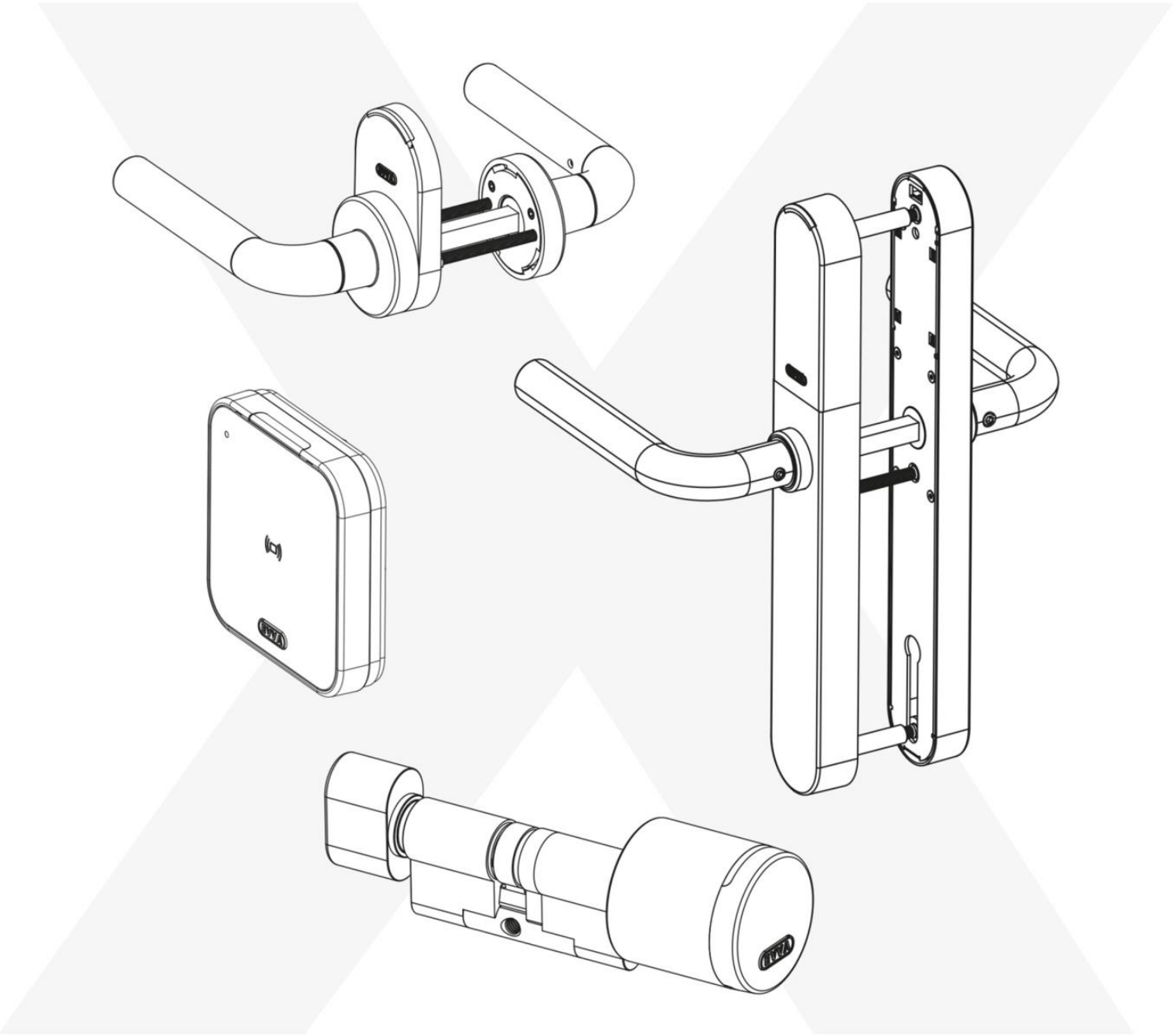
EVVA
access to security



Xesar 2.2

System manual

CONTENTS

1 Introduction

This XESAR system manual describes how to operate the Xesar software and any associated Xesar system components.

The products and/or systems described in the Xesar system manual must exclusively be operated by persons that have been adequately qualified for the corresponding task. Qualified personnel is able to identify risks when handling products/systems and prevent potential hazards on the basis of their expertise.

1.1 General legal notes

EVVA concludes the contract on the use of Xesar exclusively on the basis of its General Terms of Business (EVVA-GTB) as well as its General Licensing Conditions (EVVA-ALB) with regard for the software for the product. Please refer to http://www.evva.at/terms-and-conditions/en/ to view these documents.

We explicitly notify clients that the use of the locking system subject to this contract may trigger legal approval, reporting or registration obligations, in particular with regard to data protection (e.g. if you are establishing a comprehensive information system), as well as grant the right of co-determination to staff in the event of use on corporate premises. Customers, clients and end users shall be responsible for product use in compliance with legal stipulations.

The aforementioned information must be observed and passed on to operators and users as per the defined manufacturer product liability according to product liability legislation. Non-compliance releases EVVA from any liability.
Any use deemed as non-compliant with the contract or as unintended use, any repair work or modifications that have not been explicitly approved by EVVA as well as all types of incorrect servicing may cause malfunctions and are prohibited. Any modifications that have not been explicitly approved by EVVA render claims to liability, warranty as well as any separate guarantee claims void.

Architects and advisory institutions are obliged to request all necessary product information from EVVA and take into account all such information to comply with obligations regarding information and instructions under the Product Liability Act. Specialist retailers and installers must comply with

the information in EVVA documentation and they must pass on such information to customers, if applicable.

Please refer to the Xesar product catalogue for additional information beyond these vital instructions. Please visit: http://www.evva.at/products/electronic-locking-systems-access-control/xesar/system-overview/en/.

1.2 Customer support

We have provided our online form at http://support.evva.at/xesar/en/ in case you have any questions regarding the information below.

- You have exceeded the maximum attempts to enter credit codes.
- Unable to add credit
- A KeyCredit was redeemed, but the remaining credit has not increased

Please contact your local retailer if you have any further questions. We have provided a list of all local EVVA (Certified) Partners here: http://www.evva.at/partners/search-for-retailers/en/

For instance, select a city near you in the first step and click ***Search***. You can additionally restrict the search results here by searching exclusively for Electronic System Partners.
One of our partners near you will be happy to advise you.

For general information on Xesar visit our homepage at
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/system-overview/en/

Legal notice

2. English edition, May 2018
This edition shall not longer be valid upon publication of a new system manual.

We shall not assume any liability for technical or printing errors and their potential consequences. However, the data in this system manual is revised regularly and corrections are incorporated.

1.3 Signs and symbols

Sequences of commands are illustrated as follows.
For instance ***Persons menu > Create person*** or for commands and buttons, such as ***Save***

Warning, risk of material damage in the event of non-compliance with the corresponding safety measures.

Notices and additional information

Hints and recommendations

Error messages

Option Options

2 System overview

Figure 1: System architecture (sample image)

Xesar is the innovation from EVVA.

Developed and manufactured in Austria, the electronic locking system offers companies a wide variety of products. Each Xesar access component brings about its individual benefits to profoundly safeguard your comprehensive security demands. The ideal product for each situation most of all depends on the installation location, security demands and the level of convenience required.

2.1 Xesar access components at a glance

Figure 2: Xesar access components (sample image)

Xesar escutcheon

The all-rounder with a high level of operating convenience. Its unbeaten design is universally suitable, also for metal frame doors. Xesar escutcheons are also perfectly suitable for outdoor applications.

Xesar handle

The Xesar handle is the ideal solution for almost any internal door, from solid doors to glass doors. A convenience product that meets almost any requirements.

Xesar cylinder

Xesar cylinders are ideal if security or easy retrofitting are paramount. It locks securely and is easy to install.

Xesar wall reader (in conjunction with the control unit)

Scores high marks amongst wall readers with high-quality glass design. In conjunction with the control unit it forms an invincible team when it comes to controlling electronic locking components (e.g. automatic sliding doors).

Xesar wall reader as an updater (in conjunction with the updater control unit)

The Xesar wall reader not only unlocks electronically actuated locking elements. The Xesar wall reader with updater control unit plus the identification media in circulation always keep the system up-to-date and secure.

A maximum of 123 updater wall readers can be integrated into a system.

2.2 Xesar system requirements

- Personal computer; at minimum 1.2 GHz or faster
- At minimum 4 GB RAM (32 bit) / 8 GB (64 bit)
- 2x USB host 2.0 for coding stations and Xesar tablet
- Windows 7-32 bit, Windows 7-64 bit, Windows 8.1-32 bit, Windows 8.1-64 bit. Windows 10 32 bit or Windows 10 64 bit operating system
- 1x 100/1000-Ethernet port for network connections to the Online Updaters
- The software must be installed locally, server installations are not intended.
  The installation requires approximately 1 GB free hard disk space.
- Input/output devices:
  Keyboard | Mouse | Minimum screen resolution 1366 x 768
- Internet connection to enable KeyCredits

If, despite an existing Internet connection, the connection with the Xesar software could not be established, configure the settings of the firewall:

Server:	licence.evva.com
Port:	8072
Protokoll:	https

2.3 Xesar performance features

2.3.1 User administration

- Assign access authorisations to software users
- Different software features can be enabled per user role

2.3.2 Xesar access components

- Manual office mode -> (De)activated by an authorised Xesar identification medium at the Xesar access component
- Temporary office mode -> Controlled by time profiles saved in the software
- Enables to define up to 96 door areas -> Merge several doors to facilitate an assignment of authorisations
- Blacklist -> List of blocked identification media
- DeleteKey function -> Blocked identification media are deleted upon attempting identification at the door
- Automatically changes the time -> Summer/winter time
- Software*plus* package -> information exchange through identification medium

2.3.3 Media/user administration

- Up to 65,000 persons per system
- Assign one Xesar identification medium and one replacement medium per person
- Time profiles can be configured for identification media:
  - 7 weekdays, 5 special days
  - Allows to define 50 special days (time profile)
  - Automatically updates the Xesar identification medium upon holding it to the Xesar coding station

Xesar currently supports MIFARE DESFire EV1 with AES 128 bit encryption, all Xesar identification media are equipped with a memory of 4 kB. In version 2.0.x.x the Xesar segment requires 384 bytes, the remaining memory on the Xesar identification medium may be used for external applications (enquire for more detailed information).

Additional 1365 bytes are available for logs with the software^{plus} package.

2.3.4 Protocol/events

- Each Xesar access component logs 1,000 events.
- Events are transferred from door to software using the Xesar tablet.
- Events are transferred from door to software using identification mediums ((Software*plus*)
- It is possible to disable the collection of personal access events.
- Events saved:
    - Access granted (person, date, time, door)
    - Differentiation between identification medium, replacement medium and master key
    - Warning in the event of access using a blocked medium
    - Denial of unauthorised system media
    - Deactivation of blocked medium by component
    - Office mode (automatically and manually)
    - Differentiation between start/end
    - Warning in the event of access during office mode using a blocked medium
    - Door configuration events
    - Media system key changed
    - Firmware update key changed
    - Time change allowed
    - Time changed
    - Door ID set
    - Door area set
    - Special days reset
    - Special days, office mode set
    - Summer/winter time configuration updated
    - Authorisation for manual office mode set
    - List of blocked identification media set
    - Time changed from {date/time} to {date/time}
    - Firmware update failed or completed successfully
    - New access component initialised
    - Information, warnings and errors
    - Component restart
    - Battery empty
    - Unavoidable errors
    - Event log reformatted

- Real-time clock errors

2.3.5 Authorisation types

- Permanent access (without time profile)
- Periodic access (with time profile)
- Manual office mode (can be enabled per medium)
- Automatic office mode (with time profile)
- Expiry of authorisations can be set
- Validity can be set (extended periodically)
- MasterKey authorisation

2.3.6 Available languages

- German
- English
- French
- Italian
- Dutch
- Polish
- Slovakian
- Czech
- Spanish
- Portuguese

3 System accessories

3.1 Xesar coding station

Figure 3: Xesar coding station (sample image)

The Xesar coding station is a read/write device for any type of contactless Xesar identification media as well as the conventional Admin Card medium, which is one of the system cards (see Section: ***Admin Card***). The Xesar coding station provides a separate card slot on the front of the Xesar coding station for the Admin Card. Install the associated driver and connect the Xesar coding station to the USB port of the computer where you installed Xesar software.

We have provided the driver required for the Xesar coding station in the download section of our homepage: http://www.evva.at/products/electronic-locking-systems-access-control/xesar/system-overview/en/.

Please refer to the corresponding data sheet for additional specifications at http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

3.2 Xesar tablet

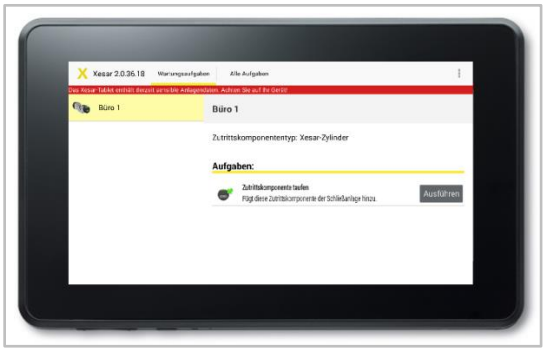


Figure 4: Xesar tablet (sample image)

The Xesar tablet is intended to synchronise and transfer information between Xesar software and Xesar access components.

The Xesar tablet delivery scope includes proprietary EVVA connection cable. Use the connection cable to link your Xesar access components to the Xesar tablet. You can identify the connection cable by the EVVA logo, located on the USB jack of the connection cable.

All Xesar access components feature an interface at the front, behind the connector cover (EVVA logo). Slightly press towards the inside on the left-hand side of the EVVA logo (near the "E") and fold out on the right-hand side (near the "A") to access it.

The integrated interface of the Xesar access component in conjunction with the Xesar tablet is designed to synchronise Xesar software and Xesar access components only.
After use, once again carefully close the connector cover (EVVA logo) of your Xesar access components to continue to protect the connector from penetrating dust and humidity.
For this purpose, do not use pointed objects to prevent damage.

3.2.1 Several tablets in one system

With Xesar version 2.2 you can now also use several Xesar tablets within one Xesar system. This helps you to minimise maintenance costs and efficiently spread updates amongst several engineers.

For this purpose, use the maintenance groups you can assign to tablets and regularly synchronise tablets.

3.2.2 New tablets in existing Xesar systems

The use of a new tablet in an existing Xesar system is relatively easy if the software version of the new tablet is the same or older than the current tablet. Please complete the following procedure for this purpose:

1. Synchronise the tablet with the software. This will load the most recent Xesar app version to the tablet for installation.
2. Then you can use the new tablet with the new software.

3.2.3 One tablet in several Xesar systems

A tablet that has already been used once in a system can also be used in another system in certain conditions.
First, the software versions of the two systems must be compared.
If the software version of the new system is the same or newer than the current system, the following steps are required and must be followed:

1. Perform all pending maintenance tasks in the current system.
2. Synchronise the tablet with the software of the current system in order to synchronise all data with the software.
3. Then all existing data of the current system must be removed from the tablet before a synchronisation in the new system may take place. For this purpose, use the Xesar tablet and go to Manage apps /Xesar tablet/Delete data in the menu structure.

Further details can be found in the data sheets under the following link:

http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

Do not install any additional applications since in this case, EVVA can no longer guarantee product safety and functionality.

Do not install any operating system updates and run the tablet in flight mode!

The Xesar tablet cannot be used as an emergency power supply for battery-powered Xesar access components.

We recommend to regularly synchronize each Xesar access component, in order to ensure a regular event synchronization (attention: max. 1000 events per access component can be synchronized after that the oldest entries will be overwritten.) In order to keep the date and time of the access components synchronized, please run the synchronization at least once a year.

3.2.4 Functional principle

Any maintenance tasks or any other tasks for the corresponding Xesar access component are loaded and listed upon each synchronisation between Xesar tablet and Xesar software.

The connecting cable enclosed with your Xesar tablet enables to connect the Xesar access component and subsequently exchange data using the Xesar app.

It enables the following:

- Initialising Xesar access components (upon commissioning)
- Synchronising changed door parameters in Xesar access components
- Transferring blacklists to Xesar access components

- Battery status queries
- Firmware updates (Xesar access components in battery mode are supplied with energy from the Xesar tablet during firmware updates)

- Retrieving Xesar access component events

- Resetting Xesar access components to construction mode

- Automatically synchronising the time in access components upon communication between tablet and access components

3.2.5 Xesar application (app)

The Xesar application is already preinstalled on your Xesar tablet. The Xesar application is automatically updated once a more recent application version becomes available, for instance following initial Xesar software installations or software updates upon synchronising with the Xesar tablet.

We have enclosed the manufacturer's independent user guide for the Xesar tablet. It is enclosed with the product packaging.

Fully charge your Xesar tablet prior to first use.

3.3 Emergency power device

Figure 5: Emergency power device (sample image)

All access components feature an interface at the front of the access component, below the EVVA logo. Slightly press towards the inside on the left-hand side of the logo (near the "E") and fold out on the right-hand side (near the "A") to access it. The installed interface in conjunction with the emergency power device is intended for emergency power supply only and it is not required as part of normal operation.

Immediately replace batteries after having used the emergency power device to operate access components and subsequently update access components using the Xesar tablet to once again enable access with all authorised identification media.

Option The emergency power device is optionally available.
Product code: E.ZU.NG.V1

Please note that you require a Xesar identification medium with MasterKey authorisation to open Xesar access components supplied with the emergency power supply as the time setting is lost if the power supply is interrupted for too long, causing standard media to be unable to open them.

4 System medium

4.1 Admin Card

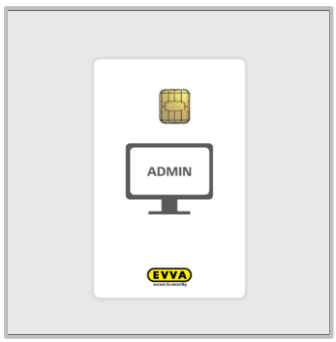


Figure 6: Admin Card (sample image)

The Admin Card is a contact-type, electronic chip card in standard format. It enables to access the Xesar software and uniquely identifies the system. Any KeyCredits purchased to make changes to authorisations are saved on the card (also applies to KeyCredits Unlimited).

Xesar software only enables the full range of functionality if a valid Admin Card with sufficient credit has been inserted into the Xesar coding station.

The Admin Card is not transferable and hence it cannot be used for other systems.

You can replace the Admin Card in the event of loss or damage.

5 Xesar identification media

Xesar identification media are non-contact RFID chips based on MIFARE DESFire EV1 with an overall memory capacity of 4 kB.

Overview of available Xesar identification media

Xesar EVVA Card

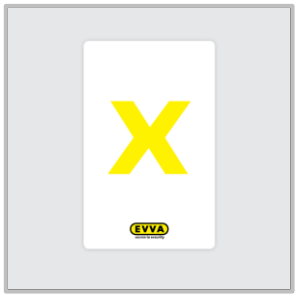


Figure 7: Xesar EVVA Card (sample image)

Xesar Partner Card

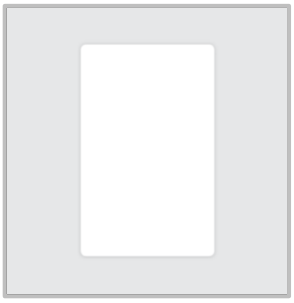


Figure 8: Xesar Partner Card (sample image)

Xesar key tag

Figure 9: Xesar key tag (sample image)

Xesar combi key[1]

Figure 10: Xesar combi key (sample image)

Do not place more than one Xesar identification medium on the Xesar coding station. Otherwise identification media may be incorrectly configured.

[1] In preparation

Please keep metal objects from the coding station as they may impair reader functionality.

Please refer to the corresponding data sheet for additional specifications at http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

Once your system is no longer in construction mode following commissioning, you can use Xesar identification media programmed with the Xesar coding station to open Xesar access components.

Construction mode is active as long as the Xesar access component has not been assigned to a system. Every Xesar access component is in this state upon delivery.

All Xesar identification media types are programmed using the Xesar coding station by placing the identification media on an operating coding station and following the corresponding instructions in the software.

media provide memory capacities to save a maximum of 96 door areas and an additional 32 doors.

5.1 Construction Card

Figure 11: Construction Card (sample image)

The Construction Card is a contactless RFID chip based on MIFARE DESFire EV1, which is able to open Xesar access components in construction mode.

Manual office mode is also available in addition to conventional access component operation (see Section: ***Manual office*** mode**)**. The Construction Card is ready for use immediately and it must not be programmed using the Xesar coding station.

Construction mode is active as long as the Xesar access component has not been assigned to a system. Upon delivery, each Xesar access component is in construction mode.

Please note that your system can be operated with any Construction Card when it is in construction mode. For this reason, initialise your system as quickly as possible.

5.2 Access with a Xesar identification medium

Xesar identification media can be used to operate access components according to the same principle. The reader unit is located in the black cap above the connector cover (EVVA logo). The cor-

responding access component reacts as configured once an authorised identification medium is held to the reader field.

5.2.1 Single access (standard configuration)

In this process, the corresponding Xesar access component unlocks for five seconds after having used a corresponding access component. Unlocking is confirmed by a visual and acoustic signal. Unlocking is then completed automatically and the system once again confirms this with a visual and an acoustic signal.

5.2.2 Manual office mode

Each Xesar access component features a manual office mode function. It enables to engage access components or keep them open. This function is also available in factory state (construction mode) in conjunction with the Construction Card.

Manual office mode is (de)activated by holding the identification medium to the corresponding Xesar access component twice within a space of two seconds. The Xesar access component indicates the status change with an acoustic and a visual signal (refer to ***How Xesar access component indicate even).*** Configure this function in the Xesar software if Xesar access components have already been assigned to the system.

Please note that you must move the identification medium away from the reader field (approximately 20 cm) each time you hold it to the access component to (de)activate office mode.

When the battery charge reaches a low level, a Battery warning is issued.
In this state, no automatic or manual office opening to be started.
Current permanent openings (automatic / manual), however, can still be closed. In addition, a clear log entry is applied to indicate not started automatic continuous openings.

5.2.3 Automatic office mode (schedule-based)

In addition to manual office mode, Xesar components can also be set to office mode automatically. In this process, you can set a certain time window in the Xesar software. The

Xesar access component indicates the status change of automatic office mode acoustically and visually (refer to ***How Xesar access component indicate even).***
Automatic office mode in factory state in conjunction with the Construction Card is not possible.

When the battery charge reaches a low level, a Battery warning is issued.
In this state, no automatic or manual office opening to be started.
Current permanent openings (automatic / manual), however, can still be closed. In addition, a clear log entry is applied to indicate not started automatic continuous openings.

5.2.4 DeleteKey function

The blacklist (= list of all blocked media within a system) is transmitted to each Xesar access component upon updating. If a medium on the blacklist is used at a door component, the access component deletes it, regardless of whether or not it was authorised for the respective door.

Manual and automatic office mode are equivalent with regard to authorisations. For this reason, users with appropriate authorisations can manually suspend or reactivate automatic office mode. Manual office mode can also be deactivated by schedule-based, automatic office mode, providing this has been configured accordingly in the software.

5.3 Xesar access component interface

All Xesar access components feature an interface to update Xesar access components. The interface may also be used as an emergency power supply for battery-operated Xesar access components.

The interface is located on the front of all Xesar access components, behind the connector cover (EVVA logo). Slightly press towards the inside on the left-hand side of the EVVA logo (near the "E") with your finger and fold out on the right-hand side (near the "A") and access the interface.

After having used the interface, once again carefully close the connector cover (EVVA logo) to protect the your Xesar access components from penetrating dust and humidity.

Do not use pointed objects to open and close the cover to prevent potential damage.

6 Xesar software

Figure 12: Xesar software (sample image)

EVVA provides the Xesar software free of charge as an administration and management tool suitable for the most diverse requirements. These include managing personal authorisations, creating and deleting electronic keys, managing different access components, setting up time zones depending on authorisations, creating and managing areas, managing schedule-based office mode options and many more functions.

In addition to password protection, the Xesar software features an additional security feature to enhance the security of your system, the Admin Card.
(Refer to Section: ***Admin Card)***

Register online to download the Xesar software:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/demand-xesar-software/en/

The Xesar software must be installed locally, server installations are not intended.
The installation requires approximately 1 GB free hard disk space.

6.1 EVVA KeyCredits

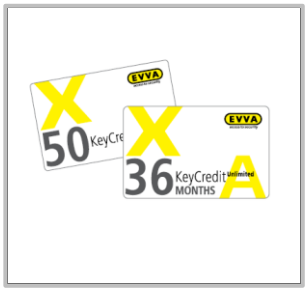


Figure 13: KeyCredits (sample image)

You benefit from all the free features of a comprehensive access software and with KeyCredits you only pay what you actually need. Merely one KeyCredit is necessary to create or change an identification medium with any number of access authorisations.

6.1.1 Credit schemes

We provide the following credit schemes:

- Quantity credit (10/50/100 KeyCredits)
- Time-based credit (KeyCredit Unlimited with an unlimited number of access authorisation changes for a duration of 12 or 36 months)
- Software^{plus}-package (to use the virtual network XVN)

6.1.2 You can merge quantity-based and time-based credit.

Any currently valid flat rate for time-based credit covers all authorisation changes that are subject to a charge and EVVA KeyCredits are only deducted from the quantity credit for authorisation changes that are subject to a charge once the time-based credit has expired.

6.1.3 Functional principle

EVVA KeyCredits are enabled and locally saved on the Admin Card once you have entered the code from the card in the Xesar software.

Time-based, limited flat rate KeyCredits, for instance with a flat rate for either 12 or 36 months, are saved on the EVVA Server and not on the Admin Card.

In the event that an Admin Card with time-based credit is lost or develops a fault, the remaining time-based credit of the 12/36-month flat rate saved on the server can be accessed and reactivated after having issued a replacement card. It is not possible to reactivate any remaining credit for quantity credits of 10/50/100 KeyCredits on faulty or lost Admin Cards.

Please note that you require an Internet connection to enable loaded KeyCredits.

Credit must have already been activated to be able to replace an Admin Card.

6.1.4 Changes charged in KeyCredits (relevant to quantity credit only)

You will be deducted **one** KeyCredit for the following changes:

- Changing access authorisations for doors/areas
- Changing time profiles (permanent access/periodic access)
- Changing the expiry date of identification media

The system always deducts one KeyCredit upon saving (after having created or changed authorisations).

6.1.5 No KeyCredits deducted

You will not be deducted **any** KeyCredits for the following changes:

- (De)activating manual office mode for a person
- Blocking persons (blacklist)
- Writing to/updating media
- Changing personal master data
- Extending the identification media validity

6.1.6 Additional information about EVVA KeyCredits

- When you load KeyCredit Unlimited, the new period is added on to any on-going KeyCredit Unlimited product validity periods.
- KeyCredit codes can be redeemed only once.
- Any KeyCredit codes available upon market launch can be redeemed for Xesar and AirKey.
- The Xesar software notifies users in due time before expiry of the KeyCredits.

The SoftwarePlus voucher code must be used from Xesar version 2.0.x.x and higher only.The code will be permanently invalidated if it is entered in an older version.

Never unplug the coding station from your PC while activating new KeyCredits, to ensure a successful charge.

6.2 Software*plus* -package

Figure 14: Software*plus*-package (sample image)

By activating the Software*plus* package, events must no longer be constantly transported via the Xesar tablet to the software, but are "picked up" by the identification medium.
If an identification medium is held to an access component, events will be written onto the media. By putting medium back on the coding station, events are transported back into the software.

Informations about the Software*plus*-package

- The Software*plus* card can be purchased from an EVVA distributor.
- Information about the Software*plus* is displayed on the Dashboard (homepage).
- Additional Credits can be activated by clicking on ***Add Software*plus*- package***
- A single Software*plus*-package is valid for 3 years, additional Software*plus*-package extend the licence accordenly
- The Software*plus*-package (XVN functionality) also works without inserted Admin-Card (if active)
- A Software*plus*-package stays valid, even after the exchange of the Admin-Card. (The additional KeyCredits acquired with the package expire however)

7 Xesar access components

7.1 Xesar escutcheon

Figure 15: Xesar escutcheon (sample image)

The Xesar escutcheon is a battery-operated access component suitable for indoor and outdoor use.

Please use the dedicated seal enclosed with the product in the event of use outdoors or in areas that are exposed to water.

The Xesar escutcheon is suitable for conventional metal frames and solid door locks with a handle range of up to 40°, for self-locking escape door locks as per EN 179/EN 1125, fire protection doors and there are also versions available for panic and emergency exit doors with bar handles or push handles as per EN 1125[1].

Please check carefully to make sure the Xesar product you selected is suitable for your application.

7.1.1 Xesar escutcheon — functional description

Figure 16: Xesar escutcheon (sample image)

Visual and acoustic feedback:

Xesar escutcheons indicate events acoustically and visually. For this purpose, there is an LED on the upper edge of the reader unit of Xesar escutcheons. For a list of all signals please refer to Section: ***How Xesar access component indicate even***

Reader unit:

The reader unit sensor is located on the outside of the Xesar escutcheon between the connector (EVVA logo) and the LED.

Connector (synchronisation, updates, emergency power supply):

Xesar escutcheons feature a connector located under the connector cover (EVVA logo). Slightly press towards the inside on the left-hand side of the EVVA logo (near the "E") and fold out on the right-hand side (near the "A") to access the connector.

The connector is intended for synchronisation with Xesar tablets as well as for emergency power supply using the optional emergency power device.

After use, once again carefully close the connector cover (EVVA logo) to protect the connector from penetrating dust and humidity. For this purpose, do not use pointed objects to prevent damage.

Functional principle:

The outside handle is disengaged by default – operating the outside handle will not change the position of the latch. Hold an authorised Xesar identification medium to the reader unit to mechatronically engage the outside handle for five seconds. If you operate the outside handle during this period, the latch or bolt (depending on the lock type) will be retrieved.

The inside handle is always engaged and can be operated at any time. In this process, the mechanism always unlocks the latch.

Xesar escutcheons feature an event memory for the last 1,000 events. Once the event memory is full, the system overwrites the oldest entries with the most recent events. For this reason, it is important to regularly synchronise events to prevent event records from being lost.

Please refer to the corresponding data sheet for additional specifications at:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

Please note the office mode function (Section: ***Xesar*** identification media) and the different acoustic and visual signals (Section:***How Xesar access component indicate even).***

Please note that if access components are installed in fire doors, the certificates are exclusively valid in conjunction with approvals from the corresponding door manufacturer.

Please note the following, important notices before use!

Conditions of use

External ambient temperatures -20 °C to +60 °C, internal ambient temperatures 0 °C to +60 °C (depending on the battery) | Humidity < 90 %, non-condensing | for ≥ 200,000 cycles as per EN 1906[1]

Climatic and environmental effects

Note the defined suitability of the escutcheon for the respective ambient conditions as per its IP rating and specific temperature range.
Do not use the escutcheon in very dusty environments.
Use the escutcheon in environments with a humidity below 90% only.
Clarify the application options with a specialist retailer before installing escutcheons in environments with a particularly high level of static charges.
Do not use escutcheons in corrosive atmospheres (e.g. chlorine, ammonia, lime water or salt water).

Information regarding installation and the correct installation situation

Exclusively specialist personnel must install escutcheons according to the specifications in the assembly manual enclosed with the product. EVVA shall assume no liability for any kind for damage resulting from improper assembly/installation.
Please note that the maximum nut correction position of the mortise lock must be 2° to ensure the Xesar escutcheon operates correctly, as otherwise malfunctions cannot be excluded.
Check the lock for damage and dirt before assembling/installing the escutcheon. Please also observe the instructions of the lock manufacturer prior to installation of the escutcheon.
EVVA recommends using correctly operating mortise locks to safeguard the escutcheon operates correctly.
Observe the corresponding international and national specifications in the corresponding legislation, directives, standards and guidelines, particularly regarding the requirements for escape routes and emergency exits, during project management and installation of the escutcheons.
Note that you must choose the correct cylinder length depending on the door panel thickness when installing mechanical lock cylinders. In installation situations or applications that are critical to security the lock cylinder must protrude from the protective escutcheon by a maximum of 3 mm.
Before installing escutcheons – in particular in metal frame doors – check the installation situation to prevent injuries (e.g. squashed limbs). In these cases, we recommend using a handle suitable for metal frame doors.
Please note that if you install the escutcheon in smoke control/fire doors, you must verify the components' suitability and potentially also obtain approval from the door manufacturer. The client shall be responsible for this.
A certificate in compliance with EN 179 or EN 1125 from the lock manufacturer is crucial for use of the escutcheon in escape or panic doors. Check the correct function of the complete panic unit,

consisting of escutcheon, panic lock and panic bar. The aforementioned certificate must confirm the escutcheons' suitability for installation.
An excessive tightening torque when fastening the fixing screws may cause escutcheon malfunctions or make it hard to operate the escutcheon. For this reason, note the data in the assembly manual.
Before completing the installation, use a Construction Card to verify the correct function of the escutcheon when the door is open as per the specifications in the assembly manual.
After having installed the escutcheon, note that you can only operate the system using a Construction Card until parameters have been completely configured.
Note that in the event of a clearance within the cylinder area of the door panel you are required to seal the area using a conventional, mechanical cylinder, a blind cylinder or fire protection laminate. EVVA explicitly declares that this is the only method to maintain the validity of the fire protection certificate for the escutcheon.

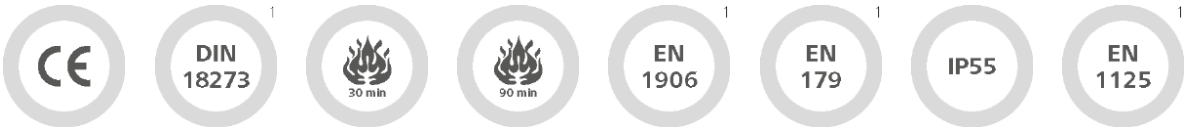
Information on operation

Instruct users of the electronic locking system to always keep identification media safe.
In the event that Xesar identification media is lost, it must be immediately blocked using the software. The mechatronic lock cylinder must be immediately updated using the Xesar tablet.
Do not carry or lift the door panel using the handle.
Do not cover the reader equipment of the escutcheon with metal materials.
Regularly check the correct condition and function of the escutcheon (at minimum once a month) as part of a functional check using authorised identification media.
We recommend you keep the locking system up-to-date by regularly installing software and firmware updates. Make sure to run firmware updates when the door is open and run a functional test after having completed the update.

Cleaning information

Use a soft, lint-free cloth and soapy water to clean any visible areas of the escutcheon. Do not use corrosive products or sprays that may be aggressive on metal surfaces, plastics or sealants and seals.

Standards and guidelines



CE tested | DIN 18273[1] | EN 1634: 30 minutes | EN 1634: 90 minutes[1] | Austrian standard 3859: 30 minutes[1] | Austrian standard 3859: 90 minutes[1] | EN 1906[1] | EN 179[1] | IP52 protection (when using enclosed seals IP55) | DIN 18257:ES0[1] (with stability plate) | ÖNORM (Austrian standard) B 5351:WB1[1] (ÖNORM B 5338:WK1)

The Xesar escutcheon for fire doors is suitable for fire doors as per EN 179[1]. Suitable for internal and external doors | Can be combined with conventional solid door locks with a handle range of up to 40° | Can be combined with self-locking fire door locks as per EN 179/EN 1125[1] | Suitable for fire protection doors

Battery replacements

We recommend to have batteries replaced by trained, specialist personnel only.
Replace batteries in due time, as soon as the escutcheon indicates "Battery low", see Section "How Xesar access component indicate even".
Repeatedly disregarding the "Battery low" warning may cause escutcheon malfunctions.
At normal ambient temperatures, the first "Battery low" warning indicates that up to 1,000 actuations are still possible within the next 4 weeks. Temperatures deviating from normal ambient temperatures may cause the escutcheon to prematurely fail.
Do not use rechargeable batteries. Please ask your specialist retailer for a list of recommended battery models.
Always replace all batteries used (three AAA batteries) in the corresponding lock cylinder! If applicable, you may be required to synchronise the system time using the Xesar tablet after having replaced the batteries.
If the sealing kit has been applied, make sure not to damage the seal upon changing batteries.
If the batteries are drained, it is exclusively possible to operate the escutcheon using the emergency power device (optional accessory).

Battery replacement procedure

1. The battery compartment is located in the top of the internal escutcheon plate. You require a T8 Torx screwdriver to open the battery compartment.

2. Turn the Torx screw clockwise until you can remove the internal escutcheon plate.
3. Hold the bottom of the internal escutcheon plate and carefully remove it from the attachment panel. You can now pull the internal escutcheon plate over the handle. Make sure you do not scratch the handle in the process. You can alternatively remove the internal handle beforehand.
4. Now remove the three empty AAA batteries and replace them with new batteries you acquired earlier. Ensure correct polarity when inserting batteries.

Battery replacements or power cuts must not exceed a duration of one minute as otherwise the escutcheon must be resynchronised using the Xesar tablet.

The component outputs a signal to confirm having correctly completed the battery replacement (signal 8 in the signal table from Section***: How Xesar access component indicate even)***
Now once again position the internal escutcheon plate on the attachment plate and proceed in reverse order to reassemble the internal escutcheon plate.

The procedure to replace batteries in Xesar escutcheons for panic doors is identical despite the different internal escutcheon plate's design.

7.2 Xesar handle

Figure 17: Xesar handle (sample image)

The Xesar handle is a battery-operated access component suitable for internal solid or glass doors. Thanks to compliance with fundamental lock standards and a handle range of up to 40° the Xesar handle is compatible with many European lock types.

The Xesar handle is suitable for conventional solid door locks with a handle range of up to 40°, self-locking escape door locks as per EN 179 and fire protection doors.

Please check carefully to make sure the Xesar product you selected is suitable for your application. We have made the required data sheet available in the download section of our homepage: http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

7.2.1 Xesar handle — functional description

Figure 18: Xesar handle (sample image)

Visual and acoustic feedback:

Xesar handles indicate events acoustically and visually. For this purpose, there is an LED on the upper edge of the reader unit of Xesar handles. For a list of all signals please refer to Section:How Xesar access component indicate even.

Reader unit:

The reader unit sensor is located on the outside of the Xesar handle between the connector (EVVA logo) and the LED.

Connector (synchronisation, updates, emergency power supply)

Xesar handles feature a connector located under the connector cover (EVVA logo). Slightly press towards the inside on the left-hand side of the EVVA logo (near the "E") and fold out on the right-hand side (near the "A") to access the connector.
The connector is intended for synchronisation with Xesar tablets as well as for emergency power supply using the optional emergency power device. After use, once again carefully close the connector cover (EVVA logo) to protect the connector from penetrating dust and humidity. For this purpose, do not use pointed objects to prevent damage.

Functional principle

The outside handle is disengaged by default – operating the outside handle will not change the position of the latch. Hold an authorised Xesar identification medium to the

reader unit to mechatronically engage the outside handle for five seconds. If you operate the outside handle during this period, the latch or bolt (depending on the lock type) will be retrieved.

The inside handle is always engaged and can be operated at any time. In this process, the mechanism always unlocks the latch.

Xesar handles feature an event memory for the last 1,000 events. Once the event memory is full, the system overwrites the oldest entries with the most recent events. For this reason, it is important to regularly synchronise events to prevent event records from being lost.

Please refer to the corresponding data sheet for additional specifications at:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

Please note the office mode function (Section***: Xesar identification media***) and the different acoustic and visual signals (Section: ***How Xesar access component indicate even).***
Please note that if access components are installed in fire doors, the certificates are exclusively valid in conjunction with approvals from the corresponding door manufacturer.

Please note the following, important notices before use!

Climatic and environmental effects

Note the defined suitability of the handle for the respective ambient conditions as per its IP rating and specific temperature range.

Do not use the handles in very dusty environments.

Use the handles in environments with a humidity below 90% only.

Clarify the application options with a specialist retailer before installing handles in environments with a particularly high level of static charges.

Do not use handles in corrosive atmospheres (e.g. chlorine, ammonia, lime water or salt water).

Conditions of use

Ambient temperature +5 °C to +50 °C (depending on the battery) | Humidity < 90 %, non-condensing | For 200,000 cycles as per EN 1906[1] | IP40 protection

Information regarding installation and the correct installation situation

Exclusively specialist personnel must install handles according to the specifications in the assembly manual enclosed with the product. EVVA shall assume no liability for any kind for damage resulting from improper assembly/installation.

Note that the maximum nut correction position of the mortise lock must be 5° to ensure the Xesar handle operates correctly, as otherwise malfunctions cannot be excluded.

Check the lock for damage and dirt before assembling/installing the handle. Please also observe the instructions of the lock manufacturer prior to assembly/installation. EVVA recommends using correctly operating mortise locks to safeguard the handle operates correctly.

Exclusively use accessories and spare parts recommended by EVVA.

Please observe the corresponding international and national specifications in the corresponding legislation, directives, standards and guidelines, particularly regarding the requirements for escape routes and emergency exits, during project management and installation of the handles.

Note that changing over the handle from one side to the other must be performed in accordance with the specifications in the assembly manual and exclusively when the battery has been removed.

Please note that if you would like to install the handle in smoke control/fire doors, you must verify the handles' suitability and potentially also obtain approval from the door manufacturer. The client shall be responsible for this.

A certificate in compliance with EN 179 or EN 1125 from the lock manufacturer is crucial for use of the handle in escape or panic doors. Check the correct function of the complete panic unit, consisting of panic lock and handle fittings. The aforementioned certificate must confirm the handles' suitability for installation.

An excessive tightening torque when fastening the fixing screws may cause handle malfunctions or make it hard to operate the handle. For this reason, note the data in the assembly manual.
Before completing the installation, use a Construction Card to verify the correct function of the handle when the door is open as per the specifications in the assembly manual.
After having installed the handle, please note that you can only operate the system using a Construction Card until parameters have been completely configured.

Information on operation

Instruct users of the electronic locking system to always keep identification media safe.
In the event that Xesar identification media is lost, it must be immediately blocked using the software. The mechatronic lock cylinder must be immediately updated.
Do not carry or lift the door panel using the handle.
Do not cover the reader equipment of the handle with metal materials.
Regularly check the correct condition and function of the handle (at minimum once a month) as part of a functional check using authorised identification media.
We recommend you keep the locking system up-to-date by regularly installing software and firmware updates. Make sure to run firmware updates when the door is open and run a functional test after having completed the update.

Cleaning information

Use a soft, lint-free cloth and soapy water to clean any visible areas of the escutcheon. Do not use corrosive products or sprays that may be aggressive on metal surfaces, plastics or sealants and seals.

Standards and guidelines

CE tested | DIN 18273[1] | EN 1634: 30 minutes | EN 1634: 90 minutes[1] | Austrian standard 3859: 30 minutes[1] | Austrian standard 3859: 90 minutes[1] | EN 1906[1] | EN 179[1] | IP40 protection

Battery replacements

We recommend to have batteries replaced by trained, specialist personnel only.
Replace batteries in due time, as soon as the handle indicates "Battery low", see Section *"How Xesar access component indicate even".*
Repeatedly disregarding the "Battery low" warning may cause handle malfunctions.
At normal ambient temperatures, the first "Battery low" warning indicates that up to 1,000 actuations are still possible within the next 4 weeks. Temperatures deviating from normal ambient temperatures may cause the handle to prematurely fail.
Do not use rechargeable batteries. Please ask your specialist retailer for a list of recommended battery models.
If the batteries have been drained, it is exclusively possible to operate the handle using the emergency power device (optional accessory).

1[1] In preparation | [2] When using the enclosed seals

Battery replacement procedure

1. The battery compartment is located in the outside handle of the Xesar handle. You require one type CR123A battery (please ask you retailer for a list of recommended battery models) and the following tools to open the battery compartment: Allen key, 2.5.
2. If you would like to remove the handle tube of the outside handle, use the Allen key and turn the attachment screw anti-clockwise until you can remove the handle tube.
3. Make sure you only screw in the attachment screw as far as absolutely necessary.
4. Now remove the empty battery and replace it with a new battery you acquired earlier. Ensure correct polarity when inserting the battery.
5. Once again position the handle tube on the outside handle and fasten it in reverse sequence.

The component outputs a signal to confirm having correctly completed the battery replacement (signal 8 in the signal table from Section*: How Xesar access component indicate even)*

Battery replacements or power cuts must not exceed a duration of one minute as otherwise the Xesar handle must be resynchronised using the Xesar tablet.

7.3 Xesar cylinder

Figure 19: Xesar cylinder (sample image)

Xesar cylinders are battery-operated access components.
The standard Xesar cylinder version already comes with a host of anti-manipulation protection measures. Please refer to the product catalogue for more information.

Xesar cylinders are suitable for indoors and outdoors as well as fire and emergency exit doors. Xesar cylinders are available as half cylinders or double cylinders with one-sided or double-sided, electronic access.

Please carefully check the Xesar cylinder you selected is suitable for your application.

Please refer to the corresponding data sheet for additional specifications at:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/system-overview/en/

7.3.1 Xesar cylinder — functional description

Figure 20: Xesar thumbturn (sample image)

Visual and acoustic feedback

Xesar cylinders indicate events acoustically and visually. For this purpose, there is an LED on the edge of the reader unit on Xesar cylinders. For a list of all available signals please refer to Section: *How Xesar access component indicate even.*

Reader unit

The reader unit sensor is located in the plastic cap of the Xesar cylinder thumbturn between the EVVA logo and the LED.

Connector (synchronisation, updates, emergency power supply)

Xesar cylinders feature a connector located under the connector cover (EVVA logo). Slightly press towards the inside on the left-hand side of the EVVA logo (near the "E") and fold out on the right-hand side (near the "A") to access the connector.

The connector is intended for synchronisation with Xesar tablets as well as for emergency power supply using the optional emergency power device.

After use, once again carefully close the connector cover (EVVA logo) to protect the connector from penetrating dust and humidity. For this purpose, do not use pointed objects to prevent damage.

Functional principle

By default, the electronic outside thumbturn of the Xesar cylinder is disengaged. The cam remains disengaged upon operating the outside thumbturn and the outside thumbturn turns without engaging with the cam.
Hold an authorised Xesar identification medium to the reader unit of the Xesar cylinder to mechatronically engage the outside thumbturn for five seconds so the cam of the Xesar cylinder engages when operating the outside thumbturn.
The purely mechanically operated inside of versions with one-sided, electronic authorisation always remains engaged on Xesar cylinders and can be operated at any time.
On Xesar cylinders with double-sided, electronic authorisation the inside thumbturn operates identically to the electronic outside thumbturn.
Xesar cylinders feature an event memory for the last 1,000 events. Once the event memory is full, the system overwrites the oldest entries with the most recent events. For this reason, it is important to regularly synchronise events to prevent event records from being lost.

Please refer to the corresponding data sheet for additional specifications at:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

FZG and FAP versions do not feature a rotary damper for technical reasons.

Please note the office mode function (Section: ***Xesar*** identification media) and the different acoustic and visual signals (Section:How Xesar access component indicate even)

Xesar cylinders feature a rotary damper as standard. Ensure it is installed in its correct position (see assembly manual) as malfunctions would otherwise occur during on-going operation. Malfunctions in unapproved installation positions do not repre-

sent product faults and are consequently not deemed as a valid reason for complaints.

Please note the following, important notices before use!

Climatic and environmental effects

Please note the defined suitability of the lock cylinder for the respective ambient conditions as per its IP rating and specific temperature range.

Do not use the lock cylinder in very dusty environments.

Use the lock cylinder in environments with a humidity below 90% only.
Clarify the application options with a specialist retailer before installing lock cylinders in environments with a particularly high level of static charge.
Do not use lock cylinders in corrosive atmospheres (e.g. chlorine, ammonia, lime water or salt water).

Information regarding installation and the correct installation situation
Exclusively specialist personnel must install lock cylinders according to the specifications in the assembly manual which is also enclosed with the product. EVVA shall assume no liability for any kind for damage resulting from improper assembly/installation.

Check the lock for damage and dirt before assembling/installing the lock cylinder. Please also observe the instructions of the lock manufacturer prior to assembly/installation. EVVA recommends using correctly operating mortise locks to safeguard the lock cylinder operates correctly.

All Xesar access components are delivered ex works in so-called construction mode. In this condition any Construction Card unlocks any Xesar access component. For this reason, immediately after having installed each Xesar access component ensure it is correctly added to the locking system so that exclusively authorised persons have access.

Exclusively use accessories and spare parts recommended by EVVA. Mechatronic lock cylinders are exclusively fully suitable for assembly/installation in locks, escutcheons, etc. if the lock cylinders are subject to the corresponding dimensional standards and the respective locks, escutcheons, etc. are exclusively designed to accommodate mechatronic lock cylinders as per said standards. In all other cases, manufacturers, retailers and users of such locks, escutcheons and similar devices must be certain that the lock cylinder they select is suitable for installation and its intended use.

Observe the corresponding international and national specifications in the corresponding legislation, directives, standards and guidelines, particularly regarding the requirements for escape routes and emergency exits, during project management and installation of the lock cylinders.

Before installing lock cylinders – in particular in metal frame doors – check the installation situation to prevent injuries (e.g. squashed limbs) or damage to the lock cylinder.

Ensure you selected the correct cylinder length for the corresponding door configuration. In installation situations or applications that are critical to security (without taking into account the thumbturn) the cylinder must protrude from the protective escutcheon by a maximum of 3 mm.

If VdS-certified mechatronic lock cylinders are installed in installation situations critical to security, the lock cylinder must be protected by VdS-certified, burglary-resistent, category B or C door plates. With regard to all other doors, the degree of anti-burglary measures must comply with the corresponding, national regulations (see also EN 1627, Austrian standard 5338 or SKG).

Please note the restrictions illustrated in the assembly manual regarding the permissible installation positions of the lock cylinder. Non-compliance with the correct installation situation may cause malfunctions – malfunctions in unapproved installation positions do not represent product faults and are consequently not deemed as a valid reason for complaints. Please note that the correct lock cylinder function can also only be ensured before and during installation of the lock cylinder if the cylinder housing is positioned correctly.
Lock cylinders must be installed in such a way that they are not subject to any external forces except when used correctly and at the designated mounting points.

A certificate in compliance with EN 179 or EN 1125 from the lock manufacturer is crucial for use of the lock cylinder in escape or panic doors. Check the correct function of the complete panic unit, consisting of lock cylinder, panic lock, panic bar and handle fittings. The aforementioned certificate must confirm the lock cylinders' suitability for installation.

Please note that if you would like to install the lock cylinder in smoke control/fire doors, you must verify the cylinders' suitability and potentially also obtain approval from the door manufacturer. The client shall be responsible for this.

An excessive tightening torque when fastening the cylinder fixing screw may cause lock cylinder malfunctions or make it hard to operate the lock cylinder. For this reason, please note the data in the assembly manual.

Before completing the installation, use a Construction Card to verify the correct function of the lock cylinder when the door is open as per the specifications in the assembly manual.

After having installed the lock cylinder, note that you can only operate the system using a Construction Card until parameters have been completely configured.

Please note that the corresponding IP rating of lock cylinders with elongated outside turn sleeves can only be safeguarded if the elongated outside turn sleeve protrudes from the protective escutcheon by a maximum of 3 mm.

