ACFA Intellect

Sphinx integration module configuration and operation manual

Last update 11/03/2019

Table of contents

1 List of terms used in Sphinx 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 *Sphinx* server over TCP/IP protocol. *Intellect* Server is the *Sphinx* server's Client.

Sphinx client – computer with installed *Sphinx ACS* software, connected to *Sphinx* 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.

Sphinx server - computer with installed *Sphinx 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 Sphinx integration module configuration and operation manual

On the page:

2.1 Purpose of the Document

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

The guide provides:

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

2.2 General information about Sphinx integration module

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

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

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

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

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

3 Supported hardware and licensing of the Sphinx 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	• Unlimied 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 (Sphinx Server). The Hasp security key is required for the Sphinx Server.

4 Configuring Sphinx integration module

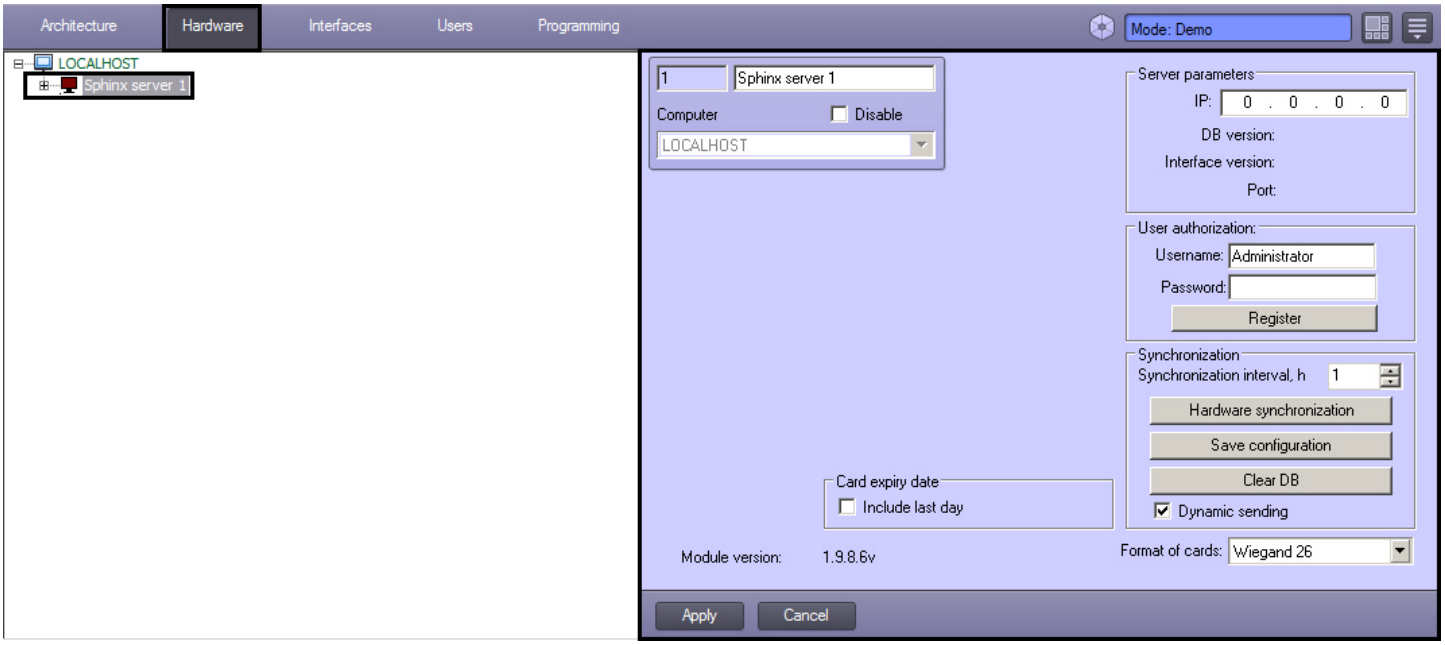
4.1 Configuration procedure for Sphinx integration module

Here is the configuration procedure for *Sphinx* integration module:

1. Configure interaction between *ACFA Intellect* and *Sphinx* server;
2. Synchronize *Sphinx ACS* and *Intellect ACFA* configurations;
3. Configure *Sphinx ACS* access points*;*
4. Configuring *Sphinx* outpus;
5. Configuring of access partition for entrance and exit.

