Adatis Door Terminals

Manual

ADATIS

Version History

Version	Date	Author	Comment
1.4	14.11.2019	mfriedrich	Initial creation based on firmware version 6.006.XXX
1.5	9.12.2019	mfriedrich	Update / Bug fixes
1.6	4.2.2020	mfriedrich	Changes in chapter 4.2.2 and 4.2.6
1.7	10.02.2020	mfriedrich	Update

Content

1 General

1.1 Adatis door terminals

The Adatis door terminals can be classified according to their functional scope. The TouchEntry series includes door communication terminals that can also be used for access control. The door terminals of the FaceEntry series are biometric access terminals, the XT version also includes an intercom function.

The manual describes the following door terminals:

- TouchEntryXS
- TouchEntryXT
- FaceEntryXS
- FaceEntryXT

Each door terminal has an LCD display and a website. Only the most important settings can be configured via the LCD display. All settings can be accessed via the website. Chapter 2.3 provides information on how to access the settings on the LCD display and on the website.

1.2 About this manual

This manual is intended to describe the complete range of functions of all the Adatis door terminals mentioned, from commissioning to complex applications. In order not to overload the document, reference is sometimes made to other documents in which the functions are described in more detail.

Not every function is available on all door terminals. Chapter 1.3 therefore describes which functions are supported by which device type.

The manual refers to the firmware version mentioned in the version history.

Adatis reserves the right to add new functions or to extend or remove existing functions in future firmware versions. This also applies to changes to the scope of delivery, form, technology and equipment. Therefore, no claims can be derived from the information and illustrations in this manual.

This manual often talks about enrollment. This means setting up access control for PIN, RFID and face.

1.3 Functions of the door terminals

The manual is designed for the FaceEntryXT where all functions are available. All other door terminals are limited in their functionality. The restrictions can affect the following topics:

- PIN
- RFID
- Biometry (face recognition)
- Intercom (Communication)
- Video

The symbols are placed at the beginning of the chapters when the corresponding function is accessed within the chapter. For example, if the symbol is next to the heading, this means that RFID is used in this chapter and that a door terminal without RFID may not have the full functionality discussed in this chapter.

The following table shows the functions of the respective door terminal:

	PIN	RFID	Biometry	Intercom	Video
TouchEntryXS	✓	optional	✗	✓	✓
TouchEntryXT	✓	✓	✗	✓	✓
FaceEntryXS	✓	optional	✓	✗	✗
FaceEntryXT	✓	✓	✓	✓	✓

Note: If you do not know which device type your door terminal is, chapter 5.11.1 can help you.

2 Commissioning

2.1 Power supply

Depending how the door terminals have been ordered, they can be connected via the Ethernet cable or 2-Wire.

If connected via Ethernet cable, power can be supplied either via Power over Ethernet (PoE or PoE Plus) or via a power supply unit.

Note: Please take care that when using Power over Ethernet a power supply unit must not be connected at the same time.

If the door terminals are connected via 2-wire, the 2Wire Converter from Adatis must be used. Power is supplied via 2-wire. Further details can be found in the document *'Manual-2Wire-Converter'*.

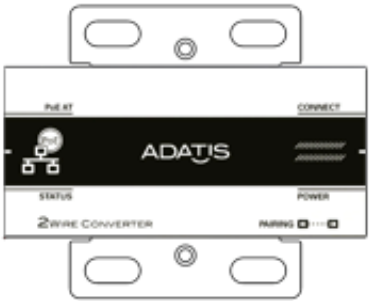


Figure 1: 2Wire-Converter

2.2 Starting the door terminal

As soon as the power supply has been connected, the door terminal starts.

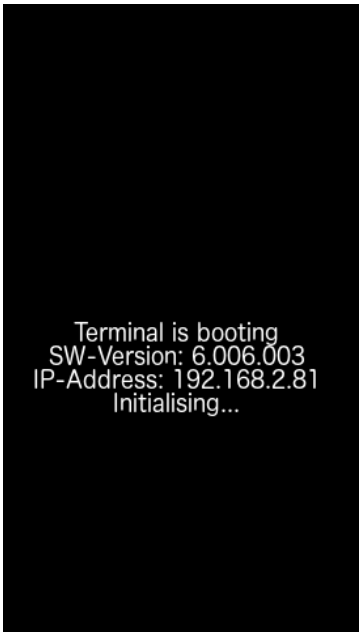


Figure 2: Door terminal during booting

While the door terminal is booting, the firmware version (SW version) and the IP-Address are displayed.

In the factory default setting, the IP address is set to the following address:

192.168.2.**81**

In order to be able to access the website of the door terminal, it is usually necessary to change the IP address directly after the first start.

Changing the network settings, especially the IP address, is described in Chapter 2.5.

As soon as the door terminal has been started, the start page of the door terminal appears on the display. The start screen differs depending on whether it is a door terminal with or without intercom functionality.

2.2.1 Start screen with intercom function

Figure 3: Start screen with intercom function

Two groups have already been added to the start page on delivery. These groups are only intended as examples and have no function.

Persons can be assigned to these groups.
How to add persons to the personal database is described in chapter 4.1.
How to edit a group and assign a person to it is described in Chapter 4.4.

The text *'Adatis GmbH'* can also be changed using chapter 5.3.1

Using the magnifying glass at the top right corner, it is possible to search the personal database for the name of a person in order to be able to call them afterwards. Chapter 4.3.6.2 describes this.

2.2.2 Start screen without intercom function (FaceEntryXS)

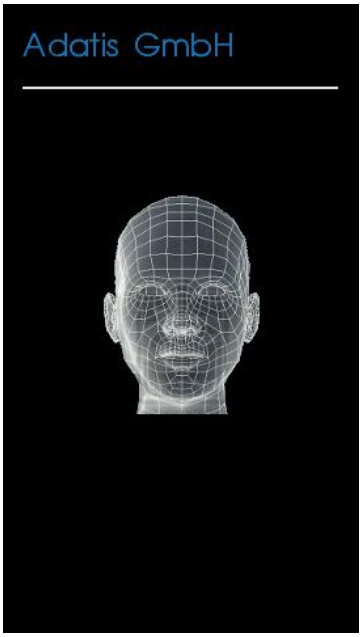


Figure 4: Start screen without intercom function (FaceEntryXS)

The start page shows the mesh mask of a face.

By touching the face, a positioning assistance for access via face recognition is displayed. (See chapter 4.2.4.3)

The text *'Adatis GmbH'* can be changed individually with the help of chapter 5.3.1.

2.3 Open the settings

The door terminals can be configured via the LCD display or via the website.

2.3.1 Configuration on the LCD display

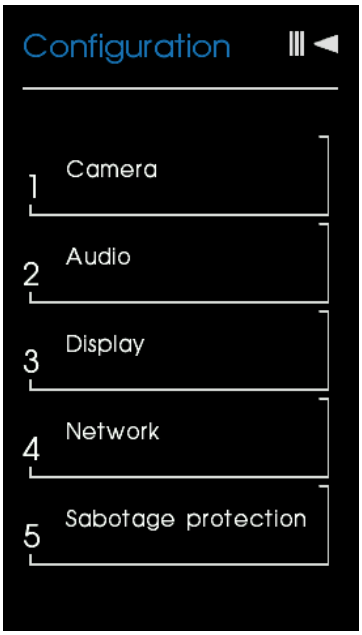


Figure 5: Setting options in the configuration on the LCD display

Camera: Here you can set the positions of the camera. (See chapter 5.6.5.2)

Audio: Here you can set the volume of the input and output. (See chapter 5.6.4)

Display: Here you can set the brightness of the display. (See chapter 5.3.3)

Network: Here you can configure the network settings, especially the IP address. (See chapter 2.5)

Sabotage protection: Here you can check the Trigger-Inputs and, if necessary, the sabotage contact. (See chapter 5.8.3)

Note: For safety reasons, the configuration on the LCD display is closed after 30 seconds, without any interim input.

2.3.1.1 Opening the configuration with the red configuration card

If the door terminal was ordered with RFID option, two RFID cards are supplied. The door terminal is preconfigured with these two cards before delivery.

If the red card is held in front of the RFID reader, the configuration on the LCD display is opened.

Note: If the door terminal is reset to factory settings, the preconfiguration of the RFID cards is lost. In this case, when the first RFID card is held in front of the door terminal, a message appears stating that the RFID card has been added for the enrollment, regardless of its color and whether the card has already been assigned to a person. The second card held in front of the door terminal is trained to open the configuration on the LCD display. Also in this case the color of the card and whether the card has already been assigned to a person is irrelevant.

Chapter 2.4.2 describes in general how to train the service RFID cards.

2.3.2 Opening the settings on the website

The website of the door terminal can be accessed directly via its IP address. As described in chapter 2.2, the following IP address is usually used during commissioning:

192.168.2.81

To open the website, simply enter the IP address into your browser.

Note: Please keep in mind that the access to the website is only possible in the same subnet. Chapter 2.5 describes how to change the IP address of the door terminal.

2.3.2.1 Login to the website

After opening the website, the login window appears.

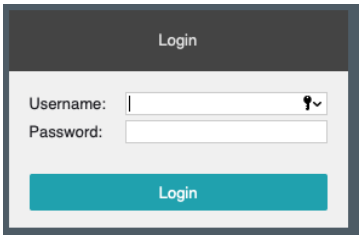


Figure 6: Login to the website

The registration data at commissioning are:

Username: **admin**
Password: **1234**

2.3.2.2 Changing the Admin Password

Changing the password for the admin is possible via the menu item *'Login/Logout'*. The username *'admin'* cannot be changed.

Note: After changing the password, the login is only possible with this password. The password can no longer be changed or read from outside the website. If the password is lost, it will no longer be possible to log in to the door terminal. The password must be kept in a safe place.

2.3.2.3 Setting options on the website

Figure 7: Website of the door terminal

Home: Shows an overview of all settings.

People: Allows the creation and editing of persons in the database. (See chapter 4)

Groups: Allows creating groups and assigning people to these groups. (See chapter 4.4)

Login/Logout: Here you can find the settings for the login to the website and the service RFID cards (See chapter 2.4).

System information: Shows all important information about the door terminal. (See chapter 5.11.1)
It is possible to set up a syslog server. (See chapter 5.11.3)

Menu Configuration:

- One- or two-column display of the groups (See chapter 4.4.2.1)
- Displaying the phone book or keypad (See chapter 5.3.2)
- Preview image during call (See chapter 5.6.3)
- Time recording (See chapter 5.4)
- Setting the idle screen (See Chapter 5.3.4)

Basic settings:

- Language (See chapter 5.2)
- Date and time (See chapter 5.1)
- Brightness of the LCD display (See chapter 5.3.3)

Network settings: The network settings of the door terminals can be configured here. (See chapter 2.5)

Administration settings: Allows changing the settings to manage the personal data via an administration server.
(See chapter 5.10)

SIP configuration: The door terminals use the SIP standard to establish VoIP communication with the remote stations. Here you will find the settings for SIP, in particular the registration of the door terminal on a SIP server (See chapter 4.3.3) and the call or connection timeout (See chapter 5.6.2).

Audio/Video: The settings for the input and output of audio and the camera / video image can be found here. (See chapter 5.6.4 respectively 5.6.5)

Interface configuration: The settings for the relays and the trigger inputs are in this section. They can be tested here.
(See chapter 5.8)

EventHandler: Here it is possible to edit the EventHandler file.
(See chapter 5.9)

Access options: Here it is possible to delegate the management of the access to an access server.
(See chapter 5.10.3)

Upload/Download: Here it's possible to
update the firmware (See chapter 5.11.4.1),
upload/download the device configuration (See chapter 5.11.2)
and upload/download the personal database (See chapter 4.5).

Camera: The camera view can be shown here.
The Motion JPEG video is used for this. (See chapter 5.7)

Diagnosis: Data that provides information for troubleshooting is available here. (See chapter 6.2)

2.4 The Service RFID Cards

If the door terminal is equipped with the RFID option, two RFID cards are included in the scope of delivery.

2.4.1 Functions of the Service RFID Cards

Before dispatch, the two cards are trained as follows:

Figure 8: Enrollment Card

The enrollment view is opened by holding the green card in front of the reader of the door terminal.

At this point it is possible to select a person and enroll this person for the following access options:

- PIN
- RFID
- face recognition

Note: Before it is possible to start the enrollment for a person, the person must be created in the personal database.
(See chapter 4.1)

Further information about the enrollment via the LCD display can be found in chapter 4.2.1.

Figure 9: Configuration Card

By holding the red card in front of the reader of the door terminal, the configuration is opened on the LCD display.

Chapter 2.3.1 shows, in an overview, which settings can be configured on this screen.

You can see that the two cards have been trained on the door terminal website, on the *'Login/Logout'* page. There the UID of both cards is displayed.

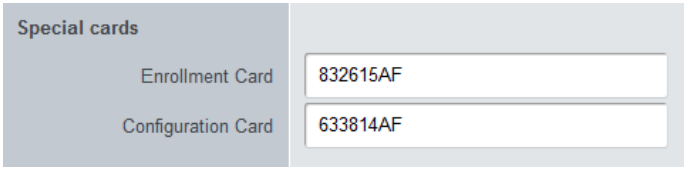


Figure 10: UID of the service RFID cards on the website

2.4.2 Training of new Service RFID Cards

If you want to train the cards again, you can either enter the UID manually on the website or first delete the old UIDs of the cards.

The cards are trained again by holding the RFID cards in front of the reader. The door terminal then interprets the first RFID card as a green (enrollment) card and the second as a red (configuration) card, regardless of the color of the RFID cards and whether the cards have already been assigned to a person or not.

Note: It does not make sense to delete the UID of the cards on the website without training new service RFID cards. The possibility of an unauthorized person training their own RFID cards is a security risk.

2.5 Changing the Network Settings

Each change of the network settings is acknowledged on the LCD display by the following message:

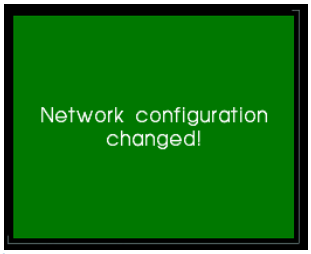


Figure 11: Notification when changing the network settings

2.5.1 Network Settings on delivery

In the delivery state, the IP address of the door terminal is the following:

192.168.2.81

In order for the door terminal to be locally accessible, whether from a remote station or another computer, all devices must be located in the same subnet.

Note: Changing the network settings should only be done by the network system administrator.

2.5.2 Changing the Network Settings via the LCD Display

For changing the setting via the LCD display, the configuration must be opened and the menu item *'Network'* must be selected.

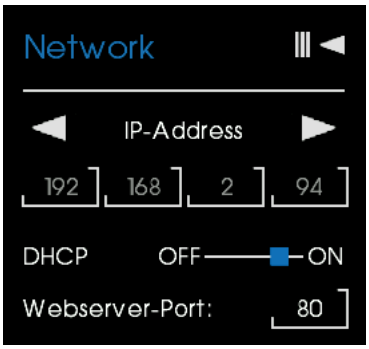


Figure 12: LCD-Display: Changing the Network Settings

Use the arrow keys to switch between the IP address, the subnet mask, the gateway address and the DNS server address.

It is also possible to enable DHCP, to fill in all fields automatically.

If a router is located within the local network, most of the time the simplest and safest solution is to enable DHCP.

How to change the web server port is discussed in chapter 2.5.5.

2.5.3 Changing the network settings via the website

For the setting via the website, the menu item *'Network setting'* must be selected on the website.

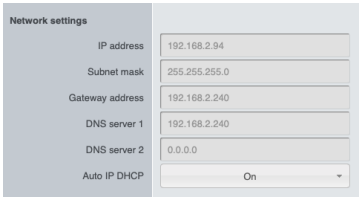


Figure 13: Website: Changing the Network Settings

The IP address, the subnet mask, the gateway address and the DNS server addresses can also be changed on the website.

If a router is located within the local network, most of the time the simplest and safest solution is to enable DHCP.

Note: After changing the IP address, the Website of the door terminal can only be accessed via the new IP address. The web page on which the change was made is no longer valid!

2.5.4 Changing the Unit Name

Changing the unit name is only possible via the website.

Figure 14: Changing the Unit Name

The unit name can be changed via the *'Network settings'* menu item.

The default name is *'FaceEntry'* and should be renamed so that the name indicates where the door terminal is mounted.

In addition, the name should only appear once within the network to avoid confusion by the user.

Note: When searching for door terminals within the DoorKeeper software, the name entered here is displayed in the DoorKeeper software.

The unit name may only consist of letters, numbers and the hyphen. Spaces and underscores are not permitted.

2.5.5 Changing the Web Server Port

The web server port can be changed via the network setting on the LCD display (see Figure 12) and via the *'Network settings'* menu item on the web page.

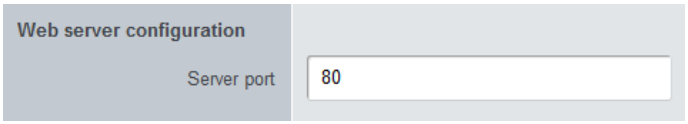


Figure 15: Changing the Web Server Port on the website

Usually the number 80 is used for the web server port. Using a number other than 80 is not common.
The port number can be changed on the web page and also on the LCD display.

After changing the web server port, the door terminal website can be reached via the following address:

<IP-address>:<Web Server-Port>

Note: The Door Terminal can also be accessed via HTTPS.
The port for HTTPS cannot be changed and is set to 443 by default.

3 Menu navigation on the LCD display

This chapter describes how to access the submenus from the start screen of the door terminal.

3.1 Start screens

Depending on the door terminal and setting, the door terminal shows one of the following start screens after start-up:

List of persons

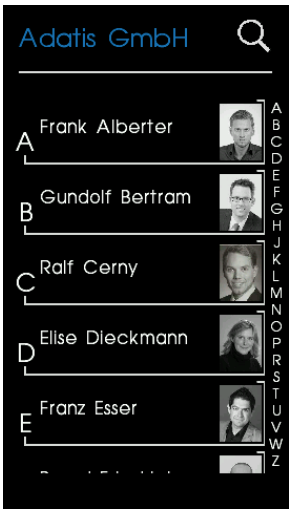


Figure 16: Start screen with list of persons

Groups

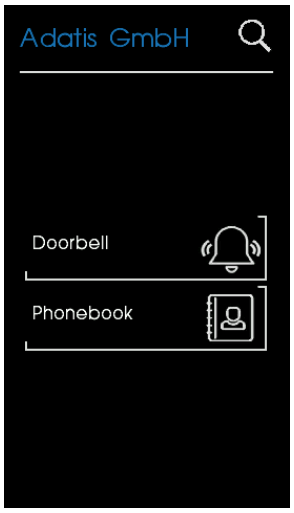


Figure 17: Start screen with groups

Keypad

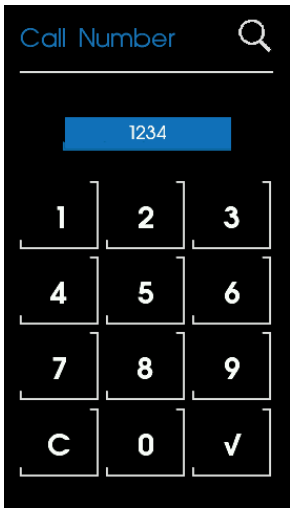


Figure 18: Start screen with keypad

Without Intercom (FaceEntryXS)

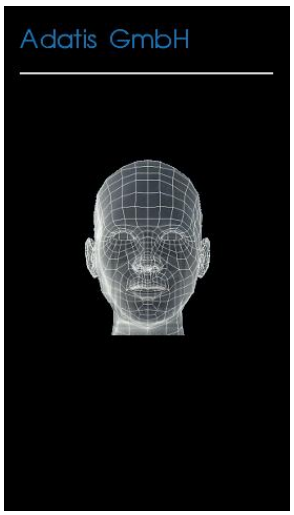


Figure 19: Start screen without intercom

3.2 Switching back to the Start screen

If a submenu is displayed, the Back button can be used to switch back to the parent menu all the way back to the start screen.

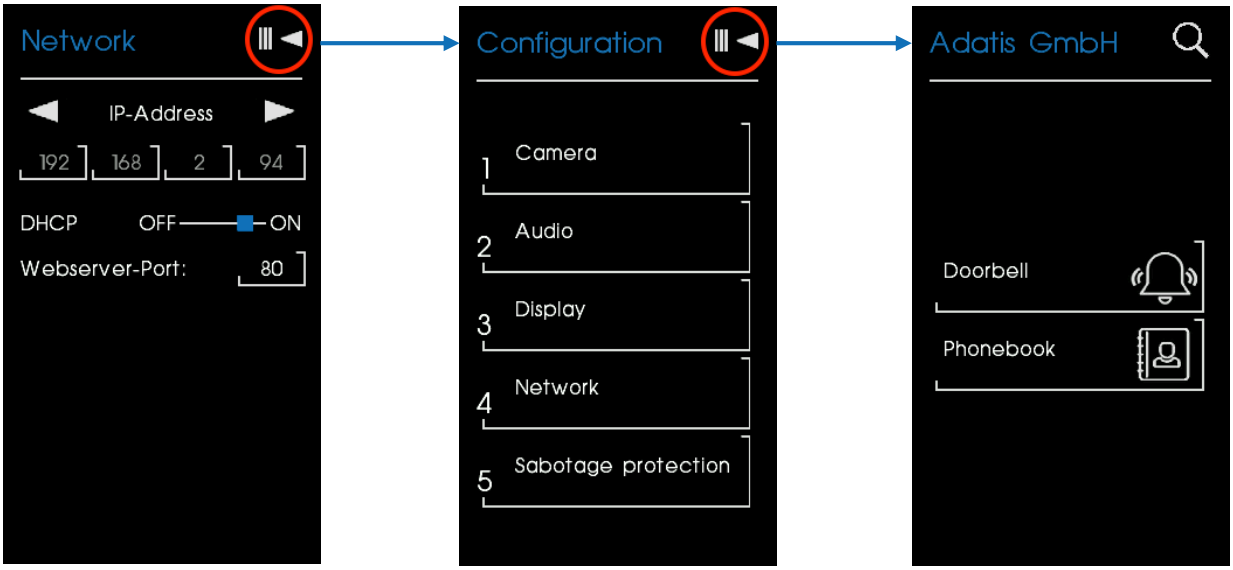


Figure 20: Example for switching back to the Start screen

Note: After 30 seconds without input, the door terminal automatically switches back to the parent menu all the way back to the start screen.

3.3 Configuration

3.3.1 Opening the configuration

The red RFID card opens the configuration on the LCD display.

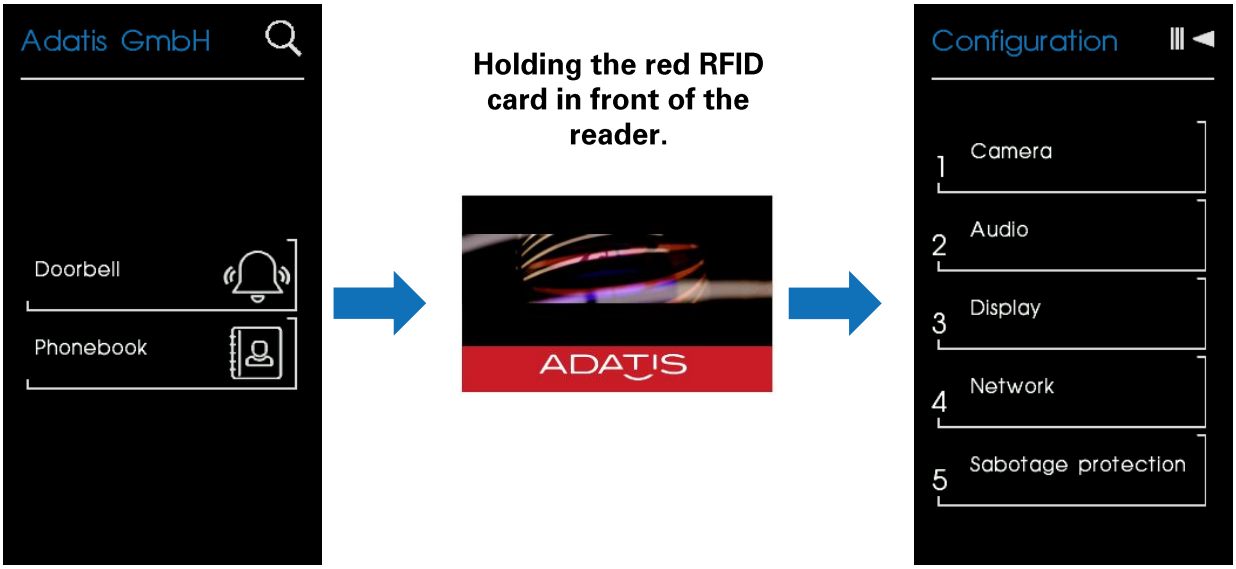


Figure 21: Opening the configuration on the LCD display

3.3.2 Submenus of the configuration

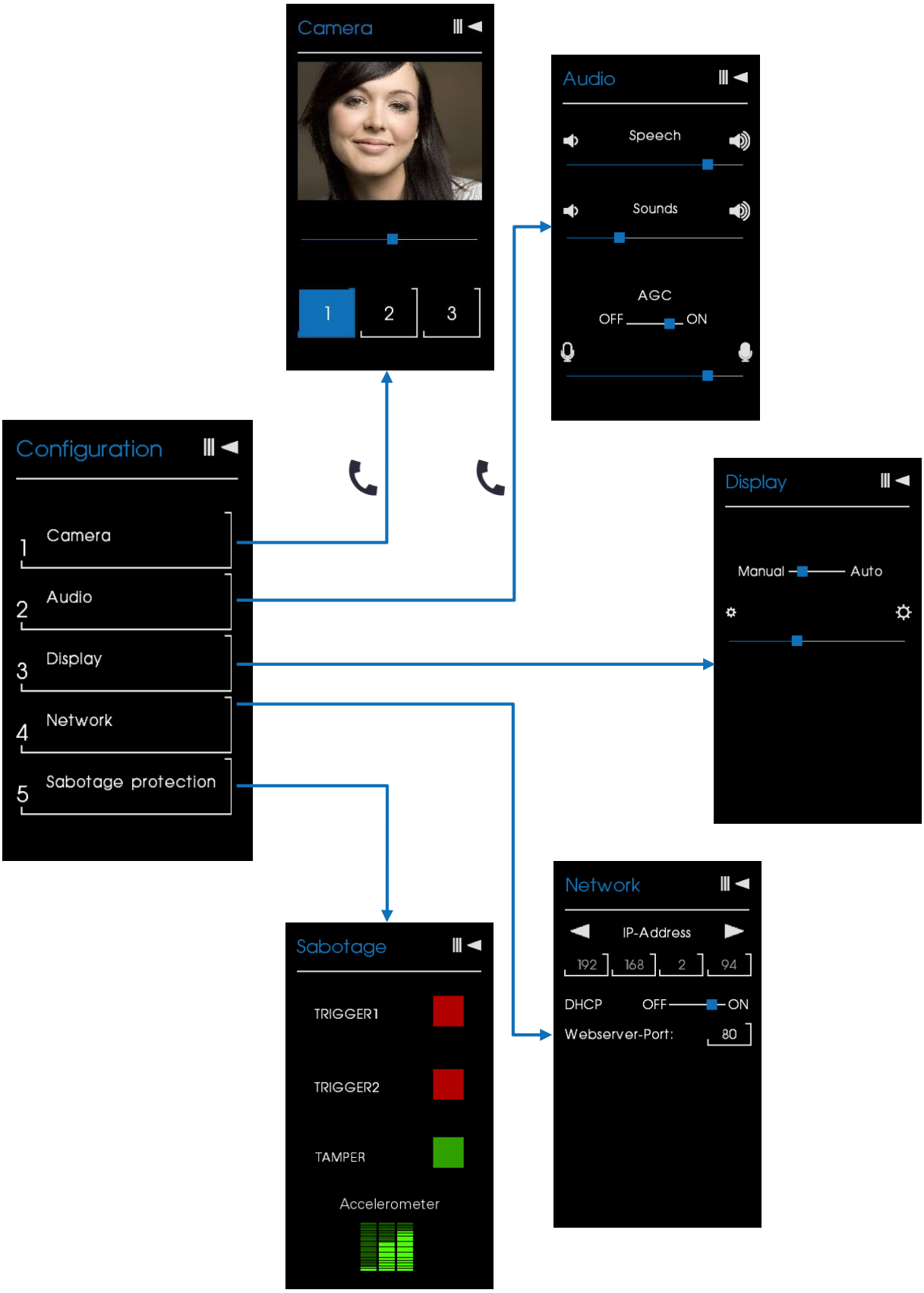


Figure 22: Submenus of the configuration

3.4 Enrollment

3.4.1 Opening the Enrollment View

The green RFID card opens the enrollment view.