Information on operation

Instruct users of the electronic locking system to always keep identification media safe.

In the event that Xesar identification media is lost, it must be immediately blocked using the software. The corresponding lock cylinder must be immediately updated using the Xesar tablet.

Please note that a door is not automatically locked after having closed it. Doors must be locked manually by turning the thumbturn. In the event that it is not possible to remove the thumbturn, attempt to set the lock cylinder to office mode and then remove it as usual it using the assembly tool. In the event that this fails, you additionally have the option of blocking the thumbturn sleeve using a slim metal pin via a small hole on the front of the electronics module and be able to consequently remove the thumbturn using the assembly tool.

The thumbturn is not intended as an object to move the door panel (as would be the knob, handle, etc.). Do not carry or lift the door panel using the thumbturn.

Do not stand on the thumbturn.

Do not cover the reader equipment of the lock cylinder with metal materials.

Regularly check the correct condition and function of the lock cylinder (at minimum once a month) as part of a functional check using authorised identification media.

We recommend you keep the locking system up-to-date
by regularly installing software and firmware updates. Make sure to run firmware updates when the door is open and run a functional test after having completed the update.

Depending on the cylinder's protrusion beyond the escutcheon or any installed cylinder rosettes, the Xesar thumbturn may be hard to operate as a result of friction caused by the seal on the escutcheon or rosette of the cylinder. There is the option to remove said seals when installing indoors.

Xesar cylinders with European profiles are equipped with a service bore at the front of the electronics module. Use it to secure the thumbturn axis with a matching metal pin and facilitate disassembly of the cylinder thumbturn.
The metal pin must have a minimum diameter of 2 mm and be at minimum 40 mm long.

Procedure:

Step 1:

Insert a matching metal pin (e.g. a
2 mm Allen key) into the front service duct of your European profile cylinder.

Step 2:

In this process, turn the thumbturn until you are able to insert the metal pin considerably deeper into the service duct. Now hold the metal pin in this position and disassemble the thumbturn as usual using the assembly tool.

Step 3:

Once again carefully remove the metal pin after having removed the thumbturn.

Cleaning information

Regularly lubricate lock cylinders – at minimum as part of battery replacements. For this purpose, use the lubricants recommended by EVVA only. Please refer to the Xesar system manual for more information on the exact lubrication processes.

Use a soft, lint-free cloth and soapy water to clean any visible areas of the lock cylinder. Do not use corrosive products or sprays that may be aggressive on metal surfaces, plastics or sealants and seals. Ensure (particularly when the thumbturn has been removed) no liquids penetrate the cylin-

der and that visible areas of the electronic thumbturn must exclusively be cleaned when the thumbturn is not open.

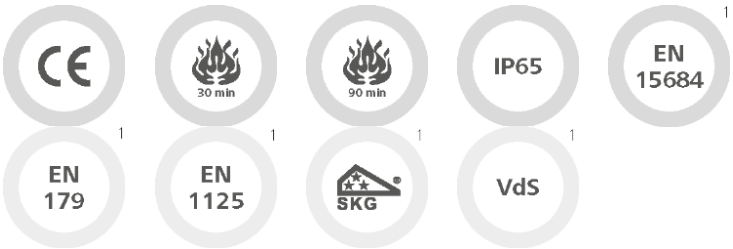
Note the information in the assembly manual regarding the correct position of the cylinder.

Reset cylinders to construction mode before moving Xesar cylinders (removing them from the door).

Conditions of use

Ambient temperature -20 °C to +55 °C (depending on the battery) | Humidity < 90 %, non-condensing | For 100,000 cycles as per EN 15684[1] | IP65 protection

Standards and guidelines



CE tested | EN 1634: 30 minutes | EN 1634: 90 minutes[1] | IP65 rating | EN 15684[1] | suitable for locks as per EN 179/1125 (when using the FAP anti-panic function)[1] | SKG[1] | VdS[1]

Xesar cylinders feature an event memory for the last 1,000 events.

Assemble the component as per the assembly manual enclosed with the product.

Battery replacements

Activate office mode for the cylinder before replacing batteries so the cylinder remains engaged.

---

[1] In preparation

Note that lock cylinder operation is permitted using type CR2 batteries only. Do not use rechargeable batteries. Please ask your specialist retailer for a list of recommended battery models.

We recommend to have batteries replaced by trained, specialist personnel only.
Replace batteries in due time, as soon as the lock cylinder indicates "Battery low". Repeatedly disregarding the "Battery low" warning may cause cylinder malfunctions. At normal ambient temperatures, the first "Battery low" warning indicates that up to 1,000 actuations are still possible within the next 4 weeks. Temperatures deviating from normal ambient temperatures may cause the cylinder to prematurely fail. If the batteries are empty, it is exclusively possible to operate the cylinder using the emergency power device (optional accessory).

Always replace all batteries used in the corresponding lock cylinder! Use the dedicated Xesar lock cylinder assembly tool to assemble or disassemble the thumbturn (also when replacing batteries). We recommend to pair up the lock cylinder using an authorised Xesar identification medium before removing the batteries. If applicable, you may be required to synchronise the system time using the Xesar tablet after having replaced the batteries.

Store batteries in a cool, dry location. Exposure to direct, strong heat may damage batteries. For this reason, do not expose battery-operated devices to strong heat sources.

Batteries contain chemical substances and for this reason, dispose of them correctly, taking into account the country-specific regulations.

Battery replacement procedure
Please proceed as described in the assembly manual to replace batteries in your Xesar cylinder, only in reverse order.

1. Completely position the cylinder tool on the dedicated recess on the rear of the outside thumbturn and turn the thumbturn and the tool in anti-clockwise direction.
2. Now remove the cylinder tool and undo the three attachment screws on the rear of the outside thumbturn using a Phillips screwdriver (PH1). Subsequently remove the thumbturn disc.

3. Carefully open the lock in the outside thumbturn by initially moving it carefully before unfolding it.

4. Now remove both empty CR2 batteries and clean the battery contacts using a soft, lint-free cloth.

5. Now insert the two new and previously acquired batteries with the correct polarity into the battery compartment and close it once again.

6. Battery replacements must not take longer than one minute. Resynchronising using the Xesar tablet may be required once this period has expired.

7. Once you have correctly replaced the batteries, the component initialises and the corresponding acoustic signal sounds (signal 8 in the signal table in Section*: Fehler! Verweisquelle konnte nicht gefunden werden.*)

8. Now once again position the thumbturn disc and fasten it using the three screws.

9. Completely position the cylinder tool on the rear of the outside thumbturn and fasten both components to the cylinder together (in clockwise direction) until you can feel resistance. Subsequently turn the cylinder in the opposite direction (anti-clockwise) until you hear a click.

10. You can now once again remove the cylinder tool.

Option

7.3.2 Cylinder tool

Figure 21: Cylinder tool (sample image)

Xesar cylinders provide a special opening mechanism to protect from manipulation and the dedicated special tool is required for assembly and disassembly as well as battery replacements.

Order the cylinder tool separately. It is not enclosed with Xesar cylinders.

The cylinder tool device is optionally available.
Product code: **E.ZU.PZ.ZW.V1**

Please note the instructions in the Xesar cylinder assembly manual
or watch the video instructions: http://video.evva.com/tutorials/xesar/expzkzs/expzkz-s-1/en/

7.4 Xesar wall reader

Figure 22: Xesar wall reader (sample image)

Xesar wall readers are suitable for indoors and outdoors, surface-mounted or flush installation and for areas critical to security.

Please use the dedicated seal enclosed with the product in the event of use outdoors or in areas that are exposed to water as well as in the event of surface-mounted installation and observe the information in the assembly manual. Xesar wall readers are connected to the Xesar control unit and supplied with power using a connecting cable.

Please note Xesar wall readers can only be used in connection with Xesar control units.

Connect the Xesar wall reader to Xesar control units to operate electronic components, such as motorised cylinders, swing doors, sliding doors, etc.

Please check carefully to make sure the Xesar product you selected is suitable for your application.

We have made the required data sheet available in the download section of our homepage: HYPERLINK "http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/" http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

7.4.1 Xesar wall reader — functional description

Figure 23: Xesar wall reader (sample image)

Visual and acoustic feedback

Xesar wall readers indicate events visually and acoustically. For this purpose, there is an LED at the top edge of the Xesar wall reader. For a list of all available signals please refer to Section: How Xesar access component indicate even).

Reader unit, ON/OFF status light

The reader unit sensor is located behind the glass panel of the Xesar wall reader, between the EVVA logo and the LED. The status light of the Xesar wall reader lights up continuously during on-going operation to facilitate localising the reader unit in dark environments.

Connector (synchronisation, updates)

Xesar wall readers feature a connector located under the connector cover (EVVA logo). Slightly press towards the inside on the left-hand side of the EVVA logo (near the "E") and fold out on the right-hand side (near the "A") to access the connector.

The connector is intended solely to synchronise the unit with the Xesar tablet, Xesar wall readers **cannot** be operated with the optionally available emergency power device.

After use, once again carefully close the connector cover (EVVA logo) to protect the connector from penetrating dust and humidity. For this purpose, do not use pointed objects to prevent damage.

Functional principle

Hold a Xesar identification medium to a reader unit and the Xesar control unit (connected to the Xesar wall reader) checks the Xesar identification medium. The correspondingly triggered relay of the Xesar control unit switches insofar as the identification medium is authorised, depending on the jumper position (see diagram in the Xesar control unit -> **JP2**) and the configuration.

Xesar control units feature an event memory for the last 1,000 events. Once the event memory is full, the system overwrites the oldest entries with the most recent events. For this reason, it is important to regularly synchronise events to prevent event records from being lost.

7.4.2 Xesar wall reader connection label

Use the connection label to connect Xesar wall readers to the connecting cables of the Xesar control unit. Please note the data and information in the assembly manual enclosed with your Xesar product; in particular the jumper position of the **JP1** jumper to prevent malfunctions.

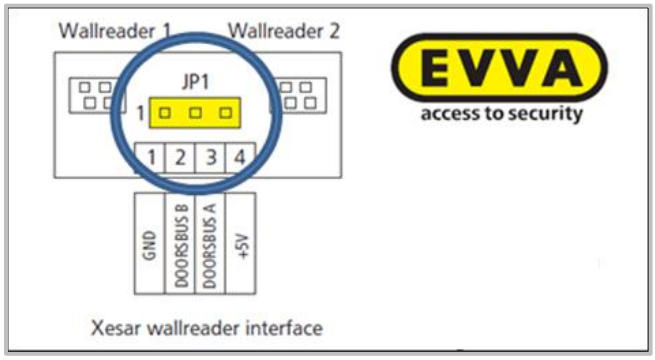


Figure 24: Xesar wall reader connection print (sample image)

We have provided the assembly manual and the data sheet of the corresponding Xesar product on our homepage:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

7.5 Xesar control unit

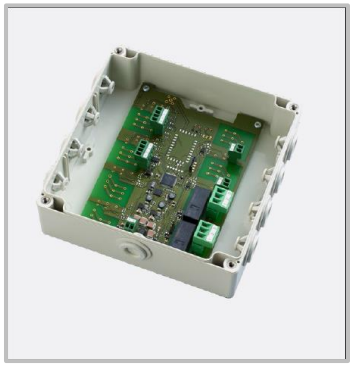


Figure 25: Xesar control unit (sample image)

The Xesar control unit can be exclusively used in conjunction with Xesar wall readers. Connect up to two Xesar wall readers to one Xesar control unit. Xesar control units connected to Xesar wall readers must be installed indoors in areas protected from manipulation.

Xesar control units are supplied with power using the power supply unit and in the event of power cuts they are equipped with data buffers for a maximum of 72 hours, providing the Xesar control unit had been previously active for a minimum of six hours.

Please refer to the product catalogue in the download section of our homepage for more detailed information:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/system-overview/en/

7.5.1 Xesar control unit connection configurations

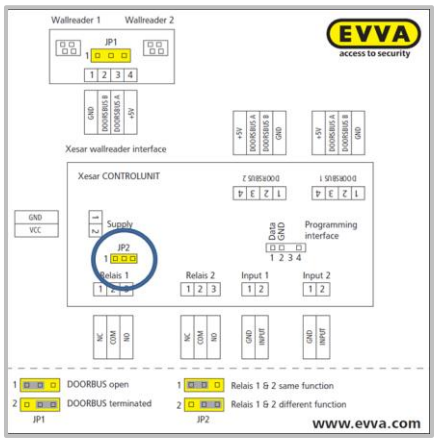


Figure 26: Diagram (sample image)

You have the following connection configurations available. Pre-set connections with the position of the **JP2** jumper (Figure 26: Diagram (sample image)).
Please note the data and information in the assembly manual enclosed with your Xesar product.
We have also made the required data and information available in the download section of our homepage: http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

7.5.2 One Xesar wall reader -> one Xesar control unit

One or both relays can be switched at the same time depending on the jumper position (**JP2**) ❷. As a result, you can use both relays for different applications (e.g. relay 1 switches with and relay 2 without an external power source).

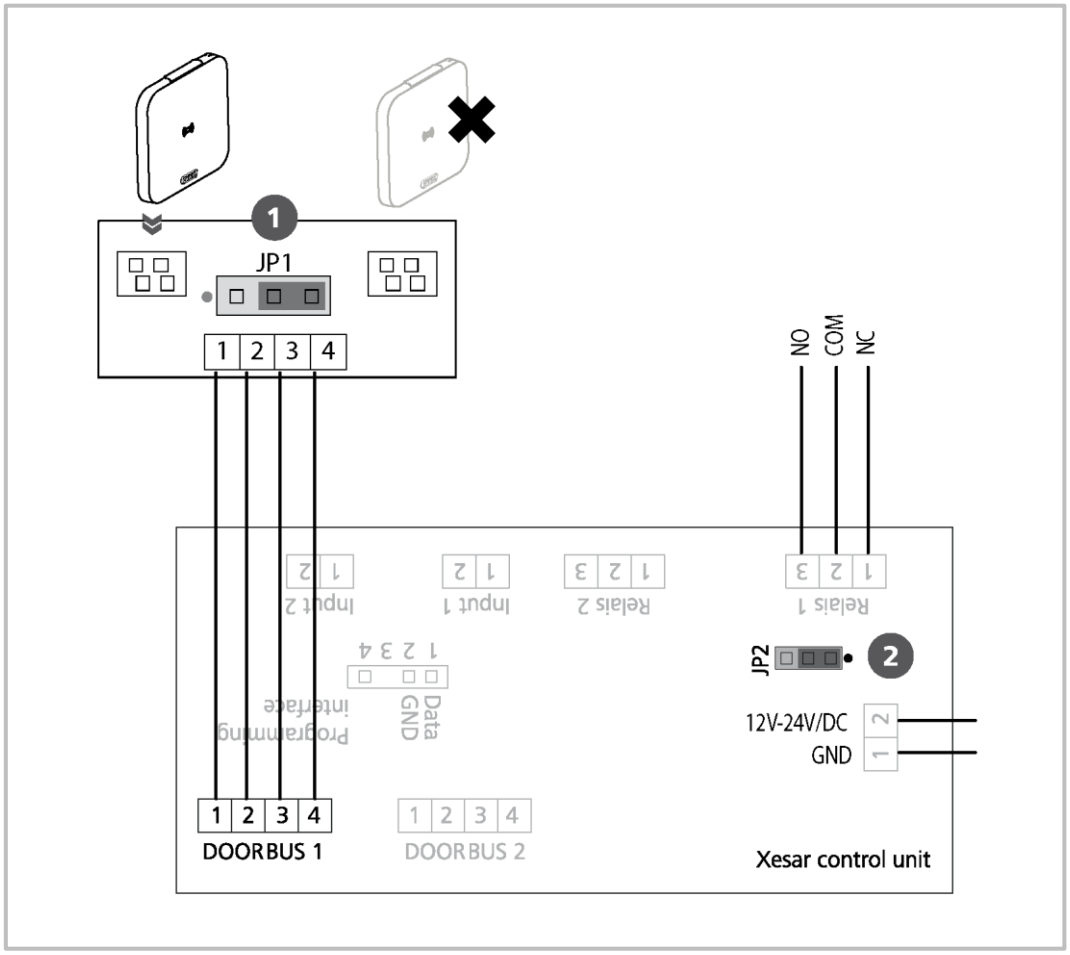


Figure 27: One Xesar wall reader (sample image)

7.5.3 **Two Xesar wall readers -> one Xesar control unit** (double-sided access)

Depending on the jumper position (**JP2**) ❷ both relays can be switched by both Xesar wall readers, for instance to implement access from both sides.

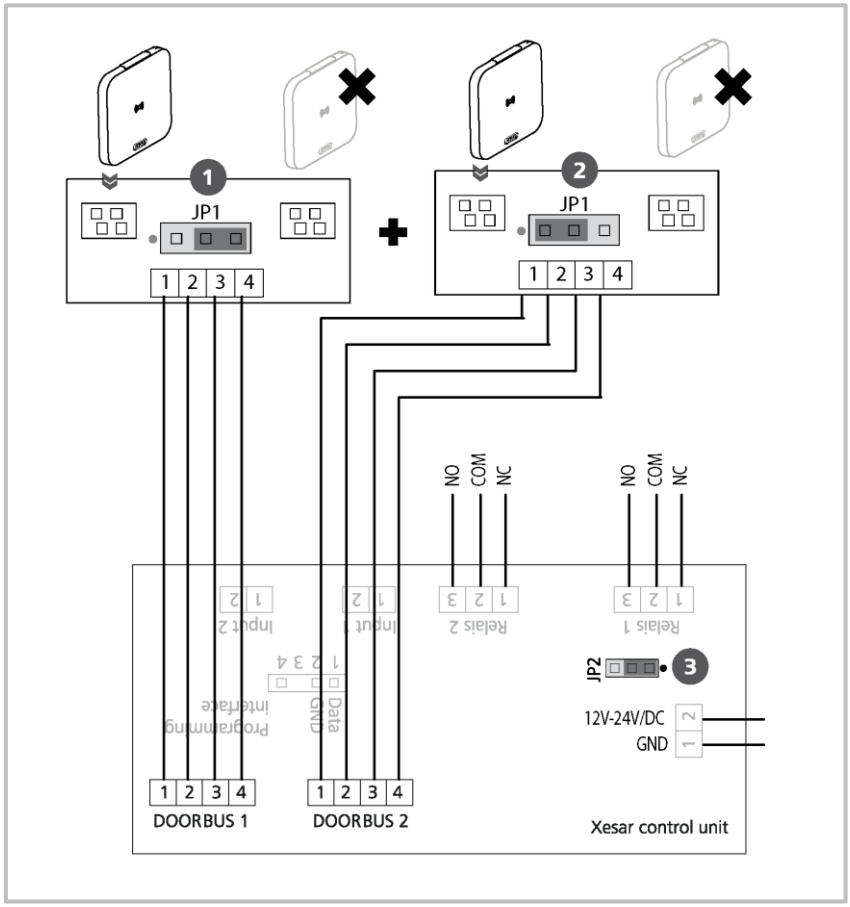


Figure 28: Two Xesar wall readers (sample image)

7.5.4 Two Xesar wall readers -> one Xesar control unit

Both relays can be switched differently depending on the jumper position (**JP2**) ❷. As a result, one Xesar control unit and two wall readers can operate two different doors.

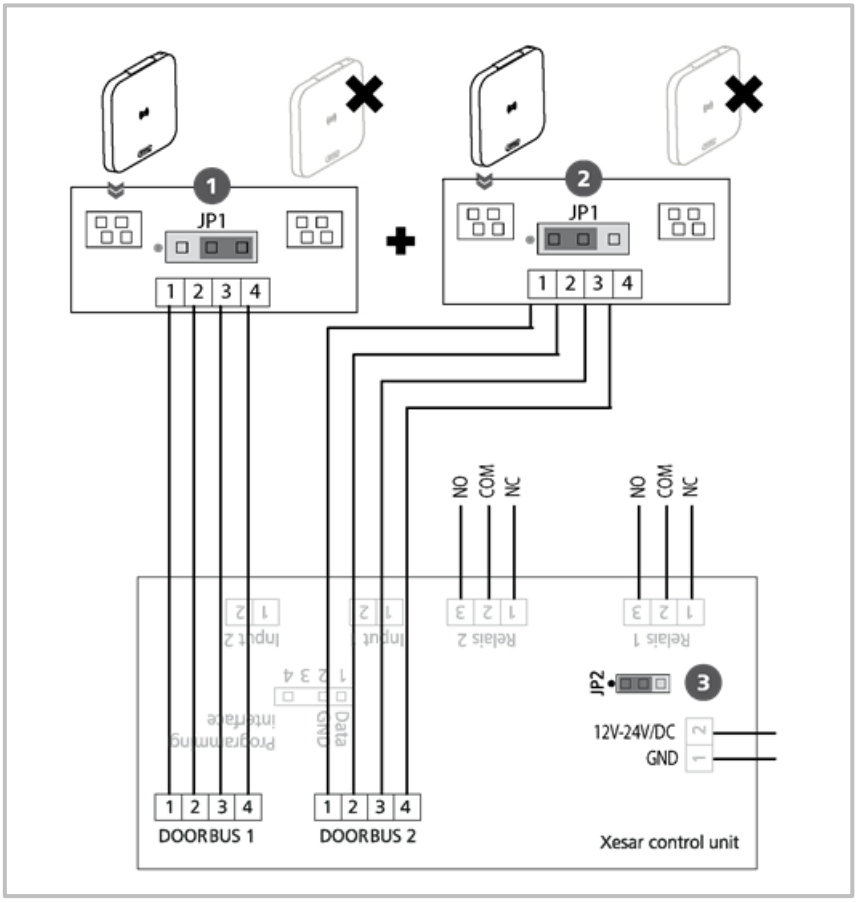


Figure 29: 2 Xesar wall reader (sample image)

EVVA recommends using a CAT5 cable to connect Xesar wall readers with Xesar control units.

Do not exceed the maximum cable length of 20 metres to safeguard correct functionality.

Maintain a minimum distance of 100 mm between Xesar wall readers to safeguard correct functionality

Please check carefully to make sure the Xesar product you selected is suitable for your application.

Please note the office mode function (Section: ***Xesar*** identification media) and the different acoustic and visual signals (Section: *How Xesar access component indicate even).*

We have made the required data sheet available on our homepage:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

Note the following, important notices regarding the use of Xesar wall readers.

Climatic and environmental effects
Note the defined suitability of the wall reader for the respective ambient conditions as per its IP rating and specific temperature range.
Use the wall reader in environments with a humidity below 90% only.
Clarify the application options with a specialist retailer before installing wall readers in environments with a particularly high level of static charges.
Do not use wall readers in corrosive atmospheres (e.g. chlorine, ammonia, lime water or salt water).

Information regarding installation and the correct installation situation
Exclusively specialist personnel must install wall readers and control units according to the specifications in the assembly manual which is also enclosed with the product. We particularly point out to exclusively install the control unit when it is de-energised. EVVA shall assume no liability for any kind for damage resulting from improper assembly/installation.
We recommend installing control units in tamper-proof areas.
Note that control unit operation requires a mains adapter. Said mains adapter is not within the control unit's scope of delivery and optionally available as an accessory.

In the event that you are using a mains adapter you have not procured from EVVA, you must make sure the power supply requirements illustrated in the product catalogue are complied with.
Wall readers and control units are exclusively intended to actuate electronic locking components and technical equipment. The control unit is actuated using the relay outputs. The maximum permitted switching performance of the relay outputs as per the product catalogue must be complied with.

All Xesar access components are delivered ex works in so-called construction mode. In this condition any Construction Card unlocks any Xesar access component. For this reason, immediately after having installed each Xesar access component ensure it is correctly added to the locking system so that exclusively authorised persons have access.
Exclusively use accessories and spare parts recommended by EVVA.
Observe the corresponding international and national specifications in the corresponding legislation, directives, standards and guidelines, particularly regarding the requirements for escape routes and emergency exits, during project management and installation of the control unit.
Before completing the installation, use a Construction Card to verify the correct function of the wall reader and control unit when the door is open.
After having installed the wall reader and control unit, note that you can only operate the system using a Construction Card until parameters have been completely configured.

Information on operation

Please note that the wall reader function can be safeguarded exclusively in conjunction with the matching control unit. Wall readers and control units are exclusively intended to actuate electronic locking components and technical equipment. EVVA shall assume no liability or accept warranty claims for the correct function of the actuated devices themselves.
Instruct users of the electronic locking system to always keep identification media safe.
In the event that Xesar identification media is lost, it must be immediately blocked using the software. The Xesar wall readers must be immediately updated using the Xesar tablet.
Please note that wall readers must be removed using the dedicated special tools only. Damage caused by other tools shall render any liability, warranty or potentially separate guarantee claims void.
Do not cover the reader equipment of the wall reader with metal materials.
Regularly check the correct condition and function of the wall reader and control unit (at minimum once a month) as part of a functional check using authorised identification media.
We recommend you keep the locking system up-to-date by regularly installing software and firmware updates. Make sure to run firmware updates when the door is open and run a functional test after having completed the update.

Cleaning information

Use a soft, lint-free cloth and soapy water to clean any visible areas of the wall reader. Do not use corrosive products or sprays that may be aggressive on glass surfaces, plastics or sealants and seals.

Note the following, important notices regarding the use of Xesar control units.

Important notice

You must comply with the following warnings and information from EVVA Sicherheitstechnologie GmbH (hereinafter referred to as "EVVA") if you install, programme and use the control unit. Keep the instructions in the vicinity of the control unit.

Carefully read the Xesar system manual before commissioning your Xesar locking system. It is available at www.evva.com.

General legal notes

EVVA concludes the contract on the use of Xesar exclusively on the basis of its General Terms of Business (EVVA-GTB) as well as its General Licensing Conditions (EVVA-ALB) with regard for the software for the product. Please refer to: http://www.evva.at/terms-and-conditions/en.

We explicitly notify clients that the use of the locking system subject to this contract may trigger legal approval, reporting or registration obligations, in particular with regard to data protection (e.g. if you are establishing a comprehensive information system), as well as grant the right of co-determination to staff in the event of use on corporate premises. Customers, clients and end users shall be responsible for product use in compliance with legal stipulations.

The aforementioned information must be observed and passed on to operators and users as per the defined manufacturer product liability according to product liability legislation. Non-compliance releases EVVA from any liability.

Any use deemed as non-compliant with the contract or as unintended use, any repair work or modifications that have not been explicitly approved by EVVA as well as all types of incorrect servicing may cause malfunctions and are prohibited. Any modifications that have not been explicitly approved by EVVA render claims to liability, warranty as well as any separate guarantee claims void.

Architects and advisory institutions are obliged to request all necessary product information from EVVA and take into account all such information to comply with obligations regarding information and instructions under the Product Liability Act. Specialist retailers and installers must comply with the information in EVVA documentation and they must pass on such information to customers, if applicable.

Please refer to the Xesar product catalogue and the Xesar system manual for additional information beyond these vital instructions. These are available at www.evva.com.

Standards and guidelines

Xesar wall reader	CE	IP65
Control unit	CE	IP54
Networkadapter	CE	

EVVA recommends to operate the Xesar wall reader control unit using an independent power supply and provide an uninterrupted 12 V power supply. This consequently prevents system failure and safeguards access.

As soon as the control unit has been connected to the power supply for six hours the system ensures the time settings are maintained for a minimum period of 72 hours in the event of a power cut.

Assemble the component as per the assembly manual enclosed with the product.

Option

7.5.5 Mains adapter for control unit

Figure 30: Mains adapter (sample image)

The control unit mains adapter is optionally available.

Product code: **E.ZU.WL.NT.V1**

Please refer to the product catalogue in the general download section of our homepage for more detailed information: http://www.evva.at/products/electronic-locking-systems-access-control/xesar/system-overview/en/

7.6 How Xesar access component indicate even

Signal number	Event	Visual signal	Acoustic signals:	Note
Signal 1	Unlocking attempt with authorised medium	●●●●●	mmmmm	
Signal 2	End of release	●●●●●	ttttt	
Signal 3	Rejected medium	●●-●●-●●-●●	hh-hh-hh-hh	
Signal 4	Unlocking attempt with authorised medium and activated office mode	●●●●--●●●●	tttt—hhhh	
Signal 5	Start of office mode	●●●●--●●●●	tttt—hhhh	
Signal 6	End of office mode	●●●●--●●●●	hhhh—tttt	
Signal 7	Unlocking attempt with authorised medium, battery low signal	●●--●●--●●--●●	h----h----h----h----	
Signal 8	Battery inserted or component reboot	●●--●●--●●	tt—mm—hh	After having inserted batteries, battery charge status display possible
Signal 9	Medium without EVVA segmentation; medium faulty, other system			No signals

Visual LED signals: ● = Red and green simultaneously

Acoustic signals h = high-pitched sound, m = medium-pitched sound, t = low-pitched sound

Each signal corresponds to a duration of 50 ms.

Pauses are indicated by "–".

8 Installing Xesar access components

Please note that specialist personnel must install Xesar access components as per the notes and information as well as the assembly manual enclosed with the product.

8.1 Installation support

EVVA provides a host of different installation support to make installing your Xesar system easier. Visit our website.

Language-neutral assembly manual

EVVA provides language-neutral assembly manuals on the packaging of the corresponding product or our homepage to support Xesar access component assembly.
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

Product-specific assembly video clips

We have provided assembly video clips with demonstrations of complex assembly steps here:
http://video.evva.com/tutorials/xesar/expzkzs/expzkz-s-1/en/

Language-neutral drilling template

EVVA provides a language-neutral, single-use, cardboard drilling template to support the assembly of versions requiring one or several drilled holes. They are printed on the corresponding product packaging and are available in our homepage in the general download section:
http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

The assembly manuals and the packaging feature QR codes which will take you directly to the corresponding video sequence or assembly manual.

You must observe the sequence of listed installation steps as otherwise malfunctions may occur.

Option

8.2 Drilling template

Figure 31: Drilling template (sample image)

EVVA provides a high-quality, metal drilling template to facilitate preparing the door for an assembly of any type of Xesar escutcheons and Xesar handles.

An adjustable stop safeguards the holes are correctly aligned and it enables to adapt the settings to match the requirements of any door situation. Hardened metal drilling sleeves guarantee a long service life even after intense use.

The drilling template is optionally available.
Product code: **E.ZU.BE.BS.V1**

9 Installing the Xesar software

Proceed as follows to install your Xesar software:

Step 1:

Register to download the most recent version of the Xesar software at: http://www.evva.at/products/electronic-locking-systems-access-control/xesar/demand-xesar-software/en//.

You require appropriate administrator rights on your computer to install the software.

Step 2:

Proceed as follows after having downloaded your Xesar installer file (.exe):
Double-click the application.
Select your language and click ***OK*** (Figure 32) to continue.

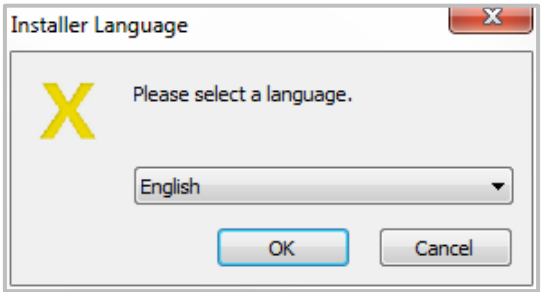


Figure 32: Language selection

Now the installation wizard opens (Figure 33: Welcome). Follow the on-screen instructions and then click ***Next.***

Please note that existing Xesar installations (V1.1, V2.0, V2.1) are not updated and the software is reinstalled instead. However, you have the option to import the database of existing Xesar installations (V1.1, V2.0, V2.1) after having installed the Xesar 2.2 software.
Please note that in this case you must exclusively use the current Xesar 2.2 system. It is not possible to reimport earlier Xesar installations.

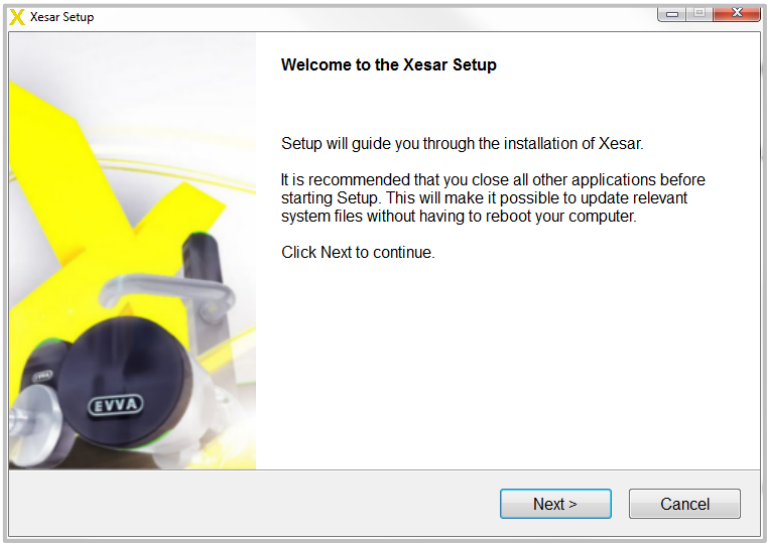


Figure 33: Welcome

Accept the terms and conditions to be able to install the software ❶ (Figure 34: Xesar installation — licence agreement). Then click ***Continue***.

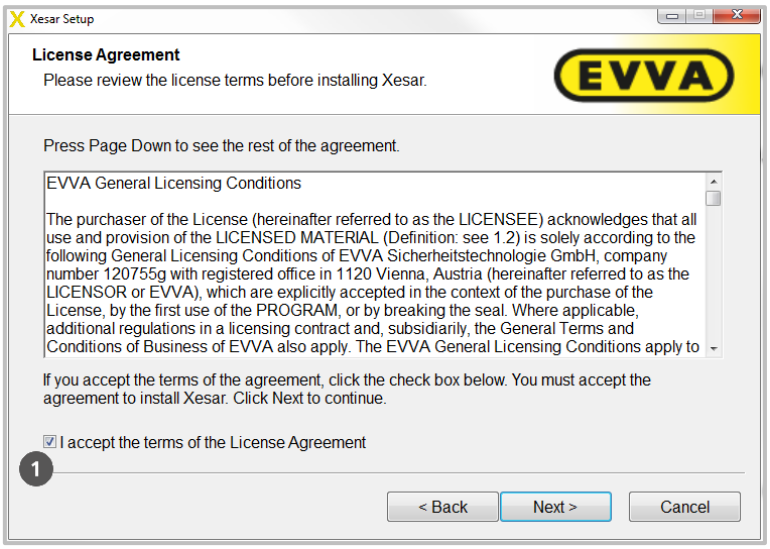


Figure 34: Xesar installation — licence agreement

By default the Xesar software is installed in a directory on the system drive ❶ (Figure 35: Xesar installation — selecting the designated directory). Click Browse ❷ (Figure 35: Xesar installation — selecting the designated directory) and select a different directory if you would like to install the Xesar software in a different directory. Then click ***Continue.***

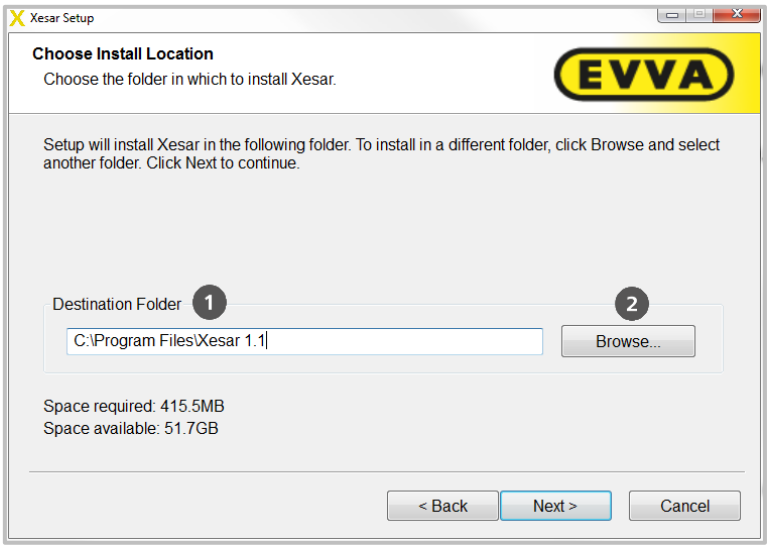


Figure 35: Xesar installation — selecting the designated directory

Please note that during installation with no administrative rights - no backup can created, because access privileges to the installation file path (drive C) are missing.

Keep the installation path short and without special characters. An invalid path is signaled via an error message.

The system automatically creates the folder for program shortcuts. If you would like to create a different folder, enter its name and then click ***Install***. (Figure 36: Xesar installation — specifying the folder)

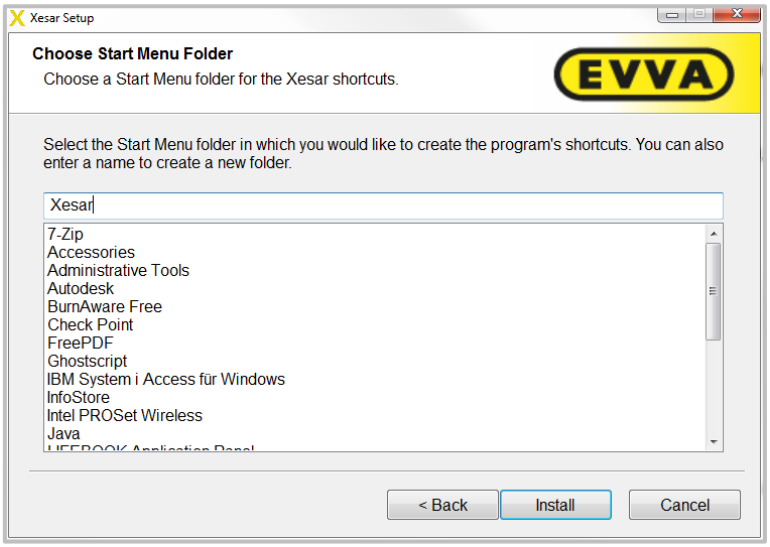


Figure 36: Xesar installation — specifying the folder

Now the system installs the Xesar software, the progress bar indicates the current activity ❶ (Figure 37: Xesar installation).

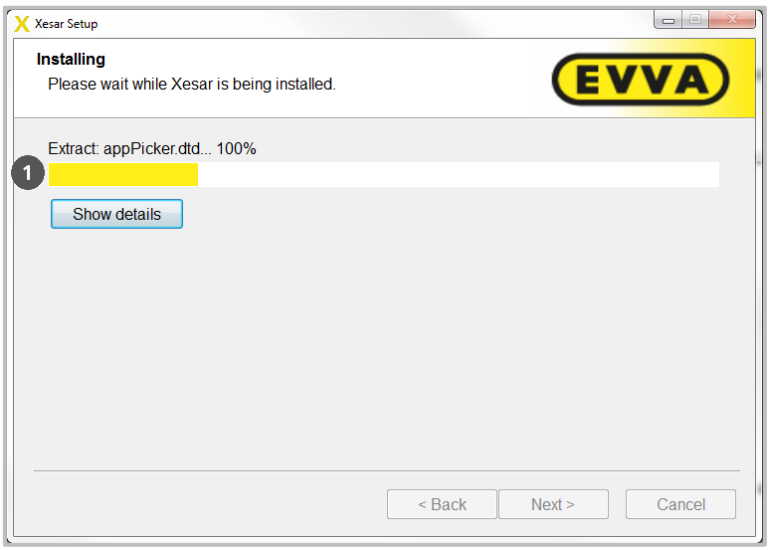


Figure 37: Xesar installation

Note:
If you are reinstalling your Xesar software, but have failed to uninstall the applica-

tion, you will be unable to install the software

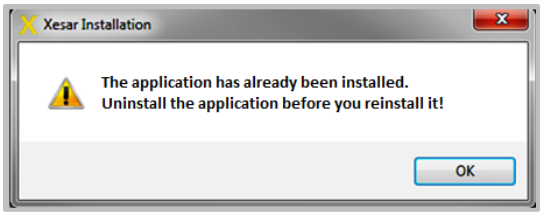


Figure 38: Error message/installation

Once the installation has completed, a message indicates the Xesar software has been successfully installed. Click ***Finish*** (Figure 39: Xesar installation) to complete the installation.

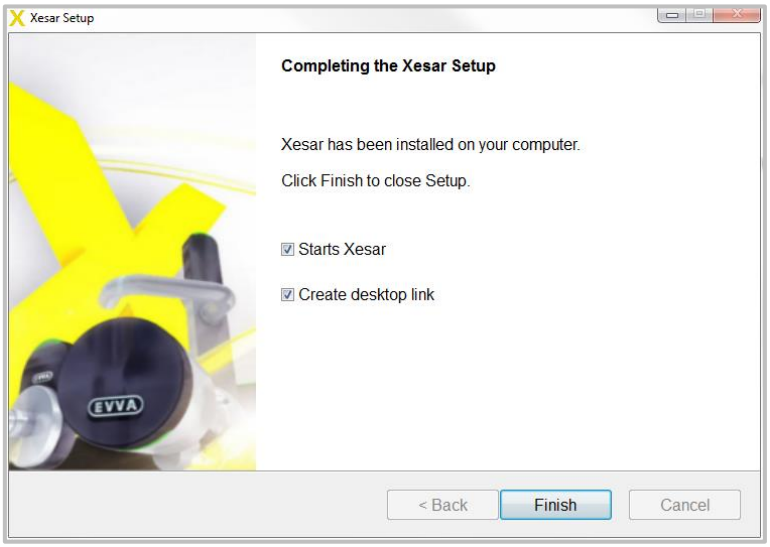
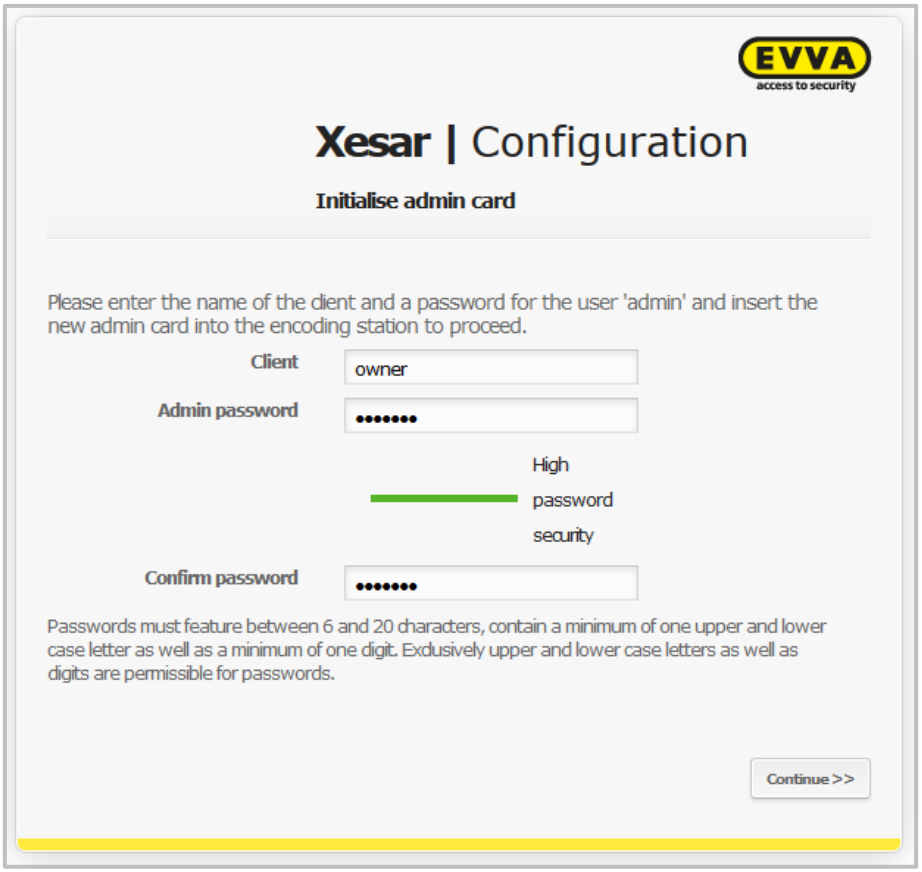


Figure 39: Xesar installation

10 Configuring Xesar software for the first time

Your Admin Card is automatically checked upon starting your Xesar software.
The following error message appears if you have inserted a faulty or invalid Admin Card or if no Admin Card has been inserted into your Xesar coding station: „**Insert a new Admin Card** ".

Enter the system name and the administrator password in **the Xesar | Configuration window** (FiguFehler! Textmarke nicht definiert.39: Initialising the Admin Cardrd) after having inserted a valid Admin Card. Then click: ***Next.***



Fehler! Textmarke nicht definiert.39: Initialising the Admin Card

Passwords must feature between six and twenty characters, contain a minimum of one upper and lower case letter as well as a minimum of one digit. Exclusively upper and lower case letters as well as digits are permitted for passwords.

Now select a path for the automatic database backup (Figure 40: Network path:). For reasons of security we recommend creating the DB backup on an external hard drive as a system hard drive failure would put your database and the backup at risk.

Then click ***Next.***

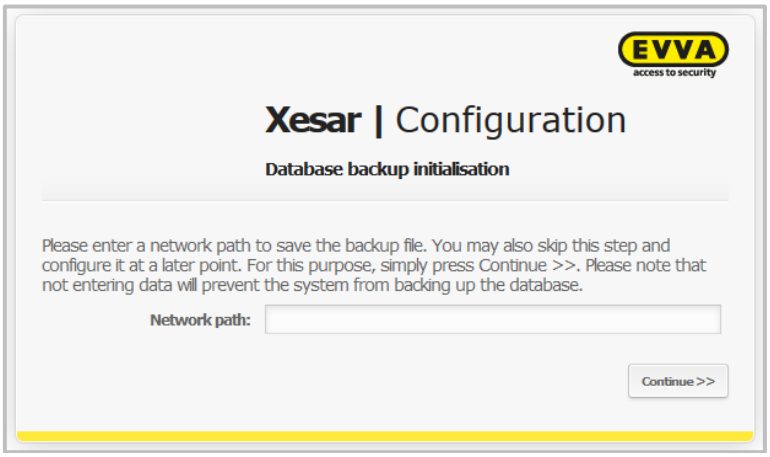


Figure 40: Network path:

Configure your system so backup files are regularly saved according to their version (Windows Preferences) to be able to recover data from a certain version in the event of a database failure.

The system now shows the name of the system you selected
(Figure 41: Access data).
Log in by clicking ***Next***.

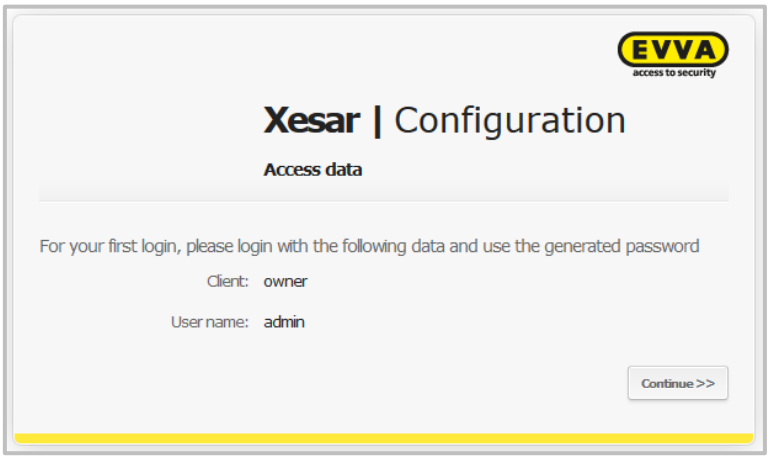


Figure 41: Access data

10.1 Backing up access data and DB key

You can exclusively view your access data ONCE and only AT THIS POINT!
A confirmation prompt asking whether you have printed and archived your system information appears to prevent you from accidentally skipping this window.

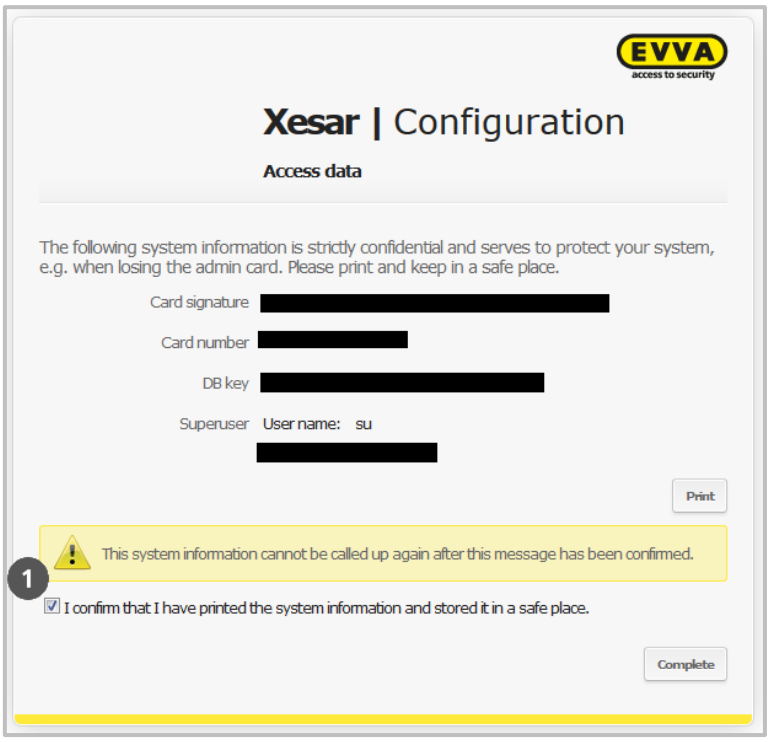


Figure 42: Configuration

Confirm the security prompt in the Xesar | Configuration ❶ application window (Figure 42: Configuration) and click ***Complete.***

After having confirmed the Xesar | Configuration with ***Complete*** you have completed the initial software configuration.

10.2 Roles

EVVA has assigned certain functions to specific roles to make it easier for you to use your Xesar software. Please note this during commissioning and operation.

Role	Function
Admin	Owner and administrator of the locking system. (management and authorisation of critical settings)
Users	Users are responsible for administrative tasks within the program and each user is assigned individual authorisations. Administrators centrally manage the system and they always have comprehensive authorisations.
Person	Persons using authorisation media. Persons are assigned access authorisations to door areas and doors.

Table 1: Software application roles

11 Xesar software

11.1 Starting the program

A program window appears after having started your Xesar software (Figure 43: Opening the program). The system automatically loads various software modules in the background while you see this screen. Once the program window has completed loading, you are automatically forwarded to the login page.

Figure 43: Opening the program

11.2 Logging in using Admin Cards

Proceed as follows if you own a valid Admin Card:
Connect the Xesar coding station and insert the Admin Card into the Xesar coding station card slot. (Figure 44: Login)

Enter the information required in the "Xesar | Login" (Figure 44: Login) login window:

- Select the software ***language*** if you would like to use a language different to the default language.
- Enter the selected client name in the ***Client*** field upon first-time configuration.
- Enter "admin" as the ***user name***.
- Enter the ***Administrator password*** you selected when you first registered and click ***Log in***.

