ABUS
Security Tech Germany

TECTIQ

System Manual

abus.com

Thank you for choosing an access system from ABUS Security Center. ABUS TECTIQ makes an important contribution to securing your property and ensures that only authorised persons can enter your secure areas.

About this manual

This manual contains all the information you need to use ABUS TECTIQ. The first part is aimed at the individual user groups of the system and provides a clear overview of all relevant applications. The second part describes the functions of the TECTIQ Access Manager software in detail.

Who is this handbook intended for

User – You are authorised to access a building with a TECTIQ access control system. You have received a TECTIQ locking medium and have been familiarised with the functions of the locking media by the operator of the TECTIQ access control system. You have been informed when and to which entrances you are granted access to the property. In the chapter **TECTIQ – for users**, you will find all the information you need about your locking media and the steps you need to take to use them on the door components. If you have any further questions, please contact the administrator of the TECTIQ access control system or your supervisor.

Administrators – You are the operator of a TECTIQ access control system or responsible for managing the door components and locking media in a TECTIQ access control system. This manual provides detailed information on the structure of the access control system, the TECTIQ control, locking media and door components, as well as other system media that will assist you in setting up, managing and customising access authorisations. In the chapter **TECTIQ – For administrators**, you can read how to use the TECTIQ Access Manager to add new groups of persons and individuals, grant or change locking permissions, and manage locking media. This will make it easier for you to get started with the TECTIQ Access Manager in your daily work.

Installer – As a service technician, planner or ABUS specialist installer, you are familiar with the installation of ABUS access control systems. You are familiar with our installation instructions for the components of the TECTIQ access control system. This manual summarises all the steps required to install the TECTIQ access control system and operate the TECTIQ Access Manager. The chapter **TECTIQ for installers** provides information on all steps required for commissioning, initial setup and handover of the TECTIQ access control system to the operator, as well as on system maintenance and support.

The **reference manual** explains the system structure, all functions, technical details, performance data and signals. You will also find information on system expansion and scalability.

Further information is available at abus.com or – for specialist dealers and installers – in the partner portal at www.partner-asc.abus.com.

Legal information

The information in this manual has been compiled to the best of our knowledge and is regularly reviewed and updated. Keep the manual and operating instructions for the products used in a safe place for the entire service life of the system.
Observe the information and instructions in the TECTIQ documentation. ABUS accepts no liability for damage resulting from incorrect installation, commissioning or other misuse. Responsibility for the operation of the locking system after installation and commissioning lies with the system operator, main user or owner of the building. Please observe our warranty conditions – online or in the TECTIQ product instructions.
Trademarks and property rights of third parties are the property of their respective owners and are recognised.

Customer Support

Dealers/installers: If you have any questions, please contact our technical support hotline.
End users: Please contact your installer with any questions. A trained ABUS installer in your area will be happy to advise you. You can find a list of ABUS dealers/installers in your region here:
https://www.abus.com/int/Dealer-map

ABUS TECTIQ

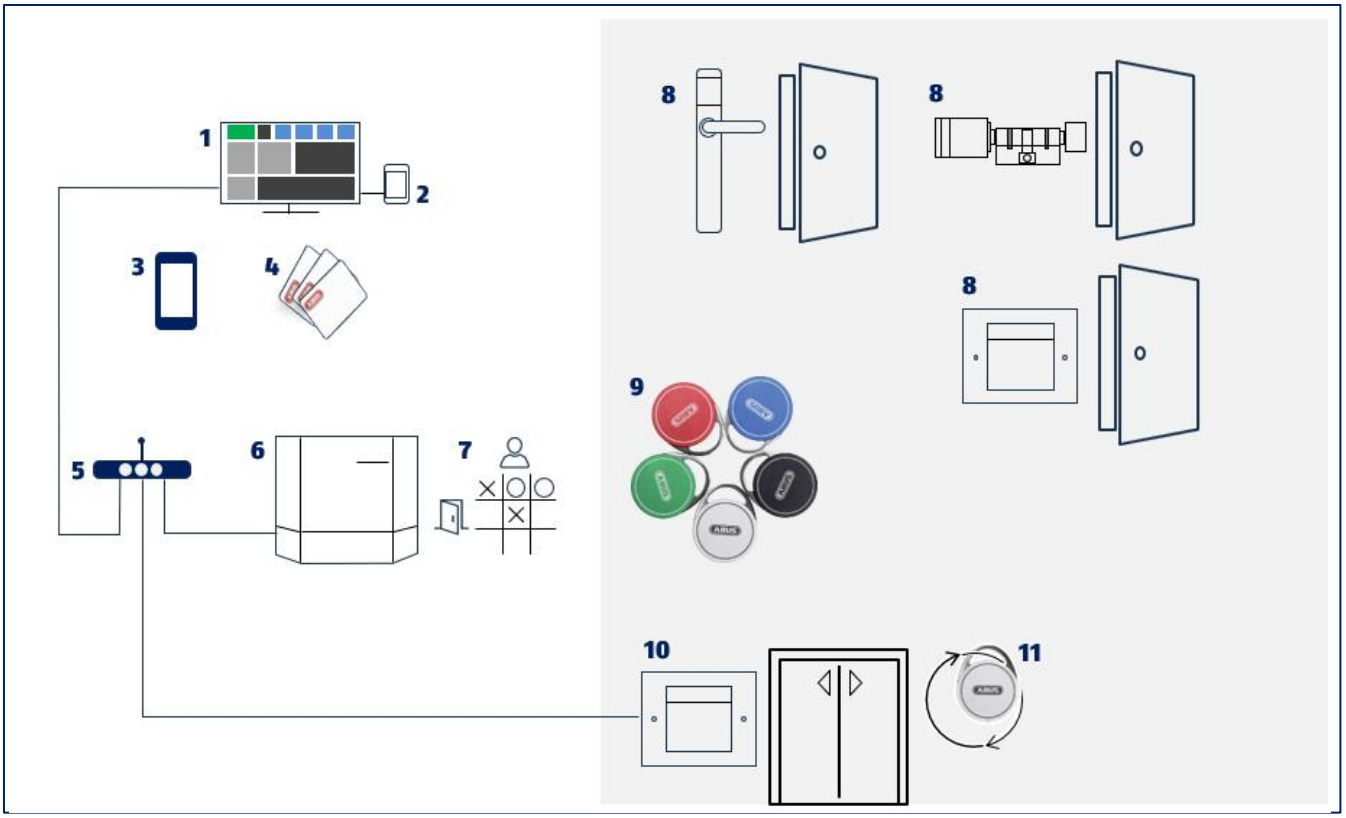
TECTIQ in a nutshell.

1. Introduction

Content

1.1. About ABUS TECTIQ

ABUS TECTIQ is the new standard among ABUS access control systems. Developed and manufactured in Germany, TECTIQ offers high-quality door components for a comprehensive, high-performance access control and security solution. TECTIQ is flexible, intuitive and easy to use and expand. TECTIQ is the electronic locking and access control system for commercial and public buildings of almost any size.



1 Software TECTIQ Access Manager
2 USB desktop reader
3 Admin App
4 System media
5 IP router
6 TECTIQ Control
7 locking plan, Schedules
8 TECTIQ fitting, electronic cylinder, wall reader
9 locking media
10 TECTIQ Update Terminal
11 Validation and updating

1.2. Features and function

ABUS TECTIQ grants authorized persons access to the secured area using electronic locking media.

- ABUS TECTIQ works according to the **data-on-card** principle. The access authorisations are stored on the locking media. If access authorisations are changed, the locking media are updated. It is not necessary to update the door component.
- The door components **TECTIQ cylinder** and **TECTIQ fitting** work offline and do not require any cabling or a network or radio connection. They can therefore be used flexibly at any location with little effort.
- The period of validity of the access authorisation on the locking medium can be set in the **TECTIQ Access Manager**. The authorized person can update the validity of their locking medium at the next **TECTIQ Update Terminal** independently using the settings saved in the **TECTIQ Control.**
- In systems without a **TECTIQ Update Terminal**, the update is carried out using the **TECTIQ desktop reader** and a PC on which the **TECTIQ Access Manager** is installed.
- The **TECTIQ Update Terminal** can be used without a locking function. However, it can also be set up to control actuators (electric strikes, door drives, n separation system, etc.).
- Access authorisations are managed and updated with the **TECTIQ Control** and the **TECTIQ Access Manager** software. The operator always has an overview and can manage his system flexibly. Data is synchronized between the TECTIQ Access Manager, the control panel and the connected update terminals in real time.

1.3. Access authorisations

Access authorisations are issued in the following steps:

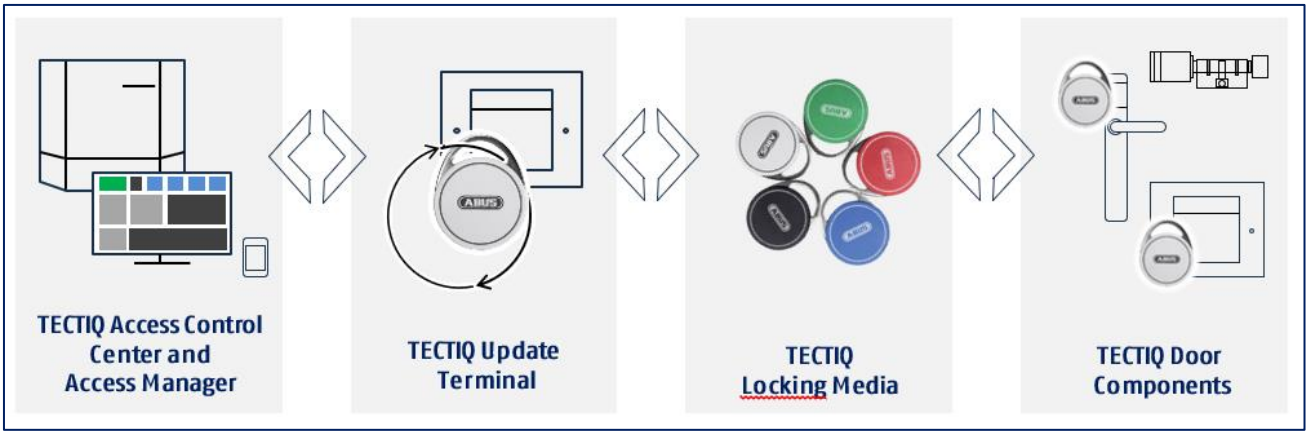
The creation of the person in the TECTIQ Access Manager: As soon as a person is entered in the system, they can be granted authorisations for access to secure areas. The person's validity can be limited by entering a validity period. Access authorisations are assigned to groups of persons or to individual persons. The user receives a personal locking medium to which the currently valid authorisations are transferred. The validity of the personal locking media is preset in the system settings and can be adjusted individually

Validation : Personal locking media must be updated regularly. Validation at a **TECTIQ Update Terminal** extends the validity of the locking media and centrally entered changes to authorisations are transferred to the locking media. locking media simply become invalid without updating the validity. Short validity periods increase security.

Schedules also organize access in terms of time, e.g. according to individual working hours, shift schedules or taking into account public holidays or vacation periods.

In systems without a **TECTIQ Update Terminal**, updating and validation is carried out using the **TECTIQ desktop reader** and **the TECTIQ Access Manager**.

1.4. TECTIQ system components



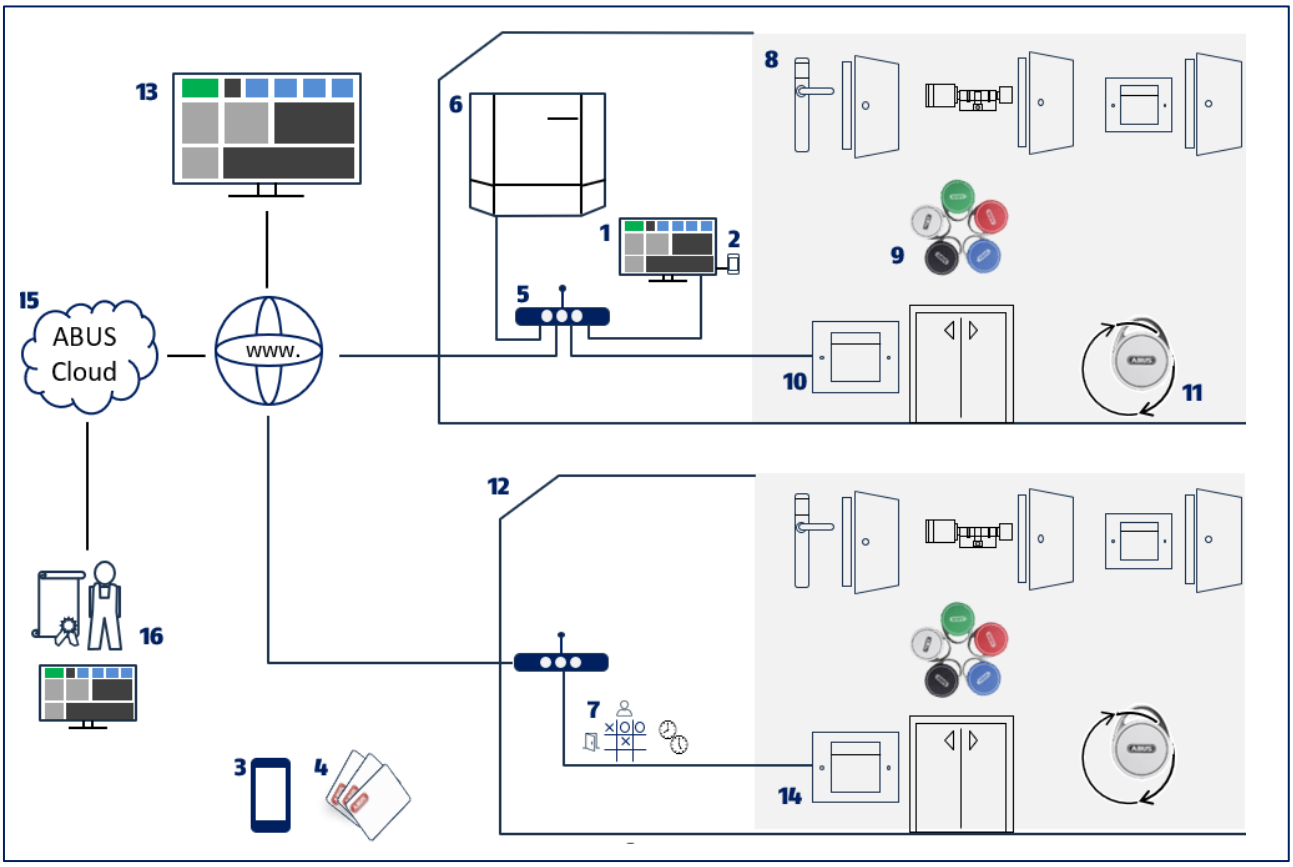
In a fully equipped TECTIQ system, the components are finely tuned to each other.

- The properties of the access control system are set in the **TECTIQ Control** - with the help of the **TECTIQ Access Manager**: This includes the locking plan with the access authorisations , the personal data and locking media as well as the data for doors and door components.
- The **TECTIQ Control** synchronizes in real time with the update terminal s in the system.
- The update terminals transfer the authorisations to the locking media and update them. At the same time, the locking media transfer log data from the system back to the control.
- The locking media store the access authorisations . This includes the individual authorisations for each individual door in the system, stored time schedules and blocking days as well as the validity for the locking medium. During operation, the door components write their log data back to the locking medium.
- The door components read the locking media when they are presented and check whether the access authorisations required for this door are present and valid. If the check is positive, authorized persons are granted access to the secured area.

Operation without a **TECTIQ Update Terminal** is possible at the customer's request with a reduced range of functions. In this case, access authorisations are granted for an unlimited period or updates and validation are carried out using a **TECTIQ desktop reader** at an administrator's workstation. Please also refer to our notes in section 1.7.

1.5. Scalable - cross-location access management, remote access and online service

TECTIQ offers a suitable solution for small, medium and large to very large access control systems. locking systems can also be managed across buildings and even locations via a network and Internet connection. Here too, access authorisations are updated upon entering the property. The operator has an overview of all relevant doors. The ABUS specialist retail partner or factory service can support you via remote access if required.



1 to 11 see above, section 1.1
12 Access control for additional locations
13 Online remote access with TECTIQ Access Manager (P2P)
14 Update terminal with online connection to the main system (P2P)
15 Access rights monitoring via the ABUS
16 Online service from ABUS specialist retail partners

1.6. Logs

The TECTIQ door components log their events and status messages, such as successful and denied access attempts, system messages and battery warnings, and transfer these to the locking media during each usage process or from the locking medium to the **TECTIQ Control** during the validation process. All events and resulting tasks (e.g. battery replacement required) are clearly displayed in the **TECTIQ Access Manager**. This makes it possible to react promptly to status and system messages and battery warnings.

1.7. Loss of locking medium

Please take care of your locking medium! It also grants unauthorised persons access to the secured areas during its validity. In the event of loss or theft, please report the incident immediately to your line manager and your administrator to arrange for the medium to be blocked without delay.

The TECTIQ access control system offers the highest possible level of protection to minimize potential damage. Once the

validity period has expired and the locking medium has been blocked in the **TECTIQ Control,** access to the secured areas is no longer granted. Unauthorised access attempts are logged in the event list.

A short validity period reduces the risk of unauthorised use. If the locking medium is found again, the authorisation must be renewed in any case.

For additional security, the locking medium is blocked in the system by adding it to the blacklist using the blacklist card. The blocking list is stored locally in each door component. If a locking medium is on the door component's blacklist, the door component will reject the locking medium even if it is valid indefinitely. This prevents unauthorised access through misuse of third-party locking media.

1.8. Data security

A well-planned and installed TECTIQ locking system does not let unauthorised persons into your property and does not leave any sensitive data to chance. That's where we come in:

- Encrypted data on the locking and transponder media
  TECTIQ uses the highly secure encryption method MIFARE® DESFIRE®. It guarantees maximum protection against tampering or copying attempts.

- Protected data exclusively in the **TECTIQ Control**
  All sensitive data is stored in the **TECTIQ Control.** You can display and edit the data using the **TECTIQ Access Manager**. The data required for access authorisation is transferred to the update terminals in real time. Saved backups are encrypted and only accessible in connection with the specific system.

- Highly secure peer-to-peer connections (P2P)
  Connections between the **TECTIQ Control** and the PC with the **TECTIQ Access Manager** do not use VPN or web server services and communicate with each other via an encrypted protocol. This minimizes the risk of tampering attempts.

- Strong password protection in the network and in the **TECTIQ Control.**
  Current network technologies with secure passwords demand a high level of computing power from potential attackers. A good password can only be overcome after many years - if you change your passwords regularly, your protection is as good as perfect.

- The correct network configuration in your Internet router
  Activate the highest possible level of protection in your network router and observe the usual security measures, such as those recommended by the German Federal Office for Information Security (bsi.bund.de).

2. TECTIQ - For users

You are a user of a building with an ABUS TECTIQ access control system. You have received your electronic locking medium and have been instructed in the locking system by your line manager or the administrator. You know your access authorisations and know when you are granted access to the secured area.

As soon as you present your locking media in front of a door component, the door component is released for you. If not, you will receive visual feedback. Read all about the important operating steps for you at.

Store the locking medium carefully.

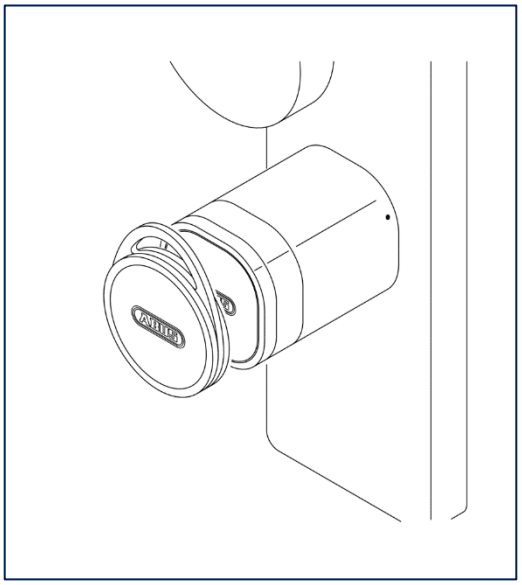
Contents

2.1. Introduction to the locking system - what you need to know

You have been informed of the following points by your line manager or the responsible employee:

- For which doors - and in which direction, if applicable - do you have access authorisations ?
- On which days do you have access and at what times?
- When do you have no access?
- Which functions can you use with your locking medium?
- How do you use your locking medium on which door?
- How and how often do you update your locking medium?
- Where are the update terminals where you can update your locking medium?
- Where can you update your locking media if no update terminals are available?
- Who do you turn to if you have a problem?

2.2. Enter the secured area



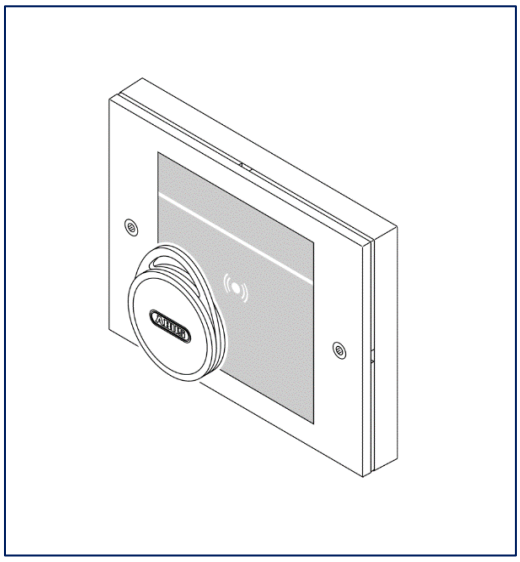
▷ Present your locking medium on the cylinder knob, fitting or wall reader.

→ The door function is enabled:
The locking cylinder engages the locking function so that you can open or lock the door by turning the cylinder.
The fitting releases the door handle.
The wall reader opens the door or releases its opening.

If:

- the door function is not enabled and the LED flashes red→ Update your access authorisation.
- a door does not open even after updating
  → Inform your supervisor or administrator.
- the fitting or cylinder reacts with a delay
  → Battery is low. Inform your administrator that the battery should be replaced as soon as possible.

2.3. Update access authorisations



The access authorisations stored on your locking medium can change and are only valid for a short time to protect against unauthorised use. You can transfer current access authorisations to your locking medium at any time.

▷ Present your locking medium at the update terminal.

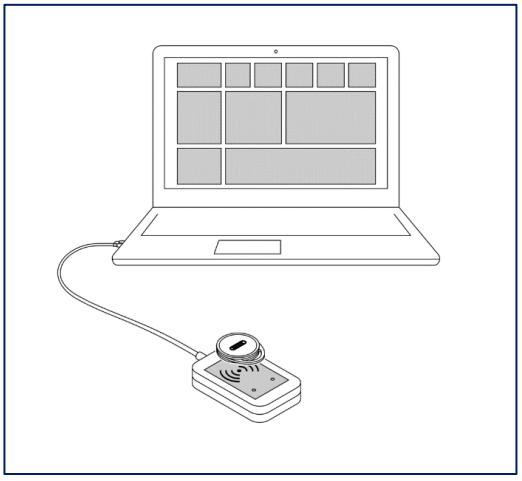
→ You will receive feedback if the transfer was successful:
LED lights up green, terminal beeps (1 s)

If the update terminal is also set up as a door component, the connected door is opened or released.

If:

- the LED flashes red and the terminal beeps twice briefly
  → Update has failed
- Inform your administrator and have your authorisation changed.

2.4. Amend access authorisations



Your workplace has moved or you have new responsibilities or the period of your access authorisation does not match your tasks.

▷ Contact your line manager or administrator to obtain new authorisations in the system.

▷ Then update your personal locking medium at the update terminal or via the TECTIQ desktop reader.

2.5. Have access authorisations blocked

Important! Lost locking media whose location is not reliably known are a risk for your company. Have the lost locking media blocked as soon as possible.

- Report the loss immediately to your line manager or administrator. They will place the locking media on the blacklist and block the locking media permanently. It can no longer be updated.
- Have a new locking medium issued to you.

2.6. LED signals

TECTIQ door components signal their status by means of an LED signal after actuation:

	At door: Access granted On update terminal: Access rights have been updated
 (0.1 s each)	Access denied locking medium expired or no authorisation for the door
 (0,1 s)  (0,5 s)	Access granted, update of the locking medium on the update terminal failed
 (0.1 s each)  (0,5 s)	Access denied, no authorisation, update of the locking medium on the update terminal
	Battery warning, access granted
	Incorrect or foreign locking medium / error
	General error
 (0.3 s each)	Hardware error
 ...	Terminal is offline; no connection to the Control
	System malfunction; no access

3. TECTIQ - For administrators

You are the operator of a TECTIQ access control system or are responsible for the secure operation of a TECTIQ access control system.

With the **TECTIQ Access Manager**, you can manage access authorisations , time schedules, locking media and system media and prepare the programming of door components. The **TECTIQ Control** ensures the real-time provision of necessary data at the update terminals and stores all entered data, system data and system statuses centrally. On the dashboard you will find an event list and a task list generated from the available data.

This section provides you with step-by-step instructions for regular tasks, such as

- the creation of groups of persons and persons,
- the creation of locking plans for the management of access authorisations ,
- setting up and managing personal locking media for users,
- the setup and management of system media,
- the programming of the door components and
- the creation of schedules.

You will also find out which steps are necessary

- if a locking medium has been lost or stolen,
- if a user's tasks change and new access authorisations need to be assigned,
- if personal working hours have changed and schedules need to be updated,
- when persons leave the company,
- if batteries in door components need to be replaced or
- a door component or a terminal reports an error.

Important! Keep access data for the **TECTIQ Access Manager** under lock and key. Coordinate with those responsible when creating new authorisations . Inform your superiors if you are unsure. If you have any technical questions, contact your ABUS specialist installer.

Contents

3.1. Handling locking media and system media

Please keep locking and system media in a secure place! If they fall into the wrong hands, grant unauthorised users access to the secured areas while they are valid.

Observe the following basic rules:

• Always keep system media (e.g. parameter card) under lock and key! Only use them when expressly required!
• Only enter locking media with active access rights in the locking system if you assign them to persons and hand them over to them!
• In particular, keep a programmed emergency opening transponder under lock and key, e.g. in the key depot!
• Do not create locking media with active access authorisations "in stock"!
• Block a locking medium or system medium in the event of loss or the possibility of unauthorised access! Access attempts with blocked locking media are logged.
• If a locking medium is to be deleted, you must present it to the reader!

Special applications may require exceptions to these rules. In this case, document the use of the locking and system media. Your ABUS specialist dealer will be happy to answer any questions you may have.

3.2. Connect TECTIQ Control with TECTIQ Access Manager

Prerequisites:

- **TECTIQ Access Manager** is installed and set up.
- **TECTIQ Control** is available, set up and connected.

▷ Start the program.
▷ Log in with your ABUS account.
After logging in, the connection window opens.

TECTIQ Access Manager

If no ABUS account exists for the system, register with a new ABUS account. Your ABUS account must be stored in the TECTIQ Control by your ABUS specialist installer.

The available TECTIQ access control panels are displayed automatically. If your control panel is not displayed, add it manually using the IP address or Connect ID. You can obtain the IP address from your IT manager and the Connect ID from your ABUS dealer.

▷ Select the desired TECTIQ Control with a mouse click.
The "Security and data protection" window opens.

▷ Read the terms of use and agree to them.
▷ Read the privacy policy and agree.

▷ Click on the "Apply" button.
The TECTIQ Access Manager work window opens.

In the following sections you will find out in brief:

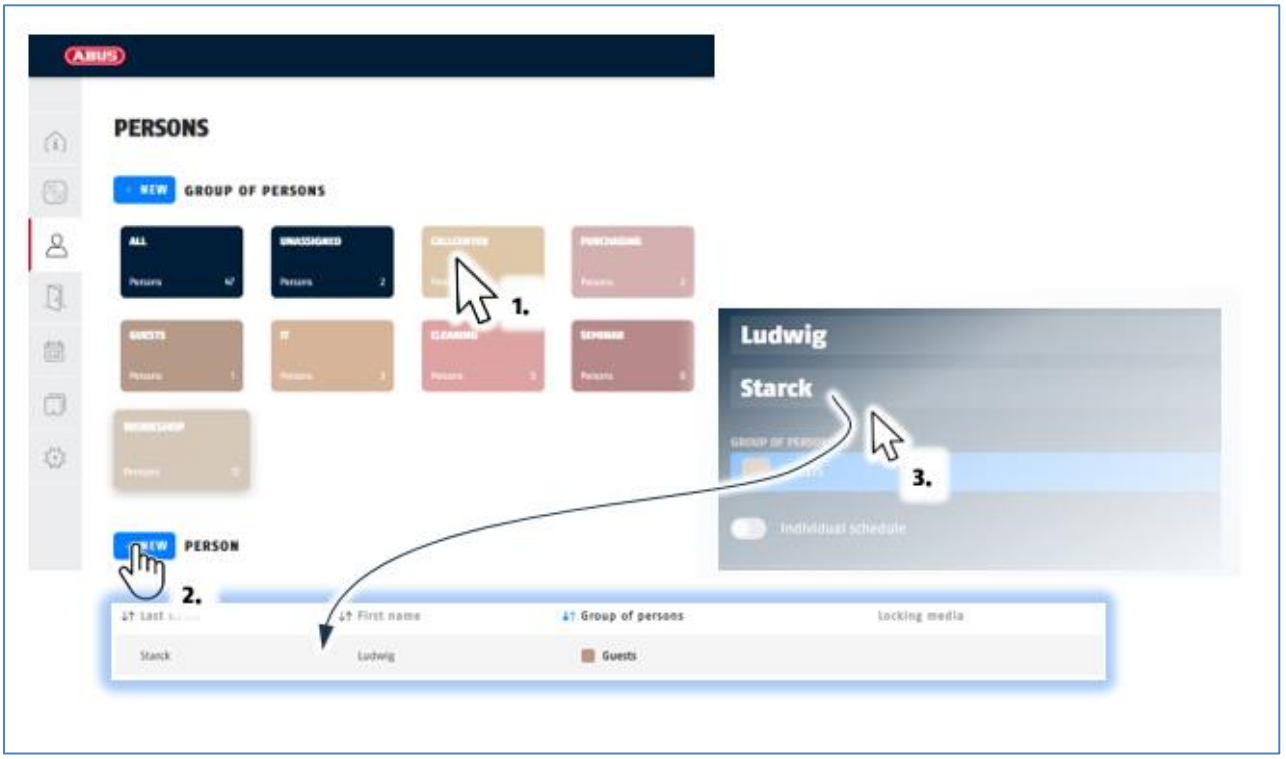
- how to create and manage persons and groups of persons,
- how to manage access authorisations ,
- how to manage personal locking media for users and system media,

- how to create and manage schedules.

For a detailed description of the structure of the TECTIQ Access Manager, its functionalities and operation, please refer to chapter 6 ff in the reference manual.

3.3. Add person

- ▷ Open the „Persons“ overview.
- ▷ Select the group of persons to which your new user should be added (1.).
- ▷ Click on the "+ NEW" button above the list of persons (2.).
- ▷ Enter the personal data (3.).



All access authorisations for the selected group of persons are automatically assigned to the new user. You can add or deselect individual authorisations for the person.

- ▷ Switch to the locking plan view and adjust the authorisations for doors or door groups individually.
- ▷ For individual access times: Select an existing schedule or create a new one.
- ▷ Set the validity of the locking medium. The default setting is the validity from the system configuration.
- ▷ Assign a locking medium to the person and program it. After programming, a receipt with all relevant data is available for printing under the menu item "More information". See sample in the appendix.
- ▷ Hand the person their locking medium and have them confirm receipt.
- ▷ Instruct the person in the system and inform them about their authorisations , times and the validation and updating of the personal locking medium.

3.4. Edit person

Edit person names

- ▷ Open the "Persons" overview.
- ▷ Select the person in the list of persons. If the person is selected in the list, the editing area switches to edit mode.
- ▷ Place the mouse pointer in the input fields and make your entries.

Change person group

Add a person to a (different) group of persons to assign them access rights to this group.

- ▷ Open the "Persons" overview.
- ▷ Select the person in the list of persons.
- ▷ Move the person from the list to the desired group of persons.

- or -

- ▷ Open the Person group list field and select the desired group.

- ▷ Complete the process by programming the locking medium.

Change access authorisation

If you want to assign a user the access authorisation of a group of persons, add them to this group (see→ Change group of persons).

Grant access authorisations to other doors or door groups in the "Persons" overview or in the locking plan overview.

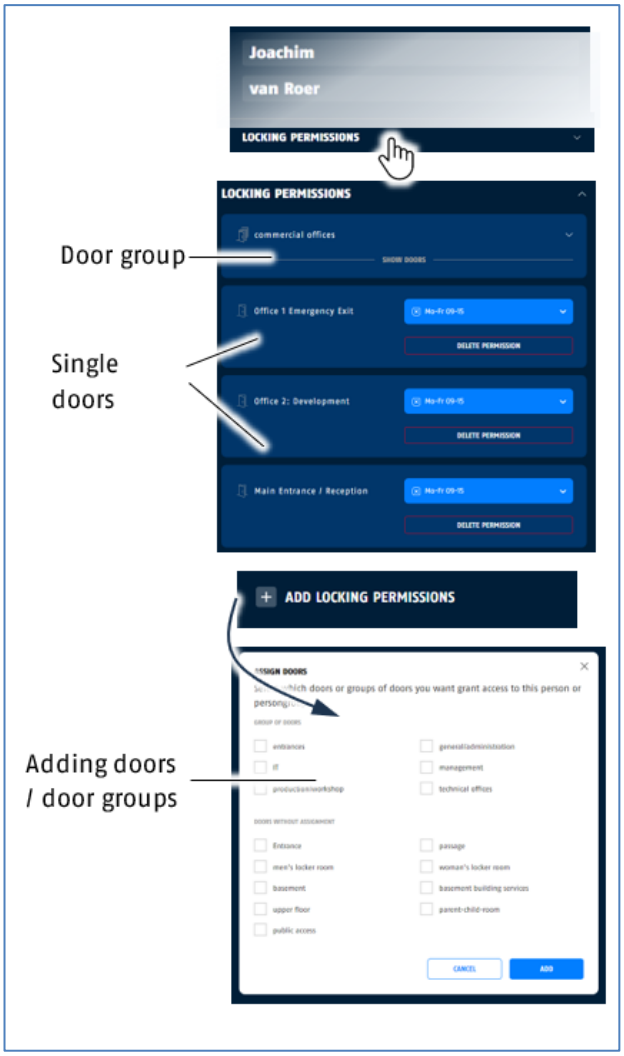
In the Persons view:

- Open the "Persons" overview.
- Select the person in the list of persons.
- Expand the "Permissions" list field.

Please note: Changes are applied immediately.

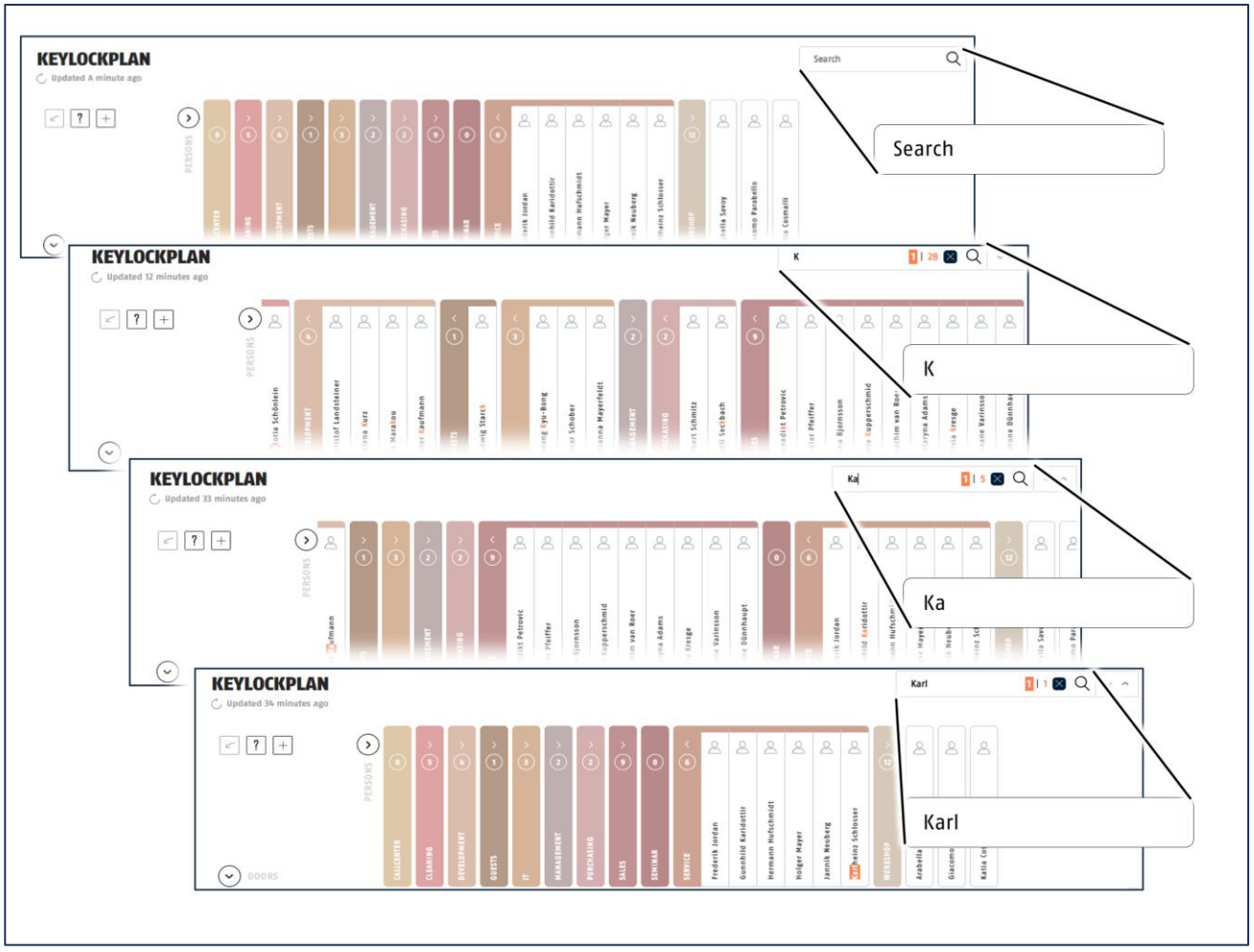
- Revoke an authorisation by pressing the "Delete authorisation" button for the door in question.

- Complete the process by programming the locking medium.



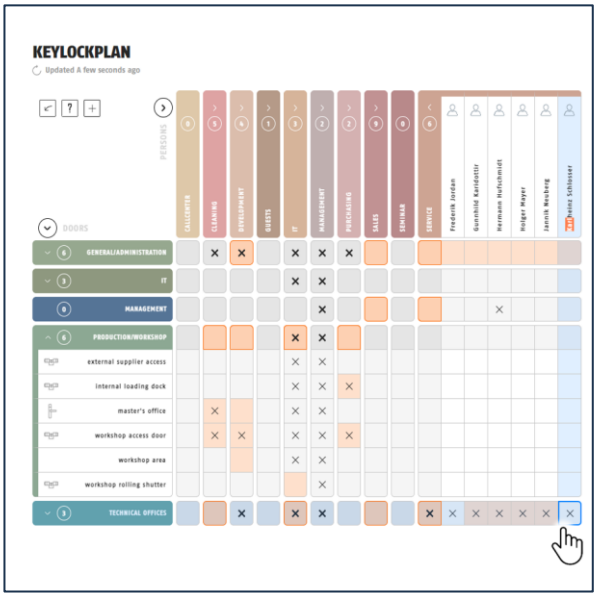
In the locking plan overview :

- Open the Keylock plan menu.
- Find the person by entering the name in the search field. The keylock plan displays suitable search results as you type.



- Assign the person the required authorisations for doors or door groups by setting a × at the appropriate point in the locking plan.
- Revoke access authorisations by deleting the × at the relevant point.

- Complete the process by programming the locking medium.



Assign schedule

A schedule restricts the person's access times. The schedule of the person group is preset.

You can assign the person a different schedule. You can also permanently grant or completely remove authorisation for individual doors.

- ⊳ Open the „Persons“ overview.
- ⊳ Select the person in the list of persons.

Assign the person a different schedule:

- ⊳ Click on the "Individual schedule" button.
- ⊳ Unfold the list of schedules.
- ⊳ Select a schedule from the list.

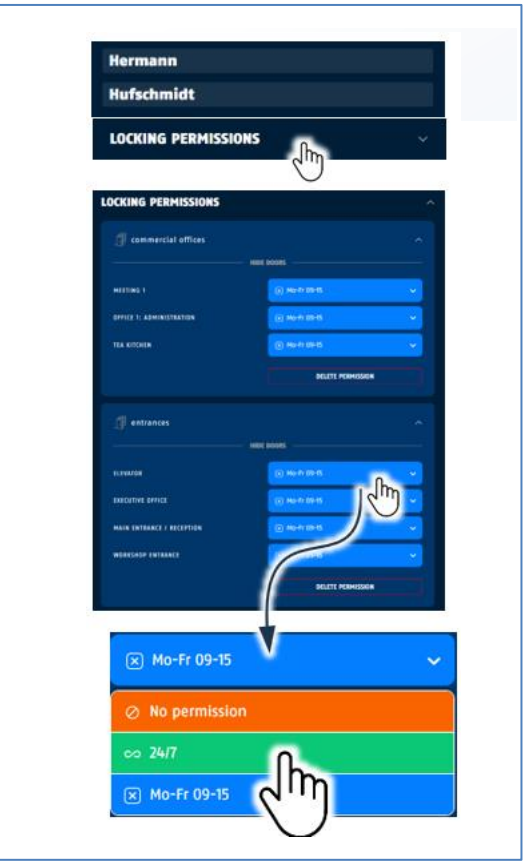
Assign the person a different schedule for individual doors:

- ⊳ Expand the "Permissions" list field.
- ⊳ Select the door or door group to be changed from the list.
- ⊳ Unfold the list of schedules.

