



Part 1: System Overview and Installation
Installation and Cabling
(for the Installer)

Part 2: Start-Up and Configuration
Software and Network
(for the **System Administrator**)

5 MP
Sensor

MxLEO



vPTZ



MxBus

USB

+50°
-30°

IP65

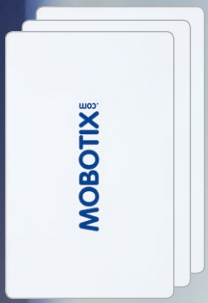


Innovations - Made in Germany

The German company MOBOTIX AG is known as the leading pioneer in network camera technology and its decentralized concept has made high-resolution video systems cost-efficient.

MOBOTIXAG • D-67722 Langmeil • Phone: +49-6302-9816-103 • Fax: +49-6302-9816-190 • sales@mobotix.com

Hemispheric IP Video Door Station with camera, KeypadRFID and Info Module • Made in Germany • www.mobotix.com



SYSTEM MANUAL PART 2 – START-UP AND CONFIGURATION

This *T25 System Manual Part 2, «Start-Up and Configuration»* is supplemented by the *T25 System Manual Part 1, «System Overview and Installation»*. If you no longer have a manual at your disposal, you can download a PDF file from the MOBOTIX website (www.mobotix.com > **Support** > **Manuals**).

CONTENTS

1	Overview of Application Scenarios	10
1.1	Standard Scenario	10
1.1.1	Description	10
1.1.2	Example	12
1.2	Advanced Scenario	14
1.2.1	Advanced Access Control	14
1.2.2	Multiple Doorbells and Voice Mailboxes (Addressees)	16
1.2.3	Multiple Door Stations	18
1.3	Expanding the System with a Computer and MxEasy	20
1.3.1	Computer as T25 Remote Station	20
1.3.2	Worldwide Two-Way Communication	21
1.3.3	Network without DHCP Server (Static IP Addresses)	22
2	Initial Setup without a Computer	24
2.1	Step 1: Perform the Auto Configuration	26
2.1.1	Starting the Video Phone	26
2.1.2	Starting the Door Station	27
2.1.3	Starting the Auto Configuration	28
2.1.4	Functional Test Part 1	29
2.2	Step 2: Set Up the KeypadRFID Access Module	32
2.2.1	Entering the Super PIN at a KeypadRFID Module	33
2.2.2	Adding Admin Cards at the KeypadRFID Module	34
2.2.3	Adding User Cards at the KeypadRFID Module	36
2.2.4	Setting the Time Zone, Time and Date	38
2.3	Step 2: Set Up the BellRFID Access Module	41
2.3.1	Entering the Super PIN at a BellRFID Module	42
2.3.2	Setting the Bell Button Set to Be Installed	43
2.3.3	Inserting the Function/Bell Buttons	45
2.3.4	Training the Admin Card	45
2.3.5	Adding User Cards at the BellRFID Module	46

2.4	Step 3: Configure the System Using a Video Phone	47
2.4.1	Changing the Menu and Voice Mailbox Greeting Language	49
2.4.2	Opening the Admin Setup	50
2.4.3	Changing the Super PIN at the Video Phone	51
2.4.4	Setting the Door Status Display	52
2.4.5	Activating Video Recording	53
2.4.6	Functional Test Part 2	55
2.5	Step 4: Protect the System Using a Video Phone	57
2.5.1	Changing the Grandstream Web Password	58
2.5.2	Disabling Auto Configuration	59
2.5.3	Saving the System Configuration	60
3	KeypadRFID Access Configuration	62
3.1	Quick Start: Access Configuration	62
3.2	Individual Configuration of Access Media	64
3.2.1	Personal, Transponder and Contact Numbers	64
3.2.2	T25 Product Pass for Recording System Information	65
3.3	Managing Transponders	66
3.3.1	Adding User Cards (Individual Number Assignment)	66
3.3.2	Erasing User Cards	68
3.3.3	Time-Restricted Access ("Tradesman Card")	70
3.3.4	Adding Admin Cards	72
3.3.5	Erasing Admin Cards	73
3.4	Managing Access PINs	75
3.4.1	Adding PINs	75
3.4.2	Deleting PINs	77
3.4.3	Changing PINs	78
3.5	Erasing All Access Privileges of a User (Cards/PINs)	80
3.6	Erasing Contacts (Doorbell/Voice Mailbox)	82
3.7	Changing the Super PIN at the KeypadRFID Module	84
4	BellRFID Access Configuration	86
4.1	Managing Transponders	86
4.1.1	Adding User Cards	86
4.1.2	Deleting Individual User Cards	87
4.1.3	Deleting All Cards of a User	87
4.1.4	Deleting All Cards (Admin and User)	89
4.2	Changing the Super PIN at the BellRFID Module	90

5	System Expansion with MxEasy	92
5.1	Setting Up Computers as T25 Remote Stations	94
5.1.1	System Requirements	94
5.1.2	Downloading and Installing MxEasy	95
5.1.3	Connecting a Door Station Using the MxEasy Wizard	96
5.1.4	Setting Date and Time	102
5.2	Integrating the Door Station into a Network with Static IP Addresses	104
5.3	Setting Up Global Connectivity Between MxEasy and Door Station	110
6	Restoring the System	116
6.1	Error Messages and Rebooting	116
6.2	Backing up and Restoring	117
6.2.1	Backing up the System	117
6.2.2	Restoring the System	117
6.2.3	Exchanging a KeypadRFID/BellRFID Module – with System Restore	118
6.2.4	Exchanging an MX-DoorMaster – with System Restore	118
6.2.5	Exchanging an Info Module	119
6.2.6	Exchanging Info Module Mx2wire+ Components	120
6.2.7	Exchanging the T25-CamCore Camera Module – with System Restore	121
6.2.8	Exchanging or Adding a Video Phone	121
7	Additional Notes	122
7.1	Weatherproofing and Care	122
7.2	Surge Protection	122
7.3	AVC Video/H.264	123
7.4	Warranty and Repair Service	123
7.5	Other Information	123
7.5.1	Safety Warnings	123
7.5.2	Declaration of Conformity	124
7.5.3	Disposal	124
7.5.4	Disclaimer	125
	Manufacturer	127



Safety Warnings

Risk of overheating when exposed to direct sunlight: When mounting a black, dark gray or amber-colored T25 IP Video Door Station in locations where the device is exposed to direct sunlight, the housing temperature can exceed the maximum allowed temperature limit. This can result in electronic failures and injuries especially when touching exterior metal parts. If the intended use of the device is at an (unprotected) outdoor location, you should only install white or silver-colored modules and frames. This product must not be installed within the reach of persons without the dome.

Electrical installation: Electrical systems and equipment may only be installed, modified and maintained by a qualified electrician or under the direction and supervision of a qualified electrician in accordance with the applicable electrical guidelines. Make sure to properly set up all electrical connections.

Electrical surges: MOBOTIX cameras are protected against the effects of small electrical surges by numerous measures. These measures, however, cannot prevent the camera from being damaged when stronger electrical surges occur. Special care should be taken when installing the camera outside of buildings to ensure proper **protection against lightning**, since this also protects the building and the whole network infrastructure.

Max. power consumption of attached extension modules: The power consumption of all attached **MxBus modules** must **not exceed 2.5 W**. When attaching modules to the MxBus connector **and** the USB connector, the **power consumption of all attached modules must not exceed 3 W, if the camera is powered by PoE class 3**. If **PoE class 2** is used, **the power consumption of all attached modules must not exceed 1 W!**

Legal aspects of video and sound recording: You must comply with all data protection regulations for video and sound monitoring when using MOBOTIX products. Depending on national laws and the installation location of the T25, the recording of video and sound data may be subject to special documentation or it may be prohibited. All users of MOBOTIX products are therefore required to familiarize themselves with all valid regulations and comply with these laws. MOBOTIX AG is not liable for any illegal use of its products.

Network security: MOBOTIX products include all of the necessary configuration options for operation in Ethernet networks in compliance with data protection laws. The operator is responsible for the data protection concept across the entire system. The basic settings required to prevent misuse can be configured in the software and are password-protected. This prevents unauthorized parties from accessing these settings.

Additional instructions:

- This product must not be used in locations exposed to the dangers of explosion.
- Make sure that you are installing this product on a solid surface.

MOBOTIX Seminars

MOBOTIX offers inexpensive seminars that include workshops and practical exercises. For more information, visit www.mobotix.com > **Seminars**.

Copyright Information

All rights reserved. MOBOTIX, the MX logo, *MxControlCenter*, *MxEasy* and *MxPEG* are trademarks of MOBOTIX AG registered in the European Union, the U.S.A., and other countries. *Microsoft*, *Windows* and *Windows Server* are registered trademarks of Microsoft Corporation. *Apple*, the Apple logo, *Macintosh*, *OS X*, *iOS*, *Bonjour*, the Bonjour logo, the Bonjour icon, *iPod* and *iTunes* are trademarks of Apple Inc. registered in the U.S.A. and other countries. *iPhone*, *iPad*, *iPad mini* and *iPod touch* are Apple Inc. trademarks. *Linux* is a trademark of Linus Torvalds. All other marks and names mentioned herein are trademarks or registered trademarks of the respective owners.

Copyright © 1999-2014 MOBOTIX AG, Langmeil, Germany. Information subject to change without notice!

Download the latest version of this and other manuals as PDF files from www.mobotix.com > **Support** > **Manuals**.



FOREWORD

Dear MOBOTIX customer,

The **T25 IP Video Door Station** is a complete outdoor system that includes a hemispheric door camera with built-in microphone, speakers, a voice mailbox function (T25-CamCore) and an access module with integrated RFID card reader for keyless access (KeypadRFID/BellRFID). The tamper-proof **MX-DoorMaster with backup power supply**, which also serves as a doorbell, is installed indoors. The **Grandstream GXV3140**, a sleek, high-quality VoIP video phone, makes the perfect remote video station.



The entire MOBOTIX system was designed to allow it to be started up and configured quickly and easily by a single user. In the first section of the manual, "Overview Of Application Scenarios," we will familiarize you with the many ways in which you can use this flexible system. You can then decide for yourself which system functions you would like to use and configure.

The different operation steps correspond to the order of the chapters of this manual and you can simply skip the sections pertaining to functions that you do not need. The IP-based system is extremely flexible, meaning that you can easily change the configuration – and the range of available functions – at any time.

You can operate and configure the entire system without the need for a computer or any other special devices. Only the optional extensions listed in *Chapter 5* require you to connect the T25 to a computer running MxEasy. The MxEasy video software is free of charge and can be downloaded directly from the MOBOTIX website (www.mobotix.com > **Support** > **Software Downloads**).

Our support and international sales staff are available at intl-support@mobotix.com from Monday to Friday, 8 a.m. to 6 p.m. (CET). We hope that you enjoy your new powerful MOBOTIX IP Video Door Station.



1 OVERVIEW OF APPLICATION SCENARIOS

1.1 Standard Scenario

1.1.1 Description

The standard application scenario for the MOBOTIX IP Video Door Station is the simple one-party scenario (for example, a single-family home or doctor's office). This scenario involves one building or apartment with a door that is secured using the T25 system. At the door, visitors can ring the doorbell for one party (meaning one or more occupants).

Hardware and Functions in the Standard Scenario:

- Outdoor station: One T25 IP Video Door Station with KeypadRFID or BellRFID and multiple transponder cards (blue user cards for day-to-day use, red admin card for system administration)
- Remote station in the house: Grandstream video phone &/or computer with MxEasy.
- Additional doorbell in the house: MX-DoorMaster (with connected door switch and door lock switch)

Visitors can press a bell button on either the camera, the KeypadRFID or the BellRFID to ring the doorbell of the building or a specific apartment. The video phone and the MX-DoorMaster then call the house phone or MxEasy.

The homeowner picks up the receiver in order to speak to the visitor. The live image of the door camera is displayed in the color display on the video phone. The homeowner can then press a button on the video phone to activate the electric door opener and, for example, switch on the light in the stairwell.

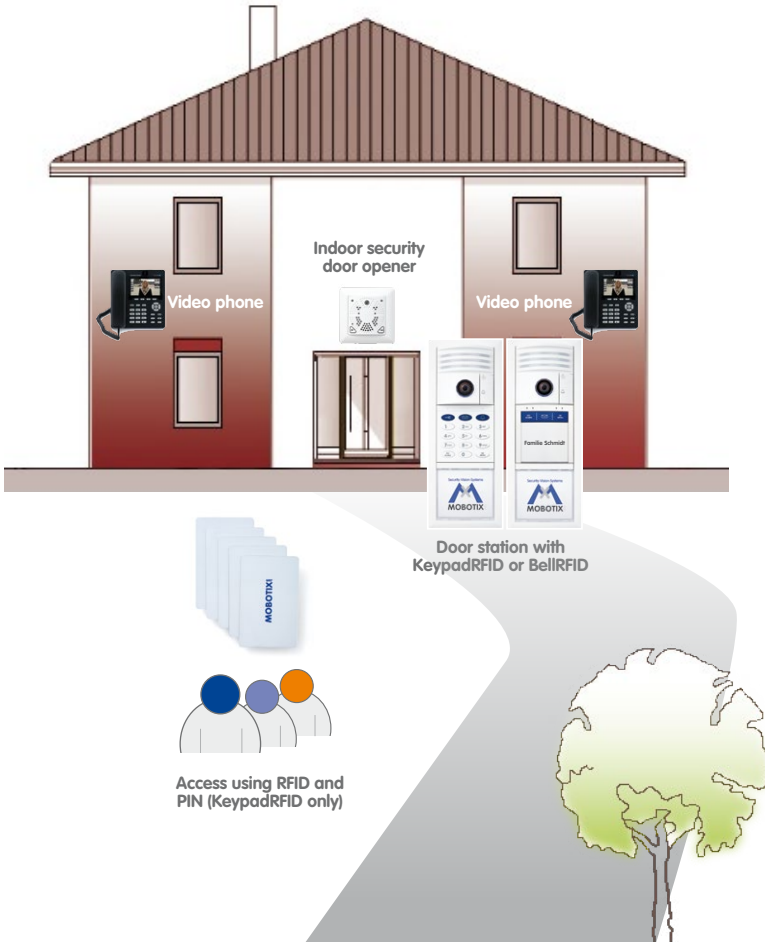
If the homeowner does not respond to the doorbell, and the **voice mailbox function** is activated, visitors can leave a message at the door – just as they would on a telephone answering machine. The homeowner can listen to these messages at the door station or at a video phone in the house.



Homeowners can use the **blue user cards** to **open the door from the outside without a key** and listen to voice mailbox messages right at the door station. In addition to using the transponder cards, homeowners can also enter an access PIN that can be used to open the door via the KeypadRFID. It is possible to use up to 1,000 cards and PIN codes for a single door station!



User card



1.1.2 Example

The Smith family consists of a husband and wife, John and Suzanne Smith, and their 15-year-old daughter, Anna. The three of them live in a single-family home. The door to their house is secured with a T25 IP Video Door Station with a KeypadRFID and a MX-DoorMaster.

One Grandstream video phone located on the first floor and another Grandstream video phone located on the second floor near the parents' bedroom serve as the **remote stations** for the system. Anna lives on the third floor and has her own Grandstream video phone.

In addition to using the **red admin card**, Mr. Smith has registered a **blue user card** to enable keyless access for himself, his wife and his daughter. Admin and user cards can be registered during initial setup. This can be done simply by holding the cards up to the KeypadRFID or the BellRFID. Once the system is operational, the user can also enter an **access PIN** (KeypadRFID only). This way, in an emergency in which the user has misplaced or forgotten his or her key or transponder, he or she can still enter the house without having to call a locksmith.

When a visitor rings the doorbell at the door station, all three video phones ring and display visual signals. In addition, the **MX-DoorMaster**, which is mounted in the entry area near the door, plays a bell sound that has been selected by the user. Thirty seconds after the visitor rings the doorbell for the first time, the system instructs the visitor to leave a message (**voice mailbox function**). In addition, the visitor can choose to leave a message without ringing the doorbell by pressing the letter button. Anna sometimes uses this function to quickly let her parents know when she is on her way to a friend's house. In summary, the following functions are available:

Open Door/Keyless Access

- With one of the user cards (or with the admin card as well)
- With the access PIN (KeypadRFID only)

Ringling the Doorbell for the Family

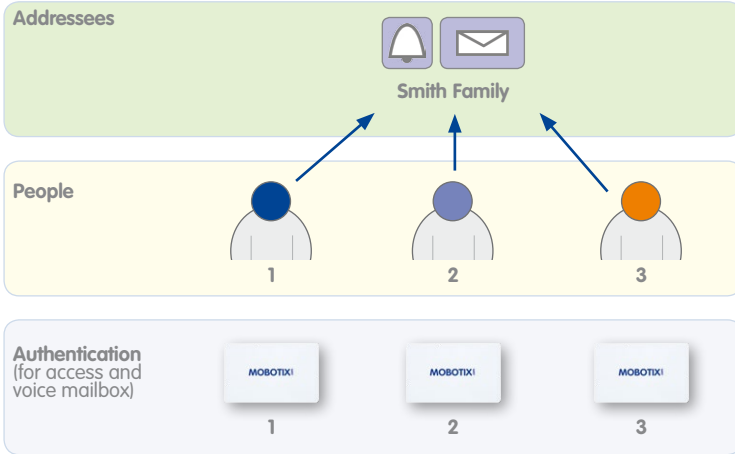
- By pressing the white bell button of the camera module
- By pressing the blue bell button of the KeypadRFID or BellRFID module
- By pressing the corresponding bell button of the BellRFID

Leaving a Voice Mailbox Message

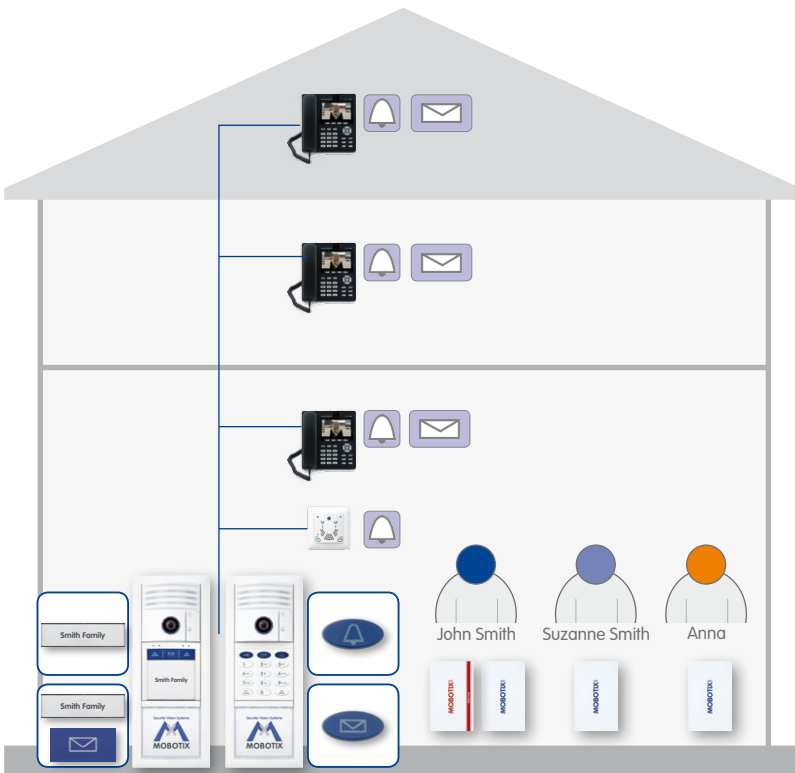
- By pressing and holding the blue letter button of the KeypadRFID/BellRFID module
- After ringing the doorbell or directly, without ringing the doorbell

Listening to Voice Mailbox Messages

- On the KeypadRFID/BellRFID module (only in connection with a user or admin card, if function has been activated)
- On the Grandstream video phone or a different remote station (can be accessed by everyone in the house)



In addition, an Access PIN was trained (not shown)



1.2 Advanced Scenario

1.2.1 Advanced Access Control

Multiple user cards or an additional access PIN can be assigned to each user with advanced access control. These assignments, which are made based on a personal number when the cards/PINs are registered in the system, make it possible to quickly and easily remove users from the system at a later time.

Setting Up Cards Using an Access Module (KeypadRFID/BellRFID)

The user cards are included with your MOBOTIX product. These cards allow you to enter the building without the need for a key and enable you to operate the voice mailbox using the KeypadRFID or BellRFID, respectively. However, the cards must first be registered in the system before they can be used. To set up a new user card, use the red admin card for authentication, enter a special key combination (KeypadRFID only) and then simply hold the card up to the access module.

