Virtual Access Server Integration Module Configuration and Operation Manual

ACFA PSIM 1.1

Last update 05/03/2024

Table of Contents

1 Introduction into Virtual Access Server Integration Module Configuration and Operation Manual

On the page:

1.1 Purpose of the Document

Configuration and operation manual for Virtual Access Server integration module is a reference and information guide meant for *ACFA PSIM*, *Auto PSIM* and *Face PSIM*.

The guide provides:

1. General information about *Virtual Access Server* module.
2. Information about how to configure *Virtual Access Server* module.
3. Information about how to work with *Virtual Access Server* module.

1.2 General information about Virtual Access Server module

Virtual Access Server module is the component of *ACFA PSIM*. It is designed for combining the work of *Auto PSIM* and *Face PSIM* with *ACFA PSIM* by creating virtual access points (without ACS hardware).

The *Virtual Access Server* module allows you to perform the following:

1. Create the virtual access points (without ACS hardware) on the basis of the face recognition (see Configuring virtual access point during face recognition) and license plates recognition (see Configuring virtual access point during vehicle license plate recognition).
2. In ACS, perform the two-factor verification in the Access card + Face mode (see Two-step verification management).
3. Monitor the temperature of a face recognized using *Face PSIM* and a thermal camera (see Face temperature monitoring and control).
4. Perform different actions in the system using scripts or macros for various events (for example, open or close a barrier, block an access point, etc.) (see *Axxon PSIM* software package. Guide for creating scripts (programming)).

The documentation on *Auto PSIM*, *Face PSIM* and *Axxon PSIM* basic access software packages is located here.

2 Licensing policy for Virtual Access Server

The module is not licensed (i.e. free to use).

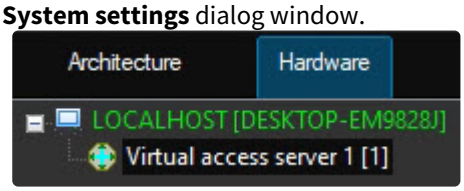
3 Configuring Virtual Access Server integration module

3.1 Configuring virtual access point during vehicle license plate recognition

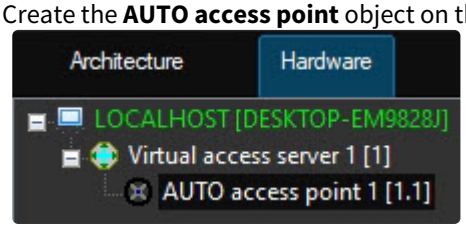
Organizing of virtual access point during vehicle license plate recognition allows fixing the access (ACCESS_IN event) while recognition the license plate which is stored in the database (in user settings specified in the *Access Manager* module).

To configure the virtual access point during vehicle license plate recognition, do the following:

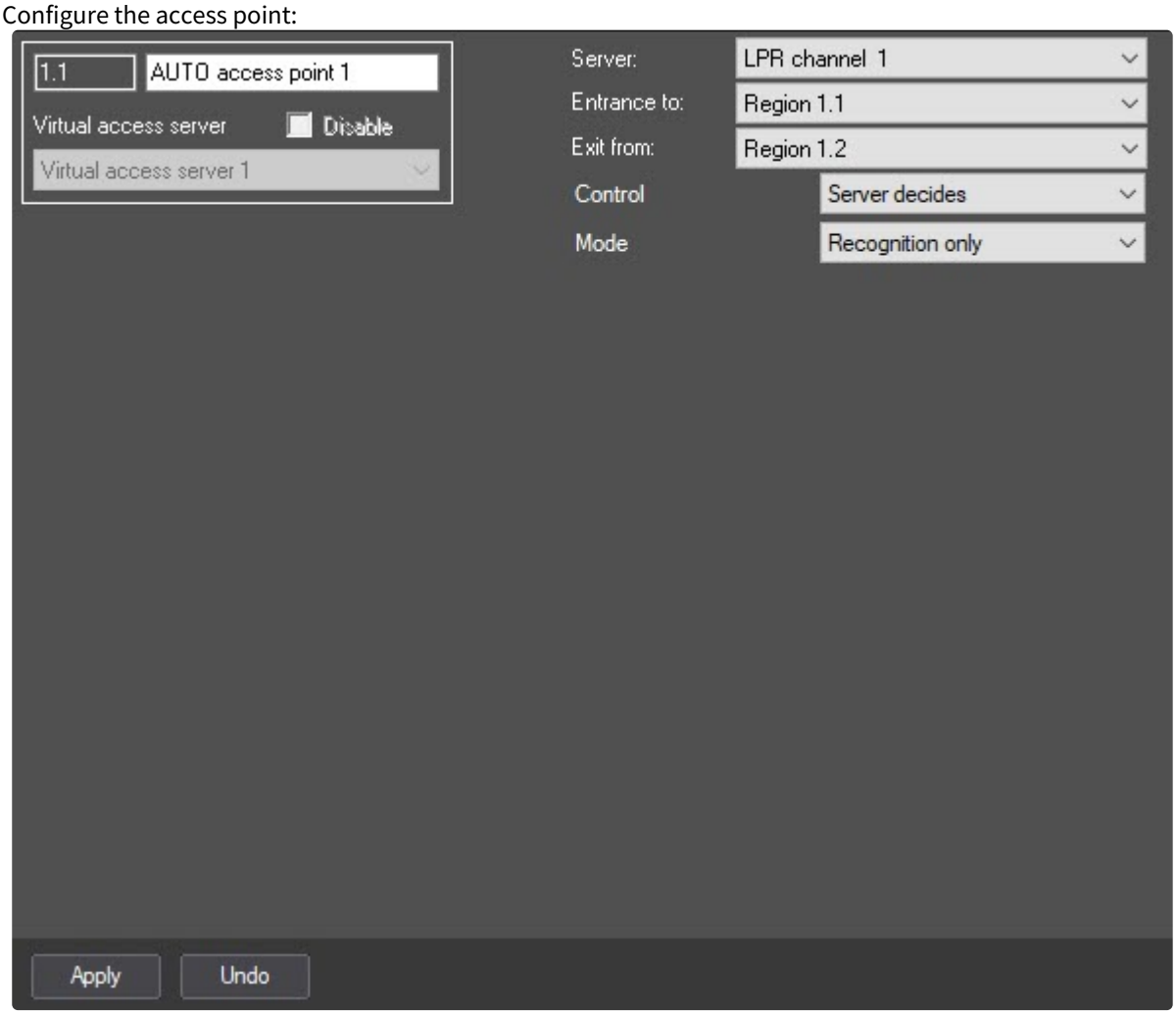
1. Create the **Virtual access server** object on the basis of the **Computer** object in the **Hardware** tab of the **System settings** dialog window.