- ⊳ Assign permanent access authorisation by selecting the entry "24/7".
- ⊳ Restrict the access authorisation in terms of time by selecting a schedule.
  If no schedule can be selected, create a schedule in the Schedules view and assign it to the person group or person.

- ⊳ Withdraw authorisation by selecting "No authorisation".
  For individual doors, this setting is the same as the "Delete authorisation" button.

- ⊳ Complete the process by programming the locking medium.



Limit access authorisation in terms of time

For time-limited access - e.g. for visitors, trainees or tradesmen who are only granted access for a limited period of time - set the start and end dates for the validity of the locking medium.

- Open the „Persons“ overview.
- Select the person in the list of persons.
- Expand the "Other settings" list field.
- Click on the "Validity of access rights (from...to)" button.
- Select a start date and an end date.
  Without a start date, the access authorisations are valid immediately.
  Without an end date, the access authorisations are valid indefinitely.

If you also want to restrict access to certain times, assign the person (or group of persons) a schedule.

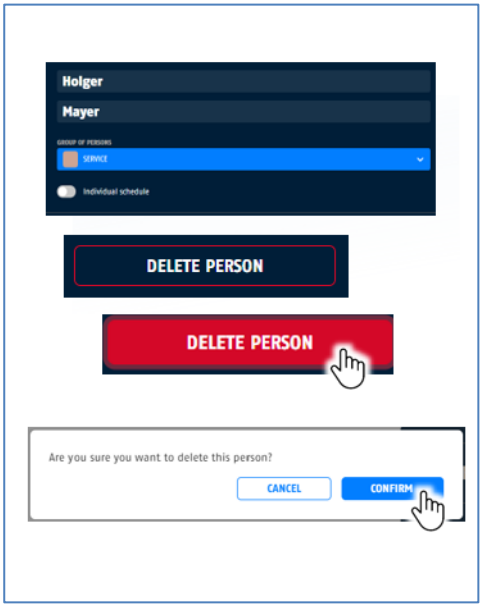
- Complete the process by programming the locking medium.

3.5. Delete person

Deleting a user has the effect of deleting all the person's data.

Please note: Persons can only be deleted if all locking media have been returned and the assignments of the media to the person have been removed. This ensures that access attempts with blocked locking media are rejected and logged. It is possible to change the person's name.

- Open the „Persons“ overview.
- Select the person in the list of persons.
- Click on the "Delete person" button.
- If you are sure you want to remove the person from the system, answer the security prompt with "Confirm".



3.6. Add group of persons

For better orientation, group persons with similar authorisations together in groups. Groups of persons make it easier to manage a locking system. Access rights can be granted or withdrawn from a group of persons, schedules can be specified and much more.

A person can be assigned to a maximum of one group of persons.

- Open the “Persons” overview.
- In the upper part of the "Persons" window, click on the "+ NEW" button (1).
- Enter a name for the group (2) in the editing area.
  As soon as the program recognizes a name, a tile (3) is created for the new group and the name is displayed.

If applicable:

- Select a schedule for the new group (4).
- Select access authorisations for doors or door groups for the person group (5).

Group authorisations are inherited by all persons belonging to the group.

Group authorisations can be granted in the Persons view or in the locking plan view.

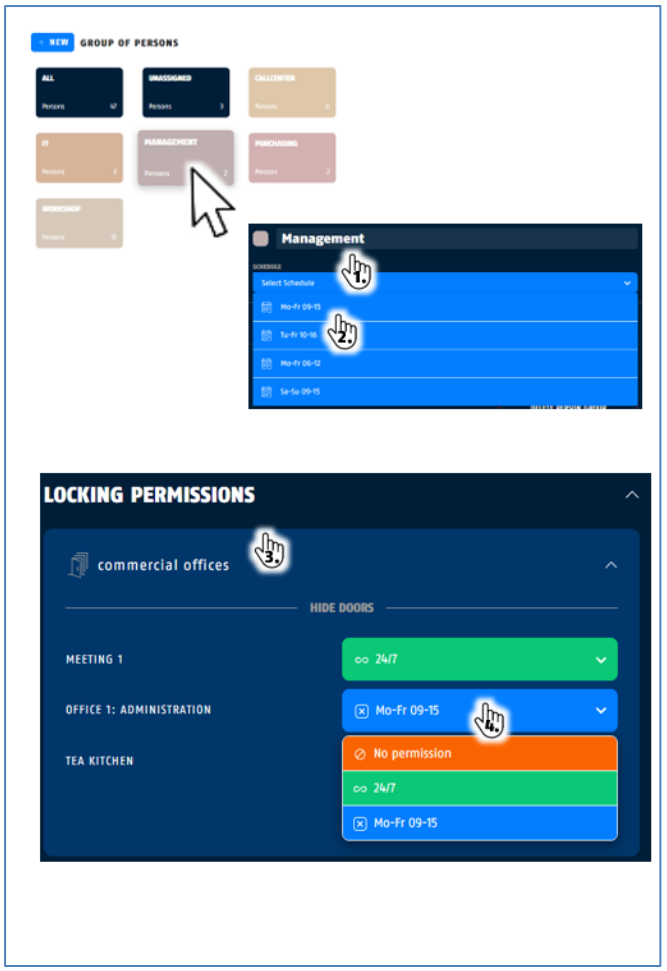
It is not possible to create and program a locking media for a group of persons. locking media can only be assigned to persons.

3.7. Edit group of persons

Change group name

- Open the „Persons“ overview.
- Select the tile for the group.
- Place the mouse pointer on the name field with the group name.
- Change the group name as required.

Assign schedule for group of persons



- If not already available, create a suitable schedule in the Schedules view.

- Open the „Persons“ overview.
- Select the tile for the group.

If a schedule is to be valid for all doors and door groups:

- Expand the "Schedule" list field and select the desired schedule from the list.

If a schedule is only to be valid for individual doors or door groups:

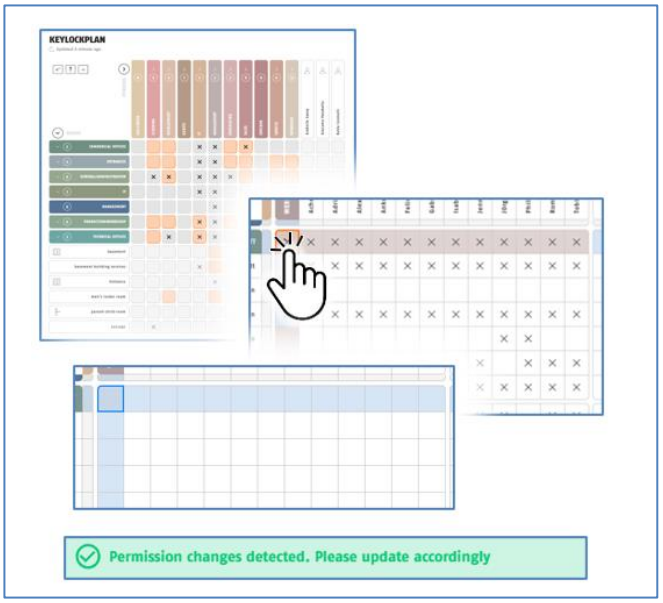
- Expand the "Authorisations " list field.
- Select the desired door or door group from the list.
- Unfold the list of schedules.
- Assign permanent access authorisation by selecting the "24/7" entry.
- Restrict access authorisation in terms of time by selecting a schedule.

- If you select "No authorisation" instead of a schedule, you revoke the corresponding authorisation.
  This setting is the same as the "Delete authorisation" button.

3.8. Revoke the authorisations to a group of persons

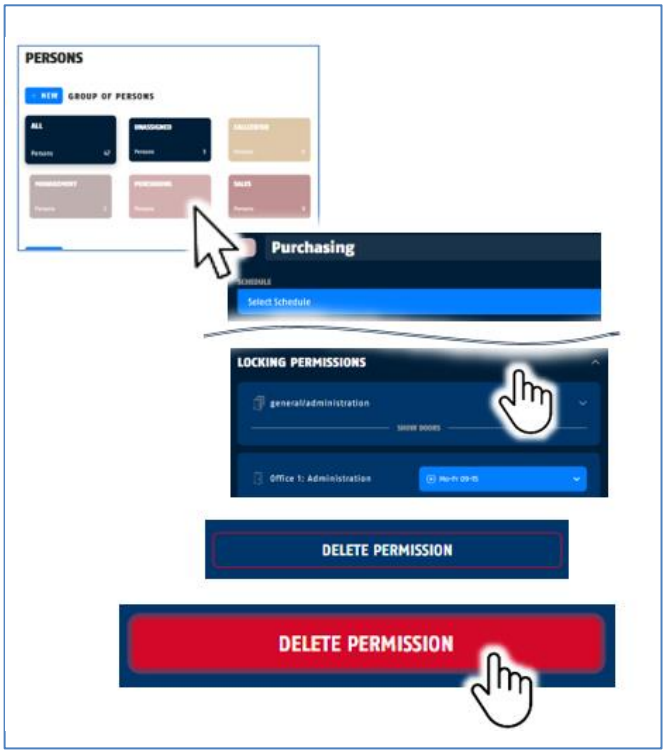
Revoke the access authorisations of all persons in a group.
If access authorisations are revoked, the data remains stored in the system and access can be actively prevented.
Denied access attempts - e.g. using locking media that have not been returned - are also logged.

- Open the "locking plan" view.
- Select the group column.
- Remove all authorisations in the complete group column by removing the. ×



Alternatively, you can revoke authorisations in the Person group view:

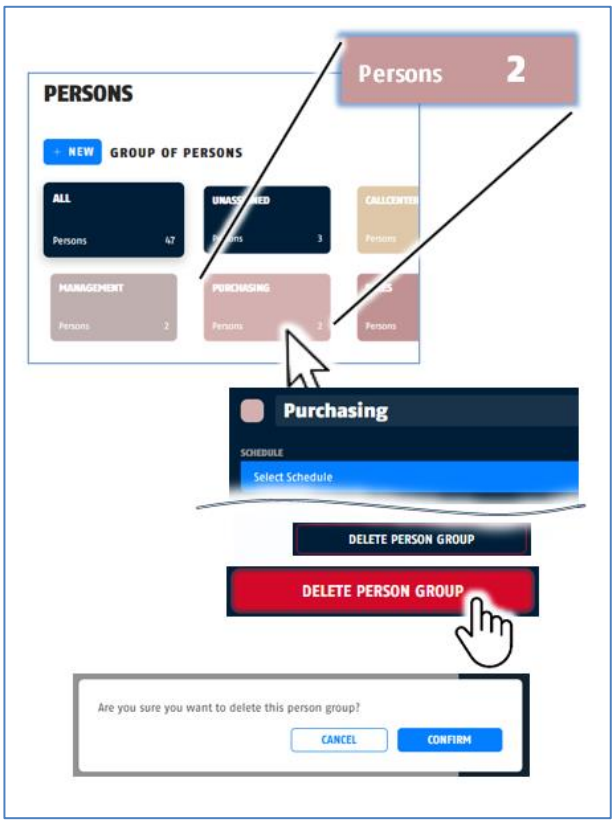
- Open the „Persons“ overview and select the tile for the group.
- Expand the "Permissions" list field.
- Select the desired door or door group from the list.
- Revoke the authorisation by clicking the "Delete authorisation" button.
  This setting is equivalent to the "No authorisation" entry in the list of schedules.



3.9. Delete a group of persons

You can delete empty groups of persons.

- ▷ Open the „Persons“ overview.
- ▷ Select the group of persons to be deleted.
- ▷ Assign the persons contained to other groups of persons by selecting the persons in the list and moving them to the relevant group.
  For a multiple selection, press the Shift key and click on the desired persons.
  Alternatively, move the persons to the "Not assigned" group or delete them.
- ▷ If the group of persons no longer contains any persons, click on the "Delete group of persons" button.



3.10. Manage locking media and system media

Under the system settings you can display all locking media and system media available in the system. This gives you a quick overview of available media.

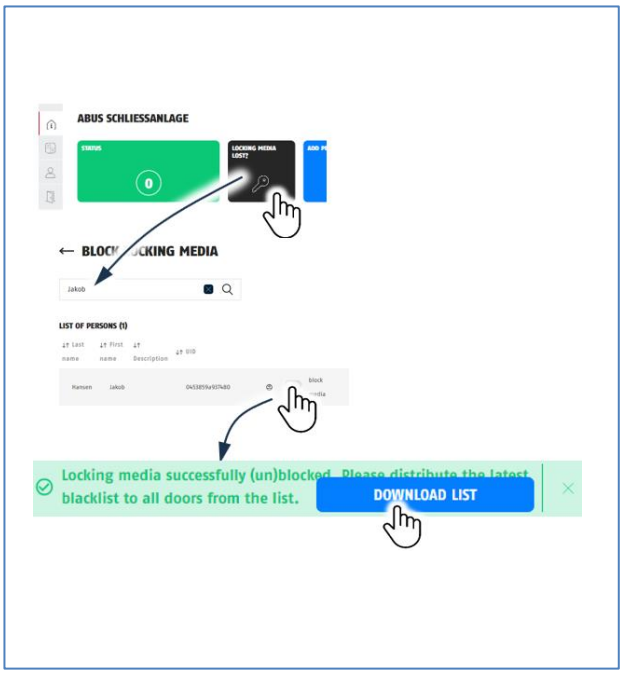
Information on the locking media can be adjusted here. The locking media are assigned during the creation and editing of new persons.

System media is used to display card information and centrally manage all system cards required for system support and maintenance, such as parameter cards, log cards, reset cards, blacklist cards and emergency opening transponders.

You can give system media a name, add a description and define the validity of the system medium. An unlimited validity is set in the system for emergency opening transponders. It cannot be changed. All system media can be deleted. Please note, however, that you cannot access important functions without a system card.

3.11. Block a locking or system medium

Block a locking or system medium if it has been lost or stolen.



Requirements for blocking a locking medium :

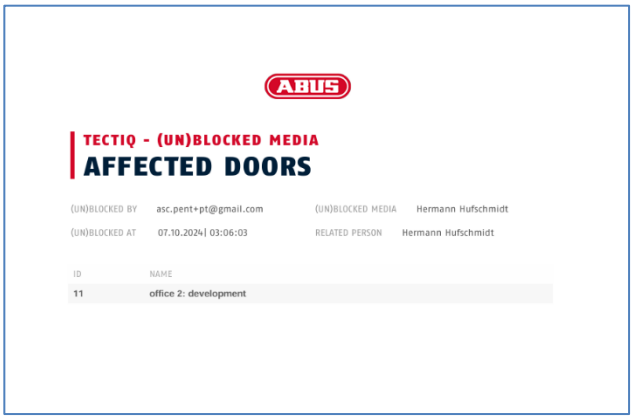
- You need a blacklist card for your locking system to activate the locking medium blocking function in all door components.

- ▷ Open the Dashboard view.
- ▷ Select the "locking media lost or stolen" tile.
- ▷ Enter the name of the person whose locking medium is to be blocked or the name of the system medium in the search field.
- ▷ The locking and system media found are displayed as a results list.

If you do not know the exact name, the search function will show you matching entries after entering just 2 letters.

- ▷ Press the "Block medium" button in the desired line.

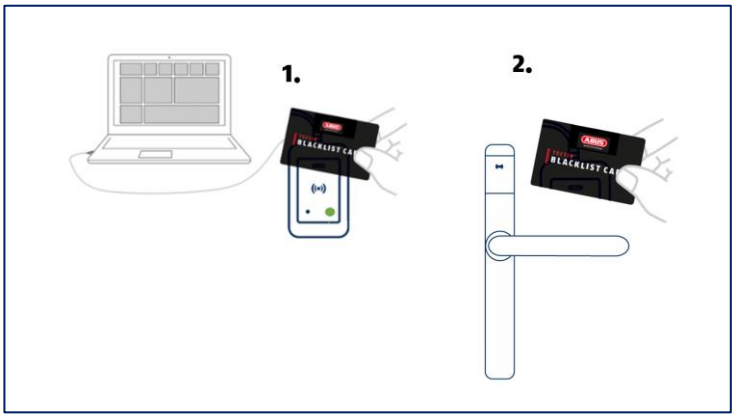
- ▷ The blocking will be confirmed and a list of all affected doors will be made available for download.
- ▷ Download the list to your PC by clicking on the blue download button.



- ▷ You will find the download list in your download directory

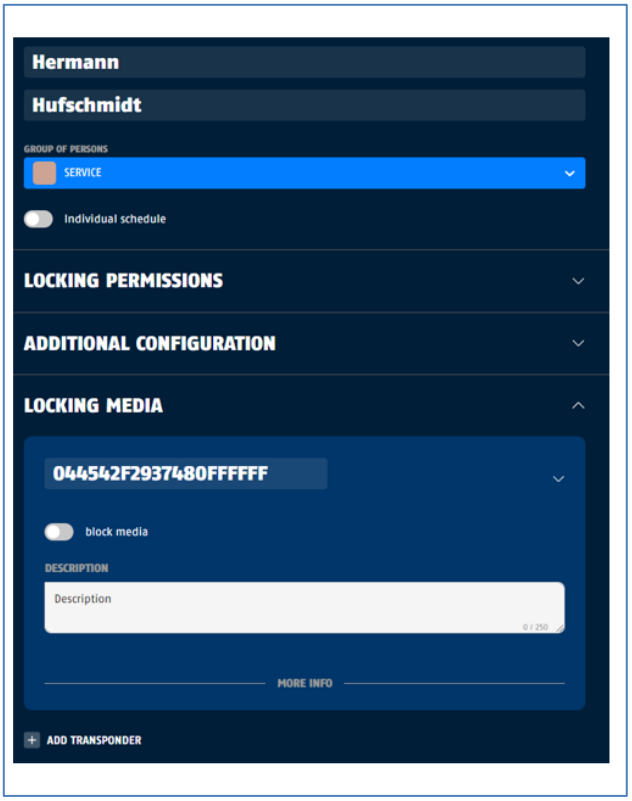
- ▷ Take the blacklist card.
- ▷ Present the blacklist card at the table reader (1).

- ▷ Go to all door components from the download list and present the blacklist card (2).



Please note:
Blocking lists are only transferred to the door components via the blacklist card!

3.12. Edit a locking medium



You can add information to the locking media in the person's editing area.

Change the name of the locking medium

- ▷ Give the locking medium a concise name.

- For example, select the transponder number "KDExxxxxx" printed on the locking medium.
- Note: Careful data maintenance makes it easier for you to assign issued locking media to persons.

locking and unlocking the locking medium

The current locking status is displayed. You can set and remove a lock, e.g. if the locking medium has been found again.

Please note: Any change to the locking status must be transferred to each door component using the locking list with the locking card (blacklist card).

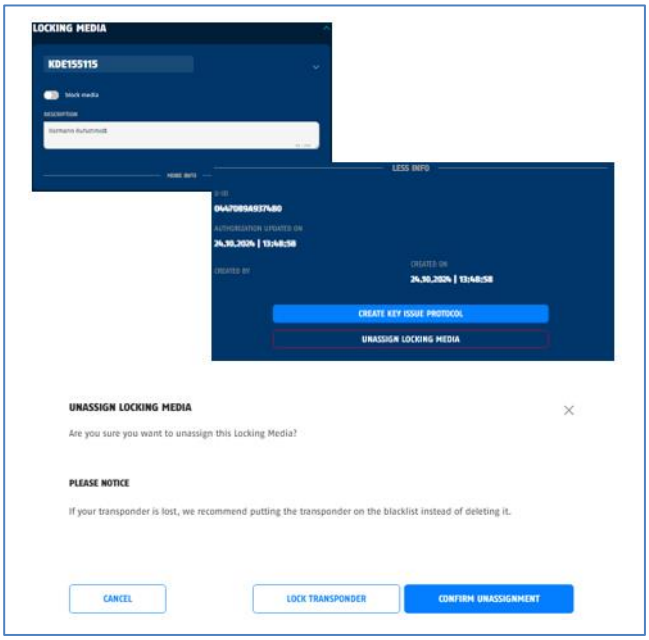
Add description of the locking medium

- ▷ You can add a description to each locking medium, e.g. "Replacement medium issued on ".

Add another locking medium

- ▷ You can create and issue another locking medium to a person.

3.13. Delete locking medium



locking media can be separated from a person by deletion.

- To do this, expand the "More info" editing view in the Persons view under locking media.
- Click on "Delete locking medium".
- If you click the "Confirm deletion" button, the assignment of the locking medium to the person is cancelled.

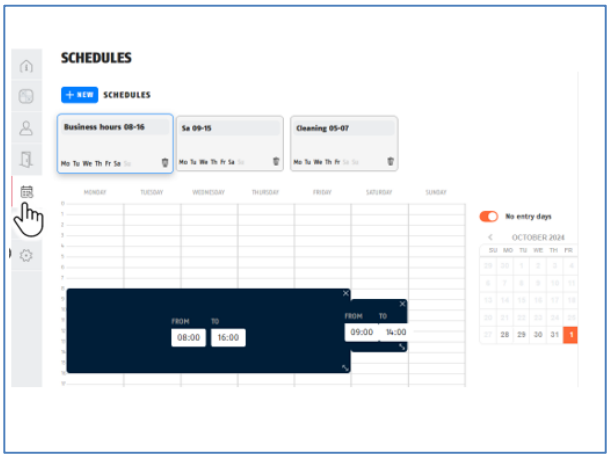
The locking media is assigned to the pool of unassigned locking media and can be deleted here and then assigned to another person

Please note:
Attempts to gain access with unassigned keys are not logged. It is therefore recommended to block a locking medium in most cases!

To delete a locking medium, it must not be blocked.

During the deletion process, the locking media must be presented at the desktop reader. Lost locking media cannot be deleted and must be blocked.

3.14. Create schedule



- Create a new schedule in the Schedules view.
- You can find out everything you need to know about creating and editing schedules in chapter 11 of the reference manual.

Up to 300 schedules with up to 15 time intervals each can be stored in the TECTIQ access control system.

Only one schedule is valid per person. The first time a schedule is created, the new user inherits the schedule of the person group to which they are assigned. The schedule can be customised, or a new individual schedule can be created.

Each schedule can be used by all groups of persons and/or persons in the system. It is therefore recommended that schedules are named simply, neutrally and uniformly (e.g. according to the set time interval "Mon-Fri 08-18").

Blocking days can be added to each schedule on which users do not have access to the secure area (e.g. company vacations).

- Please note: A schedule is only applied if it has been assigned to a group of persons or a person and the associated locking media have been updated.

3.15. Edit schedule

A schedule can be edited/changed in the Schedules view. See reference manual chapter 11.

- Please note: A schedule only becomes effective after the locking medium has been updated.
- Please note: Every change to a schedule affects all groups of persons and persons whose authorisation is linked to the schedule.

3.16. Delete schedule

A schedule can be deleted in the Schedules view. The prerequisite is that it is no longer assigned to a person group or person.

4. TECTIQ - For installers

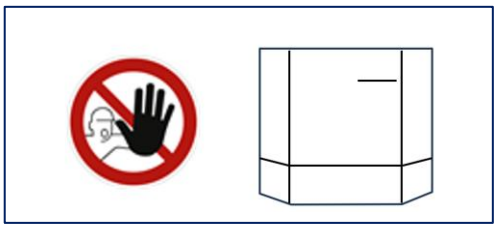
You are a service technician or ABUS specialist retail partner. You plan access control systems with ABUS TECTIQ. You plan the system, determine the requirements and order the components. You plan doors and system components. You are the contact person for your customers or have concluded service and maintenance contracts.

Contents

4.1. Realizing a TECTIQ access control system - First steps

The first steps in the implementation of a TECTIQ access control system relate to the system components central unit, update terminal, PC and desktop reader as well as the system media (parameter card).

4.1.1. Installation location of the TECTIQ Control



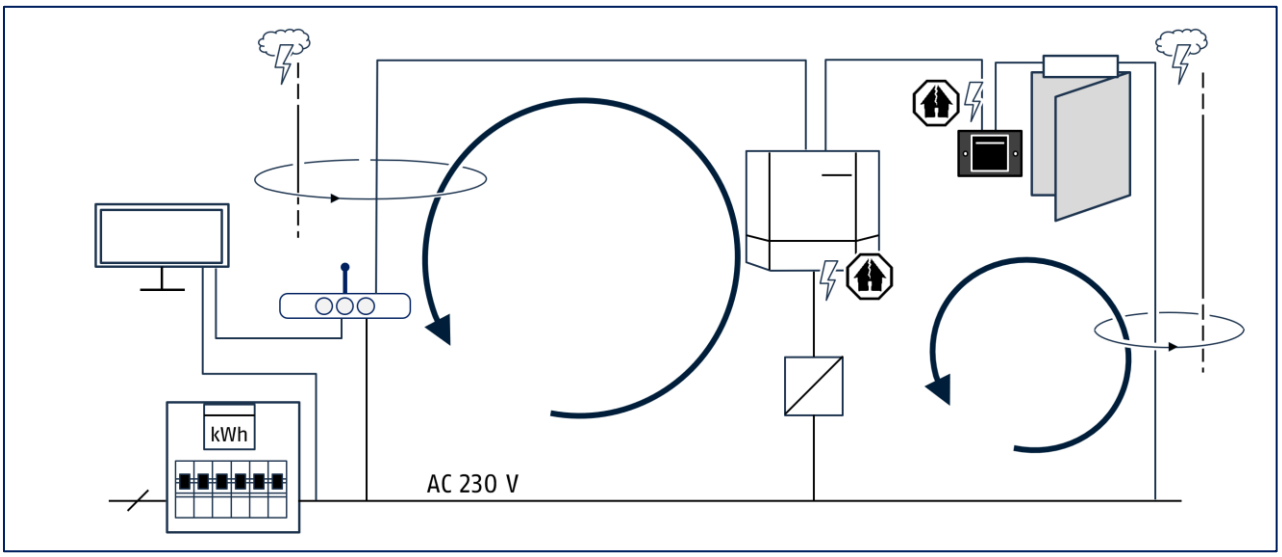
- Protected from unauthorised access - e.g. server room
  If necessary, the device must be accessible for maintenance personnel, e.g. to read the LED.
- Supply with mains voltage
- Recommendation: UPS-buffered
- Network connection
- Recommendation: own network strand
- Sufficient ventilation in closed environments (e.g. distribution cabinet)

Important! If the power supply to the control panel fails for an extended period, the access authorisations in Update Terminals are no longer updated.
- Make sure that the mains adapter cannot be unplugged from the socket!
- Secure the supply to the TECTIQ Control separately.

4.1.2. Cable routing

NOTE High-energy events in the power grid, e.g. as a result of a lightning strike, can destroy electronic devices due to overvoltage.

- Avoid conductor loops in the electrical and network installation (see illustration).
- Install lightning and surge protection.



▷ Watch out for manipulation possibilities, especially with supply and network cables. If it makes sense, lay separate lines and secure them separately.

4.1.3. Installation location of the update terminal

The update terminal consists of the wall reader unit and the control unit. The same criteria and measures apply here as for the control panel.

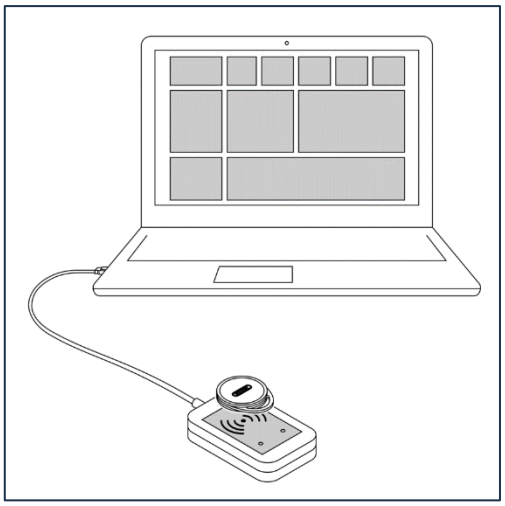
Compact installation (wall reader and control unit in a common flush-mounted box) should only be carried out in protected indoor areas where no unauthorised tampering is to be expected. In all other cases, install the wall reader and control unit separately, e.g:

- in the outdoor area,
- in publicly accessible areas (corridors, stairwells),
- if no sensitive connection cables (network, door control) are to be located at the installation site of the reader unit,

4.1.4. Setting up the PC

The PC is required for working with the access control software TECTIQ Access Manager and for writing the locking media and system media. The PC is generally not required for operating the system and updating the locking media. You need:

- Network connection
  The PC can also be connected to the network router via WLAN.
- IT administrator rights to install the software.



4.1.5. Connect desktop reader

▷ Connect the desktop reader to a free USB port on the PC.

4.1.6. Start TECTIQ Control

Prerequisites:

- TECTIQ Control connected to the network and power supply.
- A DHCP server or DNS server is present in the network or router.
- The TECTIQ Control and PC are accessible in the same network.
- PC connected to network and power supply.
- TECTIQ Access Manager access control software is installed on the PC.
- TECTIQ desktop reader is connected to PC.

Start TECTIQ Access Manager

▷ Switch on the PC.
▷ Start TECTIQ Access Manager.

Select language

Select the language for the user interface of the TECTIQ Access Manager software.

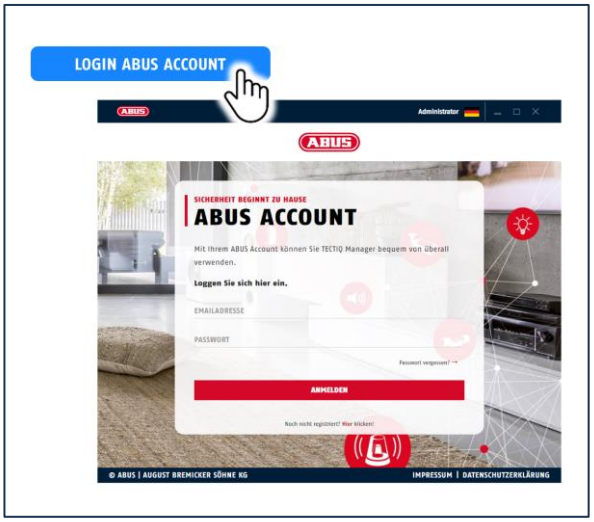
▷ Click on the flag in the header.
▷ Select the desired language from the list box.
The selected language is displayed as a flag in the header.

Log in with ABUS account

To set up a new access control panel, you need an ABUS Online Account as a specialist installer.

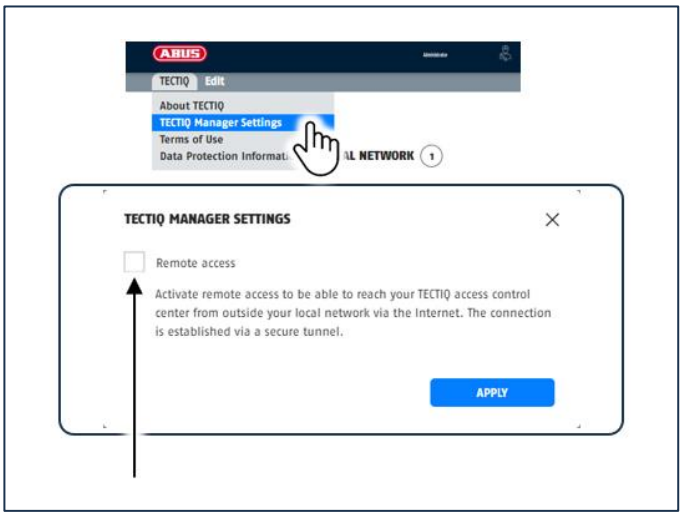
If you do not yet have an ABUS account, register and create a new ABUS account. Registration as a specialist installer is reserved for authorized specialist retail partners.

- Enter your login data.
- "Press the "Log in" button.



Settings for initial connection

- Open the TECTIQ menu.
- Open TECTIQ Manager Settings.
- Activate remote access.



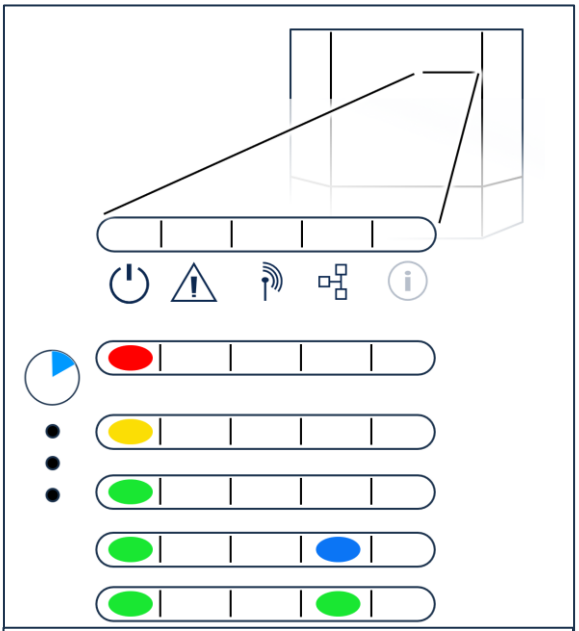
Switch on and connect the access control panel

On delivery, the TECTIQ access control panel is configured for connection via a router and addressing via DHCP. As a rule, the router should find the access control panel when it is switched on.

ⓘ Coordinate the addressing of the TECTIQ devices in the network with the administrator of the IT system.

- ▷ Switch on the power supply for the TECTIQ Control.

The Control starts up. This process may take a few minutes. As soon as the LEDs⏻ and⊞ light up green, the alarm panel is ready for operation and is connected to the network.



An TECTIQ Control found should automatically appear on the interface.

If the Control does not appear automatically on the interface:

- ▷ Press the "Search again" button.

- or -

Connect via IP address:

- ▷ Read the IP address in the network router.
- ▷ Open the "Edit" menu.
- ▷ Select "Add control via IP address".
- ▷ Enter the IP address of the control.
- ▷ Click on "Add".

If the initial recognition process has already been carried out on a control panel, it has a Connect ID and can also be added with this. The Connect ID can be copied from an Access Manager to which the access control panel is known.

If you have access to the Access Manager in which the TECTIQ Control is logged in

- ▷ Select the TECTIQ Control in the original Access Manager.
- ▷ Click on the Copy symbol next to the Trash icon.

Connect ID is copied to the clipboard.

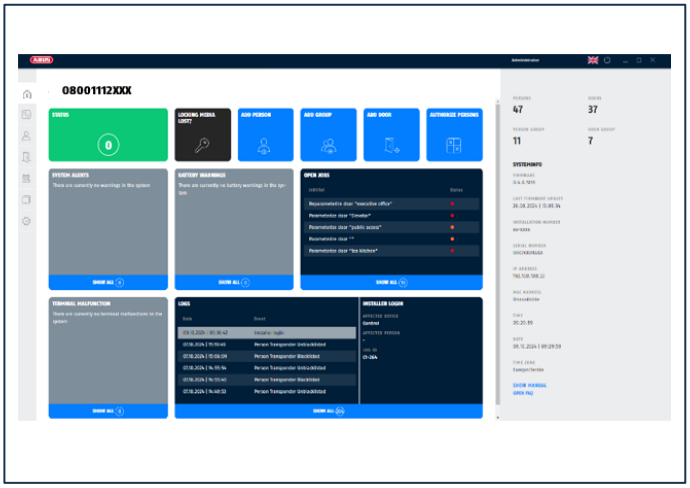
- ▷ Open the current Access Manager.
- ▷ Open the "Edit" menu
- ▷ Select "Add control via Connect ID".
- ▷ Paste the Connect ID from the clipboard.
- ▷ Click on "Add".

You identify the access control panel found using its serial number.

Connect to the control that was found:

- ▷ Click on the desired tile.

The dashboard is displayed in a new window.



Set the date and time

Check the time in the TECTIQ Control and update the settings if necessary.

ⓘ The system time is of central importance for the reliable functioning of the access control system. If the system time is not set correctly, it is possible that access to the secured area will not be granted.

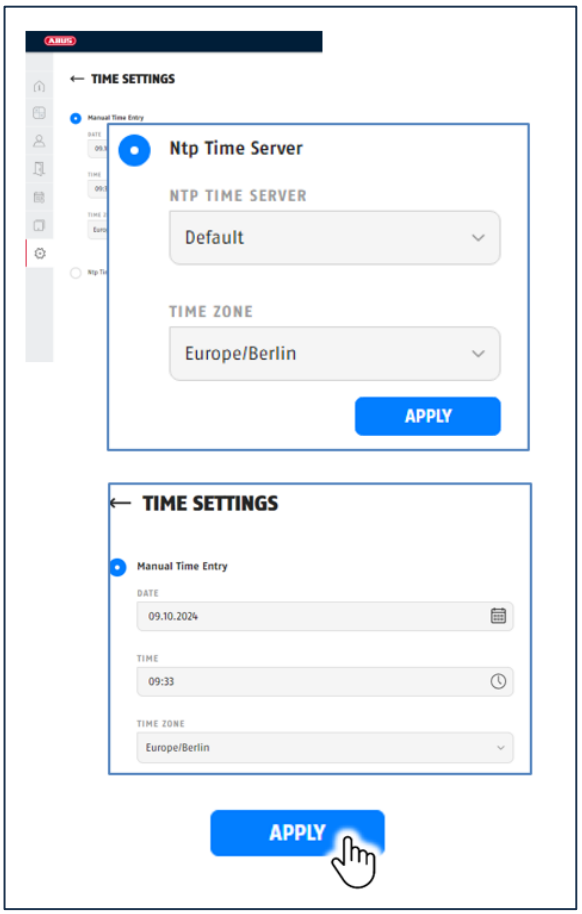
- ▷ Start the Access Manager and connect to the TECTIQ Control.
- ▷ Select the System settings view and the buttons System configuration and Time settings.

ⓘ We recommend setting the time via a time server (NTP)!

- ▷ Select "Time server (NTP)" so that the system can synchronize the date and time automatically on a regular basis.
- ▷ In the "Time server (NTP)" field, select "Default" or the option for manual entry. In the latter case, enter an Internet address for a time server - e.g. for the legal time in Germany: ptbtime1.ptb.de
- ▷ End the entry with "Apply".

- to set the time manually:

- ▷ Select "Manual time entry"
- ▷ Enter the current values for "Date" and "Time". Enter the time zone corresponding to the system location, e.g. "Europe/Berlin" for the time in Central Europe.

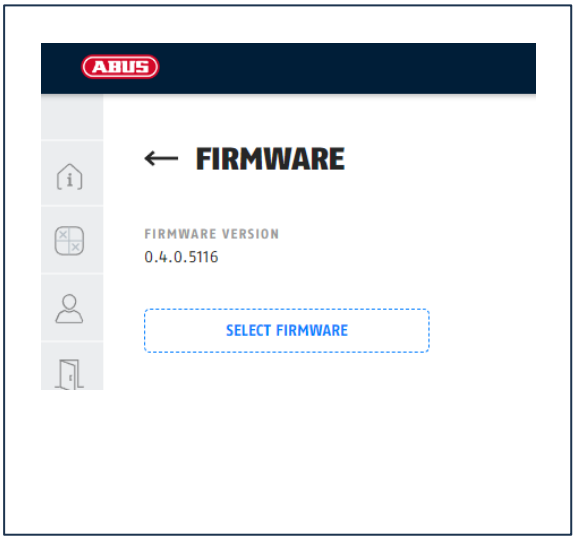


Update the firmware

Before working in the software, make sure that the firmware in the TECTIQ Control is up to date.

- ▷ Start the Access Manager and connect to the TECTIQ Control.
- ▷ Select the System settings view and the buttons System configuration and Firmware update.

The current firmware version is displayed.

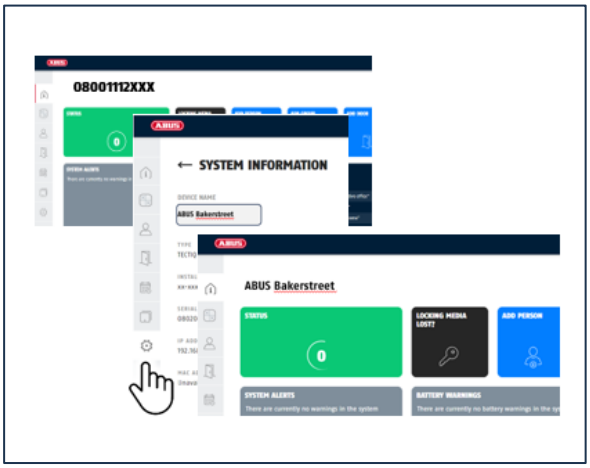


- ▷ Download an updated firmware to the local hard disk.
- ▷ Select the "Firmware Update" button and select the downloaded software on your local PC.
- ▷ Follow the further instructions.

Enter the project data

The system name is displayed at the top of the dashboard. The factory default setting here is the serial number of the access control panel.

Enter the system name agreed with the operator.



- ▷ System settings view→ System configuration→ System information
- ▷ Enter the device name.