Setting Up with Automatic Number Assignment

The system automatically assigns two numbers to each new card for quick and easy setup: a personal number and a transponder number. The **personal number** represents the owner of the card. Using the **transponder number**, it is possible to erase a card from the system, even when the card is not available (for example, if it is stolen or misplaced). The transponder number is the current number of the card, which sequentially increases along with the total number of cards registered in the system.

The system automatically assumes that each user card will be assigned to a different user. Therefore, in this simplified system operation, the system automatically assigns personal number 1 and transponder number 1 to the first blue user card to be registered. The system then assigns personal number 2 and transponder number 2 to the second blue user card, etc.

The red admin card has a special status in the system. This card is used to carry out special administrative and configuration tasks. The admin card automatically receives personal number 0 and transponder number 0 from the system.

Automatic assignment of personal numbers and transponder numbers when registering the transponder cards using the KeypadRFID:

Card	Personal number	Transponder number	Serial card number
Admin card	0	0	Printed on card
First user card	1	1	Printed on card
Second user card	2	2	Printed on card
Third user card	3	3	Printed on card
Fourth user card	4	4	Printed on card
...

Registering User Cards with Custom Personal Numbers

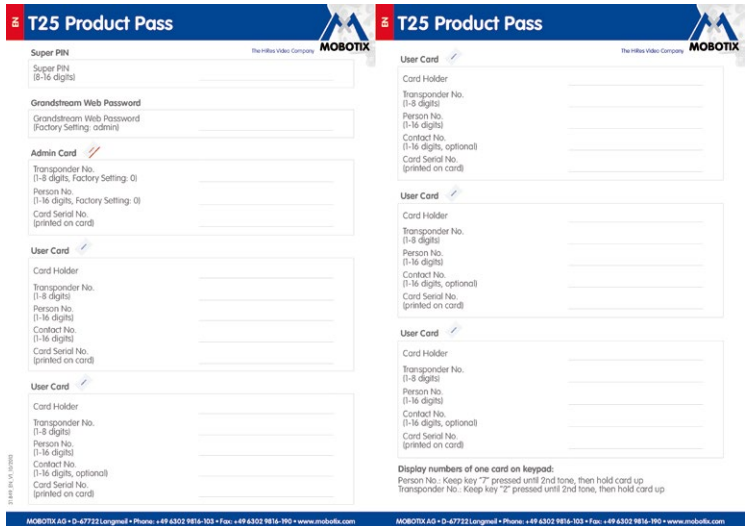
As part of the advanced access control, you can also register user cards with custom personal numbers. If individual users require more than one user card or access PIN, multiple user cards and access PINs can be assigned to the same personal number.

Registering User Cards with Custom Transponder Numbers

Normally, it is not necessary to change the transponder number assigned by the system because this number simply represents the current number of the card. However, if you would like to use longer custom transponder numbers (up to eight digits), these numbers can be derived from the **serial card numbers** printed on the back of each card, at the bottom. We recommend making a note of this number along with the user of the card. This way you can use the serial card number to help identify each card.

T25 Product Pass

We recommend making a note of all numbers, regardless of whether they are custom numbers or numbers that have been assigned automatically by the system. The T25 Product Pass (see *Chapter 3.2.2*) is ideally suited for this task. Make sure that you store these records in a safe place.



1.2.2 Multiple Doorbells and Voice Mailboxes (Addressees)

In addition, the T25 system offers the possibility of entering a **special contact number** on the KeypadRFID (similar to a telephone number) to ring at the remote station of one specific user or user group ("addressee") only. If a BellRFID module is installed, the visitor can press the doorbell of the corresponding addressee. If the addressee does not respond within a certain period of time, the visitor can leave a message on the voice mailbox (just like on a mobile phone).

In the example with the Smith family (see *Section 1.1.2*), a visitor can select to ring the doorbell for the entire family or specifically for the daughter, Anna, who lives on the third floor.



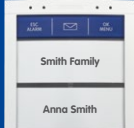





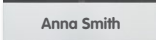


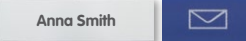
Setting Up Additional Doorbells/Mailboxes at the KeypadRFID Module

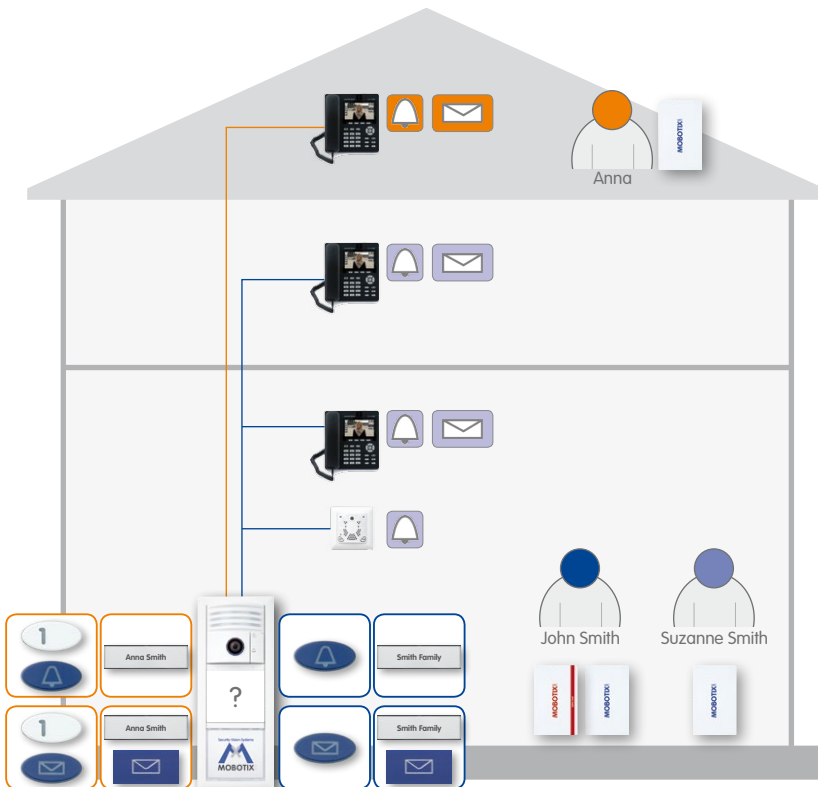
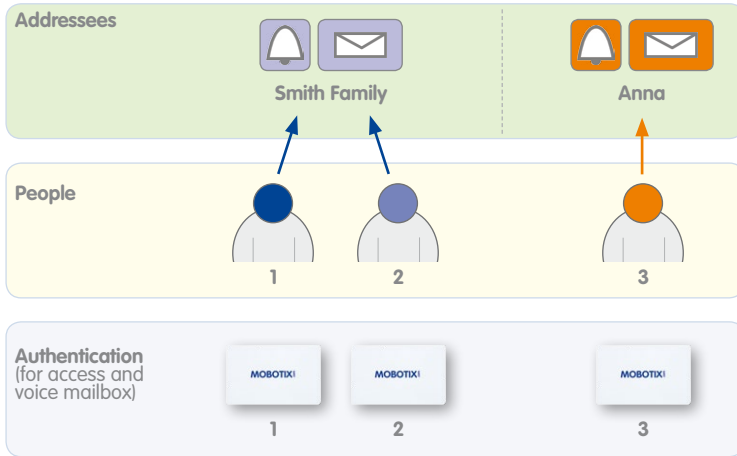
Contact numbers are important if you wish to set up additional doorbells and voice mailboxes in the system. When you set up the user cards, you can also create up to 16 different contact numbers in the system (*Section 2.2.3, «Adding User Cards at the KeypadRFID Module»*). You can set up several cards to employ the same contact number, which means that they are assigned to the same addressee.

In addition to the Family's standard doorbell and voice mailbox, which do not have an extra contact number, Mr. Smith has set up a separate doorbell and voice mailbox for his daughter, Anna (by assigning contact number 1 to Anna's user card). This way, when visitors ring the doorbell with contact number 1, only the video phone in Anna's room is ringing.

Assigning Additional Doorbells/Mailboxes at the BellRFID Module

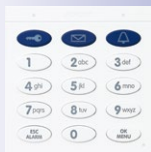
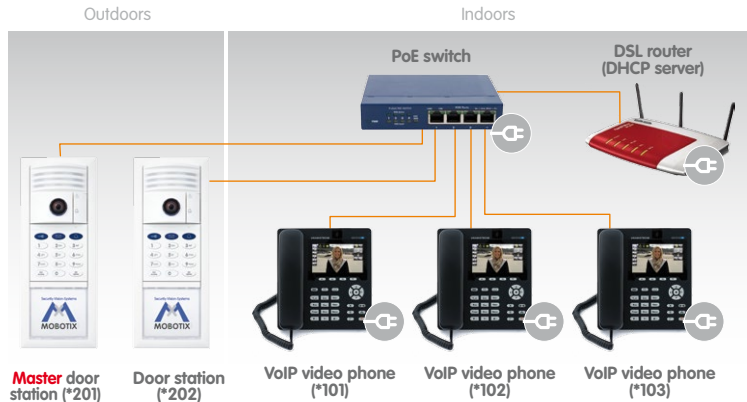
When setting up the BellRFID module and also at a later time, you can assign user cards to the individual bell buttons (see *Section 2.3.5, «Adding User Cards at the BellRFID Module»*). Similar to above, you can also assign several user cards to each bell button.

Addressee	Function	KeypadRFID	BellRFID
Smith Family			
			
Anna Smith			
			



1.2.3 Multiple Door Stations

You can also use multiple networked door stations to secure the main and side entrances of a house. To do so, select one of the door cameras as the master T25. This camera will be in charge of the Auto Configuration for all door stations and remote stations.



KeypadRFID
access module



BellRFID access
module with bell
button set F2

For initial setup, carry out the Auto Configuration for the selected T25 device (and for this device only) once you have set up the network and ensured that all system components are supplied with power (see *Section 2.1*, «*Step 1: Perform the Auto Configuration*»).

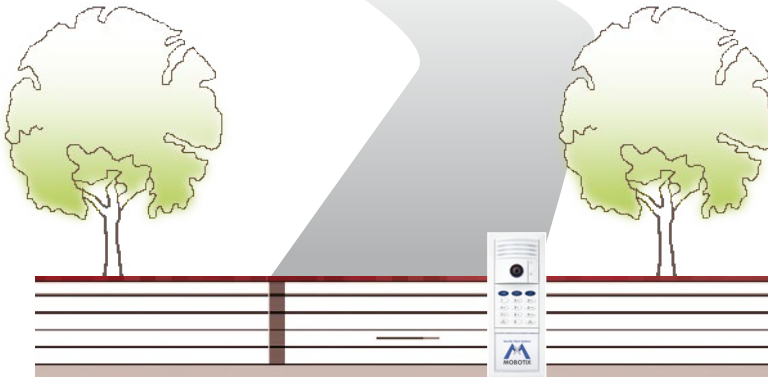
Next, you must set up each access module (by entering a Super PIN and adding cards; see *Section 2.2*, «*Step 2: Set Up the KeypadRFID Access Module*» or *Section 2.3*, «*Step 2: Set Up the BellRFID Access Module*», respectively). The numbers for each door station (Super PIN, personal number, transponder number and contact number) should be identical to the numbers for the master T25 device. We recommend using the same admin card to set up all of the door stations of the building.

Note

In order to erase cards that have been set up on multiple KeypadRFID or BellRFID modules from the system (for example, if it is lost or stolen or if the user has moved away), the card must be erased at every one of these access modules.



T25 with KeypadRFID
in double frame



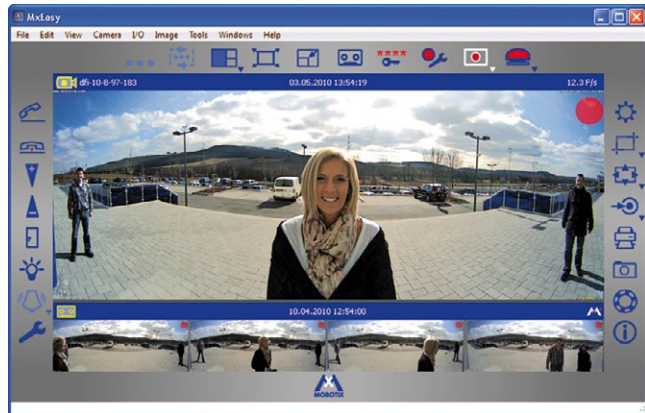
T25 complete set
in triple frame

1.3 Expanding the System with a Computer and MxEasy

1.3.1 Computer as T25 Remote Station

* version 1.5 or higher

In addition to using a Grandstream GXV3140 IP video phone, you can also use any standard computer connected to the network (in conjunction with the MOBOTIX video software MxEasy) as a T25 remote station. You can use MxEasy* to manage and operate up to 16 MOBOTIX cameras and/or door stations.



The program can run in the background of a computer screen or touchpad with a standard operating system and pop up automatically when someone rings the doorbell. Using the computer's microphone and speakers as a two-way communication intercom with lip-synchronous audio (full duplex), you can speak to visitors and by clicking on the corresponding buttons in the software, you can open the door or switch on the light. MxEasy also makes it easy to listen to voice mailbox messages or search through all of your camera recordings.

The current version of MxEasy (for Windows and Mac operating systems) can be downloaded directly from the MOBOTIX website (www.mobotix.com under **Support > Software Downloads > MxEasy**).

Before you launch MxEasy for the first time, set up the system for operation without a computer as described in *Chapter 2*.

1.3.2 Worldwide Two-Way Communication

You will never have to miss an important visitor again – even when you are on-the-go outside of your local network. Using a computer with MxEasy, you can establish an Internet connection – for example, using a Wi-Fi access point or a UMTS/3G modem – to your door station from anywhere in the world.

DynDNS (dynamic domain name system) is the perfect way to access your system. This protocol enables you to access your computer from anywhere in the world. DynDNS does not rely on one (frequently changing) IP address (for example, 213 . 117 . 53 . 215); instead, it utilizes a custom name that you can register with a DynDNS service provider (for example, www.dyn dns.org). The integrated DynDNS client in your local router transmits the new IP address to the DynDNS service provider each time a change is made. This way, you can select the door station with your DynDNS name (for example, Name.dyn dns.org:19801).



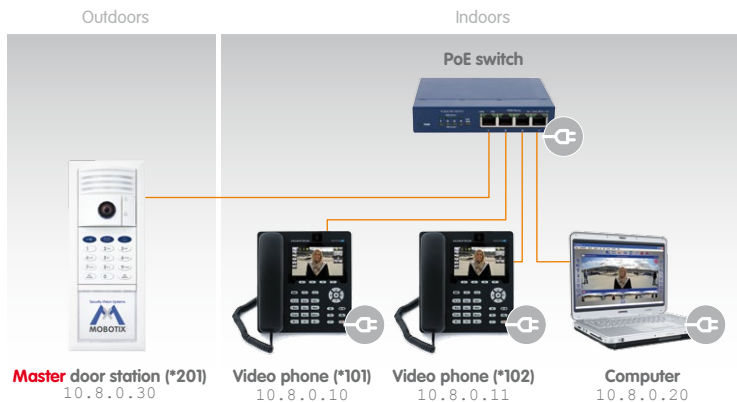
With (worldwide) access via internet, please be sure to use adequately secured and encrypted connections

When MxEasy is running, you can use an existing Internet connection to create a T25 remote station from which you can access all program functions. This way, you will receive video and audio signals when someone rings the doorbell at your house. You can view the live camera image on your monitor or display, speak with the visitor and operate the door lighting and the door opener remotely.

To set up this feature, you will need a computer with a sufficiently fast Internet connection and a router that is connected to the door camera (which has been set up without a computer). See the description in *Section 5.1, «Setting Up Computers as T25 Remote Stations»*.

1.3.3 Network without DHCP Server (Static IP Addresses)

If you are using a network with a static IP address and no DHCP server, you must manually set up all devices connected to the network. You must also configure these devices so that they are assigned to static IP addresses within the same range of addresses. This will enable the devices to communicate with one another.



You will need a computer with MxEasy and a LAN connection in order to carry out the setup. We describe the basic process of configuring one or more IP Video Door Station devices in networks with static IP addresses in *Section 5.2*. With this configuration, you can only startup the system using a computer with MxEasy. It is not possible to operate the system by pressing the bell button on the camera module.



2 INITIAL SETUP WITHOUT A COMPUTER

We recommend reading *Chapter 2* carefully before starting with the initial setup in *Section 2.1* to avoid operating errors. Please first read this selection of frequently asked questions:

How Do I Initiate the Initial Setup Process without a Computer?

With the exception of the special case described in *Section 1.3.3, «Network without DHCP Server (Static IP Addresses)»*, the initial setup always starts with the Auto Configuration process, which is activated by **pressing the bell button on the camera module**. This procedure is described in *Section 2.1, «Step 1: Perform the Auto Configuration»* and ends with a short functional test.



Access Module
KeypadRFID



Access Module
BellRFID with bell
button set F2



Start Auto Configuration

What Do I Need to Do After Auto Configuration?

If the door station has a **KeypadRFID module**, all you need to do now is to enter an **8 to 16-digit Super PIN of your choice and train the red (admin) transponder card** (see *Section 2.2, «Step 2: Set Up the KeypadRFID Access Module»*). You can also easily set up the blue user cards; however, it is not absolutely necessary to do this now.

If the door station has a **BellRFID module**, you can now enter an **8 to 16-digit Super PIN of your choice and train the supplied red admin card** (see *Section 2.3, «Step 2: Set Up the BellRFID Access Module»*). In this case, you can also easily set up the blue user cards; however, it is not absolutely necessary to do this now.

As the owner of a door station with an access module (KeypadRFID or BellRFID), you are free to choose how many of the supplied user cards you would like to train (i.e., to set up). Once you have trained a card, you can use it for keyless entry at that door (using passive RFID technology, no battery required) and listen to messages recorded in your voice mailbox on the outdoor station.

If you like, you can also use custom **Personal, Transponder and Contact Numbers** to personalize the cards. For further details and information on how to manage all your access media (cards and PINs), please refer to the documentation for the installed access module (*Chapter 3, «KeypadRFID Access Configuration»* or *Chapter 4, «BellRFID Access Configuration»*, respectively).

What Can I Do with My Door Station Now?

All the most important door station functions are now available:

- The bell button on the camera module and on the access module (KeypadRFID or BellRFID, if present) are working.
- All the door station modules, including the MX-DoorMaster and video phones, are integrated and the basic settings have been configured.
- The live image of the master door camera is automatically displayed when you pick up the receiver on a Grandstream video phone.
- Two-way communication between the camera module and remote stations is initiated by pressing "7" on the video phone.
- You can open the door conveniently via a remote station, provided an electrical door opener has been connected.
- The basic settings for voice mailbox has also been configured. If no one responds to the door bell within 30 seconds (no one picks up the receiver and opens the door), the visitor is asked to leave a message, which is recorded by the camera module and can be played back later via the access module or a video phone.

How Should I Hold a Transponder Card Up to the KeypadRFID?

When setting up a transponder card, you should ideally hold the card between the thumb and index finger of one hand and move it as close as you can to the KeypadRFID until a beep sounds. Make sure that the card does not touch and inadvertently trigger any of the buttons.



During daily operation, you can usually gain keyless access by holding your user card up to the access module while it is still in its protective case or in your wallet.

How Can I Protect My Door Station Against Unauthorized Access?

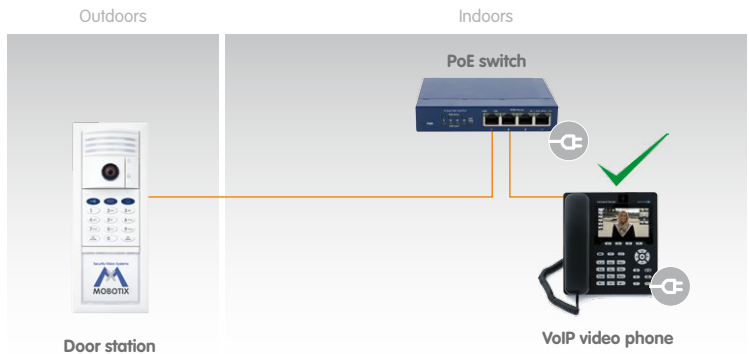
You can now leave the outdoor station and complete the initial setup by protecting your system against unauthorized external access (see *Section 2.4, «Step 3: Configure the System Using a Video Phone»* and *Section 2.5, «Step 4: Protect the System Using a Video Phone»*).