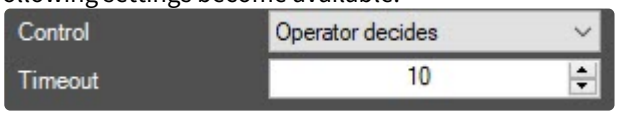
2. Create the **AUTO access point** object on the basis of the **Virtual access server** object.



3. Configure the access point:

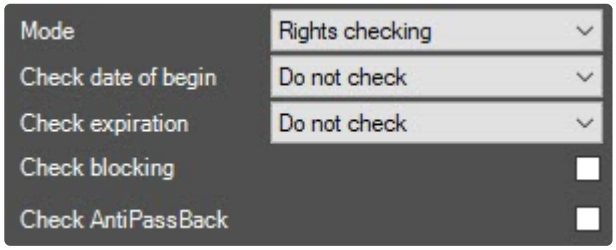


4. From the **Server** drop-down list select the LPR channel on the basis of which the access point is to be organized .
5. From the **Entrance to** drop-down list select the **Region** object corresponding to the area in which access is performed.
6. From the **Exit from** drop-down list select the **Region** object corresponding to the area from which the exit is performed.
7. From the **Control** drop-down list select the access granting mode:
   - **Server decides** – the server makes the decision for access granting or refusal (this includes the use of a script).
   - **Operator decides** – the operator makes the decision for access granting or refusal using the *Event Manager* module (see Working with the Event manager module). If this mode is selected, the following settings become available:



     - **Timeout** – sets the time interval in seconds to wait for access confirmation by the operator. All the other requests from the Face recognition server will be ignored within the specified timeout.
8. If the **Server decides** access granting mode was selected, then from the **Mode** drop-down list select the access rights checking mode:

- **Recognition only** – the server makes the access granting decision based only on license plate recognition.
- **Rights checking** – the server makes the access granting decision after successful license plate recognition and successful verification of the access rights of the user who owns the vehicle (access level, time zones, blocking, antipassback). If this mode is selected, the following settings become available:



  - **Check date of begin** and **Check expiration** - sets the mode of checking the access card validity:
    - **Do not check** – do not check the start or expiration date of the card.
    - **Do not include** – do not include the start or expiration date of the card in the check.
    - **Include** – include the start or expiration date of the card in the check.
  - **Check blocking** – set the checkbox to check if the user is blocked.
  - **Check AntiPassBack** – set the checkbox to control double pass.

9. Click **Apply** to save the changes.

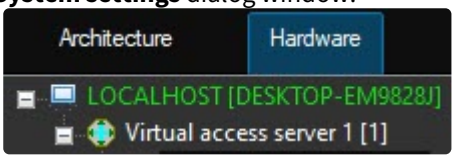
Organizing of virtual access point during vehicle license plate recognition is performed.

3.2 Configuring virtual access point during face recognition

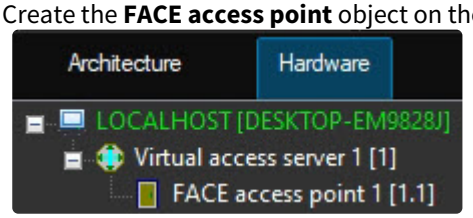
Organizing of virtual access point while face recognition allows fixing the access (ACCESS_IN event) while recognition a face which is stored in the database (see the *Face PSIM software package. Administrator's Guide* in AxxonSoft documentation repository).

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

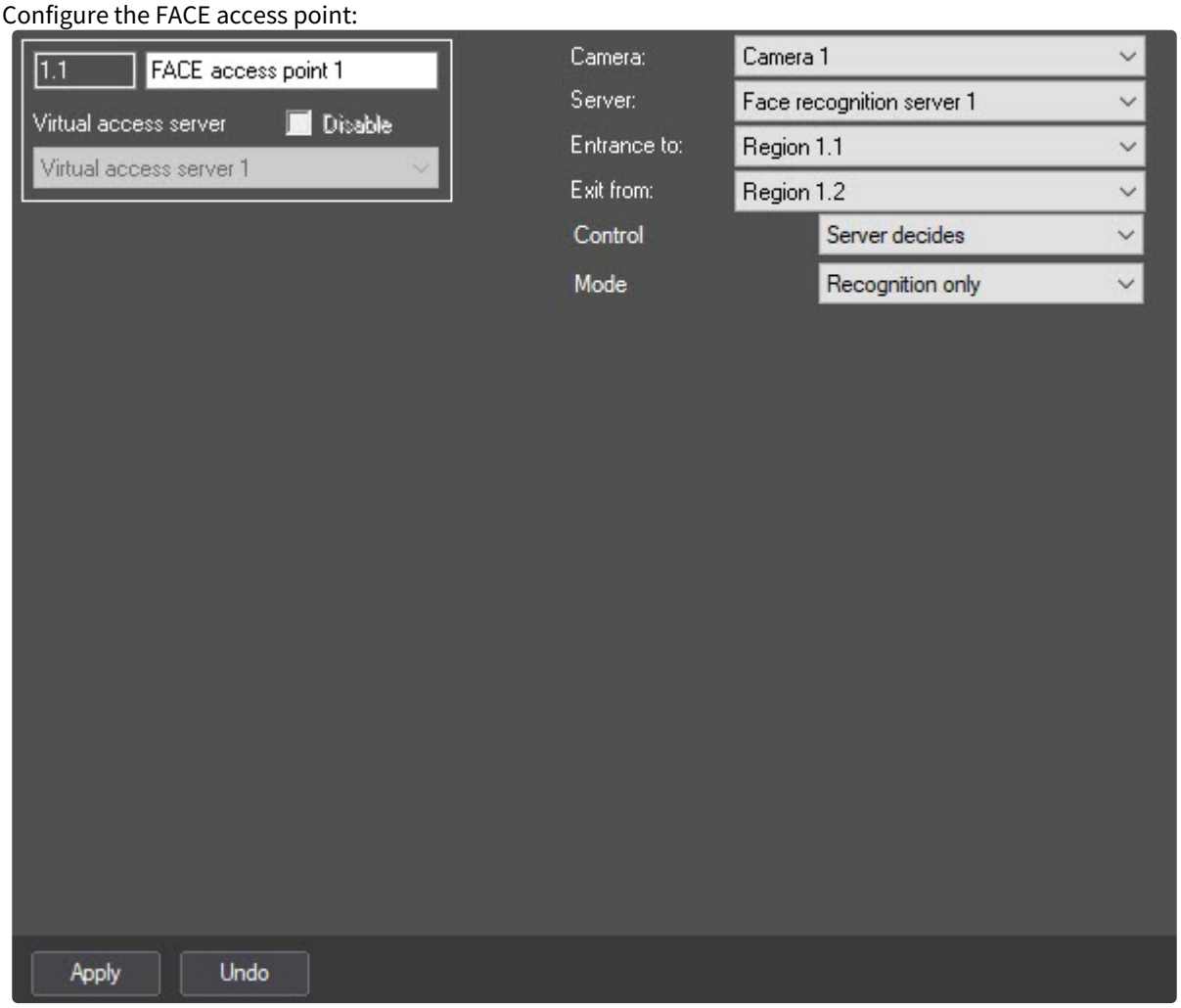
1. Create the **Virtual access server** object on the basis of the **Computer** object in the **Hardware** tab of the **System settings** dialog window.