Network settings

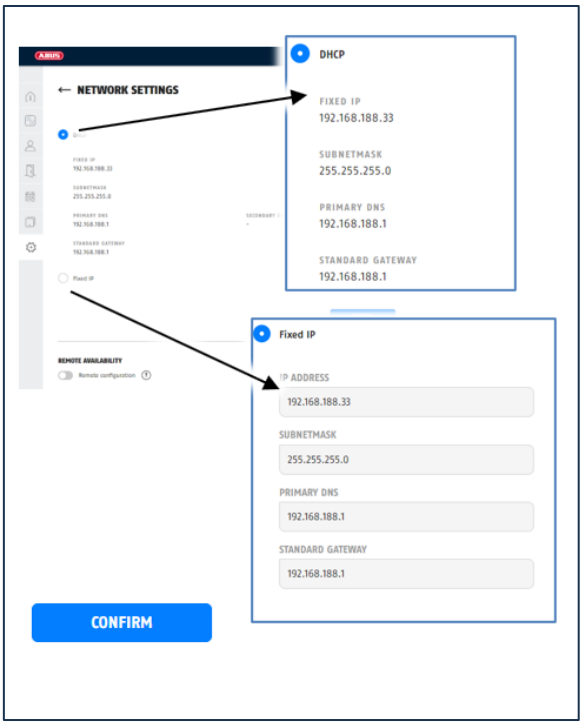
If your network settings require a fixed (static) IP address, configure the network access of the TECTIQ Control.

- ▷ Select the System settings view and the buttons System configuration and Network settings.

- ▷ Select your settings according to the network configuration at the final installation location.
- ▷ Select "DHCP" for automatic address assignment.
- ▷ Select "Static IP address" to set the Internet address manually. You can obtain the required data from the network administrator.
- ▷ Finish the entry with "Confirm".

After changing the network settings, the control restarts and disconnects. The connection to the control must then be re-established.

If you have accidentally changed the network settings and no longer have access to the control, you can reset the network settings.



4.1.7. Update Terminal Connect with TECTIQ Control

Prerequisites:

- TECTIQ Control connected and ready for operation.
- Update terminal connected to power supply and network.
- Update Terminal and TECTIQ Control accessible in the same network.

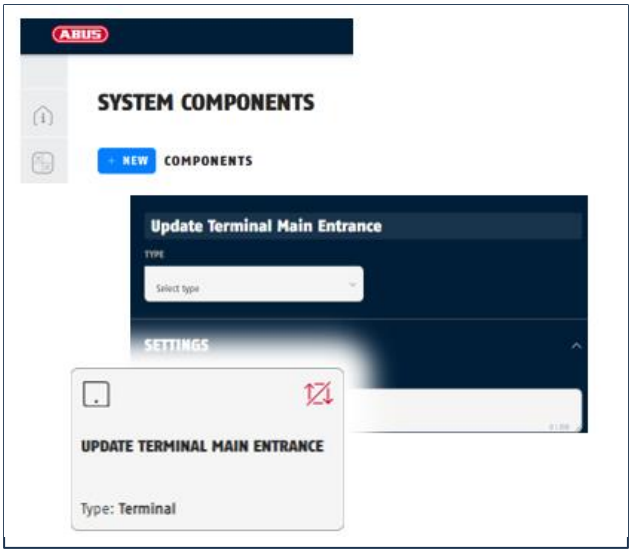
- ▷ Coordinate the addressing of the TECTIQ devices in the network with the administrator of the IT system.

Add the update terminal

- ▷ Select the System components view.
- ▷ Press the "+ NEW" button.
- ▷ Enter a name for the update terminal in the editing area.

The update terminal is displayed as a tile on the user interface.

- ▷ Select your settings according to the network configuration at the final installation location.



Connect with Update Terminal

- ▷ Click on the desired update terminal with the mouse pointer.

Add update terminal automatically:

- ▷ Select "Add system component".

The alarm panel starts a search process in the network.

If no update terminal was found, the search can be started again later ("Refresh").

Update terminals found in the network are displayed with their serial number (1.).

- ▷ Press the "Apply" button.

The control connects to the terminal.

The connected update terminal is displayed in the work area with the status "Green" (= "Connected").

Alternatively, enter the IP address for the update terminal manually (2.):

- ▷ Select IP address
- ▷ Enter the connection data from your router.
- ▷ Select "Apply".

4.1.8. Set up system media

Create the required system media for the system. You will need the desktop reader for this.

- Parameter card - required
- Blacklist card - required
- Emergency opening transponder - may be required depending on the building
- Protocol card - optional
- Reset card - optional

- ▷ Select the System settings view and System media.
- ▷ Select the media type to be described by pressing the relevant button.

- Press the "+ NEW" button.
- Enter a name for the system medium.
- Enter a date until which the medium should be valid.
- Click on the "Apply" button.
- Place the medium on the desktop reader and wait until the writing process has been completed.

The system medium on the desktop reader must match the selected media type.

4.2. Project planning and setup

When **configuring**, you first enter the system data - doors, door groups, system devices - in the TECTIQ Access Manager, then enter the personal data and finally assign the access authorisations in the locking plan.

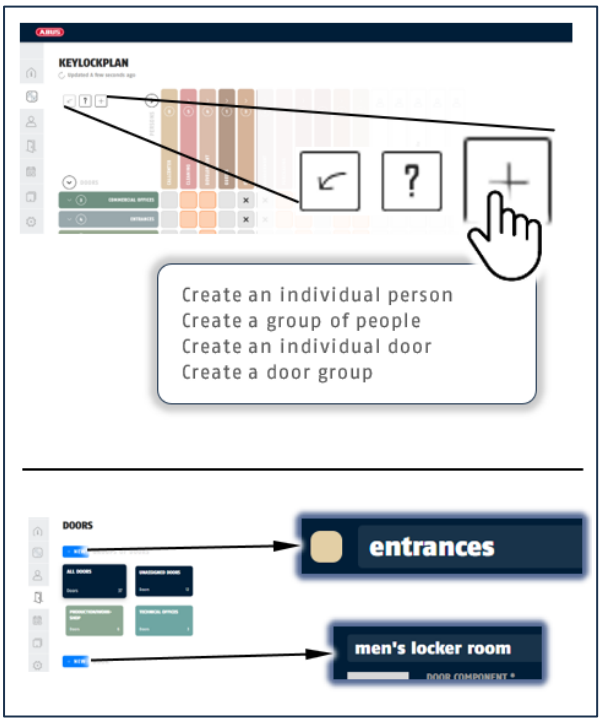
When the system is **set-up**, the configured data is written to the door components. Basically, two different procedures are useful, which can change depending on the customer or specific requirements.

- During on-site commissioning, the door components are already installed at the customer's premises, and you load the data into the door components at the door.
- During workshop commissioning, program the components first before installing them at the customer's premises.
  When doing this, please note that door components are always decoupled after programming. Without a functioning locking medium or other suitable measures, you can lock yourself out of the secured area!

In general, the following sequence is recommended for project planning and commissioning of TECTIQ access control systems.

1.	Create doors and door groups.
2.	Assign door components to the doors.
3.	Program door components.
4.	Define schedules (optional).
5.	Create persons and groups of persons.
6.	Issue access authorisations in the locking plan.
7.	Configure locking media.
8.	Program locking media.
9.	Test the function of the door components and locking media.
10.	Issue locking media to users.
11.	System handed over to operator.

4.2.1. Planning doors and door groups



Enter the planned doors and door groups in the Access Manager.
You can use two ways to do this:

In the locking plan view:

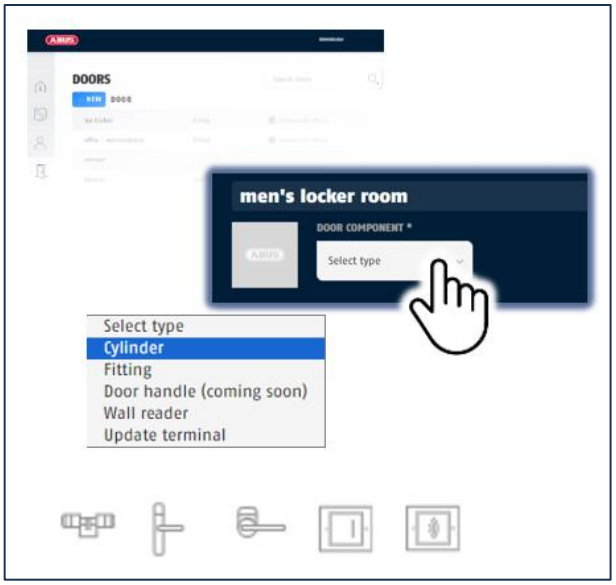
- Press the quick button [+] and select the "Create a door group | individual door]" command in the list field.
- Enter the name for the door or door group.

In the view doors:

- Press one of the two "+ NEW" buttons.
- Enter the name for the door or door group.

In the Doors view, you can then continue by selecting the door components (cylinder, fitting or wall reader).

4.2.2. Assign and set door components

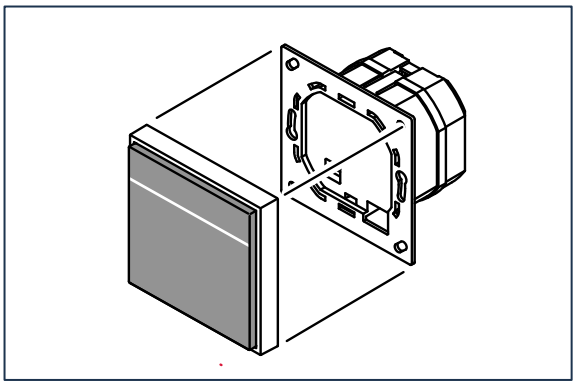


Assign the correct door component to the doors.

- Select the view doors.
- Select the desired door from the door list.
  For large lists, you can restrict the door list by preselecting the appropriate door group.
- Click on the "Door components" list field.
- Select the desired door component - cylinder, fitting, wall reader or update terminal.
  If an update terminal also controls a door, configure it not only as a system device but also as a door component.

Set the correct operating parameters for the door components. If necessary, enter further information for the doors.

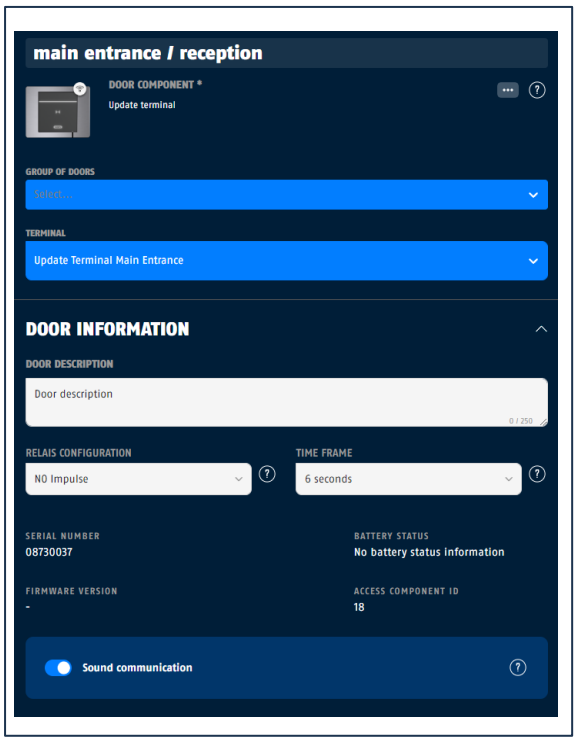
Update terminal as door component / wall reader



Select the characteristic for the relay configuration according to the actuator on the controlled door.

Note the current that flows when the door is opened.
Components such as electric strikes may only be energized for a certain duty cycle (ED).
Motorized door drives or electronic door controls usually have high-impedance inputs that may be permanently energized.

- ▷ Coordinate the settings with the intended use, especially for doors that are opened permanently.



For electric strikes or simple door drives:

- NO contact impulse: "NO impulse"

For electric strikes or door drives with closed-circuit current monitoring:

- NC impulse: "NC impulse"

For turnstiles, entrance areas

- NO impulse: "NO impulse"

Door operator with closed-circuit current monitoring:

- NO impulse: "NO impulse"

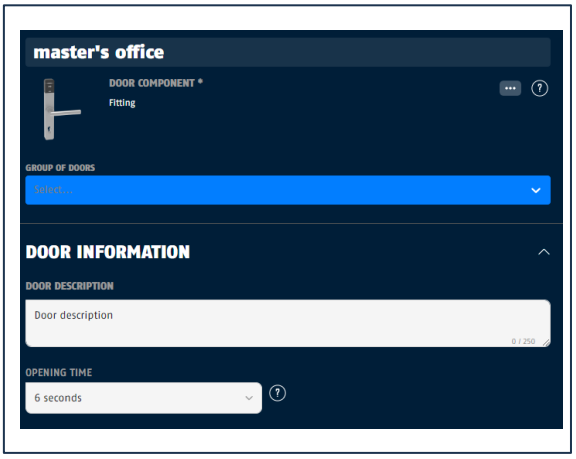
- ▷ Set the release time for the relay under Time period.

- ▷ Select whether an acoustic signal sounds when a medium is presented to the wall reader.

Fitting

- ▷ Assign a name for the door component.
- ▷ Assign the door to a door group.
- ▷ Set the door release time under Opening time.

On delivery, the electronic fitting is coupled in, i.e. access from both sides is guaranteed for installation.



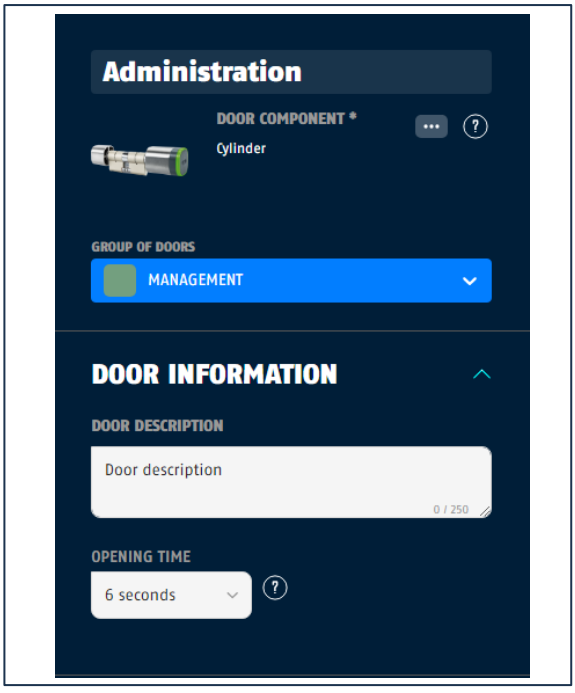
ⓘ After programming, the fitting is in the decoupled state. Access is then blocked from this side.

- If you program the fitting in advance and then install it, make sure that you do not lock yourself out.
- Keep the door open or distribute valid locking media promptly.

Cylinder

- ▷ Assign a name for the door component.
- ▷ Assign the door to a door group.
- ▷ Set the door release time under Opening time.

On delivery, the electronic locking cylinder is coupled in, i.e. access from both sides is guaranteed for installation.

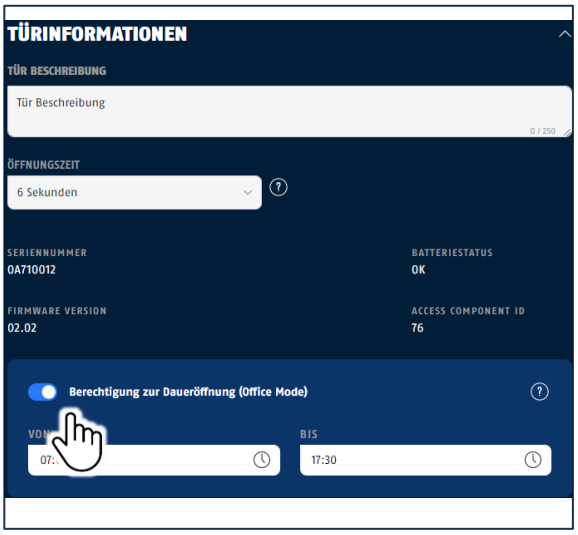


ⓘ After programming, the read head is in the decoupled state. Access is then blocked from this side.

- If you program the locking cylinder in advance and then fit it, make sure that you do not lock yourself out.
- Keep the door open or distribute valid locking media promptly.

4.2.3. Office Mode Settings

An office mode can be activated on the TECTIQ door components. This can either be provided with a time window or activated without a time restriction. Office mode can then either be activated and deactivated manually at any time, or activated within a time window and automatically deactivated when the time window expires



- ▷ Click on the the slider to activate the Office Mode
- ▷ Either select "unlimited" as the "from" and "to" value or assign a time window

After successful programming via parameter card, the Office Mode can be activated for a door with a transponder authorized for opening by presenting it twice and deactivated by presenting it three times.

4.2.4. Program door components

The door component is programmed after the door component has been assigned and set in the editing area of the door component or later in the task list.

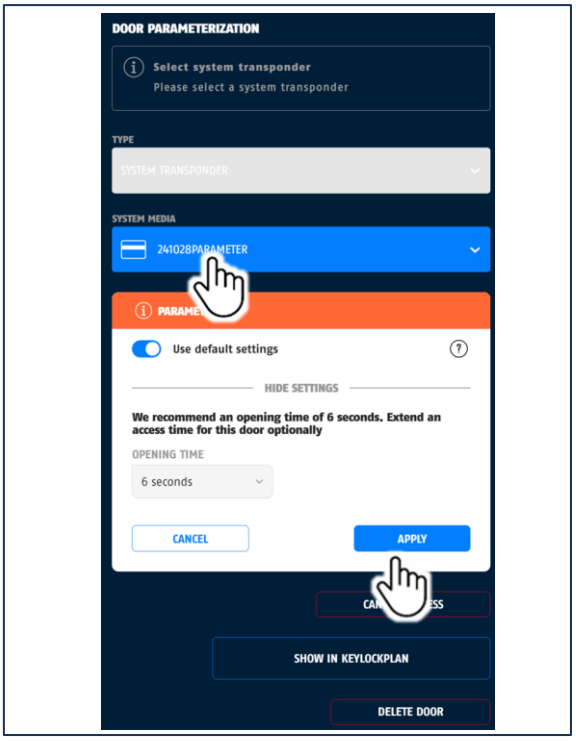
To program a door component, you need the TECTIQ Access Manager, the TECTIQ reader and a parameter card (system medium). Please note: The parameter card can only be used to parameterize the door component for 15 minutes after programming.

Select a parameter card.

- ▷ Select the "Apply" button
- ▷ Place the selected parameter card on the desktop reader and wait until the green LED lights up.

- ▷ Present the parameter card to the door component within 15 minutes. Wait until the LED on the door component lights up green.

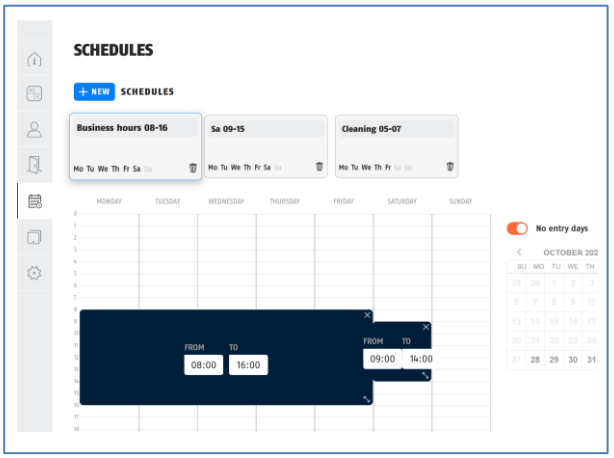
Please note: The process is only complete when you present the parameter card to the desktop reader again and the LED on the desktop reader lights up green.



4.2.5. Define schedules

Schedules are used to restrict access authorisations in terms of time. Schedules can be used for individual persons or for entire groups of persons. To access schedules when creating persons, they must be defined beforehand. The creation of schedules is optional.

- You create a new schedule in the Schedules view.
- You can find out everything you need to know about creating and editing schedules in chapter 11 of the reference manual.



Up to 300 schedules with up to 15 time intervals each can be stored in the TECTIQ access control system.

Only one schedule is valid per person. The first time a schedule is created, the new user inherits the schedule of the person group to which they are assigned. The schedule can be customised or a new individual schedule can be created.

4.2.6. Create groups of persons and persons

You can create groups of persons to easily manage authorisations . A group of persons can be granted or withdrawn access rights collectively, schedules can be specified and much more.

A person can be assigned to a maximum of one person group.

- ▷ Open the „Persons“ overview.
- ▷ In the upper part of the "Persons" window, click on the "+ NEW" button (1).
- ▷ Enter a name for the group (2) in the editing area.
    - As soon as the program recognizes a name, a tile (3) is created for the new group and the name is displayed.

If applicable:

- ▷ Select a schedule for the new group (4).
- ▷ Select locking permissions for doors or door groups for the person group (5).

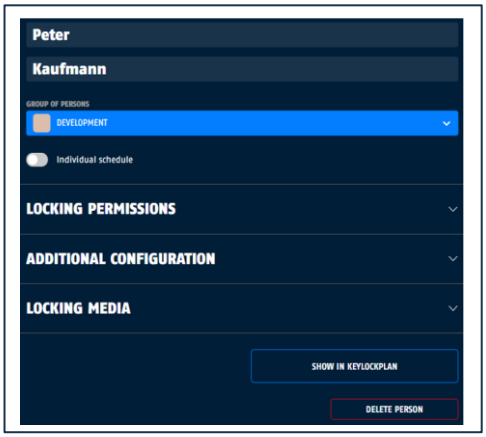
Locking permissions are inherited by all persons belonging to the group.

locking permissions can be issued in the Persons view or in the locking plan view.

It is not possible to create and program a locking media for a group of persons. locking media can only be assigned to persons.

Further information on editing groups of persons can be found in chapter 3 and in the reference manual.

Add person to the person group



Stay in the “Persons” overview.

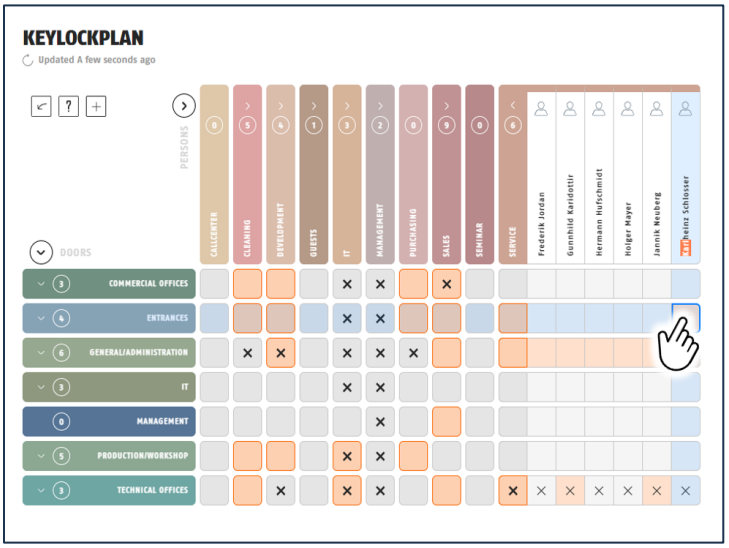
- ▷ Click on the "+ NEW" button above the list of persons.
- ▷ Enter the personal data.

After entering the name in the editing area and selecting the person group, all access authorisations for the selected person group are automatically assigned to the new user

The editing area offers you extended setting options.

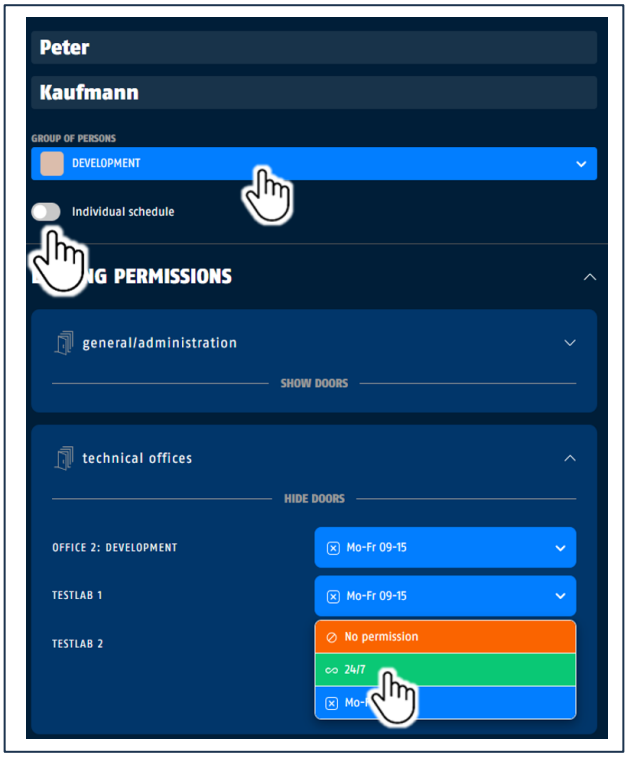
4.2.7. Assign access authorisations

In the locking plan view, you assign the authorisation for door groups and doors to groups of persons and persons in a graphical overview.



- Assign the required authorisations for doors or door groups in the locking plan to groups of persons and persons by setting a× in the appropriate place.
- First grant authorisations at group level.
- Add individual access authorisations by setting an x or remove authorisations by deleting the× in the appropriate place.

In the "Persons" overview, you assign a schedule to groups of persons or persons. The schedule of a person group is preset when a person is added to the person group. It is replaced by the selection of an individual schedule.

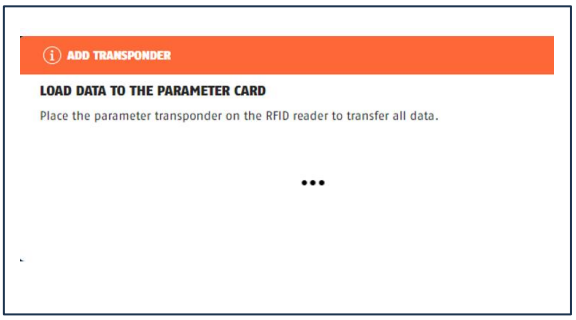


Instead of a time schedule, the setting "No authorisation" or "24/7" can be selected under Authorisations for each door for continuous authorisation.

- Define the validity of the access authorisation under Further settings.

Please note: locking authorisations and schedules must be transferred to a valid locking medium before they become effective.

4.2.8. Program locking media



- Set the validity of the locking medium. The default setting is the validity from the system configuration.
- Assign the locking medium to a person.
- Present the locking medium to the reader.

After successful programming, the system reports "locking media assigned".

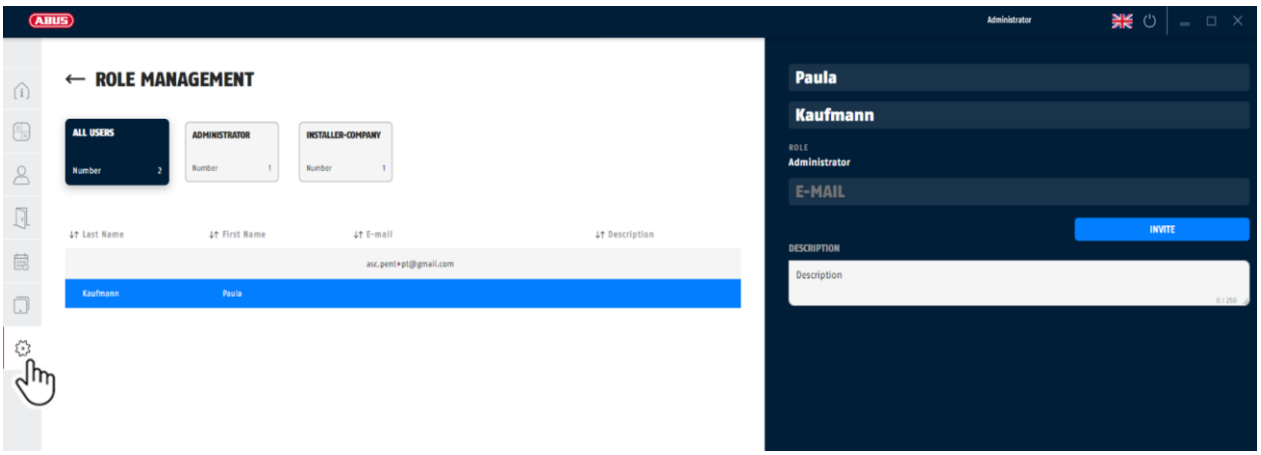
- Complete the process.

4.3. Issue TECTIQ locking media

- After programming, a receipt with all relevant locking medium data is available for printing under the "More information" menu item. See sample in the appendix.
- Hand over the locking media created for the operator to the operator.
- Inform the operator that receipts for the locking media are available in the system.

4.4. TECTIQ system handed over to the operator

- Select role management in the system settings.



- Create the operator or his authorized representative as administrator or complete the data.
- Create an ABUS Online Account for the operator.
- Log in with the operator's data.
- Complete the data for your company under Installer Company.
- If the customer wishes, deactivate your access (optional).

ABUS TECTIQ

TECTIQ Reference Manual.

5. The system

Contents

4.5. Intended use

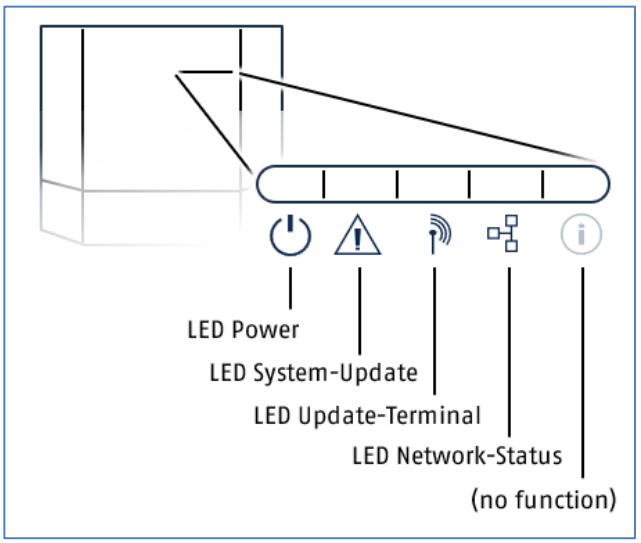
- locking media-controlled access control for private and public buildings
- Management and control of electronic door components such as door fittings, door cylinders and wall reader terminals for electric strikes, door drives, turnstiles in entrance areas and others - for interior and exterior building doors
- Managing access authorisations

Improper use, repair work or modifications not expressly authorized by ABUS and improper servicing can lead to malfunctions and result in the loss of liability, warranty and separately agreed guarantee claims.

4.6. Components

4.6.1. TECTIQ Control

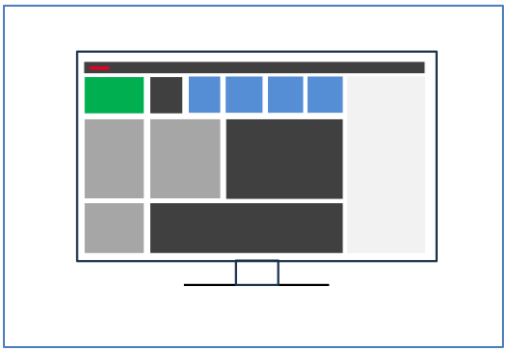
The TECTIQ Control controls the system. It is housed in a protected room, e.g. in the office of the manager responsible or in a separate technical room, and stores all system data on all locations, the doors to be controlled, the users of the system and their access rights. The TECTIQ Control is configured using an external computer - e.g. PC or notebook - and the access control software TECTIQ Access Manager. The TECTIQ Control is integrated into the local network.



The current status of the TECTIQ Control is indicated by status LEDs:

Power LED	red		System start is being prepared
	yellow		System starts up
	green		System ready
System update LED	blue		System software is updated
Update terminals LED	green		Connection to all update terminals OK
	yellow		Connection to at least one update terminal disrupted
Network status LED	green		Online connection to the Internet
	blue		Connection to the local network router
	from		No connection

4.6.2. TECTIQ Access Manager



The TECTIQ Access Manager is the configuration software for the system and runs on a standard PC. The TECTIQ Control makes its data available to the TECTIQ Access Manager locking software via the network. With an Internet connection and the remote access setting, the TECTIQ Control can also be operated from a remote location.

PC / network requirements

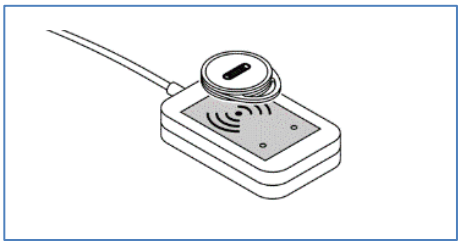
Processor	min. 2.0 GHz
Working memory	min. 2 GB
Storage space	min. 2 GB
Screen resolution	min. 1440 × 1080
Network connection	Ethernet 10/100/1000 (optional WLAN)
Interfaces	3×USB (for desktop reader, mouse and keyboard)
Operating system	Microsoft Windows 10, Windows 11 (64-bit versions)
Internet/network router	Yes

NOTE Computer systems can be spied on and sabotaged! Unauthorised persons can manipulate access authorisations and threaten your property.

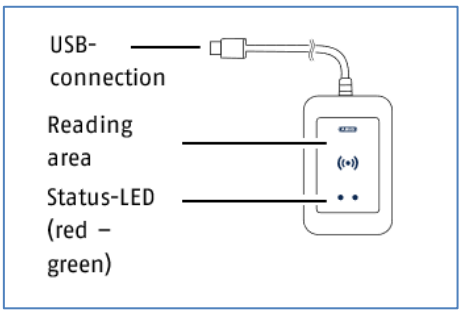
- Do not use an operating system that is no longer updated by the manufacturer.
- Replace discontinued operating systems with an up-to-date operating system as soon as possible.
- Use an antivirus program and install the latest updates.
- Find out about warnings and safety measures and follow them.
- Only use the PC with reliable software.
- Reliable information on security risks and measures can be obtained from the Federal Office for Information Security, for instance bsi.bund.de.

4.6.3. TECTIQ desktop reader

The TECTIQ desktop reader is used to read and write locking media and system media. You need the desktop reader to commission the system, make changes and grant access rights. It is connected to the computer on which the TECTIQ Access Manager locking software is running. The TECTIQ desktop reader uses two status LEDs to indicate its operating status and the status of current processes.



The media to be written are requested by the TECTIQ Access Manager. In this case, please present the locking or system medium in question on the reading surface of the desktop reader until the end of the process is signaled.



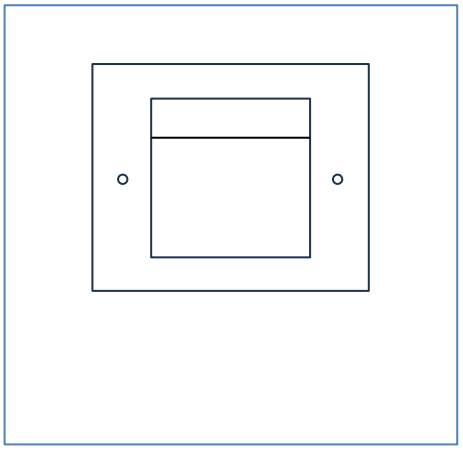
4.6.4. TECTIQ Online Update Terminal

The TECTIQ Online Update Terminal is connected to the TECTIQ Control via the network. The connection is encrypted and therefore secure against eavesdropping or other manipulation.

The TECTIQ Online Update Terminal consists of a wall reader, combined with the associated control unit. It is used for

- Reading and writing locking media and system media,
- Updating access rights and
- Forwarding of information, events and feedback from offline door components (access gained, battery warnings, etc.).

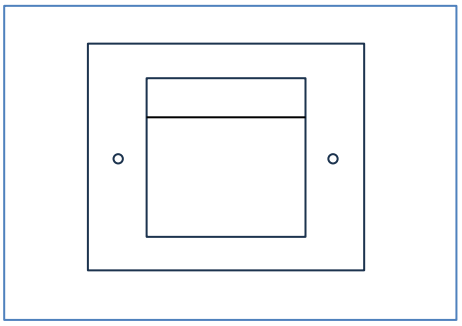
The online update terminal can also control a door opener or a door control unit. This makes it possible, for example, to simultaneously update the access authorisations on the personal locking medium when accessing the secure area for the first time at the start of work.



4.6.5. TECTIQ offline door components

Offline door components enable authorized users to access the secure area. Depending on their function, they allow access, control a door opener or activate a door drive. They also store events and data required for access control.

Wall reader



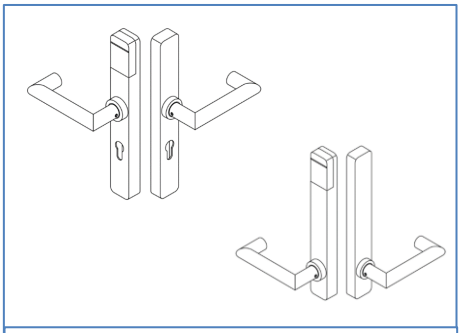
With wall readers, actuators are used to operate

- electric door openers, barriers or gates or
- Motor-driven doors, e.g. for swing doors, sliding doors, revolving doors, turnstiles

after checking the access authorisation.

The release status is signaled via an LED display, and an acoustic signal can also be set to sound when actuated.

Electronic fitting

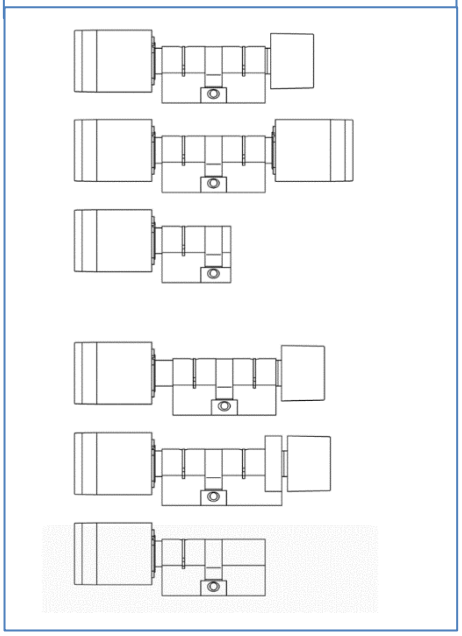


Electronic fittings enable the operation of the handles after checking the access authorisation. They are available in different versions.

Electronic fittings can be operated in combination with a locking cylinder (Euro, round or oval profile), whereby the electronic access control function is mechanically overridden.

The release status is signaled via an LED display.

Electronic locking cylinder



Electronic locking cylinders activate the locking function after the access authorisation has been checked. This allows the authorized person to open and lock the door.

Electronic locking cylinders are available in different versions.

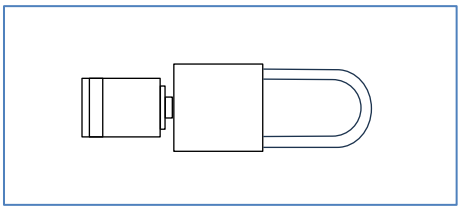
- Euro profile cylinder
- Swiss round profile
- Scandinavian oval cylinder and rococo cylinder

With the electronic locking cylinders, one-sided or double-sided access control is possible.

The release status is signaled via an LED display.

Electronic padlock

- For switch cabinets, machine areas, depots, garages, outdoor EMC areas, barbecue huts, sheds, bicycle chains and much more.
- Project planning and commissioning like an electronic cylinder



4.6.6. TECTIQ locking media

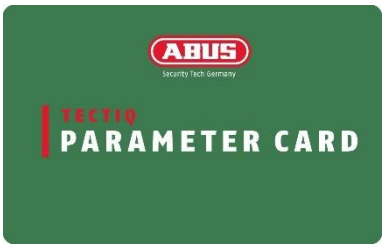
TECTIQ locking media are contactless transponder systems with the particularly secure MIFARE® DESFIRE® system. locking media are available in various forms, e.g. as key fobs or transponder cards.
The user presents their locking medium at the door component or terminal. With the appropriate authorisation, the user can also open an area permanently. This mode is particularly suitable for stores or other buildings with opening hours for customers or the public, for example.

TECTIQ locking media record information on the battery status and other events when a door component is used and transmit this back to the TECTIQ Control during the next update process on the TECTIQ Update Terminal. This ensures that the access control system is kept up to date for all door components.

4.6.7. TECTIQ System media

TECTIQ system media are used for system support and maintenance. They are used for set-up procedures, to prevent unauthorised access and to teach-in or teach-out door components, among other things. They should be stored in a safe place and only used by a small number of authorized persons.

Parameter card



The parameter card saves configuration data and transports it to the door component on site. Both during initial programming and when changes are made, the parameter card is written to with the desktop reader and read out by the respective component on site.
The parameter card is also used to transfer the current time (date and time) to the door component.

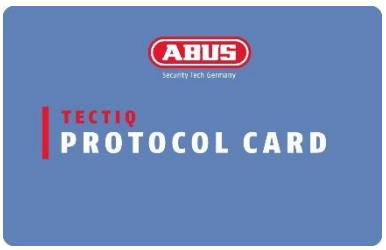
- ▷ To do this, present the parameter card to the desktop reader or to an update terminal if no active programming task is assigned.
- ▷ Then present the parameter card on the door component.

The parameter card is valid for a maximum of 15 minutes after writing.

Reset card

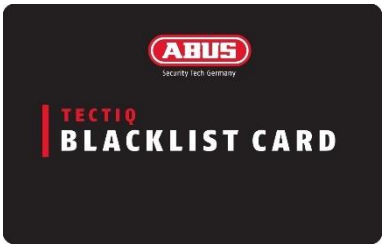
The reset card is used to reset door components in order to remove them from the TECTIQ system. To prevent accidental resetting, a staged presentation to the door component in a specified time sequence is required.

