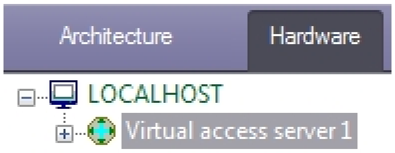
Configuring virtual access point while face recognition

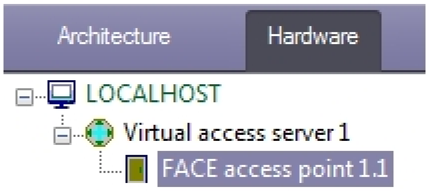
Organizing of virtual access point while face recognition allows fixing the access (ACCESS_IN event) while recognition a face which is stored in the database (see the *Face-Intellect software package. Administrator's Guide* in AxxonSoft documentation repository).

To organize the virtual access point while face recognition, do the following:

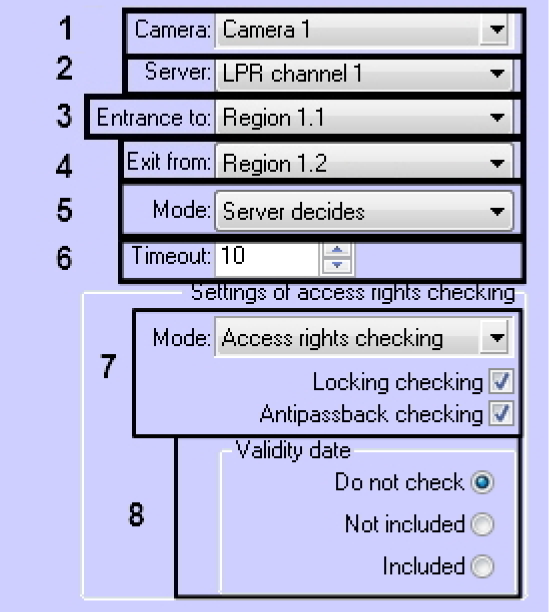
1. Create the **Virtual access server** object on the basis of the **Computer** object in the **Hardware** tab of the **System settings** dialog window.



2. Create the **FACE Access point** object on the basis of the **Virtual Access Server** object.



3. Configure the access point:
   a. Select camera which performs the face recognition. Camera must work with the face recognition server (**1**).



1 Camera: Camera 1
2 Server: LPR channel 1
3 Entrance to: Region 1.1
4 Exit from: Region 1.2
5 Mode: Server decides
6 Timeout: 10

Settings of access rights checking

7 Mode: Access rights checking
Locking checking ☑
Antipassback checking ☑

8 Validity date
Do not check ●
Not included ○
Included ○

   b. Select the face recognition server on the basis of which the access point is to be organized (**2**).
   c. From the **Entrance to:** drop-down list select the **Region** object corresponding to the area in which access is performed (**3**).
   d. From the **Exit from:** drop-down list select the **Region** object corresponding to the area from which the exit is performed (**4**).
   e. From the **Mode**: select the access granting mode - automatically (this includes the use of a script that controls the door sensors) or by approval from an operator, who has to click the button in the **Event Manager**. See Working with the Event manager module (**4**).
   f. In the **Timeout**: specify the access granting timeout in seconds (**5**).

> **Note**
>
> All the other requests from the face recognition server will be ignored within the specified timeout.

g. Select the **Only recognition** mode if it’s required to take a decision about access granting only with reference to faces recognition (**4**). Select the **Access rights checking** mode and set checkboxes corresponding to checking which are to be performed if it’s required to check the user access level which face was recognized, time zones of this access level and perform additional checking.
h. **Locking checking** – access will not granted in case of user is locked.
Antipassback checking – antipassback checking through the access point.

> **Note.**
>
> Checking of access level and its time zones will be always performed in the **Access rights checking** mode.

i. In the **Validity date** section select a radio button corresponding to the settings of checking the card validity date specified in the *Visitor Management System* interface object (**6**).
Do not check – checking of card validity date is not required.
Not included – do not include the card expire date to checking.
Included – include the card expire date to checking.

4. Click **Apply** to save changes.

Organizing of virtual access point while face recognition is performed.