



# VI-EN-DS-1 and VI-FR-DS-1 Manual



[www.visualint.net](http://www.visualint.net)

Visualint

12355 US Highway 301 North, Parrish, Florida 34219

Tel: 941-225-4925 Email: [sales@Visualint.net](mailto:sales@Visualint.net)

# VI-EN-DS-1 and VI-FR-DS-1

**Attractive all-in-one-system for access control and door communication.**

Stand-alone solution without a PC or separate controller.



# Table of Contents

- About this product ..... 5
- Wall Mounting ..... 7
- Start of operation..... 8
- Installing visitor communication ..... 14
- Using visitor communication ..... 14
- Installing access control ..... 17
- Using access control ..... 19
- Video surveillance ..... 23
- Extended configuration via browser ..... 24
- Glossary ..... 27
- Declaration of Conformity ..... 29

**About this manual**

This product is manufactured with modern manufacturing techniques and extensive quality assurance measures.

If you have questions about your device, please contact your sales representative.

Visualint is constantly working on the development of devices and versions. We reserve the right to make changes in the scope of delivery, technology and equipment.

No claims shall be made from any text and illustrations of this manual.

## About this product

The devices of the VI-FR-DS-1 and VI-EN-DS-1 family are new access control terminals, which elegantly combine access control and visitor communication. You gain a representative business card at the front door of your company.

The VI-FR-DS-1 access control solution operates on the basis of a face recognition method, which measures the face three-dimensionally and grants the highest possible security against unauthorized access at the highest possible comfort (hands-free operation).

In addition, all devices offer the access option of a RFID card and/or a PIN code.

At the same time, they also allow audiovisual communication: Visitors can connect to the reception desk or a contact person. The operation is performed intuitively with a touch screen.

The data connection is via Ethernet and is compatible with modern voice-over-IP SIP standard. Integrated interfaces support connections of external components.

### Features

**Integrated Face Detection (Available only with the VI-FR-DS-1):** The calculation of 3D coordinates and the evaluation of the facial features are held in the unit that means it will not require a separate controller or PC.

**RFID and PIN-code:** Additionally or alternatively, the access is possible via encrypted RFID cards or tags or via PIN code.

**Audiovisual communication:** The visitor communication works through hands-free talking. Meanwhile the built-in camera records with 100 degree wide-angle lens the situation at the door.

**Intuitive touch screen operation:** The familiar control of smart phones with a touch screen allows intuitive operation and flexibility for customization.

**Interfaces:** The devices are connected to the network via Ethernet (or a series optionally with 2wire option via a pair of wire) and powered with Power-over-Ethernet (PoE). Integrated relays and triggers provide connections to doors and/or to common doorbell or feedback contact.

**Attractive and functional design:** The large 5.7" LCD screen allows easy user guidance and representative display of the company logo. The high-quality stainless steel housing and hardened glass provide protection against damage.

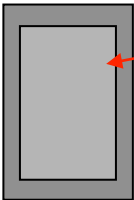


### Equipment overview

- a. Speakerphone for communication and for acoustic feedback
- b. Color camera for communication and camera for biometric
- c. LCD-touch screen for user interface and operation
- d. RFID-card reader for access via card: Place the card in front of this area
- e. Microphone for Voice-over-IP communication



- f. Terminal block/pluggable terminals for external power supply and interfaces.
- g. Ethernet-Network connection to the power supply (Power over Ethernet) and network connectivity



- h. Wall mount (holder can be used as a drilling template) or back housing

### Content of delivery for VI-EN-DS-1/VI-FR-DS-1

**Mounting kit:** Dowels and screws for wall mounting; socket wrench for housing locking or opening, seals.

**Terminal block:** Types PTR AK1350 series.

**Network cable:** Patch cable for Ethernet connection.

**RFID cards:** Green and red card with special functions for log in to configuration and enrollment sites; grey card for visitor ID card.

**Manual:** Installation manual.

## Wall Mounting

Cut out for flushing mounting: 124 x 244 47mm (4.8 x 9.6 x 1.85 in)

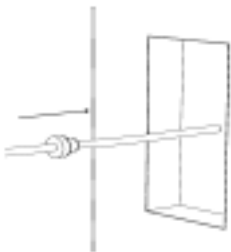
Further details on datasheet at [www.visualint.net](http://www.visualint.net).



1. Separate housing front from housing back. Loosen sealing screws.



2. Move housing front upwards and unhinge it.

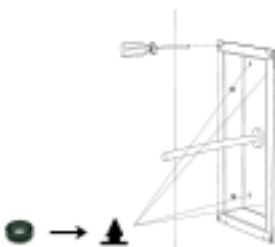


3. Put cables through rubber seal.



4. Put rubber seal with cables through the desired housing opening and snap it in.

5. Mounting housing back:



a. Flush mounting in cavity wall

If you use the outwards screw holes, close the inwards screw holes with attached rubber seals.



b. Flush mounting in solid wall.



c. Surface mounting.



