ACFA Intellect

Sphinx integration module configuration and operation manual

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.

Introduction into Sphinx integration module configuration and operation manual

On the page:

Purpose of the Document

Configuration and operation manual for Sphinx integration module is a reference and information guide meant for *Sphinx* c onfiguration 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.

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).

Configuring Sphinx integration module

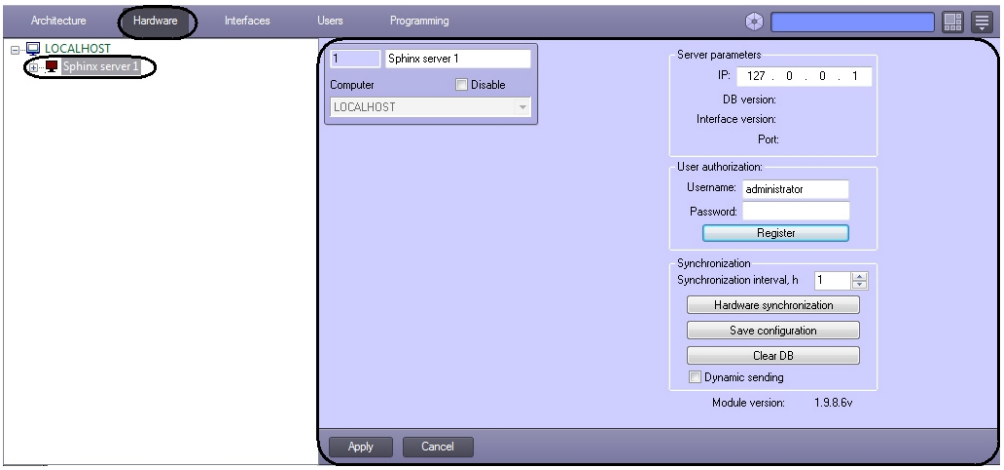
Configuration procedure for Sphinx integration module

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.

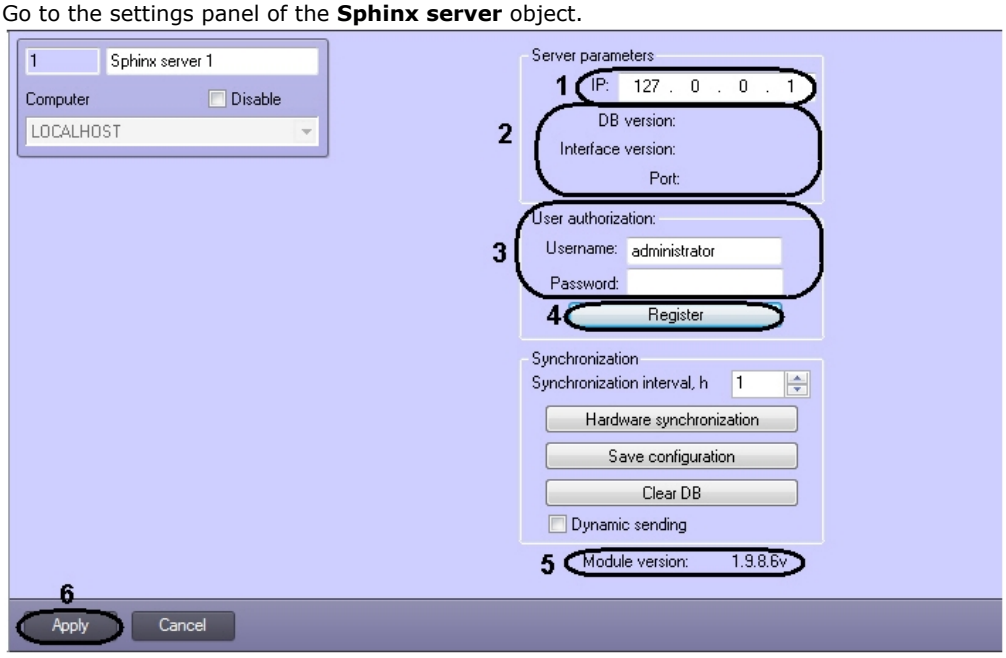
Configuring interaction between ACFA Intellect and Sphinx server

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 **Localhost** 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).