2.1 Step 1: Perform the Auto Configuration

The following assumes that the T25 has been installed and checked in conjunction with *Section 2.8, «Finishing the Installation»* of the *T25 System Manual Part 1*. First remove each required Grandstream video phone from its packaging, connect the receiver and perform the Auto Configuration as described here.

2.1.1 Starting the Video Phone

Connect the **video phone** to the network via a **switch/router** or the NPA PoE set, **connect the power plug** and wait until the telephone has started up.



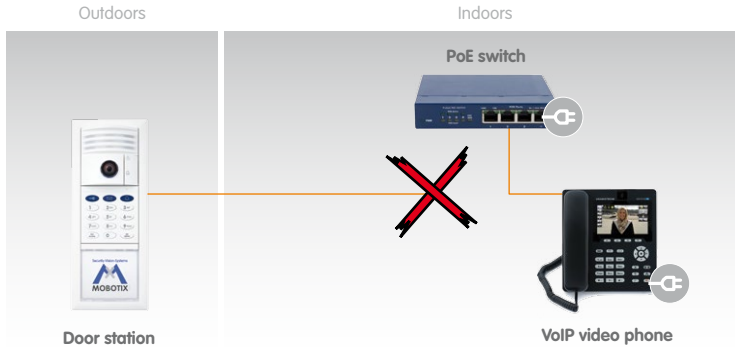
The display shows the **message "NO IP"** (no IP address). The time and date have not been updated. The preconfigured menu language is English.



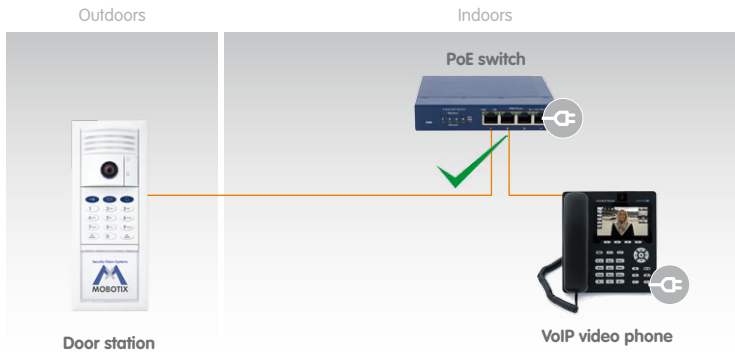
Video phone must be set to factory settings

2.1.2 Starting the Door Station

Disconnect the door station(s) for several seconds from the power supply (for example, remove the network plug).



Now reconnect the door stations power supply, (for example, plug in the network plug). This causes the door station(s) to reboot.



2.1.3 Starting the Auto Configuration

The light and bell buttons on the camera module begin to light up white while rebooting. **Within four seconds of the buttons lighting up on reboot, press the doorbell button on the camera module** (lower button) until the two buttons start to flash briefly.



This Starts the Auto Configuration Process and the Following Happens:

- The lights on the camera module start to flash as the T25 starts up.
- The current T25 IP address and network data are announced automatically.
- Each Grandstream video phone is contacted and configured by the T25.
- Each Grandstream video phone is restarted automatically each time the configuration is updated.
- Each Grandstream video phone displays its newly assigned IP address (for example, 192.168.0.20) and SIP quick dial number (for example, MX_SIP *101) on the display.
- The SIP quick dial number for the first video phone is *101 and the T25 uses *201.

The Auto Configuration process is complete when the camera LEDs light up, all the KeypadRFID* number buttons start to flash, the **ESC/ALARM** button flashes red and the **OK/MENU** button flashes blue.

* if present in the system

2.1.4 Functional Test Part 1

Once all the Grandstream video phones to be used have been detected in the network and integrated via the Auto Configuration process, you should carry out a four-stage functional test.

1. Check the Start Display of the Video Phones

The T25 is the SIP server and has VoIP profiles for all the Grandstream video phones detected in the network. The video phones are assigned a sequential quick dial number beginning with *101 (*101, *102, *103 and so on). The new **quick dial number** and IP address of the telephone are shown on the left side of the display.



The system time supplied by the T25 is shown on the right side of the display. This system time is valid for all the video phones and door stations. The T25 is normally factory-set to CET (Central European Time). Otherwise, you can manually set the time zone, time and date on the KeypadRFID (see *Section 2.2.4*).

The **menu language** of both the video phone and the time and date are factory-set to English. You can change the language on the Grandstream menu (**Menu > Personalize > Language > Select Language**):



Menu > Personalize >
Language > Select
Language

2. Check Connection Established from a Video Phone to the T25

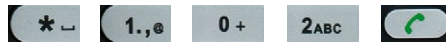
When you pick up the receiver on a video phone, a video and sound connection is established to the master door camera with the quick dial number *201.

3. Check Connection Established from One Video Phone to Another (Intercom Function)

If you want to call another video phone rather than the door station, all you need is the video phone's quick dial number (start display).

Establishing a connection:

- Press the "*" button and then enter the **three-digit quick dial number** of the video phone you require (for example, *102).
- Pick up the receiver (press F4 to reject the call).



4. Check Connection Established From the T25 to Video Phones by Ringing Doorbell

All the connected video phones will ring when you press the bell button on the camera module. Accept the call on any video phone (pick up the receiver).

You have now completed part 1 of the functional test. If the test was unsuccessful, check the connections and the power supply to all the components. Now repeat the entire Auto Configuration process as described in *Section 2.1.2* to *Section 2.1.3*. If the functional test continues to fail, please contact your MOBOTIX partner or the MOBOTIX support team (for more information, visit www.mobotix.com > **Support**).

Continue

- with **Step 2** (*Section 2.2*) if your door station has a KeypadRFID,
- with **Step 2** (*Section 2.3*) if your door station has a BellRFID,
- with **Step 3** (*Section 2.4*) if it does not have a KeypadRFID.

Operating Note: "Green Phone" And "Red Speaker" Buttons

If you press the green phone or red speaker button while the receiver is on the hook, you establish a hands-free connection. The hands-free connection remains active until you either pick up the receiver or press the red speaker button to terminate the connection to the T25.

Pressing the red speaker button when the receiver is already off the hook activates the hands-free function. After you have replaced the receiver, the hands-free connection remains active until you either pick up the receiver again or press the red speaker button to terminate the connection to the T25.



2.2 Step 2: Set Up the KeypadRFID Access Module

All actions described here are carried out on the n KeypadRFID module of the outdoor station. When setting up a BellRFID module, proceed to *Section 2.3, «Step 2: Set Up the BellRFID Access Module»*. If it does not have an access module, proceed to *Section 2.4, «Step 3: Configure the System Using a Video Phone»*.

The KeypadRFID displays the following after Auto Configuration:

- **All number buttons are flashing white**
- The **ESC/ALARM** button is **flashing red**
- The **OK/MENU** button is **flashing blue**



Now you must **enter the Super PIN** and **add the admin card**.

Although you do not need to add user cards and set the time now (*Section 2.2.3* and *Section 2.2.4*), these actions are basic configuration steps that also need to be carried out (MOBOTIX recommendation).

2.2.1 Entering the Super PIN at a KeypadRFID Module

You require the **Super PIN** during the initial setup of the KeypadRFID. The Super PIN is used to protect your system. In an emergency, the Super PIN can be used in place of the admin card for authentication on the KeypadRFID. The Super PIN therefore also allows you to erase cards or set up a new access PIN.

The Super PIN should **not** have a series of zeros only and it must be difficult for unauthorized persons to guess. Select a number that has at least eight and no more than 16 digits (using the digits 0–9). The more digits the number has, the more secure it is.

Make a note of your personal Super PIN immediately in your T25 Product Pass (see *Section 3.2.2*). Step 3 of the initial setup process requires you to enter your Super PIN on the video phone for authentication purposes (see *Section 2.4.2*, «Opening the Admin Setup»).

Enter the Super PIN

1. The KeypadRFID shows the flashing pattern of the successfully completed Auto Configuration process (**ESC/ALARM** flashes red, **OK/MENU** flashes blue).
2. Enter your personal **Super PIN** and press the **OK/MENU** button (which then flashes blue even faster).



3. Re-enter your **Super PIN** and press the (quickly flashing) **OK/MENU** button again.



4. A flashing ring pattern on the KeypadRFID confirms entry of the Super PIN.
5. After approximately ten seconds, the number buttons on the KeypadRFID light up white continuously, the KeypadRFID bell button, key button and **OK/MENU** button flash blue and the **ESC/ALARM** button flashes red. Continue with *Section 2.2.2*, «Adding Admin Cards at the KeypadRFID Module».



Note

If you make an incorrect entry (for example, you enter two different Super PINs) or if you wait longer than 60 seconds between two entries, a warning beep will sound and the KeypadRFID will return to the original state it was in after the Auto Configuration (number buttons will flash white). Repeat the procedure for entering the Super PIN, as described here.

2.2.2 Adding Admin Cards at the KeypadRFID Module

It is also necessary to set up the admin card during the initial setup of the KeypadRFID, in addition to the Super PIN. The card is required as a "T25 master key" for authentication purposes to allow you to set up and erase user cards and user access PINs and specify important system settings (time, changing the Super PIN) on the KeypadRFID.



You should keep the card in a safe place together with your T25 Product Pass. MOBOTIX recommends only using your blue user cards to avoid losing your safety-critical admin card for everyday use (open the door, access your voice mailbox from the KeypadRFID and so on).

General Information on Using Transponder Cards

When setting up a transponder card, you should ideally hold the card between the thumb and index finger of one hand and move it as close as you can to the KeypadRFID until a beep sounds. Make sure that the card does not touch and inadvertently trigger any of the buttons.

During daily operation, you can usually hold the user card up to the KeypadRFID while it is still in its protective case or in your wallet.

You can enter your Super PIN and press the **OK/MENU** button to avoid having to hold the admin card up to the KeypadRFID. However, for security reasons (people looking over your shoulder), you should only use this special function in an emergency, for example, if you have lost your admin card.

Add Admin Card:

Once you have entered your Super PIN, the number buttons on the KeypadRFID light up white continuously, the KeypadRFID bell button, key button and **OK/MENU** button flash blue and the **ESC/ALARM** button flashes red. You must set up the supplied red admin card on the KeypadRFID and add it to the system while the KeypadRFID is in this state.

1. Hold your **admin card** up to the KeypadRFID buttons for about 5 seconds until the beeping stops and the KeypadRFID shows a flashing ring pattern.



2. Afterwards, the bell button, key button, **OK/MENU** button and **ESC/ALARM** button all flash blue on the KeypadRFID. Your admin card has now been set up and automatically assigned the Personal and Transponder No. 0 by the system.
3. **You have now completed the steps that are necessary to set up the KeypadRFID. MOBOTIX recommends now setting up all the blue user cards** that you require



for keyless access. Continue with the next section (see *Section 2.2.3, «Adding User Cards at the KeypadRFID Module»*.)

4. If you do not wish to set up any user cards now, press the **ESC/ALARM** button to exit the Add mode or wait 30 seconds until this happens automatically. Proceed to *Section 2.2.4, «Setting the Time Zone, Time and Date»*) or *Section 2.4, «Step 3: Configure the System Using a Video Phone»*).

Notes

When you set up a card as part of an extended T25 scenario (see *Section 1.2*), you have the option of assigning a custom Personal, Transponder and Contact No. For further information, refer to *Chapter 3, «KeypadRFID Access Configuration»* of this manual.

In case of a wrong entry or cancellation via the **ESC/ALARM** button, a low warning tone is sounded and the system will revert to the original mode it was in after the Auto Configuration (KeypadRFID number buttons will flash white). Enter the Super PIN again.

2.2.3 Adding User Cards at the KeypadRFID Module

Registered blue user cards allow a user to open the door without a key and listen to voice mailbox messages at the door station. This section describes how to set up user cards without assigning individually-selected Personal, Contact or Transponder Numbers (standard T25 scenario).



Immediately after you have set up the admin card, the KeypadRFID remains in Add mode for a further two minutes to allow you to set up additional cards (bell button, key button, **OK/MENU** button and **ESC/ALARM** button all flash blue). In this case, continue with the "Add User Card" section (see below). Otherwise, you must first switch on Add mode again.

Add User Card (without Individual Number Assignment):

1. If you want a user of the specific card to have access to voice-mail at the T25 door station, press the blue bell button before registering that card as keyless entry. Regardless of this, you can always access your voice mailbox via your video phone.



2. Hold the first user card up to the KeypadRFID buttons until a beep sounds and the KeypadRFID shows a flashing ring pattern.



3. The first user card has now been set up and **automatically assigned the Personal and Transponder No. 1** by the system.
4. You can now **set up as many additional user cards as you require**. The next card is assigned the next sequential number, Personal and Transponder No. 2. The following cards are assigned the numbers 3, 4, 5 and so on.
5. If you do not wish to set up any more user cards, press the **ESC/ALARM** button to exit the **Add** mode or wait two minutes until this happens automatically. Proceed to *Section 2.2.4, «Setting the Time Zone, Time and Date»* or *Section 2.4, «Step 3: Configure the System Using a Video Phone»*.

Notes

When you set up a card as part of an extended T25 scenario (see *Section 1.2*), you have the option of assigning a custom Personal, Transponder and Contact No. For further information, refer to *Chapter 3* of this manual.

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than two minutes, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, switch on Add mode again.

Switch on Add Mode Again (If Necessary):

1. Switch on Configuration mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

2. Hold your **admin card** up to the KeypadRFID buttons until the **OK/MENU** button lights up blue continuously.



3. Switch on Access Configuration mode: Briefly press the **blue key button**, which then lights up blue.



4. Enter Add mode: Press the **OK/MENU** button until you hear the second beep again (button lights up blue again).



hold (2nd beep)

2.2.4 Setting the Time Zone, Time and Date

The video phone display shows the current system time. If this is incorrect, you can manually set the time, date and time zone on the KeypadRFID.



* Factory setting: GMT + 1 hour (Berlin, Germany)

You must first set the correct time zone* on the KeypadRFID to enable the switch from daylight saving time to standard time to take place automatically.

Afterwards, date and time should be adjusted.

After you have completed these time settings, continue with *Section 2.4, «Step 3: Configure the System Using a Video Phone»*, if you have not done so already.

Set Time Zone Code:

For this, you need the three-digit code for your time zone. Please refer to the list of time zone codes at the end of this manual. The list is also available as a PDF document from the MOBOTIX website (www.mobotix.com > **Support** > **Manuals**).

1. Switch on configuration mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

2. Hold your **admin card** up to the KeypadRFID buttons until the **OK/MENU** button lights up blue continuously.



3. Switch on Time Zone mode: Press **9** until you hear the second beep and it flashes (reminder: The letter "z" on the button stands for "zone").



hold (2nd beep)

4. Now enter the **three-digit time zone code** for the location to which you are closest (for example, 452 for Europe/London). Confirm your entry by pressing the **OK/MENU** button.



Time Code

5. The respective number buttons on the KeypadRFID light up to show the time zone that you have set.

If you entered the **wrong time zone code**, repeat steps 1–5.

If your door station is not connected to the Internet, you still need to manually set the time and date.

Note

After the time zone has been displayed, you remain in KeypadRFID Configuration mode for 60 seconds, before this mode switches off automatically (if you do not press any more buttons). Press the **ESC/ALARM** button to exit the mode immediately.

Set Time:

1. Switch on Configuration mode (again, if necessary): Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

2. Hold your **admin card** up to the KeypadRFID buttons until the **OK/MENU** button lights up blue continuously.



3. Switch on Time mode: Press **8** until you hear the second beep and it flashes (reminder: The letter "T" on the button stands for "time").



hold (2nd beep)

4. Now enter the **current time in the format hh:mm** (always four digits long): The first two digits indicate the hour and the next two digits indicate the minutes (for example, 0804 = 8:04 a.m. and 2259 = 22:59 p.m.) Confirm your entry by pressing the **OK/MENU** button.



5. The respective number buttons on the KeypadRFID light up to show the time (**hh:mm**) that you have set. The time is also shown on the video phone display **after several minutes**.

If you made a mistake when entering the time, repeat steps 1–5.

Note

After the time has been displayed, you remain in KeypadRFID Configuration mode for 60 seconds, before this mode switches off automatically (if you do not press any more buttons). Press the **ESC/ALARM** button to exit the mode immediately.

Set Date:

1. Switch on Configuration mode (again, if necessary): Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

2. Hold your **admin card** up to the KeypadRFID buttons until the **OK/MENU** button lights up blue continuously.



3. Switch on Date mode: Press **3** until you hear the second beep and it flashes (reminder: The letter "d" on the button stands for "date").



hold (2nd beep)

4. Now enter the **current date in the format yyyyMMdd** (always eight digits long): The first four digits represent the year (for example, 2012), the next two digits represent the month (01 for January through to 12 for December) and the last two digits represent the day (01 to 31). Confirm your entry by pressing the **OK/MENU** button.



Time Code

5. The respective number buttons on the KeypadRFID light up to show the date (**yyyyMMdd**) that you have set. The date is also shown on the video phone display **after several minutes**.

If you made a mistake when entering the time, repeat steps 1 to 5.

Note

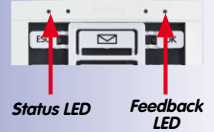
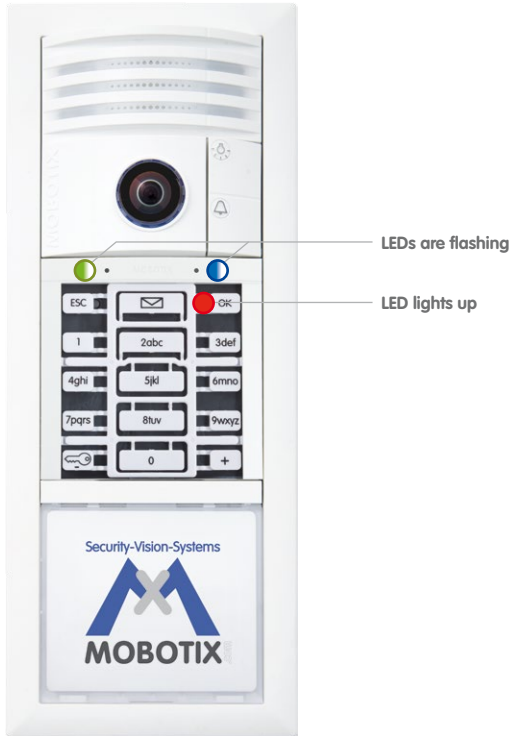
After the date has been displayed, you remain in KeypadRFID Configuration mode for 60 seconds, before this mode switches off automatically (if you do not press any more buttons). Press the **ESC/ALARM** button to exit the mode immediately.

2.3 Step 2: Set Up the BellRFID Access Module

All actions described in the following apply to the BellRFID module of the outdoor station. If this door station does not have an access module, proceed with *Section 2.4, «Step 3: Configure the System Using a Video Phone»*.

Once the autoconfiguration has been completed, the BellRFID module shows the following

- Both LEDs (**green** and **blue**) are flashing.
- The top right LED of the keypad insert (**OK** button) lights up in **red**.



LED Patterns	
	Off
	Lights up
	Blinking
	Flashing

You will now **enter the Super PIN** and **add the admin card**.

While adding the user cards is not mandatory, it is recommended since it constitutes a part of the basic configuration (MOBOTIX recommendation).

2.3.1 Entering the Super PIN at a BellRFID Module

The **Super PIN** is used to protect the system against misuse and also replaces the factory default password ("meinSM) as the new admin password. The password is also used when adding the door station to the MOBOTIX App or MxEasy, for example (user name is **admin**, new password is the current <Super PIN>). Select a Super PIN that has a minimum of 8 and a maximum of 16 digits (more and different digits make it more secure). It must **never** be only zeros and should never be easy to guess by potential intruders.

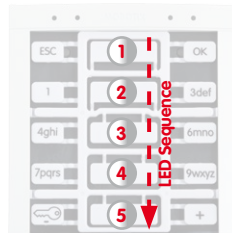
Make sure that you write down your personal Super PIN in the T25 Product Pass (see *Section 3.2.2*). The Super PIN is required in Step 3 of the initial setup for authentication at the video phone (see *Section 2.4.2*).

Entering the Super PIN

Enter your personal Super PIN on the keypad insert, then press the **OK** button in the top right corner. This button is now highlighted yellow.



Enter the Super PIN again, then confirm by pressing the **OK** button. If the two PINs are identical, the LEDs in the center are flashing repeatedly in a sequence from top to bottom.



Next, the top right button (**OK**) lights up green and the button at the center (**Letter**) lights up red.



Note

If you entered different Super PINs or more than 60 seconds passed between entering the PIN and confirming, the module emits a warning sound and returns to the state after finishing the auto configuration. In such a case, you need to repeat this step.