6. Plug in desired connections.



7. Place housing front on fulcrum pins and move it downwards.

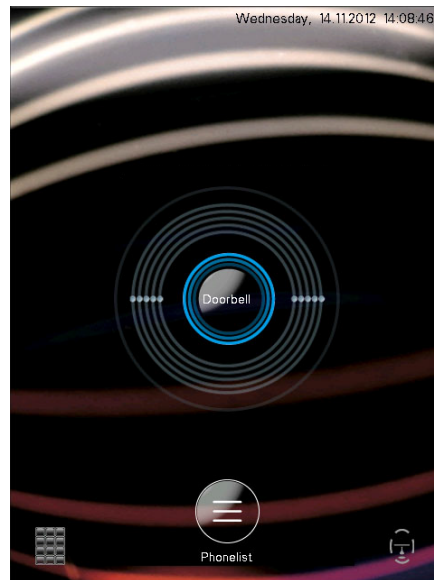


8. Tighten sealing screws to fix the housing front with the housing back.

## Start of operation

For all mounting instructions, please see the installation manual. The device can be configured before or after mounting.

The device has no separate power switch so it cannot be accidentally switched off. After the power supply has been established (see installation manual), the device starts and the home screen is on the display:



In the upper right corner, you can find the date and time display. In the middle, there is the call button and at the bottom, a button for PIN code for the phone book function and the face enrollment guidelines (**Available only with the VI-FR-DS-1**).

For further use of the device, configuration is required.

The devices have two different configuration areas:

### **Configuration via LCD-screen:**

Via the LCD screen settings can be made that require direct access to the device, such as the teaching of ID cards (enrollment). Other points can be set directly on the LCD screen but can also be configured via the web interface, such as the adjustment of the screen brightness.

### **Configuration via web browser:**

Via the web browser all settings except the enrollment can be done.



Some settings such as the display brightness can be set either via the LCD menu or the browser. However, the setting of this example is more feasible locally because the settings are directly controllable.

### Special RFID cards

Both cards have already been enrolled in the factory to be used directly (see RFID-Enrollment).



With the green card, the unit is set into enrollment mode.



With the red card, the unit is set into configuration mode.

If there is no active input via the touch screen during these modes, you will leave the opened mode automatically after a period of 30 seconds and the home screen appears again. This is for safety so that the opened mode doesn't remain activated unintentionally for a longer time. If you want to make further settings, you must use the green or red card again.

### Configuration via LCD menu

With the red card, you can configure the following sections: Camera, Audio, Display, IP Address and Sabotage protection.

By tapping the appropriate entries, the desired menu appears.

### IP address

So that the device is addressed in the network and later the browser configuration can be carried out, the IP address of the device can be adjusted.

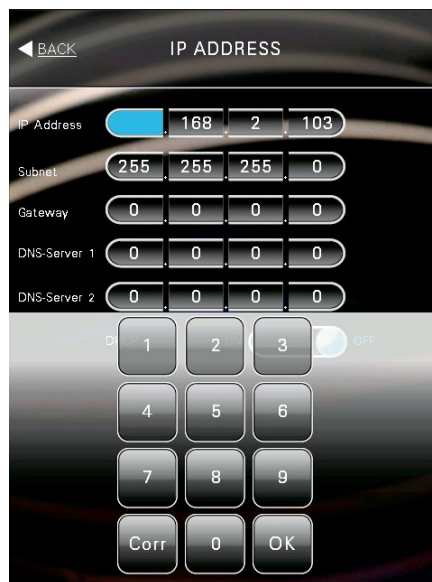
The IP address is usually provided by the system administrator of the company.

**Automatic assignment:** Basically, the IP address will be assigned automatically via DHCP or manually. Therefore, there is a slide switch in the middle.

The advantage of the automatic assignment of the IP address in DHCP mode is offset by the disadvantage of changing the IP address. When set to "DHCP ON", the assigned address will appear in this menu. In this case, the address fields for the direct input are disabled.



**Manual assignment:** In the "DHCP OFF" mode, you can manually input the IP address. Therefore, type on one of the sets of numbers of the IP address, subnet mask or gateway address. Then a 10-key pad is displayed with the numbers to be entered.



The 10-key pad also includes a button to correct the input and an "OK" button to accept the entry. If the "OK" button is pressed, the 10-key pad disappears. To enter a full address, you can jump from group to group of numbers so the 10-key pad does not need to be hidden in between.

With the "back" button, you can exit the menu and return to the selection menu.

## Camera

The unit is equipped with a wide-angle lens covering the space with a horizontal angle of about 100 degrees. Depending on the application, it may be advantageous that only a specific area in front of the entrance displays; for example, to receive a larger picture from the person located in front of the device.

The screen in this menu always shows a scaled-live picture of the portrait camera in the correct aspect ratio of 4:3, as it would appear in use on a videophone or on a PC monitor. This is for monitoring the selected zoom & pan settings.

**Pan area:** By tapping the picture with your finger, you can move it as you want providing you have zoomed in before. That means that the horizontal button is not at the left end.

**Zoom slider:** To adjust the magnification (electronic zoom) takes the horizontal slider.

On the left end, the maximum wide-angle representation is selected. Moving the slider to the right, you can zoom in to the picture. Here, the image section decreases. Now the image can be shifted within the window depending on the desired image.

If the slide is in the rightmost position, the maximum magnification is reached.

When delivered, the unit is set to maximum wide angle without any zoom and pan.

Usually the image section should be chosen so that a person in front of the station is shown clearly visible.

