Unicard Integration Module Settings Guide

ACFA PSIM 1.1

Last update 05/03/2024

Table of Contents

1 Introduction into Unicard Module Settings Guide

On the page:

1.1 Purpose of the document

This *Unicard Module Settings Guide* is a reference manual designed for *Unicard* Module configuration technicians. This module is part of an access control system (ACS) built on the *ACFA PSIM* Software System.

This Guide presents the following materials:

1. general information about the *Unicard* integration module;
2. configuration of the *Unicard* integration module;
3. working with the *Unicard* integration module.

1.2 General information about the Unicard integration module

The *Unicard* module is a component of an ACS built on the *ACFA PSIM* Software System. It was designed to perform the following functions:

1. Configuration of the *Unicard* ACS (manufactured by UNICARD SA);
2. Interaction between the *Unicard* ACS and the *ACFA PSIM* Software System (monitoring, control).

Note.

Detailed information about the *Unicard* ACS is presented in the official documentation for this system.

Before configuration the *Unicard* ACS integration module, do the following:

1. Install the *Unicard* hardware on the protected territory.
2. Connect the *Unicard* ACS hardware to the Server.

2 Supported hardware and licensing of the Unicard integration module

Manufacturer	Unicard SA ul. Lagiewnicka 54 30-417 Krakow Phone: 12 39 89 900 Fax: 12 39 89 901 http://www.unicard.pl/
Integration type	Low-level protocol
Equipment connection	Ethernet

Supported equipment

Equipment	Function	Features
U700	Access controller	Interfaces: Ethernet, RS-232 / RS-485, AbaTrackII / Wiegand 16 notification zones (digital inputs/outputs) 34 supported access control points 16 IO-700 modules connecting via CAN
Module IO-700		4 readers connected

Protection
1 reader.

3 Configuration of the Unicard integration module

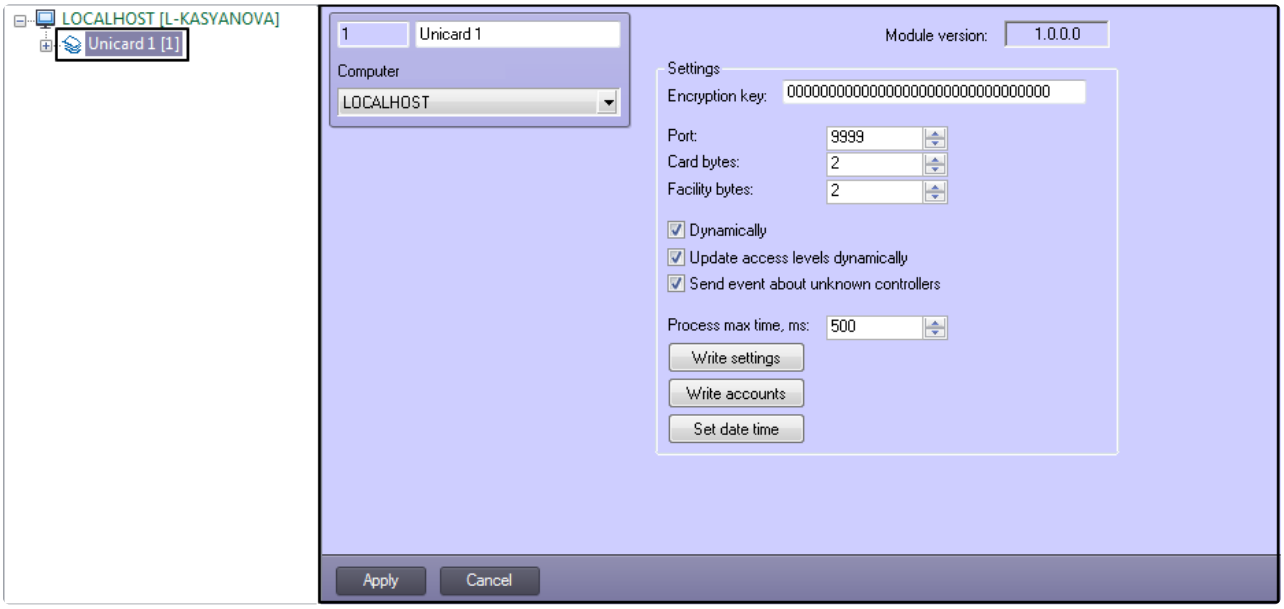
3.1 Procedure for configuring the Unicard integration module

The *Unicard* integration module is configured through the following steps:

1. Configuring the *Unicard* ACS connection to *ACFA PSIM* software package.
2. Configuring the *Unicard* controller.
3. Configuring the Unicard zones.
4. Configuring the Unicard ACP.
5. Configuring the *Unicard* reader.

