SIGUR

Sigur ACS Quick Guide

Revision dated 19.12.2025.

Table of Contents

1. Introduction

This document contains general information about the Sigur Access Control and Management System (ACS), including instructions for installing and uninstalling the software. In addition, it provides instructions for operating the server management software and Sigur ACS client workstations.

The manufacturer is responsible for the accuracy of the information provided and undertakes to provide an updated version of this document in the event of significant changes or updates to the software.

This document corresponds to software version 1.6.4.116.s.

2. System requirements

2.1. Server hardware requirements

Minimum requirements.

- OS (64-bit only): Windows 10 / Windows Server 2016 / Linux Debian 11 / RHEL 8 (with the latest service pack) / CentOS 8 / Fedora 35 – any of these versions or later.
- CPU: at least 1.5 GHz, 4 cores.
- RAM: at least 8 GB.
- Free disk space: 5 GB for installation, plus additional space for the database. The size of the database depends on the number of cardholders, the size of their photos and the operating time of the system, as information about system events, time zones, etc. accumulates over time.
- At least one available USB port (if using a HASP key for software protection).
- Uninterruptible power supply.
- Monitor resolution: at least 1280*1024.
- For large databases (tens of millions of system events or more), an SSD or RAID array is required.

Recommended requirements.

- OS (64-bit only): Windows 10 / Windows Server 2019 / Linux Debian 11 / RHEL 9 (with the latest service pack) / CentOS 8 / Fedora 35 – any of these versions or later.
- CPU: Intel Core i7 and higher (8 cores).
- RAM: at least 16 GB.
- Free disk space: 250 GB.
- Database server: MariaDB version 10.7.2 or higher (for Windows or Linux), or PostgreSQL version 13 or higher (for Linux only).
- At least one available USB port (if using a HASP key for software protection).
- Uninterruptible power supply.
- Monitor resolution: at least 1280*1024.
- SSD or RAID array.

2.2. Client workstation hardware requirements

- OS (64-bit only): Windows 10 / Linux Debian 11 / RHEL (at least version 8 with the latest service pack) / CentOS 8 / Fedora 35 – any of these versions or later.
- CPU: at least 1 GHz.
- RAM: at least 2 GB.
- Free disk space: at least 500 MB for system installation.
- Monitor resolution: at least 1280*1024.

If client and server software are installed on the same machine, follow the server's recommended hardware requirements.

Any combination of servers and workstations running different operating systems is possible (e.g., a Linux server with Linux and Windows clients).

3. Sigur software

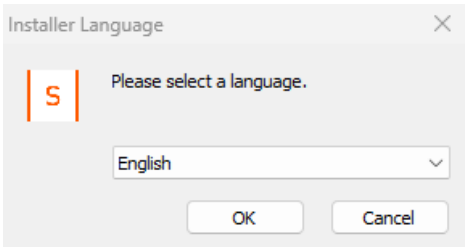
3.1. Sigur system installation

This section describes how to install the Sigur software on different operating systems.

3.1.1. Windows

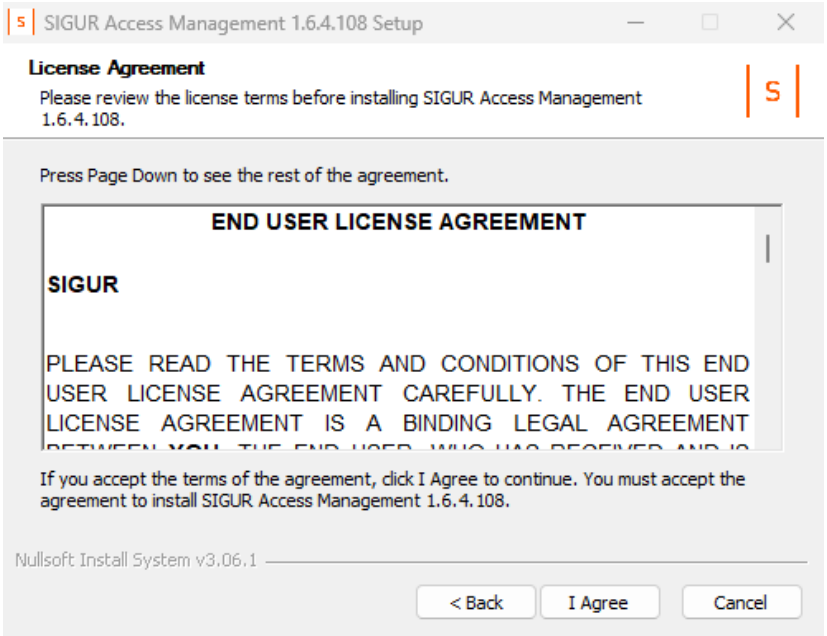
Make sure your system meets the requirements before installing the software. Log in with Administrator privileges, then run the "setup-XX.exe" file (XX is the version number).

1. Select the software language.



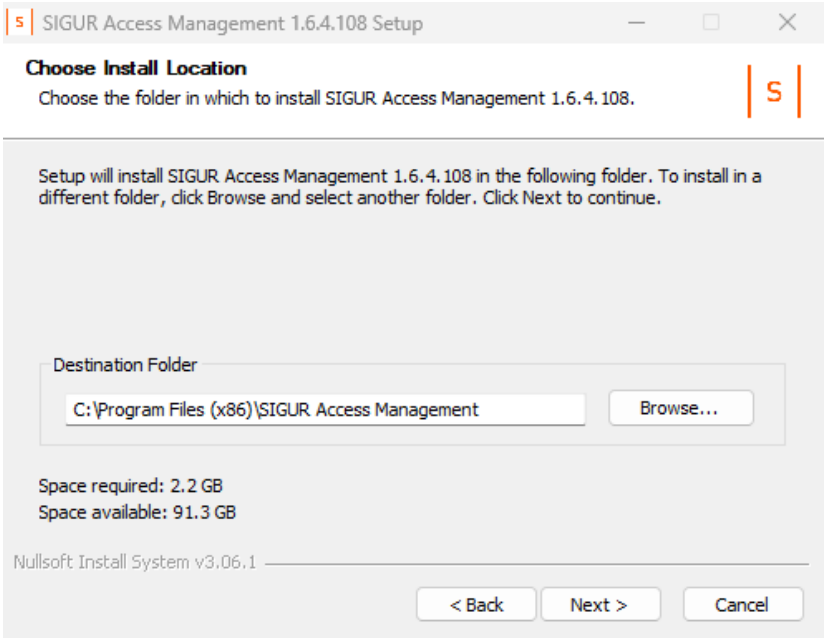
"Installer Language" window.

2. Read and accept the license agreement.



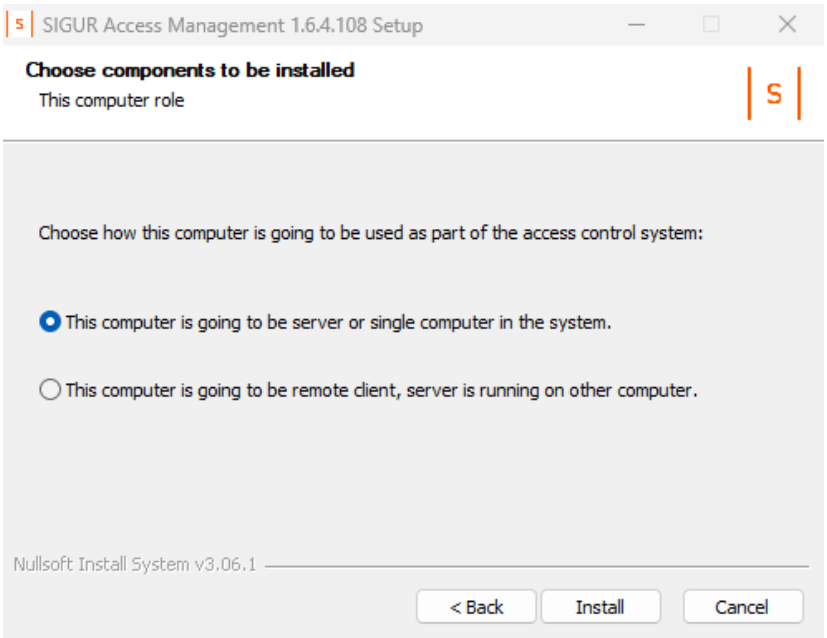
"License Agreement" window.

3. Choose the install location.



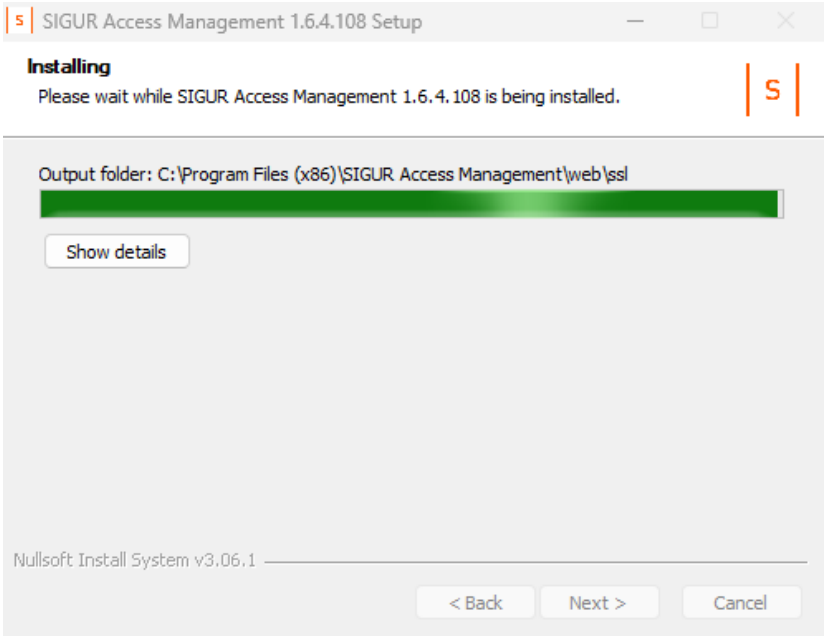
"Choose Install Location" window.

4. Choose components to be installed.



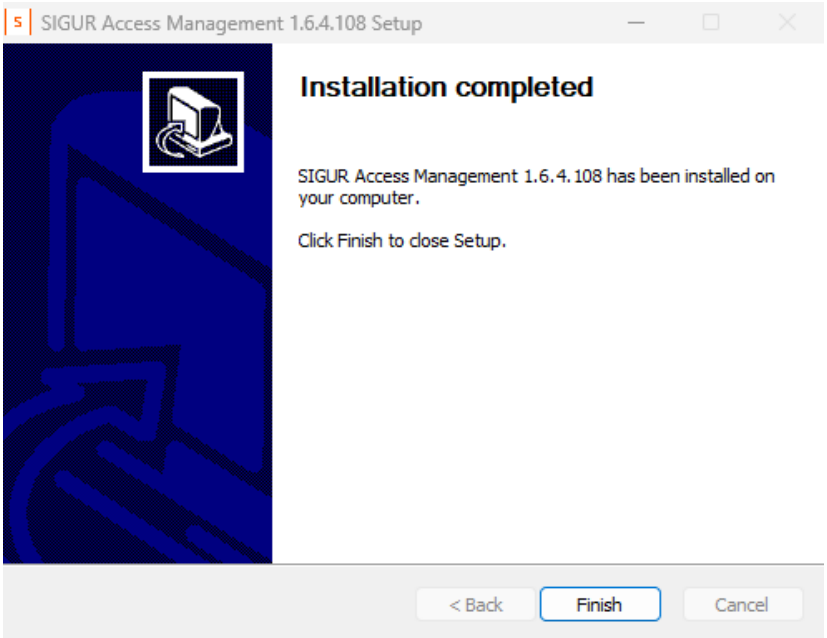
"Choose components to be installed" window.

5. The "Installing" window appears, displaying the installation progress.



"Installing" window.

6. When installation is complete, the "Installation completed" window appears. Click "Finish" to exit.



"Installation completed" window.

3.1.2. Linux

Make sure your system meets the requirements before installing the software.

1. Installing dependencies.

To ensure proper operation of the Sigur system, the following utilities are required: *sudo*, *openssl*, and Java 17.

1.1. sudo.

To check whether *sudo* is installed on the server, run the following command:

```
sudo
```

If the utility is not found, you will see a corresponding error message. To install the utility, use the following command:

Debian	*apt install sudo*
RHEL	*yum install sudo*

1.2. openssl.

To check the version of *openssl*, use the following command:

```
openssl version
```

If the utility is not found, you will see a corresponding error message. To install the utility, use the following command:

Debian	*sudo apt install openssl*
RHEL	*sudo yum install openssl*

1.3. Java 17.

To install and use the Sigur software, make sure that the installed Java version meets the minimum requirements. Sigur software version 1.6.4.x is compatible with Java 17. To check the version of Java, use the following command:

```
java -version
```

To install Java 17, you can use the following commands:

Debian	*sudo apt update* *sudo apt install openjdk-17-jre*
RHEL	*sudo dnf check-update* *sudo dnf install java-17-openjdk*

You can also download the installation files using the link.

2. Installing and configuring the database.

The Sigur system can use either MariaDB or PostgreSQL as the database server. This guide provides recommendations for configuring MariaDB.

2.1. Standard database configuration.

2.1.1. Install the MariaDB server:

Debian	*sudo apt-get install mariadb-server*
RHEL	*sudo yum install mariadb-server*

2.1.2. To ensure proper operation, disable case sensitivity in the database server settings.

To do this, you need to edit the *lower_case_table_names* parameter. This text parameter may be located in one of the database server's configuration files in the */etc/mysql/** directory. The name of the configuration file may vary depending on the system, database server build version, and other factors.

For example, the parameter may be located in */etc/mysql/mariadb.conf.d/50-server.cnf* (Debian-based Linux) or in */etc/my.cnf.d/mariadb-server.cnf* (RHEL) within the *[mysqld]* section.

Find the *[mysqld]* section in the file and add or modify the *lower_case_table_names* parameter as follows:

```
[mysqld]
lower_case_table_names=1
```

Save and close the file. Next, restart the server using the following command:

```
sudo systemctl restart mariadb
```

or use the command:

```
sudo service mysql restart
```

2.1.3. Create a user on the database server that will be used by the ACS server. Grant all privileges to access *TC-DB-MAIN, TC-DB-LOG, AUTH, EVENTS, NOTIFICATION, VISITREQUEST* databases. The database names *TC-DB-MAIN* and *TC-DB-LOG* must be enclosed in backticks (`) when used in queries.

For example, the following commands create a user named *sigur* with the password *my_password*:

```
mysql
MariaDB [(none)]> CREATE USER 'sigur'@'%' IDENTIFIED BY 'my_password';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON `TC-DB-MAIN`.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON `TC-DB-LOG`.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON AUTH.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON EVENTS.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON NOTIFICATION.* TO
'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON VISITREQUEST.* TO
'sigur'@'%';
MariaDB [(none)]> FLUSH PRIVILEGES;
```

2.2. Settings for remote workstation connections.

If the clients are intended to connect to the server remotely, grant permission to connect from other hosts in the settings of the database server. In the latest versions of MariaDB, this can be done by editing the *bind-address* parameter. You can find this text parameter in one of the configuration files of the */etc/mysql/** folder.

The file name may vary depending on the system and database server version. For instance, it can be found in the */etc/mysql/mariadb.conf.d/50-server.cnf* file in the *[mysqld]* section.

Set the value of the parameter as follows:

```
bind-address=0.0.0.0
```

Next, restart the server using the following command:

```
sudo systemctl restart mariadb
```

3. Installing Sigur software.

The latest package versions are available on our website.

3.1. Installing core packages.

Packages required for installation on the ACS Server:

- **spnxclient** – client package.
- **spnxserver** – server package (depends on the web services package).
- **deb-installer** or **sigur-web-services** – web services package (depends on the client and server packages).

Optional packages:

- **spnxclient-libs** – an optional .rpm-package containing client libraries for working with desktop readers such as ACR1252U, Sigur Reader EH, and others via PC/SC. This package is not required for installation. For example, it can be omitted on the server if the client workstation will not use desktop readers. Depends on the *spnxclient* package.

Debian	Download and install: 1. The ACS client package and all its dependencies (*spnxclient* package). *sudo dpkg -i spnxclient_*all.deb* 2. The ACS server package and all its dependencies (*spnxserver* package). *sudo dpkg -i spnxserver_*.deb* 3. The ACS web services package and all its dependencies (*deb-installer* package). *sudo dpkg -i deb-installer_*.deb* If you plan to use a desktop USB reader ACR1252U on this computer, complete the steps described in section 3.2.2.
RHEL	Download and install the client, server, and web services packages. If you plan to use desktop USB readers on this computer, also install the *spnxclient-libs* package. After that, if necessary, complete the steps described in section 3.2.2. Example command to install all components: *sudo rpm -i spnxclient-1*.rpm spnxclient-libs*.rpm spnxserver*.rpm sigur-web-services*.rpm*

3.2. Installing additional packages.

If you are planning to use the HASP key, install the HASP driver (Sentinel LDK and Sentinel HASP Run-time Environment DEB Installer for Linux). Download the driver archive from the official website of the manufacturer.

Extract the driver from the archive and install it:

```
tar -zxf Sentinel_LDK_Linux_Run-time_Installer_script.tar.gz && cd
Sentinel_LDK_Linux_Run-time_Installer_script
tar -zxf $(find . -maxdepth 1 -name "aksusbd*.tar.gz" -type f)
cd aksusbd*/
sudo ./dinst
```

3.2.2. If you are planning to use an ACR1252U desktop reader with this computer, you will also need to:

- Install *pcscd* and its libraries. To do this, you can use the following command:

Debian	*sudo apt-get install pcscd* *sudo systemctl enable pcscd* *sudo systemctl start pcscd*
RHEL	*sudo yum install pcsc-lite* *sudo systemctl enable pcscd* *sudo systemctl start pcscd*

- Install the driver for the ACR1252U reader. Download the archive with the drivers from the official website of the manufacturer. The archive contains drivers for different distributions and architectures. Find the driver for your system and install it.

  Below is an example of how to do it:

Debian	Example for Ubuntu 18.04 (Bionic Beaver) amd64: *wget "https://www.acs.com.hk/download-driver-unified/11929/ACS-Unified-PKG-Lnx-118-P.zip"* *unzip ACS-Unified-PKG-Lnx-118-P.zip* *sudo dpkg -i ACS-Unified-PKG-Lnx-118-P/ubuntu/bionic/libacsccid1_1.1.8-1~ubuntu18.04.1_amd64.deb*

RHEL	Example for Fedora Linux 36 (Server Edition): *wget 'https://www.acs.com.hk/download-driver-unified/11929/ACSUnified-PKG-Lnx-118-P.zip'* *unzip ACS-Unified-PKG-Lnx-118-P.zip* *sudo dnf install ACS-Unified-PKG-Lnx-118-P/fedora/31/pcsc-lite-acsccid-1.1.8-1.fc31.x86_64.rpm*

4. Configuring the database connection.

- Launch the "Server Administration" tool from the menu of your desktop environment, or by using the following command:

```
sudo spnxadmin
```

- On the "Database" tab, click the "Parameters" button.
- Next, enter the database server connection parameters (such as the address, port (default for MariaDB: 3306), database username and password). Save the settings, close the window.
- On the "Database" tab click the "Reset / create database" button. Make sure the database creation process has completed without errors and that the "Service's DBs Status" parameter shows OK.
- Go back to the database server connection parameters window and click "Connection test". Make sure that the test is successful. Otherwise, verify the database connection details.

5. Starting the server module.

After configuring the database connection, start the server module to complete the system setup. To do this, go to the "Status" tab in the "Server Administration" tool and click the "Start" button, or run the following command:

```
spnxcli service startSphinxd
```

6. Launching the client software.

To start the "Client" tool, use the following command:

```
spnxclient
```

3.2. Sigur system update

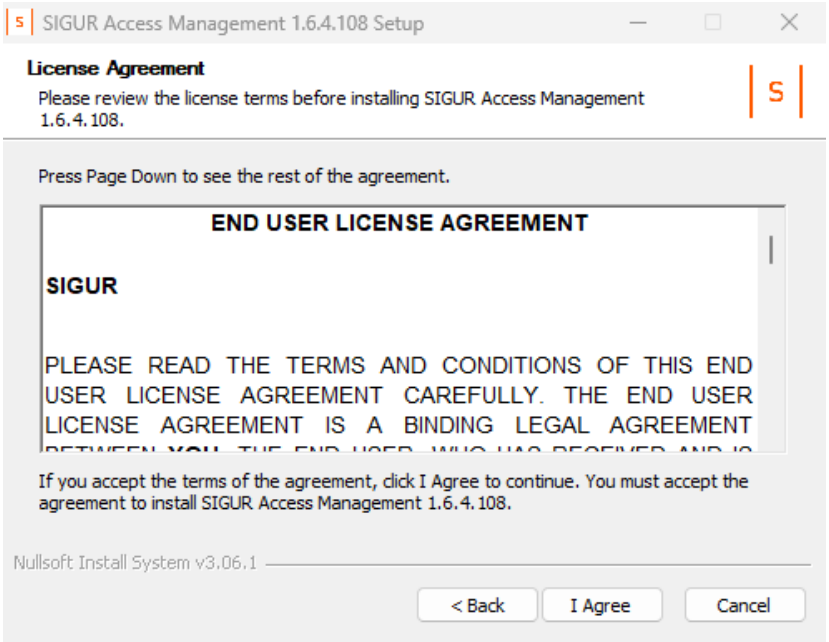
This section describes the procedure for updating the Sigur software on different operating systems.

You can update the software without uninstalling the previous version.

3.2.1. Windows

To update the Sigur software, follow these steps:

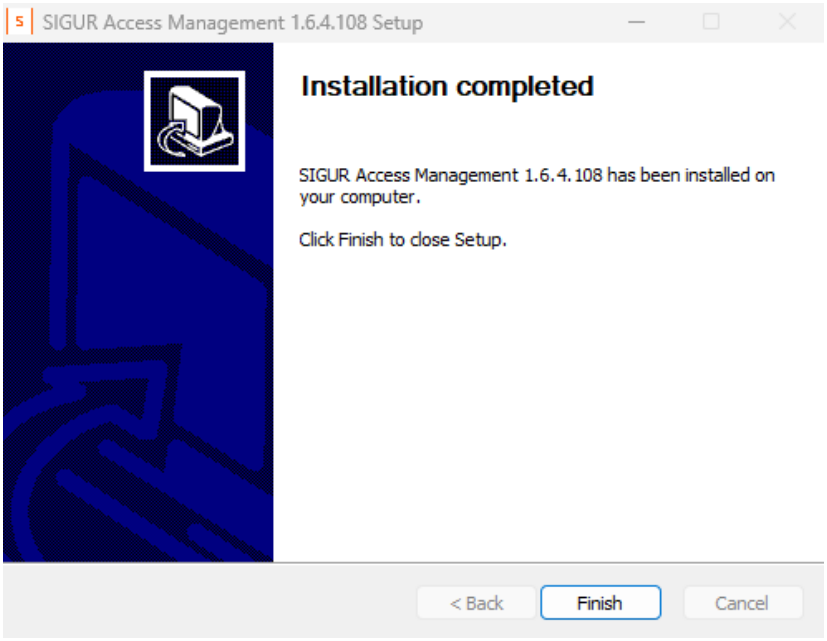
1. Download the latest version of the Sigur software from our website.
2. Back up the database.
3. Close all open windows of the Sigur software on the server and run the "sigur-X.X.X-X-web-setup.exe" file (X.X.X-X is the version number, e.g., "sigur-1.6.4-108-web-setup.exe").
4. Read and accept the license agreement.



"License Agreement" window.

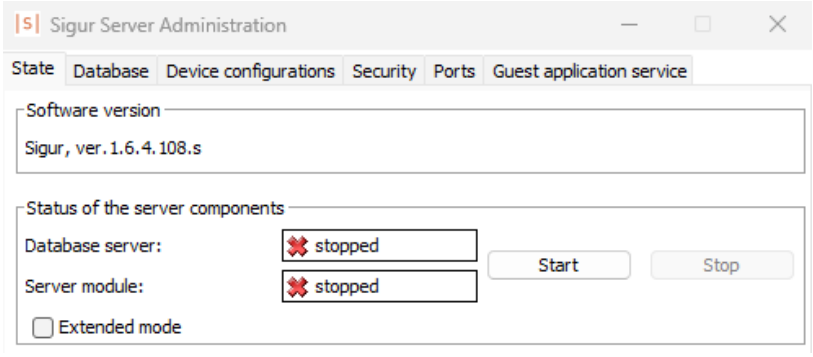
5. Click the "Next" button in the window that appears.

6. When the update is complete, the "Installation completed" window appears. Click the "Finish" button.



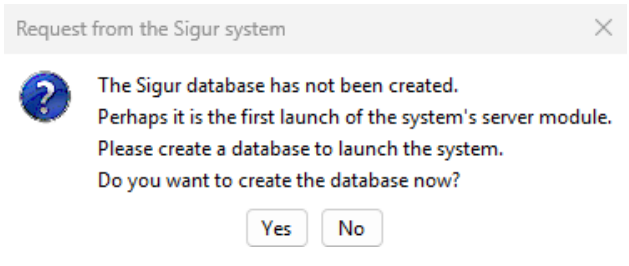
"Installation completed" window.

7. Start the "Server Administration" tool and click the "Start" button on the "State" tab.



Server Administration tool.

8. The application will prompt you to update the database. Click the "Yes" button.



Request window.

9. Once the software has been updated on the server, restart the "Client" tool on the client workstations to trigger an automatic update. If certain security policies are configured in the operating system, make sure the Sigur software has access to the following locations:

    - The software installation directory.
    - The *HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ACS Sphinx* registry branch.

    Alternatively, you can update the client workstations manually, following the same procedure as for the server.

3.2.2. Linux

To update the Sigur software, follow these steps:

1. Backing up the database.

Back up the database. Follow the link for instructions.

2. Stopping the server module.

Stop the server module by clicking the “Stop” button on the “State” tab in the “Server Administration” tool, or by running the following command:

```
spnxcli service stopSphinxd
```

You can check the system status by running the following command:

```
spnxcli service status
```

After that, close all Sigur graphical interface windows, if any are open.

3. Removing the previous Java version.

Sigur software (starting from version 1.6.3.x) requires Java 17. You can check the installed Java version by running the following command:

```
java --version
```

If the Java version is not 17, it must be reinstalled. For example, to remove Java 11 before installing a new version, run the following commands:

Debian	*sudo apt purge openjdk-11**
RHEL	*sudo yum remove java-11**

4. Installing Java 17.

Example commands for installing Java 17:

Debian	*sudo apt-get update* *sudo apt-get install openjdk-17-jre*
RHEL	*sudo yum update* *sudo yum install java-17-openjdk*

Check the installed Java version. The command must display information about Java version 17:

```
java --version
```

5. Updating the Sigur software.

Download the latest software packages and run the commands shown below (example). The latest package versions are available on our website.

Debian	Execute the commands in sequence: *sudo dpkg -i spnxclient_1.6.** *sudo dpkg -i spnxserver_1.6.** *sudo dpkg -i deb-installer_1.6.**
RHEL	List all upgradable packages: *sudo rpm -U spnxclient-1.6.* spnxserver-1.6.* spnxclient-libs-1.6.* sigur-web-services-1.6.**

6. Starting the Sigur server.

After the update is complete, start the server module by clicking the “Start” button on the “State” tab in the “Server Administration” tool, or by running the following command:

```
spnxcli service startSphinxd
```

7. Updating the database version.

If required, update the database version by clicking the “Update” button on the “Database” tab in the “Server Administration” tool, or by running the following command:

```
spnxcli database update
```

8. Updating client workstations.

Sigur client workstations running Linux must be updated manually, as automatic updates are not supported. Example commands:

Debian	*sudo dpkg -i spnxclient_1.6.**
RHEL	List all upgradable packages: *sudo rpm -U spnxclient-1.6.* spnxclient-libs-1.6.**

4. Server administration tool

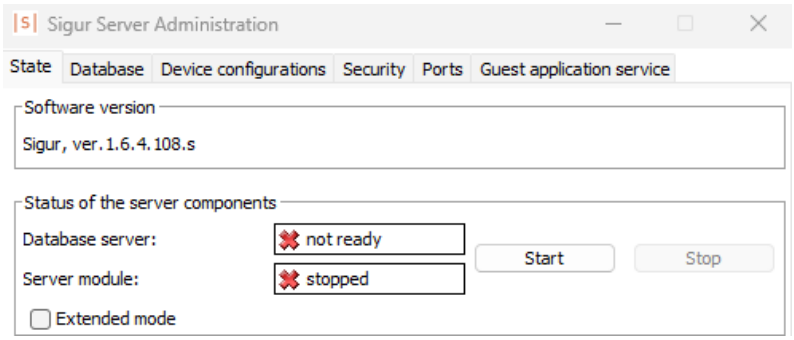
The "Server Administration" tool is designed to monitor the status of server components, configure database backup, edit controller network settings, etc.

4.1. First launch of Sigur software

The "Server Administration" tool is launched via the "Server Administration" shortcut. You can find it in the Start menu under "All apps" –> "Sigur Access Management".

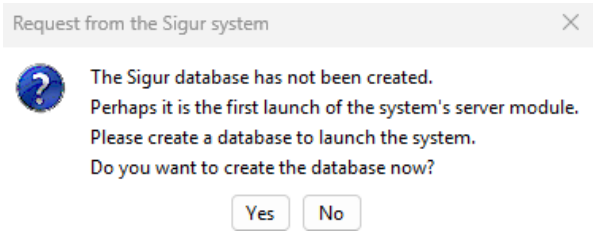
4.2. Server and database modules management

Start the server module and the database server by clicking the "Start" button on the "State" tab.



"State" tab.

When you start the database module for the first time, a window will appear prompting you to create a new database.



Request window.

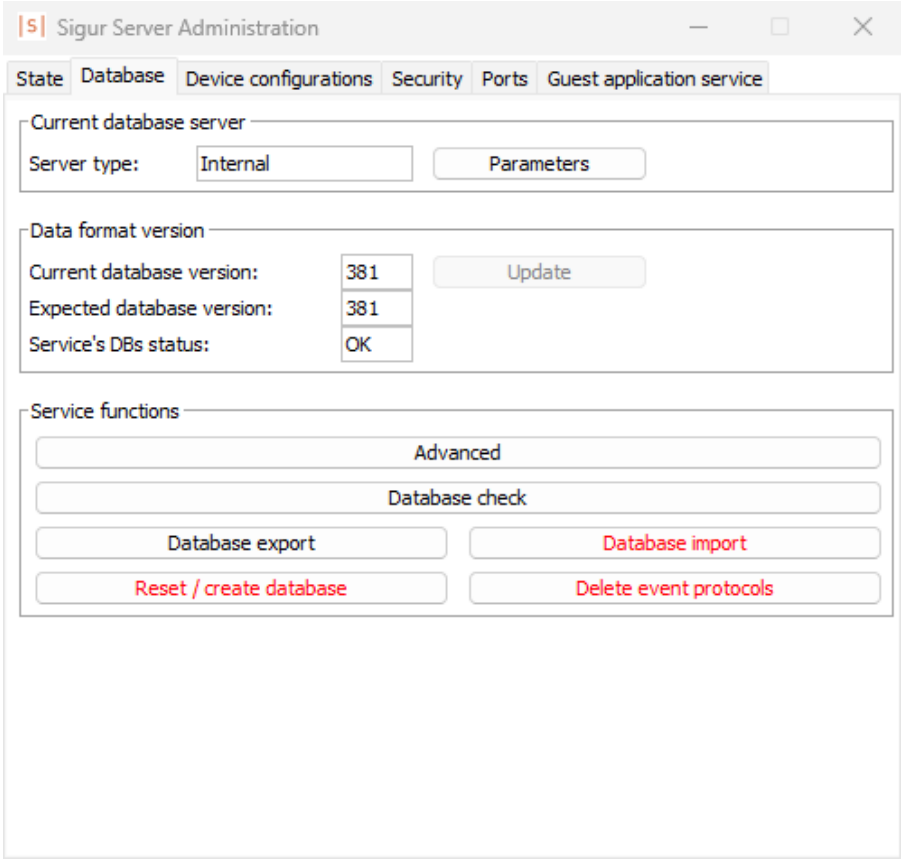
Click the "Yes" button to create a database. The database is created only once; subsequent launches do not display this prompt. By clicking the "No" button, you can choose not to create a database. In this case the database server will start but the other software components will not work. To create a database, you can also click the "Reset / create database" button on the "Database" tab.

To stop the server module and the database server, use the "Stop" button.

4.3. Automatic database backup

Automatic database backup and other service features are only available if the Sigur ACS server is deployed on Windows. For Linux, the database backup must be done manually using standard database server tools.

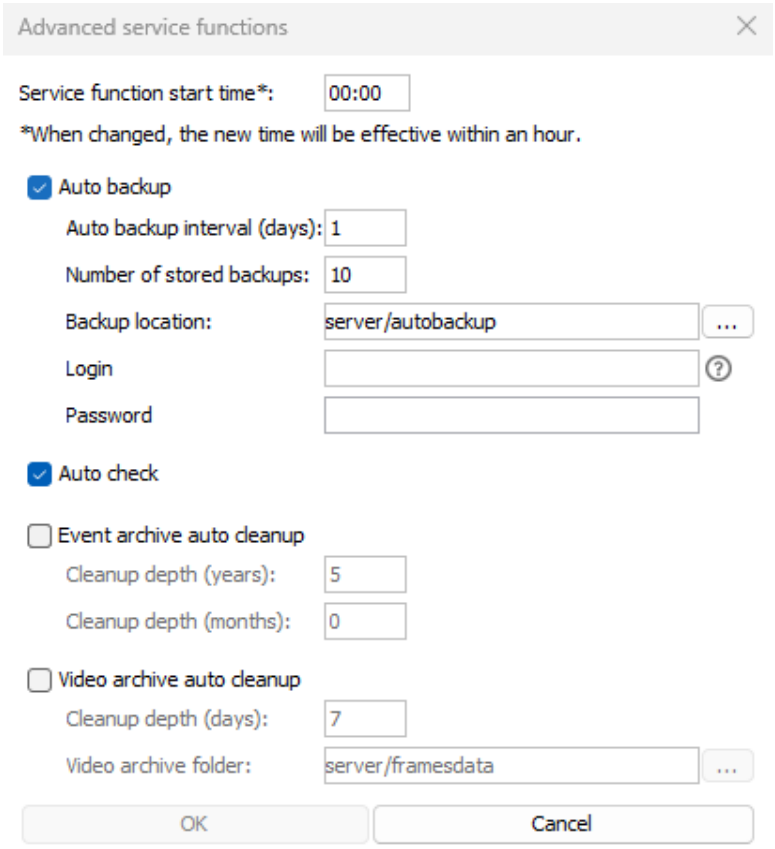
To configure automatic export of the Sigur database on Windows, go to the "Database" tab and click the "Advanced" button.



"Database" tab.

In the window that appears, do the following:

1. Enable the "Auto backup" option.
2. Specify the desired backup interval (from 1 to 999). This defines how often the database is backed up.
3. Specify the maximum number of backup copies (from 1 to 999) that the software should keep. If this number is exceeded, old copies are automatically deleted.
4. You can change the backup location if needed. It is recommended that the backups are stored on a different physical drive, or at least on a different logical drive. By default, backups are stored in the software installation directory: "..."\SIGUR Access Management\server\autobackup, where "..." is the software installation path (usually C:\Program Files (x86)).



"Advanced service functions" window.

The format of the backup files is "YYYY-MM-DD.sql". The filename defines the year, month, and day of the backup.

It is also recommended to activate the "Auto check" option. The system will perform an automatic database check once a day, starting this procedure at the "Service functions start time" configured by the user (00:00 by default).

4.4. Manual import and export of the database

Windows.

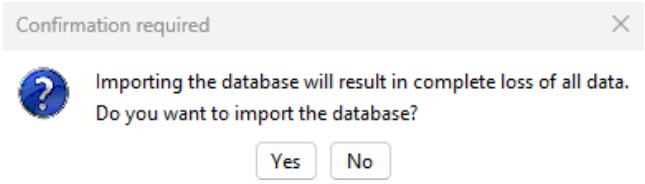
To manually back up the Sigur database, you should:

1. Start the "Server Administration" tool and go to the "Database" tab.
2. Click the "Database export" button.
3. Select a location to save the file, enter a file name, and click "Save".
4. Go to the "State" tab and click the "Start" button to initiate the backup process.

To import a database backup, you should:

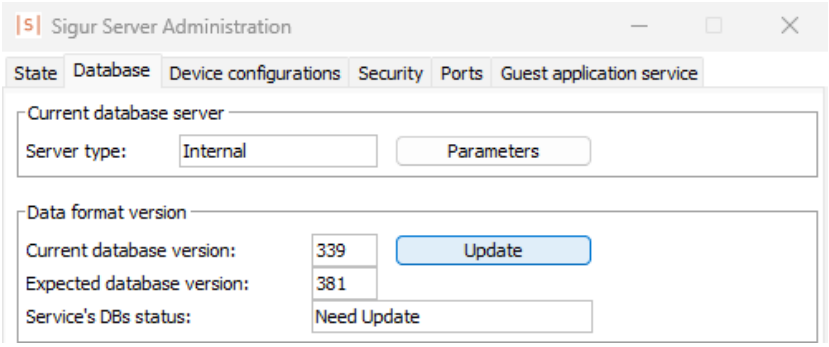
1. Start the "Server Administration" tool and click the "Database" tab.
2. Click the "Database import" button.

3. Click "Yes" in the window that appears.



"Confirmation required" window.

4. Select a backup file to import.
5. When the import is complete, check the compatibility between the current database version and the required version. If the current database version is less than the required version, update it by clicking the "Update" button in the "Data format version" block.



"Database" tab.

Linux.

For a Linux server, database management is performed using standard MySQL tools.

- You can use the following command to back up the database:

```
mysqldump -u <user> -P 3306 -p <userpass> -B TC-DB-MAIN TC-DB-LOG AUTH EVENTS NOTIFICATION VISITREQUEST > backup.sql
```

- You can use the following command to import the backup:

```
mysql -u <user> -P 3306 -p <userpass> < backup.sql
```

where *<user>* is the database username, *<userpass>* is the password of that user, and *backup.sql* is the name of the backup file.

If the backup file was originally created on a Windows machine running Sigur ACS, ensure that case sensitivity is disabled in the database server settings.

5. Controller network settings

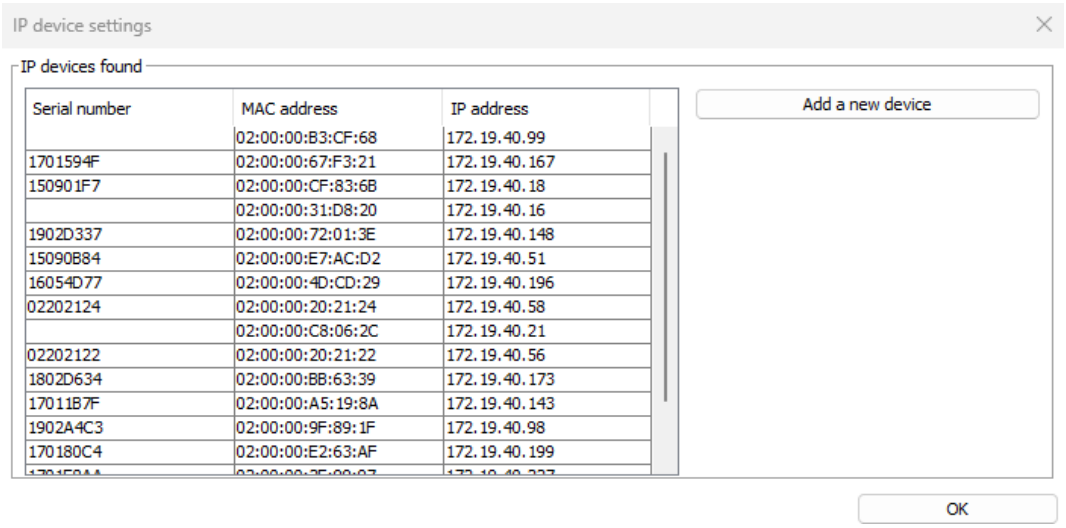
5.1. Setting up a controller's network parameters

To configure the network parameters of the controllers and view the Sigur devices currently available on the network, go to the "Device configurations" tab and click the "Set up IP devices" button.

"Device configurations" tab.

The window that appears shows detected Sigur controllers with configured network parameters. The controllers are discovered through broadcast requests on UDP port 3303. Both the controllers and the PC running the "Server Administration" tool must be on the same local network segment.

Sigur E510, E2, and E4 controllers can be configured without using the "Add a new device" button, as this button is intended for models from previous series of controllers.

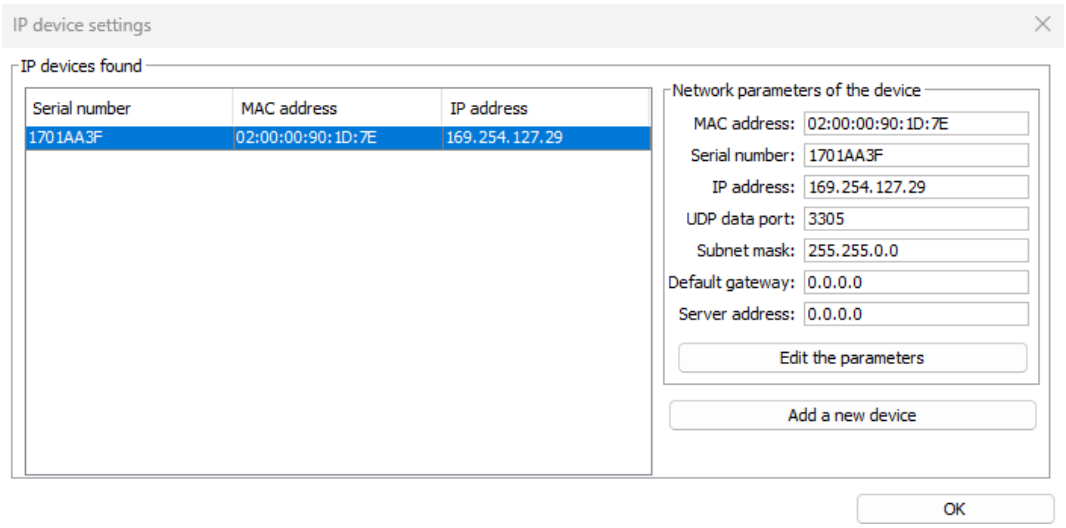


"IP device settings" window.

The "Server Administration" tool can be started either fromthe Sigur ACS server or from any other PC. In this case, it is not necessary to start the server components: the "Device configurations" tab works independently and does not require a license. Your computer must be configured to use IPv4.

When a specific device is selected from the list, its current network parameters are displayed in the right pane of the window, and the "Edit the parameters" button becomes available.

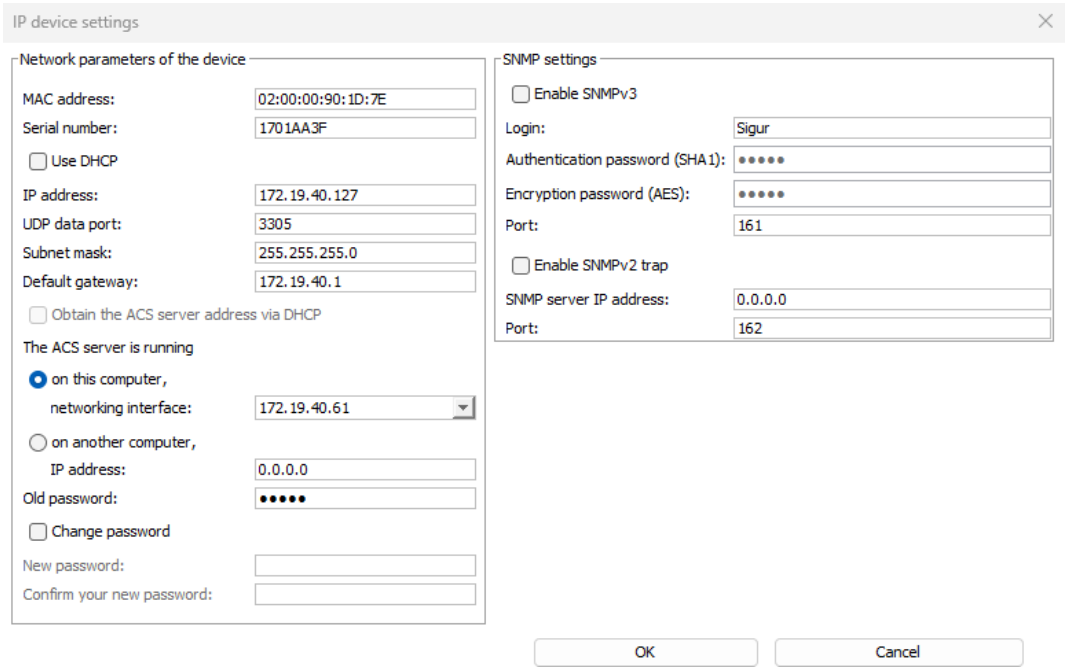
By default, the option to obtain network settings via DHCP is enabled on the controller, and is automatically enabled after resetting the device's network parameters. If there is no DHCP server running on the network where the controller is located, the controller will automatically assign itself an IP address in the range 169.254.xxx.xxx (where "xxx" is a number from 1 to 254).