Protocol card



The log card reads log data from the door components. Each TECTIQ door component - fitting, cylinder or wall reader terminal - stores up to 900 entries. These entries include, for example, access granted or denied, battery warnings or battery changes.

Blacklist card



If a TECTIQ locking medium is lost or stolen, it can be blocked against unauthorised use. The blacklist card is used to actively block the locking media in question in the offline door components. Each door component saves its blacklist with entries for blocked locking media.

If required, the blacklist card is loaded by the administrator with the necessary data and presented at each door component concerned. The TECTIQ door components read the blacklist card and update their internal blocking list. This means that access with the blocked locking medium is no longer possible. Blocking must be removed using the blacklist card in order to be able to use a locking medium that has been found again.

An attempted access with a blocked locking medium is saved in the event list of the door component and transmitted to the TECTIQ Control via the use of locking media. The event list is also transmitted to the TECTIQ Control via the log card.

Emergency opening transponder

The emergency opening transponder enables emergency services to gain access to the secured building or area. The emergency opening transponder is usually stored in a fire department key depot at the property. For ease of use, this medium is designed as a transponder.

In an emergency - this is usually an emergency call to the fire department - the operations center activates access to the key depot for the emergency services. The emergency services use the TECTIQ emergency opening transponder to permanently set the respective doors to open status when presenting them. This status must be reset again once the operation has been completed.

When delivered, the emergency opening transponder can be read by all door components and activates or deactivates the "permanently open" status.

4.6.8. Admin App

With the TECTIQ Admin App, you can use a smartphone to maintain the door components. The TECTIQ Admin App transmits data wirelessly to the door components via Bluetooth. It is used, for example

- for synchronizing the time and date after a battery change.
- to update the firmware.

The range of functions of the Admin App is constantly being expanded. You can find the latest details at Abus.com.

You can download the Admin App for iOS or Android from the App Store or Google Play Store.

4.7. System structure

Depending on customer requirements, various expansion stages of a TECTIQ access control system are possible, e.g.

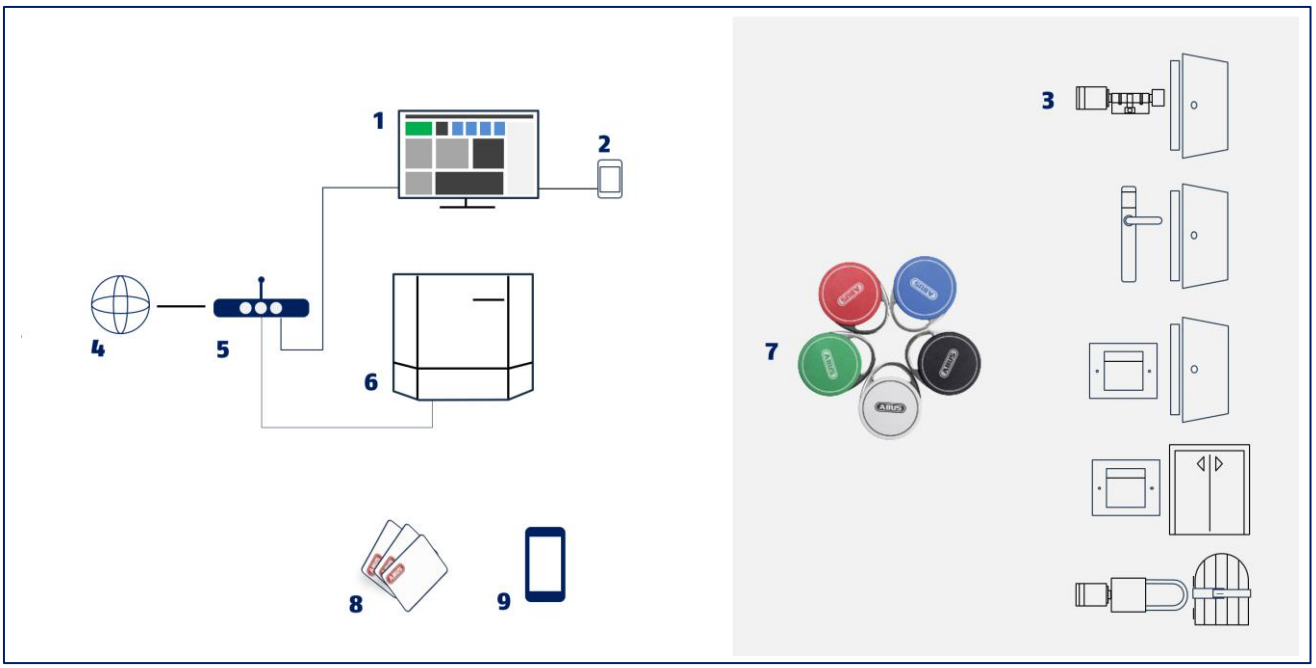
- Simple TECTIQ system without update terminal
- TECTIQ system with update terminal - at one location
- TECTIQ system with update terminals at several locations

	without update terminal	with update terminal
Number of locking media	10 locking media per person	10 locking media per person
Number of system media	25 system media per type	25 system media per type
Across buildings	Yes	Yes
Cross-location	Yes	Yes
Battery status message for door components	Only via LED or protocol card	Via LED, locking media or protocol card
Door component protocols	Only via protocol card	Via locking media or protocol card
Time limit for access authorisations	Yes, via validity of the locking medium	Yes
Automatic extension of access authorisations	No	Yes
Changing access authorisations (temporal, spatial)	Only via Admin on the desktop reader	To update terminal or desktop reader
Blocking access authorisations	Via blocking list (in door components)	Automatically (when authorisation expires) or via blocking list (in door components)
Access	Only on control panel, updating of authorisations required locally on the desktop reader.	Yes

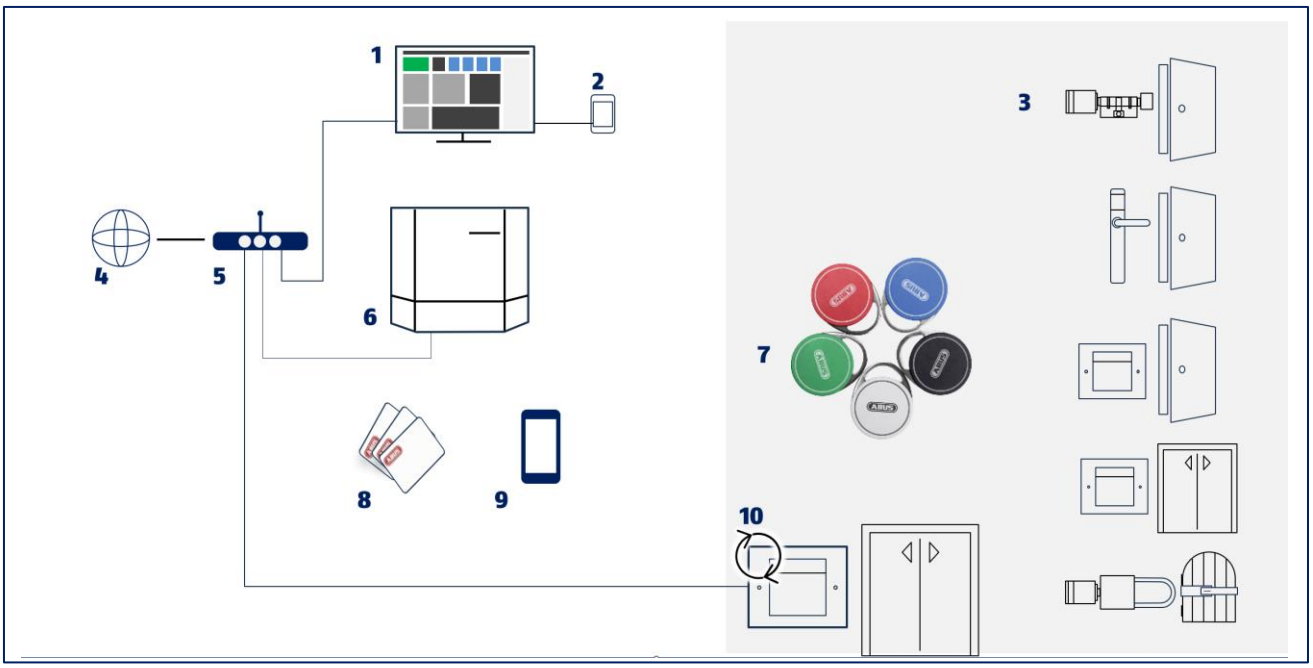
Components of a TECTIQ system
(Legend for the following illustrations)

1 TECTIQ Access Manager
2 USB desktop reader
3 TECTIQ door components, e.g.
electronic cylinder, electronic fitting,
wall reader with door opener,
wall reader with door drive,
electronic padlock
4 Internet connection (optional)
5 IP router
6 TECTIQ Control
7 Locking media
8 System media
9 Admin App
10 Update terminal: Validate access authorisations , Updating access authorisations, read status information (door components)
11 Main building
12 External building
13 Update terminal with online connection to the main system (P2P service)
14 Remote access by admin or specialist installer

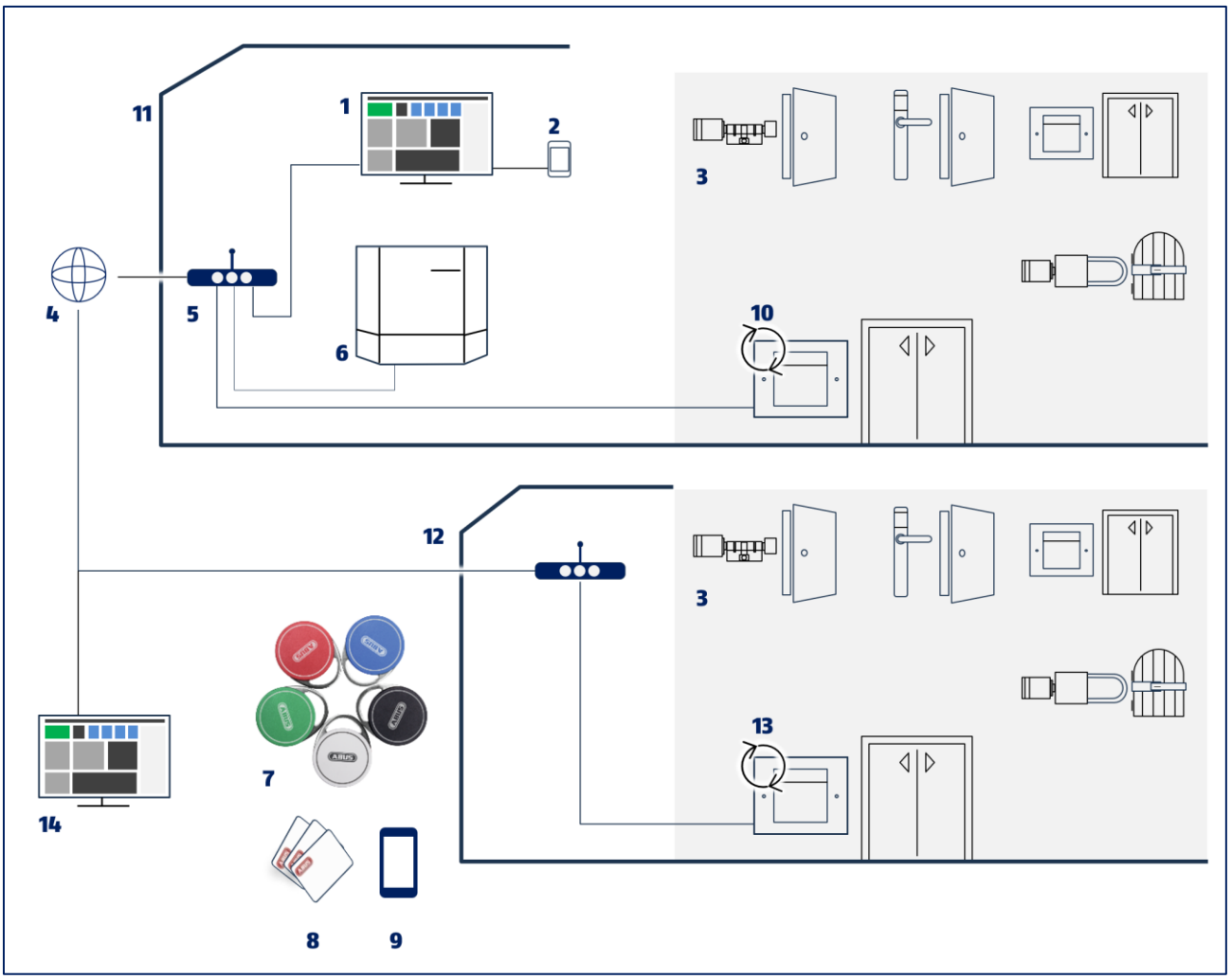
TECTIQ system without update terminal



TECTIQ system with update terminal - 1 location



TECTIQ system with update terminal - multiple buildings or locations



4.8. Technical data

System data

Number of doors	3004 (doors with access control on both sides count as 2 doors)
Number of doors/door groups	1004
Number of door components	max. 3004 (corresponds to the number of doors configured in the Access Manager)
Number of persons	2000
Number of groups of persons	200
Number of terminals	100
Number of schedules	300
Time intervals per schedule	15
Number of blocking days	30 per schedule
Number of system transponders	25 per type / max. 125
Number of administrators	5
Number of locking media per person	10
Number of system log entries	100.000

Door components

Log entries	Max. 900
Blacklist entries	Max. 120

Locking media

Type	ABUS MIFARE© DESFire© (3DES, AES128)

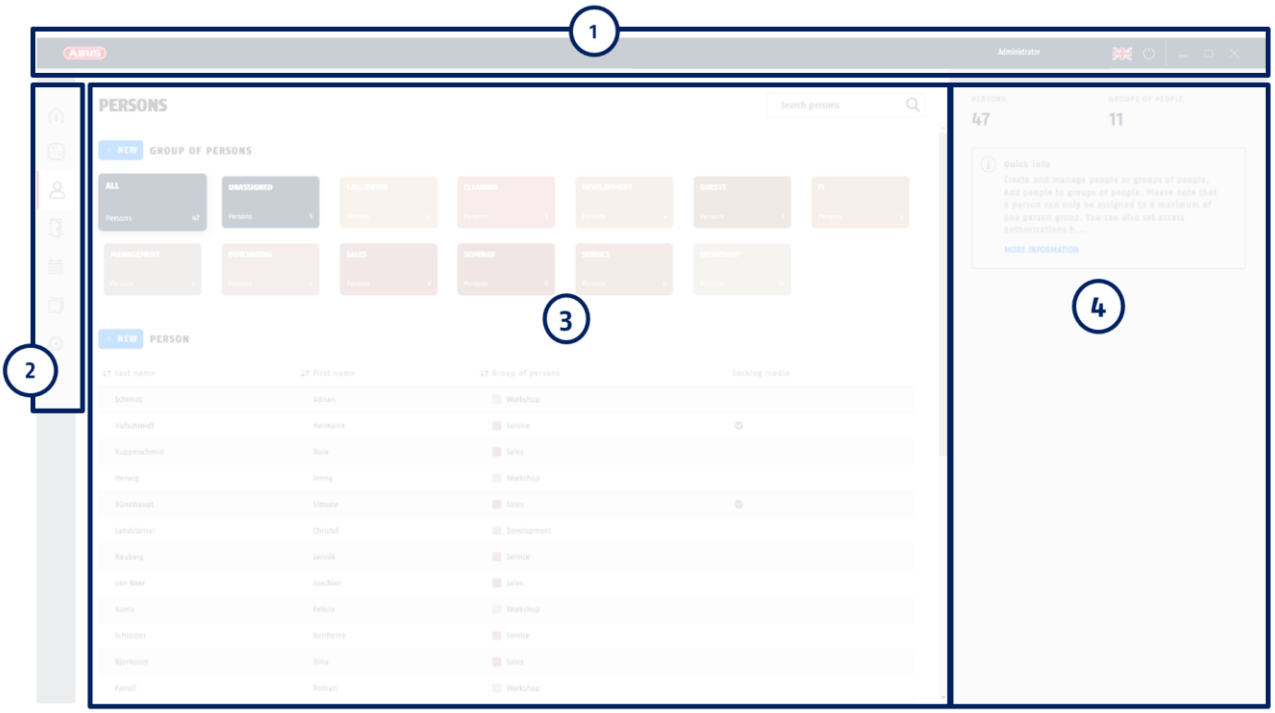
4.9. Where is which data stored?

Door components • Firmware - system and application software • Configuration data - system ID, door, door group • Operating data - access granted or denied, date/time • Block list	**TECTIQ Control** • Firmware - System software • Project data - system ID, network management, doors, door groups, door components, persons, person groups, locking media, system components, locking plan, locking list, schedules • data • Firmware for components
Locking media • Door authorisations • Validity of the authorisations • Validity of the locking medium • Schedules • Authorisations for permanent opening • Transmitted log data (temporary)	**System media** • All cards: system ID, validity (15 minutes) • Blacklist card: blacklist • Parameter card: Programming data for locking medium • Log card: Log data of a door component • Reset card: Authorisation to reset a specific door component
Update terminal • Updated access authorisations • Validity period in case of connection failure • Transmitted log data (temporary)	**Admin App** • Firmware updates for door components • Functionality will be expanded in the future, e.g. authorisation for parameterisation by administrators and ABUS specialist dealers
TECTIQ Access Manager • Application software • Data backup files (backups, encrypted)	**ABUS online account** • ABUS specialist partner / contact • Operator / Email contact

5. TECTIQ Access Manager - Interface

Contents

5.1. TECTIQ Access Manager - Interface



1 Title bar 2 Menu bar 3 Work area 4 Editing area

Title line (1)

The title bar shows the language selection and a button for logging out of the system as basic elements.

Menu bar (2)

In the menu bar, select the view for your activities. The selected view is displayed in the workspace.

Front page / Dashboard	View Doors	View
locking plan view	View schedules	
Persons view	System components view	

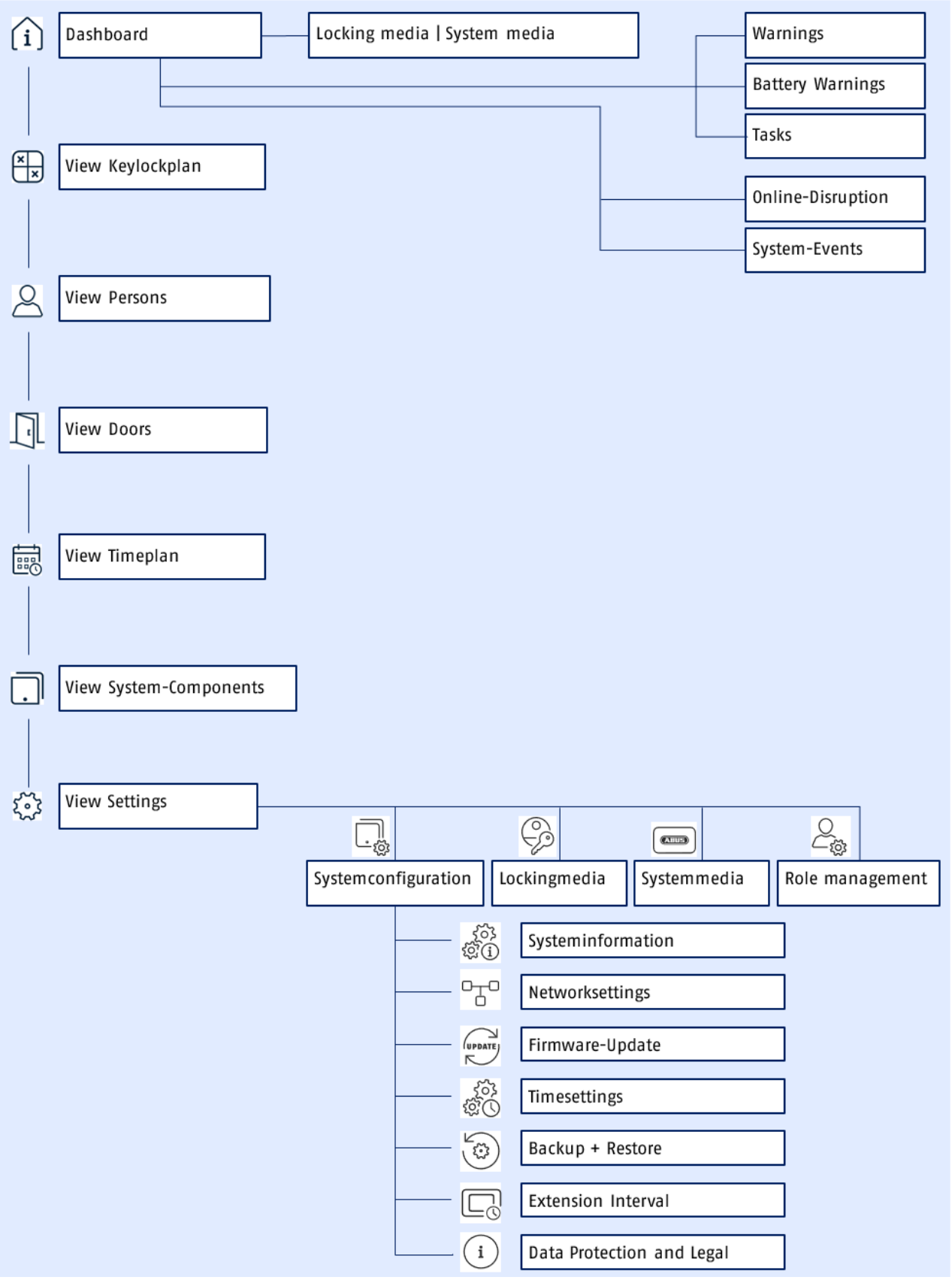
Work area (3)

Most of your activities take place in the work area. Depending on the activated view, you will find your tools for managing doors, TECTIQ door components, persons, locking plans and settings here.

Editing area (4)

The content of the editing area depends on the selected view and the respective activity in the work area, where you will find informative texts about program functions and enter data about your locking system and its users.

5.2. Menu structure



6. Main menu | Dashboard

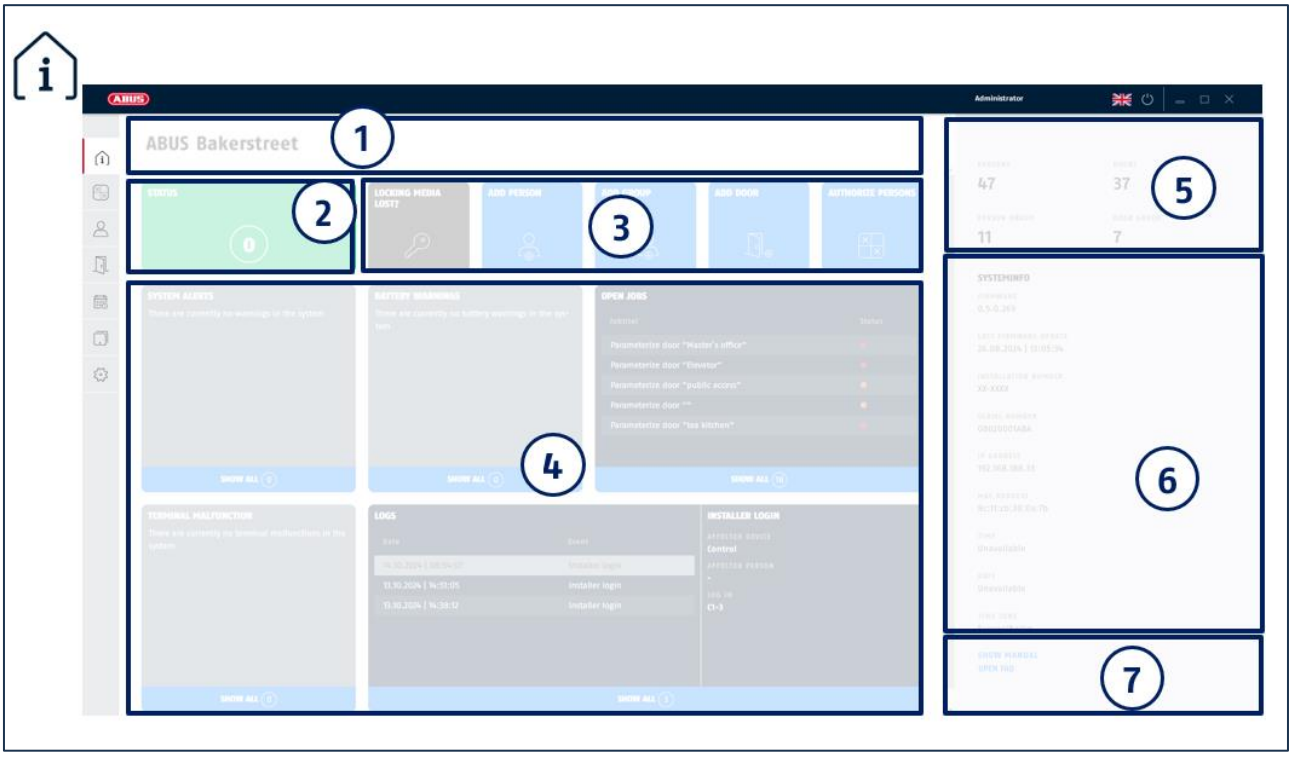
Contents

6.1. Main menu overview

The main menu - or dashboard - is displayed after starting the program and logging into the system. You can access the main menu from other views via the button. Here you have an overview of

- the current system status,
- important system events,
- open tasks (e.g. necessary battery changes),

The main menu/dashboard gives you quick access to the most important functions and takes you directly to the relevant submenus.

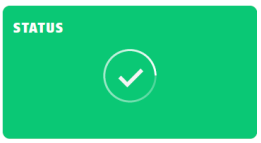


1 Plant name
2 Collective message
3 Shortcut keys
4 Lists & shortcut keys
5 Current system utilization
6 System overview
7 Links, FAQ

6.2. Collective message system status

The collective message about the system status provides a quick overview of the system status and immediately signals any activities required by the system operator.

Green: No acute message.



Orange: System message

- Software updates
- Battery warnings

Red: Connection error to an online terminal

6.3. Hotkeys | Shortcuts

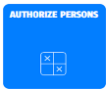
The shortcut keys in the top row take you directly to the selected function:

"locking media lost or stolen?"
Continue to the "Block locking media" menu

"Add person": Go to the "Persons" menu | Add new person

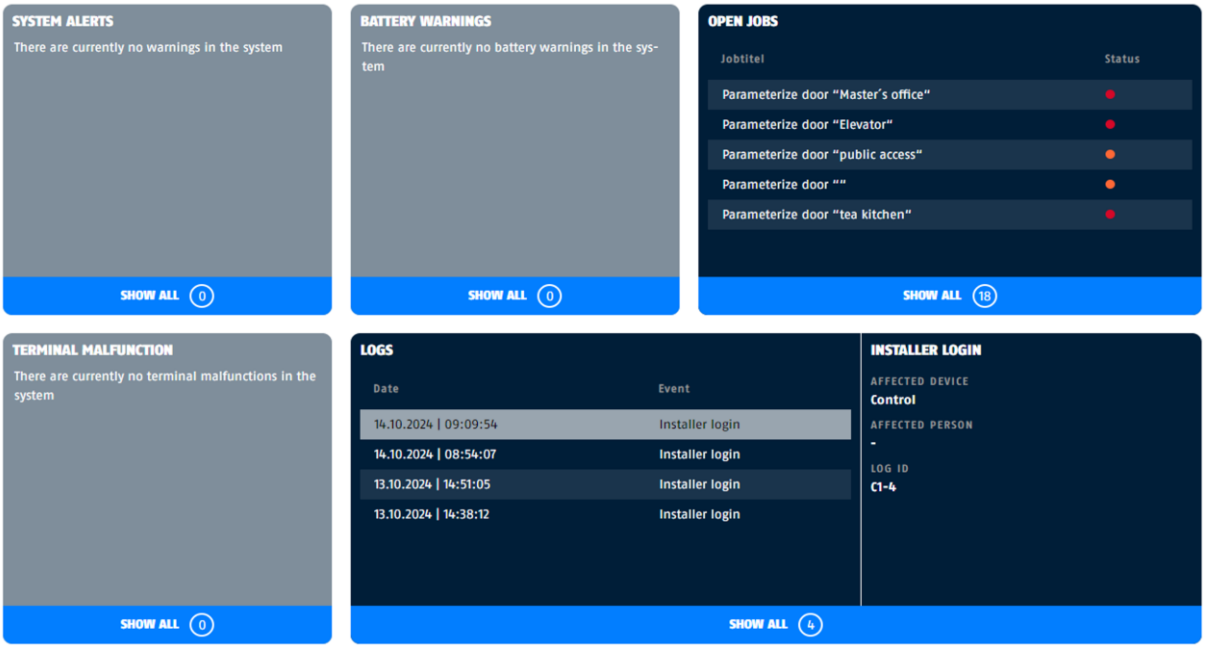
"Add group": Go to the "Persons" menu | Add new group

"Add door": Continue to the "Doors" | Add door menu



"Change authorisations ": Continue to the "locking plan" menu

6.4. Listen & shortcut keys



The list fields show the last status messages. Clicking in the blue field takes you to the editing view of the selected list, where messages can be selected, displayed and edited. The dashboard shows

- System warnings:
  System-related messages, e.g. firmware update for door components or faulty internet connection.
- Battery warnings:
  Messages about door components whose battery level has fallen below the first warning message.
- Open tasks:
  Messages about tasks to be completed in the system, e.g. required settings, parameterizations or updates.
- Terminal connection problems:
  Messages about disrupted connections to online terminals. The relevant door function is not affected in this case; access authorisations in TECTIQ locking media continue to be updated on site for up to 72 hours.
- Events:
  Information on personal and system-related events

6.5. Loss of a locking medium

The TECTIQ access control system offers the highest possible protection against unauthorised access to the secured area. By setting a short validity period for access authorisation on the TECTIQ locking medium, the duration during which unauthorised use is possible is reduced to a minimum.

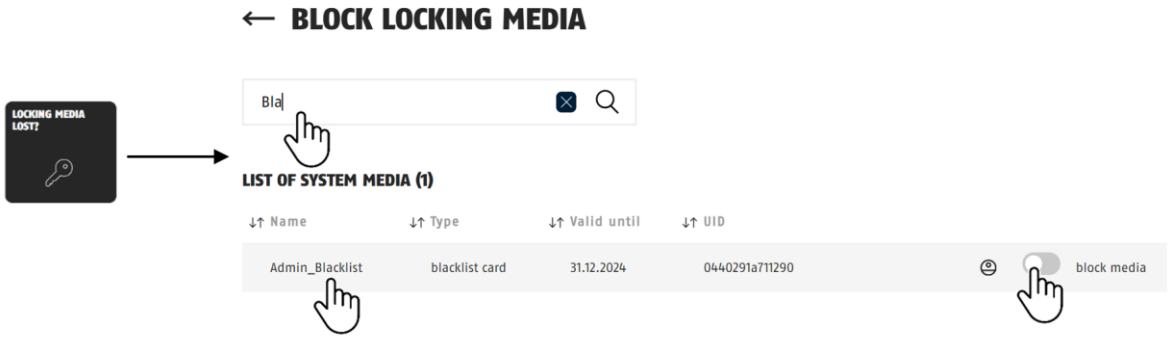
However, if a locking medium is lost, measures must be taken immediately to prevent the risk of unauthorised use. Therefore, give instructions that the administrator is informed immediately of the loss of a locking medium.

The locking medium must be blocked immediately by the administrator in TECTIQ Access manager. Deletion of the locking medium is not possible for security reasons. After expiry of the validity and blocking of the locking medium in the TECTIQ Control, access to the secured areas is no longer granted. Unauthorised access attempts are logged in the event list.

Blocking a locking medium has several effects:

- Regular updating of the access authorisation for this locking medium is prevented.
  This ensures that this locking medium cannot be misused once it has expired at the latest.
- The changed access authorisation is immediately available in the existing online terminals. This means that as soon as the locking medium is presented to one of these components, the validity on the medium is deleted.
- The blacklist in the TECTIQ Control is updated and must be saved as quickly as possible in all affected offline door components. A blacklist card is required to transfer the blacklist to the door components.

The same applies to blocking a system medium: The system medium in question is actively excluded from the system and no longer has any function.



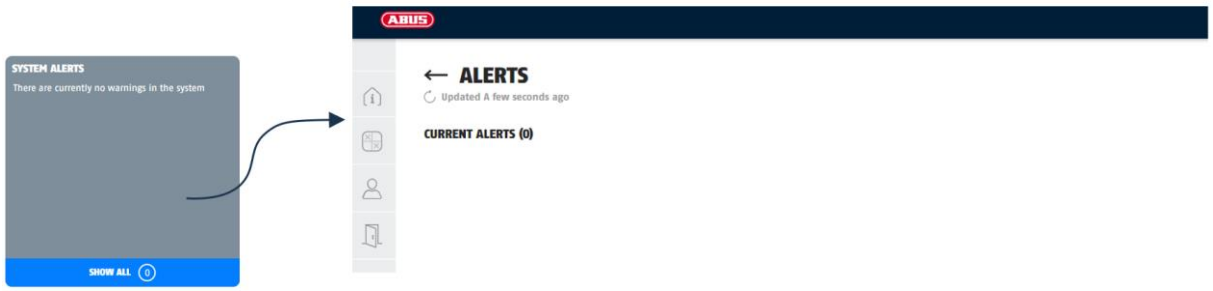
Selecting the "locking media lost or stolen?" button opens the "Lock locking media" window.
Enter the name of the relevant locking or system medium in the input field. The program displays matches immediately.

▷ Use the slider with the mouse pointer to lock or unlock the medium.

Please note: Blocking or unblocking only becomes effective in the offline door components once the blacklist has been transferred to the door components using the blacklist card!

6.6. System warnings

Clicking on the blue area in the "System warnings " list box takes you to the "Warnings" submenu. Current warning messages stored in the system are displayed here. The list can be sorted by column in ascending or descending order.



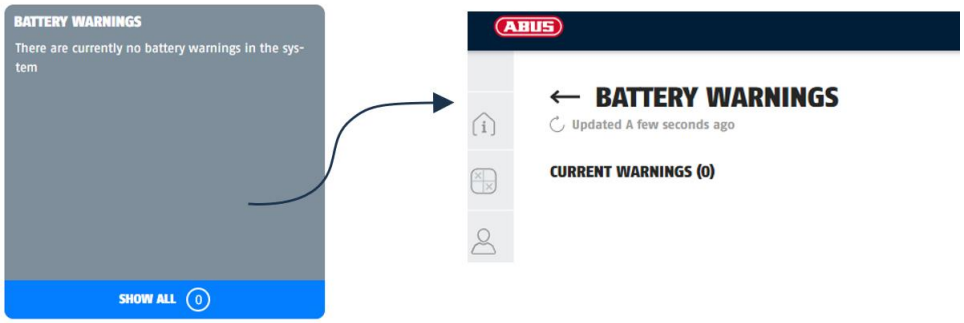
The following warning messages are displayed in the "Warnings" window:

Warning message	Meaning	What to do:
Firmware update available	Updated software is available for the specified device.	Install the updated software for the specified device.
Internet connection lost	The TECTIQ Control is no longer connected to the Internet. Connections to other locations may be interrupted (see also the separate message)	Log out of the Access Manager. Check that the network cables are correctly seated. Restart the TECTIQ Control if necessary. If there is still no IT connection, inform your IT department or contact your ABUS dealer.

Warning messages are stored in the event list after the firmware has been rectified or installed.

6.7. Battery warnings

Clicking on the blue area in the "Battery warnings " list field takes you to the "Battery warnings" submenu. Door components that have reported a low battery level are displayed here. The list can be sorted by column in ascending or descending order.



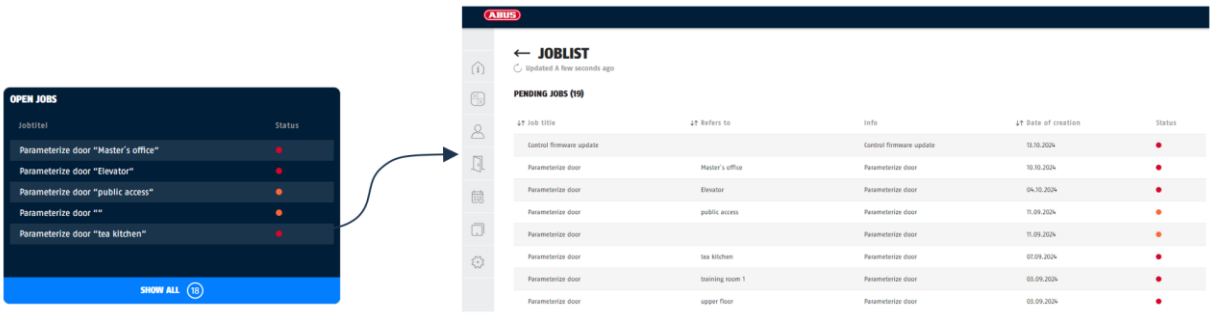
Clicking on a battery warning displays details and the relevant door component in the editing area

- ▷ Replace the batteries in the door components as soon as possible!

Battery warnings are moved to the event list after the battery has been replaced. Please note that the new status is only transferred to the access control system after using a locking medium and subsequent validation. A possible time delay has no influence on the function of the system.

6.8. Open tasks - task list

Clicking on the blue area in the "Open tasks" list field takes you to the "Task list " submenu. Tasks that require intervention by the system operator are displayed here, e.g. parameterizing new door components. The list can be sorted by column in ascending or descending order.

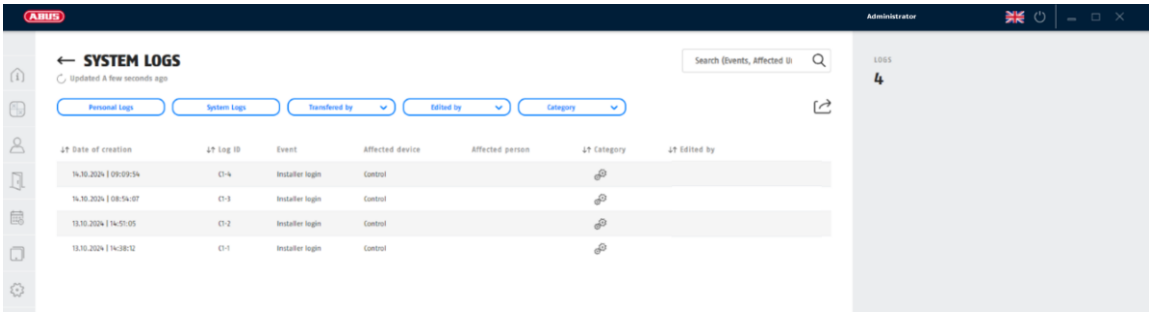


6.9. Fault messages

Disrupted connections to online terminals are displayed in the "Terminal connection faults " list field. The relevant door function is not affected by this. Access authorisations in TECTIQ locking media continue to be updated - up to a maximum of 72 hours after the fault occurs - based on the locally stored data.

6.10. Events

The event list shows you clear information on usage and system maintenance. Messages about events such as granted or denied access attempts, software updates, writing to locking media, adding or deleting door components are displayed. This gives you a quick overview of whether unusual processes have been detected in the system.
Events are displayed by default in the order in which they occur and can be sorted according to various criteria.



7. View locking plan | Keylock plan

Contents

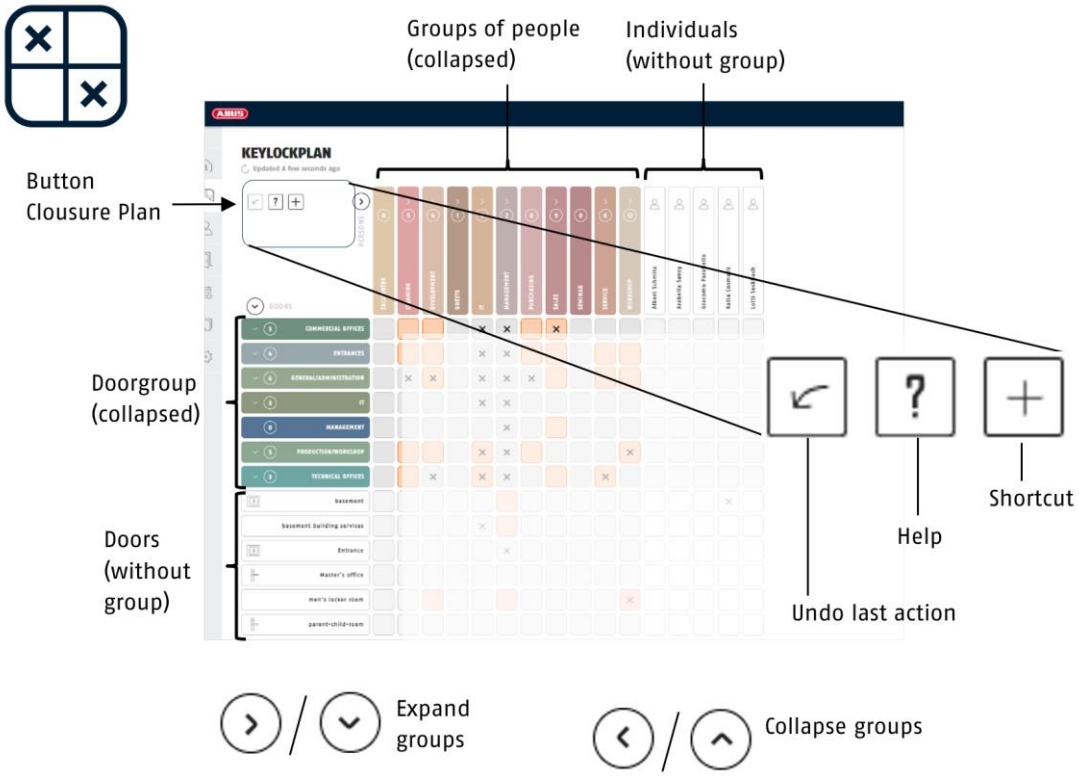
7.1. Overview

The locking plan clearly displays the current authorisations for persons and the permitted doors.