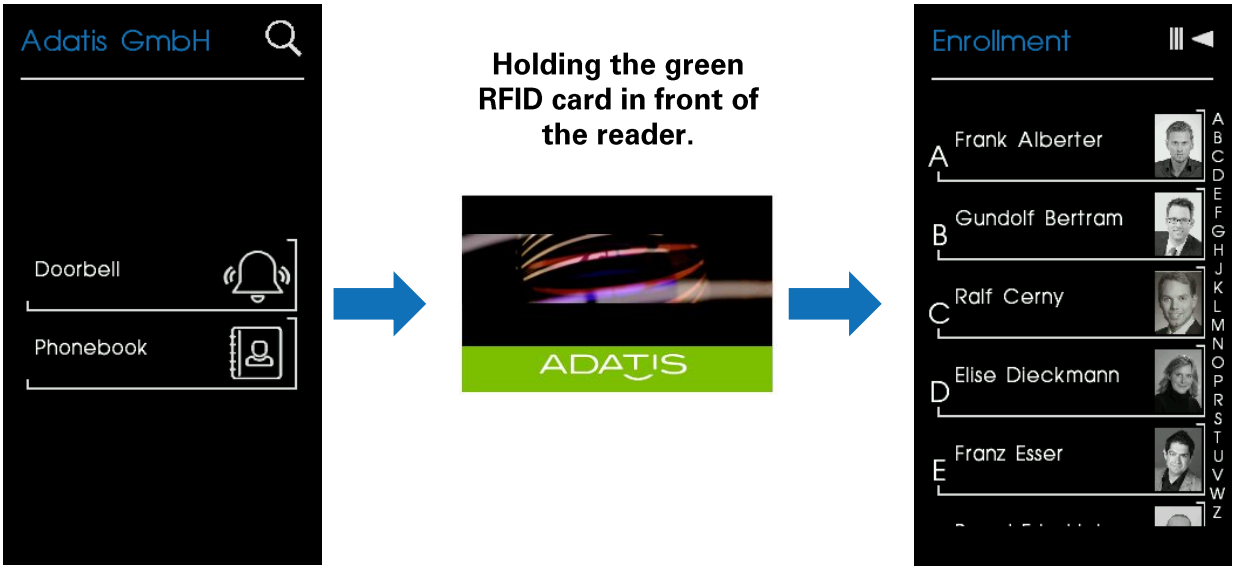


Figure 23: Opening the Enrollment View

3.4.2 Selecting a person for enrollment

The button of a person in the enrollment view opens the menu for the enrollment. Depending on the door terminal, up to three options are offered.

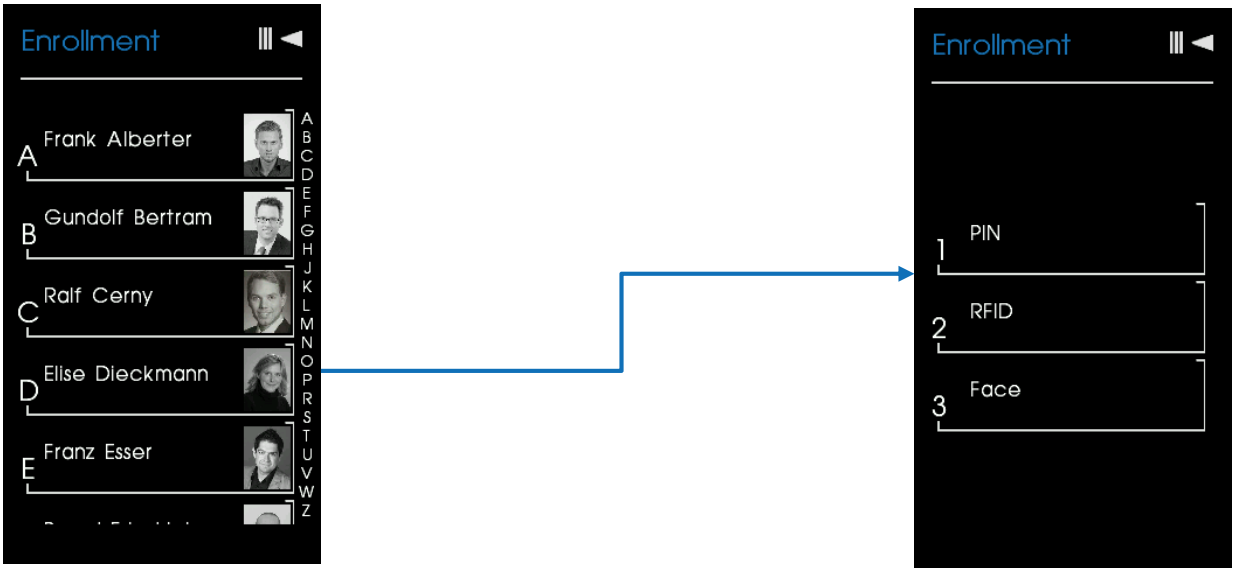


Figure 24: 3.4.2 Selecting a person for enrollment

3.4.3 Opening the enrollment options of a person

By clicking one of the buttons the enrollment for the person will be started.

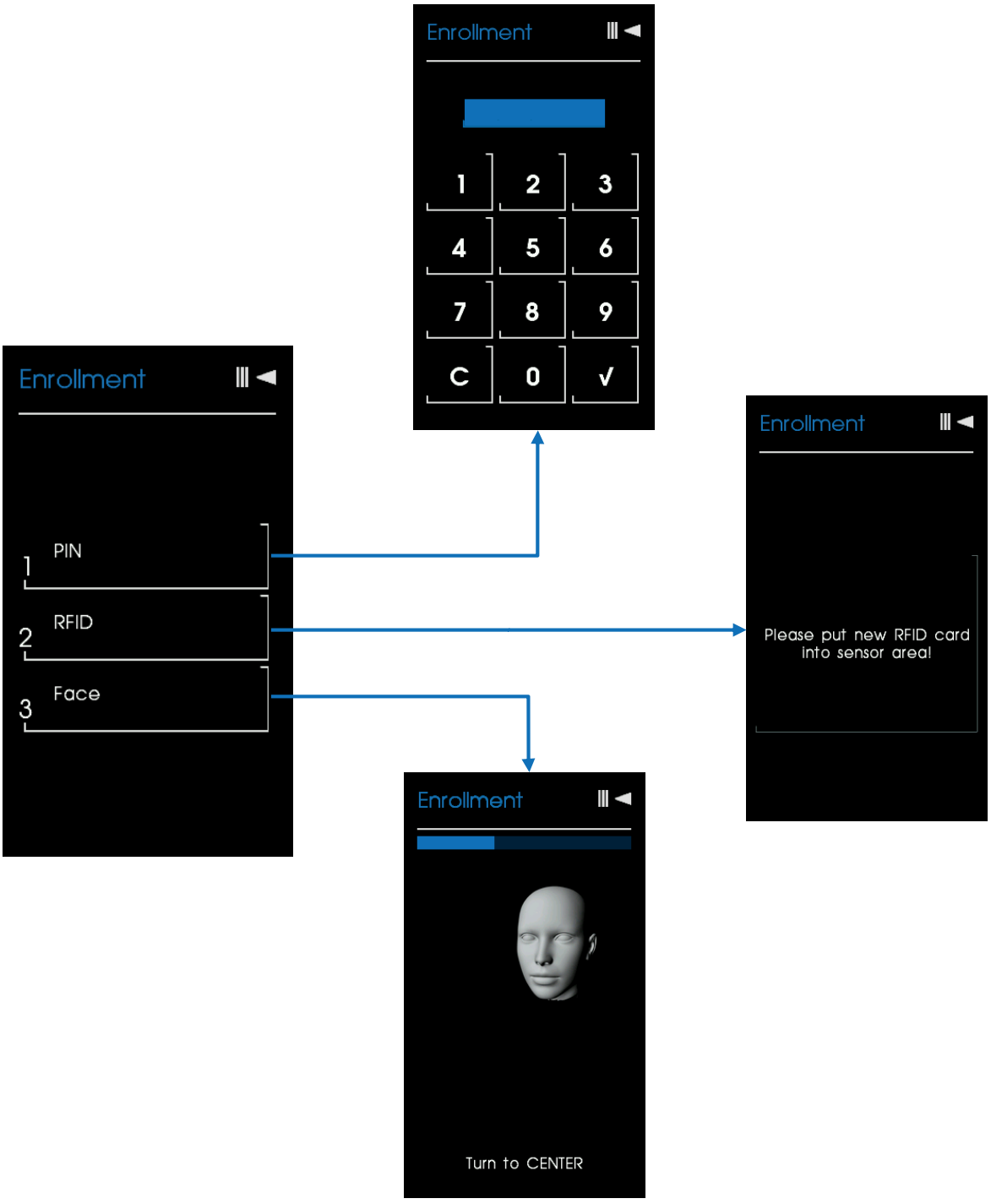


Figure 25: Opening the enrollment options of a person

3.4.4 Enrollment PIN

After entering the PIN and clicking the marked button, the PIN is saved for the corresponding person if enrollment is successful, otherwise an error message is displayed.

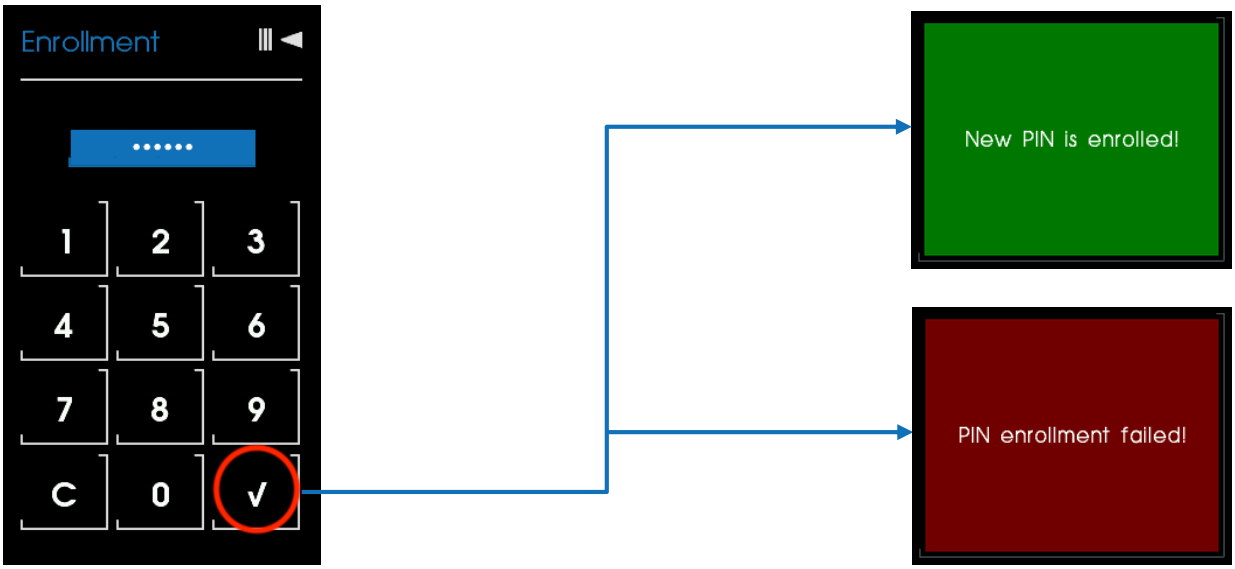


Figure 26: Menu navigation - Enrollment PIN

3.4.5 Enrollment RFID

After an RFID card has been held in front of the reader, the RFID card is registered for the corresponding person if enrollment is successful, otherwise an error message is displayed.

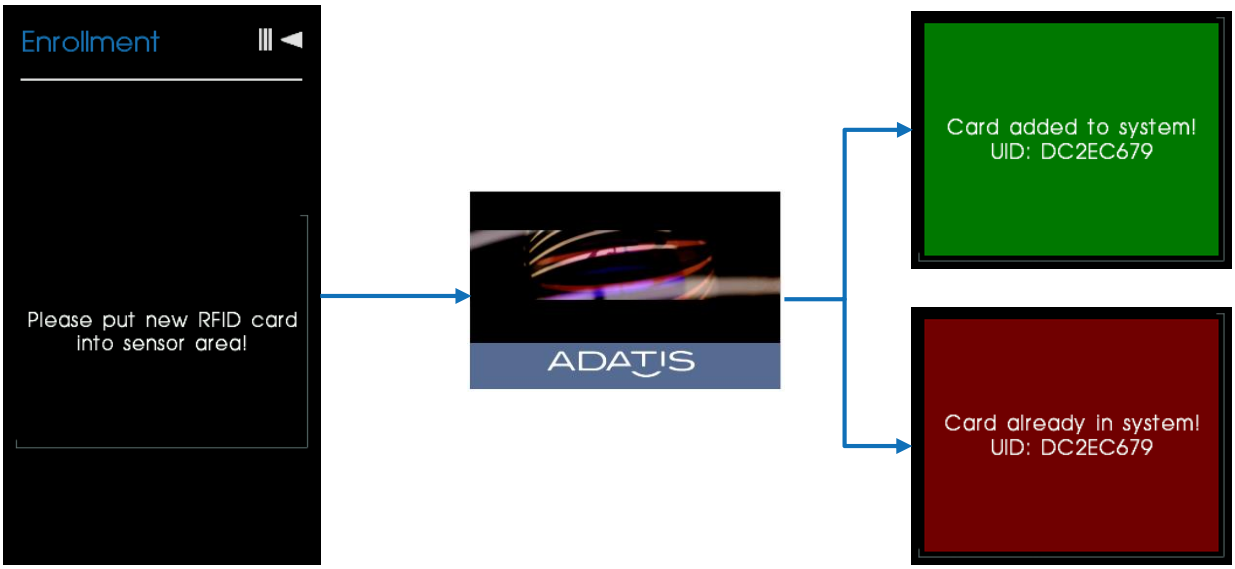


Figure 27: Menu navigation - Enrollment RFID

3.5 Access

3.5.1 Access via PIN

3.5.1.1 Opening the PIN Input

The PIN input can be called up by placing a finger on the display and then sliding the finger to the right.

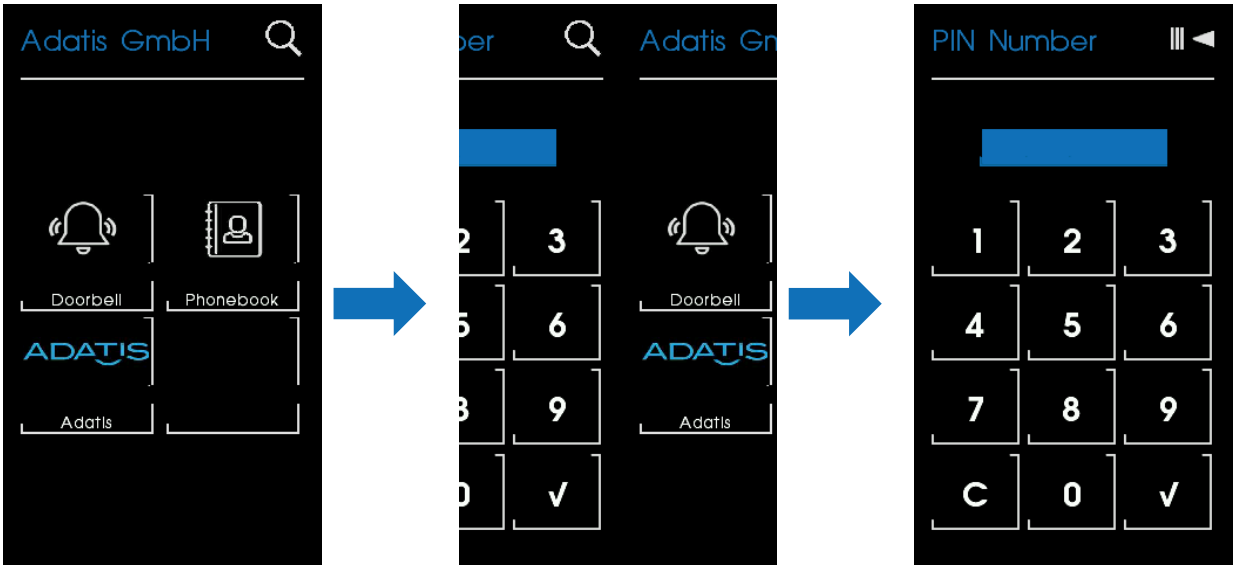


Figure 28: Opening the PIN Input

3.5.1.2 Entering the PIN

After entering a PIN and clicking the highlighted button, access is granted or an error message is displayed.

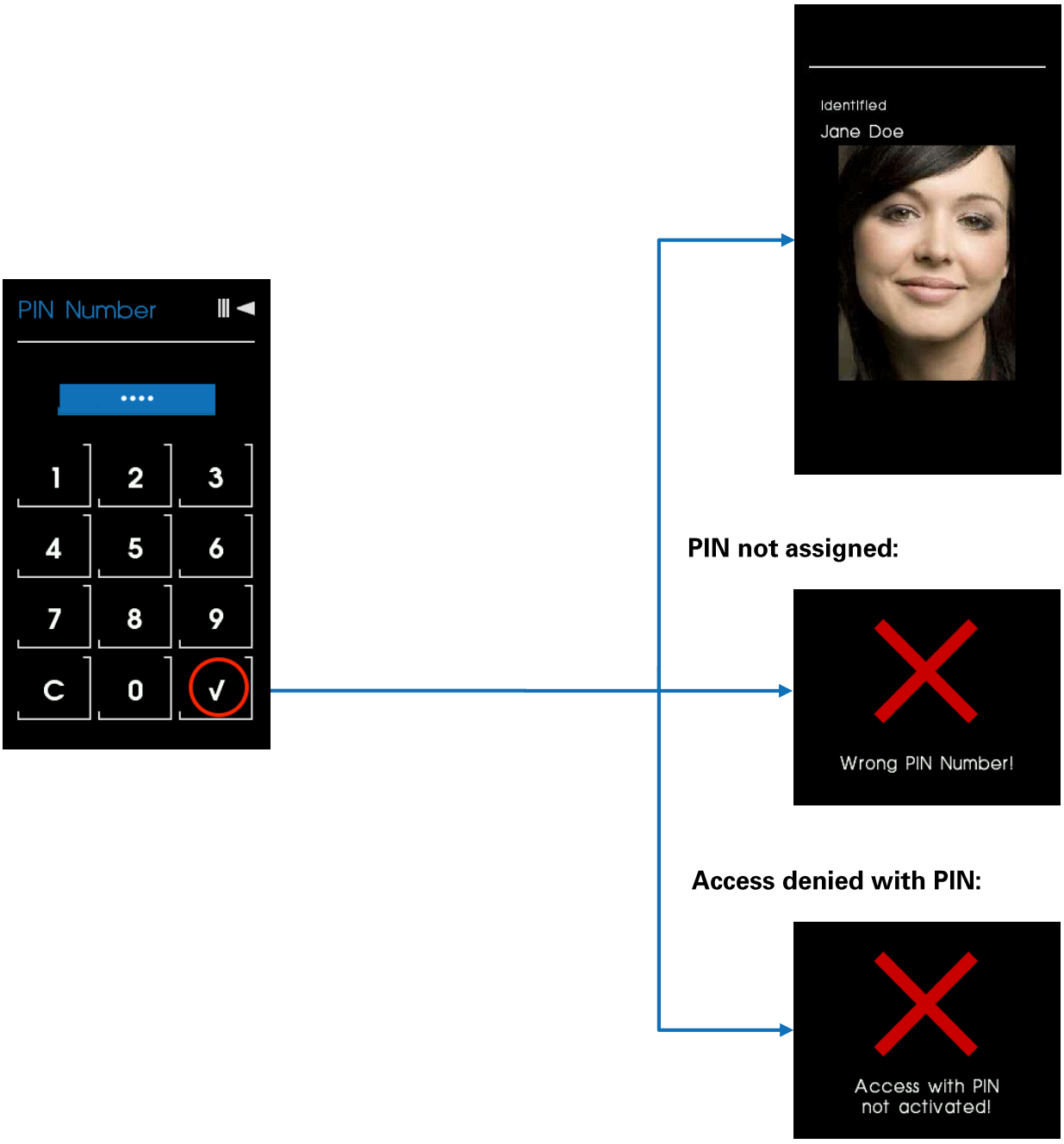


Figure 29: Menu navigation – Access via PIN

3.5.2 Access via RFID card

After an RFID card has been held in front of the reader, access is granted or an error message is displayed.

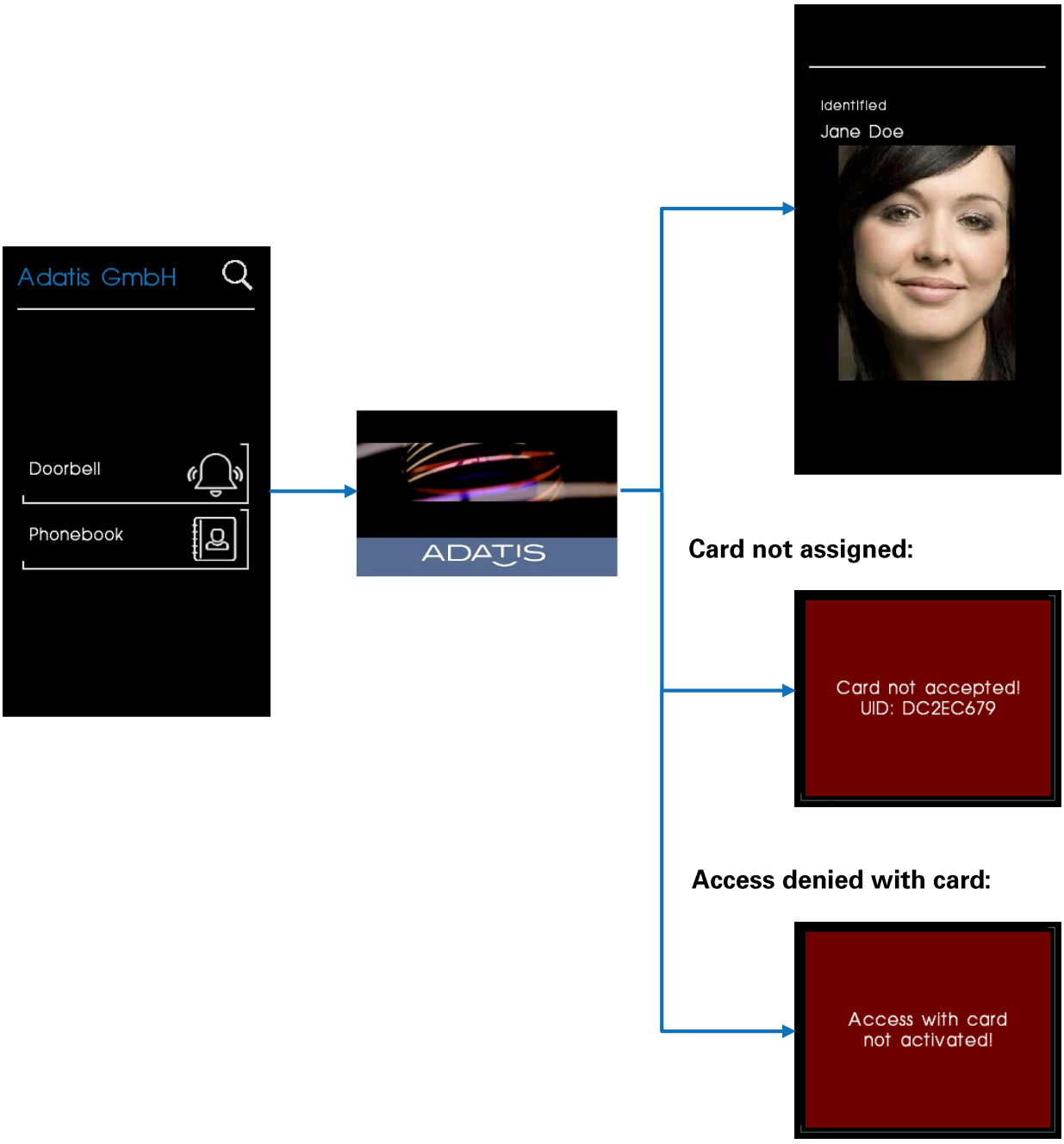


Figure 30: Menu navigation - Access via RFID

3.5.3 Access via face recognition

3.5.3.1 Getting Access via Face Recognition

As soon as a face is detected by the door terminal, the face mask will be colored blue. If the person is recognised and access is permitted for the person through the door terminal, access is granted. If access is not permitted, an error message appears.