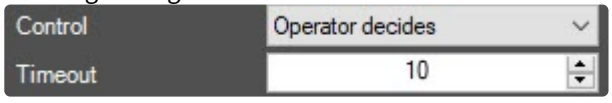
2. Create the **FACE access point** object on the basis of the **Virtual access server** object.



3. Configure the FACE access point:

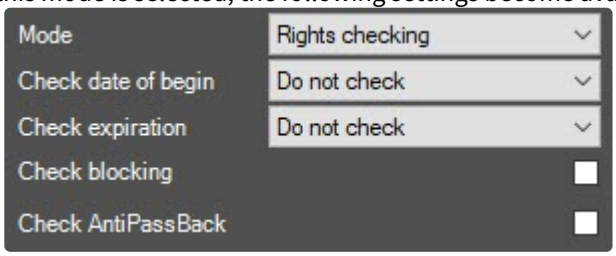


4. Select camera which performs the face recognition. Camera must work with the face recognition server.
5. Select the face recognition server on the basis of which the access point is to be organized.
6. From the **Entrance to** drop-down list select the **Region** object corresponding to the area in which access is performed.
7. From the **Exit from** drop-down list select the **Region** object corresponding to the area from which the exit is performed.
8. From the **Control** drop-down list select the access granting mode:
   - **Server decides** – the server makes the decision for access granting or refusal (this includes the use of a script).
   - **Operator decides** – the operator makes the decision for access granting or refusal using the *Event Manager* module (see Working with the Event manager module). If this mode is selected, the following settings become available:



     - **Timeout** – sets the time interval in seconds to wait for access confirmation by the operator. All the other requests from the Face recognition server will be ignored within the specified timeout.
9. If the **Server decides** access granting mode was selected, then from the **Mode** drop-down list select the access rights checking mode:
   - **Recognition only** – the server makes the access granting decision based only on face recognition.

- **Rights checking** – the server makes the access granting decision after successful face recognition and successful verification of user access rights (access level, time zones, blocking, antipassback). If this mode is selected, the following settings become available:



  - **Check date of begin** and **Check expiration** - sets the mode of checking the access card validity:
    - **Do not check** – do not check the start or expiration date of the card.
    - **Do not include** – do not include the start or expiration date of the card in the check.
    - **Include** – include the start or expiration date of the card in the check.
  - **Check blocking** – set the checkbox to check if the user is blocked.
  - **Check AntiPassBack** – set the checkbox to control double pass.
- **Temperature monitoring** – if it is required to only monitor the face temperature (see Face temperature monitoring and control).
- **Temperature control** – if it is required to only control the face temperature threshold exceeding (see Face temperature monitoring and control). If this mode is selected, the following settings become available:

  - **Lock user on temp. alarm** – set the checkbox if it is necessary to automatically block the user when the temperature is exceeded (the **User blocked – Yes** parameter will be set in the *Access Manager* module). If the joint operation with the ACS and dynamics are enabled, then such a user will be automatically removed from the controller and therefore will be denied access.

10. Click **Apply** button to save changes.

Organizing of virtual access point while face recognition is performed.