Example of controller network parameters when first connected to the network.

Controllers can be configured either to operate with amanually assigned static IP address or to obtain network parameters dynamically from a DHCP server. To manually configure the controller's network parameters, follow these steps:

1. Select the controller from the list and click the "Edit the parameters" button.
2. In the window that appears, deselect the "Use DHCP" and "Obtain the ACS server address via DHCP" options.
3. Set the IP address, subnet mask, and default gateway manually.
4. Specify where the Sigur server is running: on this PC (select the network interface address on this computer) or on another PC (enter the IP address of the server).
5. Enter the password for changing the controller's network settings (default is "sigur", without quotation marks) and click "OK".



Static IP parameters.

5.2. Obtaining network parameters via DHCP

To enable the controller to obtain network parameters via DHCP, proceed as follows:

1. Start the "Server Administration" tool on a computer on the same subnet as the controller.
2. Go to the "Device configurations" tab.
3. Select the controller from the list and click the "Edit the parameters" button.
4. Enable the "Use DHCP" option and, if necessary, "Obtain the ACS server address via DHCP" option. The manual entry fields for the network settings become inactive.
5. Enter the password to access the controller's network settings (default is "sigur", without quotation marks) and click "OK".

In general, no additional configuration is required on the DHCP server to assign network parameters to the devices.

If the controller is also to obtain the Sigur server's IP address via DHCP, ensure the following:

- When the DHCP server receives a request for an IP address in which option 60 has the value "Sigur PACS Unit" (without quotation marks), it sends 4 bytes of the Sigur server's IP address in option 43, suboption 1 of the response.
- If the controller firmware version is 16 or lower, the DHCP server should send the Sigur server's IP address in reverse byte order.

For example, if it is necessary to provide the controller with the Sigur server's IP address 172.19.40.10, the value of option 43 should be (HEX) 0104AC13280A, where:

- 01: Suboption number.
- 04: Length of the transmitted payload.
- AC13280A: The Sigur server's IP address, as (HEX) AC 13 28 0A = (DEC) 172 19 40 10.

The DHCP options used by Sigur controllers.

Option number	Option value	Note
1	Subnet mask	The subnet mask of the network where the controller is located.
3	Default gateway IP address	The IP address of the router that provides access to the Internet or to another network where the Sigur server is located.
43	Manufacturer-specific information	This field is used to specify the Sigur server's IP address. The DHCP server should return this information in suboption 1.
60	Vendor ID	= Sigur PACS Unit.

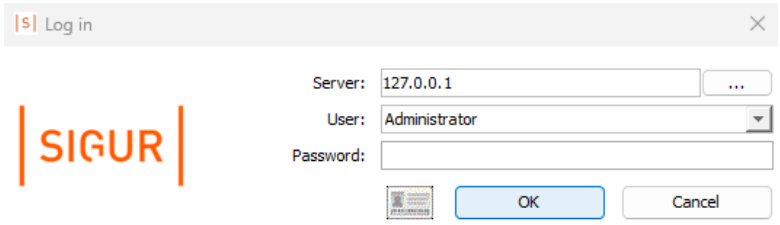
6. Client tool

The "Client" tool is designed to manage the access control system, manage the cardholder database, generate system reports, etc.

6.1. First launch of the Client tool

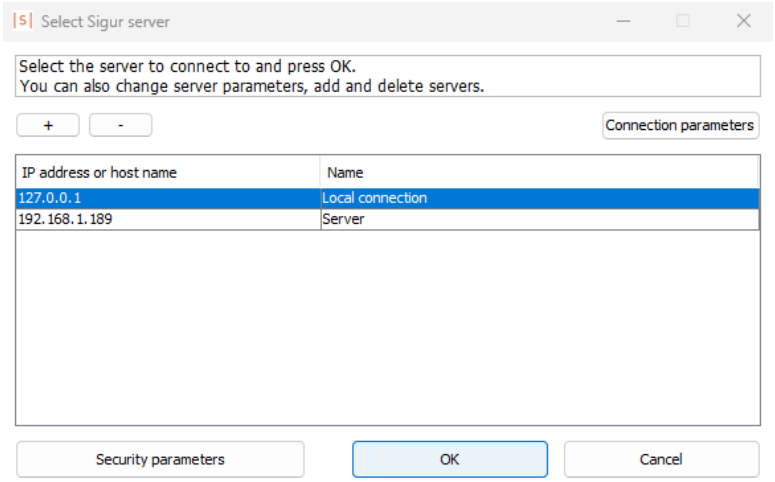
The application is started using the "Client" shortcut. You can find it in the Start menu under "All apps" –> "Sigur Access Management".

When the "Client" tool is started for the first time, it tries to connect to the server running on the local computer. If the connection is successful, the "Log in" dialogue box appears. Select the user name ("Administrator") and click "OK". By default, no password is set for the "Administrator" user. This can be configured later.



"Login" window.

If the "Client" tool fails to connect to a server on this computer, it will prompt you to connect to another server. If the server is deployed on another computer, you can add its IP address by clicking the "..." button next to the "Server" field.



Select Sigur server" window.

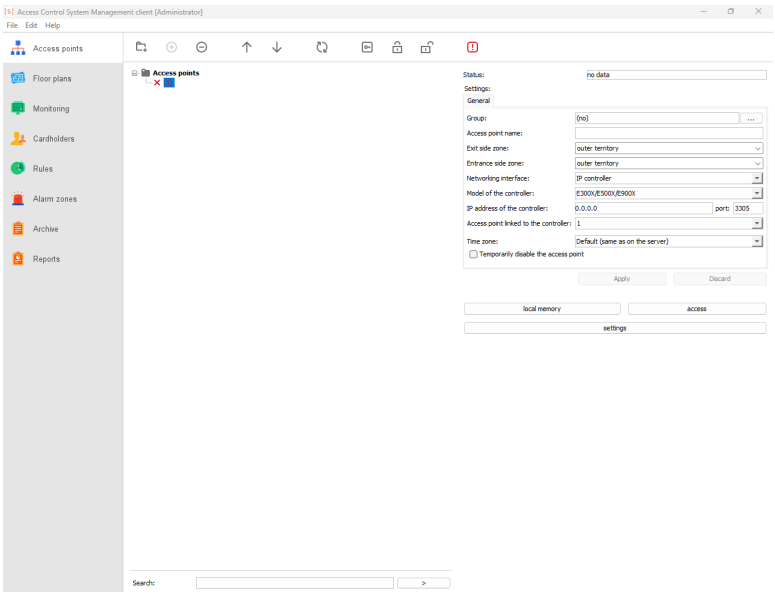
In the opened "Select Sigur server" window, add a server by clicking the "+" button. Enter its domain name/IP address and give it a name (optional). To remove a server, select it from the list and click the "-" button.

Once the server address has been added, select it from the list and click "OK".

6.2. Client tool main window

Once you have successfully connected to the server, the "Client" tool will open. The "Access points" tab is the first tab you see when you start the tool. The title bar displays the application title "Access Control System Management client" and the name of the current user.

All functions of the "Client" tool are divided into several tabs, with tab selection buttons located on the left side of the window. To switch to another tab, click on the corresponding button. The button for the currently open tab is highlighted.

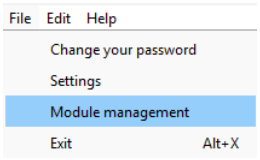


First launch of the "Client" tool.

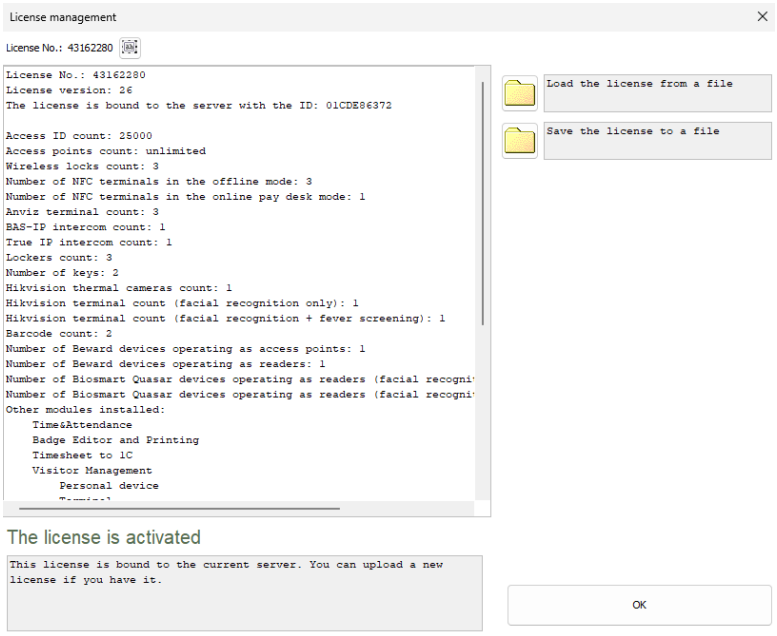
7. Software licensing

Each module of the Sigur software is subject to a license. All licensed software modules are integrated into a single software interface. If required, the functionality of the system can be extended by adding new modules to the already installed license.

If the Sigur server cannot detect a license, only basic functionality and management of a single access point (a free module) will be available. To view information about the current license, start the "Client" tool and go to the "File" –> "Module management" menu.



"File" –> "Module management" menu.



"License management" window.

7.1. Downloading and activating the software license

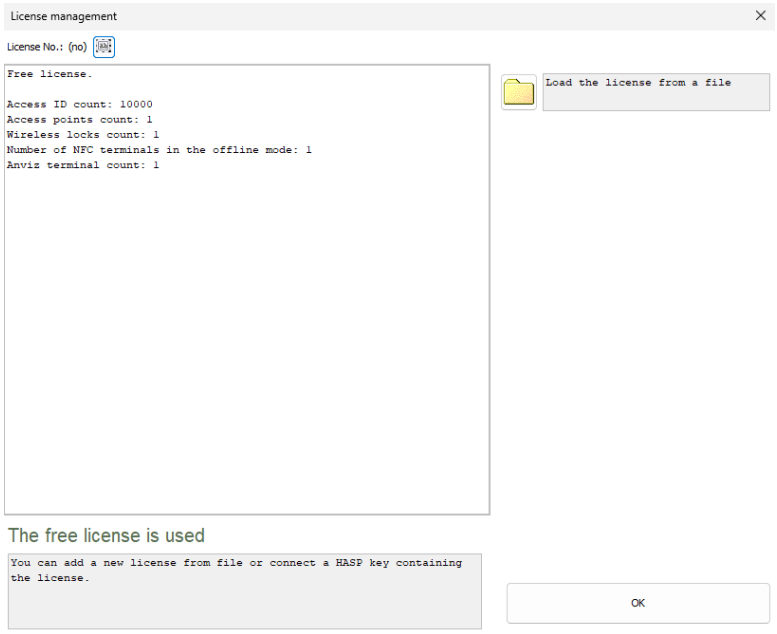
After purchasing the license, the buyer receives a file named «license_number_1.lic».

To upload the license, follow these steps:

1. Start the "Client" tool and connect to the Sigur server where you want to

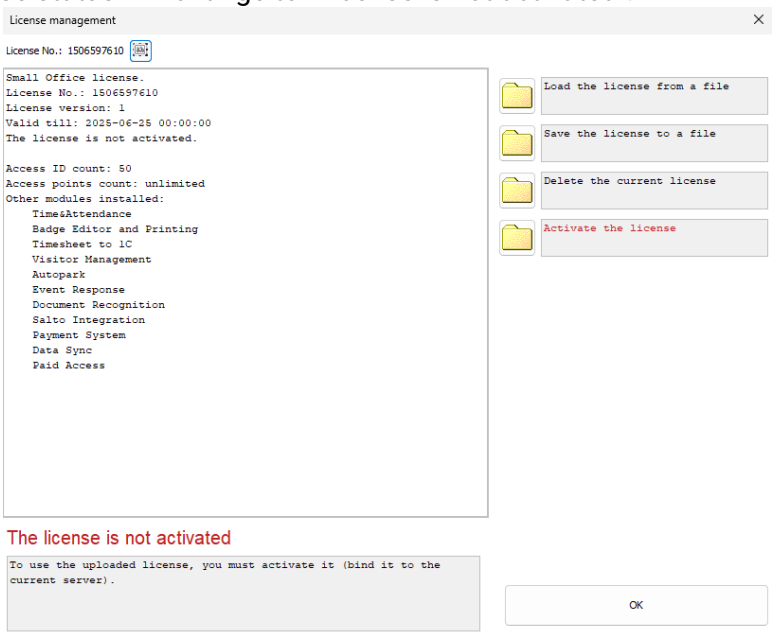
activate the license. If the Sigur server is deployed on a local PC, connect to "localhost".

2. Go to the "File" –> "Module management" menu. The software comes with a free license by default.



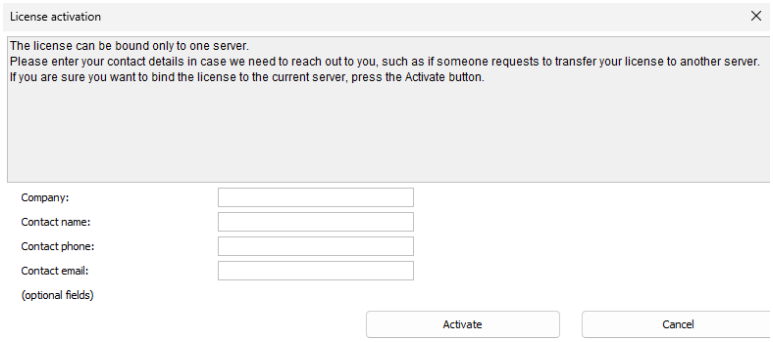
Free license.

3. Click the "Load the license from a file" button.
4. Select the license file in the window that opens and click the "Open" button. The license status will change to "License is not activated".



"License is not activated" message.

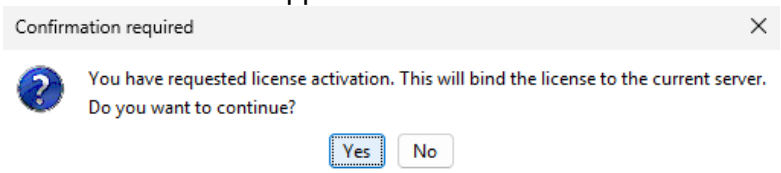
5. Click the "Activate the license" button. The license activation window opens.



"License activation" window.

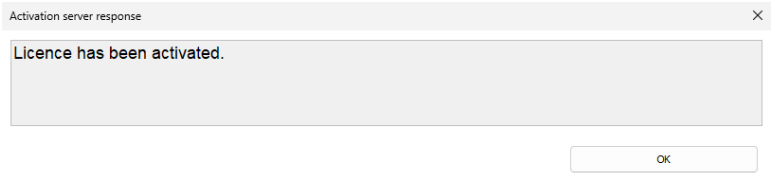
Fill in the contact details of the license end user and click the "Activate" button.

6. Click "Yes" in the window that appears.



"Confirmation required" window.

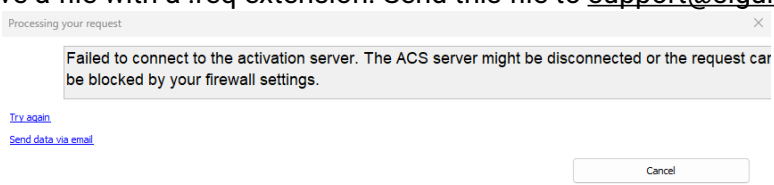
7. After clicking "Yes", an attempt will be made to automatically connect to the Sigur License Activation Server. If the connection is successful, an information message is displayed.



"Activation server response" window.

The license status will change to "License is activated".

8. If for some reason you are unable to connect to the Sigur License Activation Server, you can activate your license manually. To do this, click on the "Send data via email" link in the window that opens. A dialogue box will appear asking you to save a file with a .req extension. Send this file to support@sigur.com.



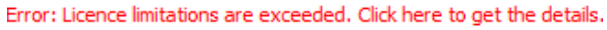
"Processing your request" window.

You will receive an email with a new license file (.lic) once this email has been

processed. This file must be uploaded to the server by clicking the "Load the license from a file" button in the "License Management" window. The license status will change to "License is activated".

9. Restart the "Client" tool.

The license is bound to the configuration of the PC where the Sigur server is deployed. If any violations are detected in the installed license, a corresponding message will be displayed at the bottom of the "Client" tool window. Clicking on the message will open a window with more detailed information.



"License limit is exceeded" message.

7.2. Transferring a license to another server

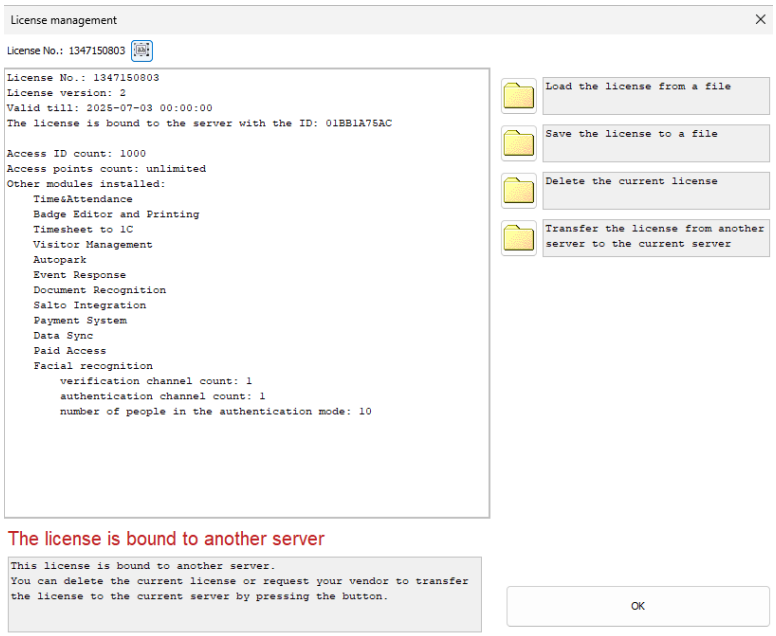
To transfer a license to another server, both servers must be connected to the Internet. If either server is not connected, the license transfer must be performed manually by sending control files by email to the technical support address support@sigur.com.

To transfer the license to a new server, do the following:

1. Start the "Client" tool on the PC where the old Sigur server is deployed. Go to the "File" –> "Module management" menu and click "Save the license to a file" button. Save the file and transfer it to the new server.

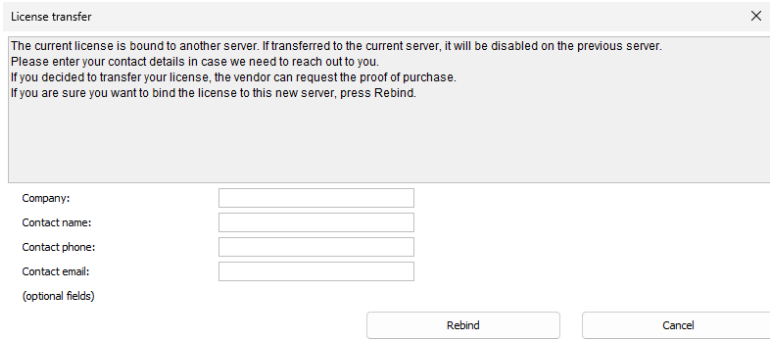
2. On the new server, similarly go to "File" –> "Module management" menu and click the "Load the license from a file" button. Load the file created in step 1.

3. Once the license file has been loaded, the license status on the new server will change to "License is bound to another server". Click the "Transfer the license from another server to the current server" button.



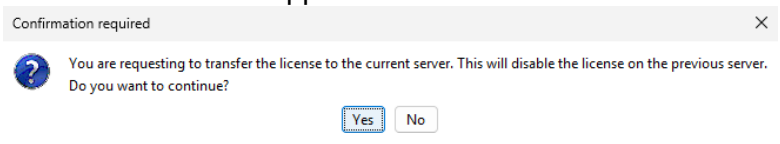
"License is bound to another server" message.

4. In the "License transfer" window, enter the contact details of the end user of the license and click "Rebind".



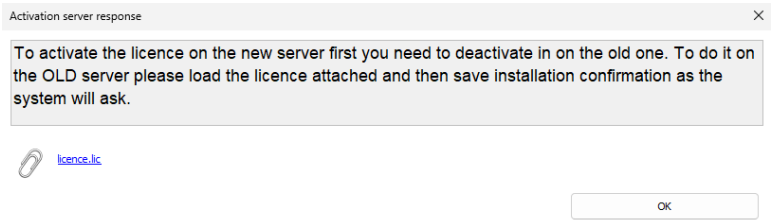
"License transfer" window.

5. Click "Yes" in the window that appears.



"Confirmation required" window.

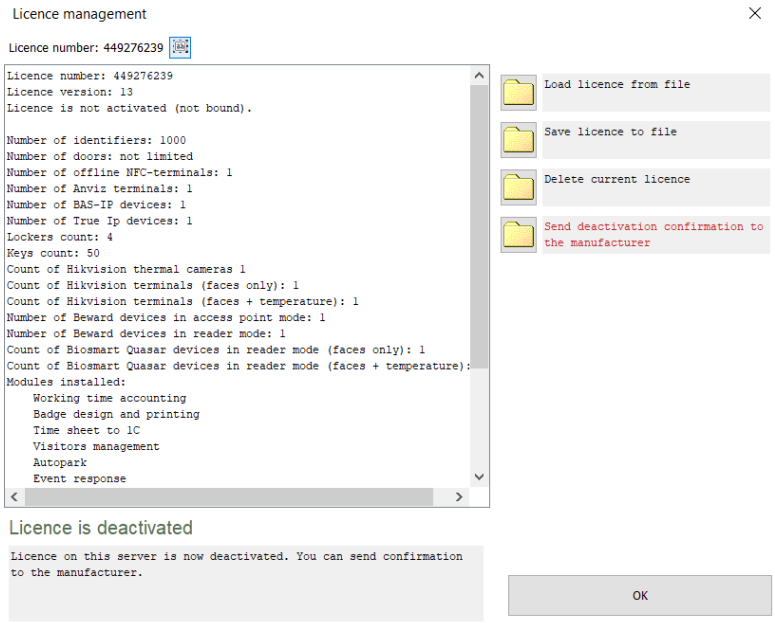
6. After clicking "Yes", an attempt will be made to automatically connect to the Sigur License Activation Server. If the connection is successful, an information message is displayed. Save the attached license file and transfer it to the old server.



"Activation server response" window.

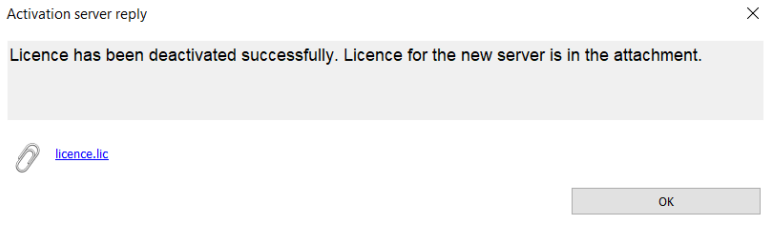
If for some reason you are unable to connect to the Sigur License Activation Server, click the "Send data via email" link in the window that opens. A dialogue box will appear asking you to save a file with a .req extension. Send this file to support@sigur.com. You will receive an email with a control file (.lic) once this email has been processed. Transfer this file to the old server.

7. On the old server, go to the "File" –> "Module management" menu and click the "Load the license from a file" button. Then select the file created in step 6. The license status on the old server will then change to "License is deactivated".



"License is deactivated" message.

8. Next, click the "Send deactivation confirmation to the manufacturer" button to inform Sigur about the license transfer. If the connection to the Sigur License Activation Server is successful, the following message is displayed. Save the attached license file.



"Activation server reply" window.

If for some reason you are unable to connect to the Sigur License Activation Server, click the "Send data via email" link in the window that opens. A dialogue box will appear asking you to save a file with a .req extension. Send this file to support@sigur.com. You will receive an email with a new license file (.lic) once this email has been processed.

At this point, the work with the old server is finished.

9. On the new server, go to the "File" –> "Module management" menu. Load the file created in step 8 by clicking the "Load the license from a file" button.

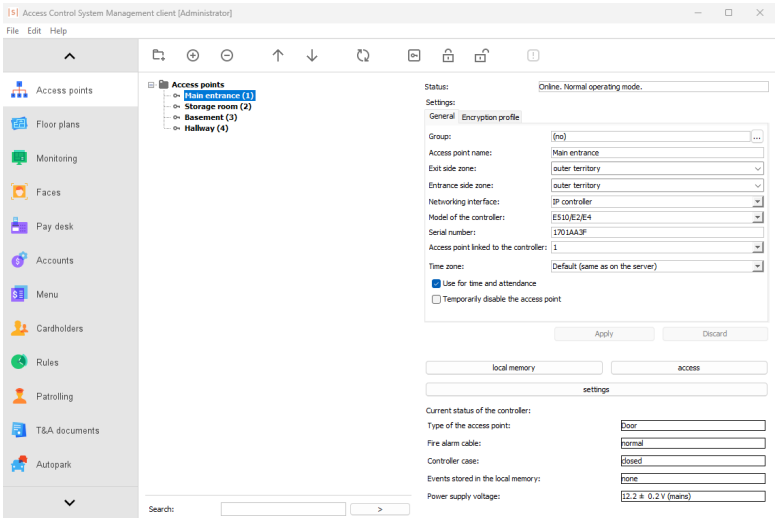
10. Restart the "Client" tool on the new server. The license has been successfully transferred.

8. Access points

The "Access points" tab is used for access point management and controller configuration.

An access point can be any access control device (door, turnstile, gate, etc.), or it can be no access control device, for example if the access point is used to register system events.

All access points in the system are listed with their name, communication status and overall status. There are buttons at the top of the window to create a new group of access points and to add or remove access points associated with a particular controller.



"Access points" tab.

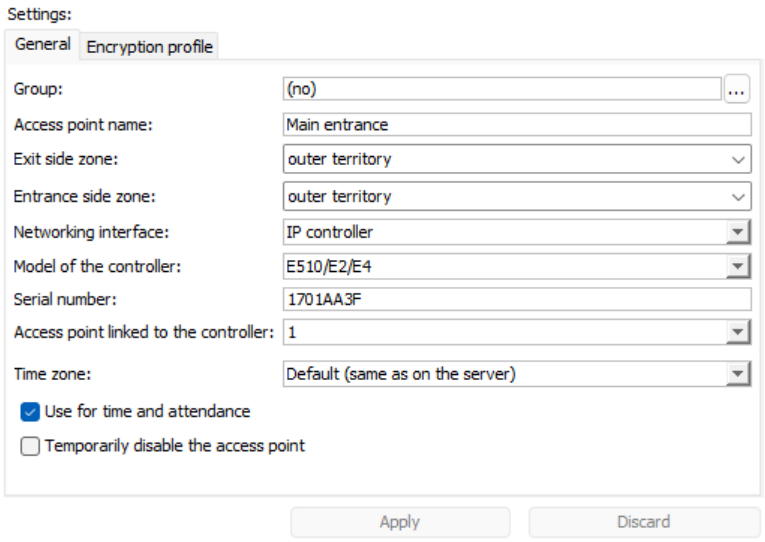
8.1. Establishing connection with access points of a controller

After installing the software, there is already an access point on the "Access points" tab with no configuration set. Let's configure it to manage an access control device. First, you need to associate the access point with a controller and establish a connection.

Select the access point in the list. In the "Settings" –> "General" block on the right side of the window, configure the following parameters:

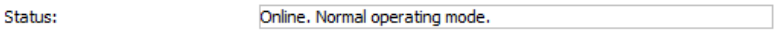
1. Enter any name for the access point.
2. In the "Networking interface" dropdown list, select "IP controller".
3. In the "Model of the controller"dropdown list, select "E510/E2/E4".
4. Enter the serial number of the controller.
5. In the "Access point linked to the controller" dropdown list, select 1.

6. Click the "Apply" button.



General settings of an access point.

The access point status changes to "Online".

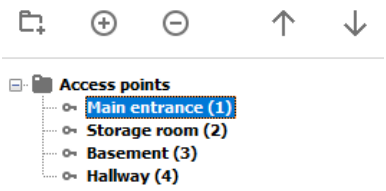


Connection status.

The necessary and sufficient condition for establishing a connection with access points is to ensure bidirectional data exchange between the Sigur server and the Sigur controller via UDP port 3305 (by default).

The number of access points on the "Access points" tab should correspond to the number of access control devices connected to the controllers. You can connect up to four access control devices to Sigur E510 and E4 controllers and up to two devices to the Sigur E2 controller.

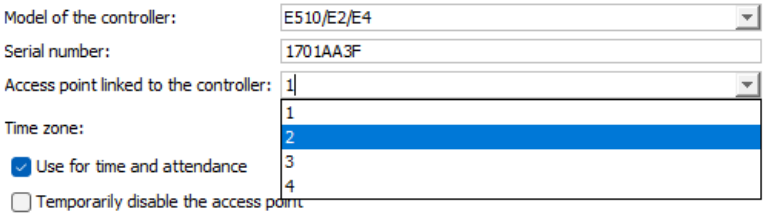
To create new access points, click the "+" button on the top toolbar of the "Access points" tab. If the "+" button is not active, it could be that you are using a free license.



Access points list.

For each access point, do the following:

1. Enter the serial number of the controller.
2. If there are several access points corresponding to one controller, number them in sequence in the "Access point linked to the controller" parameter, starting from 1.



"Access point linked to the controller" dropdown list.

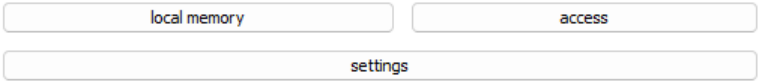
Let's consider the following case:

You have two controllers 150XXXXX and 160XXXXX . You have connected two doors to 150XXXXX and gates to 160XXXXX. In this case, you will need to create 3 access points and make the following settings:

Door 1	Door 2	Gates
Serial number: 150XXXXX.	Serial Number: 150XXXXX.	Serial Number: 160XXXXX.
Access point linked to the controller: 1.	Access point linked to the controller: 2.	Access point linked to the controller: 1.

8.2. Configuring a controller to manage access points

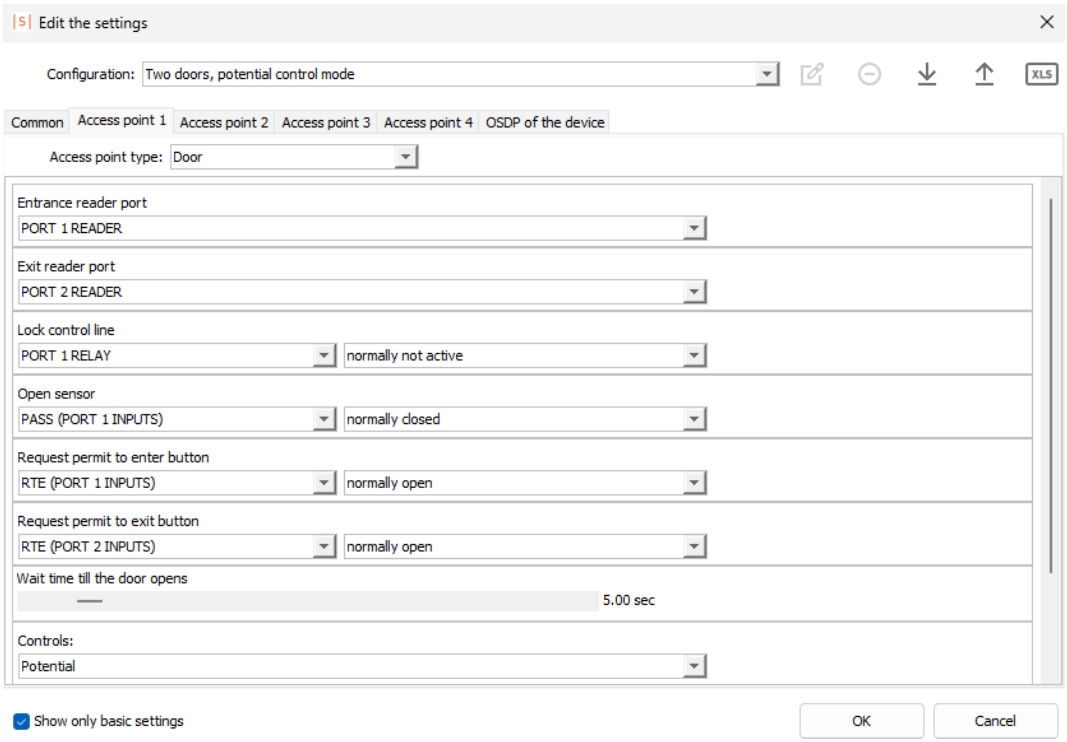
Once the connection to the access point has been established, it is necessary to configure the inputs and outputs of the controller. To do this, go to the "Doors" tab, select the access point from the list and click the "Settings" button.



"Settings" button.

In the window that opens, you can assign different functions to the controller's terminals. To view the full list of settings, clear the "Show only basic settings" checkbox.

We recommend that you use one of the default configurations to manage access control devices. To do this, click on the dropdown menu in the "Configuration" section and select the appropriate option.



"Settings edition" window.

The set of default configurations may vary depending on the controller model.

Default configurations for access points.

Configuration name	Description	E2	E4	E510
Time and attendance terminal	The controller operates as a single "Time and attendance" terminal, recording time of entry and exit. Management of access control devices is not available.	✓		
Two time and attendance terminals	The controller operates as two "Time and attendance" terminals, recording time of entry and exit. Management of access control devices is not available.		✓	✓
Door, potential control mode	The controller manages one access point of the "Door" type: a door fitted with a potential- or pulse-controlled lock.	✓		
Door, pulse control mode				
Two doors, potential control mode	The controller manages two access points of the "Door" type: two doors fitted with potential- or pulse-controlled locks.	✓	✓	✓
Two doors, pulse control mode				
Four doors, potential control mode	The controller manages four access points of the "Door" type: four doors fitted with potential- or pulse-controlled locks. Each door is equipped with an entry reader and an exit button.		✓	✓
Four doors, pulse control mode				
Turnstile, potential control mode	The controller manages one access point of the "Turnstile" type: one potential- or pulse-controlled turnstile.	✓	✓	✓
Turnstile, pulse control mode				
Two turnstiles, potential control mode	The controller manages two access points of the "Turnstile" type: two potential-controlled turnstiles.		✓	✓

Configuration name	Description	E2	E4	E510
Arm barrier / gate, Open, Close, Stop logic	The controller manages one access point of the "Gates" type in "Open, Close, Stop" or "Direct Control" logic.		✓	✓
Arm barrier / gate, Direct Control logic				

Barrier mechanisms (turnstiles, gates, etc.) typically have one or more control inputs. Pulse-controlled devices require a short pulse signal on the corresponding input in order to execute a command. Potential-controlled devices require a continuous signal on the corresponding input for the entire duration of the command.

In general, door locks can be controlled by applying or removing power. Electromagnetic locks, for instance, require continuous power to remain locked, whereas electric strikes require only a brief pulse of power to unlock. For example, if you need to configure the E510 controller to manage one or two doors with electromagnetic locks, select the "Two doors, potential control mode" default configuration. If you need to connect one or two electric strikes to the controller, select the "Two doors, pulse control mode" configuration.

You can also make any necessary changes to the configuration manually.

The description of the final controller configuration can be exported to an .xls file and used when connecting devices to the controller. To save the settings file, click the "XLS" button at the top of the "Edit the settings" window.

Toolbar of the "Edit the settings" window.

8.3. Connecting devices to a controller

8.3.1. Door with electromagnetic lock

Let's explore the process of connecting devices and configuring Sigur E510, E2 and E4 controllers to manage two doors with electromagnetic locks.

To control the devices, select the "Two doors, potential control mode" default configuration.

Wiring diagrams for connecting doors and other devices to Sigur controllers are included in the appendix to this manual.

Connecting electromagnetic locks.

The locks are controlled by relays on the controller board. The relays are assigned the function "Lock control line, normally not active".

Controller terminals for lock connection.

Controller model	Door	Terminal for lock connection
E510	1st door	K1
	2nd door	K3
E2	1st door	PORT 1 RELAY
	2nd door	PORT 2 RELAY
E4	1st door	PORT 1 RELAY
	2nd door	PORT 3 RELAY

Connecting readers.

The PORT terminals are used to connect readers via the Wiegand interface.If the reader's supply voltage matches the controller's supply voltage (10...15 V) and the maximum current consumption per port does not exceed 200 mA, you can connect the reader's supply lines to the controller's VR+ and GND terminals (or PWR and GND for E2/E4 controllers).

Controller terminals for reader connection.

Controller model	Door	Reader direction	Terminal for reader connection
E510	1st door	Entry	PORT 1
	1st door	Exit	PORT 2
	2nd door	Entry	PORT 3
	2nd door	Exit	PORT 4
E2	1st door	Entry	PORT 1 READER
	1st door	Exit	None, exit by pressing the exit button
	2nd door	Entry	PORT 2 READER
	2nd door	Exit	None, exit by pressing the exit button
	1st door	Entry	PORT 1 READER
	1st door	Exit	PORT 2 READER

Controller model	Door	Reader direction	Terminal for reader connection
E4	2nd door	Entry	PORT 3 READER
	2nd door	Exit	PORT 4 READER

In case of using OSDP readers, please refer to the corresponding section.

Connecting an entry sensor.

An entry sensor detects when someone passes through the door. The function assigned to the terminal is "Open sensor, normally closed".

If an entry sensor is not installed, it is necessary to indicate its absence. To do this, go to the "Doors" tab, select the access point and click the "Settings" button. In the window that opens, select the "not connected, always active" status for the "Open sensor" function and click "OK". The system will now consider this door as always open. Therefore, after the settings have been applied, the system will record the "Break-in" event once. This is OK as we have told the system that the door is open.

The system will now record a "Pass through an open door" event immediately after the card is presented to the reader.

Controller terminals for entry sensor connection.

Controller model	Door	Terminal for entry sensor connection
E510	1st door	D1
	2nd door	D2
E2	1st door	PASS (PORT 1 SENSORS)
	2nd door	PASS (PORT 2 SENSORS)
E4	1st door	PASS (PORT 1 INPUTS)
	2nd door	PASS (PORT 3 INPUTS)

Connecting an exit button.

It is also possible to use a push-button to unlock the door. The function assigned to the terminal is "Request permit to exit button, normally open". You can manually change the normal state of the connected push-button in the controller settings.

Controller terminals for exit button connection.

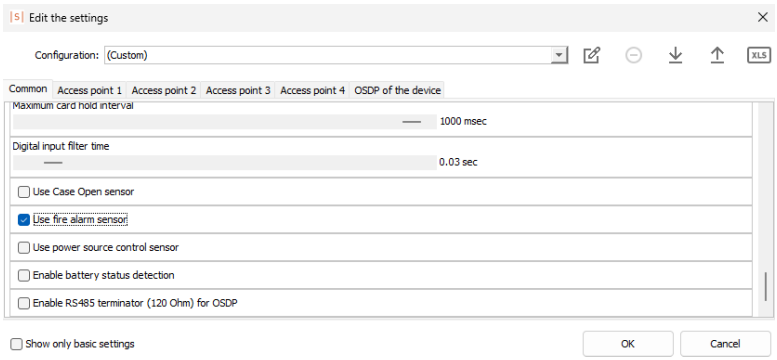
Controller model	Door	Terminal for exit button connection
E510	1st door	D4
	2nd door	D7
E2	1st door	RTE (PORT 1 SENSORS)
	2nd door	RTE (PORT 2 SENSORS)
E4	1st door	RTE (PORT 2 INPUTS)
	2nd door	RTE (PORT 4 INPUTS)

Connecting an emergency release button.

It is also possible to connect a normally closed emergency release button to a Sigur controller. When the button is pressed, the controller goes into "Fire!" mode and all access points on the controller are unlocked.

The wiring diagram for an emergency release button can be found in the appendix to this manual.

The emergency release function is disabled by default. When connecting the emergency door release button, go to the "Doors" tab, select any access point of a particular controller in the list and click the "Settings" button. In the "Edit the settings" window, go to the "Common" tab, clear the "Show only basic settings" checkbox and enable the "Use fire alarm sensor" function.



"Use fire alarm sensor" function.

8.3.2. Turnstile

Let's look at connecting devices and configuring Sigur E510, E2 and E4 controllers to manage a single level-controlled turnstile.

To control the devices, select the "Turnstile, potential control mode" default configuration. Wiring diagrams for connecting turnstiles and other equipment to Sigur controllers can be found in the appendix to this manual.

Connecting a turnstile.

The control lines of the turnstile are connected to the relays on the controller board, with the relays assigned the function "Unlock for entry/exit control line, normally not active".

Controller terminals for connecting a turnstile control line.

Controller model	Direction	Terminal for connecting a turnstile control line
E510	Entry	K1
	Exit	K2
E2, E4	Entry	PORT 1 RELAY
	Exit	PORT 2 RELAY

Connecting readers.

The PORT terminals are used to connect readers via the Wiegand interface.If the reader's supply voltage matches the controller's supply voltage (10...15 V) and the maximum current consumption per port does not exceed 200 mA, you can connect the reader's supply lines to the controller's VR+ and GND terminals (or PWR and GND for E2/E4 controllers).

Controller terminals for reader connection.

Controller model	Direction	Terminal for reader connection
E510	Entry	PORT 1
	Exit	PORT 2
E2, E4	Entry	PORT 1 READER
	Exit	PORT 2 READER

In case of using OSDP readers, please refer to the corresponding section.

Connecting optical sensors.

An optical sensor detects when someone passes through the turnstile. The turnstile can have one or two sensors of different types. The "Turnstile sensor type"

parameter determines how the output signals from the turnstile sensors are processed.

Logic used to process the output signals from turnstile sensors.

Name	Description
Simplified interface	Two sensors detect when someone passes through the turnstile in either direction.
Sensor broadcasting	Two sensors detect when someone passes through the turnstile in either direction, and they trigger one after the other.
Single wire interface	One sensor detects when someone passes through the turnstile in either direction.

In the default configuration "Turnstile, potential control mode", the default sensor interface type is "Simplified interface", which can be changed in the controller settings. If your turnstile has a single sensor, assign the "Single access control sensor line" function to the selected terminal of the Sigur controller.

The default configuration expects normally closed sensors to be connected. You can manually change the normal state of the connected sensors in the controller settings.

Controller terminals for optical sensor connection.

Controller model	Direction	Terminal for optical sensor connection
E510	Entry	D1
	Exit	D2
E2	Entry	PASS (PORT 1 SENSORS)
	Exit	PASS (PORT 2 SENSORS)
E4	Entry	PASS (PORT 1 INPUTS)
	Exit	PASS (PORT 2 INPUTS)

Connecting a control panel.

The turnstile control panel must also be connected to the Sigur controller. If the control panel is connected directly to the turnstile control board, Sigur ACS will consider all entries authorized by the control panel as intrusions.

In the default configuration, it is expected that the control panel's normally open buttons are connected to the Sigur controller. You can manually change the normal state of the connected buttons in the controller settings.

Controller terminals for control panel connection.

Controller model	Button function	Terminal for control panel button connection
E510	Entry	D3
	Exit	D4
	Block	D5
E2	Entry	RTE (PORT 1 SENSORS)
	Exit	RTE (PORT 2 SENSORS)
	Block	IN1
E4	Entry	RTE (PORT 1 INPUTS)
	Exit	RTE (PORT 2 INPUTS)
	Block	IN1 (INPUTS)

Connecting an emergency line.

If the turnstile is equipped with an emergency input, connect this line to the terminals of the Sigur controller. The function assigned to the terminal is "Door Unlocked indication line, normally not active", which is activated in the event of a fire alarm or when the access point is unlocked using the "Client" tool. The turnstile is expected to unlock and allow free passage when it receives a signal on this line.

Controller terminals for emergency line connection.

Controller model	Terminal for emergency line connection
E510	K4
E2	OUT1
E4	PORT 4 RELAY

Connecting an emergency release button.

Additionally, it is also possible to connect a normally closed emergency release button to a Sigur controller. When the button is pressed, the controller goes into "Fire!" mode, all access points on the controller are unlocked and the "Door

Unlocked indication line" is activated.

To connect the emergency release button, you can use the instructions in the "Connecting an emergency release button " section.

Switching to pulse control mode.

In this section we have considered the connection of devices to the controller in the "Turnstile, potential control mode" default configuration. For a pulse-controlled turnstile, select the "Turnstile, pulse control mode" default configuration.

In this case, the devices are connected to the controller in a similar way to the potential-controlled turnstiles, with the addition of a "Lock control line". Sigur controllers activate this line to block the turnstile when a person successfully passes through an access point or when the waiting period ends after the card has been presented to the reader.

Controller terminals for "Lock control line" connection.

Controller model	Terminal for "Lock control line" connection
E510	K3
E2	OUT1 (the emergency line is not connected)
E4	PORT 3 RELAY

8.3.3. Barriers and gates

Let's consider the connection of devices and the configuration of Sigur E510 and E4 controllers to manage a single barrier in pulse mode. The default configuration of the Sigur E2 controller does not include barrier or gate control.

