

LECTUS FP admin SW



BOSCH

en Installation manual

Table of contents

1	System overview	4
1.1	Important Information	4
1.2	Important planning notes for contactless readers	5
2	Installation	6
2.1	Server and Client Installation	6
2.2	Start LECTUS_fpa Server Config	9
2.3	LECTUS FP admin 1.0	12
3	Configuration	14
3.1	Add a new Device	15
3.1.1	Check the operation mode	19
3.1.2	Reader Settings	20
3.2	LECTUS enrollment	21
3.2.1	Add a new user	21
3.2.2	Delete a Card	26
3.2.3	Data Transfer	27
3.3	Monitoring	29
3.4	Add Devices to the BIS System	30
3.5	Add Devices to the Access PE System	32
3.6	Add users to the BOSCH system via User ID	34
3.6.1	BIS-Access Engine	34
3.6.2	Access Professional Edition	36
3.7	Define Input Signals	38
3.7.1	Connecting Diagram	38
3.8	How to use the BOSCH code	39
3.8.1	Device Operation Mode	39
3.8.2	Wiegand Device	40
3.8.3	User Card	41
3.8.4	Transfer all users to Device	42
3.8.5	APE Wiegand Card Definition	43
3.8.6	APE Personnel Management	44
4	Bosch Migration Tool	45

1 System overview

This instruction manual for authorized service providers contains instructions on the installation and commissioning of the Bosch fingerprint readers BioEntry Plus and BioLite Net.. The information in this instruction manual is, to the best of our knowledge, valid at the time of publication. As part of our commitment to customer service we nevertheless welcome suggestions for improvements

1.1 Important Information

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2016

Tel.: +49 (0)89 6290-0

Fax: +49 (0)89 6290 1020

Purpose of Equipment

This hardware comprises fingerprint readers for access control and time attendance, which are suitable for mullion mount.

Country of Origin and Production Date

The label applied under the bottom of the reader housing gives the essential information about country of origin and the production date.

The **Country of Origin** is Korea.

The **week and year of production** can be read on the left side of the label next to the word MANUFACTURED:.. Read it according to the code WW-YYYY, i.e. for example 32-2015 for week 32 in 2015.

1.2 Important planning notes for contactless readers

Influences on reading distance

- Metal in the "active" effective HF field.
- Interference with other readers in immediate vicinity (distance < 30 cm)
- Interference with high-energy sources
- Switch mode power supplies
- Cable quality, shielding, and cross-section dimension (remaining input voltage at reader, EMC)

2 Installation

The LECTUS_fpadmin_Setup software is delivered on a CD with the product.

This software is the LECTUS_fpadmin_ExpressSetup.exe.

2.1 Server and Client Installation

Notice!

If you update the first time from BioStar 1.6 or other versions to LECTUS, uninstall the BioStar (Server, Client or Express) first



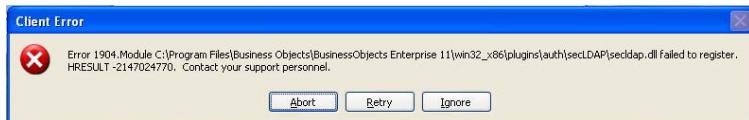
Stop the **BioStar Server Service**. Then uninstall the **BioStar SW** (Server, Client or Express).

If you want to migrate readers of an existing system to be used with LECTUS FP admin Software including all new functionalities, use the migration tool as described in chapter 4 (Bosch Migration Tool).

Install the LECTUS server and client as follows:

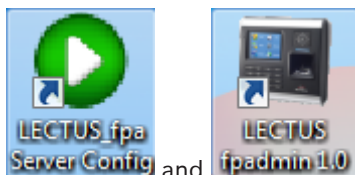
- Export LECTUS_fpadmin_ExpresSetup.exe from the CD to the computer.
- Click on the LECTUS_fpadmin_ExpressSetup.exe and **run as administrator**.

If you encounter the following error message, ignore it.



- Follow the installation guide.

After a successful installation these icons are displayed on your desktop:



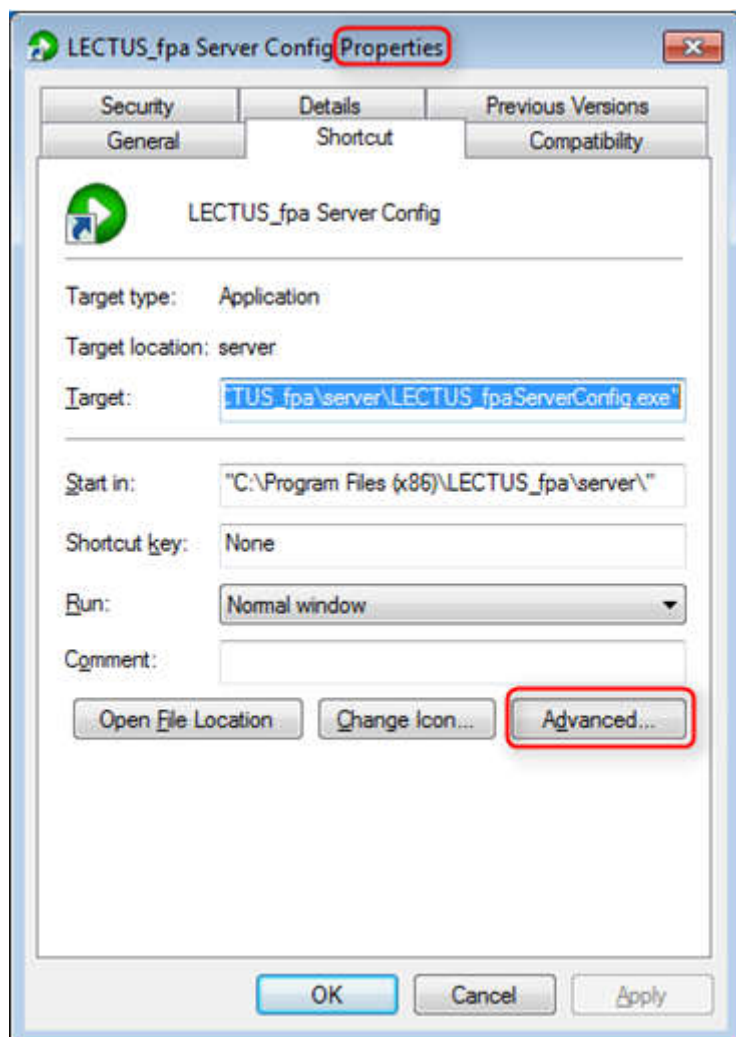
and

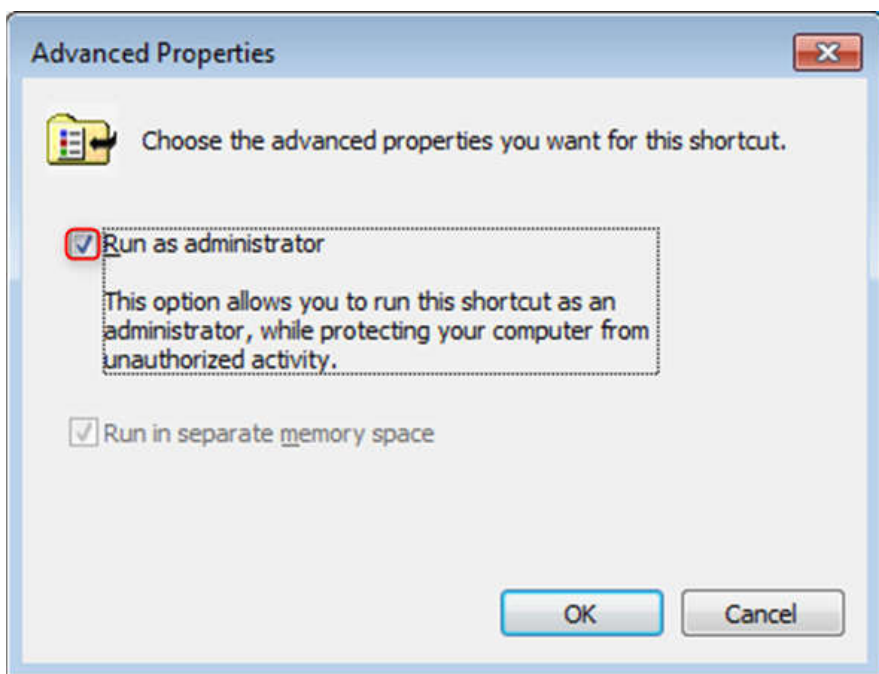
**Notice!**

For Windows 7 or higher you have to run the LECTUS fpadmin SW as Administrator
Consequences

- Right-click on the above icons and select **Start as Admin**, or
- Set the option fix with a Right-Click on the icon.
- Then select **Properties > Advance** and select **Run as administrator**.

