ACFA Intellect

Sigur integration module configuration and operation manual

Last update 10/04/2020

Table of contents

1 List of terms used in Sigur integration module configuration and operation manual

Access – movement of people, means of transport and other objects into (out of) premises, buildings, zones and territories.

Executive devices – turnstiles, gates, barriers or doors equipped with electromagnetic or electromechanical locks. Controller manages executive devices and gets information about their state.

Client – computer connected to *Sigur* server over TCP/IP protocol. *Intellect* Server is the *Sigur* server's Client.

Sigur client – computer with installed *Sigur ACS* software, connected to *Sigur* server over TCP/IP protocol.

Controller – an electronic device that is LSI microprocessor board in the metal case. It is connected to RS485 or Ethernet, readers, sensors and executive devices.

Sigur server - computer with installed *Sigur ACS* server software.

Access control system (ACS) – hardware-software system performing the access control functions.

Readers – electronic devices for entering human-memorable PINs with the keypad or for reading PINs from the system's security tokens.

Access point – a point where access control is performed. An access point may be a door, a turnstile, a gate or a barrier equipped with a reader, an electromechanical lock or other access control devices.

2 Introduction into Sigur integration module configuration and operation manual

On the page:

2.1 Purpose of the Document

Configuration and operation manual for Sigur integration module is a reference and information guide meant for *Sigur* configuration specialists and operators. This module is a part of *ACFA Intellect* software package.

The guide provides:

1. general information about *Sigur* module;
2. information about how to configure *Sigur* module;
3. information about how to use *Sigur* module.

2.2 General information about Sigur integration module

Sigur integration module is the *ACFA Intellect* component. It performs the following functions:

1. Configuring *Sigur* ACS (manufactured by PromAvtomatika , LLC);
2. Ensuring interaction between *Sigur* ACS and *ACFA Intellect* (monitoring, control).

Note.

For more information about *Sigur* ACS, please refer to official documentation for this system.

Before configuring *Sigur* integration module, do the following:

1. Install *Sigur* ACS hardware on the object under security surveillance;
2. Configure access points of *Sigur* ACS using the *Sigur* Client (see reference documentation about *Sigur* ACS).

3 Supported hardware and licensing of the Sigur integration module

Manufacturer	«PromAvtomatika Service» 603001, Nizhniy Novgorod, Chernigovskaya street, 17-A, 5th floor.
Integration type	SOFT-SOFT
Equipment connection	RS-485, Ethernet

Supported equipment

Equipment	Function	Features
E100	Access controller	• Unlimited number of users • Event log capacity: 2 • Ethernet interface • Readers interface: 2 embedded readres with EM Marine or Mifare support
E300H	Access controller	• Max. number of users: 50 • Time zones: 500 • Event log capacity: 40000 • Ethernet interface • Readers interface: Wiegand-26, Wiegand-34, Wiegand-4/6/8 (for keyboards), Dallas Touch Memory

R500D4/E500D4	Access controller	• Max. number of users: 7000
		• Time zones: 500
		• Event log capacity: 40000
		• Communication interface:
		  ◦ R500D4 RS-485
		  ◦ E500D4 Ethernet
		• Readers interface: Wiegand-26, Wiegand-34, Wiegand-4/6/8 (for keyboards), Dallas Touch Memory

R500/E500	Access controller	• Max. number of users: 7000
		• Time zones: 500
		• Event log capacity: 40000
		• Communication interface:
		  ◦ R500D RS-485
		  ◦ E500D4 Ethernet
		• Readers interface: Wiegand-26, Wiegand-34, Wiegand-4/6/8 (for keyboards), Dallas Touch Memory

Equipment	Function	Features

E500U/R500U	Access controller	• Max. number of users: 7000
		• Time zones: 500
		• Event log capacity: 40000
		• Communication interface:
		  • E500U Ethernet
		  • R500U RS-485
		• Readers interface: Wiegand-26/34/37/42/58, Wiegand-4/6/8 (for keyboards), Dallas Touch Memory

R900I/E900I	Access controller	• Max. number of users: 96000
		• Time zones: 30000
		• Event log capacity: 400000
		• Communication interface:
		  • R900I RS-485
		  • E900I Ethernet
		• Readers interface: Wiegand-26, Wiegand-34, Wiegand-4/6/8 (for keyboards), Dallas Touch Memory

