SIGUR

Guidelines for setting up integration with the Suprema devices

Revision dated 21.11.2025

Оглавление

1. Introduction

This document contains instructions on how to configure interaction between the Sigur access control and management system (ACS) software and Suprema biometric devices.

The Sigur system installation and configuration guide can be found in document: «Sigur Quick Guide».

The manufacturer is responsible for the accuracy of the documentation provided and undertakes to provide an updated version of this documentation in the event of significant modifications to the software.

2. Versions of the document

This document has the following revision history.

Revision	Date of publication	What's changed
0001	June 11, 2025.	First publication.
0002	November 21, 2025.	The information has been updated to reflect the addition of support for the Linux Debian operating system and the ability to connect to the controller via OSDP.

3. Definitions, notations and abbreviations used

ACS	Access control and management system. A hardware and software system designed to perform access control and management functions.
DB	Database.
Access Point	A place where access control is performed. For example: door, turnstile, gate, barrier, equipped with a reader, electromechanical lock and other necessary means.
Access Object	An employee, visitor, car or other vehicle whose actions are governed by access control rules.

4. System requirements

- Sigur software version: 1.6.4.116 and higher.
- Version of Suprema device integration service: 1.2.11 or higher.
- Suprema Device Gateway installer version: 1.7.1.48 or higher.
- ACS server operating system: Windows, Linux Debian.
- ACS database server: MariaDB.
- Other system requirements: see «Sigur Quick Guide».
- Licensing: each Suprema biometric device connected to the ACS (face recognition terminal, fingerprint reader) is licensed.

5. List of supported models

Fingerprint readers:

- BioEntry P2;
- BioEntry W2;
- BioLite N2.

Facial Recognition Terminals:

- BioEntry W3;
- BioStation 3;
- FaceStation 2;
- FaceStation F2.

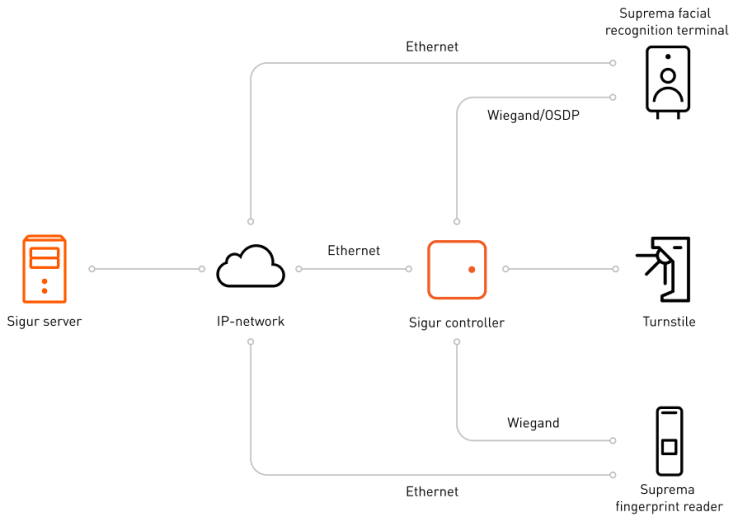
6. Integration description

The configured integration allows you to:

- connect Suprema facial recognition terminals and fingerprint readers to Sigur ACS and link them to access points in a certain direction;
- add and save fingerprint templates to Sigur software using Suprema biometric readers;
- automatically generate credentials (badge numbers) if access is by facial or fingerprint recognition only - without the use of cards;
- synchronize employees, visitors, and identifiers (credentials, card ID, face photos and fingerprint templates) from Sigur ACS to the memory of Suprema biometric devices;
- organize access by face recognition, fingerprint recognition or in two/tree-factor authentication mode: card + face, card + fingerprint, etc.;
- if the person is successfully recognized, receive via Wiegand or OSDP the code of the badge assigned to the employee or visitor to make access decision on the Sigur ACS side.