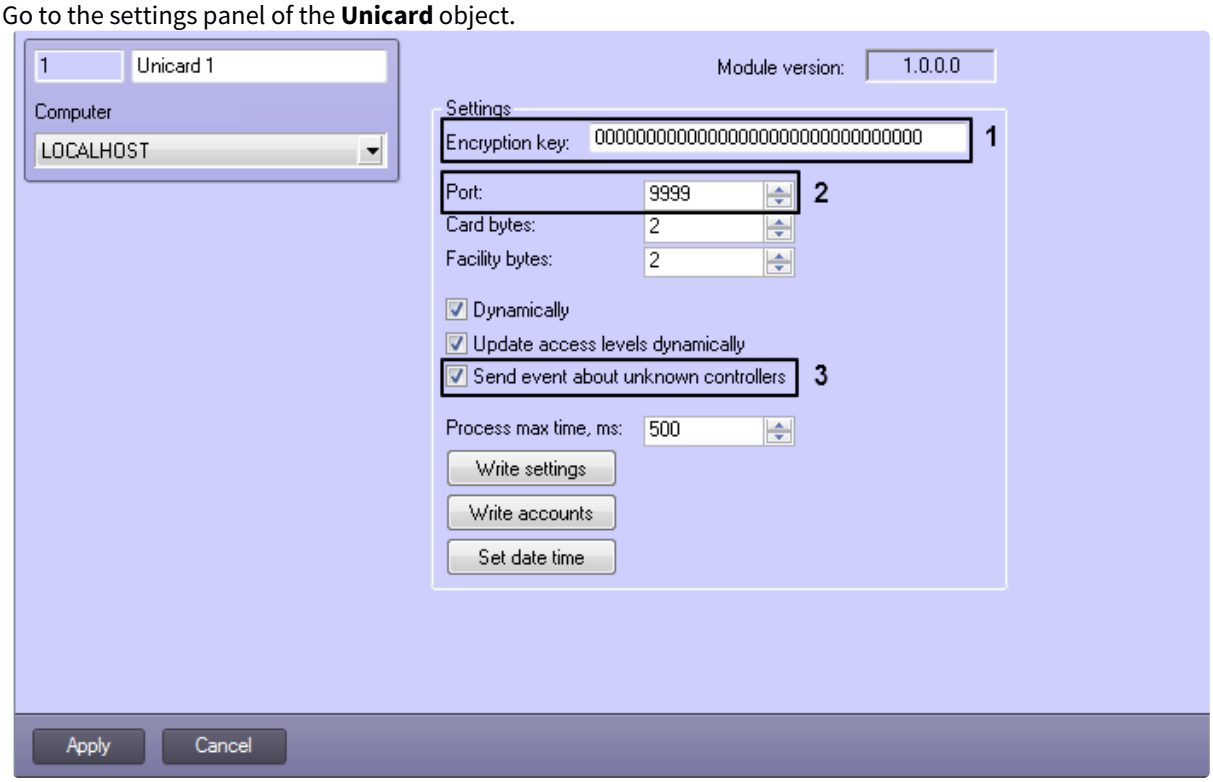
3.2 Configuration of the Unicard ACS connection to ACFA PSIM software package

Configuration of the *Unicard* ACS connection to *ACFA PSIM* software package is performed on the settings panel of the **Unicard** object. This object is created on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog window.



To configure the connection of *Unicard* ACS to *ACFA PSIM* software package do the following:

1. Go to the settings panel of the **Unicard** object.

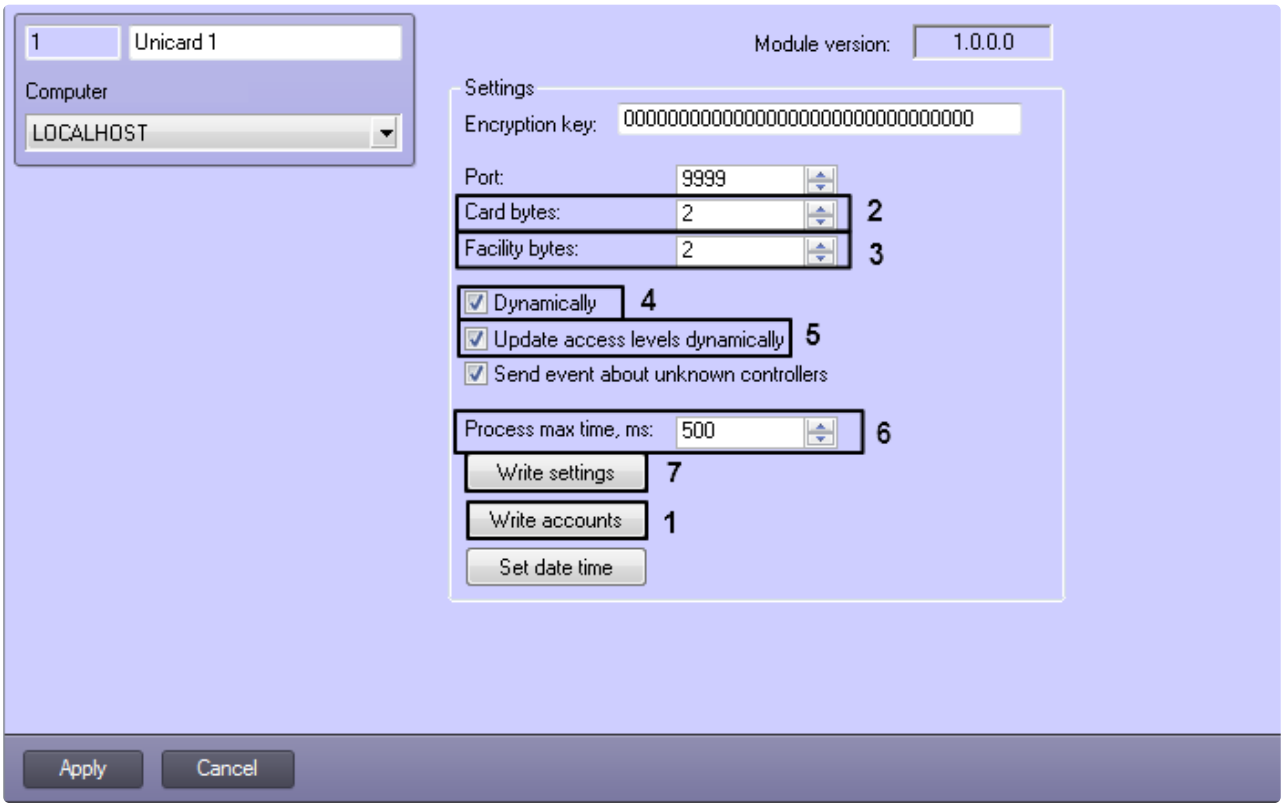


2. In the **Encryption key** field enter the encryption code of data exchange. To get the encryption code refer to the manufacturer of the Unicard hardware (**1**).
3. In the **Port** field specify the number of the COM port to connect to *Unicard* ACS (**2**).
4. Check the **Send event about unknown controllers** box to generate an event in the **Event Manager** for each new *Unicard* controller trying to connect to *ACFA PSIM* (for details on controllers see Configuring the Unicard controller) (**3**).
5. Click the **Apply** button to save changes.