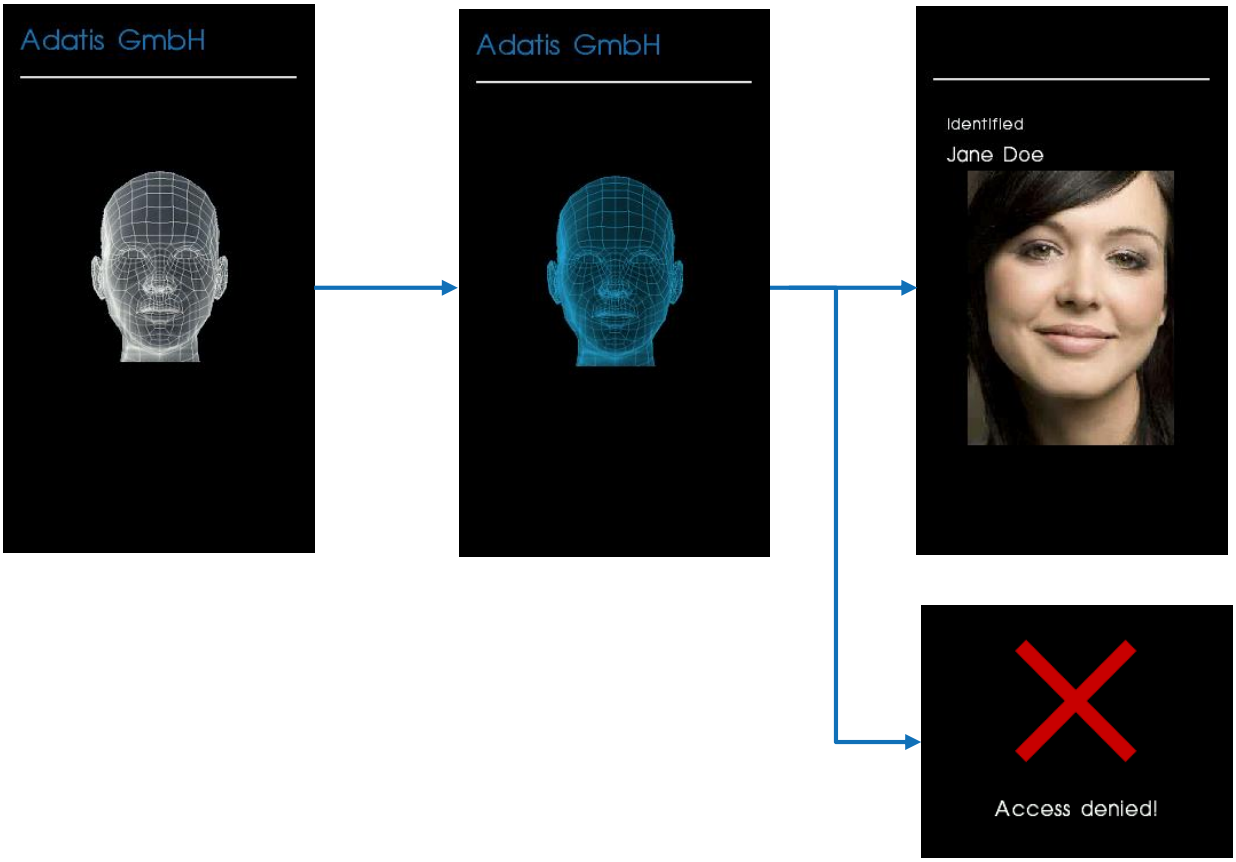


Figure 31: Menu navigation - Access via face recognition

3.5.3.2 Displaying Help for Access via Face Recognition

Display help for FaceEntryXS

Selecting the face mask will turn it blue and opens the help for face recognition.

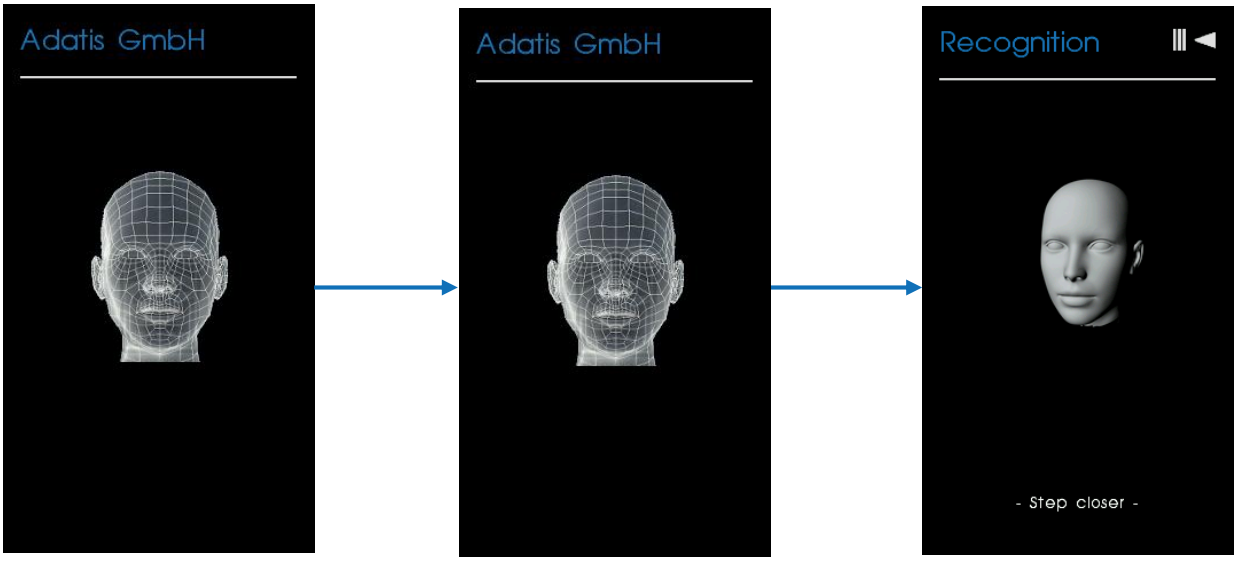


Figure 32: Display help for FaceEntryXS

Display help for FaceEntryXT

The help for face recognition can be displayed by placing a finger on the display and then moving the finger to the left.

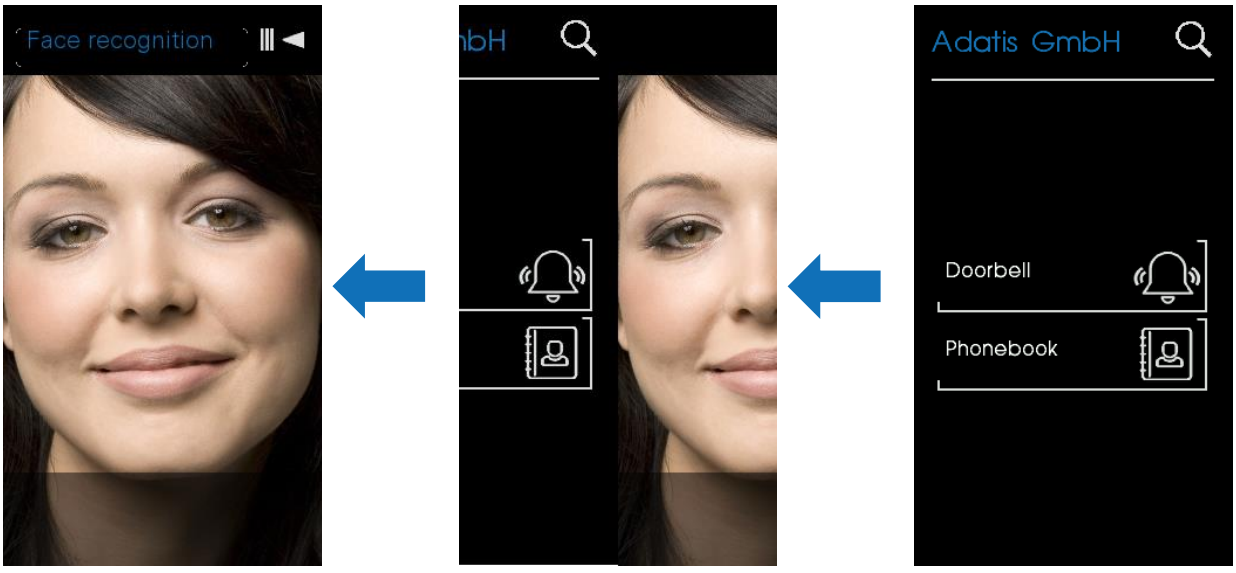


Figure 33: Display help for FaceEntryXT

3.5.4 Access in access control mode *'Wiegand Reader'*

In the access control mode 'Wiegand Reader' (see chapter 5.8.6) the LCD display shows that the access is controlled by the connected access control system:

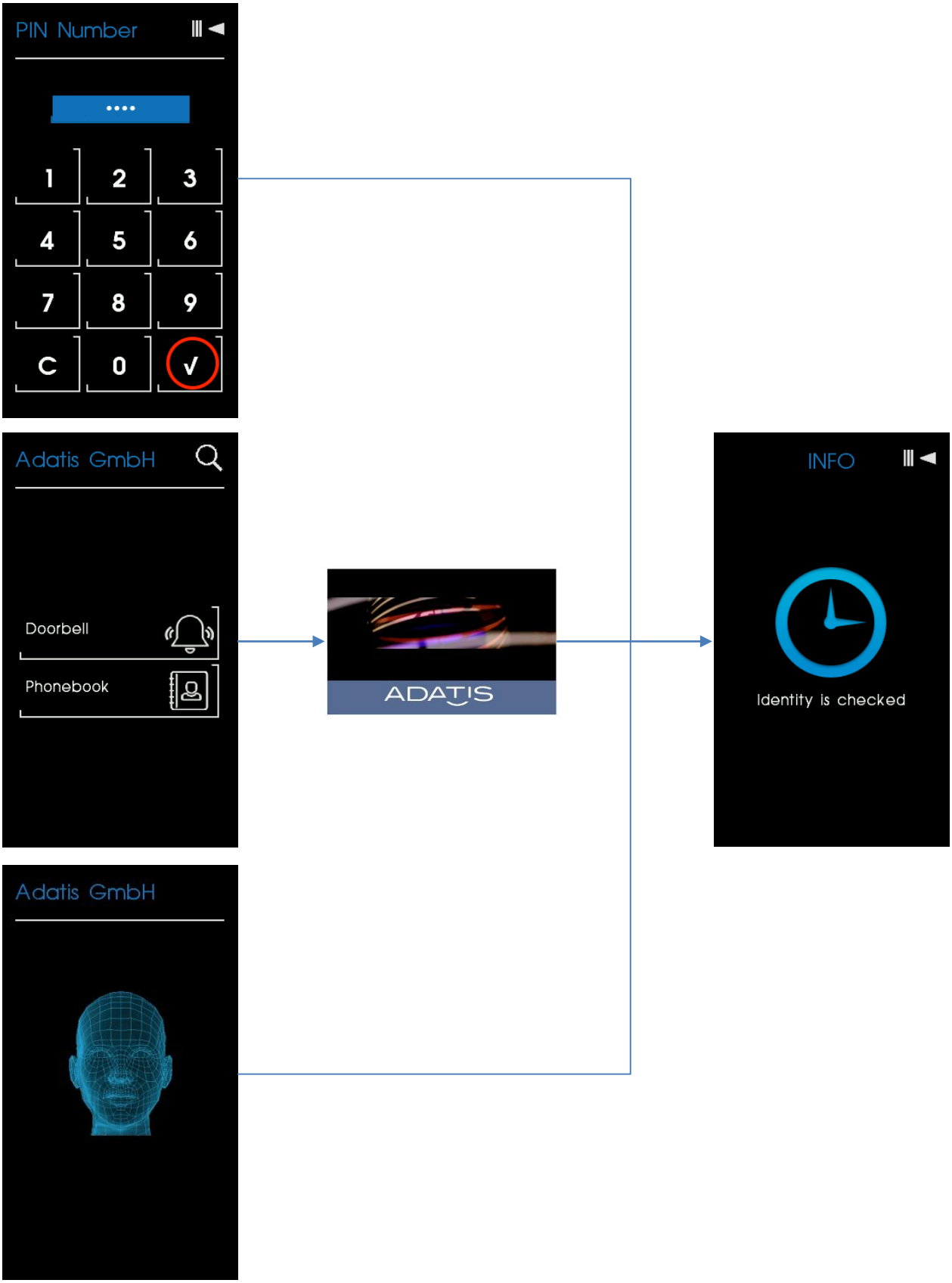


Figure 34: Access in access control mode 'Wiegand Reader'

3.6 Communicating with one person

3.6.1 Selecting a person using the search function

After entering the characters in the search field and clicking the button, the search result is displayed.

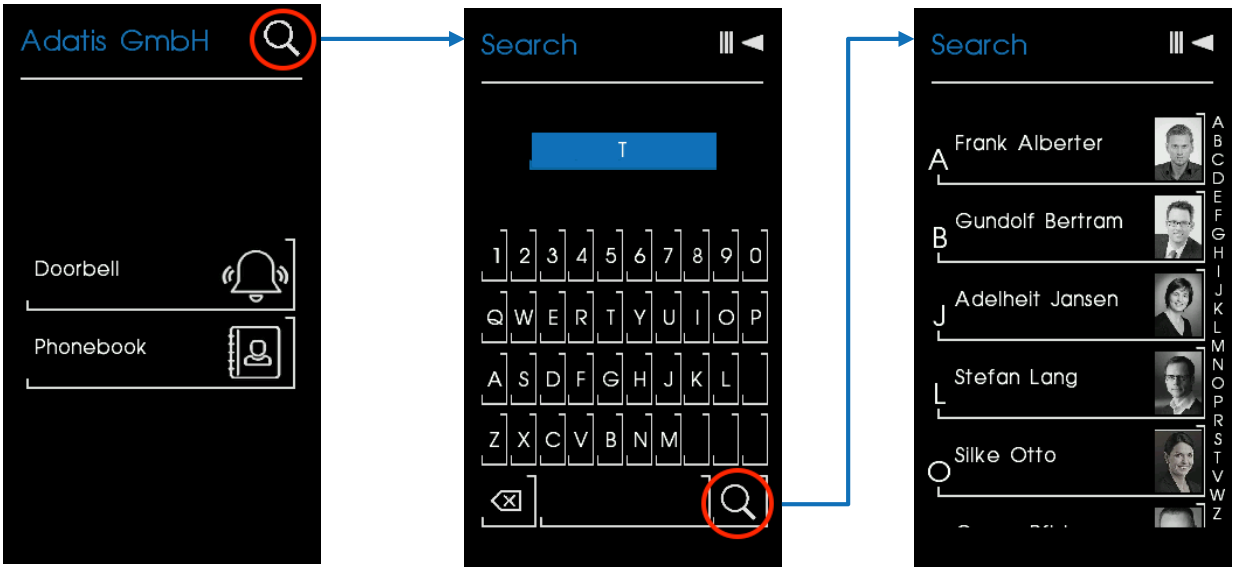


Figure 35: Selecting a person using the search function

3.6.2 Selecting a person through the groups

By selecting a group with more than one person, the list of persons which belong to the group is displayed.

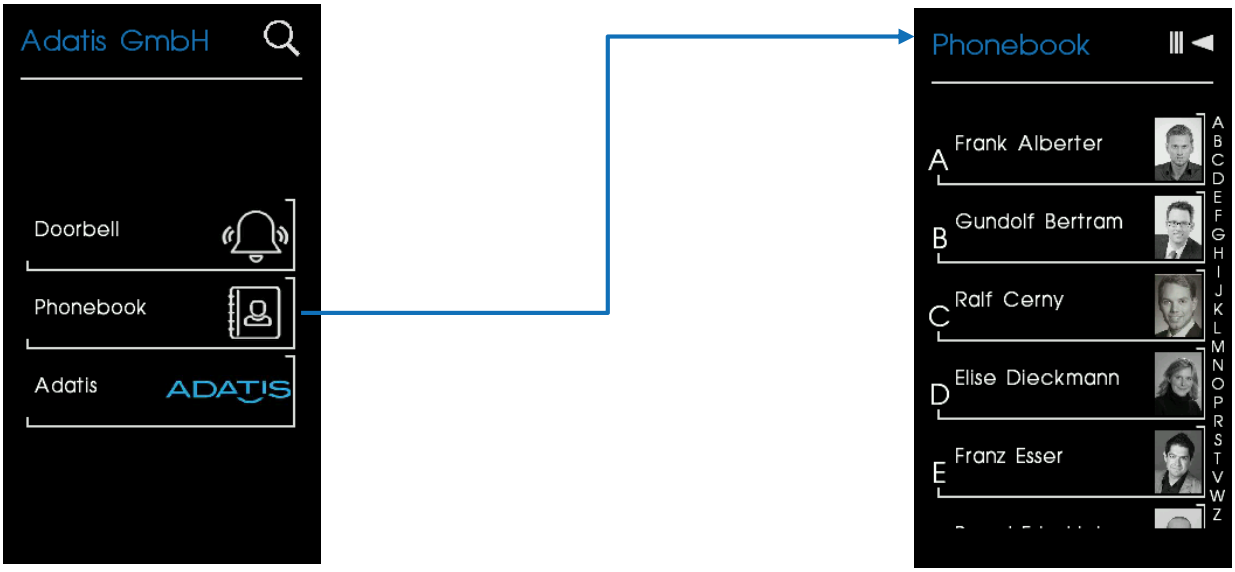


Figure 36: Selecting a person through the groups

3.6.3 Calling a Person from the Phone Book

By selecting a person from the phone book, the person is called.

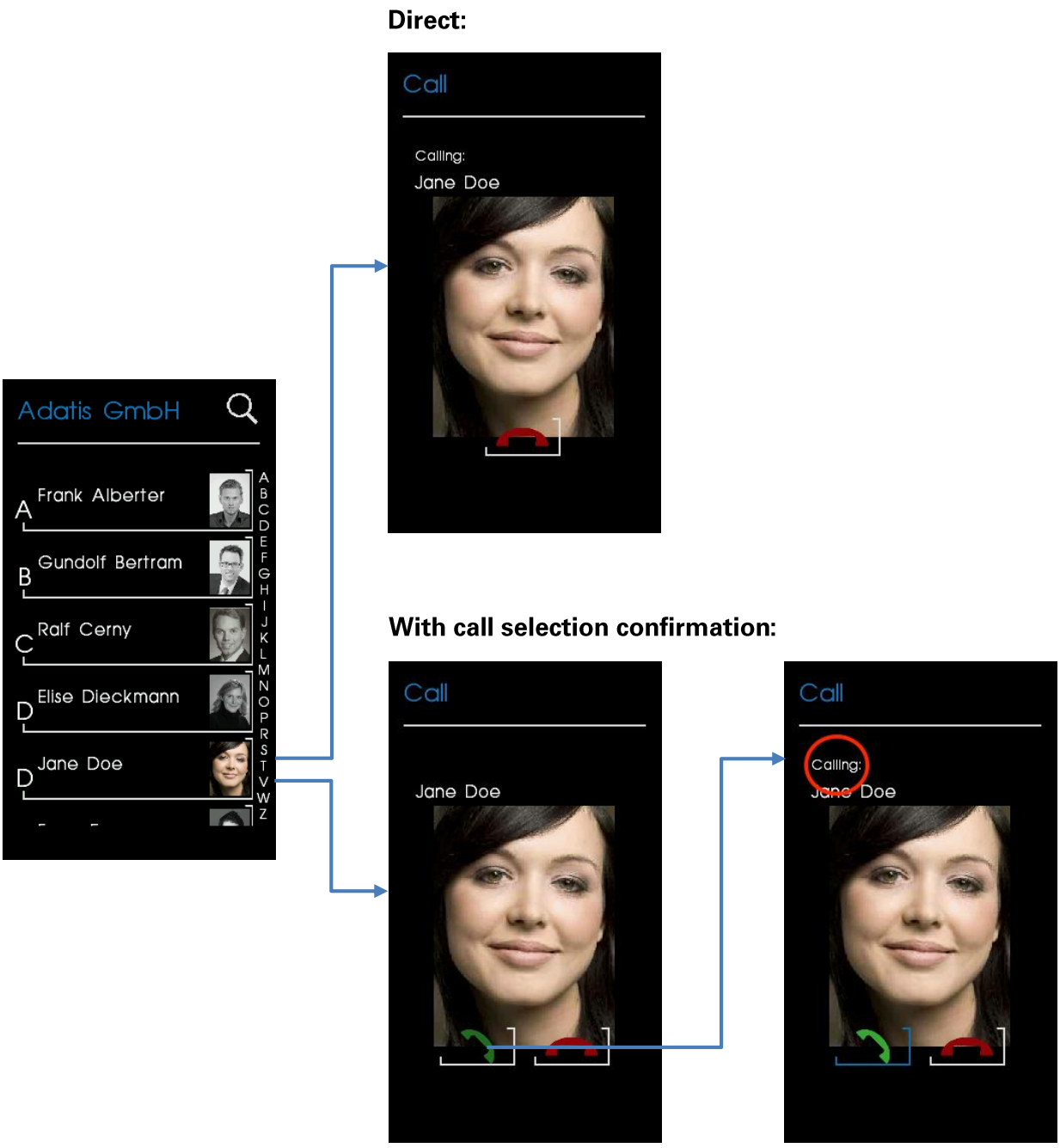


Figure 37: Menu navigation - Calling a person from the Phone Book

3.6.4 Calling a Person from the Keypad

After entering the speed dial, the person is called or an error message is displayed.

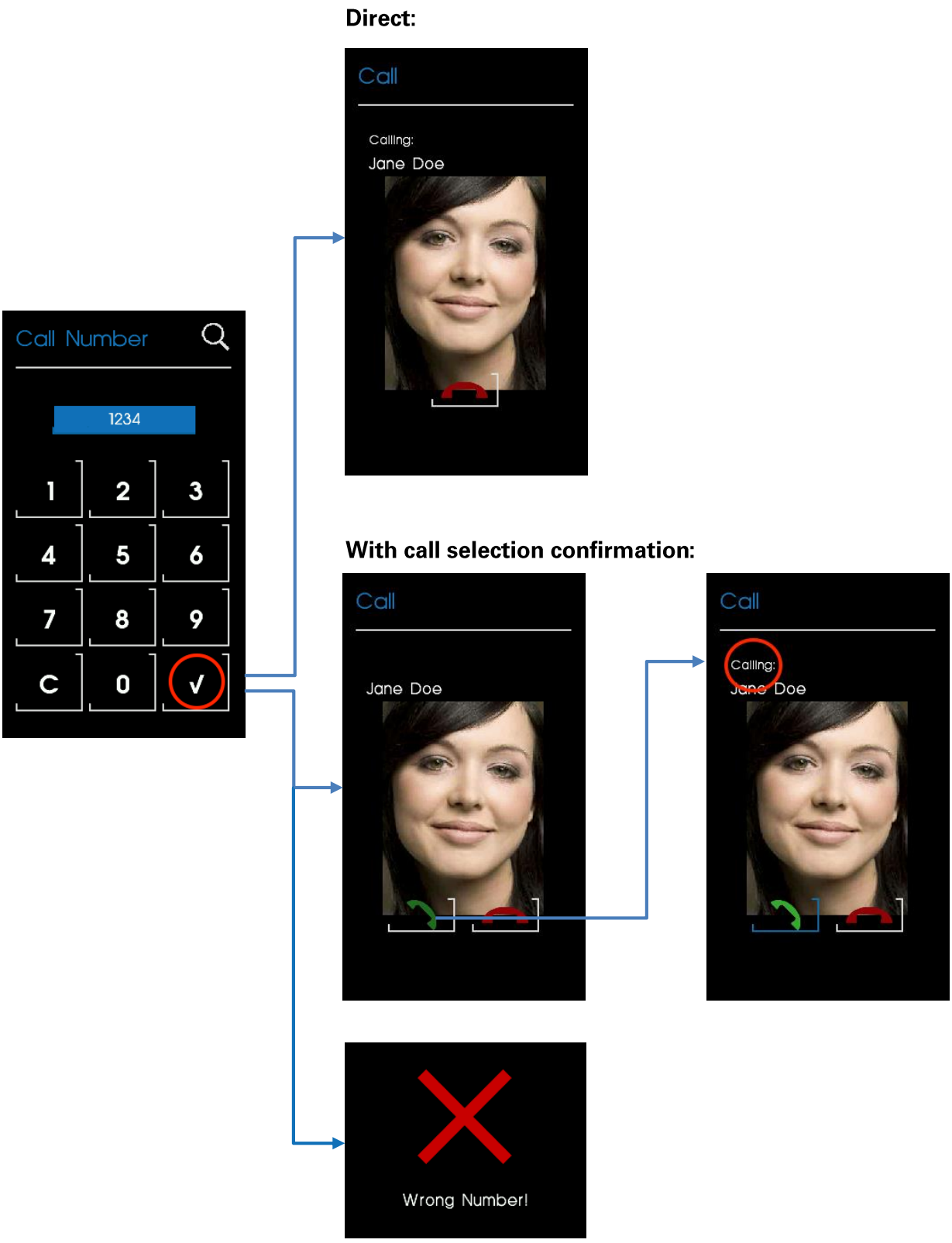


Figure 38: Menu navigation - Calling a Person from the Keypad

3.6.5 Hanging up a connection

The red telephone handset is used to terminate the connection between the door terminal and the remote terminal. Afterwards the door terminal switches to the start screen.

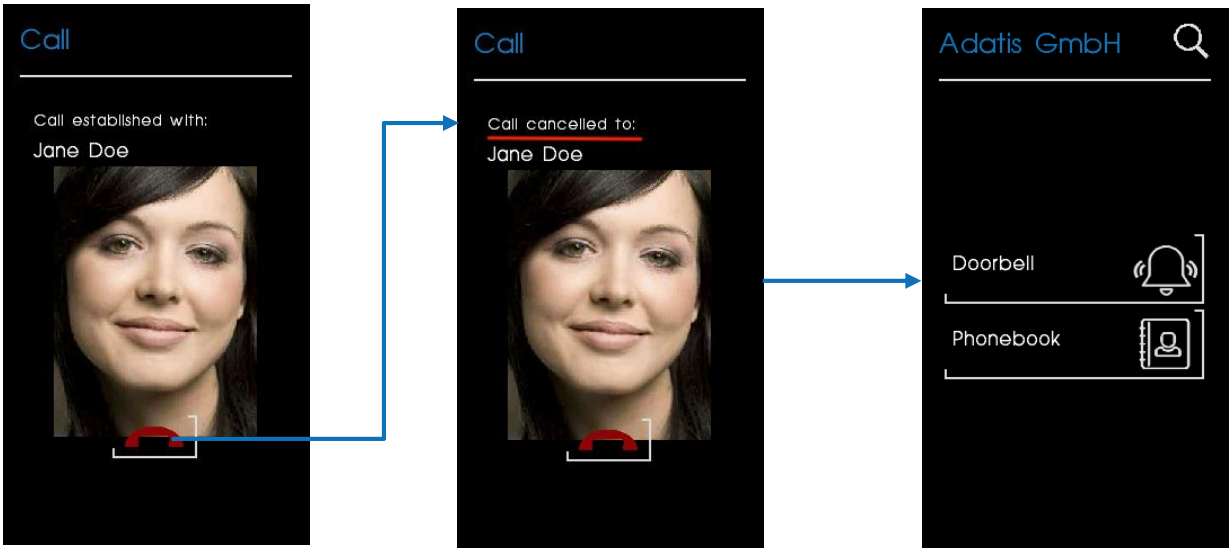


Figure 39: Menu navigation - Hanging up a connection

4 Administration of the personal data

The personal data is the central aspect within the door terminals. All persons who have been added to the door terminal together form the personal data. Persons can represent natural persons or organizational units, such as families, companies, apartments, floors, and so on. Without adding persons, it is neither possible to grant access, nor is it possible to establish communication from the door terminals.