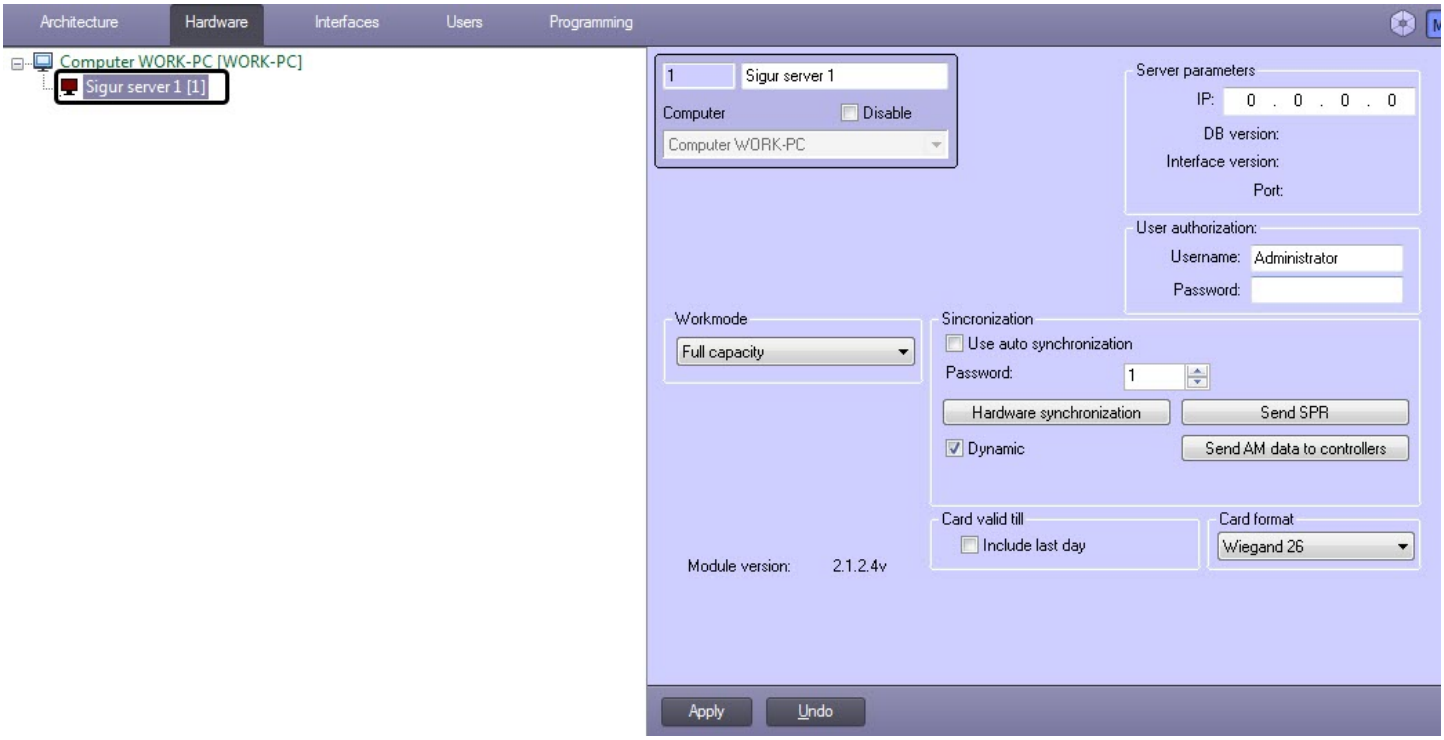
E900U/R900U	Access controller	• Max. number of users: 96000
		• Time zones: 30000
		• Event log capacity: 400000
		• Communication interface:
		  • R900U RS-485
		  • E900U Ethernet
		• Readers interface: Wiegand-26/34/37/42/58, Wiegand-4/6/8 (for keyboards), Dallas Touch Memory

Protection
1 IP address (Sigur Server). The Hasp security key is required for the Sigur Server.