Configuration of the *Unicard* ACS connection to the *ACFA PSIM* software package is completed.

3.2.1 Sending accounts to Unicard controller

To send user settings, time zones and schedules to the *Unicard* controller click the **Write accounts** button on the settings panel of the **Unicard** object (**1**).



In the **Card bytes** field you may specify the number of bytes the user's card number will take (**2**).

In the **Facility** bytes you may specify the number of bytes the user's department code will take (**3**).

If changes to the user parameters are to be dynamically sent to the *Unicard* controller, set the **Dynamically** checkbox (**4**).

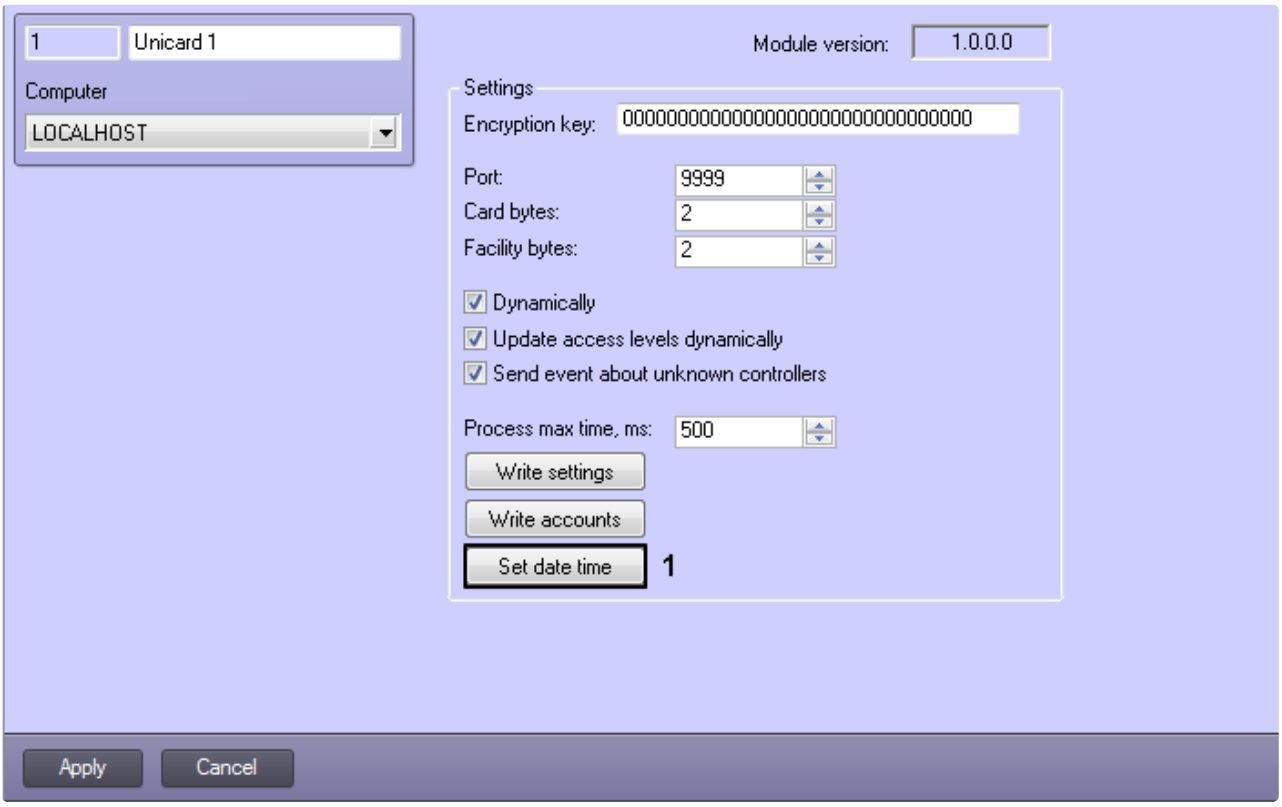
If changes to the user access levels are to be dynamically updated, set the **Update access levels dynamically** checkbox. (**5**)

In the **Process max time, ms** field you may specify the extra time limit to process the data the antipassback mode is on (in this case the data exchange is a little slower) (**6**).

To send the settings to the *Unicard* controller, click **Write settings** (**7**).

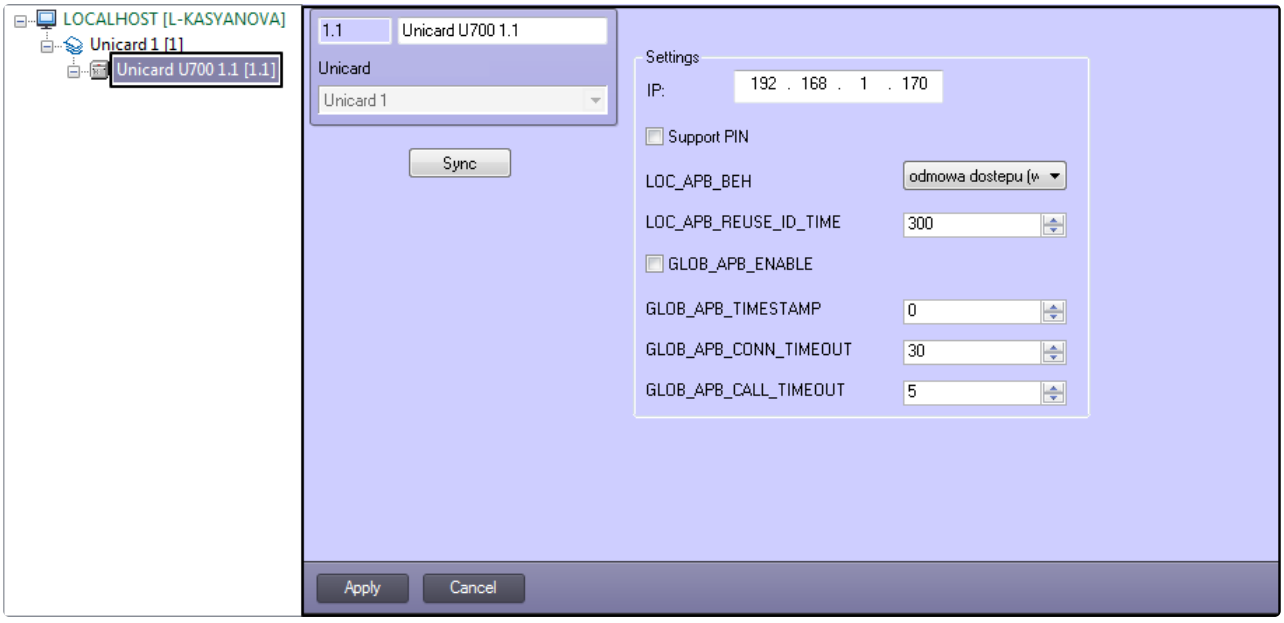
3.2.2 Synchronization of the Server time and the time of the Unicard controller