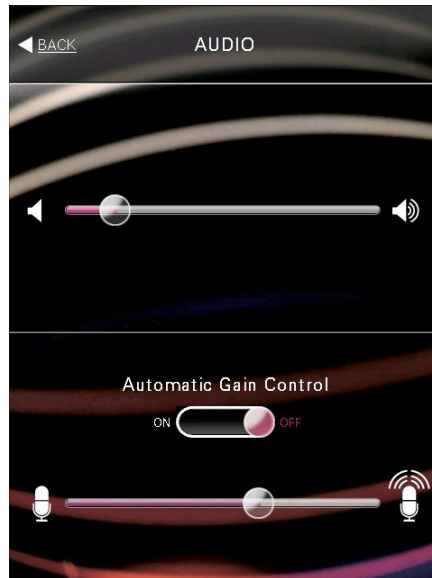
**Save image positions:** Three different zoom/pan settings can be stored in the device as fixed positions. These positions can be called up quickly during an active connection from the receiving side. You can typically save an overview display and two detailed views of the situation in the entrance area, which can then be accessed for inspection. The stored position under key 1 is displayed as the default view for a video connection.

To save a selected zoom & pan setting, press one of three buttons below the slider position until a beep sounds. The beep indicates that the setting has been saved. To check, you can access the settings by briefly pressing (without beep) the key position again.


With the "back" button, you can exit the menu and go to the selection menu.

## Audio

**Volume:** Because of the great influence of the mounting location on the acoustic properties, the audio settings should be made on the LCD menu. The values, however, are also accessible through the browser configuration.



In the top half of the menu is the slider for the volume setting. The volume can be set between the limits of the "min" and "max" based to the local conditions and the preferences of the user. If you move the slider, a voice recording is played to assess the volume.

 **Microphone:** In the lower half, there are the settings for the microphone sensitivity. The sensitivity offers two options, a digital control and an analog gain.

If the local acoustic conditions vary greatly, it is recommended to turn on automatic adaptation. Change the slide switch labeled "automatic gain control". The digital gain ensures that it is adjusted to a certain extent and to avoid clipping.

The sensitivity of the microphone can be selected independently of whether an automatic adjustment has been selected or not with the slider. The analog pre-amplification of the microphone is now adjusted.

When delivered, a mean value is the default, which should be suitable for most applications. Especially in very quiet or noisy environments, the speech intelligibility can be improved by varying the sensitivity. Because of the individually very different acoustic conditions, no general requirement for the best setting can be made.

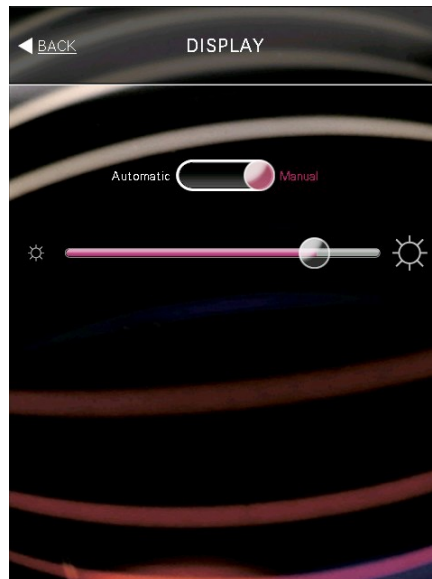
With the "back" button, you can exit the menu and go to the selection menu.

## Display

The adjustment of the display brightness is best done locally because you can only there take into account the direct influence of the ambient brightness. The adjustment of the brightness, however, is also possible through the browser configuration.

**Automatic mode:** When delivered, the slide switch is set to "automatic". In this setting, the display brightness is automatically adjusted to the ambient brightness. The determined brightness is shown in the display by the sliding switch.

This setting has the advantage that the display is automatically dimmed overnight and thereby power consumption is reduced while the display's life is extended.



**Manual mode:** If the automatic brightness control is not desired, the slide switch is set to "manual". In this setting, the control knob of the slider appears which allows the free choice of brightness

With the "back" button, you can exit the menu and return to the selection menu.

### **Sabotage protection**

**Tamper:** The device is equipped with a tamper switch. After installing the device, the two security screws on the bottom edge must be screwed with the provided socket wrench, as described in the installation manual.

In the final position, the tamper switch is closed. This can be checked on the present menu: If the area shown below the lettering "tamper" is green, the tamper switch is closed, providing security against theft of the device.

If the area is red, the tamper switch is open. Removal of the device cannot be detected. In this case, the security screws have to be screwed until a faint clicking sound indicates the switching of the tamper switch and the area is shown in green.

**Accelerometer:** The built-in acceleration sensor in the device measures changes in the orientation of the device in all three spatial axes. The movement of the device to the axes x, y, z are represented as level indicators. When a display changes in the red zone, an alarm can be generated - as at the tamper switch.

The acceleration sensor is primarily used to detect a theft without unscrewing the device or vandalism. With the alarm message, an alert to a control center and/or a video recording of evidence can follow.

## Installing visitor communication

### LCD display settings

The start screen and all labels of the LCD menu can be adjusted via the browser pages of the device (please insert IP address first).

The browser pages offer extensive tooltips to all fields.

### Installing destinations

To label the ring button and to fill the phone book with entries you have to install destinations. This is made via the browser menu "Access control" (see Installing access control).