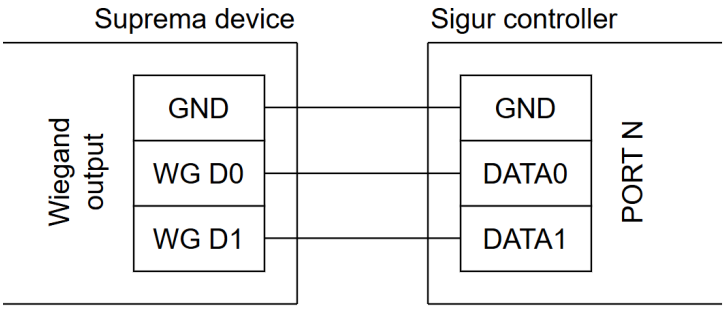
7. Connection and configuration

7.1. The general scheme of device connection

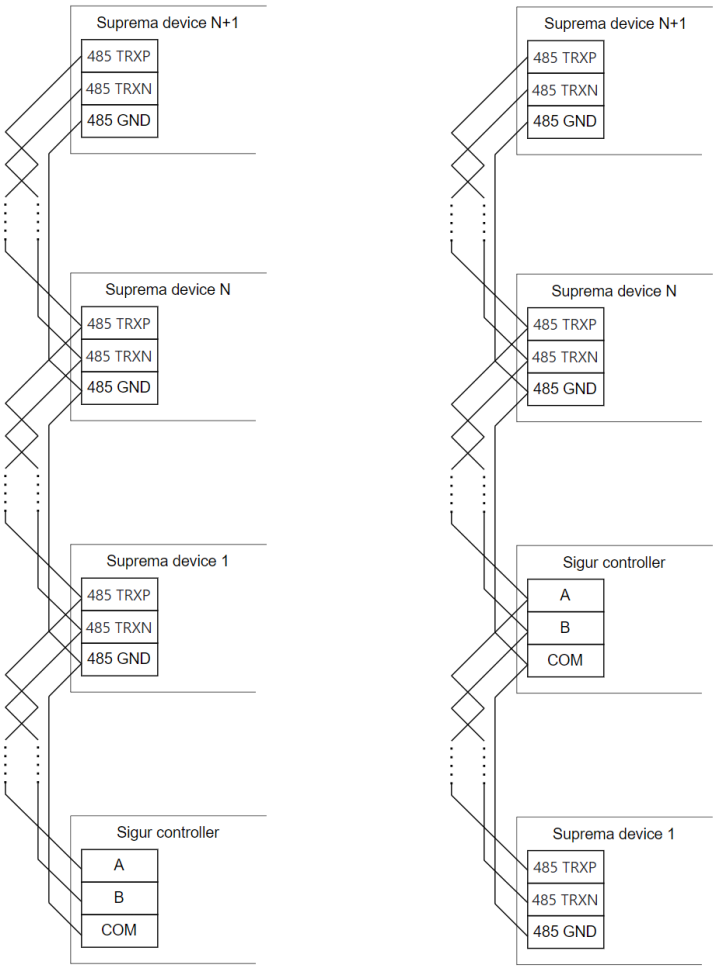


General scheme for connecting Suprema devices to the ACS Sigur.

7.2. Connecting devices to the controller



Connection diagram of Suprema devices to the Sigur controller via the Wiegand interface.



Connection diagram of Suprema devices to the Sigur controller via the OSDP interface.

7.3. Settings by Suprema

7.3.1. BioStar 2

BioStar 2 software is used to configure Suprema devices. The distribution (available for Windows only) can be downloaded after registration in the Suprema Download Center via this link.

After installing the program, launch the «BioStar 2 Setting» utility via the Start menu - «BioStar 2» - «BioStar 2 Setting». Make sure that BioStar 2 services are in Running status (except for «Video License» module). If necessary, click the Start button to start them.

BioStar Services 2.

If integration is already configured, stop the «Suprema Device Gateway service» before starting «BioStar 2».

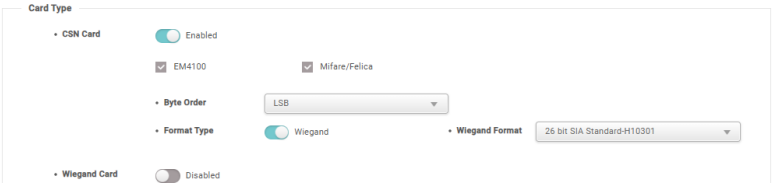
Next, you need to enter the BioStar 2 web interface. To do this, enter the address https://127.0.0.1:443 into the address bar of your browser, where:

- 127.0.0.1 - IP address of the computer where «BioStar 2» is installed;
- 443 - default port (can be changed in «BioStar 2» settings).