Here you can

- Granting persons and groups of persons access authorisation to doors or groups of doors
- Change access authorisations
- Withdraw access authorisations

You can access the locking plan via the button locking plan. Here, the persons and groups of persons are arranged horizontally and the doors and door groups vertically. Groups of persons and door groups are initially displayed collapsed but can be expanded individually or collectively at any time.



Collapse/expand groups

Within the locking plan, expand the door or person groups by clicking on the ⊙ or ⊙ symbol for the respective group.

If a door component is already assigned to a door, this is displayed as an icon next to the door designation.

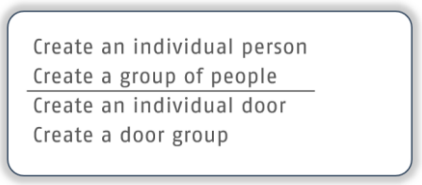
Function keys

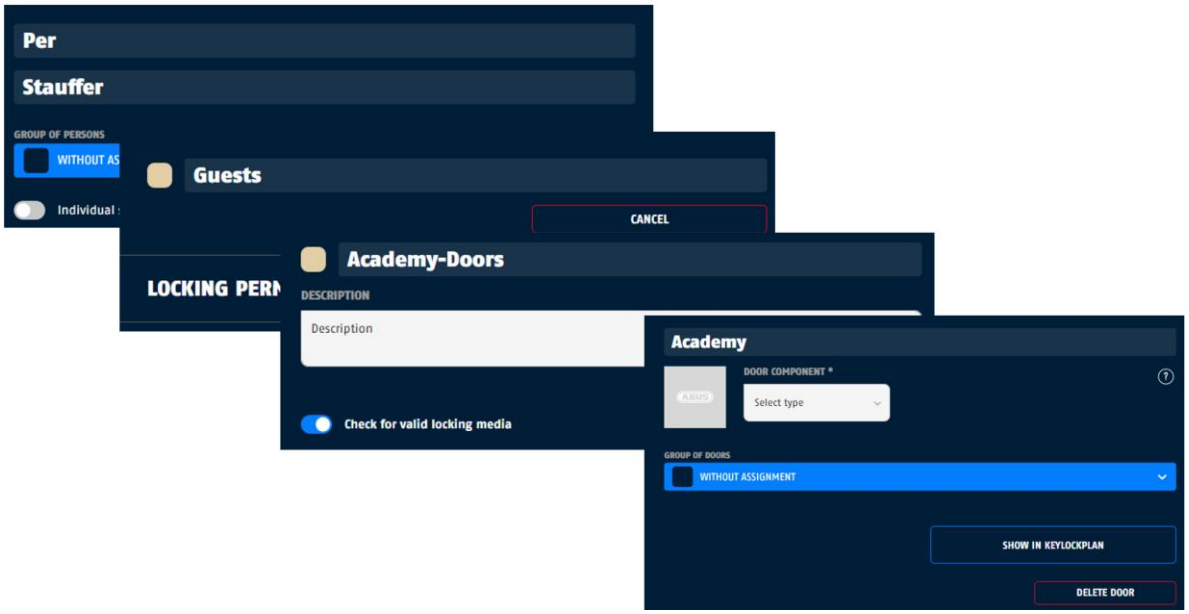
Three function buttons allow quick access for convenient and safe working:

↩ Cancels the last changed access authorisation (up to 5 steps).

? Displays a help text.

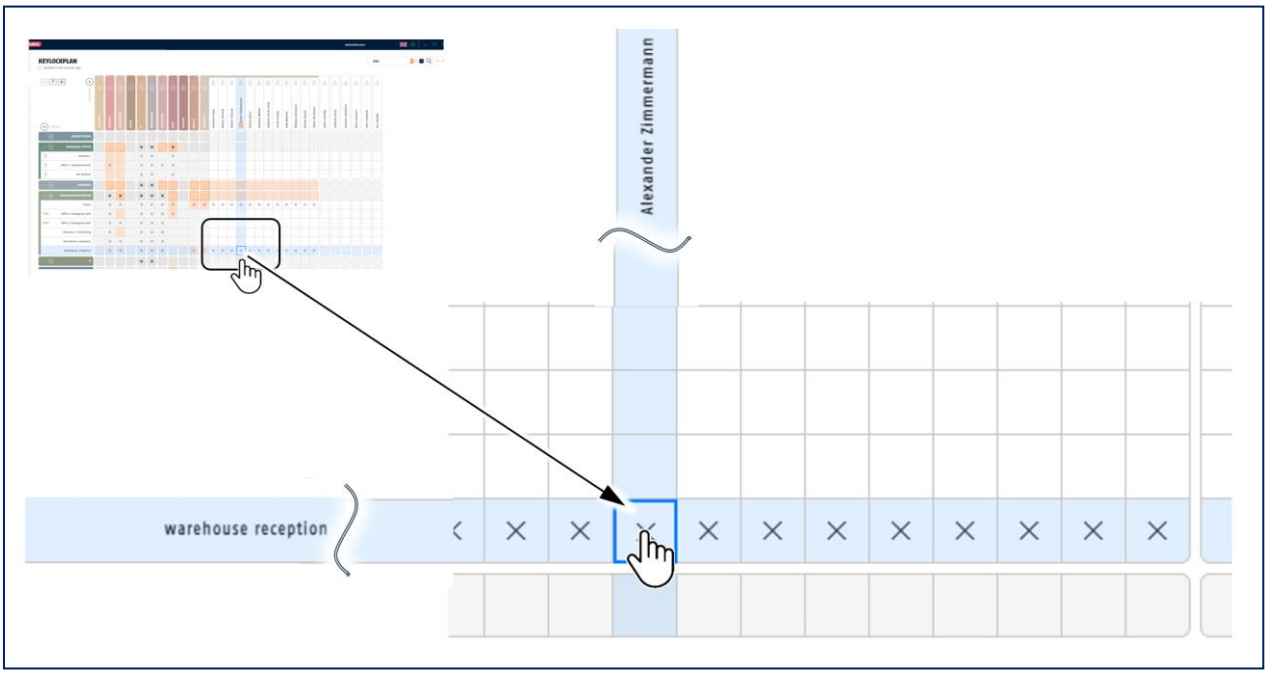
\+ Quick button: This can be used to quickly create **persons**, groups of persons, doors or door groups without leaving the locking plan.





7.2. Representation

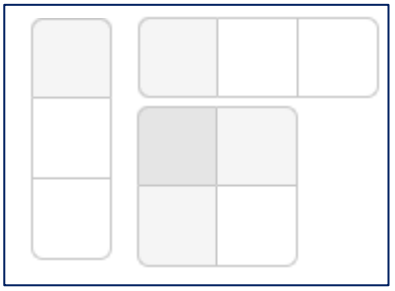
Persons and doors are shown in the locking plan in the form of a matrix. Persons groups and door groups are grouped together in blocks that can be expanded or collapsed under the respective group name. The first row or column contains the group name and is highlighted in a different color from the other cells. The current mouse position within the locking plan and the assignment in terms of person and door is highlighted in blue.



Authorisations in the locking plan

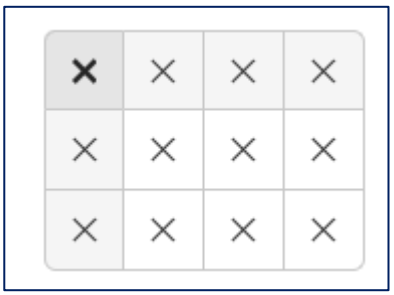
- White fields in the locking plan symbolise an individual door / person.

- Gray fields indicate the headers/columns of door groups or groups of persons.

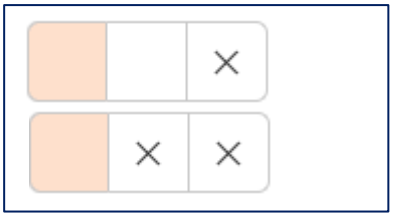


- A× indicates that a person is actively authorized to access a door.
- A× within a grey field indicates a group authorisation.

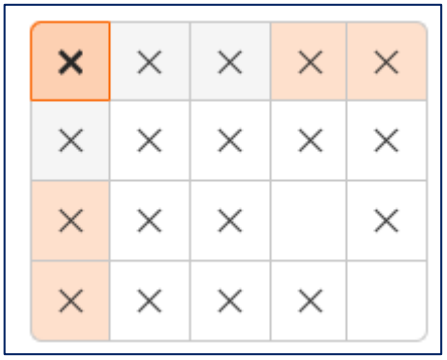
- A bold× means that the group authorisation applies to the entire block (both for the door group and for the group of persons). New doors or persons for a group inherit the group's preset authorisations .



- Orange fields only appear in the header rows/columns. They indicate whether authorisations have been individually changed - granted or revoked - in a door/person group.



- An orange field with a bold× in the locking plan matrix indicates that group authorisations are preset for the complete block of door and person groups, but individual deviations are set for individual elements.
  New doors or persons that are added to the group initially receive all group authorisations . The authorisations can then be adjusted individually.



7.3. Individual access authorisations

Individual access authorisations always apply to the selected person or door. Authorisations can be granted and revoked individually for a person or door.

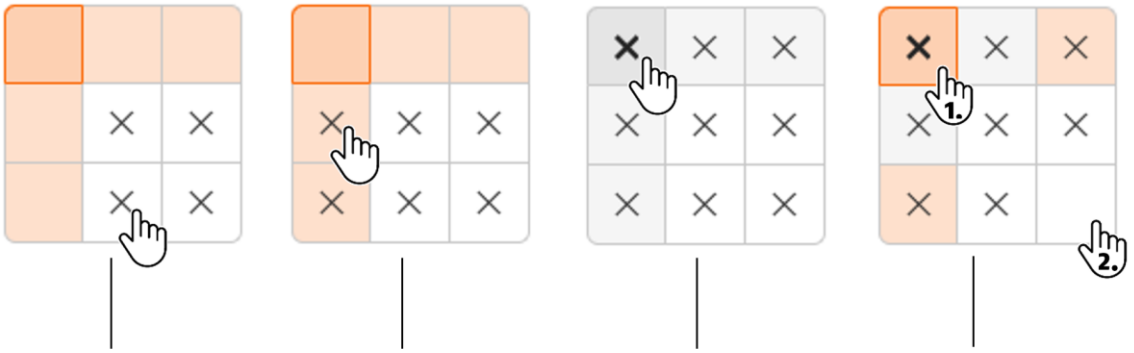
7.4. Group authorisations

Group authorisations apply to all doors or persons within this group. A group authorisation is granted or withdrawn for all doors/persons contained.

Group authorisations are inherited when new elements are added to the group.

After a group authorisation has been granted, the authorisations for individual doors/persons can be changed individually. These changes do not affect the default settings of the group - or the other elements of the group.

The possible input variants are summarized again below:



All authorizations have been granted individually. No cross in the orange group

Group authorizations have been granted for persons (crosses in orange fields). Authorizations were granted individually for doors.

All authorizations have been granted as group authorizations for the entire block. Cross top left.

Authorizations were granted as group authorizations for the entire block (1). An authorization was then withdrawn individually (2).

In the first 3 cases, the currently issued locking authorisations are the same. However, the default settings differ when a new door or person is added.

7.5. Granting access authorisation

- ▷ Grant access authorisation by ticking the relevant person and door.

Access authorisations can also be issued for complete groups of persons and doors. Existing group authorisations are inherited by the persons and doors they contain.

7.6. Withdraw access authorisation

- ▷ Revoke an individual access authorisation by removing the cross× for the person and the door in the locking plan.
- ▷ Revoke access authorisations for complete groups of persons and door groups by removing the cross**×|**× for the complete group in the locking plan.

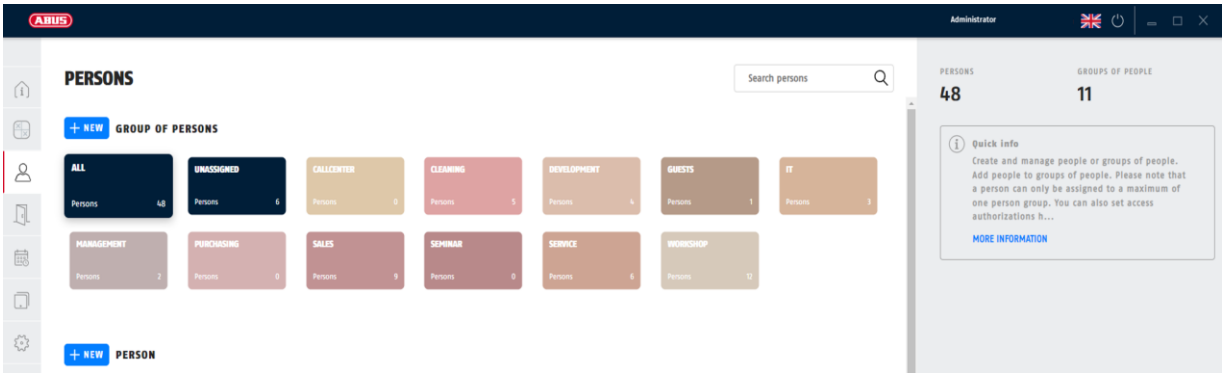
8. Persons overview | Persons

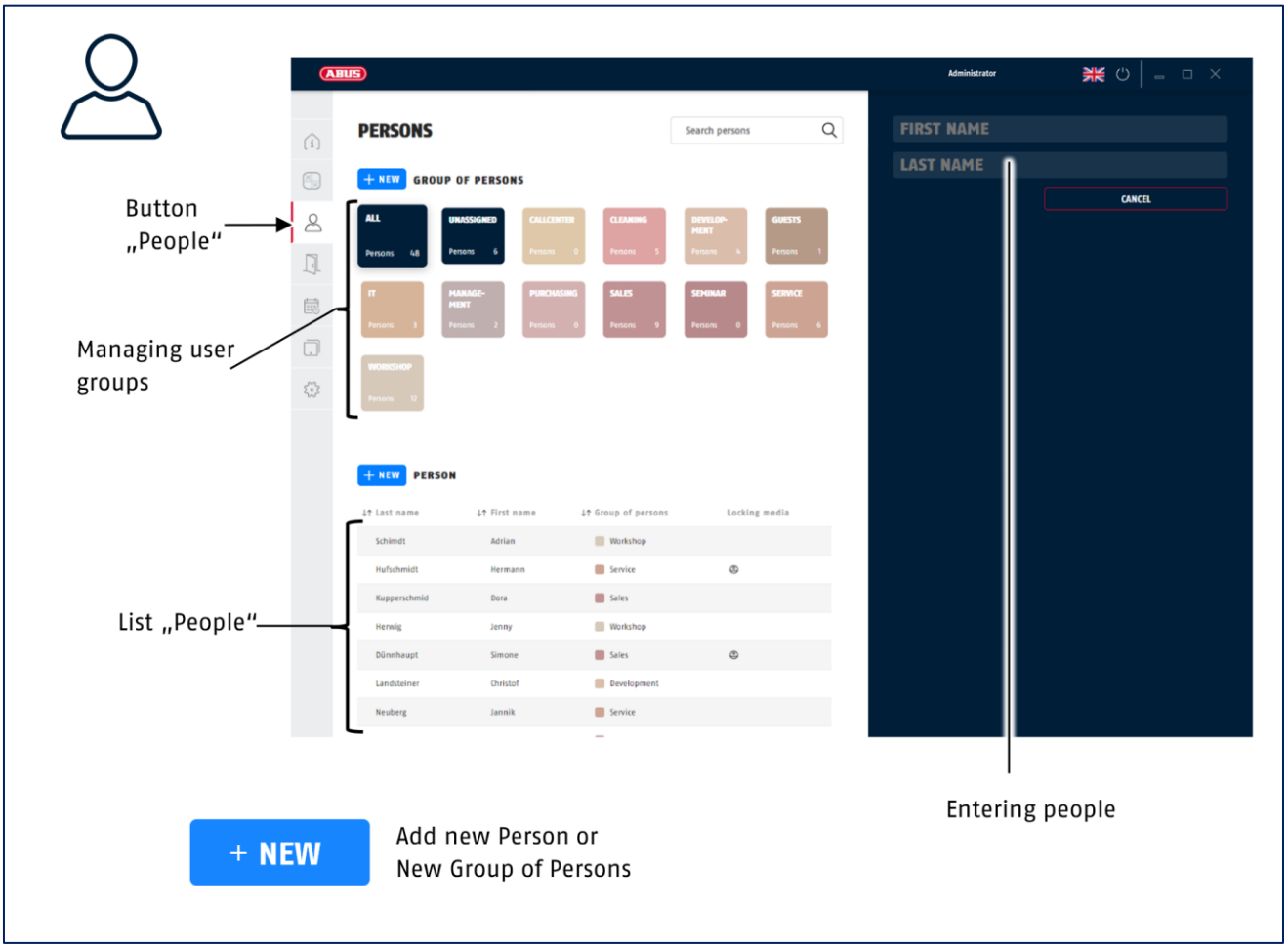
Contents

8.1. Overview

In the Persons overview, you can create and manage persons and assign locking media to them. For better orientation, combine persons with similar authorisations into groups of persons. A person can be assigned to a maximum of one person group.

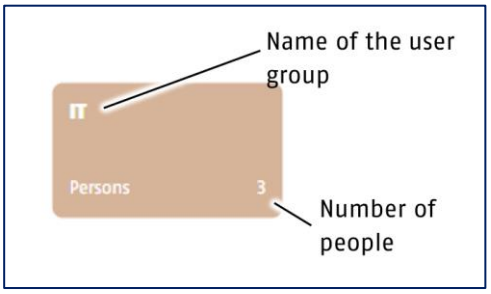
You can access the Persons view via the button.





8.2. Groups of persons

Groups of persons make it easier to manage a locking system. A group of persons can be granted or withdrawn access rights collectively and schedules can be specified. The settings of the person group are inherited by persons, but can always be customised for individual persons.

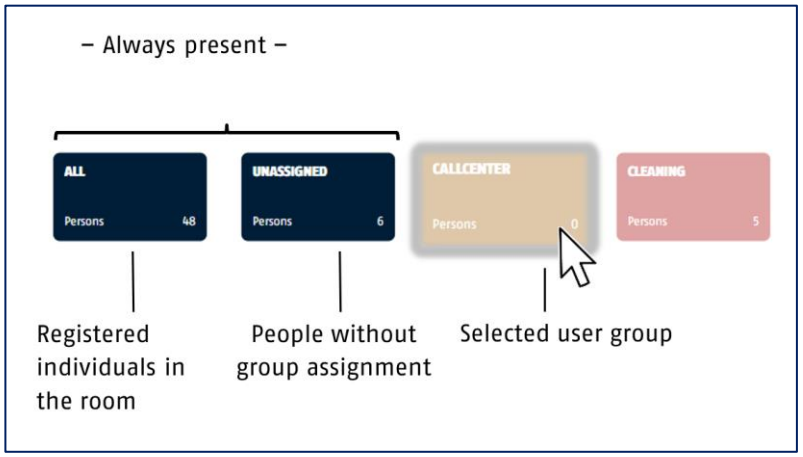


In the upper part of the Persons view, the groups of persons are displayed as tiles with the name and number of persons assigned to them.

The "All persons" and "Not assigned" tiles are always available.

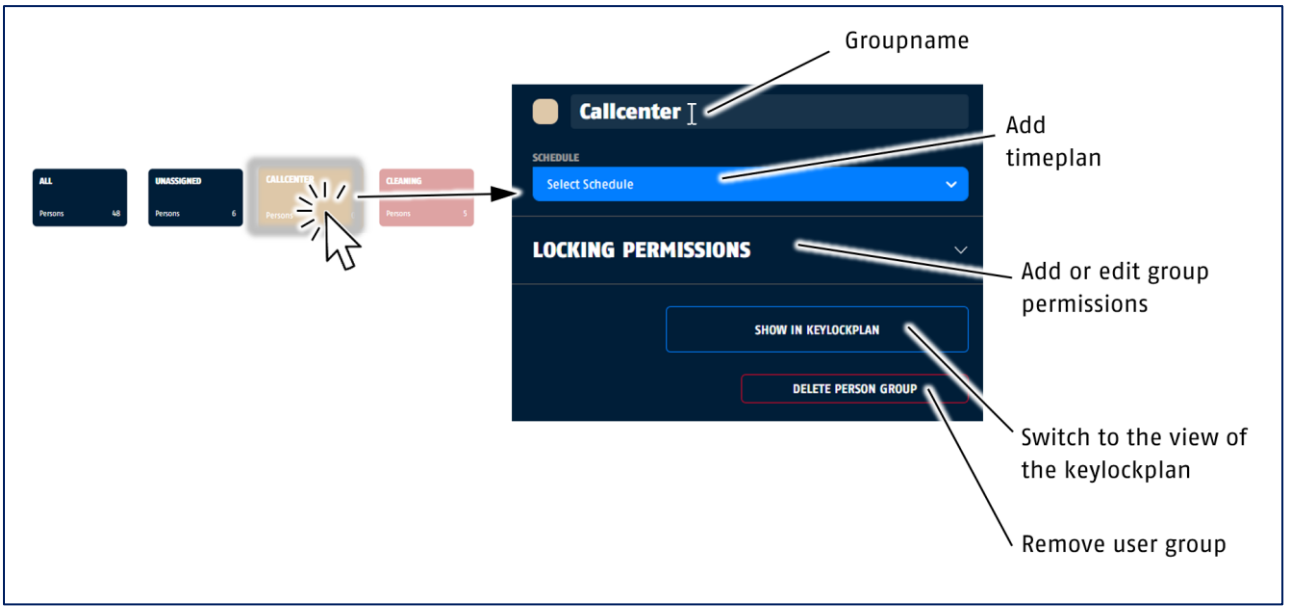
A group of persons is selected by clicking on it. The selected group of persons is highlighted.

After selecting a group of persons, the persons contained are displayed in the list of persons.



8.3. Properties of groups of persons

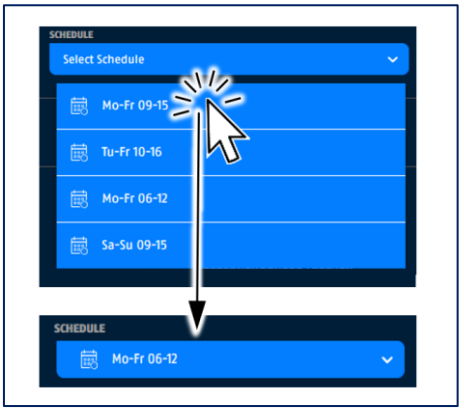
Assign additional properties to groups of persons.



Edit group name

You edit the group name by placing the insertion point in the window with the mouse pointer and making your changes.

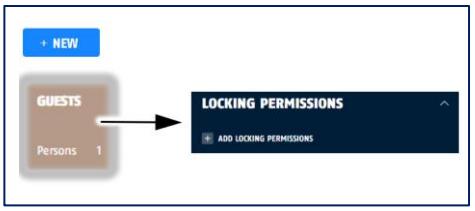
Add schedule



Assign a previously defined schedule to the group of persons by opening the list under "Schedules" and clicking on the desired schedule.

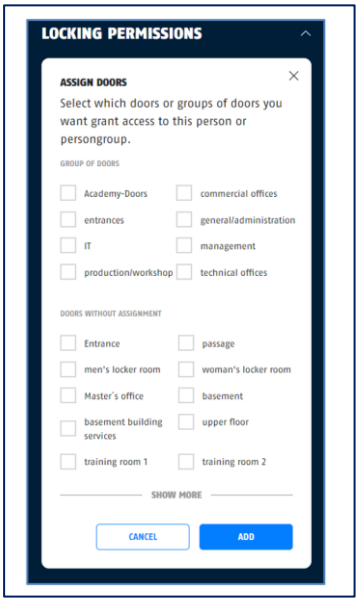
You create schedules in the Schedules view.

Edit group authorisation



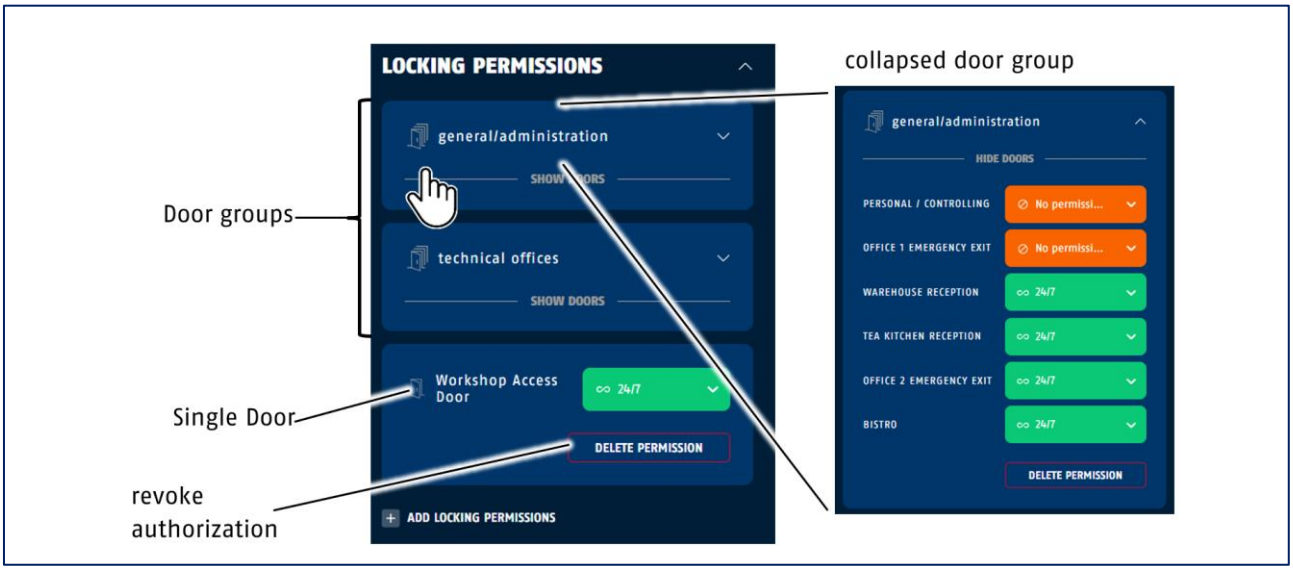
To edit the group authorisations , open the Locking permissions menu.

Here you can see the access authorisations currently granted for door groups and individual doors - with or without schedules.
The view varies depending on whether the group has already been granted authorisations or not.

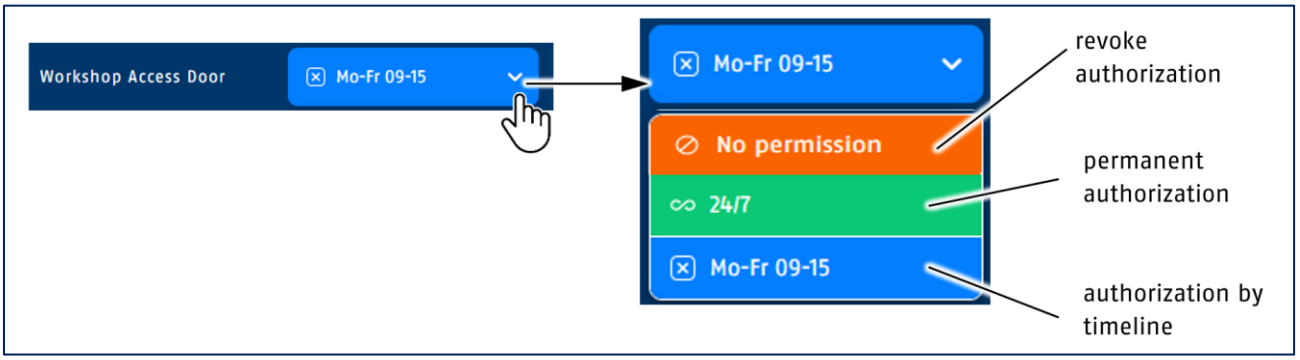


You can add access authorisations without switching to the locking plan view.

If the group of persons has already been granted authorisations , a list with the assigned door groups and individual doors appears when you expand the list.
Door groups expand when clicked and the authorisations of the individual doors become visible.



You can assign authorisations for each door permanently, within a schedule or revoke an authorisation that has been granted.

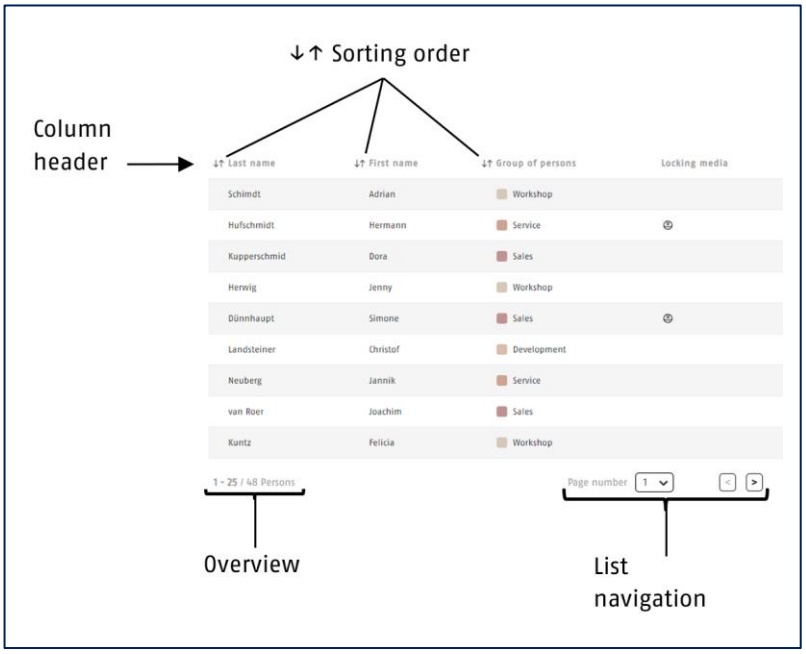


8.4. Persons

Persons are displayed in the list of persons.

The list includes

- Surname,
- First name,
- the assigned group of persons and
- the assigned locking media.



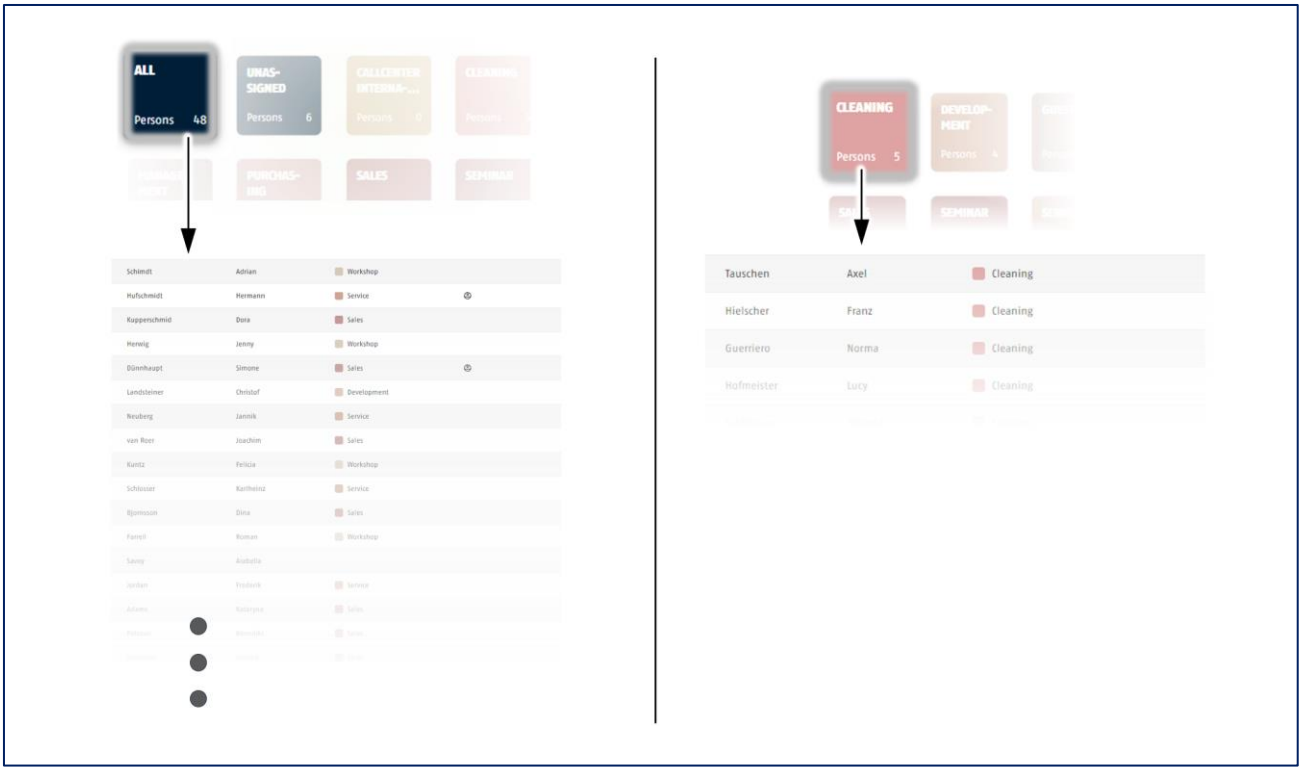
Sort persons

Sort persons by clicking on the corresponding column heading. The sorting is displayed and changes each time you click.

↓↑ in the order of entry
🡻↑ sorted alphabetically in ascending order 0...9 / A...Z
↓🡹 sorted alphabetically in descending order Z...A / 9...0

Restrict displayed persons

Restrict the display to a group of persons by clicking on the corresponding tile.

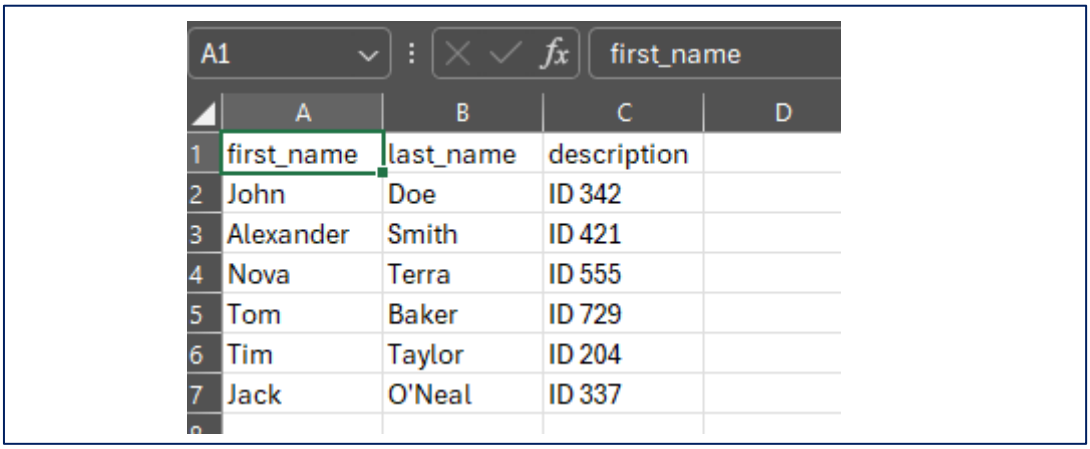


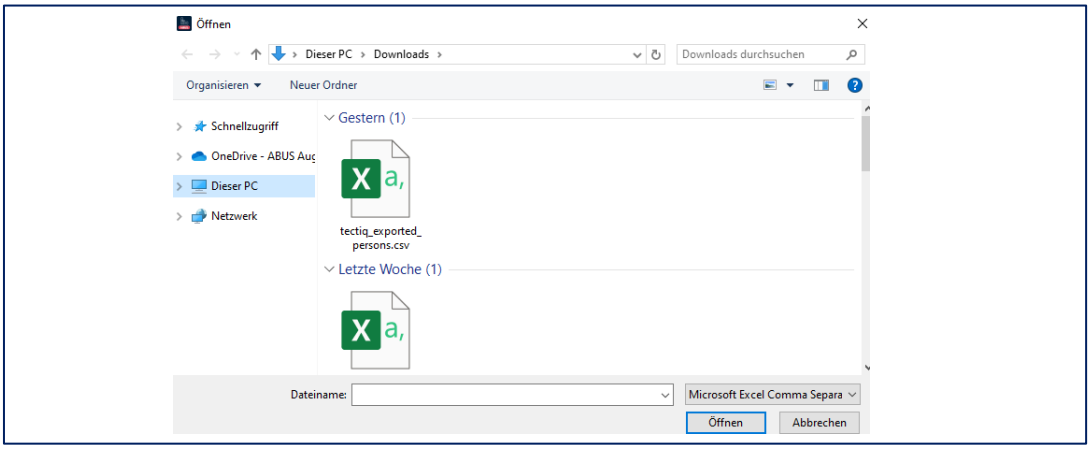
Import and export persons via.csv

Persons can be imported via.csv file to speed up the manual entry of names.
The 3 dots in the list of persons can be used to select whether an import or an export is to be carried out. A list can be exported as a template for this purpose.

ⓘ The file is output in CSV format. To display the file correctly, the UTF-8 format must be selected when opening the CSV file. locking media cannot be exported or imported.

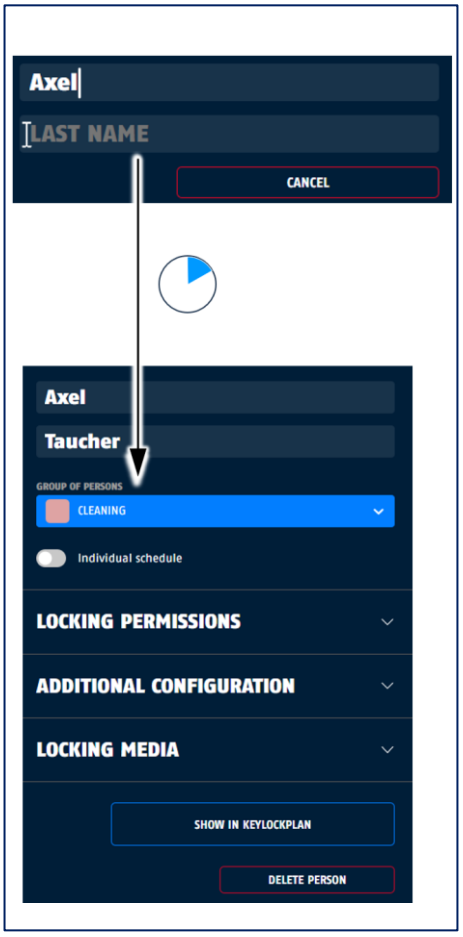
The following fields can be filled in the.csv file and imported into the system. "first_name" for the person's first name, "last_name" for the surname and "description" for the description field with further information about the person, such as a personnel number.





The import function checks for duplicates and filters them out. New entries are added to the end of the list of persons. The function can therefore be used to set up the system initially as well as to add persons later.

8.5. Properties of persons



Add new person

Add a new person by clicking on the "+ NEW" button above the list of persons.

You can enter a first name and a surname in the editing area. The entry is automatically accepted if the access control panel has recognized a surname. As soon as the entry has been accepted, further input options are made available.

You can edit the properties of persons at any time.

Edit personal name

You edit personal names by placing the insertion point in the window and making your changes.

Assign a group of persons

When assigning a group of persons, the person receives the access authorisations that are set for the group. Existing individual authorisations may have to be reset.

Groups of persons can be assigned in different ways.

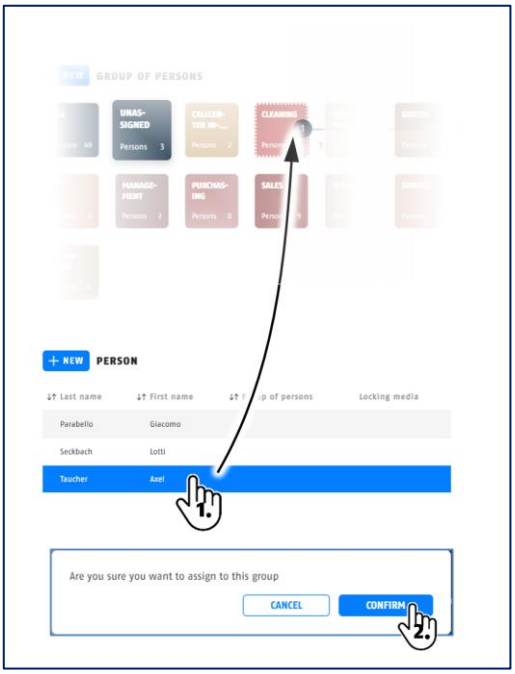
- Select a person group before creating the new person

or

- Expand the "Person group" list in the editing area and assign the desired person group

or

- Drag and drop the person from the person list to the desired person group.