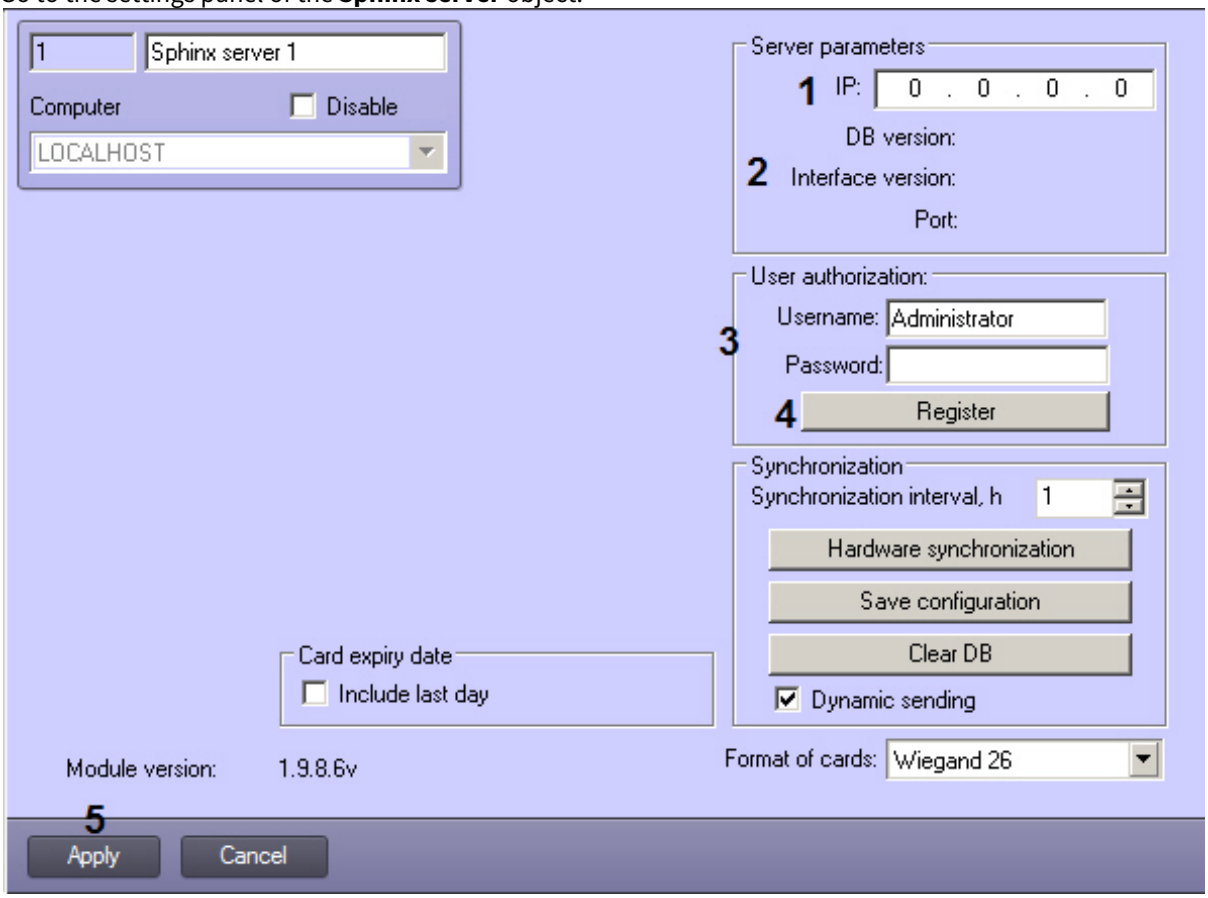
4.2 Configuring interaction between ACFA Intellect and Sphinx server

Interaction between *ACFA Intellect* and *Sphinx* server is configured on the settings panel of the **Sphinx server** object. This object is created on the base of the **Computer** object in the **Hardware** tab of the **System settings** dialog box.