To synchronize date and time of the *Unicard* controller and Server time click the **Set date time** button on the settings panel of the **Unicard** object (**1**).



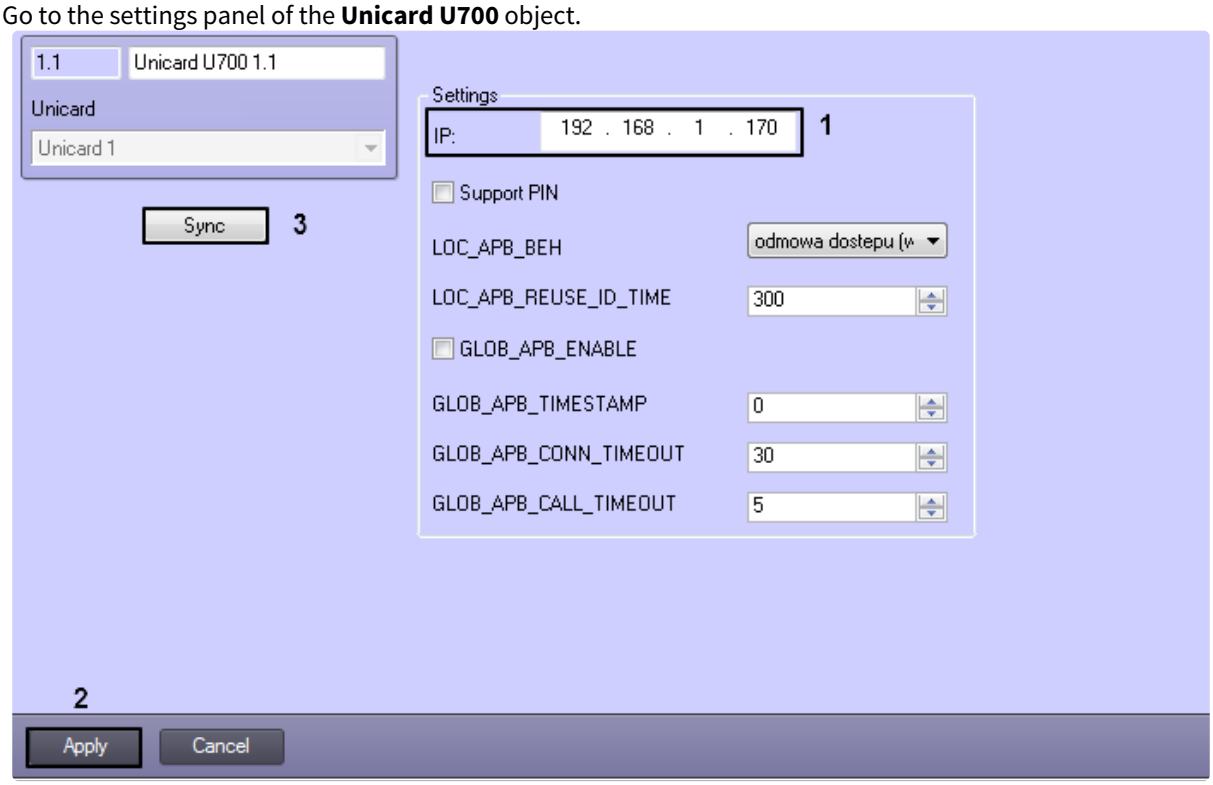
3.3 Configuring the Unicard controller

Configuring the *Unicard* controller is performed on the settings panel of the **Unicard U700** object created on the basis of the **Unicard** object on the **Hardware** tab of the **System settings** dialog window.

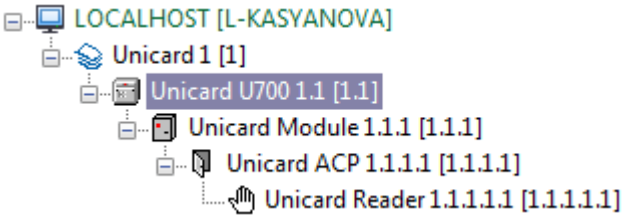


To configure the *Unicard* controller, do the following:

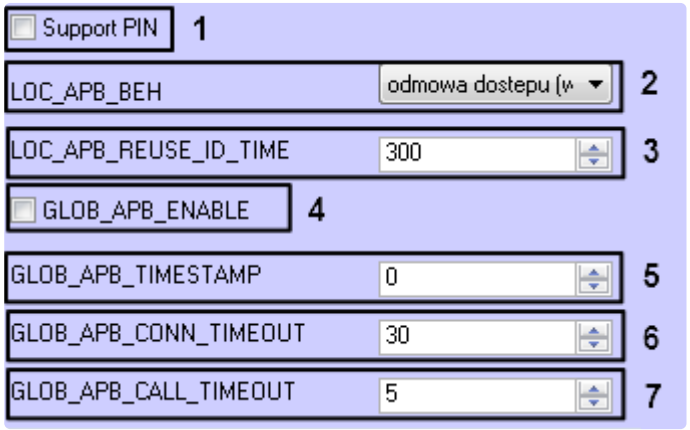
1. Go to the settings panel of the **Unicard U700** object.