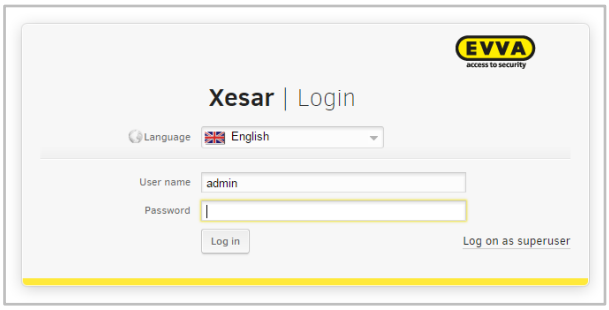


Figure 44: Login

The user name and password are case sensitive.
The system loads the database in the background ❶

Figure 45: Xesar | Login

11.3 Logging in using the DB key

If you have not connected your Xesar coding station, your Admin Card is faulty or not available, the system shows the "Xesar | Configuration" (Figure 46: DB key) application window allowing you to enter the DB key to continue. Note that you will be unable to grant authorisations to persons/identification media without an Admin Card.

The DB key ❶(Figure 46: DB key) is the automatically generated code included with your access data (see ***Backing up access data*** and DB key).

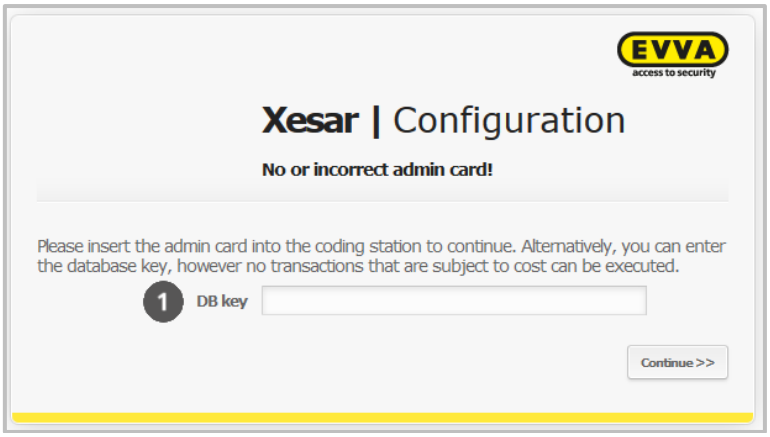


Figure 46: DB key

11.4 Several Xesar systems per installation

If you manage several Xesar systems, you can import the corresponding database – in conjunction with the correspondingly valid admin card – and run several Xesar systems in one installation.
In this process, please also note the manual database backup function to keep it up to date. In this process, also regularly synchronise your system tablets.

- Initially save your database to change between systems.
- Then quit your Xesar software.
- Now insert the desired admin card and start the Xesar software.
- Now also import the associated system database upon starting the software.

12 Homepage

The re-designed dashboard gives administrators the possibility to assess the security status of their system at a glance to be able to potentially take required actions.

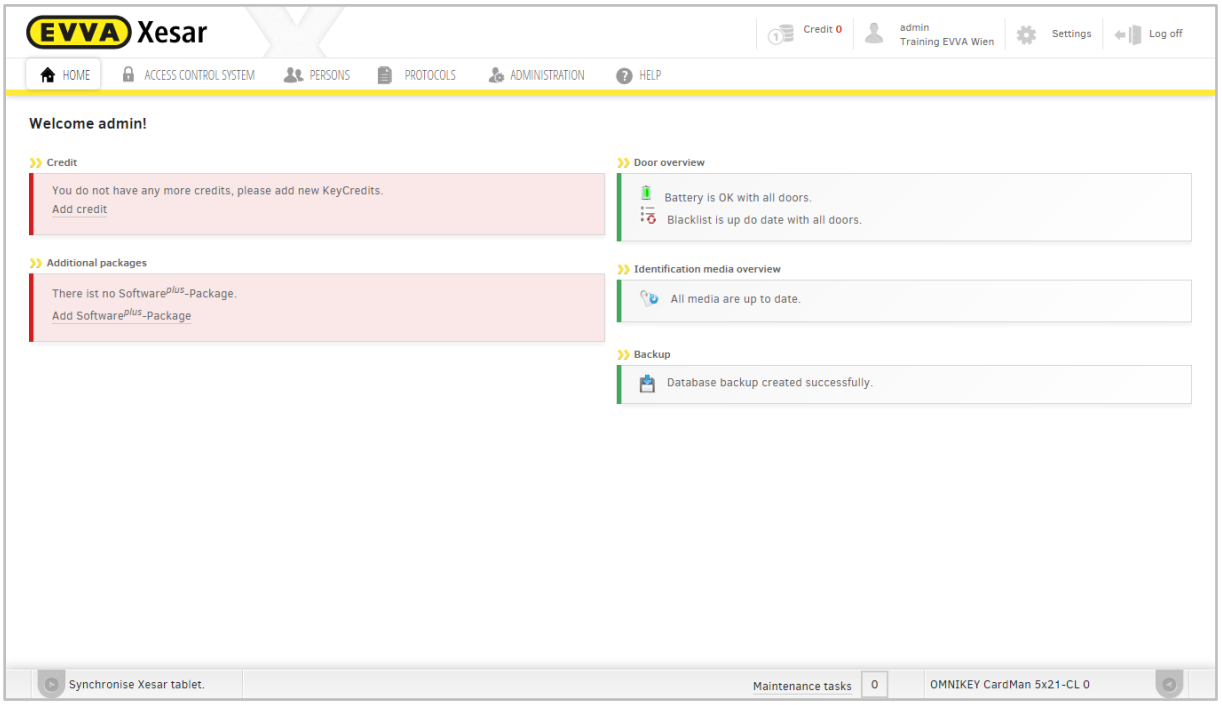


Figure 47: Home page

The following information is available on the dashboard:

- Shows opening attempts by lost/blocked identification media
- Shows valid identification media which have been blocked in the software (Fig. Xx)
- Shows doors with an out-of-date blacklist (Fig. Xx)
- Shows doors with a low battery
- Shows media with an out-of-date media status (memory extension for use with virtual networks) see link
- Shows out-of-date identification media
- Shows KeyCredits

Congratulations! You have finished installing your Xesar software!
Now you are on the Xesar software home page. The following prompt appears if you have not loaded any KeyCredits: "***You do not have any more credits, please add new KeyCredits."***

The system automatically logs off following ten minutes of inactivity for reasons of security. The "Xesar | Login"

Please note that you must click the corresponding confirmation button to accept any changes you make to your system. If you fail to do so, an error message indicating "***Unsaved changes on this page***" appears upon closing the corresponding menu.
Click ***OK*** to confirm this message and discard any changes. Click ***Cancel*** (in the error message) and confirm your changes before closing the menu to save your data.

13 Loading KeyCredits

KeyCredits enable you to create and change access authorisations. Please refer to Section

EVVA KeyCredits for a list of changes that are subject to a charge or changes that are free of charge as well as additional information about KeyCredits.

The ***Credit*** function ❶ in the header of the page shows the amount of available KeyCredits below. The information in the header is always available so you have a permanent overview of the current amount of KeyCredits. Click ***Credit*** to top up KeyCredits.

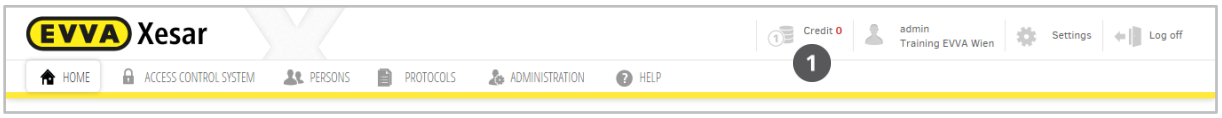


Figure 48: Credit

You require an operating Internet connection and the credit code on the back of the KeyCredit Card (concealed by a scratch field) to top up credit.

- Enter the code in the "Add credit" (Figure 49: Topping up credit) application window.
- Press the Tab key to move to the next input field.
- Click ***Add credit*** to confirm your input.
- If you entered the code correctly, the system confirms your input (green notification in the header) and adds the credit.

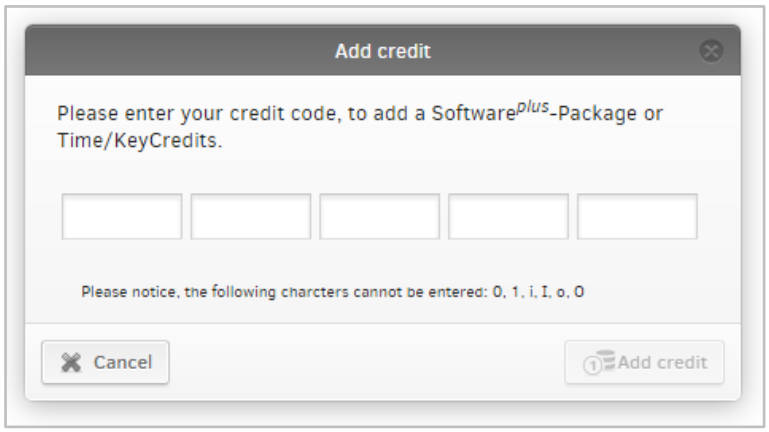


Figure 49: Topping up credit

The credit is linked to the Admin Card – any quantity credit will be rendered void in the event of a failure or loss of the Admin Card. Any time-based credit is saved centrally by EVVA and can therefore be transferred.
In this case, please directly contact EVVA Support.

Credits can be redeemed only once.

Any time-based credit is highlighted in red from 14 days before expiry.
A message appears on the home page if KeyCredit Unlimited is not active or there are no more KeyCredits available.

Invalid KeyCredit code

A message highlighted in red appears if you entered an incorrect code (Figure 50: Topping up credit — invalid input).

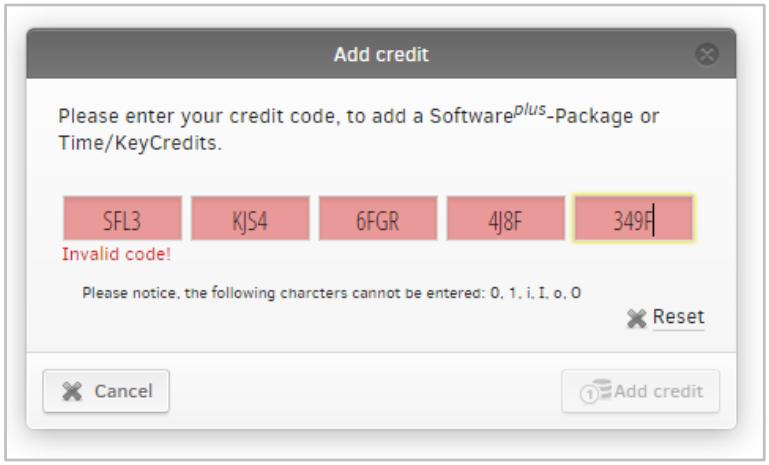


Figure 50: Topping up credit — invalid input

The Admin Card is automatically disabled after five incorrect attempts. Please contact our Online Support at http://support.evva.at/xesar/en/ if you encounter any issues.

14 Administrator

Click ***Admin*** ❶ in the tool bar to open the overview of the administrator who is currently logged in.

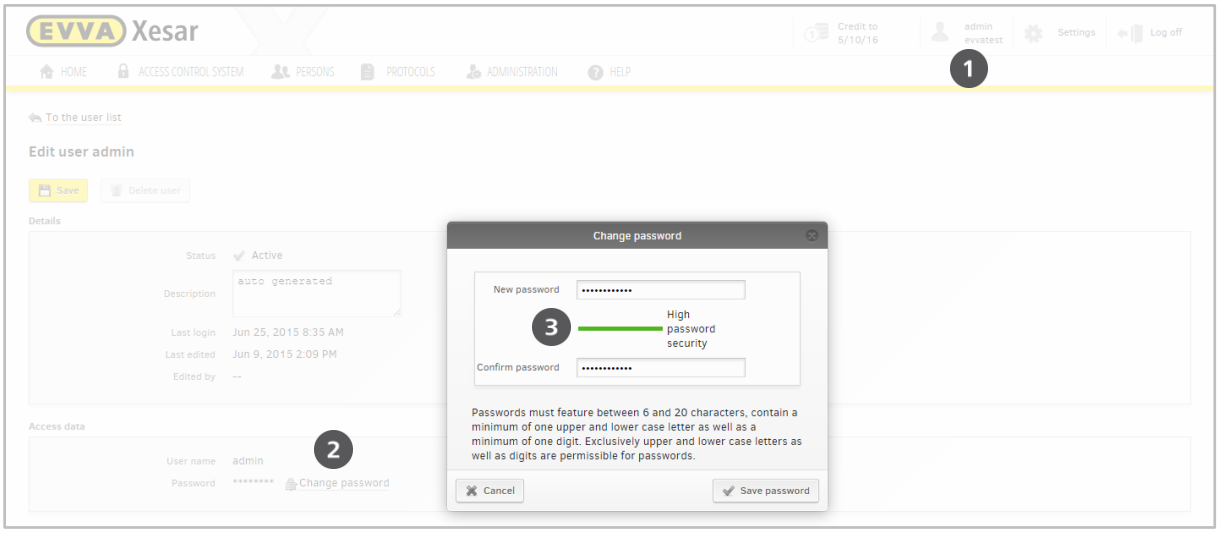


Figure 51: Changing the admin password

14.1 Changing the administrator password

1. The tool bar shows the current user name ❶.
2. Click the name – the user's application window opens. Proceed as follows to change the administrator's password who is currently logged in:
3. Click ***Change password*** ❷ – always use secure passwords ❸ consisting of upper case and lower case letters as well as digits and confirm your changes to accept them.

15 Settings

Click ***Settings***❶ (Figure 52: Settings) to open the corresponding menu.

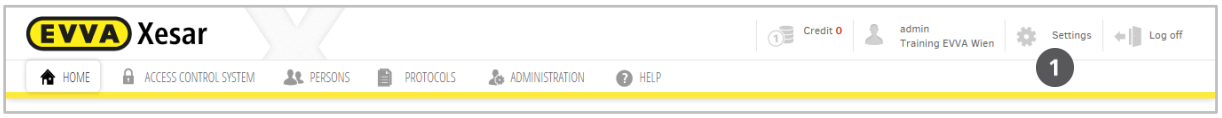


Figure 52: Settings

Your Xesar software enables you to configure various parameters, such as time settings, security settings and, if required, the host name as well as IP address of your proxy server. Proceed as follows to configure settings:

15.1 Time settings

15.1.1 Summer and winter time settings

Slide the ***Activate time change*** ❶ (Figure 53: Time settings) slider to ***On*** and enter the dates for summer and winter time in the corresponding year to activate the summer and winter time setting. It is important to manually update these settings once a year and make sure you subsequently also update your Xesar access components if you work with the summer and winter time function.

15.1.2 Setting special days

You can also specify five types of special days ❷ that are active at the same time over a period of fifty days in advance (Figure 53: Time settings).
For instance, use this function if you would like to grant a company's employees access from Monday to Friday, but not on public holidays. In such cases it is possible to define such "special days" and the access components will react accordingly. Affected persons will then no longer have access providing their time profile has been configured accordingly. The same principle also applies to automatic office modes where the system must remain locked on special days.

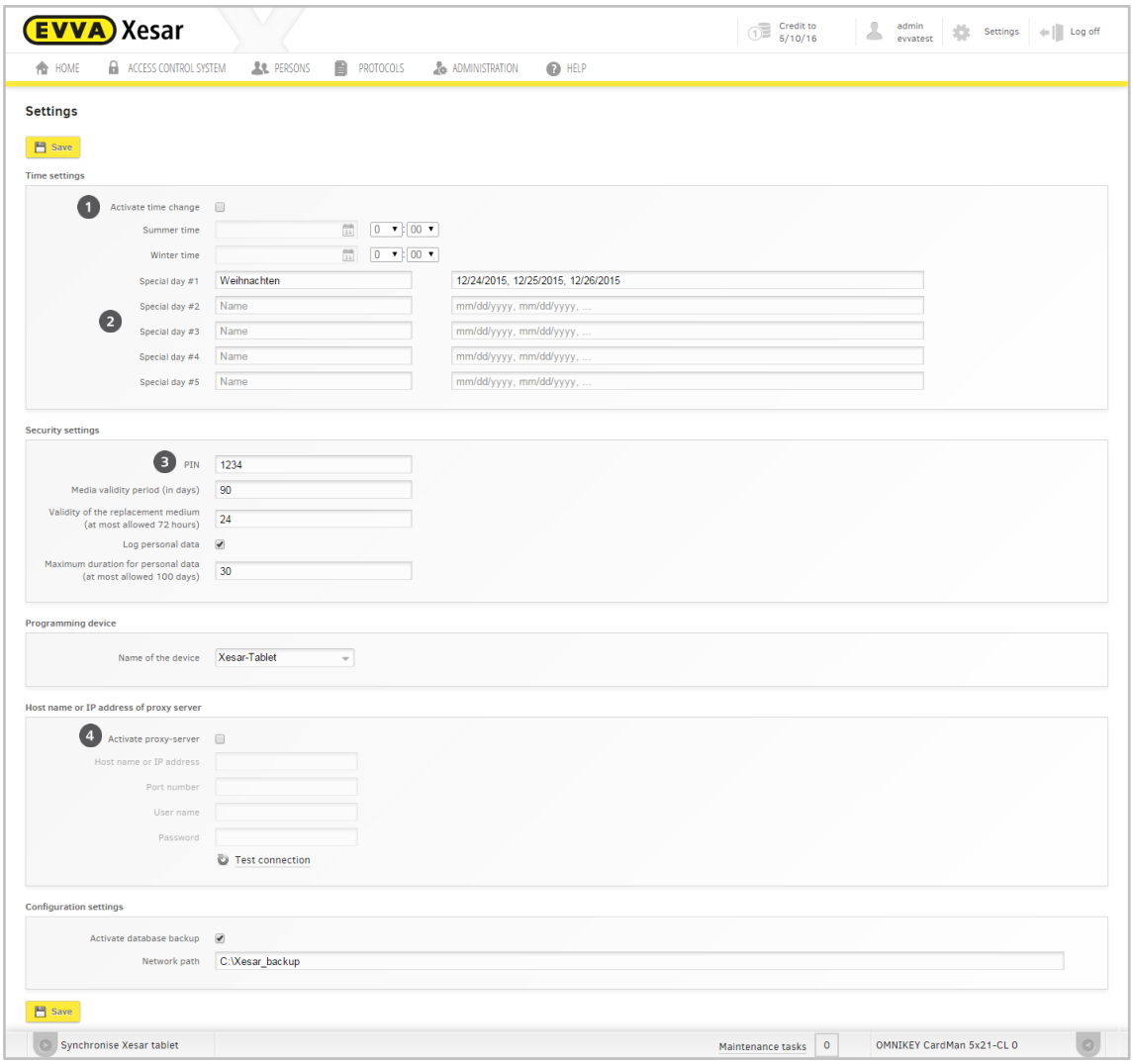


Figure 53: Time settings

15.2 Security settings

15.2.1 Security PIN

Enter a four-digit figure in the ***PIN*** ❸ field in the ***Security settings*** (Figure 53: Time settings). A PIN is mandatory and you must enter it on your Xesar tablet upon initialising Xesar access components for the first time to add them to your system.

If you open the ***Settings*** menu page for the first time, you must change the default PIN "0000" to be able to once again close the Settings menu.

15.2.2 Identification media validity periods

Specify the ***identification media validity period*** in the ***Security settings*** section for ALL Xesar identification media within your Xesar locking system.

The minimum validity period is one day and the validity period of Xesar identification media is automatically extended by the specified period as soon as you hold them to the Xesar coding station. This function is intended as a checkpoint function to enhance the security and force users to update their media within certain intervals. (The maximum validity period of a Xesar identification medium is up to the end of 2079.)

If the Xesar identification medium is not used at a Xesar coding station within the specified period, the identification medium expires and is deactivated until it is once again used at the Xesar coding station.

The Xesar identification medium is reactivated automatically once it is held to the Xesar coding station. This functionality represents a checkpoint within your system which forces users to regularly update their Xesar identification medium at this checkpoint. EVVA recommends using a very frequently used area, such as the reception or an information point for this function.

The Xesar software must be running to support this function. However, you can run it in the background, even with a locked Desktop.

Once the validity period has expired, the affected identification medium is unable to unlock any doors until it is updated at a coding station. Take this into account if you position an update unit indoors. The shorter the identification media validity period, the faster your system regains a secure status in the event that media are

lost. However, in the event that identification media are lost, we strongly recommend to transfer the blacklist to access components using the tablet.

15.2.3 Replacement media validity periods

You can issue one replacement medium per person should a Xesar identification medium be temporarily unavailable. Set the general validity period of a replacement medium here. The maximum permitted validity period is 72 hours (Figure 53: Time settings).

15.2.4 Logging personal data

If you would like to log personal data (event protocol), you can configure this in the Settings. In this case, please set the "Off" default setting to "On" (Figure 53: Time settings).

Comply with the corresponding, national statutory regulations and directives regarding data protection!

15.2.5 Maximum archiving period for personal data

You can restrict the maximum period any data is retained (Figure 53: Time settings). Data older than the specified period will be automatically rendered anonymous.

15.3 Programming device

Select your programming device (Xesar tablet) from the drop-down list if you have connected other external devices to your computer and are unable to detect the Xesar tablet.

15.4 IP address/proxy server settings

An Internet connection is briefly required to top up KeyCredits. If you access the Internet on your computer using a proxy server, you must configure the settings accordingly in the "Host name or IP address of the proxy server" section ❹(Figure 53: Time settings).

15.5 Configuration settings

The configuration settings enable to change the path for automatic backups at any time and switch the automatic backup function on or off.

Please note that any database backups saved on the same hard disk will be lost in the event of a hard disk failure. For this reason, EVVA recommends you use an external hard disk to backup the database. Archive the backups by versions to have older versions available in the event of a potential database fault.

You can edit the duration of the event saved in the protocol/events listed in Section 2.3.4 (=> 15 Settings). This significantly improves the system performance. In the configuration settings (=> 15.5) you can specify how often data is exported and saved. In the security settings (=> 15.2) you can change the duration personal data is saved in the system.

16 Administration

The Administration menu item enables to configure general system settings. Click "Administration" to open the overview (Figure 54: Administration tab).

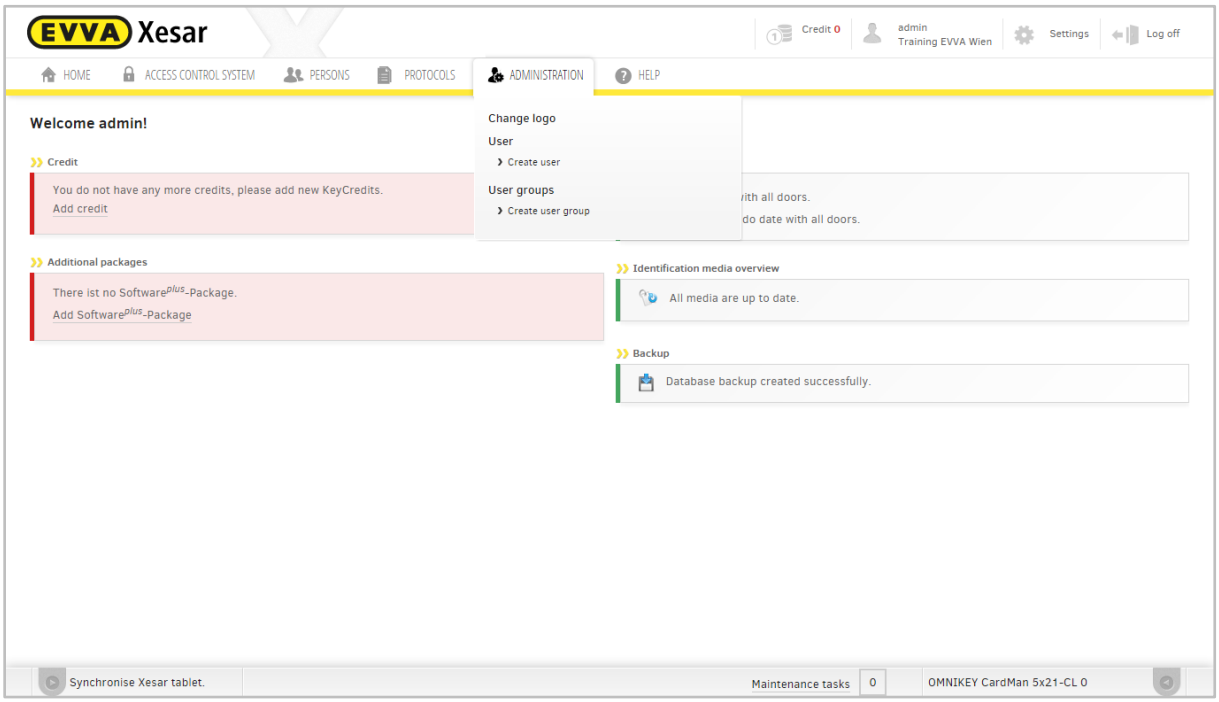


Figure 54: Administration tab

16.1 Changing the client logo

If necessary, change your client logo here. The selected logo will then be shown in the program's tool bar ❸ (Figure 55: Individual client logo).

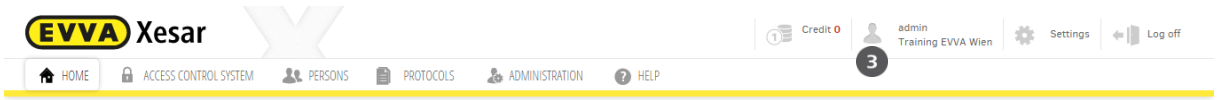


Figure 55: Individual client logo

Proceed as follows to change the logo:

- Select ***Administration*** > ***Change client logo***

- ***Select file*** ❶ (Figure 56: Changing the)
  Select the desired image file (.jpg, .png or .gif).
- Click ***Save changes*** ❷ (Figure 56: Changing the)

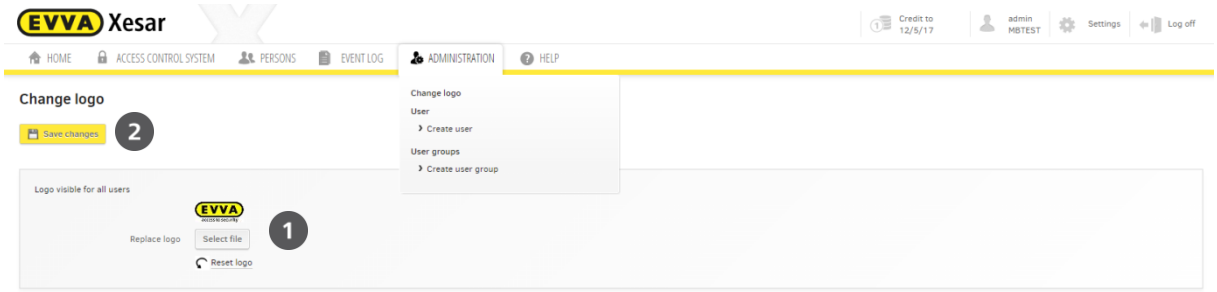
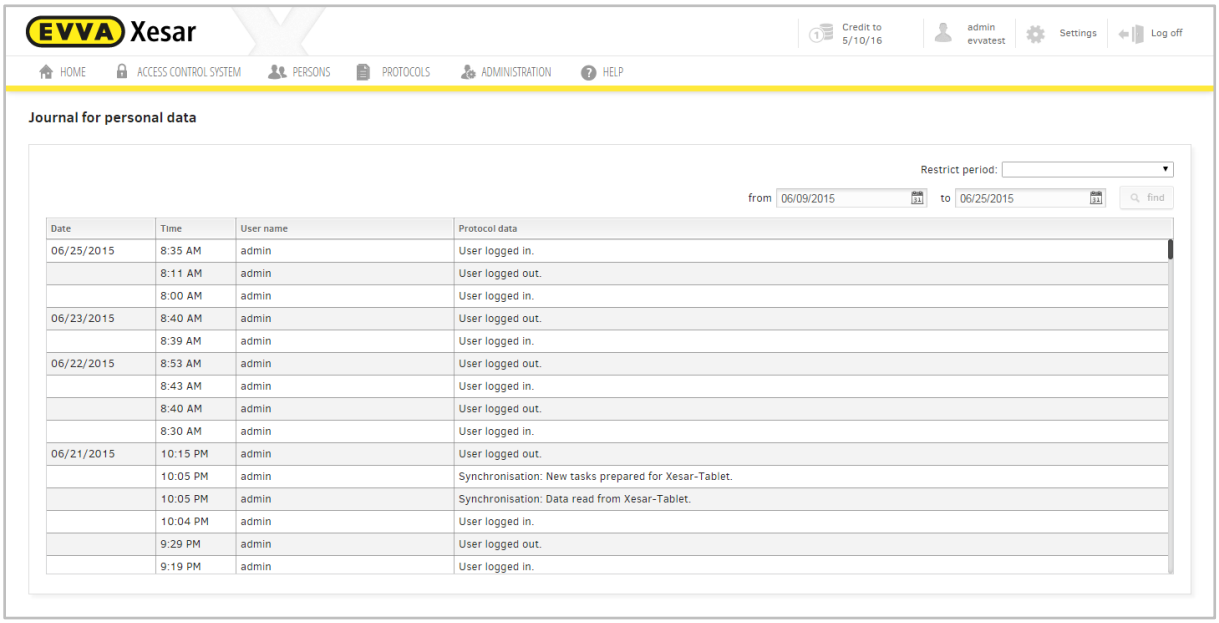


Figure 56: Changing the client logo

The desired image file must not exceed a size of 1 MB.

16.2 Journal

The Journal section records any user activities, such as login and logoff data as well as information on access to personal data. The filter function in the Journal allows to specify a period for the listed data.



Date	Time	User name	Protocol data
06/25/2015	8:35 AM	admin	User logged in.
	8:11 AM	admin	User logged out.
	8:00 AM	admin	User logged in.
06/23/2015	8:40 AM	admin	User logged out.
	8:39 AM	admin	User logged in.
06/22/2015	8:53 AM	admin	User logged out.
	8:43 AM	admin	User logged in.
	8:40 AM	admin	User logged out.
	8:30 AM	admin	User logged in.
06/21/2015	10:15 PM	admin	User logged out.
	10:05 PM	admin	Synchronisation: New tasks prepared for Xesar-Tablet.
	10:05 PM	admin	Synchronisation: Data read from Xesar-Tablet.
	10:04 PM	admin	User logged in.
	9:29 PM	admin	User logged out.
	9:19 PM	admin	User logged in.

Figure 57: Journal for personal data

Click the drop-down list in the ***Filter*** ❶ (Figure 58: Filtering journal entries) section and select the desired period to restrict the output. Click the last item in the drop-down list to activate the calendar function.

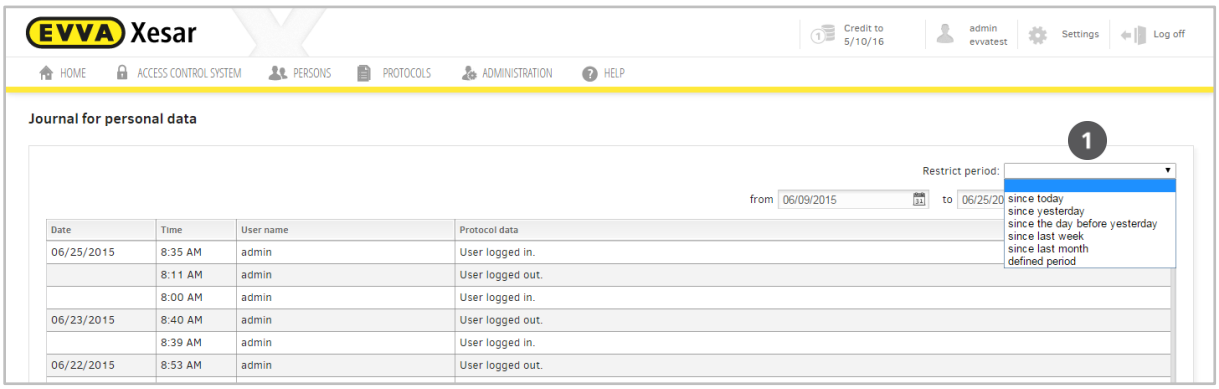


Figure 58: Filtering journal entries

Users are unable to delete the journal.

16.3 Users

Users are responsible for administrative tasks within the software. Each user is assigned individual authorisations. Administrators centrally manage the system and they always have comprehensive authorisation. It is not possible to deactivate administrator accounts.

Select ***Administration > User*** to view a list of all users and the user group assigned to the corresponding user (Figure 59: Users).

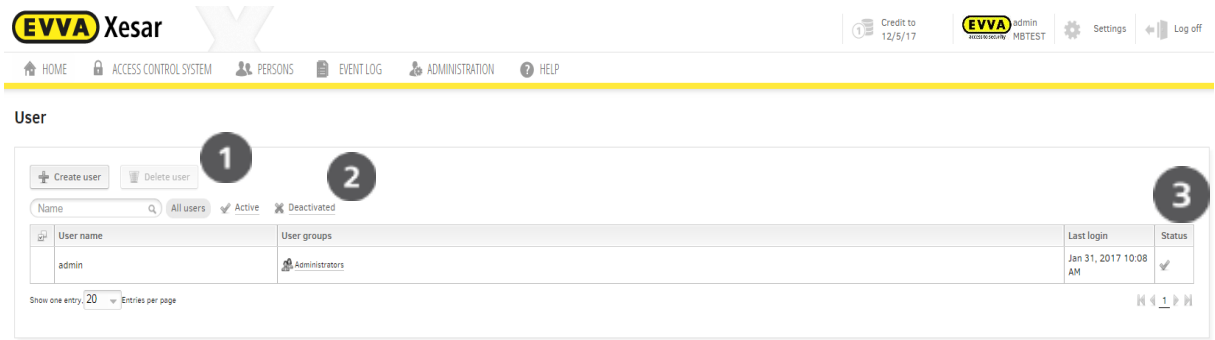


Figure 59: Users

Filtering for active and deactivated users

(Figure 59: Users)

- Click Active ❶ or Deactivated ❷ in the header of the list to filter by the corresponding user group.
- The Status ❸ column shows the corresponding icons for each user.

16.4 Editing users

Click the affected user to open the ***Edit user*** menu item. This section allows you to configure various user-specific settings and provides an overview of the selected user's current status. (Figure 60: Editing users)

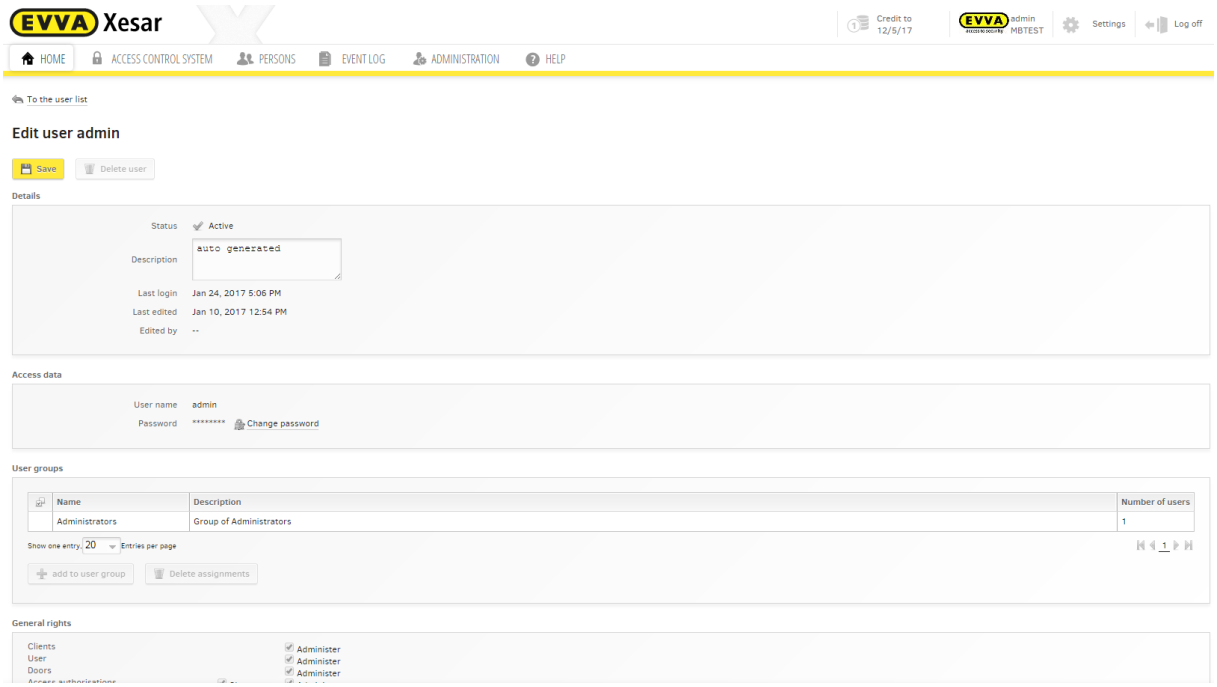


Figure 60: Editing users

16.4.1 Details

The ***Details*** field provides detailed information on users and gives you the option to activate or deactivate users, insofar as this function has been enabled.

- Description
- Last login
- Last edited
- Edited by

16.4.2 Deactivate user

- Click to select users and deactivate them.
- Change the status ❶ by clicking ***Deactivate user***.
- Click ***OK*** to confirm the security prompt and Save the changed data.

You cannot deactivate user admins.

16.4.3 Changing access data and passwords

You can change users' passwords in the ***Access data*** field.
Proceed as follows:

- Click the user name of the desired user and select ***Change password*** to open the dialogue to change the password in the ***Access data*** *section.*
- Enter a new password. It must feature between 6 – 20 characters and contain upper case and lower case letters as well as digits.

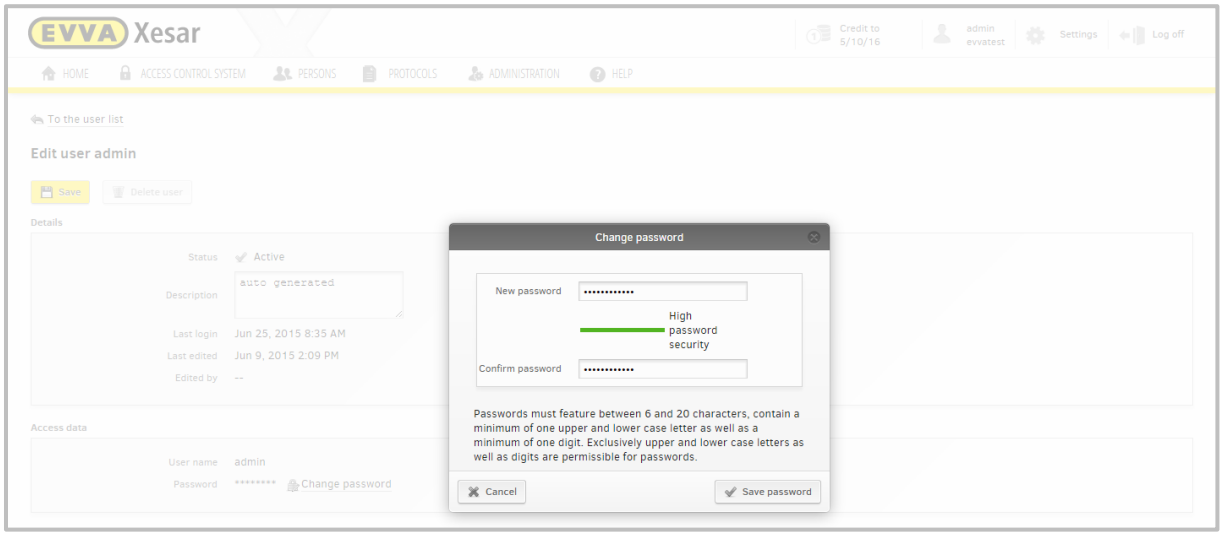


Figure 61: Changing the password

16.4.4 User groups

Open the ***User group*** field to assign or delete users from user groups. You can also (de)activate any assigned user groups.

Proceed as follows to add users to an existing user group:

- Select the ***User groups*** ❹ from the drop-down list to which you would like to assign users. Any assigned user groups are not shown in the menu.

Proceed as follows to delete assignments to user groups:

- Tick to select affected user group(s) and click the ***Delete assignments*** field. In this process, confirm your selection by once again clicking ***Delete assignment***.

16.5 Creating users

In this section, you can create one or more users with different authorisations. Please note that you must initially create new user groups before you can re-configure general authorisations for said users.

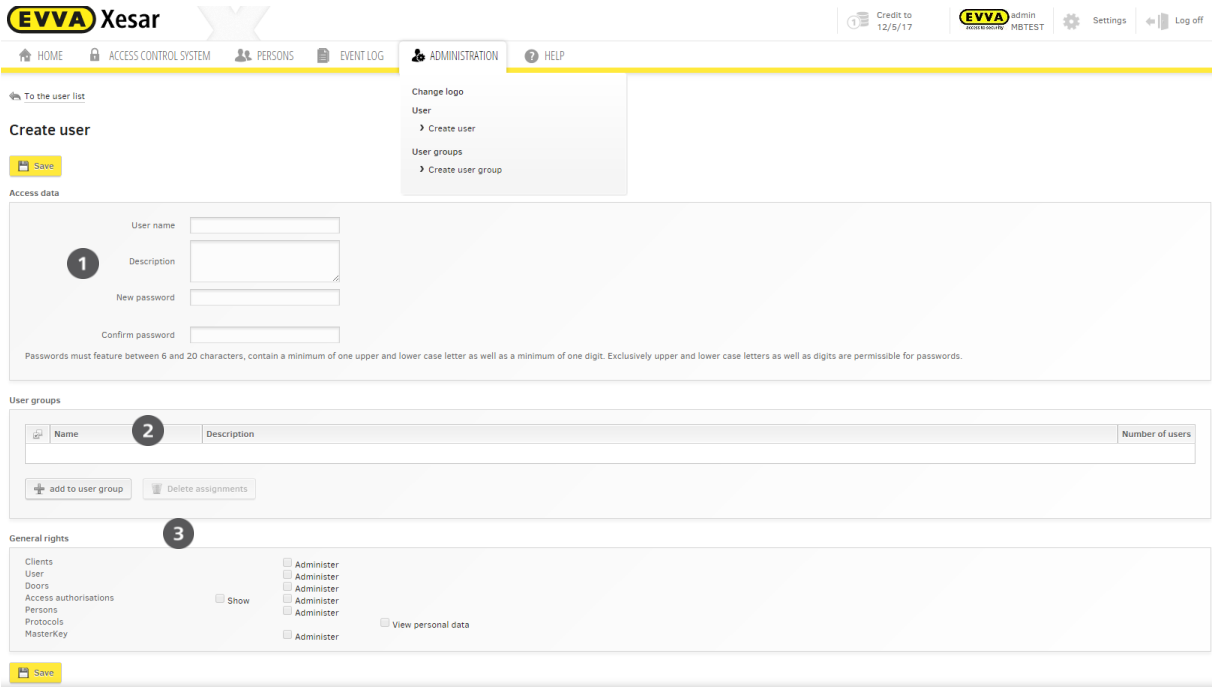


Figure 62: Creating users

16.5.1 Access data

Proceed as follows to create users (Figure 62: Creating users):

- Select ***User name*** ❶.
- If applicable, enter a ***Description*** ❷.
- Create a ***New password*** ❸ as per the following specifications:
  Between 6 and 20 characters, featuring upper case and lower case letter as well as digits. Your password will qualify as a "Secure password" once it complies with the aforementioned specifications; insecure passwords do not comply with the specifications.

16.5.2 User groups

- Select the ***User groups*** from the drop-down list to which you would like to assign users. Any assigned user groups are automatically unavailable for selection.
- Click ***Save user group*** to confirm your selection.

16.5.3 General rights

- Select the ***General rights*** ❺ you would like to assign to the person. They are transferred as specified in the users groups and cannot be adapted in this section.
- ***Save*** your changes confirm them.

The Xesar software home screen now confirms the changed data.

16.6 User groups

Specify users and user groups to manage them in the software.
You can assign different authorisations to user groups.
The ***Administrators*** user group has been pre-installed and you are unable to delete it. Said user group has been assigned comprehensive authorisations.
Please note that each user must be assigned to a minimum of one user group.

Any created user groups are listed in ***Administration*** > ***User groups***. Enter user groups in the search field to select them. You can also delete user groups in this section.

User groups are case-sensitive.

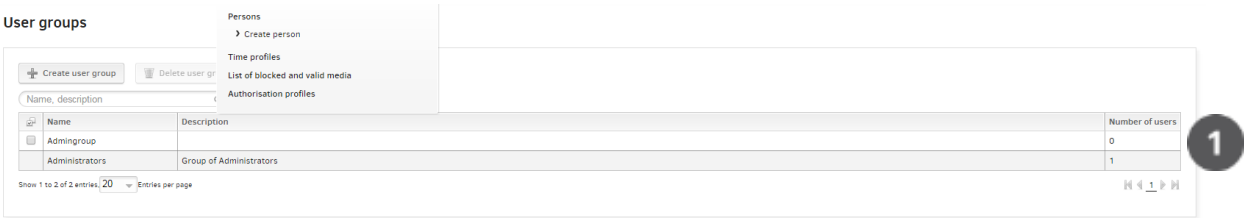


Figure 63: User groups

The ***Number of users*** section ❶ (Figure 63: User groups) shows the number of users assigned to the corresponding user group.

16.6.1 Deleting user groups

You can exclusively delete user groups if no users have been assigned to them. Proceed as follows to delete user groups:

- Tick the check box of one or more user groups(s) to select them.
- Then click the ***Delete user group*** *field.*
- Click ***Delete user group*** to confirm the security prompt. Once you have confirmed, you will be unable to undo the process.

An additional security prompt appears if users are still assigned to the user group you would like to delete.

You are unable to delete the ***admin*** user and the ***Administrator*** user group.

The entries of the deleted user group are automatically removed from the user settings.

16.6.2 Creating user groups

Different authorisation profiles may be required depending on the corresponding users' management tasks.
Open the ***Create user group*** section to create user groups for a host of requirements and assign different authorisations to said user groups. (Figure 64: Creating user groups)

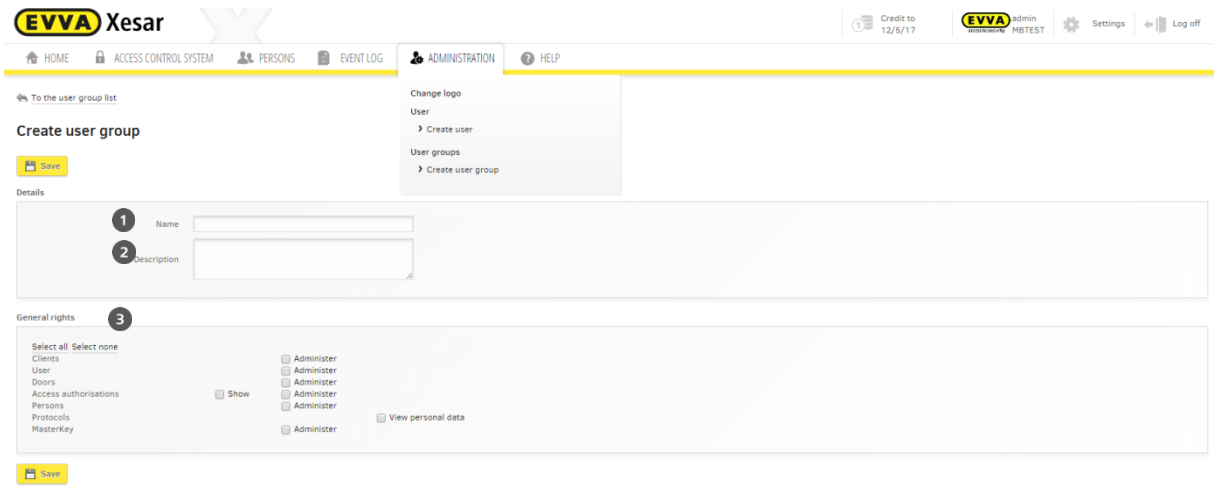


Figure 64: Creating user groups

16.6.3 Details

Specify the group name and description in the ***Details*** section.

- Specify a unique ***Name*** ❶ for the user group, for instance Facility management.
- Enter a short ***Description*** ❷ of the corresponding name.

16.6.4 General rights

This section allows to specify user rights.
Specify user authorisations in the ***General rights*** ❸ section of the user group. The section specifies the administrative tasks that influence clients, users, doors, access authorisations, persons and emergency media.

- Select "***User*** -> ***Administer***" to create, view, change or delete users.
- Select "***Door*** -> ***Administer***" to create, view, change or delete doors.
- Select "***Access authorisations*** -> ***Show***" to view access authorisations for doors. This requires additional authorisations.

- Select "***Access authorisations*** -> ***Administer***" to add, change and delete access authorisations for doors. This requires additional authorisations.
- Select "***Clients*** -> ***Administer***" to view and change system settings. You can configure all settings but the client logo.
- Select "***Masterkey*** -> ***Administer***" to issue master key authorisations. This requires additional authorisations.
- Select "***Protocols*** -> ***Administer***" to view personal events.

Click the corresponding tick box to activate the functions.

Specify authorisations according to users' administrative tasks. In this process, it is important to note the authorisations (options) you are granting users.

The ***Masterkey*** function is equivalent to a master key for all doors and it is always authorised to open doors.

16.6.5 Editing user groups

- Click the user group you would like to change in the user group list (Figure 65: Editing user).
- Check or change the details (name, description) ❶.
- Correct any activated, general rights ❷.
- ***Save*** changes ❸.

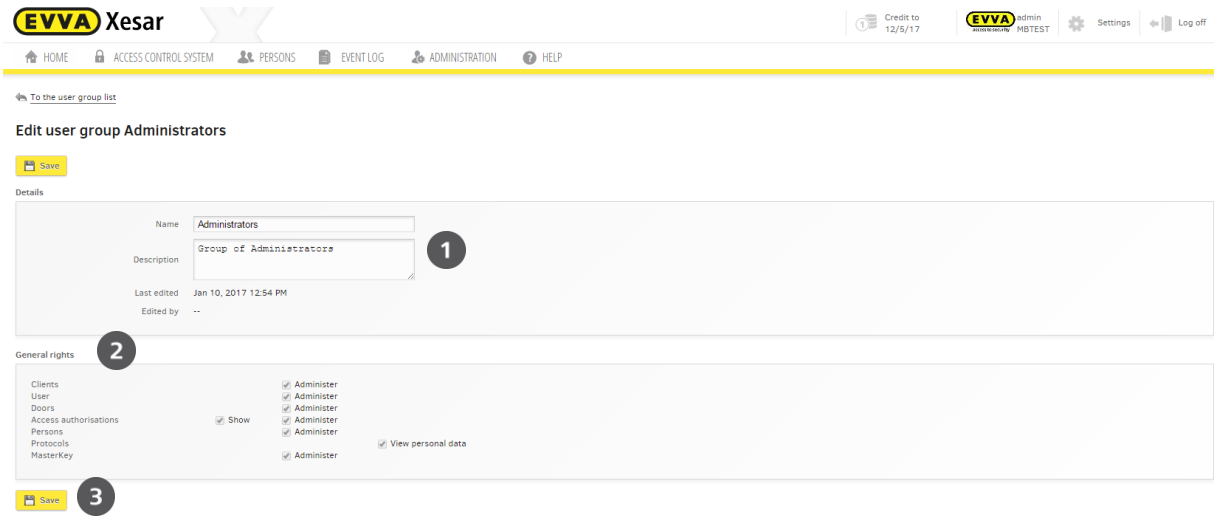


Figure 65: Editing usergroups

Your changes will come into effect after having saved them and they apply to all users linked to the specific authorisation group.

