily disabled with the “disable” button.

Random checking

Here we can assign random checking to certain readers.



ATTENTION! The user quota in the random check module and the base license has to be the same.



ATTENTION! The random checking can only be used with a reader connected to a controller. To activate, card reading is required.

First we have to select the aim of control. It is important, because the mechanics of “bagcheck” and “other control” are different.

In case of a **Bagcheck**, the user cannot try again. If the check is blocking, they have to wait for the selected input to proceed (usually a security guard presses a confirmation button).

Other checking: for example a breathalyzer, scale or ESD check, the user can freely try again. After the identification, the **contact** has to arrive **to the selected AUX input within a given time period**, otherwise the entry is refused.

The **default probability** of the check can be selected in percentage, but for certain groups, we can override this with a greater or lesser value. The system uses the access groups for defining group rules.

Settings

To change the settings, click on the “edit” button.

Default probability: every gorup will be checked with this probability. In the simplest case, setting this is enough for a random check.

Time window (only with “other control”): After the identification, the accepting contact has to arrive within this time period, otherwise the entry will be refused.

Mode:

- Warning only: The checked user can pass the gateway, but the system signals the guard that a check is required.
- Block: The checked user is held up.

Signal input (only with "other control"): After the identification, the accepting contact has to arrive to this input, within the given time period, otherwise the entry will be refused.

Release mode (only with "bagcheck"): if we use blocking mode, the user will not be able to pass the gateway until a guard uses an button - connected to the input selected here - to release the user after the check.

AUX signals

Signaling on the AUX OUT 1 or AUX OUT 2 relay can be set, both in the event of a successful or unsuccessful result.

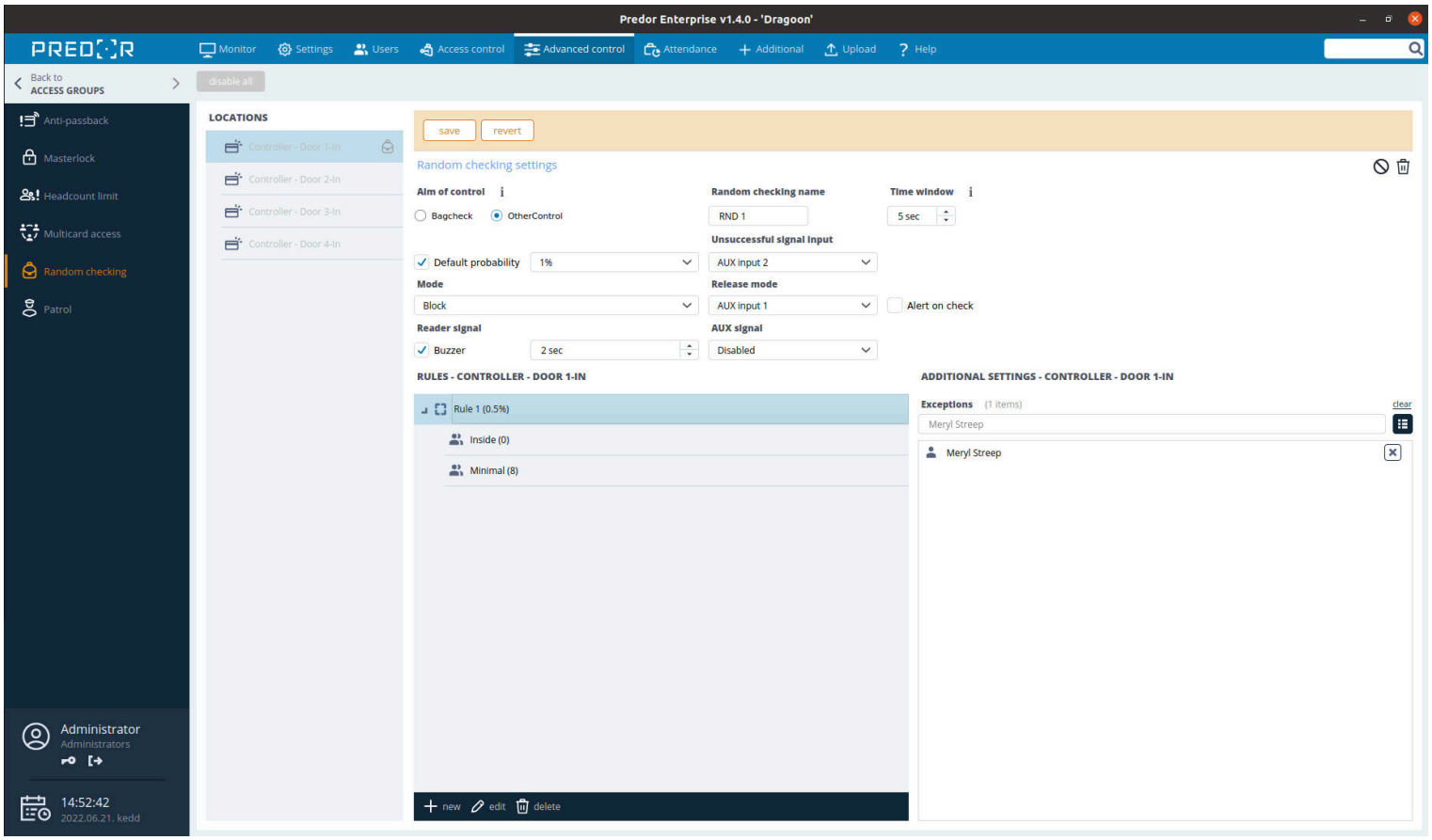


Figure 106: Editing a random checking rule

Creating a new random checking rule:

1. step: Select a reader.
2. step: Press the edit button.
3. step: Select the aim of control.
4. step: Select a default checking probability. This value is selected from a list where 0% and 100% is available. In case of “other control” set the time window too.
5. step: Select mode and the signal settings.
6. step: If some group needs different checking probability, click on the new icon, and create a group rule. Name it and select the checking probability and the groups.
7. step: Select exception users or groups; these are never checked.
8. step: Save the changes.

The rule can be temporarily disabled with the “disable” button.

Patrol

Patrol routes

We can create a patrol route from the readers in the system. The guards will use their own id cards, there is no need for expensive data collectors, or special checkpoints. The patrols are listed in detailed reports and can even be followed real time. Scheduled patrols start automatically and the guards get a notification when they are due.

To use this feature, first we need to establish a patrol route for the guards to follow. We can configure the order of the checkpoints and the time limit between each checkpoint and as a whole.

We can separately select operators who can issue (manually start) and observe a patrol. We can set up time limits between each checkpoint - the guard has to reach the next checkpoint within this time period, and to the traversal of the whole route.

The system counts any identification that is clearly associated with the guard as a check in, so invalid reads count too. The guard can use readers as checkponts, even without the necessary privileges to enter.

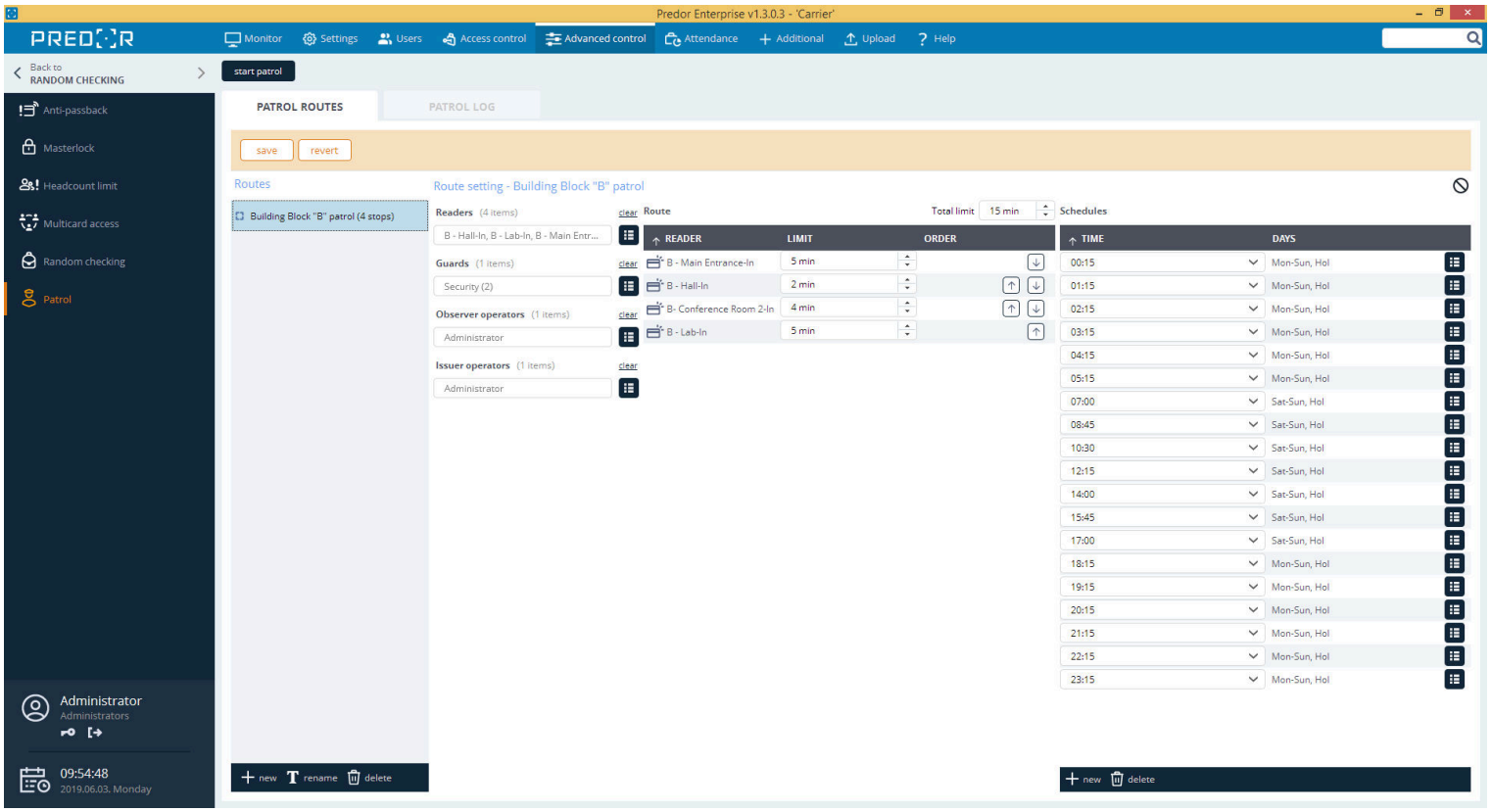


Figure 107: Setting up patrol routes

Patrols can be started in two ways:

The **“start patrol”** button above the page lets the operator select from the routes to start a patrol.

Alternatively we can **schedule an automatic patrol** start. We can schedule more than one time per route. Either way, a widget on the lower left side shows the currently running partols for every observer operator.

Patrol log

The patrol log tab enables us **to follow a running patrol or evaluate closed patrol** traversals. When a guard uses all checkpoint in the correct order and within the given time constraints, a green tick mark indicates that the patrol was successful. If any criteria fail, a red X indicates that; hovering the mouse above the icon will show more details about the detected problems.

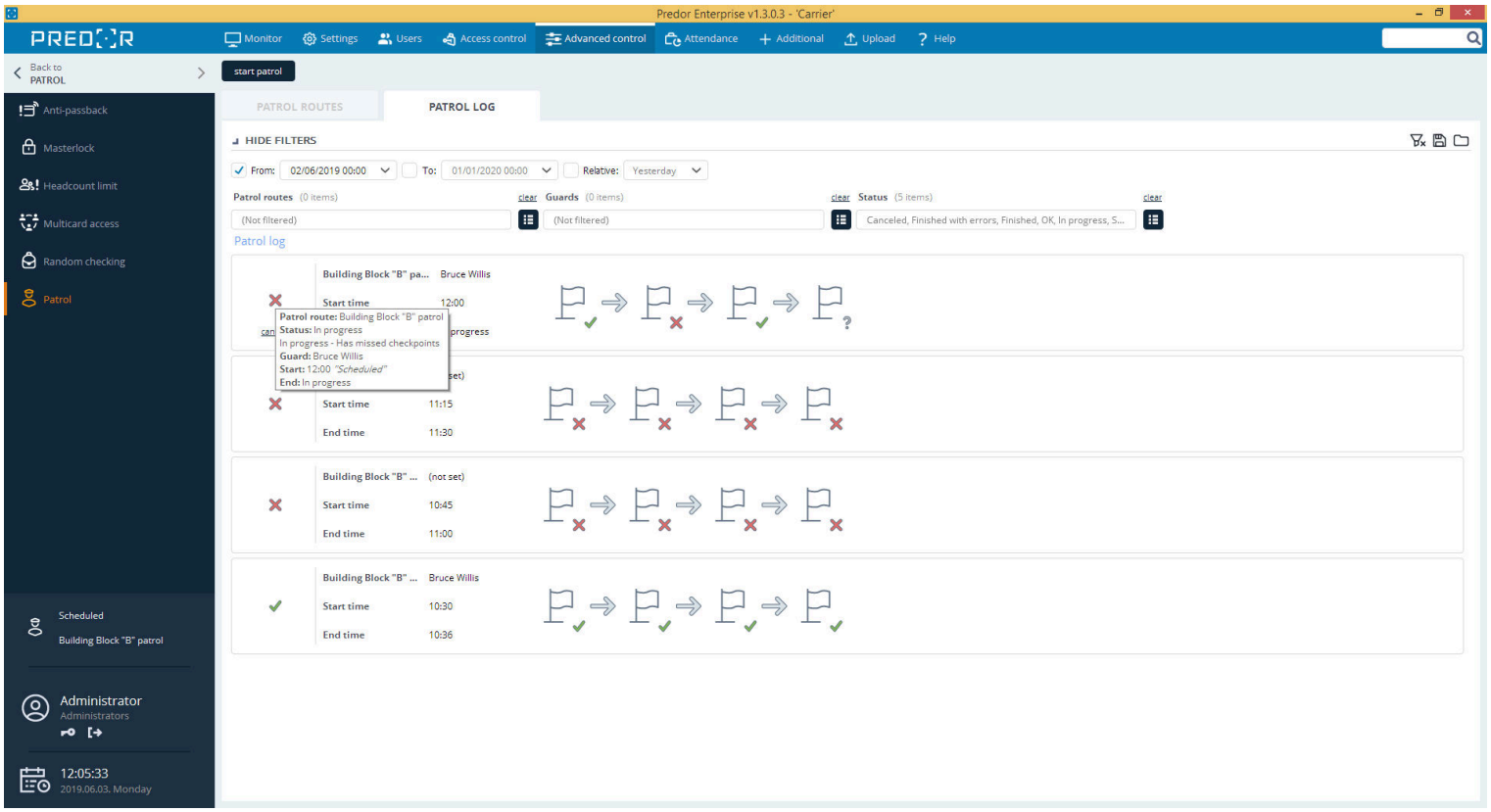


Figure 108: Patrol log view

10 ATTENDANCE MENU

Every time and attandance management related activities and settings are found in this menu, ranging from defining worktime rules and shift patterns to generating work time reports and time sheets. This menu becomes available after obtaining the *Worktime management module*.



ATTENTION! The user quota in the worktime management license and the base license has to be the same.

Work time calculation is based on movement data registered in the system. Employees identify themselves while passing through doors equipped with access control features so the system can measure the elapsed time spent at each workplace. Differentiation between working time and time spent with other activities is done with so-called activity codes. Activity codes determine if an activity counts as work time or not. Registration of activity codes (e.g. arrival, leave, off-site work, lunch break, etc.) can happen automatically using default activity codes per card reader or manually on card readers equipped with a keypad. Alternatively you can use the Predor time and attendance terminal which features a touchscreen with an intuitive menu and a built-in card reader.

Different work time rules may apply to employees in several occupations so their work schedules may differ. The software offers work time profiles to group work time rules into a single set which covers every aspect of the time related rules including time of arrival and leave, work time length, allowable breaks and their lengths, etc. The built-in profiles provide starting points for ease of customization. The software can handle work time profiles with multiple shifts, allowances, overtimes, flexible work schedules with the option to roll over work time balances and realizes complex break management.

There are special cases where work schedules have to be altered – for example on a national holiday or other special days. Such cases which can affect the operation or work schedules of the whole organization are registered in the calendar.

Calendar

In the calendar menu settings related to work time schedules and thus access control are managed. Custom day types, day off types can be created, special days (e.g. national holidays) can be registered to certain dates which can affect the work schedules throughout the company. Other settings which only affect individuals, like days off or shift assignments are managed in the user calendar.

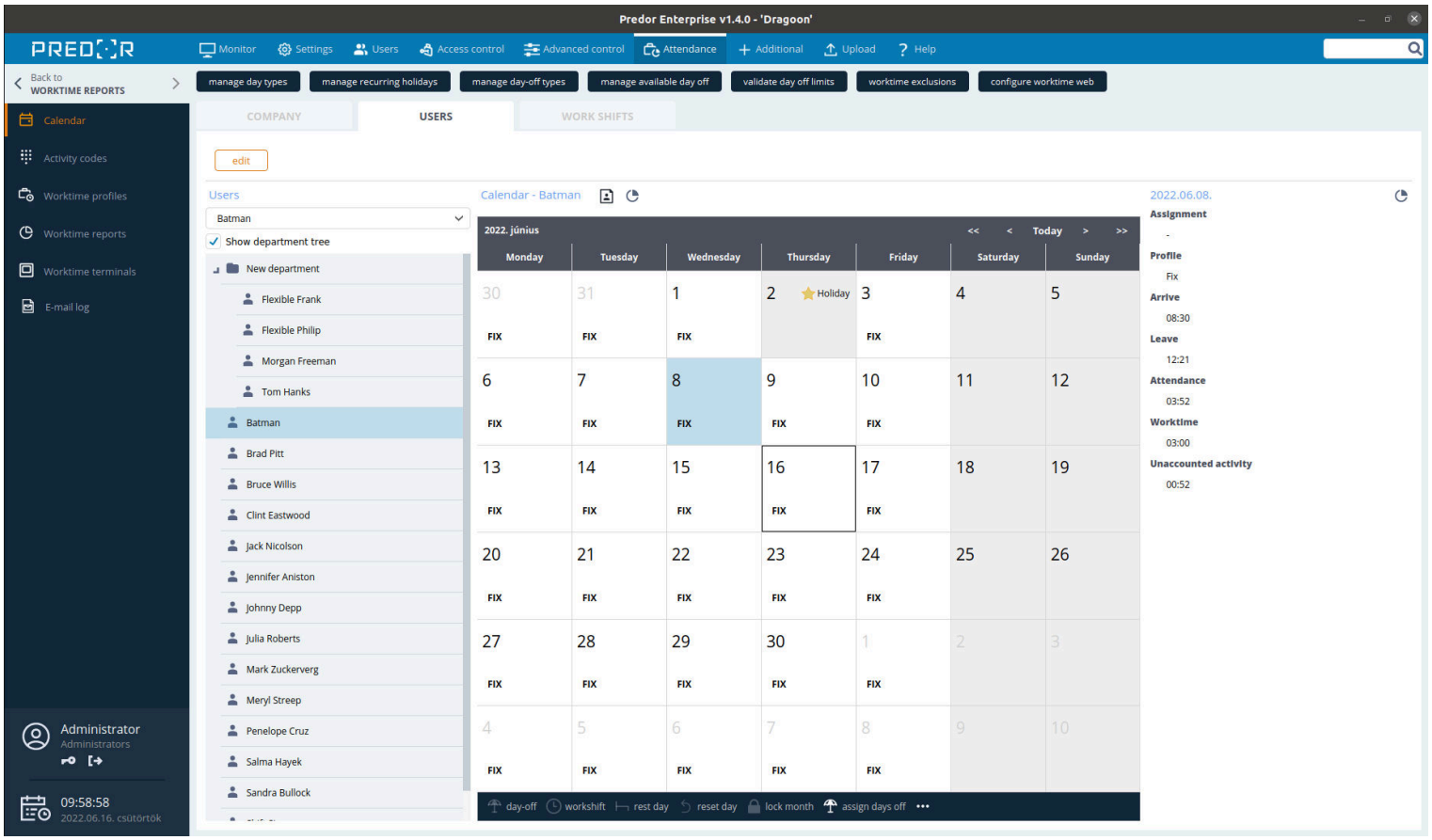


Figure 109: User calendar tab

Manage day types button: we can create special day types, with specific work schedules and we can mark these with different icons in the calendar. For example national holiday, short day, etc.

Custom day types will show up in the workdays check boxes and we can set these as workdays too.

Manage recurring holidays button: we can define holidays that are recurring in regular intervals, so, for example national holidays will automatically appear on the same day the next year. **We can use custom day types and set them to happen periodically.**

Manage day off types button: We can define day off types which can have the following parameters:

- Name: the name of the day off type
- Short name: short name of the day off type, which appears in cells of the calendars and calendar exports
- Payroll code: the day off type can be provided with a payroll code, which is necessary if our system sends data for payroll software.

- Icon: small icon which is displayed in calendars
- Default limit: Default amount of this day off type which is assigned to every user. This can be customized per user in the *Manage available day off dialog* if the *Can override limit* option is set.
- Continous limit: Maximum number of this day off type can be requested in a continous interval.
- Approval required: Determines if an employee's request for this type of day off from the worktime web is automatically approved or a manager's approval is required.
- Can override limit: If override is enabled then different amount of days can be assigned to each employee of this day off type in the *Manage available day off dialog*, otherwise it is hidden (it still appears in exports).
- Available on rest days: sets if this day off is assignable on rest days.
- Can be requested in past: Such day off types can be requested by the employee on the My calendar (Worktime web) site for a past date
- Can be carried over: unused time of this day off type in a given year can be carried over to the following year
- Unpaid: the employee will not be paid for the days on which he takes unpaid day off, and that day will not be counted as time worked.

Manage available day-off button: We can specify a day-off quota for each day-off type for each user. The users can not issue a day-off request on the worktime web, after they used up their quota.

The yearly quotas and the used day-offs are exportable. The personal quotas are even importable from a proper Excel spreadsheet! Attention! Be careful when importing personal quotas, as the amount of used day-offs cannot be imported, because it is automatically calculated from the calendar, and the import does not create calendar entries!

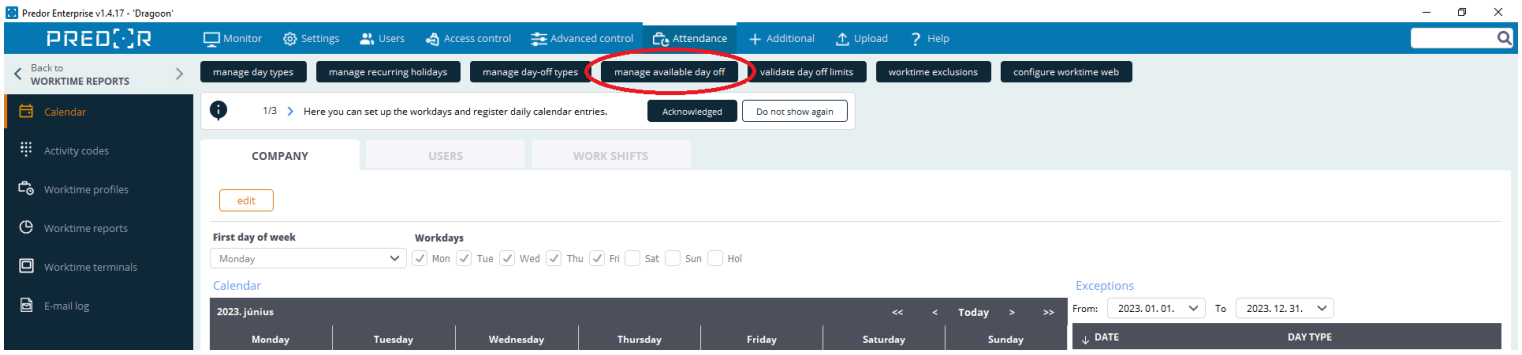


Figure 110: Manage available day off button in the calendar menu

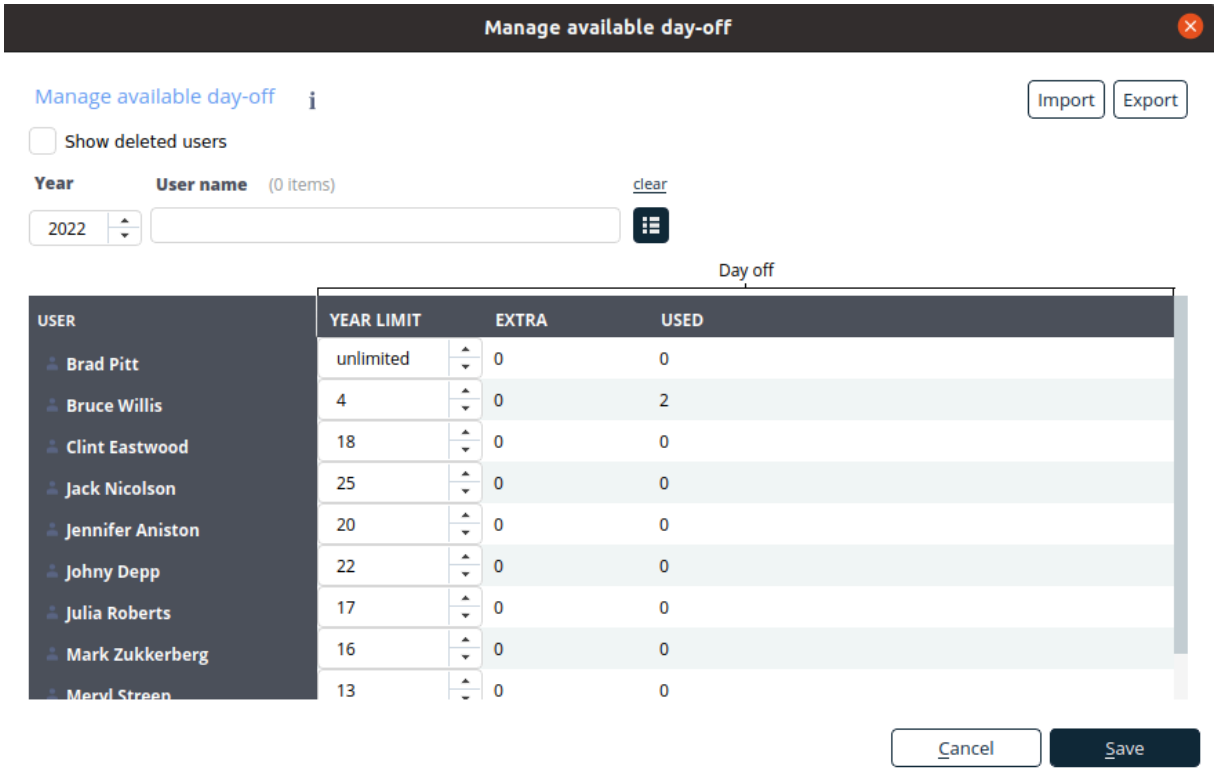


Figure 111: Manage available day-off dialog

Worktime exclusions button: On this interface, we can exclude users selected or deleted from the worktime calculation. No worktime events are generated for excluded users, and worktime reports cannot be created for them either.

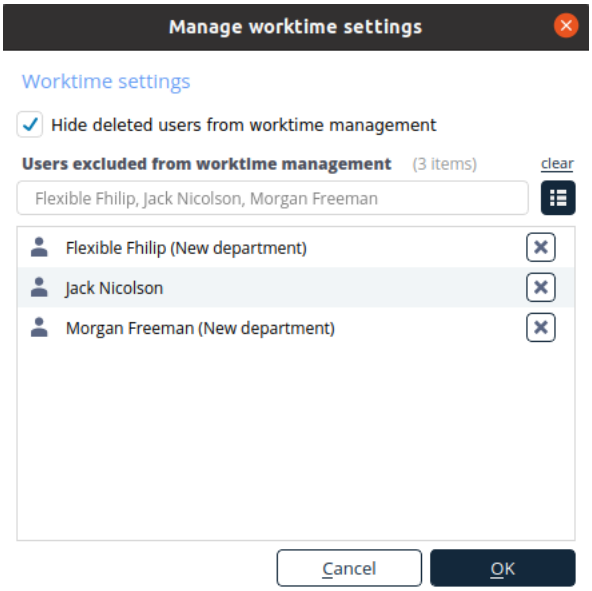


Figure 112: Editing of persons excluded from worktime menu

Company calendar

On the company calendar tab, we can specify the workdays and rest days in general. We can also create national and other holidays too. To make changes, we have to enable the edit mode first.



TIP: It is possible to add multiple company calendars to set different day changes and holidays. (Explained in Managing several company calendars section)

First day of the week: changes the calendar view. The selected day will be the first column.

The workdays are selectable via the checkboxes. Rest days will appear with a grey background while workdays with white background in the calendar.

By selecting a cell in the calendar, we can initiate swap days, for example, we can appoint a Saturday to a Monday - **so the system will enforce a Monday work schedule on that date, and the access privileges will use the Monday settings too.**

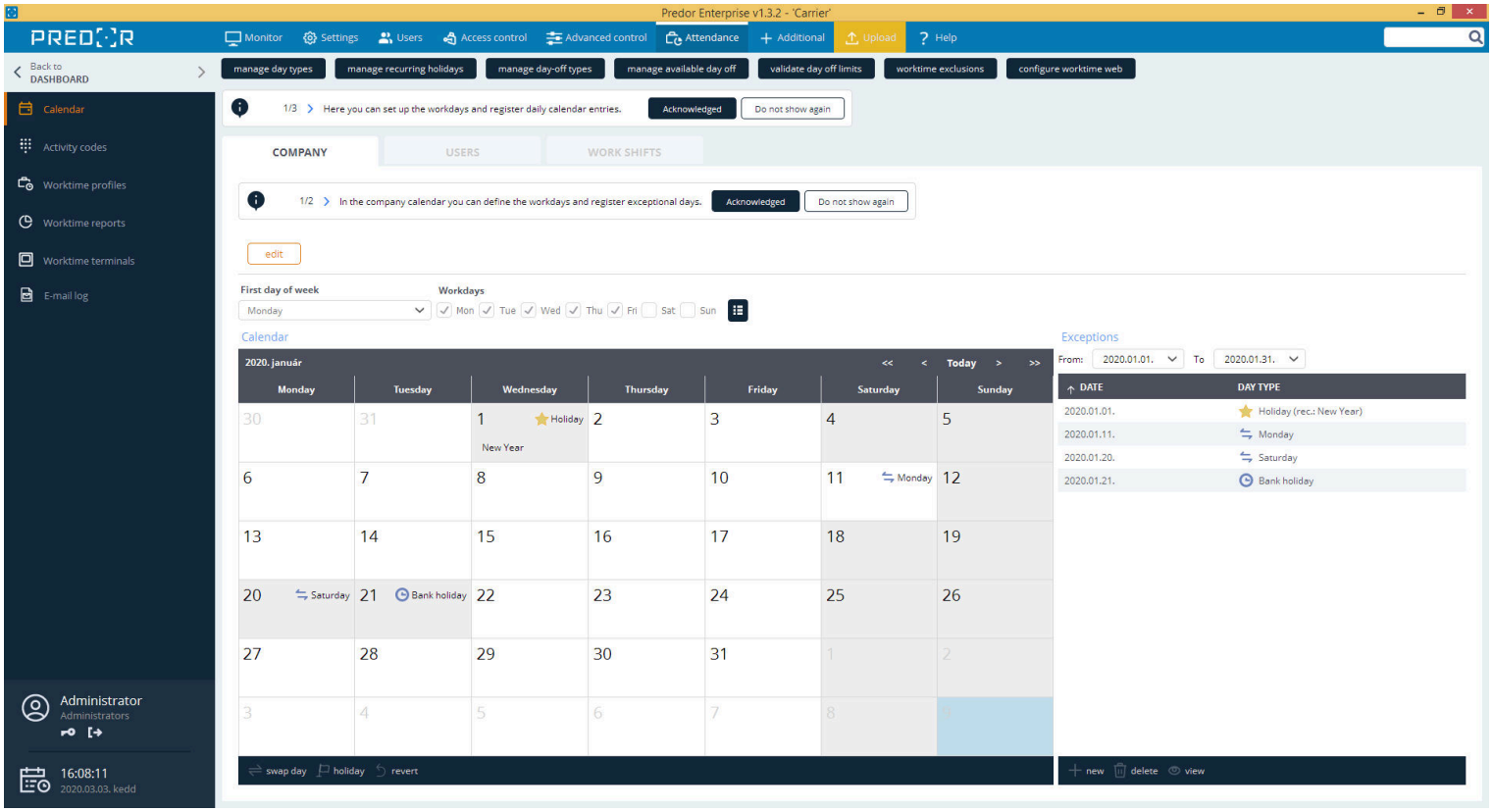


Figure 113: Company calendar view

User calendar

On this interface, we can schedule individual employees' worktime and issue day offs.

By clicking on the given person, the corresponding worktime schedule and day off will appear in the calendar. By double-clicking, you can navigate to the Daily activity report, where you get a detailed overview and additional editing options for the employee's day.

To easily issue a holiday or rest day, click the edit button and select the appropriate calendar cells. By clicking on the selected elements with the right mouse button, you can choose the type of day from the drop-down menu. If the user's day off limit is less than the amount that would be granted, the pop-up window will display "The limit will be exceeded after the operation." warning.

In edit mode, using overtime settings belonging to the corresponding profile, we can order overtime by right-clicking on the selected days. In doing so, the superior may require the employee to work overtime before, after, or at an arbitrary interval.

Create new day off types in the "manage day off types" window.

Work shifts

On this interface, you can not only review the schedule of employee shifts, holidays and rest days, but also edit them. In this way, you can issue vacations as a group, carry out the shift classification in a transparent manner, and schedule overtime in the way known from the User calendar. You can also repeat the existing assignment of each employee by section at the time you specify or until a designated date. If we want to grant day off to several people or assign them to a shift, it is enough to edit the calendar of one employee, then select the appropriate days and click on the copy to user button. In this way, we can copy off days, shift assignments, and rest days to the calendar of the persons selected in the dialog.

In the case of automatic shift classification, the system displays the determined shifts for the already completed days if you click the *load shifts* button or if *automatic load shifts* is enabled. Shifts established from events are indicated by the system with ***** inserted after the name of the shift. Guessing the shifts can take a long time for many users, so if the guess is correct, it is worth confirming the shift using the **assign guessed shift** button at the bottom of the menu bar in edit mode, so the subsequent loadings can be significantly faster. Shifts are displayed on the web interface in the same way as in the client application.

We can filter the data by departments, users, and worktime profiles and these filters can be saved too.

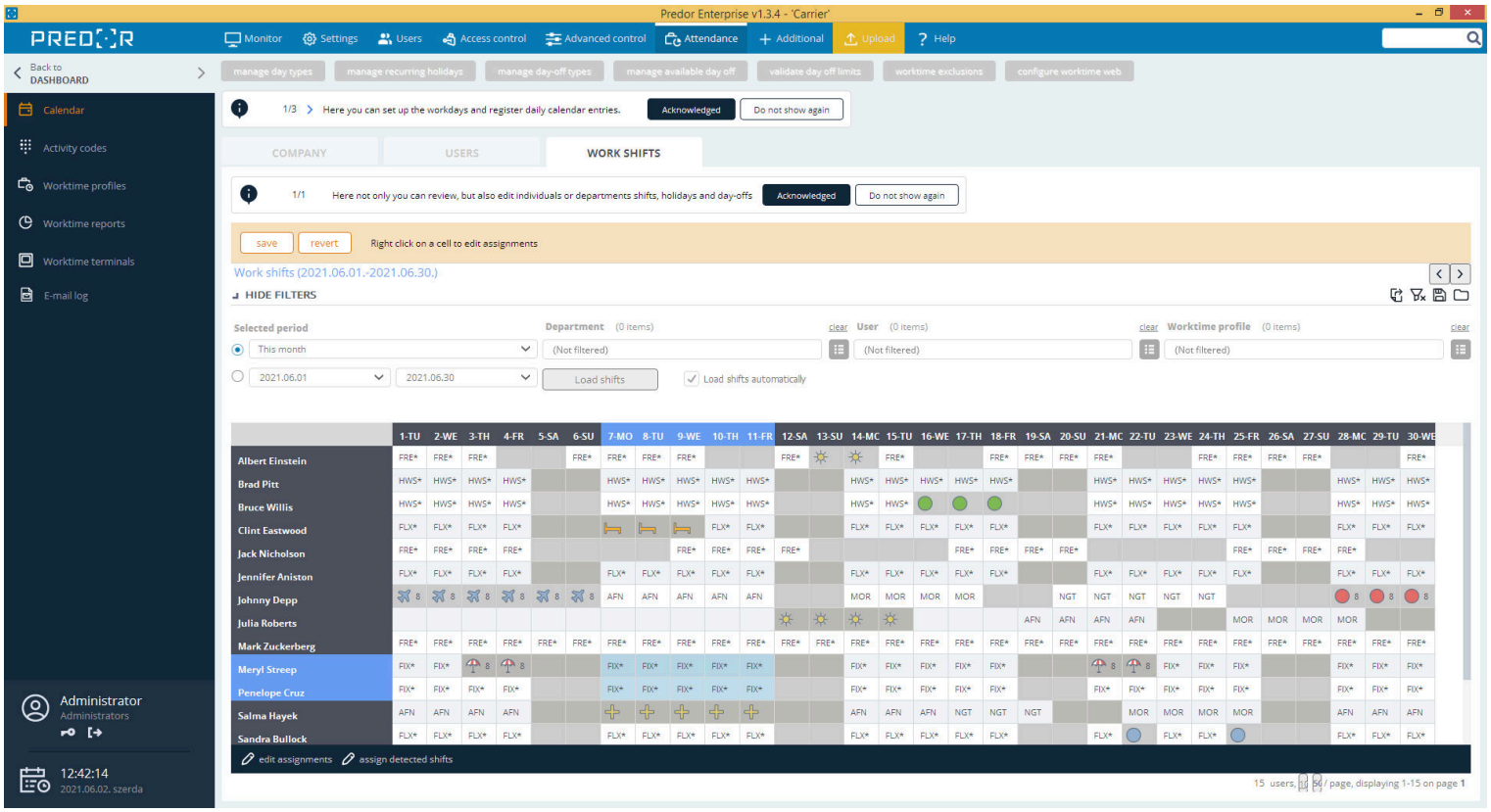


Figure 114: Work shift assignment overview

The work shifts calendar can be exported to Excel file using the button. Prior to exporting, a dialog appears where the data to be exported can be customized:

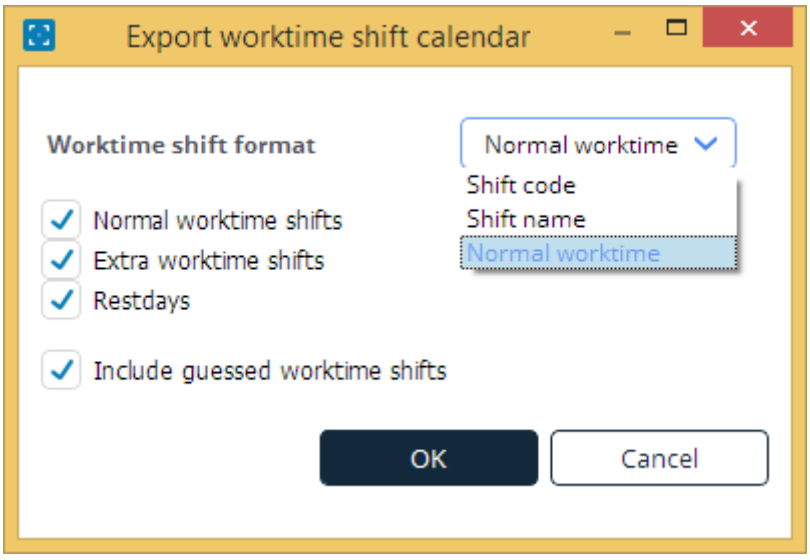


Figure 115: Work shift calendar export settings

Cells will be filled with the selected *Worktime shift format*:

- **Shift code:** Cells will contain the short code of the shift (Eg.: MOR, AFT)
- **Shift name:** Cells will contain the full name of the shift. (Eg.: Morning Shift, Afternoon Shift)
- **Normal worktime:** Cells will contain the normal working hours of the shift. (Eg.: 06:00 - 14:00, 14:00 - 22:00)

Data to be included can be:

- **Normal worktime shifts:** normal worktime shifts will be visible in the export
- **Extra worktime shifts:** extra worktime shifts will be exported
- **Restdays:** rest days will be indicated in the export
- **Include guessed worktime shifts:** shifts determined automatically based on events will be included in the export

If days off are assigned to one or more employees a confirmation window appears where the already used and available number of the day off type and selected users are displayed. A warning symbol appears if we are about to allocate more days off than the limit of an employee.

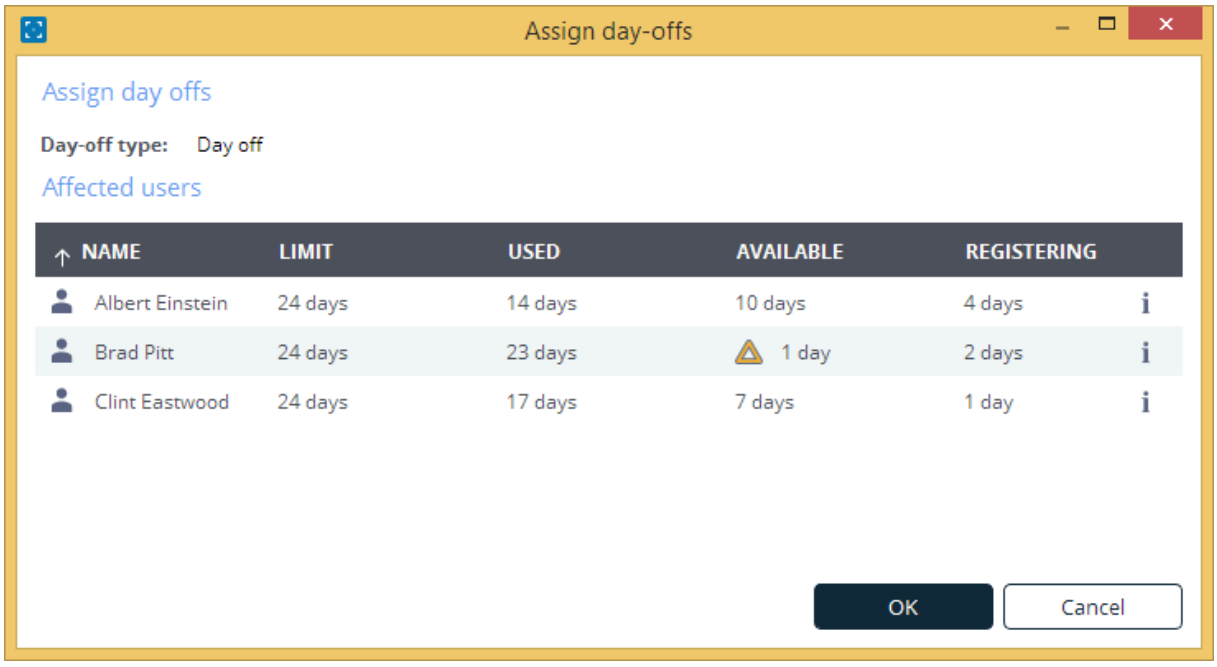


Figure 116: Day off confirmation dialog in the Work shifts calendar

Days off assigned this way must happen between the boundaries of one year and all employees on all selected days have to have the same day off calculation (day or hour-based) method.

During editing there can be cases where conflicting calendar entries are to be applied

to one or more days. If this happens the “Calendar entry collisions” dialog is automatically displayed where the conflicts can be resolved case-by-case or by selecting collision types from the top row.

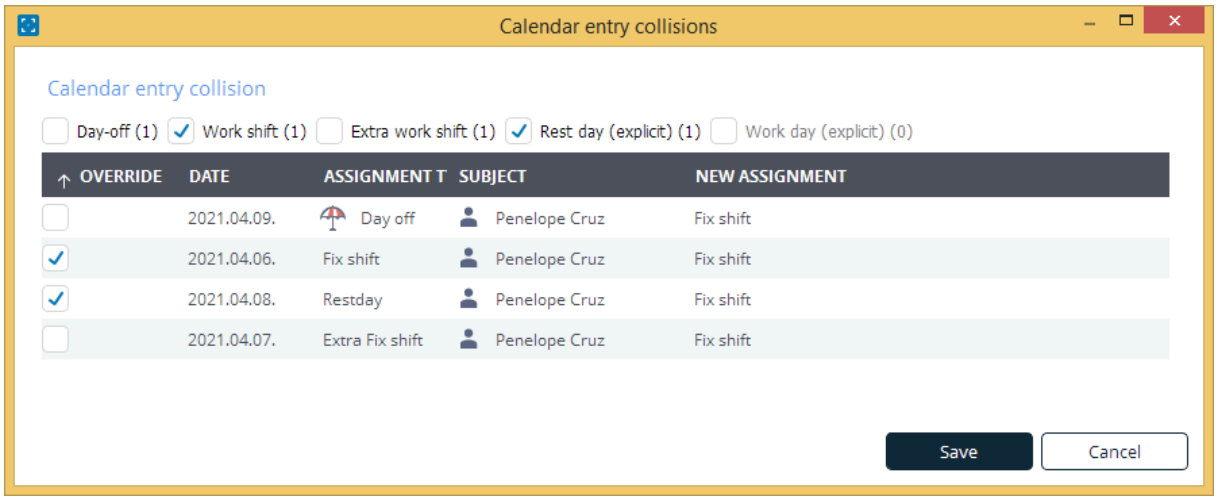


Figure 117: Calendar entry collisions dialog

Activity codes

We use activity codes to identify the users’ activities, and track their schedules. Activity codes determine - among other things - that an activity is considered as worktime or not, or is it paid or not.

We can define up to 99 activity codes.

The creation of a new activity code is initiated by pressing the “**+** new” icon below the list on left side at the acitivites tab. First we have to set the name and code of the activity code in the dialog, then use the checkbox to set whether the activity is considered as worktime or not. From the locations list, we can select the readers where the activity code is available. If the code should be available everywhere, just leave the “Restrict locations” checkbox unchecked. On the worktime terminals, the activity code will appear with the selected pictogram and background color.

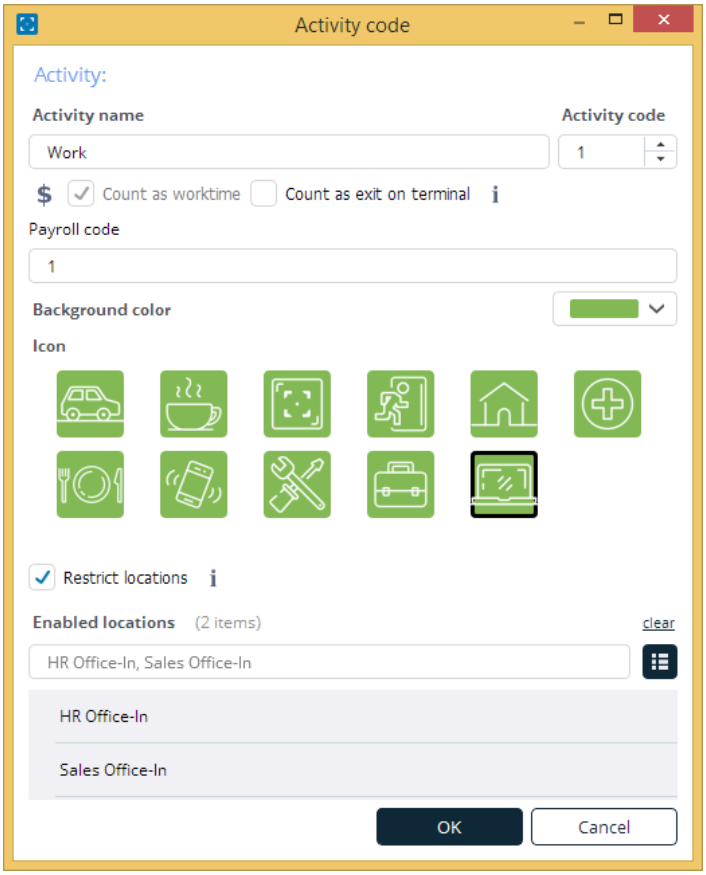


Figure 118: Edit activity code dialog

Default activity code: if an activity code is default on a given reader or zone, and the user did not input an activity code with the card read, the system will automatically account it as the default activity. This can be set up with the "set as default" button below.

ATTENTION! If you want to exclude a reader from the worktime management, select the reader then click on the **"disable"** button below the reader list.

Every reader with a keypad can handle activity code entries from the users. To enable this, the reader kind has to be set to "Card reader + keyboard" and the mode has to be either "Activity code + Card" or "Activity code + Card + PIN" in the edit controller wizard dialog. In this case we have to input the activity code then present the card.

TIP: We can handle activity codes on readers without keypads. If we set a default code on a reader, it is enough to read a card and the system will account our activity as that default activity.

Activity code defaults

Different activity codes can be assigned to each worktime profile on readers, thus different paid or unpaid activities are registered to the users automatically when they swipe their cards. Setting “None” on a reader continues the previous activity code.

EXAMPLE: Workers of a canteen can have “Work” while others have “Lunch” activity code automatically registered by entering the canteen.

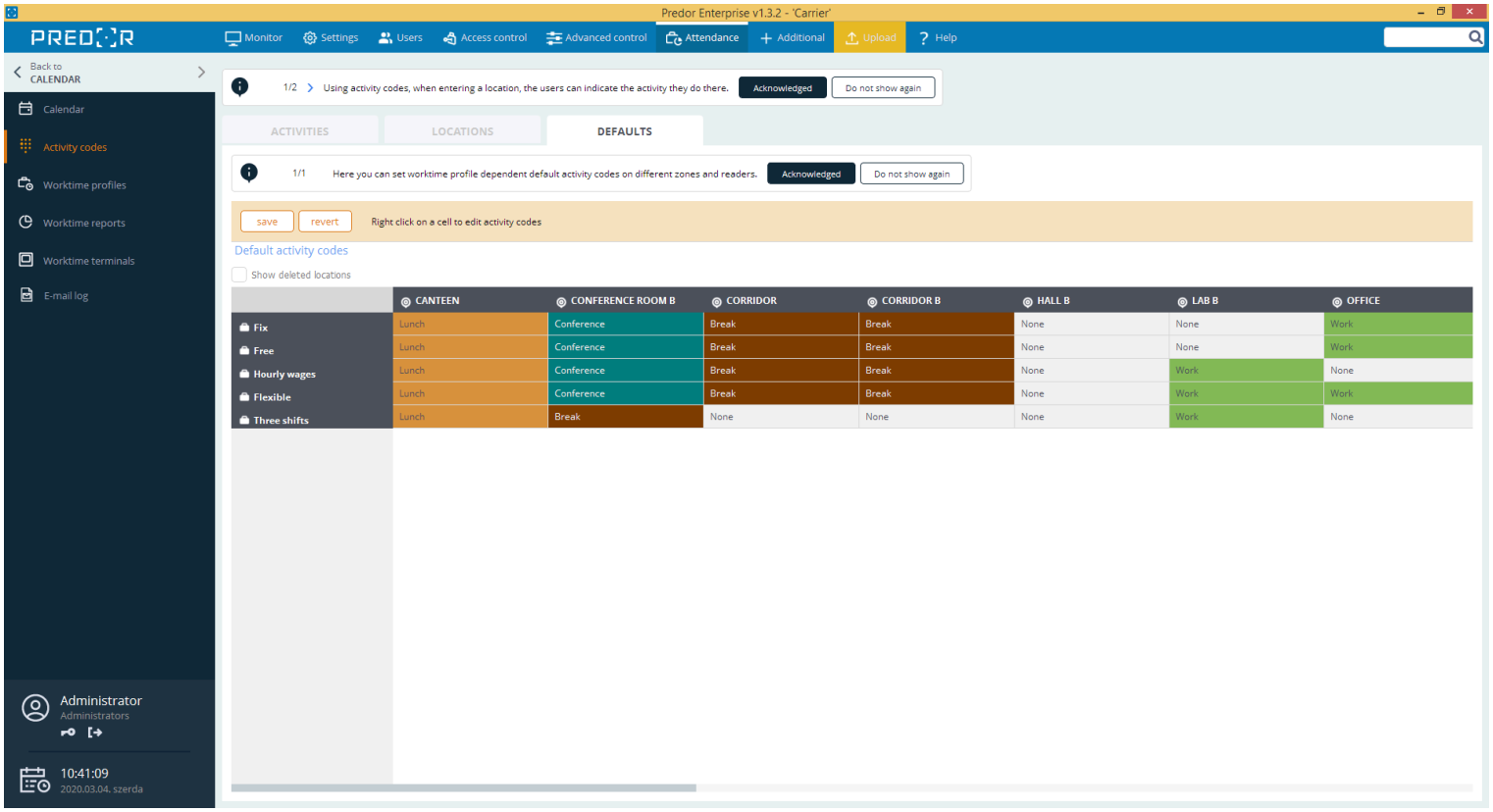


Figure 119: Worktime-profile based activity code registration on different readers / zones

Worktime profiles

On the **worktime profiles tab**, we find a list of built-in and already configured worktime profiles. The most important properties of each profile are summarized in the columns of the table.

The **“View by users”** tab lists the employee - worktime profile assignments and the starting and end dates of its validity.

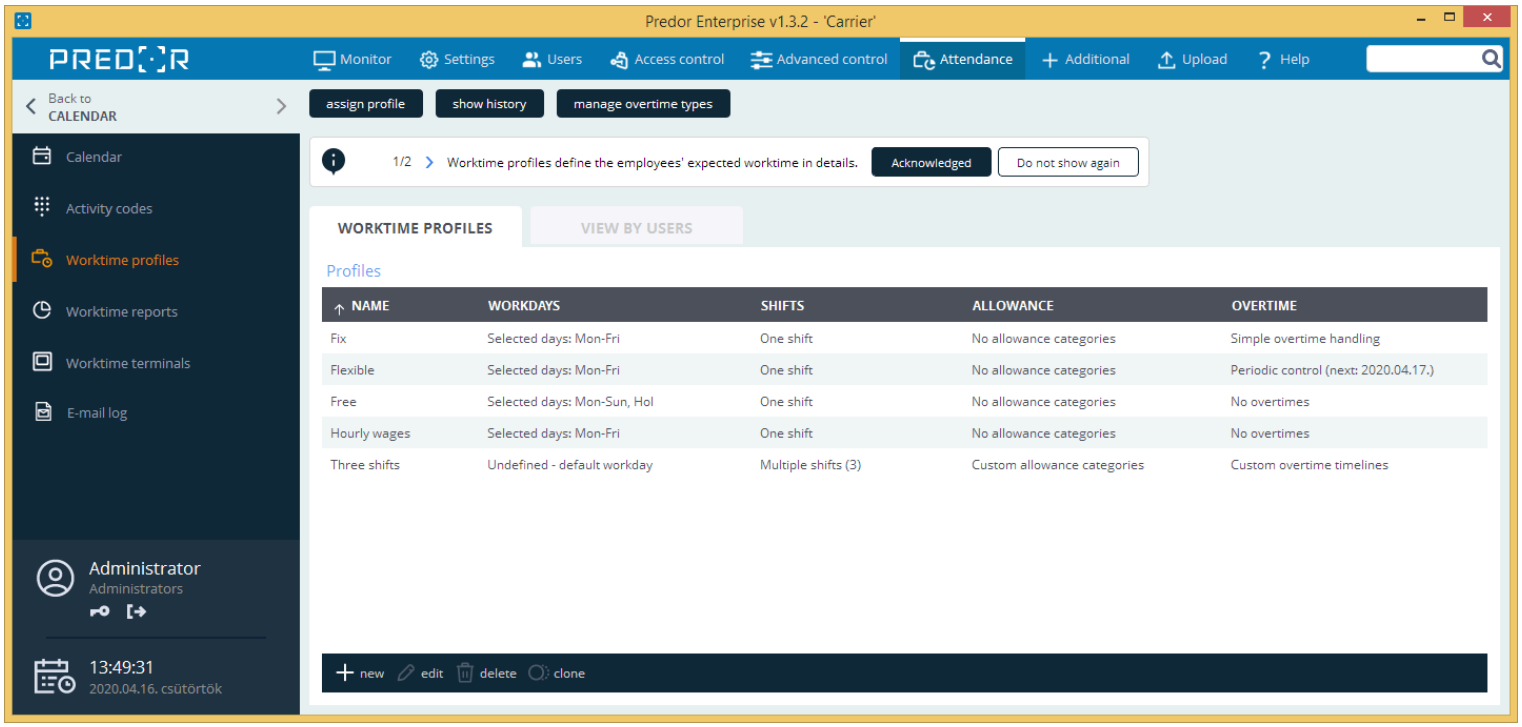


Figure 120: Worktime profiles menu

Assigning a profile to the employees: by clicking on the **"assign profile"** button, the employees can be assigned to the previously defined worktime profiles. We can select the users and departments in the dialog, and assign a worktime profile to them in a given interval. The preview calendar assists by showing the validity.

The **worktime profile history window** shows, what worktime profiles were associated with each employee in the past.

In the **overtime and allowance types** dialog, we can define overtime and allowance categories, and for flexible work time schedules the balance multipliers. Weighting is represented by percentages, where 100% means normal wage. (For example if we want to issue a 50% overtime bonus then use a value of 150%.)

The *Daily allowance* is a special type because unlike the others it cannot be assigned to timelines in the work time profile editor. Instead it will be allotted to the whole shift even if it crosses midnight, so this type of allowance takes the "day ends" setting into consideration.

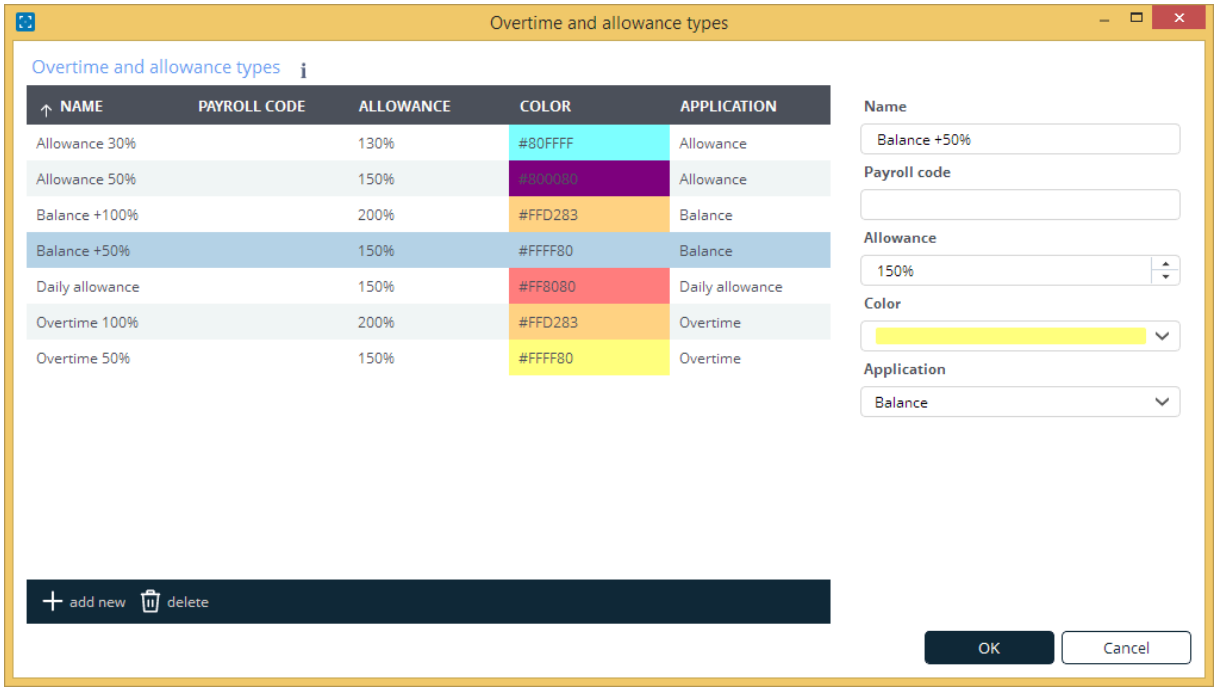


Figure 121: Overtime times are managed in this dialog

On the bottom menu row, new worktime profiles can be created with the **+ new** button. The **edit** button opens the worktime profile editor window for the currently selected profile (this can also be achieved by double clicking on the profile). The **delete** button deletes the selected profile(s). Caution is advised when deleting profiles, because it cannot be undone! Upon deleting a profile, all users ever assigned to it become unassigned for the period, even retrospectively. The **clone** button opens a profile editor window with the same settings as the currently selected profile, therefore it can be used to create profiles which only differ in some parameters. Inside the additional operations ••• menu there is a button called **Edit balance closings** which can be used to handle balance closing dates for multiple profiles simultaneously.

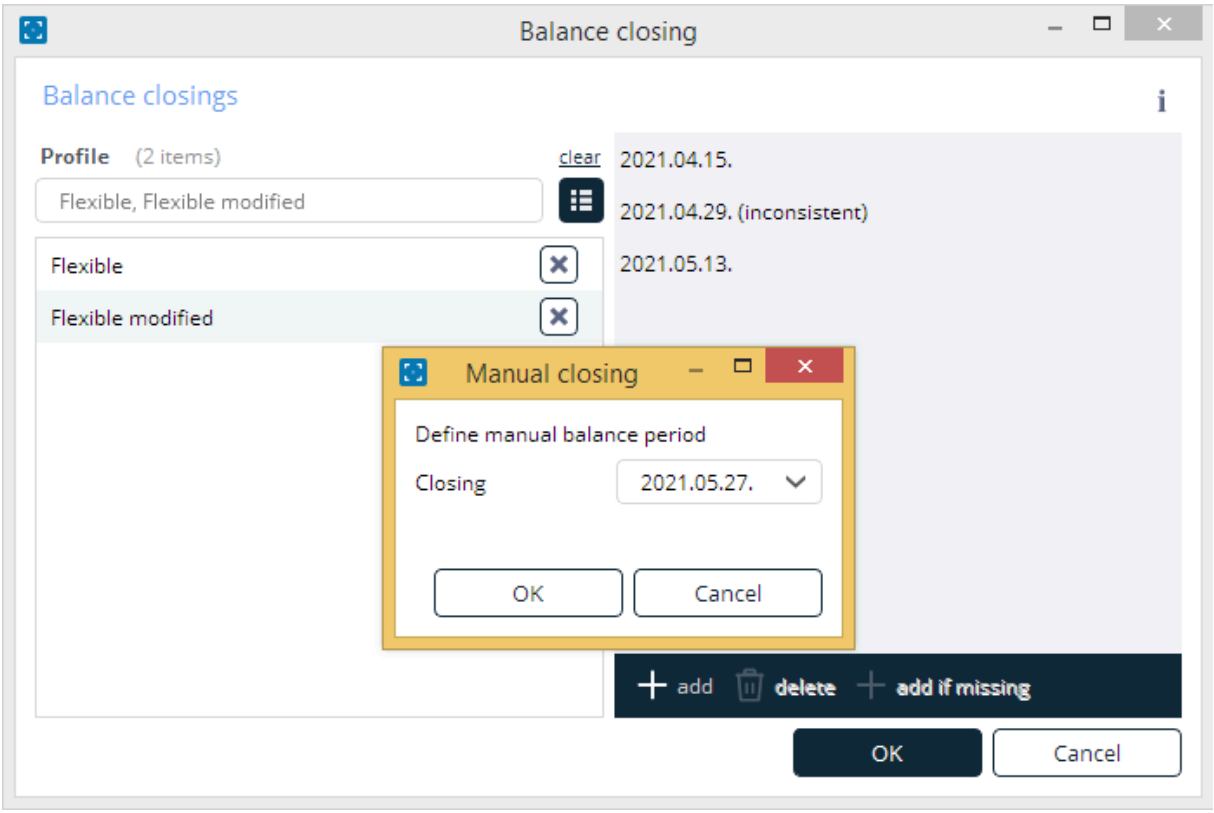


Figure 122: Group balance closing dialog window

Closing dates of the selected profiles appear on the right. Rows marked as **(inconsistent)** are missing from at least one of the currently selected profiles. Using the **add if missing** button resolves this inconsistency by addig the closing date to all of the currently selected profiles. New closing dates can be added with the **+ new** button, and deleted with the **delete** button from all currently selected profiles simultaneously.

Worktime profile configuration

By clicking on the "**+** new" button on the worktime profiles tab, we can **create a new profile**. This opens the profile editor wizard.

On the first page of the wizard, we can define the working days, limit the time accounted in different cases, select the accepted activities and decide how the result of a random check (bag check, breathalyzer, etc.) will affect the daily working hours of our employees.

When **setting up the workdays**, we can choose from these options:

- **Company calendar:** the profile uses the workdays defined by the company calendar. This option will use the swap days, rest days and holidays from the company calendar too.
- **Selected days:** the days selected in these checkboxes will be considered as workdays regardless of the company calendar settings. However, the profile will use swap days,

rest days and holidays from the company calendar.

- **Periodic:** we state the consecutive number of workdays followed by a number of rest days, regardless of the day of the week. (The starting point of the period can be adjusted when the profile is assigned to the employee)
- **Undefined:** any day of the week can be workday or rest day. We have to choose that every day is considered as a workday or a rest day by default. Every employee assigned to this profile have to be assigned every day manually to work and rest days, otherwise the default day type is used in worktime reports.

Employed times: when limiting, we can set the followings:

- **Hour based day off handling:** in the profile, vacations will be measured in hours instead of days.
- **Account worktime for holidays on workdays:** in the profile, holidays falling on a working day will be considered a full day, despite the fact that our employee did not work that day.
- **Default worktime:** determines how long the working hours are in a day in the profile.
- **Default day off:** determines how long work is calculated on a day off.
- **Accounted time on rest days:** determines how long the accounted work is for a day off.

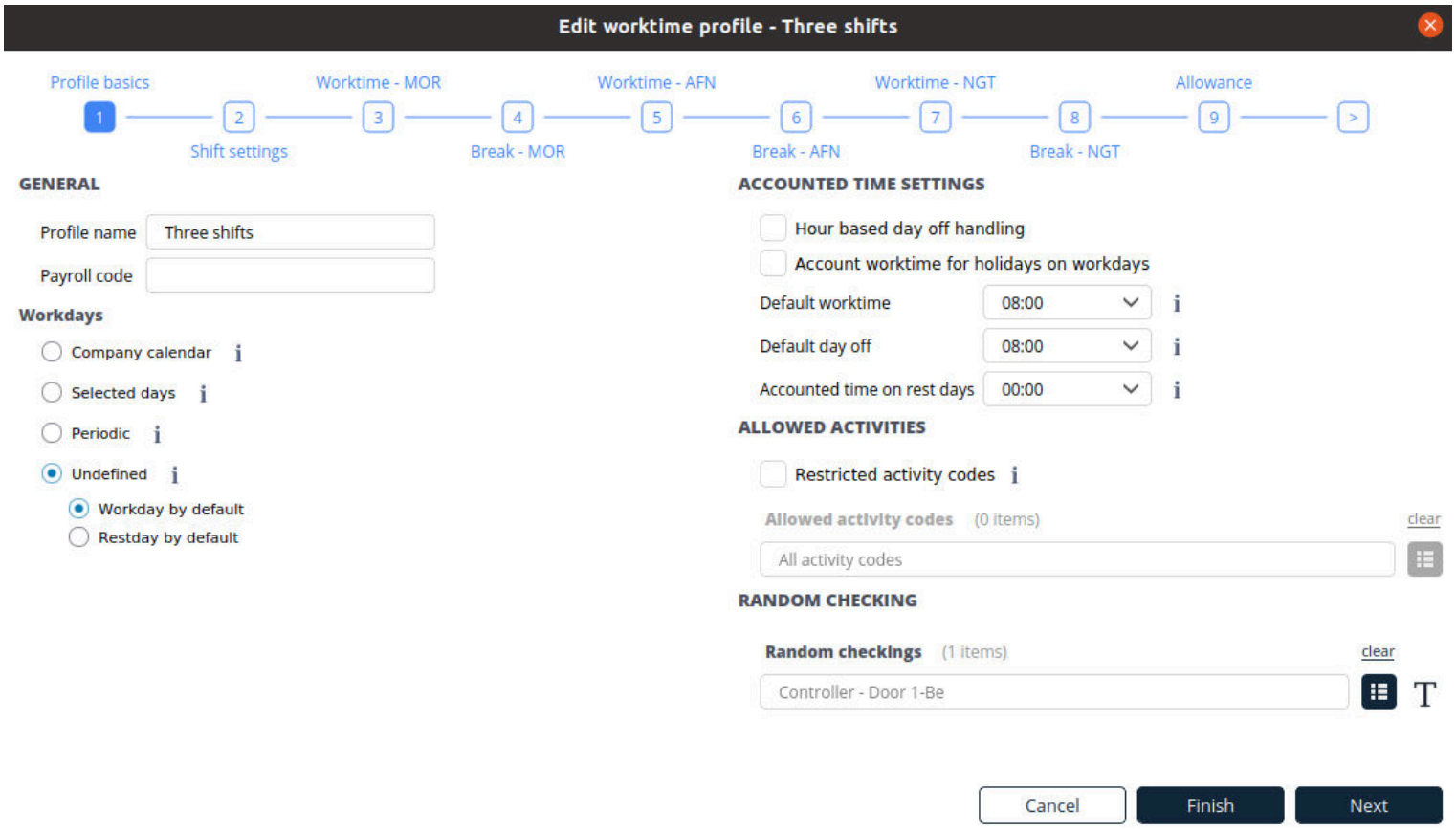


Figure 123: Configuring worktime profile - basic settings

Random check: Here you can select a Random check rule, the success, failure or timeout of which can affect the worktime calculation of our employees listed in the profile. There are two ways to do this:

- **Unaccounted work:** In the event of an unsuccessful signal or the timeout set here, the day's work is converted into unaccounted activity.
- **Warning:** In the event of an unsuccessful signal or the timeout set here, a warning signal will appear on the employee's day.

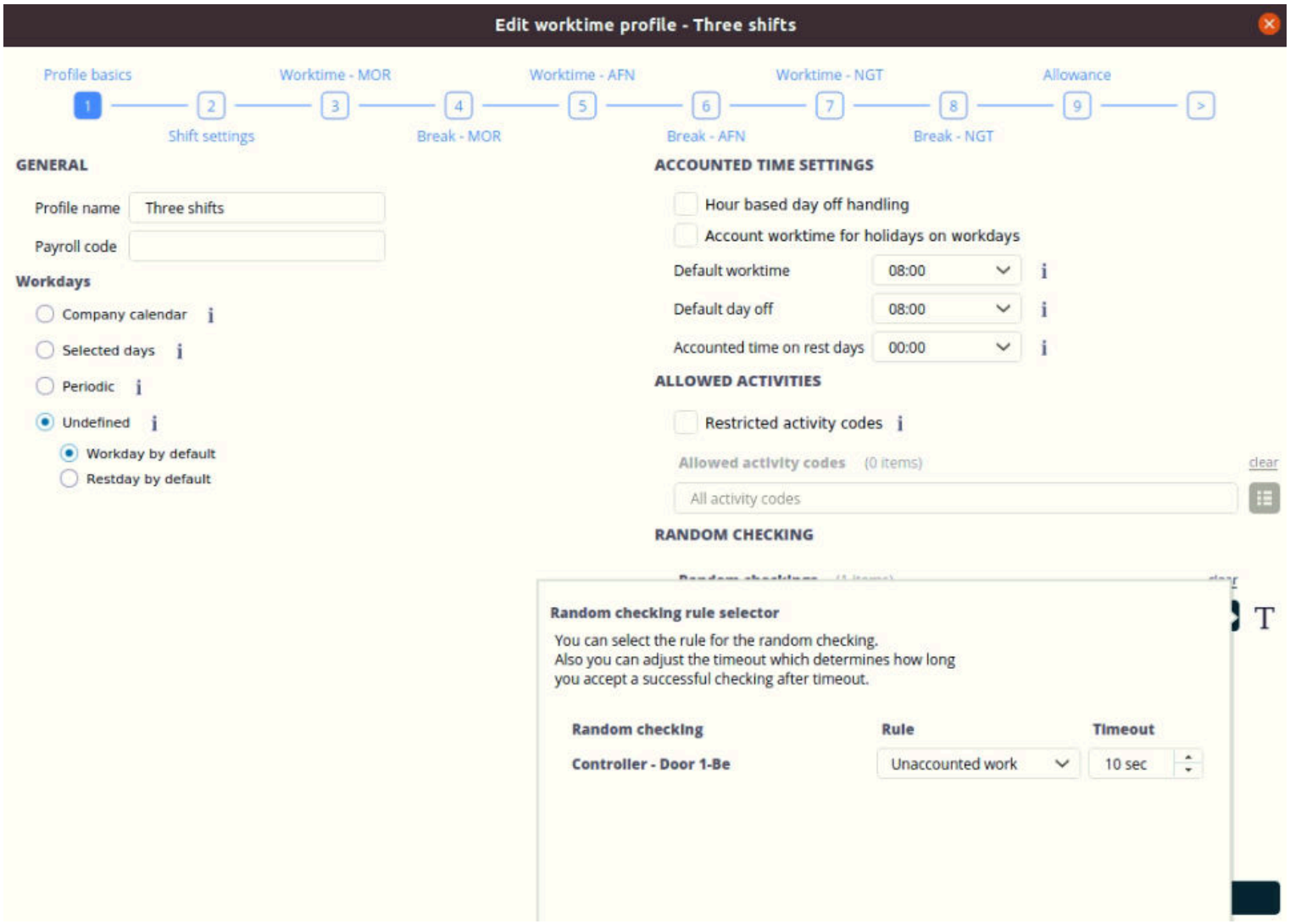


Figure 124: Configure worktime profile - basics - Configure random checking.

Shifts

If we want to use shifts that cross midnight, first we have to set which direction we want to adjust the time of day ending with the **Shift end offsets** drop down menu:

- **No offset (0-24):** the next day starts normally at 0:00. Activities done through this time will be split to two work days.
- **Towards next day:** the workday's end will be shifted towards the next day. This means that activities done in 24 hours from the "day ends" time set in the shift settings will be accounted to the actual work day. (E.g. if the shift's "day ends" setting is 8:00, then activities from Monday 8:00AM to Tuesday 7:59AM will be accounted as work time for Monday.)
- **Towards previous day:** the workday's end will be shifted towards the previous day. This means that activities done in 24 hours before the "day ends" time set in the shift

settings will be accounted to the actual work day. (E.g. if the shift's "day ends" setting is 18:00, then acitivities from Sunday 6:00PM to Monday 5:59PM will be accounted as work time for Monday.)

The following shift settings are available:

- **One shift:** only one set of worktime schedule can be defined. In case of night shifts the day's end should be aligned with the end of the shift.
- **Multiple shifts:** Multiple work schedules can be defined for each day. The day's end should be aligned with the end of each shift.

New shift(s) can be added to the profile using the **+ new** button. Shifts can be edited by double clicking on them or by selecting one and using the **edit** button.

Every shift can have a custom name and a code (this code will be visible in the work shifts calendar).

Choose the **day ends** time according to the normal work time. The system will separate activites at this time of the day, so activites in progress at this time will be accounted for two consecutive days. It is advised that the **day ends** time is chosen to a time when noone is working in this shift.

Shifts can be excluded from the automatic assignment process if we don't want them to be auto detected. These shifts will only be available by assigning them by hand. To exclude the shift, remove the check mark from the *AUTO ASSIGN* column of it.

The normal worktime column is displayed here only as a guide, editing will be possible later in the work time profile wizard. The **>** quick button can be used to jump to the selected shift's work time editor page.

The **delete** button can be used to remove unwanted shift(s) from the profile.



TIP: We don't have to assign shifts for each day beforehand. The system will fit a worktime shift with an algorithm to the actual activity data, and use that to calculate worktime data. Manual shift assignments always override this shift detection.

Accounted time settings

If the handling of days off are based on hours rather than days, it can be enabled here. By using hour based accounting the default worktime hours (amount of working hours on workdays), day off hours (amount of working hours redeemed by day off) and accounted time on rest days need to be set, which will be used when evaluating worktime. In multiple-shifts worktime profiles the amount of hours redeemed by days off need to be set for each shift.

By selecting the **Accept work on rest days** checkbox, work on rest days is *automatically* accepted, otherwise it is displayed as unaccounted work in the reports (manual accepting is still an option).

Automatical accepting of worktime has two modes:

- **No rules:** all worktime on rest days is accepted regardless of it's length or time
- **Simplified timeline:** worktime on rest days is regulated by simple rules like on normal workdays. We can limit the maximal accepted worktime, the start and end of the accepted timeframe, etc. The details can be edited later on the Work on restdays tab. These rules will be applied on all types of rest days.
- **Use normal shifts:** worktime on rest days is handled by the rules set for normal work days, all rules apply. It is important that normal timelines are applied on all rest day types, otherwise there will be no rules on rest days.
- **Explicit shift, else simplified timeline:** worktime on rest days is regulated by the simple rules set on the **Work on restdays** tab, unless extra shifts are assigned by hand, in which case the rules set for the normal work day shift are applied.

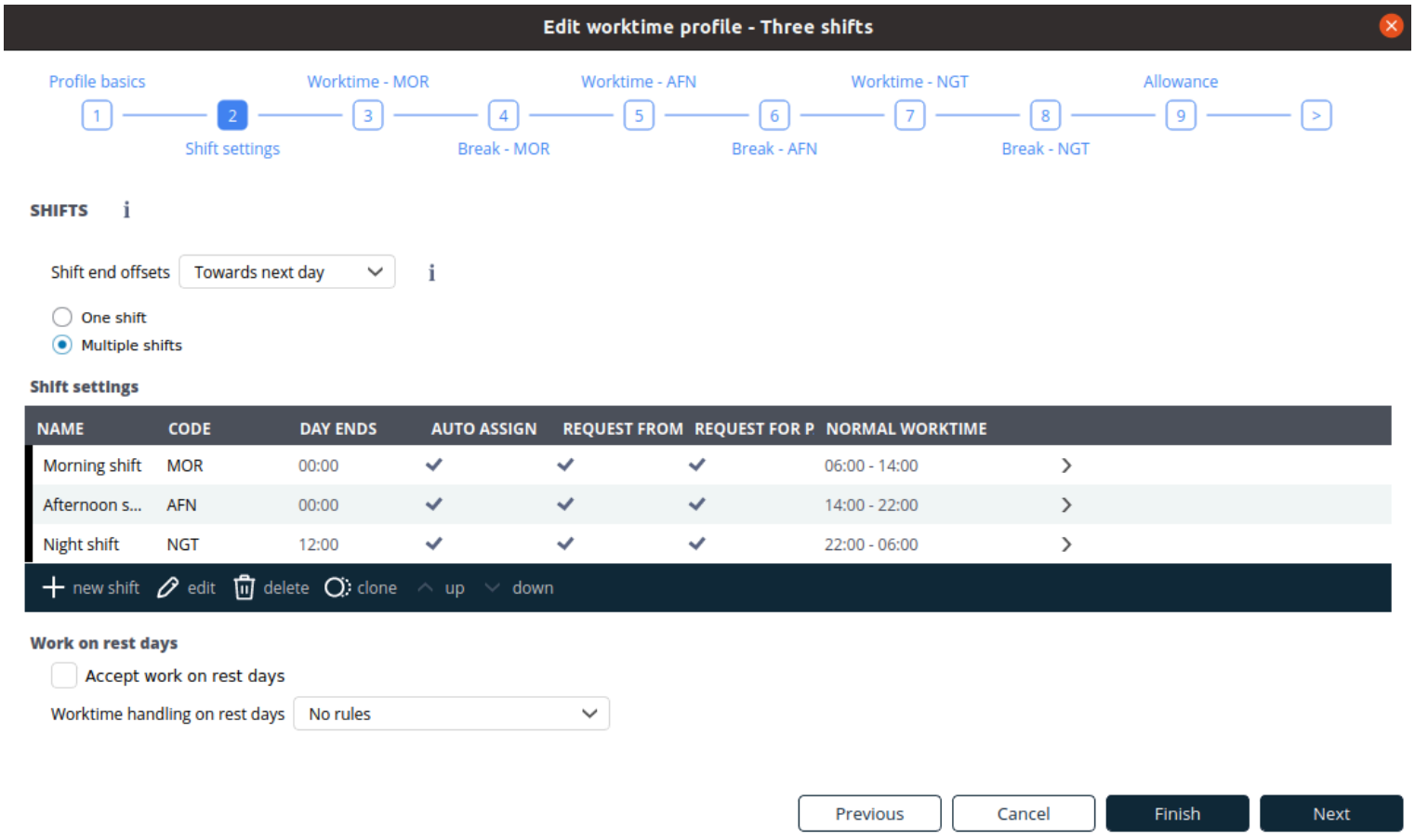


Figure 125: Configure worktime profile - Shift settings

Work time

Timelines: to set up a work schedule, first of all, we have to select the days when the schedule will be in effect. We can add multiple timelines if some days should be handled differently. For example to set up a shorter friday work schedule, add a new timeline, select the days it will be in effect and set the timeline details differently.

Worktime length: use this setting if the time of arrival and leave is not specified, only the daily workhours.

Normal attendance: by defining the work's start and end time it will appear as a green line on the timeline graph. In this case we can define further rules for the time of arrival and leaving.

Maximal worktime per day: when the daily worktime exceeds this limit the excess will be considered as unaccounted activity and will not count as worktime.