Wiring diagrams for connecting barriers, gates and other devices to Sigur controllers can be found in the appendix to this manual. For barrier/gate control, two control logics are available in the system.

Barrier/gates control logics.

Name	Description
Arm barrier / gate, "Open, Close, Stop logic"	The barrier is controlled by sending short pulses. Before sending the "Open" or "Close" commands, a "Stop" command is always sent so that the subsequent reaction of the barrier/gate drive is unambiguous.
Arm barrier / gate, "Direct control logic"	The barrier is controlled by keeping the Sigur controller's relay energized throughout the movement of the barrier arm/leaf.

Let's select the "Arm barrier / gate, "Open, Close, Stop logic" default configuration.

Connecting barrier/gates.

The control lines of the barrier or gates are connected to the relays on the controller board. The functions assigned to the terminals are "Open/Close/Stop line, normally not active".

Controller terminals for barrier or gates connection.

Controller model	Control line	Terminal for barrier or gates connection
E510	Stop line	K1
	Open line	K2
	Close line	K3
E4	Stop line	PORT 1 RELAY
	Open line	PORT 2 RELAY
	Close line	PORT 3 RELAY

Connecting vehicle detection sensors.

Vehicle detection sensors are used to detect vehicles and ensure safety, and the access control system uses them to register entry and exit events.

The sensors must be connected to the Sigur controller to avoid conflicts in control signals and loss of control of the barrier or gates.

The sensors on the entrance and exit sides of the barrier or gates are optional, while the central detection sensor under the barrier arm/leaf is mandatory. If you

want to use only the central sensor, clear the "Show only basic settings" checkbox and set the values for the "Vehicle detection sensor for entrance" and "Vehicle detection sensor for exit" functions to "not selected".

The default configuration expects normally closed sensors to be connected. You can manually change the normal state of the connected sensors in the controller settings.

Controller terminals for vehicle detection sensor connection.

Controller model	Vehicle detection sensor position	Terminal for sensor connection
E510	Outside car presence	D1
	Car presence on gate line	D2
	Inside car presence	D3
E4	Outside car presence	PASS (PORT 1 INPUTS)
	Car presence on gate line	PASS (PORT 2 INPUTS)
	Inside car presence	PASS (PORT 3 INPUTS)

Connecting readers.

The PORT terminals are used to connect readers via the Wiegand interface.If the reader's supply voltage matches the controller's supply voltage (10...15 V) and the maximum current consumption per port does not exceed 200 mA, you can connect the reader's supply lines to the controller's VR+ and GND terminals (or PWR and GND for E2/E4 controllers).

You can use one to three readers to manage the barrier or gates. The direction of passage through the barrier depends on which reader transmits the code to the controller.

When using a single reader ("Unknown direction reader port" line), two vehicle detection sensors are required on opposite sides of the barrier ("Vehicle detection sensor for entrance" and "Vehicle detection sensor for exit" lines) to determine the direction of passage through the barrier.

Controller terminals for reader connection.

Controller model	Direction	Terminal for reader connection
E510	Entry	PORT 1
	Exit	PORT 2
	Unknown direction (long range readers)	PORT 3
E4	Entry	PASS (PORT 1 INPUTS)
	Exit	PASS (PORT 2 INPUTS)
	Unknown direction (long range readers)	PASS (PORT 3 INPUTS)

In case of using OSDP readers, please refer to the instructions in the corresponding section.

Connecting a control panel.

The control panel of the barrier or gates must also be connected to the Sigur controller. In the default configuration, it is expected that the control panel's normally open buttons are connected to the Sigur controller. You can manually change the normal state of the connected buttons in the controller settings.

Controller terminals for control panel connection.

Controller model	Button function	Terminal for control panel button connection
E510	Start/Allow pass	D4
	Stop/Deny pass	D5
E4	Start/Allow pass	RTE (PORT 1 INPUTS)
	Stop/Deny pass	RTE (PORT 2 INPUTS)

Connecting an emergency release button.

Additionally, it is also possible to connect a normally closed emergency release button to a Sigur controller. When the button is pressed, the controller goes into "Fire!" mode and all access points on the controller are unlocked.

To connect the emergency release button, you can use the instructions in the

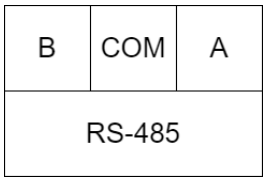
"Connecting an emergency release button" section.

8.3.4. OSDP readers

Sigur E2/E4 controllers are compatible with all readers that support OSDP v2.2. You can connect up to four readers to Sigur E2/E4 controllers via OSDP.

Connecting an OSDP reader.

OSDP readers are connected to Sigur E2/E4 controllers via the RS485 interface. The "RS-485" terminal block of a controller is used.



"RS-485" terminal block.

The communication cable is connected to terminals "A" (first wire of a twisted pair in the cable), "B" (second wire of the twisted pair in the cable) and "COM" (common wire). Any free wire in the cable except the screen could be used as the "COM" wire.

The "A" and "B" wires must be a twisted pair. Using wires from different twisted pairs is not allowed.

If more than one reader is connected to the line, you should use the "linear bus" topology. This means that all the devices connected to the cable must be connected sequentially, one after the other.

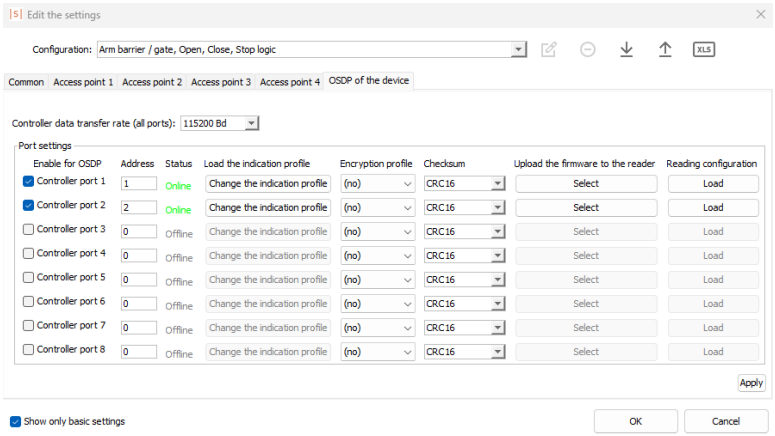
When connecting devices, it is necessary to ensure that the wires "A" and "B" of the communication line are clearly matched on the controller and on all the readers connected to this line. All the "A" ports must be connected via the same wire in the twisted pair and all the "B" ports must be connected via the second wire in the same twisted pair.

Wiring diagrams for connecting OSDP readers to Sigur E2/E4 controllers are included in the appendix to this manual.

Configuring controller.

When connecting readers via OSDP, it is necessary to define the network parameters for each reader in the controller settings. To do this, go to the "Access points" tab, select any access point of a Sigur E2/E4 controller from the list and

click the "Settings" button. In the window that opens, select the "OSDP of the device" tab. Here you can set the communication speed and configure the connection parameters for your readers and the logical ports of the controller.



"OSDP of the device" tab.

In the "Enable for OSDP" column, you can select which logical ports of the controller will be OSDP-enabled.

After enabling a logical port, it is necessary to do the following:

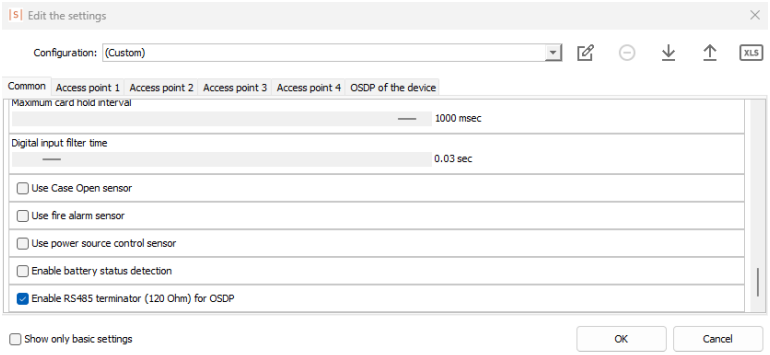
1. Enter the address of an OSDP reader on a line (valid range - 1 to 127). The address is set in the reader settings (see the reader manufacturer's manual). The settings for Sigur MR100 readers are described in the following subsection.
2. Select the way the checksum is calculated. This also depends on the reader settings. When using Sigur MR100 readers, select the default value - "CRC16".
3. Select the baud rate from the "Controller data transfer rate (all ports)" dropdown list. It should match the reader settings.
4. Click the "Apply" button. If the settings are correct, the port status will change to "Online".
5. Click "OK" to save the settings.

If a port is selected in the "Enabled" column, the controller's Wiegand port with the same number is automatically disabled.

If the controller is a terminating device on the RS-485 line, the terminating resistor must be activated. The line terminators on Sigur E2/E4 controllers are disabled by default, but can be enabled in the software. To do this, follow these steps:

1. Go to the "Access points" tab.
2. Select any access point of a particular Sigur E2/E4 controller from the list and click the "Settings" button.

3. Go to the "Common" tab and clear the "Show only basic settings" checkbox.
4. If the controller is the first or the last device on the RS-485 loop, select the "Enable RS485 terminator (120 Ohm) for OSDP" checkbox and click "OK" to save the settings.



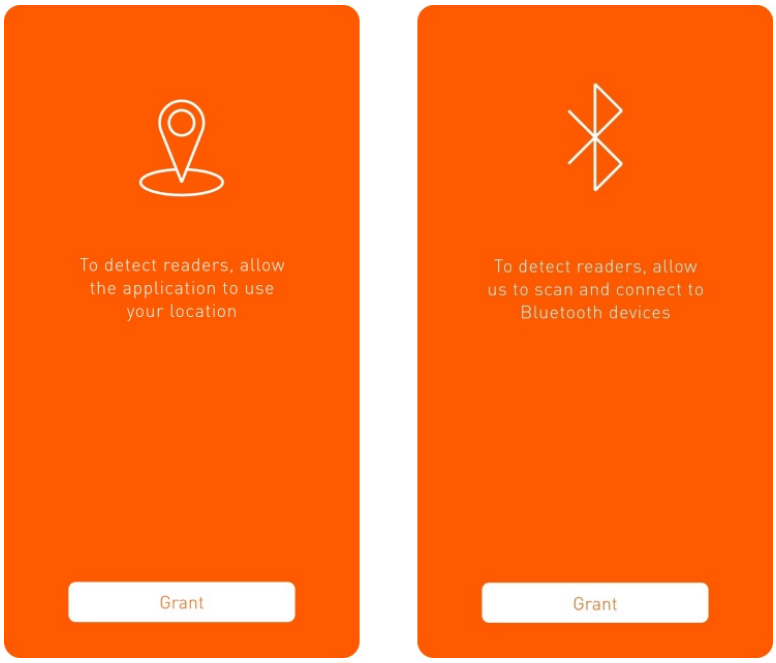
Enabling a RS-485 terminator.

Refer to the reader manufacturer's manual for information on enabling line terminators on readers. The following subsection describes the settings for Sigur MR100 readers.

Configuring Sigur MR100 readers.

By default, Sigur MR100 readers are configured for the Wiegand output interface. To set the OSDP output interface, follow these steps:

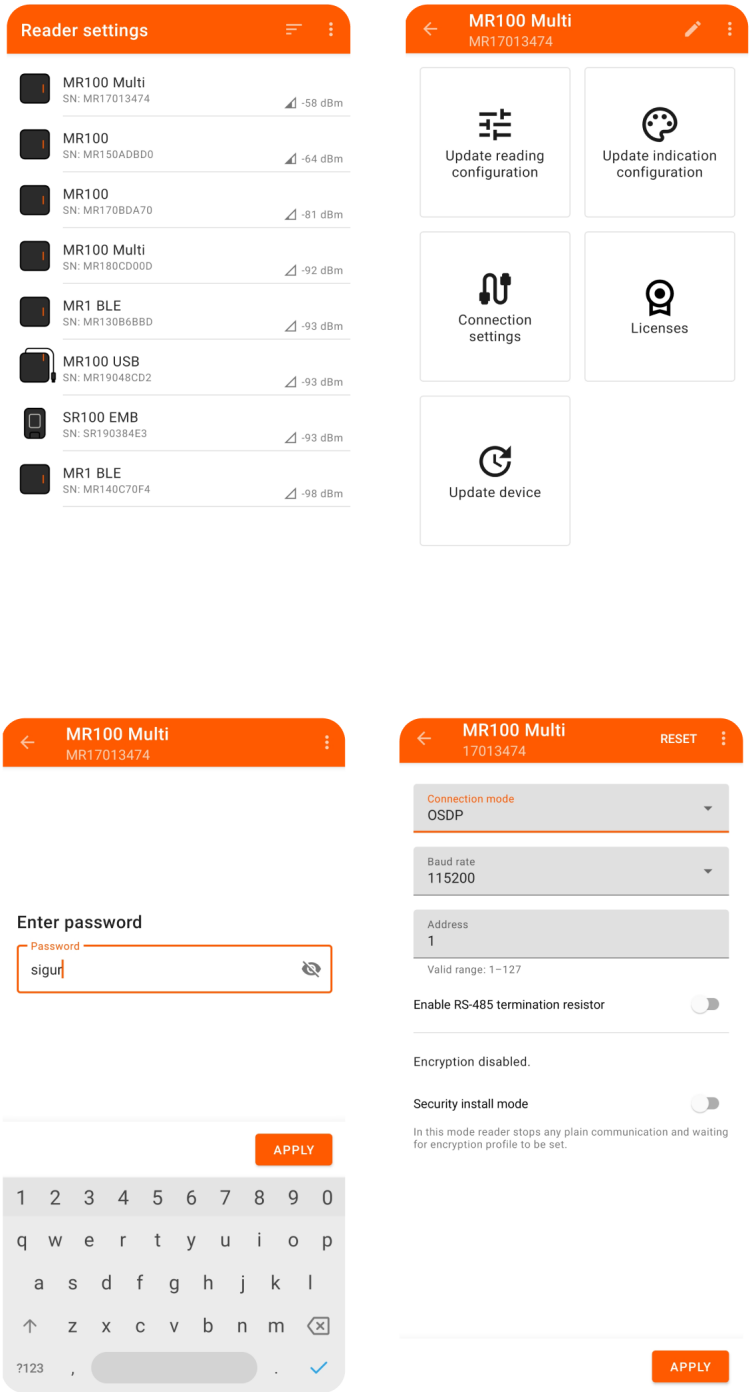
1. Turn on Bluetooth on your Android device (Android 5.0 or higher).
2. Install the "Sigur Readers Config" mobile application (Google Play, Huawei AppGallery) and open it.
3. The first time you run the application, grant it all the permissions it requests.



Mobile application permissions.

4. Select the reader from the list. You can select multiple readers in the list by long pressing.
5. Select "Connection settings" from the list of actions and enter the reader service password (the default password is "sigur", without quotation marks).
6. Select the OSDP connection mode from the dropdown list. It is also necessary to configure:

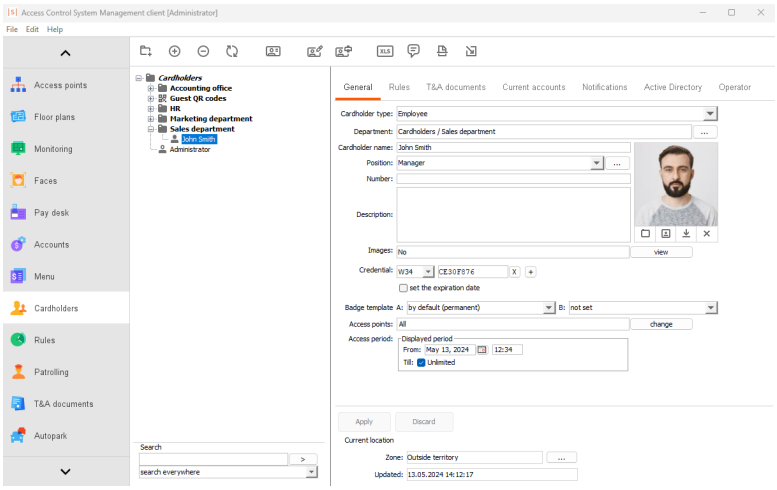
    1. "Baud rate" - the data transmission rate on the RS-485 line between the controller and the readers connected to it. Possible values: 9600, 19200, 38400, 57600, 115200 Bd.
    2. "Address" - unique address of the reader on the RS-485 line. Valid range: Integers from 1 to 127.
    3. "Enable RS-485 termination resistor" - enable this option if the reader is the first or the last device on the RS-485 loop.
    4. "Security install mode" - needs to be enabled to set the reader to encrypt OSDP data. Leave this option unchecked for now.
7. Tap "Apply" and wait for the settings to be uploaded to the reader. Once the upload is complete, the settings will be applied and there is no need to restart the reader.



Configuring Sigur MR100 readers.

9. Cardholder database management

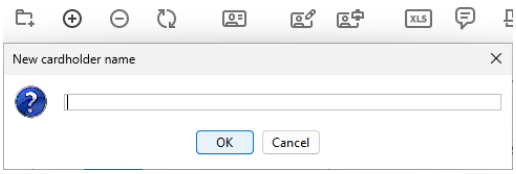
The "Cardholders" tab is used to manage the cardholder database. Here you can add and remove cardholders, create departments, restrict access to access points and more.



"Cardholders" tab.

9.1. Adding cardholders to the database

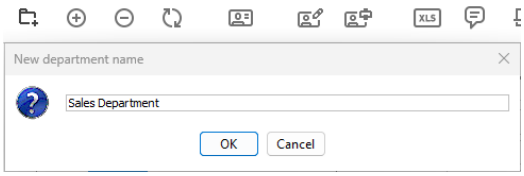
To add a new cardholder, click the "+" button on the top toolbar, enter the cardholder's name and click "OK".



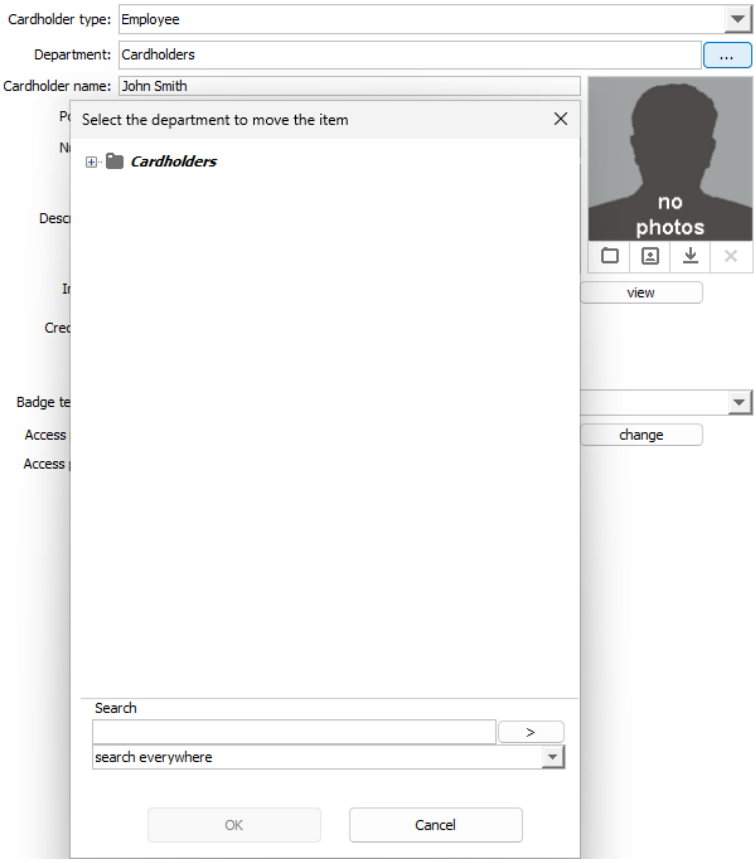
Adding a new cardholder.

After that, you can complete the remaining parameters of the cardholder's profile. In the "Cardholder type" field, the default value is "Employee", which is standard. There is no need to change this parameter in this example.

Next, you can choose the department to which the cardholder belongs. Create a "Sales Department" by clicking the "Add department to selected department" button. Then move the cardholder to the "Sales Department" by clicking the "..." button in the cardholder's profile.



Adding a new department.



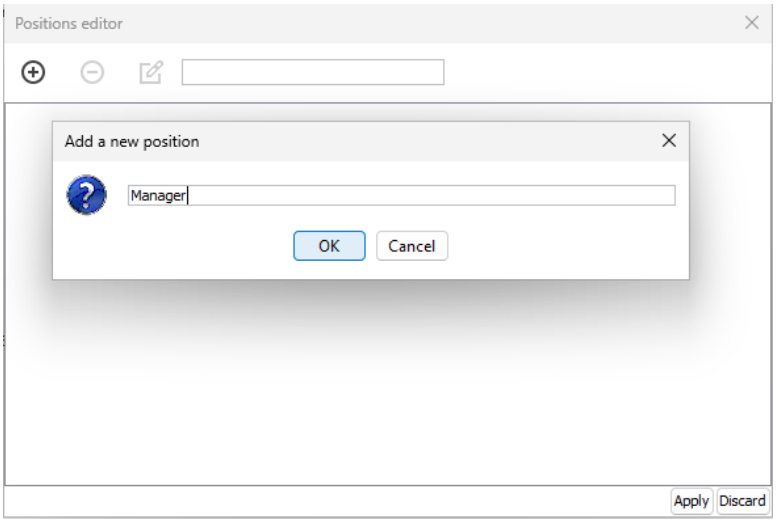
Moving the cardholder to another department.

You can then create cardholders directly in a specific department. To do this, select the department from the list and click the "+" button.

You can create a hierarchical structure of departments with an unlimited number of nested levels. To do this, select the parent department in the list and create the desired number of sub-departments by clicking the "Add a department to the selected department" button.

It is also possible to change the cardholder's position. Add a new position by clicking the "..." button in the cardholder's profile. In the "Positions editor" window, click the "+" button, enter the position name (e.g. "Manager"), click "OK" and then click "Apply". Assign the position to the cardholder using the dropdown list.

If there are many positions in the system, use the search function in the "Editing positions" window to find a specific position by its name.



Adding position.

The "Number" field is usually used to store the cardholder's personnel number or any other unique identifier.

You can also enter text of up to 255 characters in the "Description" field.

Now, let's add a personal photo for the cardholder. This can be done using a connected webcam by clicking the "Select from the camera" button or by uploading a photo in JPG, JPEG, GIF, PNG, or BMP format by clicking the "Select from file" button.

Adding a photo.

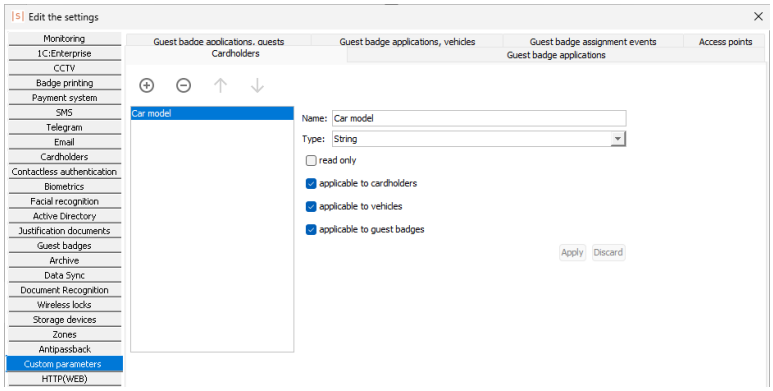
Click "Apply" to save the changes.

9.2. Creating custom fields

It is also possible to add an unlimited number of additional parameters to a cardholder profile. To do this, go to the "File" –> "Settings" menu in the "Client" tool.

In the "Settings" window, select the "Custom parameters" section and go to the "Cardholders" tab. Next, create a new custom field by clicking the "+" button, enter the name (e.g. "Car Model"), and click OK. For this custom field, set the "Type" to

"String" and select the "Employees related" checkbox.



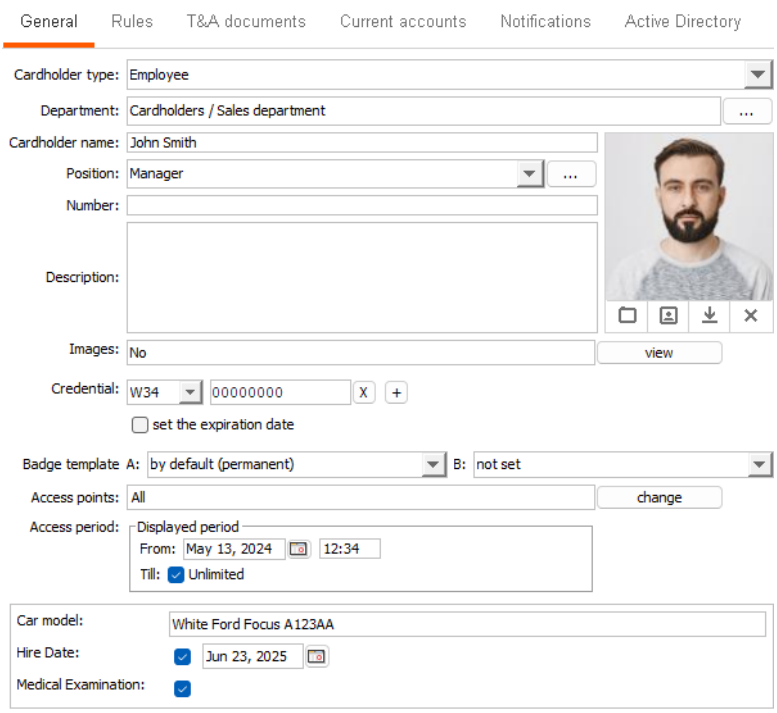
"File" –> "Settings" –> "Custom fields" –> "Cardholders" menu.

Click the "Apply" button and then click "OK" to confirm. A new field will now appear in the cardholder profile.

Similarly, let's create two more custom fields: "Hire Date" of type "Date" and "Medical Examination" of type "Boolean". Then go to the cardholder profile.

Different types of custom fields in the cardholder profile.

You can enter any value in the string custom field. To fill in the date type custom field, select the checkbox and enter the required date manually or select it by clicking on the calendar icon. The value of the boolean type custom field is logical (yes or no). You can either select or clear the checkbox.



Custom fields in a cardholder profile.

Click "Apply" to save changes to the cardholder profile.

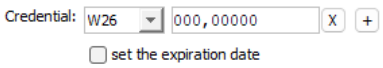
9.3. Adding cards

Now let's add an access code to a cardholder profile.

Cards, key fobs, radio frequency tags, etc. can be used as access credentials. Each cardholder can be assigned up to 5 different credentials. Please refer to the corresponding section if you wish to work with the secure memory area of Mifare cards.

There are three ways to add keys to the system:

1. You can manually enter its number in the "Credential" field. You can also change the format of the access code.

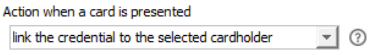


"Credential" field.

2. The access code can also be added using an integrated desktop USB reader. Use the ACR1252U for Mifare identifiers and the Iron Logic Z-2 USB for EM Marine identifiers.

   Proceed as follows:

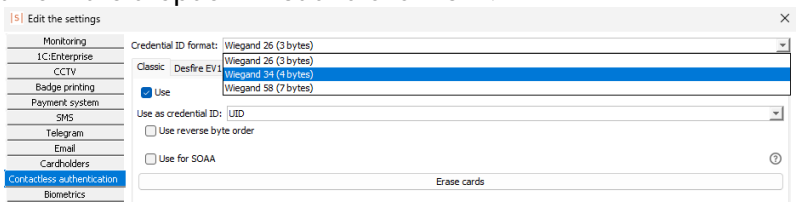
- Connect the reader to a USB port.
- Go to the "Cardholders" tab and select a cardholder.
- Make sure that a "Action when a card is presented" dropdown list appears at the top of the tab. If not, restart the "Client" tool.
- Select the "Link the credentials to the selected cardholder" option and present the card to the USB reader.



"Action when a card is presented" dropdown list.

A new access code is then added to the cardholder and the code length is automatically set. To add multiple access codes to the cardholder, select the "Add the credential to the selected cardholder" option.

To change the format of the access code issued by the integrated USB readers ACR1252U and Iron Logic Z-2 USB, go to the "File" –> "Settings" menu and open the "Contactless authentication" tab. Select the required ID format from the dropdown list and click "OK".



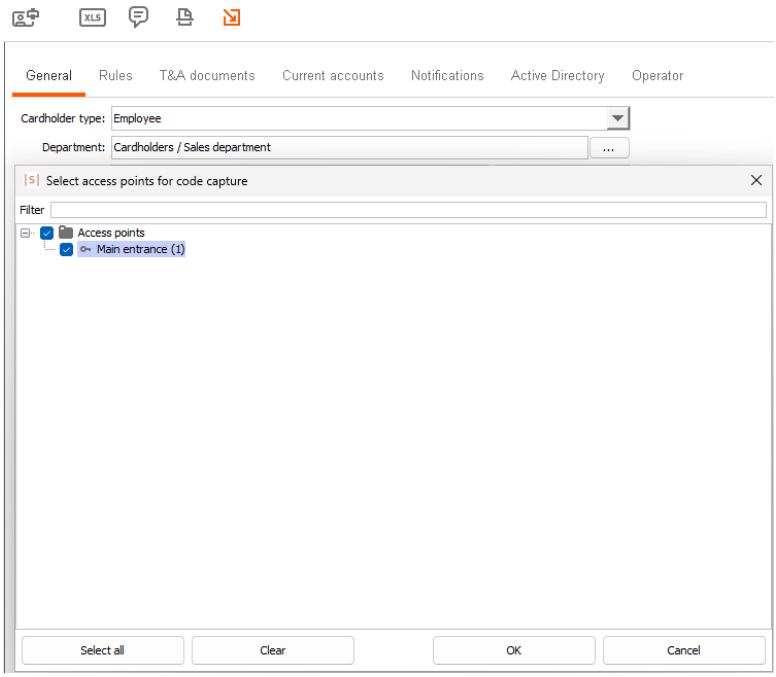
"File" –> "Settings" –> "Contactless authentication" menu.

3. You can capture codes from a wall reader associated with a specific access point. To do this, follow these steps:

   - Go to the "Cardholders" tab and select a cardholder.
   - Click the "Capture codes from access points" button at the top toolbar.

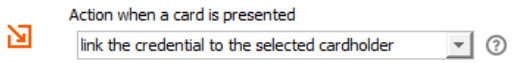
"Capture codes from access points" button.

   - In the window that appears, select the access point from the list and click "OK".



"Selecting access points for code capture" window.

- You will then have access to a "Action when a card is presented" dropdown list. Choose the "Link the credentials to the selected cardholder" option and present the card to the wall reader. To add multiple access codes to the cardholder, select the "Add the credential to the selected cardholder" option.

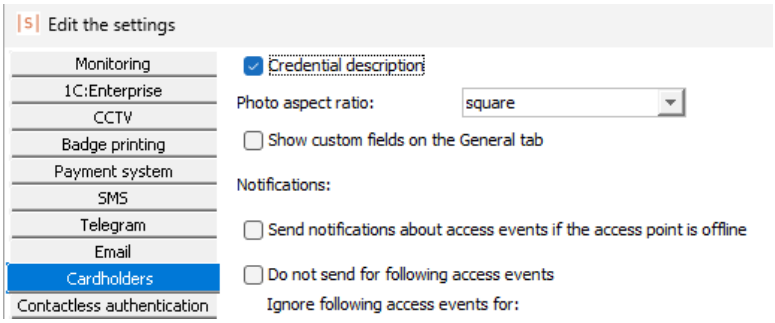


"Action when a card is presented" dropdown list.

- To stop capturing codes, click the "Capture codes from access points" button again. This will disable the capture process.

To finalize and save changes to the cardholder profile, click the "Apply" button.

You can also add comments to cardholder access codes. To enable this feature, go to the "File" –> "Settings" –> "Cardholders" menu and activate the "Credential description" checkbox.



"File" –> "Settings" –> "Cardholders" menu.

9.4. Importing data from MS Excel spreadsheet

This feature allows you to quickly create a database of cardholders, to add or change cardholder information and to reduce the amount of manual data editing required.

To do this, you will need to prepare a MS Excel spreadsheet (.xls) containing cardholder data.

Before loading the file onto the system, it is recommended to back up the database.

The first row of the spreadsheet should contain column names, and the remaining rows should contain cardholder information. The number of columns can vary: for example, you can create a table with only two columns – "Cardholder name" and "Department".

To add multiple card codes to a cardholder profile, list them in the appropriate column without filling in the remaining cells in the rows, as shown in the example below.

Department	Position	Name	Credential	Description
Sales department	Sales manager	John Smith	023CBDF4	Has three cards
			F81E9CA5	
			0A3F2B7D	
Marketing department	Senior Specialist	Mary Johnson	47D36B1F	
HR	HR manager	Charles Williams	5F1842C7	
Accounting office	Accountant Officer	Sarah Brown	EC790D63	

Example of a table.

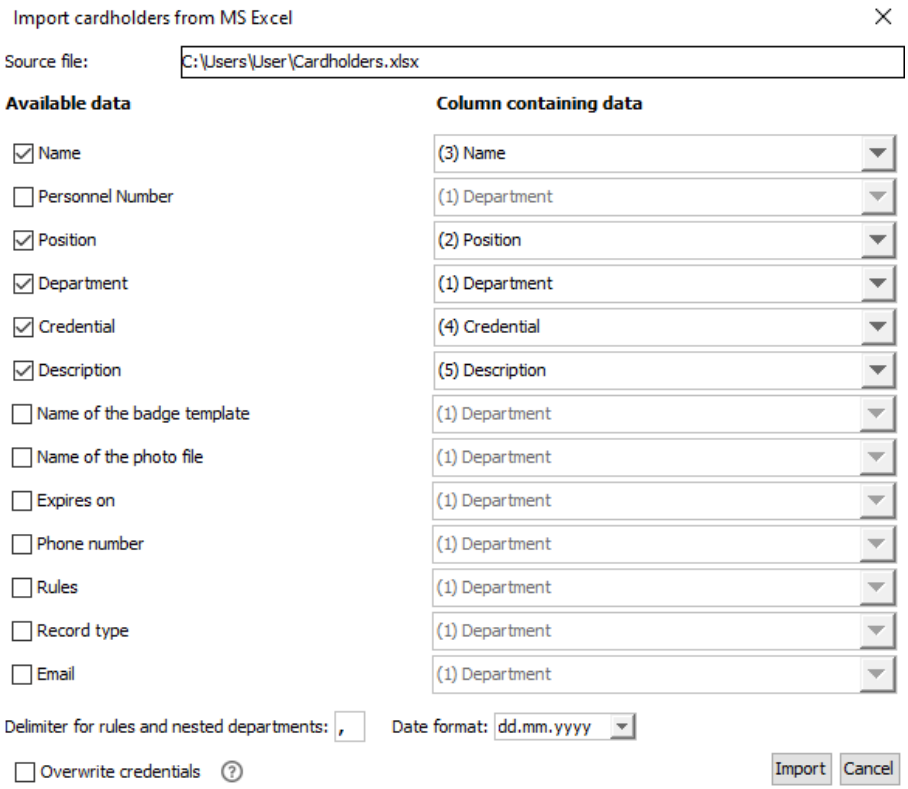
You can also import data into the custom fields created earlier. Add columns to the table that contain values to insert into custom fields.

After preparing the spreadsheet, go to the "Cardholders" tab and click the "Import from MS Excel" button.

"Import from MS Excel" button.

In the dialogue box select the previously prepared file and click the "Open" button. The "Import cardholders from MS Excel" window opens:

- In the "Data presence" column, select the parameters to be loaded into the system from the file.
- In the "Column" block, select a column from the table to be loaded by its name or number.
- When finished, click the "Import" button.

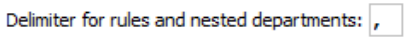


"Import cardholders from MS Excel" window.

Resulting company structure.

If you need to load the hierarchical structure of the departments, you should

specify the "Delimiter for rules and nested departments" when loading the MS Excel file.

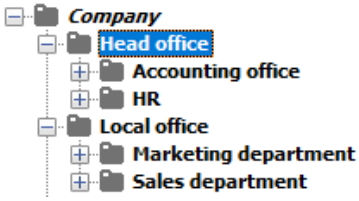


"Delimiter for rules and nested departments" parameter.

The "Department" column of the MS Excel spreadsheet should contain the name of the cardholder's department, taking into account all nesting, and the sub-departments should be separated by the selected symbol.

Department	Position	Name	Credential	Description
Local office, Sales department	Sales manager	John Smith	023CBDF4	Has three cards
			F81E9CA5	
			0A3F2B7D	
Local office, Marketing department	Senior Specialist	Mary Johnson	47D36B1F	
Head office, HR	HR manager	Charles Williams	5F1842C7	
Head office, Accounting office	Accountant Officer	Sarah Brown	EC790D63	

Example of a table.



Resulting company structure.

If required, you can also import photos of cardholders. To do this, add a column to the created table specifying the path and filename of the photo in standard Windows format.

There are two ways of specifying the path:

- Absolute path: "C:\User\Photos\John_K.jpg". The system will search for photos in the specified directory.
- Relative path: "John K.jpg" or "Photos\John_K.jpg". The system searches for photos either directly in the folder containing the spreadsheet, or in the "Photos" folder in the same directory as the spreadsheet.

When loading the spreadsheet, you will need to match the "Name of the photo file" item in the "Available data" column with the column in the MS Excel spreadsheet that contains the path and file name of the photo.

Department	Position	Name	Credential	Description	Name of the photo file
Local office, Sales department	Sales manager	John Smith	023CBDF4	Has three cards	John Smith.jpg
			F81E9CA5		
			0A3F2B7D		
Local office, Marketing department	Senior Specialist	Mary Johnson	47D36B1F		Mary Johnson.jpg
Head office, HR	HR manager	Charles Williams	5F1842C7		Charles Williams.jpg
Head office, Accounting office	Accountant Officer	Sarah Brown	EC790D63		Sarah Brown.jpg

Example of a table.

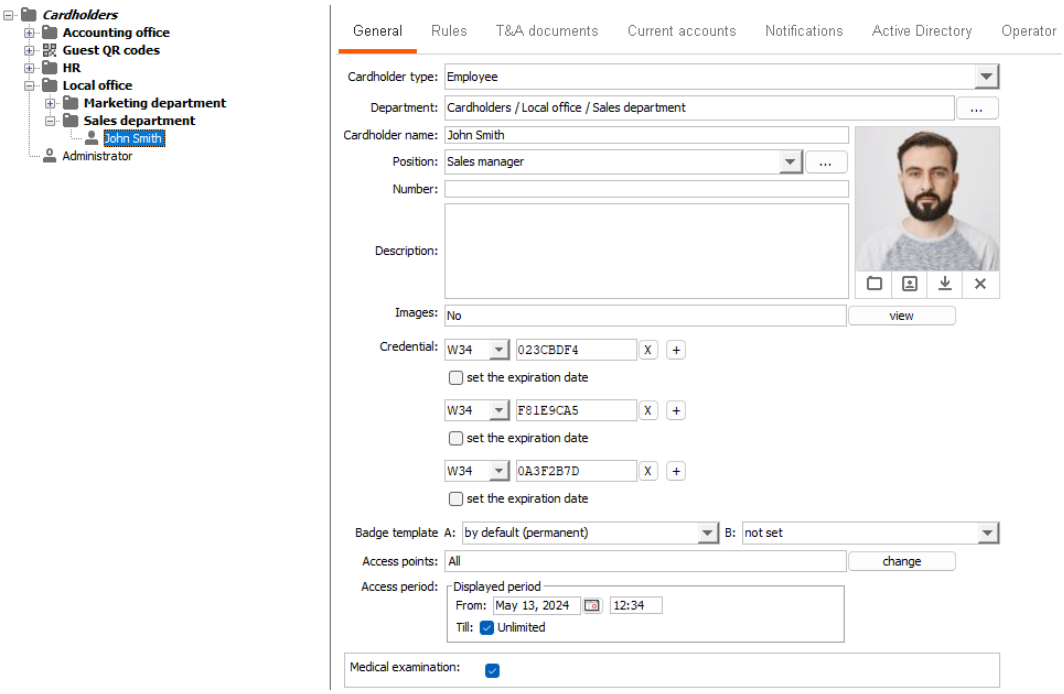
If you do not want to create new cardholders, but want to make bulk changes to existing cardholders, the MS Excel spreadsheet should contain the "Name" and "Department" parameters for each of these cardholders. These parameters should match the existing values in the system.

When loading a file to edit cardholder data, the hierarchical structure of departments should be taken into account. If the values in the spreadsheet (columns "Name" and/or "Department") differ from the existing values in the "Client" tool, the system will create a new cardholder (duplicate) instead of updating the data when processing the file.

Below is an example of a spreadsheet that can be used to change the values of a previously added custom boolean type field called "Medical examination".

Department	Name	Medical examination
Local office, Sales department	John Smith	Yes
Local office, Marketing department	Mary Johnson	Yes
Head office, HR	Charles Williams	Yes
Head office, Accounting office	Sarah Brown	Yes

Example of a table.



Changes made to the cardholder profile.

10. Using Mifare cards

Mifare cards are used to enhance the security of the access control system. Cardholder identification can be based on the card's UID or a password-protected value stored in the Mifare card's memory.

To add UIDs of Mifare cards to the system, follow the instructions in the "Adding Cards" section.

To use Mifare cards in a secure mode, they must be pre-programmed. This procedure is described below in the "Issuing Mifare Identifiers" section.

You must also transfer the Mifare card reading configuration from the software to the wall reader. If you are using a Sigur MR100 reader, follow the instructions in the "Configuring MR100 Readers" section.

If you are using a third-party reader, ensure that it has been configured to work with the secure memory area of Mifare cards. The configuration must match that used for programming Mifare cards in the Sigur software. Refer to your reader's user manual for instructions on how to configure it.

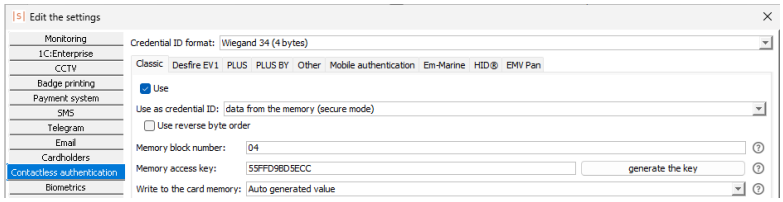
10.1. Issuing Mifare identifiers

In this section we will look at how to configure the system to work with the secure memory area of Mifare Classic cards. Other Mifare cards can also be initialised and copy protected.

To configure the secure memory area of the Mifare classic card, follow these steps:

1. Go to the "File" –> "Settings" –> "Contactless authentication" menu and open the "Classic" tab.
2. Specify the identifier format in the "Credential ID format" block. The available options in the dropdown menu are Wiegand 26 (3 bytes), Wiegand 34 (4 bytes), and Wiegand 58 (7 bytes). It is recommended that you select Wiegand 34 or Wiegand 58 to reduce the likelihood of duplicate access codes in the system.
3. In the "Use as credential ID" block, select "data from the memory (secure code)" from the dropdown menu.
4. The "Memory block number" parameter can be left unchanged (default is 04).
5. Generate a secret code to access the secure area of a card's memory by clicking the "generate the key" button.
6. The "Write to the card memory" parameter can also be left unchanged (default value is "Auto generated value").
7. Save the settings by clicking the "OK" button.

ACR1252U USB readers use this configuration when programming Mifare cards. It should also be transferred to a Sigur MR100 reader.



An example of the configuration.

To issue a pass by writing data to the secure memory area of a Mifare card, use an ACR1252U USB reader. The procedure is the same as described in the "Adding Cards " section:

1. Connect the ACR1252U reader to a USB port.
2. Go to the "Cardholders" tab and select a cardholder.
3. Check that a "Action when a card is presented" dropdown list appears at the top of the tab. If not, restart the "Client" tool.
4. Select the "Link the credential to the selected cardholder" option and present a blank Mifare Classic card to the USB reader. To add multiple access codes to a cardholder, select the "Add the credential to the selected cardholder" option.
5. Using the configuration you have previously set, the USB reader will write the data to the card's memory block and protect it with a secret code. Make sure that a new access code has appeared in the cardholder's profile.
6. Click "Apply" to save the changes.

All Mifare card settings should be configured when the cards are added to the system and should not be changed later.

Changing the system's access credentials to the card memory will result in new cards not being able to access old readers and old cards not being able to access new readers. In such cases, it will be necessary to rewrite all old cards with new credentials and reprogram all readers.

11. Configuring MR100 readers

To change the reading configuration of a Sigur MR100 reader, you need to:

1. Set the reader parameters in the "File" –> "Settings" –> "Contactless authentication" menu.
2. Transfer the settings to the reader using one of the methods described in this section.