4 Configuring Sigur integration module

4.1 Configuring the Sigur Server

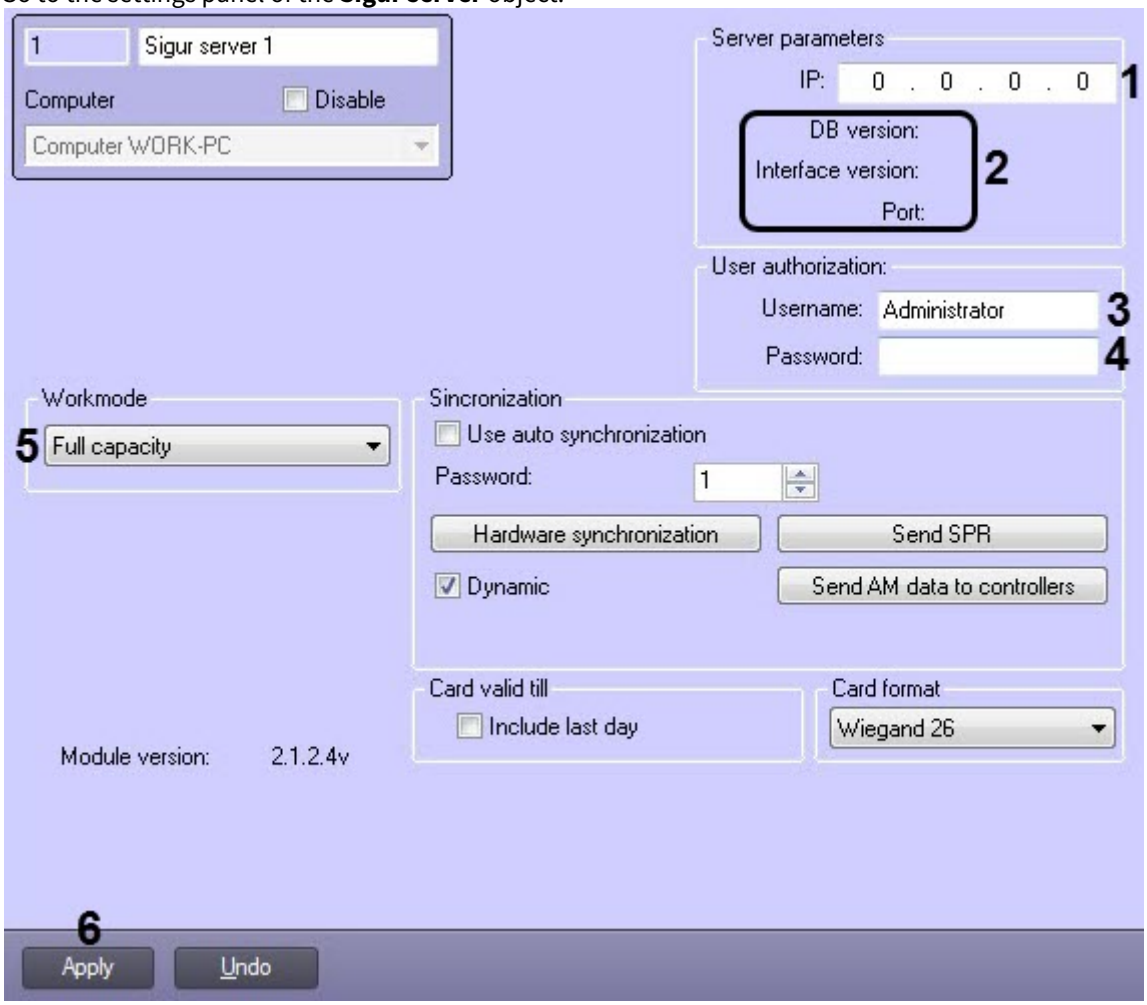
The Sigur Server is configured on the settings panel of the **Sigur server** object. This object is created on the basis of the **Computer** object on the **Hardware** tab of the **System Settings** dialog box.



4.1.1 Configuring the Sigur server connection to ACFA Intellect

To configure the *Sigur* server connection to *ACFA Intellect*, do the following:

1. Go to the settings panel of the **Sigur server** object.



In the **Server parameters** field (**1**), enter the IP address of the *Sigur* server.

> **Note.**
>
> The following information is displayed in the area (**2**):
> - **DB version** - the version of *Sigur* ACS database;
> - **Interface version** - the version of the data exchange protocol between *Sigur* server and *ACFA Intellect*;
> - **Port** - the port used for the *Sigur* server-*ACFA Intellect* connection.