To configure interaction between *ACFA Intellect* and *Sphinx* server do the following:

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



> **Note.**
> The version of *Sphinx* integration module is displayed in the **Module version** field (5).
> The following information is displayed in the **Server parameters** group (2):
> a. Version of *Sphinx* ACS database (the **DB version** field);
> b. Version of *Sphinx* server – Client data exchange protocol (the **Interface version** field);
> c. Port used for *Sphinx* server-Client connection (the **Port** field).
> *Intellect* Server is the Client in this case.

2. Specify the *Sphinx* server IP address in the **IP** field (**1**).
3. In the **User authorization** group specify the username (the **Username** field) and password (the **Password** field) used to login to the *Sphinx* server (**3**).

> **Note.**
> Any pair of values used to login to *Sphinx* Client is to be specified (see reference documentation about Sphinx ACS).

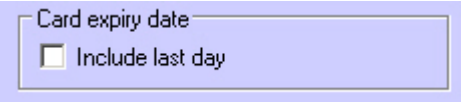
4. To login to *Sphinx* server click the **Register** button (**4**).
   As a result the **Access point** objects that correspond to *Sphinx ACS* access points are created in the objects tree of the *ACFA Intellect* objects.
5. Click the **Apply** button to save all changes (**6**).

Interaction between *ACFA Intellect* and *Sphinx* server is now configured.

4.3 Configuring user access cards in the Sphinx integration module

By default, access is not granted to a user on the day specified as a card expiration date (the **Valid till** parameter, see Settings panel of the User object).

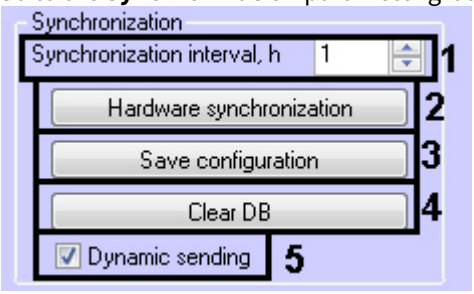
If *Sphinx* integration module is to grant access on the specified day, set the **Include last day** checkbox on the **Sphinx server** object settings panel and click **Apply**.



4.4 Synchronization of Sphinx ACS and Intellect ACFA configurations

To synchronize *Sphinx* ACS and *Intellect* ACFA configurations do the following:

1. Go to the **Synchronization** parameter group on the settings panel of the **Sphinx server** object.



> **Important!**
> The **Dynamic sending** checkbox is always to be checked for proper operation of *Sphinx* integration module (5).

2. Parameters are to be auto synchronized between *Intellect* and *Sphinx* servers. Specify the interval for parameters auto synchronization (in hours) in the **Synchronization interval** field (**1**).
3. To read *Sphinx* ACS configuration stored on *Sphinx* server click the **Hardware synchronization** button (**2**).
4. To send *ACFA Intellect* configuration to *Sphinx* server click the **Save configuration** button (**3**).

> **Important!**
> This action is to be performed after configuring interaction between Intellect and *Sphinx* servers.