16.7 Managing groups of persons using shared authorisation profiles

You can quickly and efficiently manage different users and user groups using **Shared authorisation profiles** by pre-defining time profiles and authorisations.

Create authorisation profiles in Users.
Click **Persons ❶ > Authorisation profiles ❷**

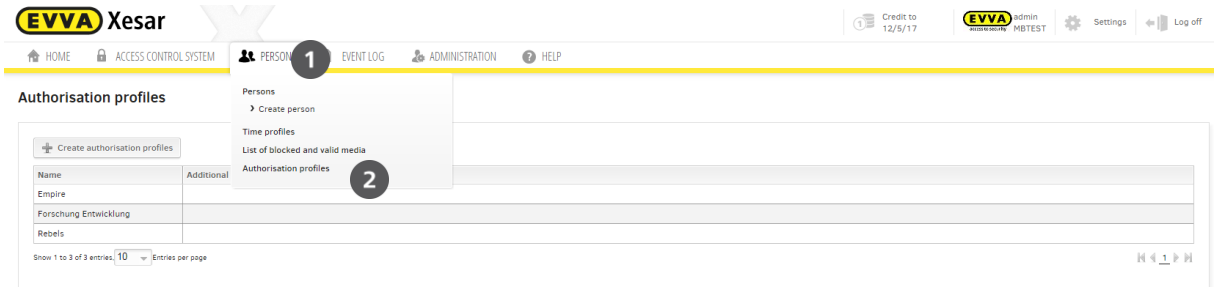


Figure 66: Creating authorisation profiles

Click **Create authorisation profile ❶**

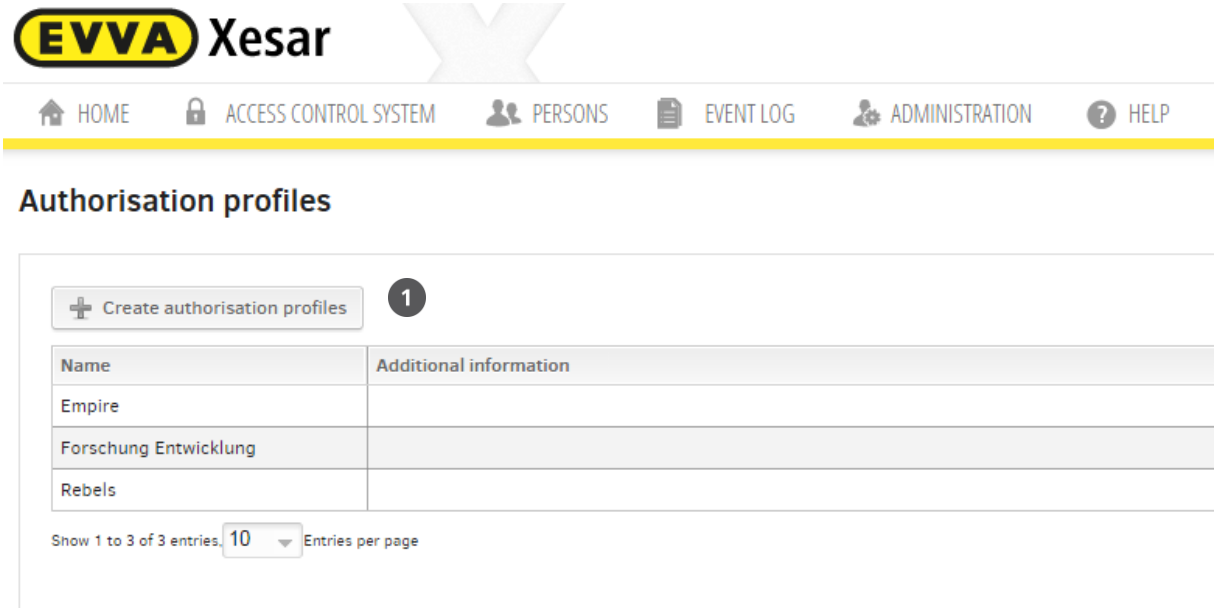


Figure 67: Creating authorisation profiles 2

Assign a name to the authorisation profile ❶ and add doors and door areas ❷ to this profile:

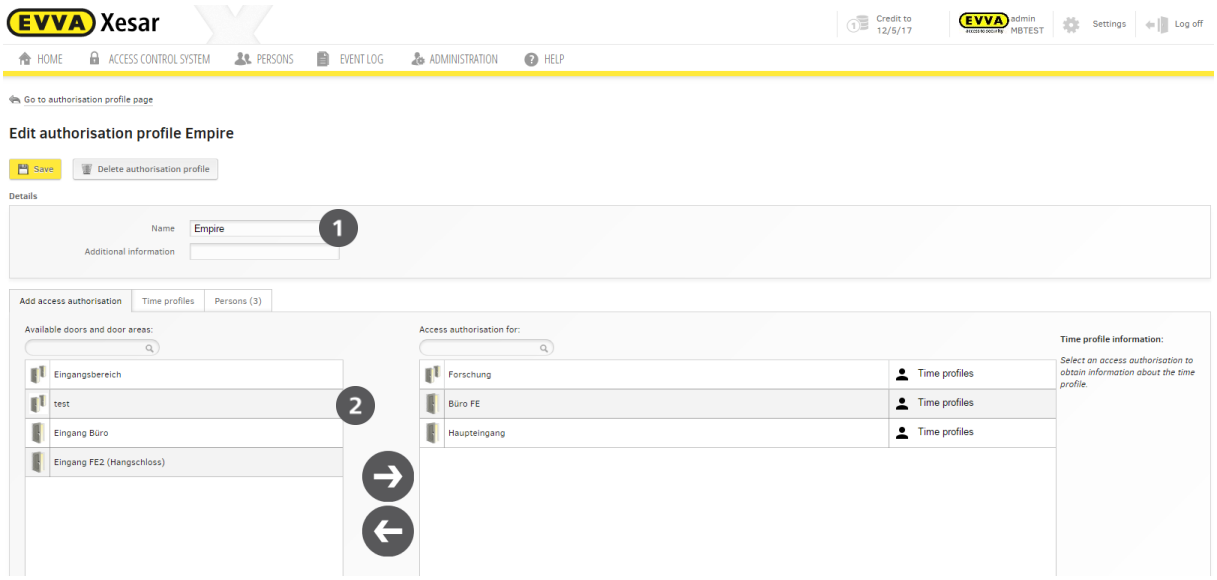


Figure 68: Adding access authorisations

Authorisation profiles can also be combined and enhanced by time profiles ❶.

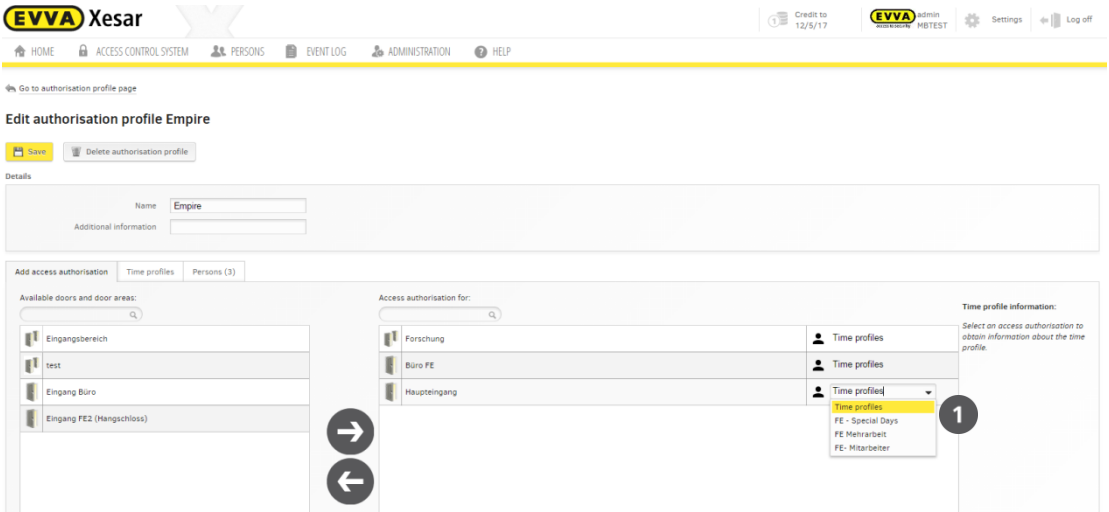


Figure 69: authorisation profiles

Click **Persons** and select the user you would like to assign an authorisation profile to if you would like to **Add an authorisation profile ❶**, to users.

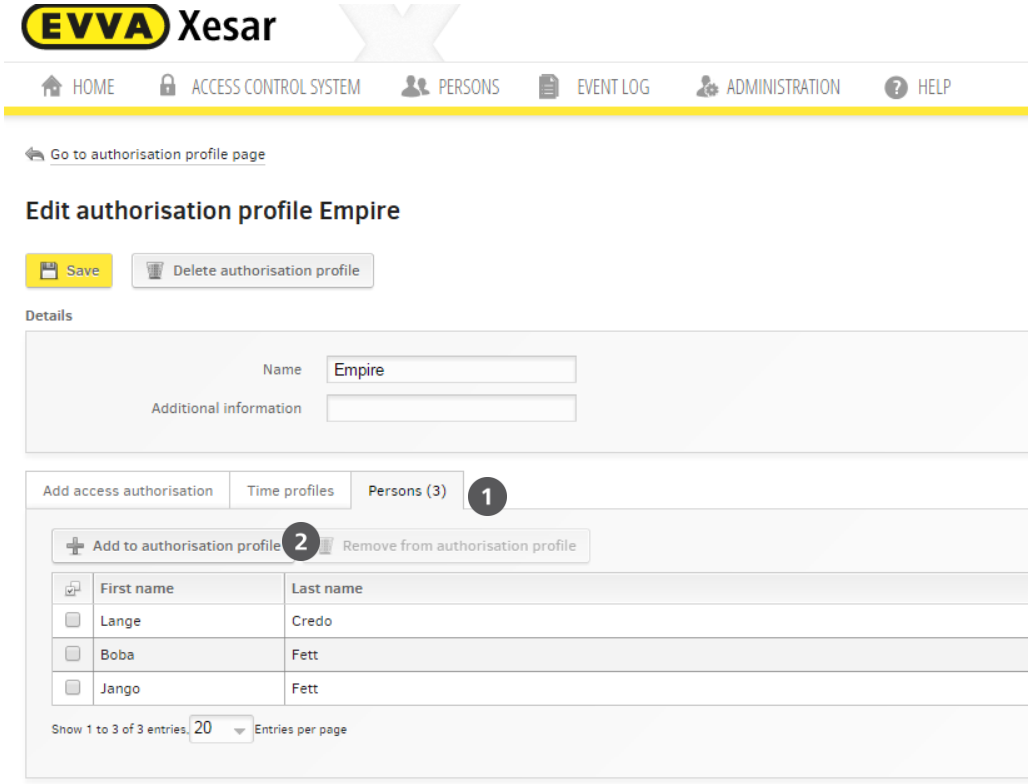


Figure 70: Adding authorisation profiles

Alternatively you can also directly change authorisations in the user profile by clicking **Authorisations ❶** and selecting an **authorisation profile ❷**

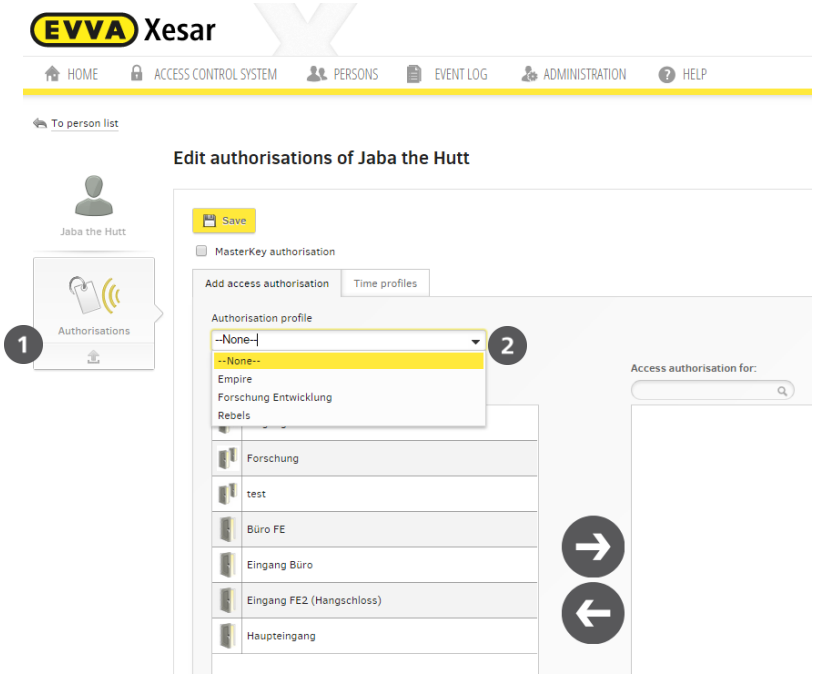


Figure 71: Authorisation profile

You can once again view the ***time profile*** ❶ after having assigned the authorisation profile to check the data:

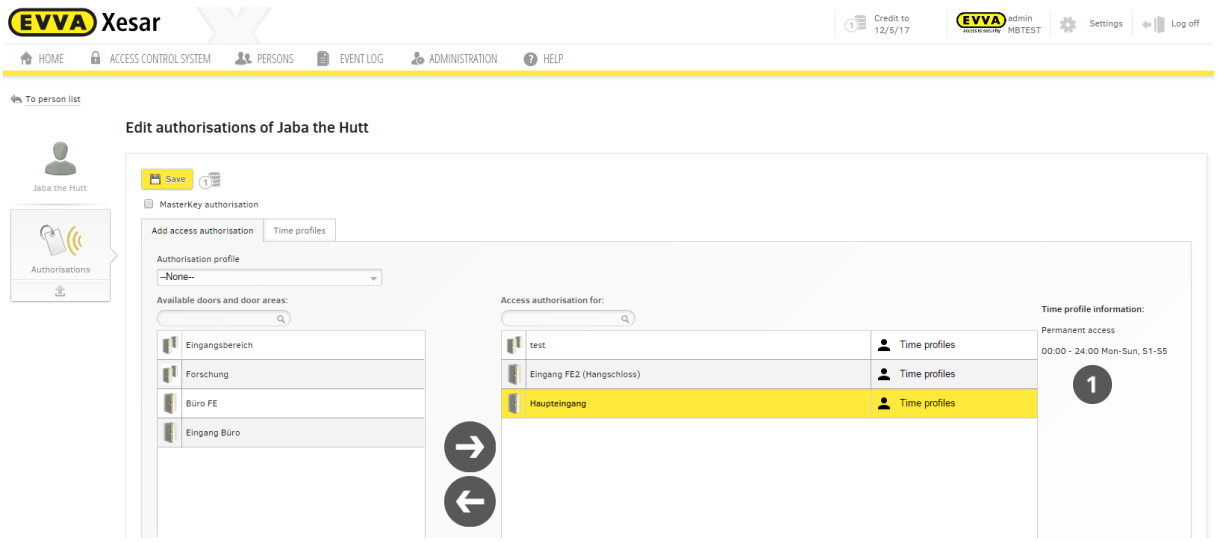


Figure 72: Editing persons' authorisations

Authorisation profiles can also be ***enhanced*** ❶ by the corresponding persons and doors/areas **individually**, depending on the demand:

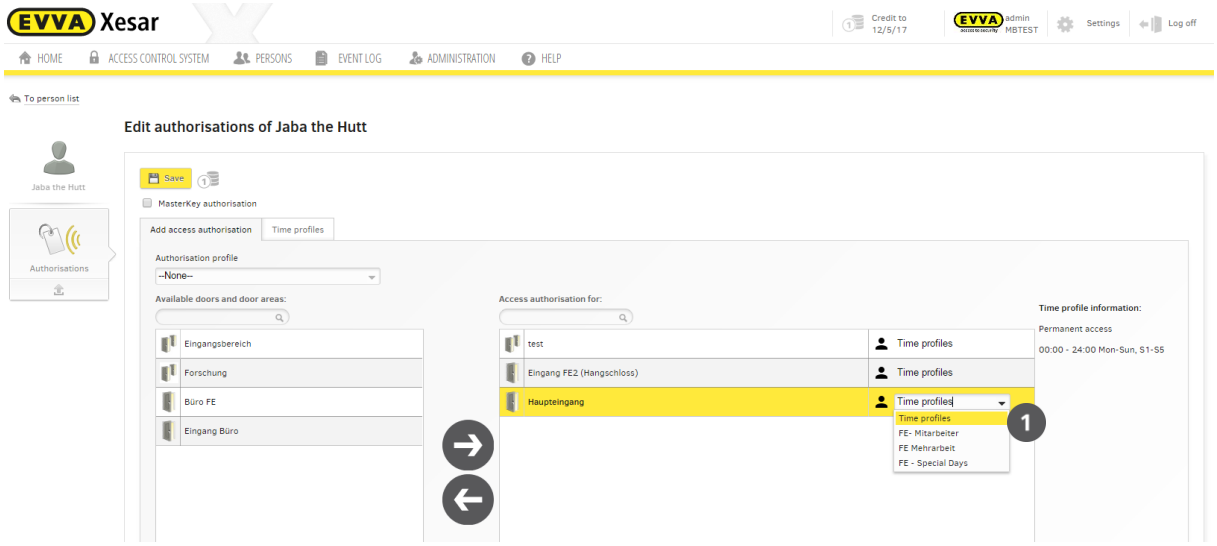


Figure 73: Individually changing or enhancing authorisation profiles

17 Doors and areas

The ***Doors & areas*** menu item enables to view and manage any doors and areas within the Xesar locking system including all created Xesar access components.

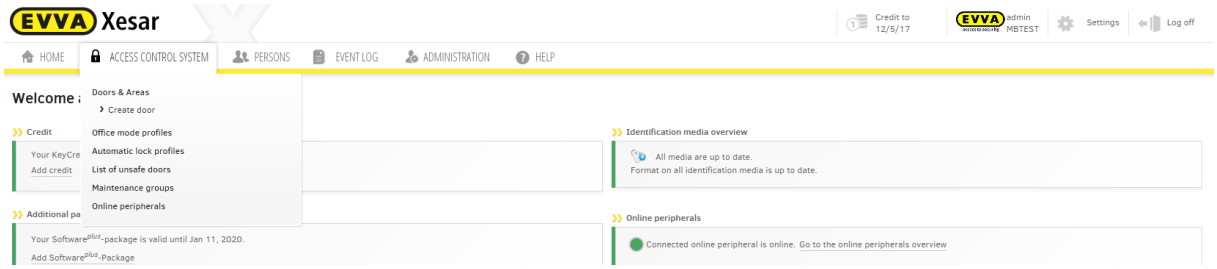


Figure 74: Doors and areas

17.1 Doors and areas

In the ***Doors & areas*** section, click the corresponding selection ❶ (select by door) or ❸ (select by area) to open a list of doors and areas which have already been created in the Xesar software and view which doors have been assigned to which areas. You can also assign doors to areas in this section. Create areas to group several doors in categories and facilitate assigning authorisations to make the overall process more transparent. For instance, if you would like to grant one or more persons access to five individual doors, you can group these in an area. Subsequently, all you need to do is assign persons to the area to enable them to unlock the aforementioned five doors. You can create a maximum of 96 areas. It is possible to assign doors to several areas. (Figure 75: Doors and areas)

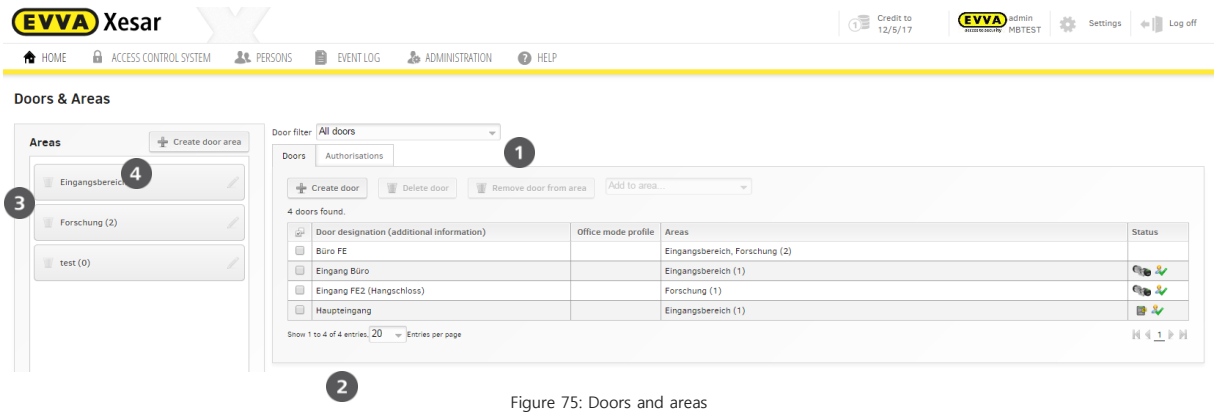


Figure 75: Doors and areas

17.1.1 Show All doors

Click ***All doors*** to show a list of all doors within the Xesar locking system, regardless of whether or not they have been assigned to an area.

17.1.2 Show Doors within an area

Click the door area you would like to view ❸. ***Doors within an area*** is selected automatically and the system shows a list of doors within this area ❷. The number of doors within this area is shown in brackets next to the area designation.

17.1.3 Show Doors that have not been assigned to areas

Click ***Doors that have not been assigned to areas*** to view all doors that have not been assigned to an area within your Xesar locking system ❷.
In addition to the overview functions, the ***Doors & areas*** section also enables to edit and manage doors and areas.

The following functions are available:

- Creating door areas
- Creating doors
- Deleting doors
- Deleting doors from a door area
- Adding doors to a door area
- Editing/deleting door areas

17.1.4 Creating door areas

Proceed as follows to create door areas:

- Click ***Doors & areas*** > ***Doors & areas***.
- Click ***Create door area*** ❹ (Figure 75: Doors and areas).
- Specify the ***Name*** of the door area ❶ (Figure 76: Creating new door areas).
- Click ***Save*** to confirm your input.

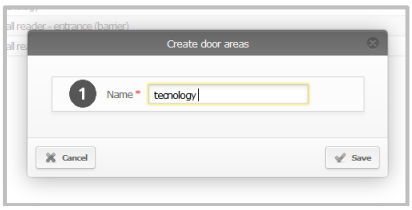


Figure 76: Creating new door areas

17.1.5 Creating **additional doors**

Proceed as follows to create an additional door:

- Click the ***Create door*** field ❶ and proceed as described in Section (
- Creating doors; Figure 77: Managing doors).

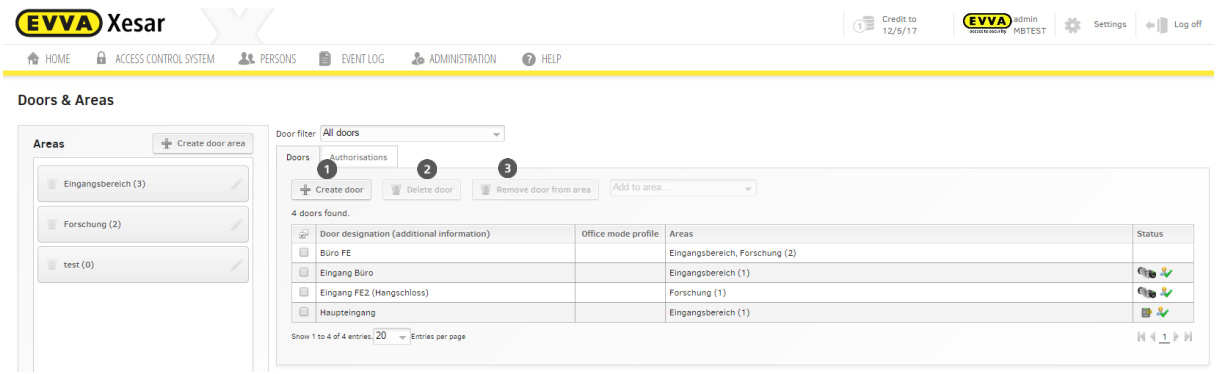


Figure 77: Managing doors

17.1.6 Deleting doors

You can also delete doors in this menu item (Figure 77: Managing doors).

- Click "All doors" or the area featuring the affected door.
- Tick the check box next to the desired door.
- Then click ***Delete door*** ❷.
- Click ***Delete door*** and confirm the following prompt to complete the process.

17.1.7 Removing doors from areas

Proceed as follows to delete doors from an area (Figure 77: Managing doors):

- Click the affected area.
- Tick the check box of the affected door.
- Click the ***Remove door from area*** ❸ field.

17.1.8 Adding doors to areas

You can add one or several doors to an area.

- Tick the check box(es) of the affected door(s).
- Then select the desired area from the drop-down list ❶.

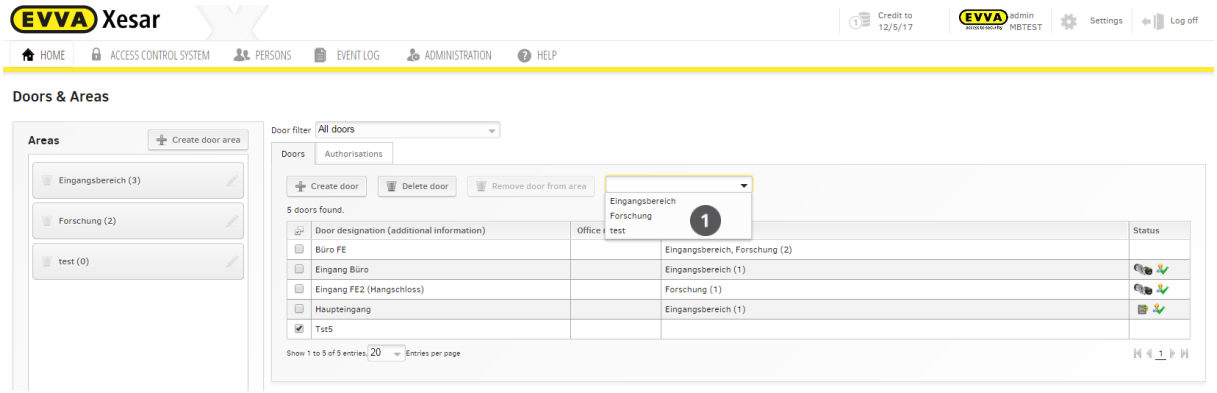


Figure 78: Adding doors to door areas

17.1.9 Listing authorised persons within an area

Door areas will automatically be highlighted in yellow once you have clicked to select them (Figure 79: Door area level 2).

The list of ***Doors*** ❸ shows all doors within thins area.

- Click the ***Authorisations*** ❸ field to view **all** persons with an authorisation to **all** doors of this area.

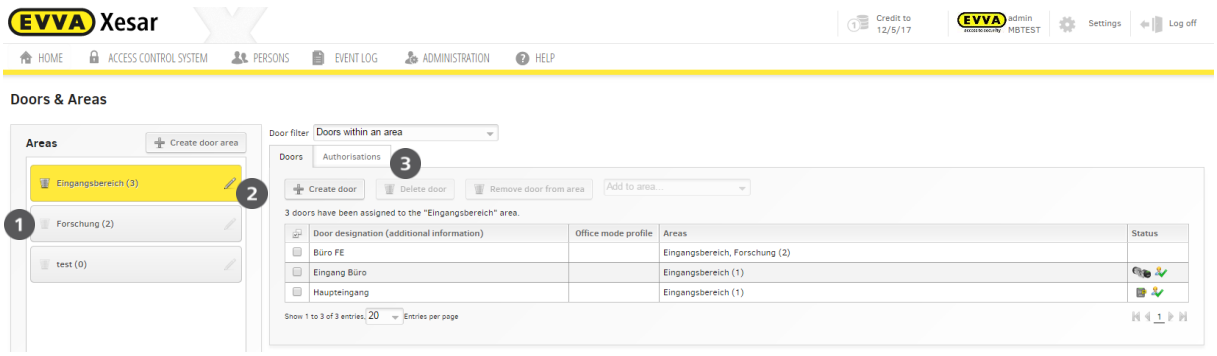


Figure 79: Door area level 2

17.1.10 Deleting door areas

- Click the affected door area to delete it.
- Then click the recycling bin icon ❶.
- Click ***Delete door area*** to confirm the prompt.

Any doors that are assigned to a door area are automatically removed upon deleting the door area. You will then have to synchronise the doors affected by the changes using the Xesar tablet.

17.1.11 Editing door areas

- Click the affected door area to rename it.
- Then click the pen icon ❷ (Figure 79: Door area level 2).
- Enter the new area designation in the ***Name*** field of the dialogue window (Figure 80: Renaming areas) and click ***Save*** to confirm.

Doors in this area remain available.

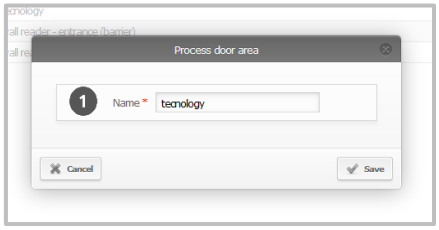


Figure 80: Renaming areas

17.1.12 Editing doors

- Click the desired door in the ***Doors & areas > Doors*** menu to open the application window.
  „***Edit doors*** enables to change door configurations.

17.1.13 Access components

- Click the icon of the corresponding access component to open the access component overview window of this door.

17.1.14 Details

- This section lists all detailed information of your access component.

17.1.15 View battery status

The ***Details*** field shows the battery status of battery-operated access components. Please note that the status dates back to the last time the access component and your Xesar software were synchronised and the actual battery status may deviate from the battery status shown.

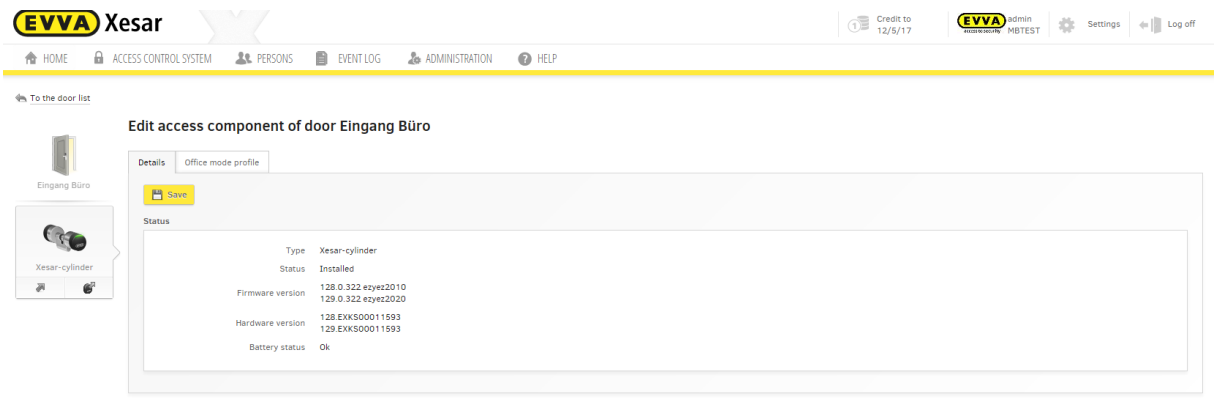


Figure 81: Xesar access components, "Installed" status

17.2 Creating doors

You can configure doors in this section. For this purpose, select ***Doors & areas*** > ***Create doors***. Subsequently click ***Save*** to save any changes.

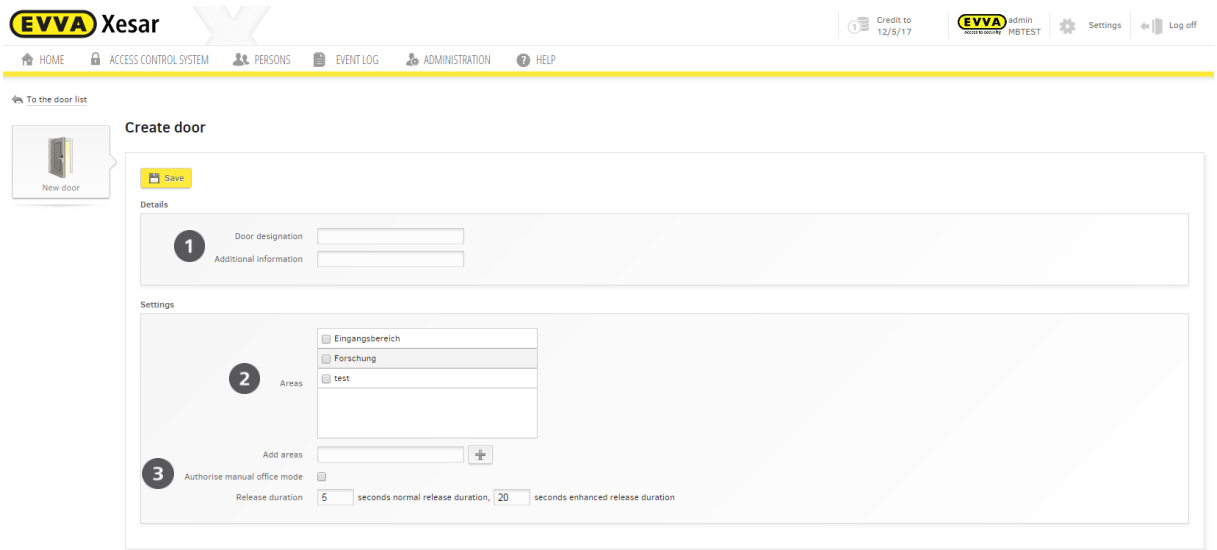


Figure 82: Creating doors

17.2.1 Details

When you create doors it is important to enter a unique ***Door designation*** ❶ (mandatory field) to safeguard the doors in the software can be assigned to the doors within the facility, e.g. Main entrance. There is also the ***Additional information*** field ❷ (optional field) intended for additional door information, e.g. the room number (Figure 82: Creating doors).

17.2.2 Settings

Select the areas to which you would like to add doors in the ***Areas*** field ❸ . You can also create additional areas in this section (Figure 82: Creating doors).

17.2.3 Manual office mode

Click the check box❸ to configure, whether or not to enable ***manual office mode with an authorised*** identification medium.
Please note that the corresponding settings must have been activated for the respective doors and persons to enable the manual office mode function.

Click ***Save*** to save any changes you made to settings. The ***New Xesar access component*** icon ❸ (Figure 83: Creating doors and logging personal data) automatically appears as soon you have saved the new door.

17.3 Editing doors

The ***Edit door*** menu item allows to edit all settings for the Xesar access components within the context of the affected door (Figure 83: Creating doors and logging personal data).

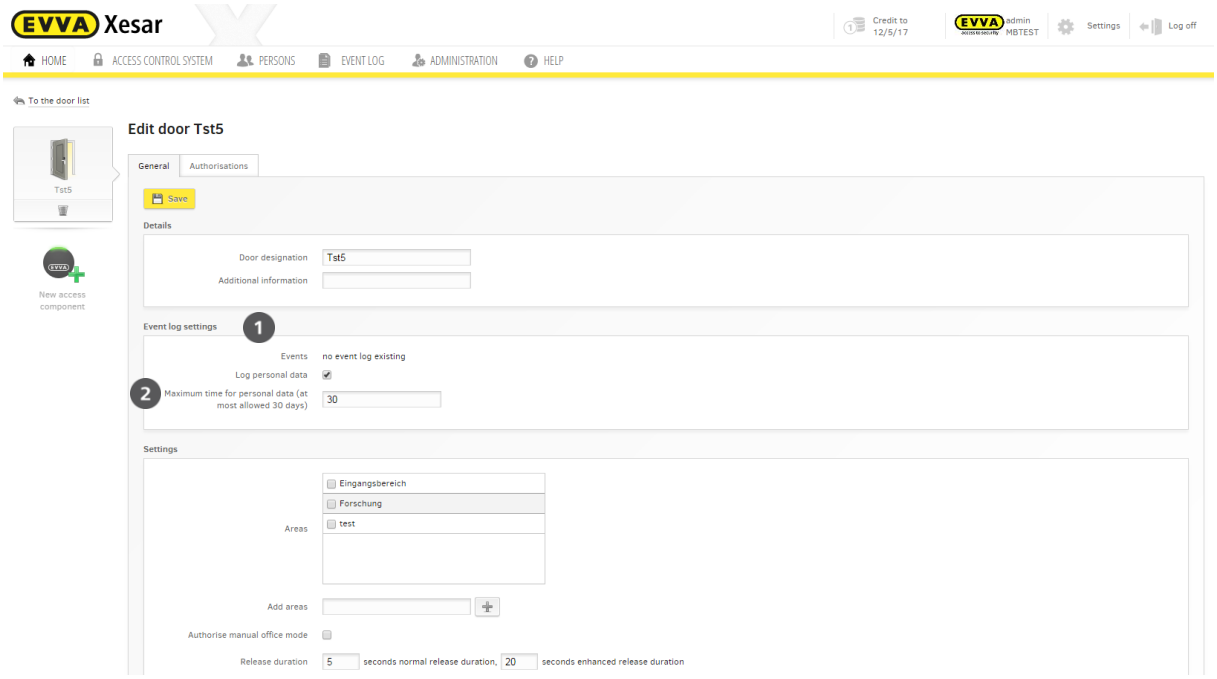


Figure 83: Creating doors and logging personal data

17.3.1 Protocol settings

Events

The "Edit doors" application window shows the ***Protocol settings*** section❶. Please refer to Section (*Fehler! Verweisquelle konnte nicht gefunden werden.*) for additional protocol information.

17.3.2 Personal data (per Xesar access component)

Select ***On/Off***❷ to specify whether or not to enable to log personal data at this door. However, the affected persons must additionally give their consent for you to be able to view their personal data.

17.3.3 Maximum retention period of personal data

Enter the maximum period you would like to retain personal data (in days). You are unable to save data for a period in excess of 99 days. The entered value also determines the maximum period door protocols are retained.

The input field is automatically activated if you set ***Log personal data*** to ***On***.

If the ***Log personal data*** function ❶ (Figure 84: Showing the personal data protocol) is on, you can click ***Show protocol*** to view the protocol list for this door ❷ ***(Protocol settings***).

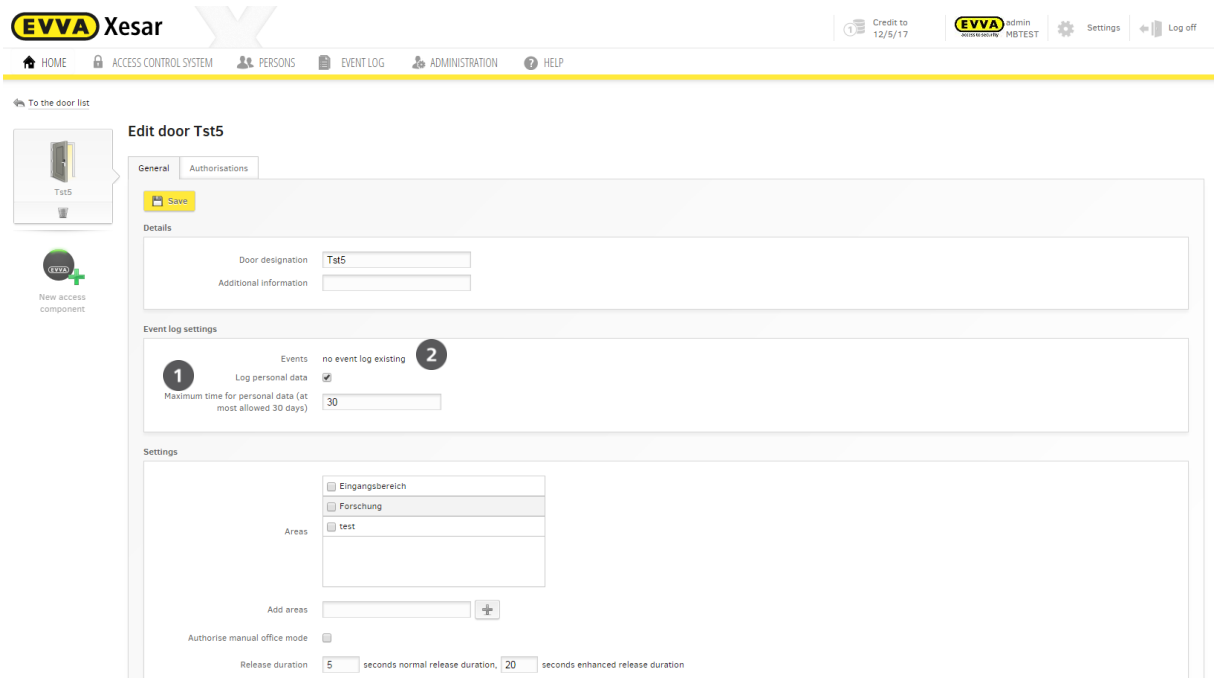


Figure 84: Showing the personal data protocol

Click ***Restrict period*** to specify a period within which to search for a certain event entry. Click the ***Access and opening processes***, ***Rejections and deletions***, ***Door configuration and Information*** or ***Warnings and errors*** buttons to filter for various event categories.

17.4 Adding Xesar access components

Proceed as follows to add a Xesar access component to your Xesar locking system:

17.4.1 Adding Xesar access components — step 1

- Click ***New access component*** to add a Xesar access component to your locking system (Figure 85: Assigning Xesar access components).

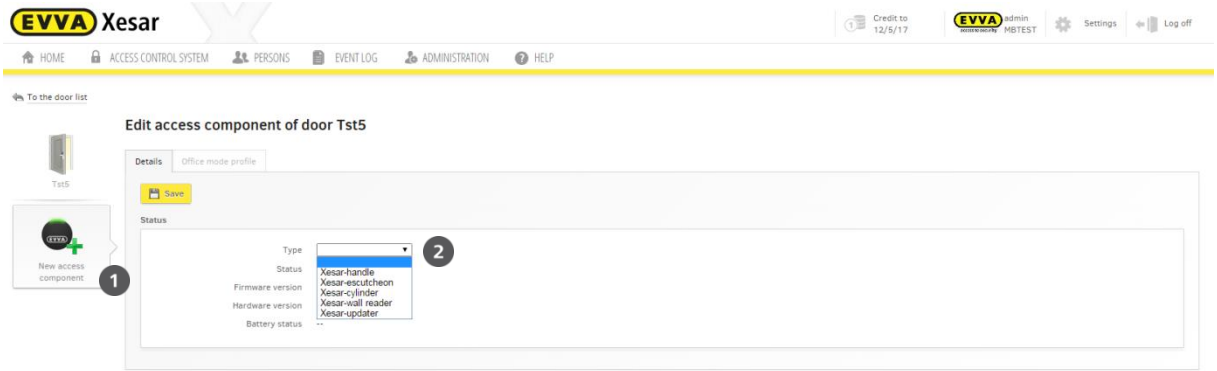


Figure 85: Assigning Xesar access components

17.4.2 Selecting escutcheon, handle or cylinder — step 2A

- In the ***Xesar access component*** application window you can now select the ***Type*** ❶ (Figure 85: Assigning Xesar access components) for your desired Xesar access component.
- The ***Status***, ***Firmware version*** and ***Hardware version*** fields are automatically completed as soon as you have initiated access components and transferred the data back to the software using the Xesar tablet.
- Click ***Save*** to confirm your selection.

17.4.3 Selecting Xesar wall readers — step 2B

The process varies depending on whether you would like to assign one or two wall readers to your control unit. Note options A, B and C:

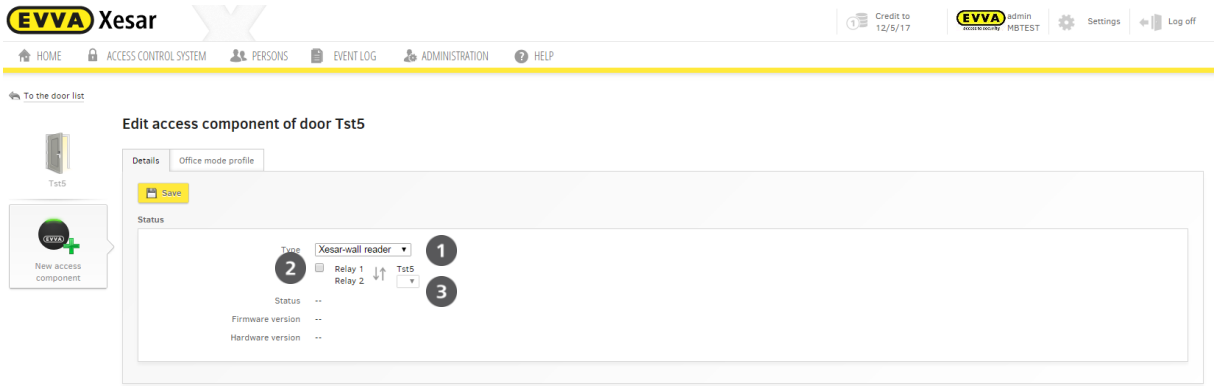


Figure 86: Connecting Xesar wall readers

17.4.4 Option A 1x Xesar wall reader with the Xesar control unit

- ***Relay 1*** ❶ (Figure 86: Connecting Xesar wall readers) is automatically assigned to the wall reader.
- Click ***Save*** to confirm.
- Now click ***To the door list*** to view the door list.

17.4.5 Option B 2x Xesar wall readers with the Xesar control unit)

- Create two new doors (refer to:
- Creating doors).
- Click ***New access component*** ❸ and select the Xesar wall reader from the drop-down list after having created the second door.
- ***Relay 1*** ❶ (Figure 86: Connecting Xesar wall readers) is automatically assigned to the wall reader.
- Tick the check box as shown in ❸ (Figure 86: Connecting Xesar wall readers).
- This will activate the "Two wall readers and one control unit" function.
- Select a different, newly created door from the drop-down list in the ❷ section. This automatically assigns a second wall reader to the selected door and the wall reader icon changes from  (icon-> one wall reader) to  (icon -> two Xesar wall readers).
- Click the arrow icon  to swap the assignments of relay 1 and relay 2. However, this is no longer possible once you have clicked ***Save*** to confirm your entries.
- Now click ***Save*** and select ***To the door list*** to view the door list.

17.4.6 Option C 1x Xesar wall reader (existing)/1x Xesar wall reader (new) <-> 1x Xesar control unit

- If you would like to enhance an existing Xesar control unit by a Xesar wall reader, you must initially remove the existing wall reader electronically. Subsequently proceed as described in Option B to connect both wall readers with the control unit.

Observe the connection instructions of the wall readers in the circuit diagram on the control unit lid.

Tip (double-sided cylinder):
Create two doors for this purpose and use the Additional information field to indicate their position – e.g. Door designation: Technology, Additional information: Outside and Door designation: Technology, Additional information: Inside.

The Status, Firmware version, Hardware version and Battery status fields are automatically updated when you synchronise using the Xesar tablet.

17.4.7 Added Xesar access components on the door list

After having added Xesar access components, they appear on the door list in the status line as icons (Figure 87: Door list status).

For example:
As you selected Option B on both doors ❹ B (**Two** Xesar wall readers connected to your Xesar control unit), the system indicates this with the icon at both affected doors.
The icon indicates that the Xesar access component is now ready for installation.
The icon indicates that the Xesar access component must still be synchronised.

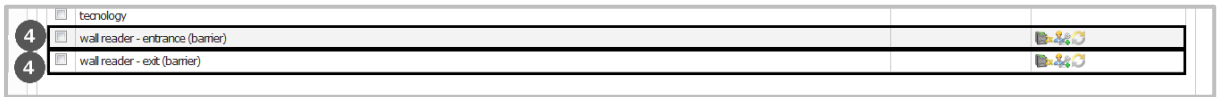


Figure 87: Door list status

Door list icons

This section lists all icons shown on the door list:

Product icon:

-  -> Xesar cylinder
-  -> Xesar escutcheon
-  -> Xesar handle
-  -> Xesar wall reader
-  -> 2x Xesar wall readers

Status information:

-  -> Ready for disassembly
-  -> Installed
-  -> Hardware replacement required
-  -> "Ready for installation" or "Replacement of Xesar access components required"

Tasks:

-  -> To be synchronised
-  -> Door will be deleted
-  -> Revoking installation or disassembly
-  -> Replace thumbturn
-  -> Xesar access component will be removed
-  -> Forced disassembly

17.4.8 Initialising Xesar access components — step 3A

Synchronise the Xesar tablet with the Xesar software to transfer the most recent data to the Xesar tablet.

After having created doors within the system and having assigned or changed Xesar access components, you must initialise Xesar access components directly at the component (for this reason, usually at the corresponding door).

Xesar access component due for synchronisation are highlighted in the ***Status*** field on the door list with the "To be synchronised" ❶ icon (Figure 88: Door list with status information).

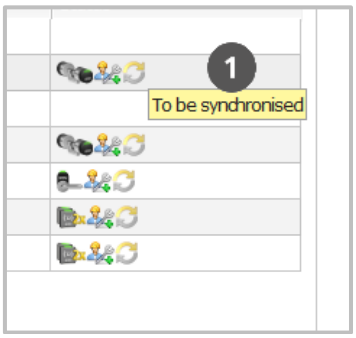


Figure 88: Door list with status information

Connect your Xesar tablet to your PC and click ***Synchronise Xesar tablet*** ❶ (Figure 89: Synchronising data with the Xesar tablet) to start synchronisation.