For this reason, this chapter discusses all the possible settings that affect a person.

The following topics will be explained:

- Creating, editing and deleting persons
- Determining access for a person
- Establishing a connection to a remote station
- The group function for persons
- Backing Up and Restoring the Personal Database

4.1 Creating, editing and deleting persons

The following settings can only be made on the website of the door terminal. The settings for a person can be accessed via the *'People'* menu.

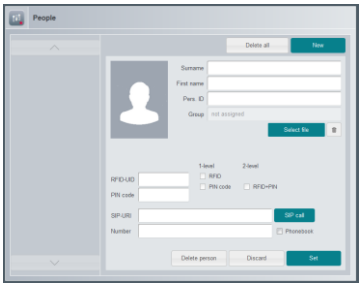


Figure 40: Menu People

On the left side is the list with all added persons. The list is sorted by surname and then by first name.

Surname/First name: The name of the person is shown on the LCD display in the phonebook, where first the first name and then the last name are shown in one line.
The phone book is sorted by surname.
If the surname is not assigned, the entry appears above the complete list. This can be used to place organizational units, such as a reception desk, at the beginning of the telephone list.

Pers.ID: A personnel number can be entered here. This number is not checked for uniqueness. It can be used if door terminals are integrated into existing access control systems.
(See Wiegand Output – Chapter 5.8.6)

Group: If the person is assigned to a group, the group is displayed here.

Select file: Here you can upload a photo for the person. By moving the slider below the image, the image can be zoomed.

RFID-UID: The number of the RFID card used for access by the person.

PIN code: The pin code used for access by the person.

SIP-URI: The Voice-Over-IP phone number to call the person.

Number: Instead of starting calls via the telephone book of the door terminal, the keypad can also be used to call the person via a speed dial. This speed dial must be entered in the *'Number'* field of the person.
Chapter 5.3.2 describes how to set up the door terminal so that the keypad can be used to enter the speed dial instead of the telephone book.
Chapter 4.3.6.3 describes how to call a person using speed dial.

Phonebook: If this option is checked, the person appears in the phone book of the LCD display and can be selected from there.

4.1.1 Creating a person

For the first person the data can be entered directly into the input mask. By *'Set'* the person is added to the database.

For further persons, the input fields first have to be reloaded with *'New'*. Adding a new person works in the same way as adding the first person.

Please note that persons do not appear on the LCD display until the checkmark in the Phone book has been set.

Note: After all persons have been added to the door terminal and the access and connection details of the persons have been defined, a backup of the personal database should be made. Chapter 4.5.1 describes how to create a backup, including the groups to which the persons are assigned.

4.1.2 Adding a picture to a person

An picture can be added by selecting the desired picture for the person on the website via *'Select file'*.

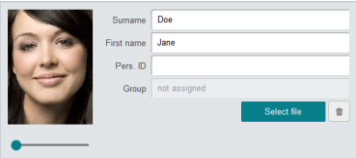


Figure 41: Adding a picture to a person

By moving the slider below the image, the image can be zoomed.

The image can be positioned with the mouse.

Depending on the door terminal, the most suitable resolution of the picture can be found in the following table:

	width (pixel)	**height (pixel)**
TouchEntryXS	**180**	**240**
FaceEntryXS	**180**	**240**
TouchEntryXT	**240**	**320**
FaceEntryXT	**240**	**320**

If the result was not satisfactory, another picture can be selected by clicking *'Select file'* again.

To delete the picture, click on the *'trash can'* icon.

Note: It is possible that an picture taken during the enrollment of the face of the person already exists.
This will be replaced by the uploaded picture, but will still be stored in the database. It is therefore possible that after deleting the uploaded picture, the picture from the enrollment will reappear. This picture can also be deleted by clicking on the *'trash can'* icon.

4.1.3 Editing a person's data

By selecting a person from the list of persons, the data of the person can be viewed. After editing the data, the changes can be updated by *'Set'*. By *'Discard'*, the changes are not applied.

Note: After changing the data, it is not possible to switch to another menu or select another person. This is only possible again after the changes have been accepted or discarded.

4.1.4 Deleting a person

A person can be removed from the database using the *'Delete person'* button.

Attention: The button *'Delete all'* offers to delete all persons. However, this also includes all groups that have been created before. The button should therefore only be pressed if the groups are to be deleted as well.

4.2 Determining access for a person

Setting up access control is called enrollment. Depending which door terminal is used, up to three of the following access options are offered.

- PIN
- RFID
- Face (resp. face recognition)

PIN and RFID can be set up directly on the door terminal's website. Alternatively, the enrollment can also be done on the LCD display. Access control via face can only be set up on the door terminal's LCD display.

4.2.1 Setting up access control on the LCD display

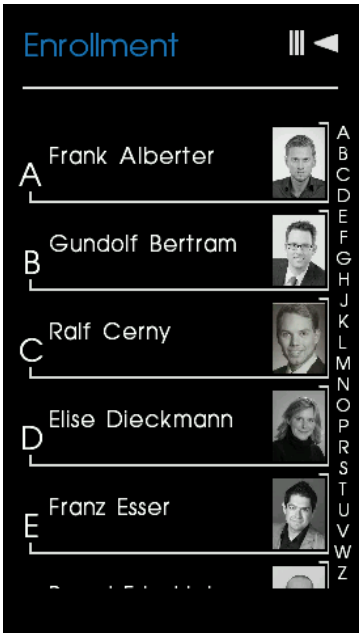


Figure 42: Enrollment on the LCD display

The enrollment can be started on the LCD display by holding the green service RFID card in front of the reader.

The heading shows that the enrolment view is active.

A list of all persons with first and surname available for enrollment is displayed.
This list can sometimes be very long, therefore an alphabet will be displayed on the right side of the screen after a certain length.
The list of persons is primarily sorted by surname.

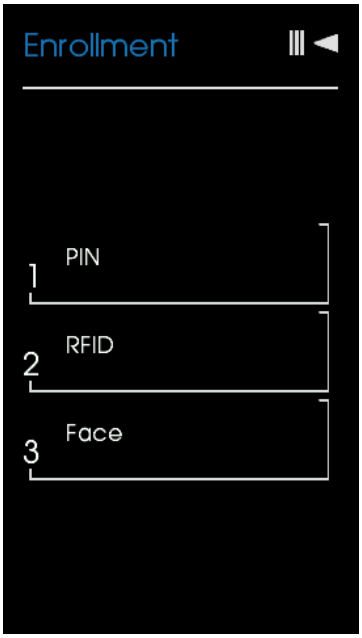


Figure 43: Enrollment View of a person

By selecting a person, you can see which enrollment options are available for that person. The enrollment is started by the respective button.

PIN: A PIN code for the person can be entered here. This must have a length of between 3 and 7 characters and must not begin with a 0. It is not possible to select a PIN code that has already been assigned.

RFID: By holding an RFID card in front of the reader which is not yet known to the door terminal, can be assigned to the person.

Face: The enrollment can be performed by following the instructions on the LCD display. To do this, the person must stand in front of the door terminal. The messages on the display give information if the position of the face has to be changed and show the progress of the enrollment.

4.2.2 Setting up access control on the website

Only PIN and RFID can be set up via the website.

To add the PIN code, select a person from the list of persons and enter the PIN code in the *'PIN'* field. The PIN code must be between 3 and 7 characters long and must not begin with 0. It is not possible to select a PIN code that has already been assigned.

In order to set up access control via RFID, the UID of the RFID card must be known. It can then be entered in the corresponding field for the person. Determining the RFID UID requires a certain amount of effort, so for single persons it is best to use the enrollment directly at the door terminal.

If many people are to be equipped with RFID cards, an RFID card reader can be ordered from Adatis. More information on reading RFID cards with the card reader can be found in chapter 4.2.6.

4.2.3 Increasing security by combining several access options

Through the website it is possible to combine several access options.

If a person wishes to gain access, that person must not only identify himself/herself by PIN, but also by RFID or facial recognition for example.

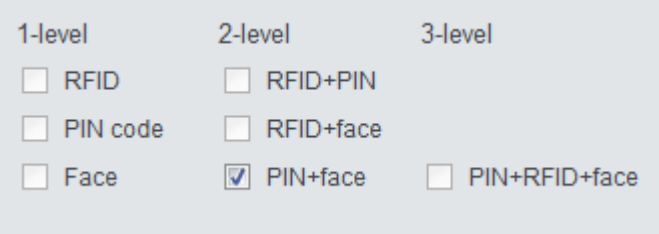


Figure 44: 2-level Authentication with PIN and Face

If the person's authentication is only set to one level, the authentication is sufficient for one of the selected options. To increase security, the person's authentication query must be set to two or three levels.

If all three authentication options are checked, security is at its highest.

Note: A combination of the authentication options is only possible for the authentication procedures for which data has been stored. For example, it is not possible to combine PIN and RFID if no PIN code has been entered. It is then not possible to check the appropriate option.

4.2.4 Getting access

As soon as access has been granted, the following message is displayed:

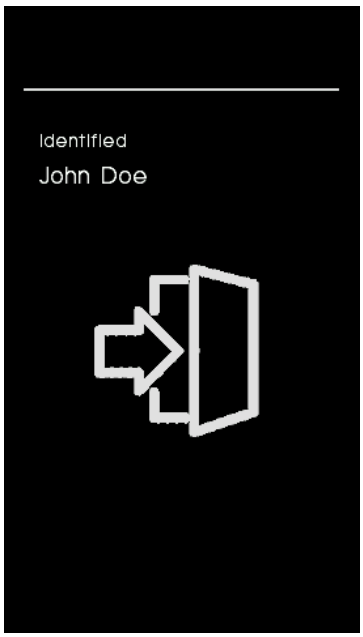


Figure 45: Access granted

If the door terminal is used in access control mode *'Wiegand reader'* (see chapter 5.8.6), the door terminal indicates that the access is controlled by the connected access control system:

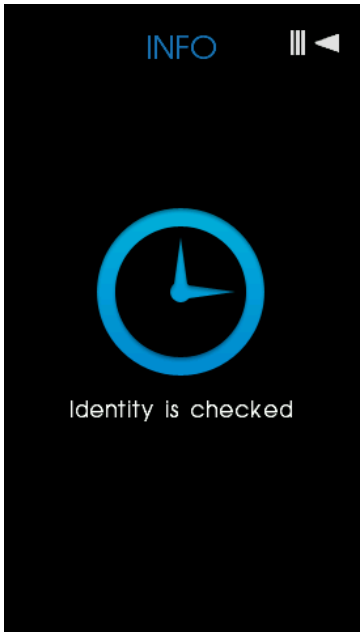


Figure 46: Getting access in access control mode *'Wiegand reader'*

4.2.4.1 Access through PIN entry

After a person has been assigned a PIN, that person can authenticate via the PIN at the door terminal.

It is possible to call up the PIN entry by placing a finger on the display and then moving the finger to the right.

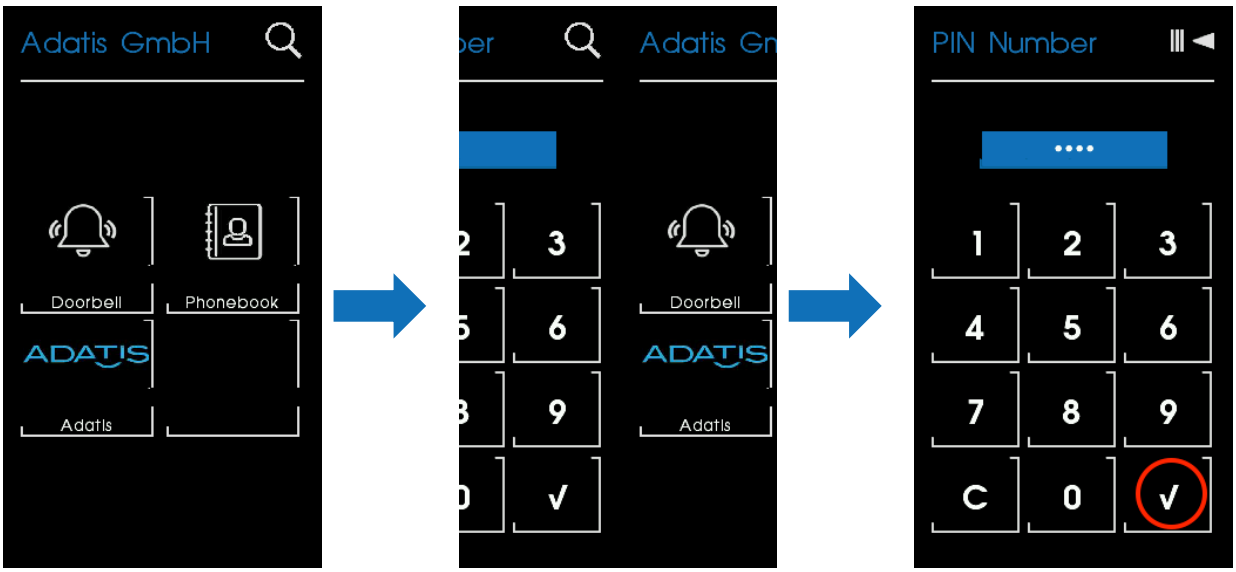


Figure 47: Opening the PIN Input

Access can be granted by entering the PIN and clicking on the marked button in Figure 45.

4.2.4.2 Access via RFID

Access can be granted by holding the RFID card in front of the reader.

Figure 48: Symbol for RFID on the door terminal

The reader is usually located below the LCD display or where the RFID symbol has been placed.

4.2.4.3 Access via face identification

To access the door terminal through face recognition, the person has to stand in the correct position in front of the door terminal. Depending on the hardware used, different types of help can be displayed.

Figure 49: Help with access through face recognition (FaceEntryXS)

The help for FaceEntryXS is displayed by touching the face on the start screen.

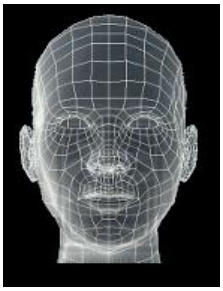


Figure 50: Starting Face Recognition Help (FaceEntryXS)

Note: If a face is detected, the face's net mask will appear blue on the home screen. (See chapter 3.5.3)

Figure 51: Help with access through face recognition (FaceEntryXT)

The help for the FaceEntryXT is displayed by placing a finger on the LCD display and then moving the finger to the left (See Figure 33)

4.2.4.4 Access via a combination of access options

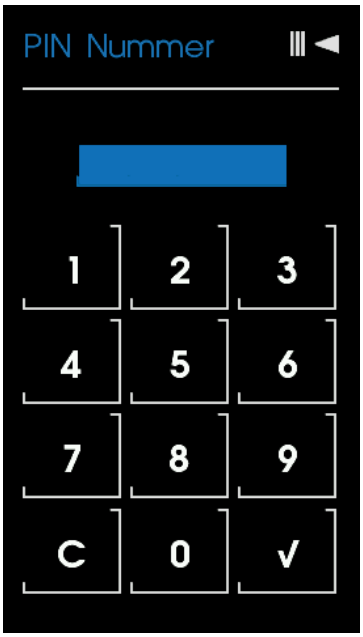
Chapter 4.2.3 describes how access options can be combined to increase security.

In order to identify yourself, it is irrelevant whether the person starts first with authentication with PIN, RFID or identification via face.

After the person has authenticated using one of the options, the door terminal directly displays the window through which the person is to authenticate next. If, for example, the person is still to authenticate by PIN, the PIN entry is displayed.

The following three windows may appear if the person has already authenticated by one option and indicate what the person should do next:

Authentication via PIN:



Authentication via RFID:

Authentication via face recognition:

Figure 52: Check PIN, RFID, and facial recognition

Access is not granted until the required access options have been checked. (See chapter 4.2.3)

Via the *'Back'* button in the upper right corner, the authentication of the person by several access options can be cancelled. You will then be taken back to the door terminal start screen.

4.2.5 Integrating an access server

In the delivery state, access is granted directly through the door terminal by comparing the data of an access event directly with the data stored on the door terminal.

Figure 53: Access Control Mode - Autonomous

The *'Access control mode'* setting, which can be accessed via the *'Access options'* menu item on the website, is set to *'Autonomous'* by default.

The door terminal then uses the locally stored data to decide whether a person is granted access or not.

However, it is possible to integrate the door terminals into an existing access control system. The Wiegand output of the door terminals can be used for this purpose. Chapter 5.8.6 describes how to configure the Wiegand interface.

It is also possible to control access through the Administration Server. Chapter 5.10.3 describes this.

4.2.6 Reading the UID of an RFID card using the card reader

With the card reader, it is possible to read the UID of a RFID card and enter it directly in the correct format in the corresponding field within the web view of the terminal. The card reader can be ordered via article number #8281.

4.2.6.1 Installing the card reader

To use the card reader, it must be connected to a free USB port. The installation is done automatically. It is ready for use immediately afterwards.

4.2.6.2 Reading the UID of an RFID card in the web view of the terminal

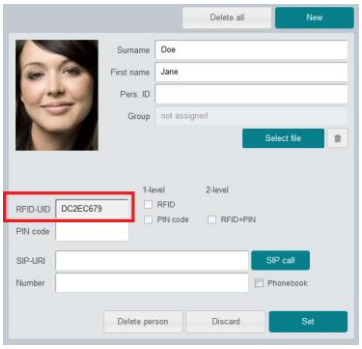


Figure 54:
Reading the UID of an RFID card in the field RFID-UID

Reading the UID of the RFID card and formatting the input into the correct format is possible in the RFID UID field of a person.

To do this, the field must be selected and the RFID card must then be placed on the reader.

Afterwards the RFID-UID for the person has to be saved by *'Set'*.

4.3 Establishing a connection to a remote station

The CommandCenter, IP telephones or the DoorKeeper software from Adatis can be used as remote stations to the Adatis door terminals. DoorKeeper is available for the Windows operating system and the mobile operating systems Android and iOS. The mobile versions can be obtained directly from the Google Play Store or App Store. The Windows version must be ordered from Adatis.

Communication is via the SIP protocol. Each participant of a SIP communication must have an address according to the following scheme:

username@domain

The address of the remote terminal must be entered in the SIP-URI field of the respective person for a call. (See chapter 4.1)

Note: It is possible to establish a maximum of 16 SIP connections transmitting video with the door terminals. However, as soon as the audio connection is established for a one SIP connection, all other connections are terminated.

How the door terminal can be controlled via the keys of an IP telephone can be read in Chapter 5.6.6.

4.3.1 Direct call

In addition to the domain, the IP address can also be used to call a person directly.

Many IP phones, such as Grandstream or Snom, can be reached directly via their IP address. In order to call a person with a corresponding IP phone, only the IP address of the IP phone must be entered in the *'SIP-URI'* field of the person. The user name and thus also the @ sign can be omitted.

A corresponding call from the remote station can also be made via the IP address. The points within the IP address are entered using the * key.

Note: The direct call only works in the local network with IP telephones that can be called directly via the IP address. If necessary, refer to the IP phone manual.

4.3.2 Internal Registrar

The door terminals have an internal registrar. This means that the door terminals themselves can act as servers where the door terminal itself is a participant in the communication. All other remote stations must register with the door terminal so that they can be called from there.

Note: The door terminals can act as registrar servers and as sip user agents (sip telephones), but not as sip proxy servers. This means that it is not possible to forward calls for which the door terminal is not a call participant.

This type of communication is also used by the DoorKeeper software (except for iOS) or the Command Center. By adding the door terminals to the DoorKeeper software, it automatically registers with the door terminals and the remote stations are accessible from the door terminals.

In principle, the DoorKeeper software only informs the door terminal from which IP address it can be reached.

4.3.2.1 Configuration of a Remote Station using the Internal Registry

In order to configure a remote station, you first have to look into the settings of the DoorKeeper software. Under *'General Settings'* the username can be found. (See Figure 55)

Note: In DoorKeeper the username is called SIP User.

If you enter the username, led by an @, into the SIP-URI field of a person, the corresponding remote station can be called directly. (See Figure 55) The @ in front of the user name tells the door terminal to search the internal registrar for a remote terminal with the same user name. The door terminal then adds the corresponding IP address that was found for the user name.

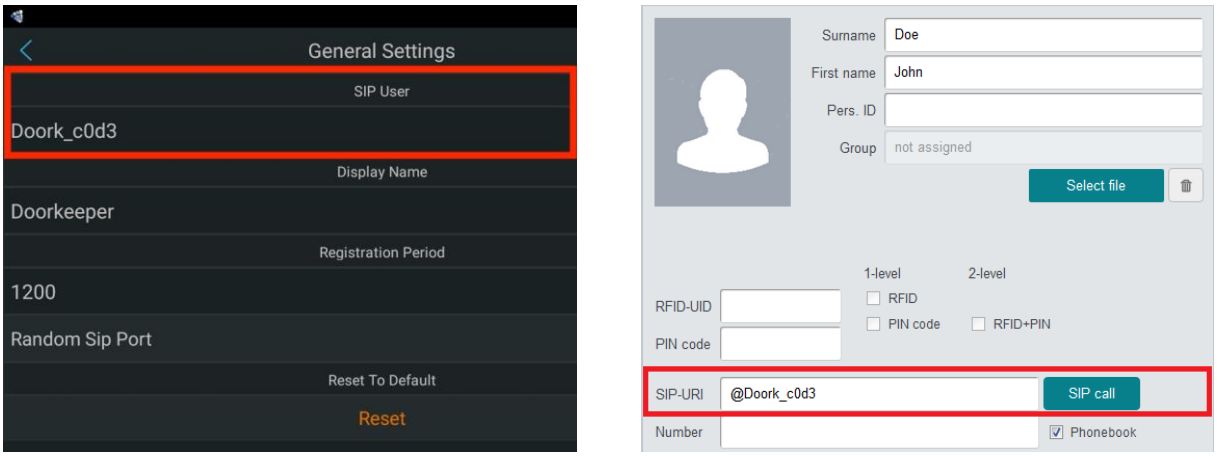


Figure 55: The same username in the DoorKeeper app and in the SIP URI field of a person on the website of the door terminal.

Example:

Input in the SIP-URI field:	**@username**
	+
IP address of the DoorKeeper:	**IP-address**
	=
The door terminal combines the following:	**username@IP-address**

This type of connection setup has the advantage that the remote station can be called even if the IP address of the remote station changes. This can be in particular the case with mobile devices, which usually obtain their IP addresses via DHCP.

4.3.2.2 Configuration for a broadcast call via the internal registrar

By entering *'DK*'* in the SIP-URI of a person, a broadcast call can be started to all registered remote sations at the door terminal by clicking on the person.

As soon as the call is answered by one of the remote stations, all other calls are terminated.

4.3.3 SIP Server

For larger systems, such as an internal company network, a SIP server or a telephone system is often used. For communication to take place via the server, both the door terminal and the remote station must be registered with the SIP server.

The configuration of the SIP server is possible under the menu item *'SIP configuration'* on the website of the door terminal.

Figure 56: SIP Server Settings

The following login data must be entered there:

Server domain: The IP address or domain name of the SIP server.

User name: The username under which the door terminal will be accessible.

Authentication: The user name for authentication on the SIP server.

Note: There is often no separation between user name and authentication and the user name must be entered for both.

Password: The password matching the username.

Server Port: The port on which the SIP protocol runs on the server. Usually this is the port: 5060

Registration period: The shorter the registration period, the more frequently the door terminal checks whether the server is still available. However, more data is sent to the server. The default setting is 600 seconds (10 minutes).

NAT Keep-Alive:If the server is in the local network, NAT Keep-Alive can be disabled. However, if the server is outside the local network, the setting must be set to *'Options'*.

Note: The SIP server must support receiving the SIP message *'Options'* for NAT Keep Alive to work**.**

The icon next to the server domain indicates whether the registration on the SIP server was successful or not.

Registration successful

Figure 57: Registration successful

Registration failed

Figure 58: Registration failed

The LCD display of the door terminal shows the following message if the connection to the SIP server is not possible

Figure 59: No SIP Server connection

Note: The Adatis SIP server is strongly recommended when using a SIP server outside the local network.
It is the only server with which the iOS version of the DoorKeeper works, because only this server can wake the Apple product from its idle state, via PUSH notification. This is the only way to receive calls.

For the configuration of the remote station, if it is a DoorKeeper, the document *'Quick Installation SIP-Server Adatis'* can help.

If the door terminal is registered with the SIP server, the remote station can be called by entering the SIP user name of the remote station followed by an @ in the SIP URI field of a person. The @ after the user name tells the door terminal to add the domain of the registered SIP server to the address.

Example: Communication through the SIP Server

Input in the SIP-URI field:	**username@**
	+
domain of the SIP server:	**sip.adatis.com**
	=
The door terminal combines the following:	**username@sip.adatis.com**

4.3.4 Direct Call through SIP URI

It is also possible to call SIP addresses where the door terminal is not registered. However, this only works if the SIP address can actually be reached.

To do this, the complete SIP address must be entered according to the scheme already mentioned:

username@domain

Note: Without registration of the door terminal with the SIP server, the door terminal cannot be reached from the remote station.

4.3.5 Calling several remote stations from one person

It is also possible to store more than one address in the SIP-URI of a person. The respective addresses must be separated with a semicolon.

When a call is established, all addresses are called at the same time. As soon as a remote station accepts the call, all other calls are cancelled.

Note: Especially when communicating via the Internet, it is important to note that the video for the video preview is sent to each remote station. The Internet connection at the door terminal must be able to provide the necessary bandwidth in the upload in order to display the videos correctly.

The document *'Quick start video formats'* gives information about how large the bandwidth has to be and what needs to be done to get an appropriate video quality.