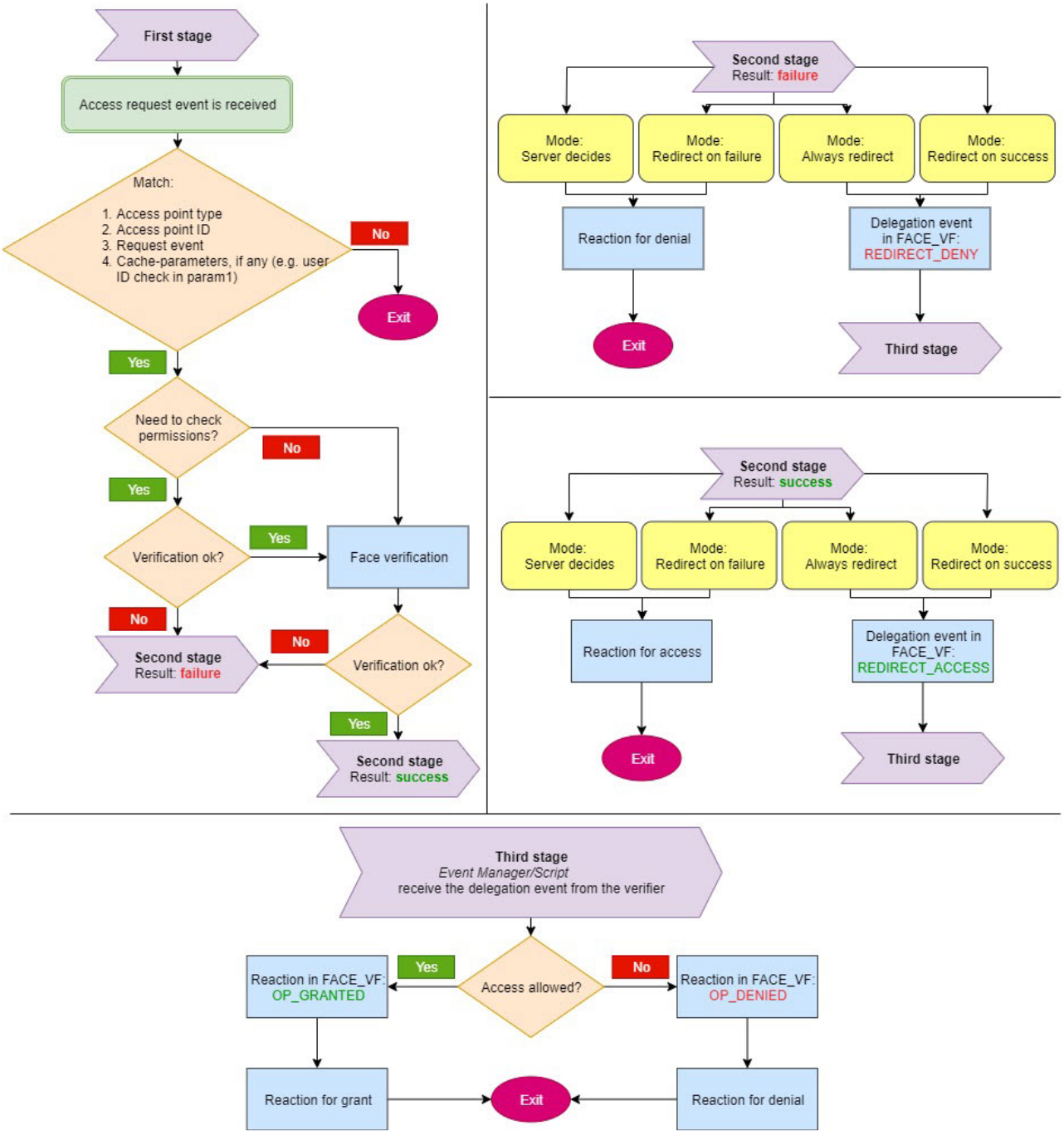
3.3 Two-step verification management

3.3.1 General information about two-step verification

In ACS systems, the two-step verification allows to grant the access only after a successful verification of both the user's access card and the user' face.

> **Attention!**
>
> In this mode, the user's access card must always be applied first, and only then the user's face will be verified.

Two-step verification is performed in several stages. The block diagram of the two-step verification operation is presented below.



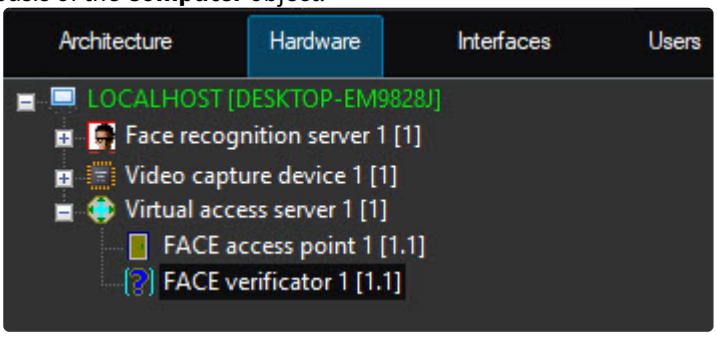
3.3.2 Configuring the two-step verification

Two-step verification includes configuration on the *ACFA* side and on the *Face PSIM* side.

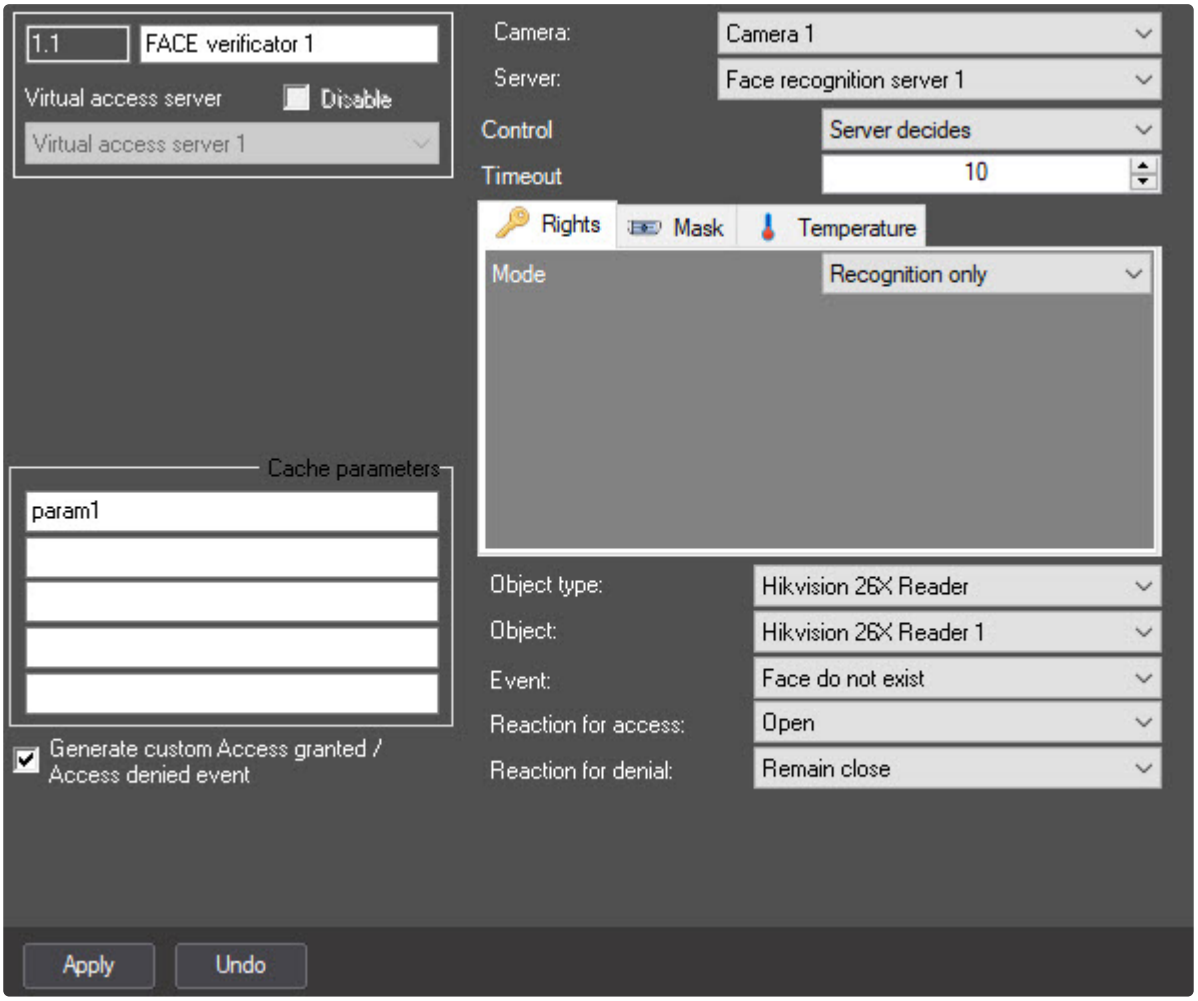
Configuring the two-step verification on the ACFA side