As an alternative or in addition to a fixed remote station for the doorbell, you can use the Cortez Connect software product, DoorKeeper for Windows, Mac or mobile devices (iOS/Android) that can be set up as audio-visual remote sites. After installing the "DoorKeeper" software, it is sufficient to put a "check" at the respective doors to be informed of door calls. For details, see the "DoorKeeper" documents.

### Installing phonebook

To see entries of the access control list in the phonebook, you have to set the check in "Phonebook" at all desired entries. This is only possible with a SIP-URI, which means the SIP phone number of each entry.

## Using visitor communication

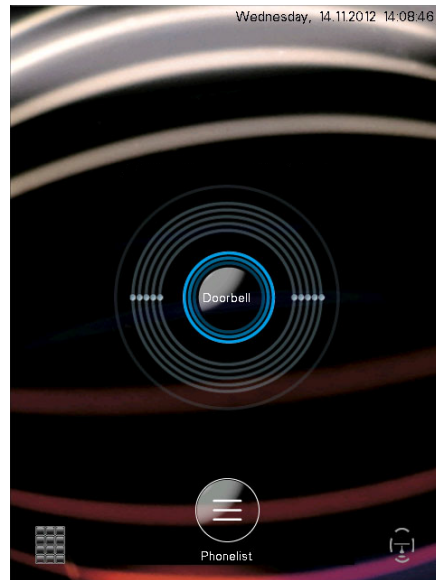
The intercom feature is used to communicate with visitors who want to talk to a special person of the company.

Through the implementation of the voice-over-IP protocol SIP, the device is compatible with modern (video) telephony infrastructures. There is no need for an additional terminal on the extension side as the call can be routed to each voice-over-IP terminal, which can be reached via the network and SIP.

The intercom feature is controlled by the operation of the ring button or by selecting a contact person from the phone list.

### Ring button

The home screen of the device shows in the middle of the screen one symbolized ring button, which can be individually labeled. In the following description, it is assumed that the ring button is labeled "Doorbell".



By tapping the screen in the call button area, the connection is started. An active call is illustrated by a ringing tone and an animation of the ring button. At the same time, the text "Calling: Doorbell" appears under the ring button.

Tapping again interrupts the animated doorbell and an existing connection. The bell returns to the idle state, the output of the ring tone stops and the message "Call cancelled: Doorbell" is displayed for a set time.

If the call is accepted by the other side, the text "Connected: Doorbell" appears and the green earphone is displayed. Now there is a two-way audio connection and a conversation can be made.

If there is a videophone or a soft phone with video functionality, such as the Cortez Connect "DoorKeeper" at the remote site, the video image of the color camera is transmitted. During an active call, various control functions are possible to open the door and to zoom the camera or change the view. This is described further below.

The existing connection can be closed, both from the device by tapping the call button (blue lettering "Hang-up") and on the remote side. In both cases, for a certain time the text "Connection cancelled: Doorbell" appears. Then the button appears in idle state again.

If an active call is not answered within an adjustable time (SIP call timeout) from the opposite side, there is no connection. The message "No response from: Doorbell" appears before the device returns to the idle state.

### **Dialing from the phonebook**



In addition to the ring button, the device offers an integrated phonebook, in which the contact persons of the company are listed. (See installing access control).

The phonebook button may be labeled with any text. The figures show the label with the text "Phonelist".

The phone book is accessed by tapping the phone book button at the bottom of the ring button. With the "back" button on the top left, the phone list can be left and switched to the home screen again.

The entries in the list appear in alphabetical order. However, only those entries are shown, in which was set the check in phonebook in the configuration.

If the list contains more items than can be shown, an ABC index bar is displayed on the right side. By tapping you can activate individual letters areas.

The scroll function is caused by the vertical sweep of the list with your finger.

When you tap an item, the contact person is called.

The selected entry is thus "opened" and a text will appear that describes the currently performed action. In addition, a button to end the call or the conversation is displayed. The following figures illustrate the process. In the example, the entry "Empfang" is tapped.

First, the call is started, which is indicated by the text "Calling: ":

Once the connection, the text changes to "Connected with: ":

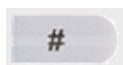
After the conversation either determined by the receiving station or by tapping the "Cancel call" button, the text "Disconnected from: " is shown for a set time:

The screen automatically returns to the home screen with doorbell button.

If there is no connection possible for a given time, the text "No response from: " appears. Then, the original phone book list appears again.

### **Control during the connection**

If there is an active connection from the device to a phone, videophone or soft phone, commands can be entered during the call via the telephone keypad. Depending on the terminal, it may be necessary to unblock the transmission of keyboard commands during a connection first. This should be described in the user manual of the phone under "SIP Info" or "DTMF Signaling". Except for the opener functions, the commands require a videophone or video-enabled soft phone to use the video controls.



**Door opener:** The pound key activates the built-in relay of the device. Usually the door opener is connected there. On the screen, a message appears "Access granted".

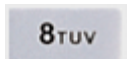
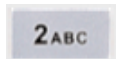




**Zoom in:** Higher magnification of the image, but with a smaller cut, details can be picked up in the picture.



**Zoom out:** Lower magnification with larger field of view, it gives you a better overview.



**Pan function:** The magnified image can move up, down, left and right.



**Center:** The image will be centered.



**Position buttons:** The view positions 1-3 stored in the device are available via these keys.

The key \* is used for video surveillance.