4.3.6 Establishing a Connection to a Person

The following options are available for calling a remote station from the door terminal:

- Calling from the Phone Book on the LCD Display
- Calling via Search on the LCD display
- Calling via Speed Dial on the LCD Display
- Call from the Website for Testing Purposes

The call is indicated on the LCD display if the call was started from the LCD display or if an incoming call is received at the door terminal as soon as an audio connection is established.

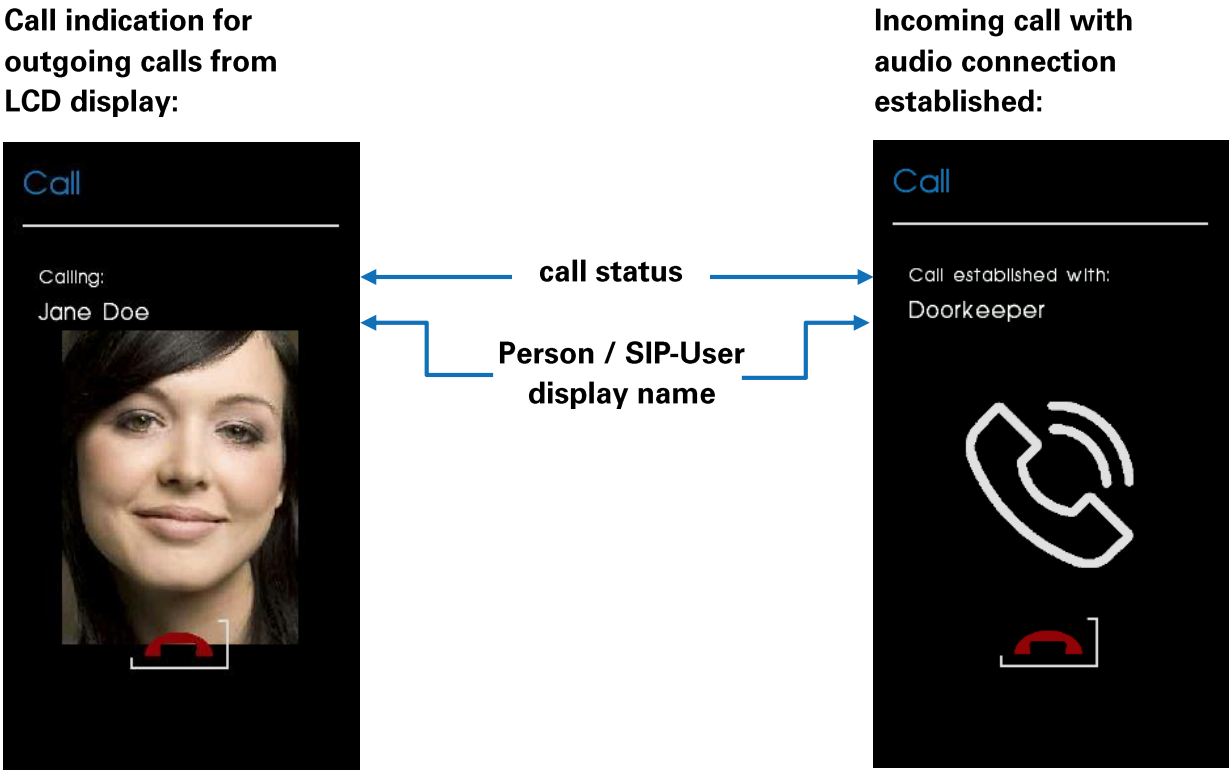


Figure 60: Call indication on the LCD display

4.3.6.1 Calling from the Phone Book on the LCD Display

Whether the persons on the door terminal have been divided into groups or not, the persons can be called directly or via the group to which they are assigned.

Call directly through the person:

The call to a person through the telephone book is possible directly by clicking the button.

Call directly from the group:

In the case that only one person is assigned to a group, the call can be made directly via the group.

At this point, the *'Doorbell'* group could initiate a direct call.

Call through the group's phone book:

If more than one person is assigned to a group, the phone book with the assigned persons appears after clicking on the group.

The heading at the top shows the current group. In this case the group is called: *'Phonebook'*.

The call is made again by clicking the person's button.

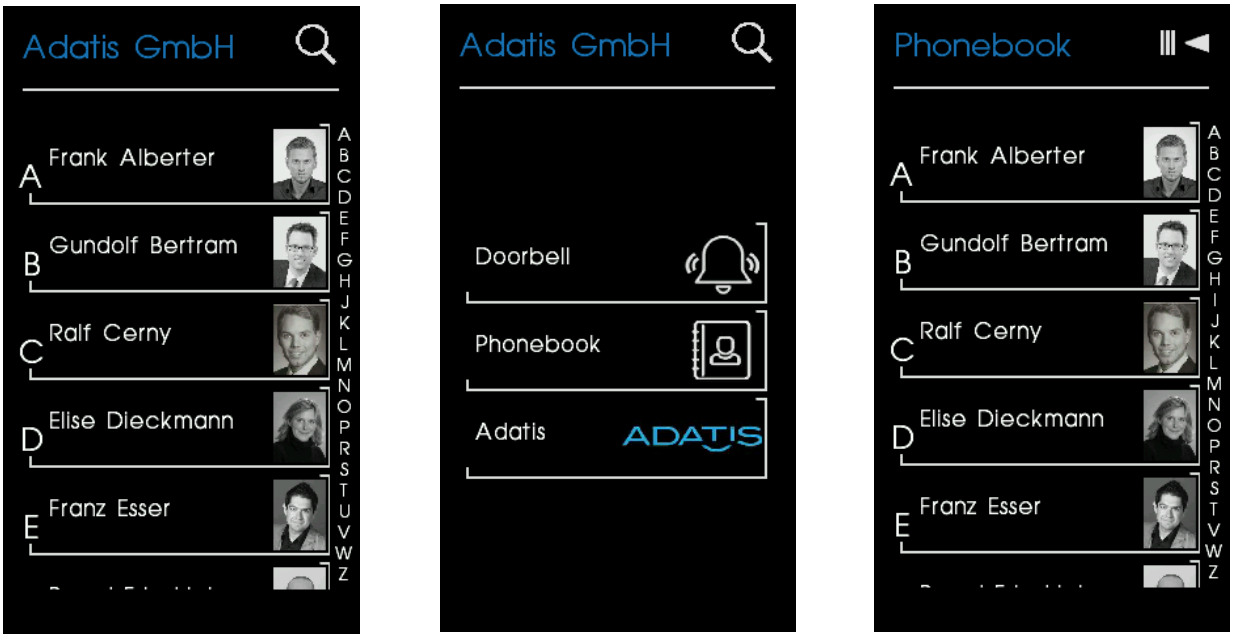


Figure 61: Calling from the list of persons, the groups and the phonebook of the group

4.3.6.2 Calling via Search on the LCD display

Irrespective of whether the telephone book or the keypad is displayed on the door terminal, it is possible to search for all persons who are in the personal database of the door terminal.

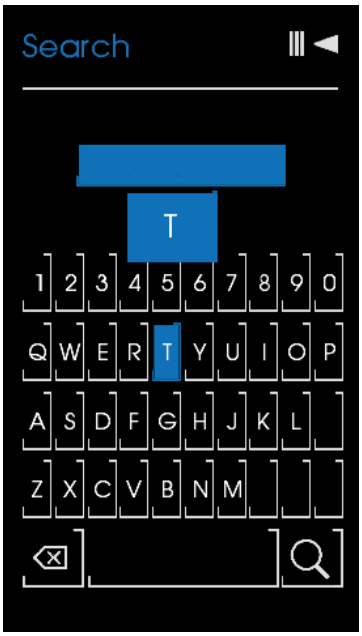


Figure 62: Comfort input when searching for persons

The search is started via the magnifying glass icon on the start screen. (See Figure 16)

The comfort input of the keyboard allows the precise input of letters and numbers.
When the keyboard is touched, the letter on which the finger rests is enlarged. By moving the finger it is possible to select another letter.
Only when the finger is released, the letter is entered into the search mask.

Figure 63: Search for Persons

The search does not distinguish between upper and lower case letters.

It makes sense to search for the surname whenever possible, since the result list is sorted by surname first.

Figure 64: List of results when searching for persons

The result is a list of all persons for whom the search criteria were successful and for whom the check mark *'Phone book'* is set. (See also chapter 4.1)

If the person is assigned and to which group, does not matter for the result of the search.

Note: If groups are configured on the door terminal, only the persons assigned to a group are displayed in the phonebook.
However, it is still possible to find persons who are not assigned to a group using the search function!

4.3.6.3 Calling via Speed Dial on the LCD Display

Before making a speed dial call, the door terminal must be configured to display the keypad. Chapter 5.3.2 describes how to change the settings for displaying the keypad.

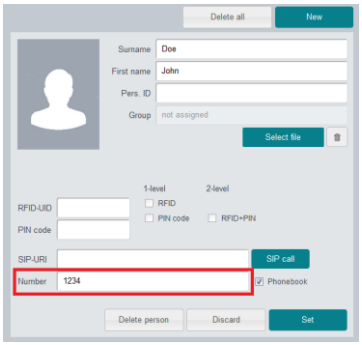


Figure 65: Assigning a speed dial to a person

Before a person can be called via their speed dial, a speed dial must be assigned to them.

This is done via the person's entry on the website.

By entering the speed dial in the *'Number'* field, the person is assigned the corresponding speed dial.

The speed dial must only consist of digits and may have up to seven digits.

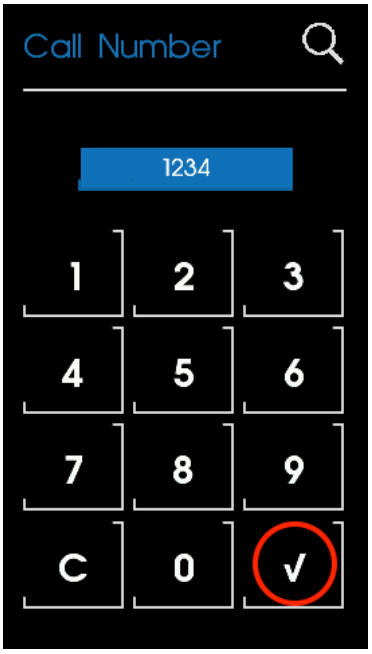


Figure 66: Calling from the keypad

The heading *'Call number'* shows that you are in the view for entering the speed dial.

The person can be called directly by entering the speed dial number of the person and then confirming with the marked button in Figure 66.

Note: Do not confuse the keypad with the pin input view.

In contrast to entering the speed dial, entering the PIN is always concealed!

4.3.6.4 Call from the Website for Testing Purposes

From the website, a call is possible via the person's entry.

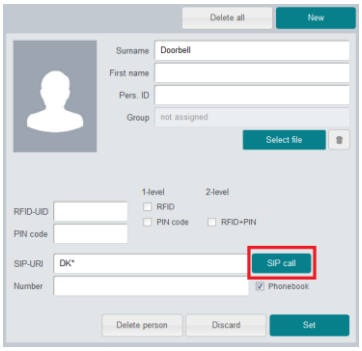


Figure 67: Call from the Website

With the button *'SIP call'*, the other party can be called.

This type of call is mainly used when setting up the remote station to test whether the remote station can be reached from the door terminal.

Note: When calling via the web page, the call is not indicated on the LCD display as shown in Figure 60. Only if the call is accepted by the other party the call is shown on the LCD display.

4.3.6.5 Special aspects when calling from a remote terminal

If the door terminal is called by a remote terminal, the door terminal answers directly. It accepts the call if there is no audio connection between the door terminal and another remote station at the time, otherwise the call is rejected. The call is accepted without audio so that it is possible to view the camera image of the door terminal first before communication is established directly with the other party.

The audio connection can be established via the *'*'* key of the remote station or via the corresponding button at the DoorKeepers.

4.4 The group function for persons

In addition to assigning a person to a group, this chapter should also show the possibilities provided by the group function. For this reason, the chapter has the following topics:

- Creating a Group
- Customizing the appearance of a group on the LCD display
- Assigning persons to a group
- Login to the Website as Group Admin

4.4.1 Creating a Group

A group can be created on the website via the menu item *'Groups'*.

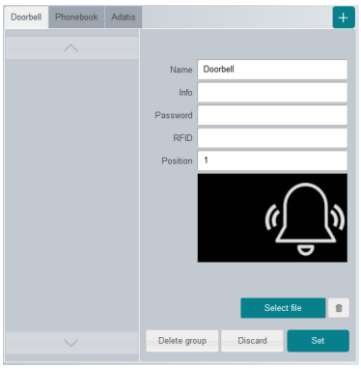


Figure 68: Creating a Group

Name:The name of the group is shown on the LCD display and is also necessary for the login of the group admin on the website. (See Chapter 4.4.4)

Info: A short additional information shown on the LCD display about the group. For example, the floor where the company is located.

Password: The password for the login of the group admin to the website. (See chapter 4.4.4)

RFID: Each group can have its own RFID card assigned to it. This serves as an enrollment card, only for the respective group.

Note: This function is not yet available in the current version of the door terminal.

Position: Indicates the order in which the groups are displayed on the LCD display. (See chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**)

Select file: Here you can upload an image for the group. (See chapter 4.4.2.2)

The data for the first group can be entered directly into the input mask. By *'Set'* the group is added to the database.

Another group can be added via the plus sign in the upper right corner. The data can be entered in the same way as for the first group.

4.4.2 Customizing the appearance of a group on the LCD display

The groups can be displayed on the LCD display either as a single column or as two columns below each other and can be backed up with a picture or logo. In addition, the order of the groups can be set.

4.4.2.1 Single-column or double-column view of the groups

Through the menu item *'Menu configuration'* on the website, it is possible to display the groups in pairs or individually. For this you have to choose either single column or double column for *'Group page layout'*.

single column group representation:

Figure 69: single column group representation

two-columned group representation:

Figure 70: two-columned group representation

If not all groups can be displayed on the LCD display at once, the list of groups can be scrolled down or up.

Note: Depending on the selected representation, the image should also be adapted to the group. (See chapter 4.4.2.2)

4.4.2.2 Adding an Image or Logo

An image can be added by selecting the desired image from the group on the web page via *'Select file'*.

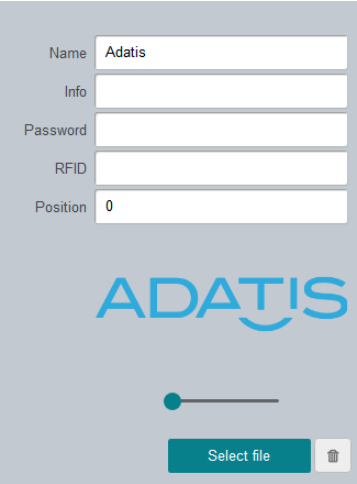


Figure 71: Adding a group image

By moving the slider below the image, the image can be zoomed.

The image can be positioned with the mouse.

Depending on whether the list is to be displayed with one or two columns, good results can be achieved with the following image properties:

single column: Height/width ratio: 1:1,2
image alignment: Right side

Example:

Two-columned: Height/width ratio: 1:1,7
image alignment: Centered

Example:

Depending on the door terminal, the optimum resolution of the images for the groups can be found in the following table:

	width (pixel)	height (pixel)
TouchEntryXS	**107**	**54**
FaceEntryXS	**107**	**54**
TouchEntryXT	**152**	**84**
FaceEntryXT	**152**	**84**

If the result was not satisfactory, another image can be selected by clicking on *'Select file'* again.

To delete the image, click on the *'trash can'* icon.

4.4.2.3 Changing the order of groups

Each group receives a value for the position when it is created. This value can be set for each group under the menu item *'Groups'*. The higher the entered number, the further to the right or further down the group is displayed.

The following shows how the value for the position affects the sequence of the groups. A distinction must be made between single-column and double-column display of the groups.

Single-column group order:

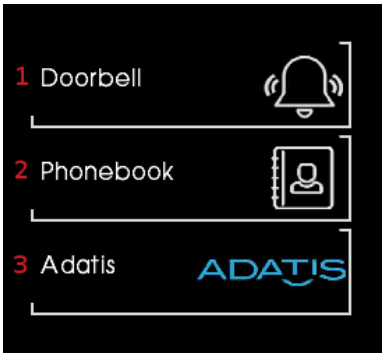


Figure 72: Single-column group order

Two-column group order:

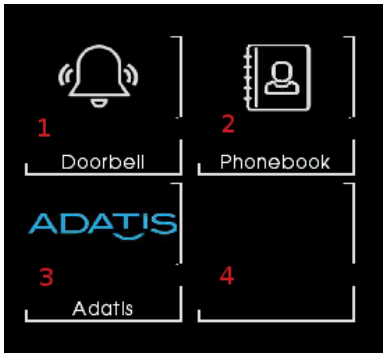


Figure 73: Two-column group order

Note: Groups for which the same number is entered for the position are sorted by alphabet.
This is the default case if all groups have the position 0.

4.4.3 Assigning persons to a group

The assignment of persons to a group can be done via the website of the door terminal. To do this, the menu item *'Groups'* must be selected.

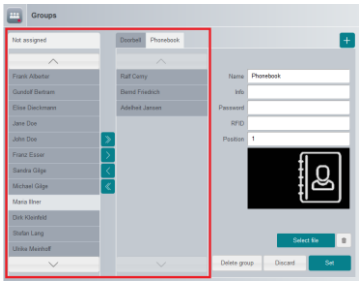


Figure 74: Assigning persons to a group

The list on the left contains all persons who have not yet been assigned to a group.

If you select the respective group, the right list contains all persons who are assigned to the group.

Assigning a person to a group works by selecting the persons and using the arrow keys between the two lists, whereby the double arrows transfer the complete list.

Note: The assignment of a person takes place without a confirmation via the *'Set'* button. This only needs to be pressed to make changes to the group settings.

After the persons have been assigned to the group, they can be accessed from the LCD display via the respective group.

Important: Only people who have the Phonebook option checked are shown on the LCD display.

If the view on the LCD display shows the groups, it is no longer possible to call people directly who are not assigned to a group. However, they can still be found and called using the search function. (See chapter 4.3.6.2)

If only one person is assigned to a group, the respective person is called directly by selecting the group.
This makes it possible, for example, to add a doorbell button as shown in Figure 69.

Groups to which no person is assigned cannot be called.

4.4.4 Login to the Website as Group Admin

A group login can be created for each group of the door terminal, which makes it possible to manage only the persons in your own group and adapt the appearance of the group, for example in terms of the logo.

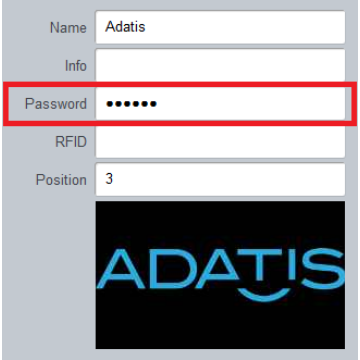


Figure 75: Setting the password for the group

A password must be assigned to the respective group to enable this function.

This can be done by selecting a group in the menu item *'Groups'* and entering the password in the corresponding text field.

Important: A secure password should be chosen here.

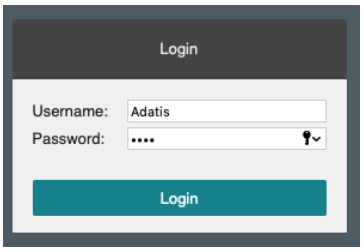


Figure 76: Login as the group admin

With the group name and the password you can then log in at the login page of the door terminal.

After logging in, access is only possible to the menu items *'Persons'* and *'Groups'*.

The persons of your own group can be created, edited and deleted in the same way as when logging in as admin.

Note: Only the persons belonging to the group are displayed. Unassigned persons are not displayed.

All persons added in this view are automatically assigned to the group.

4.5 Backing Up and Restoring the Personal Database

It is possible to download the personal database from the door terminal in order to store it externally. The entire personal database can also be outsourced to an administration server. This server is called *'FaceAdmin'* by Adatis and, in addition to managing the personal database, can also manage the configuration and access. This chapter will only show how to download the personal database manually.
Chapter 5.10 describes how to set up the Administration Server to manage the personal database.

4.5.1 Backup the personal database

The personal database can be downloaded from the door terminal website under the menu item *'Upload/Download'*. There you can download the personal database by clicking on *'Download/Export'* and then on the *'People'* button.

Usually the file is called as follows:

FaceEntry_personal.gz

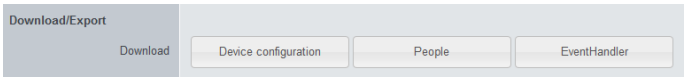


Figure 77: Backup the personal database

Not only the persons but also the groups of the door terminal are saved in this file.

4.5.2 Restoring the Personal Database from the Backup

The personal database previously downloaded in chapter 4.5.1 can also be uploaded to the door terminal again via the *'Upload/Download'* menu.

To do this, first select the file under *'Update/Import'* and then press the *'Upload'* button.

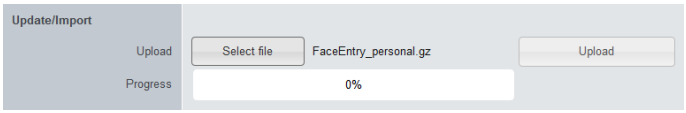


Figure 78: 4.5.2 Restoring the Personal Database from the Backup

Note: The personal database can also be uploaded to other door terminals in the same way. The data records are uniform on all Adatis door terminals.

Attention: Restoring the personal database from the backup overwrites all changes made on the door terminal. Newly added persons and groups are overwritten by the restored personal database.

5 Further functions of the door terminals

After the basic functions of the door terminals have been explained in the previous chapter, this chapter will describe the additional functions that go beyond the basic functions.

The following topics are discussed in this chapter:

- Date and time setting
- Setting the language
- Further customization of the LCD display
- Time recording
- Face Recognition Settings
- Further settings for setting up communication
- Audio
- Video-Settings
- Motion JPEG Video
- Interface Configuration (Inputs and Outputs)
- EventHandler
- Administration of the door terminals using an administration server
- System
- System
- Firmware

5.1 Date and time setting

The date and also the time can be set via the website.

All settings are accessible via the menu item *'Basic settings'*.

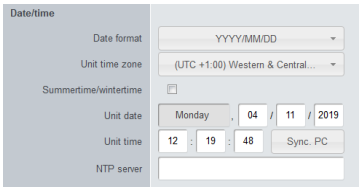


Figure 79: Date and time setting

Date format: Here you can set the date format. This will affect the appearance of the display when the door terminal idle screen is on and in *'Time'* mode.

Unit time zone: The unit time zone must be set here. The time zone set here must be based on the winter time.

Summertime/wintertime: If this setting is set, the door terminal automatically detects whether summer or winter time is current and corrects the time accordingly.

Unit date: Here the date can be entered manually.

Unit time: The time can be entered manually here.

Sync. PC: Synchronizes the time once with the PC from which the website is accessed.

NTP server: At this point, it is possible to enter the address of a time server that uses the Network Time Protocol (NTP) in order to obtain the current time and date.

If you configure a time server, the button next to the device time indicates the possibility to synchronize with the NTP server. In addition, synchronization takes place at regular intervals.

Note: Obtaining the time via a time server usually requires a connection to the Internet if the time server is not in the local network.

The time zone must always be set manually, because it cannot be obtained from the time server.

5.2 Setting the language

The language can be set on the website via the menu item *'Basic settings'*.

Figure 80: Setting the language

You can choose between the following languages:

- German
- English
- French
- Spanish

Attention: The language *'debug'* can also be selected.
However, this should not be selected, as all headings and buttons will be replaced by numbers.
If this language has been wrongly selected, the language can be changed again via menu item 7 at number 279.

5.3 Further customization of the LCD display

Not only the appearance of the groups can be changed on the LCD display, as described in chapter 4.4.2. The door terminals also offer the following adjustment options:

- Changing the heading on the start screen
- Displaying the phonebook or the keypad to establish a connection
- Changing the Display Brightness
- Configuring the idle screen

5.3.1 Changing the heading on the start screen

The text can only be changed through the website.

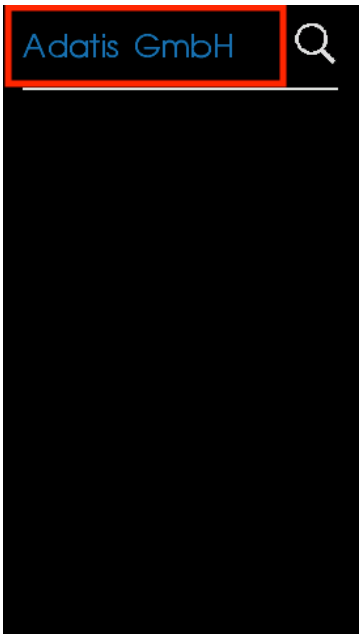


Figure 81: Heading on the Start screen

The menu item *'Menu configuration'* must be selected and the text for the *'Name LCD start page'* setting must be changed.

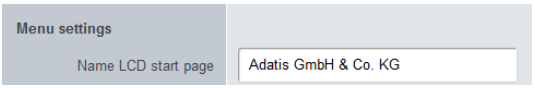


Figure 82: Changing the heading on the start screen

Depending on the device type, only a certain number of characters are displayed on the LCD.

5.3.2 Displaying the phonebook or the keypad to establish a connection

When delivered, the door terminals display the telephone book. Depending on whether the persons were divided into groups or not, a list of all added persons is displayed or the groups are displayed.

However, the door terminals can also be set so that a call can be made via the speed dial of the person.

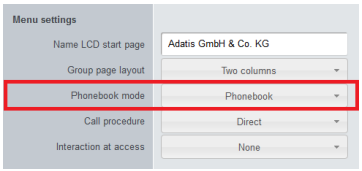


Figure 83: Displaying the Phonebook or the Keypad

The setting can be changed on the website of the door terminal.

To switch between the display of the phone book and the keypad, select the menu item *'Menu configuration'* and change the setting *'Phonebook mode'* to Phonebook or Keypad.

How a call can be established via the speed dial of the person is described in chapter 4.3.6.3.

5.3.3 Changing the Display Brightness

On delivery, the display brightness is set so that it automatically adjusts to the ambient light.

Nevertheless, it is possible to adjust the display brightness manually.

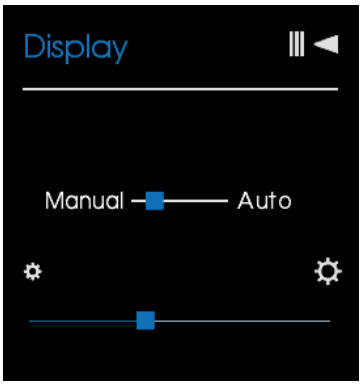


Figure 84: Setting the brightness of the LCD-display

The setting of the display brightness can be done via the configuration of the LCD display in the submenu *'Display'*.

To set the brightness manually, first switch to *'Manual'*.