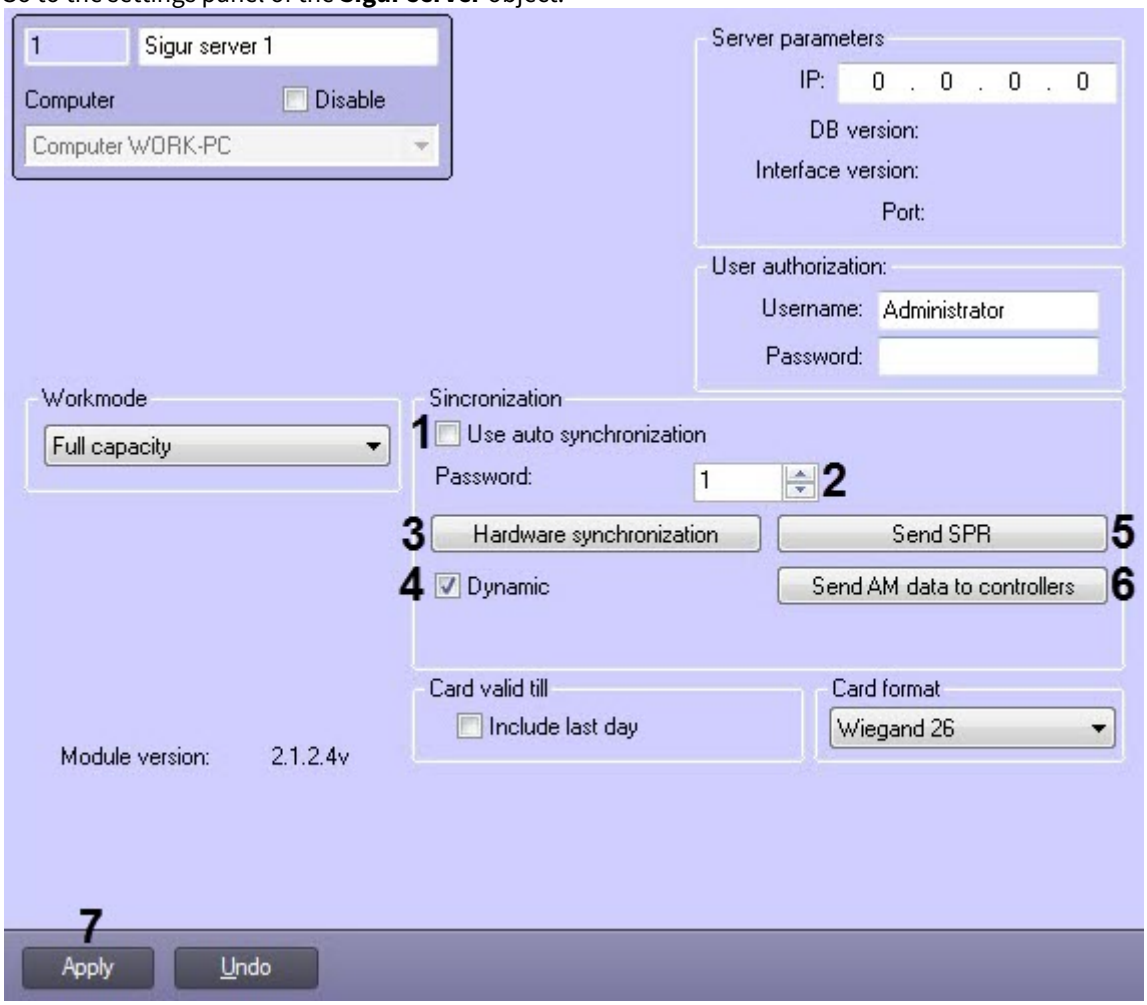
2. In the **Synchronization** (**3**) and **Username** (**4**) fields, enter the username and password, respectively, used to login to the *Sigur* ACS Client software (see the official reference documentation for the Sigur ACS).
3. From the **Workmode** drop-down list (**5**), select the operation mode of the *Sigur* server:
   - **Full capacity** - configuration, management and monitoring are available.
   - **Monitoring** - only management and monitoring are available. Also, the Synchronization and management of Sigur ACS configuration and Configuring the Sigur user access cards will be unavailable.
4. Click the **Apply** button to save the changes (**6**).

The *Sigur* server connection to *ACFA Intellect* is now configured.

4.1.2 Synchronization and management of Sigur ACS configuration

To synchronize and manage the *Sigur* ACS configuration, do the following:

1. Go to the settings panel of the **Sigur server** object.



2. Set the **Use auto synchronization** checkbox (**1**) if it is necessary to send data from the *Access Manager* module to the *Sigur* server after a specified time period.
3. In the **Password** field (**2**), enter the time period in hours after which the data of the *Access Manager* module will be sent to the *Sigur* server.

> **Note**
>
> The time period count starts from the moment the *Sigur* integration module is launched.

4. Click the **Hardware synchronization** button (**3**) to read the *Sigur* ACS configuration stored on the *Sigur* server and to build the corresponding object tree in the *ACFA-Intellect* software package.
5. Set the **Dynamic** checkbox (**4**) if it is necessary to automatically send the changed data of the *Access Manager* module to the *Sigur* server.

> **Attention!**
>
> To ensure the proper operation of *Sigur* integration module, it is required that the **Dynamic** checkbox is always set.

> **Note**
>
> In order to speed up the autosync process, the following user sending logic is used.
>
> The users who have at the time of synchronization:
>
> - the card issue date, which has not yet come;
> - the card expiration date that has already passed;
> - access levels that are unrelated to the the controllers of this Castle server;
> - or the **User locked** property
>
> are not written to the controller.

6. Click the **Send SPR** button (**5**) to send the data from the *Access Manager* module to the *Sigur* server.

> **Attention!**
>
> The *Sigur* server connection to *ACFA-Intellect* should be configured prior to performing this action.