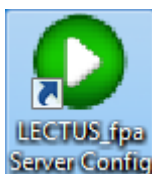
Set Run as Administrator for both icons:



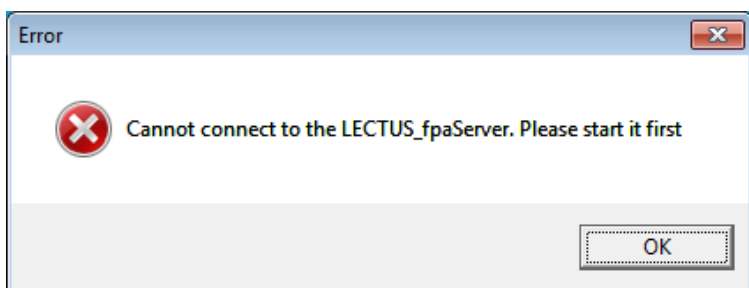


2.2 Start LECTUS_fpa Server Config

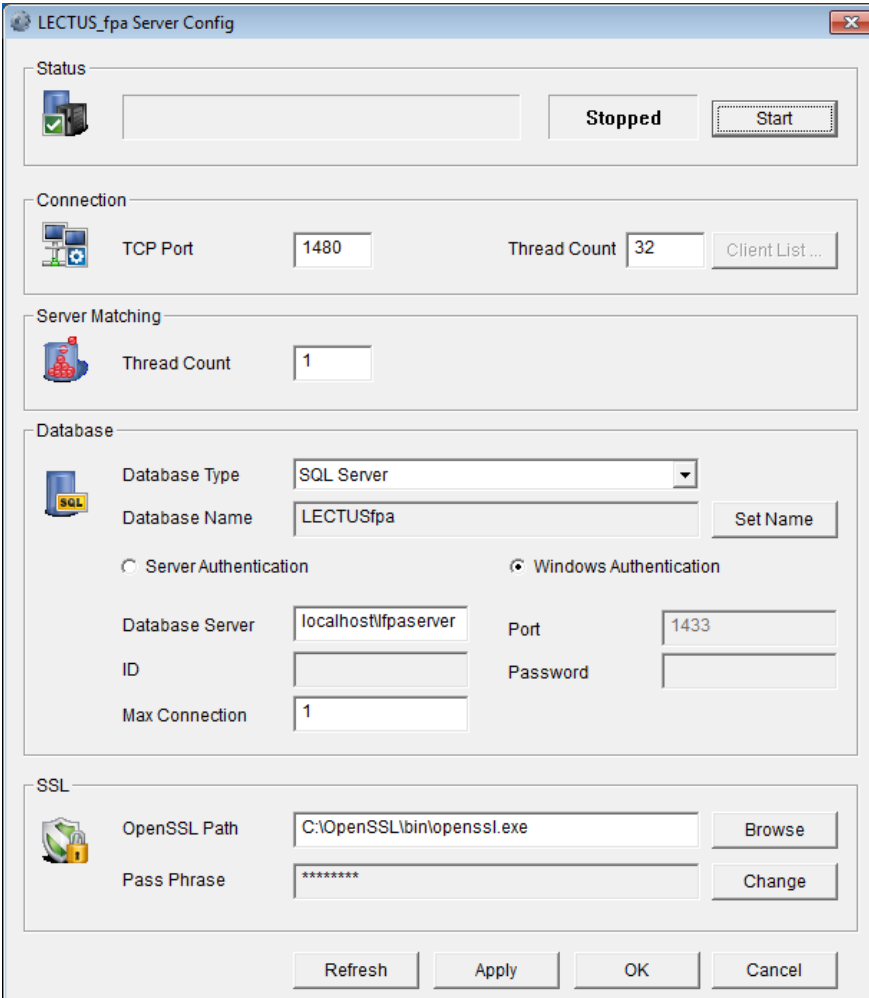
Click the following icon to start the LECTUS_fpa Server:



On starting the **LECTUS_fpa Server** following message is displayed:



- Click **OK** to continue.



The image shows the 'LECTUS_fpa Server Config' window. It has a title bar with a close button. The window is divided into several sections: 'Status' with a server icon, a status box showing 'Stopped', and a 'Start' button; 'Connection' with a network icon, 'TCP Port' set to '1480', 'Thread Count' set to '32', and a 'Client List ...' button; 'Server Matching' with a server icon and 'Thread Count' set to '1'; 'Database' with a database icon, 'Database Type' set to 'SQL Server', 'Database Name' set to 'LECTUSfpa', a 'Set Name' button, radio buttons for 'Server Authentication' and 'Windows Authentication' (selected), 'Database Server' set to 'localhost\fpaserver', 'Port' set to '1433', 'ID' and 'Password' fields, and 'Max Connection' set to '1'; and 'SSL' with a lock icon, 'OpenSSL Path' set to 'C:\OpenSSL\bin\openssl.exe', a 'Browse' button, 'Pass Phrase' set to '*****', and a 'Change' button. At the bottom are 'Refresh', 'Apply', 'OK', and 'Cancel' buttons.

Status

Stopped Start

Connection

TCP Port 1480 Thread Count 32 Client List ...

Server Matching

Thread Count 1

Database

Database Type SQL Server Database Name LECTUSfpa Set Name

☐ Server Authentication ☒ Windows Authentication

Database Server localhost\fpaserver Port 1433

ID Password

Max Connection 1

SSL

OpenSSL Path C:\OpenSSL\bin\openssl.exe Browse

Pass Phrase ***** Change

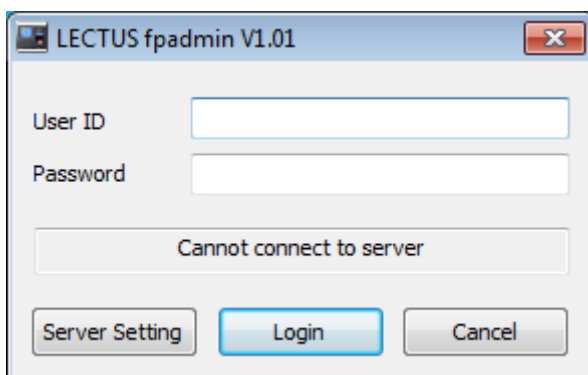
Refresh Apply OK Cancel

- Click **Start** to continue.

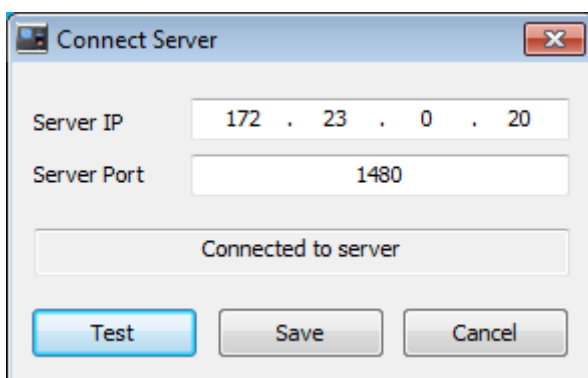
2.3 LECTUS FP admin 1.0



- Click **LECTUS fpadmin 1.0** to start
- Enter user ID and password and select **Server Settings** to continue:

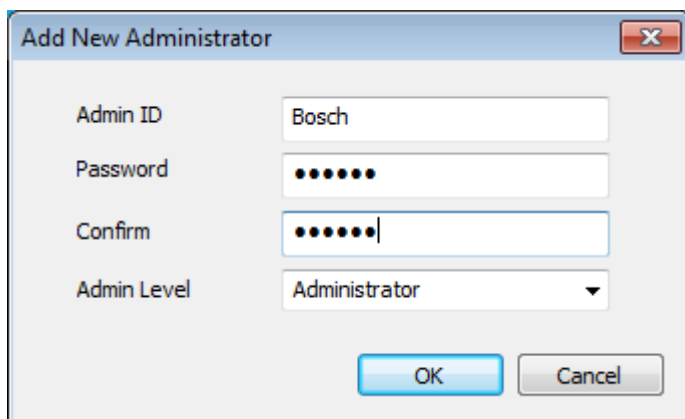


- Enter the **Server IP** address and **Server Port No.:**



- Click the **Test** button. If the server is connected select **Save** to close the window.