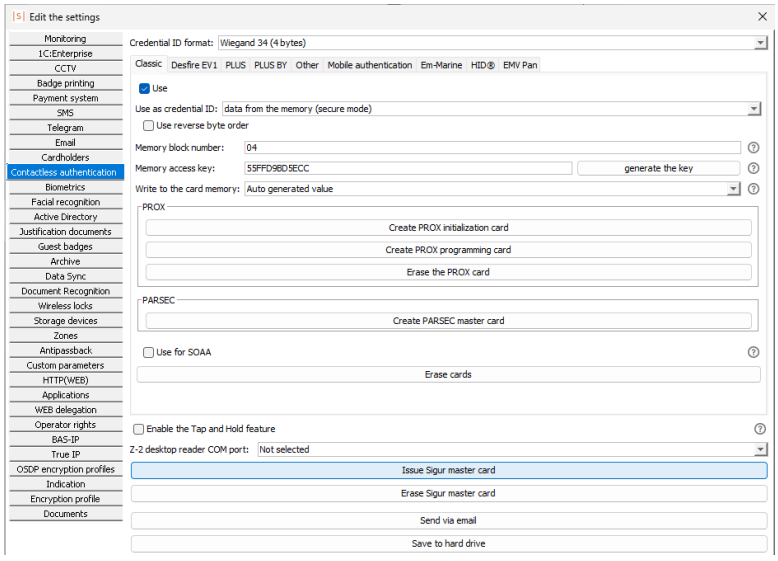
11.1. Configuring a reader using a master card

You can transfer the created reading configuration to Sigur MR100 readers using a master card. For this you need:

- Mifare Classic 1K/4K or Mifare Plus card in factory default configuration, i.e. "blank".
- ACR1252U USB reader.

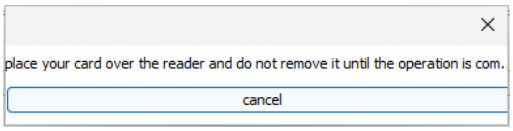
To create a master card, follow the instructions below:

1. Connect the ACR1252U reader to a USB port on your computer and restart the "Client" tool.
2. Go to the "File" –> "Settings" –> "Contactless authentication" menu and click on "Issue Sigur master card".

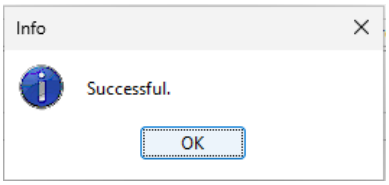


"Issue Sigur master card" option.

3. Present a blank Mifare Classic 1K/4K or Mifare Plus card to the ACR1252U reader. The software will inform you of the result of the configuration writing process.



Pop-up window.



Configuration writing result.

The next step is to configure the reader.

If the Sigur MR100 reader has never been configured before, please follow these steps to load the configuration:

1. Switch the reader off and on again.
2. Present the master card to the reader within 25 seconds of switching on. The reader beeps when it receives the master card.

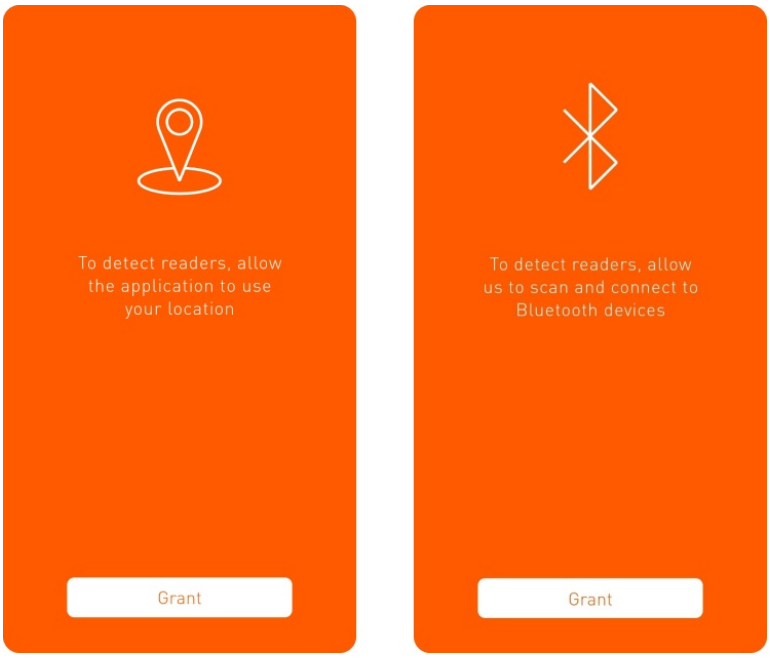
If the Sigur MR100 was previously configured, you need to reset the reading configuration before reconfiguring with the master card. There are two ways to do this:

1. Hardware reset. This does not affect the reader's indication profile. To perform a hardware reset of the reading configuration, it is necessary to:

   - Switch off the reader's power supply.
   - Short-circuit the green (DATA0) and yellow (BEEP) wires of the reader.
   - Power up the reader and then disconnect the wires. The reader beeps if the reset is successful.

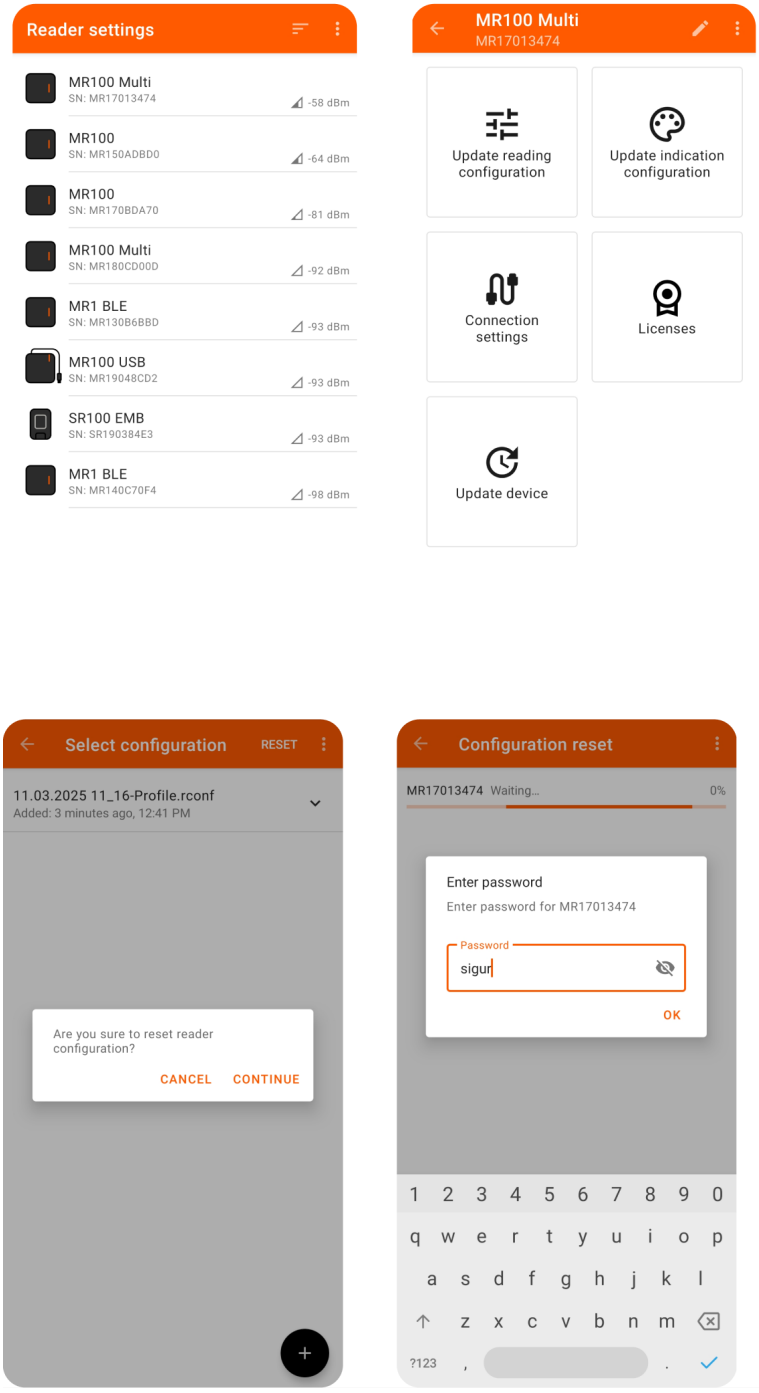
2. Reset via mobile application. You need an Android smartphone (5.0 or higher) with the "Sigur Readers Config" mobile application pre-installed (Google Play, Huawei AppGallery). Proceed as follows:

   - Turn on Bluetooth on your phone and open the application.
   - The first time you run the application, grant it all the permissions it requests.



Mobile application permissions.

- Select the reader you want to reconfigure. You can select multiple readers in the list by long pressing.
- In the list of actions that opens, select "Update reading configuration", in the next window press the button "Reset" and tap "Continue" in a window that opens.
- Enter the service password the first time you interact with the reader. The default password is "sigur" (without quotation marks).
- When the configuration reset process is complete, the reader will beep and the application will notify you of the success. Once the reset is complete, the factory configuration will be applied. It is not necessary to restart the reader.



Configuration reset.

11.2. Configuring a reader using a file

Let's look at another way of configuring the reader - using a configuration file.

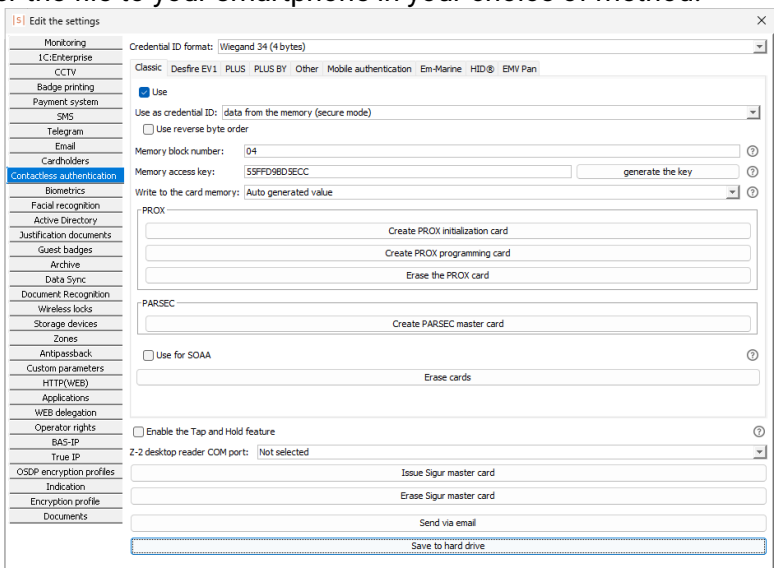
Before doing this, you need to create a reading configuration in the "File" –> "Settings" –> "Contactless authentication" menu.

To configure the reader, you need an Android smartphone (5.0 or higher) with the "Sigur Readers Config" (Google Play, Huawei AppGallery) mobile application pre-installed.

You can download the configuration file to your phone in one of the following ways:

1. By saving a file on your PC.

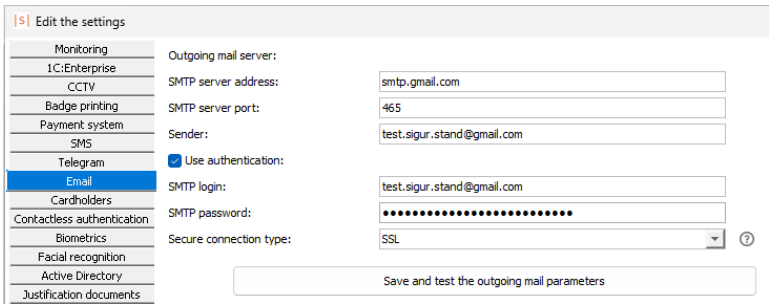
   - In the "File" –> "Settings" –> "Contactless authentication" menu, click "Save to hard drive".
   - Transfer the file to your smartphone in your choice of method.



Saving the configuration on a PC.

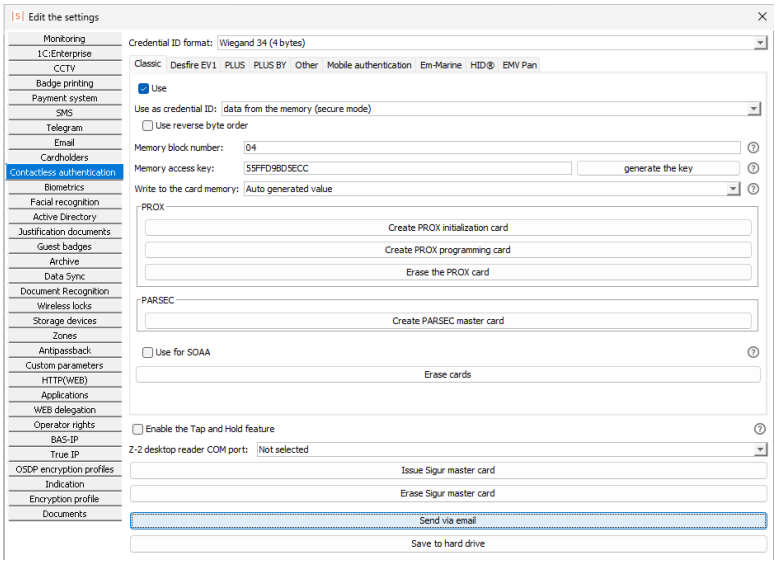
2. By sending the configuration file to a mailbox that can be accessed from the smartphone.

   - First, it is necessary to configure the system's interaction with an external SMTP server. Sigur will use this server for email distribution.
     To do this, go to the "File " –> "Settings" –> "Email" menu. Fill in the "Outgoing mail server" block according to your SMTP server settings. Test the connection by clicking the "Save and test the outgoing mail parameters" button. Click "OK" to save the settings.



SMTP server settings.

Then go to "File" –> "Settings" –> "Contactless authentication" and click "Send via email". In the window that opens, enter any name for the configuration and specify the e-mail address of the recipient in the "Send to email addresses" parameter. Click "OK" to confirm sending the reader configuration.



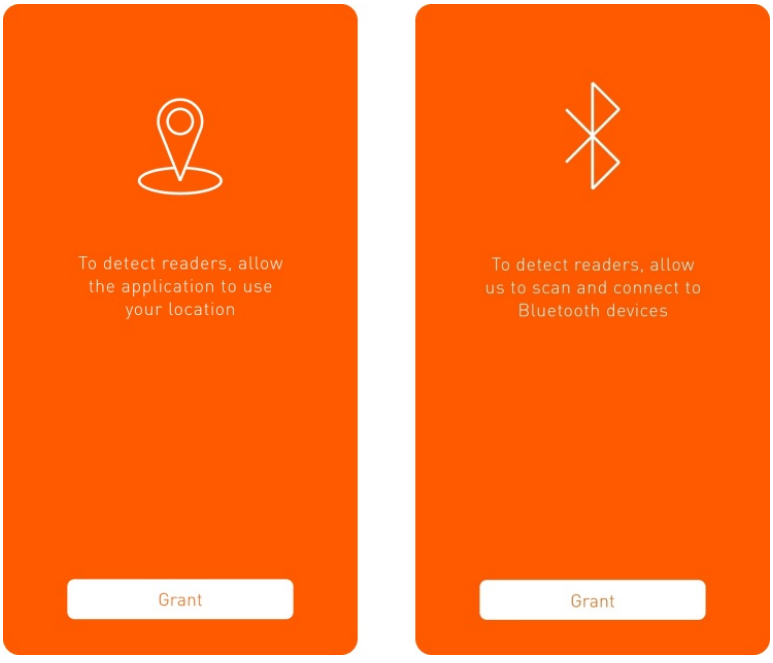
Sending the configuration by email.

- Open the received email on your smartphone. Click on the file attached to the email and open it with the "Sigur Readers Config" application.

Email containing the configuration file.

After transferring the configuration file to your phone, follow these steps:

1. Turn on Bluetooth on your phone.
2. Open the file with the "Sigur Readers Config" application.
3. When you first run the application, grant it all required permissions.

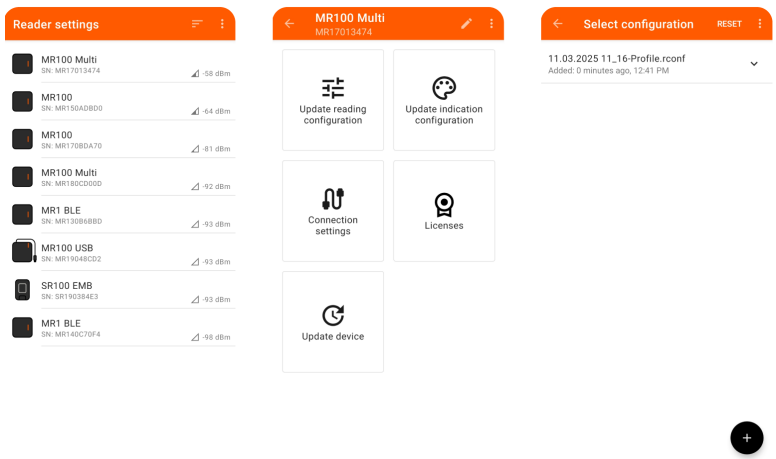


Mobile application permissions.

4. In the list that opens, select the reader to which you want to upload the new configuration. You can select several readers in the list by long pressing.

5. In the list of actions that appears, select "Update reading configuration". If this

item does not appear in the list of actions, update the reader's software by enabling Wi-Fi or mobile internet access on your smartphone and selecting the "Update device" option.

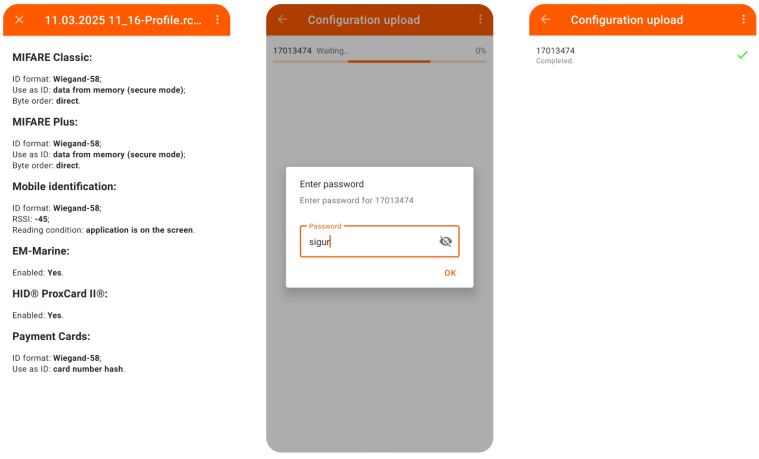


Updating reading configuration.

6. Select a configuration file from the list. You can also check the structure of the configuration file by tapping the down arrow button on the right.

7. Enter the service password the first time you interact with the reader. The default password is "sigur" (without quotation marks).

8. Wait for the configuration to be uploaded to the reader. The configuration will be applied when the upload is complete, you do not need to restart the reader. Once the new parameters have been applied, the reader will beep and the application will notify you of the success of the operation.



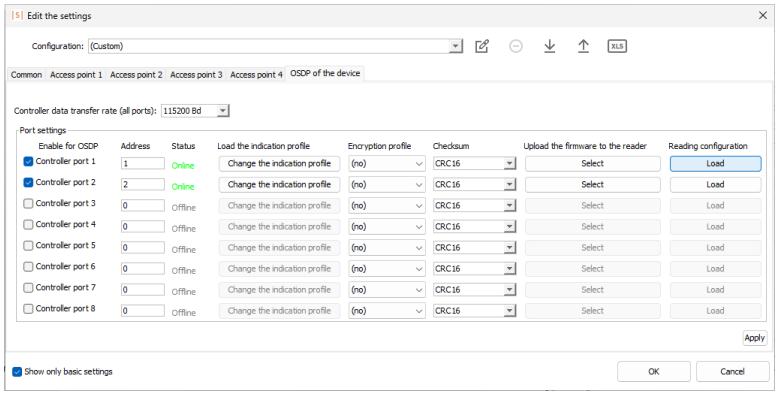
Updating reading configuration.

11.3. Configuring a reader via SSDP (Sigur Supervised Device Protocol)

This method is only relevant if a Sigur MR100 reader is connected to the Sigur E2/E4 controller via the OSDP interface.

The reading configuration created in the "File" –> "Settings" –> "Contactless authentication" menu is transferred to the reader via the "Client" tool. Follow these steps:

1. Go to the "Access points" tab.
2. Select an access point from the list and click the "Settings" button.
3. In the window that opens, select the "OSDP of the device" tab.
4. Click the "Load" button in the "Reading configuration" column for a specific Sigur MR100 reader. The process of uploading the configuration to the reader starts.



Programming a Sigur MR100 reader via SSDP.

5. Click the "OK" button in the update progress window when the upload is complete.

12. Mobile access control

The Sigur MR100 and MR100 Multi readers make it possible to use a smartphone as a means of identification alongside traditional access cards. For iOS (9.0+) and Android (5.0+) smartphones, this is possible using BLE (Bluetooth Low Energy) technology. Android smartphones can also use HCE technology.

The identification technology (BLE or HCE) is not set on the reader. You can select it from Sigur's mobile application "Access".

Sigur readers have two mobile identification modes:

1. Default mode: A reader responds to any smartphone that has the Sigur "Access" application installed and running.
2. Custom mode: A reader only responds to the smartphones that have received an invitation email from a Sigur server. This establishes an encrypted connection with the smartphones.

These modes are described in the following sections.

12.1. Default mode

Let's start by configuring the system to interact with mobile identifiers in Default mode:

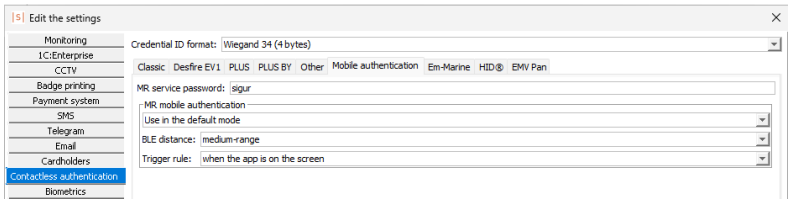
1. Go to "File" –> "Settings" –> "Contactless authentication" –> "Mobile authentication".
2. From the "MR mobile authentication" dropdown list, select "Use in the default mode".
3. From the "BLE distance" dropdown list, select the mobile identification range. There are four options:

    - Short-range: -45 dBm.
    - Medium-range: -75 dBm. You can select this option for now.
    - Long-range: < -75 dBm.
    - Custom (enter the RSSI). This option requires entering the received signal strength indicator (RSSI) in dBm. Successful identification will be performed when this level is exceeded.

4. In the "Trigger rule" block you can select the rule according to which identification will be performed. Three options are available:

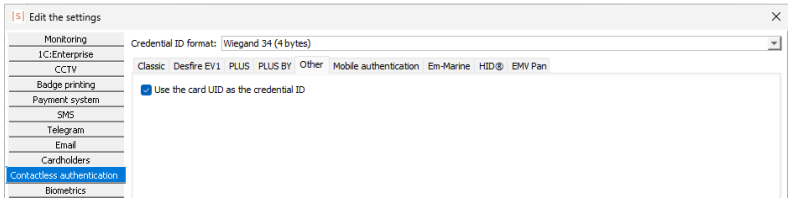
    - when the app is on the screen: the screen is unlocked and the application is open. You can select this option for now.
    - When the screen is unlocked: the screen is unlocked and the application is running in the background.
    - Always: the application is running in the background and identification

occurs even with the screen locked.



Configuring the default mode.

5. If you want to use mobile identification on Android via HCE (in addition to NFC), go to the "Others" subtab and clear the "Use the card UID as the credential ID" checkbox.



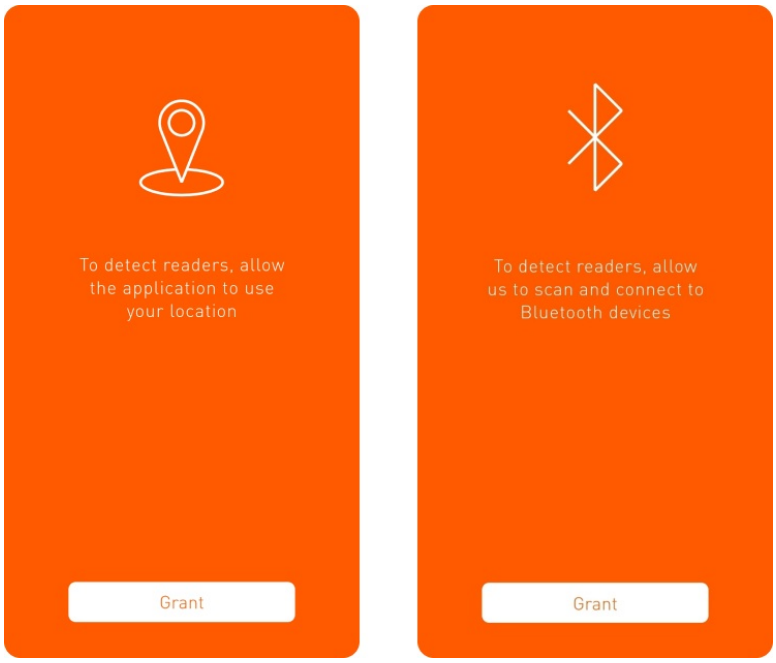
"Use the card UID as the credential ID" checkbox.

6. Transfer the created configuration to a Sigur reader using one of the methods described in the "Configuring MR100 Readers" section.

Issuing a mobile identifier in Default mode.

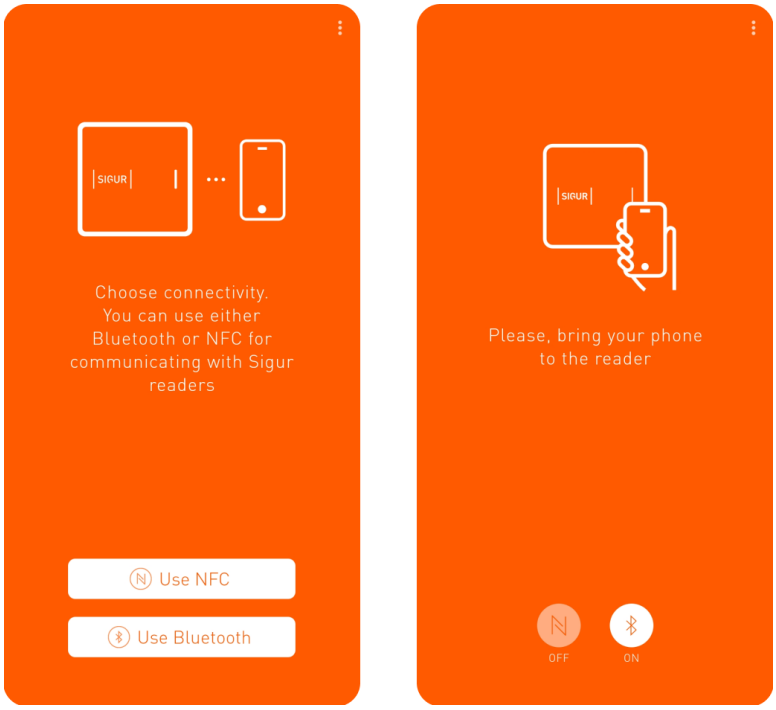
The procedure for issuing mobile identifiers in Default mode is similar to issuing passes by capturing codes from a wall reader:

1. Install the Sigur "Access" mobile application on your smartphone (Google Play, AppStore, Huawei AppGallery).
2. Open the application. The first time you run the application, grant it all the permissions it requests.



Mobile application permissions.

3. Select Bluetooth or NFC as the identification method and enable the corresponding module.



Selection of identification method.

4. Go to the "Cardholders" tab in the "Client" tool and select a cardholder from the list.
5. Click the "Capture codes from access points" button at the top toolbar (as described in the "Adding Cards" section). In the window that appears, select

the access point from the list and click "OK".

6. From the "Action when a card is presented" dropdown list that appears, select "Add the credential to the selected cardholder".
7. Present the smartphone with the Sigur "Access" application running to the Sigur reader. Make sure that a new access code has been added to the cardholder's profile and click "Apply".

12.2. Custom mode

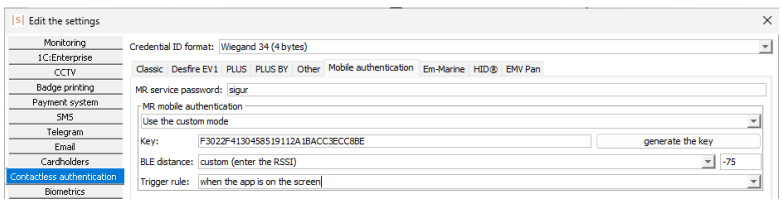
Let's set up the system to interact with mobile identifiers in Custom mode:

1. Go to "File" –> "Settings" –> "Contactless authentication" –> "Mobile authentication".
2. From the "MR mobile authentication" dropdown list, select "Use the custom mode".
3. Click the "generate the key" button.
4. From the "BLE distance" dropdown list, select the mobile identification range. There are four options:

   - short-range: -45 dBm.
   - Medium-range: -75 dBm. You can select this option for now.
   - Long-range: < -75 dBm.
   - Custom (enter the RSSI). This option requires to specify the received signal strength indicator (RSSI) in dBm. Successful identification will be performed when this level is exceeded.

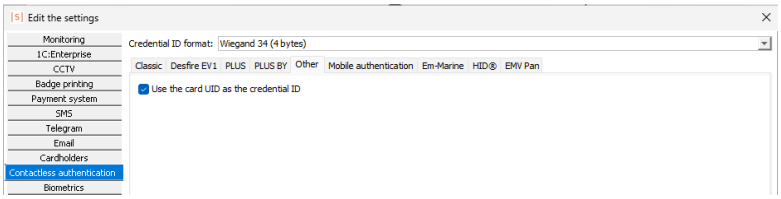
5. In the "Trigger rule" field, select the rule according to which identification will be performed. Three options are available:

   - When the app is on the screen: The screen is unlocked and the application is open. You can select this option for now.
   - When the screen is unlocked: The screen is unlocked and the application is running in the background.
   - Always: The application is running in the background and identification occurs even with the screen locked.



Configuring the custom mode.

6. If you want to use mobile identification on Android via HCE (in addition to NFC), go to the "Others" subtab and clear the "Use the card UID as the credential ID" checkbox.



Unchecking the "Use the card UID as the credential ID" box.

7. Transfer the created configuration to a Sigur reader using one of the methods described in the "Configuring MR100 Readers" section.

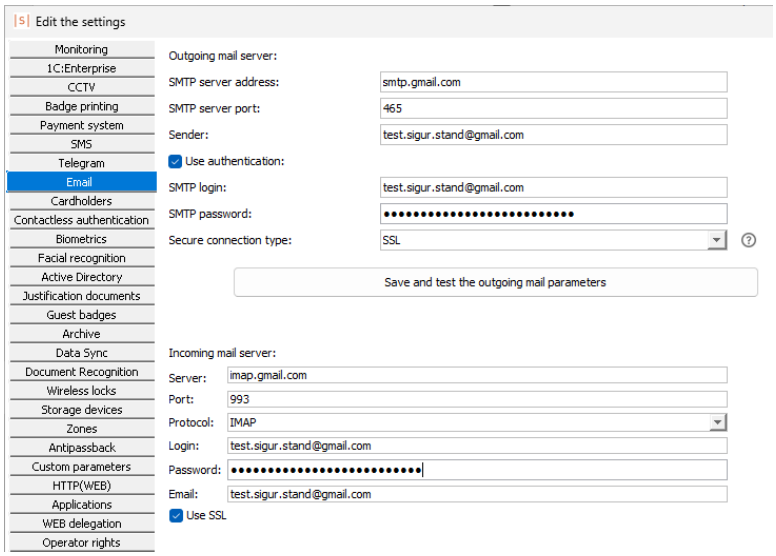
Issuing a mobile identifier in Custom mode.

The procedure for issuing a mobile identifier in Custom mode is as follows:

1. An invitation email is sent to a cardholder.
2. The cardholder installs the Sigur "Access" application on their smartphone.
3. The cardholder opens the invitation email on their smartphone and clicks on the link in the email.
4. The Sigur "Access" mobile application opens and generates a confirmation email.
5. The cardholder sends the confirmation email back to the Sigur server.

Let's send an invitation email to the cardholder. Follow these steps:

1. Go to "File" –> "Settings" –> "Email".
2. First, it is necessary to configure the system's interaction with an external SMTP server. Sigur will use this SMTP server for email distribution. Fill in the "Outgoing mail server" block according to the SMTP server settings. Test the connection by clicking the "Save and test the outgoing mail parameters" button.
3. Then fill in the "Incoming mail server" block. This is the incoming mail server that Sigur will use to receive the confirmation emails.



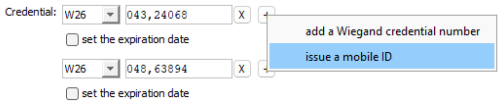
"File" –> "Settings" –> "Email" menu.

The addresses of the outgoing and incoming mail servers can be different.

It is recommended to have a separate mailbox for the needs of Sigur ACS. All emails on the incoming mail server will be deleted by the Sigur server after they are received.

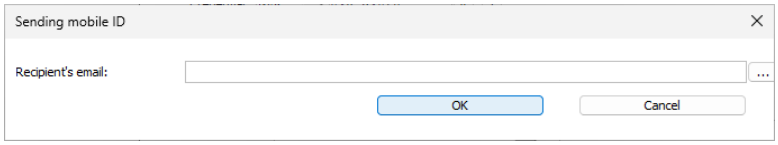
4. Go to the "Cardholders" tab and select the cardholder to whom you want to send the invitation.

5. On the "General" subtab, click the "+" button in the "Credential" block and select "Issue a mobile ID" in the pop-up window.



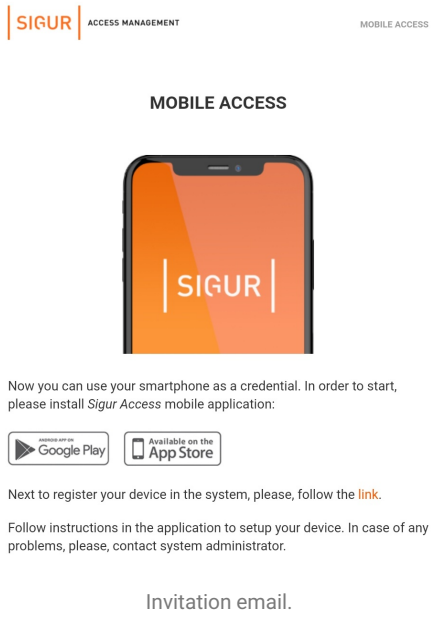
Pop-up window.

6. In the window that opens, enter the cardholder's email address and click "OK".



"Sending mobile ID" window.

An invitation email contains a service link for the Sigur "Access" application, as well as links to download this application from Google Play or App Store.


SIGUR ACCESS MANAGEMENT

MOBILE ACCESS

MOBILE ACCESS

SIGUR

Now you can use your smartphone as a credential. In order to start, please install *Sigur Access* mobile application:

Google Play Available on the App Store

Next to register your device in the system, please, follow the link.

Follow instructions in the application to setup your device. In case of any problems, please, contact system administrator.

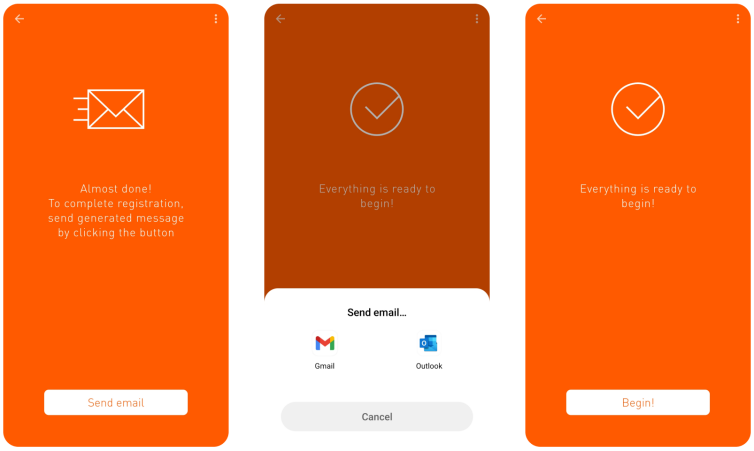
Invitation email.

Once the invitation e-mail has been received, do the following:

1. Make sure the Sigur "Access" application is installed on the cardholder's smartphone.
2. Open the invitation email using any email application.

The invitation email must be opened on the smartphone that is going to be used for access.

3. Click on the service link.
4. The Sigur "Access" application will open and generate a reply email. The reply email contains the mobile identifier associated with this smartphone. This email will be forwarded to the phone's default email application, but will not be sent.
5. Send the reply email manually to the incoming mail address previously set in Sigur settings. If you are unable to send the email from the same device, you can copy the content of the email and send it to the incoming mail address from any other device.
6. After sending the reply email, a new access code will be added to the cardholder's profile.



Sigur "Access" application.

13. Event monitoring

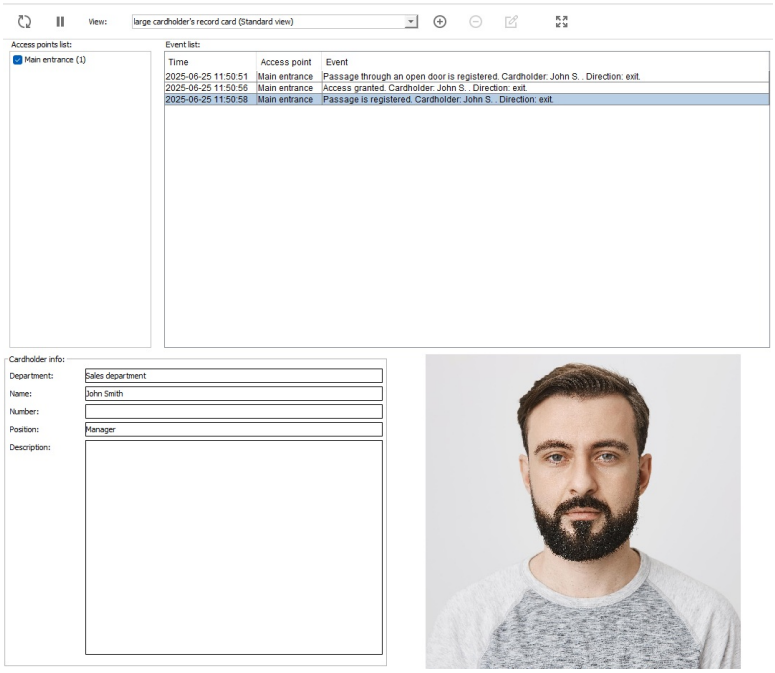
The "Monitoring" tab allows you to monitor system events in real time.

To get started:

1. Go to the tab and select the checkbox in the "Access points list" block. You can now view all system events related to the selected access point in real time.
2. Present an access card or a phone running the Sigur "Access" mobile application to a wall reader.

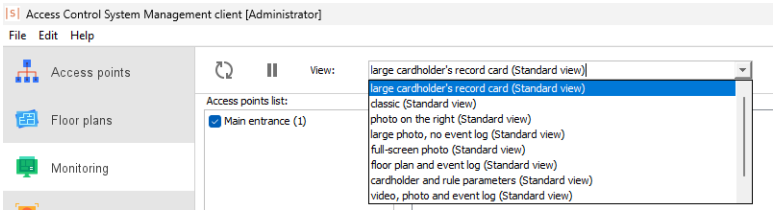
If the access code has been added to the system and the cardholder has been granted access to that access point at that time, the system will record an "Access granted" event, and you will see the cardholder's details and photo. On the controller, the relay to which the control line is connected will also change state.

When a signal is received from an entry sensor, the system will record a "Pass" type event. If the entry sensor is not installed and the "Open sensor" function in the access point settings is set to "Not connected, always active", the "Pass through an open door is registered" event will be recorded immediately after the access card is presented to the reader.



"Monitoring" tab.

There are several default view templates in the system. To change the template, click on the "View" dropdown list in the top panel.



List of default view templates.

You can also create your own custom view template by clicking the "+" button.

14. Access rules management

Access rights in Sigur ACS are controlled by two parameters:

1. The list of access points.
2. The time zones of access.

For access to be allowed, two conditions must be met:

1. A cardholder has access to an access point.
2. A time zone (applicable to both the cardholder and the access point) allows access at that time.

If at least one of these two conditions is not met, access will be denied and the system will record a system event stating the reason for the denial.

The following sections explain how to grant access to access points and assign rules to cardholders.

14.1. Granting access to access points

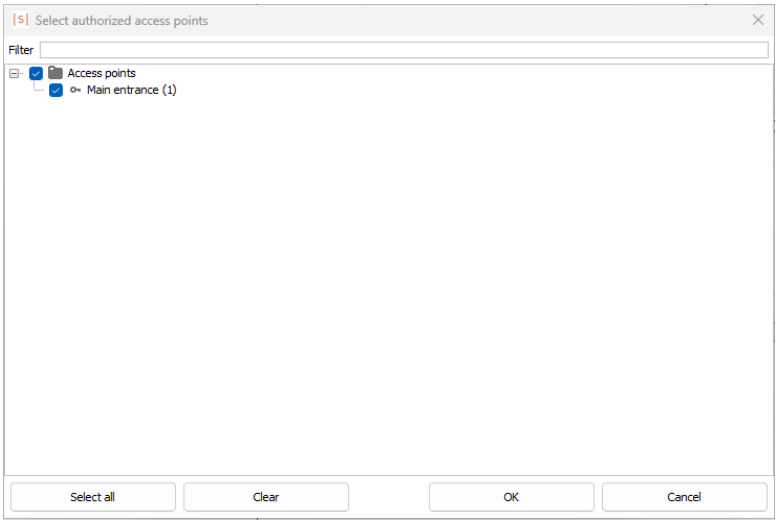
The list of access points to which the cardholder has access is displayed in the "Access points" parameter of a cardholder profile on the "Cardholders" tab.

List of access points.

New cardholders have access to all access points by default.

To allow or deny access to access points, click the "Change" button.

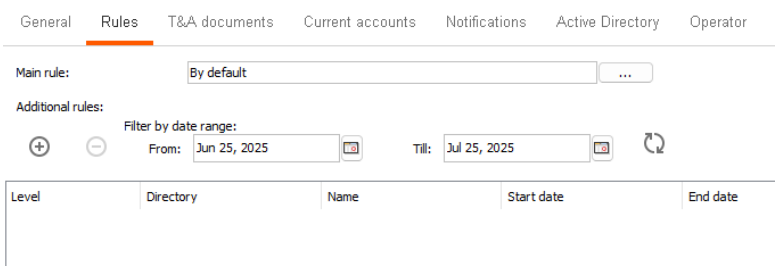
In the window that opens, select the access points that the cardholder will have access to and click "OK" to save the settings.



Granting access to access points.

14.2. Managing rules

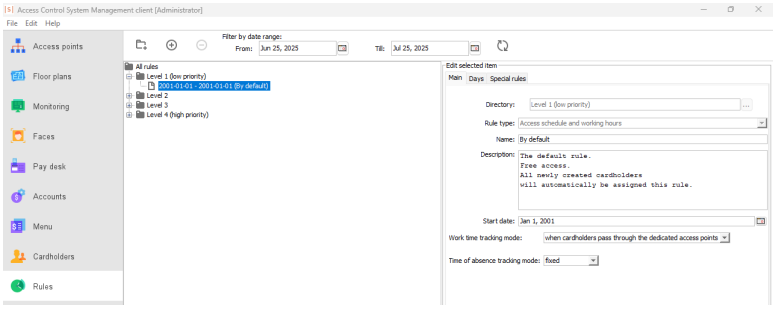
The previously created cardholder has 24/7 access to access points. This access rule is set in the "Default" main rule, which was automatically assigned to the cardholder when they were created. You can check which access rules are assigned to the cardholder by selecting the cardholder profile on the "Cardholders" tab and opening the "Rules" subtab.



"Rules" subtab.

Let's consider a case where you need to organize a special logic at one of the access points: access only after authorization by the guard at a certain time of day. To do this, you need to create two access rules: one that allows free access during selected hours, and one that restricts access, allowing the guard to make decisions about the cardholder's access to the premises.

Go to the "Rules" tab. There are four levels of rules. If a cardholder is assigned more than one rule with different levels, the system will give priority to the rule with the higher level.



"Rules" tab.

Level 1 rules have the lowest priority and apply to all access points.

The level 1 "by default" rule is assigned by default to all new cardholders in the system and applies to all access points. It cannot be deleted but can be edited.

Rules at levels 2 to 4 can be assigned to different access points. Let's create a new level 2 rule.

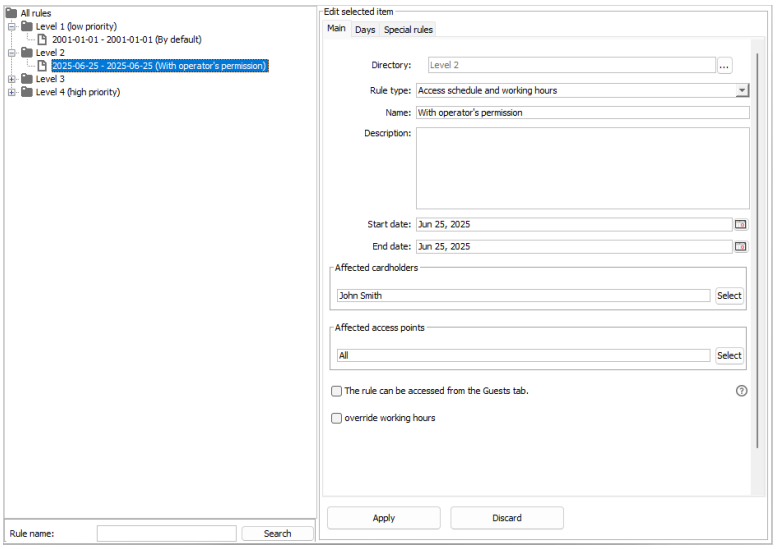
Select the "Level 2" folder in the list, click the "+" button, enter the name of the new rule and click "OK". A new rule will appear in the "Level 2" folder and the available settings will be displayed in the right pane.