## Installing access control

### Input of employee data

**IMPORTANT:** To assign access rights to the employees, they have to be listed at the access control list of the browser configuration.

This list could also be modified external and be uploaded to this or another device.


The browser pages offer extensive tooltips to all fields.

### Enrollment

Before the access control can be used, the user has to be introduced to the system. This process is known as "enrollment".

Therefore, open the LCD configuration menu "Enrollment" with the **green** card.

In the top of the display, a slide switch is located, where the desired type of enrollment can be adjusted.

By default the slide switch is in the position "RFID". 

## RFID Enrollment

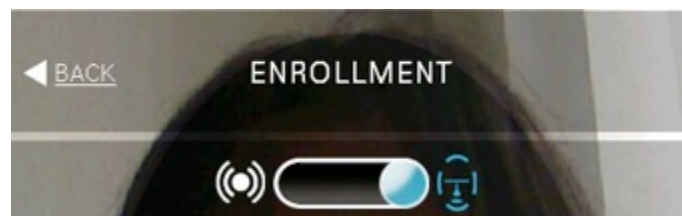
To introduce a new identification card, it has to be held in front of the read range of the device. The card is stored and a list of available contacts appears. With the arrow keys, you can assign the card to a contact.

If a system already knows a card, which shall be introduced again, the information is given that this card has already been enrolled.

## Face Enrollment (available only with the VI-FR-DS-1.)



For making the face enrollment, the slide switch has to be slipped to face recognition.



## General

On the screen, the color live image from the camera is displayed. The image is overlaid with green guidelines. In addition, a message appears when you stand too close or too far away. At the bottom of the screen a progress bar shows the status of the enrollment. The enrollment consists of three steps:

Geometry capture: Here the three-dimensional measurement of the face and the calculation of the biometric features are made.

Features check: The biometric features gained in step 1 are reviewed in terms of the quality and completeness.

Data storage: The biometric features are stored in the database of the device.

## Positioning

The green lines and the messages provide assistance to the position of the face in front of the device.

This learning process is also used to get to know the approximate distance from the subsequent use of face recognition:

The green brackets indicate that the device has found the face and now follows the position of the face in the image.

The facial expressions in front of the camera should be neutral at best. Although precautions have been taken by the software that the facial expressions have no effect for the calculation of facial features, a

neutral facial expression improves the recognition performance of the device. The facial expression should be preferably matched to the expression with which you want to be recognized in the daily use.

If the distance from the device is too large, not enough features can be recovered for recognition. In these cases, the text message will appear "Step closer".

If the face is too close to the unit, the message "Step back" is issued.

With a proper position in front of the unit, no message is sent and the progress bar moves from red through yellow to the green zone.

### **Sequence of enrollment**

Important for the rapid flow of enrollment is that the positioning of the face during the enrollment will retain. Little movements up- or downward, to the left or the right are appreciated to ensure the software to store as much face details as possible. Please do not talk during the enrollment as these influences your face expression. The progress will last about 20-30 seconds in total.

The progress bar shows progress and quality of the enrollment. If an enrollment is determined without reaching the green sector, the enrollment has to be redone.

A list with the available contacts is shown. With the arrow keys, you can assign the face image to the corresponding contact.

If the device is operated in server mode in conjunction with the Cortez Connect management software "FaceAdmin", the enrollment has to be unlocked for these contacts in the software. For more information, please see to the documentation for the "FaceAdmin".

Upon successful storage of the data, the color of the field changes from yellow to green.

With browser configuration the default user name can be changed and personal information can be completed. The check „access via face“ is automatically set at the respective entry at the access control list.

After completing an enrollment a new one can be done directly.

## **Using access control**

The unit offers for the field of access control three technologies that can be used for entrance allowance:

**Face recognition (Available only with the VI-FR-DS-1)** is a biometric method in which the three-dimensional shape of the face is detected. Biometric methods do not require any identification card and are, therefore, extremely safe because a loss or theft is eliminated. Face detection also offers the advantages of convenient (operation without a free hand) and touchless (hygienic) operation.

**RFID** is a modern smart card technology, which also works without contact. By encryption techniques high security is achieved. In the future, mobile phones will work according to the present standard NFC and can then be used as identification.

**PIN code** is a fairly simple process in which the knowledge of a number sequence is used as permission. As the sequence of numbers may also be guessed or tried, the security level here is relatively low.

#### **Access via face recognition (Available only with the VI-FR-DS-1)**

After the implementation of enrollment and the assignment of the employee data at the access control list, the face recognition can be directly used.

Starting from the basic mode of the device (= start screen), the face recognition works automatically; therefore, the device looks for the presence of face in the viewing area of the camera.

If a face is found in sufficient size, the unit attempts to identify the face. If a face is found in the range of the camera, the color of the face icon in the lower right corner of the screen turns from white to blue.

By clicking the face icon, a positioning help can be shown: As with the enrollment, the live image of the camera is shown with superimposed guidelines. The green brackets provide guidance for optimal positioning in front of the camera of the device.

For successful face recognition, a confirmation screen is displayed for an adjustable time containing the image of the person entitled, user data and the message "Access granted!" After that, the start screen appears again.