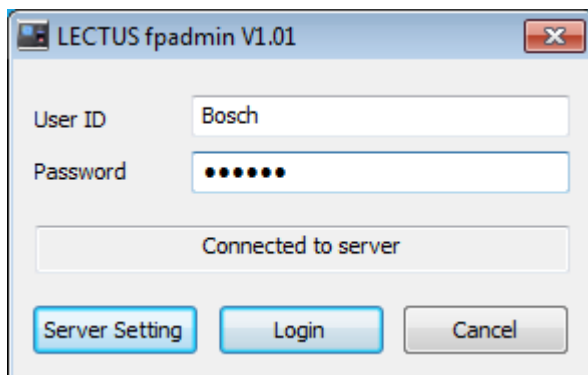
On first starting the system, define the administrator name (**AdminID**) and **Password** in the window below:



The 'Add New Administrator' dialog box contains the following fields and controls:

- Admin ID:** Text input field containing 'Bosch'.
- Password:** Password input field with 7 dots.
- Confirm:** Password input field with 7 dots and a cursor at the end.
- Admin Level:** Dropdown menu showing 'Administrator'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

- Now login using the **Admin ID** and **Password** as defined above:



The 'LECTUS fpadmin V1.01' window contains the following fields and controls:

- User ID:** Text input field containing 'Bosch'.
- Password:** Password input field with 7 dots.
- Status:** A text box displaying 'Connected to server'.
- Buttons:** 'Server Setting', 'Login', and 'Cancel' buttons at the bottom.

Click **Login** to start the LECTUS fpadmin 1.0

3 Configuration

After the Suprema software has been installed, the following features are described:

- Device configuration
- Adding a new user and its data
- Defining a new device
- Access Monitoring

Precondition

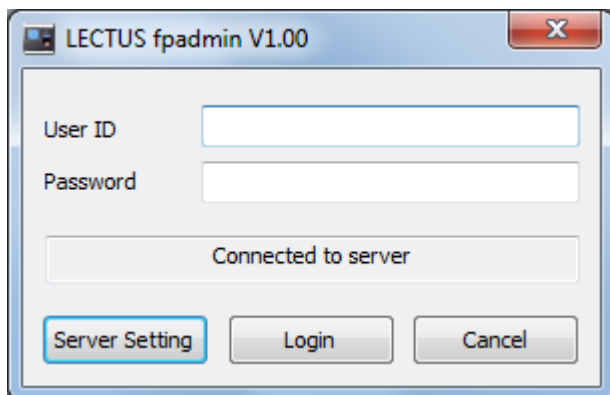
- To be able to scan a reader check whether:
 - The fingerprint readers are connected with the network,
 - Server and reader are in the same sub-network.

If the network settings of the reader are unknown, the user can initialize a network reset (described in the reader manual).

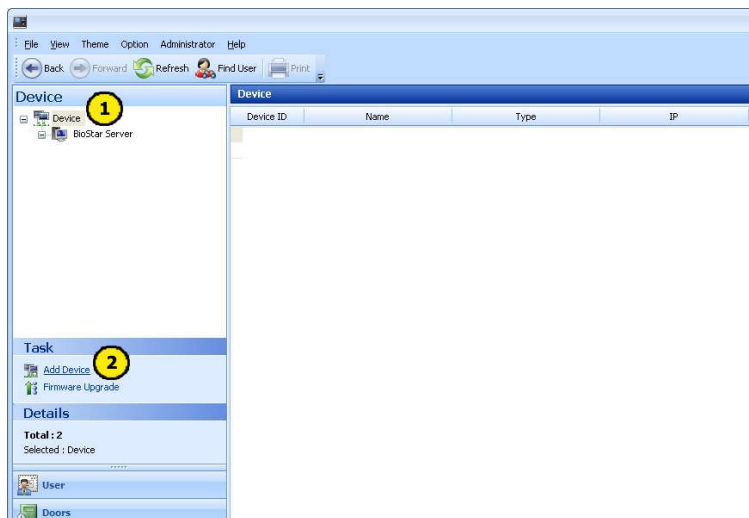
The **default network address** after reset is 192.168.0.1.

3.1 Add a new Device

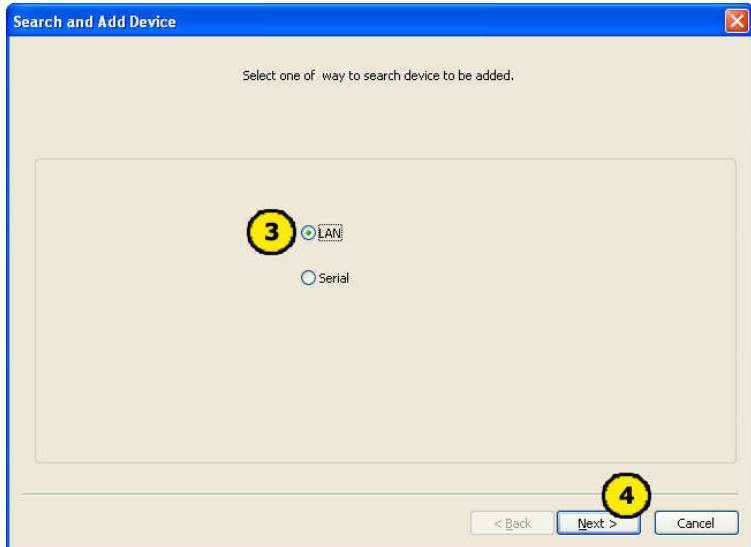
Start the LECTUS_fpadmin V1.00 client.



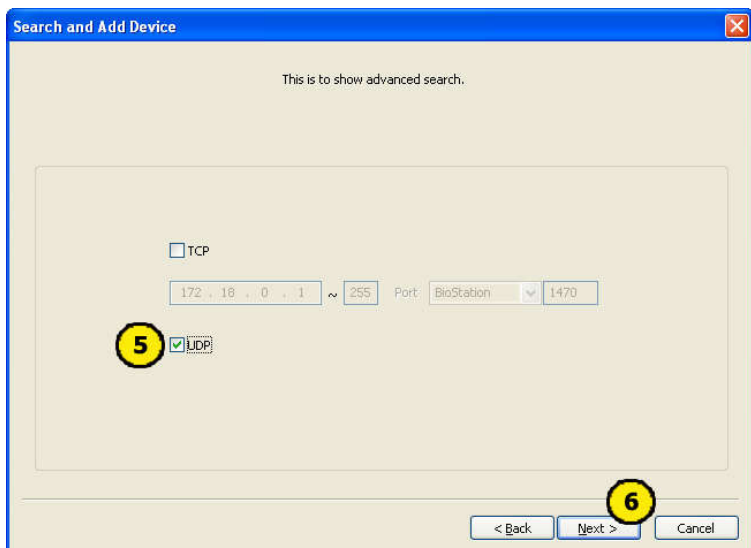
Enter user name and password.



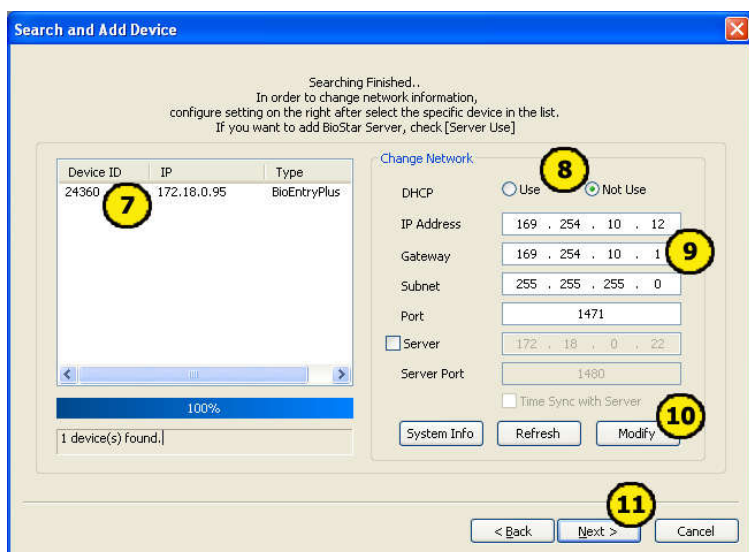
1. Open the **Device** menu.
2. Click the **Add device** task function.



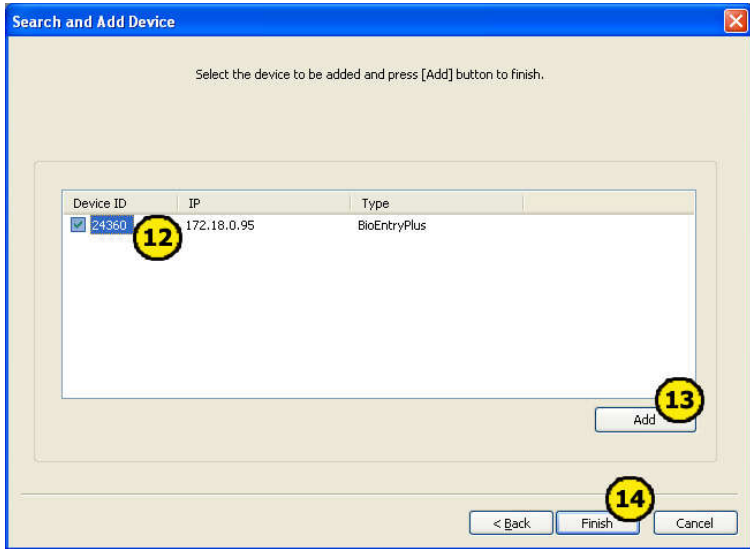
3. Select the **LAN** option.
4. Click the **Next** button.