Accepted timeframe: the activity outside of this timeframe will be considered unaccounted and will not count as worktime. An exception to this is scheduled overtime. The acceptance of overtime within the band can be adjusted in Overtime settings. (mainly useful with flexible work schedules)

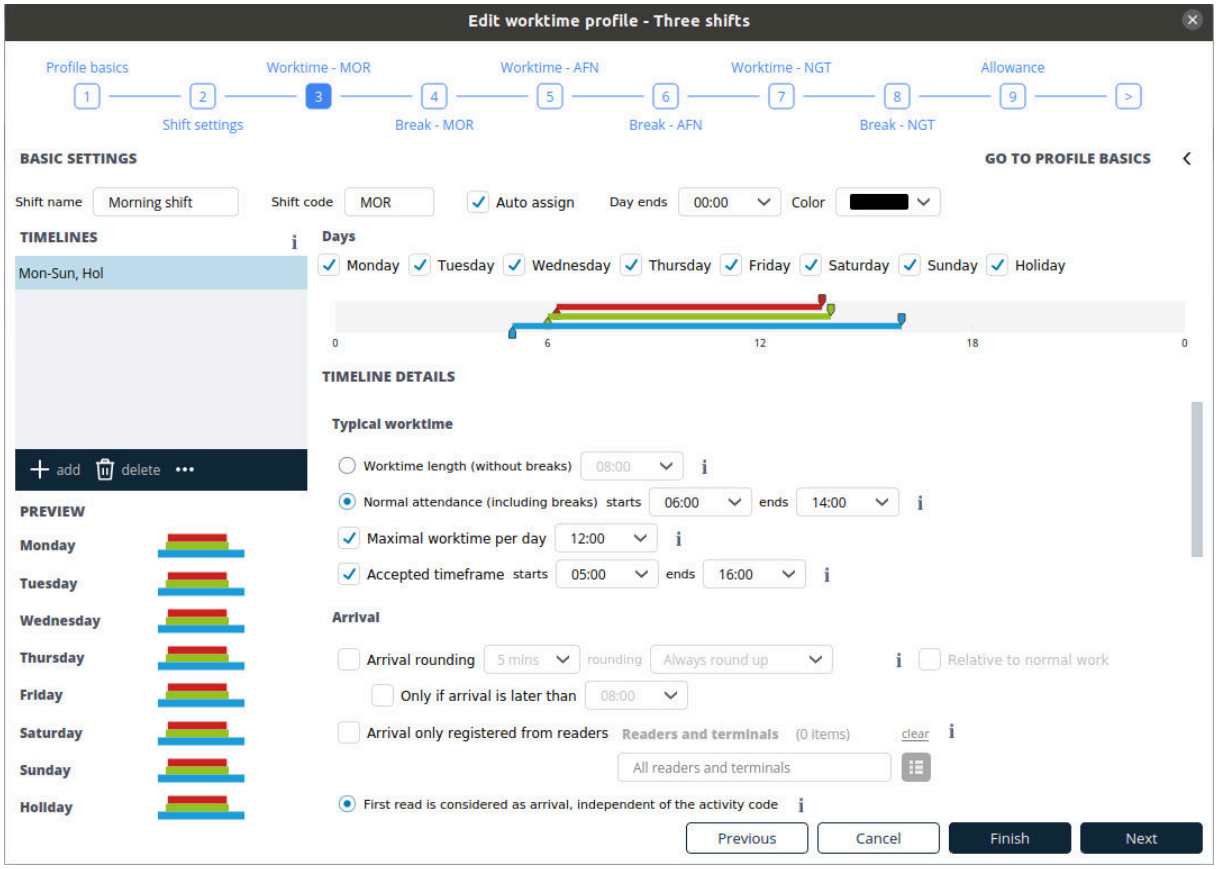


Figure 126: Configuring worktime profile - worktime preferences

Arrival

The rules of arrival are defined in this section. Arrival can be considered as the:

- first card read
- first paid activity card read

Arrival rounding: we can round the time of arrival up or down.



EXAMPLE: With 1 hour arrival rounding and round up set to 15 minutes, an arrival at 7:16 will be rounded up to 8:00 and we discard 44 minutes of work. This is suitable for sanctioning late arrival too.

Arrival only registered from readers: with this setting, we can enforce that the employees use specific readers to indicate that they started to work.

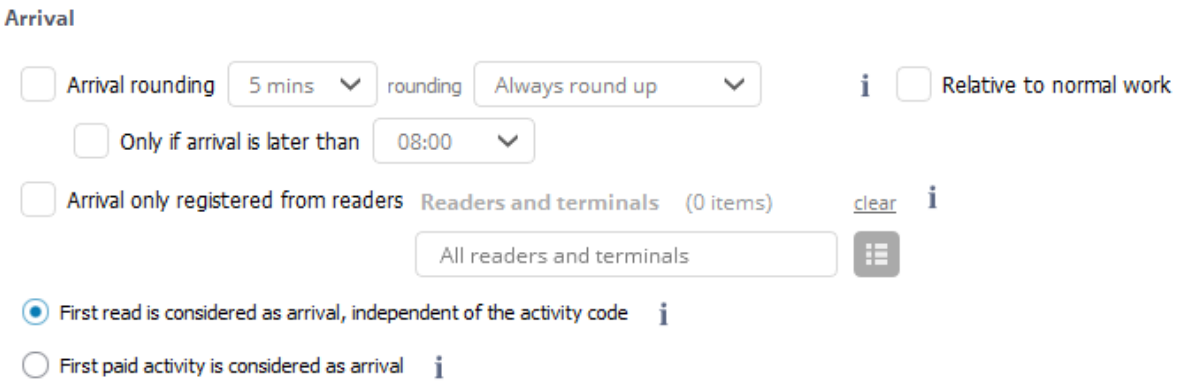


Figure 127: Configuring worktime profile - details of arrival

Leave

The rules of leave are defined in this section. Leaving can be interpreted as the:

- Last read (we use the last activity as leave even if its activity code is work).
- Last leave code: the last read where the employee used the built in “leave” code, and **if there is no such read**, we use a fixed time instead.

Leave rounding: we can round the time of leave up or down.

Leave only registered from readers: with this setting we can enforce that the employees use specific readers to register that they are leaving work.

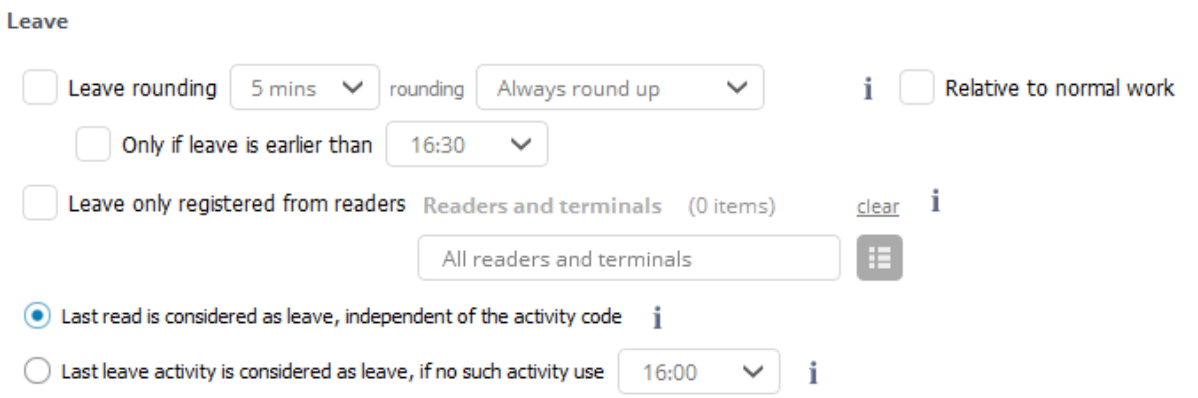


Figure 128: Configuring worktime profile - details of leaving

Worktime violations:

No action: this should be used when there is no fixed worktime or core worktime. This setting does not define rules like late arrival or leave restrictions during the day so no violations will be registered.

Late arrival: if the employee arrives after the start of the normal worktime, it appears in the reports as a violation. A tolerance can be set, so only late arrivals more than a given threshold will be reported. It can only be used when core worktime is not applicable. It is not considered as worktime.

Early leave: When the employee leaves before the end of normal worktime, the reports will highlight this violation. A tolerance can be set, so only early leaves more than a given threshold will be reported. It can only be used when core worktime is not applicable. It is not considered as worktime.

Core worktime: during the core worktime timeframe, it is mandatory that the employees are continously on the work site, working or on one of the defined break activities. If an employee leaves during this timeframe or does not start worktime before the start, it appears in reports as violations.

Minimal worktime: if the worktime is less than this value, the system will generate a violation notice.

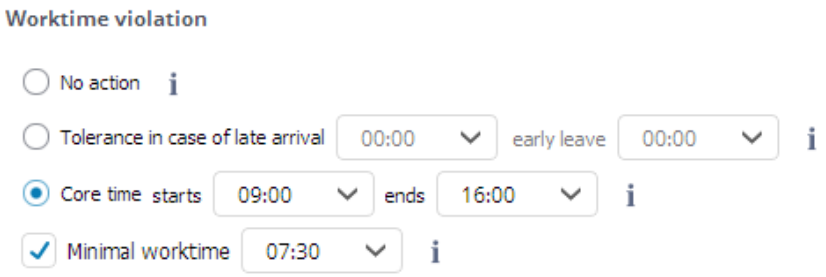


Figure 129: Configuring worktime profile - details of worktime violations

Worktime accounting

Worktime unit and rounding: the worktime unit is used to round the worktime down, to make calculations and accounting easier. The “rounding up” will round the worktime up from a given threshold.

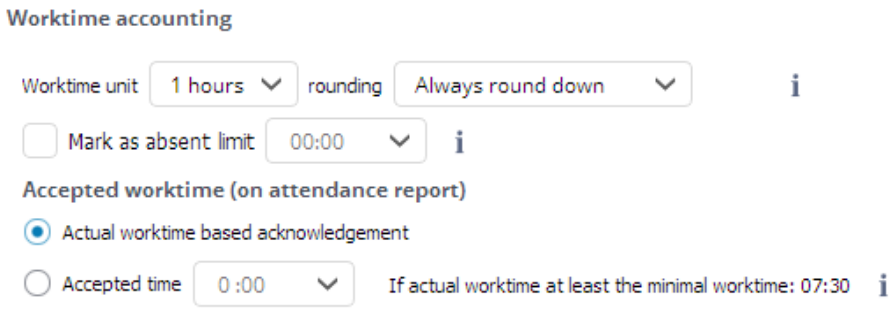


Figure 130: Configuring worktime profile - details of worktime accounting

EXAMPLE: If the work time unit is **1 hour**, and we are rounding up from **50 minutes**, **49 minutes** of work will be calculated as **0 hours** but **50 minutes** will be accounted as **1 hour**.

EXAMPLE: If the work time unit is set to **30 minutes** and we round up from **20 minutes**; **48 minutes** of work is only considered as **30 minutes** but **52 minutes** will be **1 hour** of work.

EXAMPLE: If the work time unit is **1 hour** and we **always round down**; even **1 hour and 59 minutes** will be considered as **1 hour**.

Mark as absent limit: when the daily work time is less than this value the whole day will be considered as a missed day in the accepted reports.

Actual work time based acknowledgement: the system will account the work time based on the actual movement data and the other rules.

Accepted time: if the worktime is greater than or equal to the minimal worktime, then the accepted time will appear instead of the real worktime on the attendance report.



EXAMPLE: When the accepted time = **8:00**, the minimal work time = **6:00**, and the actual work time is **7:22**, the work time in the reports will be **8:00**.



EXAMPLE: When the accepted time = **8:00**, the minimal work time = **6:00**, and the actual work time is **4:48**, the work time in the reports will be **4:48**.



EXAMPLE: When the accepted time = **8:00**, the minimal work time = **0:00**, and the actual work time is **0:00**, the work time in the reports will be **8:00**.



EXAMPLE: When the accepted time = **8:00**, the minimal work time = **6:00**, and the actual work time is **10:22**, the work time in the reports will be **8:00**.

Breaks

Breaks can be handled with the following settings:

- **Fix deduction:** intended for unpaid lunch breaks. The given value will be automatically deducted from the work time, regardless of the actual activity codes used. It can be linked to days and the accounted work hours so for example it is possible that the break deduction only happens on Mondays when the employee has worked at least 6 hours. This type of break is always deducted from the accepted work time, so the maximal worktime per day must be configured to a value which includes this break.
- **Custom breaks:** several break types can be defined linked to an activity code with their own rules, like work time threshold, usability limits and more.

The following options are available with **custom break handling**:

- **Available days:** the days when the break is allowed.
- **Activity code:** the employees will use this activity code to indicate that they are on this particular break type. It also determines whether the break is paid or not.
- **Applicable:** we can link the applicability to the work hours on a day, for example a lunch break that is only allowed if the employee worked at least 6 hours that day. Using the break otherwise generates a breaktime violation warning.
- **Time of break:** a time frame can be set, where this particular break is allowed. When the break is used outside of this interval, it will generate a breaktime violation warning.

We can define rules and limits on a daily sum and on occasional basis.

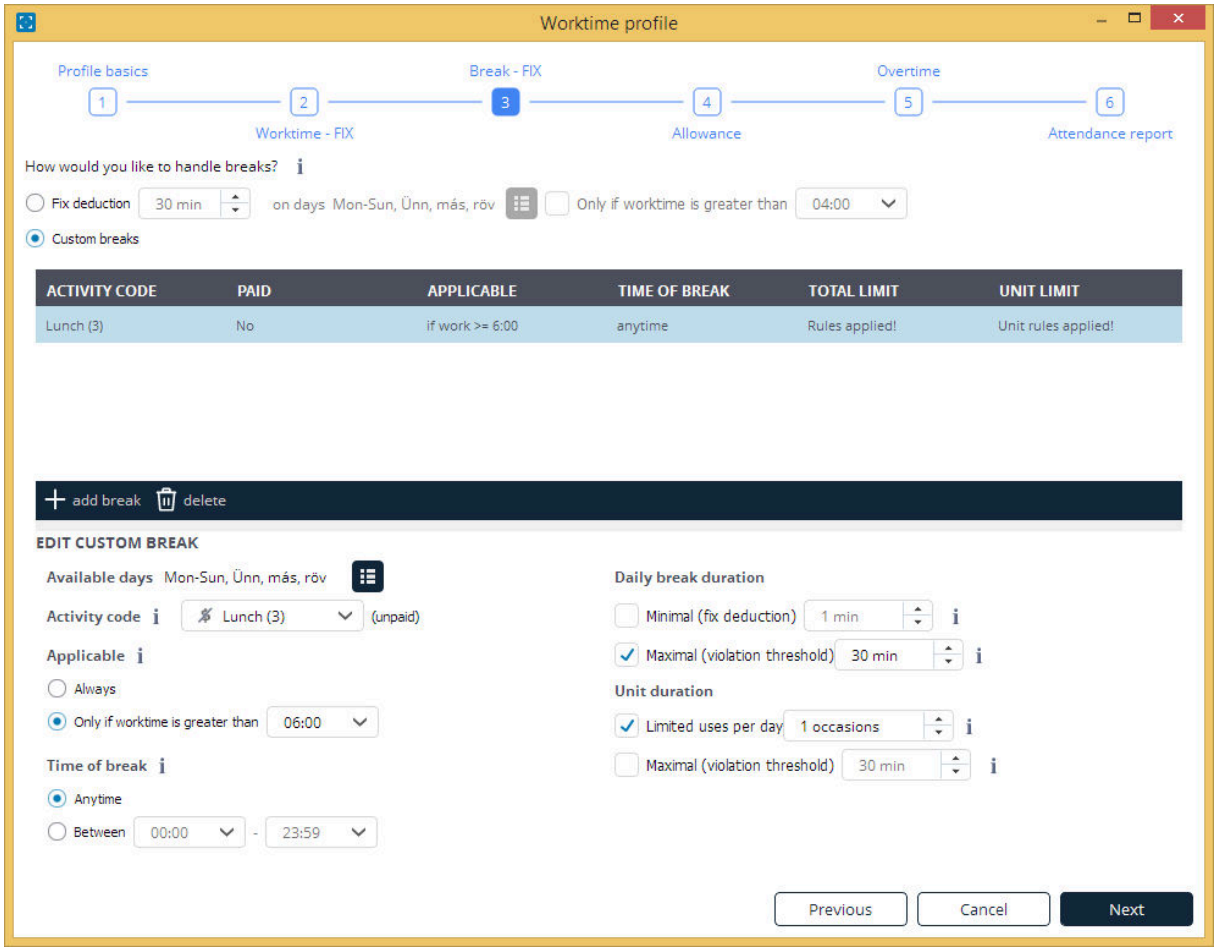


Figure 131: Configuring breaks

Paid breaks have slightly different settings from unpaid breaks.

Settings for an unpaid break

Daily break duration:

These rules are evaluated on a daily basis, using summed values.

Minimal (fix deduction): the break will be deducted from the work, even if the activity code is not used explicitly or used for less than this value. When the activity code is used, the amount above the minimal deduction will be handled normally.

Maximal (violations threshold): Breaks longer than this will be split into an allowed break and a breaktime violation interval.

Unit duration:

These rules are evaluated each time the employee uses the activity code individually.

Limited uses per day: the break activity code can only be used this many times a day. Using the activity code more will result in a violation in the reports.

Maximum (violation threshold): every time the employee uses this break activity code longer than this threshold the break will be split into a normal and a violation interval.

Settings for a paid break

Daily break duration:

These rules are evaluated on a daily basis using summed values.

Paid duration: Paid breaks can have a maximum paid duration. Breaks longer than this will be split into a paid and an unpaid part. Exceeding the paid limit will not result in a violation.

Maximal (violations threshold): Breaks longer that this will be split into an allowed break and a breaktime violation interval. This will not change the paid nature of the break, so if this is less than the paid duration, a paid breaktime violation can occur.

Unit duration:

These rules are evaluated each time the employee uses the activity code individually.

Limited uses per day: the break activity code can only be used this many times a day. Using the activity code more will result in a violation in the reports.

Paid duration: Paid breaks can have a maximum paid duration each time they are used. Break intervals longer than that will be split into a paid and an unpaid part. Exceeding the paid limit will not result in a violation.

Maximum (violation threshold): every time the employee uses this break activity code longer than this threshold the break will be split into a normal and a violation interval. This will not change the paid nature of the break, so if this is less then the paid duration, a paid breaktime violation can occur.



EXAMPLE: Minimal deduction = **20 minutes**, real activity = **12 minutes**, the system deducts **20 minutes**.



EXAMPLE: Minimal deduction = **20 minutes**, real activity = **32 minutes**, the actual deduction = **32 minutes**.

Allowance

A work time profile can define time frames where the employee is entitled to wage supplements. We can associate allowance categories to these intervals that define its type and wage bonus. Categories are managed in the overtime types window, available from the work time profiles menu. Multiple allowance types can be handled at the same time. Allowance timelines can be constrained to work time types – Normal work, Overtime, Unpaid break – and shifts.

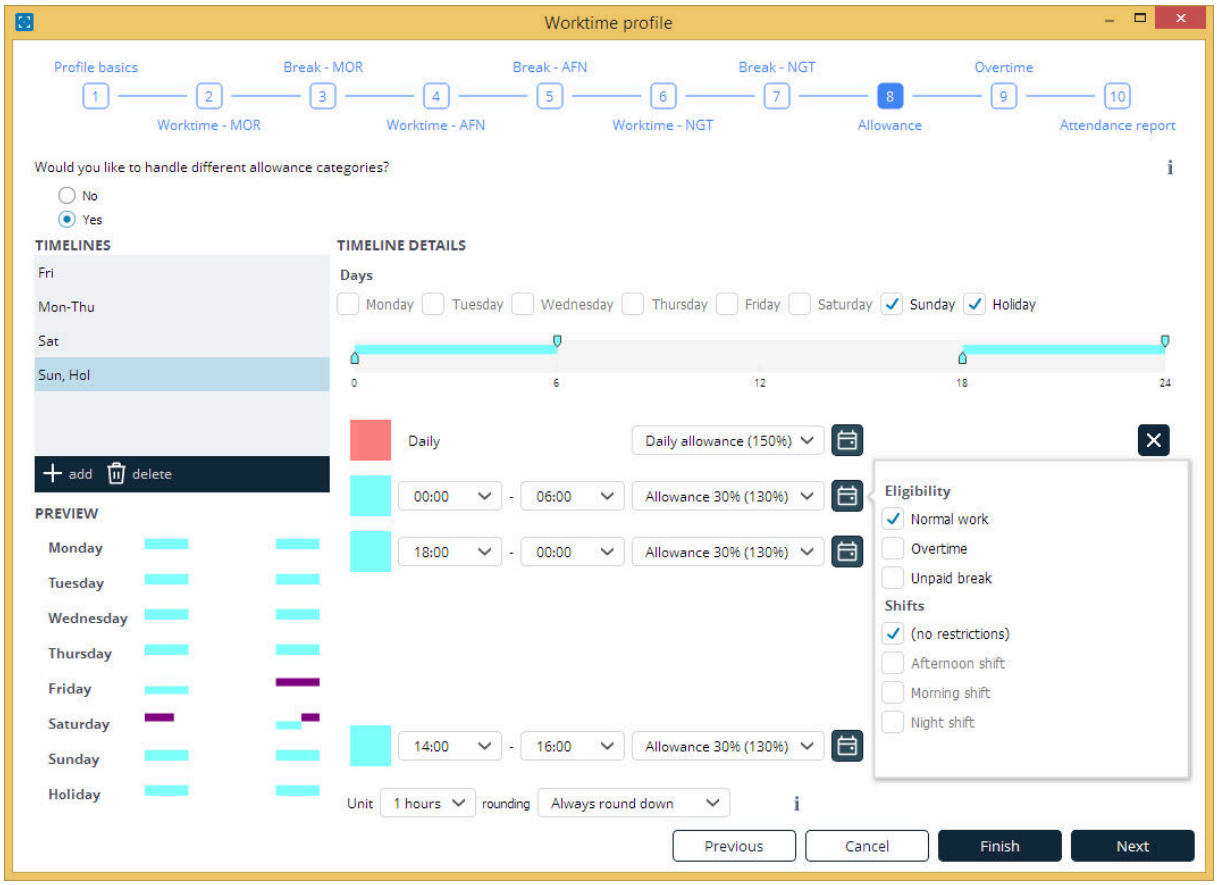


Figure 132: Configuring allowance

The daily allowance covers the whole day and is always aligned to the *day's end* setting which was configured in the profile basics settings. This means that for example in the figure above, the daily allowance set for Sunday is allotted for the whole work day, including the night shift which can extend into Monday, but the Saturday night shift which extends into Sunday is not eligible for this allowance.

Overtime

There are several ways to handle overtime:

- **No overtimes:** Choose this if no overtime is handled and no work time balance is necessary.

- **Simple overtime handling:** Work and rest days can have daily, simple overtime handling. Overtime types on workdays and rest days can be chosen, as well as the unit of overtime and rounding rules.

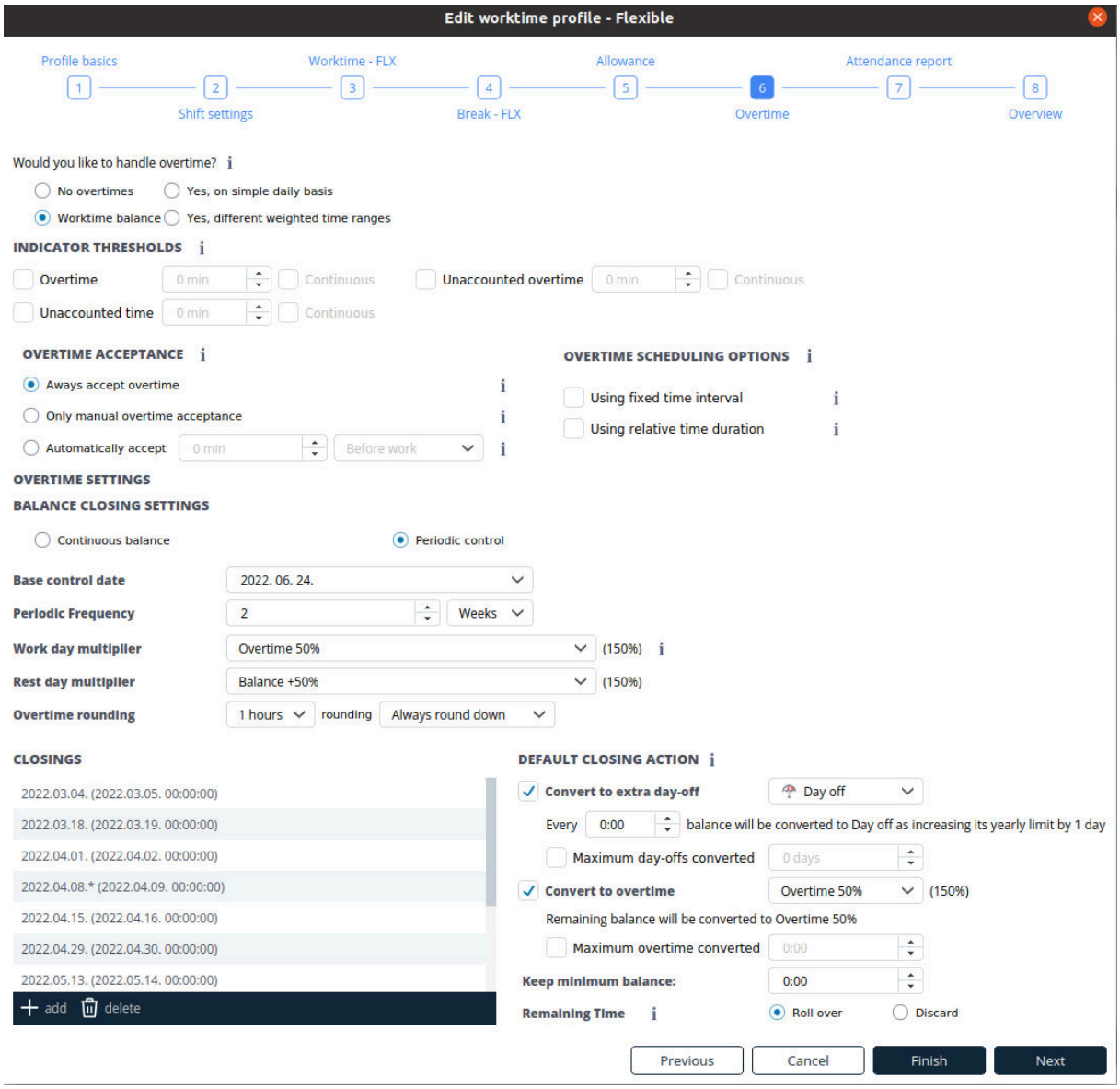


Figure 133: Overtime with work time balance handling

- **Work time balance:** An average daily work time is expected, but it is not enforced on a daily basis, instead the employee will maintain a balance, that changes each day, based on how much work hours has been accounted. It can be negative when the employee owes work hours and positive, when the employee did overtime. Work days and rest days can have different weights (work hour multipliers). Balance can be controlled continuously or periodically.

  In case of **continuous balance**, closings are not interpreted, balance is calculated from the date of the work time profile assignment.

Periodic balance, however, needs a base date (balance control date) from which the closings are calculated with the chosen frequency. If needed, additional closings can be added manually.

By setting up a **default closing action** balance can be automatically converted to days off, or overhours. Target day off type, balance-to-day off ratio (unit) and maximal amount of converted days off can be set in case of day off converting, overtime type and maximal amount of overtime converted can be defined if “convert to overtime” is chosen.

Keep minimum balance: This amount of overtime is always maintained before the automatic conversion happens, so employees always have a balance to utilize.

Remaining time: If the balance is still positive after converting, we can choose to simply discard it, or roll it over to the next balance cycle.

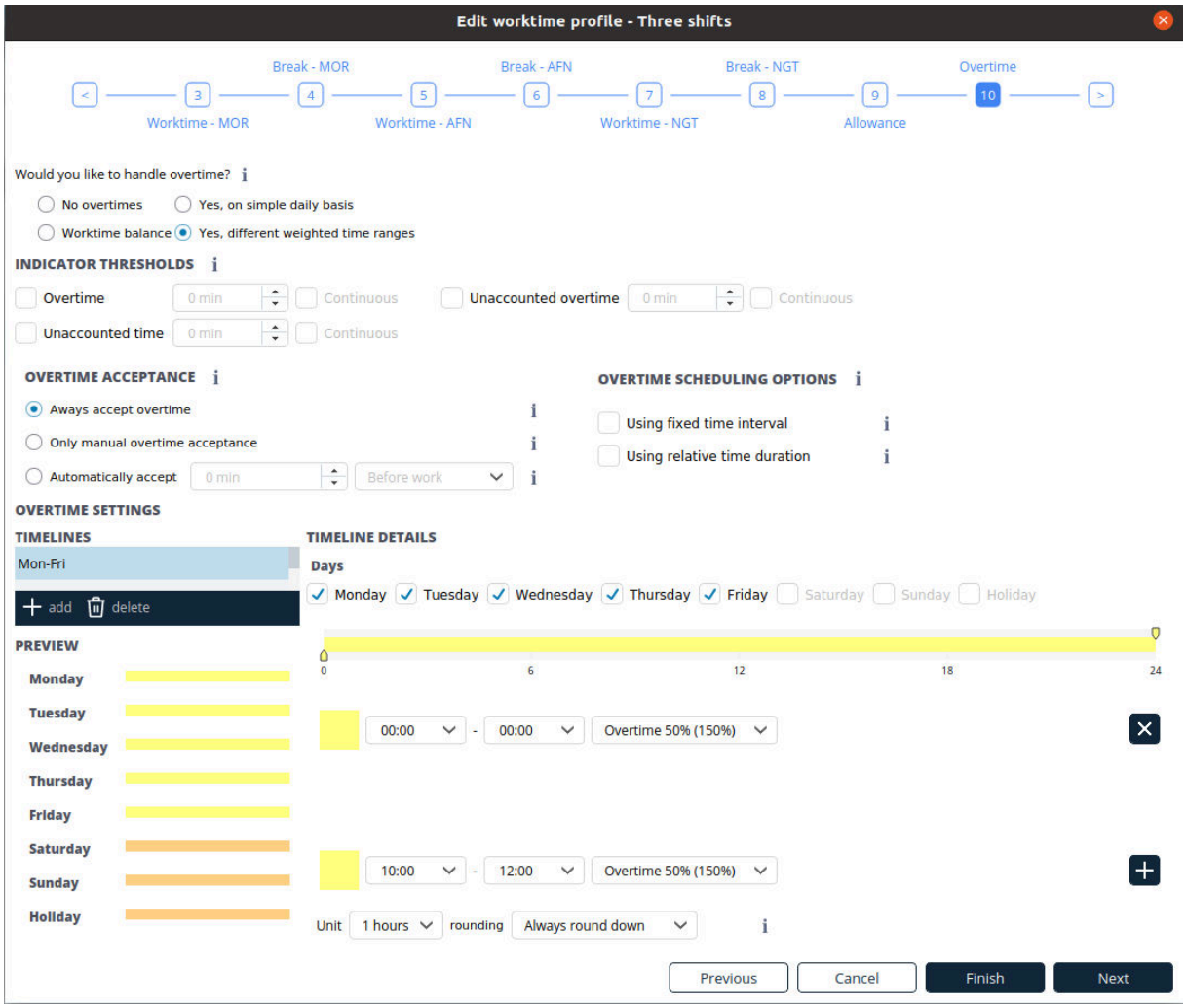


Figure 134: Overtime handling with weighted time ranges

- **Different weighted time ranges:** If necessary we can account different overtime

types for different times of the day. Each can have a different overtime type (defined in the manage overtime types window) with different wage bonus. If we check the “handle overtime on rest days” checkbox, the work done on rest days will be accounted as overtime according to the rules set on the next page. If not, work on rest days will be unaccounted and can be accepted day-by-day on the daily report. Overtime rounding will work on the sum of the daily overtimes, so the individual overtime type amounts are not guaranteed to be rounded, only their sum, and rounding happens from the end of the day.

Settings independent of the selected overtime management mode:

- **Indicator thresholds:** we can set extra indicators for the calendars of the personal web interface. Extra icons will appear on users’ days if they have overtime, unaccounted time, or unaccounted overtime that exceeds the set threshold. In the case of the continuous option, the previously mentioned markers are displayed only if the threshold value was exceeded by an independent event. In this case, the combined length of several events does not add up.
- **Overtime acceptance:** we can decide how to accept overtime in our system. We can choose from the options below:
  - **Always accept overtime:** This is the default setting. By choosing this, all overtime of our employees that they perform within the accepted range will be automatically accepted, as well as ordered overtime regardless of the accepted range.
  - **Only manual overtime acceptance:** If you select this, only the scheduled overtime will be automatically accepted, and work done on a rest day will be processed as automatically scheduled overtime. Normal overtime must be accepted manually on the appropriate report interface (Daily activity).
  - **Automatically accept:** With this setting, it is possible to set the amount of accepted overtime minute by minute, before or after worktime. In the time outside of this, unaccounted overtime is still created, which can be accepted on the appropriate report (Daily activity).
- **Overtime scheduling options:** we can dictate the ways in which we want to allow the overtime scheduling. Our possibilities are as follows:
  - **Using fix time interval:** by enabling the option, we can order overtime for a discrete time interval
  - **Using relative time duration:** by enabling the option, we can order any long overtime before or after the employee’s normal working hours

  In such ways, overtime can be ordered within the Calendar menu in the User calendar and Shift calendar sub menus, as well as in the appropriate reports (Employee monthly activity, Calendar report) is possible.

Work on restdays

If we chose to automatically accept worktime on rest days by applying simple rules on it in the profile basics, we can configure the rules here. We can limit the maximal accepted worktime, the start and end of the accepted timeframe and set rules regarding arrival and leaving. Work performed on a rest day will be accepted according to the rules for scheduled overtime.

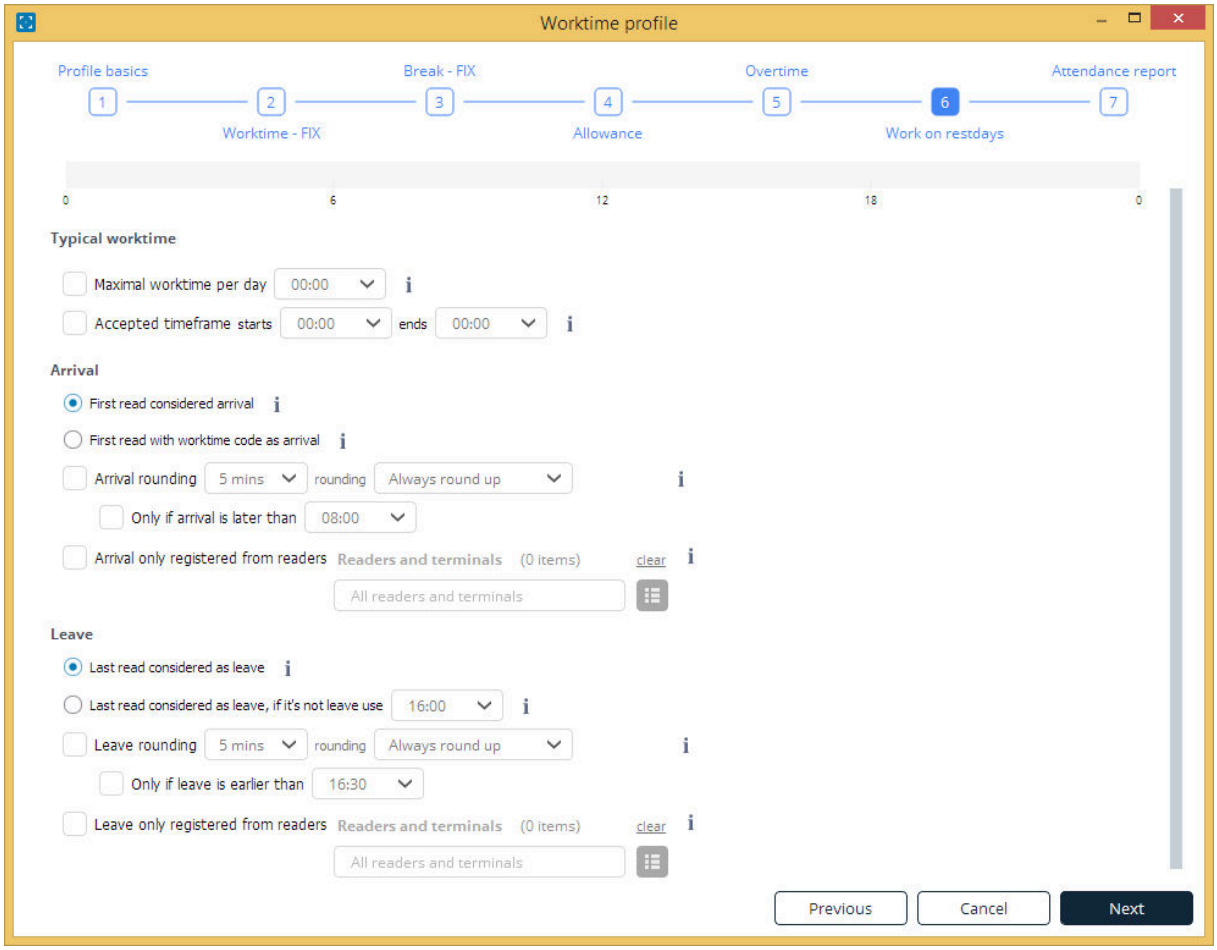


Figure 135: Configuration of overtime on restdays

Attendance report

As different worktime profiles may require different details to show up in the attendance report, the format and the displayed data can be customized here.

Optional header fields: define up to 6 fields which will be displayed in the header. Use the “list” option to customize the order of the fields to be displayed.

Optional columns: define up to 6 columns which will be visible in the table (only if the custom settings or accepted worktime based attendance report is used!) Use the “list” option to customize the order of the columns to be displayed.

Optional fields for attendance report details: We can select the detailed data on the right side of the attendance sheet, which ones we want to display.

Custom headers: Every column can be renamed optionally.

Show preview: Displays a small preview of the attendance sheet with the actual settings.

The attendance data to be shown can be:

- **Based on accepted worktime** (the output of the logged activities with the worktime rules applied on them)
- **Simplified attendance sheet**, which means the data displayed is fixed, regardless of the actual data. Simplified attendance sheet has two methods to display data:
  - **Fixed arrival and leave time**, so that arrival and leave times are always the same, which can be configured below. The user will be marked as absent if the actual working time does not reach the absence limit set in the profile, if there is any.
  - **Real arrival and fixed worktime**, so that time of arrival shows the real value, and time of leaving is automatically calculated by adding a fixed worktime to it. The user will be marked as absent if there is no valid arrival time that day or if the working time does not reach the absence limit set in the profile, if there is any.
- **Custom settings for each timeline**, which is a combination of the previous two options. Each shift can have its own setting to display values based on real or predetermined fixed arrival and leave times. Switching is done by clicking the  icon. If the fixed values option is used, the selected optional columns' values can be set too.

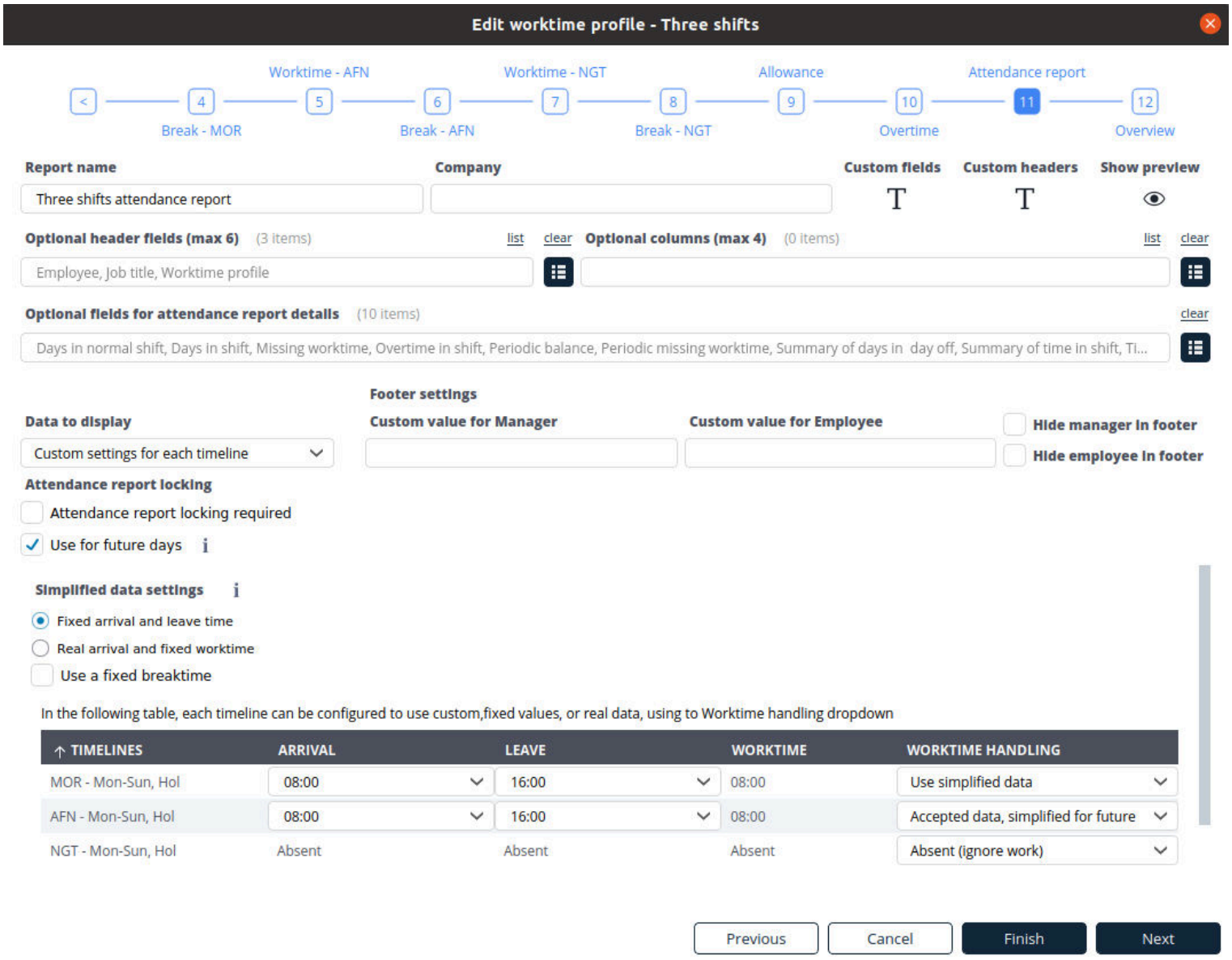


Figure 136: Attendance report settings

Overview

"Overview" is the last page of the wizard, where we can review our previous settings in a view similar to a scrollable PDF document. During the design, we strove for simplicity and good clarity, for which we created the following functions:

- Collected under each other, only the data relevant to us is displayed. Those settings that do not directly affect our compiled profile, for example because we did not enable them or because their effect is trivial due to the use of default values, will not appear.
- For easy navigation, a table of contents has been placed on the left side, in which the main headings are mappings of individual stations of the wizard, and the sub-

headings are additional internal elements within the given pages. By double-clicking on them, our “Overview” will scroll to the desired section.

- We cannot change the settings on the “Overview” page. If we notice an unwanted setting, the navigation buttons are located to the right of our main headings. With the help of these, we can go back to a previous stage of the wizard, where we can manage our settings in a customizable way.
- By clicking the icon button in the upper right corner, we can export our “Overview” to PDF format. The document is exported in the client’s current language.

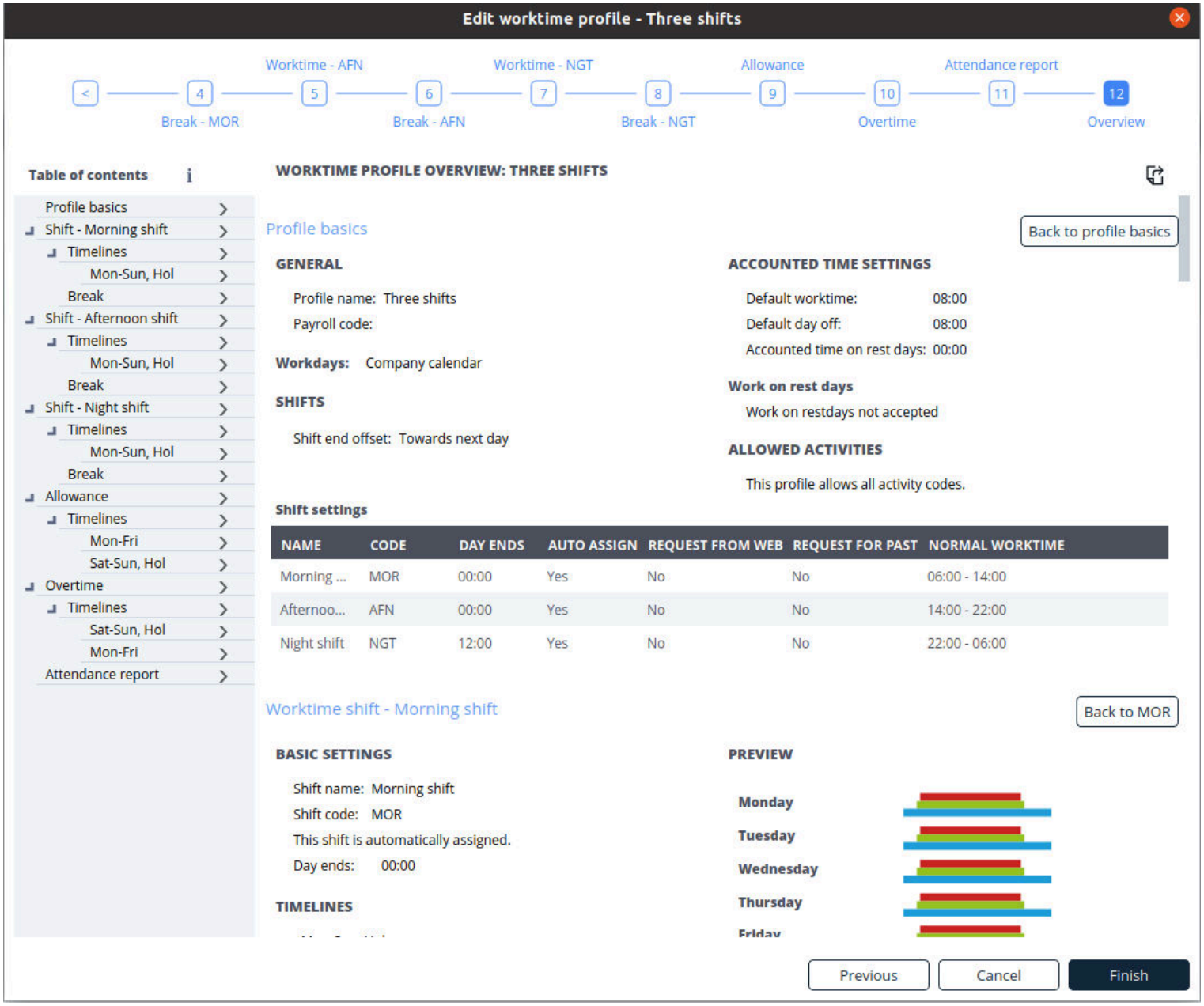


Figure 137: Profile Overview

Built-in worktime profiles

The system contains five built-in profiles, covering the most typical work schedule practices: free, flexible, hourly wages, fix, and three shifts. Understanding these can help, because it can be easier to modify and customize one of these profiles than to create a new from scratch.

In the next section we show some examples of worktime profiles.

Example - Fix (without core time)

Worktime is Monday to Friday from 8:00 to 16:30. 30 minutes of lunchtime is automatically accounted as fix deduction. Arriving 10 minutes later or leaving 10 minutes earlier is tolerated, but if it is more that that, the system marks it as a violation. The maximum worktime is 12 hours.

If the overtime happens after 6:00 and before 20:00 the system automatically counts it as overtime. Outside of this timeframe the work is “unaccounted”. On weekdays, overtime means 50% wage supplement and on weekends it is 100%. The overtime is accounted on a minute basis.

- Workday settings: using company calendar or selected days to select Monday-Friday as workdays.
- Worktime:
  - Worktime starts: 8:00 ends 16:30. The worktime shows up on the timeline as a green bar.
  - Maximum daily work: 12:00
  - Accepted timeframe: 6:00-20:00 blue bar on the timeline
- Worktime violations:
  - Late arrrival and early leave: tolerance on both is 00:10 minute
- Worktime accounting:
  - Worktime unit: 1 minute
- Accepted worktime: Actual worktime based acknowledgement
- Breaks:Fix deduction of 30 minutes, no conditions
- Allowance: not handled
- Would you like to handle overtime? Yes, on simple daily basis

Example - Fix (with core time)

Worktime is Monday to Friday from 8:00 to 16:30. 30 minutes of lunchtime is automatically accounted but if it takes more time, we deduct more. The core time is 10:00-15:00, everybody is expected to work within this timeframe, only lunch break is permitted. The maximum worktime is 12 hours.

If the overtime happens after 6:00 and before 20:00 the system automatically counts it as overtime. Outside of this timeframe the work is "unaccounted". On weekdays, overtime means 50% wage supplement and on weekends it is 100%. The overtime is accounted on a minute basis.

- Workday settings: using company calendar or selected days to select Monday-Friday as workdays
- Worktime:
  - Worktime starts: 8:00 ends 16:30. The worktime shows up on the timeline as a green bar.
  - Maximum daily work: 12:00
  - Accepted timeframe: 6:00-20:00, blue bar on the timeline
- Worktime violations:
  - Core time: 10:00-15:00, red bar on the timeline
  - No minimal worktime
- Worktime accounting:
  - Worktime unit: 1 minute
- Accepted worktime: actual worktime based acknowledgement
- Breaks: Custom Activity code: Lunch (3)
  - Available: only if worktime is more than 6 hours
  - Break length: minimum 30 minutes maximum 45 minutes (over this, core time violation)
  - Time of break: 11:00-14:00 (outside of this timeframe it is core time violation or breaktime violation)
- Allowance: not handled
- Would you like to handle overtime? Yes, on simple daily basis

Example - Hourly wages

The employees can work any time on any day of the week. We account for exactly as many hours as they are working. No lunch break or overtime or allowance bonus. Maximum worktime: 12 hours.

Worktime is rounded to an hour to make the accounting easier. 1:49 is 1 hour but 1:50 is rounded up to 2 hours.

- Workdays: every day selected
- Worktime:
  - Worktime length: 0:00
  - Maximum daily work: 12:00
  - Accepted timeframe: not defined
- Worktime violation:
  - No action
  - No minimal worktime
- Worktime accounting:
  - Worktime unit 1 hour, rounding up from 50 minutes
- Accepted worktime: actual worktime based acknowledgement
- Breaks: fix deduction 0 minutes
- Allowance: not handled
- Would you like to handle overtime? No overtimes

Example - Free

Typically lead office position. We account for 8 hours of work regardless of how many hours show up in the actual activities. No overtime, no allowance. Maximum worktime: 12 hours.

- Workday settings: using company calendar or selected days to select Monday-Friday as workdays.
- Worktime:
  - Worktime length: 8:00
  - Maximal worktime per day: not defined
  - Accepted timeframe: not defined
- Worktime violations:
  - No action
  - No minimal worktime
- Worktime accounting:

    - Worktime unit: 1 minute
- Accepted worktime: 8:00
- Breaks: Fix deduction 0 minutes
- Allowance: not handled
- Would you like to handle overtime? No overtimes

Example - Flexible

On workdays the work time frame (green bar) lasts from 8:00 to 16:30. No overtime, the profile handles balance instead. It requires a monthly average of 8 workhours, closing on the end of the month. Worktime is handled on a minute basis. At least 30 minutes of lunch break is automatically deducted, but if the employee is having lunch longer we accurately deduct the actual time.

Core time 10:00-15:00. Every employee has to be at work in this timeframe, only the lunch break is permitted. Maximum worktime: 12 hours. Outside of the accepted time frame the work will be unaccounted.

- Workday settings: using company calendar or selected days to select Monday-Friday as workdays.
- Worktime:
    - Worktime starts at 8:00, ends at 16:30. The timeline shows this interval as a green bar.
    - Maximum worktime per day: 12:00
    - Accepted timeframe starts 6:00 ends 22:00
- Worktime violations:
    - Core time starts: 10:00 ends 15:00, red bar on the timeline.
    - No minimal worktime
- Worktime accounting:
    - Worktime unit: 1 minute
- Accepted worktime: Actual worktime based acknowledgement
- Breaks: Custom Activity code: Lunch (3)
    - Available: only if worktime is more than 6 hours
    - Break length:minimum 30 minutes maximum 45 minutes (over this, core time violation)

    - Time of break: 11:00-14:00 (outside of this timeframe it is core time violation or breaktime violation)
- Allowance: not handled
- Would you like to handle overtime? Worktime balance
    - Periodic control
    - Balance control date: this selects the last day of a balance period, e.g.: 2017.03.31.
    - Periodic frequency: 1 month. Last day of month checked. This shows how often the balance is closed.
    - Below these settings the system automatically displays the date of the next closing.

Example - Multiple shifts

In our case study the employees work from Monday to Sunday in three shifts. Each shift is 8 hours long with no core time and no lunch break. Arriving 10 minutes late or leaving 10 minutes early is tolerated, but more than that is considered a violation.

Maximum worktime: 12 hours, 30% wage supplement is due between 22:00-6:00. No overtimes allowed.

Workday settings: undefined

There are three shifts in the profile: morning shift, afternoon shift and night shift. In the night shift, the day ends at 8:00 the next day, so we handle the shift stretching over midnight. Each shift has separate worktime and breaktime settings. Let's see the night shift in more detail:

- Worktime:
    - Normal attendance (worktime) starts 21:00 ends 7:00 green bar on the timelines. Notice that the timelines are shifted by the previously set 8 hours, but still 24 hours long.
    - Maximal worktime per day: 12:00
    - Accepted timeframe: 21:00-07:00 blue bar on the timeline
- Worktime violation
    - Tolerance in case of late arrival 0:10 early leave 0:10
- Worktime accounting
    - Worktime unit 1 minute
    - Actual worktime based acknowledgement
- Breaks: fix deduction 0 minutes

All shifts are configured in this fashion with different, shifted timelines.

- Allowance:
  - Create a timeline that covers monday through friday. Add a timeline section with 30% allownace bonus to 0:00-06:00 then on the same timeline add another section to 22:00-00:00.
  - Create another timeline, for saturday and sunday this time, and define a wage supplement section of 30% for the whole day(00:00-00:00)
- Would you like to handle overtime? No overtimes

Worktime reports menu

If we assigned work time profiles to the users, we can create work time reports to any time interval. The work time reports process the movement data and apply the rules set in the work time profiles to present the results in graphical and numeric format.

It is important to note that the input data (i.e. the movement data) and results of the reports can differ significantly because of the work time rules applied on them. Some reports show only the **RAW work time data which is derived directly from the movement data**, other reports display the results of the **calculations after applying the work time rules, called the ACCEPTED data**. There are some reports which can show both, the RAW and ACCEPTED data simultaneously. If manual correction is needed be careful to edit the appropriate value!



EXAMPLE: We have a work time profile with the following rules set for arrival: Rounding is set to 10 minutes and time of arrival is always rounded up. In this case if an employee arrives at 8:03AM, the RAW time of arrival will be 8:03AM too, but the ACCEPTED time of arrival will be 8:10AM.



EXAMPLE: We have the work time profile in the previous example with the following rules set for leaving: Rounding is set to 10 minutes and time of leave is always rounded down. In this case if the employee leaves at 4:09PM the RAW time of leave will also be 4:09PM, but the ACCEPTED time of leave will be at 4:00PM.



EXAMPLE: Take a look at the employee's working time in the previous examples if the work time profile has the following rules for work time: The working time unit is 30 minutes and it is always rounded down. In this case the employee's RAW working time will be 8:06 (from 8:03AM to 4:09PM), but the ACCEPTED working time will only be 7:30, because from the ACCEPTED arrival (8:10AM) to the ACCEPTED leave (4:00PM) only 7:50 has passed which is rounded down to 7:30.

Legend

In some reports the results of calculations are displayed as pictograms, so it is easy to spot days where problems or work time violations has occurred. The following pictograms are used:

 : Everyhing is ok. The employee followed all the rules within the set parameters.

 : The employee has worktime violations, like late arrival or early leave (exceeding the set tolerance), did not work enough, or left within the core time.

 : The employee did not show up, although he had a workday scheduled.

 : There were minor problems, or the employee worked on a rest day.

 : The employee was on a day-off.

 : There is no valid worktime profile assignment on the given day.

 : The work day has not ended yet, the result is unavailable.

All reports are quickly available from the start screen. Some reports can be automated or generated in batch, which is explained in the Start page section after the detailed overview of all reports.

Creating a report

On the new report tab, each report tile represents a different report type that opens in a new tab.

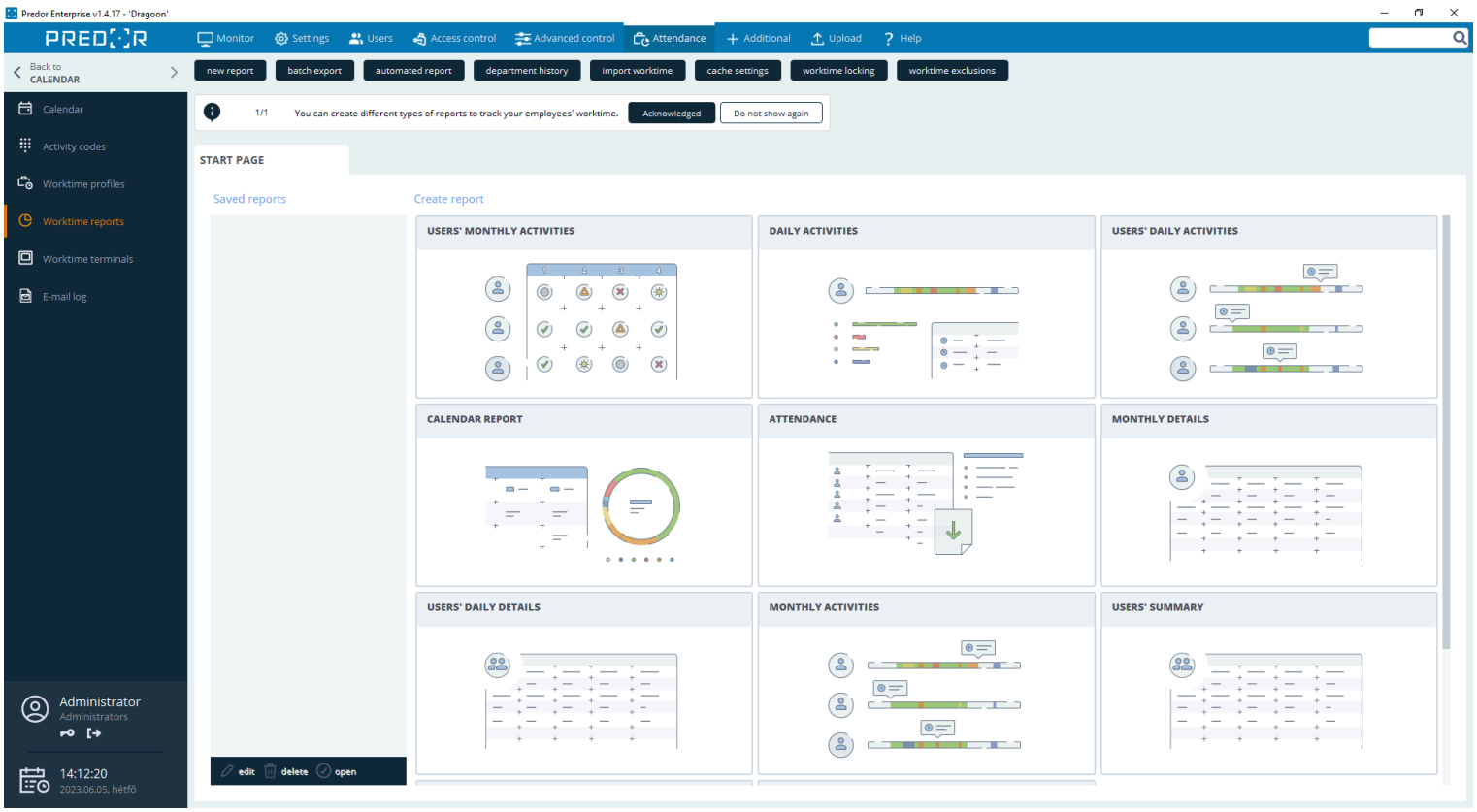


Figure 138: Work time report tiles on the start screen

When we open a new tab and execute a report with a given set of parameters, the current settings can be saved with the save icon above the parameter settings. Saved reports are listed on the left side of the start page. Clicking on these will open the report with the corresponding settings.



TIP: Let's execute a report on a relative time period - for example yesterday, last month, then select some employees. If we save this report, we will always get the data relative to the current date.

Users' monthly activities

Select the time period and multiple users then click on the **execute** button to calculate the report. The horizontal header indicates the days of the report's time frame, and the first column shows the display names of the employees.

This report displays pictograms (see: legend) corresponding to the RAW work time data to provide a quick overview of multiple users' monthly activity so work time violations can be easily spotted. By hovering over a pictogram a pop-up window is displayed with additional information about the calculated data. By double clicking on a cell a daily report is

opened for the selected user and day where further analysis can be done.

Both the horizontal and the vertical headers are navigation links to a more limited but detailed report. Double clicking on a cell will open a detailed daily report for that particular day and person, where we can even edit the activities. By clicking on the vertical header, we can open a "users' daily activities" report with the activities for all selected users on that day. Clicking on a user name will open a calendar report for that employee.

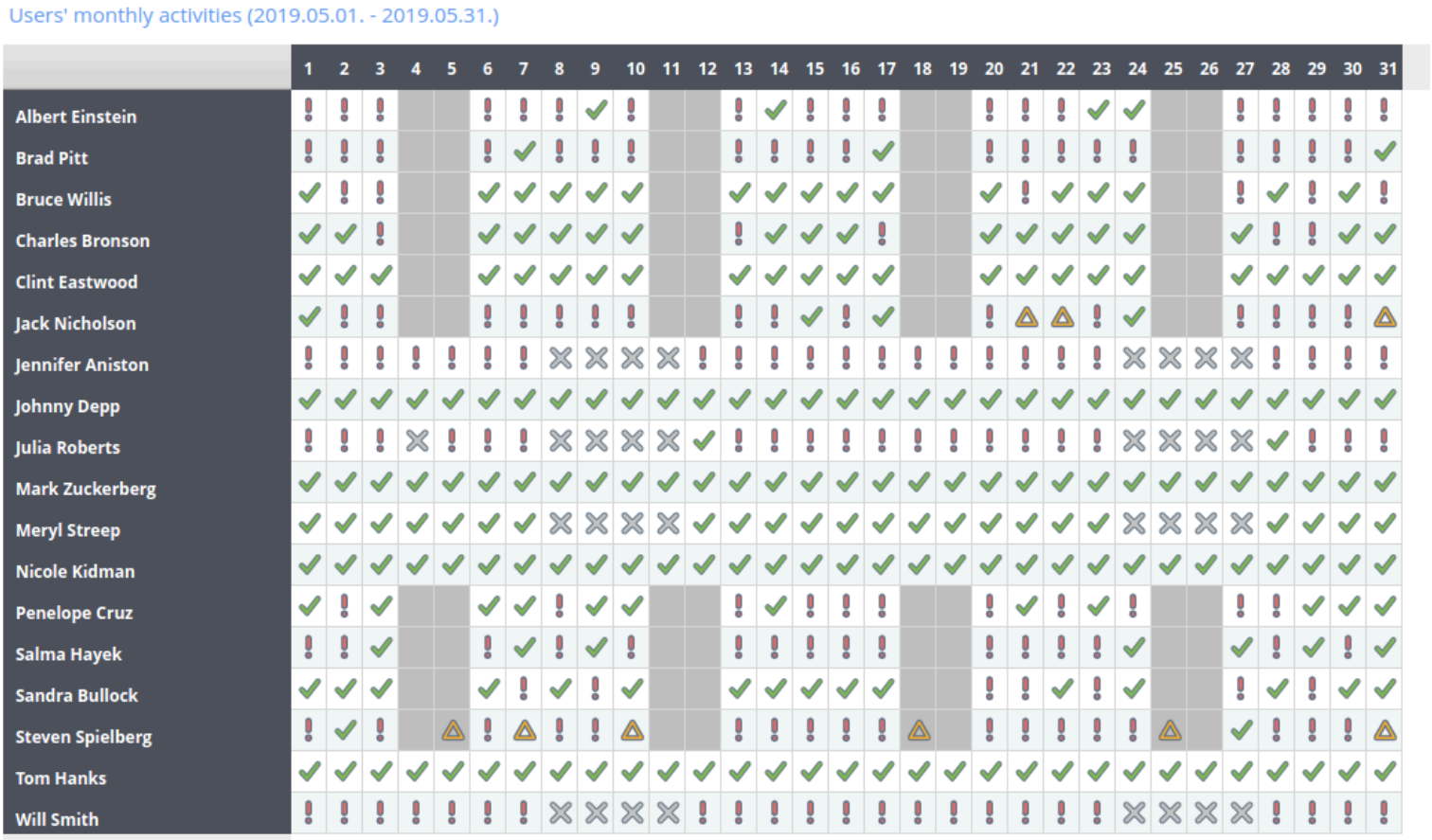


Figure 139: Users' monthly activities report



TIP: Hovering over a cell will display a tooltip with more information.

Use the violation filter to highlight specific work time violations. You can hide people who don't have the selected type of violations in the current view by using the *Hide filtered rows* checkbox.

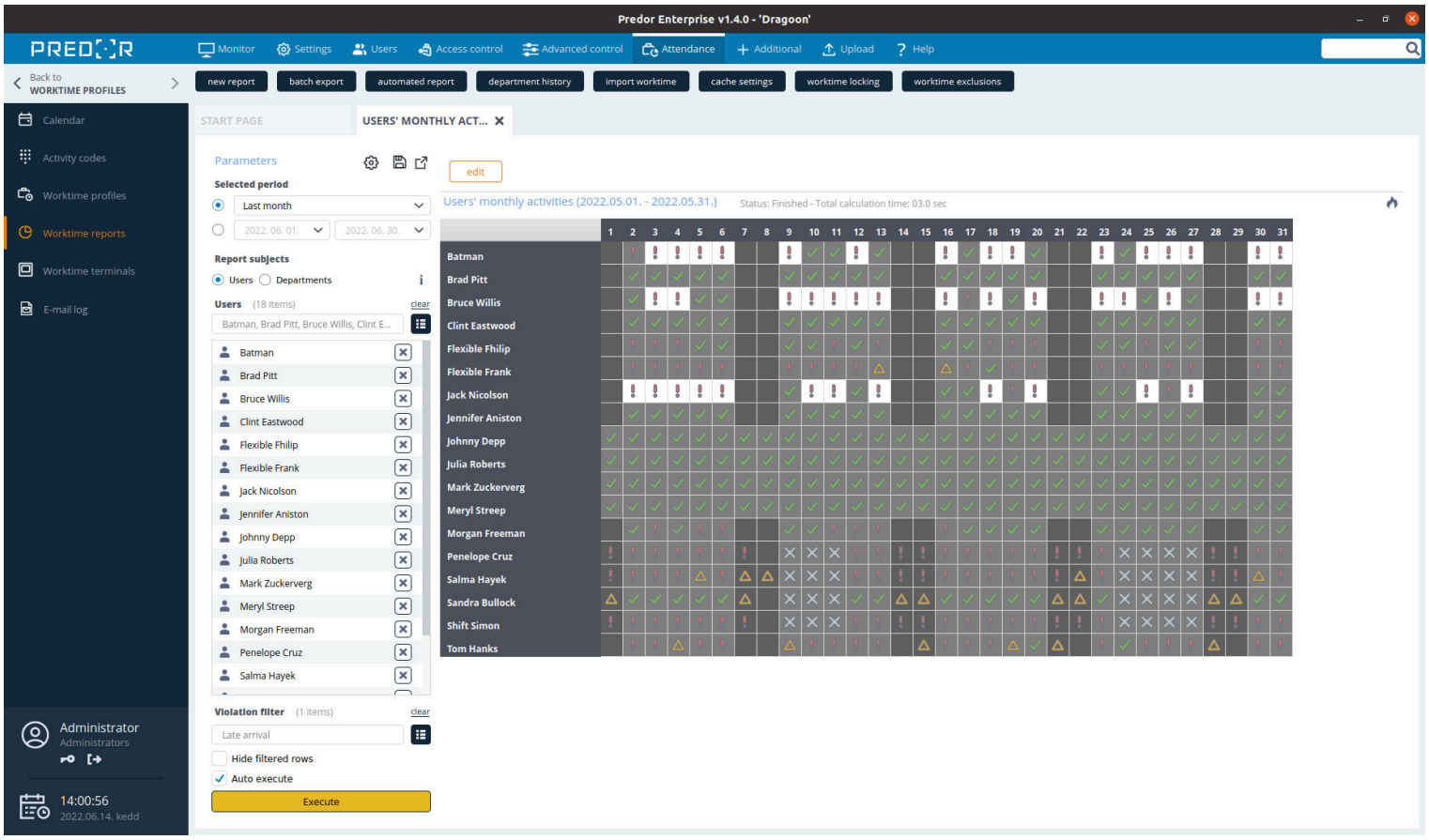


Figure 140: Users' monthly activities report with work time violation filter applied on it.

This report can be edited, and by right clicking on one or more cells the following operations are available:

- **Day-off:** the selected days can be converted to days off by choosing a day off type.
- **Shifts:** employees can be assigned to the selected shift just like in the work shift calendar.
- **Rest day:** selected days will be converted to rest days
- **Schedule overtime:** the option becomes available by using the appropriate overtime settings belonging to the profile. In doing so, the superior may require the employee to work overtime before or after the normal worktime, or at an arbitrary interval.
- **Fix day as...:** Inserts RAW activities to fit the normal work time of the selected shift, so the selected days will be corrected quickly.
- **Fix arrival and leave as...:** Overwrites the arrival and leave times to fit the shift's normal worktime. All activities remain untouched.
- **Reset:** undo all manual edits and restores the original work time data.
- **Reset day-offs:** removes days off and restores the previous state of the day.

- **Work day:** converts the selected days to work days.

Daily activities

After selecting a date and a user, the execute button below runs the report.

Using the buttons on the upper right corner of the report the previous, the next day's report and the user's data sheet can be viewed.

This report shows two timelines (RAW and ACCEPTED) representing the user activities, below it to the right lists the corresponding activities, and on the left it displays numerical data for both timelines. This is the only report where editing both the RAW and ACCEPTED activities are possible. Additionally the calculated values are also editable so for example the time of arrival and leaving can be corrected here.

Above the list of activities we can choose to view the RAW or ACCEPTED data in the list. We can follow the activities on the coloured bars. Clicking on a row in the activities table will select the corresponding time interval bar on the timeline.

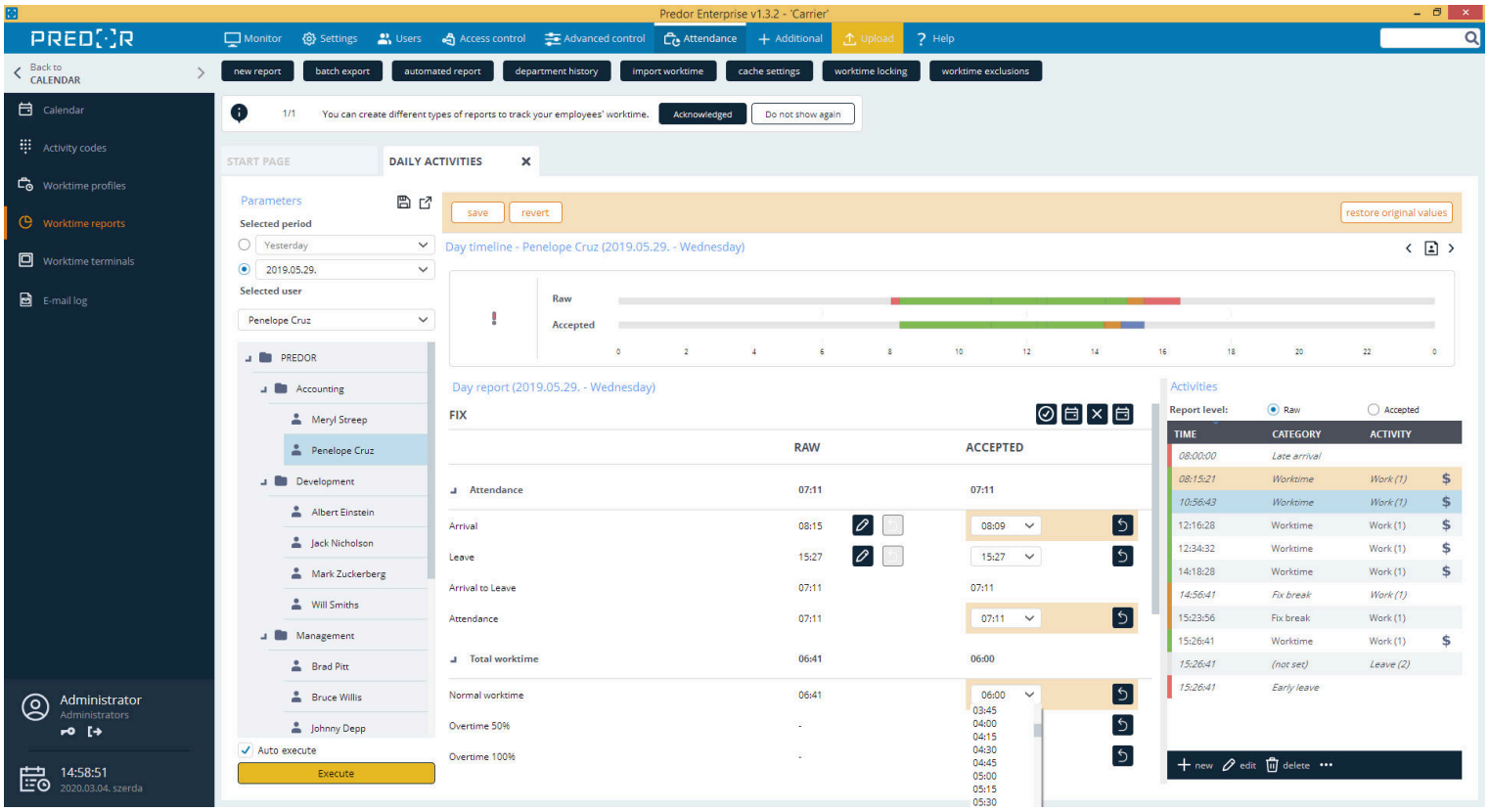


Figure 141: Daily activity report with manual corrections highlighted

By default we use the following colours:

- Green: paid work time

- Orange: breaktime
- Red: violation (core time violation, late arrival, early leave, not enough work, breaktime violation)
- Yellow: overtime (but it's colour can be changed by editing the overtime type)
- Blue: unaccounted activity. It can occur under different circumstances for example unhandled break activity, rounding or not permitted work on rest days

The report overview shows both the raw and accepted times summed. In the **raw** column the arrival, leave and every other value is calculated using the raw timeline. The **accepted** values can be different due to rounding and other rules.

The activities which are currently assigned can be listed on the selected user's day under *Current Assignments*.

At the bottom of the report is the **Audit log** which lists the work time corrections for the selected employee and date.

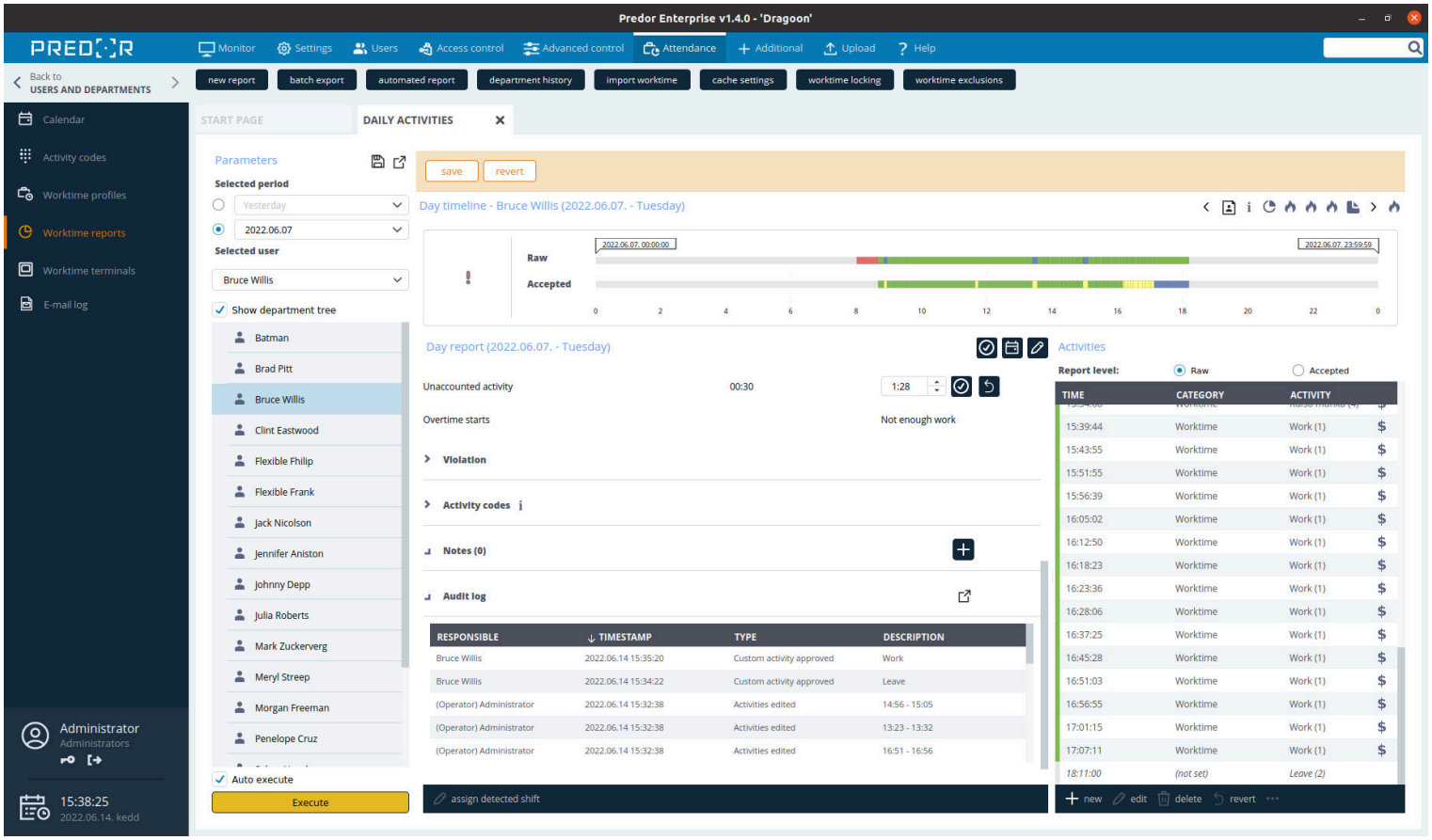
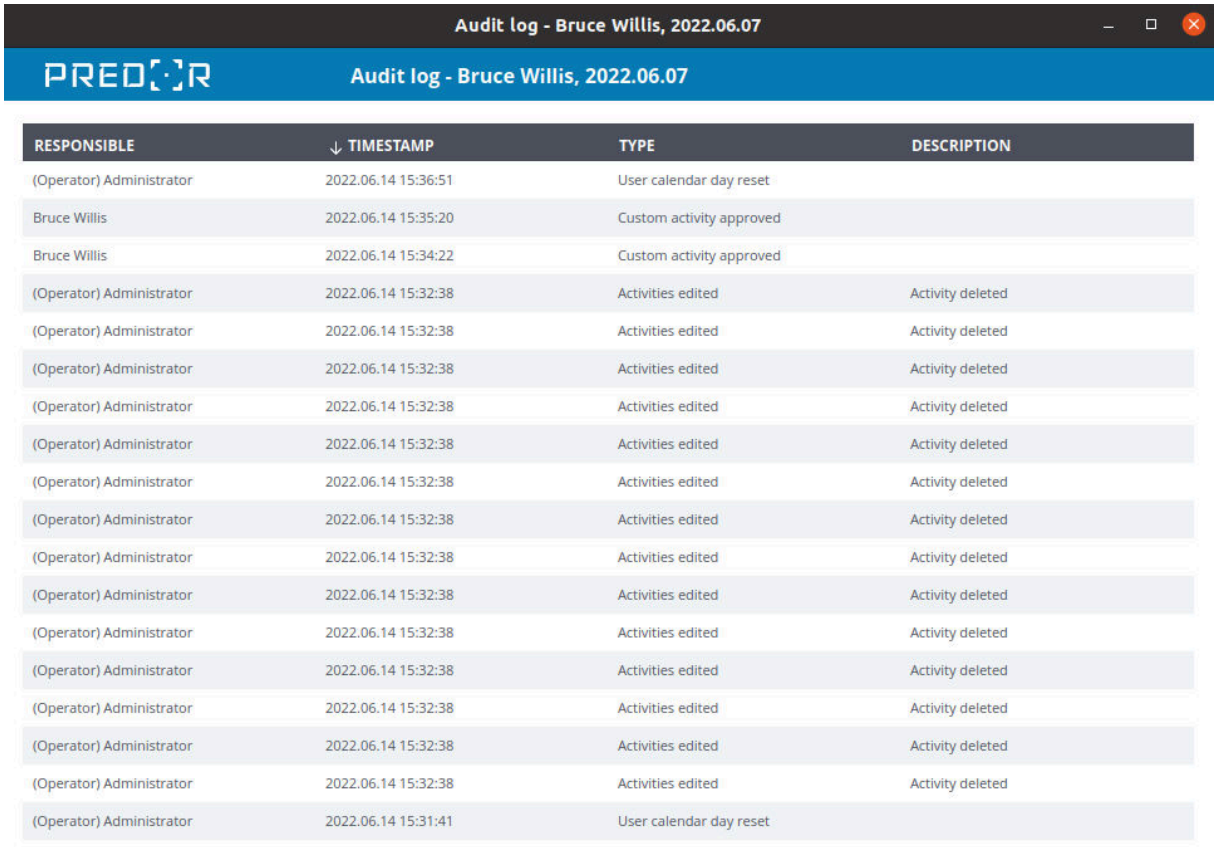


Figure 142: Audit log in the Daily activities report

The **Audit log** can also be opened in a separate window by pressing the button, for easier browsing.



