



Nitgen Integration Module Configuration and Operation Manual

ACFA PSIM 1.1

Last update 05/06/2024

Table of Contents

1	Introduction into Nitgen Integration Module Configuration and Operation Manual	3
1.1	Purpose of the document	3
1.2	General information about Nitgen module	3
2	Supported hardware and licensing of the Nitgen integration module	4
3	Configuring the Nitgen integration module	5
3.1	Configuration procedure for the Nitgen integration module	5
3.2	Configuring the Nitgen ACS connection	5
3.3	Configuring the NAC2500 controller	6
3.3.1	Configuring the Nitgen terminals	8
3.3.2	Configuring the Nitgen fingerprints	8
3.4	Configuring the Nitgen users	9
4	Working with the Nitgen Module	12

1 Introduction into Nitgen Integration Module Configuration and Operation Manual

On the page:

- Purpose of the document
- General information about Nitgen module

1.1 Purpose of the document

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

This Guide provides:

1. general information about *Nitgen ACS* module;
2. information about how to configure *Nitgen ACS* module;
3. information about how to work with *Nitgen ACS* module.

1.2 General information about Nitgen module

The *Nitgen* module is the *ACFA PSIM*-based ACS component. It performs the following functions:

1. Configuring the *Nitgen ACS* (manufactured by NITGEN Co.);
2. Ensuring interaction between the *Nitgen ACS* and *ACFA PSIM* (monitoring, control).

Note.

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

Before configuring the *Nitgen* integration module:

1. Install the *Nitgen ACS* hardware at the secure facility (refer to the *Nitgen ACS* reference documentation);
2. Install the *Access Manager SDK* which is located in the <Axxon PSIM installation directory>\Modules\Nitgen folder.
3. Connect the *Nitgen ACS* to the *Axxon PSIM* Server.

2 Supported hardware and licensing of the Nitgen integration module

Manufacturer	Nitgen Co., Ltd. Fax : +82-2-6488-3096 Sales/Marketing : sales1@nitgen.com Customer Center : customer@nitgen.com
Integration type	SDK
Equipment connection	Ethernet

Supported equipment

Equipment	Function	Features
NAC 2500	Access controller	Log capacity: 67,500 logs Template capacity: 5,000 templates (2 templates/ 1 finger, 2,500 users) Lock: Deadbolt, EM Lock, Door Strike, Automatic Door Live fingerpring detection USB memory slot

Equipment supporting the same SDK but not tested by AxxonSoft QA engineers: FINGKEY-ACCESS, FINGKEY-ACCESS 2, NAC3000, NAC5000, etc. AxxonSoft does not guarantee these devices operation with the *Nitgen* integration module. If you need them for you project, please consult with your AxxonSoft manager to arrange tests.

Protection

1 controller.

3 Configuring the Nitgen integration module

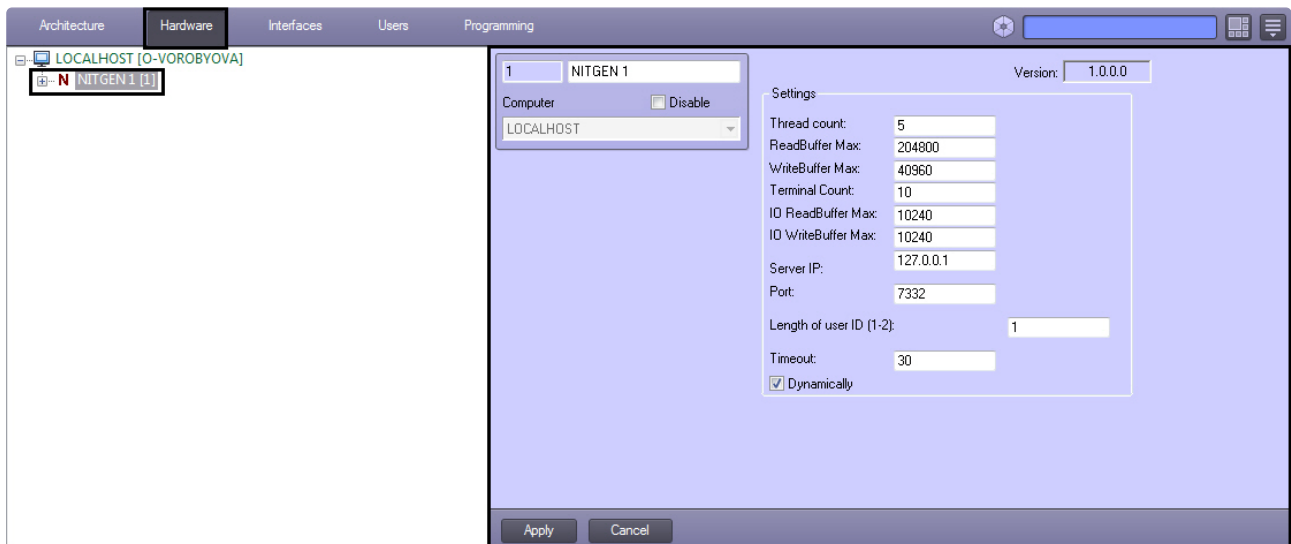
3.1 Configuration procedure for the Nitgen integration module