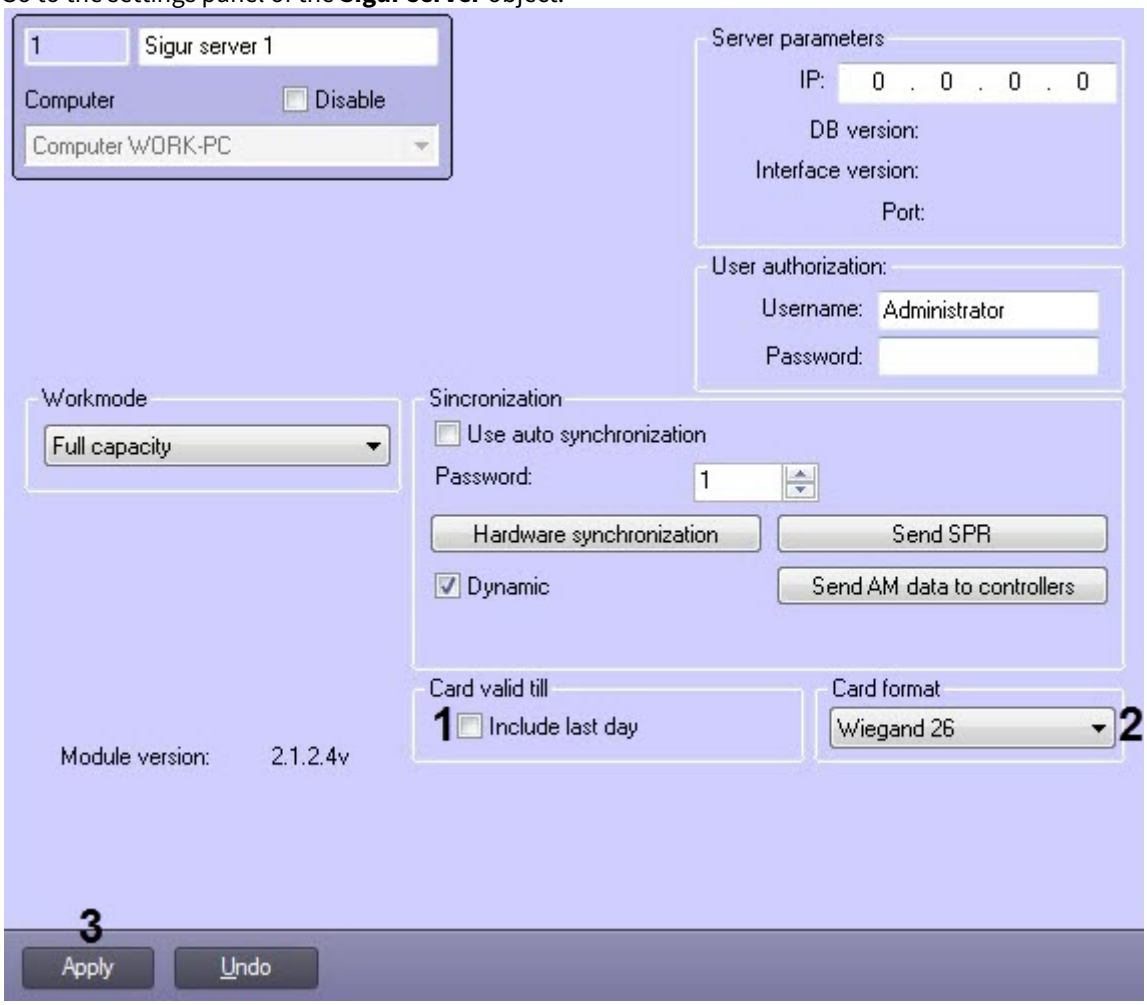
7. Click the **Send AM data to controllers** button (**6**) to send the previously sent data of the *Access Manager* module to the *Sigur* controllers.
8. Click the **Apply** button (**7**).

Synchronization and management of *Sigur* ACS configuration are now complete.

4.1.3 Configuring the Sigur user access cards

To configure the access cards for *Sigur* users, do the following:

1. Go to the settings panel of the **Sigur server** object.



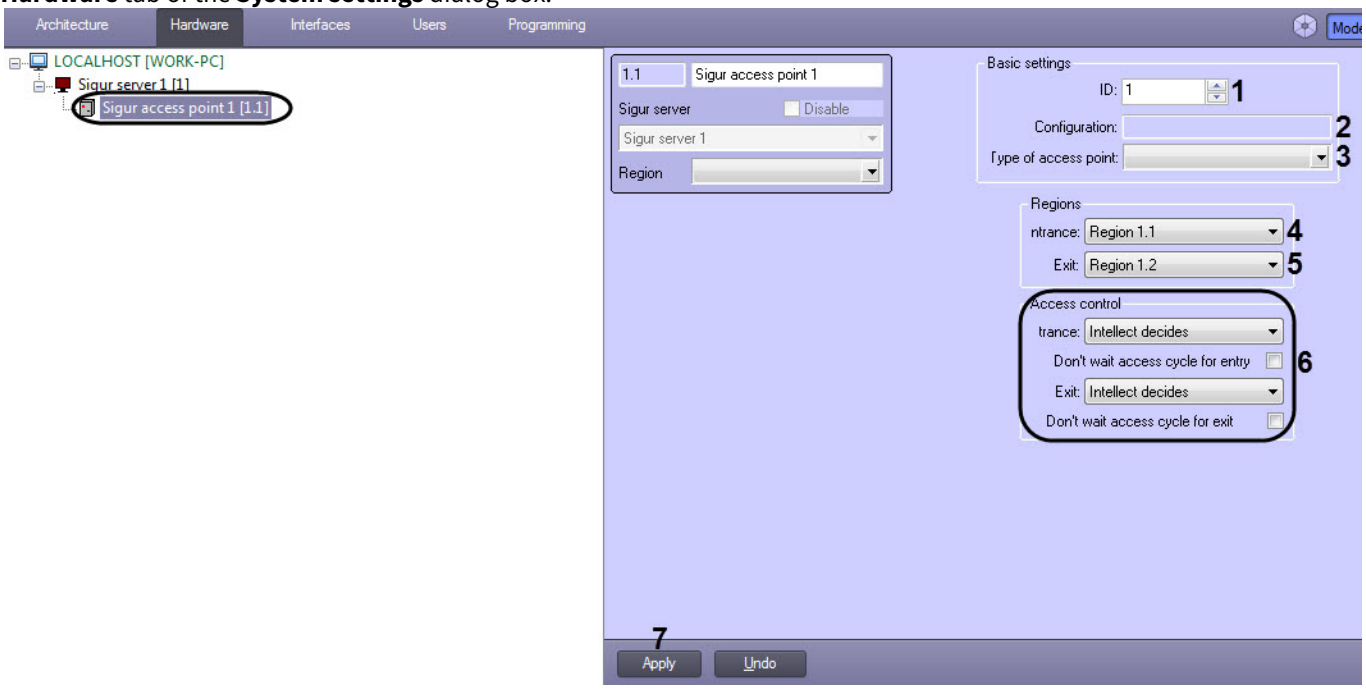
2. Set the **Include last day** checkbox (**1**) to grant users access on the day the access card expires (**Valid till** field, see Settings panel of the User object).
3. From the **Card format** drop-down list (**2**), select the access card data format: **Wiegand 26** or **Wiegand 34**.
4. Click **Apply** (**3**).

Configuring the access cards for the *Sigur* users is completed.

4.2 Configuring Sigur access points

To configure the *Sigur* ACS access points, do the following:

1. Go to the settings panel of the **Sigur access point** object, which is created on the basis of the **Sigur server** object in the **Hardware** tab of the **System settings** dialog box.



2. In the **ID** field (**1**), enter the access point number on the *Sigur* server.

> **Note**
>
> The **Configuration** field (**2**) displays the access point configuration, which is set using the switch on the card of the corresponding *Sigur* ACS controller.

3. From the **Type of access point** drop-down list (**3**), select the type of access point managed by the controller:
   - **Gate**;
   - **Door**;
   - **Turnstile**;
   - **Barrier**.
4. From the **Entrance** drop-down list (**4**), select the **Region** object corresponding to the area on the side of exit from the access point.
5. From the **Exit** drop-down list (**5**), select the **Region** object corresponding to the area on the side of entrance to the access point.
6. Set the access control parameters at entrance and exit (**6**):
   a. From the **Entrance** and **Exit** drop-down lists, select the decision-making side for granting access:
      i. **Intellect decides** - access decision is automatically made by *ACFA-Intellect*.
      ii. **Operator decides** - access decision is made by the operator.

      > **Note.**
      >
      > To process the request operator is to create a **Photo ID** interface object and configure it for the **Operator's query (Access granted)** event. For more information about this object and its functions, please refer to Photo ID User Guide.