For authorization, the admin username and the administrator password set during «BioStar 2» installation are used.

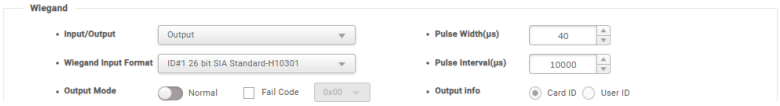
In the web interface, click the «Device» tab, search for and add a Suprema device. Click on the device to proceed to configuration. The following steps must be performed:

- in the «Authentication - Card Type» block set the order of card reading;



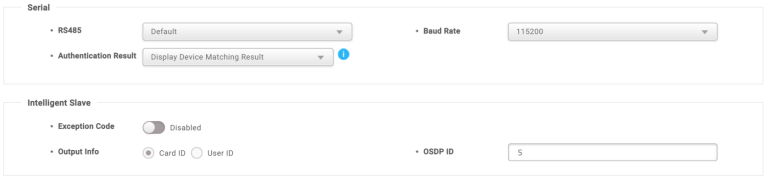
Card Reading Settings.

- if the device is connected to the Sigur controller via the Wiegand interface, configure the device's Wiegand output in the «Advanced - Wiegand» block;



Wiegand output settings.

- if the device is connected to the Sigur controller via the OSDP interface, set the RS485 parameter to Default in the «Network - Serial» block. Then, configure the Baud Rate and the device address (OSDP ID).



OSDP interface settings.

  Note that the Baud Rate and device address must also be specified in the controller settings. For this, refer to the «Sigur settings» section;
- save the settings by clicking the Apply button at the bottom of the page.

To establish a connection between the Sigur server and the Suprema device, you need to know its IP address and port. Network settings can be configured directly via the biometric device interface or via the BioStar 2 web interface under «Device» - «Network» (e.g. for models without display).

The method of identity verification (card, card and face, fingerprint, etc.) can be changed via the terminal interface or in the BioStar 2 web interface under «Device» - «Authentication».

When you finish configuring the devices, you must stop the BioStar 2 services for the integration to work correctly. If you have previously stopped the Suprema Device Gateway service, start it.

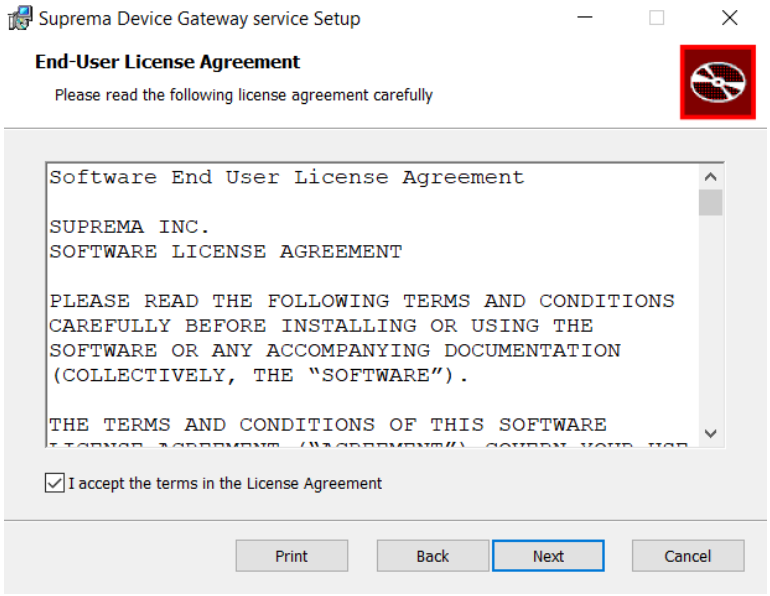
7.3.2. Suprema Device Gateway

Suprema Device Gateway installation

The Suprema Device Gateway component is required to connect and work with Suprema biometric devices. It can be installed and run either on the Sigur ACS server or on another computer running Windows or Linux Debian.