#### **Tips for rapid identification**

The right distance from the device is about an arm's length: Therefore put the thumb of an outstretched arm on the edge of the device.

You should look vertically at the camera above the display. For this purpose, it is usually necessary to lower his head slightly, as the device is mounted slightly lower for size compensation.

Rapid changes in the facial expressions or the whole position or an enrollment deviating expression impede the rapid recognition.

Also talking can prevent the detection, since the tension of the face muscles change the 3-D shape, so that no sufficient match results with the stored characteristics are found.

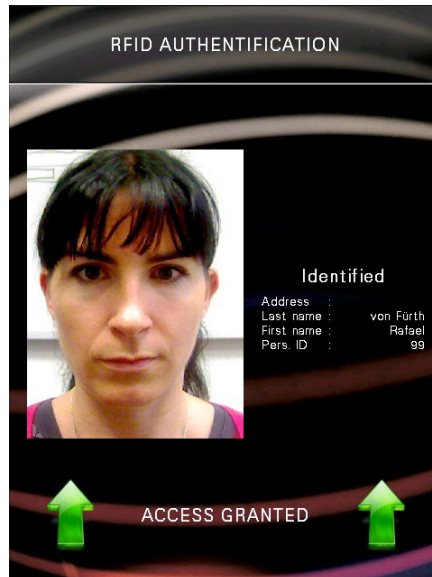
The enrollment and the recognition must be made without glasses: firstly reflections of the built-in lighting (invisible infrared light) could interfere with the detection, on the other hand, the 3D shape of the glasses and the glasses frame is also stored as a feature. So especially for large, fashionable glasses the recognition accuracy could be compromised.

## Access via RFID

The device behaves in relation to the access via RFID card as a conventional card reader. The access card is held just in front of the field marked with the RFID symbol.

The card does not need to be placed on the device but will be detected at a distance of 1 to 3 cm from the device.

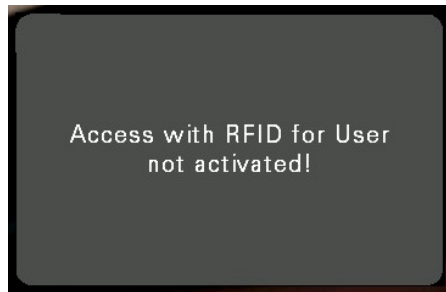
If an enrolled card is detected, the access is granted:



If an unknown card held in front of the reader, the screen message "card not in system" appears:



If the card is indeed known to the system but access is blocked (tick in the access control list is missing), this is indicated by the following message on the screen:



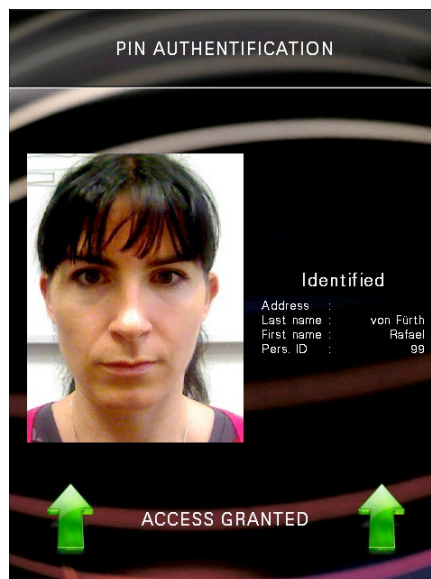
### Access via PIN code

While access via RFID requires the possession of the correct card, the access via a PIN code requires knowing the correct code.



By clicking on the PIN icon in the lower left corner of the screen, a 10-key keyboard is displayed. A mistake can be undone with the "Corr". The entry is completed by pressing the "OK" button.

If the code is entered correctly, the access is granted:



If an incorrect code is entered, there is a message for 2 seconds, that the code is not entitled to access:



In the case that the PIN code is entered in the access control list but the check is not set for PIN code, the same message on the screen is indicated.

### **Multilevel access**

By combining different credentials such as biometrics, card and PIN code, a 1 to 3-level access can be realized. If the multi-level access for a user is set at the browser, the credentials must be presented in any order. Screen messages prompt the user accordingly, to identify with the next credential to gain entry.

For example, when the 2-level access via card and PIN for a user is set up, the user is free to initially be recognized at PIN code or card. The unit will then prompt the user accordingly to present the second, missing credential before access is granted.

While only one of the three possible credential types is required in 1-level access, there are corresponding three possible combinations at 2-level access.

With a 3-level access all three credentials are required.

### **Video surveillance**

The video monitoring feature allows a visual inspection of the area outside the door over any distance. The function of the device is activated by a call from the outside via the SIP or IP address. The call takes place hidden so that an active connection to the device is not visible.

The video monitoring function is not restricted to a single observer, but up to 10 remote stations can simultaneously receive the video image from the door.

As described above, the video parameters can be changed during the call so you can pan the camera from a distance and tilt or zoom into images or zoom out for an overview (see Control during the connection). It should be noted that this possibility deserves all observers across multiple active peers. Therefore, concurrent requests can be sent by the observers on the camera of the terminal. If the camera of an observer is set to a fixed position, it is quite possible that another observer chooses a different position and zoom setting.