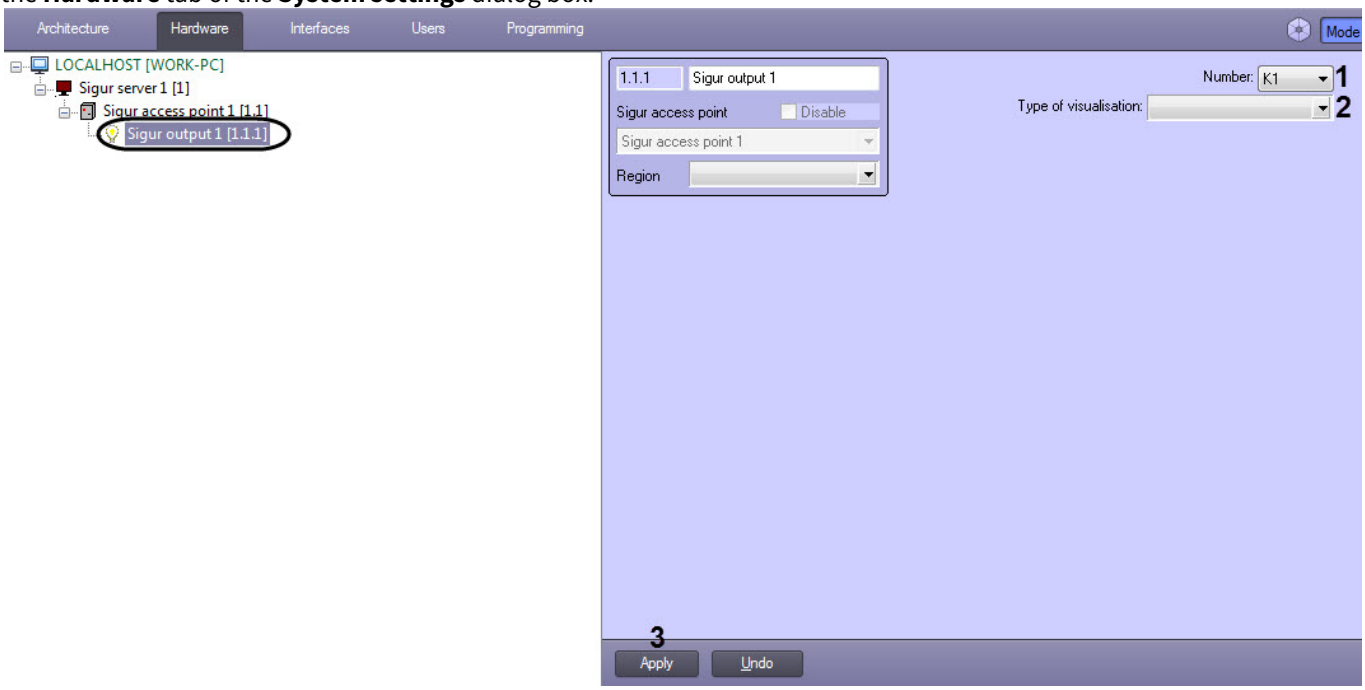
   b. Set the **Don't wait access cycle for entry** and **Don't wait access cycle for exit** checkboxes if it is necessary to record the passage immediately after placing the access card to the reader. If the passage is considered to be performed only after passing the access point (i.e. door sensor is triggered), unset this checkbox.
7. Click the **Apply** button to save all changes (**7**).

Sigur ACS access points are now configured.

4.3 Configuring Sigur output

To configure the *Sigur* ACS output, do the following:

1. Go to the settings panel of the **Sigur output** object, which is created on the basis of the **Sigur access point** object in the **Hardware** tab of the **System settings** dialog box.