RESPONSIBLE	↓ TIMESTAMP	TYPE	DESCRIPTION
(Operator) Administrator	2022.06.14 15:36:51	User calendar day reset	
Bruce Willis	2022.06.14 15:35:20	Custom activity approved	
Bruce Willis	2022.06.14 15:34:22	Custom activity approved	
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:32:38	Activities edited	Activity deleted
(Operator) Administrator	2022.06.14 15:31:41	User calendar day reset	

Figure 143: Audit log separate window

Editing: In this report, we can manually change the values by clicking on the orange edit button. Every value is recalculated after saving. If we made a mistake, the "restore original values" button can clear our manual changes.

EXAMPLE: If an employee forgot to register an activity using their ID on-site we can correct it by editing the RAW activities. This way the system handles it as if it was a normal activity registration made by the user and recalculates all the work time data, including the ACCEPTED values.
But if it isn't important to align every activity of the employee and we just want to accept the work, we can just correct the ACCEPTED work hours on that day directly, bypassing all movement data and calculations involved.

By pressing the button "**Remove entries**" , we can view the user's entries from the web, and we have the option to delete them grouped by publisher.

During editing, the calendar icon in the worktime profile row can be used to assign the user into a shift manually, or set the day as a rest day or day off, just like in the user

calendar. In case of missing work time data, this button provides two methods for quick corrections:

- **Fix day as...:** Inserts RAW activities to fit the normal work time of the selected shift.
- **Fix arrival and leave as...:** Overwrites the arrival and leave times to fit the shift's normal worktime. All activities remain untouched.

If we want to edit the current or a future day, by default only "**Restricted editing options**" are available. This indicates to the operator initiating the editing that the given day is not yet considered closed, i.e. new working time events may arise as a result of real card swiping. If you absolutely want to edit the current or a future day, eventually we have an option. The "**unrestrict**" button enables full editing, from here on we can edit the day just like a past day.

The **"Accept work"**  button can be used to override the default profile settings and accept or decline work hours. This button can create overtime in work time profiles which do not handle overtime normally. The following options are available:

- **Profile default handling:** this is the default handling method by applying the rules set in the worktime profile.
- **Accept with profile default handling:** work time will be acepted as it would be a normal work day, applying the rules set for work days in the profile.
- **Worktime is not accepted:** overrides the worktime, converts the paid activites to unaccounted.
- **Accept as balance:** available only for profiles handled with work time balance. All paid acitivities will be accepted with the chosen work time balance mmultiplier.
- **Accept as overtime:** all paid activities are accepted as overtime. We have to choose which type to account to:
  - **Accept as overtime according to profile:** accept overtimes set by the rules in the worktime profile's overtime page
  - **<Other overtime type(s) defined in the system>:** all paid activities are converted to the selected overtime type
- **Mark day as absent:** sets the accepted work time to 0:00 and marks the day as absent for this employee, as if they were missing.
- **Do not mark the day as absent:** removes the absent status from the day, the work time will be evaluated as the last valid setting.

After **editing the "RAW" arrival and leave or activity data** everything is recalculated before saving, so we can evaluate the report and save the result, if we are satisfied with it.

In editing mode we can attach a note to the user's day by pressing the "add"  button in the *Notes* field. Further customization is available by using the button where it can

be set whether the note is visible for employees or responsibe person in the work time web. The notes can be deleted with the button.

The "**Activities**" table lists the activities ordered by their starting time. Typically these activities are associated with a card or badge identification, but some activities are inserted because a profile rule dictates them - like break or core time violation. These *profile generated activities are marked with italics* in the table. Above the table, we can choose to show the raw or the accepted details.

Activity editing: The card-associated activities are editable by selecting them in edit mode and clicking on the edit button on the toolbar below the table. We can modify several lines at once by selecting them and pressing the right mouse button and selecting the correct activity. In the pop-up window we can change the activity code and the time frame of the activity too. We can also add new events to the activities, which can be a time period or point-based. By adding a time period event, you can correct overtime or balances, for example. With a point-based event, you can correct missed card swipes. An edited activity will appear as a yellow line in the table. Edited activities on raw or accepted level are handled differently. The work time rules are still applied on raw activities, so they can change categories (eg.: breaktime rules, or overtime rules can change them), however, the activities edited on the accepted level are not handled by the rules, so the category is available for editing and it can violate rules set in the work time profile (we can add overtime into a profile that does not handle overtime, or break rounding rules).

Users' daily activities

This report uses the same visual representation as the "Daily activities" and shows the **"RAW"** and **"ACCEPTED"** timelines for multiple users on a selected day. The "accept work as" button on the bottom of the report allows quick work time manipulation for the selected users. Work time can be declined, accepted or converted to overtime. This button is enabled only if the users selected in the report are assigned to profiles which handle overtimes and allowances the same way.

The details button opens the Daily activities report for that particular person.

The most important (raw) attendance data are listed on the left of every timeline, along with pictograms which represent the calculated raw data. For meanings of the pictograms see: Legend.

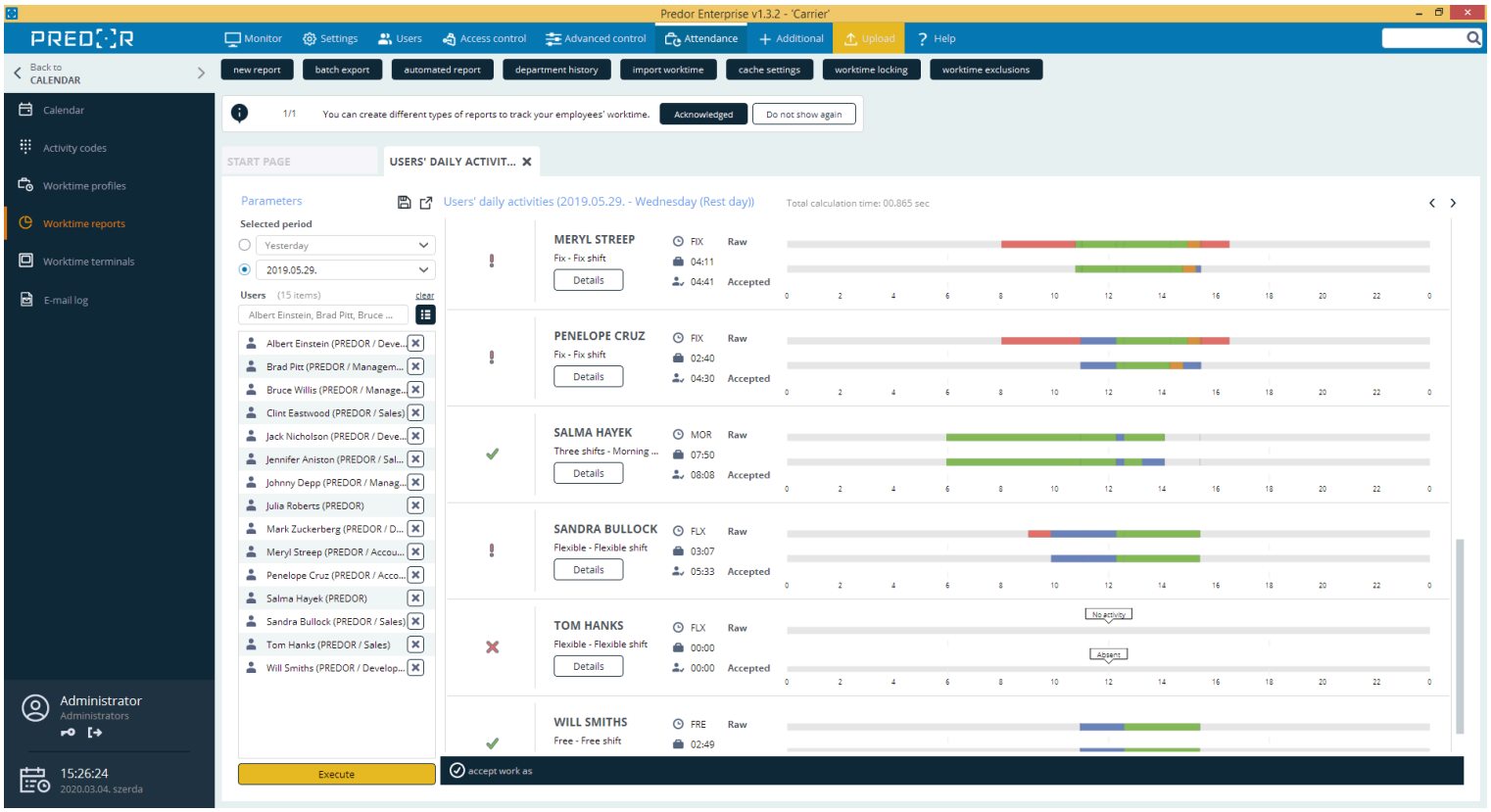


Figure 144: Multiple users' daily activities report

Calendar report

The calendar report shows the monthly activity of an employee in a calendar with customizable cell data. Along with the pictograms which represent the RAW data, each cell can hold up to 3 different data points about the day, selectable in the lower left corner of the report under "Cell data".

On the right side, two different views are available; a donut chart that shows the distribution of activities during the month and the total time spent with each activity, and a detailed breakdown of the selected day, configurable in the "Detailed data" selector in the lower left corner. We can switch between views with the chart and paper icons on the upper right corner.

Editing mode can also be activated on the report, in which case the following actions can be performed by right-clicking on a cell:

- **Day-off:** choosing from the day off types managed in the system, we can declare the designated day as a day off.
- **Shifts:** the user can be assigned to a shift on the selected day, just like in the shift calendar.
- **Extra shift:** the user can be assigned to a shift on the selected rest day. If we issue

an extra shift on a working day, the day automatically becomes a rest day.

- **Rest day:** we can declare the designated days as rest days.
- **Fix day as...:** the RAW level activities corresponding to the shift are inserted to cover the normal timeline of the shift so that the day can be quickly declared as correct.
- **Fix arrival and leave as...:** the activities will remain, only the arrival and leave will be adjusted to the normal timeline of the shift.
- **Reset:** delete all manual changes, restore the original data.
- **Reset day-offs:** restoring the granted day off to its previous state.
- **Reset shifts:** restoring the issued shift to its previous state.
- **Work day:** declares the given day as a workday.

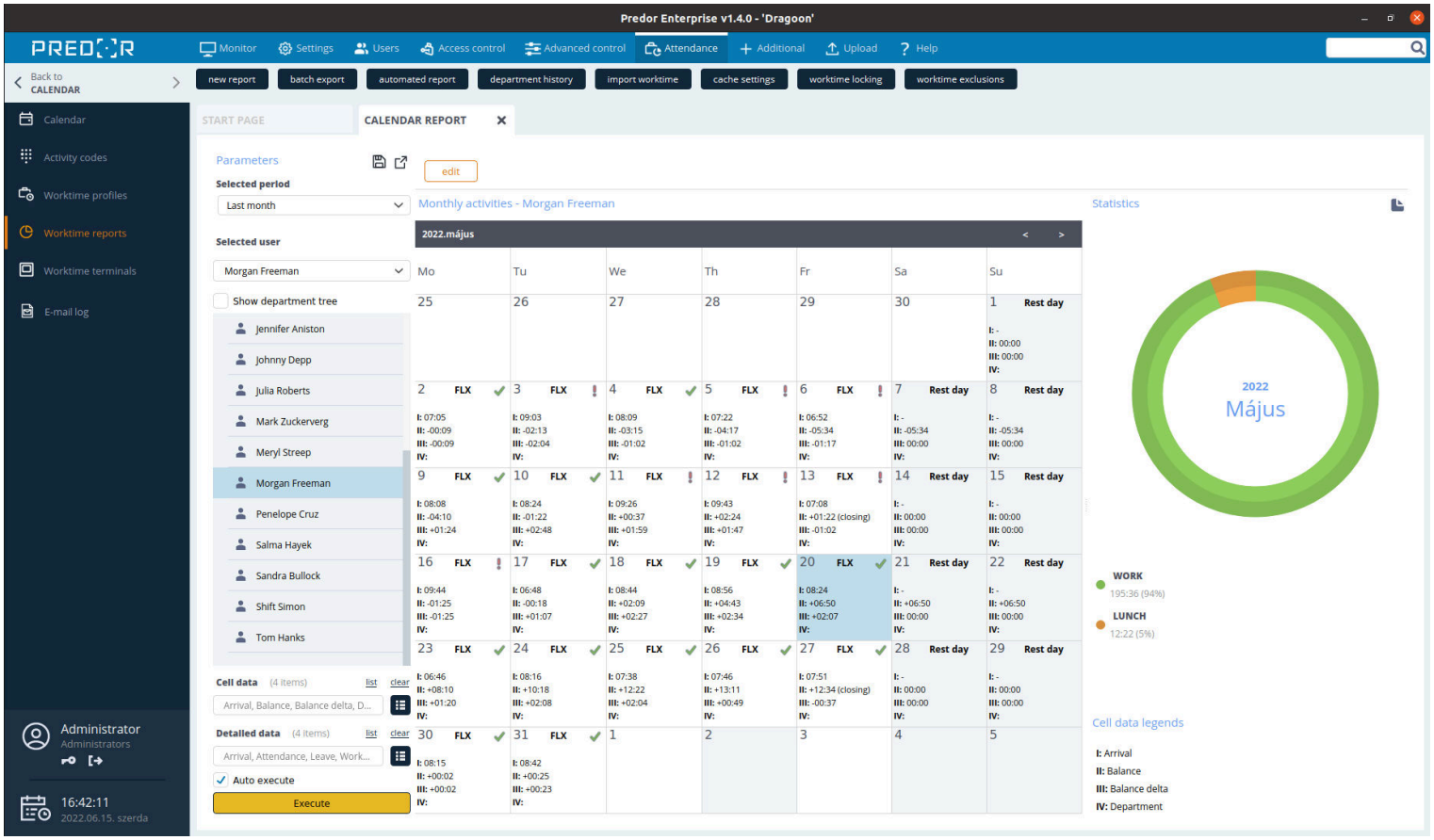


Figure 145: Calendar report with monthly statistics

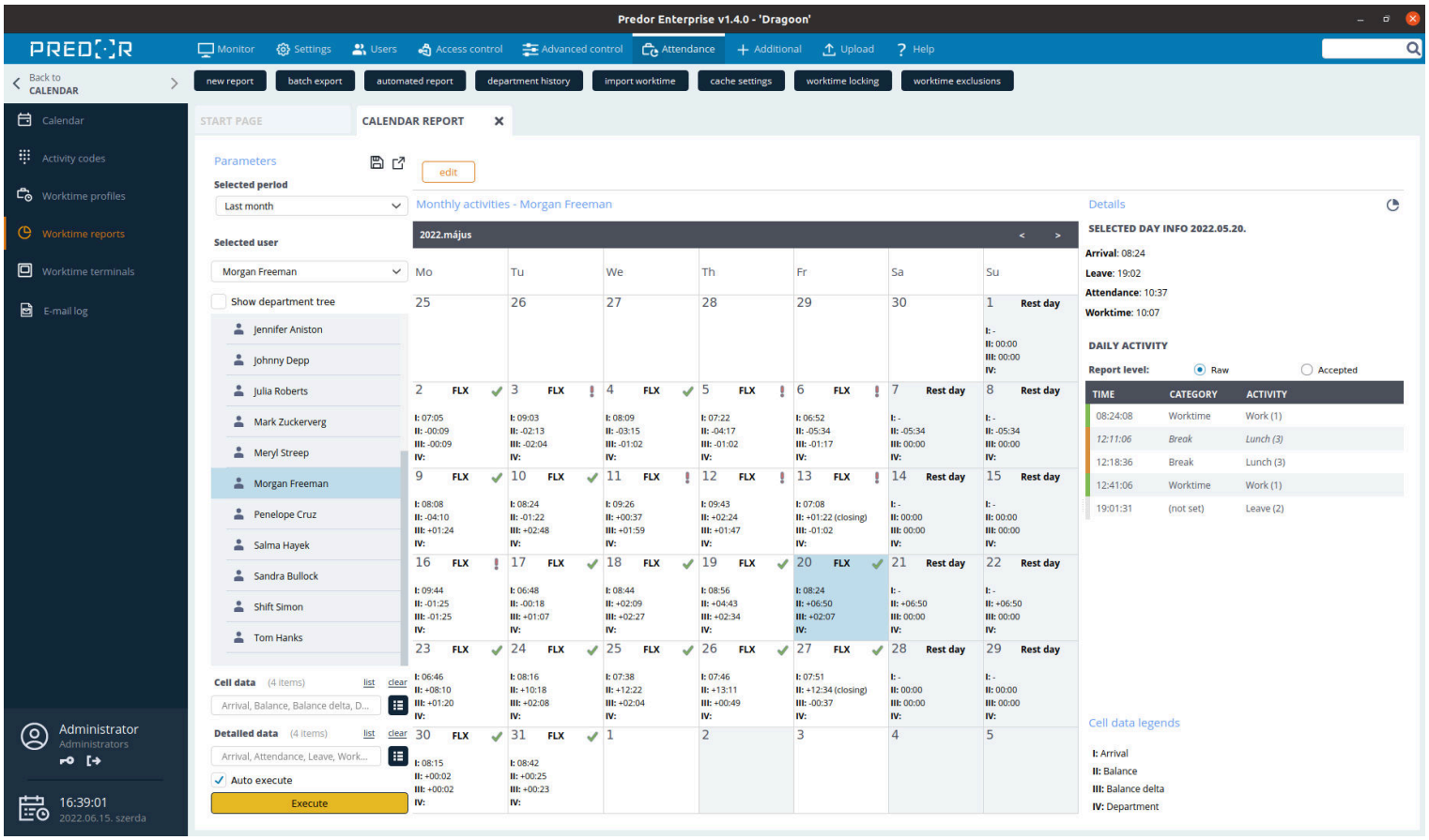


Figure 146: Calendar report with details of a chosen day

Attendance report

The attendance report lists the activities of an employee over a given period of time. The table has date, arrival and leave columns by default, but six additional columns can be added. A unique name can be set for the column headers, which will appear on the report and the export instead of their original name. Some cells are also editable (arrival, leave, work time, attendance, allowances, overtimes). Values edited here are interpreted as a third, "ATTENDANCE" level data, and thus it does not affect "RAW" and "ACCEPTED" data. The report shows monthly sums for other important values. The attendance report shows the company data, the employee's personal information and the configured work time data.



ATTENTION! The attendance reports are configured in the work time profile editor, because the data to be displayed may differ for each work time profile.

We can **save the report to a pdf** document by clicking on the export icon .

It is also possible to batch or automate the export of this report type. See Batch export for more information.

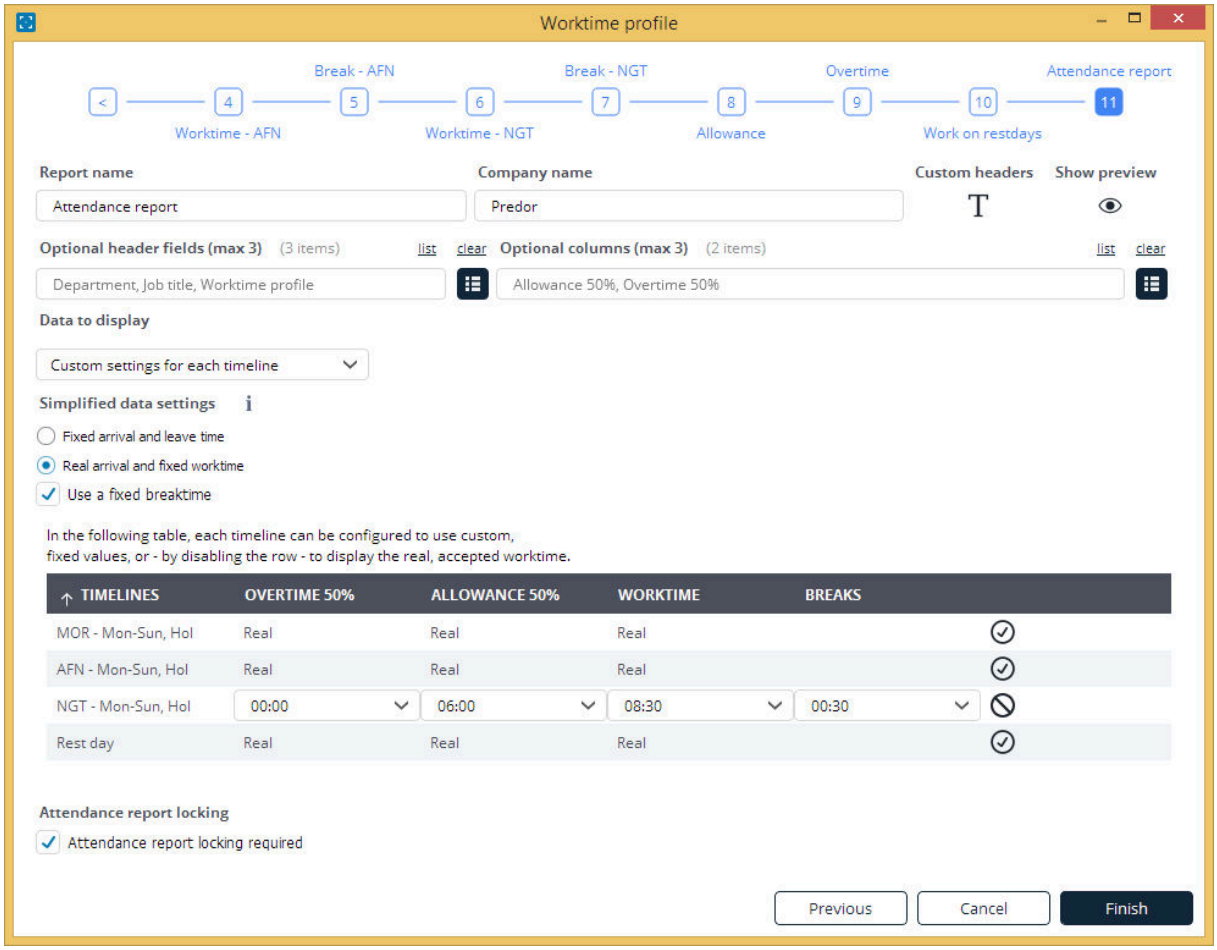


Figure 147: Attendance report settings in the work time profile wizard last page

Attendance report 2019 november

Company: Predor
Date: 2019 november
Worktime profile: Fix
Employee: Sandra Bullock
Job title:
Department:

Date	Arrival	Leave	Worktime	Shift
11.01 Fri	07:53	17:07	07:30	FIX
11.02 Sat	Rest day			
11.03 Sun	Rest day			
11.04 Mon	08:38	17:02	07:00	FIX
11.05 Tue	08:34	16:56	07:00	FIX
11.06 Wed	08:35	16:57	07:30	FIX
11.07 Thu	07:59	17:00	07:30	FIX
11.08 Fri	08:40	17:03	07:00	FIX
11.09 Sat	Rest day			
11.10 Sun	Rest day			
11.11 Mon	08:33	17:01	07:30	FIX
11.12 Tue	07:55	16:16	07:30	FIX
11.13 Wed	08:38	16:29	06:30	FIX
11.14 Thu	08:32	16:22	06:30	FIX
11.15 Fri	07:58	16:29	06:30	FIX
11.16 Sat	Rest day			
11.17 Sun	Rest day			
11.18 Mon	08:31	16:59	07:00	FIX
11.19 Tue	07:52	16:21	07:30	FIX
11.20 Wed	08:35	16:19	06:30	FIX
11.21 Thu	07:51	16:58	07:30	FIX
11.22 Fri	07:51	17:03	07:30	FIX
11.23 Sat	Rest day			
11.24 Sun	Rest day			
11.25 Mon	08:35	16:19	06:30	FIX
11.26 Tue	08:32	16:21	06:30	FIX
11.27 Wed	08:38	17:05	07:30	FIX
11.28 Thu	08:33	16:25	06:30	FIX
11.29 Fri	08:32	16:58	07:00	FIX
11.30 Sat	Rest day			
Sum			**148:00**	

Employee

Manager

Figure 148: Attendance report pdf export

Monthly details

Lists the activities of an employee in a table. The table columns are the different kinds of data tracked for each day. We can use the column selector above the execute button to pick columns to display and customize the presented data. The columns can be arranged to any order by using the *list* option above the column selector. The *hide empty rows* checkbox can be used to hide unnecessary rows and show only the relevant data.

In this report both RAW, ACCEPTED and ATTENDANCE data can appear and the following ones even can be edited if needed:

- RAW: Arrival, Leave, Core time violation, Early departure, Late arrival
- ACCEPTED: Arrival, Attendance, Leave, Work time, Allowance (multiple types), Overtime (multiple types)
- ATTENDANCE: Arrival, Leave

After the execution we can sort the data by clicking on the headers of the columns. The bottom row shows the sum of the values. Clicking on a date in the first column opens a *Daily activities* report for the user.

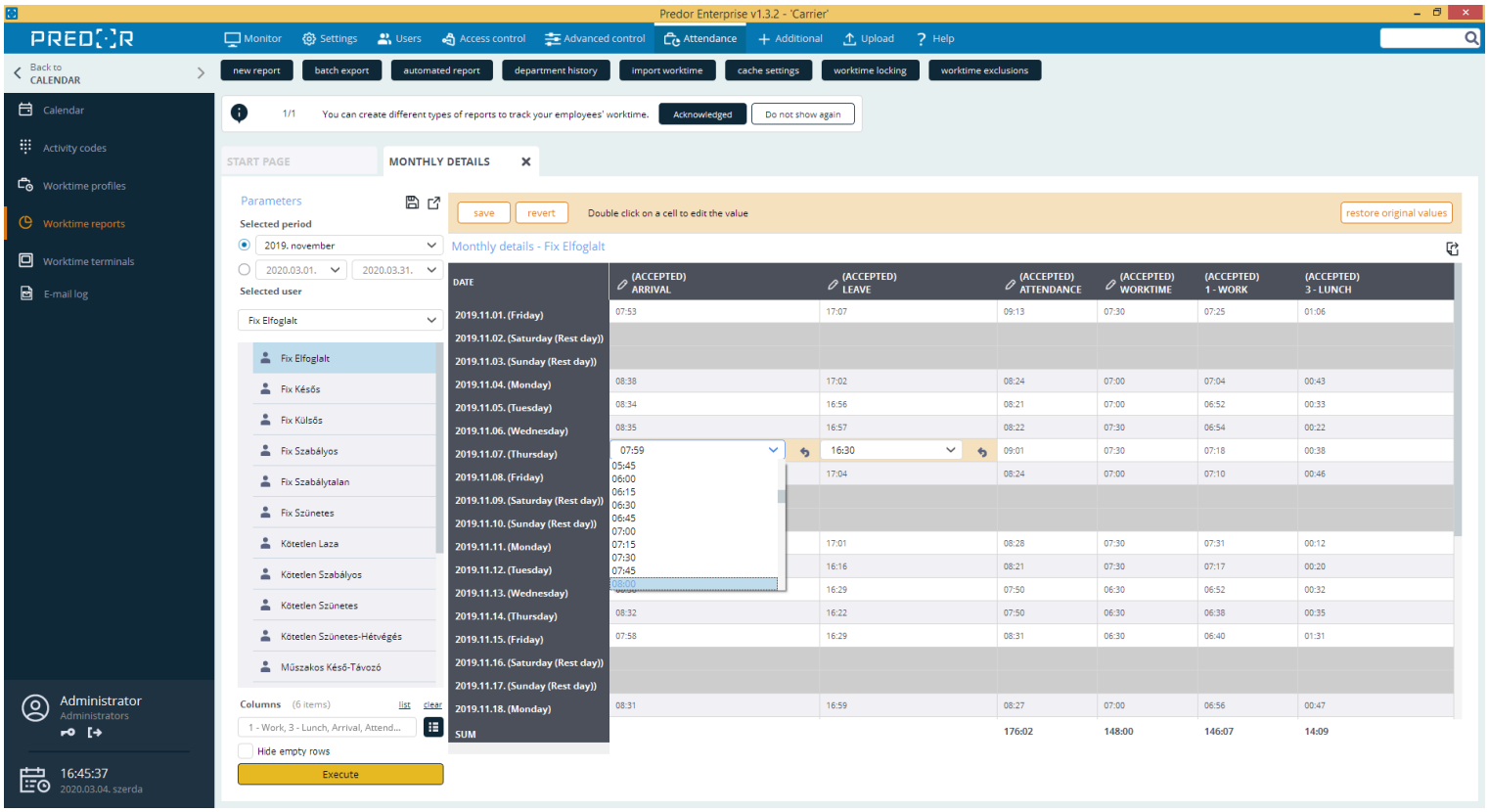


Figure 149: Editing a monthly details report

When editing, if you type something wrong, you can simply reset it to the original value by clicking the icon in the modified cell. If you want to reset all changes, you can do by

clicking on the “restore original values” button.

The report can be exported into an excel file by clicking on the export icon .

	A	B	C	D	E	F	G	H
1	PREDOR	User monthly details – Bench Mark						
2		Reporting date: 2020.03.05. 08:55						
3		Created by: Administrator						
4	Date	Day of week	(Accepted) Arrival	(Accepted) Leave	(Accepted) Attendance	(Accepted) Worktime	(Raw) Early departure	(Raw) Late arrival
5	2019.11.01.	Friday	07:53:28	17:06:52	09:13:00	07:30:00	-	-
6	2019.11.02.	Saturday						
7	2019.11.03.	Sunday						
8	2019.11.04.	Monday	08:38:05	17:01:46	08:24:00	07:00:00	-	00:38:00
9	2019.11.05.	Tuesday	08:34:21	16:55:35	08:21:00	07:00:00	-	00:34:00
10	2019.11.06.	Wednesday	08:35:02	16:57:27	08:22:00	07:30:00	-	00:35:00
11	2019.11.07.	Thursday	07:58:50	16:59:45	09:01:00	07:30:00	-	-
12	2019.11.08.	Friday	08:39:44	17:03:30	08:24:00	07:00:00	-	00:40:00
13	2019.11.09.	Saturday						
14	2019.11.10.	Sunday						
15	2019.11.11.	Monday	08:32:57	17:00:34	08:28:00	07:30:00	-	00:33:00
16	2019.11.12.	Tuesday	07:54:42	16:15:37	08:21:00	07:30:00	00:14:00	-
17	2019.11.13.	Wednesday	08:38:25	16:28:39	07:50:00	06:30:00	00:01:00	00:38:00
18	2019.11.14.	Thursday	08:32:22	16:22:02	07:50:00	06:30:00	00:08:00	00:32:00
19	2019.11.15.	Friday	07:57:55	16:28:40	08:31:00	06:30:00	00:02:00	-
20	2019.11.16.	Saturday						
21	2019.11.17.	Sunday						
22	2019.11.18.	Monday	08:31:28	16:58:42	08:27:00	07:00:00	-	00:31:00
23	2019.11.19.	Tuesday	07:51:59	16:20:37	08:29:00	07:30:00	00:09:00	-
24	2019.11.20.	Wednesday	08:35:02	16:19:12	07:44:00	06:30:00	00:11:00	00:35:00
25	2019.11.21.	Thursday	07:51:03	16:57:58	09:07:00	07:30:00	-	-
26	2019.11.22.	Friday	07:50:39	17:03:15	09:13:00	07:30:00	-	-
27	2019.11.23.	Saturday						
28	2019.11.24.	Sunday						
29	2019.11.25.	Monday	08:35:26	16:18:54	07:43:00	06:30:00	00:11:00	00:35:00
30	2019.11.26.	Tuesday	08:32:06	16:21:16	07:49:00	06:30:00	00:09:00	00:32:00
31	2019.11.27.	Wednesday	08:37:55	17:05:21	08:27:00	07:30:00	-	00:38:00
32	2019.11.28.	Thursday	08:32:49	16:24:47	07:52:00	06:30:00	00:05:00	00:33:00
33	2019.11.29.	Friday	08:31:40	16:57:39	08:26:00	07:00:00	-	00:32:00
34	2019.11.30.	Saturday						
35	SUM				176:02	148:00	01:10	08:06
36	Predor © 2014-2020 Leviathan Solutions Kft.							

Figure 150: Example of a monthy details report

Users’ daily details

Lists the activities of multiple employees on the same day in a table. The table columns are the different kinds of data tracked for each day. We can use the column selector above the execute button to pick columns to display and customize the presented data. The columns can be arranged to any order by using the *list* option above the column selector. The *hide empty rows* checkbox can be used to hide unnecessary rows and show only the relevant data.

In this report both RAW, ACCEPTED and ATTENDANCE data can appear and the following ones even can be edited if needed:

- RAW: Arrival, Leave, Core time violation, Early departure, Late arrival
- ACCEPTED: Arrival, Attendance, Leave, Work time, Allowance (multiple types), Overtime (multiple types)
- ATTENDANCE: Arrival, Leave

After the execution we can sort the data by clicking on the headers of the columns. The bottom row shows the sum of the values. Clicking on a date in the first column opens a *Daily activities* report for the user.

TIP: When we order the tables into a decreasing or increasing order, we can easily find out who has the least work or who put in the most overtime.

The report can be exported into an excel file by clicking on the export icon .

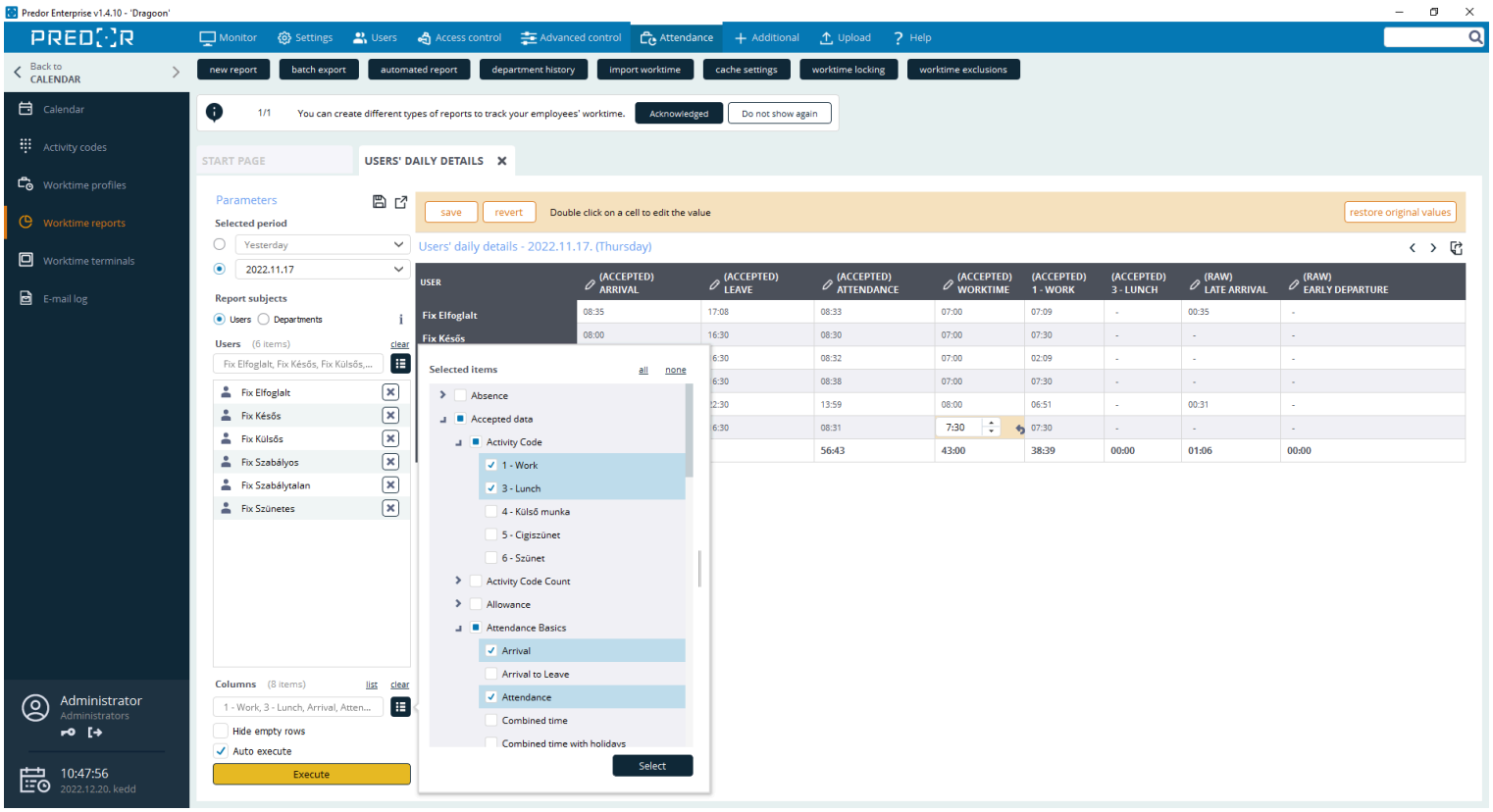


Figure 151: Users' daily details report

When editing, if you type something wrong, you can simply reset it to the original value by clicking the icon in the modified cell. If you want to reset all changes, you can do by clicking on the "restore original values" button.

Monthly activities

This report provides a more detailed overview of an employee's monthly activities in a graphical format. By hovering the cursor over the icons of the first column a summary is displayed of the given day. Hovering over the segments of the timeline shows information about that specific activity. To get an even more detailed numerical form of a specific day click on the *Details* button (this opens a daily activity report).

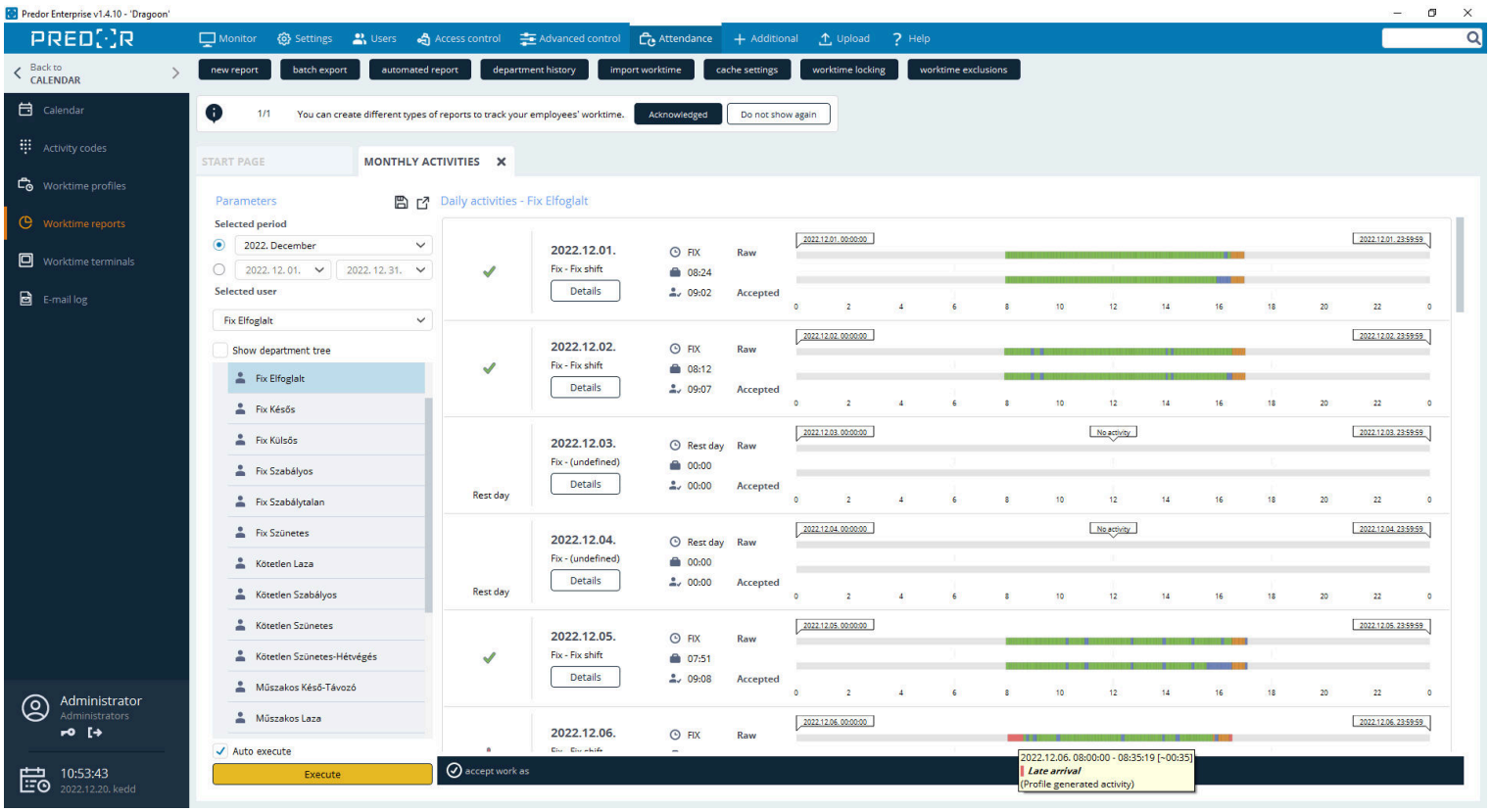


Figure 152: A user's monthly activities report

Users' summary

Lists the summary of activities of multiple employees or departments in a given time period. The table columns are the different kinds of data tracked. We can use the column selector above the execute button to pick columns to display and customize the presented data. Ordering of the columns is possible by clicking on the *"list"* text and arranging the selected columns into the necessary order.

After the execution we can sort the data by clicking on the headers of the columns. The bottom row shows the sum of the data.

The report can be exported into an excel file by clicking on the export icon .

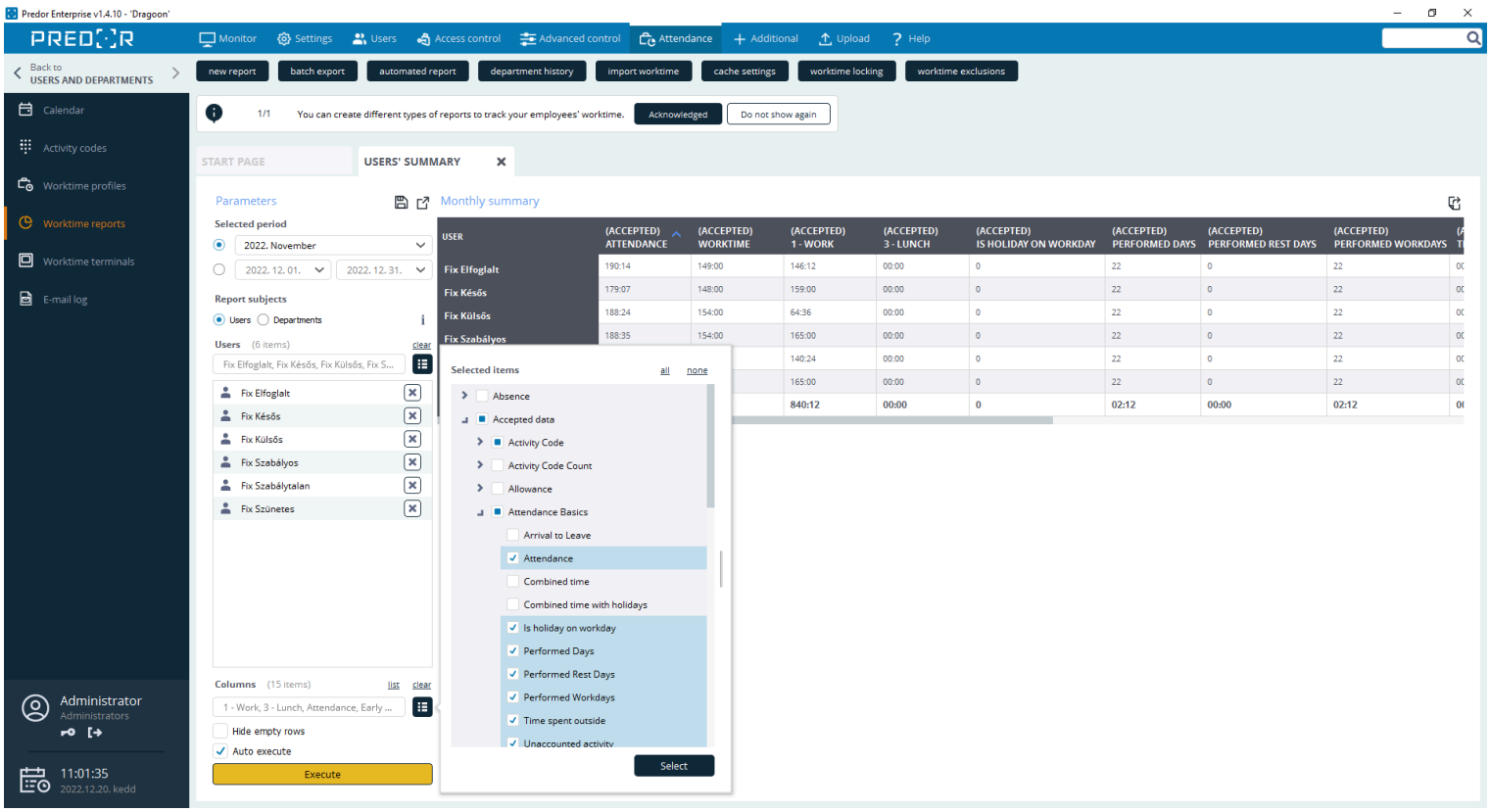


Figure 153: Users' summary report

Days off report

Lists a chosen employee's days off for a given period of time or year. The report shows the days off with the assigned day, type, yearly limit, the number of available days, the accounted time, and remaining counts. The report can be filtered to show only specific day-off types.

For listing the available and used number of days off for each employee use the Manage days off button in the Calendar menu.

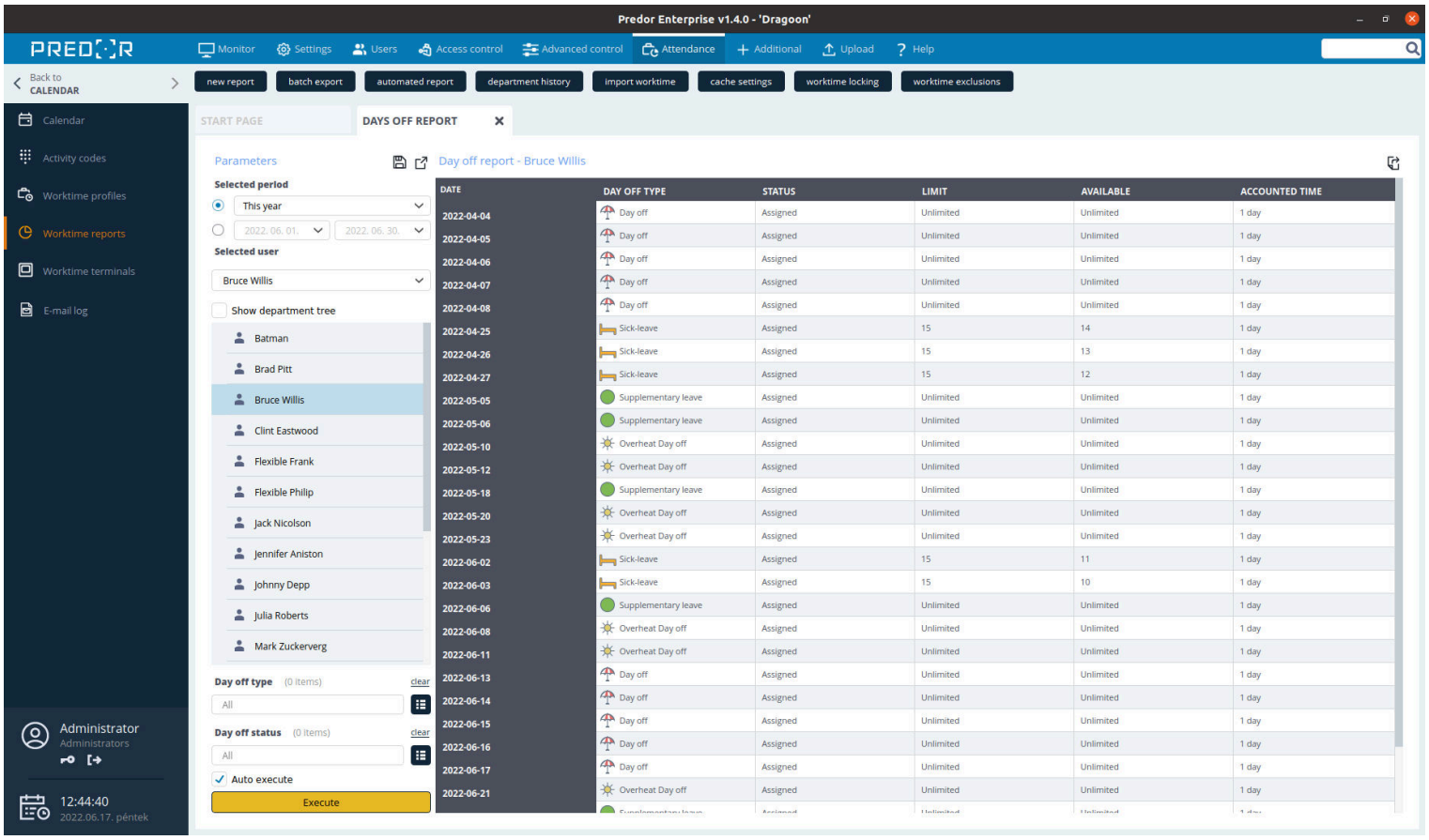


Figure 154: Days off report

Balance report

This report is only available for employees that are assigned to work time profiles which handle overtimes with work time balance. Only users assigned to the same profile can be enquired at a time so this report needs the work time profile on top the time period and users as input. Periods are calculated from the *Base control date* and the *Periodic frequency*, both are set in the work time profile.

Quick changing between periods is possible by using the arrows on the upper right of the report.

The **override configuration** button can be used to override the balance handling rules in this period (for example the remaining balance can be discarded instead of rolling it over the next period, if that's the default setting). If the configuration is overridden the title changes to **"Balance handling configuration - Overridden"**.

The **reset configuration** button restores the default balance handling configuration for this period.

The opening balance can be edited too if needed, and **extra days off or overtime can be granted** to the subjects of this report using custom rules by using the buttons in the

bottom menu bar. If an employee has changed work time profiles inside a balance period, use the **Continue previous row** button – accessible via the additional options ••• button – to continue all previous balance data on the new profile. The **select transitional rows** button helps with this process by selecting all lines in the report which can be used to continue the previous balance data. The **Restart row at 0** button can be used to set the selected row to zero, thus restart an employee's balance individually.

Edited, or extra granted values are displayed with a different background colour.

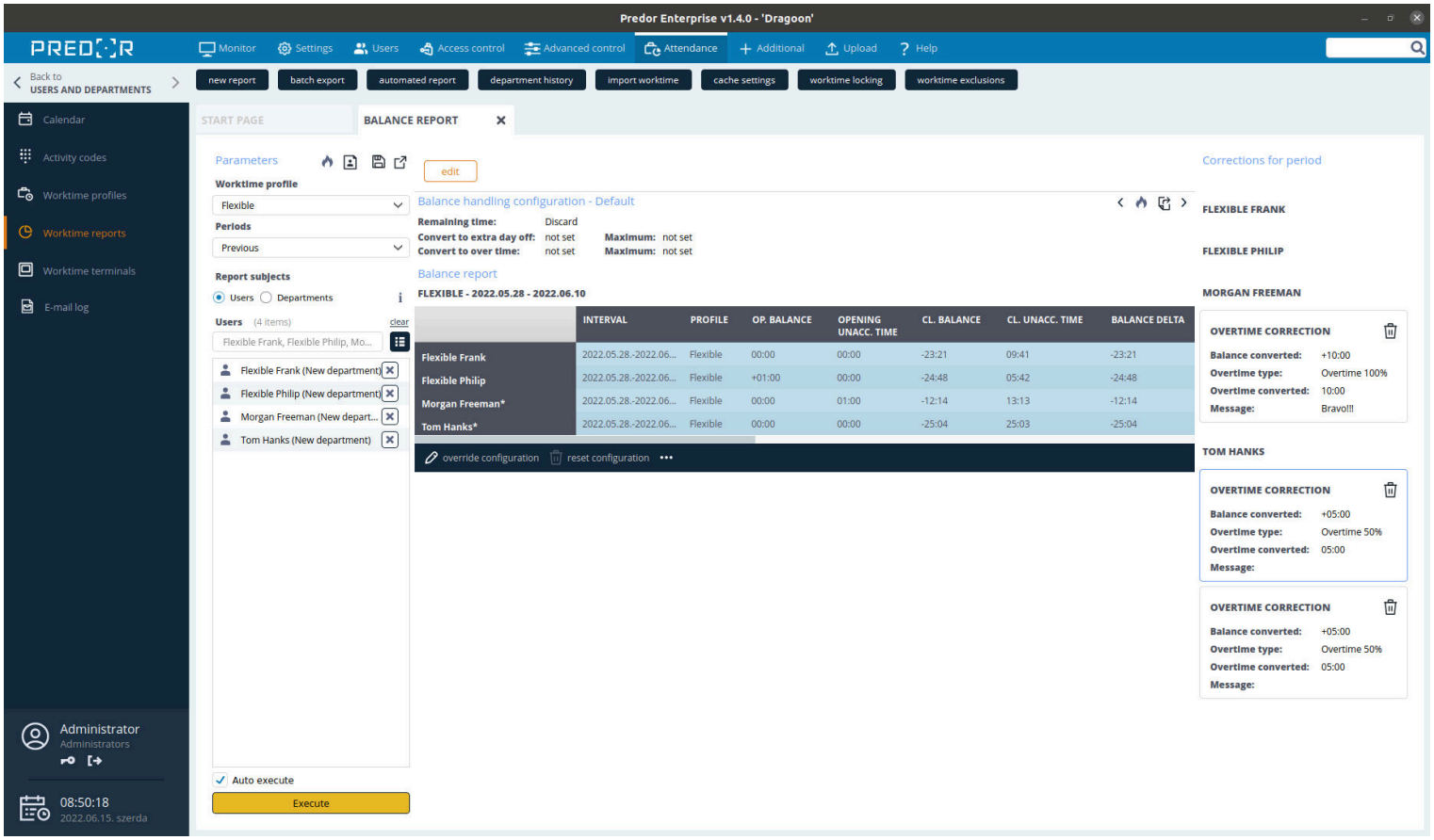


Figure 155: Balance report

Start screen

New report button

When there are a lot of report tabs open, it jumps back to the start page with a single click.

Batch export button

In this menu work time reports can be created for groups. These reports cannot be viewed in the Predor client but – depending on the report type – the output is an Excel

or PDF file. In addition to the report subjects and the selected period, the report type determines the list of other options that can be selected. You can also set which *Restricted* Operator Groups can see the report you have created and saved. Operators with *Full* access rights will always see the Working time reports submenu and those with *No access* rights will not see them. The following reports can be chosen:

- **Attendance report**
  - Single PDF document: Exports a single PDF document with multiple pages with the attendance report of the selected users. No other configuration is possible, because all settings are pre-configured in the work time profile.
- **Monthly details report**
  - Columns: Choose the list of required attendance data to be exported. Use the *headers* option to customize the name of the columns' headers in the exported table, and the *list* option to choose the order of the columns.
  - Hide filtered rows: empty rows of the report will not be exported if this is enabled
  - Name format: Choose the order of first name and last name in the export
  - Language: Headers (if not customized) and values are exported in the chosen language
  - Number of documents:
    * Multiple documents: every selected user's data will be exported to a separate document
    * Single tabbed document: one document will be exported, in which every selected user's data will be on separate sheets
    * Single merged document: one document will be exported, in which every selected user's data will be on a single sheet grouped and displayed under each other
  - Include summary: The report creates an additional file (in case of single tabbed documents, an extra tab) where all selected user's cumulative work time data is exported.
- **Users' daily activities report**
  - Columns: Choose the list of required attendance data to be exported. Use the *headers* option to customize the name of the columns' headers in the exported table, and the *list* option to choose the order of the columns.
  - Hide filtered rows: empty rows of the report will not be exported if this is enabled
  - Name format: Choose the order of first name and last name in the export

- Language: Headers (if not customized) and values are exported in the chosen language
- Number of documents:
  - Multiple documents: every selected user's data will be exported to a separate document
  - Single tabbed document: one document will be exported, in which every selected user's data will be on separate sheets
  - Single merged document: one document will be exported, in which every selected user's data will be on a single sheet grouped and displayed under each other
- Include summary: The report creates an additional file (in case of single tabbed documents, an extra tab) where all selected user's cumulative work time data is exported.

- **Users' summary report**
  - Columns: Choose the list of required attendance data to be exported. Use the *headers* option to customize the name of the columns' headers in the exported table, and the *list* option to choose the order of the columns.
  - Hide empty rows: empty rows of the report will not be exported if this is enabled
  - Name format: Choose the order of first name and last name in the export
  - Language: Headers (if not customized) and values are exported in the chosen language
- **Balance report** (There are no Advanced settings for this report.)
- **Days off report**
  - Day off type: Choose which day off types are exported. All types are exported by default.
  - Name format: Choose the order of first name and last name in the export
  - Language: Headers (if not customized) and values are exported in the chosen language
  - Number of documents:
    - Multiple documents: every selected user's data will be exported to a separate document
    - Single tabbed document: one document will be exported, in which every selected user's data will be on separate sheets

    * Single merged document: one document will be exported, in which every selected user's data will be on a single sheet grouped and displayed under each other

- **Days off summary**
    - Day off type: Choose which day off types are exported. All types are exported by default.
    - Name format: Choose the order of first name and last name in the export
    - Language: Headers (if not customized) and values are exported in the chosen language
    - Unite intervals: After ticking the checkbox, if there are only rest days between two holidays, it will count as a single interval

After configuring all the necessary settings the report can be saved by using the **Save to reports** checkbox for later use, or if we wish to make an automated report. **Automated reports can only be created from previously saved batch exports!** If the saved report is intended to be used for an automated report it is advised to choose a relative time period (like "Last month" or "This month") instead of a fixed date, so the reports are always generated for the appropriate time period. Saved report cannot be deleted if an automated report is set for it.

Saving requires a name for the report to be given and the operator groups who can access this report. Alternatively the report can be marked as private so others cannot see it.

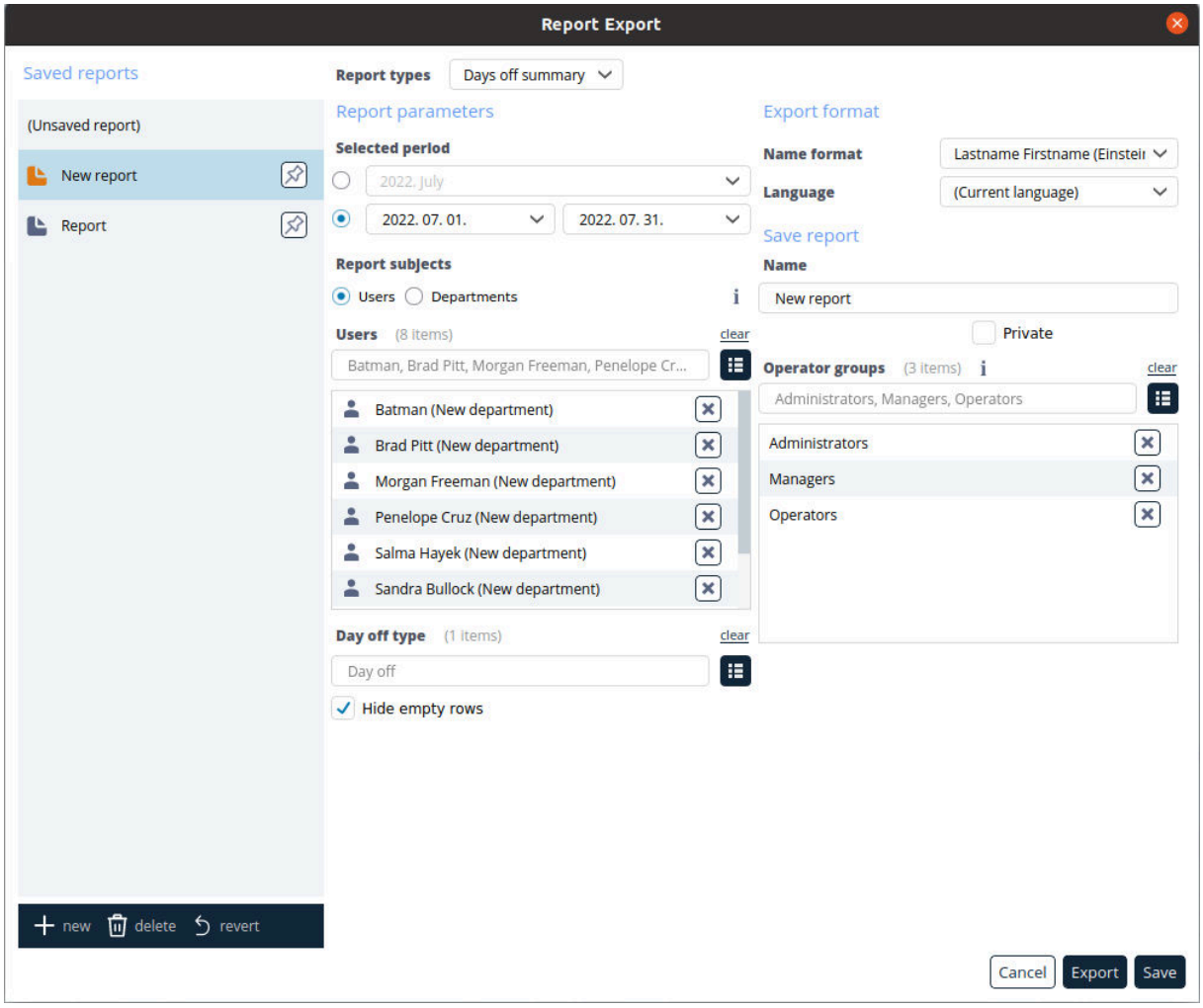


Figure 156: Batch export configuration

Automated report button

Saved batch reports can be configured here so that they are generated automatically from time to time and be sent to the appropriate e-mail addresses and/or saved to folders. To create an automated report press the "**+** new" button and fill in the required fields:

- Name: This will appear in the subject field of the e-mail and this will be the name of this report in the saved reports list.
- Saved report: Choose which previously saved batch report is to be automated. For these reports, it is recommended to use relative periods (This month, Previous month).
- Starting point: Time of the first generating of this report. If this date is in the past, the system automatically generates and sends the missed reports for the past after saving.
- Last day of month checkbox: report generation is scheduled to the last day of every month

- Frequency: reports are generated this often
- Admins to send: The chosen operators will be the recipients of this report. Each operator receives the report in their own set language in the software.
- Other recipients: The report will be sent to the e-mail addresses provided here too. Addresses must be separated by one of the following characters: space, comma or semicolon.
- Language: other recipients will get the report in the language set here
- Save path: Reports are generated and saved by the server, thus the path provided here is meant on the server. Every report of this type will be saved with the name given here. The software offers so called *Variables* to automatically generate unique file names.
- Variables button: Pressing this button shows which variables are available to be used in the file name. For example if we choose the path to be:
  "C:/autoreports/monthly_details_[YYYY]_[MM]_[USER]"
  then the actual file name saved for the report of March 2019 for the user John Doe will be:
  "monthly_details_2019_03_John Doe.xlsx"
- Other settings button:
  - Compressed file (.zip): documents are compressed and saved as a single .zip file
  - Non-empty reports only: if the base report is saved with the "Hide empty rows" option and the report yields no rows, the automated report will not be saved and/or sent.
  - Overwrite if exists: if a report already exists with the same name it will be over-written, otherwise both files will be kept with the newer files' name appended with (2), (3), etc.
  - Create cache entry: a database cache will be created for the result of the report, which will be used when the report is re-sent from the Email log menu in the future. This way the values represented in the email will be the same as when the email originally sent and will be not affected by future work time profile changes.

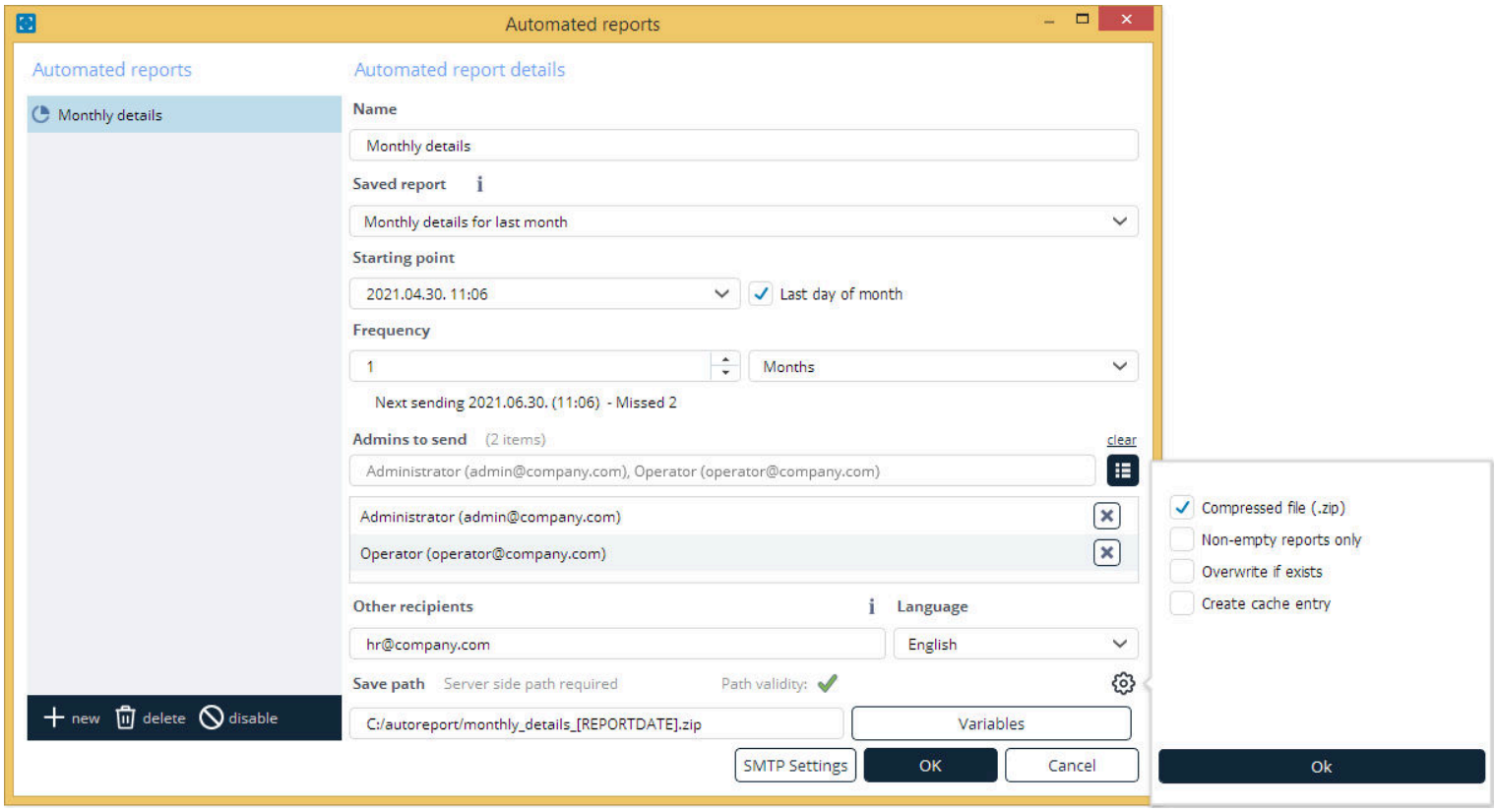


Figure 157: Automated reports configuration

Automated reports can be disabled temporarily with the disable button. Upon re-enabling if the *Starting point* is unchanged then the missed reports will be generated immediately.

Import worktime button

In this menu work time related events can be imported from a properly formatted **csv** file. The system handles these events as if the employees had identified themselves in the system at that time. The file must conform to the following format:

- data must be separated with " , " (comma) or with " ; " (semicolon)
- the first row is a header, and is not parsed
- the file must contain 4 columns in the following order:
  - **Identifier**: the identifier which will determine the eployee. It can be the **User ID**, **Card number**, **Tax number** or **Employee number**.
  - **Date**: the date of the imported work time event in the format of "YYYY.MM.DD.".
  - **Time**: the time of the imported work time event in the format of "HH:MM:SS" or "HH:MM".
  - **Code**: the *payroll code* of the associated activity code

Example file for importing work time data for User ID “1” and “23”:

```
IDENTIFIER;DATE;TIME;PRCODE
1;2021.03.25.;07:52:00;1
1;2021.03.25.;16:04:00;2
23;2021.03.25.;07:58:23;1
23;2021.03.25.;12:07:12;3
23;2021.03.25.;12:32:49;1
23;2021.03.25.;16:41:38;2
```

Before importing the file the type of identifier must be selected, and if it is the card number, the card format is also required.

Department history button

By editing a user’s department transfer timing table (“history”), the transfer date from one department to another can be trimmed accurately even before or after the actual transfer in the Predor software. Work time reports generated for departments use this timetable and therefore will show the correct results.

Cache settings

The Predor system caches the work time data associated with the reports when the reports are evaluated, so the next time for the same user and time settings no further calculations are necessary. This happens when the report is executed, or periodically, on a preset time.

The cache settings button located at the top of the work time report page offers manual caching or cache clearing and settings for the previously mentioned automated caching.

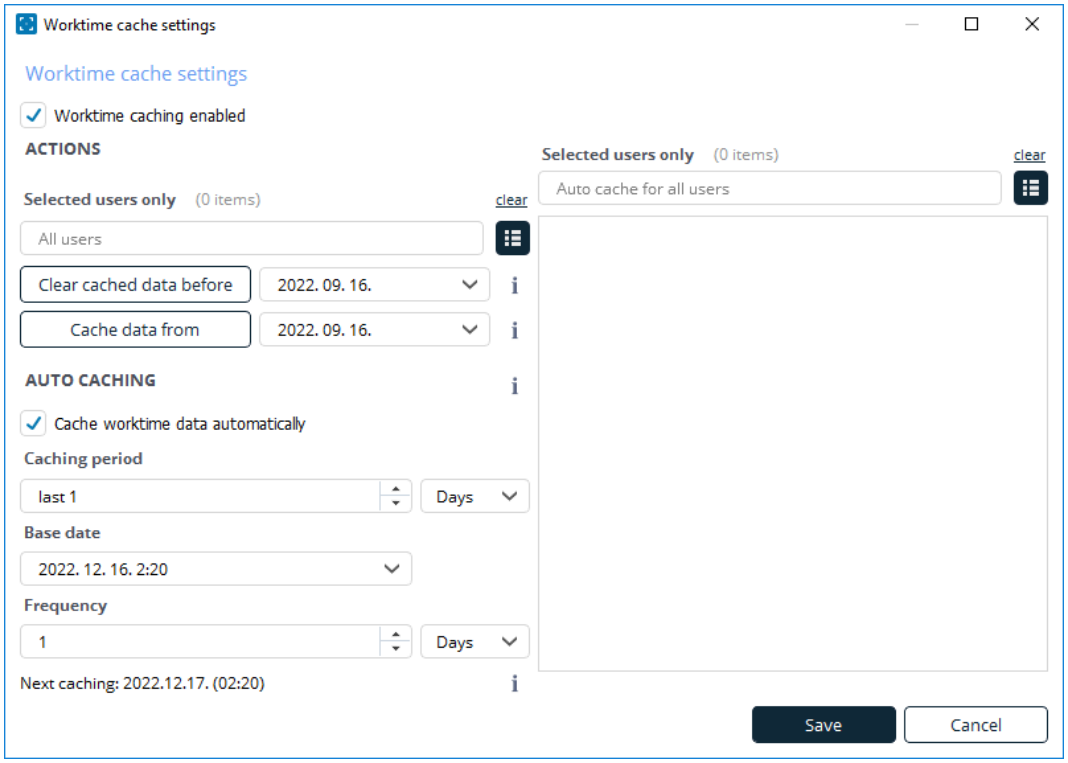


Figure 158: Work time cache settings

Below the **actions** section, we can use the **"Clear cached data before"** button to remove all cache entries older than the given date. Using the **"Cache data from"** button we can also manually create cache entries for all users from a given date. These operations run in the background and can take some minutes, depending on the number of users and events in the system.

Auto caching: Here we can set up the automated caching with controllable periodicity and time, or even a restricted group of users. Since this is a performance-intensive operation, it is advised to set the execution to the least busy period of the day, because during caching the system can experience increased response times, however auto caching can guarantee that the reports are executed faster when they are needed.

Worktime locking

Work time can be locked in blocks of months. Locking can be initiated from – if available – the personal web by responsible users or from the software by an operator. Months locked by a responsible user can still be edited by an operator, however months locked by an operator cannot be edited in any way until unlocking it. A locked month can only be unlocked by an operator.

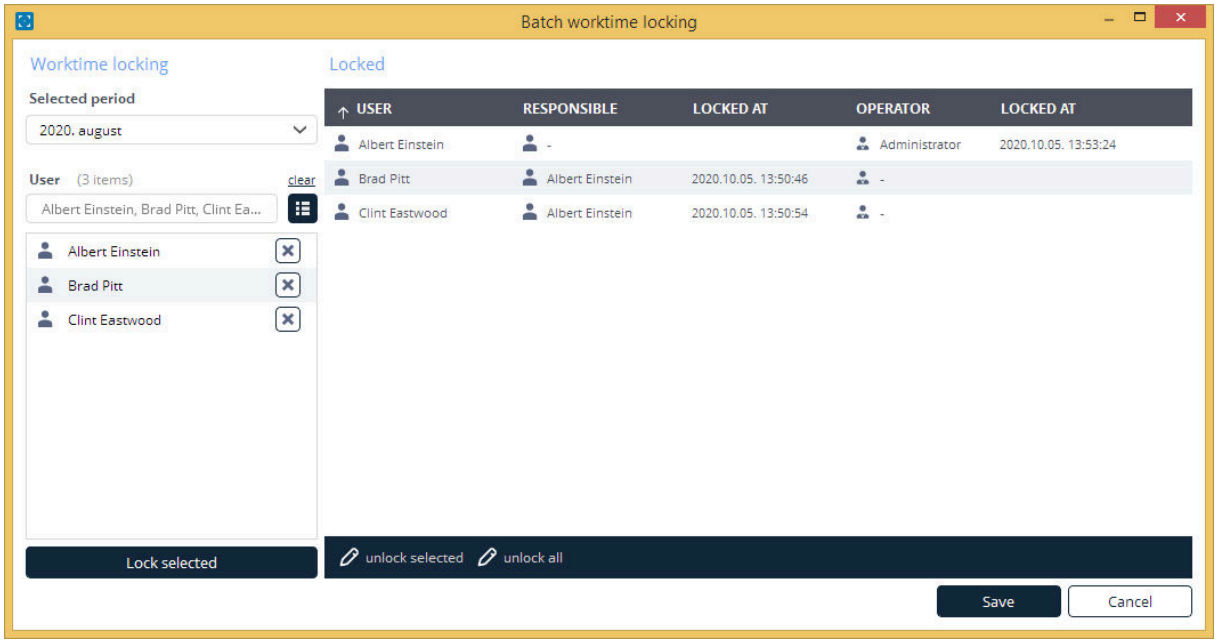


Figure 159: Batch locking of work time

After selecting the month and the users, only those appear in the right table whose month has already been locked. The selected users month can be locked with the **Lock selected** button. Unlocking is done via selecting the users on the right, then clicking on the **Unlock selected** or – if we wish to unlock all of the selected users month – **unlock all** button.

Worktime exclusions

In this dialog, we can exclude users selected or deleted from the worktime calculation. No worktime events are generated for excluded users, and worktime reports cannot be created for them either.

Worktime terminals

The worktime terminals menu is used to add worktime-terminals (terminals for short) and change settings on already added terminals.



WARNING: The terminals retrieve the exact time from the internet, so they need a stable internet connection to ensure that the time of the activity entries is accurate.

Discover terminals

Clicking on the “discover terminals” button shows the terminals available on the local network. Just like the controllers, terminals will get their IP address from the pool set in Settings/System settings and encrypt their communication with the same password.

Terminal configuration

The “Terminals” list on the left shows all terminals in the system. A menu bar at the bottom offers the following features:

- **New:** we can add a new terminal, by editing it manually. We can save its settings without filling in the serial number, so we can configure it without the actual physical device and later use the “replace terminal” operation to upload the settings.
- **Delete:** removes the selected terminal from the system
- **Rename:** renames the terminal. The name will appear on the terminal screen header.
- **Replace terminal:** Use this to upload the setting to, if a terminal device breaks down, or we use a real terminal to replace a pre-configured virtual one.
- **Reset and upload:** in case of an operational or upload problem, this feature guarantees that the all settings are re-uploaded and every faulyt settings removed.
- **Reboot:** remotely restart the terminal.
- **Upgrade firmware:** it updates the firmware on the terminal, if a newer version is available (indicated by a yellow triangle next to the terminal’s name in the list).

The currently selected terminal’s settings are editable on the right side in the “Terminal details” section.

Basic settings: We can change the network configurations and screensaver operation of the display (display logo or slideshow).

If *Affects person location* is enabled, the system will update the user’s location when an activity code is registered on the terminal. If *Handle exit codes* is enabled, the user’s location will be set to outside when any activity code marked as “count as exit” is registered.

Advanced network settings:

- Custom host: this field is used only if the work time terminal and the server is on a different network. By providing the external IP address and port for the terminal, the server can initiate the connection.
- Remote terminal: This option is also used when the terminal and the server does not share a common network, but instead of the server connecting to the terminal like in the “Custom host” setting, here the terminal connects to the server. The server connection parameters must be provided via the inner menu of the work time terminal.

This is the recommended setting for the Predor biometric mobile terminal, as it can roam on multiple wireless networks. The use of this setting is explained in the Predor biometric terminal description.

Additional read data (only with Predor biometric terminal):

- Include image: If the checkbox is ticked, the terminal takes a picture when an activity is entered. This image is saved on the server where it can be accessed at any time. A camera icon will appear in the event list next to the event's description.
- Include location data: After ticking the checkbox, the terminal will record the GPS location data (where the terminal is located) when you enter an activity. In the event list, this is indicated by a icon next to the event's description.

Worktime details: Select a collection of worktime data (3 at most) to display on the terminal screen. The order of the data can be changed with the arrows. The preview on the right will reflect the changes immediately.

Activity codes: Select the activity codes available to clock in on the device. Any number of activitiy codes can be used, but only four per page will appear on the screen at a time, the others are available by scrolling. The order of the activity codes is also customizable, and the preview will refrect the changes immediately.

Trigger on card read: You can specify which reader needs to be triggered when an activity is registered on the terminal. In this case, the controller detects the signal as a card read on the reader and, if the user has access, the door associated with the reader is opened.



WARNING: The trigger on card read function can only be used with Enterprise version and Phantom controller! If the Predor server is not running, the function will not work, because the terminal does not communicate directly with the controller.

Reader default code override: the terminal can block readers for a short time, so the reader's default code cannot override the code input from the terminal. This is useful if a door is frequently used with default code but in some cases (like before the employee goes home) the terminal should not be overwritten

The **"Overridden readers"** selector is used to select the readers, that are ignored for the duration of the time specified in the "Override within time" box, but only if the code on the terminal was one of the codes selected in the "Overriding codes" list.

