



Castle Integration Module Configuration
and Operation Manual

1. List of terms used in Castle Integration Module Configuration and Operation Manual	3
2. Introduction into Castle Integration Module Configuration and Operation Manual	3
3. Supported hardware and licensing of the Castle integration module	4
4. Configuring Castle integration module	4
4.1 Configuration procedure for Castle integration module	5
4.2 Configuring interaction between ACFA Intellect and Castle server	5
4.3 Configuring user access cards in the Castle integration module	5
4.4 Synchronization of Castle ACS and Intellect ACFA configurations	6
4.5 Configuring Castle ACS Access points	7
4.6 Configuring Castle ACS outputs	8
4.7 Configuring of access partition for entrance and exit	9
5. Working with Castle integration module	10
5.1 General information about how to use Castle integration module	10
5.2 Managing Castle access point	10
5.3 Managing Castle output	11

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

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

Castle server - computer with installed *Castle* 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.

Intellect Server – computer with installed *Intellect* software (**Server** configuration).

Introduction into Castle Integration Module Configuration and Operation Manual

On the page:

- [Purpose of the Document](#)
- [General information about Castle integration module](#)

Purpose of the Document

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

The guide provides:

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

General information about Castle integration module

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

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

Note.

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

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

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

Supported hardware and licensing of the Castle integration module

Manufacturer	«PromAutomatica Service», 603001, Nizhny Novgorod, Chernigovskaya str., 17-A
Integration type	Soft-soft
Equipment connection	RS-232, USB, Ethernet

Supported equipment

Equipment	Purpose	Feature
EP4	Access controller	7000 keys 500 time zones 40000 events Connection interface: Ethernet Readers interface: Wiegand-26, Dallas Touch Memory
EP2	Access controller	7000 keys 500 time zones 40000 events Connection interface: Ethernet Readers interface: Wiegand-26, Dallas Touch Memory
PRO4	Access controller	7000 keys 500 time zones 40000 events Connection interface: RS-485 Readers interface: Wiegand-26, Dallas Touch Memory
EP	Access controller	7000 keys 500 time zones 40000 events Connection interface: Ethernet Readers interface: Wiegand-26, Dallas Touch Memory
PRO	Access controller	7000 keys 500 time zones 40000 events Connection interface: RS-485 Readers interface: Wiegand-26, Dallas Touch Memory
ES	Access controller	96000 keys 30000 time zones 400000 events Connection interface: Ethernet Readers interface: Wiegand-26, Dallas Touch Memory
RS	Access controller	96000 keys 30000 time zones 400000 events Connection interface: RS-485 Readers interface: Wiegand-26, Dallas Touch Memory

Protection

1 IP-address (Castle Server). Castle Server requires the Hasp protection key.

Configuring Castle integration module

Configuration procedure for Castle integration module

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

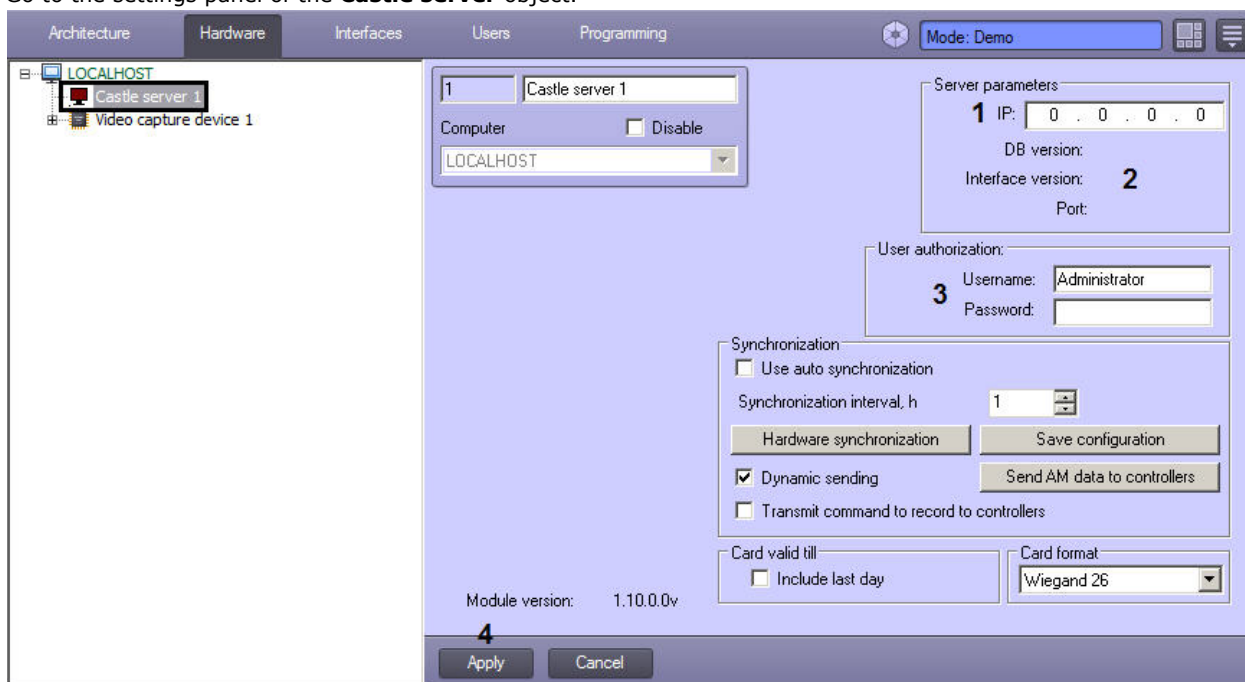
1. Configure interaction between *ACFA Intellect* and *Castle* server;
2. Synchronize *Castle ACS* and *Intellect ACFA* configurations;
3. Configure *Castle ACS* access points.