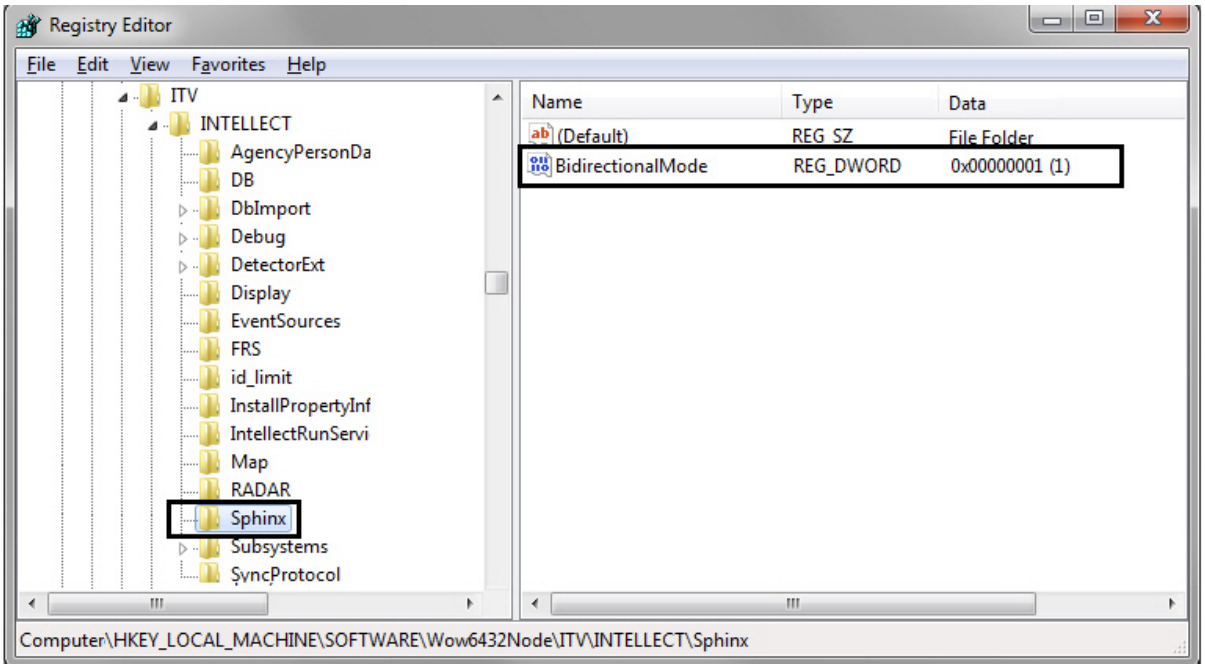


2. From the **Number** drop-down list (**1**), select the output number.
3. From the **Type of visualisation** drop-down list (**2**), select the corresponding set of icons for the output.
4. Click **Apply** (**3**).

Sigur ACS output is now configured.

4.4 Configuring of access partition for entrance and exit

To enable access partition create the DWORD (32 bits) parameter with the BidirectionalMode name and value 1 in the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITV\INTELLECT\Sphinx register section.



Access partition for entry and exit is performed using intervals of time zones in the *Access Manager* interface object.

1. Even number of time intervals – odd intervals are applyed for entrance, even intervals – for exit.
2. Odd number of time intervals – as item 1, and the last interval is applied for both readers (for entrance and for exit).

5 Using Sigur integration module

5.1 General information about how to use Sigur integration module

The following interface objects are in use when working with *Sigur* integration module:

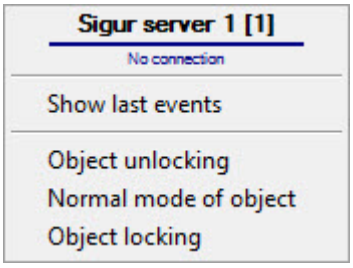
1. **Card**;
2. **Event Viewer**.

Information on how to configure these interface objects can be found in Intellect™ Software Package Administrator's Guide.

Information on how to work with these interface objects can be found in Intellect™ Software Package Operator's Guide.

5.2 Managing Sigur Server

The *Sigur* server is managed in the **Map** interactive window using the **Sigur server** object functional menu:



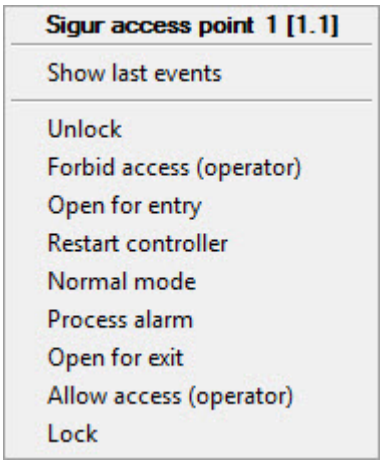
> **Note**
>
> To open the object's functional menu, right-click on the object's icon.

Menu commands of the **Sigur server** object are described in the table.

Menu command	Functionality
Object unlocking	All locks at access points are unlocked
Normal mode of object	All access points are in the normal mode
Object locking	All access points are constantly locked

5.3 Managing Sigur access point

The *Sigur* access point is managed in the **Map** interactive window using the **Sigur access point** object functional menu:



Note.

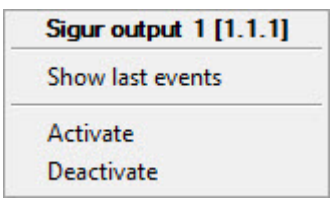
To open the object's functional menu, right-click on the object's icon.

Menu commands of the **Sigur access point** object are described in the table.

Menu command	Functionality
Unlock	The lock is unlocked at the access point
Forbid access (operator)	Access is forbidden (after receiving access request)
Open for entry	The access point is unlocked for entrance
Restart controller	Access point controller is restarted
Normal mode	Access point is in the normal mode: access point is normally locked; it is unlocked when reading the key; after passing or when the specified time expires access point is automatically locked
Process alarm	Registration of alarm at the access point is confirmed
Open for exit	The access point is unlocked for exit
Allow access (operator)	Access is allowed (after receiving access request)
Lock	Access point is locked, there is no access

5.4 Managing Sigur output

The *Sigur* output is managed in the **Map** interactive window using the **Sigur output** object functional menu:



> **Note**
>
> To open the object's functional menu, right-click on the object's icon.

Menu commands of the **Sigur output** object are described in the table.

Menu command	Functionality
Activate	Output activation
Deactivate	Output deactivation