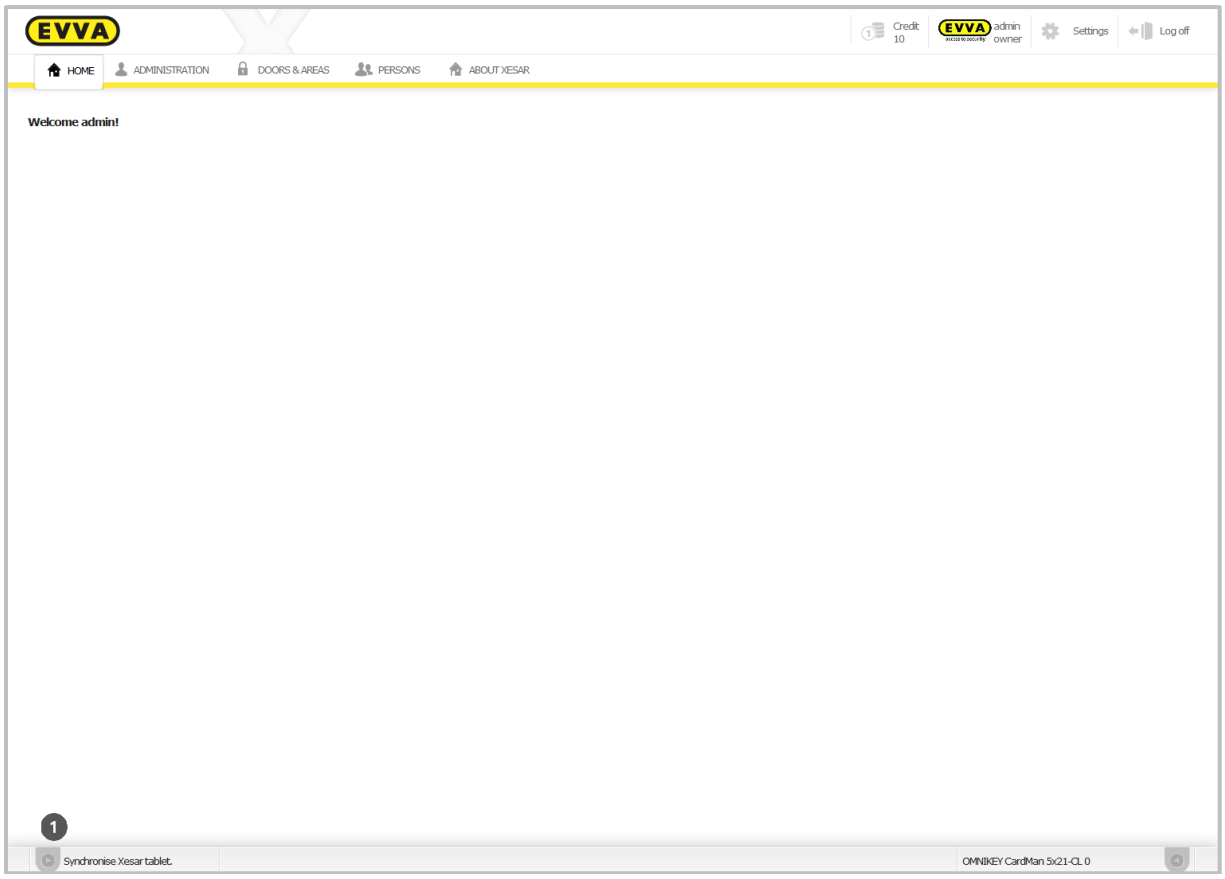


Figure 89: Synchronising data with the Xesar tablet

A notice appears in the software and on the Xesar tablet once synchronisation between PC and Xesar tablet has been completed successfully.

For reasons of security, the synchronised data remains available on the Xesar tablet for a maximum of two days. After this period you must repeat synchronisation.

You have now prepared your Xesar tablet for the initialisation of your Xesar access components. The first initialisation of a Xesar access component is shown on the Xesar tablet in the maintenance tasks as "Initialise Xesar access component".

- Connect your Xesar access component to your Xesar tablet using the connection cable and proceed as follows:
- Select the Xesar access component in the ***Maintenance tasks***.
- The Xesar tablet shows ***Initialise Xesar access component***.
- Select ***Execute*** to start the process.
  (Figure 90: Xesar tablet — initialising Xesar access components).

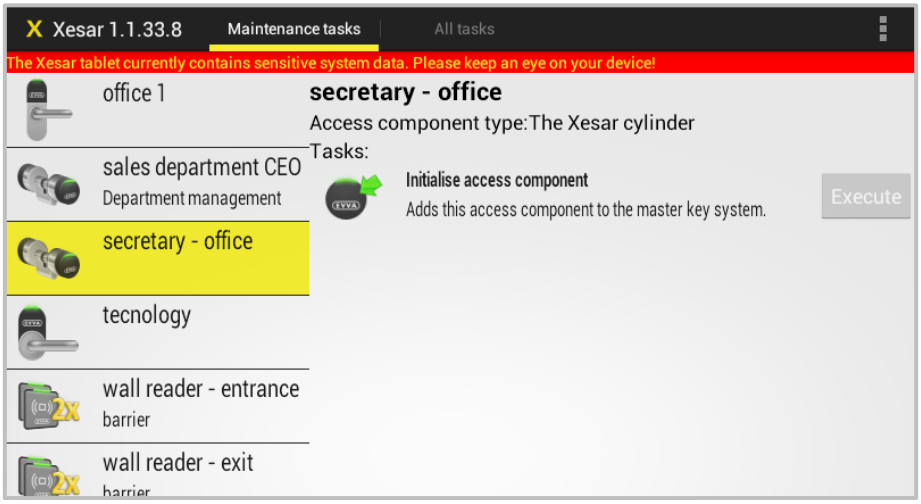


Figure 90: Xesar tablet — initialising Xesar access components

- You are prompted to enter your initialisation PIN. (Figure 91: Xesar tablet — entering the initialisation PIN) Enter the ***4-digit code***.

The initialisation PIN is the code you specified in your Xesar software in ***Settings > Security settings***.

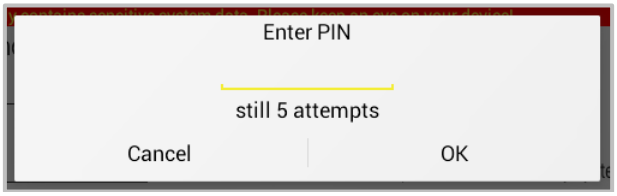


Figure 91: Xesar tablet — entering the initialisation PIN

- The system will give feedback if your input is correct.
  (Figure 92: Xesar tablet - process completed successfully

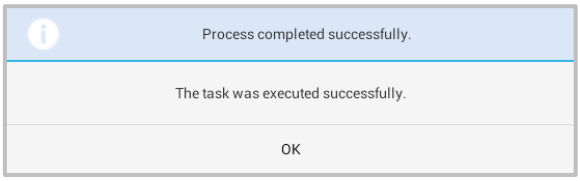


Figure 92: Xesar tablet - process completed successfully

- You have now added the Xesar access component to your Xesar locking system (Figure 93: Xesar tablet — successful initialisation).

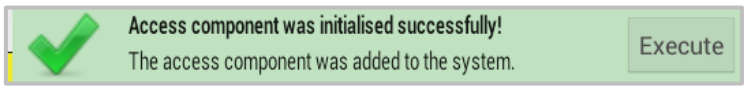


Figure 93: Xesar tablet — successful initialisation

An error message appears if your input is incorrect.

The data on the Xesar tablet is deleted after having entered an incorrect PIN five times due to a security violation. In this case, you must once again synchronise the information with the Xesar software.

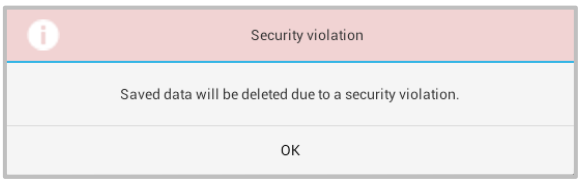


Figure 94: Xesar tablet — security violation message

17.4.9 Initialising two Xesar wall readers for one control unit – step 3B

If two wall readers have been connected to one control unit, both wall readers must be initialised one after the other. For this purpose, select the corresponding component on your Xesar tablet. There is no specific sequence in this process.
Any further synchronisations merely require one of the two Xesar wall readers to be connected to the Xesar tablet.
Each wall reader must be synchronised individually in the event of firmware updates.

17.4.10 Re-synchronisations with the Xesar software – step 4

Synchronise your Xesar tablet with your Xesar software to complete the integration of your new Xesar access component into your locking system.

- Connect the Xesar tablet to your PC using the USB cable.
- Click ***Synchronise Xesar tablet*** in the software to start synchronisation.
- The door status is now shown as "Installed" on the door list.
  (Figure 95: Door list - "Installed" status)
  The firmware version, hardware version and battery status in ***Doors > Xesar access component*** are also updated.

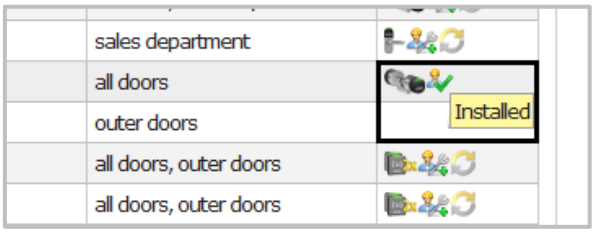


Figure 95: Door list - "Installed" status

17.5 Removing Xesar access components

You have various options to remove a Xesar access component from your locking system, depending on the application. Please read the instructions carefully as incorrect operation may cause a failure of your Xesar access components.
The following section provides an overview of the various options.

Activate office mode for the Xesar access component, particularly on the Xesar cylinder, before starting disassembly.

Overview:

Undoing assembly

Use this function if you have not yet initialised your Xesar access component with the Xesar tablet, but you would like to once again remove the component from the door.

Removing Xesar access components

Use this function if you have already initialised your Xesar access component and you would once again like to remove it from the locking system.

Do ***NOT*** **use the** Undo assembly function if you have already initialised the Xesar access component, but you have subsequently failed to synchronise the Xesar tablet with the Xesar software. Otherwise your Xesar access component will be rendered unusable and must be reset by EVVA.

Forcing disassembly

Use this function if you would like to remove a faulty Xesar access component from the Xesar software.

You will be unable to re-install a Xesar access component removed from the Xesar software using the ***Force disassembly*** function. The access component must be reset by EVVA.
Exclusively use this function if the Xesar access component is actually faulty.

17.6 Undoing assembly

If you would like to once again remove an uninitialised Xesar access component from the Xesar locking system, select the ***Undo assembly*** function.

Do ***NOT*** **use the** Undo assembly function if you have already initialised the Xesar access component, but you have subsequently failed to synchronise the Xesar tablet with the Xesar software. Otherwise your Xesar access component will be rendered unusable and must be reset by EVVA.

Proceed as follows:

- Select ***Doors & areas***.

- Click the ***door*** for which you would like to revoke installation.
- Click the Xesar access component icon in the ***Edit door*** application window. The ***Xesar access component*** application window opens.
- Click ***Undo assembly*** ❶ at the icon next to the Xesar access component.
- A security prompt appears. Click ***Undo*** ❷ to confirm.
- After having confirmed the prompt, this Xesar access component is automatically removed from your locking system and it will no longer be listed in the overview.

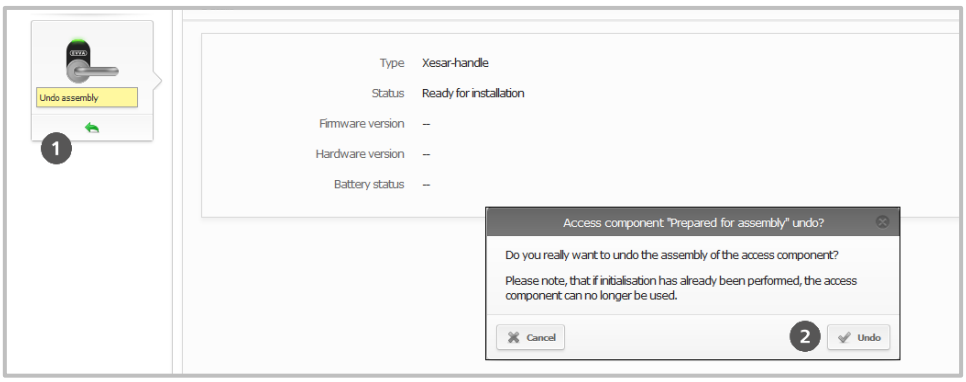


Figure 96: Undoing assembly

17.7 Removing Xesar access components

Proceed as per the three steps described below to remove a Xesar access component from the locking system if the access component has already been initialised.

Please note that this requires procedures in the software and the Xesar access component.

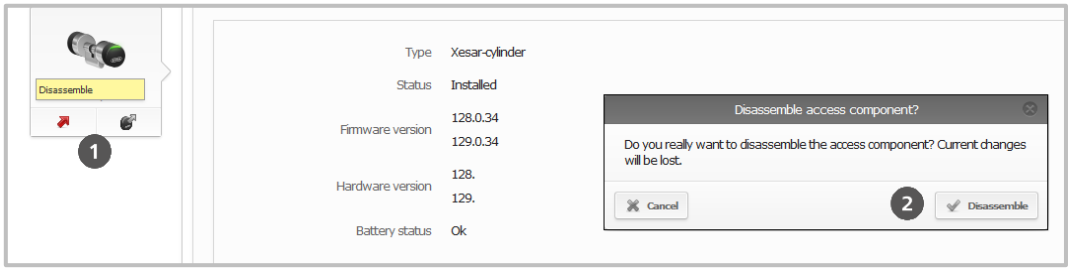


Figure 97: Removing Xesar access components

17.7.1 Removing Xesar access components from the Xesar software — step 1

Proceed as follows to remove the access component from the Xesar locking system using your Xesar software (Figure 97: Removing Xesar access components):

- Click the ***Doors & areas*** menu item.
- Select the door from which you would like to remove the Xesar access component and click it.
- Click the Xesar access component icon and click ***Disassemble*** ❶. Click the ***Disassemble*** field ❷ to confirm the security prompt.
- Subsequently synchronise your ***Xesar tablet*** with your Xesar software to transfer the data on disassembly of the Xesar access component.

17.7.2 Disassembling Xesar access components

After having removed the Xesar access component from the locking system of your Xesar software, you can disassemble your Xesar access component from the corresponding door and (if applicable) assemble it in a different door.

17.7.3 Synchronising the Xesar tablet with Xesar access components — step 2

Use the Xesar tablet to run the ***Disassemble access component*** task at the Xesar access component. Proceed as follows (Figure 98: Xesar tablet — removing Xesar access components):

- Connect your Xesar tablet with the affected Xesar access component.
- Start the Xesar application on your Xesar tablet.
- Select the affected door by opening the ***All tasks*** or ***Maintenance tasks*** menu.
- Select the ***Execute*** field of the ***Remove Xesar access component*** task (the Xesar access component will now be electronically removed from your system).
- The Xesar tablet shows a confirmation after having completely removed the Xesar access component.

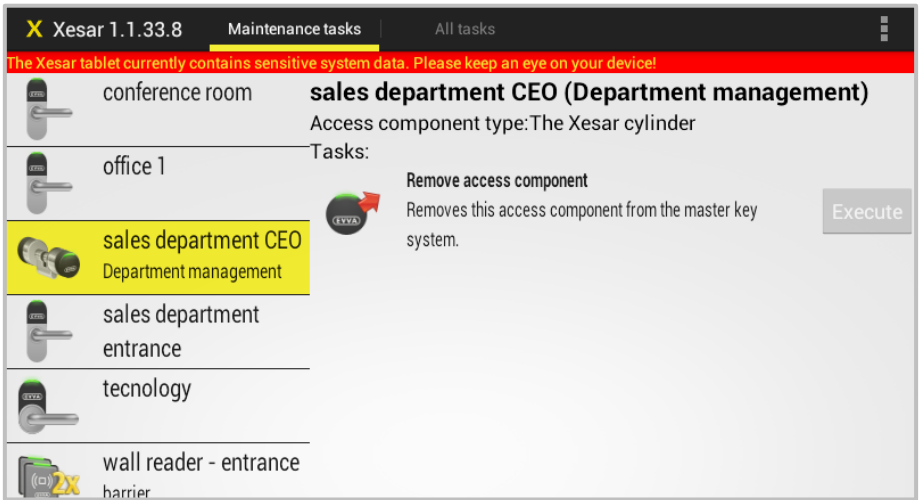


Figure 98: Xesar tablet — removing Xesar access components

If the data is transferred correctly, the Xesar application on your Xesar tablet shows a message (Figure 99: Xesar tablet — successfully removing Xesar access components).

The corresponding entries in the door list are updated once you have synchronised the Xesar tablet with the Xesar software.

Figure 99: Xesar tablet — successfully removing Xesar access components

The Xesar access component is returned to construction mode and can exclusively be operated using the Construction Card suitable for this mode.

17.7.4 Re-synchronisations with the Xesar software – step 3

After the maintenance tasks you must synchronise the information of the Xesar tablet with the Xesar software to update your Xesar software (Figure 100: Door list after having removed the Xesar access component):

- Connect the Xesar tablet to your Xesar software.

- Click ***Synchronise Xesar tablet*** in the Xesar software.
- Check the status in the door list – the Xesar access components have been removed.

17.7.5 Disassembling Xesar access components

After having removed the Xesar access component from the locking system of your Xesar software, you can disassemble your Xesar access component from the corresponding door and (if applicable) assemble it in a different door.

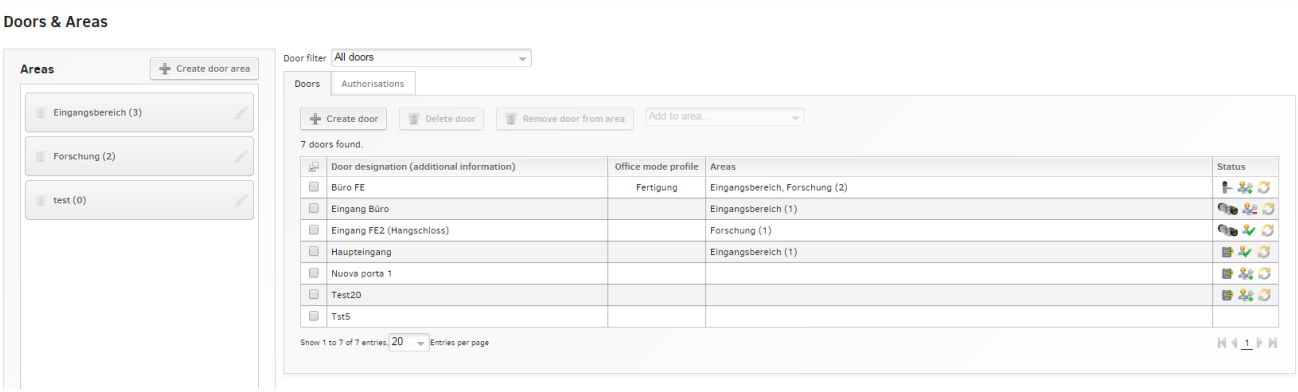


Figure 100: Door list after having removed the Xesar access component

17.7.6 Forcing disassembly

Use this function to remove a faulty Xesar access component from the locking system of your Xesar software.

You will be unable to re-install a Xesar access component removed from the Xesar software using the ***Force disassembly*** function. The access component must be reset by EVVA
Exclusively use this function if the Xesar access component is actually faulty.

Proceed as follows:

- Select ***Doors & areas***.
- Click the ***door*** from which you would like to ***force*** disassembly of the faulty Xesar access component.
- Click the Xesar access component icon in the ***Edit door*** application window. The ***Xesar access component*** application window opens.
- Click ***Undo assembly*** ❶ at the icon next to the Xesar access component. A security prompt appears. Click ***Undo*** ❷ to confirm.

All database records for this particular Xesar access component will be irrevocably deleted. You will then no longer be able to exchange data with the Xesar access component.

17.8 Replacing thumbturns

This function is available for Xesar cylinders only and gives you the option to replace a faulty or stolen thumbturn. As a result, the cylinder housing and all data and settings for this door within the locking system must not be replaced

You will be unable to re-install Xesar cylinder thumbturns removed from the Xesar software using the ***Replace thumbturn*** function. Exclusively use the function if the Xesar cylinder thumbturn is actually faulty or missing. Furthermore, please observe that an operational thumbturn (which has been reported faulty) continues to be configured with existing access authorisations and the corresponding identification media are still able to unlock it.

Position the new thumb turn and reset the component before you run the thumb turn replacement function with the new thumb turn.
This will assign a new "key" to the entire component and it is ideally prepared for thumb turn replacements.

Preparation (hardware):

Replace the faulty thumbturn with a new replacement thumbturn. In this process, proceed as described in the assembly manual. The assembly manual is enclosed with every cylinder. It is also available at any time at: http://www.evva.at/products/electronic-locking-systems-access-control/xesar/assembly-instructions-datasheets/en/

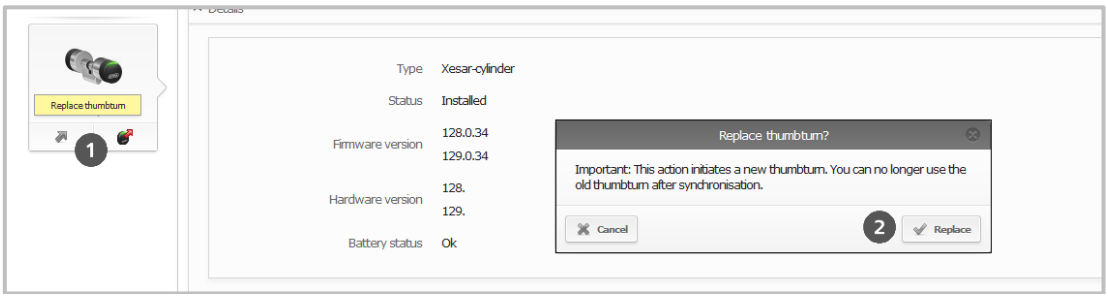


Figure 101: Replacing thumbturns

Proceed as follows (software):

(Figure 101: Replacing thumbturns)

- Open the ***Doors & areas*** menu item.
- Select the door from which you would like to remove the Xesar cylinder thumbturn and click it.
  Click the door to select it.
- Click the Xesar cylinder thumbturn and subsequently select ***Replace thumbturn***❶.
- Click the ***Replace*** field ❷ to confirm the security prompt.
- Subsequently synchronise your ***Xesar tablet*** with your Xesar software to transfer the data on replacement of the Xesar thumbturn.
- Proceed as described in sections
  Initialising Xesar access components — step 3A and ***Re-synchronisations with the Xesar software – step*** 4 to complete thumbturn replacement.

17.9 Automatic office mode (schedule-based)

Automatic office mode enables to automatically lock or unlock a Xesar access component at certain times. As a result, it will be possible to unlock access components without using identification media. You can define unlocked and locked periods using a schedule which is divided into weekdays and special days, identically to the schedules for persons.

- Click ***Office mode*** to open the screen in which you define the individual office mode times ❶ (**Fehler! Verweisquelle konnte nicht gefunden werden.**) for Xesar access components.

17.9.1 Configuring office mode

- Press❶ and hold the mouse button over the period for the desired weekdays
- or click an individual day to select it.

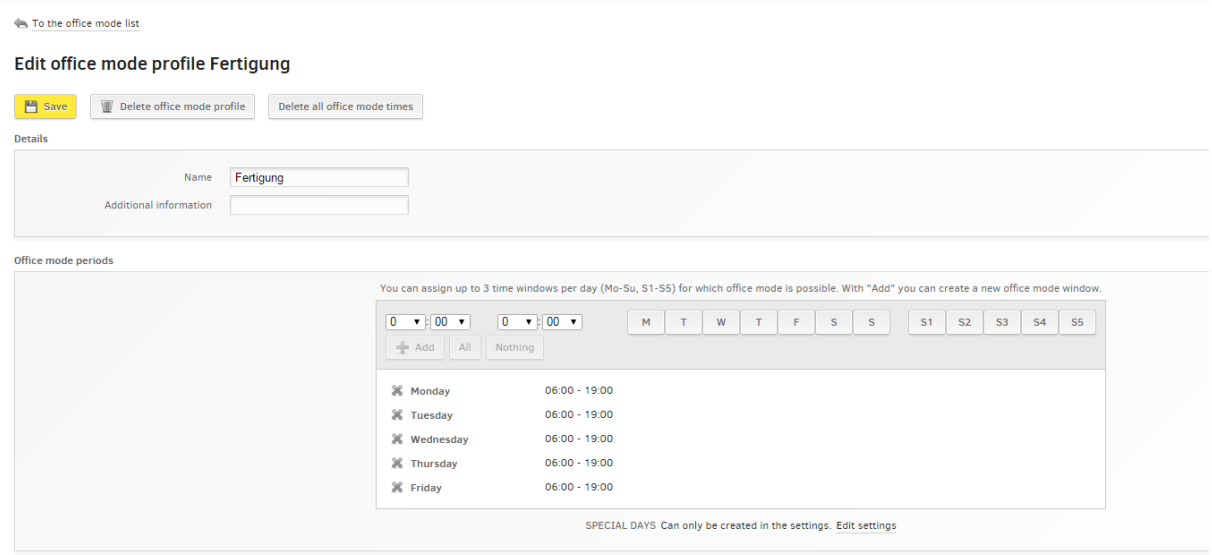


Figure 102: Changing the office mode period

The doors will be unlocked during the specified times for office mode and no identification media will be required for access.

17.9.2 Specifying the office mode period

- Click the desired day and select the desired start and end time for office mode on the corresponding day from the drop-down list (***from – to***) (**Fehler! Verweisquelle konnte nicht gefunden werden.**).

17.9.3 Deleting office mode

- Click to select the entry for the weekday you would like to delete

17.10 Release duration

The normal release duration is 5 seconds and the enhanced duration is 20 seconds. This is the factory setting. The release duration can be adjusted individually. The period ranges from 2 to 255 seconds.

The enhanced duration of release must be activated in the individual persons (See: ***Editing*** persons). Adjust the normal release time directly in the door settings. (See ***:Editing doors***).

17.11 Automatic lock profiles

This section manages all central, automatic lock profiles. Each central, automatic lock profile can be assigned to one or more doors. You can create a maximum of 30 central, automatic lock profiles.

They make sure that doors close at a defined time, even if they are affected by office mode.

Click ***Locking system > Automatic lock profiles***

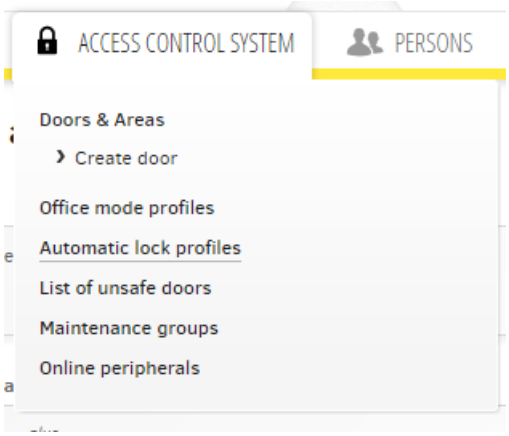


Figure :103 Lock profiles

Changing a central, automatic lock profile will affect all associated doors! It will only be possible to delete automatic lock profiles if they have not been assigned to a door.
You can specify a maximum of two times per day (Mon-Fri, S1-S5) at which manual office mode is suspended and the component once again safely locks.

Click ***Create lock profile***

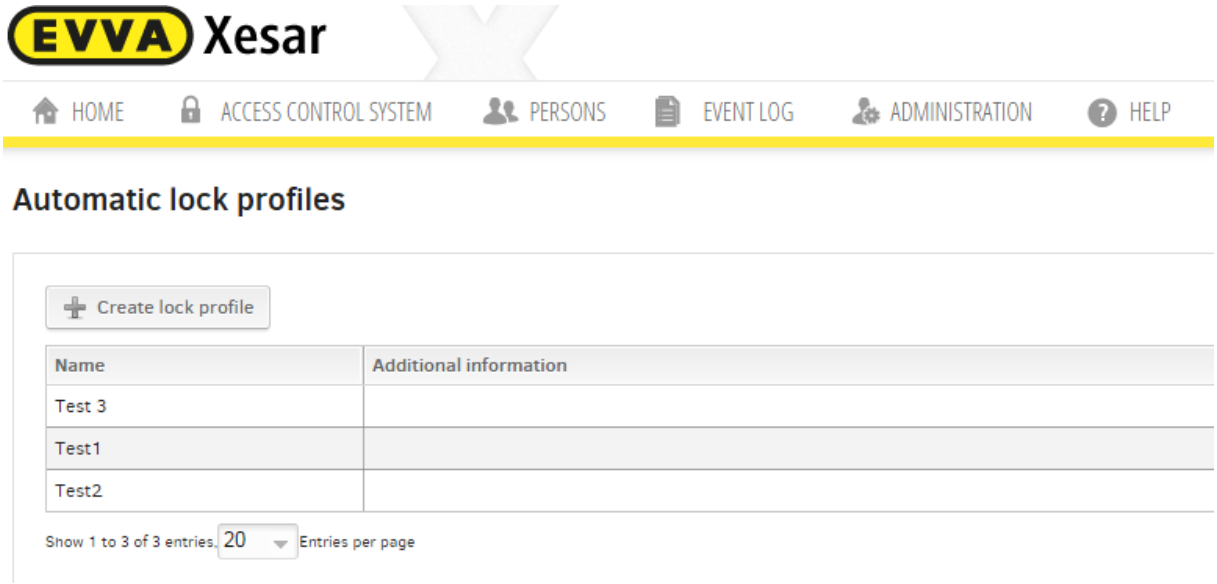


Figure 104: Automatic lock profiles

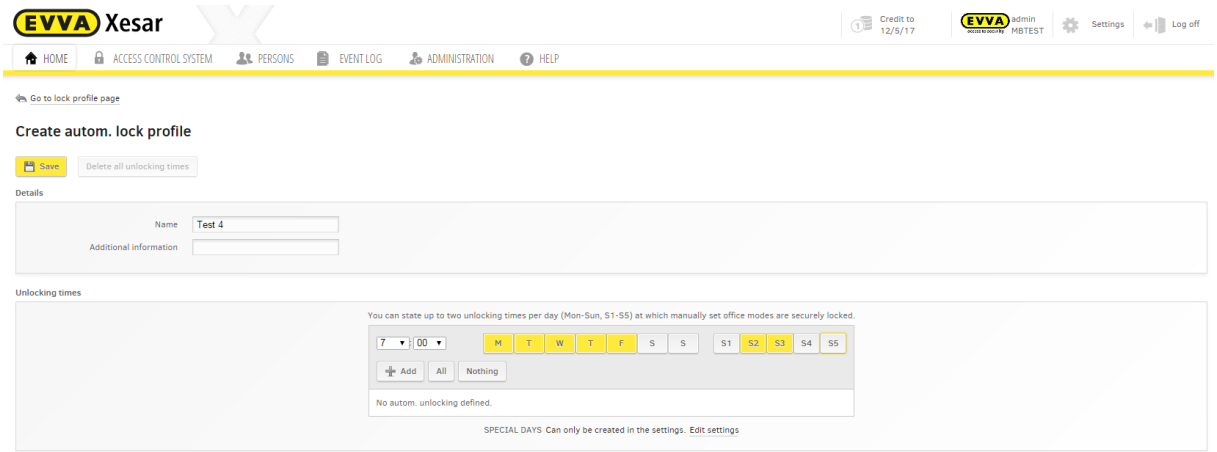


Figure 105: Automatic lock profiles 2

Now select a suitable time for your automatic lock profile, for instance in the evening, to make sure that all doors assigned to the lock profile are locked from this time onwards.

A lock profile is only active if **manual office mode** has been selected in the door details and a component has been selected in the door.

17.12 Assigning a central, automatic lock profile

The combination box shows all central, automatic lock profiles. Associated locking times are shown as information. Synchronise installed components after having changed the profile.

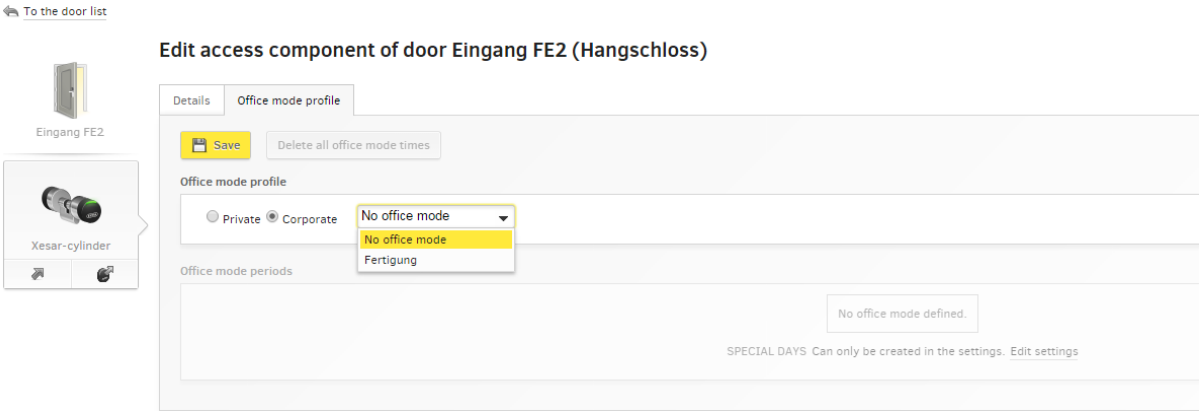


Figure 106: Central lock profiles

17.13 Private automatic lock profile

Private, automatic lock profiles are assigned to a specific door only. Synchronise installed components after having changed the private profile.

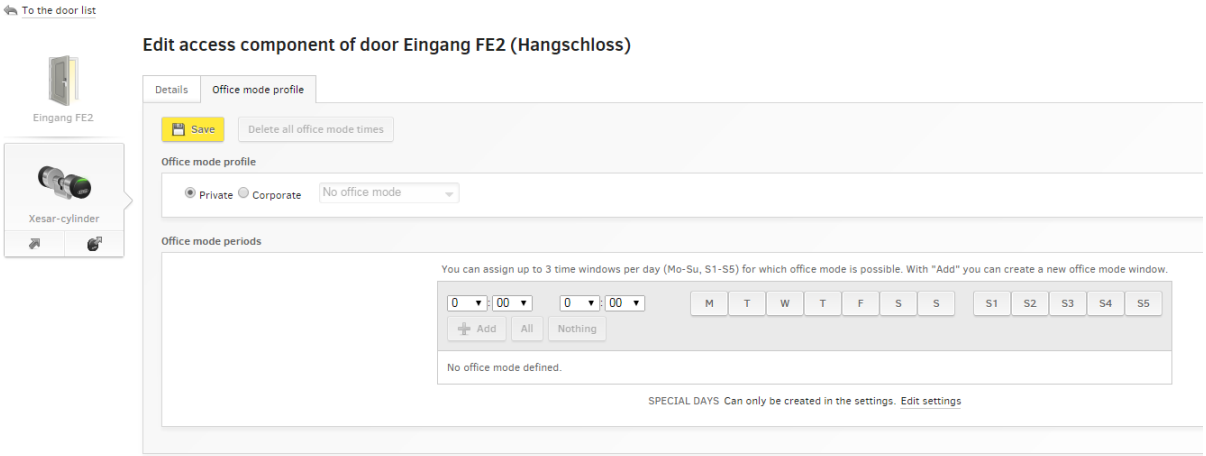


Figure 107: private lock profiles

17.14 Specifying special days

You also have five categories for special days. Special days enable to specify an exception from conventional calendar days. For example: Office mode has been set to every Monday from 8 am

to 5 pm except on public holidays. If you save the date of the public holiday as a special day, the door component will react differently (as specified) on the public holiday.

- Click ***Edit settings*** (Figure 109: Assigning special days) in the ***Time settings*** field to configure special days.

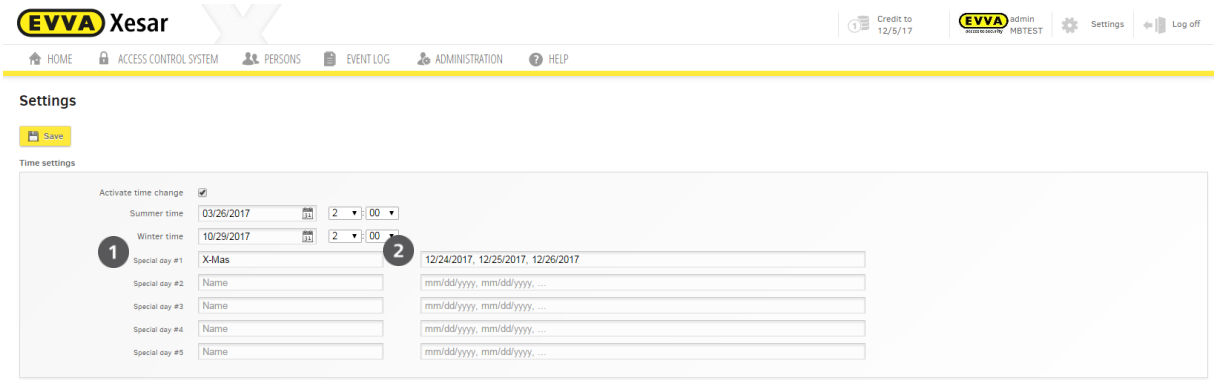


Figure 108: Configuring special days

- You can specify any designation for the special day. Enter the desired description in the corresponding field, in this case "Christmas" ❶ (Figure 108: Configuring special days).

In total, you can assign fifty days ❷ (Figure 108: Configuring special days), for instance you can assign fifty data records to a special day or five special days with ten data records each. Each date must be specified in DD.MM.YYYY format and several dates must be separated by a comma.

The start date (from) of special days ❶ must be before the end date (to).

17.14.1 Activating or deactivating special days

You can assign special days to ***access components*** and ***persons*** and in this process, they fulfil different functions.
Enter a date or several dates for a special day
(Figure 108: Configuring special days) to **activate** the special day function.

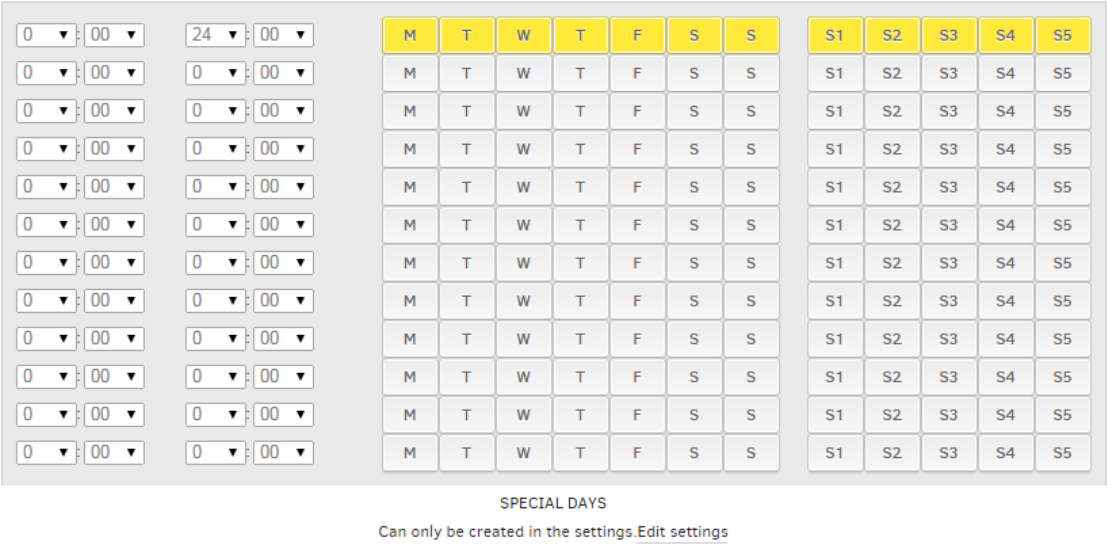


Figure 109: Assigning special days

17.14.2 How special days affect access components

In conjunction with Xesar ***access components***, special days can deactivate regular, time-based office modes or activate office mode, depending how the special day has been configured ❶. Special days take precedence over ***time-based*** or ***manual office modes*** and for this reason, any other **office modes** are bypassed on ***active special days*** and the special day configuration applies.

*Example **A:***

You have ticked the "Christmas" special day ❶ (Figure 109: Assigning special days) .

You can now specify the start and end date for office mode using the drop-down list. As a result, **automatic office mode** has been **activated** on the "Christmas" special days applicable as previously specified, from 24 December 2014 to 26 December 2014.

*Example **B:***

The "Christmas" special days ❶ (Figure 109: Assigning special days) are **not** ticked.

As a result, office mode on the previously specified days 24.12.2017 - 26.12.2017 (refer to Figure 108: Configuring special days) is **automatically deactivated** as you did not specify automatic office mode on the "Christmas" special days and special days take precedence over "normal" automatic office modes.

Automatic office mode then once again applies from 27 December 2017.

18 Persons

The ***Persons*** menu item allows to manage persons and identification media. It also provides an overview of the persons and identification media within your locking system.

Obtain an overview of the persons, media, time-based profiles and MasterKey authorisations within the locking system.

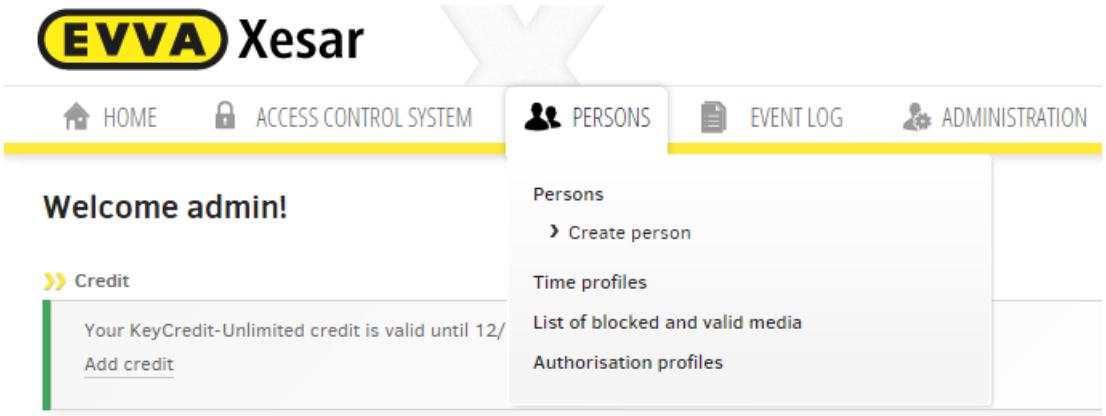


Figure 110: Persons tab

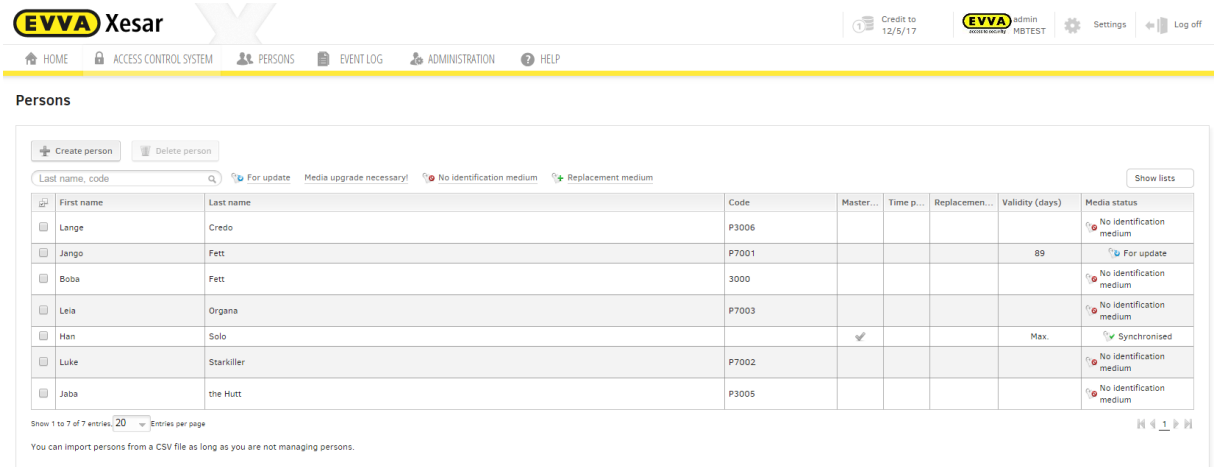


Figure 111: Persons list

18.1 Filtering entries

You have various functions available to filter entries. Click the corresponding field to select the following filters. You can activate several filters simultaneously.

For update ❶

Shows persons with expired Xesar identification media or persons who are required to update their media at Xesar coding stations following a change.

No Xesar identification medium ❷

Lists all persons for which no Xesar identification media have been issued.

Replacement medium ❸

Shows all persons that have been issued with a temporary replacement medium.

Show list ❹

Enables to differentiate between "***Active persons***" and "***Deleted persons***".

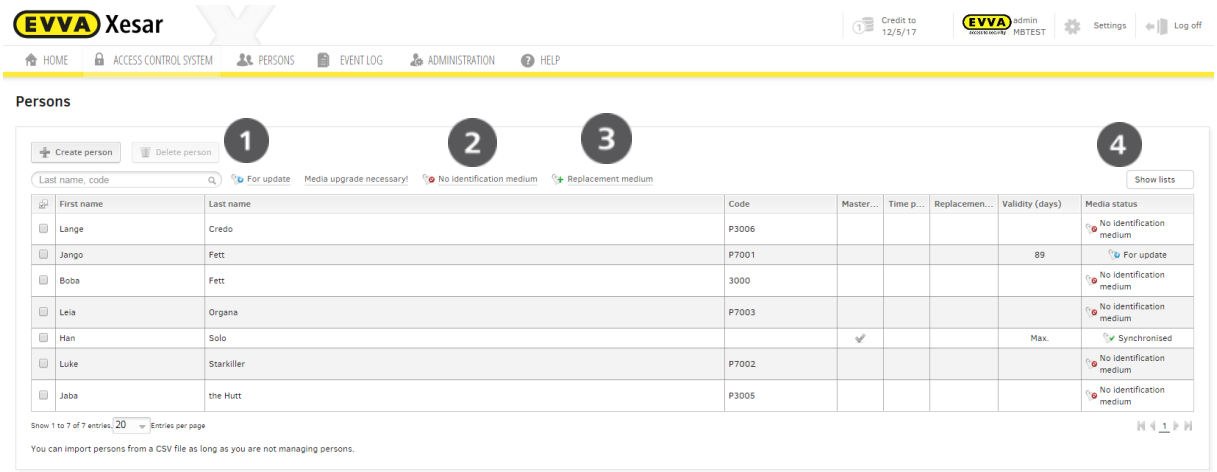


Figure 112: Unfiltered persons list

18.2 Creating persons

The ***Persons*** > ***Create person*** menu item enables you to conveniently create persons within your locking system.

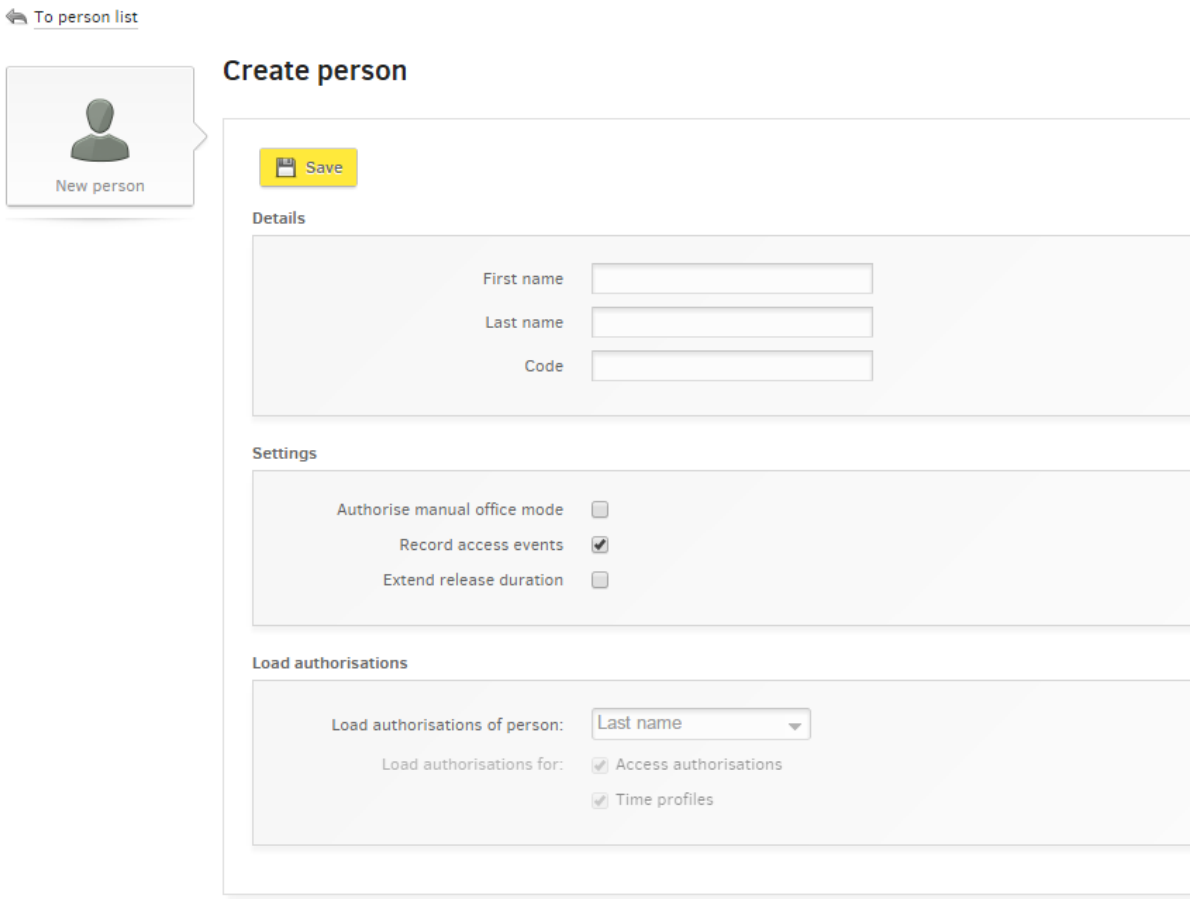


Figure 113: Creating persons

Within your Xesar locking system you can create each person only **once** in combination with **all three** criteria and for this reason, the entries must be **unique**.

Proceed as follows to create a person:

18.2.1 Details

- ***First name*** and ***Last name*** ❶ are mandatory fields
  The last name is the sorting criterion for the person list.
- ***Code*** Enter additional details, such as the staff number in this section.

18.2.2 Authorisations

The ***Settings*** section ❷ allows you to determine whether or not to enable the ***manual office mode*** function to the corresponding person.

18.2.3 Manual office mode

Click the ***On/Off*** field to specify whether or not the ***Manual office mode*** function is available to the corresponding person. Please note that this function must have also been enabled for the corresponding Xesar access component (see Section: ***Manual office*** mode***)***

18.2.4 Recording access events

Click the ***On/Off*** field, ***to specify*** whether or not to save access events (log data) of the corresponding person (please observe the locally applicable data protection regulations in the process).

18.2.5 Loading authorisations (transferring authorisations from another person)

The ***Load authorisations of person*** function ❸ enables to use existing access authorisations or time profiles of persons you have already saved.

Loading authorisations of persons
Select the person from the drop-down list whose authorisations you would like to use as a template.

Load authorisations for
Tick the box to select the authorisations to be used – ***access authorisations and/or time-based profiles***.

Save
Click the ***Save*** field to confirm the changes.

Authorisations
The application window automatically enhances after having clicked ***Save***. Proceed as described in the following section.

18.3 Importing persons from CSV files

You can use an existing CSV file to facilitate creating existing personal data in Xesar software.

The columns in the CSV file can be in any order.
When creating the CSV file, please note that the following fields can exclusively be imported: First name, Last name and Additional information.