5. Activate the **UDP** control.
6. Click the **Next** button.



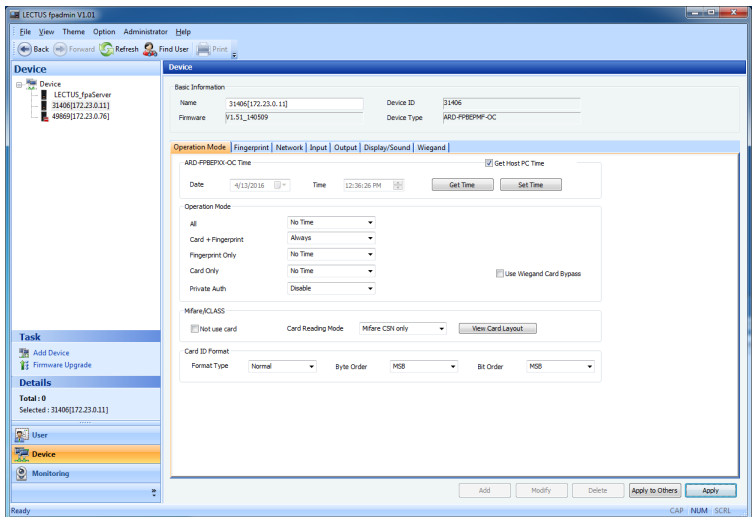
7. Select the device to be added.
8. Choose the **Not Use** option for DHCP.
9. If necessary, fill in the fields **IP address** and **Subnet**.
10. Click the **Modify** button.
11. Finally click the **Next** button.



12. Select the found device
13. Click the **Add** button
14. Click the **Finish** button.

The new device is shown in the **Device** tree of the Server Window.

3.1.1 Check the operation mode

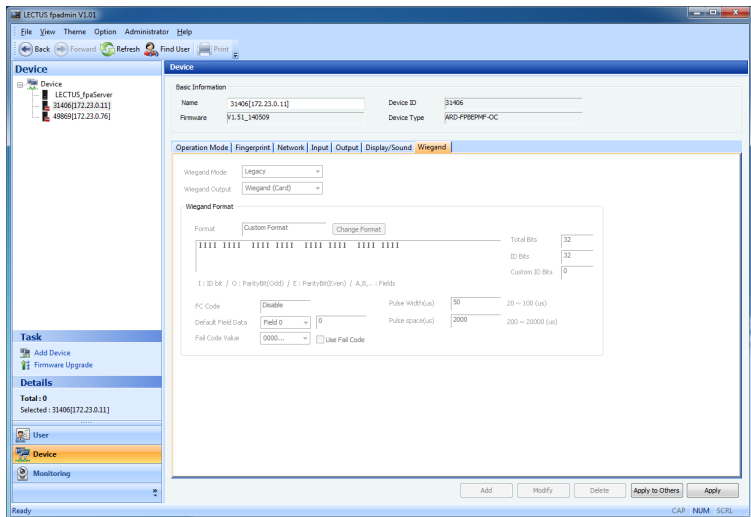


- Check if the mode is on **Card + Fingerprint**
- Set **Card Reading Mode**
- Set format type to **normal**
- Click **Apply**
- Select the device
 - Set **Get Host PC Time**
 - Check if the Operation Mode Card + Fingerprint is set to **Always**
 - Check if The Card ID Format Type is set to **Normal**
 - Click **Apply**.

3.1.2 Reader Settings

After adding the new device change the following settings:

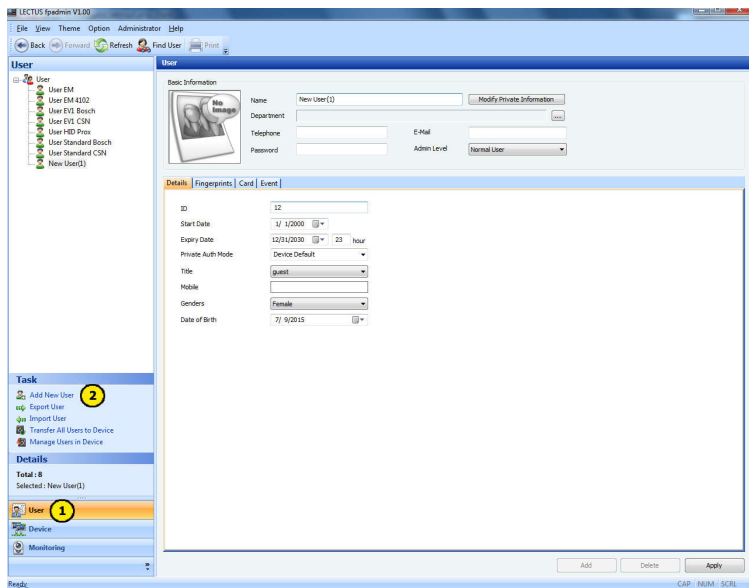
- Open the **Wiegand** tab.
- Set **Wiegand Output** to **Wiegand (Card)**.
- Click **Apply**.



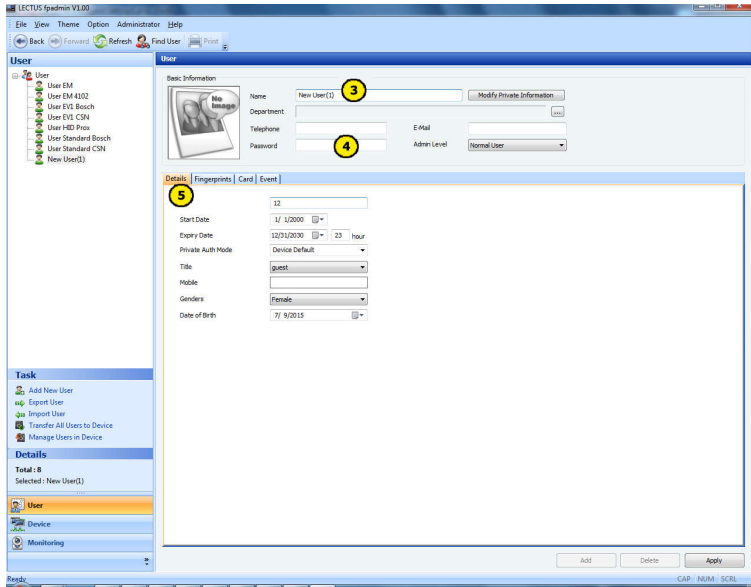
3.2 LECTUS enrollment

3.2.1 Add a new user

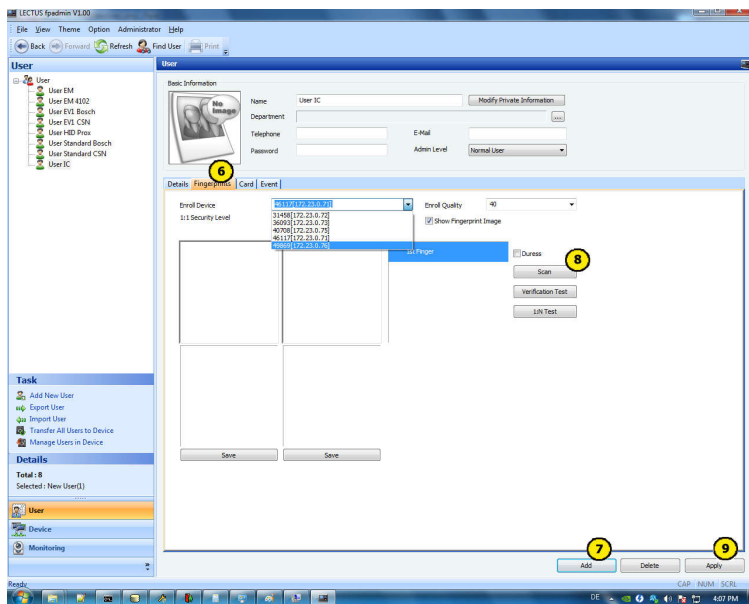
To add a new user follow the steps in the screenshots below:



1. Open the User menu.
2. Select the **Add New User** function from the **Task** menu in the left frame.



3. Enter the **Name** of the user.
4. If a pin code is required enter a number of maximum six digits in the **Password** field.
5. Additional user data can be added on the **Details** tab.