The display brightness can then be adjusted using the slider.

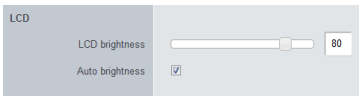


Figure 85: Changing the brightness of the LCD-Display on the website

The display brightness can also be set via the website under the menu item *'Basic settings'*.

The setting here is analogous to the setting on the LCD display.

5.3.4 Configuring the idle screen

For the LCD display, an idle screen can be set, which is displayed after an adjustable period of time without user interaction. The sleep mode is intended to increase the life of the display and prevent possible burn-in of pixels.

The door terminal wakes up as soon as the LCD display is touched or there is an access event (face detected, RFID card held). For door terminals with face recognition, it is sufficient for a person to stand in front of the door terminal to leave idle mode.

5.3.4.1 Setting up the idle screen

The settings can be done on the website of the door terminal under the menu item *'Menu configuration'*.

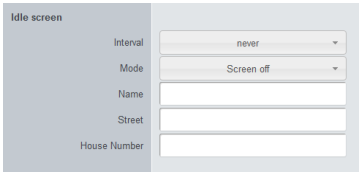


Figure 86: Setting up the idle screen

Interval: This setting specifies the time after which the idle screen should appear. By default, the interval is set to *'never'*.

Mode: Here you define what is to be displayed as an idle screen.

Name: Is displayed as a heading on the idle screen.

Street, Housenumber: If the *'Address'* mode has been selected, the information can be entered here.

To protect the display while idle, the display image is moved at regular intervals by a few pixels. For this reason, an outline font is used.

The modes are briefly described below.

Screen off

Instead of displaying an idle screen, the display is turned off. The display is turned on again upon touch or an access event, so that all functions are available.

Note: Turning off the screen in sleep mode reduces power consumption and extends display life.

Address

When this mode is selected, the address entered on the website is displayed. The house number is displayed in a particularly large format so that it can be seen from a more distance. (See Figure 87)

Note: At this moment, three-digit house numbers consisting of the following characters can be displayed:

1234567890abcdef

All other numbers can be displayed by adding a background image.
(See chapter 5.3.4.2)

Time

If this mode is selected, the current time and date are displayed. (See Figure 88)

How the date is displayed on the LCD display depends on the *'Date format'* and *'Language'* settings, which can be set via the *'Basic settings'* menu item on the website. (See chapter 5.1)

Figure 87: Idle Screen with Address Mode

Figure 88: Idle Screen with Time Mode

5.3.4.2 Selecting the background image for the idle screen

The background can be configured for the idle screen on the door terminal website under the menu item *'Menu configuration'*.

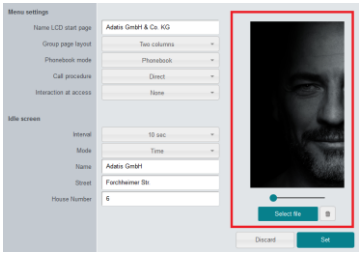


Figure 89: Background for the idle screen

With the button *'Select file'*, an image can be selected for the background.

By moving the slider below the image, the image can be zoomed.

Depending on the door terminal, the optimum resolution of the image for the idle screen can be found in the following table:

		width (pixel)	height (pixel)
TouchEntryXS		**272**	**480**
FaceEntryXS		**272**	**480**
TouchEntryXT	**5,6“**	**480**	**640**
	7“	**480**	**800**
FaceEntryXT	**5,6“**	**480**	**640**
	7“	**480**	**800**

Note: The background should be as dark as possible.

For fonts on the background image, an outline font should be used with a maximum line width of 5 pixels.

5.4 Time recording

With the door terminals it is possible to activate time recording.

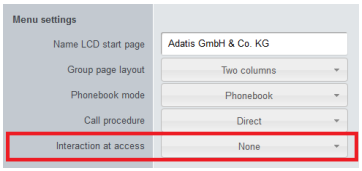


Figure 90: Enable Time Recording

Time recording can be set on the website under the menu item *'Menu configuration'*.

The time recording must be selected in the *'Interaction on access'* setting.

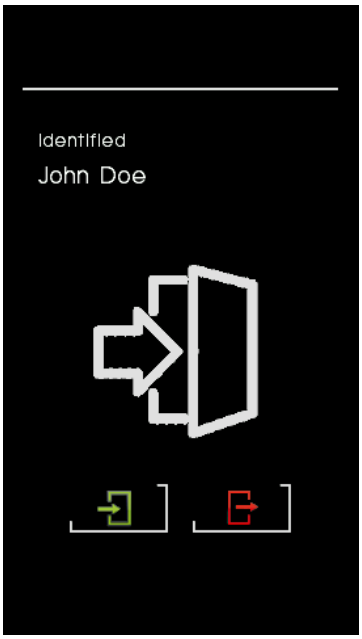


Figure 91: Time recording on access

Each time a person is granted access, two buttons are displayed. For time recording, press the green button to log in or the red button to log out.

The coming and going are acknowledged accordingly:

Figure 92: Time recording - Arrival

Figure 93: Time recording - Departure

Note: The evaluation of data from time recording can, for example, be done with the Windows application FacePCT from Adatis.

5.5 Face Recognition Settings

On the website through the menu item *'Access options'* the settings for face recognition can be configured.

Figure 94: Face recognition settings

Mode: Here you can set whether a continuous check should be performed to determine if a person is standing in front of the door terminal or the camera image should only be checked when the face recognition help is started.
Default setting: Continuous

Note: If the *'Verification'* option is selected, face recognition must always be started via the face recognition help. (See chapter 4.2.4.3)

Tolerance treshold: The tolerance in values between 0 and 550 indicates how big the difference between the treshold face on the camera image and the stored treshold face may be.
The larger the value, the faster the face recognition recognizes the person.
Default setting: 450

In order to maintain the balance between safety and usability, the tolerance should not have a value below 200.

Note: For face recognition with the 3D option on FaceEntryXS, a value below 400 must be entered for the tolerance, otherwise face recognition takes place via 2D.

5.6 Further settings for setting up communication

How the communication between the door terminal and the remote station is set up is already described in chapter 4.3.

The following topics are described in this chapter:

- Changing the local Sip Port
- Call and connection timeout
- Preview window when calling the remote station
- Audio Settings
- Video-Settings
- Using the Telephone Keypad to control the door terminals

5.6.1 Changing the local Sip Port

The local SIP port can be set on the website of the door terminal under the menu item *'SIP configuration'*.

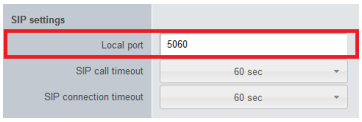


Abbildung 1: Ändern des lokalen SIP Ports

The SIP connection is established over the port.

The SIP connection is necessary to establish the connection to the remote stations.
Default setting fort he port is 5060.

If the local SIP port of the door terminal is changed, a colon and the local SIP port must be added to the address for calling the door terminal:

Address for local SIP port 5060	**If using another SIP port**
username@domain	username@domain:PORT

The door terminal can then no longer be reached directly via its IP address for direct calls:

Address for local SIP port 5060	**If using another SIP port**
IP-Adress	IP-Adress:PORT

Note: Change the local SIP port only if the connection makes it necessary, for example to the SIP server.

5.6.2 Call and connection timeout

On the website of the door terminal it is possible to set the maximum time a remote station should ring when a call is received and how long a connection may last before it is automatically terminated by the door terminal.

The settings can be made via the *'SIP configuration'* menu item.

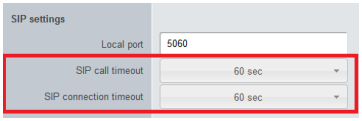


Figure 95: Call and connection timeout

SIP call timeout: The setting determines the maximum time the other station should ring. Whether the remote station actually rings that long also depends on the settings of the remote station. Default setting: 60 seconds.

SIP connection timeout: The setting describes how long a connection should be maintained before the door terminal automatically terminates the connection. Default setting: 60 seconds.

Note: This setting ensures that a connection to a remote station is not maintained indefinitely.
Otherwise, an unfinished connection with audio connected could block all communication to the door terminal, because only one audio connection to the door terminal is possible at the same time.

5.6.3 Preview window when calling the remote station

On the website under the menu item *'Menu configuration'* you can set whether a call should be started directly when selecting a person on the LCD display, or whether a preview window should appear first.

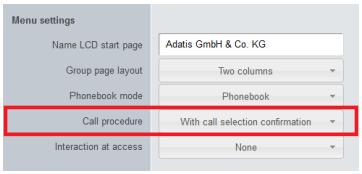


Figure 96: Set up preview window

By default, the door terminal is set to call the person directly.

To display a preview window for a call, the option *'With call selection confirmation'* must be selected under *'Call procedure'*.

Figure 97: Preview window before call

This will display a preview window showing a larger photo of the person before each call.

The person in front of the door terminal can then use the green or red buttons to decide whether they want to call the person or not.

5.6.4 Audio Settings

On the website, the settings can be found under the menu item *'Audio/Video'*.

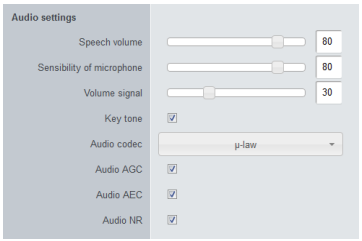


Figure 98: Audio Settings on the website

Speech volume: Corresponds to the volume at the door terminal during communication. The volume is set to 80 by default.

Sensitivity of microphone: Here you can set the sensitivity of the microphone used for communication via the door terminal. The sensitivity is set to 80 by default.

Volume signal: This setting applies to all other tones, such as signal or error tones. By default, the volume is set to 30.

Key tone: This setting describes whether tones are to be played when a button is pressed on the LCD display. This setting is switched on by default.

Audio codec: The door terminals use the G711 codec for audio transmission. You can choose between µ-law and A-law. µ-law is mainly used in North America and Japan, A-law in Europe. By default, µ-law is selected.

Audio AGC: The Automatic Gain Control (AGC) controls the background noise at the terminal down or the person's voice up so that the person's voice can be easily understood at the remote station even with loud background noise. This setting is enabled by default.

Audio AEC: The echo canceller (AEC) filters out the sounds coming out of the loudspeaker of the door station so that they are not transmitted to the remote station again. This prevents the person at the remote station from hearing their own voice. This setting is enabled by default.

Audio NR: The Noise Reduction (NR) method suppresses ambient noise generated during communication at the door terminal. This setting is enabled by default.

On the LCD display the settings can be changed in the *'Audio'* menu of the configuration.

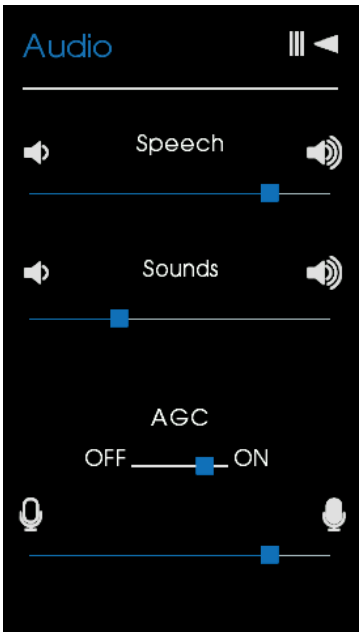


Figure 99: Audio Settings on the LCD display

The *'Speech'* slider can be used to adjust the speech volume and the *'Sounds'* slider to adjust the signal volume.

In addition, Audio AGC can be turned on or off.

The microphone sensitivity can also be adjusted here.

Note: It is recommended to leave the Audio AGC, Audio AEC and Audio NR settings at their default settings. Otherwise the audio quality may be degraded.

5.6.5 Video-Settings

5.6.5.1 Video settings on the website

On the website, the settings can be found under the menu item *'Audio/Video'*.

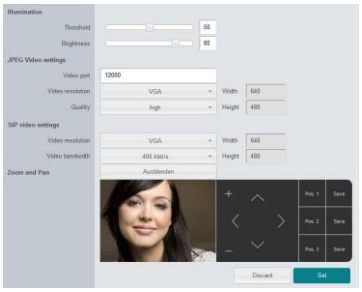


Figure 100: Video settings on the website

Illumination: The threshold indicates the ambient light at which the door terminal should switch on the infrared lighting to illuminate the surroundings. The lower the value, the earlier the light is switched on at the door terminal. Default setting: 50

Note: It is possible to turn off the infrared illumination by setting the threshold to the maximum value of 100. External lighting must then be provided!

Brightness: The exposure time of the infrared illumination can be adjusted to the local conditions via a slider for the brightness. The image of the camera can be easily overexposed, especially for outdoor shots. By setting a shorter exposure time, the face of a person can be made recognizable.
Default setting: 80

Note: As soon as the infrared illumination is switched on, only a black-and-white image is captured by the camera.

JPEG video settings:
Here you can find the settings for the Motion JPEG video.
The server port indicates the port where the video is available.
How to retrieve the video can be read in chapter 5.7.

SIP video settings:
Here you can find the settings for the video that is transmitted during communication between the door terminal and the remote station. The door terminals use the video standard H.264 for this purpose.

Note: The resolution of the Motion JPEG video image and the SIP video image is interdependent because they use the same camera sensor.

For the best video image, refer to the document *'Quick start video formats'*.

The selected resolution, the video bandwidth and the number of simultaneous video streams influence the frame rate.

Zoom and Pan: The *'Show Information'* button displays the video image at the bottom of the page. The buttons next to it can be used to zoom and move the video image.
The respective section can be selected using the position buttons and saved using the buttons next to it.

5.6.5.2 Camera Settings on the LCD Display

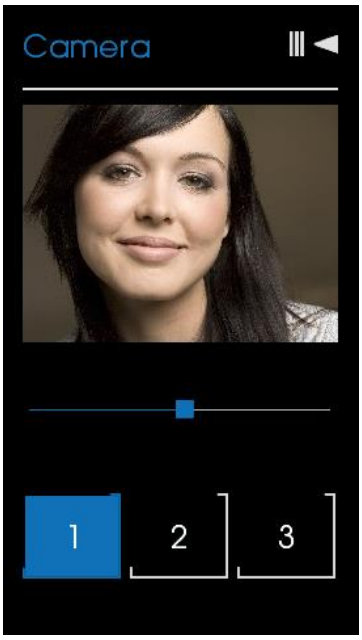
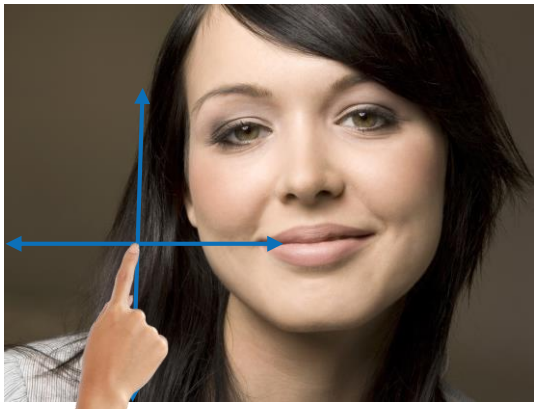


Figure 101: Camera settings on the LCD Display

All settings that can be made for zoom and pan on the website are also possible on the LCD display.

The position keys can be used to switch between the different positions. The video image can be zoomed using the slider.

By moving the finger over the video the picture can be moved.



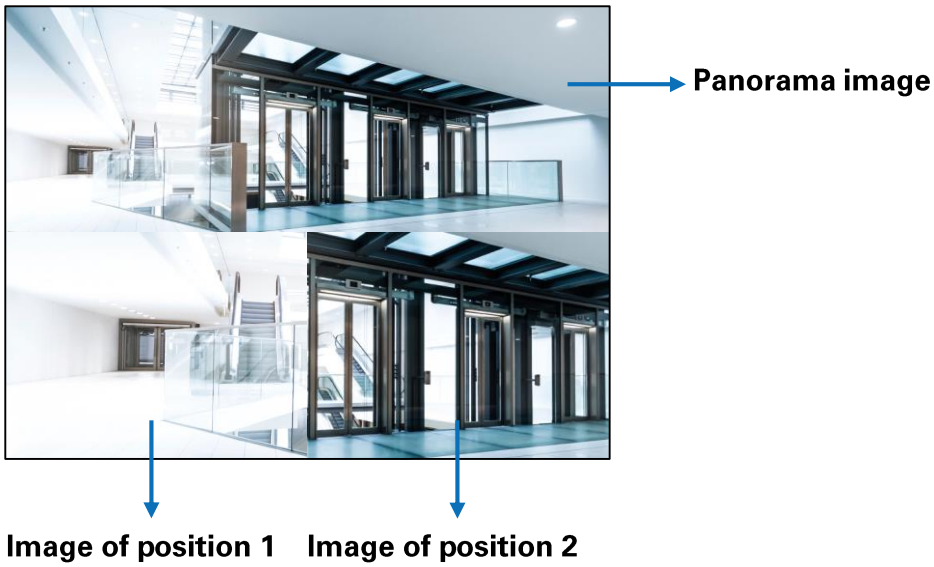
The video settings are saved by long pressing one of the position buttons.

Note: The DoorKeeper always sets the position to position 1 during a call. Position 1 should therefore be set as the default view of the door terminal.

5.6.5.3 Panorama image with TouchEntryXS

The TouchEntryXS is equipped with a 180° wide-angle lens. Position 3 displays the entire camera image as a panorama image with the sections of position 1 and 2. This makes it possible to display certain areas within the camera image without changing the position and at the same time to have an overview of the entire area in front of the door terminal.

Image of position 3:



5.6.6 Using the Telephone Keypad to control the door terminals

If no DoorKeeper from Adatis is used as remote station, the door terminal can be controlled via the keys of the IP telephone or the softphone.

Note: Controlling the door terminal is only possible with an active connection between the door terminal and the remote station.

Both SIP Info and RFC2833 are supported for transmitting DTMF signals.

The key assignment can be adapted via the EventHandler. (See chapter 5.9)

Default functions of the DTMF signals:

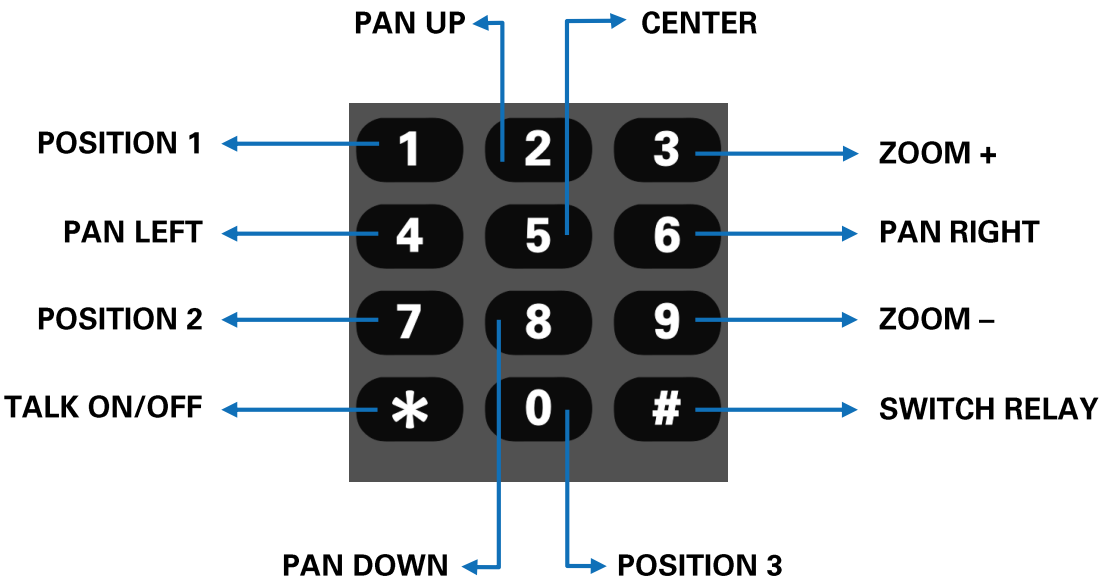


Figure 102: Telephone keypad overview

5.6.6.1 Switching the relay at the door terminal (open door)

By pressing the *'hash'* key on the IP telephone, the relay on the door terminal is switched.

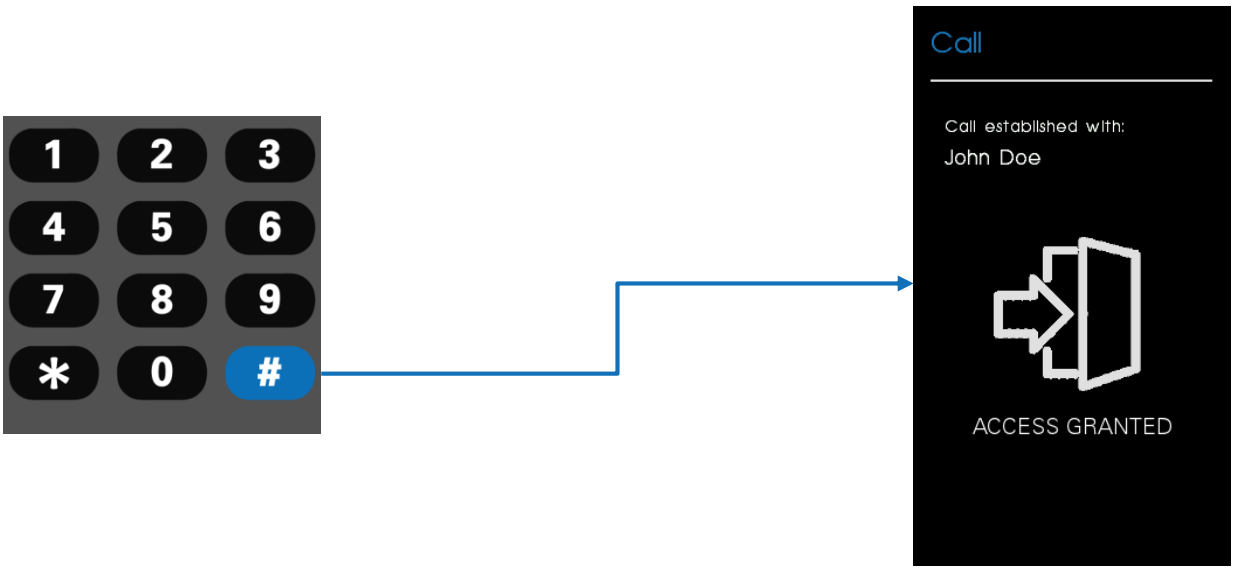


Figure 103: Switching the relay via the telephone keypad

5.6.6.2 Switching Audio Connection On/Off

The *'star'* key on the IP telephone is used to establish or terminate the audio connection.

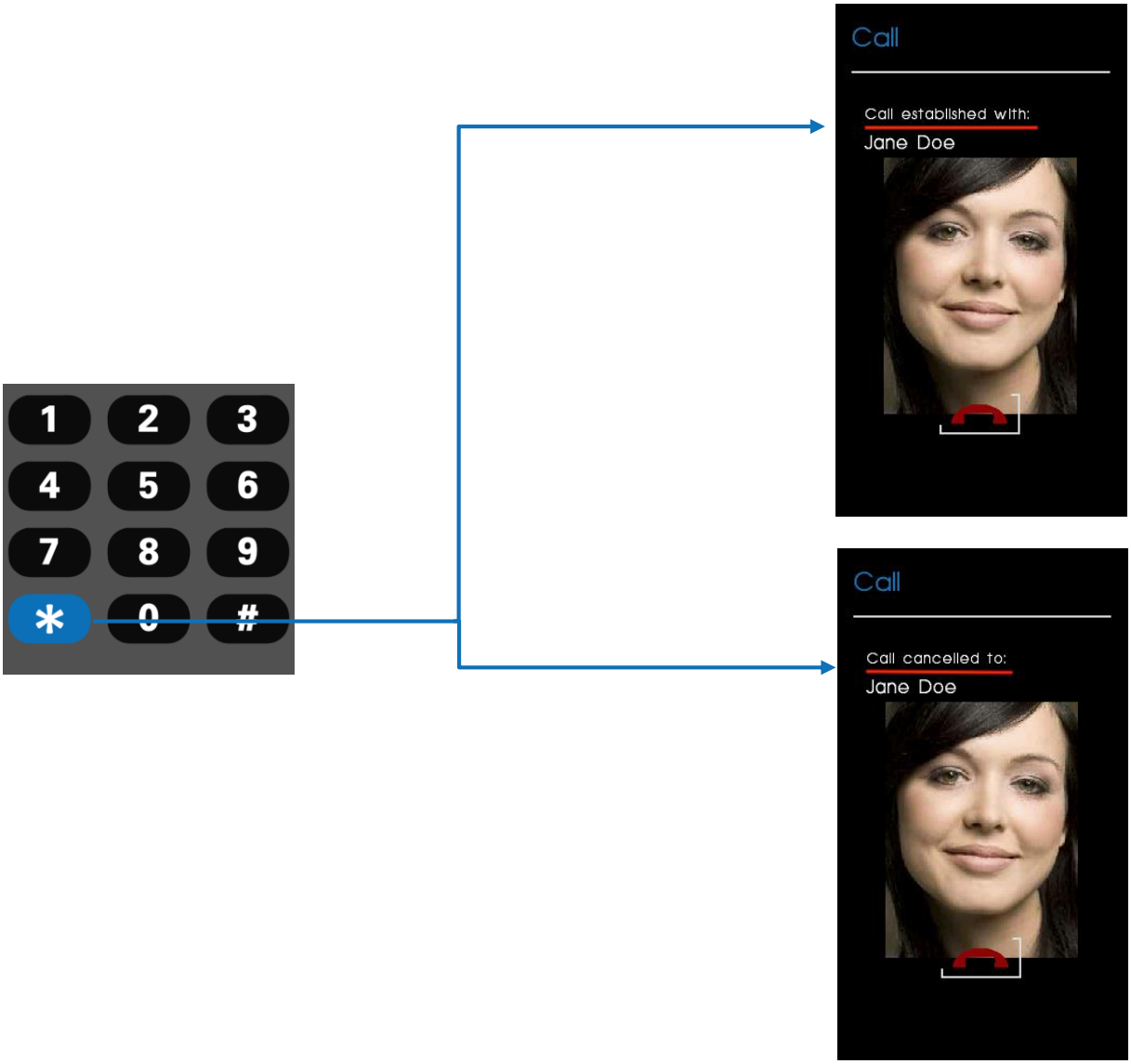


Figure 104: Switching Audio Connection On/Off

5.6.6.3 Zoom of the camera

The button *'3'* on the IP phone zooms in on the camera image and the button *'9'* zooms out.