Let's have a look at the settings in the "Main" subtab on the right. In the "Rule type" parameter, "Access schedule and working hours" is selected by default. Leave this unchanged for now.

In the "Start date" parameter, enter the current date and set the desired "End date" for the rule.

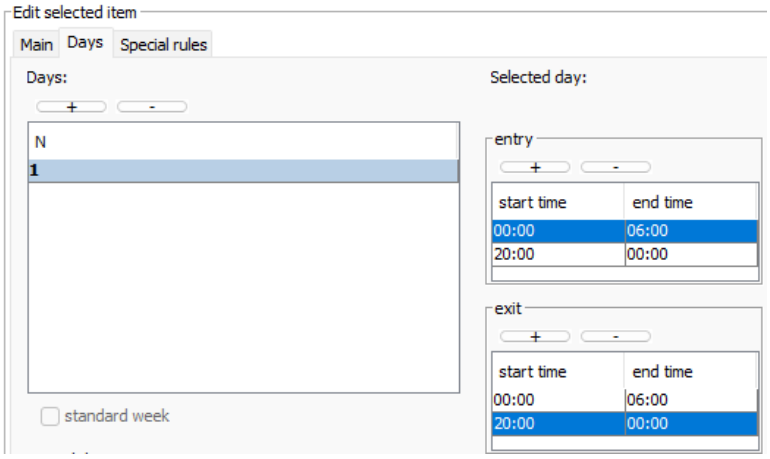
Next, click the "Select" button in the "Affected cardholders" section. Move the cardholder from the left part of the window that opens to the right using the ">>" button and click "OK".

By default, a new time zone created is applied to all access points in the system. To change it, click the "Select" button in the "Affected doors" section. Move the required access point from the left part of the window to the right using the ">>" button and click "OK".



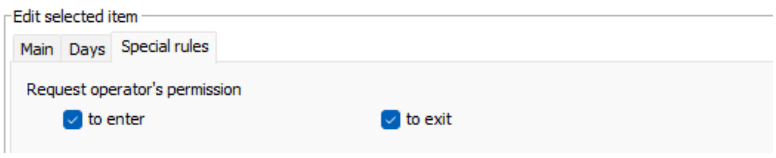
"Main" subtab.

Go to the "Days" subtab and create a new day of the rule by clicking the "+" button. It is necessary to add entry and exit access time intervals by clicking the "+" button in the "Entry" and "Exit" blocks. For example, let's limit the rule to 00:00 - 06:00 and 20:00 - 00:00 in both directions.



Access time intervals.

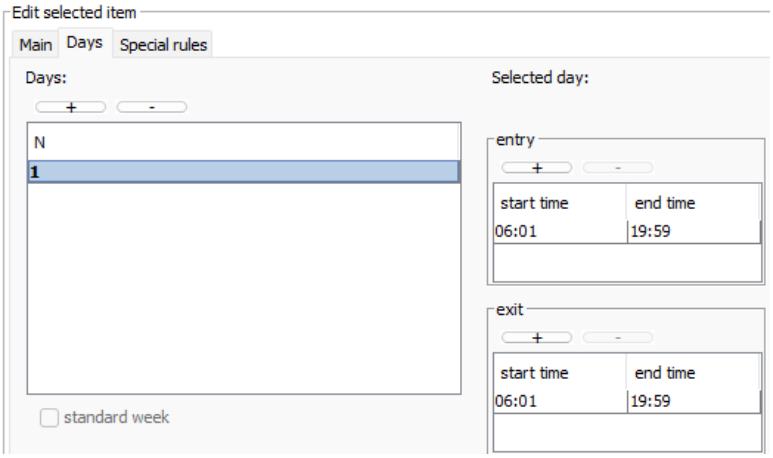
Next, go to the "Special rules" subtab and select the "to enter" and "to exit" checkboxes in the "Request operator's permission" block. Now, during the hours of 00:00 to 06:00 and 20:00 to 00:00, entry and exit access will allowed only with operator's permission. Click "Apply" to save the settings.



"Special rules" subtab.

Let's create another level 2 rule that allows free access between 06:01 and 19:59.

Ensure that this rule is assigned to the required cardholder and access point. On the "Days" subtab, add the specified free access interval to the "Entry" and "Exit" blocks. Leave the "Special rules" subtab unchanged.

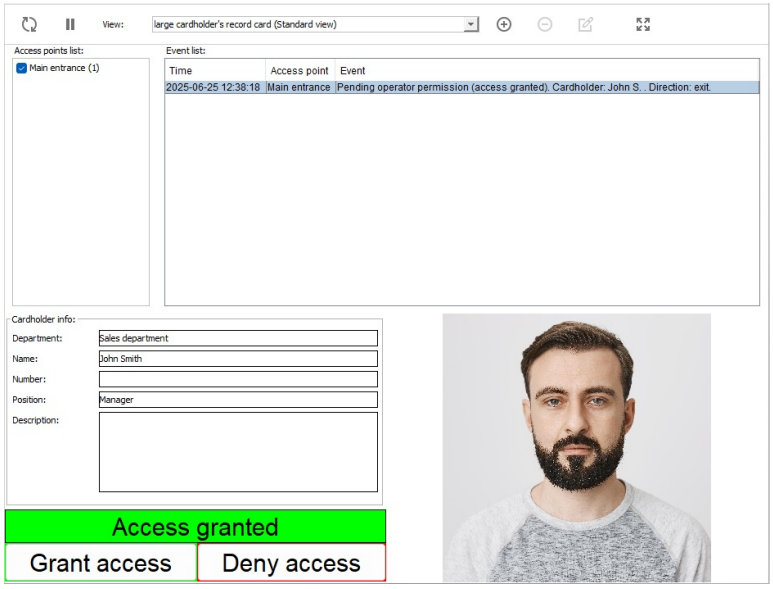


Free access interval.

Let's go to the "Monitoring" tab. Present the cardholder's access card to a wall reader.

If the current time falls within the the level 2 permissive rule intervals (06:01 - 19:59), the system will record the "Access granted" event, and the access point will be unlocked for a single entry.

If the current time falls within the level 2 restrictive rule intervals (00:00 - 06:00 and 20:00 - 00:00), the system will record the "Pending operator permission (access granted)" event and a panel with "Grant access" and "Deny access" buttons will appear. By clicking on them, you can grant or deny access.



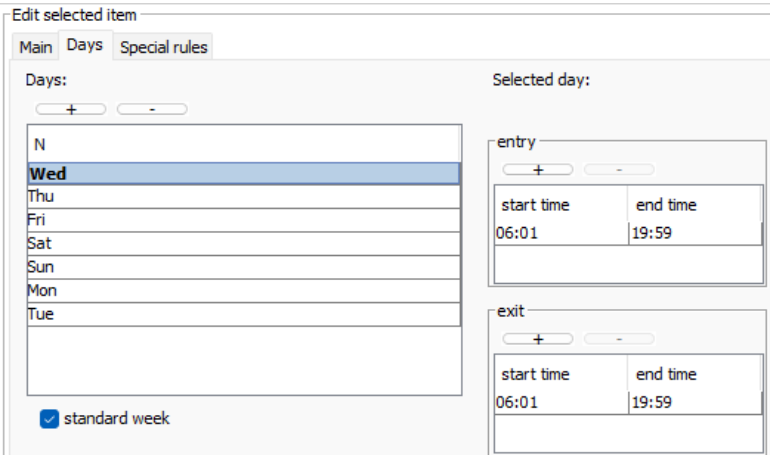
"Monitoring" tab.

Ensure that cardholders are not assigned multiple rules of the same level with overlapping time intervals.

If different equal access logics are in effect at the same time, the system may make access decisions in an unpredictable way.

Currently, only one day is added to the "Days" subtab of the rules. This means that the access rules will be the same every day. You can add a sequence of up to 32 days, which will be repeated cyclically until the rule expires.

If you add a multiple of seven days, the "Standard week" checkbox will be available. If you select this option, the day numbers will change to the names of the days of the week from the start date of the time zone.

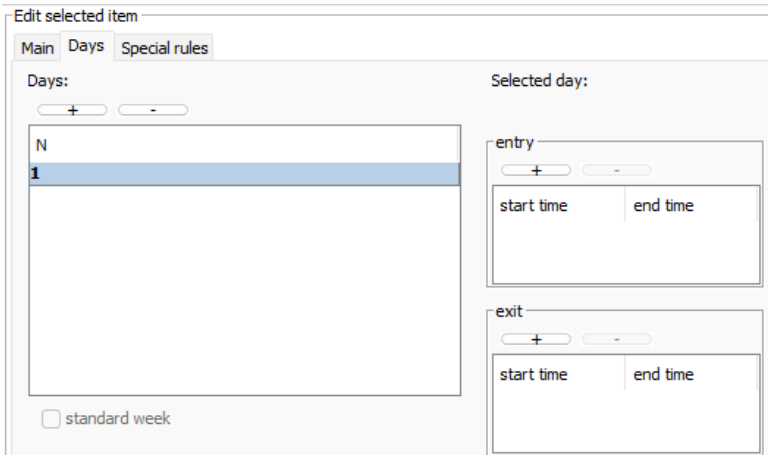


"Standard week" checkbox.

14.3. Restricting access using rules

If you need to deny access to an access point at a particular time, you can simply exclude that time interval from the "Days" subtab of a rule. This means that if a cardholder's access card is presented to a wall reader during the excluded time, the system will record the "Access denied. Access is not allowed during this time" event.

If a cardholder is assigned a rule, as in the example below, access will be denied 24 hours a day. Such rule should be set at a level above the other rules.



Example of a rule that denies access at any time of the day.

15. User management

You can assign user rights to each cardholder, restrict access to certain system functions and set a password to enter the "Client" tool.

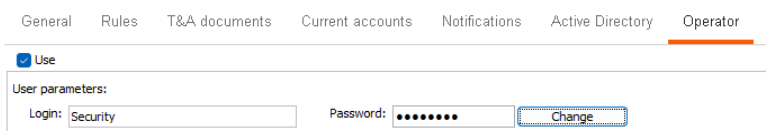
By default, there is only one user in the system - "Administrator".

Creating a new user.

Let's consider the process of creating user rights for a security operator. The operator's rights will be limited to viewing real-time system events and confirming access via the "Monitoring" tab.

To do this, go to the "Cardholders" tab, open the "Operator" subtab in the cardholder profile and select the "Use" checkbox.

Let's set the login of the user, e.g. "Security". To change the password, click the "Change" button. In the window that opens, enter the new password for the "Security" user twice and leave the "User password Administrator" field blank if you haven't already set it. Click "OK" to apply the settings.



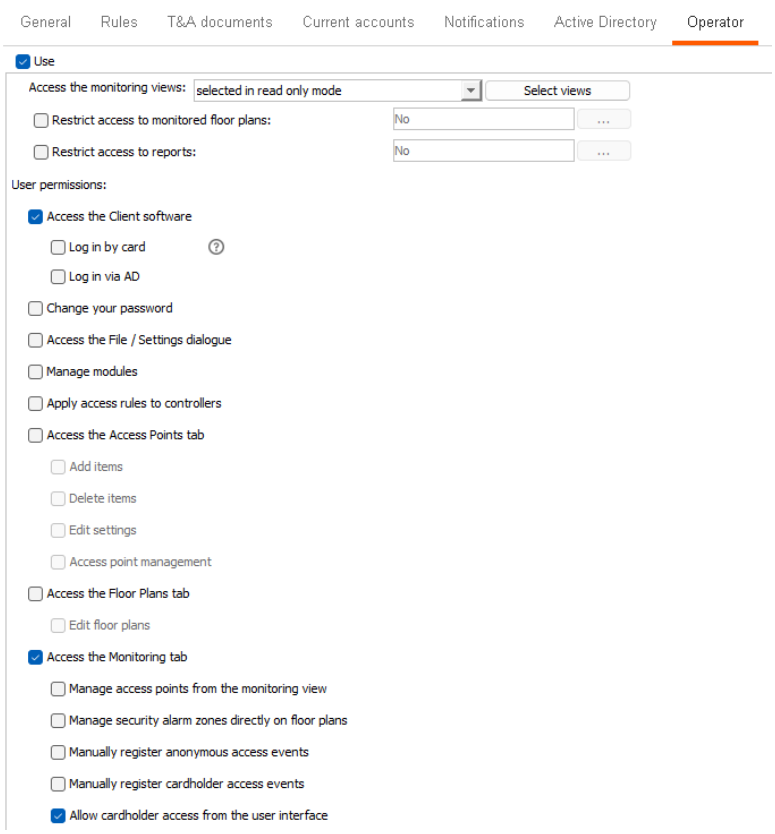
"Operator" subtab.

Next, let's restrict the user's access to view templates on the "Monitoring" tab.

In the "Access the monitoring views" block, select "selected in read only mode" from the dropdown list and click the "Select views" button. In the window that opens, select one of the templates, e.g. "Large cardholder's record card (Standard view)" and click "OK". In the "User permissions" block clear all checkboxes except the "Access the Monitoring tab" and "Allow cardholder access from the user interface".

This set of permissions allows the "Security" operator to grant access by clicking the "Grant access" button on the "Monitoring" tab, or by presenting their access card to the integrated USB reader (ACR1252U or Iron Logic Z-2 USB). The process of creating a time zone with guard authorization is described in detail in the "Access Rules Management" section.

Click "Apply" to save the settings.



"Security" operator's rights.

You will now need to restart the "Client" tool. Select the "Security" login from the "User" dropdown list, enter the password you set previously and click "OK". After successful login, only the "Monitoring" tab will be available to this user.

In this case, the "Monitoring" tab will initially open in full screen mode. To exit full screen mode, press Esc or Alt+Enter.

Setting the logout password.

You can also set a password for the user to log out of the "Client" tool. In this case, the user will not be able to close the system window. To exit the "Client" tool, the user will need to go to the "File" –>"Exit" menu and enter a password.

To enable this option, select the "Request the password to exit" checkbox in the user rights settings and enter the password in the text box.

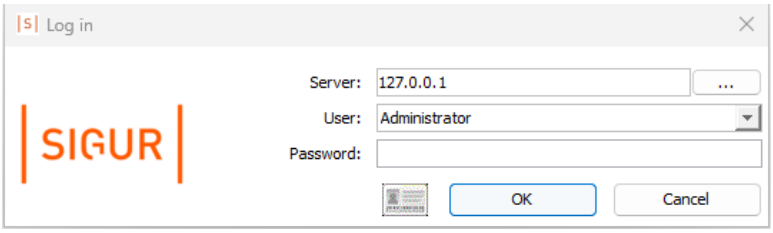
"Request the password to exit" checkbox.

Setting the password for the "Administrator" user.

The "Administrator" user does not have a password by default, but you can set it.

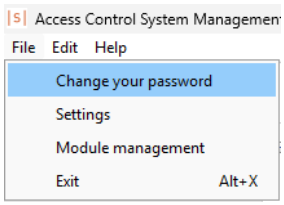
To set the password, follow these steps:

1. Log in the "Client" tool as "Administrator".



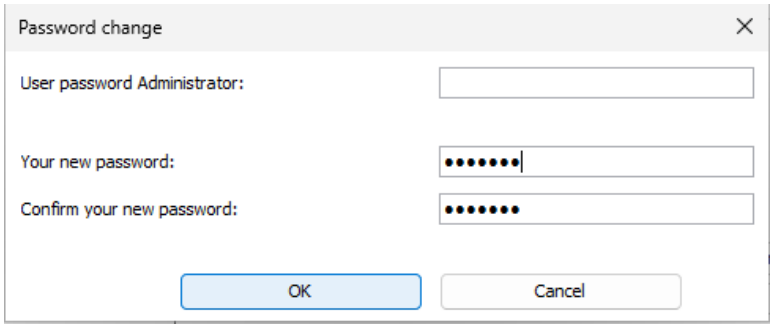
"Log in" window.

2. Click the "File" button at the top of the window and select "Change own password".



"File" menu.

3. In the window that opens, enter the new password twice and click "OK". Leave the "User password Administrator" field blank as this is the first time you are setting the password.



"Password change" window.

16. Antipassback and zone control

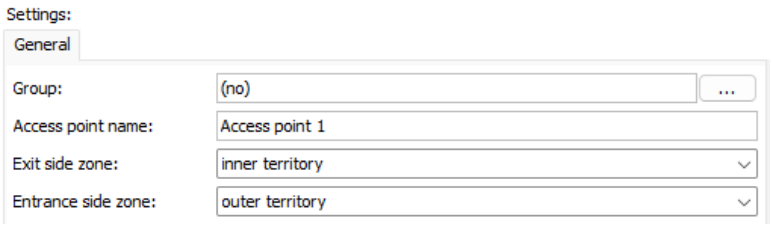
When antipassback is enabled, Sigur ACS monitors the cardholder's location and blocks access attempts from areas where the system believes the cardholder is not supposed to be at the moment.

Dividing the premises into zones.

Before using the antipassback function, you need to divide the premises into zones.

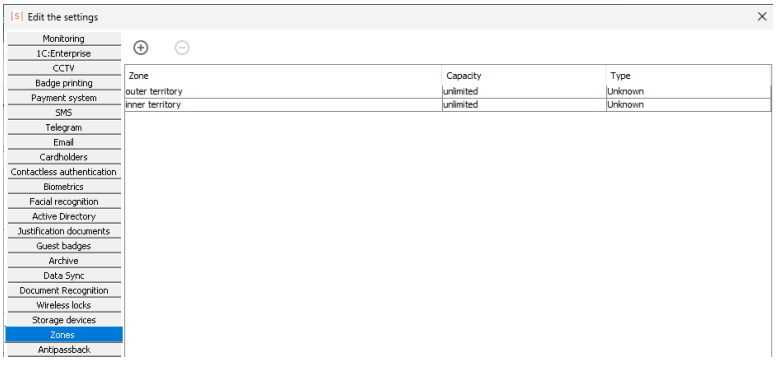
To do this, start the "Client" tool, go to the "Access points" tab and select an access point from the list. By default, the "Exit side zone" and "Entrance side zone" parameters in the "Settings" block are filled with the "outer territory" value.

The value of the "Entrance side zone" parameter applies to the zone where the exit reader is located. Similarly, the value of the "Exit side zone" parameter applies to the zone where the entry reader is located. Choose the value "Inner territory" for "Exit side zone" text box and then click "Apply".



Access point settings.

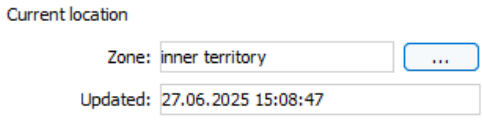
In the "File" –> "Settings" –> "Zones" menu, you can see a list of all the zones in the system.



"File" –> "Settings" –> "Zones" menu.

The location of cardholders changes when they pass through an access point with the configured zoning. Go to the "Monitoring" tab. Present the card to the entry reader and pass through the access point. Ensure that the system has recorded a "Pass" or "Pass through open door" event.

Return to the "Cardholders" tab. The cardholder's current location and the time of the location change are displayed at the bottom of the window in the "Current location" block. The "Zone" parameter now contains the value "Inner territory".



"Current location" block.

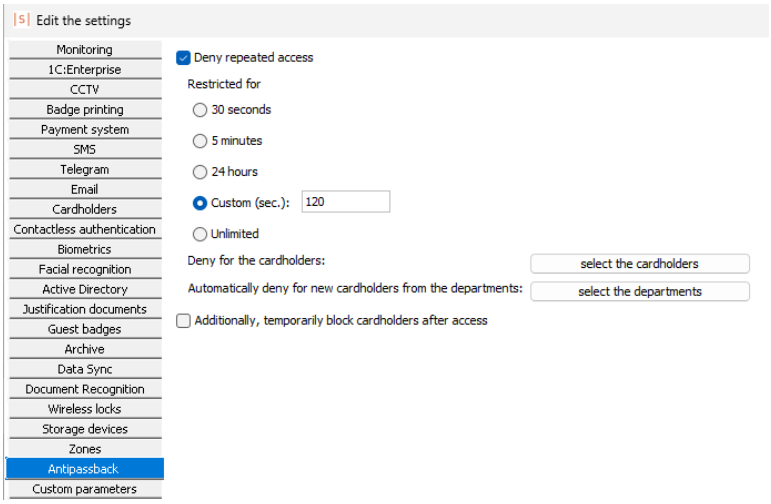
If necessary, the location can be changed manually by clicking the "..." button, selecting the required zone and clicking "OK".

Enabling antipassback.

Let's activate the antipassback function now.

Go to the "File" –> "Settings" –> "Antipassback" menu and select the "Deny repeated access" checkbox. In the "Restricted for" block you can set the time after which cardholders will be granted access, regardless of their location. Let's set the control time to 120 seconds in the "Custom" (sec) window.

By default, antipassback is applied to all cardholders in the system. You can later change the list of cardholders by clicking the "Select the cardholders" button in the "Deny for the cardholders" block. You can also apply the "Automatically deny for new cardholders from departments" action to specific departments. Click "OK" to save your settings.



"File" –> "Settings" –> "Antipassback" menu.

Present the card to the entry reader again. The system will register an "Access denied. Antipassback alert" event and the door will not be unlocked. If you present the card to the enter reader, access will be allowed.

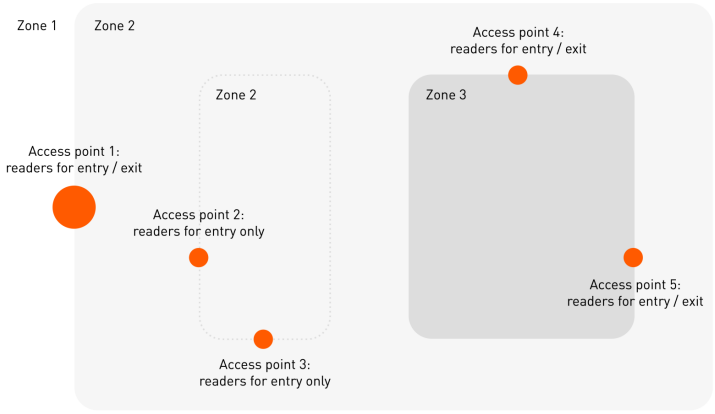
After the 120 seconds we set earlier, from the moment the cardholder passed through the access point in the "exit" direction, the system will be able to allow access in that direction again.

Time	Acc...	Event
2025-06-25 13:33:09	Main ...	Access granted. Cardholder: John S. . Direction: exit.
2025-06-25 13:33:11	Main ...	Passage is registered. Cardholder: John S. . Direction: exit.
2025-06-25 13:33:13	Main ...	Access denied. Antipassback alert. Cardholder: John S. . Direction: exit.

"Access denied. Antipassback alert" event.

If there is no exit reader and the room is exited using a push-button, the antipassback function will not work correctly for that access point. This is because the location of cardholders doesn't change when they leave the room.

In this case, you need to exclude the room from zone control by entering the same values for the "Exit side zone" and "Entrance side zone" parameters for that access point on the "Access points" tab. In the example below, access points 2 and 3 don't have exit readers, so the "Entrance side zone" and "Exit side zone" values for these access points are the same.



Zone control.

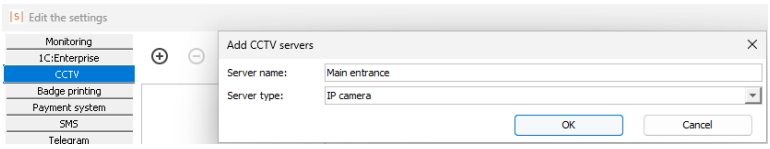
17. Video surveillance

Sigur ACS supports interoperability with various video surveillance systems and allows users to receive both live and archived video from most IP cameras that support RTSP streaming.

17.1. IP cameras integration

Let's configure the system's interaction with an IP camera.

To do this, go to "File" –> "Settings" –> "CCTV" menu and add a new source by clicking the "+" button. In the window that opens, enter any server name, set "Server type" to "IP camera" and click "OK".



"Add CCTV servers" window.

In the "Stream URL" parameter, specify the stream URL as:

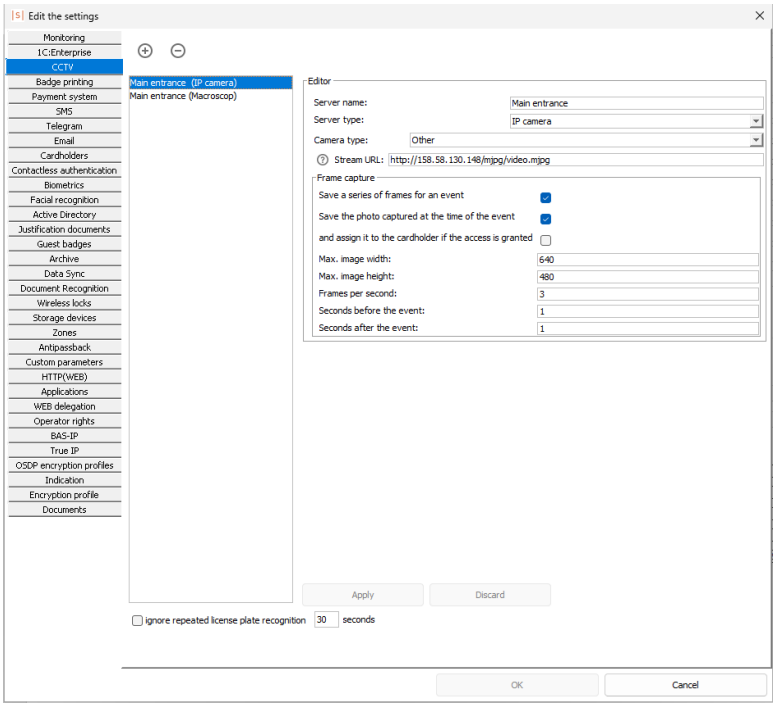
protocol://[user:password@]ip-address:port/resource

Examples of stream URLs:

- http://192.168.0.10/mjpg/video.mjpg
- rtsp://192.168.1.15:554/axis-media/media.amp
- rtsp://root:root@192.168.1.10/media0

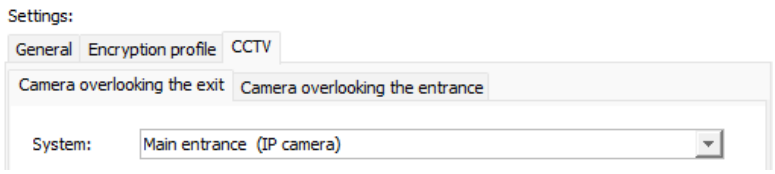
If you are not sure of the stream URL format, please contact your camera manufacturer.

Activate the "Save the photo captured at the time for an event" and "Save a series of frames for an event" checkboxes to be able to view photos and videos from the IP camera on the "Archive" tab later. Click "Apply" and "OK" to save the settings.



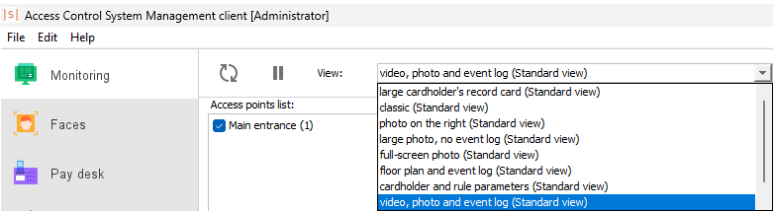
IP camera settings.

Now go to the "Access points" tab and select the access point where the IP camera is located. A new "CCTV" subtab will appear in the "Settings" block. Click on the "CCTV" subtab and select the "Camera overlooking the entrance" camera subtab. When you click on the "System" dropdown list, you will be offered a choice of all the CCTV sources added to the system. Select the previously added IP camera and click "Apply".



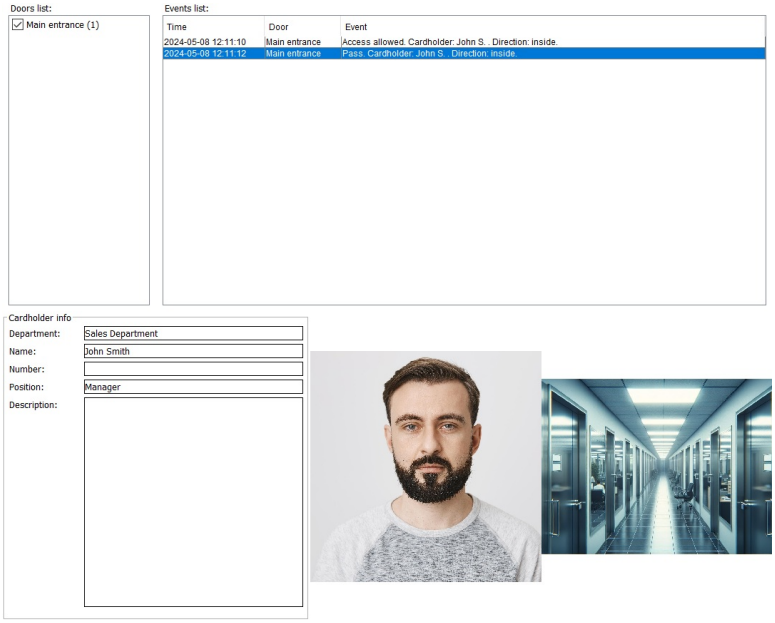
Access point settings.

Go to the "Monitoring" tab and select the default view "Video, photo and events log" from the dropdown list at the top of the window. Ensure that the checkbox for the required access point is selected in the "Access points list" block.



"View" dropdown list.

Next, present the card to the entry reader. In addition to information about the cardholder, you will see live video from the IP camera you added to the system earlier.



"Monitoring" tab.

To view the archive of images and video recordings from the IP camera, please refer to the instructions in the corresponding section.

17.2. Milestone integration

The following features are currently available as part of the integration with the Milestone video management system:

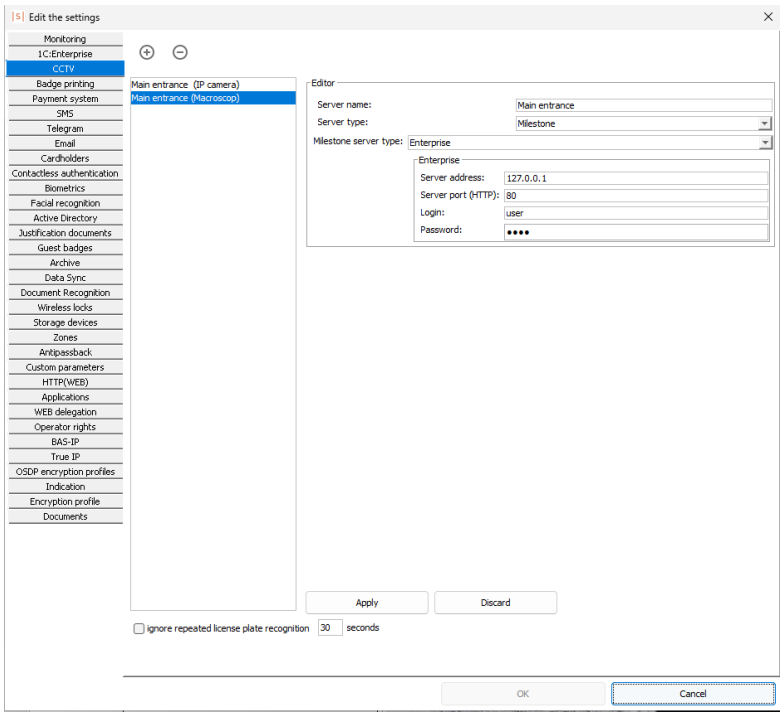
- Live video streaming on the "Monitoring" tab and on floor plans in the Sigur "Client" tool.
- Accessing the Milestone video archive from the Sigur "Client" tool.
- Sending Sigur ACS events to a Milestone server. This feature requires a special plugin:

    - To get the plugin, please follow this link.
    - For instructions on how to configure the functionality of the plugin, please contact our technical support: support@sigur.com.

Let's set up the interaction between the systems to get live and archived video.

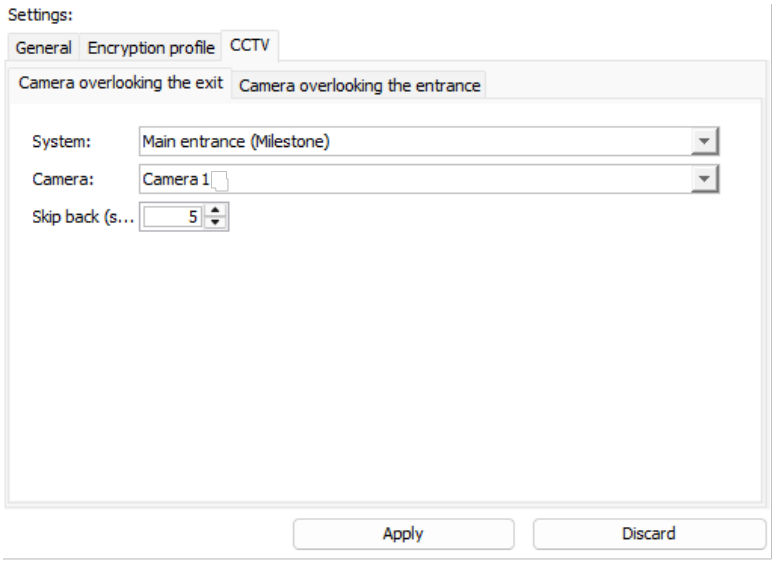
- In the "File" –> "Settings" –> "CCTV" menu, add a new source by clicking the "+" button. In the window that opens, enter the server name, set "Server type" to "Milestone" and click "OK".
- Select the Milestone server type (Enterprise or Corporate).

- Enter the IP address of the Milestone server.
- Enter the server port (HTTP). The default value is 80.
- Enter the login and password set in the Milestone software.
- Click "Apply" and "OK" to save the settings.



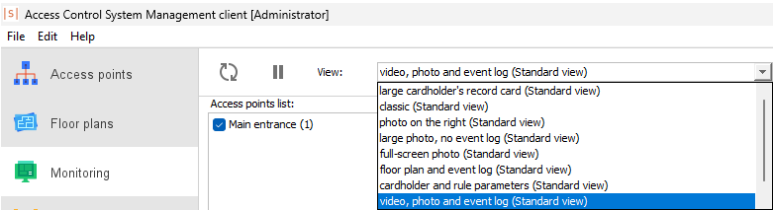
Milestone server settings.

Now go to the "Access points" tab and select the access point where the Milestone camera is located. Click on the "CCTV" subtab and then open the "Inside direction camera" subtab. When you click on the dropdown list in the "System" parameter, the added Milestone source will appear in the list. If the connection to the Milestone system is successful, a list of channels will be available in the "Camera" dropdown list. Select the required channel and click "Apply".



Access point settings.

Go to the "Monitoring" tab and select the default view "Video, photo and events log" from the dropdown list at the top of the window. Ensure that the checkbox for the required access point is selected in the "Access points list" block.



"View" dropdown list.

Next, present the card to the reader in the "Entry" direction. In addition to the cardholder information, you will see live video from the selected Milestone video channel.

To view the Milestone system snapshot and video archive, please refer to the instructions in the corresponding section.

17.3. Trassir integration

The following features are currently available as part of the integration with the TRASSIR video surveillance system:

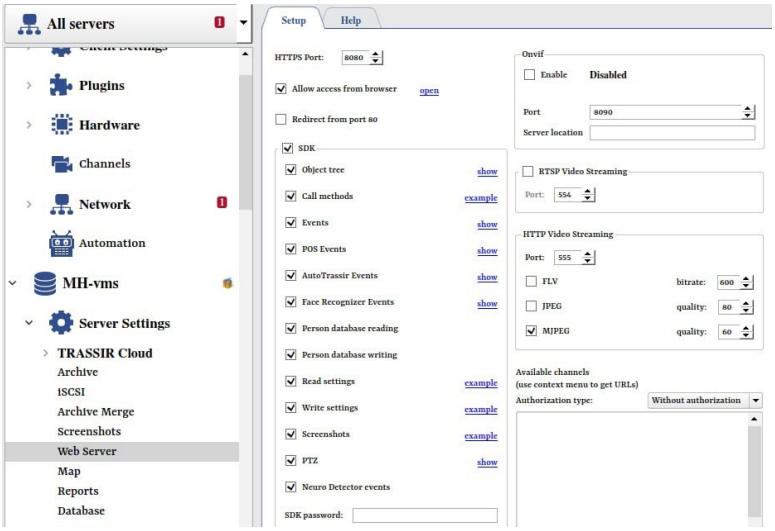
- Live video streaming on the "Monitoring" tab and on floor plans in the Sigur "Client" tool.
- Accessing the TRASSIR video archive from the Sigur "Client" tool.
- Receiving recognized vehicle license plate numbers.
- Using face recognition (TRASSIR Face Recognition module is required) and temperature measurement (TRASSIR Thermal Camera module is required).

- Sending Sigur ACS events to a TRASSIR server (requires a TRASSIR Sigur module).

Please contact TRASSIR for more details on TRASSIR modules.

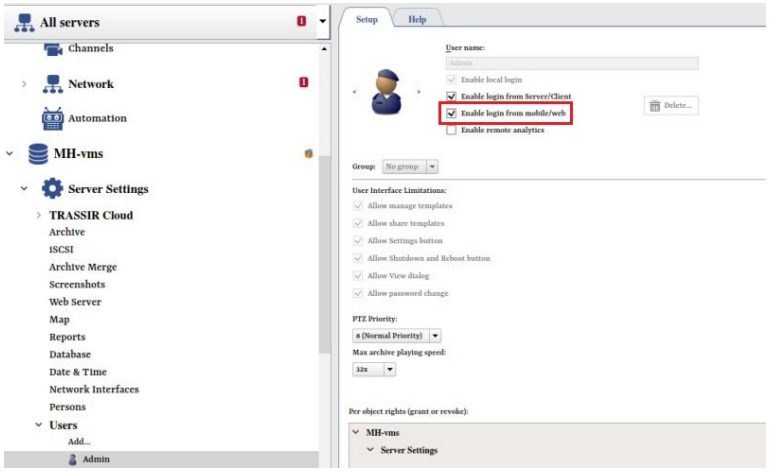
Let's set up the interaction between the systems to get live and archived video. Set up the TRASSIR server (versions 3.x, 4.x) as follows:

- Under the "Server Settings" –> "Web Server" –> "Setup":
  - Select the "SDK" checkbox and its nested checkboxes.
  - Set the SDK password.
  - Under "HTTPS Port", set the port (default - 8080).
  - Under "HTTP Video Streaming", set the port (default is 555) and select the "MJPEG" checkbox.



TRASSIR server settings.

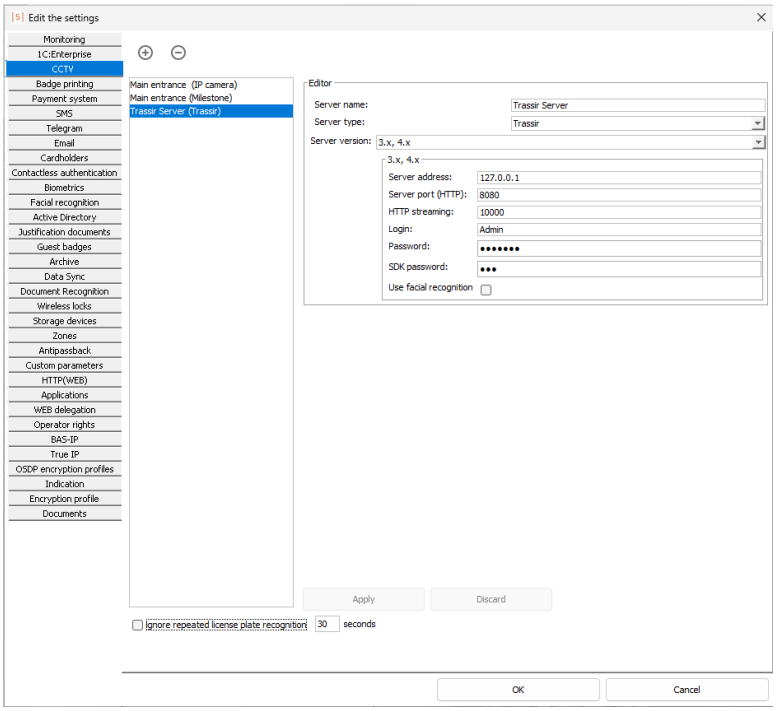
- To connect Sigur clients to the TRASSIR server you can use one of the existing user profiles or add a new one. Select the "Enable login from mobile/web" checkbox in the user profile settings (under "Server Settings" –> "Users" –> User profile –> "Setup").



Trassir user profile settings.

Sigur "Client" tool configuration:

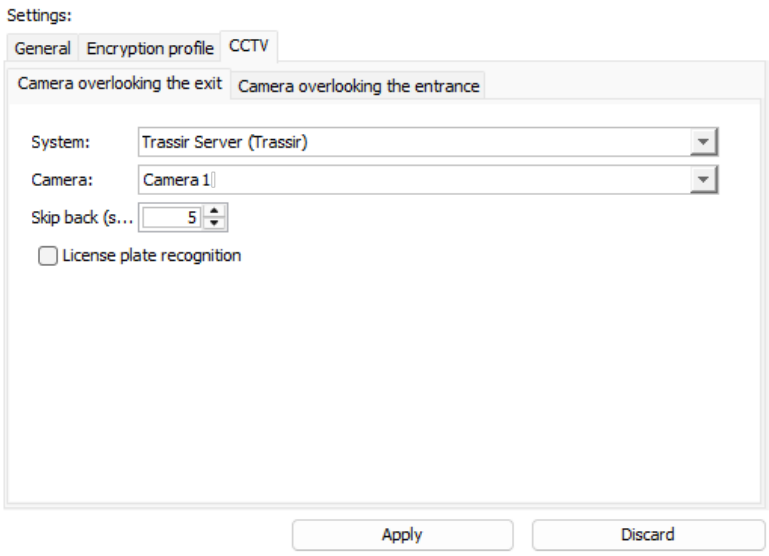
- In the "File" –> "Settings" –> "CCTV" menu, add a new source by clicking the "+" button. In the window that opens, enter the server name, set "Server type" to "Trassir" and click "OK".
- Set the TRASSIR server version to "3.x, 4.x".
- Enter the IP address of the TRASSIR server.
- Specify the server port (HTTP). The default value is 8080.
- Specify the "HTTP Streaming" port. The default value is 10000.
- Enter the login, password and SDK password.
- Click "Apply" and "OK" to save the settings.



Settings for the TRASSIR server in Sigur.

Now go to the "Access points" tab and select the access point where the TRASSIR camera is located.

Next, click on the "CCTV" tab and select the "Camera overlooking the entrance" camera subtab. Click on the dropdown list in the "System" parameter and select the added TRASSIR source. If the connection to the CCTV system is successful, a list of channels will be available in the "Camera" dropdown list. Select the required channel and click "Apply".



Access point settings.

Go to the "Monitoring" tab and select the default view "Video, photo and events log" from the dropdown list at the top of the window. Ensure that the checkbox for the required access point is selected in the "Access points list" block.

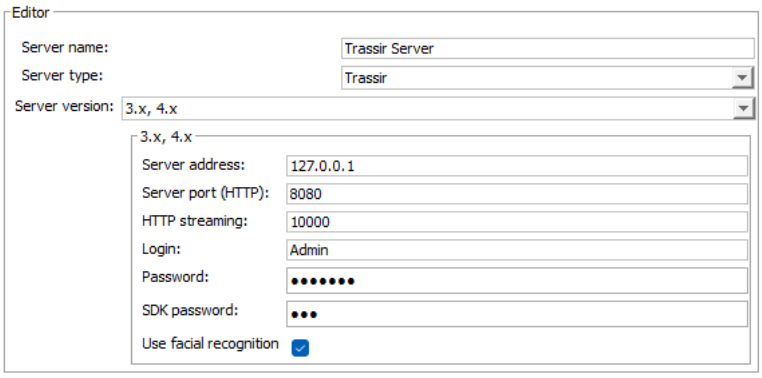
Next, present the card to the reader in the "Entry" direction. In addition to the cardholder information, you will see live video from the selected TRASSIR video channel.

To view the TRASSIR system snapshot and video archive, please refer to the instructions in the corresponding section.

17.4. Trassir facial recognition

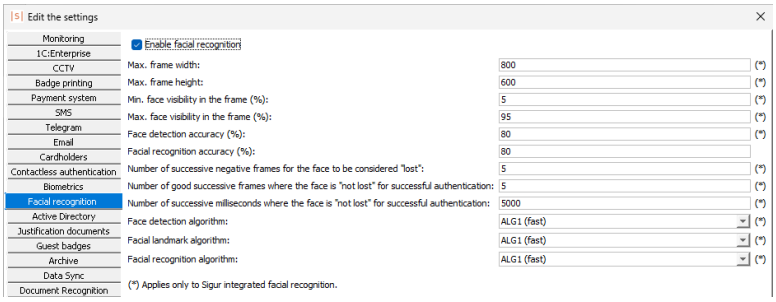
Let's set up the system to allow access to the premises via facial recognition, using TRASSIR as an example.