6. Open the **Fingerprints** tab and select a reader as enrollment device.
7. Click the **Add** button to add a fingerprint to the user.
8. Place the index finger on the reader and click the **Scan** button.
9. Follow the instructions on the screen and, if the test is positive, click the **Apply** button to confirm the changes.



Notice!

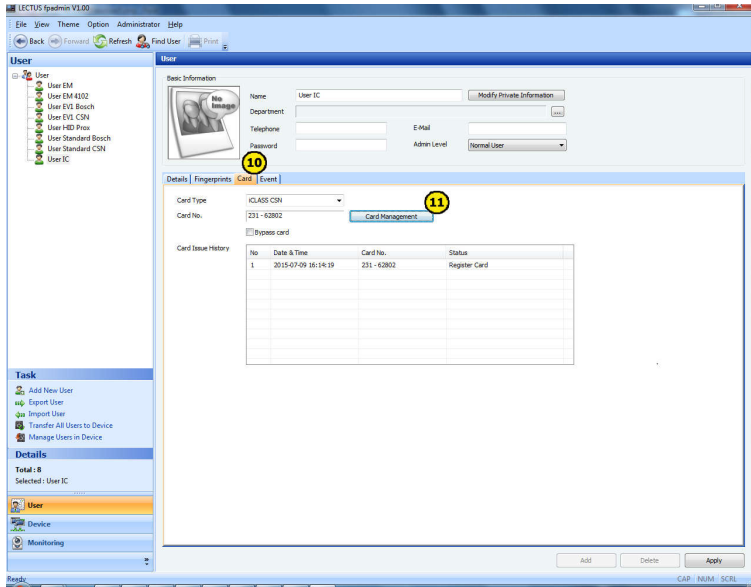
There is no warning for unsaved data.

If you leave the dialog without clicking the **Apply** button, all data will be lost

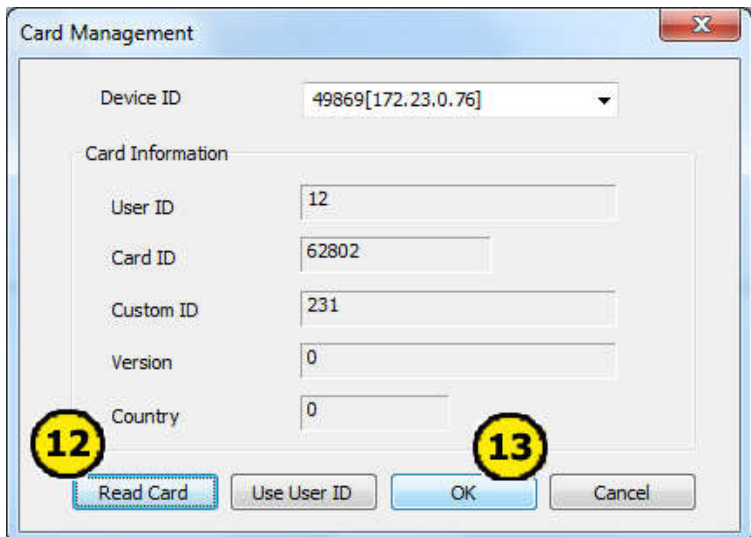


Notice!

The selected enrollment reader will remain set for all enrollment actions.

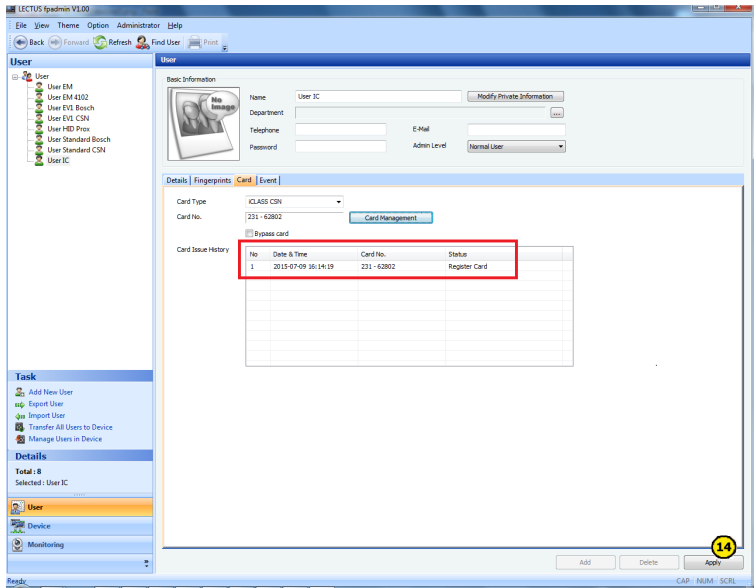


10. Open the **Card** tab and select the card type
11. Click the **Card Management** button.
 - Select the Device ID of the enrollment reader.



12. Click the **Read Card** Button and present a card to the reader.

13. Click the OK button to close the dialog.

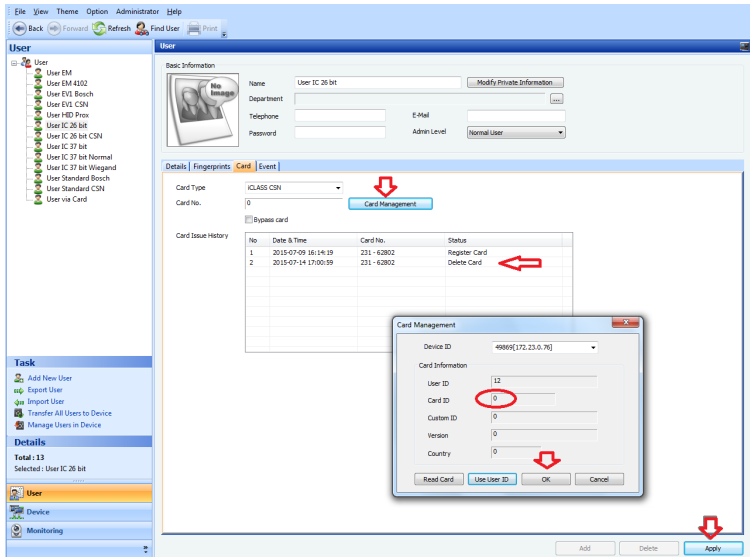


14. Click the **Apply** button to confirm the changes.

The new added card is displayed in the list control - see the red frame.

3.2.2 Delete a Card

To delete a card proceed as follows:

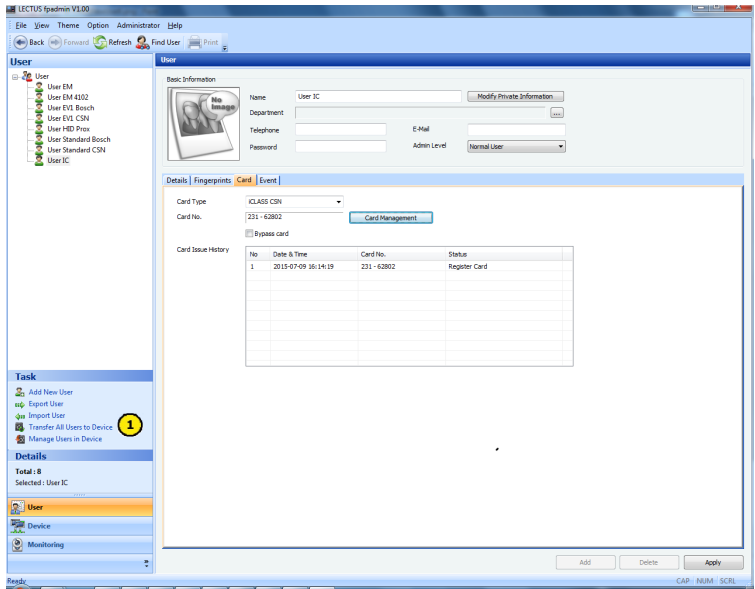


1. Select **Card Type**
2. Click **Management**
3. Check if **Card ID** is set to **Zero**
4. Click **OK** to confirm
5. Click **Apply**

The result can be found in the **Card issue history**.