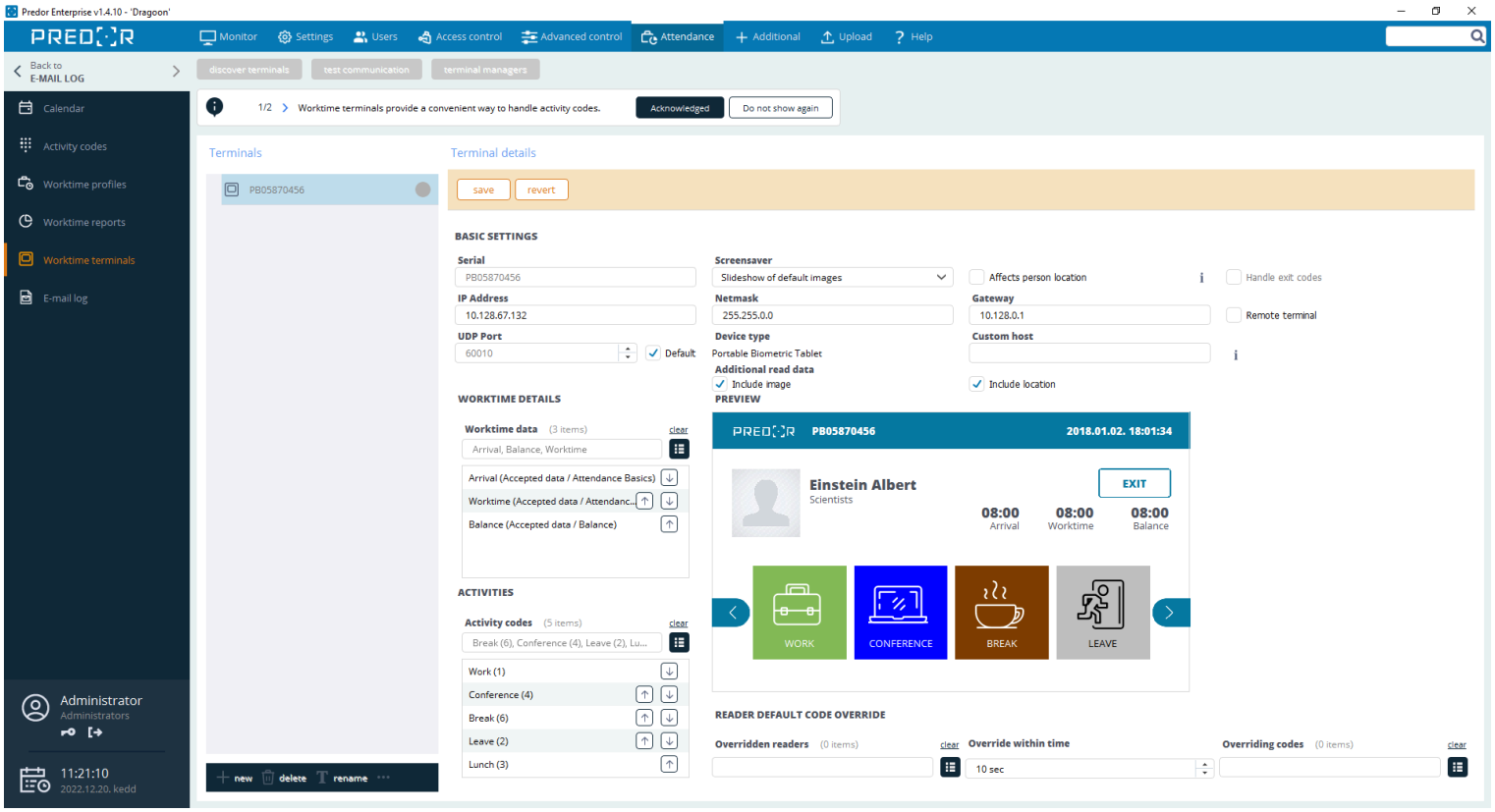


Figure 160: Configuring worktime terminals

The terminal has a built in card reader and the users have to identify themselves with a card read. Then screen shows them their user data, and custom worktime data, and offers the available activity codes.

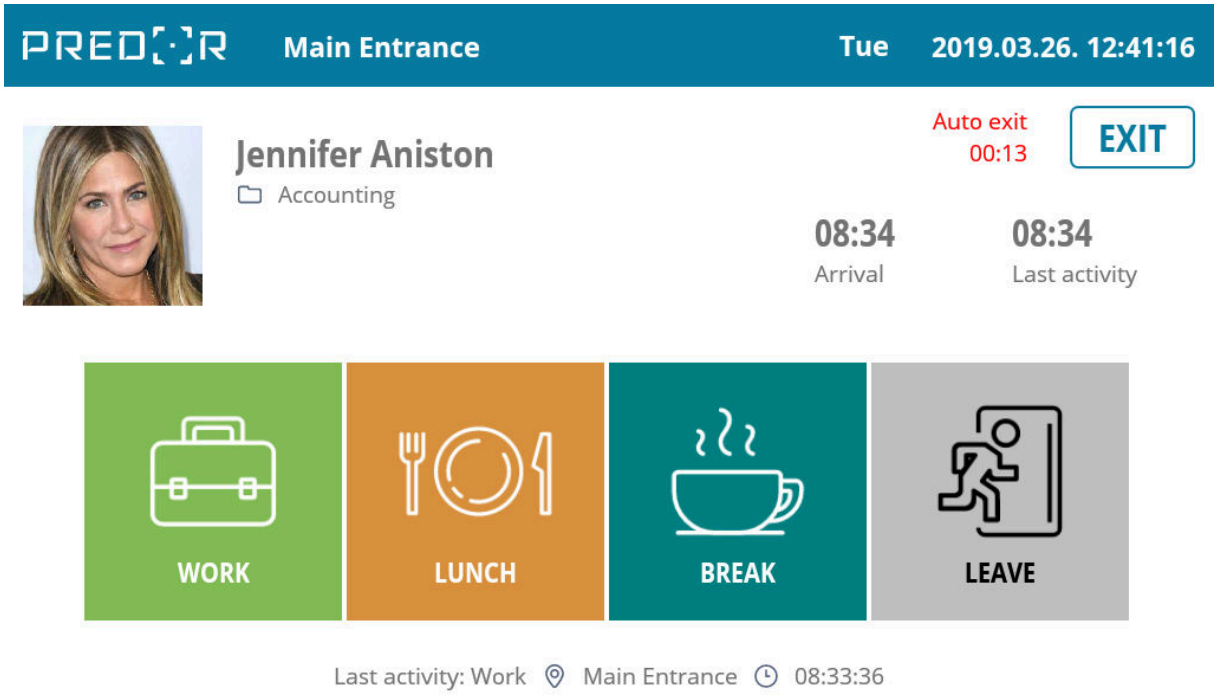


Figure 161: Worktime terminal screen after card swipe

Web settings

The web interface settings can be configured under this menu. To use it, the **Worktime web** license is required. You can configure what worktime data will be shown to the employees and to the users responsible for departments. You can also configure here what kind of operations will be avaible on the web interface.

General settings

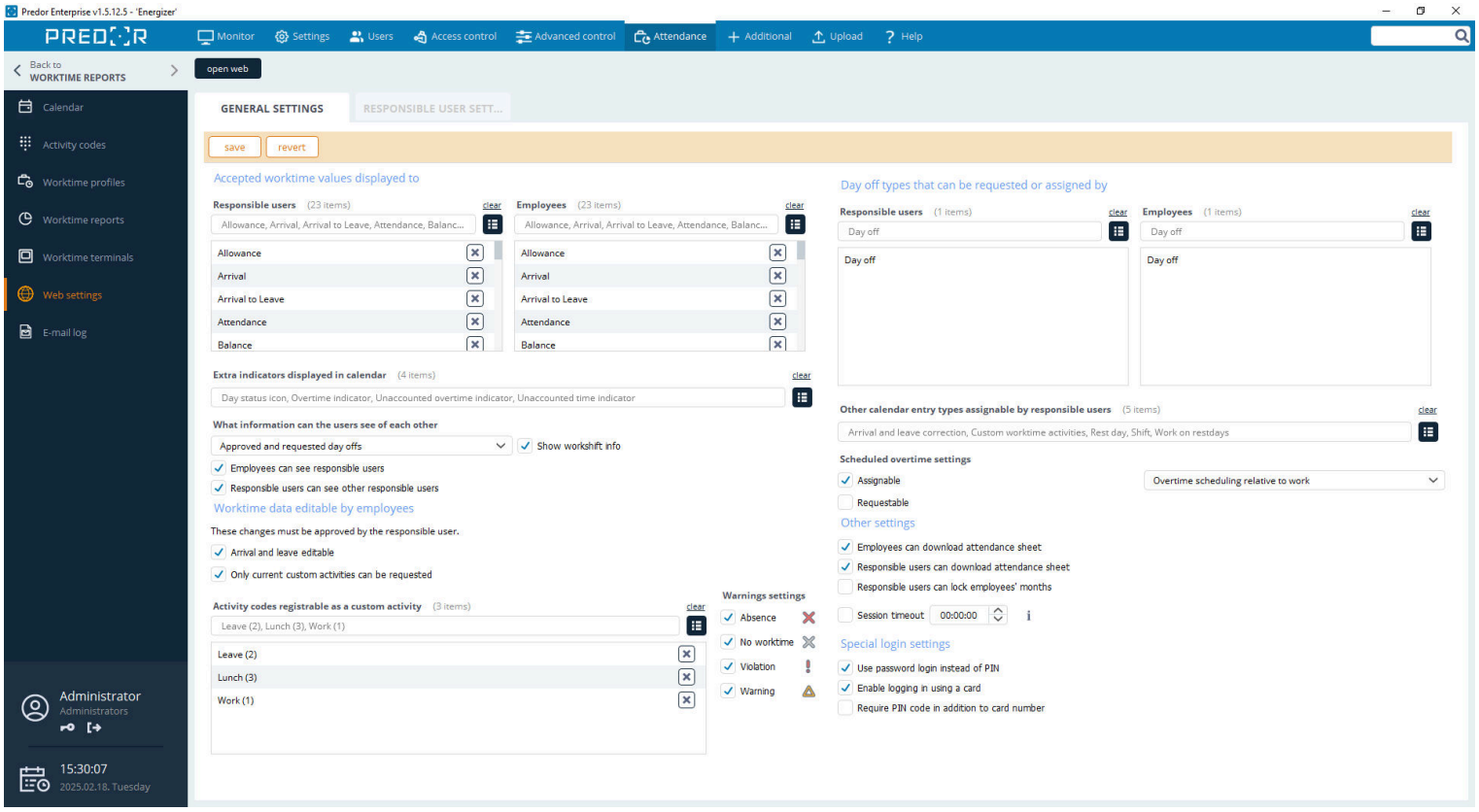


Figure 162: Web settings menu

In the **extra indicators displayed in calendar** menu we can select which indicators are to be displayed in the calendar, just like in the graphical work time reports: day status, overtime, unaccounted time indicator.

Choose if users can see each other's approved and/or requested days off or shifts in the "My colleagues" calendar.

Set if employees can request to correct arrival and leave times, or register certain activities. If the employee's department has a responsible person set, these corrections are always have to be approved by the responsible person, otherwise they are automatically approved.

Select which day off types can be requested by employees and assigned by responsible users. Also access to corrections made by responsible users can be adjusted as needed.

Responsible user settings

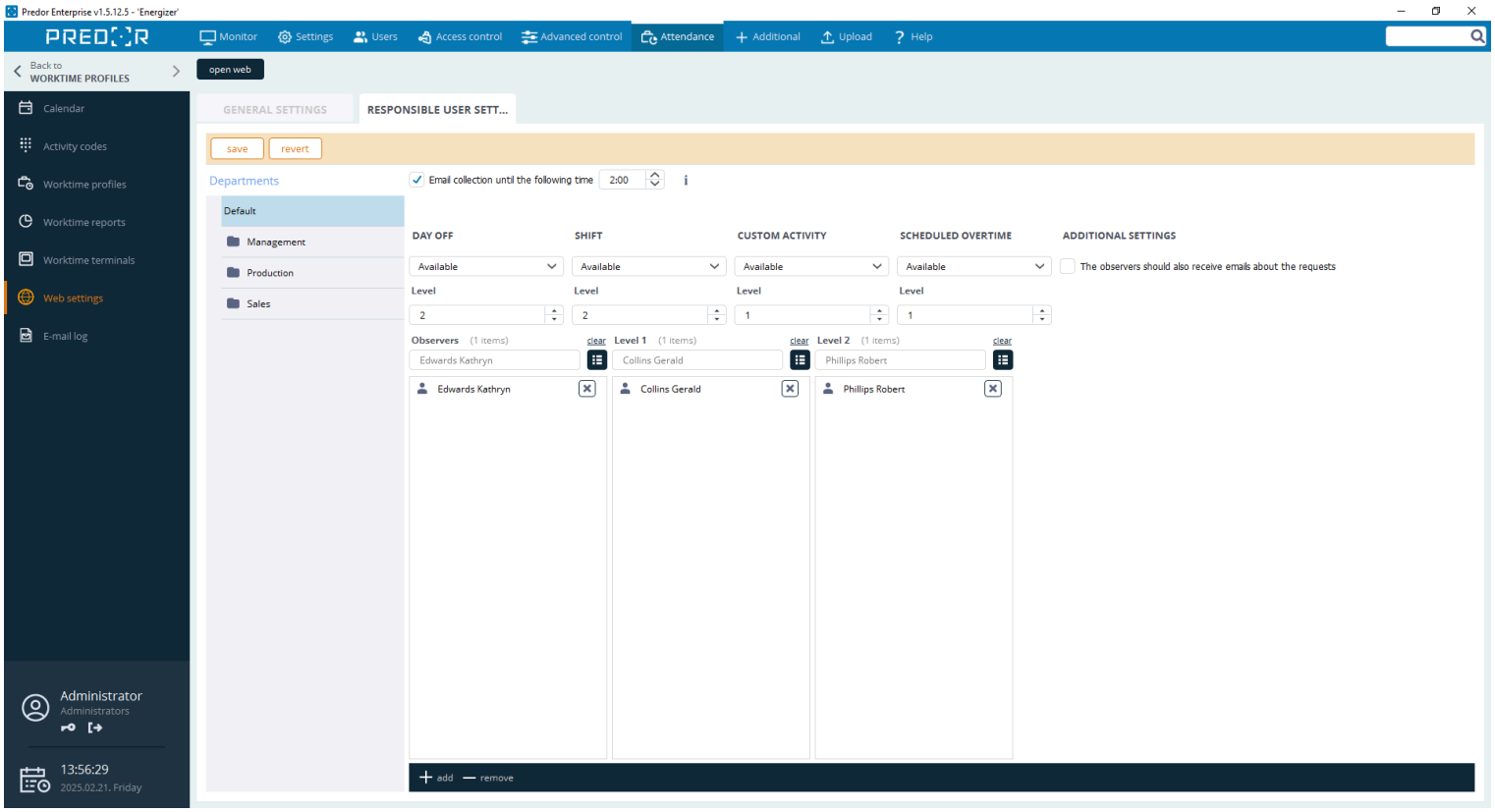


Figure 163: Responsible user settings

In this page, rules can be set for the worktime requests that can be made by employees and modified by the responsible persons. When using the default setting, the rules apply to all departments. To modify the settings, you need to enter **edit** mode, which can be done by clicking on the yellow edit button.

After activating the **Email collection until the following time** option, you can specify how long the system should collect email notifications about requests. After the time has expired, the responsible persons will receive the requests in groups.

For **Day off, Shift, Custom activity, Overtime** requests, you can set the availability and the approval level. In the case of available setting, employees can make a request and then specify the level for the final approval. In case of an approval, the request will be forwarded from the lower levels to the higher responsible persons.

To add responsible levels, click on the **add** button in the bottom menu bar. Once added, the responsible person(s) can be specified for each level.

Observers can also be selected to view the requests on the web interface. By activating the option **Observers should also receive emails about the requests**, the selected persons will also receive email notifications about the requests submitted by the employees, as well as their approval or rejection.

It is possible to deviate from the Default settings for each department to set up separate levels, assign responsible persons and observers. To do this, select the Department to be modified and then select the **Override default** option.

E-mail log

This page logs the e-mails sent by automated worktime reports, showing their status. The successful reports are marked with green checkmark, the reports in progress are represented with a grey question mark, failed reports are marked with a red X, and skipped reports are indicated with a yellow triangle.

By selecting a report, we can see more detailed information about it, with report settings, recipient list and brief information about the errors if there were any.

On the recipient list, we can resend reports to selected addresses or addresses where the sending failed. The list, like on many other pages, can be filtered, and filters can be saved and loaded too.

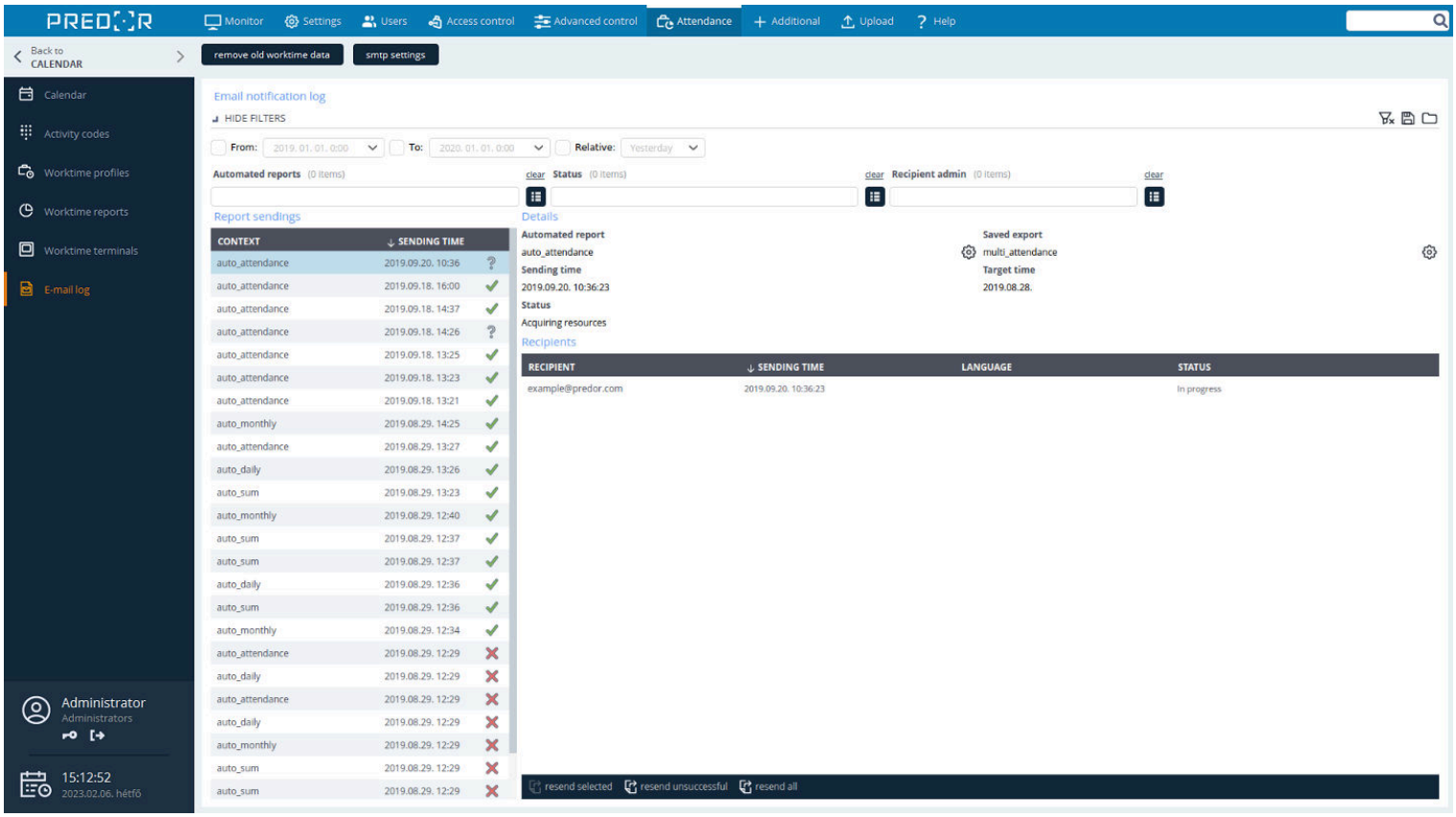


Figure 164: E-mail log view

11 WEB INTERFACE

In order to access the web interface the following licenses are required:

- Enterprise basic license
- Worktime management module
- Worktime web module



ATTENTION! The user quota in the worktime web module and the base license has to be the same.

You can access the interface with a web browser on the port provided during the server installation (3000 by default) by entering the following address:

- Without using SSL: http://<server IP address>:<port>
- With SSL: https://<server IP address>:<port>

E.g. on the server directly – using default settings – use this address: http://127.0.0.1:3000

To configure privileges and the shown data navigate to the Attendance/Calendar menu in the client software.

Under the employee interface, you can see your worktime data, register custom activities such as outside work or request a day off.

As for the managerial interface you can see your employee's data who are in departments you are responsible for. You can also assess day-offs, requested activities and assign shifts.

Off days cannot be requested or assigned for an interval containing several worktime profiles.



ATTENTION! Installing the enterprise edition, as well as the configuration of personal worktime web requires system administrator skills.

Logging in

You can identify yourself with either your user identification number or with your email address. To log in you will also need your PIN code or password. It is also possible to log in using card number, in which case the user's card number must be entered after selecting the appropriate format, and the PIN code if the "Require PIN code in addition to card number" option is selected. The user identification number and the card number, as well as your PIN code, can be seen on the Users and departments page.

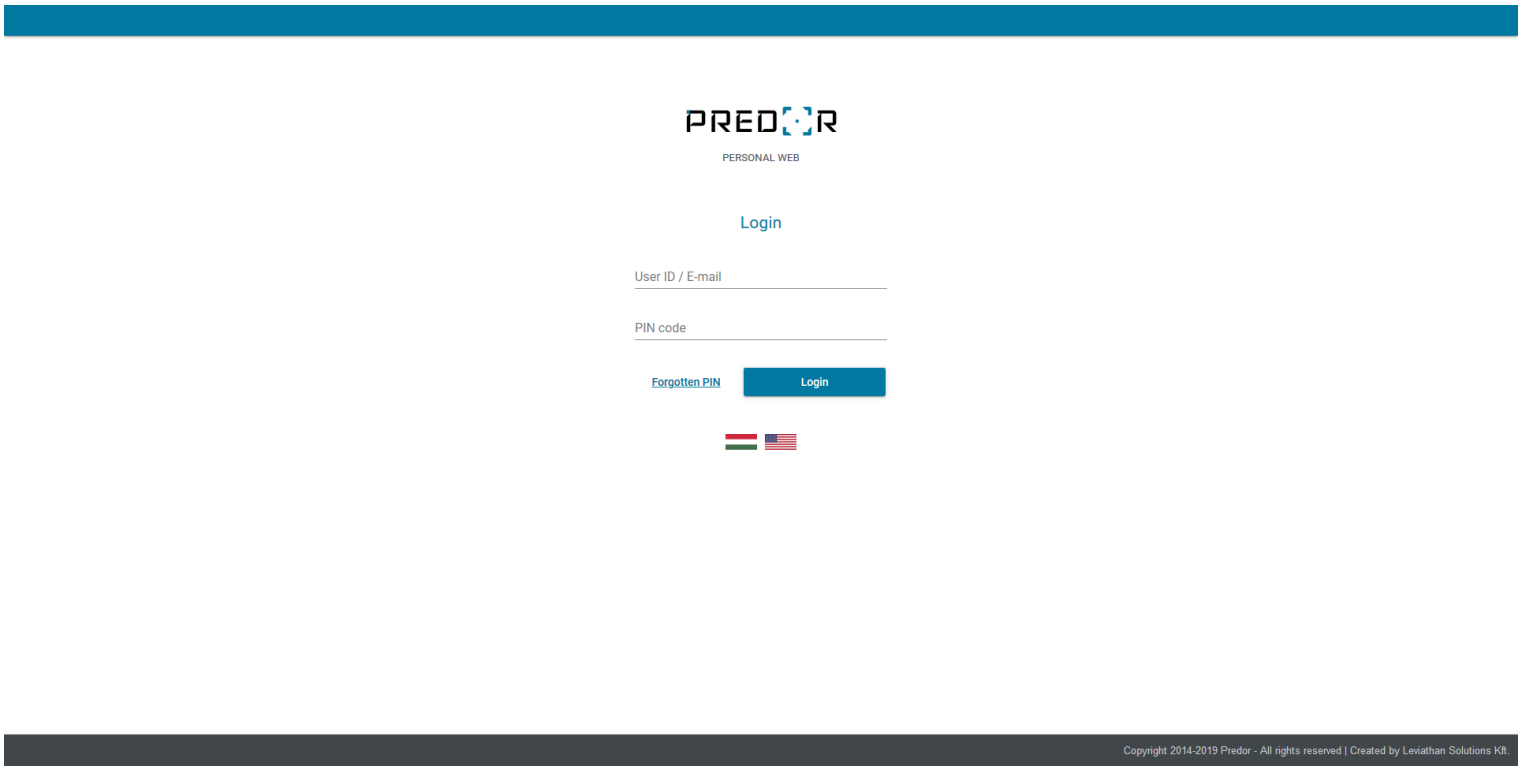


Figure 165: Web interface login page (with User ID/E-mail and PIN code)

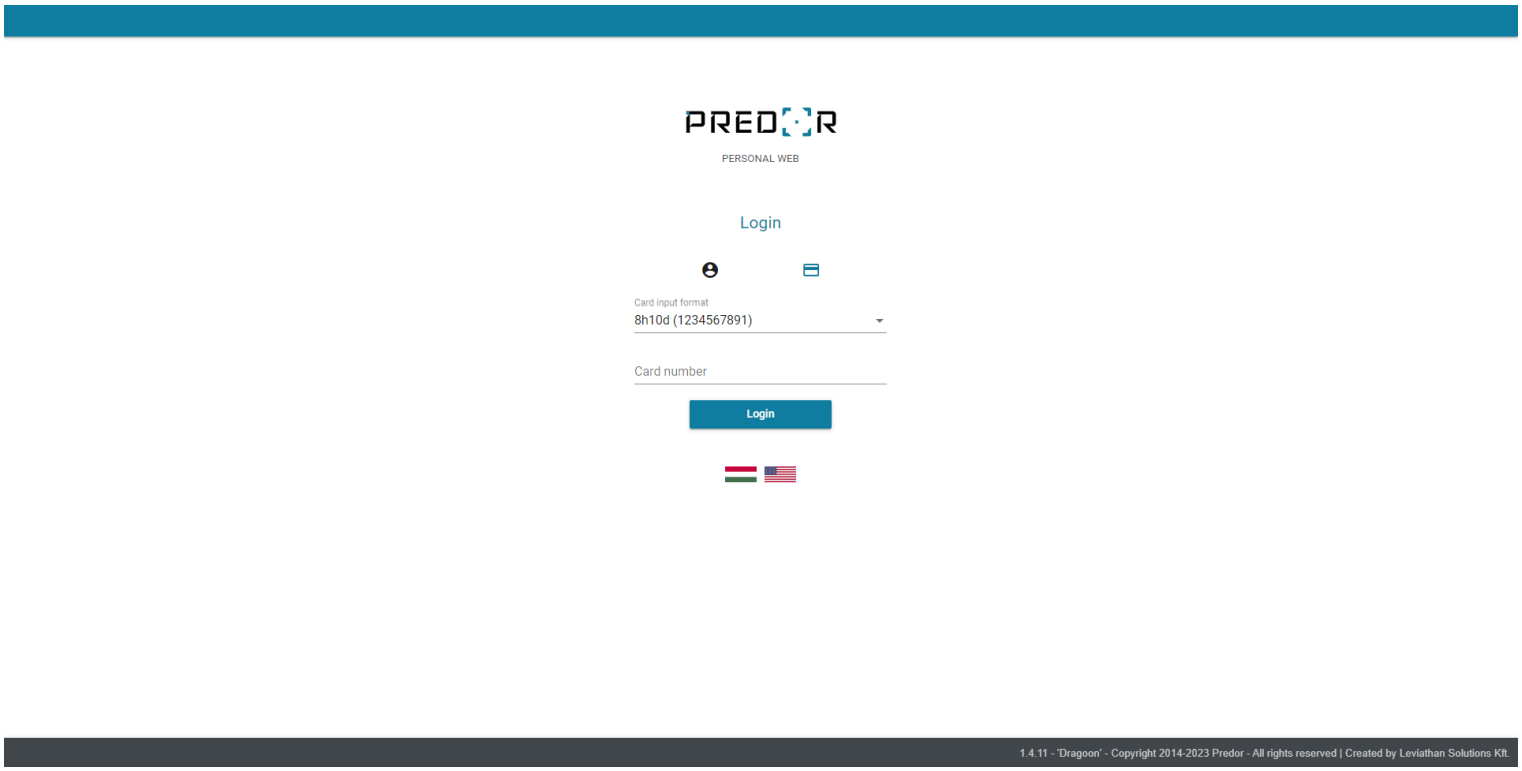


Figure 166: Web interface login page (with Card number)

After successfully logging in, you will be navigated to the “My data” page.

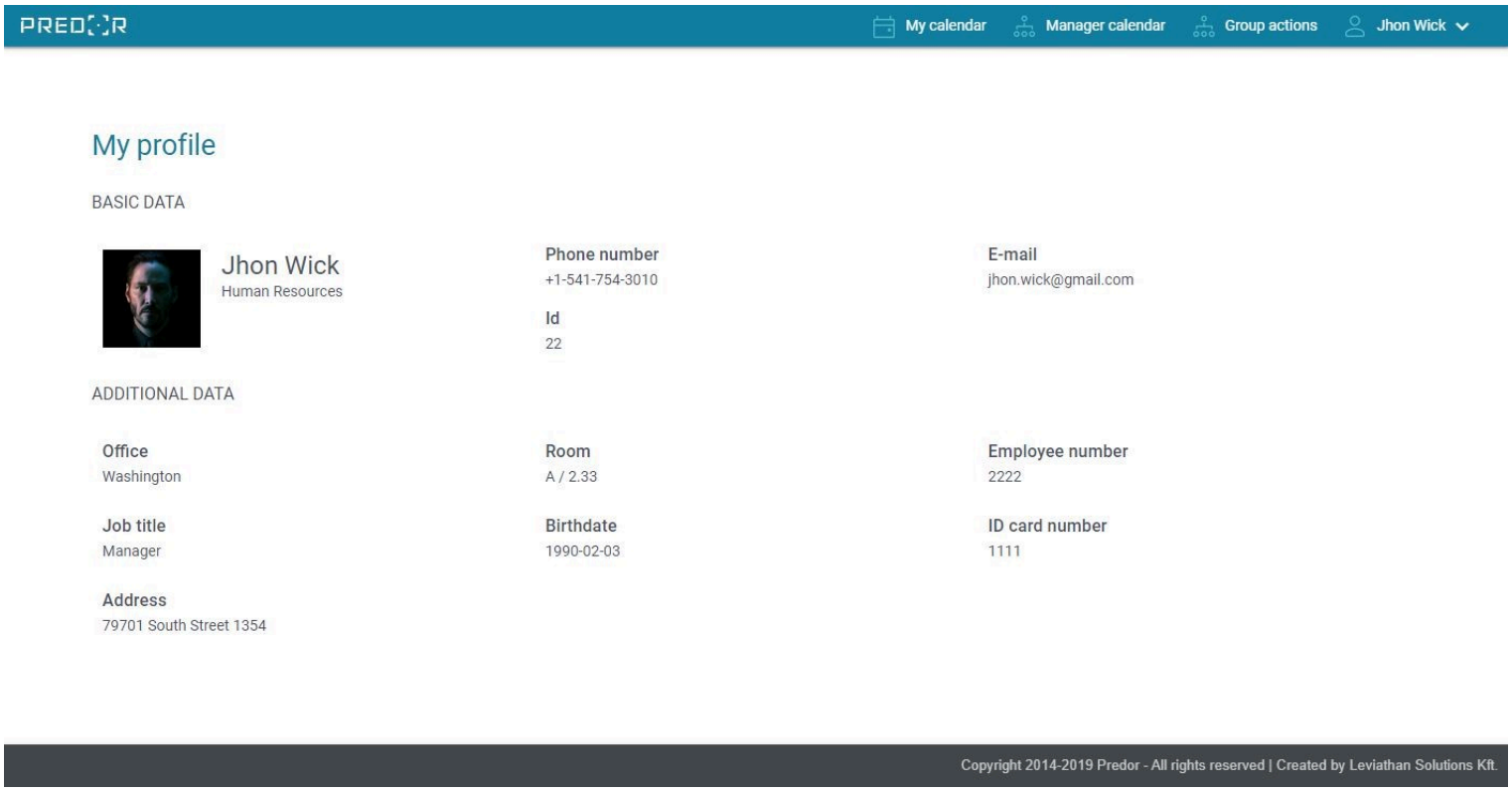


Figure 167: Web interface - my data page

You can change your PIN code by opening the drop-down menu under your name, and selecting the “Change PIN code” menu.

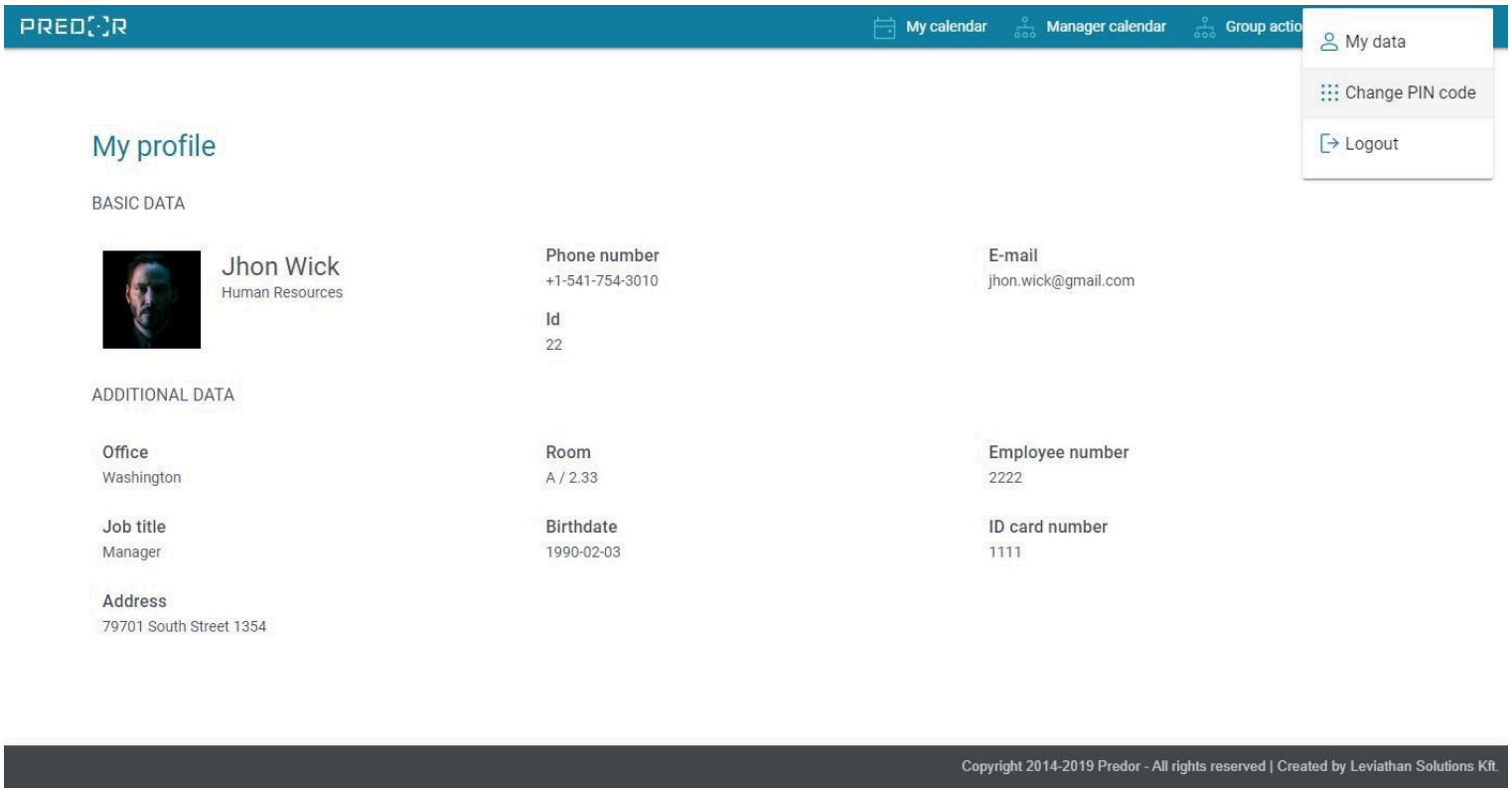


Figure 168: Web interface - change PIN code

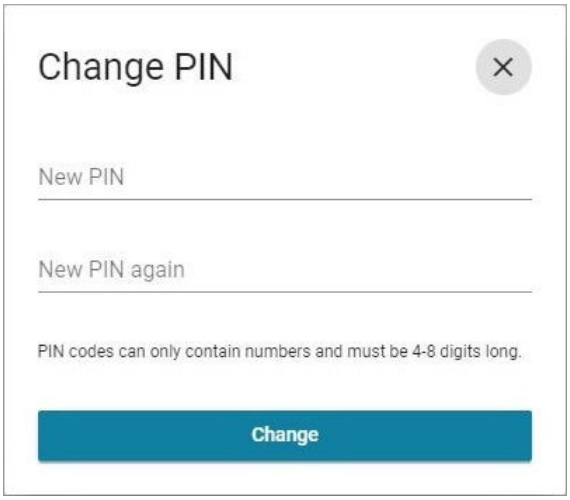


Figure 169: Web interface - change pin dialog

The worktime web settings can be configured in the **Web settings** submenu. For more information, see Web settings.

My calendar (employee web interface)

In this calendar, employees can view their assigned shifts, worktime data, worktime balance, yearly day off limits and the used days for each day off type.

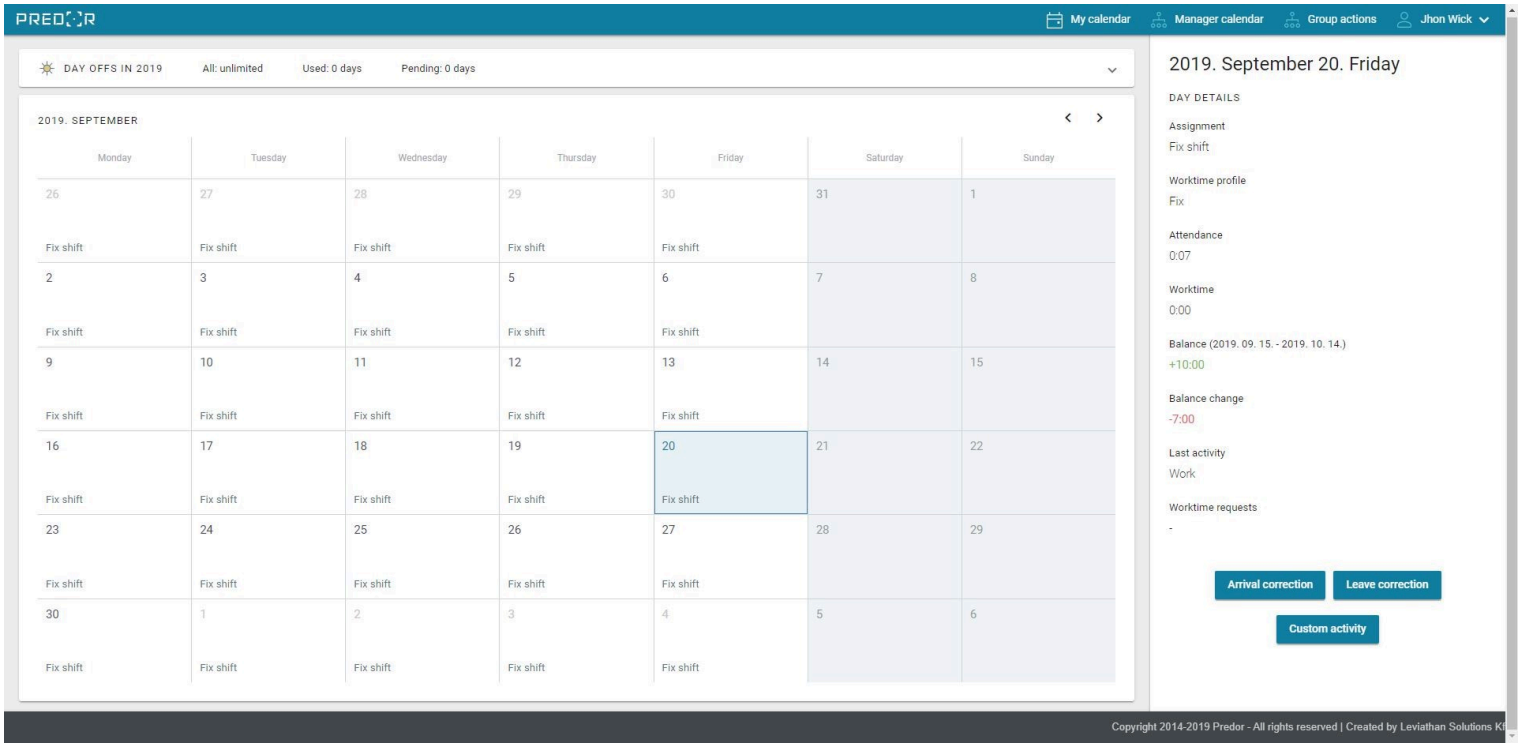


Figure 170: Worktime web - calendar view

Request day off, shift and overtime: under the “my calendar” menu select a day, and after that click the “Request day off” or the “Request shift” or the “Request overtime” button. A requested day off, shift or overtime that is not yet accepted can be withdrawn. (Employees are not able to modify off days in the past).

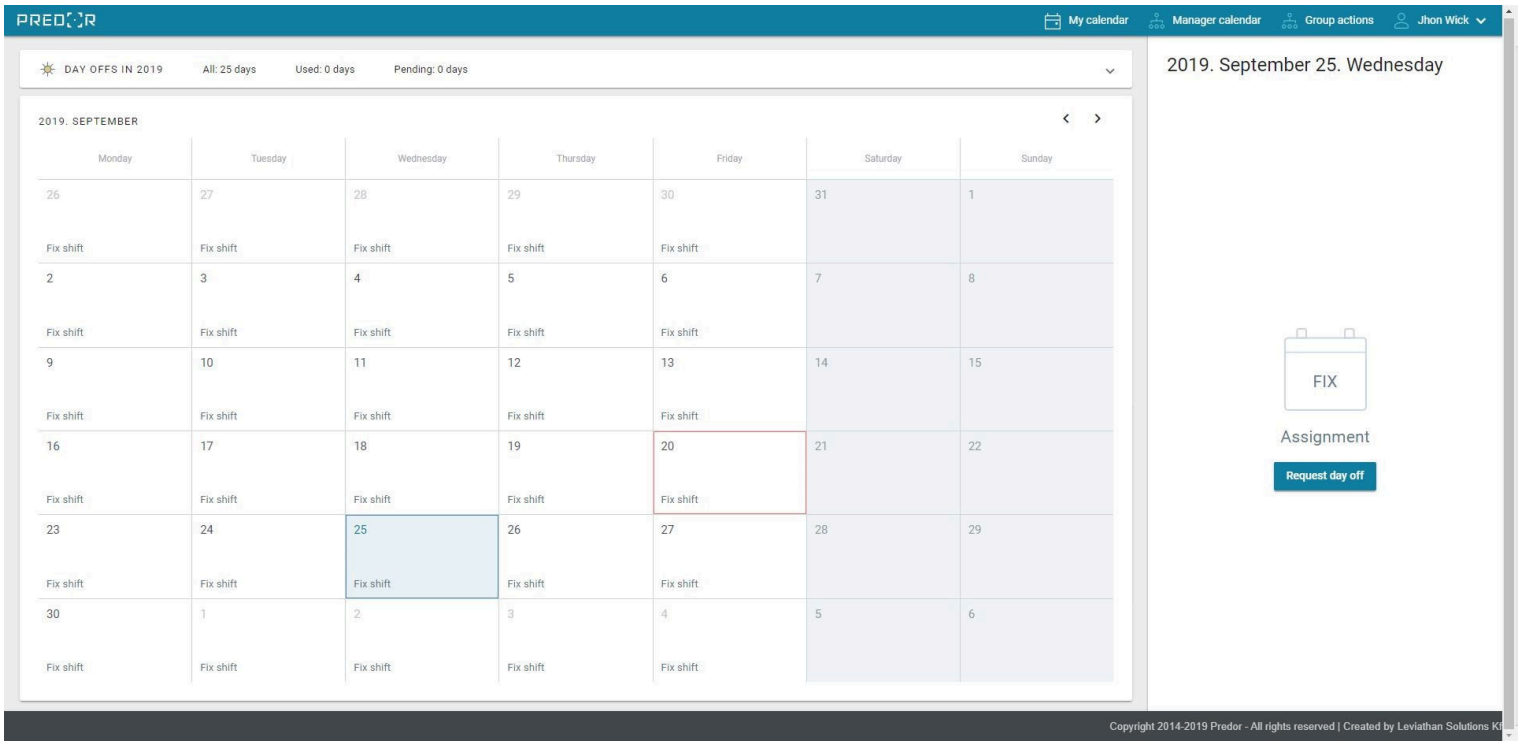


Figure 171: Requesting day-off with the sidebar button

On the pop-up window you can request a longer period.

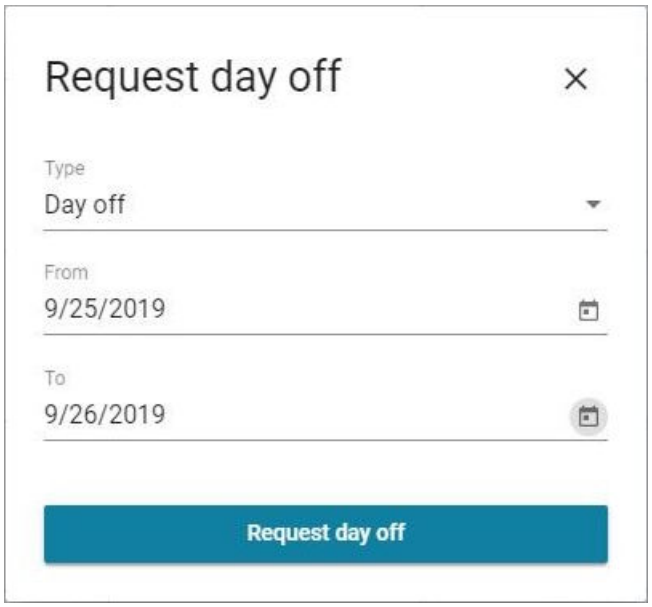


Figure 172: Requesting off day on the web interface

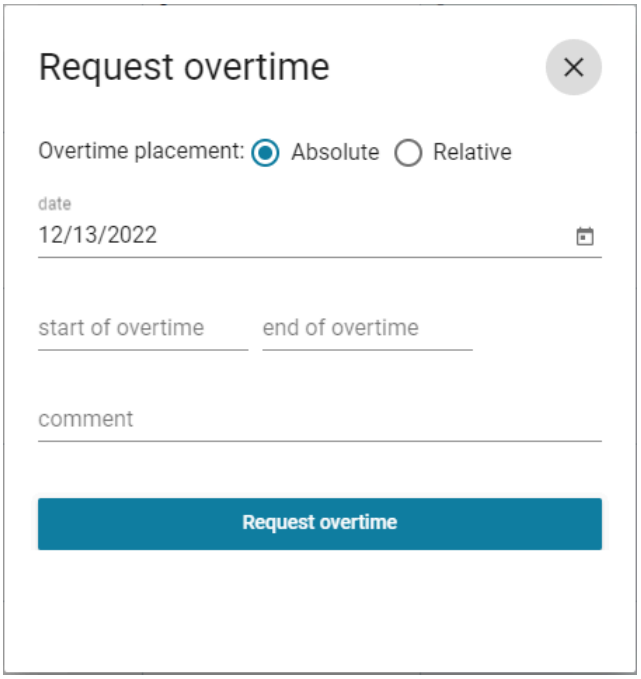


Figure 173: Requesting overtime on the web interface

Off-site work registration: You can register an off-site work by clicking the custom activity button when selecting a day; in that case you have to give the time when the work has started and ended. After that, select the activity code that represents an off-site work. (If you do not see that activity code in the drop-down menu, you have to add it the selectable activity codes on client software configuration window). If the supervisor approved it, the worktime module will process the work. You can also save the location where the work has been done by ticking the "Save location" checkbox (note that registering an activity from a desktop computer may result in an inaccurate location).

Arrival, leave correction: If the employees forgot to identify themselves upon arriving or leaving, they have the option to register a correction for that. For example, if a manager approves a leave correction, every event following the leave entry will be ignored (as if we had modified the daily activity report in the client software).

If we allowed it in the Web settings, at the top left corner of the calendar the PDF icon will appear. By clicking on it we can download the attendance sheet. If the month is not locked yet, a *draft* sheet will be downloaded in pdf format. A month can only be locked by a responsible user or operator.

Manager calendar

You can assign responsible users to departments in the client software, under the "Users and departments" menu. A responsible user will be the manager of the users in those departments.

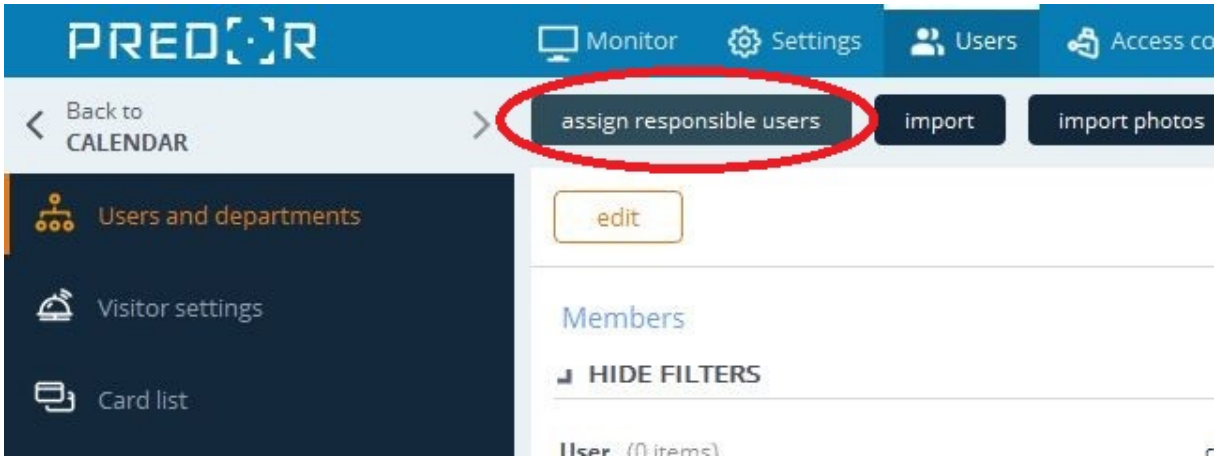


Figure 174: Assign responsible users in the Users and departments menu

The manager (responsible user) can assign shifts by selecting a user, then a day. In the dialog we can assign a shift for a range of days. The manager can also correct the time of arrival or leave, assign day off, rest day or overtime, and write notes for the given day, which can be seen by the employee optionally.

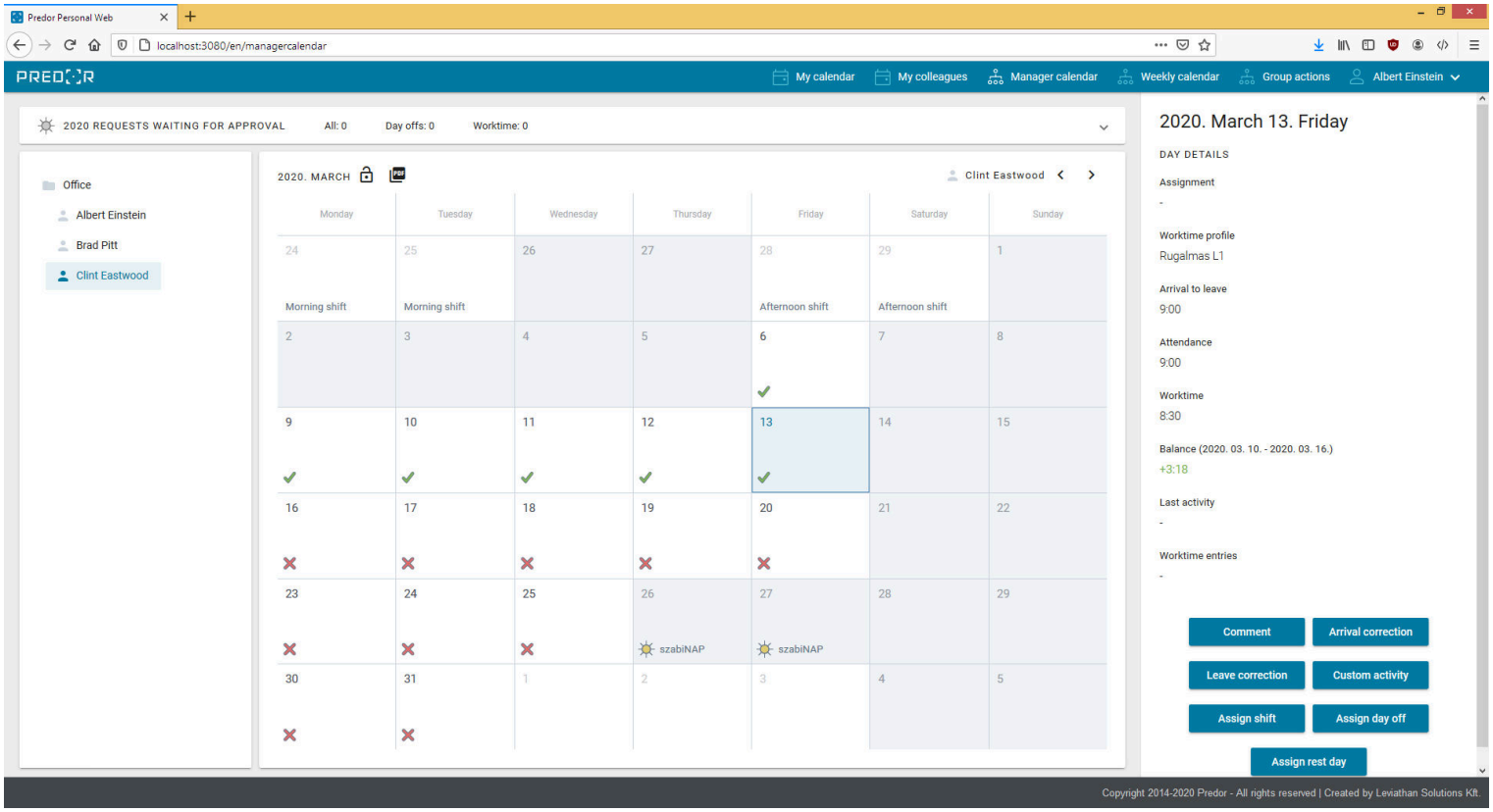


Figure 175: Manager calendar

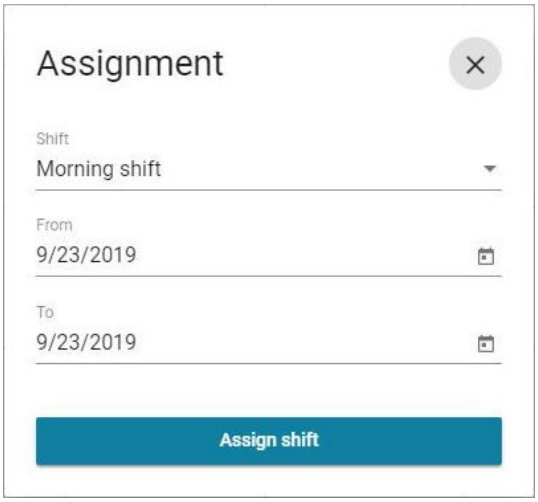


Figure 176: Employee assignment in the manager calendar

As a manager, you can assess the requests one by one via selecting the day, or in groups. An automatic e-mail notifies their superiors about the submission of subordinates' requests, if the Smtp settings are configured correctly.

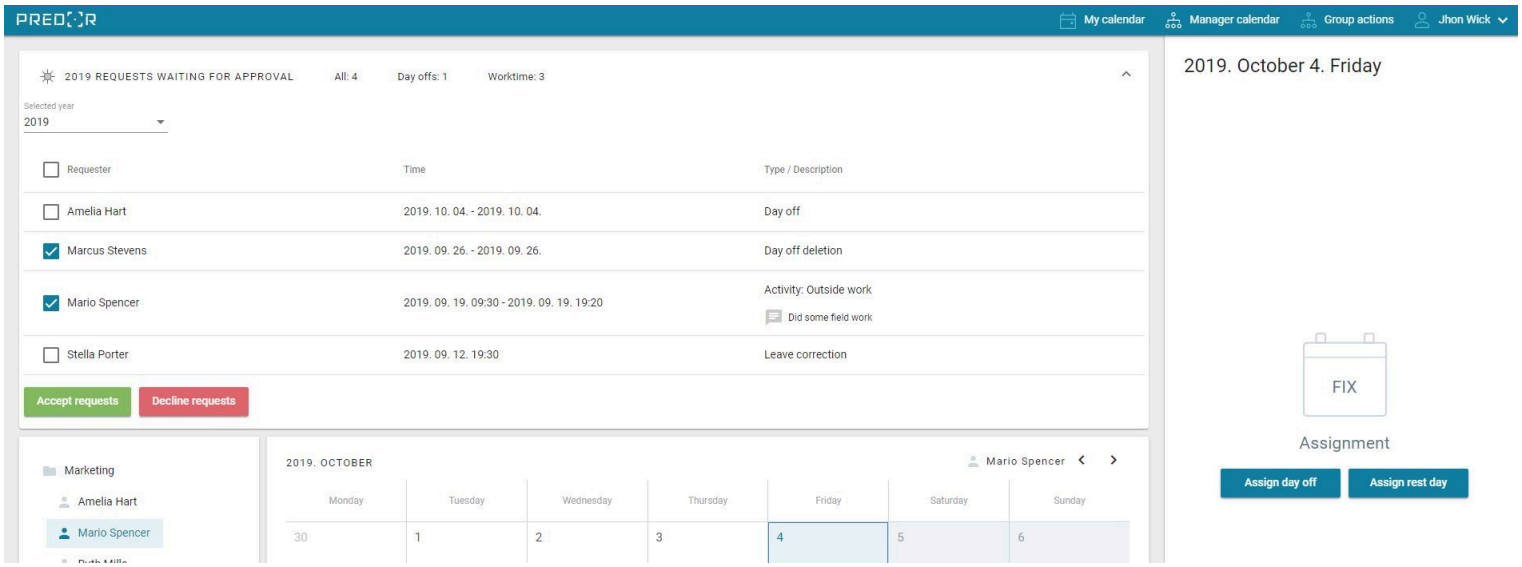


Figure 177: Assessing day-off requests

You can also order a day off without a request.

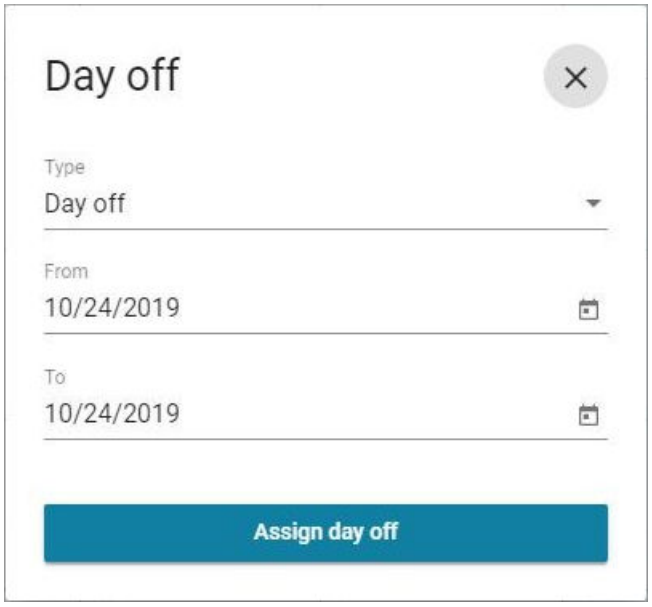


Figure 178: Assigning off day in the manager calendar

You can accept overtime requests on the manager calendar as the day-off requests. Both types of overtime (absolute, relative) can be scheduled without request.

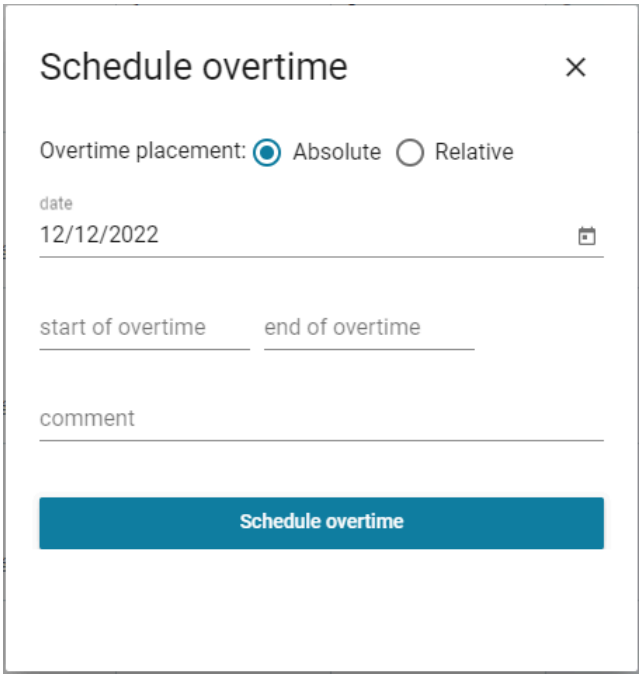


Figure 179: Scheduling overtime in the manager calendar

Clicking on the on the top left corner of the calendar will lock the month. No further corrections (arrival/leave time, day off requests) can be made to a locked month, and all pending requests will be refused. A month can only be unlocked by an operator in the client software.

Clicking on the PDF icon will download the attendance sheet. If the month is not locked yet, a *draft* sheet will be downloaded in pdf format. A month can only be locked by a responsible user or operator.

Weekly calendar (manager calendar)

This view can be used for managers to get an overview of their subordinates' shift assignment, day offs and day off requests.

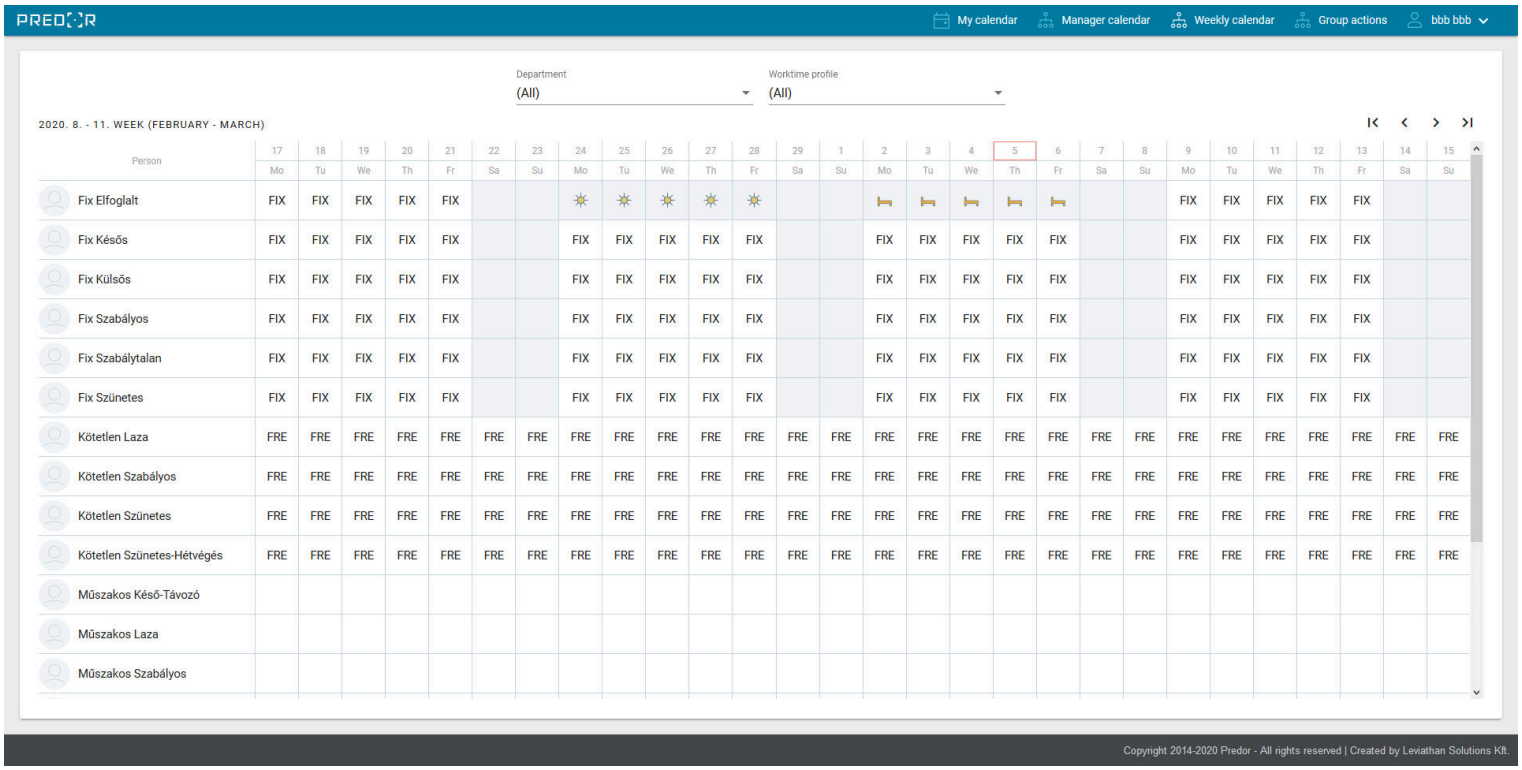


Figure 180: Weekly calendar

My colleagues (employee calendar)

If the worktime web is configured to allow viewing assignments and days off between employees, they can view it here, but only for those who are in the same exact department (sub-departments are also excluded). Employees not assigned to any departments are interpreted to be in the same department.

Webterminal

Registering an activity can only be done retroactively, closing by today. The activities can not cover each other, but multiple can be requested for one day.

Employees that do not have a superior or they are their own superior, get their requests accepted automatically. Every other employee's requests have to be handled by their supervisor using the web interface.

The arrival and leave correction work the same way. It is important to note, that the arrival and leave entry will be the first, and last eligible event for that day.

If the requested activity's time fall on a period where multiple shifts can be read, the user will be prompted to select the desired shift. The user will only one shift to choose from if he- or she already has a shift assigned to.

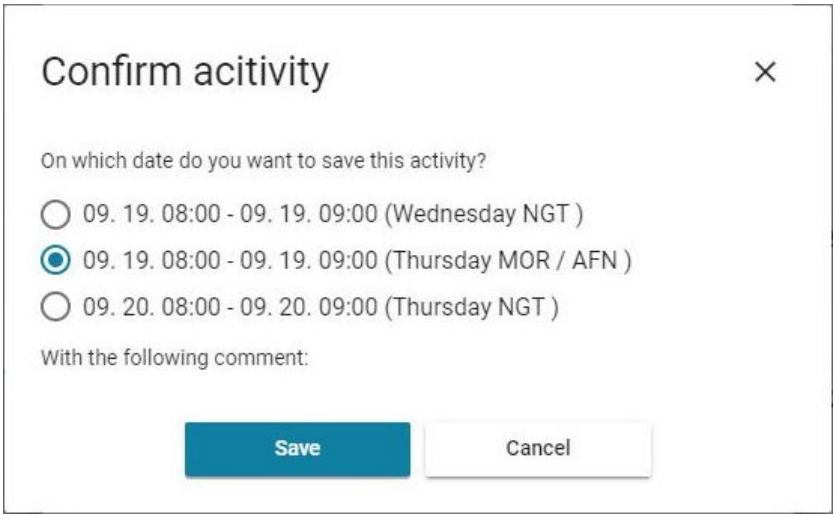


Figure 181: Registering an activity on the webterminal

Group actions

As a manager, you can register an activity for multiple users at once by selecting the "Group actions" menu. The first step is to select employees. You can filter out the departments that you want to choose from.

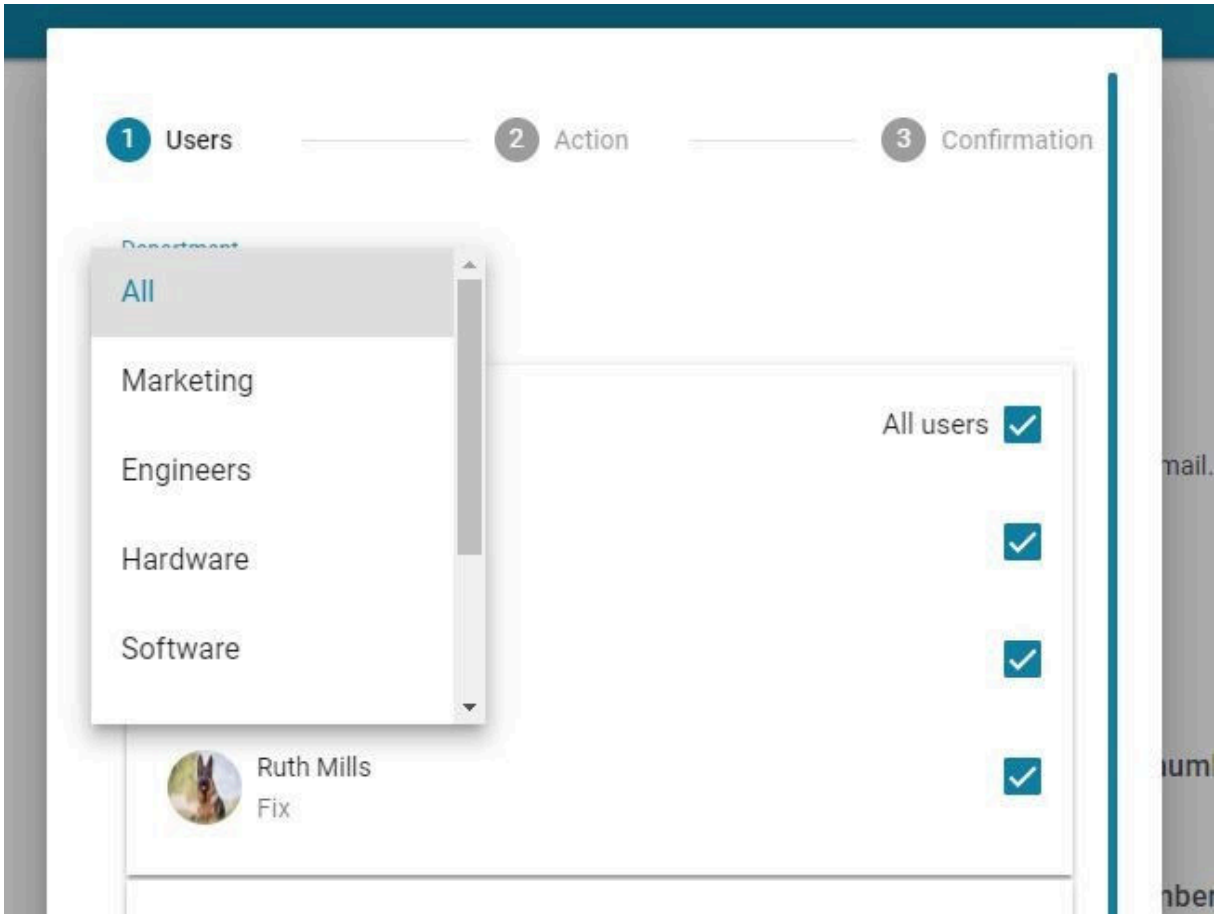


Figure 182: Selecting groups

After that, clicking on a department will list the users in it. Then you can select users individually, or an entire department.

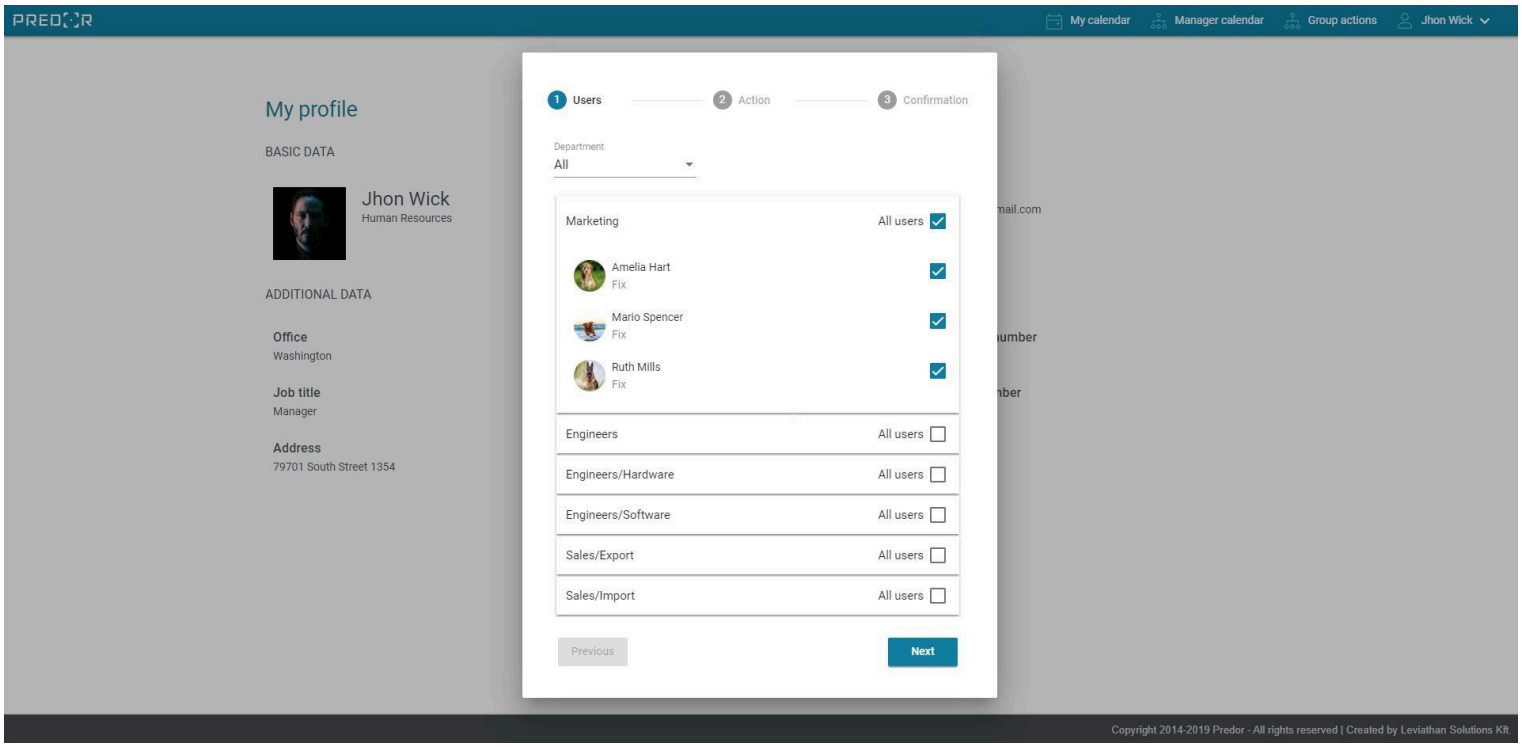


Figure 183: Selecting department on the webterminal view

Clicking the next button will take you to the next step, where you can choose the action you want to execute. This can be either a “leave correction”, an “arrival correction” or a “custom activity”. Configuring these actions works exactly the same as mentioned above.

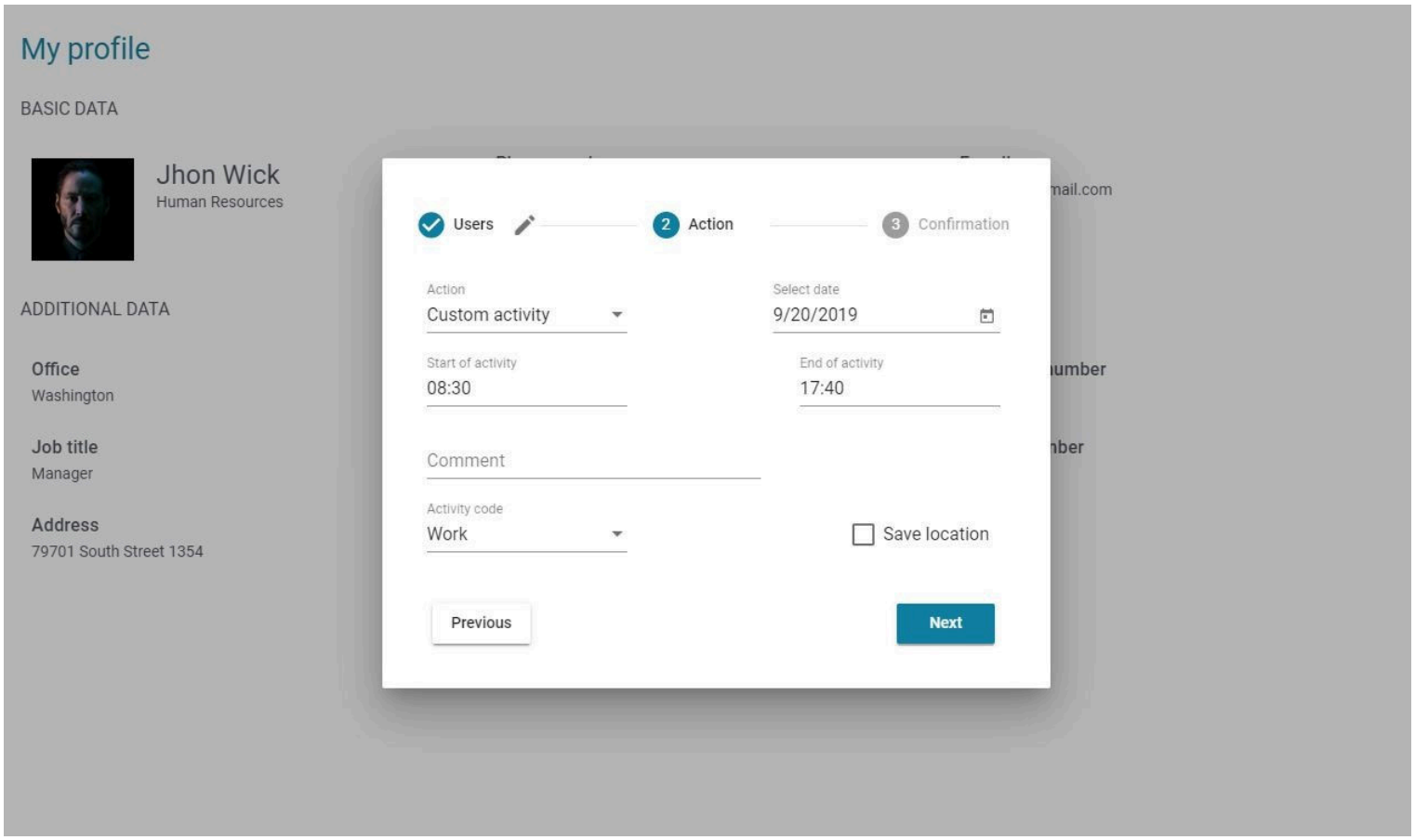


Figure 184: Registering a custom activity for a group on the webterminal

If everything filled out correctly, the last step of this process is going to be a confirmation.

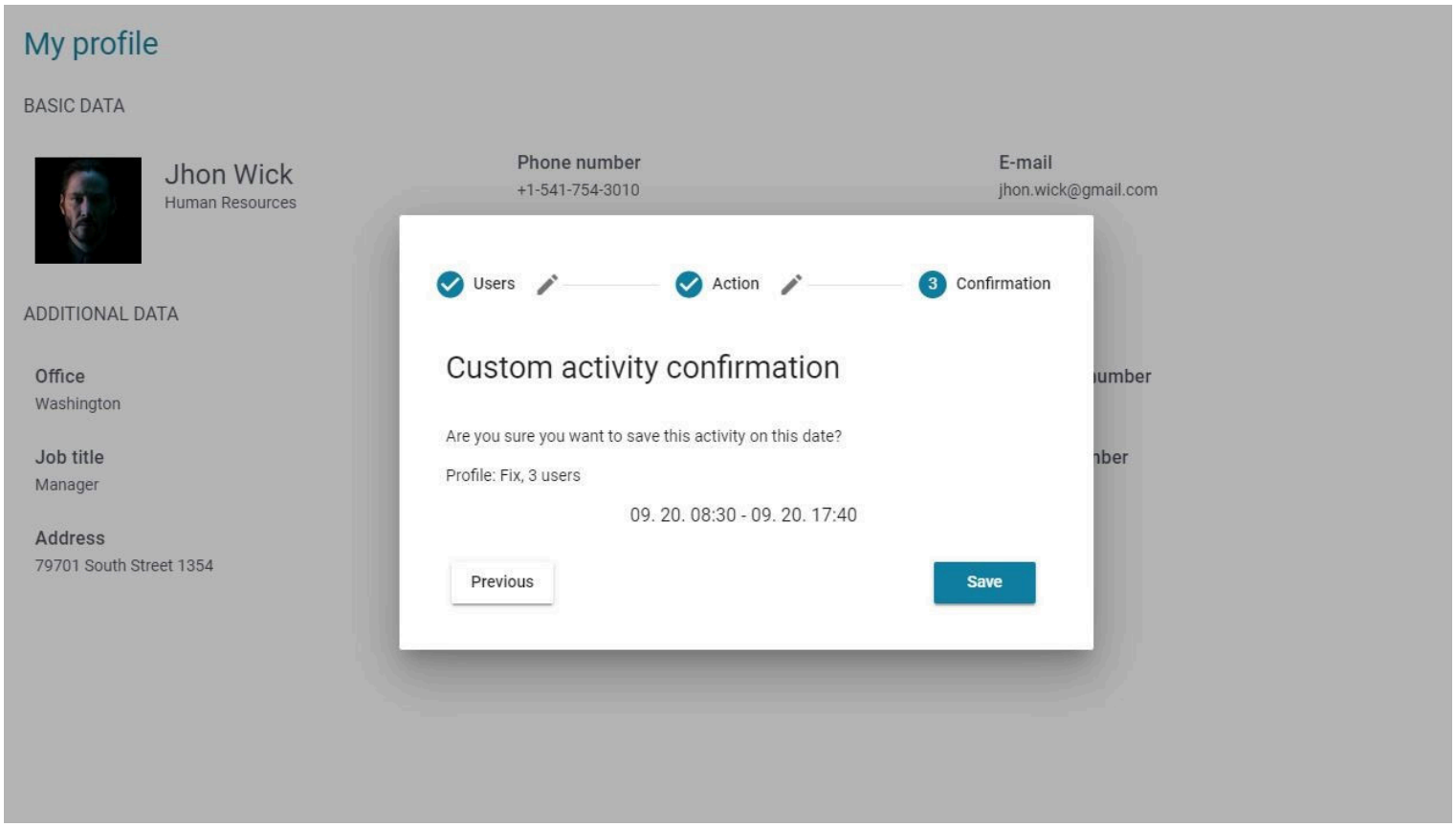


Figure 185: Custom activity confirmation window

12 OPERATION OF THE PREDOR WORK TIME PROCESSOR

For proper understanding of how the work time reports calculate the results and what value to correct if needed it is necessary to take a glance at how the Predor work time processor operates. In this section we get an insight about how movement data become work time reports.