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

1. Configure the *Nitgen* ACS connection to the ACFA PSIM Server.
2. Configure the *Nitgen* ACS controller.
3. Configure the *Nitgen* ACS users.

3.2 Configuring the Nitgen ACS connection

To configure the *Nitgen* ACS connection to the ACFA PSIM Server use the relevant **NITGEN** object which is created on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog object.



To configure the *Nitgen* integration module's connection, do the following:

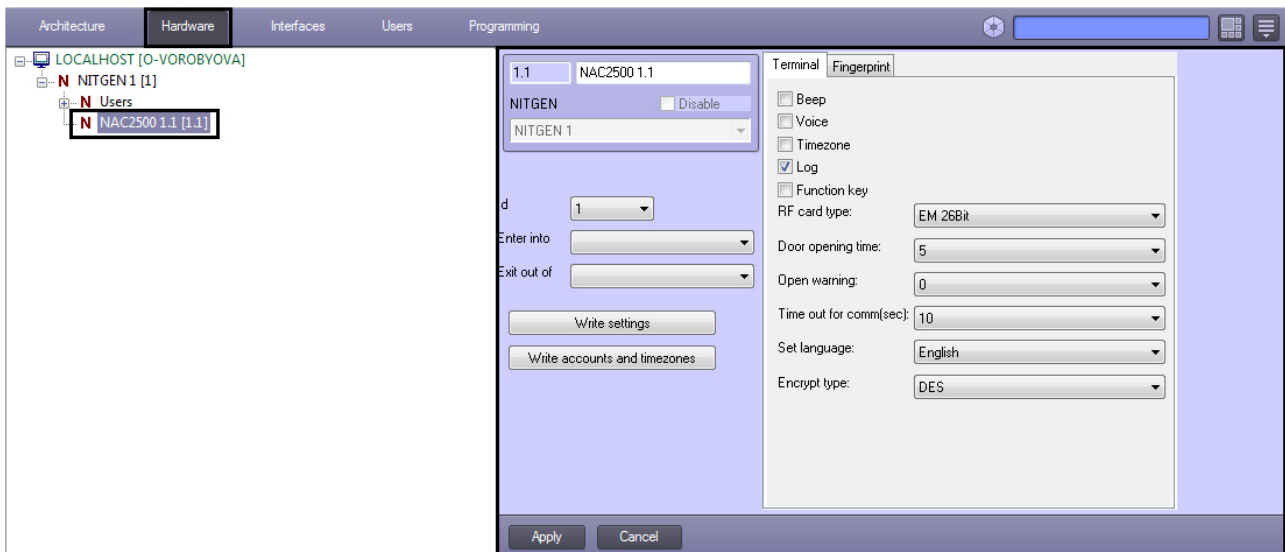
1. Go to the **NITGEN** object's settings panel.