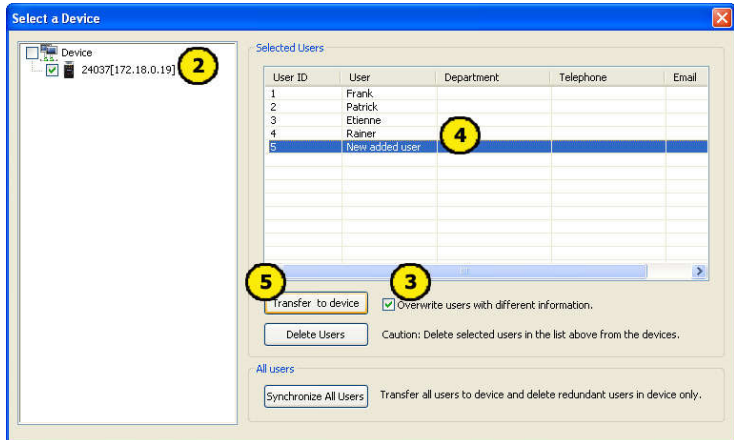
3.2.3 Data Transfer

To transfer the data to the fingerprint reader follow the steps below:



1. Select the Transfer All Users to Device function from the **Task** menu

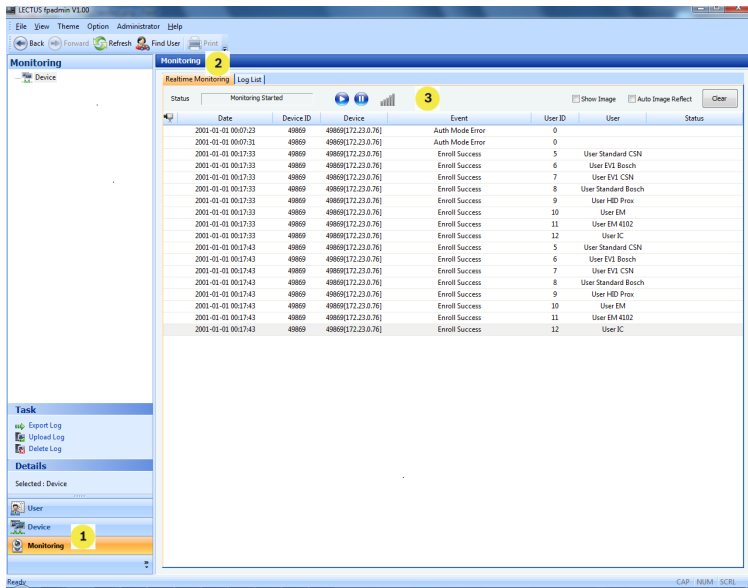
The following screen opens:



1. Select the corresponded device.
2. Activate the **Overwrite users with different information** control.
3. Select the desired user.
4. Click the **Transfer to Device** button.

3.3 Monitoring

To check the configuration of the device have a look on the events coming from the device.



1. Open the **Monitoring** menu.
 2. Select the **Realtime Monitoring** tab.
- Generate messages creating actions at the door.

1. Verify that the done actions are shown on this page.

3.4 Add Devices to the BIS System

The using of the FPL readers in association with the **AccessEngine** will be shown using a door model 1c.

Precondition

- The AMC2 4W is successfully defined in the BIS Configuration Browser and the connection is working fine.
- The fingerprint reader is connected with the AMC over Wiegand

Proceeding

New entrance

Settings:

Entrance model: DM 01c: Common door with entry or exit reader

Max. number outputs/authorizations: 8 / 0

☐ Mantrap option

Readers:

1st inbound reader: WIE1K Reader: Wiegand Reader, keyboard

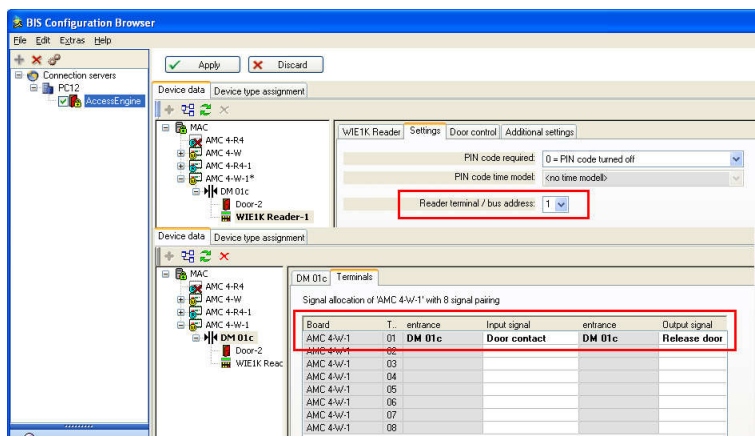
1st outbound reader: <No reader defined>

2nd inbound reader (optional): <No reader defined>

2nd outbound reader (optional): <No reader defined>

OK Cancel

The BIS software sets the reader address and the signals on the corresponding places automatically. See the below attached screen capture.



3.5 Add Devices to the Access PE System

The using of the FPL readers in association with the Access Professional Edition will be shown by using a door model 1c.

Precondition

- The AMC2 4W is successfully defined and the connection is working fine.
- The fingerprint reader is connected with the AMC over Wiegand.

Proceeding:

Define Entrance

Description:

Please configure LAC, GID and doormodel

LAC: GID: Door model: 1

☒ Video verification Surv. camera:

Reader configuration

Reader type: 2 Address (1..8): ☒ Write access

Access-reader:

Signal definition

	Signal description	On dev...	GID / Board	DID	Connection
<input checked="" type="checkbox"/>	Door sensor	AMC	0		3 1
<input checked="" type="checkbox"/>	Pushbutton: Door open				
<input checked="" type="checkbox"/>	Bolt sensor				
<input checked="" type="checkbox"/>	Entrance locked				
<input checked="" type="checkbox"/>	Sabotage signal				
<input checked="" type="checkbox"/>	Local Open Enable				
<input checked="" type="checkbox"/>	Door opener	AMC	0		4 1

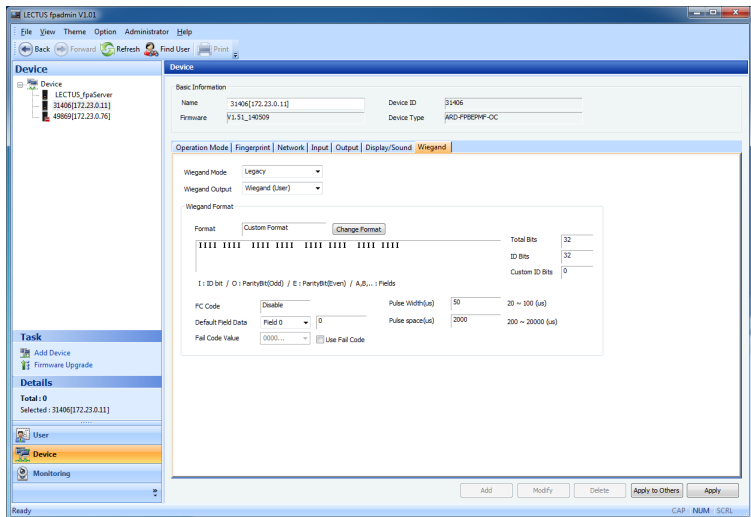
1. Add a door model 1c.
2. Add a reader with the address 1.
3. Define the input signal **Door sensor** on connection place 1.
4. Define the output signal **Door opener** on connection place 1.

3.6 Add users to the BOSCH system via User ID

The scope of this chapter is to show how the user Identification Number (ID) of the Suprema data record is used in the Access PE and in the BIS Access Engine as a card number.

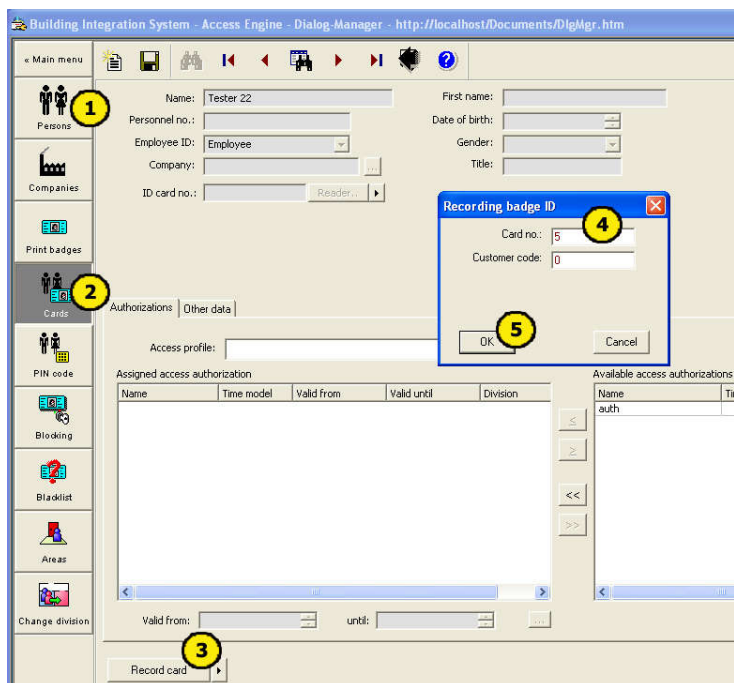
Necessary settings in the LECTUS fpadmin

- Select a device
- Go to the **Wiegand** folder
- Set **Wiegand Output** to **Wiegand (user)**



3.6.1 BIS-Access Engine

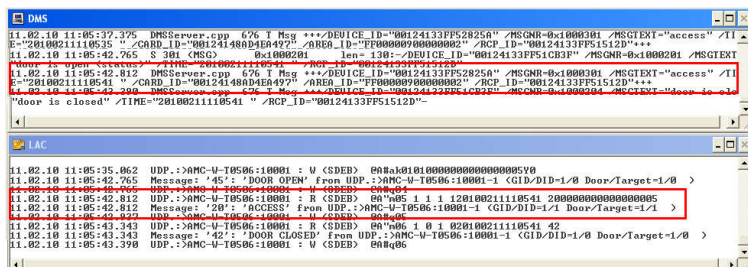
To assign the **ID** from the LECTUS_FP admin software, proceed as follows:



1. Define a new person in the Access Engine dialog **Persons** or select an existing one.
2. Open the dialog **Cards**.
3. Click the **Record card** button.
4. In the **Recording badge ID** dialog enter the **ID** into the **Card no.** field. In this example the Suprema user ID is **5**.
5. Click the **OK** button to confirm.