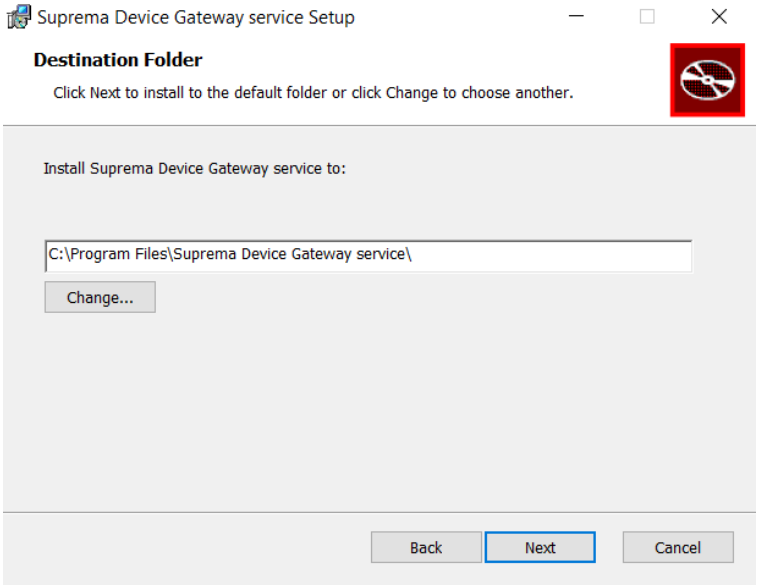
The following must be accomplished:

1. Download and run the installation file (for Windows or Linux Debian).
2. Follow the installation steps. At one stage, you will need to review and accept the Suprema End User License Agreement (EULA).



License Agreement.

3. For Windows, at the «Destination Folder» step, you can optionally specify an installation directory different from the default («C:\Program Files\Suprema Device Gateway service\»). After confirming the installation, the system will request administrative privileges. Approve the request to proceed.



Selecting a folder for installing the program.

4. During the first installation, the system will prompt you to generate user certificates. A root certificate must be created first, followed by a server certificate. The installation will be aborted if this step is skipped.

   - On the command line, values for each certificate attribute must be entered. It is allowed to use the same information for both certificates.

- At the step asking «More IPv4 address?», specify all external IP addresses or domain names that will be used to connect to the Suprema Device Gateway. If the installation is performed on the ACS server, specify the address 127.0.0.1. Example:

```
>>> More IPv4 address? [y/N]: y
>>> IPv4 Address (eg, 8.8.8.8) []: 127.0.0.1
```

5. After this, the installation will be completed.

After the installation, the «Suprema Device Gateway» service will be registered and started automatically (or «suprema-device-gateway.service» on Linux).

On Windows, the created certificates are saved in the cert directory (by default: C:\Program Files\Suprema Device Gateway service\cert). To configure the integration, a CA certificate is required. If necessary, it can be copied to the computer where the ACS server is running.

On Linux, the certificates are located in the /opt/suprema-device-gateway/cert directory.

Suprema Device Gateway update

The update is performed on top of the existing installation. Download the latest installation file, run it, and follow the installer instructions to complete all steps of the upgrade process. After the update is finished, the «Suprema Device Gateway» service will start automatically.

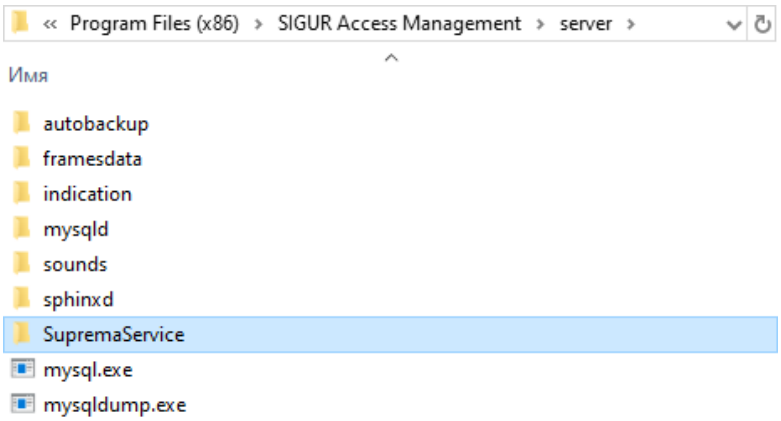
7.4. Sigur settings

The following must be accomplished:

- Verify that the Sigur software version is up to date. If the Sigur software version is lower than the one listed in the «System requirements» section, upgrade the software.
- Download the Suprema integration service (Windows version or Linux Debian version).