2. In the **Thread count**: field enter the number of data processing threads (1).
3. In the **ReadBuffer Max**: field enter the maximal size of buffer which will save data received from terminals (2).
4. In the **WriteBuffer Max**: field enter the maximal size of buffer which will save data to be sent to terminals (3).
5. In the **Terminal Count**: field enter the number of terminals connected to the server simultaneously (4).
6. In the **IO ReadBuffer Max**: field enter the maximal size of data which will read in the network at one time (5).
7. In the **IO WriteBuffer Max**: field enter the maximal size of data which will be written in the network at one time (6).
8. In the **Server IP**: field enter the IP-address of server (7).
9. In the **Port**: field enter the number of the COM port to connect to *Nitgen ACS* (8).
10. In the **Length of user ID (1-2)**: field enter the length of user ID (9).
11. In the **Timeout**: field enter the timeout of connection (10).
12. Set the **Dynamically** checkbox to send data to the controller dynamically (11).
13. Click **Apply** to save changes.

Configuring of the *Nitgen ACS*'s connection is completed.

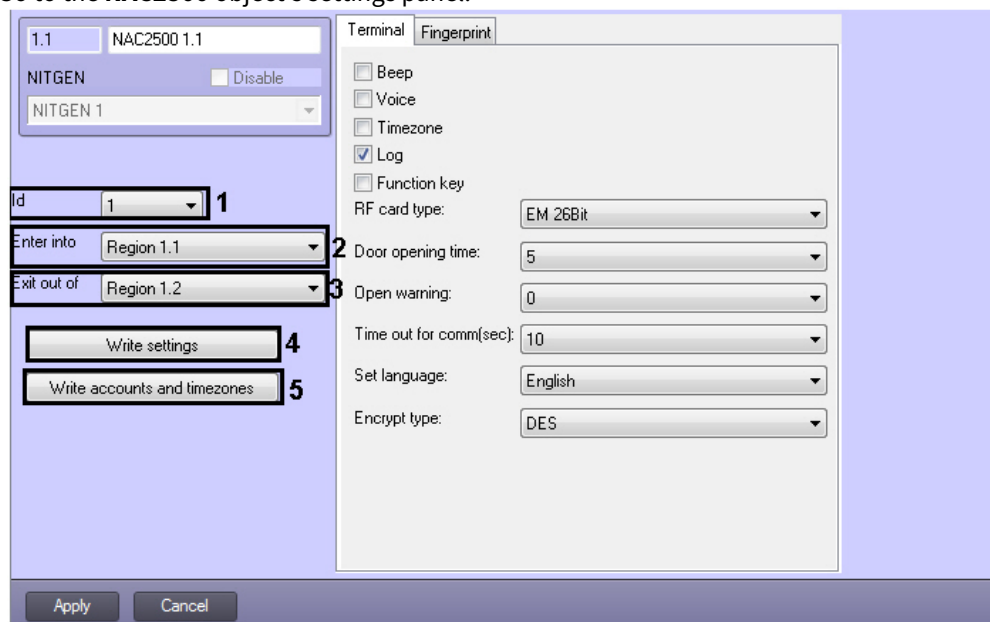
3.3 Configuring the NAC2500 controller

Configuring of the *Nitgen* controllers is performed on the settings panel of the **NAC2500** object which is created on the basis of the **NITGEN** object on the **Hardware** tab of the **System settings** dialog window.



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

1. Go to the **NAC2500** object's settings panel.



2. From the **Id** drop-down list select the id number of controller (1).
3. From the **Enter into** drop-down list select the **Region** object corresponding to the territory situated on the side of exit from the territory via the controller (2).
4. From the **Exit out of** drop-down list select the **Region** object corresponding to the territory situated on the side of entrance to the territory via the controller (3).
5. Click the **Write settings** button to send settings to the controller (4).
6. Click the **Write accounts and timezones** button to send accounts and time zones to the controller (5).
7. Click **Apply** to save changes.

Configuring the *NAC2500* controller is completed.