Remove the keypad insert and continue with the next step.

2.3.2 Setting the Bell Button Set to Be Installed

Each button set contains pre-cut name plates made of UV-resistant paper. If required, you can replace the button sets later on – in the same base module! In order to configure the system using BellRFID, the bell buttons are replaced by a keypad insert, which is delivered with the base module.

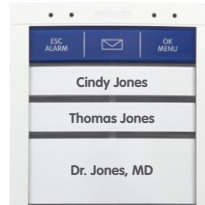
Depending on the bell button set, you need to select one of the six possible button layouts.



MX-Bell1-Button-F1
Large bell button
with function button



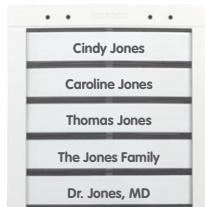
MX-Bell1-Button-F2
2 medium-size bell buttons
with function button



MX-Bell1-Button-F3
1 large, 2 small bell buttons
with function button



MX-Bell1-Button-F4
4 small bell buttons
with function button

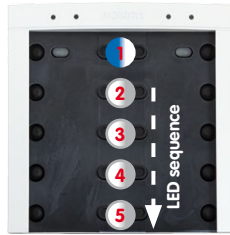


MX-Bell1-Button-O5
5 small bell buttons
(no function button)




MX-Bell1-Button-XL1
XL bell button
(no function button)

You can select the applicable bell button set by pressing any one of the button contacts in the center. The module shows the current bell button set by flashing the LEDs in a specific manner (see table below). The configuration starts with pattern **a**; pressing any button switches to the next pattern in ascending order. After the last pattern, the module returns to pattern **a**.



Pattern 1 (MX-Bell1-Button-F1):

LED 1 permanently blue (function button) LEDs 2 to 5 sequence white (4 bell buttons)

 **Press any one of these buttons**

Pattern	Button Set	Description
a ▲	MX-Bell1-Button-F1	LED 1 permanently blue, 2 to 5 flashing white
b ▬	MX-Bell1-Button-F2	LED 1 permanently blue, 2+3, 4+5 sequence white
c ▬	MX-Bell1-Button-F3	LED 1 permanently blue, 2, 3, 4+5 sequence white
d ▬	MX-Bell1-Button-F4	LED 1 permanently blue, 2, 3, 4, 5 sequence white
e ▬	MX-Bell1-Button-05	LEDs 1, 2, 3, 4, 5 sequence white
f ▼	MX-Bell1-Button-XL1	LEDs 1 to 5 flashing white simultaneously

Once you have found the proper pattern, keep any one of the buttons at the center pressed until the LEDs are flashing repeatedly in a sequence. Next, the top center and right buttons (**OK** and **Letter**) light up green and the button at the top left (**ESC**) lights up red.



The button contacts are now locked until the function and bell buttons have been inserted and the admin card has been trained.

2.3.3 Inserting the Function/Bell Buttons

In order to insert the function or bell buttons, you need to remove the BellRFID module from the frame of the door station (if you have not already done so). Use the blue MOBOTIX key for unlocking the module.

Insert the function and bell buttons in the proper order by inserting the elements from the bottom (e.g., the blue function button first). In order to avoid damaging the buttons, press the elements into the module using two thumbs as shown.



Click the BellRFID module with the buttons into the IP Video Door Station as described in step 2.

2.3.4 Training the Admin Card

Now that you have entered the Super PIN and inserted the buttons, you need to train the Admin card. This card is used as the “master key” for authentication purposes and is required for training and deleting user cards, for example. For every-day use, however (opening doors, mailbox features), you only need the blue user cards. Note that you should always keep the admin card together with the **Product Pass** of the IP Video Door Station in a safe place.



Hold the admin card in front of the BellRFID module for 5 seconds until the sound stops. The LEDs light up in a sequence to confirm that the card has been trained.



All three LEDs at the top are now green to show that the initial operation has been completed successfully. The button lock is now removed.



Continue by training the user cards (next section) or finish setting up the door station.

2.3.5 Adding User Cards at the BellRFID Module

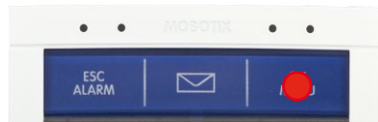
This step is not part of the initial operation of the system and can be performed at any time later on. You can skip this step if you do not intend to use the features described here.

The blue user cards are used by the inhabitants to open the door without using a key and to listen to mailbox messages directly at the IP Video Door Station. If the blue function button at the top has not been installed, make sure that you pay attention to the corresponding key position for the LED patterns described in the following.

Hold a trained admin card in front of the BellRFID module.



The **OK/MENU** button at the top right position lights up red.



If you would like to use the keyless entry features and listen to mailbox messages at the door, press the bell button of the party to which you would like to assign the user card. The selected button lights up white. If you want to use this card only for opening the door (i.e., for the nursing service) make sure that you do **not** press any button now.

Hold the user card in front of the BellRFID module for 5 seconds until the module plays a sound. The LEDs light up in a sequence to confirm that the card has been trained.



If you want to train additional user cards, repeat the steps listed in this section.

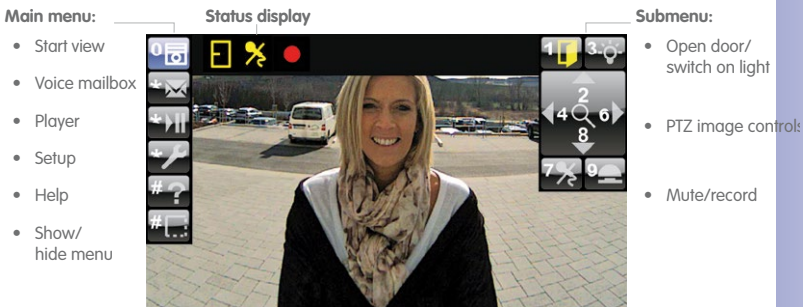
Test the trained cards by holding them in front of the BellRFID module one by one. The electrical door opener should open the door with each card.

2.4 Step 3: Configure the System Using a Video Phone

These settings are specified on the remote station menu of a connected video phone. These settings apply throughout the system and only need to be specified on one remote station, even if several video phones are in use.

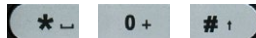
Remote Station Start View:

Once connection between a video phone and the T25 has been established (for example, by picking up the receiver), the live camera image appears with the remote station menu and following start view:



Main Menu Items (On The Left)

You select items on the main menu using the lower three buttons (*, 0, #) of the KeypadRFID on the telephone.



Submenu Items (on the Right)

Displays the subfunctions belonging to the main menu item that has been selected. To select a subfunction, press the number button that is displayed (for example, press 1 to operate the door opener).

Status Display (at the Top)

Icons are used to display the current door station statuses (for example, door opened/closed/locked, telephone microphone disabled and so on).



Open Setup Menu:

Press the "*" button three times to go from the start view to the Setup menu. Continue with the following sections.



The menu language is factory-set to English

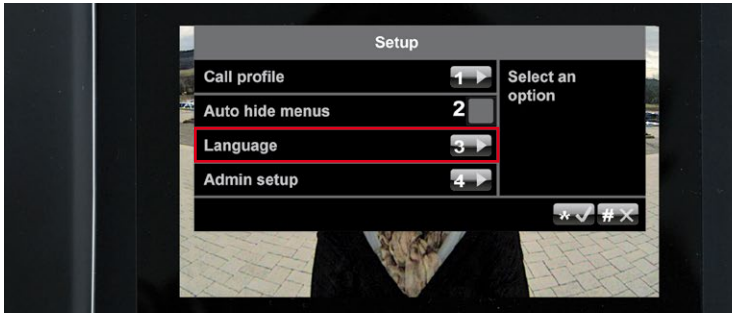
2.4.1 Changing the Menu and Voice Mailbox Greeting Language

This language setting also automatically selects the standard German/English voice mailbox greetings (for example, a prompt for a visitor to leave a message if the door is not opened).

To change the language, select Setup on the main menu.

Change Language:

1. On the Setup menu, press **3** to select the **Language** menu item.



2. Press **1** to select **English** or **2** to select **German**. Confirm your selection ("*" button) or cancel ("#" button).



Remain on the Setup menu and continue with *Section 2.4.2, «Opening the Admin Setup»*.

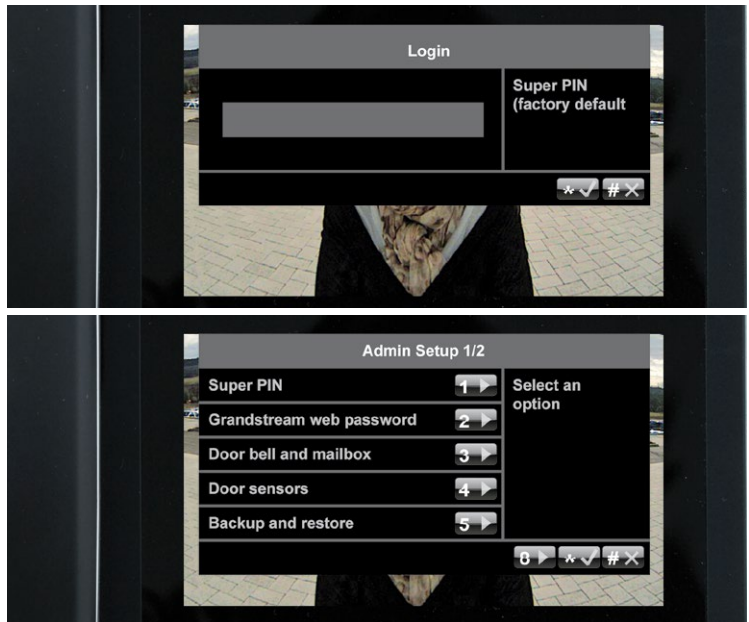
2.4.2 Opening the Admin Setup

To go to the Admin Setup menu, you require the Super PIN that you previously entered on the KeypadRFID (see *Section 2.2.1*).

Activate Admin Setup:

1. On the Setup menu, press **4** to select the **Admin Setup** menu item.
2. Enter your **Super PIN** and press the ******* button (appears after a few seconds) to confirm. If the Super PIN you entered is correct, the **Admin Setup menu** will open.

If your door station does not have a KeypadRFID, you would not have been able to enter a Super PIN during the initial setup. Thus this prompt will not appear. Remain on this menu and continue with *Section 2.4.4, «Setting the Door Status Display»*.



Note

If you enter your Super PIN incorrectly three times, you will be returned to the main menu. You will not be able to re-enter your Super PIN for up to 30 minutes (the time for the next possible PIN entry is displayed).

2.4.3 Changing the Super PIN at the Video Phone

We recommend changing the Super PIN for security reasons (protection against manipulation or unauthorized access to the door station)

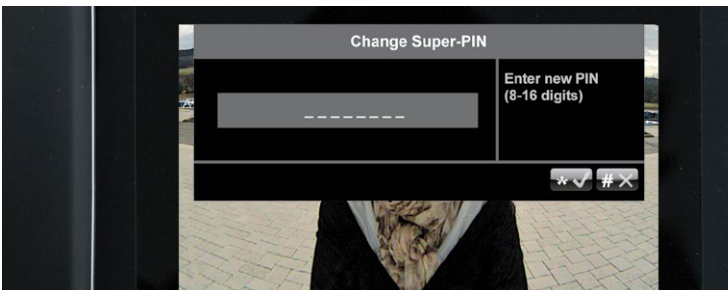
- if your door station does not have a KeypadRFID and therefore a Super PIN has not been entered yet,
- if you suspect that unauthorized persons may know your current Super PIN, or
- if you have taken over an existing door station that is still set up with the previous owner's Super PIN.

Change the Super PIN:

1. Select a new, secure 8- to 16-digit Super PIN. Refer to the information at the beginning of *Section 2.2.1, «Entering the Super PIN at a KeypadRFID Module»* or *Section 2.3.1, «Entering the Super PIN at a BellRFID Module»*, respectively.
2. On the Admin Setup menu, press **1** to select the **Super PIN** menu item.



3. Enter your **new Super PIN** and press the ****#** button to confirm.



4. Enter your new **Super PIN again** and confirm once more by pressing the ****#** button.

After you have changed your Super PIN, or pressed the **#** button to cancel, you are returned to the Admin Setup menu. Proceed to *Section 2.4.4, «Setting the Door Status Display»* to continue with the initial setup.

2.4.4 Setting the Door Status Display

To ensure that the status of the entrance door is displayed on the video phone,

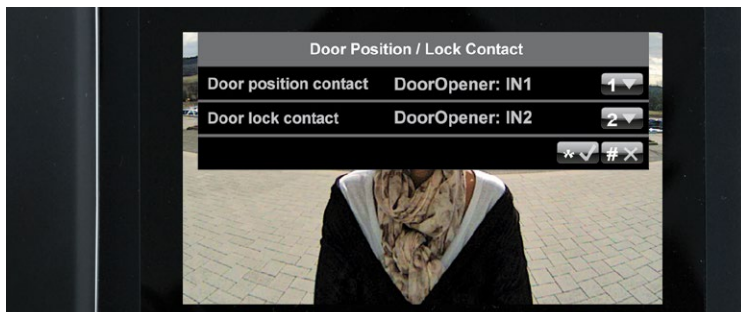
- A door contact (door opened/closed) and a door lock switch (door lock locked/unlocked) must be connected to the MX-DoorMaster or the KeypadRFID (see the *T25 System Manual Part 1*)
- And the installed door sensor connection options must be set correctly on the Admin Setup menu.

Set Door Status Display:

1. On the Admin Setup menu, press **4** to select the **Door sensors** menu item.








2. Select the required connection option for the door contact and door lock switch by repeatedly pressing **1 and 2, respectively**.



3. Confirm your selection or cancel (**/#" button). You are still on the Admin Setup menu. Proceed to *Section 2.4.5, «Activating Video Recording»* to continue with the initial setup.

If you do not know whether and where door sensors are connected, simply try out the different options and check them using the the status display.

Info Icon	Description
	Door opened
	Door closed
	Door locked
	Door unlocked
	Door sensor error/tampering

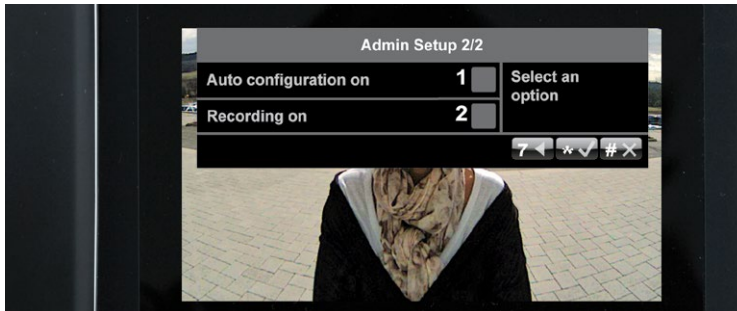
2.4.5 Activating Video Recording

The system is set up at the factory so that only voice mailbox messages are recorded by the door camera.

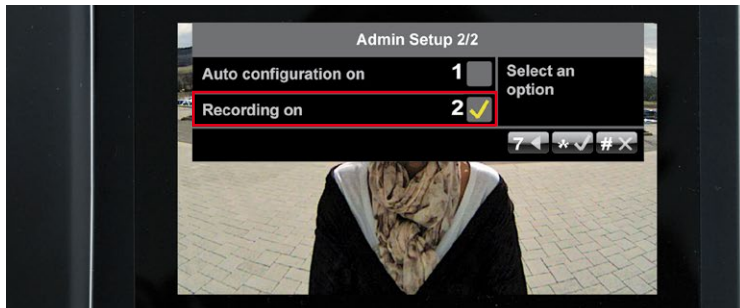
To obtain additional video clips of other door events (for example, ringing doorbell, access granted or denied, door opened), go to the Admin Setup menu and proceed as follows:

Activate Recording

1. Press **8** to go to page 2 of the Admin Setup menu.



2. Press **2** to either activate recording (yellow check mark) or deactivate it again (no check mark). Press the ****#** button to confirm.



3. Now exit the Admin Setup menu by pressing the ****#** button and complete the video phone setup by carrying out a short functional test (see *Section 2.4.6, «Functional Test Part 2»*).

Caution

If you have activated recording, please see the relevant legal guidelines for video surveillance.

2.4.6 Functional Test Part 2

After you have set up your access module and the video phone (Section 2.2, «Step 2: Set Up the KeypadRFID Access Module» or Section 2.3, «Step 2: Set Up the BellRFID Access Module», respectively, and Section 2.4), you should carry out a final functional test:

1. Check That the Blue User Cards Open the Door

Hold each blue user card that you previously trained to the access module to check that the door opening mechanism is triggered. If the mechanism is not triggered, set up the cards again on the access module (Section 2.2.3, «Adding User Cards at the KeypadRFID Module» or Section 2.3.5, «Adding User Cards at the BellRFID Module», respectively).

2. Check Date and Time Settings

Check the current settings on one of the video phone displays (receiver must be on the hook).



If the date and/or time is incorrect, modify the settings on the KeypadRFID, as described in Section 2.2.4, «Setting the Time Zone, Time and Date».

3. Check Door Status Display

Check that actual **entrance door statuses** are displayed correctly on one of the video phones.



If they are not displayed correctly, modify the settings on the video phone, as described in *Section 2.4.4, «Setting the Door Status Display»*.

4. Check the Short Recording Function (If Video Recording Is Activated)

Test the manually triggered short recording function by picking up the receiver on a video phone and pressing **9** when the live image of the door camera appears. The door camera will now record with sound and will stop recording automatically after two minutes (factory setting, can be changed via MxEasy). During recording, the red recording icon is displayed in the status bar.



You can only use **9** to trigger the short recording function if the system's video recording function has been previously activated (see *Section 2.4.5*).

If part 2 of the functional test continues to fail despite the measures recommended, please contact your MOBOTIX partner or the MOBOTIX support team (for more information, visit www.mobotix.com > **Support**).

Proceed with **Step 4** (see *Section 2.5, «Step 4: Protect the System Using a Video Phone»*) to complete the initial setup.

2.5 Step 4: Protect the System Using a Video Phone

You have now reached the last crucial step of the initial setup process. By protecting your system, you can prevent unauthorized persons from accessing the door station and its remote station(s).

As network devices, the T25 door camera and the Grandstream video phone generally allow access to their configuration by entering the IP address in the address bar of a web browser on a networked computer.

Default Access Data of Door Station Camera (Important for Using MxEasy):

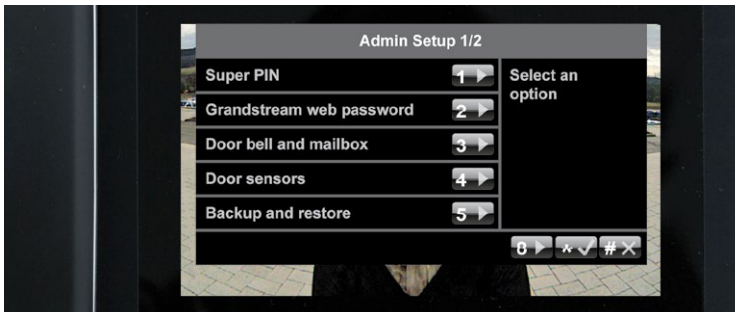
- User name: admin
- Camera admin password: <Super PIN>

Default Access Data of Grandstream Video Phones:

- User name: admin
- Grandstream web password: admin

MOBOTIX recommends changing the web password of the video phones to protect against unauthorized remote access. The door camera is already protected by the Super PIN, which only you know. For both devices, leave the user name as "admin".

To protect your system, open the **Admin Setup** menu on a video phone (as described in *Section 2.4.2*). Continue with the following sections.



2.5.1 Changing the Grandstream Web Password

Open the first **page (1/2)** of the **Admin Setup** menu and press **2** to select the **Grandstream web password** option.



Press **7** to generate a new password that includes letters and numbers. Make a note of the new password in your T25 Product Pass (see *Section 3.2.2*). Exit this menu by pressing the ****#** twice (only possible a few seconds after you have changed the password).



Note

The web password is changed simultaneously for all the Grandstream video phones connected to the network. Therefore, make sure that all the video phones are properly connected and switched on.