To configure two-step verification, do the following:

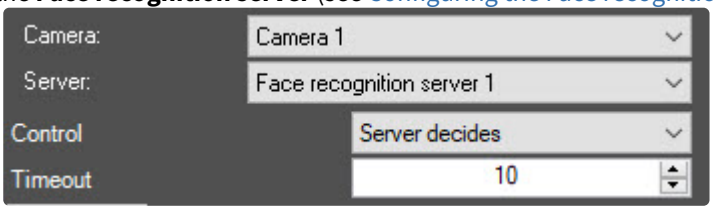
1. On the **Hardware** tab of the **System settings** dialog window, create the **Virtual access server** object on the basis of the **Computer** object.



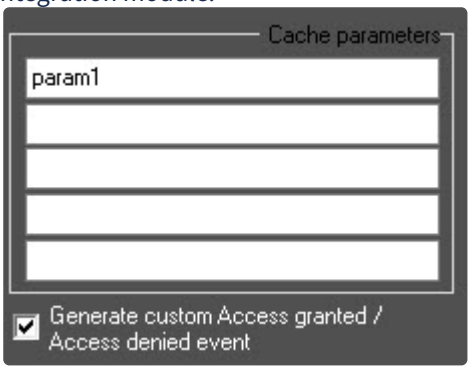
2. Create the **FACE verificator** object on the basis of the **Virtual access server** object, and go to its settings panel.



3. From the **Camera** drop-down list, select the camera that captures faces. The camera must work as a part of the **Face recognition server** (see Configuring the Face recognition server object).

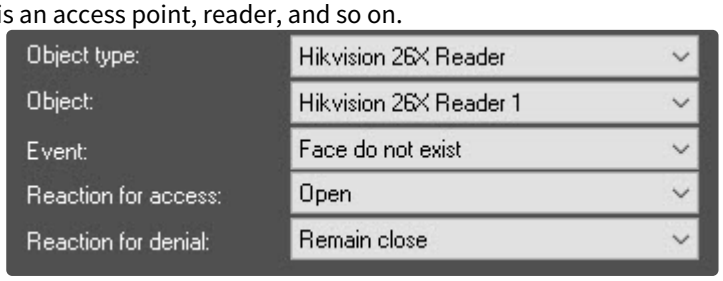


4. From the **Server** drop-down list, select the **Face recognition server**.
5. From the **Control** drop-down list, select the access granting mode:
   - **Server decides**—depending on the result of the access rights check or face verification, the access is granted or denied.
   - **Redirect always**—regardless of the result of the second stage, the verifier redirects its solution to the external verifier (*Event Manager/Script)*. Depending on the result, the access is granted or denied.
   - **Redirect if decline**—if the first stage is successful, then this mode is similar to the **Server decides** mode. If the first stage is failed, then the solution is delegated to the external verifier.
   - **Redirect if success**—if the first stage is failed, then this mode is similar to the **Server decides** mode. If the first stage is successful, then the solution is delegated to the external verifier.
6. In the **Timeout** field, enter the time in seconds after which the connection with the **Face recognition server** is terminated.
7. If necessary, in the fields of the **Cache parameters** group, set the parameters that are specific for each ACS integration module.

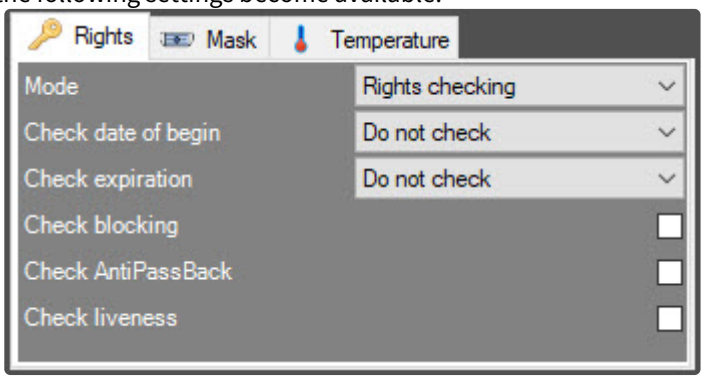


> **Note**
>
> For example, in the *PERCo-S-20 v.2* integration module, each request to the operator is accompanied by the **request_id** parameter. This parameter must be returned when confirming access, otherwise the command will be ignored. For the *Hikvision* ACS, such parameter is **param1**.

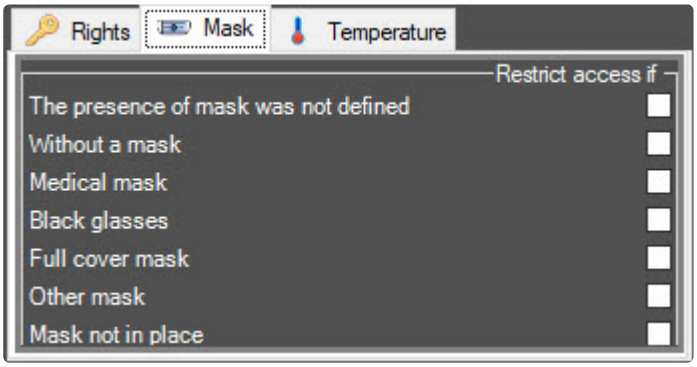
8. Set the **Generate custom Access granted / Access denied event** checkbox if it is necessary that the **FACE verificator** object generates an additional event about granting/denying access, and specifies the reason for the denial. These events can be used to work with scripts or the *Event manager* interface module.
9. From the **Object type** drop-down list, select the type of object that will initiate the face check. Typically, this is an access point, reader, and so on.