3.3.1 Configuring the Nitgen terminals

To configure the *Nitgen* terminal, do the following:

1. Go to the **Terminal** tab of the **NAC2500** object's settings panel.

The screenshot shows the configuration interface for a Nitgen terminal. On the left, there are fields for 'Id' (set to 1), 'Enter into' (Region 1.1), and 'Exit out of' (Region 1.2). Below these are 'Write settings' and 'Write accounts and timezones' buttons. The main panel is titled 'Terminal' and has a 'Fingerprint' sub-tab. It contains several checkboxes: 'Beep' (1), 'Voice' (2), 'Timezone' (3), 'Log' (4), and 'Function key' (5). Below these are several dropdown menus: 'RF card type' (6) set to 'EM 26Bit', 'Door opening time' (7) set to '5', 'Open warning' (8) set to '0', 'Time out for comm(sec)' (9) set to '10', 'Set language' (10) set to 'English', and 'Encrypt type' (11) set to 'DES'. At the bottom are 'Apply' and 'Cancel' buttons.

2. Set the **Beep** checkbox to generate sounds when screen is touched or keys are pressed on the terminal (1).
3. Set the **Voice** checkbox to receive voice instructions when authenticating fingerprint at the terminal (2).
4. Set the **Timezone** checkbox to enable time zone-related functions (3).
5. Set the **Log** checkbox to transfer the log when an event occurs in the terminal (4).
6. Set the **Function key** checkbox to use terminal function keys in application programs (5).
7. From the **RF card type:** drop-down list select the required card type if RF cards are used to authenticate users (6).
8. From the **Door opening time:** drop-down list select duration of door opening after the user is authenticated (7).
9. From the **Open warning:** drop-down list select time period after which an alarm will sound if the door remains open for longer than the specified period (8).
10. From the **Time out for comm(sec):** drop-down list select the time period after which the network connection will be considered nonexistent if the server and terminal are communicating through a network and no response occurs within the specified time (9).
11. From the **Set language:** drop-down list select the language to display on the terminal screen (10).
12. From the **Encrypt type:** drop-down list select the type of encryption for the data transmitted between the terminal and the network (11).
13. Click **Apply** to save changes.

Configuring of the *Nitgen* terminal is completed.

3.3.2 Configuring the Nitgen fingerprints

To configure the *Nitgen* fingerprints, do the following:

1. Go to the **Fingerprint** tab of the **NAC2500** object's settings panel.

The screenshot shows the 'Fingerprint' tab of the NAC2500 object's settings panel. The interface is divided into two main sections: a left sidebar and a main configuration area. The sidebar contains fields for 'Id' (set to 1), 'Enter into' (Region 1.1), and 'Exit out of' (Region 1.2), along with 'Write settings' and 'Write accounts and timezones' buttons. The main configuration area has a 'Terminal' tab and a 'Fingerprint' tab. The 'Fingerprint' tab contains the following settings, numbered 1 through 10:

Setting	Value	Number
Brightness:	40	1
Contrast:	20	2
Gain:	2	3
1:1 authentication level:	5	4
1:N authentication level:	8	5
Capture timeout:	5	6
Use 1:N timeout:	<input checked="" type="checkbox"/>	7
1:N timeout:	3	8
Use identity:	Not use	9
LFD level:	Not use	10

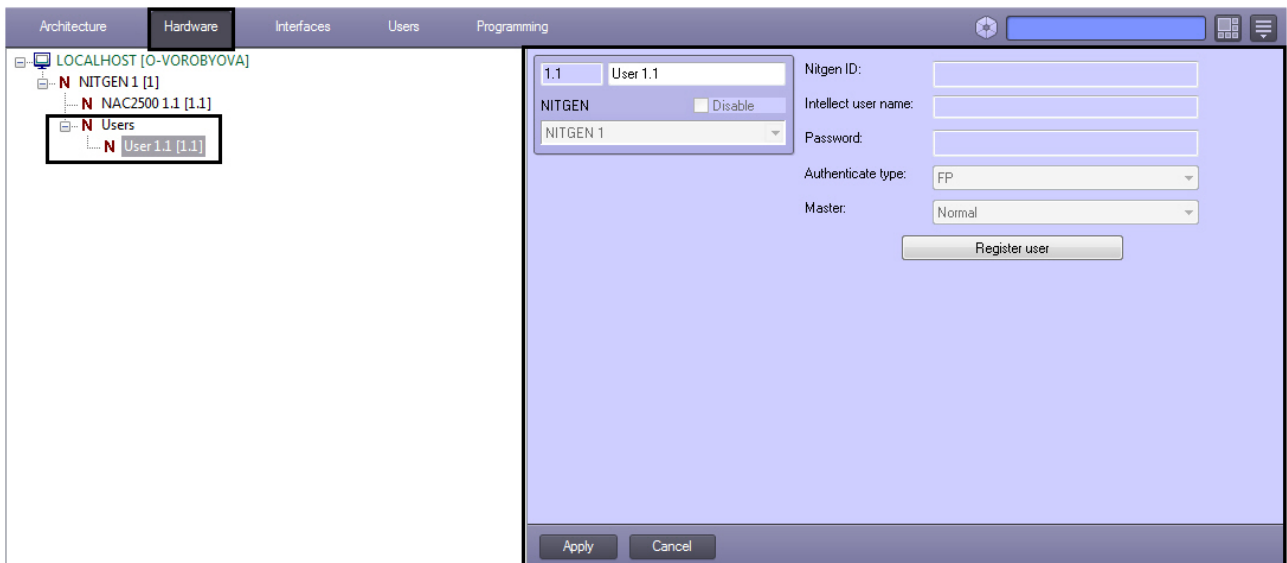
At the bottom of the panel are 'Apply' and 'Cancel' buttons.