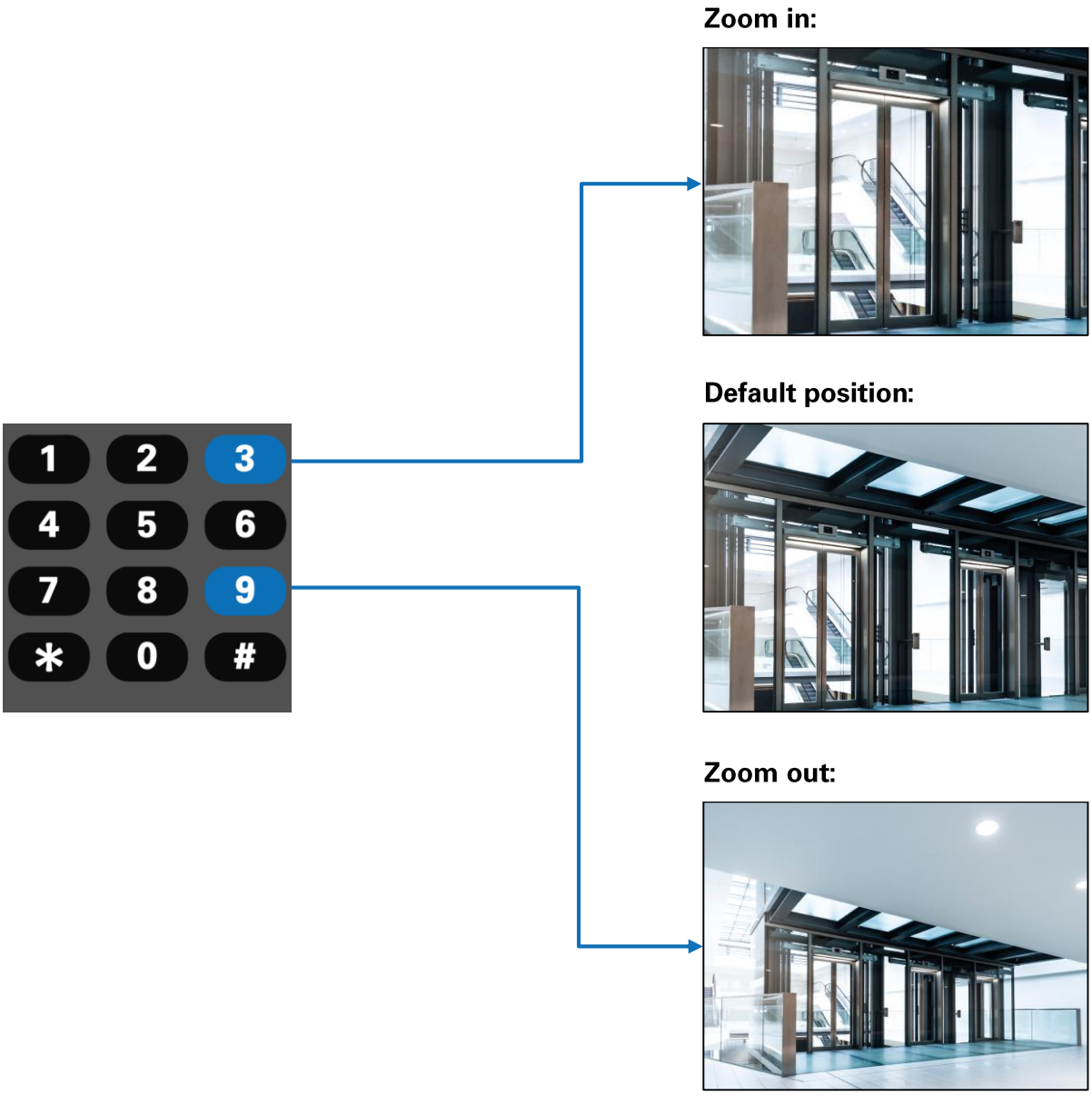


Figure 105: Zoom of the camera

5.6.6.4 Moving the Camera Image

The *'2'* key moves the camera image up, the *'8'* key moves it down.

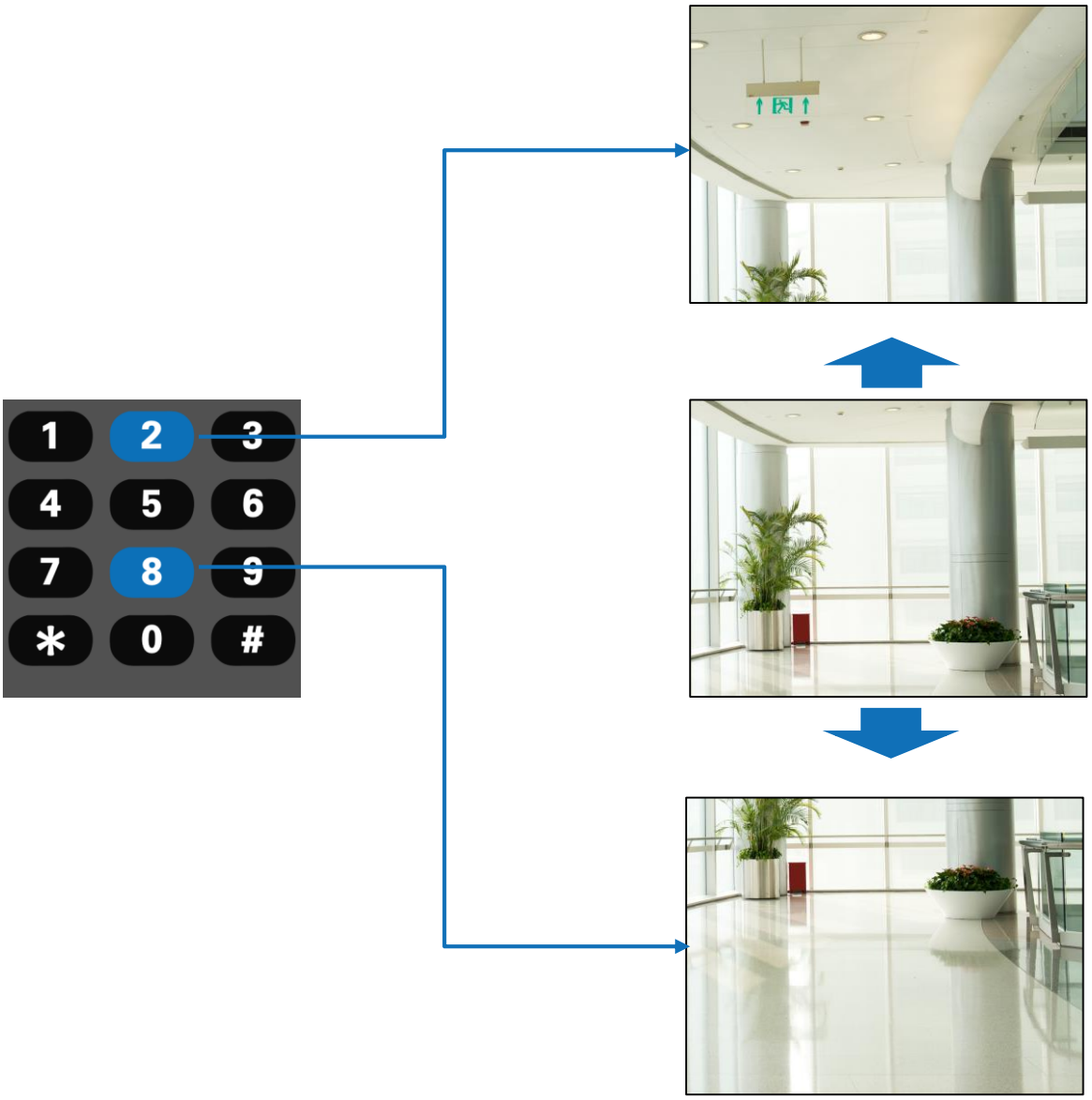


Figure 106: Moving the camera image up / down

The *'4'* key moves the camera image to the left, the *'6'* key to the right.

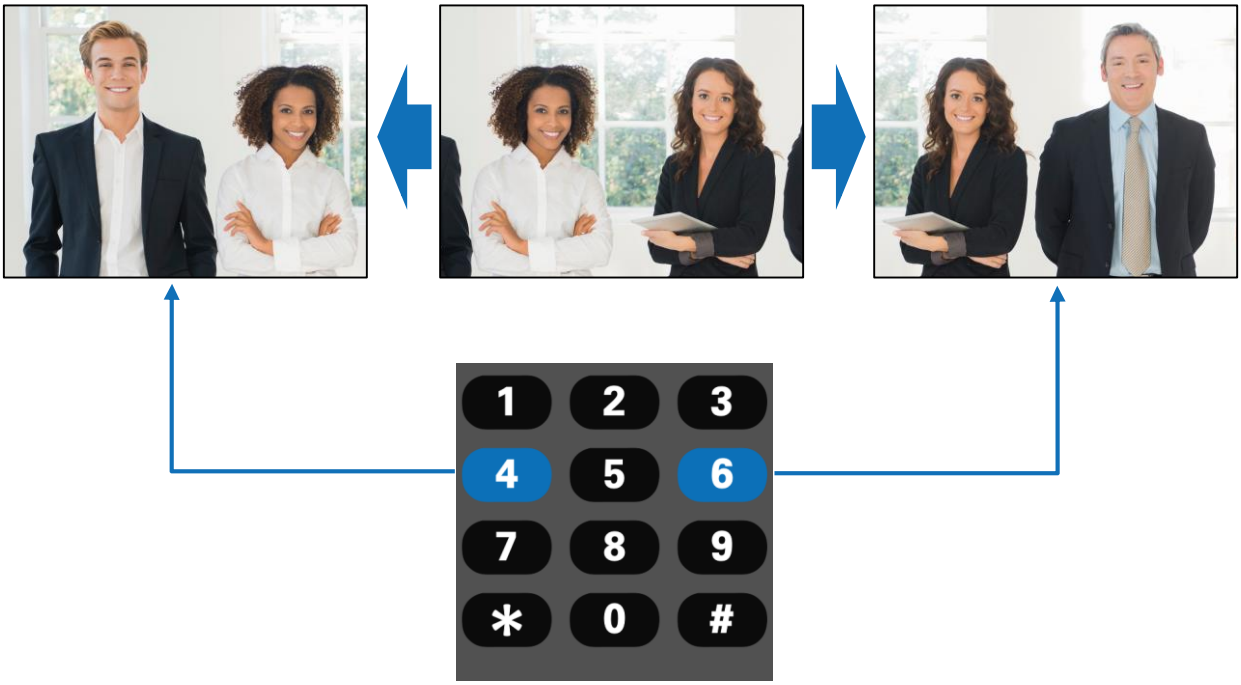


Figure 107: Moving the camera image left / right

5.6.6.5 Changing the position of the camera image

The buttons *'1'*, *'7'* and *'0'* can be used to switch between the stored positions of the camera.

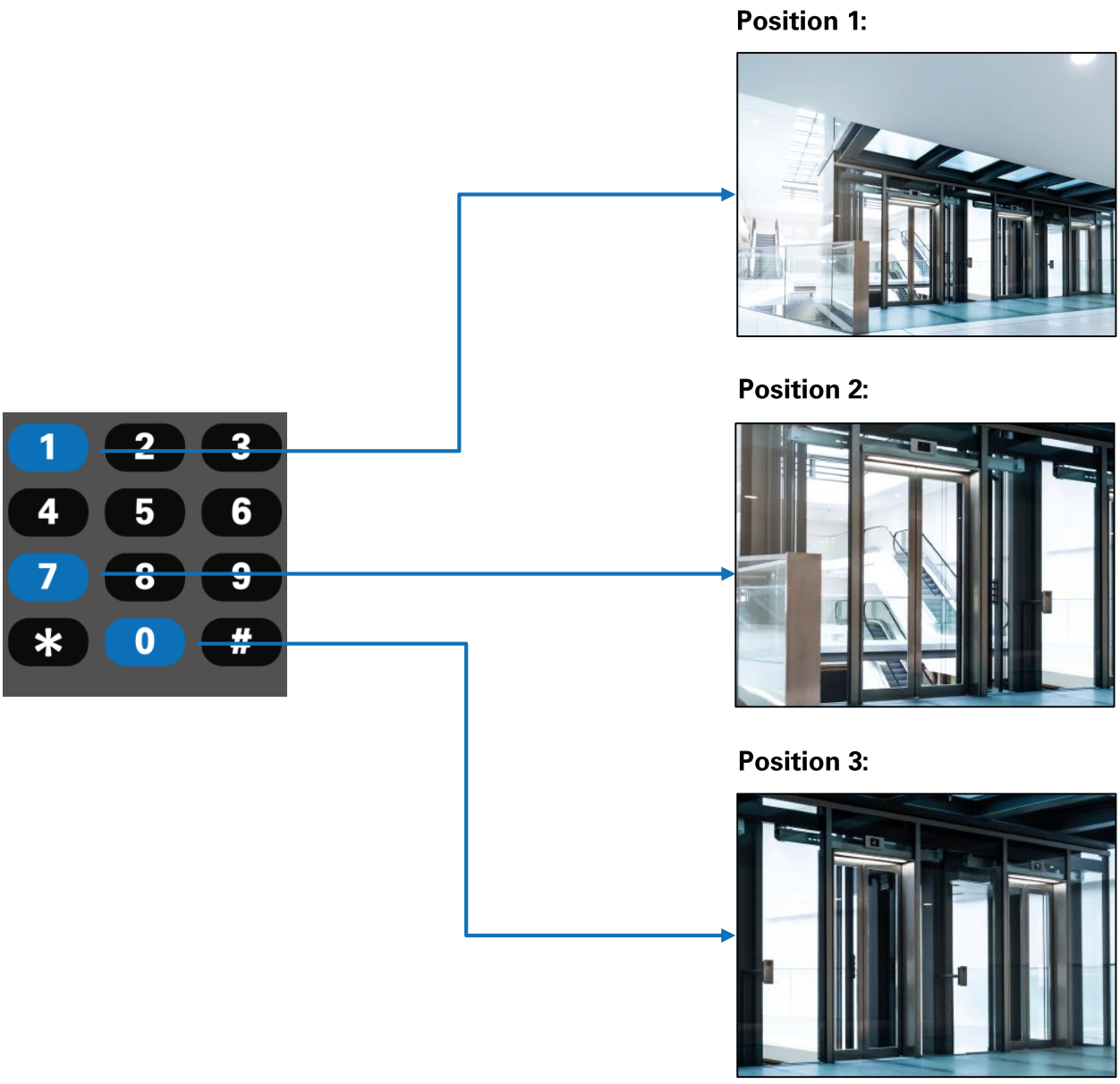


Figure 108: Changing the position of the camera image

If the current position has been changed during a connection, for example by zooming in, the *'5'* key can be used to return the camera to its original position.

Figure 109: Resetting the Camera Position Using the Telephone Keypad

5.7 Motion JPEG Video

The video image of the camera of the door terminals can be called up separately. This can be used, for example, in applications that do not support video with the SIP connection.

5.7.1 Retrieving Motion JPEG Video and Single Image from the Camera

Retrieving Motion JPEG video is only possible on the local network. The video can be retrieved via the video port of the door terminal.

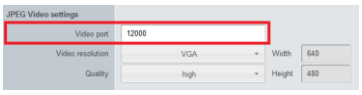


Figure 110: Video Port of the Motion JPEG Video

The video port can be looked up on the door terminal website under the menu item *'Audio/Video'*.

In the door terminal the video port is called *'Server Port'* and can be found under the heading *'JPEG video settings'*.

For the video port the port number **12000** is set by default.

A single image of the camera can be retrieved from the following two addresses:

<IP-Address>:<Video-Port>/singleframe
<IP-Address>:<Video-Port>/video.jpg

The video can be retrieved from the following two addresses:

<IP-Address>:<Video-Port>/stream
<IP-Address>:<Video-Port>/video.mjpg

Note: To make the video image available outside the local network, port forwarding must be used for the video.
This is a task of the network administrator and not a setting in the door terminal.

5.7.2 Retrieving Motion JPEG Video using Snom IP Phones

Because Snom IP telephones are frequently used and the door terminals have an interface especially for this purpose which can be used to retrieve the Motion JPEG video, it should be mentioned here how the video image can be made available on the Snom IP telephones.

First you have to switch to the Snom IP phone's website. There the page *'Function keys'* must be called up under *'Setup'*.

There any key can now be reconfigured by selecting the type *'Action URL'* instead of the *'Key event'*.

The following address must be entered as the number and the setting must be adopted:

<IP-address>/video.xml

The video can then be called up manually using the button on the Snom IP phone.

Note: The video image can only be retrieved via the local network unless a port forwarding of the video has been performed.

5.8 Interface Configuration (Inputs and Outputs)

5.8.1 Overview of Interfaces

The door terminals have two trigger inputs and, if necessary, a sabotage contact and an acceleration sensor. In addition, the door terminals have one or more internal relays, for example to switch a door opener. Additional relays can be switched via an IP relay. The Wiegand output is available for integration into existing access control systems.

The respective installation instructions show where the connections can be found on the circuit board of the door terminal.

5.8.2 Trigger Inputs

The trigger inputs can be used to connect mechanical bell buttons if a mechanical button is preferred or to ensure barrier-free operation for example of a bell.

The trigger inputs can be accessed via the menu item *'Interface configuration'* on the website.

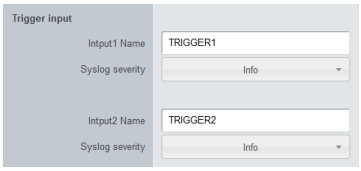


Figure 111: Trigger Inputs

Input Name: Each trigger input has its own name, which can be changed here. If the input changes, an entry with the name of the trigger input appears in the syslog.

Syslog Serverity: Every time the trigger input is triggered, this is written to the system log. (See chapter 5.11.3)
If a syslog server is used, the severity level can be set here.

Note: To switch a trigger input, the respective input must be connected to the ground of the door terminal (GND).

5.8.3 Sabotage protection

Depending on the hardware used, the door terminal has, in addition to the two trigger inputs, a sabotage contact and an acceleration sensor to protect the door terminal.

The *'Sabotage'* menu can be opened through the configuration on the LCD display.

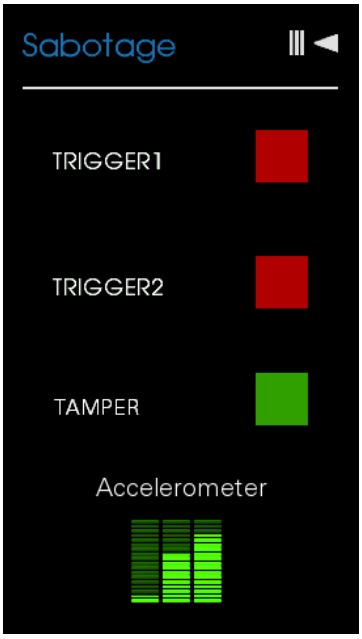


Figure 112: Configuration on the LCD display - sabotage protection

Trigger1 und Trigger2: The names of the trigger inputs 1 and 2, as they are called on the website. (See chapter 5.8.2)

Tamper: The name of the sabotage contact.

If the inputs are activated, they are shown on the LCD display in green, otherwise in red.

Note: When installing the door terminal, the display can be used to check whether the sabotage contact is correctly connected. This is the case if the rectangle next to it is green.

Accelerometer: This indicates whether the door terminal is being moved.
If the door terminal is moved too much, the same event is triggered as with the sabotage contact. The sabotage contact must therefore be used for configuration in the EventHandler.

Note: At door terminals, without additional sabotage contact and without the acceleration sensor, trigger input 1 is used as sabotage contact. However, it can also be used as a normal trigger input on request.

The connection of the sabotage protection can also be found on the website via the *'Interface configuration'* menu.

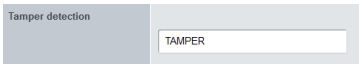


Figure 113: Tamper detection

The name of the sabotage contact can be changed here. If the sabotage contact is triggered, an entry with the name is written into the syslog.

5.8.4 Internal relay

The settings of the internal relay can be found under the menu item *'Interface configuration'* on the website.

Figure 114: Internal relay

Relay Name: The name of the relay can be changed here. This name also appears in the syslog when the relay is switched.

The relay can be switched via the button.

Usually the relay is switched by pressing the *'#'* key on the remote station or by pressing the door opener in the DoorKeeper while a connection is established.

Note: The connections for using the internal relay can be found in the installation instructions for the respective door terminal.

Caution: The use of the internal relay to open a door is considered a safety risk and is therefore not recommended. Instead, an IP relay should be used where the wiring to open the door is within the area to be secured, such as the home.

5.8.5 Using an IP relay

Up to 6 additional relays can be added to the door terminals by using the IP relay. The setup is done via the website under the menu item *'Interface configuration'*.

Note: For the simple configuration described here, use the IP relay distributed by Adatis with article number #8280.

All other IP relays must be configured directly via the EventHandler and integrated using the HTTP protocol. The document *'Manual EventHandler'* provides help for this.

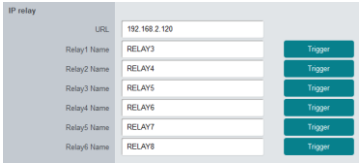


Figure 115: IP relay

To address the IP relay, the IP address of the IP relay must be entered in the URL field.

The relays are then visible with their names and can be switched using the adjacent buttons.

5.8.6 Wiegand Output

The Wiegand output can be used to integrate Adatis door terminals into an existing access control system. As soon as an access event is triggered, a corresponding message is issued at the Wiegand output.

The Wiegand interface can be configured on the website via the menu item *'Access options'*.

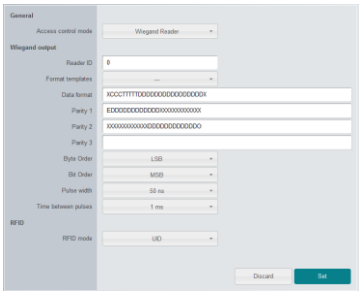


Figure 116: Wiegand Output

The access control mode must be set to *'Wiegand Reader'*.

The document *'Short manual RFID'* should be used to configure the Wiegand output.

If the access control mode is set to *'Wiegand Reader'*, access is not granted by the door terminal but by the connected access control system when a PIN is entered, an RFID card is held in front of the reader or identification is made via the face. This is shown on the LCD display as follows:

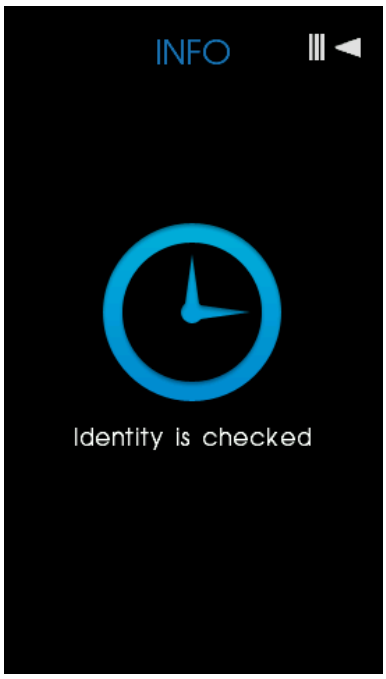


Figure 117: Identity check in the access control mode *'Wiegand Reader'*

Note: In order to receive feedback if the access control system has granted access, one of the trigger inputs can be used. An example can be found in the document *'Manual EventHandler'*.

5.9 EventHandler

The EventHandler is the main connection between the inputs and outputs. Via a simple text file, various events can be configured to trigger a certain action. For example, as soon as a person is called at the door terminal, it is possible to switch on an additional light and switch it off again after the call.

The following diagram illustrates the possibilities of the EventHandler:

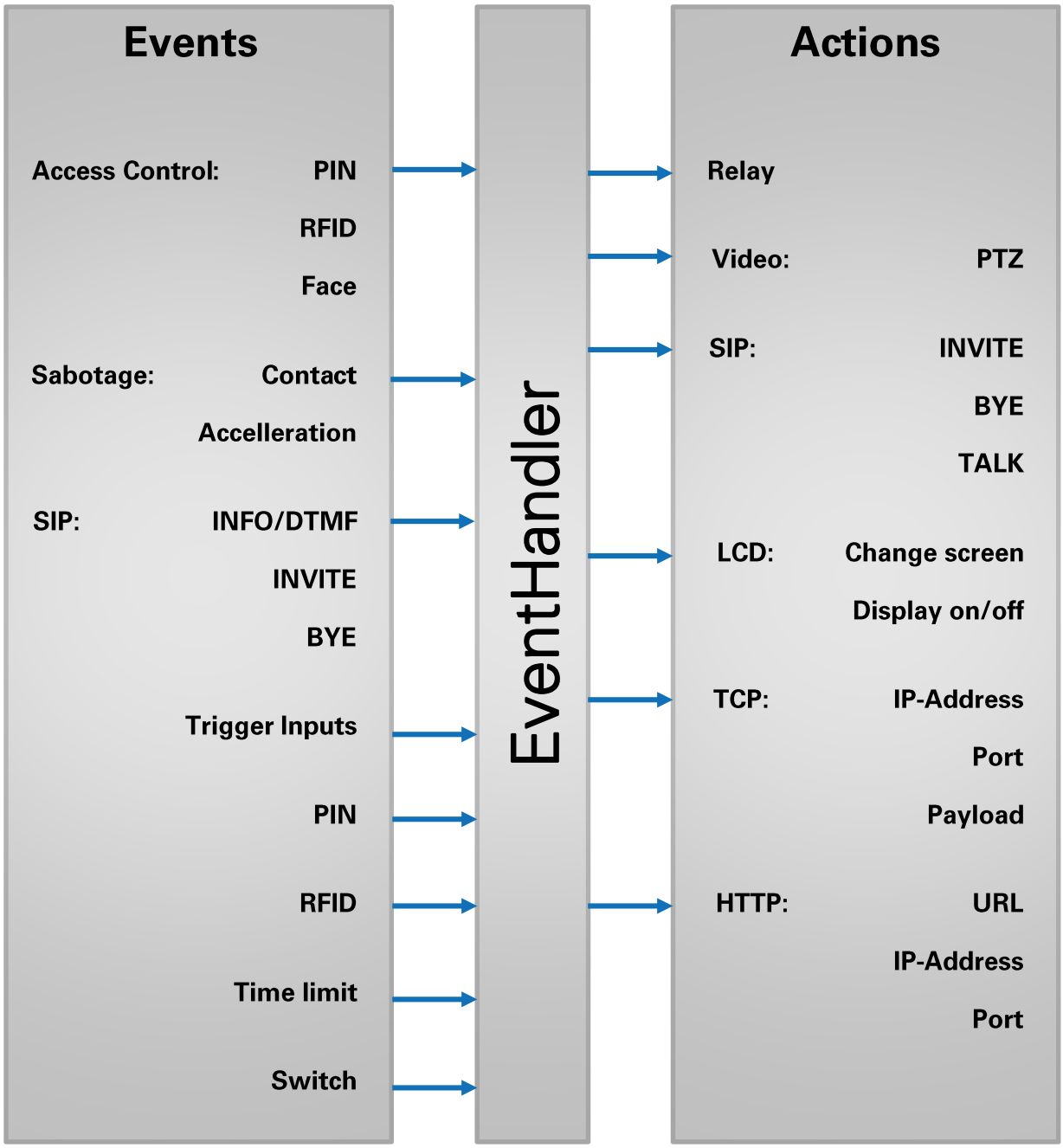


Figure 118: Diagram of the EventHandler

5.9.1 Configuration of the EventHandler

When delivered, the EvenHandler is already equipped with the most important standard functions. As long as the standard functionality is sufficient, a configuration of the EventHandler is not necessary. Otherwise the EventHandler file can be changed on the website of the door terminal under the menu item *'EventHandler'*.