Configuring interaction between ACFA Intellect and Castle server

Interaction between *ACFA Intellect* and *Castle* server is configured on the settings panel of the **Castle 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 *Castle* server do the following:

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



2. Specify the *Castle* server IP address in the **IP** field (1).

Note.

The following information is displayed in the **Server parameters** group (2):

1. Version of *Castle ACS* database (the **DB version** field);
2. Version of *Castle* server – Client data exchange protocol (the **Interface version** field);
3. Port used for *Castle* server-Client connection (the **Port** field).

Intellect Server is the Client in this case.

3. In the **User authorization** group specify the username (the **Username** field) and password (the **Password** field) used to login to the *Castle* server (3).

Note.

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

4. Click the **Apply** button to save all changes (4).

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

Configuring user access cards in the Castle 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](#)).

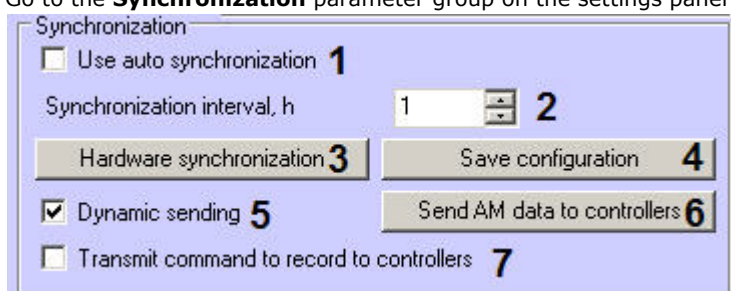
If *Castle* integration module is to grant access on the specified day, set the **Include last day** checkbox on the **Castle server** object settings panel and click **Apply**.



Synchronization of Castle ACS and Intellect ACFA configurations

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

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



2. Set the **Use auto synchronization** checkbox to automatically rewrite all access parameters to *Castle* Server with a specified interval (1). The synchronization is only performed if a change occurred in users' parameters between synchronization intervals. If there were no changes, the configuration is not rewritten.
3. In the **Synchronization interval, h** field, set the period (in hours) of parameters synchronization (2).
4. To read *Castle* ACS access points configuration stored on *Castle* server click the **Hardware synchronization** button (3).
5. To send *ACFA Intellect* configuration to *Castle* server click the **Save configuration** button (4).

Attention!

This action is to be performed after configuring interaction between *Intellect* and *Castle* servers.

6. Set the **Dynamic sending** checkbox to enable constant connection between *Intellect* and *Castle* servers (5).

Attention!

The **Dynamic sending** checkbox is always to be checked for proper operation of *Castle* integration module. If it is not, use **Save configuration** or **Send AM data to controllers** every time you change hardware or user parameters correspondingly.

7. Click **Send AM data to controllers** to send configuration of *ACFA Intellect* users to *Castle* controllers (6).
8. Set the **Transmit command to record to controllers** checkbox to enable automatic sending of *ACFA Intellect* users configuration to controllers after clicking **Save configuration** (7).

Note.

If the **Transmit command to record to controllers** checkbox is not set, click **Send AM data to controllers** (6) every time after clicking **Save configuration** (4).