2. Enter the controller's IP address in the **IP** field (**1**).
3. Click the **Apply** button (**2**).
4. Click the **Sync** buton to synchronize the objects tree (**3**).
   As a result configuration of the *Unicard* system will be read and objects tree will be created in the *ACFA PSIM* software.



The **Unicard U700** object has a set of extra settings for the controller that may be enabled in case of a need.

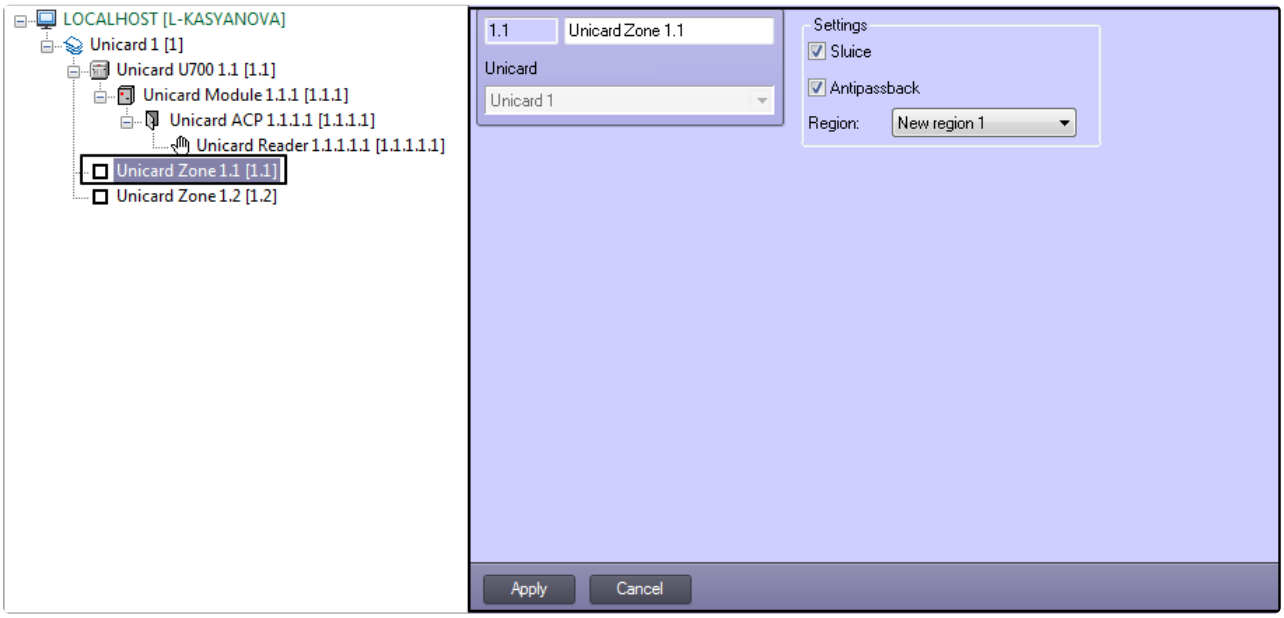


1. Check the **Support PIN** checkbox to enable PIN verification in addition to card verification. (**1**)
2. From the **LOCAL_APB_BEH** list you may select the behaviour of the controller if antipassback violation is detected: no reaction of the device, access denied (default), refusal of access for a time stated in the **LOCAL_APB_REUSE_ID_TIME** parameter. (**2**)
3. In the**LOCAL_APB_REUSE_ID_TIME** you may specify the time (in seconds) after which, despite the antipassback violation, the access is granted. Time is counted from the moment the user changes the zone. (**3**)
4. Check the **GLOBAL_APB_ENABLE** to enable global antipassback verification. (**4**)
5. In the **GLOBAL_APB_TIMESTAMP** field you may specify the global antipassback verification timestamp (**5**).
6. In the **GLOBAL_APB_CONN_TIMEOUT** field you may specify the connection failure time (in seconds), after which the device finds no communication with the global antipassback server. (**6**)
7. In the **GLOBAL_APB_CALL_TIMEOUT** field you may specify the wait time (in seconds) for the response from the global antipassback server to the query sent by the device (**7**).

Click **Apply** to write settings to the controller.