To do this, go to "File" –> "Settings" –> "CCTV", select the TRASSIR server you added earlier, select the "Use facial recognition" checkbox and click "Apply".



TRASSIR server settings.

Next, go to the "File" –> "Settings" –> "Facial recognition" and select the "Enable facial recognition" checkbox. You can leave the values of all parameters unchanged for now and save the settings by clicking the "OK" button.



"Facial recognition" tab.

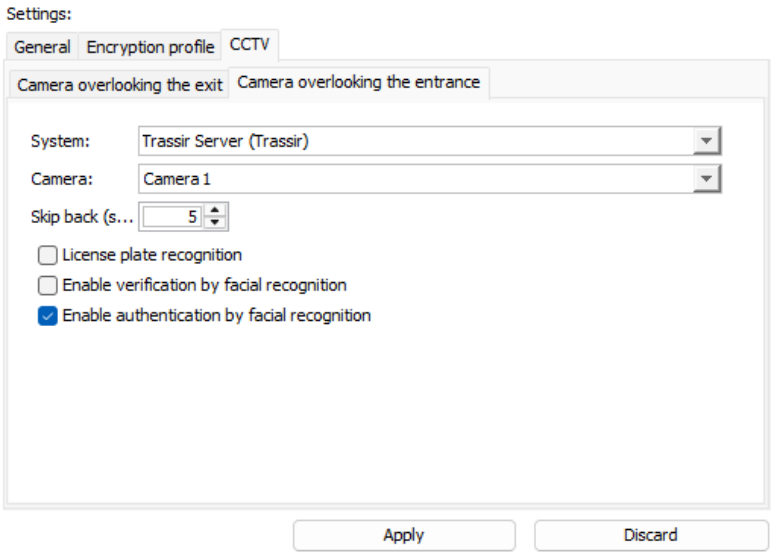
There are two facial recognition access modes available in the system:

1. Facial identification. The access decision is made by the Sigur ACS as soon as it receives a facial recognition event from an external system.
2. Facial verification. The access decision is made when a face is recognized after the main identifier (e.g., a card) is presented to a wall reader.

Facial identification.

Let's configure access in the "Entry" direction in the facial identification mode:

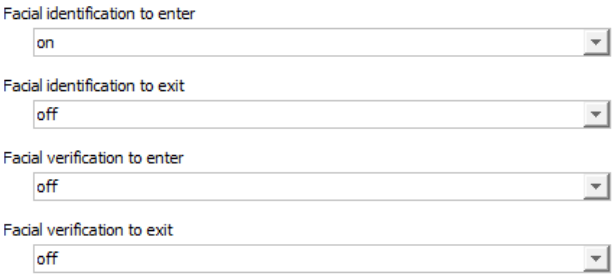
- Go to the "Access points" tab and select the access point to which the TRASSIR camera is assigned. Then click the "CCTV" tab, open the "Camera overlooking the entrance" subtab and select the "Enable authentication by facial recognition" checkbox. Click "Apply" to save the settings.



Access point settings.

- Grant a cardholder access to the TRASSIR camera's associated access point.
- Next, create a new level 2 rule on the "Rules" tab. Apply this rule to both the cardholder and the access point associated with the TRASSIR camera. Ensure that the "Days" subtab of the rule contains at least one day and time interval of access to this access point.

- Move to the "Special rules" subtab of that rule. When creating a new rule, "Facial identification to enter" and "Facial identification to exit" options are enabled by default. Ensure that the "Facial identification to enter" parameter is set to "On".



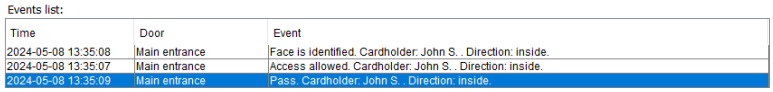
Time zone settings example.

- Save the settings by clicking "Apply".

It is very important that the direction in which the camera is assigned to the access point matches the access logic for facial recognition in the time zone settings.

Now let's move to the "Monitoring" tab.

When the TRASSIR system recognizes a face, an event of the type "Face is identified" is sent to the Sigur system. If the facial identification logic is configured, the system allows access in the "Inside" direction immediately after the cardholder's face is recognised.

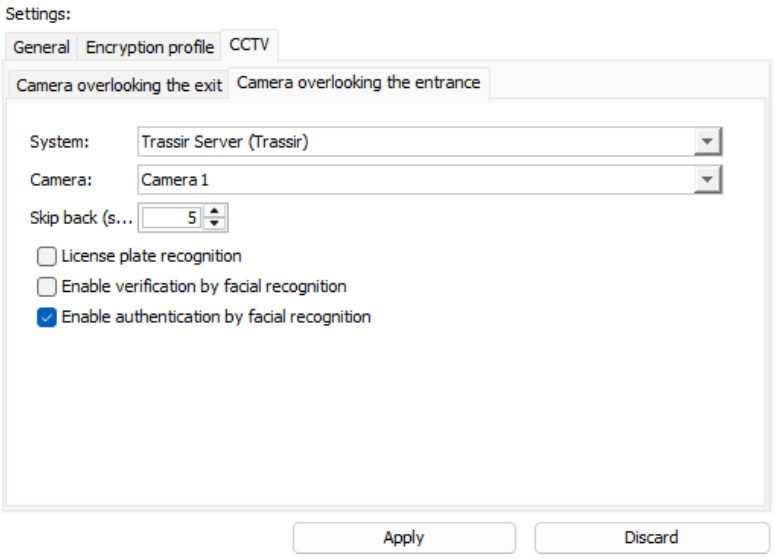


Events list.

Facial verification.

Now let's complicate the process of allowing access in the "Entry" direction by configuring the facial verification logic. In this case, the system will wait for a facial recognition event only after the cardholder's access card is presented to the wall reader.

To do this, go to the "Access points" tab and select the access point to which the TRASSIR camera is assigned. Then click the "CCTV" tab, select the "Camera overlooking the entrance" subtab and select the "Allow verification by facial recognition" checkbox. Clear the "Enable authentication by facial recognition" checkbox. Click "Apply" to save the settings.



Access point settings.

Let's go back to the "Rules" tab.

Edit the "Special rules" subtab of the level 2 rule you created earlier by setting the "Facial identification to enter" parameter to "Off".

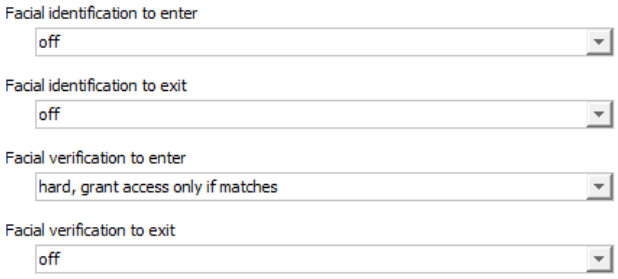
The following access options are available in the facial verification mode:

- "Soft, grant access anyway". In this case, the system allows access even if the

cardholder's face is not recognized. The event "Face is not identified" will be logged.

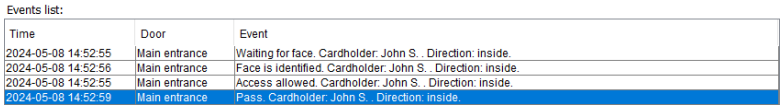
- "Hard, grant access only if matches". The system allows access only after receiving a facial recognition event of the cardholder to whom the access card belongs.
- "Soft group, grant access even if it does not match with any faces from the department". The system allows access even if the cardholder's face or the face of their colleagues from the department is not recognized. The event "Face is not identified" will be logged.
- "Hard group, grant access only if it matches a face from the department". The system allows access if the face of the cardholder or one of their departmental colleagues is recognized.

For now, in the "Facial verification to enter" block, select "Hard, grant access only if matches" from the dropdown list. Click "Apply" to save the settings.



Rule's settings example.

Go to the "Monitoring" tab. Present the card to the wall reader in the "Entry" direction. The system will start waiting for a facial recognition event to be received from the Trassir system. Access will be granted after receiving such an event.



Events list.

18. Face recognition terminals integration

At present, Sigur has integrated with several facial recognition systems. This guide focuses on setting up the system's interaction with Hikvision facial recognition terminals.

18.1. Hikvision face recognition terminals

The integration requires a license based on the number of Hikvision terminals connected to Sigur and the type of functionality used (basic - face recognition only, or advanced - face recognition + temperature measurement).

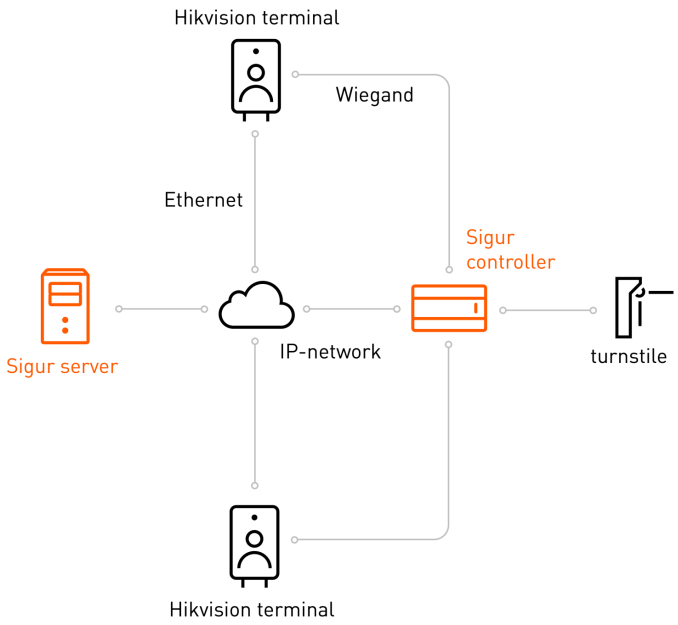
The following Hikvision terminal models are implemented and tested:

- Hikvision DS-K1TA70MIT.
- Hikvision DS-K1T671TM-3XF.
- Hikvision DS-K5671-3XF/ZU.
- Hikvision DS-K5604A-3XF/V.
- Hikvision DS-K1T671M.
- Hikvision DS-K1T341AM.
- Hikvision DS-K1T642MW.
- Hikvision DS-K1T671TMW.
- Hikvision DS-K5671-ZU.
- Hiwatch ACT-T1341M.

A Hikvision face recognition terminal must support the ISAPI protocol to interact correctly with Sigur.

18.1.1. Connecting a face recognition terminal to a Sigur controller

A face recognition terminal is connected to the local IP-network of the facility and to a Wiegand port of a Sigur controller, e.g. PORT3.



System interaction diagram.

The wiring diagram for connecting face recognition terminals to Sigur controllers can be found in the appendix to this manual.

18.1.2. Hikvision settings

The initial settings are made directly on the device itself.

It is necessary to:

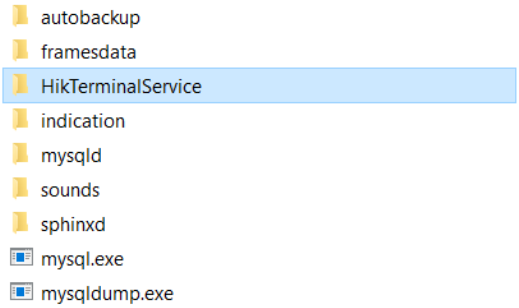
1. Create a user when activating the device (set login and password).
2. In the "Menu" –> "Communication Settings" –> "Network" section, set the static IP address of the terminal, the netmask, the gateway address and disable DHCP.
3. In the "Menu" –> "Communication Settings" –> "Wiegand" section, enable the Wiegand port, specify the "Output" direction and select the required Wiegand format.
4. In the "Menu" –> "Access Control Settings" section, select the type of identification: by face only, by card only, by card and face.

18.1.3. Sigur settings

Download the Hikvision integration service files (Windows OS, Linux Debian OS, Red Hat Linux OS).

Next, follow the instructions below:

- **Windows OS.** Extract the files from the downloaded archive to the "server" directory in the software installation folder (e.g. C:\Program Files (x86)\SIGUR access management\server\). The "server" directory should contain the "HikTerminalService" directory, which contains all the necessary components for the integration.



"SIGUR access management\server\" directory.

- **Linux Debian OS**. Install the downloaded package on the Sigur server using the command:

```
sudo dpkg -i hikterminalservice-x.x_all.deb
```

  where "x.x" is the version of the integration service.

- **Red Hat Linux OS**. Install the downloaded package on the Sigur server using the command:

```
sudo rpm -i hikterminalservice-x.x-0.el7.noarch.rpm
```

  where "x.x" is the version of the integration service.

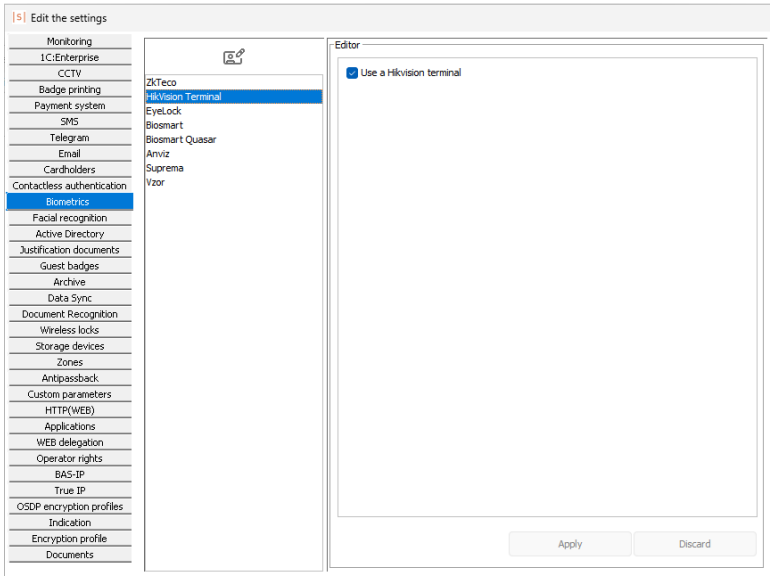
After that, restart the server module from the "State" tab in the "Server Administration" tool.

Let's assume that the Hikvision face recognition terminal is located at the entrance:

- Start the "Client" tool.
- Go to the "Access points" tab and select the access point to which you want to connect the Hikvision terminal.
- Click the "Settings" button and assign the "Port reader for enter" (or "Entrance reader port" - extended) function to the controller terminals to which the Hikvision terminal is connected (e.g. PORT3), then click "OK".

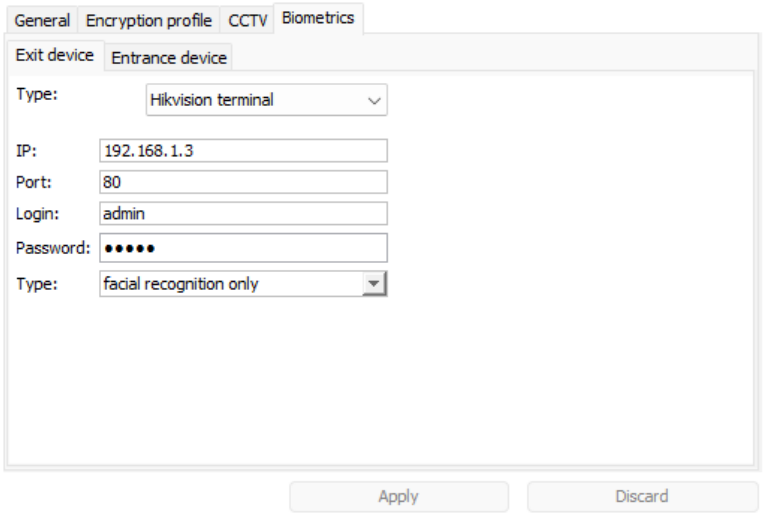
Sigur controller settings example.

- Go to "File" –> "Settings" –> "Biometrics", select the "Hikvision Terminal" and enable "Use Hikvision terminal" checkbox. Click "Apply" and "OK" to save the settings.



"File" –> "Settings" –> "Biometrics" menu.

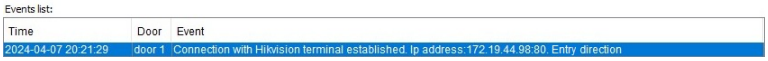
- A new "Biometrics" subtab will appear in the "Settings" block on the "Access points" tab. Expand the "Entrance device" subtab (according to the direction assigned to the controller port).
- Select "Hikvision terminal" from the "Type" dropdown list and enter the IP address of the Hikvision terminal (specified in its settings), port (port 80 is used by default), login and password of the user created when the device was activated. Click "Apply" to save the settings.



Access point's settings.

Go to the "Monitoring" tab. If the connection to the Hikvision terminal is

successful, the system will record the corresponding event.


Events list:

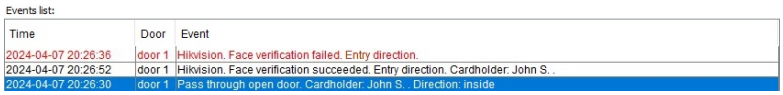
Time	Door	Event
2024-04-07 20:21:29	door 1	Connection with Hikvision terminal established. Ip address:172.19.44.98:80. Entry direction

Events list.

To transfer personnel information to the Hikvision terminal:

1. Add a photo to a cardholder's profile.
2. Assign the cardholder an access credential in Wiegand-26 or Wiegand-34 (HEX) format. If the cardholder does not have a physical access card, you can manually assign any number in these formats.
3. Grant the cardholder access to the access point to which the Hikvision terminal is assigned.

When the cardholder's face is recognized, the Hikvision terminal sends the corresponding event to the Sigur server via the IP-network and sends the Wiegand access code to the Sigur controller.


Events list:

Time	Door	Event
2024-04-07 20:26:36	door 1	Hikvision. Face verification failed. Entry direction.
2024-04-07 20:26:52	door 1	Hikvision. Face verification succeeded. Entry direction. Cardholder: John S. .
2024-04-07 20:26:30	door 1	Pass through open door. Cardholder: John S. . Direction: inside

Events list.

The Hikvision terminal also sends temperature measurement results and temperature threshold violation alerts to the Sigur server (if enabled in the terminal settings).

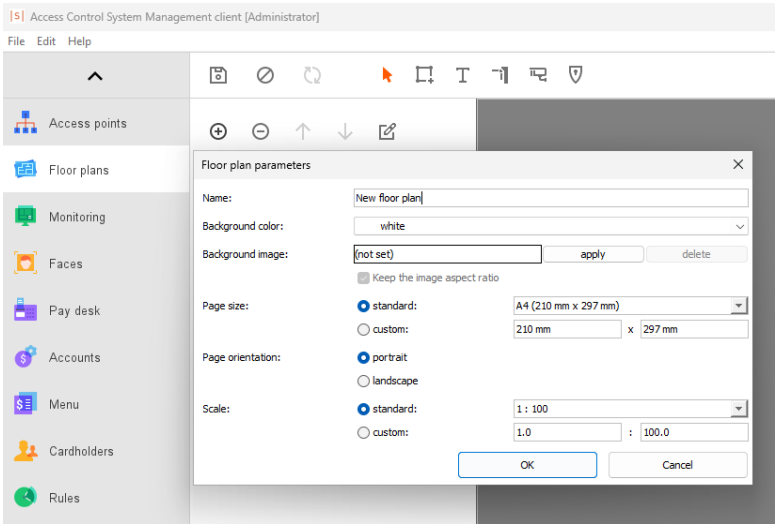
The recorded events can be viewed on the "Monitoring" and "Archive" tabs.

If you have an "Event Response" license, you can set system responses to events sent from the Hikvision terminal. Refer to the "Event Responses" section for more details on this functionality.

19. Floor plans

The "Floor plans" tab is used to create and configure floor plans, including specifying access points and CCTV cameras locations.

To create a new floor plan, click the "+" button. In the "Floor plan parameters" window that opens, you can enter any name, upload a background image and set the size and orientation of the plan. You can leave these values unchanged for now and click "OK".



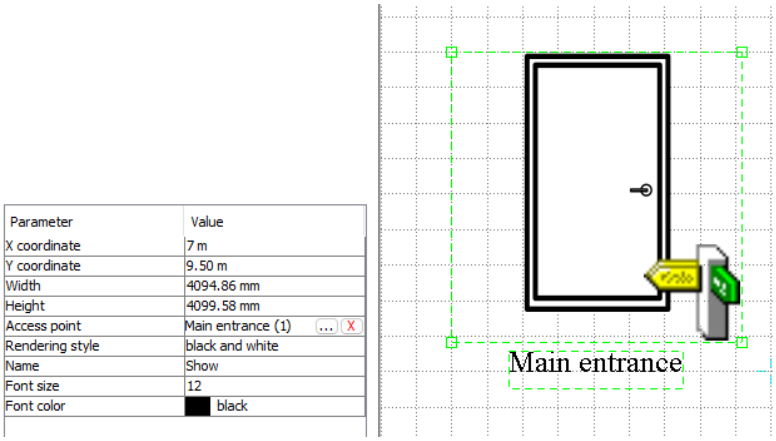
Creation of a new floor plan.

To add an access point, select the "Add access points" tool from the top toolbar. Use the mouse to place an item on the map.

"Add access points" tool.

In the properties window on the left, locate the "Access point" parameter and click the "..." button. Select the required access point from the list that appears and click "OK".

The image on the floor plan will change according to the type of access point selected.



Door on the floor plan.

The current status of the access point is also displayed on the floor plan.

Access point status icons.

Status icon	Description
	The access point is in normal mode.
	The access point is in unlocked mode.
	The access point is in locked mode.
	There is no connection with the access point.
	Access point status could not be obtained.
	The door is being held open (only for "Door" type access points with the "Time in open state for door before 'close the door' signal activation" option enabled in the settings).

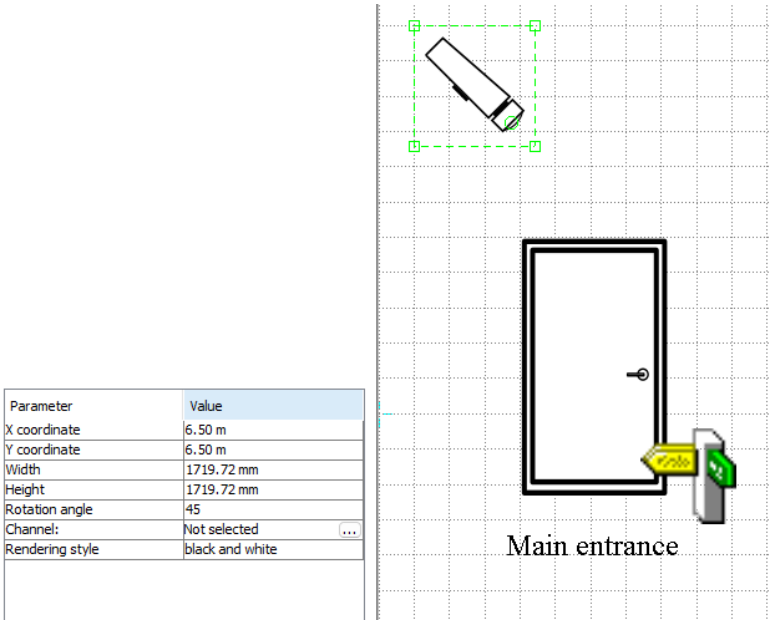
Let's add the previously configured CCTV camera to the floor plan.

To do this, select the "Add cameras" tool in the top toolbar. Use the cursor to place a camera on the map.

"Add cameras" tool.

In the window that appears on the left, locate the "..." button associated with the "Channel" parameter and click it. Select the previously configured camera from the dropdown list and click "OK".

You can also change the angle of the camera on the floor plan by entering a numeric value in the "Rotetion angle" text box. Double-click the text box, set the "Rotation angle" parameter to 45 degrees and press "Enter".

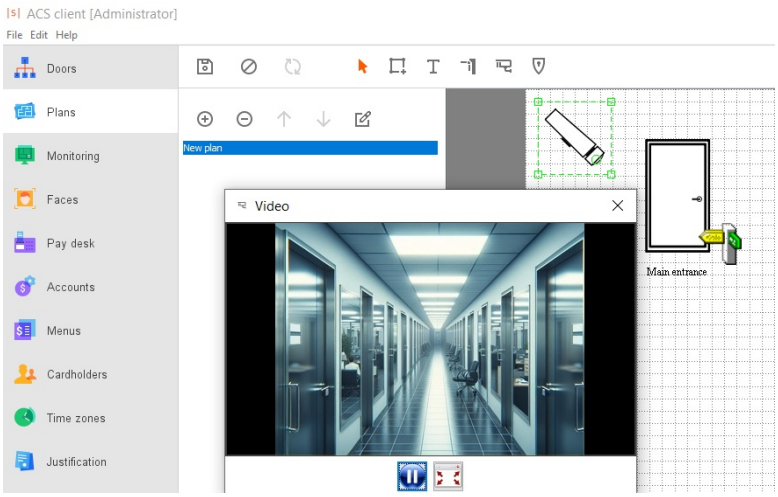


CCTV camera on the floor plan.

To save the changes to the floor plan, click the "Save changes" button in the top toolbar.

"Save changes" tool.

To view live video from the CCTV camera, double-click on its image on the map.



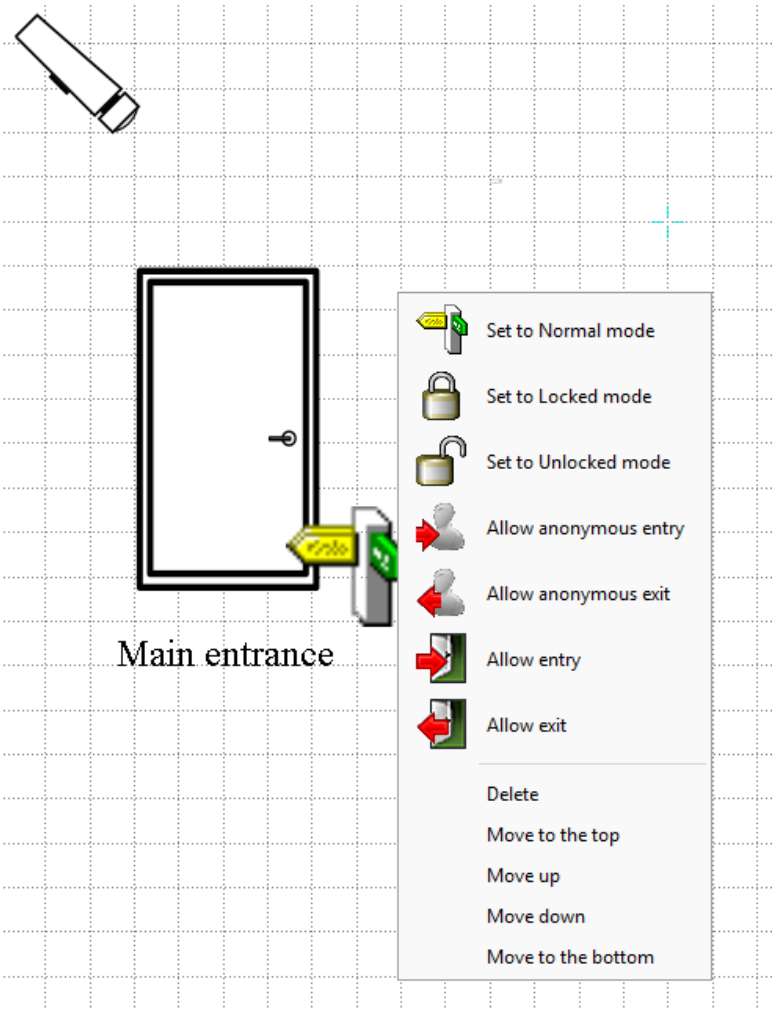
Live video display on the floor plan.

To manage the access point, right-click on its image on the plan. The following options are available in the menu that appears:

- "Set to Normal mode". Puts the access point in normal mode. The access

point is controlled by the ACS controller.

- "Set to Locked mode". Forces the locking mechanism of the access point to close.
- "Set to Unlocked mode". Forces the locking mechanism of the access point to open.
- "Allow anonymous entry". Unlocks the access point for entry (single pass). The system event is registered as "Pass allowed by button."
- "Allow anonymous exit". Unlocks the access point for exit (single pass). The system event is registered as "Pass allowed by button."
- "Allow entry". Unlocks the access point for entry (single pass). You can allow access for a specific cardholder. The system event is registered for that cardholder.
- "Allow exit". Unlocks the access point for exit (single pass). You can allow access for a specific cardholder. The system event is registered for that cardholder.

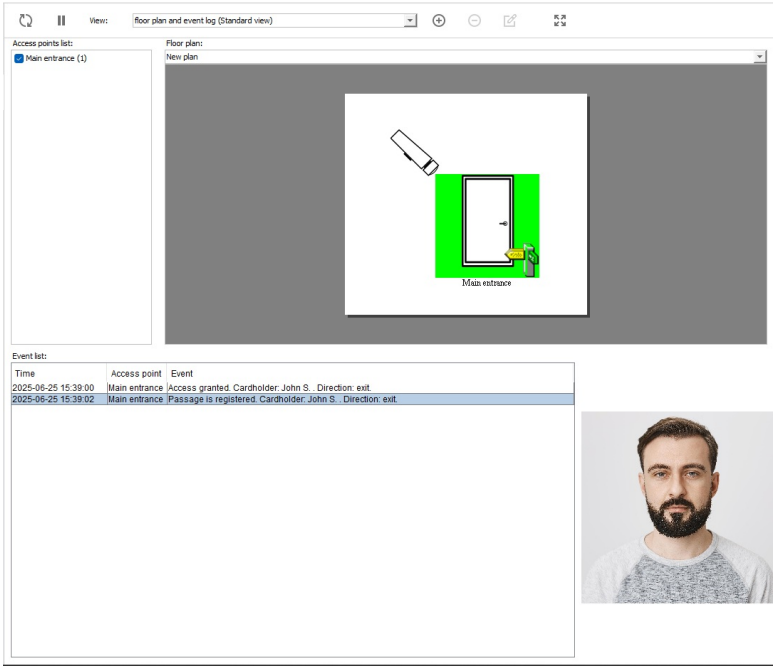


Pop-up menu.

You can also manage elements on the floor plan directly from the "Monitoring" tab. To do this, go to the "Monitoring" tab, select the default "Floor plan and event

log" template and select the checkbox in the "Access points list" block to receive system events from an access point.

You can now manage the status of the access point, unlock the access point for a single pass and view live video from the surveillance cameras by right-clicking on the elements in the floor plan.



Floor plan on the "Monitoring" tab.

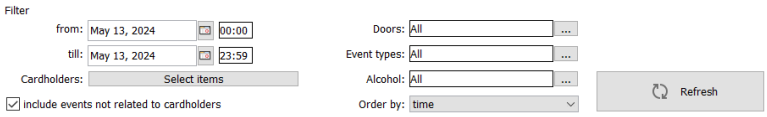
The floor plan we have created is the only one in the system so far, so it is automatically displayed in the "Monitoring" tab. If you want to manage items on more than one floor plan in the system, you will need to create a separate view template on the "Monitoring" tab for each floor plan.

20. Events archive

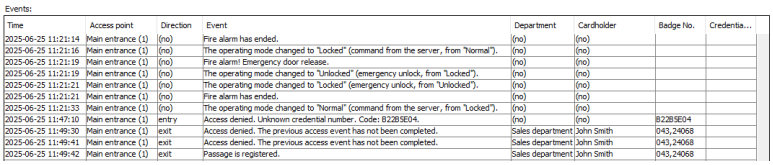
The "Archive" tab is used to obtain information about events that have occurred in the system during a given period. This tab provides quick access to information as the system does not generate reports to be opened in third party software.

Let's get the list of events that have occurred in the system for the current day:

- By default, the "from/till" period in the "Event filter" panel is already set to the current date.
- You can select the cardholders for whom the system events are to be filtered. To do this, click the "Enables, include only selected" in "Filter by cardholders block and the push "select" button. Move the cardholders to the right part of the window using the ">>" button and click "OK".
- Select the "Include events not related to cardholders" checkbox to obtain additional system events.
- Click "Update".



Filter panel.



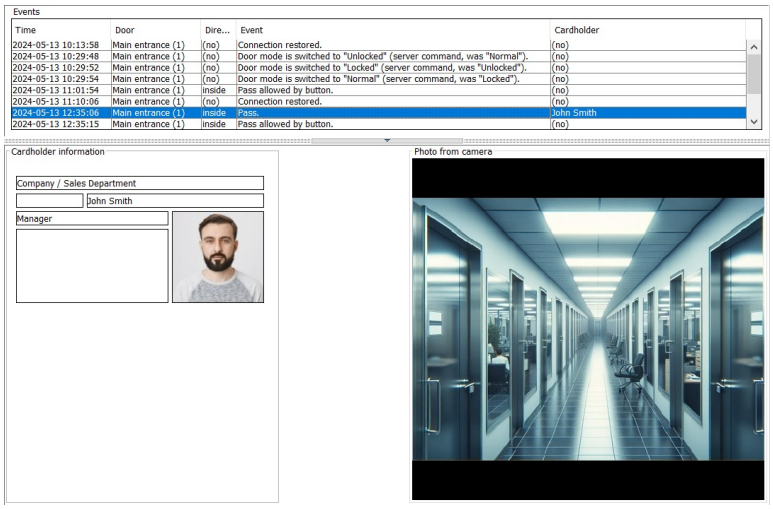
System events.

To view the video recorded by a CCTV camera at the time of the event, double-click the event in the list. You can also use the "Show the video archive from the entrance/exit camera" buttons at the top of the window.

"Show the video archive from the entrance/exit camera" buttons.

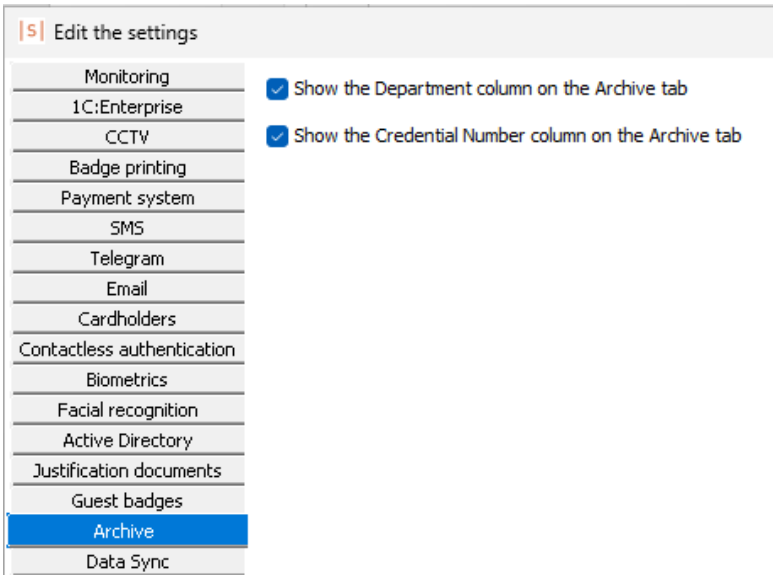
To view snapshots from the camera at the time of the event and to view cardholder information, expand the additional panel by clicking the arrow button at the bottom of the window.

The information in the panel will update as a particular event is highlighted in the list. You can save a photo from an IP camera connected via RTSP by right-clicking on the image in the panel and then selecting the "Save to file" option from the context menu (this feature does not apply to integrated video surveillance systems).



Additional panel.

If required, you can view the cardholder's department and access code (and its description, if enabled) in the system events list. To access this feature, go to the "File" –> "Settings" –> "Archive" menu and select the appropriate checkboxes.



"File" –> "Settings" –> "Archive" menu.

The list of events can be saved in an MS Excel file. To do this, click the corresponding button at the top of the "Archive" tab.

"Save the selected events to MS Excel" button.

21. System reports

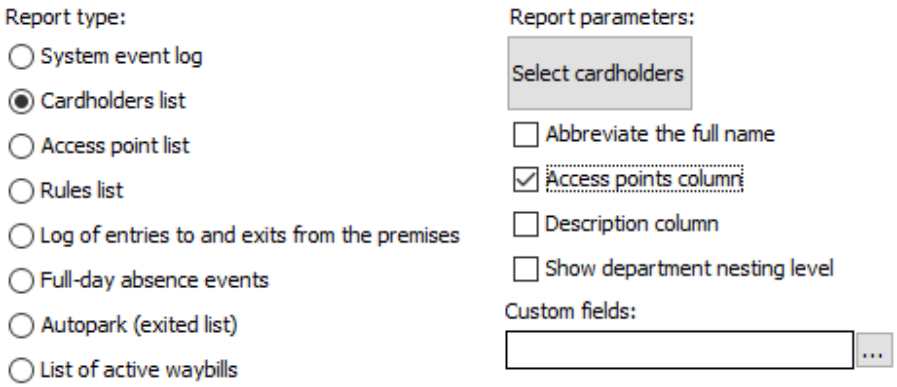
The "Reports" tab is used to generate reports on cardholders, rules, and events registered by the system throughout its operation. The reports are generated in MS Excel format (.xlsx). The number of reports available depends on the type of license you have purchased.

Let's generate the "Cardholders list" report:

1. Go to the "Reports" tab and select the "Cardholders list" option from the list.

2. Click the "Select cardholders" button in the "Report parameters" block. In the window that opens, use the ">>" button to move the required cardholders or departments from the left column to the right column and click "OK".

3. You can select some additional checkboxes to include more information in the report. You can also include values from custom fields that you have already created. To do this, click the "..." button in the "Extra params" block, select the required parameters and click "OK".



Report settings.

4. To retrieve the report, click the "Generate the report" button.

Cardholders list

Created on: 10.09.2025 15:36:53

Record type	Name	Department	Position / model	Personnel Number	Rule	Credential	Issued on	Expires on	Phone number	Operator
Employee	Charles Williams	HR	HR manager	00000003	By default	5F1842C7	2024-05-13 13:08:32	unlimited	+1 234 567-89-03	
Employee	John Smith	Sales department	Manager	00000001	By default	CE30F876	2024-05-13 12:34:44	unlimited	+1 234 567-89-02	
						042,24068	2025-09-10 15:13:35	unlimited		
Employee	Mary Johnson	Marketing department	Senior Specialist	00000002	By default	47D36B1F	2024-05-13 13:08:32	unlimited	+1 234 567-89-01	
Employee	Sarah Brown	Accounting office	Accountant Officer	00000004	By default	EC790D63	2024-05-13 13:08:32	unlimited	+1 234 567-89-00	Accountant Officer
						129,10664	2025-09-10 15:28:00	unlimited		

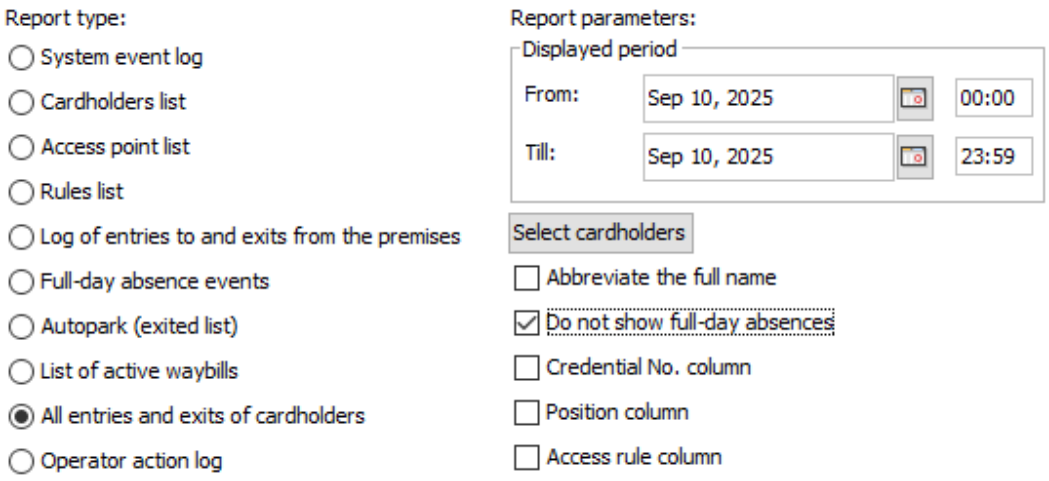
"Cardholders list" report.

Now let's get the "All entries and exits of cardholders" report:

1. In the "Report parameters" block, select the period for which you would like to generate the report.

2. Click the "Select cardholders" button, select the required number of cardholders, move them to the right column and click "OK".

3. You can also select some additional checkboxes to include more information in the report.



Report settings.

4. To retrieve the report, click the "Generate the report" button.

All entries and exits of cardholders

Created on:	10.09.2025 15:33:19
Period start date:	10.09.2025 00:00:00
Period end date:	11.09.2025 00:00:00

Date	Department	Name	Personnel Number	Access event		
				time	access point	direction
2025-09-10	Accounting office	Sarah Brown	00000004	15:28	Main entrance (1)	entry
2025-09-10	HR	Charles Williams	00000003	15:27	Main entrance (1)	entry
2025-09-10	Sales department	John Smith	00000001	15:25	Main entrance (1)	entry
				15:26	Main entrance (1)	exit
				15:27	Main entrance (1)	entry

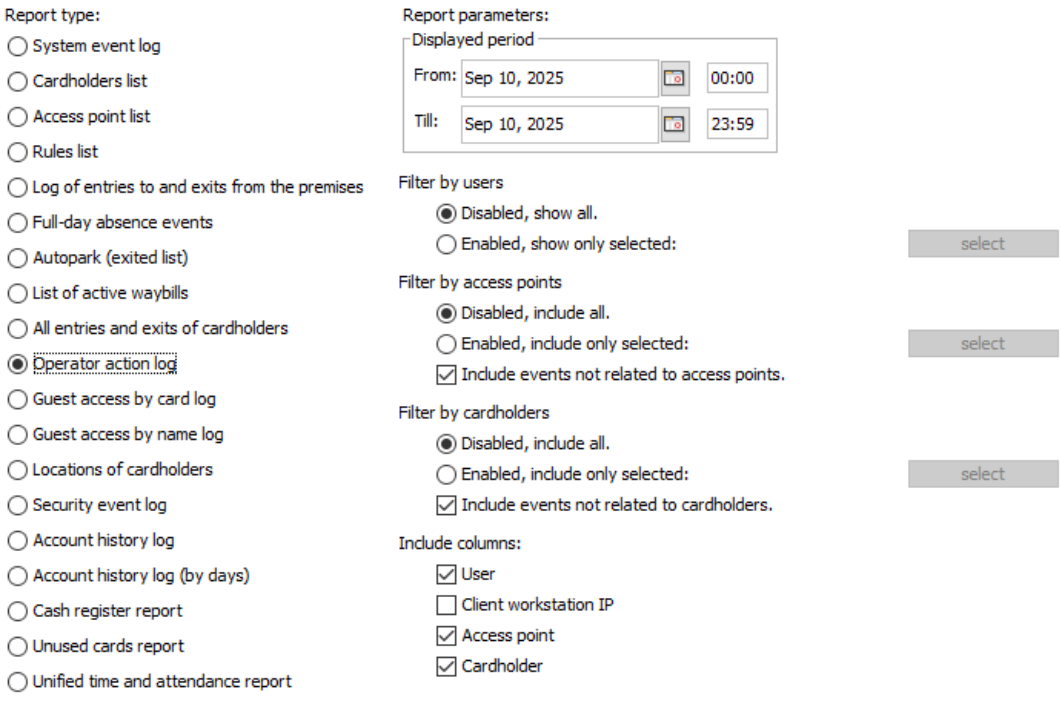
"All entries and exits of cardholders" report.

You can also generate an "Operator action log" report to track changes made by system users:

1. In the "Report parameters" block, select the period you wish to generate the report.

2. You can then filter the report by users, access points and cardholders whose profiles have been modified, or leave the filter off.

3. You can also select additional columns to include in the report.



Report settings.

4. To retrieve the report, click the "Generate the report" button.

Operator action log

Time	Operator	Access point	Cardholder		Action
			Personnel Number		
2025-09-10 15:02:38	Administrator	(no) (0)	(no)	(no)	The user has connected to the server
2025-09-10 15:04:41	Administrator	(no) (0)	(no)	(no)	The report "Cardholders list" is requested.
2025-09-10 15:12:27	Administrator	Main entrance (1)	(no)	(no)	The access point properties have been changed.
2025-09-10 15:13:07	Administrator	(no) (0)		John Smith	The cardholder has been moved to department "Marketing department".
2025-09-10 15:13:35	Administrator	(no) (0)		John Smith	Credential "042,24068" added. Expires on: unlimited.
2025-09-10 15:13:35	Administrator	(no) (0)		John Smith	The cardholder parameters have been changed.
2025-09-10 15:13:41	Administrator	(no) (0)		John Smith	The cardholder parameters have been changed.
2025-09-10 15:13:47	Administrator	Main entrance (1)	(no)	(no)	The access point operating mode change to "Unlocked" is requested.

"Operator action log" report.

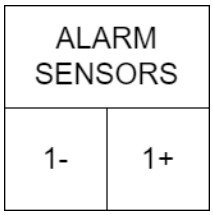
22. Alarm zones

With Sigur ACS, you can create and manage alarm zones and receive events from them.