2. From the **Brightness:** drop-down list select the brightness of the fingerprint (1).
3. From the **Contrast:** drop-down list select the contrast of the fingerprint (2).
4. From the **Gain:** drop-down list select the intensity of the fingerprint (3).
5. From the **1:1 authentication level:** drop-down list select the security level which will be used for fingerprint authentication with User ID (4).
6. From the **1:N authentication level:** drop-down list select the security level which will be used for fingerprint authentication without User ID (5).
7. From the **Capture timeout:** drop-down list select the fingerprint capture timeout (6).
8. Set the **Use 1:N timeout** checkbox to limit the fingerprint search for 1:N authentication within the specified period (7).
9. From the **1:N timeout:** drop-down list select the time period by which the fingerprint search will be limited for 1:N authentication (8).
10. From the **Use identity:** drop-down list select the way of authentication: use 1:N authentication or shorted authentication (9).
11. From the **LFD level:** drop-down list select one of four Live Finger Detection levels to detect forged fingerprints (10).
12. Click **Apply** to save changes.

Configuring of the *Nitgen* fingerprints is configured.

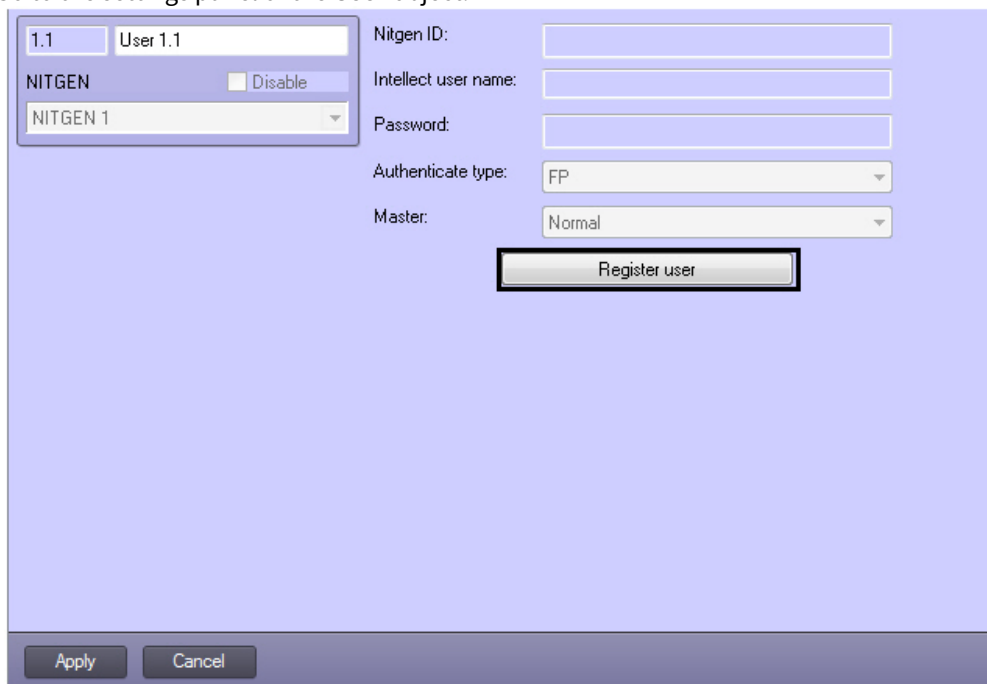
3.4 Configuring the Nitgen users

Configuring of the *Nitgen* users is performed on the settings panel of the **User** object which is created on the basis of the **NITGEN** object on the **Hardware** tab of the **System settings** dialog window.