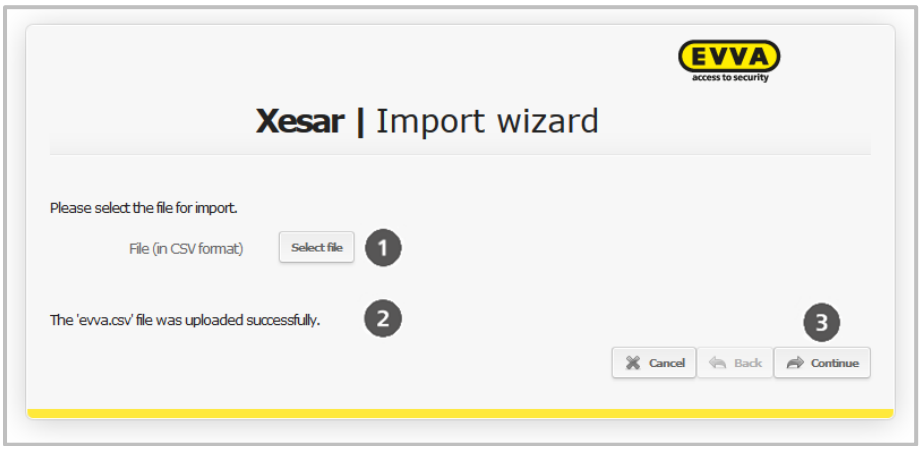
Proceed as follows to import an existing CSV file:

- Select the ***Persons*** > ***Persons*** menu item.
- Click the ***Import persons*** button ❶

Figure 114: Importing persons

This function is exclusively available if you have not yet created persons in the software. Any retrospective imports are available only after having deleted all existing personal data.

- Now click ***Select file*** ❶ to import your CSV file (



- Figure 115: Import wizard).

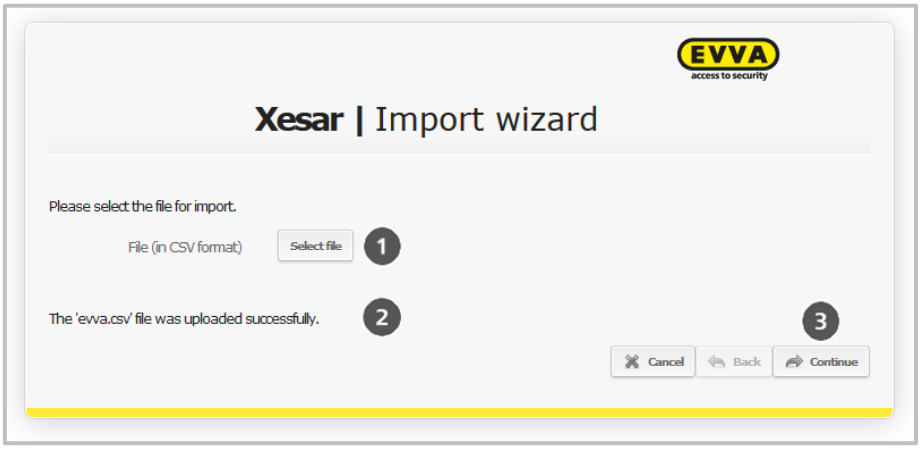
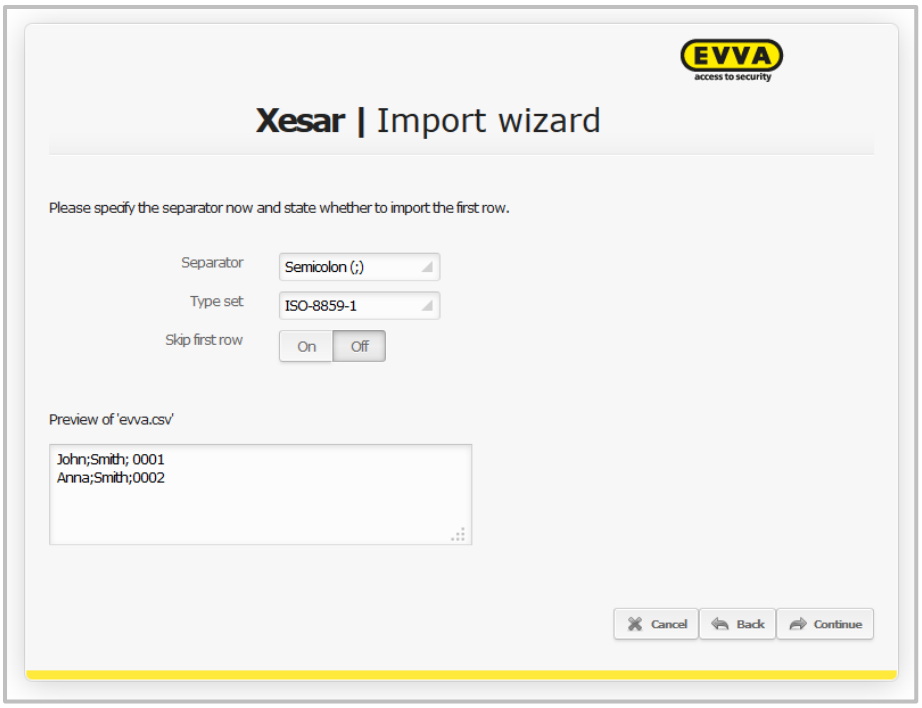


Figure 115: Import wizard

After having selected and successfully uploaded the file, the status message ❷ appears.

- Click ***Continue*** ❸ to open the Import wizard format settings (



- Figure 116: Import wizard — format).

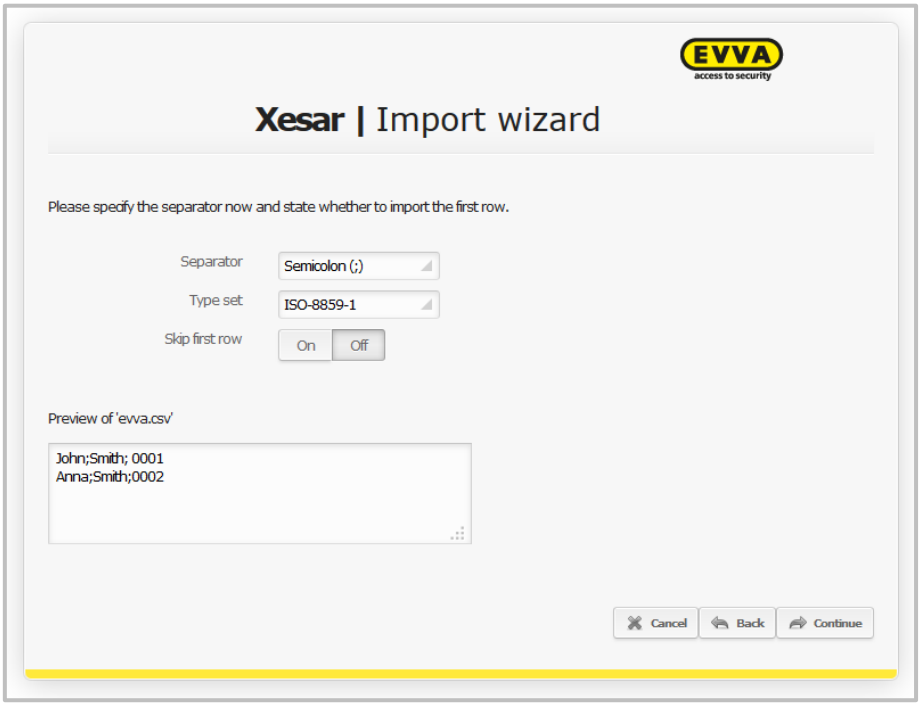
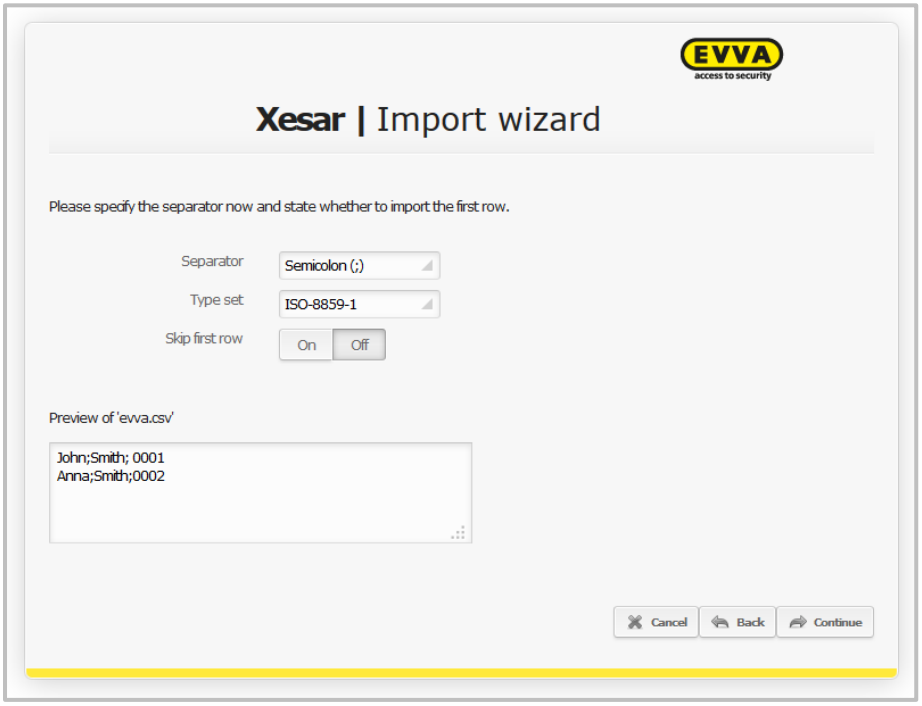


Figure 116: Import wizard — format

The first row of the CSV file can optionally be skipped as part of the import configuration.

- Select the desired ***separator/type set*** from the drop-down list to adapt the format – a preview of the imported persons will appear (



- Figure 116: Import wizard — format).
- Then click ***Continue.***

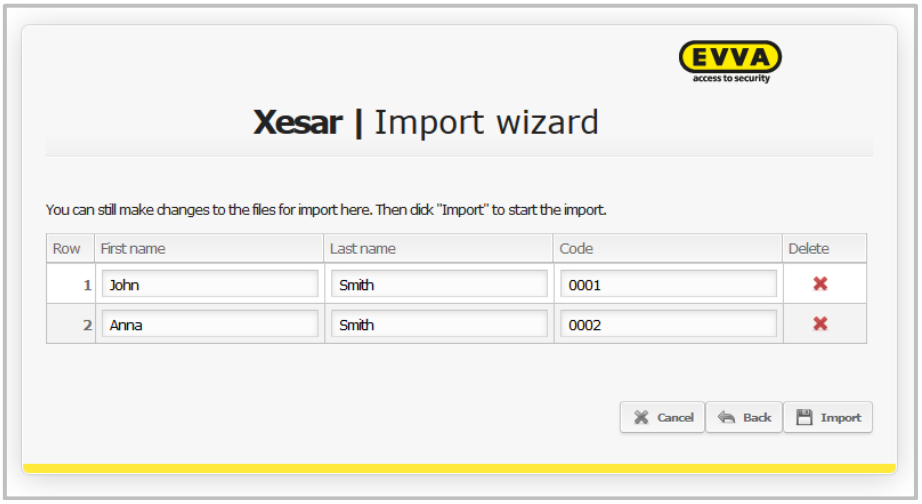
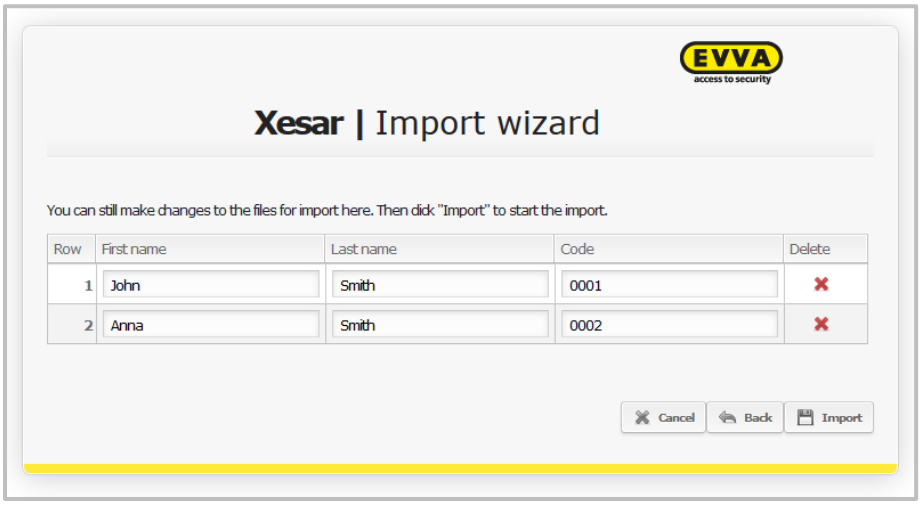


Figure 117: Import wizard — view

All persons for import are shown as part of the last step in the Import wizard.
In this section you can delete complete personal data records or change individual data.

- Then click ***Import*** to complete the CSV file import. (



- Figure 117: Import wizard — view).

18.4 Authorisations

The ***Authorisations*** application window enables you to configure authorisations.
If you use quantity credit, a notification appears after having assigned authorisations (saving your input). Click ***Save authorisation*** ❶ and one KeyCredit will be deducted from your account.

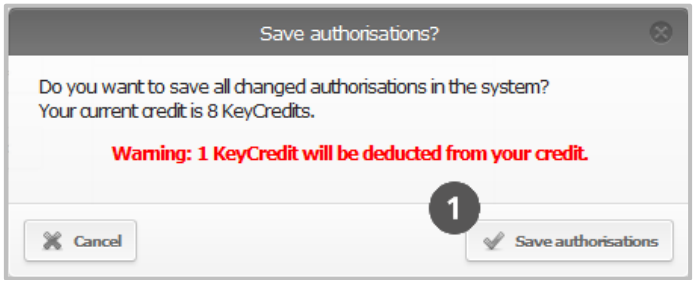


Figure 118: Saving authorisations

18.5 Editing authorisations

Open the ***Edit authorisations*** selection window to manage access authorisations and the time profile of selected persons.

- Click ***Authorisations*** ❶. The ***Edit authorisations*** application window opens.

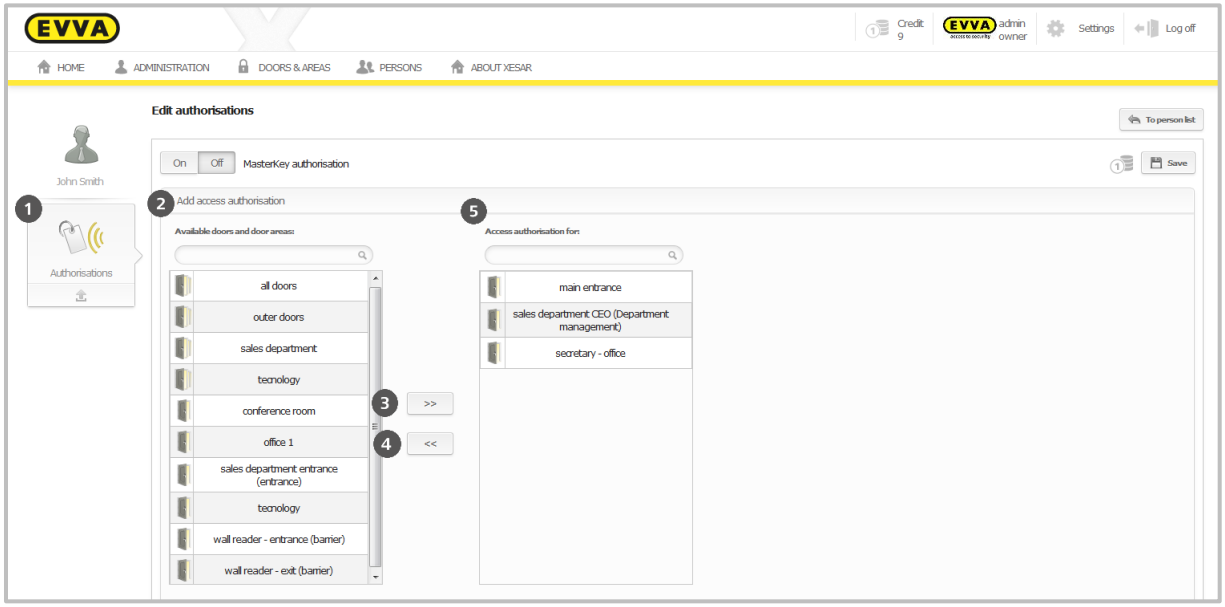


Figure 119: Editing authorisations

18.6 MasterKey authorisation

MasterKey authorisations are equivalent to a master key as they enable you to access your operational and initialised Xesar locking system **at any time**, regardless of any restrictions. One particular characteristic is that MasterKey authorisations also allow to unlock access components that were added to the system after having issued the identification medium. As a result there is no need to maintain media, such as an updated fire service medium.

It is not possible to issue replacement cards for persons that have been assigned MasterKey authorisations.

Three options are available to copy a guest medium:

- Guests with MasterKey cannot provide their media as source media.
- Copying a guest account with MasterKey will copy all elements except the MasterKey authorisation.
- If you would like to copy a guest with MasterKey, you must configure this separately to copy all the data including the MasterKey authorisation.

Adding **MasterKey authorisations**

The ***Edit authorisation*** field enables you to activate or deactivate the ***MasterKey authorisation*** by clicking the ***On/Off*** field (Figure 119: Editing authorisations)***.***

18.6.1 Adding access authorisations

- Click to select the applicable entries from ***Available doors and door areas*** ❷ in the overview list.
- Click the >> field ❸ to assign them to persons.
- To remove doors and door areas from the overview list ❺, you must highlight them and subsequently click the << field ❹ to remove them.

Access authorisations include all individual doors and entire door areas. Doors and door areas are shown simultaneously.

18.6.2 Time profiles

The ***Time profiles*** setting enables to assign an unrestricted time profile or a time-based profile to selected persons. Proceed as follows to specify ***Permanent access*** ❶ or personal ***Periodic access*** ❷:

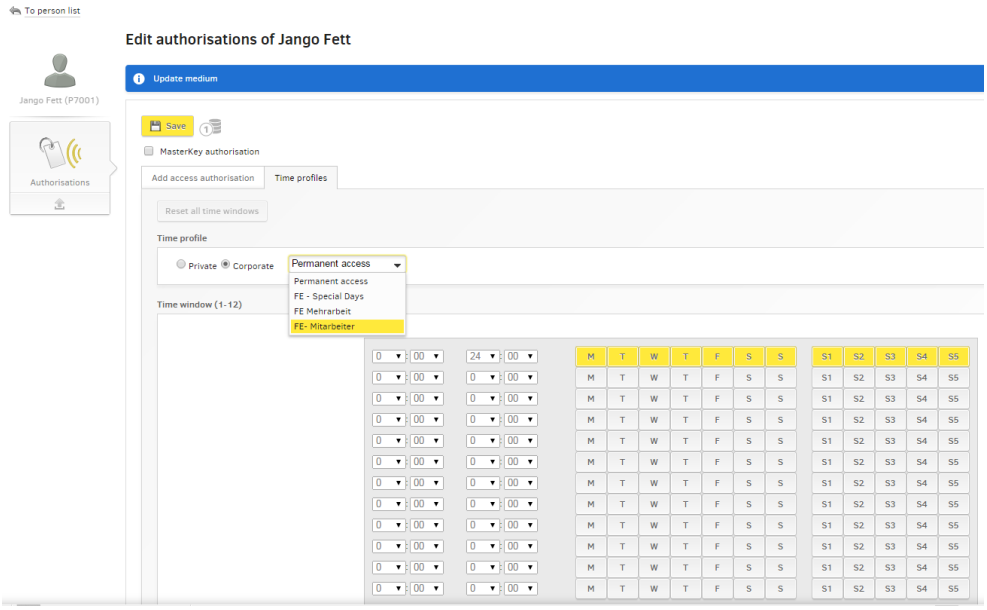


Figure 120: Time profiles

18.6.3 Several time profiles per user

You have the option to assign several time profiles to a single user.

For instance, you can assign a certain user's time profile for the main entrance and a different time profile for their personal office.

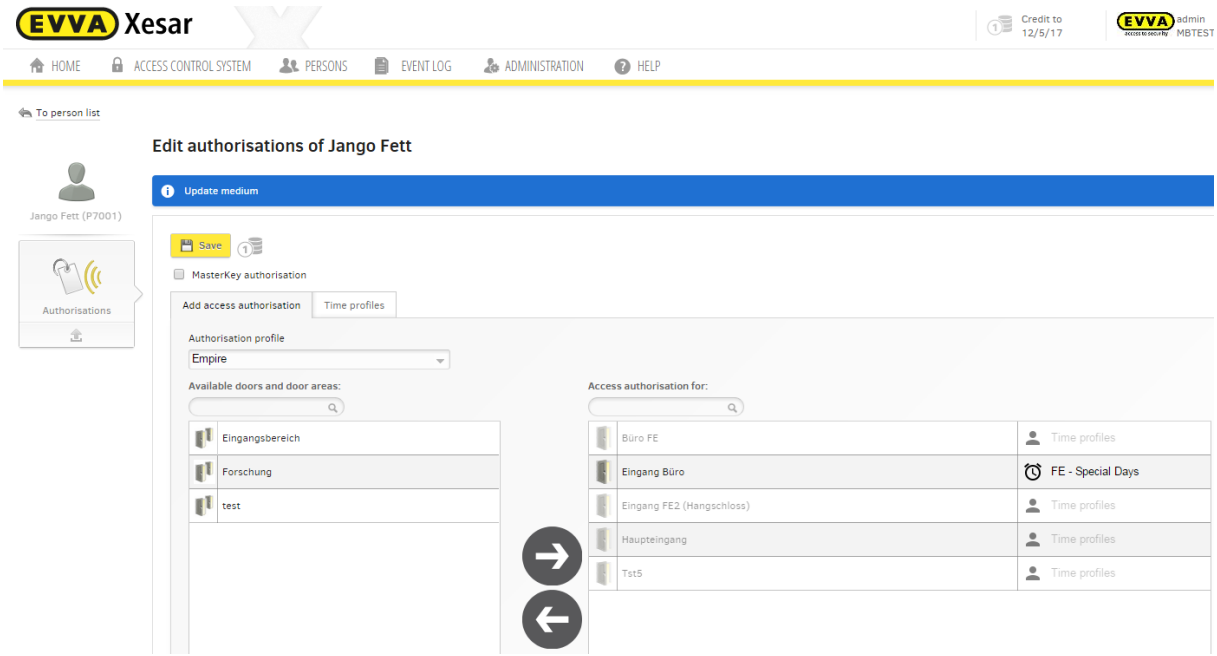


Figure 121: Time profiles

18.6.4 Permanent access (person)

- Activate the "Central" radio button in the application window and click Time-ba***sed profiles*** – ***Office mode*** to grant this person unrestricted access around the clock.

18.6.5 Periodic access (person)

- Activate the "Private" radio button in the application window and click Time-ba***sed profiles – Periodic access to*** grant this person restricted, time-based access.

18.6.6 Special days

In addition to selecting ***permanent access*** ❶ and personal ***periodic access*** ❷ the ***Special days*** function allows you to grant or revoke persons' access to your Xesar locking system on selected days.
For this purpose, please note the following section: ***Specifying special days***

Figure 122: Assigning special days

18.6.7 How special days affect periodic access authorisations

In conjunction with ***periodic access authorisations*** special days can deactivate access or, depending on the configuration of the special day ❶, activate temporary ***access authorisations***.
Special days take priority over periodic ***access authorisations*** and for this reason,
on **active special days** periodic ***access authorisations*** are bypassed
and the special day configuration applies.
Special days are already active once you have saved the specified date(s).

18.7 Editing persons

Click any person in the ***Persons*** menu item to open the ***Edit person*** menu (Figure 123: Editing persons).

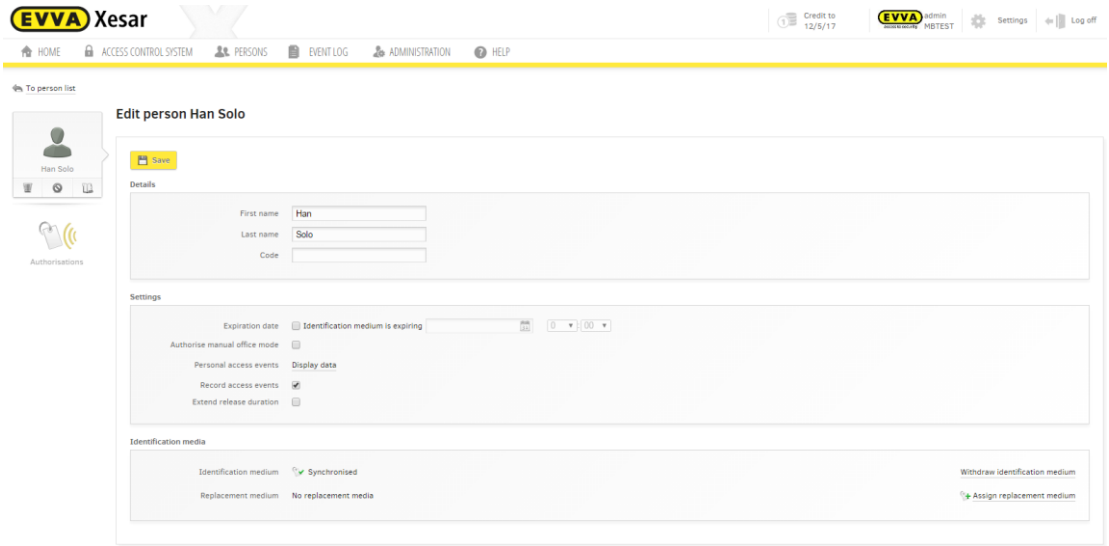


Figure 123: Editing persons

You can configure various changes and settings in the ***Details***, ***Settings*** and ***Identification media*** fields.

18.8 Details

- ***First name*** and ***Last name*** are mandatory fields
  The last name is also used as a sorting criterion for the person list.
- ***Code***. Enter additional information here, such as the staff number.

18.9 Settings

18.9.1 Expiration date

Specify the expiration date for a person's account in the ***Settings*** field. After expiration of said date the corresponding person will be unable to open any doors using their identification medium.

18.9.2 Manual office mode

Click this selection field to specify whether or not this person is authorised to use the ***manual office mode*** function. Refer to section ***Manual office*** mode)

18.9.3 Personal access events

Specify whether or not not record ***personal access events***.

19 Managing identification media

You can assign a Xesar identification medium to every person within your Xesar system using the Xesar software. You can issue a temporary replacement medium if a person has forgotten their identification medium. If persons lose their identification media, you can block the media in the software and issue a new identification medium.

19.1 Adding identification media to persons' accounts

After having created and saved authorisations for a person, you have the data available to create identification media.
Proceed as follows to create identification media for persons:
(Figure 124: Writing authorisations, new access medium):

- Place an empty identification medium on the Xesar coding station ❶.
- The following message appears: "***Access medium is not assigned to a person***".
  Click ***Write authorisations*** ❷.

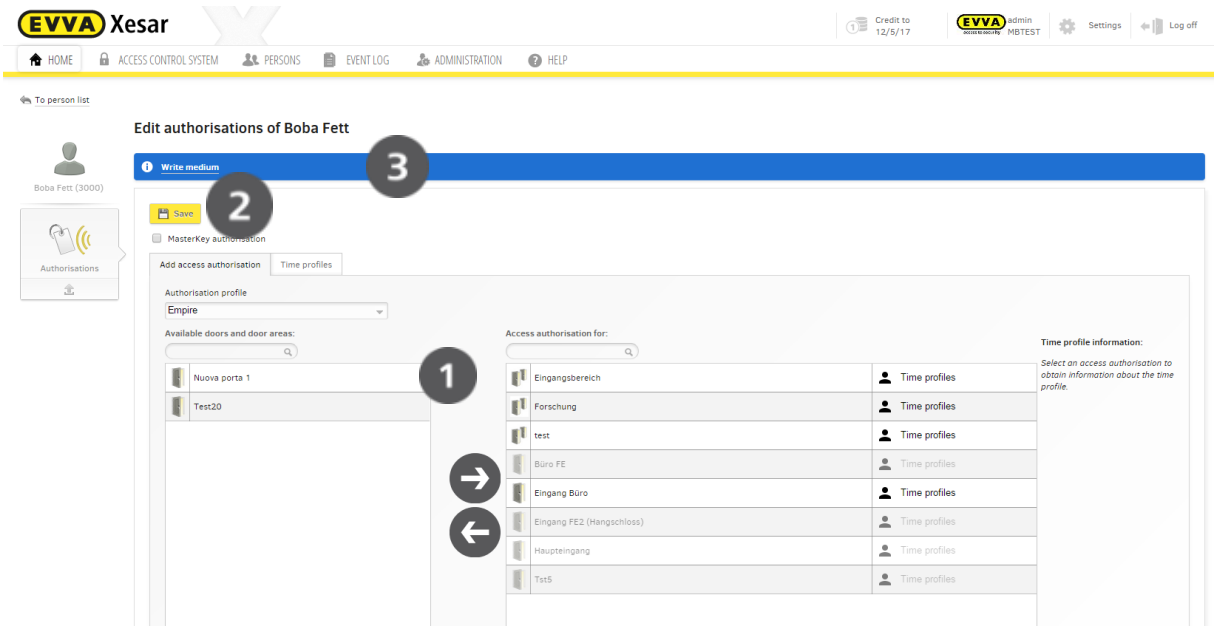


Figure 124: Writing authorisations, new access medium

The status line confirms having successfully completed the write process ❸ (Figure 125: Access medium created successfully). The Xesar identification medium is now ready for operation.

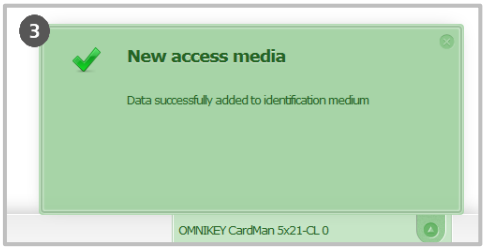


Figure 125: Access medium created successfully

Please note that if you make any changes to authorisations and click Save to confirm them, you will be deducted one KeyCredit from your account (not with KeyCredit Unlimited).

19.2 Withdrawing identification media

Withdrawing Xesar identification media means deleting the data and no longer being able to use the media at the previously authorised Xesar access components. You can withdraw Xesar identification media from any program window (pop-up).

Xesar replacement media are also Xesar identification media and for this reason, they can also be withdrawn.

Proceed as follows:

- Select the ***Persons*** menu item.
- Double-click the person whose Xesar identification medium you intend to withdraw.
- Place the Xesar identification medium on the coding station.
- Select ***Withdraw access medium*** ❶ (Figure 126: Withdrawing access media).
- After having withdrawn the identification medium, it can exclusively be used in this Xesar locking system and is shown as a ***New identification medium*** as soon as you once again position this very identification medium on the Xesar coding station.

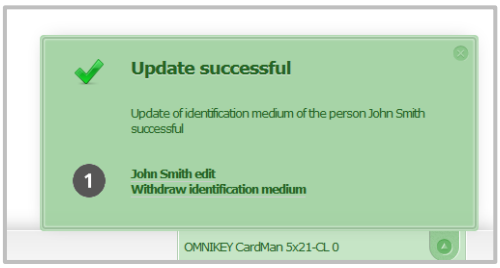


Figure 126: Withdrawing access media

If an identification medium due for deletion is "available" (i.e. not lost), we recommend you delete it using the ***Withdraw identification medium*** function as this immediately makes the medium invalid and does not create a blacklist entry.

19.3 Blocking persons

If an identification medium is no longer available, you can remove the identification medium from the Xesar locking system by blocking the person which has been assigned this particular identification medium. The block will withdraw all identification media from a person and put them on a blacklist. The blacklist is an automatically created list of all blocked identification media and it is automatically transferred upon synchronisation with Xesar access components.

If users hold a blocked identification medium to an active coding station or an updated Xesar access component, this identification medium is automatically deleted (from the system and the blacklist) and will be denied access to your locking system.

Blocked identification media attempting to unlock access components with an updated blacklist are also deactivated by the DeleteKey function.

The identification medium will only be fully transferred to your Xesar locking system once you have synchronised the affected Xesar access component with your up-to-date Xesar tablet.

If the Software*plus*-package is active, the current blacklist can also be distributed to the components by using identification medium

Proceed as follows to block a ***person*** (and thus an identification medium):
(Figure 127: Blocking Xesar identification media):

- Open the persons list.
- Select the ***person*** whose Xesar identification medium you would like to block.
- Click the ***Block person*** ❶ icon next to the selected person's icon.
- Click ***Block*** ❷ to confirm the security prompt.

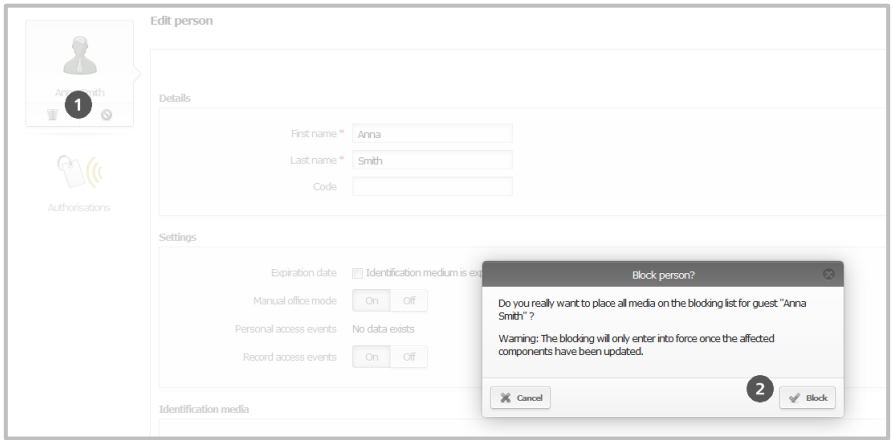


Figure 127: Blocking Xesar identification media

19.4 Deleting persons

Deleting persons is a very complex procedure that affects many areas
and for this reason, we would like to ask you to carefully read the following information.

- Any protocol entries of the deleted person will be rendered anonymous and remain available in the Xesar software of your locking system.

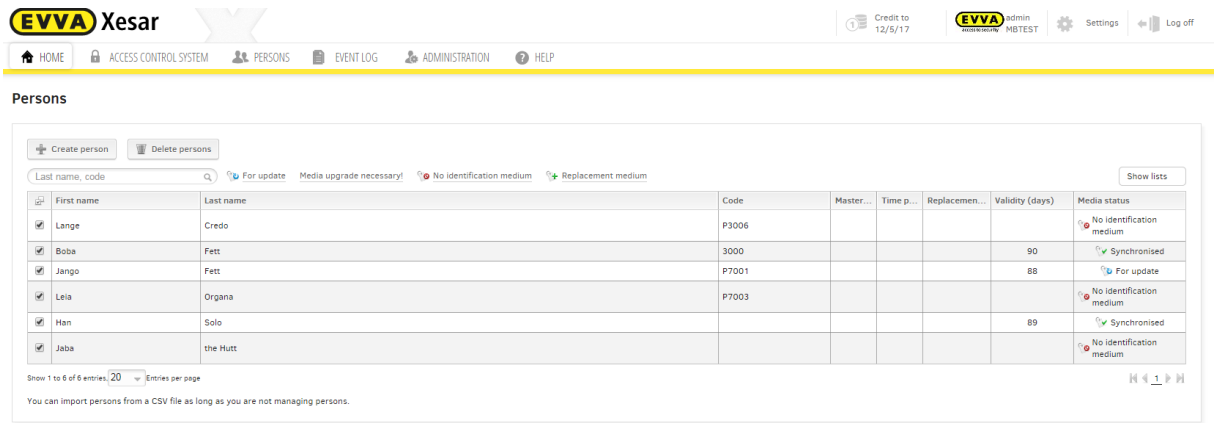


Figure 128: Filtered persons list

- You must delete the identification medium in the Xesar software before you can delete a person. Deleting persons also prepares this person's identification media for deletion.

- However, after having deleted the person you must update the identification medium at a Xesar coding station to complete the deletion procedure for the affected person's identification media.
- The deleted identification media will subsequently no longer be able to gain access.
- This deleted identification medium is now once again equivalent to a new identification medium. However, for security reasons, it can exclusively be used within the specific Xesar locking system from which it was deleted.

- Holding unauthorised identification media to Xesar access components within your Xesar locking system will trigger acoustic and visual signals to indicate access has been denied. Please refer to Section *Fehler! Verweisquelle konnte nicht gefunden werden.*.

Persons will remain in the system after having deleted them so you can continue to view their complete protocol entries.

Collect Xesar identification media or block access. If you block Xesar identification media, all information on the identification media will be deleted upon updating at a Xesar coding station. Personal entries remain saved in the database.

Proceed as follows to delete a person:

- Select ***Persons > Persons***.
- Tick the check box of the person(s) you would like to delete.
- Click ***Delete person***.
- Click ***Delete person*** to confirm the security prompt.

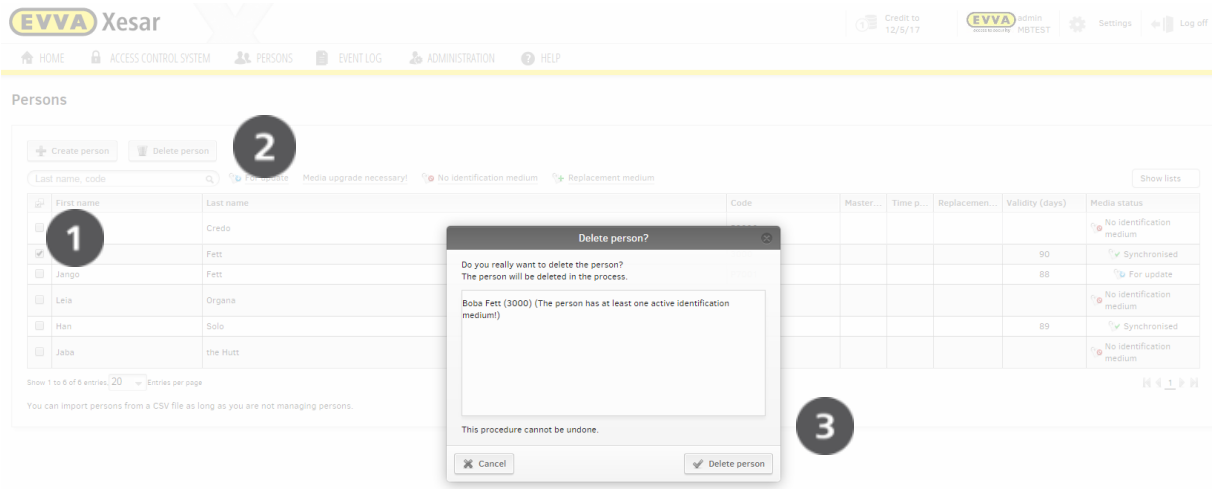


Figure 129: Deleting persons

If you have highlighted and deleted several persons and confirm ***Delete person*** this will apply to the entire selection.

19.5 Updating identification media

It is also required to update identification media after having changed authorisations. A corresponding notification appears in the identification media overview ❶ of the Xesar software dashboard.

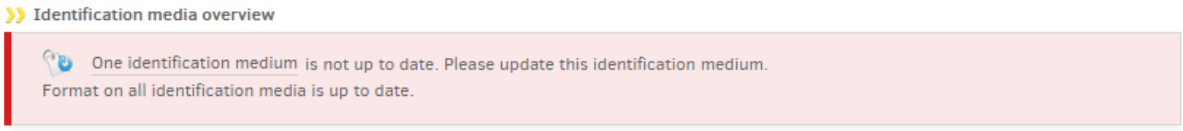


Figure 130: Home page with identification media overview

Click ***Update*** ❶.
A filtered persons list will appear, listing all identification media requiring an update because access authorisations were changed.

Identification media are automatically updated upon holding them to a Xesar coding station (regardless of the currently open menu). No interactions are required in the software.

You can view the list at any time. For this reason, select the desired filter in the "Persons" application window.

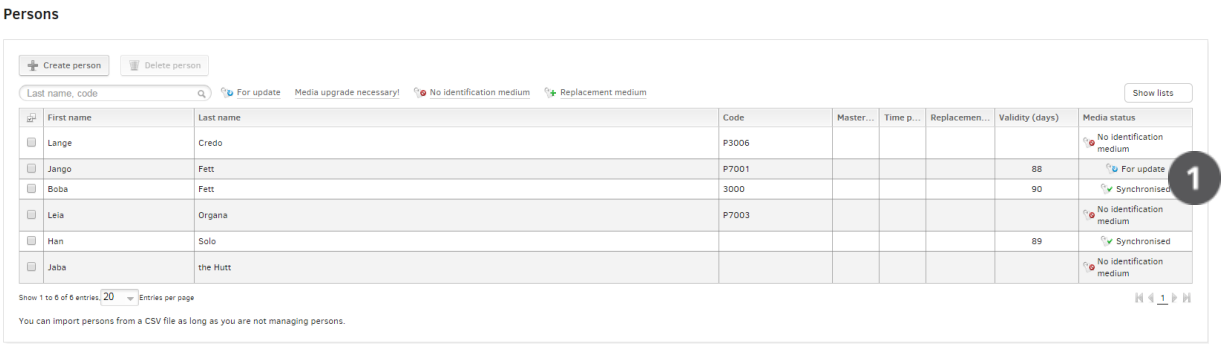


Figure 131: Persons list with Xesar identification media requiring an update

Any changes to access authorisations will only fully take effect once the affected identification media have been updated.

Updates and synchronisations are also possible if users are logged off from the system and an Admin Card has not been inserted into the Xesar coding station.

19.6 Assigning replacement media

You can issue replacement media to persons who are temporarily unable to access their personal identification media, e.g. because they left their Xesar identification medium at home.

Proceed as follows to issue replacement media (Figure 132: Assigning replacement media):

- Click ***Persons***.
- Select the person.
- Then click ***Assign replacement medium*** ❶.
- ***Save*** your changes.

You can specify the validity period of replacement media in the ***Settings*** (24h set by default, the maximum validity period is 72h).

You are unable to extend the validity period of replacement media by updating it using a Xesar coding station.

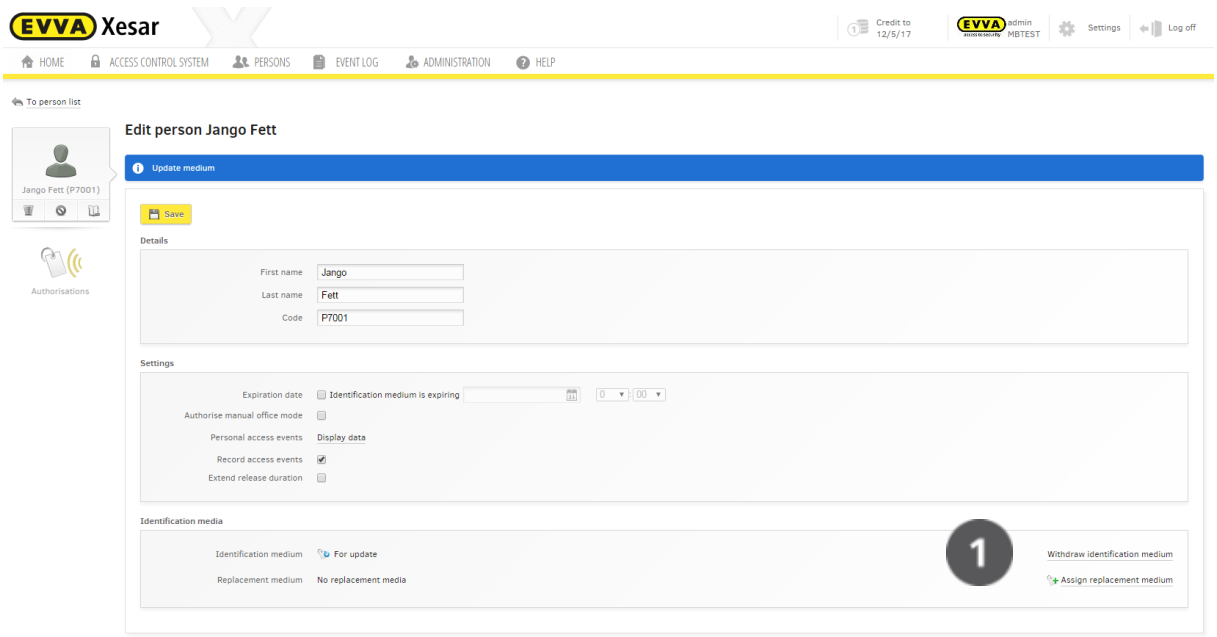


Figure 132: Assigning replacement media

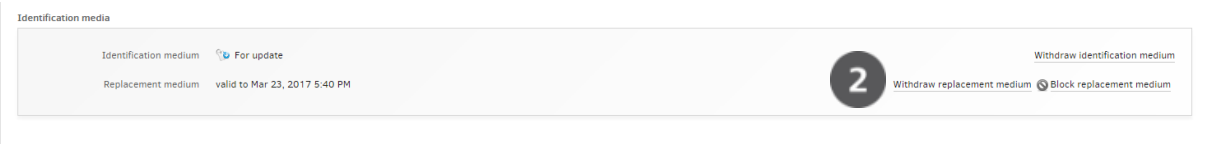


Figure 133: Assigning replacement media

20 About Xesar

The ***Help*** menu item provides information regarding the installed software version.

Figure 134: Xesar software version

21 Restoring databases

If you have activated the corresponding function, your Xesar software creates a backup in a location you specified upon closing the software.

Please note the backup must be for the same software version as your Xesar software.

Proceed as follows if you are forced to restore your system using a Xesar backup as a result of hard disk failure:

- Re-install your Xesar software, refer to (Installing the Xesar software).
- Insert the Admin Card for the locking system of your backup into the Xesar coding station.
- Enter the network path where you saved your database backup.
- Click Continue and follow the on-screen instructions until you have fully restored your Xesar locking system.

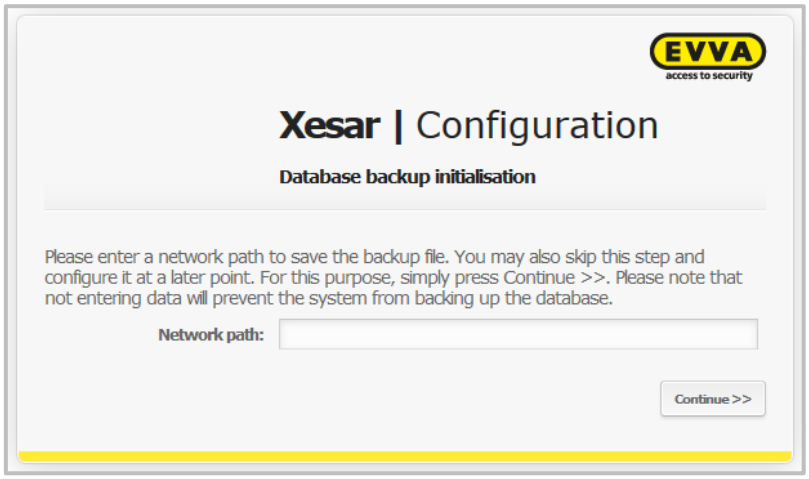


Figure: Database backup

Click the "Save" icon in the bottom left of the dashboard to manually back up databases at any time:

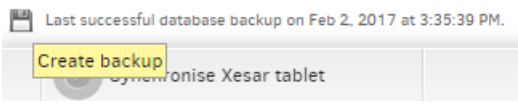


Figure 135: Creating backups

22 Replacing the Admin Card

Make sure you immediately replace any lost or faulty Admin Card. You must initialise the new Admin Card you received. For this purpose, proceed as follows.
For this purpose, please also refer to Section (***Credit*** schemes ***KeyCredit Card***)

- Insert your new Admin Card into the Xesar coding station.
- Start your Xesar software.
- Enter your system information in the Xesar | Configuration application window.
- Click ***Continue*** and the confirmation prompt to replace the Admin Card appears. Check the codes you entered and click ***Continue*** to confirm you input data correctly.

You will receive new access data for your Xesar software after having replaced the Admin Card. Print out the data, check the printout and only then click ***Finish*** to confirm. Take care when handling Xesar | Configuration access data and keep it in a secure location.

You must have added credit at minimum once to be able to replace the Admin Card.

- The system information of the old Admin Card is now no longer valid.
- The Xesar software login application window subsequently appears.
- Your new Admin Card is now ready for operation.

23 Uninstalling software

Reset all Xesar access components and Xesar identification media to construction mode (factory state) **before** you uninstall the Xesar software.

Note that uninstalling the software will delete any system-specific data.
Xesar access components that have not been removed from the locking system or active Xesar identification media will be rendered irrevocably unusable upon uninstalling the software**.**

Xesar identification media within the system are exclusively assigned to this system and it will not be possible to use them for another Xesar locking system after having reset.

Sequence for uninstalling

- Uninstall Xesar access components (Removing Xesar access components).
- Delete Xesar identification media.
- Uninstall the software.

Proceed as follows to uninstall the software:
Windows button ***Start > Control panel > Programs and Features***.
Select the Xesar program from the loaded list and click ***Uninstall*** ❶.

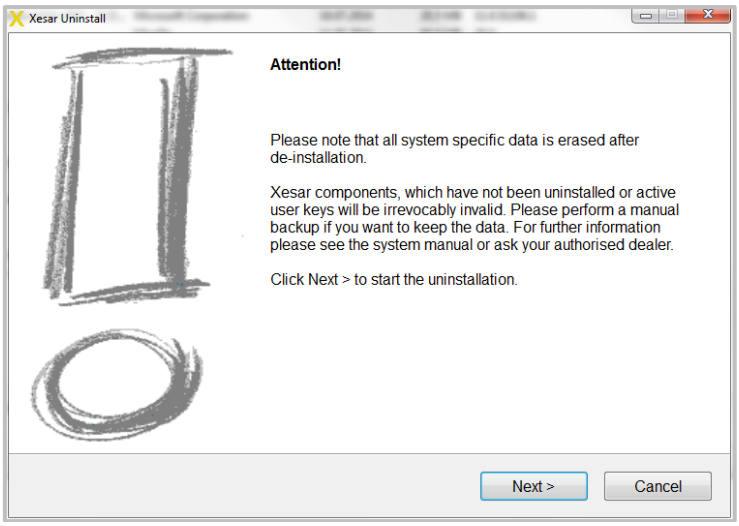


Figure 136: Attention

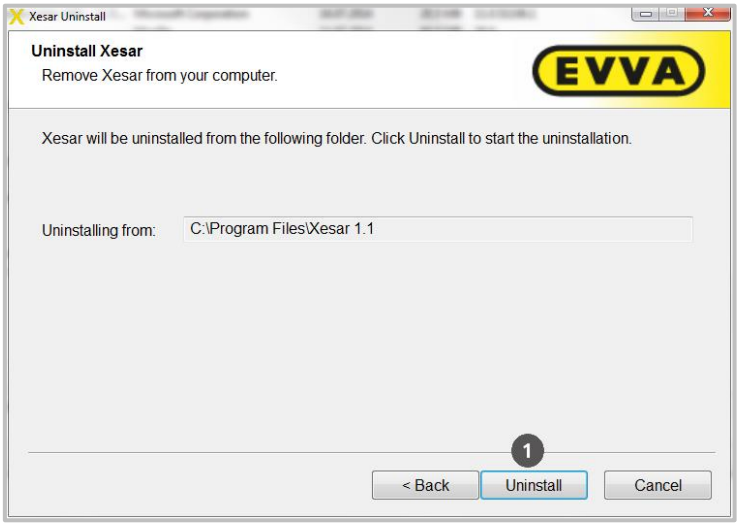


Figure 137: Uninstalling Xesar

The system now correctly uninstalls the software. Once the process is complete, click ***Continue*** to confirm, then click ***Finish.***

24 Software updates

We recommend you back up your database and save it externally prior to running software updates (e.g. on a USB pen drive). You can specify or change the network drive of the database backup by modifying it in the configuration settings (=> ***Configuration settings***). Uninstall the software if a re-installation is necessary (=> ***Uninstalling software***) and select the network path as part of the renewed, initial configuration (=>***Restoring databases***).