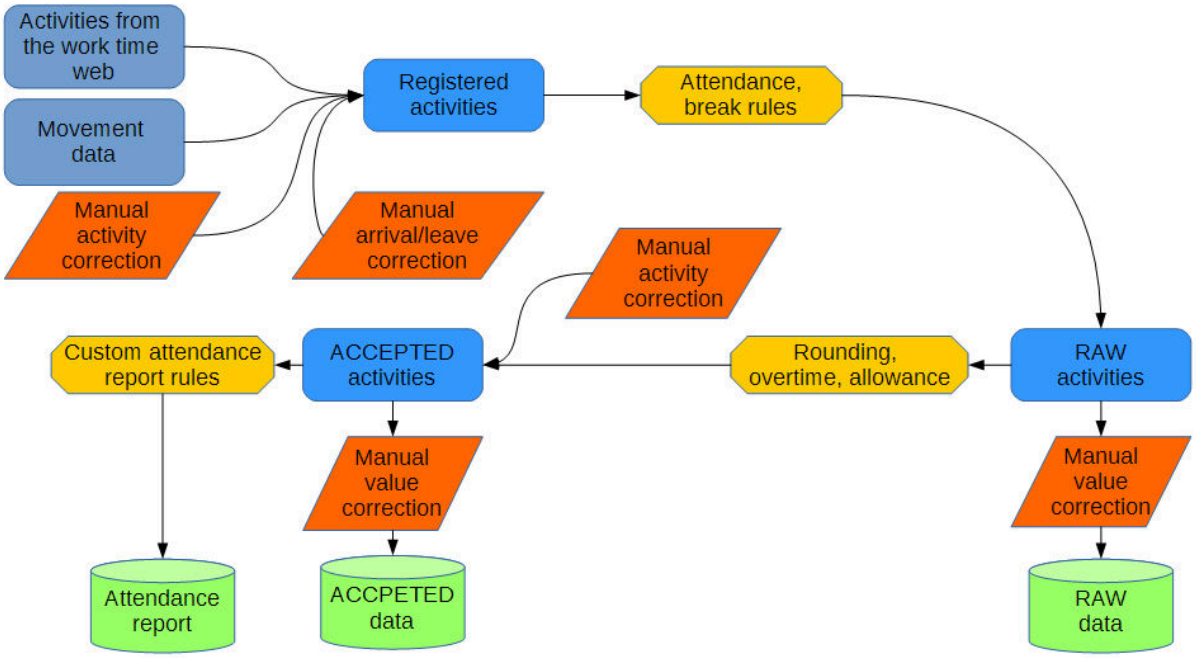


Figure 186: Flowchart of the Predor work time processor

On the figure we marked with blue the data handled by the system, yellow the rules corresponding to work time profiles, orange the manual correction inputs and green the output.

It is important to note that manual correction has two categories which are handled differently in the system: manual **activity correction** and manual **value correction**.

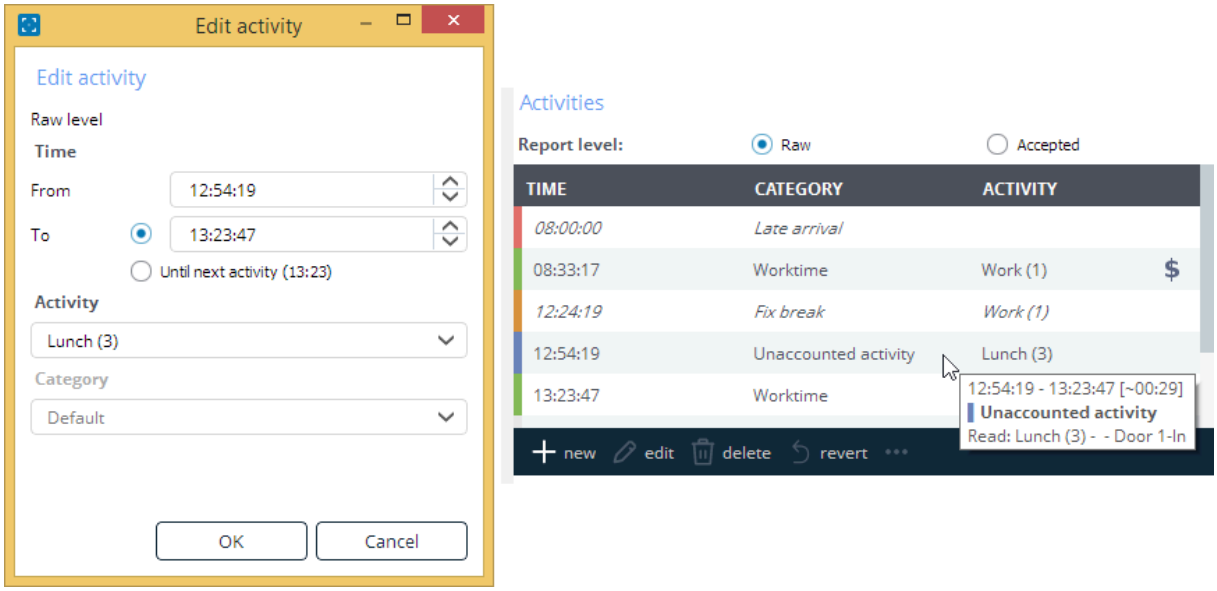


Figure 187: Editing an activity in the Daily activities report

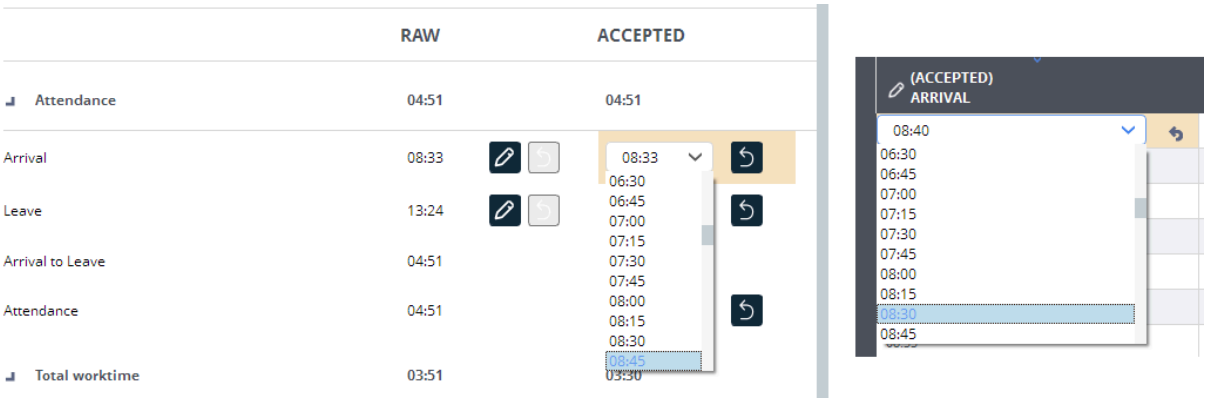


Figure 188: Value correction in various reports

The most basic information that the access control units and the work time terminal collects is the **movement data**. Movement data consists of a time, a user and a place of identification. In the Predor system this information is supplemented by an activity code which indicates the intent of the person requiring access to the area.

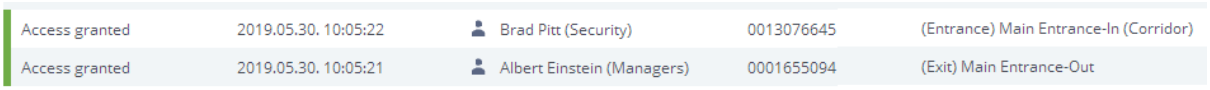


Figure 189: Movement data in the monitor view

By following every person's movement data the system can measure elapsed time spent in each area, and with the help of activity codes the system can decide if the person worked or not. These elapsed times in conjunction with the activity codes therefore are directly

generated from the movement data and are called **activities** in the system. These automatically generated activities are then completed with activities registered in the work time web interface. Activities are editable in the *Daily activities* report only. In this report time of arrival and leave can be corrected, activities can be edited, deleted or new ones registered. Registration of activities is possible on two levels regarding to the process:

- RAW: On the flow chart this is the first parallelogram. Activities registered (or modified) here work just like they were collected by the system at access points, all the work time rules are applied on them in the process.
- ACCEPTED: On the figure this is the second parallelogram, directly before the accepted activities are made. Activities registered or modified here are not subject to the work time rules set for the profile, thus it is possible to violate the rules (for example we can add overtime for a profile that normally doesn't handle it).

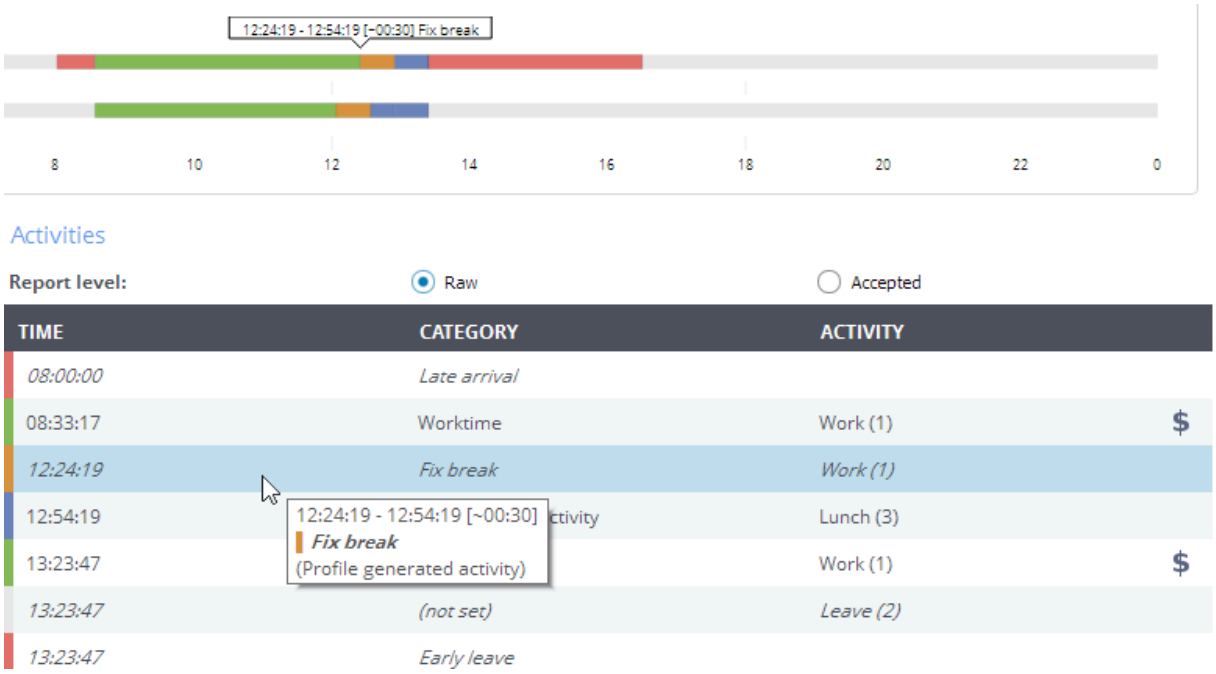


Figure 190: Activity in the software

The rules set in the work time profile regarding arrival, leave, accepted time period and brake handling are then applied to the collected and manually registered activities, which can generate work time violations. These violations can be overridden in reports where the RAW values are editable.



ATTENTION! As it is shown in the figure of the working principle, corrections of the **RAW values** – unlike corrections of the **RAW activities** – does not affect the ACCEPTED data!

After taking manual corrections of the RAW values into account, the **RAW data** which are shown in the reports are created. Such RAW data is for example the actual time of arrival, leave, late arrival, early leave and core time violation. Pictograms shown in some reports are based on the RAW data.

RAW data are processed further, rounding and other rules are applied on them, overtime and allowance is calculated, etc. Corrections of the processed values is possible in reports where the ACCEPTED values are editable. With the corrections taken into account, the **ACCEPTED data** which are shown in the reports are created.

Data on the attendance report is further processed where custom – different from ACCEPTED – data can be shown, if needed.

13 ADDITIONAL MENU

Software upgrade

When a software upgrade is available, the system will show a notification on the dashboard. Initiating an upgrade is a manual process. We have to close the currently running instance of the application and use the “Maintenance tool” located in the install directory.

It is strongly advised to create a backup of the install directory and the database before updating. The Maintenance tool connects to a remote server, then downloads and installs the newest version. After the installation is complete the upgraded software is ready to run.

License manager

If the system is not yet activated, a bright read button appears on the left side of the screen that navigates to the license manager page.



ATTENTION! The license activation has to be initiated from the computer where the software (in Enterprise edition the Server) will run.



ATTENTION! In order to activate the license, at least one controller (or terminal) has to be added to the system. Uploading settings to the controllers is only possible with activated license.

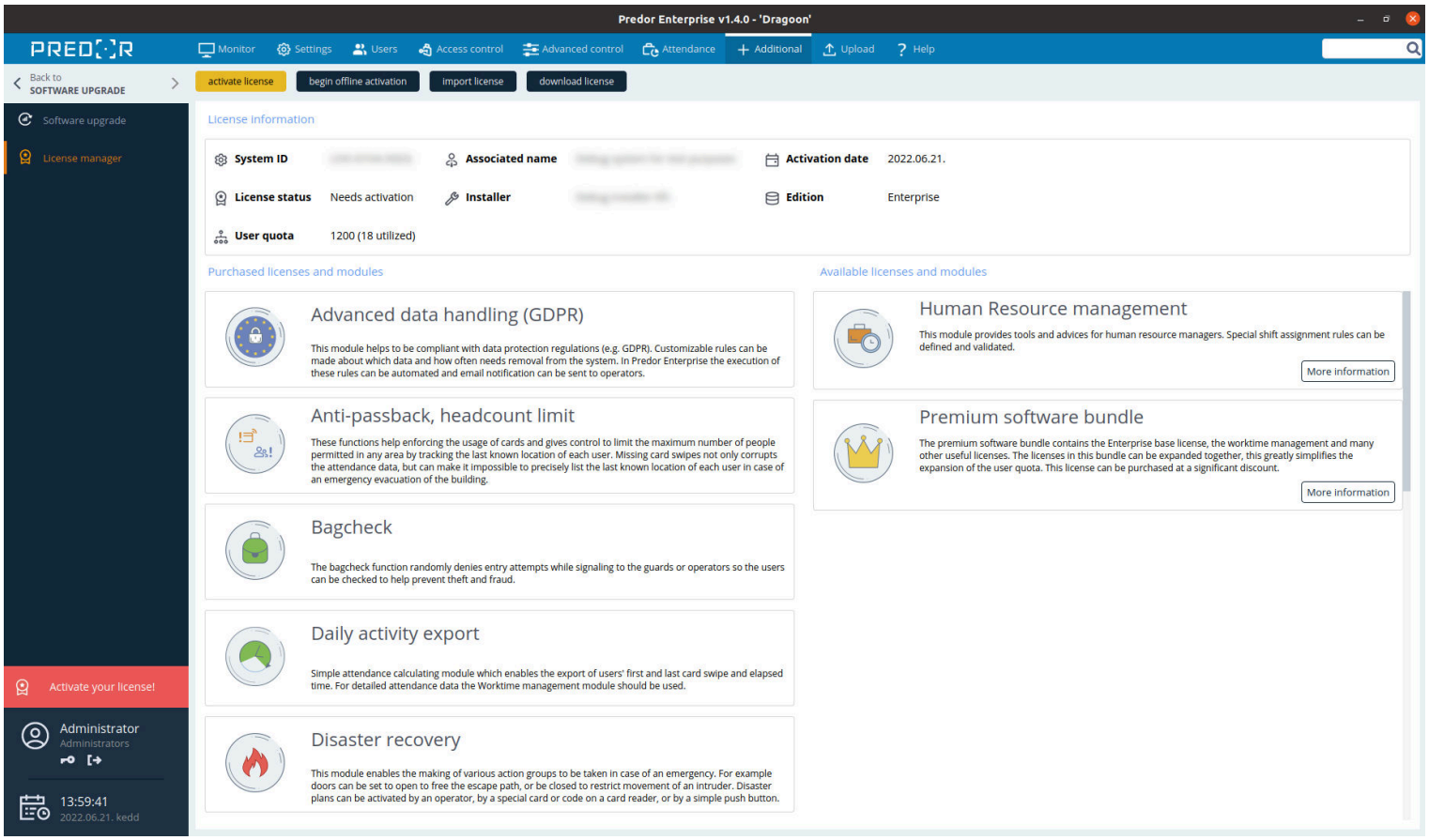


Figure 191: License manager view with purchased and available modules

Before the license activation, uploading the user (and other) data to the controllers is blocked. The activation fails if the system ID is already used on another computer.

Online license activation

If the system is able to access the Internet, you can easily activate your license with the yellow button on the upper toolbar. If you experience problems, follow the displayed instructions or contact the customer service: info@predor.hu

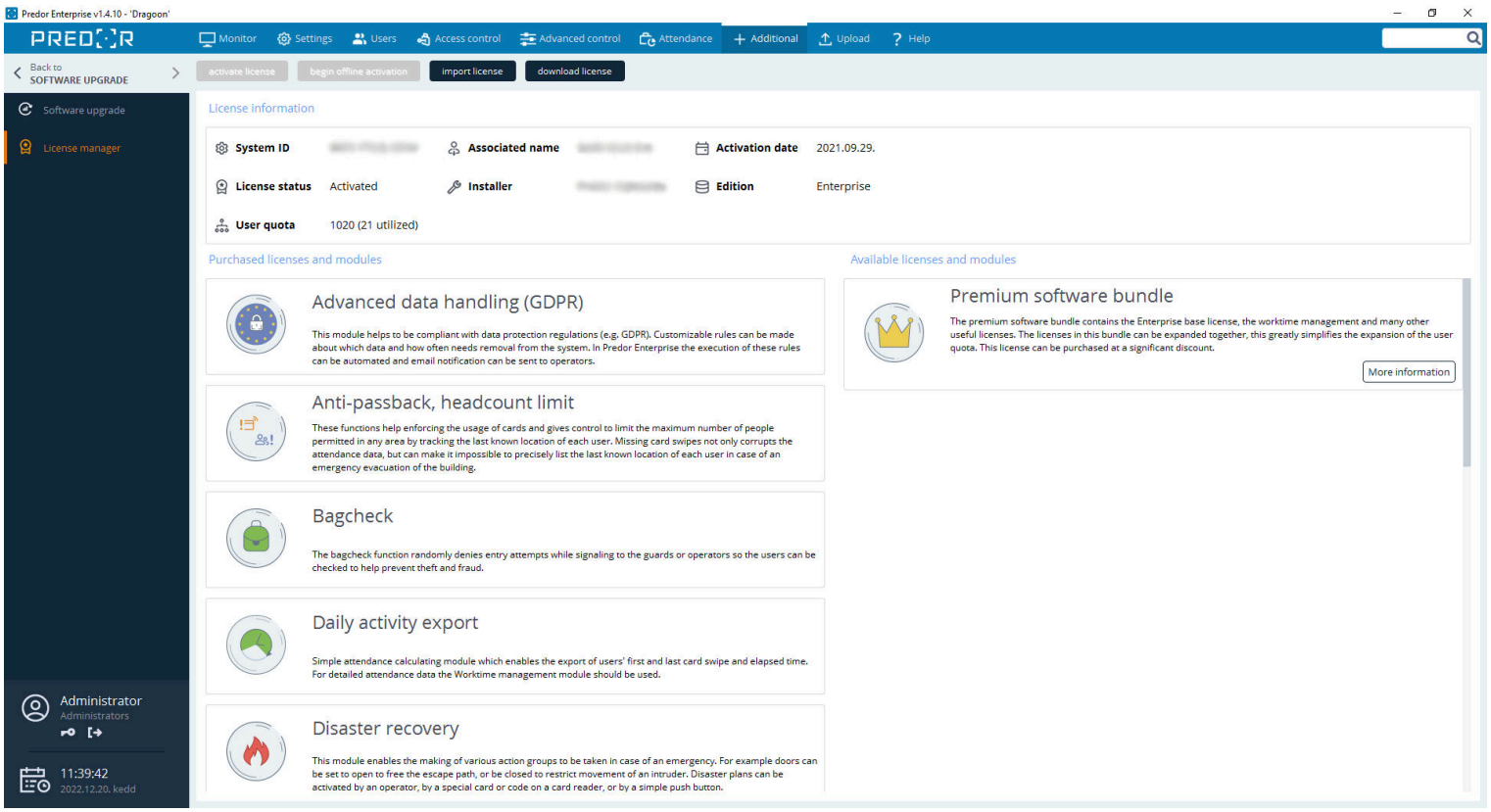


Figure 192: License manager with activated software

Offline license activation

This method is more complicated, therefore we only recommend to do this, if there is no way to access the Internet. You can start the process with the toolbar button “begin offline activation”, and then follow the instructions.

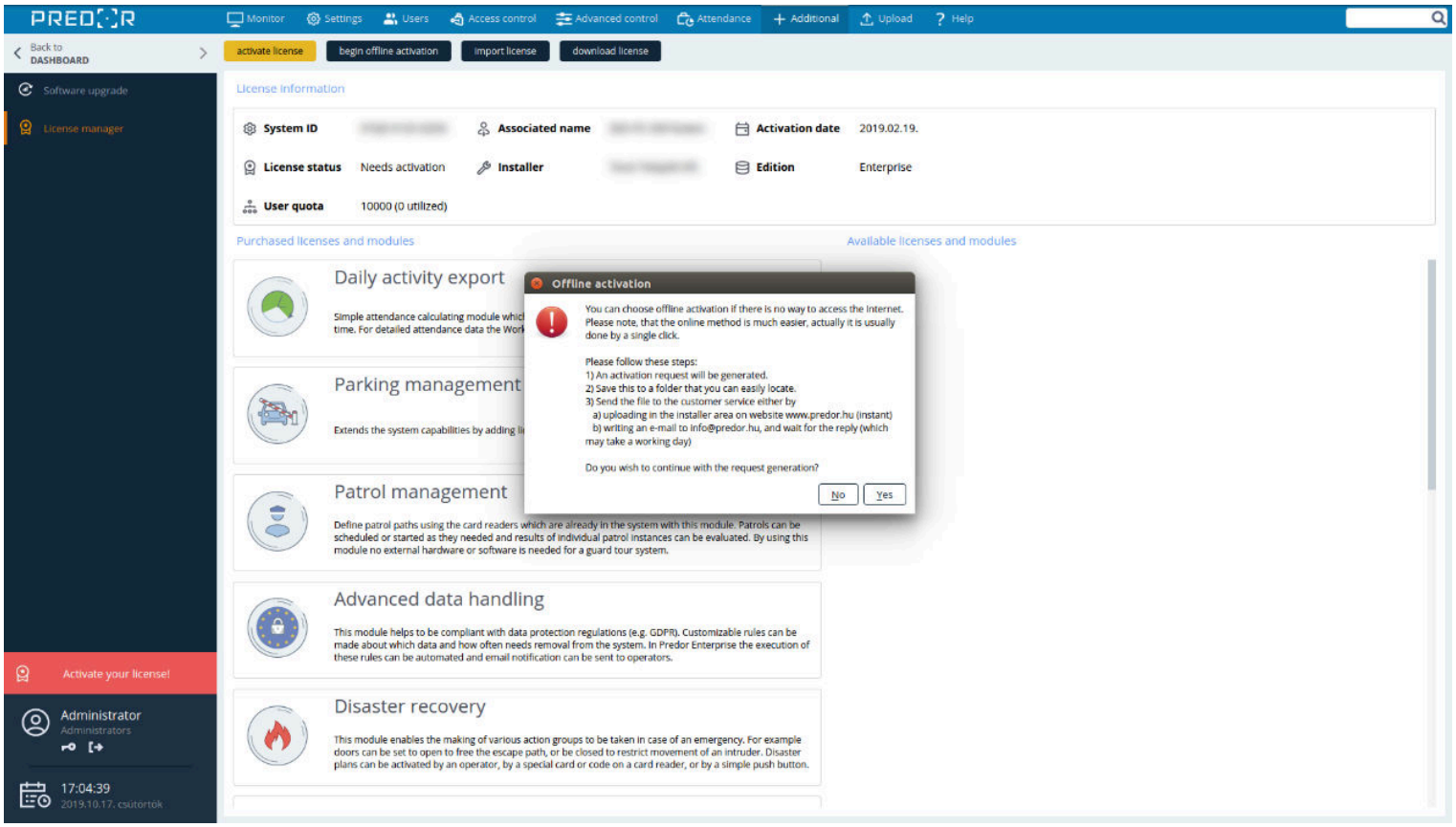


Figure 193: Initiating an offline activation

The steps in short:

1. step: Generate an activation request, save it to a file.
2. step: Copy this file to a computer, which can access the Internet.
3. step: Upload the file on the website www.predor.hu in the Installer area (after logging in), using the button “Upload activation request” on the system’s datasheet.

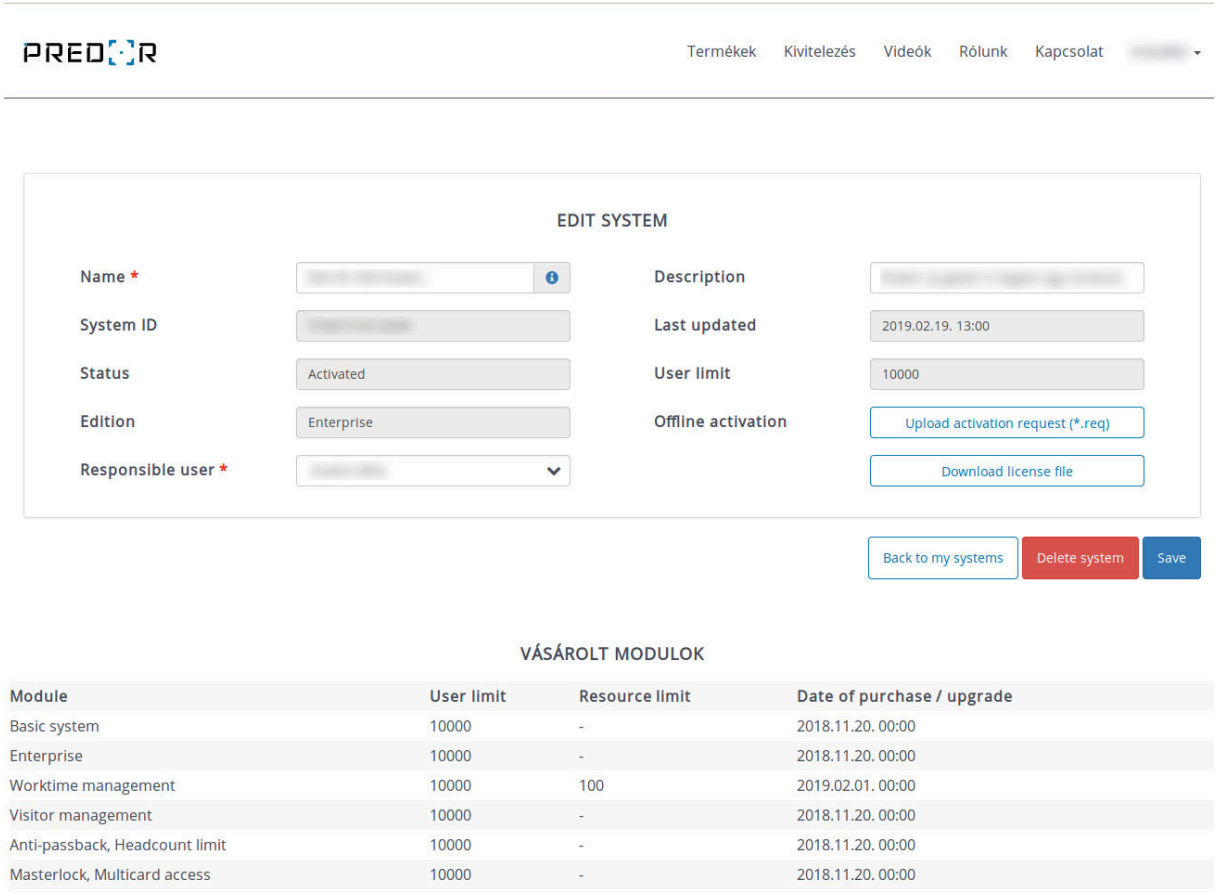


Figure 194: Predor website with the upload activation request button

If you experience problems, follow the displayed instructions or contact the customer service: info@predor.hu

4. step: After the successful activation, please download the license file, and move it to the target machine.

5. step: In the Predor client, select “import license”, and browse the file.

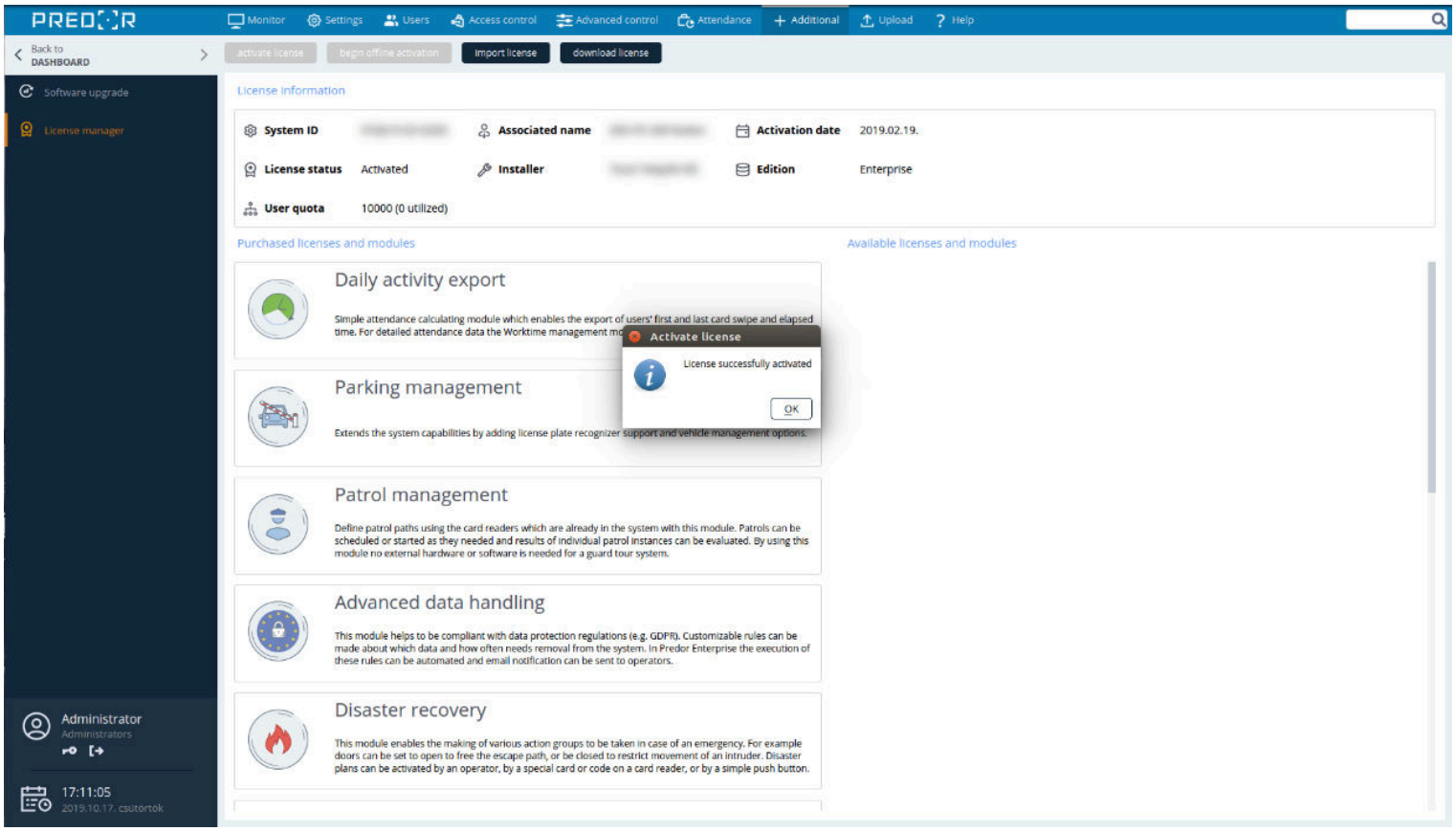


Figure 195: Successful offline activation

14 UPLOAD MENU

Upload

In the upload submenu you will see the pending changes by selecting controllers from the list.

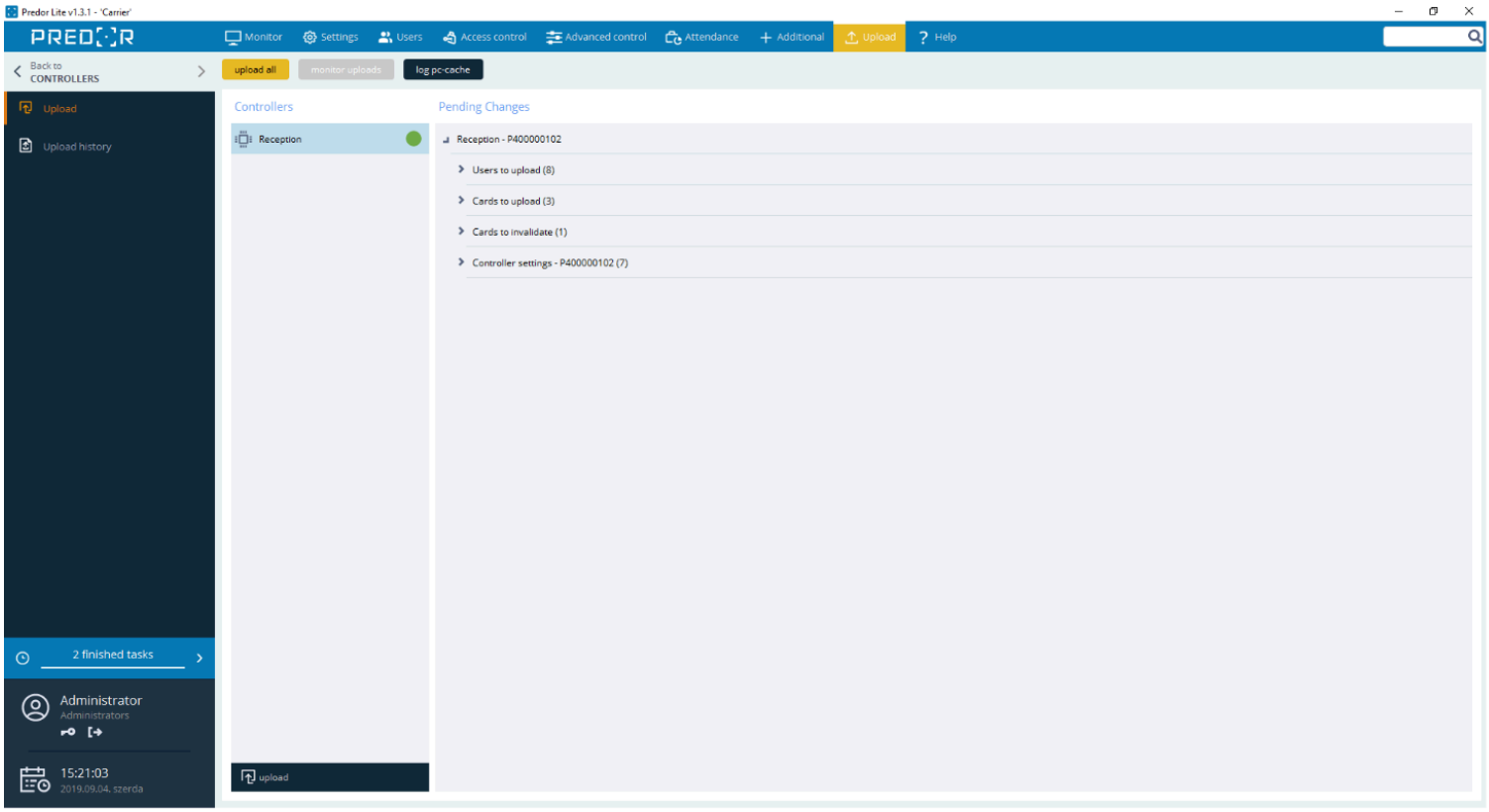


Figure 196: Data in the upload queue

The “upload” button on the bottom, will only start the process on the selected controllers, while the “upload all” button on the top will start the process on all devices.

You can track the undergoing upload procceses by clicking the **“monitor uploads”** button. This dialog is automatically displayed when initiating an upload. Closing this dialog will not cancel any running processes. If you intend to cancel the ongoing upload, there is a button with mark X in each row for each controller, or you can cancel all with the button on the bottom.

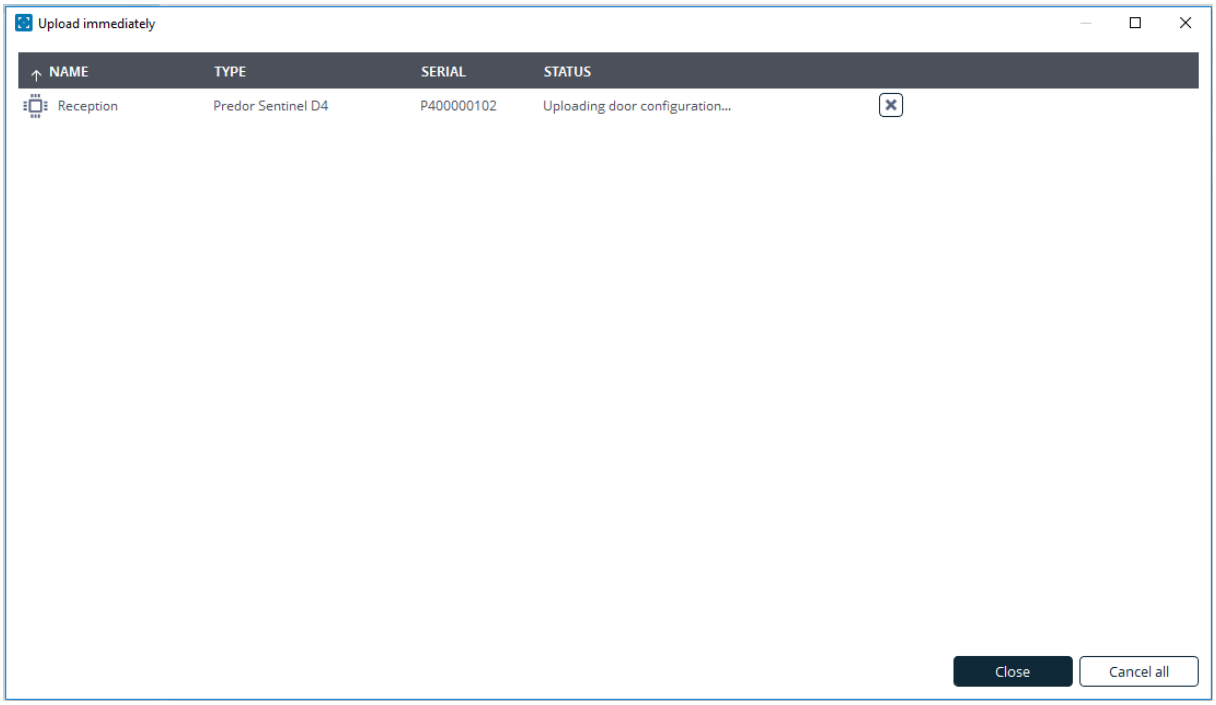


Figure 197: Uploading in progress

15 SUBSYSTEM MANAGEMENT

By purchasing the **Subsystem management module**, it is possible to manage multiple subsystems in the system. Subsystems can be managed by the Manager Company within the Subsystems submenu of the Settings menu. The manager operator has access to the data of all subsystems and can manage the access rights (by logging into the corresponding subsystem). Subsystems can manage the rights of operators and users belonging to the subsystem separately. The entire System Settings, Controller Settings and Disaster Management menus belong to the manager operator, and cannot be accessed by a subsystem-assigned operator. The manager operator has the rights to manage the settings of cameras and number plate recognition devices belonging to the system. They can share the cameras with subsystems so that their operators can view the live stream of the cameras or create recording rules. The Database menu is also only available to the manager operator. The configuration of access zones, time profiles, door profiles, interlock, advanced access is the responsibility of the manager operator, but for some of these interfaces, other subsystem operators can have read and modify rights.



TIP: The use of the module is recommended for office buildings, for example. Access rights can be set for common access points per company. Companies do not have access to each other's data, so monitoring and time recording is more transparent.



TIP: It is also recommended for companies with several sites or industrial parks. Entry points, employees, authorization groups can be separated by site, making data and events more transparent and easier to search.

Operator management

The operators of the Manager Company have access to the other subsystems' settings and data, and they can also manage the list of subsystems. Manager operators who do not belong to any subsystem are the administrators of the system. However, this does not mean that they have unrestricted access to all data of all subsystems. The availability of data/settings is defined by the operator group linked to the operator. An operator can be assigned to several subsystems with different permission groups (operator group). The assignment can be modified afterwards by an operator with the appropriate rights. Operators, if they have access to more than one subsystem (including the manager level), can choose which subsystem (or possibly as a manager) they wish to log in when logging into the client software. Based on this choice, the system will assign the appropriate operator group and their rights will be enforced. The chosen subsystem can be changed, but this will start a new session, logging out may be required.

Device management

Devices managed in the system can be linked to subsystems as described below:

- **Controller:** cannot be assigned to a subsystem, because it can handle multiple doors, so instead, card readers or zones can be assigned to a subsystem. Access to the reader and zone can be granted at three levels of privileges:
    - Read: Allows the company operator to view events at a given location that are related to users/operators assigned to the subsystem.
    - Modify: Still only events of own users/operators are displayed, but there is also the possibility to assign rights to own employees.
    - Owner: Has the rights to view all events at a given location - but only the name and subsystem of users from an other subsystem can be seen -, can manage access rights for own employees, and remote access is possible depending on the operator's other rights. If the subsystem owns all the readers of a door, it also owns the door itself. The profiles and managers of such doors can be set by the subsystem operator.
- **Terminal:** can be assigned to multiple subsystems, the settings for employees can be configured by the subsystems according to their own needs, but system settings for the device (e.g. IP address) can be configured only at the manager level.

- **Camera:** can be assigned to multiple subsystems to view the image, but the settings can only be configured by the manager operator.

User management

Users and departments can only be managed for one subsystem at a time. The department tree is completely unique and independent for each subsystem. Users can only be assigned to a single subsystem and this assignment can only be made once. After that, the user's subsystem cannot be changed. Deletion is possible. Deleting a subsystem will also delete all assigned users.

The access rights of own employees can be managed by the subsystems themselves for the access points where they have been allowed to do so.

Users can access the web interface. For them, the assigned subsystem is clear, so no choice is possible. The list of colleagues / employees is displayed according to the departmental structure set up in the subsystem. Employees of other subsystems are never visible to users on the web interface.

Event management

In the **Monitoring** and **Event List** menus, the manager operator can see events matching any of the following criteria:

- All events not related to the user
- All events related to own user (not assigned to subsystem)
- All events associated with a site for which the manager company has Owner rights

In the **Monitoring** and **Event List** menus, the operators assigned to subsystems can see events that match the following criteria:

- All events belonging to the users (assigned to the subsystem)
- All events belonging to a site for which the subsystem has Owner rights

The **Fire Alarm** events are visible to all operators for those door controllers with at least one reader allowed to view by them.

Manager settings

System settings can be configured by the manager operator. The settings listed here cannot be managed by a subsystem-assigned operator.

- **Subsystems:** The manager operator can manage subsystems in a new submenu. For each subsystem, it is required to enter a name, select the appropriate license package, and some other optional data can be entered. The manager operator can also manage the operator privileges under this menu, by defining the operator groups assigned to each operator. It is possible to deactivate or suspend operators. In the case of suspending, it is possible to restrict the access to a specific operator for a specific subsystem.



WARNING: Users, license plate numbers and the license package assigned to a subsystem cannot be changed after saving.

- **Doors and maps:** The creation of maps is mainly a manager operator task. We remove the restriction that a door can only appear on one map, and from now on it can be placed on any map. The "show on map" feature will show the door on one of the linked maps, and a button will allow to easily switch between the other maps.
- The complete contents of **System settings**, **Controllers** and **Disaster recovery** are belonging to the manager operator, they are not accessible by a subsystem operator.
- **Disaster recovery:** Evacuation is possible as a manager operator, for which all persons are displayed. Other operators do not have access to evacuation informations.
- **Cameras:** The manager operator is authorized to manage the settings of the cameras in the system. Cameras can be shared with subsystems so their operators can view a live stream and create recording rules.
- The **Database** menu is also only available to the manager operator.
- **Parking management:** The installation of number plate recognition devices can be done by the manager operator. New vehicles or vehicle groups can be added per subsystem.
- **Time profiles:** These are set by the manager operator, but read access can be granted to a subsystem operator.
- **Door profiles:** The door profiles are also set by the manager operator. A subsystem operator with read access can view the profiles and can also modify the profile on doors for which the subsystem owner has read access.
- **Interlock:** These settings can only be managed by the manager operator.
- **Advanced control:** The complete main menu belongs to the manager operator. No subsystem operator can see these settings.
- **Calendar:**

  - Manage day types: The manager operator can add different day types to the system. These can be viewed but not modified by a subsystem operator.
  - Company calendar: Several company calendars can be created in the system. These calendars define which type of day is relevant on which calendar day (changed workdays, holidays). The built-in company calendar can be viewed and used by all subsystems by default, but only the manager operator can modify its entries. (For a detailed explanation, see Company calendar chapter)

- **Manage recurring holidays:** Recurring holidays can be edited per calendar. The built-in company calendar can only be managed by the manager operator.
- The **day-off type management** and the **worktime web configuration** can be managed separately by the subsystems.
- **Worktime terminals:** The management of the terminals is handled by the manager operator, but the terminal can be shared with other subsystems. The settings for the displayed data can be customized by the subsystems, but the basic system settings of the terminal can only be managed by the manager operator.
- **License manager:** The manager operator has a complete view of the licenses purchased and can also see the number of user limit and modules assigned to each company. Activation and other operations can only be managed by the manager operator. An operator logged in to a subsystem can see their own user limit and purchased modules.
- **Upload:** The manager operator can see the changes to be uploaded without filtering. An operator of any subsystem with the appropriate rights can start uploading all changes.

Subsystem-related interfaces

The settings listed here can only be made by operators assigned to a subsystem. When logged in with a manager operator account, they should be interpreted in relation to users not assigned to any subsystem, as if they are in a virtual company.

- **Monitoring:** It is possible to view the events as described above. Each subsystem can create its own monitor profiles of the doors and terminals it has access to. These profiles are not visible to other subsystems.
- **Doors and maps:** The operator assigned to a subsystem can see the doors for which the subsystem has access to all readers. The list of doors and cameras displayed on the maps is filtered so only those doors and cameras are displayed which the subsystem has access to. Door controllers are not displayed to the subsystem operator. Maps that do not have any elements visible to the subsystem operator are not displayed at all.

- **Person location:** This menu lists the locations, where the subsystem has access. If an employee is located in another subsystem, they will be displayed under "Unknown location". For locations where the subsystem has owner rights, employees belonging to other subsystems will also be listed.
- **Surveillance:** Subsystems can view the live stream of the cameras for which they have access.
- **Publish cards:** The subsystem can provide temporary cards to its own employees or manage guests up to the quota specified in the license.
- **Data handling:** Each subsystem can set its own GDPR rules. The rules only apply to their own employees and the events that relate to them, they do not affect other subsystems. The manager rules also only handle employees assigned to the manager company.
- **Parking management:** Each subsystem can manage its own vehicles up to the quota specified in the license. Vehicle groups can also be set per subsystem.
- **Users and departments:** Each subsystem can manage its own employees and a different department structure can be set up for each subsystem.
- **Visitor settings:** Each subsystem can independently define guest types. These types will be displayed when publishing card.
- **Card list:** Only cards of employees and guests belonging to the subsystem are displayed here.
- **Access groups:** Each subsystem can independently add the access groups they wish to use.
- **Access privileges, access map:** A subsystem can only manage the permissions of its own employees on sites where it has at least "Modify" rights. The manager operator can also only see their own employees.
- **Calendar:**
    - Manage day types: day types are displayed in read-only format.
    - Company calendar: The subsystem can add a new company calendar, which can be modified freely if they want to add other day modifications or holidays to the system.
    - When managing recurring holidays, a calendar must be selected. The built-in company calendar cannot be edited here either.
    - Holiday types are managed by each subsystem itself.
    - In the users and work shifts calendars, each subsystem can see its own employees.

- **Activity codes:** In addition to the built-in codes (Arrival, Departure), each subsystem can enter individual codes, and each other's codes are not visible. The exclusion of sites from working time management can also be done for each subsystem.
- **Worktime profiles:** Each subsystem can independently set up work schedules, and each subsystem can manage their own types of overtime and allowance.
- **Worktime terminals:** The working time preferences can be managed by the firms themselves as follows:
  - The work time data to be displayed.
  - Selectable activity codes: can be entered from the subsystem's own activity codes in a sorted list.
  - Terminal managers: can be specified per subsystem. In the terminal, only users belonging to their subsystem are displayed in the user management. In addition, only own employees are listed during group logon.
- **Upload:** Among the changes to be uploaded, the subsystem will only see its own data to be uploaded, not changes related to other subsystem's employees. Every subsystem is allowed to start the upload process, but the action will send all the data to be uploaded to the controllers.

Managing several company calendars

It is possible to create multiple, independent company calendars. Day changes, holidays and recurring holidays can be managed independently in them.

The day types are common, only the manager operator can change them. For subsystems, the list is read-only. These day types are common, which may also affect access control, so door controllers and working time terminals must be assigned to a company calendar.

For Worktime Profiles, the calendar must be specified which the employees work on. This means that assigning a profile to a user also assigns a calendar to the user, together with the validity information.

For recording rules, e-mail rules, automated reports and scheduled patrols, the company calendar must be specified per rule according to which calendar the days are to be interpreted.

16 VERSION TRACKING

Short list of the features and changes in the new versions.

1.3.2.

Modifications to work time profiles handled with balance: added overtime handling and automatic periodic closing actions

New report type: Balance report

New report type: Day off report

Department history, timing of department transfers

Hour-based time off handling

Simple work time rule handling on rest days

Modifications to the configuration of data represented on attendance reports

Activity code defaults selectable for each work time profile

Weekly view on the WEB interface

Visitor and season tickets module

Password cracking protection on the system and web login page

Beep settings on readers

1.3.3.

SMTP (e-mail) setting for optional SSL certificate error handling

Optional suppression of unknown card events on selected card readers

Day delimiter (ending time of days) for shifts is more flexible

Handling of multiple allowance types at the same time

New allowance type: "Daily allowance"

Keep minimum work time balance feature

Audit log

Work time locking in the software and in the personal web

Grouped single-sheet export option for certain work time reports

New exportable columns for certain work time reports: “Time spent outside” and “Activity code count”

Attendance sheet with combined simplified and real outputs

Custom named columns on attandance sheet

File overwrite option for automated work time reports

Personal web manager calendar simplified activity registration

Work time indicators on the personal web calendars

Attendance sheets downloadable directly from personal web

Attendance data shown on personal web expanded

1.3.3.1.

Deleted card readers and terminals are selectable for arrival and leave restrictions

Changed how the fix break is deducted if the work time has exceeded the maximal daily work time: it is always deducted from the maximal work time.

On the personal work time web users not assigned to any departments are considered as if they are in the same department.

1.3.3.2.

AUX relay support for global headcount limit

Restoring the original values in the daily activites report now creates an entry for the audit log

Extra work shifts can be selected as a group in the calendar entry collisions dialog

1.3.3.3.

Operators are only able to change door profiles in any menu, if they have full access to the door profiles menu

The personal web now can show the total work time, total unaccounted time and balance change in the interval values

The attendance report now contains the time of the days off if the work time profile has hourly absence accounting

1.3.3.4.

The attendance report has new optional headers

Updated how day off limit hours calculation works to accommodate profile changes with different default day off times

1.3.3.6.

Detailed message appears on reports' accepted level instead of 00:00

Updated the way day off limit hours calculation works to accomodate profile changes with different default day-off times

1.3.3.7.

A new dialog handles balance closings for multiple profiles together. It is accessible from the Worktime Profiles tab's bottom bar.

Added attendance level columns in detailed reports and xlsx exports

It's now configurable which day off types and calendar entry types can be assigned or requested on the web

Weekly calendar and my colleagues are now paginated on web

1.3.3.8.

SMTP now works without authentication

New report column added to the violations category: Unathourized breaktime

Breaktimes are no longer handled outside of the accepted time

Balance periods can be reset from the balance report

Added an option to accept overtime not only as the profile rules dicate but as any specified overtime type

Option to import worktime data from a CSV file

Unclosed days should show a pending icon unless there is a day off entry in the calendar

1.3.3.9.

The summary report can now contain some non numeric columns

On the daily activities report, the accept worktime options have a new option: Accepting the work on a rest day, as if the worktime profile would accept it

1.3.3.12.

The workshift calendar export now has a format selector dialog

There is a new option whether to overwrite holidays when repeating entries on the work-shift tab

1.3.3.13.

Multiple custom break rules can be defined for an activity code

1.3.3.14.

Custom pass-through timeframe can be defined for tripods instead of the fixed 3 seconds

1.3.4.

Predor biometric mobile work time terminal, remote terminal mode

More detailed configuration of the work time web

Department based access for operators for the work time reports

Ability to add notes in the daily activities report

Quick work day correction in the daily activities and user's monthly activities reports

RAW arrival and leave times are editable in the monthly details and users' daily details reports

Ability to assign detected shifts in the work shift calendar

1.3.4.1

Availability of the attendance sheet on the personal web is configurable

1.3.4.2

An escorting user can be assigned to visitor users

Visitor list can be filtered by name

New button in the permanent deletion dialog: select all

Automatically detected shifts are now displayed in the User calendar too

Option to enable manual shift change request on the personal work time web

Balance report is now exportable

All shift and day off data is shown on calendar like menus for a given day, when that day is about to be edited

When batch work time exports saved with a fixed date are about to be used as automated report, an attention dialog is displayed.

Improvements of the 'manage available day off' dialog: deleted users are marked and can be hidden. Export and import now works with the users' employee number too.

Improved the audit log

Departments are now displayed in alphabet order in the work time web

1.3.4.3

Custom port support for PostgreSQL databases

Visitor list can be filtered by name

Simplified the process of anonymous visitor card publishing: the button is accessible directly from the bottom menu bar and the window showing the PIN code is only visible if there are doors in the system which allow PIN code based access

Custom day types dialog is now more verbose if an error is preventing the saving of the data

Changed some of the work time profile's default values

The e-mail for shift request acceptance or denial is more informative

Setting up the custom break rules in the work time profiles are now easier

Improved the handling of dates in the personal calendar's repeating dialog

Removed the 'fix arrival/leave' and 'fix day as...' options from the users' personal calendar and the work shifts calendar

Multiple departments are choosable in the weekly calendar on the work time web

Option to enable manual shift change request on the personal work time web

Days off limits are visible for responsible users on the work time web when assessing day off requests

Improved the handling of concurrent day off and extra shift registry

Disabled users are not allowed to use the 'Forgotten PIN' option of the personal web

Improved the error message for the personal work time web if assigning days off for multiple user failed

Added extra options for the work time web configuration: overtime and unaccounted work time icons can have a threshold under which they are not displayed

1.3.4.4

Unique e-mail addresses for users are now mandatory.

In GDPR data handling doors are selectable for movement events, so you can delete door specific events.

Added external id field to operators.

Change where the superior can lock user's month only if it is allowed in the configure worktime web.

1.3.4.5

Turning off brute force protection now releases every banned users and operators.

Assigning the same worktime profile to the same time interval as before no longer cleans up the worktime shift entries.

Break duration settings now became really convenient.

Feature where the department names has tooltip in group actions web.

Displaying user's core data in reports of future days.

Saved report filters must have a unique name.

1.3.4.6

Unified the look of system settings tabs.

More specific upload failure messages.

After setting the aux input anywhere, it automatically set Normally open.

Feature where the user can select date on my colleagues and weekly calendar web page.

Assignment menu current status messages has been unified.

Further performance improvement to Activity Codes page.

1.3.4.7

At the right side of the attendance report, the summary fields became optional. Added new checkable selector to the edit work time profile wizard report page to select the re-

quested summary fields.

On worktime web change where the shift name is not visible if there is accepted day off on the same day.

1.3.4.8

Publish card dialog no longer lists anonymous visitors.

Emailing rule Locations changed to Locations and Controllers, now the selector includes the controllers too. [CONTROLLER] variable added to variables.

Page loading and work time calculations are now canceled when navigating away in the client software, so it feels more responsive.

Added a context menu for common calendar operations to the users' monthly activities report.

Days off are no longer calculated on rest days. New column is available for work time reports which only counts days off on working days.

Users can be excluded from the time and attendance module, thus worktime reports cannot be generated for them.

Deleted users can be hidden from worktime reports using the new worktime settings dialog, available on the calendar and worktime reports pages.

Audit log can be opened in a new window.

1.3.4.9

When issuing days off in the work shift calendar, days where the specified day off type is not applicable are skipped.

The balance report will display correction cards for multiple users. The correction cards will also display if the correction comes from a balance period closing handling rule.

The Manage available days off dialog now distinguishes between active and deleted users. When exporting or importing users, they can be identified with their employee number.

Added an operation to clear raw activities on a day, hiding every activity from the user's daily activities report.

Accepted arrival and leave corrections will not appear as absent on the daily activities report and they will influence the attendance report.

1.3.4.10

The loading of the pages can now be correctly cancelled.

Requested, but not approved shifts are displayed with grey text on the work time web.

Infobutton added to Locations and controllers selector on the e-mail settings page in order to describe how the selector works.

Changed the 'departments' label to 'users' on the user's calendar page, because users are also listed there along with departments.

The calendar tabs have the option to assign batch days off.

The worktime profiles on the profiles page and on the balance report are now in alphabetic order.

The worktime cache will be automatically removed, when upgrading the software version.

The worktime profile editor will display the default allocated time of the balance periods in a tooltip.

Custom activities and arrival/leave corrections can now be requested from the work time web on rest days.

1.3.4.11

Visitor types' access privileges are editable on the access map.

1.3.4.12

A new batch export type has been added: Days off summary report.

Changed the Attendance sheet header settings options. From now all fields are optional and their names are customizable.

Worktime import errors have more meaningful messages.

Editing of parallel holidays has been expanded. From now on, multiple operators can issue long-term day off, if they edit different employee.

On the Defaults tab of the Activity codes sub menu the work time profiles are now sorted by the profiles' names.

1.3.4.13

Permanent deletion button is disabled when no user is selected.

Added navigation from the user calendar to the daily report by double clicking a day cell.

Work time import now handles both , and ; separators.

Changed where the responsible user can see other responsible users of their departments on the work time web.

The name of the reported user will show up on the day off report.

Changed Company name label to Company label because of consistency.

Hide empty row report export option will no longer insert unnecessary lines.

1.3.4.14

When replacing a controller there is an option to add the controller manually.

Notes given on the work time web or the daily activities report can be checked as a work time column.

From now on, paid breaks can have 0 minutes accepted as paid. Combining this with multiple break rules can open up new break handling options, like not paying for a break unless the working time is larger than a given amount but also not sanctioning it.

1.3.4.15

Masterlock can be activated with an AUX input.

Overtime and unaccounted web calendar indicators are now configurable from the worktime profiles.

On worktime web we saved the page state in URL and when page is reloaded then the previous state is loaded.

New columns added to detail paid and unpaid break by their respective activity code.

1.3.4.16

The controllers' AUX relay now supports the event of the depleted entry tickets for visitors.

Disaster reports now can have multiple additional e-mail addresses for notification.

Change where the shift settings have been moved to a new stage.

Added the option to schedule overtime beforehand, and profile settings to handle unscheduled, unaccounted overtimes. Scheduling options are configurable in the worktime profile, and available on the calendars and the reports.

Indicator icons for the unaccounted overtime added to the calendar report and the web. The thresholds are configurable in the worktime profile.

Added a worktime profile overview page at the end of the worktime profile editor, that summarizes the profile settings in an easy to review fashion.

From now on attendance report settings, there is an option to mark the user as "Absent".

From now the worktime shifts can be ordered.

Added 2 more optional rows to the attendance report's summary: Periodic missing worktime, periodic balance.

Created a function where the user can assign colors to the shifts, so that the appearance of the shifts in the reports is easier to distinguish

The personal web will only allow requesting or assigning day off types if the user has available limit for the given type.

Single user worktime reports has the option to hide the department tree of the user selector.

Worktime profiles have the option to account worktime by default on holidays.

Feature where the operator can clone shifts.

Change of custom activity request. From now on the users can request for current time.

Change where the pending days off also visible next to the used, unused and available on web.

1.3.5

Changed the licensing structure, please consult your license page for further information.

With random checking option, the employee have to take a breathalyser test with the selected probalitity at the entrance or the exit. If the test is positive the employee's day is alerted or it is marked unaccounted work.

You can now use Hikvision cameras for license plate recognition.

Worktime-profile overview is now exportable to pdf.

We can create unpaid day off type. These day off types have 0 hours of performed time.

You can now round overtime of balanced profile.

Performed days can be queried at reports.

Created shortcuts to certain reports from Calendar page.

Eliminated the need to save daily report to see the result of calendar changes while editing.

Requesting a custom event from the worktime web will also cause the confirmation dialog to pop up

1.3.5.1

More responsive real time feedback from the configuration of the zones.

The monitor upload function became always available.

Feature where the user can switch between tree view or without tree view in user selector on the user calendar tab.

Change where some dialog became scrollable in mobile view on worktime web.

Scheduled overtime is accepted even if it is outside of the accepted timeline.

Work on rest days, if accepted by the profile is assumed as scheduled where the profile requires scheduled overtime.

1.3.5.2

Data handling properly handles files created with recording rules.

Time profiles correctly use the implicit worktime shift assignments.

The length of access zone names can be between 1 and 100 characters.

Assigning overtime will create an audit log entry from now on.

1.4.0

When losing connection towards the server, the client will try to reconnect, instead of logging out immediately.

The worktime settings tab of the operators page has options to select the whole department tree.

The recording rule and email notification, events got separated to user related, and NOT user related categories.

The maximum port number of Hikvision LPR-s can be set to 65535.

The department based operator access has been revised on the manage available day off dialog. Access to the whole year is only necessary if the employee has been in a department in a previous year.

The built in vehicle groups now display the number of vehicles in them, on the vehicles tab.

Operators can assign the "always open" or "always closed" door profiles if they have full access to the door profiles page, even if they do not have access to remote open doors.

Masterlock configurations can now be created without a master.

In the selector components the order can be changed by dragging and dropping the selected items.

The minimum length of the names of activity codes is now only one character.

The information bar on the workshift calendar has been updated.

The daily activities report provides an option to remove the custom activities of the employee, grouped by the assigner.

The cell data on the calendar report is more readable.

The attendance report now has an option to extend the simplified attendance setting to the future.

If the terminal reports an event with a permanently deleted user, an event with an unknown user will be created.

Creating a new allowance timeline is allowed to be applied for overtimes too.

Breaks with minimal deduction now show on better fitting places when they were not used.

A new report column has been added: overtime violation.

The worktime web will display if the current worktime shift is calculated from the activities of the employee.

The worktime web can now display the overtime violations if they are selected in the configuration dialog.

From now on the responsible user can see the shift and day off request comment after it is accepted. The employee can see decision comment after the request is accepted.

From now on shift guessing considered what shift would fit best, when multiple shifts would have the same worktime in them.

From now, Ubuntu 16.04, Windows 7 and Windows 8.1 operating systems are not supported.

1.4.1

ACUs are not allowed to be deleted while uploading to any ACU.

Added the option to send a welcome e-mail for visitors and users.

Automatically enabling 'Remote open doors' when enabling 'Remote open protected doors' on the operator groups tab.

Changed the icon of the "view" icon to an eye from a pencil, reserved for "edit" operations

Changed what activity codes count as work in the activity export.

Added the ability to edit multiple events on the daily report.

From now, the users can request overtime on worktime web.

Attendance report summaries have a new paid holidays value and changed the related value calculations to handle this special case correctly.

Always accepting overtime is set as default behavior in new worktime profiles.

Balance report now handles deleted users.

Added information about the operator group handling on the batch export report.

Change where the restdays and holidays will be skipped when user assign shift on the web.

Custom events can be added from the daily reports.

Daily report has detailed assignment info now.

Off days on paid holidays are handled separately, when displayed on the attendance report summary.

Feature where the user can request or assign scheduled overtime from the predor web.

From now on, the Predor logo on the web redirects the user to the profile page.

New report column for holidays on workday. From now on there is a column for holidays on workdays and a field for the summary of holidays on workday.

New report columns for shifts. From now on there is columns for extra shift and for summary of workday shift and extra shift.

Saved balance report exports are available in automated reports dialog from now.

1.4.2

Worktime data regarding day off times are no longer available for display on the worktime terminals.

The worktime reports no longer filter out those days, when the user was not in the selected departments.

The day off summary export has an option to unite the intervals of days off.

1.4.3

Feature where more event type got infobutton about the affected access group, zone and timeprofile on monitoring table and event list table.

From now on, the users and departments page displays the limit of users.

The users tab on the worktime profiles page displays the start and end of the unassigned worktime profiles.

1.4.4

From now on there is guest type filter on the event list page.

The global anti-passback works in case of network errors.

Change where a messagebox warns if the repeated day offs exceeds the limit on the user calendar page.

Change where the dialogs won't close if there is a server error on the worktime web.

Furthermore from now cannot request/assign day off which interval includes more than one worktime profile.

Replacing a device will inherit the worktime settings of the old device.

We do not have the option to delete a report with automated report associated with it in saved reports dialog.

1.4.5

The activity export from the event list can calculate active time.

Change where the guest type filter on the events list page contains deleted guest types.

1.4.6

When saving a batch export there is a more exact error message if there are colliding report names.

1.4.7

Now you can generate a QR code for guests and send it via email, so they can use it to enter doors with appropriate readers.

From now on an indication spinner shows up on the attendace main menu button, when automated reporting is running in the background. More information is availabe from the Email log page at any time.

The worktime cache settings dialogue has a more user friendly layout.

1.4.8

Changed the selection mode from single selection to extended selection in several pages and adjusted the functionality according to the new selection.

From now, the biometric terminals can take a photo and save GPS location for activity entry event.

1.4.9

New functions are available in Phantom (random checking and "allow if assigned to work" in access control timeprofiles).

Predor D4 controllers can be replaced by Phantom controllers and Phantom is available as a controller type when the serial is provided later.

The Person location tab now shows a tooltip when hovering on the little head icon near the user's name in the table.

Added a dialog where visitor companies can be managed at Users/Visitor settings/Manage companies.

1.4.10

From now the controllers will not send IP broadcast messages in case of a fire alert in new Predor systems by default. This setting can be changed in Disaster recovery submenu.

Changes where there is a new status (skipped) for the result of e-mail log and the E-mail log page is relocated under the Attendance menu.

1.4.11

From now on, there is a card login option on the web.

1.4.12

The users daily activities export no longer has the user column twice.

1.4.13

Updated firmware versions.

1.4.14

Vehicle entry management is now available with Predor Phantom controller.

Change where the late arrival and early leave is a violation if it exceed the tolerance time by 1 second.

Created a new option in the worktime profile editor for automatic shift request approval.

Restored "Yesterday" and "Today" options on the Nexon export time selection.

1.4.16

The worktime settings dialog name has changed to worktime exclusions.

1.4.17

Change where the delete and clone tool button moved into additional buttons.

The activities export on the event list page has received some formal adjustments.

From now the biometric work time terminal accepts SIM card. (PIN must be disabled)

From now there is an option to limit the days off requested in a continous interval.

Change on worktime web where the current activity description changed to Pointwise activity.

1.5.0

Subsystems are now available - handle parts of your system as separate Predor system for companies or tenants. For more information, inquire from your installer.

Multiple company calendars are now available. Use different day settings for different controllers and worktime profiles.

1.5.3

Venue admission module is now available for purchase. For more information, please refer to your installer.

Changed the validation rules on the operator email input, because it rejected TLDs longer than 3 characters.

The controller settings dialog is larger now.

We have changed the way the worktime terminal works as follows: if the employee identifies themself and we do not receive a response from the server within a short time about the worktime data to be displayed, we will display the activity code selection page without it, and if the data is received later, it will be displayed.

1.5.5

The certificate management module is available from now to manage employees' certificates and licenses. It is also possible to restrict their access rights according to the certificates expiration. For more information, contact your installer.

E-mail notification can be sent about expiring certificates.

Added the option to override more columns on the attendance report.

The Search page is now available in the Subsystems submenu, where you can search for all users, even by card.

1.5.7

Change, if a vehicle is in a vehicle group and a user is also added then at access we check both access privileges.

Guest vehicles can be added to vehicle groups.

New access mode for vehicle access. Mixed access mode includes license plate only and user and license plate access mode and automatically applies the correct one.

Change, the weekly calender table has a 100 rows option on the web.

Added a message window after the certificate change, if the certificate type is not active.

Exceptions are available for certificate based access control.

Door profile assignment is available from doors tab with a double click.

From now on, the excel export of the evacuation list will contain the sum of peple inside, and sum of people potentially inside.

In the worktime terminals menu, you can now choose to skip the confirmation after selecting activity code.

You can add a vehicle directly to the user.

Reverse reading of the hikvision camera is also processed.

The pictures of hikvision camera can be optionally saved.

WiFi Enterprise EAP-PEAP MSCHAPv2 authentication is now available on biometric terminals.

With subsystems module, SMTP settings only available for the manager operators.

Subsystems are distinguishable on the upload page.

1.5.8

New office terminal support.

Support for the new biometric terminal.

1.5.9

Removed the tip boxes from the pages. Their information is available under the Help page and in the user manual.

Login is no longer necessary to install Predor Lite and Predor Server.

Added the option to worktime terminals to use server connection to open doors, after a card read on the terminal. (When using Phantom controllers)

Change on the web, if the overtime interval is inverted, an error message will pop up.

1.5.10

Feature, from now on, the LPR can handle the Dahua cameras too.

With Dahua license plate recognizer, you can set how long the number plate is accepted.

Feature, PIN code can be used alone to enter on doors which have readers with keypad.

New feature to generate QR codes for users.

New day off report column which shows the remaining day off count on that day.

On biometric and office worktime terminals, duplicated WiFi names are filtered out when connecting.

For office terminal, LED feedback is given for invalid or unknown cards.

For office terminals, we have increased the speed of NFC card reading.

The worktime terminal only uploads 3 images at a time instead of 5 to reduce the packet size.

1.5.11

New event for dahua camera if for some reason the entrance cannot be opened

Client will show the version of the server and provide a downloader link for the right version client.

A new feature has been added to Predor Web, allowing users to log in with a password instead of a PIN code. In the web settings, under special login settings, it is possible to specify whether employees can log in using a password or a PIN code. By default, users' passwords are set to their previously used PIN codes, which they can change on the web or in the user edit dialog. In case of a forgotten password, it is possible to request a password reset on the web.

A new feature has been added to the software that allows passwords to be generated for users based on a predefined schema during user creation. The user can log in to Predor Web with the generated password. The welcome email sent to the user initially contains the generated password, but if it is sent again, it will only include the password reset URL. The automatically generated password schema can be specified in the system settings. Macros found in the user password schema settings can be used for this. The default value for a new system is the PIN code generated for the user in the system. The administrator can change the users' password through the user editor dialog, but the password cannot be viewed.

1.5.11.1

Added corrected arrival and leave columns to worktime reports.

1.5.12.2

Change: From now on, when a middle manager assigns a worktime entry, a request is created for the subordinate.

Change: From now on, a pending worktime entry does not hide the absence icon on the web manager calendar page.

1.5.12.3

From now on, certificate import and assignment is only available for operators with full write access.

17 APPENDIX A: PREDOR SYSTEM UPDATE GUIDE

Predor Lite system update



WARNING: If your system uses plugins, you can only update them by logging in as an installer! Ask your installer for help to update! If you are not sure whether your system uses plugins, check under the software's Help/About menu!

If a newer software version is available, Predor Lite will display a notification in the **Monitor** main menu **Dashboard** submenu **Notifications** window:

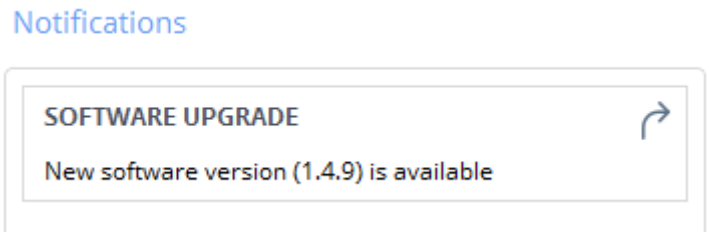


Figure 198: Software upgrade notification

Backing up the database

Before upgrading the software, it is recommended to make a backup of the database by following the steps detailed below:



WARNING: If you don't make a backup of the database, you will not be able to revert to an older version of the software after the upgrade!

- You need to locate the database file on your computer. The easiest way is to navigate to the **Database** submenu of the **Settings** menu, where the file name and path are displayed:

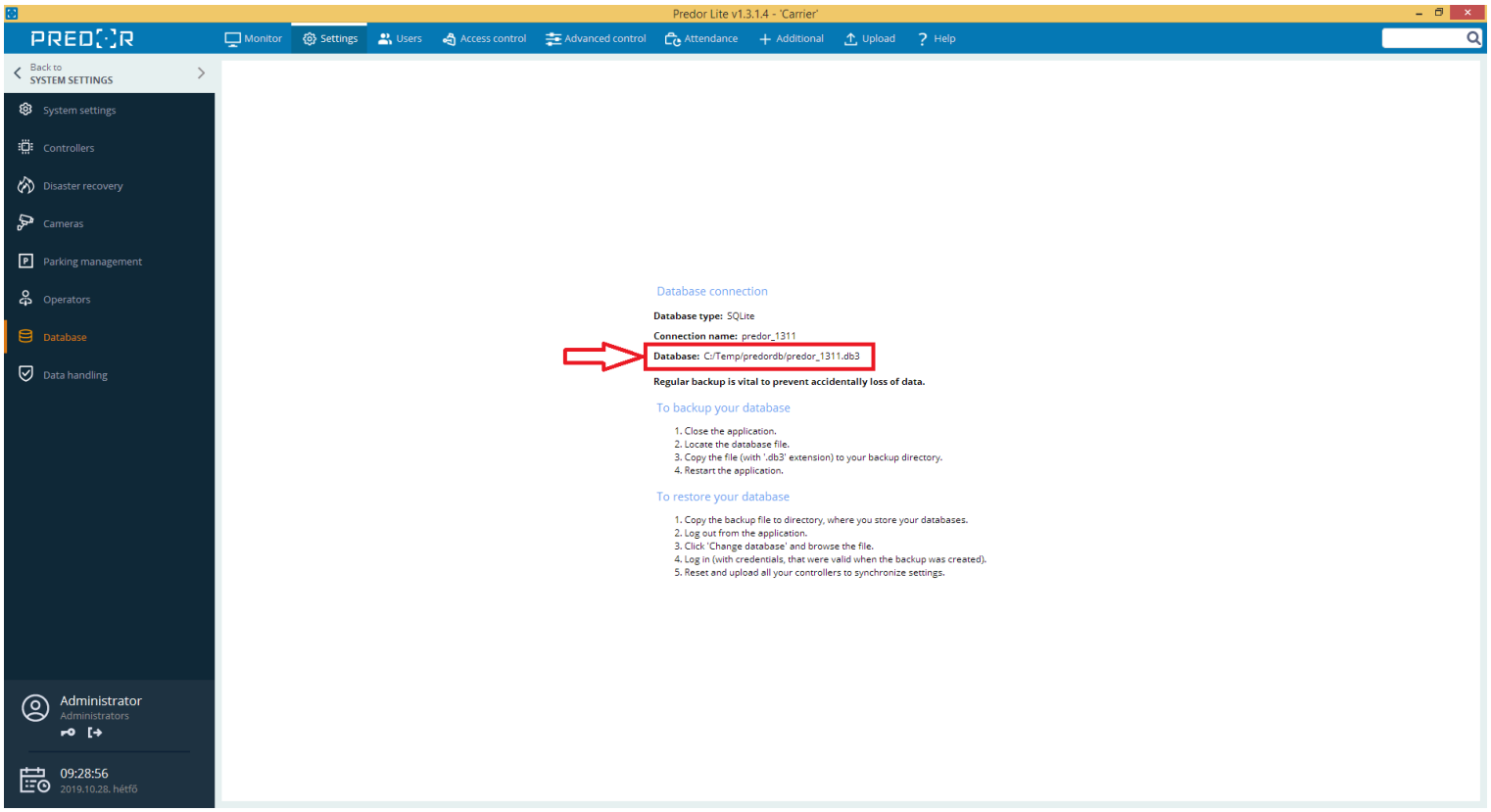


Figure 199: Determine database file location in Predor Lite software

- Navigate to the folder containing the database file.
- Close Predor Lite software!
- Copy the database file (.db3 extension) to a backup folder.

The software update can be done with a special utility called *maintenancetool*. The *maintenancetool* is installed on the computer together with the Predor Lite software and is located in the installation root directory.

Running maintenancetool on Windows operating system

On Windows, the recommended way to run *maintenancetool* is through Windows' own Programs and Features menu. Here you should look for the *Predor Lite for Windows* software and then select the modification from the local menu (or start it with double-clicking on it):

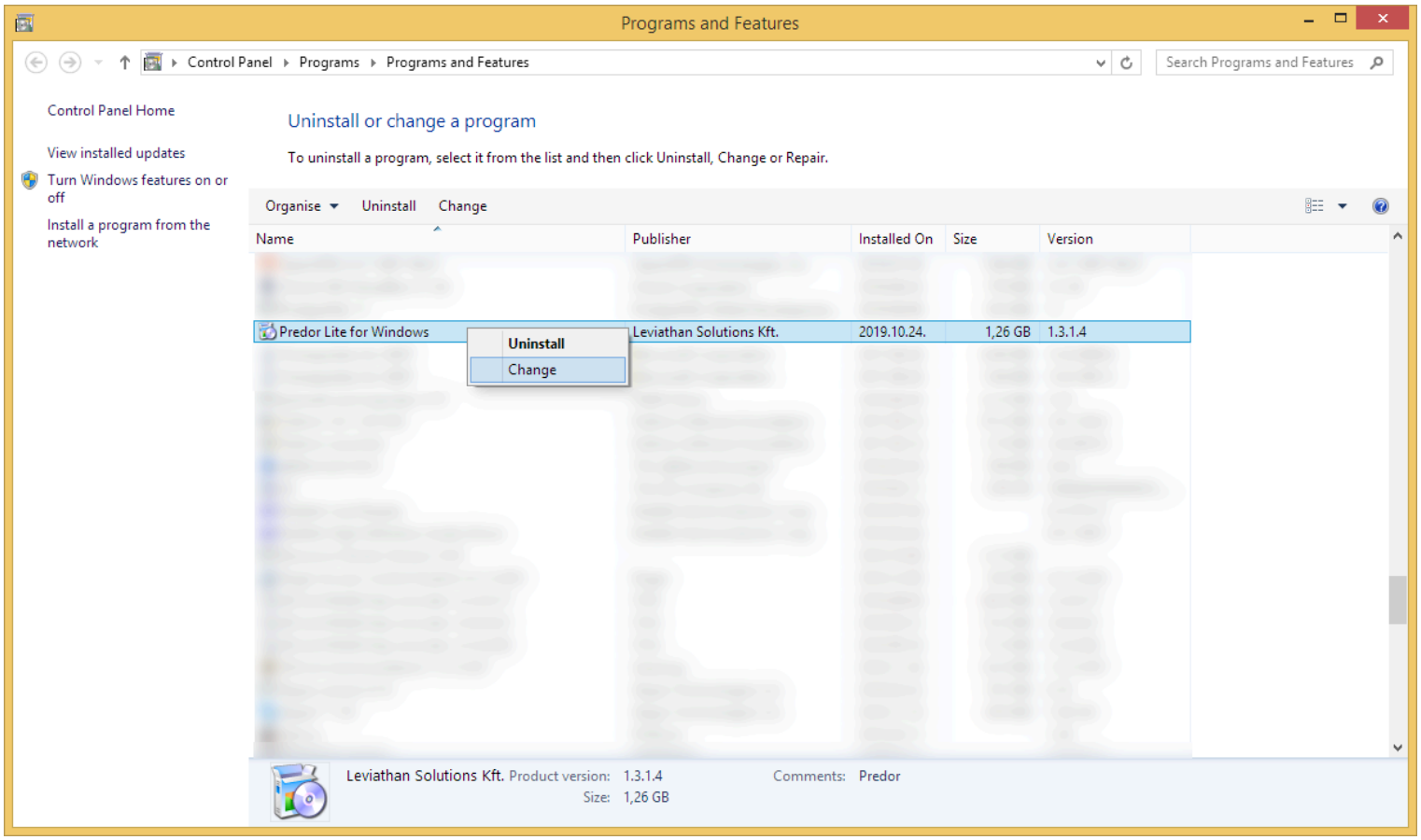


Figure 200: Update Predor using the Windows Programs and Features menu

In the window that appears, select the Update components option:

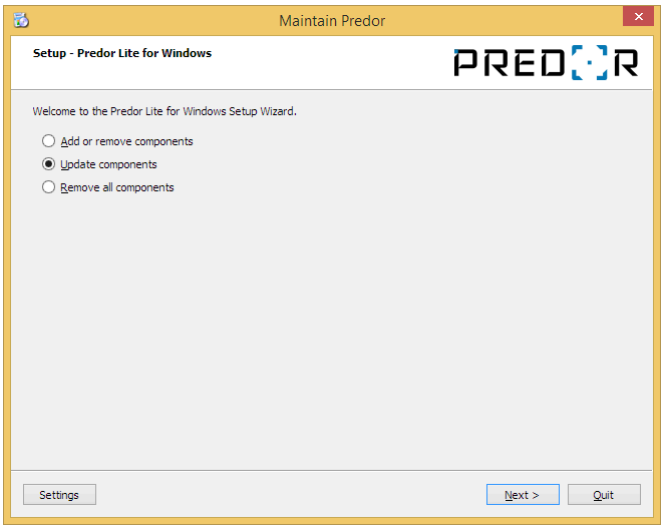


Figure 201: Predor Lite update Step 1

In the next window, you will see a list of software components that can be updated, and their old and new version numbers. Predor Lite is selected by default, so all you need to

do is click on the *"Next"* button.