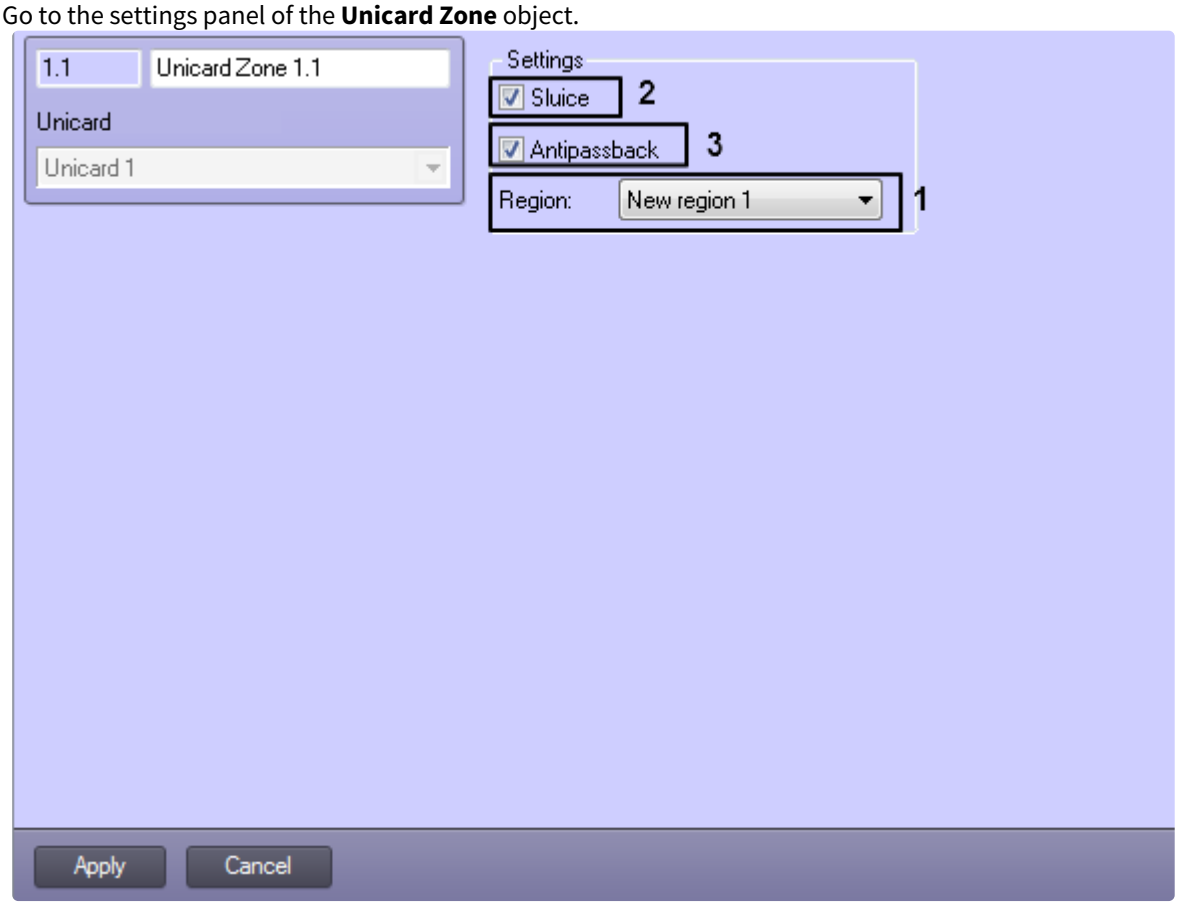
3.4 Configuring the Unicard zones

Configuring the *Unicard* zone is performed on the settings panel of the **Unicard Zone** object created on the basis of the **Unicard** object on the **Hardware** tab of the **System settings** dialog window.



To configure the *Unicard* zone, do the following:

1. Go to the settings panel of the **Unicard Zone** object.



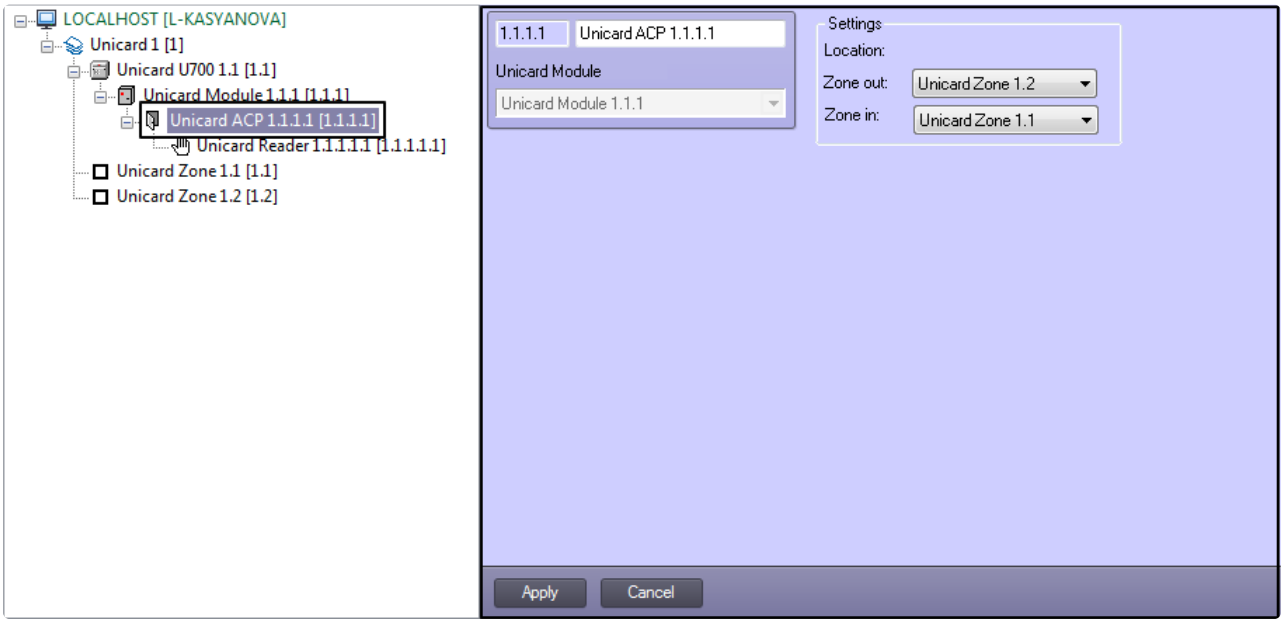
2. From the **Region:** drop-down list select the **Region** object corresponding to the zone (**1**).
3. If the access point to the zone is a sluice gate, check the **Sluice** box (**2**).
4. To enable antipassback for the zone, check the Antipassback box. (**3**)
5. Click the **Apply** button to save changes.
6. Repeat Steps 1-4 for all the zones.

Configuring the *Unicard* zones is completed.

> **Note**
>
> If more than 35 zones are created and sent to controller, this event will be registered in the **Event Manager**.