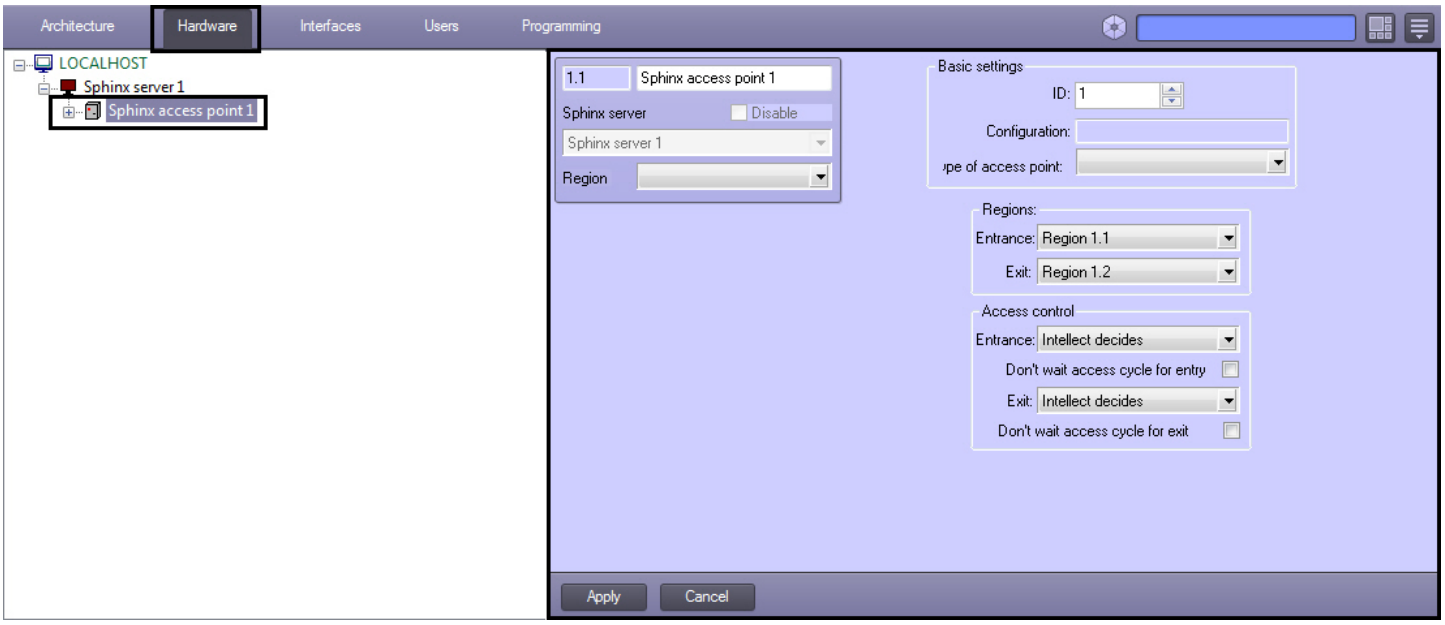
> **Note**
> In order to speed up the autosync process, the following user sending logic is used.
> The users who have at the time of synchronization:
> 1. the card issue date, which has not yet arrived;
> 2. the card expiration date that has already passed;
> 3. access levels that are unrelated to the the controllers of this Castle server;
> 4. or the **User locked** property
> are not written to the controller.

5. To clear the *Sphinx* server database click the **Clear DB** button (**4**).
6. Click the **Apply** button.

Sphinx ACS and Intellect ACFA configurations are now synchronized.