To configure the *Nitgen* users, do the following:

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

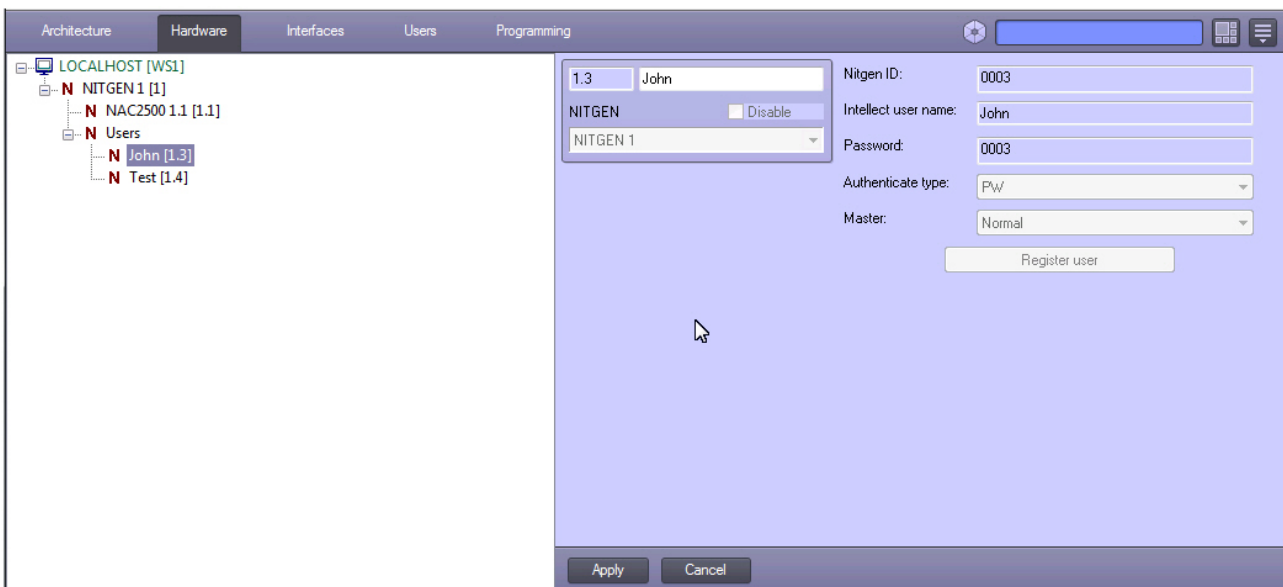


- Click the **Register user** button. The **Dialog** window will open.

- In the **NitgenID** field enter the user identification number (1).
- In the **Name** field enter the user name (2).
- From the **AccessLevel** drop-down list select the **Access level** object which is assigned to the user (3).
- From the **Department** drop-down list select the Department object to which the user belongs (4).
- From the **Reader** drop-down list select the corresponding reader (5).
- Click the **Register** button.

When all settings in the *ACFA PSIM* software are performed it's required to register user through the *Nitgen* device (see the official documentation on the *Nitgen* system).

After that the created user will be added to the *ACFA PSIM* software and to the *Visitor Management System* interface module.



Configuring of the *Nitgen* user is completed.

4 Working with the Nitgen Module

The **Event viewer** interface objects are used to work with the *Nitgen* Module.

Information about configuring this interface object is presented in the *Axxon PSIM Software System: Administrator's Guide*.

How to work with interface objects is described in detail in *Axxon PSIM Software System: Operator's Guide*.