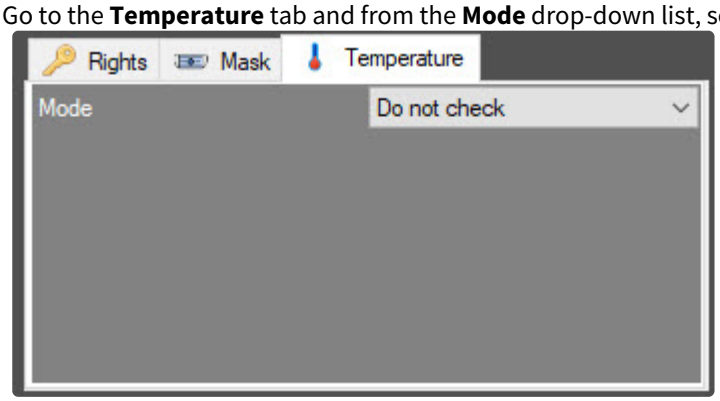
10. From the **Object** drop-down list, select the object of the type specified above.
11. From the **Event** drop-down list, select the event on which the face check will be launched. The list of available events depends on the selected object type.
12. From the **Reaction for access** drop-down list, select the command that will be sent to the initiating object upon the successful face verification. The list of available commands depends on the selected object type.
13. From the **Reaction for denial** drop-down list, select the command that will be sent to the initiating object upon the unsuccessful check/face verification. The list of available commands depends on the selected object type.
14. On the **Rights** tab, from the **Mode** drop-down list, select the access rights checking mode:
    a. **Recognition only**—the server makes the access granting decision based only on face verification.
    b. **Rights checking**—the server makes the access granting decision after successful verification of user access rights (access level, time schedules, blocking, antipassback) and, then, successful face verification. If at the stage of checking access rights, a discrepancy in rights is found, then the device will be prompted to deny access, and face verification will not be started. The access denial event from the **FACE verificator** object will not be displayed in the *Event Viewer*. If this mode is selected, the following settings become available:



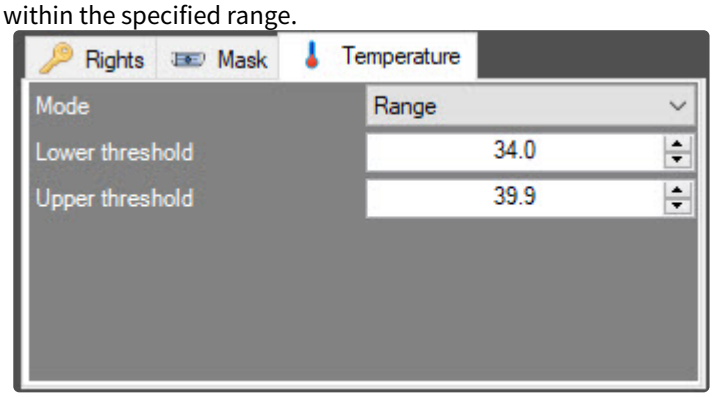
    i. **Check date of begin** and **Check expiration**—sets the mode of checking the access card validity:
        - **Do not check**—do not check the start or expiration date of the card.
        - **Do not include**—do not include the start or expiration date of the card in the check.
        - **Include**—include the start or expiration date of the card in the check.
    ii. **Check blocking**—set the checkbox to check if the user is blocked.
    iii. **Check AntiPassBack**—set the checkbox to control double pass.
    iv. **Check liveness**—set the checkbox to control whether a photo of a person was presented instead of a live person. By default, the checkbox is clear.
15. Go to the **Mask** tab and set the **Restrict access if** checkboxes to deny access in cases marked by the checkboxes. If none of the checkboxes is set in this block of settings, the mask recognition will be ignored.

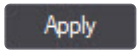


16. Go to the **Temperature** tab and from the **Mode** drop-down list, select one of the options:



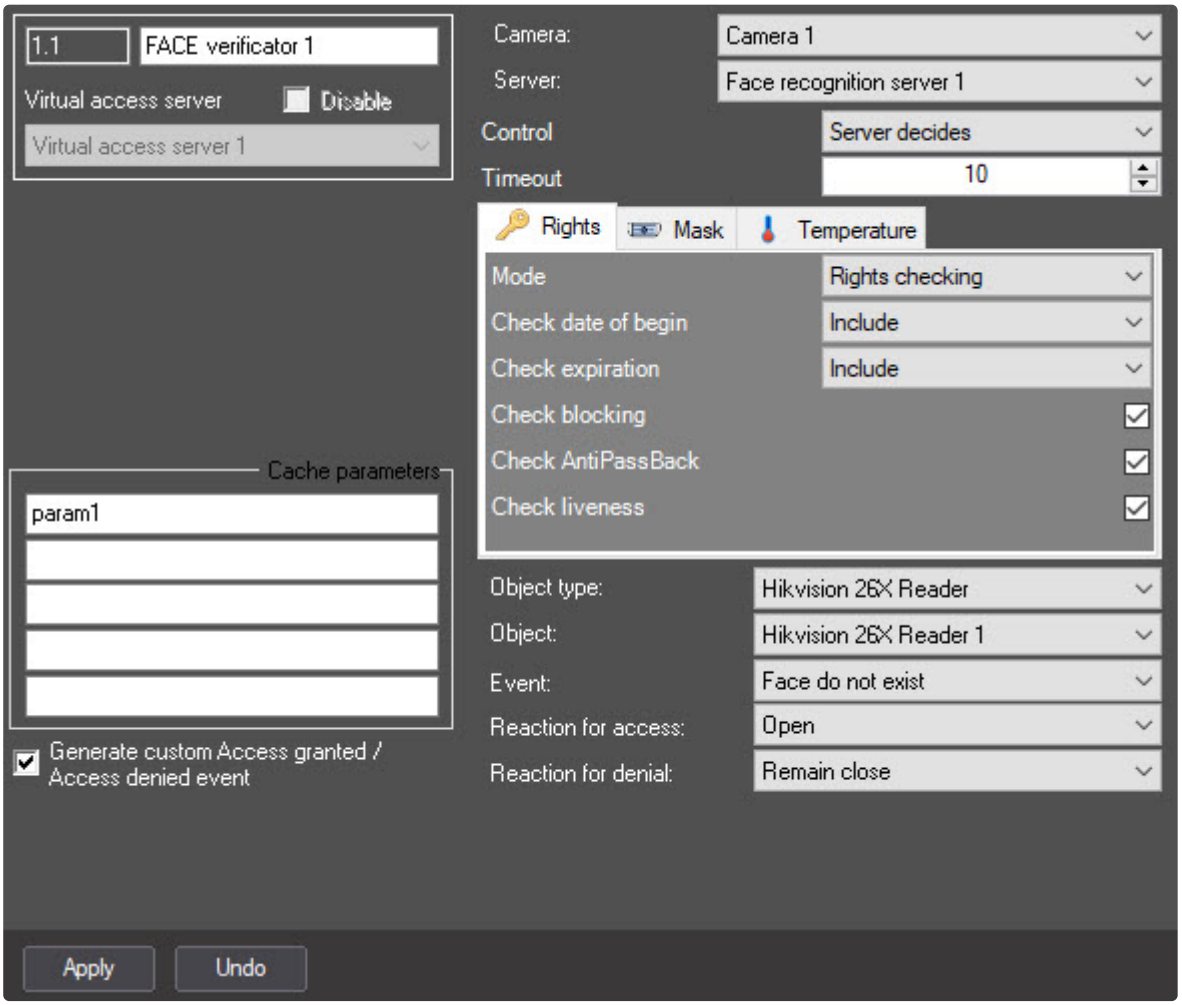
- **Do not control**—regardless of the temperature, the recognized person will be allowed access.
- **Threshold exceeding**—access denied if the temperature threshold set in the **Face recognition server** on the **Analytics** tab is exceeded (for details, see Face recognition server settings panel).
- **Range**—in the **Lower threshold** and **Upper threshold** fields, specify the minimum and maximum allowable temperatures, respectively. Access is allowed if the recognized person's temperature is within the specified range.