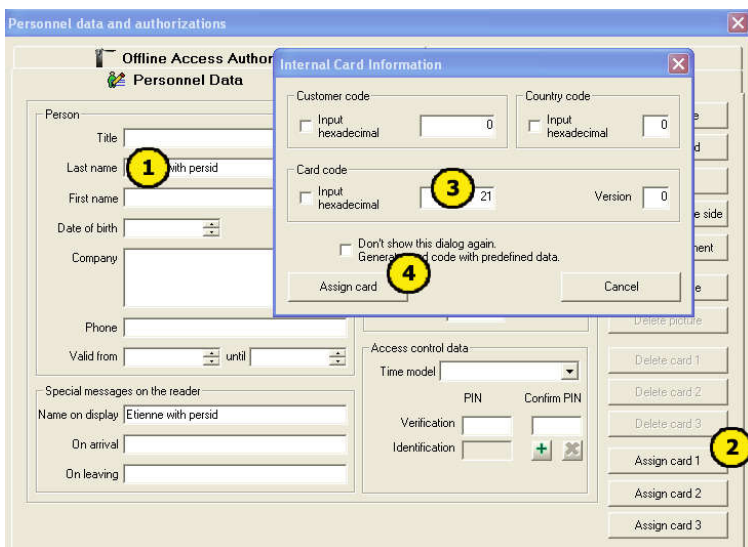
The Tester 22 has the ID 5 which has been assigned to the samecard holder in the dialog manager of the BIS client. Assign an authorization to the card holder and you will see thathe will have an access granted.

This is also to be seen in the DMS and LAC consoles



3.6.2 Access Professional Edition

To assign the **user ID** from the Suprema software, proceed as follows:



1. Define a new person in the Access PE or select an existing one.
2. Click the **Assign card 1** button.
3. Enter the User ID into the **Card code** field.
4. Click the **Assign card** button to confirm the changes.

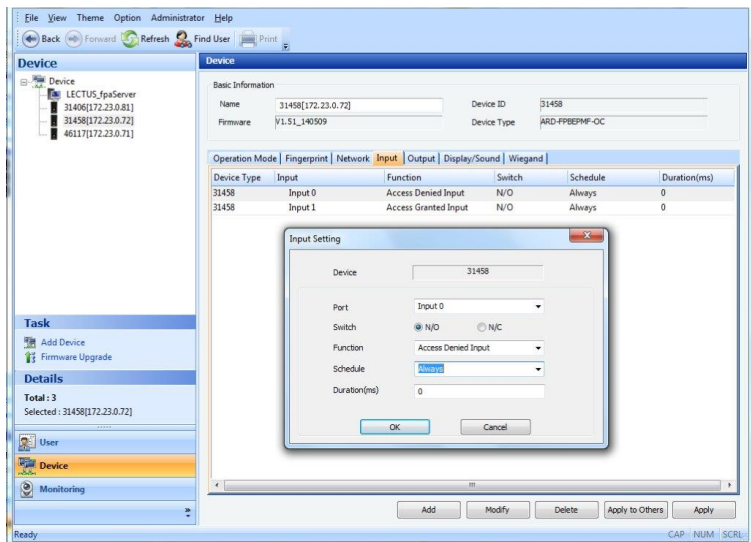
Test the card

- Present the card at the entry reader. The LogViewer will show: **not authorized**
- Assign the authorization to the card holder and he will get access granted.

3.7 Define Input Signals

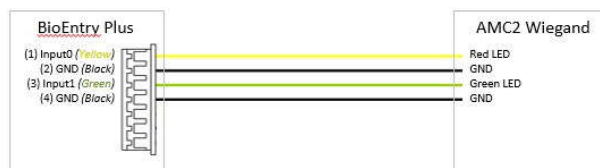
The following setting are required to control the LED of the reader with the AMC. Define input signals for **Access Denied (0)** and **Access Granted (1)**:

- Select the device
- Select Folder "Input"
- if it is the first time click on **Add**



- Input 0: Function, select: **Access Denied** Input
- Input 1: Function, select: **Access Granted** Input
- Click **OK** to continue.

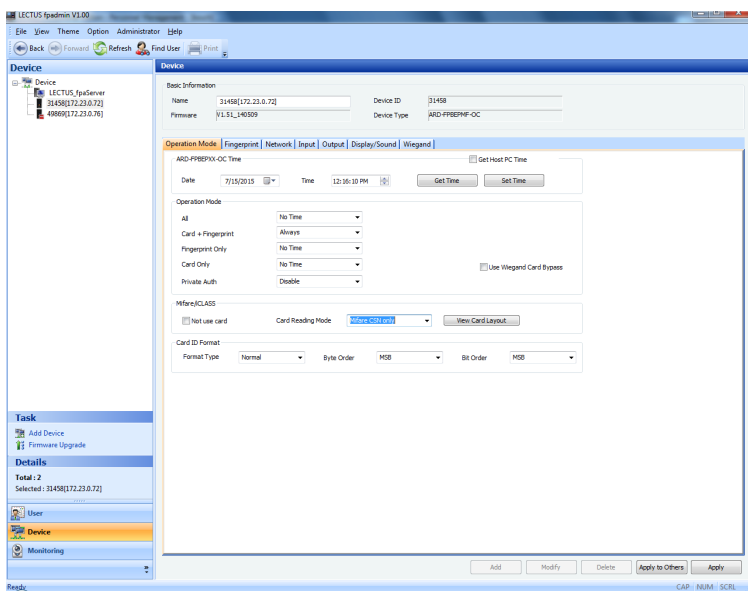
3.7.1 Connecting Diagram



3.8 How to use the BOSCH code

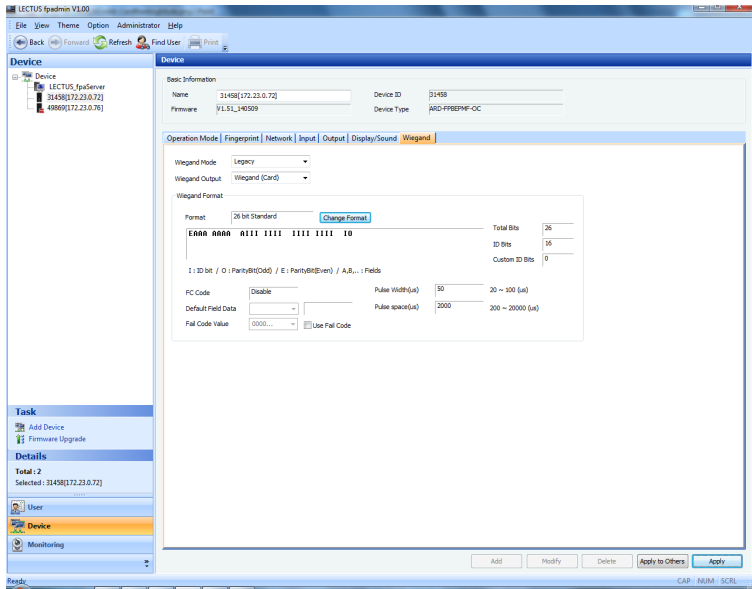
Use a Mifare Entry Plus or Bionet Lite reader as enrollment device.