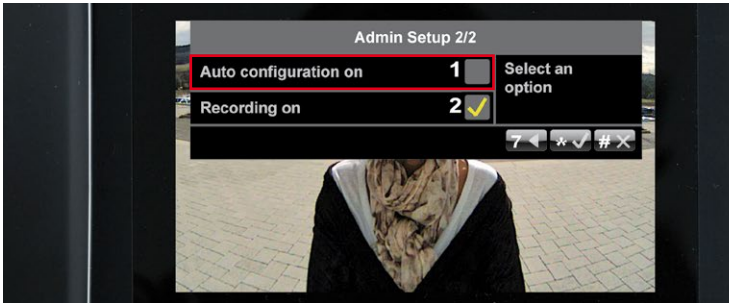
2.5.2 Disabling Auto Configuration

By disabling Auto Configuration, you can prevent access to the door station from the outside. Otherwise, the Auto Configuration could be activated again by pressing the camera bell button, allowing anyone to set up a new Super PIN and admin card and open the door.

To prevent this kind of tampering, open the second **page (2/2) of the Admin Setup menu by pressing 8.**



Press 1 to remove the yellow check mark next to the **Auto Configuration on** option.

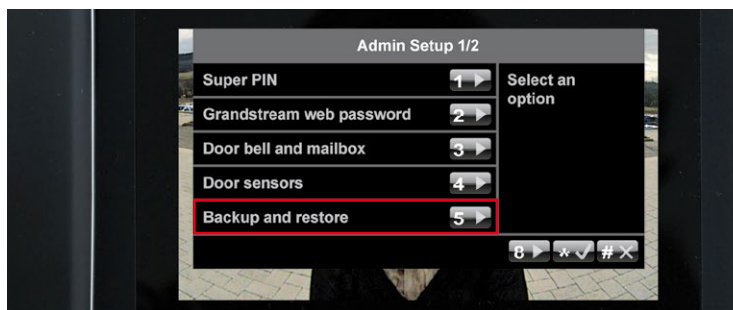


2.5.3 Saving the System Configuration

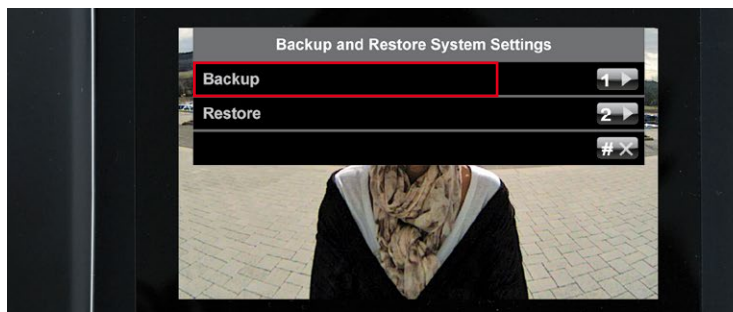
The initial setup and protection steps for the system are now complete. MOBOTIX recommends saving your current system configuration,

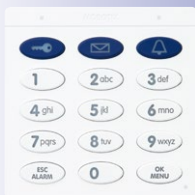
- so as to be able to easily reset inadvertent or unwanted changes made to the system configuration,
- and easily integrate a new door station module (T25-CamCore, KeypadRFID/BellRFID, MX-DoorMaster) after replacement without having to run through the initial setup process again.

The system restore procedure is described in *Chapter 6*. To save your current system configuration, open the **first page (1/2) of the Admin Setup menu** and press **5** to select the Backup and restore option.



Now press 1 to save your settings. Press the "*" button to confirm and exit the menu.





Reader's guide to the diagram: Enable Configuration mode first and then Access Configuration mode in order to add a transponder

Square brackets indicate optional entries (only required if so desired) and the "!" symbol stands for "or"

3 KEYPADRFID ACCESS CONFIGURATION

3.1 Quick Start: Access Configuration

The Quick Start guide supports your configuration work and helps you to learn the main features. It DOES NOT cover everything stated in *Section 3.3, «Managing Transponders»* and *Section 3.4, «Managing Access PINs»* of this manual. You should also read those sections.

Adding, Erasing, Changing

Enter Configuration Mode OK hold (2nd beep)

Enter Access Configuration Mode !

Add Mode OK hold (2nd beep)

Add transponder

[| | 0 ... 9]
Contact No.
[0 ... 9]
Person No.
[0 ... 9]
Transponder No. hold (2nd beep)

Add PIN

[0 ... 9]
Person No.
[0 ... 9]
Access PIN
[0 ... 9]
Access PIN

Erase Mode ESC hold (2nd beep)

Erase current transponder (User Card)

present user card

Erase current transponder (Admin Card_2)

present admin card

Erase non-present transponder

[0 ... 9]
Transponder No.
[ESC]
hold (2nd beep)
[0 ... 9]
Transponder No.
[ESC]
hold (2nd beep)

Erase access PIN



[0 ... 9]
Access PIN
[0 ... 9]
Access PIN


Erase user

[0 ... 9]
Person No.
[OK]
[0 ... 9]
Person No.
[OK]


Erase contact (doorbell/voice mailbox)


[0 ... 9]
Contact No.
[]
[0 ... 9]
Contact No.
[]


Enter Configuration Mode  hold (2nd beep) 

Enter Access Configuration Mode 


Change access PIN


0 ... 9  Access PIN old


0 ... 9  Access PIN new

0 ... 9  Access PIN new

Change Super PIN

0 ... 9  Super PIN old

0 ... 9  Super PIN new


0 ... 9  Super PIN new


Time-Restricted Access (Set Up "Tradesman Card", 1-48 Hours)


 hold (2nd beep)  0 ... 9  Access Time (h)


You do not need to be in a specific system mode to set up the "Tradesman Card" and to view system details

Recalling System Information (with Admin or User Card)


Current time  8 hold (2nd beep)


Current date  3 hold (2nd beep)

Time zone code  9 hold (2nd beep)

Software version  4 hold (2nd beep)

Recalling Transponder Information (with Admin or User Card)

Transponder number  2 hold (2nd beep)

Personal number  7 hold (2nd beep)

Function not available with the tradesman card

3.2 Individual Configuration of Access Media

As described in the extended application scenario in *Section 1.2*, the MOBOTIX transponder cards can also be set up with individually-selected personal, transponder or contact numbers. On the following pages, you will find out how to do this and how to manage cards and PINs directly via the KeypadRFID.

3.2.1 Personal, Transponder and Contact Numbers

The system automatically assigns every new card a sequential personal and transponder number during a quick card setup. The (first) red admin card is assigned personal number 0 and transponder number 0. The first blue user card is assigned personal number 1 and transponder number 1. The second blue user card is assigned personal number 2 and transponder number 2, etc.

When setting up the cards, you can also allocate these numbers individually. Any number of user cards can share the same personal number, but only one transponder number can be assigned to each door station or KeypadRFID.

Personal Number

With a custom personal number, you can set up multiple transponder or an additional access PIN for a single user. Additionally, you can erase all the access media connected to a personal number from the system at once ("Erase user from system").

Transponder Number

With the transponder number, you can erase a card without having it be physically present (theft, loss).

Contact Number

A contact number works like a telephone number that is entered on the KeypadRFID to contact specific users or user groups in the building. Only the remote station(s) of the selected user(s) will ring, and/or their voice mailbox will be accessed. For user cards, you can set up up to 16 different contact numbers.

Note

Should you want to assign new individual numbers to a user card that has already been set up previously, for example, when initially starting up a system, first erase the card as described in *Section 3.3.2* and the proceed as described in *Section 3.3.1*.

3.2.2 T25 Product Pass for Recording System Information

You will find the T25 Product Pass shown below in the appendix of this manual. Here, you should enter all user data and passwords that occur during configuration. Store the record card in a safe place.

To check the personal and transponder numbers of a card, simply view them on the KeypadRFID:

Personal Number:

7
hold (2nd beep)



Transponder Number:

2
hold (2nd beep)



Press button 7 (p = person) or 2 (c = card) until the second beep sounds, then hold up the card

3.3 Managing Transponders

3.3.1 Adding User Cards (Individual Number Assignment)

You need the red admin card to set up blue user cards.



Proceed as Follows:

1. Specify the individually-selected personal, contact and/or transponder numbers as required and immediately enter them on your T25 Product Pass (see *Section 3.2.2*).
2. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

3. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the **OK/MENU** button lights up blue continuously.



4. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



5. Enter Add Mode: Press the **OK/MENU** button until you hear the second beep (button lights up blue).



hold (2nd beep)

6. **Assign contact – method 1 (quick setup without contact number):** Press the blue bell button to enable the new card for checking and using the standard voice mailbox directly via the KeypadRFID. If you wish to exclude the user card from voice mailbox interaction via the KeypadRFID, do not press the bell button.



Assign contact – method 2 (with contact number): If you have specified a contact number, enter it now and press the blue bell button. This sets up a new doorbell with a voice mailbox that can be checked with the user card by holding it up to the KeypadRFID.

Assign contact – method 3 (with additional bell button module): If you are using an additional bell button module (such as from a third-party manufacturer), press the bell button that you wish to assign to the new user card as a contact.

- 7. Assign individual personal number: If you have specified a **personal number**, enter it now and press the **OK/MENU** button. If not, skip this step and the card will automatically be assigned a new personal number.



- 8. Assign individual transponder number: If you have specified a **transponder number***, enter it now and press the **ESC/ALARM** button until you hear the second beep. If not, skip this step and the card will automatically be assigned a new transponder number.



- 9. Present card: Hold the **user card** up to the KeypadRFID buttons until a beep sounds and the KeypadRFID shows a flashing ring pattern. Make sure that the card does not touch and inadvertently trigger any of the buttons.



- 10. As soon as the flashing pattern stops, setup for the new user card is finished. You are now back in configuration mode (the **OK/MENU** button lights up blue). **Press the ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



If you want to train additional user cards, repeat steps 4 through 10.

Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Add mode as described above.

MOBOTIX recommends setting up all the cards and access PINs associated with one person to share the same personal number

* For example, the last digits of the imprinted card serial no.



3.3.2 Erasing User Cards

If you no longer require a previously set-up blue user card, if the card is no longer available (loss, theft), or if you want to set up the card afresh with individual numbers, e.g., for a different user or voice mailbox, you should erase the card.

To do so, you will need the red admin card (or Super PIN) and the transponder number of the user card to be erased, if you no longer have the card itself. If you still have the card, you can erase it by holding it up to the KeypadRFID without requiring a transponder number.

Proceed as Follows:

1. Ready the admin card and the user card to be erased or its transponder number.
2. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

3. Hold your **admin card** up to the KeypadRFID's buttons (or enter the **Super PIN** and then press the **OK/MENU** button) until you hear a beep and the **OK/MENU** button continuously lights up blue.



4. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



5. Enter Erase Mode: Press the **ESC/ALARM** button until you hear the second beep (button lights up blue). You can now erase the user card (step 6), or if you do not have the card, use its transponder number to erase it (step 7).



hold (2nd beep)

6. **Erase current user card:** Hold the **card** up to the KeypadRFID until you hear the first beep (the key button's flashing pattern will change) and pull the card away again. Next, **confirm the card** by again holding it up to the KeypadRFID until you hear a beep.



Erase non-present user card: Enter the **card's transponder number** and press the **ESC/ALARM** button until the second beep sounds. **Re-enter the transponder number** to confirm and again press the **ESC/ALARM** button until you hear the second beep.



7. The card details have now been erased from the system and, if required, the card can be set up afresh. You are now back in configuration mode (the **OK/MENU** button lights up blue). Press the **ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



Notes

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Erase mode as described above.

3.3.3 Time-Restricted Access ("Tradesman Card")

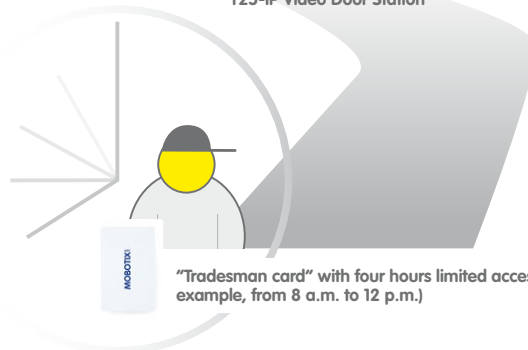
With the KeypadRFID, you can configure a user card to provide keyless entry (without voice mailbox access via the KeypadRFID) for a time span of up to 48 hours. However, this card cannot be set up for use as a regular user card.

A time-restricted card is useful, for example, for times when a tradesman you trust will be working in your apartment while you are away and he/she needs to enter/exit the building several times during the day.

When the preset time span has elapsed, you can reset the card as a tradesman card, or if you wish to turn it into a regular user card, you can erase it and then set it up as needed.



T25-IP Video Door Station



"Tradesman card" with four hours limited access (for example, from 8 a.m. to 12 p.m.)

Note that you need a red admin card in order to train a time-restricted user card.

To set up a time-restricted user card, you need the red admin card. Proceed as follows:

1. Press the **blue key button until you hear the second beep** (button flashes blue).



hold (2nd beep)

2. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the blue key button lights up blue continuously.



3. Set the validity period (1–48 hours): Enter the **desired validity period in hours** via the KeypadRFID: (min. 1, max. 48).



4. Present time-restricted user card: Hold the **user card** up to the KeypadRFID buttons until a beep sounds and the KeypadRFID shows a flashing ring pattern.



5. The system then returns to regular operating mode and setup of the time-restricted card is complete. The entered time span commences immediately; the card can be used for keyless access until the end of the validity period.

Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system immediately reverts to the regular operating mode (all buttons light up white).

3.3.4 Adding Admin Cards

As part of the initial setup, you have already set up a red admin card via the KeypadRFID (*Section 2.2.2*). If needed, you can also set up additional admin cards via the KeypadRFID (e.g., as backup cards or for other users wanting to manage the system). Contact your MOBOTIX dealer to purchase red admin cards.

To set up an additional red admin card, you need a previously set-up admin card or the Super PIN. Proceed as follows:



Proceed as Follows:

1. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

2. Hold your **previously set-up admin card** up to the KeypadRFID's buttons (or enter the Super PIN and then press the **OK/MENU** button) until you hear a beep and the **OK/MENU** button continuously lights up blue.



3. **Enter Access Configuration Mode:** Briefly press the **blue key button**, which then lights up blue.



4. **Enter Add Mode:** Press the **OK/MENU** button until you hear the second beep (button lights up blue).



hold (2nd beep)

5. Hold up new admin card to be set up: Hold the **new admin card** up to the KeypadRFID buttons until a beep sounds and the KeypadRFID shows a flashing ring pattern. Make sure that the card does not touch and inadvertently trigger any of the buttons.



- As soon as the flashing pattern stops, setup for the new admin card is finished. You are now back in configuration mode (the **OK/MENU** button lights up blue). Press the **ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



- To check the transponder number of the new admin card, hold it up to the KeypadRFID and make a note of the number. Press the **"2" button** (c = card) until you hear the second beep and then hold the new admin card up to the KeypadRFID.

Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Add mode as described above.

3.3.5 Erasing Admin Cards

If you no longer require a previously set-up red admin card, or if the card is no longer available (loss, theft), you should erase the card for security reasons.

To do so, you will need one previously set-up admin card (or Super PIN) and the transponder number of the admin card to be erased, if you no longer have another admin card. If you still have the card, you can erase it by holding it up to the KeypadRFID without requiring a transponder number.

Proceed as Follows:

- Ready the set-up admin card and the admin card to be erased or its transponder number and the Super PIN.
- Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

- Hold a **red admin card not to be erased** up to the KeypadRFID buttons (or enter the **Super PIN** and then press the **OK/MENU** button, if there is no remaining admin card) until you hear a beep and the **OK/MENU** button continuously lights up blue.



4. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



5. Enter Erase Mode: Press the **ESC/ALARM** button until you hear the second beep (button lights up blue). You can now erase the admin card at hand (step 6), or if you no longer have the admin card, use its transponder number to erase it (step 7).



hold (2nd beep)

6. **Erase current admin card:** Hold the **card to be erased** up to the KeypadRFID until you hear the first beep (the **ESC/ALARM** button lights up red) and pull the card away again. Next, confirm the card by again holding it up to the KeypadRFID until you hear a beep.



Erase non-present admin card: Enter the **transponder number of the card to be erased** and press the **ESC/ALARM** button until you hear the second beep (**ESC/ALARM** button flashes red). Re-enter the **transponder number for confirmation** and press the **ESC/ALARM** button until you hear the second beep.



...



Transponder No.



hold (2nd beep)



...



Transponder No.



hold (2nd beep)

7. The admin card details have now been erased from the system and, if required, the card can be set up afresh. You are now back in configuration mode (the **OK/MENU** button lights up blue). Press the **ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Erase mode as described above.

3.4 Managing Access PINs

The electrical door opener can also be triggered by entering an access PIN and then pressing the blue key button. You first need to set up an access PIN in the system to activate this function for a user. You can freely choose the PIN. Every user can have their own PIN.

Notes on How to Securely Use Access PINs

In general, there is an increased security risk in using an access PIN instead of a card, because a potential burglar can find out the code. PIN access should therefore be using sparingly, such as in emergencies, and they should always involve long PINs (never 1-1-1-1, date of birth, etc.) and only be used for non-critical doors (such as garage doors, inside doors of a building, etc.).

An access PIN needs to have at least four and no more than 16 digits, and it may not consist of zeros only.

MOBOTIX recommends changing your access PINs on a regular basis.

Always make a note of your access PINs on your T25 Product Pass, which should be stored in a secure location (*Section 3.2.2*).

3.4.1 Adding PINs

One way to set up access PINs is to assign them to specific users via their personal numbers. This is useful in cases where you wish to erase all the access PINs (and user cards) of a user without having to enter the access PINs (*Section 3.5*).

You need the red admin card to set up an access PIN.

Proceed as Follows:

1. Select an access PIN and enter it on your T25 Product Pass.
2. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



3. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the **OK/MENU** button lights up blue continuously.



4. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



5. Enter Add Mode: Press the **OK/MENU** button until you hear the second beep (button lights up blue).



hold (2nd beep)

6. Assign access PIN: Enter the **personal number** of the user to whom you wish to assign the access PIN and press the **OK/MENU** button. Otherwise, you can skip this step and continue with step 7.



Person No.

7. Enter PIN: Enter the **access PIN** on the KeypadRFID and press the **blue key button** (which then displays a blue flashing pattern). Re-enter the **access PIN for confirmation** and press the **blue key button**. A beep sounds and the KeypadRFID displays a flashing ring pattern.



Access PIN



Access PIN

8. Setup of the new access PIN is complete. You are now back in configuration mode (the **OK/MENU** button lights up blue). Press the **ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Add mode as described above.



3.4.2 Deleting PINs

You need the red admin card as well as the PIN itself to erase a previously set-up access PIN.

Proceed as Follows:

1. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



2. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the **OK/MENU** button lights up blue continuously.



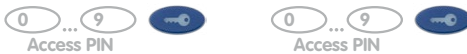
3. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



4. Enter Erase Mode: Press the **ESC/ALARM** button until you hear the second beep (button lights up blue).



5. Enter access PIN: Enter the **access PIN to be erased** and briefly press the **blue key button** (the button's flashing pattern will change). **Re-enter the PIN for confirmation** and again press the **blue key button** briefly, which then lights up blue continuously.



6. The access PIN has now been erased from the system and, if required, another PIN can be set up afresh. You are now back in configuration mode (the **OK/MENU** button lights up blue). Press the **ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Erase mode as described above.

3.4.3 Changing PINs

You require the user's old and new PINs to change an access PIN previously set up for a user. The personal number of the user to whom the access PIN may have been assigned during the original setup is not required.

Proceed as Follows:

1. Select the new access PIN and immediately make a note of it on your T25 Product Pass (*Section 3.2.2*). The **new access PIN also needs to have at least four and no more than 16 digits**, and it **may not consist of zeros only**.
2. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

3. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the **OK/MENU** button lights up blue continuously.



4. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



5. Enter old PIN: Enter the **previous access PIN** and briefly press the **blue key button** (button flashes blue).



Access PIN

- Enter new PIN: Enter the **new access PIN** and briefly press the **blue key button** (button flashes blue). Re-enter the **new access PIN for confirmation** and briefly press the **blue key button** (button lights up blue). A beep sounds and the KeypadRFID displays a flashing ring pattern.



- The access PIN is changed. You are now back in configuration mode (the **OK/MENU** button lights up blue). Press the **ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



Notes

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Add mode as described above.

You require the old and new PINs as well as the user's personal or contact number to change an access PIN previously set up for a user.

3.5 Erasing All Access Privileges of a User (Cards/PINs)

By using the red admin card and the KeypadRFID, you can erase all the access media set up for a specific user at once, i.e., all blue user cards and access PINs assigned to the same personal number. The invalidated user cards can be set up again from scratch at any time.

To invalidate all user cards and PINs sharing the same personal number, you need the red admin card.

Proceed as Follows:

1. Procure the personal number of the user for whom keyless access is to be removed.
2. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).