17. Click the **Apply** 

button to save the settings.

Example of the two-step verification configured for the *Hikvision* ACS integration module is presented below.



The two-fstep verification on the *ACFA* side is configured.

Configuring the two-step verification on the Face PSIM side

Two-step verification doesn't require the face database.

On the *Face PSIM* side, do the following:

1. On the **Hardware** tab of the **System settings** dialog window, create the **Face recognition server** object on the basis of the **Computer** object.
2. On the basis of the **Face recognition server** object, create the **Recognition channel** and **Tevian recognition module** objects.

The two-step verification on the *Face PSIM* side is configured.

3.4 Face temperature monitoring and control

3.4.1 General information about face temperature monitoring and control

The **Virtual Access Server** software module allows to receive the face temperature, which is measured by the thermal camera on the *Face PSIM* side during the face recognition. The face temperature, for example, can be

displayed on the Operator's monitor using the *Event manager* software module and, in case the specified temperature threshold is exceeded, the access point can be blocked until the alarm is processed by the Operator.

3.4.2 Configuring the face temperature monitoring and control

To configure the face temperature monitoring and control, do the following:

1. Configure *Face PSIM* according to the documentation.

   > Configuring the Face recognition server operation with thermal camera

2. Configure the **FACE access point** object according to the documentation. The required settings are shown below:
   - If it is necessary to only monitor the face temperature (display only), then select **Temperature monitoring** from the **Mode** drop-down list.
   - If it is necessary to control the face temperature threshold exceeding, then select **Temperature control** from the **Mode** drop-down list.

     > **Note**
     >
     > To simultaneously monitor and control the face temperature, it is necessary to create two **FACE access point** objects, and set the temperature monitoring/control mode for each of them.

3. Configure the *Event manager* module according to the documentation. The required settings are shown below:
   a. Create and configure the **Rule of displaying** object for each monitoring/control mode:
      - For the **Type of object** parameter, select **FACE access point**.
      - For the **Template** parameter, select a display template for the temperature monitoring or control, respectively (see step 3.b).
      - On the **Objects** tab, select the appropriate **FACE access point** object for the temperature monitoring or control.
      - On the **Events** tab, if the **Rule of displaying** object is configured for the temperature monitoring, set the checkbox for the **Face recognized (temperature log)** event. If the **Rule of displaying** object is configured for the temperature control, then set the checkbox for the **Face with high temperature recognized** event.

   b. Create and configure the **Template of displaying** object for each monitoring/control mode:

      > Database field object properties

      i. To display the name of the event for which the *Event manager* is configured, add the **Database field** object and specify the following value in the **Unusual** parameter:

      ```
      rule_service_action_name
      ```

      ii. To display the full name, add several **Database field** objects and specify the value from the database (First name, Surname, Patronymic) in the **Predefined** field, or add only one **Database field** object, and specify the following value in the **Unusual** parameter:

      ```
      {param0}
      ```

      iii. To display the date and time when the face and temperature were recognized, add the **Database field** object and specify the following value in the **Unusual** parameter:

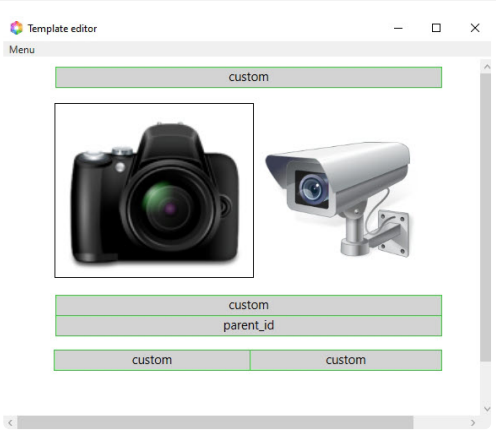
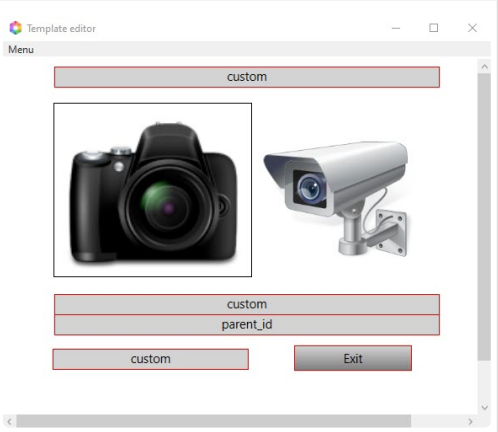
```
{date} {time}
```

iv. To display the temperature received from the thermal camera, add the **Database field** object and specify the following value in the **Unusual** parameter:

```
{temperature}
```

> **Note**
>
> For example, for a temperature control template, you can specify the following in the **Unusual** parameter:
>
> ```
> Attention! High temperature: {temperature} °C {\n} Door
> blocked.
> ```

v. The examples of display templates are shown below.