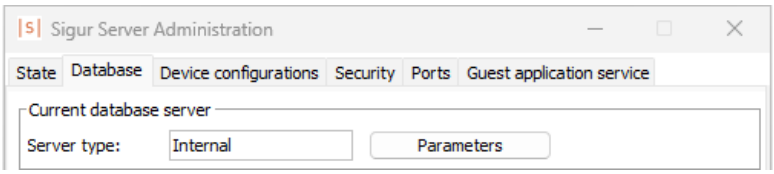
For a Sigur server installed on Windows:

1. Extract the downloaded archive to the server directory contained in the Sigur software installation folder (e.g. C:\Program Files (x86)\SIGUR access management\server). The SupremaService folder should appear in the server directory.



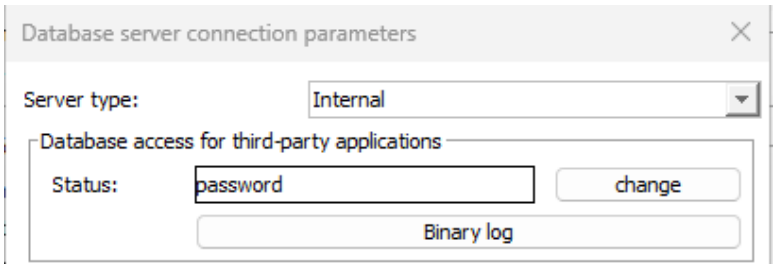
\SIGUR access management\server directory.

2. In the «Server Administration» program, go to the«Database» tab and in the «Current database server» block click the «Parameters» button.

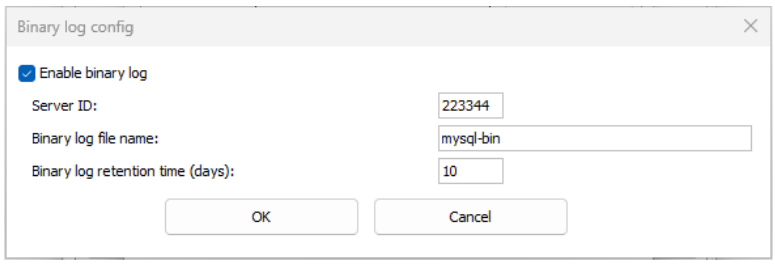


«Database» tab of the «Server Administration» program.

3. In the opened window click the «Binary Log» button, then enable the binary log, leaving the proposed default values of parameters. Save the settings by clicking «OK».



The «Database server connection parameters» window.



«Binary Log Settings» window.

4. Restart the server module and database server using the «Stop»/«Start» buttons on the «Status» tab of the «Server Administration» software.

To successfully start the integration, make sure that
BioStar 2 services are stopped

For a Sigur server installed on Linux Debian:

1. Install the downloaded integration service package.
2. Restart the server module, for example, using the «Server Administration» utility.
3. Enable the binary log for the database server.
   To do this, in the database server configuration file (e.g., /etc/mysql/mariadb.conf.d/50-server.cnf), under the [mysqld] section, set the following values:

```
server-id = 1
log_bin = mysql-bin
binlog_format = ROW
binlog_row_image = FULL
expire_logs_days = 10
```