You can connect alarm loops to Sigur E2 and E4 controllers. A Sigur E2 controller can handle one alarm loop and a Sigur E4 controller can handle two alarm loops. Each loop is treated by the system as a separate alarm zone.

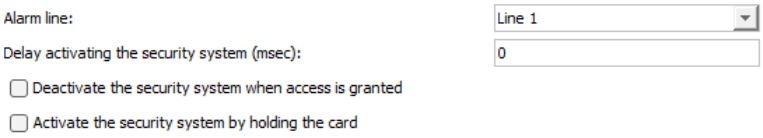
An alarm loop is connected to the "ALARM SENSORS" terminal block of a Sigur E2/E4 controller. These terminals are supplied with 12 V by the controller to power the alarm sensors. Normally, the connected alarm loop must have a constant resistance of 3.3...6.2 kOhm.

Alarm loop wiring diagrams are provided in the appendix to this manual.



"ALARM SENSORS" terminal block.

Once the alarm loop is connected to the controller, it must be assigned to an access point. To do this, go to the "Access points" tab, select the access point of a Sigur E2 or E4 controller and click the "Settings" button. In the "Alarm line" block select "Line 1" from the dropdown list and click "OK".



Controller's settings.

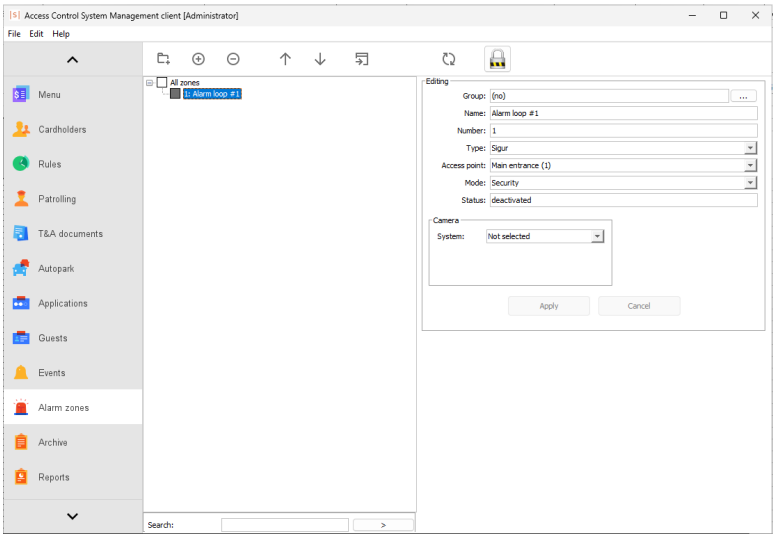
The next step is to configure the alarm loop for subsequent monitoring. Let's go to the "Alarm zones" tab.

Select "All zones" option from the list and create a new alarm zone by clicking the "+" button. The "Editing" panel will be available in the right part of the application window. Set the "Type" parameter value to "Sigur" and select the access point to which the alarm loop is assigned. Click "Apply" to save the settings.

Then restart the server module or restart the Sigur controller to which the alarm loop is connected.

The "Status" parameter value will then change to "deactivates" and the color of the

alarm zone status indicator will change to grey.



"Alarm zones" tab.

To arm the alarm loop, click the "Activate the security system" button.

"Activate the security system" button.

The "Status" parameter value will change to "activated" and the color of the alarm zone status indicator will change to green.

In the "activated" state, if any sensor on the loop is triggered and the resistance value on the "ALARM SENSORS" terminals deviates from the normal range (3.3...6.2 kOhm), the controller will record an alarm event, the "Status" parameter value for the alarm zone will change to "alarm" and the color of the alarm zone status indicator will change to red.

The alarm signal will continue until the user disarms the loop by clicking the "Deactivate the security system" button.

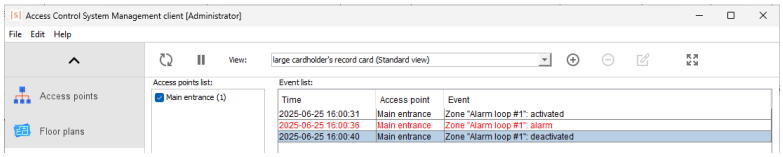
"Deactivate the security system" button.

Description of alarm zone status indicators.

Indicator colour	Description
Green	The alarm zone is successfully armed.
Orange	An unsuccessful attempt to arm the alarm zone.

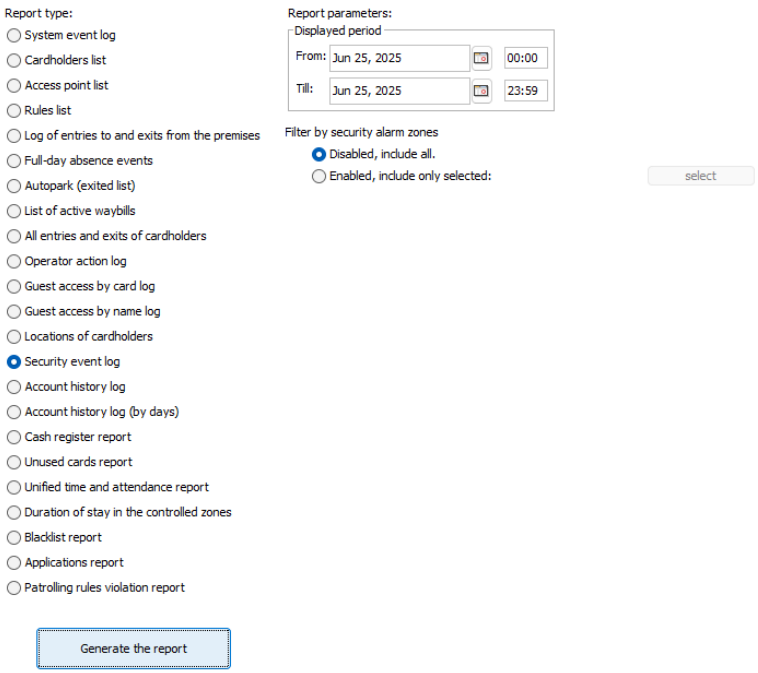
Indicator colour	Description
Red	An alarm event has been registered in the armed alarm zone.
Grey	The alarm zone is successfully disarmed.
White	There is no information on the status of the alarm zone.

Changes to the status of alarm zones are displayed on the "Monitoring" tab. You need to select the checkbox associated with the required access point in the "Access points" block beforehand.



"Monitoring" tab.

Events related to alarm zones are not included in the system events archive. To obtain the list of alarm zone events, go to the "Reports" tab. Then select the "Security event log" option from the list, set the covered period in the "Report parameters" block, select the required alarm zones and click the "Generate the report" button.



Report settings.

Date and time	Zone	Event
2025-06-25 15:58:14	Alarm loop #1	activated
2025-06-25 15:59:00	Alarm loop #1	alarm
2025-06-25 15:59:27	Alarm loop #1	deactivated
2025-06-25 16:00:31	Alarm loop #1	activated
2025-06-25 16:00:36	Alarm loop #1	alarm
2025-06-25 16:00:40	Alarm loop #1	deactivated

"Security event log" report.

You can also manage alarm zones and view their status on floor plans.

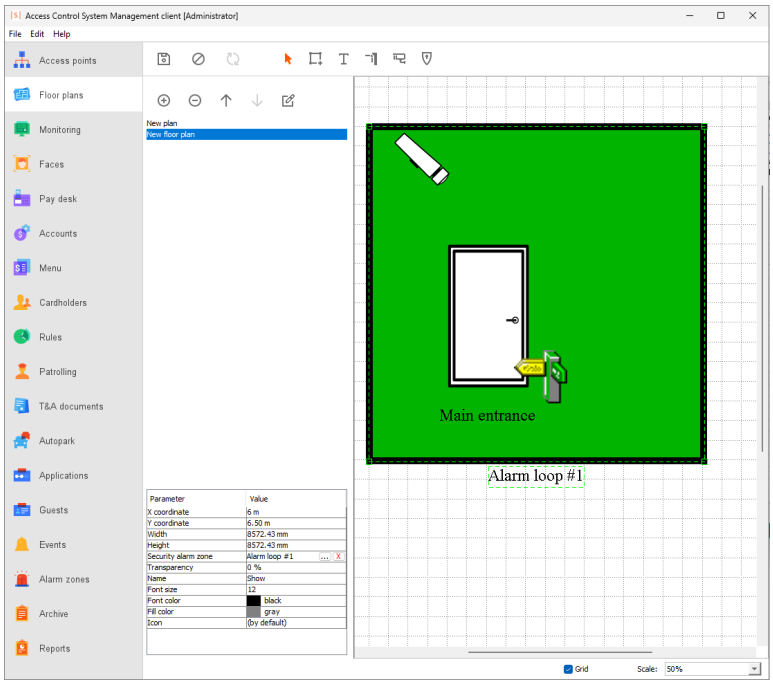
Let's go to the "Floors plans" tab. Here you can create a new floor plan or add alarm zones to the one you have already created (instructions on how to create floor plans can be found in the corresponding section).

Click the "Add a security alarm zone" button on the top toolbar and use the mouse to place an alarm zone on the floor plan.

"Add a security alarm zone" button.

In the properties window that appears on the left, click the "..." button for the "Security alarm zone" parameter. Select the required alarm zone from the list that opens and click "OK". The area created on the floor plan will change its color according to the current status of the alarm zone.

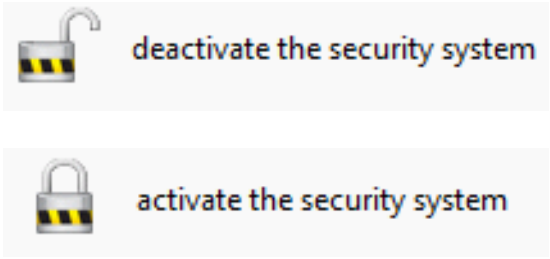
In the example below, the alarm zone has been moved to the background of the floor plan. To do the same, right-click on the alarm zone and select "Move to the bottom".



Alarm zone on the floor plan.

To save the changes you have made, click the "Save changes" button on the top toolbar.

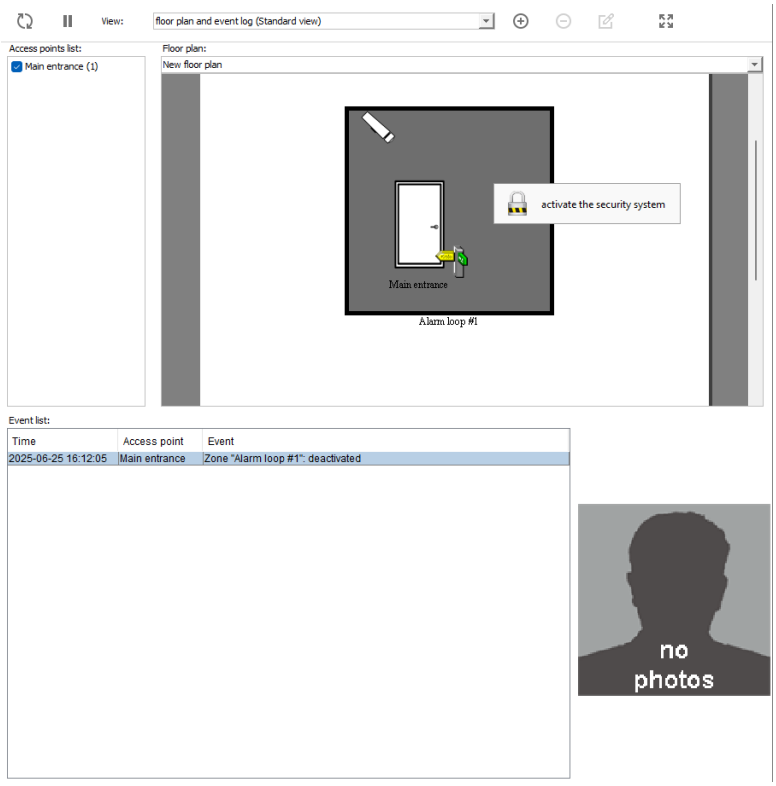
To control the alarm zone state, right-click on its area and select "Deactivate the security system" or "Activate the security system" from the pop-up window.



Pop-up window options.

You can view the floor plan and manage alarm zones from the "Monitoring" tab.

For instructions on how to manage floor plans, please refer to the corresponding section.



"Monitoring" tab.

23. Event responses

The system provides the opportunity to set up responses to various Sigur ACS events, e.g. set up actions to be performed when access is denied due to card expiration, when a fire alarm is triggered, or set up system actions to be repeated on a schedule.

System responses can include actions such as sending notifications (email, SMS), managing access points (unlock, block), etc.

The "Event Response" software module is required to configure this functionality.

Event responses are configured within the "Events" tab. To create a new response, you need to:

1. Click the "+" button on the top toolbar.
2. Select a system event in the "Event" block.
3. Configure the system response in the "Edit event response" block.
4. Click "Apply".

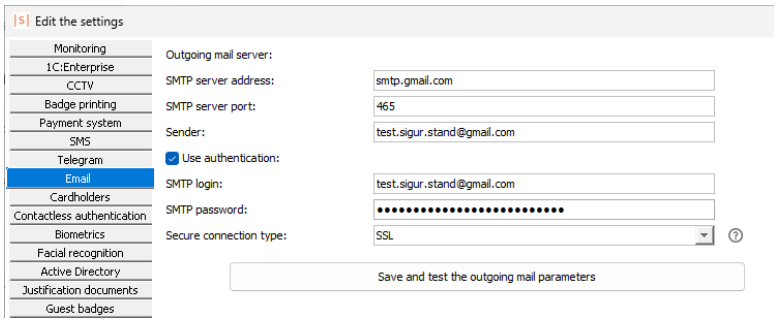
The decision to respond to an event is made by the Sigur server. If an immediate response to an event is required, there must be a connection between the controller and the server at that moment. Check the "Access points" tab to see if access points are online.

The following are examples of event response configurations for system events. If required, you can configure custom system responses by combining events and actions.

Alert messaging configuration.

Let's configure alerts to notify the system administrator by email or SMS when an access point goes offline. First:

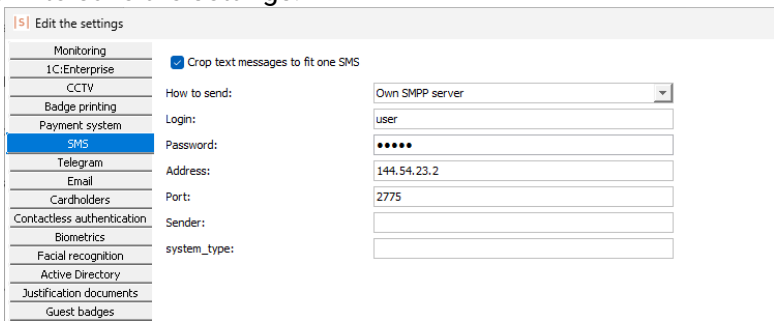
- Email: Configure the system to interact with an external SMTP server used by Sigur ACS to send emails. To do this:
  - Go to the "File" –> "Settings" –> "Email" menu.
  - Fill in the "Outgoing messages" block with your SMTP server details.
  - Test the connection by clicking the "Save parameters and test" button.
  - Save the settings by clicking "OK".



SMTP server settings.

- SMS: Select your preferred method of sending SMS messages, for example using a custom SMPP server. To do this:

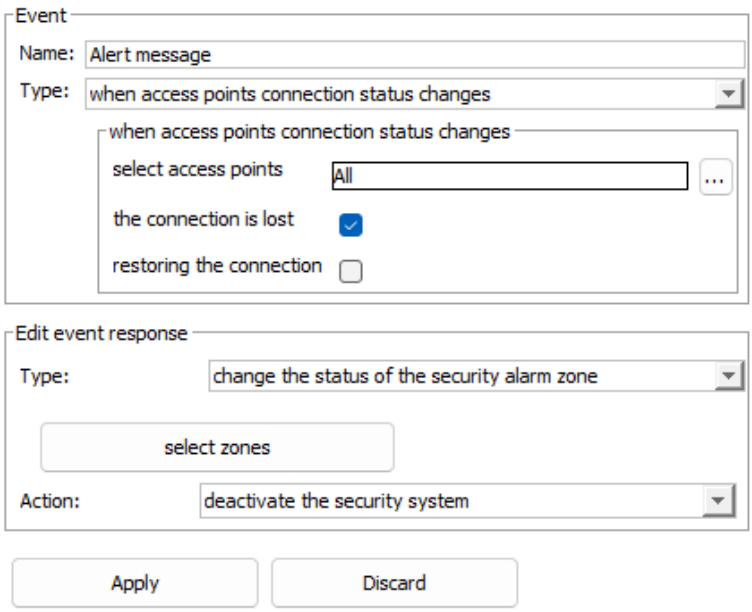
  - Go to the "File" –> "Settings" –> "SMS" menu.
  - Select "Own SMPP server" from the "How to send" dropdown list.
  - Fill in the parameters as recommended by your service provider.
  - Click "OK" to save the settings.



Own SMPP server settings.

Next, go to the "Events" tab and click the "+" button. Enter a name for the event response.

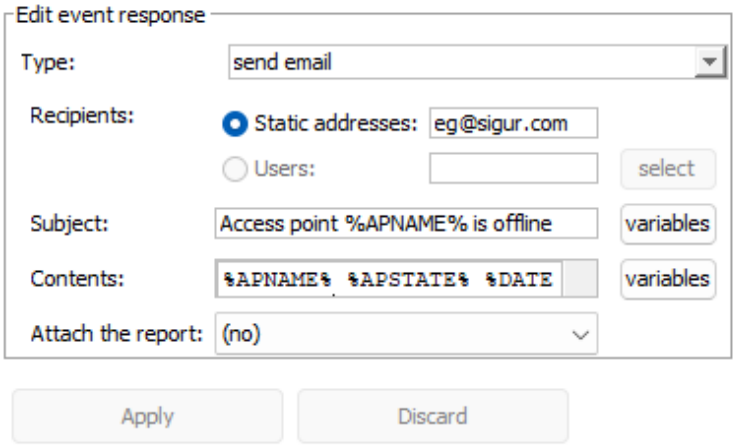
In the "Event" block, select "when access points connection status changes" from the "Type" dropdown list. Then click on the "Select access points" button, select the required access points and click "OK". Select the "the connection is lost" checkbox.



"When access points connection status changes" event type.

Next, select the type of system response in the "Edit event response" block:

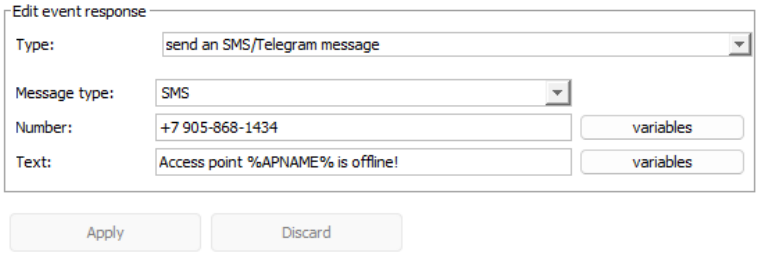
- "Send email":
  - In the "Static addresses" text box, enter the email address of the recipient.
  - In the "Subject" text box, you can type any text and use some variables. For example, type the text "Access point" and then click the "Variables" button. In the window that opens, double-click on the variable "Access point name" and then add the text "is offline". The "Subject" text box will now contain the value "Access point %APNAME% is offline".
  - Similarly, you can type any text in the "Content" text box, for example "%APNAME% %APSTATE% %DATE% %TIME%".



"Send email" reaction.

- "Send SMS/Telegram message".

- Select SMS from the "Message type" dropdown list.
- Enter the phone number in the "Number" text box. The phone number must be in E.164 format, with a "+" and the country code at the beginning of the number. You can enter multiple numbers separated by commas.
- Then type any message in the text box. To use variable values in the SMS text, click the "Variables" button and double-click the desired variable in the window that opens.



"Send SMS/Telegram message" reaction.

Click the "Apply" button to accept the changes.

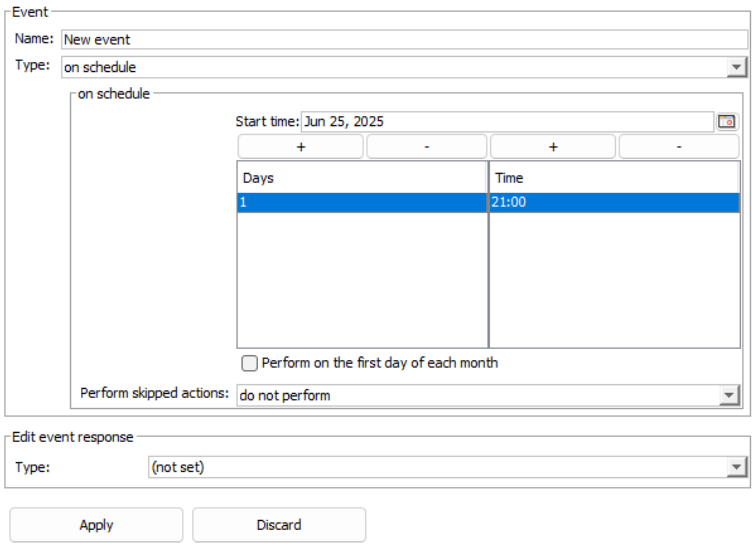
Automatic alarm zone control configuration.

Let's configure the scheduled arming and disarming of alarm zones.

Go to the "Events" tab and click the "+" button. Enter a name for the event response.

In the "Event" block, select "On schedule" option from the "Type" dropdown list. Next, set the start date and add a new entry in the "Days" block by clicking the "+" button. Then click the "+" button in the "Time" block and specify when the action should be performed.

You can also set the rule to perform event responses that were skipped because the controller did not communicate with the Sigur server. For now, select "Perform all" in the "Perform skipped actions" block. In this case event responses will be executed when the connection between the controller and the server is re-established.



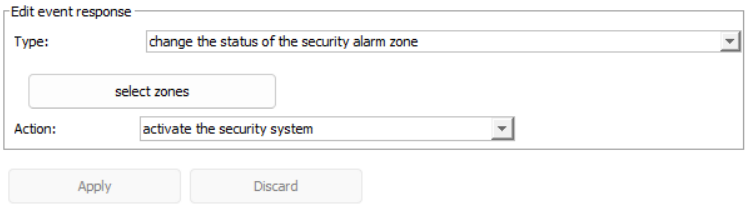
"On schedule" event type.

The selected event response will be executed repeatedly according to the schedule specified in the "Days" block. If only one day is added, the action will be executed at the same time each day.

In the "Edit event response" block, select "Change the status of the security alarm zone" from the "Type" dropdown list.

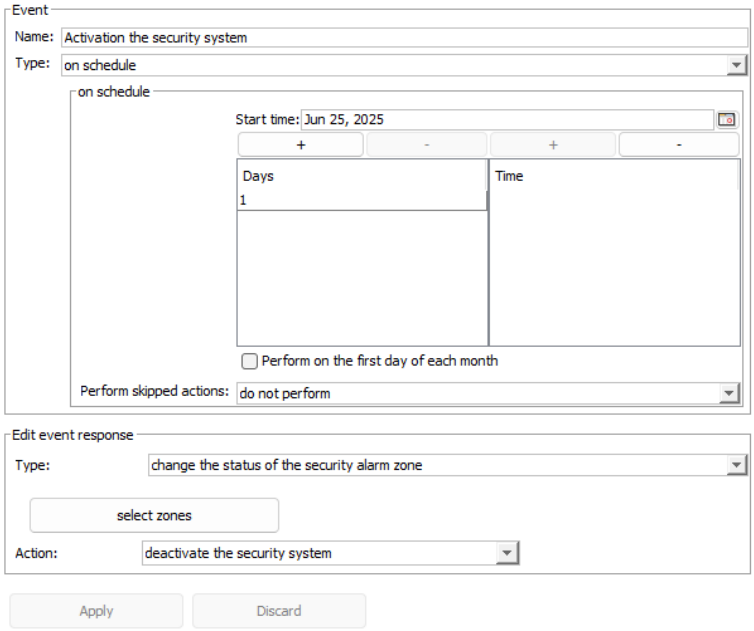
Click the "Select Zones" button. In the window that appears, use the ">>" button to move the required alarm zones to the "Selected zones" area on the right and click "OK". Next, select "Activate the security system" from the "Action" dropdown list and click "Apply".

The alarm zones will then be armed at the time you have specified.



"Change the status of the security alarm zone" reaction.

Similarly, create an event response for disarming the alarm zones.



Scheduled disarming of alarm zones.

Click "Apply" to accept the changes.

24. Synchronizing data from external sources

Sigur ACS can cyclically receive cardholder information from a third party system and transfer access card numbers and system event data to external databases. By synchronizing cardholder data from an external source, manual administration of the Sigur ACS database can be significantly reduced or eliminated.

A "Data Sync" software module is required to configure such functionality.

The following data sources are currently supported:

- Any database that can be accessed via the standard ODBC interface. This includes all major databases, including Oracle and MS SQL.
- LDAP directory services, including Active Directory.

24.1. External SQL database data synchronization

Let's synchronize data from an external SQL database via an ODBC interface.

You need to install a 32-bit ODBC driver for the selected database on the computer where the Sigur server is deployed.

24.1.1. Synchronizing cardholder data

To configure this functionality, start the "Client" tool and go to the "File" –> "Settings" –> "Data sync" menu.

Data synchronization requires a unique identifier for each cardholder in the external database.

To create a new synchronization source, proceed as follows:

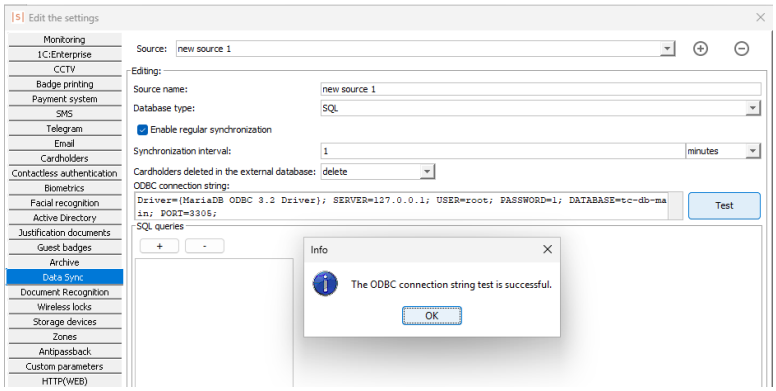
1. Click the "+" button in the "Source" block.
2. Enter any source name in the "Editing" block and select "SQL" from the "Database type" dropdown list.
3. Next, select the "Enable regular synchronization" checkbox and enter the required synchronization interval (the default is 1 minute, but it is recommended that you set a higher value).
4. You can also specify what happens to previously synchronized cardholders when they are deleted in the external system. Cardholders can be deleted in Sigur, or they can be moved to a specific department and their access cards will then expire. By default, the "People deleted in external DB" parameter is set to "Delete".
5. Next, you need to specify the ODBC connection string for the database you are

using. The required ODBC connection string can be found on third party websites (including here).

For example, to connect to MariaDB using the ODBC driver version 3.1, the following connection string can be used:

```
Driver={MariaDB ODBC 3.1 Driver}; SERVER=mydatabase.mydomain.com;
USER=odbc_user; PASSWORD=odbc_pw; DATABASE=odbc_test;
PORT=3306;
```

6. Test the connection to the external database by clicking "Test". The system will inform you whether the connection was successful or not.



Connection test.

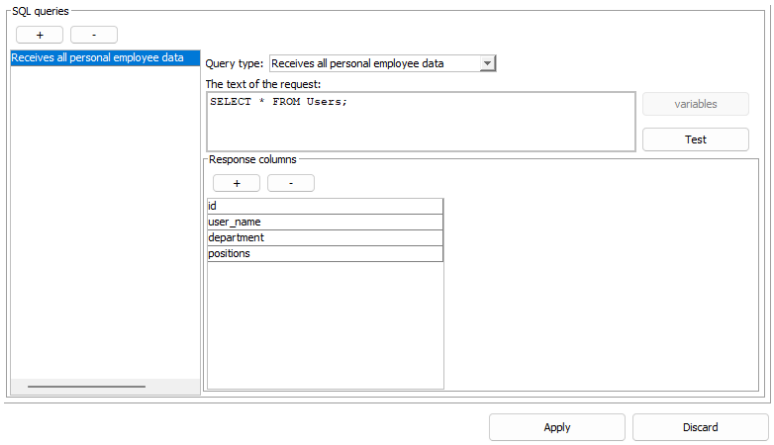
If the connection is successful, create a new query to the external database:

1. Click the "+" button in the "SQL queries" block.
2. For the "Query type" parameter, select "Receives all personal employee data" from the dropdown list.
3. In the "The text of the request" box, type the query that refers to the table containing the cardholder data. For example:

```
SELECT * FROM Users;
```

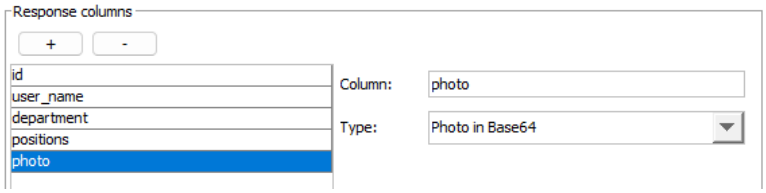
In this example, "Users" is the name of the table in the external database.

4. In the "Response columns" block, click the "+" button.
5. Fill the "Column" text box with the name of the table column containing the unique identifiers of the cardholders and select "ID" from the dropdown list for the "Type" parameter.
6. Similarly, match the table columns containing cardholder name, access code, position, etc. to the parameters in Sigur.



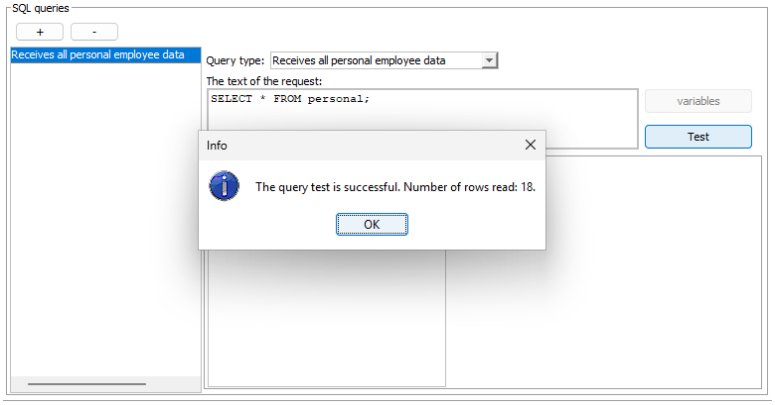
Synchronizing cardholder data.

7. To synchronize cardholder photos, the table in the external database must contain the photo file itself (JPG, PNG, GIF, BMP) in binary code or Base64 representation. Match column name with Sigur's "Photo" or "Photo in base64".



Synchronizing cardholder photos.

8. Click the "Test" button to test the query.



Successful query test.

The presence of a "Receives all personal employee data" type query is mandatory when synchronizing data. It can be the only query you use.

9. Click "Apply" to save the settings.

To check the received data, go to the "Cardholders" tab and, if necessary, update the data by clicking the "Refresh the view" button.

The data is synchronized according to the periodicity set in the "Interval of synchronization" text box and after each reboot of the server module.

24.1.2. Exporting events to an external database

You can also transfer access events to an external SQL database. This information can be used in the external system to create reports or analyze the data collected.

First you need to add and configure a synchronization source following the instructions above.

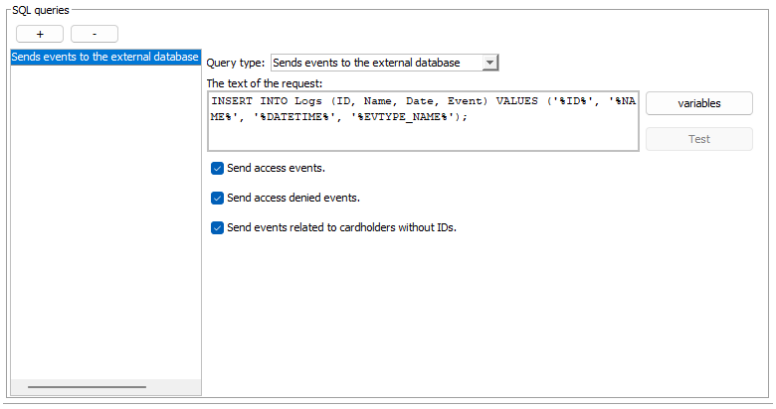
Next, click the "+" button within the "SQL Queries" block and select "Sends events to the external database" from the "Query type" dropdown list.

In the "Text of the request" box, type the query that will insert data into the required table in the external DB. For example:

```
INSERT INTO Logs (ID, Name, Date, Event) VALUES ('%ID%', '%NAME%', '%DATETIME%', '%EVTYPE_NAME%');
```

In this example, "Logs" is the name of the table in the external database and '%ID%', '%NAME%', '%DATETIME%', '%EVTYPE_NAME%' are the variables added. To add variables to the query, click the "variables" button and double-click the required item in the list.

You can use the checkboxes under the "Text of the request" box to specify what information should be sent to the external database. Select the "Send events related to cardholders without IDs" checkbox to send access events of cardholders that have been created directly in Sigur ACS and have no ID in the external database.



"Sends events to the external database" query type.

Events will be sent to the external database as soon as they are registered in Sigur ACS. The prerequisite is that the server module is running and that there is a connection between the Sigur server and the controllers.

24.2. Active Directory data synchronization

In this section we will configure data synchronization from Active Directory via LDAP.

24.2.1. Synchronizing cardholder data

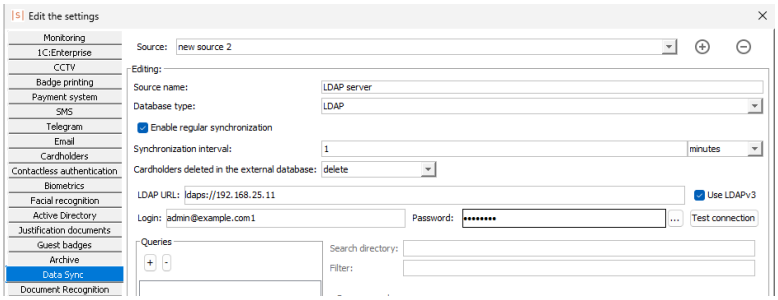
To configure this functionality, start the "Client" tool and go to the "File" –> "Settings" –> "Data sync" menu.

Data synchronization requires a unique identifier (e.g. objectGUID) for each cardholder in the external source.

To create a new synchronization source, proceed as follows:

1. Click the "+" button in the "Source" block.
2. Enter any source name in the "Source name" block and select "LDAP" from the "Database type" dropdown list.
3. Next, select the "Enable regular synchronization" checkbox and enter the desired synchronization interval (the default is 1 minute, but it is recommended that you set a higher value).
4. You can also specify what happens to previously synchronized cardholders when they are deleted in the external system. Cardholders can be deleted in Sigur, or they can be moved to a specific department and their access cards will then expire. By default, the "Cardholders deleted in the external database" parameter is set to "Delete".
5. Next, in the "LDAP URL" field, enter the connection URL to the LDAP server in one of the following formats: "*ldaps://ip-address:port*" or "*ldaps://dns-name*". If no port is specified, the default value is used (389 for "*ldap://*" and 636 for "*ldaps://*").
6. Select the "Use LDAPv3" checkbox.
7. Specify the login and password for authorization on the Active Directory server:

    - Depending on the server, the login can be in the form of a URL (*admin@example.com*) or a DN record (*cn=admin,dc=example,dc=com*).
    - To enter a password, click the "..." button, enter the password twice in the "Password change" window that opens and click "OK".



LDAP server settings.

Next, configure the "Queries" block as follows:

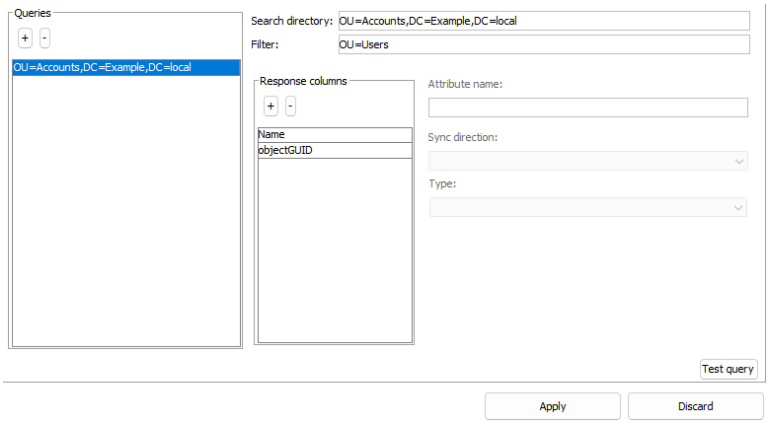
1. Click the "+" button in the "Queries" block and select the line that appears in the list below.
2. In the "Search directory" text box, enter the root directory where the cardholder information is located. The hierarchy and nesting of records from this directory will be transferred to the "Cardholders" tab of the "Client" tool during synchronization.
3. Next, fill in the "Filter" text box. Only records whose attributes match the specified filter criteria will be synchronized to the Sigur database.

   For example, the filter "cn=David N" will transfer only those records from the specified search directory where the "cn" attribute has the value "David N". You can use the filter "*(&(objectCategory=person)(objectClass=user))*" to synchronize all cardholders.

4. In the "Response columns" block, click the "+" button and select the added row in the list below.
5. Type "objectGUID" in the "Attribute Name" field, select "Receives personal employee data" from the "Sync direction" dropdown list, and select "ID" from the "Type" dropdown list.
6. Similarly, add a "cn" attribute name with the type of "Name".

The presence of attributes of type "ID" and "Name" is mandatory for each query that transfers data to the Sigur database.

7. You can also synchronise other attributes. For example, if you need to create a department hierarchy in Sigur that is different from the hierarchy in the main synchronisation directory, add an attribute of type "Department". The attribute should contain the full path to the desired cardholder department in Sigur.
8. Click "Apply" and "OK" to save the settings.



Query example.

To check the data received, go to the "Cardholders" tab and, if necessary, update the data by clicking the "Refresh the view" button.

The data is synchronized according to the periodicity set in the "Synchronization interval" text box and after each reboot of the server module.

24.2.2. Locking Active Directory domain user accounts

The Active Directory integration allows you to block access to Active Directory accounts based on the cardholder's physical location. If the cardholder is in a zone from which Sigur ACS says they cannot access their Active Directory account, they cannot log in. Once the cardholder returns to the "granted" zone, they will be able to log in with their account.

This functionality is available only on Windows and requires no additional licensing.

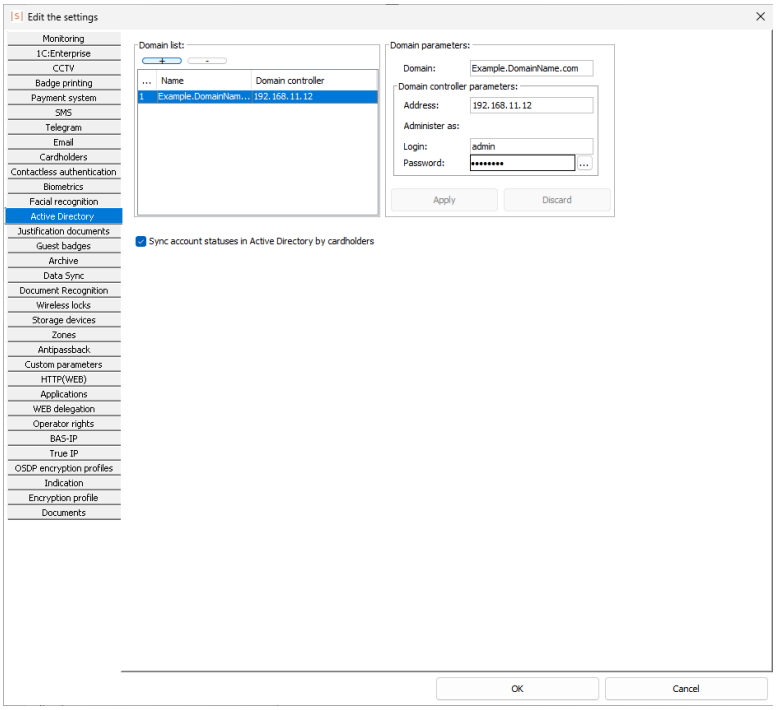
Let's configure the system:

- First, you need to divide the premises into zones.
- Then go to the "File" –> "Settings" –> "Active Directory" menu.
- Click the "+" button in the "Domain list" and enter the Windows domain name in the window that appears.
- Enter the DNS or IP address of the domain controller in the "Address" field. Optionally, specify the port number to connect to. If the port is not specified, the default port (389) will be used.

Examples for completing the "Address" field.

Example	Description
192.168.0.99	IP address.
192.168.0.99:390	IP address and port number.
PO_HOST	DNS.

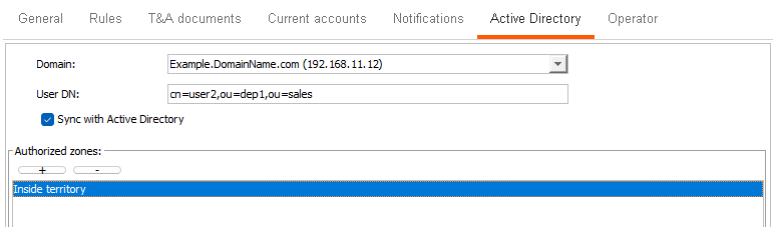
- Next, in the "Administer as" block, specify the login and password of the account that has the right to edit the data of user accounts on the Active Directory server.
- Select the "Sync account statuses in Active Directory by cardholders" checkbox.
- Click "Apply" and "OK" to save the settings.



Domain settings.

Then go to the "Cardholders" tab.

Select the required cardholder and expand the Active Directory subtab within their profile settings. Select the domain from the "Domain" dropdown list. Enter the Distinguished Name (DN) of the cardholder account in the specified domain.



Example of settings.

Next, select the "Sync with Active Directory" checkbox.

Then click the "+" button in the "Authorized zones" and select zones from the list that opens. The cardholder can log in using their domain account when in one of the selected zones.

Click "Apply" to save the settings.

A DN consists of one or more comma-separated Relative Distinguished Names (RDNs). An RDN consists of attribute=value pairs. They are listed in hierarchical order, starting with the account name.

The attributes can be:

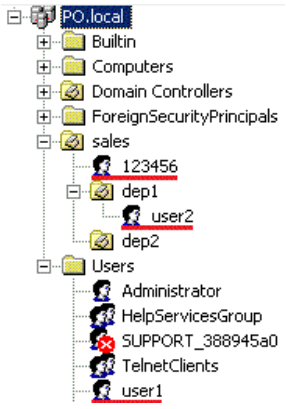
- uid: Account ID.
- cn: Common name.
- sn: Last name.
- l: Location.
- ou: Department.
- o: Organization.
- dc: Domain component.
- st: Region.
- c: Country.

You cannot specify paths to default local accounts or domain admin accounts as DNs. Once such an account is disabled, the ability to work with the domain controller may be permanently blocked.

It is not recommended to set the same account DN for different cardholders as this will cause the system to malfunction.

Below are some examples of DNs for the users shown:

- Account "123456" has DN "cn=123456, ou=sales".
- Account "user2" has DN "cn=user2, ou=dep1, ou=sales".
- Account "user1" has DN "cn=user1, cn=Users".



Sample Active Directory tree.

25. Restricting access by number of successful access attempts

If your license includes the "Paid Access" and "Payment System" software modules, you can provide paid services to cardholders using their access credentials. These modules allow you to create virtual accounts in the system, assign them to cardholders, and debit and credit the accounts with conditional units by system operators or automatically.

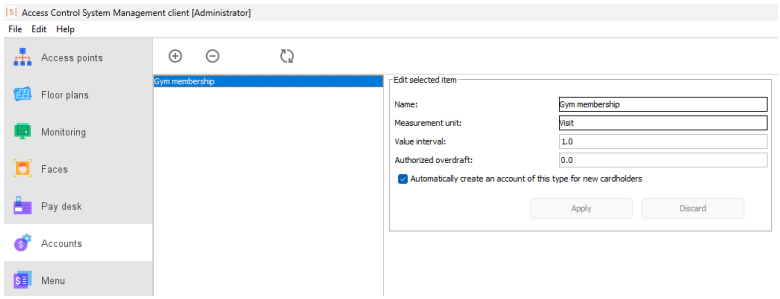
One of the most common uses of these modules is to restrict access to an access point (e.g. when a gym membership is purchased for a certain number of visits to the gym). To configure the system for this logic, you need to:

1. Create a virtual account.
2. Create a "menu" - a list of items on which a cardholder can spend conditional units.
3. Assign the virtual account to the cardholder and load it with conditional units.
4. Create a new rule with paid access rules and assign it to the cardholder and access points.

Creating a virtual account.

Let's start by creating a new virtual account in the system. To do this, go to the "Accounts" tab and click the "+" button on the top toolbar.

Enter any name for the account, for example "Gym membership". Next, enter the measurement unit (e.g. "Visit"). Leave the "Value interval", "Authorized overdraft" and "Automatically create an account of this type for new cardholders" parameters unchanged for now. Click "Apply" to save the settings.