4.5 Configuring Sphinx ACS access points

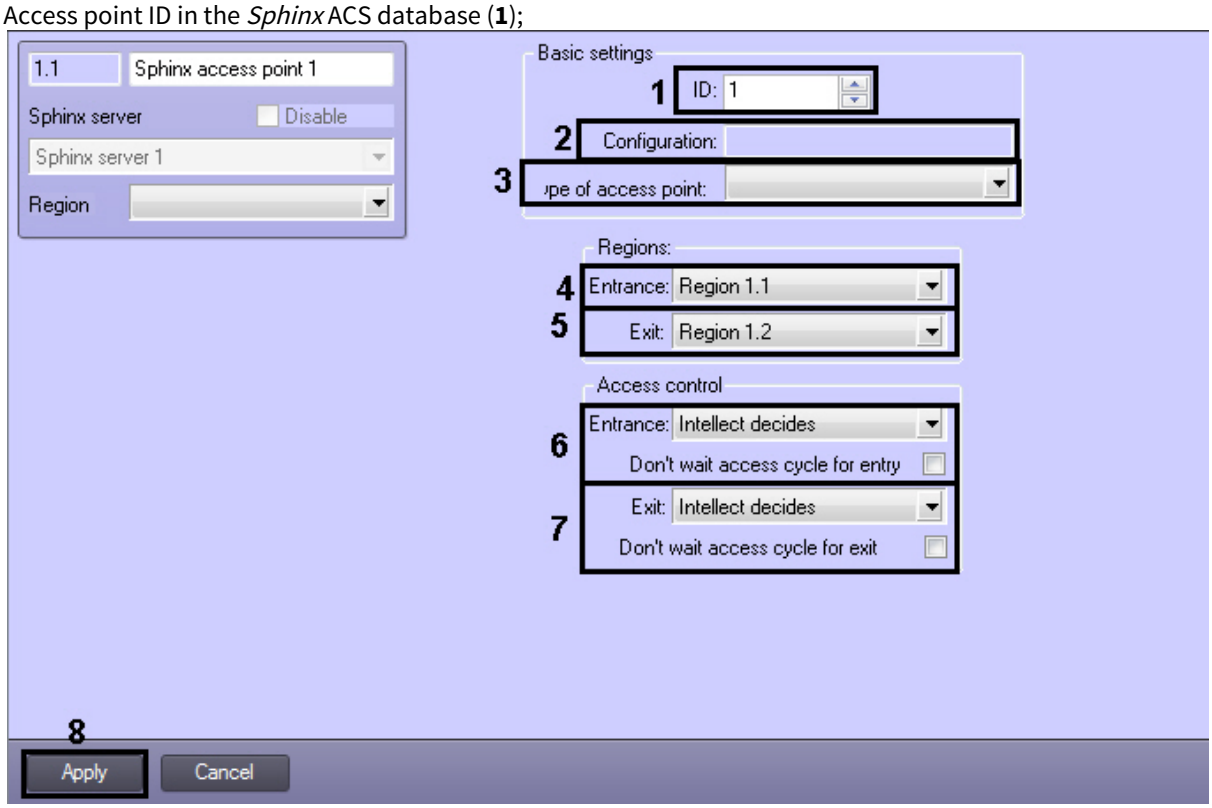
Sphinx ACS access point is configured on the settings panel of the **Sphinx access point** object. This object is created on the base of the **Sphinx server** object in the **Hardware** tab of the **System settings** dialog box.



The **Access point** object is registered automatically when reading *Sphinx ACS* configuration.

The following parameters are automatically specified when reading *Sphinx ACS* configuration:

1. Access point ID in the *Sphinx* ACS database (**1**);



2. access point configuration (**2**);

> **Note.**
> Access point configuration is set using the switch on the card of corresponding *Sphinx ACS* controller (see reference documentation about *Sphinx ACS*).

3. access control mode (**3**).

Sphinx ACS access points are configured as follows:

1. In the **Entry** dropdown list select the **Region** object corresponding to the area on the side of exit from the access point (**4**).
2. In the **Exit** dropdown list select the **Region** object corresponding to the area on the side of entrance to the access point (**5**).
3. Set parameters of access control at entrance (**6**):
    a. In the **Entry** dropdown list select the one that will decide whether to give access or not and whether to register it or not – *Intellect* Server or operator;