The audio transmission is initially turned off for privacy reasons; i.e., there is no acoustic monitoring of the entrance area. The bidirectional audio connection must explicitly be unlocked from the opposite side and then the terminal is also displayed. A person in front of the terminal can see that the microphone was turned on. With the audio connection, all other video connections that may have been installed, are stopped so that the connection will be exclusively assigned to the observer, who requested the audio connection.



**Speaker on/off:** By tapping the star button during an active video connection, the audio connection is bidirectional and the AV connection is exclusively assigned to the requesting

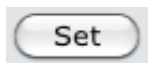
remote station. The terminal screen is switched to "CONNECTED".

By re-pressing the star button, the audio connection is terminated. Now the video surveillance function is available again for more than one observer and the display goes back to the main screen.

## Extended configuration via browser

The complete configuration of the device is done by using a web browser. For this purpose, the device has a built-in HTTP server. The configuration is divided into different menus, for each respective websites are available.

To use the convenient configuration via a web browser, you must have connected the device to the Local Area Network (LAN) and a valid IP address for the network must have been configured as described in the previous chapter. Furthermore the PC, on which the browser is running and which will be used for the configuration, has to be connected in the same network, so that the IP address of the device is achievable.



Basically, changes are applied only after pressing the respective assigned "Set" button. If pages are left without "setting", all changes made will be lost.

### Home screen

By opening the browser and entering the IP address of the client device for the first time, the website of the device appears.

The basic design of the screen for all menus consists of the following elements:

Bar at the top of the screen with a company logo

Tree-bar on the left with the hierarchical representation of all menus

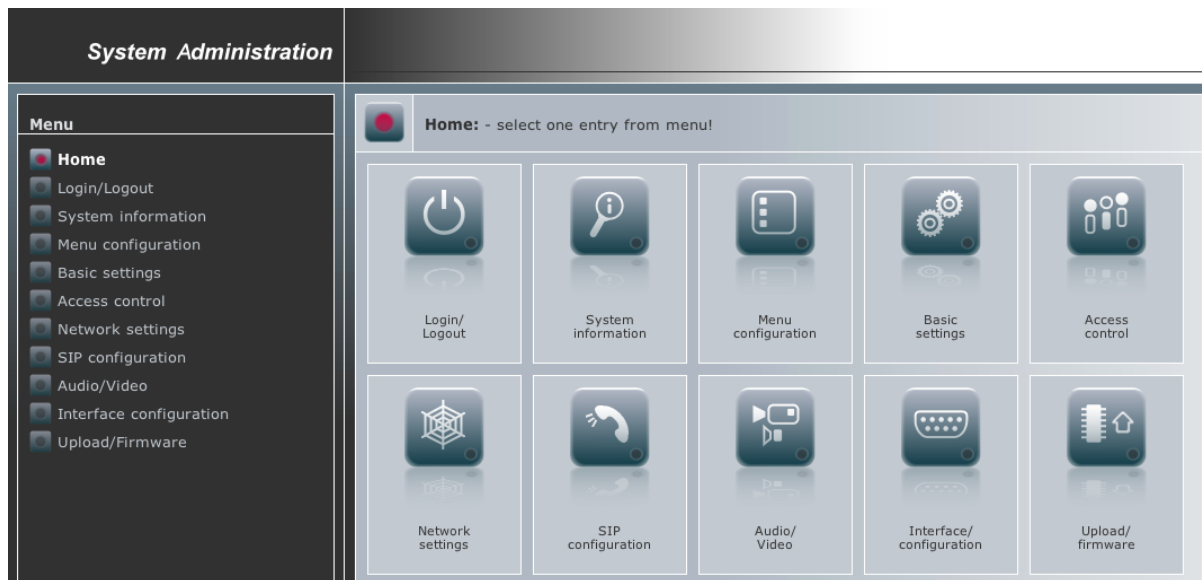
Main window for the configuration menus

The configuration menus can be selected either by using the icons in the window or on the tree.

The following description does not constitute a full documentation of the browser configuration, as the menus may change in the course of further development of the firmware.

To assist in the browser configuration, so-called "tool tips" appear: Positioning of the mouse for 2 seconds on a menu item, a small window with an explanation on this point appears. The documentation automatically adapts to the capabilities of the device firmware.





## Login/Logout

### Password protection

On delivery, the browser configuration is protected by a password, so no unauthorized changes can be done. The password can be changed in this menu.

The password should be kept with care; as with a lost password, you cannot access the browser configuration.

### Special RFID cards

The green and the red RFID card, which are delivered, can open the LCD configuration or enrollment menus. The assignment to these special functions was already done at the factory.

If you want to use other cards for these functions, you can change the assignment as follows:

**Option 1:** First, the two UID entries are deleted. Pressing the "set" button, the card detection system for opening the configuration and enrollment menus is started. Then, the green card to open the LCD configuration has to be put in front of the reader. A message will appear if the card has been detected. The red card to open the enrollment has to be put in front of the reader. Two new UIDs are entered and the unit will operate normally. To display the new UIDs in the browser, the browser page has to be reloaded.

**Option 2:** The UIDs for the two special cards can be entered in the appropriate fields. Manual entry of the UIDs always carries the danger of incorrect entry. Therefore, option 1 is always to be preferred.

### System information

The system status menu is divided into the areas of system data and system log.

The system data contain information about the device type, the hardware address and software version of the firmware. For service purposes, the built-in hardware components may be displayed.