4. After that, restart the database server with the command:

```
sudo systemctl restart mariadb
```

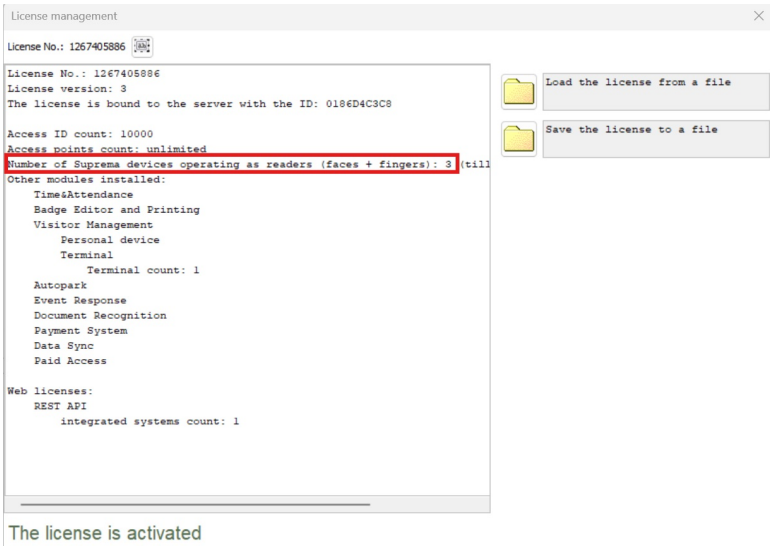
5. The Linux database user requires additional privileges to execute commands when working with the database: RELOAD, SHOW DATABASES, REPLICATION SLAVE, REPLICATION CLIENT. These can be granted with the following command:

```
GRANT RELOAD, SHOW DATABASES, REPLICATION SLAVE, REPLICATION CLIENT ON *.* TO 'user'@'%'
```

Settings in the Client software.

The following is required:

1. Check that the license for the required number of Suprema devices is present via the «File» - «Module Management» dialog in the Client software.

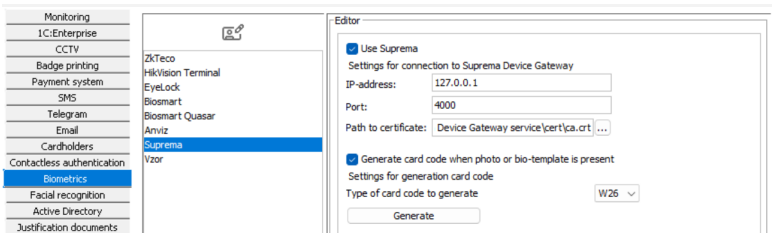


License to connect Suprema devices.

If a terminal license is missing, expired, or purchased for fewer terminals than the number of terminals added to the system, a message will subsequently be displayed indicating that the license limits have been exceeded.

2. Enable integration with Suprema. To do this:

   - Go to the software menu «Client»: «File» - «Settings» - «Biometrics» - «Suprema».
   - Enable the «Use Suprema» option.
   - Ibid:
     - IP address of the computer on which Suprema Device Gateway is running;
     - port (default is 4000);
     - path to the Suprema Device Gateway root certificate (by default C:\Program Files\Suprema Device Gateway service\cert\ca.crt).
   - Save the settings by clicking the »«Apply» and «OK» buttons.



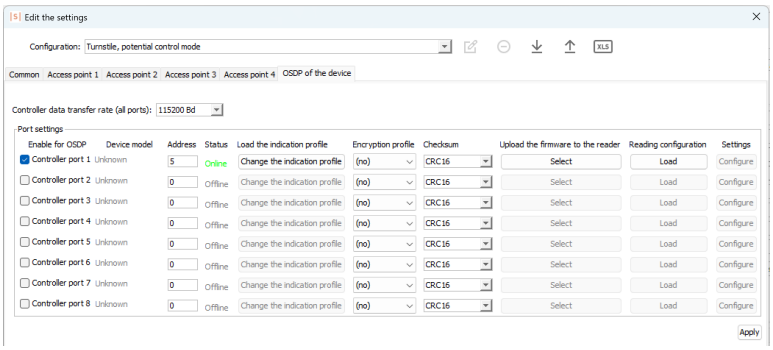
«File» - «Settings» - «Biometrics» - «Suprema» menu.

The function of pass code generation is discussed below in the «Personnel synchronization» block.

3. Next, configure the device connection to the controller via Wiegand or OSDP.

   For Wiegand: On the «Access point» tab, click the «Settings» button. In the opened window, for the parameter «Entrance reader port» (or «Exit reader port», depending on the location of the biometric device), select from the dropdown list the number of the physical Wiegand port of the controller to which the Suprema device is connected. Save the settings by clicking «OK».