3.8.1 Device Operation Mode



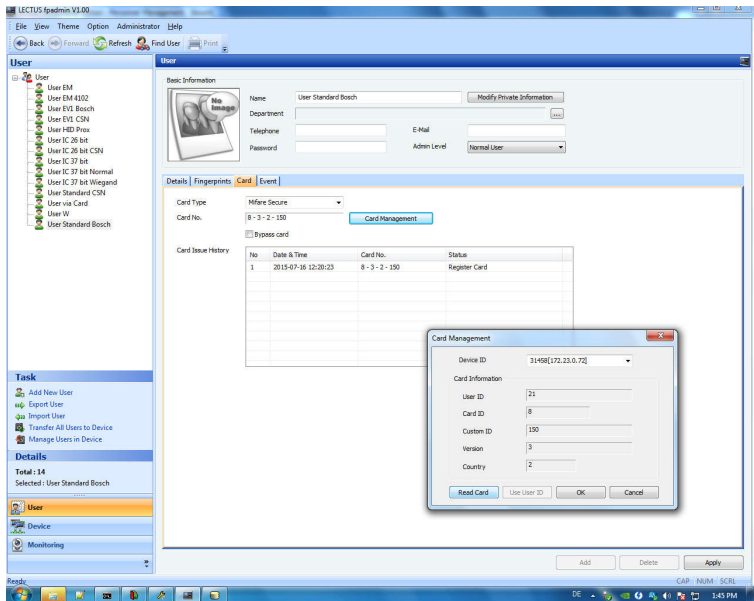
1. Select a reader device.
2. Click the tab **Operation Mode**
3. Set Operation Mode **Card + Fingerprint** to **Always**.
4. Set Card Reading Mode to the Mifare basic setting **Mifare CSN only**. The further settings for the Bosch Code are described in chapter 3.8.3.

3.8.2 Wiegand Device



1. Click the tab **Wiegand**
 2. Set Wiegand Output to **Wiegand Card**
- A change of format is not necessary.

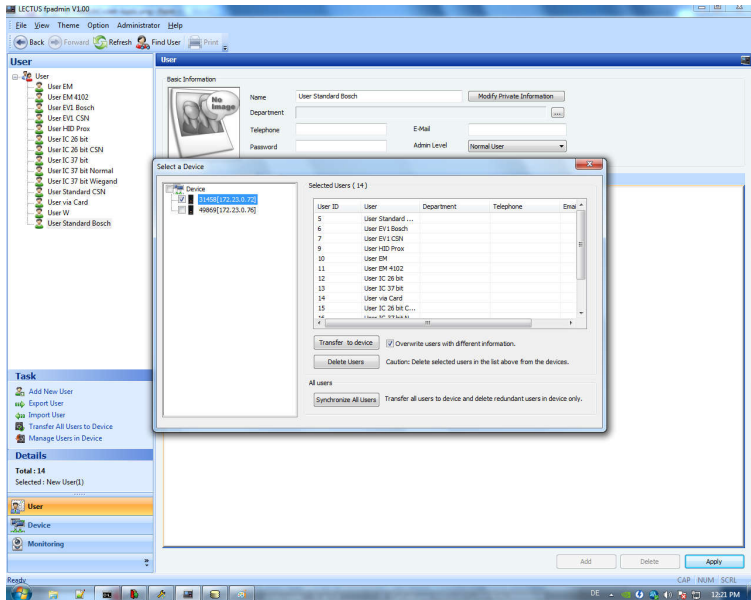
3.8.3 User Card



1. Click the tab **Card**
2. Set Card Type to **Mifare Secure**
3. Press button **Card Management**
4. Select **Device Id**
5. Press button **Read Card** -> Card values are filled in
6. Click **Ok**
7. Click **Apply**

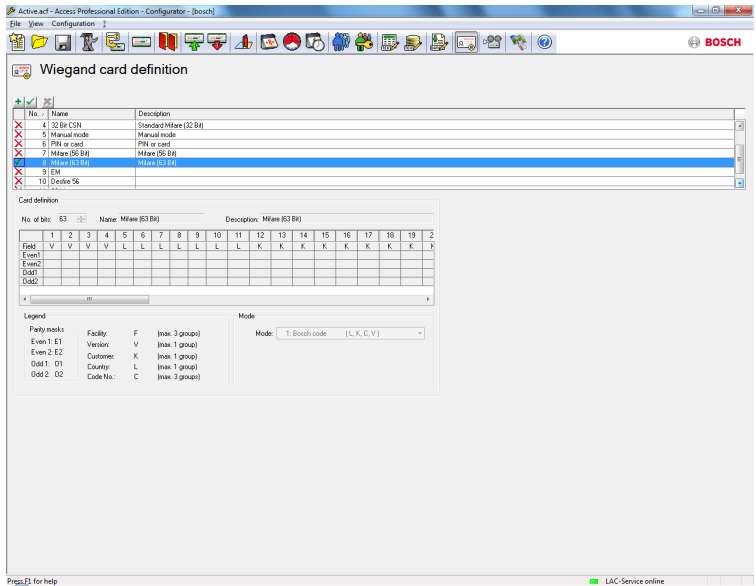
If the card ID is not unique the message **“Same card exists”** appears.

3.8.4 Transfer all users to Device



1. Select **Device**
2. Set flag **Overwrite users** with different information
3. Click **Transfer to Device**

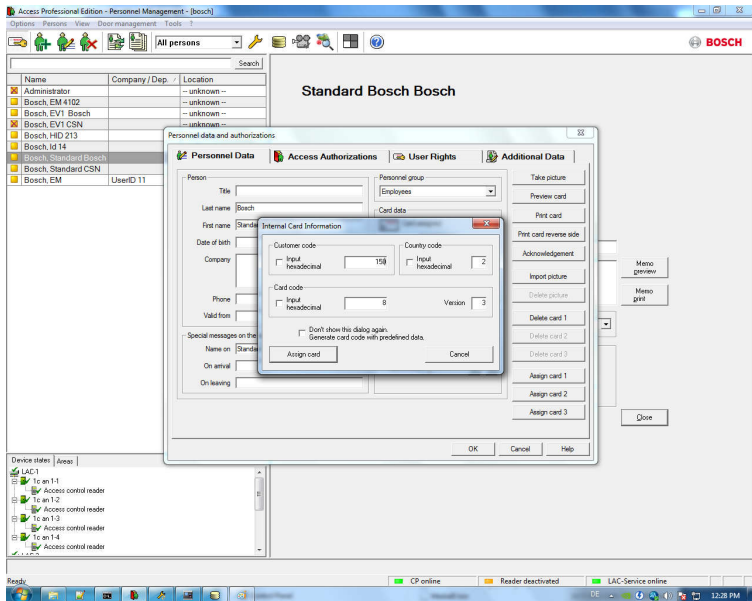
3.8.5 APE Wiegand Card Definition



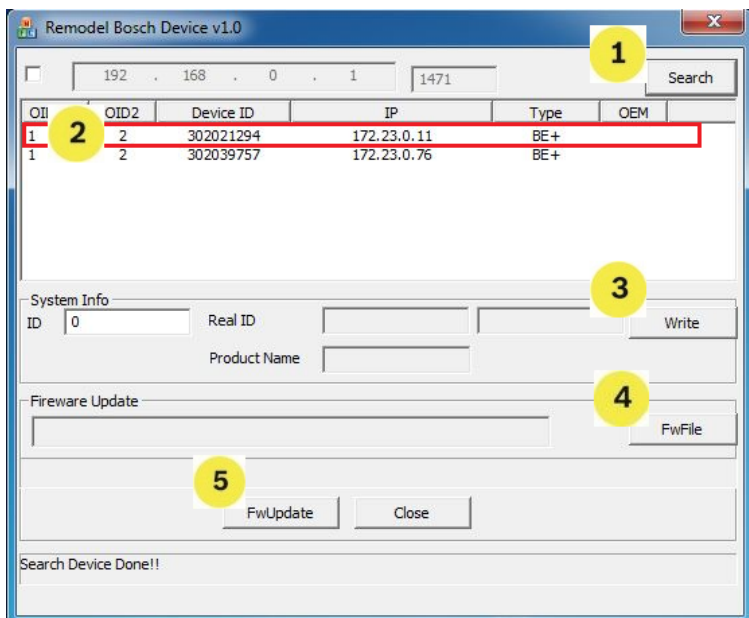
1. Select **APE Configurator > Wiegand Card Definition**
2. Set the **63 bit** card type active.

3.8.6 APE Personnel Management

1. Select **APE Personnel Management**
2. Assign the correct Bosch coded card



4 Bosch Migration Tool



Migration

Go to folder C:\Program Files (x86)\LECTUS_fpa\Server\ and start the application **RemodelBoschDevice_v1.0.exe**.

1. Click **Search** to search for a connected device.
2. Select a device to migrate
3. Click **Write** to write the Bosch ID into the device.
4. Click **FwFile** to select a firmware file to upgrade
Make sure to select the proper upgrade file.
5. Click **FwUpdate** to upgrade the selected device.
A "success" pop-up window appears if the firmware has been successfully upgraded.

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH,
2016