9. Click the **Apply** button.

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:

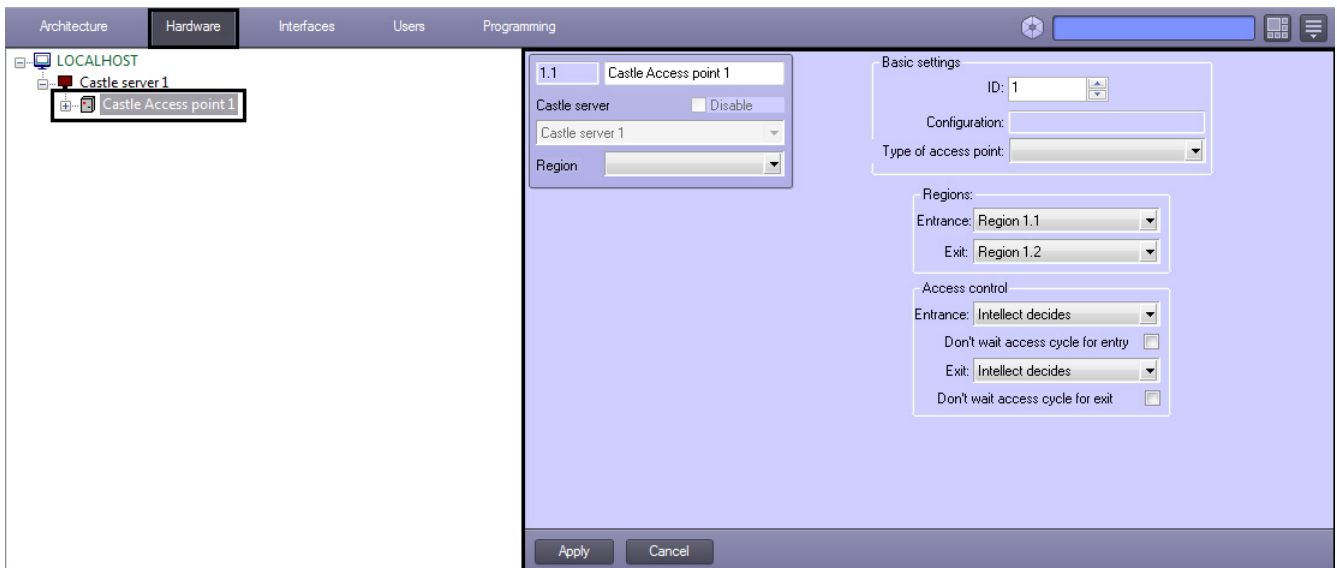
1. the card issue date, which has not yet arrived;
2. the card expiration date that has already passed;
3. access levels that are unrelated to the the controllers of this Castle server;
4. or the **User locked** property

are not written to the controller.

Castle ACS and Intellect ACFA configurations are now synchronized.

Configuring Castle ACS Access points

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



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

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

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

2. Access point configuration (2).

Note.

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

3. Access control mode (3).

Castle 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):
 1. 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.

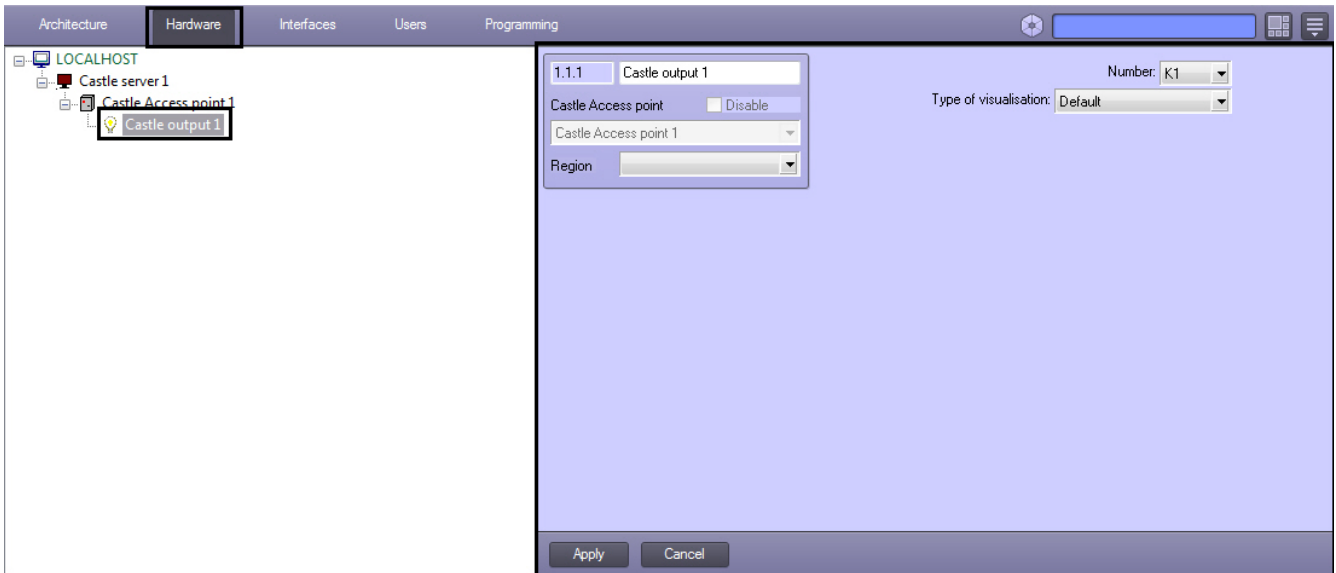
To process the request operator is to create a **Photo ID** interface object and configure it for the **Operator's query (Access granted)** event. For more information about this object and its functions, please refer to *Photo ID User Guide*.