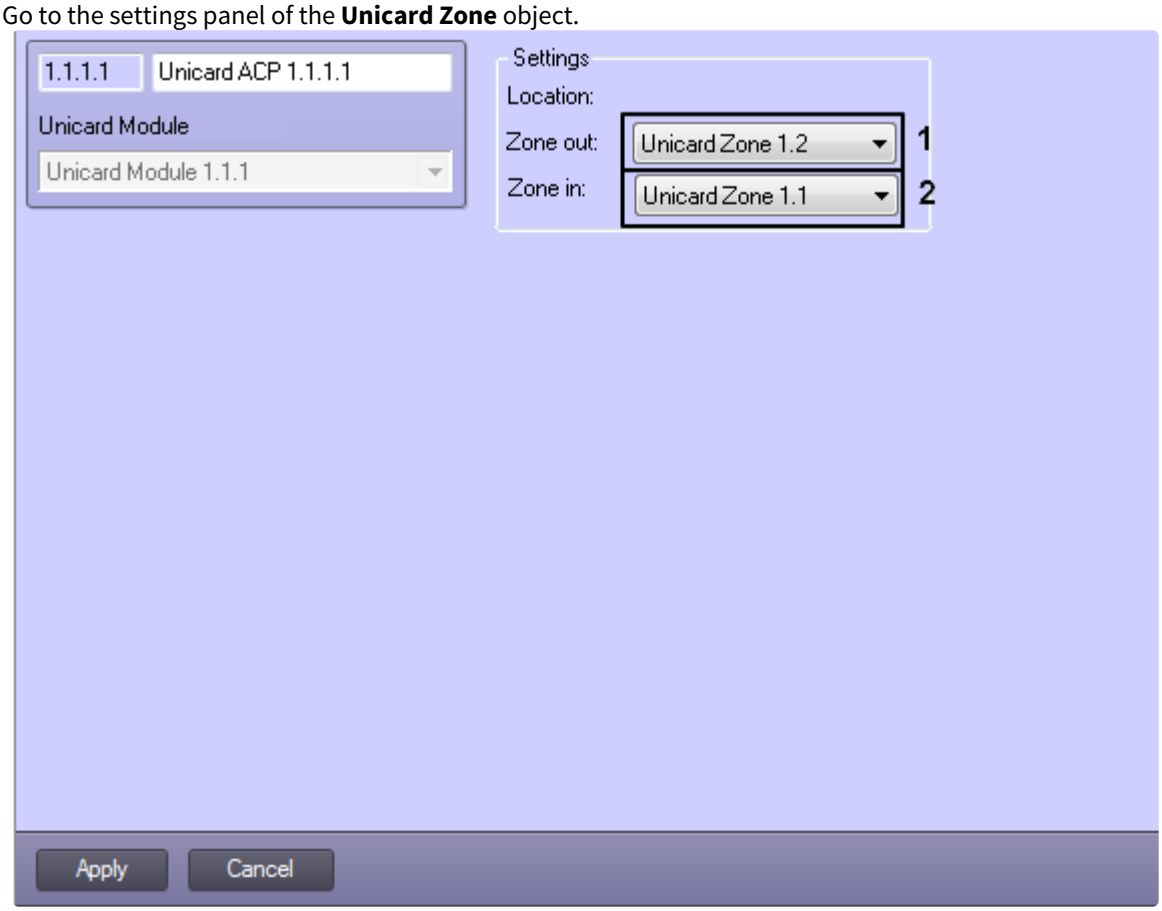
3.5 Configuring the Unicard ACP

Configuring the *Unicard* ACP is performed on the settings panel of the **Unicard ACP** object created on the basis of the **Unicard Module** object on the **Hardware** tab of the **System settings** dialog window



To configure the *Unicard* zone, do the following:

1. Go to the settings panel of the **Unicard Zone** object.

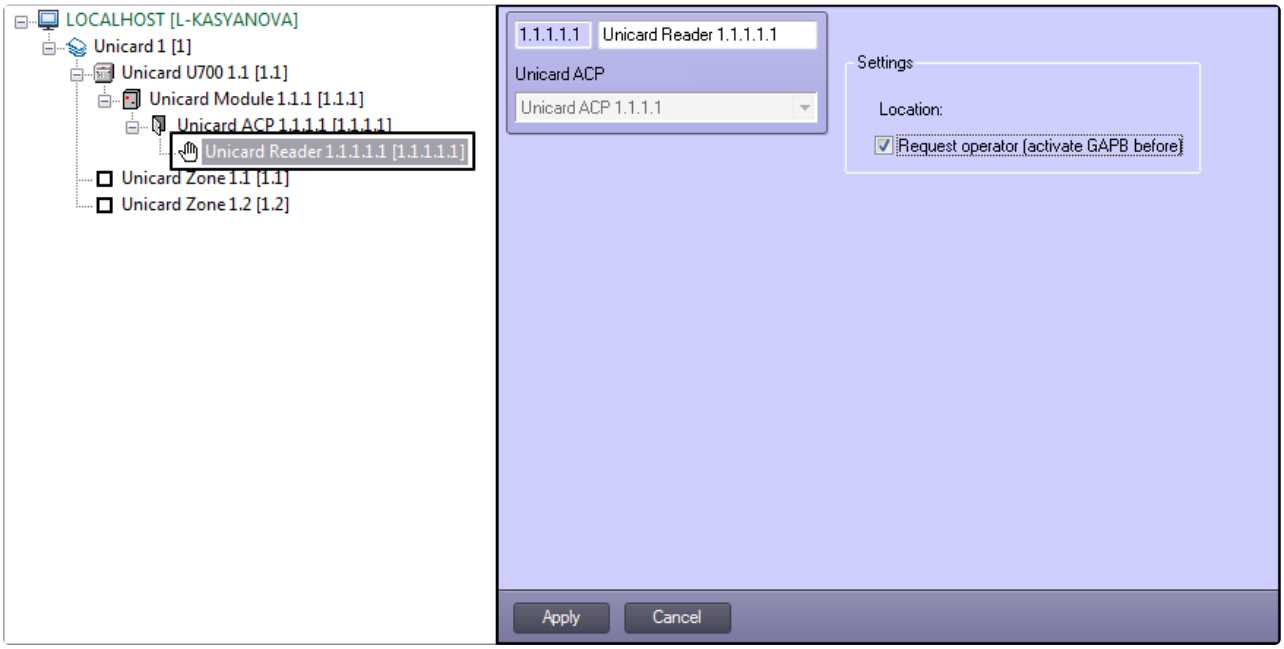


2. From the **Zone out**: drop-down list select the *Unicard* zone located in the site of exit through the reader (**1**).
3. From the **Region in:** drop-down list select *Unicard* zone located in the site of entry through the reader (**2**).
4. Click the **Apply** button to save changes.