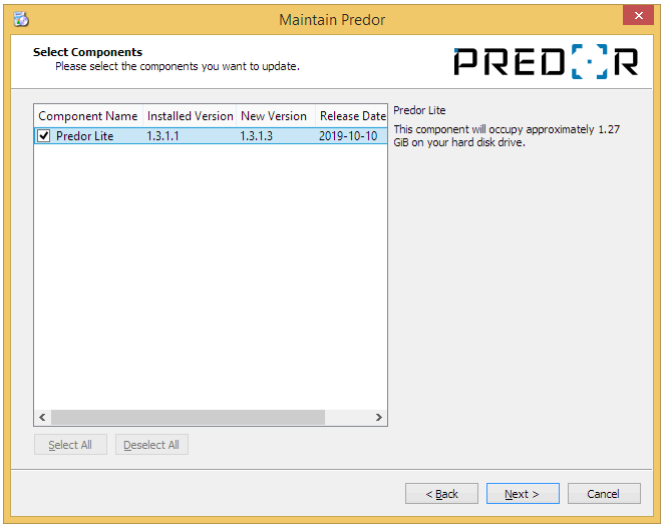


Figure 202: Predor Lite update Step 2

The next window will display the disk space required for the update, if you are sure that you have at least that much free space on your computer, click on *"Update"*:

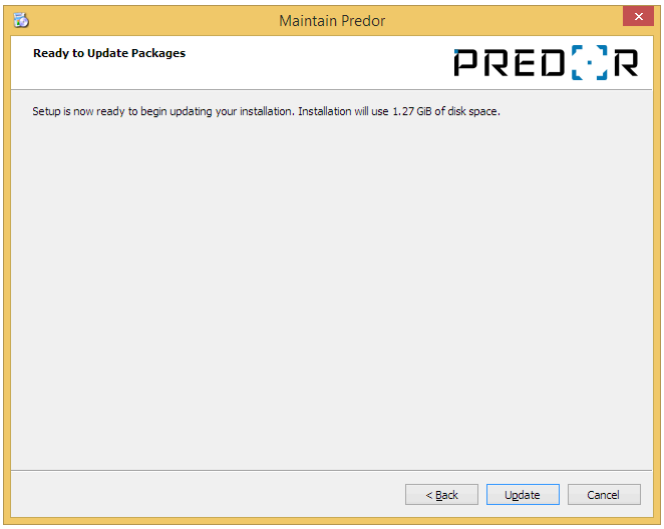


Figure 203: Predor Lite update Step 3

The maintenancetool will download and install the software update, this may take several minutes depending on your internet speed. Please be patient until the process is complete and do not attempt to launch the Predor Lite software:

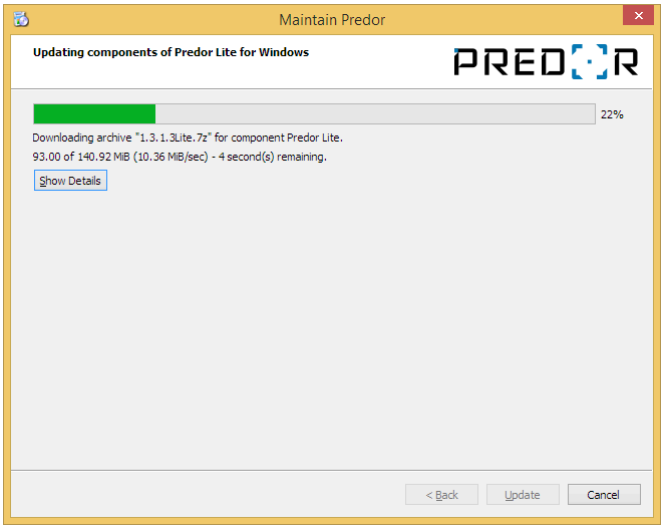


Figure 204: Predor Lite update Step 4

The following window will inform you when the update has been successfully completed. To exit the update software, click on the *"Finish"* button!

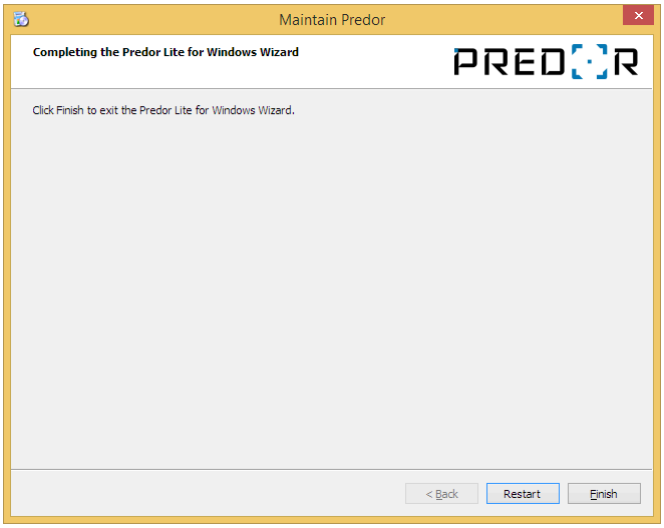


Figure 205: Predor Lite update Step 5

The software update may sometimes include firmware updates for controllers and terminals, so after logging in, the firmware of the devices associated with the system may also need to be updated. The procedure for this is explained in the Firmware update of devices section.

Running maintenancetool on Linux operating system

On Linux, the *maintenancetool* is launched from the terminal and requires root privileges, so if you don't have this, you will need to ask your administrator for help. First go to the installation folder (default: */opt/PredorLite*):

```
cd /opt/PredorLite
```

then start *maintenancetool* with root privileges:

```
sudo ./maintenancetool
```

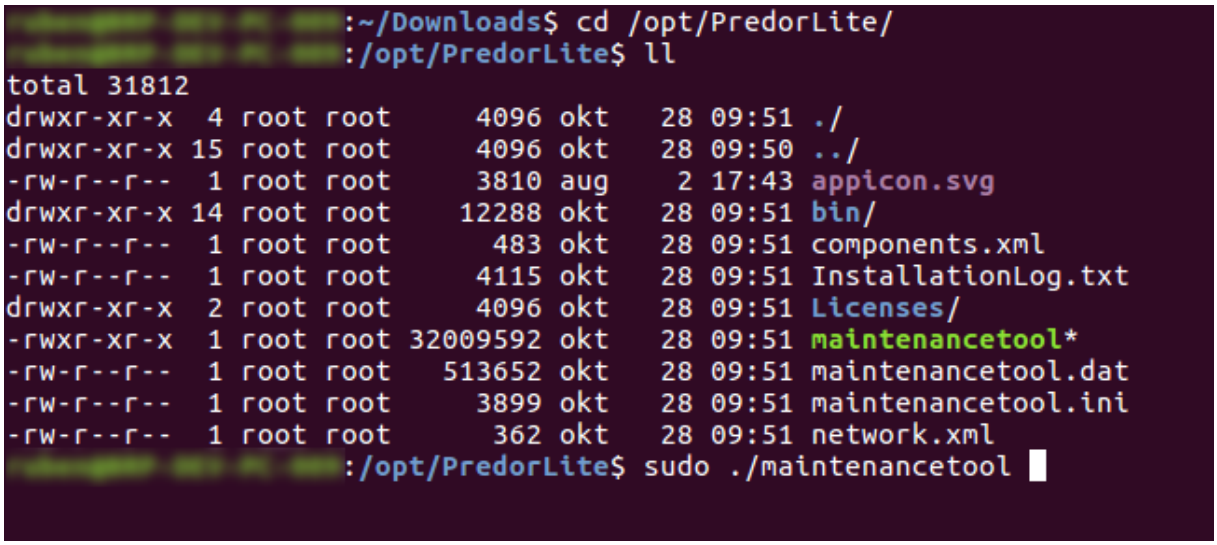


Figure 206: Launching maintenancetool on linux operating system

In the window that appears, select the Update components option:

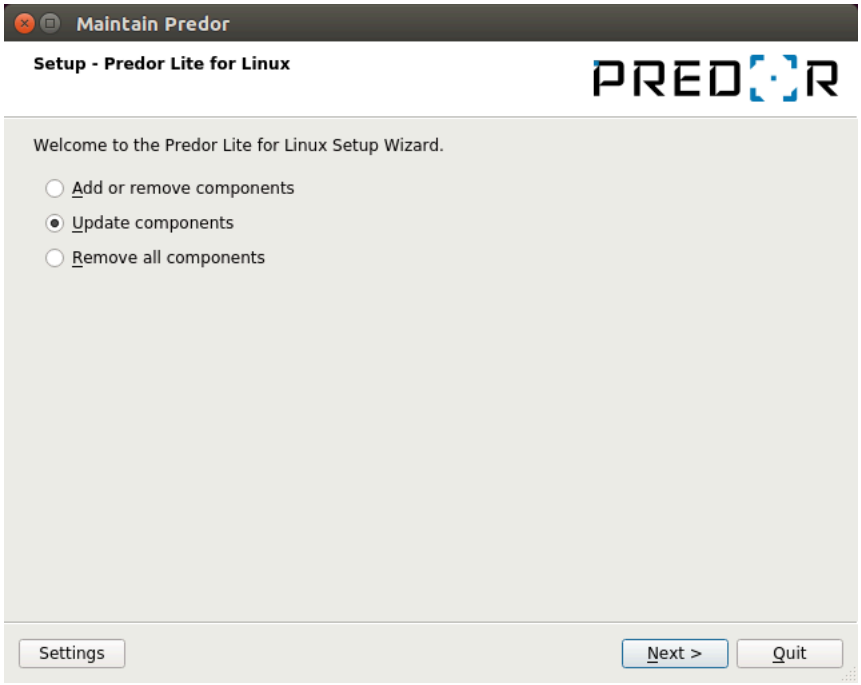


Figure 207: Predor Lite update Step 1

In the next window, you will see a list of software components that can be updated, and their old and new version numbers. Predor Lite is selected by default, so all you need to do is click on the *"Next"* button.

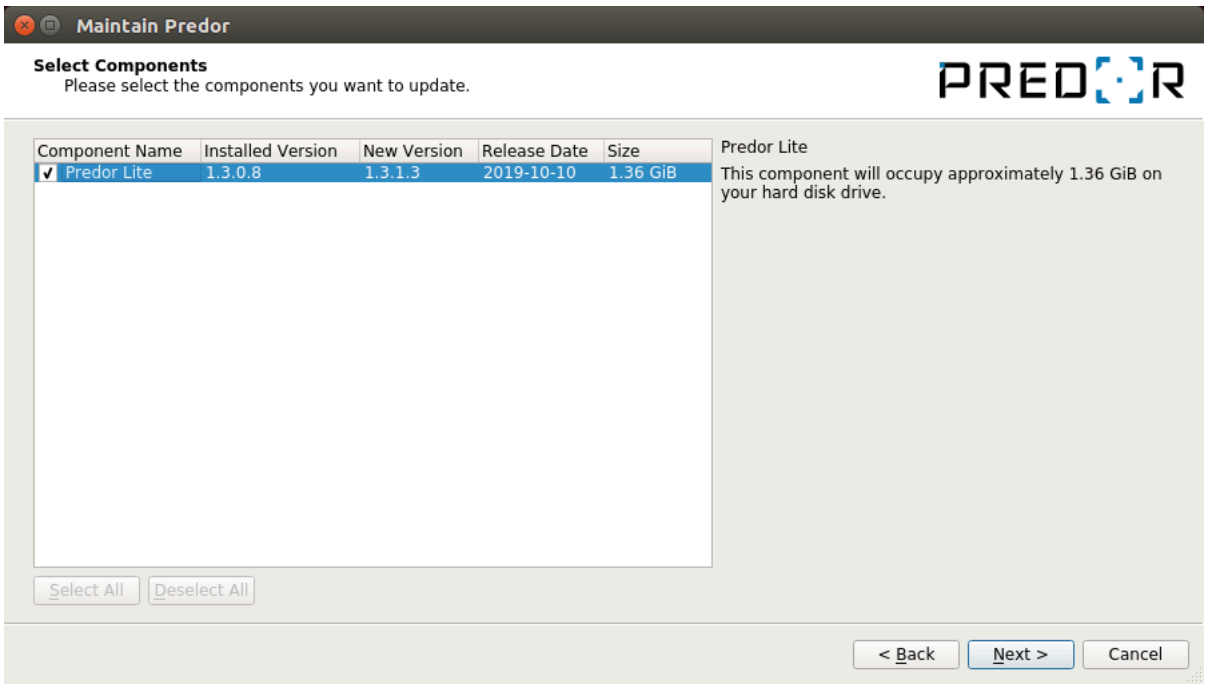


Figure 208: Predor Lite update Step 2

The next window will display the disk space required for the update, if you are sure that

you have at least that much free space on your computer, click on *"Update"*:

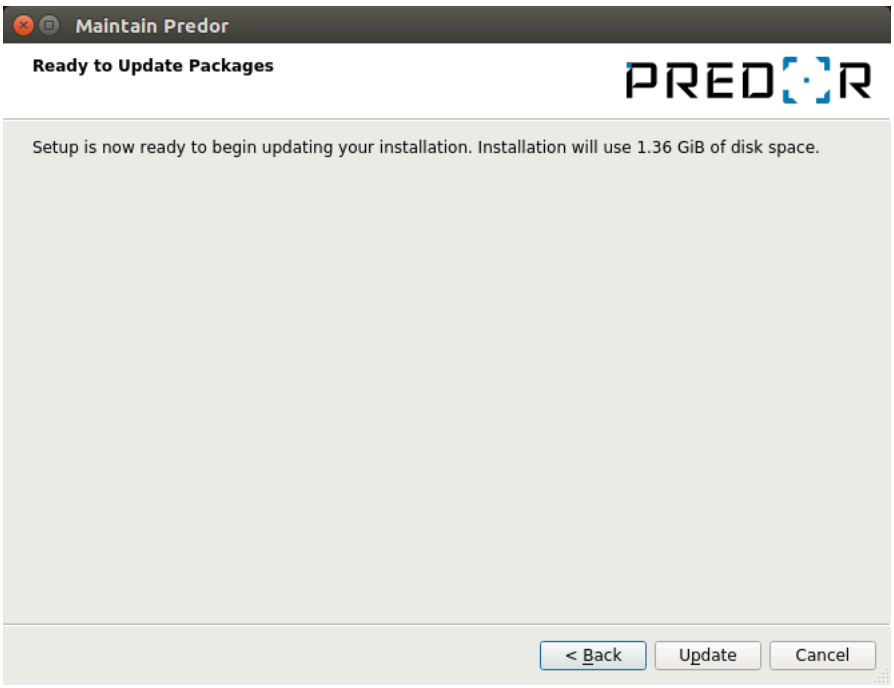


Figure 209: Predor Lite update Step 3

The maintenancetool will download and install the software update, this may take several minutes depending on your internet speed. Please be patient until the process is complete and do not attempt to launch the Predor Lite software:

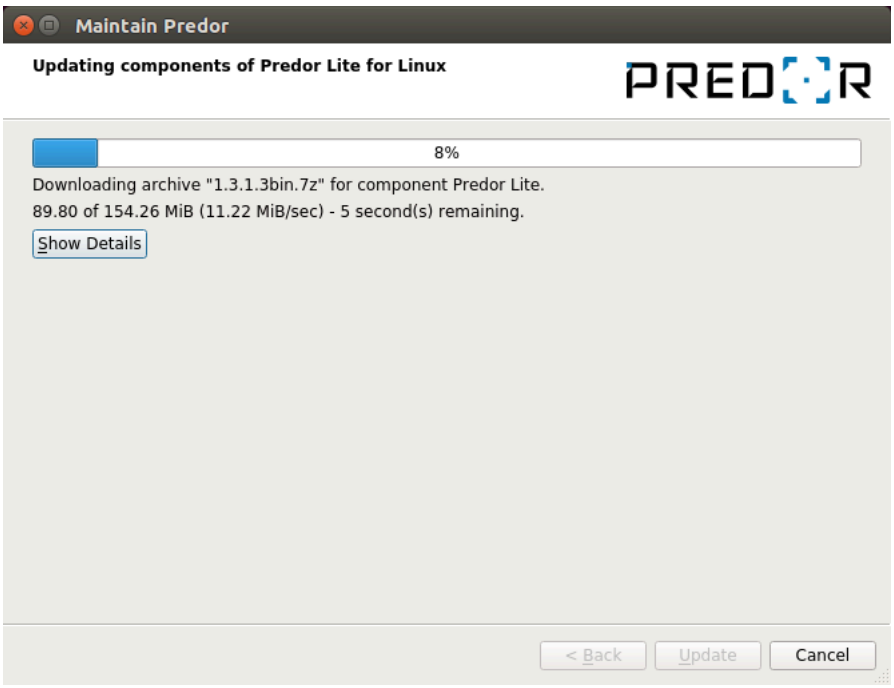


Figure 210: Predor Lite update Step 4

The following window will inform you when the update has been successfully completed. To exit the update software, click on the *"Finish"* button!

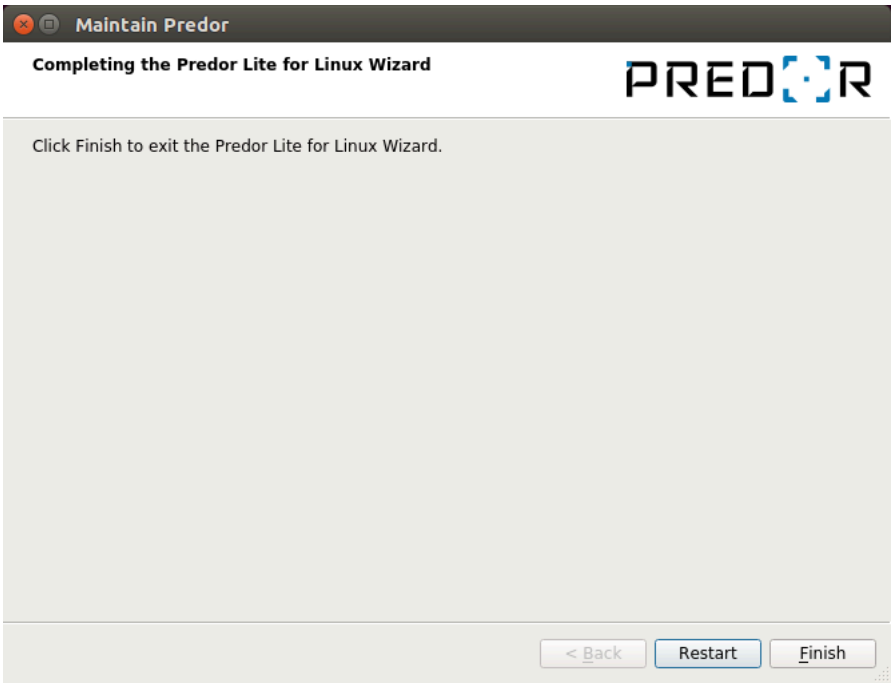


Figure 211: Predor Lite update Step 5

The software update may sometimes include firmware updates for controllers and terminals, so after logging in, the firmware of the devices associated with the system may also need to be updated. The procedure for this is explained in the Firmware update of devices section.

Predor Enterprise



WARNING: If your system uses plugins, you can only update them by logging in as an installer! Ask your installer for help to update! If you are not sure whether your system uses plugins, check under the software's Help/About menu!

If a newer software version is available, Predor Enterprise will display a notification in the **Monitor** main menu **Dashboard** submenu **Notifications** window:

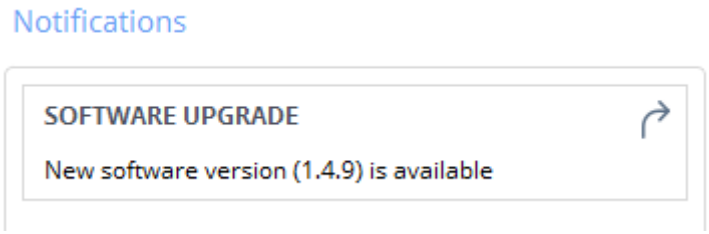


Figure 212: Software upgrade notification



WARNING: When updating, both the server and the clients must be updated, because only the same version of the server and clients will work together properly.

Backing up the database

It is recommended to backup the database and the server configuration file (*predor_server.ini*) before updating the server. The server configuration file:

- on **Linux** is located in the `/etc/predor/` folder.
- on **Windows** is located in the installation folder, next to the server executable. In the Predor Server service properties window, you can view the location of the installation folder:

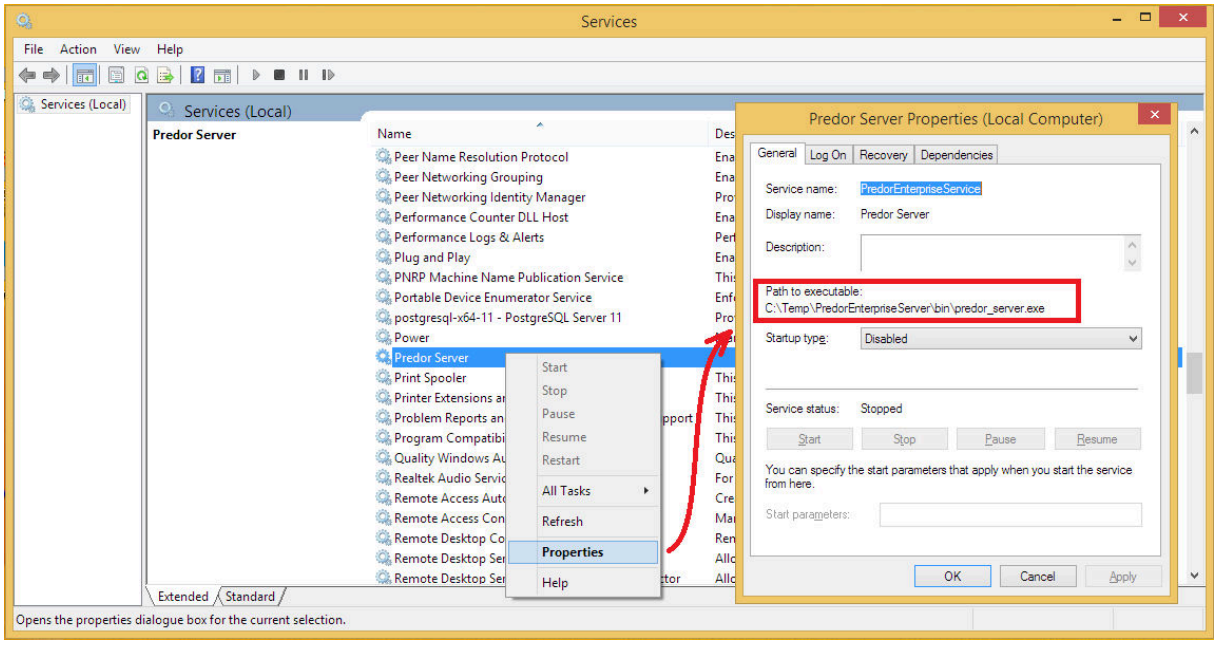


Figure 213: Predor Server installation folder identification using the services menu

Copy the configuration file (*predor_server.ini*) to the backup folder. Depending on the database engine, you can make a backup of the database by following the steps detailed below:



WARNING: If you don't make a backup of the database, you won't be able to revert to an older version of the software after the upgrade!

PostgreSQL database backup

Making a backup using a terminal/command line

If you are using Windows operating system, you need to locate the *pg_dump.exe* file inside the PostgreSQL installation folder. (Default installation folder: *C:\Program Files\PostgreSQL\11\bin*) Open a command line window here (right-click in the window while holding down the SHIFT key and select "Open command window here" option).

In the terminal or command line, type:

```
pg_dump -Fc -h hostaddress -p 5432 -U username -d dbname > backup.dump
```

where **hostaddress** = postgreSQL server address (localhost or IP address), **username** = postgre user name, **dbname** = postgre database name, **backup.dump** is the name of the backup file. For example:

```
pg_dump -Fc -h 192.168.0.23 -p 5432 -U pgpredor -d predordb > prdb_191201.dump
```

Making a backup using pgAdmin

After logging into the PgAdmin interface, right-click on the database and select *Backup...*:

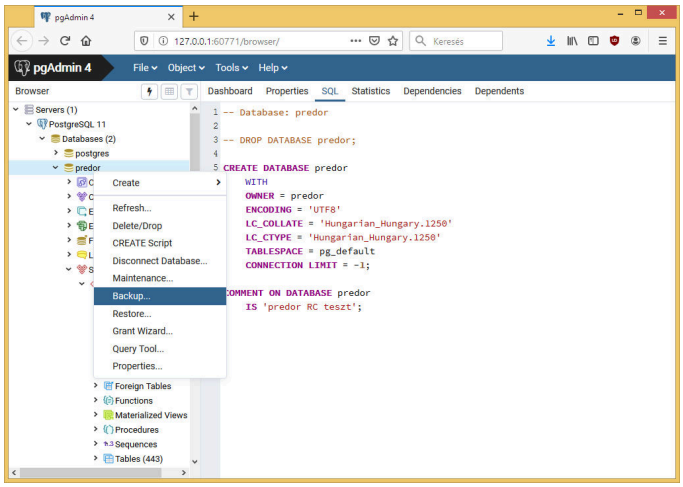


Figure 214: Backup PostgreSQL database in pgAdmin interface Step 1

In the window that appears, enter the name and path of the file you want to save in the *Filename* field. The *Format* field should be set to *Custom* and then press the *Backup* button:

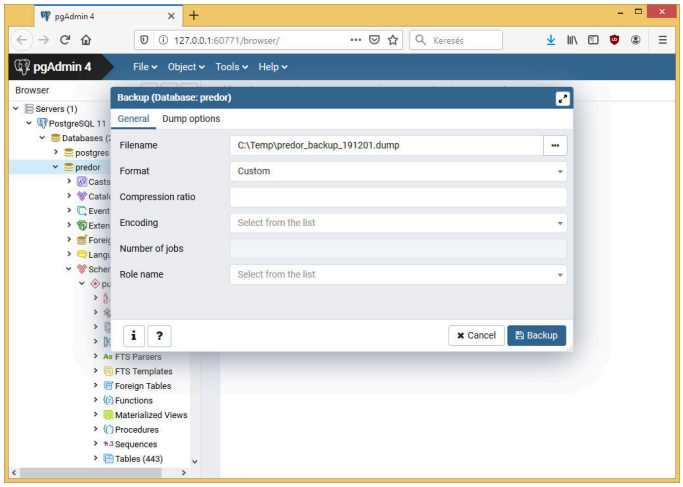


Figure 215: Backup PostgreSQL database in pgAdmin interface Step 2

A notification will appear in the bottom right corner to inform you of the status of the process. The window below will inform you when the process is finished:

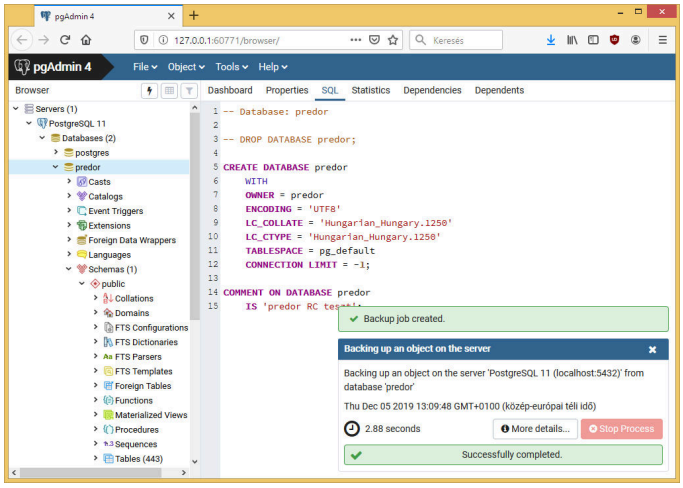


Figure 216: Backup PostgreSQL database in pgAdmin interface Step 3

SQLite database backup

- You need to locate the database file on your computer. The easiest way is to navigate to the **Database** submenu of the **Settings** menu, where the file name and path are displayed:

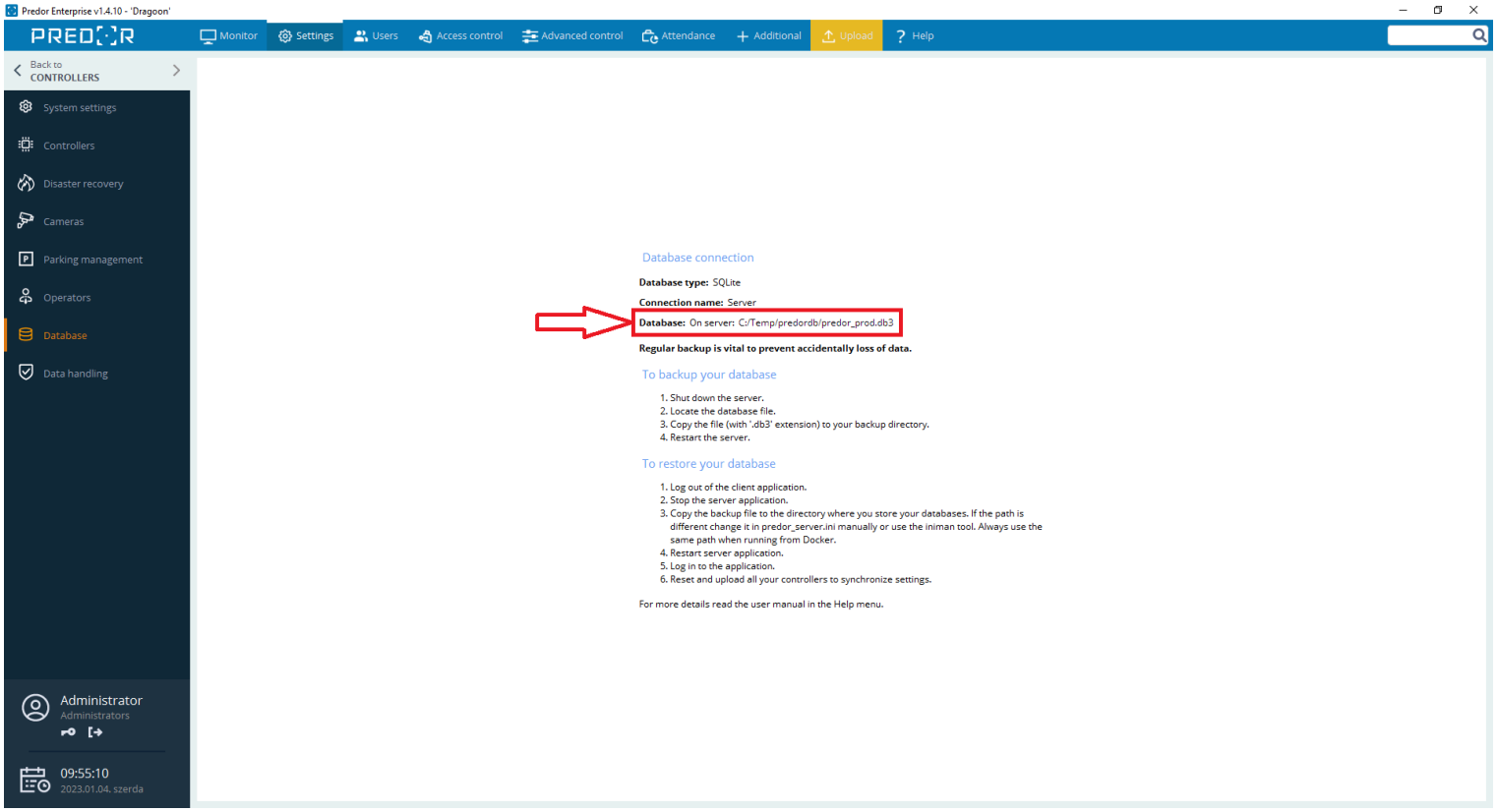


Figure 217: Database file location in Predor Enterprise software

- On the server, navigate to the folder containing the database file.
- Stop the Predor Server service!
  - on **Linux** in the terminal, run the following command:

```
sudo systemctl stop predor
```

  - on **Windows** in the local services menu (pressing the Windows+R key at the same time will bring up the run command line, where you should type *services.msc*), locate the Predor Server service and select the Stop option in the top left corner:

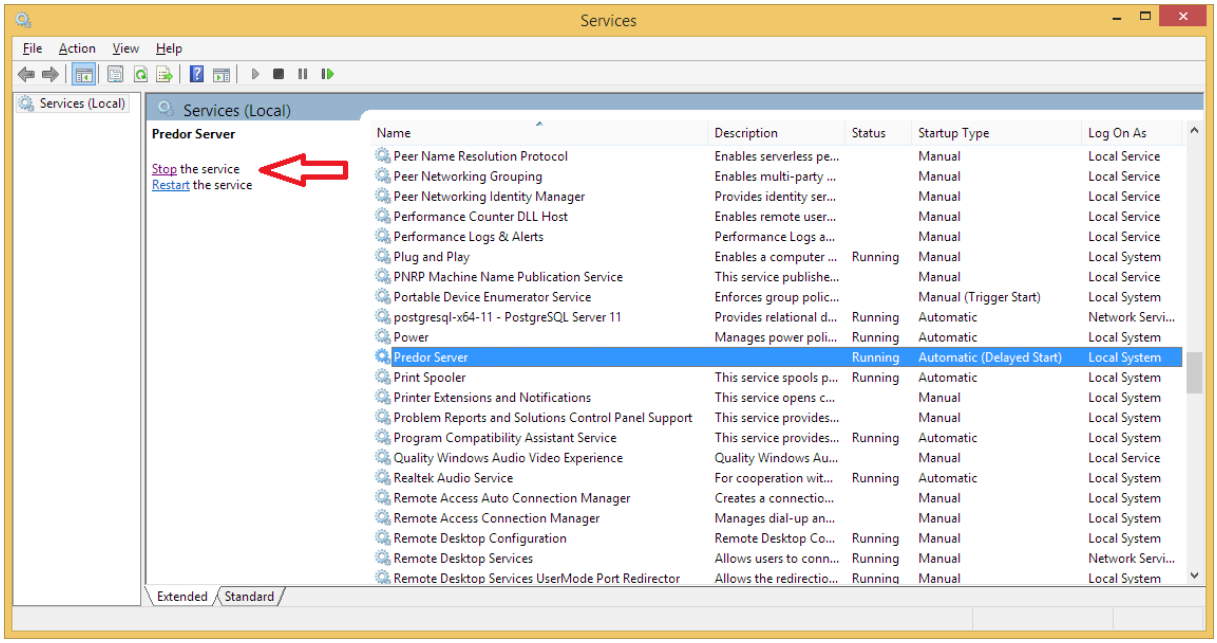


Figure 218: Stopping Predor Server service on Windows

- Copy the database file (.db3 extension) to a backup folder.

Predor Server

The software update can be done with a special utility called *maintenancetool*. The *maintenancetool* is installed on the computer together with the Predor Server software and is located in the installation root directory.

Running maintenancetool on Windows operating system

On Windows, the recommended way to run *maintenancetool* is through Windows' own Programs and Features menu. Here you should look for the *Predor Enterprise server for Windows* software and then select the modification from the local menu (or start it with double-clicking on it):

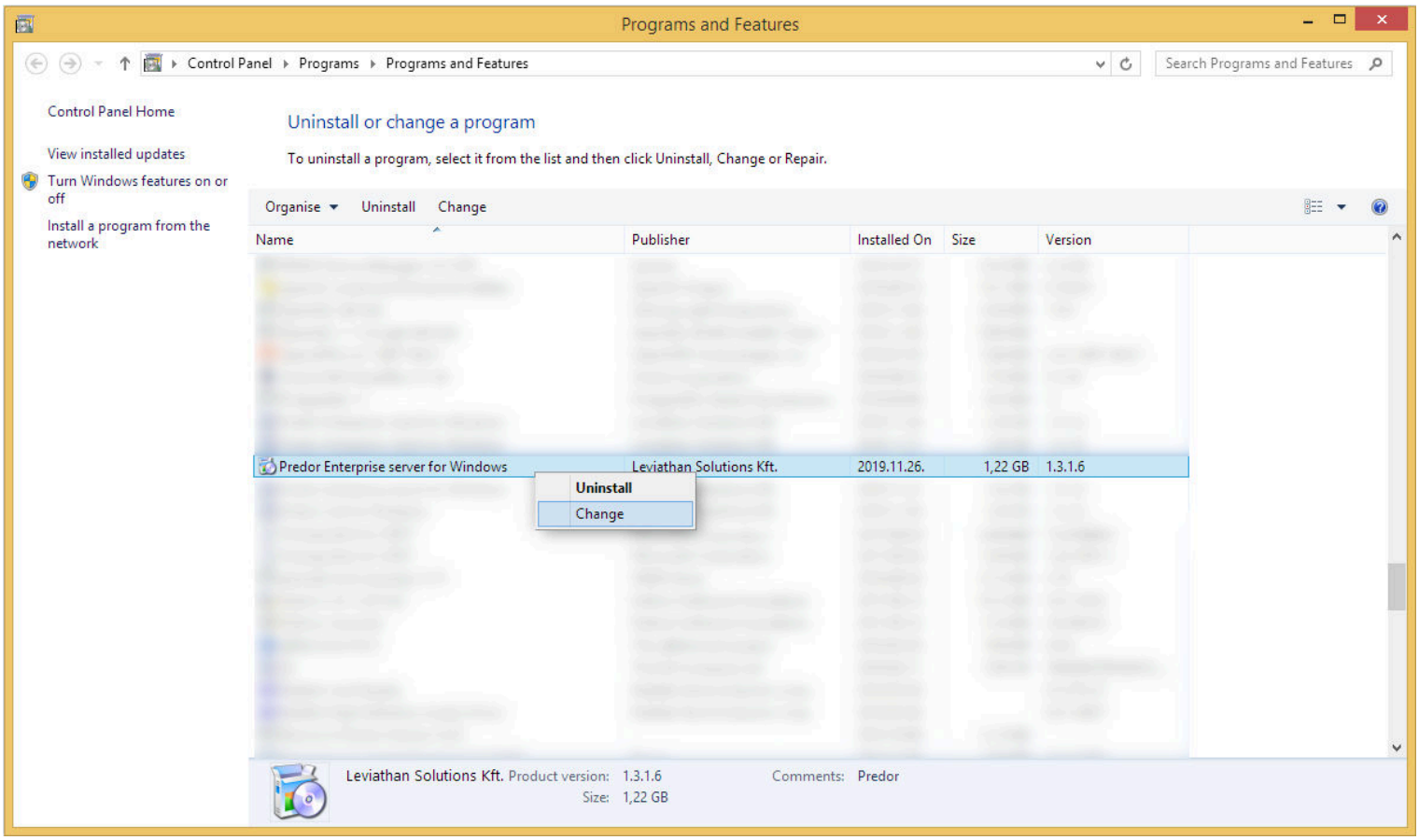


Figure 219: Update Predor Server using the Windows Programs and Features menu

In the window that appears, select the Update components option:

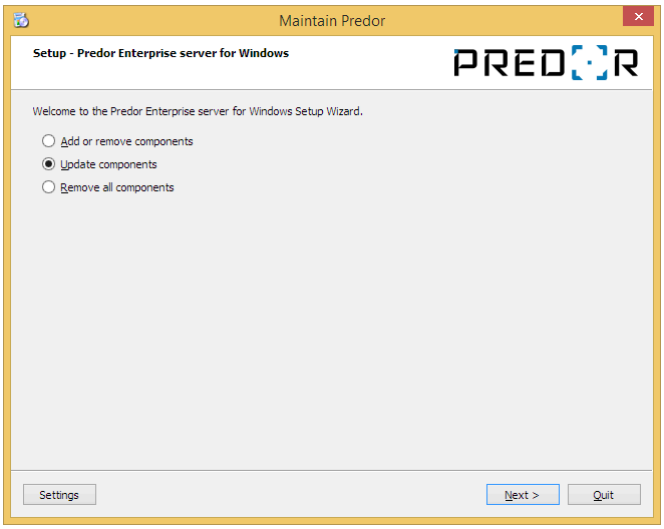


Figure 220: Predor Server update Step 1

In the next window, you will see a list of software components that can be updated, and their old and new version numbers. Predor Server is selected by default, so all you need

to do is click on the *"Next"* button.

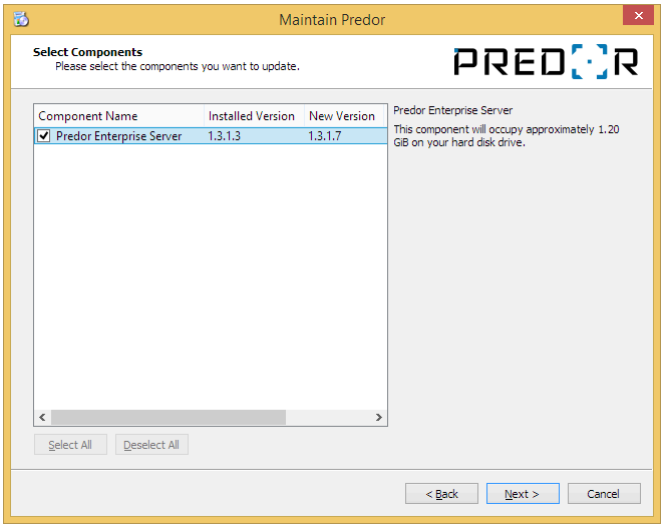


Figure 221: Predor Server update Step 2

The next window will display the disk space required for the update, if you are sure that you have at least that much free space on your computer, click on *"Update"*:

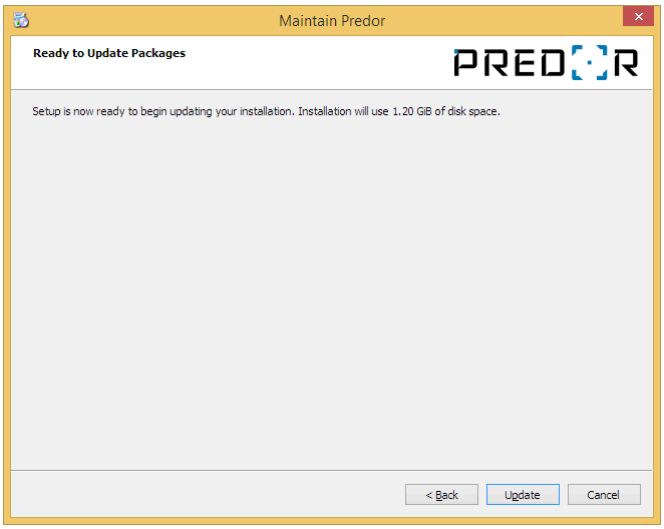


Figure 222: Predor Server update Step 3

The maintenancetool will download and install the software update, this may take several minutes depending on your internet speed. Please be patient until the process is complete and do not attempt to launch the Predor Server software:

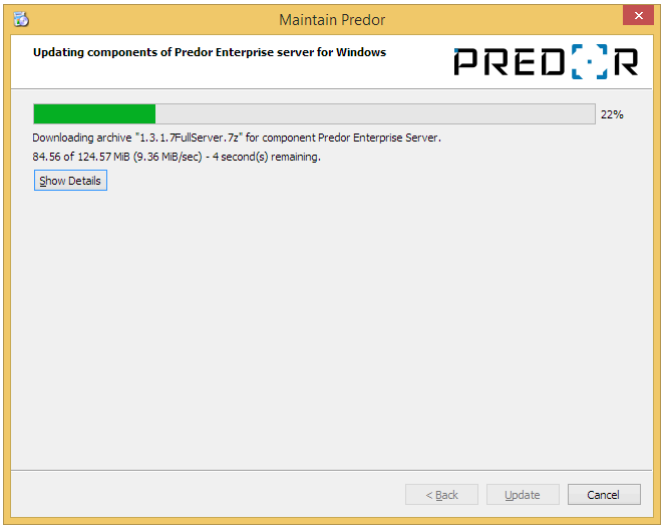


Figure 223: Predor Server update Step 4

The following window will inform you when the update has been successfully completed. To exit the update software, click on the *"Finish"* button!

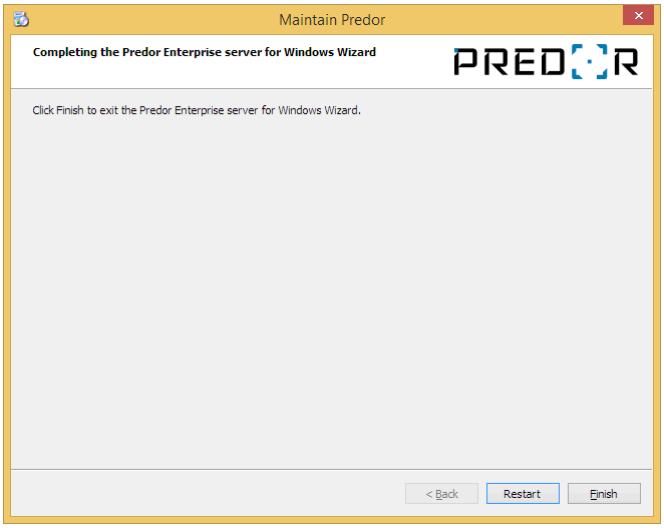


Figure 224: Predor Server update Step 5

After the update, the service will not start automatically, you will have to restart it manually for the first time in the Windows local services menu.

Running maintenancetool on Linux operating system

On Linux, the *maintenancetool* is launched from the terminal and requires root privileges, so if you don't have this, you will need to ask your administrator for help. First go to the installation folder (default: */opt/PredorEnterpriseServer*):

```
cd /opt/PredorEnterpriseServer
```

then start *maintenancetool* with root privileges:

```
sudo ./maintenancetool
```

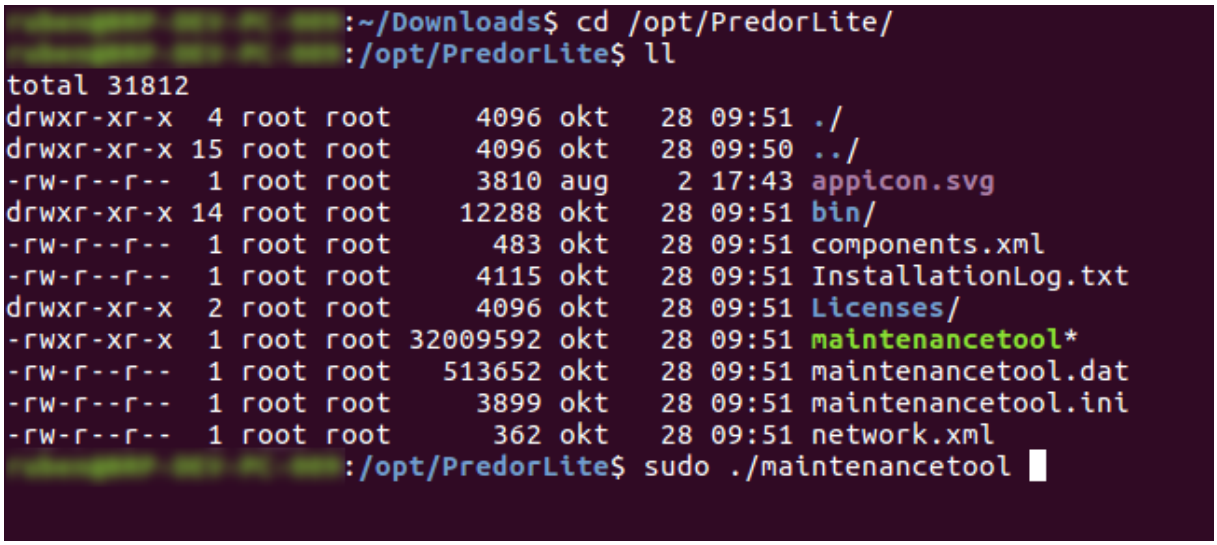


Figure 225: Launching maintenancetool on linux operating system

In the window that appears, select the Update components option:

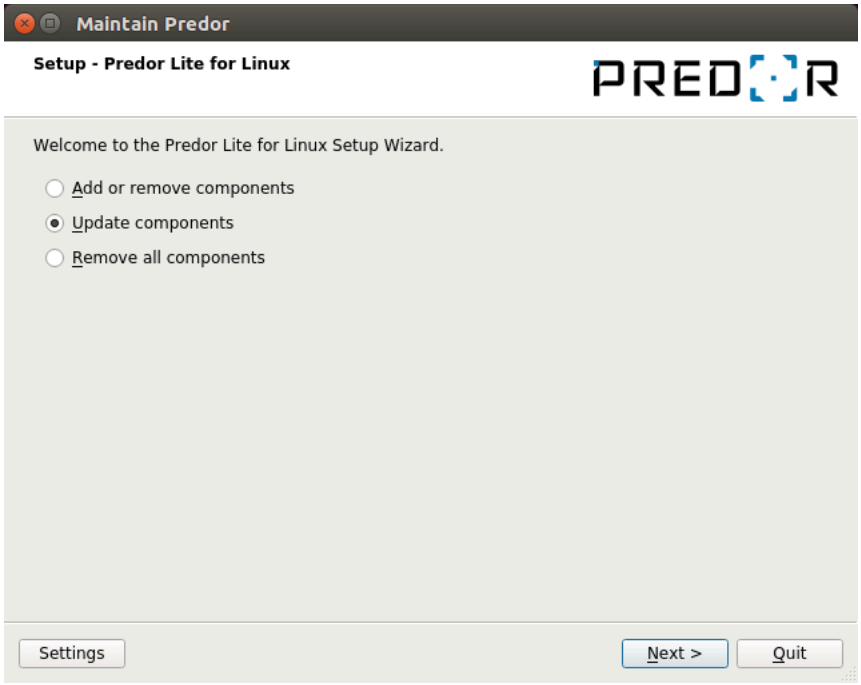


Figure 226: Predor Server update Step 1

In the next window, you will see a list of software components that can be updated, and their old and new version numbers. Predor Server is selected by default, so all you need to do is click on the *"Next"* button.

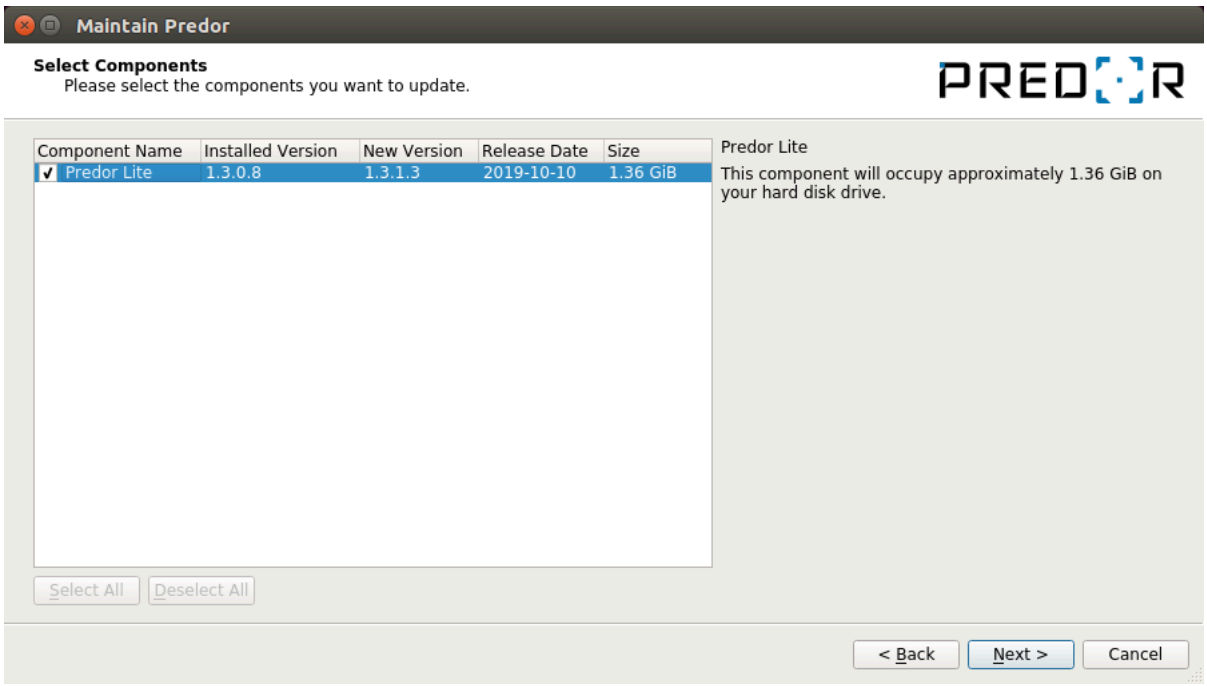


Figure 227: Predor Server update Step 2

The next window will display the disk space required for the update, if you are sure that

you have at least that much free space on your computer, click on *"Update"*:

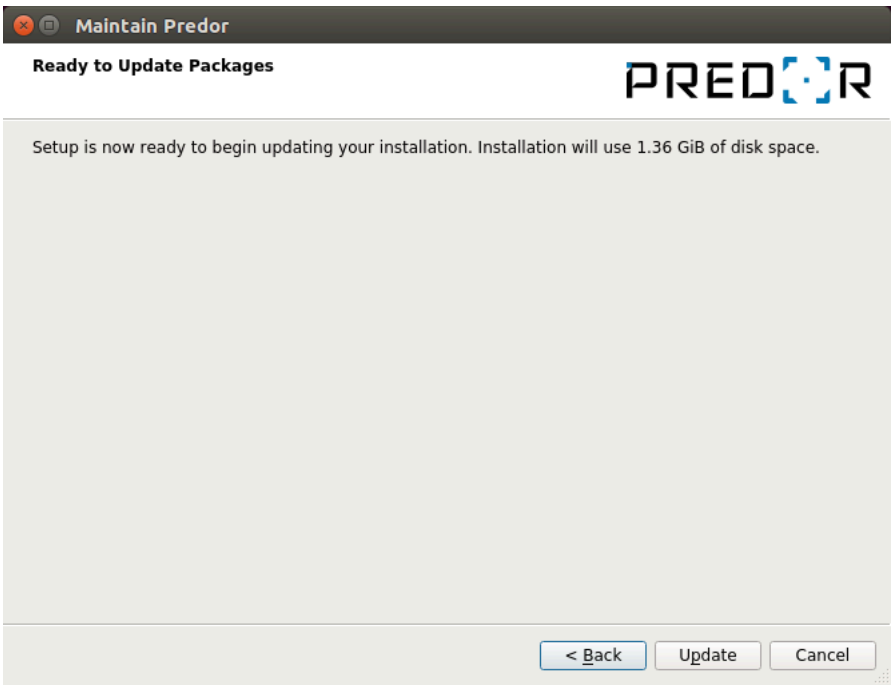


Figure 228: Predor Server update Step 3

The maintenancetool will download and install the software update, this may take several minutes depending on your internet speed. Please be patient until the process is complete and do not attempt to launch the Predor Server software:

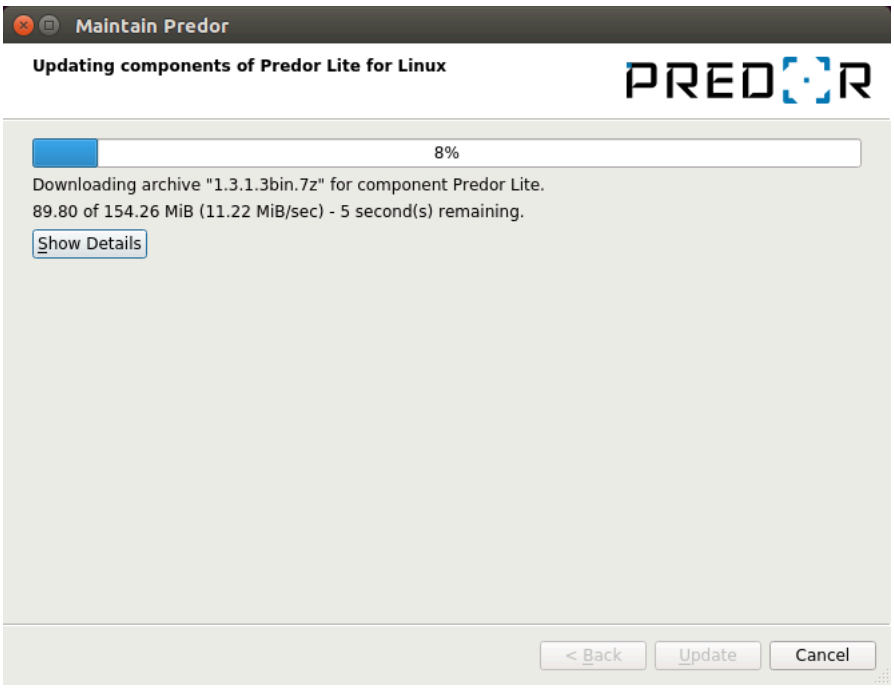


Figure 229: Predor Server update Step 4

The following window will inform you when the update has been successfully completed. To exit the update software, click on the *"Finish"* button!

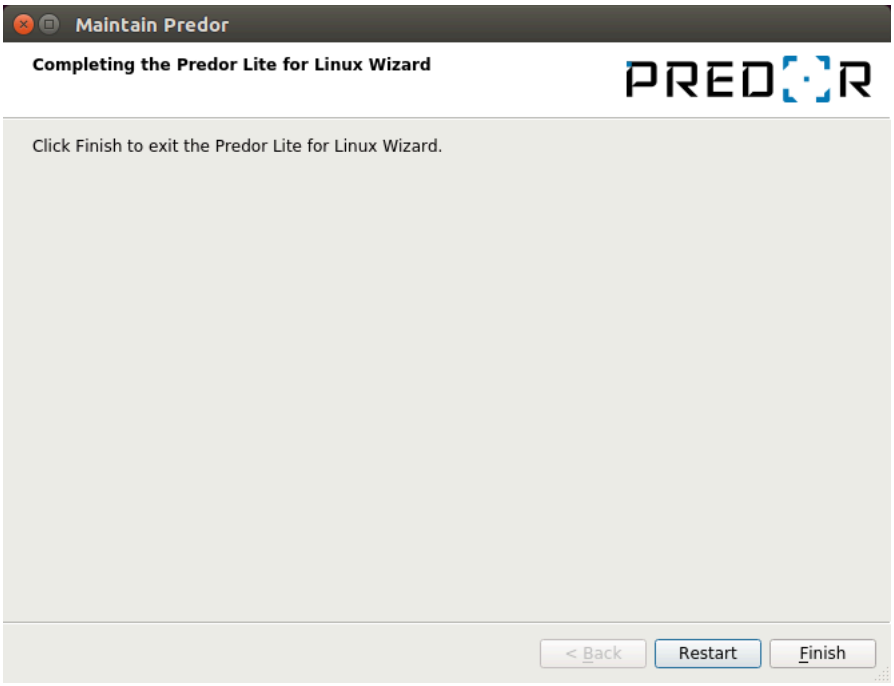


Figure 230: Predor Server update Step 5

After the update, the Predor Server service will not start automatically, you will have to restart it manually for the first time using the following command:

```
sudo systemctl start predor
```

Predor Client

Client updates are done in the same way as with the Predor Server, also using *maintenancetool*.
(On Linux, the default installation path for the client is */opt/PredorEnterpriseClient*)



WARNING: When updating, both the server and the clients must be updated, because only the same version of the server and clients will work together properly.

Firmware update of devices

The software update may sometimes include firmware updates for controllers or work time terminals, so you may also need to update the firmware of the controllers after logging in. A notification will inform you of this within the Predor Lite or Client software, similar to the software update notification:

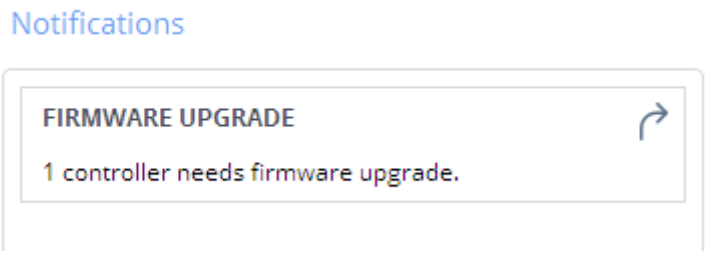


Figure 231: Firmware upgrade notification

Firmware update of controllers

To update, click on the notification, this will navigate you to the **Controllers** submenu of the **Settings** main menu, where a small yellow triangle in the *FIRMWARE* column of controllers indicates the controllers which need to be updated. Select the controllers, then at the bottom menu bar, click on the "**...**" button that collects additional actions and select *"Upgrade firmware"* option.

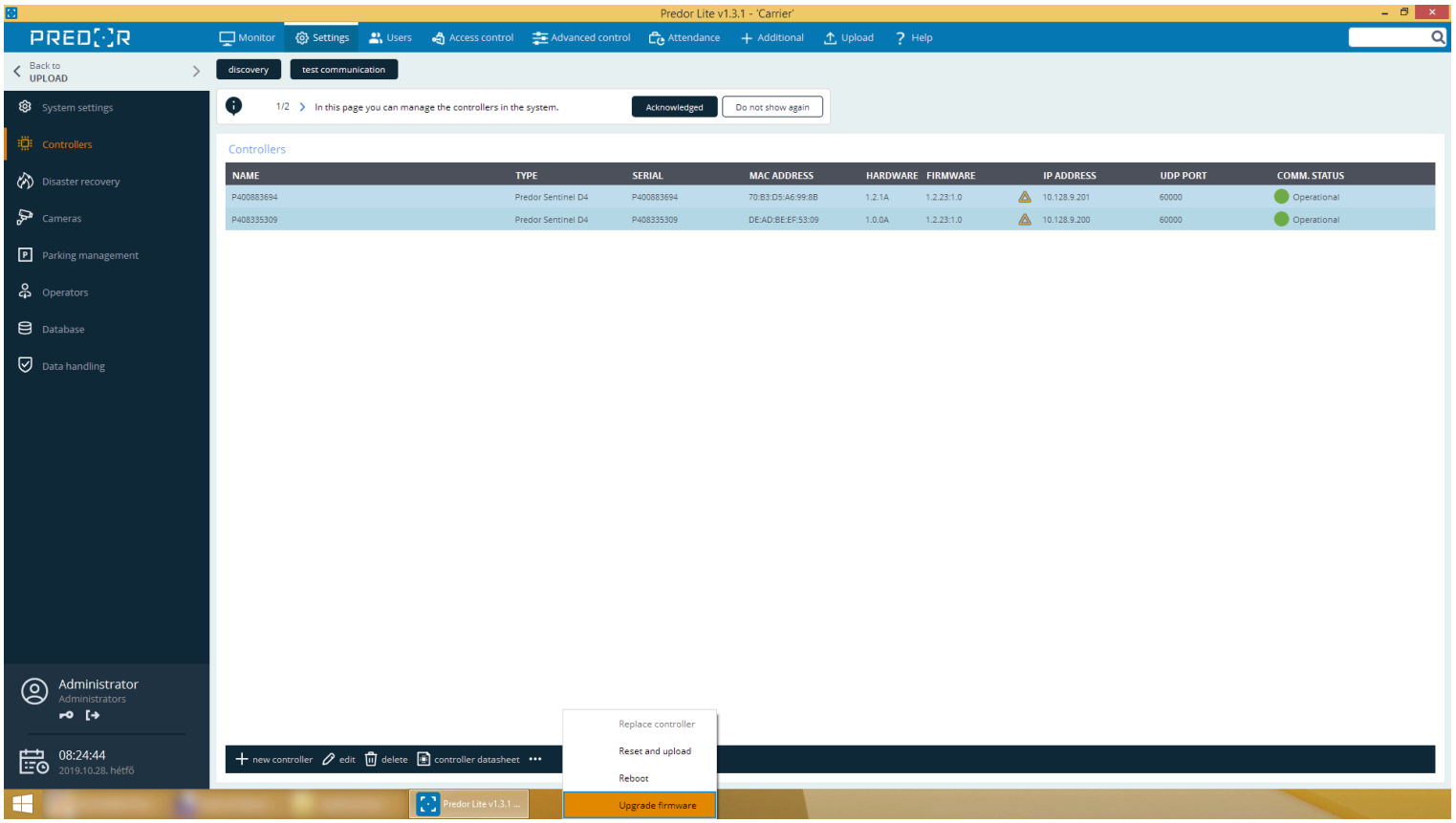


Figure 232: Firmware update of controllers

WARNING: The firmware update may take several minutes, depending on the number of controllers, during this time the controllers are not performing the access control function, so it is suggested to schedule the firmware update for a time when the access control system is less busy.

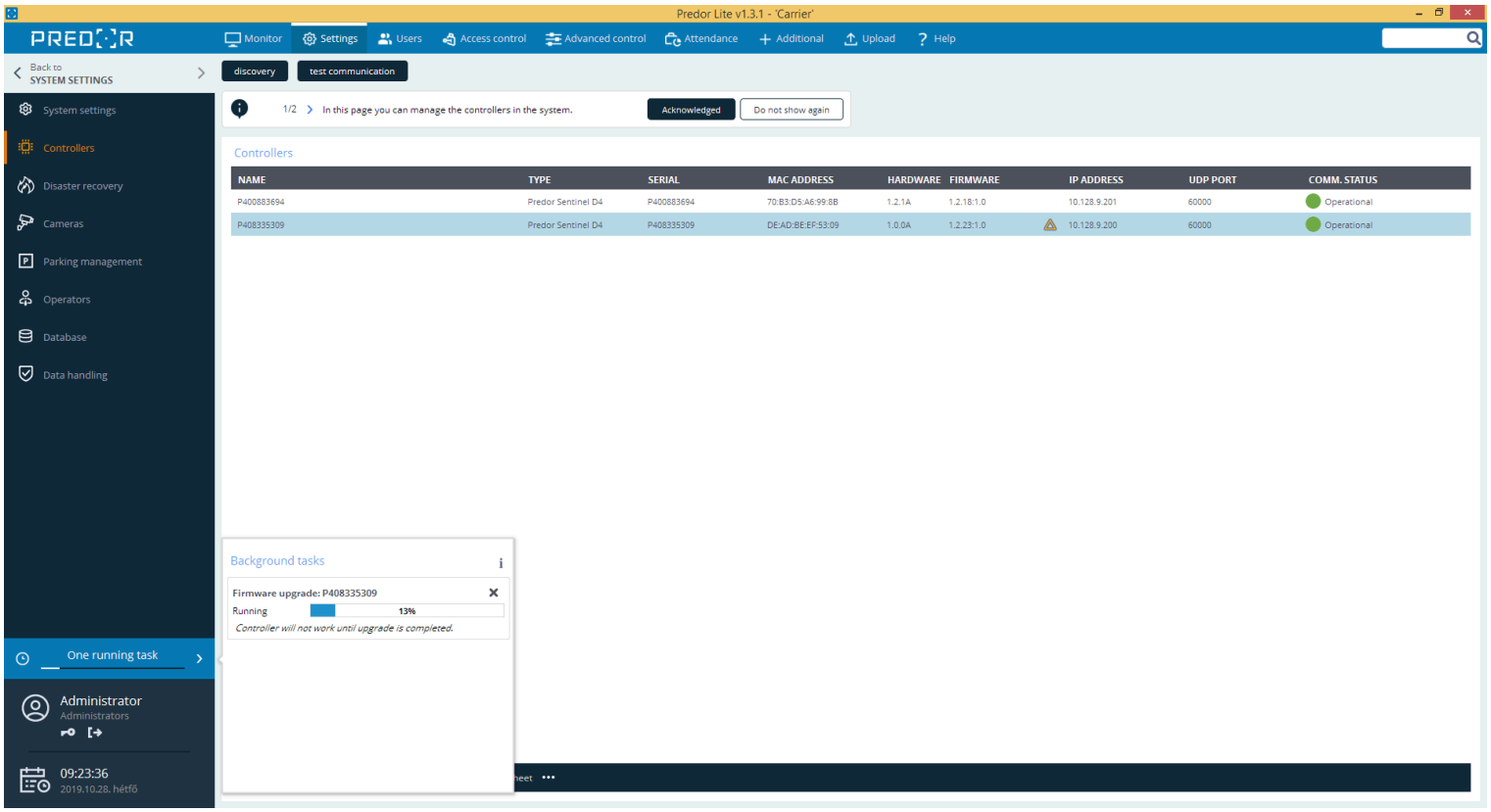


Figure 233: Firmware update in progress

The information bar on the left will tell you about the update process. After a successful firmware update, the settings for the controllers must be re-uploaded, as indicated by the *"Upload"* menu turning yellow.

Firmware update of terminals

To update, click on the notification, this will navigate you to the **Worktime terminals** submenu of the **Attendance** main menu, where a yellow triangle next to the colored ring indicating the communication status in the list of terminals indicates the terminals which need to be updated. The update of the terminals must be initiated one by one, by selecting the terminal and pressing the "**...**" button at the bottom menu bar, then selecting the “Upgrade firmware” option. The update process is indicated in the information bar on the left.

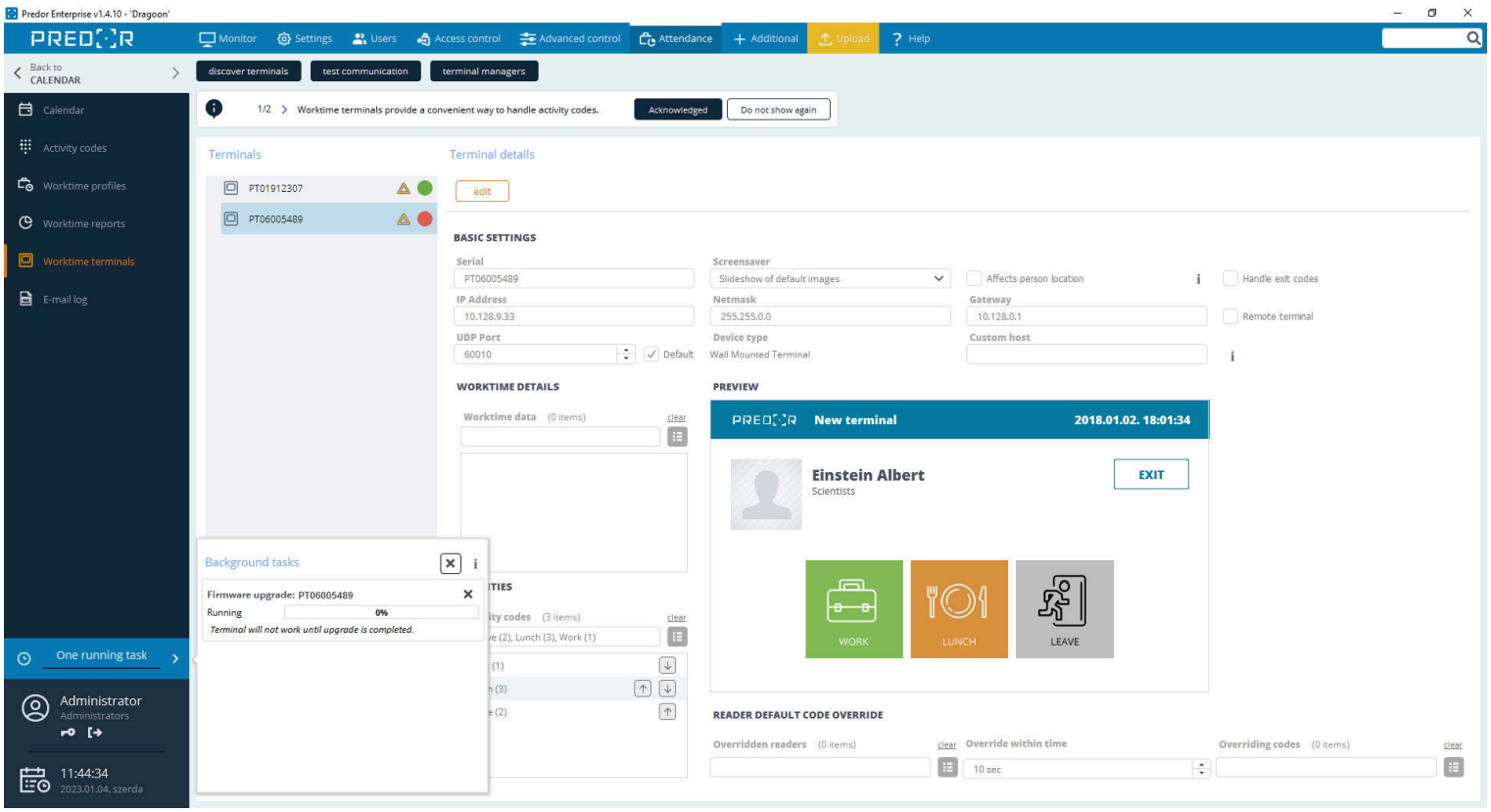


Figure 234: Firmware update of terminals

18 APPENDIX B: SYSTEM ADMINISTRATOR'S GUIDE

System overview

Software editions

The Predor system can be purchased in two basic editions:

- Predor Lite software
- Predor Enterprise software

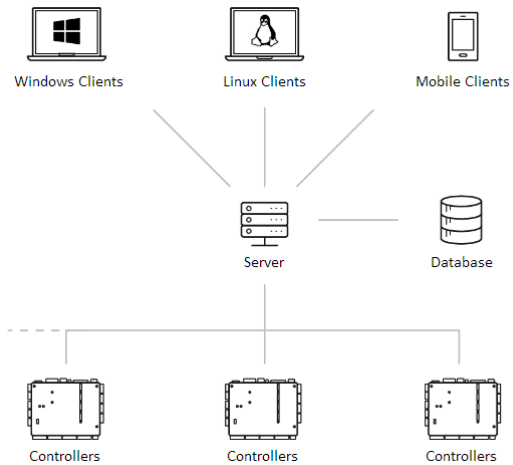
The two editions are best used in different system architectures. This guide will help decide which one to use. All editions support the following platforms:

- Microsoft Windows 10, 11 (64 bit)
- Microsoft Windows Server 2016, 2019, 2022 (64 bit)
- Ubuntu 20.04 LTS (64 bit)

Predor Enterprise edition

The enterprise edition requires a **central server**. All clients connect to this server with their computers or other devices. The system handles multiple logons simultaneously and every user can manage the system according to their operator rights.

The Enterprise edition usually uses the PostgreSQL or MSSQL system as its database engine, as it allows creating backups on the fly, without shutting down the Predor server application. For simplicity SQLite database is also available optionally.

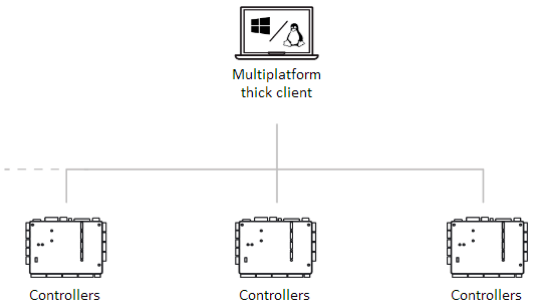


Main features:

- Multiple clients simultaneously
- Linux and Windows platform
- Mobile application
- Global functions
- Automatic e-mail functions
- Automatic reports

Predor Lite edition

A much simpler system, the multiplatform thick client directly communicates with the controllers. The database engine can be SQLite only. Only one client can connect to the database, mobile application and automatic e-mail functions are not available.



Main features:

- Only one client at a time
- Linux and Windows platform
- No mobile application available
- Only controller-level functions

System requirements

System requirements for the Predor system is heavily dependent on the following factors:

- Number of users (card holders) in the system
- Number of controllers in the system
- Number of daily events (eg. card swipes)

In the following tables, depending on the parameters mentioned above, we prescribe minimum and recommended system requirements. If our system reaches one of the parameters in order of magnitude, from then on our system should be classified in that category regardless of the other parameters.



WARNING: We've seen that running the software in Hyper-V was drastically slower because virtualization slowed down IO operations, which caused database read/write to be slow. In our experience, this was especially true when using PostgreSQL database.

Enterprise server application

Small system, enterprise server (1-2 controllers or 10-20 users or 100-200 events per day)

Component	Minimum	Recommended
Processor (CPU)	2 GHz, 2 cores (eg. 10th Gen Intel Core i3 or equivalent)	2,4 GHz, 4 cores (eg. 10th Gen Intel Core i5 or equivalent)
Memory (RAM)	4 GB DDR3	8 GB DDR3
Storage	10 GB	100 GB
Network	100 Mbit Ethernet	1000 Mbit Ethernet

Table 4: System requirements for a small system (enterprise server)

Medium system, enterprise server (10 controllers or 100 users or 2000 events per day)

Component	Minimum	Recommended
Processor (CPU)	2 GHz, 2 cores (pl. 10th Gen Intel Core i3 or equivalent)	2,4 GHz, 4 cores (pl. 10th Gen Intel Core i5 or equivalent)
Memory (RAM)	8 GB DDR3	8 GB DDR4
Storage (SSD)	100 GB	100 GB
Network	1000 Mbit Ethernet	1000 Mbit Ethernet

Table 5: System requirements for a medium system (enterprise server)

Large corporation system, enterprise server (50 controllers or 1000 users or 10 000 events per day)

Component	Minimum	Recommended
Processor (CPU)	2.9 GHz, 8 cores (e.g. 10th Gen INTEL Core i7 or equivalent)	2.3 GHz, 16 cores (e.g. Intel Xeon Gold 6140 or equivalent)
Memory (RAM)	16 GB DDR4	32 GB DDR4
Storage (SSD)	100 GB	200 GB
Network	1000 Mbit Ethernet	1000 Mbit Ethernet

Table 6: System requirements for a large corporation system (enterprise server)

In case of a significantly higher load than this, it is worth choosing a server machine with

more resources.

If we want to perform unusual resource-intensive operations in our system, e.g.: (synchronization of third-party software events, etc.), we can determine the optimal system requirements during a personal consultation.

When using the Linux operating system, the X server is also required for the operation of the Predor server! [5]

Enterprise client application

Component	Minimum	Recommended
Processor (CPU)	2 GHz, 2 cores (e.g. 10th Gen Intel Core i3 or equivalent)	2.4 GHz, 4 cores (e.g. 10th Gen Intel Core i5 or equivalent)
Memory (RAM)	4 GB DDR3	8 GB DDR3
Storage (HDD)	10 GB	20 GB
Network	100 Mbit Ethernet	1000 Mbit Ethernet
Display	1920x1080 resolution	1920x1080 resolution

Table 7: System requirements for any system (enterprise client)

[5] A Predor enterprise server edition with Docker containers is available, which does not require the presence of the X server on the host machine.

Lite client application

Small system, lite client (1-2 door controllers or 10-20 users or 100-200 events per day)

Component	Minimum	Recommended
Processor (CPU)	2 GHz, 2 cores (e.g. 10th Gen Intel Core i3 or equivalent)	2.4 GHz, 4 cores (e.g. 10th Gen Intel Core i5 or equivalent)
Memory (RAM)	4 GB DDR3	8 GB DDR3
Storage (SSD)	10	20
Network	100 Mbit Ethernet	1000 Mbit Ethernet
Display	1920x1080 resolution	1920x1080 resolution

Table 8: System requirements for small system (lite client)

Medium system, lite client (10 door controllers or 100 users or 2000 events per day)

Component	Minimum	Recommended
Processor (CPU)	2.4 GHz, 4 cores (e.g. 10th Gen Intel Core i5 or equivalent)	3.6 GHz, 8 cores (e.g. 10th Gen Intel Core i7 or equivalent)
Memory (RAM)	8 GB DDR3	8 GB DDR4
Storage (SSD)	100 GB	100 GB
Network	1000 Mbit Ethernet	1000 Mbit Ethernet
Display	1920x1080 resolution	1920x1080 resolution

Table 9: System requirements for a medium system (lite client)

In case of a significantly higher load than this, it is worth choosing the enterprise system.

Network configuration

Basic requirements

As Predor is a security technology system, it is heavily impacted on the quality (performance, security) of the network it uses. On a slower or heavily utilized network data reception can be delayed, which means the reaction time for an occasional problem or alarm rises. Easily accessible networks (eg. wireless networks) can cause security issues because they are susceptible for external interference or sabotage.

In conclusion the following design decisions were made, which the network must provide:

- The server [6] and the controllers must be on the **same subnet**.
  - Controllers are accessed directly, no internet connection is needed on either side.
  - Communication through the internet could compromise the securtiy of the system.
  - Controllers are easily manageable (discoverable on the network by using broadcast messages), the installing procedure is simple.
- The network used by the security technology devices must be separated.
  - Wireless devices are not recommended.
  - Must not be reachable for unauthorized people.
  - Utilization of the main network should not affect the security system network.
- All devices on the security system network including the controllers and the server should have an uninterruptible power supply (UPS).
  - Controllers are equipped with a battery, but they are designed for occasional power outages only. Do not connect the controllers on regularly switched power sources, because it can greatly affect the lifetime of the battery.
  - For the global functions to work properly the communication between the server and controllers must be provided, so all switches and routers on the network should have a UPS too.