2. 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.
6. Repeat steps 1-9 for all required *Castle ACS* access points.

Castle ACS access points are now configured.

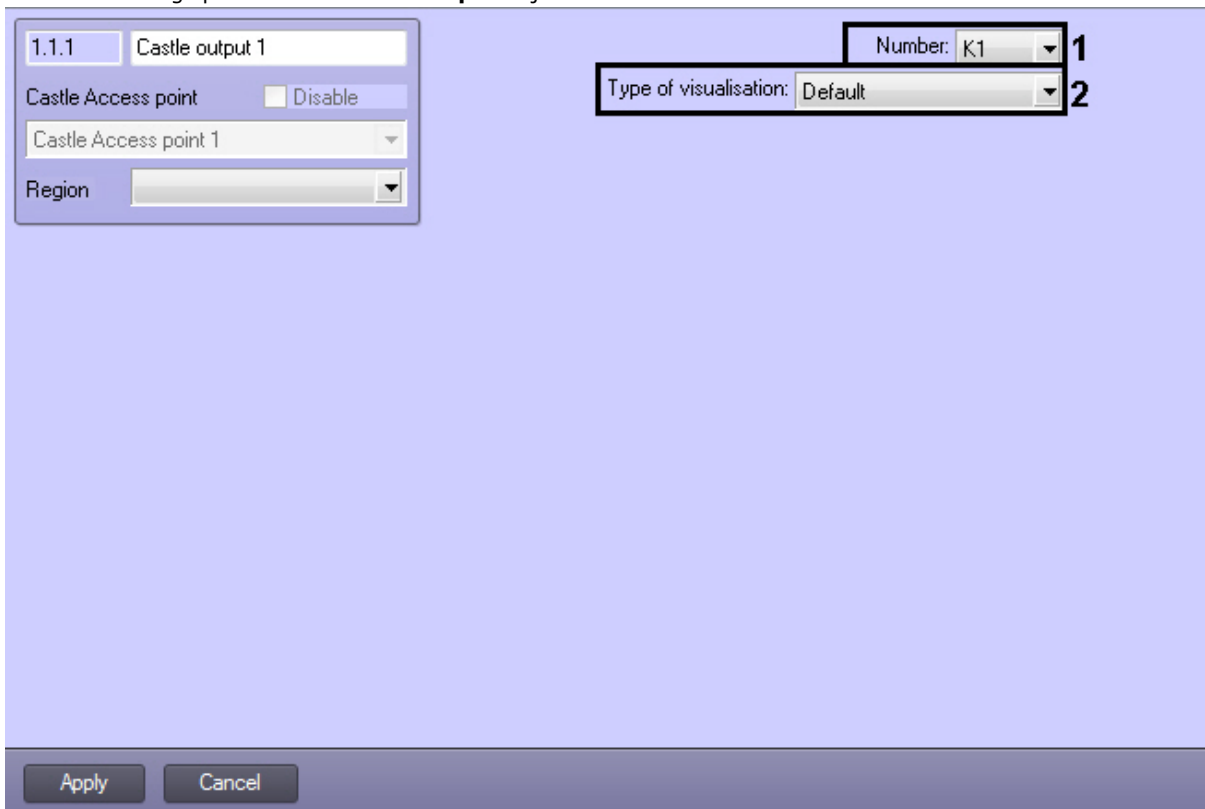
Configuring Castle ACS outputs

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



Configuring *Castle ACS* output is performed as follows:

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

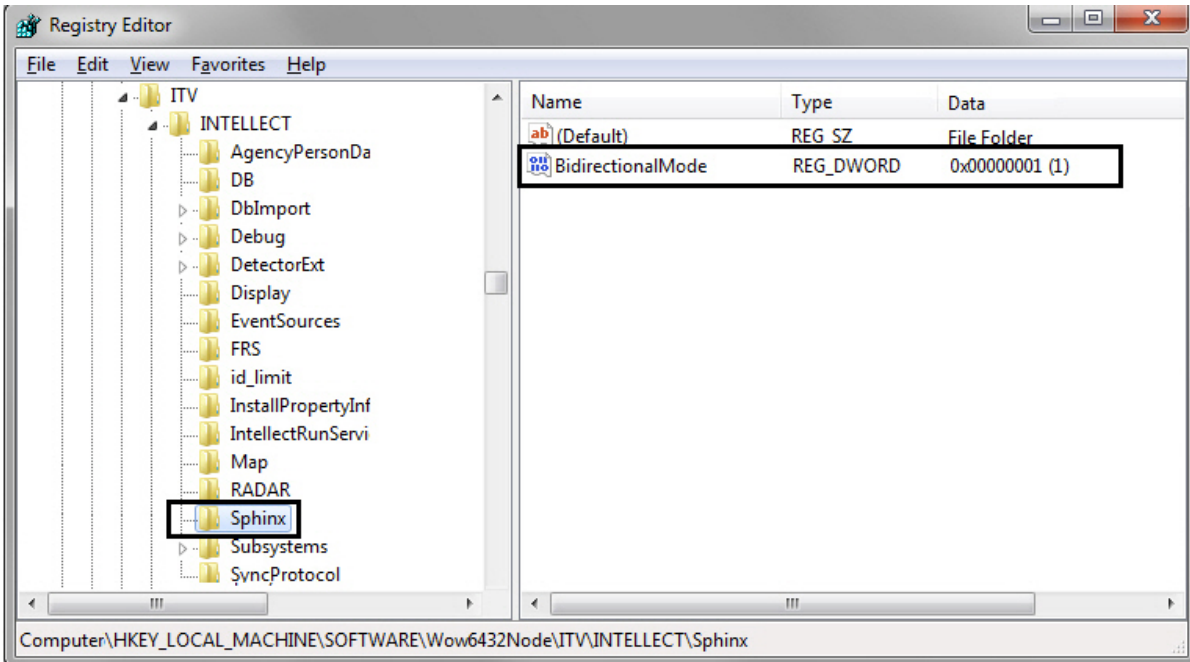


2. The output number is automatically specified when reading *Castle ACS* configuration (1).
3. From the **Type of visualisation** drop-down list select the corresponding set of icons for the output (2).
4. Click **Apply**.

Castle ACS outputs are now configured.

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 applied 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).

Working with Castle integration module

General information about how to use Castle integration module

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

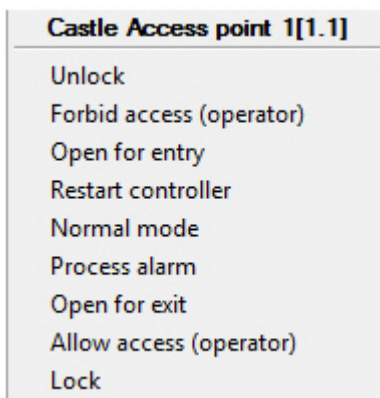
- **Card;**
- **Event Viewer.**

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 Castle access point

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



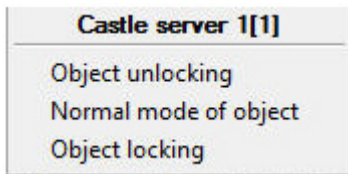
Note.

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

Description of feature menu of the **Castle** access point object is given 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 **Castle server** object.

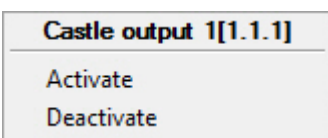


Description of feature menu of the **Castle** server object is given in the table.

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

Managing Castle output

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



Description of feature menu of the **Castle** output object is given in the table.

Menu command	Functionality
Activate	Output activation
Deactivate	Output deactivation