Display template for the temperature monitoring	**Display template for the temperature control**
	

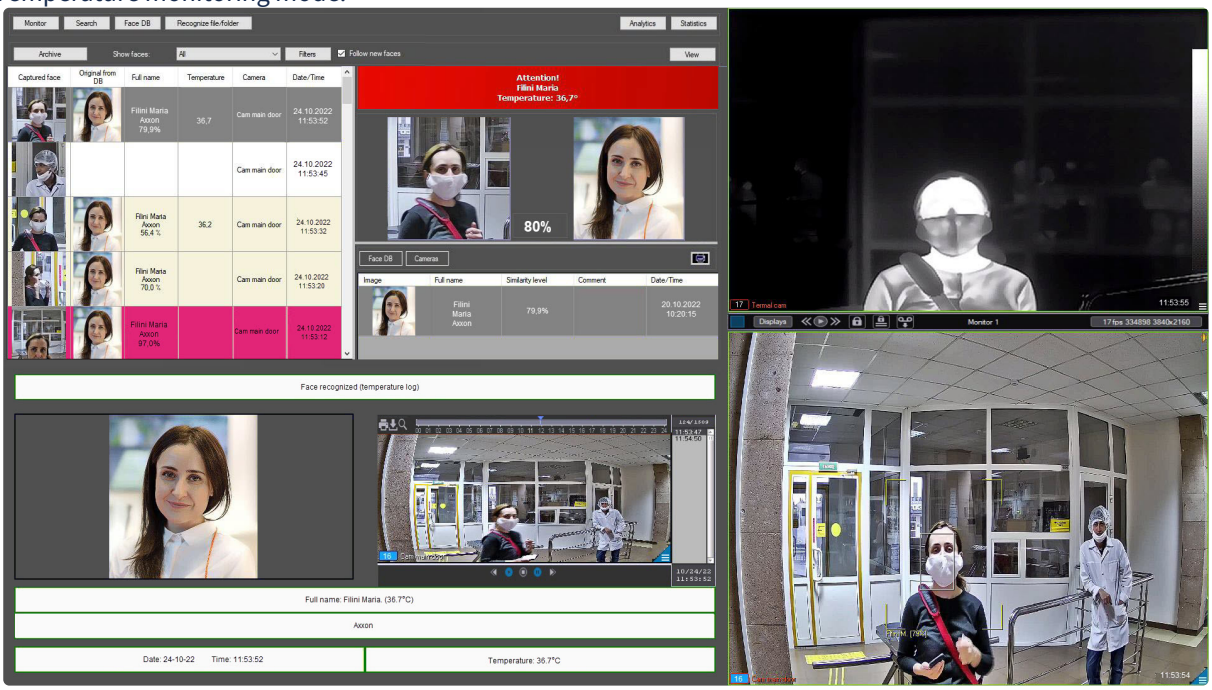
4. If it is necessary to display a face captured by the camera of the Face Recognition Server, when the face could not be recognized, then configure the *Event Manager* module according to the documentation. The following settings are required:
   a. Create and configure a new **Rule of displaying** object:
      - For the **Type of object** parameter, select **Face Recognition Server**.
      - For the **Template** parameter, select a template for displaying the unrecognized face (see paragraph 4.b).
      - On the **Objects** tab, select the corresponding **Face Recognition Server** object.
      - On the **Events** tab, set the checkbox for the **Not recognized** event.
   b. Create and configure a new **Template of displaying** object, add the **Photo** element to it, and specify the following in its **Parameter** property:

```
imageBase64
```

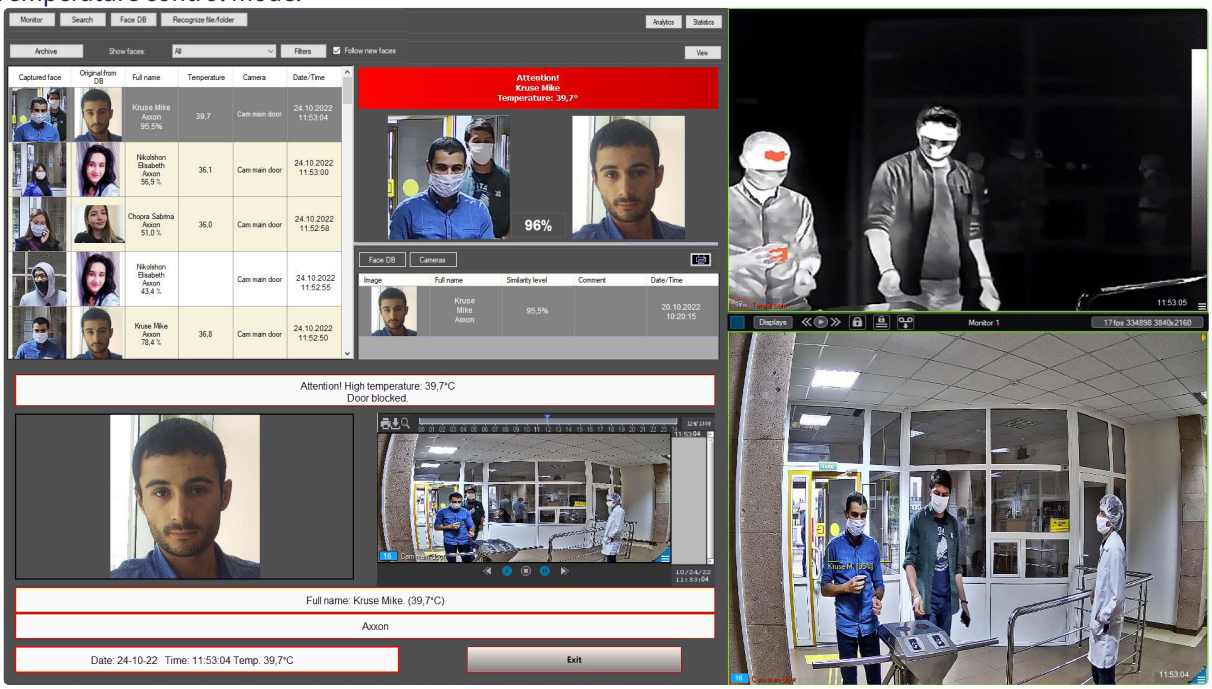
Photo object properties

The example of a configured system for the temperature monitoring and control:

1. Temperature monitoring mode:



2. Temperature control mode:



4 Working with Virtual Access Server module

The following interface objects are most often used to work with the *Virtual Access Server* software module:

- **Event viewer** (see *Axxon PSIM* software package. Administrator's Guide and *Axxon PSIM* software package. Operator's Guide);
- **Event manager** (see Event Manager Module Settings and Operation Guide);
- **Access Manager** (see Access Manager Module Settings and Operation Guide).