Multi-site access control systems

Multi-site access control systems are possible by using a VPN (Virtual Private Network) connection between sites. **The VPN connection must be provided by the network trans-**

[6] In case of Lite edition, the server means the Lite client software

parently for all devices (controller/work time terminal/mobile application/server/clients) **of the Predor system.** This type of VPN connection is called a **Site-to-Site VPN** connection. Site-to-Site VPN support is a common feature of professional, business class routers, but software solutions also exist (eg. by using OpenVPN Access Server and Gateway Clients)

Network diagnostics

Before installing the Predor server and devices in place, the network can be tested if it meets the requirements of the Predor system. The test method requires a computer on each endpoint of the network where the server and a device will be installed and uses the **NetCat** networking utility which is available for free on both Linux and Windows operating systems. A computer will act as the server, the other one will act as the Predor access control device. Connect the computers to the network and set their network parameters appropriately.

On Windows systems open a **cmd** window and navigate to the folder of netcat. On linux systems just open a terminal window. The steps written below verify the default settings. If the ports are changed in server configuration, please substitue them in these commands as well.

- Network readiness test for Predor work time terminal:
  1. UDP connection test towards the work time terminal:
     - On the computer at the work time terminal endpoint type the following:

       ```
       nc -u - L -p 60010
       ```

       then press Enter.
     - On the computer imitating the server type:

       ```
       nc -u <IP address of the work time
       terminal> 60010
       ```

       then press Enter.
     - Every text messages written into the cmd/terminal window of the server endpoint must arrive to the other computer (messages are sent when Enter is pressed).
  2. UDP connection test towards the server:
     - On the computer at the server endpoint type the following:

       ```
       nc -u -L -p 60012
       ```

       then press Enter.
     - On the computer imitating the work time terminal type:

```
nc -u <IP address of the server
endpoint> 60012
```

then press Enter.

- Every text messages written into the cmd/terminal window of the work time terminal endpoint must arrive to the other computer (messages are sent when Enter is pressed).

3. TCP connection test:
   - On the computer at the server endpoint type the following:

     ```
     nc -L -p 8888
     ```

     then press Enter.
   - On the computer at the work time terminal endpoint type:

     ```
     nc <IP address of the server endpoint>
     8888
     ```

     then press Enter.
   - Every text messages written into the cmd/terminal window of either endpoint must arrive to the other computer.

- Network readiness test for Predor access controller:

1. UDP connection test towards the controller:
   - On the computer at the controller endpoint type the following:

     ```
     nc -u - L -p 60000
     ```

     then press Enter.
   - On the computer at the server endpoint type the following:

     ```
     nc -u <IP address of the controller
     endpoint> 60000
     ```

     then press Enter.
   - Every text messages written into the cmd/terminal window of the server endpoint must arrive to the computer at the controller endpoint (messages are sent when Enter is pressed).

2. UDP connection test towards the server:
   - On the computer at the server endpoint type the following:

     ```
     nc -u -L -p 60002
     ```

     then press Enter.
   - On the computer at the controller endpoint type the following:

```
nc -u <IP address of the server
endpoint> 60002
```

then press Enter.

- Every text messages written into the cmd/terminal window of the controller endpoint must arrive to the computer at the server endpoint (messages are sent when Enter is pressed).

Default ports

If it is possible, it is advised that during the first setup of the system the firewall should be deactivated, and after confirming that everything is working as intended, then re-activate the firewall and open the required ports. By default the system uses these ports:

Port	Direction	Function
TCP 8888	Client, Terminal → Server (only Enterprise)	HTTP port of the server. This port is used to connect to the server.
TCP 8899	Client ↔ Server (only Enterprise)	Signal port of the server. This port is used to send various signals to the connected clients.
TCP 3000	Web (browser) → Server (only Enterprise)	Port of the Work time web. This port is used for employees to access the work time web interface.
UDP 60000	Server → Controller	Port for reaching the access controllers. It is used to communicate and upload settings to the controllers.
UDP 60001	Server → Controller	Service port for the access controllers. It cannot be changed but it is only used in some special cases (not needed under normal operation conditions).
UDP 60002	Server ← Controller	Listening port for the access controllers. The access controllers report to the server on this port.
UDP 60010	Server → Terminal	Port for reaching the work time terminals. This port is used to send control messages to the terminals.
UDP 60011	Server → Terminal	Service port for the work time terminals. It cannot be changed but it is only used in some special cases.

Continued on the next page...

Port	Direction	Function
UDP 60012	Server ← Terminal	Listening port for the work time terminals. The work time terminals report to the server in this port.

Table 10: Default ports used by the Predor system

First steps

If the network can provide the basic requirements, we can proceed to set things up in the Predor software.

1. Configure the IP pool – the server and controllers must be in the same subnet. This IP pool will be automatically assigned sequentially for the attached devices. It is important to note, that if a DHCP server is operating on the network, this IP pool must not overlap with the DHCP pool.
2. Set the controller password – the communication will be enciphered with this password.
3. Discover the controllers – if everything is operational, the table should contain all installed controllers.
4. Add the controllers to the system.
5. Activate the license – activation requires at least one device added to the system.
6. Update the firmware of the controllers
7. Upload the settings

Network access of controllers

The controllers in their factory default state are accessible on the IP address 192.168.0.200. The controllers can not request IP addresses from a DHCP server. If they are in the same broadcast domain with the server no pre-configuring is needed, because the server can communicate with all the controllers using broadcast messages, and can assign unique IP for them by using the serial numbers as identifiers.

Network access of work time terminals

Work time terminals can request IP addresses from DHCP servers. In fact, although static IP address is an option in the settings, they cannot operate without a DHCP server on the network. The IP address of the terminal is visible in the internal menu, which can be accessed by tapping the Predor logo in the upper left corner on the screen multiple times,

and then providing the controller password set in the Predor client (factory default is empty password).

The terminal connects to the server on two ports, and the connection protocol must be the same as the server's setting (HTTP/HTTPS). If there is an HTTP connection problem with the terminal, please check if the protocol is set appropriately. It is advised that the "Automatically select protocol" option is set to "For the first time", because this way the work time terminal tries to connect from the safest to the less safe methods, and automatically determines the usable protocol.

Troubleshooting

Below is a table of common errors, what can cause them, and solutions on how to counter them.

Phenomenon	Caused by	Solution
Discovery does not show any devices.	A firewall is operating on the computer or on the network.	Turn off the firewall or check its settings.
	Network links are not working properly.	Check the link LEDs on the controllers.
	Controllers are encpihered with a different password.	Reset the controllers. (Physical access to the controllers is needed.)
	The server and the controllers are not in the same broadcast domain.	Discovery is not possible without this, in this case the controllers have to be added manually.
Controller initialization does not start.	A firewall is operating on the computer or on the network.	Turn off the firewall or check its settings.
After successful initialization of the controllers, the communication stops.	Incorrect IP address has been uploaded to the controller.	Check the controller IP pool in the software. The misconfigured controller(s) IP address can be corrected in the “Edit controller” dialog, where it is possible to immediately update the IP address only.
After successful initialization of the controllers, the events are late, the communication status shows transmit problems.	Possible IP conflict, the IP address was already used by an other device.	Check the controller IP pool. Make sure, that there are no other devices in the IP pool and it does not overlap with a DHCP pool. The controller(s) IP address can be corrected in the “Edit controller” dialog, where it is possible to immediately update the IP address only.

Continued on the next page...

Phenomenon	Caused by	Solution
In case of Enterprise editon the client software rejects the connection to the server with an “unknown error occured” message.	The client software is unable to communicate to the server with the given ports and/or protocol.	Check the connection parameters, especially the communication and signal ports.
In case of Enterprise edition the client cannot connect to the server.	After installing the server, it does not start automatically, just after the rebooting the operating system.	Start the service manually: on Windows from the services menu, on Linux with the following command: *sudo systemctl start predor*.
	A firewall is operating on the computer or on the network.	Turn off the firewall or check its settings. Try to connect from a web browser to the server port (depending on the actual settings: http://<server IP address>:8888).
The Predor server keeps restarting continuously.	The server configuration file (*predor_server.ini*) has incorrect settings. (eg. incorrect system identifier).	Use the Predor Configuration Manager application (*predor_iniman*), or edit the file manually.
	The used server ports are already taken by other applications.	Change the ports used by the Predor server using the Predor Configuration Manager application, or stop the application(s) using the ports.
	If an older Predor server version is re-installed, then the database version may be newer than the software expects.	After reinstalling an older version of the application, restore a database backup made with that version.

Continued on the next page...

Phenomenon	Caused by	Solution
After adding a work time terminal to the system, the settings cannot be uploaded, it does not communicate with the server.	HTTP/HTTPS protocol selection error may have happened.	Check the protocol settings in the terminal's internal menu under the "Server Communication" submenu, and correct the parameters, if neccessary.
The working time web cannot be accessed from the internal network.	The web is accessible from external networks, but the hairpin NAT is not configured on the router.	The hairpin NAT must be configured on the router(s) in the internal network.

Table 11: Common errors and solutions

Special cases

Adding a controller from another subnet

If the server and controllers cannot be in the same subnet, one of these procedures can be followed to add them to the system successfully:

Temporarily connect the controller to the server, then install it to the desired place.

1. Connect the controller to the same network as the server, then add it to the system using the discovery function.
2. After successful initialization, edit the controller's network properties manually: set the appropriate IP address, mask and gateway, then press the "Upload network settins immediately" button.
3. Install the controller to the desired place and set the "Custom host" field in the controller editor window. Check if the ports are properly forwarded.

Use a second Predor software on-site to pre-configure the controller and add it manually.

1. Connect a computer to the same network (broadcast domain) as the controller. Install a Predor (Lite, unactivated or DEMO license is sufficient) software on the computer.
2. Set the network parameters (IP pool) and controller password in the Predor software, as described in the "First steps" section.

3. Add the controllers to this temporary system using the discovery function.
4. Alter the network parameters manually if needed, and also upload them with the “Upload network settings immediately” button.
5. Take notes of the controllers’ serials and corresponding IP addresses, as these will be needed for adding them manually to the server.
6. On a client connected to the server navigate to the Settings → Controllers menu. Click the “New controller” button and fill the serial number, network parameters and custom host fields.
7. Controllers that are added manually will not be usable until they are initialized, so if it does not happen automatically, use the “Reset and upload” button to initialize the controllers.

Accessing the web from an external IP address

By default, the working time web can only be accessed on the same network where the server is connected. If you want to access it from another network, the server must be accessible from external IP addresses. Once access has been granted, employees can access the interface by typing the IP address of the server into a web browser. It is advisable to buy a domain in this case, which is easier for employees to remember than an IP address.

Resetting the devices

Resetting and factory resetting of the controllers

Some incorrectly provided network parameters, forgotten controller password can lead to inaccessible controllers. In this case factory resetting the controller is needed, which resets the communication parameters and controller password to the factory default. This can only be done via the RESET button on the controller panel, which needs to be pressed and released in a special sequence:

1. Push the RESET button continuously, until the READ LED (yellow LED) keeps blinking.
2. If the READ LED stops blinking, release the RESET button. The READ LED now flashes faster.
3. If the RESET button is pressed for a short period while the READ LED flashes fast, the factory reset is initiated, in a few seconds the controller reboots, and it will be accessible via the default IP address and ports.

Pushing the RESET button in any other way or sequence just reboots the controller.

Factory resetting the work time terminals

The work time terminals are only resettable via the internal menu, which can be accessed by tapping the Predor logo in the upper left corner of the screen multiple times. To enter the menu, the controller password is needed (it is an empty password by default). In the menu, navigate to the Service submenu, and choose the “Wipe data - restore factory settings” option. All data will be deleted from the terminal: card numbers, logged data, network parameters, etc. It is advised that before doing a factory reset on the terminal it should be disconnected from the network, because if the server detects that the terminal has lost its network parameters, it tries to automatically restore them, including the controller password.

19 APPENDIX C: INSTALLING PREDOR ENTERPRISE SERVER WITH DOCKER

Preparations

On Linux operating systems the Predor Enterprise Server (and also the PostgreSQL database engine) can be installed inside a docker container virtualization image, instead of the native installer packages. Docker containers have the advantage of simpler maintenance, the independence of the host operating system version and the fact that no graphical user interface (GUI) is necessary on the host operating system, thus it can be installed to headless servers via SSH connection.

A prerequisite of installation is *root* access on the computer.

Installing dependencies on Ubuntu

Before installing the dependencies, updating the package list is advised:

```
sudo apt update
```

Then install the docker runtime packages with the following command:

```
sudo apt install docker-compose docker.io
```

Make a directory where the Predor Server's database and other files will be stored:

```
sudo mkdir /opt/predor
```

Configuration

Docker needs a configuration file which describes the needed services and their settings inside the container. It will automatically download and compose the container based on this file. Create an empty file with the name **docker-compose.yml** inside Predor's directory and copy the following content into it:



WARNING: The format of the file has to match this example, the whitespaces are important!



TIP: Inside the docker-compose.yml the # character denotes comments, thus those lines won't be interpreted. Use this to write comments or enable/disable various options.

```
version:  '3.4'

services:
   predor:
      image:  "docker.predor.hu/predor_server:1_3_4_14"
      environment:
          - PREDOR_SYSTEM_ID=YOURSYSTEMID
          #- WEBAPPS=worktimeweb
          #- API_PORT=8888
          #- SIGNAL_PORT=8899
          #- WEBAPP_PORTS=3000
          #- WEBAPP_BASEURLS=https://hostname:3000/
          #- POSTGRESQL_HOST=localhost
          #- POSTGRESQL_USER=postgres
          #- POSTGRESQL_PASS=PostgresPredor123
          #- POSTGRESQL_DB=predor
          #- POSTGRESQL_PORT=5432
      volumes:
          - ./data:/var/predor
          - ./log:/var/log/predor
          - "./share:/.local/share/Leviathan Solutions/Predor Server"
          #- ./plugins/plugin.so:/opt/PredorEnterpriseServer/bin/plugin.so
          - /etc/localtime:/etc/localtime:ro
          - /etc/timezone:/etc/timezone:ro
          #- /var/certs/default:/var/cert:ro
       network_mode:  "host"
       restart:  always
    #  depends_on:
    #      - postgresql

    #postgresql:
    #   image:  "postgres"
    #   environment:
    #       - POSTGRES_USER=postgres
    #       - POSTGRES_PASSWORD=PostgresPredor123
    #       - POSTGRES_DB=predor
    #   volumes:
    #       - ./data:/var/lib/postgresql/data
    #       - /etc/localtime:/etc/localtime:ro
    #       - /etc/timezone:/etc/timezone:ro
    #   network_mode:  "host"
    #   restart:  always
```

In this example yml:

- **every line starting with #**: comment, will not be interpreted (or the default values will be used)
- **image: "docker.predor.hu/predor_server:1_3_4_14"**: this line tells which Predor

Server version will be downloaded and used, in case of an upgrade this version number has to be updated!

- **PREDOR_SYSTEM_ID=**: the systemID must be provided here with capital letters and without spaces or dashes
- **WEBAPPS=worktimeweb**: uncommenting this line will activate the Predor Work Time Web page on the server (if applicable)
- **XXX_PORT**: various ports used by the server can be customized here, if left commented the default values will be used
- **WEBAPP_BASEURLS=https://hostname:3000/**: e-mails associated with the Work Time Web will contain this link for ease of access, point it to your host, if needed
- **POSTGRESQL_XXX**: these lines should only be used if the chosen database engine is PostgreSQL
- **./data**: the "data" directory will contain the database (in case of SQLite). The file's name will be always "database.db3", thus if an already existing database should be used, it has to be renamed.
- **./log**: the "log" directory will contain the log files
- **./share**: the "share" directory will contain the camera recordings
- **./plugins/plugin.so**: if a plugin is used, all of them should be placed inside the "plugins" directory, and all of them should be included here one per line
- **/var/certs/default**: if SSL enciphering is used the certification and private key should be placed inside the directory "/var/certs/default"



TIP: The certificate and the private key must have the following names: **certificate.cer, certificate.key, intermediate.cer, combined.cer, ca.cer**

- **depends_on:** and **lines below**: uncomment these lines only, if you wish to also run a PostgreSQL server **inside this container**

Additional services can be added to this container, for example one which makes automatic backups from the internal PostgreSQL database regularly. To add this service insert the following lines to the docker-compose.yml (the *pgbackups:* is a *service*, so it must be aligned with other services like *predor:* and *pstgresql:* in the file):

```
  pgbackups:
    image:  prodrigestivill/postgres-backup-local
    restart:  always
    user:  postgres:postgres
    volumes:
      - ./pgbackups:/backups
    depends_on:
      - postgresql
    environment:
      - POSTGRES_HOST=localhost
      - POSTGRES_DB=predor
      - POSTGRES_USER=postgres
      - POSTGRES_PASSWORD=PostgresPredor123
      - POSTGRES_EXTRA_OPTS=-Z9 --schema=public --blobs
      - SCHEDULE=@daily
      - BACKUP_KEEP_DAYS=7
      - BACKUP_KEEP_WEEKS=4
      - BACKUP_KEEP_MONTHS=6
      - HEALTHCHECK_PORT=8080
    network_mode:  "host"
```

Save the file if the configuration is complete.

Installation and running



TIP: If the logged in user is a member of the *docker* group, then the following commands won't require *sudo*. To add a user to this group execute the following command: *sudo adduser [user_name] docker*, then log out and log in again!

Prior to installation login credentials must be provided for the Predor's docker server (docker.predor.hu) with the following command:

```
sudo docker login docker.predor.hu
```

The login information for this site is the same used on www.predoraccess.com. Contect your local distributor for login details. The next command must be executed from the directory in which the docker-compose.yml is located. To install and start the container execute:

```
sudo docker-compose up -d
```

If everything is correct, the installation should start and after downloading the necessary packages the container will start in the background as a system service (i.e. it will automatically start even after rebooting the computer).

If everything is up and running, log out from the docker server, because it stores the login information locally in a temporary plain file:

```
sudo docker logout docker.predor.hu
```

Useful commands

Below are a collection of useful commands for managing the docker container. These commands always have to be executed from the directory where the docker-compose.yml is located.

- **sudo docker-compose ps**: show the state of the container
- **sudo docker-compose stop**: stop the services
- **sudo docker-compose start**: start the services
- **sudo docker-compose down**: stop and delete the container (as the database and other files are located outside the container, this command does not imply loss of data)
- **sudo docker-compose up -d**: create and start services
- **sudo docker-compose logs**: show logs for this container
- **sudo docker-compose logs –follow**: show and follow logs
- **sudo docker-compose logs –tail 100**: show the last 100 lines of logs
- **sudo docker-compose restart**: restart the services

Backing up the database

SQLite databases

In case of SQLite database engine the database file has to be backed up by copying it to a backup directory. During the copying process the Predor server cannot run, so it has to be stopped first. Make the backup by followin the instructions below:

- Stop the container:

```
sudo docker-compose stop
```

- Copy the *database.db3* file from the path defined in *docker-compose.yml*
- Restart the container:

```
sudo docker-compose start
```

PostgreSQL databases

In case of PostgreSQL database engine, the backup can be made on the fly using the console application pg_dump or other GUI enabled database handling software (pgAdmin, DBeaver, etc.).

If the container also runs the PostgreSQL server, the following command can be used to make a backup file outside the container:

```
docker-compose exec -T postgresql pg_dumpall -c -U postgres >
dump_`date +%Y-%m-%d"_"%H_%M_%S`.sql
```

Updating

Commands needed for updating the server will only work from th directory where the docker-compose.yml file is located. Please follow the instructions below to update the container:

- Change the version number of the predor_server service in the *docker-compose.yml* file.
- If our system have a plugins, it is also advised to copy them to a backup directory.
- Download the new plugins from www.predoraccess.com and overwrite the old ones.
- Log in with your credentials to Predor's docker server:

```
sudo docker login docker.predor.hu
```

- Download the new version:

```
sudo docker-compose pull
```

- When downloading has completed, log out:

```
sudo docker logout docker.predor.hu
```

- Stop the running container:

```
sudo docker-compose stop
```

- **Make a backup of the database!** Predor's database structure may be changed upon updating which older versions cannot handle correctly, thus downgrading may not be possible without a backup of the database!
- Start the container:

```
sudo docker-compose up -d
```

Restoring the database

SQLite databases

In case of SQLite database the database file has to be copied back to location defined by docker-compose.yml. During restoration the container cannot run, so it must be stopped before. Please follow the steps below to restore the database:

- Stop the container:

```
sudo docker-compose stop
```

- Copy the backup database file to the location specified in *docker-compose.yml* and rename it to "database.db3".
- Start the container:

```
sudo docker-compose start
```

If a full system downgrade is necessary, then follow the steps described in the system update section, but instead of backing up the plugins and database, their restoration is needed.

PostgreSQL databases

During restoration systems with PostgreSQL database engines are also need to be stopped. Only the Predor service must be stopped, so this time use this command:

```
sudo docker-compose stop predor
```

. To restore the database the console application pg_dump or other GUI enabled database handling software (pgAdmin, DBeaver, etc.) can be used.



ATTENTION! Databases must be restored to an empty database! Please backup/drop your current database before starting the restoration of a previous one!

For PostgreSQL running inside the container we can use the built-in psql command to restore the database, but we will need the container's identifier (CONTAINER_ID) first:

```
docker ps
```

Use the following command to start the restoration:

```
cat [dump_name].sql | docker exec -i [container_id] psql -U postgres
```

If the file to be restored is not a full dump (was not made by using pg_dumpall), then the database's name must be provided too:

```
cat [dump_name].sql | docker exec -i [container_id] psql -U postgres -d
[db_name]
```

After the restore has completed start the *predor* service again:

```
sudo docker-compose start predor
```

If a full system downgrade is necessary, then follow the steps described in the system update section, but instead of backing up the plugins and database, their restoration is needed.

20 APPENDIX D: PREDOR TERMINAL INSTALLATION GUIDE



Figure 235: Predor worktime terminal

Environmental conditions for installation

When placing the terminal, the following parameters should be taken into consideration:

- The terminal is **for indoor use only** – it cannot be installed outdoors, even in a place protected from rain!
- Must be installed in **a place protected from radiant heat** (preferably also from direct sunlight)
- It should be installed in a location protected from **high humidity** and **splashing water**.
- Must not be installed where users can use it with wet hands.

During operation of the terminal, the following environmental parameters must be guaranteed:

- Operating temperature range: 0 - 35°C
- Operating humidity range: 10 - 90%

Cabling

The terminal requires two cables to operate:

- **communication cable:** UTP (recommended Cat5E), max. 100m
- **power cable:** 2-core cable, **appropriate core thickness**

Proper construction of the power cable

The terminal is a low-voltage (5V DC) but high-current (3A) device, so **special care must be taken when wiring to ensure proper power supply!** Ensure that the correct voltage ($4.8V < U_{in} < 5.5V$) is measured at the terminal both at no load and at full load. Based on this, the following recommendations can be made:

- The terminal should preferably **be connected to the power supply with a cable with a cross-sectional area of 1mm^2 or larger**.
- The terminal should preferably **be connected to the 5V supply with a cable as short as possible, recommended < 2m**. If this is not feasible, a 12V-5V/3A DC-DC converter may help. In this case, the 12V can be connected from further away.

Power cable compliance check

Before final installation of the terminal, it is advisable to check that the power supply is correct. The way to do this:

- Remove the batteries from the terminal!
- Connect the terminal to the Ethernet network!
- Power on the terminal and check for any malfunctions (e.g. the terminal fails to start/restarts/the card reader in it beeps at regular intervals)! If it starts up successfully, let the terminal run for a few minutes and check if it restarts at any time.
    - If any abnormalities are found, check if the same phenomenon occurs with inserted (see: Replacing batteries chapter) (charged) batteries. If not, it is most likely that the power supply is not correct. If the correct voltage can be measured at the connector without load, try reducing the length of the power cable or increasing its cross-section.
- If the terminal has remained operational during the power check test, insert the batteries (see: Replacing batteries chapter) and check the terminal for a pictogram next to the clock indicating that the battery is charging: 

Replacing batteries

Features of the battery added to the terminal at the factory:

- **Technology** lithium-ion
- **Charging voltage:** 4,2V
- **Planned capacity:** 2850mAh

Only use batteries **with the same technology and charging voltage** as the factory battery!

Batteries should always be handled in pairs, so they should be removed and inserted together at the same time. Only batteries of the same type, from the same manufacturer and handled in the same way may be used.**Simultaneous use of batteries from different manufacturers is prohibited! Simultaneous usage of batteries with different rated capacities** (even from the same manufacturer) **is prohibited! Mixing batteries of different charge levels, or using them at the same time is prohibited! When inserting the batteries, make sure that the polarity is correct**, as indicated by the label on the battery cover and the mark on the battery socket:

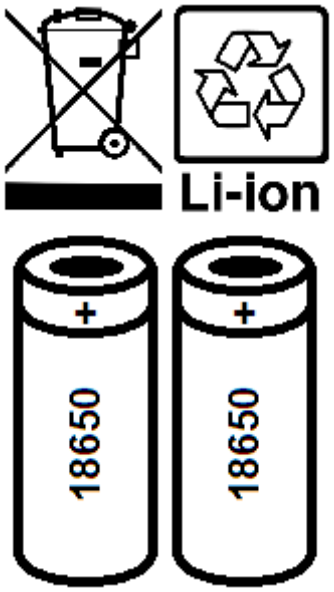


Figure 236: Label on battery cover with correct battery polarity

Configuration, network management

In the Predor software, check the network settings for the controllers (controller IP range, ports) and allow the appropriate ports through the firewall/router (**server TCP and server UDP**, which can be changed in the Predor software in **Settings**→**System Settings** page.)

Once you are sure that the settings are correct, you need to add the terminal to the software using the discover terminals function in the software.

The terminal has its own internal menu system, which can be accessed by repeatedly tapping the Predor logo in the top left corner. Once you have entered the controller password (the controller password set for controllers in the Predor software, by default an empty password), you have the option to:

- check, modify the IP address/port/gateway
- check, modify the server IP address/port
- set HTTP connection mode
- restart or shut down the terminal
- reset network parameters (IP address, password)
- enable/disable the display of card numbers
- change the terminal language

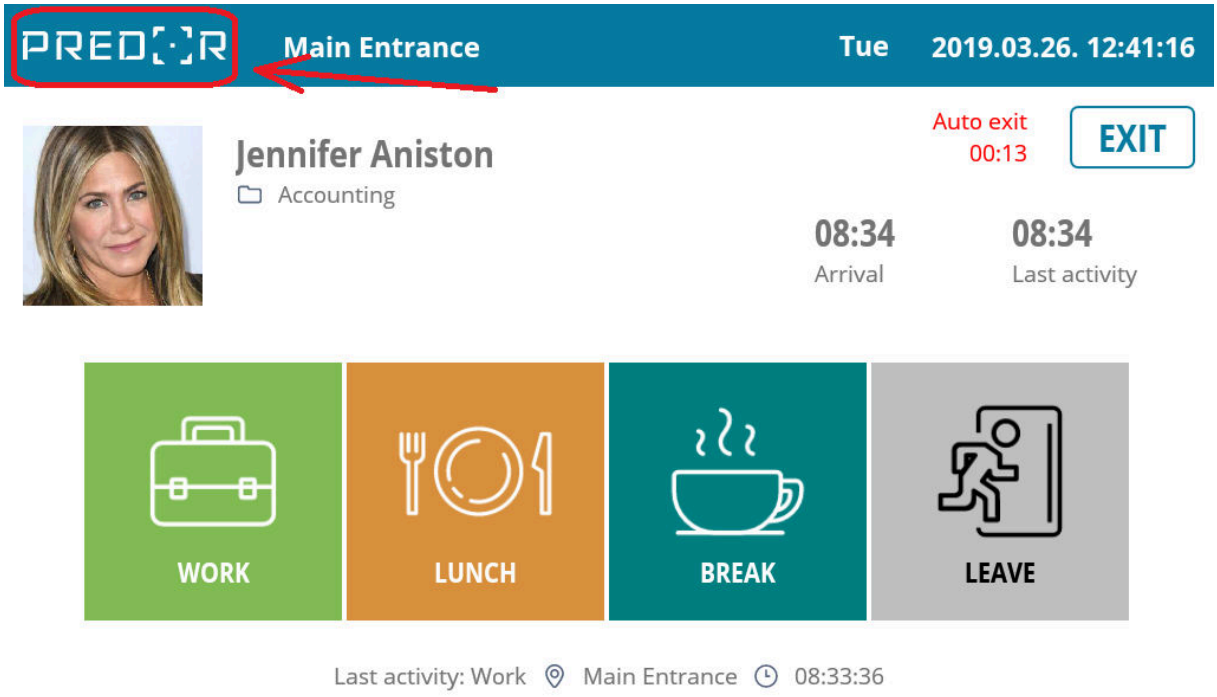


Figure 237: The terminal menu can be accessed by repeatedly tapping the Predor logo

Troubleshooting

Below we have collected some typical mistakes with possible causes and suggestions.

Phenomenon	Possible causes	Suggestions
The discovery does not display the terminal.	A firewall on your computer (or network) filters traffic.	Turn off the firewall or check its settings.
	The network links are not working properly.	Check the corresponding LEDs on the terminal.
	The terminal is protected by a different password.	Terminal must be reset. (Physical access to the device is required.)
	The terminal and the server are in different broadcast domains.	The discovery is not possible without it, so you have to add the terminal to the system manually.
The terminal initialization does not start.	A firewall on your computer (or network) filters traffic.	Turn off the firewall or check its settings.

Continued on the next page...

Phenomenon	Possible causes	Suggestions
No communication after successful initialization of the terminal.	The terminal is configured with the wrong IP address.	Check the IP domain. When editing the problematic terminal, it is possible to upload the corrected IP address immediately.
After successful initialization of the controllers, events are slow to arrive, there is a transmission problem.	There may be an IP address collision on the network, the IP address assigned to the controller was already in use.	Check the IP range, make sure that there are no devices on the network in the range you want to allocate, and there is no overlapping with the DHCP range. When editing the problematic controller, it is possible to immediately upload the corrected IP address.
After adding the terminal, the settings are not loaded, the device does not communicate with the server	HTTP/HTTPS protocol selection error may have occurred on the terminal	Check the settings under “Server communication” in the terminal’s internal menu and correct them if necessary.

Table 12: Typical mistakes and suggested solutions

21 APPENDIX E: PREDOR TERMINAL REPLACEMENT GUIDE

Predor terminal dismounting

The first step is to dismount the Predor terminal:

1. Remove the 2 cross-head screws (Philips) located at the bottom of the casing.
2. Slightly lift the bottom of the terminal away from the wall, then pull down slightly to unhook the top hook and pull the whole enclosure away from the back cover!
3. Remove the Ethernet and power cables!
4. On the back of the housing is a lid, which is also secured by a cross-head screw. The batteries for intermittent operation are located under this. Remove the screw and the lid.
5. Remove the batteries.

WARNING: Do not use any sharp or metal objects to remove the batteries, because they can easily touch the contacts or the metal casing of the device, causing a short circuit!

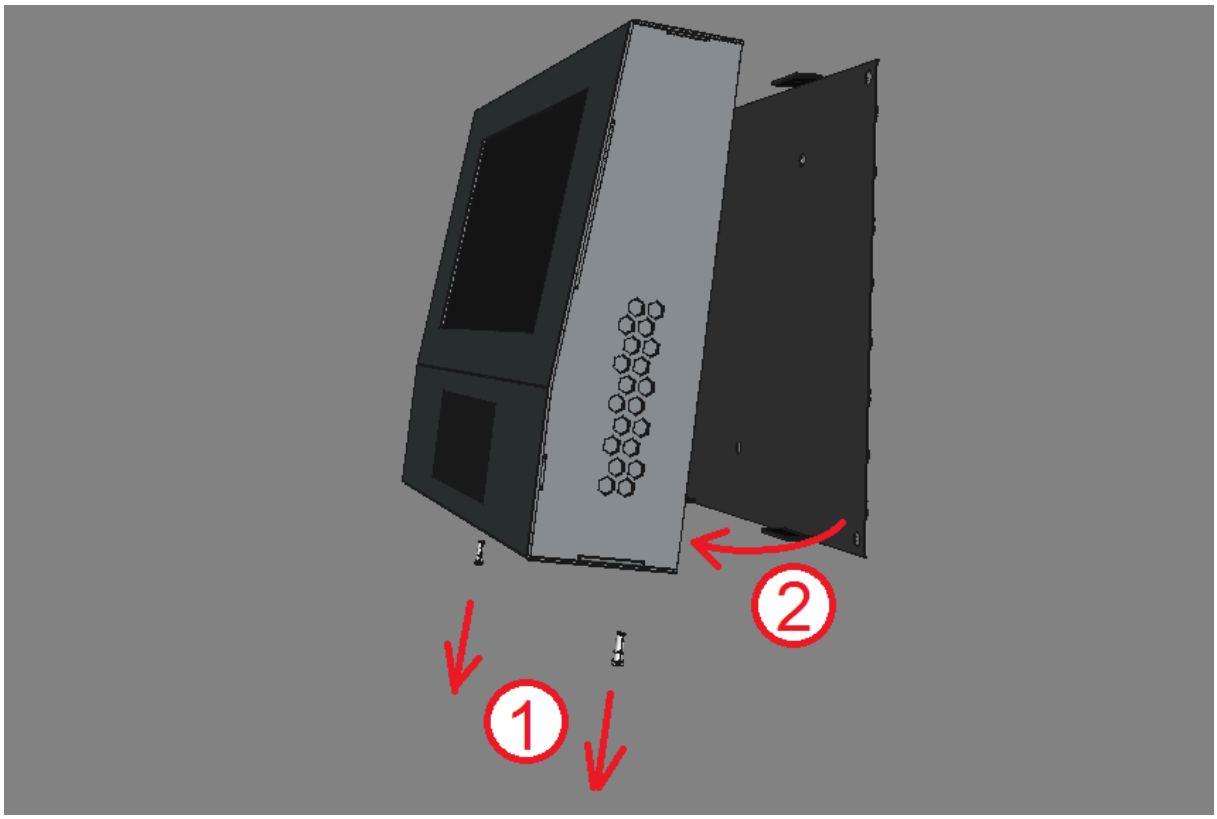


Figure 238: Dismounting the Predor terminal from the back cover

Replacement Predor terminal installation

The received replacement terminal can be mounted on the wall bracket in the reverse order of dismounting:

1. Remove the 2 cross-head screws (Philips) located at the bottom of the casing.
2. Holding the bottom of the terminal, slightly lift the rear bracket, then push the bracket slightly upwards to unhook the top hook and pull the whole enclosure away from the back cover!
3. Remove the cover screw from the back of the casing and the cover plate!
4. Insert the batteries! **Make sure the polarity is correct**, as indicated by the markings on the battery holder and the sticker on the cover!

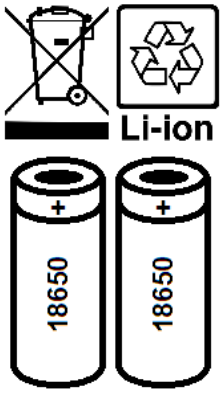


Figure 239: Label on the battery cover with correct battery polarity

5. Place the battery cover back on and secure it with the screw!
6. Connect the Ethernet and power cable.
7. Attach the top of the casing to the hook mount on the back cover, and when secured, then to the lower screw holes!
8. Fix the casing to the bracket using the 2 screws on the bottom.

Replacing a Predor terminal in the software

The terminal in the software must also be replaced with the new one. To do this in the software, navigate to the **Attendance→Worktime terminals** menu and follow the steps below:

1. Select the terminal to be replaced from the list!
2. Click on the *other actions* button at the bottom to see more options, from here select “Replace terminal”

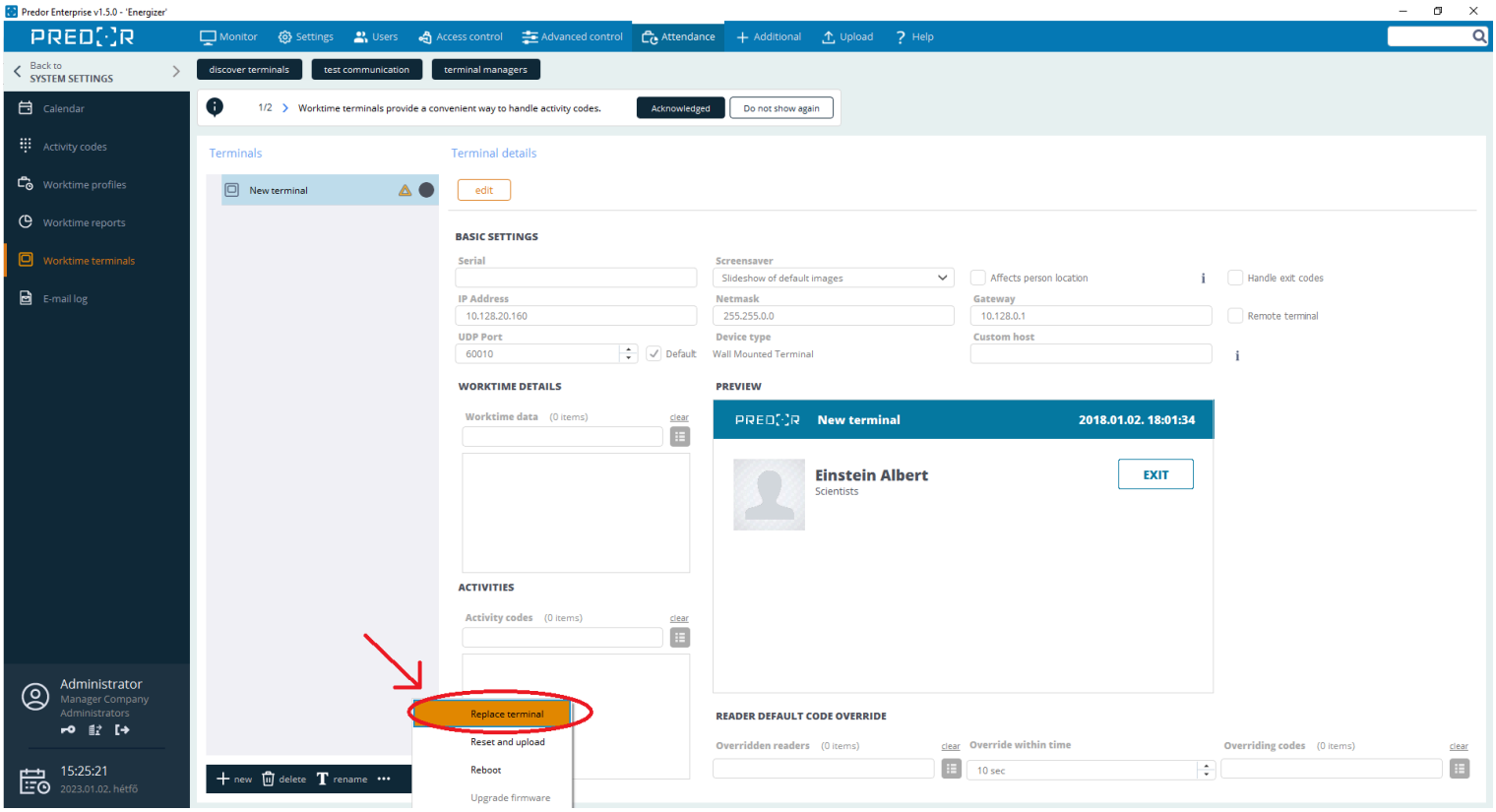


Figure 240: Terminal replacement option in Predor software

3. The new terminals detected on the network are automatically displayed in the pop-up window. Select the new terminal and click on *Replace* button.

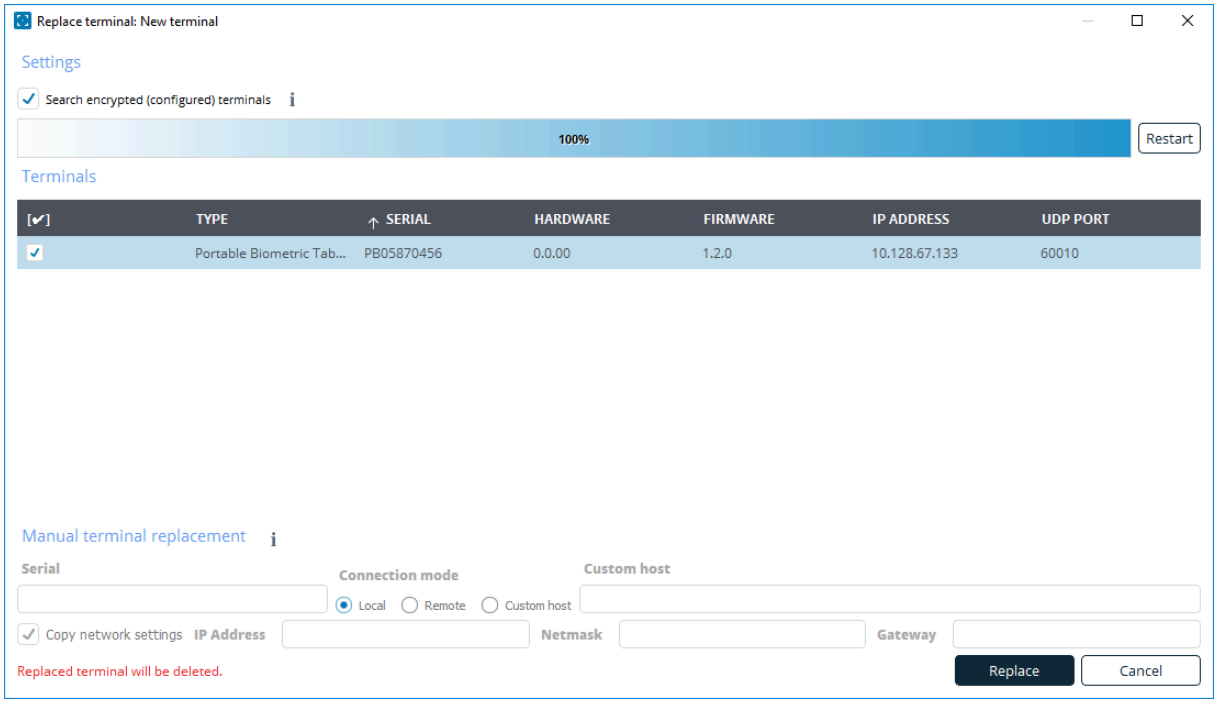


Figure 241: Selecting a new terminal from the list

4. The newly added terminal may need a firmware update. This is indicated by a small yellow triangle next to the terminal in the list:

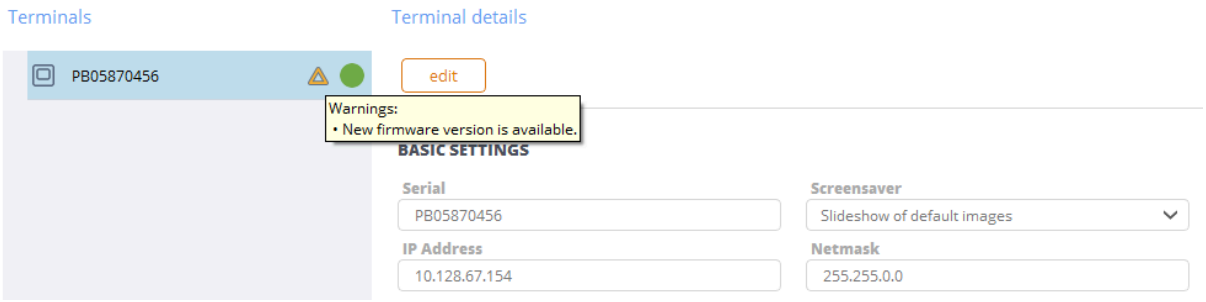


Figure 242: Terminal needing a firmware update

5. The firmware update can be accessed by clicking on the *other actions* ••• button, similar to the terminal replacement. If necessary, update the firmware, because until then (for compatibility reasons) the software will not allow you to upload any settings to the device!
6. The status of the firmware update can be found in the information bar on the left. Please wait patiently until the update is completed!

Troubleshooting

After replacing the terminal, it may not be able to communicate properly with the server. The following error message may be displayed:

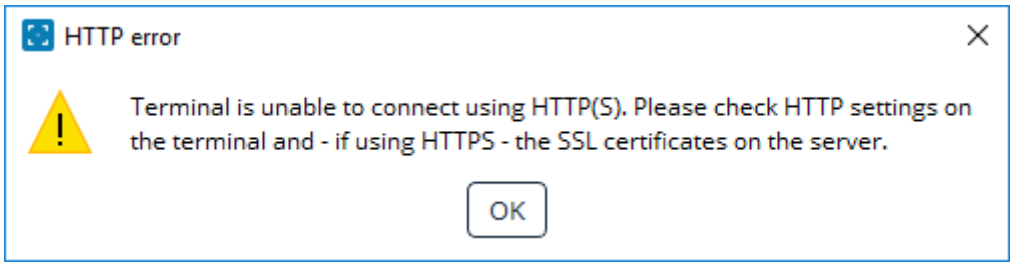


Figure 243: Terminal HTTP(S) error

In this case, you should check the terminal's communication settings, or try to restart it. Both operations require access to the terminal's internal menu, which can be accessed by repeatedly tapping the PREDOR logo at the top left of the terminal's home screen. In the window that appears, enter the *controller password* specified in the software's **Settings→System Settings** menu.

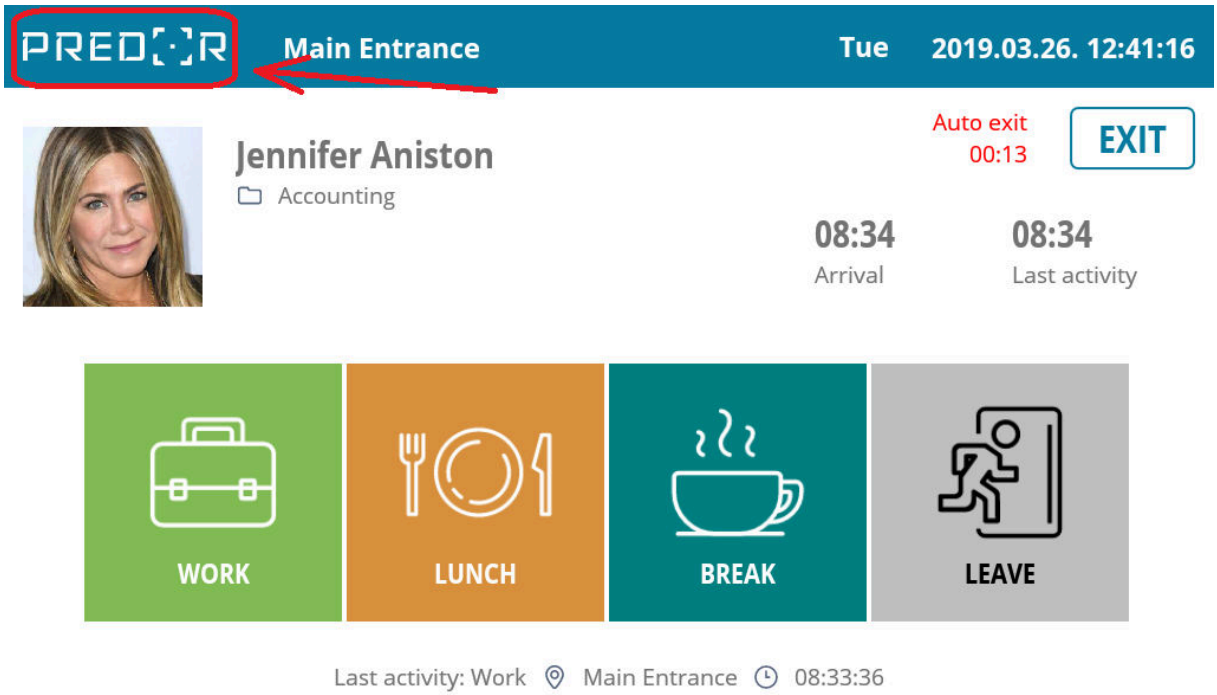


Figure 244: The terminal menu can be accessed by repeatedly tapping the Predor logo

Here we check the server communication parameters, especially the server protocol! If you are not sure about the correct parameter, change the "Automatically select protocol" option to "For the first time".

In the service menu you have the possibility to restart the terminal. Avoid using the shutdown option, because the device can only be switched on again after a complete power cut (remove batteries!).

To exit the menu, use the ← arrow at the top left.

22 APPENDIX F: PREDOR BIOMETRIC TERMINAL DESCRIPTION

Introduction

The Predor biometric work time terminal is a mobile data acquisition device for the Predor Enterprise Access Control and Time & Attendance System. It enables accurate registration of work time related activities where no network infrastructure is available.

The work time terminal stores the registered activities in its internal memory until network connectivity is available, and then it automatically synchronizes them with the Predor server.

WARNING: The terminal requires a SIM card with 4G LTE (PIN disabled, configured as remote terminal), or 2.4GHz Wi-Fi (IEEE 802.11b/g/n) Access Point for network connection.

WARNING: The Predor biometric mobile terminal is only available for the Predor Enterprise edition and requires the Time & Attendance module!

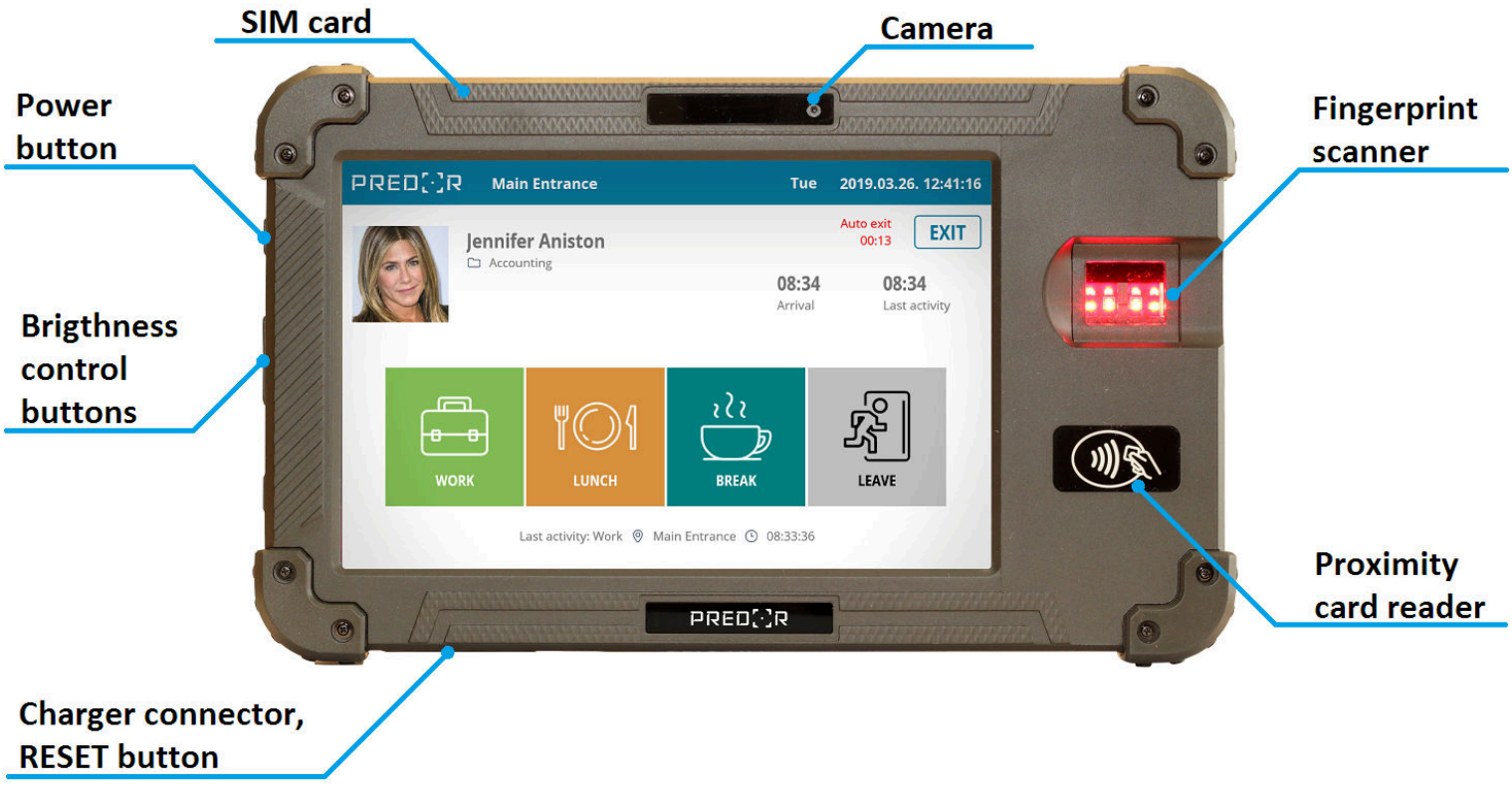


Figure 245: Predor biometric mobile terminal

- **SIM Card:** for SIM card (PIN disabled) with mobile data (4G LTE) connection.
- **Power button:** long press (3 seconds) switches the device on or off, short press activates or deactivates the screen.
- **Brightness control buttons:** manual control for the display's brightness level.
- **Charging connector, RESET button:** barrel jack, or micro-USB charging connector, 5V/2A. The RESET button is advised to be used only if the terminal does not respond to any interaction.
- **Fingerprint scanner:** Suprema optical fingerprint sensor.
- **Proximity Card reader:** 13,56MHz proximity card reader (NFC NTAG, Mifare Classic, Mifare DESFire, ISO14443-A/B compatible identifiers).

PHYSICAL PARAMETERS

Dimensions: 262x160x30mm
Display: ..... 8" touch screen, 1280x800 resolution
Case: ..... Plastic

INTEGRATED DEVICES

Proximity Card reader: ..... ISO14443 Type A/B, Mifare, ISO18092
Fingerprint scanner: ..... Suprema optical sensor (ANSI 378, ISO/IEC 19794)
Front camera: ..... 2 Megapixel, fix focus
Other: ..... GPS

ENVIRONMENTAL PARAMETERS

Operating temperature: ..... -5-45°C
Operating humidity: 10-90%
Storage temperature: ..... -25-60°C
Storage humidity: 10-90%

ELECTRICAL CHARACTERISTICS

Power supply: ..... 5V DC / 2A
Battery: ..... internal, non-replaceable Li-Ion (8540mAh, 3.8V)
Network connection: ..... 2.4GHz Wi-Fi / 4G LTE

Important Notes

Please read the following carefully before proceeding and using the appliance:

- **Use the device only in appropriate environmental conditions stated in the datasheet.**
- **Never place the terminal near fire or excessive heat source.**
- **Do not submerge or place the device near splashing water. Do not use the terminal in rain.**
- **Use only the original or equivalent micro USB charger.**
- **Do not use two chargers (barrel jack and micro USB connector) simultaneously. Connect only one type of charger at a time.**
- **Do not use the charging cable if its insulation is damaged or broken. In this case change the charger or the cable.**

Deep-discharge mode

The terminal is equipped with a special deep-discharge mode which helps maintaining a longer lifetime of the internal battery. This mode prevents the device to switch on until the battery reaches a certain charge threshold.

If the terminal is fully discharged and/or was not in use for an extended period, it is possible that it needs to be charged for a long time before it can be switched on. If this happens charge the device for 10-15 minutes then try switching it on. If it still does not start then try pushing the RESET button for 3 seconds with a small but not sharp tool, then try again.

First steps

Before using the terminal it is advised to connect it to the charger unit. If the device is switched off, a pictogram of a charging battery should show up on the screen. If nothing happens upon connecting the charger, please check if the connections are correct and the charging cable is not damaged. It is also possible that the device is in the *deep-discharge mode* as mentioned before in the **Important Notes** section.

Switch on the device by pressing the power button for 3 seconds. If the terminal has been switched on successfully the screen displays the **android** logo and starts to boot in the background. Please be patient while the system starts, as it can take a few minutes. If the terminal started successfully the homescreen appears on the screen.

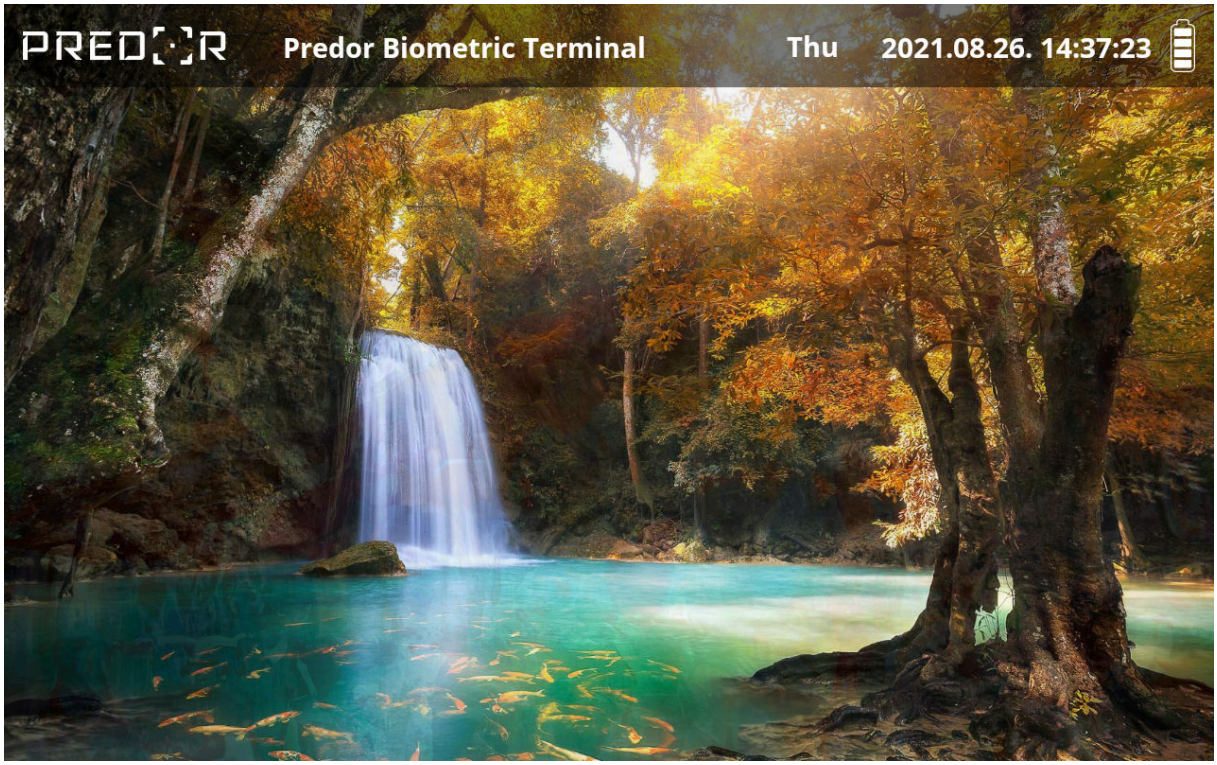


Figure 246: Predor terminal home screen

The terminal has a settings menu which is accessible by tapping the **Predor** logo on the top left of the screen multiple times. The menu is protected by a password which is the same as the *controller password* set in the Predor Client software. As the terminal is not attached to any system yet, there is no password, just tap the *OK* button.

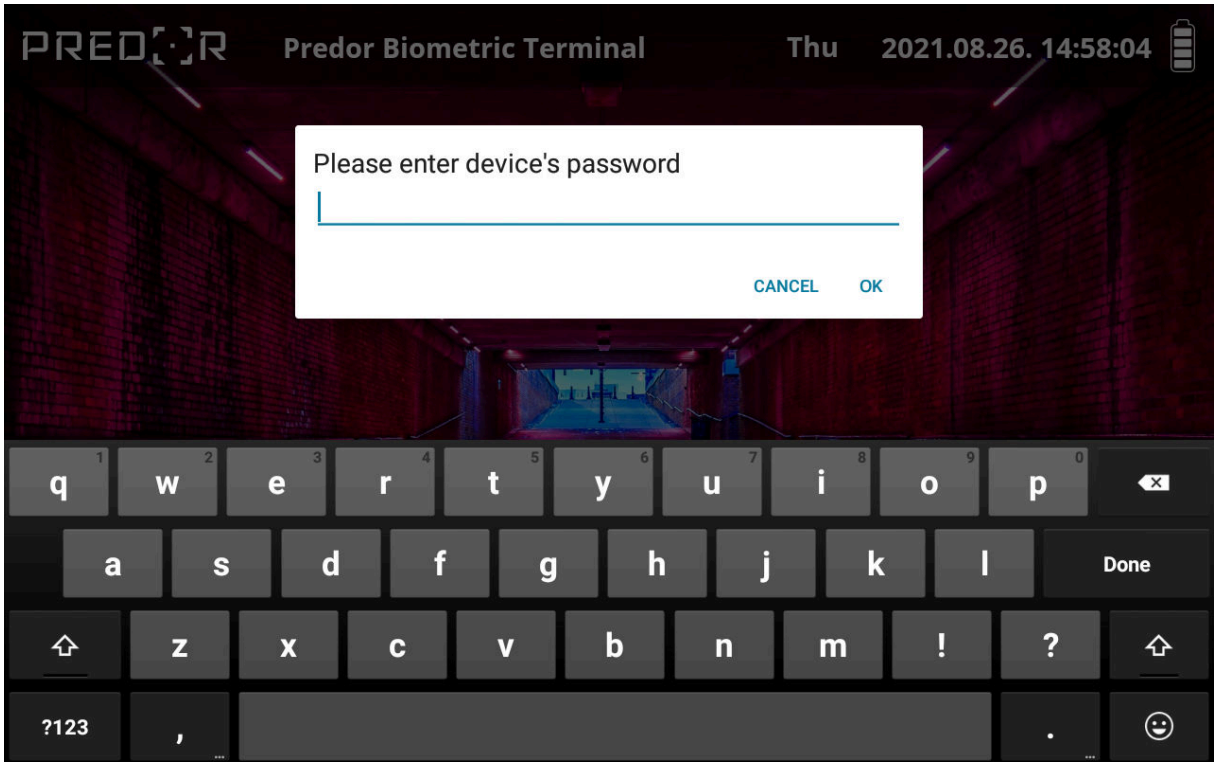


Figure 247: Accessing the Predor terminal's menu requires a password

Predor terminal menu map

The following settings and options are available in the menu:

- *General*
  - **Terminal name:** displays the terminal's current name, it is only editable in the Predor Client software.
  - **Automatically logout user:** timeout after a successful identification after which the terminal returns to the home screen.
  - **Timezone:** displays the current time zone.
  - **Locale:** changes the terminal's display language.
  - **Idle screen setup:** sets how the home screen behaves: displays a static Predor logo or stock photos.
  - **Card number length:** sets the card number format used by the terminal. It is advised that this value is aligned to the other terminal(s)/card readers already used in the system.
  - **Automatically enter sleep mode:** sets the amount of idle time after the screen automatically switches off

- **Prevent sleep mode when charging:** sets whether if automatic sleep mode is ignored while charging
- **Skip activity code approval:** can be set to register activities without validation

- *Network interface*
  - **Communication mode:**
    * **Local Predor Enterprise:** this mode should be chosen only if the terminal is only ever connected to one wireless network which is the same as the server's.
    * **Remote Predor Enterprise:** this mode is used if the terminal will be connected to various wireless networks so it can synchronize over the internet. The server must have a dynDNS or fixed IP address for this mode to operate correctly. Also the appropriate ports must be forwarded through firewalls and routers.
  - **IP address, netmask, Gateway address:** in Remote mode these are displayed for information purposes only. In Local mode these settings show the actual values and the settings tagged with *preferred* are editable. The terminal tries to apply the preferred values upon exiting from the menu.
  - **UDP port:** In case of Local mode this value sets the UDP port on which the terminal listens for incoming connections. Port given here has to be set for this terminal in the Predor Client application.
  - **MAC address:** for information purposes only, never editable.
  - **Wi-Fi settings:** this menu shows the currently connected network. Upon tapping this option the available networks list appears. If a not known network is chosen the terminal tries to connect to it, in case of an already known network there is an option to forget it.
  - **Wi-Fi:** enables or disables the wireless radio device.
- *Server communication:* Details for the Predor server communication has to be set here. Available options depend on the server communication mode (local/remote) chosen before.
  - **Server protocol:** set the HTTP protocol used by the server. (default: HTTP)
  - **Server IP address / Server host:** set the Predor server's IP address or DNS name.
  - **Server UDP port (local mode only):** set the port given in the Predor Client settings menu for the terminals. (default: 60012)
  - **Server HTTP port:** set the Predor server's HTTP port. (default: 8888)

- **Automatically select protocol (local mode only):** The terminal can try to detect the server's HTTP mode. It is advised to set this option to "For the first time", thus the terminal determines the correct option now and remembers it.
- **Login (remote mode only):** This button is used to register the device to the server in remote mode. The registration procedure is detailed in a subsequent section.
- **Server status:** gives feedback whether a Predor server is accessible with the given settings.
- **XTEA key:** currently used cipher password - displayed only for debugging purposes.
- **AUTH token:** currently used authorization token for the server - displayed only for debugging purposes.

- *Fingerprint*
  - **Fingerprint management:** A special menu for managing fingerprints for the users. Details of this option are in the Fingerprint management section.
  - **Fingerprint security level:** the fingerprint scanner's acceptance level when comparing fingerprints to already known ones can be adjusted here. At the least accurate level it is more probable that a false acceptance occurs, however at the most accurate level the fingerprint scan have to be excellent quality otherwise false denies can occur. It is advised that this setting is left at factory default level and only adjust it when needed (in case of poor recognition lower the level, in case of false acceptances raise the level).
  - **Fingerprint quality acceptance:** the scanned fingerprints' quality limit can be adjusted here. Quality depends on the finger's position, cleanness of the finger and scanner the finger's displacement during scanning among others. The system does not start evaluating fingerprints below the required quality level. Better scan quality is more difficult to achieve but it reduces the probability of false acceptance. It is advised that this setting is left at factory default level and only adjust it when needed (in case of poor recognition lower the level, in case of false acceptances raise the level).
- *Service*
  - **Display card numbers:** displays the detected card number on the screen. Use it only for debugging.
  - **Reboot device:** restarts the device.
  - **Shutdown device:** switches off the terminal. To switch back on press the power button for 3 seconds.

- **Wipe data:** deletes all setting and data from the device including IP, server and Wi-Fi settings and passwords, **stored and not yet synchronized events** and offline stored data (users, card numbers and fingerprint templates).
- **Firmware update:** tries to download the most recent software version from the Predor server and upgrades to it.
- **Time synchronisation:** starts an immediate time synchronisation for this terminal.

- *About:* displays basic information about this terminal, including the serial number.

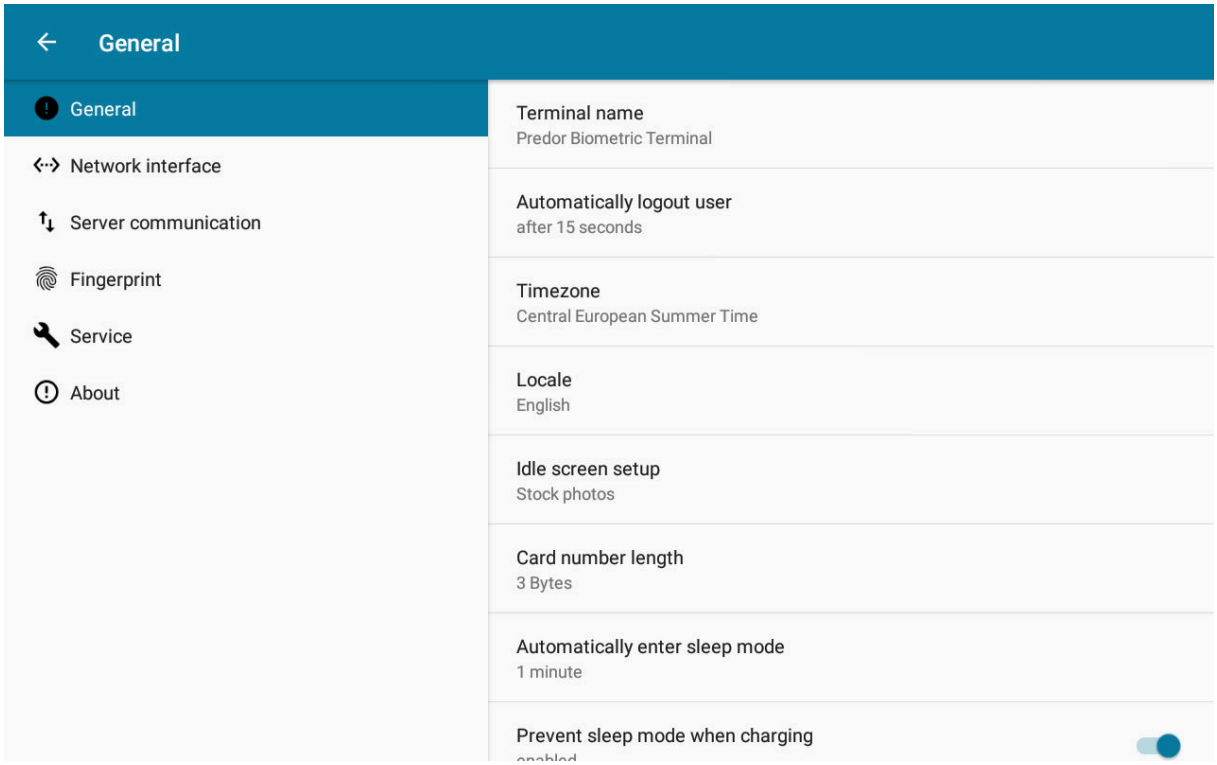


Figure 248: Menu of the biometric mobile work time terminal

Adding the terminal to the Predor Enterprise software

Before the terminal can be used it must be added to Predor Server. First, connect the terminal to the appropriate Wi-Fi network which can be done via the terminal's menu. Select the **Network interface** submenu and the **Wi-Fi settings** option. The following steps depends on which server communication mode has been chosen:

- **Local Predor Enterprise mode:** This mode should be chosen only if the terminal is only ever connected to one wireless network which is the same as the server's.

  In this case in the Predor Client Application navigate to the **Attendance** menu and **Worktime terminals** submenu then click on the "discover terminals" button. Choose the new terminal(s) and click the OK button to them to the system.

Initialisation of the terminal is commencing and after a few seconds the terminal is operational.

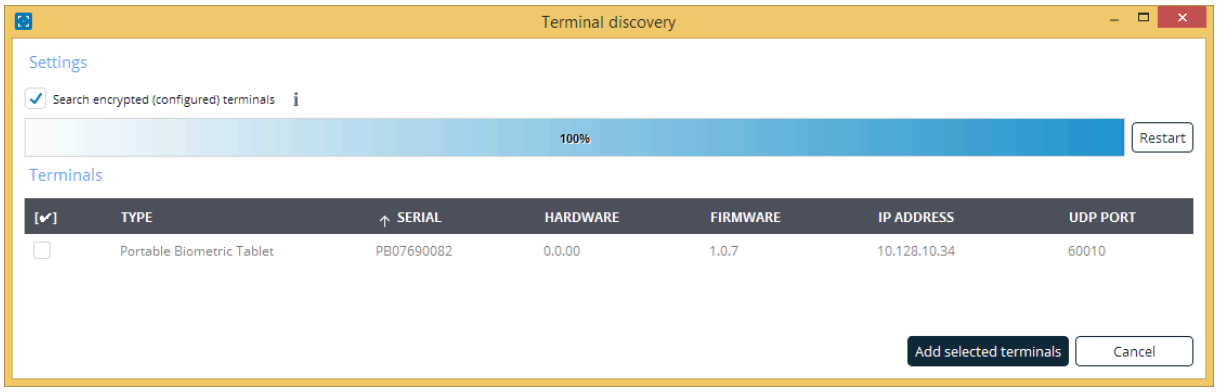


Figure 249: Adding new terminal in Local Enterprise mode via terminal discovery menu

- **Remote Predor Enterprise mode:** This mode is recommended if the server is accessible by a fixed IP or DNS address so the terminal will be able synchronize over the internet via various Wi-Fi access points.

  The first step in this mode is to manually add the terminal to the Predor system in the Predor Client application's **Attendance** menu and **Worktime terminals** submenu. Click on the **+ new** button in the lower left to add a new terminal.

  The new terminal appears in the list.

  Give a custom name for this terminal - it will be visible on the device's screen too.

  Click on the *edit* button to fill in the details: type in the terminal's serial number which can be found on the backside label or in the terminal's menu under the **About** submenu.

  Tick the **Remote terminal** option.

  Adjust the remaining options as needed.

  Check if the given serial number is correct then click on the save button. Adding the terminal to the system is now finished from the server's side, but the terminal still has to log in to be usable.

  Enter the terminal's menu. Check if the "Remote Predor Enterprise" option is selected as the *Communication mode* in the **Network interface** menu.

  In the **Server communication** menu select the appropriate *Server protocol* and type the server's address into the *Server host* field. Type the appropriate HTTP port into the *Server HTTP port* field. If the server is accessible and all parameters are correct, the *Server status* should show "Reachable".

  Press the *Login* button and type in the *controller password*.

WARNING: If no password was set in the Predor system previously, then the terminal cannot be initialised. Please set a new custom password via the Predor Client application in the **Settings** menu **System settings** submenu and click on the **controller password** button.

If the login has succeeded the terminal displays the following message: “Logging in was successful, the device is now initialized.”

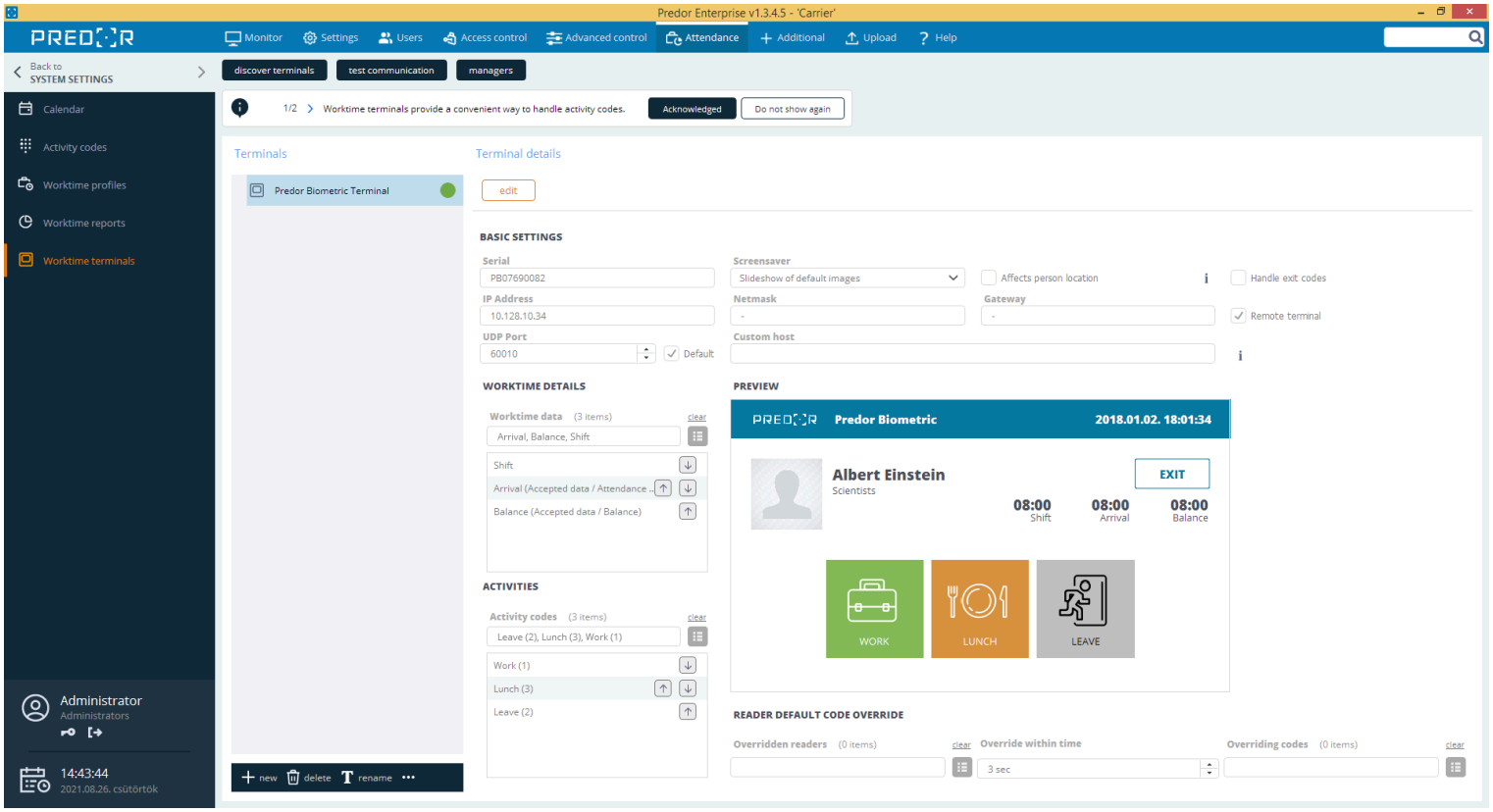


Figure 250: Biometric terminal added to the system in remote mode

General usage

Once the work time terminal has been successfully added to the Predor server synchronization of work time data happens automatically in the background. In case of remote mode synchronization may happen a bit slower, changes made in the Client application can be delayed by up to 10 seconds.

In factory default settings the sleep mode is disabled thus the screen and fingerprint scanner stays active continuously. This mode drain the battery fast so it is advised to turn on and off the screen manually when needed or connect the device to the charger permanently in case of a kiosk-like installation. The screen can be switched on and off by pressing the power button for a short time.



CAUTION: While the screen is turned off the terminal enters a standby mode and disables the internal card reader and fingerprint scanner. To use these peripherals the screen must be turned back on first.

Adding a new user

New users can only be added from the Predor Client software in the *Users* menu and **Users and departments** submenu.

If proximity card authentication is needed cards or badges can be added to the system using any card readers connected to Predor Access Control units or with a USB card reader. If none of them are available in the system – only biometric terminal(s) – then the easiest way is to just swipe the card on the work time terminal which generates an unknown card event in the Predor Client application in the *Monitor* menu. Right click on the event and choose “Copy card number to clipboard” then create the new user select to add card manually and paste the card number.

If fingerprint authentication is needed fingerprints can only be added by using the terminal’s internal menu. Procedure of adding fingerprints are detailed in the Fingerprint management section.

Registering an activity

To register an activity one must authenticate themselves first by either by using fingerprint or card authentication then select an activity from the displayed list. After confirming the selection the terminal sends it immediately to the server if there is an active network connection.

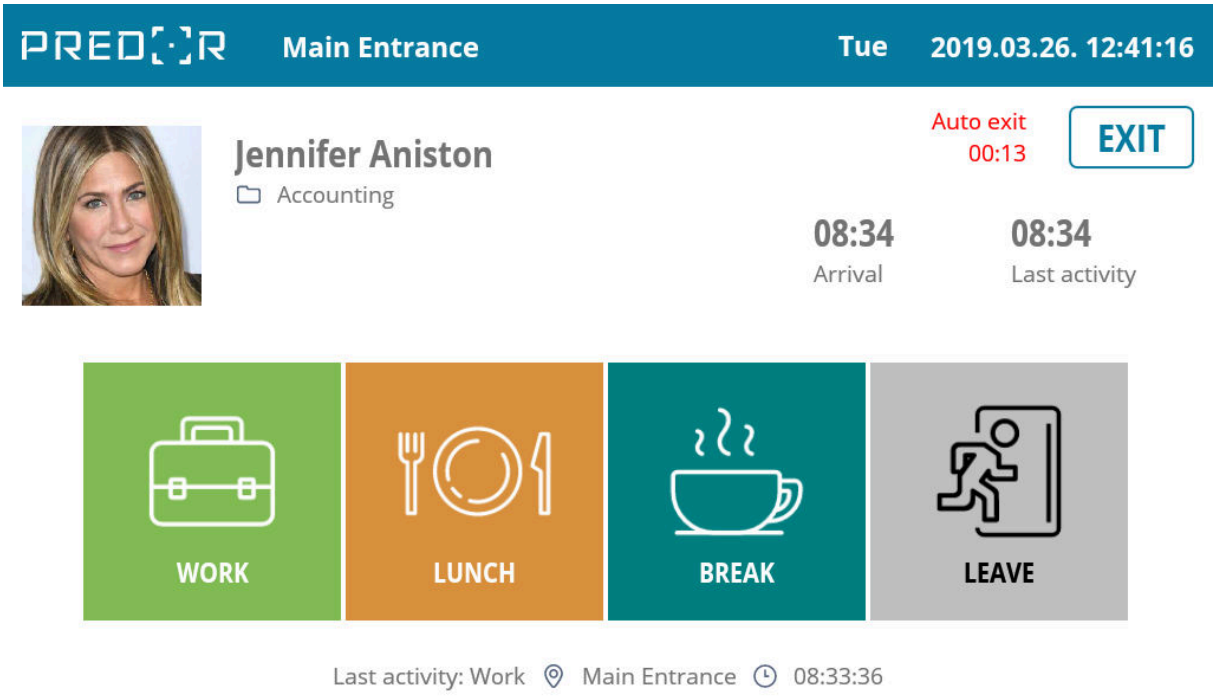


Figure 251: Registering an activity on the biometric work time terminal

Registering an activity for groups

The same activity can be registered quickly for a group of users using *Continuous login*. Continuous login can only be initiated by a *device manager*. Device managers are special users: they can manage fingerprints and use continuous login. Managers are selected from already existing users in the Predor Client software in the **Attendance** menu and **Worktime terminals** submenu by using the *managers* button.

TO initiate a continuous login the *manager* must authenticate themselves first, then select the appropriate activity then tap the *Continuous* button. A new login screen opens where users can authenticate themselves without any time limit one after another. The authentication was successful if the user has appeared in the list. Activities registered this way are also synchronized realtime if there is an available network connection. By tapping the *Done* button the continuous login session ends and the terminal returns to the home screen.