Add an individual schedule

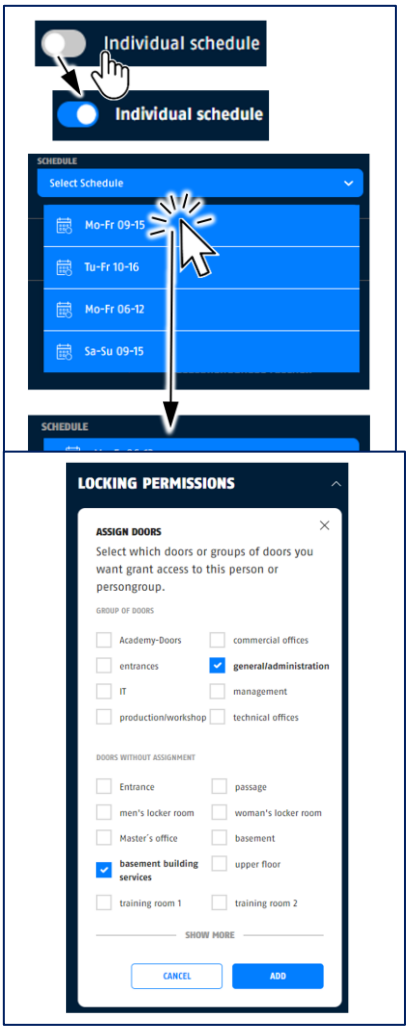
Assign the person a predefined schedule:

- ▷ Press the "Individual schedule" button.

The "Schedule" list box appears.

- ▷ Open the "Schedules" list and click on the desired schedule.

If the required schedule does not yet exist, create it in the Schedules view.



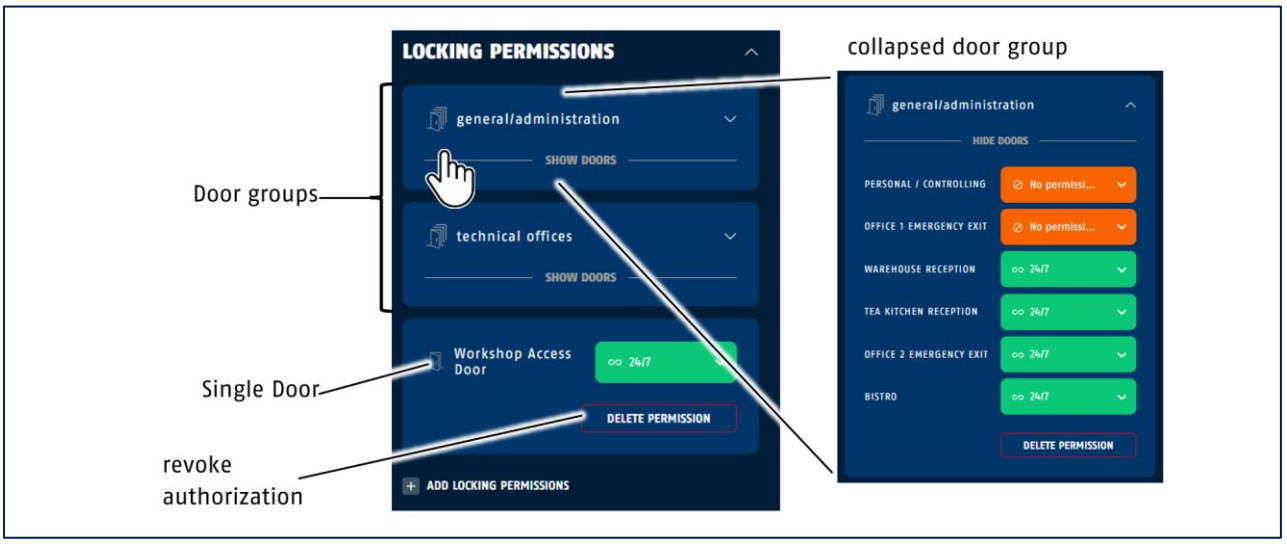
Change individual authorisations

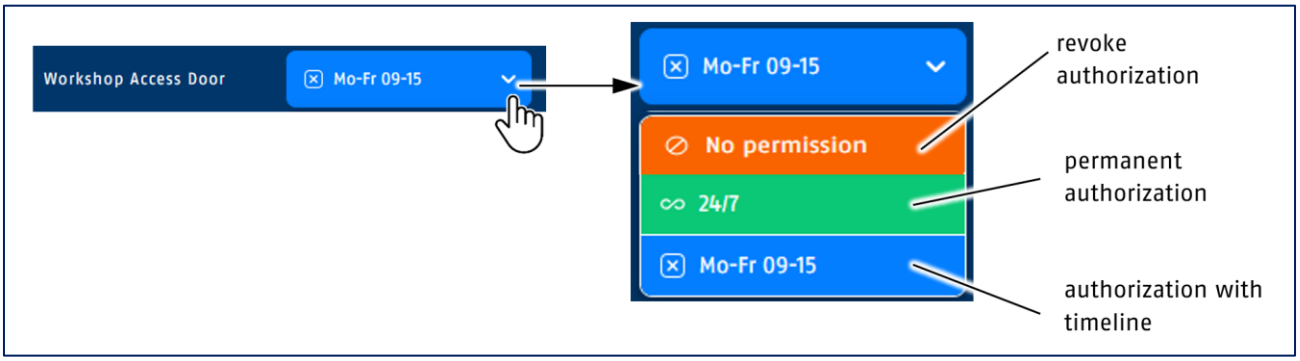
To edit the access authorisations for an individual person, expand the Authorisations menu.

Here you can see the access authorisations currently granted and any schedule selected for the person. The view varies depending on whether the person has already been granted authorisations or not. If the person is assigned to a group of persons, the group authorisations have already been inherited here.

With the "+ Add locking authorisation" command, you can add access authorisations directly without switching to the locking plan view.

If the person has already been granted authorisations , a list appears with the assigned door groups and individual doors.
Door groups expand when clicked and the authorisations of the individual doors become visible.





Notes on the person

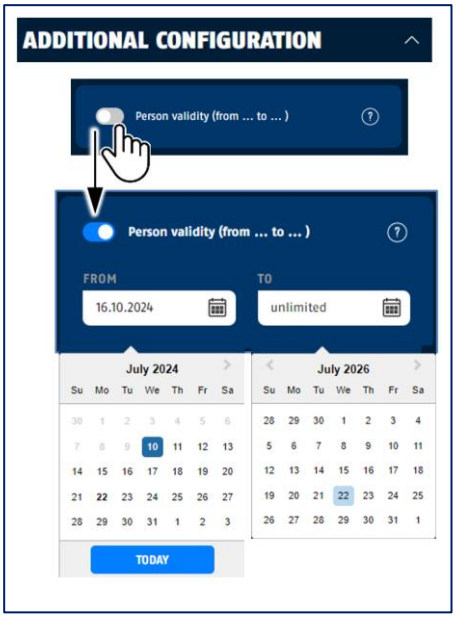
The "Description" field is available for notes on the person.

- ▷ Open the "Other settings" menu.
- ▷ Enter your notes in the "Description" field (max. 250 characters).

Limit the validity of access rights

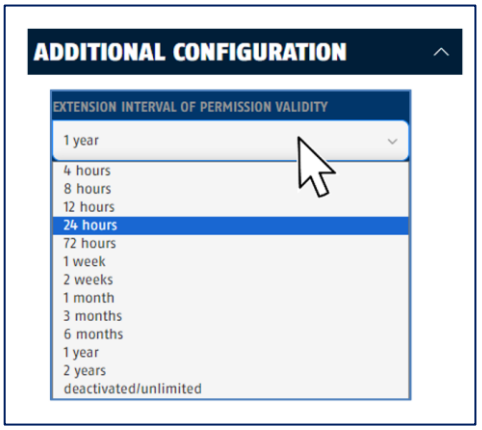
The validity of the access rights can limit the period during which access authorisation is granted for a person on the locking medium.
If no end date is set, the validity for the person is not restricted, e.g. for permanent employees.

In the case of temporary validity, e.g. for visitors or interns, the start and end of validity can be set.



- ▷ Open the "Other settings" menu.
- ▷ Press the "Validity of access rights" button.
- ▷ Enter the start and - if applicable - the end of the validity period.

Set the validity interval of the locking medium



Define the validity of the locking medium differently from the global setting (see→ chapter System configuration).

The validity of the TECTIQ locking medium is usually limited in time and must be extended at an update terminal after the validity interval has expired at the latest.

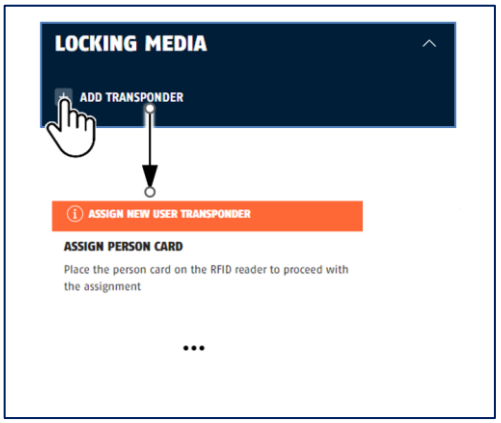
- ▷ Open the "Other settings" menu.
- ▷ Expand the "Validity of locking medium" list field and select the desired time interval.

As a rule, the validity of a locking medium should be limited to as short a period as possible, e.g. to prevent unauthorised access if a locking medium is lost.

8.6. Add locking medium

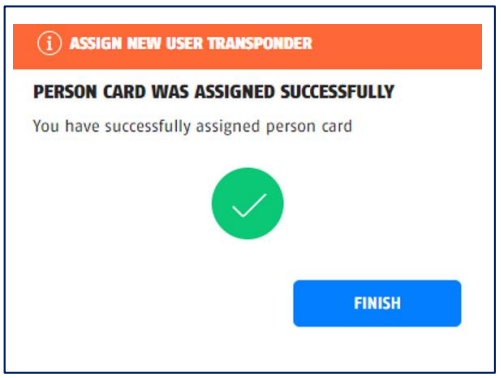
Once the system data and personal data have been determined, locking media can be added to the persons. locking media are always added physically. You will need

- the PC with TECTIQ Access Manager,
- a TECTIQ desktop reader and
- the locking medium.

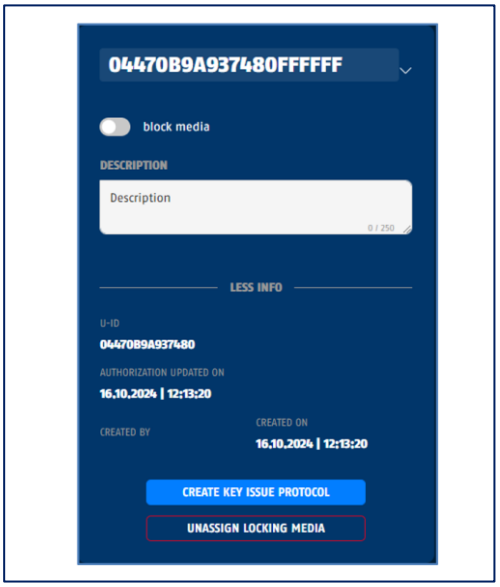


- ▷ Open the "locking media" menu.
- ▷ Click on the "Add locking medium" command.
- ▷ Place the locking medium on the desktop reader and wait until all the data has been written to the locking medium.

- After successful assignment, complete the process by clicking on the "Complete" button.



- Give the locking medium a name.
- Create the key issue log under the menu item "More info / Less info".



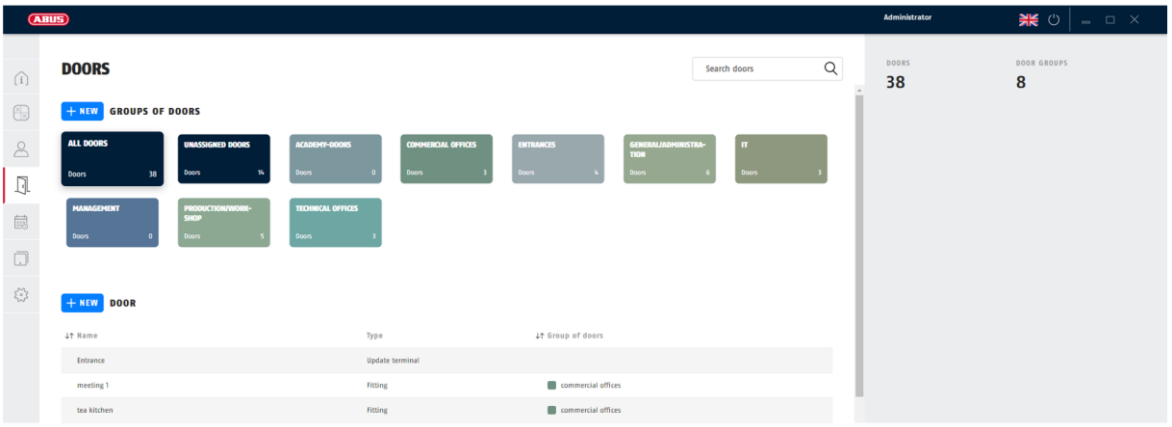
9. View Doors | Doors

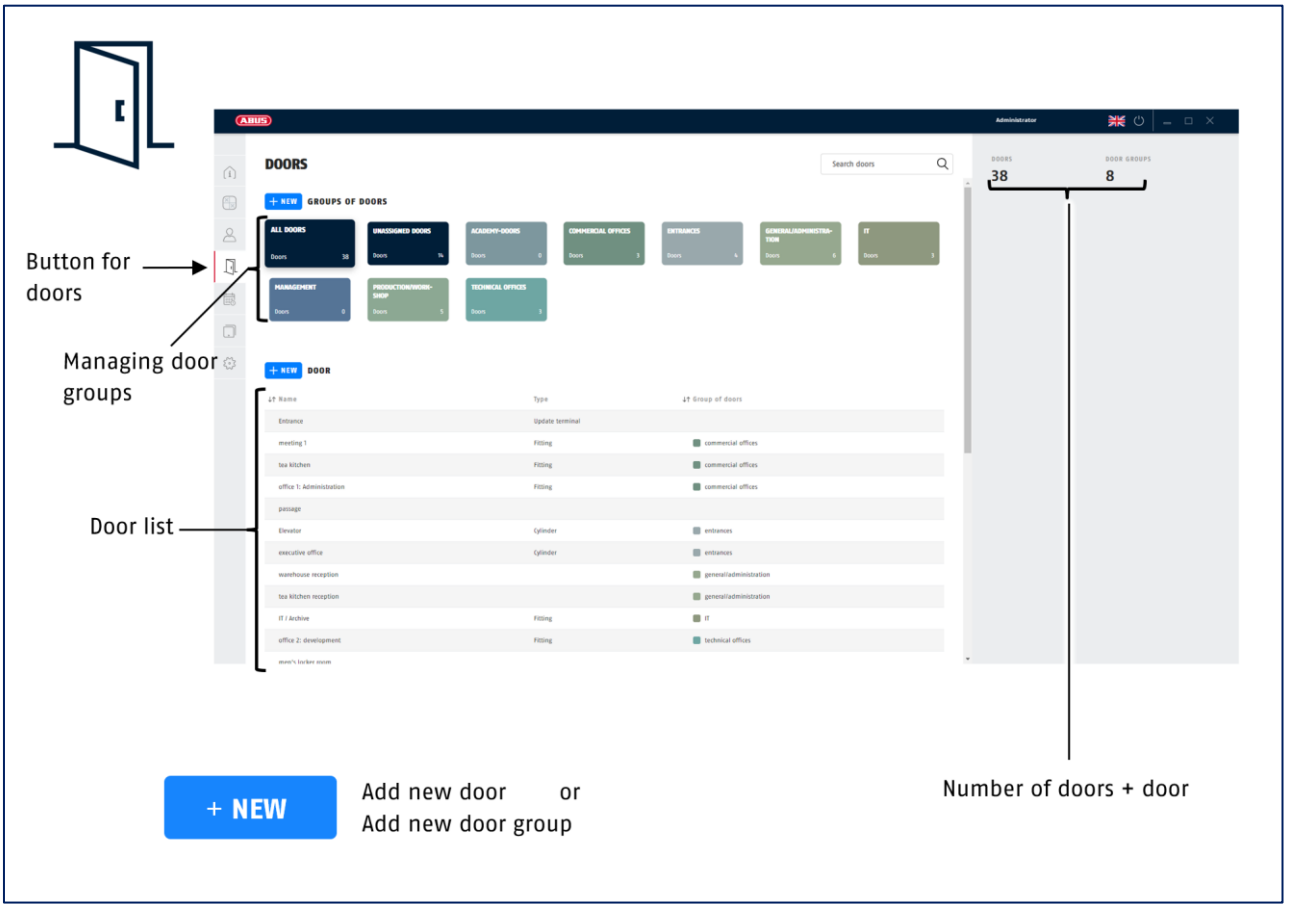
Contents

9.1. Overview

In the Doors overview, you can create and manage doors and door components in the TECTIQ locking system. Doors are simply and conveniently assigned designations. For better orientation, group doors together in door groups. After creating a door, select the door component that is installed on the door - locking cylinder, fitting or wall reader.

You can access the Doors overview via the button.

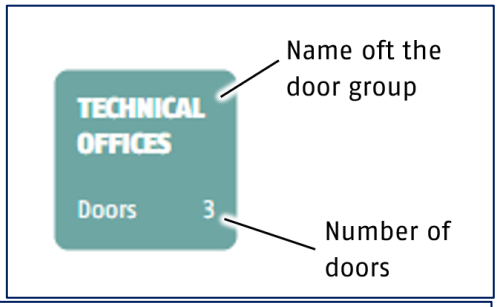




9.2. Door groups

Door groups make it easier to manage and handle a locking system. Access authorisations for entire door groups can be granted or withdrawn from individuals.

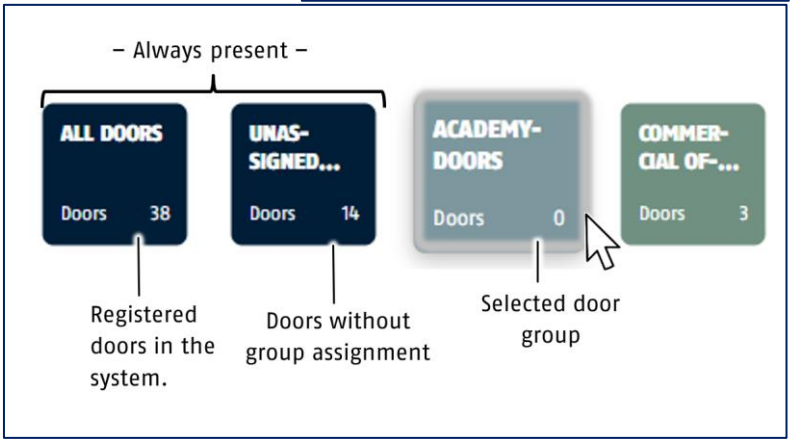
In the upper part of the Doors view, the door groups are displayed as tiles with their names and the number of assigned doors.



The "All doors" and "Not assigned" tiles are always present.

A door group is selected by clicking on it. The selected door group is highlighted.

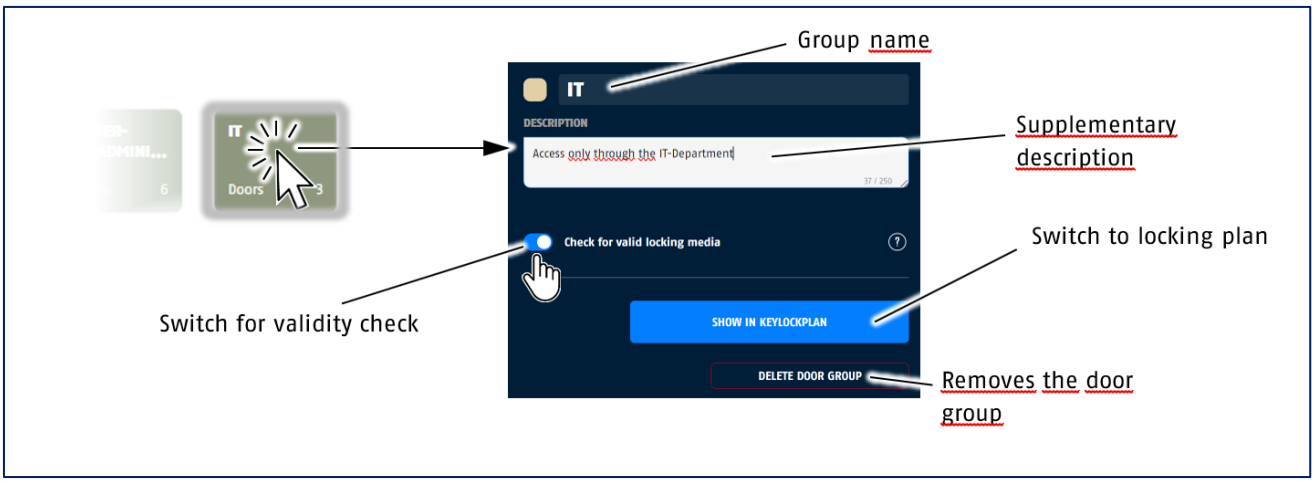
After selecting a door group, the doors it contains are displayed in the door list.



Edit group name

You edit names for the door group by placing the cursor in the window and making your changes. Entries are

automatically accepted if the TECTIQ Control has detected a plausible name. The settings can be edited at any time.



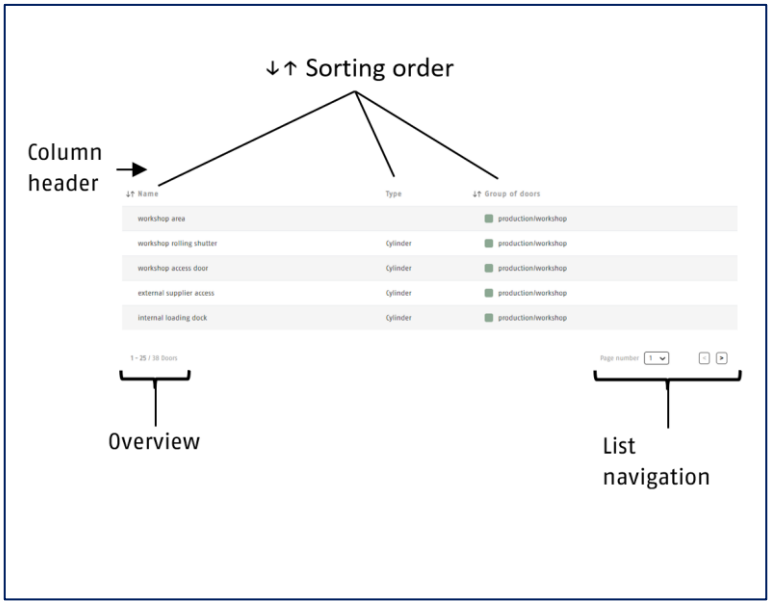
Deactivate validity check

You can deactivate the validity check for locking media for a door group. This allows you to release areas for access for all persons who have a locking medium without prior validation of the validity. This can be useful, for example, at barriers n to the parking lot or for doors to a room with an update terminal.

9.3. Doors

Doors are displayed in the door list. The list contains

- Designation of the door
- the door component mounted on the door
- the assigned door group.



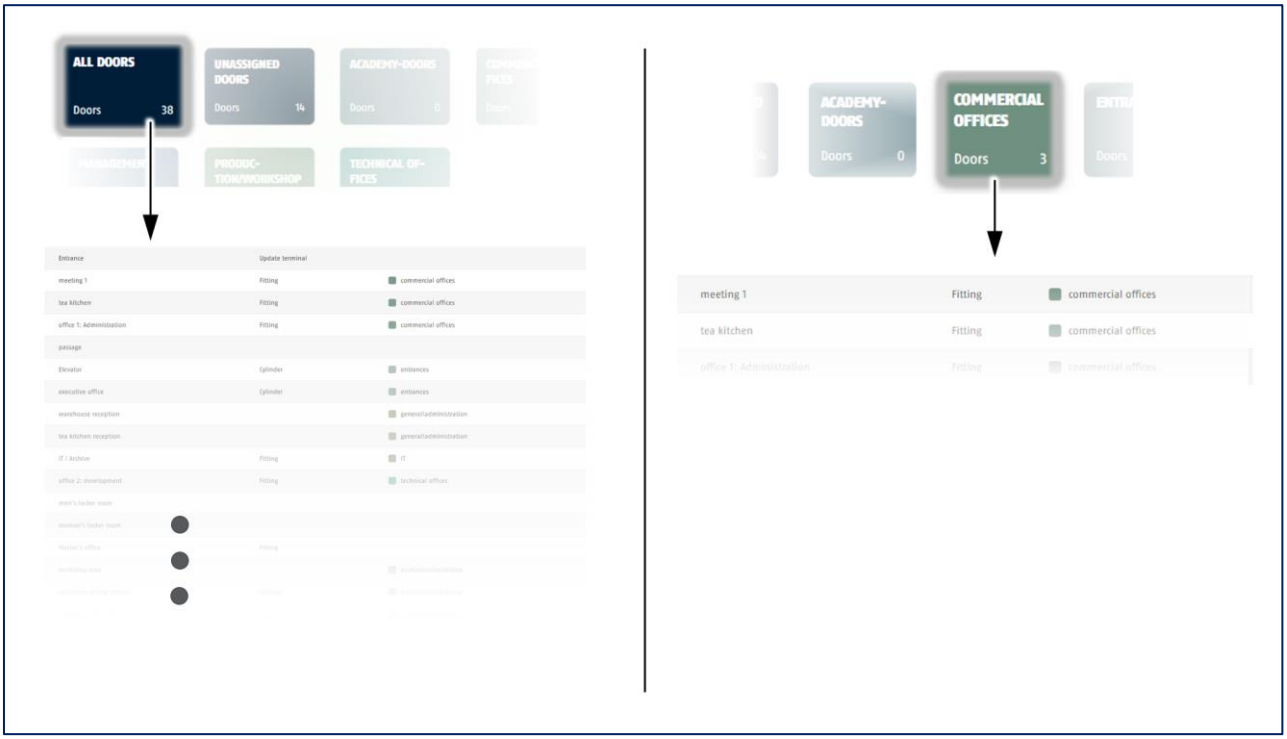
Sort doors

Sort doors by clicking on the corresponding column heading. The sorting is displayed and changes each time you click.

↓↑ in the order of entry
🡻↑ sorted alphabetically in ascending order 0...9 / A...Z
↓🡹 sorted alphabetically in descending order Z...A / 9...0

Restrict displayed doors

Restrict the display to a door group by clicking on the corresponding tile.

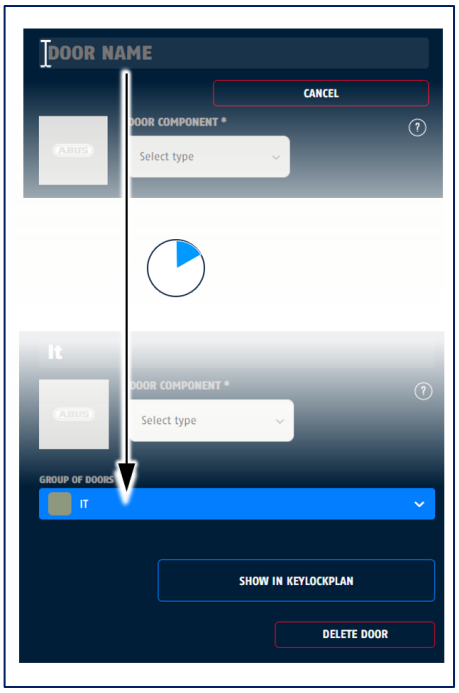


9.4. Properties of doors

Add new door

Add a door by clicking on the "+ NEW" button above the door list.

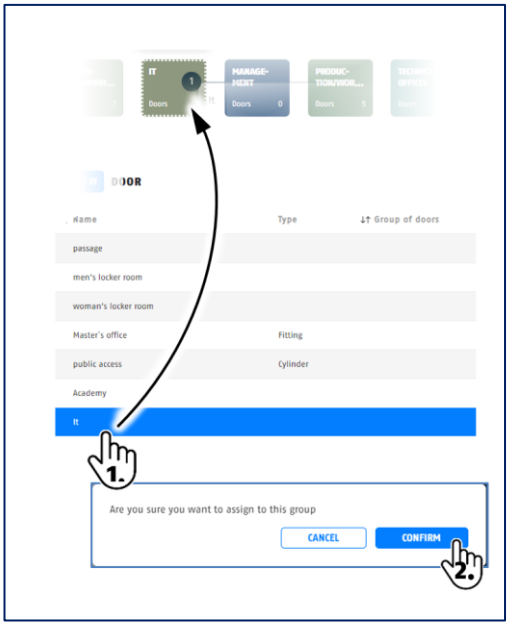
You can enter a door designation in the editing area. The entry is automatically accepted if the TECTIQ Control has detected a plausible designation. As soon as the entry has been accepted, further input options are made available. You can edit the door properties at any time.



Edit door name

You edit the door name by placing the insertion point in the window and making your changes.

Assign door group



Door groups can be assigned in different ways:

- Select a door group before creating the new door

or

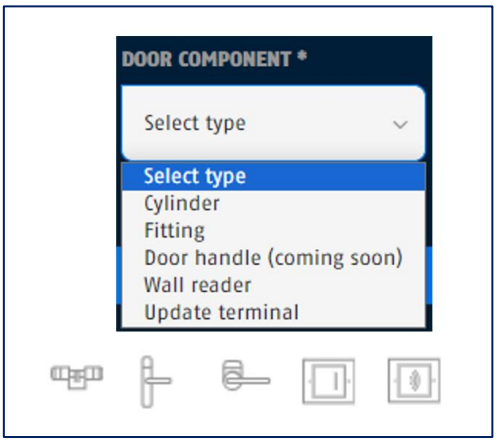
- Expand the "Door group" list in the editing area and assign the desired door group

or

- Drag the door from the door list to the desired door group using drag'n'drop.

After assignment to a door group, the door component must be reprogrammed.

Select door component



Select the door component to be fitted to the door.

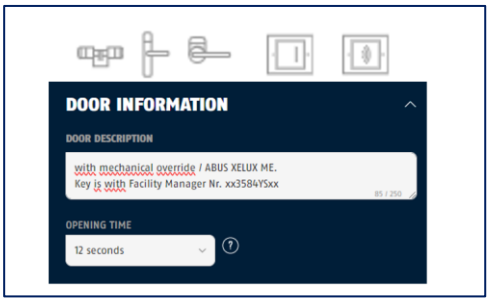
- ▷ For an electronic locking cylinder, select the entry: "Cylinder".
- ▷ For an electronic fitting, select the entry: "Fitting".
- ▷ For an electronic compact fitting (only for interior doors), select the entry: "Compact fitting".
- ▷ For an offline wall reader, select the entry: "Wall reader".
- ▷ For an online update terminal, select the entry: "Update Terminal".

Please note:

- For an electronic locking cylinder with a reader on both sides, plan two locking cylinders - one for the inside and one for the outside of the door.
- For a two-sided wall reader - this is an offline control device that controls a door (door closer or door operator) with two connected wall readers - plan two wall readers.
- First plan an online update terminal with a connected door as a system component. Then you also plan the device for access control as a "door" (also twice if two wall readers are connected).
- When the wall scanner is reset (online or offline), the relay configuration is reset to the default setting "NO".

Setting properties for door components

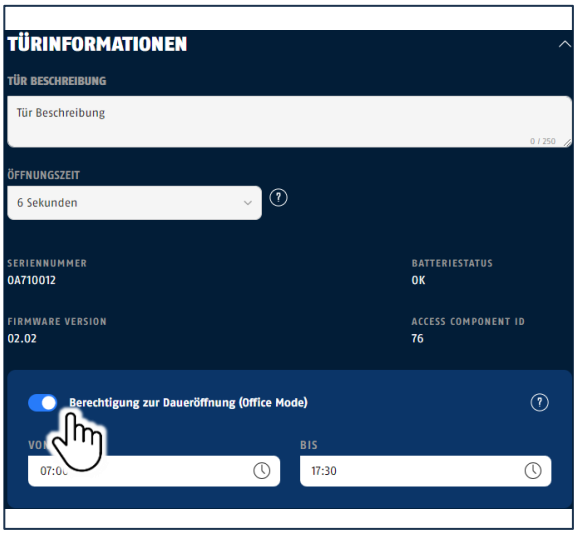
Different properties are available depending on the type of door component.



Cylinder, padlock	Fitting	Wall reader	Update terminal
Door description max. 250 characters	**Door description** max. 250 characters	**Door description** max. 250 characters	**Door description** max. 250 characters
Opening hours 6 seconds 12 seconds	**Opening hours** 6 seconds 12 seconds	-	-
-	-	**Relay configuration** NO-imp: NO contact pulse NC-imp: Normally closed pulse NO: NO contact (permanent) NC: Normally closed contact (permanent)	**Relay configuration** NO-imp: NO contact pulse NC-imp: Normally closed pulse NO: NO contact (permanent NC: Normally closed contact (permanent)
-	-	**Period** 1, 2, 4, 6, 8, 12 seconds	**Period** 1, 2, 4, 6, 8, 12 seconds
-	-	-	Acoustic signalling On / off

9.5. Activate and configure Office Mode

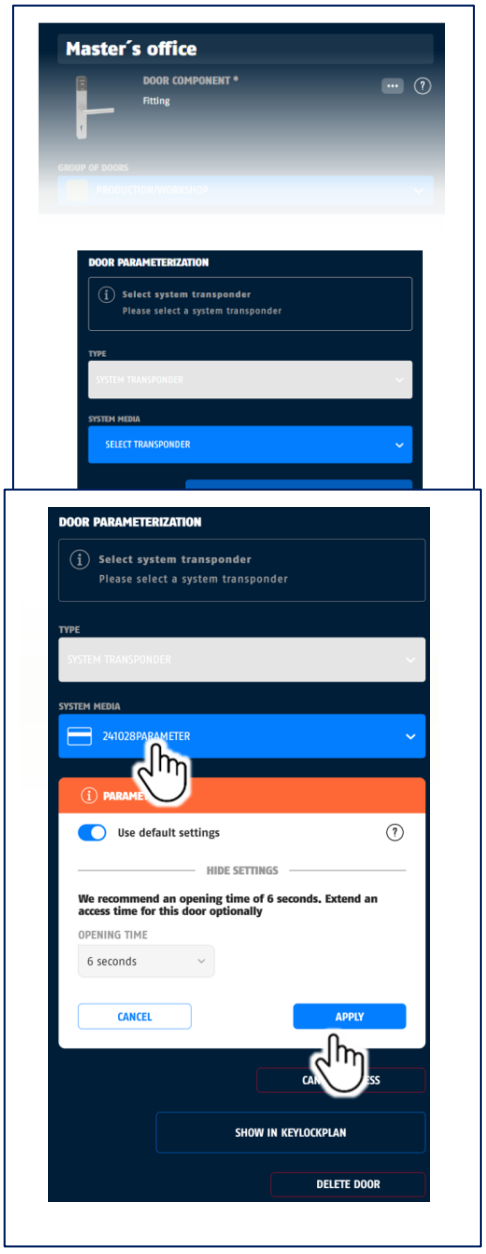
An office mode can be activated on the TECTIQ door components. This can either be provided with a time window or activated without a time restriction. Office mode can then either be activated and deactivated manually at any time, or activated within a time window and automatically deactivated when the time window expires



- ▷ Press the slider to activate office mode
- ▷ Either select "unlimited" as the "from" and "to" value or assign a time window

After successful programming via parameter card, Office Mode can be activated for a door with a transponder authorized for opening by presenting it twice and deactivated by presenting it three times.

9.6. Download data in door component



Changed configuration data must be loaded into the door component.

You will need:

- a parameter card that is initialized with the system data, see→ chapter System media.
- a USB desktop reader connected to the local PC.

▷ Select the door in the Doors view.
▷ Select the "Parameter card" system transponder type in the editing area.
▷ Select your parameter card from the "System media" list.
▷ Press the "Add door component" button ".

- You can now set the opening time of the door component or use the default settings.

▷ Press the "Apply" button
▷ When prompted, place the parameter card on the desktop reader. The write process is displayed as a flashing LED signal. Wait until the desktop reader LED indicates that the process is complete.

▷ Present the parameter card to the door component within 15 minutes. Wait until the LED on the door component lights up green.

Please note: The process is only complete when you present the parameter card to the desktop reader again and the LED on the desktop reader lights up green.

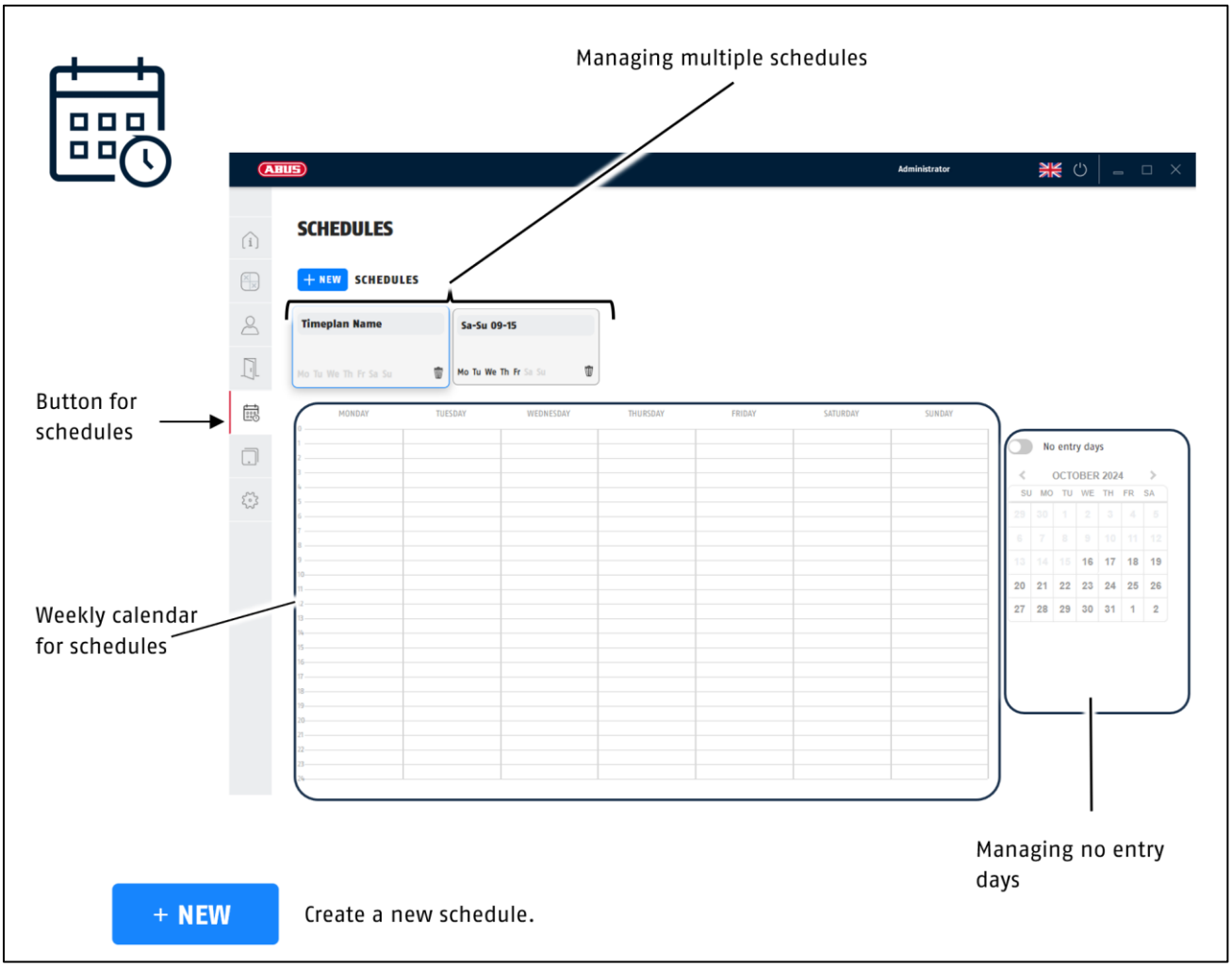
10. Schedules

Contents

10.1. Overview

In the Schedules overview, you can also organize access rights, e.g. according to individual working hours or the opening hours of properties with customer traffic. Here you can also define blocking days for non-operating times such as public holidays or company vacations.

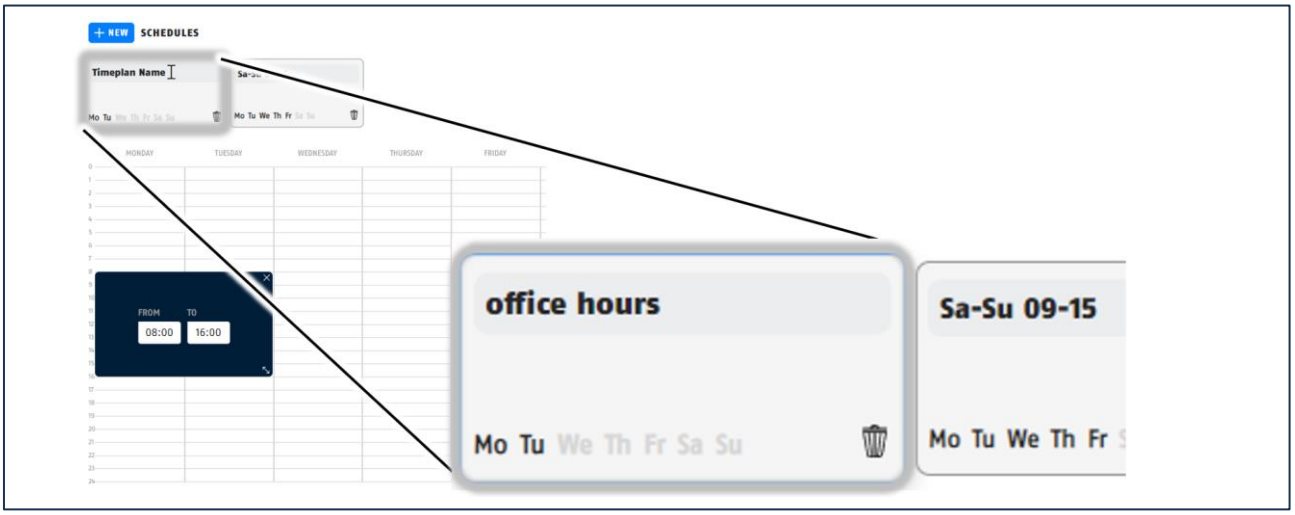
You can access the Schedules view via the button.