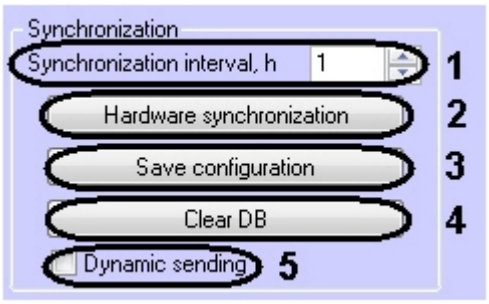
4. To login to *Sphinx* server click the **Register** button (**4**).
   As a result the **Access point** objects that correspond to *Sphinx ACS* access points are created in the objects tree of the *ACFA Intellect* objects.
5. Click the **Apply** button to save all changes (**6**).

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

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**).

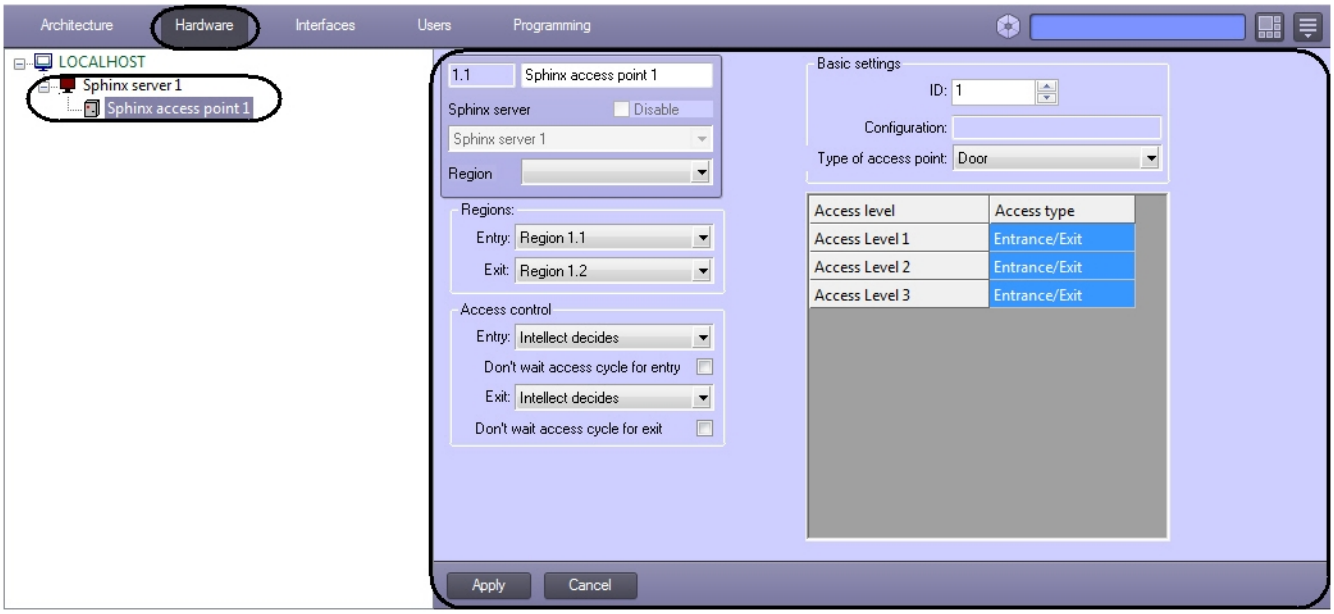
Important!
This action is to be performed after configuring interaction between Intellect and *Sphinx* servers.

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.