   For OSDP: On the «Access point» tab, click the «Settings» button. In the opened window, go to the «OSDP Devices» tab, where the communication speed between the controller and the connected readers is configured, as well as the parameters for connecting biometric devices to the controller's logical ports. First, select the same Baud Rate that was set when configuring the device in «BioStar2 Setting» (for more details, see the «BioStar 2» section).



Example of configuring OSDP devices.

In the «Enable for OSDP» column, select the logical ports of the controller that will be used with devices via the OSDP interface.

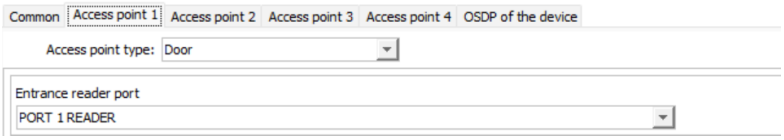
> When a specific port is «enabled» on the «OSDP Devices» tab, the physical Wiegand port of the controller with the same number is automatically «deactivated».

After selecting the port, you must specify the device address on the bus (range: 1 to 127). This parameter is set in the device settings via «BioStar 2 Setting».

After clicking the «Apply» button, you can verify the correctness of the settings and connection by monitoring the «Status» field. If everything is configured correctly, the message «Connected» will appear.

Once the OSDP device is configured, go to the «Access Point N» tab in the same window and define the device function for the corresponding logical reader port. The screenshot below shows an example of the configuration for a device connected to the first logical port of the controller, functioning as an

entry reader.



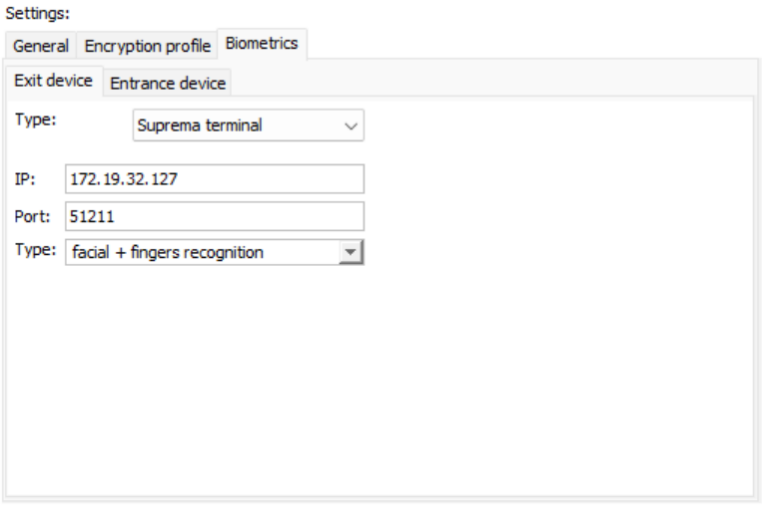
Example of configuring a controller port.

Save the settings by clicking «Apply».

- Open the «Biometrics» sub-tab and select the direction of connection of the biometric device (entrance or exit). In the «Type» drop-down list select «Suprema terminal» and then specify:

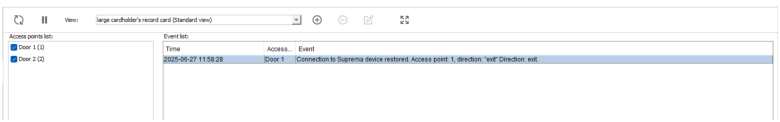
  - the IP-address of the device;
  - port (default is 51211, can be changed in the device interface or via BioStar 2 software);
  - device operation type - «faces+fingers» (default).

  Save the settings by pressing «Apply».



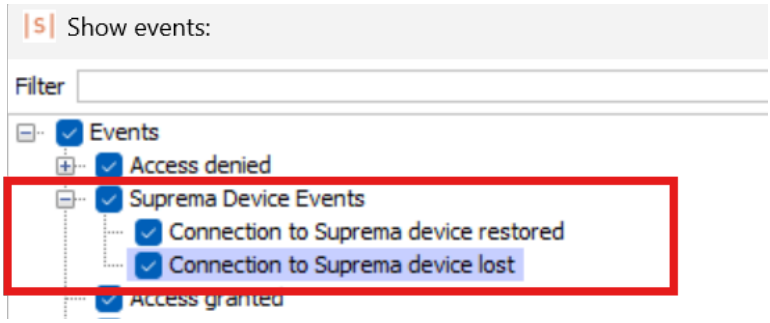
Example of access point settings on the «Biometrics» sub-tab.