10.2. Add schedule

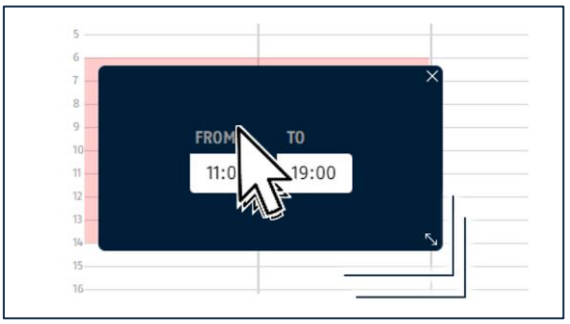
- Add a new schedule by pressing the "+ NEW" button.
  A new tile is displayed for the new schedule and a block for a time interval is suggested in the work area.

- Place the mouse pointer in the name field and enter a suitable name for the schedule.
  This name is offered to you when using schedules for persons and groups of persons. Identical names are not permitted.



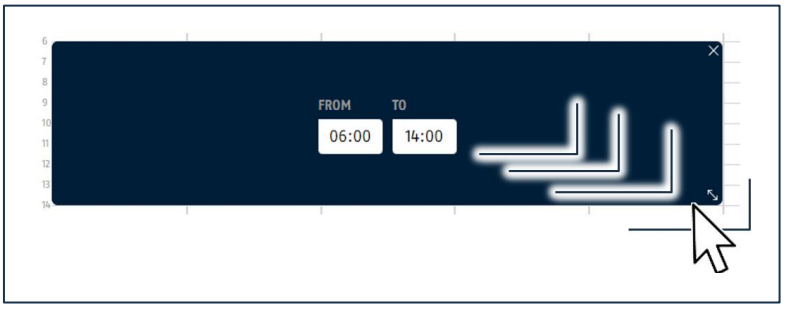
Set time interval

A time interval comprises a start time and an end time and is valid for several consecutive weekdays.

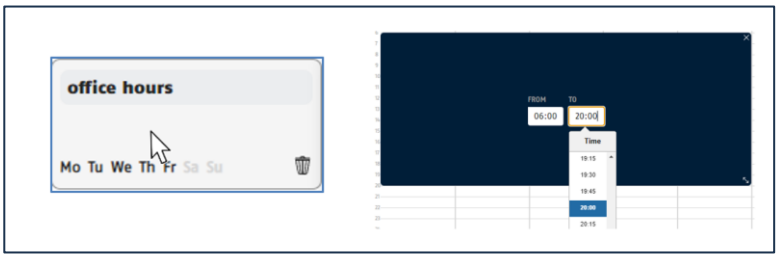


- Move the block in the weekly schedule until the top left-hand corner matches the desired day of the week and start time.

- Then drag the bottom right-hand corner of the block until it matches the desired end time and the appropriate day of the week.



▷ Alternatively, place the mouse pointer in the input field and enter the time manually.



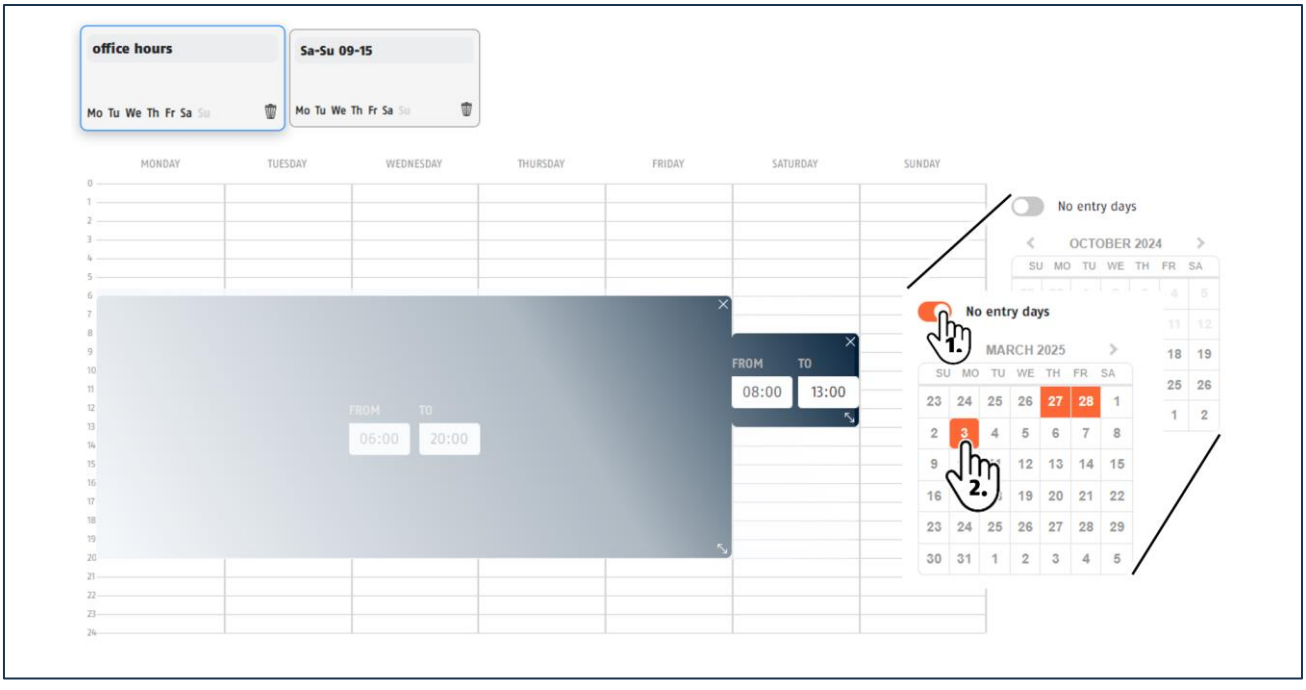
Add time interval

Each schedule can contain up to 15 individual time intervals.

▷ Add further time intervals by clicking in the weekly schedule and dragging an area of the desired size.

Add Blocking days to a schedule

You can set up Blocking days for each schedule. The persons for whom the schedule is valid have no access on the Blocking days entered.



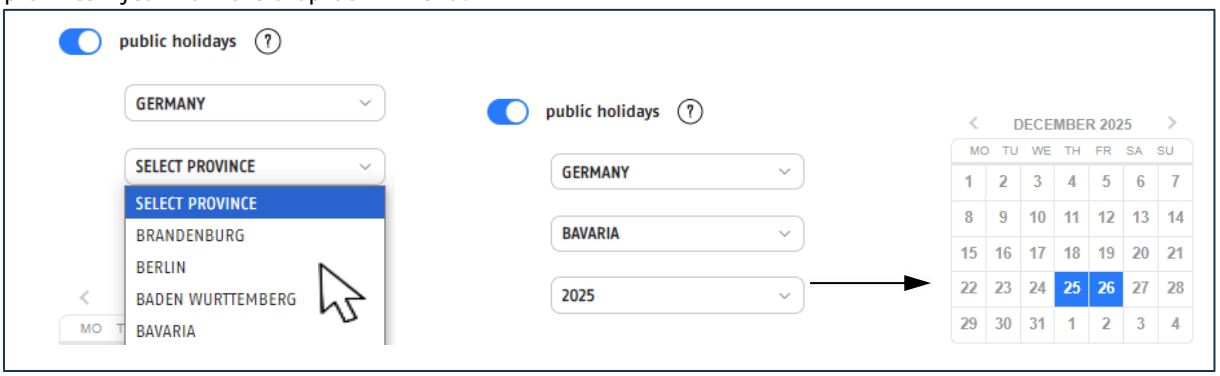
▷ Select the desired schedule.

- ▷ Press the "Blocking days" button.
- ▷ In the calendar view, use the </> buttons to select the desired month.
- ▷ Click on the desired date.

The active Blocking days are displayed in red. Up to 30 Blocking days can be set per schedule.

Import public holidays

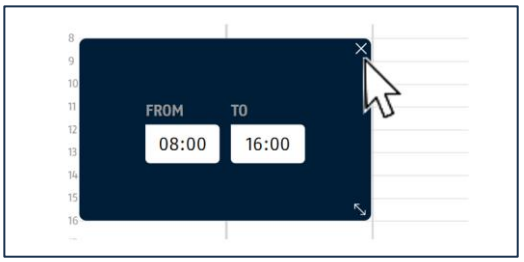
Public holidays can also be imported as blocking days. To do this, please select the desired combination of country - province - year from the drop-down menu.



10.3. Edit schedule

All settings of a schedule can be changed at any time:

- Weekday
- Start and end time
- Name of the schedule



Delete time interval

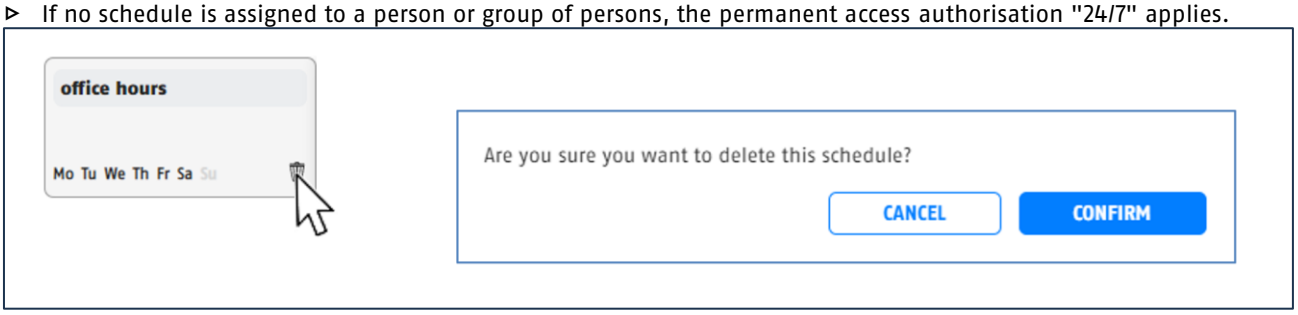
- ▷ Delete a time interval in a schedule by clicking on the top right-hand corner.

Please note: Changes to time schedules that have already been assigned to persons or groups of persons only take effect after the next validation of the locking medium on the update terminal or desk reader.

10.4. Delete schedule

A schedule can be deleted.

- ▷ Assign a different schedule to all persons and groups of persons who use the schedule that is to be deleted.
- ▷ Delete the schedule by clicking on the delete icon in the corresponding tile and answer the confirmation prompt.
- ▷ If no schedule is assigned to a person or group of persons, the permanent access authorisation "24/7" applies.



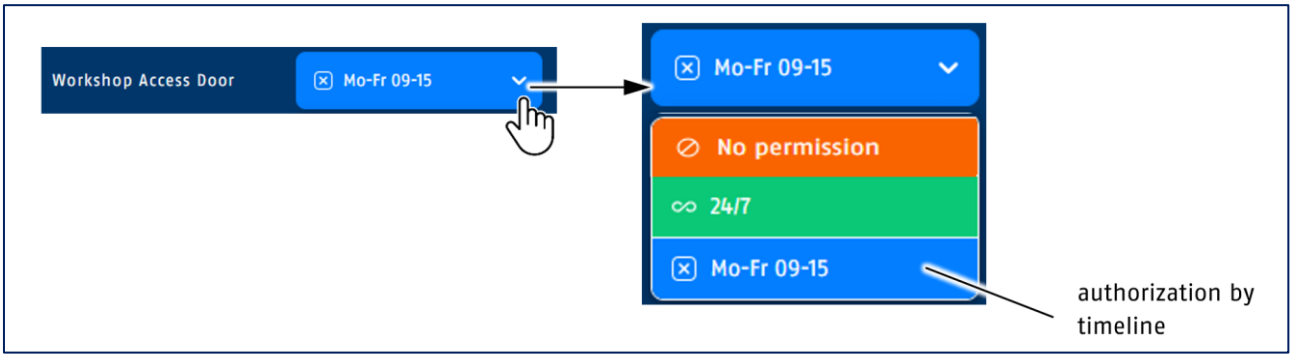
10.5. Use schedule

You can use schedules in different ways:

- Unrestricted for one group of persons
- For a group of persons related to a door group
- For a group of persons related to a specific door within a door group
- For a group of persons on a single door
- Unrestricted for an individual person
- For an individual person related to a door group
- For an individual person related to a specific door within a door group
- For an individual person on a single door

Please note: Only one schedule can be valid per person.

- ▷ Use a schedule in the Persons view and assign the schedule.



After assigning a time schedule, the locking medium must be programmed for the persons concerned.

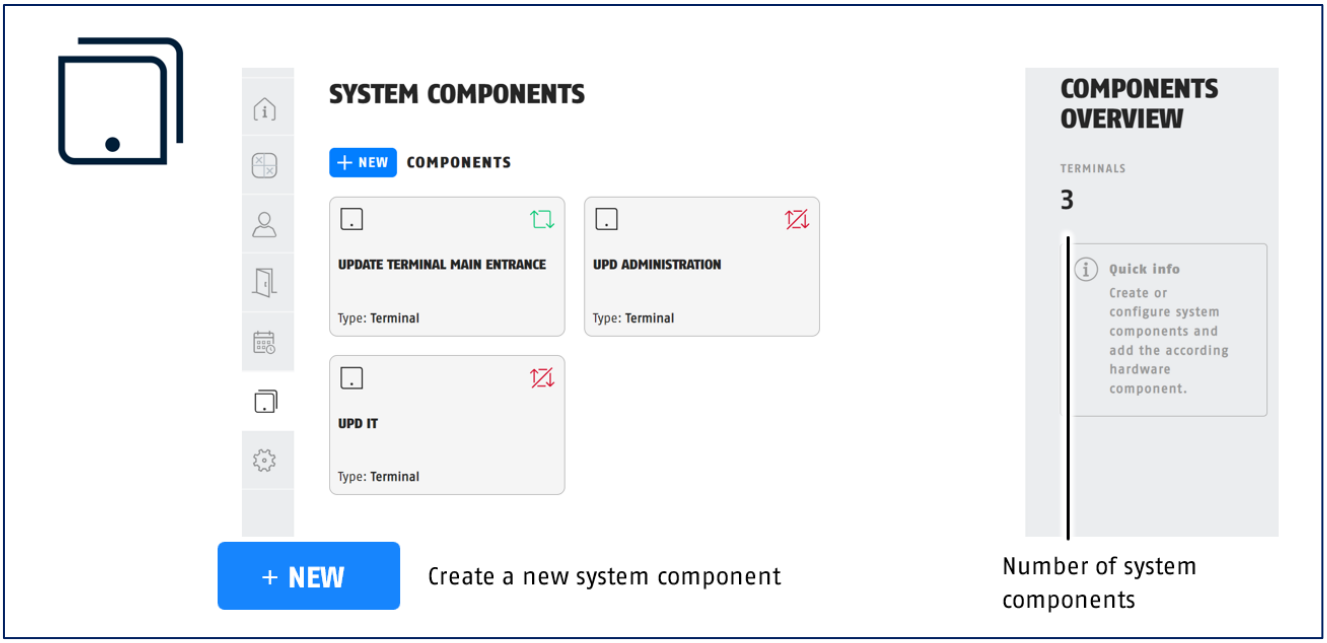
System components | Components view

Contents

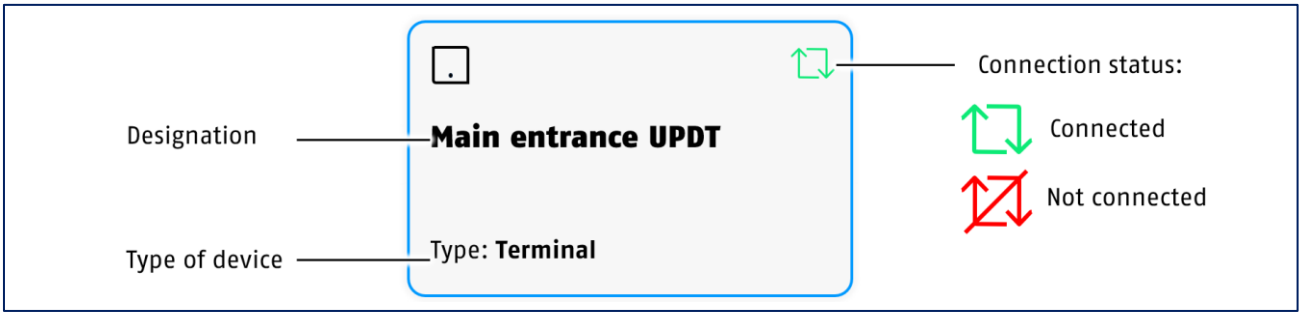
10.6. Overview

In the System components view, you manage the online update terminals at which persons update their access authorisations . The system components are always connected to the TECTIQ Control - either via the local network or via remote access at another location.

You can access the System components view via the button.



The system components are displayed in the work area with their current connection status.

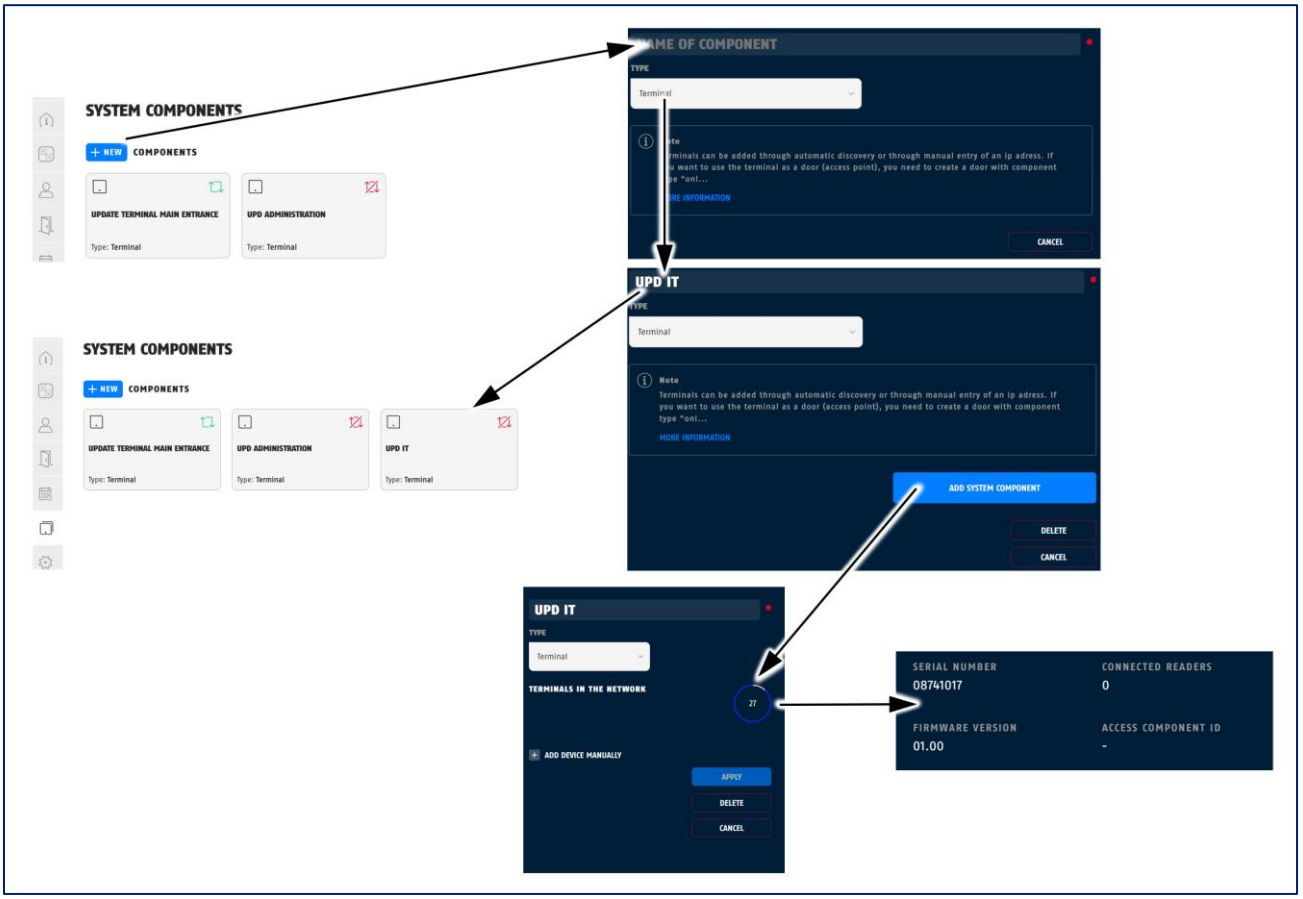


10.7. Add online update terminal

Add a system component for each terminal installed in the system:

- ▷ Press the "+ NEW" button.
- ▷ Enter a name for the system component.

The entry is accepted automatically. The system component is displayed in the form of a tile in the work area.



A so-called discovery service is integrated for the initial setup of the online terminal, with which the online terminal is automatically recognized. The prerequisite is that both components are located within a shared local network.

- ▷ Connect the online terminal to the same network as the TECTIQ Control.
- ▷ Start the connection process with the TECTIQ Control. Press the "Add system component" button in the editing area.

The control starts a search process. Terminals found are displayed in the work area with their serial number.

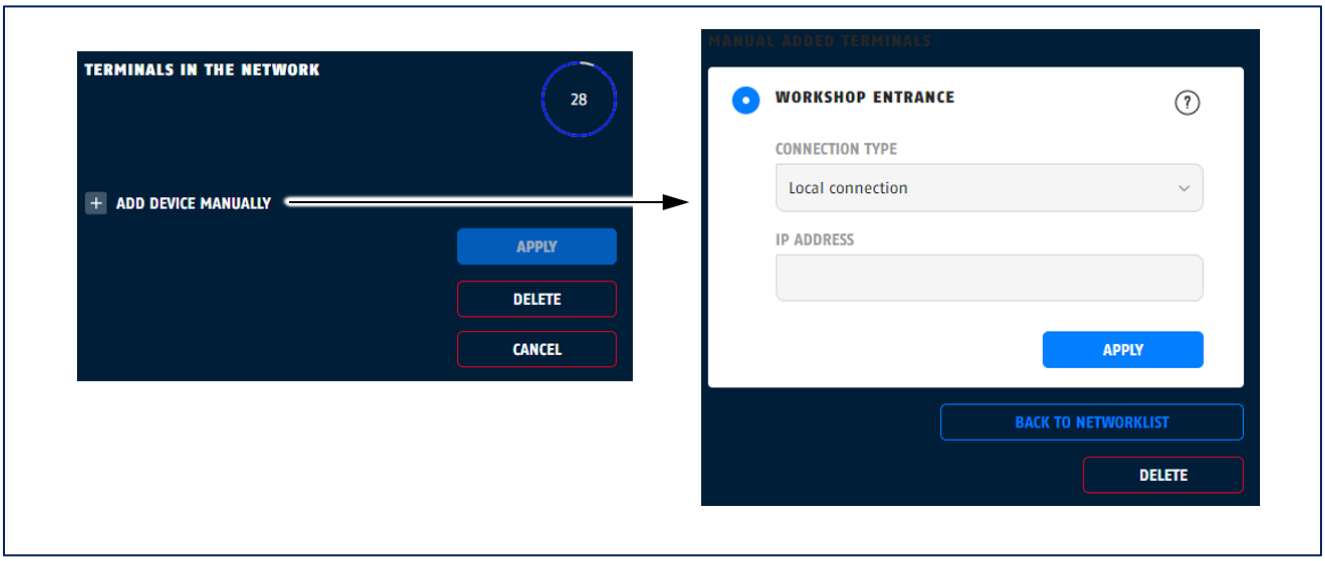
- ▷ Press the "Apply" button to connect the online terminal. The online terminal automatically receives a network address via DHCP.

The control panel connects to the update terminal and displays the connection status "green".
When all update terminals on the work surface are connected to a device in the system, the LED on the control panel shows a green light.

If the search process is not successful, check in the IP router whether the terminal is available in the network. Coordinate with your IT administrator and assign the IP address manually.

- ▷ Select the "Add devices manually" command.
- ▷ In the "Connection type" list field, select the "Local network connection" entry.
- ▷ Enter the IP address of the terminal in the "IP address" field and press the "Apply" button.

You can end the addressing process with the "Back to network search" button or the "Cancel" button.



10.8. Online terminal with door control

An online update terminal can be used on its own - as a pure update terminal - or you can also directly control door openers, door drives, door crosses and more.

In the latter case, the terminal also fulfils the task of an offline door component and is created separately in the Doors view.

- ▷ Create the terminal as a system component and start up the network connection.
- ▷ Plan the door connected to the terminal in the Doors view.
- ▷ Select "Update Terminal" as the door component.
- ▷ Expand the "Terminal" list field and select the relevant update terminal.

Assign the access authorisations in the locking plan view

10.9. USB desktop reader

The TECTIQ desktop reader can be used as a system component and update terminal.

- ▷ Connect the desktop reader to a free USB port on the PC on which the TECTIQ Access Manager is running.
- ▷ Start the TECTIQ Access Manager software.
- ▷ Establish the connection between the PC and the TECTIQ Control.
- ▷ Make sure that the software is active during the usage times.

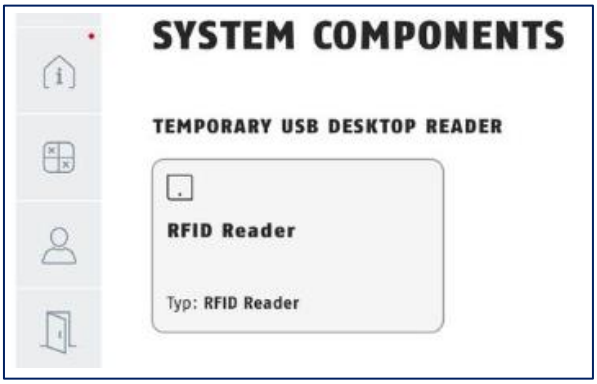
When using the desktop reader as an update terminal, you should ensure that no unauthorised access to the PC and the software is possible:

- Do not leave the PC unattended.

or

- Set up the desktop reader and the PC separately, e.g. the desktop reader in a passageway and the PC in a separate, adjacent room.

The desktop reader is displayed as a temporary desktop reader in the System components menu item.

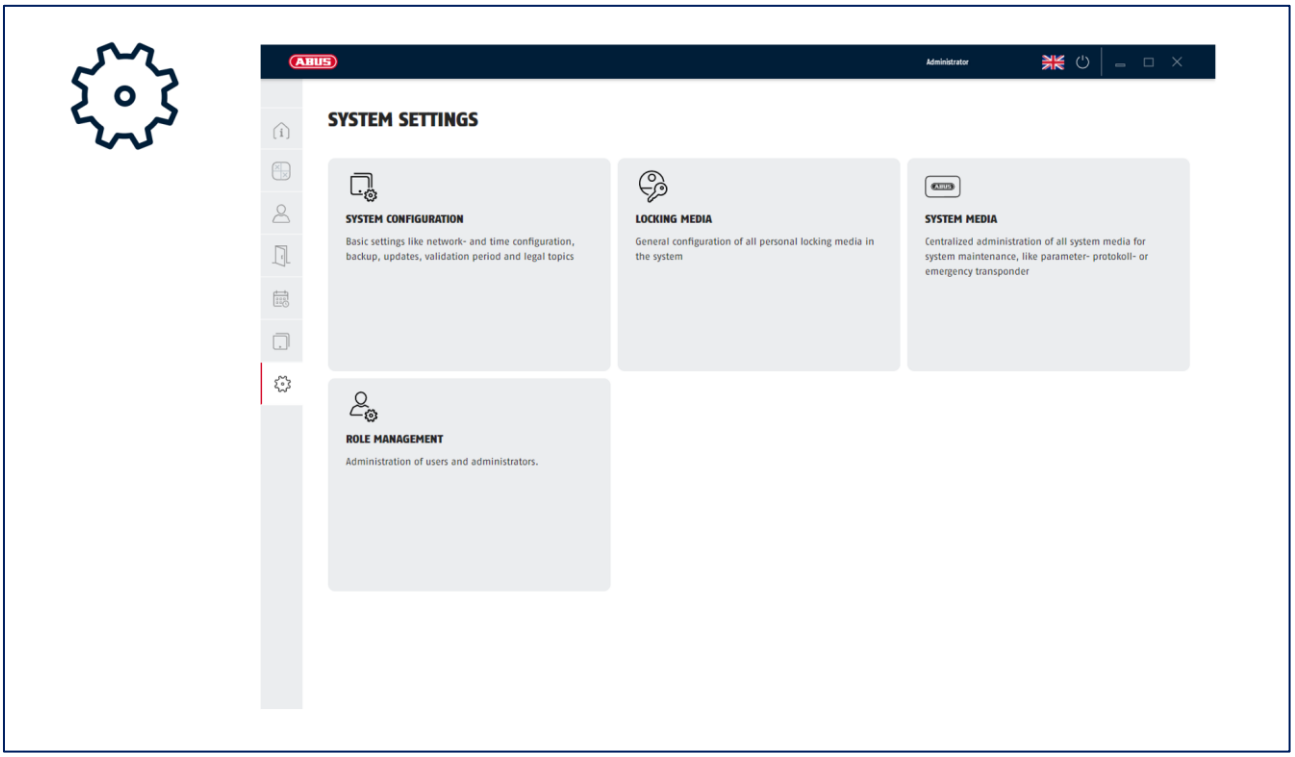


11. System settings | Settings view

Contents

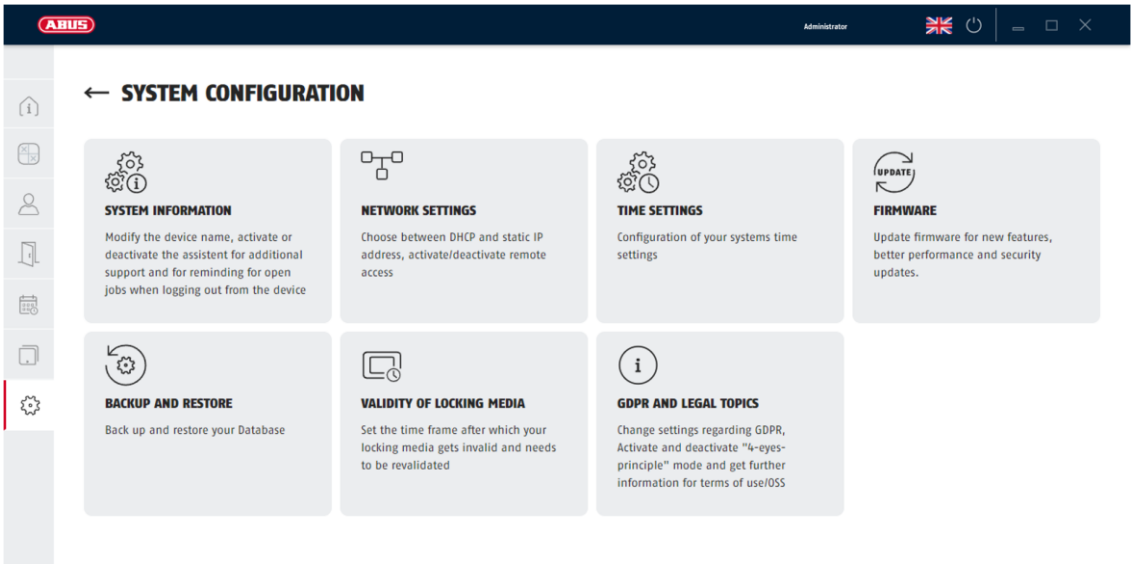
11.1. Overview of system settings

In the System settings view you will find all setting options and information about the system and for the Access Manager program.
You can access the system settings via the button.



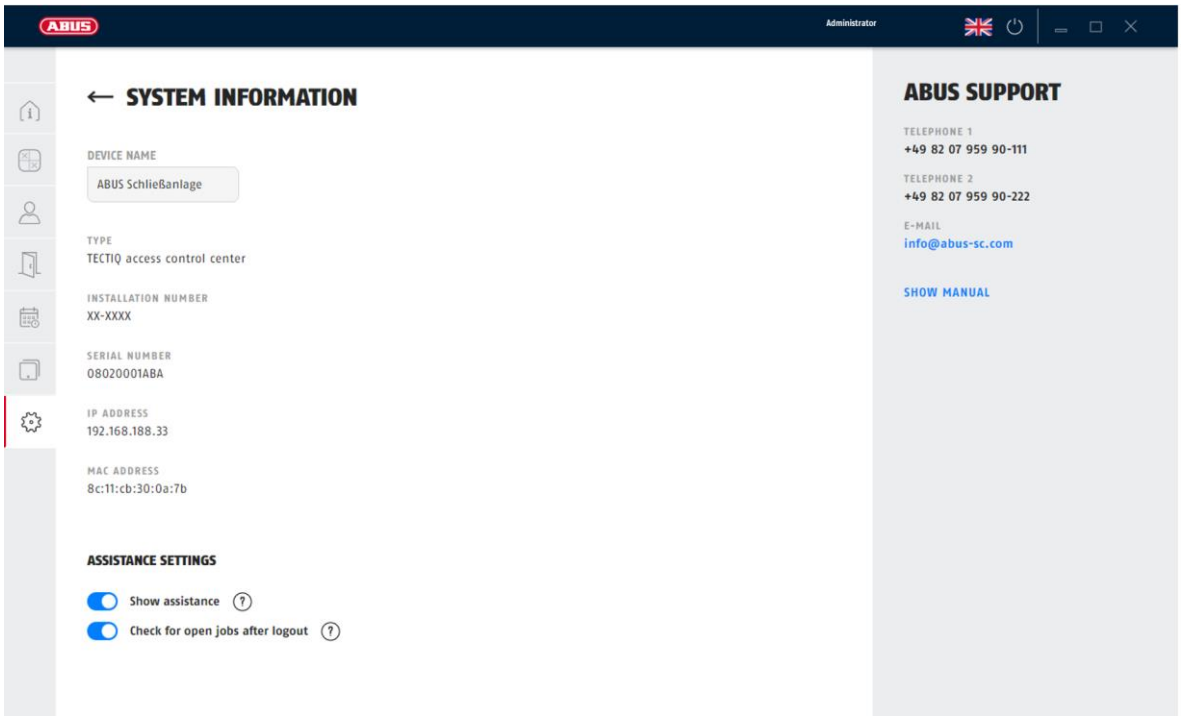
11.2. System configuration

Under System configuration you will find an overview of general information on identifying and configuring your locking system and your TECTIQ Control. You can view and adjust default settings for the operation of your system. You can access the system configuration via the System settings view and the button System configuration.



11.2.1. System information

Under System information, you will find the most important information for identifying your locking system and your TECTIQ Control. You also have the option of making default settings for program-side support of system operation.
You can access the system information via the System settings view and the buttons System configuration and System information.

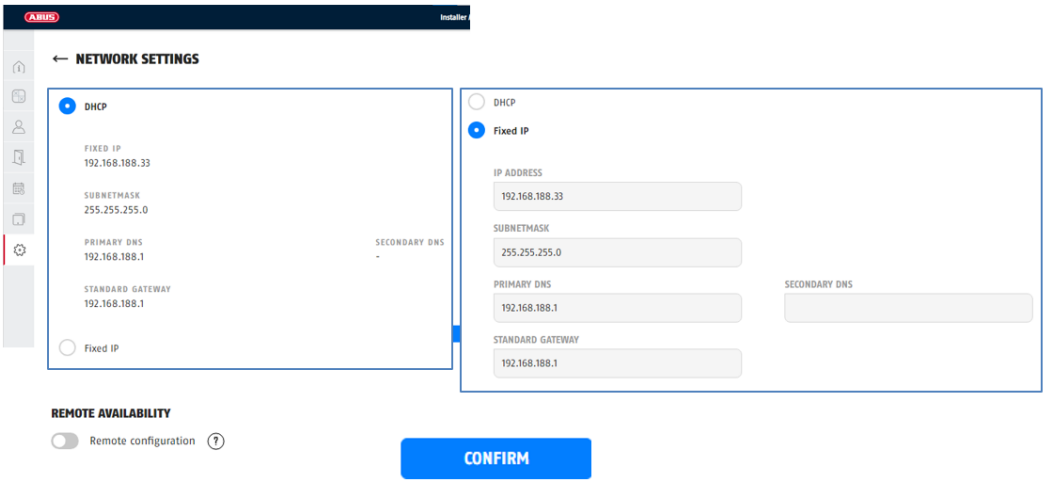


The following information is displayed:

- Device name : The name of the system that is displayed in the dashboard. You can change the device name.
- Type: The device type of the TECTIQ Control. Cannot be changed.
- System number : Identifies the TECTIQ locking system. Is set on delivery and cannot be changed.
- Serial number : Unique identification of the TECTIQ access control panel. Cannot be changed.
- IP address : The currently set IP address of the TECTIQ Control, as manually specified in the network or assigned by DHCP.
- MAC address: The unique hardware address of the network adapter of the TECTIQ Control. Cannot be changed.
- Show instructions: Internet link to the current system instructions.
- Show assistant: If this setting is activated, you will receive short help texts when you change system data, add persons or similar.
- Check for open tasks on logout: If this setting is activated, you will receive a message when you exit the program if the task list contains tasks that have not yet been completed.

11.2.2. Network settings

In the network settings you configure the network access of the TECTIQ Control.
You can access the network settings via the System settings view and the buttons System configuration and Network settings.



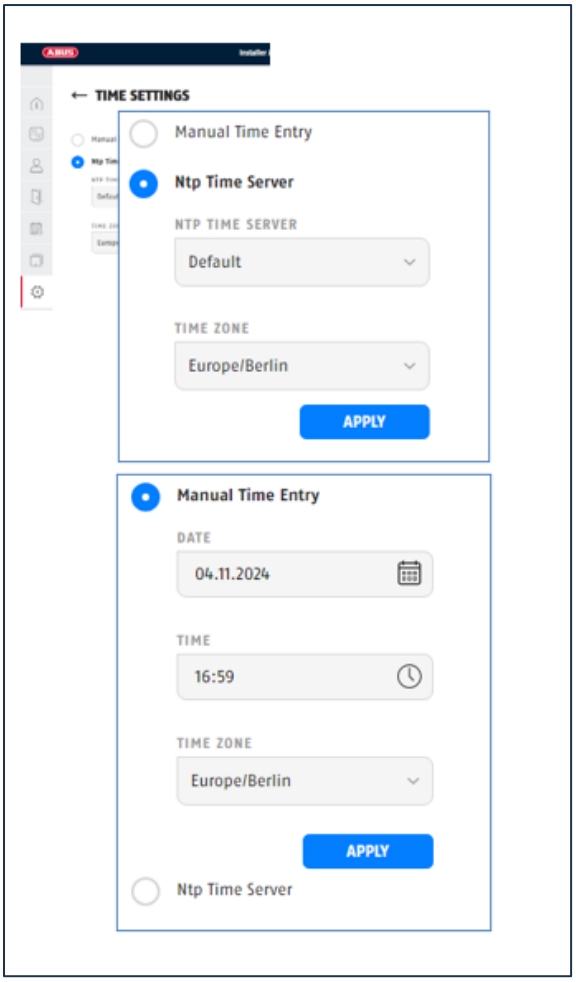
- ▷ Select your settings according to the network configuration on site.
- ▷ Select "DHCP" for automatic address assignment.
- ▷ Select "Static IP address" to set the Internet address manually. You can obtain the required data from the network administrator.
- ▷ Finish the entry with "Confirm".

▷ Activate remote access to be able to reach your TECTIQ Control from outside your local network via the Internet. The connection is established via a secure tunnel.

After changing the network settings, the control restarts and disconnects. The user must then re-establish the connection to the control.

11.2.3. Time settings

The TECTIQ system requires the current time to function securely. If the TECTIQ access control panel is connected to the Internet, the system can automatically synchronize itself with the correct time via a time server. Alternatively, you can set the date and time manually.
You can access the time settings via the System settings view and the buttons System configuration and Time settings.



ⓘ We recommend setting the time via a time server (NTP)!

- ▷ Select "Time server (NTP)" so that the system can synchronize the date and time automatically on a regular basis.
- ▷ In the "Time server (NTP)" field, select "Default" or the option for manual entry. Suggestions for your location can be found in the information window.
- ▷ Complete the entry by clicking on the "Apply" button.

- to set the time manually:

- ▷ Select "Manual time entry"
- ▷ Enter the current values for "Date" and "Time". Enter the time zone corresponding to the system location, e.g. "Europe/Berlin" for the time in Central Europe.
- ▷ Complete the entry by clicking on the "Apply" button.

11.2.4. Firmware update

As soon as updated system software (known as firmware) is available for the TECTIQ access control panel, a message is displayed on the dashboard. An updated firmware includes, for example, new functions, security updates or performance improvements.