Please note: Before you start an update to Xesar Version 2.2, please restart your computer. Open background processes could be disturb a flawless update to Xesar Version 2.2

24.1 Instructions to update from Xesar 2.1 to Xesar 2.2

24.1.1 Technical background

Xesar 2.2 software is a completely new installation in parallel to the previous Xesar installation (1.1, 2.0, 2.1). If an AdminCard that is already in use is connected upon starting X2.2, the system demands a database.
In this process, it is necessary to state the original database of the previous Xesar installation – not the backup!
This database is then updated, registered in the X2.2 software and available by inserting the corresponding AdminCard.
The former aessdb.h2.db database is changed as part of the import process, renamed and rendered unusable following this process.

24.1.2 Procedure for a database (by reimporting the DB backup)

We are assuming the system is managed. There must not be ***any due maintenance task within the system***. The associated tablet must be "empty".

Preparatory tasks:

- Synchronise the tablet with the existing software.
- Complete all maintenance tasks
- Once again synchronise the tablet with the software.
- Close the software

- Restart the Computer
- Installing the Xesar 2.2 software
- Insert the AdminCard associated with the system upon starting X2.2SW for the very first time.
- Enter the database file on request, state database in the following location: C:₩ProgramData₩Xesar 2.1₩aessdb.h2.db.
- Importing
- Only now connect and synchronise the tablet (and consequently update the Xesar app, see also below: tablet update from 2.1 to 2.2)
- Now update the firmware of all components within the system to the most recent version (process remains identical). Also update all components in construction mode (e.g. replacement components in stock) to the most recent firmware.
- In a final step, uninstall the outdated software (version 1.1, 2.0 or 2.1).

25 Synchronising the Xesar software with access components

The Xesar tablet is required to transfer information between Xesar software and Xesar access components, for instance to add new access components to a Xesar locking system, to obtain the battery status or protocol data or to run firmware updates.

You must initially transfer the most recent data (e.g. blacklists, firmware updates, new key data, etc.) from your Xesar software to the Xesar tablet to be able to update your Xesar access components. Maintenance tasks are automatically transferred to the Xesar tablet upon synchronising it with your Xesar software.
You can subsequently initialise and synchronise Xesar access components.

After having synchronised with Xesar access components you must once again synchronise the Xesar tablet with the Xesar software to have the most recent information (access events, battery status, etc.) for Xesar access components available.

Figure 138: Xesar tablet

25.1 Starting the application (tablet)

Click the Xesar icon to start the Xesar application. (Figure 139: Xesar tablet – home screen). If the Xesar icon is not available on the start screen, open the ***APPS*** menu item on your tablet and select the Xesar icon in this section to start the app.

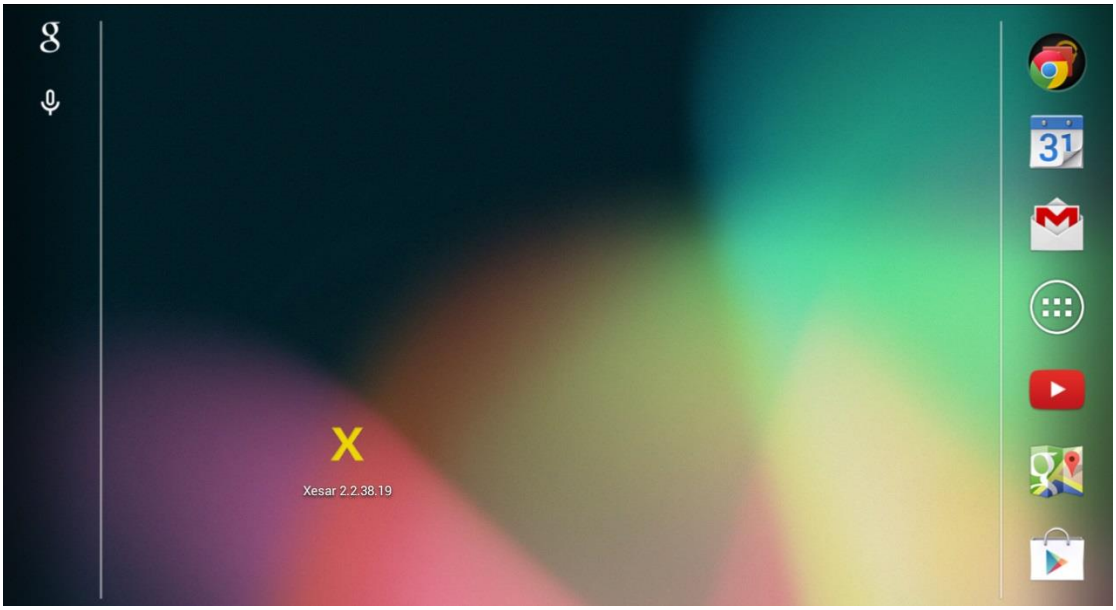


Figure 139: Xesar tablet – home screen

25.1.1 Synchronising the Xesar software with the Xesar tablet

Proceed as follows to synchronise components (*Figure 140: Synchronising the* Xesar software):

- Connect the Xesar tablet to the PC where you installed your Xesar software. For this purpose, use the enclosed USB cable
- Click ***Synchronise Xesar tablet*** in your Xesar software.
- All unresolved maintenance tasks are listed on the Xesar tablet.

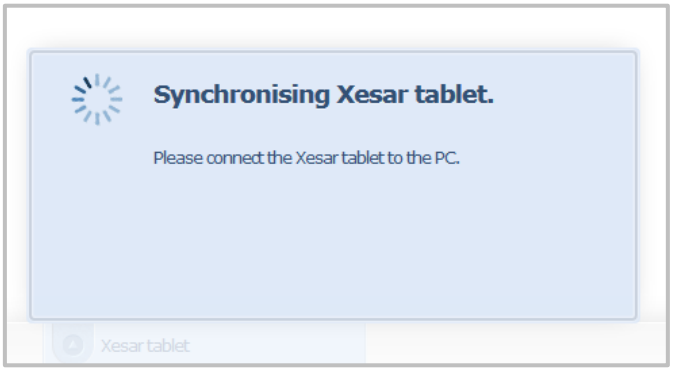


Figure 140: Synchronising the Xesar software

A notification in the Xesar software appears following successful synchronisation (Figure 141: Xesar tablet synchronised successfully). If your Xesar application is open now, a notification window will also appear (Figure 142: Xesar tablet — maintenance tasks, updated door data).

Figure 141: Xesar tablet synchronised successfully

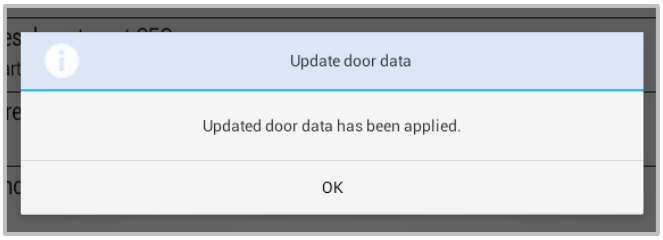


Figure 142: Xesar tablet — maintenance tasks, updated door data

25.2 All tasks

The ***All tasks*** section lists Xesar access component maintenance tasks relevant to security and also tasks to synchronise data collected for the purpose of information, such as battery states or personal protocols (Figure 143: Xesar tablet — all tasks).

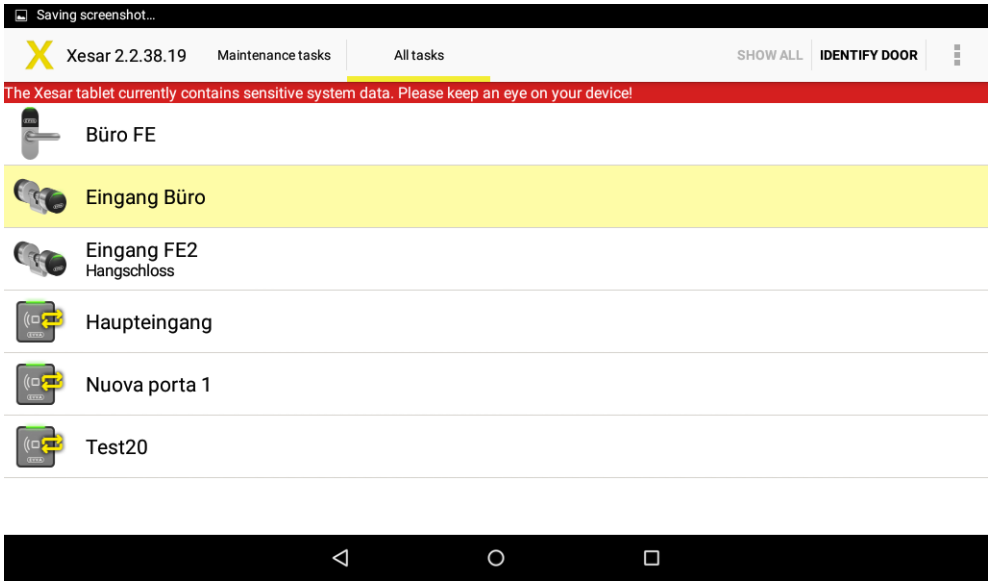


Figure 143: Xesar tablet — all tasks

25.3 Maintenance tasks

Maintenance tasks are defined as tasks relating to contents which are relevant to security, such as initialisation data for Xesar access components, blacklist updates, configuration changes, changes to special days, changes to automatic office mode, etc.

Make sure you complete maintenance tasks immediately to keep your Xesar locking system up to date.

For this reason, you can separately list maintenance tasks (Figure 144: Xesar tablet — due maintenance tasks).

- Select ***Maintenance tasks***.

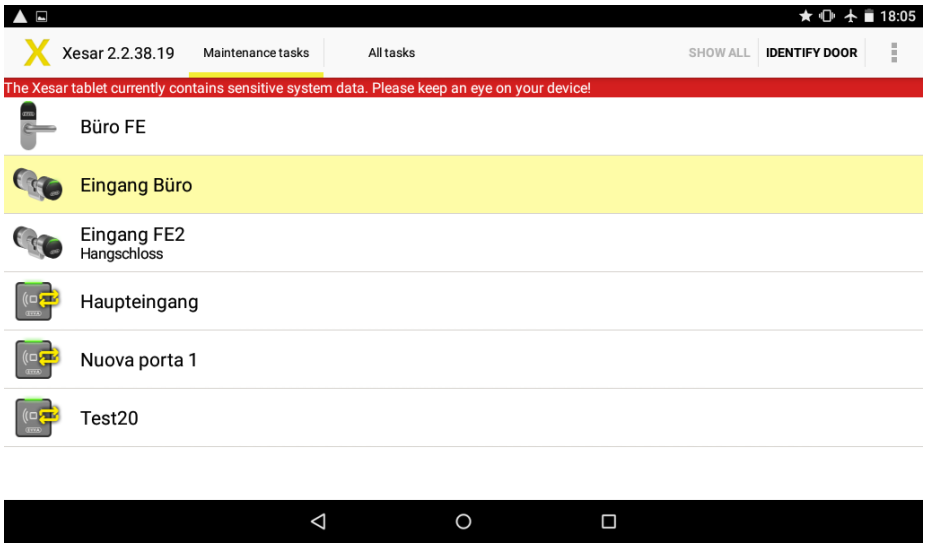


Figure 144: Xesar tablet — due maintenance tasks

The Xesar tablet indicates your device features sensitive system data (initialisation data). Make sure you do not lose your Xesar tablet during this time.

Proceed as described in Section ***Synchronising the*** Xesar software to transfer maintenance tasks to your Xesar tablet.
You can subsequently proceed as described below for all tasks and maintenance tasks.

- Select ***Maintenance tasks*** or ***All tasks***.

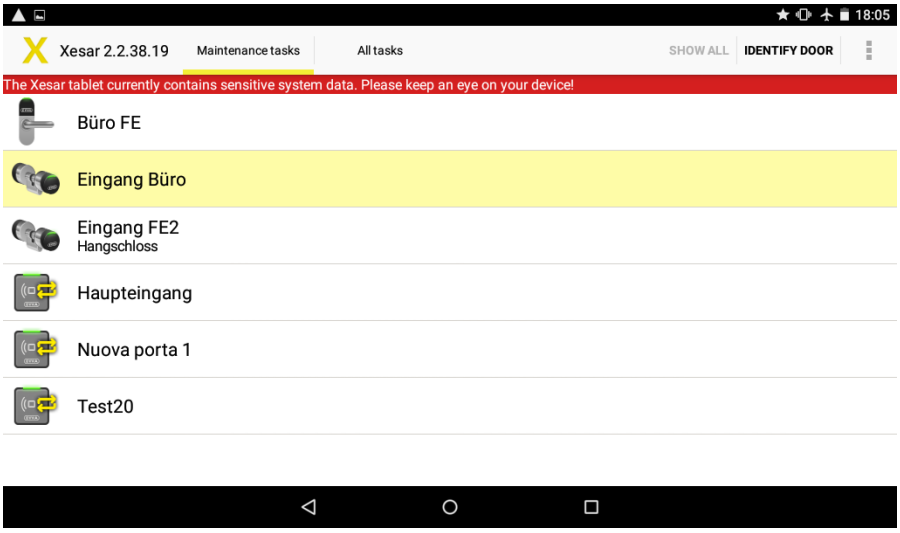


Figure 145: Xesar tablet — selecting Xesar access components

- Select the correct Xesar access component and the desired task you would like to run (Figure 146: Xesar tablet — initialising Xesar access components) from the maintenance task list on the Xesar tablet.

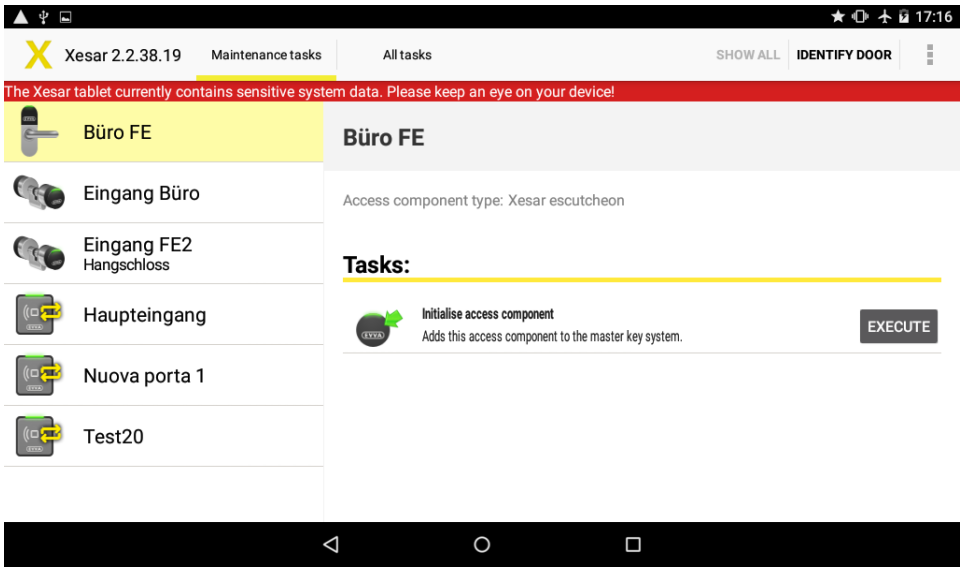


Figure 146: Xesar tablet — initialising Xesar access components

- Now go to your selected Xesar access component.
- Open the EVVA cover on the Xesar access component. For this purpose, use your finger to slightly press the flap to the left of the letter E towards the inside and subsequently pull the cover carefully towards the outside to the right of the letter A.
- Connect the Xesar tablet to the Xesar access component using the Xesar connection cable.
- Select ***Execute*** in the Xesar application.
- You are prompted to enter your ***initialisation PIN***.
- Enter the ***4-digit code***.

For reasons of security, an additional initialisation PIN is required for the ***Initialise*** and ***Replace thumbturn*** maintenance tasks. The initialisation PIN is the code you specified in the Xesar software in ***Settings > Security settings***.

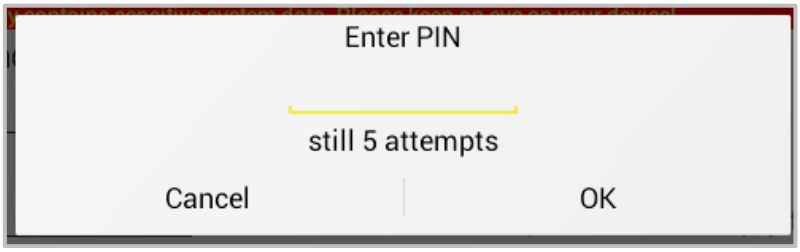


Figure 147: Xesar tablet — entering the initialisation PIN

- The system confirms having successfully completed the task (Figure 148: Xesar tablet — successful initialisation).

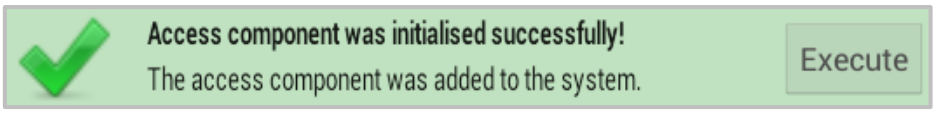


Figure 148: Xesar tablet — successful initialisation

- After having completed the tasks, carefully disconnect the connection cable from your Xesar access component and once again seal the connection socket using the EVVA cover.
- Subsequently go to the next Xesar access component on the list and repeat the process until there are no further tasks on the ***Maintenance tasks*** or ***All tasks*** lists.
- Subsequently synchronise your Xesar tablet with your Xesar software as described in Section ***Synchronising the*** Xesar software .

25.4 Maintenance groups

Maintenance groups support in completing maintenance tasks as efficiently as possible. In this process, it is possible to group doors or areas and spread them over several tablets.

In the menu, click **Locking system** > **Maintenance groups** to create maintenance groups.

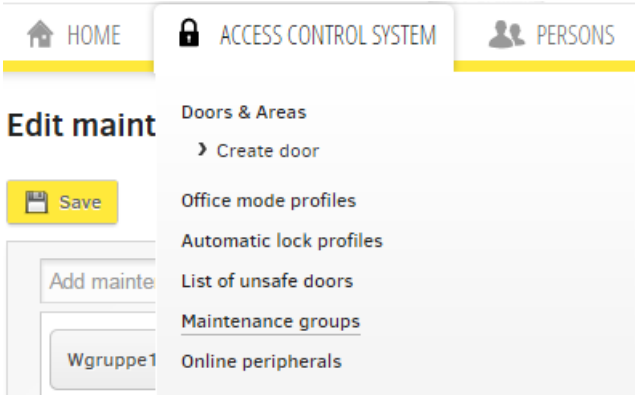


Figure 149: Maintenance groups

Then select doors and areas you would like to bundle in maintenance groups and click **Save:**

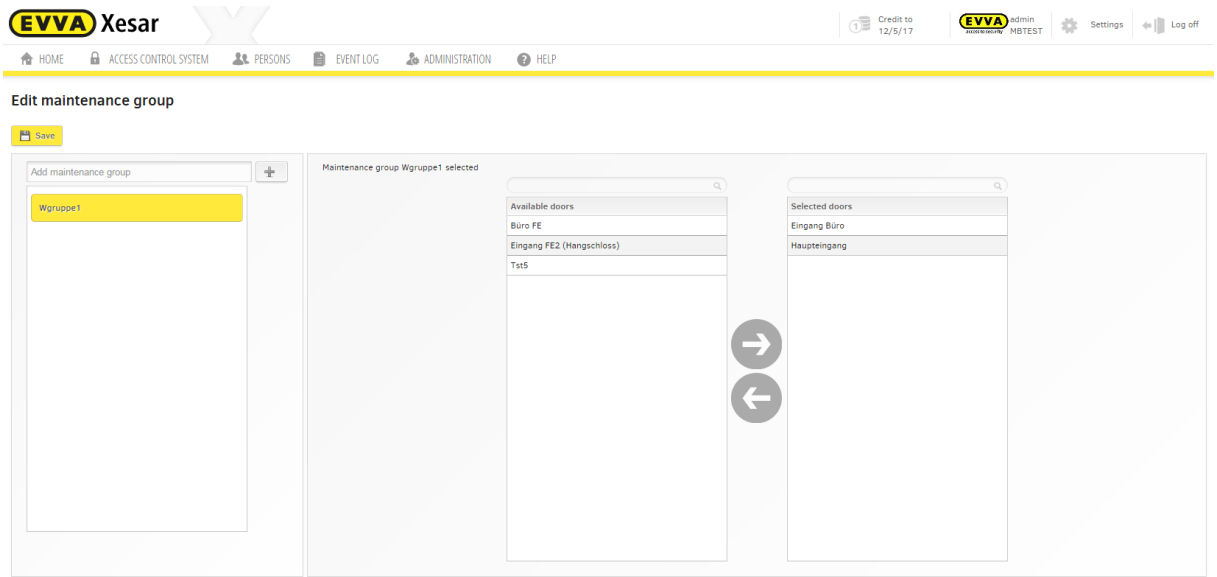


Figure 150: Maintenance groups

Now synchronise your tablet with the Xesar software.

If you use several tablets within your Xesar system, you can now assign the corresponding tablets to a maintenance group. However, you can also assign all maintenance tasks to one tablet (overall system). If you use several tablets, there are no duplicate maintenance tasks (several maintenance

groups for one component are not permitted). Please synchronise your tablet after having completed the maintenance task.

25.5 Activating access media blocks at the access component

If you have already blocked a Xesar identification medium in your Xesar software (Section ***Blocking*** persons), you must subsequently synchronise all Xesar access components to which this person was authorised to also transfer the changes to the affected Xesar access components.
For this purpose, proceed as described in Section *Fehler! Verweisquelle konnte nicht gefunden werden.*.

After having synchronised with your Xesar software, a notification in your Xesar application on your Xesar tablet in the maintenance tasks indicates ***no further tasks***.

All tasks lists all doors to enable you to implement individual tasks (e.g. battery status), regardless of the maintenance tasks synchronised in the Xesar software.

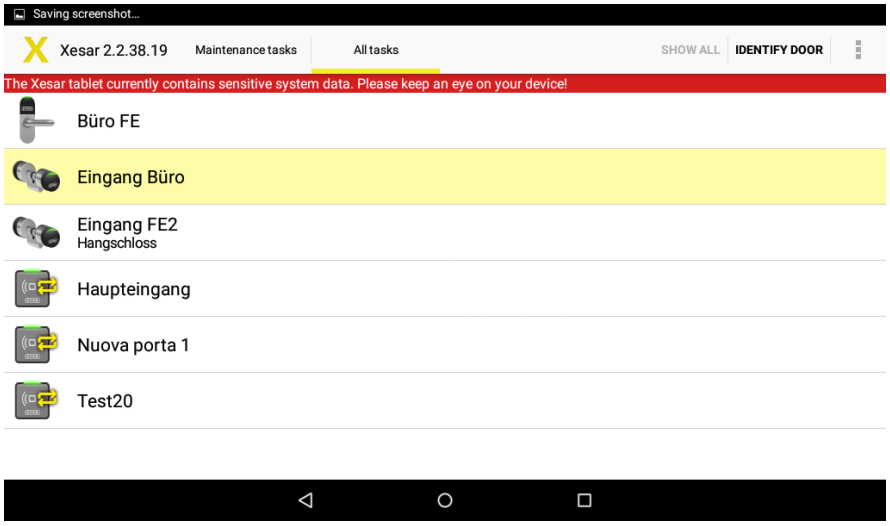


Figure 151: Xesar tablet — all tasks

25.6 Checking the battery status using the Xesar tablet

You can check the current battery status of your Xesar access component (Xesar handle, escutcheon, cylinder) at any time using your Xesar tablet.

- For this purpose, connect your Xesar tablet to the affected Xesar access component.

- Select the three, stacked rectangles in the top right of the open Xesar application.
- Then select ***Show battery status***.

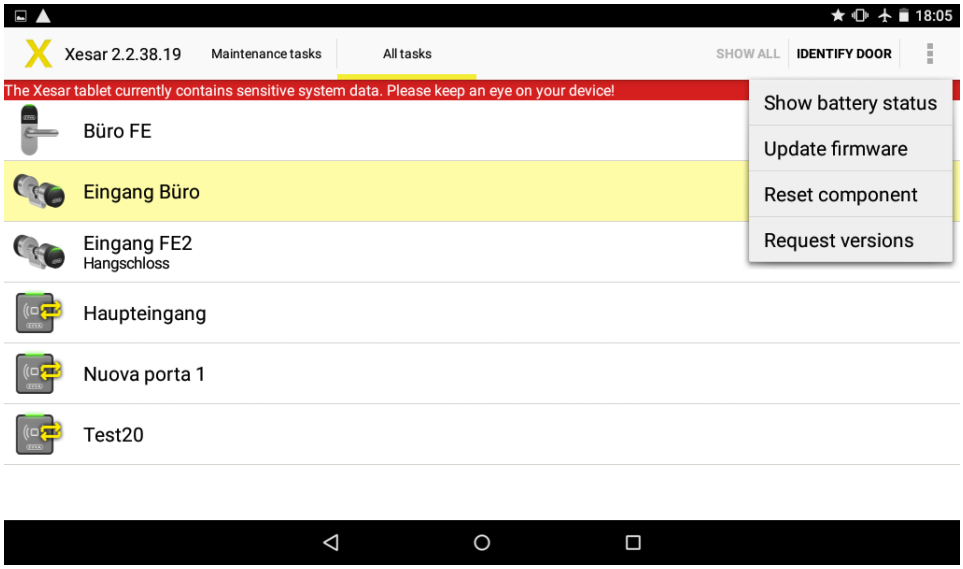


Figure 152: Xesar tablet — showing the battery status

A corresponding OK message will appear if the battery status is OK.

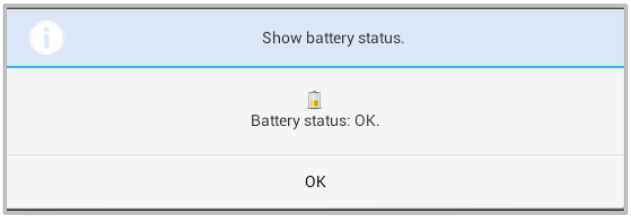


Figure 153: Xesar tablet - showing the battery status

If the battery is empty the system indicates "Battery status: empty. Immediately replace the batteries. Please refer to the description of the corresponding Xesar access component for more detailed information.

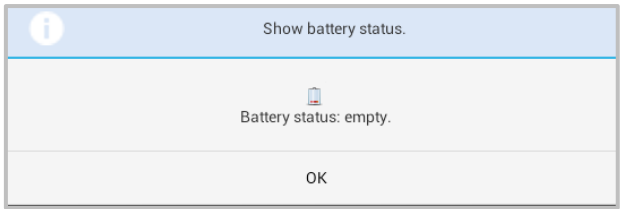


Figure 154: Battery status: empty

An acoustic and visual (four yellow flashes) battery low message will appear approximately 1,000 actuations or four weeks before the battery is empty.

Battery replacements:
Always replace batteries with batteries that have been approved by EVVA. Do not use rechargeable batteries. Rechargeable batteries typically demonstrate a different discharge curve and cause premature "Battery status: low" messages.

When replacing the batteries the date and time is lost as a result of the lack in power after the following periods:

- Xesar escutcheon > 1 minute
- Xesar cylinder > 1 minute
- Xesar handle > 1 minute

Test whether the date and time settings have been lost by attempting to operate the access component using an authorised identification medium after having replaced the batteries. Identification media will be unable to unlock the door if the date and time settings have been lost. In this case, you must transfer the date and time settings using the Xesar tablet. Test the component operates correctly **before** closing the door. If the date and time setting is lost, even identification media with MasterKey authorisation will be unable to operate the access component.

25.7 Automatically identifying doors

Use the ***Identify door*** tablet function to open the current door component and carry out maintenance tasks and updates quickly and conveniently.

For this purpose, connect your tablet to the door component and click***Identify door***. As usual, you will then see all details and tasks relevant to this component.

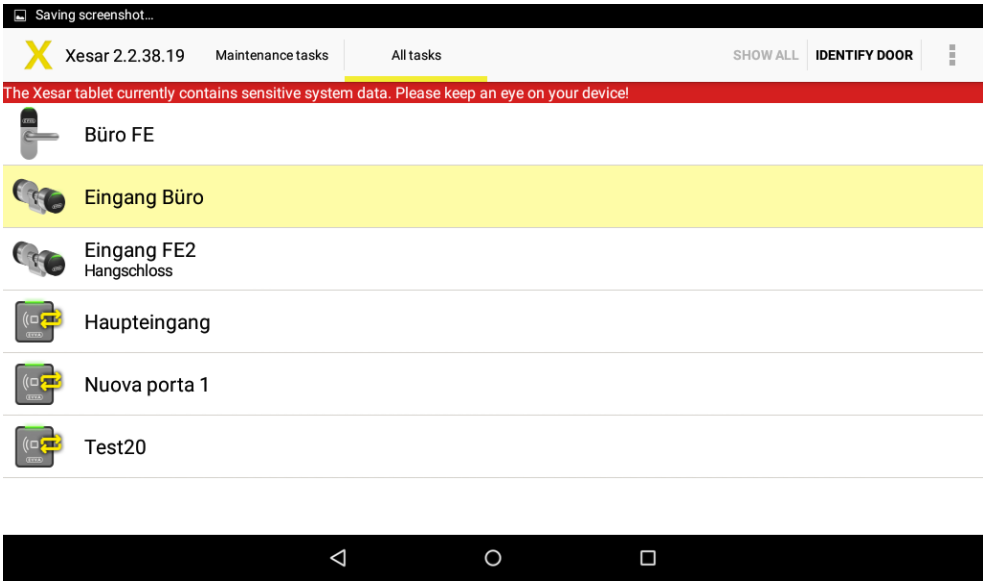


Figure 155: Identifying doors

25.8 Firmwareupdate

The Xesar tablet indicates if a firmware update is available (e.g. an update from Xesar 1.1 to Xesar 2.0).

- For this purpose, connect your Xesar tablet to the affected Xesar access component.
- Select the three, stacked rectangles in the top right of the open Xesar application.
- Check the access components' battery status beforehand.
- Then select Update firmware.

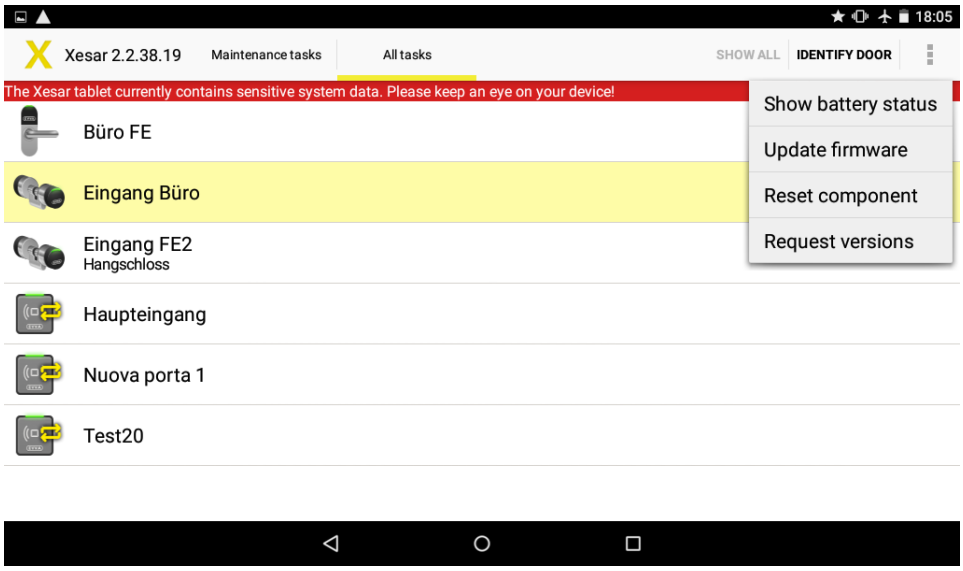


Figure 156 Xesar tablet – viewing the status

You can follow the progress of the updates on the Xesar tablet. The update may take a few minutes.

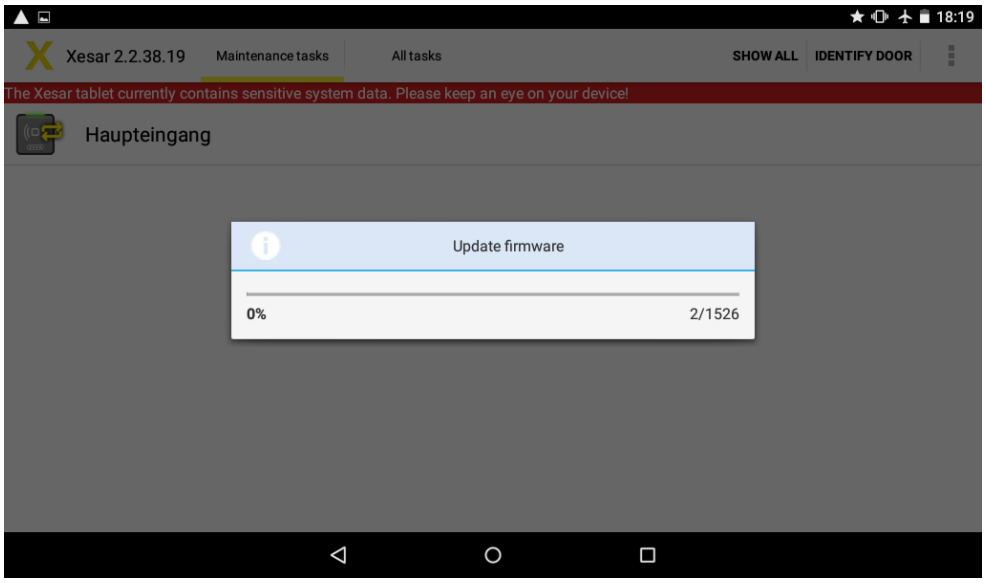


Figure 157 Xesar tablet – firmware update

Do not disconnect the connection cable during the update process as this may render the access component unusable.

A notification appears after having successfully completed the firmware update.

If the access component continues malfunctioning, it may be removed as a last resort (see section on For***cing removal)***

25.9 Additional maintenance tasks

Regularly service Xesar access components and in this process, synchronise the information with the Xesar software

The following tasks must be completed directly at the Xesar access component as part of on-going maintenance tasks:

25.10 Xesar-tablet error messages

You may experience different error messages, due to mishandling or technical problems.
The following table provides an overview of error messages and tips to avoid them

Error	Event
XTDE01	Wrong type of component
XTDE02	USB not connected
XTDE03	No responce
XTDE04	Wrong door
XTDE05	Component has no battery
XTDE09	Subcomponent doesn't reply
XTDE10	Unsupported version
XTDE11	USB communication error
XTDE12	Unknown error
XTDE13	Operation failed temporarily
XTDE14	Operation failed
XTDE15	Xesar-Tablet not synchronized
XTDE16	Displaying battery status failed

Tips

- Please make sure that the Xesar-tablet is connected to the right Xesar-component and repeat the synchronization
- Synchronize the Xesar-tablet and the access-components
- Check the USB-connection cable of your Xesar-tablet
    - In this case, remove the cable from your tablet and the accesss component, replug it and try again to synchronize
- Check the battery status of the access-component. If necessary, insert new batteries and pay attention to the polarity.
- Perform a firmware update via the Xesar-tabletXesar's Virtuelles Netzwerk (XVN)

25.11 Xesar's virtual network (XVN)

The Xesar virtual network uses the issued identification media to exchange information between software and doors to always keep the system up to date.

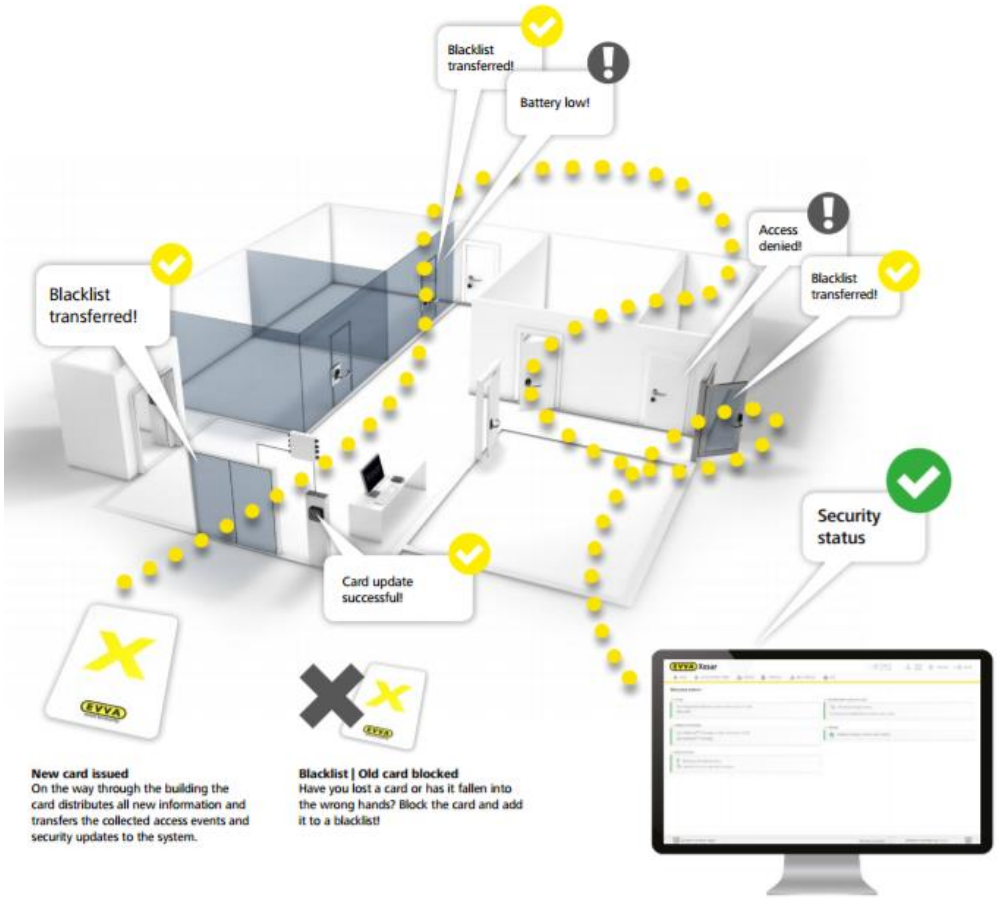


Figure 158: system overview | virtual network

Identification media are provided[1] with update information (blacklist) from the central coding station. The information is then transferred from door to door on the way through the facility. In this process, identification media update door states and collect door information (battery states, access events, deletions or unlocking attempts by blocked media). The information is subsequently passed on to coding stations, where it is evaluated to reconfigure the security status in the software.

A maximum of 123 updater wall readers can be integrated into a system.

---

[1] Also available using wall readers from autumn 2015.

25.11.1 Softwareplus package (virtual network)

To use the virtual network, please activate the software*plus*-package.
The Software*plus* card can be purchased from an authorized EVVA-distributor, the code on the back of the card can be activated just like any KeyCredit.

Figure 159: Software*plus*-package

Enter the code on the home page in the Xesar software via the menu item
Additional packages > Software*plus* package to unlock the virtual network for a time of 3 years.
In addition after the activation of the virtual network, you get 15 KeyCredits for free.

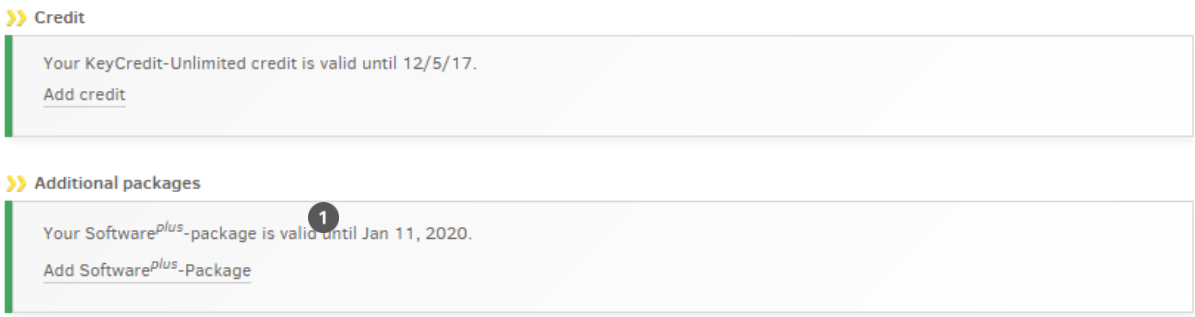


Figure 160: Software^{plus}-package | additional package

25.11.2 Transferring access events using identification media

The most recent access events (access granted, access denied, battery low, etc.) of the door component are transferred to identification media as part of every second identification process, e.g. when a door component is unlocked using identification media.

Note: this process does not require users to be logged in to the software and the Admin Card must not be in the coding station - it is sufficient to only launch the software.

25.11.3 Transferring blacklist entries using identification media

A blacklist entry represents the information regarding identification media that is blocked in the software.
Said blacklist entries are written to all identification media using the coding station. Identification media then distribute the information to all door components.

The memory of one identification medium is sufficient for up to 10 blacklist entries. As soon as identification media are once again used at the coding station, the software detects to which door components the blacklist has already been transferred and visualises the corresponding status of individual doors on the Xesar software dashboard.

We recommend transferring blacklists using the Xesar tablet if more than 10 identification media are lost/stolen at once.

An identification medium that has been blocked in the software (medium on the blacklist) can be invalidated/deleted as part of the following:

- Expiry date exceeded
- Validity period expired

- Medium has been in contact with the coding station
- Medium attempts to unlock a door at which the blacklist is up to date

25.11.4 Transfer "Unlocking attempt by medium" notifications using identification media

A medium that has been blocked in the software can open the corresponding door components as long as it is still valid. This type of information is critical to security and the data is collected by other identification media within the system before it is transferred to the Xesar software using the coding station.

A warning is output accordingly on the dashboard ❶ if unlocking attempts have taken place using identification media that have already been blocked.
These warnings will be hidden as soon as the medium's validity expires. The messages remain available in the corresponding event list.

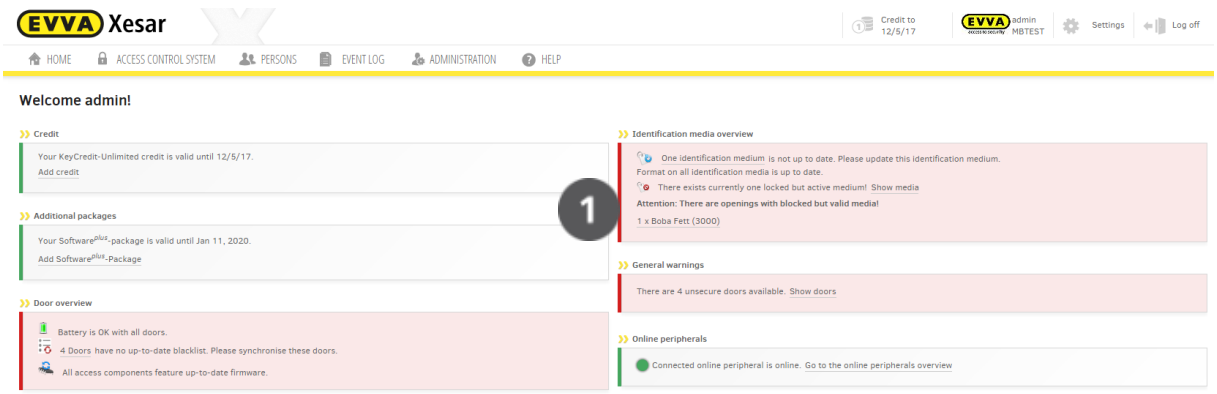


Figure 161: Dashboard | Unlocking attempt by medium

25.11.5 Transferring "Identification medium deleted by door component" notifications

The identification medium is deleted from the door component upon attempting to unlock a door component (with an up-to-date blacklist) using an identification medium that has been blocked in the software. As a consequence, this medium can now no longer open doors with an out-of-date blacklist (Xesar 1.1.x.x already features this function)

The new feature is that the information about a deleted medium is returned to the Xesar software by other identification media within the system via the virtual network. As a result, administrators

are automatically provided with information that the system is once again secure even if the blacklist has potentially not yet been transferred to all doors.

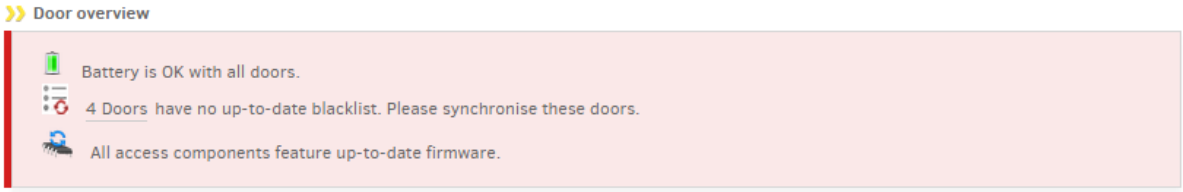


Figure 162: Dashboard | maintenance: Blacklist

25.11.6 Transferring the battery status using identification media

Identification media in circulation also return battery information to the Xesar software via the virtual network. Administrators are notified in due time if batteries must be replaced.

System administrators have the option to indirectly influence update cycles using identification media's validity periods. The validity period is automatically extended by the set value each time the identification medium is placed on the coding station.

For instance, if the period has been set to three days, each person must pass the coding station to extend the validity of their identification media within this period of time. As a result, system administrators are provided with the corresponding information at the latest after three days (events, blacklist transfers, etc.) using the identification media in circulation. For instance, if the validity is set to 30 days, it will take longer for the information to be returned to the Xesar software.

We recommend to keep the validity period to a minimum (< 10 days) when using a virtual network.

26 Commissioning the Xesar network adapter

26.1 PC configuration

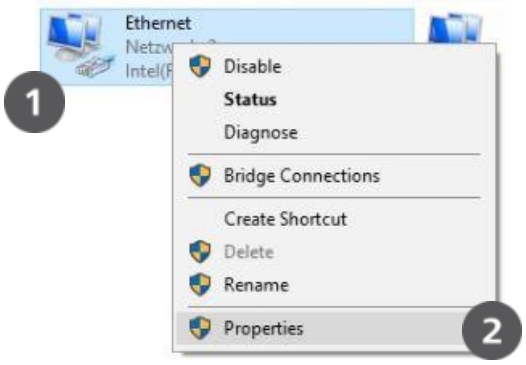


Figure 163: Windows | Adapter settings

- Any computer is suitable for configuring the Xesar network adapter and you can even use the PC running the Xesar software.
- Please configure the settings of your PC network adapter before starting to commission the Xesar network adapter.
- For this purpose, in Windows 7 go to Netwo***rk and Sharing Center > Change adapter settings.***
- Open the ***Settings*** window ❶ (right-click LAN connection)

Important: Please note that additionally active network connections (WiFi, etc.) may impair communication with the Xesar network adapter — deactivate these if necessary.

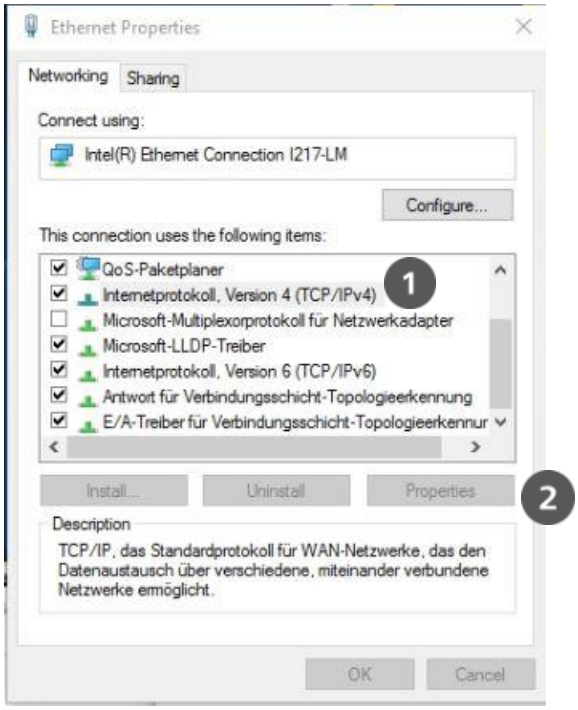


Figure 164: Windows | LAN connection

- In the window, select ***Internet protocol version 4 (TCP/IPv4)*** ❶ and click ***Settings***❷.

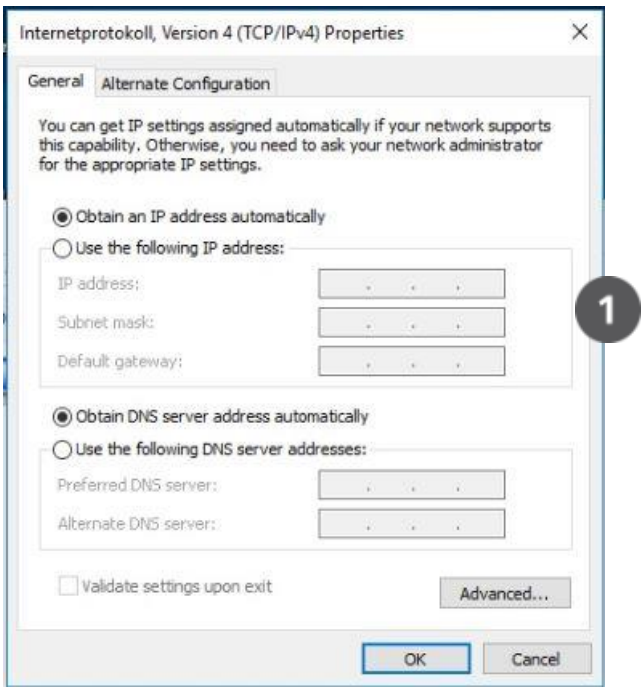


Figure 165: Windows | IP address (PC)

- Now configure the ***IP address*** and the ***Subnet mask*** ❶ of the PC you are using for the configuration.

Use the following details for this purpose:

o	IP address:	**192.168.0.**xxx (1-254)
	Subnet mask:	**255.255.255.0**
	DNS server:	-

Make sure you do no**t use** the preconfigured IP address of the Xesar network adapter (*192.168.0.100*) as otherwise there will be an IP address conflict which will inhibit a connection.

Please contact your system administrator if you encounter any issues during setup.