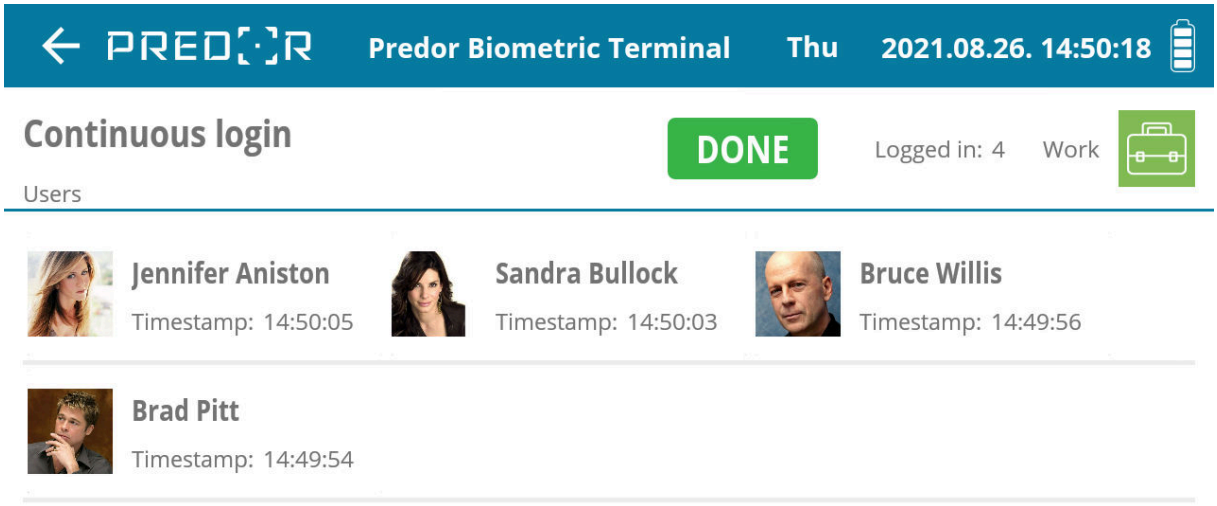


Figure 252: Continuous login with list of already registered users

WARNING: The continuous login mode does not automatically include the manager. If the manager would also like to register this activity for themselves they should authenticate again while in continuous login mode.

Fingerprint management

Managing fingerprints is done on the work time terminal inside a special menu which is accessible by either of these ways:

- After authenticating as a device manager tap the **users** button next to the photo
- Enter the terminal's menu and select the **Fingerprint** submenu and the **Fingerprint management** option

Both method lead to the same fingerprint management menu where the current users of the system are listed.

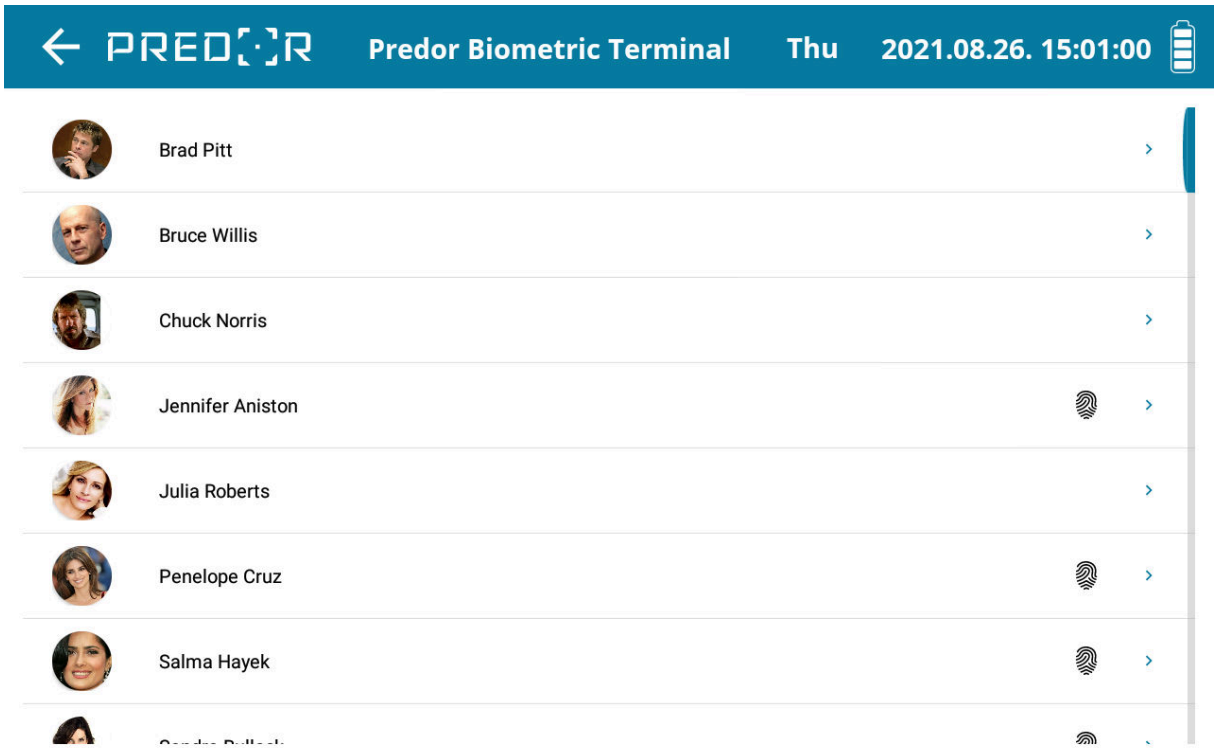


Figure 253: Fingerprint management menu on the biometric terminal

Users with already registered fingerprints are displyed along with a fingerprint symbol. To manage a user's fingerprints select the user which opens a new interface.

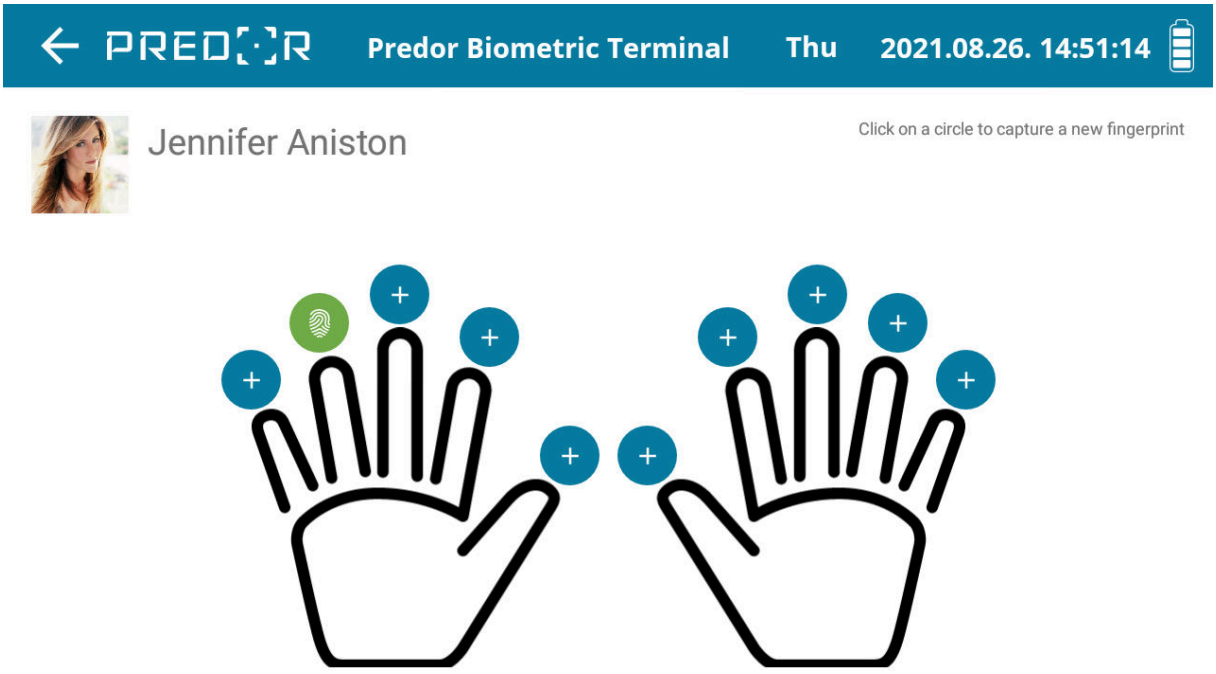


Figure 254: Registered fingerprints for a user. This menu serves as the interface to add or remove fingerprints for this user.

Registered fingerprints for this user are displayed on the screen.

To add a new fingerprint select the **+** button next to the chosen finger and place your finger onto the sensor. Status messages on the upper right corner show the state of the capture process. If the captured fingerprint quality is poor please try again. Successful captures are confirmed by the "Fingerprint saved successfully!" status message and a fingerprint symbol replaces the **+** sign.

TIP: Good quality fingerprints are achieved by placing the fingertip firmly and flat on the sensor and holding it there for about a second without moving.

TIP: When authenticating with fingerprints they must be scanned in +/-90° angle relative to the originally registered fingerprints, otherwise the authentication fails, thus it is recommended that the fingerprints are registered in a way which results in a comfortable posture during normal use.

Tapping on an already registered fingerprint there is an option to delete or replace it with a new scan.



WARNING: Deleting a fingerprint from a biometric work time terminal affects all other terminals and also the server. The fingerprint will be deleted from every device because of the background task which synchronizes data across every device in the Predor system.



CAUTION: Fingerprint management is only available in online mode, that is registering and deleting fingerprints are possible only while the device can actively communicate to the server.

Tap the ← arrow on the upper left to return to the user list and once again to return to the home screen.

Security

Security is of utmost importance when handling biometric or other sensitive personal data as they are capable of identifying individuals and are not replaceable. Some important notes about handling biometric data in the Predor system:

- Biometric data are stored in the database of the Predor server, thus it is very important that both the database and the Predor server have adequate protection against penetration attempts both physically and by software.
- During synchronization with the biometric terminals sensitive data are transferred via the network, or in remote mode even on the internet, thus it is **highly recommended to use SSL certificates for the Predor server**. By using SSL certificates the communication between the terminal and server becomes encrypted, which highly reduces the probability for a malicious attacker to capture or interpret sensitive data.
- Biometric data are also stored inside the biometric work time terminals offline, and although these are not accessible via the network but with physical access to the device they may be extracted.
- Deleting fingerprints are immediately and irreversibly deletes them from the server and currently online devices. Offline devices delete them when the first synchronization with the server happens.

The system uses and stores only some characteristic properties of the fingerprints from which the original fingerprint cannot be reconstructed.



WARNING: Inside the European Economic Area (EEA) the General Data Protection Regulation (GDPR) specifies that usage and storage of biometric identification is limited to special cases and conditions. **Please inform about legal conditions and legitimate usage of the particular use case before using biometric identification.**

Troubleshooting

Phenomenon	Caused by	Solution
The terminal is not switching on.	The battery is discharged.	Connect the terminal to the charger, wait a few minutes then try to turn on device. If it is still not turning on, try to press the RESET button near the charger connector and try to switch it on again.
The terminal is not visible by discovery.	There is a firewall operating on the computer or the network.	Turn off the firewall or check its settings.
	The terminal is not connected to the right Wi-Fi access point.	Check whether the terminal is connected to an access point which is on the same network as the server.
	The terminal uses a different controller password.	Reset the terminal to the factory default settings. Enter the terminal's menu then select the **Service** menu and choose the **Wipe data** option. Connect the terminal again to the Wi-Fi network and try discovering again.
The fingerprint scanner is not lit.	The terminal is turned off.	Check if the terminal is operational and the display shows the home screen.
	The terminal is in standby mode or some software error has occurred.	Turn on the display by pressing the *Power button* for a short period of time, or try to restart the terminal.

Table 13: Typical errors and solutions

23 APPENDIX G: HIKVISION LICENSE PLATE RECOGNISER CONFIGURATION FOR PREDOR ENTERPRISE SYSTEM

From the Hikvision ANPR (Automatic number-plate recognition) or LPR (License Plate Recognition) cameras, the H7 (iDS) and the H8 (iDS) series cameras are already available with built-in ability to transmit the recognized license plate number to a preset address, which in this case is the Predor software. *(For example: iDS-2CD7A46G0/P-IZHS or iDS-2CD7A26G0/P-IZHS cameras.)*

Besides placing the camera in the right position (height, tilt angle) and configuring the detection range, the Predor server adress must be set and enabled to send the detected license plate numbers and other metadata. In the camera settings, the **Road traffic** option must be selected in the **VCA / VCA Resource** menu.

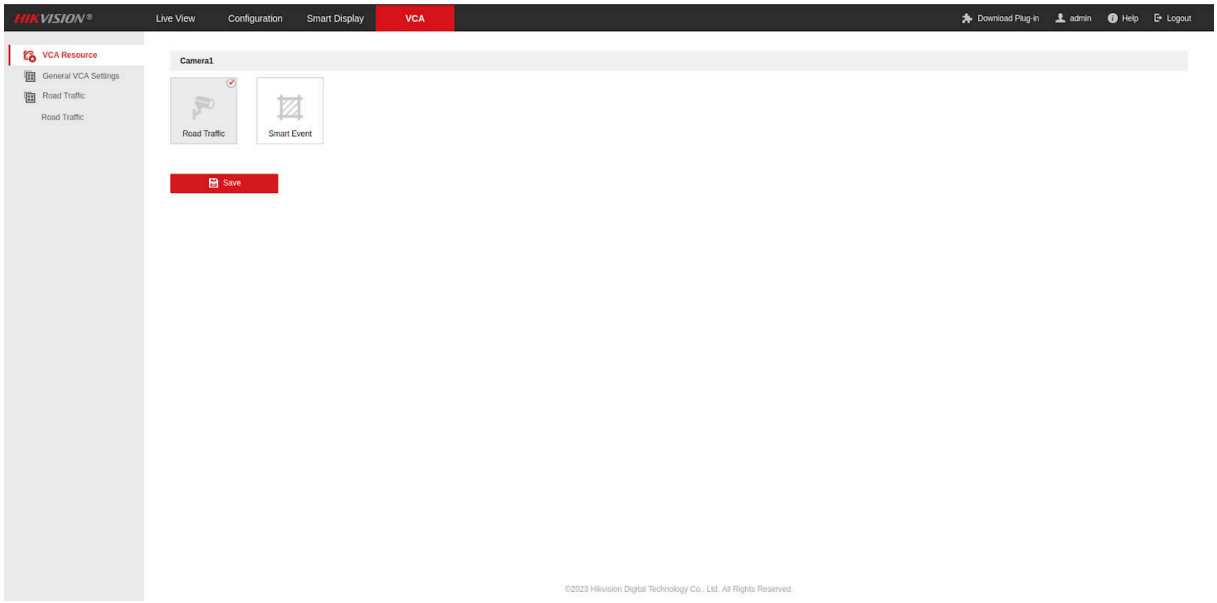


Figure 255: VCA resource configuration submenu on the Hikvision configuration interface

In the **VCA / Road traffic** submenu, vehicle detection must be enabled.

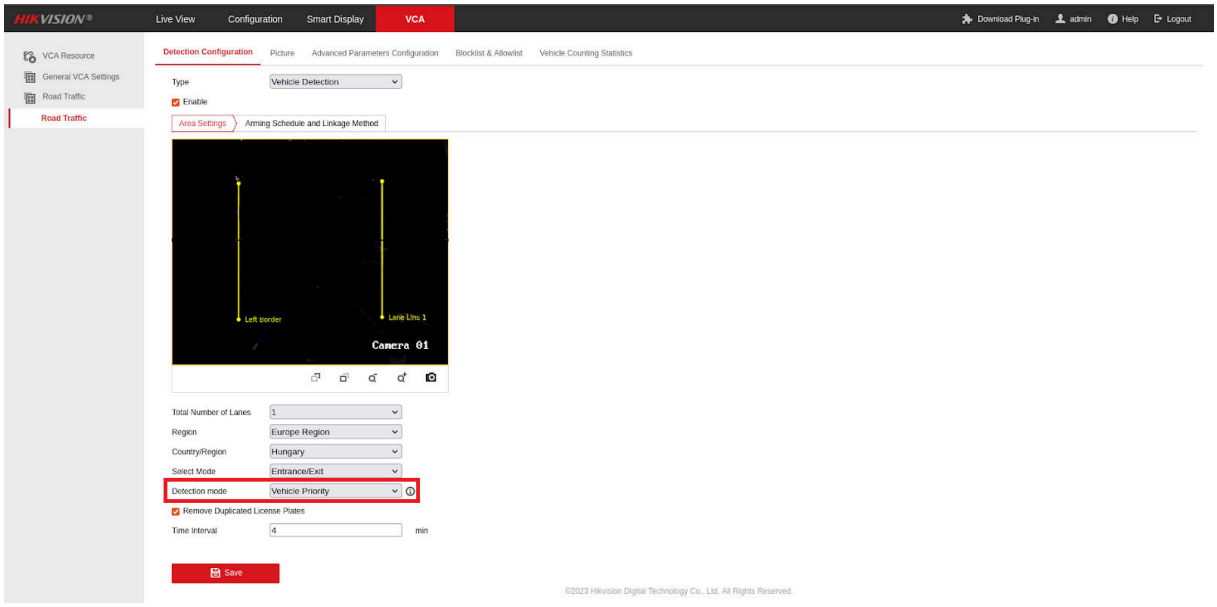


Figure 256: VCA vehicle detection setup on the Hikvision configuration interface

In the **Configuration / Advanced settings**, under the **Alert Server** tab, the availability of the Predor Enterprise server needs to be configured, which is the IP address of the server and a port. The port is an optional TCP port, which must also be specified in Predor software (on the picture, it is 12345).

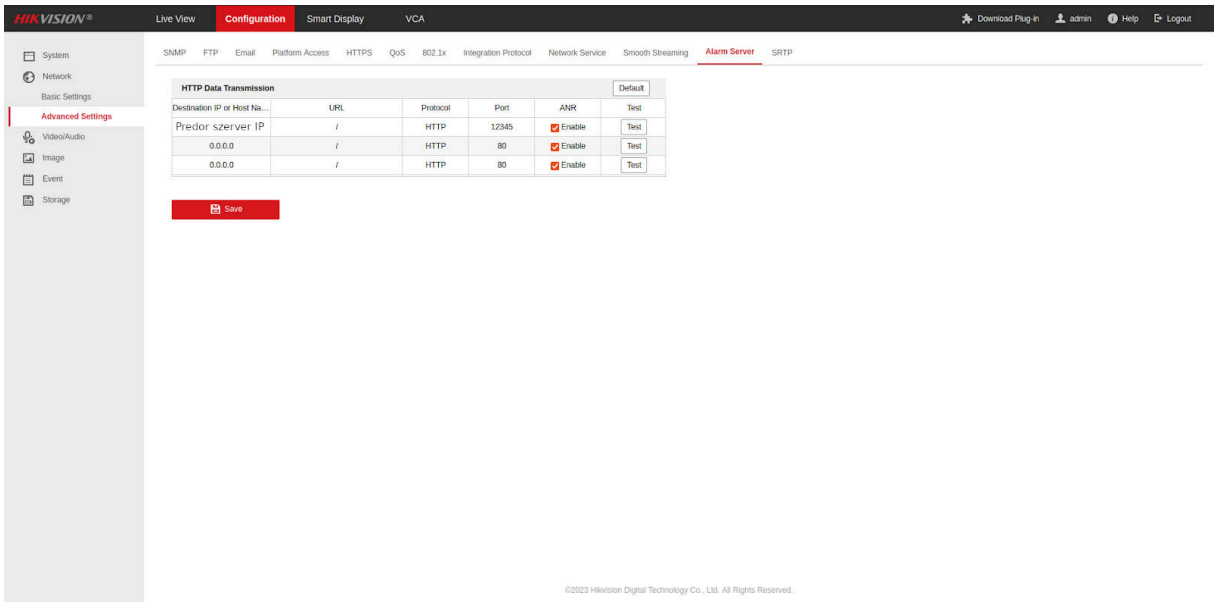


Figure 257: Predor server configuration on the Hikvision configuration interface

In the Predor client, in the Parking management submenu, click on the **hikvision settings** button on the top to enter the port on which the Predor software will receive the packets (12345 in the picture).

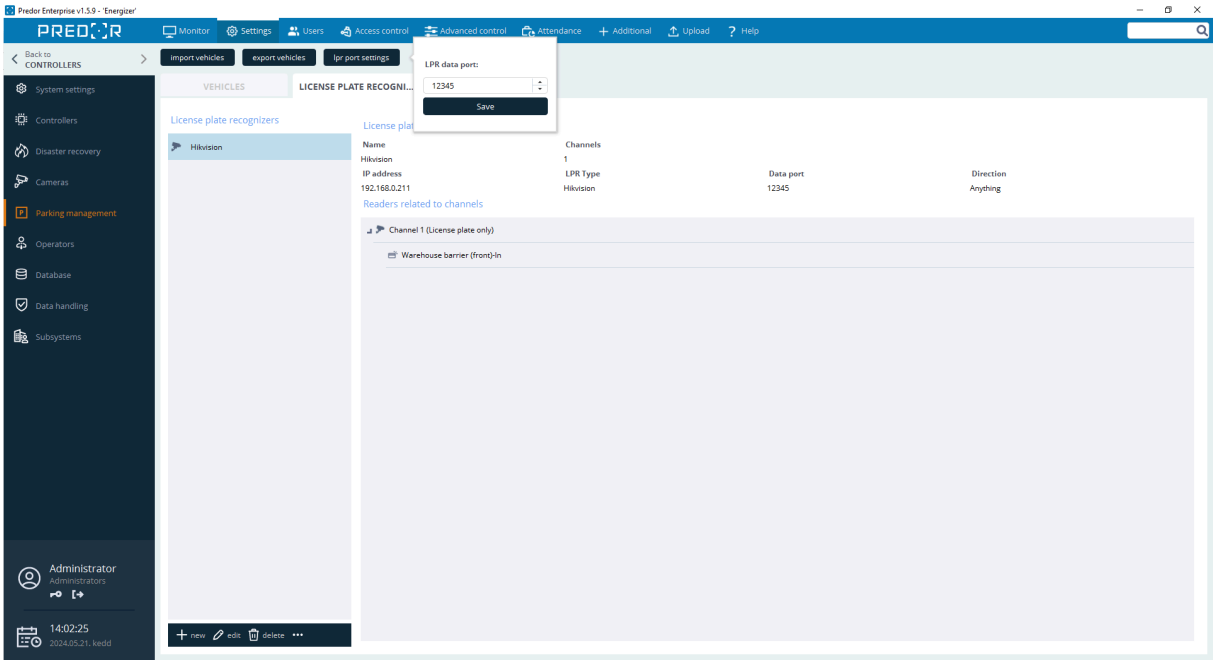


Figure 258: Enter Hikvision data port in Predor software

The configuration process of the license plate recognition is described in the License plate recognition chapter.

24 APPENDIX H: DAHUA LICENSE PLATE RECOGNISER CONFIGURATION FOR PREDOR ENTERPRISE SYSTEM

The Dahua ITC215-PW4I, ITC413-PW4D-IZ1, ITC413-PW4D-IZ3 cameras have built-in capability to forward the recognized license plate number to a preset address, which in this case is the Predor software.

Besides placing the camera in the correct position (height, tilt angle), the Predor server address must be configured and enabled to send the recognised license plate numbers and other metadata.

For older cameras, these settings can be made in the camera settings menu under **Network/ITCPUSH**. In the **Server IP** field, the IP address of the Predor server must be entered, and in the **Server Port** field, the port on which the camera forwards data to the Predor server. In the **Encode Mode** field, the UTF8 option must be selected. In the **Push Picture Config** section, the **Dig Picture** option must be selected to send the license plate image from the camera to the Predor server.

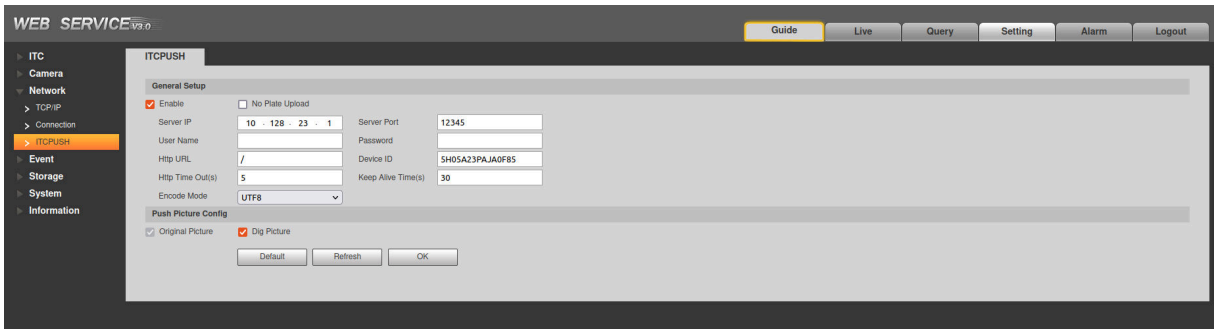


Figure 259: Configuration interface of older cameras



TIP: When using newer cameras, the camera needs a firmware update to work properly.

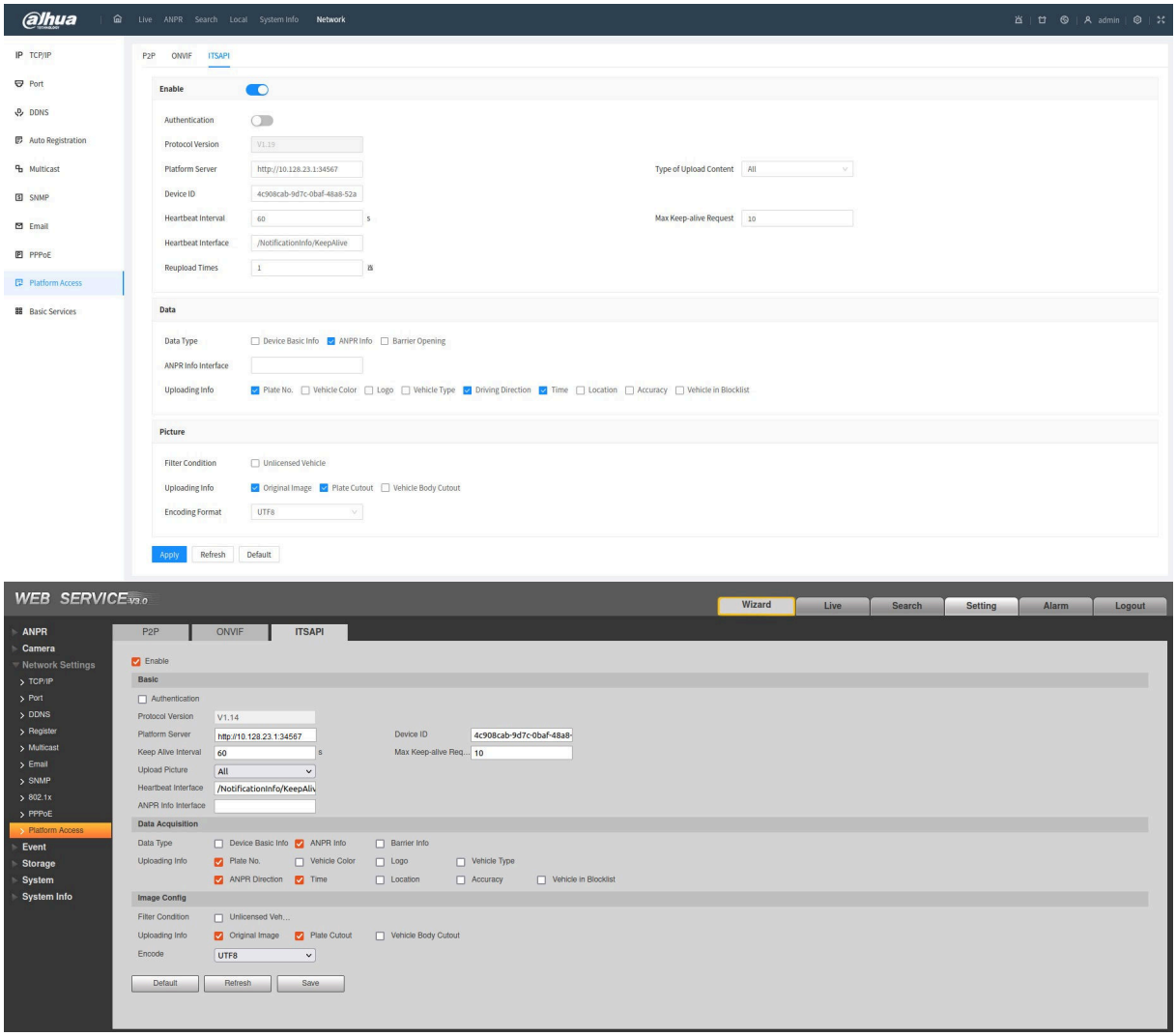


Figure 260: New camera setup interface with basic firmware version (top image) and updated firmware version (bottom image)

For newer cameras, these settings can be made under the ITSAPI tab in the camera settings menu under **Network Settings/Platform Access**. In the **Platform Server** field, you need to enter the full URL of the server, the connection type, server availability, and port (Sample: connection type://predor server IP:port). *Example: http://192.168.1.10:12345*

The value of **Reupload Time** should be set to 1, as it determines the amount of uploads. **(Setting Reupload Time to 0 will cause the camera to continuously start uploading data to the Predor server, which may cause event repetition)**

In the **Data Acquisition** section, the **ANPR Info**, **Plate No.** and **Time** data must be selected in order to forward the license plate number and the time of the recording to the Predor server.

If the license plate image needs to be saved, **Image Config** must be selected in the **Original Image** and **Plate Cutout** section.

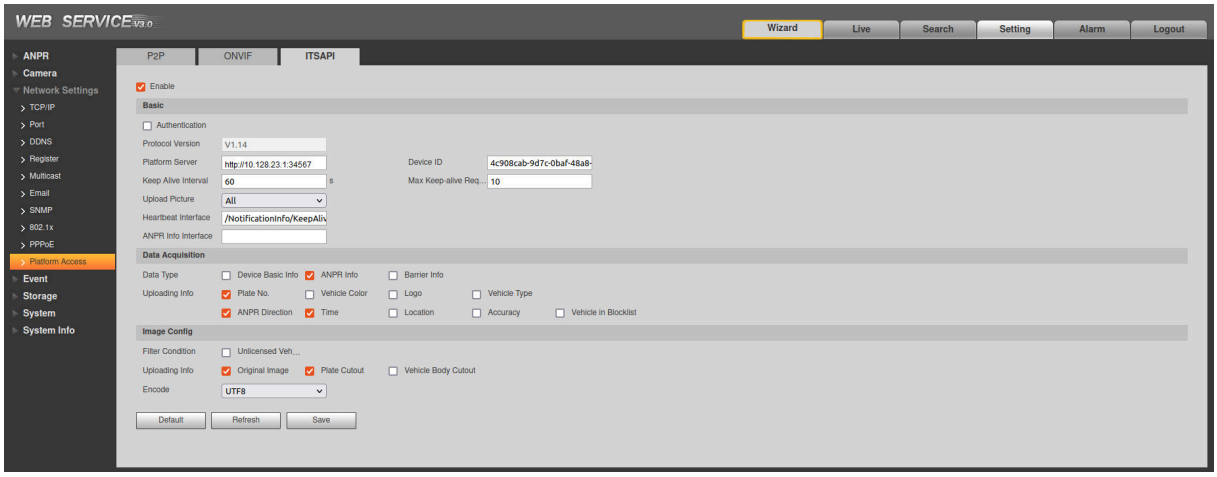


Figure 261: Newer camera's configuration interface, after firmware update

In the Predor client, in the Parking management submenu, click on the upper **lpr port settings** button and enter the port on which the Predor software will wait for the packets (12345 on the picture).

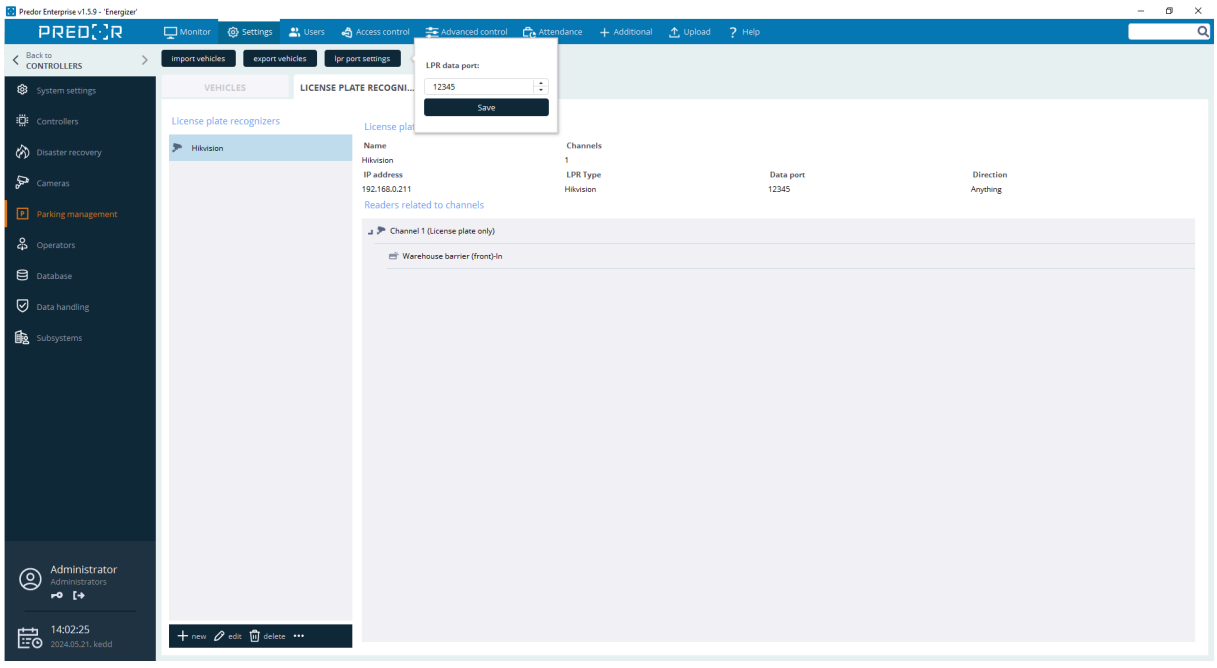


Figure 262: Specify LPR data port in Predor software

The configuration process of the license plate recognition is described in the License plate recognition chapter.

25 APPENDIX I: PREDOR OFFICE TERMINAL DESCRIPTION

Introduction

The Predor office work time terminal is a wall-mounted data acquisition device for the Predor Enterprise Access Control and Time & Attendance System and the Predor Cloud Time & Attendance System.

The work time terminal stores the registered activities in its internal memory until network connectivity is available, and then it automatically synchronizes them with the Predor server.

WARNING: The terminal requires a 2.4GHz or 5GHz Wi-Fi (IEEE 802.11b/g/n) Access Point or Ethernet for network connection.

WARNING: The Predor office terminal is only available for the Predor Cloud and the Predor Enterprise edition and requires the Time & Attendance module!

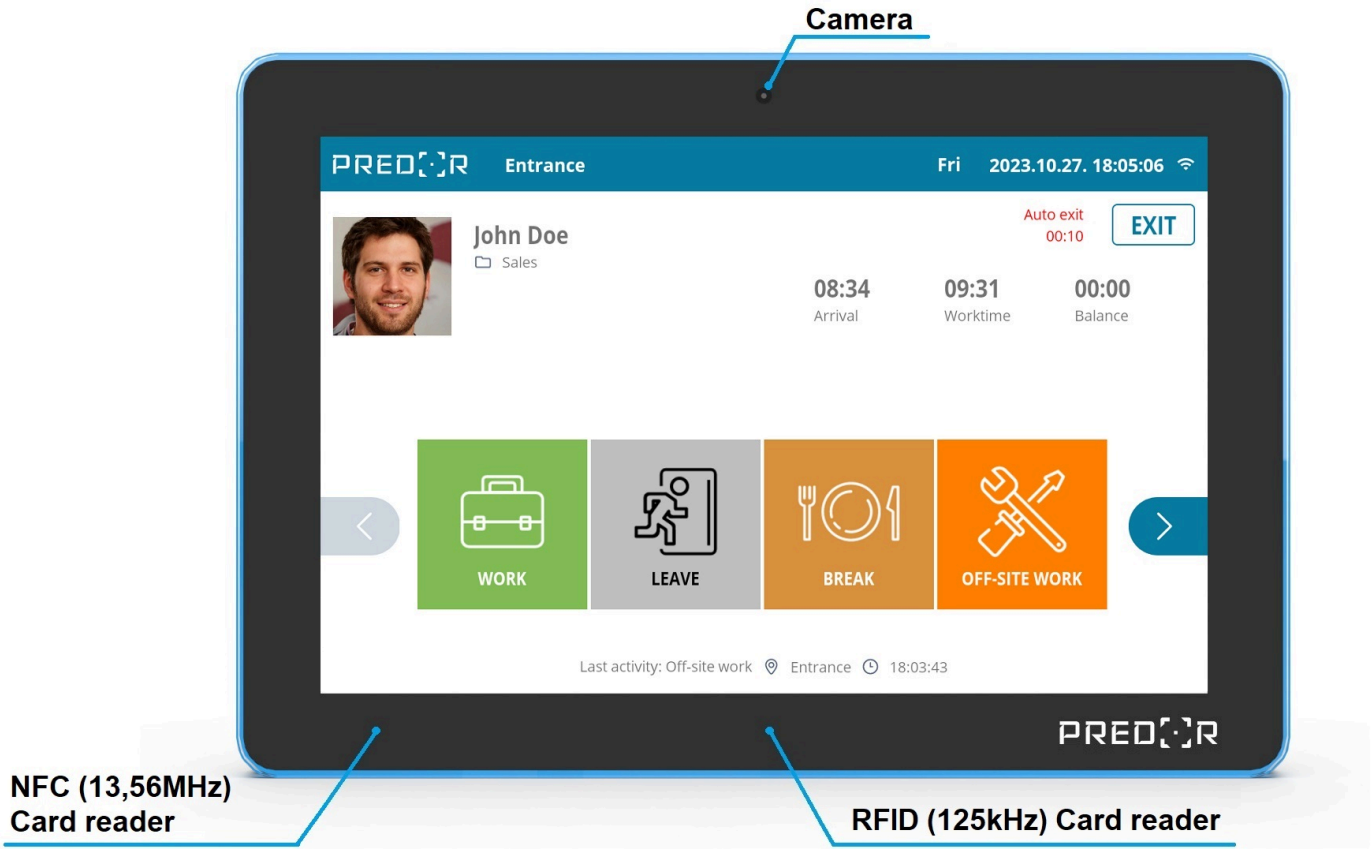


Figure 263: Predor office terminal front

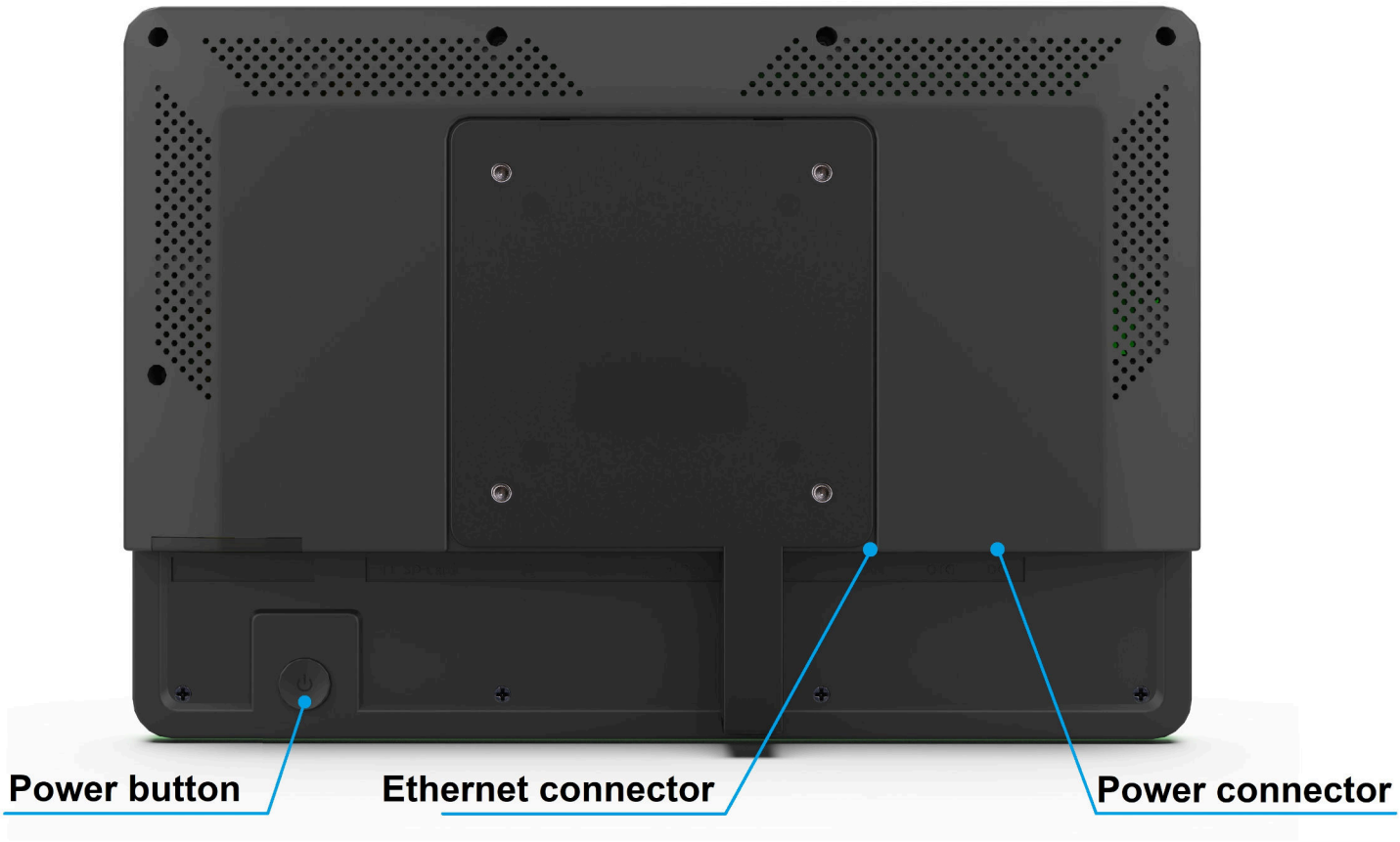


Figure 264: Predor office terminal back

- **Power button:** long press (3 seconds) switches the device on or off, short press activates or deactivates the screen.
- **Charging connector:** barrel jack, 12V/1.5A.
- **Ethernet connector:** 10/100/1000Mbit RJ45, POE.
- **NFC Card reader:** 13,56MHz proximity card reader (NFC NTAG, Mifare Classic, Mifare DESFire, ISO14443-A/B compatible identifiers).
- **RFID Card reader:** 125kHz proximity card reader (ISO/IEC 111785/11785, EM4100, EM4305, TK4100/GK4100, T5577 compatible identifiers).

PHYSICAL PARAMETERS

Dimensions: 259.36x178.36x28mm
Display: ..... 10.1" touch screen, 1280x800 resolution
Case: ..... Plastic

INTEGRATED DEVICES

NFC Card reader: ..... ISO14443 Type A/B, Mifare Classic, Mifare DES-Fire, NFC NTAG
RFID Card reader: ..... ISO/IEC 111785/11785, EM4100, EM4305, TK4100/GK4100, T5577
Front camera: ..... 5 Megapixel, fix focus

ENVIRONMENTAL PARAMETERS

Operating temperature: ..... 0-40°C
Operating humidity: 10-90%

ELECTRICAL CHARACTERISTICS

Power supply: ..... 5V DC / 2A
Network connection: ..... 2.4GHz / 5GHz Wi-Fi or Ethernet

Important Notes

Please read the following carefully before proceeding and using the appliance:

- **Use the device only in appropriate environmental conditions stated in the datasheet.**
- **Never place the terminal near fire or excessive heat source.**
- **Do not submerge or place the device near splashing water. Do not use the terminal in rain.**
- **Use only the original charger.**
- **Do not use the charging cable if its insulation is damaged or broken. In this case change the charger or the cable.**

First steps

Before using the terminal, connect the charging cable to it or an Ethernet cable from a switch which has POE. When the charging cable is connected or it can get power from a POE switch, the device will switch on automatically. When the terminal has been switched on successfully the screen displays the **android** logo and starts to boot in the background. Please be patient while the system starts, as it can take a few minutes. If the terminal started successfully the homescreen appears on the screen.

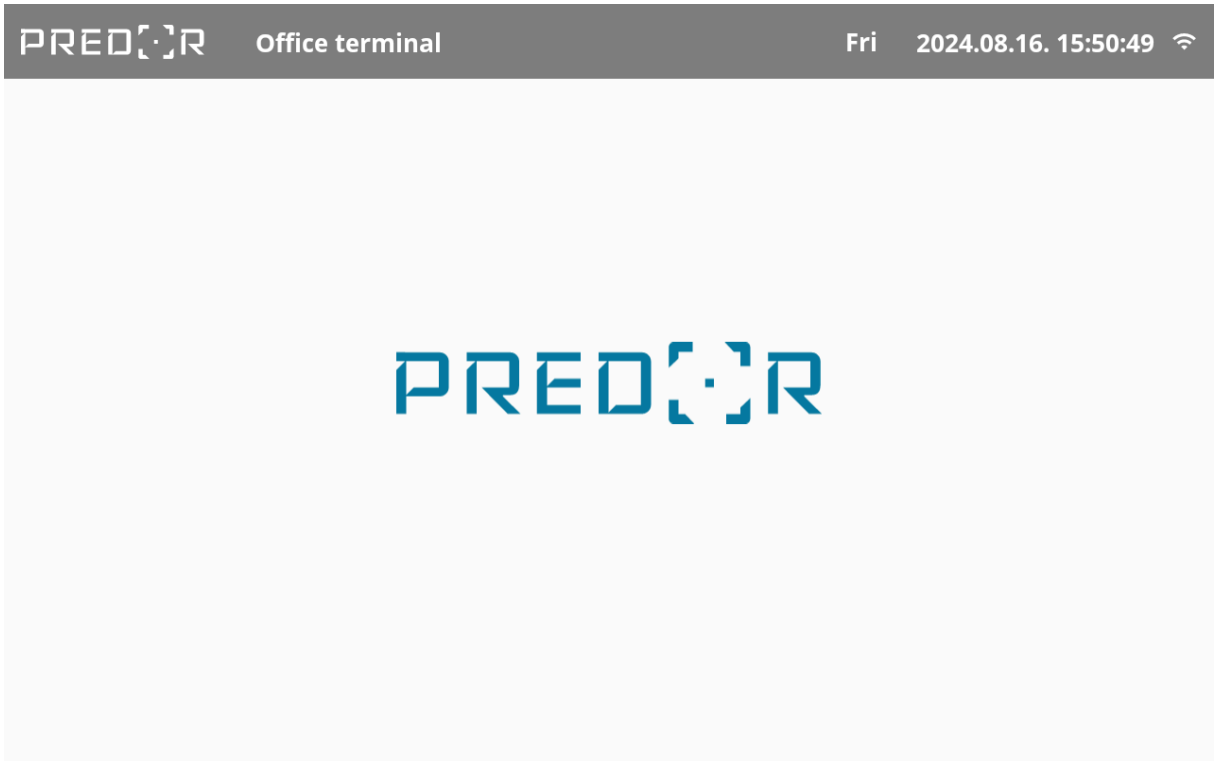


Figure 265: Predor terminal home screen

The terminal has a settings menu which is accessible by tapping the **Predor** logo on the top left of the screen multiple times. The menu is protected by a password which is the same as the *controller password* set in the Predor Client software. As the terminal is not attached to any system yet, there is no password, just tap the *OK* button.

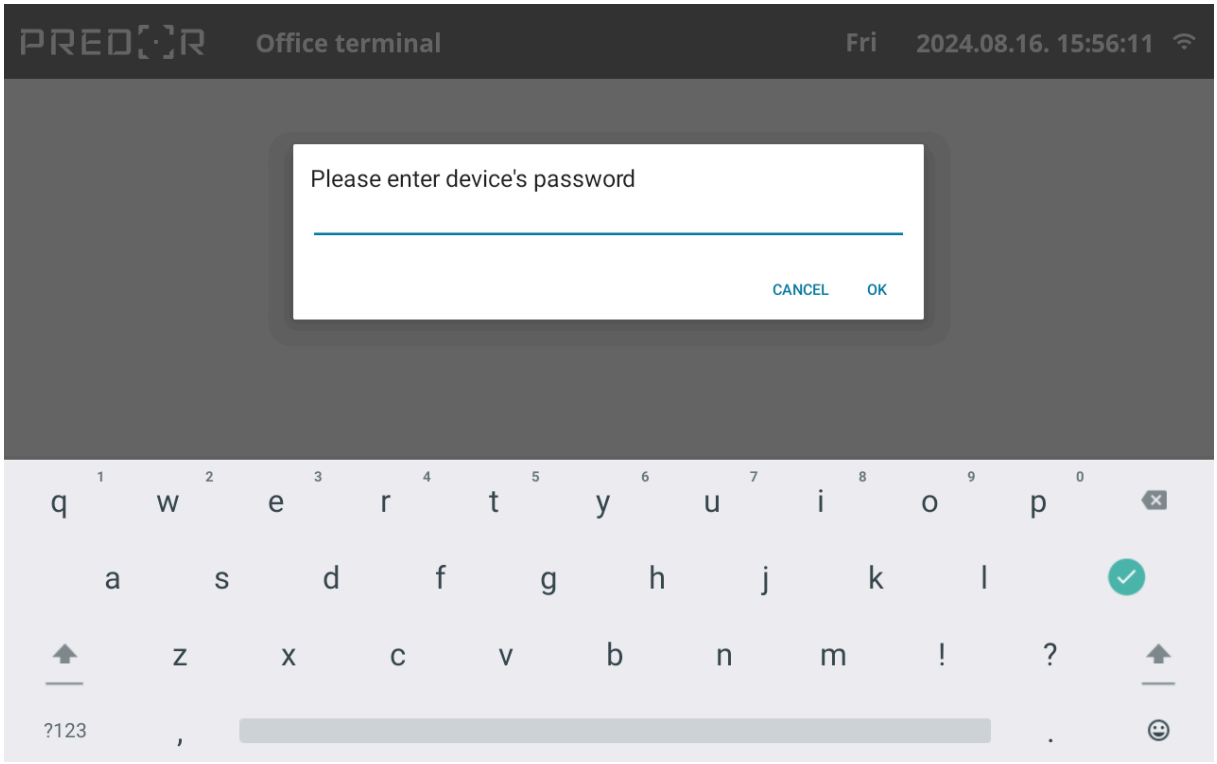


Figure 266: Accessing the Predor terminal's menu requires a password

Predor terminal menu map

The following settings and options are available in the menu:

- *General*
  - **Terminal name:** displays the terminal's current name, it is only editable in the Predor Client software.
  - **Automatically logout user:** timeout after a successful identification after which the terminal returns to the home screen.
  - **Timezone:** displays the current time zone, it cannot be changed.
  - **Locale:** changes the terminal's display language.
  - **Idle screen setup:** sets how the home screen behaves: displays a static Predor logo or stock photos. When using Predor Enterprise software, the operation set in the software overrides this setting.
  - **Card number length:** sets the card number format used by the terminal. It is advised that this value is aligned to the other terminal(s)/card readers already used in the system.
  - **Card type:** the type of cards the device should read can be selected. The terminal can read EMID (125kHz) or Mifare/NFC (13.56MHz) cards. It can read both or

only one of the types.

- **Automatically enter sleep mode:** sets the amount of idle time after the screen automatically switches off.
- **Prevent sleep mode when charging:** sets whether if automatic sleep mode is ignored while charging.
- **Skip activity code approval:** can be set to register activities without validation. After the employee identifies themselves and chooses an activity code, a pop-up window will ask them to confirm it or go back. With this option, this step can be skipped.

- *Network interface*
  - **Communication mode:**
    - **Local Predor Enterprise:** this mode should be chosen if the terminal is connected to the same subnet as the server and can access each other via UDP connection in addition to HTTP (TCP).
    - **Remote Predor Enterprise:** this mode should be used when the terminal is not on a subnet with the server. In this mode, the terminal and the server communicate only over HTTP. If the terminal connects to the server via the Internet, it will need a fixed external IP address or dynamic DNS (e.g. dynDNS) and the appropriate ports must be forwarded through firewalls and routers.
    - **Predor Cloud:** this mode must be used if the terminal is added to a Predor Cloud system. In this mode, the device communicates via the Internet.
  - **IP address, netmask, Gateway address:** The device gets its network settings from the DHCP server. **It is required to use DHCP server, static IP address cannot be assigned to the device.**
  - **UDP port:** In case of Local mode this value shows the UDP port on which the terminal listens for incoming connections. **This can be modified in the Predor client software, but the terminal only gets it if it has connection to the server**.
  - **MAC address:** for information purposes only, never editable.
  - **Wi-Fi settings:** this menu shows the currently connected network. Upon tapping this option the available networks list appears. If a not known network is chosen the terminal tries to connect to it, in case of an already known network there is an option to forget it.
  - **Wi-Fi:** enables or disables the wireless network access.
- *Server communication:* Details for the Predor server communication has to be set

here. Available options depend on the server communication mode (local/remote) chosen before.

- **Server protocol:** set the HTTP protocol used by the server. (default: HTTP)
- **Server IP address / Server host:** set the Predor server's IP address or DNS name.
- **Server UDP port (local mode only):** set the port given in the Predor Client settings menu for the terminals. (default: 60012)
- **Server HTTP port:** set the Predor server's HTTP port. (default: 8888)
- **Automatically select protocol (local mode only):** The terminal can try to detect the server's HTTP mode. It is advised to set this option to "For the first time", thus the terminal determines the correct option now and remembers it.
- **Login (remote and Predor Cloud mode only):** This button is used to register the device to the server in remote or Predor Cloud mode. The registration procedure is detailed in a subsequent section.
- **Server status:** gives feedback whether a Predor server is accessible with the given settings.
- **XTEA key:** currently used cipher password - displayed only for debugging purposes.
- **AUTH token:** currently used authorization token for the server - displayed only for debugging purposes.

- *Service*
  - **Display card numbers:** displays the detected card number on the screen. Use it only for debugging.
  - **Reboot device:** restarts the device.
  - **Shutdown device:** switches off the terminal. To switch back on press the power button for 3 seconds.
  - **Wipe data:** deletes all setting and data from the device including IP, server and Wi-Fi settings and passwords, **stored and not yet synchronized events** and offline stored data (users, card numbers).
  - **Firmware update:** tries to download the most recent software version from the Predor server and upgrades to it.
  - **Time synchronisation:** starts an immediate time synchronisation for this terminal.
- *About:* displays basic information about this terminal, including the serial number.

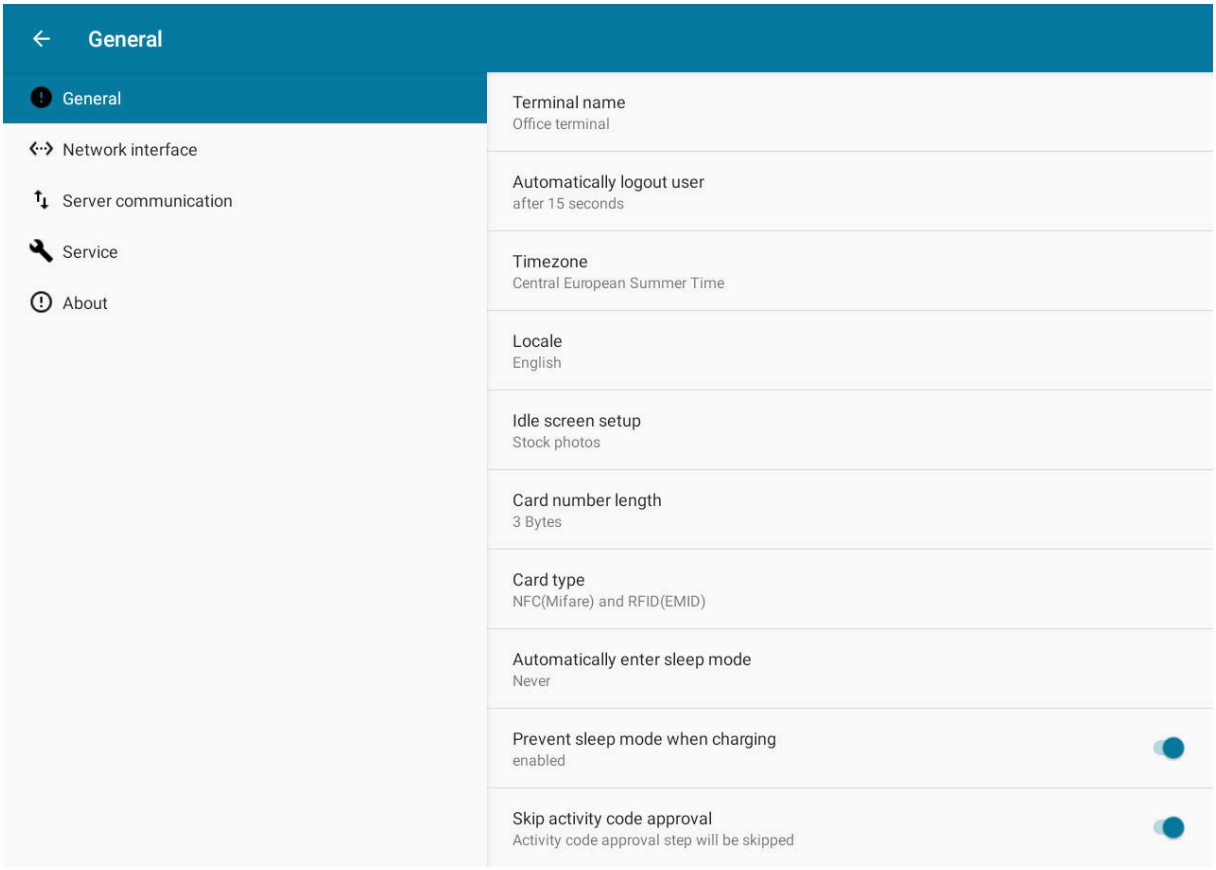


Figure 267: Menu of the office work time terminal

Adding the terminal to the Predor Enterprise software

Before the terminal can be used it must be added to Predor Server. First, connect the terminal to cable network with ethernet or the appropriate Wi-Fi network which can be done via the terminal's menu. Select the **Network interface** submenu and the **Wi-Fi settings** option.



WARNING: It is required to use DHCP server on the network. The device gets its network settings from the DHCP server, static IP address cannot be assigned.

The following steps depends on which server communication mode has been chosen:

- **Local Predor Enterprise mode:** This mode should be chosen only if the terminal is connected to the same subnet as the server and can access each other via UDP connection in addition to HTTP (TCP).

  In this case in the Predor Client Application navigate to the **Attendance** menu and **Worktime terminals** submenu then click on the "discover terminals" button. Choose the new terminal(s) and click the OK button to them to the system.

Initialisation of the terminal is commencing and after a few seconds the terminal is operational.

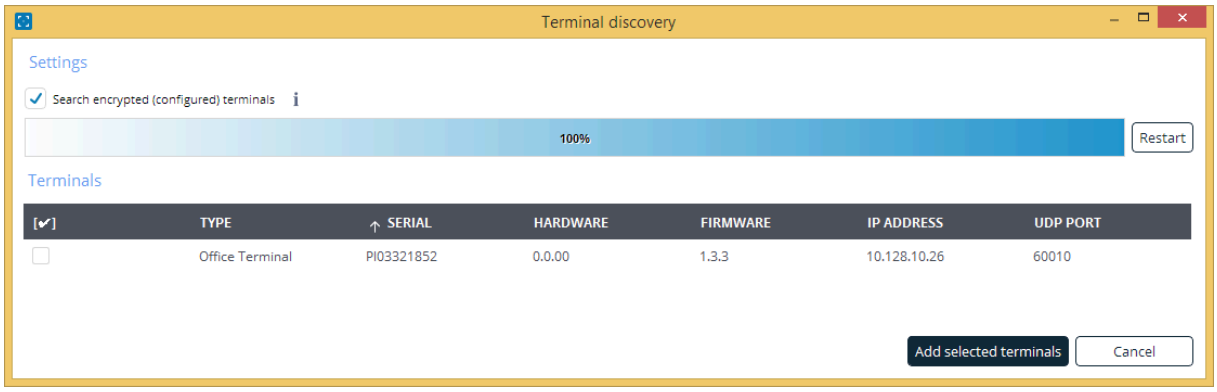


Figure 268: Adding new terminal in Local Enterprise mode via terminal discovery menu

- **Remote Predor Enterprise mode:** This mode should be used when the terminal is not on a subnet with the server. In this mode, the terminal and the server communicate only over HTTP. If the terminal connects to the server via the Internet, it will need a fixed external IP address or dynamic DNS (e.g. dynDNS) and the appropriate ports must be forwarded through firewalls and routers.

  The first step in this mode is to manually add the terminal to the Predor system in the Predor Client application's **Attendance** menu and **Worktime terminals** submenu. Click on the **+ new** button in the lower left to add a new terminal.

  The new terminal appears in the list.

  Give a custom name for this terminal - it will be visible on the device's screen too.

  Click on the *edit* button to fill in the details: type in the terminal's serial number which can be found on the backside label or in the terminal's menu under the **About** submenu.

  Tick the **Remote terminal** option.

  Adjust the remaining options as needed.

  Check if the given serial number is correct then click on the save button. Adding the terminal to the system is now finished from the server's side, but the terminal still has to log in to be usable.

  Enter the terminal's menu. Check if the "Remote Predor Enterprise" option is selected as the *Communication mode* in the **Network interface** menu.

  In the **Server communication** menu select the appropriate *Server protocol* and type the server's address into the *Server host* field. Type the appropriate HTTP port into the *Server HTTP port* field. **By default, the HTTP port of the server is 8888.** If the server is accessible and all parameters are correct, the *Server status* should show "Reachable".

Press the *Login* button and type in the *controller password*.

WARNING: If no password was set in the Predor system previously, then the terminal cannot be initialised. Please set a new custom password via the Predor Client application in the **Settings** menu **System settings** submenu and click on the **controller password** button.

If the login has succeeded the terminal displays the following message: “Logging in was successful, the device is now initialized.”

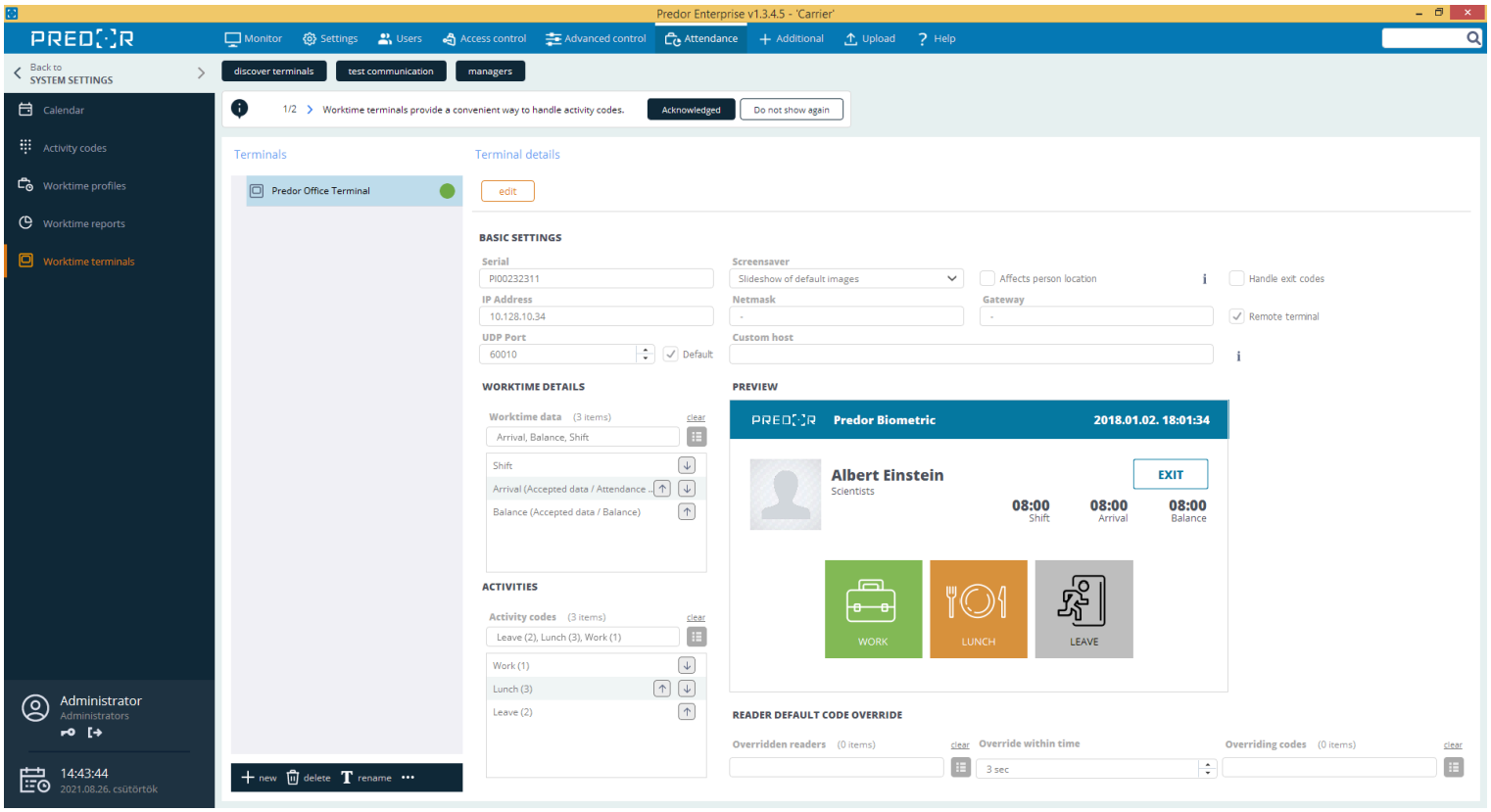


Figure 269: Office terminal added to the system in remote mode

General usage

Once the work time terminal has been successfully added to the Predor server synchronization of work time data happens automatically in the background. In case of remote mode synchronization may happen a bit slower, changes made in the Client application can be delayed by up to 10 seconds.

In factory default settings the sleep mode is disabled thus the screen stays active continuously. This operation requires a relatively large amount of power, so it is advisable to manually switch the display off and on when necessary. The screen can be switched on and off by pressing the power button for a short time.



CAUTION: While the screen is turned off the terminal enters a standby mode and disables the internal card reader. To use the card reader, the screen must be turned back on first.

Adding a new user

New users can only be added from the Predor Client software in the *Users* menu and **Users and departments** submenu.

If proximity card authentication is needed cards or badges can be added to the system using any card readers connected to Predor Access Control units or with a USB card reader. If none of them are available in the system – only biometric terminal(s) – then the easiest way is to just swipe the card on the work time terminal which generates an unknown card event in the Predor Client application in the *Monitor* menu. Right click on the event and choose “Copy card number to clipboard” then create the new user select to add card manually and paste the card number.



WARNING: When recording a card, pay attention to the input format! If you are using a USB card reader, the input format is indicated on the back of the device

.

Registering an activity

To register an activity one must authenticate themselves first by card, then select an activity from the displayed list. After confirming the selection the terminal sends it immediately to the server if there is an active network connection.

TIP: Activity entry confirmation can be skipped, this feature can be enabled from the terminal menu by activating the **Skip activity code approval** option under the general settings menu

.

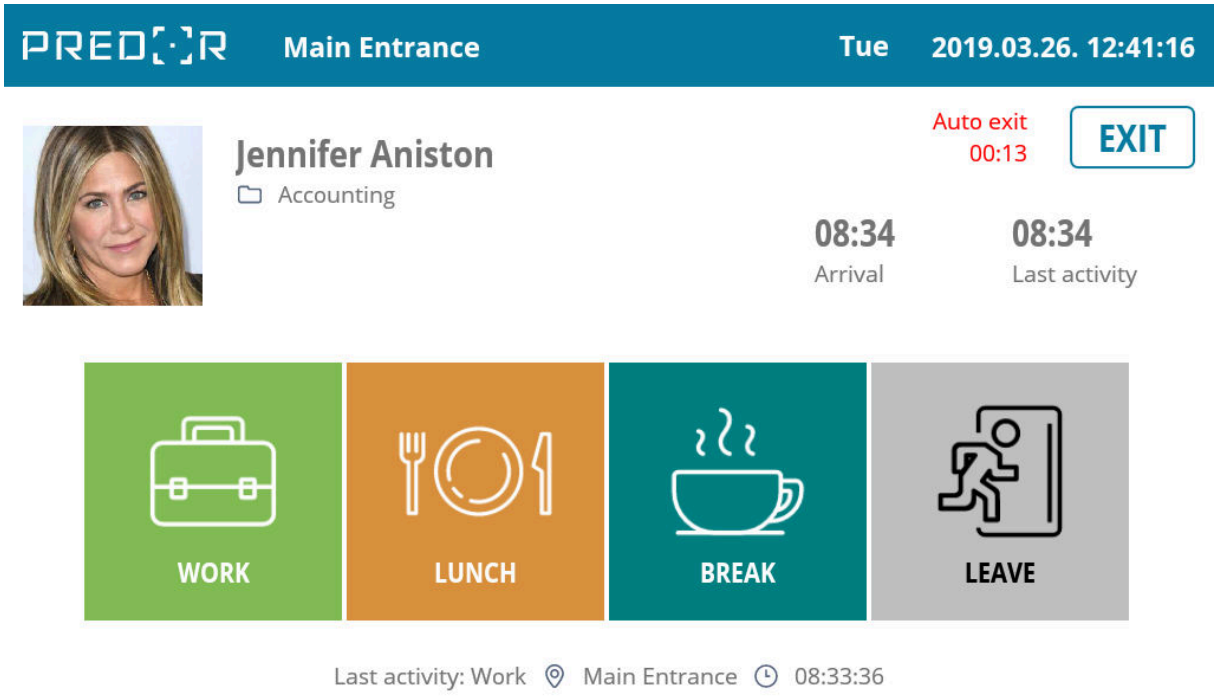


Figure 270: Registering an activity on the biometric work time terminal

Registering an activity for groups

The same activity can be registered quickly for a group of users using *Continuous login*. Continuous login can only be initiated by a *device manager*. Managers are selected from already existing users in the Predor Client software in the **Attendance** menu and **Worktime terminals** submenu by using the *terminal managers* button.

To initiate a continuous login the *manager* must authenticate themselves first, then select the appropriate activity then tap the *Continuous* button. A new login screen opens where users can authenticate themselves without any time limit one after another. The authentication was successful if the user has appeared in the list. Activities registered this way are also synchronized realtime if there is an available network connection. By tapping the *Done* button the continuous login session ends and the terminal returns to the home screen.

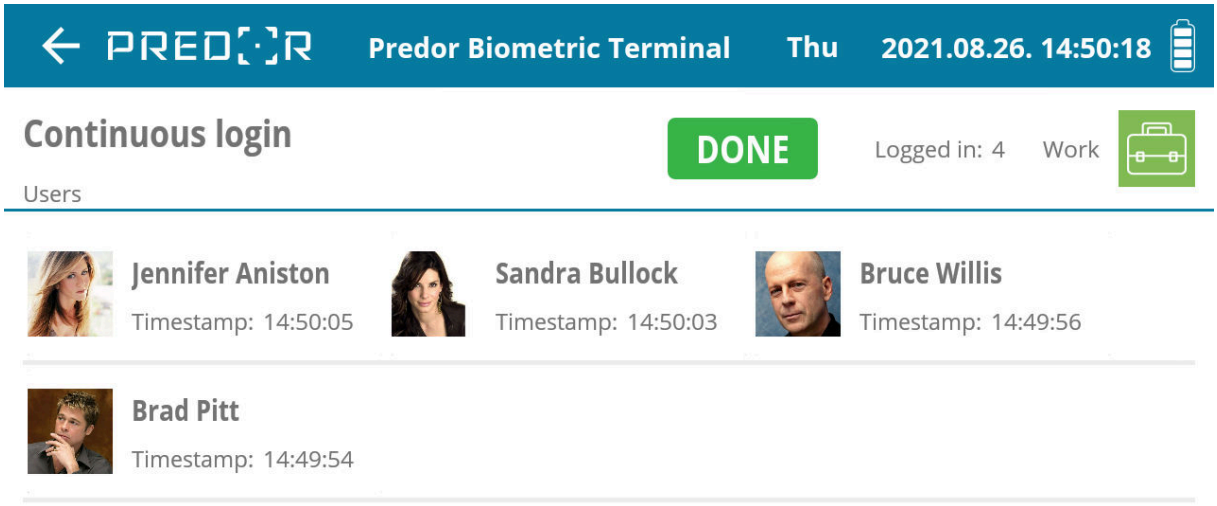


Figure 271: Continuous login with list of already registered users

WARNING: The continuous login mode does not automatically include the manager. If the manager would also like to register this activity for themselves they should authenticate again while in continuous login mode.

Troubleshooting

Phenomenon	Caused by	Solution
The terminal is not visible by discovery.	There is a firewall operating on the computer or the network.	Turn off the firewall or check its settings.
	The terminal is not connected to the right Wi-Fi access point.	Check whether the terminal is connected to an access point which is on the same network as the server.
	The terminal uses a different controller password.	Reset the terminal to the factory default settings. Enter the terminal's menu then select the **Service** menu and choose the **Wipe data** option. Connect the terminal again to the Wi-Fi network and try discovering again.
	The terminal is turned off.	Check if the terminal is operational and the display shows the home screen.

Table 14: Typical errors and solutions

26 FÜGGELÉK J: PREDOR PHANTOM NEW GENERATION FIRMWARE UPGRADE GUIDE

Predor Phantom new generation firmware upgrade

From Predor software version 1.6 , the Predor Phantom controller can be used with the new generation firmware. Starting with this version, Predor software and Phantom controllers will communicate over TCP connection instead of the previous UDP connection.

WARNING: The upgrade requires an NTP server running on the Predor server computer and TCP communication enabled on the network.

WARNING: The new generation firmware cannot be installed on Predor Sentinel controllers.

The firmware upgrade can be done in the same way as before. In the Predor client software, under Settings menu and Controllers submenu, select the controllers, then click on the 3 dots in the bottom menu bar and then on Firmware upgrade. After upgrading to Predor software version 1.6 (or later), the software will indicate the firmware update is available as usual. If the upgrade is completed, this will update the Phantom controller to the latest firmware (0.3.X) that communicates over UDP connection.

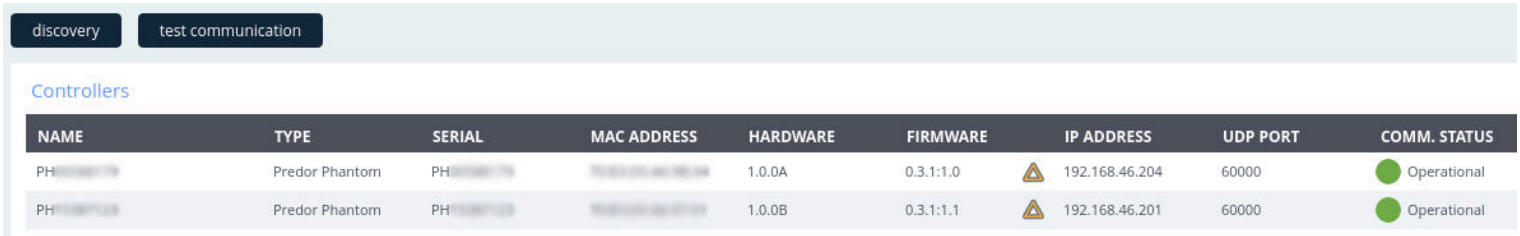


Figure 272: Phantom controllers with firmware version 0.3.X

After that, it is possible to upgrade to the new generation firmware. This has two conditions. The first is to have a NTP (Network Time Protocol) server, to which the controller is connected via UDP 123 port. By default, the device looks for this at the IP address of the Predor server. Therefore, an NTP server must be running on the server computer and communication on UDP 123 port must be enabled on the firewall. Secondly, the controllers must be able to connect to the Predor server via TCP. By default, the server opens TCP 9898 port. This can be changed in the System Defaults tab of the System Settings submenu of the Settings menu.

Version 0.3.X checks that these two conditions are met. After a successful connection, the controller sends the information about the success of the TCP and NTP connections to the server. If both are successful, a notification and a new tile **Upgrade Available** with information about the upgrade will appear in the Monitor menu, Dashboard submenu in the client software.

After that, as usual, another firmware upgrade should be started from the Controllers submenu of the Settings menu, which will load the new generation firmware to the controller. The version of this firmware is called 1.0.X.

WARNING: After upgrading to version 1.0.X, the update process will take several minutes. Expect that during this time it will not respond to card swiping, remote opening, etc.

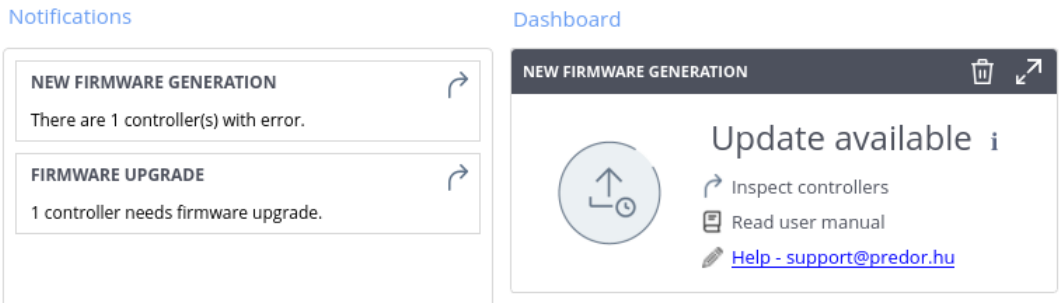


Figure 273: Firmware update available indicator in the Overview menu

If the controller cannot reach the server via TCP connection or cannot connect to the NTP server, a **Missing conditions** message is displayed on the tile.

In case of a TCP connection problem, it is necessary to check the network settings of the controllers, as well as the firewall settings on the server computer and on the network. If communication is disabled on the used TCP port (9898 by default), it must be enabled.

In case of NTP server connection problems, the NTP server functionality should be checked on the server computer and the communication on the UDP port used.

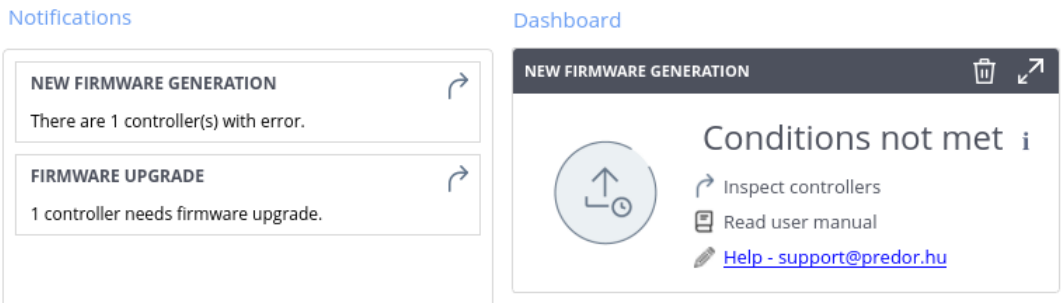


Figure 274: Missing conditions indicator in the Overview menu

The **Upgrade in progress** message is displayed on the tile if there is at least one controller in the system that has already been upgraded to the new generation firmware, but there is also at least one controller that can be upgraded but has not yet been performed. The Controllers menu can be used to check for the problematic devices.

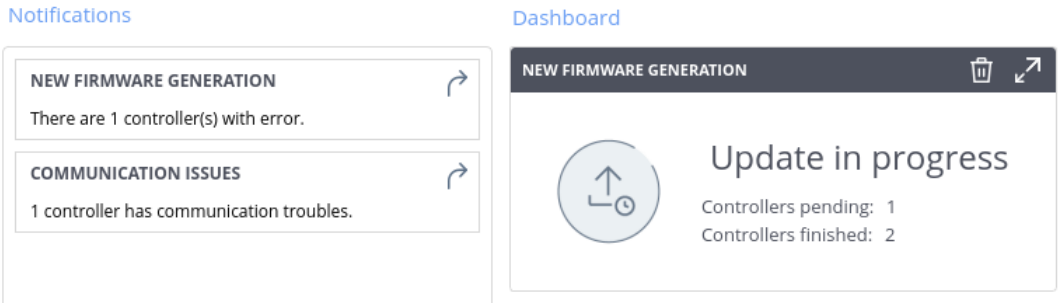


Figure 275: Upgrade in progress indicator in the Overview menu



Figure 276: Status of controllers in the Controllers menu

Two new columns will appear. TCP status and NTP status. These will indicate whether the controller has successfully connected via TCP to the Predor server and to the NTP server.

The **Upgrade Complete** message is displayed on the tile if all Predor Phantom controllers in the system have been upgraded to the new generation firmware.

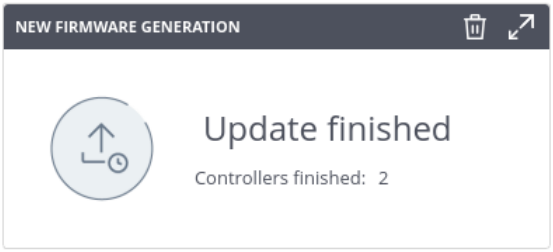


Figure 277: Upgrade completed indicator in the Overview menu

From now on, Predor Phantom controllers will communicate with the Predor software via TCP connection. Future firmware upgrades will also be done over the TCP connection.