You can access the function via the System settings view and the buttons System configuration and Firmware update.

The current firmware version is displayed.

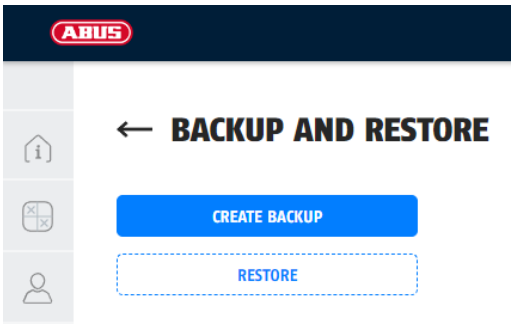
Make sure that you only use secure sources authorized by ABUS! For more information, please contact www.ABUS.com or our support team.

- Download an updated firmware to the local hard disk.
- Select the "Firmware Update" button and select the downloaded software on your local PC.
- Follow the further instructions.

11.2.5. Data backup and restore

Save the data of your locking system with the entered persons, doors and locking plan at the latest after completing the commissioning of the system.
The backed-up data is stored locally on your PC and can be loaded again if required.

You can access the data backup via the System settings view and the buttons System information and Data backup and restore.



Save TECTIQ system data

- ▷ Select "Create backup" to back up the data of the TECTIQ Control.
- ▷ Follow the instructions and enter a password.

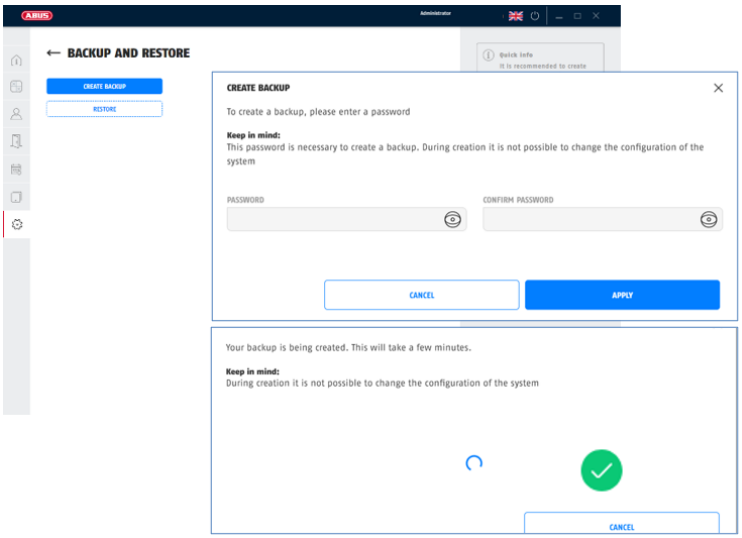
Important! Insecure passwords can be spied on or guessed - even if they formally meet the criteria (see→ image). Unauthorised persons can bypass the locking system and cause major damage to your property.

- Only use secure passwords.
- Follow the rules and guides on what a secure password should look like, e.g. from the German Federal Office for Information Security (BSI).
- If you use a password generator, change the password suggestion again, e.g. by adding or changing a character.

The TECTIQ Control only accepts passwords that

- consist of at least 8 characters,
- contain both upper and lower case letters,
- contain at least one digit,
- contain at least one special character - e.g. @$!%*?& - are included

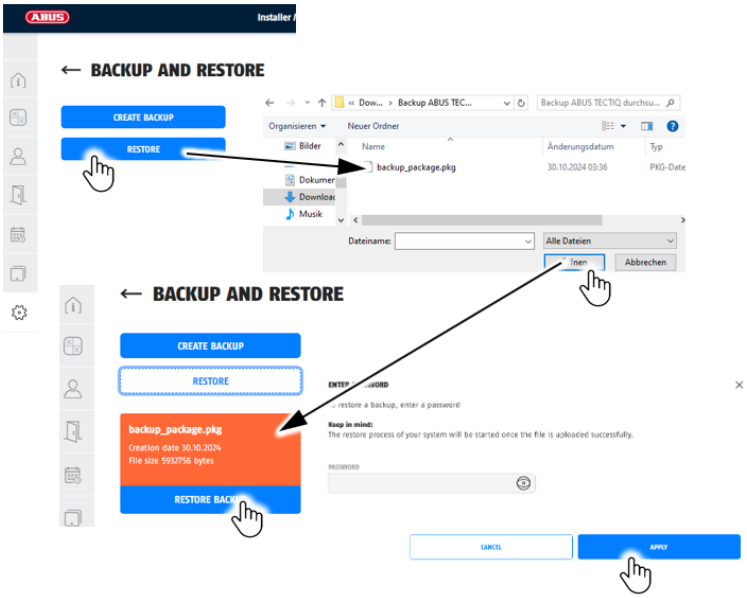
- ▷ Enter a password and make a note of it.
- ▷ Repeat the password entered in the "Confirm password" field.
- ▷ Confirm your entry with "Apply".



- Pursuant to creating the backup, download the backup to your PC.
- Enter the desired storage location.
- Confirm the completion of the process by clicking the "Done" button.

Restore TECTIQ system data

- Select "Restore".
- Select the desired backup file on your PC.
- Click on the "Open" button.
- Your backup is displayed in the Access Manager for restoration.
- Select the "Restore backup" button.
- Enter the password and select the "Apply" button.

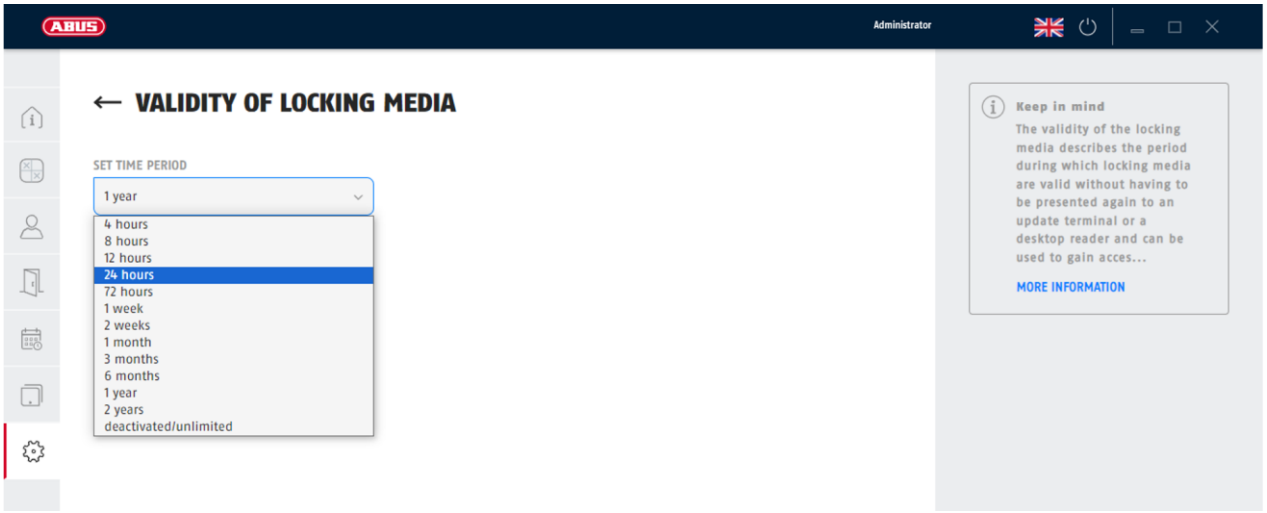


11.2.6. Validity of the locking media

The validity of the TECTIQ locking media can be limited to increase security against unauthorised use. If the function is activated, the user is required to update their access authorisation regularly. In the "Validity of locking media " menu, you specify the time interval after which the access authorisation must be renewed.

Once the period has expired, access authorisation must be renewed by presenting the locking medium in front of the online terminal or at the desk reader - which is always possible during normal operation without changing personal data.

You can access the function via the System settings view and the buttons System configuration and Validity of locking media.

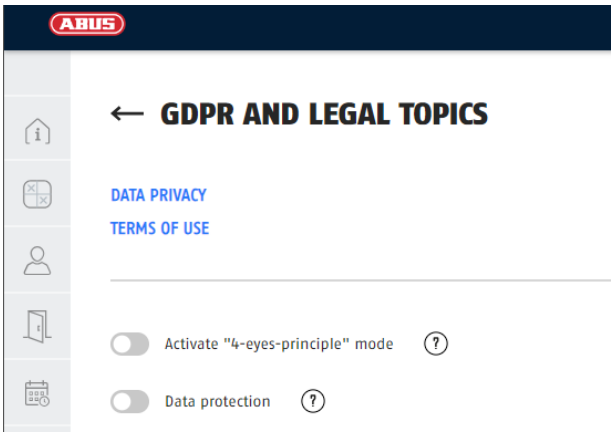


▷ Select the time interval from the "Set time interval" list box.

- The typical and recommended time interval for a business operation with employees is between 12 and 48 hours (corresponding to 1 to 2 days). Short times lead to more up-to-date data in the system, as data is written back from the door components to the TECTIQ Control more frequently. Security is increased.
- A short time interval of less than 12 hours is recommended, for example, for guests or tradesmen who are only in the secured area for a short time.
- Longer time intervals should only be set in exceptional cases.
- Unlimited access should not be set for normal locking media, but only for locking media that are created for security purposes and - removed from normal use - stored in a secure location, for example.

11.2.7. Data protection and legal issues

All topics with legal relevance can be found in the System settings view under the buttons System information and Data protection and Legal topics



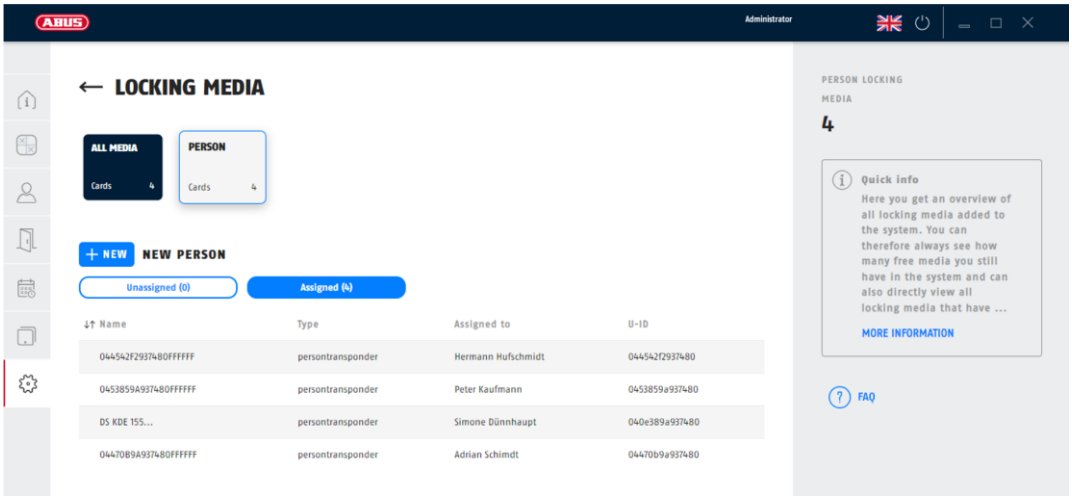
The works council mode ensures that the event list is displayed anonymously and can only be viewed once the works council password has been entered. For this purpose, a slider appears in the event list to activate "View personal data".

Important! The works council password is assigned when the function is activated and **cannot** be reset for security reasons. Please note the information on assigning secure passwords in chapter 13.2.5 Data backup and recovery

The data protection mode can be activated to limit the storage time of the event list. The storage period can be a maximum of 3 years and a minimum of 1 day and is entered as a number of days in the input field. If the works council mode is activated, the works council password must be entered to change the storage duration for security reasons.

11.3. Locking media

The Locking media overview provides an overview of all locking media known to the system. In addition to locking media currently assigned to persons, this also includes blocked locking media or locking media that have already been assigned to persons.
You can access the function via the System settings overview and the button locking media.

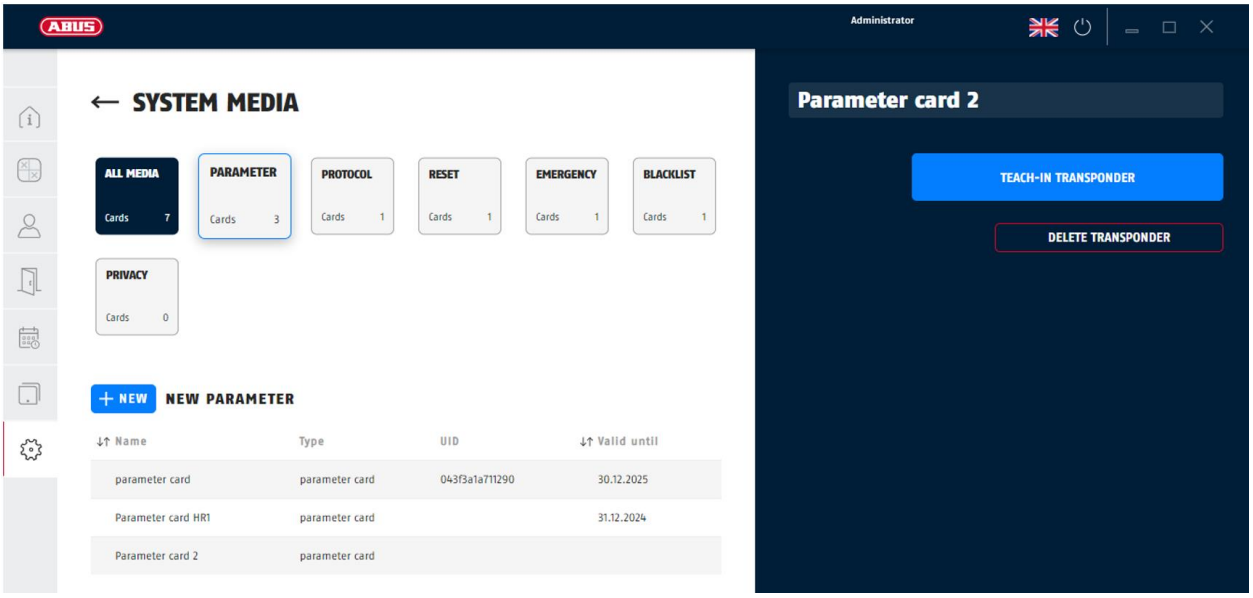


11.4. System media

The system media overview manages all media with system functions. System media are not usually assigned to persons and should be stored securely and protected from unauthorised access. This includes

- Parameter cards
- Protocol cards
- Reset cards
- Emergency opening transponder
- Blacklist cards

You can access the function via the System settings view and the button System media.

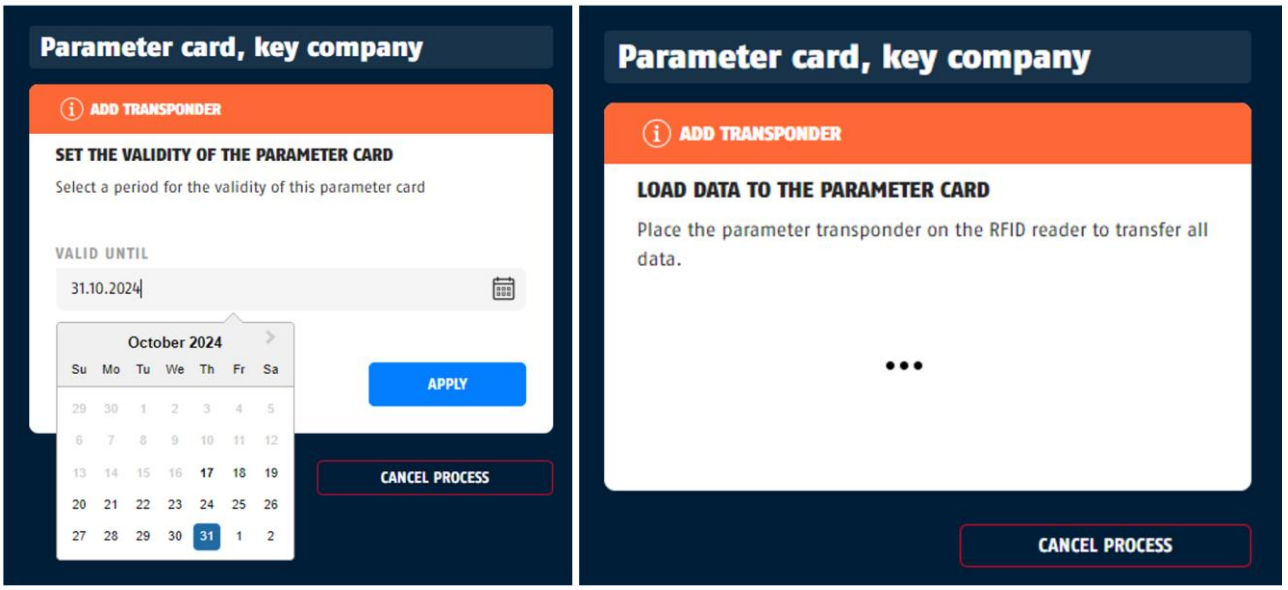


Add new system media:

- ▷ Select the desired media type by pressing the relevant button.
- ▷ Press the "+New" button.
- ▷ Enter a name for the system medium.

After adding, you can make further settings.

- ▷ Press the "Teach in transponder" button.
- ▷ Set a validity interval for the system medium.
  Caution: Select a reasonable time interval. Take suitable measures to ensure that you extend the validity of the relevant system medium in good time.
- ▷ Complete the process by writing to the medium. To do this, follow the instructions in the editing area.

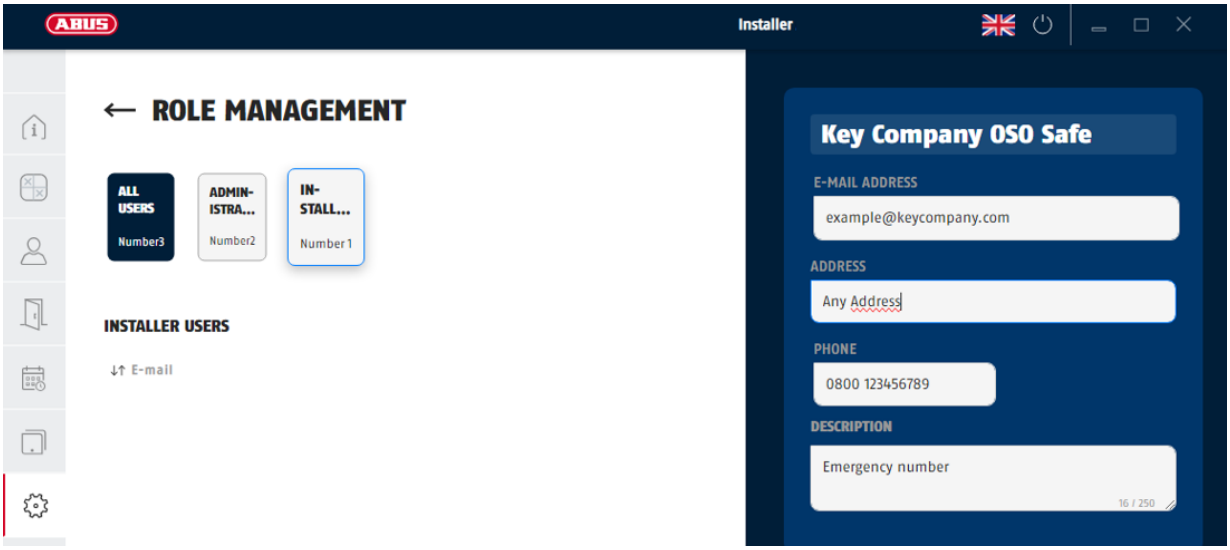


11.5. Role management

TECTIQ allows two user roles, which are stored as contact persons in the TECTIQ Control :

- The administrator is the operator of the system, e.g. the owner of the property, facility manager.
- The installer is the specialist installer, e.g. an authorized ABUS specialist retail partner.

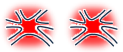
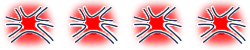
You can access the function via the System settings view and the button Role management.


Installer
← ROLE MANAGEMENT
ALL USERS
Number3
ADMIN-ISTRA...
Number2
IN-STALL...
Number1
INSTALLER USERS
↓↑ E-mail
Key Company OSO Safe
E-MAIL ADDRESS
example@keycompany.com
ADDRESS
Any Address
PHONE
0800 123456789
DESCRIPTION
Emergency number
16 / 250

12. LED signals

Contents

12.1. LED signals on door components

	Access granted.
 (0.1 s each)	Access denied. locking medium expired or no authorisation for the door.
	Battery warning, access granted with 5 second delay
	Incorrect or foreign locking medium / read error
	General error
 (0.3 s each)	Hardware error
	Line interruption (with TECTIQ fitting)
 (1 s)	Motor error when opening time has expired. Door remains open. If the error occurs 5× in succession, the appliance restarts.
	Long illumination (1 s), followed by rapid flashing: Motor fault, device restarts until the fault is rectified.
 Permanent	Software error, device is out of order.
	Software error, device must be reprogrammed.
	Device restarts (e.g. after battery change or error)
 (5 s)	Lights up for 5 seconds after restart: Device contains no data.

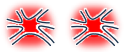
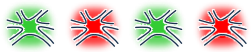
When dealing with system media

	Fast flashing (0.1 s / 0.3 s) Write/read process is running.
	0,5 s Process successfully completed.
	0,5 s Operation not successful.

When using the Admin App

	Identify smartphone with admin app and system authorisation
	Flash briefly 4×: No authorisation: process aborted
	Blink slowly: Write process is running. If the process was successful, the device will then restart.

12.2. LED signals on the update terminal

		Access rights have been updated. System medium successfully described. An existing door is opened.
	(0.1 s each)	With locking medium: Access denied. For system medium: Medium is being written.
	(0,5 s)	For locking medium: Access rights have not been updated. For system medium: Write operation failed.
	(0,1 s)	Incorrect or foreign locking medium / reading error / connection fault between wall reader unit and control unit.
		General error
	...	No connection to the TECTIQ Control ; terminal is offline.
		System fault. No connection to the TECTIQ Control ; terminal is offline. No access possible.
		Software update runs between control panel and wall reader unit (or via smartphone with Admin App)
		Wall reader restarts.
		Wall scanner unit connects to control unit
	(5 s)	Lights up for 5 seconds after restart: Device contains no data.

When handling system media or Admin App

	Fast flashing (0.1 s / 0.3 s) Write/read process is running.
	0,5 s Process successfully completed.
	0,5 s Operation not successful.

12.3. LED signals on the desktop reader

	Continuous red light	Switching on/initializing
	Continuous green light	Ready for operation / operation successful
	Short red flash (0.1 s / 0.3 s)	Incorrect medium (incorrect or missing system number)
	Flashing green	Write/read process active
	Slow red flashing (0.3 s / 0.3 s)	Process not successful

ABUS TECTIQ

ANNEX

15. Logs

The TECTIQ Access manager provides logs for documentation and as a task list for download.

15.1. Key issue protocol (sample)

ABUS SECURITY CENTER

KEY ISSUE PROTOCOL

CREATED: 24/10/2024 01:01:30

RECIPIENT

Username:	Jakob Hansen
Comment:	Access Card
UID:	0453859a937480

ISSUE	**RETURN**
Date	Date
Signature	Signature

ADDITIONAL AGREEMENT

15.2. Blocking list (sample)

TECTIQ - (UN)BLOCKED MEDIA
AFFECTED DOORS

(UN)BLOCKED BY		(UN)BLOCKED MEDIA	KDE155181
(UN)BLOCKED AT	04.11.2024 | 03:07:43	RELATED PERSON	Jakob Hansen

ID	NAME
69	CEO
45	Administration
44	Parking Gate
54	Room Munich
70	Customer Service

16. Overview - TECTIQ door components

Requirement	Wall reader / update terminal	Electronic cylinder	Electronic fitting
One-sided access control	Yes	Yes	Yes
Two-sided access control	Yes	Yes	No
For external doors	Yes	Yes	Yes
For interior doors	Yes	Yes	Yes
For door opener/door buzzer	Yes	No restriction	No restriction
For motor-driven doors	Yes	No restriction	No
For revolving doors, door crosses	Yes	No restriction	No
Door leaf thickness	No restriction	2× 30... 90 mm	32 mm... 121 mm
For FH doors	No restriction	Yes	Yes
locking function	Not applicable	Yes	With fitting with mechanical override
Suitable for escape routes	No restriction, depending on the door	Yes (one-sided variant only)	Yes
For garage doors	With drive: yes	Yes (half cylinder)	No
Installation	Flush-mounted / surface-mounted box	In door with mortise lock	In door with mortise lock
For Scandinavian doors	No restriction	Yes	Yes
For doors with Swiss round cylinder	No restriction	Yes	Yes
Independent battery supply	No (with UPS: yes)	Yes	Yes
Service life	Min. 10 years	Min. 10 years or 200,000 closing cycles	Min. 10 years or 500,000 closing cycles
Battery life	Not applicable	2-3 years or 45,000 closing cycles	3 years or 80,000 closing cycles
Power supply via 230 V	Yes (via power supply unit)	No	No
Power supply via PoE	Yes	No	No
Ambient temperature	-10... +60 °C / -20... +70 °C	-20... +65 °C	-25... +65 °C
Protection class (EN 60529)	IP44 / 67IP	IP67	IP54 (standard; other variants: IP53...IP56)
Emergency opening with emergency opening transponder	Yes	Yes	Yes
Emergency opening in the event of failure of all components	Depending on the door	Yes, via USB connection	Yes, via USB connection
Extension of access authorisation	Yes (Update Terminal)	No	No

17. Who does what and when?

What?	Who?	When?	Notes
Create user	Admin Specialist installer	If required When erecting	
Change user	Admin	If required	
Remove user	Admin	If required	Recommendation: Do not remove users but block them.
Block users	Admin	If required	Block user or locking medium
locking the locking medium	Admin	If required/loss	
Create new locking medium	Admin	If required	
Create TECTIQ project	Specialist installer	When erecting	
TECTIQ Project planning	Building owner Specialist installer	When erecting	
Configure TECTIQ project	Specialist installer	When erecting	
Putting the TECTIQ project into operation	Specialist installer	When erecting	
Create doors	Specialist installer	When erecting For conversion	Padlock by Admin
Change doors	Specialist installer	For conversion	Changing door groups also by admin
Assign door components	Specialist installer Admin if applicable	When erecting For conversion	Padlock by Admin
Convert doors	Specialist installer	For conversion	
Program doors	Specialist installer Admin	For construction/conversion	Admin for padlock or when changing door groups
Edit access authorisation	Admin Specialist installer	If required When erecting	
Troubleshooting Battery change No connection Device defect	 Operator Specialist installer Specialist installer	 With battery warning For fault messages In case of malfunction	Device defects or repairs only by specialist installers
Maintenance	Specialist installer		See assembly instructions
Repair	Specialist installer		See assembly instructions
Firmware update	Admin	With message in the Access Manager	
Replace door component	Specialist installer	In case of defect	
Programming locking media	Specialist installer Admin	When erecting If required	
Central restart	Admin	On request by ABUS Support.	
Network reset	Specialist installer	In the event of an error in the IP address, if access to the control is not possible	Without DHCP in the system, the accessibility of the control must be checked and restored.
Factory reset	Specialist installer	On request by ABUS Support.	All data will be deleted when you press this button! Be sure to back up the data beforehand!

18. TECTIQ documentation - Notes and symbols

In addition to general technical descriptions, this manual contains important instructions that must be observed. Text markings and additional elements indicate the importance of these passages.

Warning of personal injury

Warnings indicate **danger to life and limb**. Warnings differentiate according to the severity of the danger and use one of the following signal words:

Icon	Signal word	Meaning
	DANGER!	Indicates an imminent danger which, if not avoided, will result in death or serious injury!
	WARNING!	Indicates a potential hazard which, if not avoided, could result in death or serious injury.
	CAUTION!	Indicates a potential hazard which, if not avoided, may result in minor or moderate injury.

Warning of material damage

Failure to observe the instructions may result in **material damage** to the product, the building or as a result of incorrect operation, which in turn may result in consequential damage.

Icon	Signal word	Meaning
	NOTE	Indicates a possibility of damage to the product or the building.
	Important	Indicates possible malfunctions due to incorrect installation or commissioning.
	INFO	Provides additional important or useful information.

More symbols

A specific symbol can be used instead of the general warning symbol in the event of special hazards or instructions:

	DANGER!	Danger due to electric shock
	NOTE	Damage to the product due to electrostatic discharge

Further enumerations

- Text passages preceded by a period • are part of an enumeration.

▷ Text passages preceded by a triangle indicate an action step: You must do something here. Please keep to the order of the action steps - unless otherwise stated.

Further documentation

Please also refer to the documentation accompanying the ABUS TECTIQ products and the detailed installation instructions, which you can obtain at any time at abus.com.

19. Safety instructions

19.1. General safety instructions

DANGER! **Danger of electric shock!**

Electric shock when touching live parts in the installation environment of electronic devices. Electric shock can lead to death.

- Disconnect before working on the device.
- Cover live parts in the vicinity!

WARNING! **Explosion hazard!**

Installing and operating the devices in potentially explosive atmospheres can lead to serious injury or death.

- Do not install or operate the devices in potentially explosive atmospheres.

CAUTION! **Risk of injury from swallowing small parts!**

Children can swallow small parts.

- Keep small parts such as screws or locking media away from children.

CAUTION! **Risk of crushing due to motorized doors in the installation area!**

Motorized doors can cause injuries.

- Unlock motorized doors in the immediate vicinity during the work.
- Secure your construction site on all sides to prevent unauthorised access.
- Use your personal protective equipment.

19.2. Safety instructions for escape and rescue routes

WARNING! **Serious injury or death possible if escape doors or fire doors do not function properly due to improper installation or maintenance!**

Poorly installed or maintained locking cylinders or fittings can impair the function of escape doors and fire doors. In emergencies, this can lead to dangerous situations with serious or fatal injuries.

- Only have escape and fire doors with the installed components installed and maintained by qualified personnel.
- Observe and follow all manufacturer's instructions when installing and maintaining the doors, locks, locking cylinders and fittings.
- Ensure that only suitable components are installed in escape and rescue routes. Pay particular attention to the compatibility of the installed components. Observe the manufacturer's certificates.
- Observe the prescribed maintenance intervals for doors, locks and locking cylinders.
- Replace locking cylinders and fittings on escape and fire *doors* once the maximum number of locking cycles has been reached.

19.3. Safe handling of batteries

WARNING! **Danger due to improper handling of batteries!**

Batteries can overheat and cause fires.

Damage or exposure to high heat can cause fires or explosions and lead to serious injuries, burns or chemical burns.

Leakage can release hazardous substances that are harmful to your health.

- Do not reverse the polarity of the batteries. Observe the polarity (+/-).
- Do not recharge, open, throw into fire or short-circuit batteries.
- Do not use new and used batteries together.
- Do not use together with other battery types.
- Only return fully discharged batteries with the terminals taped.
- Keep batteries away from children.

19.4. Professional installation

The products/systems described here may only be installed and maintained by persons who are qualified for the respective task.
A qualified electrician is required for electrical installations.
Qualified personnel for the installation and maintenance of the system is usually a trained ABUS specialist retail partner.

20. Glossary

Access Manager
The TECTIQ Access Manager is a powerful and comprehensive management software for the ABUS TECTIQ access control system. It is used for commissioning, initial setup and handover of the TECTIQ access control system to the operator and for creating users, issuing access authorisations , creating schedules and managing locking media and system media.

Administrator, Admin
The administrator (admin for short) of the TECTIQ access control system is a person appointed by the operator who is responsible for managing users, door components and locking media. The administrator assigns access rights on behalf of the operator, enters new persons into the system and issues locking media. The TECTIQ Access Manager -, a powerful and comprehensive management software for the ABUS TECTIQ access control system, is available for this purpose. The administrator is the first point of contact for all matters, assigns users to the system and blocks locking media in the event of loss. The operator can appoint several administrators.

Actuators
Electromechanical components, such as electric strikes, door drives, separation systems. The actuators are controlled by the control units of the TECTIQ Update Terminals.

Task list
List automatically generated by the access control system with tasks to be completed (e.g. open parameterisation of door components, battery replacement, etc.). The task list is displayed on the TECTIQ Access Manager dashboard.

Authorisation
A person receives basic access authorisation to selected secure areas if they are authorized to do so - usually by possessing a personal locking medium. Access authorisations for the secured areas are stored on the locking medium and have a limited validity. They must be updated and validated (at the update terminal) and can be linked using a preset schedule.

Fitting
See "Electronic fitting"

Blacklist card
System medium for transferring a blocking list to the door components concerned.

Data-on-Card
Access authorisations are stored on the locking media and not in the offline door components. This means that changes to access authorisations can be managed quickly and easily.

Emergency services
Emergency personnel are members of the rescue service or fire department who need access to the secured building in an emergency. TECTIQ reserves an emergency opening transponder for emergency services, which is stored in a key depot at the property or at the operations centre, for example.

Electronic fitting
Electronic fittings release the operation of the handles after the access authorisation has been checked. They are available in different versions.

Electronic locking cylinder
Electronic locking cylinders activate the locking function after the access authorisation has been checked. This allows the authorized person to open and lock the door.

Event list

Event list automatically generated by the access control system with information on usage and system maintenance. Among other things, messages about granted or denied access attempts and software updates are displayed, Writing locking media, adding or deleting door components. The event list is displayed on the TECTIQ Access Manager dashboard.

Specialist installer
The specialist installer is the expert employee of the registered ABUS specialist retail partner who plans, implements and programs the access control system and instructs the administrators in the system.

Secured area
Area that is secured against unauthorised access by suitable mechanical or other means.

Group authorisation
Access authorisations for door groups or individual doors can be assigned to groups of persons. Group authorisations are inherited by the members of the group of persons. They can then be changed individually for each person. If group authorisations are changed, individual authorisations must be reset if necessary.

Validity, validity interval
The validity of access authorisations can be restricted in the Access Manager. A distinction is made between the following options:
The general personal validity is set via the start date and end date (e.g. company entry until retirement, start and end of maintenance or repairs, start and end of temporary employment). If no start date is set, the authorisation applies from the time the user is created in the system. If no end date is set, the general validity of the person is not restricted.
The validity of the TECTIQ locking medium is usually limited in time and must be extended at an update terminal after the adjustable validity interval has expired.

Validity check
Door components check whether locking media are currently valid. It is possible to deactivate the validity check for door groups. This is useful to allow persons who have a locking medium to access the company premises at a parking lot barrier, for example.

Emergency opening transponder
The emergency opening transponder is used for emergency opening of all TECTIQ door components with the special function "Permanently open". It enables emergency services to gain access to the secured building or area. The emergency opening transponder is usually stored in a fire department key depot at the property.

Users
A user of the TECTIQ access control system is a person authorized by the operator to access protected areas. The access authorisation is valid within the framework of the rules defined by the operator for the areas approved for the user. The user receives a locking medium to which their current access authorisations are transferred before use. The storage duration of the access authorisation on the locking medium can be set by the operator of the access control system. Users are entered in the TECTIQ Access Manager as a "person". Persons can be combined into groups with the same access authorisations .

Office Mode
Office mode sets the TECTIQ door component to permanently open mode. To do this, the function must be activated on the door component and persons must be authorized for permanent opening.
Office mode is activated by a special sequence when the locking medium is presented.
To do this, hold the locking medium in front of the reader of the door component for approx. 4 seconds until it briefly acknowledges "red" - remove the medium from the reading area and present it again. The activation is acknowledged by a "green" signal and the component remains in the coupled state.
Office mode is deactivated manually by presenting an authorized locking medium three times in succession and acknowledging each time with "green". After the third presentation, the door component disengages.
If a time window is selected, Office Mode only needs to be activated and is automatically deactivated at the end of the set time window.

Parameter card
The TECTIQ parameter card is a system medium and is used to transfer configuration data from the TECTIQ Control to the door component. Both during initial programming and when changes are made, the parameter card is written to using the desktop reader and read out on site by the respective component.

Persons, group of persons
Users and owners of a TECTIQ locking medium in a TECTIQ access control system. Persons can be grouped together as persons groups and assigned the same rights. The settings of a person group are inherited by the persons in the group.

Personal validity
See "Validity"

Protocol card
The TECTIQ protocol card is a system medium. It reads log data from the TECTIQ door components. Each TECTIQ door component - fitting, cylinder or wall reader - stores up to 900 entries. These entries include, for example, access granted or denied, battery warnings or battery changes.

Reset card
TECTIQ system medium for resetting TECTIQ door components. Resetting removes the TECTIQ door component from the TECTIQ access control system. The first time the reset card is presented to the door component, the component is reset. The second time it is presented, the door component is reset to the factory settings (delivery status). The system-specific system number is retained.

Locking medium
A TECTIQ locking medium is a transponder for opening and/or locking an area secured with a TECTIQ door component. Electronic locking media contain access authorisation data that is read and written using suitable devices. The data is protected by special encryption technology.

Closing plan
The locking plan clearly displays the current authorisations for persons/groups of persons and doors/door groups. In the locking plan, persons and groups of persons can be granted, changed or revoked access authorisations to doors or door groups.

locking cylinder
See "Electronic locking cylinder"

Barrier
A barrier blocks access to the company premises. Barriers can be set via door groups so that they can be opened by presenting the locking medium without checking the validity of the locking medium.

Block list
List in the TECTIQ Control in which blocked locking media are stored. The blocked list must be transferred to the door component using a blacklist card to prevent unauthorised access to the secured area. The locking medium is only blocked once it has been transferred.

Blocking days
Blocking days are days on which the assigned access authorisation is not valid (e.g. during company vacations, public holidays and other non-operating days).

System medium
TECTIQ system media are - like locking media - electronic transponder systems and have special tasks in a TECTIQ system (parameter card, protocol card, blacklist card, reset card, emergency opening transponder)

System components
Coordinated components of the ABUS TECTIQ access control system. System components are the components in the system that are not directly assigned to access at a door. This primarily concerns update terminals.

TECTIQ system
Abbreviation for a TECTIQ access control system tailored to local conditions.

Desktop reader
The TECTIQ desktop reader is used to read and write locking media and system media. The TECTIQ desktop reader is required for commissioning the system, making changes and granting access rights. It is connected to the computer running the TECTIQ Access Manager locking software via a USB port.
Optionally, the TECTIQ desktop reader can take over the function of the TECTIQ update terminal for updating access authorisations on the locking media.

Door, door group
In a TECTIQ system, a door is synonymous with the reader unit of a door component. Components with two reader units - e.g. double-sided locking cylinders or wall readers - are managed as two doors in the Access Manager software. Doors can be combined as door groups in the software and assigned the same rights. The settings of a door group are inherited by the doors it contains.

Door components
TECTIQ door components work electronically and allow authorized persons access to a secured area. The door components include electronic locking cylinders, electronic fittings and wall readers.

Update terminal
The TECTIQ Online Update Terminal is connected to the TECTIQ Control via a network. It consists of a wall reader combined with the associated control unit. The Online Update Terminal is used for reading and writing locking media and system media, updating access rights and forwarding information, events and feedback from offline door components (accesses made, battery warnings, etc.) to the TECTIQ Control.
The online update terminal can optionally control a door opener or a door operator.

Separation systems
Separation system n are structural installations for controlling access to a room or area, e.g. turnstiles.

Confidants
Confidants enjoy particular trust in their area, e.g. works or staff councils, bullying officers or medical staff.

Wall reader
The TECTIQ wall reader is a door component for activating electronic locking components such as electronic electric strikes, door drives and gates. It consists of a reader unit and control unit and is actuated by presenting the locking medium.

Schedule

Time schedules can be used to limit access authorisation to time intervals to be set (e.g. Monday to Wednesday, 9:00 a.m. to 4:00 p.m.). A schedule can contain several time intervals. Each schedule can also contain up to 30 blocking days.
Only one schedule can be assigned to each person. It can be passed on to the person via the person group or set up as an individual schedule for a person.

Access authorisation

A person receives basic access authorisation to selected secure areas if they are authorized to do so - usually by possessing a personal locking medium. Access authorisations for the secured areas are stored on the locking medium and have a limited validity. They must be updated and validated (at the update terminal) and can be linked using a preset schedule.

Access control system, also: access system

The ABUS TECTIQ access control system is a flexible and scalable electronic security system that enables operators of commercial and public buildings and properties of almost any size to use electronic locking media to grant persons access to secure areas within the framework of the rules and regulations defined by the operator.
The access control system consists of the components TECTIQ Control, TECTIQ Access Manager, TECTIQ desktop reader, TECTIQ system components, TECTIQ door components and TECTIQ locking and system media.

TECTIQ Control, also: control centre

The TECTIQ Control is the core of the access control system. All databases, configurations and services run on its hardware. It stores the doors to be controlled, the users of the system and their access rights. The TECTIQ access control system is set up and managed with the Access Manager according to the operator's requirements. The Access Manager runs on a PC and accesses the TECTIQ Control via a secure connection. The Access Manager and a TECTIQ desktop reader are used to transfer data from the TECTIQ Control to locking media and system media. In systems with TECTIQ Update Terminals, the TECTIQ Control communicates directly with the locking media and system media via fixed secure connections.

21. Index

21 Index

ABUS I Security Center GmbH & Co. KG
abus.com

Linker Kreuthweg 5
86444 Affing
Germany

Phone: +49 82 07 959 90-0
Fax: +49 82 07 959 90-100

sales@abus-sc.com

05 / 2025