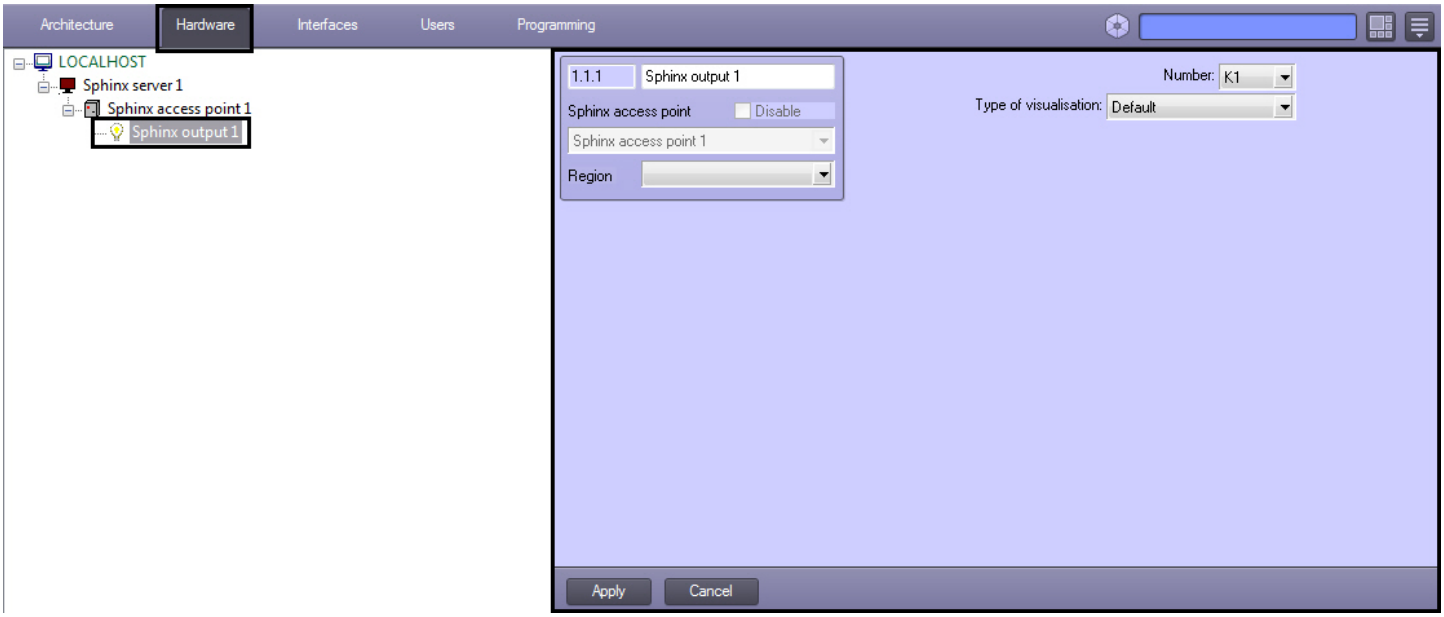
    > **Note.**
    > To process the request operator is to create a **Photo ID** interface object and configure it for the **Operator's query (Access granted)** event. For more information about this object and its functions, please refer to Photo ID User Guide.

    b. If it is considered that passing is performed just after placing the access card to the reader, then check the **Don't wait access cycle for exit** checkbox. If the passing is considered to be performed only after passing the access point (i.e. door sensor is triggered), uncheck this checkbox.
4. Set parameters of access control at exit (**7**). The parameters are the same as those of access control at entrance (see the previous item).
5. Click the **Apply** button to save all changes (**8**).
6. Repeat steps 1-9 for all required *Sphinx ACS* access points.

Sphinx ACS access points are now configured.