An oval icon containing the text "OK".

hold (2nd beep)

3. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the **OK/MENU** button lights up blue continuously.



4. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



5. Enter Erase Mode: Press the **ESC/ALARM** button until you hear the second beep (button lights up blue).

An oval icon containing the text "ESC".

hold (2nd beep)

- Identify user: Enter the **personal number of the user to be erased** and briefly press the **OK/MENU** button. **Re-enter the personal number for confirmation** and again press the **OK/MENU** button **briefly**.

0 ... 9 OK
Person No.

0 ... 9 OK
Person No.

- All user cards, PINs and data associated with the user are now erased. The system is returned to its regular operating mode (all buttons light up white).



Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system immediately reverts to the regular operating mode (all buttons light up white). If required, re-enter into Erase mode as described above.

3.6 Erasing Contacts (Doorbell/Voice Mailbox)

The steps described here are only available if you have created new contacts in the system by setting up contact numbers.

Every setup contact number represents a contact and works like a telephone line to specific user or user groups in the building. After the user has entered the contact number on the KeypadRFID, the remote station(s) of the selected user(s) will ring, and/or their voice mailbox will be accessed. You can set up to 16 different contacts with contact numbers.

When a contact is erased from the system, the associated KeypadRFID button combinations for ringing the bell and using the voice mailbox are also erased. Users whose user cards were linked to a contact during setup (*Section 3.3.1*) continue to have access to the building; however, their voice mailbox and voice mailbox access data are erased from the system.

You require the red admin card to erase a contact or a contact number from the system.

Proceed as Follows:

1. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

2. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the **OK/MENU** button lights up blue continuously.



3. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



4. Enter Erase Mode: Press the **ESC/ALARM** button until you hear the second beep (button lights up blue).



hold (2nd beep)

5. Enter Contact Number: Enter the **contact number to be erased** and briefly press the **blue bell button** (the button's flashing pattern will change). **Re-enter the contact number for confirmation** and again press the blue bell button briefly.



6. **The contact is now erased (no bell connection or voice mailbox remain for this contact number).** The system is returned to its regular operating mode (all buttons light up white).



Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system immediately reverts to the regular operating mode (all buttons light up white). If required, re-enter into Erase mode as described above.

3.7 Changing the Super PIN at the KeypadRFID Module

We recommend changing the Super PIN for **security reasons** (protection against manipulation or unauthorized access to the door station)

- if you suspect that unauthorized persons may know your current Super PIN, or
- if you have taken over an existing door station that is still set up with the previous owner's Super PIN.

The other method for changing the Super PIN (by video phone) is described in *Section 2.4.3*.

To change the Super PIN, you need the old (i.e. the current) Super PIN, a new secure Super PIN (8–16 digits) and the red admin card.

Proceed as Follows:

1. Select a new Super PIN and immediately make a note of it on your T25 Product Pass (*Section 3.2.2*). The new Super PIN also needs to have at least eight and no more than 16 digits, and it should be selected with security in mind (no obvious number combinations).
2. Enter Configuration Mode: Press the **OK/MENU** button until you hear the second beep (button flashes blue).



hold (2nd beep)

3. Hold your **admin card** up to the KeypadRFID buttons until you hear a beep and the **OK/MENU** button lights up blue continuously.



4. Enter Access Configuration Mode: Briefly press the **blue key button**, which then lights up blue.



5. Enter old Super PIN once: Enter the **old Super PIN** and briefly press the **OK/MENU** button (the button's flashing pattern will change). **Please note:** If the module software of your KeypadRFID is **release number 1.0.1.4 or older**, you do not need to enter the old Super PIN. Proceed to step 6.



6. Enter new Super PIN twice: Enter the **new Super PIN** and briefly press the **OK/MENU** button (the button's flashing pattern will change). **Re-enter the new Super PIN for confirmation** and briefly press the **OK/MENU** button (button lights up white). A beep sounds and the KeypadRFID displays a flashing ring pattern.

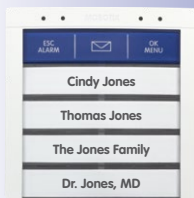


7. As soon as the pattern stops flashing, the new Super PIN has been changed. You are now back in configuration mode (the **OK/MENU** button lights up blue). Press the **ESC/ALARM** button to exit. After 60 seconds, the mode is exited automatically.



Note

In case of a wrong entry, cancellation of entry via the **ESC/ALARM** button, or a delay of more than 60 seconds, a low warning tone is sounded and the system reverts to the regular operating mode (all buttons light up white). If required, re-enter into Add mode as described above.



4 BELLRFID ACCESS CONFIGURATION

4.1 Managing Transponders

4.1.1 Adding User Cards

The blue user cards are used by the inhabitants to open the door without using a key and to listen to mailbox messages directly at the IP Video Door Station. If the blue function button at the top has not been installed, make sure that you pay attention to the corresponding key position for the LED patterns described in the following.



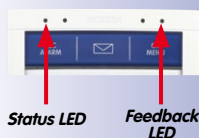
1. Hold a trained admin card in front of the BellRFID module. The **OK/MENU** button at the top right position lights up red.



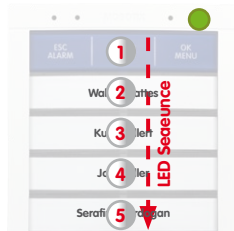
2. If you would like to use the keyless entry features and listen to mailbox messages at the door, press the bell button of the party to which you would like to assign the user card. The selected button flashes white. If you want to use this card only for opening the door (i.e., for the nursing service) make sure that you do **not** press any button now.
3. Hold the user card in front of the BellRFID module for 5 seconds until the module plays a sound.



The LEDs light up in a sequence to confirm that the card has been trained and the feedback LED of the module briefly lights up green.



LED Patterns	
	Off
	Lights up
	Blinking
	Flashing



If you want to train additional user cards, repeat the steps listed in this section.

Test the trained cards by holding them in front of the BellRFID module one by one. The electrical door opener should open the door with each card.

4.1.2 Deleting Individual User Cards

In order to delete a user card, proceed as follows:

1. Hold a trained admin card in front of the BellRFID module. The **OK/MENU** button at the top right position lights up red.



2. Again hold the admin card to the module (the **ESC/ALARM** button flashes red).



3. Hold the user card you would like to delete in front of the BellRFID module. The module acknowledges this action by one short flash of the **ESC/ALARM** button.



4. Again hold the user card you would like to delete in front of the BellRFID module. The feedback LED of the module briefly lights up green.



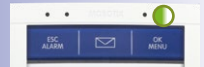
4.1.3 Deleting All Cards of a User

By means of the red admin card, you can use the BellRFID module to delete all transponders of a specific user (i.e., all blue user cards with the same person number) in one step. The invalid transponders can be re-trained at any door station later on.

1. Disconnect the power supply of the door station, remove the BellRFID module from the frame and slide the bell buttons out of the module (see *T25 System Manual Part 1, Section «Exchanging, Removing and modifying Modules»*).
2. Slide the keypad insert into the module, restore the power supply and wait until the door station has started.



Note that you cannot use the admin card to delete itself!



- Now press and hold both the **ESC** and the **OK** buttons until the feedback LED starts blinking blue.



- Hold a trained admin card in front of the BellRFID module or enter the Super PIN and press **OK**. The feedback LED lights up blue.



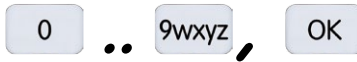
- Press the key button of the keypad insert. The feedback LED starts flashing blue.



- Press the **ESC** button of the keypad insert until the feedback LED starts blinking blue.



- Enter the person number of the transponders you want to delete and press **OK**. The feedback LED lights up blue.



- Enter the person number again to acknowledge and press **OK**. The feedback LED lights up green and then slowly fades out.



- Disconnect the power supply of the door station, remove the keypad insert and slide the bell buttons back into the module (see Section 2.3.3, «Inserting the Function/Bell Buttons»).



4.1.4 Deleting All Cards (Admin and User)

If one or more user cards have been lost, it can make sense to delete all cards (user **and** admin) and to train the remaining cards again later on:

1. Hold a trained admin card in front of the BellRFID module. The **OK/MENU** button at the top right position lights up red.



2. Again hold the admin card to the module (the **ESC/ALARM** button flashes red).



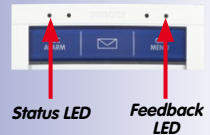
3. Now press and hold any bell button until the three LEDs at the top start flashing red and the other LEDs are flashing white. Confirm the deletion by again pressing and holding the same bell button.



The LEDs light up in a sequence to confirm that all cards have been deleted and the feedback LED of the module briefly lights up green.



The system prompts you to hold an untrained admin card to the module (Section 2.3.4, «Training the Admin Card»). To train the user cards, proceed as described in Section 4.1.1, «Adding User Cards».

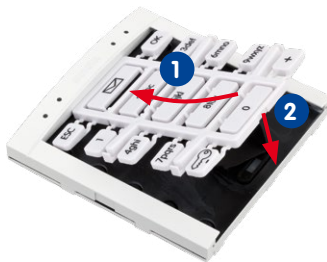


LED Patterns	
	Off
	Lights up
	Blinking
	Flashing

4.2 Changing the Super PIN at the BellRFID Module

If you want to change the Super PIN of the IP Video Door Station, proceed as follows:

1. Disconnect the power supply of the door station, remove the BellRFID module from the frame and slide the bell buttons out of the module (see *T25 System Manual Part 1, Section «Exchanging, Removing and modifying Modules»*).
2. Slide the keypad insert into the module, restore the power supply and wait until the door station has started.



3. Press the **ESC** and **OK** buttons at the same time. The feedback LED of the module briefly lights up blue.



4. Hold a trained admin card in front of the BellRFID module or enter the Super PIN and press **OK**. The feedback LED lights up blue.



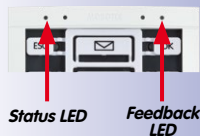
5. Press the key button of the keypad insert; the feedback LED is flashing blue.



6. Now enter the **current** Super PIN and press the **OK** button. The feedback LED of the module lights up blue.



7. Enter the **new** Super PIN and press the **OK** button. The feedback LED lights up blue.



LED Patterns

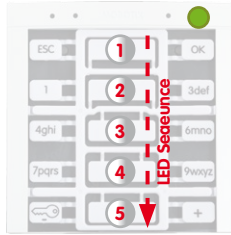
	Off
	Lights up
	Blinking
	Flashing



- Again enter the new Super PIN and press the **OK** button.



The LEDs light up in a sequence to confirm that the Super PIN has been changed and the feedback LED of the module briefly lights up green.



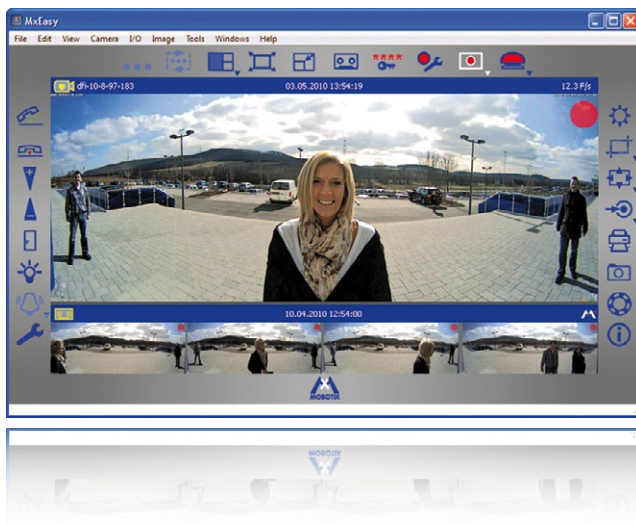
- Disconnect the power supply of the door station, remove the keypad insert and slide the bell buttons back into the module (see *Section 2.3.3, «Inserting the Function/Bell Buttons»*).



5 SYSTEM EXPANSION WITH MXEASY

This chapter provides an overview of the extended functions offered by your Door Station when used in conjunction with MOBOTIX video software MxEasy. For detailed information, please refer to the MxEasy user manual, which can be downloaded as a PDF free of charge from www.mobotix.com in the **Support > Manuals** section.

The current version of MxEasy is also available to download from the MOBOTIX website (www.mobotix.com under **Support > Software Downloads > MxEasy**).



MxEasy: Completely
free of charge

Before you launch MxEasy for the first time, you should have set up the system for operation without a computer as described in *Chapter 2* of this manual. In general, this is always possible when a DHCP server is in use in the network (T25-CamCore camera module or external server). Then follow the descriptions in *Section 5.1*, «*Setting Up Computers as T25 Remote Stations*».

Only in networks without a DHCP server (with static IP addresses) is it not possible to set up the system for operation without a computer. In this case, the system is set up for operation and Auto Configuration launched using MxEasy; only the Super PIN and the transponder cards have to be entered or set up using the KeypadRFID. See *Section 5.2* for a description of how to set up a T25 for operation in a network with a static IP address.

Global Connectivity Between Door Station and MxEasy

The Door Station can be accessed and operated over the Internet by assigning a DynDNS name. Live two-way communication over the intercom or opening the door is therefore possible from anywhere in the world where Internet access is available. If the remote station (e.g., a laptop) is also registered with a DynDNS service, a connection with MxEasy is automatically established when someone calls at the door. System setup is described in *Section 5.3, «Setting Up Global Connectivity Between MxEasy and Door Station».*



When accessing the Internet (wherever you are in the world) make sure the connection is sufficiently secure (encrypted)

Mobile T25 Remote Station: MOBOTIX App for iPad, iPhone and iPod touch

The MOBOTIX App serves as a powerful mobile remote station for all T25 Door Stations and newer MOBOTIX camera models. The MOBOTIX App is available in the App Store and can be used both in the local Wifi and while you are out in the mobile network.

The app is the perfect mobile T25 remote station:

- Two-way communication intercom
- Live camera images
- Alarms
- Event player
- and much more

Note

After the first successful use, the T25 Door Station **with KeypadRFID** will have been given the following access data during Auto Configuration:

- **User name:** admin
- **Password:** <Super PIN>

This data is needed if you are using a computer with MxEasy as the remote station or would like to directly access the software integrated in the T25 camera module via a Web browser (see www.mobotix.com > **Support** > **Manuals** > **Camera Software Manual**).

For Door Stations **without KeypadRFID** it is not necessary to enter an individual Super PIN during Auto Configuration. Unless the password is changed (urgently recommended!) – e.g., by video phone, see *Section 2.3.3* – the default password assigned at the factory meinsm continues to apply (user name remains: admin).

This access data protects the T25-CamCore, door camera and control unit for the entire Door Station against unauthorized access

5.1 Setting Up Computers as T25 Remote Stations

Apart from a Grandstream GXV3140 video phone, any computer (available in the network) can be used as a T25 remote station if MxEasy is installed on it. You can use this handy video software to manage and operate up to 16 MOBOTIX cameras and/or Door Stations easily and conveniently.

The MOBOTIX program can run in the background on a computer or touchpad with a standard operating system (Windows or OS X) and pops up automatically when someone rings the doorbell. Using the computer's microphone and speakers as a two-way communication intercom (full duplex), you can speak to visitors and you can open the door or switch on the light by clicking on the corresponding buttons in the software. MxEasy also makes it easy to listen to voice mailbox messages or search through all of your camera recordings.

5.1.1 System Requirements

To get the best out of the T25 with MxEasy as a computer remote station you need the following equipment:

- Computer with a current operating system (Windows XP SP3 or higher, Mac OS X 10.6 or higher). The processor must have a speed of at least 2 GHz and 1 GB RAM must be available. Macintosh computers with PowerPC architecture are not supported.
- Monitor with a minimum resolution of 1280 x 1024 pixels to be able to properly use the full-screen display of one or more cameras.
- The computer with MxEasy must have (like a Grandstream video phone) a network connection to the Door Station (e.g., via switch/WLAN). For the connection options available to you in this respect, see *Section 2.2, «Remote Stations and Network Connection»*, in the *T25 System Manual Part 1*. The **MxEasy manual** can be downloaded **free of charge** from www.mobotix.com in the **Support > Manuals** section.
- The T25 system was set up for operation using Auto Configuration (as described in the second section of this manual).

5.1.2 Downloading and Installing MxEasy

If you have not already done so, register as a new user through the MOBOTIX website and log on. It is free to register, download and use MxEasy. As a registered user, you have access to the entire range of MOBOTIX software and you can choose to keep yourself up-to-date with the latest product developments through our newsletter.

The convenient video management software MxEasy is available to download as a Windows or Apple version here:

www.mobotix.com > **Support** > **Software Downloads** > **MxEasy**



Windows

Download the file `MxEasy_*_Setup.exe` (release: MxEasy Windows), and save it on your computer. Run the file for automatic installation (`MxEasy_*_Setup.exe`), and follow the instructions in the installation wizard. Once the installation is complete, double-click on the desktop shortcut to launch the application.

Apple Mac OS X

Download the file `MxEasy*.mpkg.zip` from the MOBOTIX website (release: MxEasy Macintosh), and save it on your computer. Unpack the file by double-clicking on it. Run the file for automatic installation `MxEasy*.mpkg`, and follow the instructions in the installation wizard. Once the installation is complete, double-click on the application in the Programs folder to launch it.



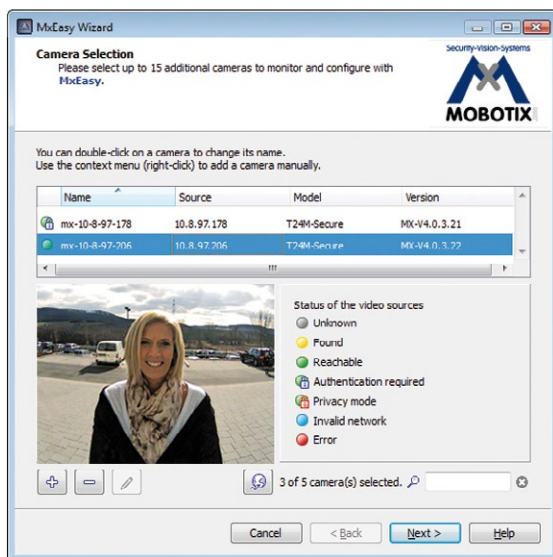
Note

If you have received an installation medium (CD, DVD, USB stick), you can launch the corresponding installation file directly from the storage device.

5.1.3 Connecting a Door Station Using the MxEasy Wizard

Step 1: Select Door Station

When you start MxEasy for the first time on a computer, the MxEasy Wizard automatically begins to search for MOBOTIX cameras and Door Stations with integrated camera modules, and displays all devices found in a list.



A Door Station already set up for operation without a computer, which is in the local network, is shown with the 'Green dot with lock' icon. This means that the Door Station can, in principle, be accessed (green), but it is protected by a password (lock). This password is (normally) the Super PIN that was assigned to this T25 when the system had been set up for operation (see *Section 2.2.1, «Entering the Super PIN at a KeypadRFID Module», Section 2.3.1, «Entering the Super PIN at a BellRFID Module» or Section 2.4.3, «Changing the Super PIN at the Video Phone»*).

Step 2: Enable Access to Door Station

Right-click on the Door Station (or the T25-CamCore camera module) and enter the currently valid data in the **User and password** window (see note at beginning of *Chapter 5*):

- **User name:** admin
- **Password:** <Super PIN>

After the data is entered correctly and confirmed the status display changes to a green dot without a lock. The **Select Integration with MxEasy** window opens.

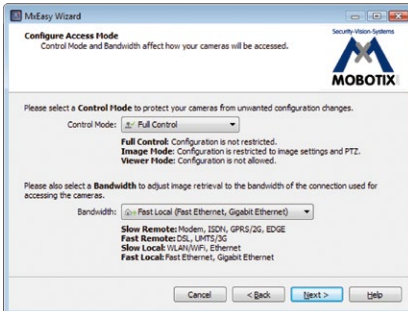
Step 3: Select Integration With MxEasy

Because the T25 was already auto-configured successfully (by pressing the lower button on the camera module during startup), you should keep the settings made automatically by the system during this process. Click on the center option field **Keep automatic configuration settings** and then **Continue**. The **Configure Access Mode** window opens.



Step 4: Configure Access Mode

The **Control Mode** can be used to prevent (accidental) configuration changes.



Setting the **Control Mode to Image Mode** for example, means that the type of recording cannot be changed.

Bandwidth determines how, in environments with connections of different speeds, frames are retrieved by the cameras and shown as live images or provided for searching. Choosing a Bandwidth enables you to determine the display quality of the camera image in MxEasy.

Click **Continue**. The **Change Camera Access** window opens.