"Accounts" tab.

Creating a "menu".

Next, go to the "Menu" tab and create a new menu by clicking the "+" button on the top toolbar.

In the "Selected menu parameters" block, enter the name "Single visit". For now, let's leave the values of the "Start date", "End date", "Menu users" and "Color"

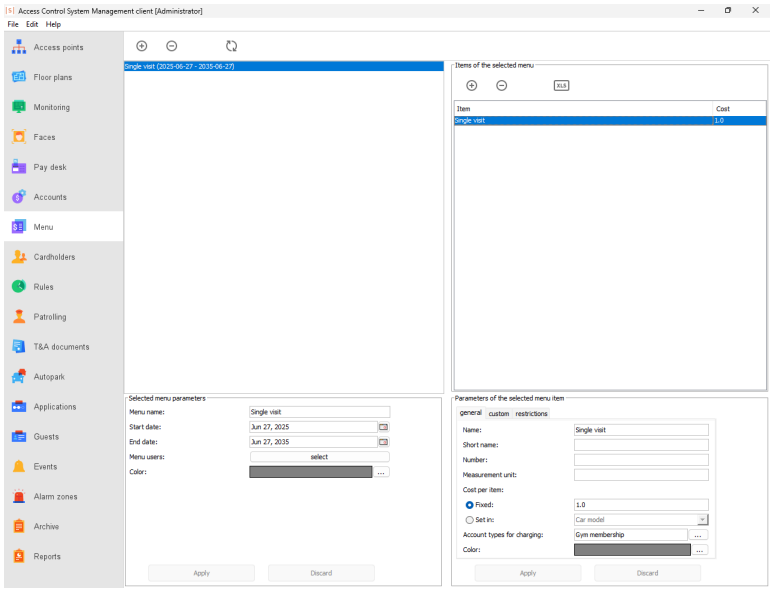
parameters unchanged. Click "Apply".

Click the "+" button in the "Items of the selected menu" block on the right. The "Parameters of the selected menu item" block appears below.

On the "general" tab of the "Parameters of the selected menu item" block, set the values of the "Name" parameter to "Single visit" and the "Cost per item" parameter to "1.0" (fixed).

You will also see that the "Account types for charging" parameter is automatically set to "Gym membership" as this is the only account in the system at the moment. Conditional units for the menu item will automatically be deducted from this virtual account.

Click "Apply" to save your changes.



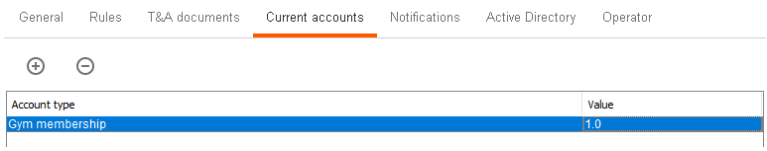
"Menu" tab.

Managing a virtual account.

Next, go to the "Cardholders" tab, select the cardholder and open the "Current accounts" subtab.

Click the "+" button, select the "Gym membership" account in the window that opens, and click "OK". A new account with a value of "0.0" has been added to the cardholder's profile.

Let's assume that this cardholder has purchased a one-time membership. Double-click on the "Value" text box, type "1.0", press "Enter" and click "Apply".



Cardholder payment account.

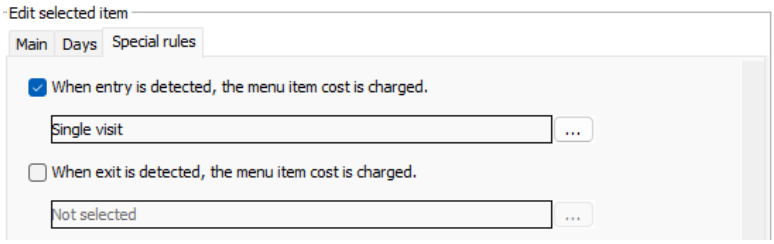
Creating a rule with paid access rules.

Now go to the "Rules" tab and create a new level 2 rule. The procedure for creating rules is described in the corresponding section.

Make sure that the rule is assigned to the cardholder and the access point. Conditional units will be deducted from the virtual account when passing through that access point. Also on the "Days" tab, add at least one day with access intervals for entry and exit.

Go to the "Special rules" subtab of the rule, select the "When entry is detected, the menu item cos is charged" checkbox and click "...". In the window that opens, select the "Single visit" option in the "Menu list" and "Items of the selected menu" blocks and click "OK".

Click "Apply" to save the settings. The system is now configured.

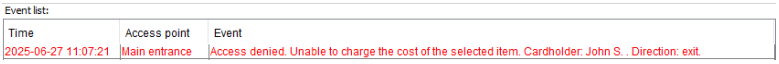


Rule's settings.

Let's go to the "Monitoring" tab and check the operation of the configured access logic.

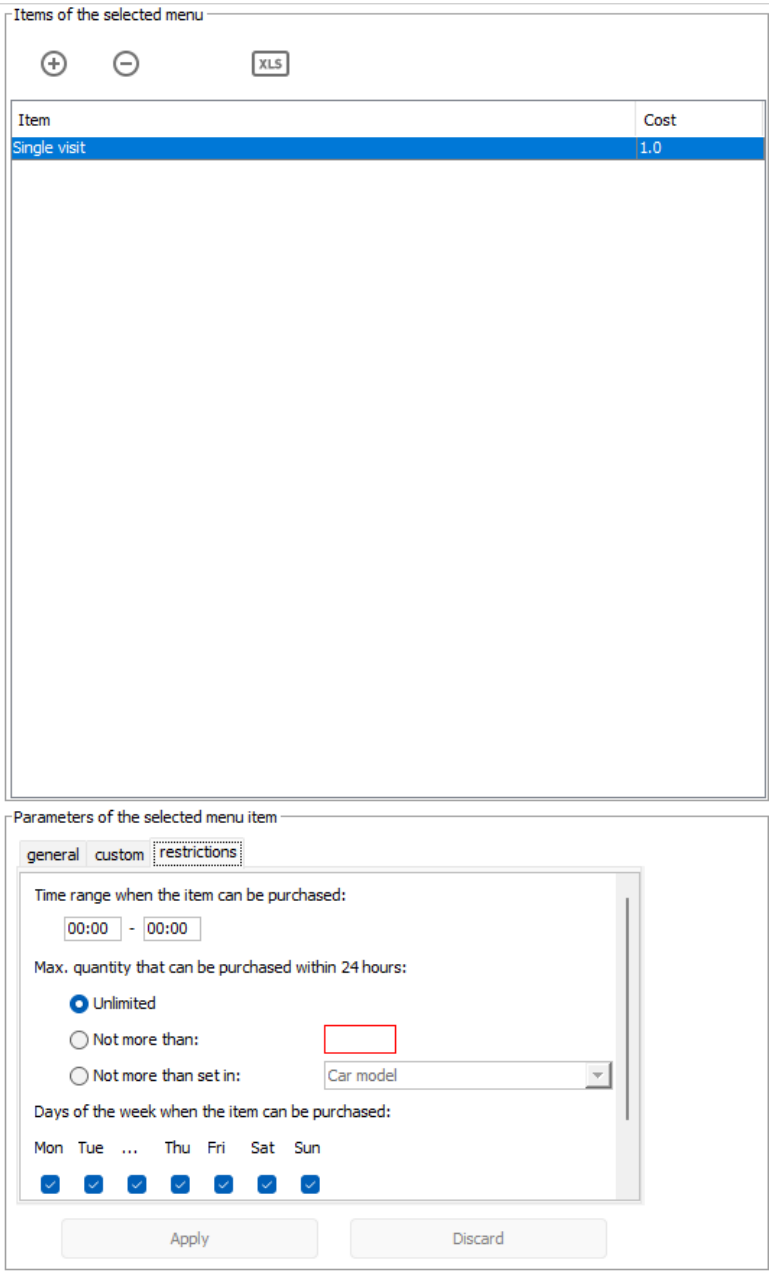
Test the system by presenting the cardholder's card to the wall entry reader. Ensure that the system detects the "Passage" event after the entry sensor has been triggered. You can return to the "Current accounts" subtab in the cardholder profile and check that the value of the "Gym membership" account has decreased by one conditional unit.

If you try to re-enter the access point from the "Inside" direction, the system will register an "Access denied. Unable to charge the cost of the selected item" event.



Event list.

You can also limit the time and days you can withdraw conditional units from your account. Use the "Menu" tab to do this. Select the menu item you created earlier, then edit the "restrictions" subtab under the "Items of the selected menu" block.

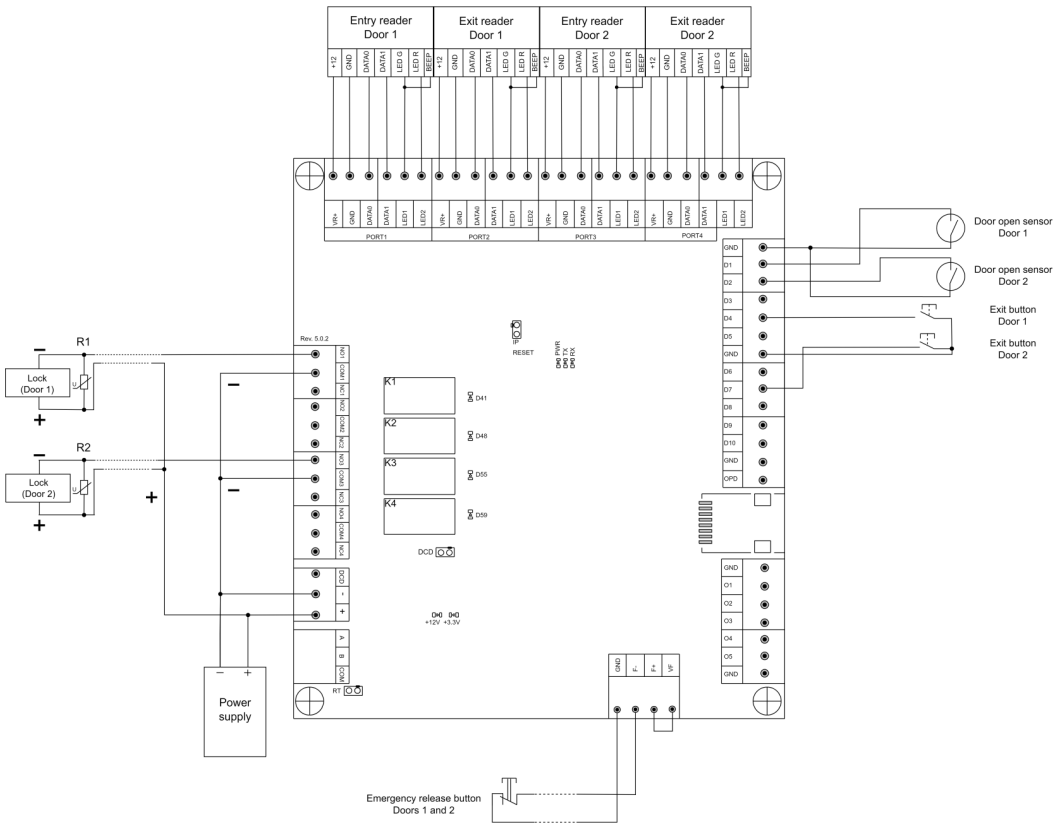


"Restrictions" subtab.

26. Appendix: equipment wiring diagrams

26.1. Connecting doors

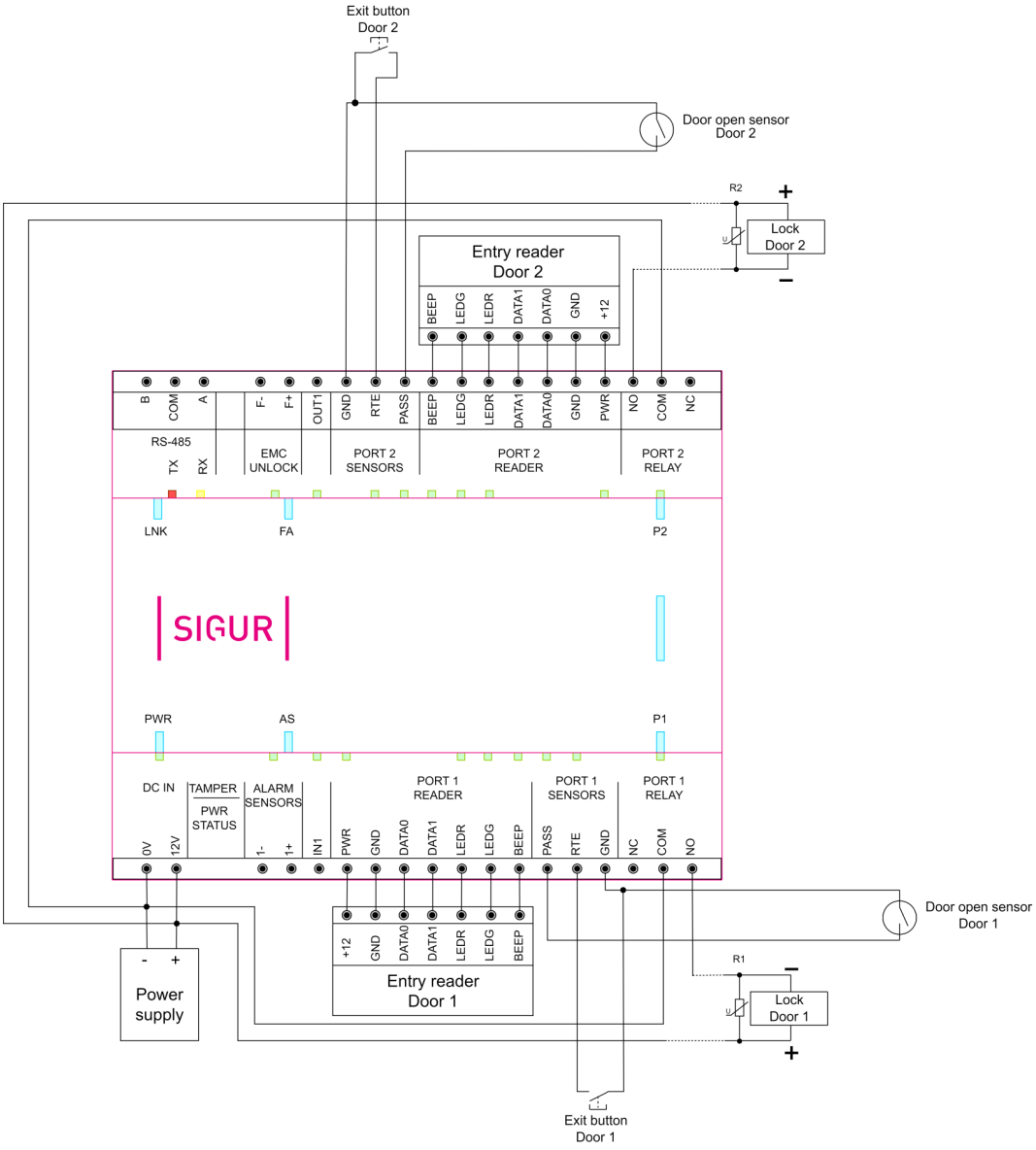
Sigur E510



Connecting two doors with level-controlled locks to Sigur E510.

- R1, R2 - Varistor (B72210S0140K101 or equivalent).

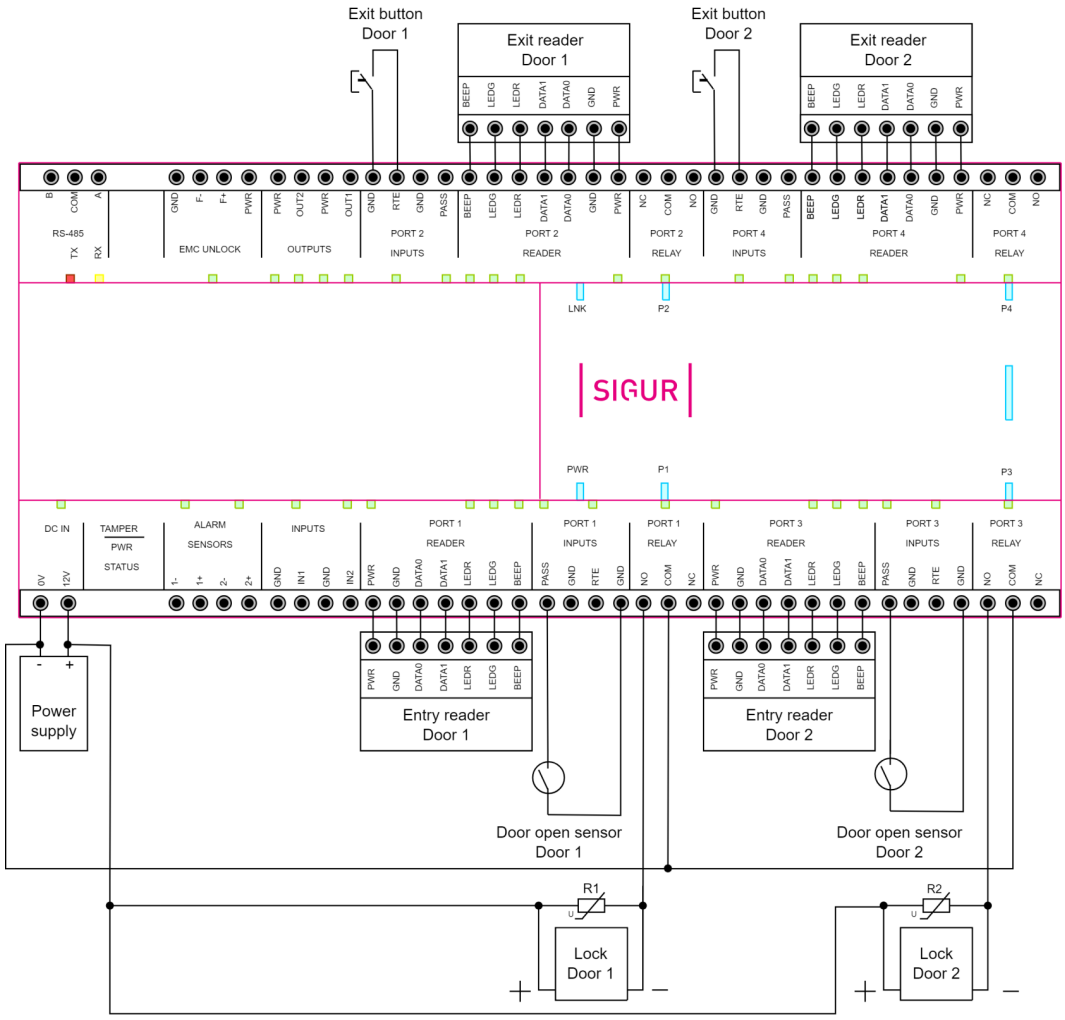
Sigur E2



Connecting two doors with level-controlled locks to Sigur E2.

- R1, R2 - Varistor (B72210S0140K101 or equivalent).

Sigur E4

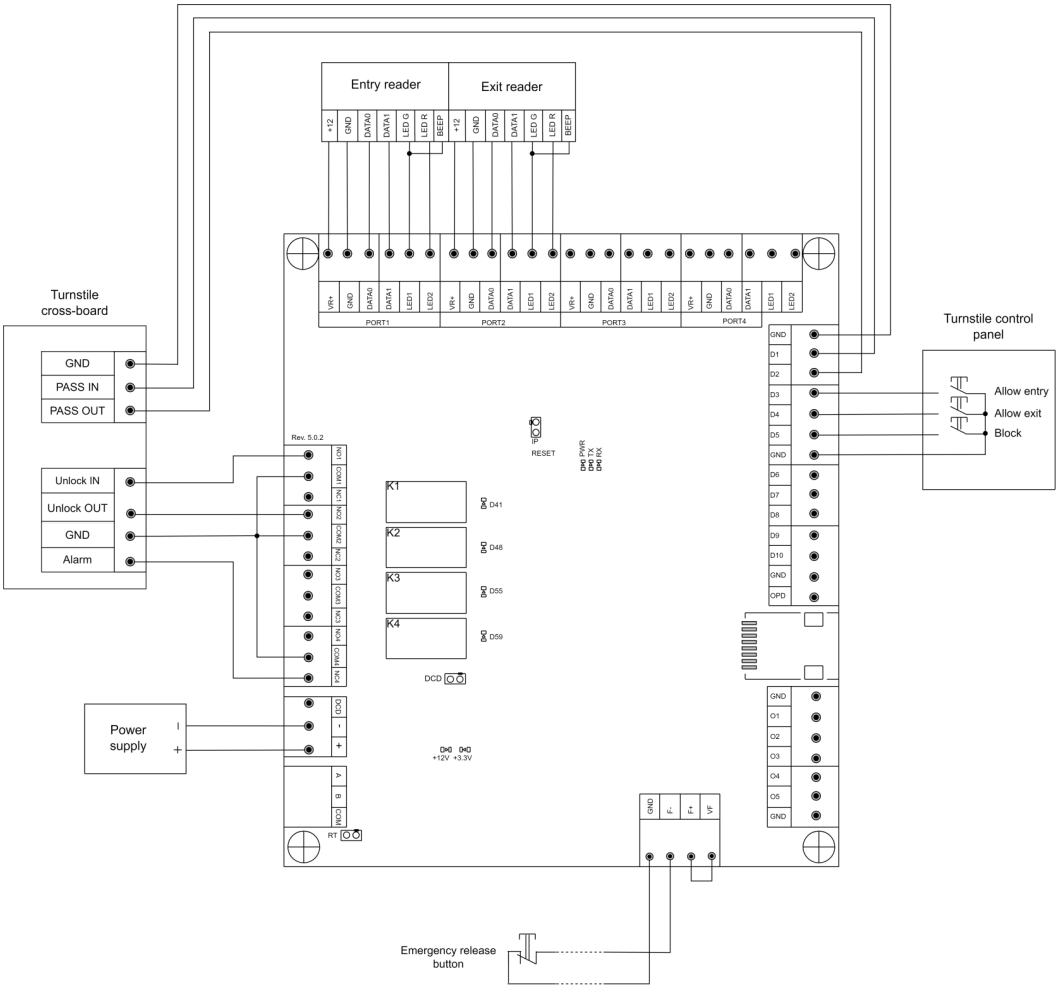


Connecting two doors with level-controlled locks to Sigur E4.

- R1, R2 - Varistor (B72210S0140K101 or equivalent).

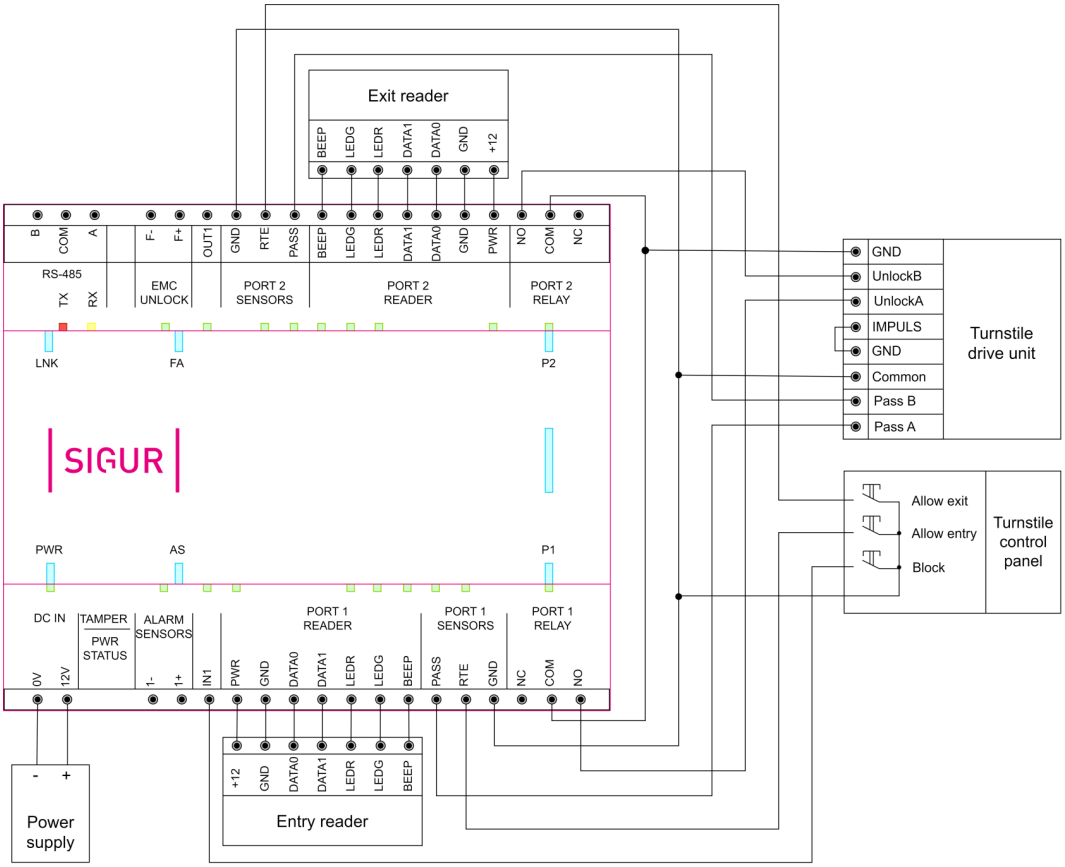
26.2. Connecting turnstiles

Sigur E510



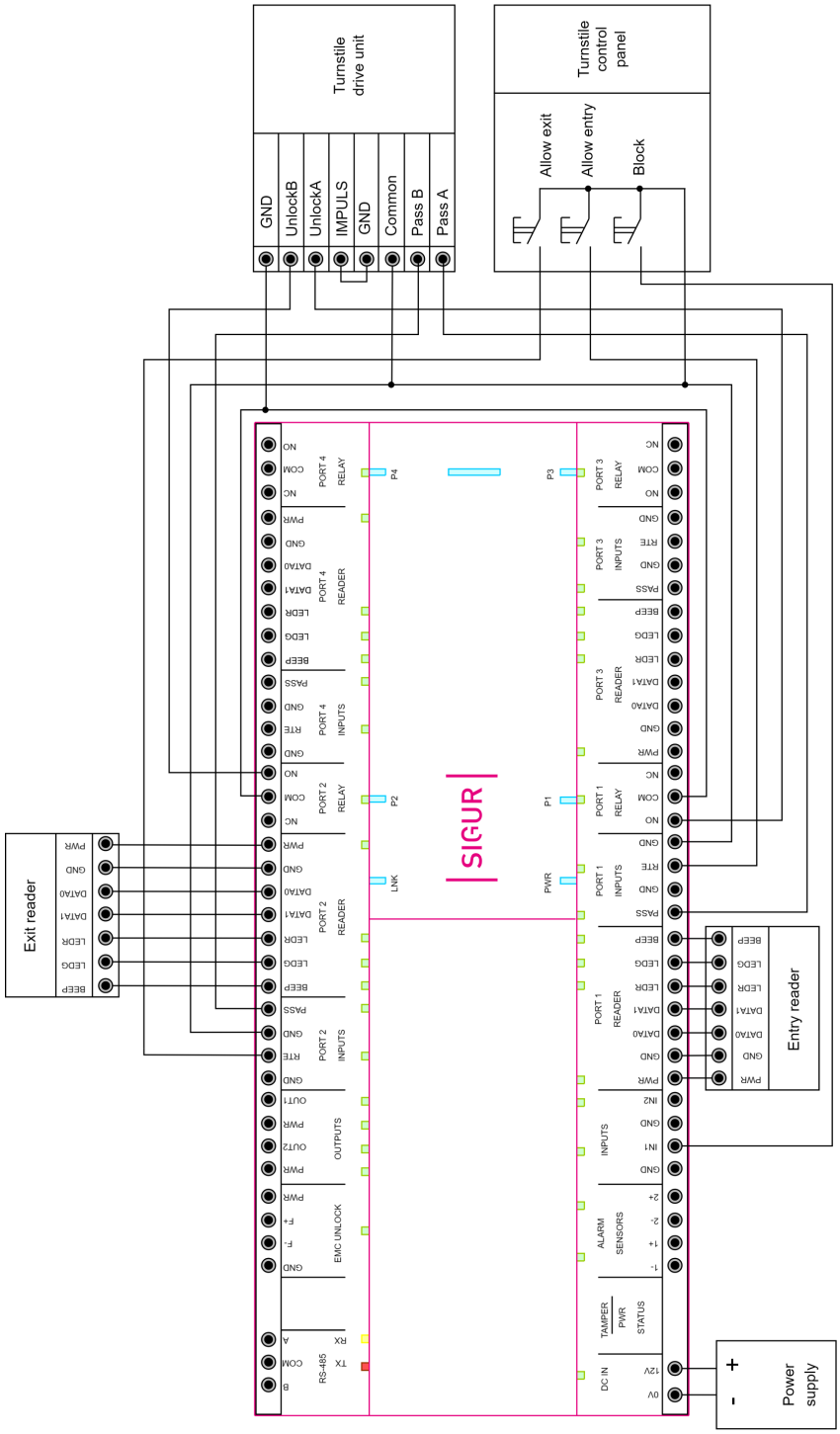
Connecting a level-controlled turnstile to Sigur E510.

Sigur E2



Connecting a level-controlled turnstile to Sigur E2.

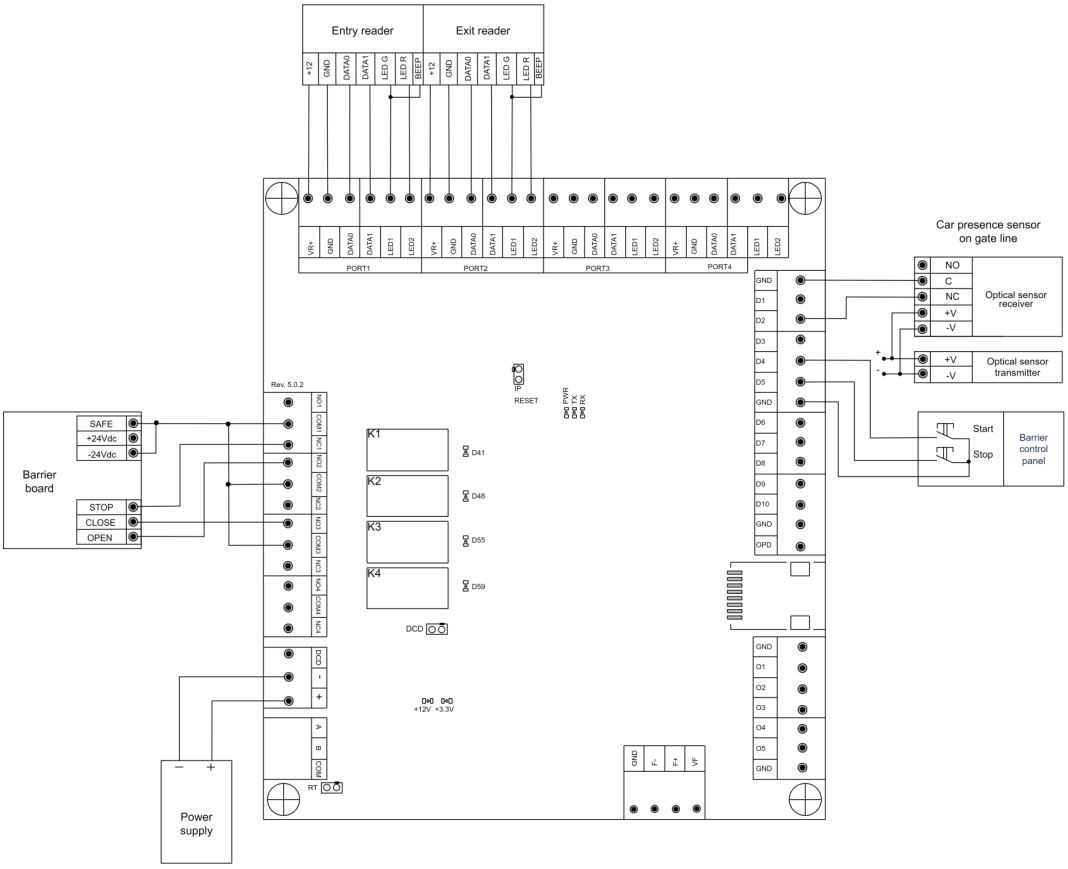
Sigur E4



Connecting a level-controlled turnstile to Sigur E4.

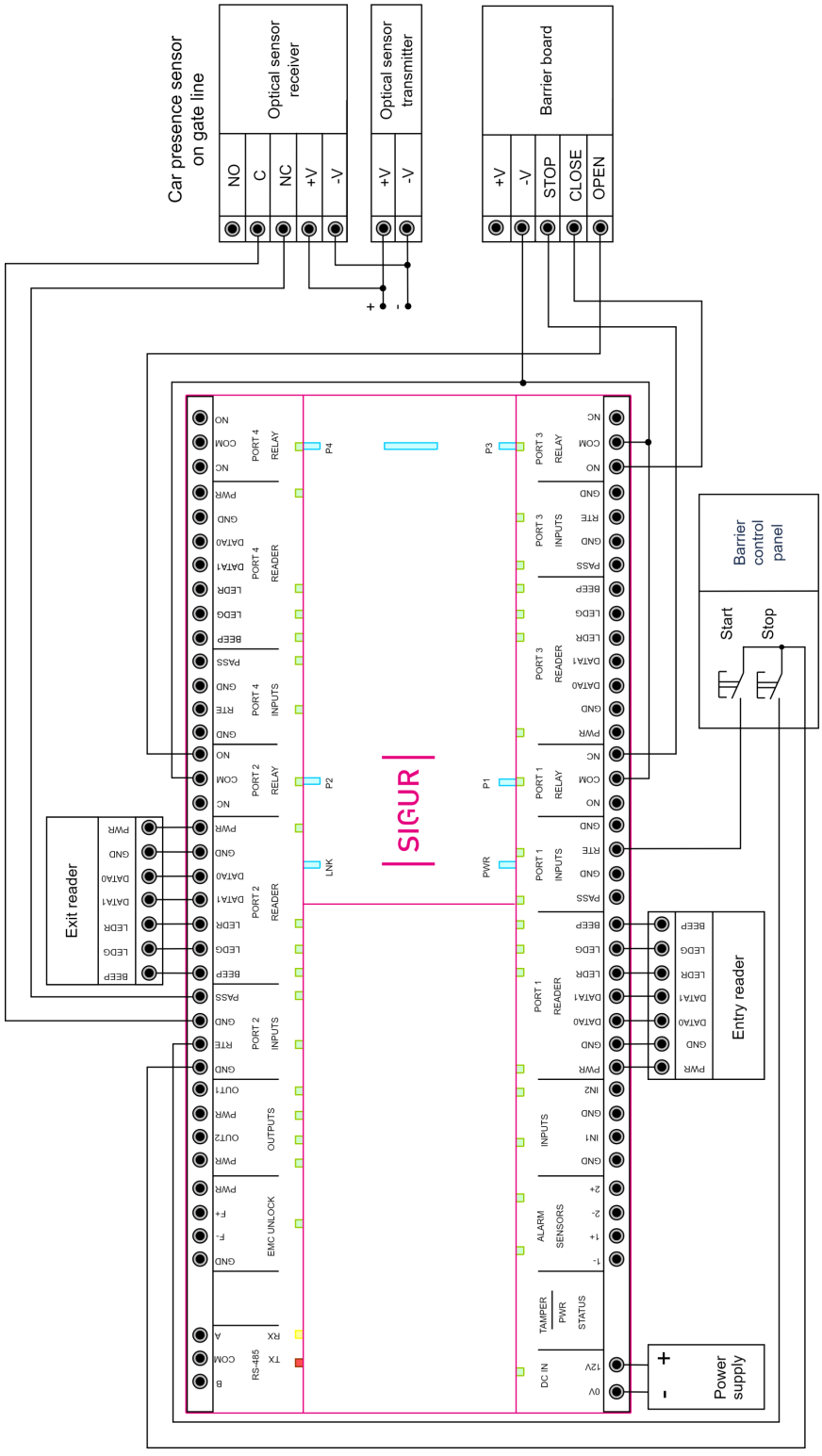
26.3. Connecting barriers/gates

Sigur E510



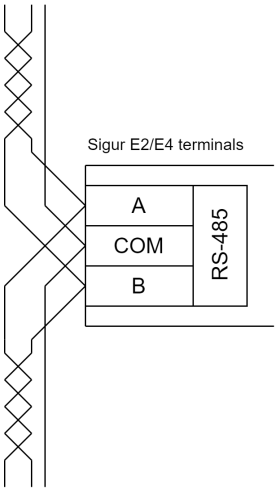
Connecting a barrier to Sigur E510 ("open, close, stop" logic).

Sigur E4

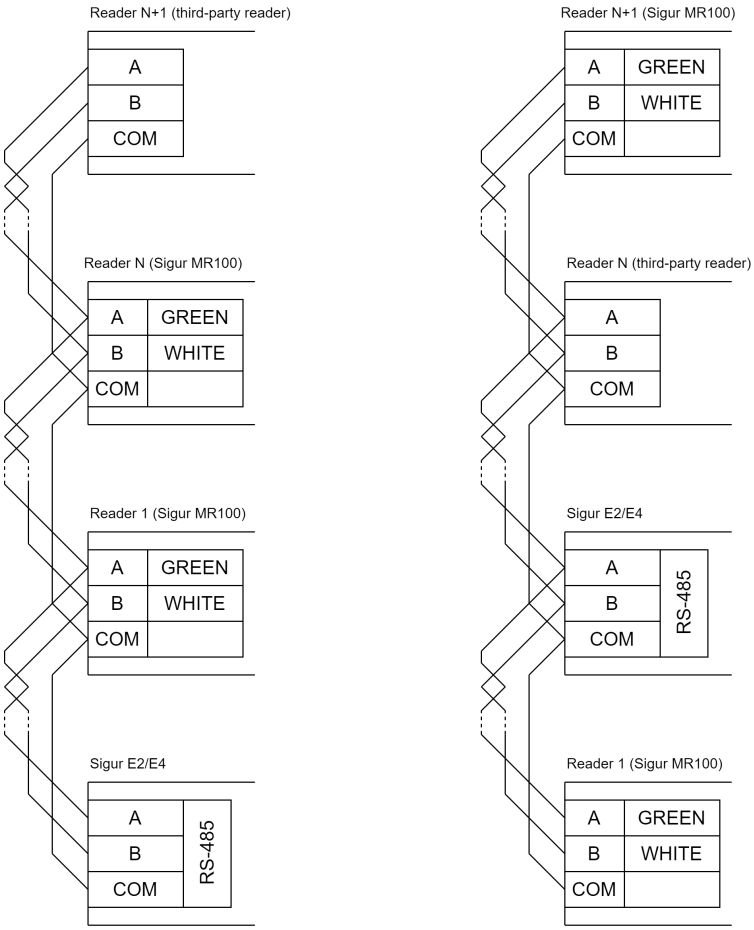


Connecting a barrier to Sigur E4 ("open, close, stop" logic).

26.4. Connecting OSDP readers



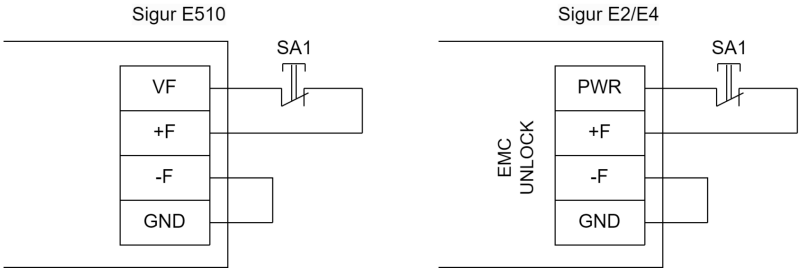
Sigur E2/E4 terminals for connecting OSDP readers.
In this case, the controller is not an end device on the RS-485 loop.



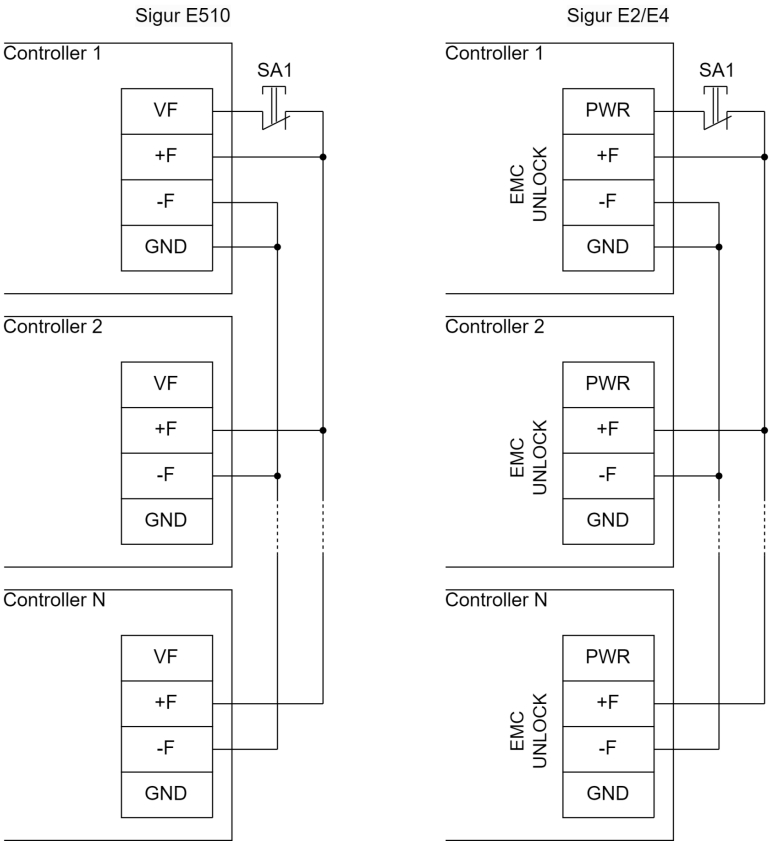
Examples of multiple reader connection via OSDP interface.

26.5. Connecting an emergency release button

The emergency release line is connected to dedicated galvanically isolated hardware inputs of the controller. You can power the line using the controller's VF and GND (PWR and GND) terminals or an alternative power source with an output voltage of 12 to 24 V. During normal operation, the emergency release line should maintain a closed circuit, ensuring a potential difference between terminals F+ and F- in the range of 12 to 24 V.



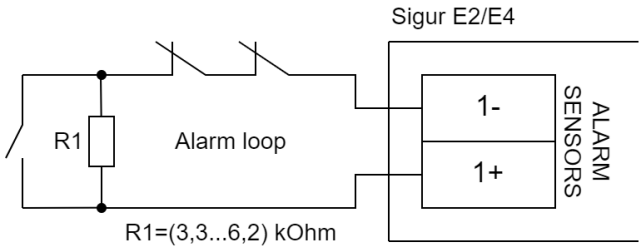
Connecting an emergency release button to a single Sigur E510/E2/E4 controller.



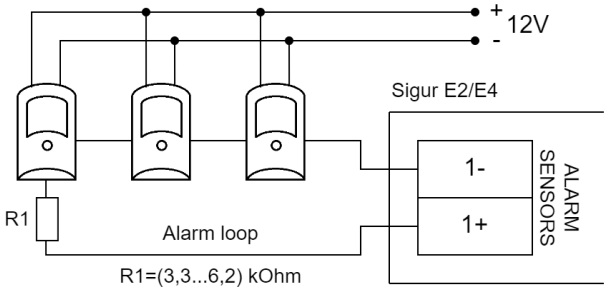
Connecting an emergency release button to multiple Sigur E510/E2/E4 controllers.

- SA1 - Normally closed button.

26.6. Connecting an alarm loop

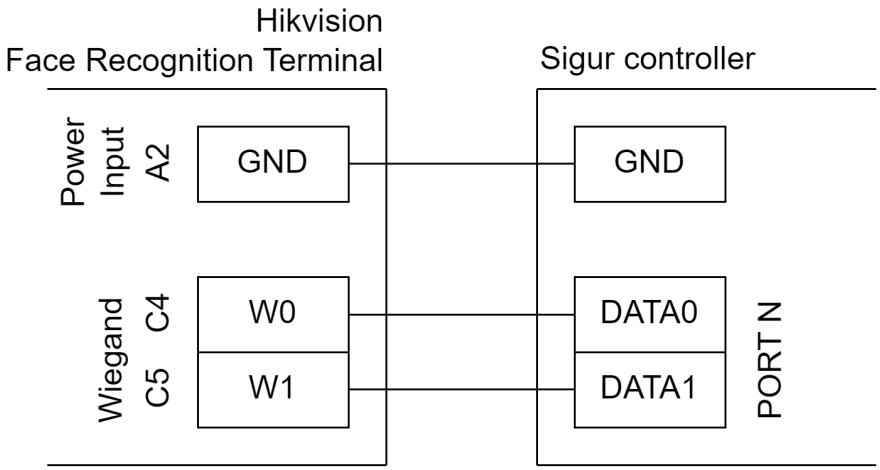


Connecting alarm sensors without external powering.



Connecting alarm sensors that require external powering.

26.7. Connecting a Hikvision face recognition terminal



Connecting a Hikvision face recognition terminal to a Sigur controller.

27. Contacts

For any inquiries or assistance, please contact us using the provided information.

Website: www.sigur.com
General Inquiries: info@sigur.com
Technical Support: support@sigur.com