Configuring Sphinx ACS access points

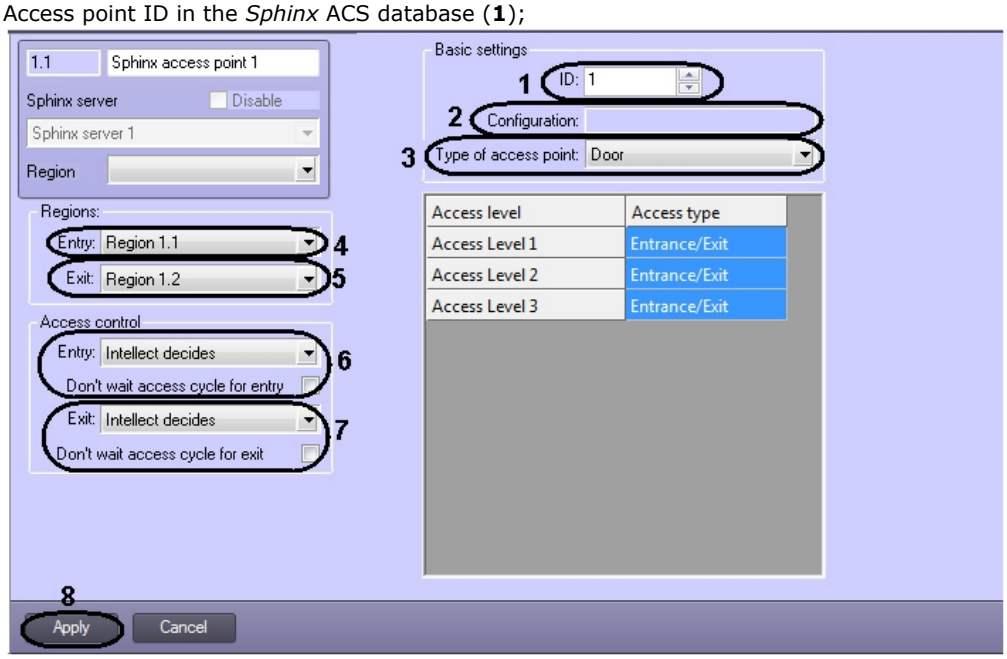
Sphinx ACS access point is configured on the settings panel of the **Sphinx access point** object. This object is created on the base of the **Sphinx server** object in the **Hardware** tab of the **System settings** dialog box.



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.

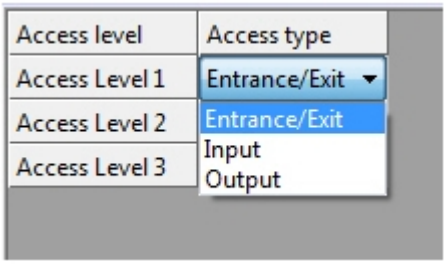
4. Set parameters of access control at exit (**7**). The parameters are the same as those of access control at entrance (see the previous item).
5. Click the **Apply** button to save all changes (**8**).
6. Repeat steps 1-9 for all required *Sphinx ACS* access points.

Sphinx ACS access points are now configured.

Setting access levels limitations at Sphinx access points

Access levels created on the Intellect Server are displayed on the settings panel of the **Sphinx access point** object. By default, they are applied when passing into and out of.

To change the default settings, select the value for each access level in the **Access type** list.



Click the **Apply** button to save all changes.

Access levels limitations at access points are now set.

Using Sphinx integration module

General information about how to use Sphinx integration module

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

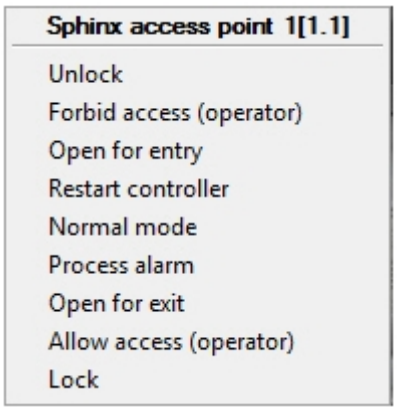
1. **Card**;
2. **Event Viewer**.

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.

Managing Sphinx access point

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



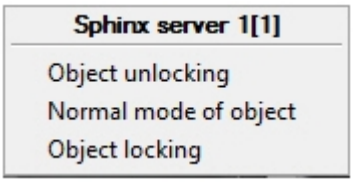
Note.
To call the feature menu of the object, right-click the object icon.

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