If the settings are correct, the event «Communication with Suprema device restored» will appear in the event archive and on the «Monitoring» tab of the Client software.



Successful establishment of communication with the Suprema device.

When building reports and archived uploads, you can customize the display of recovery and loss of connection events with Suprema devices using appropriate filters.



Suprema device event filters.

Staff Synchronization

In order to synchronize data to the device memory, it is required to grant personnel access to the access points to which Suprema equipment is bound. Access objects of the «Employee» type and issued guest credentials are synchronized.

Additionally, required:

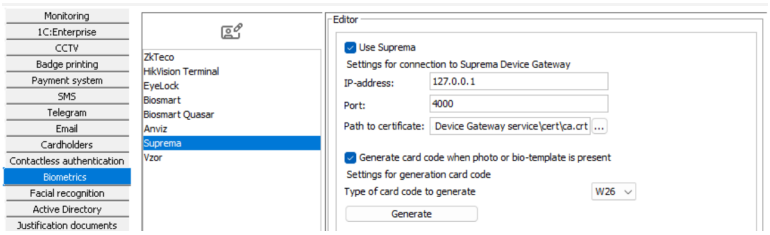
- For access by fingerprint recognition - assign a biometric fingerprint template and credential in Wiegand-26 format. You can add a biometric template by capturing it from an IP device, selecting «Suprema terminal» from the «Biometrics» drop-down list in the cardholder badge on the «Cardholder» tab.

- For access by face recognition - assign a photo and credential in Wiegand-26 format to cardholder. When synchronizing visitors, the presence of the guest's photo in the «Visitors» tab is taken into account.

The synchronization of cardholders and badges takes into account their expiration dates: if the credential or badge has expired, the credential or badge will not be synchronized.

If the cardholder does not have a physical card, you can manually assign any arbitrary number in the specified format or use the credential (card code) generation function. To do this, you need to:

1. Go to the software menu «Client» - «File» - «Settings» - «Biometrics» - «Suprema».
2. Enable the corresponding option. At the moment, the credential generation is available only in Wiegand-26 format.
3. Save the changes with the «Apply» and «OK» buttons.

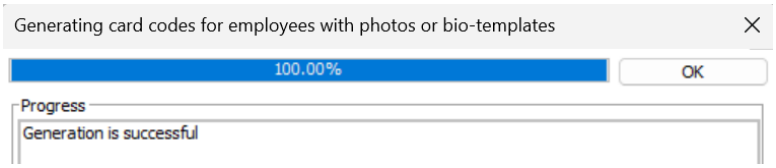


«File» - «Settings» - «Biometrics» - «Suprema» menu.

If this option is enabled, badges will be automatically generated with each subsequent addition of a photo or Suprema biometric fingerprint template. The exception is if the cardholder already has a Wiegand-26 credential or has 5 credentials assigned to it. For guest passes, generation is performed by adding a fingerprint template on the «Cardholders» tab or a photo on the «Visitors» tab.

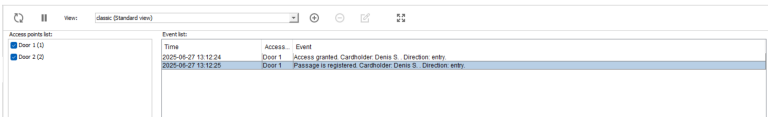
If the database already contains previously added cardholders without skips, generation for them should be started manually:

1. In the same menu, click the «Generate» button.
2. In the window that opens, select the cardholders on the left side, move them to the right side using the >> button and click «OK».
3. The system will display a message about the result of the operation. The credential will be generated only for those cardholders who have a photo or Suprema biometric fingerprint template (unless the cardholder already has a Wiegand-26 badge or 5 card numbers assigned).



The result of card code (credential) generation.

Upon successful ID recognition, the biometric device sends to the Sigur controller a pass code in Wiegand-26 format. The access decision is made on the ACS side according to the configured rules.



Display events on the «Monitoring» tab upon successful identification.

8. 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