Note: The preconfigured events are required for the functionality of the door terminal. Deleting an action from the EventHandler leads to a loss of function at the door terminal. It is recommended to only change actions or add new ones, but not to delete actions.

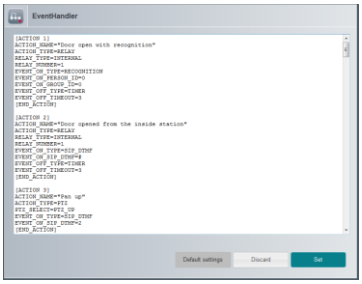


Figure 119: EventHandler

Changes to the EventHandler can be entered directly in the browser.

The EventHandler file consists of many actions that begin with the line [ACTION X] and end with the line [END_ACTION].

Factory settings: Overwrites the EventHandler file with the factory settings. All changes will be lost.

Figure 120: EventHandler - All Entries have been successfully parsed

After *'Set'* the EventHandler file is checked for possible errors. The individual actions are checked successively.

If an action cannot be interpreted by the EventHandler, an error message is displayed, otherwise a message is displayed that all entries have been processed successfully.

Note: The document *'Manual EventHandler'* describes how different events can be connected with different actions.

5.9.2 Backing Up and Restoring the EventHandler Configuration

The EventHandler configuration can be downloaded at any time from the website of the door terminal under the menu item *'Upload/Download'*. The download starts via the *'EventHandler'* button.

Usually the file is called as follows:

Events.dat

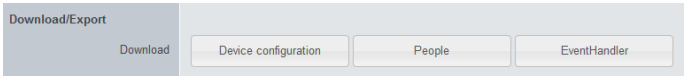


Figure 121: Backup the EventHandler file

The EventHandler configuration can be reloaded into the door terminal by opening the file in a text editor and pasting the entire content on the website of the door terminal under the menu item *'EventHandler'*.

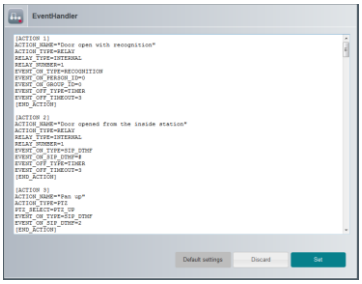


Figure 122: Recovering the EventHandler Configuration

After *'Set'* the EventHandler file is checked for possible errors and then updated.

Note: The EventHandler configuration can also be uploaded to other door terminals in the same way.

5.10 Administration of the door terminals using an administration server

The personal database, the device configuration and the access of the persons from the personal database can be managed by an administration server. The door terminals can be integrated into an existing system with an administration server through the XML-RPC interface.

Note: The company Adatis offers the product "FaceAdmin" as an administration server in different designs and different features. For example as face recognition server with artificial intelligence.

The following section describes how the Administration Server can be configured to communicate through the XML-RPC interface, what data to synchronize, and how to configure the Administration Server to manage access for people.

5.10.1 Setting up server access

The settings for the Administration Server can be found on the website under the menu item *'Administration Server'*.

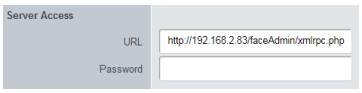


Figure 123: Address of the administration server

URL: To connect the door terminal to the Administration Server, the address of the server must be entered.

Password: Here you can enter the password that is used on the server for authenticating the door terminal.

The door terminal signs in with its unit name. To change the unit name, see chapter 2.5.4.

5.10.2 Synchronisation of data

The settings for the Administration Server can be found on the website under the menu item *'Administration server'*.

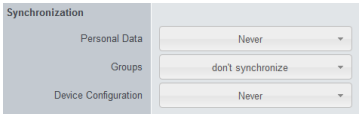


Figure 124: Administration server synchronization

Personal data: Sets the interval respectively the time when the personal data is to be synchronized from the Administration Server to the door terminal. Persons created on the door terminal are overwritten.

Groups: If the persons in the personal database have been assigned to groups, the groups must also be synchronized.

Device Configuration: Sets the interval respectively the time when the device configuration is to be synchronized from the Administration Server to the Door Terminal. Changes made locally to the device configuration are overwritten during synchronization.

5.10.3 Access control provided by the server

The setting for access control can be found on the website under the menu item *'Access options'*.

Figure 125: Access control provided by the server

To manage access through the administration server, the access control mode *'IP Reader'* must be selected.

5.10.4 Settings for the FaceAdmin

The following settings should be used with the FaceAdmin:

URL:	**http://<IP-Address>/faceAdmin/xmlrpc.php**
Personal data:	**30s**
Groups:	**synchronize**
access control mode:	**Autonomous / IP reader**

Note: If the *'Autonomous'* access control mode is selected, the locally stored data is used to check whether a person is granted access or not.
In the *'IP Reader'* mode, the Administration Server decides whether the person is granted access. This makes sense if access is time controlled.

The FaceAdmin can also be used as a syslog server. The IP address of the FaceAdmin must be entered as the address for the Syslog server.
(See chapter 5.11.3.3)

Note: Synchronizing the device configuration with the FaceAdmin is currently not possible.

5.11 System

5.11.1 Determining the system data of the door terminal

The system data includes the device type, the MAC address, the firmware version and the hardware used.

The firmware version is displayed each time the door terminal is restarted. (See chapter 2.2)

All system data can also be viewed on the website under the menu item *'System status'*.

Figure 126: System data of the door terminal

In addition to the **firmware version**, the **device type** and the **MAC address** of the door terminal are also displayed here.

By displaying the hardware configuration, it is possible to find out with which display etc. the door terminal has been delivered and also whether the door terminal has an RFID option.

5.11.2 Backing up and recovering the device configuration

The device configuration can be downloaded at any time from the website of the door terminal under the menu item *'Upload/Download'*. The download starts via the *'Device configuration'* button.

Usually the file is called as follows:

FaceEntry_config.dat

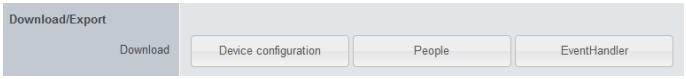


Figure 127: Back up of the device configuration

The same file can also be uploaded to the door terminal again by first selecting the file on the same page under *'Update/Import'* and then pressing the *'Upload'* button.

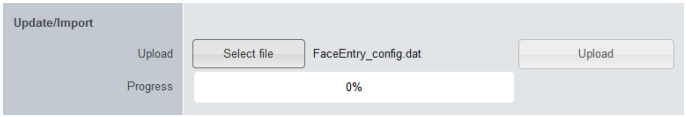


Figure 128: Restoring the device configuration

Note: The device configuration file can also be uploaded to other door terminals in the same way.

The network settings are not saved with the device configuration. The network settings are also not overwritten when the device configuration is restored.

5.11.3 System Log

The door terminals have a system log in which, for example, the following things are logged:

- - System status
- - error messages
- - access events
- - Connection establishment/disconnection to a remote station
- - Switching a relay
- - Triggering a trigger input
- - EventHandler Actions

5.11.3.1 Internal system log

The internal system log can be viewed on the website via the menu item *'Diagnosis'* and then selecting the *'Syslog'* button.

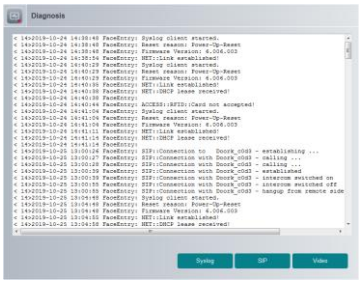


Figure 129: The system log in the web view

To update the system log, press the *'Syslog'* button again.

Note: The entries of the system log are kept in a ring buffer. This means that the oldest entries are replaced by new ones as soon as the memory is full.
For this reason, a syslog server is recommended for storing the complete system log. (See chapter 5.11.3.3)

5.11.3.2 Downloading the internal system log

The internal system log can be copied directly from the web view as shown in chapter 5.11.3.1.

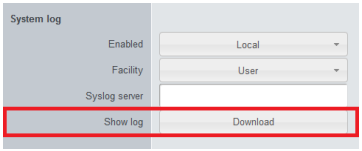


Figure 130: Downloading the internal system log

Alternatively, the internal system log can be downloaded via the *'System status'* menu item using the corresponding button.

Usually the file is called as follows:

FaceEntry_syslog.dat

This file can be opened with any text editor.

5.11.3.3 Setting Up a Syslog Server

It is possible for the door terminal to send the data to a syslog server instead of storing the system log internally.

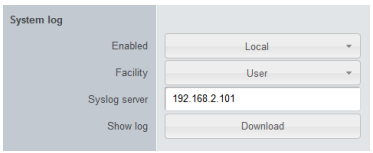


Figure 131: Setting Up a Syslog Server

Activated: This makes it possible to switch off the system log, to use only the internal memory for the system log, or to send the system log to a server. It is also possible to store the system log internally and simultaneously on a server.

Note: When using a syslog server, it makes sense to also save the system log internally.
The preferred setting should therefore be as follows:

Local+Server

Facility: It is possible to specify different locations for storing the system log on the server so that one syslog server can be used by several door terminals.
The door terminals offer *'User'* and *'Local0 -Local7'* for this.

Note: The Syslog server must be set accordingly so that each door terminal writes to a different file.

Syslog server: The URL or IP address of the syslog server must be entered here.

5.11.4 Firmware

5.11.4.1 Update of the Firmware

In order to provide new features on the door terminals, a firmware update may be necessary.

Note: A firmware update should only be performed by a trained person in consultation with Adatis or an Adatis sales partner.

Before a firmware update, it is recommended to backup the personal data (see chapter 4.5.1), the device configuration (see chapter 5.11.2) and the EventHandler configuration (see chapter 5.9.2).

The firmware update can be done on the website under the menu item *'Upload/Download'*.

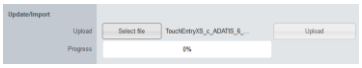


Figure 132: Update of the firmware

There the firmware file must be selected via *'Select file'*.

In the following, the name of a firmware version is given as an example:

TouchEntryXS_c_ADATIS_6_006_003.gz

Note: Even if the extension of the firmware file suggests it, the firmware cannot be edited or unpacked with other programs. The firmware data is stored in a proprietary format.

Figure 133: Firmware will be uploaded

The firmware can be uploaded to the device via *'Upload'*.

Attention: The door terminal must under no circumstances be disconnected from the power supply during the firmware update!
Otherwise it could become unusable.

After the firmware update, the door terminal restarts automatically.

The device configuration, the event handler configuration and the personal database remain untouched during a firmware update.

5.11.4.2 Resetting the door terminals to factory defaults

On the website, the door terminal can be reset to factory settings under the menu item *'Upload/Download'*.

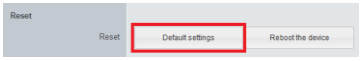


Figure 134: Reset the door terminal to factory default settings

Resetting to factory settings resets all settings of the door terminal, including the EventHandler, except the personal database.

After resetting, the door terminal restarts and can be reached again via the fixed IP address of the factory setting. (See chapter 2.5.1)

Note: The personal database including the groups can be completely deleted via the button *'Delete all'* under the menu item *'Persons'*.

6 Support

6.1 Troubleshooting

6.1.1 Troubleshooting Communication

6.1.1.1 The communication always terminates after a certain time.

If the connection to a remote station is repeatedly interrupted after a certain time, this is often due to the fact that the connection duration is set to a certain value in the settings of the door terminal and the connection is then automatically terminated by the door terminal. Chapter 5.6.2 provides information on how the setting can be changed.

6.1.1.2 Monitoring the camera is not possible with the DoorKeeper.

If the door terminal is called from the DoorKeeper, this is done without connecting the audio connection, only the video image is transmitted.

Because permanent monitoring of the door terminal's camera is not desired, the connection is interrupted by the DoorKeeper after 7.5 minutes without switching on audio.

Note: If other softphones are used, the softphone may terminate the connection much earlier.

6.1.1.3 The video image is not displayed during a connection.

If the video image does not show up when connected via the internal registrar or a direct call, please contact the Adatis support team. (See chapter 6.3)

If the connection is established over a SIP server, the following problems may occur:

Asterisk server: The Asterisk servers do not support video previews. The video should work as soon as the call from the door terminal has been accepted.

FRITZ!box as SIP server: The FRITZ!box does not support SIP video. It is therefore not possible to receive video through the Fritz!Box. If the FRITZ!Box is used locally, the use of Motion JPEG video can be set up when using the DoorKeeper software. Chapter 5.7 shows how to set it up.

Adatis SIP Server: If the Adatis SIP Server is used, the bandwidth of the Internet connection to which the door terminal is connected may not be sufficient to transmit the video. The document *'Quick start video formats'* can help in this case.

Please also note that the video must be sent for each called remote station. If there are several entries in the SIP-URI of one person, the required bandwidth increases accordingly.

6.1.1.4 *The door terminal cannot be called from the remote terminal over the Adatis SIP Server.*

If the door terminal can call the remote station over the Adatis SIP server, but a connection in the other direction is not possible, this is often a NAT problem.

This problem can be solved by changing the setting *'NAT Keep Alive'* under the menu item *'SIP configuration'* to *'Options'* on the website of the door terminal. This means that the door terminal periodically notifies the Adatis SIP server and remains accessible. (See chapter 4.3.3)

6.1.2 Troubleshooting Registration

6.1.2.1 The door terminal cannot register with the Adatis SIP Server.

If the door terminal cannot register with the Adatis SIP Server, the login data should first be checked. Figure 56 in chapter 4.3.3 shows how to enter the login information correctly.

If the login data are entered correctly and registration with the Adatis SIP server still does not work, check whether the Internet connection itself works, for example by accessing a website from a computer in the same local network.

If this also works, it must be checked whether the gateway address and the DNS server have been entered correctly in the settings for the door terminal. Chapter 2.5 shows how to change the network settings. If DHCP is activated, you must check whether the DNS server is working correctly. This should be done by the network administrator.

If the gateway address and the DNS server have been entered correctly, a support ticket can be sent to the support email address with all the details and steps that have already been done. (See chapter 6.3)

The Adatis support team will then test the SIP server accounts and give you feedback whether the accounts have errors or are working properly.

If no errors are found in the SIP server accounts, then the error is in the local network setup. Please contact your network administrator now so that he can correct the error.

6.1.3 Troubleshooting face recognition

6.1.3.1 After the door terminal has been mounted, no person will be identified by face recognition.

If the enrollment was done before the door terminal was installed, it is possible that the face recognition will not function as well due to the changed light and position after the door terminal was mounted. If possible, the enrollment should always be done after the mounting of the door terminal. Repeat the enrollment if necessary.

If this does not result in success, please check whether the tolerance for face recognition is set correctly. If necessary, increase the value for the tolerance. (See chapter 5.5)

6.1.3.2 Outdoor face recognition does not work properly.

If the sunlight is too strong or the counterlight is too strong, the camera sensor of the door terminal may not recognize the face correctly. In this case, ensure better shadowing of the door terminal or mount it in another place where there is no direct sunlight.

The installation instructions for the respective door terminal provide information on the choice of the installation location.

6.2 Troubleshooting using the diagnosis on the door terminal website

The diagnosis can be found on the website under the menu item *'Diagnosis'*.

By selecting one of the following three categories, the corresponding information is displayed.

- **Syslog:** Shows the system log if it has been saved internally. (Administration of the syslog see chapter 5.11.3 and details in chapter 6.2.1.1)
- **SIP**: Shows the current registrations and the SIP connections of the door terminal. (Details see chapter 6.2.1.2)
- **Video**: Shows whether a video connection to a remote terminal exists at the moment and whether the Motion JPEG video is retrieved. (For details, see chapter 6.2.1.3)

6.2.1.1 Diagnosis Syslog

The entries are recorded chronologically in the system log. The date and time and the name of the door terminal are written before each entry.

Of particular interest is the part after the device name. In the following only the most relevant messages will be explained.

No.	Message in the syslog	Meaning
1	SYSTEM::Successfully started!	The door terminal has been successfully booted.
2	Reset reason: Software-Reset	The door terminal was restarted by the software.
3	Reset reason: Power-Up-Reset	The door terminal was restarted after disconnecting the power supply.
4	Firmware Version: 6.006.003	Shows the firmware version at startup.
5	SYSTEM::Firmware patch processed!	A new firmware version has been uploaded.
6	ACCESS::Access granted! NACHNAME, VORNAME, Pers.-ID:	Access was granted to the person named.
7	SIP::Connection to USERNAME – establishing	The door terminal tried to establish a SIP connection with the USERNAME.
8	SIP::Connection with USERNAME – calling	A SIP connection with the USERNAME was established.
9	SIP::Connection with USERNAME - declined	The remote station has rejected the call with the USERNAME.
10	SIP::Connection with USERNAME – cancelled locally	The SIP connection with the USERNAME was terminated by the door terminal.
11	EH::Internal relay "RELAY1" switched ON /OFF	The relay with the name *'RELAY1'* has been switched.
12	EH::Action:"ACTIONNAME"	The action in the EventHandler with the ACTIONNAME was executed.

Note: If number 3 in the table occurs more often without a possible reason, there may be a problem with the power supply.

6.2.1.2 *Diagnose SIP*

This view shows all SIP connections and their registrations.

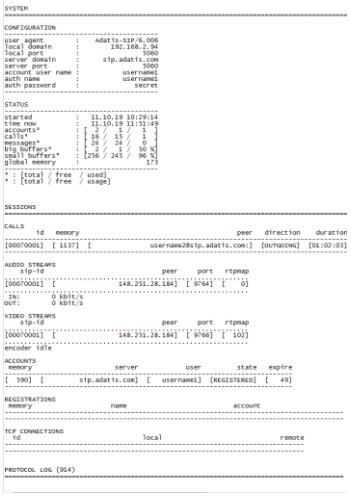


Figure 135: Diagnosis SIP

CONFIGURATION: Shows the SIP login data for the SIP server.

STATUS: Calls shows the currently available and used channels for a connection.

CALLS: Shows all SIP connections with the respective addresses and call direction.

AUDIO-STREAMS: Shows the active audio connections, with the respective address.
However, this does not indicate whether audio is actually being transmitted, as audio may first have to be activated by pressing the '*' key. (See chapter 4.3.6.5 respectively. 5.6.6)

Note: If IN and OUT are set to a value in kbit/s, audio is transmitted. Then only one SIP connection can be listed under CALLS.

VIDEO-STREAMS: Shows the active video connections with the remote stations and the respective address. Motion JPEG Video is not displayed here. (To view the Motion JPEG video connections, see chapter 6.2.1.3)

ACCOUNTS: Shows to which SIP server the door terminal is registered and the status of the registration.

REGISTRATIONS: Lists the remote stations that have registered with the internal registrar of the door terminal. The user name for a call from the remote terminal can also be read from this. (See chapter 4.3.2)

TCP CONNECTIONS: If a SIP connection is established with TCP instead of RTP, the TCP connection is shown here.

PROTOCOL LOG: The heading is followed by the last SIP messages exchanged between the door terminal and the remote stations or the SIP server.

6.2.1.3 *Diagnosis Video*

This view displays all video connections.

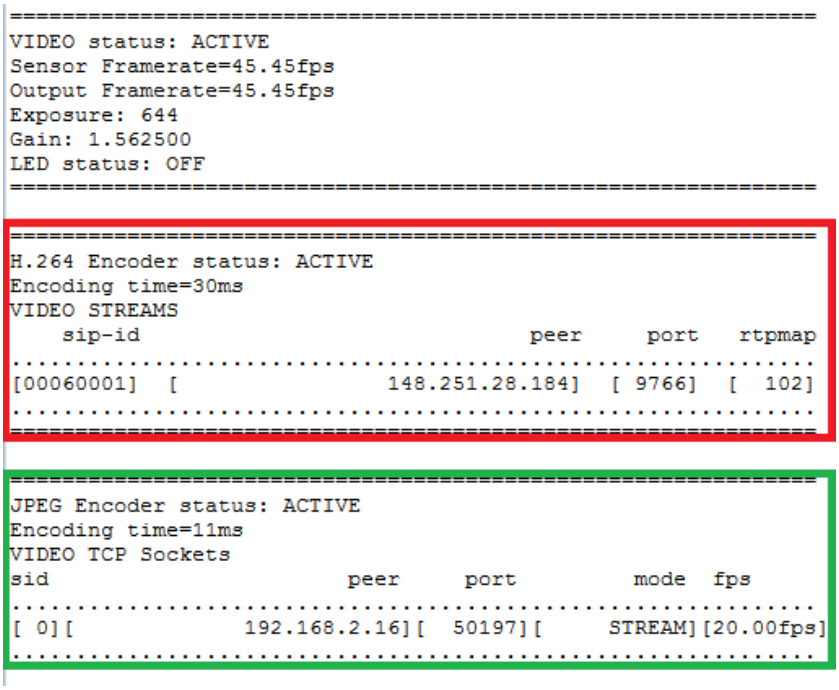


Figure 136: Diagnosis Video

If the H264 video is retrieved for communication with a remote station, a new entry will appear at the location marked in red with the address to which the video is sent.

When the Motion JPEG video is retrieved, a new entry appears at the green location with the address to which the video is sent.

6.3 Creating a Support Request

If you have any problems which the manual could not help you with, please send the completed document *'Support request'*, which can be downloaded from the Adatis homepage under the menu item *'Contact'*, together with the required documents to the Adatis support e-mail address:

support@adatis.com

7 Further guidance

In this chapter, the documents referred to in this manual are named and described briefly.

7.1 Manual FaceAdmin

The FaceAdmin user manual describes how to operate the FaceAdmin server and how to place a door terminal under the administration of the FaceAdmin. It also describes how to assign individual persons and groups to the respective door terminal in order to synchronize the personnel data from the FaceAdmin Server to the door terminal.

7.2 Manual EventHandler

This document describes the EventHandler of the door terminal. In addition to the syntax in which the individual actions must be written, many examples show what the EventHandler can be used for.

7.3 Short manual RFID

The document shows which RFID card types are supported by the door terminals and how the door terminals can be adjusted to the respective card type.

It also describes how the Wiegand interface can be set to integrate the door terminals into an existing access control system.

7.4 Quick Installation SIP-server Adatis

This document describes how to access the Adatis SIP Server in order to establish communication between the door terminal and the remote station via the Internet. It describes how to set up the door terminal and also the DoorKeeper App so that both can communicate with each other.

7.5 Quick start video formats

The document shows how to retrieve the Motion JPEG video from the door terminal. It also explains which resolutions are possible with the door terminals and how the quality and bit rate of the video should be selected so that the video image can be transmitted over the Internet in good quality.

7.6 Manual 2Wire Converter

This document describes how to use the 2Wire Converter to establish an Ethernet connection over a 2-wire line.

Glossary

2-Wire	A 2-wire is a solid copper conductor pair that is usually used for the connection of doorbell systems.
admin	Short form of the administrator. A person who performs the administrative tasks of configuring the door terminals or the network. This person has more rights than other users.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is a communication protocol that enables a client to obtain the network configuration from a DHCP server. A router is often used as a DHCP server.
DNS	The Domain Name System (DNS) is used to translate a domain that can be easily remembered by humans into an IP address so that the correct computer can be addressed. The translation is done by a name server.
DTMF	Originally, the transmission of signals in an audio connection was called dual-tone multi-frequency (DTMF -inband). When we talk about DTMF signals in a SIP connection we also mean the transmission of signals according to RFC2833 and SIP-Info.
enrollment	Setting up access for a person via PIN, RFID or face recognition.
EventHandler	The EventHandler is the central connection between inputs and outputs of a door terminal. This allows the individual configuration of the door terminal.
firmware	The firmware is the operating software of devices, in this case the door terminals. The door terminals cannot be used without the firmware.
gateway	A gateway establishes the connection between two systems. Typically, it refers to a router that allows information to be passed between a local network and a public network.
HTTP	The Hypertext Transfer Protocol (HTTP) is a stateless protocol for transferring data on the application layer over a computer network. The current version HTTP/2 is specified in RFC7540.
intercom	Interkom is a system that works without a handset and can establish a speech connection to another terminal device. Modern intercom systems, such as the door terminals from Adatis, have additional interfaces, for example for video transmission.
IP-Address	An IP address is an address based on the Internet Protocol (IP). It is assigned to devices to make them addressable and accessible within a computer network.

Motion JPEG	Motion JPEG is a video codec in which each frame is compressed separately as a JPEG image.
NTP	The Network Time Protocol (NTP) is a standard for synchronizing clocks in computer systems via packet-based communication networks. NTP uses the connectionless transport protocol UDP.
PIN	A Personal Identification Number (PIN) is a number known to only one or a few people to authenticate themselves to a machine.
PoE or PoE Plus	Power over Ethernet (PoE) is a technique used to supply power to network-compatible devices via the eight-wire Ethernet cable. Compared to PoE, PoE Plus has a higher output of 25.4 watts instead of 15.4 watts.
port	A port is the part of a network address. By using different ports, several connections can be established from one computer to another. Valid port numbers are 0 to 65535.
relay	A relay is an electric operated switch that can be triggered remotely and commonly has two switching positions.
RFID	Radio-frequency identification (RFID) is a technology for transmitter-receiver systems that automatically and contactlessly identify and locate objects using radio waves.
SIP	The Session Initiation Protocol (SIP) is used to establish the connection between the door terminals and the remote stations. It is specified in RFC3261.
subnet	A subnet is a part of a network using the Internet Protocol (IP). The subnet area is separated by bitwise masking of a certain part of the IP address by the subnet mask.
TCP	The Transmission Control Protocol (TCP) is a network protocol that defines how data is to be exchanged between network components. It is a connection-oriented, packet-switched transport protocol in computer networks.
Trigger-Input	A trigger is a circuit that generates a pulse (trigger pulse) or a switching operation (switching edge) in the event of a triggering event.
UDP	The User Datagram Protocol (UDP) is a connectionless network protocol for use in IP-based computer networks.

Table of Figures