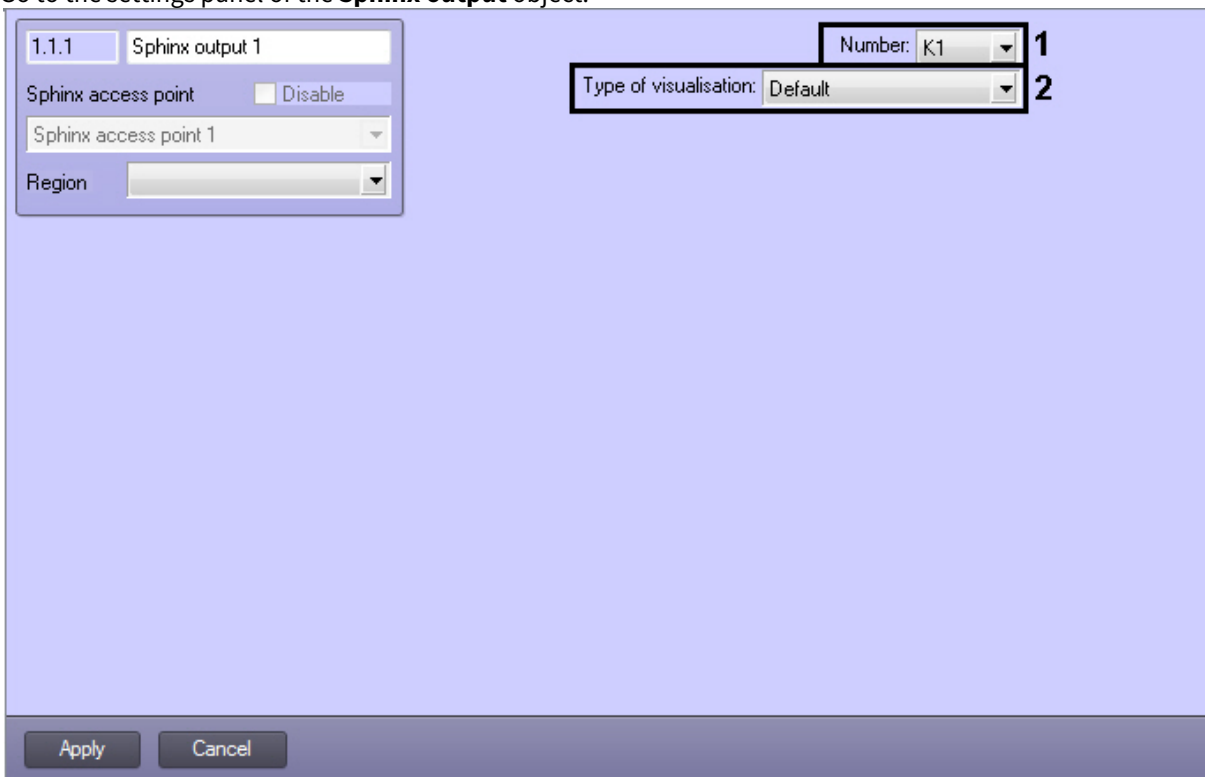
4.6 Configuring Sphinx output

Sphinx Output is configured on the settings panel of the **Sphinx output** object. This object is created on the base of the **Sphinx Access point** object in the **Hardware** tab of the **System settings** dialog box.



Configuring *Sphinx ACS* output is performed as follows:

1. Go to the settings panel of the **Sphinx output** object.

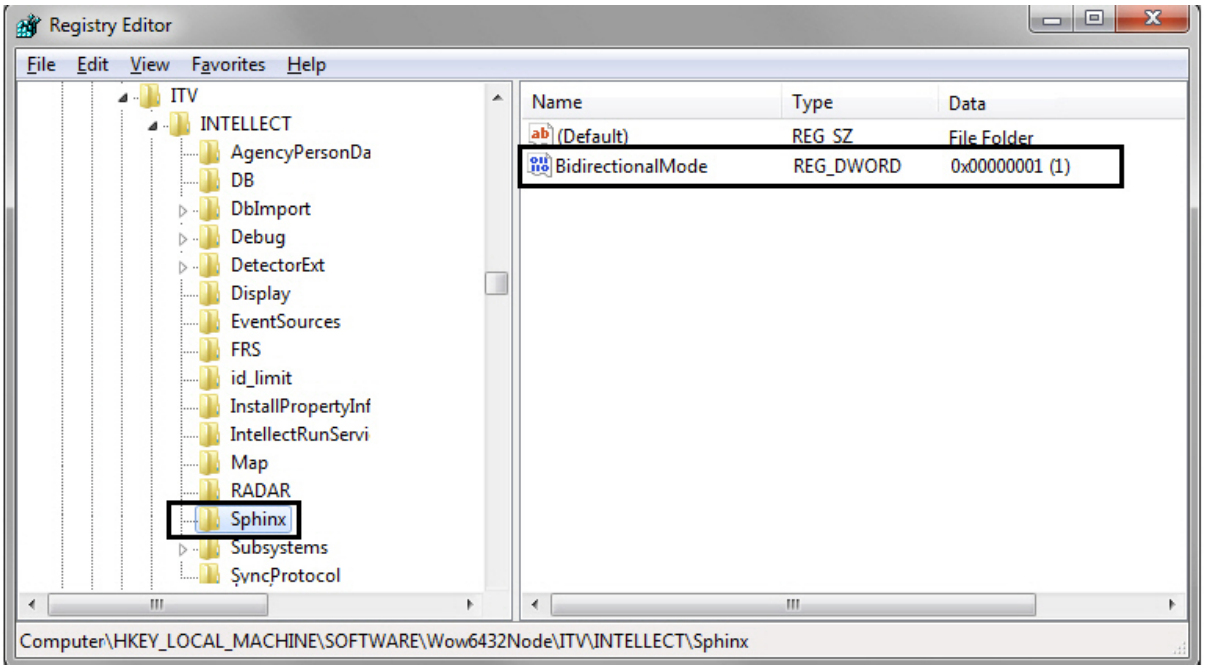


2. The output number is automatically specified when reading *Sphinx ACS* configuration (**1**).
3. From the **Type of visualisation** drop-down list select the corresponding set of icons for the output (**2**).
4. Click **Apply**.

Sphinx outputs are now configured.

4.7 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 *Visitor Management System* 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 Sphinx integration module

5.1 General information about how to use Sphinx integration module

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

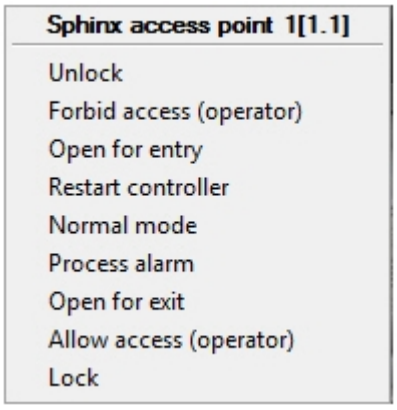
1. **Card**;
2. **Event Viewer**.

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 Sphinx access point

An access point is managed in the **Map** interactive dialog box using the feature menu of the Sphinx access point object.

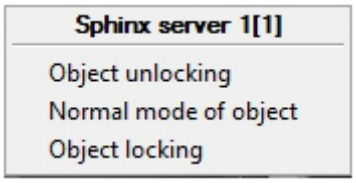


Note.
To call the feature menu of the object, right-click the object icon.

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

Menu command	Functionality
Lock	Access point is locked, there is no access
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
Forbid access (operator)	Access is forbidden (after receiving access request)
Allow access (operator)	Access is allowed (after receiving access request)
Unlock	The lock is unlocked at the access point
Restart controller	Access point controller is restarted
Process alarm	Registration of alarm at the access point is confirmed

All access points can be managed using the feature menu of the **Sphinx server** object.

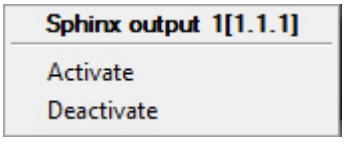


Menu commands of the **Sphinx server** object are described in the table.

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

5.3 Managing Sphinx output

An output is managed in the **Map** interactive dialog box using the feature menu of the Sphinx output object.



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

Menu command	Functionality
Activate	Output activation
Deactivate	Output deactivation