Configuring the *Unicard* ACP is completed.

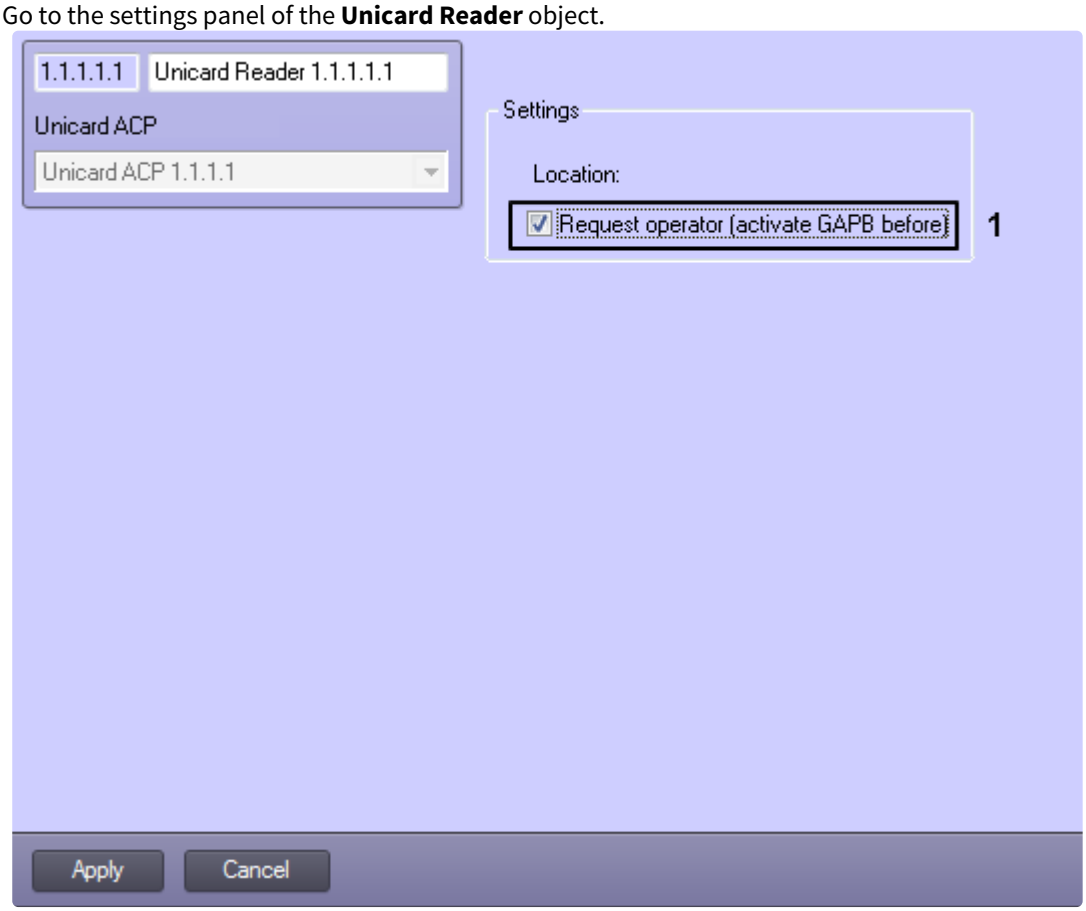
3.6 Configuring the Unicard reader

Configuring the *Unicard* reader is performed on the settings panel of the **Unicard Reader** object created on the basis of the **Unicard ACP** object on the **Hardware** tab of the **System settings** dialog window.



To configure the *Unicard* reader, do the following:

1. Go to the settings panel of the **Unicard Reader** object.



2. Check the **Request operator** box if the data supplied to the reader must be confirmed by the operator.

> **Note**
>
> In order for this functionality to work properly, enable the global antipassback first by checking the **GLOB_APB_ENABLE** box in the settings of the *Unicard* controller (see Configuring the Unicard controller).

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

Configuring the *Unicard* reader is completed.

4 Working with the Unicard integration module

4.1 General information about working with the Unicard Module

The following interface objects are used to work with the *Unicard* integration module:

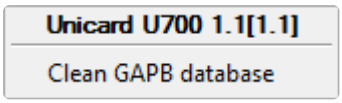
1. **Map**.
2. **Event Log.**

Information about configuring these interface objects is presented in Axxon PSIM Software Package. Administrator's Guide.

Operation of interface objects is given in details in Axxon PSIM Software Package. Operator's Guide.

4.2 Working with the Unicard controller

Working with the *Unicard* controller is performed using the functional menu of the **Unicard U700** object in the **Map** interface window.

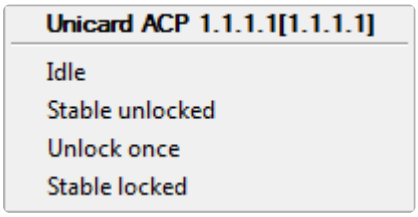


The commands of the context menu are described in the table below.

Command	Description
Clean GAPB database	Deletes all entries from the global antipassback database

4.3 Working with the Unicard access control point

Working with the *Unicard* access control point is performed using the functional menu of the **Unicard ACP** object on the **Map** interface window.



The commands of the context menu are described in the table.

Command	Description
Idle	Normal operation mode
Stable unlocked	Switches access control point to permanent unlocking mode

Command	Description
Unlock once	Unlocks access control point
Stable locked	Switches access control point to permanent locking mode

4.4 Working with the Unicard reader

Working with the *Unicard* reader is performed using the functional menu of the **Unicard Reader** object in the **Map** interface window.

The commands of the context menu are described in the table.

Command	Description
Unlock once	Unlocks access control point