More information on this can be found in the MxEasy manual at www.mobotix.com

Step 5: Skip the Camera Access Dialog

It is no longer necessary to enter a new password or user name because the Super PIN has already changed the default access data and the system is therefore securely encrypted. **Click Continue without completing the fields.** The next window, **Specify Door Station Equipment**, opens.



Step 6: Specify Door Station Equipment

The T25 includes a fixed bell button on the camera module and – if it exists for your system – one on the KeypadRFID. These bell buttons have the same functionality and have already been integrated into the system during Auto Configuration.

When using the BellRFID as access module, the module itself sets the number of bell buttons that are available. If an MX-232-IO-Box is connected, the system always has two bell buttons. In these cases, you cannot select the number of bell buttons.



Check if the system's **door sensors** have been activated and the **connection terminals** have been properly assigned in order to get the correct **door status displays** (door open/closed/locked) in MxEasy. For more information on the labels of the door sensor connections, see also *Section 2.4.4, «Setting the Door Status Display»*.

1. Select the number of bell buttons that actually available (e.g. third-party module with 1 to 4 bell buttons), without counting the bell button at the camera module (this selection is not available if a BellRFID module or an MX-232-IO-Box is attached).

2. Activate the desired checkboxes.

- **Door sensor** and/or **door lock sensor**:

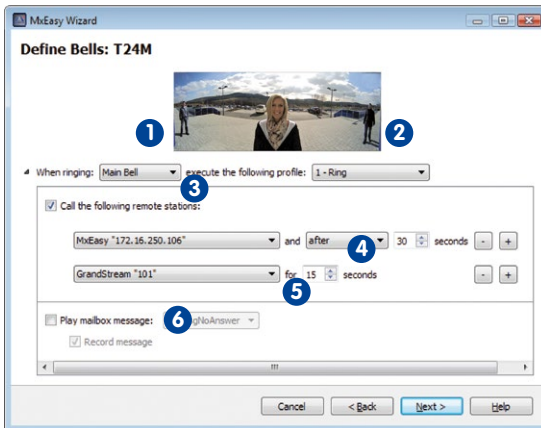
Specify the door sensors that are present in the system and which connection terminals have been connected. This is important in order to get the correct status displays in (door open/closed/locked) in MxEasy.

If you do not know, if and which door sensors are attached, test the different selections that are available and check them against the displayed status.

3. Click on **Next**. The **Define Bells** window opens.

Step 7: Define Bell Actions and Finish Wizard

This window allows selecting, **which actions are to be performed when the doorbell rings at the Door Station** (except on a Grandstream video phone). The addressees, which can be reached at the Door Station, are the equipment bell buttons and (optionally) the contact numbers set up with the blue user cards.



1. Select the **Addressee** for which an action profile is to be entered (bell button or contact number).
2. Specify how a **ringing** at the door station should be answered:
 - **No ringing** at the remote station (no phone ring)
 - Only with **ringing** (ring only)
 - With **ringing and mailbox** (ringing and visitors can leave messages if the homeowner does not answer)
 - With **mailbox only** (no ringing, visitors can leave messages immediately)
 - **Only with announcement** (visitors hears an announcement after ringing, but cannot leave a message)

3. If one of the **ringing and mailbox** or **ringing** profiles has been selected:
 - Select the remote station or add a new remote station that will play the ringing from the door station.
 - If you select **MxEasy as Remote Station**, you need to select or enter the IP address of the computer that is running MxEasy. For a Voice-Over-IP call, you need to set either a SIP phone number or the IP address of the VoIP phone that is to be called (depending on the configuration). The SIP number is displayed as **"*101"**. This is the name that had been specified for the Grandstream models on the SIP server. **"*101"** is then resolved to the actual IP address of the Grandstream phone.
 - Select how much time should elapse without the doorbell being answered before a message is played to the visitor.
 - Select the message that is played to the visitor.
 - Activate the **Record Message** checkbox, if the visitor should be able to leave a message.
4. If the **Announcement only** checkbox had been selected:
 - Select the message that is played to the visitor.
 - Activate the **Record Message** checkbox, if the visitor should be able to leave a message.
5. Click on **Next**. The door camera is reconfigured. The **Overview** window opens.

If everything has been configured, click on **Next**. The selected door camera is listed in the **Overview** window. Click on **Finish** to close the MxEasy Wizard.

The door station has been configured properly and MxEasy shows the live image of the door station camera. For more information on using MxEasy and on the other application settings (image optimization, recording, door station options, etc), please read the MxEasy User Manual (www.mobotix.com > **Support** > **Manuals**).

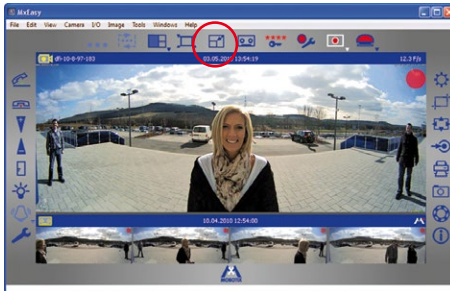
User Tip: The MxEasy Mini Viewer

If you use your computer primarily for other applications (such as Office programs, Internet, etc.) yet always want to remain informed about door activity without having to switch back and forth between program windows, then just open the Mini Viewer in MxEasy. The Mini Viewer is a smaller preview window with live camera images, important Door Station features and status display for doors and lights.



You can easily switch to the Mini Viewer by clicking on the appropriate **button in the center of the toolbar above the live image.**

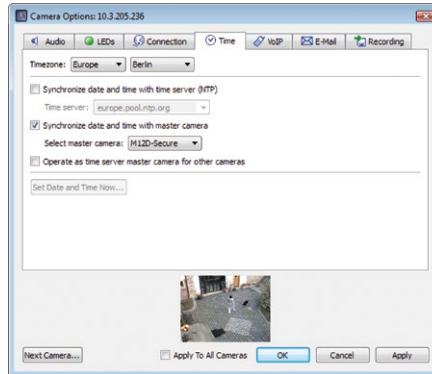
If someone rings the doorbell, a large doorbell icon is shown and the pre-configured sound generated through the computer's speakers. The two-way communication intercom function can be activated or deactivated using the telephone handset icons. The volume of the visitor (or the Door Station microphone) can be changed using the slider. An electronic door opener connected to the Door Station and/or a light can be activated by clicking on the corresponding icons.



5.1.4 Setting Date and Time

After you have completed the MxEasy Wizard, you should make sure that all integrated Door Stations, cameras and devices are running **in a synchronized manner**. You can do this by using a **time server** that synchronizes the system to a particular time.

MxEasy Camera
Options dialog box



1. Open the **Time** tab under the **Camera > Camera options** menu item.
2. Select the required **time zone** (time at the location of the T25). This allows the system to automatically switch between summer and winter time.
3. Activate the desired checkbox:
 - **Synchronize date and time with Internet time server (NTP)**
Select a time server from the list or enter the name of your preferred NTP time server. If the camera/Door Station does not automatically fetch its network data via DHCP, a valid DNS server must also be entered (Connection tab).
 - **Synchronize date and time with master camera/Door Station**
If there is no Internet connection and you have several MOBOTIX cameras or Door Stations simultaneously in one network, you should make one master camera/Door Station be the time server for all devices. This ensures that the system runs in a synchronized manner and that saved video sequences can be replayed in a synchronized format.
4. Activate the checkbox **Use as master time server camera for other cameras** to use the currently selected (door) camera as the time server.

5. If an NTP time server has not been entered and the camera/Door Station is not being used as a master time server camera, you can set the **camera time to the computer's clock**:
 - **Uncheck the synchronizing options** and click **Apply**.
 - The camera/Door Station is reconfigured and restarted.
 - Wait until the restart (or reboot) of the Door Station is complete. The time of the computer on which you are working right now will be displayed.
 - Click **Set Date and Time Now** to synchronize the camera's/Door Station's time with the computer's local time for the first time.
6. Click **OK** to confirm.

Note

The time display in the title bar of the main window will blink if the system time of an active camera (Live view) in the main window deviates from the system time of the computer by more than 15 seconds. In this case, check the computer to see if it is also synchronized with a time server. Try to set up the same time server for both the computer and the cameras/door stations.

5.2 Integrating the Door Station into a Network with Static IP Addresses

If there is no DHCP server in the network or this is not to be used, all network devices must have a static IP address in the same address range to be able to communicate with one another. This also applies to the T25 and its remote stations, which are to be newly integrated into the network (LAN – Local Area Network). You have to know the IP addresses and subnet mask currently in use on the network.

A computer that is already configured to work on the network is necessary for configuration. The MOBOTIX software MxEasy must be installed on this computer (free to download from www.mobotix.com > Support).

Note

For Steps 4 and 5 described here, which must be carried out with MxEasy, please also refer to the «*Integrating an IP Video Door Station*» section in the MxEasy manual (free to download from www.mobotix.com > Support > Manuals).

Configuration Comprises the Following Steps:

- Integrate T25 including remote stations into network
- Assign static IP addresses to video phones (on the video phone)
- Assign static IP address to operation computer (on computer)
- Assign static IP address to T25 (with MxEasy)
- Further configure T25 and initiate Auto Configuration (with MxEasy)
- Set up Super PIN and admin card (on KeypadRFID)

Step 1: Integrate T25 Including Remote Stations Into Network

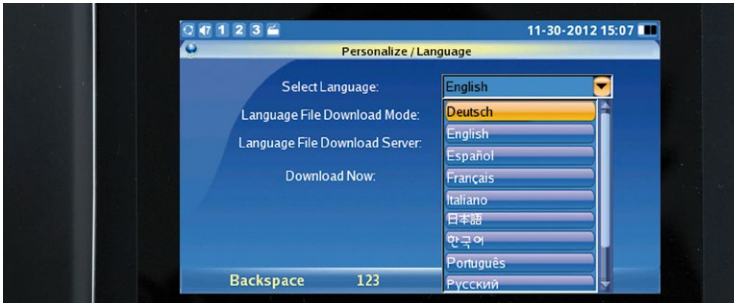
Connect (one or more) T25, the video phones being used and, if not already done, a computer with the router/switch into the network. Each T25 must have a (PoE) power supply.

Step 2: Assign Static IP Addresses to Video Phones (at the Video Phone)

Please note: The following settings refer to the menu of the Grandstream GXV3140 video phone. The settings must be made in the relevant menus for IP video phones from other manufacturers.

When first operating the **video phone**, we recommend configuring the desired **Menu language** on the display first:

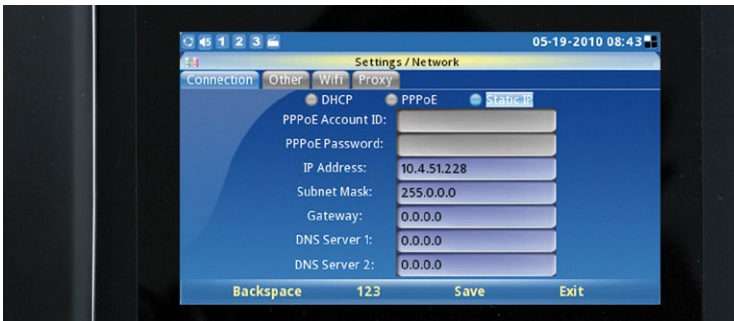
- **Menu > Personalize > Language > Select Language**



Next, change the configuration of each **Grandstream telephone** from the default DHCP settings to a user-defined **static IP address** appropriate for the existing LAN. For example, here, the address range is from 10.x.x.x (10.0.0.1 to 10.0.0.254) with the subnet mask 255.0.0.0.

- **Menu > Settings > Network**
- **Activate static IP**
- **Enter IP address** 10.0.0.10
- **Subnet mask** 255.0.0.0 > **Save**

Caution: Values specified are only placeholders or examples



Restart the Grandstream telephone:

- **Menu > Settings > Maintenance**
- **Restart > Select and activate restart**

The new static IP address of the Grandstream telephone (10.0.0.10) will now appear on its display and is ready for use.

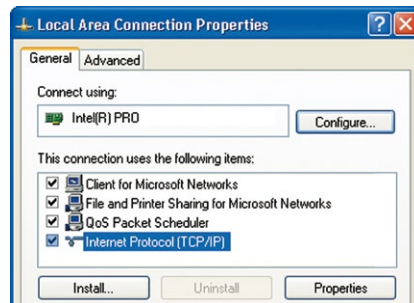
Step 3: Assign Static IP Address to Computer (at the Computer)

If a computer already integrated into the network is used to set up the T25, proceed directly to Step 4.

The MOBOTIX T25 and Grandstream telephones are set up for operation using a computer, the network parameters of which must be set up in the same IP address range. The computer's network parameters usually have to be changed for this purpose.

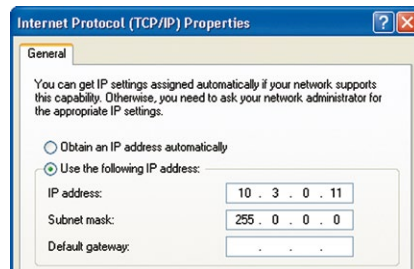
Windows

1. Open **Start > Settings > Control Panel > Network Connections**. Clicking **Properties** opens the dialog shown.



2. **Double-click Internet Protocol (TCP/IP)**. Select the option **Use the following IP address** under General and enter a static IP address (e.g. 10 . 3 . 0 . 11) with the subnet mask 255 . 0 . 0 . 0.

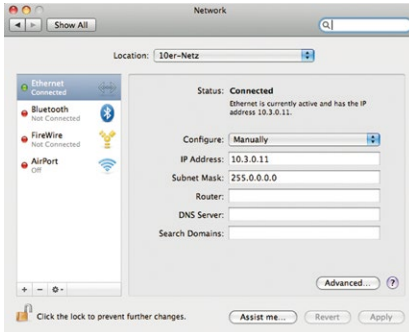
Caution: Values specified are only placeholders or examples



3. After closing all dialogs, the computer will now use the 10 . 0 . 0 . 20 IP address.

Mac OS X

1. Open **System Properties > Network**.

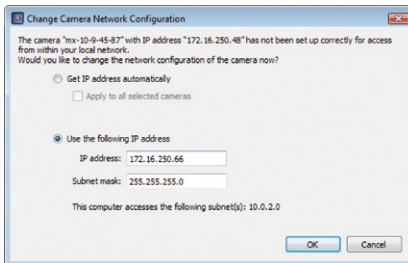


2. Select **Ethernet**. Select the option **Manual** under **Configuration** and enter a static IP address (e.g., 10.3.0.11) with the subnet mask 255.0.0.0.
3. After you have clicked **Apply**, the computer uses the IP address 10.0.0.20.

Step 4: Assign Static IP Address to T25 (See Also Section 2.3.2 of the MxEasy Manual)

Install MxEasy on a computer and start the program. The **MxEasy Wizard** opens (see Section 5.1.3, «Connecting a Door Station Using the MxEasy Wizard»):

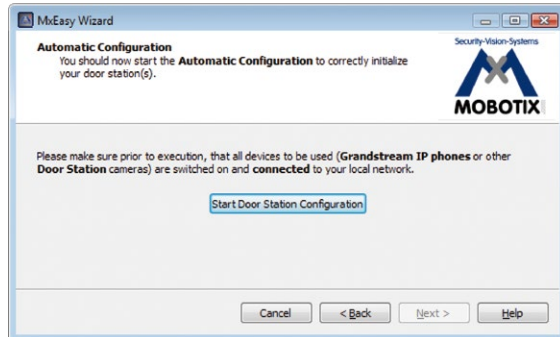
Select your T25 door camera. The **Network status icon** will probably be blue. This color indicates that even though the operation computer and the Door Station are in the same physical network, they are still in different IP address ranges and therefore cannot communicate with one another (yet). Click **Continue**. The **Network Configuration prompt** window opens. Click **OK** to confirm.



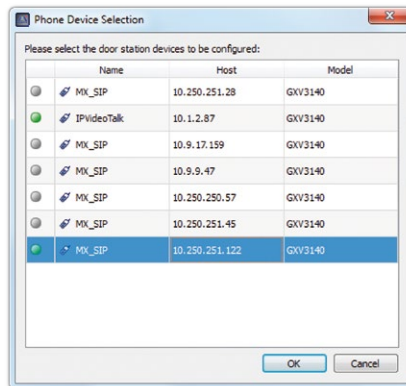
In the **Change Camera Network Configuration** dialog box that opens next, enter a static IP address appropriate for the LAN and a subnet mask for your Door Station under the activated **Use this IP address** option. Click **OK** to finish. If you have more than one T25, repeat the process for entering the IP address. The T25 is now reconfigured and the **Select Integration with MxEasy** window opens.

Step 5: Continue to Configure T25 (See Also Section 2.3.3 of the MxEasy Manual)

Proceed through the next steps of the MxEasy Wizard. For the settings in the **Select Integration** with MxEasy and **Configure Access Mode** windows, follow the description given above in Section 5.1.3, «Connecting a Door Station Using the MxEasy Wizard». Next, the **Start Automatic Configuration** windows opens.



1. Click on **Start Door Station Configuration**. The system searches for existing Grandstream IP phones and other door station cameras. If additional door station modules have been found, they will be displayed in the **Phone Device Selection** dialog. (A message will inform you if no additional modules have been found.) Click on **Next**.

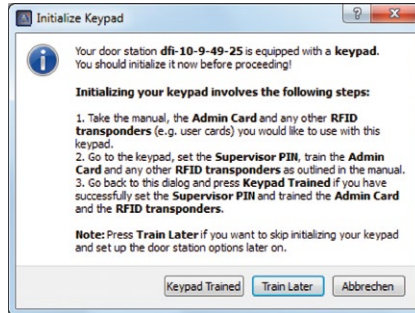


2. Select the door station modules you would like to include in the system. Click on **OK**. This will start the Automatic Configuration. Note that this may take several minutes.

Depending on which access module is connected, the **Initialize Keypad** or the **Initialize BellRFID** window opens:

- **Initialize Keypad:**

- Click on **Train Keypad**.
- Enter the Super PIN at the KeypadRFID module of the door station, train the admin card and the desired number of user cards (see *Section 2.2, «Step 2: Set Up the KeypadRFID Access Module»*).
- Next, click on **Keypad Trained**. The **Specify Door Station Equipment** window opens.



- **Initialize BellRFID:**

- Click on **Train BellRFID**.
- Enter the Super PIN at the BellRFID module of the door station and set the bell button layout (see BellRFID Quick Install, Installation and Initial Operation).
- Next, click on **BellRFID Trained**. The **Automatic Configuration** window opens once more. This runs the Automatic Configuration again, allowing you to correct a faulty entry, if required. Click on **Next**.



The **Specify Door Station Equipment** window opens. Proceed as outlined in *Section 5.1.3, step 6*.

5.3 Setting Up Global Connectivity Between MxEasy and Door Station

To be kept informed anywhere in the world of what is happening at the door back home, you can establish a connection over the Internet to your Door Station – which is also connected to the Internet and registered with a DynDNS service – using a computer installed with MxEasy. When the program is open (e.g., as Mini Viewer) and a connection is available, you can see live camera images with or without sound, you can speak with the visitor and you can operate the door lighting and the door opener remotely. And, of course, you can also use all the other functions offered by MxEasy.



MOBOTIX recommends purchasing **flat-rate** Internet access for the T25 and router; other access plans could result in high connection costs

Please note, however, that the quality of the two-way intercom connection and the live images depends on the capability of your Internet connection.

Technical Specifications: Registering the T25 With a DynDNS Service

MxEasy cannot automatically detect Door Stations that are located outside the local (WLAN) network; these must be added manually in the Camera List.

In most cases, a T25 or its camera module (T25-CamCore) is connected over the Internet with a changing IP address. DynDNS (dynamic domain name system) is the perfect way to access your system. In this way, the T25 is accessed via a self-assigned name that can no longer be changed, which was registered with a DynDNS provider. The integrated DynDNS client in your local router (e.g., Fritz!Box) transmits the new IP address to the DynDNS provider each time a change is made. The camera can therefore always be accessed with the same DynDNS name (e.g., `Fritz-Mueller.dyndns.org`), regardless of the current IP address.

You need a computer with Internet access and a router connected to the Internet to set up this service. The Door Station must also be connected to this router. **Proceed as described below (also see Section 4.8.3 of the MxEasy manual):**

Step 1: Registering a DynDNS Name

Register with a suitable DynDNS service (e.g., `dyndns.org`) and reserve a DynDNS name for the router, which you want to use for accessing the T25 (e.g., 'Fritz-Mueller' for your Fritz!Box). DynDNS providers typically provide several domains that come after the period after the DynDNS name. In our example, we chose 'dyndns.org'. The name used to access the door camera(s) therefore always begins with 'Fritz-Mueller.dyndns.org'. Keep the DynDNS access data (user name and password) that you are given in a safe place.