26.2 Commissioning a Xesar network adapter

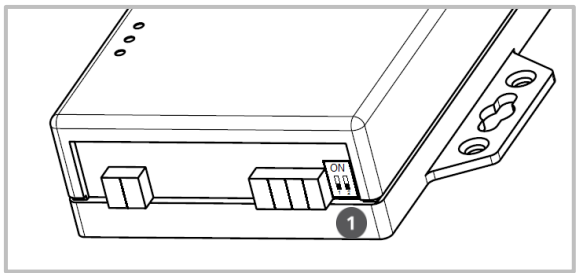


Figure 166: Xesar network adapter | Jumper position

- Check the jumper position ❶ of the Xesar network adapter.

  Both jumpers must be set to OFF (bottom position).

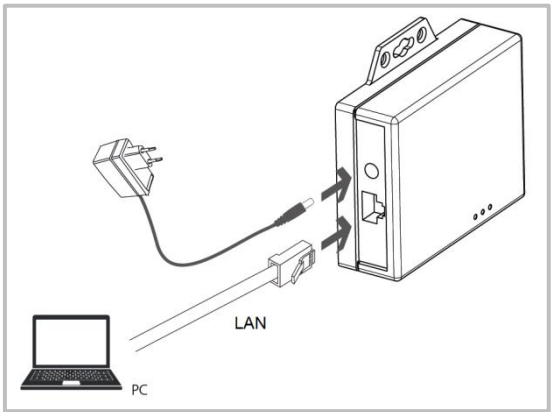


Figure 167: Xesar network adapter | Connections

- Connect the mains adapter to the Xesar network adapter.
- The green, flashing status LED indicates whether the Xesar network adapter is supplied with power.
- Then connect the Xesar network adapter to the configuration PC.

  For this purpose, use an RJ45 LAN cable and make sure the connector engages audibly in the socket.

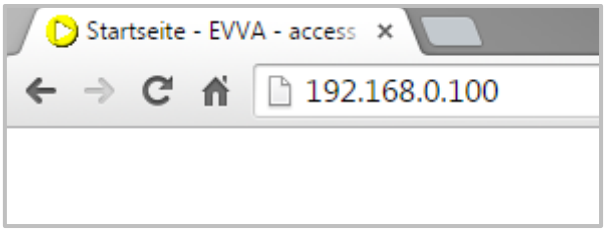


Figure 168: Xesar network adapter | IP address (updater)

- Now open your computer's Internet browser.
- Enter the standard address of the Xesar network adapter in the browser's URL bar – it is listed on the bottom of the device and has been set to **192.168.0.100** by default.

Note: Check the firewall settings, the IP settings and the cabling of the Xesar network adapter if the configuration page fails to open.

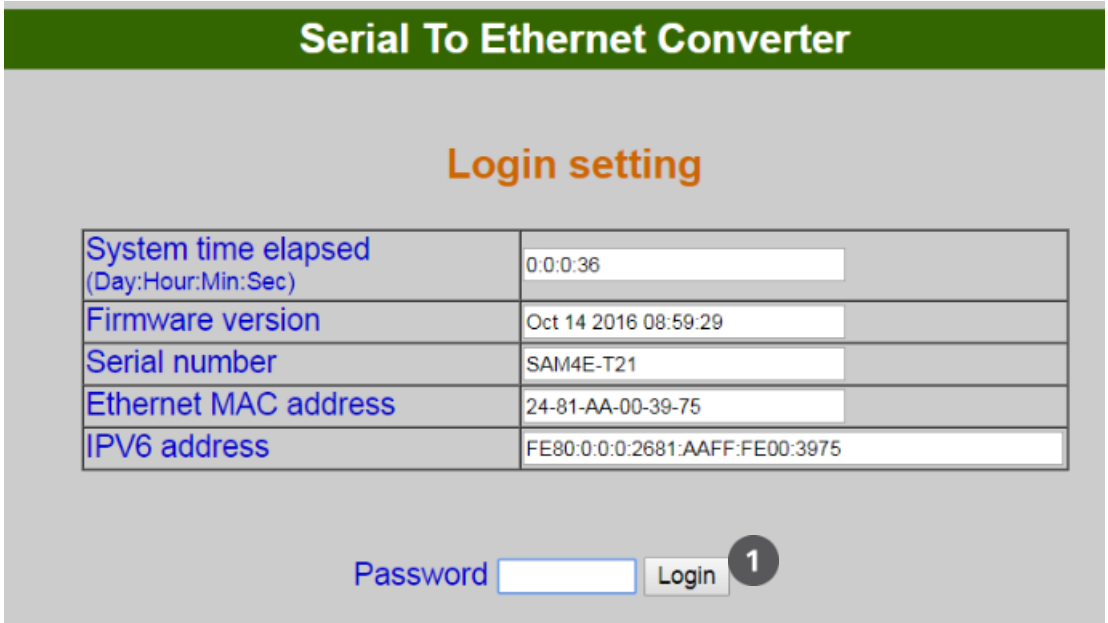
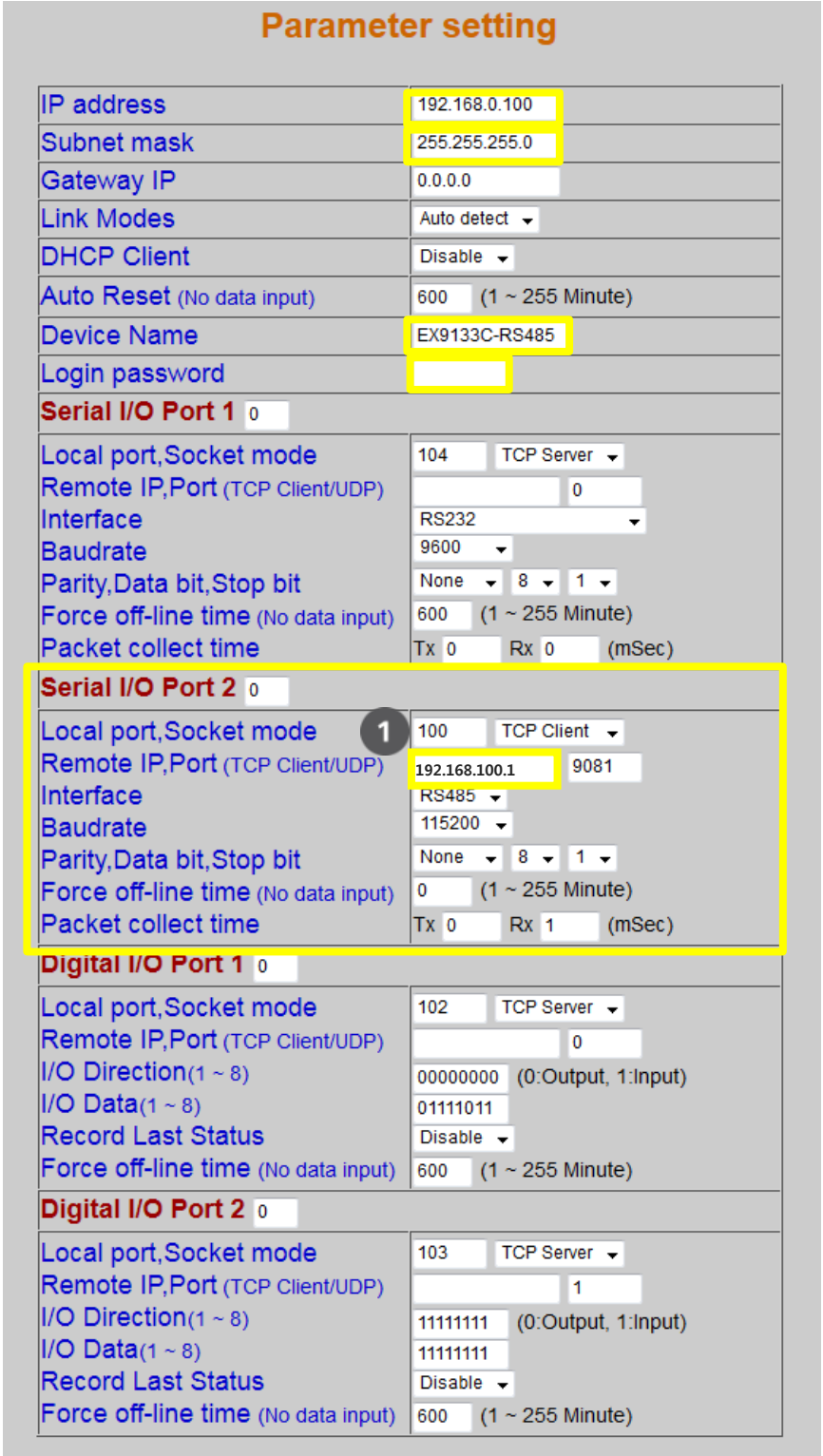


Figure 169: Xesar network adapter | Login

- The Xesar network adapter login page appears – click Login ❶; it is not nece***ssary*** to enter a password.



Parameter setting

IP address	192.168.0.100
Subnet mask	255.255.255.0
Gateway IP	0.0.0.0
Link Modes	Auto detect
DHCP Client	Disable
Auto Reset (No data input)	600 (1 ~ 255 Minute)
Device Name	EX9133C-RS485
Login password	
Serial I/O Port 1 0	
Local port,Socket mode	104 TCP Server
Remote IP,Port (TCP Client/UDP)	0
Interface	RS232
Baudrate	9600
Parity,Data bit,Stop bit	None 8 1
Force off-line time (No data input)	600 (1 ~ 255 Minute)
Packet collect time	Tx 0 Rx 0 (mSec)
Serial I/O Port 2 0	
Local port,Socket mode (1)	100 TCP Client
Remote IP,Port (TCP Client/UDP)	192.168.100.1 9081
Interface	RS485
Baudrate	115200
Parity,Data bit,Stop bit	None 8 1
Force off-line time (No data input)	0 (1 ~ 255 Minute)
Packet collect time	Tx 0 Rx 1 (mSec)
Digital I/O Port 1 0	
Local port,Socket mode	102 TCP Server
Remote IP,Port (TCP Client/UDP)	0
I/O Direction(1 ~ 8)	00000000 (0:Output, 1:Input)
I/O Data(1 ~ 8)	01111011
Record Last Status	Disable
Force off-line time (No data input)	600 (1 ~ 255 Minute)
Digital I/O Port 2 0	
Local port,Socket mode	103 TCP Server
Remote IP,Port (TCP Client/UDP)	1
I/O Direction(1 ~ 8)	11111111 (0:Output, 1:Input)
I/O Data(1 ~ 8)	11111111
Record Last Status	Disable
Force off-line time (No data input)	600 (1 ~ 255 Minute)

Figure 170: Xesar network adapter | Parameter settings

You are now on the Xesar network adapter configuration page.

As shown on the illustration, complete the white fields.

Configure the fields highlighted in yellow as follows:

- The **IP address** defines the IP address of the Xesar network adapter.

  Please note that changing this address and clicking ***Update*** (or confirming with the ***ENTER*** key) means the network adapter can exclusively be opened and configured using this address.

  It is necessary to define up to 123 different IP addresses for each of the 123 potential Xesar network adapters within a system.
  In this process, also check the network settings of the PC and observe the valid IP address range of your network.
- The **Subnet mask** defines the subnet used.
- The **Device Name** can be specified individually and it does not influence the device function.
- The ***Login password*** restricts access to the device configuration page. A default password has not been configured.
- The ***Remote IP*** corresponds to the IP address of the computer running the Xesar software and it is responsible for communication between the Xesar network adapter and the Xesar software.

  Note: The ***Remote IP*** (PC) and ***IP address*** (Xesar network adapter) must differ!

  Attention: Please use the number ❶ "100" only once at "local port, socket mode" **(serial & digital)**!

Sample configuration:

IP address	*192.168.100.10*1
Subnet mask	*255.255.255.*0
Device name	*Updater1*
Login password	*passwordupdater*1
Remote IP	*192.168.100.*1

After having completed the parameter configuration**,** click ***Update*** to complete the Xesar network adapter configuration.

Resetting network adapters:

If you are forced to reset the network adapter in the event of an error, subsequently re-check the ***Parameter settings***.

In this process, particularly check ***Socket mode*** (TCP client), **Baudrate** (115200) and ***Port*** (9081)!

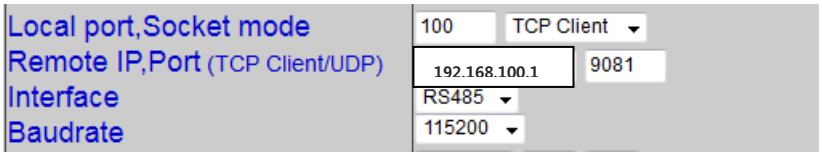


Figure 171: Port

26.3 Adding Xesar updaters

Proceed as follows to create a Xesar updater:

- Click ***Locking system*** > Create door**.**
- Specify the Name of the door/updater ❶ (Figure 76: Creating new door areas).
- ***Also click*** Save to take over the input.

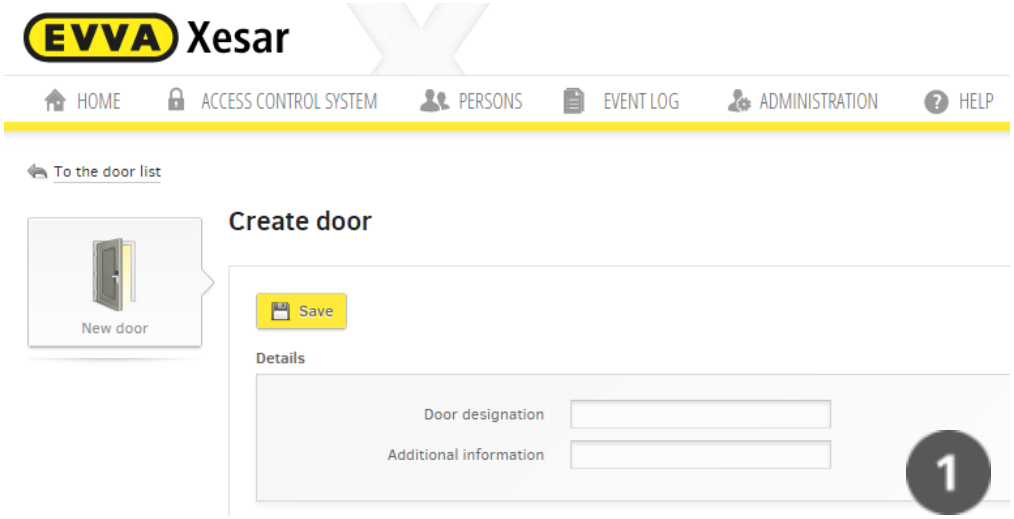


Figure 172: Updater | Creating doors

- Click ***New access component*** ❶ and select the ***Xesar updater*** ❷.
- ***Click*** Save to take over the input.

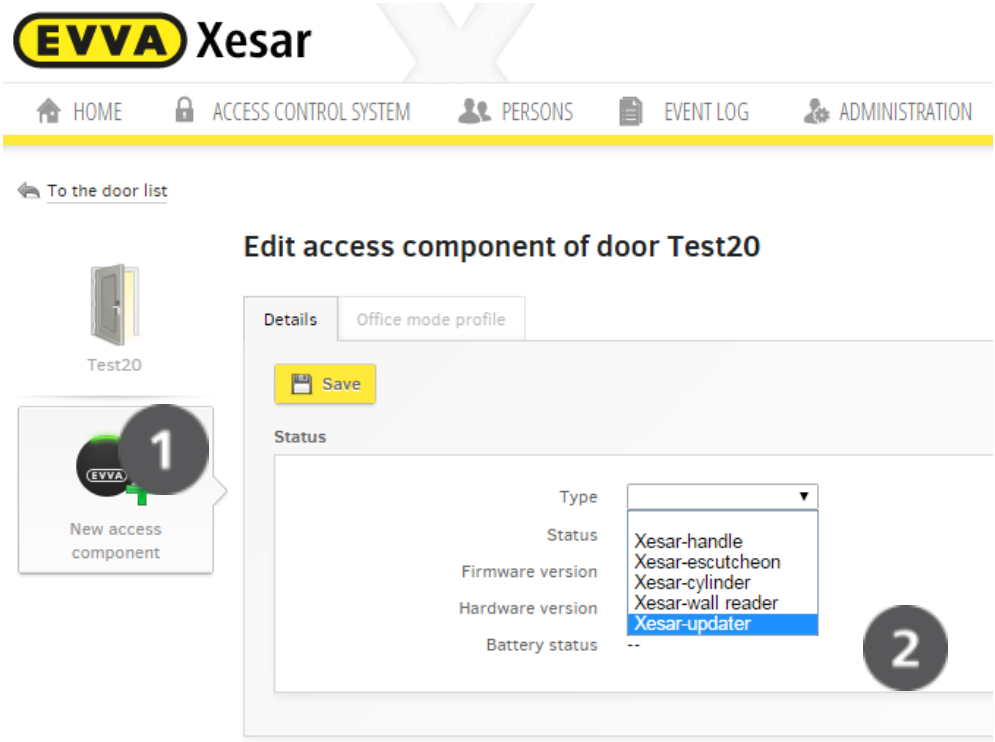


Figure 173: Updater | Access component

You have now prepared the Xesar updater for installation.

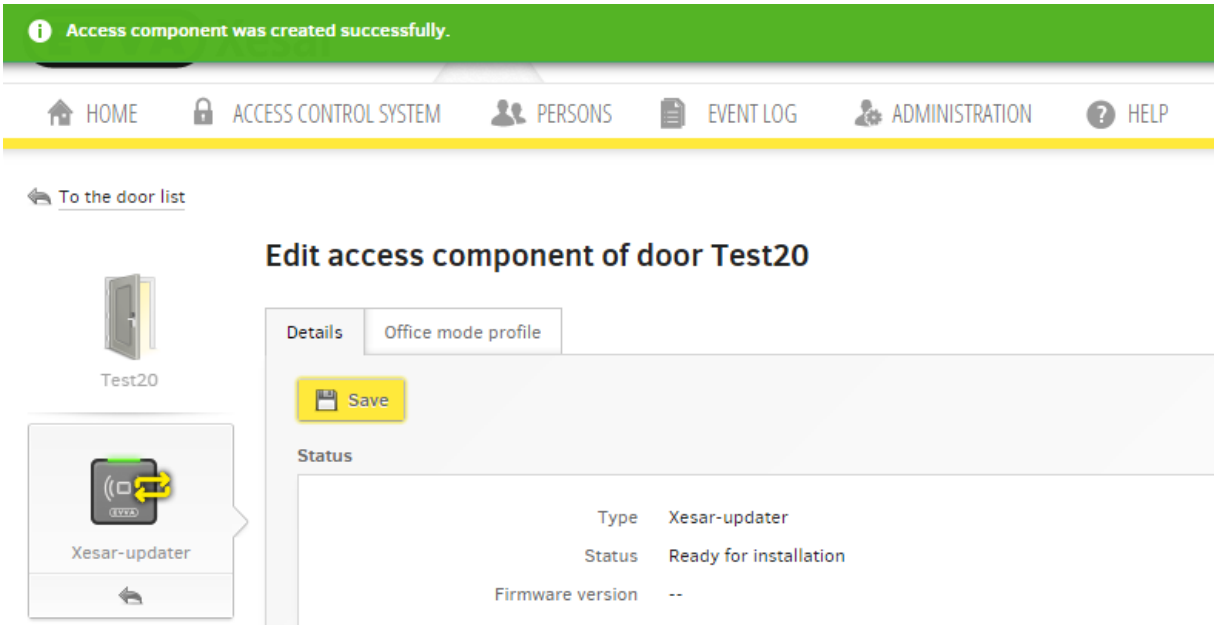


Figure 174: Updater | Access component created

Assign a name to the Xesar updater (wall reader) using the Xesar tablet and subsequently synchronise it with the Xesar software.

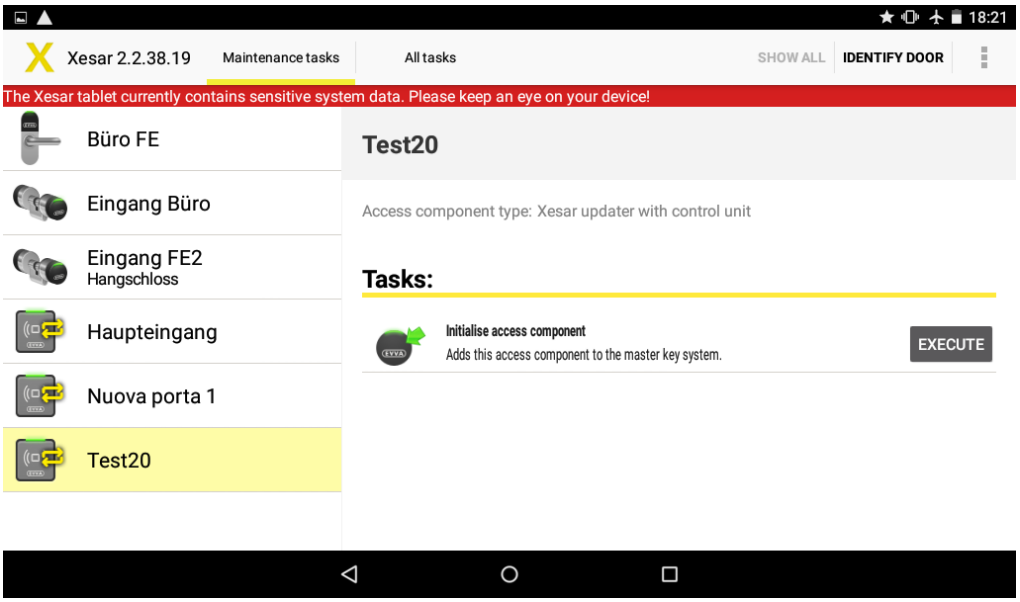


Figure 175: Updater | Assigning names to components using the Xesar tablet

You can view the Xesar updater status after having synchronised successfully.

You can also access any updaters' component details using ***Locking system > Online peripherals*** ❶ and click the corresponding updater ❷.

A maximum of 123 updater wall readers can be integrated into a system.

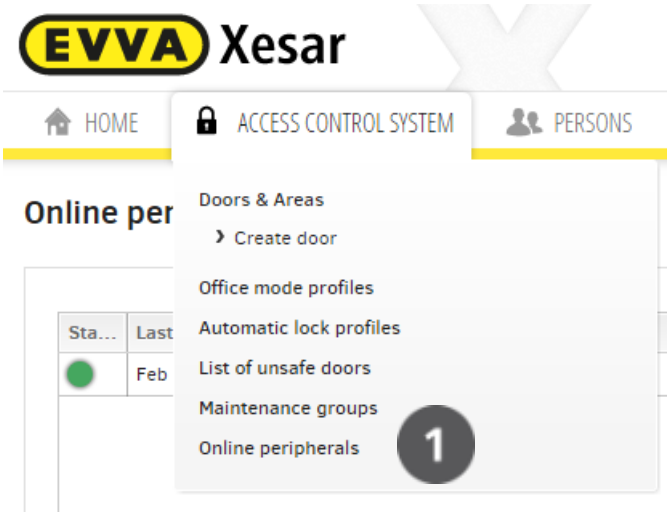


Figure 176: Updater | Online Peripherals

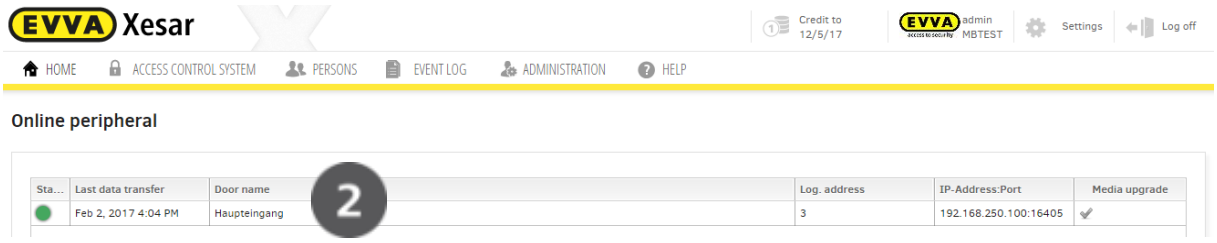


Figure 177: Updater | Online Peripherals

26.4 Xesar updater operating modes

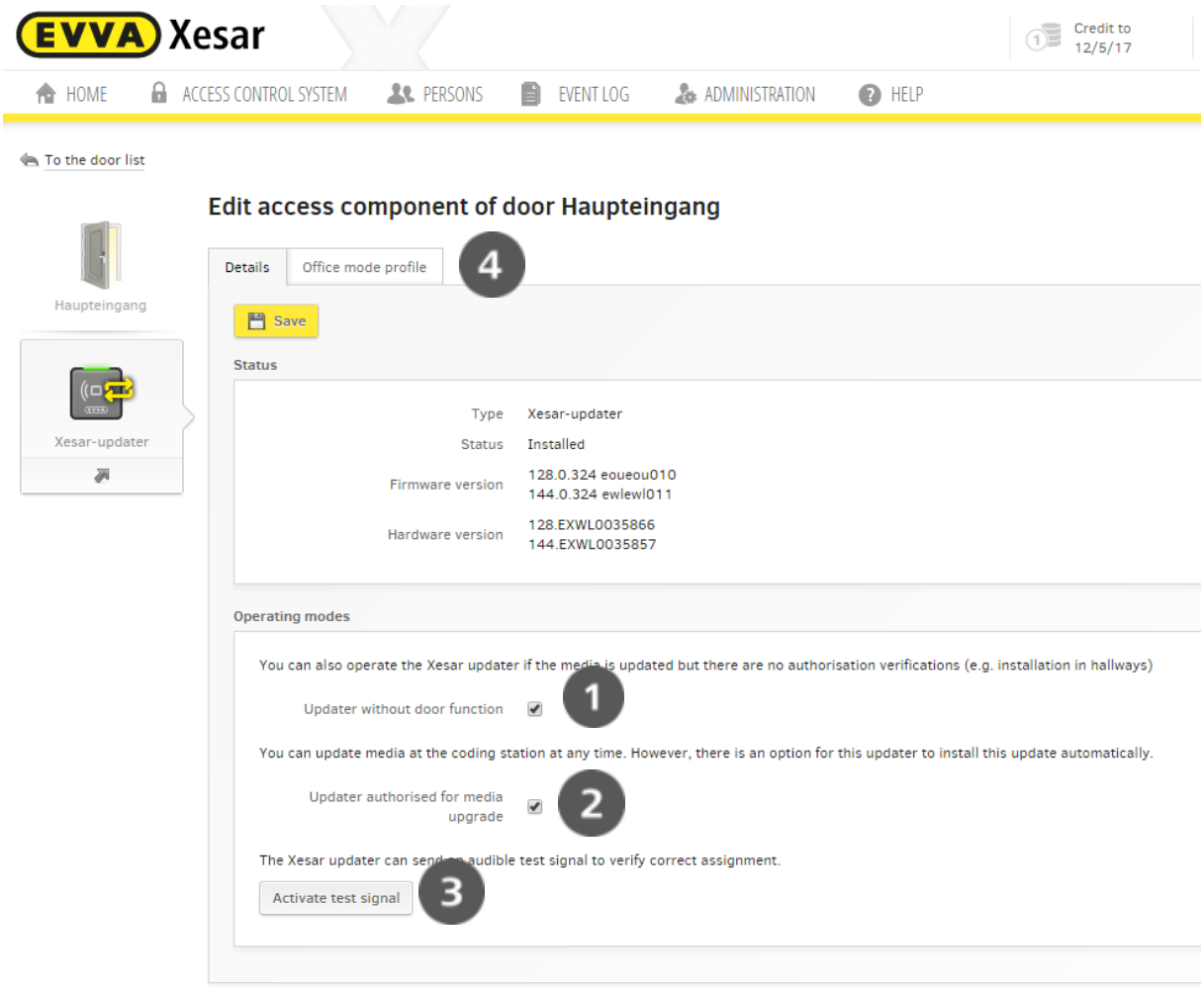


Figure 178: Updater | Operating modes

Updater without door function

Tick the ***Updater without door function*** ❶ tick box to operate the updater as a simple wall reader to update your identification media. The authorisation is not verified in this mode.

Updater authorised for media upgrade

Tick the ***Updater authorised for media upgrade*** ❷ tick box to automatically carry out media upgrades. This will allow you to also upgrade the media at different sites using the updater in addition to using the central coding station only.

Test signal

A ***test signal***
can be activated to check the connection of the corresponding Xesar updater ❸. This test signal generates a repeating, audible signal and the component also flashes twice at the Xesar updater. Click ***Deactivate test signal*** ❸ to end it.

Office mode profile

As usual, Xesar updaters also take over the function of a conventional wall reader.
For this reason, open the ***Office mode profile*** ❹ menu to create your central or private profiles as usual.

26.5 Xesar Updater - Dashboard

The Xesar software main menu now not only shows the familiar status messages and maintenance tasks, but also the status of your Xesar updater ❶.
A green light confirms the online status of the Xesar updater. If the connection to one or more updaters fails, this is indicated by a RED lamp.
For this purpose, you can also click the ***Online peripherals overview*** ❷ to obtain an overview of all Xesar updaters.

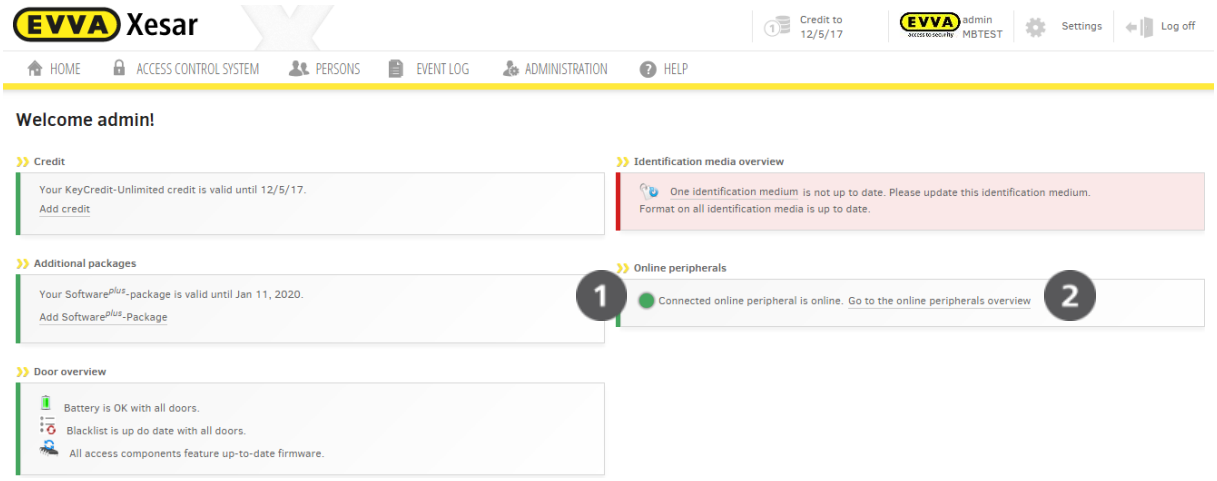


Figure 179: Updater | Dashboard

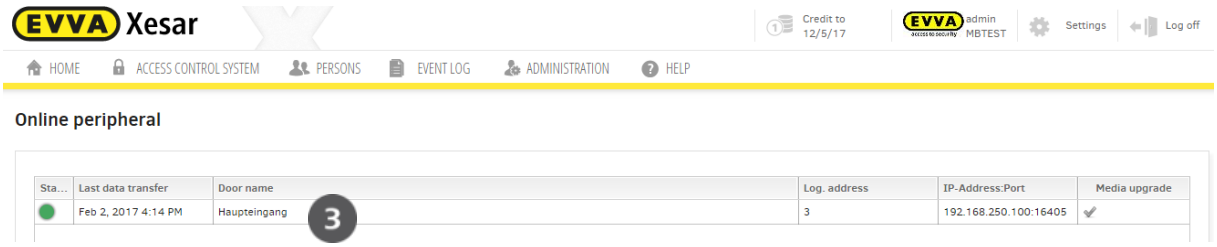


Figure 180: Updater | Peripherals online

Click an updater ❸ to access this Xesar updater's details and operating modes

The dashboard immediately indicates if communication to one or more Xesar updaters fails as a result of an error (for instance due to a power cut or sabotage). Click ***Online peripherals overview*** to view the affected updaters and take targeted action.

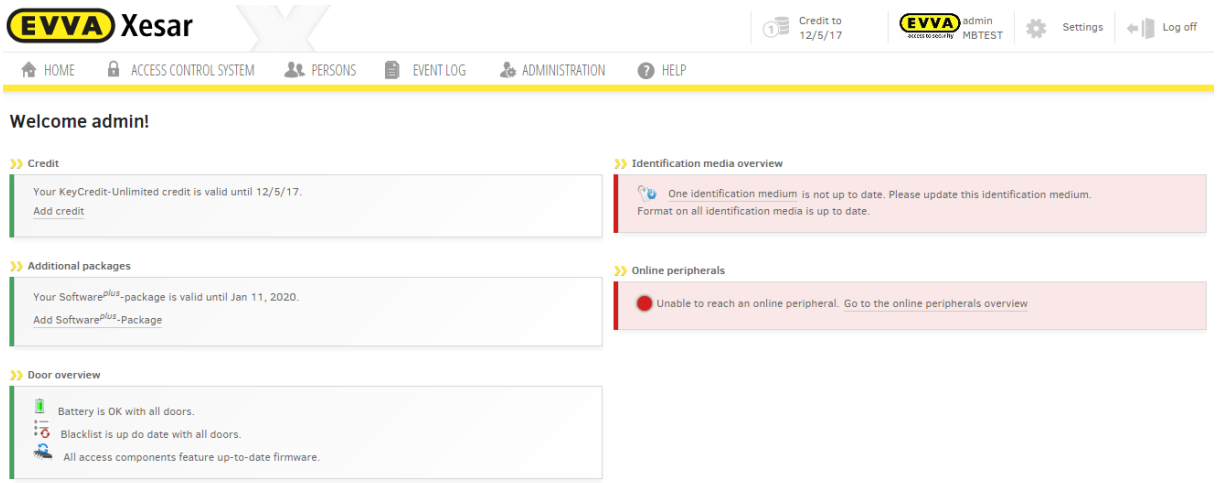


Figure 181: Updater | Dashboard – offline

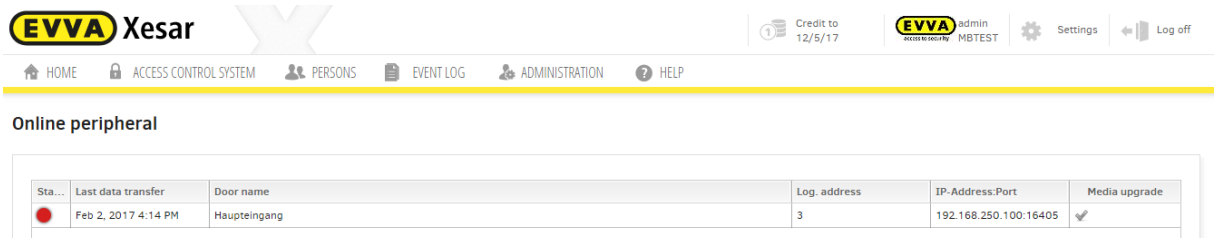


Figure 182: Updater | Peripherals offline

If communication between a Xesar updater and the Xesar software fails (but the power supply is safeguarded), the updater will show an offline signal (three red flashes) upon holding identification media to the updater to highlight the current operating mode.

26.6 Manually installing/uninstalling the Xesar app

Xesar 2.2 apk (tablet app) features a new signature. If you intend to use this tablet for Xesar installations older than V2.2, you must manually uninstall and install the Xesar app:

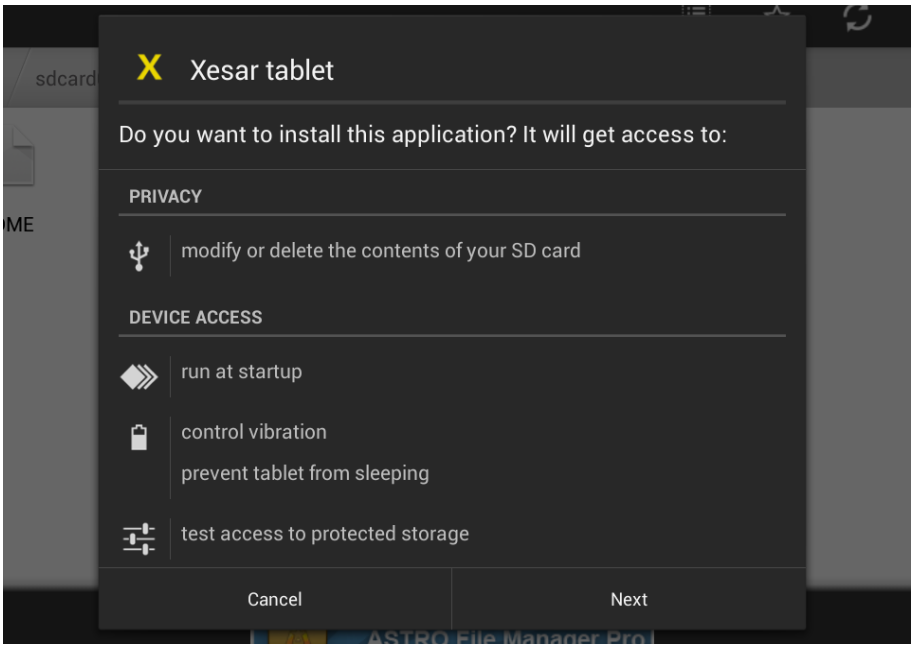


Figure 183: Manually deleting and installing the tablet app

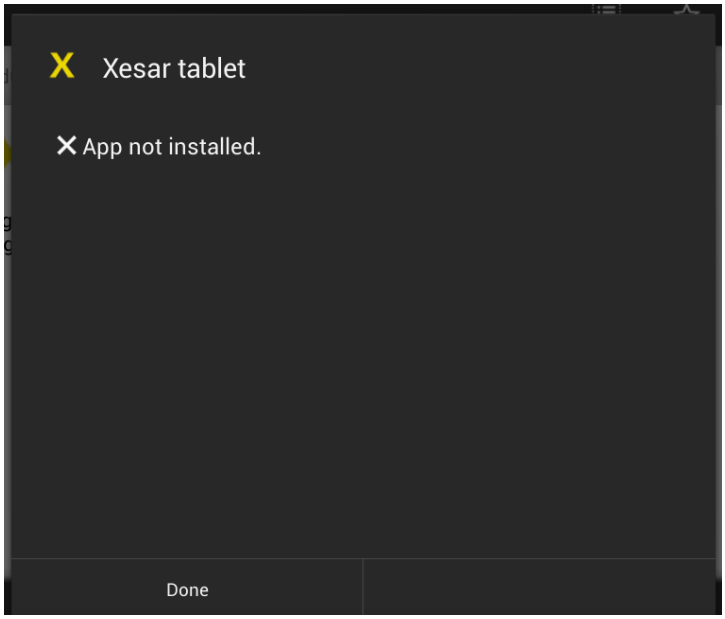


Figure 184: Manually deleting and installing the tablet app

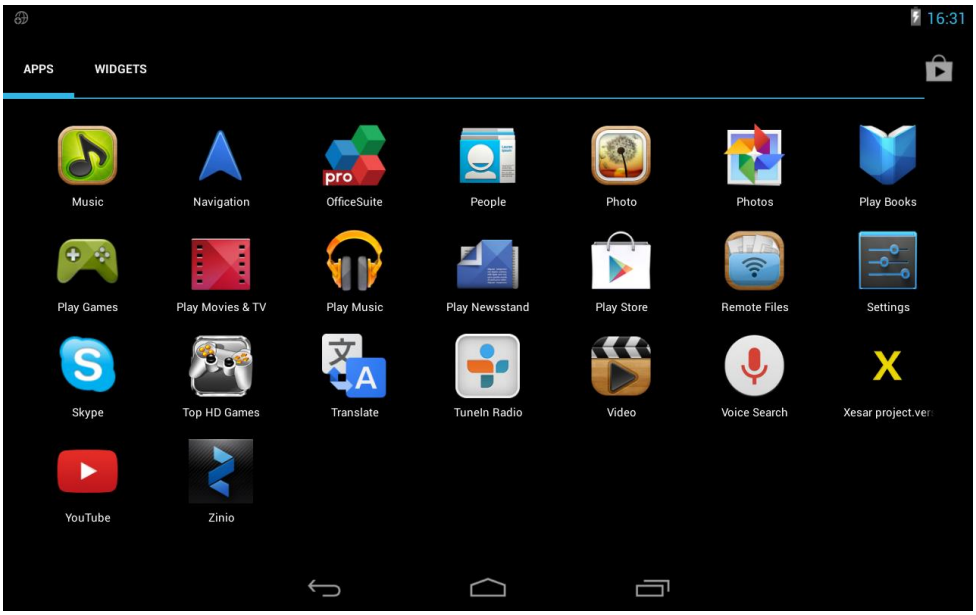
An update message is output as soon as you intend to synchronise a tablet featuring an apk older than Xesar 2.2 with Xesar 2.2.

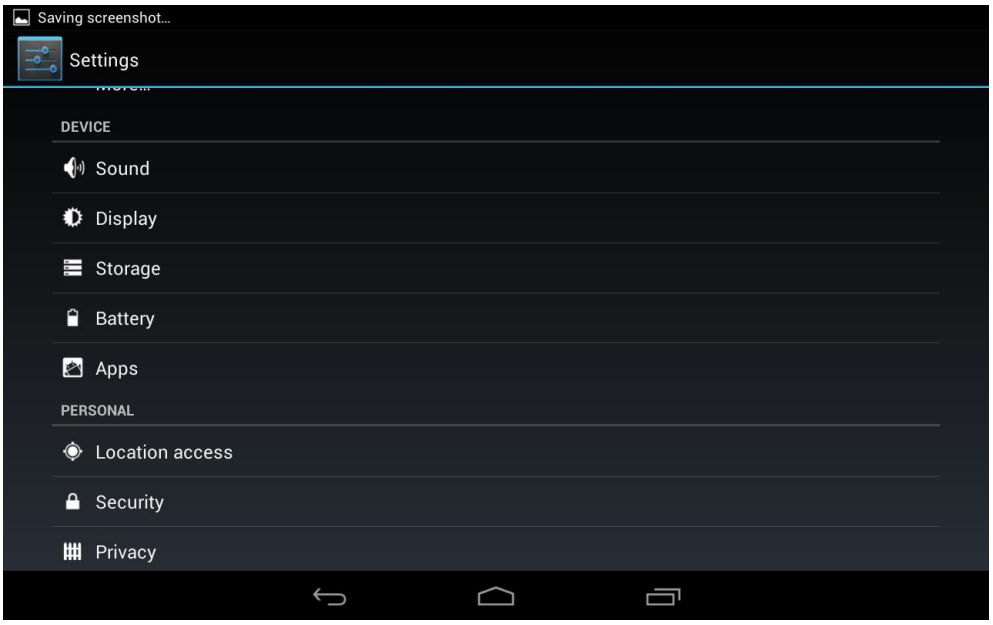
An error message is output if you attempt to install the update.

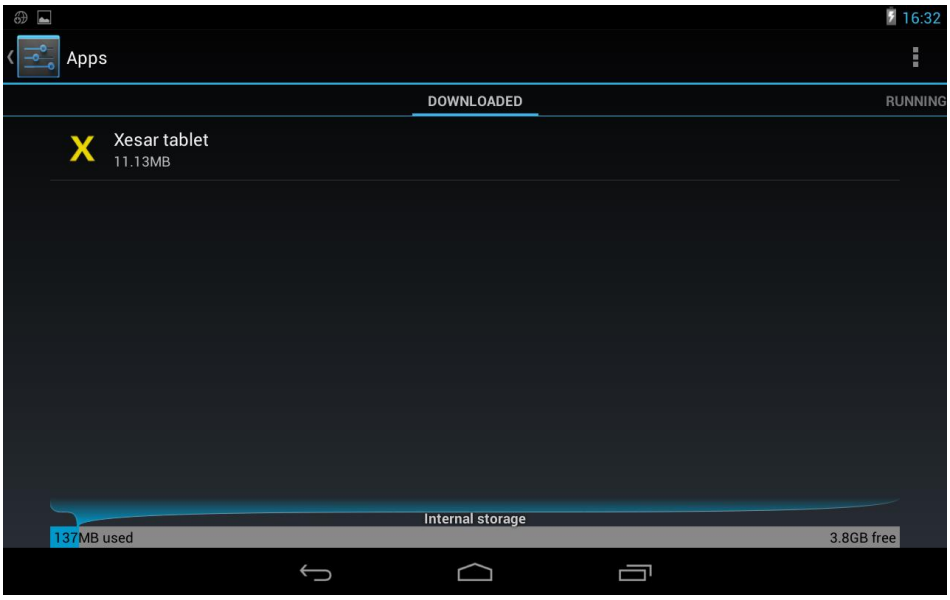
The installed, outdated Xesar app must be uninstalled manually and the most recent app must be installed instead.

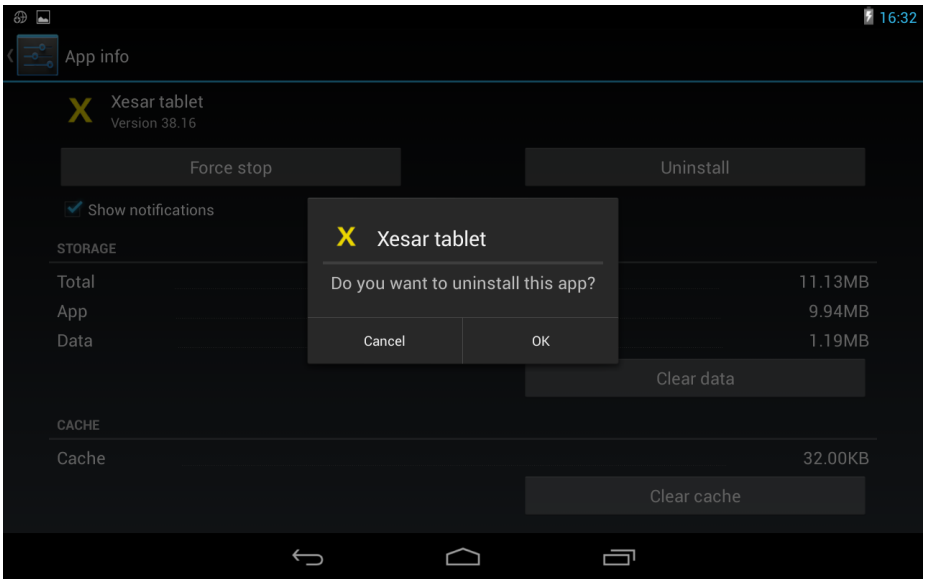
Start your tablet and proceed as follows:

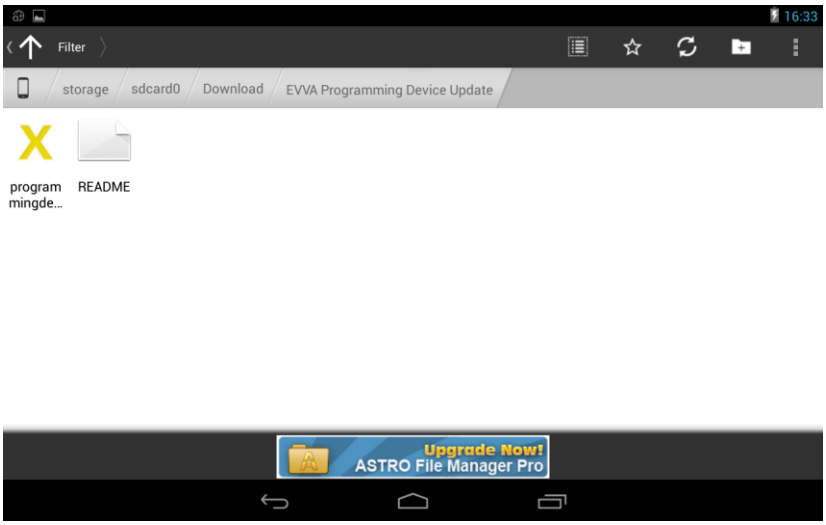
1. In the main menu, select **Settings**
2. Click **Apps**
3. Uninstall the Xesar app and delete the .apk file from the download folder
   For this purpose, open your tablet's file manager
4. Synchronise the tablet with the Xesar software (e.g. Xesar V2.2)
5. The Xesar app is copied to the Xesar tablet
6. Now click the .apk file to install the Xesar app on your tablet
7. Subsequently once again synchronise the tablet with the Xesar software and confirm synchronisation in the Xesar administration
8. Your tablet is now ready for use

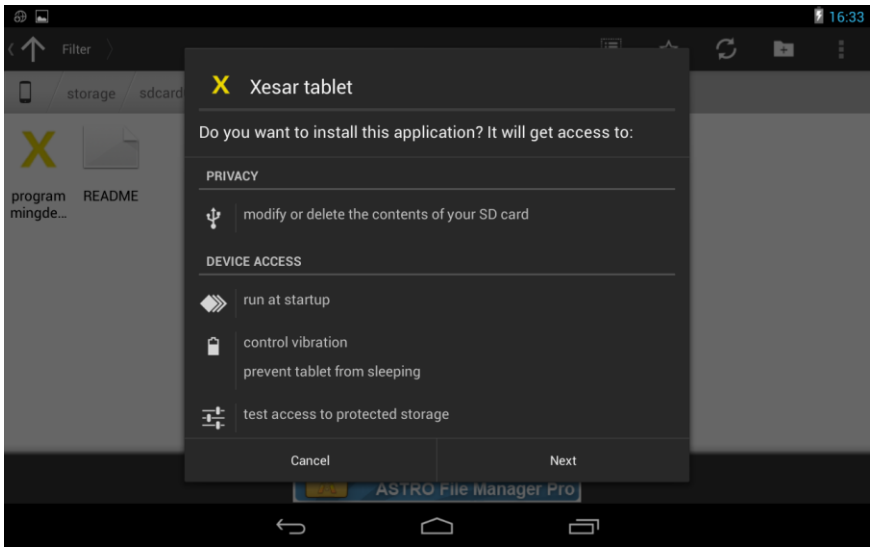



Saving screenshot...
Settings
DEVICE
Sound
Display
Storage
Battery
Apps
PERSONAL
Location access
Security
Privacy


16:32
Apps
DOWNLOADED
RUNNING
Xesar tablet
11.13MB
Internal storage
137MB used
3.8GB free







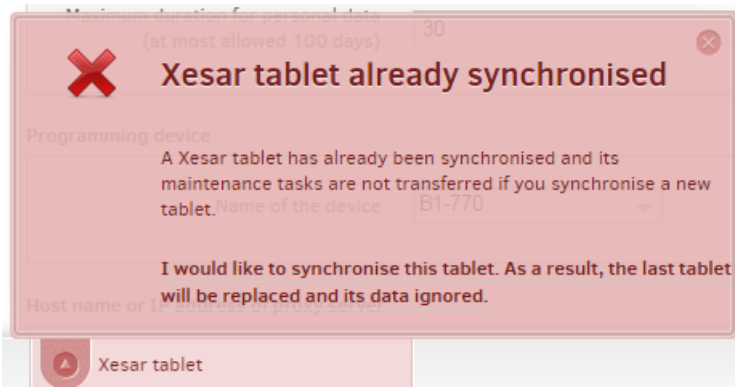


Figure 185: Manually deleting and installing the tablet app

27 List of illustrations