Please contact your system administrator for questions regarding the syslog protocol.

### **Menu configuration**

The appearance and the caption of the LCD screen can be adjusted with input of your personal preferences on this page.

### **Basic settings**

All general device settings have been grouped under this menu.

**Language selection:** The device supports not only English but also German and French menus as well.

**Unit date and unit time:** The device has an internal real-time clock, buffered and even continues if the event of power failure or when transporting the device some time (more than 1 year).

### **Access control**

In the list view, a list with last names and first names is shown. Depending of the screen size and the browser window, only the first entries are displayed. By pressing the scroll bar on the right side, you can go to the desired section of the list. With the arrow keys, you can browse the pages.

Use button "Change" to display the contact details.

### **Network settings**

The input of the network settings is analogous to the input on the LCD configuration. There exist the same entries: IP address, subnet mask, gateway address, DNS server 1 and 2, Auto-IP DHCP on/off.

Additionally, the name is entered, with which the device appears on the network (spaces are not allowed).

The change in the network settings should be done with special care because by entering incorrect values, the unit may no longer be accessed from the browser. In this case, the correct address must be re-entered via the LCD menu.

### **SIP configuration**

The intercom functionality operates on the Voice over IP standard SIP. Instead of the cumbersome IP addresses, short numbers or text name can be used for dialing. Second, the SIP server offers several convenience features, such as an answering machine for audio and video, centralized management of data and authentication of users.

## **Audio/Video**

All settings for audio and video transmissions can be edited here.

In addition, a live video stream and stored fixed positions in the device can be displayed if required.

## **Interface configuration**

The device has several inputs and relay outputs that can be extensively configured.

The available resources for the connection link target must have been previously configured with details of the SIP URI in "Access Control".

## **Upload firmware**

With "Upload", a new firmware can be programmed into the device. The already installed firmware version can be read in the browser menu "System information".

While performing a firmware upload, ensure that the unit is not disconnected from the power supply. Only after the new firmware has been programmed and the automatic restart of the unit is completed, the supply voltage can be separated.

Configuration and access control list files can also be uploaded or downloaded. This makes it possible, once set or stored data via "Download" and "Upload" transmit to other devices.

The download of the configuration data is recommended not only for safety reasons (backup), but also, if you want to configure multiple devices of the same kind and do not use the Cortez Connect software "FaceAdmin".

## **Glossary**

### **A-law**

The A-law is a method of digitization process for analog audio signals in the telecommunications sector used primarily in Europe, which is standardized in the re-commendation G.711 by the ITU-T. By this, analog voice signals are converted through the digitization with a non-linear quantization, the so-called A-characteristic curve, into digital signals. The aim is to achieve a higher dynamic range with the same number of binary digits per sample or a larger signal-to-noise ratio, in which the large signal excursions have coarser and small signal excursions have finer resolutions.

### **μ-law**

In North America and Japan, the μ-law-related method is used, similar to the A-law, but not compatible.

### **Baud-rate**

Describes the number of symbols transmitted per time unit. The baud rate is different from the lower data rate by the ratio of the number of symbols per transmitted data bit. The baud rate must be set equal on both sides when communicating via a serial interface.

**DHCP**

Dynamic Host Configuration Protocol - allows the assignment of the network configuration to devices by a DHCP server. In this setting, the user must not set the IP address and other addresses by hand.

**DNS**

Domain Name System - Service on the network, mainly for responding to requests for name resolution. This device can be addressed with a plain text name that is easier to remember and characterizes the device. Here, the name remains the same even with changing IP addresses.

**Intercom**

A station with microphone and speaker that provides an audio and often an audio-visual communication to a remote site.

**LCD**

Liquid Crystal Display - often colloquially referred to as flat.

**NIR**

Near Infrared - invisible to the human eye in the near infrared light range.

**OSDP**

Open Supervised Device Protocol - is an approach to standardize the connection of peripheral devices in the field of access control and alarm systems and to enable collaboration between devices from different manufacturers.

**PIN**

Personal Identification Number - is a number known by only one or a few persons, with which they can be authenticated against a machine.

**RFID**

Radio Frequency Identification - a modern smart card system for access control.

**SIP**

Session Initiation Protocol - is a network protocol for setting up, controlling and terminating a communication session between two or more participants. In the IP telephony SIP is a frequently used protocol.

**UID**

Unique Identifier - a unique and distinctive number, which allows the authorization of a card to the reader. This number consists of a fixed number of characters and is awarded only once.

**URI**

Uniform Resource Identifier - consists of a string, which is used for identification.

A SIP URI is used for addressing participants of SIP-based calls. It is thus the SIP phone number of a participant.

## Declaration of Conformity

Visualint

12355 US Highway 301 North

Parrish, FL 34219

Declares, that the devices

VI-EN-DS-1

VI-FR-DS-1

comply with the requirements of the directives on electromagnetic compatibility 2004/108/RG and has been developed and manufactured in accordance with the following standards:

**transient emissions:**

EN55022, EN61000-3-2, EN61000-3-3

**interference resistance:**

EN55024 (EN61000-4-2 bis -6; -8; -11)

**Note:** This declaration becomes invalid if the product without the explicit permission of Cortez Connect is modified, supplemented or changed in any other way, as well as in improper connection or improper use.