Step 2: Setting Up a DynDNS Client at the Router (e.g., Fritz!Box)

Open your router's user interface by entering its IP address or DNS name in the web browser (e.g., 'http://192.168.178.1' or 'http://fritz.box'). Open the configuration page for setting up the DynDNS client. Enter the DynDNS name that you registered with the DynDNS provider.

Step 3: Setting Up Port Forwarding

Open the configuration page for port forwarding in your router's user interface. Link a port to each local IP address for the Door Station(s) that should be accessible anywhere in the world:

e.g., Port 19801 -> 192.168.178.201 (router port and IP address for Door Station)

Step 4: Testing the DynDNS Configuration

Each T25 is equipped with integrated software, the interface for which can be called up as a website in a standard Web browser (e.g., Internet Explorer, Firefox). To do this, just enter the IP address or the DynDNS name for the T25 **in the address line of your Web browser** on a networked computer. You still need the current access data for the T25 (user name and password, see Note at the beginning of *Chapter 5*) to enable the website.

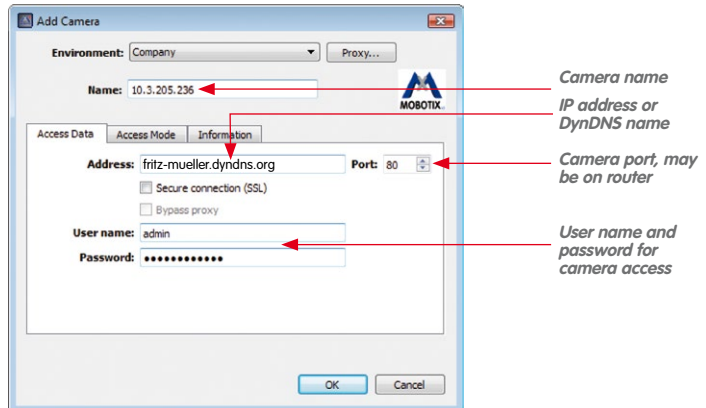
To test the DynDNS configuration, enter the DynDNS name and the port of the required T25 in your Web browser (example: `http://Fritz-Mueller.dyndns.org:19801`). You should now see the **T25 Web interface** and be prompted to enter the access data. Use the same procedure to test all of the other Door Stations/cameras that you have set up for port forwarding.



Step 5: Integrating Door Stations Over the Internet in MxEasy

Launch MxEasy as described in *Section 5.1*. You now have to manually add the T25 in MxEasy using your DynDNS name:

1. If this is not automatically displayed when the program starts, open the **Camera List** in MxEasy (e.g., under the menu item Camera >Add Cameras). Click on the **+** button to the lower left of the list. The **Add MOBOTIX Camera** window opens.



2. Enter the **DynDNS name for the router** in the **Address** field and the corresponding **Port** for the Door Station (as defined in the router).
Data from the example above:
 - Address: fritz-mueller.dydns.org
 - Port: 19801
3. Now enter the **user name and password for the Door Station**:
 - **User name:** admin
 - **Password:** <Super PIN>
4. Click **OK** to confirm and finish. If everything is set up correctly, the network status of the Door Station automatically switches to accessible (symbolized by a green dot without lock) and MxEasy displays a live preview image.

Step 6: Setting Up SSL Encryption

SSL encryption means that data sent to and from the cameras is always transmitted in an encrypted format. This technique makes the recording of data and spying on access data (nearly) impossible. To activate SSL encryption on the camera, proceed as follows:

1. Open the **Properties** window via the **Camera > Edit Cameras** menu.
2. Or: Open the Camera List via the **Camera > Show Cameras** menu. Open the shortcut menu for the desired camera. Click **Edit**. The **Properties** window opens.
3. Activate the checkbox **Use secure connections (SSL)** in the **Access data** tab.
4. Click **Apply** or **OK** to complete the changes on the camera.
5. Reboot your camera when you are prompted to do so.

The camera can now only be reached via an SSL-encrypted connection. You can also use the encrypted connection from a Web browser by entering the camera's address, as in the following example:

```
https://Fritz-Mueller.dyndns.org:19801
```

Now proceed as described above in *Section 5.1.3* from Step 3 onwards. You have now integrated a T25 into MxEasy via the Internet.

Please note: For a computer with MxEasy that is remotely connected to the T25 via the Internet, any **ringing on the door will only be signaled acoustically and optically** if the computer (and the T25) are registered with a DynDNS service with the host name and the port of its Internet router in MxEasy as the remote station. If this function (doorbell message) is also required while you are out for unknown ports (e.g., in the WLAN network of a hotel or hotspot), we recommend using the MOBOTIX App for iPhone, iPad and iPod touch, which has been developed specially for mobile use.

Notes

The IP addresses given here for cameras, routers, the ports and the DynDNS name 'Fritz-Mueller.dyndns.org' are only intended as examples. They should not be used **under any circumstances** in order to protect your system from tampering. Specify your own names and ports.

Access to the **password-protected T25 website** e.g., if you want to view live images or open the door, is also possible in the browser of mobile Internet devices. The **remote-controlled door opening function** is extremely practical if, for example, your T25 is not equipped with an RFID or PIN-controlled access module (KeypadRFID), but you do not have the door key with you at the moment.

Make sure that you have changed the default **Access data for the Door Station** (user name 'admin' and password 'meinsm') when using the system for the first time: User name remains admin, new secure password becomes the Super PIN for your system (also see the Note at the beginning of this chapter).

6 RESTORING THE SYSTEM

6.1 Error Messages and Rebooting

If any errors are encountered during the initial operation, they are announced as a numerical code via the door station's loudspeaker. The table below outlines possible reasons for errors and troubleshooting solutions. If none addresses your issues, please contact the MOBOTIX support team.

How to Reboot the System:

Disconnect the door station from the power supply for approx. 30 seconds (for example, by removing the network plug) and then repeat the operating steps you tried to carry out previously (e.g. initiate the initial setup process).

Error code	Error	Solution
1	The door station's internal battery is empty	Ensure the door station is charged continuously for at least one hour and then reboot the system
2	Auto Configuration is deactivated	Activate Auto Configuration (via video phone. See Section 2.4)
3	Internal error	Reboot system. If this does not resolve the issue, contact MOBOTIX support
4	Error during number entry (e.g., Super PIN) – number too short or too long	Repeat your entry
5	Processing error – card could not be read	Repeat your entry
6	Card is not an admin card	Use an admin card
8	Connection to card was interrupted – card could not be set up completely	Repeat your entry and hold the card up to the KeypadRFID longer
9 or higher	Communication error (for example, loose connection)	Check cabling. Reboot system or initiate the initial setup process again

6.2 Backing up and Restoring

MOBOTIX provides functions for you to store a backup of the door station's system configuration via a Grandstream video phone, as well as to restore the original settings in case the configuration has been accidentally changed.

6.2.1 Backing up the System

Follow the instructions outlined in *Section 2.5.3, «Saving the System Configuration»*.

6.2.2 Restoring the System

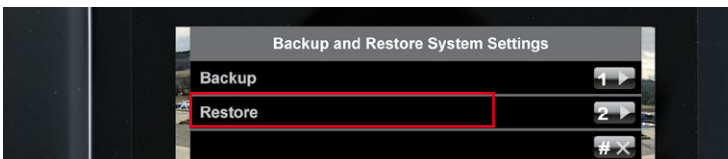
This function lets you restore the last version of the system configuration you backed up.

Proceed as Follows:

1. Using a Grandstream video phone, open the Admin Setup menu as described in *Section 2.4.2*. You will need the Super PIN for this.
2. Open the first page (1/2) of the Admin Setup menu and press 5 to select the "Backup and restore" menu item.



3. Now press 2 to restore the settings. The date and time of the last backup are shown on the display. Press the "*" button to confirm.



4. The system restore process is now running. Do not hang up the receiver until the blue start screen appears on the video phone. After this, the door station is operational again.

A special system restore procedure is required after exchanging modules. It is described in *Section 6.2.3* to *Section 6.2.8*.

6.2.3 Exchanging a KeypadRFID/BellRFID Module – with System Restore

You need to disconnect the door station's power supply before exchanging the access module (KeypadRFID or BellRFID). To restore the system after exchanging it, you will need an up-to-date backup of the system configuration.

Proceed as Follows:

1. Disconnect the door station from the power supply (for example, remove the network plug).
2. Remove the access module to be exchanged from the frame as described in the *T25-System Manual Part 1, Section 2.4.7, «Removing, Exchanging and Modifying Modules»*.
3. Exchange the access modules. Take care not to damage the cabling or mix up the connections. The connection diagrams are provided in the *T25-System Manual Part 1*.
4. Reconnect the power supply, wait until the system has booted and run a system restore via the video phone, as described in *Section 6.2.2, «Restoring the System»*. The door station is now ready for operation and can once again be used with the PINs and transponder cards set up for your system.



Contact your MOBOTIX support team to exchange a (used) access module and MX-DoorMaster that no longer have factory default condition (the devices will need to undergo a hardware reset)

6.2.4 Exchanging an MX-DoorMaster – with System Restore

You need to disconnect the door station's power supply before exchanging the MX-DoorMaster. To restore the system after exchanging it, you will need an up-to-date backup of the system configuration.



Proceed as Follows:

1. Disconnect the door station from the power supply (for example, remove the network plug).
2. Exchange the MX-DoorMaster. Take care not to damage the cabling or mix up the connections. The connection diagrams are provided in the *T25-System Manual Part 1*.
3. Reconnect the power supply, wait until the system has booted and run a system restore via the video phone, as described in *Section 6.2.2, «Restoring the System»*. The door station is now ready for operation and can once again be used with the PINs and transponder cards set up for your system.

Notes

After installation and initial setup, the batteries of the MX-DoorMaster should be charged continuously for the first 12 hours. This takes place automatically via the PoE-powered T25 door station using the MxBus two-wire cable.

During this time, the electrical door opening function should not be used (except for functional testing). This will maximize and extend the battery life of the high-quality NiMH batteries (industry standard) to several years at normal use.

When a battery has been completely drained, a functional test can only be carried out after the red LED has turned off (after approx. 15 minutes).

When replacing the batteries, always be sure to use original batteries. You can purchase these directly from MOBOTIX or your MOBOTIX partner.



6.2.5 Exchanging an Info Module

The door station remains operational despite the Info Module malfunctioning or being exchanged. Because of this, you do not need to run a system restore after exchanging it.



Proceed as Follows:

1. Disconnect the door station from the power supply (for example, remove the network plug).
2. Remove the defective Info Module from the module frame as described in the *T25-System Manual Part 1, Section 2.4.7, «Removing, Exchanging and Modifying Modules»*.
3. Exchange the Info Module. Take care not to damage the cabling or mix up the connections. The connection diagrams are provided in the *T25-System Manual Part 1*.
4. Power up the system again. After an automatic reboot, the door station is ready for operation again.

6.2.6 Exchanging Info Module Mx2wire+ Components

The T25's two-wire cabling set always consists of two devices: the outdoor station's Info Module Mx2wire+ and the Mx2wire+ indoor unit installed inside the building.

When you exchange them, the door station's power supply is disconnected automatically. The door station is automatically ready for operation again once the power supply has been reconnected. A system restore is not required.



Proceed as Follows:

1. Disconnect the door station and Info Module Mx2wire+ components from the power supply.
2. Remove the Info Module Mx2wire+ to be exchanged from the module frame as described in the *T25-System Manual Part 1, Section 2.4.7, «Removing, Exchanging and Modifying Modules»*.
3. Exchange the old Info Module and indoor unit with the new devices. Take care not to damage the cabling or mix up the connections. The connection diagrams are provided in the *T25-System Manual Part 1*.
4. Power up the system again. After an automatic reboot, the door station is ready for operation again.

Notes

The two Info Module Mx2wire+ units are matching pairs and preconfigured at the factory. Matched units share the same network ID (see labels on the back of the Info Module and on the indoor unit's circuit board). In case of a defect, both units must always be exchanged for a new Mx2wire+ pair that has been configured by MOBOTIX and shipped in its original packaging.

6.2.7 Exchanging the T25-CamCore Camera Module – with System Restore

To restore the previous system environment after a door camera has failed or been removed, contact your MOBOTIX dealer or the MOBOTIX support team. The contact details are provided on the MOBOTIX website (www.mobotix.com) in the **Support** section.



As a safeguard against unwanted manipulation, you cannot exchange the door camera yourself with a subsequent reboot or new startup of a protected system.

6.2.8 Exchanging or Adding a Video Phone

To restore a previous system configuration after exchanging or adding a Grandstream video phone, you need a computer on which MxEasy is installed and a network connection to the door station.



If you do not have such a computer, you can reset all the Grandstream video phones connected to the network and auto-configure them with a new initial setup. Note that in this case, you will have to set up all your PINs and transponder cards afresh.

If you have any questions about how to proceed with this, contact your MOBOTIX dealer or the MOBOTIX support team. The contact details are provided on the MOBOTIX website (www.mobotix.com) in the **Support** section.

7 ADDITIONAL NOTES

7.1 Weatherproofing and Care

T25 Outdoor Station Modules

Thanks to its robust, meticulously crafted design, the T25 outdoor station modules excel in terms of weather resistance and protection against dust and humidity. It does not require any further accessories to be mounted. As is certified by the outdoor station's compliance with protection class IP65 (-30 to +50°C/-22 to 122°F), it is fully dustproof and resistant against water jets.

The lens cover should be cleaned regularly in order to ensure a consistently high image quality. Use a soft, lint-free cotton cloth for this purpose. Use a mild, alcohol-free detergent without abrasive particles to clean the housing.

A lens cover can be purchased as an accessory from MOBOTIX. It ships with a special tool for removing and exchanging it.



MX-DoorMaster and Mx2wire+ Indoor Units

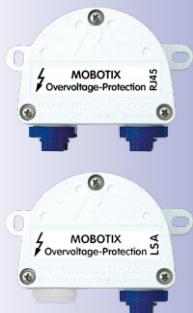
Although these devices have a robust exterior and are assembled to a very high standard, their usage should be restricted to protected interior settings (operating temperatures: Mx2wire+ indoor unit: -5 to +40°C/+23 to +104°F, MX-DoorMaster -5 to +40°C/+23 to +104°F).

Use a slightly moistened soft cloth for cleaning, making sure that no liquid enters the unit through the holes in the front panel. Never use aggressive cleaning agents or cleaning agents with abrasive particles (scouring agent). As the devices do not have any mechanical moving parts, regular servicing and maintenance is not required. MOBOTIX recommends, however, occasionally checking that the devices are functioning both reliably and properly.

7.2 Surge Protection

Electrical surges can be induced by other electrical appliances, improper wiring or also by external impact (for example, lightning strikes to phone or power lines). MOBOTIX devices are protected against the effects of small electrical surges by numerous measures. These measures, however, cannot prevent damage when stronger electrical surges occur. Particular care should be taken when installing the devices outdoors to ensure proper protection against lightning, as this also protects the building and the entire network infrastructure.

In order to avoid damage to MOBOTIX cameras from overvoltages, you should always install the MX-Overvoltage-Protection-Box. This competitively priced and weatherproof network connector provides reliable protection against overvoltages of up to 4 kV.



More information is available at an institution such as the International Electrotechnical Commission (IEC, www.iec.ch) or at a manufacturer of protection devices against lightning and electrical surges, such as Dehn (www.dehn.de).

7.3 AVC Video/H.264

Within the license of the AVC patent portfolio, this product is licensed solely for personal use by private users or for other non-commercial purposes to encode videos according to the AVC standard ("AVC Video"), and/or to decode AVC videos that were previously encoded by private users for personal/non-commercial purposes and/or that were purchased from a licensed video seller.

Beyond these terms of use, no other implied rights or licenses for other purposes are granted. Information on other purposes of use are available from MPEG, LLC (see www.mpeg1a.com).

7.4 Warranty and Repair Service

As legally required, MOBOTIX supplies a 24-month warranty and provides an original equipment repair department at its headquarters in Langmeil, Germany. This is available for all MOBOTIX customers.

When sending in a defective door station to MOBOTIX, please contact your point of sale where you purchased the product from, or an alternate MOBOTIX Distributor in your region, for an RMA number. Returned materials without an RMA number will NOT be accepted by the MOBOTIX Service Department.

7.5 Other Information

7.5.1 Safety Warnings

Risk of overheating when exposed to direct sunlight: When mounting a black, dark gray or amber-colored T25 IP Video Door Station in locations where the device is exposed to direct sunlight, the housing temperature can exceed the maximum allowed temperature limit. This can result in electronic failures and injuries especially when touching exterior metal parts. If the intended use of the device is at an (unprotected) outdoor location, you should only install white or silver-colored modules and frames. This product must not be installed within the reach of persons without the dome.

Electrical installation: Electrical systems and equipment may only be installed, modified and maintained by a qualified electrician or under the direction and supervision of a qualified electrician in accordance with the applicable electrical guidelines. Make sure to properly set up all electrical connections.

Electrical surges: MOBOTIX cameras are protected against the effects of small electrical surges by numerous measures. These measures, however, cannot prevent the camera from being damaged when stronger electrical surges occur. Special care should be taken



when installing the camera outside of buildings to ensure proper **protection against lightning**, since this also protects the building and the whole network infrastructure.



Max. power consumption of attached extension modules: The power consumption of all attached *MxBus modules* must **not exceed 2.5 W**. When attaching modules to the MxBus connector **and** the USB connector, the **power consumption of all attached modules must not exceed 3 W, if the camera is powered by PoE class 3**. If **PoE class 2** is used, **the power consumption of all attached modules must not exceed 1 W!**



Legal aspects of video and sound recording: You must comply with all data protection regulations for video and sound monitoring when using MOBOTIX products. Depending on national laws and the installation location of the T25, the recording of video and sound data may be subject to special documentation or it may be prohibited. All users of MOBOTIX products are therefore required to familiarize themselves with all valid regulations and comply with these laws. MOBOTIX AG is not liable for any illegal use of its products.



Network security: MOBOTIX products include all of the necessary configuration options for operation in Ethernet networks in compliance with data protection laws. The operator is responsible for the data protection concept across the entire system. The basic settings required to prevent misuse can be configured in the software and are password-protected. This prevents unauthorized parties from accessing these settings.



Additional instructions:

- This product must not be used in locations exposed to the dangers of explosion.
- Make sure that you are installing this product on a solid surface.

7.5.2 Declaration of Conformity

The products of MOBOTIX AG are certified according to the applicable directives of the E.U. and other countries. You can find the declarations of conformity of the products of MOBOTIX AG under www.mobotix.com, **Support > MX Media Library > Certificates > Declarations of Conformity**.

7.5.3 Disposal

Electrical and electronic products contain many reusable materials. For this reason, we would ask that you dispose of MOBOTIX products at the end of their service life in accordance with all legal requirements and regulations (or deposit these products at a municipal collection center). MOBOTIX products may not be disposed of with household waste! If the product contains a battery, please dispose of the battery separately (the corresponding product manuals contain specific directions if the product contains a battery).



7.5.4 Disclaimer

MOBOTIX AG does not assume any liability for damage that is the result of improper use of its products or failure to comply with the operating manuals or the applicable rules and regulations. Our **General Terms and Conditions** apply. You can download the current version at www.mobotix.com (using the COS link at the bottom of each page)





To demonstrate our confidence in the quality of our products, MOBOTIX cameras have been used to capture all images that appear in this manual.

Manufacturer

MOBOTIX AG
Kaiserstrasse
67722 Langmeil
Germany

Phone: +49 6302 9816-103

Fax: +49 6302 9816-190

www.mobotix.com

sales@mobotix.com

Registration Office: Kaiserslautern Local Court

Registration Number: HRB 3724

Tax Office: Worms-Kirchheimbolanden, Germany

Tax Code: 44/676/0700/4

VAT ID: DE202203501

You can find the latest version of this and other documents (e.g., declarations of conformity) at www.mobotix.com in the **Support** section.



Technical specifications subject to change without notice!



Part 1: System Overview and Installation
Installation and Cabling
(for the Installer)

Part 2: Start-Up and Configuration
Software and Network
(for the **System Administrator**)


 5 MP
Sensor


 MxLEO


 vPTZ


 MxBus


 USB


 +50°
-30°


 IP65


Innovations - Made in Germany

The German company MOBOTIX AG is known as the leading pioneer in network camera technology and its decentralized concept has made high-resolution video systems cost-efficient.

MOBOTIXAG • D-67722 Langmeil • Phone: +49-6302-9816-103 • Fax: +49-6302-9816-190 • sales@mobotix.com